A Secure Auction Mechanism for Task Allocation in Mobile Crowdsensing

Dan Li[1], Tong Liu[1,2](✉), and Chengfan Li[1,2]

[1] School of Computer Engineering and Science, Shanghai University, Shanghai, China
{ld19721539,tong_liu}@shu.edu.cn
[2] Shanghai Engineering Research Center of Intelligent Computing System, Shanghai, China

Abstract. Mobile crowdsensing has attracted widely attention as a new sensing paradigm, in which mobile users collect sensing data by their devices embedded various sensors. To motivate mobile users participating in sensing tasks, a number of auction mechanisms have been proposed. In our work, we focus on the task allocation problem with multiple constraints for the auction-based crowdsensing system to maximize profit of the central platform, which has been proved to be NP-hard. To solve the problem, a greedy-based task allocation algorithm with $(1+\gamma)$-approximation solution is proposed, in which the bid improving profit of the platform most is selected as the winning bid greedily in each iteration. However, bids for all tasks of a user submitted to the platform might let out location of the user unexpectedly. Therefore, we further design a secure auction mechanism with secret-sharing-based task allocation protocol, where each user can submit at most a winning bid to the platform instead of all bids for tasks to prevent locations of users from being inferred. The effectiveness of task allocation and location privacy protection based on our proposed secure auction mechanism is verified by theoretical analysis and simulations.

Keywords: Mobile crowdsensing · Privacy protection · Auction mechanism · Secret sharing

1 Introduction

With the improvement of 5G technology, Internet of Things (IOT) devices interact with each other at low delay and high rate to provide services such as intellisense, recognition and pervasive computing. As a new sensing paradigm of IOT, mobile crowdsensing [1] collects data through large-scale smart mobile devices embedded sensors like accelerator, camera, GPS, etc. Generally, a crowdsensing system consists of many mobile user devices to collect sensing data and a central platform resided on the cloud to extract valuable information from received sensing data. Compared with the traditional data acquisition method which takes advantage of purchasing and installing sensors, mobile user devices have more

H. Gao et al. (Eds.): CollaborateCom 2022, LNICST 461, pp. 174–193, 2022.
https://doi.org/10.1007/978-3-031-24386-8_10

flexibility to collect a large amount of data in different regions in crowdsensing system. Thanks to the effectiveness of mobile crowdsensing, it has been applied in many fields such as health care [11], environmental monitoring [9], traffic prediction [14,16].

In order to ensure the quality of service for mobile crowdsensing applications, it is important to stimulate mobile users to participant in sensing tasks. Moreover, assigning tasks to users for execution (i.e., task allocation) is a critical step to impact profit of the platform, which has become a major concern. So far, many task allocation methods have been proposed to address the problem of motivating users based on auction mechanisms [19,22,24]. Normally, a mobile user should transmit bid data including bids for all tasks to the platform for task allocation. However, the sensitive information such as location of each user might be revealed unexpectedly in an auction-based crowdsensing system without trusted third parties when raw bid data of users are submitted to the platform. The intuition of location leakage is that the smaller the bid for a task in bid data submitted by a user, the distance between the user and the task is shorter. If mobile crowdsensing applications fail to effectively protect location privacy of mobile users, users will be reluctant to take part in sensing tasks. Thus, it is vitally important to protect sensitive information of users for a crowdsensing system.

Nowadays, a number of literature is committed to protect the location privacy of mobile users for crowdsensing systems. Some location privacy protection mechanisms are proposed for crowdsensing with third trusted parties by applying encryption and differential privacy (DP). For these encryption approaches [2,4,7,20], they always assume there is a trusted authority in the crowdsensing system which is responsible for key generation and distribution to collaborate with smart mobile users to encrypt sensitive data. Differently, DP-based methods [6,18] perturb the original sensitive data of smart device users by a trusted platform to keep privacy information from leakage. However, it is not realistic to assume that there is a completely trusted third party. Fortunately, both location differential privacy (LDP) and secret-sharing method are effective tools for crowdsensing without a trusted third party. Compared to DP-based approaches, LDP-based methods [5,12,17,23] perturb sensitive data by mobile users locally instead of the platform. Differently, the research based on the secret sharing scheme [21] divides private data into multiple shares and send these shares to other users to compute collaboratively and safely through interactive communication. However, there are few methods considering location privacy leakage of users by bid information for task allocation in the auction-based crowdsensing system without any trusted third party.

Although these researches have protected the private locations of mobile users, it is very difficult for them to be applied to our proposed model. *Firstly*, we must ensure that the location privacy information cannot be inferred based on bids submitted by users during the auction mechanism for our mobile crowdsensing system, meanwhile the task allocation decisions should be decided. However, it is ignored by many existing works. *Secondly*, the DP and LDP schemes inevitably lead to performance degradation of results by adding noise. Thus, it is unjustified to adopt the methods to protect privacy for the NP-hard problem in our work which can only obtain an approximate solution in polynomial time. *Finally*, although existing works based on encryption schemes can achieve the homomorphism of the calculation to ensure the validity of decisions, they set up an authority agency to generate and distribute keys in the crowdsensing system. Moreover, encryption will generate a huge computational cost, which greatly increases the computation delay of privacy protection.

To solve the problem of task allocation for auction-based crowdsensing system, we firstly propose the greedy-based task allocation (GBTA) algorithm. Then, a secure auction mechanism utilizing secret-sharing-based task allocation (SSTA) protocol is designed, in which each user only submits the winning bid to the platform. For the auction mechanism based on GBTA algorithm, each user submits bid data for all tasks to the platform and the algorithm greedily selects a winning bid which can most improve profit of the platform in each iteration. However, as the bid data of a user should be enclosed and submitted to the untrusted platform, the location of the user might be inferred. Thus, we apply secret sharing technology to design a secure auction mechanism, in which each mobile user splits one bid into multiple polynomial bid shares and sends them to other users. After these users complete security multi-party computation according to SSTA protocol, all users will return the decision shares they hold for restoration. In the end, each user only needs to upload the price request for the assigned task, not for all tasks. As the platform cannot infer the distance relationship between tasks and a user according to the submitted winning bid of the user based on our secure auction mechanism, the location privacy of users can be well protected.

The main contributions of our work are summarized in the following:

- we consider the task allocation problem in the auction-based crowdsensing system, in which one task can be allocated to multiple users under budget constraint of the task. Meanwhile, the attack model which can infer locations of users based on bid data is presented. We prove the task allocation problem is NP-hard, then the GBTA algorithm is designed to obtain an approximate solution.
- To protect the location information of users during the auction process, a secure auction mechanism incorporating the SSTA protocol is proposed for crowdsensing without a trusted third party, in which each mobile user can only submit at most one winning bid to the platform. Moreover, the SSTA protocol can obtain the same approximate solution as GBTA. We prove that the location privacy of users is well protected from being disclosed to third parties during the execution of SSTA.
- We conduct simulations to evaluate the effectiveness of task allocation and location privacy protection level of the proposed mechanism. The results show that our method can effectively protect the location privacy of users while ensuring the profit of the platform.

