Participant Privacy in Mobile Crowd Sensing Task Management: A Survey of Methods and Challenges

Layla Pournajaf, Daniel A. Garcia-Ulloa, Li Xiong, Vaidy Sunderam
Math&CS Department
Emory University, Atlanta, GA
{lpourna, dgarci8, lxiong, vss}@emory.edu

ABSTRACT

Mobile crowd sensing enables a broad range of novel applications by leveraging mobile devices and smartphone users worldwide. While this paradigm is immensely useful, it involves the collection of detailed information from sensors and their carriers (i.e. participants) during task management processes including participant recruitment and task distribution. Such information might compromise participant privacy in various regards by identification or disclosure of sensitive attributes – thereby increasing vulnerability and subsequently reducing participation. In this survey, we identify different task management approaches in mobile crowd sensing, and assess the threats to participant privacy when personal information is disclosed. We also outline how privacy mechanisms are utilized in existing sensing applications to protect the participants against these threats. Finally, we discuss continuing challenges facing participant privacy-preserving approaches during task management.

1. INTRODUCTION

The recent increase in the use of smart phones and other mobile devices has created the opportunity to collectively sense and share information for common good. *Mobile crowd sensing* (MCS) refers to the wide variety of sensing models in which individuals with sensing and computing devices are able to collect and contribute valuable data for different applications [30]. MCS is also closely related to location-aware crowdsourcing [38, 2, 48] in which jobs are distributed to workers with regard to their locations. Examples of such applications are crowd-contributed instant news coverage, finding parking spots, monitoring traffic, and crime mapping. In MCS, a *participant* or *carrier* is an individual who collects and contributes data using a sensing device (e.g. a smart phone) that she carries. Collected data is consumed by *end users* directly or after processing by some applications.[1] Mobile crowd sensing can be categorized based on the involvement of participants in sensing actions as *participatory* or *opportunistic*. In a participatory sensing, participants agree to fulfill the requested sensing activities, and are thus explicitly involved in the sensing action (e.g. taking a picture or entering data). In an opportunistic sensing, data is collected by the device with minimum or no involvement of the participants (e.g. reporting speed while driving). Opportunistic sensing could run as a background process, so collecting data requires no interaction with the individuals carrying the sensing devices. From a different point of view, MCS can also be categorized based on the data collection target into *social sensing* and *environmental sensing*. In social sensing applications, a participant collects data about herself (e.g. her vital signs, sport activities) or social interactions (e.g. traffic patterns, parking spots) while in environmental sensing, she monitors certain aspects of the environment (e.g. air pollution, potholes).

To facilitate or coordinate the interaction between applications and participants,[2] a *task management* paradigm is needed to define tasks based on the application requirements, recruit qualified participants, distribute tasks, and possibly coordinate with participants until task completion. One of the major challenges in task management is to ensure a certain degree of privacy for participants. Such an assurance of privacy would increase the disposition of the participants to engage in MCS activity, receive tasks and contribute data, and would ultimately lead to more effective applications.

In this paper, we discuss participant privacy concerns and solutions in the context of task management in mobile crowd sensing. Previous surveys on privacy in participatory sensing applications [17, 16] mainly consider privacy issues related to data col-

[1] In this paper, we use the terms end user and application interchangeably

[2] In this paper we refer to these individuals as participants regardless of the sensing model (participatory or opportunistic)

lection and briefly mention anonymous task distribution, while our main focus is participant privacy during task management. To our knowledge, this is the first survey dedicated to participant privacy issues of task management in MCS. Our main contributions can be summarized as follows:

1. We present a detailed classification of task management in mobile crowd sensing covering all aspects of tasks and distribution methods.
2. We identify the categories of privacy threats to participants of MCS and provide a detailed classification of privacy mechanisms for each type of threat.
3. We discuss ongoing research directions and further challenges in the area of participant privacy in MCS task management.

The rest of this paper is organized as follows. In Section 2 we review and categorize task management models in MCS. We then investigate privacy threats in different tasking schemes in Section 3 followed by existing and applicable privacy solutions studied in Section 4. We discuss limitations of participant privacy in task management and other challenges in Section 5. Finally, Section 6 provides some concluding remarks.

2. TASK MANAGEMENT IN MOBILE CROWD SENSING

We identify the following three entities in task management in mobile crowd sensing:

1. *Participants* are entities that use a sensing device to obtain or measure the required data about a subject of interest.
2. *Applications* or end users are the entities that request data through tasks and then utilize the information acquired by participants.
3. *Tasking entities* are responsible for distribution of tasks to participants who meet the requirements of applications. In certain architectures, end users and participants can also act as tasking entities.

Figure 1 shows the general structure of the task flow in MCS. Task management in crowd sensing can be studied from two perspectives: the type of sensing tasks and the distribution model.

2.1 Sensing Task Schemes

Tasks can be classified into several categories based on features inherent to the tasks or the involved tasking entities. In this study, we classify tasks

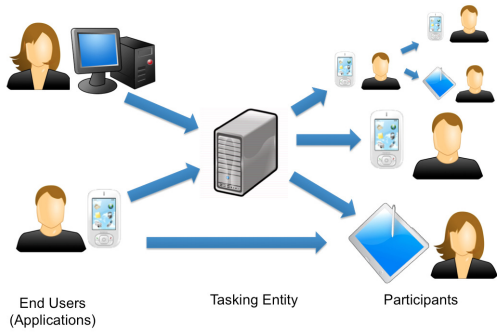

Figure 1: General structure of the task flow in mobile crowd sensing. Note that end users and participants can also act as tasking entities.

along two major dimensions: event based vs continuous, and spatial vs non-spatial. We should note that these dimensions are independent of each other and any combination is possible.

2.1.1 *Event-based vs Continuous*

One way to categorize different tasks is by the frequency with which the data is requested. The frequency could either be event-based or continuous.

Event-based tasks are triggered when a particular situation occurs. This includes special circumstances such as the presence of a participant at a specific location or an ad hoc incident. For example, the tasking entity could ask participants to act as citizen journalists and submit images or other information from a scene of interest when an event occurs [20].

Continuous tasks receive information from the participants periodically or frequently. For example, data could be requested every few minutes to monitor the speed of cars on a specific highway [42], or vital signs of a patient can be frequently requested to track the development of an illness [7]. Continuous tasks have been gaining popularity to keep a record of the different activities performed by the participants. Ganti et.al. have developed a software architecture that keeps track of the participant's activity and location using a personal wearable monitoring system [29], which can have safety, personal, and entertainment applications.

