International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 7 (2015) pp. 17695-17710

http://www.ripublication.com

A Novel Message Verification Scheme For Vehicular Interaction Networks Using EMAC Algorithm

Dr.D.David Neels Ponkumar
Associate Professor, Dr.Sivanthi Aditanar College of Engineering,

Ms. I.Elaveni
Assistant Professor, Dr.Sivanthi Aditanar College of Engineering,

Ms. C.K.Balasundari
Assistant Professor, Dr.Sivanthi Aditanar College of Engineering,

Mrs. S.Janeshwari
Einstein College of Engineering

Abstract

Vehicular Ad-Hoc Networks (VANET) is built with the intention to communicate between vehicles or infrastructures. It provides the ease of driving and the secure driving to reduce accidents. In VANET, the security and privacy are more important because they are related to accidents and tracking the location of vehicles and users' identity respectively. VANET is authenticated by Key Infrastructure and Revocation List. The Certificate Revocation List Verification process can be done after receiving a message from other vehicles at every OnBoard Units. The proposed revocation check process is Enhanced Message Authentication Code (EMAC), uses a keyed Hash Message Authentication Code where the key used in calculating the hash code. The proposed scheme discussed about the verification process at On Board Unit and Road Side Unit. Extensive simulations are conducted to verify the proposed scheme and develop a medium access control (MAC) layer analytical model to examine the packet delivery ratio and packet service time with the proposed work implemented over vehicular based networks.

Introduction

Vehicular ad-hoc networks (VANET) is a collective technology of Mobile Ad-hoc Network, can provide communications between vehicles or infrastructures. Vehicular Ad Hoc Networks (VANET) collects and distribute safety information to massively

reduce the number of accidents by warning drivers about the danger before they actually face it. Such networks comprise of sensors and On Board Units (OBU) installed in the car as well as Road Side Units (RSU). The sensors on the vehicles collect the data and display them to the driver, sent to the RSU or even broadcasted to other vehicles depending on its nature and importance. This data is distributed along with data from road sensors, weather centres, traffic control centres, etc to the vehicles and also provides commercial services such as parking space booking, Internet access and gas payment. VANET can be divided into two ways, a Vehicle-to-Infrastructure (V2I) communication, and a Vehicle-to-Vehicle (V2V) communication by communication method. The V2I communication is a communication between a vehicle and Road Side Unit (RSU), which is connected with an existing infrastructure and mainly provides convenience to users such as multimedia. The communication between near vehicles, and for exchanging critical messages mainly about preventing accidents are done by V2V Communication. There are two services provided by vehicular communications, which are safety message and non-safety message.

Vehicular ad hoc networks can be seen as a component of the intelligent transportation systems (ITS). As promoted in ITS, vehicles communicate with each other via inter-vehicle communication (IVC) as well as with roadside base stations via roadside-to-vehicle communication (RVC). Vehicular Networks (also known as VANETs) are a keystone of the envisioned Intelligent Transportation Systems (ITS). Vehicular networks will contribute to safer and more efficient roads by providing timely information to drivers and concerned authorities.

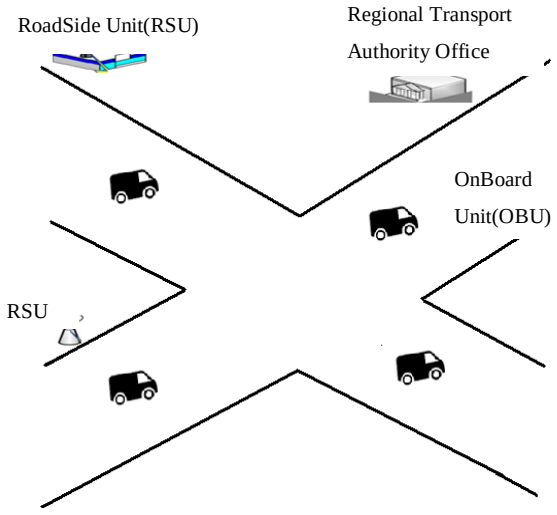

Figure 1: Vanet Architecture

The major purpose of VANET is to enlarge road safety. This is attained by the vehicles act as sensors and exchange warnings or more generally telematics information (like current speed, location or ESP activity) that permit the drivers to react early to abnormal and potentially dangerous situations like accidents, traffic

jams or glaze. The information provided by other vehicles and stationary infrastructure might also be used for driver assistant systems like adaptive cruise control (ACC) or breaking assistants. In addition, legal entities like police or firefighters should be able to send alarm signals and instructions (e.g. To clear their way or stop other road users).

