Privacy and Incentive Mechanisms in People-Centric Sensing Networks

Daojing He, Sammy Chan, and Mohsen Guizani

Daojing He (corresponding author) is with East China Normal University.

Sammy Chan is with City University of Hong Kong.

Mohsen Guizani is with the University of Idaho, ID, USA.

ABSTRACT

Leveraging on the ubiquity and increasing number of smartphone users, people-centric sensing is a new computing paradigm that enables distributed data collection by voluntary participants, using the rich sensing capabilities of smartphones. In this article we identify the challenges on two important issues for a successful people-centric sensing system, i.e., privacy and incentives, because if either there is no incentive to participate or participants' privacy is invaded, smartphone owners will be reluctant to participate. Then we review some recent works that address these two issues. Finally, we suggest directions for future work on people-centric sensing by describing several open issues.

INTRODUCTION

In recent years, smartphones have been quickly replacing traditional mobile phones. In 2013 worldwide smartphone shipments surpassed one billion units and accounted for 55.1 percent of total mobile phone shipments in the year [1]. Effectively, a smartphone is a handheld computing device with various networking capabilities. It enables its user to access the Internet via WiFi or GSM/3G/4G networks. Moreover, a myriad of third-party applications are available and they can be downloaded to smartphones in a convenient manner. More importantly, smartphones are generally embedded with a set of powerful sensors such as a gyroscope, accelerometer, compass, camera, GPS, and microphone (Fig. 1). These features together enable smartphones to participate in a new sensing paradigm that is often referred to as people-centric sensing or participatory sensing (PS).

In a PS system, smartphone users help to collect data from their surroundings and upload the data to a central processor, where data contributed by different people are processed and delivered to interested third parties. With the great potential of PS, numerous applications and systems have been developed. Some examples include applications that use collected data to generate noise maps [2] and WiFi network coverage, as well as applications for monitoring air pollution and parking availability [3].

A PS system is essentially a wireless sensor network (WSN) formed by ubiquitous sensors. However, compared with traditional WSNs, PS offers a number of advantages. First, there is no need to pre-distribute sensors into the field; smartphones already in the field are recruited to provide services, so the setup cost is lower. Second, smartphones have much greater resources than motes, so sensing tasks become less constrained. Third, due to the inherent mobility of mobile phones, better spatial and temporal coverage can be achieved.

Although PS applications offer a great deal of potential to revolutionize different sectors of our lives, such as social networks, healthcare, environment monitoring, and transportation, there are two issues that might critically hinder their successful deployment. The first issue is the participants' privacy. Different from traditional WSNs, sensing devices are not owned by the entities that will make queries to the collected data. Instead, they are personal devices that are carried by participants all the time. When participants generate reports of their sensed data, inevitably the reports would expose some of their personal and sensitive information, such as physical location, behavior, political views, health-related information, or even income. Participants need to be assured that their privacy is properly protected before they will participate in a PS system. The second issue is incentive. A PS system requires the participants to carry out sensing tasks specified by individual applications. However, carrying out the sensing activities will consume resources of the participants' smartphones, such as energy and computing power. In other words, there is a cost incurred by participants to fulfill the sensing tasks. Clearly, a smartphone owner would be reluctant to participate unless sufficient incentive is provided.

Until now, these two issues have not received sufficient research attention, and thus they need to be addressed urgently for PS applications to gain widespread acceptance. In this article we summarize some recently proposed schemes that address various aspects of these issues. We also identify new challenges and suggest several future research directions.

0163-6804/15/$25.00 © 2015 IEEE

People-Centric Sensing Services and Their Privacy and Incentive Requirements

Architecture of PS systems

As shown in Fig. 2, the basic infrastructure of a typical PS system involves the following entities.

- Mobile nodes are the smartphones carried by the participants. They are used to sense the parameters specified by the service provider, compile data reports, and submit them to the server operated by the service provider through WiFi or mobile telecommunication networks.
- Queriers subscribe to specific information collected by PS applications and receive reports from the service provider. Being customers of PS services, they could indicate which types of data they are interested to obtain.
- Service providers manage the PS service to facilitate effective sharing of data between mobile nodes and queriers. Usually, the service provider has abundant storage capacity and computation power, thus it can process the acquired data before distributing them to the queriers.
- Trusted third party (TTP) is an optional entity. It is needed in some privacy-preserving schemes.

