Optimized Conditional Privacy Preservation in VANETs

Mostafa Dikmak, Zahraa Sabra, Ayman Kayssi and Ali Chehab
Department of Electrical and Computer Engineering
American University of Beirut, Beirut, Lebanon
Email: {mkd03, zns07, ayman, chehab}@aub.edu.lb

Abstract—In this paper, we present an optimized conditional privacy preservation model for vehicle ad-hoc networks (VANETs). This model includes an ID-based cryptosystem to assure users’ anonymity using pseudonyms; however the model provides a backdoor for law enforcement authorities to trace misbehaving and suspicious users. In this model, we propose a heuristic that optimizes the pseudonym update process. This heuristic permits vehicles to switch pseudonyms at different times and locations in a way that maximizes the anonymity degree.

Keywords-ID-based cryptosystem; anonymity; traceability; pseudonyms; conditional privacy.

I. INTRODUCTION

Vehicular ad-hoc networks (VANETs), as special applications of Mobile Ad-hoc Networks (MANETs), are targeted to improve road safety and to optimize transportation systems. This emerging technology is not implemented yet but tremendous effort has been spent in this promising area. Moreover, VANETs have been positioned to provide convenient, payment services, and many vehicle-centered applications.

The architecture of a VANET generally consists of wireless communication interfaces known as On-Board-Units (OBUs) installed on vehicles and Road-Side-Units (RSUs) [1] deployed as a part of the VANETs’ infrastructure. The latter’s role is to mediate the communications between the vehicles and the backbone of the network (service providers, certification authorities, etc.).

Transmissions in a wireless medium such as in VANETs can reach all existing nodes (OBUs, RSUs) in a range of few hundred meters. An adversary can breach OBU’s privacy by monitoring the vehicle communications with another vehicle (V2V) or with the infrastructure (V2I). Hence, OBUs are prone to identity or location disclosure. Therefore, privacy arises as a compelling issue that should be considered in any VANET system. To ensure users’ privacy, many models have been suggested towards designing an anonymous system [2]- [5]. Few papers presented privacy systems without relying on pseudonyms [6]- [8]. Such solutions were proposed to overcome the drawbacks of Mix zones [9]- [11] and silent periods [2]. During silent periods, safety messages (beacons) are not sent which may cause serious problems if something urgent happens on the road.

In [8], the authors introduced a new format of a beacon packet that ensures authentication of V2V and V2I with privacy preservation. The proposed beacon format contains parameters calculated based on the private key of the vehicle and on a group key. The group key is assigned randomly by a Trusted Third Party (TTP) to each vehicle entering the network. The main drawback of this proposal is that the TTP is assumed to be trusted. TTP has the ability to get a user’s identity by brute force from the vehicle related identification (VRI). Moreover, the proliferation method to distribute group keys has never been addressed.

Group signature based protocols were presented in several works [12]- [14]. For instance, Lin et al. [12] proposed a group signature based model that allows a vehicle to sign messages anonymously on behalf of the group. However, in the case of a dispute, the identity of a signature’s originator can be revealed by the group manager. Therefore, in this model, anonymity and traceability are achieved. The main advantage of a group enforcement authorities to track the real identities of potential attackers.

The major contribution of this paper is twofold. First, we propose an anonymous system which provides conditional privacy. Second, we propose a heuristic model to optimize the pseudonym update conditions to avoid attacks.

The rest of the paper is organized as follows. In section II, the related work is surveyed. In section III, the design objectives, the system architecture and design components are described. In section IV, we discuss the operation and characteristics of the proposed scheme, then, in section V we introduce a heuristic for optimizing the update process and we conclude in section VI.

II. RELATED WORK

Most proposed solutions for privacy preservation in VANETs did not include a tracking mechanism to prevent inside attacks such as bogus message spoofing attacks, Denial of Service (DoS) attacks, or impersonation attacks. They mainly include pseudonym distribution and update schemes [2]- [5]. Few papers presented privacy systems without relying on pseudonyms [6]- [8]. Such solutions were proposed to overcome the drawbacks of Mix zones [9]- [11] and silent periods [2]. During silent periods, safety messages (beacons) are not sent which may cause serious problems if something urgent happens on the road.

In [8], the authors introduced a new format of a beacon packet that ensures authentication of V2V and V2I with privacy preservation. The proposed beacon format contains parameters calculated based on the private key of the vehicle and on a group key. The group key is assigned randomly by a Trusted Third Party (TTP) to each vehicle entering the network. The main drawback of this proposal is that the TTP is assumed to be trusted. TTP has the ability to get a user’s identity by brute force from the vehicle related identification (VRI). Moreover, the proliferation method to distribute group keys has never been addressed.

