IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 12, 2018, accepted August 13, 2018, date of publication September 10, 2018, date of current version October 17, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2869202

Incentive Mechanism Design for Crowdsourcing-Based Indoor Localization

WEI LI[1], CHENG ZHANG[1], (Member, IEEE), ZHI LIU[2,3], (Member, IEEE), AND YOSHIAKI TANAKA[3,4], (Life Senior Member, IEEE)

[1]Department of Computer Science and Communications Engineering, Waseda University, Tokyo 169-8555, Japan
[2]Department of Mathematical and Systems Engineering, Shizuoka University, Shizuoka 432-8561, Japan
[3]Global Information and Telecommunication Institute, Waseda University, Tokyo 169-8555, Japan
[4]Department of Communications and Computer Engineering, Waseda University, Tokyo 169-8555, Japan

Corresponding author: Zhi Liu (liu@shizuoka.ac.jp)

The work of W. Li was supported by the China Scholarship Council (CSC) under Grant 201706690030.

ABSTRACT Wi-Fi-based indoor localization system needs to construct a radio map by site surveys. The process of site surveys is time-consuming and crowdsourcing is one feasible option to tackle this issue. Meanwhile, privacy protection has drawn concerns from both industry and academia. In this paper, we propose two incentive mechanisms to stimulate mobile users (MUs) to contribute indoor trajectory data for crowdsourcing-based indoor localization with differential privacy to prevent MUs' privacy leakage. The first mechanism considers fixed reward for MUs and incomplete information, where each MU's sensitivity level of the data privacy is unknown to the crowdsourcing platform (CP). The interaction between MUs and CP is formulated into a two-stage Stackelberg game to maximize MUs' utility and CP's profit. The second mechanism jointly considers the variable reward for MUs and assumes CP knows each MUs' sensitivity level of the data privacy. A demand function is used to model the relationship among CP, MUs, and service customer. The optimization problem of maximizing CP's profit is studied to show the impact of the price fluctuation. Comprehensive simulations are presented to evaluate the performance of the proposed mechanisms and show some insights of the crowdsourced indoor localization incentive mechanism with privacy protection.

INDEX TERMS Crowdsourcing, indoor localization, incentive mechanism, game theory, privacy protection.

I. INTRODUCTION

Localization can help people easily access to information like navigation and product promotion in various indoor environments such as shopping malls, airport terminals, and railway stations, and has drawn great attentions from both industry and academia. Yassin *et al.* surveyed various indoor positioning techniques and discussed different indoor localization-based applications with the challenges in terms of cost, security and accuracy [1]. In particular, most existing approaches adopt *Received Signal Strength indicator (RSSI) fingerprinting* for location determination [2]–[4], where the RSSI fingerprinting records the RSSIs of the access points at each known location. Without requiring installation of additional positioning infrastructures in indoor environments, RSSI fingerprinting based indoor localization can be easily implemented and hence is widely used.

However, it is time-consuming to conduct a site survey in order to build the fingerprinting database for the indoor scenario. To reduce the effort of a manual calibration for the site survey, especially in a multi-floor building, various kinds of crowdsourcing-based indoor localization methodologies have been successfully applied [5], [6]. These approaches leverage the data collected by mobile devices' embedded sensors to obtain users' trajectory or indoor traces. Then these collected data is merged into the database of the RSSI fingerprinting for position inquires. These crowdsourcing-based indoor localization methodologies successfully collect sufficient RSSI data and provide good performances comparing with other ways to reduce the fingerprint construction cost such as constructing fingerprinting using amplitude feature deep convolutional generative adversarial network and a small amount of collected data [7].

To address these challenges, the recent active researches focus on the crowdsourced data collected by mobile devices to construct a floor plan and achieve indoor positioning. For example, the indoor movement records or activities contributed by a large amount of mobile users (MUs) were utilized to specifically depict the interior layout of a building and

construct a fingerprint database [8]. Zhou *et al.* [9] mapped MUs' crowdsourcing activities collected by smartphones sensors into an indoor map by using a pose graph optimization algorithm.

The success of these aforementioned crowdsourcing-based indoor localization systems heavily depends on MUs' sensing data, i.e. without adequate MUs' participations, it is impossible to obtain a good performance. The inherent problem then becomes how to motivate MUs to participate and the studies for incentive mechanism design attract great attentions [10], [11].

When MUs participate to help contribute the trajectory or indoor traces, plenty of valuable sensing data may include individuals' sensitive information (e.g. identity, location information, activity trace and so on), and this may cause unexpected privacy leakage [12]. For example, by integrating users' sensed indoor movement records, it is possible to infer which restaurants or shops a specific MU visits and thus some improper advertisements or promotion information may be marketed to this user. Hence, many researchers concentrate on the issue of the individual's privacy protection and attempt to adopt anonymization techniques to conceal sensitive information so that personal privacy can be protected. For instance, differential privacy is one state-of-the-art approach that can be utilized to prevent the leakage of users' indoor locations during the process of data integration [13].

The privacy issue also affects the incentive mechanism design. As far as the authors understand, however, existing incentive mechanisms with privacy considerations mainly focus on economical objectives such as utility maximization and truthfulness. These schemes lack good performance and do not consider the features of indoor localization.

This paper would like to address the aforementioned issues and help attract more users' participation in the prevention of MUs' privacy leakage. With fixed/variable reward offered to MUs and incomplete/complete information of MU's sensitivity level of the data privacy (we use *user type* to denote this in this paper), two incentive mechanisms for crowdsourcing-based indoor localization are proposed. Specifically, when each MU's precise user type is unknown to the crowdsourcing platform (CP) and with fixed total rewards paid to the MUs, the designed incentive mechanism defines the trajectory utility with privacy protection, and formulates the interaction between MUs and CP as a two-stage Stackelberg game [14] with the aim to maximize CP's profit and MUs' utility. When the CP knows each MU's user type, CP uses variable reward to further attract MUs' participation, the designed incentive mechanism uses a demand function to model the interaction between CP and service customers (SCs). The optimization problem of CP's profit is studied to show the impact of the price fluctuation. Extensive simulations are conducted to evaluate the performance of the proposed incentive mechanisms and show some design insights of the crowdsourced indoor localization incentive mechanism with privacy protection. To the best of our knowledge, this is the very first time to design incentive mechanisms to collect MUs' sensed trajectory for indoor localization with privacy preservation.

The rest of this paper is organized as follows. The related schemes are summarized in Section II. Section III describes and analyzes the incentive mechanism with fixed reward and incomplete user type information. In Section IV, we represent the incentive mechanism based on variable reward and complete information of user' sensitivity of data privacy. Simulations are conducted to evaluate the performance and the results are shown in Section V. Finally, Section VI makes a conclusion of this article.

II. RELATED WORK

Wi-Fi fingerprinting-based indoor localization methods have become prevalent in recent years since they do not need to deploy extra infrastructure. However, these existing solutions are hindered by the requirements of manual efforts to collect RSSI data from known locations to create a radio map. Thanks to the rapid development of hardware, state-of-the-art mobile devices have good communicating and sensing abilities. Equipped with various built-in sensors, mobile devices play an important role in connecting humans and environment, which can be used to collect RSSI data and the inertial data such as the acceleration, turning.

