A Privacy Preserving Authentication Technique for Vehicular ad-hoc Network

M. Senapathi[1], Dr. J. C. Miraclin Joyce Pamila[2]

[1]E-mail: manoharsena@gmail.com
[2]Professor(CAS), Department of CSE, Government College of Technology,
Coimbatore – 641013. Tamil Nadu, India. E-mail: miraclin@gct.ac.in

---***---

Abstract - *In recent years, the researchers and academicians are showing their interest and research efforts in the area of Vehicular ad-hoc Networks (VANET) because of the variety of services it can offer. Since the VANET is an infrastructure less network, due to the absence of the centralized administration VANETs are highly vulnerable to the security threats and privacy issues. In this paper, we propose an efficient pseudo identity based authentication protocol for privacy preservation. The proposed pseudo identity based authentication technique resists the security threats and preserve the personal information over the vehicular ad-hoc networks*

Key Words: OBU, Proxy Vehicles, RSU, VANET, V2I, V2V.

1.INTRODUCTION

In the recent years, VANETs are receiving increasing attentions due to the rapid growth and advances in wireless communications and networking technologies. A vehicular ad-hoc network is a special kind of Mobile Ad hoc Network (MANET) which enables communication between nearby vehicles. In this type self-organizing network the vehicles are considered as communication nodes that are able to communicate with each other without using any infrastructure or centralized administration. There are two major communication models in VANETs are, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. The two major entity of a VANET are as follows:

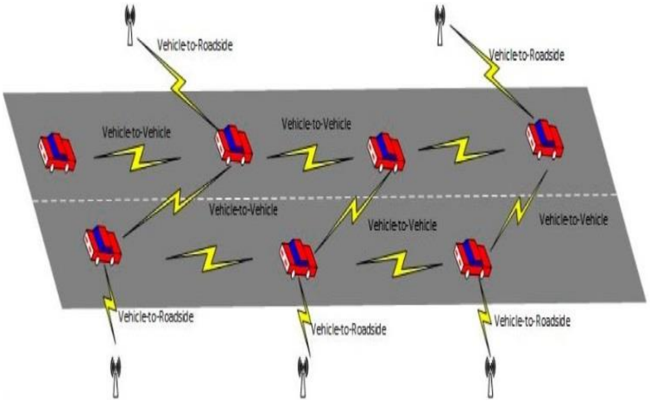

Fig -1: General Structure of VANET

OBU: An On Board Unit (OBU) is a device that resides in vehicle and helps in sharing information with Road Side Units (RSUs) or with other OBUs. Its components include a resource command processor (RCP), a user interface, a specialized interface to connect to other OBUs and a network device for short range wireless communication**.**

RSU: It is a road side infrastructure that may be fixed along roads junctions, parking slots, petrol pumps, eating joints, etc. It comprises of a device with networking capabilities that works for short range wireless communications.

1.1 Characteristics of VANET

Few important characteristics of VANETs are as follows:

Highly Dynamic Topology: The topology formed by vehicles in VANETs keeps on changing because of high speed and availability of multiple routes. Especially on highways vehicles are moving at very high speed so link between two vehicles lasts for a few seconds only.

Frequent Network Disconnection: Due to frequent change in topology there is constantly change in the link connectivity of VANETs. Where the nodes are scarce, the problem of network disconnection exaggerates and necessitate frequent requirement of RSU.

Mobility Modeling and Predication: Vehicles mobility pattern depends upon the type of road, the network of traffic light, speed of vehicle, flow of traffic and drivers mindset while driving his vehicle. The mobility modeling and prediction in VANETs is based on the availability of predefined roadmaps models.

Highly dynamic node density: The node (vehicle) density in VANET varies frequently depending upon road architecture, highways, or city environments. Communication in these situations has to be taken care.

Offline-infrastructure: Road side units are source of fixed infrastructure located at junctions, parking lots or even at selected points. But still we state this permanent source of infrastructure as offline because of high speed of vehicle, it is available to vehicle for short duration. The connection with RSU remains only when vehicle is within the range of a road side unit and not all the time.

