An Efficient Hybrid Message Authentication Scheme in Vehicular Ad Hoc Networks

H.Karthikeyan, Dr.G.Usha

Abstract*: Vehicular ad hoc networks (VANETs) are under active development phase, especially due to the latest and foremost wireless communication and networking technologies. Basically VANETs consist of some parts which play the major role to enable message authentication between vehicles which are on-board units as well as roadside units. To reduce the load on trusted authorities several roadside units are set up and message authentication using proxy vehicles has been proposed. This used to minimize the computational overhead of roadside units significantly. Due to this message authentication scheme the efficiency of roadside unit improves. In this paper we propose an Efficient Hybrid Message Authentication Scheme (EHMAS) that deals with the technique where it not only guarantees message authenticity, but it is also resistant against impersonation and modification attacks. First we explain the properties of the attacks in security model. Second we provide an EHMAS scheme where a novel authentication technique is proposed for registration and verification of users using elliptic crypto system. Finally the paper concluded with the scope of the proposed work and provides future enhancement using machine learning techniques.

***Index Terms*: Authentication, Encryption, On board Unit, Road Side Unit, and Vehicular ad-hoc network.**

I. INTRODUCTION

In the last few years, VANETs have been the most interesting and emerging topic among the researchers as well as in the academics. VANETs consists of mainly two parts for communication: - First part is on board unit (OBU) which is installed in vehicles and a wireless communication protocol named as dedicated short range communication (DSRC) is used for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Second is Road side unit (RSU) which is installed in sides of the road to serve as bridge between vehicles to infrastructure.

Due to the wireless communication mode, it is easy for an adversary to take control of communication links and can change, delete and replay messages. Hence, the impersonation, modification and man in the middle attacks are serious threats for VANETs [1]. These threats may lead to chaos in the traffic where an attacker can hack the database if it is directly connected. Hence its leads to be increase in the number of accidents in that particular area. Therefore, secure message transmission is the important requirements in VANETs. In addition, the privacy of the vehicle’s identity must be achieved because leakage of their vehicle’s identity lead to the malfunctioning and accidents which is not the policy of VANETs [1]. Therefore, the malicious vehicles must be caught and punished if found such in the database of the VANETs. Various types of secure authentication schemes has been proposed against malicious attacks.

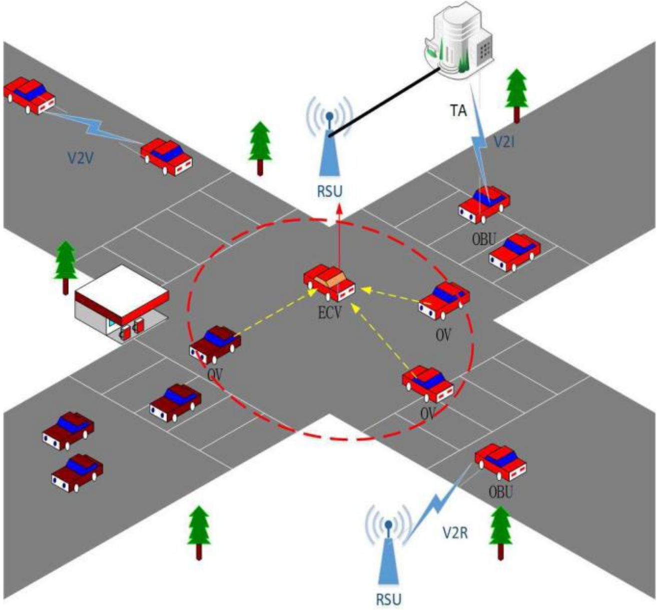

Fig 1: Model of VANET

Public Key Infrastructure-based (PKI-based) authentication schemes is proposed to ensure the safety, security and privacy in VANETs. Under these schemes, the vehicle must carry or store a large number of key pairs and their corresponding certificates, and these certificates are required to be transmitted with messages making these schemes not efficient. To get rid of such large numbers, various privacy preserving identity-based authentication schemes have been proposed. These are proposed based on bilinear pairings and due to their heavy computational cost, recently two efficient authentication schemes have been proposed. However, these schemes are not efficient when there are large number of vehicles in the coverage area of the roadside units (RSU). For example, there are 500 vehicles in an area and each vehicle sends its traffic safety message every 100-300 milliseconds according to the specification of DSRC protocol, the RSU has to verify around 1650-5000 signatures in a second. This is a big challenge for the current authentication schemes as stated by Liu et al in 2015. To tackle this problem Liu proposed another authentication protocol using proxy vehicles for vehicular networks, and called it as PBAS. In PBAS, proxy vehicles help RSUs to verify large number of signature sets simultaneously using distributed verification. In fact, using this scheme the time required to verify 3000 signatures is decreased by 88% compared to previous authentication schemes.