On the other hand, crowdsourcing as a new paradigm is firstly used in economic area, where a complicate task is completed through recruiting a large amount of workers. Then, inspired by this, many crowdsourcing applications have been developed to achieve a wide variety of services, and the results critically depend on MUs' participation [15], [16]. For example, since lane-based road network information plays a critical role in the intelligent transportation, based on crowdsourcing data collected by various vehicles, Tang *et al.* [17] presented a method called as ''CLRIC'' to extract detailed lane structure of roads, which can be used to assist reliable and safe driving.

Motivated by these observations, lots of researchers make use of crowdsourced data measured by mobile devices to create the radio map, and then determine the location. For example, a crowdsourcing-based indoor location system denoted as ''Zee'' [18] utilized the mobile phones carried by users in normal course to enable crowdsourcing of location-annotated Wi-Fi measurements in indoor environment. Wu *et al.* [19] investigated novel sensors integrated in smartphones and leveraged users' motion to construct the radio map for a known floor plan.

However, these mentioned methods mainly depend on users' voluntary participation and in general, users are unwilling to participate, as participating in a task will experience extra operational costs such as the comsumption of battery power, computing power, communication cost and so on. Hence, how to design a suitable incentive mechanism to motivate mobile users (MUs) can help improve the crowdsourcing accuracy [20], promote its applications and draw much efforts to study this topic. For instance, Yang *et al.* [21]

proposed the crowdsourcer-centric model based on game theory, and the user-centric model based on reverse auction to motivate smartphone users to participate in the crowdsensing task. Xu and Low [22] presented the Vickrey-Clarke-Groves mechanism for wholesale electricity markets and its result demonstrated that the proposed mechanism can achieve a good performance under higher electricity prices. To continuously motivate users, a crowdsourcing tournament was designed to achieve winner ranking [23].

Many of existing proposed incentive mechanisms for crowdsourcing-based applications are aware of users' locations, which can incur the leakage of users' personal privacy. To protect users' privacy, various methods have been proposed including k-anonymity [24], l-diversity [25] and differential privacy [26]. While using k-anonymity, it is difficult to determine the identity of individuals during the collection of data set that contains personal information, and l-diversity is suitable for background knowledge attacks. Without the knowledge of an adversary, differential privacy protection schemes can be used to prevent from being recognized from the collected differentially-private data.

The incentive mechanism should also be studied jointly with the privacy protection investigation. One typical work is introduced by Wang *et al.* [27], who proposed an auction-based incentive mechanism with location privacy-preserving to stimulate workers to participate in the tasks and behavior truthfully. However, this scheme is more general and the features of indoor localization are not captured.

For convenience, Table 1 lists frequently used notations in this paper.

TABLE 1. Notations.

Symbol	Description
Π, Π_i	The set of MUs and set of MUs except MU i
N	Number of MUs
ϵ	Privacy budget
Θ	The set of MUs' unit cost for privacy loss
μ_j	Number of MUs with unit cost $\theta_j \in \Theta$
d	The trajectory length
π_1, π_2, π_3	Parameters of trajectory utility function
R	Tixed reward
U_i^{MU}	MU i's utility
τ_i	MU i's unit cost for privacy loss
U^{CP}	CP's profit
χ	CP's preference on MUs' data
p	The buying price for MUs' trajectory
Q	Service demand
q	The service price for SCs
β	Slope of demand function
Ω	The set of MUs with positive utility
ω	Number of set Ω
δ	CP's preference on MUs' data

III. INCENTIVE MECHANISM WITH FIXED AWARD AND INCOMPLETE USER PRIVACY INFORMATION

When users carry out usual indoor activities in the indoor environment, trajectory sensed by users' mobile devices can be collected. Trajectory is a MU's record that includes walking steps, sampled RSS readings and barometer data when a MU walks from a starting spot to an ending spot within a considered time slot T. Then, the tuple including *walking steps*, *RSSI sequence*, *barometer reading* and *time slot indicator* forms the MU's trajectory vector. Based on the magnitude of the accelerator records, the normalized auto-correlation based step counting method utilized in [18] is adopted to calculate walking step S. Meanwhile, the altitude changes of barometer recorded by mobile devices can be used to recognize floor transition among different floors in a building. These data can be incorporated to construct the corresponding radio map. Then, indoor location-based services (LBS) such as indoor tracking and navigation are provided to customers.

To attract more MUs to contribute indoor trajectory in order to increase the localization accuracy, in this section, a fixed reward based incentive mechanism with privacy preservation is proposed. This system has N MUs, denoted as a set $\Pi = \{1, 2, \ldots, N\}$, and one CP as shown in Fig. 1.

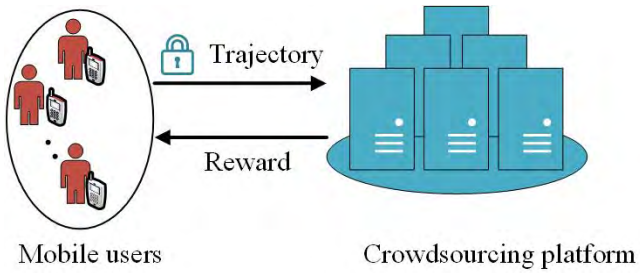

FIGURE 1. The system illustration for the incentive mechanism with fixed award and incomplete user privacy information.

To attract MUs' involvement, CP firstly announces a task that collects users' indoor trajectory under a time slot T and broadcasts a fixed reward R to MUs. Then, MUs will decide whether or not to participate in the task. From the perspective of CP, through integrating the trajectory data contributed by MUs to build a radio map, CP can benefit from offering location-based service for customers.

If MU i decides to take participation in the task, it can receive a reward based on the length d_i of its trajectory data (the unit of d_i is meter), where d_i is the product of MU i's walking steps S and step stride. However, due to the differences in height and walking style, people usually have different stride lengths. In practice, Rai *et al.* [18] found that MUs generally exhibit up to $\pm 10\%$ variations for their stride length within a single walk. Hence, to account for this variation, we could use a distributed random variable which is added to the stride length to capture the estimation error. Meanwhile, to prevent MUs from receiving more reward by faking their trajectory through the way called as "U-Turn" where a user just turns around a fixed point [28], we harness

the heading value measured by digital compass equipped with mobile phones and adopt the peak detection algorithm studied in [29] to differentiate normal turn and U-Turn. Thus, the extra length incurred by "U-Turn" can be effectively eliminated, which is of great importance for MUs' accurate trajectory length.

Then, ϵ-differentially privacy [26] is utilized to prevent the leakage of MUs' privacy, and the following definitions are given to illustrate ϵ-differentially privacy algorithm.

Definition 1 (γ_i-Adjacency): Two continuous trajectory data Tra_i and Tra_i' are γ_i-adjacency, if $|Tra_i - Tra_i'| \leq \gamma_i$, where γ_i is the range of MUs' trajectory data Tra_i.

