EPS: An Efficient and Privacy-Preserving Service Searching Scheme for Smart Community

Xiaohui Liang, *Student Member, IEEE*, Kuan Zhang, Rongxing Lu, *Member, IEEE*, Xiaodong Lin, *Member, IEEE*, and Xuemin Shen, *Fellow, IEEE*

***Abstract*— Smart community leverages information and communications technology to improve the quality of life in terms of education, health care, and government services. In smart community, residents manage their home appliances to cooperate on stabilizing renewable power supply, energy saving, and information communications. In this paper, we propose an efficient and privacy-preserving service searching scheme (EPS) for smart community to enable residents to receive some Internet bandwidth from cooperative nearby homes so as to obtain pervasive Internet access at the cheap cost. Specifically, the EPS enables a resident to send a service request to nearby homes, and the latter responds the request with either uploading data via Internet connection or forwarding data to other homes via WiFi. As the Internet and WiFi bandwidth for homes is limited, the homes assign residents with different priorities and prefer to serve residents with high priorities. The priority is determined by a proximity score between residents and home owners, and the identity information is not disclosed in the calculation process. Moreover, the EPS preserves the location privacy of residents by adopting the multiple pseudonym techniques. Detailed privacy analyses in terms of the identity privacy and the location privacy are provided. In addition, the communication efficiency is validated through extensive simulations.**

***Index Terms*— Internet of Things, smart community, privacy preservation, cooperative network.**

I. Introduction

SMART community [1]–[3], which is composed of networked smart homes in a local residential region and formed upon the agreement of participating home owners with respect to local geographic, terrain and zoning features, is a promising application of Internet of Things (IoT). Smart homes are essential components of smart community, where communication devices such as personal computers, smart phones, and tablets are connected to a wireless router (i.e., home gateway) [4]–[6]. In addition, home appliances such as anti-theft system, air conditioner can receive control instructions from the home gateway such that the residents can have an easy and real-time control. Home gateways also represent their hosting smart homes and together constitute a wireless multi-hop network through the WiFi technology. This pervasive wireless multi-hop network can cover the whole smart community from public entertaining centers to pedestrian streets where the residents often walk around. Furthermore, it allows the residents outside of home to timely upload the critical information (e.g., health information) via the Internet bandwidth shared by nearby smart homes. The bandwidth sharing concept [7] has been proposed in a mobile environment where users are able to request other communication devices in the proximity as mobile data relays and their demand on the cellular infrastructure is reduced. A commercial solution proposed and implemented by Fon company is that a member of Fon community agrees to share a small amount of WiFi at home, and gets free Internet roaming at Fon Spots (over seven million spots now) worldwide in return. Similar to Fon, in the smart community, if every home shares a small portion of bandwidth, residents with smartphones could obtain the Internet access from the cooperative homes at the cheap cost. The smart community thus extends residents communication capabilities in space and enables pervasive Internet-based mobile applications.

Privacy is another emerging issue that has received considerable attention recently. In the smart community, residents require extensive privacy protections. The identity information is the most privacy-sensitive information to individuals. Once it is revealed to the malicious attackers, the behaviors of residents are easy to be tracked and linked. Besides, residents do not want to disclose the location information to untrusted entities. In the smart community, residents may have the fixed and privacy-sensitive mobility routes, e.g., visiting the snack store in the afternoon and jogging on the street after dinner. The attackers can easily identify a resident by observing when and where the resident has visited. Thus, the access of the location information should be carefully restricted. Other than privacy, communication efficiency and reliability are essential to the services provided by smart homes. When residents move, the data relay strategies have to be adaptively adjusted such that residents can still obtain the satisfied services from the smart homes. In the following, we denote residents as users and smart home owners as homes for simplicity.

In this paper, we consider users send their service requests, e.g., how much Internet bandwidth is needed, to the nearby homes. The homes either consume the Internet bandwidth (IB)

Manuscript received January 31, 2013; revised April 25, 2013; accepted May 3, 2013. Date of publication May 17, 2013; date of current version August 28, 2013. This work was supported in part by the International Cooperative Program of Shenzhen City under Grant ZYA201106090040A. The associate editor coordinating the review of this paper and approving it for publication was Dr. Chonggang Wang.

X. Liang, K. Zhang, and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo N2L 3G1, Canada (e-mail: x27liang@bbcr.uwaterloo.ca; k52zhang@bbcr.uwaterloo.ca; xshen@bbcr.uwaterloo.ca).

R. Lu is with the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore (email: rxlu@ntu.edu.sg).

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

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

Digital Object Identifier 10.1109/JSEN.2013.2263793

to upload the data or consume the WiFi bandwidth (WB) to relay the data to other homes. If receiving multiple service requests from users, a home starts to serve the users with high priorities. The priority can be determined by a proximity score between users and homes. Specifically, we propose an efficient and privacy-preserving service searching (EPS) scheme to enable users to request the bandwidth from nearby homes and schedule the data relay strategies. We introduce a threshold-based attribute structure and develop a privacy-preserving attribute authentication scheme for preserving the identity privacy. We also adopt the multiple pseudonym techniques to preserve user location privacy. Lastly, we conduct extensive simulations based on a geographic map and evaluate the EPS in terms of average service rate and average obtained bandwidth.

The remainder of this paper is organized as follows. Section II introduces the related work. The network model and the design goals are defined in Section III. Then, the EPS is proposed in Section IV and its privacy properties are analyzed in Section IV. The performance evaluation is presented in Section V, followed by the conclusions given in Section VI.

II. Related Work

Recently, the smart community, as a typical IoT application, receives considerable attentions [1], [3], [5], [6]. Li *et al.* [1] proposed a smart community architecture, including home domain, community domain and service domain. They showed some interesting IoT applications, such as neighborhood watch and pervasive healthcare, and presented the future research challenges, such as cooperative authentication and detecting unreliable nodes. Liang *et al.* [3] developed a remote healthcare system with privacy-preservation in the smart community where the networked homes are able to help users deliver health information to online medical practitioners. They replaced the unique identity with the attributes to protect the identity privacy, and restricted the access of location information to preserve the location privacy. Han *et al.* [5] devised a smart home control system to efficiently use energy in an individual home domain through IEEE 802.15.4 and ZigBee. The disjoint multi-path routing protocol is proposed to provide a stable communication channel and save energy for data transmission. Son *et al.* [6] proposed a resource-aware smart home management system and defined a resource relation graph to hierarchically manage home resources. The proposed management system not only supports advanced future smart home services, but also improves the response time for controlling smart home. Guo *et al.* [8] proposed an opportunistic IoT, which explores social impacts and enables the opportunistic connection among smart devices, homes, and communities.