Interaction with On-Board Sensors: In VANET environment every vehicle (node) should have an OBU and GPS to provide communication among vehicles. The OBUs can read data related to direction of the vehicle, speed of the vehicle and can communicate to the data center.

Heterogeneity of Applications: There are many applications of VANET which starts from safety, to traffic optimization and data sharing applications. Road safety messages are time critical and speed of data is not of high importance whereas in infotainment applications we need proper throughput and high data transfer speed.

1.2 Security Requirements of VANET

VANET must ensure some security requirements before they are implemented. A security system in VANET must satisfy the following requirements.

Authentication: Authentication ensures that the message is generated by the legitimate user. In VANET, a vehicle response to the information came from the other vehicle hence authentication must be satisfied.

Availability: Availability means that the information must be available to all users. DoS Attacks can bring down the network and information cannot be shared to all users.

Non-Repudiation: Non-repudiation requires a node cannot decline that he/she does not transmit the message. It may be tedious to determine the correct sequence in crash reconstruction.

Privacy: The privacy of a node means that the unauthorised node should be guaranteed. This is required to eliminate the massage delay attacks.

Data Verification: A frequent verification of data is needed to eliminate the false messaging

2. RELATED WORK

Many researchers have contributed in the past in designing effective network in VANET considering the security and privacy issues. There are many cryptographic and public key infrastructure based authentication schemes that have been proposed to guarantee security as well as preserve the personal information of vehicle in the VANET network. In this section we briefly discuss some of the works they have done.

X.Lin et al. [2] proposed a novel security protocol has been proposed for the Inter-Vehicle Communication (IVC) applications based on group signature and Identity-based signature schemes. The major issue in communications between OBUs lies in the contradiction between the design requirements for vehicle anonymity from regular users when traceability by the authorities. For this, a group signature scheme is proposed. The major benefit of the group signature scheme is that it gives anonymity of the signers. A verifier can judge whether the signer belongs to a group without knowing who the signer is in the group.

C. Zhang et al. [3] proposed a RSU-aided message authentication scheme, called RAISE. With RAISE, when an RSU is detected nearby, vehicles start to associate with the RSU. Then, the RSU provides an unique shared symmetric secret key and a pseudo ID that is shared with other vehicles. With the symmetric key, each vehicle generates a symmetric keyed-hash message authentication (HMAC) code, and then broadcasts a message by signing the message with the symmetric HMAC code instead of a PKI-based message signature. Other vehicles receiving the messages signed with the HMAC code are able to verify the message by using the notice about the authenticity of the message disseminated by the RSU. The reason why the RSU knows the authenticity of the messages is that the RSU has the HMAC encryption keys shared with vehicles. Note, in any circumstance that a vehicle cannot recognize a received message, it will simply go back to use the traditional PKI-based scheme to verify the message.

R. Lu et al. [4] proposed a novel efficient conditional privacy preservation (ECPP) protocol for secure vehicular communications. The ECPP protocol can efficiently deal with the growing revocation list while achieving conditional traceability by the authorities. In Key signature based authentication schemes a huge storage space at each OBU is used to store and verify the message authenticity. Meanwhile, the proposed protocol gains merits in the fast verification on safety messages and an efficient conditional privacy tracking mechanism, which can serve as an excellent candidate for the future VANETs. The ECPP protocol in able to improve efficiency in terms of the minimized anonymous keys storage at each OBU, fast verification on safety messages, and it supports an efficient conditional privacy tracking mechanism.

T.W.Chim et al. [6] proposed a Secure and Privacy Enhancing Communications Schemes for vehicular sensor networks (SPECS). This scheme able to manage ad-hoc messages (those sent out by arbitrary vehicles) and also allow vehicles that know one another to form a group and send group messages securely among themselves.

A identity-based (ID-based) signature scheme has been proposed by D. He et al. [9] to simplify the certificate management problem by using signers' identity information as their public keys. The private keys of the signers are generated by a trusted third party, called a private key generator (PKG). In this way, the verifier does not need to store all the public keys and the corresponding certificates of the signers. This section examines our ID-based signature scheme with batch verification, and further proves that our scheme is secure under a random oracle.