The rest of the paper is organized as follows. Section II presents a description about the related works. Section III involves the brief description about the system model and preliminaries. The next section tells about the proposed scheme. Section V and VI present the performance analysis and MAC layer analysis. The paper concludes in Section VII.

Related Works

Many related studies have been reported on security and privacy preservation in VANETs. To achieve both message authentication and anonymity, Raya *et al*. in [2] proposed that each vehicle should be pre-loaded with a large number of anonymous public and private key pairs and the corresponding public key certificates. There is a pseudo identity in each public key certificate. Traffic messages are signed with a public key based scheme, and each public and private key pair has a short lifetime to achieve privacy preserving. To avoid pre-loading a large number of anonymous key materials in each vehicle, Lin *et al*. in [13] introduced a group signature scheme to sign each message. In this scheme, each vehicle has only one public and private key pair. The public key is the same for all vehicles, and the private key of each vehicle is different. For message signature, a vehicle only knows the authenticity of the signature, and the vehicle has no information on the identity of the message sender. Lu *et al*. in [14] proposed a conditional privacy preservation scheme called ECPP, which divides privacy into three levels. In ECPP, RSUs are responsible for issuing temporary public key certificates to vehicles. Zhang *et al*. in [9] developed an identity-based batch verification scheme called IBV, which employs a tamperproof device to protect privacy. Freudiger *et al*. in [15] and Sampigethava et al. in [16] respectively proposed location persevering schemes. First of all, they have not addressed the stringent time requirement for a vehicle to verify all message signatures sent by its neighboring vehicles especially when the traffic density becomes larger. Moreover, the packet length is dramatically increased due to the signatures and public key certificates attached to each message. The cryptographic operations have incurred very high computation and communication overhead when securing VANETs, which could be intolerable and make these schemes unsuitable to meet the current standard specifications. This becomes a particularly serious problem when inter-vehicle communication (IVC) is performed in a metropolitan area with many vehicles in each other's communication range. Group Signature is proposed to generate signatures by issuing the secret key from the key distribution center. The Group Signature is verified as the public key of group, which is provided without the exposure of the ID

System Model and Preliminaries

A. System Model

Vehicular network can be deployed by network operators and service providers or through integration between operators, providers, and governmental authority. The main components of VANET are:

Trusted Authority (TA) is the chief level in the system and is trustable by all the network entities. The TA has sufficient physical security measures. All vehicles that take part in the network have to register with the trusted authority.

Certification Authorities (CAs) Each CA is responsible for generating initial certificates for the RSUs and OBUs in its domain. The CAs are connected directly to the TA. CA is physically secured and cannot be compromised.

RoadSide Units (RSUs) are the fixed units distributed in the network. Road side infrastructure consists of RSUs deployed at the road sides which are in charge of key management. Traffic lights or road signs can be used as RSUs after renovation. RSUs communicate with authorities through the wired network. RSUs are semi-trust with the medium security level.

On-Board Units (OBUs) can communicate either with other OBUs through Vehicle-to-Vehicle (V2V) communications or with the infrastructure RSUs through Vehicle-to-Infrastructure (V2I) communications. Each OBU is equipped with a Global Positioning Service (GPS) receiver which contains the geographical coordinates of the RSUs. It should be noted that a GPS receiver is necessary for the operation of an OBU in VANETs according to the WAVE standard.

Each vehicle is enabled with the on-board unit for vehicle to vehicle Communication and vehicle to infrastructure communication. Vehicles are initialized by creation and registration process. The vehicles are first created in the network and get registered with the Trusted Authority (TA) using Vehicle ID (Vid) and signature id (Sig id).

After registration, TA issues Public Key Infrastructure (PKI) to each vehicle. The Public Key Infrastructure is based on the concept of asymmetric key cryptography. The PKI has different types of keys. Each of the communicating users has the keys. The message can be encoded using any of the keys.

