An Effective Scheme for Location Privacy in VANETs

Shi Xingjun
School of Economy & Trade, Zhejiang Industry & Trade Vocational College, wenzhou325003, China

Xu Huibin
Shanghai Normal University Tian-Hua College, Shanghai 201815, China

Abstract—Location privacy is an important concern in VANETs (Vehicular Ad hoc Networks). Anonymity is one of commonly adopted solution to protect location privacy. In this paper, we present a mechanism based on an ID-based cryptosystem in order to ensure vehicles’ anonymity by pseudonyms. In this mechanism, we adopt Pseudonyms Synchronously Change (PSC) scheme, which improves anonymity. In the schemes, vehicles change pseudonym at different times and locations. Simulation result demonstrates our schemes have superior performance on location privacy preservation.

Index Terms—ID-Based; Pseudonyms; Location Privacy; VANETs; Cryptosystem

I. INTRODUCTION

Enhancing vehicular safety, improving traffic management and facilitating other online services are some of the benefits that motivate research on Vehicular Ad-hoc Networks (VANETs). Since that these applications close to our daily lives, the government and academia have kept a watchful eye on VANETs [1]. In VANETs, each vehicle is equipped with an onboard unit (OBU) communication device, which allows vehicles to not only V2V (vehicle-to-vehicle) communication, but also V2I (vehicle-to-infrastructure) communication. RSU (road side units) is one of infrastructures. In addition, vehicles can access the remote services on the road by RSUs, which serve as the service gateways. A typical VANETs topological structure is shown as Fig 1.

Figure 1. A typical communication scenarios in VANETs

In VANETs, majority of these applications rely on vehicular status and time information, including velocity, position and direction, time that message generated, then each vehicle need to periodically broadcast its status to its neighbors [2]. Due to open wireless structure, information is divulged. Moreover, some adversaries eavesdropped other vehicles private information by tracking vehicles and monitoring the vehicle communications with V2V or V2I. Therefore, protecting privacy is a compelling issue that must be taken into account in VANETs.

To protect vehicle’s privacy, much research work had been done. In [3], the author designs an anonymous system. Frequently changing pseudonyms is accepted solution to hide the vehicle’s identity while keep communication with another vehicle. Although anonymous communication by pseudonym is typically used to prevent location and identity tracking, it may provide an avenue for misbehavior. Some malicious vehicles could benefit from anonymity to escape responsibility and investigation. For this reason, non-repudiation and traceability are a must to allow law enforcement authorities to investigation and find out the real identities of potential attackers, who take corresponding responsibility. An anonymous system with non-repudiation and traceability could provide conditional privacy [4].

In [5], the authors proposed a scheme by comparing the expected and actual trajectory to decide if a vehicle is sending the correct post crash notification (PCN) alert. The expected trajectory has been modeled using node’s possible behavior. For example, a lazy node might not take any action until it is very close to the site of crash. On the other hand a risk-averse node might move away very far from the site of crash. There are three aspects to be noted: the modeling of expected trajectory, the reported position of the node and the actual position of the node. However, the scheme is based on the assumption that a vehicle always sends a valid location information. It is unreasonable since that the vehicles might send wrong location information and compel other vehicles to believe that their trajectory is what is expected. Even a small change in position can make a huge difference, for example lane change.

To achieve location privacy, a common approach that vehicles periodically change their pseudonyms in VANETs when vehicles communicate with others. Vehicles broadcast safety messages, including velocity,
time, location of vehicle, and is authenticated with a signature with respect to a pseudonym. The unlinkability of pseudonyms from the same vehicle is able to achieve the vehicle’s location privacy since that vehicle communicates with other vehicles in different pseudonyms.

However, if a vehicle changes its pseudonyms in an improper time or region, the approach by changing pseudonyms cannot effectively protect location privacy, the reason is that there is linkable between new pseudonym and old pseudonym from the same vehicle.

As shown in example in Fig. 2, assume that three vehicles are running on the road. During $\Delta t$, if only one vehicle solely changes its pseudonyms, an adversary is still able to ratiocinate the link between old pseudonyms and new pseudonyms.

Figure 2. Pseudonyms link due to changing pseudonyms in improper time

Therefore, it is necessary to design the effective location privacy that is guaranteed by frequently changing pseudonyms in VANETs. In order to achieve high quality location privacy, a vehicle should choose a proper time or region, where pseudonym is changed.

