Authentication and Privacy Preservation in VANET

A Dissertation Report submitted

By

Thounaojam Korouhanbi Devi

to

Department of Computer Science & Engineering

In partial fulfillment of the Requirement for the

Award of the Degree of

Master of Technology in Computer Science & Engineering

Under the guidance of

Ms. Shabnam Sharma

(Assistant Professor, Lovely Professional University)

(May 2015)

INDIA'S LARGEST UNIVERSITY

LOVELY
PROFESSIONAL
UNIVERSITY

Transforming Education, Transforming India

School of: COMPUTER SCIENCE & ENGINEERING

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: THOUNAOJAM KOROUHANBI DEVI
Registration No: 11311289

Batch: 2013-2015
Roll No. 67

Session: 2014-2015
Parent Section: K2307

Details of Supervisor:
Designation: AP

Name SHABNAM SHARMA
Qualification: M.Tech

U.ID 14593
Research Experience: 01

SPECIALIZATION AREA: Network Security (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

1. Authentication & Privacy Preservation in VANET.
2. Security aspects in adhoc network
3. Communication Model in Adhoc Network

Shabnam 14/5/13
Signature of Supervisor

PAC Remarks: New method of group formation (cluster) will be the outcome of this research & definitely research paper will be published in the journals of Thomson Reuter.

11/10/14

APPROVAL OF PAC CHAIRPERSON: Signature: 11/10/14 Date:

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)

*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.

*One copy to be submitted to Supervisor.

CERTIFICATE

This is to certify that **Thounaojam Korouhanbi Devi** has completed M.Tech dissertation titled "**Authentication and Privacy Preservation in VANET**" 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 the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation is fit for the submission and the partial fulfillment of the conditions for the award of M.Tech in Computer Science and Engineering.

Date:

Signature of Advisor

Name: Shabnam Sharma

UID: 14593

ABSTRACT

Vehicular ad-hoc network is an emerging technology that has high applicability in our day to day life. One of the most intriguing issues in the implementation of VANET is to provide security. This study mainly focuses on the security issues in VANET in relation to authentication and privacy preservation in VANET. Vehicles need to be authenticated to ensure that the right message is received and the communicating entities are the ones as claimed. This study proposes a new cluster formation scheme for VANET. The generators of the group are calculated using cyclic additive group concept. Once, the group leaders i,e the cluster heads are selected, the remaining vehicles that comes under that range becomes member of that cluster. Grouping vehicles into clusters aids in group authentication of message. Group signing and batch verification of messages ensures preserving the privacy of vehicles. Privacy preservation deals with anonymity. This prevents an unauthorized third party from gaining information about vehicle ID, driver or the location.

ACKNOWLEDGEMENT

I feel great pleasure in submitting this report as the culmination of my guide’s efforts. This required a very hard work, sincerity and devotion that I tried my best to put in my work and in turn gained a lot of knowledge and confidence from this analysis

I am deeply grateful to my mentor respected **Miss Shabnam Sharma, Assistant Professor, CSE/IT, LPU** who has helped me in each and every step till the begin till now. She has been a constant guiding force and source of illumination for me. It entirely goes to her credit that this work has attained its final shape. I would like to thank her for her valuable advice and guidance. I would also like to thank all my friends who were always there to motivate me in every step. They helped me a lot, also thanks to all those persons who are directly or indirectly involved in completing my work.

Thounaojam Korouhanbi Devi

Regd. No. 11311289

DECLARATION

I hereby declare that the dissertation entitled, "**Authentication and Privacy Preservation in VANET**" submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date:

Thounaojam Korouhanbi Devi

Regd. No. 11311289

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION

Wireless Ad-hoc Network (WANET) is a variant of wireless network which relies on infrastructure-less network. WANET consist of Wireless Mesh Networks (WMN), Wireless Sensor Networks (WSN) and Mobile Ad-hoc Networks (MANET). Vehicular Ad-hoc network (VANET) is subpart of MANET.

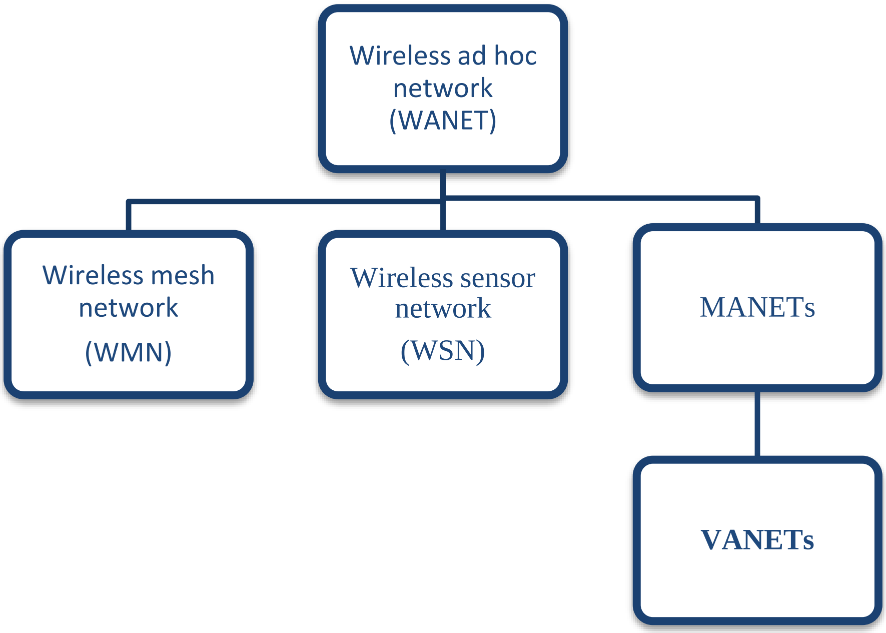

Wireless ad hoc network (WANET)
Wireless mesh network (WMN)
Wireless sensor network (WSN)
MANETs
VANETs

Figure 1.1: Types of Wireless Network

1.1 Ad-Hoc Network

Ad-hoc networks are also referred to as infrastructure-less network, where no fixed infrastructures such as access points are used for communication. It is network which can self-organize and doesn’t require any central administration for controlling and managing it. It is a sort of temporary network which is mostly deployed during emergency situations. It is further categorize into three divisions as shown in fig 1.

These three divisions are listed below:

- Wireless Sensor Network
- Wireless Mesh Network
- Mobile Ad-hoc Network

1.1.1 Wireless Sensor Network (WSN)

WSN is a network, in which hundreds to thousands of sensor nodes communicate with each other using wireless medium. Size of sensor nodes varies, it can be like a dust particle which is not easily visible to naked eye or it can be large. Transmission range of nodes is limited and so it requires intermediate nodes to transfer data from source to destination node. In this, sensor nodes collect the information and then forward that information to particular node which is known as sink node. Nodes can be homogenous or heterogeneous. WSN has various applications for example to detect earthquake, this type of sensor network is used.

1.1.2 Wireless Mesh Network (WMN)

In this radio hubs are arranged in a mesh topology. The components of WMN are gateways, mesh router and mesh client. Mesh clients are end devices such as computer, mobile phone etc. Mesh router are responsible for routing of traffic. WSN is a reliable and dependable network. If there is any interruption in the route it can self -structure itself.

1.1.3 Mobile Ad-hoc Network (MANET)

In this, mobile nodes are communicating with each other without any fixed infrastructure. In this, nodes that are in range of each other will communicate directly, and other uses the intermediate nodes for communication. In figure 2, node A want to communicate with B, both are in direct range, so they communicate directly. In figure 3, node A wants to communicate with D node, but D node is not in range of A node so it uses node B and C as intermediate node to send data to D node. It is self-organized, adaptive and infrastructure less network and the nodes are able to detect the presences of other nodes.

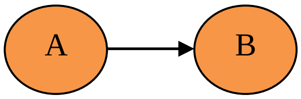


Figure 1.2: Direct communication between nodes

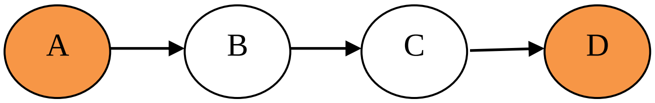


Figure 1.3: Communication by using intermediate nodes

1.2 Vehicular Ad-hoc Network (VANET)

New trends and recent development in wireless communication, vehicles industries and telecommunication manufactures led to the development of Vehicular Ad Hoc Network (VANET). VANET can be considered as an application of Mobile Ad Hoc Network (MANET). It uses moving vehicles as mobile nodes in MANET to create a network. Every vehicle under the range of 100-500 metres forms a node and becomes a participant of the VANET network. Vehicles that are within the specified range can send information and share other things. As vehicle drives out of this range it falls out of the network. It then becomes part of other network where it fits. Communication in VANET can take place in three ways viz. vehicle-to-vehicle, vehicle-to-roadside and routing based.

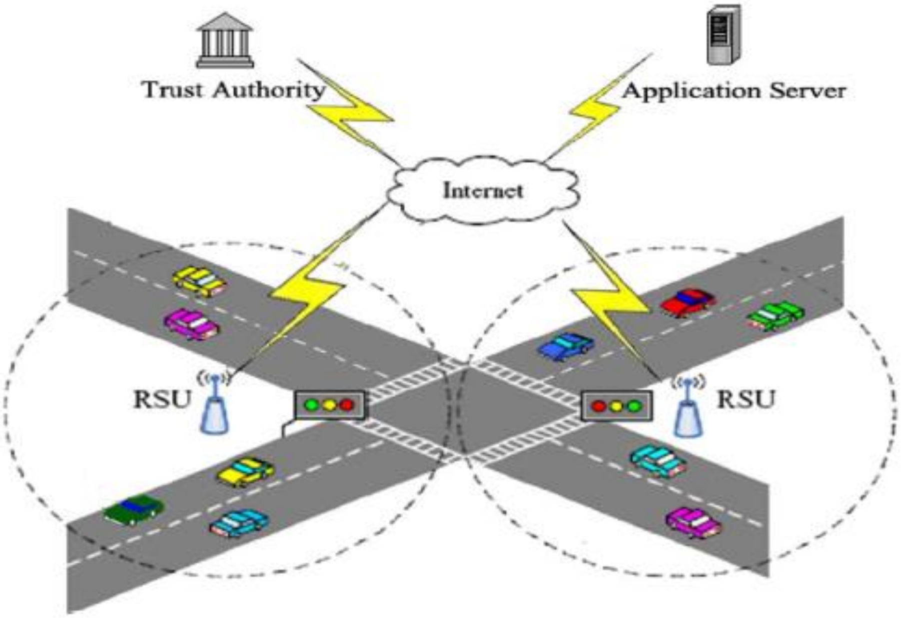


Figure 1.4: VANET network model (Sherali Zeadally, 2010)

1.3 VANET Architecture

A VANET uses cars as mobile nodes in a MANET to create a mobile network. All the participating cars are turn into a wireless router or node, allowing cars in the range of approximately 100 to 500 meters of each other to connect and create mobile vehicular network. The cars are moving in high speeds. As vehicles moves out of the network range and it drops out of the current network, other vehicles entering the specified range can join in. Advanced wireless communication devices are placed on the vehicle to aid them. In VANET any vehicle can act as a sender, receiver, or router to share information within the vehicular network. This information is then use to ensure road safety or free-flow of traffic.

The main components of VANET are:

1.3.1 On Board Units (OBUs): These are the communication devices mounted on vehicles to facilitate communication with other vehicles and roadside units. They enable short-range wireless ad hoc networks to be formed.

1.3.2 Roadside Units (RSUs): These are the communication units located aside the road that connects with the application server and the trust authority. They facilitate communication. The number and distribution of RSUs depends on the communication protocol to be used. Some protocols requires RSUs to be distributed evenly throughout the whole road network, some requires RSUs only at intersections, while others require RSUs only at region borders.

1.3.3 Trusted Authority (TA): They are third party entrusted with the job of generating certificate, distribution of certificate to authentic entity and maintain revocation list.

VANET working principle

I. A router called as Road Side Unit (RSU), where it connects the vehicular on the road with other network devices (base station).