Public Key ($PK_{U)}$ is used for both encryption and decryption purposes. Encryption is done using the algorithm password based encryption. The Public key is shared with all the vehicles in the system.

Secret Key (Kg) is used for generating MAC code to ensure message integrity and authentication. The private key is confined only to the user himself.

Shared Key is used for secure communication between vehicles.

Time Stamp denotes the time when the vehicles are registered to the network.

Certificate owned for each vehicle that binds the public key.

Finally, TA stores the information such as Vehicle ID, signature id and Time stamp for each vehicle. A VANET is hierarchically composed of two layers. The upper layer is composed of application servers (ASs) and road side units (RSUs. The ASs can connect with RSUs through secure channels, such as a transport layer security (TLS) protocol with either wired or wireless connections. The ASs provides

application data for RSUs, and RSUs work as gateways to deliver data to the lower layer. The lower layer is composed of RSUs and vehicles. The communication range of an RSU can be larger than that of the vehicles, so that some vehicles can listen to the nearby RSU while the RSU cannot hear from the vehicles.

B. Problem Statement

The current IEEE standard for VANETs security provides us a detailed documentation, including the choice of cryptosystems. OBUs and RSUs should sign the messages with their private keys before the messages are sent in order to authenticate a message sender and guarantee the message integrity. Figure 2 shows the format of a signed message according to [11]. In that a 125-byte certificate and a 56-byte ECDSA signature has to be attached for each 69-byte IVC message. Obviously, the cryptographic overhead holds up a significant portion of the total packet size.

Cryptographic operations also lead to the high computation burden for receivers to verify the messages. According to DSRC ,a vehicle sends a message within the time interval of 100-300 ms. Pubic key based signature schemes can generate a signature every 100 ms without any problem. However, in the case that 50-200 vehicles are within the communication range, the receiver needs to verify around 200-2000 messages per second. Signing and verifying each message are certainly able to achieve secure communication; however, these cryptographic operations make the security protocol not scalable to the traffic density. Therefore, the verification algorithms are required to be very fast such that the incoming messages can be processed. Unfortunately, all currently available signature schemes for VANETs based on public key infrastructure or group signature schemes are far from satisfactory to this inflexible time requirement.

C. The Key Management in VANET

When a cryptographic operation is performed in Vehicular Communication, it needs the key which is OBU installed in vehicles. In addition, vehicles should be able to get the keys safely for secure communication each other [1]. The system should provide services for key update and key revocation if malicious vehicles are detected. In all these processes, the key management is required. The key management is accomplished through the key establishment, key distribution, key usage, and key revocation phase.

1) Key establishment

The Key establishment is a process to generate a public key and private key by using cryptographic operation for secure communication. There are two ways of generating keys in VANET. In general, there is the method by Road Side Unit (RSU) and by On-Board Unit (OBU). The method generated by RSU should provide sufficient RSUs. The other uses OBU, master key of an identity-based Public Key Generator (PKG) is stored in TPD and each vehicle generates anonymous public key pairs using the master key. The above method has a problem that it does not provide a revocation mechanism required in VANET.

Table 1: Security Requirements for VANET

Security Requirements	Definition
Identification & Authentication	Identification: process of identifying the valid user Authentication: The process of verifying a user's identity
Integrity	It gives assurance that the content of the data was not modified while in transit. It differs from confidentiality in the sense that it allows for detection of data modifications
Confidentiality	It is the assurance that the data could not have been accessed by any other user than the designated recipient. Confidentiality is generally achieved by cryptography techniques
Non-repudiation	Non-repudiation is the verification that the data was sent with a user's identification so that without denial or repute the data can be associated to the sender.
Privacy	Prevents an unauthorized person from identifying the information about users and user's ID
Availability	Proportion of time that a system is in a functioning state. Each of these attributes brings its network requirements whose balance and compromises make network security challenging

2) Key distribution

Distributing the keys to secure data transmission is the responsible for the Key Distribution Phase. In IEEE 1609.2 Standard, Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol is specified [7].The ID of the user would be exposed when the user signs to key exchange in VANET. Therefore, VANET is considered as privacy threats by threats of tracking.