Privacy preservation [9]–[11] as a fundamental user requirement is also important to the applications in the smart community. A recent proposal in [12] indicated that one or few snapshots of a user's location over time might assist an adversary to identify the user's trace, and an effective attack was presented to identify victims with high probability. As a defense technique, the *multiple-pseudonym* technique providing both identity and location privacy is widely applied

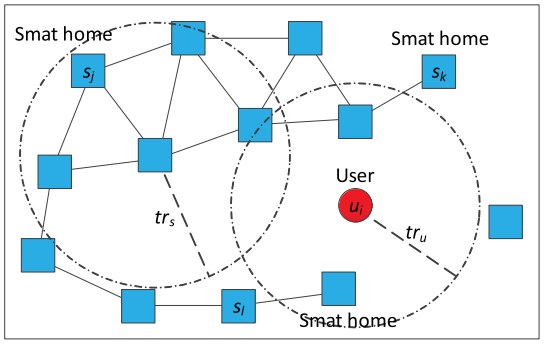


Fig. 1. The smart community with networked homes.

in literatures [13]–[16]. Freudiger *et al.* [14] developed a user-centric location privacy model to measure the evolution of location privacy over time, and they derived the equilibrium strategies on changing pseudonyms for each user from the game-theoretic perspective. Beresford *et al.* [17], [18] explored the concept of mix zone and utilized pseudonym techniques to preserve user location privacy. Lu *et al.* [19] addressed the location privacy in vehicular ad hoc networks by utilizing the social spots to deliver messages for users. Zhang *et al.* [20] further improved the location privacy preservation by exploiting Voronoi diagram features to deploy social spots. Most of research works adopt multiple-pseudonym techniques to achieve unlinkability and preserve user's location privacy.

III. Network Model and Design Goal

A. Network Model

We consider a homogeneous smart community consisting of m homes denoted by $\{s_1, s_2, \cdots, s_m\}$ as shown in Fig. 1. Homes (precisely, home gateways) have equal wireless communication range, denoted by tr_s. They are regularly distributed in the smart community. Homes are well interconnected and form a wireless multi-hop structure which provides a stable and local communication platform inside of the smart community. There are n mobile users $\{u_1, u_2, \cdots, u_n\}$ in the smart community. Each user u_i is equipped with a smartphone p_i. The smartphone p_i has a WiFi interface and can communicate with the nearby homes. The communication range of p_i is tr_u ($tr_u \leq tr_s$). A multiple pseudonym technique [14], [21], [22] is adopted, i.e., u_i is assigned with a set of asymmetric key pairs and uses the alternatively changing public keys as the user's pseudonyms $\{pid_i\}$ for the data communication. The unique identity can be protected as only literally-meaningless pseudonyms are exposed to the public. By frequently changing its pseudonym for authentication over time, users protect their identity privacy and location privacy due to the unlinkability of old and new pseudonyms. A non-exhaustive list of notations to be used throughout the rest of the paper can be found in Table I.

Service requests from users: Users in the smart community need to upload/download data to/from the Internet. Each user u_i has an initial request for the IB b_i^I. It sends a service request to nearby homes in k hops expecting that the homes share the IB or the WB with it.

TABLE I
FREQUENTLY USED NOTATIONS

u_i	A user
s_j	A home
$\mathcal{A}_u$	A universal attribute set $\{a_1, a_2, \cdots, a_l\}$
$\mathcal{A}_i, \mathcal{A}_j \subseteq \mathcal{A}_u$	Attribute sets of u_i and s_j
$\bar{s}_{i,j}$	Proximity score between u_i and s_j
b_i^I	The requested Internet bandwidth of u_i
k	The maximum hop counts between homes and users
b_j^I	The available Internet bandwidth of s_j
b_j^W	The available WiFi bandwidth of s_j
$b_{i,j}^I$	The Internet bandwidth of s_j occupied by u_i
$b_{i,j}^W$	The WiFi bandwidth of s_j occupied by u_i

Services from homes: Homes can act as either service providers to share the IB with users, or service relays to share the WB with users. A home s_j for $1 \leq j \leq m$ has the available IB b_j^I and the available WB b_j^W. The WB is generally much larger than the IB for each home. Denote I_1 as the index set of users that a home s_j agrees to share IB and I_2 as the index set of users that s_j agrees to share WB. If s_j agrees to provide users u_{i_1} for $i_1 \in I_1$ with the IB b_{j,i_1} and users u_{i_2} for $i_2 \in I_2$ with the WB b_{j,i_2}, we have $\sum_{i_1 \in I_1} b_{j,i_1} \leq b_j^I$ and $\sum_{i_2 \in I_2} b_{j,i_2} \leq b_j^W$.

Proximity of home and user: Each home s_j is unable to satisfy all the service requests when the total requested bandwidth is beyond its available bandwidth. In this case, s_j prefers to serve the user who has a closer relationship with a higher priority. The relationship between a home and a user can be identified by revealing their unique identities to each other. However, in practise, they may not be willing to disclose the unique identities due to privacy concerns. We follow the idea of attribute-based profiles [3], [23]. The attributes are associated with the homes and the users prior to the deployment of the EPS. An offline trusted authority (TA) initializes a universal attribute set $\mathcal{A}_u = \{a_1, a_2, \cdots, a_l\}$ and associates user u_i with an attribute set $\mathcal{A}_i \subseteq \mathcal{A}_u$. The attributes represent the interests of users. As well, home s_j inherits the attribute set $\mathcal{A}_j$ of the owner. The relationship between u_i and s_j is measured by the number of the common attributes of $\mathcal{A}_i$ and $\mathcal{A}_j$. The larger the number, the closer the relationship between a home and a user.

B. Design Goal

We aim to propose an efficient and privacy-preserving service searching in the smart community. Since data confidentiality can be achieved by traditional end-to-end encryption schemes, it will not be detailed in the EPS. Specifically, the following objectives should be achieved.

- *Efficient service searching and maintenance:* The EPS always consumes the minimum communication overhead to enable users to search for the cooperative homes and maintain the connections with them.
- *Identity privacy preservation:* Disclosing the unique identity incurs serious privacy violation and enables malicious attackers to track the user's behavior easily. The EPS must protect the unique identity from being accessed by unauthorized entities.
- *Location privacy preservation:* Location information is privacy-sensitive and tightly related to personal life. The location information of a user should not be continuously revealed to the malicious attackers. The EPS should restrict the access of the location information and make the disclosed locations of users unlinkable.

