Aalto University

OPEN ACCESS

This is an electronic reprint of the original article.
This reprint may differ from the original in pagination and typographic detail.

Wang, Yongfeng; Yan, Zheng; Feng, Wei; Liu, Shushu

Privacy protection in mobile crowd sensing: a survey

Published in:
World Wide Web

DOI:
10.1007/s11280-019-00745-2

Published: 20/11/2019

Document Version
Publisher's PDF, also known as Version of record

Please cite the original version:
Wang, Y., Yan, Z., Feng, W., & Liu, S. (2019). Privacy protection in mobile crowd sensing: a survey. *World Wide Web*. https://doi.org/10.1007/s11280-019-00745-2

This material is protected by copyright and other intellectual property rights, and duplication or sale of all or part of any of the repository collections is not permitted, except that material may be duplicated by you for your research use or educational purposes in electronic or print form. You must obtain permission for any other use. Electronic or print copies may not be offered, whether for sale or otherwise to anyone who is not an authorised user.

World Wide Web
https://doi.org/10.1007/s11280-019-00745-2

Privacy protection in mobile crowd sensing: a survey

Yongfeng Wang[1,2] · Zheng Yan[1,3] · Wei Feng[1] · Shushu Liu[3]

Received: 1 May 2019 / Revised: 25 July 2019 / Accepted: 30 September 2019
Published online: 20 November 2019
© The Author(s) 2019

Abstract
The unprecedented proliferation of mobile smart devices has propelled a promising computing paradigm, Mobile Crowd Sensing (MCS), where people share surrounding insight or personal data with others. As a fast, easy, and cost-effective way to address large-scale societal problems, MCS is widely applied into many fields, e.g., environment monitoring, map construction, public safety, etc. Despite the popularity, the risk of sensitive information disclosure in MCS poses a serious threat to the participants and limits its further development in privacy-sensitive fields. Thus, the research on privacy protection in MCS becomes important and urgent. This paper targets the privacy issues of MCS and conducts a comprehensive literature research on it by providing a thorough survey. We first introduce a typical system structure of MCS, summarize its characteristics, propose essential requirements on privacy on the basis of a threat model. Then, we survey existing solutions on privacy protection and evaluate their performances by employing the proposed requirements. In essence, we classify the privacy protection schemes into four categories with regard to identity privacy, data privacy, attribute privacy, and task privacy. Besides, we review the achievements on privacy-preserving incentives in MCS from four viewpoints of incentive measures: credit incentive, auction incentive, currency incentive, and reputation incentive. Finally, we point out some open issues and propose future research directions based on the findings from our survey.

Keywords Mobile crowd sensing · identity privacy · attribute privacy · data privacy · task privacy · incentive mechanism

This article belongs to the Topical Collection: *Special Issue: Trust, Privacy, and Security in Crowdsourcing Computing*
Guest Editors: An Liu, Guanfeng Liu, Mehmet A. Orgun, and Qing Li

✉ Zheng Yan
zyan@xidian.edu.cn

Extended author information available on the last page of the article

1 Introduction

With the ubiquity of mobile smart devices and the development of wireless communication technology, an increasing number of people are entitled to share observations or personal insight with others, which stimulates the emergence of Mobile Crowd Sensing (MCS) [22]. The key intuition of MCS is to motivate ordinary citizens to execute tasks and contribute data by using smart devices (such as smart phones and mobile wearable devices), the sensors installed on which can sense vast quantities of useful data. As an open system, MCS employs mobile devices as the sensors, therefore, any mobile users can provide data collecting service in MCS. Besides, as the combination of mobile communication and traditional online crowdsourcing, MCS provides a fast, easy, and cost-effective way to address large-scale societal problems. Thus, it has gained great attention from both academia and industry and been widely adopted in many fields. For instance, CarTel system [32] is one MCS network using automobile sensors to collect and deliver traffic patterns. VTrack system [1] was designed to estimate Road Traffic Delay. Location data is also utilized to calculate personalized estimates of environmental impact [54].

Despite the popularity of MCS, the privacy risk is a crucial issue to the public. Since malicious attackers can easily infer private information about MCS entities, such as age and home address from transmitted messages, like task contents, node attributes, and collected data, which poses a serious threat to the participants. Therefore, it is urgent to provide privacy protection for MCS participants. However, privacy preservation in MCS is non-trivial as MCS involves a variety of entities and different entities have different privacy requirements. Besides, the openness of MCS makes it vulnerable to various attacks especially malicious tasking since an attacker can easily join MCS as a data consumer or a data provider.

Many efforts have been made to explore privacy issues in MCS and current privacy solutions cover most of the procedures. However, users find it overwhelmed when they try to deploy such a system in practice without a comparison of different solutions under uniform criteria. Firstly, considering the complexity of privacy preservation in MCS, it is hard to evaluate the effectiveness of these solutions. Secondly, some solutions, although achieve excellent performance with regard to privacy protection, are unable to support some important features required in practice, such as accountability, high efficiency, etc. Consequently, it is vital to provide a survey with a comprehensive literature review. Numerous surveys have been presented to deal with this problem. However, these works have the following drawbacks. First, some of them focus on just one specific scenario with limited privacy protection targets and attacks to be discussed. For example, Krontiris et al. [40] only explored location privacy in MCS. Unfortunately, they ignored privacy issues in other aspects, such as data privacy and identity privacy. Ding et al. conducted a comprehensive survey on secure and privacy-preserving data fusion in IoT [15]. Despite their outstanding work, the work does not cover all mechanisms in MCS, such as trust evaluation and worker incentive. Similarly, Liu et al. explores the privacy issues in mobile edge computing, but their work only focuses on privacy preserving data analytic methods [51]. Second, some surveys comprehensively consider the privacy, security, and trust issues in MCS, but lack uniform evaluation criteria for privacy protection. For example, He et al. [28] only summarized the recent research development on privacy protection and data trust problems in the context of MCS. Third, they only concentrated on privacy preservation but ignore the practicality of privacy solutions. Feng et al. [21] presented a series of essential security, privacy, and trust requirements as evaluation criteria. However, they paid little attention to accountability and efficiency issues of the relative

countermeasures, which are important to be considered in reviewing the practicality of these schemes.

To summarize, our work differs from the existing surveys in that it holistically covers all kinds of privacy issues in MCS, and comprehensively reviews and evaluates privacy preservation schemes in MCS with uniform criteria by taking practicality into consideration. The main contributions of this paper can be summarized as follows:

- We specify the unique characteristics of MCS and summarize its security model and potential attacks on privacy, based on which we propose uniform requirements that should be taken into consideration for privacy protection.
- We employ the proposed requirements as criteria to comprehensively evaluate existing privacy preservation schemes and discuss their pros and cons.
- Based on our serious survey and discussion, we find a series of open issues and propose future research directions to motivate further efforts in the field of effective and practical privacy preservation in MCS.

The remainder of this paper is organized as following. We illustrate the typical system structure of MCS and analyze the unique characteristics of MCS in Section 2. Following that, we depict the security model, threat model, privacy issues and privacy requirements of MCS in Section 3. In Section 4, we review the schemes to protect privacy from the view of privacy protection targets with regard to identity privacy, data privacy, attribute privacy and task privacy. Besides, we survey incentive solutions with privacy issues from the point of incentive measures in MCS. In addition, we analyze some decentralized privacy protection work in MCS. In Section 5, we point out open issues and future research directions. Finally, we conclude the paper in the last section.

2 Overview on mobile crowd sensing

Though numerous works have dealt with security, privacy and incentive issues in MCS, they fail to provide a uniform system architecture, which makes it challenging to evaluate the effectiveness and efficiency of existing privacy protection methods and schemes. To tackle this problem, in this section, we unify a typical system model of MCS and analyze its unique characteristics.

2.1 System model

In this subsection, we present the composition of the MCS system. Generally, it is composed of data consumers, data providers, and server platform. We present it in Figure 1.

1) System Entities

Data Consumer (DC) accesses MCS service for the fulfillment of a certain task which normally involves massive data collection and is unable to be finished alone. They can be individuals or corporations. They initiate sensing tasks according to their requirements and then request a server platform to recruit mobile users. Generally, tasks requested by DCs can be categorized into two types: people-centric tasks and atmosphere-centric tasks. The people-centric one requires the mobile nodes to

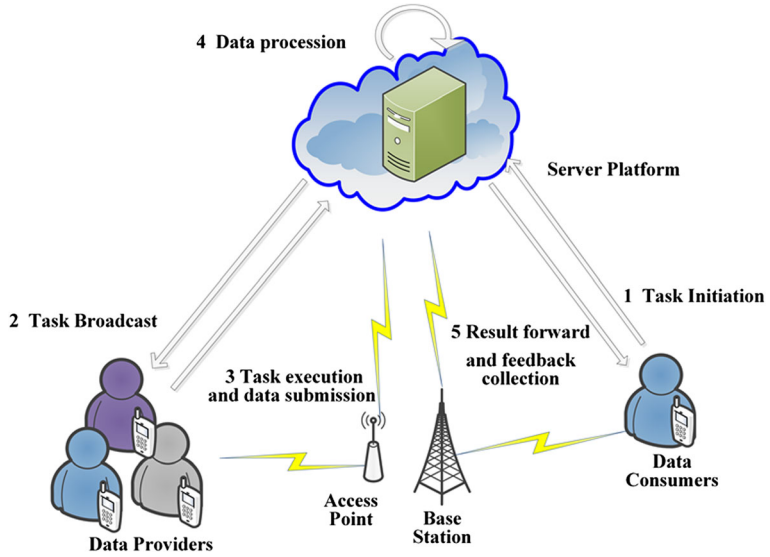

Figure 1 The System Architecture of MCS

provide their ideas, insights, or personal data directly, for example, assistive healthcare data collection in [26]. By contrast, the atmosphere-centric tasks are to collect environmental data, like images, videos, sounds, etc., such as cyclist and environmental data collection in [18]. In some systems, DCs can provide feedback on the quality of service after they receive the execution results from data providers [59].

Data Provider (DP) refers to a single person or an organization that manages mobile devices. Currently, mobile devices are equipped with abundant sensors and have the capability of sensing, computation, and communication, which enables them to act as the sensors for data collection or the computing nodes for data processing. DPs can apply for one MCS task based on their attributes, interests, and the payment amounts. It conducts the task once their application is approved and delivers the execution results to the server platform.

Server Platform (SP) acts as the intermediation between DCs and DPs. It provides a platform for task publication and execution. It receives task requests from consumers and publishes the tasks to DPs. It recruits a group of qualified DPs, processes collected data from DPs, and delivers the final results to DCs. Usually, the server platform is a centralized corporation or organization with strong capacities in storage and computation. There are also some designs that adopt decentralized structure by employing blockchain technique [75].

2) MCS Procedures

In this subsection, we describe the procedures of a typical MCS task execution. Specifically, it includes five main procedures, namely, task initiation, task broadcasting, task execution and data submission, data processing, result forward and feedback collection. We detail these procedures as following.

a) Task Initiation

Task initiation relates to the process that DC initiates a task and delivers the task to SP. Generally, DC needs to provide a task description, specification, and the budget for this task. The specification is illustrated as some restrictions, such as the frequency, deadline, location, time, reward amount, hardware requirements, etc.

b) Task Broadcasting

Task broadcasting is referred to as publishing task information to the public so that the recruited DPs can perform the task. There are two task broadcast models, i.e., push-based model [10] and pull-based model [61]. In the push-based model, SP selects a group of DPs according to the task requirements and node (i.e., DP) information. Then SP actively pushes the task to the selected DPs for execution. Obviously, it is vital that SP obtains the private attributes of these DPs in advance, like location, hardware information, task record, reputation, etc. These attributes are helpful to select qualified DPs in the push-based model. However, the disclosure of attribute information violates the security and privacy of DPs.