The flow of a PS service is described as follows. A service provider learns from queriers about the types of data that they are interested in. It then announces the tasks of collecting these data. Those mobile nodes who are willing to participate will carry out the task. Having completed a task, a mobile node submits a report to the server of the service provider. The service provider aggregates all the returned reports, extracts the appropriate information, and forwards to queriers.

Privacy and Incentive Requirements

In general, service providers should not be considered as trustworthy for protecting participants' privacy. Information collected by a service provider might possibly be exploited by malicious administration personnel belonging to the service provider. Related to this, privacy requirements often include the following.

Node Privacy: Data reports should not reveal the private information of mobile nodes, such as identities and locations, to the service provider, other mobile nodes, or queriers. Moreover, only authorized queriers can access reports to obtain information about parameters being measured and the measured values.

Querier Privacy: Personal information may be inferred from query interests. No entity in the PS system, including the service provider, mobile nodes, or other querier, can learn any information about the interests of a querier.

Anonymity, Report Unlinkability, Location Privacy: A PS system with privacy preservation should provide anonymity, report unlinkability, and location privacy. Here report unlinkability means no entity can link two or more reports associated with the same mobile node.

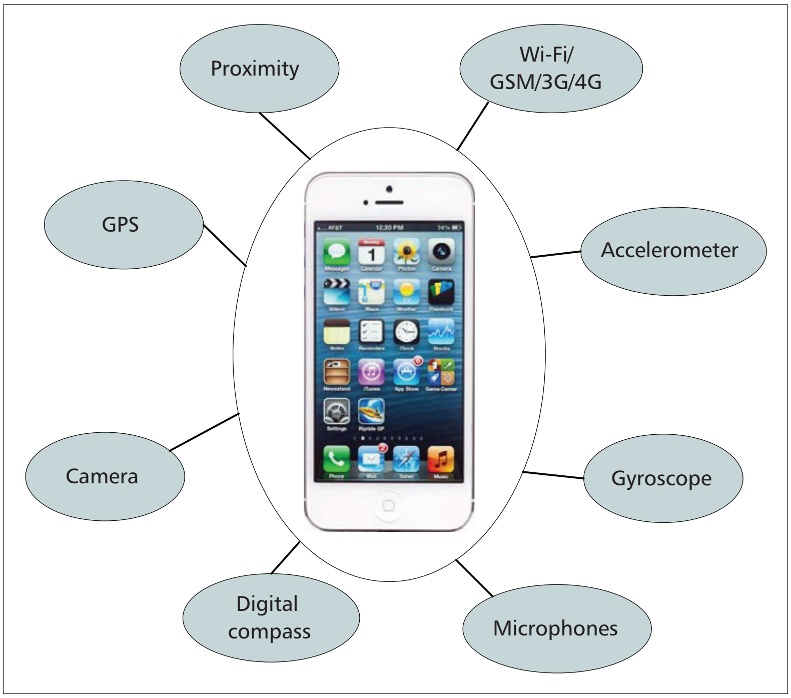

Figure 1. Sensors commonly available on smartphones.

No Trusted Third Party: Trust between different entities is limited. Since there is no trusted third party, a single point of failure is eliminated.

The following are basic requirements for the design of incentive mechanisms. First, a mechanism should motivate users to participate. That is, each participant should achieve a non-negative utility. At the same time, total payments to participants should be minimized such that the service provider does not incur any loss. Second, a mechanism should encourage participants to reveal their true costs. For example, a mechanism can be designed in such a way that no participant can increase its utility by reporting a cost that deviates from the true value, irrespective of the costs reported by other participants. This prevents participants from over charging the service provider, as it generally does not know the actual participation cost. Third, a mechanism should be computationally efficient, that is, the outcome can be computed in polynomial time.

