Efficient Authentication Scheme for Vehicular Ad Hoc Networks

E. Indhumathi, MCA.,M.Phil.,#1 Dr. Julia Punitha Malar Dhas, M.E., Ph.D.,#2
Mr. J. P. Jayan., M.C.A., M.Phil., (Ph.D.,)#3

[1]*Research Scholar in Department of Computer Science, Noorul Islam Centre for Higher Education, Kumaracoil, Kanyakumari District, Tamilnadu State, India – 629 180.*

[2] *Professor & Head , Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, Kanyakumari District, Tamilnadu State, India – 629 180.*

[3]*Assistant Professor & Head, Department of Software Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, Kanyakumari District, Tamilnadu State, India – 629 180.*

Abstract

VANET Consisting of a network of vehicles, moving at a reasonably high speed that communicate between themselves with different purposes existence the main purpose that of improving security on the road. Due to rapid topology changing and regular disconnection creates it difficult to design an efficient authentication scheme for VANETs. The existing schemes that provide authentication require high computational cost and suffer from message loss. The Proposed system offers a computationally efficient authentication scheme for VANETs. In the proposed scheme digital signature is used to sign every message. To confirm the integrity also authenticity of the messages bilinear pairing is used. The proposed scheme also provides a conditional tracking mechanism to find the malicious vehicles in VANET. The proposed system is conditionally efficient with respect to efficient authentication also maintaining privacy in VANETs.

1. INTRODUCTION

In the future years, the transport industry will see a interesting period of main changes also evolution nice one to the implementation of Intelligent Transport Systems (ITS). Probably, one of the most exciting characteristics of ITS is the interchange of data between cars that growth the traffic awareness of car user, and even of cars in case of extremely autonomous driving. The supposed Road Hazard Warning messages can be communicated upon detection of a hazardous incident. Even though these messages were primarily supposed to be locally spread, in many cases, distant cars can advantage from getting remotely produced RHW messages, e.g., more than a few kilometers away, so that the car user and the car itself can act as a result and even adjust the path VANET is another technique of Mobile Ad-hoc Network in which the vehicle can change their location individually within the coverage range and they can connecting with other vehicle without any fixed infrastructure. The nodes in the VANET may include a vehicle, or Road Side Unit (RSU). Hence the VANET technology provides good traffic efficiency and road safety. The vehicles are issued with the on-board Unit (OBU) device which performs the communication in the VANET where in the huge self-organized network communication is performed.

VANET provides safety driving and comfort to the drivers in the network. A vehicle in the network transfer its traffic information to all others vehicle in the network that makes other vehicles to avoid accidents in advance. In addition, the vehicles can able to share some other information like tourism evidence, hotel information, movie files which make their journey more comfortable. Even though the VANET have many advantages and useful applications to implement, it has some authentication, security and privacy preserving issues that must be addressed and resolved.

There are many security requirements to be satisfied by the VANET environment which include sender authentication to provide that the message is received from the valid person, privacy preserving which maintain the message between sender and receiver in private and also protect the route of the vehicle which should not be traced by other unauthorized party. If the security and privacy preserving setting are not delineated genuinely, then the real identity of the vehicle is found which leads to fraudulent activity.

2. RELATED WORK

In this sector, we briefly present the authentication scheme for the VANETs.

X. Linetal. had proposed a vehicular communications based on cluster signature and characteristics based signature techniques, called GSIS by secure and privacy preserving protocol. Their scheme guarantees anonymity, privacy and other basic cryptographic necessities. And also provide traceability service for each car. The identity of the message sender allows to see the expert witness when any difference of opinion happens. They use the cluster signature for message between one vehicle and other vehicle. And the identity based signature system is taking on at RSUs to digitally sign every message launched by RSUs to make sure its validity. But this protocol has susceptibilities compact with car movement tracing when many of the RSUs are taken by attacker.

R. Luetal. had proposed an privacy preservation protocol for secure vehicular communications founded on bilinear pairing, called ECPP. Their protocol guarantees anonymity, privacy and other basic cryptographic requirements. And also provide traceability. But this protocol has susceptibilities contract with car drive following when numerous of the RSUs remain took by attacker. It is characterized by the group of on-the-fly short-time nameless solutions amid vehicle and RSU. Then it contain contract with the growing re-vocation slope by providing traceability. But it has a large overhead for generating the anonymous key and communication.

