WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. 2015; **15**:155–169
Published online 6 December 2012 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/wcm.2324

RESEARCH ARTICLE

LTPPM: a location and trajectory privacy protection mechanism in participatory sensing[†]

Sheng Gao[1*], Jianfeng Ma[1], Weisong Shi[2,3] and Guoxing Zhan[3]

[1] School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi 710071, China
[2] Tongji University, Shanghai, China
[3] Department of Computer Science, Wayne State University, Detroit, MI 48202, U.S.A.

ABSTRACT

The ubiquity of mobile devices has facilitated the prevalence of participatory sensing, whereby ordinary citizens use their private mobile devices to collect regional information and to share with participators. However, such applications may endanger the users' privacy by revealing their locations and trajectories information. Most of existing solutions, which hide a user's location information with a coarse region, are under k-anonymity model. Yet, they may not be applicable in some participatory sensing applications that require precise location information. The goals are seemingly contradictory: to protect a user's location privacy while simultaneously providing precise location information for a high quality of service. In this paper, we propose a method to meet both goals. Through selecting a certain number of a user's partners, it can protect the user's location privacy while providing precise location information. The user's trajectory privacy can be protected by constructing several trajectories that are similar to the user's trajectory in an interval time T. Finally, we utilize a new metric, called *slope ratio*, to evaluate the partners' selection algorithm that we proposed. Then, we measure the privacy level that the location and trajectory privacy protection mechanism (LTPPM) can achieve. The analysis and simulation results show that LTPPM can protect the user's location and trajectory privacy effectively and also provide a high quality of service in participatory sensing. Copyright © 2012 John Wiley & Sons, Ltd.

KEYWORDS
participatory sensing; location privacy; trajectory privacy; similarity; privacy metric

***Correspondence**
Sheng Gao, School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi 710071, China.
E-mail: sgao@mail.xidian.edu.cn

1. INTRODUCTION

The past 10 years have witnessed an increase of three to four billion of mobile users [1]. Wireless communication techniques have penetrated very fast, such as wireless local area network, Third-generation Long-term Evolution, WiMax, Bluetooth, and Zigbee. With the rapid development of mobile devices, the area of participatory sensing [2] or urban sensing [3] has attracted many concerns from different areas such as location-based service [4], public health, and traffic. Participatory sensing [2] is the process whereby individuals and communities use evermore-capable mobile phones and cloud services to collect and analyze systematic data for use in discovery. Examples of existing systems include *CarTel* [5], *BikeNet* [6], *DietSense* [7], *PEIR* [8], and so on.

However, privacy problems are the main obstacles to the success of participatory sensing. Once users are aware of possible consequences with the reveal of their sensitive information, they are reluctant to participate the campaign and use the services. Christin *et al*. [9] analyzed the privacy threats and countermeasures in detail. They primarily addressed on location privacy in comparison with the other sensing modalities. When a user asks for a certain application, he or she uploads the request data to servers that are invariably tagged with the location (obtained from the embedded GPS in the phone, WiFi positioning, or using cell tower localization) and time when the readings are recorded. The mobile sensor data may reveal the user's location at a particular time that is related to the user's identity information, so this may invade the user's privacy information seriously. For example, recently, two users have sued Google [10] over location data that Android phones collect citing as one of the concerns 'serious risk of privacy invasions, including stalking'. The lawsuit attempts to prevent Google from

[†] A preliminary version of this paper has been published in Proceedings of MobiCASE 2011(poster). This is the full version.

selling phones with software that can track user location. However, just a week before, Apple [11] was trapped in privacy laws for keeping a log of user locations without offering users a way to disable this tracking or delete the log. Pseudonyms [12] and anonymizing [13,14] techniques have been used to preserve a user's location privacy. Nevertheless, if an adversary has prior knowledge of a user's movement patterns, it is fairly trivial to deanonymize the reports.

We consider that a user's motion patterns may also reveal his or her privacy. A study by Riley [15] shows wider trajectory privacy fears: a number of drivers in the Bay Area are not willing to use *FasTrak* (the electronic toll collection system in California) because the movement of FaskTrak users are tracked. The reveal of drivers' trajectories might threaten their privacy. Moreover, *background knowledge attack* [16] refers to the situation wherein an adversary eliminates unlikely candidates and learns information about his or her victim by using some prior knowledge about the individual such as *identity linkable* or *attribute linkable* surveyed in [17]. Adversary might use these aforementioned background knowledge to deduce the user's real trajectory. The reveal of the user's trajectory might threaten the user's privacy. Machanavajjhala *et al*. [18] proposed *l-diversity* to prevent such attack. In this paper, we consider increasing the number of possible trajectories from the adversaries' perspective to further enhance the privacy of individuals.

In this paper, we aim to protect a user's location and trajectory privacy in participatory sensing applications that require precise location information. We use the user's partners to construct an anonymous set, called an equivalence class. In order to get high quality of service, he or she and his or her partners should provide application server (AS) with precise locations information. The AS queries the results through these precise locations information and returns the result set to the equivalence class. The user can get a high quality of service by his or her precise location information without revealing his or her privacy information. To protect the user's trajectory privacy, we construct the mapping relationship between the two equivalence classes. The partners' trajectories should be similar to the user's trajectory so that it cannot be distinguished by an adversary easily.

In summary, this paper makes the following contributions:

- We propose a method to protect a user's location privacy in participatory sensing applications that require precise location.
- We propose an algorithm for selecting the user's partners. Considering the user's motion patterns, in an interval time T, when the user moves to another position, he or she selects some partners that have not been selected to form another equivalence class. Through constructing the mapping relationship between the two equivalence classes, we can protect the user's trajectory privacy.
- We utilize a new metric *slope ratio (SR)* to evaluate the partners' selection algorithm that we proposed and implement the simulation system with practical data.
- We present the privacy metric to evaluate the privacy level that location and trajectory privacy protection mechanism (LTPPM) can achieve. Then, we analyze the effectiveness and efficiency of the method in protecting a user's privacy in participatory sensing.

The rest of this paper is organized as follows. Section 2 presents the related work. Section 3 introduces the system architecture and state the privacy problems. Section 4 describes LTPPM in participatory sensing. Section 5 gives location and trajectory privacy protection framework and privacy metric. Then, we analyze the effectiveness and efficiency of LTPPM against threat model. In Section 6, we discuss the results and analyze LTPPM. Finally, we conclude this paper in Section 7.

2. RELATED WORK

User privacy protection in participatory sensing is similar to safeguard respondents' privacy in database, which contains continuous-valued fields. Shokri *et al*. [19] surveyed the existing location privacy protection mechanisms and proposed a unified framework for location privacy. Much of the work is under k-anonymity model. For example, Gruteser and Gruwald [13] presented spatial and temporal cloaking, which originated from k-anonymity, to guarantee user anonymity. Liu *et al*. [20,21] proposed a flexible privacy personalization framework to support location k-anonymity for a wide range of mobile clients with context-sensitive privacy requirements. k-anonymity is originally proposed by Sweeney [22,23] in the database community to protect sensitive information from being disclosed [24–26]. It provides a form of plausible deniability by ensuring that the user cannot be individually identified from a group of k users. This can be achieved by sending a sufficiently large '*k-anonymous region*' that encloses k users in space, instead of reporting a single GPS coordinate. Intuitively, creating a region around multiple users significantly decreases spatial accuracy. However, the k-anonymity technique provides coarse-grained location information, which may not be effective in some participatory sensing applications.