Differently, in the pull-based model, SP acts as a bulletin for task publication, and all DPs can access published task information. DPs decide whether to accept a task based on their interests, abilities, and attributes. In this model, their privacy is well protected without disclosing their personal information to any other entity. However, this model also has several drawbacks. First, it normally results in over staff or staff shortage depending on the task difficulty, specific requirements, or offered payment. Second, since no prior information provided, the skills and expertise of DPs cannot be guaranteed, which may lead to low-quality task accomplishment. Finally, in some scenarios, tasks from DCs may be too sensitive to be disclosed to the public.

c) Task Execution and Data Submission

In this procedure, each DP, if its application for a task is approved, executes the task by their mobile devices. After that, they submit their personal data, like ideas, restaurant recommendations, to SP.

d) Data Processing

SP is responsible for processing the raw material to obtain high-quality data or a final statistical report. Generally, the raw material contains inaccurate data that may deviate from the truth because of the variety of expertise, reliability, and trust value of DPs. Even worse, data submitted by one DP may conflict with that claimed by another one due to the ability variety or malicious behaviors of DPs. Therefore, it is imperative for SP to further process data, such as truth discovery [83]. Besides, some data may contain sensitive information of DPs, it is necessary to process data to reduce the disclosure risk. Finally, data aggregation is required in some scenarios. For instance, either the average pollution level in a given location or the maximum speed in the given street is required in some application scenarios. In all, data processing is an inevitable step in the MCS system.

e) Result Forward and Feedback Collection

In this procedure, SP forwards the processed data to DC. It is noted that DC provides feedback about the quality of service in some scenarios so that SP can also employ the feedback on the data provided by different DPs. This becomes an effective way to evaluate the skills, expertise, and trust of DPs, which is helpful to select better DPs in the following tasks.

2.2 Characteristics of MCS

In this subsection, we summarize the unique characteristics of MCS based on the system architecture and application scenarios.

1) Openness

MCS is an open system. That is, almost every node can participate in MCS activities as a DP or DC. Consequently, it is easy for malicious nodes or attackers to join MCS and conduct various attacks. The openness of MCS allows nodes to join or leave MCS activities freely and therefore increases the difficulty of node management.

2) Variety and Unreliability

Variety and unreliability are other key features of MCS. Owing to the difference in sensor accuracy, reliability, trust, and expertise of DP, data collected through MCS vary in terms of quality and reliability. Additionally, mobile devices are not initially designed for sensing, which leads to low data quality problem. Therefore, when designing privacy protection measures, it is necessary to conduct accountability for both mobile users and collected data.

3) Mobility

MCS can be regarded as a combination of traditional online crowdsourcing service and mobile communication technology. Therefore, MCS is featured with mobility that endows MCS more functions and great advantages compared with the traditional online crowdsourcing service. It employs mobile devices as the sensors to collect data for various purposes, such as navigation, transportation, etc. However, mobility also raises the difficulty in node management due to dynamic topology and limited communication resources.

4) Limited Computing and Communication Ability

MCS sensors are constrained by the battery, bandwidth, and computing capacity. They cannot undertake computationally expensive operations. Otherwise, it would exhaust its power drastically. Besides, although mobile devices can access the Internet much easier and faster than before, too much communication overhead involved may cause network congestion and high communication cost for mobile nodes. That is, communication and computation are another vital factor for MCS system when proposing privacy protocols.

5) Privacy Sensitivity

Information transmitted in one MCS system is probably privacy sensitive. First, some special tasks may reveal personal information about DC. Second, personal information of DC is

usually required so that SP can select a group of reliable and professional DPs for task execution. Unfortunately, the required information, such as location, job, hobbies, is quite sensitive and highly risky to user life and property once leaked. Third, MCS usually requests DP to upload their environmental data via image/video/voice, through which personal information can be inferred. However, it is unlikely that the SP is honest and powerful enough to provide data security guarantee standalone.

6) Data Massiveness

Compared with traditional online crowdsourcing services, MCS can be applied in various applications and scenarios. It is possible to collect a massive amount of data because of the popularity of mobile devices and network heterogeneity of MCS. The massiveness and diversity of data in MCS bring some disadvantages. First, it increases the difficulty of data processing as the presence of noise data. Thus, the final data presented to end users (i.e., DCs) may have deviated from the truth. Second, it is impossible to verify the accuracy of the final results. Since worker trust (WT) is related to the trust of the data he/she contributed. The hardness of accurate data trust (DT) evaluation has a negative impact on WT evaluation.

3 Threat analysis and privacy requirements

In this section, we define the security model of MCS and analyze the potential threats to privacy in MCS, based on which we further specify the privacy requirements of MCS, which will act as the criteria for the evaluation of privacy protection schemes in Section 4.

3.1 Security model

We assume that all MCS entities are benefit-driven so that they only pursue their own benefit, and they also keep curious about the others' privacy. In the following parts, we detail the security model and illustrate its reasonability.

1) DC

In MCS, DC consumes MCS service by providing a certain amount of payment. They are not necessary to be honest and could be curious about the privacy of other entities, especially the privacy of DPs. Besides, they may collude with others like SP and compromised DP to infer the privacy of other DPs. Finally, in some scenarios, they may maliciously generate dishonest feedback for the task results by SP or DPs to evade its expense.

2) SP

Although most existing solutions assumed that SP is honest but curious, or SP is powerful enough to resist various attacks, this assumption may not hold in reality. In other words, SPs have strong motivation to break the protocol for more benefits. For example, when deciding the payment for DPs, SP can maliciously reduce the amount of payment to increase its own payoff. Besides, SP suffers from single-point of failure. Data security is not guaranteed due to the emergence of various attacks. This also increases the risk of data leakage. Therefore, to

better evaluate the security and privacy preservation capacity of a scheme, in our paper, we consider SP as dishonest and curious about the privacy of DCs or DPs. They are profit-driven and may break the protocol or perform several malicious attacks for interests.

3) DP

DPs are rational and profit-driven and can conduct attacks or dishonest behaviors. First, DPs may fabricate their attributes to increase their opportunity to be selected when applying a task. Second, dishonest DPs can also upload fake data to defraud payment. In a word, we cannot consider DPs as fully trusted.

3.2 Threat model

Based on the security model and the unique features of MCS, we herein summarized the potential attack behaviors in the MCS system.

1) Eavesdropping

Eavesdropping attack refers to stealing the messages transmitted over the MCS network. As a mobile system, most MCS data are transmitted via wireless channels, and hence attackers can easily conduct eavesdropping attack. It is not secure when the message is not encrypted. Therefore, eavesdropping attack attaches high importance with data encryption, which is an effective protection measure.

2) Malicious Tasking

Malicious tasking means that a DC generates a task with the intention to obtain identity or other sensitive information from DPs. For example, a task like sensing the noise level at 3:00 AM in a given location is a malicious tasking since DP can be easily targeted in this scenario. The openness of MCS allows malicious nodes to publish a malicious attack freely and thus results in vital privacy leakage.

3) Task Tracing Attack

In tasking tracing attack, attackers (SP, DC, or outer attacker) can infer the sensitive information of the task participation by tracing their historical tasks. That is, the attackers can obtain more information such as habit, working location, home address, etc. by employing the task tracing attack.

4) Location-Based Attack

The location-based attack mainly relates to location or trajectory information disclosure. Since most MCS tasks require mobile users to collect data in a certain area, attackers can infer their location via various methods. A direct method is to collect the location information from the messages sent by DPs when applying for a task. Attackers can also infer the possible location of the victim by checking whether they are involved in a task or not. Therefore, the location-based attack is also greatly harmful to DPs.

5) Collusion Attack

There exist several kinds of collusion attacks in MCS. First, SPs may collude with each other by exchanging the information of DCs or DPs. In this way, SPs can obtain more information about them. Second, SP may collude with DCs to disclose the privacy of DPs, or conduct bad mouthing attack, i.e., set negative feedback for the data submitted by DPs, and thus lower the payment to these DPs. Third, DCs may also collude with some of DPs to maliciously reduce the payment for other DPs or disclose their privacy by sharing some confidential security parameters. Considering the openness of MCS, SP can easily deploy or recruit dishonest nodes in MCS and then work cooperatively to obtain the privacy of other MCS nodes. Since MCS is a privacy-sensitive system, the collusion attack also causes high privacy risk.

6) Sensitive Information Inference/Mining

The implicit information hidden under provided data is often ignored by DPs. However, attackers accessing the data uploaded by DPs can obtain their sensitive information by employing data mining technology. They can obtain the location, device type, even jobs, wealth, etc. by checking the task execution history of a DP and the task requirements. MCS is a privacy-sensitive system, which means information obtained from MCS data is highly related to user privacy. Besides, the massiveness of data also enables easy data analytics to retrieve useful knowledge or sensitive information, which greatly harms user privacy. Therefore, it is necessary to protect the privacy of DPs from sensitive information inference/mining attack.

3.3 Privacy issues in MCS

1) Task Privacy

Task privacy means that task information should be shared within a limited group of mobile users (i.e., DPs). Task information reveals the personal information of DCs, like, location, job, and purpose, according to which attackers may further infer the identity of DCs with extra information. Therefore, although in most cases, task information is public to all, there still exist requirements on the protection of task privacy.

2) Identity Privacy

Identity privacy means the identity information from MCS should be protected from other entities (i.e., DCs and DPs) except SPs. As aforementioned, MCS is an open system, and anyone including attackers can be involved in the MCS activities freely when they manage those mobile devices with sensing capability. If an entity is identified by attackers with background knowledge, the attackers can further infer its sensitive information and conduct malicious behaviors and even crimes to it easily. In this case, it is unwise to disclose unnecessary private identity information to all other parties.

3) Attribute Privacy

Attribute privacy relates to the attribute information of DPs, like location, hardware information, education, etc., which are required by the SP for task assignment. With this information,

SP can make a better evaluation of whether a user is suitable for a task. However, since SP is not fully trusted, it may take advantage of these attribute information to infer more privacy information of DPs. Besides, with the profit-driven nature of SP, it may also take advantage of this sensitive information for extra economic benefits. For example, SP may sell personal data to illegal parties. Apart from SP, DCs could also breach the privacy of DPs. Therefore, it is necessary to guarantee the attribute privacy of DPs in the MCS system.

4) Data Privacy

Data privacy mainly focuses on the content of the data submitted by DPs. Its importance lies in that data collected through MCS is usually sensitive to DPs, based on which it is easy for an entity to infer private information, such as the location [47], trajectory, etc. But at the same time, usability should be preserved. Therefore, the tradeoff between usability and privacy should be the key to data privacy. That is, we expect SP cannot learn private information from the submitted data and even DCs can only obtain the necessary information requested by the task.

3.4 Requirements of privacy preservation in MCS

Based on the aforementioned analysis, in this subsection, we set a series of requirements that a privacy preservation scheme should fulfill. We comprehensively consider the effectiveness with regard to privacy as well as the availability and efficiency to measure the performance of a privacy-preserving solution in MCS. We detail these requirements as following.

1) Anonymity (An)

Anonymity means that no parties, unless the authorized one, can obtain or disclose the real identity of MCS participants. Nowadays, DPs pay much attention to their privacy while identity privacy is among the most important ones. Since anonymity is directly related to the identity privacy, it is a fundamental requirement to achieve privacy.

2) Unlinkability (Un)

Unlinkability refers to that no one can distinguish whether two messages are from the same node or not. Therefore, it is impossible for an attacker to trace the behavior of nodes when the unlinkability requirement is satisfied. In MCS, the unlinkability is required during task initiation, task publishing, and data submission. To be specific, unlinkability for DC means that attackers cannot link two tasks published by the same DC together. For DP, we define unlinkability as that no one can distinguish whether two different applications for a task or two reports are generated by the same DP or not. None of the attackers can deduce whether a DP is involved in two different activities. In this way, it is impossible for attackers to trace the behavior of DPs.