2.1.2 *Spatial vs Non-Spatial tasks*

In location-based tasks, the location of the participant plays an important role in determining task initiation, distribution, or assignment while non-spatial tasks can be triggered by time or other circumstances.

Spatial tasks require the participant to be at a

specific place in order to fulfill a task. With the increasing use of smart phones with integrated GPS, the number of applications in which, tasks are assigned based on the location of participants has also grown. Examples of spatial tasks include those in which sensors such as GPS and accelerometers are positioned in vehicles to detect road conditions. Some of these tasks are opportunistic; they run in the background with little or no involvement from the participant, and they could be used to detect traffic speed, bumps, inclination, and elevation of the road [25, 62, 42]. In contrast, participatory tasks could ask the users to report potholes or the quality of the road as they drive around in their normal commute [26, 72]. Spatial tasks are not restrained to reporting road conditions. For example, a participatory spatial task could require that the participants search for the best prices located at different stores and report them to provide other users with the best prices in the region [21, 9].

Non-spatial tasks are assigned independently of the location of the participant. For example, non-spatial tasks could opportunistically monitor the participant's activities as well as certain aspects of her lifestyle [29]. Tracking a participant's movement and physiological conditions has several beneficial applications in patients with neuromotor disorders [59]. A novel example of opportunistic non-spatial tasks is a "sociometer", which requires the participants to wear sensors that register their face-to-face interactions with other participants [14]. These sensors are able to register parameters such as who the participant is talking to, and how long her conversations last. Afterwards, this information is analyzed to understand the social structure of the participants, and determine how information is diffused, how group problems are solved, and how the community reaches a consensus or forms coalitions.

2.2 Task Distribution Models

Task management models can be categorized according to the way tasks are distributed among participants. The three major categories for these models are: centralized vs decentralized vs hybrid [17], push vs pull, and autonomous vs coordinated.

2.2.1 Centralized vs Decentralized vs Hybrid

In a *centralized model*, a central server or tasking entity provides the participants with different tasks to perform [42]. For example, in a party thermometer application, a central server could choose a set of participants attending an event or party, and request that they rate it. These ratings could serve other users who are considering attending this event [20]. One major issue of a central model in the context of privacy preservation is that the server constitutes a single point of failure for interactions between participants and applications should a security breach occurs. This problem can be alleviated by considering a network infrastructure as a central entity as opposed to having a single server [45].

In a *decentralized model*, each participant can become a tasking entity and decide either to perform a task or pass it forward to other participants who might be better-suited to fulfill the task. This decision would be based on certain attributes of other participants such as location, abilities, or the available hardware in their device. A decentralized recruitment model is proposed in [76] which notifies qualified participants of a forthcoming sensing activity. Some participants selected as recruiting nodes distribute the tasks in certain locations, then in a decentralized manner each participant passes the tasks to whoever matches the task criteria. The advantage in a decentralized model is that there is no single point of failure, so a security breach in a communication does not endanger the privacy of all the users.

A hybrid model includes parts of the centralized and the decentralized models. In this scheme, a central server and a set of participants who act as tasking entities build the task management core [25]. A bubble scheme [60] requires a central server to maintain control of the sensing tasks, which are allocated mostly in a decentralized way. In this model, a task is defined and broadcasted in a particular location of interest by a participant. The task is registered in the server, and other participants who move into the location of interest are signaled by the central server and become bubble carriers. These carriers can broadcast the task and can also fulfill them and report the sensed data to the server.

2.2.2 Push vs Pull model

A different classification for task management models is based on the entity that initiates the task. The initiation model can be *push* or *pull*.

Push model based tasks are initiated by a tasking entity via pushing the tasks on the participants' devices. The platform proposed in [20] uses a push and centralized model where executable binaries of opportunistic tasks are pushed to an optimized set of participants based on predefined criteria. The criteria could depend on several factors such as the location of the participants or the time of the day. An application of this model opportunistically registers GPS and accelerometer data obtained with the participants' mobile phones to determine the

conditions of the road and detect road bumps.

Pull model tasks are queried and downloaded by participants at an arbitrary time or location. A pull based task model can be found in [70], where a set of tasks are stored in a central tasking entity and the participants pull this information and decide which tasks to perform. The decision could be based on different criteria such as preferences, location, or the sensors' capabilities. Nericell [62] represents another pull model example, in which the task of opportunistically detecting road conditions such as potholes, traffic, and noise, depend on the participant's driving route and their smart phone's sensors.

2.2.3 Autonomous vs Coordinated

Tasks can also be categorized based on the allocation scheme that is used to distribute the tasks among the participants. Two approaches that we consider are autonomous task selection and coordinated task assignment [65, 66].

Autonomous task selection is an allocation method in which the participants have access to a set of tasks and they autonomously choose one or more tasks to perform. The participants do not necessarily need to inform the task distributing entity of their decision. While this scheme results in participants sharing fewer attributes with the tasking entities and consequently disclosing less private information, the lack of coordination and global optimization for distributing the tasks can decrease the efficiency with respect to sensing cost or global utility. Another major drawback of autonomous task selection is that it can generate bias in the obtained information. For example, people in urban areas might be more inclined to participate in a sensing task due to the greater presence of sensors or smart phones. This bias would directly affect the variables that are being studied, and will have an effect in the quality of the analysis [1].

Coordinated task assignment aims at improving the quality of the sensed data by optimizing the set of participants recruited to perform tasks. This optimization is based on varied criteria including coverage, quality, sensing costs, and credibility of the sensed data [65, 66]. Reddy et al. [67] proposed a recruitment process based on three stages. The first stage finds those participants that meet the minimum requirements, the second stage aims at maximizing the coverage over an area or time period, and the third stage checks the participants' reputation over coverage and data collection. Once the appropriate set of tasks and participants have been chosen, and the participants have performed the tasks, the task manager might review the participants' progress and evaluate them for future recruitment.

3. PRIVACY THREATS IN TASK MANAGEMENT

In mobile crowd sensing, privacy concerns might discourage participants from data contribution. Such concerns include a) disclosure of participant identity, b) disclosure of sensitive attributes such as race, age, or locations (e.g. current location, home or work address), and c) disclosure of more complex information such as personal activities or conditions (e.g. lifestyle or sicknesses). From a different perspective, participant privacy concerns can be aggravated either i) directly via sharing real IDs, IP addresses, exact locations, or other sensitive attributes, or ii) indirectly by sharing insensitive information (e.g. home address inference from trajectories of participants [54]). Designing a task management model that preserves the privacy of participants can be challenging due to the nature of crowd sensing tasks and task distribution models. In this section, we investigate the information that a participant shares with other tasking entities during the task management process and discuss how this information can directly or indirectly breach her privacy. We also discuss the applicability of the privacy threats with respect to the different tasking schemes we discussed in the previous section. Table 1 provides a summary of the privacy threats for vulnerable tasking schemes.