This paper is organized as follows. We first discuss related works in Sect. 2. Then, we present our system model, attack model and problem formulation in

Sect. 3. The GBTA algorithm and the secure auction mechanism utilizing SSTA protocol with a logarithmic approximation ratio are proposed in Sect. 4. Finally, simulation results are presented in Sect. 5, and the paper is concluded in Sect. 6.

2 Related Work

In this section, we present briefly several location privacy-preserving mechanisms for mobile crowdsensing which can be classified into two categories including of trusted third party (TTP) assisted mechanisms and TTP-free mechanisms.

There are some works [2,4,6,7,18,20] focus on crowdsensing systems with TTPs. The approach proposed in [2] can prevent leakage of geo-tagged sensing data for crowdsensing with fog nodes effectively by applying Paillier encryption, in which the users send ciphertext of sensing data encrypted with a key distributed by the TTP. In [4], locations of users and regions of sensing tasks can be encrypted into a set of prefixes after key distribution by the trusted authority based on prefix encoding method. Moreover, both [7,20] are committed to design secure reverse auction mechanisms to protect locations of users by preventing bid leakage during auction period for crowdsensing with a TTP distributing keys to users. Li *et al.* [6] obfuscate position correlation weights between mobile users through trusted edge nodes based on differential privacy for edge computing. Wei *et al.* [18] assume that the cellular service provider is a TTP, and service requesters and mobile users send raw location data to the TTP for adding noise.

In other works [5,12,17,21,23], researchers assume that there is no TTP in the proposed crowdsensing system. Obviously, this assumption is more realistic. To recruit mobile users, Li *et al.* [5] guarantee the crowdsensing coverage meanwhile protecting locations of users based on LDP methods. Mobile users need upload one of frequently visited obfuscated-locations and find a set of users to maximize future crowdsensing coverage based on these perturbed locations in [17]. A novel location privacy-preserving mechanism is designed in [23] to protect the location of users in the space dimension and spatiotemporal activity. For the field of Internet of Vehicles, Qian *et al.* [12] propose a location-preserving task allocation method meanwhile improving task quality by perturbing locations on mobile devices. Different from above works, Xiao *et al.* [21] protect the sensing quality of each user to prevent location privacy leakage based on secret sharing scheme.

However, there are few works which are commited to location privacy protection at the auction stage for the crowdsensing system without any TTP.

3 System Model and Problem Formalization

In this section, we introduce our crowdsensing system model which consists of a semi-honest central platform and plenty of semi-honest mobile users. Then, a security model is introduced to measure the computation security under semi-honest model in our crowdsensing system and an attack model is presented to infer locations of users based on the received bid data. Finally, the task allocation problem formalization is given.

3.1 Crowdsensing System Model

We consider there is a central platform to announce many sensing tasks $\mathcal{T} = \{t_1, t_2, \cdots, t_m\}$ and some mobile users $\mathcal{U} = \{u_1, u_2, \cdots, u_n\}$ participate in sensing tasks in our crowdsensing system. Moreover, the platform and users are semi-honest, which means they may extract extra information from received data. After the platform announces sensing tasks, a user can be allocated at most one task to execute and each task may be allocated to multiple users so that the platform can obtain an accurate estimated value of the task based on a mass of sensing data collected by these users. For sake of convenience, geographical locations can be represented by two-dimensional grid coordinates in a 2D space. Thus, each task is denoted by a tuple $t_j \overset{\text{def}}{=} <l_j, B_j>$, where l_j is the grid coordinate location of the sensing task t_j, and B_j is the total budget of t_j.

If a user u_i's location is inconsistent with the location of the task t_j to be performed, the user should move to the location of the task to collect sensing data. The cost of the movement is denoted by c_i^j, which is positively correlated with the distance d_i^j between user u_i and task t_j. Compared to the cost of movement, the cost of performing tasks can be neglected so that the bid of user u_i performing task t_j is equivalent to the cost of movement and can be also denoted by c_i^j. That is to say, the bid increases as the distance between the user and the task increases. After the sensing data collected by user u_i of task t_j is transmitted to the platform, the platform will make a profit $\alpha_i G_j - c_i^j$, in which $\alpha_i \in [0, 1]$ represents the credit of user u_i for completing tasks according to quality of historical sensing data and G_j is the basic earning of task t_j provided by the platform.

As shown as Fig. 1, the auction process for our auction-based crowdsensing system can be divided into five steps: (1) The platform publishes m location-sensitive tasks with location tags and budget constraints. (2) Each user generates the bid set $C_i = \{c_i^1, c_i^2, \cdots, c_i^j\}$ based on the distance to tasks and submits these bid data to the platform. (3) The platform allocates tasks to users to maximize the profit of the platform according to received bid sets of all users $\mathcal{C} = \{C_1, C_2, \cdots, C_n\}$. (4) Each user submits the results of allocated sensing task to the platform. (5) The platform pays some rewards to users according to the winning bids.

However, as the raw bid sets are uploaded to the central platform in the auction-based crowdsensing system, the platform may infer the location of a user according to the distance between the user and each task contained in the bid set. Therefore, a secure auction mechanism for crowdsensing without any TTP will be designed in the Sect. 4.4 to prevent the location of each user from being revealed.

3.2 Security Model

In our work, both the platform and mobile users are semi-honest. On the one hand, the platform and mobile users follow the task allocation protocol, showing the honest aspect. On the other hand, they may infer the location privacy

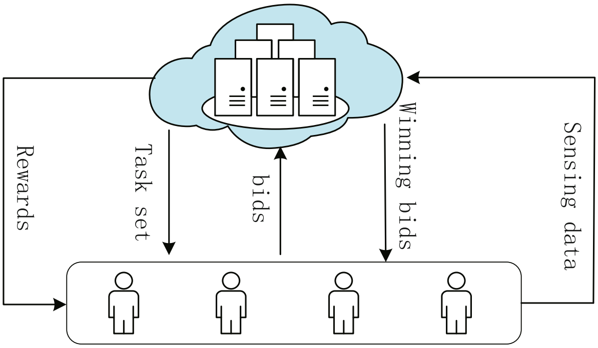

Fig. 1. An auction-based crowdsensing system model.

according to the received bid data in the course of auction, showing the dishonest aspect. Moreover, if each semi-honest party in system cannot extract extra information from the received data during execution of protocol, we can consider the computation in the protocol to be private. The private computation under semi-honest model can be defined in the following:

Definition 1 (Private computation under semi-honest model [3]). *Suppose there is a function $\mathcal{F}$ that is computed jointly by n parties, we let x_i be the input of the i-th party, and $\mathcal{F}_i$ is the output of the i-th party, i.e., $\mathcal{F}(x_1, x_2, \cdots, x_n) = (\mathcal{F}_1, \mathcal{F}_2, \cdots, \mathcal{F}_n)$. Especially, let $1 \leq i \leq n$ represent n mobile users. The view of the i-th party during the execution of the protocol is $VIEW_i = (x_i, r, m_i)$, where r represents the outcome of the i-th party's internal coin tosses and m_i represents the messages that the user has received. For $\mathcal{I} = \{i_1, i_2, \cdots, i_k\} \subset \{1, 2, \cdots, n\}$, the outcomes of these parties $\mathcal{F}_{i_1}, \mathcal{F}_{i_2}, \cdots, \mathcal{F}_{i_k}$ can be denoted by $\mathcal{F}_\mathcal{I}$. Moreover, the view of $\mathcal{I}$ is $VIEW_\mathcal{I} \overset{def}{=} (\mathcal{I}, VIEW_{i_1}, VIEW_{i_2}, \cdots, VIEW_{i_k})$. Then, for any party subset $\mathcal{I}$, the computation protocol can compute the function $\mathcal{F}$ privately if there exists a polynomial time algorithm $\mathcal{A}$ satisfying the following relationship:*

$$\mathcal{A}(\mathcal{I}, (x_{i_1}, x_{i_2}, \cdots, x_{i_k}, \mathcal{F}_\mathcal{I})) = VIEW_\mathcal{I}. \tag{1}$$

According to Eq. (1), what is acquired from a party's view can be obtained entirely from the input and output of this party. That is to say, any party in our system cannot infer the location information from they received data as long as a private computation protocol is designed.

3.3 Attack Model

For the crowdsensing system, we introduce an attack model to infer the location of a user according to bid data submitted by the user. For the convenience of expression, the candidate locations, where the distance to tasks increases as the bid increases, are denoted by $\mathcal{L}$. Then, the attacker infers the location of a user

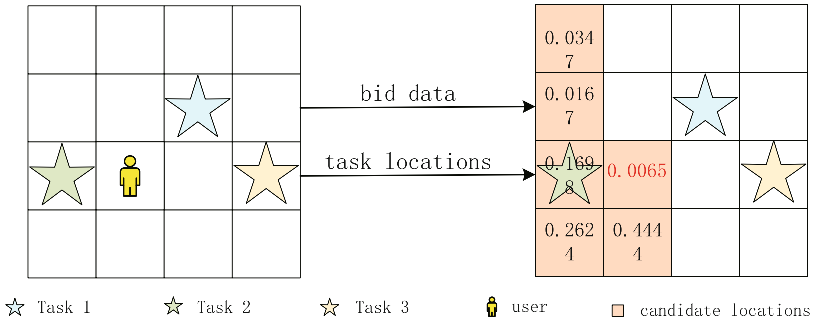

Fig. 2. An attack example.

by calculating the Euclidean distance similarity between the normalized distance vector from a candidate location to tasks and the normalized bid vector.

For example, there is a region divided to 4 * 4 grids and a user at location (1,1), three tasks located at (2,2), (0,1), (3,1) respectively as shown as Fig. 2. Suppose the original bid vector is set as (2,1,4) computed by the square function. Firstly, the candidate locations $\mathcal{L}$ can be determined as coloured areas in the figure. That is to say, the distances from a location in $\mathcal{L}$ to task 2, task 1, and task 3 are monotonically increasing and the user must be in one of these candidate locations. Next, the Euclidean distance similarity between the normalized distance vector of each candidate grid and normalized bid vector can be obtained. Finally, we can find that the value of grid (1,1) is smallest which means the user is most likely to be in the location. So far, an attacker may infer the location of a user based on the received bid information.

3.4 Problem Formalization

In the work, we focus on the secure task allocation problem in the auction-based mobile crowdsensing under the semi-honest model to maximize the total profit of the platform. Then, the problem can be formalized as follows:

$$\mathit{Maximize:} \quad \sum\nolimits_{j=1}^{m} \sum\nolimits_{i=1}^{n} (\alpha_i G_j - c_i^j) x_i^j \tag{2}$$

$$\mathit{Subject\ to:} \quad \sum\nolimits_{i=1}^{n} c_i^j x_i^j \leq B_j \tag{3}$$

$$\sum\nolimits_{j=1}^{m} x_i^j \leq 1 \tag{4}$$

$$x_i^j \in \{0,1\} \tag{5}$$

$$Eq. (1) \quad \text{holds} \tag{6}$$

Here, Eq. (3) represents the budget constraint, which means the total cost of multiple users performing a task cannot exceed budget of the task and Eq. (4) indicates that each user can be allocated at most one task. Equation (5) shows the task allocation decision x_i^j is binary. If the task t_j is allocated to the u_i (i.e., bid c_i^j is one of winning bids), the decision variable $x_i^j = 1$, otherwise $x_i^j = 0$. To protect the location of each user from being revealed, Eq. (6) should be satisfied so that additional location information of users can not be inferred during the execution of a secure computation protocol.

4 Methodology

In this section, we first introduce a GBTA algorithm for the system without security guarantee, and we analyse theoretically the approximation ratio achieved by the GBTA algorithm. Moreover, a secure auction mechanism with SSTA protocol is designed on this basis. Finally, we prove that the location of each user can be preserved well during the execution of SSTA and the accuracy of this method is same as GBTA algorithm.

4.1 Problem Complexity Analysis

Theorem 1. *The task allocation problem is NP-hard.*

Proof. We consider a special case of the task allocation problem, in which there is only one task to be allocated, i,e., $\mid \mathcal{T} \mid = 1$. Thus, each user u_i will generate a bid c_i for the task. Moreover, the credit of user u_i is denoted by α_i, G is the basic earning of the task provided by the platform and the budget of the task is B. Then, we should select some users $\mathcal{U}' \subseteq \mathcal{U}$ performing the task to maximize $\sum_{u_i \in \mathcal{U}'} (\alpha_i G - c_i)$, while the total bid of users $\mathcal{U}'$ is no more than the budget B. Obviously, the special problem is regarded as 0–1 knapsack problem equivalently which is a classic NP-hard problem: Given a knapsack with capacity B and an item set $\mathcal{U}$, the value of item u_i is $\alpha_i G - c_i$ and the weight is c_i, select some items to put into the knapsack to maximize the total value within the capacity of the knapsack. Accordingly, the general task allocation problem in our work is at least NP-hard.

4.2 Greedy-Based Task Allocation Algorithm

As the task allocation problem is NP-hard, an algorithm based on greedy strategy is designed to obtain an approximate solution in polynomial time. Firstly, let $\mathcal{X}$ be the set of decision variable x_i^j whose initial value is 0. The GBTA algorithm contains multiple iterations and the algorithm always selects the bid which most improves the profit of the platform within the budget constraints of tasks in each iteration. That is to say, if there is a bid c_i^j that makes $\alpha_i G_j - c_i^j$ the largest non-negative value, the task t_j will be allocated to user u_i, i,e., $x_i^j = 1$. Moreover, if there is no bid to meet the budget constraint or make non-negative profit in bid data of a user, the user will be not assigned tasks. Since each user is assigned at most one task, the user u_i should be removed from the user set $\mathcal{U}$ after a task is allocated to the user and GBTA terminates when the user set is empty.