Privacy Mechanisms

Privacy-Aware Data Collection

Privacy in PS systems is first addressed by AnonySense [4], which is a general framework to provide anonymous tasking and reporting based on mix network techniques. Specifically, it makes use of multiple relays and onion routing to anonymize the connections between participants and the service provider. As a result, the IP addresses and information about current locations of the participants are hidden. AnonySense also prevents leakage of participants' private information through submitted reports by providing k-anonymity. Later, this property is strengthened in [5] by achieving l-diversity. However, AnonySense suffers from several drawbacks. First, mix networks do not provide

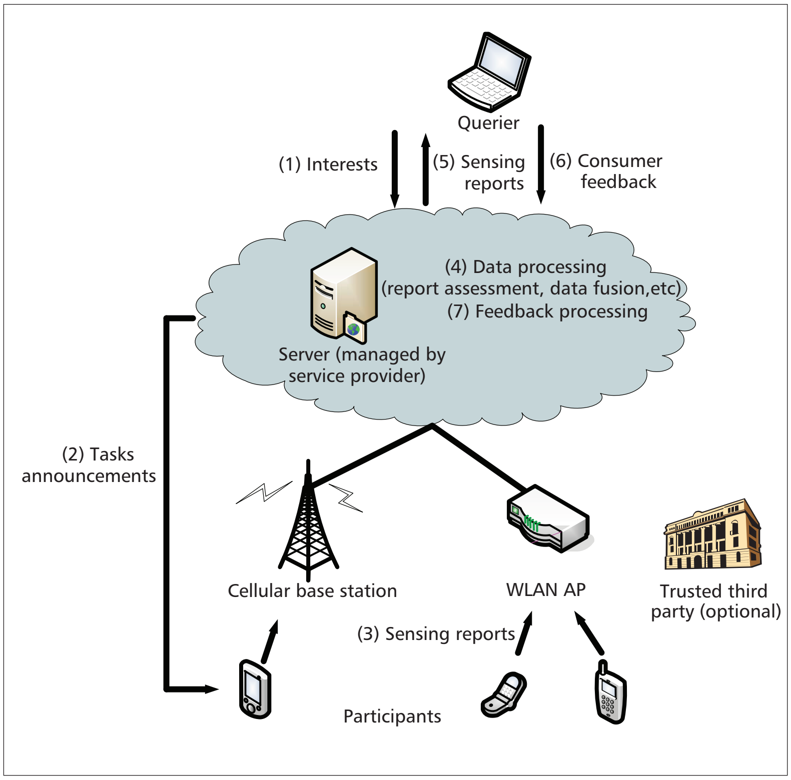

Figure 2. Architecture of a people-centric sensing system.

provable privacy guarantees. For example, anonymity in a mix network providing *k*-anonymity depends on the number of received reports. Second, AnonySense assumes WiFi as the network infrastructure of PS systems so that user unlinkability between reports with respect to access points can be guaranteed by MAC-IP address recycling techniques. Unfortunately, a ubiquitous presence of non-restricted WiFi networks is not yet a practical assumption. Third, reports are sent to the so called report server (RS), which then distributes them to queriers. The degree of report confidentiality depends on whether the RS is trustworthy.

Caceres *et al.* [6] suggest that privacy can be protected if each participant has access to a private server (e.g. a virtual machine hosted by a cloud service) and uses it as a proxy between its sensors and the service providers. However, the cost and availability of per-user proxies would severely limit the feasibility of this approach in large scale PS systems.

In [7] De Cristofaro and Soriente propose the Privacy-Enhanced Participatory Sensing Infrastructure (PEPSI) to provide node privacy and query privacy. When a mobile node submits a report to the service provider, the report is encrypted such that only queriers subscribing to the parameters contained in the report have the key to decrypt it. Since the service provider cannot access the contents of reports and queries, a tag is associated with an individual report or query. Upon receiving a report, the service provider matches its tag with queries carrying the same tag and forwards the report to the corresponding queriers.

This approach of comparing tags is a very efficient way to forward reports to the corresponding queriers. Otherwise, if a report does not carry such a tag, the service provider simply has to forward all encrypted reports to all queriers. Each querier has no clue about the type of each received report, but can only try to decrypt each one using each of its decryption keys. Only those reports that can be decrypted provide the measurements of its interest. Unfortunately, given the large number of reports generated by mobile nodes, this means that a lot of processing effort is wasted in order to obtain the desired measurements.

The cryptographic building block of PEPSI is the identity-based encryption (IBE) approach, which is an asymmetric cryptographic primitive based on bilinear map pairings. The distinguishing feature of IBE is that some unique information of the recipient's identity can be used to derive its public key, and the corresponding private key is issued by a trusted authority. In PEPSI, each report or subscription is identified by a set of labels, which naturally are parameters contained in the report. Mobile nodes encrypt their reports using the reports' labels as the public encryption keys. The privacy functionalities of the above schemes are compared in Table 1.

