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 Quality of Privacy (QoP) in vehicular ad hoc networks (VANETs), location privacy is imperative for the full flourish of VANETs. 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. Specifically, we first introduce the social spots where many 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 (ASS) as the location privacy metric, we then develop two anonymity set analytic models to quantitatively investigate the location privacy achieved by the PCS strategy. In addition, we use game theoretic techniques to prove the feasibility of 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 the proposed PCS strategy can assist vehicles to intelligently change their pseudonyms at the right moment and place.**

***Index Terms*—Vehicular Ad Hoc Networks, Security, Location Privacy, Social Spots**

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 not only communicate with each other, i.e., vehicle-to-vehicle (V-2-V) communications, but also communicate with Roadside Units (RSUs), e.g., vehicle-to-roadside (V-2-R) communications [2]. Due to this hybrid architecture of VANETs, a variety of promising applications ranging from safety (emergence reporting, collision warning) to non-saftey (infotainment) can be enabled to improve the road safety and better driving experiences. For example, vehicles equipped with sensors and GPS devices can monitor road surface conditions and detect potholes on the road [3], and then send the detected pothole warnings to the local road maintenance authority through V-2-V and V-2-R communications. Afterwards, 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 are able to drive with caution and avoid 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 which the public concerns, for example, the location privacy, one of the fundamental Quality of Privacies (QoP)[1] in VANETs [5]. Because VANETs are usually implemented in civilian scenarios, where the locations of vehicles are tightly related to the citizens who are driving them. If a VANET discloses any privacy information of citizens, e.g., location privacy, it cannot be widely 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 recommended in VANETs is that vehicles periodically change their pseudonyms when they are broadcasting *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, since an adversary could still link a new pseudonym with the old one [9]. As an example shown 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. Even though all three vehicles change their pseudonyms simultaneously, 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 achieved by frequent changing pseudonyms in VANETs [10]–[15]. Formally, we let $\overrightarrow{F} = \{F_1, F_2, F_3, \cdots\}$ be multi-dimensional character factors associated with a pseudonym changing process. For

Manuscript received January 30, 2011; revised June 17, 2011; accepted July 09, 2011. The research is financially supported by the Ontario Research Fund for Research Excellence (ORF-RE), Canada. Part of the work has been presented in IEEE International Conference on Communications ICC'11 [1]. The review of this paper was coordinated by Dr. T. Zhang.

R. Lu, H. Luan, X. Liang, and X. Shen are with Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada (e-mails: {rxlu, hluan, x27liang, 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).

[1]The term Quality of Privacy (QoP) in VANETs is analogy to the Quality of Service (QoS) [4]. It describes the privacy level a vehicle can achieve in VANETs.

example, the vector $\overrightarrow{F} = \{F_1, F_2, F_3, \cdots\}$ can represent factors $\{\texttt{Time}, \texttt{Location}, \texttt{Velocity}, \cdots\}$. In some specific scenarios, an adversary has the ability to monitor a subset $\overrightarrow{F}_n = \{F_1, F_2, \cdots, F_n\} \subset \overrightarrow{F}$ and use it for identifying a vehicle pseudonym changing process. Suppose $\overrightarrow{b}_0 = (x_1, x_2, \cdots, x_n)$ and $\overrightarrow{b}_1 = (y_1, y_2, \cdots, y_n)$ be the character vectors of two vehicles' pseudonym changing 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 pseudonyms changing processes can be regarded as indistinguishable in the eye of the adversary. Therefore, in order to protect location privacy with high quality, a vehicle should choose a proper scenario where as many as possible indistinguishable pseudonyms changing processes are taken place simultaneously.

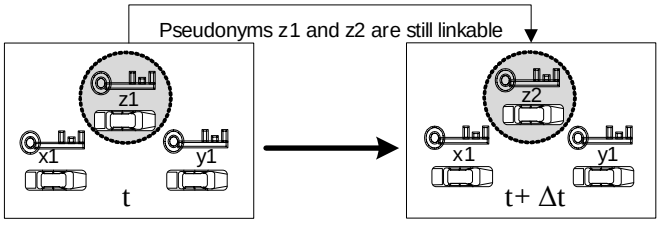


Fig. 1. Pseudonyms link due to changing pseudonyms at an improper occasion

In this paper, to facilitate vehicles to achieve high-level location privacy in VANETs, we propose an effective pseudonyms changing at social spots strategy, called PCS. In the PCS strategy, the social spots are the places where many 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 broadcasted *safety message* includes indistinguishable information `Location`= social spot, `Velocity`=0, and unlinkable `Pseudonym`. Then, the social spot naturally becomes a *mix zone*, and the location privacy can be achieved. Specifically, in this work, our contributions are threefold.

First, we utilize the unique feature of social spots, i.e., many vehicles temporarily stop at the social spot, to propose the PCS strategy. In addition, as an important technical preliminary of PCS strategy, we present a practical key-insulated pseudonym self-delegation (KPSD) model, which securely generates many 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 anonymity set size, the higher the anonymity achieved [9], [16]) to measure the Quality of Privacy (QoP) achieved in 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.

