Received August 6, 2018, accepted September 12, 2018, date of publication September 20, 2018, date of current version October 17, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2871158

Cyber-Physical-Social Aware Privacy Preserving in Location-Based Service

KONGLIN ZHU[1], WENKE YAN[1], WENQI ZHAO[2], LIYANG CHEN[1], LIN ZHANG[1], AND EIJI OKI[3], (Fellow, IEEE)

[1]School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]International School, Beijing University of Posts and Telecommunications, Beijing 100876, China
[3]Graduate School of Informatics, Kyoto University, Kyoto 606-8501, Japan

Corresponding author: Konglin Zhu (klzhu@bupt.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2016YFB0100902, in part by the National Natural Science Foundation of China under Grant 61502045, and in part by the Fundamental Research Funds for the Central Universities.

ABSTRACT The privacy leakage resulting from location-based service (LBS) has become a critical issue. To preserve user privacy, many previous studies have investigated to prevent LBS servers from user privacy theft. However, they only consider whether the peers are innocent or malicious but ignore the relationship between the peers, whereas such a relationship between each pairwise of users affects the privacy leakage tremendously. For instance, a user has less concern of privacy leakage from a social friend than a stranger. In this paper, we study cyber-physical-social (CPS) aware method to address the privacy preserving in the case that not only LBS servers but also every other participant in the network has the probability to be malicious. Furthermore, by exploring the physical coupling and social ties among users, we construct CPS-aware privacy utility maximization (CPUM) game. We then study the potential Nash equilibrium of the game and show the existence of Nash equilibrium of CPUM game. Finally, we design a CPS-aware algorithm to find the Nash equilibrium for the maximization of privacy utility. Extensive evaluation results show that the proposed approach reduces privacy leakage by 50% in the case that malicious servers and users exist in the network.

INDEX TERMS CPS-aware privacy utility maximization, location-based service, privacy leakage.

I. INTRODUCTION

Location-based Service (LBS) becomes popular as the development of smartphones and mobile networks. Mobile users can share or obtain various information in different point of interests (POIs) by mobile applications. For instance, mobile users can find a place for dinner by a restaurant application. They can also share photos when visiting some places. Such querying or sharing behaviors occurred between mobile users and LBS servers usually need mobile users to submit personal information including locations and the interests to LBS servers. If these servers are not trustworthy, they can collect these personal information and use it for tracking or they may share with other third party services, thus user privacy is leaked. Location-based Service (LBS) becomes popular as the development of smartphones and mobile networks. Mobile users can share or obtain various information in different point of interests (POIs) by mobile applications. For instance, mobile users can find a place for dinner by a restaurant application. They can also share photos when visiting some places. Such querying or sharing behaviors occurred between mobile users and LBS servers usually need mobile users to submit personal information including locations and the interests to LBS servers. If these servers are not trustworthy, they can collect these personal information and use it for tracking or they may share with other third party services, thus user privacy is leaked.

Many privacy preserving schemes are studied to avoid the privacy leakage. For instance, the dummy locations and caching approaches are applied in [11]. The dummy location approach mixes the query with others and send to LBS servers to avoid the privacy leakage of the real one. To avoid the privacy leakage by LBS servers, the caching scheme reduces the number of queries to LBS servers by caching the queries and replies at nearby nodes to reduce the privacy leakage by requesting from servers. We use Fig. 1 to illustrate how dummy location and caching schemes work for privacy preserving in LBS. When user A sends a query to LBS server $X1$, it sends k-dummy locations information, including a real

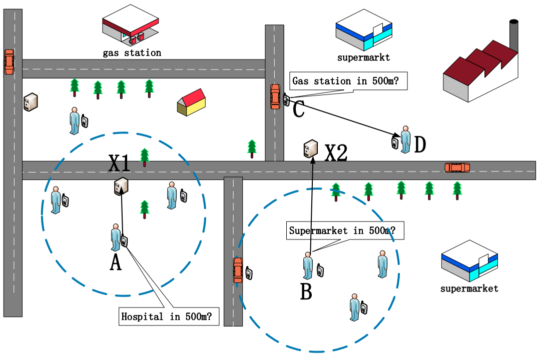


FIGURE 1. Privacy preserving in LBS and the challenges.

location and $k-1$ dummy locations, so that the LBS server cannot distinguish the real query sent by user A. The similar approach is also applied to user B when sending a query to server $X2$. With caching approach, when user C has a LBS request, instead of sending the request to server $X2$, it sends the query to other users which had such a request and reply stored locally (e.g., user D).

However, both of dummy location and caching approaches can only apply in certain conditions. Privacy preserving by dummy locations needs to coordinate with others to make sure that the query cannot be easily exposed. Privacy preserving with caching needs other nodes where the replies cached are trustworthy. In reality, these conditions are difficult to be satisfied. For instance, how users preserve their privacy in the case that not only LBS servers but also other mobile users are not trustworthy? As shown in Fig. 1, if user D is not trustworthy as well, the privacy of user C will be leaked by D.

In this work, we propose a cyber-physical-social (CPS) aware privacy preserving scheme to reduce the privacy exposing when both LBS servers and other nodes in the network are not fully trustworthy. In the case that both dummy locations and caching approaches are explored to reduce privacy exposing, we mainly target on the the questions such as who will contribute to the privacy preserving, and how they are stimulated to do so collaboratively. In particular, we compose a CPS-aware privacy utility maximization (CPUM) game to stimulate both physical neighbors and social friends to contribute to the dummy locations and caching for privacy preserving. We further prove the existence of Nash Equilibrium in CPUM game by which a minimal privacy leakage can be reached. Accordingly, we carry out a CPS-aware privacy preserving approach to collaboratively help mobile users preserve privacy for each other. The extensive evaluation results show that the CPS-aware approach invokes the motivation of mobile users to participate in the privacy preserving and the privacy leakage is reduced dramatically.

The contributions of this paper are summarized as follows:

- We formulate the CPS-aware privacy preserving problem to a CPS-aware privacy utility maximization (CPUM) problem, and exploit CPUM game to stimulate the collaboration.
- We show that the CPUM game has the Nash Equilibrium and propose a CPS-aware privacy preserving approach for the minimization of privacy leakage.
- The evaluation results show that the proposed CPS-aware privacy preserving approach reduces the privacy leakage of the CPS-aware privacy utility group by 50%.

The remainder of the paper is organized as follows. Section II reviews the related works. Section III illustrates the system model and basic formulation. In Section IV, we introduce CPS-aware privacy utility. The CPS-aware privacy utility maximization game and CPS-aware privacy preserving approach are presented in Section V. In Section VI, extensive experiments have been carried out. Finally, the paper is concluded in Section VII.