Definition 2 (ϵ_i-Differential Privacy): A random algorithm $\{\boldsymbol{r} : R \rightarrow R|\boldsymbol{r}(Tra_i) = Tra_i + \eta_i\}$ achieves ϵ_i-differential privacy, if for all pairs of γ_i-adjacency data Tra_i and Tra_i', and all possible outputs $\boldsymbol{r}$ satisfies (1):

$$\log \frac{Pr(\boldsymbol{r}|Tra_i)}{Pr(\boldsymbol{r}|Tra_i')} \leq \epsilon_i \tag{1}$$

where $\epsilon_i \in [0, 1]$ is called privacy budget and η_i is the calibrated noise. According to the characteristic of differential privacy, it is notable that a lower value of ϵ means stronger privacy guarantee and a larger perturbation noise.

When adopting ϵ_i-differential privacy, both Tra_i and Tra_i' can result in outputs $\boldsymbol{r}$ with certain probability. Hence, it is difficult for an attacker to distinguish MU i's raw sensing trajectory data with high confidence when observing $\boldsymbol{r}$. Moreover, although some encrypted approaches have been adopted, the encrypted sensing trajectory data still may reveal MUs' sensitive information, or ultimately disclose MUs' identity via de-anonymization attacks, which can incur MUs' privacy loss. Xu *et al.* [30] has demonstrated that MUs have different privacy preferences. This paper uses the ϵ-differential privacy.

If each MU's privacy preference (the sensitivity of the data privacy) is unknown to CP, it results in the incomplete information case, which means there exists information asymmetry between MUs and CP. With the fixed reward, MU i's unit cost for privacy loss is denoted by $\tau_i \in \Theta$, where $\Theta = \{\theta_1, \theta_2, ..., \theta_k\}$ is the set of MUs' unit cost with ϵ-differential privacy. Based on the knowledge of differential privacy by (1), we can use the factor ϵ to characterize the relationship between the expected utility of two neighboring trajectory vectors. Similar to [31], we define the unit cost for privacy loss as the difference between the raw trajectory vector's utility and the encrypted or perturbed trajectory vector's utility. This also can reflect how MUs care about their privacy. Moreover, the knowledge of Θ can be learnt from historical data. In this scheme, to address the issue of information asymmetry, we make the following assumption that the probability distribution of each type for MUs is known to CP, i.e., μ_j MUs belong to type θ_j. Therefore, MUs' total number can be denoted as $N = \sum_{\theta_j \in \Theta} \mu_j$.

According to Definition 1, if the value of ϵ is smaller, more noises are added to MUs' raw sensing data and trajectory utility decreases. Similar to [32], we propose an utility function $g(d_i, \epsilon_i)$ as follows to describe the relationship between trajectory utility and ϵ. It meets the following two requirements: 1) $g(.)$ is proportional to ϵ so that $\frac{\partial g(.)}{\partial \epsilon} > 0$ can be guaranteed; 2) $g(.)$ is proportional to the length d of MUs' trajectory.

$$g(d_i, \epsilon_i) = [\pi_1 - \pi_2 e^{\pi_3(1-\epsilon_i)}]d_i \tag{2}$$

where $\pi_1 > 1$ and $\pi_3 \in (0, \ln \frac{\pi_1}{\pi_2}]$ keep $g(.)$ positive. Here, we define $\pi_2 = \pi_1 - 1$ to denote that when there is no privacy preservation measure is taken *i,e.*, $\epsilon = 1$, there should be no utility loss for MUs. To better show the validity of (2) in capturing the trajectory utility, here a simulation is conducted by setting $\pi_1 = 1.2, \pi_3 = 0.55$, and the result is shown in Fig. 2.

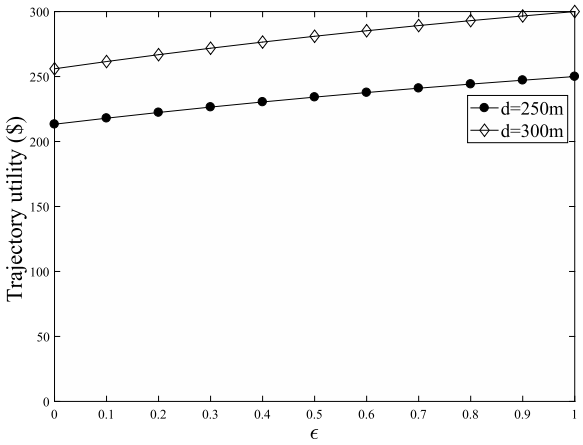

FIGURE 2. Impact of ϵ on trajectory utility.

From the results shown in Fig. 2, we can observe that trajectory utility decreases when the value of ϵ increases, and an increase in the length d can result in an increase in trajectory utility.

Then, MU i's utility function can be denoted as follows.
(1) MU i's utility function:

$$U_i^{\text{MU}} = \frac{g(d_i, \epsilon_i)}{\sum_{j \in \Pi} g(d_j, \epsilon_j)} R - \epsilon_i \tau_i d_i \tag{3}$$

where R is the fixed reward determined by CP, and $\tau_i \in \Theta$ represents MUs' unit cost for privacy loss.

MUs' contributed data benefits the CP and based on the previous work in [21], CP's profit function can be written by as follows:
(2) CP's profit function:

$$U^{\text{CP}} = \chi \log(1 + \sum_{\theta_j \in \Theta} \mu_j \log(1 + d_j)) - R \tag{4}$$

where χ is a system parameter which denotes CP's preference on MUs' contributed data. Here, the inner *log* function is utilized to reflect CP's diminishing return on the length; and the outer *log* function is used to reflect CP's diminishing return on the number of MUs participating in the crowdsourcing.

In this incentive mechanism, we formulate the relationship between MUs and CP as a Stackelberg game to maximize

MUs' utility and CP's profit, where CP is the leader and MUs are the followers. In this game, two-stages are included: Stage I, the fixed reward R is announced by CP; Stage II, MUs can achieve their own maximal utility by adjusting its strategy d. Hence, both CP and MUs are players whereby the strategy of CP is its reward.

As mentioned before, to deal with the information asymmetry, we make an assumption that the crowdsourcing platform has known the knowledge of the probability distribution of MUs' types in terms of the sensitivity of data privacy. We analyze the formulated Stackelberg game through backward introduction, and compute MU i's Nash Equilibrium (NE) strategy.

CP can achieve its maximal profit by using (4). The derivatives of U_i^{MU} with respect to d_i are computed in Stage II and we have:

$$\frac{\partial U_i^{\mathrm{MU}}}{\partial d_i} = -\frac{(\pi_1-\pi_2 e^{\pi_3\epsilon_i})(\pi_1-\pi_2 e^{\pi_3\epsilon_i})d_i R}{\left(\sum_{j\in\Pi}(\pi_1-\pi_2 e^{\pi_3\epsilon_j})d_j\right)^2} - \epsilon_i\tau_i + \frac{(\pi_1-\pi_2 e^{\pi_3\epsilon_i})R}{\sum_{j\in\Pi}(\pi_1-\pi_2 e^{\pi_3\epsilon_i})d_j} \tag{5}$$

$$\frac{\partial^2 U_i^{\mathrm{MU}}}{\partial d_i^2} = -\frac{\sum_{j\in\Pi_{-i}}(\pi_1-\pi_2 e^{\pi_3\epsilon_j})^2 d_j R}{\left(\sum_{j\in\Pi}(\pi_1-\pi_2 e^{\pi_3\epsilon_j})d_j\right)^3} \times 2(\pi_1-\pi_2 e^{\pi_3\epsilon_i}) < 0 \tag{6}$$

where Π_{-i} denotes MUs' set excluding MU i. According to (6), MUs' utility function is strictly concave in length d_i.

