International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Privacy Preserving Schemes in Vanets: A Review

Shazia sulthana, Dr. Jayanthi K Murthy

Abstract: ***Vehicular ad hoc networks (VANETs) can significantly improve traffic safety and privacy of driver. The main concern to send privacy information from OBU which is installed in a vehicle with Roadside unit. Vehicles have to be prevented from some attacks on their privacy and misuse and adaptation of their private data. For this purpose, privacy preservation issues are important prerequisites for VANETs. VANET Networks uses the privacy preserving schemes to improve traffic safety, mobility, and environmental protection with enhancing services. Privacy preservation based on pseudonyms and anonymous authentication to cover the original identity of the drivers cannot fully preserve the drivers' privacy. This survey will explore the various privacy requirements of the authentication during data delivery and as well as they way to authenticate the vehicles involved in communication.***

I. INTRODUCTION

Transportation mechanism plays an important role in our life. However, today's road transportation Networkss have several disadvantages and inefficiencies which cause problems like traffic jams and accidents. Many researchers are trying to enhance safety and efficiency on roads using intelligent transportation Networkss (ITSs). Several organizations proposed ITS projects and applications such as the U.S.A. Vehicle Safety Consortium the Japan Road and Traffic Intelligence Society Organization, the Taiwan Intelligent Transport Society[1].

An important part of Intelligent Transportation Networks is VANET. Vehicular Adhoc Network (VANET) is a kind of Ad hoc Network .which is a wireless ad hoc network consisting of mobile nodes. VANET consists of vehicles as mobile nodes and road side units (RSUs) as fixed nodes. Vehicles can communicate with each other (V2V) and with Infrastructure of RSUs (V2I), see Figure 1-1.

Privacy is very important factor to adopt VANET widely. Drivers requires to protect their identities from others. They unlike to be traced or eavesdropped by other vehicles or entities. On opposite, the vehicle identity must be determined if that vehicle misbehaves and harms other vehicles. Drivers must be responsible for their messages.

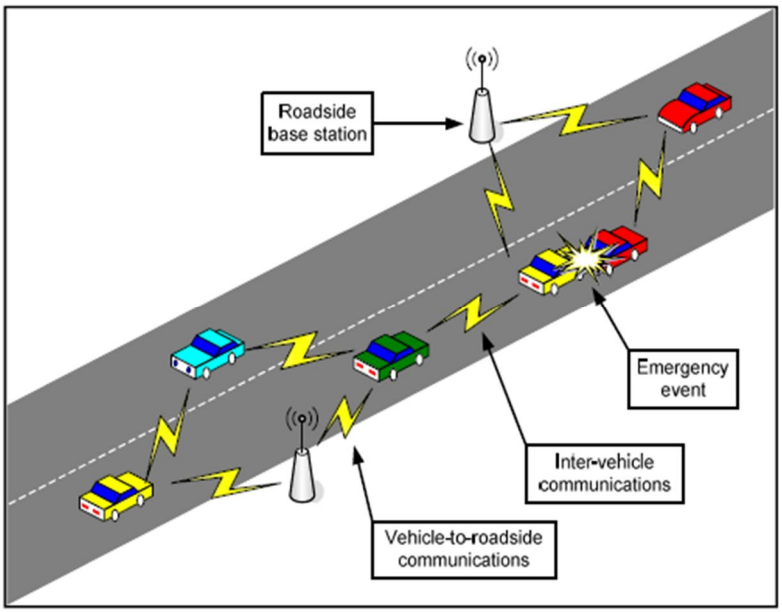

FIG 1-1: Vanet Architecture

with the advances in wireless adhoc communication technology, it is considered that vehicles will be equipped with wireless communication devices, called onboard units (OBUs), to communicate with roadside units (RSUs) located on the roadside or at a street intersection. One vehicle OBU is connected with another vehicle OBU is called as vehicle-vehicle communication.each

vehicle communicate send and receive messages by On Board Unit (OBU) and equipped with Event Data Recorder, GPS, Trusted component etc. The Roadside Units (RSU) is responsible for broadcasting safety messages periodically. Wireless communication is itself susceptible to various attacks; hence the security of VANET cannot be determined. Few malicious vehicles may send false information into the network to gain unfair advantage on the road or to cause serious accidents. thus the sender vehicles should be authenticated by the receiver before taking any action based on the received safety message. Usually origin authentication is provided by digital signature with the help of certification services. In VANET, a Trusted Authority (TA) serves the purpose, but it involves huge communication over-head and also a vehicle has to communicate with TA via RSUs. Nowadays RSUs are fixed infrastructures along the road, which periodically broadcast safety related information, Typically RSUs placed over every 300m to 1 km and they broadcast at the period of every 300ms. For this reason placing RSUs along a long highway to provide omnipresent infrastructure is not feasible economically for now. Hence vehicle should be able to authenticate others with limited help from TA or fixed infrastructure.