C. Zhangetal had proposed asite for preservative verification arrangement founded on sightless name popular the elliptic arc area. The arrangement can provide wild re-authentication, and promise privacy, anonymity, then other basic cryptographic requirements. But it doesn’t provide traceability. In order to preserve the worker site confidentiality, they usage the BLS, which is working to identify the individuality and the route of a car.

The site confidentiality preservative verification arrangement consider authentication, when car has delivery procedure in between RSU and the further RSUs. So it consumes fast re-authentication technique. However, they must have communication between vehicle and CA when the initial authentication with RSU. This process has a very large communication overhead.

Hu Xiongetal., had proposed a two counter measures that act against the fraudulent messages created by the malicious vehicles. The Trusted Authority (TA) is having the ability to find the real identity of OBU targeted to discuss the traffic events. This is possible for the trusted authority alone, but the public cannot find the real identity of any node. The second one is capable of preventing the fraudulent message generation. In this method, the receiver will accept the received message as valid only if the message has been supported by some vehicle more than the threshold. The Efficient Privacy Preserving Authentication Protocol takes achieved the posteriori and priori remedies, efficiency and threshold adaptively.

The Efficient Privacy Preserving Authentication Protocol scheme takes the four sequential steps namely: OBU Safety Message Generation, Message Verification, system initialization, and OBU fast tracing. The Trusted Authority (TA) design the signature from the On-Board Unit (OBU) and the Road Side Unit (RSU) translate that signature. The signature is again delegated with respect to the TA public key and stores the re-signature in the RSU. On the receiver side, the receiver receives the message and resigns it using re-signature key after validation. There is possibility that any vehicle in the networks can able to verify the message and use the information. So the proxy re-signature is used to cover the identity of the real OBU. This protocol is the extra time of proxy re-signature system which also maintains the authentication with trust worthy.

SubirBiswas and JelenaMisicetal, had presented priority-based safety message verification in VANET which comprises of message authentication and the prioritized verification of road safety messages as the message verification time is longer in VANET. In the heavy traffic area, the periodic authentication of safety message and checking all the signatures in emergency becomes an important problem. This problem cannot be avoid completely, but it can be reduced considerably by prioritize the received messages for verification.

This new verification method based on priority has many steps to do the verification. They are as follows: first step is key initializing module where the vehicle secret key is generated and copied in the disk space of the corresponding OBU. Second is pre-processing stage. It verifies whether the emergency message correlates with the vehicle position and the current system time. If it matches, then the session parameter is generated by using the current system time and the corresponding area location by the authorized. Third step is signature generation from which the signature of the emergency message is generated. Finally the receiver verifies the source node and the received message’s integrity. This cross layer verification scheme uses MAC layer traffic class and traffic intensity for better verification of emergency messages. Different advantages such as reduce the overhead in updating the certificate, authentication overhead and revocation overhead in the vehicular network.

Different from these schemes, we propose a original efficient nameless authentication arrangement. Our scheme guarantees anonymity,privacy and other basic cryptographic necessities. And also provide traceability. Authentication schemes in VANETs require anonymity and confidentiality preserving. At the same time, it need to provide traceability to save a car’s actual individuality.

3. PRIVACY PRESERVING ANONYMOUS AUTHENTICATION SCHEME IN VANET

The proposed scheme involve public key generation in n vehicles V = {V1,V2,...,Vn}; it contains of the six algorithms: Pseudo-Identity Generation/Private Key Extraction, System Initialization,Message Signing Phase,Traceability, Verification and Revocation, andBatch Verification.

System Initialization it implemented by trusted authority that takes as information a security limitation to produce a public key generation separately and some road infrastructure parameters. The public key generates information in individually.

Private key generation it performs by public key generation that takes as information a vehicle.

Message Signing its performed by every vehicle Vi that takings as information its pseudo-ID also relating private keys.

Singular check is implemented by every car that takings as information the ace public key, a car's pseudo-ID and relating message and it is mark σ, yield genuine if the mark is legitimate, or false something else. Clump check is implemented by RSU, also the procedure is like separate confirmation.

