Sacrificing the Plum Tree for the Peach Tree: A Socialspot Tactic for Protecting Receiver-location Privacy in VANET

Rongxing Lu[†], Xiaodong Lin[‡], Xiaohui Liang[†], and Xuemin (Sherman) Shen[†]
[†]Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
[‡]Faculty of Business and Information Technology, University of Ontario Institute of Technology,
Oshawa, Ontario, Canada L1H 7K4
Email:{rxlu, x27liang, xshen}@bbcr.uwaterloo.ca; xiaodong.lin@uoit.ca

***Abstract*—In this paper, to simultaneously protect the receiver-location privacy and improve the performance of packet delivery in VANET, we propose a socialspot-based packet forwarding (SPF) protocol by utilizing "Sacrificing the Plum Tree for the Peach Tree" — one of the Thirty-Six Strategies of Ancient China. With SPF protocol, each vehicle receiver only reveals a non-sensitive socialspot, e.g., a shopping mall, that he often visits as a stationary relay node to help packet forwarding and protect his other sensitive locations privacy. Detailed security analysis demonstrates the security of the proposed SPF protocol. In addition, extensive simulations have also been conducted to examine its good efficiency in terms of packet delivery ratio and average delay.**

***Keywords*— VANET, Packet forwarding, Receiver-location privacy, Socialspot**

I. Introduction

Recent advances in vehicular technology and wireless communication have paved the way for the rapid development of Vehicular Ad Hoc Network (VANET) [1]. As a special instantiate of mobile ad hoc network, VANET contains not only a large number of mobile vehicles equipped with wireless On Board Unit (OBU) device but also stationary Roadside Units (RSUs), which makes VANET more promising and can provide a variety of applications ranging from safety-related (e.g., emergence report, collision warning) to non-safety-related (e.g., multimedia file sharing) ones. However, the flourish of VANET still hinges up the fully understanding and managing the security and privacy challenges that the public concerns [1], [2]. In this paper, we will focus on how to protect receiver-location privacy in packet forwarding application [3] in VANET.

Location privacy is one of important privacy requirements in VANET, since the locations of vehicles are tightly related to the drivers. Therefore, if VANET doesn't protect vehicle's location privacy, it can't be accepted by the public. As for the packet forwarding application in VANET [3], to protect the receiver-location privacy, i.e., the receiver's location is unknown, a possible solution is adopting the flooding technique. However, as we know, the flooding technique will result in a large number of duplicate packets in the network. Though the flooding technique can protect the receiver-location privacy, it is very inefficient, especially when the storage at each vehicle is constrained. Therefore, how to simultaneously protect the receiver-location privacy and improve the performance of packet delivery in VANET has become a new challenging issue. Unfortunately, to the best of our knowledge, this challenging issue has not be explored.

"Sacrificing the Plum Tree for the Peach Tree" is one of the Thirty-Six Strategies of Ancient China, which means sacrificing something non-critical to ensure the overall interests. In this paper, we will use this tactic to propose an efficient socialspot-based packet forwarding (SPF) protocol to address the above challenging issue, where the socialspots are referred to the locations in a city environment that many vehicles often visit such as a shopping mall, a restaurant, or a cinema. Since socialspots are usually not sensitive to the vehicles, we can utilize the socialspot as the relay node for packet forwarding. In such a way, the performance of packet delivery can be significantly improved. Meanwhile, since many vehicles visit the same socialspot, the socialspot can't be used to trace a specific vehicle's other sensitive locations. Therefore, the socialspot tactic can protect the receiver-location privacy in VANET. The main contributions of this paper are two-fold.

- Firstly, based on the socialspot tactic, we propose an efficient SFP protocol aiming at packet forwarding application in VANET, and also conduct the comprehensive security analysis to validate its security to protect the receiver-location privacy in VANET. To the best of our knowledge, we are the *first* to utilize the socialspot tactic to resolve the above challenging issue.
- Secondly, we develop a custom simulator built in Java to examine the performance of the proposed SPF protocol. Extensive simulation results show that, the socialspot tactic can achieve good performance of packet forwarding in terms of packet delivery ratio and average delay in VANET.

The remainder of this paper is organized as follows. In Section II, we introduce the system model, privacy model and design goal. In Section III, we review the bilinear groups and complexity assumption. Our proposed SPF protocol is presented in Section IV, followed by its security analysis and performance evaluation in Section V and Section VI, respectively. We also discuss the related work in Section VII. Finally, we draw our conclusions in Section VIII.

II. Models and Design Goal

In this section, we formalize the system model, privacy model, and identify our design goal.

A. System Model

We consider a typical VANET which consists of a trusted authority (TA), a large number of vehicles and some socialspots in a city environment, as shown in Fig. 1.