3) Key Usage

The key usage means using the key to provide message generation, distribution, verification, and revocation securely. The security requirements are satisfied by using the key in signature techniques, encryption mechanisms, and hash function.

4) Key Revocation

The key revocation means that it revokes the key and the certificate when a malicious node or the device malfunction is detected. The ID of the vehicle should be periodically changed for privacy protection. Therefore, the certificate also periodically should be issued. An expired certificate should be updated and a detected attack is revoked by the public key. In addition, the information is known to all vehicles. Therefore, the CRL is distributed and the size of the canceled public key list becomes very large because the ID should be frequently changed. When driving, the time in which CRL can be distributed through the RSU is very short. The problem of large CRL size is overcome by Delta CRL, Partitioned CRL, and Compressed CRL

[2]. Firstly, the Delta CRL only lists those certificates that are added from the last update to reduce the sending cost of Base CRL that is distributed to the whole lists of CRL. The Partitioned CRL is hierarchically divided into groups for rapid search and distribution of CRL. The Compressed CRL compresses the CRL through the Bloom filter. It checks the result value of certificates through the Bloom filter.

Proposed Scheme

The proposed scheme tells about the Message verification system in Vehicular networks. The reliable operation of Vehicular system is done by increasing the amount of authentic information obtained from the received message and its revocation status is checked by the OnBoard Units in a timely manner.

A. On Board Unit Verification Process

Each OBU is ready with a Hardware Security Module (HSM), which a tamper-resistant module is used to store the security materials, e.g., secret keys, certificates, etc., of the OBU. All the cryptographic operations such as signing messages, verifying certificates, keys updating, etc. are through the HSM in each OBU. The valid OBUs is considered not being collude with the revoked OBUs.

The Trusted Authority initializes the system by public key for each OBU and corresponding secret key, pseudo identity for that OBU. The TA is the one which can relate pseudo identity to the real identity of respective OBU. A set of hash chain values to accommodate with the number of revocation processes occur during the lifetime of the network. The system model under consideration is mainly a PKI system, where each OBU has a set of anonymous certificates used to secure its communications with other entities in the network. The public key included in the certificate and the secret key are used for verifying and signing messages, respectively. Each OBU in the network is pre-loaded with a set of asymmetric keys and the corresponding public keys. Those keys are necessary for generating and maintaining a shared secret key between unrevoked OBUs.

In a generic PKI system, the details of the TA signature on a certificate and an OBU signature on a message are not discussed The only focus is on how to accelerate the revocation checking process, which is conventionally performed by checking the CRL for every received certificate. Before any OBU broadcasts a message, it calculates its revocation check REV check by the enhanced message authentication code and in verification process the calculated authentication code is compared received REV check i.e. calculated by public key. The Enhanced Message Authentication Code uses keyed hash authentication. The revocation process is starts with that the TA searches its database to determine the identity of the non-compromised secret key is shared by the majority of the non-revoked OBUs, and finds the corresponding public key and calculates the intermediate key, new secret key. The hash chain value is used by all the OBUs to update their compromised secret keys and the corresponding public keys. After that, the TA prepares a key update message, finally TA broadcasts the list of the certificates of the revoked OBU i.e.

Certificate Revocation List (CRL). Accordingly, the OBUs must use the CRL to check that the certificates of the communicating parties are not previously revoked.

B. Road Side Unit Verification Process

If the traffic density becomes larger, each vehicle cannot verify all signatures of the messages sent by its neighbors in a timely manner, which results in message loss. To overcome this RoadSide unit (RSUs) are made in charge of verifying the authenticity of the messages sent from vehicles and for informing the outcome back to the vehicles. The process starts with detecting RSU nearby after that vehicles start to associate with the RSU. Then, the unique shared symmetric secret key and a pseudo ID are assigned to RSU that is shared with other vehicles. Each vehicle generates a symmetric enhanced message authentication (EMAC) code with the symmetric key and then broadcasts a message by signing the message with that code instead of a PKI-based message signature. The messages signed with the EMAC received by other vehicles are able to verify the message by using the authenticity of the message. The authentication, encryption keys shared with vehicles are recognized by RSU therefore RSU knows the authenticity of the messages.

