Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs

Rongxing Lu, *Member, IEEE*, Xiaodong Lin, *Member, IEEE*, Tom H. Luan,
Xiaohui Liang, *Student Member, IEEE*, and Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*—As a prime target of the quality of privacy in vehicular ad hoc networks (VANETs), location privacy is imperative for VANETs to fully flourish. Although frequent pseudonym changing provides a promising solution for location privacy in VANETs, if the pseudonyms are changed in an improper time or location, such a solution may become invalid. To cope with the issue, in this paper, we present an effective pseudonym changing at social spots (PCS) strategy to achieve the provable location privacy. In particular, we first introduce the social spots where several vehicles may gather, e.g., a road intersection when the traffic light turns red or a free parking lot near a shopping mall. By taking the anonymity set size as the location privacy metric, we then develop two anonymity set analytic models to quantitatively investigate the location privacy that is achieved by the PCS strategy. In addition, we use game-theoretic techniques to prove the feasibility of the PCS strategy in practice. Extensive performance evaluations are conducted to demonstrate that better location privacy can be achieved when a vehicle changes its pseudonyms at some highly social spots and that the proposed PCS strategy can assist vehicles to intelligently change their pseudonyms at the right moment and place.**

***Index Terms*—Location privacy, security, social spots, vehicular ad hoc networks (VANETs).**

I. Introduction

THE continuing advances of vehicular ad hoc networks (VANETs) have elevated the intelligent transportation systems (ITSs) to higher levels and also made vehicle telematics more attractive to the public. In VANETs, each vehicle is equipped with an onboard unit (OBU) communication device, which allows them to communicate not only with each other, i.e., vehicle-to-vehicle (V2V) communications, but with roadside units (RSUs), e.g., vehicle-to-roadside (V2R) communication, as well [1], [2]. Due to this hybrid architecture of VANETs, a variety of promising applications, ranging from safety (e.g., emergence reporting and collision warning) to nonsafety (e.g., infotainment), can be enabled to improve the road safety and better driving experiences. For example, vehicles that are equipped with sensors and Global Positioning System (GPS) devices can monitor road surface conditions, detect potholes on the road [3], and then send the detected pothole warnings to the local road maintenance authority through V2V and V2R communications. Then, repair crews can be dispatched to fix the streets potholes, and at the same time, alerts are disseminated within the certain area where potholes are found. As a result, any approaching drivers can drive with caution and avoid the unnecessary risk of hitting a pothole.

Although VANETs can benefit us with rich applications on the road, the flourish of VANETs still hinges up fully understanding and managing the challenges that concerns the public, e.g., the location privacy, which is one of the fundamental quality of privacies (QoPs)[1] in VANETs [5]. Because VANETs are usually implemented in civilian scenarios, where the locations of vehicles are tightly related to the citizens who drive the vehicles, if a VANET discloses any privacy information of citizens, e.g., location privacy, it cannot widely be accepted by the public. Therefore, to provide guaranteed location privacy to citizens is a must for the wide acceptance of VANETs to the public.

To achieve location privacy, a popular approach that is recommended in VANETs is that vehicles periodically change their pseudonyms when they broadcast *safety messages*, where each *safety message* is a 4-tuple, including `Time`, `Location`, `Velocity`, `Content`, and is authenticated with a `Signature` with respect to a `Pseudonym` [6]–[8]. Because a vehicle uses different pseudonyms on the road, the *unlinkability* of pseudonyms can guarantee a vehicle's location privacy. However, if a vehicle changes its pseudonyms in an improper occasion, changing pseudonyms has no use to protect location privacy, because an adversary could still link a new pseudonym with the old one [9]. As shown in the example in Fig. 1, when three vehicles are running on the road, if only one vehicle changes its pseudonyms during Δt, an adversary can still monitor the pseudonyms' link. Although all three vehicles simultaneously change their pseudonyms, the `Location` and `Velocity` information embedded in *safety messages* could still provide a clue to the adversary to link the pseudonyms, making the privacy protection fail. Therefore, it is imperative for us to exploit the accuracy of location privacy that is achieved by frequently changing pseudonyms in VANETs [10]–[15]. Formally,

[1] QoP in VANETs is analogous to the quality of service (QoS) [4]. It describes the privacy level that a vehicle can achieve in VANETs.

Manuscript received January 30, 2011; revised June 17, 2011; accepted July 9, 2011. Date of publication July 25, 2011; date of current version January 20, 2012. This work was supported in part by the Ontario Research Fund for Research Excellence, Canada. This paper was presented in part at the 2011 IEEE International Conference on Communications. The review of this paper was coordinated by Dr. T. Zhang.

R. Lu, T. H. Luan, X. Liang, and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: rxlu@bbcr.uwaterloo.ca; hluan@bbcr.uwaterloo.ca; x27liang@bbcr.uwaterloo.ca; xshen@bbcr.uwaterloo.ca).

X. Lin is with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON L1H 7K4, Canada (e-mail: Xiaodong.Lin@uoit.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2011.2162864

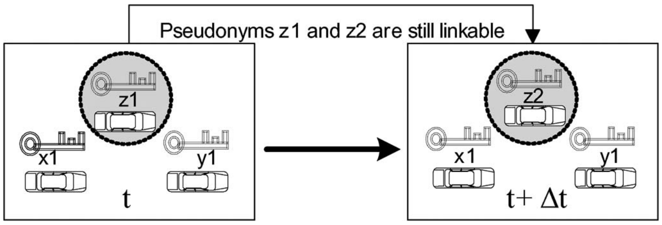


Fig. 1. Pseudonyms link due to changing pseudonyms at an improper occasion.

we let $\overrightarrow{F} = \{F_1, F_2, F_3, \ldots\}$ be multidimensional character factors that are associated with a pseudonym changing (PC) process. For example, the vector $\overrightarrow{F} = \{F_1, F_2, F_3, \ldots\}$ can represent factors $\{\texttt{Time}, \texttt{Location}, \text{and } \texttt{Velocity}$. In some specific scenarios, an adversary can monitor a subset $\overrightarrow{F}_n = \{F_1, F_2, \ldots, F_n\} \subset \overrightarrow{F}$ and use it for identifying a vehicle PC process. Let $\overrightarrow{b}_0 = (x_1, x_2, \ldots, x_n)$ and $\overrightarrow{b}_1 = (y_1, y_2, \ldots, y_n)$ be the character vectors of two vehicles' PC processes observed by an adversary. Then, the cosine-based similarity between $\overrightarrow{b}_0$ and $\overrightarrow{b}_1$ can be given by

$$\cos(\overrightarrow{b}_0, \overrightarrow{b}_1) = \frac{\overrightarrow{b}_0 \odot \overrightarrow{b}_0}{|\overrightarrow{b}_0| \cdot |\overrightarrow{b}_1|} = \frac{\sum_{i=1}^{n} x_i \cdot y_i}{\sqrt{\sum_{i=1}^{n} x_i^2} \cdot \sqrt{\sum_{i=1}^{n} y_i^2}}.$$

Obviously, when $\overrightarrow{b}_0$ and $\overrightarrow{b}_1$ are identical, $\cos(\overrightarrow{b}_0, \overrightarrow{b}_1) = 1$. Due to the monitoring inaccuracy, if $|1 - \cos(\overrightarrow{b}_0, \overrightarrow{b}_1)| \leq \epsilon$, for some small confusion value $\epsilon > 0$, two PC processes can be regarded as indistinguishable to the adversary. Therefore, to protect location privacy with high quality, a vehicle should choose a proper scenario, whereas as many as possible indistinguishable PC processes simultaneously take place.

In this paper, to facilitate vehicles to achieve high-level location privacy in VANETs, we propose an effective pseudonym changing at social spots (PCS) strategy. In the PCS strategy, the social spots are the places where several vehicles temporarily gather, e.g., the road intersection when the traffic light turns red or a free parking lot near a shopping mall. If all vehicles change their pseudonyms before leaving the spot, the first *safety message* that is broadcast includes indistinguishable information $\texttt{Location} =$ social spot, $\texttt{Velocity} = 0$, and unlinkable $\texttt{Pseudonym}$. Then, the social spot naturally becomes a *mix zone*, and the location privacy can be achieved. In particular, in this paper, our contributions are threefold.