2.1. Coarse-grained locations privacy protection

Obfuscation methods [13,27] were used to achieve coarse-gained location privacy. Mokbel *et al*. [28] presented a new framework *Casper* in which mobile and stationary users can entertain location-based services without revealing their location information. They deal with cloaked spatial regions rather than the exact location information. Tang *et al*. [29] presented asymmetric group key agreement (ASGKA) protocol to build a safe group and design a cycle-like structure to make group members have safe status. Ghinita *et al*. [30] proposed a distributed system PRIVÉ, which organized mobile users into a hierarchical overlay network and supported decentralized query anonymization using the Hilbert-based k-anonymizing spatial region (HilbASR) algorithm in location-based services. However, they do not consider the user's mobility. Beresford and Stajano [31,32] proposed the mix zone concept in which a trusted proxy removes all samples before it passes location samples to the AS. The degree of privacy offered by the mix zone was evaluated for pedestrian traffic under the assumption that an adversary uses empirical linking. However, the static mix zone concept cannot guarantee location privacy in the case that users' behavioral models have small variance and in applications with low user density. The concept of tessellation was first introduced in AnonySense [33,34] to protect user's privacy when reporting context information. Tessellation partitions a geographical area into a number of tiles large enough to preserve the users' privacy, and each user's location is generalized to a plane in space which covers at least k potential users. However, it protects the location privacy at the cost of quality of service. Thus, it is not appropriate for some participatory sensing applications that require precise location information.

2.2. Fine-grained locations privacy protection

Huang *et al*. [16] proposed a simple modification to tessellation based on micro-aggregation. They presented an application, PetrolWatch, which allows users to automatically collect, contribute, and share petrol price information by using camera phones. However, in their method, service providers are assumed to be trustworthy, which may not be always true in reality, and it also contradicted with the original intention of tessellation. If a service provider is trustworthy, it can provide adequate protection on users' privacy. In this case, no extra protection is needed. In this paper, we assume the service providers to be untrustworthy. Kido *et al*. [35] proposed a way to anonymize a user's location information. The personal user of a location-based service generates several false position data (dummies) sent to the service provider with the true position data of the user. However, the motions of dummies may be different from that of the user. It may reveal the user's privacy information. In this paper, we improve this method by selecting the dummies whose trajectories are closed to the user's trajectory. Dong *et al*. [36] proposed a method to preserve location privacy by anonymizing coarse-grained location and retaining fine-grained locations using attribute-based encryption.

2.3. Trajectory privacy protection

Trajectory privacy-preserving is a new research area that has been concerned in recent years. Terrovitis *et al*. [37] used suppression technology to protect sensitive location samples in a trajectory database but may cause serious information loss if suppressed with too much location samples. Nergiz *et al*. [38] proposed a randomization-based reconstruction algorithm for releasing anonymized trajectory data to solve the information loss problem and improve the utility of the published data. Abul *et al*. [39] proposed exploiting space translation technology to solve (k, δ)-anonymity problem for moving objects databases. It anonymizes trajectories in a same time span under uncertainty δ. You *et al*. [40] proposed two schemes, namely, *random pattern scheme* and *rotation pattern scheme*, to generate dummies that exhibit long-term user movement patterns. The random scheme randomly generates dummies with consistent movement pattern, whereas the rotation pattern explores the idea of creating intersection among moving trajectories. However, in their random pattern scheme, without taking into account factors such as distance deviation, they simply include more dummies when the privacy requirements are not satisfied. In this paper, we based on the distance algorithm to select the user's partners whose trajectories will be more closely to that of the user. It can protect the user's trajectory privacy while reducing those trajectories useless more efficient. More recently, Huo *et al*. [41] constructed the relationship graph among history trajectories and formed the k-anonymity set based on greedy method. They also proposed a method called *You Can Walk Alone*, which extracts stay points efficiently on people's trajectories [42], to improve Never Walk Alone (NWA) [39] by anonymizing the stay points. They generate k-anonymity zone based on two algorithms called *grid-based approach* and *clustering-based approach*.

3. SYSTEM ARCHITECTURE

In this section, we introduce the basic structure of participatory sensing and state the privacy problems in this system.

3.1. Overview of participatory sensing

The very basic architecture of a participatory sensing system, demonstrated by Figure 1, consists of a collection of mobile nodes (MNs), access points, report server (RS), and AS.

(1) Mobile nodes

The private MNs that constitute the mobile sensing infrastructure are devices with sensing, computation, memory, and wireless communication capabilities. They are capable of being programmed for manual, automatic, and context-aware to complete with image, audio, video, motion, proximity, and location data capture and broadband communication. These MNs are mostly carried by humans or attached to other moving objects such as vehicles.

(2) Report server

The RS functions as aggregator and classifier. It can aggregate and classify the reports that are collected by

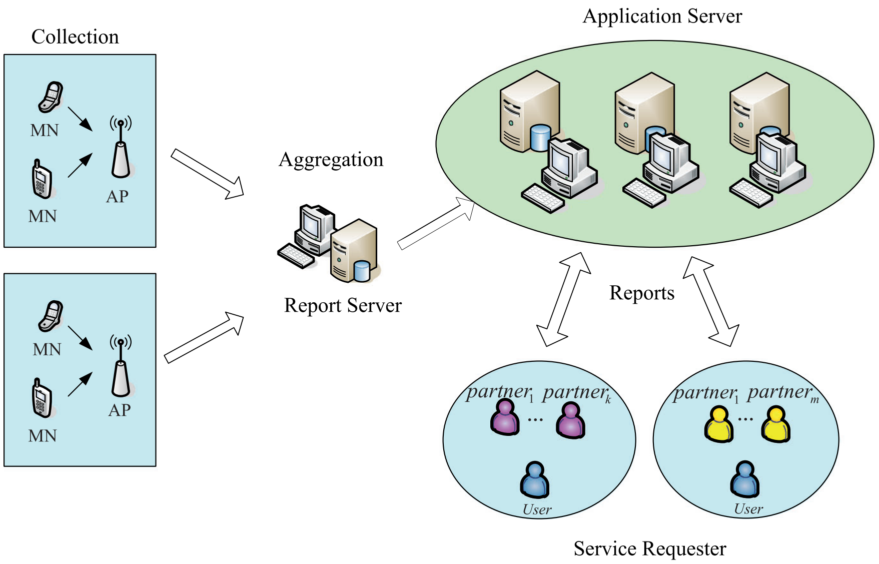


Figure 1. The basic structure of participatory sensing.

MNs according to some traits, such as category and location, and then uploads them to the AS.

(3) Application server

The AS is a server that receives reports from RS and shares the available services for users. The AS is tasked to provide the services (such as the nearest restaurant location) with the users' demands.

3.2. Problem statement

The reveal of a user's location or trajectory information would invade the user's privacy information. For example, location and trajectory information may reveal individuals personal information, such as living habits, health conditions, social customs, and work and home addresses. Once a user's locations are identified, the adversary would infer the user's trajectory information according to the exposed locations. Similarly, the reveal of a user's trajectory would also result in the disclosure of the user's locations. There is a mutual influence and mutual restraint between location and trajectory protection. The purpose of them is to protect the user's privacy from being invaded. Therefore, we will discuss the content of the user's LTPPM, respectively.

4. THE PROPOSED SCHEME

In this section, we analyze how the LTPPM functions in the contradictory between location privacy and high quality of service and trajectory privacy protection.

4.1. Location privacy with high quality of service

In this section, we present a method to solve the contradictory between the location privacy and high quality of service. Given that no trust server is available, meanwhile, wireless networks are only responsible for communication and will not reveal a user's location privacy. A user who wants to obtain a high quality of service (e.g., he or she wants to know the precise location of the nearest restaurant) should send his or her precise location information with his or her mobile device. However, the user's privacy information may be invaded by the reveal of the precise location information. In [13], they proposed a mechanism called spatial and temporal cloaking to conceal a user. To achieve a certain privacy level, the spatial or temporal accuracy of location information is reduced. Then, the accuracy of service will also be reduced. In this paper, to request a high quality of service, we propose a method in which the user's precise location information (single GPS coordinate) is sent to AS while ensuring that the user privacy will not be invaded.

A user forms an equivalence class by selecting a certain number of partners. Considering the user's mobility, in order to protect his or her trajectory privacy, the process of partners selection will be discussed in Section 4.2. To illustrate conveniently, we assume there are six partners in the equivalence class, which is shown by Figure 2. We argue that the partners will not reveal the user's location information to AS. The user sends relevant information including his or her identity signature and requirement to his or her partners. They verify the user's legality and obtain each coordinate through GPS, which is listed as follows: $(L_1, L_2, \ldots, L_6)$, where $L_i = (x_i, y_i), i = 1, 2, \ldots, 6$.

