International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Privacy Preserving in Participatory Sensing

Deepika Nair[1], Bhuvaneswari Raju[2]

[1]M. Tech Student, Department of CSE, Atria Institute of Technology, Bangalore, India

[2]Senior Lecturer, Department of CSE, Atria Institute of Technology, Bangalore, India

Abstract: ***The ubiquity of the various cheap embedded sensors on mobile devices, for example cameras, microphones, accelerometers, and so on, is enabling the emergence of participatory sensing applications. While participatory sensing can benefit the individuals and communities greatly, the collection and analysis of the participators' location and trajectory data may jeopardize their privacy. However, the existing proposals mostly focus on participators' location privacy, and few are done on participators' trajectory privacy. The effective analysis on trajectories that contain spatial-temporal history information will reveal participators' whereabouts and the relevant personal privacy.***

Keywords: Participatory Sensing; Mix Zones;Trajectory Privacy Preserving Framework

1. Introduction

Participatory sensing [2] is an emerging computing paradigm that enables the distributed collection of data by self-selected participants. It allows the increasing number of mobile phone users to share local knowledge acquired by their sensor-equipped devices (e.g., to monitor temperature, pollution level, or consumer pricing information). It allows individuals to identify, measure, and address problems as diverse as air pollution or the damage to fragile ecosystems using mobile phones with basic sensing and communication systems like cameras, global positioning systems (GPS), and text messaging. With the development of wireless communication technologies, such as WLAN, 3G/LTE, WiMAX, Bluetooth, Zig bee, and so on, mobile devices are equipped with a variety of embedded sensors that has powerful sensing, storage and processing capabilities which enables participatory sensing to emerge as a new and powerful technology. While research initiatives and prototypes proliferate, participatory sensing's real-world impact is often bounded to comprehensive user participation. If users have no incentive, or feel that their privacy might be endangered, it is likely that they will not participate.

1.1 Location Privacy

Location privacy [6] is a particular type of information privacy. Location privacy is defined as the ability to prevent other unauthorized parties from learning one's current or past location. Many technologies can determine the location of an individual. One of the earliest systems designed for location tracking is the Global Positioning System (GPS). This system uses satellites to help devices determine their location. The GPS works best outdoors where it has line-of-sight to the satellites and few obstructions. For commercial products, resolution to within 4m is achievable. The GPS is widely deployed and integrated, especially in map applications. Although GPS devices do not transmit, they are being increasing integrated into PDAs and other devices which do. In a successful privacy attack, some party obtains unauthorized information. Individuals intend that some information about themselves should be available to others, and that the rest remain private. The means by which the individual's preferences were circumvented is the attack vector. The main privacy concern with regards to ubiquitous computing is that many new automated attack vectors become possible. Loosely categorized, automated digital devices obtain information either through communication, observation, or inference.

1.2 Trajectory Privacy

A **trajectory** is the path that a moving object follows through space as a function of time. Participatory sensing applications mainly depend on the collection of data across wide geographic areas. The sensor data uploaded by participators are invariably tagged with the spatial-temporal information when the readings were recorded the published trajectories for decision making, for example, merchants may decide where to build a supermarket that can produce maximum profit by analyzing trajectories of customers in a certain area and the Department of Transportation can make an optimized vehicle scheduling strategy by monitoring trajectories of vehicles. However, it may introduce serious threats to participators' privacy. Adversary may possibly analyze the trajectories which contain rich spatial-temporal history information to link multiple reports from the same participators and determine certain private information such as the places where the data reports are collected. Thus, it is necessary to unlink the participators' identities from sensitive data collection locations. One of the methods to ensure trajectory privacy is Mix Zones.