Revised Manuscript Received on July 05, 2019.

H.Karthikeyan, Assistant Professor, Department of Software Engineering, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamilnadu, India. 603203.

Dr.G.Usha, Associate Professor, Department of Software Engineering, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamilnadu, India. 603203.

II. RELATED WORKS

In 2007, Ozan *et al.* reported the first complete version of a multi-hop broadcast protocol for vehicular ad hoc networks (VANET). The results clearly showing that broadcasting in VANET was very different from routing in mobile ad hoc networks (MANET) due to several reasons such as network topology, mobility patterns. The difference indicate that conventional ad hoc routing protocols such as DSR and AODV will not be appropriate in vehicular ad hoc networks for most vehicular broadcast applications. They tried to identify three very different regions (regimes) that a vehicular broadcast protocol needs to work in: a) dense traffic regime; b) sparse traffic regime; and c) regular traffic regime. They built upon their previously proposed routing solutions for each regime and they showed that the broadcast message can be disseminate efficiently. The proposed design of the distributed vehicular broadcast (DV-CAST) protocol integrates the use of various routing solutions.

In 2007, Marco Fiore *et al.* eyed at extending data networks and connectivity to environments where wired solutions are impracticable, so making it more practicable so to make use of wireless communications. Among these, vehicular traffic is attracting a growing and fast attention from both academia and industry, due to the amount and importance of the related applications, ranging from road safety to traffic control, up to mobile entertainment. VANETs are well self-organized networks built up from moving vehicles and in motion vehicles, and are part of the broader class of mobile ad-hoc networks or (MANETs). Because of their peculiar and not suitable characteristics, vehicular ad hoc networks or VANETs require the definition of specific networking and communication techniques, whose feasibility and performance are usually tested by means of simulation for the operation. One of the main challenges or tasks posed by vehicular ad hoc networks or VANETs simulations is the faithful or the trustable characterization of vehicular mobility at both macroscopic and microscopic levels, leading to some realistic and non-uniform distributions of cars and velocity and acceleration, and unique connectivity dynamics of the vehicles. In this paper, first present and describe VanetMobiSim, a freely available generator of realistic vehicular movement traces for networks simulators. Then, the task was to VanetMobiSim is validated by illustrating how the interaction between featured macro-mobility and micro-mobility is able to reproduce typical phenomena of vehicular traffic and security.

In 2009, Ahren Studer *et al.* coined the term public key infrastructure (PKI). A public key infrastructure (PKI) is the one which can provide the functionality using fixed public keys and certification. However, these fixed keys allow an eavesdropper to associate a key with a vehicle maybe as a dummy variable and a location, violating drivers' privacy. In this work they proposed a vehicular ad hoc network (VANETs) key management scheme based on temporary anonymous certified keys (TACKs). Their technique or scheme efficiently prevents attackers from linking a vehicle's different keys and provides timely revocation of misbehaving participants or malicious vehicles while maintaining the same or less overhead for vehicle-to-vehicle communication as the current standard for VANET security.

In 2011, Rui *et al.* aimed to clarify the validity of channel models for vehicular networks typically disregard the effect of vehicles as physical obstructions for the wireless signal by quantifying the very serious impact of obstructions through a series of wireless communication experiments. Using two cars equipped with Dedicated Short Range Communications also known as DSRC hardware designed for vehicular use, they performed experimental measurements in order to collect received signal power and packet delivery ratio information in a multitude of relevant and most suitable scenarios or viewpoints: parking lot, highway, suburban and urban canyon. Upon separating the data into line of sight (LOS) and non-line of sight (NLOS) categories, their results showed that obstructing vehicles cause significant impact on the channel and communication quality and even the operation delays. A single obstacle or obstructer can cause a drop of over 20 dB in received signal strength when two cars try to communicate at a distance of 10 m or above. At longer or far than the required distances, NLOS conditions affect the usable communication range, effectively making almost halving the distance at which communication can be achieved with 90% rate or chance of success. They presented results motivated the inclusion of vehicles in the radio propagation models used for vehicular ad hoc networks (VANET) simulation in order to increase the level of realism and effectiveness of the system.