Adversary Models

From the perspective of participant privacy, the adversaries in MCS task management may include some or all of end-users (applications), tasking entities, and other participants based on their involvement in task management. Regardless of the role of adversarial entities, they are generally modeled as either *semi-honest* or *malicious*. Here, we study these two models and privacy threats associated with each. We also discuss how different entities in different task management frameworks fall into these categories.

3.1 Semi-honest Entities

The semi-honest entities (also known as passive) are assumed to follow the task management protocols and would not actively alter the data to breach the privacy of the participants. However, these entities may attempt to exploit any acquired information from participants to learn their private data. We categorize the privacy attacks conducted by semi-

honest entities in task management into *task tracing attacks* and *location-based attacks*, both of which are described below.

3.1.1 Task Tracing Attacks

When a participant downloads specific tasks from a tasking server (i.e. pull-based tasks), shares her preferences during a coordinated task assignment, or notifies a server of accepting a pushed task, she may reveal some attributes such as location, time, the task types in which she is interested, or some attributes of the sensing device she is carrying. For example, if a task is designed for undergraduate students majoring in History and can only be handled by Android devices, performing such a task reveals some information about the participant. This information alone might not breach her privacy; however, linking multiple tasking actions might allow an adversary to trace the selected tasks by the participant and consequently reveal her identity or other sensitive attributes [70]. Continuing the previous example, if the same history student later performs another task for an application designed for Hispanic students at her university, the adversary might be able to infer her identity. Some of the attributes that can be used to trace participants are real names, pseudonyms, International Mobile Equipment Identity (IMEI), IP addresses, or other user/device identifiers. An example of task tracing attack is illustrated in Figure 2.

Some tasking models distribute tasks among the participants based on their behavior and their profile as opposed to a device ID with specific characteristics [39]. Assuming that mobile phones are almost exclusively used only by its owner, the use of the device reflects the user's preferences. In particular, mobility can reflect the user's interest and can be used to determine if the user is more capable of fulfilling a task. However, this tasking model is still prone to location-based attacks.

3.1.2 Location-based Attacks

Spatial tasks requested (i.e. a pulled task) or accepted (i.e. a pushed task) by participants might lead to disclosure of their current location and eventually their sensitive locations such as home/work addresses or even their identification through location-based attacks. Location-based attacks are widely recognized in the context of location-based services (LBS), however, certain attributes of mobile crowd sensing make it more vulnerable to some of spatial attacks. Here, we give a brief review of such attacks in MCS.

In frequent spatial tasks, even if the participant

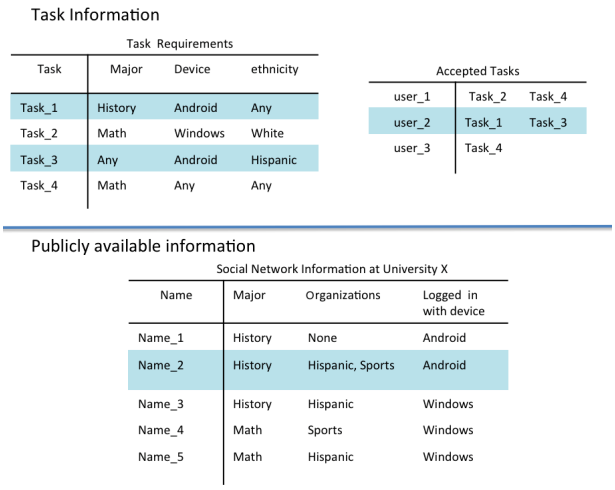

Figure 2: A task tracing attack in MCS task management using user-ids. Accepting task_1 is not enough to determine the identity of user_2, however, tracing the tasks she has performed and using available information from other sources could provide the necessary means to determine her identity.

is using the application anonymously (e.g. using pseudonyms), her trajectory might reveal her sensitive locations or commutes [55] or eventually disclose her identity using location-based de-anonymization attacks [28]. Krumm proposed several algorithms to identify a small group of anonymous participants and the home address of a larger group through location-based inference attacks [54]. They used the distribution of location traces during time, the last destinations of the day and the distribution of stay times to infer the home addresses of the participants. A location could be simply considered as a home if it is visited frequently by the same user at night [12]. Participant locations can also be exploited using trajectory data mining algorithms [61] to identify their significant locations. The trajectory data can be also used to infer the individuals' life patterns (i.e. private schedules or lifestyles) [81].

Continuous or frequent spatial tasks make MCS more prone to location-based inference attacks as more location traces of participants are collected. A simple example of this attack in mobile crowd sensing task management is illustrated in Figure 3.

Kazemi et. al. [46, 47] defined a location-based attack in campaign-based Participatory Sensing applications when participants used Spatial k-anonymity [74] to hide their location. The location attack is defined as the identification of a participant by an untrusted server by learning the location of her issued task query. They observed that all participants of a campaign query spatial tasks from the server (a.k.a. all-inclusivity property) asking for tasks closer to them than any other participants

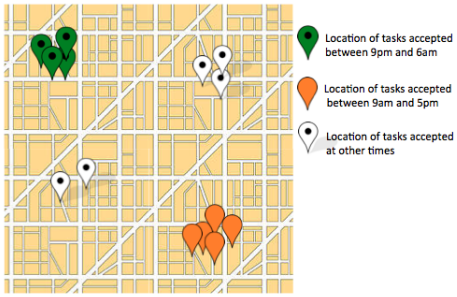

Figure 3: A simple location-based inference attack in MCS task management. The time and location of the accepted tasks can be enough to determine the participant's home and work addresses.

(a.k.a range dependency property). These properties result in the server having spatially-dependent requests from all participants, so they argued that participatory sensing is more vulnerable to such location-based attack. Gonzalez et. al. showed that people and their movements are highly correlated [36] making such attacks possible.

Another location-based attack targets applications that utilize the density distribution of participants (i.e. aggregated number of participants) in a location for task management [71]. This attack exploited by a group of terrorists can be used to identify dense areas for explosive launches.

3.2 Malicious entities

Malicious entities actively try to breach the privacy of participants. Privacy attacks associated with malicious task management entities include both aforementioned attacks along with several active de-anonymization attacks such as malicious tasking and collusion attacks. To prevent or stop these attacks, privacy countermeasures should be plugged into sensing devices or other trusted-parties.