Traceability: It is implemented by Trusted Authority that takings as information a car's pseudo-ID, yield the car's genuine character.

Revocation: It is implemented by Trusted Authority that takings as info a car'sgenuine personality, yield a refreshed enouncement list as well as the car which send to PKG.

A. System Initialization

In this phase, every appliance in VANETs performs initialization.

(1) PKG generates fundamental system parameters including a group over the chosen elliptic curve Ep(a; b), a random number SKmsk∈Zq∗ as the systemmaster key, also the system public key computed as follows,

$$\mathrm{PKpub} = \mathrm{SKmsk} \cdot P \ldots\ldots\ldots...(1)$$

(2) PKG selects a random number SKT P D ∈Zq∗ as the private key of the helper (TPD) and calculates its corresponding public key

$$\mathrm{PKT\ PD} = \mathrm{SKT\ PD} \cdot P \ldots\ldots\ldots..(2)$$

All these four parameters should be preloaded into TPD.

(3) RSU selects a random number SKrsu∈Zq∗ as its private key also computes the corresponding public key

$$\mathrm{PKrsu} = \mathrm{SKrsu} \cdot P \ldots\ldots\ldots..(3)$$

(4) PKG publishes the public parameter set: param = {a; b; p; q; P; P Kpub; P KT P D; P Krsu; H1; H2; H3; H4}.

Assume that the OBU's public key and its TPDpublic key have been preloaded.

B. Key Generation

1. Initial key generation

Set the parameter n corresponding to the time period n as n = H2(H1(IDobu) ‖ SKT PD · P Krsu‖Tn). Note that it is default for TPD to keep its OBU's identity. TPD computes 0 = H2(H1(IDobu) ‖ SKT PD · PKrsu‖ T0) and the initial private key of the OBU as SKobu0 = SKmsk · H1(IDobu) + SKT PD·0, which is preloaded into the OBU.

2. Partial key generation

TPD calculates,

$$\mathrm{Kparti} = \mathrm{SKT\ PD} \cdot (i - i-1) \ldots\ldots\ldots.(4)$$

as the partial key consistent to the time period i, and sends it to the OBU to assist in generating the temporary secret key.

3. Temporary secret key generation

OBU calculates its own temporary secret key in the time period i

$$\mathrm{SKobui} = \mathrm{SKobui}-1 + \mathrm{Kparti} \ldots\ldots.(5)$$

as soon as it receives Kparti from the TPD.

The temporary public key in the time period n of OBU is set as PKobui = SKobui and it is published by the OBU, while the partial key Kparti and the initial key SKobui−1 are removed after key updating.

4. Signing Stage

An OBU can generate the signature on message Mi in the time period i as follows,

Step 1.Selects the random number ui∈Zq∗ to compute.

$$\mathrm{Ui} = \mathrm{ui} \cdot P \ldots\ldots\ldots\ldots\ldots..(6)$$

Step 2. Uses the identity IDobu, the temporary secret key in the time period i SKobui, the public key of RSU P Krsu, the corresponding time stamp Ti and hash functions to compute

$$n = \mathrm{H1(IDobu)} \oplus \mathrm{H3(SKobui} \cdot P\ \mathrm{Krsu)} \ldots\ldots\ldots..(7)$$

$$i = \mathrm{H2(H1(IDobu)} \parallel \mathrm{SKobui} \cdot P\ \mathrm{Krsu} \parallel \mathrm{Ti)} \ldots\ldots.(8)$$

Step 3: Selects another random number i ∈Zq∗, and uses the identity and i to compute

$$n = i + i \cdot \mathrm{H1(IDobu)} \ldots\ldots\ldots\ldots\ldots..(9)$$

Step 4: Concatenates the hash value of identity

H1(IDobu), i, Ui, the message about traffic status

Mi and current time stamp Ti to compute

$$n = H4(H1(IDobu) \| i \| Ui \| Mi \| Ti)\text{……(10)}$$

Step 5: Uses the two random numbers ui and i, i, and the temporary secret key SKobui to compute

$$i = i \cdot SKobui + i \cdot ui \mod p\text{…………..(11)}$$

Step 6: Sends the message {Ui; i; !i; i; Mi; Ti} to the regional RSU.