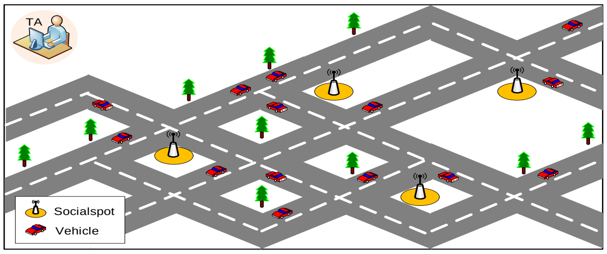


Fig. 1. System model under consideration

- Trusted Authority (TA): TA is a trustable and powerful entity, whose duties include initializing the system, deploying RSUs at some socialspots, and registering vehicles by granting a family of pseudo-IDs and the corresponding key materials.
- Socialspots $\mathcal{S} = \{\mathsf{ss}_1 \mathsf{ss}_2, \cdots\}$: Socialspots are referred to as the locations where many vehicles will visit, for example, a shopping mall, a restaurant, or a cinema. At each socialspot $\mathsf{ss}_i \in \mathcal{S}$, TA will deploy a trusted and identified storage-huge RSU, so that it can temporarily store some packets in packet forwarding application.
- Vehicles $\mathcal{V} = \{V_1, V_2, \cdots\}$: Each vehicle $V_i \in \mathcal{V}$ is equipped with the OBU device, which allows them to communicate with each other as well as those RSUs at socialspots for cooperative packet delivery in VANET. In general, the OBU device in VANET has no power-limited issue, however the storage is assumed constrained.

B. Privacy Model

In our privacy model, we consider how to protect a vehicle receiver's location privacy against an *external*, *global*, and *passive* adversary $\mathcal{A}$, where the adversary $\mathcal{A}$ doesn't compromise any RSUs or vehicles, but has a complete view to eavesdrop all packets forwarding in VANET. Note that, the adversary $\mathcal{A}$ could launch some active attacks such as black hole attack, grey hole attack to degrade the performance in cooperative packet delivery application [3]. However, since the focus of our work is on protecting receiver-location privacy, these active attacks are beyond the scope of this paper.

C. Design Goal

By utilizing the socialspot tactic, our design goal is to develop an efficient socialspot-based packet forwarding (SPF) protocol to protect receiver-location privacy in VANET. Specifically, since not all locations in a vehicle V_i's trajectory $\mathsf{Tr}_i = \{\mathsf{tr}_1, \mathsf{tr}_2, \cdots\}$ are sensitive to him, it is possible to reveal a non-sensitive socialspot that V_i often visits as a stationary relay node so that the packet delivery performance can be improved. At the same time, since many vehicles often visit the same socialspot, the RSU at the socialspot can serve as a mix server [3], then the adversary $\mathcal{A}$ can't link a specific packet to its receiver. In addition, since each vehicle V_i periodically changes his pseudo-IDs on the road, the receiver's sensitive locations are unlinkable and privacy-preserving.

III. Bilinear Maps and Complex Assumption

In this section, we review the bilinear map and required complex assumption. Let $(\mathbb{G}, +)$ be a cyclic additive group generated by P of a large prime order q, and $(\mathbb{G}_T, \times)$ be a cyclic multiplicative group with the same order q. An *admissible* bilinear pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a map with the following properties: i) *Bilinearity:* For all $P, Q \in \mathbb{G}$ and any $a, b \in \mathbb{Z}_q^*$, we have $e(aP, bQ) = e(P, Q)^{ab}$; ii) *Non-degeneracy:* There exist $P, Q \in \mathbb{G}$ such that $e(P, Q) \neq 1_{\mathbb{G}_T}$; and iii) *Computability:* There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathbb{G}$. Such an *admissible* bilinear pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ can be implemented by the modified Weil or Tate pairings [4].

In the following, we define the quantitative notion of the complexity of the required underlying problem, namely the Decisional Bilinear Diffie-Hellman (DBDH) Problem.

Definition 1: (DBDH Problem) The DBDH problem in $\mathbb{G}$ is as follows: Given an element $\widetilde{P}$ of $\mathbb{G}$, a tuple $(x\widetilde{P}, y\widetilde{P}, z\widetilde{P}, V)$ for unknown $x, y, z \in \mathbb{Z}_q^*$ and $V \in \mathbb{G}_T$, decide whether $V = e(\widetilde{P}, \widetilde{P})^{xyz}$ or a random element R drawn from $\mathbb{G}_T$.

Definition 2: (DBDH Assumption) Let $\mathcal{A}$ be an adversary that takes an input of $(x\widetilde{P}, y\widetilde{P}, z\widetilde{P}, V)$ for unknown $x, y, z \in \mathbb{Z}_q^*$, and $V \in \mathbb{G}_T$, and returns a bit $b' \in \{0, 1\}$. We consider the following random experiments.

```
Experiment $\mathbf{Exp}_{\mathcal{A}}^{\mathrm{DBDH}}$
    $x, y, z \xleftarrow{R} \mathbb{Z}_q^*; R \xleftarrow{R} \mathbb{G}_T$, $\widetilde{b} \leftarrow \{0, 1\}$
    if $\widetilde{b} = 0$, then $V = e(\widetilde{P}, \widetilde{P})^{xyz}$; else if $\widetilde{b} = 1$ then $V = R$
    $\widetilde{b}' \leftarrow \mathcal{A}\Big( \; x\widetilde{P}, y\widetilde{P}, z\widetilde{P}, V \; \Big)$
    return 1 if $\widetilde{b}' = \widetilde{b}$, 0 otherwise
```