II. RELATED WORKS

A number of privacy preserving schemes have been proposed to protect privacy for LBS. Depends on whether Trusted Third Party (TTP) is employed, existing solutions can be divided into two main categories: TTP-based privacy preserving shemes and TTP free solutions. We briefly review the related studies in the following.

Firstly, we discuss a group of privacy preserving schemes based on TTP. In LBS services, the peers are scattered around the place, and the location k-anonymity model in [7] shows excellent results theoretically. However, if multiple users are in the same location or sensitive area it is easier to leak personal information. Gedik and Liu [5] developed a suite of scalable and yet efficient spatio-temporal cloaking algorithms, called CliqueCloak algorithms, to provide high quality personalized location k-anonymity, aiming at avoiding or reducing known location privacy threats before forwarding requests to LBS providers. The work showed that a TTP is required to achieve the anonymization of users actual location. To reduce the probability of the distinguishability of the cloaking technique, it also combines with other techniques, such as game theory [8] and dummy locations [12]. Xue and Ding [22] introduced a location-based privacy-preserving authentication protocol (LPA), to preserve the location privacy by combining anonymous authentication and the top-down security system together. Pinley *et al.* [15] combined the complexities of time and space, thus introducing a context-aware privacy-preserving LBS system to protect the privacy of LBS system in aspects of both data privacy and communication anonymity. Zhu *et al.* [24] proposed a privacy preserving approach in LBS, named EPQ. The EPQ scheme is characterized by employing an improved homomorphic encryption technique over a composite order group to protect users location privacy and the confidentiality of the LBS data with low overhead in computation and communications. Sun *et al.* [18] first designed the attack model by analyzing the security risks of the current dummy-location selection (DLS) algorithm. Furthermore, they proposed a novel dummy location privacy-preserving (DLP) which involves the users' computing costs as well as their various privacy needs based on the security test. Memon *et al.* [9] proposed a privacy authentication protection protocol, by which each vehicles activities can be verified in the term of privacy preserving manner. Their scheme also takes into account some practical factors such as moving trend, velocity differences, and so on, so as to reduce the cost of common users effectively.

However, even if the encryption method is closing to perfect, it still bears great risks because TTP commands too many sensitive information of users. So researchers looked for the solutions without TTP. In order to achieve privacy preserving management of location information, Ashouri-Talouki *et al.* [1] put forward an encryption method based on group location which can achieve the incognito of users' actual locations with TTP-free. Solanas and Martĺİnez-Ballestĺę [17] indicate a TTP-free protocol for location privacy in location-based services. But the answer set becomes large if the LBS needs process many locations. Therefore we can realize privacy preserving by caching, in which mobile users send query to caching nodes instead of LBS servers to avoid the identification tracking by LBS servers. Thomsen *et al.* [19] explored the role of the cache mechanism of web search in LBSs. They exploited the optimal sub-path property so as to allow the target nodes answer the request from source nodes by caching through the shortest path. Zhu *et al.* [26] proposed a novel collaborative system, MobiCache. It is worth mentioning that based on MobiCache, they proposed a Dummy Selection Algorithm (DSA) to preserve the users' privacy and to increase the cache hit ratio. Different from the traditional k-dummy location and cache, DSA chooses dummy locations which have not been queried before to increase the cache hit ratio. Paulet *et al.* [13] proposed a major enhancement upon previous solutions by introducing a two stage approach, where the first step is based on Oblivious Transfer and the second step is based on Private Information Retrieval, to achieve a secure solution for both parties. Niu *et al.* [11] combined both dummy locations and caching approach to reduce the privacy leakage risk for query. They firstly incorporated the effect of caching on privacy and proposed a caching-based solution to keep privacy from leaking. They further explored how much caching can be used to improve privacy. Zhang *et al.* [23] employed a conditional random field to model the spatio-temporal correlations among the contexts, and proposes a speed-up algorithm to learn the weaknesses in the correlations. The TTP free solutions for privacy preserving in [6], [20], and [21] exerted differential privacy preserving schemes to reduce the privacy leakage.

This work differs from the previous studies by incorporating both physical neighbors and social friends for privacy preserving. The proposed CPUM game can stimulate mobile nodes to participate for privacy preserving and meanwhile maximize the CPS-aware privacy utility to reduce the privacy leakage.

III. PRELIMINARIES

In this section, we first describe the system model of this work, and then discuss the formulation of CPS-aware privacy preserving problem.

A. BASIC MODEL

We consider the CPS-aware privacy preserving in LBS where the LBS servers are not fully trustworthy, and there are some other peers in the network also behaving maliciously. They collect user privacy information when users send query to them. They may use the collected privacy information to perform inference attacks to deduce and learn location information from users.

In order to preserve user privacy, both dummy location and caching approaches are exerted in the system as the basic privacy preserving setup. In particular, in order to avoid the privacy violation by LBS servers, each user caches queries and corresponding replies locally to meet the future query from itself or other users. In this manner, users can reduce the number of queries to LBS servers thus lessen the privacy leakage to servers. Meanwhile, when users send queries to servers or other peer users, they send k-dummy locations information, including a real location and $k-1$ dummy locations. With dummy locations, untrustworthy entities cannot tell the real identification of the querying user. In spite that both approaches are applied for privacy preserving, it is still difficult to prevent privacy leakage. For instance, if the query result is obtained from a malicious user, the user privacy will be leaked by malicious cache user. Furthermore, the real location may be inferred by malicious user or LBS servers if dummy locations are not well chosen.

Although LBS servers and other peer users are not fully trustworthy, each user has the trustiness with their physical neighbors and social friends [2], [3]. Namely, users are willing to send query to their physical neighbors and the neighbors reply the query without leaking it to malicious users, by which users in close proximity can benefit from each other. Meanwhile, users with social relationship such as friends, family members, and colleagues, etc. who are trustworthy to conduct the query and reply with less worrying the loss of privacy by them. The user combines his or her physical neighbors and social friends to compose a CPS-aware privacy preserving group, and conduct the CPS-aware privacy preserving.