Group signature based protocols were presented in several works [12]- [14]. For instance, Lin et al. [12] proposed a group signature based model that allows a vehicle to sign messages anonymously on behalf of the group. However, in the case of a dispute, the identity of a signature’s originator can be revealed by the group manager. Therefore, in this model, anonymity and traceability are achieved. The main advantage of a group
signature based protocol is the minimization of pseudonyms storage on the OBU side which allows the law enforcement authorities to easily trace the target OBU. A drawback of this model is the assumption that the group manager is a trusted authority which may not be the case and hence leading to serious inside attacks.

Existing schemes for pseudonyms generation can be classified, from a cryptographic point of view, into two classes: Public Key Infrastructure (PKI) systems [15]- [20] and ID-based cryptosystems [4] [21]. Although a PKI provides several security services such as authentication, non-repudiation, confidentiality, and privacy, it suffers from a major setback, which is the high computational and storage overhead. In [21], an ID-based cryptosystem was introduced to reduce the overhead of a PKI. The ID-based cryptosystem was first proposed by Shamir [22] who suggested ID-based signatures that can be verified using only public information about a user. Boneh and Franklin [23] proposed an ID-based encryption scheme using the bilinear pairings property of elliptic curves that solves the problem of ID-based Encryption (IBE). In [24], Cocks suggested an ID-based Encryption scheme based on quadratic residues. The main drawback of such scheme is that private keys are generated by a private key generation (PKG) authority which is assumed to be trusted and hence again the scheme is vulnerable to inside attacks. All ID-based cryptosystems which were proposed prior to [21] have a Key Generation Center (KGC) as a trusted authority to distribute private/public keys to OBUs. The KGC generates the user’s private key using its master key. Therefore the KGC has access to these keys which creates a key escrow problem. To address this problem, the authors of [21] 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) generates only the signature value (\( \Gamma \)) given the user’s public key and ID. The V2V and V2I communications include \( \Gamma \), 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. Note that in this design, the RTA is not supposed to store all the previous pseudonyms of a user; it just stores some parameters related to the last used pseudonym, so that the user is verified at the update phase. However, maximizing anonymity level is not addressed when updating pseudonyms. While the above systems took into account the anonymity and traceability aspects in VANETs, they lacked any study of suitable conditions for pseudonyms update.

III. DESIGN MODEL

In this section, the design objectives, system architecture, and design components are presented.

A. Design Objectives

The main objective of this design is to implement an efficient conditional privacy preservation system in VANETs. The system considers the following security and privacy aspects:

1) **Anonymity**: Anonymity is a must to ensure the users’ privacy. From the perspective of the OBUs, it is not acceptable to leak identities, locations or profiles information. Moreover, the proposed mechanism should be efficient in a way to minimize the storage of anonymous keys at the OBU side and to reduce time and computational overhead associated with the updation of the revocation list.

2) **Traceability**: The existence of anonymity raises the importance of a tracking mechanism to protect VANETs from inside attackers. Traceability is also a must to allow law enforcement authorities to identify attackers.

3) **Maximizing Anonymity Level**: Pseudonym-based anonymous systems are helpless against outside attacks where an adversary monitors the network for a large period of time and tries to relate transmissions with approximated physical locations. Therefore, optimality conditions for pseudonym update are essential and hence a heuristic will be proposed to maximize the anonymity level.

B. System Architecture

Figure 1 shows the main components of the system architecture. The OBUs communicate with each other (V2V) or with RSUs (V2I). The RSUs are fixed and connected to each other and to the backbone of the network via wired connections. The CAs are responsible for the registration of OBUs and RSUs. The distribution of CAs is hierarchical; they are distributed over the country and they are coordinated by a Central Certification Authority (CCA). The number of CAs, \( N_{CA} \), is proportional to the number of vehicles.

C. ID-Based Cryptosystem

To overcome the drawbacks of PKI systems such as storage and computational overhead, an ID-based cryptosystem is chosen. In such a system, the sender can just use the receiver’s identity information like name or email address to encrypt a message. The solutions suggested in [23], [25], and [24], despite solving the ID-based Encryption problem, they suffer from several disadvantages: (1) the key escrow problem, (2) the single point of failure problem due to the use of a central trusted PKG, and (3) the large computation and storage overhead. In our cryptosystem, we address all of these problems.