Third, to guarantee the PCS strategy can be effectively 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 model, threat model, 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 model, threat model, 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

- *Vehicles:* in the urban area, a large number of vehicles are running on the road everyday. Each vehicle is equipped with an OnBoard Unit (OBU) device, which allows the vehicle to communicate with other vehicles for sharing local traffic information to improve the whole safety driving conditions.
- *Social Spots:* the social spots in the urban area refer to the places where many vehicles gather, for example, a road intersection when the traffic light is red or a free parking lot near the shopping mall, as shown in Fig. 2. Since the session of red traffic light is typically short, (i.e., 30 or 60 seconds), the road intersection is called a *small social spot*. As a shopping mall usually operates for a whole day, indicating that a number of customers' vehicles will stop at the parking lot for a long period, the free parking lot near the mall is hence called a *large social spot*. Notice that as 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* broadcasted 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 $\mathcal{A}$ equipped with radio devices to trace the vehicles' locations, where

[2]We confine our problem to pseudonym changing in the V-2-V communication mode, and do not include Roadside Units (RSUs) in current network model, although RSUs are still deployed to support V-2-R communication in the urban area.

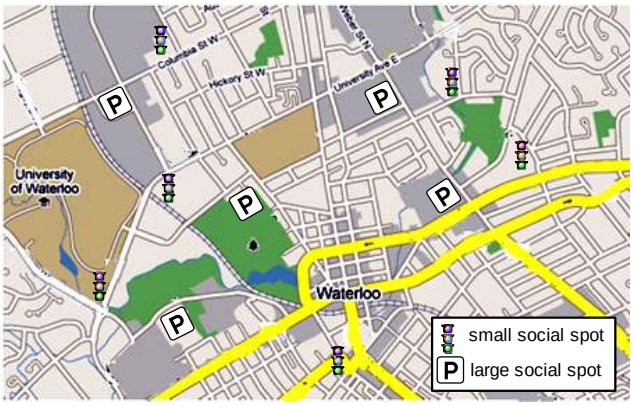


Fig. 2. Social spots including the road intersection when the traffic light turns red and free parking lots near the shopping mall

- *Global* means the adversary $\mathcal{A}$ has the ability to 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` as well as `Pseudonym`. Since `Pseudonym` is unlinkable and `Content` could be set as irrelevant, the adversary $\mathcal{A}$ primarily tracks a vehicle in terms of `Time`, `Location`, `Velocity`, i.e., in a spatial-temporal way in our model.
- *External* denotes the adversary $\mathcal{A}$ can only passively eavesdrop the communications, but does not actively attempt to compromise the running vehicles.

Notice 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 that of radio based eavesdropping [15]. Therefore, the 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 the 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 pseudonym in place of 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 location and the latter location. In addition, the pseudonyms changing 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 VANET. If a broadcasted *safety message* is in dispute, the trusted authority (TA) can disclose the real identity, i.e., TA has the ability to determine the location where a specific vehicle broadcasted a disputed *safety message*.

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

III. Proposed PCS Strategy for Location Privacy

In this section, we present our PCS strategy for achieving location privacy in VANETs. Specifically, we develop two anonymity set analytic models to investigate the location privacy level achieved in the PCS strategy, and use simplified game theoretical techniques to discuss its feasibility. Before delving into the details of the PCS strategy, we first present a practical key-insulated pseudonym self-delegation (KPSD) model, which securely generates many on-demand short-life keys and serves as the basis of the proposed PCS strategy.

A. KPSD Model for PCS Strategy

To support the PCS strategy, a vehicle must hold a certain amount of pseudonyms. In [6], a simple and straightforward solution is proposed, where an OBU device equipped on a vehicle possesses a large number of anonymous short-time keys authorized by a Trusted Authority (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 technique which can achieve conditional location privacy without pseudonyms changing. However, the pure group signature verification is usually time-consuming which may be not suitable for some time-stringent VANET applications. ECPP [5] is another anonymous authentication technique which combines group signature and ordinary signature. In ECPP, when a legal vehicle passes by an RSU, the RSU will authorize a group signature based short-life anonymous certificate to the vehicle. Then, the vehicle can use it to sign messages with ordinary signature techniques [19]. Once receiving a signed message, anyone can verify the authenticity of message by checking both the anonymous certificate and message signature. Note that, when the vehicle signs many messages, any verifier only needs execute one group signature verification operation on certificate, thus it is more efficient than GSIS. Similar to ECPP, Calandriello et al. [20], inspired by the idea of pseudonymous 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 key insulated pseudonym self-delegation (KPSD) model.

As shown in Fig. 3, in KPSD model, 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 s/he is ready to go out for a travel, like feuling enough gasoline, s/he first generates required self-delegated short-life keys, and installs them in the OBU device. Later, when the vehicle is running in the urban area, these short-life keys can be used to sign messages. Because vehicle theft is still a

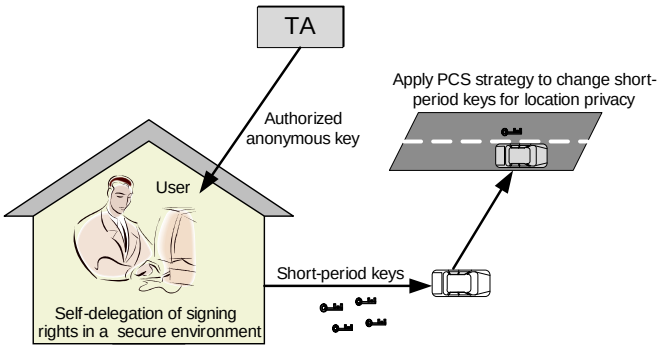


Fig. 3. Practical KPSD model for location privacy in VANETs

serious concern currently, e.g., statistics show that there have been over 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 KPSD model is not stored in the vehicle. Thus, the vehicle thieves can't generate more short-life keys. As a result, the hazards due to vehicle theft can be mitigated in KPSD model. Note that if the authorized anonymous key is protected by a password-based tamper-proof device, Calandriello et al.'s scheme [20] can fall into our key insulated pseudonym self-delegation model, but the cost will increase accordingly.

