MixZone in Motion: Achieving Dynamically Cooperative Location Privacy Protection in Delay-Tolerant Networks

Suguo Du, Haojin Zhu, *Member, IEEE*, Xiaolong Li, Kaoru Ota, *Member, IEEE*, and Mianxiong Dong, *Student Member, IEEE*

***Abstract*—Delay-tolerant networks (DTNs) are typically sparse ad hoc networks where node density is low and contacts between nodes in the network do not occur very frequently. The existing location privacy protection methods, which require mobile nodes to collectively change their pseudonyms in special regions called mix zones, may not work well in DTNs due to their unique characteristics, including low network density and limited contact duration. In this paper, we propose a novel cooperative location privacy protection scheme, which is called AVATAR, for sparse DTNs. The main idea of AVATAR is to generate a certain number of virtual nodes in the proximity of a node and allow both virtual and real nodes to make a coordinated pseudonym change in an enlarged region, which are named virtual mix zones. Each AVATAR participant benefits from increased location privacy protection at the cost of generating a series of signed position messages, which are named footprint signatures. To stimulate each node to contribute more footprint signatures to the virtual mix zones, AVATAR proposes a reward mechanism, which is modeled as a multiunit discriminatory auction game. Extensive simulations and analysis have been provided to demonstrate the effectiveness and efficiency of the proposed scheme.**

***Index Terms*—Delay-tolerant network (DTN), game theory, location privacy, mix zone.**

I. Introduction

DELAY-TOLERANT networks (DTNs) are a special class of ad hoc networks where node density is low, and contacts between the nodes in the network do not occur very frequently. Applications of this emerging communication paradigm include vehicular networks [1], wireless social networks [2], and pocket switched networks [3]. In DTNs, the messages are disseminated according to the store-carry-and-forward principle, and routing is made in an "opportunistic" way.

Recently, there has been increasing interest in DTN security, such as bundle authentication [4], [5] and secure routing [6]. However, little attention has been paid to the location privacy issue in DTNs. Similar to the traditional ad hoc networks, the broadcast nature of DTNs allows the external party or even a malicious adversary to track the user's identifier by eavesdropping on the communications and to estimate the locations of the nodes with accuracy that is sufficient for tracking the nodes [7]. A user's location disclosed by this tracking may reveal sensitive private information such as health condition, lifestyles, and so on. This private information can even be exploited by an adversary to locate the subject, and physical harm may result [8].

The *multiple-pseudonym approach* has been widely adopted by industry and academia to achieve location privacy in mobile networks [9]. In a multiple-pseudonym approach, a set of pseudonyms and their security associations (e.g., public/private keys) are preloaded into the mobile devices, and the nodes can change the pseudonyms over time. To prevent the adversary from linking old and new pseudonyms, the change in pseudonym should be spatially and temporally coordinated among the neighboring mobile nodes. A typical example of a cooperative location privacy protection method is *mix zones*, which forces the nodes to change their pseudonyms at predetermined locations under a centralized authority [10]. This approach, however, lacks flexibility because the locations of mix zones are relatively fixed and cannot provide privacy protection on users' demand. Mix zones can be also performed in a distributed way [7], [11] by allowing a requester to broadcast a pseudonym change request to its neighbors. Distributed mix zones are particularly appealing in conventional ad hoc networks because they do not require the presence of authority or prior knowledge of the location of mix zones.

Nevertheless, the existing cooperative location privacy protection approaches [7], [11] cannot be directly applied to DTNs due to the following reasons. First, the location privacy achieved in [7] and [11] heavily relies on the number of neighboring nodes involved. In the case of a network environment of low network density such as DTNs, the location privacy achieved by node cooperation is limited due to lack of

Manuscript received December 24, 2012; revised March 21, 2013; accepted May 19, 2013. Date of publication June 5, 2013; date of current version November 6, 2013. This work was supported in part by the National Natural Science Foundation of China under Grant 70971086, Grant 61003218, Grant 61272444, Grant 61161140320, Grant 61033014, and Grant 60933011; by the Doctoral Fund of Ministry of Education of China under Grant 20100073120065; by the Japan Society for the Promotion of Science A3 Foresight Program; and by the NEC C&C Foundation. The review of this paper was coordinated by Prof. H.-H. Chen. *(Corresponding author: H. Zhu.)*

S. Du and X. Li are with the Department of Management Science, Shanghai Jiao Tong University, Shanghai 200052, China (e-mail: sgdu@sjtu.edu.cn; ymingchen_123@sjtu.edu.cn).

H. Zhu is with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: zhu-hj@sjtu.edu.cn).

K. Ota is with the Department of Information and Electronic Engineering, Muroran Institute of Technology, Muroran 050-8585, Japan (e-mail: ota@csse.muroran-it.ac.jp).

M. Dong is with the School of Computer Science and Engineering, The University of Aizu, Aizu-Wakamatsu 965-8580, Japan (e-mail: mx.dong@ieee.org).

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

Digital Object Identifier 10.1109/TVT.2013.2266347

collaborators. Second, to impede an adversary from spatial and temporal correlation of users' location privacy, a certain period of mix zones is necessary to ensure a certain privacy level. However, due to limited number of neighbors and contacting time, maintaining a relatively stable mix zone for a certain period is challenging in DTNs. Finally, the cooperative location privacy protection scheme is based on an assumption that each individual node is ready to collaborate with the neighbors to change their pseudonyms. Due to the low network density and the unreliable message successful delivery rate, a selfish mobile node may decide not to get involved in location privacy protection due to the low expected privacy benefit.

To protect users' location privacy in a low-network-density environment, in this paper, we propose AVATAR, which is *A* cooperative location pri*VA*cy pro*T*ection scheme based on opportunistic coll*A*boration for spa*R*se DTNs. In contrast with the existing passive approaches, AVATAR allows the nodes to make the coordinated pseudonym change on users' demands. Motivated by James Cameron's epic motion picture, i.e., *AVATAR*, in which human intelligence could be injected into a remotely located body, the proposed scheme enables a node to make remotely virtual copies by using a series of spatial- and temporal-aware signatures, which are named *footprint signatures*. These virtual nodes can be exploited by the remote authorized nodes to increase location privacy entropy for a longer duration. With AVATAR, the real nodes and these virtual nodes are grouped into a virtual mix zone, which is named *VMixzone*. Different from the conventional mix zones, VMixzones allow the scattered nodes in a wide range to collaborate with each other in an opportunistic way.

Further, since VMixzones rely on the collaboration of DTN nodes, AVATAR requires each node to contribute its footprint signatures to others. Without sufficient incentive, a selfish (or rational) node may decide not to change its pseudonym by refusing to provide its footprint signatures. This, in turn, may jeopardize the welfare achieved by a location privacy scheme. To overcome this difficulty, we present a reward mechanism to provide incentive for the nodes to join AVATAR. The basic idea of the reward scheme is to let the VMixzone requester choose a certain number of nodes as the collaborators and reward each of them with all of the collected footprint signatures from all the participants. The incentive issue can be modeled as a multiunit discriminatory auction game. With game-theoretic analysis, we show that the AVATAR scheme does stimulate rational nodes to collaborate with each other to achieve increased location privacy.

The contributions of this paper are summarized as follows.