Compared to bilinear pairings ID-based schemes [23] [25], Shamir’s ID-based signature scheme [22] reduces the computational and storage overheads. In the proposed solution, the RSA public/private keys are generated on board. Therefore the key escrow problem is solved. Moreover, the hierarchal distribution of CAs solves the single point of failure problem. Note that RSA public/private keys generation is independent of pseudonym and signature generation. A maximum validation period is defined for the RSA keys which is normally much longer than the pseudonym/signature expiration period. Before expiration of the keys, the user generates a new pair of keys.
the V ANET entities (CAs, RSUs, and OBUs). In this model, all the CAs and publishes the parameters \( N \) as follows:

\[
N = p \cdot q
\]

The CCA generates the parameters \( \Gamma \) in the registration phase, and an update phase. Where \( \Gamma \) refers to the current time. 

Our proposed scheme consists of an initialization phase, a registration phase, and an update phase. 

In the initialization phase, the Central Certificate Authority (CCA) generates the parameters \( N \) and \( e \) and computes \( t \) and \( g \) as follows:

\[
t = r^e \\
g = ID_{CCA}^e
\]

The CCA distributes the secret parameters \( r, g, \) and \( d \) to all the CAs and publishes the parameters \( N, e, t \) and \( g \) to all the VANET entities (CAs, RSUs, and OBUs). In this model, we assume that the CAs network is secure. Every node in the network maintains a list of all the CAs including their IDs, their public keys, and their corresponding regions. Although the CAs are distributed regionally, a vehicle can register with any CA in the network.

In the registration phase, when a vehicle \( x \) wants to register to the VANET network, it selects at random a CA, say \( CA_k \). First, it generates on board its RSA private and public keys. Then it sends its identity along with its public key to \( CA_k \) encrypted with the public key of \( CA_k \):

\[
E_{PK_{CA_k}}(ID_x||PK_x^+)
\]

The \( CA_k \) computes the first pseudonym and the first signature of vehicle \( x \) as follows:

\[
P_{x_1} = h(r||ID_x||PK_x^+||T_{Exp1}||nonce_1)
\]

\[
\Gamma_{x_1} = g \cdot P_{x_1}||PK_x^+||T_{Exp1}\mod(N)
\]

Then, the \( CA_k \) sends a message to vehicle \( x \) including the necessary parameters encrypted using the public key of \( x \):

\[
E_{PK_x^+}(ID_x||P_{x_1}||\Gamma_{x_1}||T_{Exp1}||N||t||e||nonce_1)
\]

Vehicle \( x \) verifies the signature as follows:

\[
(\Gamma_{x_1})^e = ID_{CCA}.h(r||ID_x||PK_x^+||T_{Exp1})\mod(N)
\]

The registration process is shown in Figure 2.

Vehicle \( x \) can update its pseudonym whenever needed and it can do it with the same CA or with any other CA; however, the update has to be done before the expiration of the current signature. Note that the signature validation period is defined with an upper limit in order to prevent replay attacks. When updating from the old pseudonym \( P_{x_{i-1}} \) to the new pseudonym \( P_{x_i} \) with \( CA_k \), vehicle \( x \) sends a message including its identity, its current pseudonym, its current public key, the current time, and a nonce encrypted with its current private key in addition to other necessary parameters as shown below:

\[
M = E_{PK_x^-}(ID_x||P_{x_{i-1}}||PK_x^+||T_{current}||nonce_{i-1})
\]
The CA checks the current time and verifies the signature by decrypting $M$ using $x$’s public key. If successful, it verifies the (i-1) signature and pseudonym by computing those using equations (2) and (3) where the subscript is (i-1) instead of 1. If successful, $CA_k$ generates the $i^{th}$ pseudonym and signature using again equations (2) and (3) where the subscript is i. Then $CA_k$ generates and sends to $x$ a message similar to equation (4) and vehicle $x$ verifies it using equation (5). The pseudonym update process is shown in Figure 3.

