This paper was presented as part of the main technical program at IEEE INFOCOM 2011

STAP: A Social-Tier-Assisted Packet Forwarding Protocol for Achieving Receiver-Location Privacy Preservation in VANETs

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

***Abstract*—Receiver-location privacy is an important security requirement in privacy-preserving Vehicular Ad hoc Networks (VANETs), yet the unavailable receiver's location information makes many existing packet forwarding protocols inefficient in VANETs. To tackle this challenging issue, in this paper, we propose an efficient social-tier-assisted packet forwarding protocol, called STAP, for achieving receiver-location privacy preservation in VANETs. Specifically, by observing the phenomena that vehicles often visit some social spots, such as well-traversed shopping malls and busy intersections in a city environment, we deploy storage-rich Roadside Units (RSUs) at social spots and form a virtual social tier with them. Then, without knowing the receiver's exact location information, a packet can be first forwarded and disseminated in the social tier. Later, once the receiver visits one of social spots, it can successfully receive the packet. Detailed security analysis shows that the proposed STAP protocol can protect the receiver's location privacy against an *active* global adversary, and achieve vehicle's conditional privacy preservation as well. In addition, performance evaluation via extensive simulations demonstrates its efficiency in terms of high delivery ratio and low average delay.**

***Keywords* – VANETs, Packet forwarding, Social-tier-assisted, Receiver-location privacy preservation**

I. Introduction

Vehicular Ad hoc Network (VANET) has recently attracted increasing attention and will be expected as a promising approach to not only improving road safety but also providing various value-added infotainment services on the road [1]. Typically, in a VANET, each vehicle is equipped with an On-Board Unit (OBU) communication device, which allows vehicles to talk to each other, i.e., vehicle-to-vehicle (V-2-V) communication, as well as Roadside Units (RSUs), i.e., vehicle-to-infrastructure (V-2-I) communication. Therefore, compared with the traditional mobile ad hoc networks, the hybrid of V-2-V and V-2-I communications makes VANET more promising. In the near future, VANET will serve as a general platform for the development of any vehicle-centered applications enabled by V-2-V and V-2-I communications such as emergency braking warning. Nevertheless, there are still many challenges need to be conquered before it becomes reality. One of the challenging issues is how to protect vehicles' location privacy in VANETs. In general, a VANET is implemented in a city environment, and the vehicles' locations are also tightly related to the people who drive them. If the vehicle's location is not protected, people may not be willing to accept VANET, since an adversary may learn a user's health conditions, political and/or religious affiliations based on the locations that the user regularly visits [2]. Therefore, location privacy has become one of the most concerns for the successful implementation of VANET.

Furthermore, most vehicle applications require information exchange, for example, regarding traffic and road conditions, among moving vehicles and stationary RSUs. Unfortunately, an end-to-end path between communication participants may never exist as vehicles are constantly moving with frequently changing network topology. Hence, for VANET to be effective in enabling a variety of vehicle applications for road safety and efficiency improvement in current road transport system, it will require all network nodes to store, carry and forward packets to intermediate nodes within its communication range in an opportunistic way, also called opportunistic data forwarding. The behavior of VANET can be modeled as Delay Tolerant Networks (DTNs), also known as Vehicular Delay Tolerant Networks (VDTNs). Recently, many packet routing protocols suitable for VANET environment have been proposed [3]–[6], and these existing protocols assume that sender(s) knows where the packers' destination is. However, once the receiver(s) wants to keep its location privacy, these protocols don't work well. An intuitive solution to achieve the receiver location privacy in VANETs is using the flooding technique to forward the packet, i.e., the Epidemic routing [7], where all vehicles receiving a packet buffer and carry the packet as they move, passing packet on to new vehicles that they encountered. Although the Epidemic routing can protect the receiver location privacy, it heavily consumes the network resources and is very inefficient when the vehicle buffer is constrained. In our previous works [8], [9], we have presented two packet forwarding protocols for VANET, which can protect the receiver's location privacy against a *passive* global adversary. However, if the adversary is *active* and controls some vehicles, which is highly possible, the receiver's location still could be disclosed once some controlled vehicles are involved in packet forwarding. Therefore, how to design an efficient packet forwarding protocol while protecting the receiver's location privacy against an *active* global adversary is a very challenging issue in VANETs.

In this paper, we address the above challenging issue by devising a social-tier-assisted packet forwarding protocol, named STAP, for achieving receiver-location privacy preservation in VANETs, where the social tier is a virtual tier formed

by social spots, such as well-traversed shopping malls and busy intersections in a city environment. The proposed STAP protocol is characterized by disseminating packets to social tier in order to not only improve the packet delivery performance but also protect receiver-location privacy against an active global adversary. Specifically, our major contributions are as follows:

• *Fully utilizing people's lifestyle in city to design social-tier-assisted packet forwarding protocol.* One kind of lifestyle of people in city is that they often drive vehicles to visit one social spot, i.e., a shopping mall. Usually, after visiting one social spot, they will visit another one. Therefore, when storage-rich RSUs are deployed at social spots, many vehicles can often access RSUs to store and fetch packets. Thus, it is feasible to design an efficient social-tier-assisted packet forwarding (STAP) protocol in VANETs. In addition, the "store-forward" function of RSUs make the social tier as a huge mix server, which can prevent the global adversary from eavesdropping.

• *Extensive simulation studies of advantages of STAP over Epidemic routing.* By detailed simulations, we show that, in order to achieve the receiver-location privacy preservation, STAP takes substantial advantages over the Epidemic routing in terms of high delivery ratio and low average delay, especially when the vehicle buffer is constrained.

The remainder of this paper is organized as follows. In Section II, we formalize the system models and identify our design goal. Then, we present the STAP protocol in Section III, followed by the security analysis and performance evaluation in Section IV and Section V, respectively. We also discuss some related works in Section VI. Finally, we draw our conclusions in Section VII.

II. System Models and Design Goal

In this section, we first formalize the system models including social-tier-assisted VANET network model, social-tier dissemination model and location privacy threat model. Then, we identify our design goal.

A. Social-tier-assisted VANET network model

We consider a social-tier-assisted VANET deployed in a city environment, which includes a large number of vehicles $\mathcal{V} = \{V_1, V_2, \cdots\}$ and a social spot set $\mathcal{S} = \{S_1, S_2, \cdots, S_n\}$, as shown in Fig. 1. Each vehicle $V_i \in \mathcal{V}$ first sets a destination in the area, then moves to the destination by following the road-based shortest-path routing with some velocity v_i; after reaching the destination, V_i repeats the above procedure. In addition, each V_i is equipped with OBU device which allows them to communicate with each other when they encounter, and further makes it feasible to establish a vehicle-based "store-carry-forward" packet forwarding protocol in VANET. However, since OBU is usually a buffer-constraint device, a vehicle can't always serve as a mobile relay to carry packets if the OBU's buffer is insufficient.

