ACCELERATING AUTHENTICATION PROCESS USING MAPS FOR EFFICIENT VANETS

Abstract

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.

Keywords: VANET, Trusted Authority, CLR, PKI, RSU

Authors

Suchetha N V
Assistant Professor
Department of Computer Science & Engineering
Sri Dharmasthala Manjunatheshwara Institute of Technology
Ujire, Karnataka, India.
itsmesuchethanv@gmail.com

Sunitha N V
Assistant Professor
Department of Computer Science & Engineering
Mangalore Institute of Technology and Engineering
Moodabidri, Karnataka, India.
sunithanv6720@gmail.com

I. 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.

In order to achieve security, VANETs require PKI and CRL. Each network node in a PKI system has a valid certificate, and every message is digitally signed prior to communication. The list of revoked certificates is known as a CRL. Trusted Authority (TA) is the entity that issues the certificate. In this system, a received message's authenticity is determined by checking the validity of the sender's certificate and the sender's signature. If the certificate is shown in the most recent CRL, it is valid. Because the CRL is so huge, verifying the certificate in this manner takes a long time. The size of the CRL in VANETs is large because to protect the confidentiality of the drivers and 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 7 current CRL. This results in long authentication delay depending on size of the CRL.

II. LITERATURE REVIEW

1. **Literature Survey:** Entity authentication, message integrity, non-repudiation, and privacy protection are the top security needs for VANETs. PKI is the most practical method for achieving these securities [13]. In PKI, revoked certificates are effectively managed. Because the CRL is huge, it takes longer to check the certificate.

   TACK is an effective authentication and revocation approach that Studer et al. offer in [2]. Both regional authorities (RAs) and the central trusted authority are employed in this. The network is distributed with regional authorities. 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.

   Revocation using Compressed Certificate Revocation Lists (RC2RL) is introduced by Raya et al. in [3]. 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.

By transmitting a secret key per car with a revocation, Haas et al. in [6] decrease the size of the CRL. The secret key of the revoked vehicle is used to reconstruct the whole CRL and recreate the identities of the certificates loaded in that revoked vehicle after receiving the new CRL. Although each OBU constructs a CRL to check the revocation status of other entities, the size of the CRL used to check the revocation status of the certificate is still considerable even though the size of the broadcast CRL is minimised. As a result, authentication latency is not eliminated. The bloom filter uses hash tables to perform CRL validation for the received certificates' lookups.

In [9], Raya and Hubaux put up a strategy for leveraging traditional PKI to offer security and privacy for communication using VANETs. In this method, each vehicle has a substantial number of certifications preloaded. Each car has a huge number of certificates installed in it for security and privacy. During the yearly vehicle inspection, certificates are updated from central trusted sources. In this instance, revocation of one vehicle entails revocation of numerous certificates.

The GKMPAN protocol [10] is introduced by Zhu et al. It uses a probabilistic key distribution approach [14],[15] and is based on pre-arranged single keys. For wireless mobile networks, the GKMPAN is effective and scalable because it takes into account node mobility.

2. **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, the source vehicle must generate signatures for every message transmitted from that vehicle, and every vehicle must verify those signatures. When the number of vehicles and the amount of messages sent by vehicles is high, this will become a significant overhead.

Each OBU must promptly check the revocation status of any certificates it has received in order to ensure the reliable operation of VANETs and to increase the quantity of authentic information gleaned from messages. It is difficult for VANET to quickly check the Certificate Revocation Lists (CRL) for a large number of certificates. Because each received certificate is checked against the Certificate Revocation Lists (CRL), the current works experience authentication delays. The long authentication delay is solved by the system that is suggested. The suggested method makes use of keyed HMAC. There is no shared secret key between revoked OBUs that is utilised to calculate HMAC. Due to the message verification latency, the suggested system can greatly reduce message loss ratio, communication overhead, and authentication delay.

III. PROPOSED SYSTEM

Due to the wireless nature of vehicle communication, there is a considerable potential for numerous attacks to be conducted, including those that inject false information, alter the messages transferred, and replay the communications. 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. Due to the shorter message verification time than the traditional authentication techniques using CRL, the suggested system will be able to considerably reduce the authentication latency and communication cost. 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.

Objectives of the Present Study:

The objectives of the proposed project are as follows:

1. To compute authentication delay.
2. To calculate the Communication cost of updating the secret key.

IV. SYSTEM DESIGN

1. **Architecture to Proposed System:** 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. The figure 1 shows architecture of the proposed system.

   The certificate for the registered car is given by the Trusted Authority (TA). Any message must first be authenticated by checking the certificate revocation list (CRL). The suggested solution lessens the authentication lag caused by the VANET network's CRL check

   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 thesignature for every message, but it will not send the signature in each message to be sent out.

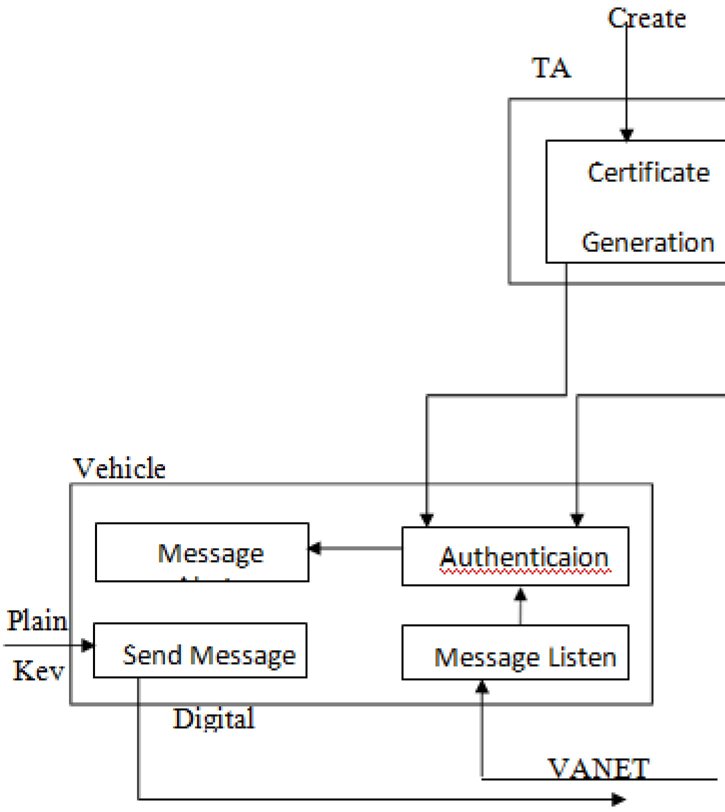


Figure 1: Architecture of the Proposed System

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.