In 2014, Ian *et al.* took the concept of Software-Defined Networking (SDN), which had mainly been designed for wired infrastructures, especially in the data centre space, and proposed Software-Designed Networking also known as SDN-based vehicular ad hoc networks or VANET architecture and its operational mode to adapt SDN to VANET environments. They also mentioned or discussed the benefits of a Software-Defined (SDN) VANET and the services that can be provided. They demonstrated or showed in simulation the feasibility of a Software-Defined (SDN) VANET by comparing SDN-based routing with traditional MANET/VANET routing protocols. They also showed in simulation fall-back mechanisms that must be provided to apply the SDN concept into mobile wireless communication scenarios, and demonstrate one of the possible services that can be provided by a Software-Defined Networks or SDNVANET. They also stated that this enabling technologies can provide a wide variety of services, such as vehicle road safety, vehicle security and even privacy enhanced traffic and travel efficiency, and convenience and comfort for passengers and drivers. However, current vehicular ad hoc network (VANET) architectures lack in flexibility and make the deployment of services/protocols in large-scale or medium-scale even a harder task. Therefore, they have demonstrated the use of Software-Defined Networks or SDN.

III. OUR CONTRIBUTIONS

Contributions of this paper are as follows: -

- First, we discuss the methods or schemes which were used earlier like PBAS which is proxy-based authentication scheme. Due to its false acceptance of batched invalid signature sent by vehicles, and also it does not have message authentication which is the main requirement of VANETs.
- Second, we'll show how to tackle the above problem of impersonation and modification attacks by using a new identity-based authentication scheme using proxy

vehicles, EHMAS, without bilinear pairings is proposed.

- Third, the most important analysis which differs it from other authentication schemes, we'll present security analysis of EHMAS to satisfy security, safety and privacy requirements of VANETs. In this direction, unforgebility of the underlying signature scheme against adaptively chosen-message and identity attack is proved under ECDLP in the random oracle model to guarantee resistance against modification and impersonation attacks.

IV.Security Model

The EHMAS fulfill the following security and privacy requirements

Message authentication: Authenticity, integrity and validity of received messages are need to check by the vehicles and RSU.

Identity privacy preserving: Real identity of the vehicle from the received messages should not be extract by any nodes except TA.

Traceability: Real identity of the vehicle extract by TA from messages sent by vehicle in case of any misbehavior.

Unlinkability: Same vehicle sent two messages the communication link should not be able to find by Vehicles and RSU.

Resistance to attacks: Common attacks in VANETs such as the impersonation attack, modification attack, the replay attack and man-in-the-middle attack and also attacks done by malicious proxy vehicles which are described below should be prevented

1) Impersonation attack: Successfully guesses the real identity of one user in VANET by this attack

2) Modification attack: Alter or modify the broadcasted messages are tried by the attacker in VANET by this attack.

3) Replay attack: In this attack, an attacker keeps a message that was sent earlier and tries to use the same message later by rebroadcasting it.

4) Man-in-the-middle attack: Attacker finds possible to alter the communication between vehicle and RSU without knowing them. The node thinks that they are directly communicating with each other.

5) Attacks done by malicious proxy vehicles: A malicious proxy vehicle may fool RSUs in a way that the batch result is valid, but it claims that it is invalid, or the batch result is invalid, but it says that it is valid.

V. EHMAS SCHEME

EHMAS Authentication Scheme is the most secured version till now which does not allows the interrupt to affect the database or does not lead to the malfunctioning of the system.

It consists of mainly two layers from which the whole system works i.e., Registration Layer and Trusted Authentication and Security Layer. The first layer works parallel with the database and with the proxy vehicles. Every vehicle is assigned the Dummy ID (DID) which is stored in the database along with their original ID in the encrypted form. This DID is available to the driver too and the message authentication can be sent to the RSU with the help of this DID. Initially the vehicle with their DID send their details to the Data Collection Layer, which sends this collected data to the Registration Layer in Generate Authentication Details part for the verification of the vehicle from the database and if it is success it proceeds with the generation of index details from the database for the generation of verification certificate.

