ISSN: 2321-7782 (Online)
Volume 2, Issue 11, November 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

An Approach for Privacy Preservation of Semantic Trajectories for Participatory Sensing Systems

Gauri R Virkar[1]
Computer Science and Engineering
BSIOER, Wagholi
Pune, Maharashtra – India

Sanchika A Bajpai[2]
Computer Science and Engineering
BSIOER, Wagholi
Pune, Maharashtra – India

Abstract: ***With the advancement of technology in fields of wireless communication, different mobile communicating devices equipped with variety of embedded sensors and powerful sensing have been emerged. Participatory sensing is the process that enables individuals to collect, analyze and share local knowledge with their own mobile devices. Although the use of participatory sensing offers numerous benefits on deployment costs, availability, spatial- temporal coverage, energy consumption and so forth, it has certain threats which may be compromise the participator's location and trajectory data. Henceforth, to ensure the participators' privacy is the most urgent task. The existing proposals emphasized more on participators' location privacy and very few of them consider about participators' trajectory privacy. In this paper, a semantic trajectory privacy-preserving framework for participatory sensing applications has been proposed. Based on the proposed framework, the theoretical mix zones model are been improved by considering time factor from the viewpoint of the graph theory.***

Keywords: Participatory Sensing, Location Privacy, Trajectories, Mix zones, Semantic Trajectories.

I. INTRODUCTION

With the growth of mobile phones, along with their pervasive connectivity, offers large volume of digital information to be generated as well as processed daily. This has driven analysts and IT experts to discuss about and develop a novel sensing ideal model, where sensors are not sent in particular areas, however are carried by individuals. Subsequently, information gathered by sensor-equipped devices becomes of extreme interest to different clients and applications. For example mobile phones may report actual (continuously) temperature or sound level; likewise, vehicles may notify about traffic conditions. This paradigm is known to as Participatory Sensing (PS) – sometimes also referred to as *opportunistic* or *urban* sensing[1] . The main idea behind participatory sensing is to encourage the ordinary citizens to collect as well as share the sensed information from their surrounding environment using their mobile phones. This trend has already been observed in a variety of software domains such as transportation systems including MetroSense[2] where by multiple users share their own local traffic observations in order to determine the traffic acitivites such as congestion detection. Similar examples include CarTel [3], Bikenet[4], PEIR[5] and so on.

Almost all participatory sensing systems collect sensor readings related to the participants and/or their own environments. Certainly, the actual collected information may be used to extract or derive private information about the user's "private life, routines, act and relations". At the same time, contributed sensor information is generally important to any of the participatory sensing system and their deficiency endangers the success of participatory sensing systems. Therefore the need is to raise the user awareness of the effects of the disclosure of sensor data as well as provide solutions to preserve the user privacy in order to ensure the actual strength of the strategy and prevent participants from opting out.

In a typical participatory sensing system mobile users sense and accumulate the data through sensing devices embedded on the phones. The vast amount of trajectory data gets collected and progressively increases as the tracking time goes by. For example, a taxi-tracking system collects 7.2 millions GPS positions each day. Motivating individuals to be involved in community-based data sensing as well as collection has essential benefits with regards to enhancing the quality of the systems. The focus on movement data is been increasing day by day. In particular, a new promising approach has been devised to provide applications with richer and more meaningful knowledge about movement. This is achieved by combining the raw mobility tracks (e.g. the GPS records) with related contextual data. These enriched track records are referred to as ***semantic trajectories***. However, one important challenge in these settings is how to preserve the user privacy when sharing participatory data, and focus here is specifically on the participatory data that contain locations that a user has visited and his trajectories. If users has no motivation, or believe that their privacy might be endangered, it is likely that they will not be involved. Considering , this paper proposes an approach, STrPF, to provide user privacy to the semantic trajectories for participatory sensing applications.