Step 1. Service Request

In order to obtain a high quality of service and protect privacy information at the same time, the user and his or her partners in the same equivalence class send their locations and service requests without

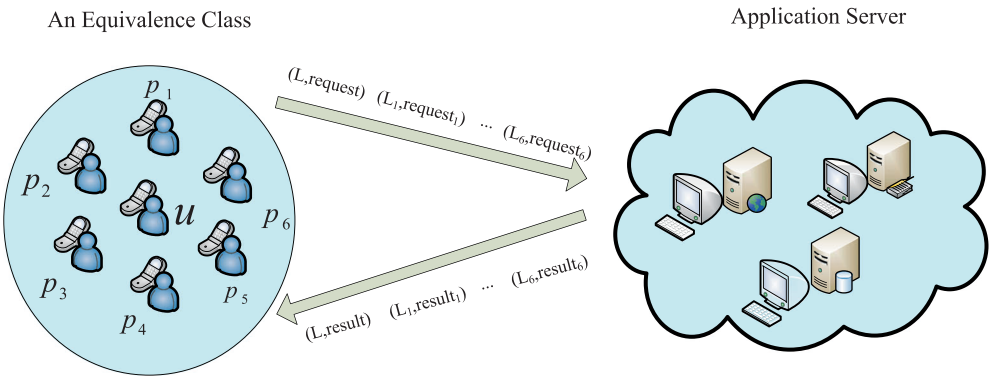


Figure 2. The process of service.

any identity information to AS. For example, they query the nearest restaurant location to each of their current locations, which are described as $(L, Request), (L_1, Request_1), \ldots, (L_6, Request_6)$.

Step 2. Service Query

In participatory sensing applications, the AS exploits the information shared by the mobile sensing devices to provide services. As a result of the precise locations information, the AS can get the query result reports, which are described as $(L, Result), (L_1, Result_1), \ldots, (L_6, Result_6)$, where $Result_i$ refers to the contents of the service related to L_i, and then return them to the equivalence class.

Step 3. Service Distribution

All the members in the equivalence class receive the result reports. The others cannot obtain the nearest restaurant location to the real user, and only the user can pick out the result he or she desires with his or her precise location information.

As showed by Figure 2, there are seven participators in the equivalence class. Even the adversary obtains all the location coordinates, the probability that he or she can identify the real user is one seventh. When the number of participators in the equivalence class is huge, the possibility that he can distinguish is very low. It will be analyzed in Section 5 in detail.

4.2. Partners selection

Each participant is equipped with two wireless network interface cards. One is dedicated to the communication with the AS through a base station or wireless modem. The other one is dedicated to the peer-to-peer communication among the peers through a wireless local area network (e.g., Bluetooth or IEEE 802.11). Also, each participant is equipped with a positioning device (e.g., GPS), which can determine its current location [43].

In order to produce trajectories those are similar to that of the user. In this paper, we adopt distance-based method to select partners. The server might be untrustworthy. Thus, all the partners in the same equivalence class will not expose the user's relevant information to the AS. The partners ensure the legality of the source message by verifying the user's signature. Algorithm 1 depicts the process of partners selection. The inputs of the algorithm are interval time T, geographic information Map, and a user's location, and the output is an equivalence class formed by the user's partners. The specific selection process is described as follows:

(1) The user maintains a table including partners' identities and locations information. In an interval time T, the user computes the distances between him or her and the surrounding partners.
(2) The user sends his or her signature and the request information to the surrounding partners. Then, they ensure the request information that is derived from the user by verifying the user's signature.
(3) Select k partners who are close to the user. If a participator has been selected by the user, it cannot be selected again in the interval time T.
(4) Construct the mapping relationship on the basis of the corresponding distance, we can obtain several trajectories that are similar to that of the user. The process will be displayed in Section 4.3.

4.3. Trajectory privacy protection

In this section, we focus on the user's trajectory privacy protection. The user's privacy would be invaded with the reveal of his or her trajectory. In order to solve the problem, Kido *et al.* [35] presented two algorithms named moving in a neighborhood (MN) and moving in a limited neighborhood (MLN). The next location of the dummy is decided in a neighborhood of the current location of the dummy. However, the dummies' trajectories may be different from the user's trajectory. It might result in identification of the user's trajectory easily among them.

In this paper, we construct two equivalence classes in an interval time T on the basis of the user's partners. Take note

DOI: 10.1002/wcm

Algorithm 1 Partners selection

```
Require: $T \vee Map \vee User$
Ensure: Partners of the user
Procedure
repeat
  for $i = 1$ to $k$ do
    Convert map into Coordinate axis;
    User's original location $(x, y)$ && Participators' location $(m_i, n_i)$;
    $D(i) = sqrt\left((x - m_i)^2 + (y - n_i)^2\right)$;
  end for
  Sort(D);
  Send (signature (UsrID));
  if verify(UsrID) & participators have not been selected then
    Location $[1 : k]$ = response(PartnerLocation, PartnerID);
  end if
  Select $k$ different participators as the user's partners;
  Record their coordinates to form an equivalence class;
until (User's next location! =User's current location);
```

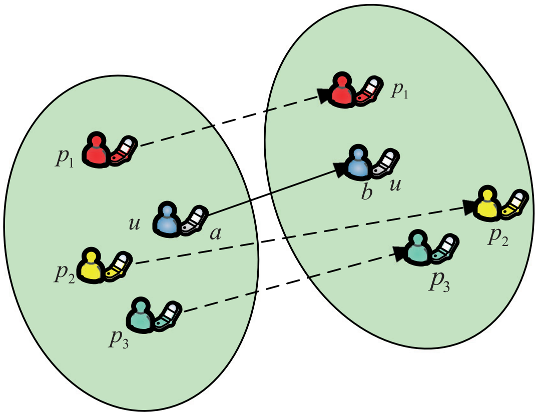


Figure 3. The trajectories of the user and his or her partners.

that the uploaded reports only include each location and request, thus adversary can hardly identify the real user by comparing the two equivalence classes for different values. We employ the assumption [39] that the user's trajectory is linear in the interval time T. According to the corresponding distance away from the user in the two equivalence classes, we map the partners' corresponding locations to produce k similar trajectories to that of the user. The effectiveness will be discussed in Section 5.3. To demonstrate more clearly, we take an example to reconstruct the process. As illustrated by Figure 3, a user stays at point a. Before he or she requests a service (e.g., find the nearest restaurant), he or she selects $k(k = 3)$ partners as an equivalence class to cloak herself. Then, all the participators in the equivalence class send their locations to the AS. When the user moves to point b, he or she follows the same process. Note that the partners he or she selected may be different. The partners' trajectories can be constructed upon the distance away from the user, such as the nearest partner in an equivalence class mapping to the nearest one in another equivalence class. Thus, the user's trajectory can be hidden by constructing the partners' trajectories between the two equivalence classes. With the distances between the user and his or her partners, the partners' trajectories are similar to that of the user. We will utilize a new metric SR to evaluate the similarity between the user's trajectory and that of his or her partners. It will be discussed in Section 5.

5. EVALUATION AND EXPERIMENT

In this section, we discuss location and trajectory privacy protection framework and threat model first, and then, we present a new metric, named SR, to evaluate the method we proposed in Section 4 with the practical data. Finally, we formalize the privacy metric and measure the privacy level that LTPPM can achieve against the threat model. Then, we analyze the results to evaluate the effectiveness and efficiency of LTPPM.

5.1. Framework

We present a framework based on [44,45] to evaluate the LTPPM. In this paper, we define the location and trajectory privacy protection framework as a tuple as follows $\langle Ac(Lo, Tr),\ LTPPM,\ Ob(Lo, Tr),\ Adv,\ Metric \rangle$, where $Ac(Lo, Tr)$ is the actual location and trajectory set of the user and $Ob(Lo, Tr)$ is the observed location and trajectory set of the members in equivalence class. LTPPM stands for location and trajectory privacy protection mechanism presented in this paper. *Adv* is an entity who implements some typical attacks against LTPPM to get the actual user's location and trajectory. The effectiveness of breaking the user's location and trajectory privacy is measured by *Metric*.

