ABSTRACT

Suchetha N V

Moving vehicles in Vehicular network can exchange information with each other either through inter vehicle communication or road-side units (RSUs). Vehicles use wireless channels. Different types of attacks can easily occur, such as injecting false information, modifying and replaying the messages. Hence achieving security in communication is essential before using it in any application.

PKI and CRL are used in Vehicular ad hoc networks (VANETs) to gain security. In PKI system all units in the network holds a legal certificate, and each data before its communication should be digitally signed. A CRL is the set of revoked certificates. The certificate is issued by Trusted Authority (TA). In this system, the authentication of a received data is done through verifying whether sender's certificate is valid or not and by verifying the sender signature. Certificate is valid if it is present in the recent CRL. Verifying the certificate in this way spend large amount of time, because of large size of the CRL. Here the objective is to enhance the speed of Authentication Process, which resolves the disadvantages found in the existing method, such as reducing the authentication delay.

The proposed system also decreases the communication overhead and authentication delay. It tries to prove that proposed system is secure and efficient. Finally performance of the entire network will be improved by this mechanism.

CHAPTER 1

1.1 Overview

INTRODUCTION

In vehicular ad hoc network (VANET) mobile nodes are vehicles. Every vehicle is turns into wireless router or node, to connect vehicle to each other for communicating approximately over 100 to 300 meters in VANET. Vehicles can come within the network range, can go out of range, other vehicles can connect to one another so creates mobile network. This technology is used for safety purpose in police and fire vehicles.

In vehicular network, vehicles can communicate with each other either through vehicle-to-vehicle communication or vehicle-to-infrastructure communication. To make sure trustworthy operation of VANET s and raise the amount of authentic information obtained from the message, each OBU should be able to check the revocation status in a timely manner.

Vehicles communicate using wireless channels. Different types of attacks such as injecting fake information, modifying and replaying the messages can be easily occur. In any system security attack can harm the user data. Hence achieving security in communication is essential before using it in any application.

PKI and CRL are used in VANETs to achieve security. In PKI system each unit in the network holds a legal certificate, and every message before its communication is digitally signed. A CRL is the set of revoked certificates. The certificate is issued by Trusted Authority (TA). In this system, the authentication of a received message is done by verifying whether certificate of the sender is valid or not and by verifying the sender signature. Certificate is valid if it is present in the current CRL. Verifying the certificate in this way spend large amount of time, because of large size of the CRL.

The size of the CRL in VANETs is large for the following reason:

- To protect the confidentiality of the drivers.
- VANET range is very large.

According to DSRC for every 300ms every OBU sends the message about it location, velocity and other traffic information. Hence number of message received over 300ms is large. For each received message it has to verify the certificate against current CRL. This results in long authentication delay depending on size of the CRL.

1.2 Characteristics of VANET

The Main feature characteristics of Vehicular Ad-hoc Networks are listed below.

- Dynamic topology: There are multiple paths, it allows choosing alternate path. This defines dynamic topology for VANET.
- Recurrent disconnected network: vehicles are moving, so while moving there is chances of jump from one network to another or it may fall out of the network range. The lack of road side unit results in recurrent disconnection of network.
- Vehicle location prediction: Determining the location of the vehicle is very difficult. This feature of VANETs is based on the predefined roadmaps models. The speed of the vehicle is also considered while determining its location.
- Relations with onboard sensors*:* Sensors are used to read the data related to the situation of the traffic. The data the sensors can read includes speed, location, direction etc. these information's are communicated with data center i.e. with the onboard unit.
- Limitless Battery Power and Storage: In VANET nodes have infinite storage and power. Therefore optimizing the duty cycle is not important.

1.3 Application of VANETs

- Helpful Message Transfer: To help other vehicle either slow downed or stopped Vehicle will exchange messages to other vehicles. It may avoid accidents.
- Pre collide Notification*:* A vehicle that encountered with accident will sends announcement message to other vehicle, so that other vehicle can take the decision to take alternate path. Also incident about the accident is known and can take required action.

- Road risk manage Notification*:* Vehicles can also send the information about the road quality such as curve, road diversion, slop etc. It will help the driver to improve his driving.
- Parking slot information: Drivers can also get information regarding parking slot, it helps the driver to find the available parking slot in the geographical area.

1.4 Project Objective

The objective behind this project is to provide the authentication. Authentication process involves checking the sender certificate against the certificates given to the vehicles in that network present in the Certificate Revocation List (CRL). In this project we are trying to reduce the time required to perform the authentication by using Merkel hashing technique. Also we are comparing the following with the existing system.

- To compute authentication delay.
- Calculate the Communication cost of updating the secret key.

1.5 Organization of the report

The organization of the project report is explained as follows. The project report is designed with 7 chapters, references and appendices. Introductory part is explained in Chapter 1. Chapter 2 gives information about the referred papers and websites. Chapter 3 specifies system requirements. Chapter 4 explains architecture and design. Chapter 5 explains about implementation steps. Chapter 6 discusses validation testing. Chapter 7 includes simulation model and the acquired results are analyzed in comparison with the existing model results. Chapter 8 includes conclusion.

CHAPTER 2

LITERATURE SURVEY

Literature survey is done to study the background of the project. It helps to find out defects in the existing system & provides the idea on which not solved problems we can work out. Following section explores different references that discuss about several topics related to project.

In VANETs, the most important security requirements are identified as entity authentication, message integrity, non repudiation, and privacy preservation. To achieve these securities, PKI is the most feasible technique [13]. Revoked certificates are efficiently managed in PKI. Size of the CRL is large, so time required checking the certificate is more.

In [2], Studer et al. propose an efficient authentication and revocation technique called TACK. In this central trusted authority and regional authorities (RAs) are used. Regional authorities are distributed all over the network. In TACK before sending the new certificate to the requested vehicle, RA has to wait. During this period vehicle won't able to send message to neighbouring vehicle. According to WAVE standard every vehicle sends messages for every 300ms. So TACK is not suitable for safety application. TACK also requires the RAs to completely cover the network; or else, the TACK technique might misbehave.

A different way of reducing the size of the CRL involves using types of compression techniques.

In [3], Raya et al. introduce Revocation using Compressed Certificate Revocation Lists (RC2RL). In this CRL that is issued by TA is compressed to reduce its size before its transmission using Bloom filter. This method sends out certificate revocation lists that are compressed using about half the number of bytes to specify the certificate ID for revocation. This shortens the already hashed value so that the number of false positive increases.

In [4] Papadimitratos et al. CRL is partition into tiny pieces and distribute each portion separately. Laberteaux et al.[5] use car to car communication to speed up the CRL broadcasting.

In [6] Haas et al. size of the CRL is reduced, by sending a secret key per revoked vehicle. After receiving the new CRL, the secrete key of the revoked vehicle is used to reproduce the identities of the certificates loaded in that revoked vehicle and to construct the entire CRL. Although the size of the broadcast CRL is minimized, to check the revocation status of other entities, the CRL is constructed at each OBU, still size of the CRL used to check the revocation status of the certificate is large. Hence authentication delay is not reduced. To perform CRL checking for the received certificates lookup hash tables are used in the bloom filter.

In [9], Raya and Hubaux proposed a method to provide security and privacy for communication through VANETs using conventional PKI. In this approach large amount of certificates are preloaded to each vehicle. To provide security and privacy the large number of certificates loaded into each vehicle. Certificates are updated from central trusted during the yearly inspection of the vehicle. In this case revoking one vehicle means revoking large number certificates.

Zhu et al. introduce the GKMPAN protocol [10], which adopts a probabilistic key distribution approach [14],[15], which is based on pre arranged single keys. The GKMPAN is efficient and scalable for wireless mobile networks, because it takes the node mobility into consideration.

2.1 Simulation Environment

In simulation, by changing the variables we can study the performance of the system. Using this tool we can virtually examine the behavior of the system under study.

Through the help of computer program a simulation tool is helps in simulating the mathematical model or a physical model. Now the network behavior is simulated using the NS-2.3.5 network simulator.NS2 is an open-source event-driven simulator. NS2 is developed as a collaborative environment [11].

2.1.1 NS2 Simulator

NS2 is built using object oriented methods in C++ and OTcl. Fig 3.2, NS2 interprets user view of NS2. The different components such as network components libraries and setup module libraries, event scheduler objects can be set up in the simulation environment. The

simulation is written as a OTcl script. The event scheduler triggers the events of the simulation.

Part of the NS2 is written in C++. The data paths are written in C++ and control path is written in OTcl. The objects of the C++ are controlled by OTcl objects. Data path object are compiled and these are made available to the OTcl interpreter using an OTcl linkage. OTcl likage maps the methods and member variables of the C++ object to methods and variables of the linked OTcl object.

