Chapter 5
Privacy, Trust and Incentives in Participatory Sensing

Mehdi Riahi, Rameez Rahman, and Karl Aberer

5.1 Introduction

In this chapter, we study the socioeconomic issues that can arise in distributed computing environments such as distributed and open, participatory sensing systems. Due to the decentralized nature of such systems, they present many challenges, some of which are equally socioeconomic and technical in essence. Three such major challenges arise in participatory sensing, one economic and two social. The economic problem is centered around the provision of incentives. How can participants be provided with incentives to ensure that they contribute to the system; that they provide sensed data when requested; and take part in various sensing activities?

The social problems are related to issues of *Trust* and *Privacy*. Trust issues revolve around determining which participants send accurate and truthful data and consequently which participants could be deemed more reliable. Privacy issues revolve around the fact that participants by taking an active part in sensing campaigns, risk exposing private details about themselves, such as their location at particular points in time.

In practice all three challenges are interlinked. For example, in order to ensure participants privacy, a system could provide anonymization of the users' identity. However, given that every node/participant is anonymized, it becomes harder to put in place an effective trust mechanism, which requires the identification of both trustworthy nodes and malicious/unreliable ones. In the same vein, system designers can use incentive schemes to incentivize users to sacrifice their privacy so that an efficient trust mechanism could be put in place.

M. Riahi (✉) • R. Rahman • K. Aberer
School of Computer and Communication Sciences, École Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland
e-mail: meriahi@gmail.com; rrameez@gmail.com; karl.aberer@epfl.ch

V. Loreto et al. (eds.), *Participatory Sensing, Opinions and Collective Awareness*,
Understanding Complex Systems, DOI 10.1007/978-3-319-25658-0_5

In the rest of this chapter, we examine various approaches that have been utilized in participatory sensing projects for ensuring privacy, setting up trust mechanisms, and providing incentives. Finally, we end with a discussion that highlights the major research areas that need to be examined in more detail. We note that participatory sensing systems are related to citizen science and urban informatics, and the problems we study in this Chapter are also relevant for those fields. Therefore, our discussion here would also benefit researchers working in those fields.

5.2 Privacy

5.2.1 The Challenge of Privacy

In participatory sensing systems, data is collected and shared by the participants to satisfy the goal of the system, be it community awareness, community services, or understanding social or environmental phenomena. Inevitably, the collected measurements directly or indirectly reveal some information about the participants and their environment. If the provided data can be used to infer additional information about the participants than what they actually intend to reveal, their *privacy* is threatened.

Privacy protection can be concurrently enforced in different phases of a participatory sensing system. On the sensing devices, the users should be able to choose when, where, and with what granularity to perform sensing and reporting. Local privacy protection measures such as location obfuscation or data perturbation can be employed by the mobile nodes. On the server side, privacy protection measures such as anonymization, secure and privacy-aware storage could be put into place.

Privacy-aware data storage, processing, and visualization are crucial for implementing a complete privacy-preserving participatory sensing system. Access control, usage monitoring, and data management tools should also be provided to the participants to have a fine-grained control on *who* accesses *what* data, for *how long* and with which *granularity*. In this section we don't cover these topics in detail; a thorough review of these requirements can be found in Christin et al. (2011). Here we outline the most important privacy requirements in participatory sensing and review the privacy protection mechanisms that have been proposed in the community.

Even though individuals have different perception of privacy, it is critical to the widespread adoption and success of participatory sensing to educate the participants about the privacy implication of their participation and to develop countermeasures against possible privacy threats. Ideally, participants should be able to understand the amount of privacy protection or privacy leakage in a tangible way. They should also be provided with the tools to tune the level of their protection based on their personal preferences and the incentives they receive for contributing data. *Location* and *context* privacy protection are major privacy challenges that must be addressed

to ensure privacy protection of the participants and hence the sustainability of participatory sensing systems.

In most participatory sensing applications, reports from participants have to be tagged with the location of the measurement and the time at which the measurement has been taken. However, location is private information for many people and when it is combined with time, sensitive information about habits, trajectories and relations of participants can be inferred. As stated in Johnson et al. (2007) one of the privacy challenges in participatory sensing is that participants have concerns about their context being revealed or inferred by others. For example, based on the reported data, others can discover that the participant is awake, sleeping, jogging, shopping, or in a conversation. Moreover, even social context of the participants might be inferred through the reported data. For example, if several participants attending a (private) meeting in a hotel report data, the data receiver can easily infer that they are in that hotel and in the same meeting.

Assigning sensing tasks to participants can be a threat to their privacy. For example, if user u_i is assigned a task to report temperature at location l and u_i performs the task at time t, then the creator of the task will know that user u_i has been at location l at time t. Therefore it is essential to protect privacy of participants while tasking by employing an *anonymous tasking mechanism*.

Including the identity of the user who reports data values in the reports is a clear way to disclose private information such as locations or trajectories. In order to make it difficult for an adversary to link data reports to the reporter, the reports must be *anonymized*. However, anonymization per se is not a strong measure against privacy attacks as long as the attacker can link several data reports from the same user or can analyze the reports to infer information about the user who has performed the sensing (Shin et al. 2011).

Privacy threats concern not only data providers, but also data consumers. Private information about the users who issue sensing tasks can also be inferred by adversaries. Consider a user u_i who regularly creates sensing tasks, requesting measurements of a phenomenon at a specific location l. It is easy to conclude that l is a point of interest for u_i. If the identity of u_i is known, discovering her point of interests can be a potential privacy threat. Even if the identity of u_i is not known a priori, with the help of some background knowledge it is possible to find her identity. Therefore, *queriers' privacy* is another challenge of participatory sensing that has to be addressed.

5.2.2 Privacy Protection Mechanisms

In this section we categorize the privacy protection mechanisms proposed in the literature that try to address some of the issues outlined above and give a short overview of each approach.

5.2.2.1 Privacy-Preserving Tasking

A solution proposed for privacy-preserving tasking is *task beaconing* (Johnson et al. 2007). In this approach, tasks are periodically broadcast to the users. The users who are interested in performing a task, inform the system without identifying themselves. The drawback of this approach is that no guarantees can be provided either for task completion or the quality of the results. Another proposed approach is called *attribute-based tasking* (Johnson et al. 2007). In this approach users who possess a particular set of attributes can identify themselves to the system without revealing their identities. For example, users can use cryptographic-based credentials to prove that they belong to a certain group. For instance, a user could belong to a group of users who have certain sensing modalities or have specific sensing qualities. Data integrity and quality assurance of data reports cannot be ensured in this approach due to the lack of knowledge about the identity of the users.