Privacy-Aware Data Collection and Reward Claiming

The schemes in [4–7] only focus on how participants upload the collected data to the server without revealing their identities, but they do not consider the privacy aspect in the reward claiming process. To address this issue, some approaches have been proposed. In [8] Zhang *et al.* propose a method to protect the privacy of a mobile node when submitting a report and claiming the corresponding reward. Their method requires the existence of a TTP, which is called a certification center. In the system initialization phase, the service provider first chooses a suitable one-way hash function, a master key, and an asymmetric encryption function. The one-way hash function is distributed to all mobile nodes and the certification center, while the master key and the encryption function are sent to the certification center via a secure channel.

In the data collection and upload phase, data is collected by mobile nodes according to the specifications sent from the service provider. Then a report containing the data, hash value of a randomly generated pseudonym, and a timestamp is sent to the service provider via an ordinary channel. Upon receiving the report, the service provider generates a certificate using the encryption function based on the master key, received hash value, and timestamp. This certificate is contained in a confirmation message that is returned to the mobile node via an ordinary channel. Later, when the mobile node wants to claim its reward, it prepares a message containing the pseudonym, certificate, and the timestamp, and sends the message to the certification center via a secure channel. Upon receiving the claim message, the certification center only needs to generate a certificate from the received parameters and then compares it with the received certificate. If they match, the mobile node can obtain a reward for its uploaded report.

	AnonySense [4] and its extended version [5]	Caceres's method [6]	PEPSI [7]
Node privacy	Not guaranteed	Yes	Yes
Querier privacy	Not guaranteed	Yes	Yes
Report unlinkability and location privacy	Not guaranteed	No	No
Trusted third party	Needed	Needed	Needed

Table 1. Privacy functionality comparison among the existing methods.

In this scheme, since only pseudonyms are used in reports and claims, the real identities of mobile nodes are not revealed and thus their privacy is protected. In addition, an adversary cannot steal any reward by eavesdropping the confirmation message, because when it claims the reward, it needs to provide the pseudonym. However, the confirmation message only contains the hash value of the pseudonym. Due to the irreversible property of hash functions, it is infeasible for the adversary to recover the pseudonym from its hash value. Thus, it cannot generate a legitimate claim. Moreover, since the master key is only kept by the service provider and the certification center, no adversary can generate any fake certificate to claim a reward.

In [9] Li and Gao propose another scheme to protect the privacy of a mobile node when submitting a report and claiming the corresponding reward. The scheme assumes that there exists a certificate authority, which is responsible for issuing different sets of public and private keys to the service provider and mobile nodes, and that anonymous communication between mobile nodes and the service provider are maintained. Similar to [8], pseudonyms are used to protect the privacy of mobile nodes. For a given report, the service provider cannot tell which mobile node has submitted the report. In addition, reports submitted by the same mobile node are unlinkable, which means that the service provider cannot tell if those reports are submitted by the same mobile node. When a mobile node claims the reward, its claim is also identified by a pseudonym rather than the real identity. Most importantly, a comprehensive mechanism is included in the scheme to ensure that the reward claimed by each mobile node is no more than that allowed by the service provider. In other words, if the service provider is only willing to pay c credits for one report of a task, each mobile node can claim at most c credits even though it submits more than one report.

To achieve the above goal, the mechanism enforces the following three conditions:

- Each mobile node can only accept a task at most once.
- The mobile node can only submit at most one report for each accepted task.
- The mobile node can earn c credits from a report.

For the first condition, the basic idea is to associate each task with a request token. When a mobile node is interested to accept a task, it needs to send the *request token* to the service provider to obtain approval. If only one request token for each task is issued to a mobile node and the token is consumed when the mobile node accepts the task, then a mobile node cannot accept a task more than once. Similarly, for the second condition, each report is associated with a *report token* and each mobile node is only given one report token for each task. When a mobile node submits a report, it consumes the report token and hence cannot submit more reports. To ensure that the appropriate tokens are consumed by mobile nodes, each token is also associated with a *commitment*, which is used by the service provider to verify the validity of a token.

In its simplest version, the scheme in [9] assumes the existence of a TTP, which is responsible for generating tokens for each mobile node and their commitments. Since most computations are carried out by the TTP, the computation and storage cost incurred at each mobile node is low.

