Research Article

A Privacy-Preserving Incentive Mechanism for Participatory Sensing Systems

Xiaoguang Niu ^{1,2}, Jiawei Wang ¹, Qiongzan Ye ¹, and Yihao Zhang ¹

¹*School of Computer Science, Wuhan University, Wuhan, China*

²*Collaborative Innovation Center of Geospatial Technology, Wuhan, China*

Correspondence should be addressed to Xiaoguang Niu; xgnu@whu.edu.cn

Received 6 September 2017; Accepted 4 December 2017; Published 16 January 2018

Academic Editor: Krzysztof Szczypiorski

Copyright © 2018 Xiaoguang Niu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The proliferation of mobile devices has facilitated the prevalence of participatory sensing applications in which participants collect and share information in their environments. The design of a participatory sensing application confronts two challenges: “privacy” and “incentive” which are two conflicting objectives and deserve deeper attention. Inspired by physical currency circulation system, this paper introduces the notion of E-cent, an exchangeable unit bearer currency. Participants can use the E-cent to take part in tasks anonymously. By employing E-cent, we propose an E-cent-based privacy-preserving incentive mechanism, called EPPI. As a dynamic balance regulatory mechanism, EPPI can not only protect the privacy of participant, but also adjust the whole system to the ideal situation, under which the rated tasks can be finished at minimal cost. To the best of our knowledge, EPPI is the first attempt to build an incentive mechanism while maintaining the desired privacy in participatory sensing systems. Extensive simulation and analysis results show that EPPI can achieve high anonymity level and remarkable incentive effects.

1. Introduction

Mobile computing devices, such as smartphones, wearable devices, and tablet PCs, have become popular in our daily life. These devices have contributed to the advent of numerous participatory sensing systems (PSS) [1]. In a PSS, an application server stimulates a large number of participants to sense and transmit measurements of the variables of interest (e.g., images, videos, sounds, locations, trajectories) via the sensors in their devices to a data collection entity in charge of task monitoring or addressing a particular problem. Although deploying such application has enormous social and technical benefits, several participants’ privacy and participation concerns arise [2, 3].

The design of a participatory sensing application confronts two challenges: “privacy” and “incentive.” On one hand, if multiple sensing reports are associated with a participant identity, the participant’s privacy information may leak, since the report is stamped with time and location [4]. Thus, the requirement of privacy in PSS is unlinkable between identities and sensing data. On the other hand, the

number of participation times in PSS is the key to provide adequate level of service quality. Most of the mobile crowd sensing-based applications rely on voluntary participation. To complete a task with a mobile device, participants have to consume their own resources such as battery, storage, and network traffic. A user may not be interested in the task, unless he receives a satisfactory reward to compensate for his resource consumption and potential privacy breach. Therefore, incentive mechanisms have been proposed to attract adequate participants [5–7].

Nevertheless, if the server provides full anonymity to participants for privacy-preserving consideration, it could be difficult to guarantee the trustworthiness of participants’ submitted data. PSS is vulnerable to false data submission. As the smartphone sensors are controlled by the contributors, it is easy for malicious adversaries to configure the devices to send false sensing data. Meanwhile, to reduce false data submission, reputation systems [8] have been widely used to encourage valid participation and punish misbehavior, where a participant’s behavior and identity are bound to a reputation account. However, as most of them require linking

participants' identities with their reports in order to provide rewards for participants, the server can easily infer the participants' privacy just by analyzing the correlation between participants' personal information (identity, reputation) and the sensing data in each report. Therefore, a privacy-preserving incentive mechanism is hard to design because "privacy" and "incentive" are two conflicting objectives.

Inspired by physical currency circulation system, this paper firstly proposes a novel notion of E-cent which is an exchangeable and untraceable unit bearer currency. Participants in PSS can take part in tasks without leaking any individual's privacy due to E-cent's exchange. By using E-cent, we propose EPPI, an E-cent-based incentive mechanism to motivate users to participate in tasks. In EPPI, a bidding model is proposed to simulate and predict the bidding behavior of participants based on the expectancy theory of motivation in psychology defined by Vroom [9]. Then user selection strategy of the server is proposed to minimize tasks cost and assign tasks to selected users more averagely. It can be proved that EPPI can provide full anonymity to participants and dynamically adjust the budget to regulate the performance of task. To the best of our knowledge, our work is the first attempt to build an incentive mechanism while maintaining the desired privacy in PSS.

To summarize, the contributions include the following.

- (i) The notion of E-cent is proposed as a unit bearer currency for the PSS system. E-cent is exchangeable and untraceable. Participants can participate in tasks anonymously by using E-cent's.
- (ii) An E-cent-based privacy-preserving incentive mechanism called EPPI is designed with user bidding model based on the expectancy theory of motivation in psychology.
- (iii) A user selection strategy is proposed to finish tasks at minimal cost and with balanced task assignment. EPPI can not only maintain the anonymity but also motivate users to participate in tasks.
- (iv) Extensive simulations and analysis are conducted to demonstrate that EPPI can provide full anonymity to participants and achieve incentive objectives.

The remainder of this paper is organized as follows. In Section 2, we discuss related work. Section 3 describes E-cent system. Section 4 presents our proposed EPPI mechanism in detail. The performance of EPPI is evaluated in Section 5. Finally, we make a conclusion in Section 6.

2. Related Works

Many pieces of works have specially studied the incentive mechanism in participatory sensing [10–13]. Most of existing incentive mechanisms mainly focus on utility maximization and cost minimization of the server. In [14], Singer and Mittal proposed a pricing mechanism, which enables automating the process of pricing and allocating tasks for requesters in complex markets. In [15], Duan et al. considered different incentive mechanisms to motivate the collaboration of smart-phone users on data acquisition and distributed computing.

However, these incentive mechanisms only focus on the reward for good participants without taking the punishment for false data submission into account. In addition, different market-based incentive mechanisms are proposed [16–18]. In such incentive mechanisms, the users bidding model and game theory in economics are widely used. Lee and Baik [19] designed a dynamic pricing incentive for participatory sensing, where participants bid for the sensed data and the server selects users as participants to minimize and stabilize the incentive cost while maintaining adequate level of participants by preventing users from dropping out. But they do not take the balance of task assignment into consideration. One participant may win most of the tasks with lower price. In fact, tasks should be assigned to users as uniformly as possible, such that more users can participate in tasks. More importantly, none of these mechanisms can meet the high requirements of privacy and anonymity in participatory sensing, because in such incentive mechanisms the server needs to know user ID so as to give rewards to users, which will reveal the participants' privacy. The mechanism in preliminary work [20] intends to incent people to move to the location as system needs. However, it cannot apply to most situations for the incentives are often too few for users. Most participatory users move according to the intended purpose, rather than depending on the incentive situation to determine the direction of the next movement [5, 7].