B. PROBLEM FORMULATION

Based on the above-mentioned basic model, we show the basic formulation of the privacy preserving problem in LBS. Given a LBS, we assume that a LBS server $\mathcal{X}$ stores all the information with respect to the information $\mathcal{D} = \{d_1, d_2, \ldots, d_m\}$. For a set of mobile users $U = \{u_1, u_2, \ldots, u_n\}$, each mobile user u_i can store the reply obtained from LBS server, denoted D_i, obviously, $D_i \subset \mathcal{D}$. When a user u_i sends the LBS query, it selects either LBS server or other caching users who can provide the corresponding information and meanwhile maintain the minimal privacy leakage. Then the user u_i sends k-dummy locations to the information provider. In this process, the user privacy may be thieved by untrusted LBS servers or other malicious users. We use p_i to denote the query probability of the ith dummy location. We use normalized query times to represent the value of p_i. If the user i is never queried before, the value of p_i of k dummy location are considered equal to zero. Accordingly, the higher the query frequency, the higher the value of query probability. Furthermore, if all users have the same query probability, no users are distinguished. Thus, it is a good preservation of privacy. For k-dummy locations, we choose those dummy locations queried with the same probability. The more close the querying probability, the more difficult the untrusted LBS server or malicious users can infer the real location. To quantify the identification of the real location out of k-dummy locations, we define identification entropy (I-Entropy) [16] as:

$$H_i = -\sum_{j=1}^{k}(p_j \cdot logp_j), \qquad (1)$$

The larger value of H_i suggests that the uncertainty to identify the real location is larger resulting in a higher privacy degree.

IV. CPS-AWARE PRIVACY AND THE UTILITY

In this section, we discuss the CPS-aware privacy by taking physical neighbors and social friends into consideration. We show the composition of CPS-aware privacy group and the corresponding CPS-aware privacy utility.

A. CPS-AWARE PRIVACY GROUP

The CPS-aware privacy preserving requires each user to have a group of users protect privacy by exploring social and physical relationships. Such a group of users is named *CPS-aware privacy group*. Each user in the group contains physical neighbors and social friends, in which physical neighbors help each other for privacy preserving to reach a "win-win" case and social friends have the intrinsical intention to help users with social ties. Indeed, physical neighbors or social friends may involve un-intentioned privacy leakage. For instance, when a user sends a query to the server, and meanwhile a physical neighbor also sends the query to the server, such conflict may help to infer the real identification of the user and also the physical neighbor. Besides, the query of a user can also be used to infer the privacy of his or her social friends if they own similar trajectory for visiting POIs. If a user is in the social set and at the same time in the physical neighbor set, it may have the double effects to the privacy leakage. Therefore, we compose them in one group to prevent the privacy leakage jointly. We illustrate the quantification of physical neighbors and social friends as follows.

Physical neighbors are bounded by physical coupling between two users. We define the physical coupling as the time duration of their contact period over the total time period. In particular, given two users i and j, we define that they are in contact if they are in the communication range. Their kth contact duration is denoted by t_{ij}^k. Assume they have x contacts in a time period T [25]. Then the physical coupling metric is defined as $L_{ij} = \frac{\sum_{k=1}^{x} t_{ij}^k}{T}$. A larger L_{ij} suggests a closer physical coupling between i and j. Since physical coupled neighbors are more frequent with physical contact to collect information from each other, k-dummy locations are selected in the physical coupled users. In particular, dummy locations are selected in the physical coupled users with the same query frequency with user i.

Two users with social ties are considered social friends, which are quantified by strength of social ties. We measure social tie strength by four different social metrics, including the number of social interactions, common social profile, common social friends and common social interest groups. Specifically, given user i and j with social ties, the number of social interactions is quantified by the interactions between i and j over the total number of messages sent and received by both i and j. Similarly, common social profile is measured by the number of common friends over the total friends owned by i and j. Common social profile and social interest groups are also defined in the similar manner. Then the overall social tie strength between i and j is calculated by the weighted similarity of above-mentioned metrics, denoted by $S_{ij} = \sum_{k=1}^{\alpha}(w_k \cdot s_{ij}^k)$, where α is the total number of the factors that affect S_{ij}, w_k is the weight, and s_{ij}^k is the value of kth metric. A greater S_{ij} suggests a closer social relationship between node i and j.

Combining both physical neighbors and social friends, the CPS-aware privacy group of user i contains user i itself, physical neighbors G_i^p, and social friends G_i^s, represented by $G(i) = \{i, G_i^p, G_i^s\}$, where $G_i^p = \{j \in U : L_{ij} > \theta_p\}$, suggesting that the physical neighbors of i contain all users with $L_{ij} > \theta_p$; $G_i^s = \{j \in U : S_{ij} > \theta_s\}$, suggesting that the social friends of i contain all users having social ties with i and their $S_{ij} > \theta_s$. We use Fig. 2 as an example to illustrate the CPS-aware privacy group. The query frequency of each user is $\{0.3, 0.7, 0.5, 0.7, 0.8, 0.2, 0.1\}$ in the network. For user 4, its physical coupled users contains $\{4, 5, 2, 3, 6\}$, and social

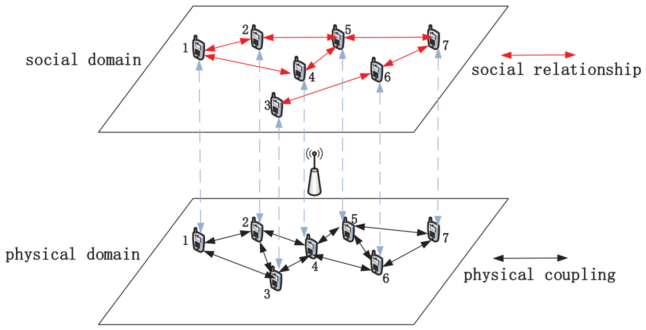


FIGURE 2. CPS-aware privacy group.

friends of user 4 are {4, 1, 5}. Therefore, The CPS-aware privacy group of mobile user 4 contains users {4, 1, 2, 3, 5, 6}.

Overall, combining physical coupling and social tie metric, we define the CPS distance between i and j in the CPS-aware privacy group as

$$d_{ij} = \frac{1}{L_{ij}} \cdot \frac{1}{S_{ij}}. \tag{2}$$

The smaller d_{ij} is, the more closely that the user i and j are bounded up with each other.

B. CPS-AWARE PRIVACY UTILITY

Users consider their CPS-aware privacy group when sending queries. On the one hand, if a user sends the k-dummy location query to LBS server, the privacy leakage is inferred from its k-dummy locations. Then the inferred privacy leakage comes from the product of I-Entropy of dummy locations, the CPS distance between the user and the dummy locations users in the case that the dummy location users also query from the LBS server. On the other hand, if a user sends the query to other users, the inferred privacy leakage is measured by the product of I-Entropy, the proportion of malicious users and the distance between the user and dummy locations. Let $X_i = \{i_s, i_1, i_2, \ldots, i_n\}$ be the selection profile to obtain the reply from of user i, where $n = |U_i|$ is the number of users in the i's CPS-aware privacy group. i_s is the indicator whether i selects the LBS server for query. The LBS server is selected if $i_s = 1$, otherwise $i_s = 0$. Similarly, i_k is the indicator of whether the kth mobile user is selected for query in the network. Let $\mathbf{a} = \{a_1, a_2, \ldots, a_n\}$ be the query strategy set of all users in the CPS-aware privacy group. Then incorporating both cases, the privacy leakage of user i is defined as:

$$P_i(\mathbf{a}) = i_s\Big(\sum_{j\in\mathbf{G}_i^p} \frac{1}{H_j} \cdot \frac{1}{d_{ij}} \cdot j_s\Big) + \sum_{k=1}^{n} i_k\Big(\sum_{j\in\mathbf{G}_i^p} \frac{1}{H_j} \cdot \beta \cdot \frac{1}{d_{ij}} \cdot j_k\Big), \tag{3}$$

where $\beta \in [0, 1]$ is the proportion of malicious users in all cache information contributors. We uniform the Eq. 3 as follows:

$$P_i(\mathbf{a}) = \Big(\sum_{j\in\mathbf{G}_i^p} \frac{1}{H_j} \cdot \gamma \cdot \frac{1}{d_{ij}} \cdot I_{\{X_i = X_j\}}\Big) \tag{4}$$

where $\gamma = 1$ if $i_s = j_s = 1$ and $\gamma = \beta$ if $i_k = j_k = 1, k \in \{1, 2, ..., n\}$. $I_{\{\cdot\}} = 1$ if the condition $\{\cdot\}$ is true, indicates both physical neighbors send query to the same place. Otherwise, $I_{\{\cdot\}} = 0$, indicates no privacy leaks if physical neighbors q uery from different places. We use the negative value of $P_i(\mathbf{a})$ as the individual utility of i. Namely, $Y_i(\mathbf{a}) = -P_i(\mathbf{a})$.

Collaboratively considering the social ties, social friends also involve the preserving of privacy measured by the strength of social ties. Therefore, the CPS-aware privacy utility is measured by

$$\psi_i(\mathbf{a}) = Y_i(\mathbf{a}) + \sum_{j\in\mathbf{G}_i^s} Y_j(\mathbf{a}) \cdot W_{ij} \tag{5}$$

where G_i^s is the social friends set of the user i and W_{ij} is the social tie strength between i and j. The CPS-aware privacy utility shows the privacy violation that can be avoided by social friends. The greater value of the CPS-aware privacy utility, the less privacy is leaked in the CPS-aware privacy group. Therefore, the objective of the CPS-aware privacy preserving is to maximize the CPS-aware privacy utility, which is *max* $\psi_i(\mathbf{a})$.

V. CPS-AWARE PRIVACY UTILITY MAXIMIZATION

In this section, we investigate the CPS-aware privacy preserving incentives and study to minimize the privacy cost for sending LBS query.

A. CPS-AWARE PRIVACY UTILITY MAXIMIZATION GAME

In the context of CPS-aware privacy preserving, each user considers the privacy of the group and tries to maximize the CPS-aware privacy group utility when sending queries. The problem falls into the CPS-aware privacy utility maximization game, which is formulated as $\mathcal{G} = (U, \{X_i\}_{i\in U}, \{\psi_i(\mathbf{a})\}_{i\in U})$, where U denotes the set of players in the game, X_i is the selection profile to obtain the reply from of i, and $\psi_i(\mathbf{a})$ is the CPS-aware privacy utility of i. In particular, each user is a player and the query strategy a_i of player i indicates the query strategy of i. The strategy combination of all players excluding i is defined as $\mathbf{a}_{-i} = \{a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n\}$. Thus, $\mathbf{a} = \{a_i, \mathbf{a}_{-i}\}$. Given the strategy set $\mathbf{a}_{-i}$, user i chooses the best query strategy so that $\psi_i(a_i^*, \mathbf{a}_{-i}) > \psi_i(a_i', \mathbf{a}_{-i})$ for all a_i', to maximize CPS-aware privacy utility. If such a_i^* is found, it is the best query strategy for i with respect to query strategy set $\mathbf{a}_{-i}$.

To find the maximal CPS-aware privacy utility, we attempt to find the Nash Equilibrium of CPUM game, where Nash Equilibrium is a kind of strategy combination that makes the strategy of each player to the best response for other players at the same time [4]. Nash Equilibrium exists when none can benefit from changing its own strategy unilaterally. Namely, a strategy combination $\mathbf{a}^* = \{a_1^*, a_2^*, \ldots, a_n^*\}$ is called Nash Equilibrium if and only if for $\forall i \in U$, it always satisfies $\psi_i(a_i^*, \mathbf{a}_{-i}) > \psi_i(a_i', \mathbf{a}_{-i})$, which conforms the goal of CPS-aware privacy utility maximization.

To find the Nash Equilibrium of CPUM game, we introduce potential game [10] in which Nash Equilibrium exists with uniqueness. A game is a potential game if and only if $\forall i \in U$ there always exists a function $\phi(\mathbf{a})$, which satisfies $\psi(a_i', \mathbf{a}_{-i}) - \psi(a_i, \mathbf{a}_{-i}) = \phi(a_i{}', \mathbf{a}_{-i}) - \phi(a_i, \mathbf{a}_{-i})$. Therefore, we show the existence of Nash Equilibrium in CPUM game by Theorem 1 as follows:

Theorem 1: The CPS-aware privacy utility maximization game $\mathcal{G} = (U, \{X_i\}_{i\in U}, \{\psi_i(\mathbf{a})\}_{i\in U})$ is a potential game.

Proof: We use the following potential function $\phi(\mathbf{a})$ to prove that the CPUM game is a potential game.

Combining Eq. 4 and Eq. 5, we define the potential function as:

$$\phi(\mathbf{a}) = \underbrace{-\frac{1}{2}\sum_{i=1}^{n}\sum_{j\in \mathbf{G_i^p}}(\frac{1}{H_j}\cdot\gamma\cdot\frac{1}{d_{ij}}\cdot I_{\{X_i=X_j\}})}_{\phi_1(\mathbf{a})}$$

$$\underbrace{-\frac{1}{2}\sum_{i=1}^{n}\sum_{j\in \mathbf{G_i^s}}W_{ij}\cdot(\frac{1}{H_j}\cdot\gamma\cdot\frac{1}{d_{ij}}\cdot I_{\{X_i=X_j\}})}_{\phi_2(\mathbf{a})} \quad (6)$$