II. Each vehicle has On Board Unit (OBU), where it connects the vehicle with RSU via DSRC radio.

III. Each vehicle has Tamper Proof Devices (TPD), where it holds vehicle secrets such as driver’s identity, speed, acceleration, route etc.

1.4 Communication Configuration in VANET:

Communication in VANET can be configured in three ways. These ways are listed below:

1.4.1 Inter-Vehicular communication (IVC): Vehicles within the specified range communicates with one another. Such type of communication configuration is also termed as Vehicle-to-Vehicle communication (V2V). It uses multi-hop multicast/broadcast to transmit traffic related information over multiple hops to a group of receivers. In IVC messages can be forwarded in two ways viz. naïve broadcasting where vehicles send broadcast messages periodically at regular intervals and intelligent broadcasting where vehicles send limited number of messages for a given emergency event.

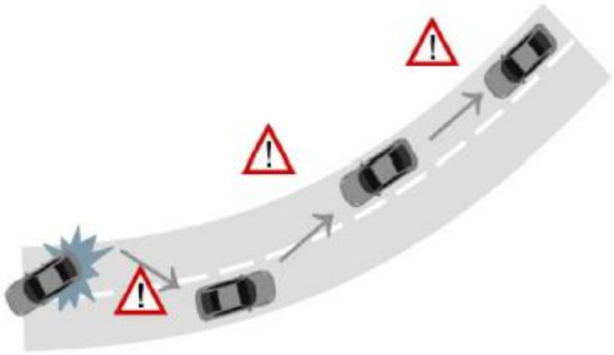


Figure 1.5: Inter-Vehicular Communication (Sherali Zeadally, 2010)

1.4.2 Vehicle-to-Roadside communication (VRC): Vehicles communicates with the infrastructure located aside the road that facilitates communication. This communication configuration is also referred to as Vehicle-to-Infrastructure communication (V2I). VRC represents a single hop broadcast where the RSUs send a broadcast message to all equipped vehicles in its range.

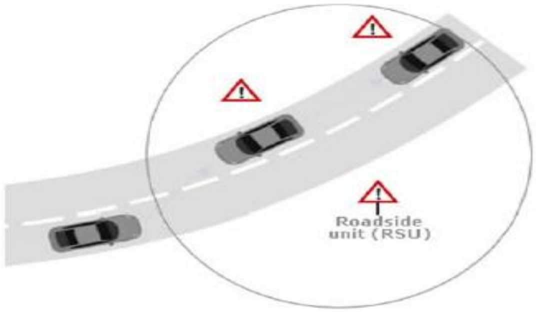


Figure 1.6: Vehicle-to-roadside communication (Sherali Zeadally, 2010)

1.4.3 Routing-based communication: This is a multi-hop unicast where a message is forwarded in a multi-hop fashion until the vehicle carrying the desired data is reached. When vehicle having the desired data receives the request, it immediately replies with a unicast message comprising of the desired data to the vehicle from which it has received the message, which is then forwarded till the vehicle that had generated the message receives it.

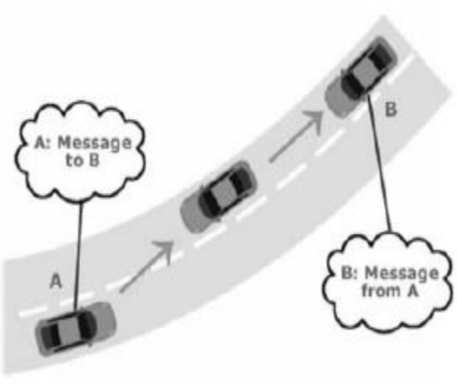


Figure 1.7: Routing-based communication (Sherali Zeadally, 2010)

1.5 Standards for wireless access in VANETs

Standards that have been specified for implementing VANET in a reliable way are dedicated short range communication (DSRC) and IEEE 1609-standards for wireless access in vehicular environments (WAVE) (IEEE 802.11p). These standards provides various protocols that ranges from protocols applicable to Transponder equipment and communication protocols through security specification, routing, addressing services, and interoperability protocols.

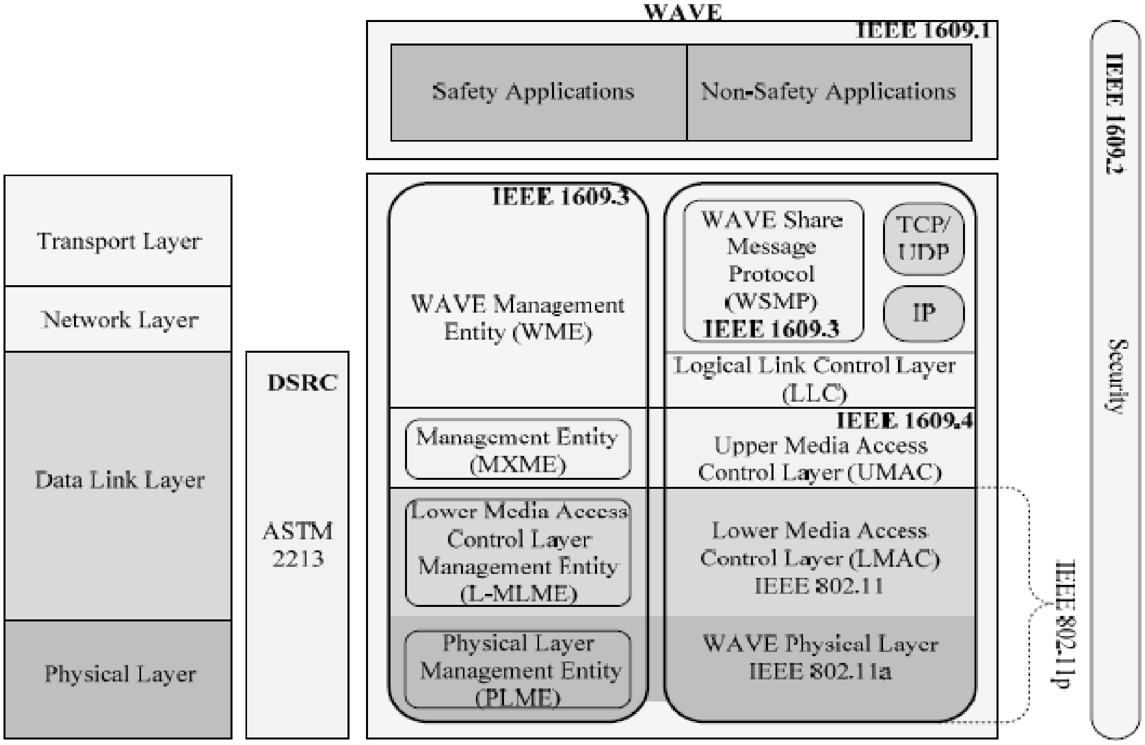

WAVE
IEEE 1609.1
Safety Applications
Non-Safety Applications
IEEE 1609.2
Security
Transport Layer
Network Layer
Data Link Layer
Physical Layer
DSRC
ASTM 2213
IEEE 1609.3
WAVE Management Entity (WME)
WAVE Share Message Protocol (WSMP)
IEEE 1609.3
TCP/ UDP
IP
Logical Link Control Layer (LLC)
Management Entity (MXME)
IEEE 1609.4
Upper Media Access Control Layer (UMAC)
Lower Media Access Control Layer Management Entity (L-MLME)
Lower Media Access Control Layer (LMAC) IEEE 802.11
Physical Layer Management Entity (PLME)
WAVE Physical Layer IEEE 802.11a
IEEE 802.11p

Figure 1.8: Wireless access in vehicular environments (WAVE) IEEE 1609, IEEE 802.11p and the OSI reference model (Sherali Zeadally, 2010)

1.6 VANET Application

VANETs provide the user with a broad range of applicability comprising of both safety related application and non- safety related application. Two applications categories where VANET plays crucial role are:

1.6.1 Safety Related Application

Safety related applications as the name suggests are used to provide safety on the road. This application mainly deals in preventing road accidents, providing a safe route etc. This class of application can be further divided into sub classes listed below.

- **Collision Avoidance:** More than 60% of accidents on the road will be avoided if they get warning message before they collide with each other. If the car or vehicle driver gets warning at right time then the collision can be avoided.

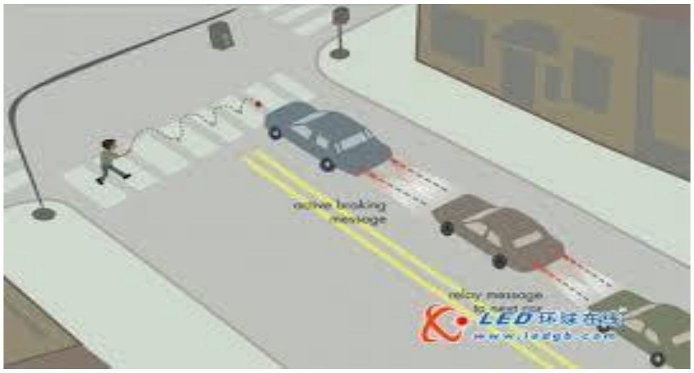


Figure 1.9: Collision Avoidance in VANET

- **Cooperative driving:** Drivers get messages for traffic related warnings such as lane changing or curve speed warning etc. With the help of these signals it co-operates the driver for the safe driving.

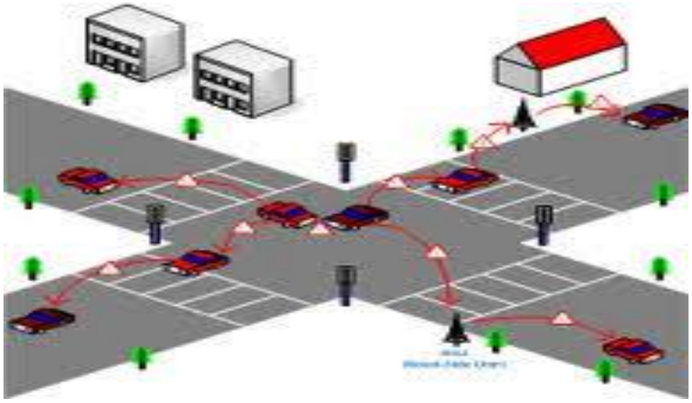


Figure 1.10: Cooperative driving in VANET

- **Traffic Optimization:** Traffic can be coordinated and controlled by sending signals like jamming, accidents etc. To the vehicles so that they can choose another path and thus save their time or avoid an accident.

1.6.2 Non-Safety Application:

Also refer to as user related application, such applications provide comfort to the users apart from safety. Further these can be classified into the following sub categories:

- **Peer to peer application:** In peer to peer application it provides the infotainment facilities like sharing music and movies among the vehicles in the network.

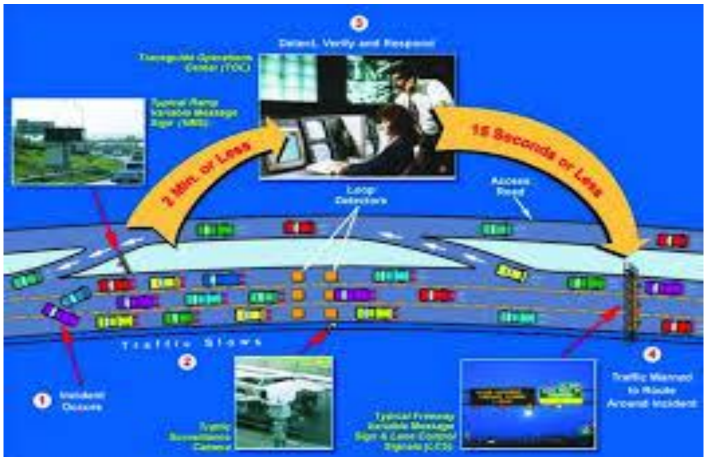

5
Detect, Verify and Respond
Transguide Operations Center (TOC)
Typical Ramp Variable Message Sign (VMS)
2 Min. or Less
15 Seconds or Less
Loop Detectors
Access Road
Traffic Slows
2
1 Incident Occurs
Traffic Surveillance Camera
Typical Freeway Variable Message Sign & Lane Control Signals (LCS)
4
Traffic Warned to Route Around Incident

Figure 1.11: Peer to Peer application in VANET

- **Internet Connectivity:** Now a day's people always want to connect to internet all the time. Hence VANET provides internet connectivity constantly without any interruption to the users.