Plenty of researches on privacy in PSS have been proposed. The majority of them focus on spatial and temporal cloaking techniques [21–23]. For instance, as the most popular technique [23], K-anonymity blurs a participant's private information in a cloaked area or a cloaked time interval so that the sensitive information is indistinguishable from other $k-1$ participants. Nevertheless, these spatial and temporal cloaking techniques are not suitable to dealing with privacy problem in incentive mechanism. Another well-known technique to protect the anonymity and privacy of the participants is to adopt pseudonyms rather than the true name in every operation [24]. Nonetheless, analysis of the reported data and reporting pattern may disclose the participants' important information such as residences [4].

To solve the conflict between privacy and incentive, anonymous reputation architectures have been proposed. For instance, reputation value is used to measure the participation and reliability level of participants in [25], while pseudonyms are utilized to provide anonymity for participants in [26]. However, all of them are vulnerable to identity-based attacks since participants cannot control an arbitrary number of pseudonyms and hence the service provider can recognize the participants' identity by analyzing their behaviors of data contribution and service accessing. Kinader and Pearson [8] proposed a privacy-enhanced peer-to-peer reputation system, but unfortunately it cannot be adapted to participatory sensing systems, as both participants and the server are not trustworthy in PSS. IncogniSense [27] extends the idea of pseudonyms-based reputation, which focuses on periodic pseudonyms and transfer of reputation between pseudonyms and a trusted third party is supposed to be available to transfer the reputation score of users between consecutive pseudonyms. However, it introduces additional

overhead for users to create pseudonyms; ARTSense [28] maintains the reputation anonymity properties and enforces reputation updates but does not consider the incentive requirement of the application server.

3. What is E-Cent?

There are many e-cash/e-coin solutions, why not use them directly? In this solution, E-cent is not dividable, and each one shall be a separate item such that the storage requirement is very high.

A PSS consists of participants and an application server (hereafter referred to as the “server”), where participants sample the objects with their smartphones and send the samples to the application server. The server analyzes and processes the samples and then provides services to participants with them. After that, the server will generate feedback (either reward or penalty) for participants based on their report quality. Moreover, participants can buy services from the server with the reward which can be circulated between participants and the server. The server is considered to be honest-but-curious. That is to say, the server will fulfill its functions, but may attempt to associate a sensing report with a particular participant to reveal his privacy. However, participants are not trustworthy for submitting true sensing data.

To achieve the goal of “participating and participation feedback without identity,” inspired by physical currency circulation system, we propose E-cent, a unit bearer digital currency which can circulate between the server and all participants. It is generated and authorized by the server with the public-key cryptographic primitives. On one hand, E-cent can be exchanged among participants such that the correlation between participant and E-cent is broken. If a participant submits an exchanged E-cent to the server, the server cannot identify the identity of the participant just based on the submitted E-cent. Hence, E-cent provides full anonymity for participants. On the other hand, the server can use E-cent as a reward to encourage participants to participate in tasks. To distinguish the authority of E-cent, we design two types of E-cent: (i) basic E-cent, which is designed for new participants. It cannot be used to purchase services, but can be used as pledge when sending reports; (ii) normal E-cent, which is designed to reward participants for contributing data. It can be used as pledge and to purchase services. Therefore, new participants are not able to enjoy the services on the server unless they participate in the sensing task.

There are four operations about E-cent, as illustrated in Figure 1. We now describe each of these operations in detail and the notations frequently used in this paper are listed in Notations.

(1) *E-Cent Generation*. When a new participant wants to participate in a task, he needs to send a request to the server to register. The server gives some basic E-cents (denoted as BC) to the new participant. For other cases, when a participant contributes sensing data to the server, the server will reward the participant with normal E-cents (denoted as C). The server will generate a nonrepetitive random number and sign it with the private key of server. The server saved a valid copy

of E-cent; when the E-cent is used, the server will tab it as “used.”

(2) *E-Cent Exchange*. The E-cent is required to be exchanged before use. Before exchanging, the participant P_i marks an E-cent with a secret number b_i , which is randomly selected and only known to the participant, and then encrypts it with the server’s public key. A marked E-cent of P_i (denoted as MC_i) is represented as

$$MC_i = \{C_i \mid b_i\}_{\text{spub}}. \quad (1)$$

Every time a participant marks an E-cent, he can choose a different secret number b . Therefore, b cannot be used by the server to link E-cents with the participant.

A special area called mix zone is open on the server to provide E-cent exchange service for all participants. Participants can log in mix zone with a pseudonym. Every time a participant logs in, he can choose a different pseudonym. The pseudonym list of online participants is open for all participants. A participant (via pseudonym PS_i) can randomly select a participant (via pseudonym PS_j) from the list for E-cent exchange. Note that this process does not go through the server and the server is blind to the selection of exchangers. Participant P_i sends his marked E-cent MC_i to another participant P_j , and then P_j sends his E-cent MC_j to P_i . To reduce the possibility of being identified by the server, every participant should exchange his E-cents with different participants at different time and exchange only one E-cent in any exchange process. After E-cent exchange, both participants need to renew the exchanged marked E-cent on server within a period T_{MaxR} to avoid the loss caused by malicious participants.

(3) *E-Cent Renewal*. For P_i , since MC_j is encrypted, it cannot be used directly. Thus, the participant P_i needs to submit it to the server for renewal. After receiving a marked E-cent, the server will check the following.

- (a) Whether the public-key encryption of the submitted marked E-cent MC_j is valid. If positive, the server extracts the original E-cent C_j and the secret number with its private key.
- (b) Whether the private-key signature of C_j is valid.
- (c) Whether C_j has not been used before.
- (d) Whether server has received dispute arbitration of C_j .

If MC_j pass all the above validations, the server will send a new E-cent C'_i to P_i . Accordingly, the original E-cent C_j will be invalidated. Otherwise, the server is notified of the invalidation of MC_j , and P_i will launch dispute arbitration to server to get the loss back.

(4) *Exchange Dispute Arbitration (EDA)*. In EDA, P_i is required to submit C_i and the secret number b_i to the server to prove the ownership of marked E-cent MC_i . After checking C_i and b_i , the server will compensate P_i with a new E-cent C'_i and invalidate MC_i and C'_j which has been allocated to P_i ’s exchanger P_j . Then the server will announce the information about this dispute arbitration to all participants.

FIGURE 1: Operations of E-cent.

4. EPPI: An E-Cent-Based Privacy-Preserving Incentive Mechanism

In this section, we propose an E-cent-based incentive mechanism called EPPI, which is a dynamic balance regulatory mechanism. It can not only protect the privacy of participants, but also adjust the total participatory sensing system to the ideal situation, under which the rated tasks will be finished with minimum cost. Definition of notations for the subregion and definition of notations for the j th user in the i th subregion are listed in the Notations.