3.2.1 Malicious Tasking

In the process of task definition, a malicious entity might create tasks that impose strict limitations on participant attributes or the device she is carrying (e.g. requiring a special lifestyle or a rare sensor type to qualify for the task). This attack which is called narrow tasking [70] might result in disclosure of identity or other sensitive attributes of the participant who accepts such a specialized task. In another variation of malicious tasking (a.k.a. selective tasking [70]), the tasking entity may share tasks with a limited set of participants to be able to learn their attributes or trace them (e.g. pushing or assigning a task to only one participant).

3.2.2 Collusion Attack

Several applications (end users) or tasking entities might collude to link the information of the participants for de-anonymization of the individuals or acquire their other private information. These attacks known as collusion attacks might be hard to detect in mobile crowd sensing systems since individuals might contribute to different applications using separate task management systems with no control over how their information is shared with others. For example, individuals might share some information with application A1 and other information with application A2 considering none of this information being personally identifiable separately. However, in reality, if applications A1 and A2 share pieces of her information, they might be able to de-anonymize her identity. Moreover, a malicious entity might create several applications with different contexts in an attempt to collect more private data from individuals. To avoid such attacks, while individuals might not be able to stop the collusion, they can at least control the amount of information they share with each application and also the overall information they share with all of the applications. We discuss this concept in detail in Section 4.3.

4. PRIVACY COUNTERMEASURES IN TASK MANAGEMENT

We categorize privacy solutions in MCS task management based on the applicable state-of-the-art privacy mechanisms. These mechanisms can be adopted in MCS based on privacy threats relative to task schemes and distribution models and the privacy preferences of the participants. In other words, there is no privacy-preserving method suitable for every user and application. For example, a participant who uses her real name to register to MCS applications cannot benefit from anonymization techniques. Table 1 summarizes privacy countermeasures that can be used for different privacy threats.

4.1 Anonymization

Anonymization techniques remove or hide identification information from all the interactions between the participant and other entities during task management. We review some of the anonymization techniques here.

4.1.1 Pseudonyms

One of the basic methods to preserve the anonymity of the participants includes using pseudonyms by replacing the identification information with an alias [17]. While this technique prevents location-based inference attacks, it does not protect the par-

Table 1: Summary of privacy threats and countermeasures for different tasking scenarios.

Privacy Threats	Tasking Scenarios	Countermeasures
Task tracing	Pulling specific tasks Coordinated task assignment Push-based tasks with notification	Anonymization Temporally constrained sharing Policy-based privacy preferences
Location-based attacks	Spatial tasks	Spatial cloaking Temporally constrained sharing Private information retrieval Differential privacy Policy-based privacy preferences
Narrow tasking	All tasking schemes	K-Anonymization Policy-based privacy preferences
Selective tasking	Coordinated task assignment Push-based tasks	K-Anonymization Policy-based privacy preferences
Collusion attacks	All tasking schemes	Policy-based privacy preferences

ticipants from task tracing or location-de-anonymization attacks (see Section 3.1.2). For a detailed review of these methods in MCS refer to a recent survey [16].

4.1.2 Connection Anonymization

These methods can be used to avoid tracing attacks using network-based identifiers such as IP addresses or device identifier such as International Mobile Equipment Identity (IMEI), and SIM card identifiers (IMSI, ICC-ID). One such technique which is adopted in crowd sensing applications [70] is onion routing [23] which hides the IP addresses of the participants from the other entities.

4.1.3 K-Anonymization

K-anonymization [73] is an established anonymization technique in database privacy [5]. A user is considered to be k-anonymous if her identity is indistinguishable from $k-1$ other users. In MCS task management, participants can adopt this method to avoid malicious tasking attacks by accepting a task only if there exists $k-1$ other qualifying participants for it. For example, if a user learns that she is the only qualified participant for a task, she would avoid performing it. K-anonymization is also widely adopted for location privacy which is discussed separately in Section 4.2.

4.2 Spatio-Temporal Privacy Methods

With the growing advance of location-based services, several spatio-temporal privacy mechanisms have been developed recently (see recent surveys in [31, 56, 4]). Although the context in mobile crowd sensing is different from location-based services, these mechanisms can be used to address location privacy problems in such scenarios as well. However, since location and time are two crucial pieces of information in an effective task management model, applying the existing spatio-temporal privacy-preserving techniques can be challenging. Here, we study some of the applicable methods in MCS task management.

4.2.1 Spatial Cloaking

In some crowd sensing applications, a perturbed or cloaked location can be used for spatial task management instead of exact locations. Spatial cloaking or perturbation hides the participant location inside a cloaked region using spatial transformations [50], generalization (e.g. k-anonymity) [44, 78], or a set of dummy locations [51] in order to achieve location privacy. Some MCS applications do not require exact locations (e.g. pollution or weather monitoring), but for the majority of the applications with utility depending on location accuracy, adopting cloaking methods remains a challenge. In recent work [65], participants of a coordinated spatial task assignment would share their cloaked location to obtain a set of closest tasks. They developed probabilistic methods to deal with uncertainty for a globally optimized task assignment.

Kazemi et. al. [46, 47] showed that spatial k-anoymity methods used in location-based services are not directly applicable to Participatory Sensing. Therefore, they proposed that a group of the representative participants ask for spatial tasks from an untrusted server, and share their results with the rest of participants. They would also adjust the spatial regions in queries to make queries independent from the location of other participants. Vu et. al. [77] proposed a spatial cloaking mechanism for Participatory Sensing based on k-anonymity and locality-sensitive hashing (LSH) to preserve both locality and k-anonymity.

While most traditional location cloaking methods rely on syntactic privacy models and are subjective to inference attacks, recent works applied more rigorous privacy notion based on differential privacy. The work in [3] proposed a location perturbation method based on a rigorous notion of indis-

tinguishability, which is similar to the differential privacy concept. Another recent work [79] protects the exact locations with differential privacy in a proposed *delta*-location set, which is derived in Markov model to denote the possible locations where a user might appear at any time.

4.2.2 Temporally Constrained Sharing

Some approaches share exact locations for tasking; however, they avoid or mitigate the location based attacks to some extent by controlling the timing of disclosures. For example, to avoid frequent revealing of location of participants in spatial tasks, Krause et al. [52] use a spatial obfuscation approach. In their solution, they divide the space into a set of regions, then with a certain probability distribution, a subset of participants is selected in each region to report their exact location. Such methods can be used in traffic monitoring applications.