(1) $Ac(Lo, Tr)$ and $Ob(Lo, Tr)$

The user takes k partners to construct an equivalence class. We sort the partners according to the distances from the user, which is described as $(u, u_1, u_2, \ldots, u_k)$. When he or she moves to another location v, he or she follows the same operation to form another equivalence class including m partners, which are described as $(v, v_1, v_2, \ldots, v_m)$. At present, we get two equivalence classes in the interval time T. The mapping relationship is constructed on the basis of the corresponding distances in the two equivalence classes. We can construct several trajectories between the two equivalence classes, which are showed by $\langle (u, v), (u_1, v_1), \ldots, (u_{\min\{k,m\}}, v_{\min\{k,m\}}) \rangle$. Thus, we can get $\min\{k, m\} + 1$ trajectories presented by $Ob(Lo, Tr)$. But only $Ac(Lo, Tr)$ is the user's real trajectory among them.

(2) LTPPM

To ensure that the user's location and trajectory privacy would not be invaded, we have discussed the LTPPM in Section 4.1 and Section 4.3, respectively. Given the user's location $Lo(u)$ and trajectory $Tr(u)$, we obscure them to $Lo = \langle Lo(u), Lo(u_1), \ldots, Lo(u_k)\rangle$ and $Tr = \langle Tr(u), Tr(u_1), \ldots, Tr(u_m)\rangle$ using the aforementioned LTPPM.

Neither the disclosure of location nor trajectory would violate a user's privacy information. For example, if the user's trajectory is exposed, the adversary might deduce the user's location by combining his or her knowledge about the user and vice versa. Therefore, both the user's location and trajectory should be protected together. The aim of the adversary is to infer the user's privacy with the probability function depicted by Equation (1). In other words, LTPPM is to make the probability low so that the user's privacy information can be highly protected.

$$\begin{aligned} P(u) &= \Pr\{Ac(Lo(u) \cup Tr(u))|Ob(Lo, Tr)\} \\ &= \Pr\{Ac(Lo(u))|Ob(Lo)\} \\ &\quad + P\{Ac(Tr(u))|Ob(Tr)\} \\ &\quad - \Pr\{Ac(Lo(u) \cap Tr(u))|Ob(Lo, Tr)\} \end{aligned} \tag{1}$$

In the following, we will present the privacy metric to evaluate the correctness of the adversary to get the real user and the effectiveness of LTPPM in privacy protection.

(3) Privacy metric

We consider all the slopes are exist and present a new metric, named SR, to measure similarity among trajectories and define their indiscernibility relationship. Then, we formalize the correctness that adversary can identify a real user and define the location and trajectory privacy level.

Defination 1 (Slope Ratio). *In an interval time T, we assume that the user's trajectory is linear. We get the user's source location coordinate $A(x_1, y_1)$ and the destination coordinate $B(x_2, y_2)$. The user's trajectory slope can be calculated by $k_1 = (y_2 - y_1)/(x_2 - x_1)$. Similarly, we can get the partners' trajectories slopes $k_2, k_3, \ldots, k_m$. SR is defined as $\alpha(\alpha_i = k_i/k_1, i = 2, 3, \ldots, m)$, where when α is within the threshold we define, the two trajectories are considered to be similar.*

Defination 2 (Indiscernibility Relationship). *Let σ be a threshold we define; when the ratio α of partners' trajectories slope $k_i (i = 2, 3, \ldots)$ to the user's trajectory slope k_1 is within $[0, +\sigma]$, we consider the user's trajectory and his or her partners' trajectories cannot be distinguished. The closer the SR α is to one, the more difficult it is for an adversary to distinguish the user's trajectory from his or her partners' trajectories.*

Location and trajectory privacy of a user is defined as the error of the adversary in estimating the actual location and trajectory of the user. The correctness of the adversary is quantified using the expected difference between the real outcome $(Lo(u), Tr(u))$ and the estimator on the basis of the probability function $P(u)$. In formalization, the correctness of the adversary to get the real user can be calculated by Equation (2).

$$Correct_{Adv} = \begin{cases} P(u)(\alpha_i \cdot \beta_i) & \text{if } \alpha_i > 1 \\ P(u)((1-\alpha_i) \cdot \beta_i) & \text{if } 0 \le \alpha_i \le 1 \\ 1 & \text{if } \alpha_i < 0 \end{cases}$$

$$\text{where} \quad \beta_i = \frac{Lo(u) - Lo(u_i)}{\| Lo(u) - Lo(u_i) \|} \tag{2}$$

We define the difference as the relationship between α_i and β_i, where α_i means the similarity between the user's trajectory and his or her partners' trajectories set Tr and β_i represents the distances between the user's location and the observed locations set Lo, which are converted into $[0, 1]$ interval. As an example, when the distances are non-zero, that is $\beta_i \neq 0$, the difference is defined to be equal to 0 if and only if $\alpha_i = 1$. Specially, if $\alpha_i < 0$, it means that the trajectories of the user's partners go in different directions. Therefore, it is easier for an adversary to deduce the user's trajectory and location in an interval time T. Thus, we define the correctness of the adversary is 1 and remove the trajectory.

Theorem 1. *When the distances are constant, it can be seen that the closer α_i is to one, the lower of the correctness that adversary observes the real user is. Otherwise, if the α_i is far away from one, it is easy for the adversary to distinguish the user's trajectory and location from the observed sets.*

Proof. See Appendix A. □

We quantify the privacy of a user as the error of the adversary in estimating the actual location and trajectory of the user. Hence, the privacy metric can be calculated as $1 - Correct_{Adv}$. The higher $Correct_{Adv}$ is, the lower the privacy is. Therefore, adversary can identify the user's trajectory easily if the user's trajectory is different from that of his or her partners greatly. To solve the problems, the user's partners' locations should not be far away from the user, and SR should be close to one. We can see that the closer the partners' location and trajectory is to that of the user, the lower $Correct_{Adv}$ is. Therefore, the privacy of the target will be highly protected.

5.2. Threat model

The goal of the adversary is to locate the user's location or trajectory in an interval time T through the observed locations and trajectories. More formally, we consider that the adversary possesses certain background knowledge about the user such as the location and trajectory information distribution, the characteristics of services, and also privacy-preserving mechanism. The most general one is to recover all the trajectories of all participants, that is, to compute the probability $P\{Ac(Lo,Tr)|LTPPM, Ob(Lo,Tr)\}$. Besides, we assume that there is no special information to reveal the user's privacy information from the observed information. It means that the user and his or her partners would be distinguished at the same probability.

Theorem 2. *Given k and m partners in the two equivalence classes separately,* $\min\{(k+1),(m+1)\}$ *trajectories have been constructed. The average location and trajectory re-identification probability are bounded by Equations (3) and (4).*

$$P_1 = \Pr\left\{u = Ac(Lo(u))|\bigcap_i Ob(Lo(u_i))\right\} = \frac{1}{k+1}$$
$$P_2 = \Pr\left\{u = Ac(Lo(v))|\bigcap_i Ob(Lo(v_i))\right\} = \frac{1}{m+1} \tag{3}$$

and

$$P_3 = \Pr\left\{u = Ac(Tr(u))|\bigcap_i Ob(Ac(Tr(u_i)))\right\} = \frac{1}{\min\{(k+1),(m+1)\}} \tag{4}$$

Proof. In this attack model, we assume that the adversary can access all the public locations and trajectories. Adversaries do know the distribution of the places on the map, but they do not know which is the real user when they request for services. Given two published equivalence classes, there are k and m partners. $\min\{k+1, m+1\}$ trajectories are constructed. The re-identification probability depends on the number of partners in the two equivalence classes are bounded by Equations (3) and (4). □

Take a simple example; suppose there are two partners in each equivalence class. Three trajectories are constructed, and only one of them is the real user's trajectory. Because of the similarity among trajectories, the identification probabilities of the user's real location and trajectory are $1/3$, respectively. When there are lots of partners in each equivalence class, which means that k and m are very large, the probabilities that an adversary can identify the user's location and trajectory are very low. It means that our method can protect the user's location and trajectory privacy effectively.

