Research Article

GLPP: A Game-Based Location Privacy-Preserving Framework in Account Linked Mixed Location-Based Services

Zhuo Ma ^{1,2}, Jiuxin Cao ^{1,2}, Xiusheng Chen,² Shuai Xu,² Bo Liu,² and Yuntao Yang²

¹Key Laboratory of Computer Network Technology of Jiangsu Province, School of Cyber Science and Engineering, Southeast University, Nanjing, China

²School of Computer Science and Engineering, Southeast University, Nanjing, China

Correspondence should be addressed to Jiuxin Cao; jx.cao@seu.edu.cn

Received 13 January 2018; Revised 12 March 2018; Accepted 3 April 2018; Published 20 May 2018

Academic Editor: Laurence T. Yang

Copyright © 2018 Zhuo Ma et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In Location-Based Services (LBSs) platforms, such as Foursquare and Swarm, the submitted position for a share or search leads to the exposure of users' activities. Additionally, the cross-platform account linkage could aggravate this exposure, as the fusion of users' information can enhance inference attacks on users' next submitted location. Hence, in this paper, we propose GLPP, a personalized and continuous location privacy-preserving framework in account linked platforms with different LBSs (i.e., search-based LBSs and share-based LBSs). The key point of GLPP is to obfuscate every location submitted in search-based LBSs so as to defend dynamic inference attacks. Specifically, first, possible inference attacks are listed through user behavioral analysis. Second, for each specific attack, an obfuscation model is proposed to minimize location privacy leakage under a given location distortion, which ensures submitted locations' utility for search-based LBSs. Third, for dynamic attacks, a framework based on zero-sum game is adopted to joint specific obfuscation above and minimize the location privacy leakage to a balanced point. Experiments on real dataset prove the effectiveness of our proposed attacks in *Accuracy*, *Certainty*, and *Correctness* and, meanwhile, also show the performance of our preserving solution in defense of attacks and guarantee of location utility.

1. Introduction

In a platform with Location-Based Services (LBSs), a relevant position is submitted for a share or search (e.g., check-in, local search), which connects the physical world with cyber world and social world together [1]. However, users' locations are exposed to LBS providers and stored in a LBS server during this procedure. Once misused or attacked, users' habits or activities can be inferred through their historical trajectories. For example, the WeChat (<https://web.wechat.com>) user, who uses the surrounding search to explore new friends nearby, may disclose his current location [2, 3]. Another example is for Foursquare (<https://foursquare.com>) users using local search at a relatively private place (e.g., the hospital, the bank). In above cases, location privacy protection is a need, while the user experience should also be ensured in search-based LBSs.

Existing researches on location privacy protection have worked out many feasible solutions in this traditional area, including access control [4–6], data distortion [7–9], and

cryptography [10]. However, little attention has been paid to the location privacy leakage in account linked mixed LBSs, where the situation becomes more complex. The account linked mixed LBSs refer to two or more LBSs, varied in kind, whose base platforms are linked by account. According to functionality, LBSs can be divided into two groups, namely, share-based LBSs (e.g., check-in) and search-based LBSs (e.g., local/remote search), respectively. With these mixed LBSs linked, privacy protection becomes more difficult from the view of either individual platform or comprehensive platforms.

Individually, for account linked mixed LBSs, different strategies should be developed corresponding to different situations in specific LBSs. Similar to users in search-based LBSs facing the trade-off between privacy protection and user experience, users using share-based LBSs can also be caught in a dilemma when some locations are considered to be private for themselves. Traditional obfuscation is efficient for the former case but does not work in the latter case.

FIGURE 1: A location profile from Foursquare.

Since locations published in share-based LBSs are aimed at requiring a sentimental value from online friends, user status and locations submitted should not be obfuscated. As a result, users need to weigh the gains and loss by themselves to decide whether to make the location public.

Comprehensively, account linkage [11] shares user information cross platforms, which leads to a boost in location inference attacks about both the users and their friends. For an anchor user who has linked accounts cross platforms, his sequential locations in time order are connected to form a relatively complete trajectory. On the other hand, the different friend circles maintained in different platforms are integrated into a new one, which provides more abundant information for location inference attacks.

Based on challenges mentioned above, in this paper, we would like to preserve users' location privacy in account linked LBSs, which is formally defined as the "account linked LBSs caused location privacy leakage" (AL-LPL) problem. AL-LPL is a typical problem belonging to the "account linked services caused privacy leakage" (AL-PL) problem, which is very urgent under the prevalence of account linked platforms. Once a user's location leaked, the harm is greater than in single platform as more friends are exposed. The solution we have proposed in this paper could not only solve AL-LPL, but also provide a feasible method for the following work in this area. Furthermore, AL-LPL is a general problem and can be applied to a kind of account linked platforms providing LBSs, like Facebook (<https://www.facebook.com>), Yelp (<https://www.yelp.com>), WeChat, and DIAN PING (<http://www.dianping.com>). In addition, AL-LPL is a novel problem when compared with traditional privacy leakage problems. Different from traditional location privacy leakage [12, 13] in a specific kind of LBS, AL-LPL has discussed location privacy leakage caused by linking different LBSs. AL-LPL is also distinct from the work [14] discussing location privacy leakage in mixed LBSs in one platform because LBSs in AL-LPL are organized in more than one system such that network alignment is needed between two platforms.

Here, we use the Foursquare-Swarm as the research case to show the effectiveness of our proposed attacks and test the

performance of corresponding protection mechanism. For information integration, we make use of existing anchor users and adopt the location profile system of Foursquare to be the knowledge base [15]. As shown in Figure 1, every Point of Interest (POI) in this system has a unique profile with detailed information, which can tolerate light deviation of coordinates and address name, respectively. Hence, a location in any forms of coordinates or address can be unified in this system, represented by a location profile with a unique location ID.

Based on the network alignment of two platforms, a new heterogeneous social network with mixed LBSs is constructed, where specific inference attacks are formed to guess user's next submitted location. These inference attacks are supported by previous analysis of user's behavior in social network [16–19], which suggests that user's location can be predicted by both friends' trajectory and his periodic mobility pattern. Besides, to avoid the disturbance from overactive users with friends or trajectory across the world, we limit the range of inference attacks to a predefined geographical region (e.g., a city).

To defend the attacks above, we use a framework (shown in Figure 2) based on noncooperative game to help a user to obfuscate both his historical locations and his online location before the submission in search-based LBS. The basic hypothesis here is that "service providers and LBS location servers are untrustworthy." Therefore, our design does not rely on any trusted third party (TTP). Here, every location in search-based LBS is obfuscated through a unified method. The solution imitates users' random walk to a near Point of Interest (POI), takes the trade-off between obfuscation and submission's utility into consideration, and implements optimal obfuscation to fend off dynamic inference attacks. For details, an obfuscation model is established for specific fixed attack where AL-LPL is transformed into a multiobjective optimization problem to reduce attack's performance in *Accuracy* and *Correctness*. Based on every obfuscation solution against every listed inference attack, a game-based framework is adopted to defend the dynamic attacks where AL-LPL is transformed into a minimax optimization problem

FIGURE 2: The framework of location privacy protection.

to avoid the worst case for location privacy leakage under any given attacks. Our main contribution of this paper consists of the following:

- (i) To the best of our knowledge, this is the first work to give a specific protection solution for location privacy leakage caused by account linked LBSs.
- (ii) New attack models are established to infer users' next submitted location based on users' and their friends' historical trajectory and proved to have boosts in attack effectiveness through information fusion when compared with the state-of-the-arts [20, 21].
- (iii) To defend continuous and dynamic attacks formed from the above, an improved gamed-based framework is proposed to obfuscate every location in search-based LBS, which consists of the offline combination of obfuscation solutions generated by our proposed obfuscation model and the online updating according to whether a new location is produced in any LBS.
- (iv) The experiments, based on real dataset, demonstrate the effectiveness of our solutions in defending multi-source continuous attacks and prove that the location utility of our solutions is under users' control.