2. **Class Diagram:** The figure 2 depicts the 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.

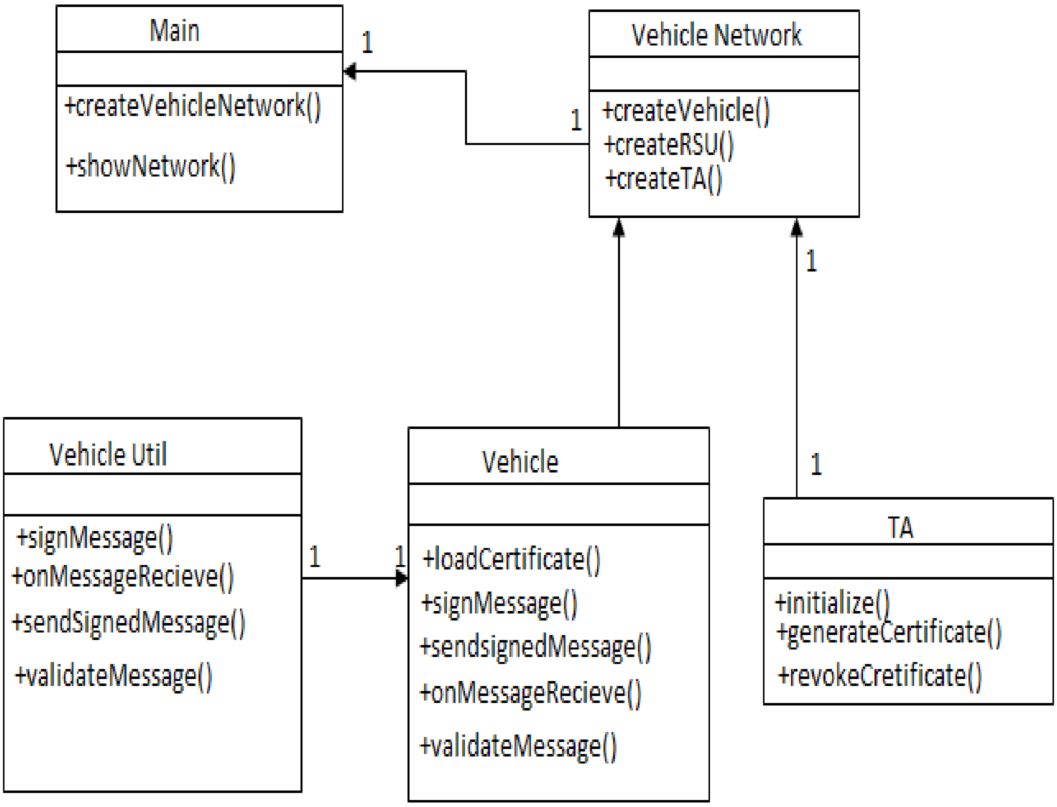


Figure 2: Class Diagram

3. Use Case Diagram:

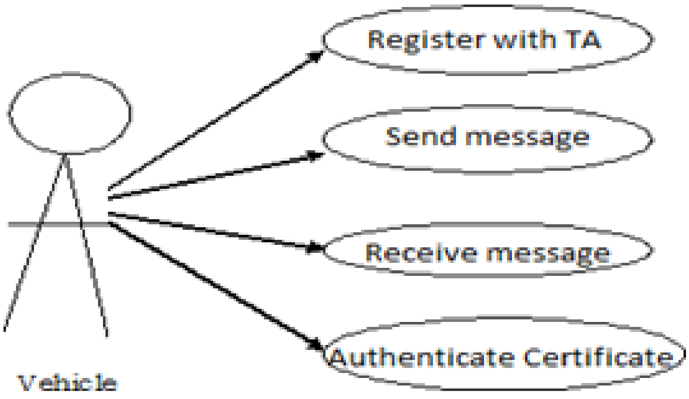


Figure 3: Use Case Diagram for Vehicle

The figure 3 shows the use case diagram of vehicle, figure 4 shows uses case diagram of trusted authority.

