DOI: 10.19884/j.1672-5220.202306003

PRPS: Privacy-Preserving and Reputation-Aware Participant Selection Scheme for Mobile Crowd Sensing

AZHAR Shanila*, LIU Guohua
College of Computer Science and Technology, Donghua University, Shanghai 201620, China

Abstract: As an emerging sensing paradigm, mobile crowd sensing (MCS) comprises a collection of mobile users that utilize their sensing devices to efficiently execute and send data contributions. However, the integration of privacy and reputation mechanisms (evaluating reliability) is crucial requirements for building secure and reliable MCS applications. Firstly, participants are assured that their privacy is preserved even if they contribute sensitive personal data. Secondly, the reputation mechanism allows the server to monitor participant behaviors and reliability, as biased or inaccurate contributions may demote the system quality, making it essential for the server to validate participants. Integrating a reputation mechanism with privacy is a challenging and contradictory objective. The reputation mechanism measures the participant behavior during the entire sensing activity, while privacy aims to preserve participant credentials. Thus, a novel privacy-preserving and reputation-aware participant selection (PRPS) scheme for MCS has been proposed. The PRPS scheme integrates privacy with a reputation mechanism, preserves the privacy of participant identities and reputation values by employing pseudonyms and cloaking techniques, respectively, and protects the location and data privacy. Extensive simulations have been conducted. Using performance evaluation, we affirm precision, efficacy and scalability of the PRPS scheme by comparing privacy-preserving and utility-aware participant selection (PUPS) and utility-aware participant selection (UPS) schemes, respectively, and demonstrate the impact of privacy and reputation on data contributions. Next, the outcomes of the PRPS scheme are assessed. Finally, we estimate the efficiency and the accuracy of the PRPS scheme in evaluating participant reliability and behavior.

Key words: mobile crowd sensing (MCS); reputation; privacy; pseudonym; cloaking
CLC number: TP309.7 **Document code**: A
Article ID: 1672-5220(2024)02-0195-11

Open Science Identity (OSID)

0 Introduction

With the proliferation of smart devices and the progress of sensing and communication technology, a growing number of individuals are sharing observations and fueling the creation of mobile crowd sensing (MCS)[1-4]. MCS offers a variety of advantageous applications including detecting, collecting and scrutinizing the surrounding sensing data, as it completes sensing tasks by involving ordinary mobile users with high-performance sensing devices without any additional sensor deployment[5-8]. MCS are generally applied to various fields, such as road and traffic information, smart cities and environment monitoring[7, 9-10].

MCS has recently emerged as a hot research topic in industry and academia due to its low energy consumption, high mobility, friendly installation and maintenance, long operational time, and so on[11-13]. Thus, it is considered among the essential technologies in sensing applications of the Internet of Things (IoTs)[14]. However, despite the advantages, MCS encounters issues of privacy and security, data quality and reliability and rewarding the participants[15-18]. The openness characteristic of MCS can allow inaccurate contributions, malicious attacks, and participant data and information discloser[19]; the presence of malicious mobile users not only undermines the accuracy of the sensing data but also damages the MCS application[20]. Moreover, participant enthusiasm may be reduced due to the risk of their privacy leakage. Thus, MCS must evaluate each participant reliability[19, 21].

Therefore, this paper proposes a novel privacy-preserving and reputation-aware participant selection (PRPS) scheme. The PRPS scheme assesses each participant reliability by evaluating contribution and their past reputation values and finally rewarding them with a new reputation value. The PRPS scheme comprises three key stages: preserving participant privacy for identity, contribution, location and reputation value; selecting reliable participants according to the reputation value and contribution; assigning and updating participant reputation values. Each stage must follow multiple steps to accomplish its tasks, including equations and functions that compute reputation values. This research is an extension of our earlier work reported in Ref. [22].

The key contributions of the research are outlined

Received date: 2023-06-25
* Correspondence should be addressed to AZHAR Shanila, email: 415029@mail.dhu.edu.cn
Citation: AZHAR S, LIU G H. PRPS: privacy-preserving and reputation-aware participant selection scheme for mobile crowd sensing [J]. *Journal of Donghua University (English Edition)*, 2024, 41(2): 195-205.

below.

1) We consider that participant private information can be compromised during the sensing activity. Thus, preserving the data contribution and the location is not enough. In addition, mobile users are anonymized using the pseudonym technique by the authentication server (A_{th} server). This results in reliable participation and alleviates the abnormal effect of corrupted data and malicious users.

2) We state that the accuracy of contribution and the reliability of participants are essential for MCS. A way to assess participant contribution and reliability is evaluating their reputation values.

3) The PRPS scheme computes participant reputation values based on their current contribution and the reputation of their previous contribution (historical behaviors). The reputation of participants is concealed by using a masking/cloaking mechanism to transmit the reputation securely.

4) Simulations are conducted, and the efficacy and the effectiveness of the suggested strategy are assessed. Simulation and experimental outcomes demonstrate that the PRPS scheme achieves privacy and security objectives with an accurate evaluation of participants and rewarding them with reputation values. The PRPS scheme is compared with privacy-preserving and utility-aware participant selection (PUPS) scheme and utility-aware participant selection (UPS) scheme to show the impact of privacy and reputation on data contribution.

The remainder of this paper is structured as follows. Section 1 covers related research work. The system model, the attack model and design goals are presented in Section 2. Section 3 presents the PRPS scheme. The performance assessment, simulation setup and outcomes are discussed in Section 4. The conclusions are outlined in Section 5.

1 Related Work

In the MCS context, the open, large and dynamic environment makes it challenging to assess the participant reliability. Vital concern of a service provider (SP) is to gather data from reliable participants. The rational participant will not actively submit the sensing data voluntarily and requires a reward to participate. The unreliable participants may deliberately send inaccurate data to get more rewards or mislead system results[23].

A few research analyzes confined strategies for addressing mobile user participation in the MCS system with suitable incentives such as reputation. The participant selection scheme[24] chose suitable mobile users for sensing tasks and considered a reputation mechanism to assess the reliability of the data, but ignored the participant privacy. Reputation mechanisms can minimize threats and damage of manipulative and malicious mobile users. Thus, the mobile user reputation is crucial for the MCS system[25-26].