As shown in Fig 3, there are three major phases: setup, task assignment, and report submission. In the setup phase, the TTP pre-computes a set of request tokens and their commitments that each mobile node and the service provider will use for the next M tasks. Then it distributes the request tokens and commitments to mobile nodes and the service provider, respectively. Moreover, the TTP also sends a secret key to the service provider to generate report tokens and commitments. In the task assignment phase, the service provider broadcasts a list of tasks to the mobile nodes. If a mobile node decides to accept task i, it sends a request message containing the request token to the service provider. The service provider verifies the validity of the request token by comparing it with the commitment obtained from the TTP. If the result is positive, it sends the mobile node an approval message, which contains the necessary parameters for the mobile node to generate the report token. Clearly, this steps ensures that a mobile node cannot generate the report token for a task without the approval from the service provider. Subsequently, the service provider generates the corresponding commitment for the report token. In the report submission phase, after the mobile node has generated a report for task i, it submits both the report and its corresponding token. If the service provider verifies that the report token is indeed committed to task i, it sends pseudo-credits to the mobile node. From the pseudo-credits, the mobile node computes c credit tokens. Later, a mobile node can deposit its earned credits, but using its real identity.

Incentive Mechanisms

Another important issue in the design of a PS system is how to design incentive mechanisms to motivate mobile nodes to participate in a PS system. For example, it is assumed in [8] and [9] that c credits are awarded to a mobile node for a submitted report. How should c be determined such that the requirements in the previous section are satisfied.

In [10] the problem is modeled as a reverse auction in which mobile nodes bid for participa-

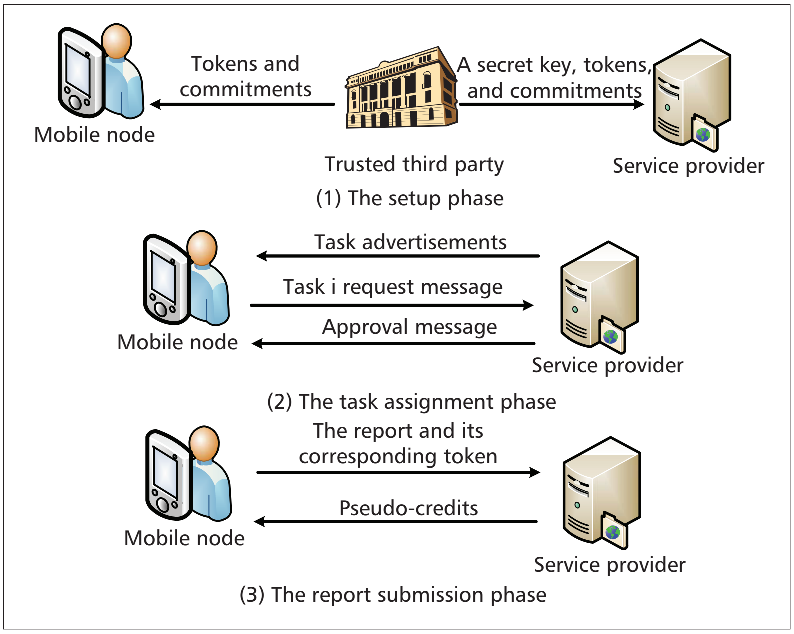

Figure 3. Information processing flow in the TTP-based scheme of [9].

tion, and the service provider then selects a predefined number of participants with the lowest bid prices. Those selected participants receive their bid prices as rewards for their participation. Each mobile node has its true cost of participation, which is private information. In order to gain positive utility from participation, each mobile node is expected to submit a bid price which is higher than its cost. This simple reverse auction suffers from the problem of *incentive cost explosion*, in which mobile nodes with high costs eventually drop out of the auction. Such dropping out of mobile nodes reduce price competition among the remaining nodes, who can afford to increase their bids in future auction rounds and yet are still selected by the service provider. As a result, the total reward paid by the service provider explodes.

To address this problem, the authors of [10] design a mechanism which, in each auction round, awards some virtual credits to those mobile nodes who are not selected. Then, when selecting participants in each auction round, the selection criterion used by the service provider is the competition bid prices, which is the actual bid price minus the accumulated virtual credits. The selected participants are awarded according to their bid prices. This mechanism increases the probability of previously rejected nodes being chosen and hence encourages their continuous participation. Simulation results have shown that the total reward made by the service provider is reduced. Note that enforcing truth-telling is not an objective of this work.