The rest of this paper is organized as follows. Section 2 introduces the preliminary work. Section 3 gives the corresponding solution, and empirical experiments are reported in Section 4. Section 5 discusses the related work. Section 6 draws the conclusion.

2. Preliminaries

In this section, we first introduce *background information* about Foursquare and Swarm (<https://www.swarmapp.com>),

followed by *network alignment* between these platforms, which provide a foundation for *problem formulation*.

2.1. Background Information. As representative LBS platforms, Foursquare and Swarm are adopted to be the research case to prove the effectiveness of our proposed attacks and protection. As a companion application separated from older Foursquare, Swarm allows users to share their current location with friends and develops into a Location-Based Social Network (LBSN) with the share-based LBS. Meanwhile, new Foursquare provides a local search and recommendation service and transforms into a popular mixed LBS platform (i.e., local search is a search-based LBS and recommendation service is a share-based LBS). Here, the recommendation service is provided based on tips written in Foursquare, which reflects users' preference for POI. During the separation, old Foursquare users coexist between these two new platforms, which produces sufficient cross-platform account linkage. On the other hand, once new users register in Swarm, they could choose to use their existing Foursquare account. In addition, a redirection linkage is also provided on the web page of Foursquare, which directs to the web page of Swarm. As a result, the two online platforms are closely coaligned with each other. In this typical case, the AL-LPL problem potentially exists for all these linked accounts.

2.2. Network Alignment. As the foundation of user information fusion, network alignment [22] is a reflection between the nodes of different networks, so as to combine two or more networks into a new hybrid network with global information. For platforms with LBSs, their networks are composed of two kinds of nodes (i.e., user node and location node) and two kinds of edges (i.e., user-user friendship edge, user-location

submission edge). As a consequence, the reflection should be established both between users and between locations.

As for network alignment between Foursquare and Swarm, for one thing, the sufficient account linkages provide adequate anchor users, which leads to a complete reflection between user nodes cross platforms. For another thing, Foursquare and Swarm share the same location profile system as a result of earlier separation, so they share the same reflection between a given position (e.g., coordinates, address) and location ID. Hence, the location mapping is not a problem. For platforms not sharing the unified reflection with each other, Foursquare can also be used as the mapping standard because of its well-defined location profiles, where coordinates can be clustered to the nearest POI to alleviate location drift and incomplete address can be matched with the key words.

2.3. Problem Formulation. In LBS, a user u submits a (longitude, latitude) pair to location server when he prefers a kind of services. Suppose u 's real location is r ; without location privacy protection, this information can be used by adversary for his inference attacks. For our solution, in local search service, a pseudolocation r' is selected in a specific location set, which is composed of all the historical locations produced by u and u 's friends. Here, from the specific location set, the k -nearest POIs are sorted out, each with an obfuscated probability p . Then the pseudolocation r' is chosen from these POIs according to the certain probability distribution P . Here, k is called protection level.

From adversary's point of view, when location servers are compromised, adversary obtains three parts of user u 's information: (1) u 's mixed historical trajectory $\text{tr}(u)$ from two platforms; (2) u 's friendship list $F(u)$ in Swarm; (3) any friend u_f 's mixed historical trajectory $\text{tr}(u_f)$ from two platforms. Meanwhile, adversary can guess the protection level k if u 's home address has been exposed in his profile, so we suppose k is known to adversary. As a result, adversary's background knowledge about u is $\text{KnL}(u) = \langle \text{tr}(u), F(u), \text{tr}(u_f), k \rangle$.

Armed with above knowledge $\text{KnL}(u)$, when getting u 's current pseudolocation r' , adversary would guess u 's true location according to candidates' probability distribution G . Here, all possible inference attacks ASet are established to compute G where candidates are k -nearest positions that can be obfuscated to r' .

Therefore, the AL-LPL problem can be defined as follows: given (1) u 's setting about lower bound of location utility Q after obfuscation (Q is a real number between 0 and 1, and larger Q represents better location utility); (2) u 's current location r ; (3) adversary's background knowledge $\text{KnL}(u)$ about u ; and (4) adversary's possible attacks set ASet, how to get optimal obfuscation distribution P under maximum loss of location utility Q_l ($Q_l = 1 - Q$)?

3. Solution

In this section, our proposed solution for AL-LPL is given through (1) *analyzing potential inference attacks*, (2) *establishing specific obfuscation model for corresponding attacks*,

and (3) *using the improved game-based framework to defend continuous dynamic attacks*.

3.1. Potential Attacks Analysis. Here, the analysis of potential inference attacks consists of two steps: (1) we enumerate the common-used guessing methods based on all the meaningful combination of background knowledge (2) and adopt two tracking methods, namely, distribution tracking and maximum likelihood tracking, to determine the final probability distribution of guessed results.

(1) *For the first thing, ways to compute initial candidates' probability distribution G are as follows.*

(1.1) Basic Guessing E/B. Basic Guessing refers to the guessing without any background knowledge. With user's pseudolocation r' given, the candidates' probability is represented as $g(r'' | r')$. Here, two common conditional probability distributions are adopted for their wide usage, namely, even distribution and Bayesian distribution. The guessing following these distributions are represented by **E** and **B**, and their candidates' probabilities are defined as follows:

$$\begin{aligned} G_E &= g(r'' | r') = \frac{1}{n} \\ G_B &= g(r'' | r') = \frac{p(r' | r'') p(r'')}{p(r')}, \end{aligned} \quad (1)$$

where n is the number of candidates. $p(r'')$ and $p(r')$ represent the probability of u 's appearance in location r'' and r' , respectively. Here, they are based on the statistics of u 's historical trajectory. $p(r' | r'')$ is the probability of submitting r' when r'' is the real location. Since real value of $p(r' | r'')$ is difficult for adversary to infer, obfuscation is supposed to follow an even distribution. With protection level k known, $p(r' | r'')$ equals $1/k$.

(1.2) Friendship-Based Guessing F. Friendship-Based Guessing is the guessing based on similarity between u and u 's friend u_f . According to previous research carried out by Cho et al. [23], there is a positive correlation between social relationship and human movement. A friend with higher similarity intends to visit more common places with u . Suppose the similarity score in guessing **F** is $\text{sim}(u, u_f)$; then the calculation of the candidates' probability distribution G is as follows:

$$\begin{aligned} G_F &= g(r'' | \text{KnL}(u)) = \sum_{u_f \in F_u} \text{sim}(u, u_f) \\ &\cdot \left(1 - \prod_{r'_{u_f} \in \theta(r'')} (1 - g(r'' | r'_{u_f})) \right), \end{aligned} \quad (2)$$

where $\theta(r'')$ refers to the location set of all the possible obfuscation when user locates at r'' . Here, $\text{sim}(u, u_f)$ is used as a weight, to multiply the probability that u_f has ever visited at least one position in obfuscation set $\theta(r'')$. As a result, all friends of u are taken into account to decide

every candidate's probability. Additionally, $\text{sim}(u, u_f)$ is the similarity score between u and u_f , which are calculated through two-item attribute information, namely, *common friend ratio* and *trajectory similarity*.