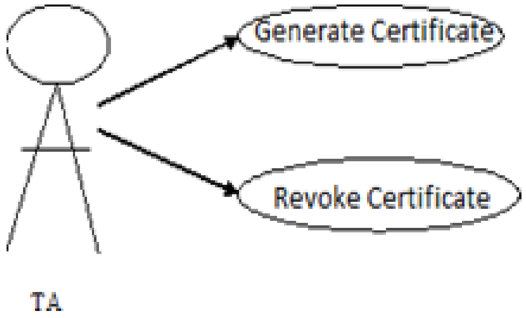


Figure 4: Use Case Diagram for TA

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. **Sequence Diagram:**

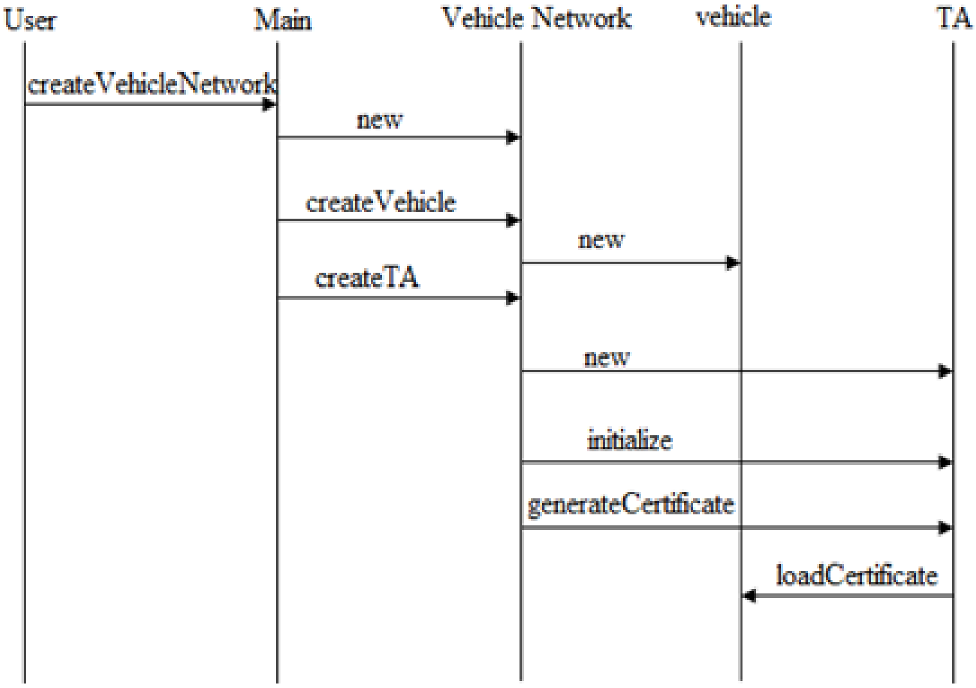


Figure 5: Sequence for Network Initialization

Figure 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.

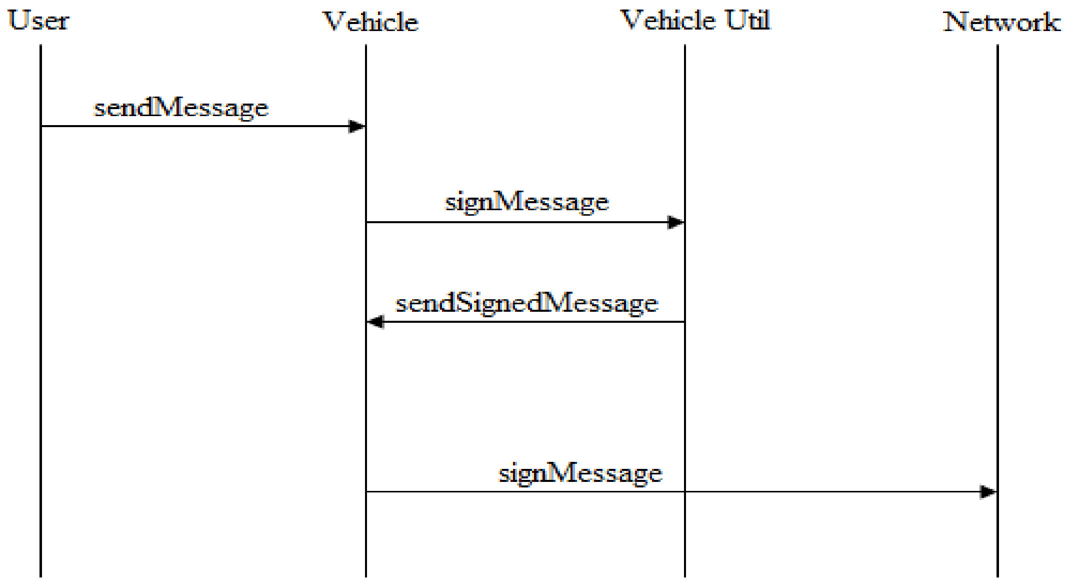


Figure 6: Sequence for message sending flow

The Figure 6 depicts the sequence diagram for message sending. Sender will sign themessage and then sends the signed message to all vehicles.

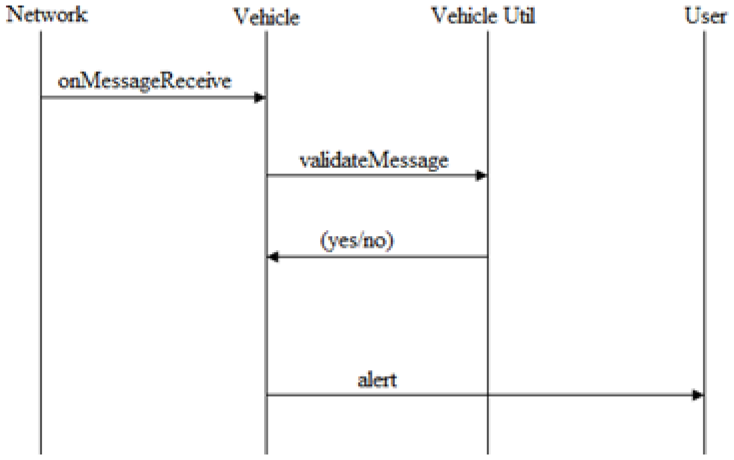


Figure 7: Sequence for Receiving Message Flow

The Figure 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 willbe rejected.

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:** The Figure 8 shows level 0 data flow diagram. It shows interaction between the system and external agent, which acts as source and sink

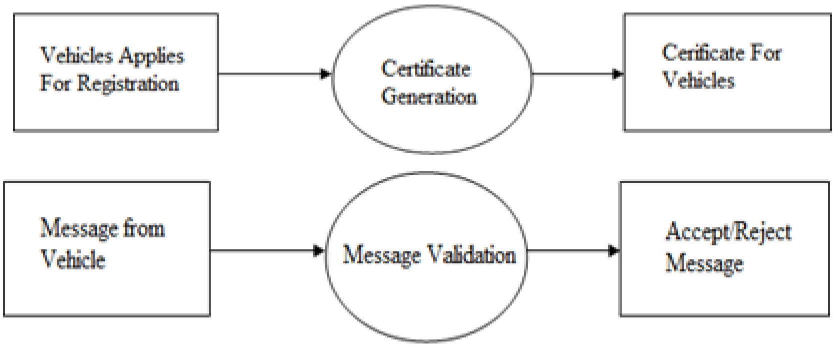


Figure 8: level 0 Data Flow Diagram

- ***Level 1 Data flow diagram:*** The Figure 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