A. Location Privacy

Location privacy is defined as the ability to prevent other unauthorized parties from learning one's current or past location. Traditionally, privacy of personal location information has not been a critical issue but, with the advancement of location tracking systems capable of following user movement twenty-four hours a day and seven days a week, location privacy becomes crucial: records of everything from the particular rack a person visit in the library to the clinics a person visit in a hospital can represent a very invasive list of data. Numerous systems could figure out the location of person. One of several original systems designed for position following could be the Global Positioning System (GPS). This technique makes use of satellites to aid devices figure out their own position. Generally, automated digital devices obtain information either through communication, observation, or inference.

B. Trajectory Privacy

A trajectory is the path that a moving object follows through space as a function of time. Example of trajectories could be monitoring of wild animals, birds, people, a soccer player, etc. Trajectories may be uni-dimensional or perhaps multi-dimensional. Participatory sensing systems primarily depend on the collection of information across large geographic areas. The sensor data uploaded by participators are usually tagged with the spatial-temporal information when the readings were recorded the published trajectories for decision making. For example, merchants may possibly decide where to build a food store that could produce maximum gain by analyzing trajectories associated with consumers in a selected spot and also the Department of Transportation can make an optimized vehicle scheduling strategy by monitoring the trajectories connected with motor vehicles. However, it will add considerable threats to the participators' privacy. Adversary may perhaps examine the particular trajectories which contain abundant spatial-temporal background information to be able to link numerous reports that are collected. Hence, it is crucial to be able to unlink the particular participators' identities from sensitive data collection locations.

C. Semantic Trajectory Privacy

Recently a new trajectory concept has been introduced in for reasoning over trajectories from a semantic point of view, the *semantic trajectory*, based on the notion of stops and moves. Stops are the important parts of a trajectory where the moving object has stayed for a minimal amount of time. Moves are the sub-trajectories describing the movements between two consecutive stops. Based on the concept of stops and moves the user can enrich trajectories with semantic information according to the application domain. Semantic trajectory is a temporally ordered sequence of important places that the moving object has visited. In semantic trajectories each location of stop can be attached to some contextual information such as the visited place or the purpose - either by explicit sensing or by inference. An example of semantic trajectory is the sequence of places visited by a moving individual such as home, work, shopping center, gym, etc as shown in Fig 1. The new form of data of semantic trajectories poses important privacy threats. The main problem introduced by this form of data is that, from the fact that a person

has stopped in a certain sensitive location (e.g., an cardiology clinic), an attacker can infer private personal information (that person's health status, in the example). So the need is to preserve privacy of semantic trajectories for the participatory sensing applications.

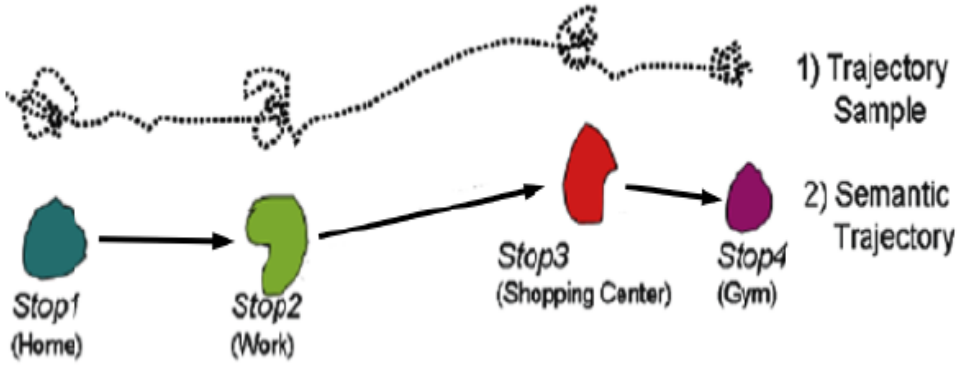

Fig. 1. Example of Trajectory Sample and Semantic Trajectory.

II. Related Work

In the literature there exist several approaches to protect the particular position of the user. The vast majority of them attempt to prevent disclosure of unnecessary data, explicitly or implicitly controls what information is actually given to whom, and when.