In the following, 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 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 $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ are equipped with a pairing, i.e., a non-degenerated and 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 $\mathbb{G}_1$, that we assume to be one-way (easy to compute, but hard to invert). 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, TA also chooses a public collision-resistant hash function: $H : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$. In the end, 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, TA first chooses a random number $s_i \in \mathbb{Z}_q^*$ such that $s_i + u \neq 0 \bmod q$, computes $A_i = g_1^{\frac{1}{s_i+u}}$. Then, TA stores (ID_i, A_i^u) in the tracking list and returns $ASK_i = (s_i, A_i = g_1^{\frac{1}{s_i+u}})$ 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 first runs the following steps to generate the required anonymous short-life keys used for the travel, which is very analogous to the fueling of a vehicle before a travel.

1) $\mathcal{U}_i$ first chooses l random numbers $x_1, x_2 \cdots, x_l \in \mathbb{Z}_n^*$ as the short-life private keys and computes the corresponding public keys $Y_j = g^{x_j}$, for $j = 1, 2, \cdots, l$ 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 $\alpha, r_\alpha, r_x, r_\delta \in \mathbb{Z}_q^*$ and compute $T_U, T_V, \delta, \delta_1, \delta_2, \delta_3$, where
   $$\begin{cases} T_U = {U_1}^\alpha, T_V = A_i \cdot {V_1}^\alpha, \delta = \alpha \cdot x_i \bmod q \\ \delta_1 = {U_1}^{r_\alpha}, \delta_2 = T_U^{r_x} / {U_1}^{r_\delta} \\ \delta_3 = e(T_V, {g_2}^{r_x}) / e(V_1, {U_2}^{r_\alpha \cdot g_2 {}^{r_\delta}}) \end{cases} \quad (1)$$
   - Compute $c = H(U_1||V_1||Y_j||T_U||T_V||\delta_1||\delta_2||\delta_3)$ and s_α, s_x, $s_\delta \in \mathbb{Z}_q^*$, where
   $$\begin{cases} s_\alpha = r_\alpha + c \cdot \alpha \bmod q, s_x = r_x + c \cdot x_i \bmod q \\ s_\delta = r_\delta + c \cdot \delta \mod q \end{cases} \quad (2)$$
   - 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 $Cert_j$, $j = 1, 2, \cdots, l$, are generated, $\mathcal{U}_i$ installs them to the vehicle, i.e., implanting all $x_j||Y_j||Cert_j$, $j = 1, 2, \cdots, l$, into the OBU device.

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

$$msg = (M||\sigma||Y_j||Cert_j) \quad (3)$$

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

1) If the certificate $Y_j||Cert_j$ has not been checked, the verifier first computes
   $$\begin{cases} \delta_1' = U_1^{s_\alpha} / {T_U}^c, \delta_2' = {T_U}^{s_x} / U_1^{s_\delta} \\ \delta_3' = \frac{e(T_V, {g_2}^{s_x} \cdot {U_2}^c)}{e(V_1, {U_2}^{s_\alpha} \cdot {g_2}^{s_\delta}) e(g_1, {g_2}^c)} \end{cases} \quad (4)$$
   and checks whether
   $$c = H(U_1||V_1||Y_j||T_U||T_V||\delta_1'||\delta_2'||\delta_3') \quad (5)$$
   If it does hold, the certificate $Y_j||Cert_j$ passes the verification. The corrections are as follows: i) $\delta_1' = U_1^{s_\alpha} / T_U^c = U_1^{r_\alpha + c \cdot \alpha} / U_1^{c \cdot \alpha} = \delta_1$; ii) $\delta_2' = T_U^{s_x} / U_1^{s_\delta} = T_U^{r_x + c x_i} / U_1^{r_\delta + c\delta} = \delta_2$; iii) $\delta_3' = e(T_V, {g_2}^{s_x} \cdot {U_2}^c) / e(V_1, {U_2}^{s_\alpha} \cdot {g_2}^{s_\delta}) e(g_1, {g_2}^c) = e(T_V, {g_2}^{r_x}) / e(V_1, {U_2}^{r_\alpha} \cdot {g_2}^{r_\delta}) = \delta_3$.
2) Once the certificate $Y_j||Cert_j$ passes the verification, the verifier checks
   $$e(Y_j \cdot {g_1}^{H(M)}, \sigma) \stackrel{?}{=} e(g_1, g_2) \quad (6)$$
   If it holds, the message M is accepted, otherwise, M is rejected, since $e(Y_j \cdot {g_1}^{H(M)}, \sigma) = e(g_1^{x_j + H(M)}, {g_2}^{\frac{1}{x_j + H(M)}}) = e(g_1, g_2)$. Note that the value of $e(g_1, g_2)$ can be pre-computed in advance.