The process starts with a vehicle detects an RSU nearby and begins a mutual authentication process and establishes a shared secret key. This process can be achieved by adopting the public key based signature scheme. Vehicles revise their anonymous certificates once they get out of the communication range of an RSU. The vehicle obtains the symmetric key from the RSU and uses the key to compute the message authentication code. In this the RSU is responsible to aggregate multiple authenticated messages in a single packet and also the RSU can distinguish the unique sender of a message. Thus, in case that a malicious vehicle sends a fake message, the RSU can trace back to the message sender by finding out its certificate. The certificate to a trusted authority is report by RSU for further analysis.

When a vehicle receives messages sent by the other vehicles, it only buffers the received messages in its local database without verifying them immediately. Vehicles are able to verify the buffered messages one by one obtain the signed packet from the RSU. If it is valid, vehicles will check the validity of the previously received messages buffered in the record in the local database. This process is undergone by comparing whether there is a match between the buffered record with the de-aggregate message. In this a vehicle can verify all incoming messages sent by neighboring vehicles, which means all messages received by the vehicle can be received by its corresponding RSU as well.

Performance Evaluation

The performance of the proposed scheme for On Board Unit verification and RoadSide Unit verification is evaluated using Network Simulator-2 in terms of the packet delivery ratio, the message delay, and the message loss ratio. RSUs are located at an intersection. The distance limit for Inter Vehicle Communication and Road Vehicle Communication is 300m and 600 m, respectively. Messages are sent every

300 ms at each vehicle. IEEE 802.11a is used to simulate the medium access control layer transmission protocol.

Packet Delivery Ratio (PDR):
It is the fraction of generated packets by received packets. That is, the ratios of packets received at the destination for those of the packets generated by the source. As of relative amount, the usual calculation of this system of measurement is in percentage (%) form. The higher the percentage, the more privileged is the routing protocol. Packet delivery ratio is a very important factor to measure the performance of routing protocol in any network. The performance of the protocol depends on various parameters chosen for the simulation. The major parameters are packet size, no of nodes, transmission range and the structure of the network.

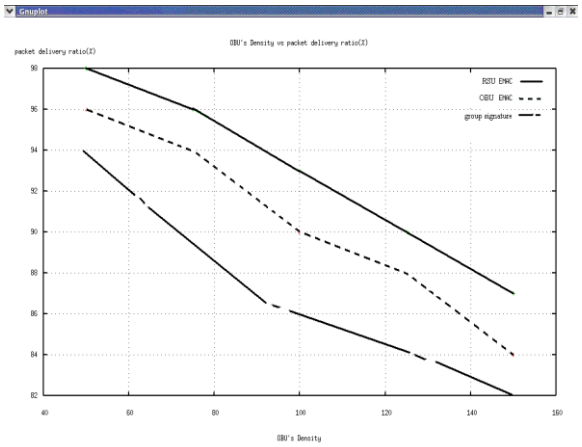

Figure 2: OBU Density Versus Packet Delivery Ratio (%)

Figure 2 shows the comparison of Packet Delivery Ratio with OBU Verification Process and RSU Verification Process to the existing Group Signature Method. In that the PDR of RoadSide Unit Verification is higher than the other. The better network utilization and security performance are obtained by the higher PDR.

Message End-to-End Delay (E2E Delay):
It is the calculation of typical time taken by the packet (in average packets) to cover its journey from the source end to the destination end. In other words, it covers all of the potential delays such as route discovery, buffering processes, various in-between queuing stays, etc., during the entire trip of transmission of the packet. The classical unit of this metric is millisecond (ms).