We then define the advantage of $\mathcal{A}$ via

$$\begin{aligned}\mathbf{Adv}_{\mathcal{A}}^{\mathrm{DBDH}} = \Big| &\Pr\Big[\mathbf{Exp}_{\mathcal{A}}^{\mathrm{DBDH}} = 1 | \widetilde{b} = 0\Big] \\ &- \Pr\Big[\mathbf{Exp}_{\mathcal{A}}^{\mathrm{DBDH}} = 1 | \widetilde{b} = 1\Big]\Big| \geq \epsilon\end{aligned}$$

Let $\tau \in \mathbb{N}$ and $\epsilon \in [0, 1]$. The DBDH is called (τ, ϵ)-secure if no adversary $\mathcal{A}$ running in time τ has an advantage $\mathbf{Adv}_{\mathcal{A}}^{\mathrm{DBDH}} \geq \epsilon$.

IV. Our Proposed SPF Protocol

In this section, we will present our Socialspot-based Packet Forwarding (SPF) protocol for protecting receiver-location privacy in VANET. Before proceeding the SPF protocol, the rationale of socialspot tactic is first introduced.

A. Rationale of Socialspot Tactic

In reality, the locations in a driver's trajectory is almost fixed. For example, a driver may often drive to his home, school, and shopping mall. As for a driver, his home and school could be privacy locations, which is sensitive to him; while the shopping mall is a socialspot, which is usually not cared about. Therefore, it is possible to apply "Sacrificing the Plum Tree for the Peach Tree" tactic to reveal a receiver's socialspot as a stationary relay node to improve the performance of packet forwarding in VANET while protecting the receiver's other locations privacy, as shown in Fig. 2.

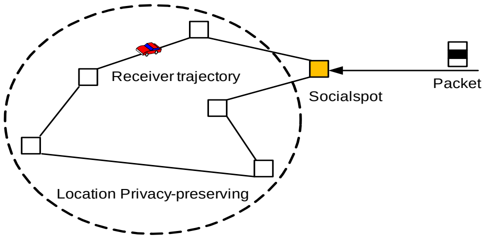


Fig. 2. Socialspot tactic to improve the performance of packet forwarding while protecting the receiver's sensitive locations privacy

B. Description of SPF Protocol

The SPF protocol consists of four phases: system initialization phase, packet generation phase, packet forwarding phase, and packet receiving phase.

1) System Initialization Phase: In the system initialization phase, the TA first configures the system parameter, chooses social spots in a city environment, and registers vehicles in the system. Specifically, the TA runs the following steps.

Step 1. Given the security parameter κ, the bilinear map groups $(\mathbb{G}, \mathbb{G}_T, e, P, q)$ are chosen, where $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, P is a generator of $\mathbb{G}$ and q is a large prime with $|q| = \kappa$. Then, TA chooses an random element $Q \in \mathbb{G}$, and a random number $s \in \mathbb{Z}_q^*$ as the *master key*, and computes the corresponding system public key $P_{pub} = sP$. In addition, TA chooses two secure cryptographic hash functions $\mathcal{H}_0, \mathcal{H}_1$, where $\mathcal{H}_i : \{0,1\}^* \to \mathbb{Z}_q^*$, for $i = 0, 1$, and a secure symmetric encryption algorithm $\mathbf{Enc}()$. In the end, TA sets the system public parameters $params$ as $(\mathbb{G}, \mathbb{G}_T, e, P, q, Q, P_{pub}, \mathcal{H}_0, \mathcal{H}_1, \mathbf{Enc}())$.

Step 2. TA chooses a set of socialspots $\mathcal{S} = \{\mathsf{ss}_1, \mathsf{ss}_2, \cdots\}$ in a city environment. Then, at each socialspot $\mathsf{ss}_i \in \mathcal{S}$, a storage-huge RSU is placed, which can be identified and trusted by passing-by vehicles.

Step 3. Assume the trajectory of a vehicle $V_i \in \mathcal{V}$ is $\mathsf{Tr}_i = \{\mathsf{tr}_1, \mathsf{tr}_2, \cdots\}$ such that $\mathsf{Tr}_i \cap \mathcal{S} \neq \phi$, i.e., at least there exists one location $\mathsf{tr}_a = \mathsf{ss}_b$, with $\mathsf{tr}_a \in \mathsf{Tr}_i$ and $\mathsf{ss}_b \in \mathcal{S}$. Then, when V_i registers himself, he submits his identity and the socialspot ss_b to TA. TA then grants a family of pseudo-IDs $\mathsf{PID} = \{\mathsf{pid}_0, \mathsf{pid}_1, \cdots\}$ and the corresponding pseudo-ID-based key materials for V_i by invoking the Algorithm 1. In such a way, V_i can use pid_0 at socialspot ss_b and constantly change its pseudo-IDs $\mathsf{pid}_i \in \mathsf{PID}$, $i \geq 1$, at other places to achieve identity privacy [5] and location privacy in a city environment.