3) Accountability (Aco)

Accountability is provided to detect fake or unreliable data to reduce their negative impacts on the final task results. MCS, as a typical application scenario of IoT, requires accountability such as trust evaluation [71]. In our analysis, we consider two types of accountabilities, i.e.,

profile accountability and data accountability. Profile accountability implies that the privacy-preservation scheme can well support the accountability of MCS participants, such as conditional identity disclosure, trust evaluation, etc. The data accountability mainly deals with the problem of low data quality due to variations in reliability, trust, and capacity, data collected through MCS. Besides, when SP recruits DPs for a task, DPs may submit faulty information intentionally to earn more benefits and thereby affects the trust of the final result.

4) Confidentiality and Integrity (Ci)

Confidentiality and integrity are the basic requirements in the communication systems. Messages transmitted in MCS, including task, personal information, data, etc., should be encrypted so that the system can resist eavesdropping attack. Besides, the system should also guarantee that messages received are the same as original without modification.

5) Access Control (Acl)

Access control refers that the task content, the personal information, and the collected data should only be accessed by an authorized or honest party based on the small granularity of an access policy, which normally take into account a user's personal profile and other factors.

6) Availability (Av)

Availability indicates that it should not cause any obstacle to the normal operation of MCS when a privacy-preservation measure is applied. Note that, some scholars proposed solutions to location privacy by employing spatial-temporal cloaking techniques, such as k-anonymity. However, it is tricky to find optimal k that can preserve the availability and privacy at the same time.

7) Computation Efficiency (Cp)

DPs are limited in computation ability, battery power as a mobile device. That is, complex computation is not allowed since it impacts the enthusiasm of DPs negatively when battery running out drastically. Thus, computation efficiency is an inevitable factor when researchers design an MCS-based protocol.

8) Communication Efficiency (Cm)

Communication cost is another consideration in efficiency requirements. High communication not only increases the expense of DPs but also accelerates their power consumption. Considering that there may be numerous mobile users involved in the MCS activities and massive data are transmitted, researchers are dedicated to reducing the interaction round amount. In a word, it is significant to provide communication efficient privacy-preservation methods.

4 Schemes of privacy protection

In this section, we review the existing literature on privacy protection by taking the proposed requirements as evaluation criteria. Based on different privacy targets, we categorize existing

privacy protection schemes into four categories with regard to identity privacy, data privacy, attribute privacy, and task privacy.

4.1 Identity privacy preservation (id)

Identity of one person refers to any subset of his attributes that can be uniquely detected. These attributes can be used to distinguish oneself from others, such as social security number or international mobile subscriber identification. As attackers can trace users activities by employing identity information, identity privacy protection is of utmost importance.

The *pseudonym* is adopted in many schemes to prevent attacks targeted on identity privacy. However, it cannot support unlinkability when attackers can easily link the activities of a user with its pseudonym. This can be addressed by changing pseudonyms frequently, but it is impractical in practice since it introduces excessive communication overhead. Therefore, pseudonym is not enough to preserve identity privacy with communication efficiency and fine unlinkability at the same time.

The concept of *ℓ-anonymity* is also introduced to solve this problem by hiding the real identity of DPs in a group of users. One classical example is AnonySense, a privacy-preserving scheme for MCS [36], aiming at both identity privacy and location privacy. In AnonySense, SP is composed of the registration authority, report server, and task server. The scheme adopts the spatial-temporal cloaking technique to guarantee location privacy. Besides, the tessellation map technique is leveraged to resist various attacks, where the location is presented as a region instead of a point. The authors adapted ℓ-anonymity report aggregation technique so that the SP cannot associate the report with the identity of DP.

In [36], identity privacy of DP is ensured by Direct Anonymous Attestation. MAC address recycling technique targets unlinkability. Additionally, the authors preserved integrity with the adoption of a server-based SSL channel. But, the availability is not supported here because of spatial-temporal cloaking technique. Confidentiality is guaranteed by encryption. In conclusion, the scheme in [36] achieves good computation efficiency but has a high communication cost with a redundant report from multiple parties. Besides, the scheme does not consider accountability.

Similarly, Yao et al. proposed an anonymous data reporting protocol [76]. The protocol includes two stages: slot reservation and message submission. The privacy countermeasure in the first stage is message shuffle to disguise a single DP into a group of N members. As a result, the scheme can protect identity privacy well and support both anonymity and unlinkability. On the data submission stage, the key idea is *DC-Nets*. Availability is also guaranteed because of the original raw data. Nevertheless, the scheme fails to support accountability, data confidentiality, and data integrity. In addition, the same length of all messages is used to defend against collusion attack. Unfortunately, the proposed protocol is only suitable for small scale scenarios owing to the high communication and computation overhead. Furthermore, the scheme allows SP to access raw data and thus fails to support data privacy.

The idea of *DC-Nets* is also adopted by Zhang et al. in a novel privacy-preserving data aggregation protocol [80]. The authors demonstrated an optimal grouping solution in terms of different privacy requirements when there are numerous users. In this design, there exists a trusted authority to be responsible for key management, and thus support accountability since it is easy to perform the trust evaluation and user revocation with the presence of a trusted authority. Besides, identity information from DPs can be concealed in a group of people, which

ensure both anonymity and unlinkability. Nonetheless, some disadvantages are inevitable. A major disadvantage is that the assumption of fully trusted authority and secure channel, which restricts its application scenarios. For example, they assume SP can access data content even when SP is not fully trusted. Furthermore, the scheme does not fulfill computation and communication efficiency when there exist dummy data that are evitable in MCS scenarios.

Another effective and popular tool for identity privacy preservation is a *group signature*. It is a signature method that enables a signer to sign a message on behalf of a group. As a result, attackers cannot decide the real signer of a message. A typical scheme using the group signature for anonymity and unlinkability is presented in [12]. It introduces a mixed network that provides unlinkability to the system. Identity privacy of DP is ensured by the group signature. This scheme requires a registration stage so that all nodes have to register with the trusted authority that is responsible for identity management. Correspondingly, it is easy to achieve profile accountability in this scheme as the trusted authority can easily link activities or disclose the real identity of malicious nodes. The scheme adopts encryption for confidentiality, and public key encryption to prevent data disclosure to an unauthorized party, and thus achieve confidentiality, integrity, and can support access control to a certain degree. Unfortunately, privacy is achieved at the cost of computation overhead because encryption algorithms contain many bilinear pairing operations. Because multiple parties are involved in this scheme, communication overhead is also tremendous. Besides, availability is not discussed in this paper.

All the work mentioned above aims at privacy preservation for DPs but ignores the identity privacy of DCs. Besides, they pay little attention to accountability when protecting identity privacy. Different from them, Ni et al. proposed a privacy-preserving MCS system which considers the identity privacy of both DCs and DPs [55]. The proposed MCS system employs a trusted authority and denotes the geographical region as a matrix. Apart from identity privacy, the system also achieves preservation on data privacy and location privacy, which is also known as a kind of attribute privacy. To be specific, it resolves location privacy by randomizing the matrix so that the attackers could not ascertain the specific location. Additionally, it adopts proxy re-encryption to protect sensing data. Therefore, data confidentiality is ensured at the same time. Since the system introduces a trusted authority for node management, it can well support user management, like the trust evaluation, user revocation, etc., and reach accountability. Anonymity is guaranteed as long as the Decisional Diffie-Hellman (DDH) assumption is held. The main drawback of the scheme lies in the high communication and computation overhead. Although measures like preprocessing mechanism can alleviate the overhead, it is still an obstacle that limits the application of the system.

Another scheme addressing the accountability problem in identity privacy preservation is presented in [66], where Vergara-Laurens et al. proposed a hybrid privacy preserving mechanism. They introduced a data broker and points of interest generator server in the system. The former one acts as the SP and the latter one is responsible for dividing the target area and allocating tasks. Besides, the authors designed a data verification model in the system and compared its performance with other privacy protection mechanisms. The underlying idea is to adopt different solutions for different scenarios. In essence, double encryption for data privacy protection is used to process small-size data. The scheme further utilizes anonymity and obfuscation to protect location privacy and identity privacy. Nonetheless, the obfuscation degrades the accuracy of location and thus harms availability. Therefore, though the scheme protects privacy, it is not practical in reality because of its limited application scenarios and low efficiency.

Qiu et al. presented another data aggregation privacy-preserving protocol on multimedia, i.e., SLICER [58]. SLICER adopts coding and encryption and concentrates on MCS data transfer strategy. By employing generalization technique, SLICER protects identity privacy of DPs. The scheme adopts encryption for data confidentiality and thus protects data privacy. Moreover, communication and computation cost is also affordable.

Different from all the aforementioned schemes, Kazemi and Shahabi explored the issue of identity privacy preservation resisting to the location-based attacks. To tackle this problem, they proposed a privacy-aware framework named PiRi [37]. The authors were concerned about how to assign a set of task points to a node without identity and location disclosure. The key algorithm consists of query formation and query selection. Query formation generates independent queries to prevent linkage attack. Query selection selects representative members to query the server by a voting mechanism. The scheme achieves anonymity and unlinkability at the cost of communication overhead. Besides, it does not consider data confidentiality, data integrity, and accountability.

4.2 Data privacy preservation (Da)

As analyzed above, data collected in MCS contain abundant sensitive information, such as health, identity, job, belief, etc. Consequently, it is necessary to provide data privacy preservation methods in MCS for the security and privacy consideration of DPs.

One solution to data privacy issue is data aggregation. Shi et al. proposed a privacy-preserving data aggregation method in MCS [60]. The method focused on divided additive function (e.g. summation and average) and non-additive function (e.g. maximum, median and others). For the aggregation of additive function, its main idea is *slice technique*, which, instead of delivering the data directly, the DPs first slice the collected data and then send them to other nodes in a given set. Finally, SP collects the data from these nodes. Consequently, SP access to the sum by summarizing all received data. Meanwhile, the authors proposed three cover-selection schemes and evaluated them by the virtue of hidden probability and communication cost. Considering that non-additive aggregations are related to counting queries, the authors integrated data slicing technique with the binary search while computing non-additive aggregation function. Data privacy preservation is achieved in the system. The applied scenario is a general one. Moreover, anonymity and unlinkability are also ensured owning to slicing technique. However, neither accountability nor data integrity is held. Obviously, both the slicing technique and count queries will induce huge communication and computation overhead. Hence, the scheme is not efficient enough to be deployed for massive data collection.

Another method for data privacy preservation is *secret perturbation*, as presented in [19]. Erfani et al. proposed four data summation schemes and evaluated them by the metrics of hidden probability and communication overhead. Since the authors analyzed and pointed out potential drawbacks of the first three schemes, we only consider the last one, key splitting scheme with integrity. The last scheme applies secure homomorphism MAC to verify the integrity of aggregated keys. For data privacy, the scheme employs encryption so that illegal entities have no access to data. Unfortunately, anonymity and unlinkability are not considered. A major drawback of the scheme resides in its failure to support data accountability while preserving data privacy.

In [11], Cristofaro and Pietro have taken both data privacy and identity privacy into consideration. To be specific, the proposed scheme guarantees query privacy with a tag

matching system, which indicates that the identity of the queried sensor is secure, and as a result, the schemes achieve anonymity of DPs. Since identity characteristic is unavailable in the communication process, unlinkability holds in the design. Besides, they further employed symmetric encryption to ensure data confidentiality and integrity. However, accountability is not considered. Besides, the query could fail if there is no successful match result, and hence it also does not fulfill availability. Furthermore, replication of data during matching produces high communication overhead and computation cost.