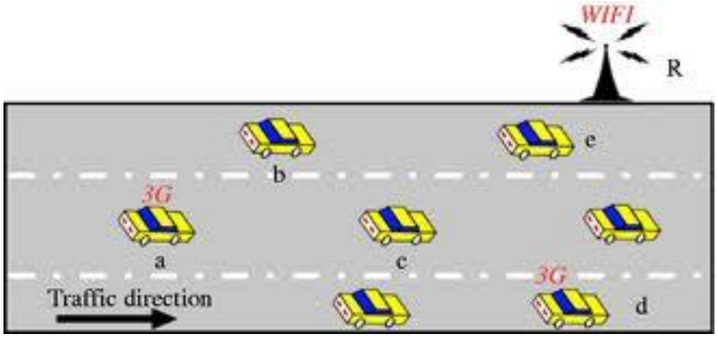


Figure1.12: Internet facilities

- **Other Services:** Other services that VANET provides to its user are services such as payment services to collect all taxes, navigation services, location-based services such as to locate vehicles to fuel station, restaurant or police station or to the fire station etc.

1.7 Security Issues: Authentication and Privacy Preservation in VANET

VANET has a wide range of applicability including both safety applications and non safety applications. Safety applications involves avoiding road accidents which is a life threatening situations, so if we want to implement VANET in such a way so as to fully utilize it we need to concentrate on the security of VANET. We need to ensure that vital information are not inserted or modified by a malicious user. The system must be able authenticate users and also should maintain their privacy. Implementing VANET in real time situation forms a large wireless network, considering the fact that vehicles forming the nodes of the VANET network are mobile, and the random topology of the vehicles, it is difficult to provide a secure network. There are three main types of attackers in VANET viz. insider versus outsider, malicious versus rational, active versus passive. Attacks in VANET can be classified into three categories viz. threats to availability, confidentiality and authenticity. This study particularly emphasizes on threats to authenticity and privacy preservation of vehicle’s identity.

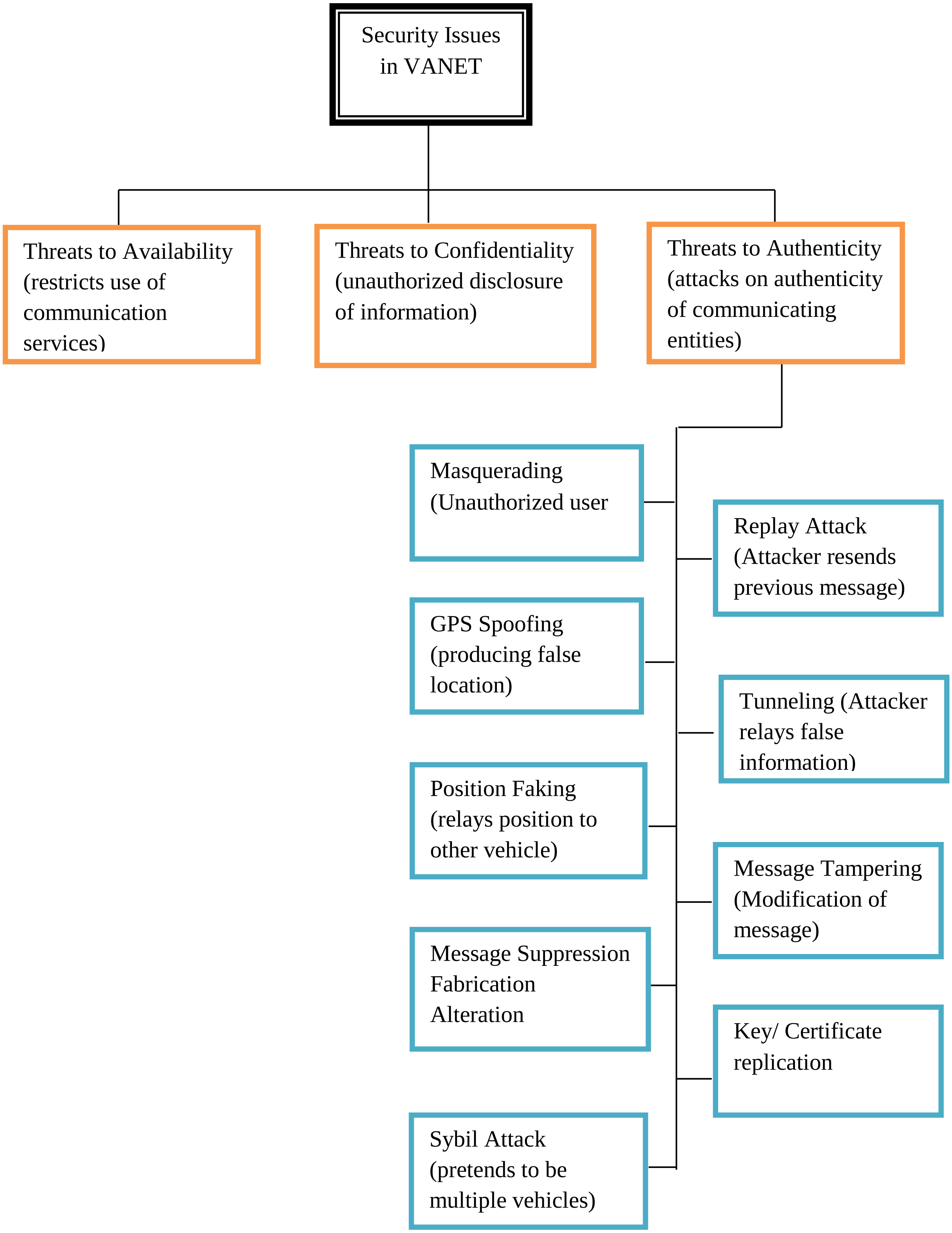

Security Issues in VANET
Threats to Availability (restricts use of communication services)
Threats to Confidentiality (unauthorized disclosure of information)
Threats to Authenticity (attacks on authenticity of communicating entities)
Masquerading (Unauthorized user
Replay Attack (Attacker resends previous message)
GPS Spoofing (producing false location)
Tunneling (Attacker relays false information)
Position Faking (relays position to other vehicle)
Message Tampering (Modification of message)
Message Suppression Fabrication Alteration
Key/ Certificate replication
Sybil Attack (pretends to be multiple vehicles)

Figure1.13: Types of security issues in VANET

Chapter 2

REVIEW OF LITERATURE

(M.Raya, 2007) suggested a scheme in which public key infrastructure is used to guarantee client legitimacy. It uses asymmetric key cryptography which uses two keys public key and private key and digital signature algorithm as the cryptographic basis. Digital signature Algorithm is used to provide message authenticity by signing the encoded message. Certificate Revocation Lists (CRLs) are maintained to keep track of invalid and misbehaving vehicles. RSUs maintain CRLs. The problem with PKI is that it requires large memory storage area for key and certificate storage.

(G.Clandriello, 2007) proposed a scheme for efficient and robust pseudonym authentication in VANETs that concerns with effective and simple to-oversee security and privacy-enhancing components as they are crucial for the widespread acceptance of VANETs. This scheme uses pseudonym authentication and group signature to provide message authentication, integrity and non-repudiation. This algorithm lessens the security overhead for safety, beaconing and retain robustness for transportation safety, even in adverse network setting. It likewise upgrades ease of use and accessibility. Further work should emphasize on system generated deployment, CRL distribution & existence of multiple CAs.

(Rongxing Lu, 2008) proposed a scheme which uses bilinear pairing and group signature as the cryptographic basis for providing fast anonymous authentication and privacy preservation, to minimize memory necessities for storing short time anonymous keys. ECPP issues on the fly short time anonymous certificates to OBUs by utilizing a group signature scheme. Since RSUs can check the legitimacy of the requesting vehicle amid the short time anonymous certificate generation phase, such revocation check by an OBU itself is not required. ECPP doesn't provide unlinkability and traceability under practical presumption.

(Ahren Studer, 2009) came up with a new scheme using TESLA++ and signature called VANET authentication using signature and TESLA++ (VAST) which is an improvement to time efficient stream loss tolerant authentication (TESLA). It uses elliptic curve digital signature algorithm (ECDSA) to provide fast authentication and non-repudiation. TESLA uses symmetric key cryptography with delayed key disclosure to give fundamental asymmetry to perform broadcast authentication. Accordingly it counteracts computational DoS however it is not versatile to memory based DoS attack as the receiver needs to store the message till the key is revealed. So TESLA++ was acquainted to mitigate memory based DoS attack by simply storing self produced MAC to mitigate memory prerequisites. But again neither TESLA nor TESLA++ can provide non-repudiation so ECDSA was utilized.

(Hsin-Te Wu, 2010) proposed an authentication scheme for VANET enable the message authentication in intra and inter RSU range, and the handoff within the different RSUs. It adjusts the processing and correspondence expense and the expense of security against the attack. It protects certificates from long term exposure. This scheme likewise provides conditional privacy to abstain the exposure of the vehicles identuity. If any unexpected event that undermines the security happens then RSU will give the real identity of each vehicle. It uses Diffie-Hellman key establishment protocol for secure exchange of keys and HMAC. As Man-in the- middle attack is possible in Diffie-Hellman, this scheme will also be vulnerable to the man-in-the-middle attack, so an enhancement to this scheme may be proposed in future to prevent such attack. HMAC is a fast and effective message authentication scheme.

(Karuppanan, 2011) proposed Secure Privacy and Distributed Group Authentication for VANET which aims at providing group authentication, message integrity and conditional privacy. Conditional Privacy deals with anonymity and tracing. Anonymity refers to hiding the identity of vehicle while tracing refers to the fact that different interactions of the same vehicle cannot be related. Group authentication algorithm (GAP) is a distributed authentication scheme. It uses session based pseudonym to support anonymous communication. Batch verification method is used which helps in significantly reducing the message delay. It enables the vehicle to verify a large number of messages in the case of high vehicular density and also improves message loss ratio. GAP can efficiently handle the growing CRLs while achieving conditional traceability by the trust authority. Further enchancement in batch verification can be done in future.

(Shi-Jinn Horng, 2013) proposed an improve scheme of secure privacy enhancing communication scheme (SPECS). The cryptographic basis used for b-SPECS+ are PKI, bilinear pairing and batch verification. It is a software-based solution and doesn't rely on any special tamper-proof hardware devices on vehicle. A vehicle is permitted to create a distinct pseudo-identity for every message to ensure its privacy with respect to the genuine identity and private data by utilizing shared secrets with TA and RSU. The real identities of the vehicles can be uniquely revealed by the TA under exceptional cases. Substantial number of signature can be verified at the meantime. Any vehicle can form cluster with other vehicle and can communicate with one another safely without the intercession of RSU even in the wake of moving into the area of another RSU. It can withstand against impersonation attack. In future we have to address the problem of inside attacker about the compromised RSU or packet collisions between RSU and all vehicles within the RSU range. More assessment on vast scale VANETs should likewise be done.

(Albert Wasef, 2013) proposed an expedite message authentication protocol for VANET (EMAP) which replaces the time consuming CRLs checking process by an efficient revocation checking process. It uses keyed HMAC, where the key used in calculating the HMAC is shared only between non-revoked OBU. It uses a novel probabilistic key distribution which enables non-revoked OBUs to securely share and update a secret key. This system significantly decreases the message loss ratio due to the message verification delay compared with the conventional authentication methods employing CRL. It is a secure an efficient authentication scheme for VANET. It is the first work that proposes a rekeying mechanism capable of updating compromised keys corresponding to previous missed rekeying process. The modular feature of this scheme makes it easily integrable with any PKI system. It doesn't require any modification to the core of the PKI architecture. It only needs a key distribution module to be added to the TA during system initialization. Thus it is suitable for any network employing PKI. It is resistant to forging attacks, replay attacks and colluding attacks. It guarantees forward secrecy.

