Scalable Privacy-Preserving Participant Selection in Mobile Crowd Sensing

Ting Li* Taheo Jung† Hanshang Li* Lijuan Cao* Weichao Wang* Xiang-Yang Li‡† Yu Wang*
*College of Computing and Informatics, University of North Carolina at Charlotte, Charlotte, NC 28223, USA
†Department of Computer Science, Illinois Institute of Technology, Chicago, IL 60616, USA
‡School of Computer Science, University of Science and Technology of China, Hefei, Anhui, China

***Abstract*—Auction based participant selection has been widely used for mobile crowd sensing (MCS) to achieve user incentive and assignment optimization. However, mobile crowd sensing problems solved with auction-based approaches usually involve participants' privacy concerns because a participant's bids may contain her private information (such as location visiting patterns), and disclosure participants' bids may disclose their private information as well. In this paper, we study how to protect such bid privacy in a temporally and spatially dynamic MCS system. We assume that both sensing tasks and mobile participants have dynamic characteristics over spatial and temporal domains. Following the classical VCG auction, we carefully design a scalable grouping based privacy-preserving participant selection scheme, which leverages Lagrange polynomial interpolation to perturb participants' bids within groups. The proposed solution does not affect the operation of current MCS platform. Both theoretical analysis and real-life tracing data simulations verify the efficiency and security of the proposed solution.**

I. Introduction

The proliferation of mobile devices equipped with built-in sensors enables a new sensing paradigm, mobile crowd sensing (MCS), which has been widely used in numerous applications [1]. Compared with traditional static sensing, MCS leverages existing sensing and mobile communication infrastructures to provide unprecedented spatiotemporal coverage. Meanwhile, it brings many new challenges in the system design. Participant selection is one of them, where appropriate participants are selected to perform certain sensing tasks [2]–[11].

Auction based participant selection is a common solution, where participants submit their bids (reflecting their sensing costs) over different sensing tasks to the MCS system and the platform selects the winners (usually with the lowest bids) among all the bidders to perform the tasks. Fig. 1 illustrates the architecture of such a MCS system. Here we assume that various sensing tasks may request sensing data at different locations and time. Further, different mobile participants may have their own mobility patterns, as a result, they perform these sensing tasks at various costs. The optimal goal is to pick the appropriate participants who can perform the tasks with the minimum cost. In addition, to guarantee the truthfulness of participants on their bids, a Vickrey-Clarke-Groves(VCG)-based auction [12] or other game theoretical approaches [8], [9] can be applied.

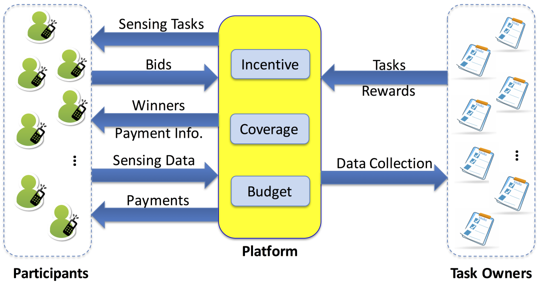


Fig. 1. **MCS System:** the platform distributes sensing tasks to participants, collects their bids, decides the winning bids (i.e., selecting participants for each task), collects sensing data, and makes payment to the participants.

Existing auction-based solutions solved the participant selection and incentive issues, but we observed that there exists user privacy concerns on the other hand. In most cases, bids are related to participants' contexts (*e.g.,* location), and such information may leads to privacy breach (*e.g.,* a participant with a higher bid in certain MCS problems indicate closer proximity of his/her location to the place where crowdsensing is performed). Recently, various privacy-preserving schemes [13]–[21] have been proposed for the protection of the participants' privacy, however none of them consider the privacy leakage from the bid values. In this paper, we would like to complement existing works by protecting the bid values in order to achieve better anonymity and privacy protection.

Notice that the platform in an auction-based MCS system (Fig. 1) has the bid information and can easily conjecture the bid patterns of each participant through a long time learning process because the bids are temporally and spatially correlated in MCS auctions. For a more concrete example, the platform may know particular participant route if that participant often bids on some particular location and time. Furthermore, the bidding value (i.e., the private sensing cost value) may also reflect certain level of privacy information, such as the likeness of visiting that place or the distance to the task location. Therefore, exposing the bid information to the platform brings privacy concerns of users and may hurt the users' enthusiasm to participate. Further, this may result in insufficient participants for the completeness of sensing tasks. Therefore, it is a critical issue for the MCS system. In this paper, we focus on a new solution to protect the bid privacy of participants while still guarantee the truthfulness property of auction and the efficient operation of the MCS system. For potential participants, bid privacy is preserved unless they win the competition and perform the assigned sensing tasks.

Achieving the bid privacy in MCS problems involves multiple challenges. First, we focus on a temporally and spatially dynamic MCS system, where both sensing tasks and mobile participants have dynamic characteristics in both spatial and temporal domains. This makes bids in the auctions temporally and spatially correlated, making it hard to protect end-to-end bid privacy over the long time. Second, the users in the bidding system are dynamic. Mobile devices can join and leave, thus the bidder pool keeps changing over different tasks. This makes most of the existing privacy-preserving data aggregation schemes ([22]–[24]) unfitting since one suite of keys need to be distributed to one specific group of users. Third, we aim to achieve accurate sensing results. This is a critical issue as noisy bid information may lead to unnecessary overpayment and/or even the failure in completing the sensing task. As a result, traditional perturbation-based approaches such as Laplacian mechanism with differential privacy [25] is hardly applicable. Fourth, we target at protecting bid privacy without a trusted third party (TTP) participating in every round of auctions, considering that such a party capable of coordinating every single auction hardly exists. Finally, we hope that the proposed solution is built on the existing MCS system and does not affect the operation of current platform.

We assumes that both the participants and the platform are semi-honest (i.e., they follow the protocol but try to infer sensitive information). Further, we introduce one or multiple semi-honest third parties (TPs) to perform grouping of participants (Section III). By leveraging Lagrange polynomial interpolation (LPI) and key values generated by a key generator (KG), bid information is protected during the group bidding and the final platform bidding (Section IV). Here, KG is only in charge of key generation and does not participate in the auction and crowd sensing process, and its participation is minimized. Notably, our theoretical analysis (Section V) shows that no statistical information about bids is disclosed from the ciphers generated by our solution (semantic security), implying that even the temporally and spatially correlated bids can be protected by our approach. Experiments with two real-life datasets (Section VI) also confirm that the method is efficient compared with other existing methods.

II. Related Work

Participant Selection in Mobile Crowdsensing: Due to the large number of participants and the diverse sensing tasks in mobile crowdsensing, the selection of participants for different tasks (i.e. task assignment) becomes a challenging task. On one hand, assigning more participants for certain task can lead to better quality of the sensed data. On the other hand, MCS have to pay more rewards to the participants to cover their sensing cost. Recently, there are several studies on participant selection in MCS with various optimization goals such as coverage maximization [2]–[4], energy efficiency [5]–[7], user incentive and truthfulness [8], [9]. In this paper, we also consider the participant selection problem, but focus on a different aspect: bidding privacy. We only consider a simple bidding scenario where the MCS platform aims to minimize the payment by choosing the lowest bid among all bids.