- First, we introduce a new location privacy model by considering the spatial and temporal factors jointly.
- Second, we propose AVATAR, which is a novel location privacy protection scheme for sparse DTNs based on opportunistic collaboration of mobile nodes.
- Third, AVATAR provides a reward mechanism to provide incentive for each node to contribute to VMixzone. We estimate the Nash equilibrium of the footprint signature provided by each rational node by modeling AVATAR as a multiunit discriminatory auction game.
- Finally, we implement AVATAR under a specific application scenario setting, i.e., pocket switched networks. The extensive simulations have demonstrated the effectiveness and efficiency of AVATAR with extensive simulations.

To the best of our knowledge, this is the first research effort on opportunistic location privacy protection in DTNs. The remainder of this paper is organized as follows. In Section II, the state of the art of location privacy in mobile networks is discussed. In Section III, we present the system model, which is the adversary model considered throughout this paper. In Section IV, we propose the spatial and temporal location privacy model. In Section V, the proposed AVATAR scheme is presented in detail. A game-theoretic analysis is given in Section VI. Simulation results and performance analysis are given in Section VII, followed by conclusions in Section VIII.

II. Related Work

Protecting the location privacy of mobile users has been receiving much attention recently. Previous works on location privacy show that the adversary can implicitly derive the identity information from the analysis of its location information, such as the location traces collected in an office environment [10] or Global Positioning System traces from vehicles [12].

To protect location privacy, in [10], Beresford and Stajano proposed an innovative scheme based on the idea of Chaum's mix, which enables the nodes to update at predetermined locations called mix zones. In [11], Huang *et al.* proposed the random silent period technique to allow the nodes to update at random locations and times. However, the spatial and temporal relation between the locations of a mobile node can enable its entry and exit locations and times from a mix zone to be correlated, hence lowering entropy [10]. To maximize the location privacy provided by each update, a Swing and Swap protocol was proposed in [7] to allow the nodes to cooperate to enable exchange of nodes' identifier and, thus, achieve higher location privacy. However, exchange of identifier and associated public/private keys may potentially introduce other security threats such as the Sybil attack. Different from [7], in this paper, we allow nodes to exchange their footprint signatures rather than their identifier to generate the virtual nodes.

The anonymity of mobile nodes at different levels of the communication stack can be very challenging. To achieve medium access control (MAC) layer anonymity, the node could choose to change the MAC address every time a pseudonym is changed [13] or simply use an identifier-free link layer protocol [14]. Similarly, it is possible to identify devices relying on their distinctive characteristics (i.e., fingerprints) at the physical layer. However, a recent study shows that it is possible to perform impersonation attacks on physical layers [15]. Further, the identification techniques on physical layers require high-end hardware components that capture the radio signals of wireless devices, which is costly and cannot be deployed in a large scale. Therefore, in this study, we focus on the higher layer privacy mechanisms such as changing the pseudonym in a mix zone.

An incentive issue for cooperative privacy preservation is another important topic. In [16], it is pointed out that in a mix-zone-based cooperative privacy protection scheme, the selfish nodes may refuse to cooperate with others due to low location privacy benefits. It further analyzes the noncooperative behavior of mobile nodes by using a game-theoretic model [17], where each player aims at maximizing its location privacy at a minimum cost. Different from [16], we propose a new cooperative location privacy protection scheme and then analyze the noncooperative behaviors of mobile nodes in the auction game model [18].

III. Preliminaries

This section describes our system and threat models.

A. System Model

We focus exclusively on a general DTN network architecture, where mobile nodes are autonomous entities equipped with WiFi or Bluetooth-enabled devices that communicate with each other upon coming in range. We do not consider communications with the infrastructure (such as cellular networks or wireless local area networks). The application scenario of the considered networks can be vehicular networks [19], pocket switched networks, or mobile social networks, in which mobile nodes advertise their presence by periodically broadcasting proximity beacons (e.g., every 100 ms over a range of 300 m in vehicular networks) containing the node's authentication information (e.g., the position and speed in vehicular networks). We assume that the DTN network is loosely synchronized. In terms of data forwarding, we consider a general DTN forwarding model, under which a source node can deliver packets to a destination node by following the store-carry-and-forward principle.

At the system initialization phase, we follow a general assumption as in [16] that an *Offline Security Manager (OSM)* exists to take charge of preestablishing the security credentials for each device. In line with the multiple-pseudonym approach to protect location privacy, we assume that prior to entering the network, every mobile node i registers with the OSM and obtains a set of public/private key pairs $\{Pub_i^k, Prv_i^k\}_{k=1}^M$ to provide verification and signature functionalities, respectively. Here, Prv_i^k enables node i to digitally sign messages, whereas Pub_i^k serves as the identifier of node i and is also referred to as its pseudonym.

B. Threat Model

Consider an external adversary $\mathcal{A}$ aiming to track the location of mobile nodes. We assume that $\mathcal{A}$ does not have the security credentials issued by the Certificate Authority and, thus, cannot impersonate a legitimate node to disrupt the system. In practice, the adversary can eavesdrop a specific node's communications and then track it. In the worst case, $\mathcal{A}$ can obtain complete coverage and track nodes throughout the entire network, which is also referred to as a global attacker.

$\mathcal{A}$ collects identifying information (i.e., pseudonyms or public keys) from the entire network and obtains location traces that allow him to track the location of mobile nodes. Although AVATAR focuses on the node identification information of application layers, it is also possible to extend AVATAR to the lower layers such as MAC or physical layers by exploiting the MAC-address-changing technique [13] or the physical-layer impersonation technique [15].

IV. Spatial–Temporal Location Privacy Model

The basic idea of AVATAR is to specify a spatial region (or VMixzone), in which the real identity of a node is hidden by the virtual neighbors generated by its collaborators. To measure the location privacy level provided by the VMixzone, we use the concept of entropy from Shannon's information theory [20]. Suppose that the existence of a virtual node could be demonstrated by a series of location- and time-aware signatures, these signatures, each called a footprint signature, can then be used to measure the location privacy of a spatial region as follows.

Definition 1: Let $\mathcal{R}$ be a spatial region observed by the attacker and $S(\mathcal{R}) = \{U_1, U_2, \ldots, U_m\}$ be the set of nodes/virtual nodes whose footprint signatures appear in this region during period T. Here, T is the period during which pseudonym changes occur, and m is the total number of users. Specifically, each node $U_i (1 \leq i \leq m)$ broadcasts $n_i (1 \leq i \leq m)$ footprint signatures within T. We define the uncertainty of the adversary and, thus, the location privacy level of a node involved in a successful pseudonym change within T to be

$$\mathcal{A}(m) = -\sum_{i=1}^{m} \frac{n_i}{N} \log \frac{n_i}{N} \tag{1}$$

where $N = \sum_{i=1}^{m} n_i$ refers to the total number of footprint messages.

The achievable location privacy is determined by both the number of nodes m and the distribution of their footprint signatures. Therefore, entropy $A(m)$ has the maximum value when every node in $\mathcal{R}$ has the same number of footprints in $\mathcal{R}$. In other words, the entropy is the maximum for a uniform probability of the number of footprint signatures, which could provide the node with a location privacy level of $\log(m)$. On the other hand, $A(m)$ has the minimum value when one user in $\mathcal{R}$ has $N - m + 1$ footprint signatures while each of the rest has only 1. Therefore, to obtain higher location privacy, the nodes need more collaborators (both real and virtual nodes), and at the same time, the footprint signatures should be uniformly distributed.