The major contribution of this paper is twofold. First, a mechanism based on an ID-based cryptosystem is proposed, and it provides conditional privacy. Second, we adopt Pseudonyms Synchronously Change (PSC) scheme and it improves anonymity.

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 PSC scheme, for optimizing the update process, then in section V, we analyzes the feasibility of scheme. In final, conclusion is presented in section VI.

II. RELATED WORK

There have been lots of prior efforts on location privacy preservation in VANETs. For various attacks, most corresponding pseudonym generation and update solutions are proposed.

There are a few existing pseudonyms generation solutions. For a cryptographic perspective, these solutions can be classified into two classes. First class is the Public Key Infrastructure (PKI) systems [6-7]. PKI system can provides several security services such as authentication, non-repudiation, confidentiality, and privacy, however, it has some deficiency, such as high computational and storage overhead. For this, ID-based cryptosystem [3][8] is proposed to lower the system overhead, which belongs to the second class. The ID-based cryptosystem use the identity information to signatures, which can be verified by only public information about a user. However, there is a key escrow problem in ID-based cryptosystem.

In location-based schemes, a user may want to retrieve location-based data without revealing her location. For the purpose, techniques such as $k$-anonymity [9] and private information retrieval [10] is proposed. In [11], Deng proposed a technique to protect the locations privacy from a local eavesdropper by hashing the ID field in the packet header. Moreover, in [12], it was shown that an adversary is able to monitor the location privacy by time correlation and rate monitoring attacks.

In [13], the global-adversary-based scheme is proposed to protect location privacy. The scheme assumes that adversaries are able to monitor the traffic of the entire network. Each vehicle must periodically send packets, and send dummy packets if it does not have sensed data so that it is infeasible for the adversaries to distinguish between the real and dummy packets.

In update pseudonyms process, a few prior efforts are spent. In [14], Gerlach proposes context mix scheme. In the scheme, a vehicle permanently assesses its neighborhood and changes its pseudonyms only if the vehicle detect $m$ vehicle with a similar direction in a confusion radius.

In [15], considering the needs required by VANETs, the mix-zone concept is proposed because that mix-zones are anonymizing regions, where vehicles change their identifiers in order to obfuscate location tracking attacks from adversary. In [16], vehicular density-based location privacy scheme is analyzed to address attacks that correlate pseudonyms of vehicles entering and exiting a mix-zone. Only when a vehicle finds a threshold number of vehicles within its region, the vehicle must change its pseudonym.

In [17], shao proposes a notion of statistically strong anonymity in wireless sensor networks to provide location privacy against traffic analysis attacks through dynamic anonymous authentication. In [18], L. Huang et al. propose an approach of using a random silent period between update of pseudonyms. In [19], J.Liao et al. propose a synchronous pseudonym change scheme. In the scheme, a wait flag in beacon is used to improve the probability of changing pseudonyms simultaneously.

III. MECHANISM PRESENTATION

In this section, we formalize the network structure and identify our design goals. Moreover, the ID-based cryptosystem are presented.

Figure 3. Network structure
A. Network Structure
The RSUs are the backbone of the network in wired way, which are fixed and connected to each other. We assume that the RSUs are credible, which are responsible for the registration of vehicles. They are managed and coordinated by a Certification Authority (CA). The network structure is shown as Fig. 3.

B. Design Goals
Under the aforementioned network structure, our design goal is to establish ID-based cryptosystem providing conditional privacy. Concretely, three desirable objectives should be achieved.

Anonymity: Anonymity is a necessity to protect the vehicle’s privacy. For a vehicle, it is not acceptable to reveal privacy information, such as identities, locations and direction etc. In addition, to minimize the storage of anonymous keys in vehicle side and reduce time and computational burden while keeping anonymity.

Aon-repudiation and traceability: non-repudiation and traceability are a must to allow regulatory agencies to investigate and winkle the corresponding facts.

Improving anonymity: for outside attack, pseudonym-based anonymous scheme is not effective since adversary tries to link eavesdropping communicated message with approximated physical locations by monitoring the network for a large period of time. Therefore, we proposed PSC scheme to optimize pseudonym update process and maximize the anonymity level.