In [11] Yang *et al.* consider two types of incentive mechanisms: *platform-centric* and *user-centric*. In the platform-centric incentive mechanism, the service provider offers a total reward R for a single task to a set of participants. The level of participation of mobile node i is represented by the number of time units t_i that it is willing to provide the sensing service. It is assumed that the sensing cost per unit time of each participant is known by all other participants. For a given R, the participants are playing a non-cooperative game in which the strategy of participant i is t_i. The problem of assigning tasks is modeled as a Stackelberg game, with the solution specifying the optimal value of R which maximizes the utility of the service provider, and the corresponding unique Nash equilibrium strategy profile of mobile nodes. The incentive to each participant is that it will earn a payment that is not less than its cost of sensing.

Alternatively, in the user-centric incentive mechanism, the sensing cost of each mobile node is kept confidential and only known to itself. When a mobile node is interested in participating in a task, it announces a reserve price, the lowest price at which it is willing to participate. Then, based on the bids submitted by mobile nodes, the service provider needs to select a subset of mobile nodes and determine the payment to each participant. This problem is modeled as a reverse auction with two objectives. First, in order to provide incentive to participants, the payment to an individual participant cannot be less than its reserve price. Second, the utility of the service provider (due to task completion) minus the total payment is maximized. This objective is to ensure that the service provider has incentive to operate the service. The authors of [11] solve this problem by a heuristic algorithm. Very importantly, the resultant payment mechanism has the desirable property that each mobile node truthfully sets its bid equal to its sensing cost because it cannot obtain a higher utility by doing otherwise. As a result, over-payment is implicitly controlled.

In [12] the above problem is significantly generalized. First, rather than selecting a subset of mobile nodes as participants, the service provider allocates tasks in a finer level. Mobile nodes can be allocated with different participation levels in terms of, for example, the number of sensing samples per unit time. Second, the service provider needs to fulfill a constraint of the quality of service (QoS) delivered to users. Since this QoS depends on the quality of data contributed by participants, when the service provider allocates tasks to participants, it takes into account the quality of their past contributed data. The author of [12] derives a mechanism that explicitly computes the payment and participation level for each mobile node, while minimizing the total payment. Moreover, the mechanism also ensures that each mobile node truthfully sets its bid equal to its sensing cost, and the payment to an individual participant is not less than its cost.

The works in [11, 12] require the concurrent presence of bidding mobile nodes for the service provider to execute the mechanism in each round of task assignment. They are offline approaches that deal with a static population of mobile nodes. In a practical environment, mobile nodes may join or leave the auction dynamically. In [13] Zhang *et al*. propose an online mechanism for the problem in [11] to distribute tasks to participants on their arrivals such that immediate decisions are made according to bids at those instants. The characteristics of these incentive schemes are summarized in Table 2.

	[10]	[11]-Platform-centric	[11]-User centric	[12]	[13]
Enforce truth-telling	No	Not relevant	Yes	Yes	Yes
Minimize over payment	Implicitly	Implicitly	Implicitly	Explicitly	Implicitly
Online/offline	Offline	Offline	Offline	Offline	Online
Task assignment	Coarse	Coarse	Coarse	Fine	Coarse

Table 2. Characteristics comparison among the reviewed incentive schemes.

Research effort can be channeled to define some general privacy metrics which can capture the level of privacy protection regardless of the application scenarios. Such metrics are useful to compare the performance of different privacy-preserving schemes.

PROSPECTS

Despite the proposed solutions to privacy-preservation and incentive mechanisms summarized in the previous sections, there are still challenging issues that require more research. Here we discuss some of the important ones.

Developing General Privacy Metrics: Currently, different metrics, criteria, or methods are used to evaluate the performance of different proposed privacy-preservation schemes. Ideally, a set of universal metrics should be available to quantify privacy. However, it would be very difficult, if not impossible, to define such metrics. Alternatively, research efforts can be channeled to define some general privacy metrics that can capture the level of privacy protection regardless of the application scenarios. Such metrics are useful to compare the performance of different privacy-preserving schemes.