For that reason, this information is mainly the identity as well as the location of an individual. For that reasons, different properties of an individual, for example, investments, conduct, or correspondence examples could prompt the identity and location information by inference or statistical analysis. Sometimes giving out information cannot be prevented. This can be a risk to individual protection if an adversary has the capacity to access distinctive sources and link the retrieved information. Undesirable individual issues may be the result. To avoid this, individuals ask for that their data be dealt with confidentially. For the automated world of databases and data mining, analysts created various policy plans. These may empower satisfactory protection insurance, in spite of the fact that they likewise depend on laws or goodwill of outsiders. 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 next parties.

A. Location Privacy Protection

There are several works that analyze the location privacy-preserving schemes. They can be classified into the following aspects.

a. Obfuscation

It is defined as the means of intentionally degrading the quality of information about an individual's location in order to protect that individual's location[6].

b. Mix Networks

Mix Networks [6] 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. In addition, there could be situations where a moderately long time could pass before the desired level of anonymity is arrived at (when "enough" reports have been

gathered). Accordingly, Mix Networks might strikingly diminish framework throughput and can't be utilized as a part of settings where regular reports are needed.

c. K-Anonymity

k-anonymity is a wide-spread general privacy concept not limited to location privacy. It gives the assurance that in a set of k objects (in these case, mobile users) the target object is indistinguishable from the other k – 1 object. Subsequently, the likelihood to distinguish the target user is 1/k. The thought behind k-anonymity is that a user reports a obfuscation region to a customer containing his position and the positions of k – 1 different customers rather than his exact position that is secured by a pseudonym. As an example consider that Alice is currently at home and queries a location based service for the nearest cardiology facility. Without utilizing anonymization, this inquiry could reveal to the customer implementing the service that Alice has health issues. By utilizing k-anonymity, Alice would be indistinguishable from atleast k – 1 different customer, such that the customer couldn't link the actual request to Alice. As a result, it is necessary that all k customers of the calculated anonymization set sent to the customer have the same obfuscation [6] region such that the customer can't connect the issued position to the home location of Alice.

d. Mix-Zones

Pseudonym is used to break the actual linkage between the user's identity with his/her events. This task is normally performed in most pre-determined areas known as mixzones. The task of the modify is normally performed in most pre-determined areas known as mixzones. Throughout these cpa networks, the facilities offers an anonymity services. Your facilities delays and also reorders messages via customers in a combination region to be able to confound an viewer. A difficulty with this particular method is actually of which there must be adequate customers from mix zone to offer a acceptable level of anonymity.

e. Dummy Locations

This process mostly employsthe idea of dummy locations[7] to protect the user's location privacy. A location-dependent issue is actually abstracted as Q = (pos; P), where parameter pos is actually the mobile user location and also parameter P denotes the user specified predicates. We call such a query Q the original query. While using the location dummy strategy, the original problem is typically converted into a query Q0 = (pos1; pos2;:::; posk; P), where the pos1 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 Q0 a location privacy query, since it hides the user location.

B. Trajectory Privacy Protection

To prevent adversary from inferring a user's unknown locations by using his/her partial trajectory knowledge. Location suppression technique was proposed to convert a database of trajectories, which can prevent the disclosure of the user's whole trajectory with high probability. However, once the user's trajectory is actually determined, the user's locations are usually exposed. To accomplish trajectory privacy most instant and easy means are usually dummy trajectories and also suppression technique. One example is, to produce a user's dummy trajectories as a result of random pattern and rotation pattern. To be precise, the random pattern generated dummy trajectory randomly from the starting point towards the destination and the later did it by rotating the user's trajectory. Nevertheless, the trajectory similarity may well impact the anonymity quality. Hence, the best way to produce dummy trajectories which seem similar to normal user's trajectory is among the major issues of such work.