Privacy Protection in Mobile Crowdsensing: To protect the participants' privacy in mobile crowd sensing or participatory sensing, several privacy preserving schema have been proposed using different techniques, such as data transform language [13], data aggregation [14] , location obfuscation [15], cloaking [16], k-anonymity [17], pseudonym [18] and adding noise [19]. These solutions usually introduce additional entities (registration authority / trusted third part) [13], [17], [18] or an aggregation server [14], [15] to achieve the protection of the sensing data privacy, participants' anonymity or their location privacy. Note that TTP-free method in [18] uses pseudonym and bling signature to protect user privacy, but its encryption operations may bring a burden of cost. Recently, Jin *et al.* [26] also jointly consider both participants' privacy from aggregated data and incentive mechanisms in MCS. In contrast to all of these existing solutions, this paper focuses on protecting the participants' bid privacy during the bidding process for participant selection. The only similar work is [27], where bid privacy is considered in an aggregated MCS system. However, it defines the bid privacy with differential privacy over the aggregated sensing data (labels) and all sensing tasks are binary classification (labelling) tasks. Instead, we consider a more general and direct model where sensing tasks have sensing requests on both temporal and spacial domains and the privacy is defined on the bids from participants.

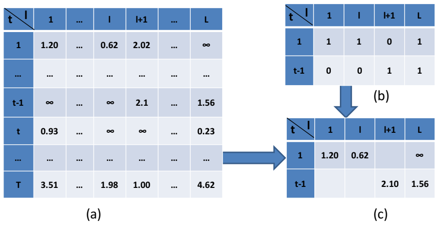
Secure VCG Auction: In our work, Vickrey-Clarke-Groves(VCG) auction [12] is leveraged as a building block, and we propose a novel privacy-preserving design of VCG auction in order to protect users' bid privacy. Related research exists in the literature, who targets at protecting bid privacy in the VCG auction as this paper does. However, existing works have common limitations due to the building blocks they employed to realize secure VCG auctions, and this made them less attractive than our approaches when implemented and deployed in the real-life applications.

Naor *et al.* [28] proposed how to design general auctions with mechanism design without revealing private bid information by leveraging the secure multi-party computation (MPC) with garbled circuits [29]. However, it is shown that auction mechanisms based on secure multi-party computation is inefficient because the complexity inherently increases exponentially with the number of goods to be auctioned and the bit-length of the bid, and the actual overhead is large as well as due to the large constant factors [30]. Besides, an auction issuer, who is a party that is assumed not to collude with the auctioneer, needs to engage every time an auction is run.

Huang *et al.* [31] and Lipmaa *et al.* [32] proposed approaches that are both based on homomorphic encryption , but they require a third party at every auctioning as well. Larson *et al.* [33] proposed to use the homomorphism in homomorphic encryption to enable secure VCG auction without revealing individual bids. However, they introduce a group key among the group of users in extra, and this limits the application in real world where users may come and go because group key sharing must occur for every new group, and this will not be practical in many cases as users cannot communicate with each other during the auction.

A series of works have been proposed by different researchers to realize privacy-preserving VCG auctions [34]–[39]. All of these works are based on the homomorphic encryption, and they do not require a third party engagement as in our approach. However, they achieved this by generating one cipher per possible bid value. That is, if the bid length is b bits and the size of bid space is 2^b, the computation/communication/storage complexities are inherently exponential to the input size.

Unlike all aforementioned existing works, our solution does



t \ l	1	...	l	l+1	...	L
1	1.20	...	0.62	2.02	...	∞
...	...	...	...	...	...	...
t-1	∞	...	∞	2.1	...	1.56
t	0.93	...	∞	∞	...	0.23
...	...	...	...	...	...	...
T	3.51	...	1.98	1.00	...	4.62

(a)

t \ l	1	l	l+1	L
1	1	1	0	1
t-1	0	0	1	1

(b)

t \ l	1	l	l+1	L
1	1.20	0.62		∞
t-1			2.10	1.56

(c)

Fig. 2. **Spatiotemporal Matrixes:** (a) private cost matrix C_i of participant u_i; (b) binary task matrix S; and (c) bidding matrix B_i generated from u_i, in which the bid value may not be equal to the real cost value.

not require third-party[1] engagement in every auction running, and our solution scales well with the number of goods, number of bidders, and the bit-length of the bid values.

III. Problem Definition and Security Models

A. *Participation Selection Problem and VCG Mechanism*

In general, a MCS system includes three main components, as shown in Fig. 1: a large number of *mobile participants* who can perform sensing tasks and contribute sensing data, a set of *task owners* who generate various sensing tasks and are willing to pay for sensing data (acting as data consumers), and the *platform* who plays a vital role in the MCS system and acts as the MCS marketplace to connect the mobile participants with the task owners. The participation selection aims to select a set of participants who could complete the sensing tasks but with the minimum payment. This could be a challenging task because of large number of participants and various requirements of the tasks.

In our model, there are n mobile participants $U = \{u_1, u_2, \cdots, u_n\}$. Each participant u_i keeps a dynamic spatiotemporal matrix about her real sensing cost $C_i = \{c_i(t,l)\}$ privately, as shown in Fig. 2(a), where $c_i(t,l)$ is the real sensing cost for u_i to obtain sensing value at location l at time t. The real sensing cost information is sensitive since it may reveal the visiting pattern of this participant. We assume that we have finite number of l and t, i.e., $t \in \{t_1, t_2, \cdots, t_T\}$ and $l \in \{l_1, l_2, \cdots, l_L\}$.

Suppose there are m sensing tasks $S = \{s_1, s_2, \cdots, s_m\}$ and each of them has a strict spatiotemporal coverage requirement, s.t., task s_j could be described as a binary spatiotemporal matrix $S_j = \{s_j(t,l)\}$, where $s_j(t,l) = 1$ represents that s_j request data at location l during time slot t and $s(t,l) = 0$ otherwise. Since we assume that each requested cell within the binary spatiotemporal matrix can be fulfilled by one selected participant within the same requested cell, we take a union of all sensing tasks into a single binary spatiotemporal matrix $S = \{s(t,l) = \oplus_{j=1}^{m} s_j(t,l)\}$, as shown in Fig. 2(b), where $s(t,l) = 1$ represents that there is at least one task requesting the data from l at t. Then, the task assignment can be treated as assigning a single participant to each cell with $s(t,l) = 1$.

Each participant u_i, if interested, can submit a bidding matrix $B_i = \{b_i(t,l)\}$, as shown in Fig. 2(c), to the platform based on her real cost. Note that $b_i(t,l)$ may be different from $c_i(t,l)$. After receiving bids from all participants, the platform will make a decision about winning bids for tasks at $s(t,l) = 1$ based on certain strategy and pay the corresponding rewards $p(t,l)$ to the winners of these tasks. We assume that the mobile participants can finish the tasks assigned to them as long as they participate and win the bid competition. In other words, the completeness of tasks is guaranteed if enough bidding participants can cover the task spatiotemporal matrix.

Based on bidding matrices $\{B_i\}$ provided by participants U for task set S, the mission of the platform is to efficiently find the optimal set of participants for tasks such that the total payment (i.e., $P = \sum_{t,l} p(t,l)$) is minimum. At the same time, the platform wants the selection mechanism to be truthful, i.e., the participant bids at its real sensing cost for each cell. To achieve this goal, we adopt the classical Vickrey-Clarke-Groves (VCG) auction [40]–[42] in our participation selection problem. Each participant has no knowledge about others' bids during the auction since the bid matrix is private. The lowest bidder wins but the payment is equal to the second lowest bid, which gives the participants an incentive to bid at their true cost value in this optimal strategy. The whole VCG auction process includes the winning bid decision and the critical payment calculation.

Definition 1: ***Winning Bid and Critical Payment.*** The winning bid is the lowest bid among all bids submitted by participants within U for each cell $s(t,l) = 1$, which could be defined as follows:

$$b(t,l) = \min_{u_i \in U_{(t,l)}} b_i(t,l) \ \mathit{and} \ w(t,l) = \arg\min_{u_i \in U_{(t,l)}} b_i(t,l),$$

where $w(t,l)$ is the single winner for this requested cell (if there is a tie, an arbitrary one can be selected as the winner) and $U_{(t,l)}$ are the set of participants who submit their bids for task cell (t,l). The payment $p(t,l)$ for winner $w(t,l)$ is defined as the lowest bid among all the bids except the winner's bid. i.e.,

$$p(t,l) = \min_{u_i \neq w(t,l)} b_i(t,l)$$

By applying the VCG mechanism, it is easy to prove the bid truthfulness, i.e., the participant will maximize its utility when it bids truthfully at its real sensing cost (i.e., $b_i(t,l) = c_i(t,l)$). In addition, the VCG mechanism minimizes the total payment for the participant selection. Both the winning bid and critical payment can be decided very efficiently with a simple sorting. Notice that it is possible for a task cell, there are bid ties. This will not affect the effectiveness of VCG mechanism.