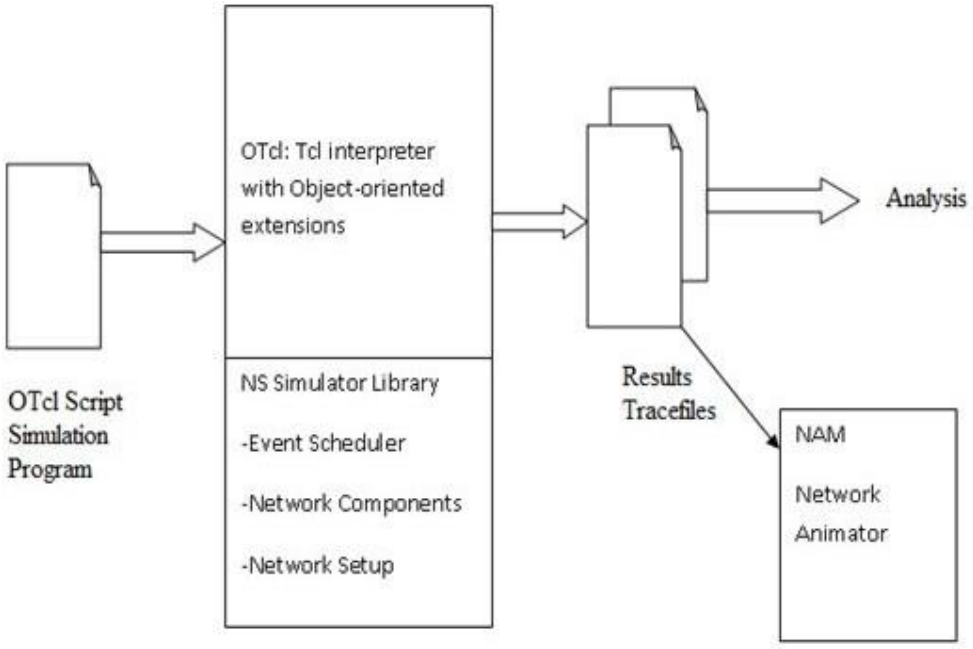

Fig 2.1 Simplified User's View of NS

2.1.2 Functionalities of NS2.35

Functionalities for of NS2 are as follows:

- Support for the wired world include
    - Routing DV, LS, and PIM-SM.
    - Transport protocols: TCP and UDP for unicast and SRM for multicast.
    - Traffic sources: web, ftp, telnet, cbr (constant bit rate), stochastic, real audio.
    - Different types of Queues: drop-tail, RED, FQ, SFQ, DRR.
    - Quality of Service: Integrated Services and Differentiated Services.
    - Emulation.

- Support for the wireless world include
    - Ad hoc routing with different protocols, e.g. AODV, DSR, DSDV, TORA
    - Wired-cum-wireless networks
    - Mobile IP
    - Directed diffusion
    - Satellite
    - Sensor-MAC
    - Multiple propagation models (Free space, two-ray ground, shadowing).
    - Energy models
- Tracing & Visualization
    - Network Animator (NAM)
    - Trace Graph
- Utilities
    - Mobile Movement Generator

2.2 GNU plot

gnuplot is a command-line program. It can plot two and three-dimensional of data. This program is developed in the year 1986.

gnuplot can produce output on screen, or in many formats of graphics files, including PNG, SVG, Encapsulated PostScript (EPS), JPEG and many others. By using LaTeX's fonts and powerful formulae abilities it is possible to produce LaTeX code that can be included directly in document LaTeX. In various languages, including Perl, Python, Java, Ruby, Ch and Smalltalk gnuplot can be used.

2.3 PKI System

PKI is related with the digital signature, asymmetric key encryption and digital certificates. Using public key cryptography, PKI provides storage and exchanges of data in a secure way and the types of security services offered:

- Confidentiality – Confidentiality gives security to the client's touchy data.

- Integrity – Ensuring that the message has not been changed during transmission. Digital signature is used to obtain Integrity by verifying the signature.
- Authenticity - Verifying the identity of an individual or an application which transmits the message is done using a digital signature.
- Non-repudiation – Property providing security as the certainty that the message can't deny it.

If large numbers of certificates are assigned to the each vehicle, checking the certificates takes long time. It reduces the authentication delay.

2.4 Existing System

EMAP removes the overhead of checking the CRL for verifying signature, by calculating hash code [1]. In this sender along with sending message it will also sends the hash code, for each message. At the receiving end it will verifies the time stamp, signature and hash value for each received message. If all the verification is succeeded then the message is accepted. Hash value is calculated based on id of vehicle, timestamp and secrete key.

In EMAP for every message sent from a vehicle, signature generation must be done by source vehicle and signature verification must be done by all vehicles. This will become huge overhead when the number of vehicles and number of messages sent by vehicle is high.

To make sure trustworthy operation of VANETs and to raise the amount of authentic information gained from the message that is received, every OBU has to check the revocation status of all the received certificates in a well-timed manner. Checking the Certificate Revocation Lists (CRL) for a large number of certificates in a timely manner is challenge to VANET. The existing works suffering from the authentication delay resulting from checking the Certificate Revocation Lists (CRL) for each received certificate. The proposed a system overcomes the problem of the long authentication delay. The proposed system employs keyed HMAC. To calculate HMAC secrete key is used, that is shared between no revoked OBUs. Therefore, proposed system can significantly decrease the Authentication delay, communication overhead and message loss ratio due to message verification delay.

Disadvantage

- The attacks such as injecting fake information, modifying and replaying the disseminated messages can be easily occur.
- To withhold the leakage of the real identities and location information of the drivers from any external eavesdropper.
- VANET size is very large.

2.5 Proposed System

Because vehicles communicate through wireless channels, there is high possibility for various attacks to be launched; attacks like injecting false information, modifying the messages transferred and replaying the messages. More importance is given towards Security for VANET and as a solution for providing security, PKI and CRL are been deployed for managing the process.

In proposed system, concentration is on CRL, which is found to be unsatisfactory due to resulting in long delay because of increased CRL size.

In this project system is developed to enhance the sped of authentication process and overcomes the disadvantages found in the existing method. The proposed system will be able to significantly decrease the authentication delay and communication cost due to the less message verification time compared with the conventional authentication methods employing CRL. It tries to prove that proposed system is secure and efficient. Finally performance of the entire network will be improved by this mechanism.

We are using Hash Message Authentication Code in the revocation checking process. To calculate HMAC secret key is used, this is shared between unrevoked OBUs.

Advantages

- Computation complexity is less in proposed method.
- The number of messages that can be verified within 300 msec is increased.
- Decreases Authentication delay

CHAPTER 3

REQUIREMENT ANALYSIS

3.1 Hardware and Software Specification

Hardware Specification

Hard Disk/Processor	:	500GB with Intel processor
RAM	:	64 MB

Software Specification

Operating System	:	Ubuntu
Language	:	TCL/C++
Visual Interface	:	Command line/Terminal
Simulation tool	:	NS2

CHAPTER 4

DESIGN

The system Design is defined as "The process of applying various techniques and principles for the purpose of defining a process or a system in sufficient detail to permit its physical appearance". To develop the system various design features are followed. Design specification describes the systems components or elements, the features of the system and their appearance to end-users.

4.1 System Architecture

System architecture defines structure of the system, behavior and views of the system. It consists of component of the system, properties of the component and the relation between those components.

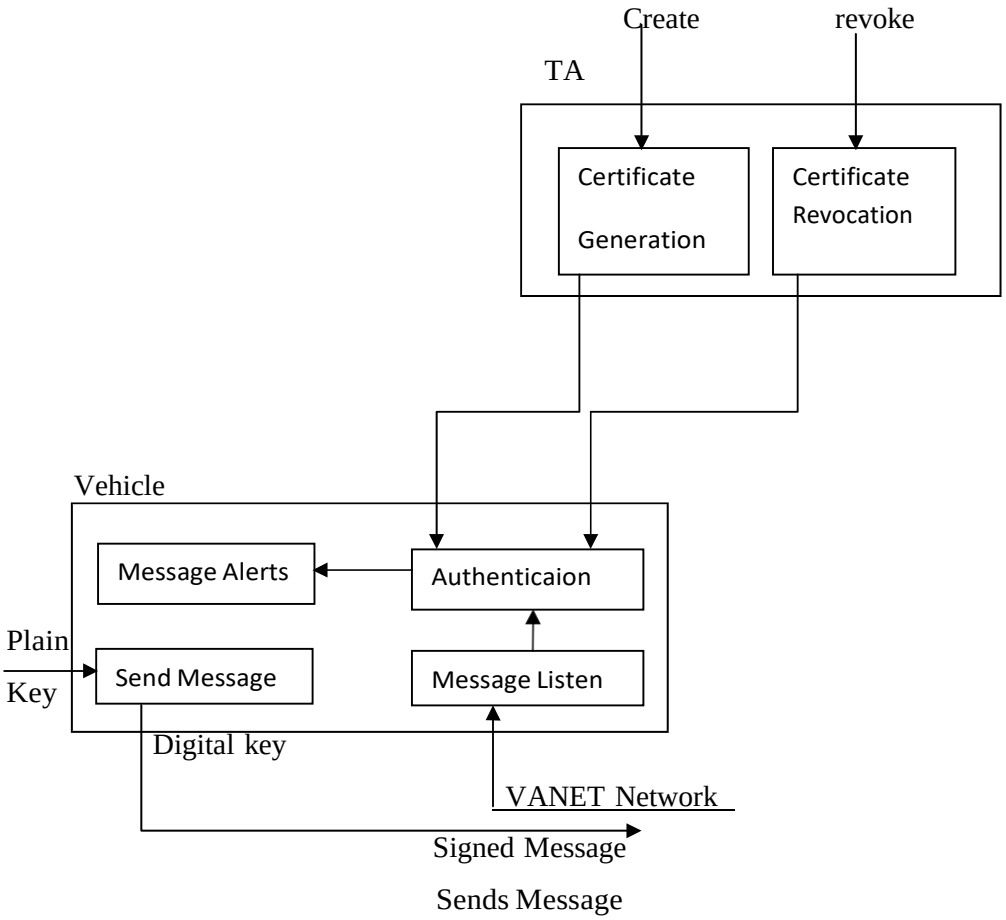

Fig 4.1: System Architecture

Trusted Authority (TA) is provides certificate to the registered vehicle. The authentication of any message is performed by first checking certificate revocation list (CRL). Proposed method reduces the authentication delay resulting from checking the CRL in VANET network.