(Xuedan Jia, 2013) suggested a new scheme for authentication in VANETs called Efficient privacy preserving authentication scheme for VANETs-based emergency communication (EPAS) which is an efficient identity based signature scheme which satisfies conditional privacy requirements through software solution. EPAS contains two efficient communication patterns viz. vehicle-to-disaster relief authority (DRA) and vehicle group communication. We employ both lightweight signature and batch verification to provide effective authentication. There is no delivery and management of certificates. Point multiplication instead of bilinear operation is used to generate lightweight signature saving computation overhead and communication overhead. Specific to the privacy destruction problem caused by key preload, session key agreement protocol is proposed to establish an individual session key between vehicle and the credible authority. This provides conditional privacy protection. EPAS uses pseudonym based signature to prevent the leak and tracking of vehicle's privacy information efficiently. The performance analyses are not very comprehensive so need to explore the specific revocation mechanism.

(Hui Zhu, 2013) proposed the Privacy preserving authentication scheme (PPAS) that performs local authentication and roaming authentication based on bilinear pairing. It makes use of bilinear pairing and ECDSA. It provides an effective protection of privacy and anonymity among vehicles and infrastructure. Anonymous authentication is one of the significant methods to preserve privacy, which is a key problem of large scale application of VANET.

(Liu, 2013) proposed a scheme which provides fast mutual authentication between vehicle and RSU. LIAP employs dynamic session secret process which utilizes a dynamic sequence with one time pad properties as authentication credentials and challenge response procedure for authentication. LIAP uses a common secret key so there is no need for key exchange process between vehicle and RSU. The authentication credentials are pre deployed at RSU. This scheme provides efficient and confidential authentication. It also prevents from malicious attack.

(Lai, 2013) proposed a new scheme that performs batch verification. This scheme employs batch scheme based on bilinear pairing and batch authentication. This algorithm was designed to improve the quality of traffic. This scheme verifies message in group so limiting the chances of information delay. This scheme provides message authentication, privacy preservation and auditability. It also prevents replay attack. In future we can work on to identify illegal signature and designing more efficient scheme.

(M.Wang, 2014) proposed an algorithm for VANET authentication which utilizes a lightweight symmetric encryption and HMAC. It uses a self created pseudo identity to provide both privacy preservation and conditional traceability. Only the key management centre (KMC) and trusted authority can expose the identity of the vehicle from its pseudo identity. This algorithm also prevents DOS attack. Vehicles do not maintain certificate revocation list (CRL) so there is no CRL related overhead. The drawback of this system is that once the KMC is compromised the whole system doesn’t work efficiently. So to improve this scheme we need to maintain decentralized KMC or have a backup KMC.

Table 2.1: Comparison Chart of VANET Authentication and Privacy Preservation Algorithm

Sl no	**Authentication Algorithm**	**Cryptographic Basis**	**Security requirements**	**Future scopes**
1	PKI	asymmetric key cryptography, digital signature	authentication, message integrity	large key & certificates storage area
2	Efficient & Robust Pseudonym authentication	pseudonym authentication, group signature	enhances usability efficiency	system deployment, CRL distribution & existence of multiple CAs
3	ECPP	bilinear pairing, group signature	fast anonymous authentication& privacy tracking minimize required storage for short time anonymous keys	unlinkability& traceability when multiple RSUs are compromised
4	VAST	ECDSA signatures & symmetric key cryptography	DoS resilient reduces memory requirements resolves non-repudiation	No privacy preservation
5	RSU-based message authentication	Diffie-Hellman Key establishment protocol and HMAC for authentication	Enables authentication in intra & inter RSU range Enables rapid handoff Provides source authentication, message integrity, non-repudiation &anonymity	Man in the middle attack

6	GAP	Group authentication protocol, session based pseudonym, batch verification	Group authentication, message integrity & conditional privacy engages fast verification on safety messages to optimize delay	should be tested with different batch verification time slots tested using a roadway traffic simulation
7	b-SPECS+	PKI, bilinear pairing, batch verification	Overcomes impersonation attacks Prevents malicious vehicle in a group to counterfeit another vehicle to send fake messages message integrity, authentication & collusion resistance Achieves conditional privacy	Insider attack on compromised RSUs Packet Collision between RSUs & all vehicles within range Better security & efficiency Test on large scale with varying vehicle mobility model
8	EMAP	HMAC, novel probabilistic key distribution	accelerates authentication Significantly decreases the message loss ratio Proposes a rekeying mechanism resistance to common attack	certificate and message signature authentication acceleration
9	PPAS	bilinear pairing & elliptic curve	protection against forgery attack	Test with larger network

10	EPAS	identity based cryptography pseudonym based signature	allows vehicular communication in emergencies prevents leak & track of vehicle’s privacy information	performance analysis is not very comprehensive explore specific revocation mechanism
11	LIAP	Dynamic session secret process & challenge response procedure	Efficient & confidential authentication, Prevents VANET from malicious attack	Performance should be compared with other simulator
12	Toward secure batch verification with group testing for VANET	Bilinear pairing, batch authentication & batch verification	Message authentication, privacy preservation & auditability	Identify illegal signature & design more efficient scheme
13	LESPP	HMAC & Symmetric encryption	Authentication, privacy preservation & DOS resilience	Backup KMC or Distributed KMC

Chapter 3

PRESENT WORK

3.1 Problem Formulation

VANET forms a vast network of vehicles where the vehicles can communicate with one another. This communication channel can be compromised. Attacker can try to mislead vehicles by either modifying the messages sent between the vehicles, or by claiming to be an authentic user etc. Research are being conducted with the objectives to provide a secure scheme in which vehicles can communicate freely and there communication will not be compromised. Authentication scheme ensures us that the communicating entities are the ones that it claims to be. There are a number of ways in which an attacker can try to claim to be one of authorized entity. This study focuses on studying and analyzing various secure authentication schemes for VANET. This study aims to analyze the performance of group authentication protocol for VANET and propose an enhancement in group authentication to increase efficiency of the protocol for VANET.

3.2 Objectives

1. To study authentication and privacy preservation schemes for VANET.
2. To form cluster of vehicles.
3. To select a cluster head.

3.3 Research Methodology

The first step is to study VANET, its architecture and applications. The next step is to study the various security issues and threats in implementing VANET. Then in the third step different type of authentication schemes are studied. Further a comparison is drawn out of all the authentication schemes. This is represented in a comparison chart. The main focus is to provide a security scheme that offers authentication and privacy preservation.

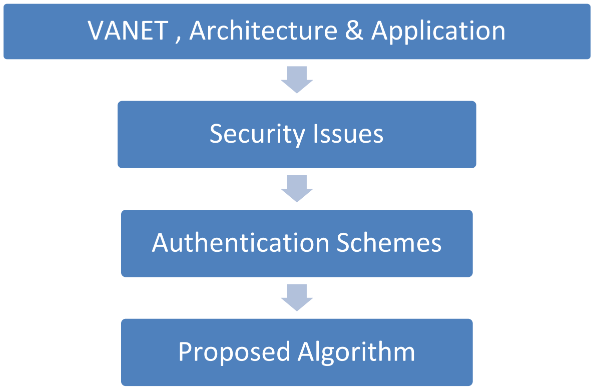


Figure 3.1: Research Methodology

The proposed algorithm aims to provide an efficient scheme for authentication and privacy preservation in VANET based on group authentication scheme. Firstly the user forms a message, M consisting of timestamp Ts, vehicle's number N and a randomly generated prime number P of the form $M=\{T_s,N,P\}$. This message is then encrypted using RSU's public key PU_{RSU}. The encrypted message is then forwarded to the RSU where it is decrypted using its Private key PR_{RSU}. Then the user is authenticated by comparing N with information stored in the database. Once valid users are recognized RSU calculates multiplicative inverse of P, MI_{RSU} generates unique identification number, UID for every new user registered. This information is forwarded to user. The user than computes multiplicative inverse of its P, MI_U and is compare with MI_{RSU}. The maximum number of users forming a group is determined. Group generators are calculated and one of it is selected as group leader and vice leader. After this member of the group are computed.

3.3.1 Proposed Algorithm

The proposed algorithm comprises of the following steps:

1. Vehicle Authentication

The user creates a message, M consisting of timestamp T_s, vehicle's number N and a randomly generated prime number P of the form $M=\{T_s,N,P\}$. This message is then encrypted using Public key, PU_{RSU}. For encryption we use RSA algorithm. The encrypted message is then forwarded to the RSU where it is decrypted using Private Key, PR_{RSU}. The user is authenticated by comparing N with information stored in the database. Once the authenticity of the user is proved, RSU calculates the multiplicative inverse, MI_{RSU} generates unique identification number, UID for every new user registered. This information is forwarded to user. The user then computes multiplicative inverse of its P, MI_U and is then compared with MI_{RSU}. If the exact match is found, then, further operations are executed otherwise, the request is rejected.

2. Selection of Group Leader

From group, $G=\{Z_N,+\}$,where Z_N denotes the maximum number of vehicles that are the part of From group, $G=\{Z_N,+\}$,where Z_N denotes the maximum number of vehicles that are the part of same group, selection of Group Leader and Vice Group leader is done on the basis of Cyclic Group Property with respect to additive operation. Cyclic group is a group that is generated by a single element g, called the generator of the group. All the elements of the group may be obtained by repeatedly applying the group operation or its inverse to g. More than one generator may exist in a group. In such case, once of the generator is selected as the group leader and the other is elected as vice leader.

3. Determine Group member

Once group leader is determined, all the remaining vehicles that belong to the group become the members of the group.

4. Further operation

Once the cluster is formed and a cluster head is selected, it can be utilize to perform group message signing and verification.

Algorithm:

```
Begin
      Vehicle input $M = \{T_s, N, P\}$
      Perform encryption $e = E(M, PU_{RSU})$
        Forward k to RSU
        RSU perform decryption $d = D(e, PR_{RSU})$
        Compare N with stored information in database
        If N is valid then
            Calculate $MI_{RSU}$, generate UID
            Forward UID, $MI_{RSU}$ to user
            User computes $MI_U$
            If $MI_{RSU} = MI_U$then
                  Keep UID, determine maximum member of group
                  Compute group generator, assign group leader, vice leader
                  Generate member of group
                  Perform further operation
            End if
            Else
                  Reject the request
        End if
        Else
              Reject the request, update CRL
End
```