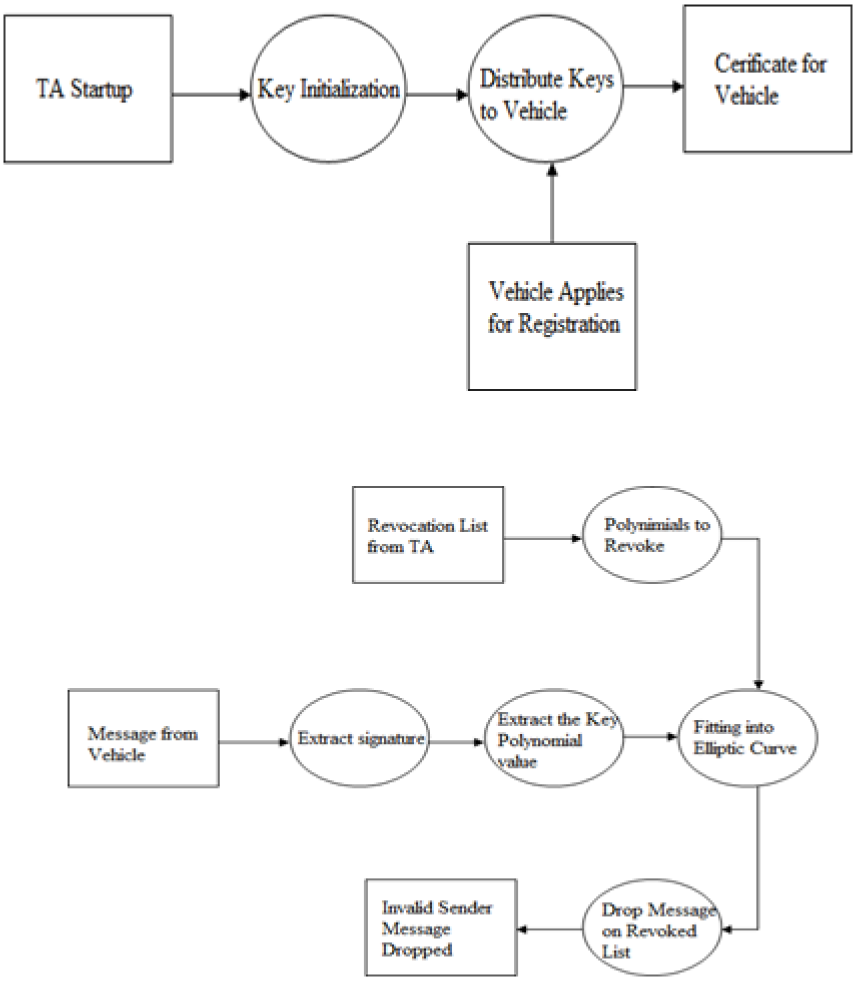

TA Startup
Key Initialization
Distribute Keys to Vehicle
Cerificate for Vehicle
Vehicle Applies for Registration
Revocation List from TA
Polynimials to Revoke
Message from Vehicle
Extract signature
Extract the Key Polynomial value
Fitting into Elliptic Curve
Invalid Sender Message Dropped
Drop Message on Revoked List

Figure 9: Level 1 Data Flow Diagram

V. IMPLEMENTATION

1. **Mobile Node: Creating Wireless Topology:** The table 1 shows available options for node configuration, table 2 shows available options for node configuration in both satellite and wireless oriented. The table 3 shows available options for node configuration with wireless oriented.

Table 1: Available Options for Node Configuration in general

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

Table 2: Available Options for Node Configuration in Both Satellite and Wireless Oriented

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 3: Available Options for Node Configuration in 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

2. **System Model:**

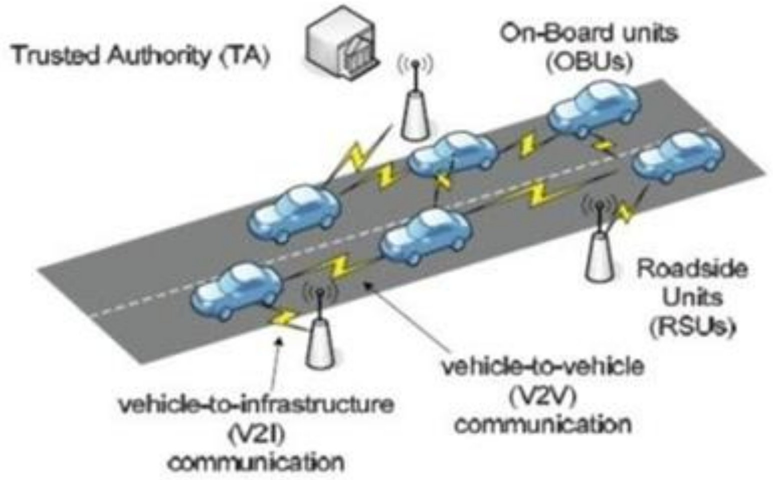

Trusted Authority (TA)
On-Board units (OBUs)
Roadside Units (RSUs)
vehicle-to-vehicle (V2V) communication
vehicle-to-infrastructure (V2I) communication

Figure 10: System Model of VANET

The figure 10 shows system model of VANET, it 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 toTA, 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.

3. **Implementation Steps:**

- System Initialization: Select the prime numbers. Here generate the public key andprivate key.

- For OBU, select the random number and upload secret key and public key.
- Generate anonymous certificate for privacy preserving authentication.
- Message verification done by trusted authority based on certificate signature of OBU
- 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 $(M\|\ T_{stamp}\ \|cer\ u(PID_u, PK_u, sig_{TA}(PID_u \| PK_u))\|REV_{check})$.