The spatial location privacy model evaluates the location privacy achieved in VMixzones of the network. However, it fails to consider the temporal factor, which may have an impact on privacy protection. When a short-interval VMixzone is launched, the adversary can still correlate users' old and new pseudonyms by leveraging the predictability of the movement of pedestrians and vehicles. Although Li *et al.* in [7] have proposed a series of approaches to maximize location privacy,

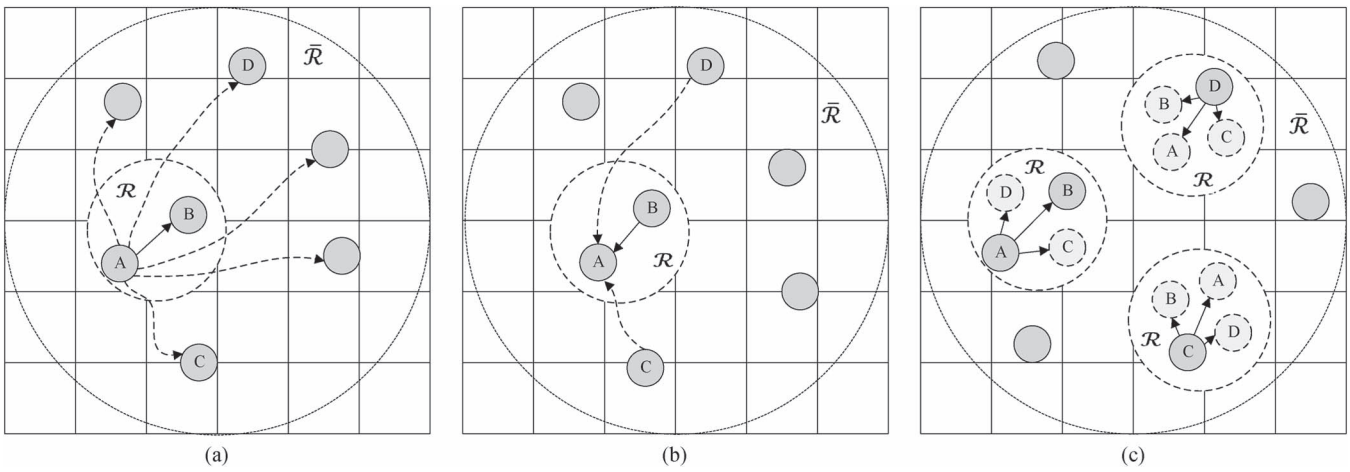


Fig. 1. Running example of the AVATAR protocol. (a) VMixzone request broadcasting phase. (b) VMixzone request response phase. (c) VMixzone generation phase.

a short VMixzone period may prevent such kind of tracking mitigation approaches from being adopted.

Therefore, when a certain period of VMixzone is generated to protect users' location privacy, the privacy level should not be less than a predefined threshold $A(m)$. In other words, the VMixzone must achieve a certain privacy level $A(m)$ in both spatial–temporal dimensions, which is also called the $(A(m), T)$ spatial and temporal privacy model [$(A(m), T)$-ST privacy model].

Definition 2: Let T be multiple continuous time slots $T_1, \ldots, T_n$, and $A(m)$ is a predefined privacy entropy threshold. A user in observation region $\mathcal{R}$ achieving the $(A(m), T)$-ST privacy model should satisfy that (1) $\mathcal{R}$ covers the user's position for all time slots $T_1, \ldots, T_n$ and that (2) in each time slot T_i, the privacy level should be no less than $A(m)$.

Definition 2 indicates that to satisfy the $(A(m), T)$-ST privacy model, a node in observation region $\mathcal{R}$ should achieve $A(m)$ privacy level for a certain period. In practice, the period needs to be as long as possible to guarantee the quality of the required privacy level. In the rest of this paper, we focus on how to generate the VMixzone that satisfies the $(A(m), T)$-ST privacy model.

V. Proposed AVATAR Protocol

Here, we present the details of AVATAR protocols.

A. Overview of AVATAR

The existing literature on cooperative location privacy protection assumes that there are enough collaborators that are physically close to each other. This assumption, however, does not hold in sparse DTNs, which are typically characterized with low network density and short contact duration. Therefore, how to improve the network density is a key issue to achieving cooperative location privacy in DTNs.

On the other hand, the adversary cannot determine the number of nodes in a specific observation region by only eavesdropping in on the communications. In other words, node A could broadcast a position beacon information on behalf of another remote node B, and the adversary will accept B as a "real" neighboring node, although B is actually not physically close to A. The only condition for proving B's existence is that this position beacon information is indeed generated by B (signed with B's private key). This observation provides a possible way to generate some virtual nodes around the tracking target.

The basic idea behind AVATAR is introducing k virtual nodes in the neighborhood of the target node. To do so, the nodes in a specific region $\overline{\mathcal{R}}$ should pregenerate a series of signed position beacon messages according to the predetermined VMixzone region and duration. The pregenerated footprint signatures are encrypted with the target node's public key and then transmitted to the target node via opportunistic routing protocols before the response expiration time t_1. The target node could broadcast these collected footprint signatures together with its own footprint signatures at the predetermined VMixzone starting time t_2. To prevent Sybil and replay attacks, we define that the footprint signatures are only valid in the predefined range $\overline{\mathcal{R}}$ and starting time t_2 of VMixzone.

Fig. 1 shows a running example for the AVATAR algorithm, where each solid/dashed line represents direct/opportunistic transmission, and each solid/dash node refers to a real/virtual node. In Fig. 1(a), node A only has neighboring node B. Hence, A broadcasts a collaborator search request to the nodes within a predefined range $\overline{\mathcal{R}}$. This broadcast message is transmitted to B via direct transmission while to other nodes, including C and D, by opportunistic routing. In Fig. 1(b), nodes B, C, and D respond to A by providing their footprint signatures. At t_2, node A sends the collected footprint signature set to B, C, and D for the rewarding. Therefore, in Fig. 1(c), it forms a VMixzone, in which each node benefits from privacy improvement by making a coordinated pseudonym change with real/virtual nodes. Generally, AVATAR is comprised of the following three phases: 1) VMixzone collaborator search phase; 2)VMixzone collaborator response phase; and 3) participant rewarding and VMixzone generation phase, which are presented in detail in the following sections.

Algorithm 1: AVATAR: VMixzone Requester N_s

Function: AVATAR-Requester $(\overline{\mathcal{R}}, t_1, t_2, k)$
//VMixzone request broadcasting phase
while $\widehat{k} < k$ **do**
Broadcast a VMixzone request $Req, \langle Req \rangle_{Prv_{\mathcal{N}_s}}$ to the peers in the range of $\overline{\mathcal{R}}$;
Let $\mathcal{P}$ be the number of peers responded;
$\widehat{k} = |\mathcal{P}|$;
if $\widehat{k} < k$ **then**
Enlarge the size of region $\overline{\mathcal{R}}$;
else
Choose k replying nodes as the collaborators;
Collect the corresponding footprint signatures $\{\mathcal{S}_i^j | i = 1, \ldots, k; j = 1, \ldots, m_i\}$
Send collected footprint signatures to each pariticipant;
end
end

B. VMixzone Collaborator Search Phase

Mobile node $\mathcal{N}_s$ broadcasts its pseudonym change collaboration request to the peers. The request includes VMixzone region $\overline{\mathcal{R}}$, response expiration time t_1, VMixzone starting time t_2, and number of requested collaborators k, i.e.,

$$\mathcal{N}_s \rightarrow * : Req = \langle \overline{\mathcal{R}}, t_1, t_2, k \rangle, \langle Req \rangle_{Prv_{\mathcal{N}_s}}$$

where $\langle Req \rangle_{Prv_{\mathcal{N}_s}}$ refers to the signature generated by $\mathcal{N}_s$ with its private key. The nodes receiving this message will rebroadcast this message until t_1. At time t_1, if the number of participants is less than k, $\mathcal{N}_s$ could enlarge the range of $\overline{\mathcal{R}}$. This process will continue until enough peers are found.

