USER PRIVACY AND DATA TRUSTWORTHINESS IN MOBILE CROWD SENSING

DAOJING HE, SAMMY CHAN, AND MOHSEN GUIZANI

ABSTRACT

Smartphones and other trendy mobile wearable devices are rapidly becoming the dominant sensing, computing and communication devices in peoples' daily lives. Mobile crowd sensing is an emerging technology based on the sensing and networking capabilities of such mobile wearable devices. MCS has shown great potential in improving peoples' quality of life, including healthcare and transportation, and thus has found a wide range of novel applications. However, user privacy and data trustworthiness are two critical challenges faced by MCS. In this article, we introduce the architecture of MCS and discuss its unique characteristics and advantages over traditional wireless sensor networks, which result in inapplicability of most existing WSN security solutions. Furthermore, we summarize recent advances in these areas and suggest some future research directions.

INTRODUCTION

Since the introduction of Apple's iPhone, mobile phones have evolved into *smartphones*. Supported by advances in mobile and wireless communication technologies such as third/fourth generation (3G/4G) and Wi-Fi, smartphones have better networking capabilities, allowing them to transmit data at higher rates. Moreover, they are equipped with more processing power and storage capacities. More important, they are programmable. A myriad of paid or free applications (often referred to as *apps*) are available to be downloaded in a convenient manner. Overall, this evolution makes mobile phones so powerful that many novel applications can be executed on them. Moreover, recently, devices equipped with similar capabilities are emerging as wearable accessories (e.g., Google Glass and Galaxy Gear). All together, they are referred to as *mobile wearable devices.*

Another important feature of mobile wearable devices is, as shown in Fig. 1, that they come with a growing set of powerful embedded sensors, such as gyroscope, accelerometer, microphone, digital compass, and camera. Based on these sensors, a variety of sensing applications can be executed on mobile wearable devices; among them mobile crowd sensing (MCS, also known as participatory sensing or people-centric sensing) is a prominent family. MCS relies on individual participants to collect data from their activities and surrounding environments by their wearable devices, and then upload the data to the application server via any available networking facility. The application server will process all data reported by the participants, extract the information in which queriers are interested, and forward such information to the queriers.

The emergence of MCS has led to the development of a wide range of novel applications. In general, these applications can be classified under different categories such as healthcare, business, environment, transportation, and social networking. For example, there are MCS applications that collect and share information about air quality and noise level in urban areas, dietary patterns, and oil prices. More specific example applications include Micro-Blog [1], which allows users to feed sensed data from their surroundings to multimedia blogs, and Vtrack, which estimates travel time based on timestamped positions collected by position sensors of smartphones. Also, in personal health monitoring, wearable accelerometers are used to monitor the physiological state and health of patients/participants.

Although a lot of research and development activities on MCS have taken place, they mainly focus on new applications and the solution of data collection. There are a number of other issues that need to be addressed. Among these are user privacy and data trustworthiness. As MCS applications involve data collection across wide geographical areas, spatial-temporal information is invariably associated with the data uploaded by participants. This imposes possible threats to user privacy because the collected data may disclose their locations and trajectories. Other possible privacy invasions include recording intimate discussions and capturing private scenes. Such threats would discourage people from becoming participants in MCS. Since altruistic data collection is a critical element of MCS, this issue of privacy invasion needs to be addressed immediately before the success of MCS is explored further.

Another security issue of MCS is the reliability of the uploaded data. As data are reported by participants, they could possibly be falsified. Hence, this raises the issue of data trustworthi-

Daojing He is with East China Normal University.

Sammy Chan is with City University of Hong Kong, Kowloon.

Mohsen Guizani is with Qatar University.

1536-1284/15/$25.00 © 2015 IEEE

ness. Furthermore, this issue inherently conflicts with the privacy issue. This is because if participants' identities are not disclosed, those participants reporting falsified or even fabricated data cannot be identified and eliminated. In other words, if full anonymity is provided to MCS participants, guaranteeing the trustworthiness of reported data is difficult. Hence, data trustworthiness in MCS becomes more crucial than in traditional wireless sensor networks (WSNs), which deploy a large number of wireless sensor devices managed by the network owner.