In AnonySense (Cornelius et al. 2008; Shin et al. 2011), privacy-preserving tasking is achieved as follows: a sensing task is created by an application and sent to the 'Registration Authority' (RA). RA checks the validity of the task for privacy safeness and forwards it to the Task Service (TS). The users *pull* the tasks from the TS through an anonymization network such as Tor (Dingledine et al. 2004). By using Tor, the identity and location (IP address) of users are protected when they connect to the TS. The TS verifies the tasks acceptance conditions to prevent too restrictive conditions that are vulnerable to what the authors call *narrow tasking* attacks. In narrow tasking attack, a malicious application tries to find the identity of the reporters by creating tasks with too restrictive acceptance conditions. The adversary knows that the number of users who can accept such tasks is small and consequently can discover their identity. Further, by having the users to pull tasks from the TS, what the authors call the *selective tasking* attack can also be prevented. In selective tasking attack, the adversary, who has control over TS, tries to distribute the tasks to only a few users so that their reports can be easily linked.

In certain participatory sensing campaigns, the participants query the server for data collection points (DCs), the locations for which data is required. Users generally wish to provide data for locations which are close(r) to them. However, in order to do this, users have to reveal their exact locations, and a malicious server can infer the identity of the users based on their locations, using additional background knowledge. This process is called *location-based attack*. To resolve this problem, a solution based on P2P spatial k-anonymity has been proposed (Kazemi and Shahabi 2011). Each user identifies its Voronoi cell in a distributed manner by communicating with other users. Then using multi-hop routing, each user finds at least $k - 1$ other users in the neighborhood and identifies the cloaked area. However, simply sending the cloaked area along with the range query to the server does not guarantee privacy protection of the users. This is due to a special property of such participatory sensing campaigns called *all-inclusivity*, where all the participants query for their closeby locations. This property can help the malicious server to de-anonymize the users. In order to alleviate this problem, only a subset of

representative queries are submitted to the server. The query results are then shared among all the users. In this approach, it is assumed that users trust each other not to reveal sensitive information about their peers.

5.2.2.2 Privacy-Preserving Reporting

As countermeasures against finding the identity of the reporter by linking data reports, several approaches have been proposed in the literature which fall into two classes: *anonymous reporting* and *location blurring*.

Anonymous Reporting

AnonySense prevents identification of the origin of the reports and the identity of the reporter by providing a mix network (MIX) for the users to send their reports to the Report Server (RS) (Cornelius et al. 2008; Shin et al. 2011). MIX acts as an anonymizing channel by routing reports through multiple servers, mixing similar reports from different sources and to different destinations, and inserting delays.

A technique called *spatial obfuscation* for privacy-preserving sensor selection has been proposed (Krause et al. 2008). In this approach, instead of selecting and contacting individual sensors, the space is divided into a set of cells and instead of individual sensors, cells are selected. Then in the selected cell, a sensor is (randomly) selected by a trusted arbitrator. Thus, the selected sensor can report its exact location and data without revealing its identity.

In order to alleviate the need of the trusted third party and for protecting location privacy and ownership privacy (i.e., associating reports to users) of the users, an algorithm called HP^3 has been proposed, which takes advantage of the social network that is formed by the participants (Hu and Shahabi 2010). Instead of uploading the report directly to the server, the user randomly chooses one of its friends and sends the report to her, which in turn forwards the report to another friend. The data is encrypted in order to prevent the intermediate nodes from exploiting the contents. To avoid data corruption, the data is segmented and redundantly sent through different routes.

In all these approaches privacy protection is achieved at the cost of more communication overhead.

Location Blurring

In order to prevent identifying the exact location of users from their reported data, the location should be blurred or should not be easily distinguishable from the location of other users. This technique is also called *spatial cloaking* and in general is achieved by *generalization* or *perturbation* of the location. In generalization, a value with higher granularity is reported instead of the actual value. In perturbation

techniques, the value is replaced by a different value, e.g., by the result of a function applied to a group of values. To protect the privacy of users '*k*-anonymity concept' is widely used (Sweeney 2002). *k*-anonymity is based on the idea that from the perspective of an external observer, individuals in a group of *k* entities which share a common attribute are not distinguishable if the group is known only by that common attribute.

Even though *k*-anonymity can prevent *identity disclosure*, it is shown that it cannot prevent *attribute disclosure* (Machanavajjhala et al. 2007). Attribute disclosure refers to the case where confidential information about an individual is obtained from the semantic meaning of an attribute. *Background knowledge attack* and *homogeneity attack* are two known attacks that can lead to attribute disclosure (Machanavajjhala et al. 2007). *l*-diversity is an approach that is proposed to ameliorate privacy preservation of users (Machanavajjhala et al. 2007). The basic idea behind *l*-diversity is that each group of users (or reports) contains at least *l* well-represented values for the sensitive attributes. In the simplest case, we can say that values are well-represented if they are distinct.

In AnonySense (Kapadia et al. 2008; Shin et al. 2011) the geographical area is divided into large enough *tiles* to provide *k*-anonymity for the users. Instead of reporting their location, users report the tile in which they are located. This generalization technique is called *tessellation*. Each user knows in which tile she is located, since she can consult a pre-built tessellation map of the area. Therefore, users need not reveal their location to find out in which tile they are located.

Microaggregation technique (Domingo-Ferrer and Mateo-Sanz 2002) for anonymous location reporting is proposed in Huang et al. (2010). Microaggregation is a perturbation scheme in which users are divided into 'Equivalent classes' (ECs) and the mean of the EC represents the perturbed location of the users that form that EC. An EC is created based on the Euclidean distance between location of users and it also conforms to *k*-anonymity. That is, the number of users in each EC is at least *k*. The heuristic that is used for creating ECs is called *Variable size Maximum Distance to Average Vector* (VMDAV). The authors show that both *tessellation* and *microaggregation* have mutual advantages and propose a hybrid approach called *hybrid VMDAV* to combine these advantages. To overcome the shortcomings of *k*-anonymity, the authors employ *l*-diversity and propose LD-VMDAV, an improvement on VMDAV based on *l*-diversity.

In addition to the cloak size *k* in *k*-anonymity, it has been argued that the size of the cloaked region and the distance of the cloaks to each other are important for the privacy of users (Shokri et al. 2010). The impact of the cloak size and *k*, the size of the anonymity set, on the quality of the information has also been investigated (Rodhe et al. 2012). It has been shown that data quality is more influenced by the cloak size as compared to the size of the anonymity set.

Using *cloud-based agents* for mobile nodes and a *quadtree* which is maintained in a distributed fashion, has been proposed (Krontiris and Dimitriou 2013). The stationary agents that reside in a cloud represent mobile nodes and collaborate with each other to support location privacy without needing any third party entity that can threaten the privacy of the users. Mobile nodes send their updated locations to their

agents. An agent obfuscates the location of its mobile node by choosing a region in the quadtree which best corresponds to the desired obfuscation level. The querier consults the quadtree to find the agents in the regions that overlap the queried region.