As is shown in Eq. 6, the potential function is divided into two parts. The former part $\phi_1(\mathbf{a})$ is generated due to the physical coupling in physical domain, and the latter part $\phi_2(\mathbf{a})$ is generated due to the social relationships in social domain. We prove $\psi(\mathbf{a}')-\psi(\mathbf{a}) = \phi(\mathbf{a}')-\phi(\mathbf{a})$ by separately proving $\psi(\mathbf{a}') - \psi(\mathbf{a}) = \phi_1(\mathbf{a}') - \phi_1(\mathbf{a}) + \phi_2(\mathbf{a}') - \phi_2(\mathbf{a})$. Then we have

$$\begin{aligned}
&\phi_1(\mathbf{a}') - \phi_1(\mathbf{a}) \\
&\quad = \phi_1(\mathbf{a}_k{}', \mathbf{a}_{-k}) - \phi_1(\mathbf{a}_k, \mathbf{a}_{-k}) && (7)\\
&\quad = -\frac{1}{2}\sum_{j\in G_k^p}(\frac{1}{H_j}\cdot\gamma\cdot\frac{1}{d_{kj}}\cdot I_{\{X_k'=X_j\}}) && (8)\\
&\qquad -\frac{1}{2}\sum_{i=1,i\neq k}^{n}\sum_{j\in G_i^p}(\frac{1}{H_j}\cdot\gamma\cdot\frac{1}{d_{ij}}\cdot I_{\{X_i=X_j\}}) && (9)\\
&\qquad +\frac{1}{2}\sum_{j\in G_k^p}(\frac{1}{H_j}\cdot\gamma\cdot\frac{1}{d_{kj}}\cdot I_{\{X_k'=X_j\}}) && (10)\\
&\qquad +\frac{1}{2}\sum_{i=1,i\neq k}^{n}\sum_{j\in G_i^p}(\frac{1}{H_j}\cdot\gamma\cdot\frac{1}{d_{ij}}\cdot I_{\{X_i=X_j\}}) && (11)
\end{aligned}$$

Note that the strategy of user k is irrelevant to those users who are not in the physical neighbor set of k, which results in the subtraction eliminating all elements that is irrelevant to k. Therefore, we have

$$\begin{aligned}
&-\frac{1}{2}\sum_{i\neq k}\sum_{j\in \mathbf{G_i^p}}(\frac{1}{H_j}\cdot\gamma\cdot\frac{1}{d_{ij}}\cdot I_{\{X_i=X_j\}}) && (12)\\
&\quad +\frac{1}{2}\sum_{i\neq k}\sum_{j\in \mathbf{G_i^p}}(\frac{1}{H_j}\cdot\gamma\cdot\frac{1}{d_{ij}}\cdot I_{\{X_i=X_j\}}) && (13)\\
&= -\frac{1}{2}\sum_{i\in \mathbf{G_k^p}}(\frac{1}{H_k}\cdot\gamma\cdot\frac{1}{d_{ik}}\cdot I_{\{X_i=X_k{}'\}}) && (14)\\
&\quad +\frac{1}{2}\sum_{i\in \mathbf{G_k^p}}(\frac{1}{H_k}\cdot\gamma\cdot\frac{1}{d_{ik}}\cdot I_{\{X_i=X_k\}}) && (15)
\end{aligned}$$

It is obvious that Eq. 8 is equivalent with Eq. 14, and Eq. 10 is equivalent with Eq. 15. Therefore, $\phi_1(\mathbf{a}') - \phi_1(\mathbf{a})$ is further simplified as:

$$\begin{aligned}
&\phi_1(\mathbf{a}') - \phi_1(\mathbf{a}) \\
&\quad = -\frac{1}{2}\Big(\sum_{j\in G_k^p}(\frac{1}{H_j}\cdot\gamma\cdot\frac{1}{d_{kj}}\cdot I_{\{X_k{}'=X_j\}})\Big) * 2\\
&\qquad +\frac{1}{2}\Big(\sum_{j\in G_k^p}(\frac{1}{H_j}\cdot\gamma\cdot\frac{1}{d_{kj}}\cdot I_{\{X_k=X_j\}})\Big) * 2\\
&\quad = -\sum_{j\in G_k^p}(\frac{1}{H_j}\cdot\gamma\cdot\frac{1}{d_{kj}}\cdot I_{\{X_k{}'=X_j\}})\\
&\qquad +\sum_{j\in G_k^p}(\frac{1}{H_j}\cdot\gamma\cdot\frac{1}{d_{kj}}\cdot I_{\{X_k=X_j\}})\\
&\quad = Y_k(a_k{}', \mathbf{a}_{-k}) - Y_k(a_k, \mathbf{a}_{-k})
\end{aligned}$$

Similarly, we can also prove that

$$\begin{aligned}
&\phi_2(\mathbf{a}') - \phi_2(\mathbf{a}) \\
&\quad = \phi_2(a_k', \mathbf{a}_{-k}) - \phi_2(a_k, \mathbf{a}_{-k})\\
&\quad = \sum_{j\in G_k^s}W_{kj}\cdot(-\frac{1}{H_k}\cdot\gamma\cdot\frac{1}{d_{kj}}\cdot I_{\{X_k{}'=X_j\}})\\
&\qquad +\sum_{j\in G_k^s}W_{kj}\cdot(\frac{1}{H_k}\cdot\gamma\cdot\frac{1}{d_{kj}}\cdot I_{\{X_k=X_j\}})\\
&\quad = \sum_{j\in G_k^s}W_{kj}\cdot\Big(-\frac{1}{H_k}\cdot\gamma\cdot\frac{1}{d_{kj}}\cdot I_{\{X_k{}'=X_j\}}\\
&\qquad -\sum_{i=1,i\neq k}^{n}\sum_{i\in G_j^p}\frac{1}{H_i}\cdot\gamma\cdot\frac{1}{d_{ij}}\cdot I_{\{X_j=X_i\}}\\
&\qquad +\frac{1}{H_k}\cdot\gamma\cdot\frac{1}{d_{kj}}\cdot I_{\{X_k=X_j\}}\\
&\qquad +\sum_{i=1,i\neq k}^{n}\sum_{i\in G_j^p}\frac{1}{H_i}\cdot\gamma\cdot\frac{1}{d_{ij}}\cdot I_{\{X_j=X_i\}}\Big)\\
&\quad = \sum_{j\in G_k^s}W_{kj}\big(Y_j(a_k{}', \mathbf{a}_{-k}) - Y_j(a_k-, \mathbf{a}_{-k})\big)
\end{aligned}$$

Combining above equations, we have $\psi(\mathbf{a}') - \psi(\mathbf{a}) = \phi_1(\mathbf{a}') - \phi_1(\mathbf{a}) + \phi_2(\mathbf{a}') - \phi_2(\mathbf{a})$, thus $\psi(\mathbf{a}') - \psi(\mathbf{a}) = \phi(\mathbf{a}') - \phi(\mathbf{a})$.

Hence, the strategy game $\mathcal{G} = (U, \{X_i\}_{i\in U}, \{\psi_i(\mathbf{a})\}_{i\in U})$ is a potential game. □

Thus far, we show that the CPUM game is a potential game and it has a unique Nash Equilibrium. The CPUM problem is equivalent to find the Nash Equilibrium of CPUM game. The detail of the notations is illustrated as Table 1.