Y. Liu et al. [10] a proxy-based authentication scheme (PBAS) has been proposed to tackle the efficiency problem of the existing authentication schemes. In this proposed scheme, each proxy vehicle plays a major role, which is used to authenticate many messages at the same time. In addition, batch key negotiations can also be accomplished in the proposed scheme, in which an RSU can complete the batch process of vehicles' key negotiations by broadcasting a single message. In the PBAS, proxy vehicles plays an important role to authenticate multiple messages with a verification function at the same time. In addition, the RSU can verify the outputs from the verification function of the proxy vehicles.

3. System Model and Preliminaries

3.1 System Model

In Pseudo-ID based Authentication scheme, there are three participants which are explained below:

The Trusted Authority (TA): The TA is a trusted third party which generates system parameters and master public key and secret key, generates members' secret key, preloads them into vehicles. In addition, TA deliberates some benefits for vehicles with extra computational capabilities to promote them to behave as proxy vehicles. Note that computation and communication capabilities of TA are high.

The RSUs: The RSUs are the fixed infrastructure at roadsides, communicate with vehicles (proxy vehicles), can verify the validity of received messages from vehicles (proxy vehicles), and sends them to the TA authority (i.e.) traffic control center. In addition, RSUs store proxy vehicles' pseudo identities and their history to send to TA.

Vehicles: These are equipped with OBUs, and communicate with each others and RSUs. In addition, if they have extra computational resources, they can be proxy vehicles and serve for RSUs in verifying received messages.

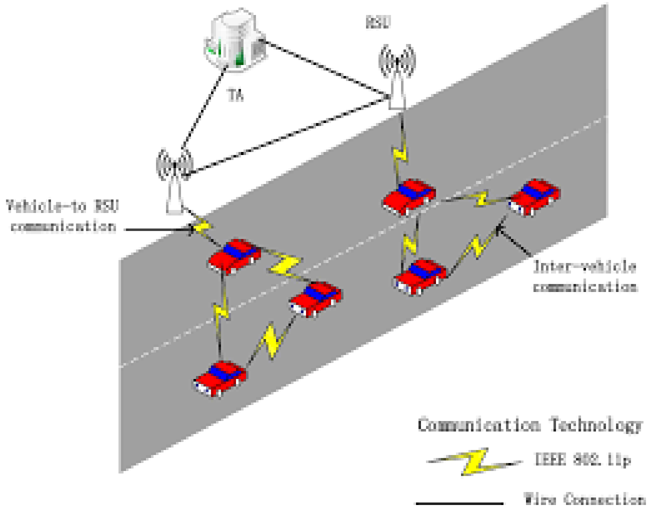

Fig -2: System model

3.2 Problem Statement

According to the above system model, this paper is based on the following assumptions: 1) RSUs are tamper-proof, and is hard to be compromised. 2) RSUs computation capability is higher than the vehicles; In our proposed scheme the vehicles are getting the pseudo id from the RSU, and the pseudo id is generated by hashing the original id of the vehicle. While the vehicle broadcasts the messages with the pseudo id only. The proposed scheme is resist the common security threats such as impersonation attack, modification attack, replay attack, etc., as well as users personal information also preserved keep data, including a small amount of read-only memory. It has details about owner information and vehicle details.

4. The Proposed System

In this section, we propose our Pseudo-ID-based Authentication scheme for VANETs to preserve the private information about the vehicles as well as the owner. The proposed scheme could be used for both Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V) communications. There are five phases in the proposed Pseudo-ID based Authentication scheme: the setup, Anonymous identity generation, Message Generation, Verification of messages by Proxy vehicle, Verification of proxy vehicles output by RSUs. We define the notations used below as follows.