Algorithm 1 Vehicle Registration Algorithm

```
procedure VehicleRegistration
Input: a vehicle $V_i \in \mathcal{V}$ and a socialspot $\mathsf{ss}_b \in \mathcal{S}$
Output: a family of pseudo-IDs and the corresponding pseudo-ID based key materials
    choose a family of unlinkable pseudo-IDs $\mathsf{PID} = \{\mathsf{pid}_0, \mathsf{pid}_1, \cdots\}$
    compute the private key $S_0 = \frac{1}{s+\mathcal{H}_0(\mathsf{pid}_0||\mathsf{ss}_b)}Q$ with respect to the pseudo-ID $\mathsf{pid}_0 \in \mathsf{PID}$ and the socialspot $\mathsf{ss}_b$
    for other pseudo-ID $\mathsf{pid}_i \in \mathsf{PID}$, $i \geq 1$ do
        compute the corresponding private key $S_i = \frac{1}{s+\mathcal{H}_0(\mathsf{pid}_0)}Q$
    end for
    return all tuples $(\mathsf{pid}_i, S_i)$ to $V_i$
end procedure
```

2) Packet Generation Phase: Assume that a stationary source wants to send a message M to a vehicle $V_i \in \mathcal{V}$ in the city environment. However, the source doesn't know the exact location of V_i, what he knows is only V_i's pseudo-ID pid_0 and the socialspot ss_b. Then, the source executes the following steps to generate a packet on M.

Step 1. The source first chooses a random number $x \in \mathbb{Z}_q^*$, and computes $k = e(P, Q)^x$, and C_1, C_2, C_3, where

$$\begin{cases} C_1 = x(P_{pub} + \mathcal{H}_0(\mathsf{pid}_0||\mathsf{ss}_b)P) \\ C_2 = \mathcal{H}_1(k||0), C_3 = \mathbf{Enc}(k, M) \end{cases}$$

Note that, (C_1, C_3) is a ciphertext of the anonymous identity-based encryption [6], which thus can achieve the receiver-identity anonymous.

Step 2. The source then packs the packet $\mathcal{P}$ with the format shown in Fig. 3, where $\mathsf{Head} := C_1$, $\mathsf{Auth} := C_2$, $\mathsf{Encrypted\text{-}Payload} := C_3$, and $\mathsf{Socialspot} := \mathsf{ss}_b$, and waits for some vehicles to help with forwarding the packet $\mathcal{P}$ to ss_b.

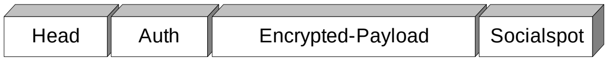


Fig. 3. The format of packet in the SPF protocol

3) Packet Forwarding Phase: Generally, the law of proximity shows that if a packet is located close to the socialspot ss_b, it is more likely that it can be carried to ss_b by some vehicles as soon as possible. Therefore, in this phase, the source will ask a passing-by vehicle to help with carrying the packet $\mathcal{P}$ to the socialspot ss_b or other socialspots close to ss_b. Specifically, the source invokes the Algorithm 2 to forward the packet $\mathcal{P}$.

Algorithm 2 Packet Forwarding Algorithm

```
procedure PacketForwarding
    When a vehicle is passing-by the source, the source asks for the help. If vehicle can forward $\mathcal{P}$ to $\mathsf{ss}_b$ or other socialspots close to $\mathsf{ss}_b$, the source forwards $\mathcal{P}$ to the vehicle.
end procedure
```

If the packet $\mathcal{P}$ is successfully forwarded to the socialspot ss_b, this phase is ended. Otherwise, when the packet is forwarded to other socialspots close to ss_b, then the RSU at the socialspot will temporally store the packet $\mathcal{P}$, and also invoke the Algorithm 2 to help with forwarding $\mathcal{P}$ to ss_b. The above RSU forwarding is iterative, and the packet $\mathcal{P}$ can be forwarded to ss_b eventually.

4) Packet Receiving Phase: Once the packet $\mathcal{P}$ reaches the socialspot ss_b and is stored at the RSU, the vehicle V_i can pick up the packet $\mathcal{P}$ by the following steps, when it comes across the socialspot ss_b.

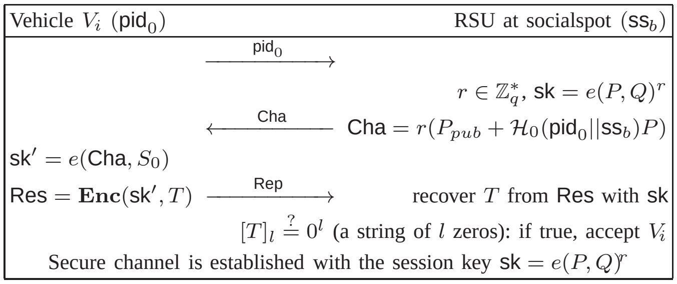

Vehicle V_i (pid_0)
RSU at socialspot (ss_b)
pid_0
$r \in \mathbb{Z}_q^*$, $\mathsf{sk} = e(P,Q)^r$
Cha
$\mathsf{Cha} = r(P_{pub} + \mathcal{H}_0(\mathsf{pid}_0||\mathsf{ss}_b)P)$
$\mathsf{sk}' = e(\mathsf{Cha}, S_0)$
$\mathsf{Res} = \mathbf{Enc}(\mathsf{sk}', T)$
Rep
recover T from Res with sk
$[T]_l \overset{?}{=} 0^l$ (a string of l zeros): if true, accept V_i
Secure channel is established with the session key $\mathsf{sk} = e(P,Q)^r$

Fig. 4. Secure channel establishment between V_i and a trusted RSU located at socialspot ss_b

Step 1. The vehicle V_i first establish a secure channel with the RSU by the following interactions, as shown in Fig. 4.