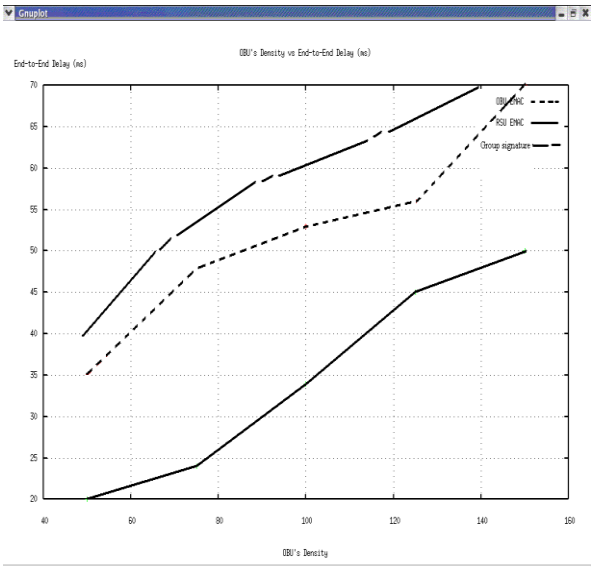

Figure 3: OBU Density versus Message End to End Delay (ms)

Figure 3 shows the connection between the proposed two schemes and existing Group signature method. Message Delay depends on the number of vehicles taken part in the simulation, Number of messages sent and also the number of adjacent vehicles. The graph shows the relation between the message delay and traffic density. In this group signature scheme has the highest message delay. The highest delay is due to the verification of a message signature. The OBU and RSU Verification yields lowest message delay compared with the existing. The Message delay is reduced further by decrease the time interval of message arrival.

Message Loss Ratio:

The average message loss ratio is termed as the average ratio between the number of messages dropped every 300 msec, due to the message authentication delay, and the total number of messages received every 300 msec by an OBU.

According to DSRC, each OBU has to disseminate a Message containing information about the road condition every 300 msec. Message Loss Ratio depends on the total number of vehicles in the simulation, number of messages received by the vehicle and the number of messages consumed by the vehicle.

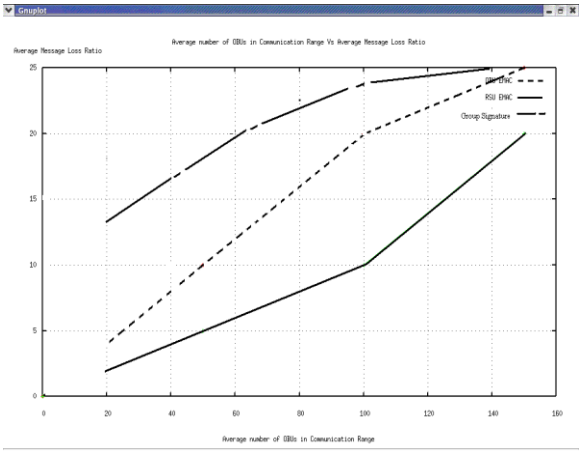

Figure 4: OBU Density versus Message Loss Ratio (%)

Figure 4 shows the relationship between the message loss ratio and the traffic load. Traffic load is represented by the number of vehicles associated with the RSU. The message loss ratio can be observed in the three schemes increases as the traffic load increases. The group signature scheme has the highest loss ratio. Group Signature Method considers the message loss incurred by delays due to the security protocol rather than the wireless transmission channel. The RSU Verification Scheme provides a lowest message ratio. From this the observation is that most of the message losses come from the two-hop wireless transmission.

Mac-Layer Performance Analysis

This section develops an analytical model for MAC layer performance analysis. Consider 802.11 based VANETs, where the broadcast from each vehicle is controlled with a distributed coordination function (DCF). The assumption is that the vehicles are uniformly distributed along the road, and thus the number of vehicles in an area has a Poisson distribution. Given the fixed road width, the density of vehicles along the road, denoted as β, is represented as "vehicles per kilometer". All vehicles have the same communication range R, and the carrier sensing range equals the communication range. For mathematical traceability, the hidden-terminal effect is ignored. The hidden terminal effect is small, because the authentication scheme can effectively reduce the traffic load generated by each vehicle.

A. MAC-layer Channel Behavior

The MAC-layer channel behavior observed by a tagged vehicle. Each vehicle can be modeled as a *G/G/*1 queue. Let p_0 denote the probability that the queue is empty; the probability that a vehicle access channel in an idle slot can be expressed as $(1 - p0)\tau$.