Kantarci et al.[27] and Sun et al.[28] considered the reputation-awareness incentive scheme to collect data and increase data quality. A reputation management system that involves the participant analysis prior to the sensing task has been demonstrated by Yang et al.[29]. The applicant specifies the requirement list and later rates and selects participants who fit these criteria based on their reputation values. Restuccia et al.[30] proposed a reputation management system that maintained a list of trusted individuals who consistently sensed reliable data and were protected from outside threats. Hence, the system determined nearby a trusted participant and evaluated other participant contributions based on these trusted participant contributions. A reputation technique depending on the participant prior contributions assessed by the quality of sensor data was suggested by Manzoor et al.[31]. The quality evaluator evaluates the data quality and past reputations to analyze the participant recent reputations. However, the privacy of participants was not targeted in Ref. [31].

Approaches proposed in Refs. [32-35] implemented a reputation mechanism for measuring the participant reliability. Upon completion of the sensing task, a high-reputation value was assigned to reliable participants, whereas a low-reputation value was allotted to malicious participants. Nevertheless, these assigned reputation values relied on the current sensing report and disregarded the past reputation values, leading to inaccurate results.

Many reputation techniques and privacy-protecting methods have been examined in the literature. However, due to the conflict between privacy-preservation and rewarding reputation, several studies focused on privacy and reputation challenges separately[20]. The integration of these systems in MCS is still in its infancy. A reputation mechanism is crucial for a reliable MCS system that allows the server to select the optimal set of reliable participants. To achieve good quality of sensing data, recruiting participants possibly requires compensating rewards to mobile users to encourage and ensure reliable contributions[25]. Amintoosi et al.[36] demonstrated the user quality and the reputation level in social networks, and Huang et al.[37] considered data and reputation based on time. However, both ignored the rewarding mechanism. Hu et al.[38] proposed the reputation mechanism for vehicular networks based on the reputation value; the third-party reputation management center, in this case, was accountable for managing reputation. The past reputation of the mobile users reflects the participant past behavior and reliability. We aim to consider the contribution and the past reputation as parameters for recruiting mobile users to reduce the threat of dishonest users. However, the needless necessity of a reputation center is eliminated. Christin et al.[39] discussed the issue of managing the reputation of anonymous participants by applying pseudonyms and secret transfers of reputation using blind signatures. Reference [36] also proposed a reputation system for anonymous participatory sensing,

and preserved privacy by separating participant identities from their reputations.

The privacy concerns with the reputation design in mobile sensing are emphasized by Wang et al.[40] and Yang et al.[34]. The reputation values connected to a particular identity and data contribution may potentially lead to identifying participants[29, 39-40]. However, schemes proposed in Refs. [33-34, 41] overlooked the privacy of participants and the reputation scheme. In practice, the majority of the present privacy approaches in MCS focused on either sensed data privacy[34], reputation privacy[35], location privacy[39], or participant privacy[40], separately, but failed to consider all the above into one study[42].

Zheng et al.[43] and Li et al.[44] utilized a pseudonym-based method to provide anonymity to mobile users (also known as random pseudonyms). However, the un-linkability between real identities and pseudonyms can be assured. Merging it with another approach, e. g., cloaking or encryption, can hide other information. To prevent identification, the cloaking approach substitutes the original data with its corresponding anonymized data[45]. The reputation mechanism is excessively used in assessing participant trustworthiness[42]. Integrating anonymity and encryption prevents adversaries from inferring and linking the sensing information of the participants.

Due to the above reasons, the light-weight privacy-preserving scheme[22] is used to preserve the reputation, contribution and location of participants and it is integrated with the proposed reputation mechanism to effectively select reliable participants. In contrast to previous approaches, our scheme preserves participant privacy, and evaluates and assigns the reputation values. Importantly, the suggested scheme does not need a reputation authority (RA) or reputation server (RS), and scales effectively with the number of participants.

2 Problem Formulation

In this section, we delineate the system model (Fig. 1), the attack model, and aimed design goals.

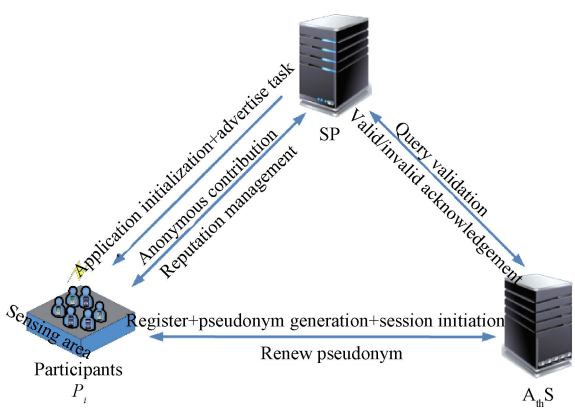

Fig. 1 System model for MCS

2.1 System model

The MCS system model, as depicted in Fig. 1, comprises three entities in the sensing campaign, namely, SP, $A_{th}S$ and participants P_i ($i=1, 2, \cdots, n_m$, where n_m is the number of mobile users), and shows the relationship between the three entities. $A_{th}S$ is the trustworthy entity engaged in the attack model. The following definitions emphasize the basic responsibilities in steps and assumptions pertaining to each entity.

1) P_i is an entity that participates in data collection and is capable of executing the sensing task assigned by SP. Firstly, P_i authenticates with $A_{th}S$, and requests and receives a pseudonym. Secondly, P_i selects a task broadcasted by SP. Thirdly, P_i generates the sensing contribution C_i and sends C_i together with its reputation $R_{v,i}$ to SP. Fourthly, P_i re-authenticates with $A_{th}S$ for a new task after completion of the sensing task. P_i cannot alter their pseudonyms and cannot fake their identity and reputation values.

2) SP is responsible for broadcasting and distributing tasks to mobile users. Firstly, SP initiates a sensing campaign. Secondly, SP queries participant validation from $A_{th}S$ and receives valid/invalid acknowledgement report from $A_{th}S$. Thirdly, SP collects and aggregates the sensing reports, applies a reputation mechanism, and evaluates contribution and reputation. Fourthly, SP computes a new reputation $R'_{v,i}$, and assigns and forwards it to P_i. SP knows the participant contributions and reputation values. However, the participant actual locations and identities are concealed.

3) $A_{th}S$ is a trusted entity responsible for authenticating participants and generating pseudonyms. Firstly, $A_{th}S$ generates and sends the pseudonym identity PID_i^0 to P_i. Secondly, $A_{th}S$ renews and transfers these pseudonyms PID_i^n after each campaign to P_i. $A_{th}S$ maintains a record of the participant pseudonyms in succession, knows the participant P_i, but is unaware of the participants' other attributes. $A_{th}S$ discards the old pseudonym PID_i^0, so an adversary cannot use it again. Only $A_{th}S$ knows old and new PID_i^1 and can identify the malicious user in the attack detection process.