5.2.2.3 Data Perturbation

The key idea behind privacy protection through data perturbation is to add enough and appropriate noise to the data so that the data cannot be reconstructed. However, it has been shown that just adding random noise to each data item does not render reconstruction impossible because of the correlation among different data reports or between data and the context (Ganti et al. 2008). On the other hand, data which is largely perturbed is not useful for the applications. PoolView (Ganti et al. 2008) is a participatory sensing architecture with no trusted third party component in which users can locally perturb their data with application-specific noise so that data items cannot be reconstructed accurately, but the aggregate value can be computed correctly. In this approach, a priori knowledge about the characteristics of the phenomenon is required and only statistical trends about the phenomenon, such as average and standard deviation, can be reconstructed from the perturbed data reported by the participants. The noise model that is selected has to be similar to the actual phenomenon model and the distribution of the noise is a common knowledge in the community.

Another, similar idea has also been proposed for reconstruction of multidimensional data maps in vehicular participatory sensing (Pham et al. 2010). The proposed algorithm can correctly reconstruct the joint density from the perturbed data and the known noise density. This approach is shown to be effective against *filtering attack*, *range attack* and *leak attack*, but it is vulnerable against *map-based attack*. In filtering attack, the adversary uses filtering techniques to remove the additive noise from individual data. When the boundaries of the real data values and noise are finite, it is possible to find out the actual data value. This case is called range attack. In leak attack, the adversary might be able to estimate the seed of the pseudo random number generator and try to reconstruct the noise values given the noise distribution. In map-based attack, the adversary might be able to combine the real map with an estimation technique to infer the most likely trajectory.

5.2.2.4 Location Hiding and Adding Dummy Locations

In this type of privacy protection, the user does not accept sensing tasks when she is in sensitive locations. Alternatively, a user accepts tasks in long enough intervals in order to make trajectory inference more difficult. For example, in *sparse querying*, the queries to each user are imposed sparsely and infrequently (Krause et al. 2008). However, this approach cannot guarantee a high level of privacy protection if the adversary has access to enough background information about the participants. A selective hiding approach is employed in PEIR (Personal

Environmental Impact Report) (Mun et al. 2009). Users can select their sensitive locations and the algorithm creates alternative traces that are realistic but do not contain the sensitive locations. These candidate traces are further modified by time shifting and adjusting the duration of the activities so that the output is still similar to the actual output for the applications. Works like You et al. (2007), Lu et al. (2008), and Kido et al. (2005) propose to report locations from dummy trajectories which look like realistic trajectories and are also close to the real trajectories of mobile users in order to make location and trajectory inference difficult for the adversaries.

5.2.2.5 Data Aggregation

Providing aggregated data by the community to the participatory sensing system can protect the privacy of the participants. If anonymization is performed appropriately, the adversary cannot tell apart the individual contribution of participants in the aggregated report. However, in many cases, aggregated data does not satisfy the purpose of the system.

Anonygator is a distributed anonymous data aggregation service which leverages P2P aggregation (Puttaswamy et al. 2010). Each user contributes data in the from of a histogram, which is aggregated with other histograms contributed by other users in a privacy preserving manner. Anonymity is achieved through an anonymous routing scheme. Distributed aggregation is performed by using a tree-based aggregation construct which is called *multi-tree*.

The concepts of *data slicing* and *mixing* are used in Shi et al. (2010) to support statistical additive and non-additive aggregation functions. For additive aggregation functions, the key idea is that each node slices its data into $n + 1$ slices. Then, it randomly chooses n nodes, called its *cover nodes*, from its neighborhood and sends each slice to one of them. Each node sends to the aggregation server (AS) the sum of its left slice and the slices received form other nodes. In this way, the aggregation server cannot find out the individual data and its origin. Non-additive aggregation functions, such as Max/Min, Median, Histogram, and Percentile are supported by enabling the possibility of answering *count queries* in a privacy preserving manner. The basic idea is that the AS asks queries to the nodes which have "yes" (1) or "no" (0) answers. The sum of the "yes" answers is reported to the AS as outlined for additive aggregation functions. Similar to binary search, adapted queries are successively asked until the desired answer is found. This approach can protect privacy of the users unless when all other users and the AS conspire. However, intermediate nodes can make inferences about their neighbors or the whole network. In addition, the authenticity of the data cannot be guaranteed as the intermediate nodes can modify the slices they have received from other nodes.

The work in Erfani et al. (2013) tries to mitigate the shortcomings of the approach in Shi et al. (2010). The aggregator and the mobile nodes are assumed to be untrusted. Nodes can act maliciously by trying to infer measurements from their neighbors or by manipulating the aggregated data. The idea is based on additive homomorphic encryption used in secret perturbation (Castelluccia et al. 2005), and

data splitting (He et al. 2007). The scheme work as follows: when a node sn_i receives a query, it generates a random key $\widetilde{K_i}$ and encodes its measurement D_i using that key and sends it directly to the AS. The random key is then transmitted to the AS via n randomly chosen cover nodes as $\widetilde{K_i} = \sum_{j=1}^{n} \tilde{k}_{i,j}$, using the random slicing technique. The AS can check the integrity of the data using the proposed secure *homomorphic MAC*.

5.2.2.6 Encrypted Data Reporting

PEPSI (Privacy-Enhanced Participatory Sensing Infrastructure) is a privacy preserving data reporting and querying approach based on Identity-Based encryption (De Cristofaro and Soriente 2011). The key idea is that each data type corresponds to a label and the labels requested in a query or provided by a participant as data reports identify the query and the reports. Upon registration, each mobile node receives an ID corresponding to the type of data of its reports and a token for allowing it to announce data. Upon query registration, the querier obtains a private decryption key that corresponds to the ID of the query. Mobile nodes upload to the Service Provider (SP) their data reports encrypted using the public keys corresponding to their IDs. Finally, SP *blindly* matches the encrypted data reports to the encrypted queries. In this way, only the registered queries for a specific type of data reports can decrypt and see the information in the reports. The major drawback of this approach is that all the types of data should be associated with a label. However, if fine-grained locations are needed, this approach does not provide location privacy as it is easy to obtain location information from the labels used by the queriers and mobile nodes.

5.2.2.7 Privacy-Preserving Querying

A simple approach for protecting privacy of a querier is to introduce some *dummy query targets* along with the real query targets. However, this approach requires more resources.

The afore-mentioned PEPSI mechanism (De Cristofaro and Soriente 2011) also provides querier privacy by allowing the querier to encrypt the query. Neither the Service Provider nor data providers can identify the real identities of the queriers. A privacy enhancing protocol for participatory sensing (PEPPeR) is proposed with the aim of protecting privacy of the queriers (Dimitriou et al. 2012). In this work, queriers directly contact the data providing node and don't have to trust the service provider. The querier first obtains a token from the service provider without revealing its identity. Then it directly contacts the mobile nodes who can answer the query. The mobile node validates the token and then serves the query. Following this protocol and by using appropriate cryptographic mechanism, querier's privacy is assured and misuse of the tokens is detected.