3.3.2 Flowchart

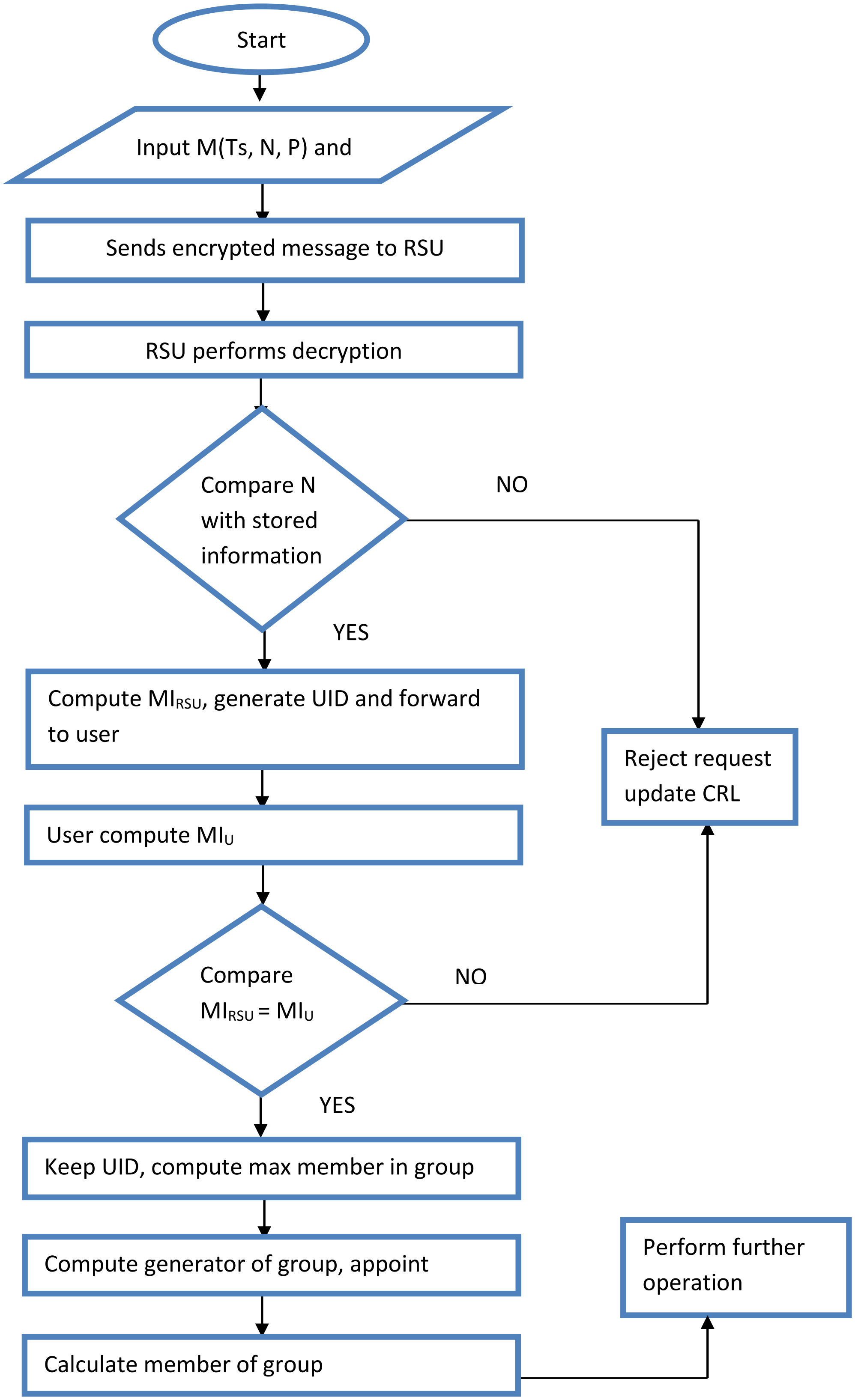

Start
Input M(Ts, N, P) and
Sends encrypted message to RSU
RSU performs decryption
Compare N with stored information
NO
YES
Compute MI_{RSU}, generate UID and forward to user
Reject request update CRL
User compute MI_U
Compare $MI_{RSU} = MI_U$
NO
YES
Keep UID, compute max member in group
Compute generator of group, appoint
Perform further operation
Calculate member of group

Figure 3.2: Flowchart of Proposed Algorithm

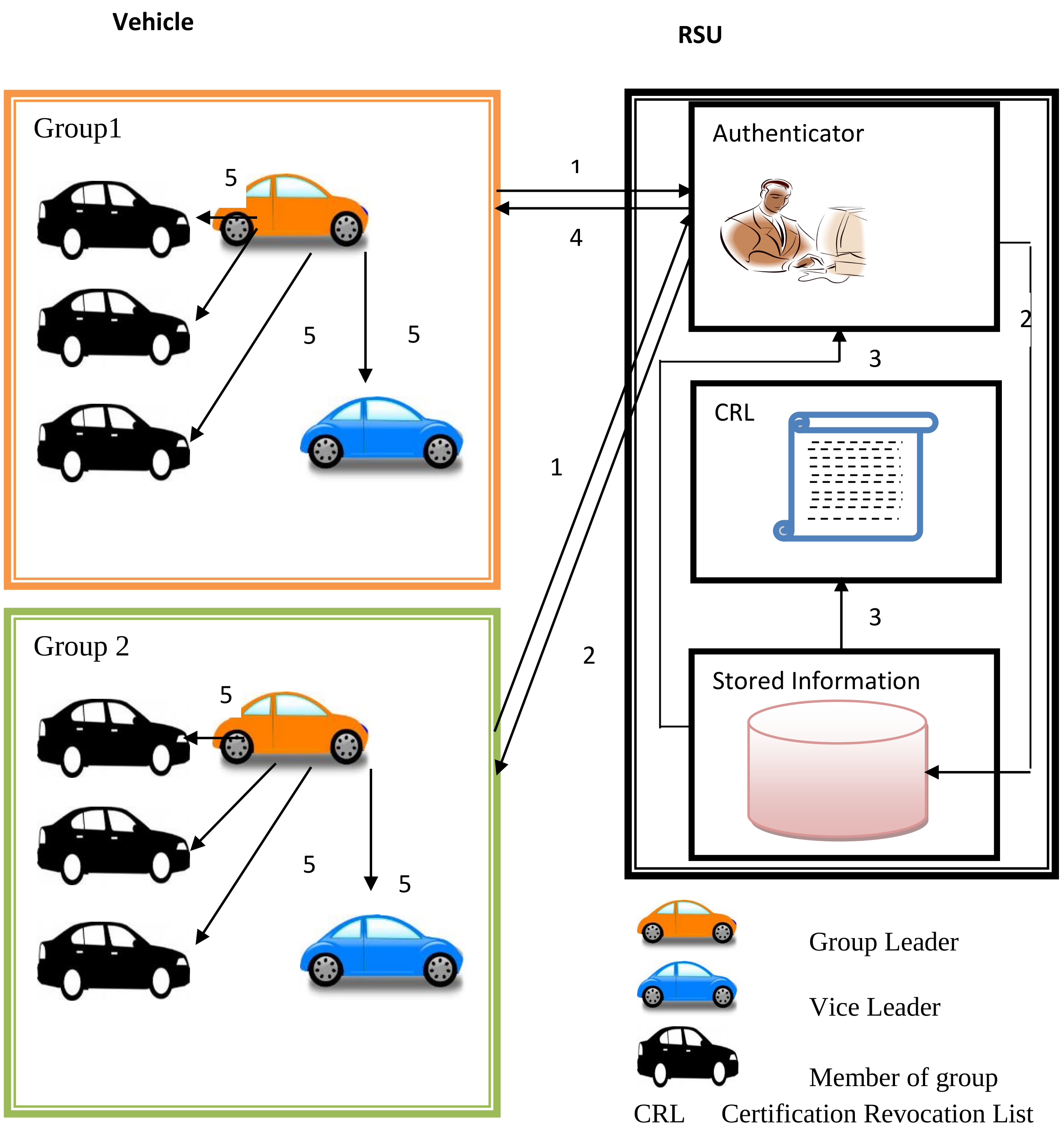


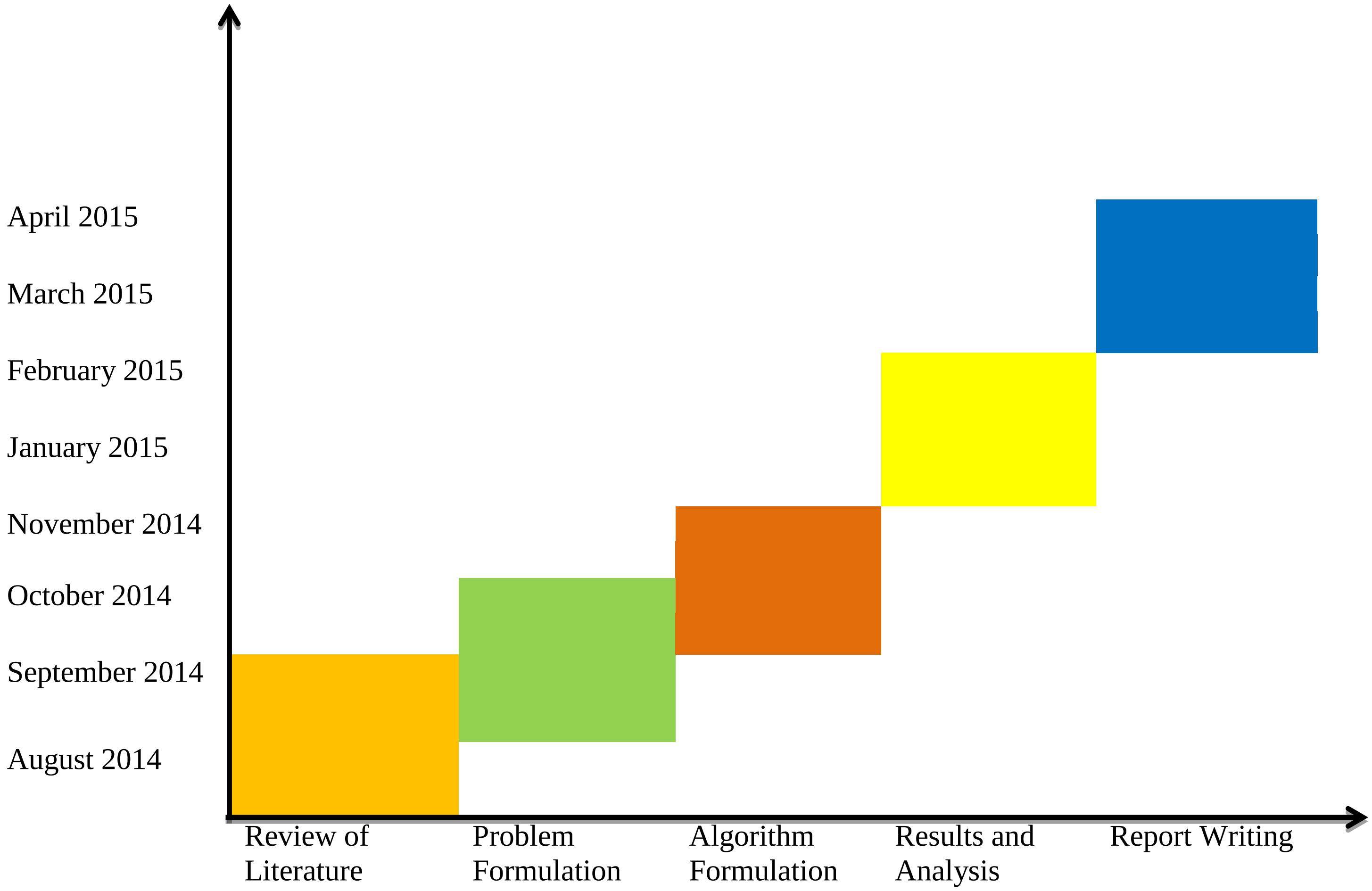
Figure 3.3: Diagrammatical representation of Proposed Algorithm

1. Vehicles forwards encrypted message to RSU.
2. RSU decrypts it, authenticator compares with the stored information
3. If it is valid then request is accepted else rejected and CRL is updated
4. Information forwarded to vehicles
5. Vehicles forms group, group leader and vice leader are assigned

3.4 TOOL: MATLAB

MATLAB is the abbreviation for matrix laboratory. It is a 4th generation high level programming language developed by MathWorks. It provides an interactive environment for numerical computation, visualization, iterative exploration, programming, application development, design and problem solving. MATLAB has a wide range of pre-defined library functions that help us to implement complex problem in simple way. It provides built in tools and graphics that help in creation of custom plots and visualization of data. Applications with graphical user interfaces can be built with the aid of various tools available in MATLAB. The programming interface of MATLAB provides development tools which improves code quality and performance. Algorithms implemented using MATLAB can be easily integrated with other external applications and languages such as C, JAVA etc. Simulation and Model-Based Design generally called Simulink is integrated with MATLAB which aids us in designing model and simulating the model. In the current scenario MATLAB has become one of the most used computational tools in science and engineering. MATLAB has a wide range of application such as implementing image and video processing, computational finance neural network, computational biology, mathematical computation, control system, database connectivity and reporting, vehicular network etc. MATLAB will be an ideal tool for implementing the proposed scheme.

3.5 TIMELINE CHART



Chapter 4

RESULT AND DISCUSSION

This chapter discusses the results that are obtained during implementation of the proposed algorithm in MATLAB. The variation in the time taken for formation of cluster and selection of cluster with respect to different number of vehicles has been analysed.