In the remainder of this article, we first give an overview of MCS, and discuss its unique characteristics and advantages over traditional WSNs. Then we discuss how adversaries can invade user privacy and corrupt the reported data. Subsequently, we review some recent works that address these two issues, and suggest some future research directions.

Mobile Crowd Sensing

Architecture of MCS

Note that different MCS applications may have different system models. To make it more general, here we consider a typical MCS architecture as shown in Fig. 2, which has three stages: *sensing, learning and mining, disseminating*. In the sensing stage, before the owner of a mobile wearable device can participate in an MCS application, he/she first needs to download the corresponding app published by end users from the appropriate channel, e.g., Apple's App Store or Google's Play Store. After installing and running the app, he/she becomes a participant. For a certain query, the application server informs all participants about their sensing tasks. Then, the app starts collecting data using the relevant sensors. In the learning and mining stage, there are two possible data collection models. In the first model, participants play an active role by deciding when to report data. In the second model, reporting occurs whenever the state of the mobile wearable device satisfies the tasks' requirements. So, the sensed data are uploaded to the application server through Wi-Fi or cellular networks. The application server then processes the sensed data to extract the desired information using techniques such as machine learning and data mining. In the disseminating stage, the results are formatted into suitable forms and made available to queriers. The role of each entity of an MCS system is summarized in Table 1.

Unique Characteristics and Advantages of MCS over WSNs

Although MCS is also based on a network of sensors, it has unique characteristics and advantages over WSNs as tabulated in Table 2.

First, different from WSNs, the sensors in MCS are housed in mobile wearable devices belonging to voluntary participants. With a large number of participants, MCS can provide fine-grained monitoring of interested parameters without setting up the sensing infrastructure beforehand. Moreover, with the proliferation of mobile wearable devices and the ubiquity of wireless broadband connections, MCS can operate in an environment which is not feasible or economical for WSNs. Second, since mobile wearable devices have much more resources than sensor nodes in terms of computing power, memory, and energy, more requirements can be met by MCS applications. Third, sensing devices in MCS are mobile in nature. Therefore, they can collect spatio-temporal data in a much easier way than traditional WSNs. Fourth, the sensing process is more intelligent as participants can take control of the sensing process. Fifth, sometimes WSNs have high installation and maintenance cost, and possibly insufficient node coverage. However, as MCS leverages existing sensing devices and communication infrastructure, there is virtually no establishment cost.

Figure 1. Sensors on typical mobile wearable devices.

Challenges of MCS over WSNs

Due to the unique characteristics of MCS systems shown in Table 2, many of the solutions for preserving user privacy and data trustworthiness for WSNs are not applicable. Here, we illustrate this by considering two features, data generator and owner, as examples. In a traditional WSN, the network owner configures and deploys his/her own sensor nodes as a wireless ad hoc network to collect the desired data. The nodes only sense the surrounding environment but not human behavior. The main security concerns of WSNs are interception or modification of data in transit, disruption of routing packets, and illegal retasking of nodes. On the other hand, the network infrastructure used by an MCS system is usually not owned by the MCS operator, participants, or queriers. Thus, none of these parties will necessarily trust the network infrastructure. Moreover, the MCS operator and queriers may not trust the sensor nodes or their owners. As a result, the trust models would be more complex than those adopted in WSNs.

Since MCS relies on the participation of third-party participants, the first new challenge in MCS applications is how to encourage owners of mobile wearable devices to actively participate in data collection. Second, in some existing MCS applications [1], data uploaded by participants may contain their private and sensitive informa-