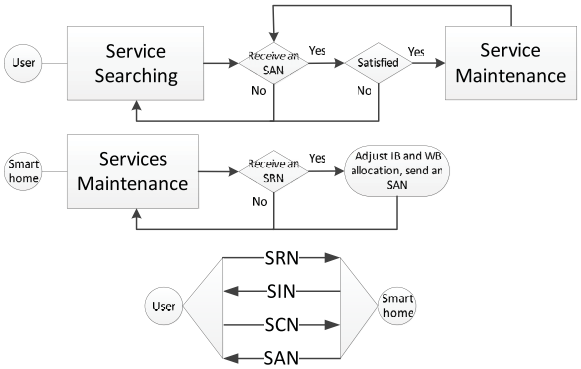


Fig. 2. The communication phase of users and homes.

IV. EPS CONSTRUCTION

In this section, we describe the proposed EPS in details. We give an overview of the EPS including a communication phase of users and a communication phase of homes. Then, we introduce the proximity score calculation algorithm and the two phases in details.

A. Overview

The EPS includes the communication phase of users and the communication phase of homes. The users will run the EPS according to Fig. 2. The user u_i is initially in the "service searching" status. In this status, u_i keeps sending a service request notification (SRN) to the nearby homes. When u_i receives a service information notification (SIN) from a home s_j, u_i knows how much IB and WB s_j can provide. Then, u_i chooses the homes and sends the service confirmation notifications (SCNs) to them. After receiving the service acceptance notifications (SANs) from the chosen homes, u_i checks if its request is satisfied, i.e., the obtained IB $\bar{b}_i^I$ is no less than the requested IB b_i^I. If satisfied, u_i changes its status to the "service maintenance"; otherwise, u_i is still in the "service searching" status and continuously sends an SRN for requesting the IB $b_i^I - \bar{b}_i^I$. In the "service maintenance" status, u_i does not send the SRNs, but keep communicating with the service providers.

The homes will run the EPS according to Fig. 2. When receiving an SRN from u_i, s_j checks the current services and sends an SIN to indicate how much IB and WB that it can provide. If the IB is positive, s_j is willing to serve u_i as a service provider; if the WB is positive, s_j is willing to serve as a service relay and forward the SRN to other homes. When receiving an SCN from u_i, s_j updates the services and ensures that the user with a larger proximity score can be served with

a higher priority. After the service update, s_j sends the SANs to the users with the updated IB and WB.

Four notifications transmitted between users and homes are explained in the following. They are service request notification (SRN), service information notification (SIN), service confirmation notification (SCN), and service acceptance notification (SAN). The protocol in Fig. 2 shows the order of those four types of signals.

- SRN: $u_i \rightarrow s_j$. It includes the attribute proof and a new pseudonym of u_i. From the SRN, s_j is able to calculate the proximity score and determine how much IB and WB it can provide for u_i.
- SIN: $s_j \rightarrow u_i$. It includes the available IB and WB for s_j. From the SIN, u_i chooses s_j as a service provider, a service relay or both to obtain the satisfied service.
- SCN: $u_i \rightarrow s_j$. It includes the chosen homes and the corresponding IB and WB assigned by u_i. s_j deducts the occupied IB and WB from its available IB and WB.
- SAN: $s_j \rightarrow u_i$. It includes the accepted IB and WB by s_j. u_i deducts the obtained IB and WB from the total requested IB and WB.

In the EPS, time is divided into equal slots. In each time slot, users firstly send their SRNs to homes if they need the available IB. After receiving all SRNs from users, homes make a bandwidth allocation based on the service priority. Homes always firstly assign the bandwidth to the users with higher priorities. Based on the new allocation, homes send SANs to users who obtain different amount of bandwidth compared to the previous time slot. Note that, the duration of one time slot directly impacts the overhead of the maintenance operations. If the duration of a time slot increases, homes perform the maintenance less frequently. As a result, users with higher priorities may not immediately obtain their services because they may miss the maintenance operation and need to wait for the new allocation until the next time slot. In this case, it is unfair for the users with high priorities, but the average obtained bandwidth of all users may not be influenced.

B. Proximity Score Calculation

We first introduce the proximity score calculation algorithm which will be used in the communication phase of homes. The proximity score calculation algorithm is used for ranking the priority levels of users. Homes obtain the attribute proof of users from their SRNs. The attribute proof is designed as a threshold-based attribute structure with the maximum threshold gate value d. An example 3-of-8 structure is shown in Fig. 3. By using this structure, a user is able to prove that he/she has at least three of the eight attributes $(a_1, \cdots, a_8)$. In the following, we adopt the bilinear pairing technique [24] to implement the authentication scheme.

Bilinear Pairing Notations: Let $\mathbb{G}$ and $\mathbb{G}_T$ be two finite cyclic groups of the same large order n, where $n = pq$ is a product of two large primes p and q. Suppose $\mathbb{G}$ and $\mathbb{G}_T$ are equipped with a pairing, i.e., a non-degenerated and efficiently computable bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ such that i) $\forall g, h \in \mathbb{G}$, $\forall a, b \in \mathbb{Z}_n$, $e(g^a, h^b) = e(g, h)^{ab}$; and ii) $\exists g \in \mathbb{G}$, $e(g, g)$ has order n in $\mathbb{G}_T$.

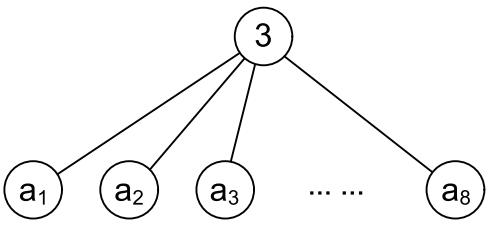


Fig. 3. Threshold-based attribute structure.

Initialization: System public parameters $\mathsf{pub} = (n, g, u, h, \mathbb{G}, \mathbb{G}_T, e, H, \Delta, T_y (1 \leq y \leq l + d - 1), \mathcal{A}_u \cup \mathcal{A}_r)$, where an offline trusted authority generates a redundant attribute set $\mathcal{A}_r = \{a_{l+1}, \cdots, a_{l+d-1}\}$, two generators (g, u) of $\mathbb{G}$, a generator h of $\mathbb{G}_q$ ($\mathbb{G}_q$ is a subgroup of $\mathbb{G}$ with order q), a secure cryptographic hash function $H : \{0, 1\}^* \rightarrow \mathbb{Z}_n^*$, a random number $\delta \in \mathbb{Z}_n^*$, random numbers $t_y \in \mathbb{Z}_n^*$ for $1 \leq y \leq l + d - 1$, $T_y = g^{t_y}$, and $\Delta = e(g, u)^{\delta}$. $(\delta, (t_y)_{1 \leq y \leq l+d-1})$ are the master keys.