The most general one is to recover the user's location and trajectory together in the interval time T. It can be computed at the probability depicted by Equation (5).

$$P_4 = \Pr\{u = Ac(Lo(u), Tr(u))|Ob(Lo,Tr)\} = P_1 \cdot P_2 \cdot P_3 \tag{5}$$

As indicated in Equation (1), the function presents the probability that the adversary derives the user's location or trajectory. The correctness of invasion of the user's privacy under the probability $P(u)$ with various differences is depicted by Equation (2). We can see that the higher Equation (1) is, the higher the success rate of the adversary is.

5.3. System simulation

In this section, we evaluate the effectiveness and efficiency of LTPPM in protecting a user's privacy while his or her location or trajectory exposes in an interval time T. We measure the user's location and trajectory privacy with the privacy metric presented above and demonstrate the robustness of LTPPM against threat model.

5.3.1. Simulation setting.

The dataset we acquired from GeoLife (Microsoft Research Asia) [46,47] contains more than 8000 trajectories by 165 users in a period of over 2 years (from April 2007 to August 2009). According to their dataset specification, a sequence of time-stamped points contains the information of latitude, longitude, height, speed, heading direction, and so on. These data were recorded by different GPS loggers or GPS phones, and have a variety of sampling rates. Of the trajectories, 95% are logged in a dense representation, for example, every 2–5 s or every 5–10 m per point, while a few of them do not have such a high density being constrained by the devices.

We captured the map information from Geolife. Figure 4 shows the location information of Beijing [46,47]. We randomly chosen part of the data and imported them into a two-dimensional relative coordinate system, as Figure 5 displays.

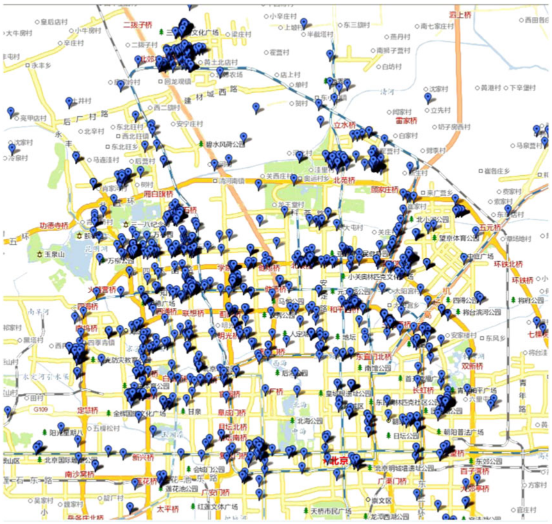


Figure 4. Data distribution in Beijing [46,47].

DOI: 10.1002/wcm

5.3.2. Simulation results.

The user's location in the coordinate system is showed by a blue circle in Figure 6. In order to protect the user's location privacy information, we assume that he or she forms an equivalence class with 20 partners. When he or she moves to another location, he or she forms another equivalence class with the same number of partners. On the basis of Algorithm 1, we select the partners and construct the mapping relationship between the two equivalence classes. The process is depicted by Figure 7.

The user's trajectory can also be protected among the mapping relationship. However, if the partners' trajectories are different from the user's trajectory, it might be easy to identify the real user. Therefore, we utilize a new metric SR defined by Definition 1 to evaluate the similarity between the user's trajectory and that of his or her partners.

We select a threshold $\sigma = 1$ and analyze the result. The similarity relationship between the user's trajectory and that of his or her partners is depicted in Figure 8. We can obverse that there are lots of partners' trajectories whose SRs are fluctuating around 1. It proves that the algorithm can produce lots of trajectories that are similar to the user's trajectory under the threshold that is set by the user. We change the threshold σ ($\sigma = 2, 3, \ldots, 6$). Figure 9 shows the number of partners that satisfy the condition defined in Definition 2 with the six different thresholds.

As we can see, the higher the threshold σ is, the more partners we can choose. Through defining the threshold value σ, we can decide how many partners we should select to protect the user's location and trajectory privacy in participatory sensing.

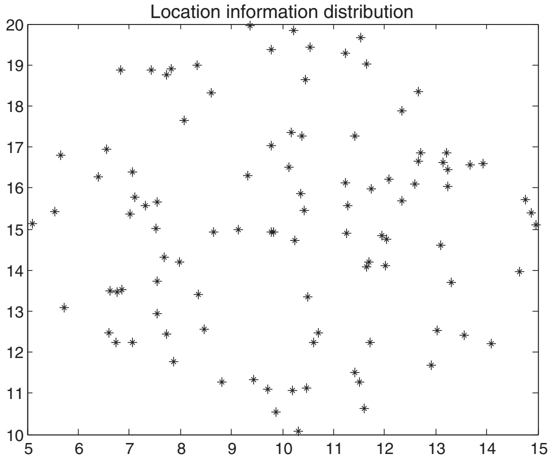


Figure 5. Part of data in two-dimensional relative coordinate system.

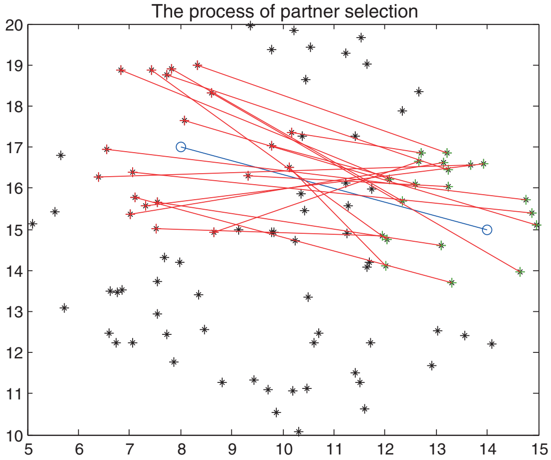


Figure 7. The process of partner selection.

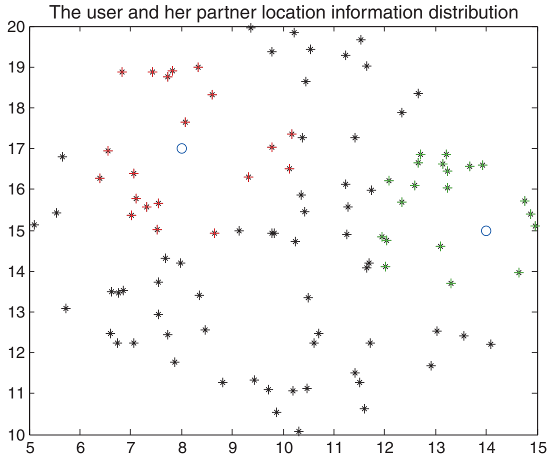


Figure 6. The user and his or her partner location information distribution.

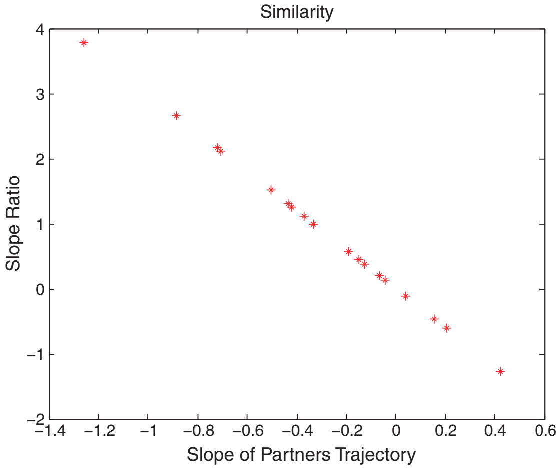


Figure 8. The similarity relationship between the user's trajectory and that of his or her partners.

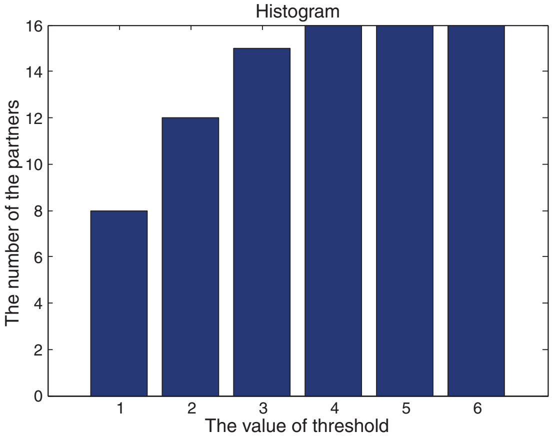


Figure 9. The number of partners with different thresholds.