Figure 2 illustrates in detail the complete protocol of the PRPS scheme and highlights the key activities that are carried out in the entire sensing process, while taking reputation and privacy into consideration. By broadcasting a sensing task, SP aims to collect data from the specified region. Each P_i (within the vicinity) interested to participate in the sensing task is related with following characteristics.

1) Reputation $R_{v,i}$ indicates reliability, credibility and trustworthiness of P_i with regard to the past contribution. SP evaluates the participant reliability based on the previous behavior and recently transmitted contribution, and computes the new reputation value. It is a vital

attribute, and SP aims to select participants with high $R_{v,i}$, as low $R_{v,i}$ can degenerate MCS reliabilty.

2) Contribution C_i is the sensed data that P_i provides at a particular sensing location. The accuracy of C_i is essential, as it can lead to task results success or failure, and can affect MCS performance and reliability.

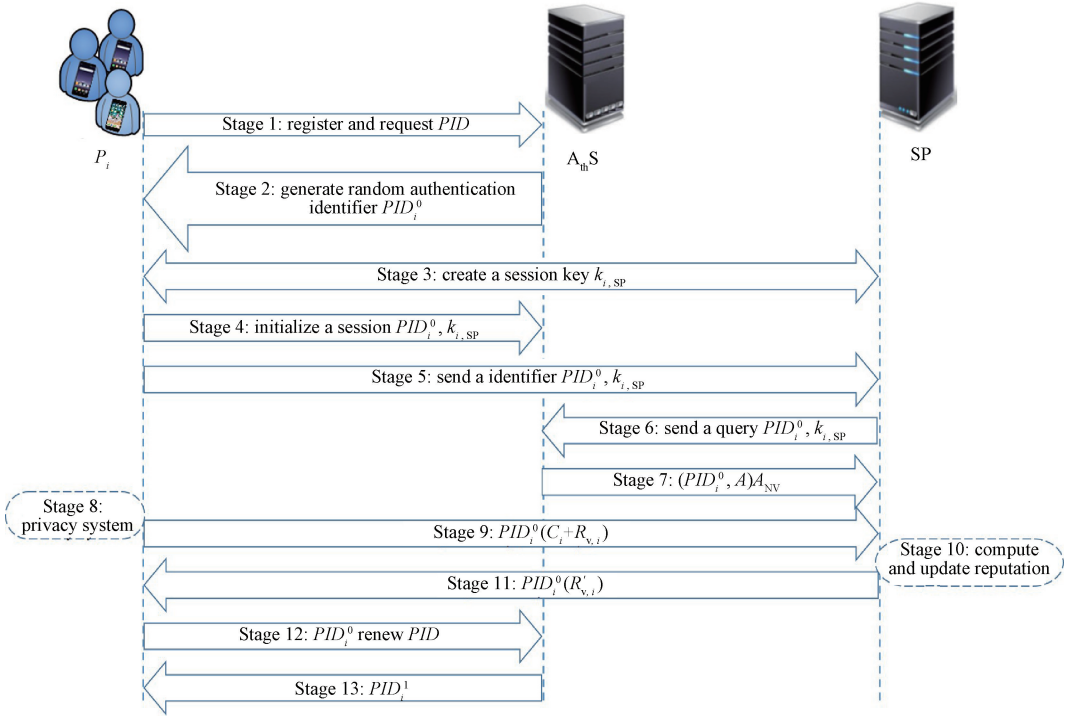

Fig. 2 Protocol of PRPS scheme for MCS system

In addition, $R_{v,i}$ and C_i are privacy sensitive and should not be disclosed or inferred.

The stages below depict the sensing processes in the PRPS scheme for the MCS system, as identified in Fig. 2. (Note: presuming that the participants have necessary Apps on their smartphones).

Stage 1: P_i initially registers with $A_{th}S$.

Stage 2: $A_{th}S$ generates the first random authentication identifier PID_i^0, and allocates it to P_i.

Stage 3: P_i and SP collaborate to create a session key $k_{i,SP}$.

Stage 4: to start the session, P_i transmits $k_{i,SP}$ to $A_{th}S$.

Stage 5: $A_{th}S$ stores this key and acknowledges P_i, informing that the session has begun at $A_{th}S$. P_i sends its first anonymous identitier PID_i^0 to SP.

Stage 6: SP sends a query about PID_i^0 to $A_{th}S$.

Stage 7: if the identification matches the received identifiers, $A_{th}S$ verifies it. A valid acknowledgement is replied to SP. This certificate contains its current identifier and valid acknowledgement PID_i^0 and A. Otherwise, a non-valid acknowledgement A_{NV} is replied.

Stage 8: if P_i is correctly verified by $A_{th}S$, PID_i^0 senses its environment and constructs its first C_i, adopting a privacy-preserving scheme[22] on the report contents.

Stage 9: this report $P_{r,i}$ contains PID_i^0 first contribution and existing reputation $PID_i^0(C_i + R_{v,i})$; $P_{r,i}$ is then forwarded to SP.

Stage 10: SP receives the report, assesses PID_i^0 contribution and previous reputation (using the PRPS scheme), and calculates a new reputation.

Stage 11: after computation, the new reputation $R'_{v,i}$ is sent back to PID_i^0, indicating the completion of a task.

Stage 12: P_i contacts the $A_{th}S$ to get a new pseudonym PID_i^1 by submitting its most recent pseudonym PID_i^0.

Stage 13: the new pseudonym is forwarded to P_i.

The pseudonym and the cloaking are only valid within the duration of the task activity; after that, it is discarded and reusable for another activity.

2.2 Attack model

During the participant selection, participants seek to conceal sensing locations and contributions from malicious participants. Therefore, the main privacy leakage risks are caused by internal adversaries who participate in the sensing and reporting processes. Adversaries are defined as follows.

1) Honest-but-curious: P_i and SP are viewed as passive adversaries and adhere to the semi-honest model. It indicates that they follow the pre-defined protocols honestly, yet are interested in confidential data, location, contribution and reputation of others and attempt to infer as much as possible. However, SP is considered as a curious but trusted entity.

2) Collusive: P_i may also conspire with one another or with SP to divulge additional private information via sharing.

3) Trusted: $A_{th}S$ is the trusted entity incorporated to manage the attack model. Under the attack model, it enables adversaries with low reputations to submit requests in sensing tasks.