Let n (= $2\beta R$) denote the average number of vehicles within the transmission range of the tagged vehicle. The tagged vehicle has a packet to send in an idle slot, it is simple to see that the packet delivery ratio (PDR) equals the value *pi*,

$$PDR = \frac{e^{-n(1-p_0)\tau} - e^{-n}}{[1-(1-p_0)\tau](1-p_0)}$$

In the above equation, τ denotes the probability of a vehicle transmitting in a randomly chosen slot within the contention window CW with no exponential back off.

$$\tau = \frac{2}{CW+1}$$

The Contention Window value which gives better performance out of other is chosen as 16. From this τ value is calculated. Let n be the number of vehicles in the transmission range, it can be different values. Generally probability values are ranged between 0 and 1.The respective values are substituted for different traffic densities. Graphical representation for lower and higher vehicular densities are as follows.

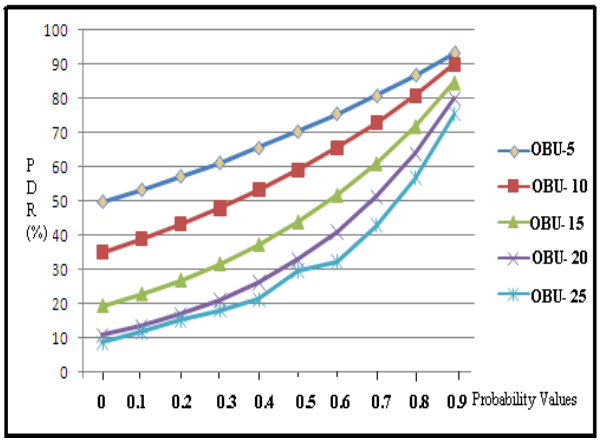

Figure 5: Packet Delivery Ratio Versus Probability Values For Lower Vehicle Densities (5-25)

The graph explains that the PDR for lower vehicle density is larger. As the number of vehicles increases the Packet delivery gets lower. In the case of probability of a particular vehicle, the delivery ratio goes better. The lowest number of vehicle yields highest packet delivery up to 93.19%. The packet delivery ratio is about 51.11% can be obtained for large vehicle density. The highest packet delivery value is obtained only when there is a chance of maximum probability value.

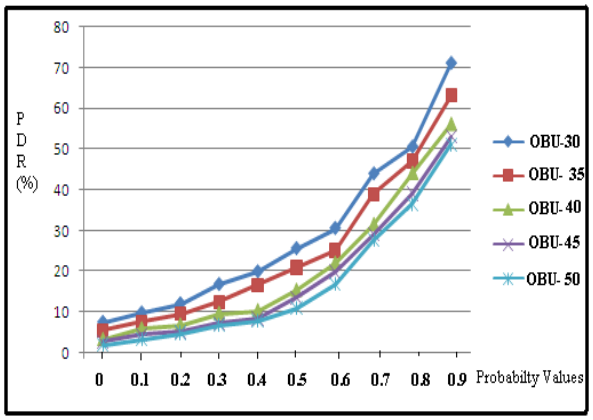

Figure 6: Packet Delivery Ratio Versus Probability Values For Lower Vehicle Densities (30-50)

Figure 5 and 6 shows the packet delivery ratio for different vehicle densities. First the graph is plotted for lower vehicle density value and then for highest. Consider a particular vehicle for that packet delivery ratio increases as the probability value rises the reason is that there is a greater chance for the queue to be empty and a vehicle can access the channel to transmit data. Therefore PDR gets increased in the above condition. The other scenario is the large number of vehicles taking part in the network makes the packet delivery lower because the communication between the vehicle is affected as their number goes larger.

B. Average Packet Service Time

The average packet service time is defined as the average time period from the instant that a packet becomes the head of the queue and starts to contend for transmission to the instant when that the packet is transmitted. Let λ denote the average rate of generating messages in a vehicle. μ denote the average service rate in terms of "packets per slot".