First, we utilize the unique feature of social spots, i.e., several vehicles temporarily stop at the social spot, to propose the PCS strategy. In addition, as an important technical preliminary of the PCS strategy, we present a practical key-insulated pseudonym self-delegation (KPSD) model, which securely generates several on-demand short-life keys and can mitigate the hazards due to vehicle theft.

Second, we take the anonymity set size (ASS) as the privacy metric (the larger the ASS, the higher the anonymity achieved [9], [16]) to measure the QoP that is achieved in the PCS strategy. To our best knowledge, most previously reported schemes [9], [15] use the simulations to gauge the achieved location privacy in VANETs, and thus, our anonymity set analytic models will shed light on this research line.

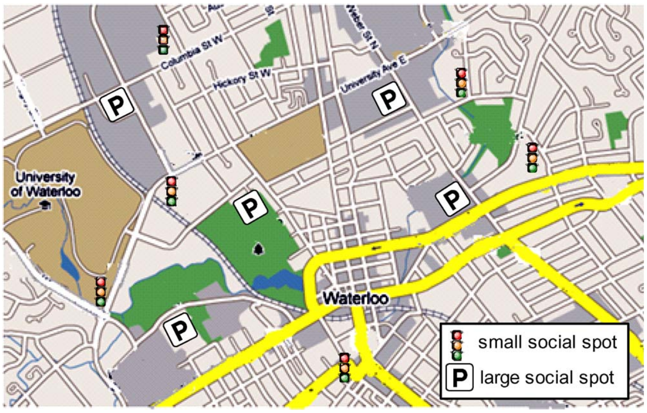


Fig. 2. Social spots, including the road intersection when the traffic light turns red and free parking lots near the shopping mall.

Third, to guarantee that the PCS strategy can effectively be adopted in practice, we use the simplified game-theoretic techniques to formally prove the feasibility of the PCS strategy. As a result, the PCS strategy can really guide vehicles to intelligently change their pseudonyms for better location privacy at the right moment and place.

The remainder of this paper is organized as follows. In Section II, we formalize the problem by describing the network and the threat models and identifying the requirements of location privacy in VANETs. Then, we present the PCS strategy in Section III, followed by the performance evaluations in Section IV. We also review some related work in Section V. Finally, we draw our conclusions in Section VI.

II. Problem Definition

In this section, we define the problem by formalizing the network and the threat models and identifying the requirements of location privacy in VANETs.

A. Network Model

We consider VANET in the urban area, which consists of a large number of vehicles and a collection of social spots[2] as follows.

- *Vehicles*. In urban areas, a large number of vehicles are on the road every day. Each vehicle is equipped with an OBU device, which allows the vehicle to communicate with other vehicles to share local traffic information to make driving conditions more safe.
- *Social spots*. The social spots in the urban area refer to the places where several vehicles gather, e.g., a road intersection when the traffic light is red or a free parking lot near the shopping mall, as shown in Fig. 2. Because the session of a red traffic light is typically short, (i.e., 30 or 60 s), the road intersection is called a *small social spot*. Because a shopping mall usually operates for a whole day, indicating that a number of customers' vehicles will

[2] We confine our problem to pseudonym changing in the V2V communication mode and do not include RSUs in the current network model, although RSUs are still deployed to support V2R communication in the urban area.

stop at the parking lot for a long period, the free parking lot near the mall is hence called a *large social spot*. Note that, because social spots usually hold many vehicles, if all vehicles indistinguishably change their pseudonyms in the spots, the social spots naturally become *mix zones*.

B. Threat Model

Unlike other wireless communication devices, the OBU devices equipped on the vehicles cannot be switched off once vehicles are running on the road [17]. Then, an eavesdropper, through the *safety messages* that are broadcast by the OBU, can monitor the location information of a specific vehicle at all times. Concretely, in our threat model, we consider a global external adversary $\mathcal{A}$ that is equipped with radio devices to trace the vehicles' locations, where the following two conditions hold.

- *Global* means that the adversary $\mathcal{A}$ can monitor and collect all *safety messages* in the network with radio devices plus some special eavesdropping infrastructure mentioned in [15], where each safety message includes `Time`, `Location`, `Velocity`, `Content`, and `Pseudonym`. Because `Pseudonym` is unlinkable and `Content` could be set as irrelevant, the adversary $\mathcal{A}$ primarily tracks a vehicle in terms of `Time`, `Location`, and `Velocity`, i.e., in a spatial–temporal way in our model.
- *External* denotes that the adversary $\mathcal{A}$ can only passively eavesdrop the communications but does not actively attempt to compromise the running vehicles.

Note that an adversary $\mathcal{A}$ of course can track vehicles by using cameras in the urban area. However, the cost of *global* eavesdropping with cameras is much higher than radio-based eavesdropping [15]. Therefore, camera-based global eavesdropping is beyond the scope of this paper.

C. Location Privacy Requirements

To resist the global external adversary's tracking and achieve location privacy in VANETs, the following requirements must be satisfied.

- *R-1*. Identity privacy is a prerequisite for the success of location privacy. Therefore, each vehicle should use a pseudonym in place of a real identity to broadcast messages. Then, by concealing the real identity, the identity privacy can be achieved.
- *R-2*. Each vehicle should also periodically change its pseudonyms to cut down the relation between the former and the latter locations. In addition, the PC should be performed at the appropriate time and location to ensure that the location privacy is achieved.
- *R-3*. Location privacy should be *conditional* in VANETs. If a broadcast *safety message* is in dispute, the trusted authority (TA) can disclose the real identity, i.e., the TA can determine the location where a specific vehicle broadcast a disputed *safety message*.

Recall that the social spots can naturally serve as *mix zones*. In the following section, we explore this feature and propose the PCS strategy for achieving location privacy in VANETs.

III. Proposed Pseudonym Changing at Social Spots Strategy for Location Privacy

In this section, we present our PCS strategy for achieving location privacy in VANETs. In particular, we develop two anonymity set analytic models to investigate the location privacy level that is achieved in the PCS strategy and use simplified game-theoretic techniques to discuss the feasibility of the PCS strategy. Before delving into the details of the PCS strategy, we first present a practical KPSD model, which securely generates several on-demand short-life keys and serves as the basis of the proposed PCS strategy.

A. KPSD Model for the PCS Strategy

To support the PCS strategy, a vehicle must hold a certain amount of pseudonyms. In [6], a simple straightforward solution is proposed, where an OBU device equipped on a vehicle possesses a large number of anonymous short-time keys that are authorized by a TA. Obviously, this solution can achieve conditional location privacy when periodically changing the pseudonyms. However, it may take a large storage space to store these short-time keys in OBU device. GSIS [18] is a group-signature-based (GSB) technique that can achieve conditional location privacy without PC. However, the pure group signature verification is usually time consuming, which may be not suitable for some time-stringent VANET applications. Efficient conditional privacy preservation (ECPP) [5] is another anonymous authentication technique that combines group and ordinary signatures. In ECPP, when a legal vehicle passes by an RSU, the RSU will authorize a GSB short-life anonymous certificate to the vehicle. Then, the vehicle can use it to sign messages with ordinary signature techniques [19]. Upon receiving a signed message, anyone can verify the authenticity of message by checking both the anonymous certificate and the message signature. Note that, when vehicle signs several messages, any verifier only needs to execute one group signature verification operation on the certificate; thus, it is more efficient than GSIS. Similar to ECPP, Calandriello *et al.* [20], inspired by the idea of pseudonymous public key infrastructure (PKI) for ubiquitous computing [21], also combine group signature and ordinary signature techniques to achieve anonymous authentication in VANETs. Because the short-life anonymous certificate is generated by the vehicle itself, their scheme is very flexible. However, once a vehicle is stolen, the vehicle thief can arbitrarily generate valid short-life anonymous certificates before being detected. Then, the potential hazards could be large. To mitigate such negative affects, we propose a practical KPSD model.