5.3 Trust and Reputation

5.3.1 The Problem of Trust

Due to the openness nature of participatory sensing, data with different qualities can be contributed. It is crucial to the success of the participatory sensing systems to assess the quality of the reported data and to devise mechanisms that take into account the quality while analyzing the data. For example, in order to obtain a more accurate outcome while computing the average value of a phenomenon over a region, lower weights can be assigned to the data with lower quality. The quality of a sensor reading can be specified by a value, called *trust score*, which takes values in [0, 1]. Trust scores of data reported by a person or device can depend on the *reputation* of that person or device and vice versa. This means that, in the absence of certainty about the match of the reported data to the ground truth, past behavior of a person captured by her reputation plays an important role in assessing the trustworthiness of the data.

Trust score of a sensor reading is the level of confidence in how close the reading is to the (usually unavailable) true value. Trust of a sensing report r, is defined in Wang et al. (2011) as the probability of r being correct from the perception of the receiver. Reputation of a person is the opinion of others about the actions of that person. Reputation of a sensing node is defined in Wang et al. (2011) as a global value that synthesizes the correctness probability of the past sensing reports made by the node. Therefore, trust and reputation are two different concepts, even though they have been used interchangeably.

Several sources of quality distortion can be identified in a typical participatory sensing system: (1) sensor malfunctioning due to various reasons such as calibration problems, (2) using low-quality sensors, (3) position of the sensing device that affects the level of the exposure to the phenomenon, (4) perturbation by privacy protection mechanisms, and (5) malicious behavior of the participants.

Quality assessment in participatory sensing is a challenging task. This is due to the lack of access to the ground truth or supporting evidence in many situations or the subjective view about the desired quality. Reputation systems and trust assessment have been studied in wireless sensor network domain (e.g., Ganeriwal et al. 2008; Lim et al. 2010; Yu et al. 2012). However, the unique characteristics of participatory sensing, such as human involvement, necessitates more adapted approaches.

5.3.2 Trust Assessment Mechanisms

The existing work in the area of trust and reputation management in participatory sensing can be classified in three major groups. *Reputation-based recruitment* approaches aim for recruiting participants based on their reputation computed from

their past behavior in order to achieve better results for the campaign. *Privacy-aware trust and reputation management* approaches aim at providing frameworks for assessing trustworthiness of the contributions while protecting participants' privacy even though these two goals naturally contradict each other. *Privacy-oblivious trust and reputation management* methods provide trust assessment frameworks without taking into account privacy of the participants. Next, we discuss all three in more detail.

5.3.2.1 Reputation-Based Recruitment

A recruitment framework for participatory sensing has been proposed that is composed of three steps: *qualification*, *assessment*, and *progress review* (Reddy et al. 2010). In the qualification step, the minimum participation requirements such as availability, transport mode, and reputation identify the candidate participants. Recruitment is done in the assessment stage where based on some criteria such as maximizing coverage or minimizing budget, the participants are selected. Finally, the progress review continually evaluates the reputation and coverage of the participants to ensure that they are not significantly diverting from their base profile. The Beta distribution is used to calculate the reputation scores of the participants which can also incorporate aging factor.

Another reputation framework for participatory sensing is proposed in Yang et al. (2011). In this framework, reputation is a weighted sum of three factors: (1) *direct reputation*, which is calculated based on participant's past behavior and data report qualities; (2) *personal information*, including personal and device capabilities; and (3) *indirect reputation*, which includes community and organizer's trust in the participant. Based on the quality requirement specifications, participants are classified in four categories, namely, *very trustworthy*, *trustworthy*, *untrustworthy*, and *very untrustworthy*. Depending on the recruiter's criteria, participants can be recruited from these categories.

A reputation framework for *social participatory sensing* is proposed in Amintoosi and Kanhere (2013). In a social participatory sensing, existing online social networks are used as the underlying infrastructure and participants can be identified and recruited based on friendship relations. Only one-hop friends are selected as participants. The trust scores of the participants are calculated based on the quality of contributed data and the trust of participants (ToP). ToP consists of *personal factors*, such as expertise, timeliness, and locality (being local to the region of the sensing task), and *social factors* such as friendship duration and interaction time. A fuzzy inference system combines these two factors and produces a trust score for each contribution. Based on these trust scores a reputation score is calculated for each participant using the PageRank algorithm. This framework is further extended in Amintoosi and Kanhere (2013) to enable selection of friends of friends for recruitment and hence to expand the pool of participants.

5.3.2.2 Privacy-Oblivious Trust and Reputation Management

In the context of sensor networks, a reputation framework for dealing with faulty sensor readings is proposed in Ganeriwal et al. (2008). The framework consists of two components, namely a *watchdog* component and a *reputation* component. The watchdog component is responsible for detecting faulty readings based on outlier detection methods and providing the reputation component with the status of each reading. The reputation component maintains a reputation score for each sensor and updates this score based on the input from the watchdog component. Based on this approach, a reputation system for participatory sensing has been proposed (Huang et al. 2010). The space and time are divided into grids and the redundancy in each grid is used in the watchdog component to calculate a *cooperative rating* for each reading using an outlier detection algorithm. The cooperative ratings in the current epoch are then fed to the reputation component, which also uses the past cooperative ratings of the sensors to update their reputation scores. Reputation scores are computed using the Gompertz function that satisfies gradual trust build up for honest behavior and rapid trust tear down for untrustworthy behavior.

Trusted Platform Module (TPM) hardware can be used to ensure that the data reported by the mobile node is indeed the data that is measured by the sensor (Dua et al. 2009). However, this assurance does not always satisfy trust requirements and also it can threaten privacy of the users. Moreover, this technique does not prevent malicious or inadvertent behavior. For example, the user can put the sensing device in a place where the phenomenon cannot be correctly measured (e.g., putting the temperature sensor in the fridge). In many applications sending trusted raw data to the server is expensive in terms of resources. For instance, sending raw sound and video consumes too much bandwidth and one should process them before transmission to reduce their size. Therefore mechanisms are needed to ensure trustworthiness of the data not only after sensing but also after processing and transformation by third party applications (Gilbert et al. 2010). For protecting privacy of users, two platform features are provided in Gilbert et al. (2010): (1) preventing applications from accessing local resources without authorization; and (2) monitoring applications for making sure they do not release private information.

5.3.2.3 Privacy-Aware Trust and Reputation Management

A drawback of approaches such as the ones presented by Huang et al. (2010) is that for computing reputation scores, the history of user behavior is required. However, in a system that uses pseudonyms for protecting privacy of users, different contributions of a user cannot be linked together. A trusted third party that performs anonymization can be used to compute reputation scores (Huang et al. 2012), since

this entity knows the real identity behind the pseudonyms. Yet, naively transferring reputation information to the applications can inadvertently help an adversary to link the reputation information to the anonymized users. In order to avoid this threat, (Huang et al. 2012) uses a k-anonymity scheme that ensures that at least k users have the same reputation scores at the same time. Christin et al. (2013) further enhances the robustness of the privacy-aware reputation mechanism, by allowing the users to periodically change their pseudonyms and apply blind signatures (Chaum 1983) to prevent linking pseudonyms by the reputation and pseudonym manager (corresponding to the trusted third party in Huang et al. (2012)). In order to reduce the risk of inferring the true identities while reputation scores are transferred from the current pseudonym to the next one, users *cloak* their reputation score. In this way, users can achieve more anonymity protection at the cost of reducing their reputation.