a. Dummy Trajectory Obfuscation

Protecting trajectory privacy from a data publication viewpoint is performed with simple dummy trajectories obfuscation approach. This approach proposes to generate dummy trajectories so that you can confuse the adversaries. In order to confuse fake trajectories as well as the true ones, dummy trajectories are usually generated under two rules: first, the movement patterns

of dummy trajectory needs to be similar to end users; second, the intersections of trajectories needs to be as more as possible. According to these rules, dummy trajectories are usually generated by rotating true users' trajectories.

b. Suppression-Based Method

It is based on the assumption that various adversaries may have diverse and disjoint part of users' trajectories. Suppression-based method decreases the probability of exposing the whole trajectories. Trajectory pieces should be suppressed, publication of these pieces may raise the whole trajectory's breach probability over a particular threshold.

c. Trajectory K-Anonymity

In this approach 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 by arbitarily choosing sample points from the anonymized region.

C. Semantic Trajectory Privacy Protection

A framework, C-safety [8], proposes that when a dataset of semantic trajectories is actually provided, an anonymous semantic trajectory dataset is actually generated. This new dataset helps to ensure that it is not possible to be to infer the identity of any individual as well as the visited sensitive locations which has a probability greater than a fixed threshold, fixed by the data owner.

III. Overview of the STRPF System

In this part, first the semantic trajectory privacy preserving framework, STrPF, for participatory sensing applications is depicted and then the privacy problem related to users' trajectories are focused.

A. The Architecture Of Strpf For Participatory Sensing Applications :-

Mix Network functions as an anonymzing intermediary between Mobile Nodes and the Report Server that is extensively utilized [9], [10]. Consider [11] for example, it routes reports using multi-hop transmission, adding delays and mixing with the data from different sources to different destinations. Such process makes an adversary to neither link a mobile node's reports together nor identify which mobile node dispatched the report, or discover when and where the locations were reported. Based on [11], a semantic trajectory privacy preserving framework STrPF for participatory sensing scheme is proposed as depicted as Fig.2. Contrasted with the preceding architecture, the component of participators' privacy is considered and the mix network with a Trusted Third Party Server component is subsituted. Due to the exemption of mix network, it will optimize the data reports transmission. The addition of Trusted Third Party Server can function as a privacy-preserving agent, which can trade off the performance of data transmission and privacy protection. It can minimize the network hops of data reports transmission path through wireless networks. Based on various features of function characteristics, the primary constituents of STrPF are made up of the following entities.

a. Data Collectors:

Mobile Nodes are devices having capability to sense, compute, store and communicate wirelessly. They work as the data collectors in participatory sensing system. They can be utilised for capturing context-aware information and can be carried along easily with each participator. The involvement of data collectors in this sensing paradigm is voluntary. Any participator which desire to provide application server with shared data needs to obtain a certificate from Trusted Third Party Server. To prevent adversary from disguising as a legal participator to upload malicious data, only the one who has been validated can access the participatory sensing system and upload his/her collected data reports. We formalize the data reports collected by participator Pi as: Ri = <IDpi, Data, Location, Time>, where IDpi denotes identity of participator Pi, Location and Time refers to spatial- temporal information added with the collected data which compose trajectories of data collectors.

b. Trusted Third Party Server (Ttps):

TTPs are mainly responsible for storing participators' relevant information such as certificates and pseudonyms information in order to ensure the system security and participators' privacy. Certificates are used for verifying participators' validity in order to prevent malicious attacker from masquerading. The disclosure of the spatial-temporal information may also endanger the participators' privacy. The linkage between the participators' spatial-temporal information and their identities are removed based on pseudonym technique.

c. Report Server:

Report Server is responsible for handing with two main aspects: (a) Communicate with TTPs to verify the validity of the participators' identities by the certificates contained in the data reports; (b) Simplify the uploaded data reports and then send the data reports to Application Server.

d. Application Server:

Application Server acts as a data center. It can provide different types of data services for end users and play the following roles: (a) Data Storage: It is used to store the processed data reports received from data report server; (b) Data Sharing: Any legitimate end user can access the available data services; (c) Data Publish: publish the data reports for the end users to query. However, in this system architecture, Application Server may be untrustworthy. It may leak participators' sensitive information to adversary. For example, the disclosure of participators' trajectories may indicate where the data reports are collected. Maybe some of the locations such as home address are sensitive. Adversary can use the published trajectories to link participators' data reports with sensitive locations. As a result, the participators are aware that their privacy might be invaded seriously so that they may not want to share their collected data reports with end users.

e. Queriers:

Queriers are end users that request sensor reports in a given participatory sensing application. They can be personal users or community users. They access and check if the data is gathered by the data collectors according to their requirements. The queriers include, for example, data collectors are intending to consult their own collected data, doctors checking their patients' records, environmentalists querying the climate data of a certain area or the general public for other purposes. Note that only the registered end users can access the shared data reports. End users request certificate authentication requests to TTPs. Only the registered end users can get the access authorization and only the legitimate end users can access the shared data reports that are provided by data collectors.

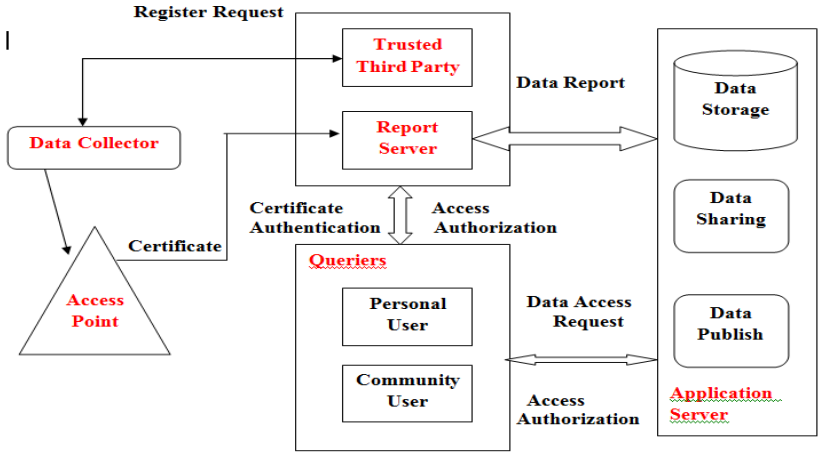

FIG.2. SYSTEM ARCHITECTURE

B. Problem Statement

The participatory sensing applications allows individual to sense, collect, share and analyze their locations using their own mobile devices. The user data is collected in the form of spatial temporal data i.e (x,y,t) where x,y are the coordinates of the user location and t is time at which the sensor information is sent. Such a kind of data is called as raw movement data or a movement track. A trajectory can built using this raw movement tracks. Such a trajectory is known as **raw trajectory**. The query like "Return cars which stopped at (x, y) at time t" can be answered with this knowledge. Raw movement tracks may be used as such for further analysis or be transformed into other kinds of representation of movement. Simply, additional information or semantics are added to this raw trajectory. This leads to the development of semantic trajectories. A **semantic trajectory** is a relatively recent paradigm aiming to provide applications with knowledge about the movement of entities. For example, the query such as query is "Return number of cars which stopped during working days last week at a gas station owned by one of our customers" can be answered using semantic trajectories.

An adversary can infer the user identity and/or location identity of the user from these trajectories. A prominent attack called as Trajectory Inference attack could occur since the location and user identification information can be inferred an adversary. For instance, assume an adversary adapts through background knowledge that the data collector Pi has visited a particular location at a certain time ti, while the location happens to be some sample on Pi's trajectory at time ti in the data reports. The adversary would combine this data to gather the entire trajectory of Pi, which may relate to certain sensitive attribute.

Furthermore, the analysis of trajectories over several data reports may help adversary to take advantage of the frequently visited areas and disclose the participators' identities, e.g., a data collector typically invests the same time on arriving at a specific location from an altered location consistently in the morning. Adversary can utilize the continuous data to infer the starting location in the morning which may be his/her home and the location reached after the time may be the work place. Therefore, the participators' protection would suffer an enormous danger with the disclosure of sensitive information.