A. Hardware Required for VANET Privacy Module

Event Data Recorder (EDR) are responsible for storing the vehicles critical data, such as position, speed, time, received messages etc. during emergency events which will help in crash reconstruction and the attribution of liability. It should be tamper-proof.

Trusted Component (TC) all the cryptographic materials (keys) of a vehicle need proper hardware protection, namely TC. The TC stores all the cryptographic data and performs all the cryptographic operations. The TC also includes its own clock and battery that is periodically recharged from vehicles electric circuits.

Electronic Licence Plate (ELP) these are unique ID of vehicles equivalent to the traditional license plates. The advantage of ELPs is that they will automate the paper-based document checkup of vehicles, detection of stolen cars. An

Vehicular Public Key Infrastructure (VPKI) The large number of vehicles registered in different countries and travelling long distances requires a robust, inter-operable and scalable key management scheme. The need for Vehicular Public Key Infrastructure (VPKI) where Trusted Authority (TA) will issue certified public/private key pairs to vehicles. There will be several TAs corresponding to different regions; they should cross certify each other. Vehicle manufactures can also take the role of TAs. e cryptography), the most compact public key crypto Networks is used due to its less .

B. Security Requirements

We focus on security and privacy in VANETs. A secure IBV scheme should satisfy the following security objectives: message authentication, identity privacy preserving, traceability, nonrepudiation, nlinkability, and replaying resistance. The detailed descriptions of the given requirements are listed as

Follows.

1) *Message authentication*. Any RSU should be able to verify that a message is indeed sent and signed by a certain legitimate vehicle without being modified or forged by anyone.
2) *Identity privacy preserving*. The real identity of a vehicle should be kept anonymous from RSUs and other vehicles. Any third party should not be able to reveal the vehicle's real identity by analyzing multiple messages sent by it.
3) *Traceability*. Although the vehicle's real identity should be hidden from RSUs and other vehicles, if necessary, TA should have the ability to retrieve the vehicle's real identity. In addition, once the malicious vehicle wants to escape from its guilty of causing the accident or crime, TA still enable to trace its real identity from its message sent under the proposed scheme.
4) *Nonrepudiation*. A malicious vehicle is unable to broadcast wrong messages to mislead an RSU and deny the behaviors when TA traces it by its message signatures.
5) *Unlink ability*. A malicious vehicle or RSUs cannot successfully distinguish an anonymous entity by linking some of its message signatures.
6) *Replaying resistance*. A malicious vehicle cannot collect and store a signed message and attempt to deliver it at a later time when the original message is invalid.

C. Classification Of The Privacy Preserving Schemes

During the last decade, there are number of research work related to PPA in VANETs. Because the particular actual identities of vehicles are confidential for privacy preservation in PPA, authentication is based on the encryption/decryption technologies. Categorized the PPA schemes by authentication key cryptographies and privacy preservation mechanisms

respectively as follows.

D. Categorization on authentication

The common objectives of PPA schemes are to minor communication overhead, preserve node anonymity, isolate the misbehaving nodes, and non-repudiation. According to the key cryptographies applied for authentication in VANETs, categorize the existing PPA schemes as follows.

1) Symmetric-key-based authentication (SKBA) schemes: The SKBA schemes use symmetric key cryptographies for message authentication. Each node uses its own key or a shared group key for creating/verifying message authentication codes (Media access codes).

2) Asymmetric-key-based authentication (AKBA) schemes: The AKBA schemes use public key Cryptographies or digital signatures for sign-ing/ verification in authentication. The public/private key pair can be the group-based public key with multiple corresponding private keys or the node's own public key with the individual private key for the digital signature. Meanwhile, according to the probability and frequency of infrastructure access

(e.g., RSUs and RTAs), further categorize AKBA schemes as follows. Public-key-infrastructure-based (PKI-based) authentication schemes: The PKI-based schemes require infrastructure access frequently to verify certificates, revoke keys, or gather new keys; such as Conventional PKI-based schemes require additional communication to manage the certificate revocation lists, which causes heavy overheads.