B. *Adversary Model and Assumptions*

Recall that we aim to design a MCS system with grouping and security techniques to protect the bid privacy of participants while still guarantee the truthfulness property of auction and the operation of MCS system. We assume that task owners, the platform, and the participants in the system may all become semi-honest adversaries. A semi-honest adversary follows the protocol specification, however she may try to infer sensitive information from the communication strings generated by the protocol. More specifically, the task owners as well as the platform may try to infer true bids of the participants, and the participants may try to infer other participants' true bids as well as owing to the bidding competition. Further, in order

[1] Note that the third party (TP) we defined in next section is the auctioneer in the group auction. It is called third party since it is a new entity added between the platform and the participants.

to bootstrap the mobile crowdsensing, we introduce a semi-honest third party (TP) and the only single trusted party in our system – key generator (KG). TP is used for grouping bids, while KG is in charge of key generation only and it does not participate in the auction and crowd sensing process.

Notably, we assume that the adversaries may have certain background knowledge about the participants' true bids, and we also assume that they are capable of the cryptanalysis. Such adversaries are quite powerful in the attack, and therefore the protection scheme must be strong enough such that no side information is leaked from the communication strings.

C. Security Model

The security of our system is defined by following standard security game between the adversary and the challenger.

Secure Bidding Game:

- Setup: two disjoint time domains are chosen: T_1 for phase 1, T_c for challenge phase, and T_2 for phase 2.
- Init: The adversary declares that one role in the MCS system will be under his control (*i.e.,* the platform or a participant). The challenger controls the remaining entities in the MCS system. Subsequently, both of them engage themselves in the exchange of public/private parameters according to the protocol specification.
- Phase 1 in T_1: The adversary receives all the communication strings generated during multiple auctions in T_1. The only constraint is that the auctions occur in the time domain T_1.
- Challenge in T_c: The adversary declares any victim participant, and he declares two distinct challenge bids b_0, b_1. The challenger then flips a fair binary coin $\mu = \{0, 1\}$ and generates the disguised bid of b_μ.
- Phase 2 in T_2: Phase 1 is repeated adaptively, but the time window should be chosen from T_2.
- Guess: The adversary gives a guess μ' on μ.

The advantage of an adversary $\mathcal{A}$ in this game is defined as $\mathsf{adv}_{\mathcal{A}}^{MCS} = \left|\mathbf{Pr}[\mu' = \mu] - \frac{1}{2}\right|$.

Definition 2: An MCS protocol is indistinguishable against chosen-plaintext attack (IND-CPA) if all polynomial time adversaries' advantages in the above game are of a negligible function *w.r.t.* of the security parameter λ when T_1, T_c, T_2 are all pair-wise disjoint.

Intuitively, our security definition indicates that the followings hold in a MCS protocol with IND-CPA.

- Even if adversaries have some knowledge on the distribution of victims' bids, they are still not able to infer any information about the bids from the communication strings.
- Even if temporal or spatial correlation exists in victims' bids, adversaries are not able to link disguised bids whose true bids are correlated to each other.
- Adversaries are not able to learn any information about the victim's private key if they do not know the exact value of the victim's bid.

In other words, the bid disguising is semantically secure against polynomially bounded adversaries and therefore no statistical information about the bids is disclosed.

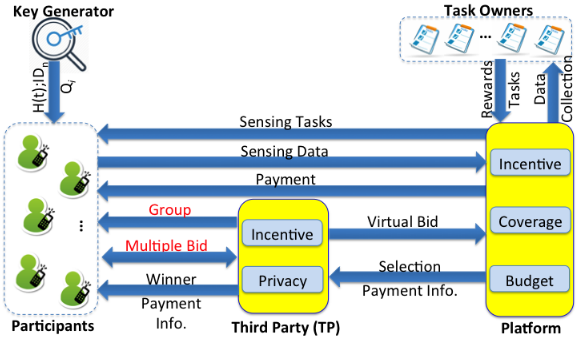


Fig. 3. **Privacy-preserving participant selection:** each new participant receives her ID, public parameter $H(t)$ and retrieves a set of polynomial values for all requested cells in spatiotemporal matrix S with her ID; task owners give out the tasks and rewards to platform; TP is in charge of grouping and privacy-preserving auction; the platform selects final participants to complete the tasks and make the payments.

IV. Privacy-Preserving Participation Selection

In this section, we present our design of privacy-preserving participation selection, which leverages combinatorial group strategy to find the minimum bid for each task cell in the group while the bid information of every participant is unknown by anyone else except for the participant himself. To preserve privacy, two additional parts, key generator (KG) and third party (TP), are added to the original MCS framework, as shown in Fig. 3. The Key generator randomly generates and distributes a series of polynomials outcomes and IDs for all enrolled participants. The third party is the data aggregator, and it calculates the minimum bid among all the participants without the knowledge of each individual bid value. The introducing of KG and TP does not affect the operation of MCS platform. In the view of the platform, TP and KG together are agents of virtual participants (groups).

A. Preliminaries

We use the following theories to obtain the minimum bid and the critical payment (second lowest bid) without leaking the bid privacy of participants to any of the other parts, including TP. Further, the calculation could be verified by using fixed point representation.

- Minimum Approximation: For a large integer number R and the upper bound Υ, known by the whole system, the approximation of the minimum number among all the $x_i, i \in [1, I]$ could be obtained by:

$$\Upsilon - \sqrt[R]{\sum (\Upsilon - x_i)^R} \approx \min (x_1 \dots x_i \dots x_I).$$

- Lagrange Polynomial Interpolation (LPI): Given a polynomial $Q^j(x)$ with a highest degree j no more than $W-1$ (i.e., $j \le (W-1)$) who passes through the W points $(x_1, q^j(x_1)), (x_2, q^j(x_2)), \dots (x_W, q^j(x_W))$, any other point $(x, q^j(x))$ can be given by

$$q^j(x) = \sum_{w=1}^{W} \left(q^j(x_w) \prod_{\substack{v=1 \\ v \neq w}}^{W} \frac{x - x_v}{x_w - x_v} \right).$$

If $Q^j(x)$ is a polynomial where $q^j(0) = 0$, then the right part of equation is equal to 0, which is

$$\sum_{w=1}^{W}\left(q^j(x_w)\prod_{\substack{v=1\\v\neq w}}^{W}\frac{0-x_v}{x_w-x_v}\right)=0.$$

- Fixed Point Representation: We can transfer one type of fixed point data type with scaling factor A to another data type with scaling factor B by multiplying A and dividing B. We could use the fixed point representation to represent real numbers so that the key in our proposed strategy could be trivially verified as shown in Section IV-D.

B. Sketch of Basic Idea

Our basic idea is inspired by [43]. We let participants form groups first and then the privacy preserving auction is performed within each group. Then the winning bids within each group will be disguised as the virtual participants and submitted to the platform for the final participation selection. VCG auction is performed during both the group bid session and the final participation selection process. The challenges are: (1) how to perform privacy preserving auction within the groups to prevent from leaking the participants' bid information to any party, including TP, and (2) how to make these operations efficient without causing much overhead. Fig. 3 shows the structure of our design.