5.3.3. Effectiveness.

In this section, we evaluate the effectiveness of LTPPM against the threat model defined in Section 5.2. Figure 10 shows the conditions of different number of partners ($\text{num} = 10, 20, 25$). The left figures depict the correctness that the adversary could obtain the user's real location or trajectory information, and the right figures show the privacy level that LTPPM can achieve. It presents the effectiveness of LTPPM in protecting the user's location and trajectory privacy.

Comparing the results of different numbers of the user's partners, we conclude that the correctness of the adversary in identifying the user's real location and trajectory decreases with the number of the user's partners increases. That is because the increase of the user's partners would cause the adversary to have more difficulty in identifying the real user. Thus, the user's location and trajectory privacy can be enhanced.

To be more specific, the x-axis shows the SR between the user's trajectory and that of his or her partners. In the left figures, the y-axis stands for correctness of adversary. We can see that there are lots of data around $SR = 1$. The closer the SR is to one, the correctness of adversary to identify the user's real location and trajectory decreases. The closer the SR is to one means that the user's trajectory is more similar to that of his or her partners, which is proved by Theorem 1. This may make it difficult for the adversary to distinguish the real user's location and trajectory from a set of observed locations and trajectories. Therefore, the correctness of the adversary is low where the SR is close to one. In the right figures, the y-axis represents the location and trajectory privacy, which is defined in Section 5.1. In contrast to the left, the closer the SR is to one, the higher location and trajectory privacy is. Overall, we can see that when the number of the user's partners is enough, the probability of location and trajectory privacy is more than 0.5. Hence, it can be concluded that the LTPPM is effective on privacy protection.

5.3.4. Efficiency.

To evaluate the cost of our approach, we mainly concern on anonymous communication time and storage overhead in quantitative analysis. In our LTPPM, anonymous communication time and storage overhead increase are generated as a side effect to enhance location and trajectory privacy. Because the processing cost for each equivalence class is low, we do not consider process cost in this paper.

As we mentioned in Section 4.1, in the service request phase, to obtain a high quality of service, each participator in the equivalence class sends their location data $\{(x, y), (x_1, y_1), \ldots, (x_k, y_k)\}$ to AS, where $L = (x, y)$ is the real user's location and $L_i = (x_i, y_i)$, $i = 1, 2, \ldots, k$, are the user's partners' locations. The cost of anonymous communication time is $O(k)$. Therefore, the anonymous communication time increases proportionally with the number of partners in the equivalence class increases. Similarly, in the service query and distribution phase, because $Result_i$ corresponds to L_i, the cost of anonymous communication time is $O(k)$.

To protect the user's trajectory privacy, we construct $k + 1$ similar trajectories based on the two equivalence classes in the interval time T in Section 4.3. To confuse the adversary, we need to store the partners' trajectories. The overhead of storage is $O(k)$, which is proportional to the number of trajectories.

6. DISCUSSIONS

In this paper, a user's location and trajectory privacy can be protected. We discuss and analyze LTPPM as follows.

6.1. Location privacy protection

We expect that the location privacy of a user at the micro level is inversely proportional to locate the user at a given interval time T. That is, the more accurate the adversary can locate a user, the poorer the location privacy of the user will be. Most of the existing work protects a user's location privacy by the accuracy reduction technique, such as transforms the accurate location of the user into a cloak spatial area. Although location privacy is enhanced, the quality of service may reduce. It is not applicable in some participatory sensing applications that require precise location information for high quality of services.

To overcome this contradiction between privacy and quality of service in this paper, a user selects several partners to construct an equivalence class. All the partners in the equivalence class provide their accurate locations together with the user to confuse adversary for a high privacy level. Meanwhile, the user can obtain a high quality of service. Note that they would not send any other information with identity-related information. Even though the user changes the partner groups very frequently, the adversary cannot identify the real user because all coordinates of the user and his or her partner groups are different

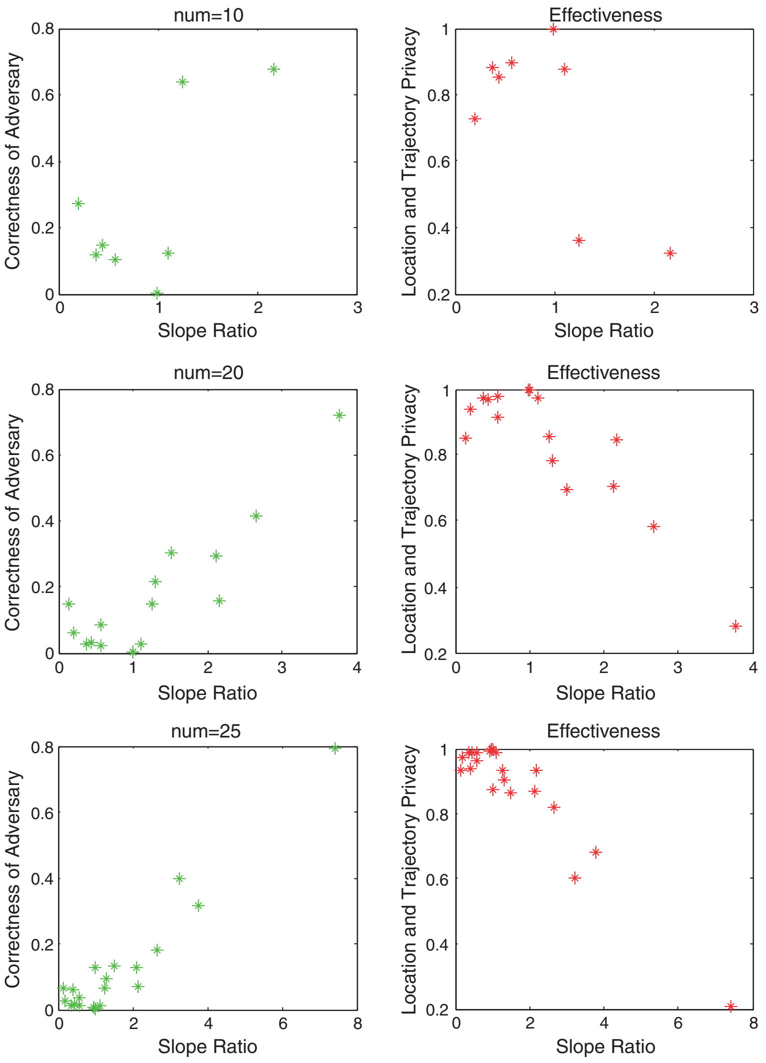


Figure 10. Correctness of adversary and effectiveness of *LTPPM*.

each time. Although AS can obtain the user and his or her partners' accurate locations, they cannot identify the user's accurate location by comparing different partner groups. Compared with the accuracy reduction technique, our method could provide a more accurate location for quality of service while the privacy level will not decrease.

6.2. Trajectory privacy protection

Once a user's trajectory is identified, it might threaten his or her location privacy. Therefore, it is important to protect a user's motion trajectory in participatory sensing.

To prevent an adversary from identifying the user's trajectory, we construct several partners' trajectories that are similar to that of the user in an interval time T. The construct process is depicted in Section 4.3 in detail. The effectiveness is evaluated in Section 5 through theoretical proof and simulation. Although the adversary may observe all possible trajectories, he or she can hardly make a distinction between the user's real trajectory and his or her partners' trajectories. Through the method, the user's trajectory can be hidden among the partners' trajectories.

7. CONCLUSIONS

In this paper, we propose a method to protect a user's location privacy while providing high quality of service. Through selecting a certain number of the user's partners to construct an equivalence class, we can hide the user's location. Considering that the user's motion trajectory might also reveal the user's privacy, we propose an algorithm to construct several trajectories that are close to the user's trajectory. It can prevent an adversary from identifying the user's real trajectory from his or her partners' trajectories effectively. Finally, we utilize a new metric, named SR, to evaluate the similarity between the user's trajectory and that of his or her partners. Then, we formalize the location and trajectory privacy protection framework and analyze the threat model. Aiming at the threat model, we measure the privacy level that the LTPPM can achieve and analyze the effectiveness and efficiency of LTPPM through the results.