Conditional Tracking: Once an accepted message M under the certificate

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

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

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

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

2) Security: Since both the short signature [24] and 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 also mitigate the hazards due to vehicle theft, since the authorized anonymous key ASK_i is *key-insulated*, i.e., it is stored in a secure environment, then vehicle thieves can not obtain ASK_i from the stolen vehicle, and consequently can not generate new self-delegated short-life keys arbitrarily.

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 msec. Let T_{pair}, $T_{\text{exp-1}}$, $T_{\text{exp-2}}$ be the time costs for pairing operation, 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 group signature-based (GSB) anonymous authentication are $(3+n)T_{\text{pair}}$ + $(4+n)T_{\text{exp-1}}$ + $5T_{\text{exp-2}}$ and $3nT_{\text{pair}}$ + $4nT_{\text{exp-1}}$ + $5nT_{\text{exp-2}}$, respectively. Since T_{pair} is dominant over $T_{\text{exp-1}}$ and $T_{\text{exp-2}}$, we set T_{pair} as 4.5 ms as in [5] and make the comparison in Fig. 4. Clearly, it can be seen, when n is large, the proposed anonymous authentication is much more efficient than the pure GSB anonymous authentication.

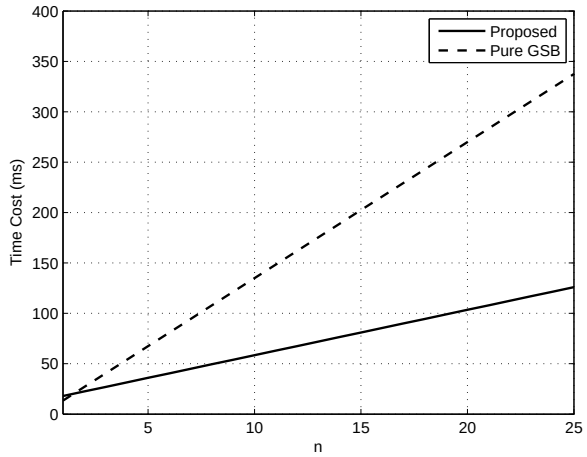


Fig. 4. Time cost comparison between the proposed anonymous authenticaiton and the pure GSB anonynous authentication

Algorithm 1 Pseudonym Changing at Social Spots Strategy

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

B. Anonymity Set Analysis for Achieved Location Privacy

With the above 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 achieved in small social spots and large social spots, respectively.

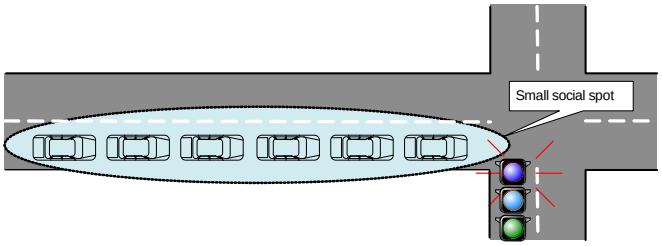


Fig. 5. Pseudonym changing at an intersection

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*, since a fleet of vehicles will stop at the intersection [15]. Consider 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 stopped at the intersection, we will have the expected anonymity set size (ASS) $= S_a$. Clearly, the larger the anonymity set size 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 provided by the small social spot.

Let $T_s = t$, where $t = 30, 60$ seconds, be the fixed stop time period of a specific road intersection. Let *vehicle arrival* (VA) at the road intersection be a Poisson process, and t_a be the inter-arrival time for VA, where t_a has an exponential distributions with the mean $\frac{1}{\lambda}$. Let X be the random variable of vehicles arriving 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

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

and the expected number of X can be computed as

$$\mathsf{E}[X|T_s = t] = \sum_{x=1}^{\infty} x \Pr[X = x|T_s = t] = \lambda t \quad (9)$$

Since all vehicles leave the intersection after the traffic light turns to green[3], the anonymity set size ASS is

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

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 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 user can be achieved.

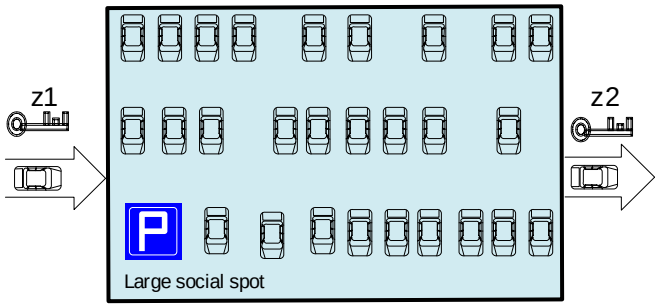


Fig. 6. Pseudonym changing at a free parking lot

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

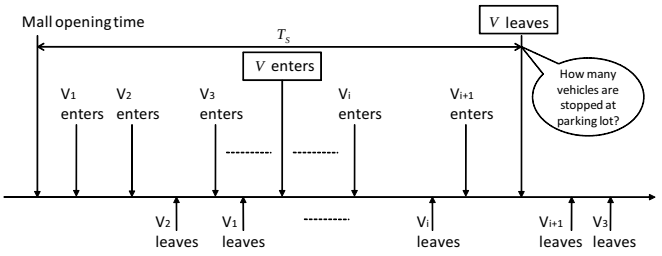


Fig. 7. Timing diagram (considering there is no vehicle stopping in the parking lot before the mall opening.)