As shown in Fig. 3, in the KPSD model, the TA does not directly preload authorized anonymous key to the vehicle; instead, it provides the authorized anonymous key to the user—the owner of the vehicle. The user usually stores the authorized anonymous key in a secure environment, i.e., at home. When he/she is ready to go out for a travel, e.g., fueling enough gasoline, he/she first generates required self-delegated short-life keys and installs them in the OBU device. Then, when the vehicle is running in the urban area, these short-life

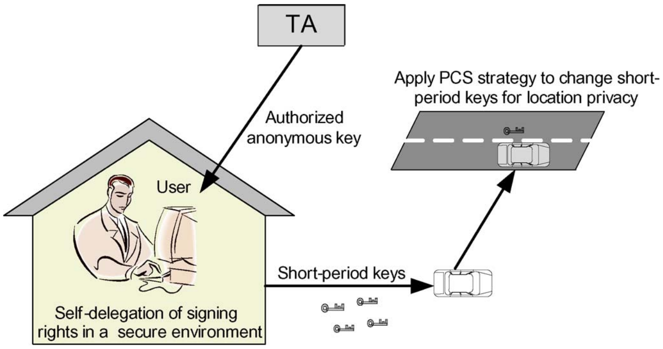

TA
Apply PCS strategy to change short-period keys for location privacy
Authorized anonymous key
User
Short-period keys
Self-delegation of signing rights in a secure environment

Fig. 3. Practical KPSD model for location privacy in VANETs.

keys can be used to sign messages. Because vehicle theft is still currently a serious concern (for example, statistics show that there have been more than 170 000 vehicles stolen each year in Canada [22]), these short-life keys could be abused by the thieves once the vehicle is stolen. However, different from previous works [5], [6], [18], [20], the authorized anonymous key in the KPSD model is not stored in the vehicle. Thus, the vehicle thieves cannot generate more short-life keys. As a result, the hazards due to vehicle theft can be mitigated in the KPSD model. Note that, if the authorized anonymous key is protected by a password-based tamper-proof device, the scheme of Calandriello *et al.* [20] can fall into our KPSD model, but the cost will accordingly increase.

In the following discussion, we construct an efficient KPSD scheme with bilinear pairing techniques [23], which serves as the basis of the PCS strategy.

1) Construction: Our proposed KPSD scheme is based on the Boneh–Boyen short signature [24] and the conditional privacy preservation authentication technology [5], [25], which mainly consists of the following four parts: system initialization; key generation; pseudonym self-delegated generation; and conditional tracking.

System initialization: Similar to the notations used in [23], let $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ be three (multiplicative) cyclic groups of the same large prime order q. Suppose that $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ are equipped with a pairing, i.e., a nondegenerated efficiently computable bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ such that $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab} \in \mathbb{G}_T$ for all $a, b \in \mathbb{Z}_q^*$ and any $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$. We denote by ψ the isomorphism from $\mathbb{G}_2$ onto $\mathbb{G}_1$, which we assume to be one way (easy to compute but hard to invert). The TA first chooses two random numbers u, $v \in \mathbb{Z}_q^*$ as the *master key* and computes $U_1 = {g_1}^u, U_2 = {g_2}^u$, and $V_1 = {g_1}^v$. In addition, the TA chooses a public collision-resistant hash function: $H : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$. In the end, the TA publishes the system parameters $params = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2, U_1, U_2, V_1, H)$.

Key generation: When a user $\mathcal{U}_i$ with identity ID_i joins the system, the TA first chooses a random number $s_i \in \mathbb{Z}_q^*$ such that $s_i + u \neq 0 \bmod q$ and computes $A_i = g_1^{1/s_i+u}$. Then, the TA stores (ID_i, A_i^u) in the tracking list and returns $ASK_i = (s_i, A_i = g_1^{1/s_i+u})$ as the authorized anonymous key to the user.

Pseudonym self-delegated generation: After receiving the authorized anonymous key ASK_i, $\mathcal{U}_i$ places it in a secure environment (e.g., at home). When $\mathcal{U}_i$ starts to travel in the city, he/she first runs the following steps to generate the required anonymous short-life keys used for the travel, which is analogous to the fueling of a vehicle before a travel.

1) $\mathcal{U}_i$ first chooses l random numbers $x_1, x_2, \ldots, x_l \in \mathbb{Z}_n^*$ as the short-life private keys and computes the corresponding public keys $Y_j = g^{x_j}$ for $j = 1, 2, \ldots, l$ for the travel.
2) For each short-life public key $Y_j, \mathcal{U}_i$ computes the anonymous self-delegated certificate $Cert_j$ as follows:
   - Randomly choose α, r_α, r_x, and $r_\delta \in \mathbb{Z}_q^*$, and compute T_U, T_V, δ, δ_1, δ_2, and δ_3, where

$$\begin{cases} T_U = {U_1}^\alpha, T_V = A_i \cdot V_1^\alpha \quad \delta = \alpha \cdot x_i \bmod q \\ \delta_1 = {U_1}^{r_\alpha} \quad \delta_2 = T_U^{r_x} / {U_1}^{r_\delta} \\ \delta_3 = e\left(T_V, {g_2}^{r_x}\right) / e\left(V_1, {U_2}^{r_\alpha \cdot {g_2}^{r_\delta}}\right). \end{cases} \tag{1}$$

   - Compute $c = H(U_1 \| V_1 \| Y_j \| T_U \| T_V \| \delta_1 \| \delta_2 \| \delta_3)$, as well as s_α, s_x, and $s_\delta \in \mathbb{Z}_q^*$, where

$$\begin{cases} s_\alpha = r_\alpha + c \cdot \alpha \bmod q \\ s_x = r_x + c \cdot x_i \bmod q \\ s_\delta = r_\delta + c \cdot \delta \bmod q. \end{cases} \tag{2}$$

   - Set $Cert_j = \{Y_j \| T_U \| T_V \| c \| s_\alpha \| s_x \| s_\delta\}$ as the certificate.
3) After all anonymous self-delegated certificates $Cert_j$, $j = 1, 2, \ldots, l$, have been generated, $\mathcal{U}_i$ installs them to the vehicle, i.e., implanting all $x_j \| Y_j \| Cert_j$, $j = 1, 2, \ldots, l$, into the OBU device.

THEN, when $\mathcal{U}_i$ drives the vehicle in the city, he/she can use one short-life key $x_j \| Y_j \| Cert_j$ to authenticate a message M by signing $\sigma = {g_2}^{1/x_j+H(M)}$ and broadcast

$$msg = (M \| \sigma \| Y_j \| Cert_j). \tag{3}$$

Upon receiving $msg = (M \| \sigma \| Y_j \| Cert_j)$, everyone can check the validity as follows.

1) If the certificate $Y_j \| Cert_j$ has not been checked, the verifier first computes

$$\begin{cases} \delta_1' = U_1^{s_\alpha} / {T_U}^c \\ \delta_2' = {T_U}^{s_x} / U_1^{s_\delta} \\ \delta_3' = \frac{e(T_V, {g_2}^{s_x} \cdot {U_2}^c)}{e(V_1, {U_2}^{s_\alpha} \cdot {g_2}^{s_\delta}) e(g_1, {g_2}^c)} \end{cases} \tag{4}$$

   and checks whether

$$c = H\left(U_1 \| V_1 \| Y_j \| T_U \| T_V \| \delta_1' \| \delta_2' \| \delta_3'\right). \tag{5}$$

   If it holds, the certificate $Y_j \| Cert_j$ passes the verification. The corrections are given as follows: 1) $\delta_1' = U_1^{s_\alpha} / T_U^c = U_1^{r_\alpha + c \cdot \alpha} / U_1^{c \cdot \alpha} = \delta_1$; 2) $\delta_2' = T_U^{s_x} / U_1^{s_\delta} = T_U^{r_x + c x_i} / U_1^{r_\delta + c\delta} = \delta_2$; and 3) $\delta_3' = e(T_V, {g_2}^{s_x} \cdot {U_2}^c) / e(V_1, {U_2}^{s_\alpha} \cdot {g_2}^{s_\delta}) e(g_1, {g_2}^c) = e(T_V, {g_2}^{r_x}) / e(V_1, {U_2}^{r_\alpha} \cdot {g_2}^{r_\delta}) = \delta_3$.
2) Once the certificate $Y_j \| Cert_j$ has passed the verification, the verifier checks

$$e\left(Y_j \cdot {g_1}^{H(M)}, \sigma\right) \overset{?}{=} e(g_1, g_2). \tag{6}$$

   If it holds, the message M is accepted; otherwise, M is rejected, because $e(Y_j \cdot {g_1}^{H(M)}, \sigma) = e(g_1^{x_j + H(M)}, {g_2}^{1/x_j + H(M)}) = e(g_1, g_2)$. Note that the value of $e(g_1, g_2)$ can be precomputed.