Identity-based (ID-based) authentication schemes: the ID-based schemes have been proposed to reduce communication overheads by using ID-based cryp-to Networks in authentication .Conventional ID-based schemes simplify the certificate management process by using the vehicle's identity in signing and verification of digital signatures.

E. Categorization on privacy preservation

In VANETs, vehicles usually do not want their private information such as name, position, moving routes, and user data to be revealed against illegal tracing and user profiling. Thus, the authorization of the third parties, anonymous communications, or the anonymity of user identities should be supported to preserve privacy in VANETs. On the other hand, when traffic accidents or certain crimes occur, vehicle anonymity should be conditional and the identity information has to be revealed by the legal authority to establish the liability of accidents or crimes, which is so-called conditional privacy. In this survey, according to the different mechanisms applied for privacy preservation in VANETs, categorize the mechanisms for privacy preservation as follows.

1) Authorization-based privacy preservation (ABPP: The mechanisms used in ABPP usually apply anonymous key management to preserve privacy in authentication .Anonymous key pairs, which do not contain any information of vehicle IDs, are certificated by the RTA or CA. In this way, the relationship between the anonymous key pairs and the actual vehicle identity cannot be discovered by a third party without a special authorization. Normally, a vehicle will manage a set of anonymous keys to prevent tracking. The key point in ABPP is the distribution of authorized materials among authorities, where authorities access the database of key management and match anonymous key pairs with the real vehicle identities.

2) Pseudonym-based privacy preservation (PBPP): The usage of pseudonyms to achieve vehicle anonymity is a superior solution for privacy preservation to PPA, which intimately links a real world ID to the corresponding pseudonyms.. The pseudonym may be generated by RSUs, RTAs, the vehicle itself, or even can be downloaded from a trusted site periodically. The adoption of pseudonyms in PPA conceals the real-world identity of vehicles; even though peer vehicles cannot identify the sender of a specific message, it is still able to authenticate the sender. By frequently updating the pseudonyms during communication, PBPP defends legitimate vehicles against location tracing and user profiling.

Both ABPP and PBPP prevent malicious vehicles from abusing anonymous authentication techniques to achieve malicious goals or escape from their liabilities. An ideal PPA scheme in VANETs must have a mechanism to validate authenticated transmissions and conditional privacy preservation.

F. Overview of identity batch schemes

Lee and Lai's IBV scheme exists some security risks in VANETs. First, the sender's real identity can be traced or revealed by anyone who only holds the publicly known Networks parameters. Thus, their scheme does not achieve the requirement of privacy preserving. Second, a malicious vehicle broadcasts messages on behalf of another legitimate vehicle and even uses a fake identity to avoid being traced. For the above weaknesses, Lee and Lai's IBV scheme

is not secure and suitable for VANETs. Moreover, their scheme also lost an advantage. The private keys cannot be generated offline by the tamper-proof device. A vehicle cannot get a list of private keys along with the corresponding pseudo identities early. Some computation delays will be caused in the message signing process at the vehicle side

Raya and Hubaux proposed a scheme to hide the real identities of users by anonymous certificates .Each vehicle is preloaded with a large number of anonymous public/private key pairs and the corresponding public key certificates. The conventional public key infrastructure (PKI) is adopted as the security foundation to achieve both message authentication and integrity. In addition, the vehicle takes advantage of a public/private key pair with a short lifetime to avoid movement tracking. However, the main problem is that each vehicle demands a large storage capacity to save a number of key pairs and the corresponding certificates and incurs the high cost of message verification. The authority also needs to store all anonymous certificates of vehicles, which causes inefficiency for certificate management and is expensive for deployment.

Lin *et al*. proposed a scheme based on a group signature . With this scheme, only a group public key and a private key are stored in the vehicle. The group public key is the same for all vehicles, and the private key of each vehicle is different. Any receiver only confirms the authenticity of the signature by the group public key, and the vehicle has no identity information of the message sender in the transmitted message. Despite decreasing the overhead of preloading a large number of anonymous key materials in each vehicle, this scheme increases a large computational overhead through its requirement to maintain a certificate revocation list. In addition, the length of group signature is much longer than one of the ordinary signature, and the computational cost of verifying group signature is high.