- V_i sends his pseudo-ID pid_0 to the RSU;
- RSU chooses a random number $r \in \mathbb{Z}_q^*$, computes the session key $\mathsf{sk} = e(P,Q)^r$, and sends the challenge $\mathsf{Cha} = r(P_{pub} + \mathcal{H}_0(\mathsf{pid}_0||\mathsf{ss}_b)P)$ back to V_i;
- After receiving the challenge Cha, V_i first computes $\mathsf{sk}' = e(S_0, \mathsf{Cha})$, and the response $\mathsf{Res} = \mathbf{Enc}(\mathsf{sk}', T)$, where T is a random number with the least significant l bits $[T]_l = 0^l$, and then sends Rep back to RSU.
- Upon receiving the response Res, RSU recovers T from Res, and checks whether the least significant l bits $[T]_l \overset{?}{=} 0^l$. If it is true, V_i is authenticated; and the secure channel with the session key $\mathsf{sk} = e(P,Q)^r$ is established. The correctness is as follows

$$\begin{aligned}\mathsf{sk}' &= e(\mathsf{Cha}, S_0)\\ &= e(r(P_{pub} + \mathcal{H}_0(\mathsf{pid}_0||\mathsf{ss}_b)P, \frac{1}{s + \mathcal{H}_0(\mathsf{pid}_0||\mathsf{ss}_b)}Q)\\ &= e(P,Q)^r = \mathsf{sk}\end{aligned}$$

Note that, because the RSU is trusted and can be identified by the vehicle, the unilateral authentication on vehicle here is suitable for the application scenarios.

Step 2. Once the secure channel is established, the vehicle V_i picks up each packet's Head and Auth from RSU by checking the relation

$$\mathsf{Auth} = C_2 \overset{?}{=} \mathcal{H}_1(k'||0), \text{ where } k' = e(\mathsf{Head}, S_0)$$

If the relation holds, V_i requests the packet's $\mathsf{Encrypted\text{-}Payload}$ from RSU and recovers the message M with k' from the encrypted-payload $C_3 = \mathbf{Enc}(k, M)$. The correctness is also as follows

$$\begin{aligned}k' &= e(\mathsf{Head}, S_0) = e(C_1, S_0)\\ &= e(x(P_{pub} + \mathcal{H}_0(\mathsf{pid}_0||\mathsf{ss}_b)P, \frac{1}{s + \mathcal{H}_0(\mathsf{pid}_0||\mathsf{ss}_b)}Q)\\ &= e(P,Q)^x = k\end{aligned}$$

In such a way, the message M is successfully received by the receiver V_i, and the SPF protocol ends. Note that, because the receiver V_i is mobile, when he happens to move to the location of the stationary source, he can also establish a secure channel with the source and directly get the message M.

V. Security Analysis

In this section, we will discuss the security issues of the proposed SPF protocol, i.e., the receiver-location privacy-preservation against an *external*, *global* and *passive* adversary $\mathcal{A}$ in VANET.

• *The packet $\mathcal{P}$ in the proposed SPF protocol can protect the receiver's identity privacy.* Since Head and $\mathsf{Encrypted\text{-}Payload}$ in the packet $\mathcal{P}$ is (C_1, C_3), where

$$\begin{cases} C_1 = x(P_{pub} + \mathcal{H}_0(\mathsf{pid}_0||\mathsf{ss}_b)P) \\ C_3 = \mathbf{Enc}(k, M)) \end{cases}$$

is a valid ciphertext of the anonymous identity-based encryption [6], (C_1, C_3) is provably secure and won't disclose the receiver's identity. At the same time, the Auth is $C_2 = \mathcal{H}_1(k||0)$, where $k = e(P,Q)^x$ is also irrelative to the receiver identity pid_0. Due to these two reasons, the packet $\mathcal{P}$ can protect the receiver identity privacy, which is a prerequisite for protecting receiver-location privacy.

• *The session key $\mathsf{sk} = e(P,Q)^r$ between the vehicle and RSU is semantic secure and can protect the receiver's session privacy.* Because the RSU is deployed at the socialspot, it thus will store many different vehicles' packets. If the session key is secure, it is hard for an adversary to link a packet to a receiver. In the following, based on the DBDH assumption, we first prove that the session key $\mathsf{sk} = e(P,Q)^r$ is semantic secure, which serves as the necessary condition for receiver's session privacy. Assume that there is an adversary $\mathcal{A}'$ which runs in a polynomial time and has a non-negligible advantage ϵ' to break the semantic security of the session key sk in the proposed SPF protocol, then we can use the capability of $\mathcal{A}'$ to construct another adversary $\mathcal{A}$ to break the DBDH problem, i.e., given $(x\widetilde{P}, y\widetilde{P}, z\widetilde{P}, V)$, decide whether or not $V = e(\widetilde{P}, \widetilde{P})^{xyz}$ for unknown $x, y, z \in \mathbb{Z}_q^*$. First, $\mathcal{A}$ sets the system parameters $P = x\widetilde{P}$ and $Q = z\widetilde{P}$, which implicitly shows that $Q = z\widetilde{P} = \frac{z}{x}P$. Then, $\mathcal{A}$ chooses a random number $t \in \mathbb{Z}_q^*$, and implicitly define the master key $s = \frac{t}{x} - \mathcal{H}_0(\mathsf{pid}_0||\mathsf{ss}_b) \bmod q$. Note that, due to unknown x, the implicitly defined s is also unknown to $\mathcal{A}$, but it doesn't affect the interactions between $\mathcal{A}$ and $\mathcal{A}'$. Next, $\mathcal{A}$ also implicitly defines a random number $r = \frac{y}{t} \bmod q$ used in the challenge Cha. Then, the challenge Cha is