In short, this paper proposes an approach, STrPF, to provide user identity and location privacy to the semantic trajectories for participatory sensing applications. To prevent from linking participators' identities with their uploaded data reports, a approach to protect participators' identities and trajectories privacy from the perspective of graph theory based on mix-zones model and pseudonym technique is proposed. Actually, just parts of the locations on or close-by their trajectories are sensitive. On this basis, only the sensitive parts of participators' trajectories in their collected data reports needs to be protected.

IV. Trajectory Mix-Zones Graph Model

In trajectory mix-zones graph model, sensitive trajectory segments are anonymized from the perspective of graph model. To decrease information loss and costs at a certain privacy-preserving level, the whole area is divided into several parts. Based on the sensitive locations on or close by the trajectories, the whole trajectories are split up into sensitive trajectory segments and non-sensitive trajectory segments. Only sensitive trajectory segments are protected based on mix-zones model and pseudonym technique. Any Data Collector who goes into the Sensitive area should choose a pseudonym provided by TTPs to anonymize the linkability between his identity and his collected data reports. Meantime, they record their ingress and egress time. A participator's information is recorded as a tuple:

Ii = (IDp,Ri, Si,tingress, Δtegress), where IDp represents the participator 's pseudonym supplied by TTPs, Ri is the mapping from participator's identity to his pseudonym, Si is the sensitive area the participator passes by ,tingress presents the set of participators' arrival time and Δtegress is the participator's egress time interval.

A. Trajectory Graph Construction

To suggest, the Trajectory Mix-zones as Directed Weighted Graph (DWG), which is formalized as G = {V,E} .V is the set of vertexes which are made up of pseudonyms supplied by TTPs. A participator enters into the sensitive area with a pseudonym and leaves it with another pseudonym. It can be depicted as V = {(v11,v12,….v1n),(v21,v22,….v2n)}. E is the set of edges that represent the participators' trajectory mapping from the ingress to the egress in the sensitive area. As a result of pseudonym method, there may be some difficulties for adversary to connect the ingress and egress participator with the same identity.

In detail, DWG is an entire bipartite graph with unique weights on each edge. The time for which participators resides in mix-zones can either be constant or varying. Palanisamy*et al*. [12] analyzed the two distinct situations in road networks. They pointed out that if the residence time was constant, it would meet with First In First out (FIFO) attack. That is to state, the first exit participator corresponds to the first one that goes into the mix-zones and the pseudonym method takes no effect. In STrPF, it is assumed that the arrival of participators at the trajectory mix-zones follow a Poisson process. Given a time interval T, k participators enter in the trajectory mix-zones with mean appearance rate λ to accomplish k-anonymity. Note that the time interval and the arrival rate decide the number of participators that enter into the trajectory mix-zones. Additionally, the participators' arrival should not differ by a large number, or adversary could infer the first exit might correspond to the first enter. The time the data collectors that spend in mix-zones is random. The participators arrive and remain in sensitive area with random time interval. Even if adversary observes the time information, they cannot identify the pseudonyms mapping. Each edge weight represents the mapping probability between an ingress pseudonym and egress pseudonym.

B. Weight Construction Algorithm

The *WeightConstruct* algorithm is used compute the weight of each edge. A participator vi goes into 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) denotes the probability that the participator exits the mix-zones in the time gap [tj,tj+1]. P(vi,t) is numerically equal to the probability that participator vi takes data collection time in mix-zones from tj – tingress(vi) to tj+1 – tingress(vi) . The data collection time in mix-zones Δ'(t) pursues normal distributions Δ'(t) □ N(μ,σ). Similarly, the other participators exit in the time interval[tj,tj+1] can be computed. Thus, the probability of all participators exit in the interval time can be computed by

$$P(v',t) = \sum_{i=1}^{k} P(vi,t) \qquad (1)$$

However, only one of them is the legitimate participator. Therefore, the probability that participator vi exits in [tj, tj+1] is vi , denoted as P (vi[tj, tj+1]) is granted by the following conditional probability

$$P(Vi[tj, tj+1]) = \frac{P(vi,t)}{P(v',t)} \quad ,i = 1,2,\dots,k \qquad (2)$$

Each participator enters with one of the k pseudonyms and exits the sensitive area with a different one after he/she finishes the data collection.