2. Related Work

In the literature there exist several approaches to protect the location of a user. Most of them try to prevent disclosure of unnecessary information, explicitly or implicitly controls what information is given to whom, and when. For the purposes, this information is primarily the identity and the location of an individual. However, other properties of an individual such as interests, behavior, or communication patterns could lead to the identity and location by inference or statistical analysis. In some cases giving out information cannot be avoided. This can be a threat to personal privacy if an adversary is able to access different sources and link the retrieved data. Unwanted personal problems may be the result. To prevent this, people request that their information

be treated confidentially. For the automated world of databases and data mining, researchers developed policy schemes. These may enable adequate privacy protection, although they similarly rely on laws or goodwill of third parties.

a) ANODR

This is a routing protocol addressing the problems of route anonymity and location privacy [6]. The intention is that packets in the network cannot be traced by any observing adversary. Additionally, their routing scheme provides unlink ability. Prior to one node's ability to send a message to another, a route must be established through route discovery. This route discovery is achieved by broadcasting and forwarding packets. The sender of a message is anonymous because it is impossible to judge whether a node is actually sending a message it generated or is simply forwarding a packet as part of a route.

b) Obfuscation

Protect a user's location privacy by deliberately degrading the accuracy of his/her spatial-temporal information. Obfuscation [7] is a class of the important approaches in location privacy.

c) Mix Networks

Mix Networks [7] uses anonymizing channels to de-link reports submitted by sensors before they reach the applications. In other words, Mix Networks act as proxies to forward user reports only when some system-defined criteria are met. Mix Network may wait to receive k reports before forwarding them to the application, e.g., to guarantee k-anonymity. However, the anonymity level directly depends on the number of reports received and "mixed" by the Mix Network. They rely on statistical methods to protect privacy and do not guarantee provably-secure privacy. Moreover, there could be scenarios where a relatively long time could pass before the desired level of anonymity is reached (when "enough" reports have been collected). As a result, Mix Networks may remarkably decrease system throughput and cannot be used in settings where timely reports are required .

d) k-Anonymity

K-anonymity [9] is a wide-spread general privacy concept not restricted to location privacy. It provides the guarantee that in a set of k objects (in our case, mobile users) the target object is indistinguishable from the other k – 1 objects. Thus, the probability to identify the target user is 1/k. The idea behind k-anonymity is that a user reports an obfuscation [7] area to a client containing his position and the positions of k – 1 other users instead of his precise position that is protected by a pseudonym. As an example consider that Alice is currently located at home and queries a location-based service for the nearest cardiology clinic. Without using anonymization, this query could reveal to the client implementing the service that Alice has health problems. By using k-anonymity, Alice would be indistinguishable from at least k – 1 other users, such that the client could not link the request to Alice. Therefore, it is required that all k users of the calculated anonymization set sent to the client share the same obfuscation [7] area such that the client cannot link the issued position to the home location of Alice.

e) Mix-Zones

Pseudonym [5] is used to break the linkage between a user's identity and his/her events. The process of its change is usually performed in some pre-determined areas called mix-zones. In these networks, the infrastructure provides an anonymity service. The infrastructure delays and reorders messages from subscribers within a mix zone [4] to confuse an observer. A problem with this system is that there must be enough subscribers in the mix zone to provide an acceptable level of anonymity.

f) Dummy Locations

This method mainly employs the idea of dummy locations [2] to protect a user's location privacy. A location-dependent query is abstracted as Q = (pos; P), where parameter pos is the mobile user location and parameter P denotes user-specified predicates. We call such a query Q the original query. With the location dummy approach, the original query is typically converted into a query Q

0 = (pos1; pos2; : : : ; posk; P), where the posi include the user's real location and k - 1 dummy locations, and P is the original query predicate that applies to all k-locations. We call query Q 0 a location privacy query, since it hides the user location.