Hence, when given reward $R > 0$, MU i can achieve its unique best response strategy, only if it has existed. When setting the first derivative of U_i^{MU} to 0, we can solve for d_i can be calculated as follows:

$$d_i = \frac{1}{(\pi_1-\pi_2 e^{\pi_3\epsilon_i})}\sqrt{\frac{R\sum_{j\in\Pi_{-i}} d_j}{\tau_i}} - \sum_{j\in\Pi_{-i}} d_j \tag{7}$$

According to MUs' different types, we can sort MUs' unit privacy loss cost τ_i by ascending order to ensure $\tau_i \le \tau_2 \le \ldots \le \tau_N$. Meanwhile, by summing up (5) over MUs, we can get:

$$\sum_{j\in\Pi}(\pi_1-\pi_2 e^{\pi_3\epsilon_j})d_j = \frac{(N-1)R}{\sum_{j\in\Pi}\tau_j} \tag{8}$$

Then, we substitute (8) into (5):

$$d_i^{\mathrm{NE}} = \frac{(N-1)R}{\sum_{j\in\Pi}\tau_j(\pi_1-\pi_2 e^{\pi_3\epsilon_j})}\left(1-\frac{(N-1)\tau_i}{\sum_{j\in\Pi}\tau_j}\right) \tag{9}$$

In Stage I, by integrating d_i^{NE} into (4), we have

$$U^{\mathrm{CP}} = \chi\log\left(1+\sum_{\theta_j\in\Theta}\mu_j\log(1+\Psi_j R)\right) - R \tag{10}$$

where

$$\Psi_j = \frac{(N-1)}{\sum_{j\in\Pi}\tau_j(\pi_1-\pi_2 e^{\pi_3\epsilon_j})}\left(1-\frac{(N-1)\tau_i}{\sum_{j\in\Pi}\tau_j}\right) \tag{11}$$

The second-order of U^{CP} about R can be computed as follows:

$$\frac{\partial^2 U^{\mathrm{CP}}}{\partial R^2} = -\chi\frac{\sum_{\theta_j\in\Theta}\mu_j\frac{\Psi_i^2}{(1+\Psi_i^2 R)^2}}{1+\sum_{\theta_j\in\Theta}\mu_j\log(1+\Psi_j R)} - \chi\frac{\left(\sum_{\theta_j\in\Theta}\mu_j\frac{\Psi_i^2}{1+\Psi_i^2 R}\right)^2}{\left(1+\sum_{\theta_j\in\Theta}\mu_j\log(1+\Psi_j R)\right)^2} < 0 \tag{12}$$

Thus, (12) demonstrates that CP's profit function is strictly concave with respect to R. We adopt Newton's method [33] to obtain the optimal reward R^*. The first-order of U^{CP} with respect to R is computed:

$$\frac{\partial U^{\mathrm{CP}}}{\partial R} = \chi\frac{\sum_{\theta_j\in\Theta}\mu_j\frac{\Psi_j}{1+\Psi_j R}}{1+\sum_{\theta_j\in\Theta}\mu_j\log(1+\Psi_j R)} - 1 \tag{13}$$

For convenience, we set $G(R) = U^{\mathrm{CP}}(R)$ and the steps are denoted as follows:

Algorithm 1 Algorithm: Newton's Method

given start point R_0, and tolerance $\eta > 0$.
repeat
1. *Compute the Newton step and decrement.*
$\triangle R_{kt} = -\nabla^2 G(R)^{-1}$; $\varepsilon^2 := \nabla G(R)^T \nabla^2 G(R)^{-1}\nabla G(R)$
where $\nabla G(R) = \frac{\partial G(R)}{\partial R}$ and $\nabla^2 G(R) = \frac{\partial^2 G(R)}{\partial R^2}$
2. *Stopping criterion.* **quit** if $\varepsilon^2 \le \eta$.
3. *Line search.* Choose step size t by backtracking line search.
4. *Update.* $R := R + t\triangle R_{kt}$

IV. INCENTIVE MECHANISM WITH VARIABLE AWARD AND COMPLETE USER PRIVACY SENSITIVITY INFORMATION

Section III formulates the interaction between MUs and CP as a noncooperative game, where each MU competes for the fixed reward. When selling service to service customers (SCs), the price to purchase sensing data from MUs will be affected by the service price decision. In this section, to study the price influence, an incentive mechanism with variable award and complete user privacy sensitivity information is proposed and the framework is shown in Fig. 3.

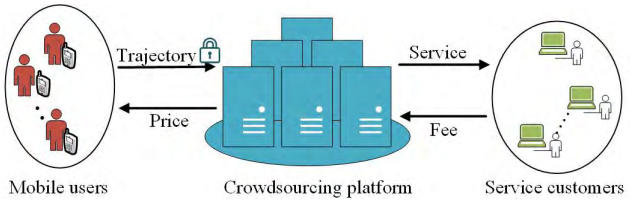

FIGURE 3. Framework illustration of the incentive mechanism with variable award and complete user privacy sensitivity information.

Given there are different options of ϵ, CP provides a price menu for MUs to make the best choice. Here, the complete

information scenario is taken into account, where each MU's precise type in terms of the sensitivity to the data privacy is known to CP. Similar to [30], we make an assumption that CP is trusted.

We assume that MU's unit cost θ for privacy loss is uniformly distributed over the interval $[\underline{\theta}, \overline{\theta}]$ where $\underline{\theta}$ and $\overline{\theta}$ are the lower bound and upper bound of MUs' unit cost θ incurred by privacy loss, respectively. Similarly, we only consider MUs' unit cost incurred by privacy loss and other type of costs like sensing cost can be incorporated in this paper with some modifications. The utility of MU i is given by the reward from CP minus the cost incurred by privacy loss:

$$U_i^{\mathrm{MU}} = p - \epsilon\theta_i \tag{14}$$

where p is the price for purchasing trajectory data from MUs and it is a variable determined by CP. θ_i represents MU i's unit cost for the loss of privacy.