The average service time can be computed as

$$\mu = \frac{\lambda}{1 - p_0}$$

Let p_0 be the probability that the queue is empty, it ranges from 0 to 1.The average packet service time is calculated for different probabilities and tabulated the highest probability values as follows

Table 2: Average Packet Service Time

(ms)	Probability Values	Average Packet Service Time(ms)
8	0.9	7.854
16	0.9	14.354
24	0.9	21.058
32	0.9	29.754
40	0.9	38.576
48	0.9	45.373
64	0.9	63.900

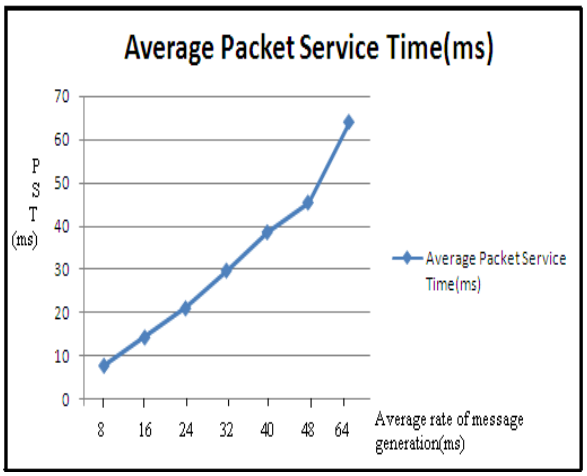

Figure 7: Packet Service Time (PST) Versus Message Generation Rate For Probability Value (0.9)

Figure 7 shows the average packet service time for different message generation rate. The graph is plotted for the highest probability value, the message generation rate is taken as the multiple of 8.

The packet service time gets increased as the message generation rate rises. The higher packet service time makes the packet to move in front of the queue and boost up the packet transmission.

Conclusion

In this paper, the message authentication uses a newer verification process done on vehicles and infrastructure. The authenticity of the messages sent by vehicles are verified at On Board Units and Road Side Units. The CRL Verification done by Road Side Unit reduces the delay occurred during traffic load increases in On Board Unit verification Scheme. Extensive Performance Evaluation compared the verification process done at OBU and RSU. Verification Process is done at RSU had the lowest message loss ratio and delay than the OBU based scheme without losing the desired

security and privacy requirements. It is clear that the proposed work contributes to an effective and efficient security along with reduction in delay of authenticated messages.

References

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

[2] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68,2007.

[3] 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 Vehicular Inter NET working, pp. 89-98,2009.

[4] Wasef and X. Shen, "MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks," Proc. IEEE Globe Com, 2009.

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

[6] Studer, E. Shi, F. Bai, and A. Perrig, "TAC King 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.

[7] 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.

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

[9] C. Zhang, X. Lin, R. Lu, P.-H. Ho and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Trans. Veh. Technology.*, vol. 57, no. 6, pp. 3357-3368, 2008.

[10] K. P. Laberteaux, J. J. Haas, and Y. Hu, "Security certificate revocation list distribution for VANET," *Proc. 5th ACM international workshop on Vehicular Inter-NETworking*, pp. 88–89, 2008.

[11] H. Chan, A. Perrig, and D. Song, "Random key pre distribution schemes for sensor networks," *Proc. 2003 IEEE Symposium on Security and Privacy*, pp. 197–213, 2003.

[12] L. Eschenauer and V. D. Gligor, "A key-arrangement scheme for distributed sensor networks," *Proc. ACM conference on Computer* and communications security, pp. 41–47, 2002.

[13] X. Lin, X. Sun, P.-H. Ho, and X. Shen, " GSIS: a secure and privacy preserving protocol for vehicular communications" IEEE Transaction on Vehicular Technology, Vol. 56, No. 6, pp. 3442-3456, 2007.

[14] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," in *Processings of the IEEE International Conference on Computer Communications (INFOCOM'08)*, Phoenix, Arizona, 2008.

[15] J. Freudiger, M. Raya, and M. Feleghhazi, "Mix zones for location privacy in vehicular networks," in Proncessings of the First International Workshop on Wireless Networking for Intelligent Transportation Systems(WiN-ITS '07), Vancouver, Canada, Aug. 2007.

[16] K. Sampigethaya, Mi. Li, L. Huang, and R. Poovendran, "AMOEBA: robust location privacy scheme for VANET," IEEE Journal on Selected Areas in Communications (JSAC), Special issue on Vehicular Networks, Vol. 25, No. 8, pp. 1569-1589, Oct. 2007.