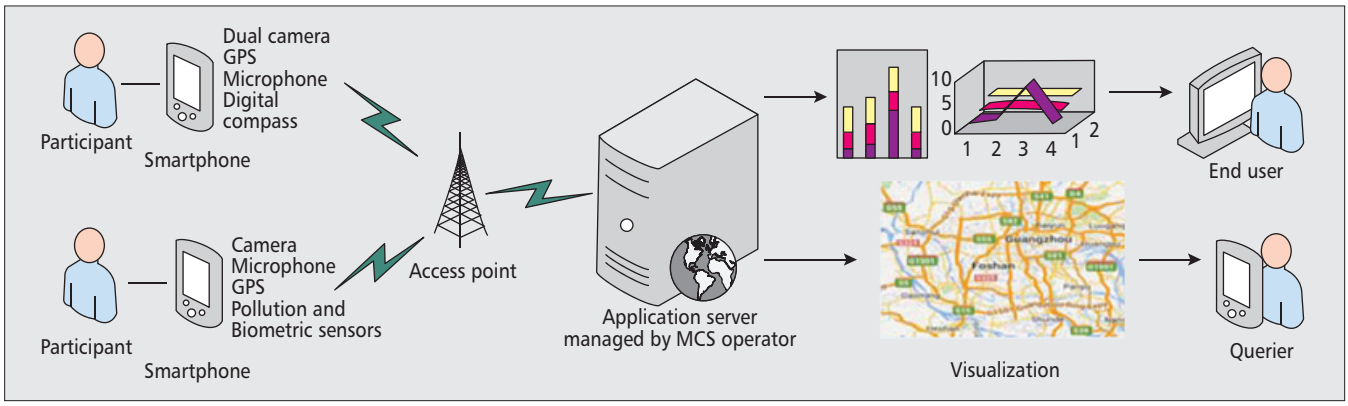

Figure 2. The architecture of a typical mobile crowd sensing application.

tion. The second new issue is how to protect the privacy of the participants. Moreover, since sensor data originate from third parties, falsified data may be reported. How to ensure data trustworthiness is another issue that WSNs do not have. In the next section, we outline specific attack models regarding user privacy and data trustworthiness.

Problem Statements and Attack Models on User Privacy and Data Trustworthiness

Problem Statements on User Privacy

In a typical MCS application, the sensing data uploaded by participants are invariably tagged with important contextual information such as sensing location and time. Clearly, disclosure of this information can have serious implications on participants' privacy. Moreover, multiple reports from the same participant can be linked to extract more private information such as the location of his/her home and/or office.

Attack Models on User Privacy

In MCS, privacy concerns arise due to the disclosure of private information such as participants' identities, IP addresses, locations, trajectories, and lifestyle-related information. MCS applications even aggravate the privacy problem because they make large volumes of information easily available through remote access. Thus, adversaries need not be physically present to maintain surveillance. They can gather information in a low-risk and anonymous manner. Remote access also allows a single adversary to monitor multiple users simultaneously. We consider users' location information as an example. Consider a scenario where the goal of an MCS application is to collect pictures or short videos from riots occurring in different parts of a city. Each participant would first send a query to the application server for the set of nearby locations from which data collection is needed. If a participant is not willing to disclose his/her identity, the query can be sent to a trusted sever, which removes the ID from the query and then forwards it to the application server. However, the application server still needs to know the location information of the participant in order to answer the query. Due to the strong correlation between participants and their movements, a malicious server can identify a participant from his/her location information [2]. Some of the more common attacks against privacy are:

- Monitor and eavesdrop: This is the most direct attack to privacy: the adversary just listens to the data to learn the communication content.
- Traffic analysis: Based on monitoring and eavesdropping, traffic can be analyzed. Through the analysis process, some participants with special roles or activities can be effectively identified.
- Collusion: Several attackers (e.g., end users) might collude to correlate the information of participants for de-anonymization. A malicious end user might orchestrate multiple applications in an attempt to extract more private information from the collected data.

From the gathered reports containing location information of participants, the following three types of attacks can be pursued by adversaries:

- User identification attacks: to expose the identities of users who issue queries about a spatial region.
- Sensitive location tracking: to identify the locations that a participant has often visited. From this information, more specific information about the user, such as health, lifestyle, and habits, can be revealed.
- Sequential tracking attacks: to track down a participant by issuing a set of queries that involve spatio-temporal regions adjacent to each other. Then the participant's trajectories are analyzed to identify the places he/she has visited [3].

Also, a task management paradigm is needed in MCS to define tasks according to the requirements of end users, distribute tasks, and coordinate participants until task completion. A major challenge in task management is to ensure a certain level of privacy for participants, which would then encourage owners of mobile wearable devices to become participants, receive tasks, and contribute data. Privacy attacks in MCS task management include task tracing attacks and location-based inference attacks:

- Task tracing attacks: When a participant selects tasks or shares his/her preferences during the assignment of a coordinated task, he/she may disclose some attributes such as

location, time, and task types in which he/she is interested. Although such information alone may not breach his/her privacy, dispatching multiple concerted tasks might allow an adversary to correlate the information and consequently reveal the participants' identities or other sensitive attributes.

