DIARY: A Differentially Private and Approximately Revenue Maximizing Auction Mechanism for Secondary Spectrum Markets

Chunchun Wu, Zuying Wei, Fan Wu, and Guihai Chen
Shanghai Key Laboratory of Scalable Computing and Systems
Department of Computer Science and Engineering
Shanghai Jiao Tong University, China
{bubble_chun, zu_ying_hi}@sjtu.edu.cn, {fwu, gchen}@cs.sjtu.edu.cn

Abstract—It is urgent to solve the contradiction between limited spectrum resources and the increasing demand from the ever-growing wireless networks. Spectrum redistribution is a powerful way to mitigate the situation of spectrum scarcity. In contrast to existing truthful mechanisms for spectrum redistribution which aim to maximize the spectrum utilization and social welfare, we propose DIARY in this paper, which not only achieves approximate revenue maximization, but also guarantees bid privacy via differential privacy. Extensive simulations show that DIARY has substantial competitive advantages over existing mechanisms.

I. Introduction

Recent years have witnessed the fast development of wireless technology, which has brought about a great increase in demand of spectrum resources. Spectrum is a scarce commodity controlled by governmental agencies(e.g., Federal Communications Commission (FCC) in US). Traditionally, static spectrum allocation scheme is adopted to determine resources distribution. However, studies show that such a static spectrum allocation scheme is inefficient due to the dramatic changes of spectrum utilization in both spatial and temporal dimensions [12]. The current spectrum allocation problem is that, large chunks of allocated spectrum are left idle most of the time at lots of places, meanwhile unlicensed secondary users are badly in need of spectrum to carry out their work. To solve this problem and improve spectrum utilization, a number of auction-based dynamic spectrum allocation schemes are proposed [7], [17], [21], [23]. In fact, there are already some companies like Spectrum Bridge [1] conducting spectrum auctions, which makes such dynamic schemes no longer merely theoretical.

Auctions are well-studied protocols in economic theory for allocating scarce resources, and attractive because of their well-defined notions for various objective. A major difference between economic auctions and spectrum auctions is the spatial reusability of spectrum. A single chunk of spectrum can be leased to multiple secondary users as long as they do not interfere with each other. A natural goal of such auctions is to maximize the revenue for primary users, since primary users may not be willing to share their own spectrum resources unless there are sufficient incentives.

Another major difference between spectrum auctions and traditional auctions is that spectrum auctions are held repeatedly due to the dramatic changes of spectrum utilization. Mostly previous studies on this issue neglect the repeatability of spectrum auctions. Clues about others' private information may be concluded form historical records or previous rounds, so that spiteful secondary users can use such information to cheat or collusion. These malicious manipulations not only abate victims' enthusiasm for participation in auctions, which reduces the long-term revenue of primary users, but also cause some vindictive actions from secondary users who never have a chance to win [24].

The problem of analyzing sensitive data with an eye towards maintaining its privacy has existed for some time. However, most of the existing mechanisms cannot guarantee the bid privacy. For instance, lots of revenue maximization mechanisms [11], [19], which make participators to bid truthfully in order to guarantee strategy-proofness, obviously violate the bid privacy. The recent notion of *differential privacy* [2], [3], in addition with its own intrinsic virtue, can assure that participants have limited effect on the outcome of the mechanisms. As a consequence, participants will have limited incentive to lie and little worry about privacy violations.

For the reasons mentioned above, designing a channel auction mechanism, which could maximize the revenue of the primary users and guarantee the bid privacy, is precisely the goal of our work. Obviously, designing such an auction mechanism has its own challenges:

- *Computing Complexity*: We all know that to find optimal solutions to the general problem of the channel allocation

is NP-complete [20], which means that the the optimization problem of revenue maximization is NP-hard. It's impossible to find a deterministic solution to the revenue maximization problem in polynomial time.

