International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 13, Issue 2 (February 2017), PP.25-29

Enhanced Conditional Privacy Preservation In VANETs

Chitra A. Parmar[1], Sunil P. Khachane[2]
[1,2]Rajiv Gandhi Institute of Technology, Mumbai, India

Abstract:- The Vehicle drivers (users) do not want their personal information such as vehicle names, license plate, speed, positions, moving routes, and user information to be revealed, in order to protect them against any illegal tracing or user profiling. Thus, this information must be protected from any kind of misuse or attacks. For this the obscurity of vehicular nodes should be supported to preserve privacy of vehicles and their users. Also, we should be able to investigate for accidents or liabilities from non-repudiation. Hence, we present an enhanced conditional privacy preservation scheme for vehicular ad-hoc networks (VANETs). This scheme includes an ID-based cryptosystem to assure user's obscurity using pseudonyms; however the model provides a backdoor for authorities to track misbehaving and suspicious users.

Keywords:- Conditional Privacy, Identity-Based Cryptography, Obscurity, Pseudonym, Traceability, Vehicular Adhoc Network

I. INTRODUCTION

The Vehicular Ad-Hoc Network (VANET) is a technology that uses moving vehicles as nodes in a network to create a mobile network. VANET turns every participating vehicle into a wireless router or node, allowing vehicles to connect with each other in range of approximately 100 to 300 meters thus resulting in a wide range network of vehicles. It is predicted that the first systems that will adapt this technology are cops and fire vehicles to communicate with each other for safety purposes. In VANET, communication takes place between vehicles, or between vehicles and fixed equipment's which are road side units and certification authorities. Hence, a VANET generally consists of three network components: road side units (RSUs), on board units (OBUs) or vehicles and certification authorities (CA).

A geographical area is divided into many regions; each region is served by one certification authority (CA). This scenario consisting of one CA, specific number of RSUs along roadside and a large number of vehicles on or by the road is considered as the general urban vehicular communication (UVC) structure.

Vehicular ad-hoc networks (VANETs) are targeted to improve road safety and traffic optimization. Moreover, they also provide payment services (e.g., toll collection), location-based services (e.g., finding the closest fuel station), infotainment (e.g., Internet access) and many vehicle-centred applications. Obviously, security is also required in this application category. The security in VANET is most critical issue because the information is propagated in open access environment. VANET's are exposed to various threats and attacks. It is necessary that all the data which is transmitted should not be changed by the attackers [1].

A. Related Work

There are many research works for privacy preservation in VANETs. These approaches have mechanism for pseudonym generation and updating but they lack tracking mechanisms [2] - [4]. Some privacy schemes [5], [6] and [7] were such which did not used pseudonyms for privacy preservation. These schemes were based on group signatures and mostly used ID-based cryptography. For example, in [7] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho and Xuemin Shen designed a conditional privacy-preserving vehicular communications protocol based on group signatures and ID-based signatures. The most important benefit of using group signature schemes is that they assure the unlinkability of the messages because group members can anonymously sign on behalf of the group. A disadvantage of this model is that if a malicious vehicle is selected as a group leader, all group members privacy may be leaked by the malicious leader.

Moreover, several proposals suggest the use of a public key infrastructure (PKI) and digital signatures to secure VANETs. To evict misbehaving vehicles, Raya et al. proposed protocols focusing on revoking certifications of malicious vehicles [8]. A big challenge arising from the PKI-based schemes in VANETs is the heavy burden of certificate generation, storage, delivery, verification, and revocation. Most of the ID-based cryptosystems which were proposed prior to [9] have a Key Generation Center (KGC) as a trusted authority to distribute private/public keys to vehicles. The KGC uses a master key to generate the user's private key. Hence, the KGC has access to these keys which creates a key escrow problem. To address this problem, the authors of [9] suggested a new model where private/public RSA keys of each vehicle are generated on board, and changed often to ensure privacy over a long period of time. A third party referred to as Regional Transport Authority (RTA) uses the user's public key and ID and computes the signature value for users. The V2V and V2I communications includes these signature values, which is verified based on RTA ID and public parameters stored in the RTA's list. When violations such as car accidents occur, the RTA can trace a user by computing the Privacy ID (PID) with the public parameters of PID and all IDs registered in the RTA.

B. Security Goals

1) Privacy*:* The profile or a driver's personal information (such as driver's name, the license plate, speed, position, and traveling routes, etc.) must be maintained against any sort of illegal access. We consider the following two cases:

- Communication between OBUs and RSUs: In this case, privacy means that a malicious node must not be able to determine whether two different messages come from the same vehicle.
- Communication between OBUs: Here, privacy means that deciding whether two different valid messages coming from the same vehicle is sort of burden for all other nodes except an authorized node [10].