B. CPS-AWARE PRIVACY PRESERVING APPROACH

In this section, we propose a CPS-aware privacy utility maximization approach according to the property that Nash Equilibrium exists when none can benefit from changing its strategy unilaterally.

The CPUM approach is proposed in an iteratively manner. In the initial phrase, the query strategy is assigned and the

TABLE 1. Notation table.

Symbol	Definition
$\mathcal{D}$	the set of information of the server
D_i	the set of information of user i
U	a set of users
H_i	the entropy of k dummy location of user i
d_{ij}	the distance between user i and user j
W_{ij}	the social tie strength between user i and user j
G_i^p	the physical neighbors of user i
G_i^s	the social friends of user i

primary CPS-aware privacy utility is calculated. In particular, the query candidates are firstly selected by information exchanging, and the LBS server is the default query candidate. Then for each user i randomly selects one query destination from the candidates, and the query strategy is denoted as a'_i. Each user i calculates the CPS-aware privacy utility $\psi_i(a_i, \mathbf{a}_{-i})$ according to Eq. 5. In the iteration phrase, the utility is iteratively updated to reach the Nash Equilibrium. It iteratively selects an optional query candidate that has not been chosen, and marks the query strategy as a_i^x. It compares $\psi_i(a_i^x, \mathbf{a}_{-i})$ with current $\psi_i(a_i, \mathbf{a}_{-i})$. If $\psi_i(a_i^x, \mathbf{a}_{-i}) > \psi_i(a_i, \mathbf{a}_{-i})$, it replaces the current query strategy a_i to a_i^x. If none of users needs to change its strategy and no larger CPS-aware privacy utility is found, the algorithm comes to an end and the output reaches a Nash Equilibrium. The pseudo code of the CPS-aware privacy preserving algorithm which can be found in Algorithm 1. The algorithm is designed in a distributed manner and thus can apply for LBS users located in different places.

Algorithm 1 CPS-Aware Privacy Preserving Algorithm

```
Input:
The physical coupling and social relationships of all users
Output:
The Nash Equilibrium strategy combination $\mathbf{a}^* = (a_1^*, a_2^*, a_3^*, ..., a_n^*)$.
Initialization: initialize all users' choose strategies
for $i = \{1, 2, \ldots, n\}$ do
    step 1: user $i$ asks if users nearby have the information he needs. These who answer "yes" and the server are being marked as candidates.
    step 2: user $i$ selects one from the candidates randomly as his information provider, and the present choose strategy is named as $a_i$.
    step 3: Calculate $\psi_i(a_i, \mathbf{a}_{-i})$ according to (7).
end for
Iteration: to find the Nash Equilibrium
for $i = \{1, 2, \ldots, n\}$ do
    repeat
        step 1: For a candidate $x$, calculate $\psi_i(a_i^x, \mathbf{a}_{-i})$.
        step 2: If $\psi_i(a_i^x, \mathbf{a}_{-i}) > \psi_i(a_i, \mathbf{a}_{-i})$, change the present choose strategy to $a_i^x$. Namely, $a_i \leftarrow a_i^x$.
    until $\psi_i(a_i, \mathbf{a}_{-i})$ is largest for $i$
    $i \leftarrow i + 1$.
end for
```

VI. PERFORMANCE EVALUATION

In this section, we evaluate the proposed CPS-aware approach to show the effectiveness for privacy preserving in LBSs.

A. EXPERIMENT SETUP

In the experiment, we setup one LBS server in the field and 76 mobile users. The LBS server is able to offer all users with any kind of LBS information. There are 76 mobile users in the experiment, and we introduce Sigcomm2009 data trace [14] to compose the physical coupling and social ties among users. The Sigcomm2009 data trace was collected during the Sigcomm conference in 2009. The data trace contains social information of 76 users according to their Facebook social profiles. Meanwhile, it incorporates user physical coupling information by their Bluetooth contacts. Among all mobile users, randomly selected one third users serve as cache to serve specific LBS information. Different LBS information may be served by different sets of mobile users. Among all users, social strength threshold θ_s is set to 0.5. We compare the proposed CPS-aware privacy preserving approach with "non-cooperative" approach in which users are selfish and thus they do not help each other socially for LBS requests. However, they may still request for service from their physical neighbors.

In the following experiments, we set up the proportion of malicious users to 1/3. For each experiment, we run 1000 times for the convergence of the results.

B. EVALUATION RESULTS

We show the evaluation results with respect to privacy preserving in different conditions. We compare the results of CPS-aware approach (CPUM) with non-cooperative approach.

Fig. 3 shows CPUM performance on CPS-aware privacy utility and average privacy leakage as a function of the number of iterations. Fig. 3a shows the CPS-aware privacy utility as a function of the number of iterations. The results show that the utility value increases rapidly with the increasing of iterations until the number of iterations reach 100. Afterwards, the utility value increases with a much slower speed until it reaches 250 iterations, and then it keeps steady. The results suggest that the proposed CPUM approach reaches a relatively stable value after 100 iterations and it gets converged after about 250 iterations. Fig. 3b shows the average privacy leakage as a function of the number of iterations. It presents that the average privacy leakage of CPUM reaches a steady state within 100 iterations, which is in line with the convergence trend of CPS-aware privacy utility. In spite that the non-cooperative approach has the similar tendency, the non-cooperative approach suffers from more than 20% of privacy leakage compared with the CPUM approach. This is because that the CPS-aware privacy group stimulates the collaborations among users to serve for each other thus reduces

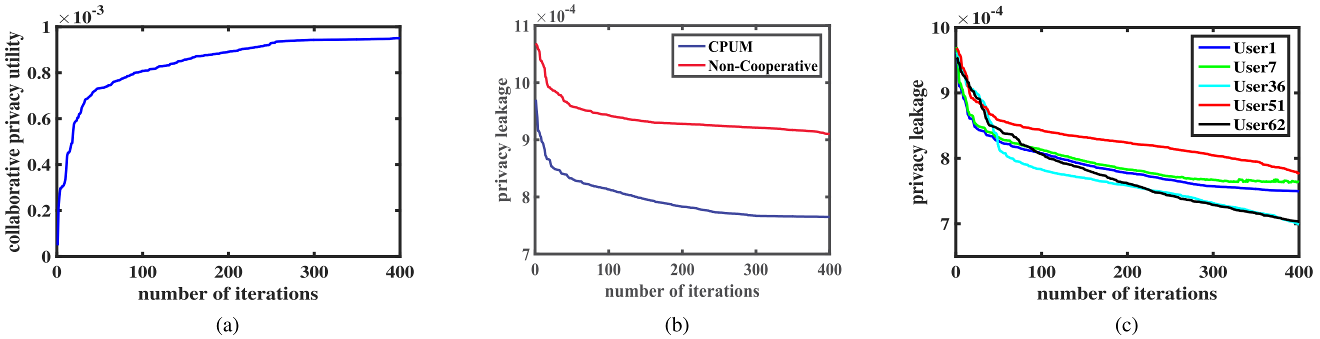


FIGURE 3. CPUM performance on CPS-aware privacy utility and privacy leakage. (a) Social group utility. (b) Average privacy leakage. (c) Random privacy leakage.