4.1. System Architecture. In EPPI, the system first detects the sensing field and divides it into m regions of the same size, each of which corresponds to a task. Thus, the set of tasks can be represented as $\Gamma = \{\tau_1, \tau_2, \dots, \tau_m\}$. Total rewards of R are prepared for the m tasks. Each task $\tau_j \in \Gamma$ attracts at least n_j participants to ensure high trustworthiness of sensing data. The three purposes of the user incentive mechanism are (1) to finish the rated task; (2) to assign the task to the chosen users as fairly as possible to enable more users to participate in the task and prevent a few users from taking over all tasks with extremely low price; (3) to make the cost as low as possible. The importance of these three purposes decreases with order. When the three purposes of our system are achieved at the same time, we say that the ideal situation is reached. In fact, the ideal situation is a kind of Nash equilibrium in economics, which will be proved later. In game theory, the Nash equilibrium is a solution of a noncooperative

game involving two or more players [29]. In EPPI, the server interacts with participants through a three-stage process in each task cycle.

Stage 1. If a user wants to take a task, he/she needs to register for the task by submitting some E-cents (more than a pledge threshold) to the server as pledge. The number of pledges depends on the quality of sending reports. If the participant wants to submit a high-quality report to obtain more rewards, he/she thus needs to pledge more E-cents. At the beginning of each task cycle, the server sends the information including N_i , N'_i , A_i , reg_i , R_{ij} , X_i , and act_i of the previous cycle to all the users. Each user chooses to participate or not independently considering their own privacy level and participation cost and then submit his bidding price profile to the server including participating or not, bidding unit price, and number of participation times.

Stage 2. The server will wait for a certain time to collect users' quotes, and those users from whom the sever fails to collect the quotes within the stipulated time will be considered as unwilling participants. Based on the bidding situation analysis of historic cycle and the current cycle and the prediction of user behavior, the server will strategize to select participants to finish tasks and minimize the cost as well and then distribute the rated task to selected users. After that, each user will receive a feedback message from server to inform whether he/she can participate in this cycle and number of participation times if he/she can.

Stage 3. Selected users will collect sensing data and submit it to the server. These sensing data will be uniformly distributed in cycle. To guarantee the trustworthiness of received data, the server will check the legitimacy of data. After that, the server will pay the reward to user with E-cent or notify user of the illegality of data.

Users can set up their privacy level and default unit price. They can use earned virtual currency to purchase a service the server provided.

4.2. Bidding Model. The users who intend to participate in the task will send a bidding (including the unit price and the maximum times they would like to join in this cycle) to the server.

Psychologist Vroom [9] defines the motivation as a process governing choice among alternative forms of voluntary activities, a process controlled by the individual. Expectancy of motivation theory introduces that an individual will behave or act in a certain way which he has considered. It is the expectancy of result that motivates individuals to make their decision and control their behavior. The expectancy of motivation is

$$M = \beta \cdot V \cdot E \cdot T, \quad (2)$$

where β are the constant coefficient. M represents the power of stimulation, which means the strength of the internal potential to mobilize the enthusiasm of one person. V represent valence, a psychology concept, which means the actual value of the goal to oneself. One same goal may confer different valences to different people. In our mechanism, $V = R_{ij} \cdot E$ is the expected value, which means the possibility of achieving the goal according to experience, which is negatively related to the user's privacy. In our mechanism, $E = 1/R_{ij} \cdot T$ means the nonpersonal factors that can help individuals to achieve the goal. In our mechanism, T refers to the cost of the participants' mobile phone for participating in one task.

$$T = w_{rnt} \cdot x_{rnt} + w_{rp} \cdot x_{rp} + w_p \cdot x_p + w_{id} \cdot x_{id} + w_{ba} \cdot \frac{1}{x_{ba}} + w_o \cdot x_o, \quad (3)$$

where x_{rnt} , x_{rp} , x_p , x_{id} , x_{ba} , and x_o are defined in Notations and w_{rnt} , w_{rp} , w_p , w_{id} , w_{ba} , and w_o are the corresponding constant coefficients.

Correspondingly, the expectancy of motivation of i th user in i th subregion is

$$M_{ij} = \beta \cdot R_{ij} \cdot \frac{1}{P_{ij}} \cdot T. \quad (4)$$

If $M_{ij} \geq K_{ij}$ in a certain task cycle, the user will participate in the task in that cycle. Subsequently, the bidding price for that user is

$$p = C + \frac{K_{ij}}{M_{ij}} \cdot C, \quad (5)$$

where K_{ij} is the psychological threshold for users whether participating or not, M_{ij} is the expectancy of motivation for

the j th user in the i th subregion, and C is the j th user's cost for one task.

$$C = x_{ent} + x_{pc} + \gamma \cdot t/x_p, \quad (6)$$

where t is the expected completion time of the task and γ is the constant coefficient.

4.3. Participant Selection Strategy. The server's strategy is to choose users to complete the rated tasks while minimizing the cost under the given budget and pay reward to them when they finish task according to the users' bidding price. Specifically, the target area is divided into l subregions equally, and tasks are distributed to task cycles $\{t_1, t_2, \dots, t_n, t_{n+1}, \dots\}$. In each cycle of a subregion, N'_i is the number of rated tasks that need to be completed. The symbol σ_i reflects the proportion of unqualified data and should meet the condition $0 < \sigma_i < 1$. Each area possibly has certain number of bad data, so the actual number of rated tasks should have redundancy to keep the quality of task completion. For instance, the number of final rated tasks $N_i = N'_i \cdot (1 + \sigma_i)$. The allocation of budget for the total target region uses budget pool, which receives the surplus budget from some subregions and distributes them into other subregions averagely if they need. The budget of the i th subregions is R_i .

The server will calculate a unit price threshold R_{ij} by predicting users' behavior and a reasonable adjustment formula to choose the user who has a bidding price lower than the threshold. Hence, the total expense in the i th subregions R'_i is

$$R'_i = \sum_{k=1}^{\text{act}_i} p_k \cdot n'_k \leq \sum_{j=1}^{X_i} R_{ij}, \quad (7)$$

where act_i is the number of users in the activated users, p_k is the final unit price for one task, and n'_k is the number of tasks assigned to the chosen user. It is necessary for server to predict user's behavior to roughly estimate the number of participants. The prediction must refer to the statistic information of last several past cycles.

Because too many factors will influence user's decision, we now just make a reasonable simplified assumption that the relationship between unit price and number of participants obeys the normal distribution, which is $F(\hat{R}_{ij}) \sim N(\mu, 1)$. So, the probability density function is

$$f(x) = \frac{1}{\sqrt{2\pi}} e^{-(x-\mu)^2/2}. \quad (8)$$

And distribution function is

$$F(\hat{R}_{ij}) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\hat{R}_{ij}} e^{-(x-\mu)^2/2} dx. \quad (9)$$

The expectation of number of finished tasks in every cycle is

$$\bar{X}_i = \delta \cdot F(\hat{R}_{ij}), \quad (10)$$

where δ is the predefined constant. Now we hope the rated tasks all will be finished; that is,

$$\begin{aligned}\widehat{X}_i = N_i = \delta F(\widehat{R}_{ij}) &= \frac{\delta}{\sqrt{2\pi}} \int_{\infty}^{\widehat{R}_{ij}} e^{(x-\mu)^2/2} dx \\ &\approx \delta \cdot \Phi(\widehat{R}_{ij} - \mu).\end{aligned}\quad (11)$$

Hence, $\widehat{R}_{ij}$ can be worked out.