The generated index details of a particular DID is sent to the Trusted Authentication and Security Layer for further verification. The RSU collects the data and sends to this layer through 1 or 2 layers so that it remains secured and as we use DID instead of the original ID its gets impossible for the hackers to attack the system and database through debugging or backtracking. Trusted Authentication and Security Layer generates Trusted Authentication Security Layer Information (TASLI) which is in encrypted form through processes, this same TASLI is collected back from the vehicle when they try to connect with RSUs which in further is decrypted by Trusted Authentication and Security Layer and is sent for the certificate verification in the database. If the match is found in the database and if there is no error report in the past of that DID then it generates the Certificate which is sent to the vehicle. But if some wrong is found in the past history of that DID then it gets blocked and is taken under consideration.

This system can change the idea of country's traffic if it gets used efficiently in the particular area. Due to the several layers involved in the system, it gets impossible for the attackers, hackers and interpreters to malfunction the system or hack the system. They can never reach to the original ID of the proxy vehicles. And most importantly due to this layers sever gets less load all the time it gets executed. Here the server is acted by TA- Trusted Authority which manages and holds all the functioning of the system. The RSUs acts as a transceiver which collects and sends the data to the proxy vehicles using their DID, which is stored in the database of the system.

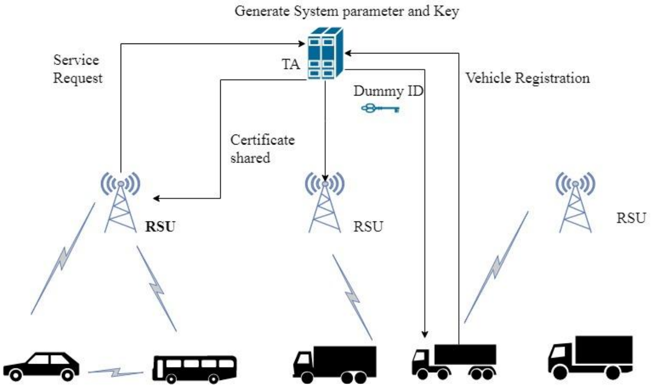

FIG2: EHMAS SCHEME

A) Security Objectives

A well-designed message authentication scheme should achieve the following security objectives:

1) Message Authentication and integrity: After receiving a message, the recipient of the message must determine the legitimacy of the message owner, and whether the message itself is tampered with or whether it is forged.
2) Identity Privacy Preserving: The real identity of the vehicle should remain anonymous, which means that the vehicle should use the pseudo identity when sending traffic-related information. No third party except for TA can extract the real identity of the vehicle based on multiple messages sent from the same vehicle.
3) Traceability: TA can trace the real identity of the vehicle by analysing its pseudo identity

extracted from its message.

4) Replay Attack: A malicious vehicle cannot collect and store a signed message and attempt to deliver it later when the original message expired.

B) Elliptic Curve Cryptosystem

In 1984, Miller applied the elliptic curve to cryptography for the first time. After Kobilitz built the elliptic curve cryptography (ECC) with elliptic curve discrete logarithm problem (ECDLP), ECC began to be widely applied to encryption, protocol and other safety-related areas. Let F_p be a finite field, which is determined by a prime number p. Let a set of elliptic curve point E over be defined by the equation: $y^2 = x^3 + ax + b \bmod p$, where $a, b \in F_p$. Let the point at infinity be O, then O and other points on E make up an additive elliptic curve group G with the order q and other generator P. The elliptic curve group G has the three following properties.

- Additive: Let P and Q be two points of group G. If P is not equal to Q, then we can get $R = P + Q$ where R is the intersection of E and the straight line connecting P and Q. If $P = Q$, then $R = P + Q$. If $P = -Q$, then $P + Q = O$.
- Scalar point multiplication: Let $P \in G_p$ and $m \in Z_q{}^*$, the scalar multiplication of E is defined as $m \cdot P = P + P + \cdot\cdot\cdot + P$.
- Elliptic curve discrete logarithm problem (ECDLP): Given two randomly generated points, it is difficult to calculate x in the case of known P and Q.