- Location-based inference attacks: Spatial tasks that are frequently carried out by a participant would disclose his/her private information such as home address or eventually his/her identification via inference attacks.

Problem Statements on Data Trustworthiness

Since MCS allows any voluntary participant to contribute data, the application server is exposed to erroneous or even malicious data. For example, participants may inadvertently put their wearable devices in an undesirable position while collecting sensor readings (e.g., Galaxy Gear kept in a pocket while sampling street-level noise). Moreover, malicious participants may deliberately contribute bad data. Both behaviors result in erroneous contributions, which need to be identified and eliminated to ensure the reliability of the computed summaries. For this purpose, some reputation systems tailored to MCS have been proposed [4–8]. They initially establish reputation scores of the participants based on the quality of their contributions, and later on use these scores to eliminate contributions from less reputable participants.

To establish the reputation of a participant, these systems [4–8] need to observe his/her contributions for an extended period of time and require linkability across multiple contributions. Since the sensing data usually contain spatio-temporal information, an adversary can de-anonymize the volunteers and hence compromise their privacy by exploiting these links. Thus, the main goal of data trustworthiness research is how to address this inherent conflict between user privacy and reputation requirements.

Attack Models on Data Trustworthiness

In MCS environments, an adversary does not need to capture a mobile wearable device before sending falsified data; it can simply act as a participant and report falsified data.

- Erroneous and malicious contributions: Unfortunately, MCS openness can allow any participant to contribute data, which means that applications may receive erroneous and malicious contributions. For example, participants may purposely record incorrect measurements by placing their mobile wearable devices in inappropriate positions. In addition, malicious participants may pollute reports for their own benefit (e.g., an estate agent may contribute artificially generated low noise readings to promote the properties in his/her portfolio) [4].
- Collusion attacks: In the current reputation systems of MCS, every participant can publish false reports to the application server and provide arbitrary feedback about the trust values during the process of reputation voting. Furthermore, adversaries can even collude to disrupt MCS applications. Such an attack is difficult to handle and certainly severely degrades the accuracy of the trust evaluation.

Participants	Measuring the required data about a subject of interest using mobile wearable devices.
End users or queriers	Requesting data through tasks and then utilizing the information acquired by participants.
MCS operator	Distributing tasks to participants who meet the requirements of applications. In certain architectures, end users or queriers can also act as MCS operators.

Table 1. Roles of entities of an MCS system.

	Wireless sensor networks	Mobile crowd sensing
Owner	Company or government	Individual
Sensor energy	Limited	Rechargable
Sensor mobility	Low	High
Sensing context	Physical phenomena only	Physical phenomena as well as human daily life
Data generator	Some specific environment (e.g., forest)	Humans and their surroundings
Sensors	Large volume of small devices, normally based on special hardware	Off-the-shelf devices (e.g., smartphone)
Scalability	Low	High
Cost	High	Low

Table 2. Traditional wireless sensor networks vs. mobile crowd sensing.

Recent Works on Privacy Preservation

Anonymization is the technique that removes identification information from all interactions between the participants and other entities of an MCS system. Below are two anonymization techniques.

1) Pseudonyms or suppressing user identity: These are basic and simple methods to make participants anonymous by replacing their identification information with pseudonyms or suppressing users' identities. However, these methods may not always work. For example, from a user's movement pattern, it is straightforward for an adversary to de-anonymize his/her reports. To address this challenge, some methods with the connection anonymization concept have been proposed in recent years for securing user privacy in MCS systems.

2) Connection anonymization: Such methods can be used to avoid some tracing attacks (e.g., network-based tracing attacks based on IP addresses). In [9], the authors attempted to achieve anonymity of users by using Mix Networks. A Mix Network is a statistical-based anonymizing infrastructure achieving the k-anonymity property,

IBE is used as the cryptographic primitive in PEPSI. Here, we assume that each report is identified by a set of labels. These labels are used as identities in an IBE scheme. Thus, mobile nodes can derive a unique public encryption key from such labels and use it to encrypt the reports to be transmitted to the service provider.

which ensures that the operator cannot identify the originator of each sensing record from a group of k or more participants. It routes reports via multihop transmission, adding delays and mixing with the data between different sources and destinations. It aims to prevent an adversary from linking all reports of a mobile node, identifying which mobile node sent the report, and learning when and where the reports were generated. Unfortunately, Mix Networks are unsuitable for many MCS settings. On one hand, they do not attain provable privacy guarantees. On the other hand, the degree of confidentiality is relatively limited: reports are encrypted under the public key of the so-called report server (RS) — a trusted party collecting reports and distributing them to queriers. In that case, the RS may learn both sensors' reports and the interest of queriers.