Key Generation: When registering to the system, an offline trusted authority generates a unique random number $t \in \mathbb{Z}_n^*$, a random polynomial $q(x) = \kappa_{d-1}x^{d-1} + \kappa_{d-2}x^{d-2} + \cdots + \kappa_1 x + \delta$. User u_i obtains the secret key $E_i = \langle k_d, (d_y)_{a_y \in \mathcal{A}_i \cup \mathcal{A}_r} \rangle$, where $k_d = t$ and $d_y = u^{\frac{q(y)}{t+t_y}}$.

Attribute Proof Generation: Let u_i's attribute structure be $\mathcal{T}_i$, the threshold value be th, and an attribute set corresponding to $\mathcal{T}_i$'s leaf nodes be Θ_i. Let $\Phi_i \subseteq \mathcal{A}_i \cap \Theta_i$ be an attribute set with size th. u_i chooses a subset $\mathcal{A}_{r'} = \{a_{l+1}, \cdots, a_{l+d-th}\} \subseteq \mathcal{A}_r$ ($|\mathcal{A}_{r'}| = d - th$). Then, for each attribute $a_y \in \Psi = \Phi_i \cup \mathcal{A}_{r'}$, u_i computes the Lagrange coefficient $\omega_y = \sum_{w | a_w \in \Psi, w \neq y} \frac{0-w}{y-w}$. u_i randomly selects $r_t, r_p, r_y \in \mathbb{Z}_n^*$ for $a_y \in \Theta_i \cup \mathcal{A}_{r'}$ and computes S_y for $a_y \in \Theta_i \cup \mathcal{A}_{r'}$ as follows

$$S_y = \begin{cases} d_y^{\omega_y} \cdot h^{r_y}, \text{ if } a_y \in \Psi \\ h^{r_y}, \text{ if } a_y \in \Theta_i \setminus \Phi_i \end{cases} \tag{1}$$

u_i outputs the attribute proof

$$\sigma_i = \langle pid_i, \mathcal{T}_i, S_t, S_p, (S_y)_{a_y \in \Theta_i \cup \mathcal{A}_{r'}}, \pi_1, \pi_2 \rangle,$$

where $S_t = g^{k_d} \cdot h^{r_t}$, $S_p = g^{\frac{1}{k_d + H(pid_i)}} \cdot h^{r_p}$ and

$$\pi_1 = S_p^{r_t} (g^{H(pid_i)} g^{k_d})^{r_p}, \ \pi_2 = \prod_{a_y \in \Psi} (d_y^{\omega_y})^{r_t} \prod_{a_y \in \Theta_i \cup \mathcal{A}_{r'}} (S_t T_y)^{r_y}$$

Verification: s_j receives σ_i and checks

$$\begin{cases} e(S_t g^{H(pid_i)}, S_p) \stackrel{?}{=} e(g, g) \cdot e(h, \pi_1) \\ \prod_{a_y \in \Theta_i \cup \mathcal{A}_{r'}} e(S_y, S_t T_y) \stackrel{?}{=} \Delta \cdot e(h, \pi_2), \end{cases}$$

If the two equations hold, s_j confirms that a user with pseudonym pid_i has an attribute set that satisfies $\mathcal{T}_i$. Then, u_i proves that it has pid_i using the corresponding secret keys to generate signatures. Note that, s_j is unable to check if u_i has a specific attribute because s_j without q is unable to differentiate $d_y^{\omega_y} \cdot h^{r_y} \in \mathbb{G}$ from $h^{r_y} \in \mathbb{G}_q$. This is subgroup decision problem which is considered as a computationally-hard problem [24], [25].

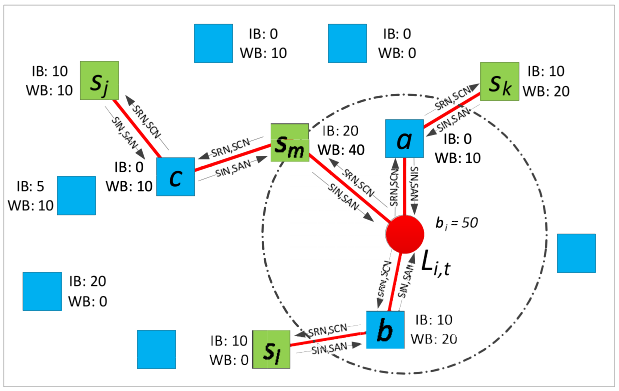


Fig. 4. Service searching.

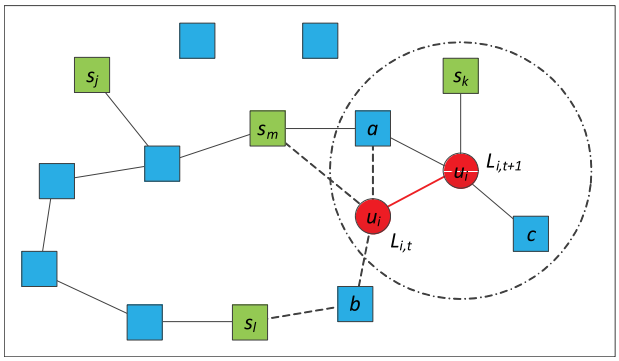


Fig. 5. Service maintenance.

Home s_j has an attribute set $\mathcal{A}_j$. Let Θ_i be the attribute set of $\mathcal{T}_i$. Denote $\psi_{i,j} = \mathcal{A}_j \cap \Theta_i$, $|\Theta_i| = \alpha$, and $|\psi_{i,j}| = \beta$. In order to output the attribute proof, u_i must use a th-size subset $\bar{\mathcal{A}}_i \subseteq \mathcal{A}_i$ which satisfies $\mathcal{T}_i$. We define $\bar{s}_{i,j}$ as the expected value of the number of attributes that appear in both $\psi_{i,j}$ and $\bar{\mathcal{A}}_i$ as follows:

$$\bar{s}_{i,j} = \sum_{x=1}^{th} x \cdot \Pr[x] = \sum_{x=1}^{th} x \cdot \frac{\binom{\beta}{x} \cdot \binom{\alpha-\beta}{th-x}}{\binom{\alpha}{th}} = \frac{th \cdot \beta}{\alpha}. \quad (2)$$

From the above equation, it can be seen that $\bar{s}_{i,j}$ increases as th or β increases and α decreases.

C. Communication Phase of Users

The user u_i has a service request aiming to obtain b_i^I IB from the cooperative nearby homes. It generates an SRN including its attribute proof and sends the SRN to the nearby k-hop homes. k is an adjustable parameter. When k is larger, more homes could be possibly the service providers. However, the shared IB and WB from faraway homes are not reliable because the data relay path may be disabled if one cooperative home switches to serve other users. The attribute proof helps the homes calculate the proximity score and determine the service priority. After sending the SRN, u_i sets a time threshold T_{SIN} and waits the SIN from the homes. When T_{SIN} expires, a user receives the SINs from multiple homes s_j. Each SIN contains the available IB and WB from each individual home. If an SIN is not received in T_{SIN}, u_i considers the home is unable to provide any IB and WB due to either communication failure or the fully occupied bandwidth. In addition, the SIN also contains the geographical information (e.g., hops and relaying path between the home and the user) such that users can find the appropriate strategy. An example is shown in Fig. 4. In the figure, u_i knows the IB and WB that it can obtain from the nearby homes.