C. VMixzone Collaborator Response Phase

When a node receives a VMixzone forming request, it will first check if it is a duplicate request. If so, it simply drops the messages. Otherwise, the receiver rebroadcasts the request to its next opportunistic contacts. This process will be terminated once response expiration time t_1 is passed.

Receiver $\mathcal{N}_i$ will decide whether to join the VMixzone and change the pseudonym by considering the expected benefit and costs, which will be discussed in Section VI. In joining the VMixzone, $\mathcal{N}_i$ should determine its preferred VMixzone duration $\{T_i^j | j = 1, \ldots, m_i\}$ and generate the footprint signatures for each time slot with its new pseudonym $\overline{\mathcal{N}}_i$. Note that the duration of a VMixzone satisfying the $(A(m), T)$-ST privacy model should be as long as possible, which means the generated signatures should be as many as possible. The generated footprint signatures could be represented as $\mathcal{S}_i = \{sig_i^1, \ldots, sig_i^{m_i}\}$, where $sig_i^j = \{\mathcal{N}_i, R, T_i^j, \{N_r \| R \| t_i\}_{Prv_{\overline{\mathcal{N}}_i}}\}$, and $Prv_{\overline{\mathcal{N}}_i}$ corresponds to $\mathcal{N}_i$'s new pseudonym $\overline{\mathcal{N}}_i$ at t_2. After that, $\mathcal{N}_i$ encrypts the footprint signature with N_s's public key and then sends $\{\mathcal{S}_i\}_{PK_{N_s}}$ to N_s via a specific DTN routing protocol, such as in [21].

Algorithm 2: AVATAR: Receiver $\mathcal{N}_i$

Function: AVATAR-Receiver $(\overline{\mathcal{R}}, t_1, t_2, k)$
//Collaborator Response Phase
Let T be the current time;
if *the request is duplicate* **then**
Reply with an ACK message;
else
if $T < t_1$ **then**
if $\mathcal{N}_i$ decides to join the VMixzone **then**
Choose preferred time duration $\{T_i^j | j = 1, \ldots, m_i\}$;
Generate $\{\mathcal{S}_i = sig_i^1, \ldots, sig_i^{m_i}\}$ with its new pseudonym $\overline{\mathcal{N}}_i$;
Send $\langle \mathcal{S}_i \rangle_{PK_{N_s}}$ to N_s by a specific DTN routing protocol;
end
Broadcast the VMixzone forming request to the next opportunistic contact;
else
Drop the message;
end
end

D. Participant Rewarding and VMixzone Generation Phase

To stimulate the nodes to contribute more signatures for VMixzone, we design a reward mechanism, that is, requestor $\mathcal{N}_s$ will choose k nodes who generate the most footprint signatures as the collaborators from all replying peers in region $\overline{\mathcal{R}}$. Then, $\mathcal{N}_s$ collects their corresponding footprint signatures $\{\mathcal{S}_i^j | i = 1, \ldots, k; j = 1, \ldots, m_i\}$. For each participant $\mathcal{N}_i$, $\mathcal{N}_s$ encrypts the collected footprint signatures with $\mathcal{N}_i$'s public key, which is denoted as $\{\mathcal{S}_i^j | i = 1, \ldots, k; j = 1, \ldots, m_i\}_{PK_{N_i}}$, and sends it to $\mathcal{N}_i$. Therefore, requestor N_s forms a VMixzone with k peers by exchanging and sharing their footprint signatures. At time t_2, each participant starts to broadcast the received footprint signature. Specifically, for the subsequent time slot $\{T_j | j = 1, \ldots, \overline{m}\}$, where $\overline{m}$ refers to the maximum value of $\{m_i | i = 1, \ldots, k\}$, a participating node broadcasts $\{\mathcal{S}_i^j | i = 1, \ldots, k\}$ in a randomized order. Note that these footprint signatures are from k different nodes and represent the new pseudonyms of these nodes. From the attacker's point of view, these k identifiers are undistinguishable. Therefore, the new pseudonym of each node is hidden by other k real/virtual nodes. In the following section, we will discuss the expected benefit brought by AVATAR in detail.

Algorithm 3: AVATAR: VMixzone Participant $\mathcal{N}_i$

Function: AVATAR-Participant $(\mathcal{S}_i^j)$
Let $\overline{m} = MAX\{m_i | i = 1, \ldots, k\}$;
for *each time slot* $\{T_j | j = 1, \ldots, \overline{m}\}$ **do**
Broadcast the footprint signature set $\{\mathcal{S}_i^j | i = 1, \ldots, k\}$ in a randomized order;
Make a coordinated pseudonym change;
end

E. Comparison of AVATAR With the Conventional Mix Zone Approaches

With AVATAR, an adversary cannot distinguish a real VMix-zone node from a virtual node by eavesdropping in on the transmission messages in DTNs. This statement also holds in the presence of global attack, which could have full knowledge of the presence of each node at the beginning and after the end of the VMixzone. However, even if the global attacker could recognize the real node at the start or the end of the VMixzone, it cannot distinguish the contact of several real nodes from the case of one real node with several virtual nodes. The insight here is that, from the adversary's point of view, the real and virtual nodes are using the same transmission pattern to transmit a message and, thus, cannot be distinguished due to the fact that the adversary can only eavesdrop in on the node's communications but cannot tell the exact number of real nodes by physical observation.

The traditional mix zone approaches such as in [16] could achieve the equivalent privacy gains by collaborative pseudonym changes for multiple times. Due to lack of enough collaborators for each pseudonym change, it is required that it be performed multiple times to obtain the same privacy level. However, we argue that AVATAR could still achieve the following advantages compared with the traditional mix zones.

- *Less Number of Pseudonyms Required*: As pointed out by Freudiger *et al.* in [16], the existing mix-zone-based approaches require multiple pseudonyms due to lack of enough collaborators for each time in sparse DTNs. However, a pseudonym change causes considerable overhead and, thus, reduces the networking performance (e.g., the routing tables). Further, the pseudonyms and their corresponding public/private key pairs are costly to acquire and use because they are owned in limited number and require contact to a central authority for refill [16]. Different from the existing approaches, AVATAR only requires one pseudonym for a virtual mix zone.
- *Supporting Communications During Mix Zone Period*: In conventional mix zone approaches, it has a certain silent period, while the adversary cannot observe DTN nodes' mobility at the cost of no data transmission. However, in AVATAR, it can still support the data transmission by using the encrypted data, which follows a certain format. From the attacker's point of view, it cannot distinguish real messages from dummy messages if both of them are encrypted.

In the following section, we will give a detailed analysis on the expected privacy gain for AVATAR participants.

F. Estimating the Expected Benefit of AVATAR Participants

To measure privacy improvement by AVATAR, we study the $(A(m), T)$-ST location privacy model. Generally, the expected location privacy achieved by participant $\mathcal{N}_i$ could be expressed by

$$\mathcal{B}_i = (\mathcal{A}(m_i + k) - \mathcal{A}(m_i)) * p_i * q_i \tag{2}$$

where m refers to the number of neighboring nodes, k refers to the number of virtual neighboring nodes, p_i is the probability that the requester successfully receives the response from $\mathcal{N}_i$ before t_1, and q_i is the probability that $\mathcal{N}_i$ successfully receives the reward from the requester before t_2.