As to the SCs, increasing the service selling price q decreases SCs' willingness to use the service. On the other hand, increasing p attracts more MUs to contribute the trajectory data, this results in higher service quality and more SCs are willing to buy service. To reflect this, we utilize the linear demand function [34] to formulate this relationship as follows:

$$Q = Q_0 + V(p) - \beta q \tag{15}$$

where $Q > 0$ denotes quantity of service subscribed by SCs and Q_0 is the basic service demand. The mid term $V(p)$ represents *positive externality* and denotes the impact of buying price p. This *positive externality* satisfies the following requirements that the first-order derivative of $V(p)$ with respect to p is nonnegative and the the second-order derivative of $V(p)$ with respect to p is zero. $\beta > 0$ is the slope of the demand curve, which shows the impact of price q on the demand. Then, CP's profit can be denoted as follows:

$$U^{\mathrm{CP}} = Qq\delta \log(1 + \sum_{i\in\Omega} \log(1 + d_i)) - \sum_{i\in\Omega} p \tag{16}$$

where Ω denotes the set of MUs whose utility is nonnegative and its number is denoted as ω. δ is CP's preference on MUs' trajectory data. The inner function *log* reflects the CP's diminishing return on MUs' trajectory data, and the outer *log* function reflects CP's diminishing return on participating MUs.

CP's profit maximization problem can be derived by using following equation:

$$\begin{aligned} \max_{p,q} \ & (U^{\mathrm{CP}}) \\ & p > 0 \\ & q > 0 \\ & \epsilon \in [0, 1] \end{aligned} \tag{17}$$

Given the buying price p, according to (14), the number of MUs ω who sell data to CP can be calculated as follows:

$$\omega(p) = \sum_{i=1}^{N} 1_{p-\epsilon\theta_i>0} \tag{18}$$

where N is the number of potential MUs, and $1_{p-\epsilon\theta_i>0}$ is the indicator function that returns 1 if MU i's utility is greater than 0.

In this scheme, a basic model $V(p) = \alpha p$ is used to denote the *positive externality*, where α is nonnegative. By merging (15) and (18) into CP's profit function (16), we have:

$$U^{\mathrm{CP}} = [Q_0 + \alpha p - \beta q]q\delta \log(1 + \sum_{i=1}^{\omega(p)} \log(1 + d_i)) - \omega(p)p \tag{19}$$

The derivatives of U^{CP} with respect to q can be computed:

$$\frac{\partial U^{\mathrm{CP}}}{\partial q} = [Q_0 + \alpha p - 2\beta q]\delta \log(1 + \sum_{i=1}^{\omega(p)} \log(1 + d_i)) \tag{20}$$

$$\frac{\partial^2 U^{\mathrm{CP}}}{\partial q^2} = -2\beta\delta \log(1 + \sum_{i=1}^{\omega(p)} \log(1 + d_i)) < 0 \tag{21}$$

Since the second-order derivative of U^{CP} with respect to q is negative, U^{CP} is strictly concave in q. Moreover, in the next section, the numerical method is adopted to verify the concavity of U^{CP} in p and q.

We also study a special case to illustrate the concavity of CP's profit in p and q. In this case, we assume MUs' unit cost θ follows a uniform distribution, then $\omega(p) = \frac{NP}{\epsilon(\overline{\theta}-\underline{\theta})}$ when $\frac{P}{\epsilon(\overline{\theta}-\underline{\theta})} < \overline{\theta}$, and its derivatives with respect to p satisfy that $\omega'(p) = k_1 > 0$ where $k_1 = \frac{N}{\epsilon(\overline{\theta}-\underline{\theta})}$ and $\omega''(p) = 0$. MUs are willing to contribute the trajectory when the price p increases, and this results in longer trajectory length. Here, we use the following equation to derive the relationship between the buying price p and the trajectory length:

$$d_i = d_0(e^{\eta_i p} - 1) \tag{22}$$

where d_0 is the basis trajectory length that can be obtained from MUs' historical data and $\eta_i \in (0, 1)$ denotes MUs' heterogenous preferences of the buying price p on trajectory where $\sum_{i\in\Omega} \eta_i = 1$.

For ease of exposition, we set $G(p, d_i) = \log(1 + \sum_{i=1}^{\omega(p)} \log(1 + d_i))$. Because of $1 + d_i \gg 1$, we can have $G(p, d_i) = \log(1 + \sum_{i=1}^{\omega(p)} \log d_i)$. Combining with (22), we can know that $G(p, d_i) = \log[1 + \sum_{i=1}^{\omega(p)} \log(d_0 e^{\eta_i p} - d_0)]$. Then, by approximating $\sum_{i=1}^{\omega(p)} \log(d_0 e^{\eta_i p} - d_0)$ to $\sum_{i=1}^{\omega(p)} (\log d_0 + \log e^{\eta_i p})$, the derivatives of $G(p, d_i)$ with respect to p can be computed as follows:

$$\frac{\partial G(p, d_i)}{\partial p} = \frac{k_2}{1 + k_2 p} \tag{23}$$

where $k_2 = 1 + k_1 \log(d_0)$

$$\frac{\partial G^2(p, d_i)}{\partial p^2} = \frac{-k_2^2}{(1 + k_2 p)^2} \tag{24}$$

The derivatives of U^{CP} with respect to p can be calculated:

$$\frac{\partial U^{\mathrm{CP}}}{\partial p} = \alpha q \delta \log(1 + k_2 p) + [Q_0 + \alpha p - \beta q] q \delta \frac{k_2}{1 + k_2 p} - 2k_1 p \tag{25}$$

$$\frac{\partial^2 U^{\mathrm{CP}}}{\partial p^2} = 2\alpha q \delta \frac{k_2}{1 + k_2 p} + [Q_0 + \alpha p - \beta q] q \delta \frac{-k_2^2}{(1 + k_2 p)^2} - 2k_1 \tag{26}$$

From (26), we can note that when given the price $p > 0$, the second-derivative of $U^{\mathrm{CP}} < 0$, and U^{CP} is concave in p. When setting $\frac{\partial U^{\mathrm{CP}}}{\partial q} = 0$ and $\frac{\partial U^{\mathrm{CP}}}{\partial p} = 0$, we can obtain the solution (p^*, q^*).

V. SIMULATIONS

Comprehensive simulations are presented to evaluate the performance of our proposed mechanisms and to show some insights of the crowdsourced indoor localization incentive mechanism with privacy protection. The simulation setup and results are introduced in this section.

A. INCENTIVE MECHANISM WITH FIXED AWARD AND INCOMPLETE USER PRIVACY INFORMATION

We vary MUs' number N from 100 to 1000 with the increment of 100, and set the value range of unit cost τ to $\in [1, 10](\$ \cdot m^{-1})$. Here, the symbol \$ denotes Unite States dollar. Meanwhile, the value of CP's preference χ on MUs' contributed data is set to 10\$. For convenience, the simulation settings are listed in Table 2.

TABLE 2. Simulation settings.