- **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 acceptthe 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: $(M\|\ T_{stamp}\ \|cer\ u(PID_u, PK_u, sig_{TA}(PID_u\ \|\ PK_u))\|sig_u(M\|\ T_{stamp})\|REV_{check})$ 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
```

VI. VI.TESTING

1. **Validation Testing :** The outcome of the integration testing is completed and assembled software package. Validation testing can be defined in several ways. Table 4 lists some of the functionalitiesused to test the system.

Table 4: Validation Testing Table

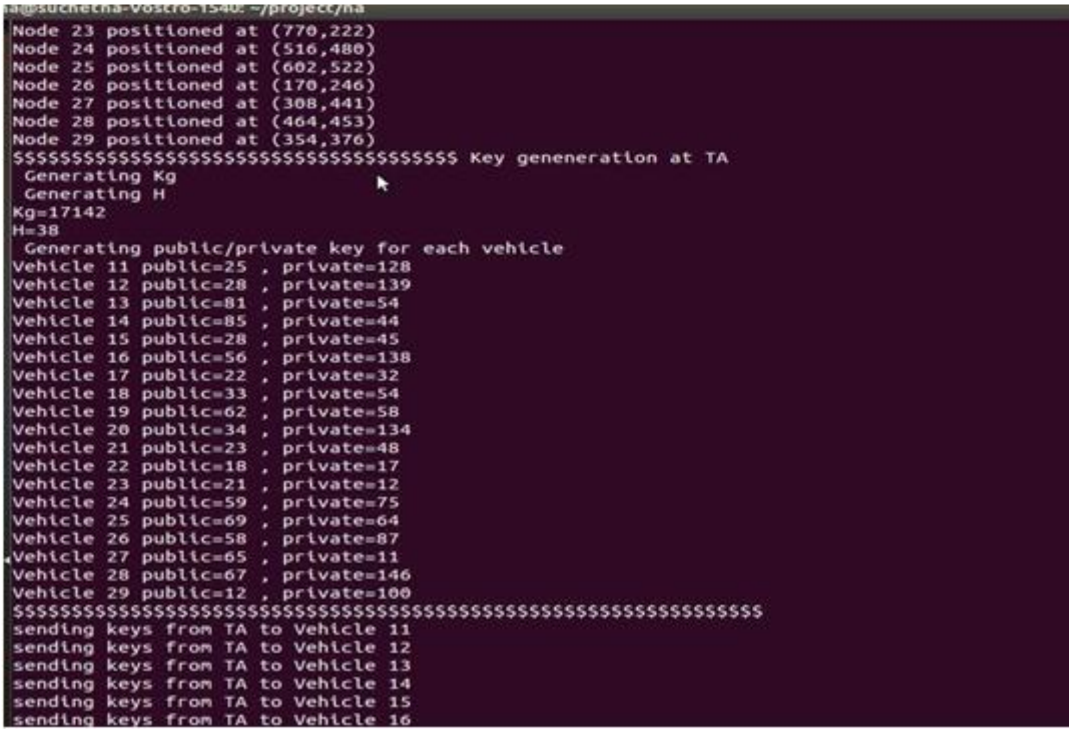
System	Functionality to be tested	Input	Expected output	Actual Output	Remark
MAP	Working of NAM	User interaction through mouse & Keyboard	NAM window appear with nodes placed	NAM window appear with nodes placed	The system is working as expected. So testing is success
	Working of simrun	Node sense events 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	

VII. RESULTS AND ANALYSIS

The work is validated by using simulation and compared it with existing Expedite Message Authentication Protocol (EMAP). The table 5 depicts the simulation parameters and their values adopted for the proje

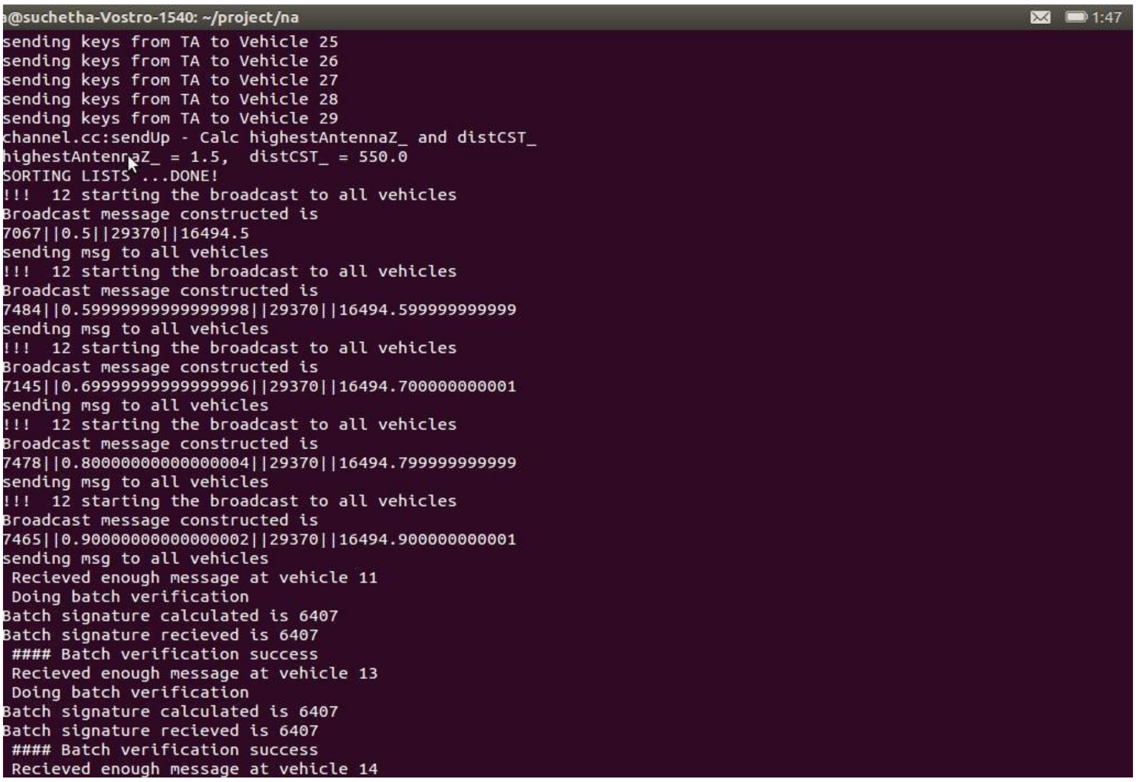
Table 5: Simulation Parameter and their Values

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



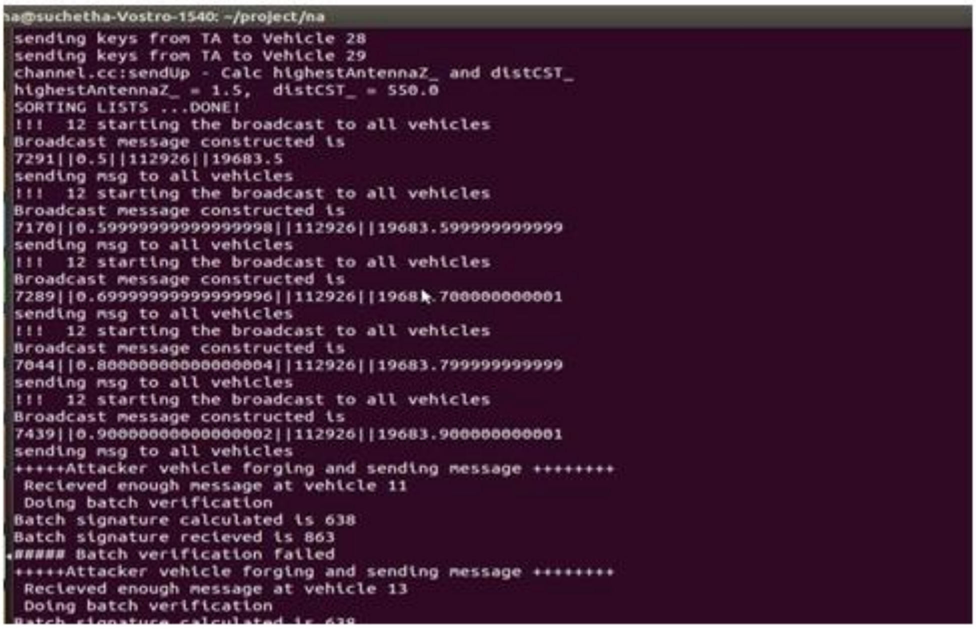
```
Node 23 positioned at (770,222)
Node 24 positioned at (516,480)
Node 25 positioned at (602,522)
Node 26 positioned at (170,246)
Node 27 positioned at (308,441)
Node 28 positioned at (464,453)
Node 29 positioned at (354,376)
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$ Key geneneration at TA
 Generating Kg
 Generating H
Kg=17142
H=38
 Generating public/private key for each vehicle
Vehicle 11 public=25 , private=128
Vehicle 12 public=28 , private=139
Vehicle 13 public=81 , private=54
Vehicle 14 public=85 , private=44
Vehicle 15 public=28 , private=45
Vehicle 16 public=56 , private=138
Vehicle 17 public=22 , private=32
Vehicle 18 public=33 , private=54
Vehicle 19 public=62 , private=58
Vehicle 20 public=34 , private=134
Vehicle 21 public=23 , private=48
Vehicle 22 public=18 , private=17
Vehicle 23 public=21 , private=12
Vehicle 24 public=59 , private=75
Vehicle 25 public=69 , private=64
Vehicle 26 public=58 , private=87
Vehicle 27 public=65 , private=11
Vehicle 28 public=67 , private=146
Vehicle 29 public=12 , private=100
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
sending keys from TA to Vehicle 11
sending keys from TA to Vehicle 12
sending keys from TA to Vehicle 13
sending keys from TA to Vehicle 14
sending keys from TA to Vehicle 15
sending keys from TA to Vehicle 16
```

Figure 11: Generation and Distribution of key’s