2) Non-repudiation: Non-repudiation requirement means that an entity is not able to deny having sent or received some message, if it has sent or received that message. It is required for the sending node in V2V warnings and beacons. In this way, if a vehicle sends some malicious data, there will be a proof that could be used for liability purposes [11].

C. Attacks on Privacy and Non-Repudiation

1) Attacks on privacy: Attacks on privacy in VANETs are mainly related to illegally getting secret/private information about vehicles. Getting information about a specific vehicle's status could put its driver's privacy at risk, as there is a direct relation between a vehicle and its driver. These attacks can then be classified as follows:

- **Identity revealing attack:** Obtaining the owner's identity of a particular vehicle could put its owner's privacy at risk as mostly; a vehicle's owner is also its driver, so it would result in obtaining personal data about that person [12].
- **Location tracking attack:** The location of a vehicle at a specific moment, or the route followed by a vehicle over a long period of time are considered as its personal data. Access to such information allows malicious users to build that vehicle's profile and thus, that of its driver [12].

2) Attacks on non-repudiation*:* In VANETs, the non-repudiation means that a vehicle cannot deny of having sent a specific message if it has sent that message. Typically, by generating a signature for the message in VANETs, the vehicle cannot later disagree on the sent messages. The attack on non-repudiation is as follows:

- **Repudiation attack:** Repudiation refers to disagreement of participation in all or part of communications in VANETs. For example, a malevolent driver could disagree of having conducted an operation on a credit card purchase, or malicious vehicles could abuse anonymous authentication techniques to achieve their selfish goals or escape from their liabilities [12].

II. SYSTEM DESCRIPTION AND REQUIREMENTS

A. Desired Requirements

The main purpose of this design is to employ an efficient conditional privacy preservation system in VANETs. The system considers the following aspects:

1) Obscurity: Obscurity is needed to secure the user's privacy. From the OBUs point of view; leaking identities, locations or profiles information is not tolerable as it puts user's privacy at risk.

2) Traceability: The presence of obscurity raises the need of a tracking mechanism to secure VANETs from inside attackers. Traceability is also required to allow law enforcement authorities to find the attackers.

B. Proposed System

The main components of VANET – CCA, CAs, RSUs and OBUs are shown below in Fig. 1. The OBUs communicate with each other (V2V communication) or with RSUs (V2I communication). The RSUs are immovable and they are in a fix number which do not change frequently. They are connected to each other and to their regional certification authority through wired connections. The categorization of CAs is hierarchical; they are categorized over the country, states, cities or regions and they are governed by a Central Certification Authority (CCA). It is duty of CA to register the OBU's and RSU's. The number of CAs is proportional to the number of vehicles. It means that with the increase or decrease in number of vehicles the number of CAs also increases or decreases respectively. Our proposed design consists of three phases: initialization phase, vehicle (OBU) registration phase and pseudonym update phase.

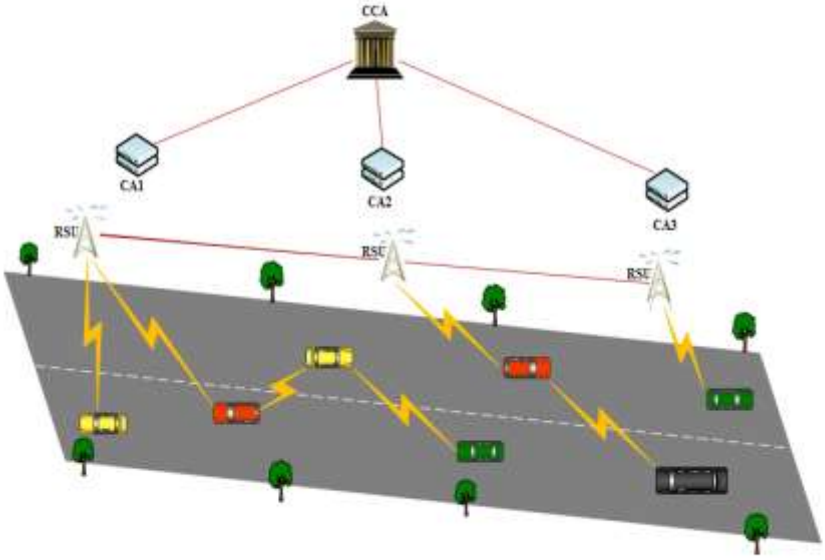

Fig. 1: Model for Proposed System

1) Initialization Phase: In the initialization phase, the CCA generates and computes public as well as secret parameters required for communication using ID-based cryptosystem. Then it delivers the secret parameters to all the CAs and declares the public parameters to all the VANET components (CAs, RSUs, and OBUs). In this model, we consider that the CAs network is secure.