Blind signature mechanism is also used in Wang et al. (2013) for enabling anonymous reputation. This framework consists of three components: *provenance model*, *sensing report trust assessment*, and *anonymous reputation management*. Provenance is the meta-data that describes the origin of the data and is composed of *user provenance* and *contextual provenance*. User provenance contains the pseudonym and the certified reputation level of the user, while contextual provenance includes the sensing environment factors such as time, location, traveling mode, and sensing mode (e.g., text, image, video). Trust of a sensing report is calculated considering the reputation level of the user, and the contextual provenance of the report, as well as the similarity to the other existing reports for the same task. Similarly to Christin et al. (2013), the blind signature mechanism is used to update the reputation level of users, based on the feedback from sensing report trust calculation, without the need to reveal their actual identity.

Collaborative path hiding is an approach for protecting location privacy of participants, in which participants exchange their reports upon meeting each other and then they submit the exchanged reports. Consequently, the application server cannot link the reports to the reporter. TrustMeter is a scheme proposed to evaluate the degree of collaboration and also to identify malicious users (Christin et al. 2012). Users give feedback about each other, to the application server, without revealing any private information about the peers, regarding how many of the exchanged reports have been transmitted by the peers.

In a participatory sensing setting where participants ask the server for the closest data collection points to them, the problem of location privacy and trust in collected data is slightly different. A privacy protection mechanism called PiRi is proposed in Kazemi and Shahabi (2011) for this setting. In order to ensure trustworthiness of the contributed data while using PiRi as the privacy protection mechanism, a solution has been proposed based on redundant allocation of data collection point to users assuming that the majority of users are truthful (Kazemi and Shahabi 2012).

5.4 Participatory Incentives

5.4.1 The Question of Incentives

Distributed systems, in which participants/nodes interact freely without any centralized authority require robust incentives to ensure contribution. Since crowdsensing/participatory sensing systems are also not owned by anyone in particular, they too require the provision of social and economic incentives for participants. In the last Chapter, the question of incentives was briefly touched upon, limited to the provision of incentives for users to do high quality work. However, the provision of incentives can be used to achieve a host of goals, including incentives for adherence to the protocol; abstention from malicious activities; and contribution of resources. Furthermore, most existing incentive schemes do not depend on *financial* rewards, due to the problems identified in the previous chapter *(Motivating workers in crowdsourcing markets)* plus some additional issues that we explicate next.

The design of such incentive schemes could be guided by various approaches, including mechanism design, heterodox economics, and other socially inspired mechanisms.

Usually, incentive schemes are developed with a particular model of user-behavior in the background, which is the rational model. We first concentrate on such works because they are pre-dominant in the literature.

Certain works bring up the conflict between fairness and social welfare. Fairness can be loosely defined as the provision of best quality or highest utility to the participant who contributes the most. Social Welfare is described as the increase in the overall utility of all users.

LiveCompare is a system that allows participants to hunt for bargains in grocery shopping via participatory sensing using mobile phone cameras (Deng and Cox 2009). It uses barcode decoding for the automatic identification of grocery products, and also localization techniques for accurately spotting store locations.

In order to incentivize users to contribute, it uses a very clever incentive mechanism, which is built into the user's query for services. When a user goes to a grocery store and wants to compare prices of particular items in other grocery stores, she submits her query by taking a photograph of the item in question. This includes the unique UPC barcode. The location of the store is also sent as part of the query. So the server is able to enrich its database with pricing and location information of the particular product; information that other participants can later make use of.

A purely game-theoretical approach for incentivizing people to contribute in participatory sensing has been proposed (Luo and Tham 2012). Using a rational actor model, the system links users demands to their contributions, i.e., quality of service for particular demand is related to users contributions. Two approaches are considered: one which focuses on ensuring fairness, as in providing best service to the highest contributors; and the second approach which ensures maximum social welfare. It is proved that the solution is a Nash Equilibrium.

SenseUtil is a system in which consumers have to pay producers to carry out sensing jobs (Thepvilojanapong et al. 2013). Using principles from microeconomics, the sensed data is valued by supply and demand. Demand and supply depend on factors such as location, user's preference, type of data required, etc.

An auction mechanism for incentivizing participation has also been presented (Jaimes et al. 2012). Similarly, monetary incentives in order to increase users participation have been put forward (Krontiris and Albers 2012). It is noted that providing monetary incentives is problematic because it is hard to determine the price at which users would want to sell their data. In order to solve this problem, a reverse auction mechanism to determine the value of sensed data is introduced. The novel point in this approach is that the auction is multi-attributive to accommodate the fact that different sensing data could be of different quality. The proposal helps users select and buy the highest quality sensed data (thus implicitly providing incentives for all data providers to improve their quality).

A credit based scheme in which users earn credit by contributing data has also been employed to offer incentives (Li and Cao 2013). The system uses a 'Trusted Third Party' to ensure that contributed data is not revealed, and privacy is protected.

In order to stimulate user participation, Reverse Auction based Dynamic Price (RADP) uses a bidding system where users can sell their sensing data to a service provider (Lee and Hoh 2010). The system uses the rational user model. The aim is to minimize the cost while incentivizing users to remain in, and not drop out of, participatory sensing applications.

An incentive scheme has also been proposed for road traffic prediction system based on participatory sensing (Lan and Wang 2013). It employs a credit based scheme earlier used in other participatory systems as well (Mawji and Hassanein 2008). Users earn virtual credits when they upload their data, and when they want to avail the service i.e., they want to know the future traffic condition, they have to spend credits.

The above works relied on a rational use model and/or purely game-theoretic approaches. However, it is likely that users that take part in participatory communities have unequal resources and also exhibit different behavior. Borrowing from Axelrod and Hamilton (1981), we can assume that user behavior can simply reflect standard operating procedures, rules of thumb, instincts, habits, or imitation, etc. Furthermore, for a tractable analysis of complex behavior, a game-theoretic approach requires a high level of abstraction of the design space. It follows that different designers can choose different abstractions to reach equally valid but different (sometimes contradictory) results. Thus, it is worthwhile to model a wide variety of user behavior and study the effects of different models on the underlying incentive scheme. Agent based modeling (or simulation-based) approaches can aid designers in complementing game-theoretic approaches to explore the design space of behavioral space more comprehensively.

In line with this thinking, *NoiseMap*, a participatory sensing application used to accurately measure noise levels, proposes different kinds of incentive schemes to motivate user participation (Schweizer et al. 2012). In this mechanism, *External Incentives* work by showing users each others performance via ranking. The

basic idea behind this is that competition with, and emulation of, others is a big psychological motivator for human beings. Therefore, if each user could see her performance rank in the global rankings, she could be incentivized to perform better. The ranking is available as daily, weekly, monthly and total, giving new users a chance to claim top spots fast. This is an example of *gamification* and can make the users feel excited and happy.