C. ID-based Cryptosystem
1) System Initialization
We assume that a CA will bootstrap the whole system. For a single authority VANET under consideration, it is reasonable. Concretely, given the security parameters $r$, $d$ and $N$, $e$, then computes $g$ by running $g = ID_{CA}^e$ and $\gamma = r^e$. Note that, the parameters $e$ and $d$ are an integer and $gcd(e,d) = 1$. In the end, the parameters $g$ and $d$ are distributed to all RSUs. In addition, CA publish parameters $N$ and $e$, $\gamma$ to the VANETs. Each vehicle in the system obtains a list of all the RSUs including their IDs, their public key and their corresponding communication regions. Every vehicle can register with a RSU in the system.

2) Vehicle User Joining
In the vehicle joining scheme, we consider that a vehicle $x$ is moving in the area. When a vehicle $x$ wants to register to the VANETs, it will contact a nearby RSU, e.g. $RSU_i$. First, vehicle generates on board its private and public key by RSA algorithm, which is expressed as $PR_x$, $PU_x$, respectively. Then it transfers its personal information to $RSU_i$, including its IDs and public key. The message is encrypted with the public key of $RSU_i$:

$$E_{PU_{RSU_i}}(ID_x \parallel PU_x) \rightarrow RSU_i,$$  \hfill (1)

After receiving the messages, $RSU_i$ computes the first pseudonym and the first signature of vehicle $x$ as follows:

$$ps_{x}^1 = h(r \parallel ID_x \parallel PU_x \parallel T_{Exp} \parallel timestamp)$$ \hfill (2)

$$\text{sig}_{x}^1 = g \cdot r^{h[ID_x || PU_x || T_{Exp} || timestamp]}$$ \hfill (3)

Then, $RSU_i$ send an encrypted message to a vehicle $x$. The message contains the necessary parameters, which is as follow:

$$E_{PU_x}(ID_x \parallel ps_{x}^1 \parallel \text{sig} \parallel T_{Exp} \parallel N || e \parallel \text{randn})$$ \hfill (4)

where, $\text{randn}$ is a random number. After receiving the message, vehicle $x$ uses its private key to decode and verifies the validity of message by checking the signature $\text{sig}_{x}^1$ with

$$\text{sig}_{x}^1 \uparrow = ID_{CA} \cdot g^{h[ID_x || PU_x || T_{Exp} || timestamp]} \cdot \gamma^{r^{h[ID_x || PU_x || T_{Exp} || timestamp]}}$$ \hfill (5)

If it holds, the message is accepted and registered successfully. The correctness is given as follows:

$$\text{sig}_{x}^1 \uparrow = \left(g \cdot r^{h(ID_x || PU_x || T_{Exp} || timestamp)} \right)^{\gamma \cdot r^{h(ID_x || PU_x || T_{Exp} || timestamp)}}$$ \hfill (6)

The vehicle joining process is as follows:

| Step1: | $x \rightarrow RSU_i$, $E_{PU_x}(ID_x \parallel PU_x)$ |
| Step2: | receiving the message, computer $ps_{x}^1$ and $\text{sig}_{x}^1$ |
| Step3: | $RSU_i \rightarrow x$, $E_{PU_x}(ID_x \parallel ps_{x}^1 \parallel \text{sig} \parallel T_{Exp} \parallel N || e \parallel \text{randn})$ |
| Step4: | verify the signature. If it holds, join successfully |

3) Vehicle Pseudonym Update Process
Vehicle $x$ can update its pseudonym whenever needed and it can do it with the same RSU which it registered in joining process, or with any other nearby RSU. Indeed, the update process has to be done before the expiration of the using signature. When vehicle $x$ need to update its current pseudonym $ps_{x}^1$ by $RSU_i$, it sends an encrypted message, given as:

$$Mes = E_{PU_{RSU_i}}(ID_x \parallel ps_{x}^1 \parallel PU_x \parallel T_{current} \parallel \text{randn})$$ \hfill (7)

where, $ps_{x}^1$ denotes its current pseudonym and $T_{current}$ is current time.

$$E_{PU_{RSU_j}}(ID_x \parallel ps_{x}^1 \parallel \text{sig}_{x}^1 \parallel PU_x \parallel T_{Exp} \parallel T_{current} \parallel Mes)$$ \hfill (8)

After receiving the message, $RSU_j$ checks the current time and verifies the signature by decrypting $Mes$ using the public key of $x$. If it holds, it also checks the signature $\text{sig}_{x}^1$ and the pseudonym $ps_{x}^1$ by computing equations (2) and (3). If it holds, $RSU_j$
calculate the next pseudonym and signature in the same way. Similarly, RSU sends a message to vehicle $x$. Then, next step is similar to the Vehicle User Joining.