2.1 Trajectory Privacy Protection

Once a user's trajectory is identified, the user's locations are exposed. To achieve trajectory privacy [10] most immediate and simple ways are dummy trajectories [2] and suppression technique [12]. For example, to produce a user's dummy trajectories through random pattern band rotation pattern. To be specific, the former generated dummy trajectory randomly from the starting point towards the destination and the later did it by rotating the user's trajectory. However, the trajectory similarity may affect the anonymity quality. Thus, how to generate dummy trajectories [2] that look like a normal user's trajectory is one of the main challenges of this kind of work. To prevent adversary from inferring a user's unknown locations by using his/her partial trajectory knowledge. Location suppression technique [12] was proposed to convert a database of trajectories, which can prevent the disclosure of the user's whole trajectory with high probability. However, those trajectory segments that are suppressed would cause the collected data lost. Trajectory k-anonymity that extends from location k-anonymity [9] is widely used in trajectory privacy protection. .

a) Dummy trajectory confusion

Protecting trajectory privacy in a data publication perspective is done with a simple dummy trajectories [11] confusion method, this method propose to generate dummy trajectories in order to confuse the adversaries. In order to confound fake trajectories and the true ones, dummy

trajectories are generated under two principles: first, the movement patterns of dummies should be similar to real users; second, the intersections of trajectories should be as more as possible. Based on these rules, dummy trajectories are generated by rotating real users' trajectories.

b)Suppression-based method

It is based on the assumption that different adversaries may have different and disjoint part of users' trajectories. Suppression-based method [12] reduces the probability of disclosing the whole trajectories. Trajectory pieces should be suppressed, publication of these pieces may increase the whole trajectory's breach probability above a certain threshold.

c) Trajectory k-anonymity

In this method first, trajectories are clustered based on log cost metric, then each sample location on trajectories is generalized to a region containing at least k moving objects. Then trajectories are reconstructed through randomly selecting sample points from the anonymized region [12].

3. Proprosed Work

A trajectory privacy-preserving framework, for participatory sensing the proposed system helps to prevent linking of participators' identities with their uploaded data reports .The proposed method protects participators' identities and trajectories privacy from the perspective of graph theory based on mix-zones model and pseudonym technique. The locations on or nearby participators' trajectories may not all be sensitive, and with this thought, proposed system only deals with the sensitive trajectory segments. Here the theoretical mix-zones model is improved to construct trajectory mix-zones model for protecting sensitive trajectory segments from the perspective of graph theory. Compared with existing trajectory privacy-preserving proposals, the proposed method has advantages of lower costs and lower information loss while the privacy level would not decrease.

3.1 Trajectory Privacy Preserving Framework

TRPF anonymizes the sensitive trajectory segment from the perspective of graph theory. To reduce information loss and costs at a certain privacy-preserving level, the whole area should be divided into several parts. According to the sensitive locations on or nearby the trajectories, the whole trajectories need to be divided into sensitive trajectory segments and no sensitive trajectory segments. TRF identifies and protects sensitive trajectory segments based on mix-zones model and pseudonym technique.

