Towards Location and Trajectory Privacy Protection in Participatory Sensing

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

[1] Xidian University, Xi'an, Shaanxi 710071, China
[2] Wayne State University, Detroit, MI 48202, USA
{sgao,jfma}@mail.xidian.edu.cn, {weisong,gxzhan}@wayne.edu

Abstract. The ubiquity of mobile devices has facilitated the prevalence of participatory sensing, whereby ordinary citizens using their private mobile devices to collect regional information and share with participators. However, such applications may endanger 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 which require precise location information for high quality of service. In this paper, we present a method to protect the user's location and trajectory privacy with high quality of service in some participatory sensing applications. Then, we utilize a new metric, called *Slope Ratio (SR)*, to evaluate the method we proposed. The analysis and simulation results show that the method can protect the user's location and trajectory privacy effectively.

Keywords: participatory sensing, location privacy, trajectory privacy, similarity.

1 Introduction

Participatory Sensing [1] is the process whereby individuals and communities use evermore-capable mobile phones and cloud services to collect and analysis systematic data for use in discovery. However, when a user asks for a certain application, she uploads the request data to servers which are invariably tagged with the location (obtained from the embedded GPS in the phone or using Wi-Fi based localization) and time when the readings are recorded. The mobile sensor data may reveal the user's location at particular time which is related to the user's identity information. It may invade the user's privacy information seriously. We also consider that the user's motion pattern may reveal her trajectory privacy. *Background knowledge attack* [2] exploits the prior knowledge about the user to conclude her privacy information.

In this paper, we aim to protect a user's location and trajectory privacy in participatory sensing applications which require precise location information. We exploit the user's partners to construct an anonymous set, called an equivalence class. The user and her partners send the same service request and their precise locations information to Application Server for high quality of service. The user's location can be concealed by the equivalence class. To protect the user's trajectory privacy, we construct the mapping relationship between the two equivalence classes. The partners'

J.Y. Zhang et al. (Eds.): MobiCASE 2011, LNICST 95, pp. 381–386, 2012.

trajectories should be similar to the user's trajectory so that it cannot be distinguished by adversary. Also, we utilize a new metric *Slope Ratio (SR)* to evaluate the method we propose and implement the simulation system with practical data.

2 Related Work

K-anonymity is originally proposed by Sweeney [3] in the database community to protect sensitive information from being disclosed. 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. Much work has been done to protect location privacy based on *k-anonymity* model [4, 5]; whereas, little work has been done to achieve privacy protection while providing precise location information.

2.1 Coarse-grained Locations Privacy Protection

Tang et al [6] presented ASGKA protocol to build safe group and design a cycle-like structure to make group member have safe status. However, they didn't consider the user's mobility. Beresford and Stajano [7, 8] proposed Mix Zone concept in which a trusted proxy removes all samples before it passes location samples to Application Server. The degree of privacy offered by the Mix Zone was evaluated for pedestrian traffic under the assumption that an adversary used empirical linking. The concept of tessellation was first introduced in AnonySense [9] to protect user's privacy when reporting context information. Tessellation partitions a geographical area into a number of tiles large enough to preserve the user's privacy and each user's location is generalized to a plane in space which covers at least *k* potential users.

2.2 Fine-grained Locations Privacy Protection

Kido et al. [10] 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. Because the service provider cannot distinguish the genuine position data, the user's location privacy is protected. Huang et al. [2] 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 using camera phones. Dong et al. [11] proposed a method to preserve location privacy by anonymizing coarse-grained location and retaining fine fine-grained locations using Attribute Based Encryption.

2.3 Trajectory Privacy Protection

You et al [12] 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, while the rotation pattern explores the idea of creating intersection among moving trajectories.

3 Methodology

3.1 Basic System Structure

The very basic architecture of a participatory sensing system consists of collection of mobile nodes (MNs), some Access Points (APs), Report Server (RS), and Application Server (AS). In Participatory Sensing, MNs collect relevant regional information and send these reports to RS to aggregate, and then send the reports to AS which is showed by Figure.1.