OBU uses batch verification technique to provide signature. Suppose a source Vehicle has a batch of messages (batch size we are treating as 5 messages). Then vehicle will compute the signature for every message, but it will not send the signature in each message to be sent out.

Instead of that MERKEL Hash is computed for the five signatures as follows

MH (sig1, sig2) → M1

MH (sig3, sig4) → M2

MH (M1, M2) → M3

MH (M2, sig5) → M4

Send the M4 alone with the fifth message.

Once the receiver vehicles receives all 5 messages from the source, they will compute signatures and MERKEL Hash, let it be MX, if MX==M4 then all the batch messages are verified at one shot, otherwise all the batch messages are dropped at one shot.

4.2 Class Diagram

The fig 4.2 depicts the class diagram.

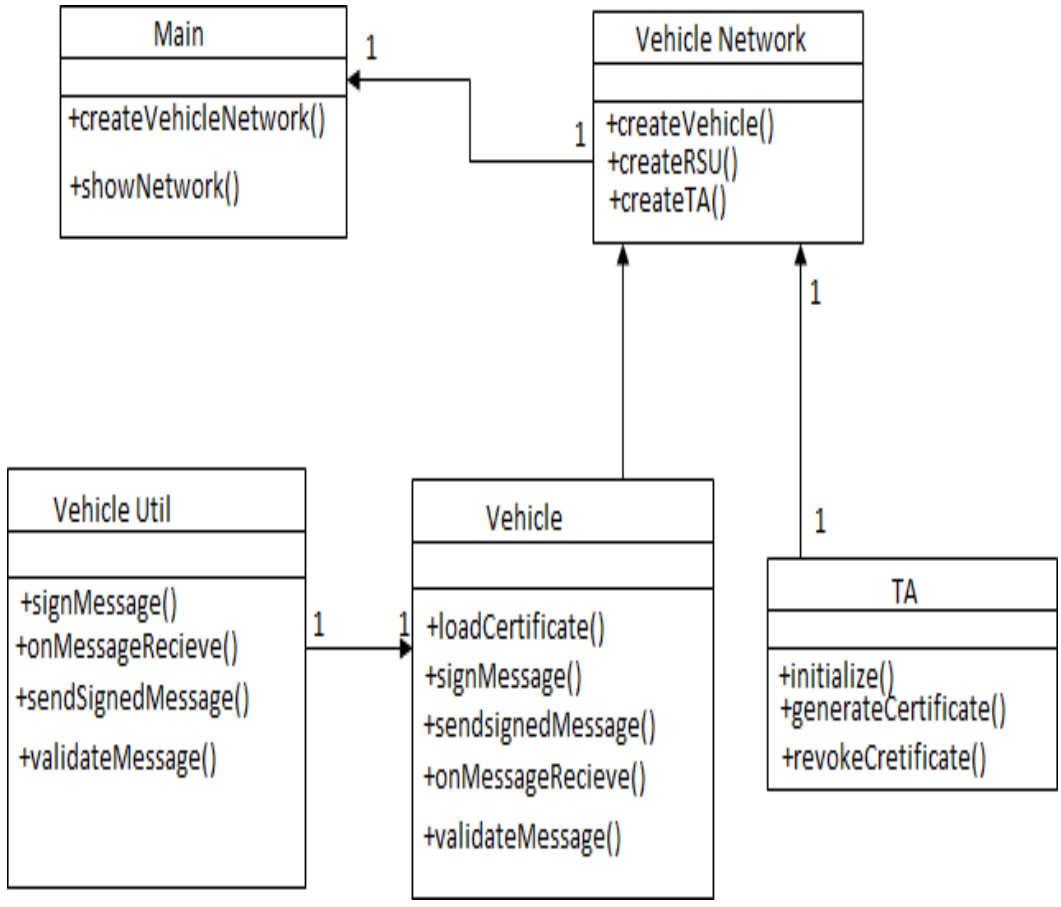

Fig 4.2: Class Diagram

Main class generalizes the class vehicle network; it creates the vehicle network and shows that network. Vehicle network class generalizes the vehicle and trusted authority (TA). It creates vehicle, RSU and TA. Certificate loading, message signing, send the signed message and validate the message operations are done in the vehicle class. TA initializes, generate and revoke the certificates. Vehicle util class sign the message, receives message, sends the signed message and validates the message.

4.3 Use Case Diagram

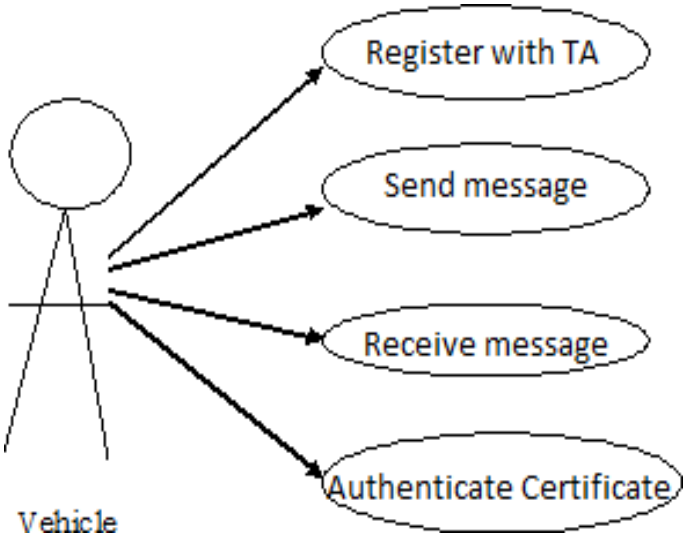

Fig 4.3: Use Case Diagram for Vehicle

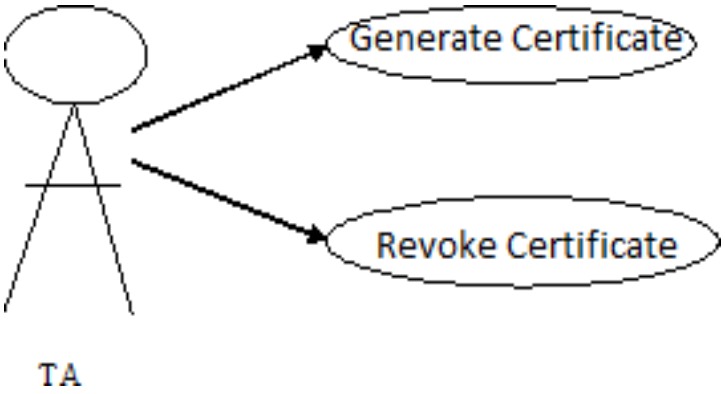

Fig 4.4: Use Case Diagram for TA

Vehicles and TA are the actors used here. Vehicles registers with the TA, send the messages to the other vehicle, receives the messages from other vehicle and authenticate the received messages. TA generates the certificates for the vehicle that is applied for registration if it is authentic vehicle and revokes the certificates.

4.4 Sequence diagram

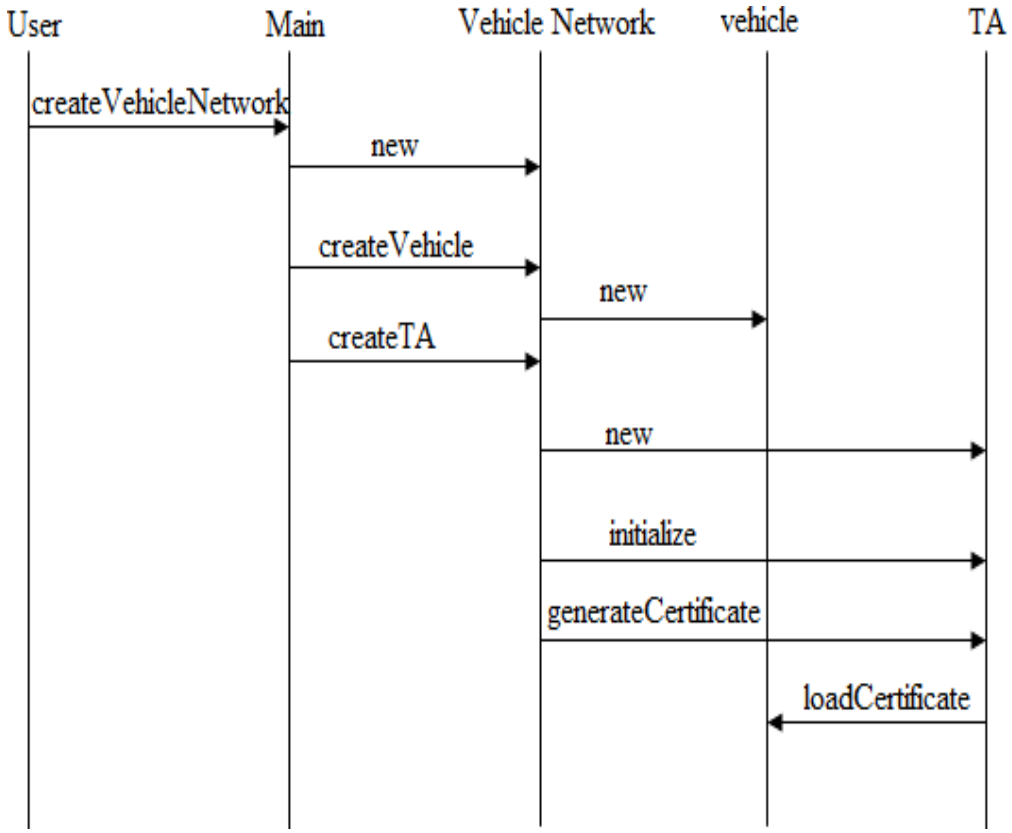

Fig 4.5: Sequence for network initialization

Fig 4.5 depicts the sequence diagram for network initialization. All vehicles have to register with Trusted Authority (TA) before sending the message. Trusted Authority will generate the certificate for the registered vehicle.