Liu et al. proposed a privacy preserving data sharing scheme for Location-Based Service (LBS) in the Internet of Vehicles (IoV) [51]. The scheme leverages k-nearest neighbors (KNN) to protect the location privacy of service provider. Besides, it employs Oblivious Transfer (OT) to hide queries of end users. As a result, attackers cannot analyze the content of queries to infer the location information of end users. CP-ABE helps protecting data privacy and enables end users to load the encrypted data ahead of time. Thereby, service provider only needs to transfer the decryption key to the end users, which greatly reduces communication overhead. In summary, the scheme achieves data privacy, location privacy, and trace privacy, but does not consider identity privacy. It also well realizes Ac using CP-ABE and can support Ci, Acl, and Cm.

A common drawback of the aforementioned schemes is that they fail to support data accountability simultaneously when data content is protected. To be specific, these schemes cannot support processing on data by SP. While in practice, SP needs to conduct a series of operations on the raw data, such as truth discovery, statistics, etc. To tackle this problem, homomorphism encryption is applied.

In [44], Li et al. presented novel privacy-preserving data summation and minimum protocols using *additive homomorphism encryption*. The authors implemented a sum aggregation protocol and offloaded computation of SP to DPs. In essence, secrets are distributed to the different node so that the adversary is unable to decrypt the message until gathering all secrets. Moreover, the authors utilized the sum protocol to compute the minimum value. To reduce computation cost, they compute approximate minimum value additionally. The applied scenario is time series data. Encryption algorithm ensures that data confidentiality and data availability. Communication efficiency is ensured by reduplication. The scheme also achieves anonymity and unlinkability since identity character is not traceable in it. However, this scheme still violates data privacy with the assumption of a fully trusted key dealer with access to all data.

Similarly, Zhang et al. employed Paillier homomorphism encryption for data privacy preservation and designed a data summation protocol [81]. Utilization of homomorphism encryption protects data privacy and supports data accountability. Besides, the authors also leverage data perturbation to conceal the identity information of DPs. That is, the scheme realizes anonymity and unlinkability. With homomorphism message authentication code, the integrity of aggregation result is preserved by virtue of homomorphism message authentication code. The drawback of the scheme is that the utilization of the slicing technique brings excessive computation and communication overhead. It is impractical due to the high communication and computation overhead.

Zhang et al. [82] presented privacy-preserving data aggregation protocols, minimum and k-th minimum, with untrusted SP. The key idea is *probabilistic coding schemes* besides *a cipher system*. The process is depicted as “report-determine-broadcast-compare”. In essence, trusted authority sends the private key to every node. After that, nodes send encrypted bit string (plaintext may be a bit string of q 0 s or a random q bit string according to the situation) to SP

when they receive the query request. Then, SP sets bit value to either 1 or 0 by bitwise XOR of all received data strings. By making an inquiry bit by bit, SP computes the minimum number. A similar idea is also utilized to compute k-th min. The difference is the coding scheme. It is straightforward that bitwise XOR improves computation efficiency. Communication cost is (nq + 1)l bits on average per time period. Because data report does not appear in the protocol, it is secure against SP and others. Unfortunately, the solutions in [82] also have their flaws. The assumption of trusted authority does not hold in all situations.

4.3 Attribute privacy preservation (at)

In this section, we explore the attribute privacy preservation issue in MCS. Different from identity privacy and data privacy, the variety of attribute types makes the protection quite challenging. Besides, the attribute information may be leaked in various ways. Attackers can obtain attribute content through direct information disclosure, or infer node attributes through the tasks that the DPs are involved in. Therefore, it is impossible to cover all attribute topics simultaneously. Considering this, we herein focus on three most representative attributes, i.e., location, trajectory, and bidding.

1) Location Privacy Preservation

Location privacy refers to one's current or past location [3]. In MCS, location privacy disclosure impacts user experience even may also harm the security of one's properties. Therefore, it is highly important to protect location privacy.

There is already a considerable number of work on location privacy preservation in other fields, like location-based services [38, 62] and cognitive radio network [23]. Duckham and Kulik [17] presented four typical strategies for protecting location privacy: regulatory, privacy policies, anonymity and obfuscation. Unfortunately, these solutions cannot be directly applied to the MCS scenario due to the unique characteristics of MCS, like openness and dynamic topology.

In essence, there is some work addressing location privacy issue in the context of MCS. A popular method is to adopt k-anonymity. For example, Krontiris et al. [40] employed k-anonymity stemming from the database community for location privacy protection. K-anonymity is a generalization technique, by applying which, it is infeasible to distinguish one among other k-1 nodes when k nodes share the same attribution. Inspired by Krontiris's work, many k-anonymity based location privacy protection methods were proposed [8, 27, 29].

To better protect location privacy, Huang et al. further employed l-diversity as an extension of k-anonymity [29]. The scheme utilizes two main techniques in k-anonymity, i.e. micro-aggregation and tessellation. To be specific, micro-aggregation is leveraged to ensure the character of the corresponding tile. To achieve k-anonymity, k nodes sharing the same value of sensitive attribute are included in every tile. The tessellation technique divides an area into multiple groups and disguises every group with at least k DPs. Considering the tradeoff between availability and confidentiality, the authors proposed a hybrid algorithm by combining the respective advantages of two algorithms. Besides, they applied the perturbation scheme to eliminate a trusted third server. Additionally, the authors further improved the scheme with l-diversity to defend against attribute disclosure resulting from background knowledge attack. K-anonymity or l-diversity conceal identity information and ensure both unlinkability and anonymity. However, the aforementioned scheme cannot well support availability or accountability.

In [8], Christin et al. employed k-anonymity to resist privacy leakage caused by the collusion between a curious SP and other malicious parties. The scheme is composed of partitioning spatial cloaking, private location matching, and joint information leakage. It leverages encryption so that data privacy can be protected from outer attacker. A Boolean circuit is used to defend against location disclosure.. Besides, both anonymity and unlinkability are ensured by the secret sharing algorithm. Although the scheme can well achieve location privacy preservation, the problem of data auditing due to k-anonymity keeps unsolved. Besides, every data needs to be divided into shares, distribute to other nodes, and then transmitted to the SP. As a result, the communication cost is extremely high. The public key system, Boolean circuit, and secret sharing algorithm in the scheme also incurs high computation overhead. Finally, data integrity, availability and accountability are not discussed.

From the above analysis, we could find that although k-anonymity based approaches guarantee anonymity and unlinkability, they usually face poor availability problem. To address this problem, Dong et al. presented another location protection solution aiming at fine availability, called P3S [16]. Its objective is to protect location privacy when providing fine-grained location service, namely. In the scheme, DPs generate two copies of location information. Then, they send the anonymized coarse-grained location information to SP and encrypted fine-grained one to DCs. Considering the dynamic attributes of DPs in MCS, the authors solved the revocation and key distribution issues by masquerading location information. In this way, availability is achieved at low communication and computation overhead.

Chen et al. [4] also presented a privacy-preserving data aggregation scheme to address the weaknesses of k-anonymity based schemes. It targets accountability and location privacy. The intuition is that one node submits multiple data reports to the SP with different pseudonyms. They also provided a mechanism to resist the Sybil attack. To be specific, they introduced a pseudonym certificate authority (PCA) and a key-managing server (KMS). Anonymity is achieved due to the anonymous credentials. Data integrity is preserved with zero knowledge verification protocol. Encryption algorithm ensures data privacy. Unlinkability holds as PCA generates different pseudonyms for the same node. Unfortunately, it still violates data privacy since the aggregation result is exposed to PCA. In the advanced one, an authentication server is in charge of data verification and pseudonym revocation, and thus achieves accountability. However, real identities of DPs and DCs are public to PCA, which may harm the identity privacy. Besides, both the computation overhead and communication cost are high in these two schemes.

Christin et al. were also dedicated to addressing location privacy for MCS in [6]. The intuition is to break the association between the spatial context and identity information. The specific method is that nodes exchange sensing data when they meet each other so that location information will be blurred to the adversary. The authors also presented a series of strategies and reporting strategies. The scheme emphasizes how to prevent privacy from being disclosed through the process of data reporting. As a result, location privacy, anonymity and unlinkability are preserved. Nonetheless, the scheme cannot support data integrity and accountability. Besides, the scheme cannot resist the privacy leakage by a dishonest SP.

2) Trajectory Privacy Preservation (tr)

Location privacy preservation mainly deals with static location privacy issue, while dynamic location privacy issue, i.e., trajectory privacy, is rarely studied. Although there is a significant amount of trajectory privacy work in the scenario of location-based services [5, 63], little effort has been taken in the scenario of MCS.

Huo and Meng [33] classified trajectory privacy techniques into three categories, i.e., dummy location-based methods [65], generalized trajectory k-anonymity based methods, and suppression methods [64].

Gao et al. proposed a trajectory privacy preserving framework called TrPF [24]. The system architecture is similar to that of [9], and the main difference is that TrPF replaces the mix network with a trusted third server that stores nodes' pseudonyms and certificates. Therefore, it guarantees user accountability by excluding malicious users from the MCS system with the certificate-based authentication mechanism. The scheme provides privacy preservation on sensitive trajectory segment, rather than the whole trajectory. Additionally, pseudonym and mix zone are applied in TrPF. Both anonymity and unlinkability are held because of the pseudonym technique. Trajectory mix-zone graph model is employed to protect trajectory privacy.

Badra and Hamida proposed another trajectory privacy preserving architecture in [2]. The main contribution is the introduction of a user group. They also assumed the SP to be a trusted party that can access the location information directly. Data privacy and trajectory privacy are protected by encryption technologies. Similarly, data integrity is held. Because identity is disguised with a group's identifier, unlinkability is fulfilled. However, accountability is not held here. Also, low computation efficiency is not negligible.

A lot of work is dedicated to addressing the tradeoff between service quality and privacy protection. Specifically, Gao et al. proposed a method to protect the location and trajectory privacy in [25]. The intuition is to conceal location information by the virtue of the equivalence class and hide trajectory characteristic by using the mapping relationship between two equivalence classes. Confidentiality is held thanks to the equivalence class. Unlinkability is ensured even location is disclosed and availability is also held. Other requirements are orthogonal to it. For disadvantages, high communication overhead from internode communication among one equivalence class is not negligible.

3) Bidding Privacy Preservation

Apart from location privacy and trajectory privacy, we also consider bid privacy, which mainly exists in the incentive mechanism of MCS. An incentive mechanism aims at motivating mobile users to take part in the MCS activities by issuing a mental or material reward to the DPs. Luo et al. Summarized six categories of incentive countermeasures [53], i.e., auction, lotteries, trust and reputation systems, bargaining game, contract theory, and market-driven mechanisms. In an incentive mechanisms, it usually requires DPs to submit a bid to the SP, which includes his possible costs for the task execution, its work plan, its ability, etc. Obviously, bid information will be highly related to DPs' personal privacy. Considering this, we herein analyze the bid privacy preservation in the incentive mechanisms for MCS.

Although enormous solutions to incentive problem have been carried out in the context of MCS, only some of them consider privacy [13, 34, 42, 43, 45, 48–50, 56, 57, 69, 72–74, 77, 79]. Initial privacy-aware incentive work in MCS is from [42]. Subsequently, more researchers have focused on this topic. To better analyze the fulfillment of these schemes for the proposed requirements, we first divided the incentive mechanisms into four types, i.e., credit-based incentive, auction-based incentive, currency-based incentive, and reputation-based incentive, and then discuss the privacy issues of incentive methods in each type.

a) Privacy protection in credit-based incentive (Cr)

Credit is a kind of incentive measure. It can not only be convertible to discount goods or sensing service quota but also can be accumulated as time goes by. Therefore, some scholars started to address the privacy protection incentive problem by the virtue of credit measure. However, some requirements on privacy usually conflict with those of credit-based incentive mechanism. To be specific, from the point of incentive, it is necessary to ascertain whether two different reports are submitted by the same one so that the credit value from the same user can be accumulated. Whereas, it is a conflict with the requirement of unlinkability, which is inevitable in identity privacy.