However, only relying on the prediction of unit price ($\widehat{R}_{ij}$) is inaccurate and not persuasive. Any changes such as the sudden cutdown on budget and the movement of people will make the situation disobey the normal distribution temporarily. Therefore, the formula of the unit price should be a reasonable and adjustable definition.

The price is determined by three factors: (1) the ratio of R_i and N_i is the average price in the subregion, which is called the basic price; (2) P_{ij} is the user's privacy level, while user can get more reward if he/she gives some extra privacy information like GPS location; (3) A_i is the adjustment coefficient which is influenced by statistic information of last cycle.

$$R_{ij} = w_0 \cdot \frac{R_i}{N_i} + w_1 \cdot P_{ij} + w_2 \cdot A_i \quad (12)$$

$$A_i = \alpha \cdot \frac{\text{reg}_i - \text{act}_i}{\text{reg}_i} \cdot \frac{R_i - R'_i}{N_i}, \quad (13)$$

where w_0, w_1, w_2 , and α are coefficients; $(\text{reg}_i - \text{act}_i)/\text{reg}_i$ is the proportion of inactivated users accounts to the total users. If the proportion is large, that indicates that the total motivation of users is very low, and A_i should make the price adjust fast to improve users' motivation in time. $(R_i - R'_i)/N_i$ is the deviation of budget and expense. R'_i is the final expense in the i th subregion:

$$R'_i = \sum_{k=1}^{\text{act}_i} p_k \cdot n'_k. \quad (14)$$

Because the privacy level of user obeys the standard normal distribution, $\sum_{j=1}^{X_i} w_1 \cdot P_{ij}$. In addition, the budget R_i should be adjusted in each cycle:

$$R_i(t_n) = \left[1 + \frac{N_i(t_{n-1}) - \sum_{j=1}^{\text{act}_i} n'_j}{N_i(t_{n-1})} \right] \cdot R_i(t_{n-1}). \quad (15)$$

The budget in subregion will be adjusted according to the completeness of tasks in last cycle. In fact, one method is to directly let $R_i(t_n) = \widehat{R}_{ij} \cdot N_i$, but this result heavily relies on the accuracy of hypothesis and has little robustness towards various deviation and data change.

Therefore, the budget will roundly adjust the unit price and the number of participants and finally reach the ideal condition.

To achieve the target, we should define and optimize the coefficient α .

The final unit price threshold $R_{ij}(t_n)$ is

$$\begin{aligned}R_{ij}(t_n) &= w'_0 \cdot \frac{R_i(t_n)}{N_i(t_n)} + w'_2 \cdot \alpha(t_n) \\ &\quad \cdot \frac{\text{reg}_i(t_{n-1}) - \text{act}_i(t_{n-1})}{\text{reg}_i(t_{n-1})} \\ &\quad \cdot \frac{R_i(t_{n-1}) - R'_i(t_{n-1})}{N_i(t_n)}.\end{aligned}\quad (16)$$

In formula (16), we temporarily ignore the privacy level because it can be added when the calculation is completed.

According to the prediction of users and formula (11), we can get the number of rated tasks at t_n th cycle:

$$N_i(t_n) \approx \delta \cdot \Phi(\widehat{R}_{ij}(t_n) - \mu). \quad (17)$$

Thus, the prediction of unit price threshold $\widehat{R}_{ij}(t_n)$ can be obtained. Furthermore, we deform formula (12) and substitute $\widehat{R}_{ij}(t_n)$ in it:

$$\begin{aligned}\alpha(t_n) &= \frac{1}{w'_2} \cdot \frac{\widehat{R}_{ij}(t_n) - w'_0 \cdot (R_i(t_n)/N_i(t_n))}{\text{reg}_i(t_{n-1}) - \text{act}_i(t_{n-1})} \\ &\quad \cdot \frac{\text{reg}_i(t_{n-1}) \cdot N_i(t_n)}{R_i(t_{n-1}) - R'_i(t_{n-1})},\end{aligned}\quad (18)$$

where α is also influenced by historic values. And the value has fewer influential effect on α as the time is longer. We define the width of sliding window as follows:

$$\alpha(t_n) = \frac{\sum_{k=1}^{\text{width}-1} \alpha'(t_{n-k}) \cdot e^{-k^2/2}}{\sum_{k=1}^{\text{width}-1} e^{-k^2/2}} \quad (19)$$

From formula (16) to formula (19) we can get the final unit price threshold $R_{ij}(t_n)$. Then we propose a user selection algorithm for the server to select participated users. In this algorithm, the server distributes tasks to each user who has relatively low bidding price which does not exceed unit price threshold in each round. It guarantees that the rated tasks will be finished with minimum cost. In addition, the server will distribute tasks round by round. And in each round one user can receive only one task even if it has a very low bidding price, which makes task distribution more average and fair. As a result, more people can join in the task rather than a few users with extremely low price.

The server will send feedback message $L'_{ij} = (Y/N, p, n')$ to all users. The feedback message notifies user of whether he/she could participate in the mission. If yes, n' tells them how many tasks he/she needs to finish.

Computation Complexity Analysis. The time and space complexity of the calculation of R_{ij} are $O(n)$ obviously. In Algorithm 1, n tasks will be allocated to users who have price lower than R_{ij} . The Merge sort over L_{ij} has the time complexity of $O(n \log_2 n)$ and the space complexity of $O(1)$. The execution in each loop examines whether the necessary

```

INPUT: set of user willingness  $L_i = \{L_{i1}, L_{i2}, L_{i3}, \dots, L_{iact_i}\}$ ,  $L_{ij} = (Y, p, n)$ ,  $N_i$ ,  $R_{ij}$ 
PARAMETERS: flag  $f$ 
OUTPUT: set of feedback information  $L'_i = \{L'_{i1}, L'_{i2}, L'_{i3}, \dots, L'_{iact_i}\}$ ,  $L'_{ij} = (Y, p, n')$ 
(1) sort the  $p$  of  $L_{ij}$  in ascending order
(2) initialization:  $c = 0$  for  $j = 1$  to  $act_i$ ,  $L'_{ij} = (N, p, 0)$ 
(3) while  $N_i > 0$  &&  $f == 1$ ;
(4)    $f = 0$ ; for  $j = 1$  to  $act_o$  do
(5)     if  $p \leq R_{ij}$  &&  $N_i > 0$ 
(6)       if  $n' < n$ 
(7)          $f = 1$ ,  $n' = n + 1$ ,  $L'_{ij1} = Y$ ,  $N_i = N_i - 1$ ;
(8)       end;
(9)     else break;
(10)   end;
(11) end;
(12) return  $L'_i$ ;

```

ALGORITHM 1: User selection.

condition is satisfied. If not, the loop will break. This means that every task distribution operation may only run once at most. So, the time complexity is $O(n \log_2 n)$. And the space complexity is $O(n)$.