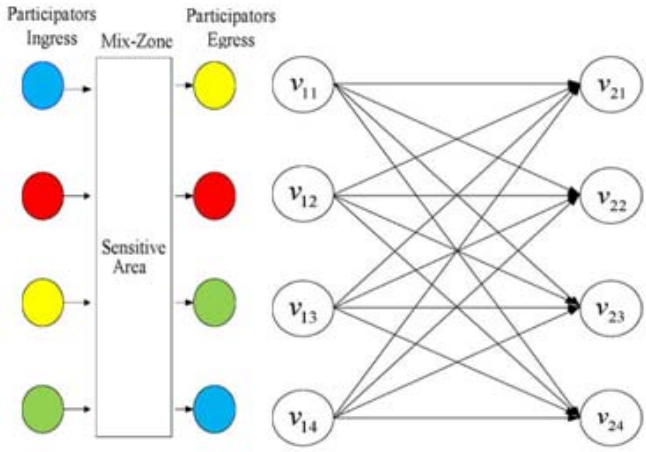

Figure 1: Mix Zone Graph Model

Any data collector who enters the Sensitive Area should select a pseudonym provided by TTPs to anonymize the link ability between his identity and his collected data reports. Meanwhile, they record their ingress and egress time. A participator's information we describe as a tuple which consists of the participator's pseudonym provided by TTPs, mapping from participator's identity to his pseudonym, sensitive area the participator passes by, participators' enter time and participator's egress time interval. Trajectory Mix-zones is modeled as Directed Weighted Graph (DWG), which is formalized as the set of vertexes which are constructed by the pseudonyms provided by TTPs. It can be depicted as the set of edges that represent the participators' trajectory mapping from the ingress to the egress in the sensitive area. DWG is a complete bipartite graph with different weights on each edge. As a result of pseudonym technique, there may be some difficulties for adversary to link the ingress and egress participator with the same identity.

The time of participators stays in mix zones can either be constant or vary, if the residence time was constant, it would encounter First in First out (FIFO) attack, that is, the first exit participator corresponds to the first one that enters the mix-zones and the pseudonym technique takes no effect. In order to prevent FIFO attack TRPF allows the time of participator's stay in mixzones to be random. Since the time interval of data collection in sensitive area is random, even though adversary obtains the related information such as ingress and egress order and time, it cannot link the ingress pseudonym to egress pseudonym. A participator vi enters the mix-zones at time tingress (vi) and exits the mix-zones in a time interval from tj to tj+1. Let P (vi,t) present the probability of participator vi exits the mix-zones in time interval [tj, tj+1].

4. Conclusion

The disclosure of data collectors' trajectories poses serious threats to participators' personal privacy. It may prevent participators from data sharing. This project, proposes a trajectory privacy-preserving framework TrPF for participatory sensing and a trajectory mix-zones graph model to protect participators' trajectories from the perspective of graph theory. . It may be more realistic in practice. In the future, the paper can be extended to work on

the semantic trajectory privacy problems of multiple mix-zones in detail.