**TABLE I.** \textbf{Frequently used notations in the paper}

<table>
<thead>
<tr>
<th>ID$x$</th>
<th>the identity of node $x$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N$</td>
<td>the product of two large prime number</td>
</tr>
<tr>
<td>\text{gcd}(m,n)=1</td>
<td>$m$ is relatively prime to $n$</td>
</tr>
<tr>
<td>$h(t)$</td>
<td>a strong one way hash function</td>
</tr>
<tr>
<td>$ps_x$</td>
<td>Pseudonym of node $x$</td>
</tr>
<tr>
<td>$PR_x$</td>
<td>Private key of node $x$</td>
</tr>
<tr>
<td>$PU_x$</td>
<td>Public key of node $x$</td>
</tr>
<tr>
<td>$Sig_x$</td>
<td>The signature from $x$</td>
</tr>
<tr>
<td>$E_x(t)$</td>
<td>RSA encryption using key $k$</td>
</tr>
<tr>
<td>$T_{exp}$</td>
<td>Signature expiration time</td>
</tr>
<tr>
<td>$T_{current}$</td>
<td>Refers to the current time</td>
</tr>
</tbody>
</table>

**IV. PSC SCHEME**

Although the ID-based cryptosystem protects the privacy within a VANET network, communicated message can be easily eavesdropped by outside attackers with radio range to track vehicles. The privacy information of vehicle is compromised since there is usually a strong correlation between the location of vehicle and the physical identity of vehicle. Pseudonym update is a solution to reduce the correlation, but such efforts are not enough. We must optimize the pseudonym update process to maximize the anonymity. In general, the anonymity of a vehicle is limited by the cardinality of the anonymity set [20], which is the number of vehicles that synchronously change pseudonym. Synchronously change pseudonym can veil judgment so that attacker is inability to pinpoint a vehicle as the source of the communication in anonymity set. The larger the anonymity set, the higher the degree of anonymity of vehicle is. Therefore, increasing the number of vehicles changing their pseudonyms synchronously can strengthen anonymity since increasing the number is tantamount to increasing anonymity. For this reason, the PSC scheme is proposed, which make $k$ neighbors synchronously change pseudonyms, $k$ is the threshold, and $k \geq 1$.

In PSC scheme, if a vehicle have more than or equal to $k$ neighbors, it change pseudonyms. The vehicle sends a requested message and requests its neighbor to change pseudonym together. Therefore the size of the anonymity set becomes sufficiently large to hide the vehicle within a large crowd. Each RSU periodically broadcasts the number of transmitting vehicles in its vicinity. In this case, all vehicles can utilize the broadcast to obtain the number of neighbors. When its neighbors have more than or equal $k$, it send a message to neighbors to request changing synchronously pseudonym. RSU can take the time and place into account so that the size of the anonymity set becomes sufficiently large to hide the vehicle within a large crowd. PSC scheme process is as follows:

**V. PERFORMANCE ANALYSIS**

In this section, the location privacy Feasibility in the PSC scheme is analyzed.

The aforementioned PSC scheme carries out under the assumption that all vehicles synchronously change their pseudonyms. Unfortunately, self-interested vehicle might decide not to change pseudonym. Therefore, we analyze self-interested behavior of vehicle by using a simplified game-theoretic model [21]. In the model, each vehicle aims at maximizing its gain (location privacy) at a minimum cost. It will show the proposed scheme is feasible through analysis. Rational vehicle user is cooperative to change pseudonym to achieve its location privacy. When the number of neighbors is not smaller $k$, it send a requested message.

Assume that the number of neighbors of a vehicle $x$ is denoted by $|NS_x|$. The anonymity set size is also denoted by $|AS|$. $|AS| \leq |NS_x| + 1$. When a neighbor $U_i$ receives a requested message, $1 \leq i \leq |NS_x|$, it has twice choices: a) change the pseudonym together with probability $pr_i$ and b) not change the pseudonym with probability $1 – pr_i$. For the sake of simplicity, the twice choices is denoted by $Yes$, $No$, respectively.

If $U_i$ do not change pseudonym, it will still be tracked with probability 1. The loss of $U_i$’s location privacy is not changed. Let $h_i \in (0,1)$ is the $U_i$’s self-evaluation on the importance of location privacy. That is, if $U_i$ choose $No$, the payoff in this choice is a normalized location privacy loss of $-h_i$.