4.4. Incentive Mechanism Analysis

Lemma 1. *The system can reach the ideal condition.*

- (1) All rated tasks are finished.
- (2) Tasks are distributed to participants as averagely as possible.
- (3) The expense is minimum and lower than the budget.

Proof. In our mechanism, we have macroadjustment and microadjustment to make the system reach the ideal condition. In formula (15), we can change the budget of subregion R_i gradually to adjust the unit price R_{ij} and number of participating users act_i , which is called macroadjustment.

If some rated tasks did not finish ($N_i > X_i$), more users are needed in the next cycle; according to $R_i(t_{n+1}) > R_i(t_n)$, the raise of budget increases the unit price R_{ij} , and users' motivation M_{ij} will increase, which will lead to the raise of the number of activated users, and finally make X_i add to reach N_i . On the contrary, the proof is similar.

Microadjustment is the automatic balance mechanism inside a subregion in order to find the balance number of finished tasks X_i under the current budget R_i .

If the number of finished tasks is decreasing, ($X_i(t_{n-1}) > X_i(t_n)$), $A_i(t_{n+1}) > A_i(t_n)$, $R_{ij}(t_{n+1}) > R_{ij}(t_n)$, the raise of unit price will increase the users' motivation M_{ij} and lead to the raise of X_i and finally make X_i reach the balanced value under the current budget. On the contrary, the proof is similar.

In conclusion, for (1) when the microadjustment and macroadjustment price threshold R_{ij} , expense R'_i , and number of finished tasks X_i approach the balance value, the rated tasks are ensured to be all finished, because macroadjustment guarantees that the budget is enough to finish the rated tasks while microadjustment makes sure that the actual number of

finished tasks reaches the balance value under this budget. For (2) and (3), due to the user selection algorithm, it is certain that tasks will be distributed to activated users averagely and the actual expense is the minimum in every cycle, because the algorithm chooses users in their price from the lowest one in loop, and in each loop a user can only have one task at most. So far, we achieved the three targets which have been mentioned in the beginning of this chapter. $\square$

Lemma 2. *The ideal condition is the Nash equilibrium.*

Proof. Under the ideal condition, for the subregion i , $X_i = N_i$, $A_i = 0$, $R_{ij} = w_0 * R_i / N_i + w_1 * P_{ij}$, the rated tasks are all to be finished and the expense reaches minimum and is lower than budget. When each subregion reaches the ideal condition, the whole region reaches the ideal condition. When the ideal condition is reached, the Nash equilibrium is reached.

Under the ideal condition, any change of any side will not bring more benefit.

(1) *To Any User.* Increasing price will lower the chance to be chosen. Yet decreasing price will lead to fewer rewards. If p increases, $p > R_{ij}$, which means the user cannot participate in any mission in this cycle. The benefit will become zero. If p reduce to p' , the user can take part in the task but gets less profit than before, because $p' < p$.

(2) *To the Server.* If unit price R_{ij} increases, budget R_i and users' participating motivation M_{ij} will increase correspondingly. After all rated tasks having been finished, the rise of R_{ij} only leads to unnecessary expense. On the contrary, the abatement of R_{ij} will decrease M_{ij} , which may make the rated tasks uncompleted. $\square$

5. Performance Evaluation and Security Analysis

In this paper, we consider a participatory sensing system with a similar scenario as [5]. The system consists of *Max-user* mobile participants and an application server. As shown in

FIGURE 2: Simulation scene.

Figure 2, we assume that simulation scene is Information Department of Wuhan University whose length is 612 m from west to east, and 856 m from north to south. The field is divided into l regions. Correspondingly, the whole system is comprised of X periodic tasks, each of which corresponds to a region. Total rewards of R E-cents of budget are given out to all participants in each cycle. In the initial phase, participants are unequally distributed in the sensing field. We used the Pathway Mobility Model [30] with geographic restriction as mobility model of each participant. The speeds of participants are randomly distributed from 1 m/s to 5 m/s. The maximum residence time for each site is 30 seconds. Each participant's task set includes all tasks within the range of 30 meters. In each participant's trajectory, the tasks will be sensed in every 5 meters. If any task is within 30 m from the participant, it will be added to his task set. The budget is distributed uniformly to each subregion at the beginning. The attack probability of a malicious participant is defined as the probability of the malicious participant sending a false report. The privacy and incentive performance of EPPI are evaluated firstly. Then we analyze the security of the mechanism itself. The data is set to match the real-world cases approximately. In fact the preset values have little impact on the tendency of balance. We make a survey of 13 students in our lab to get the weight coefficient. As for the constant coefficient, we do several tests and choose an appropriate group. The default values of parameters in EPPI mechanism experiment environment are listed in Table 1.

5.1. Evaluation Metrics

- (i) Anonymity level is the probability that the server traces a participant.
- (ii) Incentive effect is the impact of different price threshold and privacy level on participants' bidding price, the change of a particular user's bidding price, the adjustment of price threshold, number of finished tasks and expense, the comparison of two methods to predict users' behavior, and the motivation of a user in different cases.

TABLE 1: Default parameter settings.

Parameter	Value
Number of participants Max_user	1000
Number of subregions l	9
Number of rated tasks X_i	9
The budget for whole target region R	2000
The weight coefficient for users $w_{rnt}, \dots, w_{of}$	0.2, 0.3, 0.1, 0.3, 0.1, 0
The weight coefficient for price threshold w'_1, w'_2, w'_3	0.4, 0.3, 0.3
Constant parameters t, x_{ent}, x_{pc}	20, 0.01, 0.001
Constant coefficients $\beta, \gamma, \delta, \mu, \sigma$	100, 0.1, 10, 7, 0.05

5.2. Privacy Evaluation. Tracing attack takes place when the server distinguishes a participant from other participants by associating submitted reports with the participant. In this attack, the server needs to link a certain ratio of reports with a participant. If the server succeeds in tracing a participant, the server will be able to analyze and profile the participant's location trace or at least reduce the anonymity level of the participant. We evaluate the anonymity level of a participant in terms of its resilience against tracing attacks by calculating tracing probability. Though the selection of exchanger is anonymous and random, the server can link an E-cent to a participant by randomly matching the exchange pair. Its difficulty depends on the number of online participants in the mix zone. When a participant wants to send a report, he/she needs to randomly select y_i E-cents from y E-cents of her/his own and submit them to the server as pledge. As long as one of the y_i E-cents is linked to him/her, the server can link the report to the participant. Therefore, the probability that a report is linked with a participant can be calculated as follows:

$$P(\text{a report is linked with a participant } y_i) = \sum_{j=1}^{C_y^{y_i}} \sum_{C \in \Theta} \frac{1}{C_y^{y_i}} \frac{1}{n_C}, \quad (20)$$

where Θ represents the selected E-cent set and n_C represents the number of online participants at the moment the E-cent C is exchanged.