Symbol	Description	Value
N	MUs' number	100∼1000
ϵ	Privacy budget	[0 1]
τ	MUs' privacy unit cost	[1 10]\$
χ	CP's preference on MUs' data	$10\$ \cdot m^{-1}$

The platform-centric mechanism studied in [21] models the interaction between users and the platform as a game, where a fixed reward is adopted. But it ignores the impact of privacy. Here, this mechanism is served as a benchmark. To verify the performance of our proposed fixed reward based mechanism, comparison simulations are conducted, where we fixed $\tau_{max} = 10\$$ and the results are shown as follows:

Fig. 4 shows the impact of MUs' number on CP's profit and we can observe that the platform's profit obviously demonstrates diminishing marginal returns as the number of MUs increases. Meanwhile, when keeping MUs' number constant, CP's profit of our proposed scheme is higher than that of the platform-centric mechanism. The simulation result shows the superiority over the platform-centric mechanism. The impact

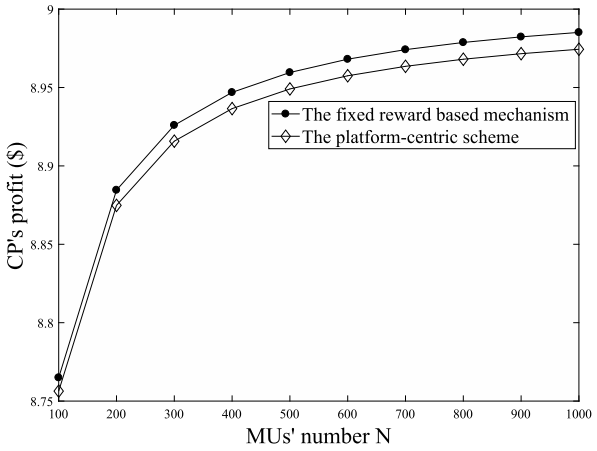

FIGURE 4. Impact of N on CP's profit.

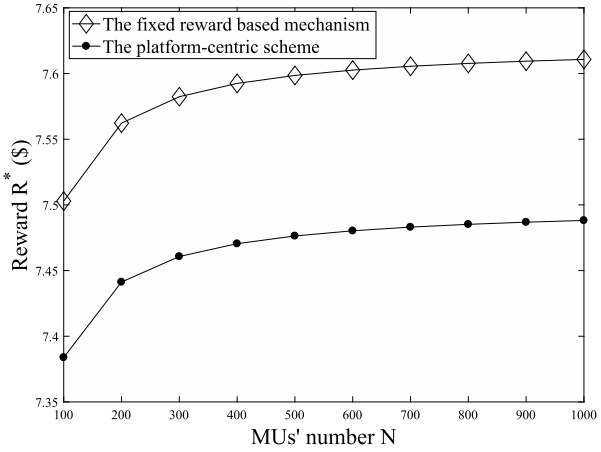

FIGURE 5. Impact of N on R^*.

of MUs' number on the optimal reward R^* is shown in Fig. 5. Compared with the platform-centric mechanism without privacy protection, it is notable that our proposed mechanism with privacy protection can achieve a better performance due to the designed mechanism and consideration of the privacy protection.

In order to show the impact of MUs' unit cost for privacy loss on CP's profit, MUs' number N is fixed at 1000. Based on the analytics presented in Section III, we know that different value of MUs' unit cost τ actually presents MUs' different types. From Fig. 6, we can see that CP's profit decreases when the range of unit cost τ for MUs' privacy loss becomes larger, which also denotes that MUs' types become more diverse.

Fig. 7 shows the impact of MUs' unit cost τ on the optimal reward R^*. We can observe that as the value of MUs unit cost τ increases, the optimal reward R^* decreases severely. We can also observe that the optimal reward's value in our proposed mechanism has a lower decreasing rate.

B. INCENTIVE MECHANISM WITH VARIABLE AWARD AND COMPLETE USER PRIVACY SENSITIVITY INFORMATION

We also conduct simulation for the incentive mechanism with variable award and complete user privacy sensitivity

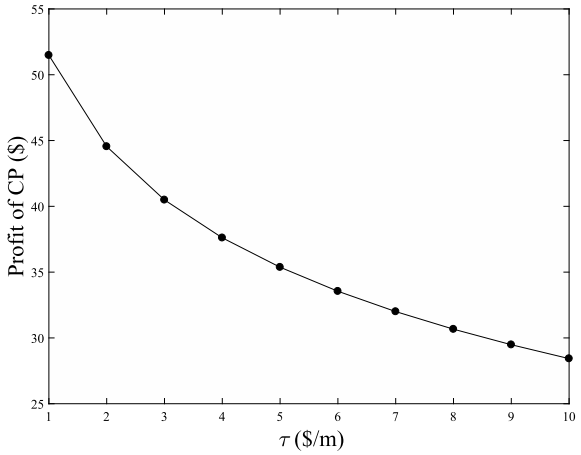

FIGURE 6. Impact of τ on CP's profit.

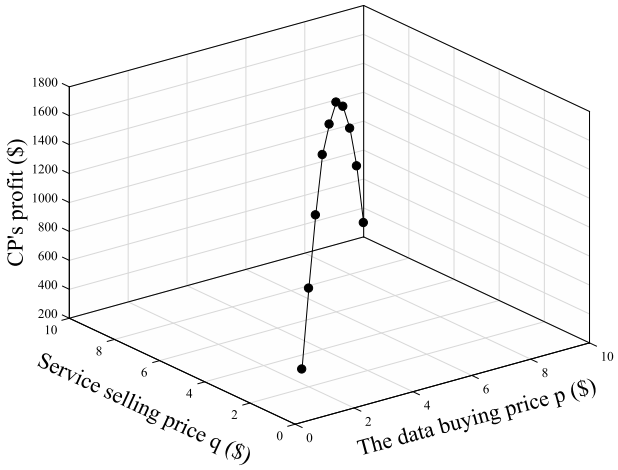

FIGURE 8. CP's profit.

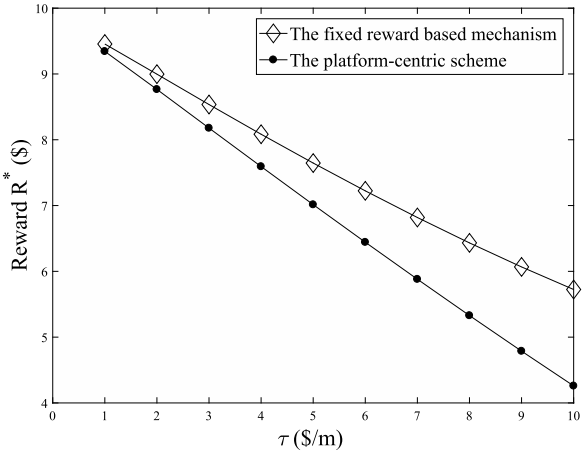

FIGURE 7. Impact of τ on R^*.

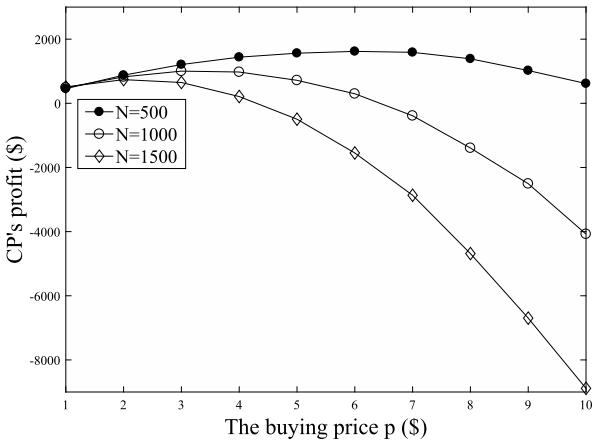

FIGURE 9. Impact of N on CP's profit.

information. For convenience, the notations and simulation parameters are shown in Table 3.