Home selecting process: The user u_i first checks if the one-hop neighboring homes can provide larger IB than the requested IB. Denote $b_{i,1-hop}^I$ as the total IB shared by one-hop homes. If $b_{i,1-hop}^I \geq b_i^I$, u_i selects some of the one-hop homes and obtain the requested IB from them; otherwise, u_i needs to check if the two-hop homes can provide enough IB and if the one-hop homes have enough WB to act as the service relays. Denote $b_{i,2-hop}^I$ as the IB that are shared by two-hop homes, and $b_{i,1-hop}^W$ as the WB that are shared by one-hop homes. Based on $b_{i,2-hop}^I$, $b_{i,1-hop}^W$ and the geographic information, u_j schedule the relay path to obtain the largest IB from two-hop homes. If the obtained IB is larger than $b_i^I - b_{i,1-hop}^I$, u_i selects some two-hop homes as service providers and some one-hop homes as service relays to obtain $b_i^I - b_{i,1-hop}^I$; otherwise, u_i further checks the three-hop homes and possible service relays.

After the home selecting process, u_i chooses homes $s_j (j \in \mathcal{J}_{j,1})$ as service providers and homes $s_j (j \in \mathcal{J}_{j,2})$ as service relays. We have $b_i^I = \sum_{j \in \mathcal{J}_{j,1}} b_{i,j}^I$. A result of the home selecting process is shown in Fig. 4 where s_j, s_k, s_l, s_m are four service providers and a, b, c are three service relays for u_i. In this example, a is the service relay for s_k, and the WB (10 kb/s) shared by a must be no less than the IB (10 kb/s) shared by s_k. User u_i then sends the SCNs to both service providers and service relays where the occupied IB and WB are indicated. In the example, u_i sends s_m the SCN with $b_{i,m}^I = 20, b_{i,m}^W = 10$, s_j the SCN with $b_{i,j}^I = 10, b_{i,j}^W = 0$. u_i also sends the SCNs to the service relays to confirm the occupied WB.

If u_i's service request can be satisfied, i.e., u_i obtains the IB b_i^I, u_i switches to "service maintenance" status and stops sending the SRN to the nearby homes. However, if not obtaining enough IB ($\bar{b}_i^I < b_i^I$), u_i stays in "service searching" status and continuously sends the SRN for the rest IB $b_i^I - \bar{b}_i^I$.

If u_i moves to another location, the data relay path needs to be redirected according to the updated location. An example is shown in Fig. 5 where u_i moves from $L_{i,t}$ at time t to $L_{i,t+1}$ at time $t+1$. There are three possible conditions of the neighbor change. In case 1, a home a being a neighbor at time t is still a neighbor at time $t+1$. In case 2, a home b being a neighbor at time t is not a neighbor at time $t+1$. In case 3, a home c not being a neighbor at time t becomes a neighbor at time $t+1$. After arriving at $L_{i,t+1}$, u_i will check if any one-hop home who provides either IB or WB at time t is missing at time $t+1$. Consider u_i has shared the total IB $\tilde{b}_i^I$ and WB $\tilde{b}_i^W$ from the missing neighboring homes. In the example in Fig. 5, the shared IB from s_j, s_m, s_l are disabled. u_i changes its status to "service searching" and sends SRN with bandwidth requirement $\tilde{b}_i^I + \tilde{b}_i^W$. Further, u_i will also check if any non one-hop home who provides either IB or WB

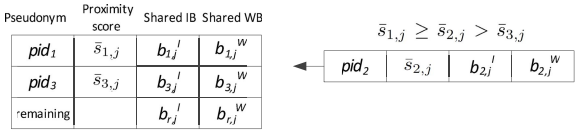


Fig. 6. Bandwidth allocation table by home s_j.

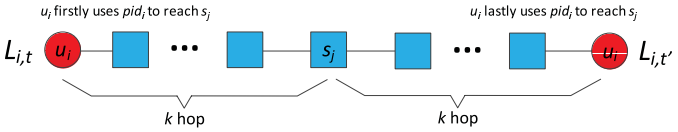


Fig. 7. Linkability of user location information.

at time t becomes a one-hop neighbor at time $t+1$. In the example, u_i has a new neighbor s_k. u_i notifies s_k that s_k could directly serve u_i without the service relay a. In this way, the communication overhead can be largely reduced. If no homes have been found in the above two checks, u_i keeps using the strategy at time $t+1$.

D. Communication Phase of Homes

Home s_j initially has the IB b_j^I and the WB b_j^W to share with users. s_j maintains a bandwidth allocation table which denotes the pseudonyms of served users and the corresponding bandwidth usage details. The table includes four columns for the pseudonyms of the users, the proximity scores between the users and s_j, the shared IB, and shared WB, respectively. In the table, users are sorted by the proximity scores in a descending order. The last row denotes the remaining IB $b_{r,j}^I$ and remaining WB $b_{r,j}^W$. Consider a home s_j serves two users u_1, u_3 at time t. The table is shown in Fig. 6, where $\bar{s}_{1,j} > \bar{s}_{3,j}$, $b_j^I = b_{1,j}^I + b_{3,j}^I + b_{r,j}^I$, $b_j^W = b_{1,j}^W + b_{3,j}^W + b_{r,j}^W$.

Consider s_j receives an SRN from a user u_2 at time $t+1$. By the proximity score calculation algorithm, s_j calculates $\bar{s}_{2,j}$ between u_2 and itself. It compares $\bar{s}_{2,j}$ with other proximity scores from other served users, and finds $\bar{s}_{1,j} \geq \bar{s}_{2,j} > \bar{s}_{3,j}$. Since u_3 has a smaller proximity score than u_2, s_j ignores the current service for u_3 and serves u_2 with a higher priority. Thus, s_j responds u_2 with an SIN indicating the available IB $b_{2,j,SIN}^I = b_{3,j}^I + b_{r,j}^I$ and the available WB $b_{2,j,SIN}^W = b_{3,j}^W + b_{r,j}^W$.