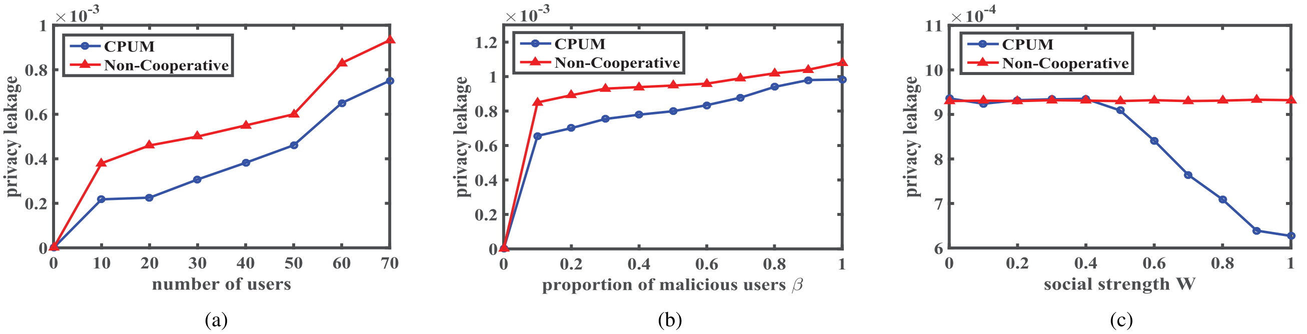


FIGURE 4. Privacy leakage under different conditions. (a) User numbers. (b) Proportion of malicious users. (c) Social strength.

the chances to request from untrustworthy LBS servers. In order to illustrate the consistence of the coverage tendency, we show the privacy leakage of five different users with respect to the number of iterations in Fig. 3c. In particular, we measure the privacy leakage of user 1, 7, 36, 51, and 62. The privacy leakage of all users decreases as the increasing of the number of iterations. Although the convergence speed of each node is different, they reach a relatively convergence when the number of iterations in a range of 100 to 200. Overall, the proposed CPUM approach converges rapidly and it achieves low privacy leakage.

Fig. 4 shows the average privacy leakage in terms of the number of users, the proportion of malicious users and the social strength. In particular, Fig. 4a shows the privacy leakage as a function of the number of users. It presents that the average privacy leakage increases as the increasing of users due to the augmentation of malicious users, which draws more difficulties to find the Nash Equilibrium. However, the Nash Equilibrium always can be found. Taking advantage of CPS-aware factors, the privacy leakage of the proposed CPUM approach has 50% less privacy leakage compared with the non-cooperative approach when the number of users is 10, and the CPUM approach still consumes 14% less privacy leakage than the non-cooperative approach. Fig. 4b shows the privacy leakage as a function of the proportion of malicious users. The privacy leakage increases as the increasing of proportion of malicious users. The proposed approach has 25% less privacy leakage than non-cooperative approach when the proportion of malicious users is 10% of the population. When the proportion of malicious users reaches 80%, the CPUM approach still has 4% less privacy leakage compared with non-cooperative approach. As the increasing of malicious users up to 50%, CPUM approach starts to convert its request from neighbors to LBS severs while non-cooperative may still request from physical neighbors. Finally, we evaluate the privacy leakage as a function of the social tie strength as shown in Fig. 4c. We manually set social strength as the experimental value in this experiment. It presents that the non-cooperative approach is not affected by the social tie strength because it takes no account of social ties. The proposed CPUM approach has the same amount of privacy leakage as the non-cooperative approach since the small value of social tie takes little effect. When the social tie strength surpasses 0.5, the privacy leakage of CPUM approach rapidly decreases up to 50% compared with non-cooperative approach. This is because the social strength threshold θ_s is set to 0.5 in the whole experiment. Overall, the proposed CPUM approach has less privacy leakage than non-cooperative approach in terms of different experimental conditions.

VII. CONCLUSIONS AND FUTURE WORK

In this work, we aimed to reduce privacy leakage in the case that both LBS servers and other participants are malicious. We formulated the privacy preserving problem as a CPUM game. Then we show the existence of Nash Equilibrium in the game by proving that CPUM game is a potential game. A CPS-aware privacy preserving approach is proposed to stimulate the privacy preserving collaboration by coupling social and physical distance, and maximize the privacy utility by reaching the Nash Equilibrium. The extensive evaluation results show that the proposed CPS-aware privacy preserving approach reduce the privacy leakage up to 50% compared with non-cooperative approaches. In the future work, besides the dummy location and cache methods, we will also explore other privacy preserving such as differential obfuscation associating with CPUM game for privacy preserving.

REFERENCES

[1] M. Ashouri-Talouki, A. Baraani-Dastjerdi, and A. A. Selçuk, "The Cloaked-Centroid protocol: Location privacy protection for a group of users of location-based services," *Knowl. Inf. Syst.*, vol. 45, no. 3, pp. 589–615, 2015.

[2] X. Chen, X. Gong, L. Yang, and J. Zhang, "A social group utility maximization framework with applications in database assisted spectrum access," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr./May 2014, pp. 1959–1967.

[3] X. Chen, X. Gong, L. Yang, and J. Zhang, "Exploiting social tie structure for cooperative wireless networking: A social group utility maximization framework," *IEEE/ACM Trans. Netw.*, vol. 24, no. 6, pp. 3593–3606, Dec. 2016.

[4] I. Esponda and D. Pouzo, "Berk–Nash equilibrium: A framework for modeling agents with misspecified models," *Econometrica*, vol. 84, no. 3, pp. 1093–1130, 2016.

[5] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in *Proc. 25th IEEE Int. Conf. Distrib. Comput. Syst.*, Jun. 2005, pp. 620–629.

[6] Y. Gong, C. Zhang, Y. Fang, and J. Sun, "Protecting location privacy for task allocation in ad hoc mobile cloud computing," *IEEE Trans. Emerg. Topics Comput.*, vol. 6, no. 1, pp. 110–121, Jan./Mar. 2018.

[7] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. Int. Conf. Mobile Syst., Appl., Services*, 2003, pp. 31–42.

[8] X. Liu, K. Liu, L. Guo, X. Li, and Y. Fang, "A game-theoretic approach for achieving k-anonymity in location based services," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2985–2993.