Conditional tracking: Once an accepted message M under the certificate

$$Cert_j = \{Y_j \| T_U \| T_V \| c \| s_\alpha \| s_x \| s_\delta\}$$

has been disputed, the TA uses the master key (u, v) to compute

$$T_V^u / T_U^v = A_i^u \cdot V_1^{u\alpha} / U_1^{v\alpha} = A_i^u \cdot g^{uv\alpha} / g^{uv\alpha} = A_i^u \tag{7}$$

and can then efficiently trace the real identity ID_i by looking up the entry (ID_i, A_i^u) in the tracking list.

2) Security: Because both the short signature [24] and the conditional privacy preservation authentication [5] are secure, the security of the proposed KPSD scheme can be guaranteed, i.e., it can effectively achieve anonymous authentication with conditional tracking to fulfill the requirements of location privacy. In addition, the proposed KPSD scheme can mitigate the hazards due to vehicle theft, because the authorized anonymous key ASK_i is *key insulated*, i.e., it is stored in a secure environment; then, vehicle thieves cannot obtain ASK_i from the stolen vehicle and, consequently, cannot arbitrarily generate new self-delegated short-life keys.

3) Performance: In VANETs, it is a very challenging issue for a vehicle to verify too many signed messages in a stringent time, e.g., within 300 ms. Let $T_{\texttt{pair}}$, $T_{\texttt{exp-1}}$, and $T_{\texttt{exp-2}}$ be the time costs for pairing operation and exponentiation in $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. Then, to check n messages from the same source, where $n \geq 1$, the verification cost of the proposed KPSD anonymous authentication and the pure GSB anonymous authentication is $(3+n)T_{\texttt{pair}} + (4+n)T_{\texttt{exp-1}} + 5T_{\texttt{exp-2}}$ and $3nT_{\texttt{pair}} + 4nT_{\texttt{exp-1}} + 5nT_{\texttt{exp-2}}$, respectively. Because $T_{\texttt{pair}}$ is dominant over $T_{\texttt{exp-1}}$ and $T_{\texttt{exp-2}}$, we set $T_{\texttt{pair}}$ as 4.5 ms as in [5] and make the comparison in Fig. 4. Clearly, it is shown that, when n is large, the proposed anonymous authentication is much more efficient than the pure GSB anonymous authentication.

```
Algorithm 1: PCS strategy.
procedure PCS STRATEGY
    Case 1: Small social spot.
        A vehicle $V_i$ stops at a road intersection when the traffic light turns red. When the traffic light turns to green, $V_i$ changes its pseudonym.
    Case 2: Large social spot.
        A vehicle $V_i$ stops at a free parking lot near a shopping mall. When leaving the parking lot, $V_i$ changes its pseudonym.
end procedure
```

B. Anonymity Set Analysis for the Achieved Location Privacy

With the aforementioned KPSD scheme, each vehicle can hold a number of pseudonyms on the road; then, it can apply the PCS strategy, as shown in Algorithm 1, to protect its location privacy. To gauge the benefits from the PCS strategy, we next develop two anonymity set analytic models to investigate the location privacy that is achieved in small and large social spots, respectively.

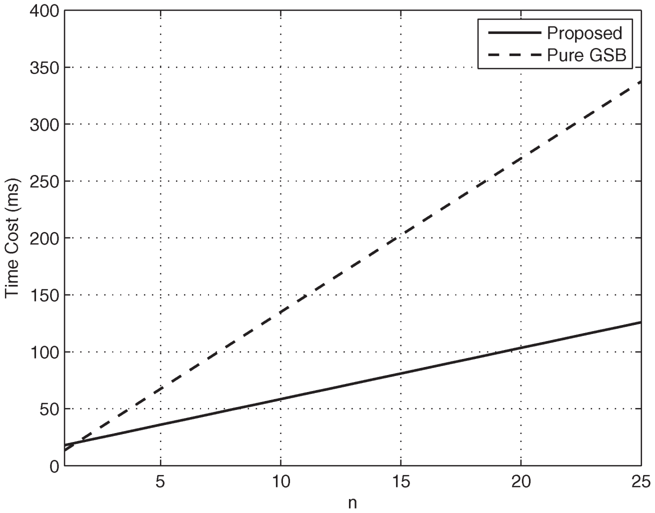


Fig. 4. Time cost comparison between the proposed anonymous authentication and the pure GSB anonymous authentication.

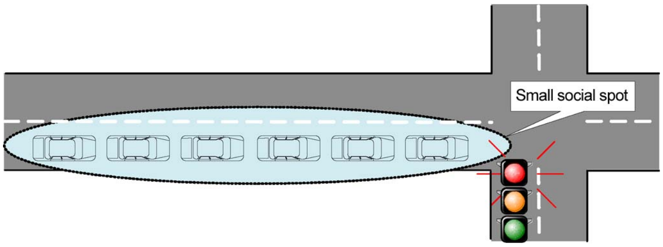


Fig. 5. PC at an intersection.

1) Anonymity Set Analysis at Small Social Spots: As shown in Fig. 5, when the traffic light turns red, the road intersection can be regarded as a *small social spot*, because a fleet of vehicles will stop at the intersection [15]. Consider that all vehicles will simultaneously change their pseudonyms when the traffic light turns to green. Then, the road intersection naturally becomes a *mix zone*. Let S_a be the number of vehicles that stopped at the intersection; then, we will have the expected ASS $(\text{ASS}) = S_a$. Clearly, the larger the ASS, the greater the anonymity offered in the small social spot. We can use a trivial anonymity set analytic model on ASS to investigate the anonymity level that is provided by the small social spot.

Let $T_s = t$, where $t = 30, 60$ s, be the fixed stop time period of a specific road intersection. Let the *vehicle arrival* (VA) at the road intersection be a Poisson process and t_a be the interarrival time for the VA, where t_a has an exponential distributions with the mean $1/\lambda$. Let X be the random variable of vehicles that arrive at the road intersection during the period T_s. Then, based on [26], [27], the probability $X = x$ during $T_s = t$ can be expressed as

$$\Pr[X = x | T_s = t] = \frac{(\lambda t)^x}{x!} e^{-\lambda t} \tag{8}$$

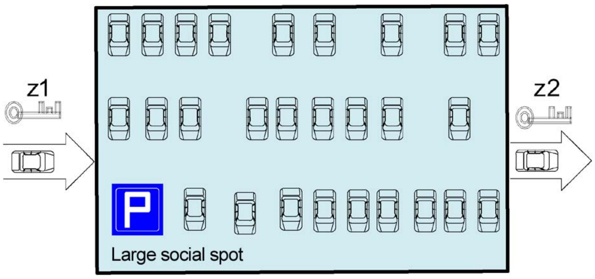


Fig. 6. PC at a free parking lot.

and the expected number of X's can be computed as

$$\mathtt{E}[X|T_s = t] = \sum_{x=1}^{\infty} x \Pr[X = x|T_s = t] = \lambda t. \tag{9}$$

Because all vehicles leave the intersection after the traffic light turns to green,[3] the ASS is

$$ASS = S_a = \mathtt{E}[X|T_s = t] = \lambda t \tag{10}$$

if all vehicles follow the PCS strategy.

2) Anonymity Set Analysis at Large Social Spots: As shown in Fig. 6, a large social spot could be a free parking lot near a shopping mall [22]. Because a parking lot usually holds many vehicles and each vehicle randomly leaves the parking lot at the user's own will, such a parking lot also naturally becomes a *mix zone* if all users change their pseudonyms in the parking lot and leave the parking lot after a random delay. Because a parking lot can obfuscate the relation between the arriving and leaving vehicles, the location privacy of a user can be achieved.

Let S_a be the number of vehicles in the parking lot when a vehicle is ready to leave. Then, the ASS denotes ASS $= S_a$. In the following discussion, we propose an anonymity analytic model on ASS to investigate the anonymity level that is provided by the large social spot.