Zhang *et al.* [7] proposed an IBV scheme for V2I and V2V communications in VANETs. They adopted a one-time identity-based signature, which eliminates the verification and transmission costs of certificate for public keys. It reduces the overall verification delay of a batch of message signatures, and its batch verification process for signatures from multiple vehicles is much faster than that of other PKI-based schemes, such as the elliptic curve digital signature algorithm (ECDSA). In addition, the vehicle related information has to be protected from malicious access, although the TA can reveal the sender if a dispute appears. The TA is capable of tracing a sender's real identity from its pseudo identity. Therefore, the conditional privacy can be achieved. An adversary may simulate a fake condition, such as traffic jam, by collecting and storing the vehicle messages and signatures in the corresponding condition. Next, the adversary can replay the information to mislead the traffic control center when she/he wants. This scheme does not satisfy the property of nonrepudiation. A malicious vehicle can broadcast wrong information to mislead other vehicles and deny the behavior when the TA traces her/him by signature. For the given two threats, Lee and Lai proposed an improved scheme to enhance the security and also held the efficiency of this scheme.

Chim *et al[2].*described some limitations of the Zhang *et al.*'s IBV scheme and proposed a new identity based authentication scheme using two shared secrets to satisfy the privacy requirement and also the bloom filter and the binary search techniques. First, the IBV scheme relies heavily on a tamper-proof hardware device, installed in each vehicle, which preloads the Networks-wide secret key. is broken, the whole Networks will be compromised. Second, a vehicle's real identity can be traced by anyone, thus the IBV scheme does not satisfy the privacy requirement. Third, the IBV scheme has a flaw such that a vehicle can impersonate another vehicle (impersonation attack) or even use a fake identity to avoid being traced (anti-traceability attack). Finally, in their batch verification scheme, if one of the signatures is erroneous, the whole batch will be dropped. This is uneconomical because most signatures in the batch may actually be valid, thus may imply a not satisfactory successful rate.

Horng *et.a[4].* indicated that Chim *et al.*' scheme is not resistant against impersonation attack, and they show how a malicious vehicle can broadcast fake messages on behalf of another or how a malicious vehicle in a group can fake another member to send group messages securely among themselves. Then they modified the message signing phase of their scheme in a way that it can meet security and privacy requirements of Chim *et al.*' scheme. Generating a notification message, handle invalid signatures in the batch and extract valid ones from the batch instead of dropping the whole batch are the same in SPECS .

II. CONCLUSION

In this paper , reviewed the significance of privacy in vehicular adhoc Networks .security requirements and components involved. various identity batch techniques for both vehicle-to-vehicle along vehicle to infrastructure. The batch-based verification for multiple message signatures is more efficient than one-by-one single verification when the receiver has to confirm a large number of messages. In particular, the batch verification process of the proposed IBV scheme needs only a constant number of pairing and point multiplication computations, independent of the number of message signatures. these schemes still rely heavily on a tamper-proof hardware device in each vehicle. Therefore, the batch verification can dramatically decrease the time cost on verifying a large number of message signatures, which can achieve much better scalability

REFERENCES

[1] Shiang-Feng Tzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and Muhammad Khurram Khan" Enhancing Security and Privacy for Identity-Based Batch Verification Scheme in VANETs" IEEE Transactions on Vehicular Technology, Vol. 66, No. 4, April 2017

[2] Yokohama Research Laboratory, Hitachi, Ltd.,Yokohama, Kanagawa, 244-0817, Japan "Privacy-preserving authentication schemes for vehicular ad hoc networks: a survey" Wireless Communications And Mobile Computingwirel. Commun. Mob. Comput. 2016; 16:643–655

[3] Debiao He, Sherali Zeadally, Baowen Xu and Xinyi Huang' An Efficient Identity-based Conditional Privacy-preserving Authentication Scheme For Vehicular Ad-hoc Networks"10.1109/TIFS.2015.2473820,IEEE Transactions on Information Forensics and Security

[4] Jie Cui , Jing Zhang, Hong Zhong, and Yan Xu "SPACF: A Secure Privacy-Preserving Authentication Scheme for VANET With Cuckoo Filter" Ieee Transactions On Vehicular Technology, Vol. 66, No. 11, November 2017

[5] Priyanka patel, Nilesh Marathe Survey of Privacy Preservation in VANETs International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol.6, No1, Jan-Feb 2016.

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

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