2) Vehicle Registration Phase: Every VANET entity maintains a table which includes information of all the CAs along their IDs, public keys, and their respective regions. We know that the CA's are distributed regionally but it is not necessary for a vehicle to register to its regional CA, it can register itself to any CA in the network. When a vehicle 'a' wants to register to the VANET network, first it itself generates its RSA public and private keys. Then it will choose a random CA say CA_x, perform encryption using public key of CA_x on its own identity and public key and will send it to CA_x as shown below:

$$E_{pk(x)}(ID_a, pk_a) \tag{1}$$

where; $E_{pk(x)}$ is encryption by public key of CA_x, ID_a is identity of vehicle 'a' and pk_a is public key of vehicle 'a'. When CA_x receives registration request it computes the first pseudonym and the first signature of vehicle 'a' and sends it to vehicle 'a' including the other necessary parameters such as signature expiration time, nonce, etc. encrypted using public key of vehicle 'a' as described in following equation:

$$E_{pk(a)}(ID_a, P_{a1}, Sig_{a1}, T_{exp1}, N_1) \tag{2}$$

where; $E_{pk(a)}$ is encryption by public key of vehicle 'a', ID_a is identity of Vehicle 'a', P_{a1} is new pseudonym computed by CA_x, Sig_{a1} is new signature computed by CA_x, T_{exp1} is the signature expiry time associated with Sig_{a1} and N_1 is nonce value associated with newly computed pseudonym and signature.
On receiving this message, vehicle 'a' verifies the signature if it is valid it accepts the message. This completes vehicle registration phase. Note that every CA in the network maintains a table containing the vehicle ID, update date and the latest pseudonym it generated for each vehicle. This information is helpful in tracing a vehicle whenever required.

3) Pseudonym Update Phase: There are two different cases in which Pseudonym update can occur. They are as follows:

(i) Normal pseudonym update case: Normally, a vehicle has to update its pseudonym before its current signature expires. However, if a vehicle wants to update its pseudonym even if there is long time left for current signature expiration time, it can do it. A vehicle can update its pseudonym from the same CA where it generated its current pseudonym or can update it from any other CA. We assume that CA's are not being trusted so following conditions must be met while selecting a CA for updating pseudonym:

- A vehicle cannot update its pseudonym back-to-back from the same CA for more than two times in a sequence.
- CA will be selected randomly from the group of remaining CA.

For updating pseudonym, vehicle ‘a’ composes following message which includes its identity, current pseudonym, current signature, current public key, current time, and a nonce encrypted with its private key:

$$M = E_{sk(a)}(ID_a, P_{ai-1}, pk_a, t, N_{i-1}) \tag{3}$$

where; $E_{sk(a)}$ is encryption by private key of vehicle ‘a’, P_{ai-1} is the current pseudonym of vehicle ‘a’, t is current time, N_{i-1} is the nonce value when current pseudonym & signature was composed.

Then it sends this message 'M' with some other necessary parameters to a CA_x by encrypting it with public key of CA_x as follows:

$$E_{pk(x)}(ID_a, P_{ai-1}, Sig_{ai-1}, pk_a, T_{expi-1}, t, M) \tag{4}$$

where; Sig_{ai-1} is current signature, T_{expi-1} is expiry time of current signature.

When CA_x receives such update request message, it checks the current time and validates the signature and pseudonym present in the message. If it is found correct, then CA_x will generate new pseudonym and signature and send it to vehicle ‘a’. Vehicle ‘a’ verifies the signature; if successful then it accepts the message. Thus, the vehicle’s pseudonym is updated.

(ii) Special pseudonym update case: There is a special case in the pseudonym update phase; when vehicle ‘a’ has updated its RSA public and private keys and wants to update its pseudonym. In this case, vehicle ‘a’ needs to send it’s old as well as the new public key in the update request message to CA_x. The update request message for special pseudonym update case in equation (3) becomes like following:

$$M = E_{sk(a)}(ID_a, P_{ai-1}, pk_{a(new)}, pk_{a(old)}, t, N_{i-1}) \tag{5}$$

Then, the CA_x perform verification by generating the old pseudonym using the old public key. If old pseudonym received in the message matches with the generated pseudonym, verification is successful. Next, the CA_x generates the new pseudonym and signature by using the new public key.