Algorithm 1: Greedy-Based Task Allocation algorithm

```
Input: $\mathcal{U}, \mathcal{S}, \mathcal{C}, \{\alpha_i \mid i \in \mathcal{U}, j \in \mathcal{T}\}, \{B_j, G_j \mid j \in \mathcal{T}\}$
Output: $\mathcal{X}$
    initialization: $\mathcal{X} = \mathbf{0}$, $max = -1$
 1: while $\mathcal{U} \neq \varnothing$ do
 2:     for each user $i$ in $\mathcal{U}$ do
 3:         construct task set of each user $u_i$:
            $T_i' = \{t_j \mid c_i^j \leq B_j, \alpha_i G_j - c_i^j \geq 0\}$
 4:         if $T_i' = \varnothing$ then
 5:             $\mathcal{U} = \mathcal{U} \backslash u_i$;
 6:     for each user $i$ in $\mathcal{U}$ do
 7:         for each task $j$ in $T_i'$ do
 8:             if $\alpha_i G_j - c_i^j > max$ then
 9:                 $max = \alpha_i G_j - c_i^j$
10:                 $allocTask = j$
11:                 $selUser = i$
12:     $x_{selUser}^{AllocTask} = 1$
13:     $\mathcal{U} = \mathcal{U} \backslash selUser$
14:     $B_{allocTask} = B_{allocTask} - c_i^j$
15: return task allocation decision $\mathcal{X}$
```

The detailed GBTA algorithm is as shown as Algorithm 1. From step 2 to step 5, we construct a candidate task set for each user, in which each task has enough budget and the profit of the platform will be improved by assigning the task to the user. If the candidate task set of a user u_i is empty, the user will not be assigned any task. Then, a winning bid which produces largest non-negative profit $\alpha_i G_j - c_i^j$ within task budget constraint is determined in step 6–11 for each iteration and we record the index of the winning bid. When a bid c_i^j is winning bid, the task t_j will be allocated to the user u_i. Thus, we remove the user who has been assigned a task from the user set and update the budget of the task t_j in step 12–14.

4.3 Approximation Performance Analysis

Theorem 2. *Suppose the profit produced by Algorithm 1 is F_{alg} and the profit generated by the optimal solution is F_{opt}. They satisfy the following equation:*

$$\frac{F_{opt}}{F_{alg}} \leq 1 + \gamma, \ \textit{where } \gamma = max\{\frac{B_j}{c_i^j} \mid t_j \in \mathcal{T}, u_i \in \mathcal{U}\} \tag{7}$$

Proof. Then, we can prove Eq. (7) by adopting mathematical induction method.

(1) Firstly, when $\mid \mathcal{U} \mid = 1$, we can find obviously that the greedy solution is same as optimal solution and $F_{opt}/F_{alg} = 1 (< 1 + \gamma)$.

(2) Next, suppose $F_{opt}/F_{alg} \leq 1 + \gamma$ holds when $\mid \mathcal{U} \mid = n$.

(3) Given $\mid \mathcal{U} \mid = n+1$. Without loss of generality, we assume that $\alpha_1 G_1 - c_1^1 = max\{\alpha_i G_j - c_i^j \mid u_i \in \mathcal{U}, t_j \in \mathcal{T}\}$ and the value is non-negative. According to the

GBTA algorithm, u_1 must be assigned task t_1, i,e., $x_i^j = 1$. Now, we consider two cases in the following:

In the Optimal Solution, Task t_1 is also Allocated to User u_1. Consider the sub-problem P' in which the user set is $\mathcal{U}' = \mathcal{U} - \{u_1\}$ and the budget of task t_1 is $B_1' = B_1 - c_1^1$. After running the GBTA algorithm for the sub-problem P', we can get the profit $F_{alg|P'}$. Moreover, the profit generated by optimal solution for the sub-problem is denoted by $F_{opt|P'}$. Then, we have $F_{alg} = F_{alg|P'} + (\alpha_1 G_1 - c_1^1)$ and $F_{opt} = F_{opt|P'} + (\alpha_1 G_1 - c_1^1)$ based on optimal structure of our problem. According to the step (2) of the mathematical induction, we find $F_{opt|P'} \le (1+\gamma) F_{alg|P'}$. Accordingly, we have:

$$\frac{F_{opt}}{F_{alg}} = \frac{F_{opt|P'} + (\alpha_1 G_1 - c_1^1)}{F_{alg|P'} + (\alpha_1 G_1 - c_1^1)} \le 1 + \gamma \tag{8}$$

In the Optimal Solution, Task t_1 is Not Allocated to User u_1. Thus, the task t_1 is assigned to other users $\mathcal{U}_{opt}^{(1)}$ and the profit generated by the allocated task t_1 based on optimal solution is denoted by $F_{opt}^{(1)}$. Then, we have:

$$F_{opt}^{(1)} = \sum_{u_i \in \mathcal{U}_{opt}^{(1)}} (\alpha_i G_1 - c_i^1) \le \gamma (\alpha_1 G_1 - c_1^1) \tag{9}$$

Without loss of generality, we assume the user u_1 is allocated task t_2 in optimal solution. Consider the sub-problem P'' in which the user set is $\mathcal{U}'' = \mathcal{U} - \{u_1\} - \mathcal{U}_{opt}^{(1)}$, the task set is $\mathcal{T}'' = \mathcal{T} - \{t_1\}$ and the budget of task t_2 is $B_2 - c_1^2$. The profit produced by optimal solution for the sub-problem can be denoted by $F_{opt|P''}$. Then, we have:

$$F_{opt} = F_{opt|P''} + F_{opt}^{(1)} + (\alpha_1 G_2 - c_1^2) \tag{10}$$

It should be noted that the sub-problem P'' is contained in problem P' so that $F_{opt|P''} \le F_{opt|P'}$. Moreover, as $|\mathcal{U}'| = n$ in sub-problem P', we can get $F_{opt|P'} \le (1+\gamma) F_{alg|P'}$. Thus, the following inequality exists:

$$F_{opt|P''} \le (1+\gamma) F_{alg|P'} \tag{11}$$

From Eq. (9) to Eq. (11) and $\alpha_1 G_1 - c_1^1 = max\{\alpha_i G_j - c_i^j \mid u_i \in \mathcal{U}, t_j \in \mathcal{T}\}$, we have:

$$\begin{aligned} \frac{F_{opt}}{F_{alg}} &= \frac{F_{opt|P''} + F_{opt}^{(1)} + (\alpha_1 G_2 - c_1^2)}{F_{alg|P'} + (\alpha_1 G_1 - c_1^1)} \\ &\le \frac{(1+\gamma) F_{alg|P'} + \gamma(\alpha_1 G_1 - c_1^1) + (\alpha_1 G_2 - c_1^2)}{F_{alg|P'} + (\alpha_1 G_1 - c_1^1)} \\ &\le 1 + \gamma \end{aligned} \tag{12}$$

So far, Theorem 2 is proved. That is to say, GBTA algorithm can achieve $(1+\gamma)$-approximation solution where $\gamma = max\{\frac{B_j}{c_i^j} \mid t_j \in \mathcal{T}, u_i \in \mathcal{U}\}$.

4.4 A Secure Auction Mechanism for Task Allocation

For the basic auction-based crowdsensing system, the location of a user could be leaked out as the bid set of the user is submitted to the platform to execute the GBTA algorithm. To protect the bid information from third parties, we apply the secret sharing scheme to the GBTA. Firstly, we introduce the preliminaries of a well-known Shamir secret sharing scheme and then a secure auction mechanism with SSTA protocol is designed for protecting sensitive information and assigning tasks to users.