Notation	Descrptions
Ri	The i-th RSU
Vi	The i-th Vehicle
IDvi	The real identity of the i-th vehicle
PIDvi	The pseudo identity of a vehicle
mi	a message sent by the vehicle vi
ti	The timestamp of the message
tp	The timestamp of the proxy vehicle
mp	a message sent by the proxy vehicle vp
H(.)	H(.): a one-way hash function such that SHA-1
||:	message concatenation operation, which appends several messages together in a special format

4.1 Setup: In this phase, system parameters are generated by TA, and have been loaded into RSUs and vehicles tamper proof devices. To do this, the following steps are done by the TA. The TA initializes the RSUs which are connected to that and assigns unique Id to each of the RSUs.

4.2 Anonymous identity generation: In this phase, each vehicle Vi hides its real identity, IDvi by getting a pseudo identity PIDvi from its registered RSUs. For doing this, the tamper proof device of a vehicle vi, which is preloaded with its original information such as vehicle owners information, registration details, etc., Then, it computes pseudo id by hashing its original information with the RSUs detail by the one way hash function SHA1 PIDvi = H(Ri || IDvi).

4.3 Message generation: In this phase, a vehicle generates a broadcast messages with its pseudo identity as follows, hi = h(mi, PIDvi, ti, Ri) and the broadcasted messages further forwarded by the proxy vehicles as hi = h(mp, PIDvi, tp, Ri), where ti and tp is a timestamp of a vehicle and the proxy vehicle respectively.

4.4 Verification of messages by proxy vehicles: In this phase, a proxy vehicle verifies the integrity and senders' identities of received messages, (PIDvi, ti, mi ,Ri). For this goal, the proxy vehicle first checks the freshness of the received message by the timestamp Ti and the validity period of pseudo identities. If messages are fresh and pseudo identities are valid, the proxy vehicle computes hi = h(mi, PIDvi, ti, Ri).

4.5 Verifying proxy vehicles' output by RSUs: In this phase, RSU verifies the results received from proxy vehicles to identify and remove malicious proxy vehicles and also detect faulty results.

The Proposed pseudo identity based authentication protocol ensures the security of the VANET by hiding the original identity of the vehicle and owners information by proving pseudo identity and it also resists the common security threats such as impersonation attack, modification attack and replay attack. The proposed scheme also revokes the malicious vehicle from the network.

5. Conclusion

In this paper, we have proposed an efficient pseudo identity based authentication protocol for privacy preservation in order to enhance the security of VANETs. The proposed scheme hides the original identity and owner's information by providing a pseudo id. The computation complexity and the verification of messages in the proposed scheme is easier than the previously proposed security protocols. There is no need to store the key signatures or certificates to authenticate the messages. The proposed scheme preserves the personal information as well as resist the common security threats in the VANETS.

REFERENCES

[1] Maryam Rajabzadeh Asaar, Mahmoud Salmasizadeh, Willy Susilo,Akbar Majidi, 2018 "A Secure and Efficient Authentication Technique for Vehicular Ad-Hoc Networks", IEEE Transactions On Vehicular Technology, VOL. 67, NO. 6. pp. 5409-5423.

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

[3] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, 2008, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in Proc. 27th Int. Conf. Comput. Commun., pp. 1903– 1911.

[4] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, 2008, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in Proc. IEEE Int. Conf. Commun., pp. 1451–1457.

[5] Memon, I. 2015, "Authentication user's privacy: An integrating location privacy protection algorithm for secure moving objects in location based services", Wireless Personal Communications, 82, 1585–1600.

[6] T.W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, 2011, "SPECS: Secure and privacy enhancing communications schemes for VANETs," Ad Hoc Netw., vol. 9, no. 2, pp. 189–203.

[7] Ram Shringar Raw, Manish Kumar, Nanhay Singh, 2013, "security challenges, issues and their Solutions for VANET", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, pp. 95-105.

[8] Ankita Agrawal, Aditi Garg, Niharika Chaudhiri, et.al., 2013, "Security on Vehicular Ad Hoc Networks (VANET): A Review Paper", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 1, pp.231-235.

[9] D. He, S. Zeadally, B. Xu, and X. Huang, 2015, "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.

[10] Y. Liu, L. Wang, and H.-H. Chen, 2015, "Message authentication using proxy vehicles in vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 64, no. 8, pp. 3697–3710.