Li and Cao proposed two credit-based privacy-preserving incentive schemes in [42]. The difference between them is that the first one includes a Trusted Third Party (TTP). The proposed schemes leverage partial/blind signature to delink the request (report) with DC (DP). The two schemes are designed for the single-report task scenario, i.e., one node only submits one data for a given task., In this case, SP deletes each task once it is claimed by a DC so that the same task cannot be claimed by more than one DCs. This method is also used in the steps of report submission and credit deposit. In the first scheme, TTP generates request tokens, report tokens and credit tokens and respective commitments by employing a series of hash functions. DPs choose different pseudonyms in the task assignment step and in report submission step to disguise their identities, which helps improving anonymity and unlinkability. However, sensing data is public to the SP, which means that data privacy cannot be fully protected. The first scheme is computationally efficient since the computation overhead is offloaded to TTP. In this scheme, at most two hash functions are transacted in each communication step. Therefore, it achieves communication efficiency.

Based on the work in [42], Li and Gao further extended their work to a multiple report scenario, where each DP submits multiple data reports for a given task in [43]. When task request is approved, multiple report tokens are generated for it as the awards for task execution. Its novelty is to introduce the concept of receipt token. A receipt is used to support the multi-task report. Besides, DCs pay flexible credit number for any tasks by consuming their receipt tokens. In addition, Extended Merkle tree is applied to reduce the computation costs. Unlinkability is ensured because the report tokens and request tokens are generated independently. Moreover, the scheme achieves anonymity based on the application of the pseudonym. The scheme does not introduce much computation overhead. Thus, it is quite efficient.

Li et al. leveraged encoded vector to achieve bid privacy preservation in incentive solution in [45]. Owing to bulk transfer technique and public key cryptosystem, it successfully achieves anonymity and unlinkability. Besides, the scheme achieves both computation efficiency and communication efficiency. However, it is vulnerable to collusion attack.

b) Privacy protection in credit-based incentive (Cr)

Credit-based incentive methods are able to select a group of qualified DPs, but they usually ignore the budget of DCs as well as the payment to DPs. As a result, they usually fail to motivate the honest behaviors of DPs. To tackle this problem, some researchers adopted the auction model in game theory and explored how to motivate the honest execution of tasks.

The initial work to address the incentive problem by leveraging auction in MCS is [41]. The authors employed a reverse auction to resolve the incentive problem in MCS, which includes multiple sellers (i.e. DPs) and one buyer (i.e. DC). In the reverse auction-based incentive model, DPs act as bidders who submit bids to compete for a task, and SP acts as the auctioneer, who aims to maximize its own benefit. Inspired by the work in [41], a number of incentive

work based on reverse auction has to be carried out, but only a few of them [34, 48, 69, 74] take into account the privacy issues. In this subsection, we focus on analyzing the requirement fulfillment of these schemes.

Jin et al. [34] proposed an auction-based incentive mechanism for a special scenario, i.e. binary classification tasks execution, which is a differential private incentive mechanism based on the single-minded reverse combinational auction algorithm. It protects bid privacy by randomizing the price. The proposed incentive algorithm is efficient with polynomial time complexity. Besides, communication cost is also efficient. The main drawback of the scheme is the assumption of a fully trusted SP, which is not practical.

Another similar solution to the bid privacy is presented in [48]. The scheme aims at bid privacy-preserving for an auction mechanism with approximately minimizing the social cost. In detail, the authors proposed two auction models, single bid model, where each node submits a bid for a set of tasks, and multi-bid model, where each node submits an independent bid for each task in the task set. Bid privacy is ensured by the exponential mechanism. It is computationally efficient and communication overhead is low.

In [69], Wang et al. presented a reverse auction based incentive mechanism with location privacy preservation. It employs k-anonymity for bid privacy preservation. To alleviate the information loss resulting from k-anonymity, the authors promote a location aggregation method, i.e. Variable Centroid Location Aggregation scheme. In the proposed reverse auction algorithm, one node is added to the winner set only when his/her marginal efficiency is the highest one. The proposed model can be easily adapted to different scenarios and thereby achieves flexibility and fine availability. Besides, it also achieves computation efficiency. Unfortunately, the bid privacy preservation relies on the existence of a TTP, which is vulnerable to a single point of failure. Moreover, the scheme also suffers from high communication overhead.

Yang et al. adopted k-anonymity for bid privacy preservation and proposed three auction-based incentive location privacy protection mechanisms [74]. The first solution is applicable to the scenario where all DCs have the same privacy requirements; the second one is proposed to deal with different privacy requirements in the real world; the last one is suitable for the case where a DP can cheat on both their valuations and degree requirement. All these schemes adopt single round sealed-bid double auction with the assumption of a fully trusted central authority, which improves accountability but harms availability since this kind of party may be available in many scenarios. The authors employed k-anonymity technique for anonymity and unlinkability. In terms of efficiency, the scheme is efficient in computation but suffers from high communication overhead.

Dimitriou and Krontiris proposed a privacy-respecting multi-attribute reverse auction scheme [13] and replaced SP with an auction infrastructure. The scheme consists of an auction phase and a rewarding phase. The auction stage aims to select a group of winners (DPs) for task execution according to their utility score when protecting identity privacy. In the rewarding phase, the authors present an e-cash scheme and a decentralized token-based scheme with identity privacy preservation. Pseudonym is employed to ensure anonymity-time pseudonymous ID and ephemeral public key cooperatively ensures unlinkability. However, the authors paid little attention to achieving accountability. Although these schemes utilize encryption to protect data content, the misbehavior of SP may harm data integrity. The authors designed a hash-based mechanism to keep bid value secret, which can protect bid privacy meanwhile keep low computation communication cost.

c) Privacy protection in currency-based incentive (Cu)

An alternatively attractive solution to the incentive problem is introducing currency to effectively motivate DPs to engage in the MCS system. However, it could also introduce more misbehaviors for benefits and increases the risk of bid privacy leakage. Some scholars have concentrated on these problems and we will present a systematic survey on these solutions in this subsection.

Niu et al. proposed an E-cent based privacy preserving incentive mechanism [57]. To restrict malicious behavior from DPs, SP will punish or reward them according to the accuracy of their reported data. To maximize the sensing quality with a constrained incentive budget, the authors presented a dynamic reward allocation scheme. Mix-zone and encryption are adopted to protect identity privacy. Meanwhile, the mechanism of dispute arbitration is used to defend against unfair income from greedy or malicious DPs. Both the communication overhead and computation overhead of this scheme are low.

Zhang et al. [79] took DCs into consideration to achieve incentive and privacy. They adapted virtual currency/money to incentive high-quality task execution and proposed two privacy preserving incentive schemes. The main idea is to ensure identity privacy with encryption technique, cash break technique and blind signature. The authors aimed to protect data linkage privacy, work linkage privacy, and transaction linkage privacy of DPs. Identity privacy of the DP is protected in both two schemes, i.e., they achieve anonymity as well as unlinkability. Accountability holds because of the Schnorr scheme. However, in the two schemes, data reports are uploaded in the plaintext. Thus, the authors fail to support confidentiality. Besides, the two schemes suffer from high computation and communication efficiency.

Ni et al. proposed a similar work [56] to address privacy and incentive problem when taking DC into consideration. In detail, they presented one reward sharing based incentive mechanism based and protected identity privacy by randomization techniques. They adapted a coin-based incentive strategy and introduced a trusted authority and a bank in the system. Identity privacy from both DP and DC is protected. Thus, the proposed scheme supports both anonymity and unlinkability. Moreover, accountability is ensured by the Schnorr scheme. However, both the task content and sensing data face disclosure risks. Additionally, neither data availability nor data integrity holds in the scheme. Although communication cost is quite low, the scheme fails to achieve computation efficiency because of the involvement of many bilinear pairing operations.

d) Privacy protection in reputation-based incentive (Re)

The key intuition behind the reputation based incentive is to associate a reputation score with a device. Here, we adopt the concept of reputation as depicted in [67]. The reputation of a DP is "the synthesized probability that the past sensing reports sent by the node are correct, as perceived by the server".

The first reputation system in MCS is presented by Huang et al. [30]. It computes reputation scores by using the Gompertz function. Subsequently, some scholars proposed to incentive nodes by using reputation. For example, to motivate nodes to contribute data by high level of effort, the authors in [78] set reputation value, whereby nodes will be excluded from the system if their reputation values are not lower than a predefined threshold value.

The first work, which integrated privacy protection with the reputation in the context of MCS, is shown in [7]. The authors introduced a reputation and pseudonym manager in the system for trust evaluation pseudonym management. The key idea is to provide an anonymous reputation framework by using *blind signature* technology. The framework consists of two parts. The first one is to report data by using a periodic pseudonym. The second one is to transfer reputation score by virtue of reputation tokens. Besides, to prevent privacy disclosure risk resulting from reputation transfer, the authors adopted three reputation cloaking solutions. Periodically updated *pseudonym* helps achieve anonymity and unlinkability. Since there exists a fully trusted party for pseudonym management, the schemes simultaneously achieve accountability. However, the scheme pays no attention to data privacy preservation, and reputation cloaking mechanism may well incur the reputation loss.

Wang et al. proposed another reputation based privacy preserving incentive mechanism [68]. The key idea is to design an incentive mechanism by taking the advantages of auction incentive. In detail, the authors presented two incentive measures, which are an improved two-stage auction algorithm and an improved online reputation updating algorithm. The intuition of them is to recruit a DP by virtue of the density of marginal utility and his/her reserved price. In the whole process, data content is protected by an encryption algorithm. Furthermore, both bidding value and updated reputation value are kept confidential. Computation of the incentive scheme is executed in polynomial time. However, communication cost is relatively high as a major drawback of the public key encryption algorithm.

Another privacy-preserving reputation-based incentive system is shown in [31]. The key idea is to transfer reputation score from one pseudonym to another one with the assistance of TTP. To be specific, TTP manages the mapping between a real identity and a pseudonym and updates the reputation value for all entities. The utilization of pseudonym preserves anonymity. Besides, it also introduces a k-anonymity based reputation update mechanism for unlinkability, which fulfills location privacy.

4.4 Task privacy preservation (TAsk)

Task privacy is highly related to the privacy of DCs. However, recent research lacks investigation on the preservation of task privacy. The probable reason may be that task content has to be published to DPs, otherwise they cannot undertake the task. However, this ignores the extra information revealed by task requirements on user attributes. That is, even attackers cannot obtain the task content, they can still infer the probable content of a task with its unique requirements the DPs should fulfill. However, how to find enough DPs with limited information disclosure still lacks exploration.

4.5 Decentralized privacy preservation for MCS

The aforementioned methods are based on centralized architecture as illustrated in Section 2. Centralized MCS architecture can offer a more stable services. However, the trust of centralized SPs cannot be guaranteed in the real world. Owing to the profit-driven facts of SPs, when the privacy preservation goes conflict with their profit, they are probably to perform dishonest, even malicious behaviors. Besides, the emergence of various attacks, especially for inner attacks, currently, SPs cannot provide full protection for task information, attribution information, or collected data. In fact, there is already serious privacy leakage due to the compromise of a centralized entity. Therefore, decentralized architecture for MCS is urgently needed.

A basic solution to this issue is to adopt a decentralized data storage system and deploy a fine-grained access control for data preservation. In this way, the privacy of the whole system is still preserved even some data access points are compromised and the system can still guarantee safety for other data. For example, PEPPeR proposed by Dimitriou et al. [14] is a decentralized access control system, in which, DCs can anonymously ask for data content without employing SP as intermediation. The key idea behind it is a *partial blind signature*. The authors introduced the application provider and witness service in the system. The application provider distributes the token to a DC and redeems it for DPs. The witness service is used to detect double-spending activity. The identity of DC is protected by a blind signature scheme. Whereas, link-ability is not preserved because DCs can use different pseudonyms for each message sent. Accountability is not met because it does not detect the identity detection even double spending can be found because it is concentrated on how to purchase, verify, spend these tokens, rather than how to submit and forward sensing data, data requirements. Efficiency is not to be considered either.