References

[1] TrPF: A Trajectory Privacy-Preserving Framework for Participatory Sensing Sheng Gao, Jianfeng Ma, Weisong Shi, Senior Member, IEEE, Guoxing Zhan, and Cong Sun
[2] PAD: Privacy-Area Aware, Dummy-Based Location Privacy in Mobile Services Hua Lu Christian S. Jensen Man Lung Yiu Department of Computer Science, Aalborg University, Denmark {luhua, csj, mly}@cs.aau.dk
[3] Participatory Sensing: Applications and Architecture Deborah EstrinUniversity of California, Los Angeles
[4] Effective Mix-zone Anonymization Techniques for Mobile Travelers BalajiPalanisamy and Ling Liu
[5] J. Freudiger, M. H. Manshaei, J. Y. Le Boudec, and J. P. Hubaux, "On the age of pseudonyms in mobile ad hoc networks," in Proc. IEEE INFOCOM, 2010, pp. 1–9.
[6] Survey on Location Privacy in Pervasive Computing Andreas orlach, Andreas Heinemann, and Wesley W. Terpstra Darmstadt University of Technology (TUD), Department of Computer Science, D-64283 Darmstadt, Germany, fgoerlach,terpstrag@ito.tu-darmstadt.de, aheine@gkec.tu-darmstadt.de
[7] M. Duckham and L. Kulik, "A formalmodel of obfuscation and negotiation for location privacy," in Proc. 3rd Int. Conf. Pervasive Computing (PERVASIVE'05), 2005, pp. 152–170.
[8] Juels, R. L. Rivest, and M. Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In V. Atluri, ed. 8th ACM Conference on Computer and Communications Security, pages 103{111. ACM Press, 2003.
[9] Gruteser, M., Grunwald, D.: Anonymous usage of location-based services through spatial and temporal cloaking. In: Proceedings of the 1st international conference on Mobile systems, applications and services (MobiSys '03), New York, NY, USA, ACM (2003) 31–42
[10] Z. Huo, X. Meng, H. Hu, and Y. Huang, "You can walk alone Trajectory privacy-preserving through significant stays protection," in Proc. 17th Int. Conf. Database Systems for Advanced Applications (DASFAA2012), 2012, pp. 351–366.
[11] T. H.You, W. C. Peng, and W. C. Lee.Protecting moving trajectories with dummies. In Proc. MDM 2007, pages 278–282, 2007.
[12] M. Terrovitis and N. Mamoulis.Privacy preserving in the publication of trajectories. In Proc. MDM 2008, pages 65–72, 2008.
[13] O. Abul, F. Bonchi, and M. Nanni. Never walk alone: uncertainty for anonymity in moving objects databases. In Proc. ICDE 2008, pages 376–385, 2008.
[14] TrPF: A Trajectory Privacy-Preserving Framework for Participatory Sensing Sheng Gao, Jianfeng Ma, Weisong Shi, Senior Member, IEEE, Guoxing Zhan, and Cong Sun
[15] PAD: Privacy-Area Aware, Dummy-Based Location Privacy in Mobile Services Hua Lu Christian S. Jensen Man Lung Yiu Department of Computer Science, Aalborg University, Denmark {luhua, csj, mly}@cs.aau.dk
[16] Participatory Sensing: Applications and Architecture Deborah EstrinUniversity of California, Los Angeles
[17] Effective Mix-zone Anonymization Techniques for Mobile Travelers BalajiPalanisamy and Ling Liu
[18] J. Freudiger, M. H. Manshaei, J. Y. Le Boudec, and J. P. Hubaux, "On the age of pseudonyms in mobile ad hoc networks," in Proc. IEEE INFOCOM, 2010, pp. 1–9.
[19] Survey on Location Privacy in Pervasive Computing Andreas orlach, Andreas Heinemann, and Wesley W. Terpstra Darmstadt University of Technology (TUD), Department of Computer Science, D-64283 Darmstadt, Germany, fgoerlach,terpstrag@ito.tu-darmstadt.de, aheine@gkec.tu-darmstadt.de 7. M. Duckham and L. Kulik, "A formalmodel of obfuscation and negotiation for location privacy," in Proc. 3rd Int. Conf. Pervasive Computing (PERVASIVE'05), 2005, pp. 152–170.
[20] Juels, R. L. Rivest, and M. Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In V. Atluri, ed. 8th ACM Conference on Computer and Communications Security, pages 103{111. ACM Press, 2003.
[21] 9.Gruteser, M., Grunwald, D.: Anonymous usage of location-based services through spatial and temporal cloaking. In: Proceedings of the 1st international conference on Mobile systems, applications and services (MobiSys '03), New York, NY, USA, ACM (2003) 31–42
[22] Z. Huo, X. Meng, H. Hu, and Y. Huang, "You can walk alone Trajectory privacy-preserving through significant stays protection," in Proc. 17th Int. Conf. Database Systems for Advanced Applications (DASFAA2012), 2012, pp. 351–366.
[23] T. H.You, W. C. Peng, and W. C. Lee.Protecting moving trajectories with dummies. In Proc. MDM 2007, pages 278–282, 2007.
[24] M. Terrovitis and N. Mamoulis.Privacy preserving in the publication of trajectories. In Proc. MDM 2008, pages 65–72, 2008.
[25] 13. O. Abul, F. Bonchi, and M. Nanni. Never walk alone: uncertainty for anonymity in moving objects databases. In Proc. ICDE 2008, pages 376–385, 2008.14.
[26] http://en.wikipedia.org/wiki/Wireless_sensor_network

Author Profile

Deepika Nair received the BE degree in Information Science from Visvesvaraya Technological University, India .She is currently working toward M. Tech degree at Atria Institute of Technology, Visvesvaraya Technological University. Her current research interests include mobile computing, participatory sensing, and cloud computing with focus on security and privacy issues.