Furthermore, an *Internal Incentives* scheme has also been proposed, which allows users to get complete feedback on their measurement history including number of measurements taken, time spent with the application etc. There is also a scale reflecting at what time the application is used. By looking at their history users can evaluate the time and effort put into NoiseMap and set new goals for themselves.

'Top of the Worlds' is another incentive scheme not based on the rational model, which seeks to improve motivation to participate in sensing services by showing rankings in multidimensional hierarchical sets (Kawasaki et al. 2012). It is noted that previously proposed methods only rank a user among all other users, and this means that many people have little chance of being ranked in the top group, resulting in little motivation to continue. 'Top of Worlds' creates many sets with varying granularity to increase the chance of many users being ranked high. Subsequently, these rankings are presented to the users to incentivize more participation.

5.4.2 Empirical Observations

While the above are models that need to be implemented to see what effects they might have, some researchers have carried out projects in the field to explore the incentivizing models and choices that can make an impact on people's behavior. For instance, Reddy et al. carried out a project to learn more about sustainability practices at a university (Reddy et al. 2010). Study campaigns documenting use of various resources were carried out. Their findings include: (a) participants desired mobile visualizations to motivate them to participate more effectively; (b) participants were willing to accommodate minor diversions to their daily routines to help with the data collection campaign. However, they stated that drastic changes would require extra incentives; and (c) finally, participants felt that daily contribution summaries and reminders would foster increased participation.

In another work by the same authors, micro-payment system as an incentive model in an actual case study is analyzed (Reddy et al. 2010). Their findings include: (a) monetary incentives were more beneficial when combined with other motivating factors such as altruism or competitiveness (self or with others); and (b) micro-payments based on competition might be better suited for short bursty data collections unless mechanisms are added to offset participant fatigue. Making the incentive payment fair for all participants was important—very low baseline micro-payments discouraged individuals even when the potential to earn money existed.

Also, if properly designed, micro-payments have the potential to extend participant coverage both spatially and temporally.

5.5 Discussion

In this Chapter, we studied the major economic and social challenges faced by open distributed systems, such as Participatory Sensing systems. These are primarily related to Privacy and Trust on the social front, and provision of Incentives on the economic front. We have reviewed the state of the art techniques that have been proposed to address these challenges.

In this section, we will discuss three key challenges that the research community needs to address for designing successful participatory sensing systems.

5.5.1 Trusted Third Parties: Can They Be Eliminated?

A major differentiating factor in existing participatory sensing system architectures is the presence (or lack thereof) of one or more components that are fully trusted by the participants.

AnonySense (discussed in Sect. 5.2.2) architecture includes two components that are assumed to be trusted by mobile nodes, namely the *Registration Authority* and the *Anonymization Service*. A trusted third party, which is called *Anonymization Server (AS)*, is assumed to be present for creating equivalent classes in Huang et al. (2010). However, the authors propose a location perturbation approach to relax the assumption of full trust in AS. Anonygator uses a trusted entity called the *bank* for accounting and preventing malicious users from injecting disproportionate amount of false data (Puttaswamy et al. 2010). In addition, a P2P communication is assumed among participants.

PoolView does not assume the existence of any trusted third party (Ganti et al. 2008). The implication of this assumption and the approach proposed based on that, is that only aggregate community trends can be measured—not the actual value of the phenomenon sensed by the community. PEPSI (De Cristofaro and Soriente 2011) proposes a more realistic architecture composed of mobile nodes, queriers, network operator that provides GSM or 3G, registration authority, and service provider. No trusted third party is considered in the architecture. However, registration authority is an entity that has to be trusted for providing authorization and certificates. Hu and Shahabi (2010) proposes a node to node communication in a social network structure created by friendship relations among users. Therefore, no trusted third party is needed. However, for security and integrity purposes, an entity is required to issue certifications. Kazemi and Shahabi (2011) assumes P2P communication among users (*collaboration*) and therefore, the need for a trusted third party is eliminated. Another proposal suggests using cloud-based agents for

mobile nodes to eliminate the need of a trusted entity and the P2P communication among mobile nodes, which is not always possible (Krontiris and Dimitriou 2013).

It can be concluded that in all the works mentioned above, regardless of the architecture, some sort of trust between entities has to be present. However, the P2P communication among users does not seem realistic. The reason is that most of the existing participatory sensing systems rely on participants carrying smartphones with Internet connectivity provided by their network operator (3G or GSM). Moreover, it is not a realistic assumption that the participants always have access to wireless access points or other network media. Finally, it is not clear if smartphone users are open to directly communicate with other users because of the lack of trust.

5.5.2 Interdependency Among Trust, Privacy, and Incentives

Privacy and trust are for all practical purposes contradictory to each other. Generally speaking, data providers use obfuscation as a defensive mechanism for protecting their privacy. However, as the level of obfuscation increases, the consumer's trust in the provider decreases. Moreover, certain types of obfuscation can even render the reported data completely useless for the consumer. Drawing a boundary between defensive action and deceptive action therefore becomes nontrivial. If it is beneficial, a provider might be willing to reduce her level of obfuscation in order to gain more trust of the consumer. In other words, providers trade the privacy in return for some benefit. Therefore, for increasing the utility of participatory sensing systems, it is essential to provide effective mechanisms that enable privacy-trust negotiations.

It is worthwhile noting that the success of most of the mechanisms mentioned in Sect. 5.3.2 depends on the existence of enough redundant participants. Without this requirement it is rather straightforward for an adversary to link the reports or the reputation transfers to corresponding participants. This stresses the need for recruiting as many participants as possible to contribute enough and useful data and for guaranteeing their privacy protection and finally an efficient data analysis based on reputation of the participants and trust scores of the contributed data. For achieving this, effective incentive mechanisms must be employed to engage a large number of participants.

5.5.3 The Need for Diverse Incentive Models

Incentive mechanisms usually rely on either the rational user model inherited from mainstream economics or they try to take inspiration from other fields such as psychology and the social sciences in general. We showed that engineers and researchers in participatory systems, utilize various types of user-models in their works. In our view, it is clear that while some scenarios necessitate the usage of

a rational actor model, often this model proves to be limited and fails to provide adequate incentive to much of the 'population': those who are not well-equipped to contribute highly or those who don't respond to such incentives. Therefore, it is needed to properly explore other facets such as psychological considerations, e.g., peer imitation, feel-good factor, simple heuristics etc, that people in participatory systems (may) use.