5. *Verification Stage*

Upon receiving the signature, RSU proceeds with the given steps for verification: Step 1. Examines the freshness of Ti. If it is fresh, goes to step 2; otherwise, the signature is rejected. Step 2. Uses own secret key SKrsu, the private key in the time period i of the vehicle P Kobui and Ti to count the hash value of identity of the vehicle:

$$H1(IDobu) = Ti * H3(SKrsu \cdot P\,Kobui)\text{…….(12)}$$

3. Uses the hash value of IDobu, its own secret key SKrsu, the private key of the car, the private key of TPD and current time stamp Ti to evaluate.

$$n = H2(H1(IDobu) \| SKrsu \cdot P\,KT\,P\,D \| Ti)\text{ ...(13)}$$

and

$$n = H2(H1(IDobu) \| SKrsu \cdot P\,Kobui \| Ti)\text{….(14)}$$

4. Uses the hash value of IDobu,

5. Concatenates the hash value of IDobu, i, Ui, the message about transaction status Mi and current time stamp Ti to evaluate

$$n = H4(H1(IDobu) \| i \| Ui \| Mi \| Ti)\text{…………..(15)}$$

6. Checks whether the equation

$$i \cdot P = (H1(IDobu) \cdot PKpub + PKTPD \cdot i) \cdot i + Ui \cdot i$$

If it holds, the signature is valid.

The proposed scheme, a Road Side Unit will effectively certify vehicles in an anonymous manner in advance provided that Site Founded Care Info mails to cars. Similarly, buses may certify an RSU in an nameless way in advance receipt Location Based Safety Information (LBSI) messages from RSUs.

The proposed scheme with relevance message integrity, source verification, conditional privacy preservation and identity privacy preserving. Within the Efficient unknown Authentication Scheme with Privacy Preserving scheme, certificate and signature are used for basic security defenses in contrast to shoot up, masquerade, impersonate and also key duplication attacks. Using this scheme, an external attacker can't create a valid certificate and signature and using different vehicles anonymous signature and also certificates, for the reason that acknowledgment is kept back in secure surroundings like TPD by the user. It's unfeasible to insert false mails into the scheme and also achieve crucial duplication bouts. It's unfeasible to insert false messages into the scheme and furthermore accomplish key duplication assaults. To accomplish a pantomime assault, the assailant should determine the transitory little time keys claimed by suitable vehicle and furthermore the confirmation key give out by the Trusted Authority to a particular vehicle. Then again, the assailant can't trade off the enlistment convention because of it's accomplished in disconnected mode straight at the Trusted Authority the Trusted Authority. From this time our system is semantically secure in contradiction of impersonation attack.

C. *Architecture design*

The Trusted Authority is in charge for keep up the complete VANET system. The Trusted Authority is well thought-out to be totally trusted and incapable of being carried out for any rival to compromise. The Trusted Authority also need to check the Road Side Units and vehicles, as soon as they are connected to the net. In this arrangement, the complete street transport scheme stays split hooked on more than a few geographical regions and every region has a Trusted Authority. As soon as a car changes since unique geographical area to extra geographical division, the car is genuine in the Trusted Authority of the fresh geographical area using the community price of the Trusted Authority of the listed geographical region. The civic price of every Trusted Authority remains exchanged by the Trusted Authorities of extra geographical areas to cheered the legality of the cars within the circumstance of car wandering after solitary geographical area to additional geographical area.

The Trusted Authority delivers the underlying security confinements aimed at entirely cars then Road Side Units then these impediments are delivered toward cars and Ride Side Units afterward the effective fruition of their registering. Road Side Units stay steady frameworks, sent happening the roadside. Ride Cross Units action on the grounds that the scaffolds between the Trusted Authority and vehicle client that associate with Trusted Authority by make safe wire connections and vehicles by a remote system. Both cars inside the VANET is settled by an OBU, which enables the car toward associate by various cars and Road Side Units to part mails to brand heavy extra agreeable. The OBUs must stayed settled in the vehicles, the cars remain known as scholarly transportation cars.