Fig. 8 shows CP's profit defined in (16) under varied buying price p and service price q. We can observe that CP's profit is strictly concave in p and q. In this case, a low buying price p will lead to fewer MUs who want to sell data, and CP can not charge a higher service price for SCs. Due to the existence of Q_0, CP still can gain some profit. If CP determines a too high buying price p, more MUs participate in contributing data. Although the quality of service can improve, the payment to MUs increases and CP's profit plunges. Similarly, when charging a low service price q, the revenue from SCs is small. If q is high, according to the defined demand function, fewer SCs will buy the service, As a result, CP's profit will tumble.

Then we study the impact of potential number of MUs. Here, we fix MUs' total number as $N = 500$, $N = 1000$ and $N = 1500$. The simulation results are shown in Fig. 9.

From Fig. 9, we can observe that the increasing price p attracts more MUs' participation, which increases CP's profit. When the price p is too high, CP's cost incurred by paying to MUs decreases the profit. Meanwhile, with a same price p, since MUs' total number N increases, CP's cost increases and the profit plunges. Fig. 10 shows how the tuple (α, β) affects CP's profit. As shown in Fig. 10, on the one hand, CP can obtain the maximal profit since the price p increases; on the other hand, if given same p, CP can gain a higher profit when α is larger than β. Generally speaking,

TABLE 3. Simulation parameters.

Symbol	Description	Value
N	MUs' number	500, 1000, 1500
$\overline{\theta}$	The upper bound of unit cost	10$
$\underline{\theta}$	The lower bound of unit cost	1$
p	Buying price for MUs' data	$[1\ 10]$$
q	Service price	$[1\ 10]$$
ϵ	Privacy budget	$[0\ 1]$
Q_0	Basic service demand	100
δ	CP's preference on MUs' data	$0.5\$ \cdot m^{-1}$
α, β	Demand function parameter	1, 2

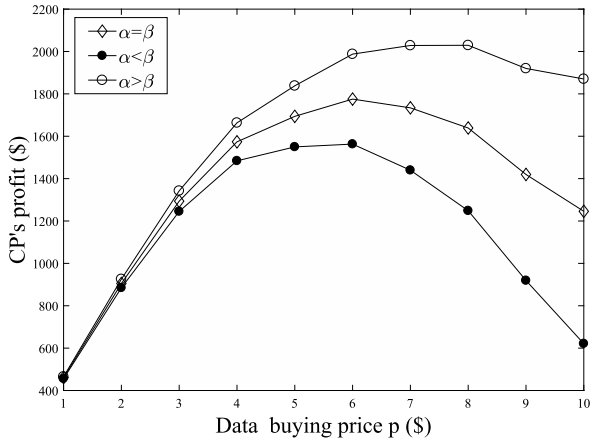

FIGURE 10. Impact of (α, β) on CP's profit.

the number of participating MUs is decided by the same data selling price, although MUs are heterogenous incurred by different unit cost for privacy loss. According to the function of the defined service demand, we know that the impact of data buying price p and service subscription price q are denoted by α and β, respectively. Hence, the increasing α can increase the service demand, CP can make higher profit. Similarly, when β decreases, larger service demand can achieve, higher profit CP can obtain.

VI. CONCLUSION

This paper studied the crowdsourced indoor localization incentive mechanism with privacy protection, and proposed two incentive mechanisms to stimulate MUs to contribute indoor trajectory data. The first mechanism considered fixed reward and incomplete information where each MU's sensitivity level of the data privacy was unknown to CP. The interaction between MUs and CP was formulated into a two-stage Stackelberg game to maximize MUs' utility and CP's profit. The second mechanism jointly considered the variable reward and assumed CP knew each MUs' sensitivity level of the data privacy. A demand function was used to model the relationship among CP, MUs and SCs. The optimization problem of CP's profit was studied to show the impact of the price fluctuation. Extensive simulations were conducted to demonstrate the performance of our proposed mechanisms.

REFERENCES

[1] A. Yassin *et al.*, "Recent advances in indoor localization: A survey on theoretical approaches and applications," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1327–1346, 2nd Quart., 2016.

[2] X. Tian, R. Shen, D. Liu, Y. Wen, and X. Wang, "Performance analysis of RSS fingerprinting based indoor localization," *IEEE Trans. Mobile Comput.*, vol. 16, no. 10, pp. 2847–2861, Oct. 2017.

[3] Q. Li, W. Li, W. Sun, J. Li, and Z. Liu, "Fingerprint and assistant nodes based Wi-Fi localization in complex indoor environment," *IEEE Access*, vol. 4, pp. 2993–3004, 2016.

[4] Q. Li, H. Fan, W. Sun, J. Li, L. Chen, and Z. Liu, "Fingerprints in the air: Unique identification of wireless devices using RF RSS fingerprints," *IEEE Sensors J.*, vol. 17, no. 11, pp. 3568–3579, Jun. 2017.

[5] S. He and S.-H. G. Chan, "Wi-Fi fingerprint-based indoor positioning: Recent advances and comparisons," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 466–490, 1st Quart., 2015.

[6] X. Zhang, A. K.-S. Wong, C.-T. Lea, and R. S.-K. Cheng, "Unambiguous association of crowd-sourced radio maps to floor plans for indoor localization," *IEEE Trans. Mobile Comput.*, vol. 17, no. 2, pp. 488–502, Feb. 2018.

[7] Q. Li, H. Qu, Z. Liu, N. Zhou, W. Sun, and J. Li. (2018). "AF-DCGAN: Amplitude feature deep convolutional GAN for fingerprint construction in indoor localization system." [Online]. Available: https://arxiv.org/abs/1804.05347

[8] R. Gao *et al.*, "Multi-story indoor floor plan reconstruction via mobile crowdsensing," *IEEE Trans. Mobile Comput.*, vol. 15, no. 6, pp. 1427–1442, Jun. 2016.

[9] B. Zhou *et al.*, "A graph optimization-based indoor map construction method via crowdsourcing," *IEEE Access*, vol. 6, pp. 33692–33701, 2018.

[10] Y. Zhang, L. Song, W. Saad, Z. Dawy, and Z. Han, "Contract-based incentive mechanisms for device-to-device communications in cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 10, pp. 2144–2155, Oct. 2015.

[11] Y. Zhang, Y. Gu, M. Pan, N. H. Tran, Z. Dawy, and Z. Han, "Multi-dimensional incentive mechanism in mobile crowdsourcing with moral hazard," *IEEE Trans. Mobile Comput.*, vol. 17, no. 3, pp. 604–616, Mar. 2018.

[12] D. Christin, "Privacy in mobile participatory sensing: Current trends and future challenges," *J. Syst. Softw.*, vol. 116, pp. 57–68, Jun. 2016.

[13] J. W. Kim, D.-H. Kim, and B. Jang, "Application of local differential privacy to collection of indoor positioning data," *IEEE Access*, vol. 6, pp. 4276–4286, 2018.