C) System Initialization Phase

At this phase, the TA generates the necessary system parameters and then the TA preloads these system parameters into all vehicles' TPD and all RSUs' memory. Because the RSU connect with the TA via secure wired network, the para-meter transmission can be processed anytime. And the vehicle can get the parameters in some special situation like ETC gate or vehicle inspection under pre-store strategy [3]. Specific steps in system initialization phase are as follows:

1) TA randomly selects two large prime p,q, and a non-singular elliptic curve E where is defined as $y^2 = x^3 + ax + bmodq$, and the generator element P is randomly selected in the group.
2) TA randomly selects $s \in Z_q{}^*$ as the system private key, and calculates the system public key $P_{pub} = s\,P$.
3) TA randomly selects $x \in Z_q{}^*$ as the private key of RSU, and calculates the RSU's public key $PK_R = x\,P$.
4) TA chooses the secure hash function h: $\{0, 1\}^* \rightarrow Z_q$.
5) TA assigns the real identity RID and password PWD to each vehicle, and preloads {R $I\,D$, $P\,W\,D$, s} to the TPD of the vehicle.
6) TA sends the private key x to the RSU.
7) TA publishes system public parameters $\{p, q, a, b, P, P_{pub}, P\,K_R, h\}$ to the RSU and all vehicles.

D) The Generation Phase of Vehicles' Pseudo Identity and Signature

Before sending a message, the vehicle must provide a signature of the message in order to ensure the authenticity. The following work is completed by the TPD, used to generate the vehicle's pseudo identity, public key and signature.

1) The vehicle sends its own real identity $R\ I\ D$ and pass-word $P\ W\ D$ to the TPD for identity check. If the two values are equal to the pre-stored values in the TPD, the vehicle passes the authentication and proceeds to the following steps. Otherwise, the authentication fails and the service is rejected.
2) TPD randomly selects a number $r_i \in Z_q{}^*$
3) The vehicle gets message signature by combining message M and current timestamp T , and TPD inputs

Security Analysis In this section, we show that our proposed scheme satisfies several security requirements.

1) Message Authentication: In this scheme, the signature of the message guarantees the integrity of the message and the legitimacy of the message owner. Theorem 1 has proved that the signature used in our scheme cannot be forged under the random oracle model. Therefore, malicious attackers cannot forge valid signatures. In theorem 2, we show that ECV cannot cheat the RSU successfully.

Theorem 2: ECV cannot successfully fake valid message signature authentication results in order to cheat the RSU. *Proof:* Let $T\ ask\ Li\ st_{EC\ Vi}$ denote the message signature list which is verified by $E\ C\ V_i$, and let $I\ nv\ ali\ d\ Li\ st_{EC\ Vi}$ denote the invalid signature list which is the output of $E\ C\ V_i$.

The RSU get the valid signature list by executing Valid Listec=TasliVi-invalidTasli for all signatures in list *Valid* $List_{EC\ Vi}$, the RSU performs batch authentication as described in Equation (4). Obviously, if the batch authentication is passed, it would imply that the RSU is not deceived by ECV_i . For all signatures in *Valid* $List_{EC\ Vi}$, the RSU performs single authentication as described in Equation (5) one by one. If ECV_i had not deceived RSU, then none of these single authentication would pass, otherwise, at least one single authentication would get passed. Because the RSU checks the lists *Valid* $List_{EC\ Vi}$ and *Invalid* $List_{EC\ Vi}$ at the same time, ECV_i cannot deceive the RSU successfully.

VI. CONCLUSION

Being a broadcast based messaging system it need more efficient methods for broadcasting message. EHMAS provides the most promising authentication scheme for proxy vehicles than other existing schemes. Providing reliable broadcasts in a VANET environment is still an open issue of research. While routing the messages in a VANET the time plays an important factor because if the alert message reaches the receiver behind the scheduled time then there is no use of having such system. So the routing mechanisms are choosing in such a way to minimize the time delay in the message communication. Numerous researchers and industry players accept as true that the assistance of vehicular networks on traffic security and many commercial applications should be able to validate the cost. With such a vehicular network and communication, many data delivery applications and tasks can be supported without extra hardware cost. Though, existing protocols are not appropriate for supporting delay tolerate applications in sparingly connected vehicular networks. To handle this problem EHMAS is used. In VANETs, vehicles are mobile nodes which communicate with each other and also with the Road Side Unit (RSU). Provides many useful applications such as traffic optimization, payment services, location-based services, and infotainment. We have analysed the threat, general classification of attacks, posed on the vehicular networks. It provides most important ones in term of active safety. There are no standardized protocols, but lot of research is going on this area. Vehicular ad hoc networks or VANETs are likely to become the most important realization of mobile ad hoc networks.