The update mechanism benefits from the distributed architecture of CAs; a CA is able to generate the new pseudonym and signature without being the generator of the previous ones. In this model, each CA maintains a table containing the vehicles IDs and the last pseudonym it generated for each of these vehicles along with the update date. Note that this pseudonym is not necessarily the one currently being used by the vehicle as it could have been updated by another CA. Note that there is a special case in the pseudonym update process; when a vehicle $x$ updates its public and private keys and wants to update its pseudonym, it has to send the old public key along with the new one in the update request. The message in equation (6) becomes:

$$M = E_{PK_x}^+ (ID_x||P_{x_{i-1}}||\Gamma_{x_{i-1}}||PK_{x_{i}}||T_{Exp_{i-1}}||T_{current}||M)$$

(7)

The CCA checks if the ID is in the revocation list and if it finds it, it checks if the ID is in the revocation list and if it finds it, the CA blocks the update process and eventually the current pseudonym and signature will expire. Then, each CA sends the current pseudonym of the revoked vehicle to all vehicles in its region. Each vehicle maintains a list of revoked pseudonyms. Thus, a revoked vehicle will not be able to communicate with other vehicles.

V. Heuristic for Pseudonym Update Optimization

None of the proposed privacy systems has addressed the mobility issues during the pseudonym update process. The ID-based cryptosystem preserves the privacy within a VANET network. However, an outside attacker having the ability to observe the network for a sufficient period of time might disclose this privacy. Although the changes in location due to motion and pseudonym update reduce the correlation between the location and the physical identity of a vehicle, such an attacker is capable of making the link even if the time interval between transmission prior to and after the pseudonym update is short [26].

Moreover, in our design, a vehicle is not obliged to update its pseudonym with the CA of the region where it exists; a vehicle can choose any CA to update its pseudonym. In this case, the expression in equation (7) is prepended by the corresponding CA ID. Since the CAs have the ability to know the location of the RSUs that forward the vehicles requests, the update process can be disclosed by the CAs to regionally
track the vehicles. Therefore a heuristic is needed to (1) solve the problem of outside attackers by determining the optimal conditions for pseudonym update and to (2) choose the optimal CA for pseudonym update.

Chaurasia et al. [8] [27] studied the pseudonym update process and determined the conditions and cases to update pseudonyms. In their work, the road is modeled as a set of consecutive clusters. Each cluster contains a set of vehicles and these vehicles are moving from one cluster to the neighboring ones. When a vehicle under observation moves from one cluster to another and changes its pseudonym, it can be spotted with high probability as soon as it transmits. This can happen if the number of vehicles moving from the previous cluster to the current cluster is small and the pseudonyms of vehicles belonging to the current cluster are known a priori.

The anonymity of the vehicle under observation is limited by the cardinality of the anonymity set which is the number of vehicles that join the current cluster from the previous cluster [28] [29]. The degree of anonymity of a vehicle is the inability of the adversary to pinpoint a vehicle as the source of the communication in the set of vehicles V (anonymity set) in the region estimated from the communication. Therefore, the degree of anonymity is a function of the cardinality of the anonymity set. Increasing anonymity is tantamount to increasing the number of vehicles in the intersection set close to the threshold k. The value of k is generally taken as 3 for vehicular networks [27].

The proposed heuristic aims to achieve this objective by changing a pseudonym at a time and place so that the size of the anonymity set becomes sufficiently large to hide the vehicle within a large crowd. This heuristic gives priority to safety messages; if something urgent happens on the road, the pseudonym update process is postponed.

The RSU periodically broadcasts the number of transmitting vehicles in its vicinity. Therefore a moving vehicle Vi can use the RSU broadcast to measure its degree of anonymity. In this case, the anonymity set is equivalent to the vehicles detected by the RSU in its area. The heuristic for pseudonym update is shown below as Algorithm 1. If sufficient time has elapsed, Vi should update its current pseudonym. However, Vi will remain silent until the number of transmitting vehicles is more than k. Usually, the change must be followed by a time delay before the next transmission [27].

In our model, the CAs are not assumed to be trusted. Therefore, the heuristic should decide which CA to choose when pseudonym update is needed. Each vehicle maintains a list of all the CAs. The conditions followed in the heuristic to choose the CA are: (1) the vehicle should not update its pseudonym with the same CA for two or more consecutive times and (2) The CA is selected randomly from the set of remaining CAs.

### VI. Conclusion

We have introduced an optimized conditional privacy protocol which takes into account both inside and outside attacks. In this protocol, the certificate authorities and the RSUs are not considered as trusted parties. The proposed anonymous system uses pseudonyms generated using the ID-based cryptosystem with backdoor for authorities to track misbehaving vehicles. A heuristic was also proposed in order to optimize the anonymity level during the pseudonym update process. This scheme is meant to preserve conditional privacy along with other security services such as authentication, and confidentiality.

### References