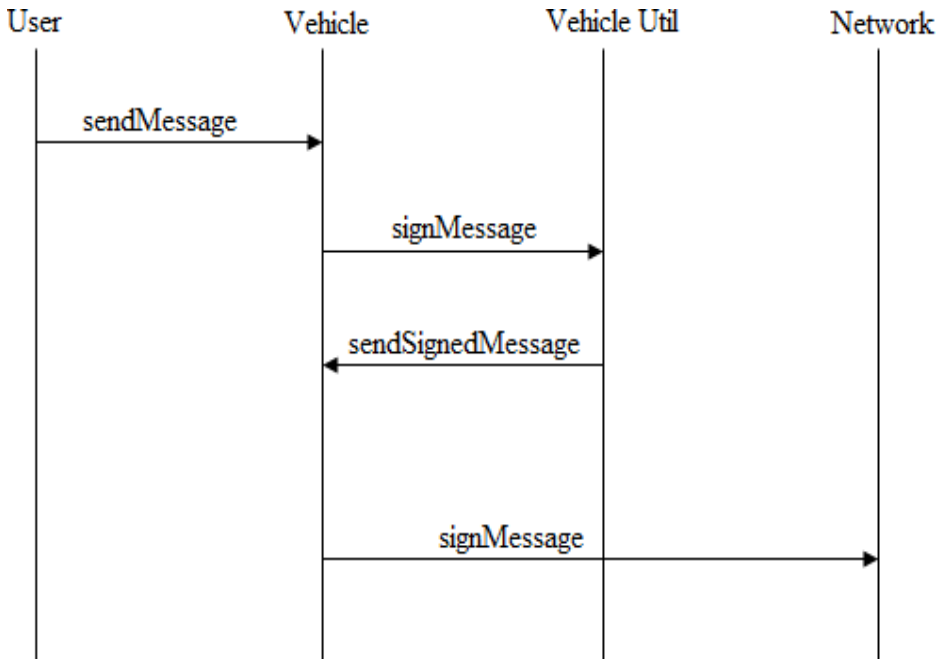

Fig 4.6: Sequence for message sending flow

Fig 4.6 depicts the sequence diagram for message sending. Sender will sign the message and then sends the signed message to all vehicles.

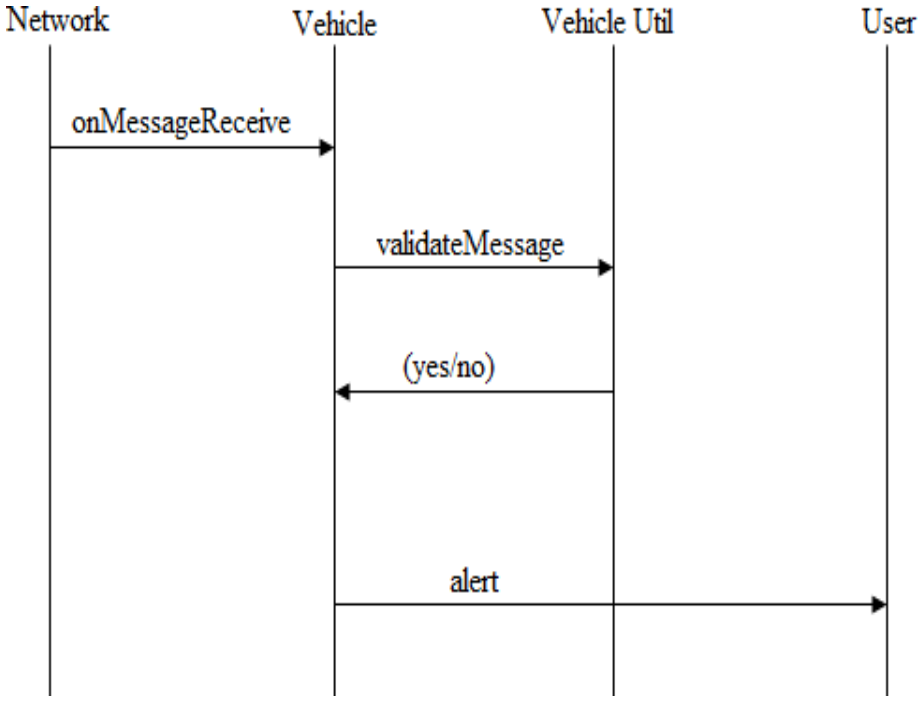

Fig 4.7: Sequence for receiving message flow

Fig 4.7 depicts sequence diagram for receiving message. On receiving the message receiver validates the message. Received message is processed if it is valid, otherwise it will be rejected.

4.5 Data Flow Diagram

A data-flow diagram (DFD) represents graphically the flow of data in system. DFDs can also be used for the visualization of data processing (structured design).

Level 0 Data flow diagram

Fig 4.8 shows level 0 data flow diagram. It shows interaction between the system and external agent, which acts as source and sink

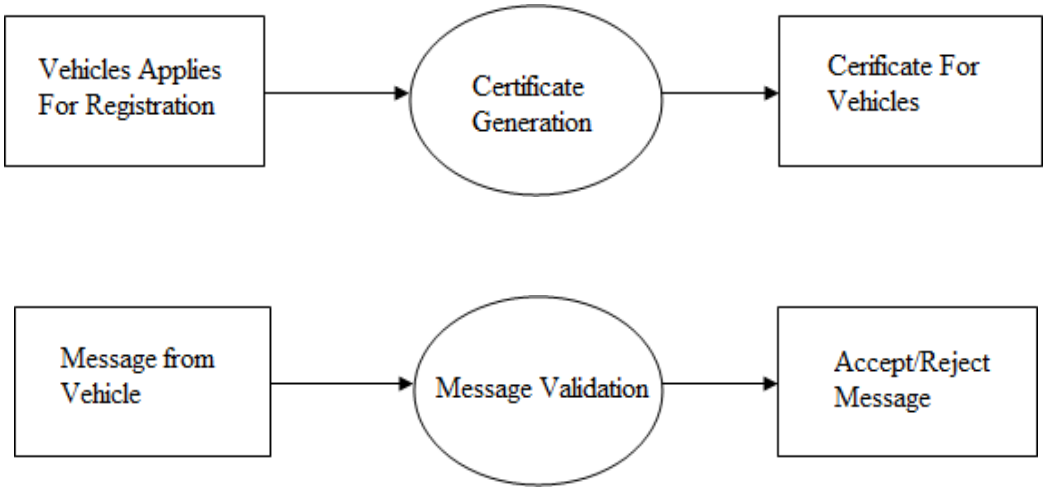

Fig 4.8: level 0 data flow diagram

Level 1 Data flow diagram

Fig 4.9 shows level 1 data flow diagram. In this system is divided into sub-system. Each sub-system deals with one or more data flow to or from external agent. Also it provides functionality of the system.