III. OPERATION OF PROPOSED SYSTEM

A. Broadcasting Safety Message

When a vehicle ‘a’ wants to send a safety message ‘SM’, it encrypts the message, the current time, and the expiration time using its private key and then it broadcasts this message in its vicinity along with some other necessary parameters as shown below:

$$P_{a1}, Sig_{a1}, pk_a, E_{sk(a)}(SM, t, T_{expi}) \tag{6}$$

The signature is verified by the destination node. If successful, the destination decrypts the message using the public key of sending vehicle.

B. Traceability

When CCA receives complaint of malevolent behaviour of some vehicle having pseudonym ‘xyz’, the CCA sends a Find Request to all the CAs. This request includes the malevolent pseudonym. As stated earlier, each CA maintains a list of IDs and their corresponding pseudonyms. The CAs checks for the pseudonym ‘xyz’ in their databases. The one that finds it reverts back the corresponding ID to the CCA. The search for the malevolent pseudonym is done in linear time which minimizes the computational overhead.

C. Revocation

When the CCA makes a determination to revoke a vehicle, it will inquire for the present pseudonym of this vehicle. For this the CCA circulates the ID of the vehicle to all CAs in the network. Each CA that has communicated earlier with this vehicle will reply a triplet containing vehicle ID, corresponding pseudonym and update date. The present pseudonym of this vehicle is the one that has the most recent update date. Once the CCA figures out the present pseudonym of this vehicle, it sends this present pseudonym along with the ID to all CAs. Each CA maintains a revocation list that includes the IDs of the revoked vehicles. When a vehicle approaches to a CA for updating its pseudonym, the CA checks for the ID (contained in the pseudonym update request) in the revocation list and if it finds it, the CA interrupts the pseudonym update process and ultimately the current pseudonym and signature will expire. Then, each CA circulates the present pseudonym of the revoked vehicle to all the vehicles in its vicinity. Each vehicle maintains a list of revoked pseudonyms. Hence, a revoked vehicle will not be able to communicate with other vehicles.

IV. CONCLUSION

The proposed enhanced conditional privacy preservation scheme considers attacks on privacy as well as non-repudiation. According to this scheme, the CAs and the RSUs are not considered as trusted parties. The proposed scheme uses pseudonyms generated using the ID-based cryptosystem for authorities to trace malevolent vehicles. This scheme preserves conditional privacy along with other security services such as authentication, confidentiality and non-repudiation.

REFERENCES

[1]. Maxim Raya and Jean-Pierre Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007.

[2]. Levente Buttyan, Tamas Holczer, Andre Weimerskirch, and William Whyte, “Slow: A practical pseudonym changing scheme for location privacy in VANETs,” in IEEE Vehicular Networking Conference (VNC), October 2009.

[3]. Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, “An identity-based security system for user privacy in vehicular ad hoc networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239, September 2010.

[4]. Wu Yuntian, Wu Ting, and Zhang Jin, “Multi-PKG id-based signcryption with anonymity and traceability for ad hoc networks,” in Second International Workshop on Computer Science and Engineering, October 2009.

[5]. Krishna Sampigethaya, Leping Huang, Mingyan Li and Radha Poovendran, "AMOEBA: Robust location privacy scheme for VANET," IEEE Journal on Selected Areas Communication, vol. 25, no. 8, pp.1569-1589, October 2007.

[6]. Leping Huang, Kanta Matsuura, Hiroshi Yamane, and Kaoru Sezaki, "Enhancing Wireless Location Privacy Using Silent Period" Wireless Communications and Networking Conference, pp. 1187- 1192, March 2005.

[7]. Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, and Xuemin Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3442–3456, November 2007.

[8]. Maxim Raya, Panagiotis Papadimitratos, Imad Aad, Daniel Jungels, Jean-Pierre Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1557–1568, October 2007.

[9]. Jaeduck Choi and Souhwan Jung, "A security framework with strong non-repudiation and privacy in VANETs," Consumer Communications and Networking Conference, January 2009.

[10]. Vinh Hoa LA and Ana Rosa Cavalli, "Security attacks and solutions in vehicular ad hoc networks: A survey," International Journal on Ad Hoc Networking Systems, vol. 4, no. 2, April 2014.

[11]. Namarpreet Kaur and Aman Arora, "A research on various attacks in VANET," International Journal of Advanced Research in Computer Science, vol. 6, no. 6, pp. 85-88, June-July 2015.

[12]. Jie Li, Huang Lu and Mohsen Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," IEEE transactions on parallel and distributed systems, vol. 26, no. 4, pp. 938-948, April 2015.