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

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

and the expected number of X can be computed as

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

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 pseudonyms changing. Since T_s is exponentially distributed, the density function $\sigma(\chi)$ for the distribution χ can be expressed as

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

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

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

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

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

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

$$\Pr[t_u < \chi] = 1 - \Pr[t_u \geq \chi] = 1 - (1 - f_u^*(u)) = f_u^*(u) \tag{16}$$

[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 to 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 intersection, i.e., $ASS = N_v + \lambda t$.

After that, Eq. (14) can be rewritten as

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

and the expected number of Y can be computed as

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

Therefore, the expected anonymity set size ASS for the specific vehicle $\mathcal{V}$'s pseudonyms changing is

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

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

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

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

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

C. Feasibility Analysis of PCS Strategy

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

Let the anonymity set size ASS be $N=n+1$, where $n\geq 0$, at social spots, which can be estimated by the above 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 two possible actions: change (C) the pseudonym with probability p_j and 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 there are other vehicles taking the same action as well, the anonymity set size will become S. After this social spot, V_j remains being tracked only with probability $\frac{1}{S}$. As such, the loss of location privacy in this case is reduced to $-\frac{d_j}{S}$. Let $c_j\in(0,1)$ be V_j's normalized cost of changing a pseudonym, so the payoff in this action is $-\frac{d_j}{S}-c_j$. For all vehicles except 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 average anonymity set as

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

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

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

Since 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

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

With the adopted KPSD scheme, all vehicles generate and manage their pseudonyms by themselves, they can generate enough pseudonyms before a travel, then the cost of changing pseudonym can be very low. Nevertheless, when np_m is 0, Eq. (23) does not hold, which indicates when there is no neighboring vehicle changing its pseudonym, V_j also does not change its pseudonym. However, when np_m is large than 0, V_i is always able to reduce the cost c_j such that $c_j<\frac{np_md_j}{np_m+1}$. 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 increase 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 $\frac{n}{n+1}\cdot d_j=\frac{(N-1)}{N}\cdot d_j$. Since each vehicle is rational to maximize its location privacy gain, it would be a win-win situation when they all change their pseudonyms. As a result, the feasibility of PCS strategy in practice is shown.

IV. Performance Evaluation

In this section, we evaluate the location privacy level 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 anonymity set size (ASS) and location privacy gain (LPG). Our simulations are based on a discrete event simulator coded in C++, where the simulation parameters are listed in Table I for two scenarios: the small social spot and 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.

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

We first validate the location privacy level achieved at small social spot, i.e., a road intersection when the traffic light turns red. Consider the stopping time period $T_S = 30, 60$ seconds for a low traffic intersection and a high traffic intersection, respectively. Fig. 8 shows the ASS and LPG versus $1/\lambda$ varying from 2 seconds to 10 seconds with increase of 2. From the figure, it can be seen that ASS and LPG decrease with the increase of $1/\lambda$. The reason is that with a large $1/\lambda$, less vehicles drive at the road intersection when traffic light is red, which leads to a small number of vehicles gather at the intersection, as a result, it causes a smaller ASS as well as a lower LPG. In addition, a large T_S also has a positive impact on 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 achieved at large social spot, we consider a free parking lot near a shopping mall. Parameterized with $1/\mu = 4$ hours, Fig. 9 shows the impacts of $1/\omega$ on the performance metrics in terms of ASS and LPG. From the figure, it can be seen, as $1/\omega$ increases, both ASS and LPG also increase. The reason is that the larger $1/\omega$, the more vehicles will park at the parking lot. In addition, the smaller $1/\lambda$ also 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. From the figure, it can also be seen that the simulation and analysis results match very well, which justifies the accuracy of the analytical model.

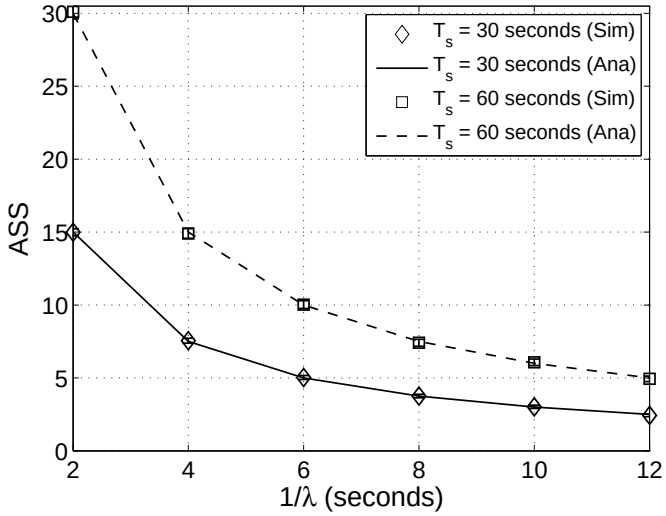
Fig. 10 shows the impacts of the parameter $1/\mu$ on ASS and LPG. We can see, except the first two hours, with the increase of $1/\mu$, both ASS and LPG smoothly increase. The results indicate that a vehicle can change its pseudonyms at most of daytime for better location privacy at large social spot, no matter in the morning or afternoon. In the figure, the gaps between the simulation results and the analytical results are small, which can be further reduced if larger number of simulation runs is conducted.