2.3 Design goals

The proposed PRPS scheme for MCS applications has the following design goals.

1) The sensing reports in the PRPS scheme do not contain the real identity of P_i, and SP cannot associate it with a particular participant. Similarly, mobile users cannot falsify identity, and be revealed to other users.

2) The un-linkability between a participant actual identity and pseudonym is achieved through $A_{th}S$. Only P_i and $A_{th}S$ are aware of the participant identity. However, $A_{th}S$ is unaware of other attributes of participants.

3) Reputation of each participant is determined by the previous behavior, and P_i does not have control over the update process. Further, this reputation value cannot be falsified or discarded. Each participant reputation is updated and managed in a way that does not compromise their anonymity.

4) The privacy attacks are mitigated or avoided by evaluating contribution and reputation values of mobile users, distinguishing them from malicious ones.

3 PRPS Scheme

A summary of the PRPS scheme and the algorithms is provided.

3.1 PRPS scheme overview

To preserve the privacy of participant contribution and reputation values, it is cloaked by using a one-time padding cloaking technique[22]. One-time padding cloaking relies on the fact that when SP gets reports from all participants and computes the summation, the secret values S_v will be nullified. In this way, there is no undesirable impact on the accuracy of the contribution and reputation values.

S_v is shared in advance as a collective seed to avoid the overhead of quadratic communication due to swapping between participants. However, in consideration of security, S_v will only be used once. Thus S_v is subjected to the secure hash function $h(\cdot)$ that is already known to every participant. For updating S_v, the new mask is calculated as $h(S_v)$.

The participants obtain the SP public key (Pk_{sp}) by public key infrastructure (PKI). For instance, in a scheme, P_i and P_j encrypt Reports (1) and (2) and send them to SP, respectively.

$$E_{Pk_{sp}}(PID_i^0(C_i + R'_{v,i}) + S_v), \quad (1)$$

$$E_{Pk_{sp}}(PID_j^0(C_j + R'_{v,j}) - S_v). \quad (2)$$

When SP receives the two cipher-texts, it decrypts the cipher-texts using the secret key (Sk_{sp}), i.e.,

$$P_{r,i} = D_{Sk_{sp}}[E_{Pk_{sp}}(PID_i^0(C_i + R'_{v,i}) + S_v)], \quad (3)$$

$$P_{r,j} = D_{Sk_{sp}}[E_{Pk_{sp}}(PID_j^0(C_j + R'_{v,j}) - S_v)], \quad (4)$$

and gets the following Report (5) to perform further operations on them.

$$P_r = PID_i^0(C_i + R'_{v,i}) + PID_j^0(C_j + R'_{v,j}). \quad (5)$$

Figure 3 shows the data flow from participant smartphones to SP through the PRPS scheme. The PRPS scheme consists of three main stages. Stage I involves receiving the privacy-preserving participant report. In stage II, the scheme computes each participant reputation weight in a sensing area, selects contribution of participants with the highest reputation value, and collects at SP. In stage III, the PRPS scheme updates participant reputation value based on their contributions and past reputations, and assigns a positive value to the selected participants with the highest reputation value.

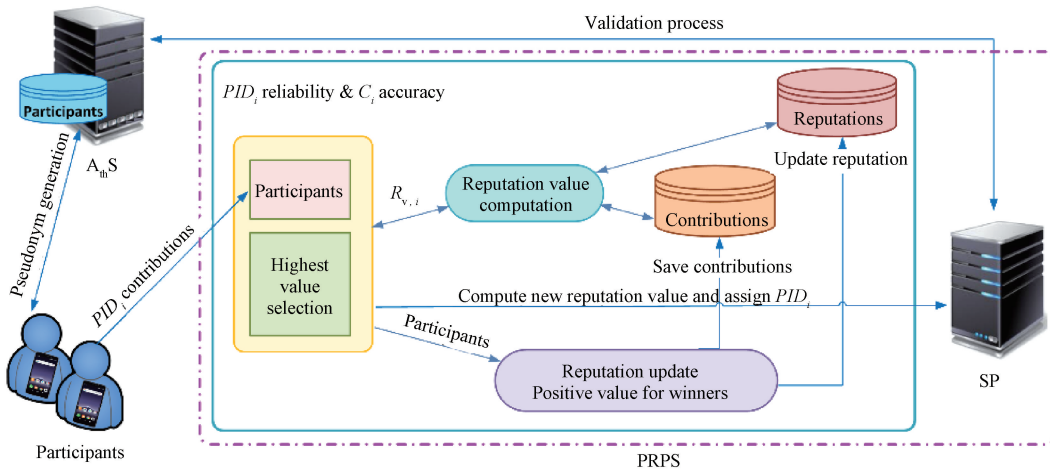

Fig. 3 Layout of reputation mechanism in PRPS scheme

SP maintains two databases at the PRPS scheme: the reputation database (RDB) that records each participant reputation information, and the contribution database (CDB) that records all contributions that are executed by participants. Further, the PRPS scheme provides two modes of operation, namely, oldie and newbie, to help make decisions in selecting reliable participants.

3.2 Reputation-based selection algorithm

In Algorithm 1, the PRPS scheme firstly collects participant contributions as input. It then chooses participants with reliable contributions and reputation values, and evaluates participants. Finally, it assigns participants new reputation values as output.

Algorithm 1 PRPS scheme

Input: participant contributions
Output: accurate contributions; update reputation

Sensing area weight $S_{w,i}$ calculation
1. Get participant reputation values // *Call Algorithm* 2
2. for $x \leftarrow 1$ to n do
3. $R_{v,x} \leftarrow \sum R_{v,i}$
4. for $i \leftarrow 1$ to n do
5. $W_i \leftarrow \dfrac{R_{v,i}}{R_{v,x}}$
6. $S_{w,i} \leftarrow \sum W_i R_{v,i}$

Highest reputation value R_{vh}
7. for $i \leftarrow 1$ to n do
8. if $R_{v,i+1} \leqslant R_{v,i} \geqslant R_{v,i+2}$
9. then $R_{vh} \leftarrow R_{v,i}$
10. else if $R_{v,i+1} \geqslant R_{v,i+2}$
11. then $R_{vh} \leftarrow R_{v,i+1}$
12. else $R_{vh} \leftarrow R_{v,i+2}$

Send C_i of R_{vh} to SP

V_P or V_N, updating reputation value
13. for $i \leftarrow 1$ to n do
14. if $R_{v,i} = R_{vh}$
15. then
16. for $i \leftarrow 1$ to n do
17. $V_{P,i} \leftarrow V_{P,i} + 1$
18. else
19. for $i \leftarrow 1$ to n do
20. $V_{N,i} \leftarrow V_{N,i} + 1$
21. $R'_{v,i} = \delta C_i + (1 - \delta) R_{v,i}$

Send $R'_{v,i}$ of *PID* to SP and *PID*

After gathering all participant sensed data (contribution C_i), the PRPS scheme computes the total sensing area weight $S_{w,i}$. The next stage involves calculating participant reputation values $R_{v,i}$ from Algorithm 2, for $i = 1, 2, \cdots, n$, where n is the total number of participants. When the reputation values of participants (Step 1) are computed, the scheme computes each participant reputation weight W_i among all other participants (Steps 2-5). The total weight of all participants in the sensing area is one.