$$\begin{aligned}\mathsf{Cha} &= r(P_{pub} + \mathcal{H}_0(\mathsf{pid}_0||\mathsf{ss}_b)P)\\ &= \frac{y}{t}\left(\left(\frac{t}{x} - \mathcal{H}_0(\mathsf{pid}_0||\mathsf{ss}_b)\right)P + \mathcal{H}_0(\mathsf{pid}_0||\mathsf{ss}_b)P\right)\\ &= \frac{y}{t}\left(\frac{t}{x}P - \mathcal{H}_0(\mathsf{pid}_0||\mathsf{ss}_b)P + \mathcal{H}_0(\mathsf{pid}_0||\mathsf{ss}_b)P\right)\\ &= \frac{y}{x}P = y\widetilde{P}\end{aligned}$$

In addition, $\mathcal{A}$ computes $V^{\frac{1}{t}} \in \mathbb{G}_T$ and uses it to encrypt a random number T with $[T]_l = 0^l$ as the response $\mathsf{Res} = \mathbf{Enc}(V^{\frac{1}{t}}, T)$. In the end, $\mathcal{A}$ sends $(P, Q, \mathsf{Cha}, \mathsf{Res})$ to $\mathcal{A}'$ for creating the attack environment of $\mathcal{A}'$.

Upon receiving $(P, Q, \mathsf{Cha}, \mathsf{Res})$, $\mathcal{A}'$ sends a request of guess on the session key. Then, A flips a coin $b \in \{0, 1\}$ and sends $V^{\frac{1}{t}}$ to $\mathcal{A}'$. When $\mathcal{A}'$ receives the $V^{\frac{1}{t}} \in \mathbb{G}_T$, he returns a bit b' as the guess of b.

Let E be the event that $(P, Q, \mathsf{Cha}, \mathsf{Res})$ are all valid. When the event E occurs, $\mathcal{A}'$ can launch his attacking capability, and we define $\mathbf{Adv}_{\mathcal{A}'}^{\mathsf{sk}} = 2\Pr[b' = b|\mathsf{E}] - 1 \geq \epsilon'$ to be the advantage probability of $\mathcal{A}'$, i.e.,

$$\Pr[b' = b|\mathsf{E}] = \frac{\mathbf{Adv}_{\mathcal{A}'}^{\mathsf{sk}}}{2} + \frac{1}{2} \geq \frac{\epsilon'}{2} + \frac{1}{2}$$

If the DBDH challenge $(x\widetilde{P}, y\widetilde{P}, z\widetilde{P}, V)$ is actually a bilinear pairing tuple $(x\widetilde{P}, y\widetilde{P}, z\widetilde{P}, V = e(\widetilde{P}, \widetilde{P})^{xyz})$, i.e., $\widetilde{b} = 0$ in $\mathbf{Exp}_{\mathcal{A}}^{\mathrm{DBDH}}$, then

$$V^{\frac{1}{t}} = e(\widetilde{P}, \widetilde{P})^{\frac{xyz}{t}} = e(x\widetilde{P}, z\widetilde{P})^{\frac{y}{t}} = e(P, Q)^r$$

and $\mathsf{Res} = \mathbf{Enc}(V^{\frac{1}{t}}, T)$ is also valid. Therefore,

$$\Pr\left[\mathbf{Exp}_{\mathcal{A}}^{\mathrm{DBDH}} = 1|\widetilde{b} = 0\right] = \Pr[b' = b|\mathsf{E}] = \frac{\mathbf{Adv}_{\mathcal{A}'}^{\mathsf{sk}}}{2} + \frac{1}{2}$$

However, if the DBDH challenge $(x\widetilde{P}, y\widetilde{P}, z\widetilde{P}, V)$ is a random tuple $(x\widetilde{P}, y\widetilde{P}, z\widetilde{P}, V = R)$, i.e., $\widetilde{b} = 1$ in $\mathbf{Exp}_{\mathcal{A}}^{\mathrm{DBDH}}$, we know $V^{\frac{1}{t}} \neq e(P, Q)^r$, the response Res is not valid, and the event E doesn't occur. Then, the guess of $\mathcal{A}$ is independent of b. Therefore,

$$\Pr\left[\mathbf{Exp}_{\mathcal{A}}^{\mathrm{DBDH}} = 1|\widetilde{b} = 1\right] = \Pr[b' = b|\neg\mathsf{E}] = \frac{1}{2}$$