By substituting (1) into (2), we can obtain $\mathcal{B}_i$ as

$$\mathcal{B}_i = \left(\sum_{j=1}^{m_i} \frac{\widehat{n}^j}{\widehat{N}} \log \frac{\widehat{n}^j}{\widehat{N}} - \sum_{j=1}^{m_i+k} \frac{n^j}{N} \log \frac{n^j}{N} \right) * p_i * q_i. \tag{3}$$

Here, $\widehat{n}^j$ and $\widehat{N}$ refer to the number of footprint signatures generated by each real neighboring node $\{\mathcal{N}_j | 1 \leq j \leq m_i\}$ in this period and the total number of footprint signatures, respectively, whereas n^j and N refer to the number of footprint signatures generated by each real or virtual neighboring node $\{\mathcal{N}_j | 1 \leq j \leq m_i + k\}$ and the total number of footprint signatures. Note that if the number of footprint signatures generated by different nodes follows a uniform distribution, $\mathcal{B}_i$ can achieve a maximum value $(\log\{m_i + k\} - \log m_i) * p_i * q_i$.

It is worth noting that the duration of a VMixzone satisfying the $(A(k), T_d)$-ST privacy model is determined by the minimum value of $\{m_i | i = 1, \ldots, k\}$, i.e., $T_d = \tau * \mathrm{Min}\{m_i | i = 1, \ldots, k\}$, where τ is the length of a time slot. In other words, in duration T_d, even if there are no neighboring nodes in the attacker's observation range $\mathcal{R}$, this node can still satisfy the $(A(k), T_d)$-ST privacy model. From this fact, we can conclude that the more footprint signatures each participant contributes, the longer the duration of $(A(k), T_d)$-ST privacy the VMixzone can achieve. In the following section, we will discuss how to increase the number of collected footprint signatures with the auction game and estimate the number of footprint signatures provided by each rational node in the Nash equilibrium.

G. Estimating p_i and q_i

In the previous section, it is shown that the expected location privacy benefit of AVATAR participants is tightly related to p_i and q_i. However, without clear knowledge of how these factors interact, it is extremely hard to theoretically model p_i and q_i. Therefore, we adopt a similar approach in [3] to estimate the message-dropping probability in DTNs, which is based on supervised classification problems of data mining techniques. The main idea for estimating p_i and q_i is that p_i and q_i are similar to some historical packets that have similar feature values. Suppose we match a response message to a set of $\mathcal{M}^1$ of similar messages and its received subset is $\mathcal{M}^1_{\mathrm{received}}$, then p_i can be estimated by

$$p_i = \left| \mathcal{M}^1_{\mathrm{received}} \right| / |\mathcal{M}^1|. \tag{4}$$

Similarly, we can obtain the estimation of q_i as $|\mathcal{M}^2_{\mathrm{received}}|/|\mathcal{M}^2|$, where $\mathcal{M}^2$ and $\mathcal{M}^2_{\mathrm{received}}$ refer to the set of similar footprint signature set and its dropping subset, respectively.

VI. AVATAR GAME: A GAME-THEORETIC ANALYSIS

In the previous section, we introduced the details of the AVATAR protocol. By discussing the expected benefit of AVATAR participants, it can be seen that each node in range $\overline{\mathcal{R}}$ is willing to join VMixzone since it can take the opportunity to increase its privacy level. However, from the requestor's point of view, it only needs to collaborate with a certain number of neighboring nodes (i.e., k) to obtain a VMixzone because more participants mean more traffic loads and more energy consumption to transmit the replying message and footprint signatures. As a result, there is tension between limited available participating positions and an excessive number of response nodes. On the other hand, the duration of $(A(k), T_d)$-ST VMixzone is determined by the minimum number of footprint signatures collected from each participant. This motivates the requester to collect as many footprint signatures as possible from k participants. To do so, the requestor stimulates the nodes to contribute more footprint signatures through the proposed reward mechanism in that only those who provide k most signatures could be rewarded with all the footprint signatures. Here, we model AVATAR as a multiunit discriminatory auction to answer the question as to how many footprint signatures a rational node should provide to maximize its profit.

A. Modeling AVATAR as a Multiunit Discriminatory Auction

In a multiunit discriminatory auction, a seller, with k objects for sale, wishes to sell his objects to k highest bidder at one go in a single auction. Specifically, the auctioneer ranks the bids according to the price from the highest to the lowest and then announces the k highest bidders win the auction game. It should be noticed that the k winners do not need to pay the same price for identical items. Instead, each winner only needs to pay its real bid to get the item, i.e., there exists a discriminatory price in the auction.

We design AVATAR as a multiunit discriminatory auction game among N nodes $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ within the range of $\overline{\mathcal{R}}$, competing for one of k participants of VMixzone. We let the requestor be the auctioneer. We assume that the requestor and the players are honest in following the AVATAR games and that malicious nodes are not taken into consideration since external attackers cannot join the game due to lack of authorized key pairs. In the DTNs, several of these games can be played in parallel, and a node can join several games at different times. Without loss of generality, in this study, we consider a single game where all the nodes join at the same time.

The game includes three stages. In the request broadcasting phase, the requestor periodically broadcasts its pseudonym change request. Each player chooses its bid (generating a certain number of footprint signatures) and sends it back to the requestor. The requestor continues to receive the bids until a predefined time t_1. Any delayed or lost bids will be considered a bidding failure, and the bidder will not pay any cost. At t_1, the requestor chooses k highest bidding players as the VMixzone collaborators and set their submitted signatures as the VMixzone footprint signatures. In the rewarding phase, the requestor sends back all the footprint signatures to each chosen collaborator.

TABLE I
MAPPING BETWEEN A MULTIUNIT DISCRIMINATORY AUCTION AND OUR AVATAR GAME

Multi-unit Discriminatory Auction	Virtual Mix Zone Auction
Buyer: $\mathcal{P}_i$	Nodes in the range $\mathcal{R}$
Value: v_i	Own private value : $\mathcal{B}_i$
$F(v_i)$	$F(\mathcal{B}_i)$
Price : c_i	$u(n_i)$
$Profit : v_i - c_i$	$\mathcal{B}_i - u(n_i)$

Table I shows mapping between a traditional multiunit discriminatory auction and our AVATAR game. The objects to be sold are the positions of attending the pseudonym change, and there are k auction items in this game (k available positions for the VMixzone). Each node will bid for only one position since the extra participating positions will not increase its privacy level. In the multiunit discriminatory auction, the value of the object is denoted by v_i. It is now replaced by $\mathcal{B}_i$, representing a node's expected location privacy gain in the VMixzone. Since each node has a different estimation on p_i and q_i and the number of real neighboring nodes m_i also varies, each node has different estimated values of $\mathcal{B}_i$. It is assumed that each node only knows his own $\mathcal{B}_i$ but not the values of other nodes. However, since each node in the VMixzone is symmetrical, $\mathcal{B}_i$ is independently and identically distributed. Without loss of generality, $F(\mathcal{B}_i)$ is supposed as uniformly distributed. Thus, each node can estimate other nodes' value of $\mathcal{B}_i$.