After participants receive the requirements of the sensing task, they will form several groups (with their own group size requirements, which reflects their privacy level). The groups can be formed by either the participants themselves or by TP. Further, the groups may have different sizes, and a larger group size usually leads to better privacy. For simplicity, hereafter, we consider the group is formulated by TP and the size is a standard system parameter. Each participant in a group uses her group member ID and her related polynomial value to disguise the original bid information. With the feature of LPI pass through origin and the minimum approximation, TP could obtain the minimum bid within each group. The second lowest bid in the group could also be obtained in the same way after excluding the winner. These two bids in each group will be reported to the platform as virtual bids from regular participants. Then the platform uses the VCG method to select the winner and calculates her payment.

Except for the bid winner, all the bid information could be well-protected by our strategy with light overhead and efficient computation. Also, the bid truthfulness could be protected by VCG. Note that this method does not affect the operation of current VCG-based MCS platform. The virtual bids from groups can be treated as regular participants of the platform. Our method can support hybrid participants (both virtual and regular participants) at the platform and also multiple TPs (as different agents) for grouping. In the next section, we will describe the design details of the proposed system.

C. Detailed Design of Privacy-Preserving Group Bidding

For the simplicity, we omit all the modulo operations, however all numbers appearing in our mechanisms are within a finite field $\mathbb{Z}/p\mathbb{Z}$ where p is a safe prime number of bit length λ, and λ is also denoted as the *security parameter*. We also focus on the a single requested cell (t,l) where $s(t,l)=1$.

Initialization: KG generates a set of polynomials $Q=\{Q(t,l)\}$, where $Q(t,l)=\{q^2_{(t,l)}(x)\dots q^{\kappa}_{(t,l)}(x)\dots q^{K-1}_{(t,l)}(x)\}$, for the requested cell (t,l) in the spatiotemporal matrix securely, in which all constants are equal to 0. Here K is the upper bound of the group size. The polynomials with same degree κ are distinct from each requested cell. For the consideration of security, the polynomials need to be updated once they are used in a group, whose overhead will be analyzed in Section V-B. Every participant u_i retrieves her polynomial values Q_i for the whole spatiotemporal matrix with each degree using her ID$_i$ from KG. In requested cell (t,l), each participant u_i holds the polynomial set $Q_i(t,l)=\{q^2_{(t,l)}(\text{ID}_i)\dots q^{\kappa}_{(t,l)}(\text{ID}_i)\dots q^{K-1}_{(t,l)}(\text{ID}_i)\}$. The $q^{\kappa-1}_{(t,l)}(\text{ID}_i)$ for tasks $s(t,l)=1$ should be used when the group size is κ. The participants only know the values of polynomials on their spatiotemporal matrix with their ID$_i$ but not the polynomial themselves. Also, KG assigns a public parameter V to each participants, which will be used for breaking bid tie later. Note that KG does not participant in the actual auction processes.

Group and disguised bid formulation: Platform broadcasts the tasks S and the bid upper bound Υ. For these tasks, at current time τ, TP randomly allocate the κ participants $(u_1^j,u_2^j,\cdots,u_\kappa^j)$ into a group set U_j (with $U=\cap_{j=1,\cdots,\lfloor\frac{n}{\kappa}\rfloor}U_j$) and asks for the bid information from these participants. The true bid from participant u_i^j in a group U_j is denoted as $b_i^j(t,l)$. Participant u_i^j in group U_j can calculate her disguised bid using the group members' IDs and report her bid to TP:

$$f(ID_i,b_i^j(t,l))=$$
$$q^{\kappa-1}_{(t,l)}(ID_i)\prod_{\substack{o=1\\o\neq i}}^{\kappa}\frac{0-ID_o}{ID_i-ID_o}\cdot H(\tau)+(\Upsilon-b_i^j(t,l))^R,$$

where $H()$, a hash function, is a public secret among the participants.

Winning bid decision within groups: First, TP aggregates all the participants' disguised bids together,

$$\sum_{i=1}^{\kappa}f(ID_i,b_i^j(t,l))=\sum_{i=1}^{\kappa}(\Upsilon-b_i^j(t,l))^R,$$

and then uses the Minimum Approximate to find the minimum bid in the current group.

$$b^j(t,l)=\Upsilon-\sqrt[R]{\sum_{i=1}^{\kappa}(\Upsilon-b_i^j(t,l))^R}=\Upsilon-\sqrt[R]{\sum_{i=1}^{\kappa}f(ID_i,b_i^j(t,l))}.$$

Note that all κ,Υ, and R are the public system parameters. After calculating the minimum bid, TP broadcasts it among all the group members.

Next, TP needs to find the winner, find the second lowest bid and break bid ties in each group. To select a single winner and break bid ties, we use the following procedure (also illustrated in Fig. 4). The participants whose bids are larger than the winning bid report the pre-assigned value V to TP and assume that the number of values received is F. If $F<\kappa-1$, TP knows that there is a tie and the second lowest bid in current group is the same as the winning bid. In this case, TP could randomly select one from the participants who did not provide the V value in this step as the group winner

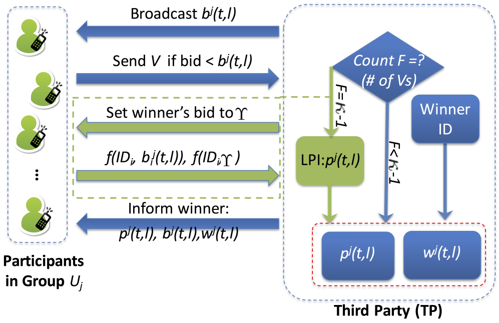

Broadcast $b^j(t,l)$
Send V if bid < $b^j(t,l)$
Count F =? (# of Vs)
F=κ-1
Set winner's bid to ϒ
Winner ID
$f(ID_i, b_i^j(t,l)), f(ID_i ϒ)$
LPI: $p^j(t,l)$
F<κ-1
Inform winner: $p^j(t,l), b^j(t,l), w^j(t,l)$
$p^j(t,l)$
$w^j(t,l)$
Participants in Group U_j
Third Party (TP)

Fig. 4. **Breaking ties within a group**: TP selects a single winner and obtains the second lowest bid after knowing $b^j(t,l)$. Note that the green exchanges are only needed when there is no tie (i.e. $F = \kappa - 1$).

since ID is a public parameter. Further, TP can consider other parameters such as credit or worker ability [44] to select the winner when there is a tie. Otherwise, if $F = \kappa - 1$, TP will set the winner's bid to the bid upper bound and repeat the process again to get the second lowest bid in the current group. After this procedure, TP obtains the winner $w^j(t,l)$, its winning bid $b^j(t,l)$, and the second lowest bid $p^j(t,l)$ in this group U_j.

Winning bid decision at platform: For each group U_j, TP will presents two virtual participants (with virtual bids at the winning bid $b^j(t,l)$ and the second lowest bid $p^j(t,l)$) to the platform. The platform receives $2G$ virtual participants' bids for sensing tasks cell (t,l), where G is the number of groups. Then, the platform will make the virtual participants selection and obtain the lowest bid $b(t,l)$ and the critical payment $p(t,l)$ over all participants. The group selection is the same as optimizing participant selection in general case without the third party. The lowest bid (winner) and the critical payment calculated by platform is described as below:

$$b(t,l) = \min_{j=1}^{G} b^j(t,l), w(t,l) = \arg\min_{j=1}^{G} b^j(t,l)$$
$$p(t,l) = \min_{j\in[1,G], b^j(t,l)\neq b(t,l)} \{b^j(t,l), p^j(t,l)\}$$

After the selection decision, platform broadcasts the winning bid (and the winning group) the payment information to the TP. Then TP notifies winner, who then perform the corresponding task. Note that our proposed solution do not affect the selection algorithm (VCG auction) at the platform. The platform can also accept bids from real participants.