Definition 1 In a task for n participants with contributions, the participant reputation weight is

$$W_i = \frac{R_{v,i}}{\sum_{i \in n} R_{v,i}}. \tag{6}$$

Definition 2 The sensing area weight is

$$S_{w,i} = \sum_{i \in n} W_i R_{v,i}. \tag{7}$$

Steps 7 - 12 compare the reputation values of participants, select among them the highest value R_{vh} as the reputable participants, and accept C_i of the winner at SP for further computations.

Lastly, $R_{v,i}$ values of the selected participants are updated by the PRPS scheme as a positive value V_P and a negative value V_N for accurate and inaccurate C_i, respectively (Steps 13-21), which either rise or decline $R_{v,i}$. Suppose that from previous (total 9) contributions, $R_{v,i}$ of participant P_i is 77.8% from $7V_P$ and $2V_N$. If P_i acquires a V_P in a new contribution, $R_{v,i}$ becomes 80%. However, if it receives a V_N, $R_{v,i}$ becomes 70%.

Algorithm 2 Participant reputation value computation

Input: participants
Output: participant reputation values

1. for $i \leftarrow 1$ to n do
2. if $X_i < z$ // *Newbie*
3. then $R_{v,i} \leftarrow$ np
$\delta \leftarrow I$ // $I = 0.60$
4. else if $X_i < Q$ // *Oldie*
5. then $V_{PT,i} \leftarrow \sum V_{P,i}$
6. $T_i \leftarrow X_i$
$\delta \leftarrow D$ // $D = 0.50$
7. else for $x \leftarrow X_i - (Q - 1)$ to X_i do
8. $V_{PT,i} \leftarrow \sum V_{P,x}$
9. $T_i \leftarrow Q$
10. $R_{v,i} \leftarrow \dfrac{V_{PT,i}}{T_i}$

3.3 Reputation value computation algorithm

Reputation metrics demonstrate participant steadiness and reliability and allow the PRPS scheme to make a selection decision.

Definition 3 To evaluate the reliability, a new definition is introduced to compute the recent reputation value of the participant:

$$R'_{v,i} = \delta C_i + (1 - \delta) R_{v,i}, \tag{8}$$

where C_i is the current contribution (calculated as in Ref. [46]); $R_{v,i}$ is the past reputation value; δ is the

coefficient that decides the weightage among C_i and $R_{v,i}$ to compute participants new reputation value. The MCS application may set the value of δ depending on their requirements for reliability criteria.

The process to compute $R_{v,i}$ is shown in Algorithm 2. $R_{v,i}$ could be calculated by the two criteria as newbie and oldie. For a new participant (np) newbie (Steps 2-3), the scheme firstly assigns $R_{v,i} = 0.50$, an initial value. Then, participant P_i constructs recent reputation through their submitted contributions. Finally, the scheme assigns δ to be 0.60. For a mature participant, i.e., an oldie, it gives disreputable P_i chance to re-establish their reputations (Steps 4-9) in case of multiple contributions. The PRPS scheme selects the minimum number of two sets of contributions, X or Q, where X denotes the overall individual contributions and Q represents the required number of contributions to be qualified as an oldie.

When X is the minimum number of contributions, the total positive value $V_{PT,i}$ of P_i equals the sum of positive values of participant reputation in the past contributions (Steps 4-6). When Q is the minimum number of contributions, $V_{PT,i}$ is the sum of positive values of participant reputations in the last Q contributions (Steps 7-9). Lastly, the historic reputation value $R_{v,i}$ of P_i is computed (Step 10)

$$R_{v,i} = \frac{V_{PT,i}}{T_i}. \tag{9}$$

4 Performance Evaluation

Extensive simulations were performed to provide accurate results of the PRPS scheme to assess their performance. The PRPS scheme assesses all participant reputations, chooses the most reliable contributions, transfers them to SP, and updates and assigns the computed reputation values to participants. Initially, we compared the PRPS scheme with PUPS[22] and UPS[46] schemes and examined their performance trends to show the inferiority of the PRPS scheme. Later, we illustrated the scenarios of participant behaviors and the impact on reputation values. Finally, we investigated the PRPS scheme for its evaluation accuracy.

4.1 Simulation setup

In the MCS system, the sensing area of approximately 10 km × 10 km was considered. In the given area, 200 mobile device users were randomly distributed in the grid. The data contributions and reputation values are real values between [0, 1]. The uniform distribution is employed to generate sensing contribution and reputation values of each participant. We conducted different simulations and analyzed the trends while building the related parameters. Then, we evaluated the PRPS scheme and illustrated the reputation value patterns. The parameters for the simulations are shown in Table 1.

Table 1 Simulation parameters

Parameter	Value
Simulation area/km^2	100
Total No. of P_i	50 to 200
Total No. of contributions X	$0 < X < 10$
C_i	$0 < C_i < 1$
$R_{v,i}$	$0 < R_{v,i} < 1$

4.2 Performance comparison

In the simulation, we determine the scheme performance and notice the trend of accumulated contributions achieved for 10 rounds. Figure 4 depicts the contribution curves and clearly shows that our light-weight PRPS scheme achieves higher contribution levels in the existence of reputation and privacy than the other two schemes.