Level 1

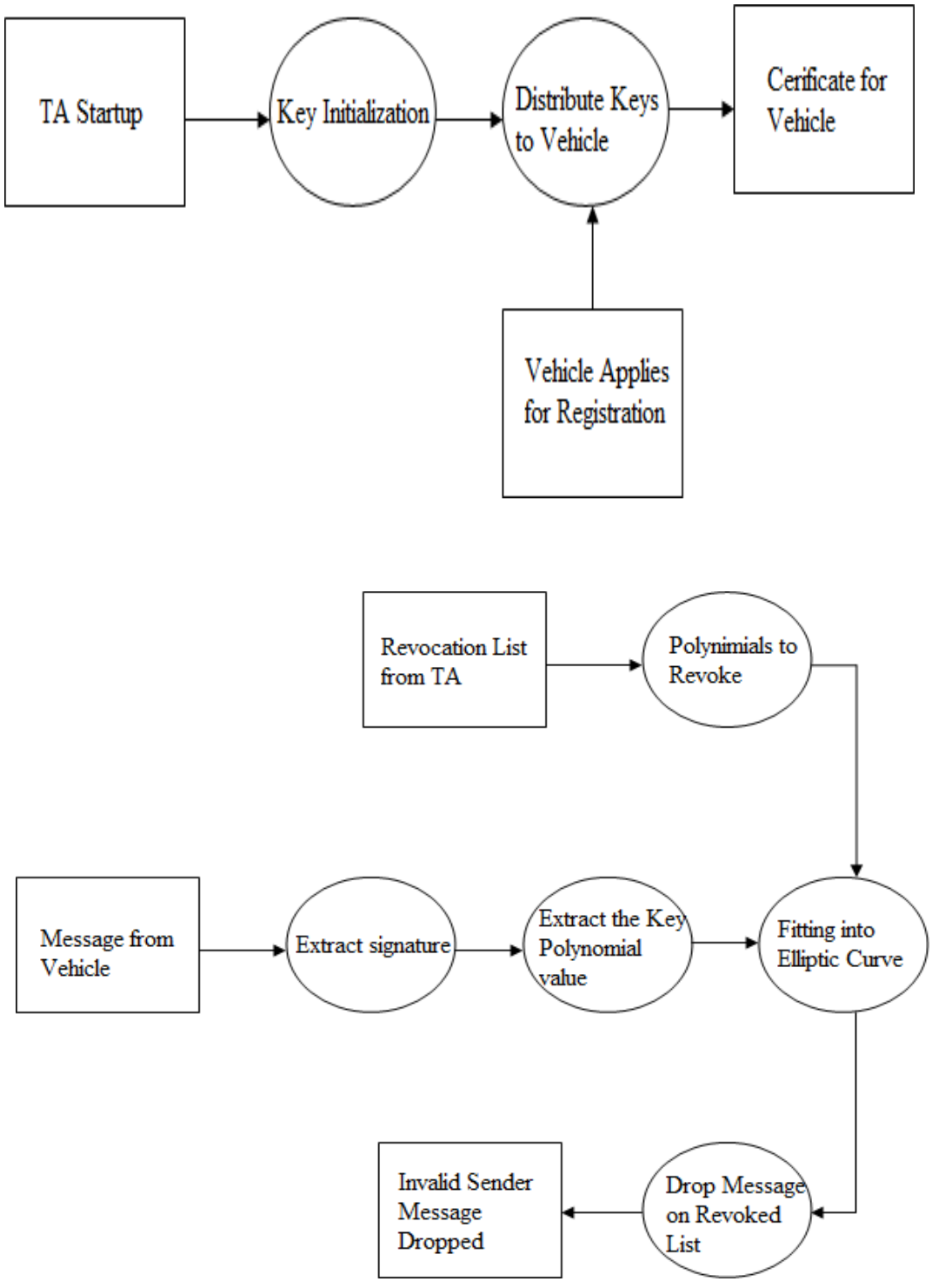

Fig 4.9: level 1 data flow diagram

CHAPTER 5

IMPLEMENTATION

In implementation design is converted into working system.

5.1 Language used for implementation

In this project, TCL/C++ programming language is used for implementation the reasons for selecting TCL as a programming language are:

- Tcl is simpler.
- Tcl is smaller.
- Tcl/Tk is portable.
- TCP networking is more concise.
- Tcl's socket, open and exec are gems of accessible and portable functionality, in comparison to the analogous Perl offerings.
- As of spring 2001, Tcl's Unicode [18] capabilities are considerably more mature.
- All operations are commands, including structure of the language. They are written in prefix notation.
- Dynamically it can be redefined and overridden.
- Event-driven interface to files and sockets. Time-based and user-defined events are also possible.
- Commands defined by Tcl generates error message on its incorrect usage.
- Interpreted language using byte code.

5.2 Mobile Node: Creating Wireless Topology

Option	Available Values	Default
Address type	Flat, Hierarchical	Flat
MPLS	ON,OFF	OFF

Table 5.1: Available Options for Node Configuration in general

Option	Available Values	Default
Wired Routing	ON,OFF	OFF
II Type	LL,LL/sat	OFF
Mac Type	Mac/802_11,Mac/Csma/Ca, Mac/Sat/Unslotted/Aloha,Mac/Tdma	OFF
ifq Type	Queue/DropTail, Queue/Droptail/PriQueue	OFF
Phy Type	Phy/wirelessPhy,Physat	OFF
downlinkBW	<bandwidth value>	OFF

Table 5.2: Available Options for Node Configuration in Both Satellite and Wireless Oriented

Option	Available Values	Default
Adhoc Routing	DIFFUSION/RATE,DIFFUSION/PROB, DSDV,FLOODING,OMNICAST,AODV,TORA	OFF
propType	Propagation/2RayGround,Propagation Shadowing	OFF
propInstance	Propagation/2RayGround,Propagation Shadowing	OFF
AntType	Antenna/Omni Antenna	OFF
Channel	Channel/Wireless Channel,Channel/sat	OFF
topoInstance	<toplogy file>	OFF
MobileIP	ON,OFF	OFF
Energy model	Energy model	OFF
Initial Energy	<value in joules>	OFF
RxPower	<value in W>	OFF
txPower	<value in W>	OFF
AgentTrace	ON,OFF	OFF
routerTrace	ON,OFF	OFF
macTrace	ON,OFF	OFF
movementTrace	ON,OFF	OFF
Errproc	UniformErrorProc	OFF
toraDebug	ON,OFF	OFF

Table 5.3: Available Options for Node Configuration in Wireless Oriented

5.3 System Model

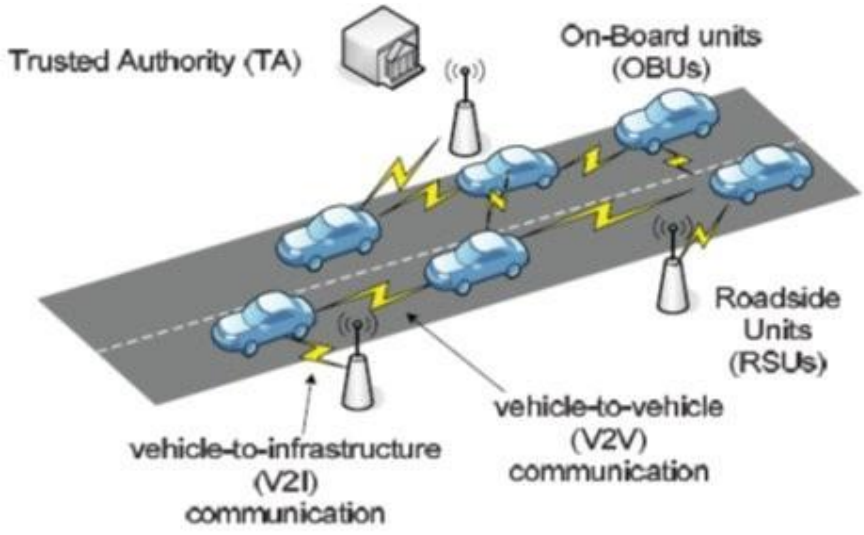

Fig 5.1: System Model of VANET

The system model includes following components:

Trusted Authority (TA): Trusted Authority will provide certificate to all registered vehicle. Initially all vehicle must go and register to the TA. TA will provide broadcast keys in each round to the unrevoked nodes in the network. If a vehicle is an attacker and it is informed to TA, then TA will revoked this vehicle and will not send the broadcast key to the vehicle.

Roadside units (RSUs): RSU is a fixed unit, scattered throughout the network. The RSUs communicate with TA securely.

Vehicles: On-Board Units (OBUs) is equipped in vehicle. Which are communicating with each other to share traffic information.

5.4 Implementation Steps

1. System Initialization: Select the prime numbers. Here generate the public key and private key.
2. For OBU, select the random number and upload secret key and public key.
3. Generate anonymous certificate for privacy preserving authentication.
4. Message verification done by trusted authority based on certificate signature of OBU
5. Processing of Revocation messages.

Implementation of the system can be explained with respect to Trusted Authority (TA), sending vehicle and receiving vehicle.

TA (Trusted Authority)

Trusted Authority (TA) will provide certificate to all registered vehicle. Initially all vehicle must go and register with the TA. TA will provide broadcast keys to the unrevoked nodes only. If a vehicle is an attacker and it is informed to TA, then TA will revoked this vehicle and will not send the broadcast key to the vehicle.

Sending Vehicle

Before vehicle sending any message to any other vehicle, it has to register with TA. After receiving certificate from TA vehicle that wants to send a message will use the Broadcast key given by TA in that round to encrypt and sign the message. The signed and encrypted message is then broadcast to other vehicle.

To verify the multiple digital signature in less time than the time required verifying individual Batch Verification is used.

OBU uses batch verification technique to provide signature. Suppose a source Vehicle has a batch of messages (batch size we are treating as 5 messages). Then vehicle will compute the signature for each message, but it will not send the signature in each message to be sent out.

In its place of this MERKEL Hash is computed for the five signatures as follows

MH (sig1, sig2) → M1

MH (sig3, sig4) → M2

MH (M1, M2) → M3

MH (M2, sig5) → M4

Send the M4 alone with the fifth message.

Once the receiver vehicles receives all 5 messages from the source, they will compute signatures and MERKEL Hash, let it be MX, if MX==M4 then all the batch messages are verified at one shot, otherwise all the batch messages are dropped at one shot.

Message is authenticated by attaching the trusted authority's and sender's signature.
Format of the message that is sent is ($M|| T_{stamp} ||cer_u(PID_u,PKu,sig_{TA}(PID_u || PK_u))||REV_{check}$).