The social spot set $\mathcal{S} = \{S_1, S_2, \cdots, S_n\}$ forms a social tier in VANET. Each social spot $S_i \in \mathcal{S}$ is informally referred to as the spot that many vehicles will often visit, such as the shopping malls. Let the vehicle arrival at each social spot in the area be the Poisson process, we can formally define S_i as a social spot if its vehicle arrival rate $\lambda_i \geq \lambda_T$, where λ_T is a predefined threshold arrival rate, and the corresponding social spot set $\mathcal{S}$ becomes $\mathcal{S} = \{S_i | \lambda_i \geq \lambda_T\}$. At each social spot $S_i \in \mathcal{S}$, there is a trusted and storage-rich RSU device R_i deployed, which provides a prerequisite for the social tier $\mathcal{S}$ serving as the stationary relay to temporarily assist in storing and forwarding packets in VANET.

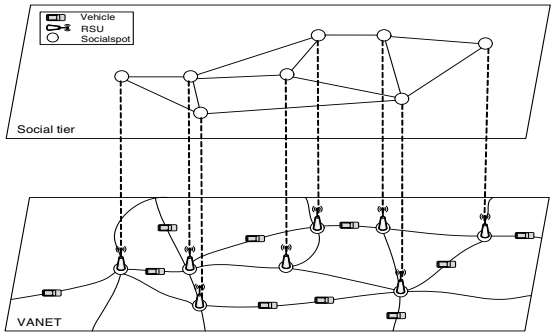


Fig. 1. Social-tier-assisted VANET network model under consideration

B. Social-tier dissemination model

In reality, a large number of vehicles $\mathcal{V}$ often visit one social spot and then move to another one, the traffic between any two social spots is high and nearly stable for some period. As a result, social spots $\{S_1, S_2, \cdots, S_n\}$ can not only temporarily store the packets but also quickly disseminate the packets in social tier $\mathcal{S}$. Here, we model the social tier $\mathcal{S} = \{S_i | \lambda_i \geq \lambda_T\}$ as a connected graph and study the packet dissemination model in social tier $\mathcal{S}$. Specifically, we model the social tier as a direct graph $\mathcal{G} = (\mathbf{V}, \mathbf{E})$, where the vertices $\mathbf{V}$ is the set of social spots $\{S_1, S_2, \cdots, S_n\}$ in $\mathcal{S}$, the degree of each vertex S_i is defined as $\deg(S_i) = \lambda_i$, and $\mathbf{E}$ is the set of directed traffic edges. A directed traffic edge e_{ij} belonging to $\mathbf{E}$ is defined as $e_{ij} = \lambda_{ij}$ if *there exists a road directly connecting S_i and S_j, and no other social spot $S_k \in \mathcal{S}/\{S_i, S_j\}$ lying between S_i and S_j on the road, and the vehicle arrival from S_i to S_j follows a Poisson process with arrival rate $\lambda_{ij} > 0$*; and $e_{ij} = 0$ otherwise. Then, the degree of each vertex S_i, $\deg(S_i) = \lambda_i$, can be written as

$$\deg(S_i) = \lambda_i = \lambda_i^* + \sum_{S_j \in \mathcal{S}, j \neq i} e_{ji} = \lambda_i^* + \sum_{S_j \in \mathcal{S}, j \neq i} \lambda_{ji} \quad (1)$$

where λ_i^* is the cumulative vehicle arrival rate whose sources are not in $\{S_1, S_2, \cdots, S_n\}$, but the destination is S_i.

Traffic Edge Delay Weight (TEDW): For any traffic edge $e_{ij} \in \mathbf{E}$ with $e_{ij} = \lambda_{ij} > 0$, we know the vehicle inter-arrival time follows the exponential distribution with the probability density function (pdf) $f(t) = \lambda_{ij} e^{-\lambda_{ij} t}$, where $t \geq 0$. Assume that the distance between S_i and S_j is $d(i, j)$ and the average velocity of vehicles on e_{ij} is $E[v_{ij}]$, we define e_{ij}'s TEDW as

$$t_{ij} = \int_0^\infty t f(t) dt + \frac{d(i,j)}{E[v_{ij}]} = \frac{1}{\lambda_{ij}} + \frac{d(i,j)}{E[v_{ij}]} \quad (2)$$

where $\frac{1}{\lambda_{ij}}$ is average interval (waiting) time and $\frac{d(i,j)}{E[v_{ij}]}$ is the average propagation time from S_i to S_j.

Shortest-Delay-Path (SDP): Since $\mathcal{G} = (\mathbf{V}, \mathbf{E})$ is a connected graph and each edge $e_{ij} = \lambda_{ij} > 0$ is marked with TEDW t_{ij}, we can easily use the Dijkstra algorithm with delay weight to calculate the SDP from one social spot S_i to any other social spot $S_j \in \mathcal{S}/\{S_i\}$, i.e., $\text{SDP}_{ij} = e_{ik_1}, e_{k_1k_2}, \cdots, e_{k_lj}$, and obtain the corresponding average path delay

$$\begin{aligned} T_{ij} &= t_{ik_1} + t_{k_1k_2} + \cdots + t_{k_lj} \\ &= \frac{1}{\lambda_{ik_1}} + \frac{1}{\lambda_{k_1k_2}} + \cdots + \frac{1}{\lambda_{k_lj}} + \frac{d(i,k_1)}{E[v_{ik_1}]} + \\ &\quad \frac{d(k_1,k_2)}{E[v_{k_1k_2}]} + \cdots + \frac{d(k_l,j)}{E[v_{k_lj}]} \end{aligned} \tag{3}$$

Delay Bound of Social-tier Dissemination: We define the delay bound of dissemination from a specific social spot S_i as

$$T_i = \max\{T_{ij} | S_i, S_j \in \mathcal{S}, j \neq i\} \tag{4}$$

Then the average delay bound of social-tier dissemination is

$$T = \frac{1}{n}\sum_{i=0}^{n} T_i = \frac{1}{n}\sum_{i=0}^{n} \max\{T_{ij} | S_i, S_j \in \mathcal{S}, j \neq i\} \tag{5}$$

which indicates that once a packet is forwarded to the social tier in VANETs, i.e., to a specific social spot in social tier firstly, the packet can be quickly disseminated to the whole social tier $\mathcal{S}$ with average time T. Thus, it can guarantee the performance of packet forwarding in terms of average delay in VANETs.

C. Location privacy threat model

The goal of the adversary aims to break the vehicle location privacy, i.e., obtaining the exact vehicle location at a specific time, and/or linking multiple locations that a vehicle once visited. Specifically, in our location privacy threat model, we consider an active global adversary equipped with radio devices to track vehicle's location. Here, *Global* shows the adversary has full traffic information of the whole VANETs, and *Active* denotes the adversary can not only eavesdrop the V-2-V and V-2-I communications, but also control some vehicles. Note that, the active global adversary can also use cameras to track vehicle in a city area. However, the cost is much high than that of radio based eavesdropping. Therefore, the cameras based global eavesdropping is beyond the scope of this paper.

D. Design goal

Our design goal in this paper is to develop an efficient packet forwarding protocol while achieving receiver-location privacy preservation in privacy-preserving VANETs. Especially, the following two requirements should be satisfied:

- The proposed receiver-location privacy preserving packet forwarding protocol shouldn't degrade the packet delivery performance, i.e., high delivery ratio and lower average delay should be guaranteed.
- Vehicle conditional privacy preservation (CPP) [10] should also be satisfied, which thus can serve the second line of defense to resist the possible inside attacks, i.e., source bogus attack and black/grey hole attacks [8].