First, the similarity score between users' friends is calculated with measure Jaccard's coefficient [24]; that is, for u and his friend u_f ,

$$\text{sim}(F(u), F(u_f)) = \frac{|F(u) \cap F(u_f)|}{|F(u) \cup F(u_f)|}, \quad (3)$$

where $F(u)$ and $F(u_f)$ are the friend list of u and u_f , respectively.

Second, the trajectory similarity between u and his friend u_f is measured by Jaccard's coefficient where $\text{sim}(\text{tr}(u), \text{tr}(u_f))$ can be defined as follows:

$$\text{sim}(\text{tr}(u), \text{tr}(u_f)) = \frac{|\text{tr}(u) \cap \text{tr}(u_f)|}{|\text{tr}(u) \cup \text{tr}(u_f)|}, \quad (4)$$

where u and u_f are the historical locations generated by u and u_f on both Foursquare and Swarm in time order, respectively.

With $\text{sim}(F(u), F(u_f))$ and $\text{sim}(\text{tr}(u), \text{tr}(u_f))$ known, the similarity score between u and his friend u_f is defined as follows:

$$\begin{aligned} \text{sim}(u, u_f) &= \alpha \frac{\text{sim}(F(\cdot), F(\cdot))_{\max} - \text{sim}(F(u), F(u_f))}{\text{sim}(F(u), F(u_f)) - \text{sim}(F(\cdot), F(\cdot))_{\min}} \\ &+ \beta \frac{\text{sim}(\text{tr}(\cdot), \text{tr}(\cdot))_{\max} - \text{sim}(\text{tr}(u), \text{tr}(u_f))}{\text{sim}(\text{tr}(u), \text{tr}(u_f)) - \text{sim}(\text{tr}(\cdot), \text{tr}(\cdot))_{\min}}, \end{aligned} \quad (5)$$

where α and β are weight coefficients, whose optimal value can be learnt from data theoretically. However, this will make the model too complicated. To focus on the AL-LPL problem itself, in this paper, we assume α and β are equally important and assign them with the same weight (i.e., $\alpha = \beta = 0.5$) for simplicity concerns. Besides, normalization is used to calculate a relative similarity score, so as to eliminate the effect of different value ranges which is caused by different attribute information.

(1.3) Mobility-Pattern-Based Guessing M. Mobility-Pattern-Based Guessing is the guessing based on periodic mobility pattern of u . Previous studies [23] show that a user tends to visit the same place at a regular time. Here, POIs on u 's trajectory can be extracted and listed based on their proposed timestamps and are classified into seven time windows, which represent seven days of a week, from Sunday to Saturday. As a consequence, the corresponding guessing process is represented as

$$\begin{aligned} G_M &= g(r'' | \text{KnL}(u)) \\ &= 1 - \prod_{\text{tw}(r'_h) = \text{tw}(r'') \& r'_h \in \theta(r'')} (1 - g(r'' | r'_h)), \end{aligned} \quad (6)$$

where $\text{tw}(\cdot)$ is the time window of input location and r'_h denotes the submitted location in the past. Other definitions have been demonstrated in expression (2). Therefore, the candidates' probability distribution G equals the probability that u has ever paid a visit to at least one location in obfuscation set $\theta(r'')$ and meanwhile the visit belongs to the same time window of current pseudolocation r'' .

From all the possible combination of the above guessing, in this paper, we form four kinds of representative attacks: (1) Basic Attacks: attacks only adopt Basic Guessing **E/B**; (2) Friendship-Based Attacks: attacks integrate Basic Guessing **E/B** with Friendship-Based Guessing **F**; (3) Mobility-Pattern-Based Attacks: attacks integrate Basic Guessing **E/B** with Mobility-Pattern-Based Guessing **M**; (4) Comprehensive Attacks: attacks integrate Basic Guessing **E/B** with Friendship-Based Guessing **F** and Mobility-Pattern-Based Guessing **M**. Here, linear combination is used in this integration due to its simplicity and wide usage. That is,

$$\begin{aligned} G_C &= g(r'' | \text{KnL}(u), r') \\ &= \frac{\omega_1 G_B + \omega_2 G_F + \omega_3 G_M}{\sum_{r' \in \theta(r'')} g(r'' | \text{KnL}(u), r')}, \end{aligned} \quad (7)$$

where ω_i is the weight coefficient of every guessing and is learnt through experiments. G_C is candidates' probability distribution G of Comprehensive Attacks based on guessing **B**, **F**, and **M**. The denominator is used for normalization.

(2) Moreover, tracking methods are introduced as follows.

As for tracking methods, some adversary believe only locations with maximum likelihood are qualified for candidates such that they remove positions with less likelihood in inferring u 's real location. Others regard all k points around r' as candidates and select guessed location by following candidates' probability distribution G . Figure 3 provides an example for these two tracking methods.

Suppose distribution tracking is denoted by **T1** and maximum likelihood tracking is represented by **T2**; all possible attacks are listed as follows: **ET1**, **ET2**, **EFT1**, **EFT2**, **EMT1**, **EMT2**, **ECT1**, **ECT2**, **BT1**, **BT2**, **BFT1**, **BFT2**, **BMT1**, **BMT2**, **BCT1**, **BCT2**.

3.2. Obfuscation Model. As is mentioned before, our work aims to get the optimal obfuscation distribution G under maximum loss of location utility Q_l . Here, two targets are aimed at in our obfuscation according to Raza Shokri et al.'s work in [25]. In that paper, three criteria are put forward to measure the attacks' effectiveness, namely, *Accuracy*, *Certainty*, and *Correctness*. *Accuracy* is defined as the hit probability of real position r , *Certainty* shows the entropy of candidates' probability distribution G , and *Correctness* is the distance expectation between guessed location r'' and true location r . As is analyzed in [25], *Certainty* is less important than the other two factors in determining whether an attack is effective. Hence, *Accuracy* and *Correctness* are selected as optimum targets in our protection solutions.

As the opposite of adversary, our protection solutions need to decrease the hit probability EA and increase r'' and r 's

FIGURE 3: An example of distribution tracking and maximum likelihood tracking.

distance expectation ED as much as possible. The definitions of EA and ED are as follows:

$$EA = \sum_{r'} f(r' | r) g(r'' = r | \text{KnL}(u), r') \quad (8)$$

$$ED = \sum_{r'', r'} f(r' | r) g(r'' | \text{KnL}(u), r') d(r, r''), \quad (9)$$

where $f(r' | r)$ is the obfuscation probability of r' given that r is the real location. $g(r'' = r | \text{KnL}(u), r')$ is the hit probability based on knowledge $\text{KnL}(u)$ when r' is pseudolocation. In addition, $g(r'' | \text{KnL}(u), r')$ is candidates' probability based on knowledge $\text{KnL}(u)$ when r' is pseudolocation, and $d(r, r'')$ is the distance between real position and guessed result. Here, all the possible r' with corresponding guessed results are accumulated for ED, and the Euclidean distance is used to calculate $d(r, r'')$.

Besides, the loss of location utility Q_v with the limit of maximum value at Q_l is defined as follows:

$$Q_v = \sum_{r'} f(r' | r) d(r, r'). \quad (10)$$

Based on restrictions mentioned above, including EA, ED, and Q_l , we have proposed our obfuscation model corresponding to the situation where the attack is identified.

Measured by hit probability EA and the distance expectation ED, the score of our obfuscation model can be represented as

$$\text{score}(P) = \varphi_1 \times (-ED) + \varphi_2 \times EA, \quad (11)$$

where φ_1 and φ_2 are the weight of ED and EA, respectively. $\varphi_1, \varphi_2 \geq 0$ and $\varphi_1 + \varphi_2 = 1$. Here, we assume that EA is the most important index and set $\varphi_1 = 0.1$ and $\varphi_2 = 0.9$, respectively. Definitely, it is convenient for users to modify these factors when they expect higher performance in ED and do not so much care about the performance in EA.