References

Amintoosi, H., Kanhere, S.S.: A reputation framework for social participatory sensing systems. Mobile Netw. Appl. **19**(1), 88–100 (2014)

Amintoosi, H., Kanhere, S.S.: A trust-based recruitment framework for multi-hop social participatory sensing. In: 2013 IEEE International Conference on Distributed Computing in Sensor Systems, pp. 266–273 (2013)

Axelrod, R., Hamilton, W.D.: The evolution of cooperation. Science **211**(4489), 1390–1396 (1981)

Castelluccia, C., Mykletun, E., Tsudik, G.: Efficient aggregation of encrypted data in wireless sensor networks. In: The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2005), pp. 109–117. IEEE, New York (2005)

Chaum, D.: Blind signatures for untraceable payments. In: Advances in Cryptology Proceedings of Crypto 82, pp. 199–203 (1983)

Christin, D., Reinhardt, A., Kanhere, S.S., Hollick, M.: A survey on privacy in mobile participatory sensing applications. J. Syst. Softw. **84**(11), 1928–1946 (2011)

Christin, D., Pons-Sorolla, D.R., Kanhere, S.S., Hollick, M.: Trustmeter: a trust assessment framework for collaborative path hiding in participatory sensing applications. Technical Report, Technische Universität Darmstadt (2012)

Christin, D., Roßkopf, C., Hollick, M., Martucci, L.A., Kanhere, S.S.: Incognisense: an anonymity-preserving reputation framework for participatory sensing applications. Pervasive Mob. Comput. **9**(3):353–371 (2013)

Cornelius, C., Kapadia, A., Kotz, D., Peebles, D., Shin, M., Triandopoulos, N.: Anonysense: privacy-aware people-centric sensing. In: Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services, MobiSys '08, pp. 211–224. ACM, New York (2008)

De Cristofaro, E., Soriente, C.: Short paper: pepsi - privacy-enhanced participatory sensing infrastructure. In: Proceedings of the Fourth ACM Conference on Wireless Network Security, WISEC '11, pp. 23–28. ACM, New York (2011)

Deng, L., Cox, L.P.: Livecompare: grocery bargain hunting through participatory sensing. In: Proceedings of the 10th Workshop on Mobile Computing Systems and Applications, p. 4. ACM, New York (2009)

Dimitriou, T., Krontiris, I., Sabouri, A.: Pepper: a querier's privacy enhancing protocol for participatory sensing. In: Security and Privacy in Mobile Information and Communication Systems, vol. 107, pp. 93–106. Springer, Berlin, Heidelberg (2012)

Dingledine, R., Mathewson, N., Syverson, P.: Tor: the second-generation onion router. In: Proceedings of the 13th Conference on USENIX Security Symposium, SSYM'04, vol. 13, pp. 21–21. USENIX Association, Berkeley, CA (2004)

Domingo-Ferrer, J., Mateo-Sanz, J.M.: Practical data-oriented microaggregation for statistical disclosure control. IEEE Trans. Knowl. Data Eng. **14**(1), 189–201 (2002)

Dua, A., Bulusu, N., Feng, W.-C., Hu, W.: Towards trustworthy participatory sensing. In: Proceedings of the 4th USENIX Conference on Hot Topics in Security, HotSec'09, pp. 8–8. USENIX Association, Berkeley, CA (2009)

Erfani, S.M., Karunasekera, S., Leckie, C., Parampalli, U.: Privacy-preserving data aggregation in participatory sensing networks. In: 2013 IEEE Eighth International Conference on Intelligent Sensors, Sensor Networks and Information Processing, pp. 165–170 (2013)

Ganeriwal, S., Balzano, L.K., Srivastava, M.B.: Reputation-based framework for high integrity sensor networks. ACM Trans. Sens. Netw. **4**(3), 15:1–15:37, June 2008.

Ganti, R.K. Pham, N., Tsai, Y.-E., Abdelzaher, T.F.: Poolview: stream privacy for grassroots participatory sensing. In: Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems, SenSys '08, pp. 281–294. ACM, New York (2008)

Gilbert, P., Cox, L.P., Jung, J., Wetherall, D.: Toward trustworthy mobile sensing. In: Proceedings of the Eleventh Workshop on Mobile Computing Systems and Applications, HotMobile '10, pp. 31–36. ACM, New York (2010)

He, W., Liu, X., Nguyen, H., Nahrstedt, K., Abdelzaher, T.: Pda: privacy-preserving data aggregation in wireless sensor networks. In: 26th IEEE International Conference on Computer Communications, pp. 2045–2053. IEEE, New york (2007)

Hu, L., Shahabi, C.: Privacy assurance in mobile sensing networks: go beyond trusted servers. In: 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 613–619 (2010)

Huang, K.L., Kanhere, S.S., Hu, W.: Are you contributing trustworthy data?: the case for a reputation system in participatory sensing. In: Proceedings of the 13th ACM International Conference on Modeling, Analysis, and Simulation of Wireless and Mobile Systems, MSWIM '10, pp. 14–22. ACM, New York (2010)

Huang, K.L., Kanhere, S.S., Hu, W.: Preserving privacy in participatory sensing systems. Comput. Commun. **33**(11), 1266–1280 (2010)

Huang, K.L., Kanhere, S.S., Hu, W.: A privacy-preserving reputation system for participatory sensing. In: 37th Annual IEEE Conference on Local Computer Networks, pp. 10–18 (2012)

Jaimes, L.G., Vergara-Laurens, I., Labrador, M.A.: A location-based incentive mechanism for participatory sensing systems with budget constraints. In: 2012 IEEE International Conference on Pervasive Computing and Communications (PerCom), pp. 103–108. IEEE, New York (2012)

Johnson, P., Kapadia, A., Kotz, D., Triandopoulos, N., Hanover, N.H.: People-centric urban sensing: security challenges for the new paradigm. Technical report, Dartmouth College, Computer Science, Hanover, NH (2007)

Kapadia, A., Triandopoulos, N., Cornelius, C., Peebles, D., Kotz, D.: Anonysense: opportunistic and privacy-preserving context collection. In: Pervasive Computing. Lecture Notes in Computer Science, vol. 5013, pp. 280–297. Springer, Berlin, Heidelberg (2008)

Kawasaki, H., Yamamoto, A., Kurasawa, H., Sato, H., Nakamura, M., Matsumura, H.: Top of worlds: method for improving motivation to participate in sensing services. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing, pp. 594–595. ACM, New York (2012)

Kazemi, L., Shahabi, C.: A privacy-aware framework for participatory sensing. SIGKDD Explor. Newsl. **13**(1), 43–51 (2011)

Kazemi, L., Shahabi, C.: Towards preserving privacy in participatory sensing. In: 2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 328–331 (2011)

Kazemi, L., Shahabi, C.: TAPAS: trustworthy privacy-aware participatory sensing. Knowl. Inf. Syst. **37**(1), 105–128 (2013). doi:10.1007/s10115-012-0573-y. http://dx.doi.org/10.1007/s10115-012-0573-y

Kido, H., Yanagisawa, Y., Satoh, T.: An anonymous communication technique using dummies for location-based services. In: Proceedings of International Conference on Pervasive Services, ICPS '05, pp. 88–97 (2005)

Krause, A., Horvitz, E., Kansal, A., Zhao, F.: Toward community sensing. In: Proceedings of the 7th International Conference on Information Processing in Sensor Networks, IPSN '08, pp. 481–492. IEEE Computer Society, Washington, DC (2008)