```
sending keys from TA to Vehicle 25
sending keys from TA to Vehicle 26
sending keys from TA to Vehicle 27
sending keys from TA to Vehicle 28
sending keys from TA to Vehicle 29
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
!!!  12 starting the broadcast to all vehicles
Broadcast message constructed is
7067||0.5||29370||16494.5
sending msg to all vehicles
!!!  12 starting the broadcast to all vehicles
Broadcast message constructed is
7484||0.59999999999999998||29370||16494.599999999999
sending msg to all vehicles
!!!  12 starting the broadcast to all vehicles
Broadcast message constructed is
7145||0.69999999999999996||29370||16494.700000000001
sending msg to all vehicles
!!!  12 starting the broadcast to all vehicles
Broadcast message constructed is
7478||0.80000000000000004||29370||16494.799999999999
sending msg to all vehicles
!!!  12 starting the broadcast to all vehicles
Broadcast message constructed is
7465||0.90000000000000002||29370||16494.900000000001
sending msg to all vehicles
 Recieved enough message at vehicle 11
 Doing batch verification
Batch signature calculated is 6407
Batch signature recieved is 6407
 #### Batch verification success
 Recieved enough message at vehicle 13
 Doing batch verification
Batch signature calculated is 6407
Batch signature recieved is 6407
 #### Batch verification success
 Recieved enough message at vehicle 14
```

Figure 12: Authentication for the message from sending vehicle without modification