III. Proposed STAP Protocol

In this section, we propose our social-tier-assisted packet forwarding protocol (STAP) for protecting receiver's location privacy. Before proceeding the details of our protocol, we first review the pairing technique which will serve as the basis of the proposed STAP protocol.

A. Pairing Technique

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative cyclic groups of the same prime order q, and g be a generator of $\mathbb{G}$. Suppose $\mathbb{G}$ and $\mathbb{G}_T$ are equipped with a pairing, i.e., a non-degenerated and efficiently computable bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ such that $e(g,g) \neq 1_{\mathbb{G}_T}$ and $e(u^a, v^b) = e(u,v)^{ab} \in \mathbb{G}_T$ for all $a, b \in \mathbb{Z}_q^*$ and any $u, v \in \mathbb{G}$. We refer to [11], [12] for a more comprehensive description of pairing technique, and complexity assumptions.

Definition 1: A bilinear parameter generator $\mathcal{G}en$ is a probabilistic algorithm that takes a security parameter κ as input, and outputs a 5-tuple $(q, \mathbb{G}, \mathbb{G}_T, g, e)$, where q is a κ-bit prime number, $\mathbb{G}, \mathbb{G}_T$ are two groups with order q, $g \in \mathbb{G}$ is a generator, and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a non-degenerated and efficiently computable bilinear map, i.e., $e(g,g) \neq 1_{\mathbb{G}_T}$.

B. The Description of STAP Protocol

The proposed STAP protocol mainly consists of the following four phases: system initialization phase, packet sending phase, social-tier dissemination phase, and packet receiving phase, as shown in Fig. 2.

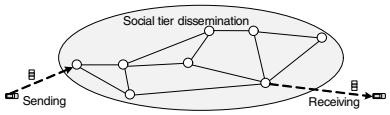


Fig. 2. Proposed STAP protocol for achieving receiver-location privacy

1) System initialization phase: For a single-authority VANET under consideration, we assume a trusted authority (TA) will bootstrap the whole system. Specifically, given the security parameter κ, TA first generates the bilinear parameters $(q, \mathbb{G}, \mathbb{G}_T, g, e)$ by running $\mathcal{G}en(\kappa)$, and chooses one secure symmetric encryption algorithm $\mathbf{Enc}()$, i.e., AES, and two secure cryptographic hash functions H_0 and H, where $H_0 : \{0,1\}^* \to \mathbb{G}$ and $H : \{0,1\}^* \to \mathbb{Z}_q^*$. In addition, TA also chooses two elements (h_1, h_2) in $\mathbb{G}$, two random numbers $(a, \alpha) \in \mathbb{Z}_q^*$ as the *master key*, and computes $b = H(a)$, $A = g^a$, and $e(g,g)^\alpha$. Finally, TA keeps the *master key* (a, b, α) secretly, and publishes the system parameters $\text{params} = (q, \mathbb{G}, \mathbb{G}_T, g, e, H_0, H, h_1, h_2, A, e(g,g)^\alpha, \mathbf{Enc}())$.

In a specific city area, TA first investigates some social spots $S = \{S_1, S_2, \cdots, S_n\}$, where the vehicle arrival rate λ_i of each $S_i \in \mathcal{S}$ is higher than a threshold λ_T, i.e., $\lambda_i \geq \lambda_T$. Then, TA deploys a trusted RSU device R_i at each social spot S_i, and authorizes the key materials to R_i by the following steps:

- choose two random numbers $(t_{i1}, t_{i2}) \in \mathbb{Z}_q^*$, and compute the secret key $sk_i = (g^{\alpha + at_{i1}}, g^{t_{i1}}, g^{t_{i2}}, h_1^{t_{i1}} h_2^{t_{i2}})$;

- equip the RSU R_i at social spot S_i with sk_i as well as params.

When a vehicle $V_i \in \mathcal{V}$ registers itself in the system, TA runs the following steps:

- check the eligibility of V_i, generate a family of pseudo-IDs $\text{PID}_i = \{pid_{i0}, pid_{i1}, \cdots\}$ for V_i, where each pid_{ij} with 28-byte length is encrypted from the real identity V_i and a random number $R_{ij} \in \mathbb{Z}_q^*$ with the master key b, i.e., $pid_{ij} = \mathbf{Enc}_b(V_i||R_{ij})$;
- for each $pid_{ij} \in \text{PID}_i$, compute the identity-based private key $sk_{ij} = H_0(pid_{ij})^a$;
- grant a family of pseudo-IDs $\text{PID}_i = \{pid_{i0}, pid_{i1}, \cdots\}$ together with the corresponding private keys and params to V_i.

After receiving $\text{PID}_i = \{pid_{i0}, pid_{i1}, \cdots\}$, V_i exclusively uses pid_{i0} for receiving encrypted data from others, i.e., the pseudo-id pid_{i0} is known to the packet senders in VANETs; and uses $\text{PID}_i/\{pid_{i0}\}$ for achieving location privacy, i.e., periodically changing the pseudo-ids on the road.

2) Packet sending phase: Assume that a source S with pseudo-id pid_{s0} wants to send a sensitive message m to a vehicle $V_d \in \mathcal{V}$, where the pseudo-id pid_{d0} of V_d is known by S. However, since the receiver-location information is protected, the source S doesn't know where the receiver V_d is. To fulfill such receiver-location privacy preserving packet forwarding in VANETs, the source S runs the following steps.

Step 1. The source S first makes an id-based signature $sig(m)$ [12] with respective to pid_{s0} for achieving source authentication. Then S chooses a random number $r \in \mathbb{Z}_q^*$ and uses the receiver's pseudo-id pid_{d0} to encrypt the sensitive message m together with $pid_{s0}||sig(m)$ as $c = (c_1, c_2)$, where

$$c_1 = g^r, c_2 = \mathbf{Enc}_{k_0}(pid_{s0}||m||sig(m)) \tag{6}$$

with $k_0 = H\left(e(A, H_0(pid_{d0}))^r\right)$.

Step 2. S chooses another random number $s \in \mathbb{Z}_q^*$ and encrypts $M = pid_{d0}||c$ into the single-attribute-based ciphertext $C = (C_1, C_2, C_3, C_4)$ [13], where

$$\begin{aligned} &C_1 = \mathbf{Enc}_k(M) \text{ with } k = H(e(g,g)^{\alpha s}); \\ &C_2 = g^s; C_3 = A^s h_1^{-s}; C_4 = h_2^{-s} \end{aligned} \tag{7}$$

Then, S waits a passing-by vehicle to help carrying the packet C to one social spot in social tier $\mathcal{S}$. Note that the single-attribute-based encryption enables all legal RSUs at social spots with different private keys to recover the same $M = pid_{d0}||c$ from $C = (C_1, C_2, C_3, C_4)$, which is essential for the success of the receiver-location privacy preservation in VANETs.

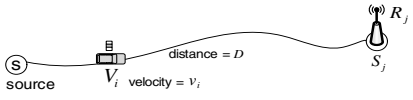


Fig. 3. Vehicle V_i carries the packet C from the source S to the social spot S_j with velocity v_i

Suppose that a passing-by vehicle $V_i \in \mathcal{V}$ has available buffer space and is willing to help forwarding the packet C to one social spot $S_j \in \mathcal{S}$, the source S and the passing-by V_i will do the following interactive operations.