- *Bid Privacy*: Due to the spatial reusability of the spectrum, differential private mechanisms belonging to the family of exponential mechanisms [10], [15] cannot be adopted directly.

In this paper, we propose DIARY, which is a <u>DI</u>fferentially private and <u>A</u>pproximately <u>R</u>evenue maximizing auction mechanism for secondar<u>Y</u> spectrum markets. DIARY not only achieves approximate revenue maximization, but also guarantees bid privacy. To our best knowledge, we are the first to investigate the auction mechanisms which achieve both bid privacy and approximate revenue maximization. Our key contributions are listed as follows.

- First, we model the channel redistribution problem as an auction, and propose a novel non-deterministic mechanism, DIARY, to achieve approximate revenue maximization and bid privacy via differential privacy.
- Second, we prove that DIARY satisfies all requirements of our goal.
- Third, we conduct extensive experiments to compare the performance of DIARY with existing mechanisms RGTS [11], TSA [19] and PFR [8]. Results show that DIARY has substantial competitive advantages over existing mechanisms, especially when the competition for channels is fierce.

The rest of this paper is organized as follows. In Section II, we introduce our auction model and review some solution concepts. In Section III, we show the design of our auction mechanism DIARY. Extensive experiments are presented in Section IV to compare the performance of the proposed mechanism with others. In Section V, we discuss the related works. In the end, we draw our conclusion and introduce our future work in Section VI.

II. PRELIMINARIES

In this section, we show our problem model and introduce some solution concepts about differential privacy.

A. Model

We model the problem of spectrum allocation as a sealed-bid auction. Usually, in a spectrum auction, we refer to secondary users as *bidders* or *buyers*, and the primary user as the *seller*. In this auction model, there are a number of buyers and a single seller. The seller, who has m idle channels, wants to lease the channels out to get profit. We denote the m channels by $C = \{c_1, c_2, \ldots c_m\}$. A channel can be leased to multiple buyers, if these buyers can communicate simultaneously and send/receive signals with an adequate Signal to Interference and Noise Ratio (SINR).

We assume that there are n buyers, such as access points(AP), who want to lease/buy channels to carry out their works, denoted by $N = \{1, 2, \ldots, n\}$. The buyers' bids are represented as $\vec{b} = (b_1, b_2, \ldots, b_n)$. Each buyer has a per-channel valuation, which is private to himself, represented by $\vec{v} = (v_1, v_2, \ldots, v_n)$. We use $\vec{r} = (r_1, r_2, \ldots, r_n)$ to indicate the demands profile of the buyers.

We use a matrix T to indicate the allocation of the channels, where $T_{ik} = 1$ indicates that we allocate channel c_k to buyer i. What's more, we use p_{ik} to indicate the price of buyer i for using channel c_k. Utilities of the buyers are defined as the difference between his valuation and the price for using the channel. For example, price of buyer i is $\sum_{k=1}^{m} p_{ik}$. His utility after participating in this auction will be:

$$\sum_{k=1}^{m} (v_i - p_{ik})T_{ik}.$$

Following the tradition, we assume buyers are selfish and rational, which means they select strategies to maximize their utilities. The seller wisher for a channel allocation without interference, and charges ingeniously to maximize his own revenue. The revenue of the seller is the sum of the charges to the buyers, denoted by $f(\vec{b}, p)$:

$$f(\vec{b}, p) = \sum_{i=1}^{n} \sum_{k=1}^{m} p_{ik}T_{ik}.$$

B. Solution Concepts

We review some solution concepts used in this paper about *differential privacy* here.