After sending the SIN, s_j sets a time threshold T_{SCN} and waits the SCN from u_2 for T_{SCN}. If it receives any other SRN, s_j records the requests but does not respond to them. If s_j does not receive the SCN from u_2 during T_{SCN}, it responds another SRN from the user with the largest proximity score. If s_j receives the SCN indicating $b_{2,j}^I (\leq b_{2,j,SIN}^I)$ and $b_{2,j}^W (\leq b_{2,j,SIN}^W)$, it assigns the requested bandwidth to u_2. Then, it checks the previous bandwidth allocation of the users with lower priorities. If $b_{2,j,SIN}^I - b_{2,j}^I \geq b_{3,j}^I$, u_3 will be continuingly served with no change and s_j checks if the user with a further lower priority can be served; otherwise, s_j prepares an SAN indicating $b_{3,j}^I = b_{2,j,SAN}^I - b_{2,j}^I$ and no available IB for other users who have a lower priority than u_3. The allocation adjustment of WB is similar to that of IB. s_j always sends the SANs to the users about their changed IB or WB from s_j.

Due to the user mobility, an established data relay path could possibly be disabled. An example is shown in Fig. 5, when u_i moves from $L_{i,t}$ to $L_{i,t+1}$, s_m is not a neighbor of u_i at time $t+1$. s_m makes the following adjustments immediately. If s_m shares the IB $b_{i,m}^I$ to u_i, it releases the IB $b_{i,m}^I$ and increases the available IB. If s_m shares the WB $b_{i,m}^W$ to u_i, it not only releases the WB $b_{i,m}^W$ and increases the available WB, but also notifies other homes which deliver services to u_i through s_m of canceling the shared IB and WB for u_i. In the communication phase of users, u_i waits time $T_{release}$ to ensure that the disconnected homes release the shared bandwidth for itself, and re-sends the SRN to request the missing bandwidth from nearby homes at time $t+1$.

V. Privacy Analysis

In this section, we analyze the privacy properties of the EPS. Our analysis focuses on how the scheme can achieve the identity privacy and the location privacy. In particular, collusion attacks launched by multiple compromised homes are considered.

a) Identity Privacy Preservation.: In the EPS, unique identities are not used in the service searching and the service maintenance. Instead, we use attributes to describe the users and the home owners. The attributes are defined as the common interests. The users and the home owners can easily obtain the attributes from the Internet social communities, e.g., Facebook, Twitter. Note that the direct disclosure of the attributes might violate user privacy and make users easily identifiable. Thus, in the EPS, we devise a privacy-preserving attribute authentication scheme where a user is able to generate an attribute proof. The attribute proof provides fuzzy attribute information such that the verifier is not clear about the user's attributes but can still calculate the approximately proximity score to determine the service priority. In addition, the multiple pseudonym technique is adopted, i.e., users apply the literally-meaningless pseudonyms in the communications. Thus, the disclosed pseudonyms do not reveal the unique identities of the users, i.e., the identity privacy is preserved.

b) Location Privacy Preservation.: In the EPS, the location information is necessarily disclosed for service searching and service maintenance. When u_i sends an SRN to the nearby homes within k-hops, the homes are able to identify the user by a pseudonym $pid_{i,1}$. After choosing the service providers, the user continuously applies $pid_{i,1}$ and the home reserves the bandwidth for the user with $pid_{i,1}$. If the user keeps using the same service strategy in different time slots, the location information of the user in different time slots will be linked by $pid_{i,1}$. However, in different time slots, if the user generates a new SRN, the EPS requires the user to apply another pseudonym $pid_{i,2}$. From the view of homes, due to the unlinkability of $pid_{i,1}$ and $pid_{i,2}$, they will treat the user who occupies the bandwidth with $pid_{i,1}$ different from the user who sends the SRN with $pid_{i,2}$. In Fig. 7, s_j is the last home that serves u_i. If u_i uses $pid_{i,1}$ to reach s_j at $L_{i,t}$ and lastly uses $pid_{i,1}$ at $L_{i,t'}$. The distance

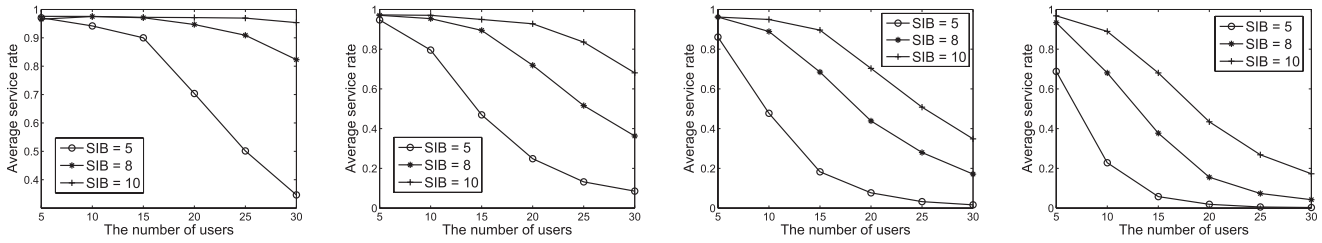


Fig. 8. Average service rate per number of users. (a) Requested IB = 20 kb/s. (b) Requested IB = 30 kb/s. (c) Requested IB = 40 kb/s. (d) Requested IB = 50 kb/s.

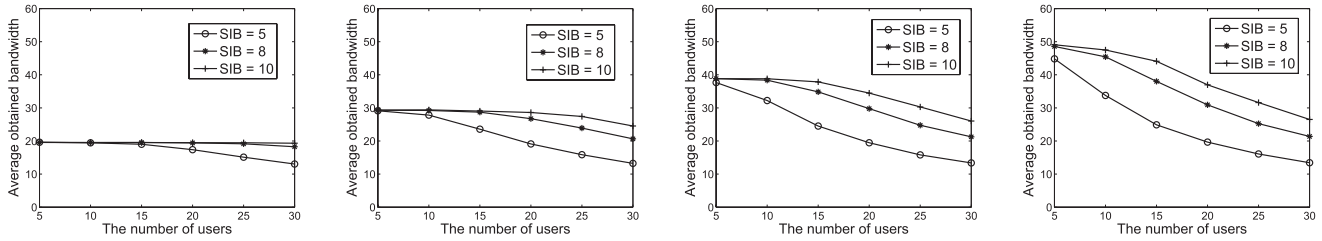


Fig. 9. Average obtained bandwidth per number of users. (a) Requested IB = 20 kb/s. (b) Requested IB = 30 kb/s. (c) Requested IB = 40 kb/s. (d) Requested IB = 50 kb/s.

Fig. 10. A geographical map of the smart community.

between two locations is maximally $2k$ hops. Thus, even if the compromised homes collude, they can only link the locations of u_i in maximum $2k$ hops.

VI. Performance Evaluation

In this section, we evaluate the performance of the EPS through the simulations. The performance metrics are the average service rate and the average obtained bandwidth. The average service rate is defined as the number of the users who obtain satisfied service to the total number of users. The average obtained bandwidth is defined as the the bandwidth obtained by all users divided by the number of users.