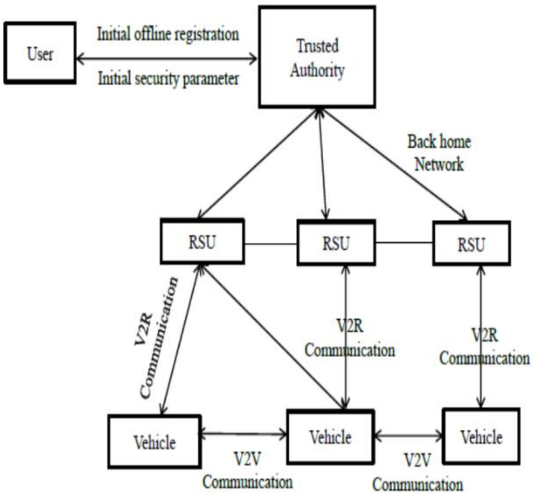

Fig. 1 Architecture Design

D. *System flow design*

The VANET user registered in TA. The user submitting essential user data such as name, license number, phone number etc. TA starts generating keys for every vehicle by the key generation process. If denote vehicle user as OID then TA generates ID as user original identity. Then TA generates dummy identity for the same user. In terms of temporary identity of a user, TA selects a random number. The same way Trusted Authority generates the dummy identities of Road Side Units. Since every vehicle has to verify the message source, Trusted Authority is only responsible authority to do the mapping from unique identities to fake identities.

Vehicles and Road Side Unit’s use anonymous signatures and certificates to protect their original characteristics since different vehicle workers. On the other hand, the Trusted Authority takes the competence to suggestion the innovative individuality of a vehicle or a Road Side Unit after its unknown document. Aimed at example, once a car sends a fake message along with an anonymous certificate the Trusted Authority can checked the at ease of the message. If it’s fake, then the Trusted Authority change to the unknown certificate of that message and maps the anonymous certificate with the tracking list. Since the mapping, the Trusted Authority can trace the actual identity of a car successfully. The Trusted Authority can make known the privacy of the car user and revoke that user from VANET. Verification of anonymous messages: For the given message receiver performs couple of steps as follows: Receiver is unable to verify the message directly, Thus receiver the receiver authenticates the sender otherwise receiver discards the message as unauthorized message. Receiver can also authenticate ID to confirm that only registered vehicles are permitted to broadcast messages.

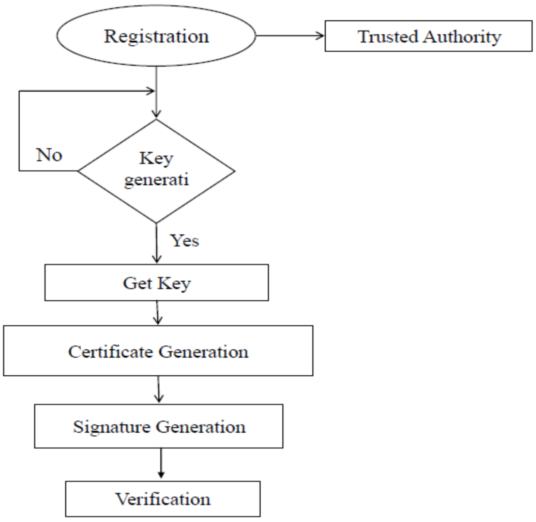

Fig. 2 System Flow Diagram

IV. PERFORMANCE ANALYSIS

The volumetric mass density, of a substance is its mass each unit measurements. The image frequently utilized for thickness is ρ (the lower case Greek letter rho), despite the fact that the Latin letter D can likewise be utilized. Numerically, density is characterized as mass by volume:

$$\rho=x/v$$

where, ρ is the density, V is the volume and m is the mass. Sometimes, density is inexactly characterized as its weight per unit volume, in spite of the fact that this is experimentally incorrect – this amount is called particular weight.