REFERENCES

[1] S. Zeadally, R. Hun, Y.-S. Chen, A. Irwin, and A. Hassan, “Vehicular ad hoc networks (VANETs): Status, results, and challenges,” Telecommun. Syst., vol. 50, no. 4, pp. 217–241, 2012.
[2] M. Ghosh, A. Varghese, A. Gupta, A. A. Kherani, and S. N. Muthaiah, “Detecting misbehaviors in VANET with integrated root-cause analysis,” Ad Hoc Netw., vol. 8, no. 7, pp. 778–790, 2010.
[3] Y. Toor, P. Muhlethaler, and A. Laouiti, “Vehicle ad hoc networks: Applications and related technical issues,” IEEE Commun. Surveys Tuts., vol. 10, no. 3, pp. 74–88, Third Quarter 2008.
[4] D. He, S. Zeadally, B. Xu, and X. Huang, “An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.
[5] K.-A. Shim, “CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks,” IEEE Trans. Veh. Technol., vol. 61, no. 4, pp. 1874–1883, May 2012.
[5] J. Zhang, M. Xu, and L. Liu, “On the security of a secure batch verification with group testing for VANET,” Int. J. Netw. Security, vol. 16, no. 5, pp. 355–362, 2014.
[6] A. Miyaji, M. Nakabayashi, and S. Takano, “New explicit conditions of elliptic curve traces for FR-reduction,” IEICE Trans. Fundamentals, vol. E84-A, no. 5, pp. 1234–1243, 2001.
[7] Y. Liu, L. Wang, and H.-H. Chen, “Message authentication using proxy vehicles in vehicular ad hoc networks,” IEEE Trans. Veh. Technol., vol. 64, no. 8, pp. 3697–3710, Aug. 2015.
[8] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” in Proc. 21st Ann. Int. Crypto. Conf., Adv. Cryptol., Aug. 19–23, 2001, pp. 213–229.
[9] Y. Liu, Z. He, S. Zhao, and L. Wang, “An efficient anonymous authentication protocol using batch operations for VANETs,” Multimedia Tools Appl., vol. 75, no. 24, pp. 17 689–17 709, 2016.
[10] Y. Li, H. Duan, and H. Deng, “An efficient authentication scheme with privacy preserving for vehicular ad-hoc networks,” in Proc. 95th Annu. Conf. Transp. Res. Board, Jan. 14–16, 2016, pp. 1–14.
[11] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, “Informationoriented trustworthiness evaluation in vehicular ad-hoc networks,” in Proc. Int. Conf. Netw. Syst. Secur., 2013, pp. 94–108.
[12] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, “A social network approach to trust management in VANETs,” Peer Peer Netw. Appl., vol. 7, no. 3, pp. 229–242, 2014.
[13] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle, “Trust on the security of wireless vehicular ad-hoc networking,” Ad Hoc Sensor Wireless Netw., vol. 24, nos. 3–4, pp. 283–305, 2015.
[14] R. Hussain, W. Nawaz, J. Lee, J. Son, and J. T. Seo, “A hybrid trust management framework for vehicular social networks,” in Proc. Int. Conf. Comput. Social Netw., 2016, pp. 214–225.
[15] M. Monir, A. Abdel-Hamid, and M. A. El Aziz, “A categorized trustbased message reporting scheme for VANETs,” in Advances in Security of Information and Communication Networks. Berlin, Germany: Springer, 2013, pp. 65–83.
[16] W. Li and H. Song, “ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks,” IEEE Trans. Intell. Transp. Syst., vol. 17, no. 4, pp. 960–969, Apr. 2016.
[17] C. Sommer, R. German, and F. Dressler, “Bidirectionally coupled network and road traffic simulation for improved IVC analysis,” IEEE Trans. Mobile Comput., vol. 10, no. 1, pp. 3–15, Jan. 2010.
[18] L. Malina, J. Castellà-Roca, A. Vives-Guasch, and J. Hajny, “Shortterm linkable group signatures with categorized batch verification,” in Proc. Int. Symp. Found. Pract. Secur., 2012, pp. 244–260.
[19] S. K. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, “A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs,” Future Generat. Comput. Syst.,.
[20] T. Peng, Q. Liu, D. Meng, and G. Wang, “Collaborative trajectory privacy preserving scheme in location-based services,” Inf. Sci., vol. 387,pp. 165–179, May 2017.

AUTHORS PROFILE

H.Karthikeyan, Assistant Professor, Department of Software Engineering, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamilnadu, India. 603203.

Dr.G.Usha, Associate Professor, Department of Software Engineering, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamilnadu, India. 603203.