Consequently, the optimal obfuscation distribution $P^* = f^*(r' | r)$ that can minimize the score function will be

$$\begin{aligned} P^* \arg \min_P \quad & \text{score}(P) \\ & = \arg \min_P (\varphi_1 \times (-ED) + \varphi_2 \times EA), \\ \text{s.t.} \quad & Q_v \leq Q_l, \\ & \sum_{r'} f(r' | r) = 1, \quad f(r' | r) \geq 0. \end{aligned} \quad (12)$$

To solve the objective function, (1) the set L_s of k -nearest locations is initialized for every POI. (2) Next, three targets including EA, ED, and Q_l are initialized according to (8), (9), and (10), respectively. (3) After that, simplex algorithm [26] is used with the input of objective function and the constraints. Here, the time complexity of this algorithm is $O(n \log(k))$ where n is the number of POIs in dataset and k is the protection level.

As a consequence, 16 protection solutions are formed according to specific attacks proposed before. They are **ET1P**, **ET2P**, **EFT1P**, **EFT2P**, **EMT1P**, **EMT2P**, **ECT1P**, **ECT2P**, **BT1P**, **BT2P**, **BFT1P**, **BFT2P**, **BMT1P**, **BMT2P**, **BCT1P**, and **BCT2P**.

3.3. Improved Game-Based Framework. Based on every obfuscation solution against every listed inference attack, a game-based framework is adopted to defend the continuous and dynamic attacks. The improved game-based framework is to obfuscate every location in search-based LBS, which consists of the *offline model* combining obfuscation solutions generated by our proposed obfuscation model and the *online updating* according to whether a new location is produced in any LBS.

(1) *Offline Model.* For dynamic inference attacks, a mapping is established from attack-and-defense process to a noncooperative game, corresponding to the main elements of game,

namely, players, the strategy, and the profit. In our work, (1) players refer to adversary and users. (2) The adversary's strategy space AStra is a subset of possible inference attacks set ASet, containing relatively efficient attacks selected from ASet, while users' strategy space PStra is composed of corresponding protections to defend attacks in AStra. (3) For users, the profit E_p is measured by how efficiently their locations in local search are protected, and corresponding target functions have already been analyzed in formula (11). For adversary, the obtained profit EA can be regarded as the profit loss of users, so the sum of these two profits is zero. Therefore, profits of both sides are defined as below:

$$E_p = \varphi_1 \times (-ED) + \varphi_2 \times EA \quad (13)$$

$$E_A = -(\varphi_1 \times (-ED) + \varphi_2 \times EA), \quad (14)$$

where we assume that EA is the most important index and set $\varphi_1 = 0.1$ and $\varphi_2 = 0.9$, respectively. Definitely, it is convenient for users to modify these factors when they expect higher performance in ED and do not so much care about the performance in EA.

To defend dynamic attacks, specific obfuscation solution is mixed based on our proposed obfuscation model through the minimax theorem [27] as

$$f_{\text{mix}}(r' | r) = \sum_{i=1}^n \sigma_i \times \text{PStra}_i, \quad (15)$$

where PStra_i is every obfuscation solution based on the obfuscation model, which belongs to PStra. σ_i is its weight which is learnt through experiments. After several rounds, an equilibrium will be achieved, from which we can obtain hybrid protection solution as is described below.

To produce a proper pseudolocation r' as user's submission, (1) the set L_s of k -nearest locations is initialized for every POI. (2) After that, the set of protection strategy PStra is established corresponding to adversary's strategy space AStra. (3) Then, every entry of users' profit matrix is calculated through formula (13). (4) Furthermore, the zero-sum game is transformed into a dual linear programming problem, and the simplex optimization method is used to get the final obfuscation probability $f^*(r' | r)$. (5) At last, selection is done following the probability of $f^*(r' | r)$ to produce a pseudolocation r' . For time complexity, this algorithm needs $O(an \cdot \log(k))$, where n is the number of POIs in dataset, k is the protection level, a is the size of attack space AStra ($a \ll n$), and b is the size of protection space PStra ($b \ll n$).

From the above, it is uncertain whether the loss of location utility Q_v is still lower than u 's setting in this game-based protection. Derivation below is the analysis of this issue, which proves that the Q_l constraint is still satisfied; that is,

$$\begin{aligned} Q_v &= \sum_{r'} f_{\text{mix}}(r' | r) d(r, r') \\ &= \sum_{r'} \left(\sum_{i=1}^n \sigma_i \times \text{PStra}_i \right) d(r, r') \end{aligned}$$

$$\begin{aligned} &= \sigma_1 \sum_{r'} \text{PStra}_1 \times d(r, r') + \dots \\ &\quad + \sigma_n \sum_{r'} \text{PStra}_n \times d(r, r') \leq \sigma_1 Q_l + \dots + \sigma_n Q_l \\ &\leq Q_l, \quad \left(\sum_{i=1}^n \sigma_i = 1 \right). \end{aligned} \quad (16)$$

(2) *Online Updating Strategy.* Every time a location is submitted for share-based LBSs in two platforms, the online updating is carried out for our game-based solution where the optimal obfuscation distribution P is recalculated. On the other hand, if a location is proposed for local search, our protection would work out its fuzzy location following P and begin updating afterwards. Additionally, every updating refers to a recalculation of P , so as to support consecutive protection.

4. Experiments

In this section, *dataset, compared methods, evaluation metrics*, and experiment setup are introduced, followed by our *experiment result* and some *corresponding analysis*.

4.1. Dataset Description. In our experiments, we use trajectory produced by New York users in Foursquare and Swarm. A user is considered New York-based if he specifies New York in the location field of his profile.

Here, we adopt the method mentioned in [28] to crawl users' check-ins in Swarm and get users' tips in Foursquare through Foursquare API. Unfortunately, users' submitted locations in local search are unavailable through public data collection, so we use the location list drawn from tips in Foursquare to simulate the locations in local search due to their tight coupling in temporary-space. Here, we make two assumptions: (1) For a common user, his tips are always published after local searching to share his experience. (2) Not every user would share tips after using local search service. As a result, the tips used for simulation in our experiment provide relatively sparse data compared with practical local search. Though locations are comparatively sparse in local search, considering the attack-and-defense process based on the same dataset, the utility of dataset cannot be determined. Therefore, additional experiments in Section 4.5.3 would further discuss this problem and find the influence of location sparsity on effectiveness testing in attack-and-defense process.

Here, data are preprocessed in both Foursquare and Swarm. We filter users through their HomeCity (a tag that can be found in user profile and it is included in our initial dataset; HomeCity indicates the user's living city), eliminate inactive users with less than 5 positions, and get the initial research dataset D . As a result, in D , users are all New York citizens, and their proposed locations are limited in New York, in which tips were produced from 2008-10-14T22:53:35Z to 2017-10-18T09:24:30Z and check-ins

FIGURE 4: The check-ins/tips distributions on users and locations, respectively.

TABLE 1: Detailed information of initial dataset D .