Based on the work of [14], Krontiris and Dimitriou proposed a sensing platform in [39], in which DCs can discover DPs within a specific region. Apart from the identity privacy of DCs and DPs, they also took location privacy into consideration. To ensure the privacy of DPs, they introduce a Mobile object agent to represent a DP so that the DC only interacts with the Mobile object agent, rather than that DP. Therefore, privacy from DPs is ensured. For the fulfillment of efficiency requirement, the result is similar to that in [14]. Both anonymity and unlinkability are met. Tokens are used to ensure flexible access control. Spatial cloaking techniques are applied to obfuscate location. Nonetheless, availability is sacrificed. DC is anonymous because of the token and DP is anonymous with the cryptographic tools involved. The token reveals no information about DC. Other requirements are neglected.

Wei et al. [70] proposed a privacy-preserving system, PPSense. The authors add Access Point in the system. The key techniques are Cipher Policy Attribute-Based Encryption (*CP-ABE*) and *Mix scheme*. In CP-ABE, the access policy is embedded in the private key of a DC. Only when a DC fulfills access policy, can he/she decrypt the message. SP is composed of a data server and a management server. The former one is in charge of the broadcasting task and receiving data from DPs. While the latter one not only functions the authority of CP-ABE, but also manages identity-related information and the registration from DPs. The management server generates private keys for others. Anonymity is realized by virtue of the Mix scheme. Because the report includes data and ID, accountability is held with the sacrifice of unlinkability. Availability is ensured by encryption so that data is integrity. All parties in the system are assumed to be malicious. Unfortunately, both task content and report data are public to Data Server. Whereas, the authors assumed that the party could be controlled by an adversary. Thus, it will be disclosed to an adversary. Furthermore, Mix scheme leads to low computation and communication efficiency.

Recently, the drawbacks of a centralized MCS system and the popularity of blockchain motivates researchers to build up a decentralized MCS with blockchain, like CrowdBC [46] and MCS-Chain [20]. However, blockchain itself faces several problems in terms of privacy. Blockchain is an open and transparent system, attackers can also access the data on-chain, which presents a severe data privacy leakage problem. Besides, although blockchain achieves anonymity by allowing users to use public key rather than real identities, attackers can still link and trace user activities by analyzing on-chain data. This may cause crucial user identity leakage. Notably, existing blockchain-based MCS systems pay little attention to privacy preservation [20, 46].

Although the aforementioned methods help improving data privacy to some degree, they fail to consider other privacy issues due to dishonest SP. Therefore, it is not sufficient to ensure privacy with the presence of dishonest SPs by employing decentralized storage system only. In summary, decentralized MCS architecture still needs further exploring. We summary the above mentioned analysis results in Table 1. Specifically, we concentrate on key technique, privacy target and privacy requirements.

5 Open issues and future reseach directions

In this section, we present open issues based on our survey analysis. Besides, we also pose a series of future research directions.

5.1 Open research issues

5.1.1 Preservation on implicative privacy

Though many efforts have been put into privacy preservation of MCS, they only consider the explicit information like data content, task content, or personal attribution. However, sensitive information can also be inferred from massive data by analyzing task requirements or historical tasks. For example, we can extract gender and age from the transaction record in E-market personal data or shopping history from the pharmacy.

The reason is that almost every procedure in MCS can reveal personal information or provide attackers a chance to infer user information. Thereby, dishonest or malicious entities should not access the plaintext of bids or data of data collectors since they could infer their private information by analyzing the information they can get. For example, malicious entities can obtain location information by analyzing the task execution history of data collectors since most MCS tasks are location related. Similarly, when a data requestor publishes a special task, attackers may also infer the real identity with some extra information.

Another reason that prevents MCS from achieving fine implicative privacy is that full privacy preservation may hinder accountability or availability of the system. For example, it is difficult for SP to evaluate user trust if all users keep anonymous and unlinkable to SP. This also results in the difficulty to support preservation on implicative privacy. Considering that implicative information is also highly related to user privacy, the study on implicative privacy preservation is an open and significant issue [35].

5.1.2 Efficient privacy preservation with accountability and availability

As we can see from Table 1, most of the schemes can achieve fine anonymity, unlinkability, and confidentiality. However, none of them fulfill all requirements holistically, they either suffer from low efficiency or fail to achieve fine availability or accountability simultaneously, which greatly limits the applications of these schemes. The possible reasons can be analyzed as follows. First, the limited computation and communication capacities of mobile devices make it difficult to employ computationally expensive cryptographic tools to achieve privacy protection. Second, sometimes privacy conflicts with accountability or availability. For example, preservation on identity privacy requires anonymity and unlinkability. However, anonymity and unlinkability make it difficult to accurately evaluate trust. In practical applications,

Table 1 Privacy Preservation Schemes in MCS

Ref	Key techniques	Incentive measures				Privacy target				Privacy requirements							
		Cr	Au	Cu	Re	id	da	at	ta	An	Un	Ac	Ci	Acl	Av	Cp	Cm
[36]	spatial-temporal cloaking	–	–	–	–	Y	N	loc	N	Y	Y	N	Y	N	N	N	N
[76]	DC-Nets	–	–	–	–	Y	N	N	N	Y	Y	N	N	N	Y	N	N
[80]	DC-Nets	–	–	–	–	Y	N	N	N	Y	Y	Y	N	N	N	N	N
[12]	Group signature	–	–	–	–	Y	N	N	N	Y	Y	Y	Y	Y	Y	N	N
[55]	Proxy re-encryption	–	–	–	–	con/pro	Y	loc	Y	Y	N	Y	Y	N	N	N	N
[66]	Hybrid approaches	–	–	–	–	Y	N	loc	N	Y	N	Y	Y	N	N	N	N
[58]	Erasure coding& encryption	–	–	–	–	Y	Y	N	N	Y	N	N	Y	N	N	Y	Y
[37]	Partial-inclusivity and Range independence	–	–	–	–	Y	N	N	N	Y	Y	N	N	N	N	N	N
[60]	Slice technique	–	–	–	–	N	Y	N	N	Y	Y	N	Y/N	N	N	N	N
[19]	secret perturbation	–	–	–	–	N	Y	N	N	N	N	N	Y	N	N	N	N
[11]	Paillier encryption	–	–	–	–	Y	Y	N	N	Y	Y	N	Y	N	N	N	N
[44]	additive homomorphic encryption	–	–	–	–	N	Y	N	N	Y	Y	N	Y	N	Y	Y	N
[81]	Paillier encryption	–	–	–	–	N	Y	N	N	Y	Y	Y	Y	N	N	N	N
[82]	probabilistic coding	–	–	–	–	N	Y	N	N	N	N	N	Y	N	N	Y	Y
[29]	k-anonymity	–	–	–	–	N	N	loc	N	Y	Y	N	Y	N	N	Y	Y
[8]	k-anonymity	–	–	–	–	N	Y	loc	N	Y	Y	N	Y	N	N	N	N
[16]	Attribute Based Encryption	–	–	–	–	N	N	loc	N	N	N	N	N	N	Y	Y	Y
[4]	pseudonym	–	–	–	–	N	N	loc	N	Y	Y	Y	Y	N	N	N	N
[6]	Exchange strategy	–	–	–	–	N	N	loc	N	Y	Y	N	N	N	N	N	N
[24]	Pseudonym mix-zone	–	–	–	–	N	N	tra	N	Y	Y	Y	N	N	N	N	N
[2]	User group	–	–	–	–	N	N	tra	N	Y	Y	N	Y	N	N	N	N
[25]	the equivalence class	–	–	–	–	N	N	loc /tra	N	N	Y	N	Y	N	N	N	N
[42]	(Partial) blind signature	Y	N	N	N	N	N	bid	N	Y	Y	N	N	N	N	Y	N
[43]	Pseudonym Merkle tree	Y	N	N	N	N	N	bid	N	Y	Y	N	N	N	N	Y	Y
[45]	DC-Nets	Y	N	N	N	N	N	bid	N	Y	Y	N	N	N	N	Y	Y
[34]	Differential privacy	N	Y	N	N	N	N	bid	N	N	N	N	N	N	N	Y	Y
[48]	Exponential mechanism	N	Y	N	N	N	N	bid	N	N	N	N	N	N	N	Y	Y
[69]	Micro-aggregation	N	Y	N	N	N	N	bid	N	N	N	N	N	N	N	Y	N
[74]	k-anonymity	N	Y	N	N	N	N	bid	N	Y	Y	N	N	N	N	Y	N
[13]	pseudonym	N	N	Y	N	N	N	bid	N	Y	Y	N	N	N	N	Y	Y
[57]	E-cent, Mix-zone	N	N	Y	N	N	N	bid	N	Y	N	N	N	N	N	Y	Y
[79]	Partial blind signature	N	N	Y	N	con/pro	N	bid	N	Y	Y	N	N	N	N	N	N
[56]	Randomization techniques	N	N	Y	N	con/pro	N	bid	N	Y	Y	Y	N	N	N	N	Y
[7]	Pseudonym	N	N	N	Y	N	N	N	Y	Y	Y	Y	N	N	N	N	N
[68]	Time-lapse cryptography	N	N	N	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N
[31]	Pseudonym	N	N	N	Y	Y	N	loc	N	Y	Y	N	N	N	N	N	N
[14]	Partial blind signature	–	–	–	–	con	N	N	N	Y	N	N	N	Y	N	N	N
[39]	Blind signature	–	–	–	–	con/pro	N	loc	N	Y	Y	N	N	Y	N	N	N

Table 1 (continued)

Ref	Key techniques	Incentive measures				Privacy target				Privacy requirements							
		Cr	Au	Cu	Re	id	da	at	ta	An	Un	Ac	Ci	Acl	Av	Cp	Cm
[70]	CP-ABE, Mix scheme	–	–	–	–	pro	N	N	N	Y	N	N	N	N	N	N	N

Y represents that the scheme satisfies the corresponding requirement;

N represents that the scheme does not satisfy the corresponding requirement;

- represents that the corresponding requirement is out of the scope of the scheme;

Loc/bid/tac represents that the scheme achieves location/bidding/trajectory privacy;

Con/pro represents that the scheme supports privacy for consumer/provider

privacy preservation should also guarantee availability, that is, the privacy protection measures should not hinder the normal operation of MCS task execution, and should be flexible in various scenarios. However, these issues are rarely explored.

5.1.3 Privacy preservation without fully trusted SP

As the most popular architecture, the centralized MCS system gets a lot of attention in current research. However, fully trusted and secure centralized server is not available in priactice. First, centralized SPs are vulnerable under various attacks with the risk of information leakage. Especially, it is quite difficult to resist inner attacks. Second, a compromised SP may bring severe single point failure. Third, SP is a profit-driven entity, which means it may behave maliciously to infer valuable sensitive information of DCs or DPs for gaining more profits.

As a result, the traditional centralized architecture confronts a series of privacy issues in identity privacy, bidding privacy, etc. Some schemes directly employ a centralized SP for identity management, user selection, and data processing. A compromised or dishonest SP will certainly cause severe personal information leakage regarding identity information, location information, and collected data. Besides, the malicious SP may collude with data requestors or data collectors to obtain more information of honest users. For example, by issuing a malicious task, SP may infer location information of data collectors. Even if some schemes try to address this issue, they only solve the problem in a specific procedure of MCS task execution, and cannot provide full privacy insurance as a whole. Therefore, how to preserve privacy without the presence of a fully-trusted SP is still an open issue deserving special attention.