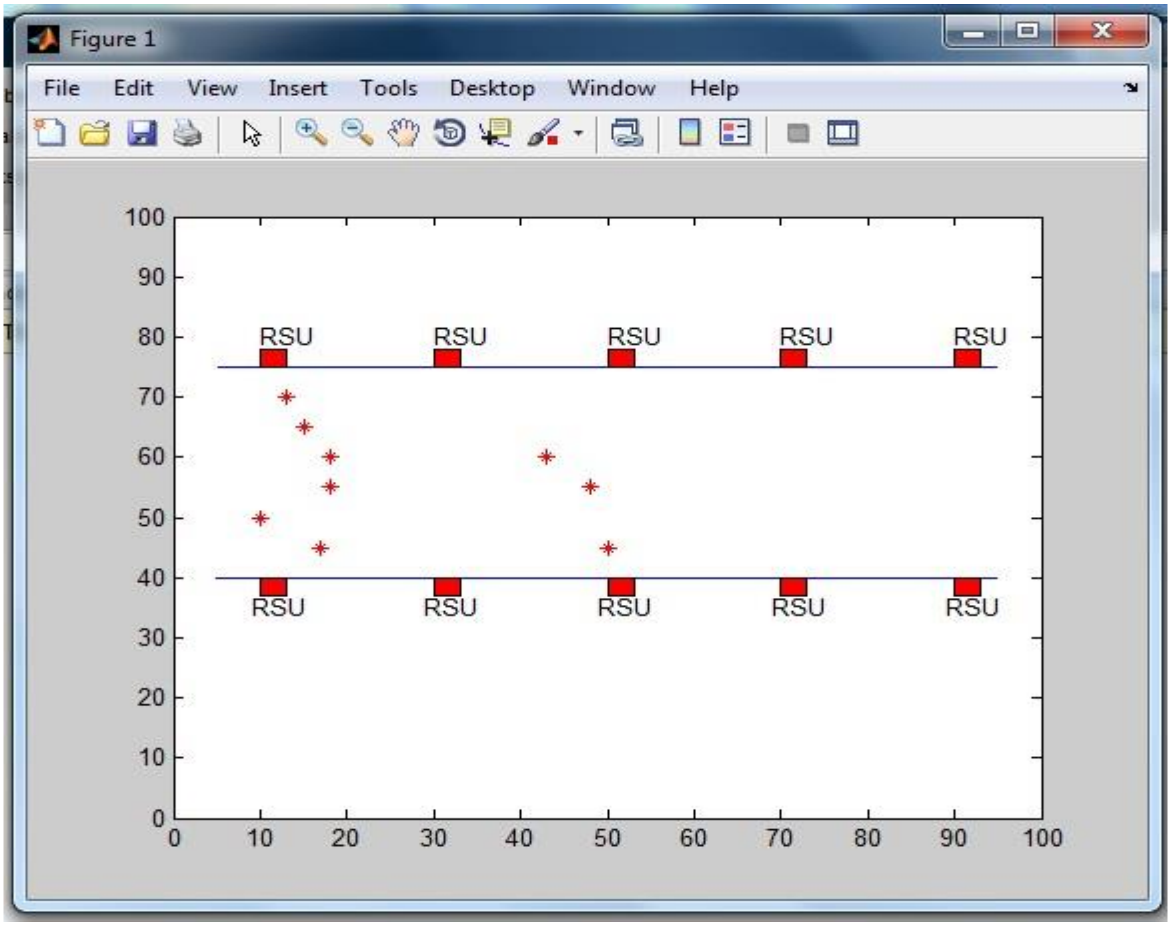
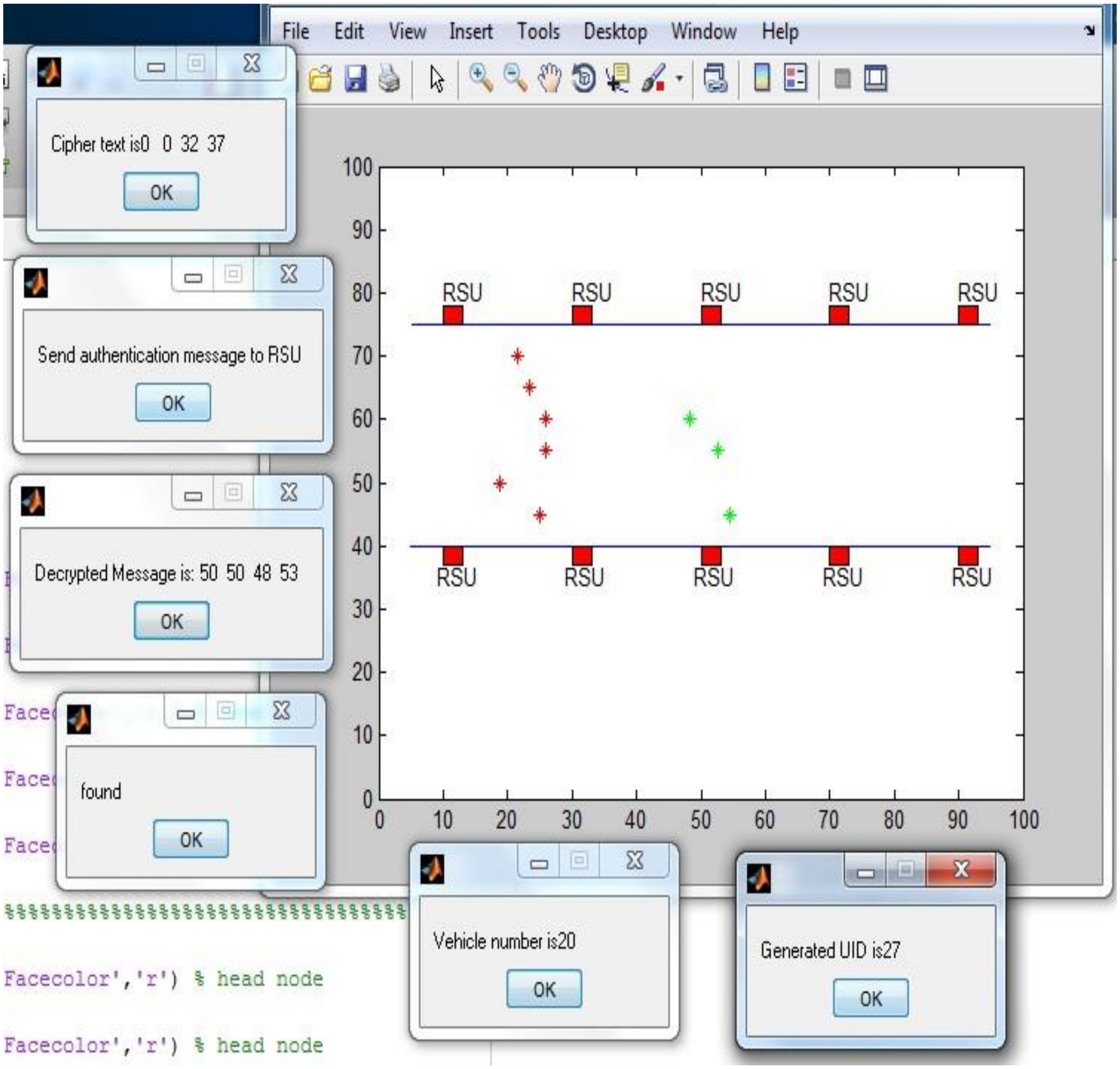


Figure 4.1: Vehicles on the road

The above figure represents the simulation of VANET in MATLAB. Asterick (*) represents vehicles and rectangle represents the roadside units.



Cipher text is0 0 32 37

Send authentication message to RSU

Decrypted Message is: 50 50 48 53

found

Vehicle number is20

Generated UID is27

```
Face
Face
Face
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
Facecolor','r') % head node
Facecolor','r') % head node
```

Figure 4.2: New vehicles joining the network register itself with the RSU.

As shown in the figure 17, new vehicle that joins the network registers itself to its nearest RSU. To authenticate vehicle will send its credentials, comprising of timestamp, vehicle number and a prime number to RSU unit. This message is encrypted using RSA algorithm. The RSU decrypts the message and checks its validity. If the vehicle is valid then a UID is generated.

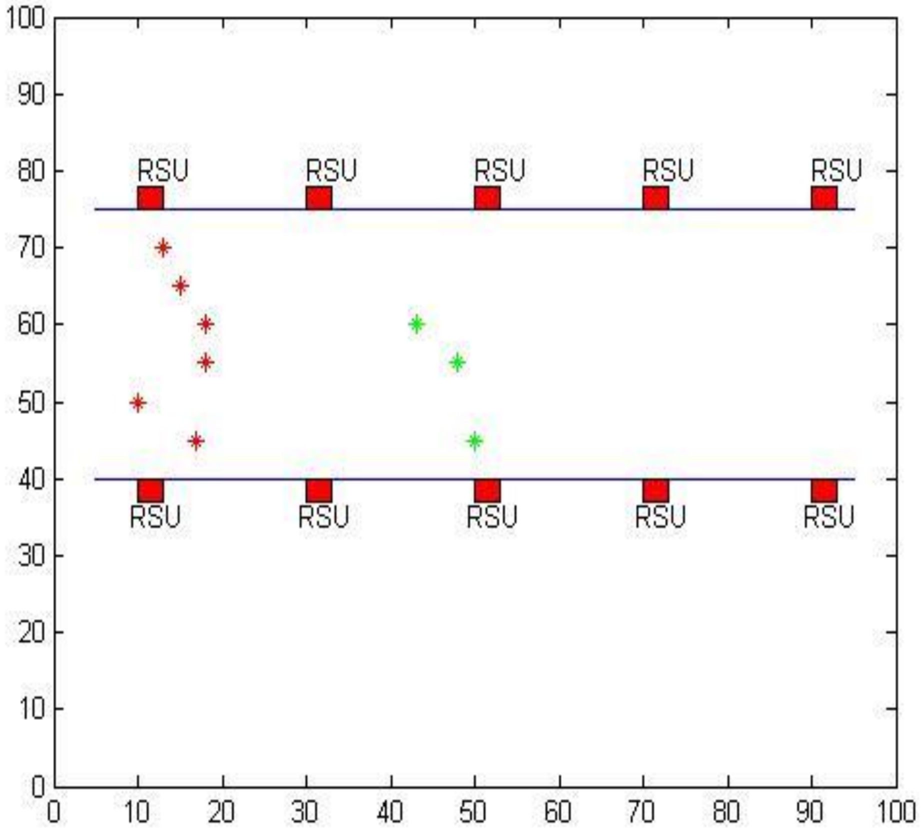


Figure 4.3: Vehicles on the road.

As illustrated in figure 18, the cluster formation process is successfully implemented. The cluster is formed based on location i,e coordinates. Two clusters are formed and is depicted by different colours.

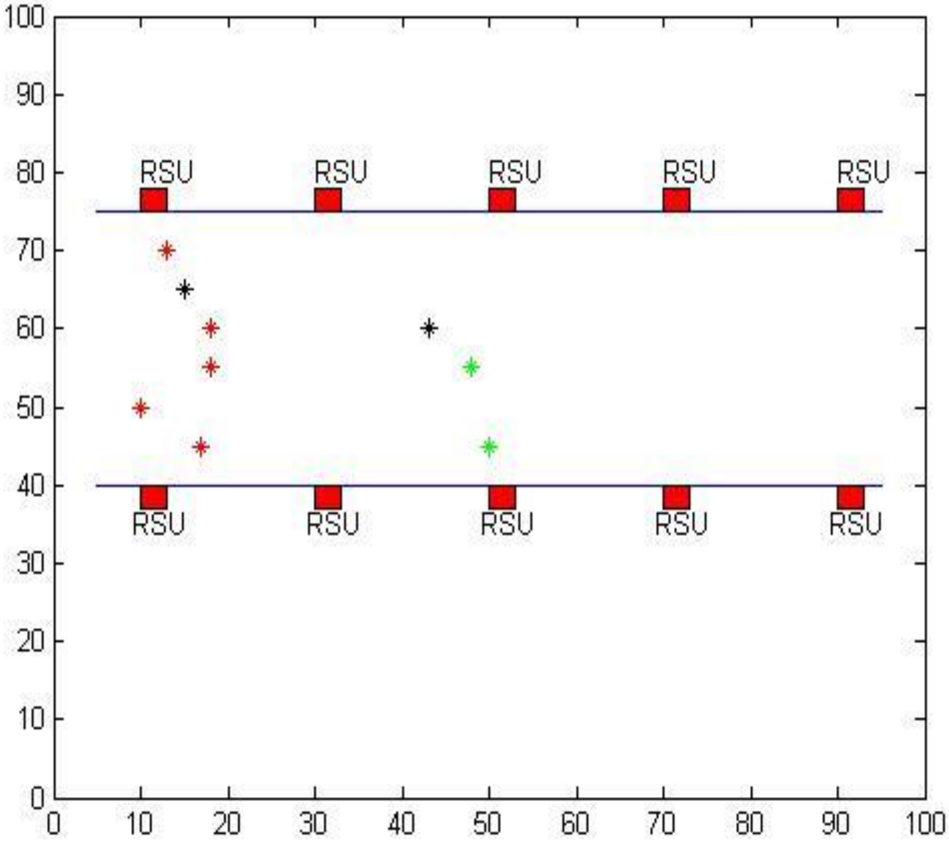


Figure 4.4: Selection of cluster head

After the formation of cluster, the next step is the selection of cluster head for each cluster. Figure 19 represents the selection of cluster head. The RSU keeps a count of the vehicles that are in its range. This count value is taken as the maximum number of vehicle in the group. Cluster heads are selected by using cyclic group concept under additive property. Black colour in each group depicts the cluster head.