Another method [52] assigns spatial tasks to participants in a way that the number of tasks for each participant is minimized. In such an approach, there will be longer intervals between each location disclosure, mitigating location-based inference attacks. This scheme can be further controlled by participants by setting explicit policies regarding the intervals in which they prefer to share their location. We discuss these methods in Section 4.3.

4.2.3 Aggregated Location with Differential Privacy

Differential Privacy [24] is a promising privacy-preserving approach with a strong protection guarantee. This method is adopted in privacy-preserving publishing of statistical information about location-based datasets [31] guaranteeing that individual location information disclosure does not occur. It can also prevent privacy attacks on the aggregated number of participants in a location as discussed in 3.1.2. In recent work, differential privacy is adopted for spatial crowdsourcing task assignment [75] in which a trusted aggregator (e.g. a cell service provider) computes differentially private aggregated counts of participants in various spatial regions and provides them to tasking entities for task assignment.

4.2.4 Private Information Retrieval

In autonomous pull-based tasking schemes, participants can retrieve the best suited tasks without providing their attributes using private information retrieval (PIR). PIR-based methods have been adopted for location-based services recently [31] since they guarantee cryptographic privacy by allowing data retrieval from a database without revealing any information to the database server about the retrieved item. Such an anonymous tasking scheme suffers from overlapping task selection and bias since sharing entities do not learn which tasks are retrieved.

4.3 Policy-based Privacy Preferences

To avoid direct or inference-based privacy breaches, participants should be able to set fine-grained preferences to control information sharing in a way that a curious party cannot learn or infer any private attributes. Such policies may include settings to ignore location-based tasks when the participant is within a specified range of a sensitive location (e.g. home or work), ignore narrow tasks, limit the number of tasks per time periods, or avoid sharing information that could be linked to previously disclosed data.

Shilton et. al. [69] introduced the concept of participatory privacy regulation in MCS which promotes participants' involvement in developing their own privacy policies and setting their personal boundries. Some methods provide a trusted cloud-based storage and processing entity for each participant to store and fully control sharing of her personal information with applications and end users [13, 63, 10]. A recent incentive-based task assignment approach allows participants to set their preferred privacy levels, which are then incorporated into a tasking cost model to limit the frequency of location disclosures (i.e. a task that requires location disclosure will be more costly for a participant with strict privacy preferences) [68].

5. DISCUSSION

In this section, we discuss further research directions and challenges of participant privacy in MCS including the limitations of privacy preserving tasking solutions, and privacy issues related to other components of MCS such as data collection.

5.1 Private Tasking Limitations

5.1.1 Trust and Credibility

Privacy and trust generally follow conflicting goals since the participant's trust is gained by higher accuracy and exactness of provided data, but privacy aims at hiding or perturbing identifying data (which includes majority of exchanged data in MCS) to protect the participant [1, 35]. Furthermore, trust issues become more challenging for anonymous tasking since they may result in tasking to untrustworthy or unqualified participants [17].

A trustworthy privacy-aware framework is proposed in [49], which defines the relationship between

trust and privacy in participatory sensing as a reverse k-nearest problem. Participants' privacy is procured in [34] by installing trusted software on the mobile device to encrypt the data before it is sent to the remote server. While this approach ensures the integrity of data during transmission to the server, the credibility of the participants is not evaluated.

Assessing the reputation of the participants while maintaining their anonymity and preserving their privacy is particularly difficult when a task requires the users to be at a certain location to collect the data more efficiently. Anonymous participants are prone to provide falsified or faulty data and it would be challenging to evaluate their participation, especially if different task actions cannot be linked due to privacy mechanisms [41, 18]. One approach to avoid trust issues in coordinated task management might be to assign a task to several participants to avoid the effect of malicious or faulty participation, however such method would result in a waste of resources.

Huang et. al. [41] proposed an anonymous reputation system for participatory sensing, which preserves the privacy of participants by separating their reputation from their identity. Another recent work [18] also addresses the issue of maintaining the reputation of the anonymous participants by using pseudonyms and anonymous transfer of the reputation information. They also use simulations to analyze the trade-off between privacy and reputation.

5.1.2 Reward-based Tasking

The challenge for rewarding participants in the presence of privacy mechanisms is very similar to the trust challenges since both require participant evaluations. However, trust models need to trace and review participants progress while incentives can be handled per task completion without linking it to other tasks. Several recent privacy-preserving incentive models are proposed in the literature [82, 58].

An anonymous credential system (or pseudonym system) can preserve the privacy of users while allowing internet transactions with service providers [11], so that an incentive-based system that supports privacy can be implemented. Zhang et. al [82] proposed a model based on pseudonym, encryption, and hashing to protect participant privacy.

A delayed rewarding model is proposed in [70] which aims at preventing task-reward linkage. Assuming that only the application can calculate the rewards for each task, their reward scheme includes a payment service that receives an anonymous claim message from the user after one or several tasks have been completed. The anonymity of the message is ensured by the application in the user's device, that encrypts a new identity for the user each time a message is sent. The payment service uses a one-way function to verify the message and forwards the reward to the user. The user's privacy will be preserved if the message is new for each report and the one-way function is secure.

5.1.3 Utility and Efficiency

Privacy mechanisms that obfuscate location, time, or other attributes challenge task management with uncertain or incomplete information. Therefore, the tasking entities may need to task a larger set of participants or conduct more computation to reach a certainty similar to non-private models. A recent work [65, 66] proposed a two-stage tasking model in which participants would share their cloaked locations rather than exact locations. Their model consists of a central tasking server which deals with location uncertainty and recommends globally optimized tasks to participants, and then each participant locally refines and further self-assigns tasks strictly following the global recommendation. Although this model achieves a comparable utility as the non-private method, the sensing and computational costs are higher due to uncertainty.

5.2 Data-related Privacy Concerns

In addition to how tasks are managed, task context (i.e. captured sensor data) might also lead to privacy issues for participants. For instance, noise monitoring tasks might record participants' voices, or if participants continuously report their driving habits during a trip, the destination of the trip may still be inferred even without sharing specific locations [22]. Another example of data-related privacy problems is contributing images that contain identifying information about the participants such as faces or locations [6] which can be de-identified before uploading to protect their privacy [64]. Fine-grained privacy preferences can also help participants to ignore tasks requiring sensitive contexts. Other privacy-preserving data collection solutions such as differential privacy can be used to perturb aggregated data before submitting to a server [80, 27]. If a trusted aggregator is not available, participants can use secure multi-party computation protocols [37] to aggregate their data before submitting to the data collector.