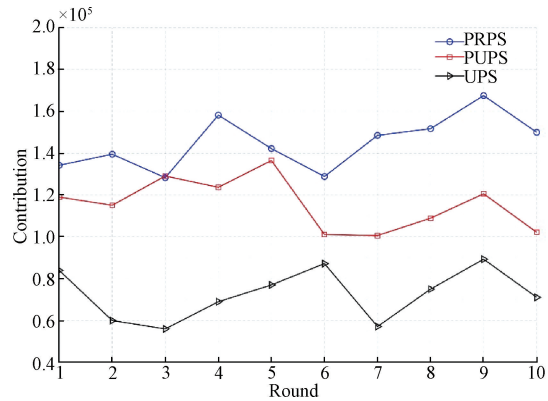

Fig. 4 Comparison of achieved data contributions among PRPS, PUPS, and UPS schemes for 10 rounds

4.3 Impact of participant behavior on reputation values

Accuracy performance of the PRPS scheme was estimated for distinct participant behaviors through Algorithms (1) and (2) and Eqs. (6)-(9). For a sensing campaign, an outcome of 200 participants was studied, and the behavior of participants was split into two categories: category A and category B.

In category A, participants with high $R_{v,i}$ and high C_i acquire high $R'_{v,i}$. Similarly, participants with low $R_{v,i}$ and high C_i acquire high $R'_{v,i}$.

In category B, participants with high $R_{v,i}$ and low C_i get a penalty resulting in a drop in their $R'_{v,i}$. Similarly, participants with low $R_{v,i}$ and low C_i receive low $R'_{v,i}$. Figure 5 (a) depicts the resultant reputation values of participants.

Then, we considered the scenario X where it was assumed that 15 out of 100 participants changed their behaviors, which caused their transition from category A to category B. In Fig. 5 (b), a drop in reputation values reflects the transitions of categories. This scenario enables us to evaluate the performance of the PRPS scheme.

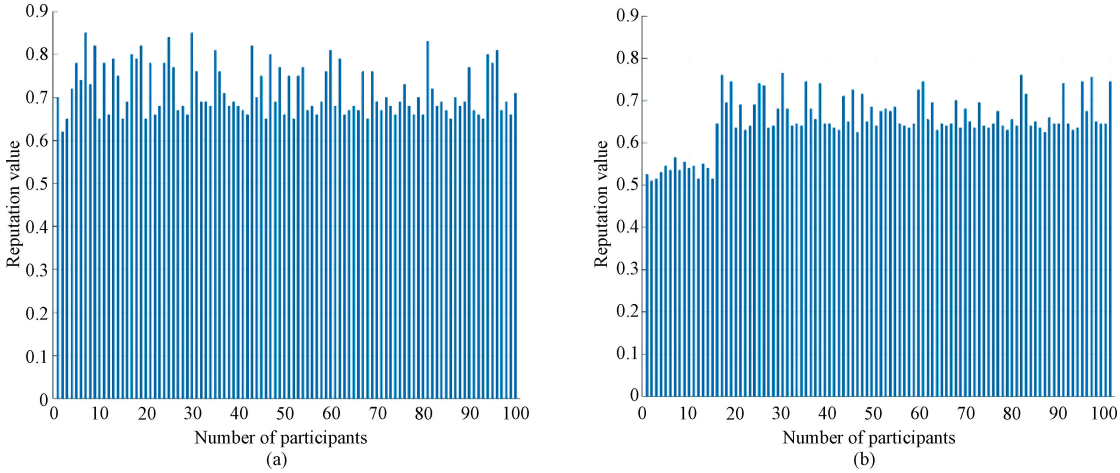

Fig. 5 Reputation values: (a) participants; (b) in scenario X

To recapitulate, the PRPS scheme outperforms in providing high accumulated contributions; it accurately assesses the reliability of participants and their reputations and successfully assigns the reputation values to distinct behavior participants.

4.4 Assessing PRPS scheme outcomes

Determining the participant reliability and identifying precise contributions are vital duties of SP. Therefore, we use a false positive rate (FPR) R_{FP} and a false negative rate (FNR) R_{FN} as two indicators to assess the accuracy of PRPS scheme outcomes in participant evaluation.

False positive (FP) means that the participant is actually unreliable, yet outcomes show that calculated reputation values are above the specified threshold. False negative (FN) means that the participant is actually reliable, while outcomes show that computed reputation values are below the threshold value. To distinguish participants (reliable ones from unreliable ones), a threshold percentage is assigned to reputation values. Depending on the predetermined threshold value, there is an inverse connection between FP and FN. Higher thresholds result in a lower FPR and a higher FNR.

In our system, we randomly classified participants into reliable ones and unreliable ones, and randomly selected participants for different ranges from 50, 100, 150 and 200 and set the metrics to three different thresholds (65%, 75% and 85%) to display the accuracy rates of evaluating participants in distinct settings. FPR and FNR are computed as

$$R_{FP} = \frac{P_U}{T_{PT}}, \tag{10}$$

$$R_{FN} = \frac{P_R}{T_P - T_{PT}}, \tag{11}$$

where P_U represents the total sum of all unreliable participants with reputation values higher than the threshold value in T_P (a set of a total number of participants $T_P = \{50, 100, 150, 200\}$); P_R is the total sum of all reliable participants with reputation values lower than T_P threshold; T_{PT} is the total number of participants whose reputation values are above the threshold value in T_P.

By executing FPR and FNR in Eqs. (10) and (11), for a set of 50 participants with a threshold of 65%, we get a subset of 40 participants above the threshold and 10 participants below the threshold. Similarly, for a set of 100, 150 and 200 participants, we obtain a subset of 75, 108 and 165 participants above the threshold and 25, 42 and 35 participants below the threshold, with FPR of 5%, 6% and 7%, and FNR of 4%, 2% and 2%, respectively. Figure 6 reflects FPR and FNR outcomes for all three threshold levels.

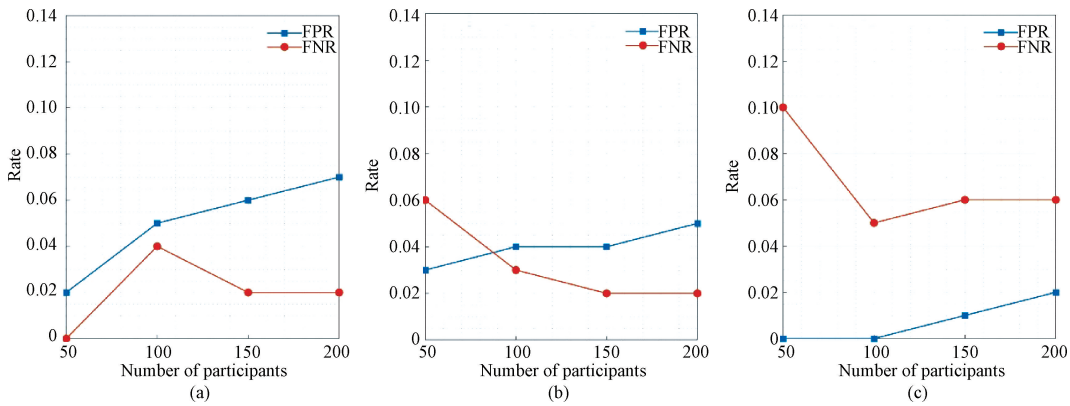

Fig. 6 FPR and FNR with three thresholds for PRPS scheme: (a) 65% threshold; (b) 75% threshold; (c) 85% threshold