To address these challenges, Gao *et al.* enhanced the framework in [9] by replacing the Mix Network with a trusted third party server [10]. With the removal of the Mix Network, transmission of data reports can be optimized. The trusted third party server functions as a privacy-preserving agent, which trades off the efficiency of data transmission and privacy protection. Moreover, the authors proposed a method to protect participants' identities and trajectories privacy from the perspective of graph theory based on the mix-zones model and pseudonym techniques.

Note that connection anonymization may not be suitable for those applications that require fine-grained information. For example, for the application that collects information from riots as discussed earlier, a report generated by a participant at one particular location will only be annotated with a region encompassing other k – 1 participants rather than the exact location of the participant. Then this report conveys little information to the application server as the latter cannot ascertain which location is being referred to by the report.

The architectures of [8, 10] store the reports in a centralized database. In [3], it is considered that each mobile node maintains its own local database. The authors in [3] developed a privacy-preserving MCS system, LOCATE, for Android-based devices. LOCATE allows users to sense and store data locally, and issue queries about data across the whole system. They assume that user-sensitive data can be derived from users' trajectories. Therefore, LOCATE is equipped with a data exchange approach that enables users to disclose their trajectories without compromising their privacy. The main idea is to distribute user data trajectories among multiple users within the system based on the local entropy so that all trajectories are equiprobable to be sensitive data. Their approach can defend against common attacks in MCS applications as well as attacks specifically arising from the use of the Android operating system.

Some existing privacy preserving approaches [11–13] rely on the existence of a trusted infrastructure (usually a private server or a service provider), but the establishment and maintenance of this entity in a distributed environment is not trivial. Moreover, in MCS, the data are usually collected/analyzed by service providers, which may possibly disclose the private information of each participant. Caceres *et al.* [11] argued that privacy can be protected if each user has access to a private server and uses it as a proxy between itself and the application server. In [12], a privacy-enhanced architecture for MCS applications, PEPSI, was proposed. In the architecture of PEPSI, as shown in Fig. 3, there is a service provider that manages MCS applications. Mobile nodes send reports of sensed data to the service provider, which, after some processing, forwards the reports to the queriers. PEPSI also involves another entity referred to as a registration authority. It is responsible for the initial setting of system parameters, and handles the registration of mobile nodes and queriers. Since one of the main objectives of PEPSI is to hide reports of sensed data and queries from unconcerned parties, reports and queries are all encrypted.

Identity-based encryption (IBE) is used as the cryptographic primitive in PEPSI. Here, we assume that each report is identified by a set of labels. These labels are used as identities in an IBE scheme. Thus, mobile nodes can derive a unique public encryption key from such labels and use it to encrypt the reports to be transmitted to the service provider. During registration, mobile nodes register these labels to a registration authority, which then acts as the private key generator of the IBE scheme. It generates the private decryption key corresponding to those labels, and passes the private key to the interested queriers upon their registration. Another feature of PEPSI is that the service provider does not just relay all reports to all queriers. This would incur heavy processing load in queriers because they need to try all their private keys in order to decrypt a report. Instead, the service provider imposes a tagging mechanism by which it can efficiently match the reports with queries. The mechanism requires mobile nodes to tag each report with a cryptographic token that identifies the report type only to authorized queriers, without leaking any information of the report. The tag is computed from the same labels used to derive the public key. At the same time, due to the properties of bilinear mapping inherent in IBE, queriers can compute the same tag for the same report using their private encryption keys and provide the tag to the service provider when they make a query subscription. Then the service provider only forwards a tagged report to those queriers that have provided the same tag.

Shi *et al.* [13] focused on privacy-preserving data aggregation in MCS. They proposed a scheme called PriSense, which provides an additive aggregation function. It requires each mobile node to slice its data into, say, $n + 1$ slices. Then it randomly chooses n other nodes and sends a unique data slice to each of the n nodes. Upon a request from the aggregation server, each node returns the remaining slice together with other slices received from other nodes. This function prevents a node's data from being disclosed.