Krontiris, I., Albers, A.: Monetary incentives in participatory sensing using multi-attributive auctions. Int. J. Parallel Emergent Distrib. Syst. **27**(4), 317–336 (2012)

Krontiris, I., Dimitriou, T.: Privacy-respecting discovery of data providers in crowd-sensing applications. In: 9th IEEE International Conference on Distributed Computing in Sensor Systems, DCOSS'13 (2013)

Lan, K.C., Wang, H.Y.: On providing incentives to collect road traffic information. In: International Wireless Communications and Mobile Computing Conference (IWCMC 13) (2013)

Lee, J.S., Hoh, B.: Sell your experiences: a market mechanism based incentive for participatory sensing. In: 2010 IEEE International Conference on Pervasive Computing and Communications (PerCom), pp. 60–68. IEEE, New York (2010)

Li, Q., Cao, G.: Providing privacy-aware incentives for mobile sensing. In: IEEE International Conference on Pervasive Computing and Communications (PerCom), vol. 18, p. 22 (2013)

Lim, H.-S., Moon, Y.-S. Bertino, E.: Provenance-based trustworthiness assessment in sensor networks. In: Proceedings of the Seventh International Workshop on Data Management for Sensor Networks, DMSN '10, pp. 2–7. ACM, New York, (2010)

Lu, H., Jensen, C.S., Yiu, M.N.: Pad: privacy-area aware, dummy-based location privacy in mobile services. In: Proceedings of the Seventh ACM International Workshop on Data Engineering for Wireless and Mobile Access, MobiDE '08, pp. 16–23. ACM, New York (2008)

Luo, T., Tham, C.-K.: Fairness and social welfare in incentivizing participatory sensing. In: 2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), pp. 425–433. IEEE, New York (2012)

Machanavajjhala, A., Kifer, D., Gehrke, J., Venkitasubramaniam, M.: L-diversity: Privacy Beyond K-anonymity. ACM Trans. Knowl. Discov. Data **1**(1), article no. 3 (2007). doi:10.1145/1217299.1217302. http://doi.acm.org/10.1145/1217299.1217302

Mawji, A., Hassanein, H.: A utility-based incentive scheme for p2p file sharing in mobile ad hoc networks. In: IEEE International Conference on Communications, ICC'08, pp. 2248–2252. IEEE, New York (2008)

Mun, M., Reddy, S., Shilton, K., Yau, N., Burke, J., Estrin, E., Hansen, M., Howard, E., West, R., Boda, P.: Peir, the personal environmental impact report, as a platform for participatory sensing systems research. In: Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services, MobiSys '09, pp. 55–68. ACM, New York, (2009)

Pham, N., Ganti, R.K., Uddin, Y.S., Nath, S., Abdelzaher, T.: Privacy-preserving reconstruction of multidimensional data maps in vehicular participatory sensing. In: Proceedings of the 7th European Conference on Wireless Sensor Networks, EWSN'10, pp. 114–130. Springer, Berlin, Heidelberg (2010)

Puttaswamy, K.P.N., Bhagwan, R., Padmanabhan, V.N.: Anonygator: privacy and integrity preserving data aggregation. In: Proceedings of the ACM/IFIP/USENIX 11th International Conference on Middleware, Middleware '10, pp. 85–106. Springer, Berlin, Heidelberg (2010)

Reddy, S., Estrin, D., Hansen, M., Srivastava, M.: Examining micro-payments for participatory sensing data collections. In: Proceedings of the 12th ACM International Conference on Ubiquitous Computing, pp. 33–36. ACM, New York (2010)

Reddy, S., Estrin, D., Srivastava, M.: Recruitment framework for participatory sensing data collections. In: Proceedings of the 8th International Conference on Pervasive Computing, Pervasive'10, pp. 138–155. Springer, Berlin, Heidelberg (2010)

Rodhe, I., Rohner, C., Ngai, E.C.-H.: On location privacy and quality of information in participatory sensing. In: Proceedings of the 8th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Q2SWinet '12, pp. 55–62. ACM, New York (2012)

Schweizer, I., Meurisch, C., Gedeon, J., Bärtl, R., Mühlhäuser, M.: Noisemap: multi-tier incentive mechanisms for participative urban sensing. In: Proceedings of the Third International Workshop on Sensing Applications on Mobile Phones, p. 9. ACM, New York (2012)

Shi, J., Zhang, R., Liu, Y., Zhang, Y.: Prisense: privacy-preserving data aggregation in people-centric urban sensing systems. In: Proceedings of the 29th Conference on Information Communications, INFOCOM'10, pp. 758–766. IEEE, Piscataway, NJ (2010)

Shin, M., Cornelius, C., Peebles, D., Kapadia, A., Kotz, D., Triandopoulos, N.: Anonysense: a system for anonymous opportunistic sensing. Pervasive Mob. Comput. **7**(1), 16–30 (2011)

Shokri, R., Troncoso, C., Diaz, C., Freudiger, J., Hubaux, J.-P.: Unraveling an old cloak: k-anonymity for location privacy. In: Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society, WPES '10, pp. 115–118. ACM, New York (2010)

Sweeney, L.: k-anonymity: a model for protecting privacy. Int. J. Uncertainty Fuzziness Knowledge Based Syst. **10**(5), 557–570 (2002)

Thepvilojanapong, N., Tsujimori, T., Wang, H., Ohta, Y., Zhao, Y., Tobe, Y.: Impact of incentive mechanism in participatory sensing environment. In: SMART 2013: The Second International Conference on Smart Systems, Devices and Technologies. IARIA, pp. 88–92 (2013). ISBN: 978-1-61208-282-0

Wang, X., Govindan, K., Mohapatra, P.: Collusion-resilient quality of information evaluation based on information provenance. In: 2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), pp. 395–403 (2011)

Wang, X.O., Cheng, W., Mohapatra, P., Abdelzaher, T.F.: ARTSense: anonymous reputation and trust in participatory sensing. In: INFOCOM, 2013 Proceedings IEEE, pp. 2517–2525. IEEE, New York (2013). http://dblp.uni-trier.de/db/conf/infocom/infocom2013.html#WangCMA13

Yang, H., Zhang, J., Roe, P.: Using reputation management in participatory sensing for data classification. Procedia Comput. Sci. **5**, 190–197 (2011) The 2nd International Conference on Ambient Systems, Networks and Technologies (ANT-2011)/The 8th International Conference on Mobile Web Information Systems (MobiWIS 2011).

You, T.-H., Peng, W.-C., Lee, W.-C.: Protecting moving trajectories with dummies. In: Proceedings of the 2007 International Conference on Mobile Data Management, MDM '07, pp. 278–282. IEEE Computer Society, Washington, DC (2007)

Yu, Y., Li, K., Zhou, W., Li, P.: Trust mechanisms in wireless sensor networks: attack analysis and countermeasures. J. Netw. Comput. Appl. **35**(3), 867–880 (2012)