Note that we argue the partners will not reveal the user's location. Once the partners collude with AS, they may reveal the user's information to AS. Thus, the user's location and trajectory privacy will be invaded. With the proposed LTPPM having much space to extend, in the future, we will consider to prevent such collusion attack; besides, we plan to address anonymity of static user's continuous query services and extend our proposal to continuous location and trajectory privacy protection.

APPENDIX A

The proving process can be depicted as following. From Figure A.1, $\overrightarrow{T_1} = (x_B - x_A, y_B - y_A)$ and $\overrightarrow{T_2} = (x_{B'} - x_{A'}, y_{B'} - y_{A'})$ represent two vector trajectories. Suppose the slopes of the two trajectories are exist and equal to k_1 and k_2, respectively. The angle of the two trajectories can be computed as follows:

$$\begin{aligned}\cos\theta &= \frac{\overrightarrow{T_1}\cdot\overrightarrow{T_2}}{|\overrightarrow{T_1}||\overrightarrow{T_2}|}\\ &= \frac{(x_B - x_A)\cdot(x_{B'} - x_{A'}) + (y_B - y_A)\cdot(y_{B'} - y_{A'})}{\sqrt{(x_B - x_A)^2 + (y_B - y_A)^2}\cdot\sqrt{(y_{B'} - y_{A'})^2 + (x_{B'} - x_{A'})^2}}\\ &= \frac{1 + k_1\cdot k_2}{\sqrt{1 + k_1^2}\cdot\sqrt{1 + k_2^2}}\end{aligned}$$

where $\theta \in [0, \pi]$. We construct trajectory function

$$f(x) = \frac{1 + k_1 x}{\sqrt{1 + k_1^2}\cdot\sqrt{1 + x^2}}$$

where k_1 represents the slope of user's trajectory.

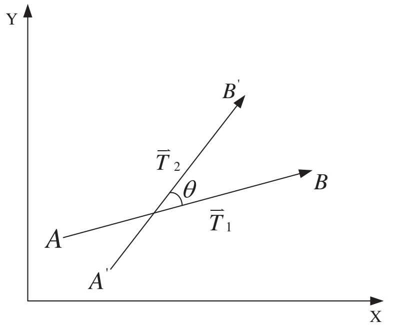


Figure A.1. Diagram.

Now, we discuss the slope trajectory relationship between partners and the user. Because $f(x)$ is continuously differentiable, we can compute the derivative $f'(x)$ with respect to x:

$$f'(x) = \frac{k_1 - x}{\left(1 + k_1^2\right)^{1/2}\cdot\left(1 + x^2\right)^{3/2}}$$

when $x < k_1$, then $f'(x) > 0$, $f(x) \nearrow$; otherwise, $x > k_1$, then $f'(x) < 0$, $f(x) \searrow$; $f(x)$ gets the maximum value if and only if $x = k_1$.

As we define $\alpha = x/k_1 (x = k_2, k_3, \ldots, k_m)$. When $x \to k_1$, then $\alpha \to 1$ and $f(x) \to \max\{f(x)\}$. Therefore, $\theta \to 0$, which means that the two trajectories keep indiscernibility relationship; it is hard to identify the real user. Otherwise, if the α_i is far away from one, it is easy for the adversary to distinguish the user from the observed sets.

ACKNOWLEDGEMENTS

We would like to thank the anonymous referees for carefully reading the paper. Their useful comments and suggestions improved the quality for the paper. This work was supported by Program for Changjiang Scholars and Innovative Research Team in University(IRT1078), the Key Program of NSFC-Guangdong Union Foundation (U1135002), Major National S&T Program (2011ZX03005-002), and the Fundamental Research Funds for the Central Universities (JY10000903001).

REFERENCES

1. Mobile phone. http://en.wikipedia.org/wiki/Mobile_phone [accessed on 2011, WIKI].
2. Burke J, Estrin D, Hansen M. Participatory sensing, In *Workshop on World-sensor-web (WSW'06): Mobile Device Centric Sensor Networks and Applications*, Colorado, USA, 2006; 117–134.
3. Campbell AT, Eisenman SB, Lane ND, Miluzzo E, Peterson RA. People-centric urban sensing, In *Proceedings of the 2nd Annual International Workshop on Wireless Internet*, NY, USA, 2006; 2–5.
4. Mobile location-based services on the move. http://www.emarketer.com/Article.aspx?R=1006609 [accessed on October 2008, eMarketer].
5. Hull B, Bychkovsky V, Zhang Y, Chen K, Goraczko M, Miu A, Shih E, Balakrishnan H, Madden S. Cartel: a distributed mobile sensor computing system, In *Proceedings of the 4th International Conference on Embedded Networked Sensor Systems*, Colorado, USA, 2006; 125–138.
6. Eisenman SB, Miluzzo E, Lane ND, Peterson RA, Ahn GS, Campbell AT. Bikenet: a mobile sensing system for cyclist experience mapping. *ACM*

Transactions on Sensor Networks (TOSN) 2009; **6**(1): 1–39.

7. Reddy S, Parker A, Hyman J, Burke J, Estrin D, Hansen M. Image browsing, processing, and clustering for participatory sensing: lessons from a dietsense prototype, In *Proceedings of the 4th Workshop on Embedded Networked Sensors*, Cork, Ireland, 2007; 13–17.
8. Mun M, Reddy S, Shilton K, Yau N, Burke J, Estrin D, Hansen M, Howard E, West R, Boda P. Peir, the personal environmental impact report, as a platform for participatory sensing systems research, In *Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services*, Wroclaw, Poland, 2009; 55–68.
9. Christin D, Reinhardt A, Kanhere S, Hollick M. A survey on privacy in mobile participatory sensing applications. *Journal of Systems and Software* 2011; **84**(11): 1928–1946.
10. Mills E. Google sued over android data location collection. http://news.cnet.com/8301-27080_3-20058493-245.html [accessed on April 2011, CNET News].
11. Lowensohn J. Apple sued over location tracking in iOS. http://news.cnet.com/8301-27076_3-20057245-248.html [accessed on April 2011, CNET News].
12. Calandriello G, Papadimitratos P, Hubaux JP, Lioy A. Efficient and robust pseudonymous authentication in VANET, In *Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks*, Montreal, Canada, 2007; 19–28.
13. Gruteser M, Grunwald D. Anonymous usage of location-based service through spatial and temporal cloaking, In *Proceeding of the 1st International Conference on Mobile Systems, Application, and Service*, CA, USA, 2003; 31–42.
14. Gruteser M, Hoh B. On the anonymity of periodic location samples, In *Proceedings of the 2nd International Conference on Security in Pervasive Computing*, Boppard, Germany, 2005; 179–192.
15. Riley P. The tolls of privacy: an underestimated roadblock for electronic toll collection usage, In *Proceeding of the 3rd International Conference on Legal, Security, and Privacy Issues in IT*, Prague, Czech, 2008; 521–528.
16. Huang K, Kanhere SS, Hu W. Preserving privacy in participatory sensing systems. *Computer Communications* 2010; **33**(11): 1266–1280.
17. Mohammed N, Fung B, Debbabi M. Walking in the crowd: anonymizing trajectory data for pattern analysis, In *Proceeding of the 18th ACM Conference on Information and Knowledge Management*, Hong Kong, China, 2009; 1441–1444.
18. Machanavajjhala A, Kifer D, Gehrke J, Venkitasubramaniam M. l-diversity: privacy beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data (TKDD)* 2007; **1**(1): 3.
19. Shokri R, Freudiger J, Hubaux JP. A unified framework for location privacy, In *Proceeding of the 3rd Hot Topics in Privacy Enhancing Technologies (hotPETs)*, Berlin, Germany, 2010; 203–214.
20. Gedik B, Liu L. Location privacy in mobile systems: a personalized anonymization model, In *Proceeding of the 25th IEEE International Conference on Distributed Computing Systems*, Ohio, USA, 2005; 620–629.
21. Gedik B, Liu L. Protecting location privacy with personalized k-anonymity: Architecture and algorithms. *IEEE Transactions on Mobile Computing* 2008; **7**(1): 1–18.
22. Sweeney L. k-anonymity: A model for protecting privacy. *International Journal Of Uncertainty Fuzziness and Knowledge Based Systems* 2002; **10**(5): 557–570.
23. Sweeney L. Achieving k-anonymity privacy protection using generalization and suppression. *International Journal Of Uncertainty Fuzziness and Knowledge Based Systems* 2002; **10**(5): 571–588.
24. Bayardo RJ, Agrawal R. Data privacy through optimal k-anonymization, In *Proceeding of the 21st International Conference on Data Engineering*, Tokyo, Japan, 2005; 217–228.
25. LeFevre K, Dewitt DJ, Ramakrishnan R. Incognito: efficient full-domain k-anonymity, In *Proceeding of SIGMOD Conference*, Maryland, USA, 2005; 49–60.
26. LeFevre K, Dewitt DJ, Ramakrishnan R. Mondrian multidimensional k-anonymity, In *Proceeding of the 22nd International Conference on Data Engineering*, Georgia, USA, 2006; 25–25.
27. Meyerowitz J, Roy Choudhury R. Hiding stars with fireworks: location privacy through camouflage, In *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking*, ACM, Beijing, China, 2009; 345–356.
28. Mokbel MF, Chow CY, Aref WG. The new casper: query processing for location services without compromising privacy, In *Proceedings of the 32nd International Conference on Very Large Data Bases*, VLDB Endowment, Seoul, Korea, 2006; 763–774.
29. Tang M, Wu Q, Zhan G, He L, guo Zhang H. A new scheme of LBS privacy protection, In *Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing*, Beijing, China, 2009; 1–6.