Furthermore, in most applications, captured sensor data contains meta-data such as time/location of individual sensing actions which might result in

location-based inference attacks. By linking reports to participants, other tracing attacks would arise. To assure participant privacy in mobile crowd sensing, privacy-preserving methods should be developed during both task management and data collection. Privacy issues during reporting has been extensively studied in literature, and several privacy-preserving data collection and aggregation methods have been proposed [17, 16].

Hu et. al. proposed a decentralized model to protect the privacy of participants in a social network while reporting data to an untrusted server. In their approach, participants pass data to their friends in a chain-like fashion before it is uploaded to the server. An spatial cloaking method based on generalization is used in [70] to hide the location of participants during data reporting. Huang et. al. [40] argued that location generalization methods decrease the utility of collected data significantly, particularly in traffic data monitoring applications. They proposed an alternative approach based on microaggregation and also a hybrid approach including both generalization and microaggregation.

5.3 Privacy Mechanism Enforcement

In Section 4 we discussed how suitable privacy mechanisms could be determined by the types of threats, but enforcing these mechanisms still remains as a challenge. In MCS, privacy mechanisms can be enforced on sensing devices (participants), semi-honest or trusted tasking entities, or other trusted third-parties. On the other hand, privacy-preserving architecture could be centralized or decentralized [30]. However, different models might introduce further complications and security issues which need to be considered in choosing an enforcement model.

A trusted third-party is one of the commonly used privacy-preserving approaches in MCS. Many works use a centralized server to anonymize the participants information, cloak their locations or perturb the aggregated number of participants in a region [75] while satisfying the users privacy requirements. In these architectures, the tasking entity (entities) receives anonymized information from the trusted party including perturbed or cloaked locations. Other methods use a decentralized architecture in which either participants trust each other and use peer-to-peer methods for spatial cloaking [46, 15] or they benefit from secure multi-party computation [30]. Moreover, a decentralized model may include a group of trusted agents [53] who share a complex data structure [32] to store and enforce privacy policies.

Krontiris et. al. [53] proposed trusted decentralized cloud-based agents to cloak the location of participants and enforce their preferred privacy policies. The agents are organized in a quadtree structure which is stored and managed in a decentralized fashion. While decentralized approaches avoid bottlenecks of centralized methods such as having a single point of failure and scalability problems, they introduce more complications for privacy enforcement and maintenance.

5.4 Privacy-Awareness

Another important topic regarding participants' privacy in crowd sensing task management is the users' privacy awareness. Several studies [54, 43, 19] show that individuals are generally unaware of threats of using location-based services and place a low value on the privacy of their location data. In general, with no or little incentives the participants might willingly share their sensitive location information and moving patterns. Other studies [8, 56] explore participants' attitude in sharing their location for incentives (i.e. the value of location) and their willingness and preferences for using location obfuscation methods for sharing highly sensitive data such as their home or workplace address. Their attitude towards sharing their location data depends on several factors such as the usefulness of the application, the amount of data to be shared, the incentives to share it, and if it will be used for commercial or other purposes [56, 54, 33, 57].

6. CONCLUSION

Mobile crowd sensing is an emerging topic with a wide variety of possible applications. However, the functionality of MCS relies on the participation of individuals who might be concerned about their privacy. In particular, task management as a central part of crowd sensing structure poses several threats to participant privacy, which should be identified and addressed. In this survey, we have classified different potential privacy risks and outlined their solutions for task management in MCS in an effort to raise awareness and preserve the privacy of the participants.

Acknowledgment

This research is supported by the Air Force Office of Scientific Research (AFOSR) DDDAS program under grant FA9550-12-1-0240.

7. REFERENCES

[1] C. C. Aggarwal and T. Abdelzaher. Social sensing. In *Managing and Mining Sensor Data*, pages 237–297. Springer, 2013.

[2] F. Alt, A. S. Shirazi, A. Schmidt, U. Kramer, and Z. Nawaz. Location-based crowdsourcing: extending