Figure 3(a) shows the probability of the server identifying a participant through tracing attack under varying required pledge of one report when the ratio of traced reports is set to 0.2. We can observe that as the pledge increases, the participant is more likely to be traced. This is because if a participant submits more E-cents to the server as pledge, the server will have more alternative information to trace the participant. However, we notice that even though the pledge is set to the highest value, the tracing probability still maintains a very low value (less than 0.23). As the number of task cycles increases, more participants participate due to the incentive mechanism. That is why the tracing probability keeps decreasing as the number of cycles increases. Figure 3(b) shows the impact of traced report ratio on tracing probability when pledge is set to 20. Even though the ratio is set to 0.1, the

FIGURE 3: Resilience against tracing attack.

tracing probability is less than 0.2. When the ratio is set to 0.3, the tracing probability approaches 0, which means that it is almost impossible for the server to trace a participant.

5.3. Incentive Evaluation. Figure 4 shows the influence of different price threshold and subregions on users. The parameters for users are initialized in the range randomly obeying the normal distribution. The users' sensitivity of privacy leakage levels P_{ij} is initialized in $[1, 5]$, and level 5 represents the highest sensitivity of privacy leakage level. User's psychological thresholds K_{ij} are generated in range $[0, 50]$. The remaining flow of user's mobile x_1 and the remaining power of user's mobile x_2 are represented in percentage. The performance of user's mobile x_3 and user's idle degree x_4 are restricted in $(0, 0.5)$, while the balances in users' accounts x_5 are represented by the number in $[0, 10]$.

Figure 4(a) shows how users respond to different price threshold of last cycle which the server sends them. Three different budgets are chosen to evaluate the distribution of participants in various price thresholds. As the expected price adds, the number of participants increases. At the meanwhile, the number of users with lower price also increases. This is due to the expected increase in profits that will stimulate the users' motivation to participate, which increases the number of participants and decreases price according to our theory.

Figure 4(b) exhibits the impact of different users with various sensitivity of privacy leakage levels on their price bidding. Data of the experiment reflect the strong relationship between user sensitivity of privacy leakage level and their bidding price as we expected in definition. Privacy level 1 is the lowest level and level 5 is the highest. In all participants, privacy level 1 is the majority and no users with level 5 take part

in the project. According to the definition of user motivation, the sensitivity of privacy leakage level indicates user's possibility of finishing task. The lower the sensitivity of privacy leakage level is, the more accurate the data the user will send is, and the chance to join the mission successfully is larger.

Figure 4(c) shows the bidding price of a particular user who would like to participate. The case starts with budget $R_i = 200$. Because the motivation of user has the positive correlation with R_{ij} , the change of R_{ij} will lead to change in user's motivation; furthermore, the bidding price will be influenced by motivation. In other words, the change of user's motivation will finally reflect on the change of his/her bidding price and number of tasks he/she wants to participant in.

Figure 5 shows the change of unit price threshold and the result of user selection in a given subregion. Three cases are designed to test the performance of MPI mechanism. These cases start with different budgets: surplus budget $R_i = 50$, excessive budget $R_i = 400$, and approximate appropriate budget $R_i = 200$. In Figure 5(a) the unit price threshold of server will be adjusted by A_i and R_j , which leads to the fluctuation of number of price thresholds R_{ij} . And as expected, the unit price threshold will finally converge to the balanced value no matter what the initial condition is. The balanced value of R_{ij} reflects the average cost of one task for users. Figure 5(b) is the result of user selection. Results of selection of three cycles (1st, 6th, and 9th) which start with surplus budget $R_i = 50$ are exhibited. In each cycle, we calculate the budget to see the impact of budget on a number of participants.

We evaluate our reward allocation scheme by comparing its incentive result with three representative allocation schemes [31]: grey prediction (GP), proportional allocation (PA), and random allocation (RA). Figure 6 shows the total

FIGURE 4: The influence factor of bidding price.

number of received sensing reports using four schemes in different task cycles. In this figure, EPPI received more reports at all cycles, which means it achieves the best incentive effect among all allocation schemes. Compared with other schemes, EPPI considers the historical distribution of participants and models the problem specifically with logistic function. According to Figure 6, the number of reports increases gradually over time until a steady status is reached. As the expectation of Algorithm 1, in each cycle, participants with bidding price lower than the threshold were chosen in increasing order by price averagely, which makes sure that the total expense will be minimum. In addition, the average distribution of task achieves the second target of EPPI.

Figure 7 shows the result of two methods to predict users' behavior which have been mentioned in Section 4.3. Two situations are designed to compare the methods, both of which have the same condition starting with excessive

budget $R_i = 400$. In addition, in order to better evaluate the reaction of two methods to the external stimulation, the number of rated tasks doubled from 20 to 40 in the 4th cycle, and the number of registered users reduced by half in the 9th cycle. The data of normal distribution model is the result that only relies on the prediction of unit price calculated by normal distribution function. And the data of EPPI prediction model is the result using the optimized adjustment mechanism in EPPI. Obviously, normal distribution model is not accurate enough and the result is always a constant which cannot be adjusted to deal with different situation. Owing to the design of adjustment function against external changes, EPPI are much more robust than the normal distribution method. In conclusion, the optimization using formula (11) is necessary and reasonable.

Figures 8 and 9 exhibit the impact of budget and number of rated tasks on the final expense and number of finished

FIGURE 5: The adjustment of unit price and result of user selection.

FIGURE 6: Number of received sensing reports over time.

FIGURE 7: Prediction of users' behavior with two methods.

tasks. Figure 8(a) shows the adjustment of expense R_i in the three cases which start with different budget. Figure 8(b) shows the adjustment of expense R_i starting with different number of rated tasks. Obviously, the expense has the positive correlation with R_{ij} and X_i and will converge to the minimum balanced value as the cycle grows. According to the micro and macroadjustment, the price threshold will adjust and converge to a balance value to make the rated tasks all finished, no matter what the initial conditions are. Under this value the user selection algorithm will work out a plan which has the minimum expense.

Figure 9(a) exhibits the number of finished tasks adjustment for the different initial budget value. Figure 9(b) shows the impact of different number of rated tasks on the number

of finished tasks. The primary object of EPPI is to finish all the rated tasks. The results of these cases all finally reached target owing to the adjustment mechanism. The amount of finished tasks converges to a balance value. And these balance values of X_i are converged to equal to the number of rated tasks. These results of experiments indicate the user incentive mechanism in EPPI is feasible and effective.