Receiving Vehicle

The receiving vehicle that has broadcast key for that round will be able to verify the signature included along with the broadcasted message. If the signature matches it will accept the message. If the signature mismatch, then it will reject the message. So if any attacker vehicle, who don't have broadcast key for current round, but use the key of last round to sign and send message, this message will be rejected at other vehicle, since signature mismatch. Also if any outer vehicle, who don't know broadcast key and send any message, it will be dropped at other vehicle, since no signature will be there.
By this way vehicle can authenticate messages in the network.

Algorithm used for message verification in EMAP is:
Algorithm: message verification

Input: ($M|| T_{stamp} ||cer_u(PID_u,PKu,sig_{TA}(PID_u || PK_u))||sig_u(M|| T_{stamp})||REV_{check}$)

Validity of T_{stamp} is checked

If T_{stamp} is notvalid then
Leave the message
Else
REV_{check}=HMAC(Kg,$PID_u|| T_{stamp}$) is checked
If REV_{check} is not valid then
Leave the message
Else
TA sign is checked
If sign is not valid then
Leave the message
Else
Check the sign of the OBU
If sign is not valid then
Leave the message

Else

Accept & process the message

End if

End if

End if

End if

CHAPTER 6

TESTING

System testing is carried out with a sequence of different kind of tests. The goal of testing is to check the functioning of the system. Each test have its own purpose, but overall testing is done to verify whether all the elements of the system is integrated properly and whether it's working exactly as needed. Following are the goals to be achieved: -

- Quality assessment of the project.
- To identify & resolve the errors found in the previous stages.
- To provide operational reliability of the system.

6.1 Validation Testing

The outcome of the integration testing is completed and assembled software package. Validation testing can be defined in several ways. Table 6.1 lists some of the functionalities used to test the system.

System	Functionality to be tested	Input	Expected output	Actual output	Remark
MAP	Working of NAM	User interaction through mouse & keyboard	NAM window appear with nodes placed	NAM window appear with nodes placed	The system is working as expected. So testing is success
	Working of simrun	Node sense events and forwards the packets to the router	Packet transfers & sensor range should be displayed	Packet transfers & sensor range should be displayed	
	Working of plotgraph	User runs simrun & types ./plotgraph.sh	Graph of delay v/s no. of revocation is displayed	Graph of delay v/s no. of revocation is displayed	

Table 6.1: Validation testing table

CHAPTER 7

RESULTS AND ANALYSIS

The work is validated by using simulation and compared it with existing Expedite Message Authentication Protocol (EMAP). The table 7.1 depicts the simulation parameters and their values adopted for the project.

Parameter	**Value**
Network Size in meters	900X900
No of nodes	30 0 Trusted Authority (TA) 1-11 Road Side Unit (RSU) 12-29 Vehicles
Data packet size	1Kbits
Mobility model	Random way point model
Initial node energy	100 joules
Queue Size	50 packets

Table 7.1: Simulation parameter and their values

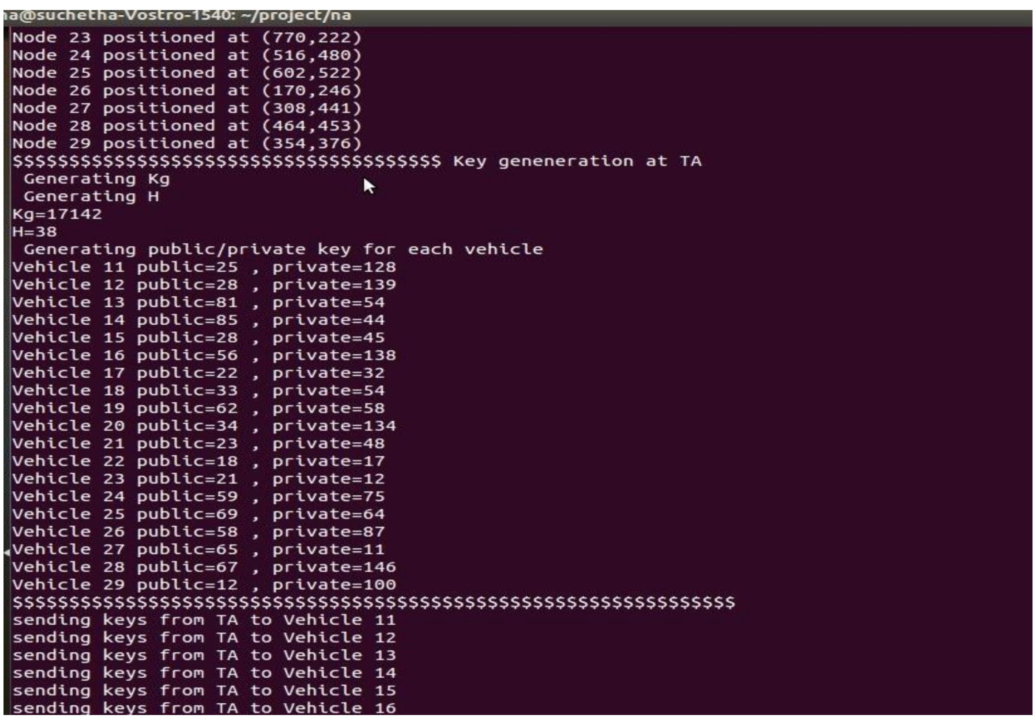

Fig 7.1: Generation and Distribution of key's

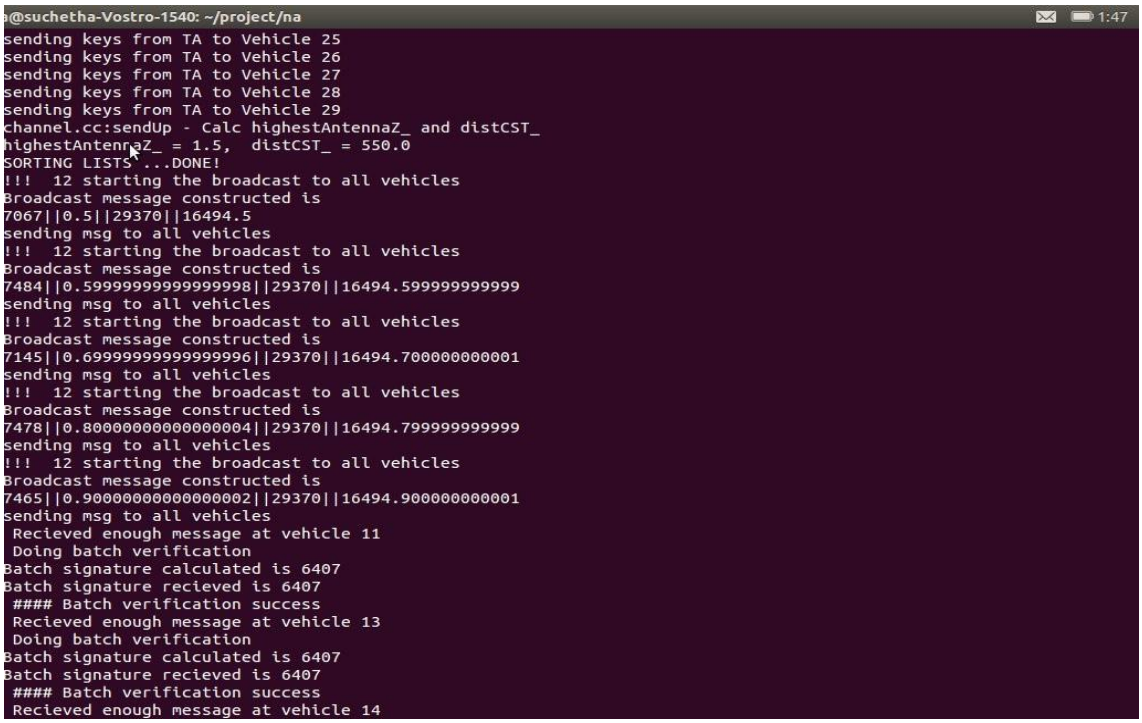

Fig 7.2: Authentication for the message from sending vehicle without modification.