Similarly, Ganti *et al.* presented a privacy-preserving architecture for time-series data using data perturbation [14]. They demonstrate that the privacy of the data can be preserved if the noise used to perturb the data is itself generated from a process that approximately models the data.

When the sensing data evolve from simple parameters (e.g., velocity, temperature) to multimedia data (e.g., image and video files), the data volume increases substantially. Unfortunately, due to this increase, the existing privacy preserving schemes are not suitable for MCS applications involving multimedia data because high communication cost would be incurred or the utility/accuracy of the data would be degraded. Qiu *et al.* [15] addressed this problem by developing a *k*-anonymous privacy preserving scheme, SLICER, for MCS applications with multimedia data. Based on erasure coding and efficient slice transfer strategies, SLICER achieves strong privacy preservation and high tolerance to data loss, and also has low computation and communication overhead. However, some related issues, such as privacy preservation in the query process, were not considered in [15].

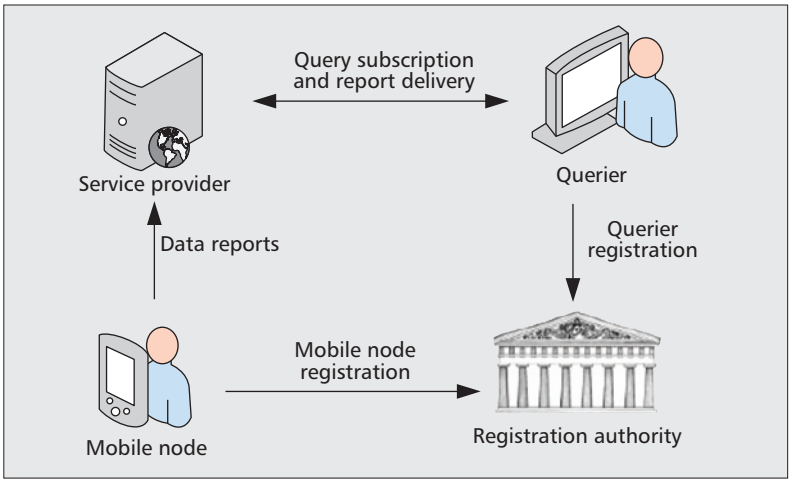

Figure 3. The architecture of PEPSI.

Recent Works on Data Trustworthiness

Trust systems for data reliability have been widely used for a wide range of networks such as the Internet, mobile ad hoc networks, peer-to-peer networks, and WSNs. However, most of them are inapplicable for MCS systems due to the special characteristics of MCS systems mentioned earlier. Recent research on data trustworthiness in MCS can be found in [4–8]. These systems focus on how to evaluate the trustworthiness of the shared data and how to maintain the reputation of data processing network entities. In particular, Huang *et al.* [4] proposed a reputation system based on the Gompertz function to compute reputation scores of devices to measure the trustworthiness of the contributed data. However, it does not take privacy preservation into account.

More recently, several reputation schemes that are privacy-aware have been proposed [5–8]. Some of the approaches [5, 6] rely on the existence of a trusted third party, but the establishment and maintenance of this entity in a distributed environment is not trivial. In the scheme of [5], multiple pseudonyms are assigned for each participant. A trusted server is required to manage the mapping between the real identity of a participant and his/her pseudonyms, and transfer reputation values between different pseudonyms. Compared to other methods, this method does not require expensive cryptographic operations and has low communication overheads. Also, Dua *et al.* [6] proposed and implemented a trusted platform module (TPM), which is a micro-controller embedded within each mobile device, to attest the integrity of sensor readings. However, TPM chips are not yet widely adopted in mobile devices.

Some methods that do not rely on the existence of a trusted third party have been proposed. In [7], an anonymity-preserving reputation solution called IncogniSense was proposed. It generates periodic pseudonyms using blind signatures, and cloaks exact reputation values dynamically into reputation groups. The assumption that the manager of reputation and pseudonym must be trusted is eliminated. However, additional management overhead is incurred. For example, the solution depends on a redundant number of participants and incurs heavy communication overheads. Li *et al.* [8] proposed another solution based on blind signature techniques. The authors considered the problem from the point of view of incentive, and aim to allow participants to earn credits through contributing data without leaking the details of the data. Thus, the necessity to penalize malicious participants does not need to be considered.