For a specific vehicle $\mathcal{V}$ that has entered a parking lot near a shopping mall to change pseudonyms, we consider that the time period from the mall's opening time, e.g., 8:00 A.M., to the vehicle $\mathcal{V}$'s leaving time after PC T_S, as shown in Fig. 7, is exponentially distributed with the density function $f(t)$, the mean $1/\mu$, and the Laplace transform $f^*(s) = (\mu/\mu + s)$. On the other hand, other vehicles enter or leave a parking lot at the drivers' own will; for example, a driver determines when and how long he/she will shop at the mall. Let the VA at the parking lot be a Poisson process and t_a be the interarrival time for VA. Then, t_a has exponential distributions with the mean $1/\lambda$. In addition, the time period between the time when a vehicle arrives at the parking lot and the time when it leaves t_u is assumed to have the density function $f_u(\cdot)$, the mean $1/\omega$, and the Laplace transform $f_u^*(s)$. Let X be the random variable of vehicles that arrive at the parking lot during the time period T_s. Then, the probability $X = x$ during the period $T_s = t$ follows $\Pr[X = x|T_s = t] = ((\lambda t)^x/x!)e^{-\lambda t}$, and for $t \geq 0$, we have

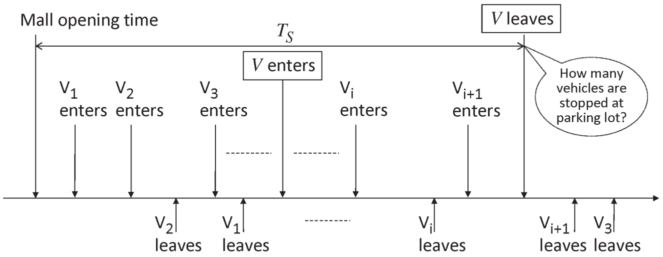


Fig. 7. Timing diagram (considering that no vehicle stops in the parking lot before the mall opening).

$$\begin{aligned}
\Pr[X = x] &= \int_{t=0}^{\infty} \Pr[X = x|T_s = t] f(t)\, dt \\
&= \int_{t=0}^{\infty} \frac{(\lambda t)^x}{x!} e^{-\lambda t} f(t)\, dt \\
&= \left(\frac{\lambda^x}{x!}\right) \int_{t=0}^{\infty} t^x e^{-\lambda t} f(t)\, dt \\
&= \left(\frac{\lambda^x}{x!}\right) \left[(-1)^x \frac{d^x f^*(s)}{ds^x} \right]\Bigg|_{s=\lambda} \\
&= \frac{\mu \lambda^x}{(\mu + \lambda)^{x+1}}.
\end{aligned} \tag{11}$$

The expected number of X can be computed as

$$\mathtt{E}[X] = \sum_{x=1}^{\infty} x \Pr[X = x] = \frac{\lambda}{\mu}. \tag{12}$$

Let χ be the time period between the time when a vehicle arrives at the parking lot and the time when the specific vehicle $\mathcal{V}$ leaves the parking lot after PC. Because T_s is exponentially distributed, the density function $\sigma(\chi)$ for the distribution χ can be expressed as

$$\sigma(\chi) = \mu \int_{t=\chi}^{\infty} f(t)\, dt = \mu \left[1 - F(t)\right]|_{t=\chi} = \mu e^{-\mu \chi}. \tag{13}$$

During the period T_s, several vehicles may leave the parking lot before $\mathcal{V}$'s leaving, i.e., $t_u < \chi$, whereas other vehicles leave after $\mathcal{V}$, i.e., $t_u \geq \chi$. Assume that Y is the number of vehicles that leave the parking lot before $\mathcal{V}$. The probability $\Pr[Y = y|X = x]$ can be computed as

$$\Pr[Y = y|X = x] = \binom{x}{y} \left(\Pr[t_u < \chi]\right)^y \left(\Pr[t_u \geq \chi]\right)^{x-y}. \tag{14}$$

[3] Note that, when the number of waiting vehicles is larger than some threshold, only part of the waiting vehicles can leave the intersection after the traffic light turns green, and some vehicles have to wait for the next green light. In this case, the number of waiting vehicles N_v can be regarded as the initial value for the next anonymity set size at the intersection, i.e., $ASS = N_v + \lambda t$.

Then, the probability $\Pr[t_u \geq \chi]$ can be calculated as

$$\begin{aligned}\Pr[t_u \geq \chi] &= \int_{t_u=0}^{\infty} \int_{\chi=0}^{t_u} \mu e^{\mu\chi} d\chi f_u(t_u)\, dt_u \\ &= \int_{t_u=0}^{\infty} (1-e^{-\mu t_u}) f_u(t_u)\, dt_u \\ &= 1 - \int_{t_u=0}^{\infty} f_u(t_u) e^{-\mu t_u}\, dt_u = 1 - f_u^*(\mu) \qquad (15)\end{aligned}$$

and $\Pr[t_u < \chi]$ can be derived from $\Pr[t_u \geq \chi]$ as

$$\Pr[t_u < \chi] = 1 - \Pr[t_u \geq \chi] = 1 - (1 - f_u^*(u)) = f_u^*(u). \qquad (16)$$

Then, (14) can be rewritten as

$$\Pr[Y = y | X = x] = \binom{x}{y} \left(f_u^*(u)\right)^y \left(1 - f_u^*(u)\right)^{x-y} \qquad (17)$$

and the expected number of Y can be computed as

$$\begin{aligned}\mathtt{E}[Y] &= \sum_{x=1}^{\infty} \sum_{y=1}^{x} \{y \Pr[Y = y | X = x] \Pr[X = x]\} \\ &= \sum_{x=1}^{\infty} \left\{ \left\{ \sum_{y=1}^{x} y \binom{x}{y} \left(f_u^*(u)\right)^y \left(1 - f_u^*(u)\right)^{x-y} \right\} \right. \\ &\qquad \left. \times \left[\frac{\mu \lambda^x}{(\mu+\lambda)^{x+1}} \right] \right\}. \qquad (18)\end{aligned}$$

Therefore, the expected ASS for the specific vehicle $\mathcal{V}$'s PC is

$$\begin{aligned}ASS = S_a &= \mathtt{E}[X] - \mathtt{E}[Y] \\ &= \frac{\lambda}{\mu} - \sum_{x=1}^{\infty} \left\{ \left\{ \sum_{y=1}^{x} y \binom{x}{y} \left(f_u^*(u)\right)^y \left(1 - f_u^*(u)\right)^{x-y} \right\} \right. \\ &\qquad \left. \times \left[\frac{\mu \lambda^x}{(\mu+\lambda)^{x+1}} \right] \right\}. \qquad (19)\end{aligned}$$

Because the exponential distribution has widely been used in modeling several realistic scenarios [26], we assume that t_u also follows the exponential distribution. Then, the Laplace transform $f_u^*(u)$ becomes

$$f_u^*(u) = \left(\frac{\omega}{\omega + \mu} \right). \qquad (20)$$

As a result, S_{anony} can be rewritten as

$$\begin{aligned}ASS &= \frac{\lambda}{\mu} - \sum_{x=1}^{\infty} \left\{ \left\{ \sum_{y=1}^{x} y \binom{x}{y} \left(\frac{\omega}{\omega+\mu} \right)^y \left(1 - \frac{\omega}{\omega+\mu} \right)^{x-y} \right\} \right. \\ &\qquad \left. \times \left[\frac{\mu \lambda^x}{(\mu+\lambda)^{x+1}} \right] \right\} \\ &= \frac{\lambda}{\mu} - \sum_{x=1}^{\infty} \left\{ x \cdot \frac{\omega}{\omega+\mu} \times \left[\frac{\mu \lambda^x}{(\mu+\lambda)^{x+1}} \right] \right\} \\ &= \frac{\lambda}{\mu} - \frac{\omega\mu}{(\omega+\mu)(\mu+\lambda)} \sum_{x=1}^{\infty} x \cdot \left(\frac{\lambda}{\mu+\lambda} \right)^x \\ &= \frac{\lambda}{\mu} - \frac{\omega\lambda}{\mu(\omega+\mu)} = \frac{\lambda}{\omega+\mu}. \qquad (21)\end{aligned}$$

C. Feasibility Analysis of the PCS Strategy

The aforementioned anonymity set analyses are under the assumption that all vehicles change their pseudonyms. In this section, we use the simplified game-theoretic techniques to show the feasibility of the PCS strategy, i.e., we prove that each vehicle is really willing to change the pseudonym at social spots to achieve its location privacy in practice.