Preliminaries

Definition 2 (Shamir secret sharing). *Let p be an odd prime and $\mathbb{Z}_p$ be a prime field. A secret $s \in \mathbb{Z}_p$ means that $s \in \{0, 1, 2, \cdots, p-1\}$. If a secret s is shared among n parties based on a random polynomial $f_s = s + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_t x^t \bmod p$ with randomly chosen $\alpha_k \in \mathbb{Z}_p$ for $1 \leq k \leq t \leq \frac{n}{2}$, $[s]_p = \{f_s(i) \mid 1 \leq i \leq n\}$ is a share set of the secret $s \in \mathbb{Z}_p$. Moreover, the share of secret s received by party i in the $[s]_p$ is denoted by $[s]_p^i$.*

Suppose that there are two secrets a, b to be shared and the random polynomials with degree t of them are $f_a = a + a_1 x + a_2 x^2 + \cdots + a_t x^t \bmod p$ and $f_b = b + b_1 x + b_2 x^2 + \cdots + b_t x^t \bmod p$, respectively. For the sake of writing, we use $[\cdot]$ instead of $[\cdot]_p$ in the following. Then, there are some mathematical operations of secure multi-party computation to calculate one function based on Shamir secret sharing scheme. The addition operation and subtraction operation can be redefined and computed as follows:

$$[a] + [b] \triangleq [(a+b) \bmod p] = ([a] + [b]) \bmod p \tag{13}$$

$$[a] - [b] \triangleq [(a-b) \bmod p] = ([a] - [b]) \bmod p \tag{14}$$

The Eq. (13) above can be established as $f_a + f_b = (a+b) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_t + b_t)x^t \bmod p$ and in a similar way, Eq. (14) is correct. Obviously, we can find that each user u_i can calculate the redefined addition and subtraction of own shares locally by the received share $[a]_p^i$ and share $[b]_p^i$.

However, the multiplication operation $[a] * [b] \triangleq [(a*b) \bmod p]$ and comparison operation $Comp([a], [b])$ can not be realized locally for any party. Let l be the bit size of the prime p. In our work, $[a] * [b]$ is computed by communicating with other parties according to the secure distributed multiplication protocol [8] based on Newton's interpolation theorem, in which the computation complexity is $O(n^2 l)$ bit-operations per user and the communication complexity is $O(nl)$. To compare the value a and value b, a multiparty comparison computation protocol [10] is proposed, in which the communication complexity is $279l + 5$ times as large as the multiplication operation and the computation complexity depends on 15 rounds of performing the multiplication protocol in parallel. Note that if $a \leq b$, the comparison protocol determines $Comp([a], [b]) = [1]$, otherwise $Comp([a], [b]) = [0]$. Then, the max selection operation $Max([a], [b]) \triangleq [max(a, b)]$ can be calculated by $[a] + (Comp([a], [b]) * ([b] - [a]))$.

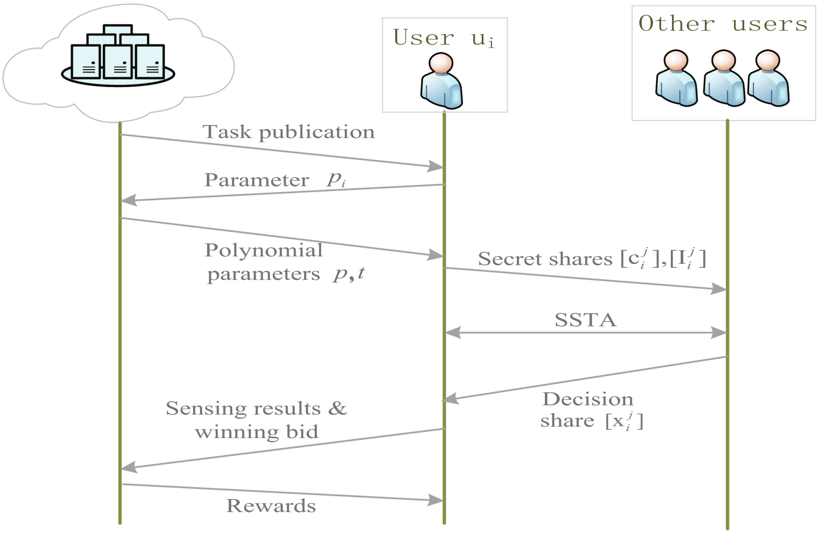
User u_i
Other users
Task publication
Parameter p_i
Polynomial parameters p, t
Secret shares $[c_i^j], [I_i^j]$
SSTA
Decision share $[x_i^j]$
Sensing results & winning bid
Rewards

Fig. 3. A secure auction mechanism for crowdsensing system.

Design for Secure Auction Mechanism. In auction-based crowdsensing system, if only the winning bid of a user is submitted to the platform, the platform can not infer location of the user according to the distance relationship between the user and tasks contained in bid set of the user. This gives us the inspiration to design our secure auction mechanism to maximize total profit of the platform by task allocation. The main steps of our secure auction mechanism are as shown as Fig. 3.

(1) *Task Publication:* The platform publishes m tasks, the location l_j and the budget B_j of each task $t_j, 1 \leq j \leq m$. Moreover, the platform computes the value of $\alpha_i G_j$ and sends the value to each user u_i.

(2) *Parameters Generation:* Each user u_i submits an odd prime p_i which is larger than $max(c_i^1, \cdots, c_i^m)$. Then, the platform determines the odd prime p which is larger than $max(\alpha_i G_j + 1, \{p_i \mid u_i \in \mathcal{U}\}, \{B_j \mid t_j \in \mathcal{T}\})$ and the degree of polynomial is $t(\leq n)$. The parameters including the odd prime p and degree t are released to all users.

(3) *Secret Sharing:* Each user u_i computes function I_i^j according to the received value $\alpha_i G_j$ and bid c_i^j as follows:

$$I_i^j = \begin{cases} \alpha_i G_j - c_i^j + 1, \text{if } \alpha_i G_j - c_i^j \geq 0 \\ 0, \qquad\qquad\qquad \text{if } \alpha_i G_j - c_i^j < 0. \end{cases}$$

Then, each user u_i generates a share set $[c_i^j]$ of secret c_i^j and a share set $[I_i^j]$ of secret I_i^j and transmits the shares $[c_i^j]_p^{i'}, [I_i^j]_p^{i'}$ to each other user $u_{i'}$.