A. Simulation Settings

We adopt a geographic map shown in Fig. 10, where a total of 74 homes are distributed in a $650m \times 300m$ rectangular area. Each home has a communication range of $100m$. There are $n = 5, \cdots, 30$ users walking along the circular route at average speed $1.5m/s$. They always choose a destination on the route and move to it from the start point by following one of the two directions as shown in Fig. 10. After arriving at the destination, users set the current locations as the start points and choose random-selected destinations on the route and continue to move toward the destinations. Each user has a smartphone with the communication range $50m$. 25 attributes are generated in total, and 8 randomly selected attributes are associated to each user and each home. Each user generates an attribute structure which is in the form of "4 of 8" for simplicity. To generate the attribute proof, a user randomly selects 4 attributes that it has and other 4 attributes that it does not have.

In the simulation, we consider that each home initially has shared Internet bandwidth (SIB) $SIB = (5, 8, 10)$ (kb/s) and 500 (kb/s) shared WB. If a home shares 5 kb/s to the users from 8 am to 8 pm, it may maximally consume 5 * 3600 * 12 * 30 = 6.48 (gb) for either uploading or downloading the Internet data for users. From Rogers company, the home owner could have a monthly Internet cable plan with an upper bound of the usage (500,250,150,120,80,20) gb, and it is possible that a home has less than 10 gb unused Internet usage every month. In this case, the home can share some of the unused Internet bandwidth adaptively based on their own Internet usage. Each user has a service request for (20,30,40,50) (kb/s) IB and it only requests the service from homes less than two hops. We conduct a total of 2000 simulation runs for different parameters and obtain the average results which will be analyzed in the next sub-section.

B. Simulation Results

c) Average Service Rate: In Fig. 8, we plot the average service rate in terms of the number of users, the shared IB of homes, and the requested IB of users. From Fig. 8, it can be seen that when 5 users have service requests with

10 (kb/s) IB and homes provide 10 (kb/s) IB, more than 90% of users' requests can be satisfied. Because any single home can well serve a user, the 5 users can easily find nearby homes to obtain the satisfied IB. However, when the number of users increases to 20 and the homes reduces the shared IB to 5 (kb/s), only 35% of users' requests can be satisfied. In this case, a home cannot provide enough IB for a user, and multiple homes have to cooperatively serve a user. Thus, the competition among users becomes intensive; users with higher service priorities can obtain more bandwidth from homes. In addition, at some time, users may locate in the close locations, and the nearby homes have limited IB and are unable to satisfy the users. From other figures 8(b), 8(c) and 8(d), it can be seen that the average service rate reduces when the IB of the service requests increases. Especially when each user requests 40 (kb/s) and each home shares 5 (kb/s), 8 fully cooperative homes can satisfy only one user's service. However, the average service rate of $n = 15$ is 0.06, which means no user has obtained a satisfied service. It happens because users are assigned with random attributes and any of them can hardly obtain a high service priority from a large number of homes.

d) Average Obtained Bandwidth: In Fig. 9, we plot the average obtained bandwidth similar to the average service rate. From Fig. 9, it can be seen that in the case of $SIB = 5$ and $n = 30$, the average obtained bandwidth is about 13 (kb/s) though the average service rate is only 34%. In other words, though most users cannot obtain satisfied services, they still obtain considerable IB from the nearby homes. Then, by comparing the figures 9(a),9(b),9(c), and 9(d) we observe that if users increase the requested IB, the average obtained bandwidth in some cases increases while remains at the same level for other cases. For example, when $n = 10$ and $SIB = 8$, if the requested IB increases from 10 (kb/s) to 40 (kb/s), the average obtained bandwidth increases from 19.55 (kb/s) to 45.42 (kb/s); when $n = 25$ and $SIB = 5$, if the requested IB increases from 10 (kb/s) to 40 (kb/s), the average obtained bandwidth stays around 15 - 16 (kb/s). In the first case, the number of users (10) is relatively small and the shared bandwidth 8 (kb/s) of each home is relatively large. Thus, the IB of homes is not fully occupied. The average obtained bandwidth can be increased. In the second case, the shared bandwidth of homes are not enough, and thus the average obtained bandwidth reach its upper bound.

VII. Conclusion

In this paper, we have proposed an efficient and privacy-preserving service searching (EPS) scheme in the smart community. The EPS enables users outside of homes to search the cooperative nearby homes which can share the Internet bandwidth or WiFi bandwidth. When homes share the bandwidth, the service priority is determined by the proximity score between users and home owners. The homes prefer to serve the users with higher priorities. In the EPS, the Internet bandwidth shared by homes can be efficiently searched and the data relay strategies via the shared bandwidth can be managed by users. In addition, the EPS preserves both identity privacy and location privacy for users. To evaluate the EPS, we have provided its privacy analysis and conducted simulations based on a geographic map to show its efficiency in terms of average service rate and average obtained bandwidth. In our future work, we will consider the radio interference and study how to optimize the bandwidth sharing performance by adaptively controlling the transmission power of homes.

References

[1] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart community: An internet of things application," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 68–75, Nov. 2011.

[2] P. Rashidi, D. J. Cook, L. B. Holder, and M. Schmitter-Edgecombe, "Discovering activities to recognize and track in a smart environment," *IEEE Trans. Knowl. Data Eng.*, vol. 23, no. 4, pp. 527–539, Apr. 2011.

[3] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "Enabling pervasive healthcare with privacy preservation in smart community," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2012, pp. 3451–3455.

[4] C. Wu, C. Liao, and L. Fu, "Service-oriented smart-home architecture based on OSGI and mobile-agent technology," *IEEE Trans. Syst., Man, Cybern., Part C, Appl. Rev.*, vol. 37, no. 2, pp. 193–205, Mar. 2007.

[5] D. M. Han and J. H. Lim, "Smart home energy management system using IEEE 802.15.4 and zigbee," *IEEE Trans. Consum. Electron.*, vol. 56, no. 3, pp. 1403–1410, Aug. 2010.

[6] J. Son, J. H. Park, K. D. Moon, and Y. Lee, "Resource-aware smart home management system by constructing resource relation graph," *IEEE Trans. Consum. Electron.*, vol. 57, no. 3, pp. 1112–1119, Aug. 2011.

[7] E. Jung, Y. Wang, I. Prilepov, F. Maker, X. Liu, and V. Akella, "User-profile-driven collaborative bandwidth sharing on mobile phones," in *Proc. 1st ACM Workshop Mobile Cloud Comput. Services, Social Netw. Beyond*, Jun. 2010, pp. 1–9.