```
sending keys from TA to Vehicle 28
sending keys from TA to Vehicle 29
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
!!!  12 starting the broadcast to all vehicles
Broadcast message constructed is
7291||0.5||112926||19683.5
sending msg to all vehicles
!!!  12 starting the broadcast to all vehicles
Broadcast message constructed is
7170||0.59999999999999998||112926||19683.599999999999
sending msg to all vehicles
!!!  12 starting the broadcast to all vehicles
Broadcast message constructed is
7289||0.69999999999999996||112926||19683.700000000001
sending msg to all vehicles
!!!  12 starting the broadcast to all vehicles
Broadcast message constructed is
7044||0.80000000000000004||112926||19683.799999999999
sending msg to all vehicles
!!!  12 starting the broadcast to all vehicles
Broadcast message constructed is
7439||0.90000000000000002||112926||19683.900000000001
sending msg to all vehicles
+++++Attacker vehicle forging and sending message ++++++++
 Recieved enough message at vehicle 11
 Doing batch verification
Batch signature calculated is 638
Batch signature recieved is 863
##### Batch verification failed
+++++Attacker vehicle forging and sending message ++++++++
 Recieved enough message at vehicle 13
 Doing batch verification
Batch signature calculated is 638
```

Figure 13: Authentication for the message that is modified by the attacker.

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:** It is calculated with respect to number of revocation. The figure 14 and figure 15 shows delay Vs number of revocation for proposed method and EMAP method respectively.

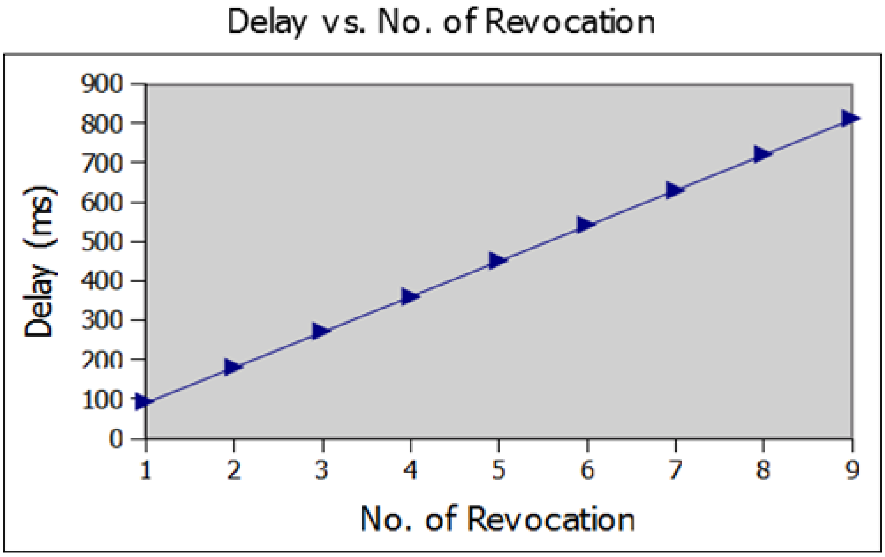


Figure 14: Delay vs. No. of Revocation in EMAP

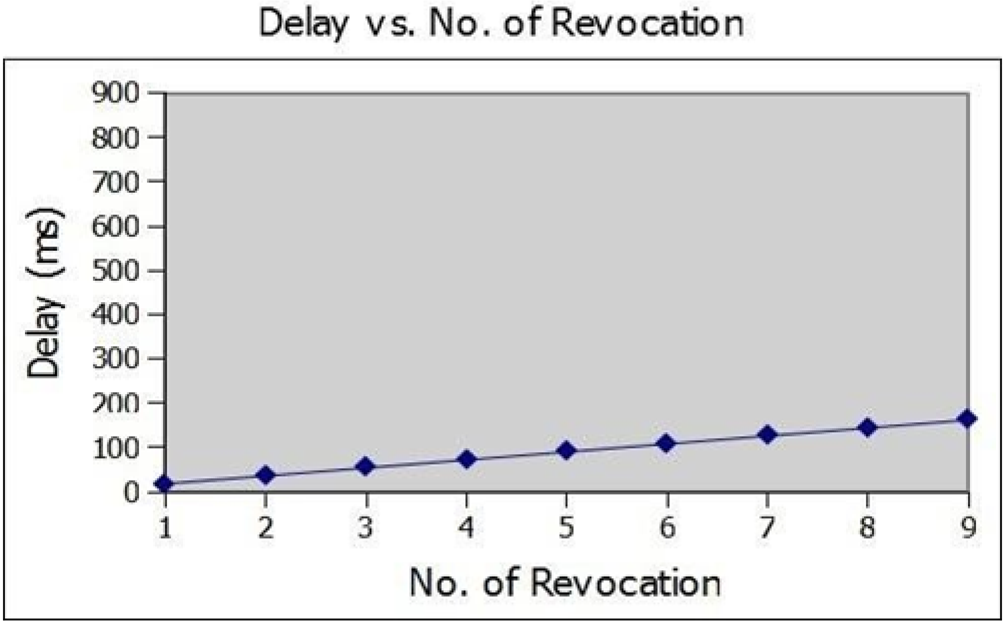


Figure 15: Delay vs. No. of Revocation in MAP