- V_i first picks up the current timestamp/location information CTL with 8-byte length, and randomly uses a fresh pseudo-id $pid_{ia} \in \text{PID}_i/\{pid_{i0}\}$ and its corresponding private key sk_{ia} to make a signature $sig(\text{CTL})$ with 128-byte length, and sends $pid_{ia}||\text{CTL}||sig(\text{CTL})$ to S.
- After checking the validity of $sig(\text{CTL})$, S keeps $\text{Log}: pid_{ia}||\text{CTL}||sig(\text{CTL})$ for the late exceptional case process, i.e., tracking the inside black/grey hole attackers. Then, S uses a fresh pseudo-id $pid_{sa} \in \text{PID}_s/\{pid_{s0}\}$ and its corresponding private key sk_{sa} to make a signature $sig(\text{CTL}||H(C))$, and sends $pid_{sa}||\text{CTL}||C||sig(\text{CTL}||H(C))$ to V_i.
- Upon receiving $pid_{sa}||\text{CTL}||C||sig(\text{CTL}||H(C))$, V_i checks the validity of $sig(\text{CTL}||H(C))$, and keeps $\text{Log}: pid_{sa}||\text{CTL}||H(C)||sig(\text{CTL}||H(C))$ for the late exceptional case process, i.e., identifying the source bogus message attack. Then, V_i carries the packet C from the source to the social spot $S_j \in \mathcal{S}$ with velocity v_i, as shown in Fig. 3. Suppose the distance between the source S and social spot S_j is $d(\text{S}, j)$, then the source S can estimate the packet C will be carried to the social spot S_j after a time period $\tau_1 = \frac{d(\text{S},j)}{v_i}$.

Assume the length of packet C follows the exponential distribution with mean 3 Mb. By setting the packet transmission bitrate to be 5 Mbps [14], the transmission range and the velocity of vehicle are 300 m, 60 km/h, respectively, the packet transmission between S and V_i can be implemented within their communication interval 36.1 s [8].

After the time period τ_1, V_i arrives at the social spot S_j, and meets the RSU R_j deployed at S_j. Then, V_i and R_j make the mutual authentication, as shown in Fig. 4, and the detailed steps are as follows:

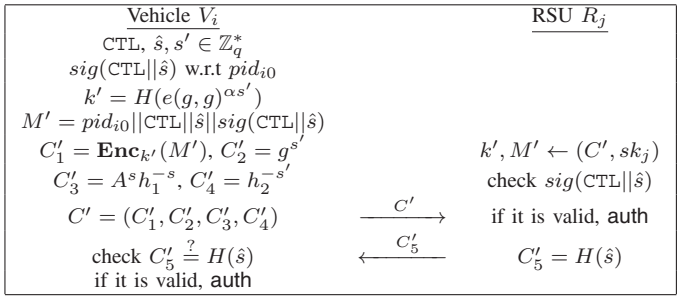


Fig. 4. Mutual authentication between the vehicle V_i and the RSU R_j

Step 1. V_i first chooses a session key $\hat{s} \in \mathbb{Z}_q^*$, picks up the CTL, and uses the pseudo-id $pid_{i0} \in \text{PID}_i$ to make an id-based signature $sig(\text{CTL}||\hat{s})$. Then, V_i chooses a random number $s' \in \mathbb{Z}_q^*$, and encrypts $M' = pid_{i0}||\text{CTL}||\hat{s}||sig(\text{CTL}||\hat{s})$ into $C' = (C'_1, C'_2, C'_3, C'_4)$, where

$$\begin{aligned} &C'_1 = \mathbf{Enc}_{k'}(M') \text{ with } k' = H(e(g,g)^{\alpha s'}); \\ &C'_2 = g^{s'}; C'_3 = A^{s'} h_1^{-s'}; C'_4 = h_2^{-s'} \end{aligned} \tag{8}$$

In the end, V_i sends C' to the RSU R_j.

Step 2. Upon receiving $C' = (C'_1, C'_2, C'_3, C'_4)$, the RSU R_j uses its private key $sk_j = (g^{\alpha+at_{j1}}, g^{t_{j1}}, g^{t_{j2}}, h_1^{t_{j1}} h_2^{t_{j2}})$ to compute

$$\begin{aligned} & \frac{e(C'_2, g^{\alpha} g^{at_{j1}})}{e(g^{t_{j1}}, C'_3) \cdot e(g^{t_{j2}}, C'_4) \cdot e(h_1^{t_{j1}} h_2^{t_{j2}}, C'_2)} \\ = & \frac{e(g^{s'}, g^{\alpha} g^{at_{j1}})}{e(g^{t_{j1}}, g^{as'} h_1^{-s'}) \cdot e(g^{t_{j2}}, h_2^{-s'}) \cdot e(h_1^{t_{j1}} h_2^{t_{j2}}, g^{s'})} \\ = & \frac{e(g^{s'}, g^{\alpha}) e(g^{s'}, g^{at_{j1}})}{e(g^{t_{j1}}, g^{as'}) \cdot e(g, h_1^{-s't_{j1}} h_2^{-s't_{j2}}) \cdot e(h_1^{t_{j1}} h_2^{t_{j2}}, g^{s'})} \\ = & e(g^{s'}, g^{\alpha}) = e(g,g)^{\alpha s'} \end{aligned} \quad (9)$$

and $k' = H(e(g,g)^{\alpha s'})$. Then, R_j recovers $M' = pid_{i0}||\texttt{CTL}||\hat{s}||sig(\texttt{CTL}||\hat{s})$ from C'_1 with k', and checks the validity of $sig(\texttt{CTL}||\hat{s})$. If $sig(\texttt{CTL}||\hat{s})$ is valid, the vehicle V_i with pseudo-id pid_{i0} is authenticated, and R_j returns $C'_5 = H(\hat{s})$ back to V_i.

Step 3. After verifying the received $C'_5 = H(\hat{s})$, V_i can also authenticate the RSU R_j is valid, since only the authorized RSUs deployed at social spots can recover the session key $\hat{s}$. As a result, the mutual authentication between V_i and R_j is achieved.

After the mutual authentication between the vehicle and the RSU, V_i forwards the packet C to R_j by the following interactive operations.

- For achieving the data integrity of C, V_i first computes the message authentication code $\texttt{MAC} = H(C||\hat{s})$ and sends $C||\texttt{MAC}$ to R_j.
- On receiving $C||\texttt{MAC}$, R_j uses the session key $\hat{s}$ to check whether $\texttt{MAC} = H(C||\hat{s})$. If it holds, the packet $C = (C_1, C_2, C_3, C_4)$ is verified. Then, R_j again uses the private key $sk_j = (g^{\alpha+at_{j1}}, g^{t_{j1}}, g^{t_{j2}}, h_1^{t_{j1}} h_2^{t_{j2}})$ on C to compute

$$\begin{aligned} & H\left(\frac{e(C_2, g^{\alpha} g^{at_{j1}})}{e(g^{t_{j1}}, C_3) \cdot e(g^{t_{j2}}, C_4) \cdot e(h_1^{t_{j1}} h_2^{t_{j2}}, C_2)}\right) \\ = & H(e(g,g)^{\alpha s}) = k \end{aligned} \quad (10)$$

  and recovers $M = pid_{d0}||c$ from $C_1 = \mathbf{Enc}_k(M)$ with k. In the end, R_j temporarily stores the recovered $pid_{d0}||c$, and the encrypted packet C enters into the social-tier dissemination phase.