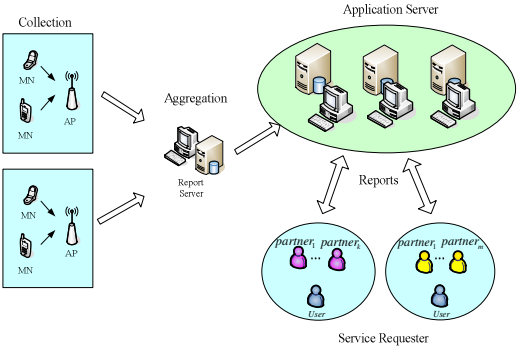

Fig. 1. The basic structure of participatory sensing

3.2 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 won't reveal a user's locations privacy. A user forms an equivalence class by selecting a certain number of partners. The process of partners' selection will be discussed in Section 3.3. There are six partners in the equivalence class which is shown by Figure.2. We argue that the partners won't reveal the user's location information to the AS. The user sends relevant information including her identity signature and requirement to her partners. They verify the user's legality and obtain each coordinate through GPS which are listed as follows: *(L_1, L_2…L_6)*.

(Step1.Service Request) In order to obtain high quality of service and protect privacy information at the same time, the user and her partners send the same service request to the servers which describe as *(L, Request), (L_1, Request), (L_2, Request)… (L_6, Request)*.
(Step2.Service Query) In participatory sensing applications, the AS exploits the information shared by the mobile sensing devices to provide services. Through the precise locations information, it gets the result reports which describe as follows: *(L, Result), (L_1, $Result_1$), (L_2, $Result_2$)… (L_6, $Result_6$)*. Then the AS returns the service result reports to the equivalence class.
(Step3. Service Distribution) All members in the equivalence class receive the result reports. Only the user can pick out the result she desires with her precise location information. The possibility the user can be distinguished will be analyzed in Section 4.

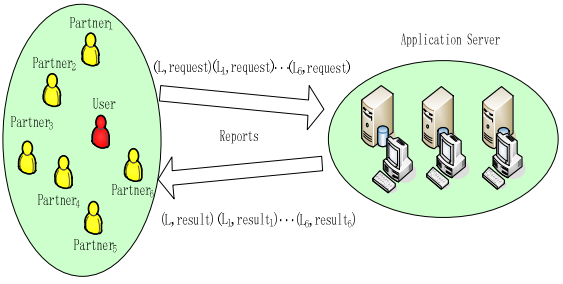

Fig. 2. The Process of Service

3.3 Partners Selection

In order to produce the trajectories those are similar to that of the user. In this paper, we adopt distance-based method to select partners. The pseudo code of the partners' selection is given in Algorithm as follows:

```
T: The public time interval
Input: (Map information, User information)
Output: Partners of the user
```

```
1. Procedure
2.  Do {
3.   For i=1: k
4.     Convert map information into Coordinate axis;
5.     User's location (x, y) && Destination location (mi, ni)
6.     D (i) = sqrt ((x-mi)^2+(y-ni)^2);
7.   End;
8.     Sort (D);
9.     Send (signature (UsrID));
10.  If signature (UsrID) & participators haven't been selected;
11.    Location [1: k] =response (PartnerLocation, PartnerID);
12.  End;
13.  Select k different participators as the user's partners;
14.  Record their coordinates to form an equivalence class;
15.    } while (User's next location! =User's current location);
```

3.4 Trajectory Privacy Protection

In this section, we focus on the user's trajectory privacy protection. We exploit the user's partners to construct two equivalence classes. Through mapping the two equivalence classes, we can produce the partners' trajectories that are similar to that of the user in an interval time *T*. Since the crooked trajectory can be divided into several linear trajectories, we assume the user's trajectory is linear in an interval time *T*. When she moves from a to b showed by Figure.3, she selects several partners in the two equivalence classes separately by the algorithm we propose in section 3.3. We can hide the user's trajectory by constructing the partners' trajectories between the two

equivalence classes. Based on the distance between the user and her partners, the partners' trajectories we construct are similar to that of the user. We will utilize a new metric *Slope Ratio (SR)* to evaluate the similarity between the user's trajectory and that of her partners. It will be discussed in section 4.

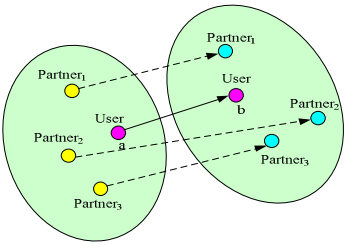

Fig. 3. The trajectories of the user and her partners

4 Experiment and Results

4.1 Theoretical Calculation

The user takes k partners to construct an equivalence class. When she moves to another location, she follows the same operation to form another equivalence class including m partners. At present, we get two equivalence classes in the interval time T. Through the mapping relationship, we can get $min\ \{(k+1), (m+1)\}$ trajectories. Only one of them is the user's real trajectory.