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. The figure 16 depicts the comparison between proposed method and existing method i.e. Expedite message authentication protocol (EMAP).

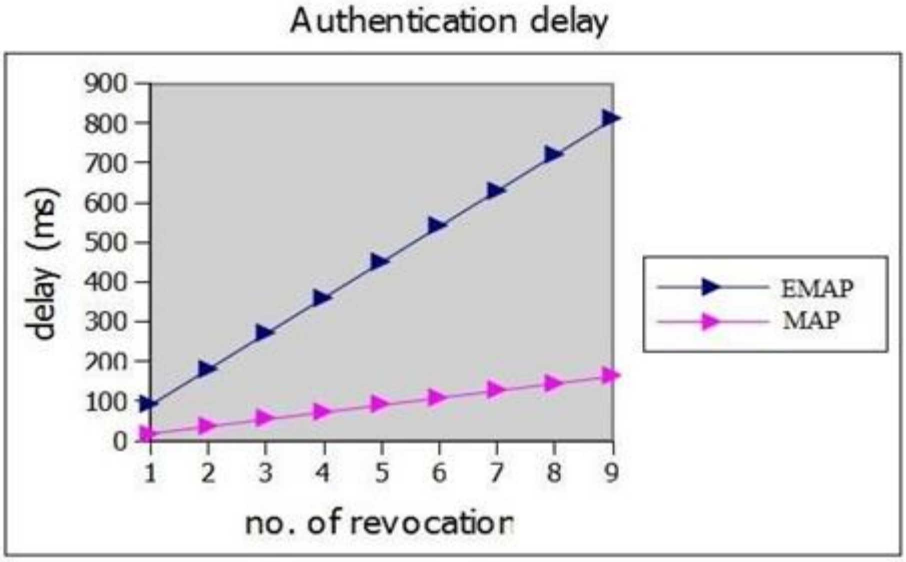


Figure 16: Comparison of Authentication delay of EMAP and MAP

2. **Communication Overhead:** It is calculated with respect to number of revocation. The figure 17 and figure 18 shows delay Vs number of revocation for proposed method and EMAP method respectively.

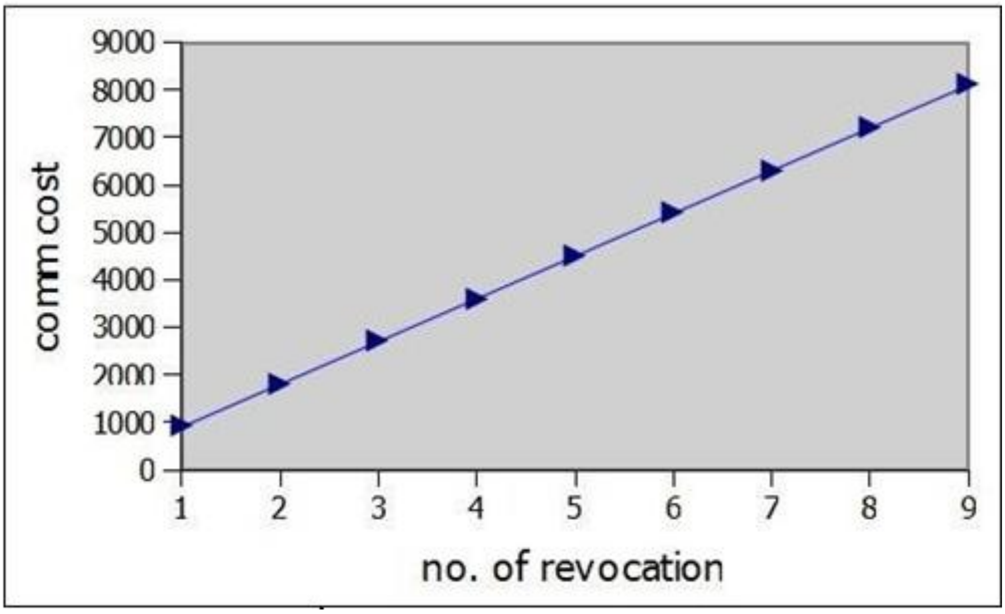


Figure 17: Communication Cost in EMAP

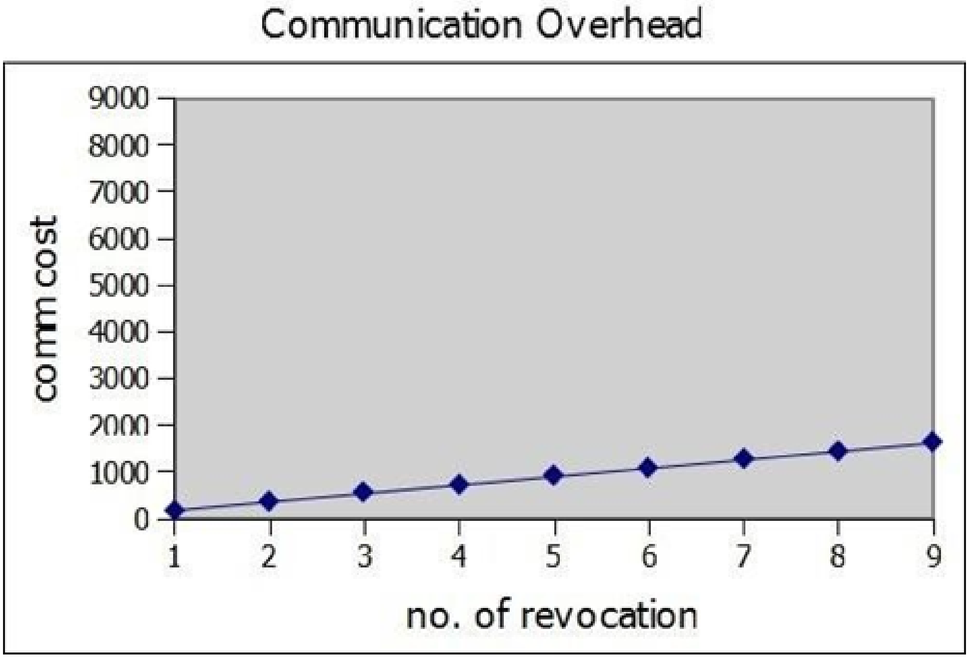


Figure 18: Communication Overhead in MAP

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

- Sending signature in each message by the sender.
- Receiver verifying the Hash for every message.

So that communication overhead is reduced. Figure 19 depicts the comparison between proposed method and existing method i.e. Expedite message authentication protocol (EMAP).

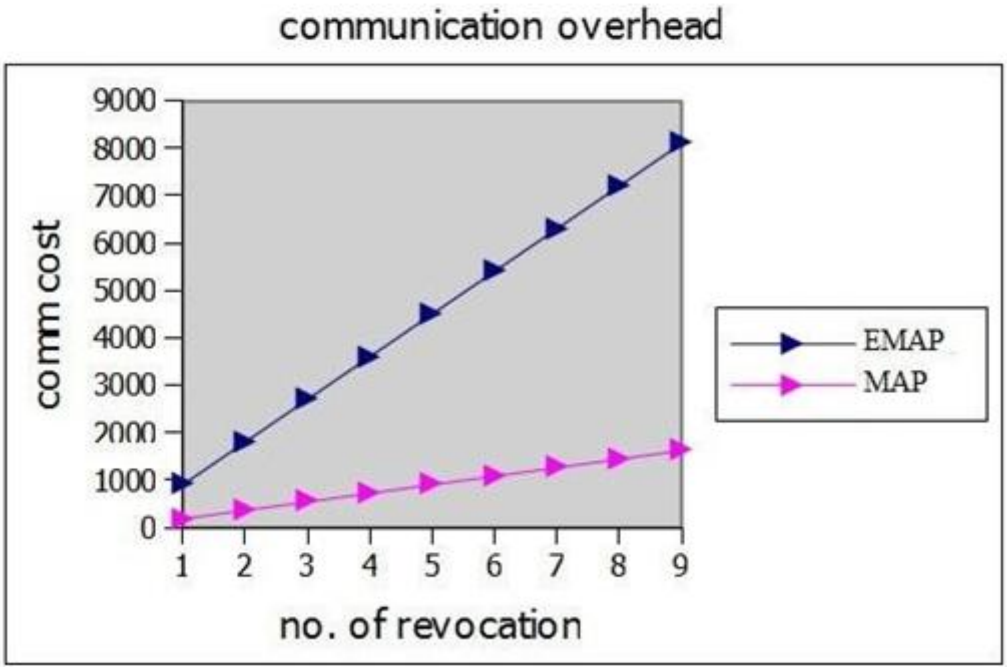


Figure 19: Comparison of Communication Overhead of EMAP and MAP

VIII. CONCLUSION AND FUTURE WORK

1. **Conclusion:** In this project, the authentication process is accelerated for VANETs, swapping out the time-consuming CRL checking procedure for a quick revocation checking process that uses the HMAC function to reduce authentication delay. Therefore, compared to traditional authentication methods that use CRL checking, it greatly reduces the message loss ratio due to message verification time. Additionally, it lessens communication and authentication overhead. Additionally, it is resistant to collusion, replay, and forging assaults.

2. **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 forVehicular 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 SensorNetworks,” 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 AuthenticationScheme 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.