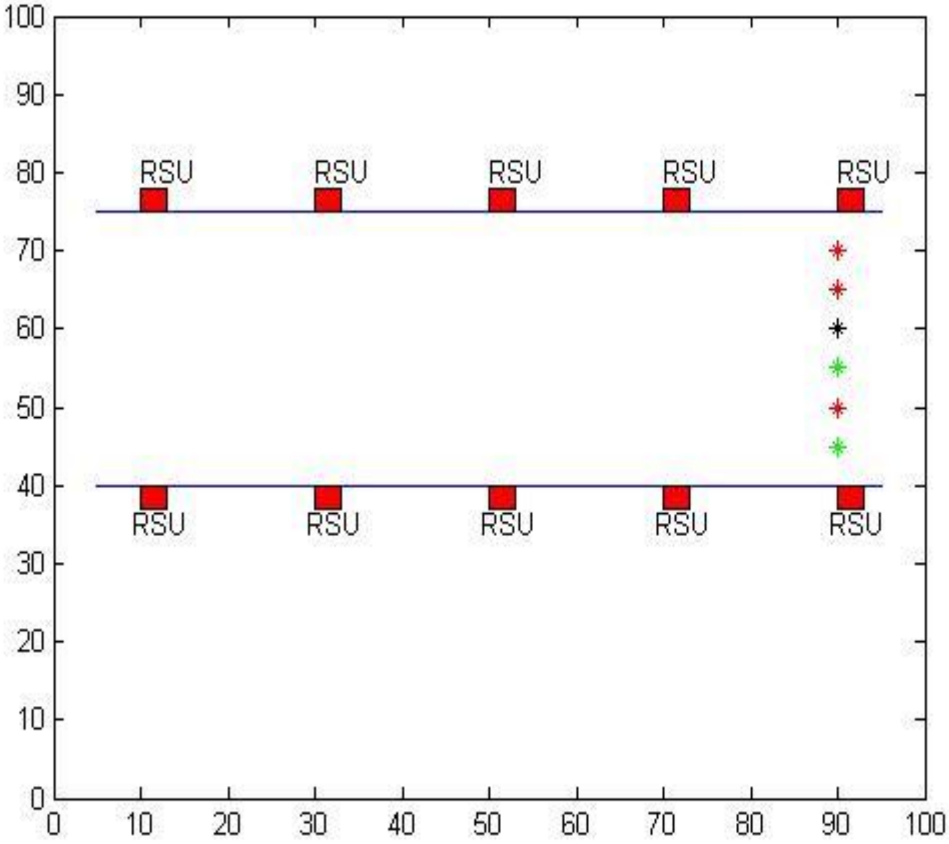


Figure 4.5: One of the vehicles becomes the cluster head

The vehicles will move and cluster heads will retain its position. If all the vehicles come under one cluster then one of the vehicles which is more stable, among the two cluster head will be chosen as the cluster head.

Table 4.1: Encryption and Decryption time recorded during simulation

Process	Time (Seconds)
Encryption	0.10178
Decryption	1.8713

Table 1.2: Time Taken for cluster Formation w.r.t no. of vehicles

No. of vehicles	Cluster Formation Time (Seconds)
3	2.8863
5	2.9445
6	2.975
7	3.1518
10	3.3945
12	3.8381

Table 4.3: Time taken for selection of cluster heads w.r.t no. of vehicles

No. of Vehicles	Cluster Head Selection Time (seconds)
3	0.27225
5	0.14193
6	0.20892
7	0.27107
10	0.3338
12	0.3982

Table 4.1, 4.2 and 4.3 illustrates the values of time in seconds recorded for different processes during implementation of the proposed algorithm. In table 4.1 the time taken during the process of encryption and decryption are recorded. Table 4.2 shows the time taken by varying number of vehicles to form cluster. Table 4.3 represents the time taken by each cluster to select a cluster head with respect to the number of vehicles in the cluster.

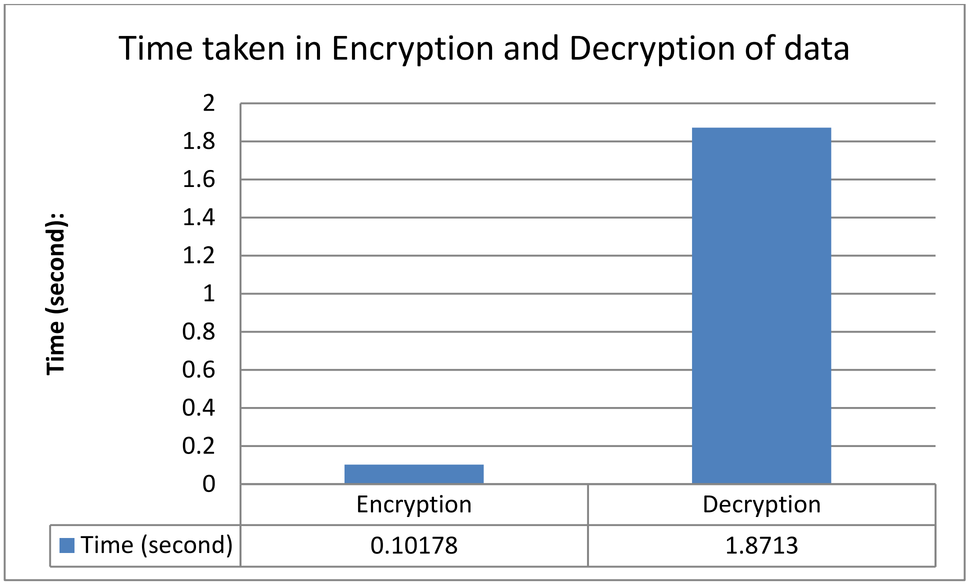


Figure 4.6: Graph depicting the time taken in encryption and decryption of data

The above figure represents the analysis of time taken during the encryption and decryption process. RSA algorithm was used during simulation for encrypting the message, comprising of the timestamp, vehicle number and a prime number. This message was encrypted and forwarded to the RSU for further processing. RSU decrypts the message and compares the vehicle number with the numbers store in the database, and validates it.

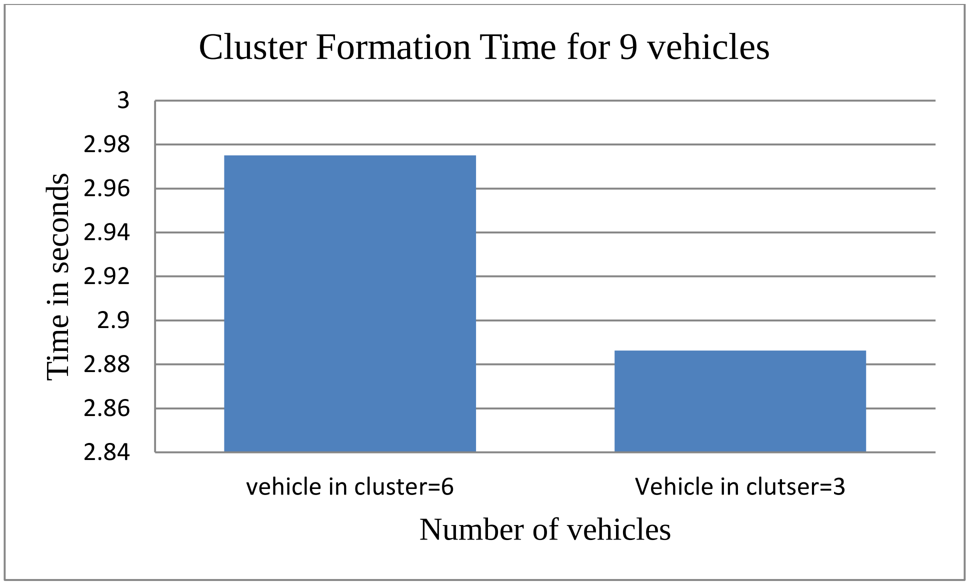


Figure 4.7: Graph illustrating the time taken in Cluster formation for 9 vehicles

Figure 4.7 illustrates the time taken for the formation of cluster. A counter was kept by the RSU to count the number of vehicles that registers with it. The cluster is then form based on the coordinates i,e the location. When 9 vehicles are deployed in the network, 2 clusters were formed. The first cluster comprises of 6 vehicles and the second cluster comprises of 3 vehicles. After the clusters were formed, a cluster head was selected for each cluster. The cluster heads are selected based on the concept of cyclic group with respect to additive property, where a generator of the group is generated. The generator is the number that can generate all other members of the group. For the first cluster the algorithm takes 0.20892 seconds and for the second cluster the algorithm takes 0.27107 seconds for selection of cluster head.

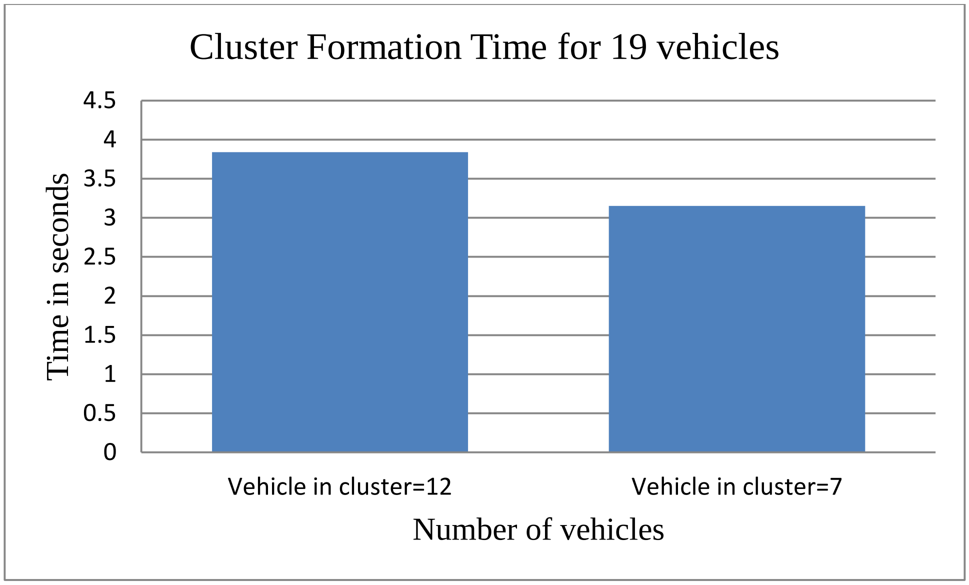


Figure 4.8: Graph illustrating the time taken in Cluster formation for 19 vehicles

The above graph illustrates the time taken to form cluster, when 19 vehicles were deployed in the network. 0.3982 seconds and 0.3338 seconds are taken by each cluster to select a cluster head.