Resisting Corrupted Data While Preserving Privacy: While it is important for PS systems to preserve participants' privacy, such systems are vulnerable to the corrupted data purposely submitted by malicious participants. As a possible way to address this problem, the service provider should have methods to evaluate the reliability of the data, e.g. using the reputation of individual participants. Moreover, for incentive mechanisms it is common to select participants based on their bids. It would be interesting to take into account the reputation of individual mobile nodes in the selection process.

Maintaining a Balance Between Privacy Preservation and Accountability: Alternatively, in order to ensure data trustworthiness, participants should be made accountable for their submitted data. Clearly, this requires the identities of participants to be disclosed and counteracts privacy-preserving schemes. Therefore, how to maintain an acceptable balance between privacy preservation and accountability is an important issue that needs to be addressed.

Designing Efficient Incentive Mechanisms: For incentive mechanisms, further research can be directed to improve existing mechanisms to be more efficient. For example, similarity of measurements from devices near each other can be considered when allocating tasks and deciding payments. This could reduce the payment made by the service provider and eliminate possible redundancy in measured data [12].

Developing Efficient Privacy-Preservation Methods: More work should be done to improve the efficiency of privacy-preservation methods. For example, although PEPSI [7] can offer node privacy and query privacy, it suffers from heavy communication and computation costs because its underlying pairing-based IBE method involves bilinear pairing, which is known as a costly operation against the operations executed in elliptic curve groups.

Privacy and Reward Claiming: From the above reviewed works, we learn that privacy and payment determination are two orthogonal problems and their solutions can be designed independently. However, we do need to consider how privacy is preserved when participants claim their entitled rewards, and how rewards can be correctly distributed when privacy is preserved. For example, with the protection of anonymity, credits may be claimed by a greedy user who uses different anonymous identifiers to submit many duplicated reports for the same sensing task, or a malicious user who steals and uses other users' credentials. Although the methods described above address these two interplaying issues, they suffer from some security weaknesses and efficiency problems. For example, the method in [8] relies on the existence of a TTP. Also, the method in [9] is designed for a special scenario in which each sensing task only requires one report from each user. Thus, more novel solutions are required.

Privacy in Incentive Mechanisms: Privacy is not only important in report submission and reward claiming, but also in incentive mechanisms. For example, users may not want their bid information to be known by others as this reflects their true valuations on the sensing tasks. Another example is that the service provider wants to protect the threshold payment. Thus, privacy preservation for both users and the service provider should be taken into account in the design of incentive mechanisms. Recently, researchers started addressing this issue [14].

CONCLUSION

Privacy preservation and incentives are two factors that can hinder the large-scale deployment of people-centric sensing. In this article we have reviewed a number of proposed solutions to these two issues, and suggested some future research directions. We hope this article will stimulate more research from the community.

Privacy is not only important in report submission and reward claiming, but also in incentive mechanisms. For example, users may not want their bid information to be known by others as this reflects their true valuations on the sensing tasks.

Acknowledgment

This research is supported by a strategic research grant from City University of Hong Kong (project no. 7004429), the Pearl River Nova Program of Guangzhou (no. 2014J2200051), the National Science Foundation of China (grant no. 51477056), the Shanghai Knowledge Service Platform for Trustworthy Internet of Things (no. ZF1213), the Shanghai Rising-Star Program (no. 15QA1401700), and a visiting scholar project of the State Key Laboratory of Power Transmission Equipment & System Security and New Technology (no. 2007DA10512713406).

References

[1] IDC, "Worldwide Smartphone Shipments Top One Billion Units for the First Time, According to IDC," press release, 27 Jan 2014.

[2] N. Maisonneuve, M. Stevens, and B. Ochab, "Participatory Noise Pollution Monitoring using Mobile Phones," *Information Policy*, vol. 15, no. 1–2, 2010, pp. 51–71.

[3] S. Mathur *et al*., "Parknet: Drive-by Sensing of Road-Side Parking Statistics," *Proc. ACM MobiSys*, 2010, pp. 123–36.

[4] C. Cornelius *et al.*, "AnonySense: Privacy-Aware People-Centric Sensing," *Proc. ACM MobiSys.*, 2008, pp. 211–24.

[5] K. L. Huang, S. S. Kanhere, and W. Hu, "Preserving Privacy in Participatory Sensing Systems," *Comput. Commun*., vol. 33, no. 11, Jul. 2010, pp. 1266–80.