Algorithm 2: Secret-Sharing-based Task Allocation protocol

```
    Input: $\mathcal{U}, \mathcal{S}, [c_i^j], \{\alpha_i G_j, B_j \mid i \in \mathcal{U}, j \in \mathcal{T}\}$
    Output: $[\mathcal{X}]$
      initialization: $[x_i^j] = [0], [y_i] = [0], [s_j] = [B_j]$
 1: for round 1 to $n$ do
 2:   for $i$ in candidate user set $\mathcal{U}$ do
 3:     for $j = 1$ to $m$ do
 4:       $[f_i^j] = [I_i^j] * Comp([c_i^j], [s_j])$
 5:   $[f_{max}] = Max([f_i^j] \mid 1 \le i \le n, 1 \le j \le m)$
 6:   users compute and reveal $Comp([f_{max}], 0)$.
 7:   if $Comp([f_{max}], 0) == 1$ then
 8:     break;
 9:   else
10:     for $i$ in candidate user set $\mathcal{U}$ do
11:       for $j = 1$ to $m$ do
12:         $[z] = Comp([f_{max}], [f_i^j]) * (1 - [y_i]) * Comp([c_i^j], [s_j])$
13:         $[x_i^j] = [z] + [x_i^j]$
14:         $[y_i] = [y_i] + [z]$
15:         $[s_j] = [s_j] - ([z] * [c_i^j])$
        each user $u_{i'}$ send $[y_i]_p^{i'}$ to user $u_i$ for restoration,
16:     if $y_i = 1$ then
17:       the user $u_i$ communicates with the platform, then the platform updates
          and broadcasts the candidate user set $\mathcal{U} = \mathcal{U} - \{u_i\}$ to all users.
18:     else
19:       continue;
20: return polynomial decision share $[\mathcal{X}]$
```

(4) *Task Allocation:* This step is also regarded as the process of selecting winning bids. Users jointly make the task allocation decision share $[\mathcal{X}] = \{[x_i^j] \mid \forall u_i \in \mathcal{U}, \forall t_j \in \mathcal{T}\}$ according to SSTA protocol.

Specially, Users compute jointly the function $[f_i^j], \forall u_i \in \mathcal{U}, \forall t_j \in \mathcal{T}$. If the bid c_i^j is larger than the budget B_j, SSTA determines the function $[f_i^j] = [0]$, otherwise $[f_i^j] = [I_i^j]$ in step 2–4. Step 5–8 indicates that the maximum value of the function is determined as f_{max} privately and the protocol will be terminated in advance if $f_{max} < 0$. From step 12–17, users determine the winning bid and make task allocation decisions. If the function f_i^j is largest and user u_i has not been assigned a task on the condition that the budget of t_j is adequate, users determine the decision share set $[x_i^j] = [1]$ and execution flag of the user is $[y_i] = [1]$. Then, the budget of task t_j should be updated and the user u_i should be removed from the candidate user set. Moreover, the decision share set $[\mathcal{X}]$ can be decided after at most n iterations. When the $[\mathcal{X}]$ is decided, each user $u_{i'}$ sends $\{[x_i^j]_p^{i'} \mid \forall t_j \in \mathcal{T}\}$ to user u_i. Then, the task allocation decision $\{x_i^j \mid \forall t_j \in \mathcal{T}\}$ can be derived by user u_i according to decision share $[x_i^j]$ based on Newton's interpolation theorem.

(5) *Task Submission:* If the task allocation decision $x_i^j = 1$, user u_i arrives the location of task t_j. Moreover, the user sends the sensing data of task t_j and the winning bid c_i^j to the platform. Note that the platform only obtains the winning bid and the allocated task of each user so that the locations of users can be protected.

(6) *Reward Users:* The platform pays rewards for each user u_i according to the winning bid c_i^j submitted by the user.

Theorem 3. *The SSTA protocol in the secure auction mechanism can protect location of each user from being revealed to other semi-honest mobile users and the platform, even if* $t-1$ *users are monitored at the same time by other attackers.*

Proof. In the step 1 and step 2 of our proposed mechanism, each user submits some random numbers which are independent of the user's location. Then, each user receives some bid polynomial shares uploaded by other users in step 3. As the coefficients of polynomials are random, users cannot infer bid information from received bid shares. Thus, the inputs of SSTA will not leak the bid information of each user. Since the multiplication operation and comparison operation have been proved to be secure [8,10], we just focus on proof of the computation security of SSTA protocol itself. Let $\mathcal{I} = \{i_1, i_2, \cdots, i_k\} \subset \{1, \cdots, n\}$ represent any $k = t-1$ users selected from mobile users $\mathcal{U}$. According to the SSTA protocol, we can obtain the received message of user i_h, denoted by $m_{i_h} = \{[f_i^j]_p^{i_h}, [z]_p^{i_h}, [x_i^j]_p^{i_h}, [y_i]_p^{i_h}, [s_j]_p^{i_h}, [f_{max}]_p^{i_h}\}$. Thus, the view of user i_h is $VIEW_{i_h} = (\{n, m, c_{i_h}^j, \alpha_i G_j, B_j\}, r, m_{i_h})$. Then, the view of user set $\mathcal{I}$ can be denoted as $VIEW_{\mathcal{I}} = \{\mathcal{I}, VIEW_{i_1}, \cdots, VIEW_{i_k}\}$. In $VIEW_{\mathcal{I}}$, the number of shares of each secret is no larger than the degree t, so that information of these secrets cannot revealed by these shares according to the secret sharing scheme. Moreover, the platform obtains only some flags 0 or 1 independent of locations of users to determine whether the protocol can be terminated in advance. Thus, Eq. (6) holds and the whole SSTA protocol is secure.

Theorem 4. *The SSTA protocol can also produce* $(1+\gamma)$*-approximation solution, where* $\gamma = max\{\frac{B_j}{c_i^j} \mid t_j \in \mathcal{T}, u_i \in \mathcal{U}\}$.

Proof. Originally, the SSTA protocol applies secret sharing scheme based on the GBTA algorithm to protect sensitive information of users. By analysis of GBTA and SSTA, we can find that both of them select a bid which can most improve profit of the platform as the winning bid in each iteration. Thus, SSTA protocol can obtain the same task allocation decisions as GBTA, and then the Theorem 4 is proved.

5 Evaluation

In this section, we first introduce compared algorithms and simulation settings, and then the SSTA protocol is evaluated in two perspectives, i,e., task allocation performance measured by total profit of the platform and privacy protection level evaluated by location privacy leakage rate.

5.1 Algorithms for Comparison

Although many existing researches have focused on task allocation in mobile crowdsensing, the various crowdsensing models and problems in these works are not exactly same as ours. Generally, greedy strategies are often adopted to deal with NP-hard task allocation problems. In order to measure the validity of task allocation results of GBTA algorithm and SSTA protocol, we design two task allocation algorithms in the following based on the basic idea of algorithms proposed by [13,15] for comparison, which can be applied to our work.

The first comparison method is Minimum Bid First (MBF) task allocation algorithm, in which the platform selects the smallest bid in each iteration for task allocation. Another approach is Maximum Profit per Cost First (MPCF) algorithm, where the bid with the largest platform profit obtained by unit cost is decided as a winning bid in each round of execution, i,e., $max\{\frac{\alpha_i G_j - c_i^j}{c_i^j} \mid u_i \in \mathcal{U}, t_j \in \mathcal{T}\}$. In addition, we compare the task allocation algorithm without privacy protection GBTA and SSTA protocol to analyse the impact of secret-sharing-based privacy protection approach applied in SSTA on the total profit of the platform.