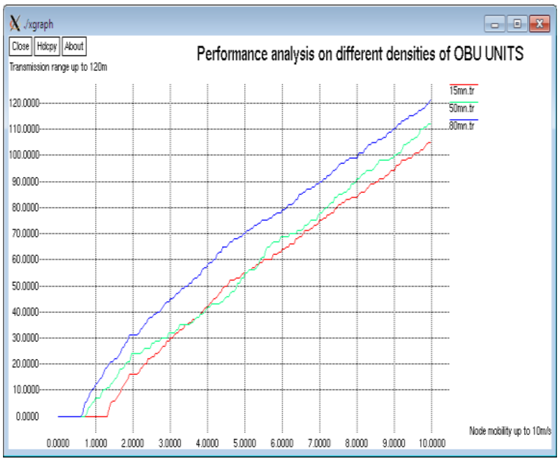

Fig. 3 Performance Analysis on DifferentDensities of OBU Units

A. *Throughput*

As a rule terms, throughput is the most maximum rate of generation or the greatest rate at which approximately can be prepared. At the point when utilized as a part of the setting of communication systems, for example, Ethernet or bundle radio, throughput or system throughput is the amount of message transportation over a communication channel. The information messages have a place with might be taken over a physical or consistent association, or it can go through a specific system hub.

Throughput is normally estimated in bits every second (piece/s or bps), and some of the time in information parcels every second (p/s or pps) or information bundles per availability. Throughput of receiving packets: It says the throughput of receiving packages on XY axis, by throughput of receiving parcels i.e. no. of packets got per second on y axis and time on y axis.

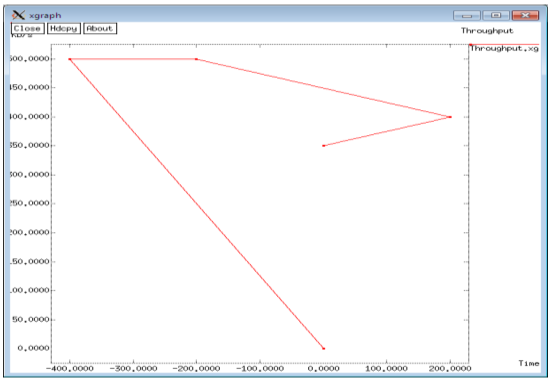

Fig. 4 Throughput

B. Packet delivery ratio

The control of Packet Delivery Ratio (PDR) depends on the received and created packages as recorded in the following document. When all said is done, PDR is characterized as the proportion between the received packets by the goal and the created bundles by the source.

The pack sending ratio is the amount of the quantity of packages received by the goal to the quantity of bundles created by the source hub. The Proposed system plays out the best regarding parcel conveyance proportion took after by AODV. This is grounded to built up course by proposed convention are remained alive longer time contrasted with that of different conventions and stable in nature. Thus, the quantities of parcels dropped are lesser because of absence of vitality at halfway hub of the course amongst source and goal.

.

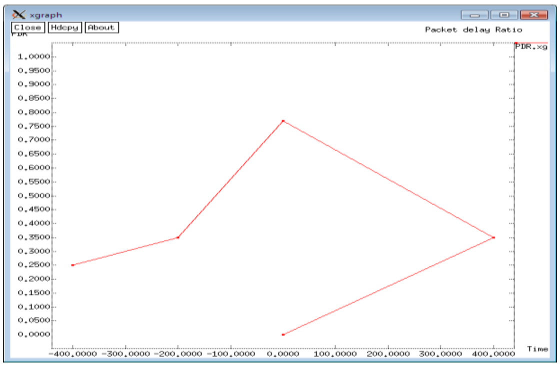

Fig. 5 Packet Delivery Ratio

C. Packet drop

Packet drop status tells the actual status of the packets (i.e. how many packets are send, how many are received and how many of them are dropped during the process). Here is a graph plotted on the XY axis. Time in seconds is on the X axis and traffic on the Y axis. Red color signifies the message, blue is indicating the acknowledgement and green one is showing TCP. TCP sink basically tells us about the source node i.e which node can be considered as a source node also the path of the node.

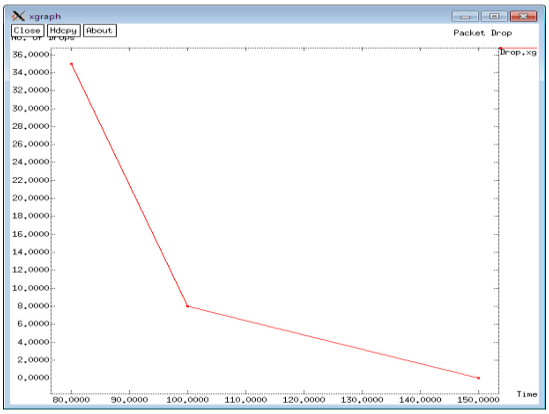

Fig. 6 Packet Drop

D. End to end delay

It says us about how many packs are generated other than their pack identification. Here is a graph in which packs are generated is plottedon the XY axis. When a pack is transmitted, some packet delay comes. Like if 1000 packets are to be transmitted, all the 1000 cannot be transferred at one time, but the packs can be transferred in installments, thereby resulting in the pack delay.