[8] B. Guo, Z. Yu, X. Zhou, and D. Zhang, "Opportunistic IoT: Exploring the social side of the internet of things," in *Proc. IEEE 16th Int. Conf. Comput. Supported Cooperat. Work Design*, May 2012, pp. 925–929.

[9] X. Liang, R. Lu, X. Lin, and X. Shen, "Message authentication with non-transferability for location privacy in mobile ad hoc networks," in *Proc. IEEE Global Telecommun.Conf.*, Dec. 2010, pp. 1–5.

[10] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing and swap: User-centric approaches towards maximizing location privacy," in *Proc. 5th ACM Workshop Privacy Electron. Soc.*, Jan. 2006, pp. 19–28.

[11] R. Lu, X. Lin, T. H. Luan, X. Liang, X. Li, L. Chen, and X. Shen, "Prefilter: An efficient privacy-preserving Relay Filtering scheme for delay tolerant networks," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 1395–1403.

[12] C. Y. T. Ma, D. K. Y. Yau, N. K. Yip, and N. S. V. Rao, "Privacy vulnerability of published anonymous mobility traces," in *Proc. 16th Ann. Int. Conf. Mobile Comput. Netw.*, Sep. 2010, pp. 185–196.

[13] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "A novel anonymous mutual authentication protocol with provable link-layer location privacy," *IEEE Trans. Veh. Technol.*, vol. 58, no. 3, pp. 1454–1466, Mar. 2009.

[14] J. Freudiger, M. Manshaei, J.-P. Hubaux, and D. Parkes, "On non-cooperative location privacy: A game-theoretic analysis," in *Proc. 16th ACM Conf. Comput. Commun. Security*, Aug. 2009, pp. 324–337.

[15] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–88, Feb. 1981.

[16] D. Anthony, T. Henderson, and D. Kotz, "Privacy in location-aware computing environments," *IEEE Pervas. Comput.*, vol. 6, no. 4, pp. 64–72, Oct. 2007.

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

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

[19] R. Lu, X. Lin, and X. Shen, "SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 632–640.

[20] K. Zhang, X. Liang, R. Lu, X. Shen, and H. Zhao, "VSLP: Voronoi-socialspot-aided packet forwarding protocol with receiver location privacy in msns," in *Proc. IEEE Global Commun. Conf.*, Dec. 2012, pp. 1–5.

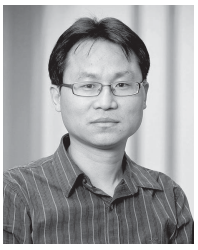
[21] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, Jan. 2012.

[22] X. Liang, X. Li, T. H. Luan, R. Lu, X. Lin, and X. Shen, "Morality-driven data forwarding with privacy preservation in mobile social networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 7, pp. 3209–3222, Sep. 2012.
[23] M. Li, N. Cao, S. Yu, and W. Lou, "FindU: Privacy-preserving personal profile matching in mobile social networks," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 2435–2443.
[24] X. Boyen and B. Waters, "Full-domain subgroup hiding and constant-size group signatures," in *Proc. Public Key Cryptogr. Conf.*, 2007, pp. 1–15.
[25] X. Liang, Z. Cao, J. Shao, and H. Lin, "Short group signature without random oracles," in *Proc. Int. Conf. Inf. Commun. Security*, Dec. 2007, pp. 69–82.

Xiaohui Liang (S'10) received the B.Sc. degree in computer science and engineering and the M.Sc. degree in computer software and theory from Shanghai Jiao Tong University, Shanghai, China, China, in 2006 and 2009, respectively. He is currently pursuing the Ph.D. degree at the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His current research interests include information and network security, mobile social networks, and applied cryptography.

Kuan Zhang received the B.Sc. degree in electrical and computer engineering and the M.Sc. degree in computer science from Northeastern University, Shenyang, China, in 2009 and 2011, respectively. He is currently pursuing the Ph.D. degree at the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His current research interests include packet forwarding, and security and privacy for mobile social networks.

Rongxing Lu (S'09–M'11) received the Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2006, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2012. He is currently a Post-Doctoral Fellow with the Broadband Communications Research Group, University of Waterloo. His current research interests include wireless network security, applied cryptography, and trusted computing.



Xiaodong Lin (S'07–M'09) received the Ph.D. degree in information engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 1998, and the Ph.D. degree (with Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008. He is currently an Assistant Professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON, Canada. His current research interests include wireless network security, applied cryptography, computer forensics, software security, and wireless networking and mobile computing. He was a recipient of the Natural Sciences and Engineering Research Council of Canada Canada Graduate Scholarships Doctoral and the Best Paper Awards of the 18th International Conference on Computer Communications and Networks in 2009, the 5th International Conference on Body Area Networks in 2010, and the IEEE International Conference on Communications in 2007.

Xuemin Shen (M'97–SM'02–F09) received the B.Sc. degree from Dalian Maritime University, Dalian, China, and the M.Sc. and Ph.D. degrees from Rutgers University, Piscataway, NJ, USA, in 1982, 1987, 1990, respectively, in all in electrical engineering. He is a Professor and University Research Chair of the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. He was the Associate Chair for Graduate Studies from 2004 to 2008. His current research interests include resource management in interconnected wireless/wired networks, wireless network security, wireless body area networks, vehicular ad hoc, and sensor networks. He is the co-author and an editor of six books, and he has published more than 600 papers and book chapters in wireless communications and networks, control, and filtering. He served as the Technical Program Committee Chair for IEEE VTC in 2010, the Symposia Chair for IEEE ICC in 2010, the Tutorial Chair for IEEE VTC in 2011 and IEEE ICC in 2008, the Technical Program Committee Chair for IEEE Globecom in 2007, the General Co-Chair for Chinacom in 2007 and QShine in 2006, the Chair for IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking. He has served as the Editor-in-Chief for *IEEE Network*, *Peer-to-Peer Networking and Application*, and *IET Communications*, a Founding Area Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, *Computer Networks*, and *ACM/Wireless Networks*, and the Guest Editor for the IEEE JSAC, the IEEE WIRELESS COMMUNICATIONS, the IEEE COMMUNICATIONS MAGAZINE, and *ACM Mobile Networks and Applications*. He received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award from the University of Waterloo in 2004, 2007, and 2010, the Premier's Research Excellence Award from the Province of Ontario, Canada, in 2003, and the Distinguished Performance Award from the Faculty of Engineering, University of Waterloo, in 2002 and 2007. He is a Registered Professional Engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, and a Distinguished Lecturer of the IEEE Vehicular Technology Society and Communications Society. He has been a Guest Professor with Tsinghua University, Shanghai Jiao Tong University, Zhejiang University, Beijing Jiao Tong University, Northeast University.