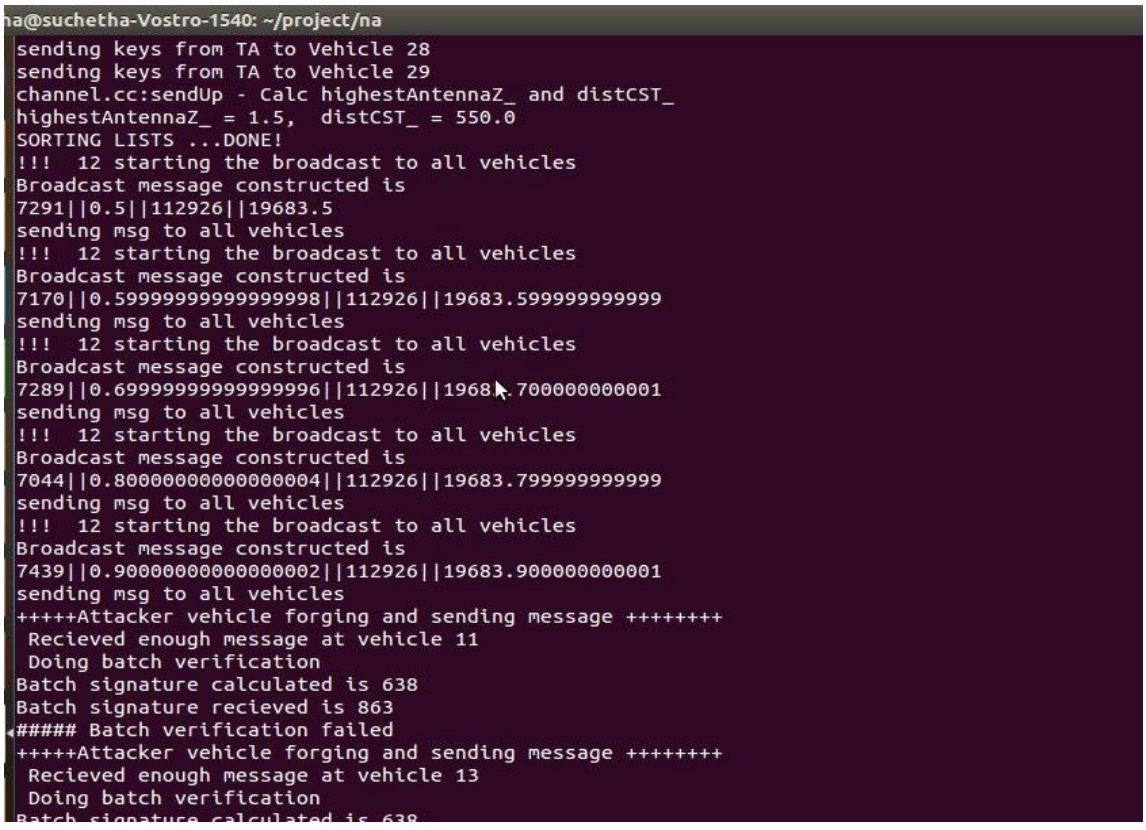

Fig 7.3: Authentication for the message that is modified by the attacker.

7.1 Performance Analysis

To check the performance of the proposed method, different metrics are used. Here we used Authentication Delay and Communication Overhead.

1) **Authentication delay** is calculated with respect to number of revocation. The fig 7.4 and fig 7.5 shows delay Vs number of revocation for proposed method and EMAP method respectively.

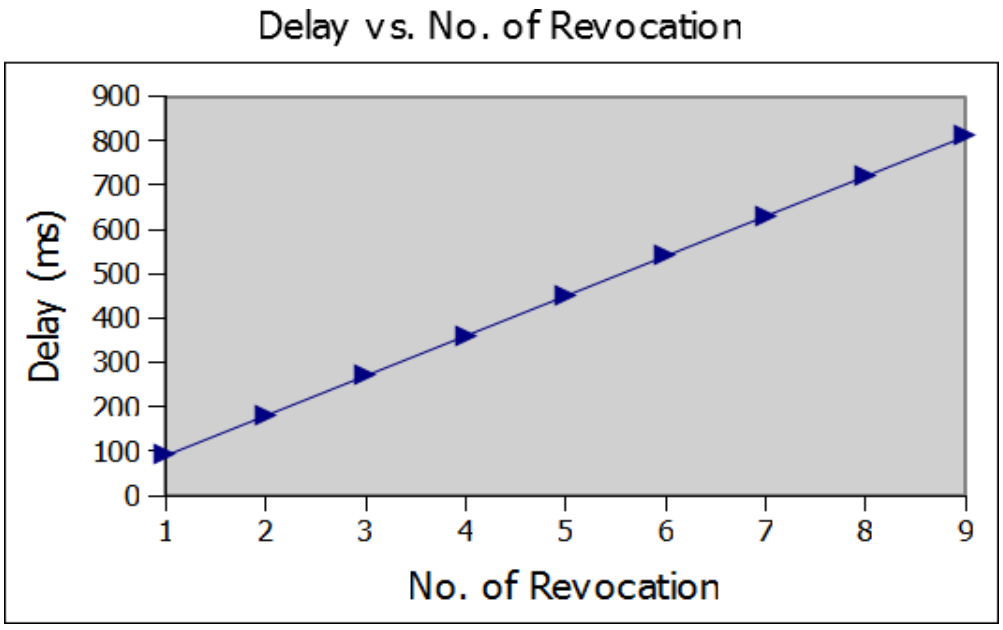

Fig 7.4: Delay vs. No. of Revocation in EMAP

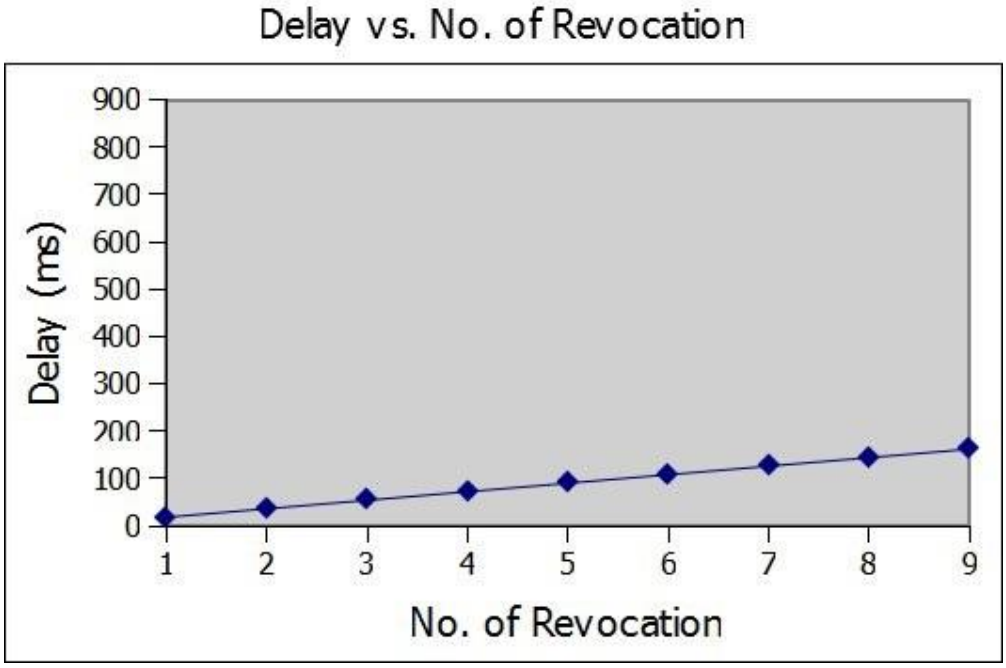

Fig 7.5: Delay vs. No. of Revocation in MAP

Compared to existing system proposed system is having less Authentication Delay. In this project we are verifying received message at a time for batch of messages. So that authentication delay is reduced. Fig 7.6 depicts the comparison between proposed method and existing method i.e. Expedite message authentication protocol (EMAP).

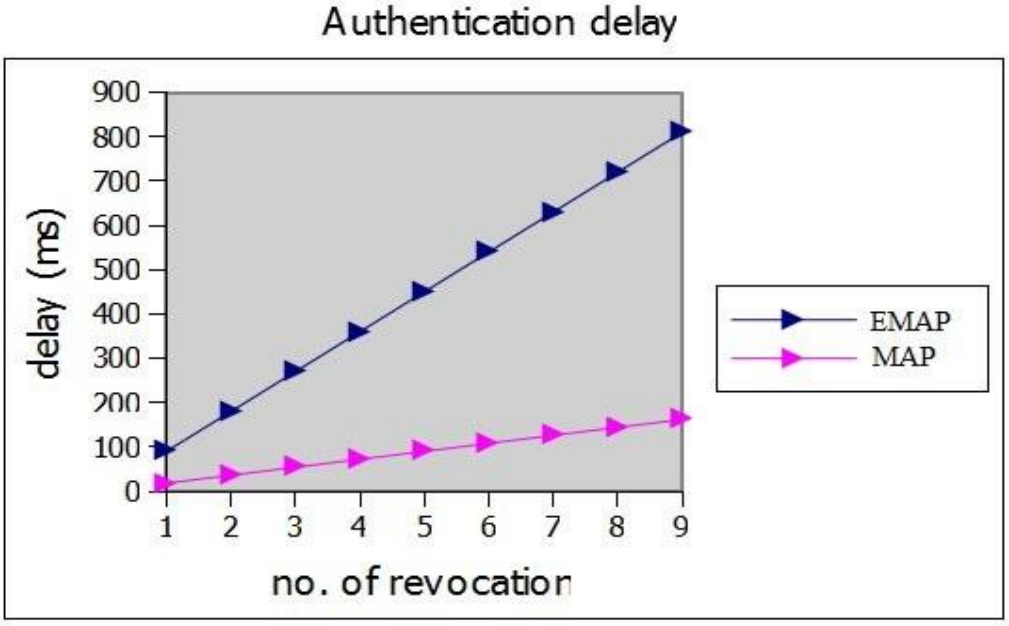

Fig 7.6 Comparison of Authentication delay of EMAP and MAP

2) **Communication Overhead** is calculated with respect to number of revocation. The fig 7.7 and fig 7.8 shows delay Vs number of revocation for proposed method and EMAP method respectively.