5.1.4 Summary

It is not trival to solve the above issues all together, since these issues are not alone. First, it is difficult to preserve implicative privacy while well supporting accountability. For example, it is easy to preserve implicative privacy with encryption. However, SP cannot process encrypted data with ciphertext to select data collectors, find the truth, or evaluate user trust. Homomorphic encryption could help, but it is too heavy and not practical so far. In this case, the MCS system achieves poor accountability. Though some homomorphic encryption based methods are applied in MCS incentive, they fail to resist collusion between MCS SP and dishonest workers. Besides, in some schemes, the data requestors may still obtain the private information

of data collectors. Second, achieving privacy preservation in decentralized MCS will harm availability because of lack of a centralized party. A popular method is to build MCS with blockchain. However, blockchain itself faces such problems as efficiency, which harms availability because it cannot process numerous MCS messages quickly. To summarize, it is necessary to take all these open issues into consideration when designing privacy preservation methods.

5.2 Future research directions

5.2.1 Implicative privacy preservation

As mentioned, current research ignores the protection of implicative privacy. Attention has been paid to the protection of the content of the task, data, bid, etc., while privacy disclosure by indirect inference still lacks exploration. Since implicative privacy also contains a lot of sensitive information, it becomes essential to provide implicative privacy preservation in MCS.

5.2.2 Efficient identity privacy preservation with accountability

Current identity privacy preservation emphasizes anonymity and unlinkability but underestimates accountability on MCS entities. Accountability, such as malicious behavior detection, trust evaluation, and user revocation, helps exclude malicious entities from the MCS system and assists users to judge rationally. While the study is important for MCS security and privacy preservation, the challenge is that accountability may conflict with identity privacy. That is, providing unlinkability makes it hard to trace DPs or DCs. However, it also increases the difficulty in linking the activities of a single user together, and checks its honesty, evaluates its trust, etc. Also, Existing schemes that support identity privacy and accountability usually suffer from low efficiency. A typical example is the scheme using group signature. In short, while the challenge exists, it is still significant to provide an efficient privacy preservation scheme with accountability to enhance privacy and security in MCS.

5.2.3 Data privacy preservation with accountability

Data privacy preservation in MCS has been widely studied so far. The unreliability of MCS makes it necessary to support data accountability, such as statistics, truth discovery and quality evaluation as well. One effective tool is homomorphic encryption, but it suffers from high computational overhead. Obviously, cryptography techniques are unable to solve this problem standalone. Therefore, it is necessary to employ more efficient and effective solutions [52] to address this problem.

5.2.4 Decentralized MCS with privacy preservation

Since centralized architecture is vulnerable to single point failure and dishonest behaviors of SPs, decentralized MCS system is highly expected. Currently, with the emergence of blockchain, numerous decentralized systems based on blockchain are proposed in the field of Internet of Things (IoT), vehicular ad-hoc network (VANET), smart city, etc. Since the security of blockchain relies on the underlying consensus mechanism rather than the security of a single party, it can work as an effective tool to build a decentralized MCS system [20].

However, due to the openness and transparency of blockchain in nature, how to build a decentralized MCS system with privacy preservation with blockchain becomes a promising research topic.

5.2.5 Summary

Though we list the above future research directions separately, they may relate to each other and we should integrate them in our study. For example, when designing preservation on identity privacy or data privacy with accountability, we should consider how to efficiently preserve implicative privacy. In addition, decentralized privacy preservation should take into account efficiency, since high computation or communication overhead may harm availability because of the restricted capability of a blockchain system. What is more, the leakage of data privacy may also lead to the disclosure of identity or location, since MCS data usually contain sensitive information like workplace. Therefore, a holistic scheme become critically essential to comprehensively preserve the privacy of identity, data, attribute and task.

6 Conclusion

In this paper, we summarized the unique characteristics of MCS and analyzed its potential privacy risks. We setup a series of requirements for privacy preservation in MCS. Different from existing survey work, we pointed out that when designing privacy preservation schemes, apart from privacy issues, the fulfillment of accountability, availability, and efficiency is also necessary for practically protecting privacy in a holistic way. Based on the proposed requirements, we performed a serious survey on privacy protection in MCS and analyzed the pros and cons of existing work. Finally, we summarized several open issues and propose some significant future research directions to direct additional efforts in this research field.

Acknowledgements This work was supported in part by the NSFC under Grant No. 61672410, 61802293 and U1536202, in part by Research project of Yun Cheng University under Grant No. XK- 2018029 and Grant No. SWSX201301, in part by the National Natural Science Foundation of Shanxi Grant No. 201601D021014, the Academy of Finland under Grants 308087 and 314203.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

1. Arvind, T. et al.: VTrack: Accurate, energy-aware road traffic delay estimation using mobile phones. In: Proc. 7th ACM Conference on Embedded Networked Sensor Systems, pp. 85–98 (2009)
2. Badra, M., Ben Hamida, E.: A novel cryptography based privacy preserving solution for urban mobility and traffic control. In: Proc. of 2015 7th Int. Conf. New Technol. Mobil. Secur. (2015)
3. Beresford, A.R., Stajano, F.: Location privacy in pervasive computing. IEEE Pervasive Comput. **2**(1), 46–55 (2003)
4. Chen, J., Ma, H., Wei, D.S.L., Zhao, D.: Participant-density-aware privacy-preserving aggregate statistics for mobile crowd-sensing. In: Proc. of Int. Conf. Parallel Distrib. Syst. - ICPADS, pp. 140–147 (2016)
5. Chow, C.-Y., Mokbel, M.F.: Trajectory privacy in location-based services and data publication. ACM SIGKDD Explor. Newsl. 13(1) (2011)

6. Christin, D., Guillemet, J., Reinhardt, A., Hollick, M., Kanhere, S.S.: Privacy-preserving collaborative path hiding for participatory sensing applications. In: Proc. of 8th IEEE Int. Conf. Mob. Ad-hoc Sens. Syst. MASS 2011, pp. 341–350 (2011)
7. 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)
8. Christin, D., Bub, D.M., Moerov, A., Kasem-Madani, S.: A Distributed Privacy-Preserving Mechanism for Mobile Urban Sensing Applications. In: Proc. of IEEE 10th Int. Conf. Intell. Sensors, Sens. Networks Inf. Process. ISSNIP 2015, pp. 7–9 (2015)
9. Cornelius, C., Kapadia, A., Kotz, D., Peebles, D., Shin, M., Triandopoulos, N.: Anonysense: privacy-aware people-centric sensing. In: Proc. of the Sixth Int. Conf. Mob. Syst. Appl. Serv.-Mobisys08, pp. 211–224 (2008)
10. Das, T., Mohan, P., Padmanabhan, V.N., Ramjee, R., Sharma, A.: PRISM: Platform for Remote Sensing using Smartphones. In: Proc. of the 8th international conference on Mobile systems, applications, and services - MobiSys '10, pp. 63–76 (2010)
11. De Cristofaro, E., Di Pietro, R.: Adversaries and countermeasures in privacy-enhanced urban sensing systems. IEEE Syst. J. **7**(2), 311–322 (2013)
12. De Cristofaro, E., Soriente, C.: Extended capabilities for a privacy-enhanced participatory sensing infrastructure (PEPSI). IEEE Trans. Inf. Forensics Secur. **8**(12), 2021–2033 (2013)
13. Dimitriou, T., Krontiris, I.: Privacy-respecting auctions and rewarding mechanisms in mobile crowd-sensing applications. J. Netw. Comput. Appl. **100**(August), 24–34 (2017)
14. Dimitriou, T., Krontiris, I., Sabouri, A.: PEPPeR: A querier's privacy enhancing protocol for participatory sensing. In: Proc. of International Conference on Security and Privacy in Mobile Information and Communication Systems Springer, Berlin, Heidelberg, 2012., pp. 93–106 (2012)
15. Ding, W.X., Jing, X.Y., Yan, Z., Yang, L.T.: A survey on data fusion in internet of things: towards secure and privacy-preserving fusion. Information Fusion. **51**, 129–144 (2019)
16. Dong, K., Gu, T., Tao, X., Lu, J.: Privacy protection in participatory sensing applications requiring fine-grained locations. In: Proc. Int. Conf. Parallel Distrib. Syst. - ICPADS, pp. 9–16 (2010)
17. Duckham, M., Kulik, L.: Location privacy and location-aware computing. Proc. of 3rd Int. Conf. Pervasive Comput., vol. 819, no. 3, pp. 34–51 (2006)
18. Eisenman, S.B., Miluzzo, E., Lane, N.D., Peterson, R.A., Ahn, G.-S., Campbell, A.T.: BikeNet:a Mobile sensing system for cyclist experience mapping. ACM Trans. Sens. Networks. **6**(1), 1–39 (2009)
19. Erfani, S.M., Karunasekera, S., Leckie, C., Parampalli, U.: Privacy-preserving data aggregation in Participatory Sensing Networks. In: Proc. of 2013 IEEE 8th Int. Conf. Intell. Sensors, Sens. Networks Inf. Process. Sens. Futur. ISSNIP 2013, pp. 165–170 (2013)
20. Feng, W., Yan, Z.: MCS-chain: decentralized and trustworthy mobile crowdsourcing based on blockchain. Futur. Gener. Comput. Syst. **95**, 649–666 (2019)
21. Feng, W., Yan, Z., Zhang, H., Zeng, K., Xiao, Y., Hou, Y.T.: A survey on security, privacy, and trust in mobile crowdsourcing. IEEE Internet Things J. **5**(4), 2971–2992 (2018)
22. Ganti, R.K., Ye, F., Lei, H.: Mobile crowdsensing: current state and future challenges. IEEE Commun. Mag. **49**(11), 32–39 (2011)
23. Gao, Z., Zhu, H., Liu, Y., Li, M., Cao, Z.: Location privacy in database-driven Cognitive Radio Networks: Attacks and countermeasures. In: Proc. of 32th IEEE Int. Conf. Comput. Commun., pp. 2751–2759 (2013)
24. Gao, S., Ma, J., Shi, W., Zhan, G., Sun, C.: TrPF: a trajectory privacy-preserving framework for participatory sensing. IEEE Trans. Inf. Forensics Secur. **8**(6), 874–887 (2013)
25. Gao, S., Ma, J., Shi, W., Zhan, G.: LTPPM: a location and trajectory privacy protection mechanism in participatory sensing. Wirel. Commun. Mob. Comput. **15**(1), 155–169 (2015)
26. Giannetsos, T., Dimitriou, T., Prasad, N.R.: People-centric sensing in assistive healthcare : privacy challenges and directions. Secur. Commun. Networks, pp. 1–12, (2010)
27. Gruteser, M., Grunwald, D.: Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In: Proc.of 1st Int. Conf. Mob. Syst. Appl. Serv. - MobiSys '03, pp. 31–42 (2003)
28. He, D., Chan, S., Guizani, M.: User privacy and data Trustworthiness in Mobile crowd sensing. IEEE Wirel. Commun. **14**(5), 28–34 (2015)
29. Huang, K.L., Kanhere, S.S., Hu, W.: Preserving privacy in participatory sensing systems. Comput. Commun. **33**(11), 1266–1280 (2010)
30. Huang, K.L., Kanhere, S.S., Hu, W.: Are You Contributing Trustworthy Data ? The Case for a Reputation System in Participatory Sensing. In: Proc. of 13th ACM Int. Conf. Model. Anal. Simul. Wirel. Mob. Syst., pp. 14–22 (2010)
31. Huang, K.L., Kanhere, S.S., Hu, W.: A privacy-preserving reputation system for participatory sensing. In: Proc. of Conf. Local Comput. Networks, LCN, pp. 10–18 (2012)