In the multiunit discriminatory auction, each buyer's price c_i is less than his value v_i for the object so that his profit is positive, i.e., $v_i - c_i > 0$. However, in VMixzone, each node's profit of location privacy is very difficult to model because it is impossible to compare n_i (the number of signatures each node provided) with privacy gain value $\mathcal{B}_i$. To solve this problem, similar to [16], we introduce utility function $u(n_i)$, which describes the location privacy cost of n_i footprint signatures generated by node i. This $u(n_i)$ can be expressed in privacy units (e.g., bits), thereby the profit of location privacy can be calculated as $\mathcal{B}_i - u(n_i)$. It should be pointed out that utility function $u(n_i)$ involves various costs, including the costs of generation and transmission of footprint signatures. It is an increasing function of n_i. In this paper, it is modeled as a linear function of n_i.

B. Equilibrium

We assume that all nodes act rationally and try to maximize their benefits. However, the best strategy for a given player depends upon the strategies adopted by other players in the game. In this game, every player should decide its price, i.e., how many footprint signatures it intends to bid. The optimal strategy can be obtained by using the Nash equilibrium. A set of strategies (one strategy for each player) is called a Nash equilibrium if no player can increase his payoff by unilaterally changing his strategy. Our goal in the VMixzone auction game is to find the optimal signatures a node should provide.

Theorem 1: Multiunit Discriminatory Auction Game: If N buyers have independent values $\mathcal{B}_i$, which have the distribution

of $F(v)$, then the best bidding price $p(\mathcal{B}_i)$ for a buyer with private value $\mathcal{B}_i$ is [22]

$$p(\mathcal{B}_i)=\mathcal{B}_i-\frac{\sum_{i=1}^{k} C_{N-1}^{i-1}\int_0^{\mathcal{B}_i}[1-F(v)]^{i-1}F(v)^{N-i}dv}{\sum_{i=1}^{k} C_{N-1}^{i-1}[1-F(\mathcal{B}_i)]^{i-1}F(\mathcal{B}_i)^{N-i}}. \quad (5)$$

With the bidding equilibrium, we can obtain the optimal bidding strategy for an AVATAR participant to be $n_i = u^{-1}(p(\mathcal{B}_i))$.

Without loss of generality, we assume that $F(v)$ is uniformly distributed in [0,1]. In a simplest case where $k = 1$, i.e., a requestor only needs one collaborator, the equilibrium is given by

$$p(\mathcal{B}_i) = \mathcal{B}_i - \frac{\mathcal{B}_i}{N}. \quad (6)$$

It is observed that the equilibrium number of footprint signatures significantly relies on the number of rational nodes in the VMixzone auction game. We can see from (6) that the equilibrium price is less than a node's value estimation. However, with the growth in the number of players, i.e., when $N \to \infty$, the equilibrium price tends to be the node's value estimation $\mathcal{B}_i$. This is because the more players there are, the more intense the competition is. Hence, a node has to provide a price that is close to its value to win the auction game.

In the case of $k = 2$, where a requestor needs two collaborators, we can obtain the equilibrium as

$$p(\mathcal{B}_i) = \mathcal{B}_i - \frac{1-\frac{N-2}{N}\mathcal{B}_i}{\frac{N-1}{\mathcal{B}_i}-(N-2)}. \quad (7)$$

By setting $\mathcal{B}_i = 0.7$ and $u(n_i) = 0.01n_i$, we show a plot of the equilibrium price (number of footprint signatures) for $k = 1$ and $k = 2$ in Fig. 2. In Fig. 2, we can see that for fixed N, the number of footprint signatures a node provides when $k = 2$ is less than that in the case of $k = 1$. This confirms our experience that the more items are auctioned, the lower the price a buyer will pay. In Fig. 2, it can be also noticed that even for the limited number of players, e.g., five nodes, there can still be collected a certain number (around 50) of footprint signatures from each participant. These results show that our AVATAR scheme does stimulate rational nodes to collaborate with each other to achieve the optimal location privacy.

VII. Implementation and Performance Evaluation

We implement the AVATAR scheme on a public available DTN simulator called the *Opportunistic Networking Environment Simulator* [23] and evaluate its performance under a specific application scenario, i.e., pocket switched networks. We run simulation with 150–250 mobile nodes that are uniformly deployed in an area of 4000 m × 4000 m. The average speed of each node varies from 1.8 to 5.4 km/h, and the transmission coverage of each node is 100 m. Each mobile node is first randomly scattered on one position of the roads and moves toward another randomly selected position along the paths in the map. AVATAR could build on a specific public key signature scheme, such as the Rivest–Shamir–Adleman algorithm or the Elliptic Curve Digital Signature Algorithm (ECDSA). In the simulation, we choose the ECDSA as the basic footprint signature generation and verification scheme. Based on the given scenario setting, we implement AVATAR on top of a typical multicopy DTN routing protocol, i.e., the Spray and Wait routing (S&W) protocol [21]. At the end of this simulation, we also compare the S&W protocol with two other protocols, including epidemic routing [24] and Prophet [25].

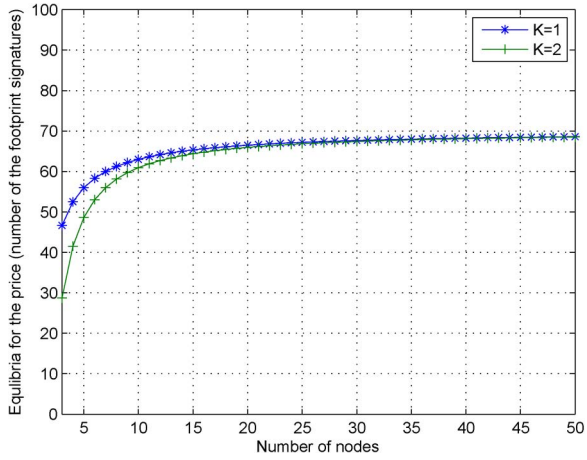


Fig. 2. Equilibria versus number of nodes in a VMixzone auction game.

A. Evaluation of Message Delivery Rate p_i and q_i

The expected benefit of AVATAR participants depends on the following factors: ΔT_1, the interval between the moment of $\mathcal{N}_i$ receiving the request and t_1; ΔT_2, which is defined as the interval between t_1 and t_2; and network density D. For an applicable AVATAR, under a specific network density setting, we should ensure that the message between the requester and the AVATAR participants could be delivered within a predefined duration, i.e., ΔT_1 and ΔT_2, at a high probability. Without loss of generality, we use a uniform parameter time-to-live (TTL) to represent ΔT_1 and ΔT_2 and the node number to represent network density D. To demonstrate the applicability of AVATAR, we implement AVATAR with different node numbers and obtain the response successful delivery rate p_i and rewarding successful delivery rate q_i under different TTL settings.

In Fig. 3(a), we evaluate p_i under three specific kinds of node number (150/200/250 nodes) and obtain the value of p_i under different TTLs, which range from 5 to 30 min. It is observed that p_i grows along with the increase in TTL. It is also observed that the number of nodes has little impact on response delivery rate p_i. The simulation results show that, under various node numbers, the response delivery rate could achieve more than 50% if TTL is set to more than 10 min. This is because the position between the requester and the collaborators is within a predefined range $\overline{\mathcal{R}}$, which has a positive effect on p_i.

Similarly, in Fig. 3(b), we investigate the impact of network nodes and TTL on rewarding message successful delivery rate q_i. It is observed that, unlike p_i, after reaching a certain TTL such as 15 min, q_i could achieve more than 50%. However, the number of nodes has little effect on the delivery rate.