5 Conclusions

This paper proposes a PRPS scheme for the MCS application. The PRPS scheme adopts a light-weight privacy system to preserve identity, location, sensing contribution and reputation value privacy. In addition, participant reliability is ensured by the incorporation of a reputation system. The PRPS scheme assesses participants, validates the contributions and reputation values, and effectively assigns reputation values to them. Further, the PRPS scheme is presented via the theoretical analysis and the experimental assessment. The evaluation results show that the PRPS scheme accurately assesses the participants, and it identifies participant behaviors in the sensing task and assigns them new reputation values. For future work, we propose to expand the MCS system for multi-purpose sensing tasks.

References

[1] LV Z H, QIAO L, HOSSAIN M S, et al. Analysis of using blockchain to protect the privacy of drone big data[J]. *IEEE Network: the Magazine of Global Internetworking*, 2021, 35(1): 44-49.

[2] GANTI R, YE F, LEI H. Mobile crowdsensing: current state and future challenges[J]. *IEEE Communications Magazine*, 2011, 49(11): 32-39.

[3] WU Y B, SHENG H, ZHANG Y, et al. Hybrid motion model for multiple object tracking in mobile devices[J]. *IEEE Internet of Things Journal*, 2023, 10(6): 4735-4748.

[4] MA J Y, HU J P. Safe consensus control of cooperative-competitive multi-agent systems via differential privacy[J]. *Kybernetika*, 2022: 426-439.

[5] HU J H, WANG Z B, WEI J, et al. Towards demand-driven dynamic incentive for mobile crowdsensing systems[J]. *IEEE Transactions on Wireless Communications*, 2020, 19(7): 4907-4918.

[6] PENG Y, ZHAO Y Y, HU J P. On the role of community structure in evolution of opinion formation: a new bounded confidence opinion dynamics[J]. *Information Sciences*, 2023, 621: 672-690.

[7] MONTORI F, BEDOGNI L, BONONI L. A collaborative Internet of Things architecture for smart cities and environmental monitoring[J]. *IEEE Internet of Things Journal*, 2018, 5(2): 592-605.

[8] PENG Z N, HU J P, SHI K B, et al. A novel optimal bipartite consensus control scheme for unknown multi-agent systems via model-free reinforcement learning[J]. *Applied Mathematics and Computation*, 2020, 369: 124821.

[9] JIANG H B, WANG M Y, ZHAO P, et al. A utility-aware general framework with quantifiable privacy preservation for destination prediction in LBSs[J]. *IEEE/ACM Transactions on Networking*, 2021, 29(5): 2228-2241.

[10] GUO L H, CHENG S, LIU J, et al. Does social perception data express the spatio-temporal pattern of perceived urban noise? A case study based on 3137 noise complaints in Fuzhou, China[J]. *Applied Acoustics*, 2022, 201: 109129.

[11] CHEN X L, XU S S, FU H H, et al. ASC: actuation system for city-wide crowdsensing with ride-sharing vehicular platform[C]//Proceedings of the Fourth Workshop on International Science of Smart City Operations and Platforms Engineering. Quebec: [s. n.], 2019: 19-24.

[12] WANG H, CUI Z W, LIU R G, et al. A multi-type transferable method for missing link prediction in heterogeneous social networks[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2023, 35(11): 10981-10991.

[13] CAO K R, WANG B H, DING H Y, et al. Achieving reliable and secure communications in wireless-powered NOMA systems[J]. *IEEE Transactions on Vehicular Technology*, 2021, 70(2): 1978-1983.

[14] LIU J W, SHEN H Y, NARMAN H S, et al. A survey of mobile crowdsensing techniques: a critical component for the Internet of Things[J]. *ACM Transactions on Cyber-Physical Systems*, 2018, 2(3): 1-26.

[15] OWOH N P, SINGH M M. Security analysis of mobile crowd sensing applications[J]. *Applied Computing and Informatics*, 2022, 18(1/2): 2-21.

[16] BOUBICHE D E, IMRAN M, MAQSOOD A, et al. Mobile crowd sensing Taxonomy, applications, challenges, and solutions[J]. *Computers in Human Behavior*, 2019, 101: 352-370.

[17] YU J D, LU L, CHEN Y Y, et al. An indirect eavesdropping attack of keystrokes on touch screen through acoustic sensing[J]. *IEEE Transactions on Mobile Computing*, 2021, 20(2): 337-351.

[18] KONG H, LU L, YU J D, et al. Continuous authentication through finger gesture interaction for smart homes using WiFi[J]. *IEEE Transactions on Mobile Computing*, 2021, 20(11): 3148-3162.

[19] ZHANG X L, LIANG L Y, LUO C W, et al. Privacy-preserving incentive mechanisms for mobile crowdsensing[J]. *IEEE Pervasive Computing*, 2018, 17(3): 47-57.

[20] MOUSA H, BEN MOKHTAR S, HASAN O, et al. Trust management and reputation systems

in mobile participatory sensing applications: a survey[J]. *Computer Networks*, 2015, 90: 49-73.

[21] LI M J, TIAN Z H, DU X J, et al. Power normalized cepstral robust features of deep neural networks in a cloud computing data privacy protection scheme[J]. *Neurocomputing*, 2023, 518: 165-173.

[22] AZHAR S, CHANG S, LIU Y, et al. Privacy-preserving and utility-aware participant selection for mobile crowd sensing[J]. *Mobile Networks and Applications*, 2022, 27(1): 290-302.

[23] DOWNS J S, HOLBROOK M B, SHENG S, et al. Are your participants gaming the system? Screening mechanical Turk workers [C]// Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Georgia: [s.n.], 2014: 2399-2402.

[24] REN J, ZHANG Y X, ZHANG K, et al. SACRM: social aware crowdsourcing with reputation management in mobile sensing[J]. *Computer Communications*, 2015, 65: 55-65.