D. Some Critical Issues

$H(\tau)$ **and IDs.** Note that $H(\tau)$ is the common secret which is known by all participants but not by the third party. $H(\tau)$ could let the whole system be securer since it changes each time when TP aggregates bids from each group. This requires the synchronization among all participants. The participants' IDs are also public in our system so that they could be directly used in the calculation.

Verification for $q^X_{(t,l)}(ID_i)$. Each participant could only receive the value of polynomials with her own ID$_i$. Although KG is assumed to be a trusted party, it is possible that an erroneous value is delivered to the participants due to unknown errors. However, since the polynomial is the master secret which is kept hidden to anyone except KG, the participants are not able to verify the correctness the received values. To solve this problem, we extend the zero-knowledge proof (ZKP) [45] and introduce a simple verification protocol below. The protocol allows the participants to verify that the value is indeed calculated from the polynomial owned by KG, but the entire protocol keeps the polynomial itself hidden to the participants.

Key generator publishes the generator g of a multiplicative cyclic group $\mathbb{G}$ where the DDH assumption holds (*e.g.,* a Schnorr group). Then, a series of g^{c_x}'s, where each c_x is the coefficient for ID$_i^x$, are published. Each participant can calculate the following formula:

$$\prod (g^{c_x})^{ID_i^x} = g^{c_1 \cdot ID_i^1 + \cdots + c_x \cdot ID_i^x + \cdots + c_X \cdot ID_i^X}.$$

If this value is equal to $g^{q^X_{(t,l)}(ID_i)}$, where $q^X_{(t,l)}(ID_i)$ is the received value from KG before, the participant verifies that the received value is correctly calculated. Because the DDH assumption holds in the group $\mathbb{G}$, no statistical information about c_x is leaked from g^{c_x}, therefore this verification does not tamper the IND-CPA guaranteed by our MCS protocol.

ID Updates. From the formula of the disguised bid, we know that the polynomial value is the only secret except the true bids. As the ranges of polynomial value is much larger than bids, the attackers could estimate the bid value in several rounds with the same polynomial value applied. As a result, we need to update the used ID$_i$ and the related $q^{\kappa}_{(t,l)}(ID_i)$. In our current system, each participant has multiple unduplicated IDs. For each participation selection round, the bidders need to mark the polynomial value they used. When the selection with same group size is performed in the same requested cell, the participants should request to renew the polynomial values. We will analyze the involvement of KG in Section V-B.

V. Theoretic Analysis

A. Security Proof

Theorem 1: Our bid disguising is semantically secure.

Proof: A bidder's (with ID ID_i) bid $b_i(t,l)$ for the auction occurring at the (t,l) of the spatiotemporal matrix is disguised as the following format:

$$f(ID_i, b_i(t,l)) =$$
$$q^{\kappa-1}_{(t,l)}(ID_i) \prod_{\substack{o=1 \\ o\neq i}}^{\kappa} \frac{0 - ID_o}{ID_i - ID_o} \cdot H(\tau) + (\Upsilon - b_i(t,l))^R,$$

when κ bidders participate in the auction. The IDs of the bidders, the current time slot τ as well as the hash function $H(\cdot)$ are public parameters. The only two unknown secrets are $q^{\kappa-1}_{(t,l)}(ID_i)$ and $(\Upsilon - b_i(t,l))^R$. Therefore, multiple disguised bids with distinct polynomial values cannot be used to infer the true bids because there are more unknown variables than the equations.

In reality, there are three cases. First, the disguised bids are received from different auctions occurring at different cells in the spatiotemporal matrix. Second, the auctions occur at the same cell in the spatiotemporal matrix and the number of bidders are different in the auctions. In these situations, different polynomials are used to disguise the bids, therefore the adversaries do not benefit. Third, multiple auctions with the same number of bidders occur at the same cell in the spatiotemporal matrix. Note that every time an auction occurs at a cell at which another auction with the same number of bidders has occurred before, our mechanism ensures that the participants' IDs are refreshed, and all participants will receive new polynomial values corresponding to the new IDs. Therefore, even in this case, the disguised bids from multiple auctions are based on different polynomials. In summary, no matter how auctions are performed, combining multiple disguised bids does not help to infer the true bids.

In the sequel, we further prove that our mechanism guarantees semantic security by disguising the true bids . For any single disguised bid $f(ID_i, b_i(t,l))$, let us simplify the terms first. Let $f(ID_i, b_i(t,l))$ be simplified as

$$f(ID_i, b_i(t,l)) = q \cdot \Pi \cdot H + b$$

where q, Π, H, and b represent $q^{\kappa-1}_{(t,l)}(ID_i)$, $\prod \frac{0-ID_o}{ID_i-ID_o}$, $H(\tau)$, and $(\Upsilon - b_i(t,l))^R$ respectively. Then, for any b and its disguised bid $f(ID_i, b_i(t,l))$, there must exist $b' \neq b, q' \neq q$ such that

$$q \cdot \Pi \cdot H + b = q' \cdot \Pi \cdot H + b'$$

Such b', q' exist because of the following reason. Recall that all operations are closed under the finite field $\mathbb{Z}/p\mathbb{Z}$ with a safe prime p. Then, ΠH and p must be coprime, and therefore the inverse $(\Pi H)^{-1} \mod p$ must exist, which implies $q' = (q\Pi H + b - b')(\Pi H)^{-1}$ will make the above equation hold. In other words, for any $b' \in \mathbb{Z}/p\mathbb{Z}$, the disguised bid created with $q' = (q\Pi H + b - b')(\Pi H)^{-1}$ will be exactly the same as b's disguised bid $f(ID_i, b_i(t,l))$.

Recall that the coefficients of the polynomials are chosen from $\mathbb{Z}/p\mathbb{Z}$ uniform randomly. Then, a given disguised bid can be the disguised bid of any valid bid with equal likelihood, which indicates that the disguised bid does not disclose any statistical information about the true bid. ■

Theorem 2: Our MCS protocol guarantees ciphertext indistinguishability against chosen-plaintext attack (IND-CPA).

Proof: In the aforementioned Secure Bidding Game, although the adversary can adaptively query communication strings corresponding to any input bid he submits, the semantic security of our bid disguising guarantees that he does not gain any statistical information about the bid or the polynomial value. This implies that, even if the adversary submits two challenge bids and receive their disguised bids in Phase 1 or Phase 2, they are not able to statistically correlate them to the disguised bid of b_μ he receives in the Challenge phase. Therefore, his advantage will be a negligible function of the security parameter λ. ■

B. Involvement of Key Generator

As we illustrated in IV-C, a participant may need to refresh her ID and polynomial value from the key generator for privacy protection. Note that KG only needs to refresh the parameters for the participant who wants to respond to a task request. The request occurs in the same cell (t,l) of the spatiotemporal matrix S as a previous task that she participated in, and the participant wants to require the same group size κ for both tasks. In the worst case, assume that each participant is willing to bid for tasks falling in each cell of S. Thus, when the participant encounters the same group size at the same cell, she has to contact the key generator to renew her parameters. Therefore, the involvement of KG is influenced by the task distribution over the spatiotemporal matrix ($T \times L$ choices) and participant's required group size κ ($K-2$ choices from 3 to K). We now analyze the average frequency of KG involvement using amortized analysis.

For each cell (t,l) in the $T \times L$ spatiotemporal matrix the possible group size κ varies from 3 to K. Each combination (t,l,κ) can be represented by a box. A task (which the participant want to bid) belongs to a box if it has the corresponding values of t,l,κ. Clearly, there are $D = TL(K-2)$ boxes.