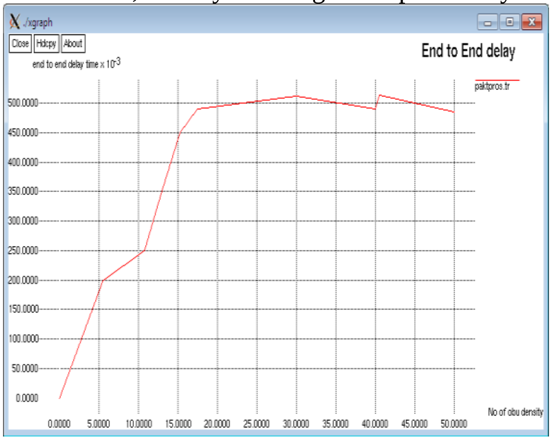

Fig. 7 End to End Delay

V. CONCLUSION

The proposed new system called EAAP for protected vehicular message in VANETs. In the future EAAP plot, a RSU container adequately confirms buses in an unknown way ahead of giving LBSI mails to buses. Additionally, buses can likewise confirm a RSU in a mysterious way before getting LBSI mails from RSUs. EAAP conspire not just gives the unknown validation little down certificate then symbols verification prices which are basically necessary in the VANET functions, yet additionally ready to give an efficient security following component to uncover the genuine personality of the vindictive car for improving the effectiveness of the VANET scheme. The future EAAP system gives improved effectiveness as far as quick verification of certificates and symbols than the beforehand announced plans, ECPP, KPSD, BLS, GSB and CAS. The future augmentation of this work is to give cluster confirmation low computational rate in an efficient system.

The proposed EAAP system gives better efficiency as far as quick verification on certificates and marks than the beforehand announced plans efficient restrictive protection conservation convention (ECPP), Certificate less Aggregate Signatures (CAS), Group signature Based (GSB) and Key-protected Pseudonym Self Delegation (KPSD). The future augmentation is to give cluster verification low computational cost in an efficient way.

REFERENCES

[1] R.Lu, X. Lin, T. H. Luan, X. Liang, and X.Shen, "Anonymity analysis on social spot based pseudonym changing for location privacy in VANETs," in Proc. IEEE ICC, Kyoto, Japan,Jun. 2011, pp. 1–5.

[2] X.Lin, R. Lu, C. Zhang, H. Zhu, P. H. Ho, andX. Shen, "Security in vehicular ad hoc networks," IEEE Commun. Mag., vol. 46, no. 4, pp. 88–95, Apr. 2008.

[3] I.Blake, G.Seroussi, and N.Smart, Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series), vol. 317. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[4] N.Koblitz, "Elliptic curve cryptosystems," Math.Comput., vol. 48, no. 177, pp. 203–209, 1987.

[5] A.Dhamgaye and N.Chavhan, "Survey on security challenges in VANET," Int. J. Comput. Sci. Netw., vol. 2, no. 1, pp. 88–96, 2013.

[6] I.F.Blake, V. K. Murty, and G. Xu, "Refinements of Miller's algorithm for computing the Weil/Tate pairing," J.

[7] M.Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Secur., vol. 15, no. 1, pp. 39–68, 2007.

[8] C.Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in Proc.IEEE INFOCOM, Apr. 2008, pp. 246–250.

[9] H.Zhu, X. Lin, R. Lu, P. H. Ho, and X. Shen, "AEMA: An aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks," in Proc.IEEE ICC, May 2008, pp. 1436–1440

[10] M.Raya, P. Papadimitratos, and J.-P. Hubaux Securing vehicular communications," IEEEWireless Commun., vol. 13, no. 5, pp. 8–15, Oct.2006.

[11] M.Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," in Proc. 3rd ACMWorkshop Secur. Ad Hoc Sens. Netw., 2005, pp.11–21.