Let the ASS be $N = n + 1$, where $n \geq 0$, at social spots, which can be estimated by the aforementioned anonymity set analysis. Then, we investigate the scenario where all vehicles are rational to protect their location privacy. At social spots, each vehicle V_j, $1 \leq j \leq N$ has the following two possible actions: 1) change (C) the pseudonym with probability p_j and 2) keep (K) the pseudonym with probability $1 - p_j$. If V_j keeps its pseudonym at the social spot, it will still be tracked with probability 1. Then, the loss of V_j's location privacy is unchanged, and the payoff in this action is a normalized location privacy loss of $-d_j$, where $d_j \in (0, 1)$ is the V_j's self-evaluation on the importance of location privacy. On the other hand, when V_j changes its pseudonym at the social spot, if other vehicles also take the same action, the ASS will become S. After this social spot, V_j is still tracked only with probability $1/S$. As such, the loss of location privacy in this case is reduced to $-d_j/S$. Let $c_j \in (0, 1)$ be V_j's normalized cost of changing a pseudonym; therefore, the payoff in this action is $-(d_j/S) - c_j$. For all vehicles, except for V_j, let p_m be the minimum of all probabilities $\{p_i | 1 \leq i \leq N, i \neq j\}$. Then, when V_j is ready to change its pseudonym at social spots, it can estimate the low bound of the average anonymity set as

$$S = \sum_{i=0}^{n} \binom{n}{i} \cdot p_m^i \cdot (1 - p_m)^{n-i} \cdot (i + 1) = np_m + 1.$$

As a result, the payoff function of vehicle V_j can be summarized as

$$Payoff = \begin{cases} -\frac{d_j}{np_m+1} - c_j, & \text{if action C is taken} \\ -d_j, & \text{if action K is taken.} \end{cases} \qquad (22)$$

Because vehicle V_j is rational and its goal is to protect its location privacy, the condition that V_j changes its pseudonym at the social spot is

$$-\frac{d_j}{np_m + 1} - c_j > -d_j \Rightarrow c_j < \frac{np_m d_j}{np_m + 1}. \qquad (23)$$

With the adopted KPSD scheme, all vehicles generate and manage their pseudonyms by themselves, and they can generate enough pseudonyms before a travel; then, the cost of changing a pseudonym can be very low. Nevertheless, when np_m is 0, (23) does not hold, which indicates that, when there is no neighboring vehicle that changes its pseudonym, V_j does not also change

TABLE I
PARAMETER SETTINGS

Parameter	Values
T_S: time period at small social spot	30, 60 seconds
$1/\lambda$: at small social spot	$[2, 4, 6, 8, 10, 12]$ seconds
$1/\mu$: mean of T_S at large social spot	$[1, 2, \cdots, 10]$ hours
$1/\lambda$: at large social spot	$[2, 4, 6]$ minutes
$1/\omega$: at large social spot	$[10, 20, \cdots, 90]$ minutes
d_i: a vehicle's self-evaluation on the importance of its location privacy	normalized

its pseudonym. However, when np_m is larger than 0, V_i can always reduce the cost c_j such that $c_j < (np_m d_j/np_m + 1)$. Then, V_j can actively change the pseudonym at social spots. We define each vehicle V_j's location privacy gain (LPG) function as

$$LPG_j = -\frac{d_i}{np_m + 1} - (-d_i) = \frac{np_m}{np_m + 1} \cdot d_j.$$

Then, LPG_j is an increasing function in terms of p_m. When $p_m = 1$, i.e., all vehicles change their pseudonyms at social spots, LPG_j can reach its maximal gain $(n/n + 1) \cdot d_j = ((N - 1)/N) \cdot d_j$. Because each vehicle is rational to maximize its LPG, the case would be a win–win situation when all vehicles change their pseudonyms. As a result, the feasibility of the PCS strategy in practice is shown.

IV. PERFORMANCE EVALUATION

In this section, we evaluate the location privacy level that is achieved in the PCS strategy. In particular, extensive simulations are conducted to demonstrate the impacts of different parameters on the performance metrics in terms of the ASS and LPG. Our simulations are based on a discrete-event simulator coded in C++, where the simulation parameters are listed in Table I for the following two scenarios: 1) the small social spot and 2) the large social spot. For each case, we repeat the simulation 100 times with different random seeds and calculate the average value with 95% confidence intervals. In addition, we compare the simulation results (denoted as Sim) with the numerical ones (denoted as Ana) to validate the developed analytical models.

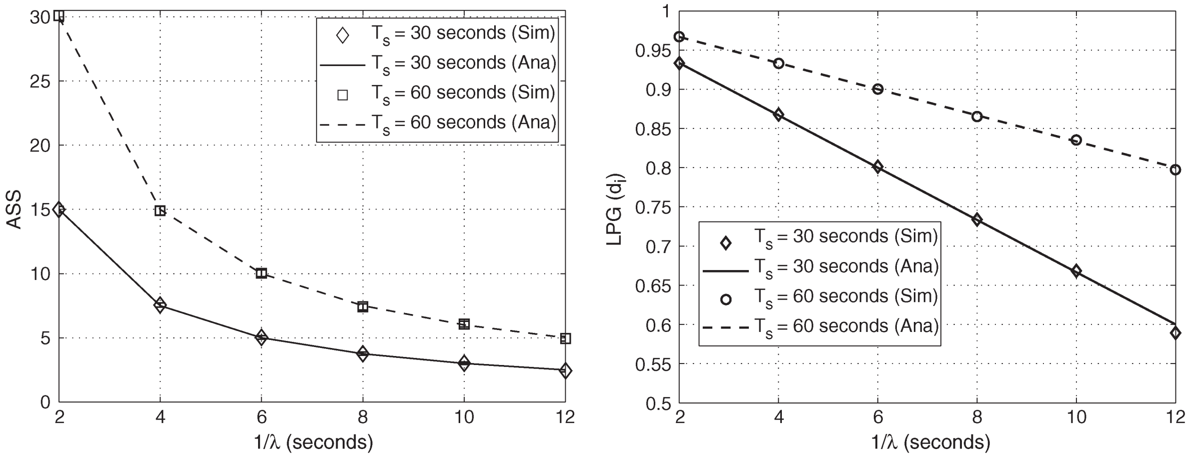
We first validate the location privacy level that is achieved at a small social spot, i.e., a road intersection when the traffic light turns red. Consider the stop time period $T_S = 30, 60$ s for a low traffic intersection and a high traffic intersection, respectively. Fig. 8 shows the ASS and LPG versus $1/\lambda$, which varies from 2 s to 10 s, with an increase of 2. In the figure, it is shown that the ASS and LPG decrease with the increase of $1/\lambda$. The reason is that, with a large $1/\lambda$, fewer vehicles drive at the road intersection when the traffic light is red, which leads to a small number of vehicles that gather at the intersection. As a result, it causes a smaller ASS and a lower LPG. In addition, a large T_S has a positive impact on the ASS and LPG. Therefore, to achieve a high location privacy level, a large intersection with high traffic is a good choice for vehicles, which tallies with our common sense.

To evaluate the location privacy level that is achieved at a large social spot, we consider a free parking lot near a shopping mall. Parameterized with $1/\mu = 4$ h, Fig. 9 shows the impacts of $1/\omega$ on the performance metrics in terms of the ASS and LPG. In the figure, it is shown that, as $1/\omega$ increases, both the ASS and LPG also increase. The reason is that the larger $1/\omega$ is, the more that vehicles will park at the parking lot. In addition, the smaller $1/\lambda$ achieves a larger ASS and a higher LPG. Therefore, when a vehicle changes its pseudonyms in a parking lot near a prosperous shopping mall (with small $1/\lambda$ and large $1/\omega$), the high location privacy level can be guaranteed. In the figure, it is also shown that the simulation and analysis results match very well, which justifies the accuracy of the analytical model.

Fig. 10 shows the impacts of the parameter $1/\mu$ on the ASS and LPG. We can see that, except for the first two hours, with the increase of $1/\mu$, both the ASS and LPG smoothly increase. The results indicate that a vehicle can change its pseudonyms mostly during the daytime for better location privacy at a large social spot, regardless of whether it is in the morning or the afternoon. In the figure, the gaps between the simulation and the analytical results are small, which can further be reduced if a larger number of simulation runs are conducted.