3) Social-tier dissemination phase: In this phase, the packet C will be disseminated to the whole social tier $\mathcal{S}$ by the large number of vehicles moving among different social spots. For example, as shown in Fig. 5, the packet C can be propagated from social spot S_j to the neighboring social spot S_i through vehicle $V_k \in \mathcal{V}$. Specifically, each social spot $S_j \in \mathcal{S}$ who holds the packet C will invoke the Algorithm 1 to disseminate the packet C.

In Algorithm 1, before forwarding the packet C to V_k, the RSU R_j at S_j first uses the same steps in Fig. 4 to make the mutual authentication with the vehicle V_k. Only if V_k with a pseudo-id pid_{kl} is authenticated, R_j forwards the packet C to V_k and keeps $\texttt{Log}: pid_{kl}||H(C)$ for the late exceptional case process. When V_k arrives at the social spot S_i, V_k and the RSU R_i at S_i also first make mutual authentication. If R_i is authenticated, V_k forwards the packet C to R_i, and R_i uses its private key sk_i to recover $pid_{d0}||c$ from C and also temporarily store $pid_{d0}||c$[1].

Fig. 5. Packet propagation from one social spot S_j to its neighboring social spot S_i through vehicle V_k

Since the RSU R_i is deployed at the social spot S_i, there could be other vehicles waiting and communicating with R_i when V_k arrives at S_i. Because the length of packet C follows the exponential distribution, we can assume the process time of R_i on C is also exponentially distributed with the probability density function (pdf) $f_i(t) = \mu_i \cdot e^{-\mu_i \cdot t}$ and the mean $E(t) = \frac{1}{\mu_i}$. Since the vehicle arrival at social spot S_i of degree $\deg(S_i) = \lambda_i$ follows the Poisson process with rate λ_i, we can use M/M/1 queueing model to analyze the average time for V_k waiting and communicating with R_i, i.e., $t_i = \frac{1}{\mu_i - \lambda_i}$. Because the RSU is a powerful device, we can surely assume $\mu_i \gg \lambda_i$. Then, the time $t_i = \frac{1}{\mu_i - \lambda_i}$ is negligible, when we compare it with the packet propagation time from S_j to S_i. According to the social-tier dissemination model in Section II-B, the packet C can be disseminated in the social tier $\mathcal{S}$ within time T.

Algorithm 1 Packet Dissemination in Social tier

```
procedure PACKET DISSEMINATION IN SOCIAL TIER(Packet C, social tier S = {S_1, S_2, ..., S_n})
    for each social spot S_j ∈ S do
        if S_j has received the packet C then
            S_j will request vehicles to help forwarding the packet C to its neighboring social spots NS_j, where NS_j = {S_i | S_i ∈ S, traffic edge e_ji > 0}; when there is a vehicle V_k ∈ V moving from S_j to S_i ∈ NS_i and S_j didn't send the packet C to S_i before, S_j asks V_k to help carrying the packet C to S_i;
        end if
    end for
end procedure
```

4) Packet receiving phase: When the receiver $V_d \in \mathcal{V}$ visits one social spot $S_i \in \mathcal{S}$, it uses its pseudo-id pid_{d0} to make the mutual authentication with the RSU R_i at S_i. Once V_d is authenticated, R_i can identify the pseudo-id pid_{d0}. Then, if R_i has already stored the item $pid_{d0}||c$, it can forward the packet c to the receiver V_d; otherwise, V_d should visit other social spots for picking up the packet c. Once V_d gets the packet $c = (c_1, c_2)$ from R_i, it executes the following steps to recover the message m.

- V_d uses the private key $sk_{d0} = H_0(pid_{d0})^a$ corresponding to the pseudo-id pid_{d0} to compute

$$H(e(c_1, sk_{d0})) = H(e(g, H_0(pid_{d0}))^{ar}) = k_0 \quad (11)$$

  and recovers $pid_{s0}||m||sig(m)$ from the ciphertext $c_2 = \mathbf{Enc}_{k_0}(pid_{s0}||m||sig(m))$ with k_0.

[1]Note that, although the RSUs at social spots are storage-rich, they still should periodically remove the outdated packet, i.e., deleting some packets after they are picked up by the receivers, or batch-removing outdated packets every a specific period.

- If the id-based signature $sig(m)$ is valid with respect to the pseudo-id pid_{s0}, V_d accepts the message m.

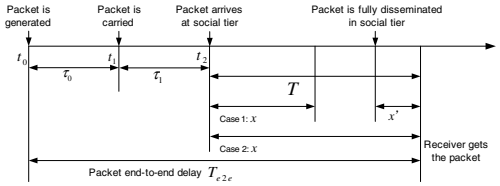


Fig. 6. The timing diagram

Average Packet End-to-End Delay: Consider the timing diagram shown in Fig. 6, where the packet C was generated at time t_0 by the source S, carried by vehicle V_i at time t_1, and arrived at the social-tier at time t_2. Let x be the time period between t_2 and the time when the receiver V_d gets the packet C from one social spot in $\mathcal{S}$. Then, two cases of x can be considered.

- *Case 1:* $x < T$. In this case, the receiver V_d obtained the packet c before T — the time that the packet is fully disseminated in the social tier $\mathcal{S}$. For example, when the receiver V_d visited several social spots within T, and at least one of these visited social spots has already temporarily stored the packet c. Then, the receiver V_d can get the packet once it visits the social spot. However, the time period x in this case is highly dependent on the receiver's mobility, the analysis for $x \leq T$ is too complicated, the average time period $E[x]_1$ in this case is hard to analyze.
- *Case 2:* $x \geq T$. In this case, the receiver obtained the packet c after the packet is fully disseminated in the social spot. Then, once the receiver V_d visits the social tier at time $t_2 + T + x'$, it can immediately get the packet c from the social spot, i.e., $x = T + x'$. Assume that the time period x' that the receiver V_d arrives at the social tier after T follows the exponential distribution with the density function $f_d(t_d) = \lambda_{ds} \cdot e^{-\lambda_{ds} \cdot t_d}$. Then, the average time period x in this case is

$$E[x]_2 = E[T + x'] = T + \frac{1}{\lambda_{ds}} \tag{12}$$

Let η represent the probability that *Case 1* occurs, and $1-\eta$ the probability that *Case 2* occurs. Then, the average time period $E[x]$ is defined as

$$\begin{aligned} E[x] &= \eta \cdot E[x]_1 + (1-\eta) \cdot E[x]_2 \\ &= \eta \cdot E[x]_1 + (1-\eta) \cdot \left(T + \frac{1}{\lambda_{ds}}\right) \end{aligned} \tag{13}$$

Although both η and $E[x]_1$ are unknown, when we set $\eta = 0$, we can get the upper bound of $E(x)$ as

$$\overline{E[x]} = 0 \cdot E[x]_1 + 1 \cdot \left(T + \frac{1}{\lambda_{ds}}\right) = T + \frac{1}{\lambda_{ds}} \tag{14}$$

Because the source S can calculate $\tau_0 = |t_1 - t_0|$, also knows $\tau_1 = |t_2 - t_1| = \frac{d(\mathtt{S},j)}{v_i}$, the source S can estimate the upper bound of average end-to-end packet delay T_{e2e} as

$$\overline{T_{e2e}} = \tau_0 + \tau_1 + T + \frac{1}{\lambda_{ds}} \tag{15}$$

IV. Security Analysis

In this section, we analyze the security of the proposed STAP protocol. Especially, we are most concerned with the following two security aspects, i.e., how STAP can achieve the receiver-location privacy against an active global adversary, and how STAP can achieve vehicle conditional privacy-preservation (CPP), and use CPP as *the second line of defense* to resist the possible source bogus attacks, and inside black/grey hole attacks.