crowdsourcing to the real world. In *Proceedings of the 6th Nordic Conference on Human-Computer Interaction: Extending Boundaries*, pages 13–22. ACM, 2010.
[3] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi. Geo-indistinguishability: Differential privacy for location-based systems. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 901–914. ACM, 2013.
[4] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. Di Vimercati, and P. Samarati. Location privacy protection through obfuscation-based techniques. In *Data and Applications Security XXI*, pages 47–60. Springer, 2007.
[5] R. J. Bayardo and R. Agrawal. Data privacy through optimal k-anonymization. In *Data Engineering, 2005. ICDE 2005. Proceedings. 21st International Conference on*, pages 217–228. IEEE, 2005.
[6] A. Besmer and H. Richter Lipford. Moving beyond untagging: photo privacy in a tagged world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1563–1572. ACM, 2010.
[7] L. Brown, B. Grundlehner, J. van de Molengraft, J. Penders, and B. Gyselinckx. Body area network for monitoring autonomic nervous system responses. In *Pervasive Computing Technologies for Healthcare, 2009. PervasiveHealth 2009. 3rd International Conference on*, pages 1–3. IEEE, 2009.
[8] A. Brush, J. Krumm, and J. Scott. Exploring end user preferences for location obfuscation, location-based services, and the value of location. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*, pages 95–104. ACM, 2010.
[9] N. Bulusu, C. T. Chou, S. Kanhere, Y. Dong, S. Sehgal, D. Sullivan, and L. Blazeski. Participatory sensing in commerce: Using mobile camera phones to track market price dispersion. In *Proceedings of the International Workshop on Urban, Community, and Social Applications of Networked Sensing Systems (UrbanSense 2008)*, pages 6–10, 2008.
[10] R. Cáceres, L. Cox, H. Lim, A. Shakimov, and A. Varshavsky. Virtual individual servers as privacy-preserving proxies for mobile devices. In *Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds*, pages 37–42, 2009.
[11] J. Camenisch and E. Van Herreweghen. Design and implementation of the idemix anonymous credential system. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 21–30, 2002.
[12] X. Cao, G. Cong, and C. S. Jensen. Mining significant semantic locations from gps data. *Proceedings of the VLDB Endowment*, 3(1-2):1009–1020, 2010.
[13] H. Choi, S. Chakraborty, Z. M. Charbiwala, and M. B. Srivastava. Sensorsafe: a framework for privacy-preserving management of personal sensory information. In *Secure Data Management*, pages 85–100. Springer, 2011.
[14] T. Choudhury and A. Pentland. Sensing and modeling human networks using the sociometer. In *2012 16th International Symposium on Wearable Computers*, pages 216–216. IEEE, 2003.
[15] C.-Y. Chow, M. F. Mokbel, and X. Liu. Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. *GeoInformatica*, 15(2):351–380, 2011.
[16] D. Christin. Privacy in mobile participatory sensing: Current trends and future challenges. *Journal of Systems and Software*, 2015.
[17] D. Christin, A. Reinhardt, S. S. Kanhere, and M. Hollick. A survey on privacy in mobile participatory sensing applications. *Journal of Systems and Software*, 84(11):1928–1946, 2011.
[18] D. Christin, C. Roßkopf, M. Hollick, L. A. Martucci, and S. S. Kanhere. Incognisense: An anonymity-preserving reputation framework for participatory sensing applications. *Pervasive and mobile Computing*, 9(3):353–371, 2013.
[19] G. Danezis, S. Lewis, and R. J. Anderson. How much is location privacy worth? In *WEIS*, volume 5. Citeseer, 2005.
[20] T. Das, P. Mohan, V. N. Padmanabhan, R. Ramjee, and A. Sharma. Prism: Platform for remote sensing using smartphones. pages 63–76. in Proceedings of the 8th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys), 2010.
[21] L. Deng and L. P. Cox. Livecompare: grocery bargain hunting through participatory sensing. In *Proceedings of the 10th workshop on Mobile Computing Systems and Applications*, page 4. ACM, 2009.
[22] R. Dewri, P. Annadata, W. Eltarjaman, and R. Thurimella. Inferring trip destinations from driving habits data. In *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*, pages 267–272. ACM, 2013.
[23] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. Technical report, DTIC Document, 2004.
[24] C. Dwork. Differential privacy. In *Automata, languages and programming*, pages 1–12. Springer, 2006.
[25] S. B. Eisenman, E. Miluzzo, N. D. Lane, R. A. Peterson, G.-S. Ahn, and A. T. Campbell. Bikenet: A mobile sensing system for cyclist experience mapping. *ACM Transactions on Sensor Networks (TOSN)*, 6(1):6, 2009.
[26] J. Eriksson, L. Girod, B. Hull, R. Newton, S. Madden, and H. Balakrishnan. The pothole patrol: using a mobile sensor network for road surface monitoring. In *Proceedings of the 6th international conference on Mobile systems, applications, and services*, pages 29–39. ACM, 2008.
[27] L. Fan and L. Xiong. Real-time aggregate monitoring with differential privacy. In *Proceedings of the 21st ACM international conference on Information and knowledge management*, pages 2169–2173, 2012.
[28] S. Gambs, M.-O. Killijian, and M. Núñez del Prado Cortez. De-anonymization attack on geolocated data. *Journal of Computer and System Sciences*, 2014.
[29] R. K. Ganti, P. Jayachandran, T. F. Abdelzaher, and J. A. Stankovic. Satire: a software architecture for smart attire. In *Proceedings of the 4th international conference on Mobile systems, applications and services*, pages 110–123. ACM, 2006.
[30] R. K. Ganti, F. Ye, and H. Lei. Mobile crowdsensing: Current state and future challenges. *Communications Magazine, IEEE*, 49(11):32–39, 2011.
[31] G. Ghinita. *Privacy for Location-Based Services*. Synthesis Lectures on Information Security, Privacy, and Tru. Morgan & Claypool, 2013.
[32] G. Ghinita, P. Kalnis, and S. Skiadopoulos. Mobihide: a mobilea peer-to-peer system for anonymous location-based queries. In *Advances in Spatial and Temporal Databases*, pages 221–238. Springer, 2007.
[33] A. Ghosh and A. Roth. Selling privacy at auction. *Games and Economic Behavior*, 2013.
[34] P. Gilbert, L. P. Cox, J. Jung, and D. Wetherall. Toward trustworthy mobile sensing. In *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, pages 31–36. ACM, 2010.
[35] P. Gilbert, J. Jung, K. Lee, H. Qin, D. Sharkey, A. Sheth, and L. P. Cox. Youprove: authenticity and fidelity in mobile sensing. In *Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems*, pages 176–189. ACM, 2011.
[36] M. C. Gonzalez, C. A. Hidalgo, and A.-L. Barabasi. Understanding individual human mobility patterns. *Nature*, 453(7196):779–782, 2008.
[37] S. Goryczka and L. Xiong. A comprehensive comparison of multiparty secure additions with differential privacy. *IEEE Transactions on Dependable and Secure Computing*, 2015.
[38] J. Howe. *Crowdsourcing: How the power of the crowd is driving the future of business*. Random House, 2008.
[39] W.-J. Hsu, D. Dutta, and C. Ahmed Helmy. A paradigm for behavior-oriented profile-cast services in mobile networks. *Ad Hoc Networks*, 10(8):1586–1602, 2012.
[40] K. L. Huang, S. S. Kanhere, and W. Hu. Towards privacy-sensitive participatory sensing. In *Pervasive Computing and Communications, 2009. IEEE International Conference on*, pages 1–6. IEEE, 2009.
[41] K. L. Huang, S. S. Kanhere, and W. Hu. A privacy-preserving reputation system for participatory sensing. In *Local Computer Networks, 2012 IEEE 37th Conference on*, pages 10–18, 2012.