Figure 10 shows the reward payment of six participants. For good participants (GP), the more they participate in tasks, the more the E-cents they will obtain. For malicious participants (MLP) with different attack probabilities, E-cents of malicious participants who have higher attack probabilities drop down more quickly. But their E-cents are not always decreasing, because malicious participants may send correct

FIGURE 8: Changes of expense over time.

reports to gain E-cent and then send false reports randomly, known as on-off attacks [24]. However, the E-cents of malicious participants still maintain a trend of decline and drop down to a very low level eventually. This is because the punishment has a larger influence on E-cents compared to reward.

5.4. Security Analysis

Theorem 3. *The server cannot associate a sensing report with a particular participant.*

Proof. No matter participants want to participate in a task or buy service from the server, they only need to submit E-cents and their participant IDs are never needed. Suppose that the server recorded the correlation between E-cents and participants when giving E-cents to participants. It implies that the server can associate a participant with its report by recognizing the pledge of the report. Nevertheless, since E-cent is bearer currency, a participant can exchange its E-cents with other participants in the mix zone before submitting them. Since the exchange of E-cent is random and anonymous, the original correlation between E-cents and participants will be broken. The server will not be able to recognize a participant with its submitted E-cents. $\square$

Theorem 4. *Multiple reports sent by the same participant are not linkable.*

Proof. Suppose that the server recorded the correlation between E-cents when giving E-cents to participants. It implies that the server knows which E-cents are sent to the same participant and thus can associate multiple reports with the same participant. But after a participant exchange its E-cents with others in the mix zone, the original correlation

between E-cents will be broken. Moreover, every time a participant exchanges E-cents in mix zone, he/she can choose a different exchanger for each E-cent. Though one of exchangers is collusion attacker, the attacker can only collude with the server to recognize the participant once but cannot associate multiple reports with the same participant.

Malicious participants may try to exploit the flaw of E-cent operations to obtain additional unfair profits. The following theorems prove that EPPI is resilient against such malicious behaviors. $\square$

Theorem 5. *A malicious participant P_i cannot get an additional unfair E-cent by exchanging its fake E-cent MC_i^* with another participant P_j .*

Proof. When P_j delivered MC_i^* to the server for E-cent renewal, P_j would be informed that MC_i^* is fake. Though P_j has sent MC_j to P_i during exchange, P_j still had the copy of MC_j and knew the secret number b_j in MC_j . Therefore, P_j could prove the ownership of MC_j by submitting C_j and b_j to the server, while P_i could not. The server would compensate P_j with an E-cent after checking b_j and C_j . The server also invalidated MC_j and new E-cent given to P_j . Finally, P_i did not get any unfair E-cent from the case. Meanwhile, P_j did not suffer any loss. $\square$

Theorem 6. *A greedy participant P_i cannot get an additional unfair E-cent from its exchanger P_j by launching the dispute arbitration operation for its own marked E-cent and the renewal operation of the received marked E-cent.*

Proof. When P_i launched dispute arbitration and proved the ownership of MC_i with C_i and b_i , the server would announce the information to all participants. When P_j knows MC_i is invalidated, P_j could also launch dispute arbitration to prove

(a) Impact of budget on number of finished tasks

(b) Adjustment to number of finished tasks

FIGURE 9: Adjustment of expense and number of finished tasks.

FIGURE 10: Reward payment based on participants' behavior.

the ownership of MC_j , which would invalidate P_i 's new E-cent C'_i during the renewal operation and generate a new E-cent C''_i for P_j . Finally, P_i did not get any unfair E-cent from the case. Meanwhile, P_j did not suffer any loss. $\square$

6. Conclusions

This paper firstly proposed a unit bearer exchangeable digital currency called E-cent and a corresponding incentive mechanism EPPI to achieve privacy preservation and incentive

enhancement simultaneously for participatory sensing systems. E-cent is exchangeable and can be utilized to participate in tasks anonymously by participants. EPPI is an E-cent-based user incentive mechanism, which uses theory in economics and psychology. It can dynamically adjust the budget to regulate the number of completed tasks to reach the amount of rated tasks. It can not only protect the privacy of participant, but also adjust the distribution of tasks to participants averagely as well as adjust the cost to minimum. Extensive simulation results and theoretical analysis have shown that EPPI is substantially resilient against different kinds of attacks and achieves both anonymity and incentive requirement simultaneously.

Notations

U, P_i :	Set of participants and the i th participant
spub, spriv:	Public key and private key of the server
b_i :	Secret number of participant i
MC_i :	A marked E-cent of participant P_i
Γ, τ_i :	Set of tasks and the i th task
R, R_i :	Reward and subtask reward
C_i :	An E-cent of participant P_i
$A \parallel B$:	Concatenation of message A and message B .

Definition of Notations for the Subregion

I :	The number of subregions
R :	The total budget of the target region
R_i :	The budget of the i th subregion
R'_i :	The final cost of the i th subregion
X_i :	The final number of finished task in i th subregion
σ_i :	The proportion of unqualified data in i th subregion

- N'_i : The rated number of task in i th subregion
 N_i : The actual rated number of task in i th subregion
 A_i : The adjustment coefficient of unit price in i th subregion
 R_{ij} : The unit price of j th user in i th subregion
 act_i : The number of activated users in i th subregion
 reg_i : The number of registered users in i th subregion.

Definition of Notations for the j th User in the i th Subregion

- P_{ij} : The privacy level of j th user in i th subregion
 x_{rnt} : The remaining network traffic of user's mobile phone
 x_{ent} : The expense of network traffic for one task
 x_{rp} : The remaining power of user's mobile phone
 x_{pc} : The power consumption for one task
 x_p : The performance of user's mobile phone
 x_{id} : The idle degree of user
 x_{ba} : The balance in user's account
 x_o : Other facts that may influence user's decision
 K_{ij} : The psychological threshold of user to decide whether participate or not
 m : The motivation of user to participate in one task
 t : The time cost for one task.

Additional Points

We consider the incentive mechanism in preliminary work not feasible enough for the constraint for this mechanism is too rigorous. That mechanism intends to incent people to move to the location as system needs. However, it cannot be applied to most situations because the incentives offered to users in that mechanism are far from stimulating users' movement. So a completely new privacy-preserving incentive mechanism for participatory sensing systems was designed (in Section 4). The new mechanism adjusts incent value in each subregion in order to complete rated tasks rather than count on movement of users. Also the corresponding experiments are conducted to verify the design (in Section 5). The improvement is made on other parts of the paper to ensure the rationality and validity of our work. The new content in this paper accounts for over 60%.

Disclosure

This preliminary version of this paper appeared in the 33rd IEEE International Performance, Computing, and Communication Conference-IPCCC [20].

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This work was partially supported by the National Key Research Development Program of China (2016YFB0502201), the National Natural Science Foundation of China NSFC (U1636101, U1736211), and CERNET Next Generation Internet's Technology Innovation Project (NGII20150612, NGII20160324).