V. Conclusion

Disclosure of personal data collector's trajectories introduces serious threats to participator's privacy. This may restrict the participator from sharing their data. In this paper, a semantic trajectory privacy preserving framework, STrPF, has been proposed for participatory sensing applications in order to preserve the location and user identities of the participants. Then, a trajectory mix-zones graph model to protect participators' trajectories from the perspective of graph theory is been proposed. Here, the time factor is taken into consideration in order to improve the mix-zones model.

References

1. T. Campbell, S. B. Eisenman, N. D. Lane, E. Miluzzo, and R. A.Peterson, "People-centric urban sensing," in Proc. 2nd Ann. Int. Workshopon Wireless Internet, 2006, p. 18, ACM.
2. S. Eisenman, N. Lane, E. Miluzzo, R. Peterson, G. Ahn, and A. Campbell, "MetroSense Project:People-centric Sensing at Scale," in Proceedings of the 1stWorkshop onWorld-Sensor-Web (WSW), 2006, pp. 6–11.
3. B. Hull, V. Bychkovsky, Y. Zhang, K. Chen, M. Goraczko, A. Miu, E. Shih, H. Balakrishnan, and S. Madden, "CarTel: A Distributed Mobile Sensor Computing System," in Proceedings of the 4th ACM International Conference on Embedded Networked Sensor Systems (SenSys), 2006, pp. 125–138.
4. S. Eisenman, E. Miluzzo, N. Lane, R. Peterson, G. Ahn, and A. Campbell, "BikeNet: A Mobile Sensing System for Cyclist Experience Mapping," ACM Transactions on Sensor Networks, vol. 6,no. 1, pp. 1–39, 2009.
5. M. Mun, S. Reddy, K. Shilton, N. Yau, J. Burke, D. Estrin,M. Hansen,E.Howard, R.West, andP. Boda, "Peir, the personal environmental impact report, as a platform for participatory sensing systems research," in Proc. 7th Int. Conf. Mobile Systems, Applications, and Services, 2009, pp. 55–68, ACM.
6. M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in Proc. 3rd Int. Conf. Pervasive Computing (PERVASIVE'05), 2005, pp. 152–170.
7. H. Lu, C. S. Jensen, andM. L. Yiu, "Pad: Privacy-area aware, dummy based location privacy in mobile services," in Proc. 7th ACM Int.Workshop on Data Engineering for Wireless and Mobile Access, 2008, pp. 16–23, ACM.
8. A. Monreale, R. Trasarti, D. Pedreschi, C. Renso, and V. Bogorny, "C-safety: A framework for the anonymization of semantic trajectories," Trans. Data Privacy, vol. 4, no. 2, pp. 73–101, 2011.
9. K. L. Huang, S. S. Kanhere, and W. Hu, "Preserving privacy in participatory sensing systems," Comput. Commun., vol. 33, no. 11, pp. 1266–1280, 2010.
10. A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz, "Anonysense: Opportunistic and privacy-preserving context collection," Pervasive Comput., vol. 5013, pp. 280–297, 2008.
11. C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "Anonysense: Privacy-aware people-centric sensing," in Proc. ACM 6th Int. Conf. Mobile Systems, Applications, and Services, 2008, pp. 211–224.
12. B. Palanisamy and L. Liu, "Mobimix: Protecting location privacy with mix-zones over road networks," in Proc. IEEE 27th Int. Conf. Data Engineering (ICDE), 2011, pp. 494–505.