Based on the above relations, we have

$$\begin{aligned}\mathbf{Adv}_{\mathcal{A}}^{\mathrm{DBDH}} &= \left|\Pr\left[\mathbf{Exp}_{\mathcal{A}}^{\mathrm{DBDH}} = 1|\widetilde{b} = 0\right]\right. \\ &\qquad \left. - \Pr\left[\mathbf{Exp}_{\mathcal{A}}^{\mathrm{DBDH}} = 1|\widetilde{b} = 1\right]\right| \\ &= \left|\frac{\mathbf{Adv}_{\mathcal{A}'}^{\mathsf{sk}}}{2} + \frac{1}{2} - \frac{1}{2}\right| = \frac{\mathbf{Adv}_{\mathcal{A}'}^{\mathsf{sk}}}{2} \geq \frac{\epsilon'}{2}\end{aligned}$$

This result indicates that the session key $\mathsf{sk} = e(P, Q)^r$ is semantic secure in the proposed SPF protocol, as required. Furthermore, because the session key $\mathsf{sk} = e(P, Q)^r$ is semantic secure, when it is used to encrypt the communications between the vehicle and the RSU, the vehicle's session privacy is protected, i.e., an adversary $\mathcal{A}$ can't know which packet the vehicle has picked up from the RSU.

- *The receiver's sensitive locations are unlinkable in the proposed SPF protocol.* As we know, each vehicle V_i holds a family of unlinkable pseudo-IDs and the corresponding key materials, and only pseudo-ID pid_0's key is related to the socialspot ss_b, other keys are independent of the locations. Therefore, when V_i periodically changes its pseudo-IDs on the road, other sensitive locations of V_i are unlinkable.

In summary, we can clearly see that the proposed SPF protocol can protect the receiver-location privacy in VANET.

VI. Performance Evaluation

In this section, we evaluate the average-case performance of the proposed SPF protocol, using a custom simulator built in Java. The performance metrics gauged in the evaluation are average packet delivery ratio (DR) and average packet delay (AD), where the DR is defined as the average ratio of the packets successfully reach their destinations with respect to those generated by the sources within a given time period, and the AD is defined as the average between when a packet is generated at source and when it is successfully delivered to its destination.

A. Simulation Settings

In the simulation, $N = \{40, 80\}$ vehicles with transmission radius of 300 meters and velocity varying from 40 km/h to 60 km/h are moving in an interest area of $10,000 \times 10,000$ m^2, as shown in Fig. 5. In addition, 6 socialspots are randomly chosen in the region, each socialspot is deployed with a storage-huge RSU to help with temporarily storing the packets.

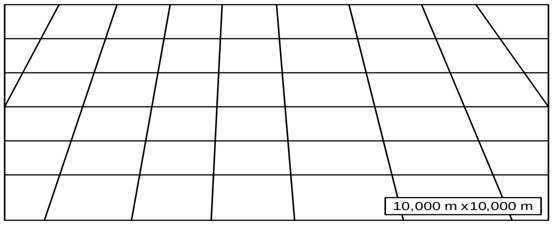


Fig. 5. Interest area considered for simulation

Mobility model. In VANET, the performance of packet forwarding is highly contingent upon the mobility of the vehicles. Meanwhile, since the rationale of socialspot tactic is based on the assumption that each vehicle often visits at least one socialspot, we consider a special but more realistic mobility model in the simulation. Set each vehicle V_i's trajectory $\mathsf{Tr}_i = \{\mathsf{tr}_1, \mathsf{tr}_2, \cdots\}$ contain the same number of locations, i.e., $|\mathsf{Tr}_i| = S = \{3, 5\}$. In the trajectory Tr_i, at least one location belongs to the socialspots, and the rest locations are randomly distributed in the area. In the simulation, each vehicle moves around his individual trajectory. Specifically, each vehicle V_i first equally chooses one location in his trajectory $\mathsf{Tr}_i = \{\mathsf{tr}_1, \mathsf{tr}_2, \cdots\}$, and gets there using the map-based shortest path routing. After reaching the destination, with 2-minute pause time, the vehicle again equally chooses a new destination in Tr_i and repeats the above.

The detailed parameter settings in the simulations are summarized in Table I. We perform the experiments with different $N = \{40, 80\}$ and different $S = \{3, 5\}$. For each case, we run the simulation 10 hours, and the average delivery ratio and average packet delay over 50 runs are reported.

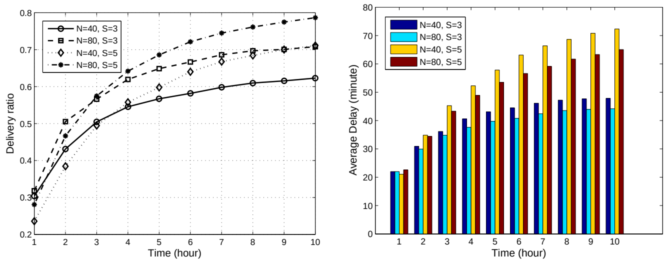
B. Simulation Results

Fig. 6-(a) shows the average DR varies with the time period from 1 hour to 10 hours. From the figure, we can observe that, with the increase of time, the DR will increase accordingly.