Also, making use of the fact that multiple information sources are usually available in a network, Wang *et al.* [16] proposed to assess the similarity of multiple pieces of information from different sources about the same event and then adjust the trust scores of each piece of information. Based on the trust evaluation, the trust scores of nodes can also be dynamically adjusted.

Future Directions

The problems of user privacy and data trustworthiness are quite new. Notwithstanding the recently proposed works, much remains to be done. Some future directions for each problem are suggested below.

User Privacy

- Protecting query privacy with respect to the registration authority.
- Protecting node privacy with respect to the network operator. With the current technology, users' locations and identities are not allowed to be hidden from the network operator.
- Addressing collusion attacks, which invade the privacy of mobile nodes or queriers through collaboration. While available cryptographic techniques support simple aggregate function evaluation over encrypted data, enabling efficient evaluation of complex predicates is still an open challenge [12].
- Currently, different privacy-preservation schemes are evaluated by different metrics or criteria. It is useful to have some general privacy metrics based on which the performance of different schemes are compared. Ideally, such metrics should quantify privacy. However, defining such metrics would be very difficult, if not impossible. To tackle this problem, perhaps researchers could first aim to define some met-

If participants are malicious, they would provide falsified data and it is difficult to identify them especially when different task actions are not linked due to privacy protection. The simple solution that assigns a task to multiple participants simultaneously to reduce the effect of malicious participation just consumes too many resources.

rics that capture the level of privacy protection independent of the application scenarios.

Data Trustworthiness

Data trustworthiness and user privacy preservation are two conflicting objectives in an MCS application. Strong mechanisms for protecting privacy might influence data trustworthiness. On the other hand, protecting the data trustworthiness counteracts the mechanisms for preserving privacy. Therefore, a trade-off between safeguarding user privacy and ensuring data trustworthiness is necessary. Future work should focus on how to employ some simple cryptographic operations to transfer a reputation value (which is a proxy for assessing data trustworthiness) between anonymous contributions without the involvement of any trusted third party and high communication overheads. Also, recent studies [5] have shown if the user reputation is used as a proxy to assess data trustworthiness, user reputation can inadvertently leak user privacy in the context of MCS. Thus, a good privacy-preserving reputation system for MCS should consider the linkability exposed by reputation values. Moreover, although participants' reputations can be used to enhance the reliability of the sensed data they provide, it remains a research challenge to develop a unified and fair approach to adjust participants' reputation scores based on their performance in different applications.

Trust is also an issue for anonymous tasking since tasks are assigned to unknown participants. If participants are malicious, they would provide falsified data, and it is difficult to identify them, especially when different task actions are not linked due to privacy protection. The simple solution that assigns a task to multiple participants simultaneously to reduce the effect of malicious participation just consumes too many resources. More effective solutions are needed.

Conclusion

MCS is an innovative computing paradigm that bears great potential and can lead to a wide range of novel applications relating to, for example, environmental monitoring, transportation, and entertainment. In this article, we have presented the advantages of MCS over traditional WSNs. At the same time, we have also identified two important challenges of MCS, user privacy and data trustworthiness. They are the two major barriers to the success and massive deployment of MCS systems. It is important to overcome these challenges in order to move this field forward.

Acknowledgment

This research is supported by a strategic research grant from City University of Hong Kong [Project No. 7004225], the Pearl River Nova Program of Guangzhou (No. 2014J2200051), the National Science Foundation of China (Grants: 51477056 and 61021004), the Shanghai Knowledge Service Platform for Trustworthy Internet of Things (No. ZF1213), Shanghai Rising-Star Program (No. 15QA1401700), and the Specialized Research Fund for the Doctoral Program of Higher Education. Daojing He is the corresponding author of this article.