Now assume that we have m tasks randomly distributed to the D boxes. Let $N(t,l,\kappa)$ be the number of tasks in box (t,l,κ) and let $p(t,l,\kappa)$ be the probability that a task is located in box (t,l,κ). Note that $N(t,l,\kappa) \sim B(m, p(t,l,\kappa))$, where $B(m, p(t,l,\kappa))$ represents the binomial distribution with parameters m and $p(t,l,\kappa)$. We have

$$\sum_{t,l,\kappa} p(t,l,\kappa) = 1 \text{ and } \sum_{t,l,\kappa} N(t,l,\kappa) = m.$$

Assuming that each participant participates in each task, then the number of KG involvements corresponds to

$$\sum_{t,l,\kappa} (N(t,l,\kappa) - 1) 1_{[N(t,l,\kappa)\geq 2]},$$

where $1_{[\dots]}$ is the indicator function. We have

$$\begin{aligned}
&\mathrm{E}(\textit{frequency of KG involvement}) \\
=&\mathrm{E}[\sum_{t,l,\kappa}(N(t,l,\kappa)-1)1_{[N(t,l,\kappa)\geq 2]}] \\
=&m - D - \mathrm{E}[\sum_{t,l,\kappa}(N(t,l,\kappa)-1)1_{[N(t,l,\kappa)\leq 1]}] \\
=&m - D - \sum_{t,l,\kappa}\mathrm{E}[(N(t,l,\kappa)-1)1_{[(N(t,l,\kappa)\leq 1]}] \\
=&m - D - \sum_{t,l,\kappa}(-1)P(N(t,l,\kappa)=0) \\
=&m - D + \sum_{t,l,\kappa}(1-p(t,l,\kappa))^m.
\end{aligned}$$

In the case of a uniform distribution, where $p(t,l,\kappa) = 1/D$ we have

$$\mathrm{E}(\textit{frequency of KG involvement}) = m - D + \frac{(D-1)^m}{D^{m-1}}.$$

Similarly, the probability that a task type at (t,l) with group size requested at κ requests x KG involvement is

$$\begin{aligned}
&P(\textit{x KG involvements in box}(t,l,\kappa)) = P(N(t,l,\kappa) = x+1) \\
&\quad = C_m^{x+1}\left(\frac{1}{D}\right)^{x+1}\left(1-\frac{1}{D}\right)^{m-x-1},
\end{aligned}$$

where C_m^y refers to y choose m.

TABLE I. PARAMETERS USED IN D4D-BASED SIMULATIONS

Parameter	Value or Range
Unit of time/Task duration	1 day
Number of locations (towers)	18
Number of tasks M	$60, 80, 100, 120, 140$
Number of candidate participants N	$2000, 4000, 6000, 8000, 10000$
Group size K	$20, 40, 60, 80, 100$
Length of whole sensing cycle	one week (7 days)
Number of data records	46613
Total period of traces used	Dec 5, 2011 to Jan 8, 2012

TABLE II. PARAMETERS USED IN SFC-BASED SIMULATIONS

Parameter	Value or Range
Unit of time/Task duration	$10, 20, 30, 40, 50, 60$ Minutes
Number of tasks M	$60, 80, 100, 120, 140$
Number of candidate participants N	504
Group size K	$10, 20, 30, 40, 50$
Length of whole sensing cycle	one day
Number of data records	508979
Total period of traces used	May 17, 2008 to June 10, 2008

VI. SIMULATIONS

A. Datasets and Configuration

1) D4D Dataset: D4D dataset is a mobile phone call tracking data, from the Orange for the *Data for Development (D4D) challenge* [46]. The data is anonymized call detailed records of phone calls between $50,000$ Orange mobile users in Ivory Coast between December 1, 2011 and April 28, 2012. We use a dataset of individual mobile phone call tracking trace with high spatial resolution (*SET2* in D4D datasets), which contains the access records of antenna (cellular tower) of each mobile user in every two weeks. Since the density of phone call is very sparse, we merge records from multiple weeks into a single week and use one week (7 days) as the whole sensing cycle T. There are $46,613$ records for the user showing up in all cellular towers without duplication, and the number of such users is $10,704$. We assign the location of each task randomly from the locations of 18 cellular towers, which are with the highest call records. Most of these towers are located in the downtown region of Abidjan. We treat the distance between a participant (her current tower) and the task (its location at one of the 18 towers) as the bid value[2] for each participant to that task. In other words, when a participant is far away from a task location, her cost to perform the sensing task is high. Since the records of mobile phone call (tower location) is not the exact position of participants, in our simulations, we add an additional random distance with range $[0, 1]$ to the estimated distance as the original bid value. The parameters for tasks and participants are listed in Table I.

2) SFC Dataset: Although D4D dataset provides a real-life large scale traces for human mobility, it does not have high spatial resolution (still at cellular tower level). Therefore, we also use the San Francisco Cab (SFC) Dataset [47] for simulations, which includes the GPS traces (total $11,200,335$ data records) from 536 cabs in total 25 days from $May17, 2008$ to $June10, 2008$. We believe that SFC can provide complemental scenarios for our simulations. Here, we use a subset of all traces (tailored both on temporal and spacial domains), which has 504 participants with $508,979$ data records. Since the GPS records are accurate locations, we randomly generate the locations of sensing tasks and use the distance between the participant and the task as the true bid. Table II summarizes the parameter settings.

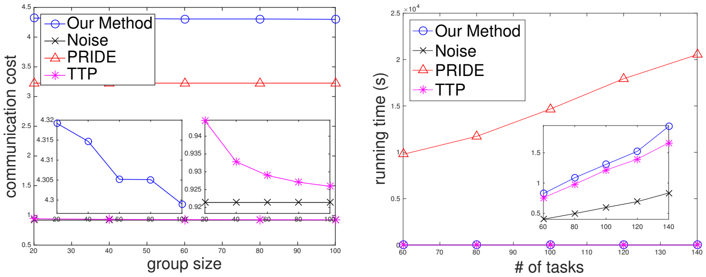
B. Compared Methods and Metrics

In all the experiments, we compare our proposed method with three alternative mechanisms: PRIDE [48], the group mechanism with trusted third party (TTP) and the location obfuscation method (Noise). PRIDE [48] is a privacy-preserving and strategy-proof spectrum auction in cognitive radio networks, which leverages complex cryptographic techniques (such as secure multiparty computation, order-preserving encryption, and oblivious transfer) to obtain the lowest bid and preserve bid privacy. We have adopt it to our scenario and use RSA with modulus of 1024 bits for encryption/decryption. In TTP, we introduced a completely trusted third party to perform group bidding. All information about participants such as bid, ID and spatiotemporal matrix, are transparent to TTP. It could absolutely protect the participants' privacy from platform but rely on TTP entirely. Noise applies a standard privacy preserving technique, adding certain noise (range from 0 to 10) in the bids (i.e. the distance between the participant and the task) from each participants.

We test all these methods under different settings (with various number of participants, number of tasks, group size, and task period), and evaluate them with the following metrics. *Running time*: the time between the tasks is broadcast and all participants have been selected. Here we assume that the participant selection algorithm is the same for all method, picking the participant with the smallest bid as the winner. *Communication cost*: the communication costs in all steps, including task broadcast, group formation, winner decision and second bid calculation in each group, and winner decision for tasks. It is measured as the average round of message exchanges from each participant per task. *Overpayment/Accuracy*: since $b(t, l)$ acts as the bid of winner $w(t, l)$ and $p(t, l)$ as the related payment to her for this task, the overpayment for this task is defined as $p(t, l) - b(t, l)$. Then the total average overpayment is an average over all tasks.