[6] R. Caceres, L. P. Cox, H. Lim, A. Shakimov, and A. Varshavsky, "Virtual Individual Servers as Privacy-Preserving Proxies for Mobile Devices," *Proc. MobiHeld Workshop*, 2009., pp. 37–42

[7] E. De Cristofaro and C. Soriente, "Extended Capabilities for a Privacy-Enhanced Participatory Sensing Infrastructure (PEPSI)," *IEEE Trans. Inf. Forens. Security*, vol. 8, no. 12, Dec. 2013, pp. 2021–33.

[8] J. Zhang *et al.*, "A Novel Privacy Protection Scheme for Participatory Sensing with Incentives," *Proc. IEEE CCIS*, 2012, pp. 1017–21.

[9] Q. Li and G. Cao, "Providing Privacy-Aware Incentives for Mobile Sensing," *Proc. IEEE PerCom*, 2013, pp. 76–84.

[10] J.-S. Lee and B. Hoh, "Dynamic Pricing Incentive for Participatory Sensing," *Pervasive and Mobile Computing*, vol. 6, no. 6, Dec. 2010, pp. 693–708.

[11] D. Yang *et al.*, "Crowdsourcing to Smartphones: Incentive Mechanism Design for Mobile Phone Sensing," *Proc. ACM MobiCom*, 2012, pp. 173–84.

[12] I. Koutsopoulos, "Optimal Incentive-driven Design of Participatory Sensing Systems," *Proc. IEEE INFOCOM*, 2013, pp. 1402–10.

[13]X. Zhang *et al*., "Free Market of Crowdsourcing: Incentive Mechanism Design for Mobile Sensing," *IEEE Trans. Parallel Distrib. Syst*., vol. 25, no. 12, Dec. 2014, pp. 3190–3200.

[14] J. Sun and H. Ma, "Privacy-Preserving Verifiable Incentive Mechanism for Online Crowdsourcing Markets," *Proc. IEEE ICCCN*, 2014, pp. 1–8.

Biographies

Daojing He (S'07, M'13) received his B.Eng. (2007) and M.Eng. (2009) degrees from Harbin Institute of Technology, P.R. China, and his Ph.D. degree (2012) from Zhejiang University, P.R. China, all in computer science. He is currently a professor at the Software Engineering Institute, East China Normal University, P.R. China. His research interests include network and systems security. He is an associate editor or on the editorial boards of several international journals such as *IEEE Communications Magazine* and *IEEE/KICS Journal of Communications and Networks*.

Sammy Chan (S'87-M'89) received his B.E. and M.Eng.Sc. degrees in electrical engineering from the University of Melbourne, Australia, in 1988 and 1990, respectively, and a Ph.D. degree in communication engineering from the Royal Melbourne Institute of Technology, Australia, in 1995. From 1989 to 1994 he was with Telecom Australia Research Laboratories, first as a research engineer, and between 1992 and 1994 as a senior research engineer and project leader. Since December 1994 he has been with the Department of Electronic Engineering, City University of Hong Kong, where he is currently an associate professor.

Mohsen Guizani (S'85, M'89, SM'99, F'09) received the B.S. (with distinction) and M.S. degrees in electrical engineering, and the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is currently a professor and Chair of the Electrical and Computer Engineering Department at the University of Idaho, USA. He was a professor and the Associate Vice President for Graduate Studies at Qatar University, Doha, Qatar. He was the Chair of the Computer Science Department at Western Michigan University, Kalamazoo, MI, USA, from 2002 to 2006, and the Chair of the Computer Science Department at the University of West Florida, Pensacola, FL, USA, from 1999 to 2002. He has held academic positions at the University of Missouri-Kansas City, MO, USA; the University of Colorado-Boulder, CO, USA; Syracuse University, Syracuse, NY, USA; and Kuwait University, Kuwait City, Kuwait. His research interests include computer networks, wireless communications and mobile computing, and optical networking. He currently serves on the editorial board of six technical journals and is the founder and the editor-in-chief of the *Wireless Communications and Mobile Computing Journal* published by John Wiley. He is the author of eight books and more than 300 publications in refereed journals and conferences. He has guest edited a number of special issues in IEEE journals and magazines. He has also served as a member, Chair, and General Chair of a number of conferences. He has served as the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of TAOS Technical Committee. He was an IEEE Computer Society Distinguished Lecturer from 2003 to 2005. He is a Senior Member of the ACM.