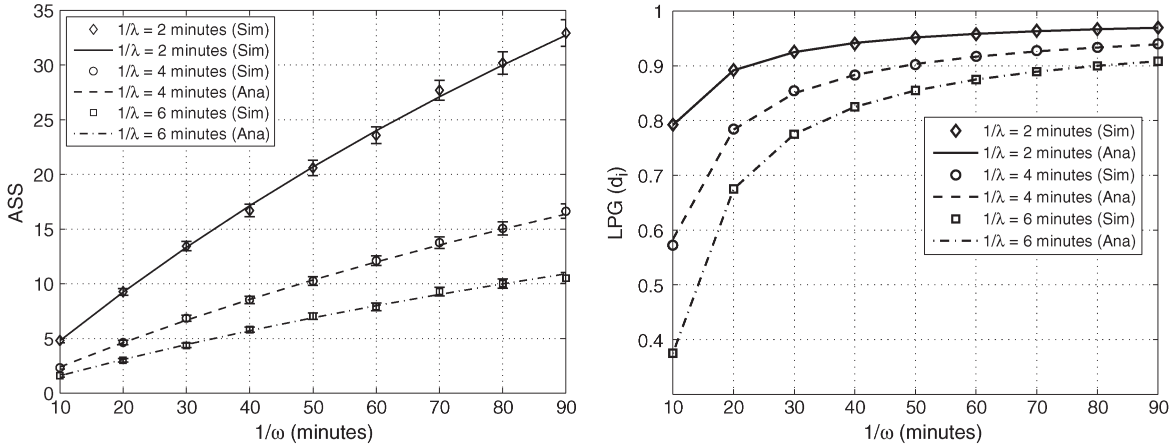
V. RELATED WORK

There have been a few prior efforts on frequently changing pseudonyms in mix zones to achieve location privacy in VANETs. In the following discussion, some research works that are closely related to ours are reviewed. In [28], Gerlach proposes an approach called *context mix* to protect the location privacy of vehicles. In *context mix*, a vehicle permanently assesses its neighborhood and changes its pseudonyms only if the vehicle detects k vehicle with a similar direction in a confusion radius. The *context mix* is an intuitive approach for achieving location privacy in VANETs. However, how k vehicles in neighborhood can be detected and how neighboring vehicles can be guaranteed to similarly react should further be exploited. In [13], Li *et al.* propose two user-centric location-tracking mitigation schemes called *swing* and *swap*, where *swing* can increase location privacy by enabling the nodes to loosely synchronize updates when changing the velocity, and *swap* enables the vehicle to exchange the identifiers to potentially maximize the location privacy that is provided by each update. In [9], Butyan *et al.* define a model to study the effectiveness of changing pseudonyms to provide location privacy in VANETs. Concretely, they characterize the tracking strategy of the adversary in the model and introduce a metric for quantifying the level of location privacy enjoyed by the vehicles. In addition, they use extensive simulations to study the relationship between the strength of the adversary model and the level of the privacy that is achieved by changing pseudonyms. In [15], Freudiger *et al.* use cryptographic techniques to create mix zones at road intersections, combine these mix zones into vehicular mix networks, and then leverage on the mobility of the vehicles and the dynamics of road intersections to mix vehicle identifiers. Finally, they evaluate the effectiveness of the proposed mix system by simulations. Different from the aforementioned works, our PCS strategy suggests that the vehicles change pseudonyms at



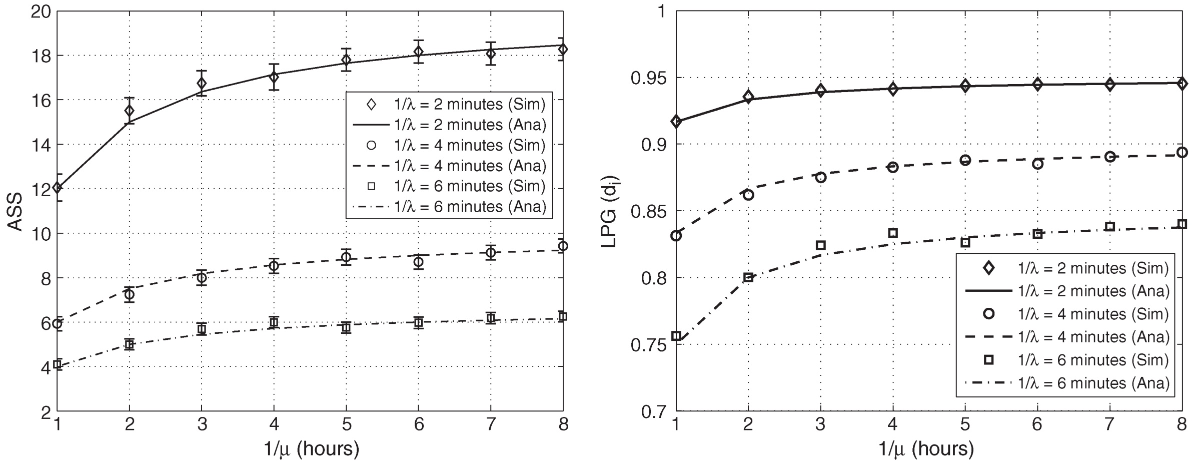
(a) (b)

Fig. 8. ASS and LPG versus $1/\lambda$ with different T_S's at a small social spot. (a) ASS versus $1/\lambda$. (b) LPG versus $1/\lambda$.



(a) (b)

Fig. 9. ASS and LPG versus $1/\omega$ with $1/\mu = 4$ h and different $1/\lambda$'s at a large social spot. (a) ASS versus $1/\omega$. (b) LPG versus $1/\omega$.



(a) (b)

Fig. 10. ASS and LPG versus $1/\mu$ with $1/\omega = 40$ min and different $1/\lambda$'s at a large social spot. (a) ASS versus $1/\mu$. (b) LPG versus $1/\mu$.

social spots (as mix zones) to maximize the location privacy and theoretically analyze the location privacy achieved.

In the research line of the placement of mix zones, Freudiger *et al.* [29] analyze the optimal placement of mix zones with combinational optimization techniques and show that the optimal mix-zone placement performs comparatively well to the full-deployment scenarios. This paper is instructive, which guides the placement of mix zones in VANETs. In our

PCS strategy, due to the characteristics of social spots and, at the same time, because the KPSD model can provide each vehicle enough secure pseudonyms for changing, social spots are, in nature, of mix zones to achieve better location privacy.

The size of the anonymity set and the entropy of the anonymity set are two popular quantitative measurements of location privacy in VANETs [30]. Following Beresford and Stajano's seminal work [10], the location privacy of a vehicle that corresponds to a PC event is the entropy of $P_{i\to PC}$, i.e., $H(PC) = -\sum_{i=1}^{N} P_{i\to PC} \cdot \log_2(P_{i\to PC})$, where $P_{i\to PC}$ is the probability of the mapping of a vehicle i to a PC event, and N is the total number of vehicles in the mix zone. When N increases and $P_{i\to PC}$ is uniformly distributed, i.e., $P_{i\to PC} = 1/N$, the entropy reaches the maximum $H(PC) = \log_2 N$. Therefore, when PC events are indistinguishable in social spots, both the size and the entropy of the ASS can measure the achieved location privacy. In this paper, our PCS strategy adopts the ASS as the metric and focuses on developing anonymity set analytical models to investigate the location privacy level.

In [31], Freudiger *et al.* observe that self-interested mobile nodes may not cooperate in changing pseudonyms in a mix zone and would jeopardize the achieved location privacy. To address this issue, they use game-theoretic techniques to analyze the noncooperative behavior of mobile nodes. In our PCS strategy, we also use the game theory to analyze the feasibility. Because the adopted KPSD scheme provides each vehicle with enough pseudonyms, each vehicle is willing to change its pseudonym at a social spot to achieve better location privacy. As a result, the feasibility is easily analyzed.

VI. Conclusion

In this paper, we have proposed an effective PCS strategy for location privacy in VANETs. In particular, we developed two anonymity set analytical models in terms of the ASS to formally analyze the achieved location privacy level, and we used game-theoretic techniques to prove its feasibility. In addition, we introduced a practical KPSD model to mitigate the hazards caused by vehicle theft. To the best of our knowledge, most previously reported works on *mix-zone-based PC only* use the simulations to evaluate the achieved location privacy. Therefore, our analytical models on location privacy at a social spot *shed light on* this research line. In our future work, we will carry out more experiments to verify the effectiveness of the PCS strategy in practice. In addition, because the current threat model primarily considers that an adversary can track a vehicle in a spatial–temporal way, another research direction in our future work is to consider an adversary that can utilize more character factors to track a vehicle and to explore new location-privacy-enhanced techniques under such a stronger threat model.