V. Related Work

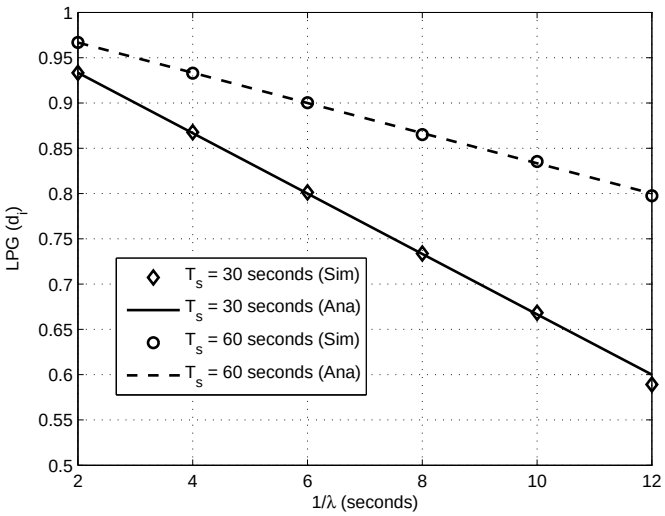
There have been a few prior efforts on frequently changing pseudonyms in mix zones to achieve location privacy in VANETs. In the following, some research works closely related to ours are reviewed. In [28], Gerlach proposes an approach, called *context mix*, to protect the location privacy of vehicles. 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 to detect k vehicles in neighborhood and how to guarantee neighboring vehicles to react similarly should be further 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 their velocity, and *Swap* enables the vehicle to exchange their identifiers to potentially maximize the location privacy provided by each update. In [9], Butyan et al. define a model to study the effectiveness of changing pseudonyms to provide location privacy in VANET. Concretely, they characterize the tracking strategy of the adversary in the model, and introduce a metric to quantify the level of location privacy enjoyed by the vehicles. Additionally, they also use extensive simulations to study the relationship between the strength of the adversary model and the level of the privacy achieved by changing pseudonyms. In [15], Freudiger et al. use cryptographic techniques to create mix zones at road intersections and combine these mix zones into vehicular mix networks, 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 above works, our PCS strategy suggests the vehicles to change pseudonyms at social spots (as mix zones), to maximize the location privacy, and theoretically analyze the achieve location privacy.

In the research line of the placement of mix zones, Freduiger 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 fully deployment scenarios. This work 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, since the KPSD model can provide each vehicle enough secure pseudonyms for changing, social spots are in nature of mix zones for achieving 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