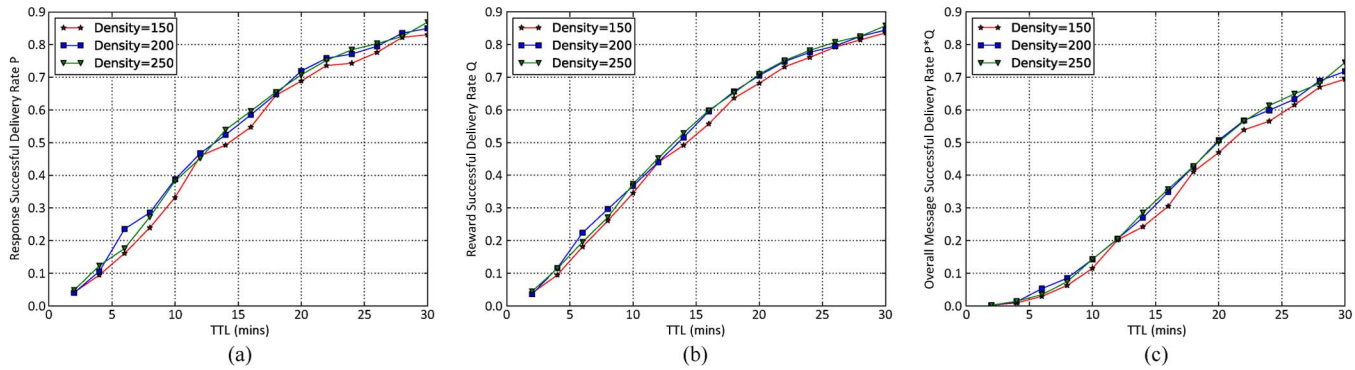


Fig. 3. Message delivery rate under different TTLs. (a) p_i. (b) q_i. (c) Overall message delivery rate.

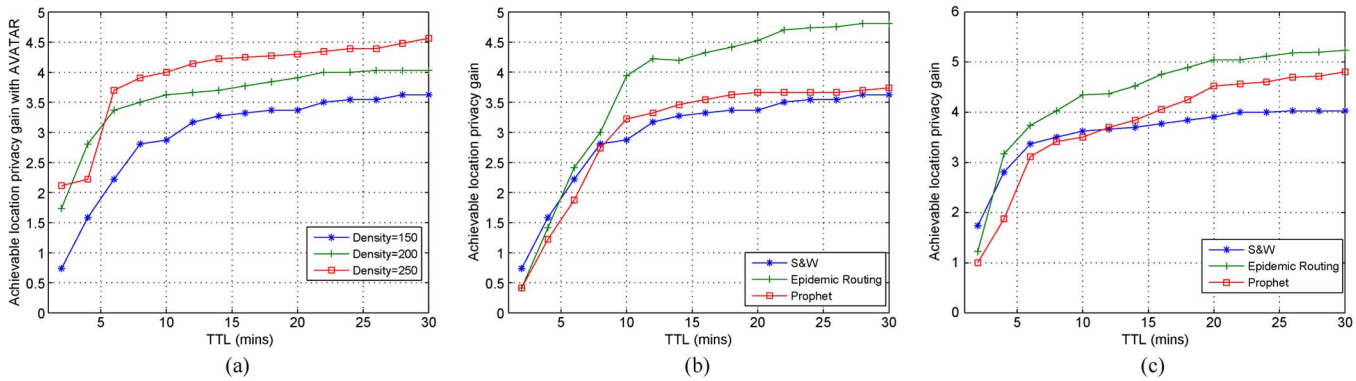


Fig. 4. Location privacy gain of AVATAR with different routing protocols. (a) Location privacy gain of the S&W protocol under different TTLs. (b) Comparison of S&W, Epidemic, and Prophet protocols under different TTLs. (c) Comparison of S&W, Epidemic, and Prophet protocols under different TTL node $= 200$.

In Fig. 3(c), we evaluate the overall message successful rate by combining the simulation results of p_i and q_i. It is observed that, in the case of a small node number such as 150 nodes, the overall message successful rate grows from 10% to 70% when increasing TTL from 10 to 30 min. In the case of 250 nodes, the overall message successful rate could achieve more than 50% given a 20-min TTL, which ensures that the AVATAR participants could receive rewarding at a high probability.

B. Location Privacy Gain With AVATAR

Here, we investigate the location privacy gain by adopting the AVATAR scheme. We set the attacker's observation range at 100 m and the VMixzone range at 500 m. With the AVATAR scheme, the nodes with the range of 500 m could improve location privacy by exchanging their footprint signatures. We compare the location privacy entropy before and after using AVATAR, and we also compare the privacy gains by using different routing protocols.

In Fig. 4(a), we evaluate the location privacy gain with S&W routing protocols. It can be seen that in three network density settings, the location privacy gain grows along with the increase in TTL. For example, with 150 nodes in our simulation, when increasing the TTL from 5 to 30 min, the achievable location privacy gain increases from 0.65 to 3.25. It is also observed that a higher network density (node number) results in a higher location privacy gain. When the node number increases from 150 to 250, the achievable location privacy gain increases from 3.25 to 4.5 when the TTL is set to 30 min. This is because faster data propagation could be achieved in DTNs under a higher network density even under the same TTL.

In Fig. 4(b) and (c), we evaluate the impact of different routing protocols on the performance of AVATAR. It is shown that epidemic routing achieves fast data propagation speed and, thus, achieves a higher location privacy gain under a specific TTL setting. This may be because epidemic routing incurs a higher transmission overhead. However, the S&W protocol achieves a similar privacy gain as the Prophet protocol when the node number is 150. For the node number of 200, the Prophet protocol shows its advantage over the S&W protocol after a particular TTL threshold, i.e., TTL $= 13$.

In summary, the given evaluations demonstrate the performance of AVATAR in terms of response delivery rate p_i, rewarding message delivery rate q_i, and location privacy improvements. The simulation results show that AVATAR could significantly improve location privacy under a reasonable TTL and network density setting. Our simulations also show that the different choice in routing protocols may affect the overall AVATAR performance. However, no matter which kind of DTN routing protocol is adopted, location privacy improvement is obvious, which further justifies our motivations.

VIII. Conclusion and Future Work

In this paper, we have introduced AVATAR, which is a novel location privacy protection scheme for DTNs. AVATAR takes advantage of the opportunistic collaborations of DTN nodes to increase location privacy by allowing remote nodes to generate some virtual nodes around the target node. To encourage each AVATAR participant to contribute more signatures to the VMixzone, we introduced a reward mechanism by modeling it as the multiunit discriminatory auction game and discussed its Nash equilibrium price. The simulation result has verified the effectiveness of our AVATAR scheme. However, the current AVATAR scheme design in this paper is under the assumption of external attackers. For the case of internal attackers, which hold the real authorized credential from the OSM, AVATAR can still be secure when the requester can be trusted because a malicious AVATAR participant cannot link the old/private pseudonyms of the others. Our future work includes designing a secure protocol to prevent attacks launched by a malicious requester.

References

[1] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A new VANET-based smart parking scheme for large parking lots," in *Proc. IEEE INFOCOM*, Rio de Janeiro, Brazil, Apr. 19–25, 2009, pp. 1413–1421.

[2] T. Hossmann, T. Spyropoulos, and F. Legendre, "Know the neighbor: Towards optimal mapping of contacts to social graphs for DTN routing," in *Proc. IEEE INFOCOM*, 2010, pp. 1–9.