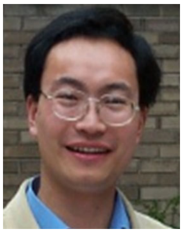
30. Ghinita G, Kalnis P, Skiadopoulos S. Prive: anonymous location-based queries in distributed mobile systems, In *Proceedings of the 16th International Conference on World Wide Web*, ACM, Banff, Canada, 2007; 371–380.
31. Beresford AR, Stajano F. Location privacy in pervasive computing. *IEEE Pervasive Computing* 2003; **2**(1): 46–55.
32. Beresford AR, Stajano F. Mix zones: user privacy in location-aware services, In *IEEE Workshop on Pervasive Computing and Communication Security (PerSec)*, Concepcion, Chile, 2004; 127–131.
33. Kapadia A, Triandopoulos N, Cornelius C, Peebles D, Kotz D. Anonysense: opportunistic and privacy-preserving context collection. *Pervasive Computing* 2008; **5013**: 280–297.
34. Cornelius C, Kapadia A, Kotz D, Peebles D, Shin M, Triandopoulos N. Anonysense: privacy-aware people-centric sensing, In *Proceeding of the 6th International Conference on Mobile Systems, Applications, and Services (MobiSys'08)*, Colorado, USA, 2008; 211–224.
35. Kido H, Yanagisawa Y, Satoh T. An anonymous communication technique using dummies for location-based service, In *Proceedings International Conference on Pervasive Services (ICPS'05.)*, Santorini, Greece, 2005; 88–97.
36. Dong K, Gu T, Tao X, Lu J. Privacy protection in participatory sensing applications requiring fine-grained locations, In *Proceeding of the 16th International Conference on Parallel and Distributed Systems*, Tainan, Taiwan, 2010; 9–16.
37. Terrovitis M, Mamoulis N. Privacy preservation in the publication of trajectories, In *Proceeding of the 9th International Conference on Mobile Data Management, 2008 (MDM'08.)*, IEEE, Beijing, China, 2008; 65–72.
38. Nergiz ME, Atzori M, Saygin Y. Towards trajectory anonymization: a generalization-based approach, In *Proceedings of the Sigspatial ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS*, CA, USA, 2008; 52–61.
39. Abul O, Bonchi F, Nanni M. Never walk alone: uncertainty for anonymity in moving objects databases, In *Proceeding of the 24th International Conference on Data Engineering*, IEEE, Cancun, Mexico, 2008; 376–385.
40. You TH, Peng WC, Lee WC. Protecting moving trajectories with dummies, In *International Conference on Mobile Data Management*, IEEE, Mannheim, Germany, 2007; 278–282.
41. Huo Z, Huang Y, Meng X. History trajectory privacy-preserving through graph partition, In *Proceedings of the 1st International Workshop on Mobile Location-based Service*, ACM, Beijing, China, 2011; 71–78.
42. Huo Z, Meng X, Hu H, Huang Y. You can walk alone: trajectory privacy-preserving through significant stays protection, In *Proceedings of the 17th International Conference on Database Systems for Advanced Applications (DASFAA2012)*, Busan, South Korea, 2012; 351–366.
43. Kazemi L, Shahabi C. Towards preserving privacy in participatory sensing, In *IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM workshops)*, WA, USA, 2011; 328–331.
44. Shokri R, Theodorakopoulos G, Boudec J, Hubaux J. Quantifying location privacy, In *IEEE Symposium on Security and Privacy*, Oakland, 2011; 247–262.
45. Shokri R, Theodorakopoulos G, Boudec J, Hubaux J. Quantifying location privacy: the case of sporadic location exposure, In *Processing of the 11th Privacy Enhancing Technologies Symposium (PETS)*, Waterloo, Canada, 2011; 57–76.
46. Zheng Y, Li Q, Chen Y, Xie X. Understanding mobility based on GPS data, In *Proceedings of ACM Conference on Ubiquitous Computing (UbIComp'2008)*, Seoul, South Korea, 2008; 312–321.
47. Zheng Y, Li Q, Chen Y, Xie X. Mining interesting location and travel sequence from GPS trajectories, In *Proceeding of International Conference on World Wide Web (WWW 2009)*, Madrid, Spain, 2009; 791–800.

AUTHORS' BIOGRAPHIES

Sheng Gao is a PhD candidate at Xidian University. He received the BSc degree in information and computation science from the Xi'an University of Posts and Telecommunications, Xi'an, China, in 2009. His interests include mobile computing, participatory sensing, and mobile data management with focus on security and privacy issues.

Jianfeng Ma received his BS degree in mathematics from Shaanxi Normal University, China, in 1985, and obtained his ME and PhD degrees in computer software and communications engineering from Xidian University, China, in 1988 and 1995, respectively. From 1999 to 2001, he was with Nanyang Technological University of Singapore as a research fellow. He is an IEEE member and a senior member of Chinese Institute of Electronics (CIE).

Now he is a professor and PhD supervisor in School of Computer Science at Xidian University, Xi'an, China. His current research interests include distributed systems, wireless and mobile computing systems, computer networks, and information and network security.



Weisong Shi is an associate professor of Computer Science at Wayne State University. He received his B.S. degree from Xidian University in 1995 and Ph.D. degree from the Chinese Academy of Sciences in 2000, both in Computer Engineering. His current research focuses on computer systems, mobile computing, and cloud computing. Shi has published 120 peer-reviewed journal and conference papers in these areas, with an H-index of 23. He has served the program chairs and technical program committee members of numerous international conferences, including WWW and ICDCS. He is a recipient of the NSF CAREER award, one of 100 outstanding Ph.D. dissertations (China) in 2002, a recipient of the Career Development Chair Award of Wayne State University in 2009, and a recipient the "Best Paper Award" of ICWE'04, IPDPS'05, HPCChina'12, and IISWC'12.

Guoxing Zhan is currently a software engineer at Cisco Systems Inc. He received his Ph.D. in Computer Science from Wayne State University in 2012 and his M.S. in Mathematics from the Chinese Academy of Sciences in 2007. Zhan has a broad interest in research on data center networking, participatory sensing, wireless sensor network, mobile computing, networking and systems security, trust management, and information processing.