A. The proposed STAP protocol can achieve receiver-location privacy against a global external adversary in VANETs

To achieve the receiver-location privacy preservation in VANET, the first prerequisite is that the exact locations of vehicle should be unlinkable. In the proposed STAP protocol, the receiver $V_d \in \mathcal{V}$ holds a family of pseudo-ids $\mathrm{PID}_d = \{pid_{d0}, pid_{d1}, \cdots\}$, where each pseudo-id $pid_{di} = \mathbf{Enc}_b(V_d || R_{di})$. Without knowing the master key b, these pseudo-ids are unlinkable. Hence, when the receiver V_d moves on the road and periodically changes its pseudo-ids in $\mathrm{PID}_d / \{pid_{d0}\}$ can achieve the location unlinkable. Although the pseudo-id pid_{d0} is repeatedly used in the mutual authentication between V_d and the RSUs at social spots, it is encrypted in $C' = (C'_1, C'_2, C'_3, C'_4)$, and only the trusted RSU can recover it. Therefore, in the eye of an external adversary, the knowledge on the pseudo-id pid_{d0} and the information on when the receiver V_d visits a social spot are not available, even though the adversary is an active global observer.

The second prerequisite for achieving the receiver-location privacy preservation in VANET is that the packet $C = (C_1, C_2, C_3, C_4)$ sent from the source S and the packet $c = (c_1, c_2)$ received by the receiver V_d should be unlinkable. In the proposed STAP protocol, since the single-attribute encryption is employed [13], the ciphertext

$$\begin{aligned} &C_1 = \mathbf{Enc}_k(M) \text{ with } k = H(e(g,g)^{\alpha s}); \\ &C_2 = g^s; C_3 = A^s h_1^{-s}; C_4 = h_2^{-s} \end{aligned}$$

can be decrypted by any legal RSU $R_i \in \mathcal{R}$ with its private key $sk_i = (g^{\alpha + a t_{i1}}, g^{t_{i1}}, g^{t_{i2}}, h_1^{t_{i1}} h_2^{t_{i2}})$, and recover the same $M = pid_{d0} || c$. Since each RSU is powerful and trustable, and won't be compromised to disclose information $M = pid_{d0} || c$ to the adversary. The active global adversary has no idea the relation between C and c. As a result, as shown in Fig. 7, the social tier $\mathcal{S}$ can serve a huge mix-server with high anonymity level, and thus cuts the global adversary's linkability between the receiver V_d and the source S.

The third prerequisite for achieving the receiver-location privacy preservation in VANETs is that the adversary can not impersonate either RSU or uncontrolled vehicles. As the mutual authentication shown in Fig. 4, only the legal RSU R_j, who is granted the private key sk_j from TA, can recover the encrypted challenge $M' = pid_{i0} || \mathtt{CTL} || \hat{s} || sig(\mathtt{CTL} || \hat{s})$ from

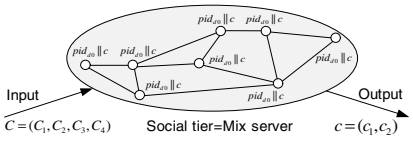


Fig. 7. Social tier serves a huge mix-server to cut the linkability between the input $C = (C_1, C_2, C_3, C_4)$ and the output $c = (c_1, c_2)$

C', and only the legal vehicle with valid pseudo-id pid_{i0} can generate the signature $sig(\texttt{CTL}||\hat{s})$, which can pass RSU's verification. Therefore, the mutual authentication between uncontrolled vehicle and RSU at social spot prevents the global adversary from launching the impersonation attack.

By summarizing the above three prerequisites, the proposed STAP protocol can achieve the receiver-location privacy preservation again an *active* global adversary in VANETs.

B. The proposed STAP protocol can achieve vehicle conditional privacy-preservation in VANETs

In the proposed STAP protocol, each vehicle $V_i \in \mathcal{V}$ holds a family of pseudo-ids $\text{PID}_i = \{pid_{i0}, pid_{i1}, \cdots\}$ with each pseudo-id $pid_{ij} = \mathbf{Enc}_b(V_i||R_{ij})$, where V_i is the real identity, R_{ij} is a random number, and b is the master key. Without knowing the master key b, these pseudo-ids are unlinkable. However, TA, with the master key b, can recover V_i from pid_{ij}. Therefore, the proposed STAP protocol can achieve vehicle conditional privacy preservation (CPP) [10]. CPP is a very important property required in VANETs, which can serve the *second line of defense* to resist the potential inside attacks, such as source bogus attack and black/grey hole attacks. In source bogus attack, a source deliberately inject bogus data to the VANET aimed at wasting the limited buffer resource of vehicles. If the source is an outsider or revoked vehicle, the bogus attack will be immediately filtered because the proposed STAP protocol employs the signature-based authentication. However, if the source of bogus data is a vehicle controlled by the adversary, the source can not be immediately detected. Then, CPP becomes the second line of defense to identify the source based on the vehicle's log information. In black/grey hole attacks, a vehicle drops all/part of packets to degrade the packet forwarding performance of VANET. Similar to the source bogus attack, if the attacker is an outsider or revoked vehicle, the black/grey attacker can be prevented. if the attacker is an insider, CPP can also identify the attacker when the source's log and RSU's log are reported to TA.

V. Performance Evaluation

In this section, we study the performance of the proposed STAP protocol using a custom simulator built in Java. The simulator implements the network layer and makes simple assumptions regarding lower layers as well. For example, it assumes the bandwidth is enough available for V-2-V and V-2-I communications, but the vehicle's buffer is constrained. Since the Epidemic routing is the only traditional routing technique to achieve the receiver-location privacy against an active global adversary in VANETs, we will present the results of our simulation of the proposed STAP protocol in comparison with the Epidemic routing in terms of two performance metrics: *average delivery ratio* (ADR) and *packet average delay* (PAD), where the ADR is defined as the average ratio of the packets successfully delivered to the destinations with respect to those generated by the sources within a given time period, and the PAD is defined as the average time between when a packet is generated at its source and when it is successfully delivered to the receiver.

A. Simulation Environment

In our simulation, we generate a social-tier-assisted VANET containing both N vehicles and 10 social spots in a $10,000 \times 6,000$ m^2 city area, as shown in Fig 8. These social spots form a social tier $\mathcal{S}$, and at each social spot in $\mathcal{S}$, there is a storage-rich RSU device with transmission radius of 1000 meters deployed, which provides the functions of temporarily storing and forwarding packets.