Dataset	Foursquare (New York)
#User node	11776
#Location node	117658
#Tips edge	182342
Dataset	Swarm (New York)
#User node	11776
#Location node	395215
#Friendship edge	223610
#Check-in edge	1830368

were produced from 2009-04-13T06:23:53Z to 2017-10-27T20:19:39Z. As shown in Table 1, in dataset D , we can find that every user has nearly 19 friends and has made

about 15 tips and 155 check-ins in average. Furthermore, the mean check-ins that happened on every location is over 46 while the mean tips produced on every location is about 2. Besides, the distribution of initial dataset is analyzed, including count of users with varied numbers of check-ins/tips in corresponding LBSs and count of locations with different numbers of check-ins/tips in corresponding LBSs. As is shown in Figure 4, all submitted locations distributions both follow the power-law distribution and have scale-free properties, which accords with the basic characteristics of LBSN. Therefore, our research dataset is representative and general.

4.2. Compared Methods. To show the improving effectiveness of multisource attacks, we compare our proposed inference attacks with two other attacks, namely, Maximum Movement Boundary (MMB) [20] and Context-aware Location Attack (CLA) [21].

(1) **MMB** is an attack introduced in [20] based on user's maximum movement boundaries. In this attack, user's real location can be inferred from the overlapping area of two continuous movement boundaries. In our experiment, the user's maximum movement speed is set to 6 km/h according to empirical human walking speed.

(2) **CLA** is an attack based on association of locations in the context and is proposed in [21]. For u 's any two pseudolocations r'_i and r'_{i+1} , the corresponding reference attack targeting at AL-LPL problem can be represented as

$$h(r'' | K(u), r'_i, r'_{i+1}) = \frac{\sum_{p_i \in \theta(r'_i), p_{i+1} \in \theta(r'_{i+1})} P_{\text{CLA}}(r'' | p_i, p_{i+1})}{|\theta(r'_i)| \times |\theta(r'_{i+1})|}, \quad (17)$$

where $P_{\text{CLA}}(r'' | p_i, p_{i+1})$ can be calculated by sixth formula proposed in [21] and $\theta(\cdot)$ contains all the possible obfuscation when user locates at the input position.

To show the performance of our proposed Improved game-based protection **I-GAMEP**, two kinds of protection are adopted here to make a comparison, namely, **I-INIP** and **I-BASICP**, respectively.

Here, **I-INIP** is the continuous obfuscation solution which follows even distribution. Its offline solution is represented by **INIP**. **I-BASICP** and **I-GAMEP** are both established based on initial protection **I-INIP**. **I-BASICP** refers to the corresponding obfuscation protections combined with our proposed updating strategy in defense of specific attacks. For comparison, **I-GAMEP** is the continuous protection solutions in defense of the combination of five representative inference attacks (i.e., **ET1**, **ECT1**, **ECT2**, **BCT1**, and **BCT2**).

4.3. Evaluation Metrics. Here, *Accuracy*, *Certainty*, and *Correctness* proposed in [25] are used to verify the effectiveness of our attack models at one point. Furthermore, their mean values $\overline{\text{ACC}}$, $\overline{\text{CER}}$, and $\overline{\text{COR}}$ are proposed to measure the performance of our proposed continuous protection and are defined as follows:

$$\begin{aligned} \overline{\text{ACC}} &= \frac{1}{N} \sum_N P(r | \text{KnL}(u), r') \\ \overline{\text{CER}} &= \frac{1}{N} \sum_N \sum_{r''} P(r'' | \text{KnL}(u), r') \log \frac{1}{P(r'' | \text{KnL}(u))} \\ \overline{\text{COR}} &= \frac{1}{N} \sum_N \sum_{r''} P(r'' | \text{KnL}(u), r') d(r, r''), \end{aligned} \quad (18)$$

where N is the frequency of attack and defense in the testing set. $\text{KnL}(u)$ is u 's background knowledge. r is u 's real position, r' is pseudolocation, and r'' is guessed location. $d(\cdot)$ is measured by Euclidean distance.

When it comes to the location utility, on the one hand, from theoretical aspect, we adopt two representative protections as examples to show the tendency of privacy leakage under different value of location utility loss, which aim to

verify that the location utility loss has an upper limit for the minimized privacy leakage. On the other hand, from practical aspect, we use the Precision@N to measure the *Accuracy* of the location list returned by local search service when submitting pseudolocation. Here, the list returned by local search before the obfuscation is set to be the benchmark. The list, as a result of Foursquare local search, contains nearby requested locations from the closest to furthest within limited distance range. Hence, the Precision@N is used to reflect the physical distance between pseudo- and true location in a direct way.

4.4. Experiment Setup. All of our experiments were conducted on a machine running Windows 7 with an Intel⁵ Core™ i5 processor and 8 GB of RAM. Our solutions have been implemented in C++.

In our experiments, (1) to test the effectiveness of attacks, the initial protection **INIP** following even distribution is carried out to locations in local search. (2) For performance analysis of protection solution, 400 users are selected to train the weight coefficient ω_i of the hybrid attacks, and the optimized combination of weights is selected through these cases. (3) To evaluate the performance of our protection methods, the same method is adopted while the training set of randomly selected 400 users is used to find the optimized weight σ_i combination of users' strategy space PStr. (4) Then, other 100 users are randomly selected to compose the testing set to evaluate the performance of baseline and our proposed protection methods.

For parameters introduced in this paper, we set the protection level $k \in \{3, 5, 7, 9, 11, 13, 15\}$ and the loss of location utility $Q_l \in \{0.05, 0.06, \dots, 0.18, 0.19\}$. If there is no specific explanation, the default values are assigned where $k = 7$ and $Q_l = 0.08$.

4.5. Experiment Results. The experiment results of addressing the AL-LPL problem are available in Tables 2-3 and Figures 5-7. In this part, we test the effectiveness of our proposed inference attacks, prove the priority of our game-based protection through comparison, and measure the loss of location utility.

4.5.1. Attacks' Effectiveness Analysis. To test the performance of our proposed 7 representative attack methods, **INIP** is carried out on local search part of dataset D . Here, we fix $Q_l = 0.08$ and vary the protection level k from 3 to 15 in a step of 2. From the results shown in Table 2, we can observe the following: (1) In most cases, **BCT2** performs the best among all the compared methods in inferring user future location evaluated by *Accuracy* and *Certainty*. If not the best, its performance is also near the best. This demonstrates that the joint of multisource information can deeply aggravate the leakage of location privacy. By comparison, for *Correctness*, the performance seems to have no obvious regularity. (2) In most cases, **EMT1** can achieve better performance in *Accuracy* and *Correctness* than **EFT1**, while **EFT1** performs better in *Certainty*, which suggests that both close friends' trajectory and users' historical trajectory

FIGURE 5: Performance comparison of different representative attacks ($k = 7$ and $Q_l = 0.08$).

FIGURE 6: Relation between location utility and privacy leakage under ECTIP and GAMEP ($k = 7$).

FIGURE 7: Local search results comparison of our proposed protection ($k = 7$ and $Q_l = 0.08$).

can reveal more location privacy in different aspects and also proves the supplemental role of linked platforms in location disclosure. (3) By comparing ECT2/BCT2 with ECT1/BCT1 correspondingly, we observe that tracking method T2 is more effective than T1 in most cases when measured by *Accuracy*, *Certainty*, and *Correctness*. (4) With the increase of protection level, most attacks' *Accuracy* falls down steadily while most

of their *Certainty* and *Correctness* show a rise trend instead, which agrees with the correlation analysis in [25].