5.2 Simulation Settings

In our simulations, we conduct the experiments on geographic areas which are divided into 50∗50 grids. The basic earning of task G_j is constrained in the range $[20, 100]$. To obtain bids by mobile users, four basic monotonically increasing functions are considered as follows:

$$c_i^j = f_i(d_i^j) = \begin{cases} a_i * d_i^j & \text{if } u_i \text{ selects linear function} \\ a_i * {d_i^j}^2 & \text{if } u_i \text{ selects square function} \\ a_i * \sqrt{d_i^j} & \text{if } u_i \text{ selects square root function} \\ a_i * \log(1 + d_i^j) & \text{if } u_i \text{ selects logarithmic function} \end{cases} \quad (15)$$

where $a_i \in (0, 20]$.

Table 1. Parameter Settings

Parameter name	Values
Number of users n	$100, 200, \mathbf{300}, 400, 500$
Number of tasks m	$50, \mathbf{100}, 150, 200, 250$
Range of task budget B	$[50, 60], [50, 70], \mathbf{[50, 80]}, [50, 90], [50, 100]$
Mean of user credit α	$0.5, 0.6, \mathbf{0.7}, 0.8, 0.9$

Moreover, we consider four variable parameters including the number of users n, the number of tasks m, the range of task budget B and the mean of user credit

α. The values of these parameters are shown in Table 1, in which default values of the parameters are highlighted in bold. When we change one of the variable parameters, the other parameters will remain as the default values.

5.3 Evaluation on Task Allocation Performance

To evaluate the influence of the number of users and the number of tasks on task allocation performance, we compare the total profit of the platform obtained by MBF, MPCF, GBTA and SSTA. The results are depicted as Fig. 4 and Fig. 5.

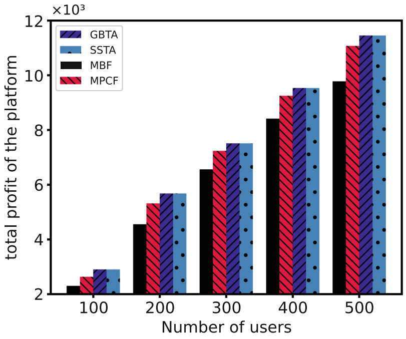

Fig. 4. Total profit of the platform v.s. number of users.

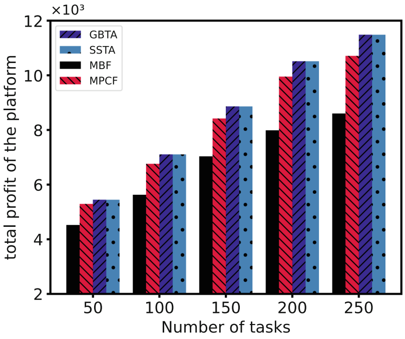

Fig. 5. Total profit of the platform v.s. number of tasks.

On the one hand, we can find that our approach GBTA and SSTA can achieve more profit than MBF and MPCF when the number of users participating sensing tasks increases from 100 to 500 or the number of tasks increases from 50 to 250. This is because MBF only takes the cost of the platform into consideration but ignores the benefits obtained by the platform. Moreover, only if a winning bid is less than 1, the profit obtained by MPCF will be greater than that of GBTA and SSTA. On the other hand, we can observe that the profit of the platform increases significantly as the number of users and tasks increases. Additionally, the results obtained by GBTA are consistent with those obtained by SSTA due to the same basic idea which is discussed in Theorem 4.

In addition, we also report experimental results of profit of the platform with different range of task budget and various mean of user credit in Fig. 6 and Fig. 7, respectively. With the changes of the two parameters B and α, we can find that the results of SSTA and GBTA are superior to the comparison methods MBF and MPCF. Moreover, we can observe that the profit of the platform obtained by our approach improves in either situation. In particular, when the range of task budget extends, the profit obtained by MPCF, GBTA, SSTA slightly but steadily increases. This is because the task allocation decisions change only when the budget of a task is insufficient.

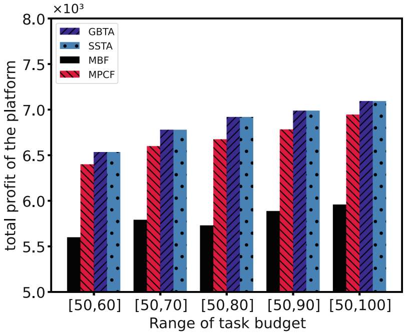

Fig. 6. Profit of the platform v.s. range of task budget.

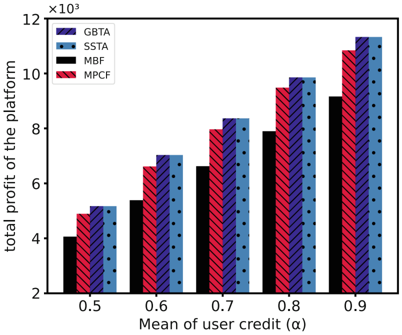

Fig. 7. Profit of the platform v.s. mean of user credit.

5.4 Evaluation on Privacy Protection Level

To evaluate the privacy protection level of our proposed auction mechanism, the location privacy leakage rate (i,e., the percentage of users who let out their positions) is considered. Here, we will not evaluate whether users participating in multi-party security computing can infer the locations of other users or not during the execution of SSTA since the security has been proved in Theorem 3. Specifically, when the privacy protection method is not adopted, the platform infers location of each user based on the original bids for all tasks of the user according to attack model mentioned in Sect. 3.3. Moreover, the platform can only obtain the results of the auction including the winning bid and an assigned task of a user in the case of applying our mechanism so that the platform can only infer the location of a user by blindly assuming that the location of the assigned task is the user's location.

As shown as Fig. 8, we can observe that the privacy leakage rate with our approach remains around 0.02 while the locations of 98% of users are exposed to the platform without any protection method as the number of users increases. The essence of stability is that a constant number of bids submitted by a user does not allow the platform to extract more location information during the auction without protection. Naturally, the increase of users may lead to an increase in the number of users consistent with the location of the assigned task. However, the privacy leakage rate keeps stable by adopting our effective mechanism in the crowdsensing system.

In Fig. 9, although there are only 50 tasks in the region of crowdsensing system, the location privacy of users is revealed with probability 0.963. Moreover, the privacy leakage rate is closer to 1 which means almost all locations of users can be inferred by the platform as the number of tasks increases. This is because the platform may deduce the location of a user according to more bid information, in which the number of bids is consistent with the number of tasks. We also report the privacy leakage rate for our auction mechanism with protection

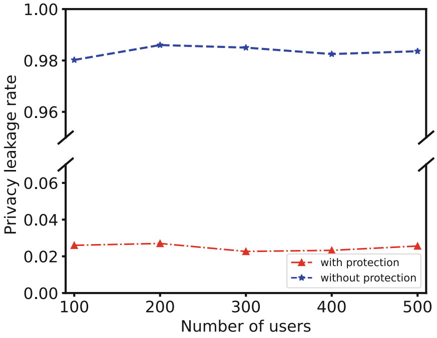

Fig. 8. Profit of the platform v.s. number of users.