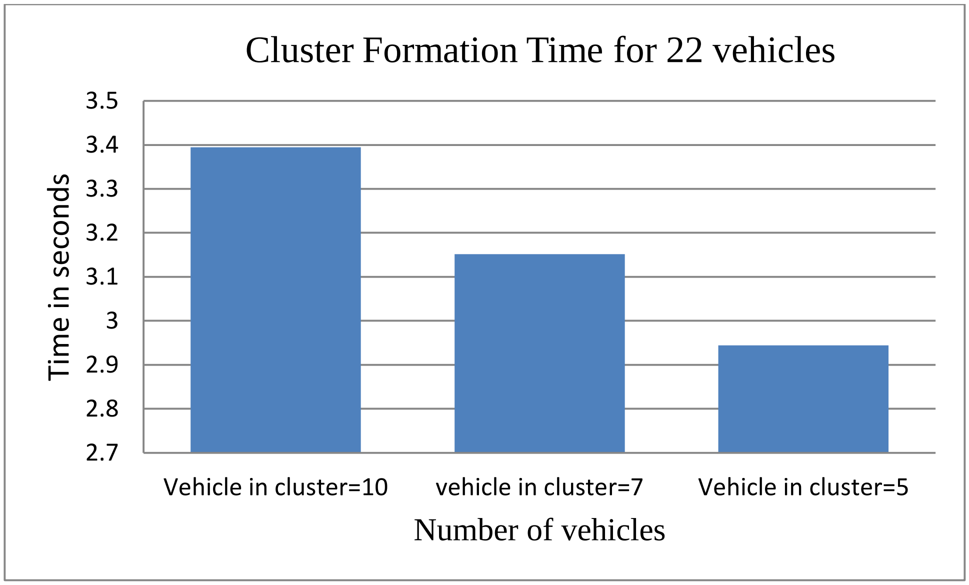


Figure 4.9: Graph illustrating the time taken in Cluster formation for 22 vehicles

Figure 4.9 represents the time taken to form cluster when 22 vehicles are deployed in the network. 3 clusters are form comprising of 10, 7 and 5 vehicles respectively in each cluster.

The 3 cluster takes 0.338, 0.27107 and 0.14193 seconds respectively for cluster head selection.

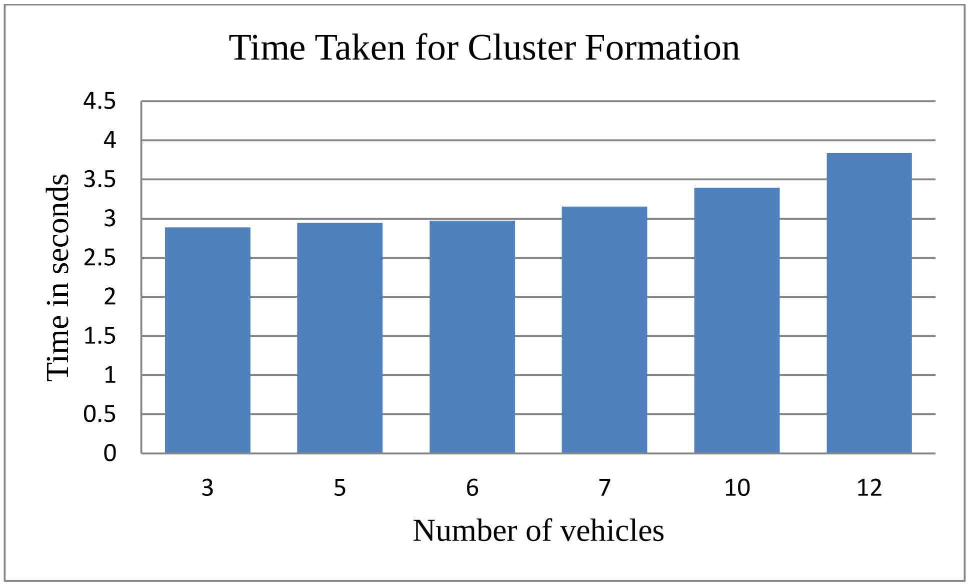


Figure 4.10: Variation in time during Cluster Formation

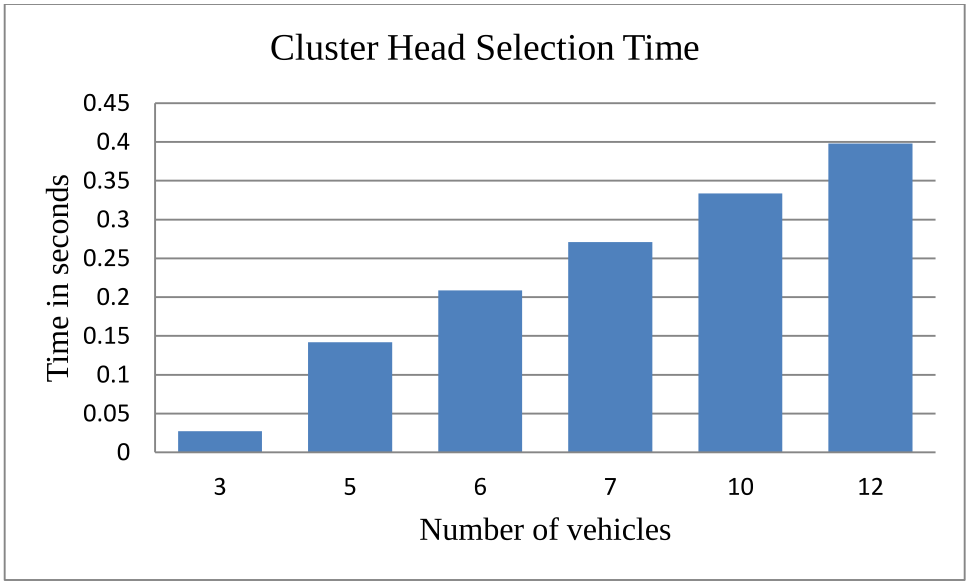


Figure 4.11: Variation in time during selection of Cluster Head

Figure 4.10 and 4.11 illustrates the variation in time for cluster formation and selection of cluster head with respect to the varying number of vehicles.

Chapter 5

CONCLUSION AND FUTURE SCOPE

Vehicular Ad-hoc network is an upcoming technology which permits vehicles to correspond with each other. VANET offers many applications. VANET has its own pros and cons. It is still a challenge to implement VANET considering the tremendous size of the network, the quickly changing topology, restricted memory, the time constraints and the high velocity of the vehicles. It is susceptible to various threats. This study mainly analyses the authentication and privacy preservation scheme in VANET. To ensure a secure and reliable VANET, vehicles and messages needs to be authenticated. Group authentication and verification ensures anonymity and conditional privacy. In this study, a new scheme for cluster formation in VANET has been discussed. MATLAB was used as a tool to implement the proposed algorithm. MATLAB is an interactive programming language developed by MathWorks. The results were recorded and analysed based on different parameters. Graphs were generated to view the variations. Further work will involve generation of short signature to perform group message signing and verification i,e group authentication of messages that are being sent between vehicles to communicate with one another.

Chapter 6

REFERENCES

Ahren Studer, f. b. (2009). Flexible, Extensible and Efficient VANET Authentication. *Jornal of Communications and Networks* .

Albert Wasef, X. (. (2013). EMAP: Expedite message Authentication Protocol for Vehicular Ad Hoc Networks. *IEEE transactions on Mobile Computing* (pp. 78-89). IEEE.

Euler, L. (1763). Theoremata arithmetica nova methodo demonstrata. *Novi Commentarii academiae scientarum Petropolitanae* , 74-104.

G.Clandriello, P. P. (2007). Efficient and Robust Pseudonymous authentication in VANET. *Workshop VANET*, (pp. 19-28).

Hellman, W. D. (1976). New directions in Cryptography. *IEEE Transactions on information theory*.

Hsin-Te Wu, W.-S. L.-S.-S. (2010). A Novel RSU-based Message Authentication Scheme for VANET. *International Conference on System and Network Communication.*

Hui Zhu, T. L. (2013). PPAS: Privacy Preservation Authentication Scheme for VANET. *Cluster Computing* (pp. 873-886). Springer.

Karuppanan, K. a. (2011). Secure Privacy and Distributed Group Authentication for VANET. *International Conference on Recent Trends in information technology.* IEEE.

Lai, C.-C. L.-M. (2013). Toward a secure batch verification with group testing for VANET. *Springer*.

Liu, J.-S. L.-H. (2013). A lightweight Identity Authentication Protocol for VANET. *Telecommun Syst* , 425-438.

M.Raya, J. (2007). Securing vehicular ad hoc network. *Journal of Computer Security* , 39-68.

M.Wang, D. L. (2014). LESPP: lightweight and efficient strong privacy preservation authentication scheme for secure VANET Communication. *Springer*

Norman, C. (2012). Finitely generated abelian groups and similarity of matrices over a field. *Springer Undergraduate Mathematics Series* , 47-51.

Rongxing Lu, X. L.-H. (2008). ECPP: Efficient Conditional Privacy preservation Protocol for Securing vehicular communications . *IEEE INFOCOM.*

Sherali Zeadally, R. H.-S. (2010). Vehicular ad hoc networks (VANETS): status,results, and challenges. *Springer* .

Shi-Jinn Horng, S.-f. T. (2013). b-SPECS+: Batch Verification for secure pseudonymous authentication in VANET . *IEEE transactions on Information Forensics and Security*. IEEE.

Shoup, V. (2005). *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press.

Xuedan Jia, X. Y. (2013). EPAS: Efficient Privacy preserving Authentication Scheme for VANETs-based Emergency Communication. *Journal of Software* .

MY PUBLICATION:

Thounaojam Korouhanbi Devi, S. S. (2015). New cluster formation scheme for vehicle authentication in VANET. *WECON.*

Chapter 7

APPENDIX

List of Abbreviation

VANET	Vehicular Ad-Hoc Network
MANET	Mobile Ad-Hoc Network
OBU	On-Board Unit
RSU	Road-Side Unit
TA	Trusted Authority
TPD	Tamper Proof Device
DSRC	Dedicated Short Range Communication
WAVE	Wireless Access in Vehicular Environment
ASTM	American Society for Testing and Materials
IP	Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
PKI	public Key Infrastructure
TESLA	Time Efficient Stream Loss Authentication
ECDSA	Elliptic Curve Digital Signature Algorithm
DoS	Denial of Service
MAC	Message Authentication Code
HMAC	Hash MAC
SPECS	Secure Privacy Enhancing Communication Scheme
CRL	Certificate Revocation List
DRA	Disaster Relief Authority

Glossary of Term

Anonymity: Hiding the identity of the vehicle.

Authentication: The assurance that the communicating entity is the one that it claims to be.

Certificate Revocation List (CRL):A list vehicles with invalid identities.

Cluster: A group of vehicles belonging to same network.

Conditional Privacy: Related to anonymity and tracing.

Confidentiality: Protection of message from unauthorized disclosure.

Cyclic Group: A group that can be generated by a single element called the generator of the group.

Decryption: Changing the cipher text back to the plain message.

Encryption: Transforming the plain message to a cipher text.

Euler Totient's Function (Φ(n)): The number of positive integers less than n and relatively prime to n.

Generator: An element of the group which can generate all the other members of the group.

On-Board Units (OBU): Devices mounted on vehicles to facilitate wireless communication.

Private key: A secret key.

Public key: A key shared by everyone

Road-Side units (RSU): Communication units located aside the road that connects to the application server and the trusted authority.

Traceability: Different interaction of a vehicle should not be correlated.

Trusted authority: A third party who performs certificate generation, issue and revocation.

UID: Acronym for unique identification number, it is a unique number assigned to each vehicle that registers itself with the RSU.

VANET: A technology that allows vehicles to form a network and communicate with one another, as well as the roadside infrastructure.

Meaning of Notation

Notation	Meaning
M	Message
T_s	Timestamp
N	Vehicle’s number
P	Prime number
E	Encrypted message
sD	Decrypted message
PU_{RSU}	Public key
PR_{RSU}	Private key
MI	Multiplicative Inverse
UID	Unique Identification Number