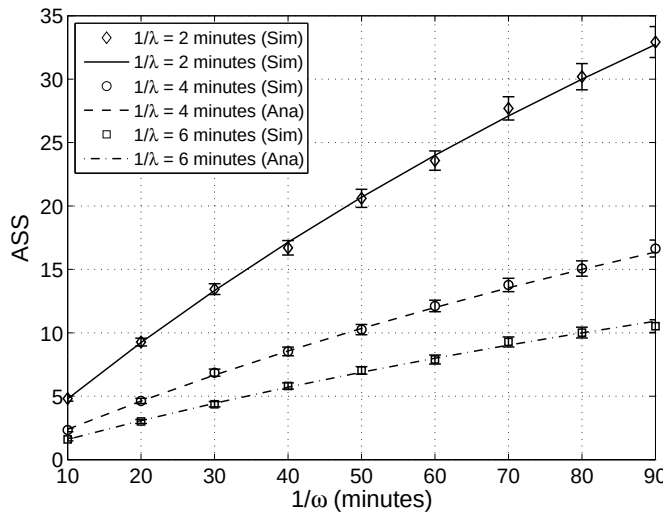


(a) ASS versus $1/\lambda$

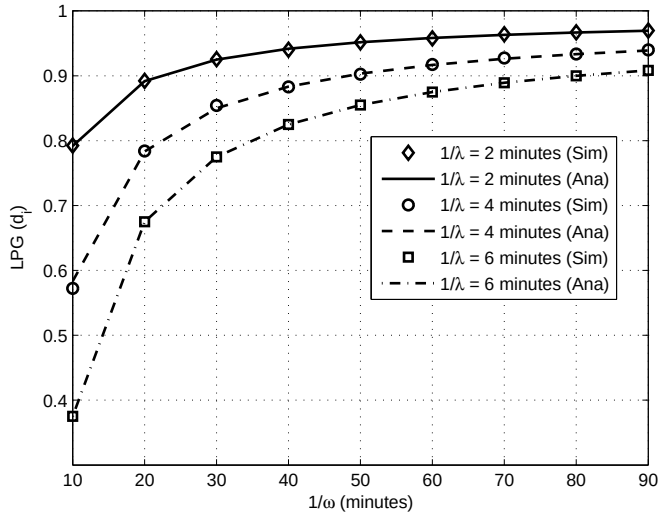


(b) LPG versus $1/\lambda$

Fig. 8. ASS and LPG versus $1/\lambda$ with different T_S at small social spot



(a) ASS versus $1/\omega$



(b) LPG versus $1/\omega$

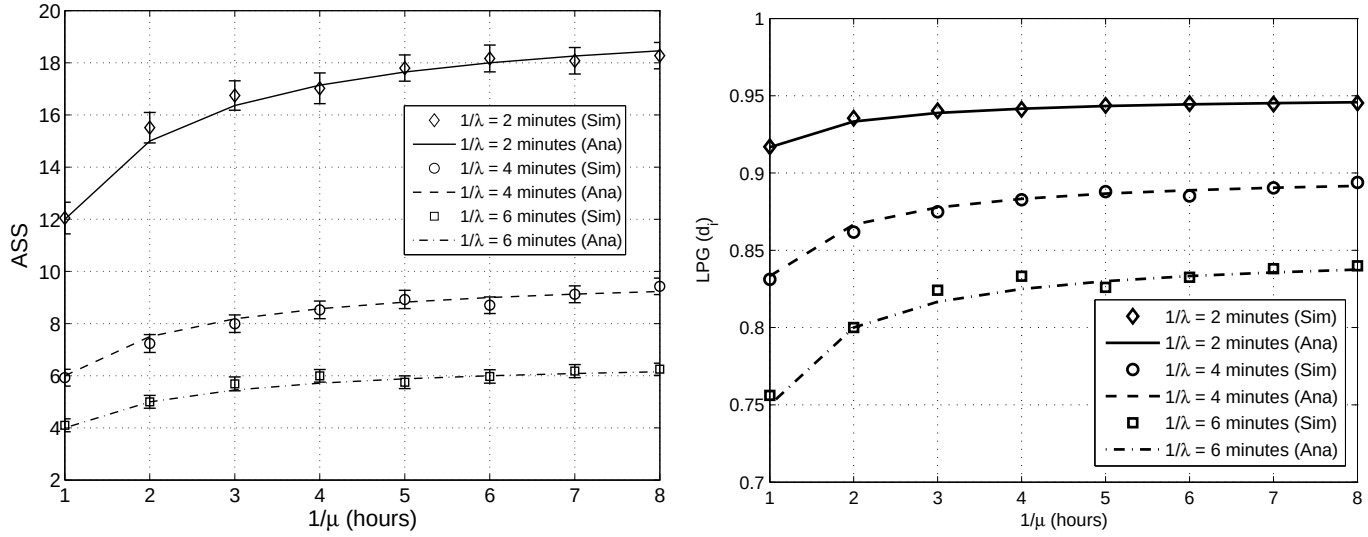
Fig. 9. ASS and LPG versus $1/\omega$ with $1/\mu = 4$ hours and different $1/\lambda$ at large social spot

vehicle corresponding to a pseudonyms changing (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 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 pseudonyms changing events are indistinguishable in social spots, both the size and the entropy of the anonymity set size can measure the achieved location privacy. In this work, our PCS strategy adopts anonymity set size 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 mix zone and would jeopardize the achieved location privacy. To address this issue, they use the game-theoretical techniques to analyze the non-cooperative behavior of mobile nodes. In our PCS strategy, we also use game theory to analyze the feasibility. Since the adopted KPSD scheme provides each vehicle with enough pseudonyms, each vehicle is willing to change its pseudonym at social spot for achieving better location privacy. As a result, the feasibility is easily analyzed.

VI. Conclusions

In this paper, we have proposed an effective pseudonym changing at social spots (PCS) strategy for location privacy in VANETs. In particular, we developed two anonymity set analytical models in terms of 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 pseudonyms changing *only*



(a) ASS versus $1/\mu$

(b) LPG versus $1/\mu$

Fig. 10. ASS and LPG versus $1/\mu$ with $1/\omega = 40$ minutes and different $1/\lambda$ at large social spot

use the simulations to evaluate the achieved location privacy. Therefore, our analytical models on location privacy at social spot *shed light on* this research line. In our future work, we will carry out more experiments to verify the effectiveness of PCS strategy in practice. In addition, since the current threat model primarily considers 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 explore new location privacy enhanced techniques under such stronger threat model [32].

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'11*, Kyoto, Japan, June 2011.

[2] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 88–95, 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 *Proceeding of the 6th international conference on Mobile systems, applications, and services*, ser. MobiSys '08. New York, NY, USA: ACM, 2008, pp. 29–39.

[4] M. Tentori, J. Favela, and V. M. González, "Quality of privacy (qop) for the design of ubiquitous healthcare applications," *The Journal of Universal Computer Science*, 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 *the 27th Conference on Computer Communications (INFOCOM 2008)*, Phoenix, Arizona, USA, April 2008, pp. 1229–1237.

[6] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sesnor Networks*, vol. 15, no. 1, pp. 39–68, 2007.

[7] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE Communications Magazine*, vol. 44, no. 10, pp. 8–15, 2006.

[8] C. Zhang, X. Lin, R. Lu, P. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, pp. 3357–3368, 2008.

[9] L. Buttyan, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in vanets," in *ESAS 2007*, ser. Lecture Notes In Computer Science, vol. 4572. Springer-Verlag, 2007, pp. 129–141.

[10] A. Beresford and F. Stajano, "Mix zones: user privacy in location-aware services," in *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, March 2004, pp. 127 – 131.

[11] L. Huang, H. Yamane, K. Matsuura, and K. Sezaki, "Towards modeling wireless location privacy," in *PET 2005*, ser. Lecture Notes In Computer Science, vol. 3856. Springer-Verlag, 2005, pp. 59–77.

[12] ——, "Silent cascade: Enhancing location privacy without communication qos degradation," in *SPC 2006*, ser. Lecture Notes In Computer Science, vol. 3934. Springer-Verlag, 2006, pp. 165–180.