References

[1] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Anonymity analysis on social-spot-based pseudonym changing for location privacy in VANETs," in *Proc. IEEE ICC*, Kyoto, Japan, Jun. 2011.

[2] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 88–95, Apr. 2008.

[3] J. Eriksson, L. Girod, B. Hull, R. Newton, S. Madden, and H. Balakrishnan, "The pothole patrol: Using a mobile sensor network for road surface monitoring," in *Proc. 6th Int. Conf. Mobile Syst., Appl., Serv.*, 2008, pp. 29–39.

[4] M. Tentori, J. Favela, and V. M. González, "Quality of privacy (QoP) for the design of ubiquitous healthcare applications," *J. Universal Comput. Sci.*, vol. 12, no. 3, pp. 252–269, 2006.

[5] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. 27th Conf. Comput. Commun.*, Phoenix, AZ, Apr. 2008, pp. 1229–1237.

[6] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security—Special Issue Security Ad Hoc Sensor Netw.*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

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

[8] C. Zhang, X. Lin, R. Lu, P. 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.

[9] L. Buttyan, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in *Proc. ESAS*, 2007, vol. 4572, pp. 129–141.

[10] A. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in *Proc. 2nd IEEE Annu. Conf. Pervasive Comput. Commun. Workshops*, Mar. 2004, pp. 127–131.

[11] L. Huang, H. Yamane, K. Matsuura, and K. Sezaki, "Towards modeling wireless location privacy," in *Proc. PET*, 2005, vol. 3856, pp. 59–77.

[12] L. Huang, H. Yamane, K. Matsuura, and K. Sezaki, "Silent cascade: Enhancing location privacy without communication QoS degradation," in *Proc. SPC*, 2006, vol. 3934, pp. 165–180.

[13] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & swap: User-centric approaches towards maximizing location privacy," in *Proc. WPES*, 2006, pp. 19–28.

[14] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," in *Proc. ESCAR*, 2005.

[15] J. Freudiger, M. Raya, and M. Feleghhazi, "Mix zones for location privacy in vehicular networks," presented at the Workshop on Wireless Networking for Intell. Transp. Syst., Vancouver, BC, Canada, Aug. 2007, LCA-CONF-2007-016.

[16] A. Pfitzmann and M. Köhntopp, "Anonymity, unobservability, and pseudonymity—A proposal for terminology," in *Proc. Workshop Des. Issues Anonymity Unobservability*, 2000, vol. 2009, pp. 1–9.

[17] P. Papadimitratos, A. Kung, J. P. Hubaux, and F. Kargl, "Privacy and identity management for vehicular communication systems: A position paper," presented at the Workshop on Standards for Privacy in User-Centric Identity Management, Zurich, Switzerland, 2006, LCA-CONF-2006-020.

[18] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communication," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[19] W. Mao, *Modern Cryptography: Theory and Practice*. Englewood Cliffs, NJ: Prentice-Hall, 2003.

[20] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proc. VANET*, Montreal, QC, Canada, Sep. 2007, pp. 19–28.

[21] K. Zeng, "Pseudonymous PKI for ubiquitous computing," in *Proc. EuroPKI*, Turin, Italy, Jun. 2006, pp. 207–222.

[22] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A new VANET-based smart parking scheme for large parking lots," in *Proc. 28th Conf. INFOCOM*, Rio de Janeiro, Brazil, Apr. 2009, pp. 1413–1421.

[23] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *J. Cryptology*, vol. 17, no. 4, pp. 297–319, Sep. 2004.

[24] D. Boneh and X. Boyen, "Short signatures without random oracles and the SDH assumption in bilinear groups," *J. Cryptology*, vol. 21, no. 2, pp. 149–177, Feb. 2008.

[25] R. Lu, X. Lin, and X. Shen, "SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *Proc. 29th IEEE INFOCOM*, San Diego, CA, Mar. 2010, pp. 1229–1237.

[26] L. Kleinrock, *Queueing Systems*. Hoboken, NJ: Wiley, 1975.

[27] S.-M. Cheng, W.-R. Lai, P. Lin, and K.-C. Chen, "Key management for UMTS MBMS," *IEEE Trans. Wireless Commun.*, vol. 7, no. 9, pp. 3619–3628, Sep. 2008.

[28] M. Gerlach, "Assessing and improving privacy in VANETs," in *Proc. 4th Workshop ESCAR*, Nov. 2006, pp. 1–9.

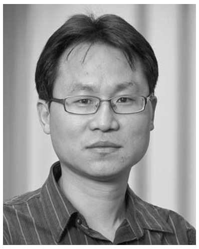
[29] J. Freudiger, R. Shokri, and J.-P. Hubaux, "On the optimal placement of mix zones," in *Proc. Privacy Enhancing Technol.*, 2009, pp. 216–234.

[30] Z. Ma, F. Kargl, and M. Weber, "Measuring long-term location privacy in vehicular communication systems," *Comput. Commun.*, vol. 33, no. 12, pp. 1414–1427, Jul. 2010.

[31] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On non-cooperative location privacy: A game-theoretic analysis," in *Proc. ACM Conf. Comput. Commun. Security*, 2009, pp. 324–337.

Rongxing Lu (S'09–M'11) is currently working toward the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada.

He is also currently a Research Assistant with the Broadband Communications Research Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.



Xiaodong Lin (S'07–M'09) received the Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1998 and the Ph.D. degree (with an Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008.

He is currently an Assistant Professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON. His research interests include wireless network security, applied cryptography, computer forensics, and software security.

Dr. Lin was the recipient of a Canada Graduate Scholarships Doctoral Award from the Natural Sciences and Engineering Research Council of Canada and the Best Paper Awards at the 2009 IEEE International Conference on Computer Communications and Networks and the 2007 IEEE International Conference on Communications Computer and Communications Security Symposium.

Tom H. Luan received the B.E. degree in Xi'an Jiaotong University, Xi'an, China, in 2004 and the M.Phil. degree in electronics engineering from the Hong Kong University of Science and Technology, Kowloon, Hong Kong, in 2007. He is currently working toward the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada.

His research interests include wired and wireless multimedia streaming, peer-to-peer streaming, and vehicular network design.

Xiaohui Liang (S'10) is currently working toward the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada.

He is also currently a Research Assistant with the Broadband Communications Research Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and e-healthcare systems.

Xuemin (Sherman) Shen (M'97–SM'02–F'09) received the B.Sc. degree in electrical engineering from Dalian Maritime University, Dalian, China, in 1982 and the M.Sc. and Ph.D. degrees in electrical engineering from Rutgers University, Camden, NJ, in 1987 and 1990, respectively.

He is currently a Professor and the University Research Chair with the Department of Electrical and Computer Engineering, University of Waterloo, ON, Canada. He has served as the Editor-in-Chief of *Peer-to-Peer Networking and Applications*, Associate Editor for *Computer Networks* and *ACM/Wireless Networks*, and a Guest Editor for *ACM Mobile Networks and Applications*. He is a coauthor of three books and has published more than 400 papers and book chapters in wireless communications and networks, control, and filtering. His research interests include resource management in interconnected wireless/wired networks, ultra-wideband wireless communications networks, wireless network security, wireless body area networks, and vehicular ad hoc and sensor networks.

Dr. Shen is a Registered Professional Engineer of Ontario, Canada, and a Distinguished Lecturer of the IEEE Communications Society. He served as the Technical Program Committee Chair of the 2010 IEEE Vehicular Technology Conference and the 2007 IEEE Global Communications Conference. He was the Tutorial Chair of the 2008 IEEE International Conference on Communications and a General Cochair of the Second International Conference in Communications and Networking in China, in 2007, and the Third International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks in 2006. He is the Founding Chair of the IEEE Communications Society Technical Committee on per-to-peer Communications and Networking. He has also served as a Founding Area Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS, and the *IEEE Communications Magazine*. He received the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo, the Premier's Research Excellence Award from the Province of Ontario in 2003, the Outstanding Performance Award from the University of Waterloo in 2004 and 2008, and the Excellent Graduate Supervision Award in 2006.