We assume the user and her partners can be distinguished at the same probability. Adversary may get all locations and trajectories information.

1) Location probability. There are k and m participators in the two equivalence classes separately, the probabilities the real user's location information can be distinguished are $P_1=1/(k+1)$ and $P_2=1/(m+1)$.

2) Trajectory probability. Since the partners' trajectories are similar to the user's real trajectory, $min\ \{(k+1), (m+1)\}$ trajectories have been constructed so that the probability of getting the real trajectory is $P_3=1/min\ \{(k+1), (m+1)\}$.

4.2 System Simulation

We utilize a new metric *Slope Ratio (SR)* to evaluate the similarity of trajectory between the user and her partners.

Definition 1. *(Slope Ratio)* In an interval time T, we assume 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 $k= (y_2-y_1)/(x_2-x_1)$.Similarly, we can get the partners' trajectories slope $k_2, k_3 \ldots k_m$. *Slope Ratio* is defined as $\alpha(\alpha = k_i / k_1, i = 2,3,\cdots m)$, where when α is within the threshold we define, the two trajectories are considered to be similar.

Definition 2. (*Indistinguishability*) When the ratio α of partners' trajectories slope $k_i (i = 2,3,\cdots)$ to the user trajectories slope k_1 is within $[0,+\sigma]$, we consider the user's trajectory and her partners' trajectories cannot be distinguished. σ is a threshold, defined by the user.

We have implemented the simulation system with practical data. Detailed evaluation results are available at the technical report version of the paper [13]. The metric shows that the method can protect the user's location and trajectory privacy effectively.

5 Conclusions

In this paper, we propose a method to protect user's location privacy while providing precise location information. Through selecting a certain number of user's partners to construct an equivalence class, we can hide the user's location. Besides, we propose an algorithm to construct several trajectories that are closer to that of the user, which can effectively prevent adversary from identifying the user's trajectory. Finally, we utilize a new metric *Slope Ratio* to analyze the results in theory and experiment.

References

1. Burke, J., Estrin, D., Hansen, M.: Participatory Sensing. In: Workshop on World Sensor Web: Mobile Device Centric Sensor Networks and Applications, USA, pp. 117–134 (2006)
2. Huang, K.L., Kanhere, S.S., Hu, W.: Preserving privacy in participatory sensing systems. Computer Communications 33, 1266–1280 (2010)
3. Sweeney, L.: K-anonymity: A model for protecting privacy. International Journal Of Uncertainty Fuzziness And Knowledge Based Systems, 557–570 (2002)
4. Gruteser, M., Grunwald, D.: Anonymous usage of location-based service through spatial and temporal cloaking. In: Proceeding of the First International Conference on Mobile Systems, Applications, and Service, pp. 31–42 (2003)
5. Gedik, B., Liu, L.: Protecting Location Privacy with Personalized k-anonymity: Architecture and Algorithms. IEEE Transactions on Mobile Computing, 1–18 (2008)
6. Tang, M., Wu, Q.H., Zhang, G.P., He, L.L., Zhang, H.G.: A New Scheme of LBS Privacy Protection. In: Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1–6 (2009)
7. Beresford, A.R., Stajano, F.: Location Privacy in Pervasive Computing. IEEE Pervasive Computing 2(1), 46–55 (2003)
8. Beresford, A.R., Stajano, F.: Mix zones: User privacy in location-aware services. In: IEEE Workshop on Pervasive Computing and Communication Security, pp. 127–131 (2004)
9. Kapadia, A., Triandopoulos, N., Cornelius, C., Peebles, D., Kotz, D.: AnonySense: Opportunistic and privacy-preserving context collection. Computer Science (2008)
10. Kido, H., Yanagisawa, Y., Satoh, T.: An anonymous communication technique using dummies for location-based service. In: Proceedings of International Conference on Pervasive Service, pp. 88–97 (2005)
11. Dong, K., Gu, T., Tao, X.P., Lu, J.: Privacy protection in participatory sensing applications requiring fine-grained locations. In: 16th International Conference on Parallel and Distributed Systems, pp. 9–16 (2010)
12. You, T.H., Peng, W.C., Lee, W.C.: Protecting moving trajectories with dummies. In: 2007 International Conference on Mobile Data Management, pp. 278–282 (2007)
13. Gao, S., Ma, J., Shi, W., Zhan, G.: Technical Report MIST-TR-2011-101 (March 2011)