[42] 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 international conference on Embedded networked sensor systems*, pages 125–138. ACM, 2006.
[43] E. Kaasinen. User needs for location-aware mobile services. *Personal and ubiquitous computing*, 7(1):70–79, 2003.
[44] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias. Preventing location-based identity inference in anonymous spatial queries. *Knowledge and Data Engineering, IEEE Transactions on*, 19(12):1719–1733, 2007.
[45] A. Kansal, M. Goraczko, and F. Zhao. Building a sensor network of mobile phones. pages 547–548. in Proceedings of the 6th International Conference on Information Processing in Sensor Networks (IPSN), 2007.
[46] L. Kazemi and C. Shahabi. A privacy-aware framework for participatory sensing. *ACM SIGKDD Explorations Newsletter*, 13(1):43–51, 2011.
[47] L. Kazemi and C. Shahabi. Towards preserving privacy in participatory sensing. In *Pervasive Computing and Communications Workshops, 2011 IEEE International Conference on*, pages 328–331, 2011.
[48] L. Kazemi and C. Shahabi. Geocrowd: enabling query answering with spatial crowdsourcing. In *Proceedings of the 20th International Conference on Advances in Geographic Information Systems*, pages 189–198. ACM, 2012.
[49] L. Kazemi and C. Shahabi. Tapas: Trustworthy privacy-aware participatory sensing. *Knowledge and information systems*, 37(1):105–128, 2013.
[50] A. Khoshgozaran and C. Shahabi. Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. In *Advances in Spatial and Temporal Databases*, pages 239–257. Springer, 2007.
[51] H. Kido, Y. Yanagisawa, , and T. Satoh. An anonymous communication technique using dummies for location-based services. In Proceedings of the IEEE International Conference on Pervasive Services, 2005.
[52] A. Krause, E. Horvitz, A. Kansal, and F. Zhao. Toward community sensing. In *Proceedings of the 7th international conference on Information processing in sensor networks*, pages 481–492. IEEE, 2008.
[53] I. Krontiris and T. Dimitriou. Privacy-respecting discovery of data providers in crowd-sensing applications. In *Distributed Computing in Sensor Systems, 2013 IEEE International Conference on*, pages 249–257, 2013.
[54] J. Krumm. Inference attacks on location tracks. In *Pervasive Computing*, pages 127–143. Springer, 2007.
[55] J. Krumm. A survey of computational location privacy. *Personal and Ubiquitous Computing*, 13(6):391–399, 2009.
[56] J. Krumm. A survey of computational location privacy. *Personal and Ubiquitous Computing*, 13(6):391–399, 2009.
[57] C. Li, D. Y. Li, G. Miklau, and D. Suciu. A theory of pricing private data. *ACM Transactions on Database Systems (TODS)*, 39(4):34, 2014.
[58] Q. Li and G. Cao. Providing privacy-aware incentives for mobile sensing. In *Pervasive Computing and Communications, 2013 IEEE International Conference on*, pages 76–84, 2013.
[59] K. Lorincz, B.-r. Chen, G. W. Challen, A. R. Chowdhury, S. Patel, P. Bonato, M. Welsh, et al. Mercury: a wearable sensor network platform for high-fidelity motion analysis. In *SenSys*, volume 9, pages 183–196, 2009.
[60] H. Lu, N. D. Lane, S. B. Eisenman, and A. T. Campbell. Bubble-sensing: Binding sensing tasks to the physical world. *Pervasive and Mobile Computing*, 6(1):58–71, 2010.
[61] H. J. Miller and J. Han. *Geographic data mining and knowledge discovery*. CRC Press, 2009.
[62] P. Mohan, V. N. Padmanabhan, and R. Ramjee. Nericell: rich monitoring of road and traffic conditions using mobile smartphones. In *Proceedings of the 6th ACM conference on Embedded network sensor systems*, pages 323–336. ACM, 2008.
[63] M. Mun, S. Hao, N. Mishra, K. Shilton, J. Burke, D. Estrin, M. Hansen, and R. Govindan. Personal data vaults: a locus of control for personal data streams. In *Proceedings of the 6th International Conference*, page 17. ACM, 2010.
[64] E. M. Newton, L. Sweeney, and B. Malin. Preserving privacy by de-identifying face images. *Knowledge and Data Engineering, IEEE Transactions on*, 17(2):232–243, 2005.
[65] L. Pournajaf, L. Xiong, V. Sunderam, and S. Goryczka. Spatial task assignment for crowd sensing with cloaked locations. In *Proceedings of the 2014 International Conference on Mobile Data Management. IEEE*, 2014.
[66] L. Pournajaf, L. Xiong, V. Sunderam, and X. Xu. Stac: Spatial task assignment for crowd sensing with cloaked participant locations. In *23rd ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, 2015.
[67] S. Reddy, D. Estrin, and M. Srivastava. Recruitment framework for participatory sensing data collections. pages 138–155. in Proceedings of the 8th International Conference on Pervasive Computing, Springer Berlin Heidelberg, May 2010.
[68] M. Riahi, T. G. Papaioannou, I. Trummer, and K. Aberer. Utility-driven data acquisition in participatory sensing. EDBT/ICDT, ACM, March 2013.
[69] K. Shilton, J. A. Burke, D. Estrin, M. Hansen, and M. Srivastava. Participatory privacy in urban sensing. 2008.
[70] M. Shin, C. Cornelius, D. Peebles, A. Kapadia, D. Kotz, and N. Triandopoulos. Anonysense: A system for anonymous opportunistic sensing. *Journal of Pervasive and Mobile Computing*, 7(1):16–30, 2010.
[71] R. Shokri, G. Theodorakopoulos, J. Le Boudec, and J. Hubaux. Quantifying location privacy. In *Security and Privacy (SP), 2011 IEEE Symposium on*, pages 247–262. IEEE, 2011.
[72] G. Strazdins, A. Mednis, G. Kanonirs, R. Zviedris, and L. Selavo. Towards vehicular sensor networks with android smartphones for road surface monitoring. In *2nd International Workshop on Networks of Cooperating Objects (CONET11), Electronic Proceedings of CPS Week*, volume 11, 2011.
[73] L. Sweeney. Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):571–588, 2002.
[74] L. Sweeney. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570, 2002.
[75] H. To, G. Ghinita, and C. Shahabi. A framework for protecting worker location privacy in spatial crowdsourcing. *Proceedings of the VLDB Endowment*, 7(10), 2014.
[76] G. S. Tuncay, G. Benincasa, and A. Helmy. Autonomous and distributed recruitment and data collection framework for opportunistic sensing. *ACM SIGMOBILE Mobile Computing and Communications Review*, 16(4):50–53, 2013.
[77] K. Vu, R. Zheng, and L. Gao. Efficient algorithms for k-anonymous location privacy in participatory sensing. In *INFOCOM, 2012 Proceedings IEEE*, pages 2399–2407, 2012.
[78] S. Wang and X. S. Wang. In-device spatial cloaking for mobile user privacy assisted by the cloud. In *Mobile Data Management, 2010 Eleventh International Conference on*, pages 381–386. IEEE, 2010.
[79] Y. Xiao and L. Xiong. Protecting locations with differential privacy under temporal correlations. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1298–1309, 2015.
[80] L. Xiong, V. Sunderam, L. Fan, S. Goryczka, and L. Pournajaf. Predict: Privacy and security enhancing dynamic information collection and monitoring. *Procedia Computer Science*, 18:1979–1988, 2013.
[81] Y. Ye, Y. Zheng, Y. Chen, J. Feng, and X. Xie. Mining individual life pattern based on location history. In *Mobile Data Management: Systems, Services and Middleware, 2009. Tenth International Conference on*, pages 1–10. IEEE, 2009.
[82] J. Zhang, J. Ma, W. Wang, and Y. Liu. A novel privacy protection scheme for participatory sensing with incentives. In *Cloud Computing and Intelligent Systems, 2012 IEEE 2nd International Conference on*, volume 3, pages 1017–1021, 2012.