[25] ZHOU T Q, CAI Z P, WU K, et al. FIDC: a framework for improving data credibility in mobile crowdsensing[J]. *Computer Networks*, 2017, 120: 157-169.

[26] XU L, YU S J, FENG Z N, et al. Trustworthy and efficient data trading in decentralized mobile crowd sensing systems[J]. *Journal of Donghua University (English Edition)*, 2024, 41(1): 89-101.

[27] KANTARCI B, MOUFTAH H T. Reputation-based sensing-as-a-service for crowd management over the cloud[C]//2014 IEEE International Conference on Communications (ICC). New York: IEEE, 2014: 3614-3619.

[28] SUN J Y, PEI Y Y, HOU F, et al. Reputation-aware incentive mechanism for participatory sensing[J]. *IET Communications*, 2017, 11(13): 1985-1991.

[29] YANG H F, ZHANG J L, ROE P. Using reputation management in participatory sensing for data classification[J]. *Procedia Computer Science*, 2011, 5: 190-197.

[30] RESTUCCIA F, DAS S K. FIDES: a trust-based framework for secure user incentivization in participatory sensing[C]//Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks. New York: IEEE, 2014: 1-10.

[31] MANZOOR A, ASPLUND M, BOUROCHE M, et al. Trust evaluation for participatory sensing [C]//Mobile and Ubiquitous Systems: Computing, Networking, and Services: 9th International Conference. Berlin: Springer, 2013.

[32] GAO S, CHEN X H, ZHU J M, et al. TrustWorker: a trustworthy and privacy-preserving worker selection scheme for blockchain-based crowdsensing[J]. *IEEE Transactions on Services Computing*, 2022, 15(6): 3577-3590.

[33] DAI M H, SU Z, XU Q C, et al. A trust-driven contract incentive scheme for mobile crowd-sensing networks[J]. *IEEE Transactions on Vehicular Technology*, 2022, 71(2): 1794-1806.

[34] YANG X X, ZHANG J, PENG J, et al. Incentive mechanism based on Stackelberg game under reputation constraint for mobile crowdsensing[J]. *International Journal of Distributed Sensor Networks*, 2021, 17(6): 155014772110230.

[35] NI J B, ZHANG K, XIA Q, et al. Enabling strong privacy preservation and accurate task allocation for mobile crowdsensing[J]. *IEEE Transactions on Mobile Computing*, 2020, 19(6): 1317-1331.

[36] AMINTOOSI H, KANHERE S S. A reputation framework for social participatory sensing systems[J]. *Mobile Networks and Applications*, 2014, 19(1): 88-100.

[37] HUANG K L, KANHERE S S, HU W. On the need for a reputation system in mobile phone based sensing[J]. *Ad Hoc Networks*, 2014, 12: 130-149.

[38] HU H, LU R X, HUANG C, et al. TripSense: a trust-based vehicular platoon crowdsensing scheme with privacy preservation in VANETs[J]. *Sensors*, 2016, 16(6): 803.

[39] CHRISTIN D, ROßKOPF C, HOLLICK M, et al. IncogniSense: an anonymity-preserving reputation framework for participatory sensing applications[J]. *Pervasive and Mobile Computing*, 2013, 9(3): 353-371.

[40] WANG X O, CHENG W, MOHAPATRA P, et al. ARTSense: anonymous reputation and trust in participatory sensing[C]//2013 Proceedings IEEE INFOCOM. New York, IEEE, 2013: 2517-2525.

[41] WU D P, SI S S, WU S E, et al. Dynamic trust relationships aware data privacy protection in mobile crowd-sensing[J]. *IEEE Internet of Things Journal*, 2018, 5(4): 2958-2970.

[42] ZHAO B W, TANG S H, LIU X M, et al. PACE: privacy-preserving and quality-aware incentive mechanism for mobile crowd sensing[J]. *IEEE Transactions on Mobile Computing*, 2021, 20(5): 1924-1939.

[43] ZHENG Y, XIE X, MA W Y. GeoLife: a collaborative social networking service among user, location and trajectory[J]. *IEEE Data (base) Engineering Bulletin-DEBU*, 2010, 33(2): 32-39.

[44] LI Q H, CAO G H. Providing privacy-aware incentives for mobile sensing [C]//2013 IEEE International Conference on Pervasive Computing and Communications (PerCom). New York: IEEE, 2013: 76-84.
[45] HUANG K L, KANHERE S S, HU W. A privacy-preserving reputation system for participatory sensing [C]//37th Annual IEEE Conference on Local Computer Networks. New York: IEEE, 2014: 10-18.
[46] AZHAR S, CHANG S, LIU Y, et al. Utility-aware participant selection with budget constraints for mobile crowd sensing [C]//15th EAI International Conference. Cham: Springer, 2020: 38-49.

PRPS：用于移动群智感知的隐私保护和信誉感知的参与者选择方案

AZHAR Shanila*，刘国华
东华大学 计算机科学与技术学院，上海 201620

摘　要：作为一种新兴的感知范式，移动群智感知（mobile crowd sensing，MCS）包括一组移动用户，这些用户利用他们的传感设备有效地执行和发送数据贡献。然而，隐私和信誉机制（可靠性评估）的集成是构建安全可靠的 MCS 应用程序的关键。首先，即使参与者提供敏感的个人数据，也能确保他们的隐私得到保护。其次，由于有偏见或不准确的贡献可能会降低系统质量，信誉机制允许服务器监控参与者的行为和可靠性，服务器必须对参与者进行验证。将信誉机制与隐私相结合具有挑战性和矛盾性。信誉机制衡量参与者在整个感知活动期间的行为，而隐私旨在保护参与者的身份。因此，提出了一种针对 MCS 的新型隐私保护和信誉感知的参与者选择（privacy-preserving and reputation-aware participant selection，PRPS）方案。PRPS 方案将隐私与信誉机制相结合，使用假名和隐身技术来分别保护参与者身份和信誉值隐私，并保护位置和数据隐私。通过仿真模拟和性能评估，分别比较了 PRPS 方案、隐私保护和效用感知的参与者选择（privacy-preserving and utility-aware participant selection，PUPS）方案及效用感知的参与者选择（utility-aware participant selection，UPS）方案，证明了 PRPS 方案的精度、有效性和可扩展性，并证明了隐私和信誉机制对数据贡献的影响。再次，评估了 PRPS 方案的结果。最后，估计了 PRPS 方案在评估参与者可靠性和行为方面的效率和准确性。

关键词：移动群智感知（MCS）；信誉；隐私；假名；隐身