On the other hand, if $U_i$ accept the request and choose $Yes$ and other neighbors also take the same choice, the $|AS| = |NS_x| + 1$. In this case, $U_i$ is still tracked only with probability $1/|AS|$. The loss of location privacy is lowered to $-h_i/(NS_x + 1)$. Assume that the cost of choosing $No$ is normalized as $h_i$, $h_i \in (0,1)$. Therefore, the payoff in this choice is $-h_i/(NS_x + 1) - h_i$.

Next, we estimate the low bound of the average anonymity. Let $pr_m$ be the minimum of all probabilities, which is given as:

$$pr_m = \min \{ pr_i | 1 \leq i \leq |AS| \}$$

(9)

If $pr_m = 1$, all neighbors change synchronously their pseudonyms. The low bound of the average anonymity set is denoted by $|AS|_{\min}$ [22]:

Step1: Receive the message from the RSU
Step2: if number of neighbors > $k$
then send a request message to neighbor
Step3: else Wait()
\( |AS_{i,v}^{NS}| = \sum_{i=0}^{n_{\text{NS}}} \left( NS_i \right) \cdot pr_m^{n_{\text{NS}}} \cdot (1 - pr_m)^{n_{\text{NS}}-i} \cdot (i+1) = npr_m + 1 \) \( (10) \)

Therefore, the payoff \((Pf)\) function of vehicle \(U_i\) can be summarized as
\[
Pf = \begin{cases} 
-\frac{b}{|NS_i|pr_m + 1} - h, & \text{if Yes is chose} \\
-b, & \text{if No is chose} 
\end{cases}
\]
\( (11) \)

For a rational vehicle, it tries to protect its location privacy. Then it changes synchronously its pseudonym with neighbors together. On those rational vehicles behalf, the condition should be hold, which is given as:
\[
h < \frac{|NS_i|pr_m b}{|NS_i| pr_m + 1}
\]
\( (12) \)

If \( |NS_i| = 0 \), equation (12) does not hold. That is, there is no neighbor vehicle to change synchronously its pseudonym. In this case, \(U_i\) does not also change its pseudonym. If \( |NS_i| \) is larger than 0, \(U_i\) can always reduce the cost \( h\). Therefore, neighbors of vehicle \(x\) can actively choose Yes and change pseudonyms together. We define a function that describing vehicle \(U_i\)'s location privacy gain \((G)\).
\[
G = -\frac{b}{|NS_i| pr_m + 1} - (-h) = \frac{|NS_i|pr_m b}{|NS_i| pr_m + 1}
\]
\( (13) \)

According to equation (13), we know that \(G_i\) is an increasing function in terms of \(pr_m\). In the game-theoretic model, each vehicle tries to maximize its location privacy and improve its \(G\) at a minimum cost. Therefore, when all neighbors change their pseudonyms together, all vehicle benefits from the synchronous action. Based on the above analysis, PSC scheme is feasibility.

VI. SIMULATION RESULTS

In our simulations, 100~200 vehicles are deployed in 3000m*3000m area. The Levy walk mobility model is used in simulation.

In order to evaluate the performance of proposed scheme, we use computation time and location privacy gain to measure the efficiency and effectiveness, respectively. We also compare the proposed scheme with the scheme in [3] and [4].

A. Computation Time

Fig. 4 shows the computation time of the proposed scheme and other schemes. As shown in Fig. 4, the proposed scheme run faster than scheme in [3] and [4], the results show that proposed scheme has smaller amount of computations, high velocity.

B. Location Privacy Gain

Fig. 5 shows the location privacy gain of the proposed scheme and other schemes. As shown in Fig. 5, the proposed scheme outperform scheme in [3] and [4] in term of location privacy gain. The illustrates that the proposed scheme can effectively protect user’s privacy.

VII. CONCLUSION

In this paper, we have proposed an effective scheme to protect location privacy in VANETs. In the pseudonyms generated process, we use the ID-based cryptosystem with conditional privacy that track misbehaving vehicles. In the pseudonyms update process, we propose pseudonyms synchronous change scheme to improve the anonymity size. In addition, we introduced simplified game-theoretic model to analyze the feasibility. In our future work, we will carry out simulation to prove the effectiveness of the PSC scheme in practice.

ACKNOWLEDGMENT

This work was supported by National Natural Science Foundation of China under Grant No. 60972036.

REFERENCE