C. Simulation Results

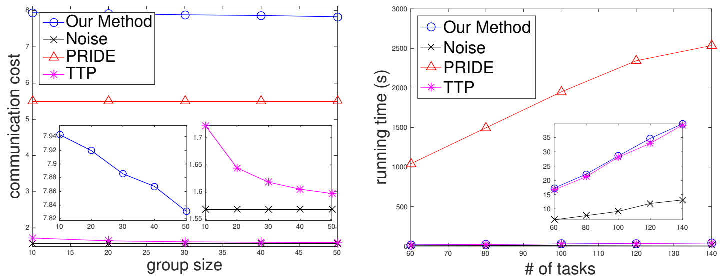
We first test the performance of all methods using both D4D and SFC datasets in terms of communication cost and running time. Simulation results are shown in Fig. 5 and Fig. 6, respectively. For communication cost, we consider the average number of message exchanges per task per participant with



(a) communication cost (b) running time

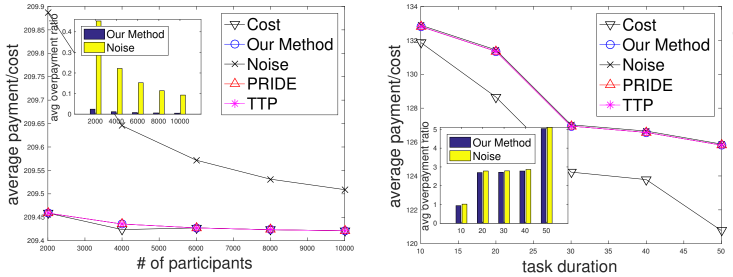
Fig. 5. **D4D Simulation:** with $6,000$ participants (a) average communication cost per task per participant with different group size over 100 tasks. (b) total running time with different number of tasks when group size is fixed at 60.

[2] Note that the bid value can be others, e.g., users' ability to perform the task. Here we just use the distance as an example, which is easy to obtain from both datasets.



(a) communication cost (b) running time

Fig. 6. **SFC Simulation:** with 504 participants (a) average communication cost per task per participant with different group size over 100 tasks. (b) total running time with different number of tasks when group size is fixed at 30.

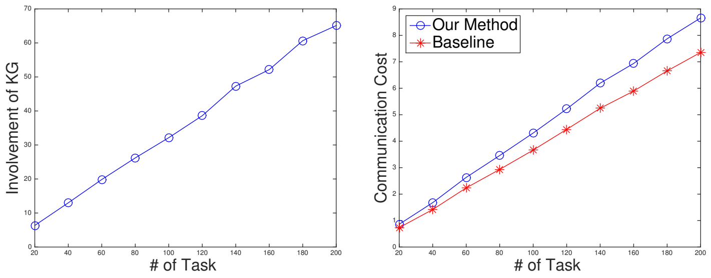


(a) D4D (b) SFC

Fig. 7. **Average cost and payment** for all the tasks by different methods in (a) D4D simulations and (b) SFC simulations. Smaller plots show the overpayment ratios of our method and Noise.

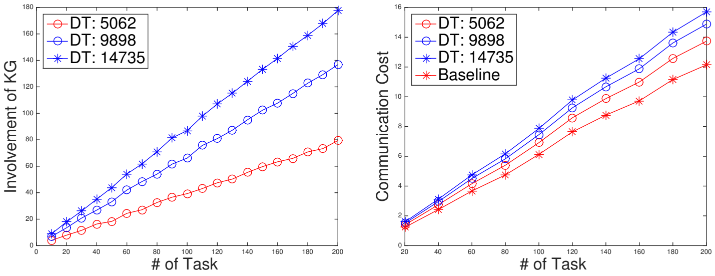
different group sizes, as shown in Fig. 5(a) and Fig. 6(a). First, the communication costs of Noise and PRIDE do not change with group size, while those of TTP and our method decrease with the growth of group size as the virtual participants on behalf of each group decease with the larger group size. Compared with TTP or PRIDE, our method needs more message exchanges to achieve privacy preserving. However, for running time (Fig. 5(b) and Fig. 6(b)), PRIDE takes significantly more time than other methods because its encryption process is time consuming. TTP and our method use similar time, which is slightly longer than Noise (mainly for group creation and group bidding). In addition, with increasing number of tasks, more time is needed for all methods. Overall, our method can achieve privacy-preserving with similar running time but larger communication cost compared with TTP. The communication overhead is the price for privacy-protection.

We also measure the payments of different methods and compare them with the true cost. Results are shown in Fig. 7. First, both cost and payment decrease with the increase of number of participants (Fig. 7(a)) and the task duration (Fig. 7(b)). With more participants, the platform/group can choose lower minimum bid and pay less rewards to the winners. With longer task duration, participants have more chances to bid less. Further, our method, TTP and PRIDE pay the same amount, and Noise pays the most. This can be clearly seen in the smaller plots within the figures, which show the overpayment of our method and Noise. Obviously, Noise sacrifice the overpayment to protect the privacy. Note that the difference of overpayments between Noise and our method is not significant in SFC simulations. This may be because the range of added random noises is much smaller than the distances (true bids) in SFC dataset.



(a) KG involvement (b) communication cost

Fig. 8. **D4D simulation:** KG involvement and communication cost with different number of tasks.



(a) KG involvement (b) communication cost

Fig. 9. **SFC simulation:** KG involvement and communication cost with various DT value and the number of tasks.

Last, we consider the involvement of KG. Recall that when a participant wants to bid a task which has the same spatiotemporal requirement and desired group size with a previous task she bided, the participant needs to refresh her ID and polynomial values from KG. In the following experiments, we fix the group size and consider the effect of the number of tasks. Fig. 8 and Fig. 9 clearly show that, more involvements of KG (also extra communication cost) are needed when there are more tasks. This confirms the theoretical analysis we had in Section V-B. Here, the baseline is the method without any refreshing of IDs and values. Since we do not have tower location as the task location for SFC dataset, we consider the distance among tasks instead for refreshing decision. We assume that a participant needs to refresh her ID and values from KG when the distance between the current task she wants to bid and any of her former tasks is less than the predefined distance threshold (DT). As shown in Fig. 9, with larger distance threshold, both KG involvement and communication cost become larger. This is reasonable, since the current task will interfere with more tasks in the larger range, which then results in more involvements of KG and more message exchanges.

VII. Conclusion

In this paper, we propose a new privacy-preserving participant selection mechanism for protecting bid privacy of participants in a dynamic auction-based MCS system. By grouping mobile participants into groups with semi-trusted TPs and carefully disguising their bids within the groups, we can achieve scalable selection and guarantee the overall truthfulness and security while protect the individual bids from participants. Both theoretical analysis and real-life tracing data simulations confirm the efficiency and security of our proposed mechanism.

Acknowledgement: The work is supported by the US National Science Foundation under Grant No. ECCS-1247944, CNS-1319915, CNS-1343355, CMMI-1436786 and CNS-1526638, the National Natural Science Foundation of China under Grant No. 61428203, 61572347, and 61520106007, the China National Funds for Distinguished Young Scientists with No.61625205, and the Key Research Program of Frontier Sciences, CAS. No. QYZDY-SSW-JSC002. Y. Wang is the corresponding author.

References

[1] B. Guo, Z. Wang, Z. Yu, Y. Wang, et al., "Mobile crowd sensing and computing: The review of an emerging human-powered sensing paradigm," *ACM Computing Surveys*, 48(1), 2015.

[2] D. Zhang, H. Xiong, L. Wang, and G. Chen, "Crowdrecruiter: selecting participants for piggyback crowdsensing under probabilistic coverage constraint," in *Proc. of ACM UbiComp*, 2014.

[3] H. Li, T. Li, and Y. Wang, "Dynamic participant recruitment of mobile crowd sensing for heterogeneous sensing tasks," in *IEEE MASS*, 2015.

[4] H. Li, T. Li, F. Li, et al., "Enhancing participant selection through caching in mobile crowd sensing," in *Proc. of IEEE/ACM IWQoS*, 2016.

[5] H. Xiong, D. Zhang, L. Wang, J. Gibson, and J. Zhu, "EEMC: Enabling energy-efficient mobile crowdsensing with anonymous participants," *ACM Trans. on Intelligent Systems and Technology*,6(3), 2015.