Extra experiments are performed to compare the effectiveness of different attacks, which are controlled by variables $k = 7$ and $Q_l = 0.08$. In Figure 5, comparison is made between our proposed inference attacks (i.e., ECT1, BCT1), MMB, and CLA with the same tracking method T1. Here, (1) it is shown that BCT1 performs best in all the cases, which reflects the general optimization of our proposed attacks towards location inference in most linked platforms. (2) Furthermore, the attack effectiveness of MMB is undesirable because of the locations' sparsity in online social networks. The reason why CLA has a bad performance is that CLA only considers the correlation between locations but neglects friendship and user behavioral periodicity. As a result, attacks considering these factors perform better.

4.5.2. Protection Effectiveness Analysis. In this experiment, k and Q_l are both set to the default value. Here, Table 3 provides the performance comparison between different protection methods. I-BCT1P and I-BCT2P are chosen as the typical I-BASICP. We observe that (1) our proposed protection methods both perform better than baseline protection I-INIP in defensive *Accuracy* and *Correctness* while I-INIP has a better performance in *Certainty*. (2) When compared with the typical I-BASICP, I-GAMEP shows its general defense of varied changed attacks such that the I-GAMEP can always avoid the worst case in defense of varied attacks. Hence, the I-GAMEP is proved to have priority in semantic level to avoid adversary's accurate guessing in POI level.

4.5.3. Location Utility Analysis. Here, from the view of our model, to verify that the location utility loss has a limit for the minimized privacy leakage, the relation between location utility and privacy leakage is analyzed for each attack and defense through experiment where the value of k is fixed as before. Here, we use the latest attack and defense to be the example and measure the privacy leakage by E_p through formula (13). As is shown in Figure 6, we specify BASICP to be ECT1P and compare it with GAMEP. To find out the relation between location utility and privacy leakage towards ECT1 attack under these two protections, respectively, we compute every privacy leakage under different Q_l (from 0.05 to 0.19 step by 0.01) and describe the tendency by connecting every discreet point. Corresponding conclusions

TABLE 2: Performance comparison of our proposed representative attacks ($Q_l = 0.08$).

Measure	Attacks	k						
		3	5	7	9	11	13	15
Accuracy	ET1	0.3287	0.2050	0.1555	0.1078	0.0930	0.0778	0.0703
	EFT1	0.3288	0.1995	0.1495	0.1217	0.0871	0.0808	0.0738
	EMT1	0.3598	0.2443	0.1733	0.1402	0.1029	0.0886	0.0680
	ECT1	0.3557	0.2337	0.1761	0.1419	0.1082	0.0874	0.0762
	BCT1	0.3565	0.2506	0.1836	0.1418	0.1412	0.0875	0.0764
	ECT2	0.3575	0.2452	0.1690	0.1420	0.0986	0.0905	0.0752
	BCT2	0.3797	0.2894	0.2166	0.1420	0.1380	0.0905	0.0752
Certainty	ET1	1.1996	1.6409	1.9480	2.272	2.4347	2.6300	2.7343
	EFT1	1.1287	1.4657	1.6292	1.8960	2.0019	2.1145	2.1022
	EMT1	1.0803	1.4689	1.8034	1.9976	2.1998	2.3529	2.3943
	ECT1	1.0904	1.4794	1.7212	1.9720	2.1334	2.3768	2.4118
	BCT1	1.0669	1.4116	1.6392	1.9732	1.8159	2.3845	2.4193
	ECT2	1.0163	1.3310	1.4886	1.6808	1.798	1.9438	1.8737
	BCT2	0.8621	1.1053	1.1562	1.6808	1.3726	1.9438	1.8737
Correctness	ET1	1.9921	2.8420	3.1874	3.5907	3.7248	4.5631	5.6136
	EFT1	2.0154	2.8323	3.9738	4.0259	4.2842	4.6688	5.7081
	EMT1	1.8052	2.9663	2.7542	3.7408	4.3406	4.1665	4.1655
	ECT1	1.8280	2.9747	3.5454	4.1643	4.5196	4.1452	4.3230
	BCT1	1.8539	2.9241	3.5403	4.1643	4.4722	4.1448	4.3230
	ECT2	1.8285	2.9563	3.5406	4.1764	4.4138	5.1953	4.2702
	BCT2	1.8119	2.4967	3.1009	4.1764	4.1689	5.1953	4.2702

TABLE 3: Comparison of protection under different continuous attacks ($k = 7$ and $Q_l = 0.08$).

Measure	Protections	Attack methods							
		ECT1	BCT1	BCT2	ET1	BT1	BT2	MMB	CLA
$\overline{ACC}$	I-INIP	0.1589	0.1666	0.1930	0.1438	0.1792	0.1795	0.1443	0.1442
	I-BCTIP	0.1581	0.1659	0.1926	0.1434	0.1791	0.1793	--	--
	I-BCT2P	0.1583	0.1660	0.1924	0.1435	0.1789	0.1792	--	--
	I-GAMEP	0.1570	0.1649	0.1915	0.1434	0.1788	0.1790	--	--
$\overline{CER}$	I-INIP	1.7925	1.6959	1.1541	1.9364	1.5387	1.4240	1.9891	1.7934
	I-BCTIP	1.7916	1.6942	1.1513	2.0120	1.4657	1.4237	--	--
	I-BCT2P	1.7886	1.6916	1.1489	2.0109	1.4643	1.4223	--	--
	I-GAMEP	1.7906	1.6931	1.1503	2.0115	1.4638	1.4218	--	--
$\overline{COR}$	I-INIP	3.9488	3.8434	3.5323	3.9236	3.4416	3.4447	4.5573	2.7132
	I-BCTIP	3.9507	3.8453	3.5341	3.9393	3.4427	3.4458	--	--
	I-BCT2P	3.9549	3.8477	3.5365	3.9421	3.4451	3.4482	--	--
	I-GAMEP	4.0049	3.9054	3.6255	4.0186	3.5297	3.5341	--	--

are as follows: (1) It is easy to find that the leaked privacy decreases with the increase of Q_l and converges to a stable value. Here, the stable value is supposed to be the limit of the location utility loss Q_l when privacy leakage maintains minimum. This is because the protection methods cannot select a pseudolocation which has an infinite distance from real position. According to our mechanism, the selected candidates are limited by the locations of user's and his friends' daily visit. (2) Besides, for the same Q_l , privacy leaked by **ECTIP** is always smaller than using **GAMEP**. We suggest that this is because **GAMEP** has involved the defense of other

localization attacks so that its performance is more inferior than **ECTIP** in defense of **ECT1** attack.

Moreover, when it comes to the specific analysis of local search results, we make the comparison between different protection solutions, which contains the **BCT2P** as a typical **BASICP** and the **GAMEP**. Here, we use the latest attack and defense to be the example. Since each local search in Foursquare will return 30 locations at first, we use 30 to be the upper bound in our precision computing. On the other hand, one topic is selected, namely, "Shop & Service", in order to provide real-world scenarios in our verification.

The topic “Shop & Service” is a relatively wide range, which includes ATM, bank, and market. With k and Q_l at the default value, based on three criteria, the results shown in Figure 7 suggest the following: (1) Both **BASICP** and the **GAMEP** could support local search service since the searching results have some overlapping parts when compared with the results produced by user’s real position. (2) Additionally, the precision of **GAMEP** seems better than the results from **BASICP** in most cases.

5. Related Work

Previous studies on location privacy protection have mainly paid their attention to the leakage problems that occurred in search-based LBS through mobile phone data [29], whose solutions are all provided from the view of LBS providers, system design, and users.

From the stand of LBS providers, the earliest work is a protocol named Geopriv [30] proposed by The Internet Engineering Task Force (IETF), which is aimed at making specifications about location presentation and transformation. After that, a growing number of works are carried out about access control [4–6]; however, most provisions need to be observed conscientiously. With no legal restraint and no benefit for LBS providers, corresponding protocols are difficult to be effective.