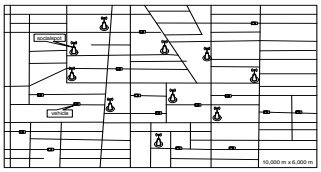


Fig. 8. Simulation area under consideration

Vehicle mobility model. The performance of packet forwarding in social-tier-assisted VANET is highly dependent on the mobility of vehicles. By long-term empirical observations, we know the mobility pattern of a vehicle is relatively stable over time. For example, a vehicle often visits several social spots continuously. Therefore, based on the long-term empirical observations, we model the following mobility pattern of vehicles. Let $\mathbf{s}_0$ represent the state that a vehicle is located at any spot other than the social spots in $\mathcal{S}$, and $\mathbf{s}_i$, $i \in \{1, 2, 3\}$ represent the state that a vehicle has already visited i different social spot(s) in $\mathcal{S}$ continuously. A vehicle stays at each state $\mathbf{s}_j$, $j \in \{0, 1, 2, 3\}$ around 2 minutes, and then chooses the next state. As shown in Fig. 9, if the current state is $\mathbf{s}_0$, the vehicle will choose $\mathbf{s}_1$ as the next state with probability ρ, and $\mathbf{s}_0$ with the probability $1 - \rho$. If the current state is $\mathbf{s}_k$, $k \in \{1, 2\}$, the vehicle will choose $\mathbf{s}_{k+1}$ as the next state with probability 90%, and $\mathbf{s}_0$ with probability 10%. If the current state is $\mathbf{s}_3$, the vehicle will choose $\mathbf{s}_0$ as the next state. Specifically, once the next state is determined, the vehicle chooses and moves to the destination by following the road-based shortest path routing with the velocity V.

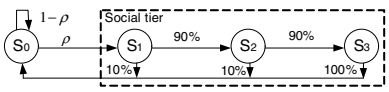


Fig. 9. Vehicle mobility model in simulation

To show the better performance achieved by the proposed STAP protocol, we compare STAP of buffer size 20 M with Epidemic routing of i) infinite buffer size; ii) buffer size 20 M, TTL 2 hours; iii) buffer size 20 M, TTL 4 hours, and iv) buffer

size 40 M, TTL 4 hours under the same mobility pattern with $\rho = 50\%$. In addition, we examine the performance impacted by the parameter ρ, where $\rho = 20\%, 40\%, 80\%$. The detailed parameter settings are shown in Table. I.

TABLE I
SIMULATION SETTINGS

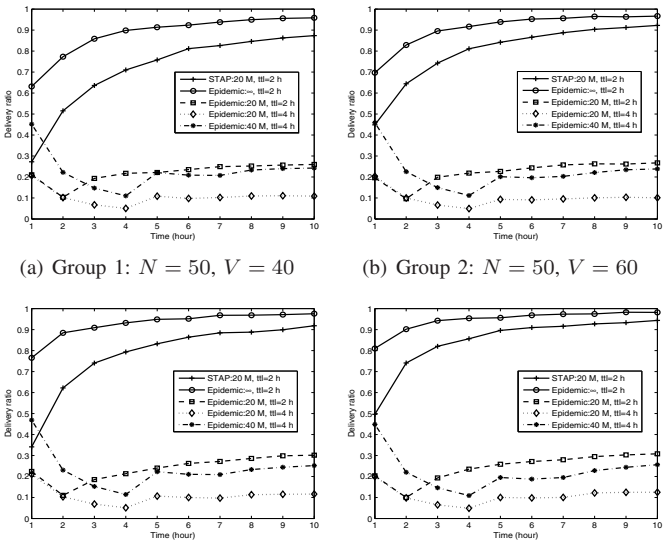
Parameter	Setting
Simulation duration time; area	10 hours; $10,000$ m $\times$ $6,000$ m
social spots number	10
RSU transmission radius; storage	$1,000$ m, $10,000$ M
Vehicle	
number; storage; transmission radius	$N = \{50, 100\}$; 20 MB; 300 m
velocity; waiting time	$V = \{40$ km/h, 60 km/h$\}$; 2 min
ρ in mobility model	$\{50\%, 20\%, 40\%, 80\%\}$
Message size; generation interval	mean size 3 MB, 120 ± 60 seconds
message time-to-live (TTL)	2 hours

In the following, we conduct the simulations with different parameter settings. For each case, we run the simulation for 10 hours, and the average performance results over 10 runs are reported.

B. Simulation Results and Discussions

1) Comparison between STAP and the Epidemic routing: Fig. 10 shows the performance comparison in terms of delivery ratio of STAP and Epidemic routing with $\rho = 50\%$ and different N and V. From the figure, we can see the Epidemic routing with infinite buffer achieves the best delivery ratio. With the time increase, the delivery ratio increases quickly. However, once the vehicle buffer is constrained, the performance in terms of delivery ratio is not efficient. For the case of 20 M vehicle buffer, the delivery ratio will first decrease to the TTL settings, and then increase slowly. Intuitively, when the average delay is un-estimated, the longer the TTL, the higher the delivery ratio, since the packet won't be dropped quickly. However, the TTL is not the dominant factor when the buffer is constrained. Contrarily, as shown in the figure, the long TTL causes lower delivery ratio, and it will positively affect the delivery ratio only when the vehicle buffer size also increases. For example, when the buffer size is 40 M, the 4-hour TTL can increase the delivery ratio. From these observations, we can see, when the vehicle's buffer is limited, the Epidemic routing is not efficient for achieving receiver-location privacy preservation. Now, let us observe the delivery ratio of STAP with 20 M vehicle buffer in the figure. Clearly, the figure shows that the delivery ratio increases quickly as time goes, and almost approaches that of the Epidemic routing with infinite vehicle buffer. Therefore, when the vehicle buffer is constrained, the proposed STAP protocol can achieve better delivery ratio for receiver-location privacy-preserving packet forwarding in VANET. Further observing the four subfigures, the number of vehicles N and the vehicle velocities V also positively affect the delivery ratio.

Fig. 11 shows the corresponding average delay within 10 hours. From the figure, we can see the Epidemic routing with infinite vehicle buffer can achieve the lowest average delay. When the vehicle buffer size is constrained, the long TTL will increase the average delay, but doesn't guarantee the delivery



(a) Group 1: $N = 50$, $V = 40$ (b) Group 2: $N = 50$, $V = 60$

(c) Group 3: $N = 100$, $V = 40$ (d) Group 4: $N = 100$, $V = 60$

Fig. 10. Delivery ratio versus specified time period with $\rho = 50\%$, $N = 50, 100$, and $V = 40, 60$ km/h

ratio will also increase. For example, for the cases of the same 20 M vehicle buffer, the average delay of TTL= 4 hours is higher than that of TTL= 2 hours, but the corresponding delivery ratio in Fig 10 is lower than that of the latter. As for the average delay of STAP, though it is higher than that of the Epidemic routing with infinite vehicle buffer, it is lower than that of the Epidemic routing with constrained vehicle buffer. Therefore, the proposed STAP protocol is also efficient in terms of the average delay. Further observing the results in groups 1, 2, 3, and 4, we can conclude that both the large N and the large V can reduce the average delay of the proposed STAP protocol.