TABLE I
SIMULATION SETTINGS

Parameter	Setting
Simulation area	$10,000 \times 10,000$ m^2
Simulation duration	10 hours
Number of socialspots, RSU storage	6, 10000 M
Number of vehicles	$N = \{40, 80\}$
Number of locations in vehicle's trajectory	$S = \{3, 5\}$
Vehicle velocity and transmission	40 $\sim$ 60 km/h, 300 m
Vehicle storage and waittime	20 M, 2 minutes
Package size, generation interval	1 M, 5 minutes

When the number of socialspots S is fixed, the DR in $N = 80$ case is higher than that in $N = 40$ case. The reason is that, when more vehicles move around the area, more packets can be carried to the socialspots, then the receivers can get their packets when they visit the socialspots. Furthermore, when the number of vehicles N is fixed, the DR in $S = 5$ case is lower than that in $S = 3$ case at the initial stage and will be higher in the late stage. The reason for the phenomena is that at the initial stage, the number of generated packets is small, fewer packets should be carried to the socialspots. When $S = 5$, receivers have lower frequency to visit the socialspots to pick up their packets. Therefore, the DR is lower than that in $S = 3$ case. However, in the late stage, the number of generated packets is larger. When $S = 5$, vehicles can carry more packets to the socialspots. Accordingly, when the receivers visit the socialspots, they can receive more packets. Therefore, the DR is larger than that in $S = 3$ case.



(a) delivery ratio

(b) average delay

Fig. 6. The average packet delivery ratio and average delay versus specified time period

Fig. 6-(b) shows the AD varies with the time period from 1 hour to 10 hours corresponding to the DR in Fig. 6-(a). From the figure, we can see, with the increase of time, the AD will also increase, but the increased delay can improve the DR. When the number of socialspots S is fixed, 80 vehicles can more quickly carry packets to the socialspots than 40 vehicles. As a result, the AD in $N = 80$ case is lower than that in $N = 40$ case. Meanwhile, when the number of vehicles N is fixed, vehicles will visit more locations in $S = 5$ than that in $S = 3$ case. Therefore, the AD in $S = 3$ is lower than that in $S = 5$ case, but the corresponding DR is also lower.

VII. RELATED WORK

Recently, several research works have been reported [3], [7], [8], which are closely related to the proposed SPF protocol. Jian et al. [7] study the packet-tracing attack and propose a location privacy routing (LPR) protocol in combination with fake packet injection technique to protect receiver-location privacy in wireless sensor networks. In [8], Cheng et al. propose an efficient packet cloaking routing mechanism to protect the privacy of a receiver. The main idea in packet cloaking is to transmit multiple copies of a sent packet to a selected group of k receivers, so that an adversary may only identify the true receiver with a probability of $1/k$. Although both LPR protocol and packet cloaking mechanism can protect the receiver-location privacy, they can't be applied to VANET, since the receivers in VANET are vehicles, which move around in the city environment. Our previous work SPRING [3] studies how to utilize the vehicle mobility model, i.e., map-based shoretest routing, to improve the performance of packet forwarding in vehicular DTN. However, SPRING only addresses the stationary receiver, and doesn't consider the receiver-location privacy. Different from SPRING, the proposed SPF protocol considers the more realistic mobility model, which not only protects the receiver-location privacy, but also improve the performance of packet delivery.

VIII. CONCLUSIONS

In this paper, based on the "Sacrificing the Plum Tree for the Peach Tree" — one of the Thirty-Six Strategies of Ancient China, we have proposed a socialspot-based packet forwarding (SPF) protocol for protecting receiver-location privacy in VANET. Detailed security analysis has shown that, only when a receiver sacrifices one socialspot that he often visits, all his other sensitive locations can be protected against an external, global, passive adversary. In addition, through extensive performance evaluation, we have demonstrated that the temporarily storing packets at socialspots can achieve much better efficiency in terms of delivery ratio and average delay in VANET. In our future work, we will further evaluate its effectiveness and workability in realistic scenarios.

REFERENCES

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

[2] A. Wasef and X. Shen, "REP: Location privacy for vanets using random encryption periods," *ACM Mobile Networks and Applications (MONET)*, vol. 15, no. 1, pp. 172–185, 2010.

[3] R. Lu, X. Lin, and X. Shen, "Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *INFOCOM 2010*, San Diego, California, USA, March 2010, pp. 1–9.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, 2003.

[5] Z. Chai, Z. Cao, and R. Lu, "Efficient password-based authentication and key exchange scheme preserving user privacy," in *WASA*, 2006, pp. 467–477.

[6] M. Izabachene and D. Pointcheval, "New anonymity notions for identity-based encryption," in *SCN '08*, ser. LNCS 5229, 2008, pp. 375–391.

[7] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting receiver-location privacy in wireless sensor networks," in *INFOCOM 2007*, Anchorage, AK, May 2007, pp. 1955 – 1963.

[8] R. Cheng, D. K. Y. Yau, and J. Fu, "Packet cloaking: Protecting receiver privacy against traffic analysis," in *3rd IEEE Workshop on Secure Network Protocols*, 2007, pp. 1–6.