Moreover, solutions trying to promote system design are most based on data distortion [8, 9, 31–33] and cryptography [10]. For data distortion, methods like cloaking [8, 31], suppression [9], and perturbation [32, 33] are proposed. Here, cloaking [8, 31] requires the submission of a larger region to avoid privacy leakage while suppression [9] is aimed at breaking the periodic mobility pattern through the removal of location data. In addition, differential privacy [32, 33], as a typical perturbation-based method, adds noise to the aggregate data to prevent information disclosure between continuous query. Besides, Imran Memon et al. propose an asymmetric cryptograph based anonymous communication for LBS in [10]. Despite having performed well, most of works mentioned above draw support from a TTP or the location anonymizer, which is not easy to establish and maintain for a developed LBS platform, such as Foursquare and Yelp.

For user-centric solutions, Raza Shokri et al. use the Stackelberg Bayesian game to formalize the mutual optimization of user-adversary objectives in LBS in [7], which is easier to be put into effect. As a result, the game-based protection framework we used in this paper draws on the experience of Raza Shokri et al.’s work, combined with an update strategy to defend dynamic continuous inference attacks. Other user-centric solutions more or less have their drawbacks, such as Shokri et al.’s another work in [34]. It hides most of the user’s queries through collaboration with other peers: context information has been kept in a buffer and passed to someone who is seeking it. Although it does not rely on the TTP, the QoS is also not measured in this situation.

Combined with the above methods, there are two common frameworks. One is Mix-Zone proposed in [35] and improved in [36, 37] to provide a space for a set of users entering, changing pseudonyms, and exiting. The key point of this

framework is to establish a mapping between users’ old and new pseudonyms, but this exchange does not apply to social networks. Another famous example is k -anonymity [38, 39], which needs a trusted third party to collect information of the $k - 1$ nearest users for obfuscation. Having realized this problem, many researchers proposed extensions to avoid this problem including Raza Shokri et al. in [7].

With the prevalence of smartphones and the development of LBS platforms, attention has been turned to the location privacy protection in search-based LBS platforms and shared-based LBS platforms, where new challenges are faced due to different application scenarios and varied data sparsity. For location privacy protection in search-based LBS platforms, some new possible attacks [2, 40] are focused on and solved. Other works [41, 42] are devoted to traditional location privacy leakage problem, such as that of Cheng and Aritsugi in [41], who have designed a system with obfuscated region maps generated in mobile devices to provide a user-centric protection. And our work is similar to them in storing user related locations in their mobile phone. As for share-based LBS platforms, new attacks are proposed including untrusted friends’ inference attacks [43, 44] and destination inference attacks [45].

Above all, existing researches have not paid much attention to location privacy leakage in account linked LBSs, not to mention corresponding protection solutions. As a new problem full of challenges, it has been solved in this paper with a continuous game-based preserving framework.

6. Conclusions

In this paper, we focus on a new circumstance where the information linked by accounts is fused by the adversary to make a more accurate inference attacks about user’s next proposed location. Our analysis shows a remarkable influence of multisource data on location privacy disclosure. To defend the continuous multisource attacks, we propose an improved game-based location privacy-preserving framework GLPP to obfuscate every location in local search before submission. Here, the obfuscation model is used to provide specific obfuscation solutions according to varied inference attacks while the user experience is ensured under user’s control. During the attack-and-defense process, the online updating strategy in GLPP provides a dynamic obfuscation distribution, which, as a result, supports consecutive protection. Experimental results show that our proposed GLPP performs better than initial protection in *Accuracy*, *Certainty*, and *Correctness*. Meanwhile, GLPP is also proved in our experiments to provide a good user experience without much loss in location utility.

Additional Points

Highlights. In this paper, Location-Based Services (LBS) are divided into two kinds of services: (1) The **search-based LBSs** provide search service for users, which would still work with submission obfuscated under a limited distortion. (2) The **share-based LBSs** refer to check-in services and other check-in based LBSs, which cannot work with obfuscated submission due to their functionality.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work is supported by National Natural Science Foundation of China under Grants no. 61772133, no. 61472081, no. 61402104, no. 61370207, no. 61370208, no. 61300024, no. 61320106007, no. 61272531, no. 61202449, and no. 61272054; Collaborative Innovation Center of Wireless Communications Technology; Collaborative Innovation Center of Social Safety Science and Technology; Jiangsu Provincial Key Laboratory of Network and Information Security under Grant no. BM2003201; and Key Laboratory of Computer Network and Information Integration of Ministry of Education of China under Grant no. 93K-9.

References

- [1] C. R. Vicente, D. Freni, C. Bettini et al., "Location-Related Privacy in Geo-Social Networks," *IEEE Internet Computing*, vol. 15, no. 3, pp. 20–27, 2011.
- [2] J. Peng, Y. Meng, M. Xue, X. Hei, and K. W. Ross, "Attacks and defenses in location-based social networks: a heuristic number theory approach," in *Proceedings of the International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec)*, pp. 64–71, IEEE, Hangzhou, China, 2015.
- [3] M. Xue, Y. Liu, and K. W. Ross, "I know where you are: Thwarting privacy protection in location-based social discovery services," *Security Communication Networks*, pp. 179–184, 2015.
- [4] M. E. Kabir and H. Wang, "Conditional purpose based access control model for privacy protection," in *Proceedings of the Conditional Purpose Based Access Control Model for Privacy Protection. Twentieth Australasian Conference on Australasian Database. Australian Computer Society*, pp. 135–142, Australian Computer Society, 2009.
- [5] X. Sun, H. Wang, Y. Zhang, and J. Zhang, "Privacy-aware access control with trust management in web service," *World Wide Web-internet & Web Information Systems*, vol. 14, no. 4, pp. 407–430, 2011.
- [6] H. Wang, L. Sun, and E. Bertino, "Building access control policy model for privacy preserving and testing policy conflicting problems," *Journal of Computer and System Sciences*, vol. 80, no. 8, pp. 1493–1503, 2014.
- [7] R. Shokri, G. Theodorakopoulos, C. Troncoso et al., "Protecting location privacy: optimal strategy against localization attacks," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, pp. 617–627, ACM, New York, NY, USA, 2012.
- [8] L. Kuang, Y. Wang, P. Ma, L. Yu, C. Li, L. Huang et al., "An improved privacy-preserving framework for location-based services based on double cloaking regions with supplementary information constraints," *Security and Communication Networks*, vol. 2017, Article ID 7495974, 15 pages, 2017.
- [9] X. Chen, X. Wu, X. Y. Li, Y. He, and Y. Liu, "Privacy-preserving high-quality map generation with participatory sensing," in *Proceedings of the IEEE INFOCOM*, vol. 15, pp. 2310–2318, IEEE, Toronto, Canada, 2014.
- [10] I. Memon, I. Hussain, R. Akhtar, and G. Chen, "Enhanced privacy and authentication: an efficient and secure anonymous communication for location based service using asymmetric cryptography scheme," *Wireless Personal Communications*, vol. 84, no. 2, pp. 1487–1508, 2015.
- [11] Y. Chen, C.-F. Zhuang, Q. Cao, and P. Hui, "Understanding cross-site linking in online social networks," in *Proceedings of the 8th Workshop on Social Network Mining and Analysis (SNAKDD)*, pp. 1–9, ACM, New York, NY, USA, 2014.
- [12] H. Zheng and X.-F. Meng, "A survey of trajectory privacy-preserving techniques," *Chinese Journal of Computers*, vol. 34, no. 10, pp. 1820–1830, 2011.
- [13] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches," *Personal and Ubiquitous Computing*, vol. 18, no. 1, pp. 163–175, 2014.
- [14] D.-Q. Yang, D.-Q. Zhang, B.-Q. Qu, and C. Philippe, "PrivCheck: privacy-preserving check-in data publishing for personalized location based services," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*, pp. 545–556, ACM, New York, NY, USA, 2016.
- [15] Z. Ji, A. Sun, G. Cong, and J. Han, "Joint recognition and linking of fine-grained locations from tweets," in *Proceedings of the 25th International Conference on World Wide Web (WWW)*, pp. 1271–1281, 2016.
- [16] E. Cho, S. A. Myers, and J. Leskovec, "Friendship and mobility: user movement in location-based social networks," in *Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 1082–1090, ACM, San Diego, Calif, USA, 2011.
- [17] Q. Li, Y. Zheng, X. Xie, Y. Chen, W. Liu, and W. Y. Ma, "Mining user similarity based on location history," in *Proceedings of the 16th ACM Sigspatial International Conference on Advances in Geographic Information Systems*, p. 34, ACM, New York, NY, USA, 2008.
- [18] M. Ye, P. Yin, W. C. Lee, and D. L. Lee, "Exploiting geographical influence for collaborative point-of-interest recommendation," in *Proceedings of the 34th International ACM SIGIR Conference on Research and Development in Information Retrieval*, pp. 325–334, ACM, New York, NY, USA, 2011.
- [19] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Achieving k-anonymity in privacy-aware location-based services," in *Proceedings of IEEE INFOCOM*, pp. 754–762, Toronto, Canada, 2014.
- [20] G. Ghinita, M. L. Damiani, C. Silvestri, and E. Bertino, "Preventing velocity-based linkage attacks in location-aware applications," in *Proceedings of the 17th ACM Sigspatial International Conference on Advances in Geographic Information Systems*, pp. 246–255, ACM, New York, NY, USA, 2009, <https://doi.org/10.1145/1653771.1653807>.
- [21] H. Zhang, Z. Xu, Z. Zhou, J. Shi, and X. Du, "CLPP: Context-aware location privacy protection for location-based social network," in *Proceedings of the IEEE International Conference on Communications*, pp. 1164–1169, 2015.
- [22] J. Zhang and P. S. Yu, "PCT: Partial Co-Alignment of Social Networks," in *Proceedings of the 25th International Conference on World Wide Web*, pp. 749–759, ACM, Montreal, Canada, 2016.
- [23] E. Cho, S. A. Myers, and J. Leskovec, "Friendship and mobility: user movement in location-based social networks," in *Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 1082–1090, ACM, New York, NY, USA, 2011.