32. Hull, B., et al.: CarTel: A Distributed Mobile Sensor Computing System. In: Proc. of the 4th international conference on Embedded networked sensor systems - SenSys '06, pp. 125–138 (2006)
33. Huo, Z., Meng, X.-F.: A survey of trajectory privacy-preserving techniques. Proc. of IEEE Int. Conf. Mob. Data Manag., vol. 34, no. 10, pp. 1820–1830 (2011)
34. Jin, H., Su, L., Ding, B., Nahrstedt, K., Borisov, N.: Enabling Privacy-Preserving Incentives for Mobile Crowd Sensing Systems. In: Proc. of Int. Conf. Distrib. Comput. Syst., pp. 344–353 (2016)
35. Johnson, P., Kapadia, A., Kotz, D.: People-centric urban sensing: Security challenges for the new paradigm. Dartmouth Comput. Sci. Tech. Rep. (2007)
36. Kapadia, A., Triandopoulos, N., Cornelius, C., Peebles, D., Kotz, D.: AnonySense: Opportunistic and Privacy-Preserving Context Collection. In: Proc.of Sixth Int. Conf. Pervasive Comput., pp. 280–297 (2008)
37. Kazemi, L., Shahabi, C.: A privacy-aware framework for participatory sensing. Acm Sigkdd Explor. Newsl. **13**(1), 43 (2011)
38. Khoshgozaran, A., Shahabi, C.: A taxonomy of approaches to preserve location privacy in location-based services. Int. J. Comput. Sci. Eng. **5**(2), 86 (2010)
39. Krontiris, I., Dimitriou, T.: A platform for privacy protection of data requesters and data providers in mobile sensing. Comput. Commun. **65**, 43–54 (2015)
40. Krontiris, I., Freiling, F.C., Dimitriou, T.: Location Privacy in Urban Sensing Networks: Research Challenges and Directions. IEEE Wirel. Commun., pp. 30–35 (2010)
41. Lee, J.-S., Hoh, B.: Sell your experiences: a market mechanism based incentive for participatory sensing. In: Proc. of 2010 IEEE Int. Conf. Pervasive Comput. Commun., pp. 60–68 (2010)
42. Li, Q., Cao, G.: Providing privacy-aware incentives for mobile sensing systems. IEEE Int. Conf. Pervsive Comput. Commun. **15**(6), 76–84 (2013)
43. Li, Q., Cao, G.: Providing efficient privacy-aware incentives for mobile sensing. In: Proc of International Conference on Distributed Computing Systems, pp. 208–217 (2014)
44. Li, Q., Cao, G., Porta, T.F.L.: Efficient and privacy-aware data aggregation in mobile sensing. IEEE Trans. Dependable Secur. Comput. **11**(2), 115–129 (2014)
45. Li, Y., Zhao, Y., Ishak, S., Song, H., Wang, N., Yao, N.: An anonymous data reporting strategy with ensuring incentives for mobile crowd-sensing. J. Ambient. Intell. Humaniz. Comput. **0**(Preprints), 1–15 (2018)
46. Li, M., Weng, J., Yang, A., Lu, W., Zhang, Y., Hou, L., Deng, R.H.: CrowdBC: a blockchain-based decentralized framework for crowdsourcing. IEEE Trans. Parallel and Distributed Systems. **30**(6), 1251–1266 (2019)
47. Liang, Y., Cai, Z., Han, Q., Li, Y.: Location privacy leakage through sensory data. Secur. Commun. Networks. **2017**, 1–12 (2017)
48. Lin, J., Yang, D., Li, M., Xu, J., Xue, G.: Frameworks for privacy-preserving Mobile Crowdsensing incentive mechanisms. IEEE Trans. Mob. Comput. **17**(8), 1851–1864 (2018)
49. Liu, A., Li, Z., Liu, G., Zheng, K., Zhang, M., Li, Q., Zhang, X.: Privacy-preserving task assignment in spatial cowdsourcing. J. Comput. Sci. Technol. **32**(5), 905–918 (2017)
50. Liu, A., Wang, W., Shang, S., Li, Q., Zhang, X.: Efficient task assignment in spatial crowdsourcing with worker and task privacy protection. GeoInformatica. **22**(2), 335–362 (2018)
51. Liu, D., Yan, Z., Ding, W., Atiquzzaman, M.: A survey on secure data analytics in edge computing. IEEE Internet of Things J. **6**(3), 4946–4967 (2019)
52. Liu, S.S., Liu, A., Yan, Z., Feng, W.: Efficient LBS queries with mutual privacy preservation in IoV. Vehicular Communications. **16**, 62–71 (2019)
53. Luo, T., Kanhere, S.S., Huang, J., Das, S.K., Wu, F.: Sustainable incentives for mobile crowdsensing: auctions, lotteries, and trust and reputation systems. IEEE Commun. Mag. **55**(3), 68–74 (2017)
54. Mun, M., et al.: PEIR, the Personal Environmental Impact Report, as a Platform for Participatory Sensing Systems Research Min. In: Proc. of the 7th international conference on Mobile systems, applications, and services - MobiSys, pp. 55–68 (2009)
55. Ni, J., Zhang, K., Lin, X., Xia, Q., Shen, X.S.: Privacy-preserving mobile crowdsensing for located-based applications. In: Proc. of IEEE International Conference on Communications, pp. 1–6 (2017)
56. Ni, J., Lin, X., Xia, Q., Shen, X.: Dual-anonymous reward distribution for mobile crowdsensing. In: Proc. of IEEE International Conference on Communications (2017)
57. Niu, X., Li, M., Chen, Q., Cao, Q., Wang, H.: EPPI: An E-cent-based privacy-preserving incentive mechanism for participatory sensing systems. In: Proc. of IEEE 33rd Int. Perform. Comput. Commun. Conf. (2015)
58. Qiu, F., Wu, F., Chen, G.: Privacy and quality preserving multimedia data aggregation for participatory sensing systems. IEEE Trans. Mob. Comput. **14**(6), 1287–1300 (2015)
59. Restuccia, F., Ghosh, N., Bhattacharjee, S., Das, S.K., Melodia, T.: Quality of Information in Mobile Crowdsensing: Survey and Research Challenges. ACM Trans. Sen. Netw, 13(34), (2017)

60. Shi, J., Zhang, R., Liu, Y., Zhang, Y.: PriSense: Privacy-preserving data aggregation in people-centric urban sensing systems. In: Proc. of 29th IEEE Int. Conf. Comput. Commun., pp. 1–9 (2010)
61. 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)
62. Shokri, R., Theodorakopoulos, G., Papadimitratos, P., Kazemi, E., Hubaux, J.-P.: Hiding in the Mobile crowd: location privacy through collaboration. IEEE Trans. Dependable Secur. Comput. **11**(3), 266–279 (2014)
63. Tao Peng, G.W., Liu, Q., Meng, D.: Collaborative trajectory privacy preserving scheme in location-based services. Inf. Sci. **387**, 165–179 (2017)
64. Terrovitis, M., Mamoulis, N.: Privacy preservation in the publication of trajectories. In: Proc. of IEEE Int. Conf. Mob. Data Manag., pp. 65–72 (2008)
65. Tun, Y., Peng, W., Lee, W.: Protecting Moving Trajectories with Dummies. In: Proc. of IEEE International Conference on Mobile Data Management (2007)
66. Vergara-Laurens, I.J., Mendez, D., Jaimes, L.G., Labrador, M.: A-PIE: an algorithm for preserving privacy, quality of information, and energy consumption in participatory sensing systems. Pervasive Mob. Comput. **32**, 93–112 (2016)
67. Wang, X., Cheng, W., Mohapatra, P., Abdelzaher, T.: Enabling reputation and trust in privacy-preserving mobile sensing. IEEE Trans. Mob. Comput. **13**(12), 2777–2790 (2014)
68. Wang, Y., Cai, Z., Yin, G., Gao, Y., Tong, X., Wu, G.: An incentive mechanism with privacy protection in mobile crowdsourcing systems. Comput. Netw. **102**, 157–171 (2016)
69. Wang, X., Liu, Z., Tian, X., Gan, X., Guan, Y., Wang, X.: Incentivizing Crowdsensing with location-privacy preserving. IEEE Trans. Wirel. Commun. **16**(10), 6940–6952 (2017)
70. Wei, Z., Zhao, B., Liu, Y., Su, J.: PPSense: A novel Privacy-Preserving system in people-centric sensing networks. In: Proc. of 8th Int. ICST Conf. Commun. Netw. China, CHINACOM 2013, pp. 461–467 (2013)
71. Wu, Y.L., Yan, Z., Choo, K.K.R., Yang, L.T.: Special session editorial: internet-of-things (IoT) big data trust management. IEEE Access. **7**(1), 65223–65227 (2019)
72. Xiao, M., Wu, J., Huang, L., Cheng, R., Wang, Y.: Online task assignment for crowdsensing in predictable mobile social networks. IEEE Trans. Mobile Computing. **16**(8), 2306–2320 (2017)
73. Xiao, M., Ma, K., Liu, A., Zhao, H., Li, Z., Zheng, K., Zhou, X.: SRA: secure reverse action for task assignment in spatial crowdsourcing. IEEE Trans. Knowledge and Data Engineering. (2019). https://doi.org/10.1109/TKDE.2019.2893240
74. Yang, D., Fang, X., Xue, G.: Truthful incentive mechanisms for k-anonymity location privacy. In: Proc. of 32th IEEE Int. Conf. Comput. Commun, pp. 2994–3002 (2013)
75. Yang, M., Zhu, T., Liang, K., Zhou, W., Deng, R.H.: A blockchain-based location privacy-preserving crowdsensing system. Futur. Gener. Comput. Syst. **94**, 408–418 (2019)
76. Yao, Y., Yang, L.T., Xiong, N.: Anonymity-based privacy-preserving data reporting for participatory sensing. IEEE Internet Things J. **2**(5), 381–390 (2015)
77. Zhai, D., Sun, Y., Liu, A., Li, Z., Liu, G., Zhao, L., Zheng, K.: Towards secure and truthful task assignment in spatial crowdsourcing. World Wide Web. (2019). https://doi.org/10.1007/s11280-018-0638-2
78. Zhang, Y., Van Der Schaar, M.: Reputation-based Incentive Protocols in Crowdsourcing Applications. In: Proc. of 31th IEEE Int. Conf. Comput. Commun, pp. 2140–2148 (2012)
79. Zhang, Y., Mao, Y., Zhang, H., Zhong, S.: Privacy preserving market schemes for mobile sensing. In: Proc. of the International Conference on Parallel Processing, pp. 909–918 (2015)
80. Zhang, Y., Chen, Q., Zhong, S.: Privacy-preserving data aggregation in Mobile phone sensing. IEEE Trans. Inf. Forensics Secur. **11**(5), 980–992 (2016)
81. Zhang, L., Wang, X., Lu, J., Li, P., Cai, Z.: An efficient privacy preserving data aggregation approach for mobile sensing. Secur. Commun. Networks. **9**(16), 3844–3853 (2016)
82. Zhang, Y., Chen, Q., Zhong, S.: Efficient and privacy-preserving min and κth min computations in Mobile sensing systems. IEEE Trans. Dependable Secur. Comput. **14**(1), 9–21 (2017)
83. Zheng, Y., Duan, H., Wang, C.: Learning the truth privately and confidently: encrypted confidence-aware truth discovery in Mobile Crowdsensing. IEEE Trans. Inf. Forensics Secur. **13**(10), 2475–2489 (2018)

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Affiliations

Yongfeng Wang [1,2] · Zheng Yan [1,3] · Wei Feng [1] · Shushu Liu [3]

Yongfeng Wang
316475890@qq.com

Wei Feng
weifeng.imk@gmail.com

Shushu Liu
liu.shushu@aalto.fi

[1] The State Key Lab of ISN, School of Cyber Engineering, Xidian University, Xi'an, China

[2] School of Mathematics and Information Technology, Yun Cheng University, Yun Cheng, China

[3] Department of Communications and Networking, Aalto University, Espoo, Finland