[3] Q. Li, S. Zhu, and G. Cao, "Routing in socially selfish delay tolerant networks," in *Proc. IEEE INFOCOM*, 2010, pp. 1–9.

[4] H. Zhu, X. Lin, R. Lu, X. Shen, D. Xing, and Z. Cao, "An opportunistic batch bundle authentication scheme for energy constrained DTNs," in *Proc. IEEE INFOCOM*, 2010, pp. 1–9.

[5] H. Zhu, X. Lin, R. Lu, PH. Ho, and X. Shen, "SLAB: A secure localized authentication and billing scheme for wireless mesh networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 10, pp. 3858–3868, Oct. 2008.

[6] F. Li, A. Srinivasan, and J. Wu, "Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets," in *Proc. IEEE INFOCOM*, 2009, pp. 2428–2436.

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

[8] T. Xu and Y. Cai, "Feeling-based location privacy protection for location-based services," in *Proc. ACM CCS*, 2009, pp. 348–357.

[9] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A secure multilayer credit-based incentive scheme for delay-tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 8, pp. 4628–4639, Oct. 2009.

[10] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Comput.*, vol. 2, no. 1, pp. 46–55, Jan. 2003.

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

[12] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Enhancing security and privacy in traffic-monitoring systems," *IEEE Pervasive Comput.*, vol. 5, no. 4, pp. 38–46, Oct.–Dec. 2006.

[13] M. Gruteser and D. Grunwald, "Enhancing location privacy in wireless LAN through disposable interface identifiers: A quantitative analysis," *Mob. Netw. Appl.*, vol. 10, no. 3, pp. 315–325, Jun. 2005.

[14] B. Greenstein, D. McCoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall, "Improving wireless privacy with an identifier-free link layer protocol," in *Proc. ACM Mobisys*, 2008, pp. 40–53.

[15] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *Proc. ACM WISEC*, 2010, pp. 89–98.

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

[17] S. Du, X. Li, J. Du, and H. Zhu, "An attack-and-defence game for security assessment in vehicular ad hoc networks," *Peer-to-Peer Netw. Appl.*, pp. 1–14, Mar. 2012.

[18] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A probabilistic misbehavior detection scheme towards efficient trust establishment in delay-tolerant networks," *IEEE Trans. Parallel Distrib. Syst.*, [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6463402

[19] H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service-oriented vehicular networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 4, pp. 16–22, Aug. 2008.

[20] C. Shannon, "The mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 30, no. 1, pp. 50–64, Jan. 1948.

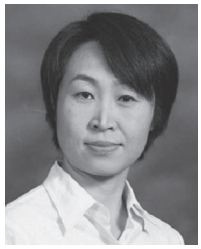
[21] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Efficient routing in intermittently connected mobile networks: The multiple-copy cast," *IEEE/ACM Trans. Netw.*, vol. 16, no. 1, pp. 77–89, Feb. 2008.

[22] W. Vickrey, "Auctions and bidding games," in *Recent Advances in Game Theory*. Princeton, NJ, USA: Princeton Univ. Press, 1962.

[23] The One Simulator. [Online]. Available: http://www.netlab.tkk.fi/tutkimus/dtn/theone/

[24] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," Duke Univ., Durham, NC, USA, Tech. Rep., 2000.

[25] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," in *Proc. SAPIR*, 2004, pp. 239–254.



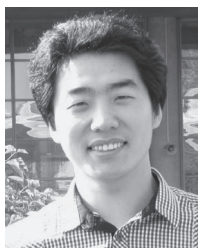
Suguo Du received the B.Sc. degree in applied mathematics from the Ocean University of China, Qingdao, China, in 1993; the M.Sc. degree in mathematics from Nanyang Technological University, Singapore, in 1998; and the Ph.D. degree from Coventry University, Coventry, U.K., in 2002.

She is currently an Associate Professor with the Department of Management Science, Antai College of Economics and Management, Shanghai Jiao Tong University, Shanghai, China. Her current research interests include risk and reliability assessment, fault tree analysis using binary decision diagrams, fault detection for nonlinear systems, and wireless network security management.

Haojin Zhu (M'09) received the B.Sc. degree in computer science from Wuhan University, Wuhan, China, in 2002; the M.Sc. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2005; and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2009.

He is currently an Associate Professor with the Department of Computer Science and Engineering, Shanghai Jiao Tong University. His current research interests include wireless network security and distributed system security.

Dr. Zhu was a co-recipient of best paper awards at the IEEE International Conference on Communications (ICC 2007) Computer and Communications Security Symposium and the Third International Conference on Communications and Networking in China (Chinacom 2008) Wireless Communications Symposium. He served as a Guest Editor for the IEEE Networks and an Associate Editor for the *KSII Transactions on Internet* and *Information Systems* and *Ad Hoc and Sensor Wireless Networks*. He currently serves on the Technical Program Committees of several international conferences, such as the International Conference on Computer Communications, the Global Communications Conference, the International Conference on Communications, and the Wireless Communications and Networking Conference.



Xiaolong Li received the B.Eng. degree in communication engineering from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2009 and the M.Sc. degree from Shanghai Jiao Tong University, Shanghai, China, in 2013, where he is currently working toward the Ph.D. degree with the Department of Management Science.

His research interests include risk and reliability assessment, network security assessment, and other areas of system and management science.

Kaoru Ota (M'12) received the M.Sc. degree in computer science from Oklahoma State University, Stillwater, OK, USA, in 2008 and the Ph.D. degree in computer science and engineering from The University of Aizu, Aizu-Wakamatsu, Japan, in 2012.

From March 2010 to March 2011, she was a Visiting Scholar with the Broadband Communications Research Group, University of Waterloo, Waterloo, ON, Canada. Moreover, she was a Japan Society for the Promotion of Science Research Fellow with the Graduate School of Information Sciences, Tohoku University, Sendai, Japan. She is currently an Assistant Professor with the Department of Information and Electronic Engineering, Muroran Institute of Technology, Muroran, Japan. Her research interests include wireless sensor networks, vehicular ad hoc networks, and ubiquitous computing.

Mianxiong Dong (S'07) received the B.S. and M.S. degrees in computer science and engineering from The University of Aizu, Aizu-Wakamatsu, Japan, in 2006 and 2008, respectively.

He was a Japan Society for the Promotion of Science (JSPS) Research Fellow with the School of Computer Science and Engineering, The University of Aizu. From April 2010 to March 2011, he was with the Broadband Communications Research Group, University of Waterloo, Waterloo, ON, Canada, supported by the JSPS Excellent Young Researcher Overseas Visit Program. From January 2007 to March 2007, he was a Visiting Scholar with West Virginia University, Morgantown, WV, USA. From August 2007 to September 2007, he was a Research Associate with Tsukiden Software Philippines, Inc. He was also a Foreign Research Fellow with the NEC C&C Foundation, Japan, and a Research Fellow with the Circle for the Promotion of Science and Engineering, Japan. He is currently a Research Scientist with the A3 Foresight Program (2011–2014) funded by the JSPS, the National Natural Science Foundation of China, and the National Research Foundation of Korea. His research interests include wireless sensor networks, vehicular ad hoc networks, wireless network security, and pervasive computing.

Mr. Dong received the Best Paper Award at the Tenth IEEE International Conference on High-Performance Computing and Communications (HPCC 2008) and the IEEE International Conference on Embedded Software and Systems (ICESS 2008).