References

- [1] J. A. Burke, D. Estrin, M. Hansen et al., "Participatory Sensing," in *Proc. of ACM workshop WSW at SenSys*, pp. 117–134, Boulder, Colorado, USA, 2006.
- [2] D. Christin, A. Reinhardt, S. S. Kanhere, and M. Hollick, "A survey on privacy in mobile participatory sensing applications," *The Journal of Systems and Software*, vol. 84, no. 11, pp. 1928–1946, 2011.
- [3] R. K. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: current state and future challenges," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 32–39, 2011.
- [4] I. Boutsis and V. Kalogeraki, "Privacy preservation for participatory sensing data," in *Proceedings of the 11th IEEE International Conference on Pervasive Computing and Communications (PerCom '13)*, pp. 103–113, IEEE, March 2013.
- [5] D. Yang, G. Xue, X. Fang, and J. Tang, "Incentive Mechanisms for Crowdsensing: Crowdsourcing with Smartphones," *IEEE/ACM Transactions on Networking*, vol. 24, no. 3, pp. 1732–1744, 2016.
- [6] C. C. Cao, Y. Tong, L. Chen, and H. V. Jagadish, "Wisemarket: a new paradigm for managing wisdom of online social users," in *Proceedings of the 19th ACM SIGKDD international conference*, p. 455, Chicago, Illinois, USA, August 2013.
- [7] L. G. Jaimes, I. Vergara-Laurens, and M. A. Labrador, "A location-based incentive mechanism for participatory sensing systems with budget constraints," in *Proceedings of the 10th IEEE International Conference on Pervasive Computing and Communications, PerCom 2012*, pp. 103–108, Switzerland, March 2012.
- [8] M. Kinader and S. Pearson, "A Privacy-Enhanced Peer-to-Peer Reputation System," in *E-Commerce and Web Technologies*, vol. 2738 of *Lecture Notes in Computer Science*, pp. 206–215, Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.
- [9] V. H. Vroom, *Work and motivation*, John Wiley sons. Inc, New York, 1964.
- [10] M. Riahi, T. G. Papaioannou, I. Trummer, and K. Aberer, "Utility-driven data acquisition in participatory sensing," in *Proceedings of the 16th International Conference on Extending Database Technology, EDBT 2013*, pp. 251–262, Italy, March 2013.
- [11] Y. Han and Y. Zhu, "Profit-maximizing stochastic control for mobile crowd sensing platforms," in *Proceedings of the 11th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2014*, pp. 145–153, USA, October 2014.
- [12] M. Musthag, A. Raj, D. Ganesan, S. Kumar, and S. Shiffman, "Exploring micro-incentive strategies for participant compensation in high-burden studies," in *Proceedings of the 13th International Conference on Ubiquitous Computing, UbiComp'11 and the Co-located Workshops*, pp. 435–444, China, September 2011.
- [13] A. Singla and A. Krause, "Truthful incentives in crowdsourcing tasks using regret minimization mechanisms," in *Proceedings of the 22nd International Conference on World Wide Web, WWW 2013*, pp. 1167–1177, bra, May 2013.

- [14] Y. Singer and M. Mittal, "Pricing mechanisms for crowdsourcing markets," in *Proceedings of the 22nd International Conference on World Wide Web, WWW 2013*, pp. 1157–1166, Rio de Janeiro, Brazil, May 2013.
- [15] L. Duan, T. Kubo, K. Sugiyama, J. Huang, T. Hasegawa, and J. Walrand, "Incentive mechanisms for smartphone collaboration in data acquisition and distributed computing," in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM '12)*, pp. 1701–1709, Orlando, Fla, USA, March 2012.
- [16] J.-S. Lee and B. Hoh, "Sell your experiences: A market mechanism based incentive for participatory sensing," in *Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications, PerCom 2010*, pp. 60–68, April 2010.
- [17] I. Koutsopoulos, "Optimal incentive-driven design of participatory sensing systems," in *Proceedings of the 32nd IEEE Conference on Computer Communications, IEEE INFOCOM 2013*, pp. 1402–1410, Italy, April 2013.
- [18] X. Zhang, Z. Yang, Z. Zhou, H. Cai, L. Chen, and X. Li, "Free market of crowdsourcing: Incentive mechanism design for mobile sensing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 12, pp. 3190–3200, 2014.
- [19] J.-S. Lee and H. Baik, "Dynamic pricing incentive for participatory sensing," *Pervasive and Mobile Computing*, vol. 6, no. 6, pp. 693–708, 2010.
- [20] X. Niu, M. Li, Q. Chen, Q. Cao, and H. Wang, "EPPI: An E-cent-based privacy-preserving incentive mechanism for participatory sensing systems," in *Proceedings of the 33rd IEEE International Performance Computing and Communications Conference, IPCCC 2014*, USA, December 2014.
- [21] A. Machanavajjhala, D. Kifer, and J. Gehrke, "L-diversity: privacy beyond k -anonymity," *ACM Transactions on Knowledge Discovery from Data (TKDD)*, vol. 1, no. 1, article 3, 2007.
- [22] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," *IEEE Transactions on Knowledge and Data Engineering*, vol. 19, no. 12, pp. 1719–1733, 2007.
- [23] B. Gedik and L. Liu, "Protecting location privacy with personalized k -anonymity: architecture and algorithms," *IEEE Transactions on Mobile Computing*, vol. 7, no. 1, pp. 1–18, 2008.
- [24] K. L. Huang, S. S. Kanhere, and W. Hu, "Preserving privacy in participatory sensing systems," *Computer Communications*, vol. 33, no. 11, pp. 1266–1280, 2010.
- [25] E. Androulaki, S. Choi et al., Reputation systems for anonymous networks, *Privacy Enhancing Technologies*, pp. 202–218, 2008.
- [26] Q. Li and G. Cao, "Providing privacy-aware incentives for mobile sensing," in *Proceedings of the 11th IEEE International Conference on Pervasive Computing and Communications, PerCom 2013*, pp. 76–84, USA, March 2013.
- [27] D. Christin, C. Roßkopf, M. Hollick, L. A. Martucci, and S. S. Kanhere, "IncogniSense: An anonymity-preserving reputation framework for participatory sensing applications," *Pervasive and Mobile Computing*, vol. 9, no. 3, pp. 353–371, 2013.
- [28] X. Wang, W. Cheng, P. Mohapatra, and T. Abdelzaher, "ART-Sense: Anonymous reputation and trust in participatory sensing," in *Proceedings of the 32nd IEEE Conference on Computer Communications, IEEE INFOCOM 2013*, pp. 2517–2525, Italy, April 2013.
- [29] M. J. Osborne and A. Rubinstein, *A Course in Game Theory*, MIT Press, Cambridge, Mass, USA, 1994.
- [30] F. Bai and A. Helmy, "A survey of mobility models wireless ad hoc networks," in *Wireless Ad Hoc Networks*, vol. 206, University of Southern California, USA, 2004.
- [31] F. Wu, C. J. Liu, and Y. T. Wang, "A Grey Prediction for Optimization Technique in Mobile Computing," *Applied Mathematics & Information Sciences*, vol. 6, no. 2, pp. 521–529, 2012.