[6] H. Xiong, D. Zhang, L. Wang, and H. Chaouchi, "EMC^3: Energy-efficient data transfer in mobile crowdsensing under full coverage constraint," *IEEE Trans. on Mobile Computing*, 14(7):1355-1368, 2015.

[7] D. Zhao, H. Ma, and L. Liu, "Energy-efficient opportunistic coverage for people-centric urban sensing," *Wireless Networks*, 20(6):1461-1476, 2014.

[8] D. Zhao, X.-Y. Li, and H. Ma, "Budget-feasible online incentive mechanisms for crowdsourcing tasks truthfully," *IEEE/ACM Transactions on Networking*, 24(2):647-661, 2016.

[9] Z. Feng, Y. Zhu, Q. Zhang, L. M. Ni, and A. V. Vasilakos, "TRAC: truthful auction for location-aware collaborative sensing in mobile crowdsourcing," in *Proc. of IEEE INFOCOM*, 2014.

[10] B. Guo, H. Chen, Q. Han, Z. Yu, D. Zhang, and Y. Wang, "Worker-contributed data utility measurement for visual crowdsensing systems," *IEEE Transactions on Mobile Computing*, to appear.

[11] Y. Wang, H. Li, and T. Li, "Participant selection for data collection through device-to-device communications in mobile sensing," *Personal and Ubiquitous Computing*, to appear.

[12] N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani, *Algorithmic Game Theory*. New York, NY, USA: Cambridge University Press, 2007.

[13] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "AnonySense: Privacy-aware people-centric sensing," in *Proc. of ACM MobiSys*, 2008

[14] J. Shi, R. Zhang, Y. Liu, and Y. Zhang, "PriSense: Privacy-preserving data aggregation in people-centric urban sensing systems," in *Proc. of IEEE INFOCOM*, 2010

[15] B. Agir, T. G. Papaioannou, R. Narendula, K. Aberer, and J. Hubaux, "User-side adaptive protection of location privacy in participatory sensing," *GeoInformatica*, 18(1):165-191, 2014.

[16] L. Pournajaf, L. Xiong, V. S. Sunderam, and S. Goryczka, "Spatial task assignment for crowd sensing with cloaked locations," in *Proc. of IEEE MDM*, 2014.

[17] K. L. Huang, S. S. Kanhere, et al., "Preserving privacy in participatory sensing systems," *Comput. Commun.*, 33(11):1266-1280, 2010.

[18] Q. Li and G. Cao, "Providing privacy-aware incentives for mobile sensing," in *Proc. of IEEE PerCom*, 2013

[19] R. K. Ganti, N. Pham, et al., "Poolview: Stream privacy for grassroots participatory sensing," in *Proc. of ACM SenSys*, 2008

[20] Y. Wang, D. Xu, X. He, C. Zhang, F. Li, and B. Xu, "L2P2: Location-aware location privacy protection for location-based services," in *Proc. of IEEE INFOCOM*, 2012.

[21] Y. Wang, D. Xu, and F. Li, "Providing location-aware location privacy protection for mobile location-based services," *Tsinghua Science and Technology*, 21(3):243-259, 2016.

[22] E. Shi, H. Chan, E. Rieffel, R. Chow, and D. Song, "Privacy-preserving aggregation of time-series data," in *Proc. of NDSS*, 2011.

[23] M. Joye and B. Libert, "A scalable scheme for privacy-preserving aggregation of time-series data," in *Proc. of International Conf. on Financial Cryptography and Data Security*, 2013.

[24] T. Jung, X. Mao, X.-Y. Li, S.-J. Tang, W. Gong, and L. Zhang, "Privacy-preserving data aggregation without secure channel: Multivariate polynomial evaluation," in *Proc. of IEEE INFOCOM*, 2013.

[25] C. Dwork, A. Roth, "The algorithmic foundations of differential privacy," in *Foundations and Trends in Theoretical Computer Science*, 9(3-4):211-407, 2014

[26] H. Jin, L. Su, B. Ding, K. Nahrstedt, and N. Borisov, "Enabling privacy-preserving incentives for mobile crowd sensing systems," in *Proc. of IEEE ICDCS*, 2016.

[27] H. Jin, L. Su, H. Xiao, and K. Nahrstedt, "Inception: Incentivizing privacy-preserving data aggregation for mobile crowd sensing systems," in *Proc. of ACM MobiHoc*, 2016.

[28] M. Naor, B. Pinkas, and R. Sumner, "Privacy preserving auctions and mechanism design," in *Proc. of ACM EC*, 1999.

[29] O. Goldreich, "Secure multi-party computation," *Manuscript. Preliminary version*, 1998.

[30] T. Jung and X.-Y. Li, "Enabling privacy-preserving auctions in big data," in *Proc. of IEEE INFOCOM WKSHPS*, 2015.

[31] Q. Huang, Y. Gui, F. Wu, G. Chen, and Q. Zhang, "A general privacy-preserving auction mechanism for secondary spectrum markets," *IEEE/ACM Transactions on Networking*, 24(3):1881-1893, 2016.

[32] H. Lipmaa, N. Asokan, and V. Niemi, "Secure Vickrey auctions without threshold trust," in *Proc. of Financial Cryptography*, 2002.

[33] M. Larson, R. Li, C. Hu, et al., "A bidder-oriented privacy-preserving VCG auction scheme," in *Proc. of WASA*, 2015.

[34] K. Suzuki and M. Yokoo, "Secure generalized Vickrey auction using homomorphic encryption," in *Proc. of Financial Cryptography*, 2003.

[35] M. Yokoo and K. Suzuki, "Secure generalized Vickrey auction without third-party servers," in *Proc. of Financial Cryptography*, 2004.

[36] F. Brandt, "Fully private auctions in a constant number of rounds," in *Proc. of Financial Cryptography*, 2003.

[37] D.-H. Shih, H.-Y. Huang, and D. C. Yen, "A secure reverse Vickrey auction scheme with bid privacy," *Information Sciences*, 176(5): 550–564, 2006.

[38] F. Brandt, "Cryptographic protocols for secure second-price auctions," in *Proc. of Workshop on Cooperative Information Agents V*, 2001.

[39] F. Brandt, "Secure and private auctions without auctioneers," in *Technical Report FKI-245-02*. Institut fur Informatick, Technishce Universitat Munchen, 2002.

[40] W. Vickrey, "Counterspeculation, auctions and competitive sealed tenders," *Journal of Finance*, 16(1):8–37, 1961.

[41] E. Clarke, "Multipart pricing of public goods," *Public Choice*, 11:17–33, 1971.

[42] T. Groves, "Incentives in teams," *Econometrica*, 41(4): 617–31, July 1973.

[43] T. Jung, J Han, and X.-Y. Li, "PDA: Semantically Secure Time-Series Data Analytics with Dynamic Subgroups," in *IEEE Transactions on Dependable and Secure Computing*, 2016, IEEE Early Access.

[44] L. Pu, X. Chen, J. Xu, and X. Fu, "Crowdlet: optimal worker recruitment for self-organized mobile crowdsourcing," in *Proc. of IEEE INFOCOM*, 2016.

[45] M. Blum, P. Feldman, and S. Micali, "Non-interactive zero-knowledge and its applications," in *Proc. of ACM STOC*, 1988.

[46] The Data for Development (D4D) Challenge, http://www.d4d.orange.com.

[47] M. Piorkowski, N. Sarafijanovic-Djukic, and M. Grossglauser, "Dataset of mobility traces of taxi cabs in San Francisco, USA," CRAWDAD dataset epfl/mobility (v. 2009-02-24), Downloaded from http://crawdad.org/epfl/mobility/20090224, Feb. 2009.

[48] F. Wu, Q. Huang, Y. Tao, and G. Chen, "Towards privacy preservation in strategy-proof spectrum auction mechanisms for noncooperative wireless networks," *IEEE/ACM Transactions on Networking*, 23(4): 1271–1285, 2015.