[13] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & swap: user-centric approaches towards maximizing location privacy," in *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 *Proceedings of Embedded Securit in Cars (ESCAR)*, 2005.

[15] J. Freudiger, M. Raya, and M. Feleghhazi, "Mix zones for location privacy in vehicular networks," in *Proceedings of WiN-ITS 2007*, Vancouver, British Columbia, August 2007.

[16] A. Pfitzmann and M. Köhntopp, "Anonymity, unobservability, and pseudonymity - a proposal for terminology," in *Workshop on Design Issues in Anonymity and Unobservability*, ser. Lecture Notes In Computer Science, vol. 2009. Springer-Verlag, 2000, pp. 1–9.

[17] P. Papadimitratos, A. Kung, J. P. Hubaux, and F. Kargl, "Privacy and identity management for vehicular communication systsms: a position paper," in *Proceedings of Workshop on Standards for Privacy in User-Centric Identity Management*, 2006.

[18] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communication," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[19] W. Mao, *Modern Cryptography: Theory and Practice*. Prentice Hall PTR, 2003.

[20] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in *Proceedings of VANET' 07*, Montreal, Quebec, Canada., September 2007, pp. 19–28.

[21] K. Zeng, "Pseudonymous pki for ubiquitous computing," in *Proceedings of EuroPKI' 06*, Turin, Italy, June 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 *The 28th Conference on Computer Communications (INFOCOM 2009)*, Rio de Janeiro, Brazil, April 2009.

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

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

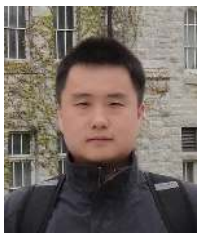
[25] R. Lu, X. Lin, and X. Shen, "SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant

networks," in *the 29th IEEE International Conference on Computer Communications (INFOCOM 2010)*, San Diego, California, USA, March 2010, pp. 1229–1237.
[26] L. Kleinrock, *Queueing Systems Vol. 1: Theory*. Wiley, 1975.
[27] S.-M. Cheng, W.-R. Lai, P. Lin, and K.-C. Chen, "Key management for umts mbms," *IEEE Transactions on Wireless Communications*, vol. 7, no. 9, pp. 3619–3628, 2008.
[28] M. Gerlach, "Assessing and improving privacy in vanets," in *Proceedings of Fourth Workshop on Embedded Security in Cars (ESCAR)*, November 2006.
[29] J. Freudiger, R. Shokri, and J.-P. Hubaux, "On the optimal placement of mix zones," in *Privacy Enhancing Technologies*, 2009, pp. 216–234.
[30] Z. Ma, F. Kargl, and M. Weber, "Measuring long-term location privacy in vehicular communication systems," *Computer Communications*, vol. 33, no. 12, pp. 1414–1427, 2010.
[31] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On non-cooperative location privacy: a game-theoretic analysis," in *ACM Conference on Computer and Communications Security*, 2009, pp. 324–337.
[32] B. Wiedersheim, F. Kargl, Z. Ma, and P. Papadimitratos, "Privacy in inter-vehicular networks: why simple pseudonym change is not enough," in *Proceedings of the Seventh International Conference on Wireless On-demand Network Systems and Services (WONS 2010)*, February 2010.

Rongxing Lu (S'09-M'11) is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently a research assistant with the Broadband Communications Research (BBCR) 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 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, Canada. His research interests include wireless network security, applied cryptography, computer forensics, and software security. Dr. Lin was the recipient of a Natural Sciences and Engineering Research Council of Canada (NSERC) Canada Graduate Scholarships (CGS) Doctoral and the Best Paper Awards of the IEEE International Conference on Computer Communications and Networks (ICCCN 2009) and the IEEE International Conference on Communications (ICC 2007) - Computer and Communications Security Symposium.

Tom L. Luan received the B.E. degree in Xi'an Jiaotong University, China in 2004 and the M.Phil. degree in electronic engineering from the Hong Kong University of Science and Technology, Kowloon, Hong Kong in 2007. He is now pursuing the Ph.D. degree at the University of Waterloo, ON, Canada. His current research interests focus on wired and wireless multimedia streaming, peer-to-peer streaming and vehicular network design.



Xiaohui Liang (S'10) is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently a research assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and e-healthcare system.

Xuemin (Sherman) Shen (M'97-SM'02-F'09) received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a Professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo, Canada. Dr. Shen's research focuses on resource management in interconnected wireless/wired networks, UWB wireless communications networks, wireless network security, wireless body area networks and vehicular ad hoc and sensor networks. He is a co-author of three books, and has published more than 400 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen has served as the Technical Program Committee Chair for IEEE VTC'10, the Tutorial Chair for IEEE ICC'08, the Technical Program Committee Chair for IEEE Globecom'07, the General Co-Chair for Chinacom'07 and QShine'06, the Founding Chair for IEEE Communications Society Technical Committee on P2P Communications and Networking. He has also served as a Founding Area Editor for IEEE Transactions on Wireless Communications; Editor-in-Chief for Peer-to-Peer Networking and Application; Associate Editor for IEEE Transactions on Vehicular Technology; Computer Networks; and ACM/Wireless Networks, Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications, etc. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004 and 2008 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada, and a Distinguished Lecturer of IEEE Communications Society.