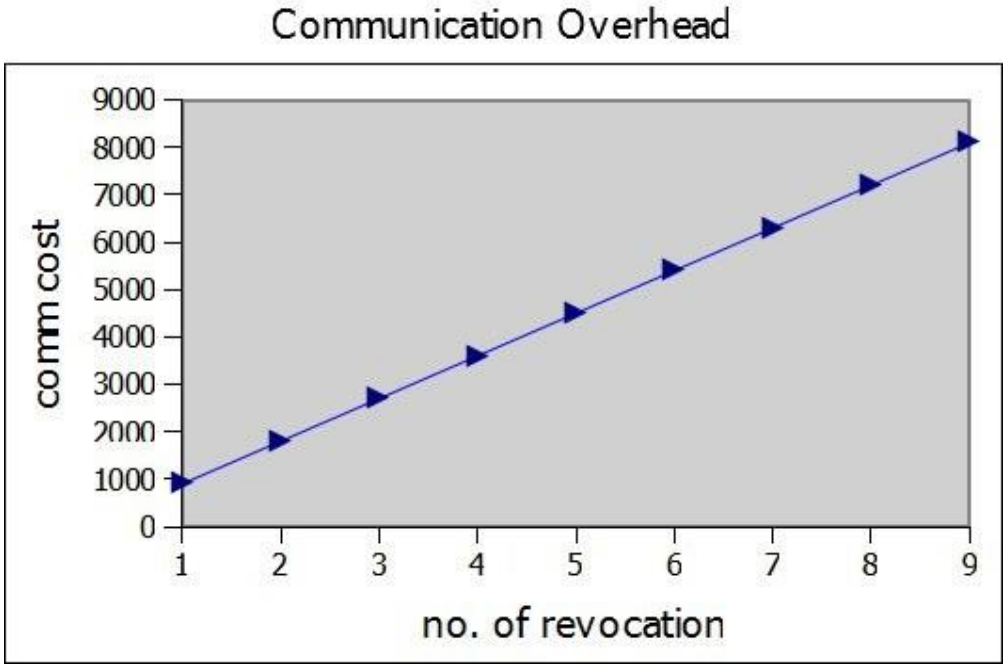

Fig 7.7: Communication Cost in EMAP

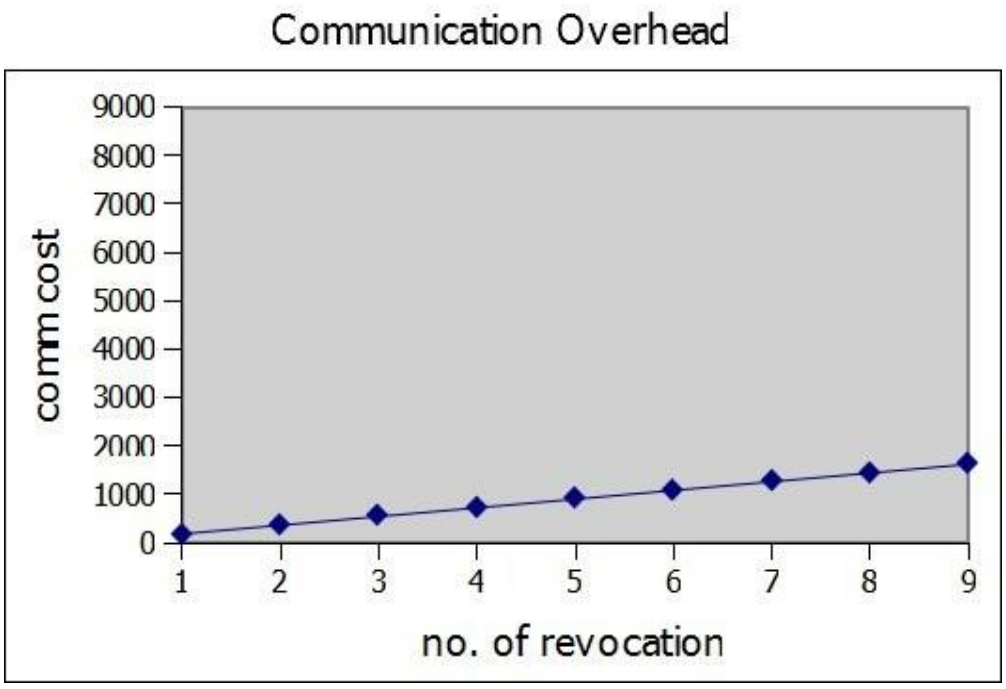

Fig 7.8: Communication Overhead in MAP

Compared to existing system proposed system is having less communication overhead. In this project we are verifying received message at a time for batch of messages. So with this method, following overheads are avoided

1. Sending signature in each message by the sender.

2. Receiver verifying the Hash for every message.

So that communication overhead is reduced. Fig 7.9 depicts the comparison between proposed method and existing method i.e. Expedite message authentication protocol (EMAP).

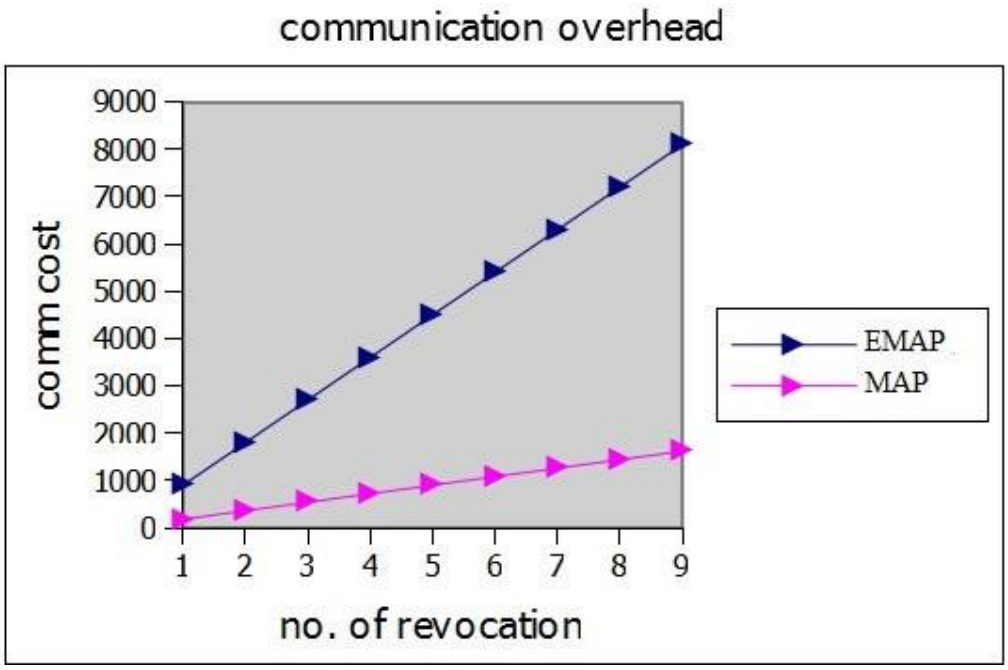

Fig 7.9 Comparison of Communication Overhead of EMAP and MAP

CHAPTER 8

CONCLUSION AND FUTURE WORK

Conclusion

In this project authentication process is for VANETs, accelerated replacing the time-consuming CRL checking process with a fast revocation checking process employing HMAC function so authentication delay is minimized. Therefore, it significantly decrease the message loss ratio due to message verification delay compared to the conventional authentication methods employing CRL checking. It also reduces the authentication delay and communication overhead. Furthermore, it is secure against replay, forging attacks and colluding attack.

Future Work

The current way of batch verification, only detects if any packet is faulted, but we can add redundancy in each packet, so that if batch verification fails, we can still recover the attacked portions. This is the future work.

REFERENCES

[1] Albert Wasef and Xueminshen, "EMAP: Expedit Message Authentication Protocol for Vehicular Ad Hoc Networks", IEEE Transaction on Mobile Computing, VOL. 12, NO.1, January 2013.

[2] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," Proc. IEEE CS Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. And Networks (SECON '09), pp. 1-9, 2009.

[3] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P.Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 1557-1568, Oct. 2007.

[4] P.P. Papadimitratos, G. Mezzour, and J. Hubaux, "Certificate Revocation List Distribution in Vehicular Communication Systems," Proc. Fifth ACM Int'l Workshop VehiculAr Inter-NETworking, pp. 86-87, 2008.

[5] K.P. Laberteaux, J.J. Haas, and Y. Hu, "Security Certificate Revocation List Distribution for VANET," Proc. Fifth ACM int'l Workshop VehiculAr Inter-NETworking, pp. 88-89, 2008.

[6] J.J. Haas, Y. Hu, and K.P. Laberteaux, "Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET," Proc. Sixth ACM Int'l Workshop VehiculArInterNETworking, pp. 89-98, 2009.

[7] C.SelvaLakshmi, N.SenthilMadasamy, T.Pandiarajan, "Secured Multi Message Authentication Protocol for Vehicular Communication", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 12, December 2013.

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

[9] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[10] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad-Hoc Networks," J. Computer Security, vol. 14, pp. 301-325, 2006.

[11] NS Simulation for Beginners – Lecturer notes 2003-2004.

[12] A. Wasef and X. Shen, "MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks," Proc. IEEE GlobeCom, 2009.

[13] J.P. Hubaux, "The Security and Privacy of Smart Vehicles," IEEE Security and Privacy, vol. 2, no. 3, pp. 49-55, May/June 2004.

[14] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. IEEE Symp. Security and Privacy, pp. 197-213, 2003.

[15] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. ACM Conf. Computer and Comm. Security, pp. 41-47, 2002.

[16] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.

[17] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing Location Privacy for VANET," Proc. Embedded Security in Cars (ESCAR) Conf., Nov. 2005.

[18] P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, "Privacy and Identity Management for Vehicular Communication Systems: A Position Paper," Proc. Workshop Standards for Privacy in User- Centric Identity Management, July 2006