References

[1] S. Gaonkar *et al.*, "Micro-Blog: Sharing and Querying Content Through Mobile Phones and Social Participation," *Proc. ACM MobiSys*, 2008, pp. 174–86.
[2] P. Narula *et al.*, "Security in Mobile Ad-Hoc Networks Using Soft Encryption and Trust-Based Multi-Path Routing," *Comp. Commun.*, vol. 31, no. 4, Mar. 2008, pp. 760–69.
[3] I. Boutsis and V. Kalogeraki, "Privacy Preservation for Participatory Sensing Data," *Proc. IEEE PerCom*, Mar. 2013, pp. 103–13.
[4] K. L. Huang, S. S. Kanhere, and W. Hu, "Are You Contributing Trustworthy Data? The Case for a Reputation System in Participatory Sensing," *Proc. ACM MSWiM*, 2010, pp. 14–22.
[5] L. K. Huang, S. K. Salil, and H. Wen, "A Privacy-Preserving Reputation System for Participatory Sensing," *Proc. IEEE LCN*, 2012, pp. 10–18.
[6] A. Dua *et al.*, "Towards Trustworthy Participatory Sensing," *Proc. USENIX HotSec.*, 2009, pp. 1-6.
[7] D. Christin *et al.*, "IncogniSense: An Anonymity-Preserving Reputation Framework for Participatory Sensing Applications," *Pervasive and Mobile Computing*, vol. 9, no. 3, 2012, pp. 353–71.
[8] Q. Li, G. Cao, and T. La Porta, "Efficient and Privacy-Aware Data Aggregation in Mobile Sensing," *IEEE Trans. Dependable Sec. Comp.*, vol. 11, no. 2, Mar.–Apr. 2014, pp. 115–29.
[9] C. Cornelius *et al.*, "AnonySense: Privacy-Aware People-Centric Sensing," *Proc. ACM MobiSys.*, 2008, pp. 211–24.
[10] S. Gao *et al.*, "TrPF: A Trajectory Privacy-Preserving Framework for Participatory Sensing," *IEEE Trans. Info. Forensics Security*, vol. 8, no. 6, June 2013, pp. 874–87.
[11] R. Caceres *et al.*, "Virtual Individual Servers as Privacy-Preserving Proxies for Mobile Devices," *Proc. MobiHeld Wksp.*, 2009, pp. 37–42.
[12] E. De Cristofaro and C. Soriente, "Participatory Privacy: Enabling Privacy in Participatory Sensing," *IEEE Network*, vol. 27, no. 1, Jan.–Feb. 2013, pp. 32–36.
[13] J. Shi *et al.*, "PriSense: Privacy-Preserving Data Aggregation in People-Centric Urban Sensing Systems," *Proc. IEEE INFOCOM.*, 2010, pp. 1–9.
[14] R. Ganti *et al.*, "PoolView: Stream Privacy for Grassroots Participatory Sensing," *Proc. ACM SenSys.*, 2008, pp. 281–94.
[15] F. Qiu, F. Wu, and G. Chen, "SLICER: A Slicing-Based *k*-Anonymous Privacy Preserving Scheme for Participatory Sensing," *Proc. IEEE MASS*, 2013, pp. 113–21.
[16] X. Wang *et al.*, "Collusion-Resilient Quality of Information Evaluation Based on Information Provenance," *Proc. IEEE SECON.*, 2011, pp. 395–403.

Biographies

DAOJING HE [S'07, M'13] (hedaojinghit@gmail.com) received his B.Eng.(2007) and M. Eng. (2009) degrees from Harbin Institute of Technology, China, and his Ph.D. degree (2012) from Zhejiang University, China, all in computer science. He is currently a professor in 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 some international journals such as *IEEE Communications Magazine* and *IEEE/KICS Journal of Communications and Networks*.

SAMMY CHAN [S'87, M'89] (eeschan@cityu.edu.hk) 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. He is an associate professor in the Department of Electronic Engineering, City University of Hong Kong.

MOHSEN GUIZANI [S'85, M'89, SM'99, F'09] (mguizani@ieee.org) is currently a professor and associate vice president for Graduate Studies at Qatar University. He received his B.S. (with distinction) and M.S. degrees in electrical engineering, and M.S. and Ph.D. degrees in computer engineering in 1984, 1986, 1987, and 1990, respectively, from Syracuse University, New York. His research interests include computer networks, wireless communications and mobile computing, and optical networking. He currently serves on the Editorial Boards of six technical journals and is the founder and Editor-in-Chief of the *Wireless Communications and Mobile Computing Journal* published by Wiley (http://www.interscience.wiley.com/jpages/1530-8669/). He is a Senior Member of ACM.