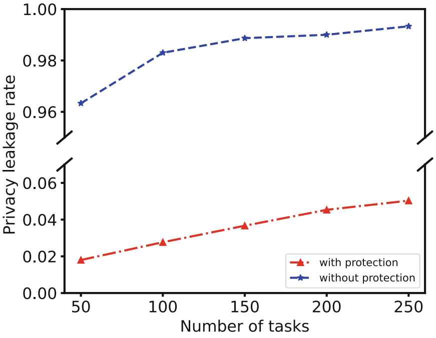

Fig. 9. Profit of the platform v.s. number of tasks.

in the figure, and we can find that the probability of location privacy disclosure increases slowly and monotonously as the number of tasks increases. The reason is that an increase in the number of tasks makes it more likely that users and tasks are in the same location. However, when there are 250 tasks, the privacy leakage rate descends about 95% by adopting the proposed auction.

6 Conclusion

In this paper, we consider the problem of task allocation with location privacy protection in an auction-based crowdsensing system without any trusted third party. We first formalize the problem as a NP-hard problem and propose GBTA algorithm with $(1 + \gamma)$-approximation solution for task allocation without the security constraint. However, the bid information of a user is positively and strongly correlated with the distance from the user to tasks, which may lead to the location leakage of the user in the crowdsensing based on the attack model. Thus, we next design a secure auction mechanism by applying SSTA protocol to assign tasks privately which can achieve the same results as GBTA. It is proved that the security of the auction mechanism is guaranteed. Finally, the simulation results show that our approach has excellent performance in task allocation and it can protect location privacy of users effectively.

Acknowledgements. This work is supported by Grant No. 20CG47 from Shanghai Chen Guang Program and Grant No. 22ZR1423700 from Shanghai Committee of Science and Technology. This work is also supported by the Shanghai Foundation for Development of Science and Technology, China (No. 21142202400). We also appreciate the High Performance Computing Center of Shanghai University and Shanghai Engineering Research Center of Intelligent Computing System for providing the computing resources.

References

1. Ganti, R.K., Ye, F., Lei, H.: Mobile crowdsensing: current state and future challenges. IEEE Commun. Mag. **49**(11), 32–39 (2011)
2. Gao, J., Fu, S., Luo, Y., Xie, T.: Location privacy-preserving truth discovery in mobile crowd sensing. In: 2020 29th International Conference on Computer Communications and Networks (ICCCN), pp. 1–9. IEEE (2020)
3. Goldreich, O.: Foundations of Cryptography: volume 2, Basic Applications. Cambridge University Press, Cambridge (2009)
4. Huang, W., Lei, X., Huang, H.: PTA-SC: privacy-preserving task allocation for spatial crowdsourcing. In: 2021 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–7. IEEE (2021)
5. Li, L., Zhang, X., Hou, R., Yue, H., Li, H., Pan, M.: Participant recruitment for coverage-aware mobile crowdsensing with location differential privacy. In: 2019 IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE (2019)
6. Li, M., Li, Y., Fang, L.: ELPPS: an enhanced location privacy preserving scheme in mobile crowd-sensing network based on edge computing. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 475–482. IEEE (2020)
7. Liu, T., Zhu, Y., Wen, T., Yu, J.: Location privacy-preserving method for auction-based incentive mechanisms in mobile crowd sensing. Comput. J. **61**(6), 937–948 (2018)
8. Lory, P.: Secure distributed multiplication of two polynomially shared values: enhancing the efficiency of the protocol. In: 2009 Third International Conference on Emerging Security Information, Systems and Technologies, pp. 286–291. IEEE (2009)
9. Mun, M., et al.: Peir, the personal environmental impact report, as a platform for participatory sensing systems research. In: Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services, pp. 55–68 (2009)
10. Nishide, T., Ohta, K.: Multiparty computation for interval, equality, and comparison without bit-decomposition protocol. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 343–360. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-71677-8_23
11. Pryss, R., Reichert, M., Herrmann, J., Langguth, B., Schlee, W.: Mobile crowd sensing in clinical and psychological trials-a case study. In: 2015 IEEE 28th International Symposium on Computer-Based Medical Systems, pp. 23–24. IEEE (2015)
12. Qian, Y., Ma, Y., Chen, J., Wu, D., Tian, D., Hwang, K.: Optimal location privacy preserving and service quality guaranteed task allocation in vehicle-based crowdsensing networks. IEEE Trans. Intell. Transp. Syst. **22**(7), 4367–4375 (2021)
13. Song, T., et al.: Trichromatic online matching in real-time spatial crowdsourcing. In: 2017 IEEE 33rd International Conference on Data Engineering (ICDE), pp. 1009–1020. IEEE (2017)
14. Thiagarajan, A., et al.: Vtrack: accurate, energy-aware road traffic delay estimation using mobile phones. In: Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems, pp. 85–98 (2009)
15. To, H., Ghinita, G., Shahabi, C.: A framework for protecting worker location privacy in spatial crowdsourcing. Proc. VLDB Endow. **7**(10), 919–930 (2014)
16. Wan, J., Liu, J., Shao, Z., Vasilakos, A.V., Imran, M., Zhou, K.: Mobile crowd sensing for traffic prediction in internet of vehicles. Sensors **16**(1), 88 (2016)

17. Wang, L., Qin, G., Yang, D., Han, X., Ma, X.: Geographic differential privacy for mobile crowd coverage maximization. In: Thirty-Second AAAI Conference on Artificial Intelligence (2018)
18. Wei, J., Lin, Y., Yao, X., Zhang, J.: Differential privacy-based location protection in spatial crowdsourcing. IEEE Trans. Serv. Comput. **15**(1), 45–58 (2022). https://doi.org/10.1109/TSC.2019.2920643
19. Wen, Y., et al.: Quality-driven auction-based incentive mechanism for mobile crowd sensing. IEEE Trans. Veh. Technol. **64**(9), 4203–4214 (2014)
20. Xiao, M., et al.: SRA: secure reverse auction for task assignment in spatial crowdsourcing. IEEE Trans. Knowl. Data Eng. **32**(4), 782–796 (2019)
21. Xiao, M., Wu, J., Zhang, S., Yu, J.: Secret-sharing-based secure user recruitment protocol for mobile crowdsensing. In: IEEE INFOCOM 2017-IEEE Conference on Computer Communications, pp. 1–9. IEEE (2017)
22. Xu, Q., Su, Z., Dai, M., Yu, S.: APIs: privacy-preserving incentive for sensing task allocation in cloud and edge-cooperation mobile internet of things with SDN. IEEE Internet Things J. **7**(7), 5892–5905 (2019)
23. Yang, Q., Chen, Y., Guizani, M., Lee, G.M.: Spatiotemporal location differential privacy for sparse mobile crowdsensing. In: 2021 International Wireless Communications and Mobile Computing (IWCMC), pp. 1734–1741 (2021). https://doi.org/10.1109/IWCMC51323.2021.9498951
24. Zhang, Q., Wen, Y., Tian, X., Gan, X., Wang, X.: Incentivize crowd labeling under budget constraint. In: 2015 IEEE Conference on Computer Communications (INFOCOM), pp. 2812–2820. IEEE (2015)