[9] I. Memon, Q. A. Arain, H. Memon, and F. A. Mangi, "Efficient user based authentication protocol for location based services discovery over road networks," *Wireless Pers. Commun.*, vol. 95, no. 4, pp. 3713–3732, 2017.

[10] A. Moragrega, P. Closas, and C. Ibars, "Potential game for energy-efficient RSS-based positioning in wireless sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 7, pp. 1394–1406, Jul. 2015.

[11] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Enhancing privacy through caching in location-based services," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2015, pp. 1017–1025.

[12] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Achieving k-anonymity in privacy-aware location-based services," in *Proc. IEEE Con. Comput. Commun. (INFOCOM)*, Toronto, ON, Canada, 2014, pp. 754–762.

[13] R. Paulet, M. G. Koasar, X. Yi, and E. Bertino, "Privacy-preserving and content-protecting location based queries," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 5, pp. 1200–1210, May 2014.

[14] A.-K. Pietilainen and C. Diot. (Jul. 2012). *CRAWDAD Dataset Thlab/SIGCOMM2009 (V. 2012-07-15)*. [Online]. Available: http://crawdad.org/thlab/sigcomm2009/20120715/mobiclique

[15] A. Pingley, W. Yu, N. Zhang, X. Fu, and W. Zhao, "A context-aware scheme for privacy-preserving location-based services," *Comput. Netw.*, vol. 56, no. 11, pp. 2551–2568, 2012.

[16] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Proc. Int. Conf. Privacy Enhancing Technol.*, 2003, pp. 41–53.

[17] A. Solanas and A. Martínez-Ballesté, "A TTP-free protocol for location privacy in location-based services," *Comput. Commun.*, vol. 31, no. 6, pp. 1181–1191, 2008.

[18] G. Sun *et al.*, "Efficient location privacy algorithm for Internet of Things (IoT) services and applications," *J. Netw. Comput. Appl.*, vol. 89, pp. 3–13, Jul. 2017.

[19] J. R. Thomsen, M. L. Yiu, and C. S. Jensen, "Effective caching of shortest paths for location-based services," in *Proc. ACM SIGMOD Int. Conf. Manage. Data*, 2012, pp. 313–324.

[20] L. Wang, D. Yang, X. Han, T. Wang, D. Zhang, and X. Ma, "Location privacy-preserving task allocation for mobile crowdsensing with differential geo-obfuscation," in *Proc. Int. Conf. World Wide Web*, 2017, pp. 627–636.

[21] Y. Xiao and L. Xiong, "Protecting locations with differential privacy under temporal correlations," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2015, pp. 1298–1309.

[22] X. Xue and J. Ding, "LPA: A new location-based privacy-preserving authentication protocol in VANET," *Secur. Commun. Netw.*, vol. 5, no. 1, pp. 69–78, 2012.

[23] S. Zhang *et al.*, "PLP: Protecting location privacy against correlation-analysis attack in crowdsensing," in *Proc. 44th Int. Conf. Parallel Process.*, Sep. 2015, pp. 111–119.

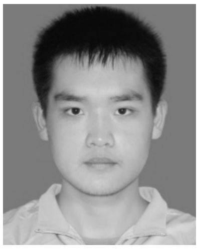
[24] H. Zhu, R. Lu, C. Huang, L. Chen, and H. Li, "An efficient privacy-preserving location-based services query scheme in outsourced cloud," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7729–7739, Sep. 2016.

[25] K. Zhu, W. Zhi, L. Zhang, X. Chen, and X. Fu, "Social-aware incentivized caching for D2D communications," *IEEE Access*, vol. 4, pp. 7585–7593, 2016.

[26] X. Zhu, H. Chi, B. Niu, W. Zhang, Z. Li, and H. Li, "MobiCache: When k-anonymity meets cache," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 820–825.

KONGLIN ZHU received the master's degree in computer science from the University of California at Los Angeles, Los Angeles, CA, USA, in 2009, and the Ph.D. degree from the University of Göttingen in 2014. He is currently an Associate Professor with the Beijing University of Posts and Telecommunications. His research interests include mobile social networking, vehicular networks, and network virtualization. He serves as TPC members for many international conferences, including GLOBECOM, ICC, and WCNC.

WENKE YAN received the bachelor's degree from the Nanjing University of Posts and Telecommunications in 2016. She is currently pursuing the master's degree with the Advanced Networking Technology Laboratory, Beijing University of Posts and Telecommunications. Her research interests include game theory, privacy, and security in vehicular networks.



WENQI ZHAO is currently pursuing the bachelor's degree with the Advanced Networking Technology Laboratory, Beijing University of Posts and Telecommunications. His research interests include privacy and security in vehicular networks.

LIYANG CHEN received the master's degree from the Beijing University of Posts and Telecommunications in 2009, where he is currently pursuing the Ph.D. degree with the Advanced Networking Technology Laboratory. His research interests include privacy and security in vehicular networks.

LIN ZHANG received the B.S. and Ph.D. degrees from the Beijing University of Posts and Telecommunications (BUPT), China, in 1996 and 2001, respectively. He was a Post-Doctoral Researcher with Information and Communications University, South Korea, from 2000 to 2002. He went to Singapore and held a Research Fellow position at Nanyang Technological University, Singapore, from 2003 to 2004. He joined BUPT in 2004 as a Lecturer, then an Associate Professor in 2005 and a Professor in 2011. He has been the Dean of the School of Information and Communication Engineering since 2014. His research interests are mobile cloud computing and Internet of Things.

EIJI OKI (M'95–SM'05–F'13) received the Ph.D. degree in electrical engineering from Keio University, Yokohama, Japan, in 1999. He is a Professor at Kyoto University, Kyoto, Japan. He has been active in the standardization of the path computation element (PCE) and GMPLS in the IETF. He has written over ten IETF RFCs. He has authored/co-authored four books, *Broadband Packet Switching Technologies* (Wiley, 2001), *GMPLS Technologies* (CRC Press, 2005), *Advanced Internet Protocols, Services, and Applications* (Wiley, 2012), and *Linear Programming and Algorithms for Communication Networks* (CRC Press, 2012). He was a recipient of several prestigious awards, including the 1998 Switching System Research Award and the 1999 Excellent Paper Award presented by IEICE, the 2001 Asia–Pacific Outstanding Young Researcher Award presented by the IEEE Communications Society for his contributions to broadband network, ATM, and optical IP technologies, the 2010 Telecom System Technology Prize by the Telecommunications Advanced Foundation, the IEEE HPSR 2012 Outstanding Paper Award, and the IEEE HPSR 2014 Best Paper Award Finalist, First Runner Up.