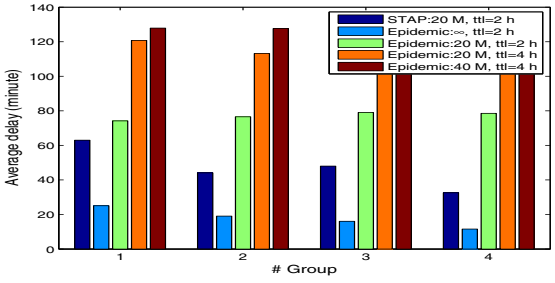
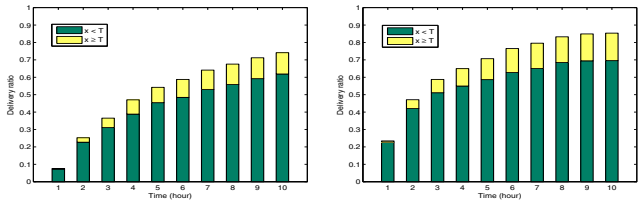


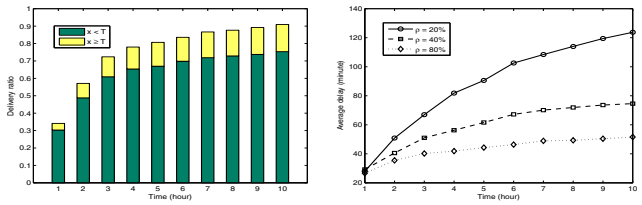
Fig. 11. Average delay within 10 hours in different groups

2) Impact of the Mobility Pattern Parameter ρ: To examine the performance impact due to the mobility pattern parameter ρ, Fig. 12 further shows the delivery ratio and average delay of the proposed STAP protocol for $\rho = 20\%, 40\%, 80\%$, and $N = 50$, $V = 40$ km/h, where the green bar shows the delivery ratio of packets which are received by the receiver *before* the full social-tier dissemination, and the yellow bar shows the delivery ratio of packets which are received by the receiver *after* the full social-tier dissemination. From the subfigures (a), (b), and (c), we can see the larger ρ will improve the delivery ratio quickly. The reason is that, when ρ is large, vehicles will visit the social spots more often, then packets can be quickly forwarded to one social spot and disseminated

in the whole social tier, the receiver can also quickly receive the packet from the social tier. In addition, with the increase of ρ, more receivers can get the packets before the packets' full dissemination in the social tier. Therefore, we can conclude that mobility pattern parameter ρ can affect the probability η in Eq. (13), i.e., the large ρ correspondes the large η. Further observing the average delay in subfigure (d), the large ρ can lead to a low average delay, which means the unknown x_1 in $E[x] = \eta \cdot x_1 + (1-\eta) \cdot \left(T + \frac{1}{\lambda_{ds}}\right)$ is also affected by ρ. Therefore, when ρ increases, the proposed STAP protocol can achieve better packet delivery performance, i.e., high delivery ratio and low average delay.



(a) delivery ratio, $\rho = 20\%$ (b) delivery ratio, $\rho = 40\%$



(c) delivery ratio, $\rho = 80\%$ (d) average delay

Fig. 12. Delivery ratio and average delay versus specified time period for $\rho = 20\%, 40\%, 80\%$, and $N = 50$, $V = 40$ km/h

VI. Related Work

Epidemic routing can achieve receiver-location privacy preservation, but it is not efficient when the vehicle buffer is constraint. Therefore, in this section, we briefly discuss some other research works [8], [9], [15] closely related to STAP. In [15], in order to protect the receiver's location privacy in wireless sensor network, Jian et al. propose a location-privacy routing protocol, called LPR, and combine the routing protocol with fake packet injection to not only provide path diversity but also minimize the information that an adversary can deduce from the overheard packets about the direction towards the receiver. The proposed solution can efficiently protect the receiver's location privacy against *non-global* adversary.

In [8], Lu et al. propose a social-based privacy-preserving packet forwarding protocol, called SPRING, for VANET. With the assistance of RSU, SPRING is not only very efficient in terms of packet delivery ratio, but also protects receiver's location against a global eavesdropper. However, since the source and vehicles who helped carrying the packets know the receiver's fixed location, once a global active adversary controls one of them, the receiver's fixed location will be exposed. Therefore, SPRING can not protect receiver's location against an active global adversary. In [9], Lu et al. adopt the "Sacrificing the Plum Tree for the Peach Tree" tactic to protect receiver's sensitive location privacy in VANETs, where the source and vehicles who helped carrying the packets only know the receiver's non-sensitive location. Therefore, even though an active global adversary controls one of them, only the receiver's non-sensitive location is disclosed, and the receiver's sensitive locations are still unknown. Different form the above works, neither the source nor the vehicles who helped carrying the packet knows the receiver's location in the proposed STAP protocol, and therefore the receiver's location privacy can be fully protected against an active global adversary.

VII. Conclusions

In this paper, we have proposed a social-tier-assisted packet forwarding protocol (STAP) for VANET, which mainly exploits the people's lifestyle and the characteristics of social tier in VANETs to improve the packet delivery performance, and achieve the receiver-location privacy preservation. Detailed security analysis shows that social tier can act as a huge mix server to protect the receiver location privacy, and the vehicle conditional privacy preservation (CPP) can serve as the second line of defense to resist the possible inside attacker. In addition, through extensive performance evaluation, we have also demonstrated the proposed STAP protocol is very efficient in terms of delivery ratio and average delay.

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. Pingley, W. Yu, N. Zhang, X. Fu, and W. Zhao, "Cap: A context-aware privacy protection system for location-based services," in *ICDCS*, 2009, pp. 49–57.

[3] J. Nzouonta, N. Rajgure, G. Wang, and C. Borcea, "Vanet routing on city roads using real-time vehicular traffic information," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, 2009.

[4] J. Zhao and G. Cao, "Vadd: Vehicle-assisted data delivery in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 3, pp. 1910–1922, 2008.

[5] C.-H. Chou, K.-F. Ssu, and H. C. Jiau, "Geographic forwarding with dead-end reduction in mobile ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 4, pp. 2375–2386, 2008.

[6] X. Ma, M.-T. Sun, G. Zhao, and X. Liu, "An efcient path pruning algorithm for geographical routing in wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 4, pp. 2474–2488, 2008.

[7] X. Zhang, G. Neglia, J. Kurose, and D. Towsley, "Performance modeling of epidemic routing," *Comput. Netw.*, vol. 51, pp. 2867–2891, 2007.

[8] 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.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Sacrificing the plum tree for the peach tree: A socialspot tactic for protecting receiver-location privacy in vanet," in *IEEE Globecom'10*, Miami, Florida, USA, December 2010.

[10] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: efficient conditional privacy preservation protocol for secure vehicular communications," in *INFOCOM 2008*, Phoenix, Arizona, USA, April 2008.

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

[12] B. Libert and J.-J. Quisquater, "The exact security of an identity based signature and its applications," Tech. Rep., 2004, eprint.iacr.org/2004/.

[13] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: the essential of bread and butter of data forensics in cloud computing," in *ASIACCS*, 2010, pp. 282–292.

[14] P. Shankar, T. Nadeem, J. Rosca, and L. Iftode, "Cars: Context-aware rate selection for vehicular networks," in *ICNP 2008*.

[15] 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.