[14] B. Gu, Z. Liu, C. Zhang, K. Yamori, O. Mizuno, and Y. Tanaka, "A Stackelberg game based pricing and user association for spectrum splitting macro-femto HetNets," *IEICE Trans. Commun.*, vol. 101, no. 1, pp. 154–162, 2018.

[15] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell, "A survey of mobile phone sensing," *IEEE Commun. Mag.*, vol. 48, no. 9, pp. 140–150, Sep. 2010.

[16] S. Consolvo *et al.*, "Activity sensing in the wild: A field trial of ubifit garden," in *Proc. 26th Annu. ACM SIGCHI Conf. Hum. Factors Comput. Syst.*, 2008, pp. 1797–1806.

[17] L. Tang, X. Yang, Z. Dong, and Q. Li, "CLRIC: Collecting lane-based road information via crowdsourcing," *IEEE Trans. Intell. Transport. Syst.*, vol. 17, no. 9, pp. 2552–2562, Sep. 2016.

[18] A. Rai, K. K. Chintalapudi, V. N. Padmanabhan, and R. Sen, "Zee: Zero-effort crowdsourcing for indoor localization," in *Proc. ACM MobiCom*, 2012, pp. 293–304.

[19] C. Wu, Z. Yang, and Y. Liu, "Smartphones based crowdsourcing for indoor localization," *IEEE Trans. Mobile Comput.*, vol. 14, no. 2, pp. 444–457, Feb. 2015.

[20] H. Gao *et al.*, "A survey of incentive mechanisms for participatory sensing," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 918–943, 2nd Quart., 2015.

[21] D. Yang, G. Xue, X. Fang, and J. Tang, "Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones," *IEEE/ACM Trans. Netw.*, vol. 24, no. 3, pp. 1732–1744, Jun. 2016.

[22] Y. Xu and S. H. Low, "An efficient and incentive compatible mechanism for wholesale electricity markets," *IEEE Trans. Smart Grid*, vol. 8, no. 1, pp. 128–138, Jan. 2017.

[23] Y. Zhang, C. Jiang, L. Song, M. Pan, Z. Dawy, and Z. Han, "Incentive mechanism for mobile crowdsourcing using an optimized tournament model," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 4, pp. 880–892, Apr. 2017.

[24] X. Wang, Z. Liu, X. Tian, X. Gan, Y. Guan, and X. Wang, "Incentivizing crowdsensing with location-privacy preserving," *IEEE Trans. Wireless Commun.*, vol. 16, no. 10, pp. 6940–6952, Oct. 2017.

[25] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "L-diversity: Privacy beyond k-anonymity," *ACM Trans. Knowl. Discovery Data*, vol. 1, no. 1, 2007, Art. no. 3.

[26] C. Dwork, "Differential privacy: A survey of results," in *Proc. Int. Conf. Theory Appl. Models Comput.* Berlin, Germany: Springer, 2008.

[27] Y. Wang, Z. Cai, X. Tong, Y. Gao, and G. Yin, "Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems," *Comput. Netw.*, vol. 135, pp. 32–43, Apr. 2018.

[28] B. Zhou, Q. Li, Q. Mao, W. Tu, and X. Zhang, "Activity sequence-based indoor pedestrian localization using smartphones," *IEEE Trans. Human-Mach. Syst.*, vol. 45, no. 5, pp. 562–574, Oct. 2015.

[29] M. Mladenov and M. Mock, "A step counter service for java-enabled devices using a built-in accelerometer," in *Proc. 1st Int. Workshop ContextAware Middleware Services, Affiliated 4th Int. Conf. Commun. Syst. Softw. Middleware*, 2009, pp. 1–5.
[30] L. Xu, C. Jiang, Y. Chen, Y. Ren, and K. J. R. Liu, "Privacy or utility in data collection? A contract theoretic approach," *J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1256–1269, Oct. 2015.
[31] A. Ghosh and A. Roth, "Selling privacy at auction," *Games Econ. Behav.*, vol. 91, pp. 334–346, May 2015.
[32] M. A. Alsheikh, D. Niyato, D. Leong, P. Wang, and Z. Han, "Privacy management and optimal pricing in people-centric sensing," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 4, pp. 906–920, Apr. 2017.
[33] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[34] W. C. Cheung, D. Simchi-Levi, and H. Wang, "Dynamic pricing and demand learning with limited price experimentation," *Oper. Res.*, vol. 65, no. 6, pp. 1722–1731, 2017.

WEI LI received the B.S. degree in automation and the M.S. degree in control engineering from the Hefei University of Technology, China, in 2014 and 2017, respectively. He is currently pursuing the Ph.D. degree with the Department of Computer Science and Communications Engineering, Waseda University. His research interests include crowdsourcing, network economics, game theory, and indoor localization.

CHENG ZHANG (M'16) received the Ph.D. degree from Waseda University, Tokyo, Japan, in 2015. From 2008 to 2015, he was a Research Engineer at Sony Digital Network Applications, Japan, and HGST Japan, Inc., (formerly Hitachi Global Storage Technologies), where he researched and developed control algorithms for image stabilization module of Sony digital camera, and servo control algorithms for next generation high capacity HDD. He is currently an Assistant Professor of the Graduate Program for Embodiment Informatics (Program for Leading Graduate School) at the Graduate School of Fundamental Science and Engineering, Waseda University. His research interests include machine control algorithm, embedded software, game theory, network economics, and machine learning. He is a member of IEICE. He received the IEICE Young Researcher's Award in 2013.

ZHI LIU (S'11–M'14) received the B.E. degree from the University of Science and Technology of China, China, and the Ph.D. degree in informatics from the National Institute of Informatics. He was a Junior Researcher (Assistant Professor) at Waseda University and a JSPS Research Fellow with the National Institute of Informatics. He is currently an Assistant Professor at Shizuoka University. His research interests include video network transmission, vehicular networks and mobile edge computing. He is a member of IEICE. He was a recipient of the IEEE StreamComm2011 Best Student Paper Award, the 2015 IEICE Young Researcher Award, and the ICOIN2018 Best Paper Award. He has been serving as the chair for number of international conference and workshops. He is and has been the Guest Editor of *Wireless Communications and Mobile Computing*, *Sensors* and *IEICE Transactions on Information and Systems*.

YOSHIAKI TANAKA (S'74–M'79–SM'97–LSM'17) received the B.E., M.E., and D.E. degrees in electrical engineering from the University of Tokyo, Tokyo, Japan, in 1974, 1976, and 1979, respectively. He became a Staff at the Department of Electrical Engineering, The University of Tokyo, in 1979, and has been engaged in teaching and researching in the fields of telecommunication networks, switching systems, and network security. He is currently a Professor at the Department of Communications and Computer Engineering, Waseda University. He is an Honorary Member of IEICE. He received the IEICE Best Paper Award, the IEICE Achievement Award, the IEICE Distinguished Achievement, and the Contributions Award, the Okawa Publication Prize, and the Commendation by Minister for Internal Affairs and Communications.