- [24] D. Liben-Nowell and J. Kleinberg, "The link prediction problem for social networks," in *Proceedings of the 12th International Conference on Information and Knowledge Management*, vol. 58, pp. 556–559, ACM, New York, NY, USA, 2003.
- [25] R. Shokri, G. Theodorakopoulos, J. Y. L. Boudec, and J. P. Hubaux, "Quantifying location privacy," in *Proceedings of the IEEE Symposium on Security & Privacy*, vol. 42, pp. 247–262, 2011.
- [26] G. B. Dantzig, *Programming in a linear structure. Report of the September meeting in Madison*, vol. 17, pp. 73–74, 1948.
- [27] J. V. Neumann, "Zur Theorie der Gesellschaftsspiele," *Mathematische Annalen*, vol. 100, no. 1, pp. 295–320, 1928.
- [28] T. Zhou, J. Cao, B. Liu, S. Xu, Z. Zhu, and J. Luo, "Location-based influence maximization in social networks," in *Proceedings of the 24th ACM International Conference on Information and Knowledge Management*, pp. 1211–1220, New York, NY, USA, 2015.
- [29] J. K. Laurila, D. Gatica-Perez, I. Aad et al., "From big smart-phone data to worldwide research: the Mobile Data Challenge," *Pervasive and Mobile Computing*, vol. 9, no. 6, pp. 752–771, 2013.
- [30] J. R. Cuellar, J. B. Morris, D. K. Mulligan, J. Peterson, and J. Polk, "Geopriv reqs," *IETF Internet Draft*, 2003.
- [31] B. Niu, Q. Li, X. Zhu, and H. Li, "A fine-grained spatial cloaking scheme for privacy-aware users in Location-Based Services," in *Proceedings of the International Conference on Computer Communication and Networks*, pp. 1–8, IEEE, 2014.
- [32] E. ElSalamouny and S. Gambs, "Differential privacy models for location-based services," *Transactions on Data Privacy*, vol. 9, no. 1, pp. 15–48, 2016.
- [33] L. Yu, L. Liu, and C. Pu, "Dynamic Differential Location Privacy with Personalized Error Bounds," in *Proceedings of the Network and Distributed System Security Symposium*, 2017.
- [34] R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi, and J.-P. Hubaux, "Hiding in the mobile crowd: Location privacy through collaboration," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 3, pp. 266–279, 2014.
- [35] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46–55, 2003.
- [36] A. R. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-aware Services," in *Proceedings of the Second IEEE Conference on Pervasive Computing and Communications Workshops*, pp. 127–131, IEEE, Florida, FL, USA, 2004.
- [37] B. Niu, Z. Zhang, X. Li, and H. Li, "Privacy-area aware dummy generation algorithms for Location-Based Services," in *Proceedings of the IEEE International Conference on Communications*, pp. 957–962, Sydney, Australia, 2014.
- [38] X. Sun, H. Wang, J. Li, and Y. Zhang, "Satisfying privacy requirements before data anonymization," *The Computer Journal*, vol. 55, no. 4, pp. 422–437, 2012.
- [39] B. Gedik and L. Liu, "Location Privacy in Mobile Systems: A Personalized Anonymization Model," in *Proceedings of 25th IEEE International Conference on Distributed Computing Systems (ICDCS)*, pp. 620–629, IEEE, Columbus, OH, USA, 2005.
- [40] G. Theodorakopoulos, "The Same-Origin Attack against Location Privacy," in *Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society*, pp. 49–53, ACM, New York, NY, USA, 2015, <http://dx.doi.org/10.1145/2808138.2808150>.
- [41] W. C. Cheng and M. Aritsugi, "A User Proprietary Obfuscate System for Positions Sharing in Location-Aware Social Networks," *Journal of Computer & Communications*, vol. 3, no. 5, pp. 7–20, 2015.
- [42] X. Gong, X. Chen, K. Xing, D.-H. Shin, M. Zhang, and J. Zhang, "From social group utility maximization to personalized location privacy in mobile networks," *IEEE/ACM Transactions on Networking*, vol. 25, no. 3, pp. 1703–1716, 2017.
- [43] Y. Wu, H. Peng, X. Zhang, and H. Chen, "Publish me and protect me: Personalized and flexible location privacy protection in mobile social networks," in *Proceedings of the 23rd International Symposium on Quality of Service*, pp. 147–152, IEEE, Portland, OR, USA, 2015.
- [44] W. C. Cheng and M. Aritsugi, "A User Sensitive Privacy-preserving Location Sharing System in Mobile Social Network," *Procedia Computer Science*, vol. 35, pp. 1692–1701, 2014.
- [45] D. Xue, L.-F. Wu, H.-B. Li, Z. Hong, and Z.-J. Zhou, "A novel destination prediction attack and corresponding location privacy protection method in geo-social networks," *International Journal of Distributed Sensor Networks*, vol. 13, no. 1, 2017.