Definition 1 (Differential Privacy [13]): A randomized function M gives ϵ-differential privacy if for any input vector $\vec{b} = (b_i, \vec{b}_{-i})$ and $\vec{b}' = (b'_i, \vec{b}_{-i})$ differing on a single item b_i's bid, where b_{-i} indicates the bid vector of other buyers except i, and all $P' \subseteq P = Range(M)$,

$$Pr[M(\vec{b}) \in P'] \leq e^{\epsilon} \times Pr[M(\vec{b'}) \in P'].$$

Definition 2 ($\Delta f - Sensitivity$ [14]): For user i, when $b'_i \neq b_i = v_i$, let Δf be the difference of $f((b'_i, \vec{b}_{-i}), p)$ and $f((b_i, \vec{b}_{-i}), p)$ over all $p \in P$. If for all $(b'_i, \vec{b}_{-i})$ over all $p \in P$, the following inequality holds, we say that the objective function $f(\vec{b}, p)$ is $\Delta f - Sensitivity$.

$$|f((b'_i, \vec{b}_{-i}), p) - f((b_i, \vec{b}_{-i}), p)| \leq \Delta f. \quad (1)$$

The solution concept of differential privacy is proposed by Dwork [2]. McSherry and Talwar [13] combined differential privacy and mechanism design for the first time.

$\Delta f - Sensitivity$ guarantees that a single bidder's misreporting has limited effects on the output. If the objective function is $\Delta f - Sensitivity$, Δf will be a deterministic value, and it cannot be manipulated by the buyer.

III. DESIGN OF DIARY

In this section, we show the design details of DIARY. DIARY uses a novel method to achieve bid privacy and approximate revenue maximization in channel allocation. For clear illustration, we discuss the scenario in which each buyer is equipped with a single radio, and can just request one channel. Multi-radio scenario can be easily extended by using elementary buyers to indicate each radio equipped.

A. Design Details

To achieve bid privacy, we use a probabilistic mechanism M_q^ϵ to determine the price for the winners. The mechanism can be divided into three phases: grouping, price determination, and winner selection.
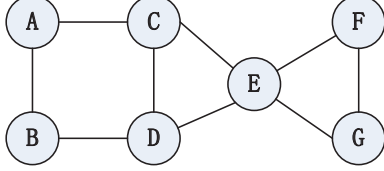
Phase 1: Grouping

Fig. 1. A simple conflict graph, in which there are 7 buyers A, B, C, D, E, F and G. The link between two buyers indicates a confliction.

As the channel has spatial reusability, we can model the confliction constraints by a conflict graph. In the conflict graph, each node indicates a buyer and each link between two buyers in the conflict graph indicates a confliction. In other words, the two buyers linked by an edge cannot work on the same channel simultaneously. With the method proposed in [22], such a conflict graph can be figured according to an adequate Signal to Interference and Noise Ratio(SINR). We divide the buyers into λ groups in a bid independent way , using existing graph coloring algorithms (e.g., [16]). The λ groups are denoted by $G = \{g_2, g_2, \ldots, g_\lambda\}$.

Fig. 1 shows a toy example, in which there are seven buyers who want to lease the channels, denoted by A, B, C, D, E, F and G. We divides all the buyers into groups. For example, in Fig. 1, the 7 elementary buyers can be divided into 3 groups: $g_1 = \{A, D, F\}$, $g_2 = \{B, E\}$ and $g_3 = \{C, G\}$ or $g_1 = \{A, E\}$, $g_2 = \{B, C, F\}$ and $g_3 = \{D, G\}$.

Phase 2: Price Determination

After dividing the buyers into non-conflicting groups, we determine the price for the winners in each group. A too low price will cause a loss to final revenue, but increasing the offered price casually has the potential to send all buyers home empty-handed. So the key point is to find an adequate price for each group to maximize the revenue of the seller.

Here, we use three steps to determine the price for each buyer group κ.

Step 1: We declare prices set P_κ.

The prices set, which is exactly the bids set in each group κ, is enumerated as follows.

$$P_\kappa = \{b_i | i \in g_\kappa\}.$$

Step 2: We calculate all potential revenues of group κ according to its all potential prices.

For each $p \in P_\kappa$, we use $\varphi_i(p)$ to indicate whether buyer i in group κ wins (can afford the price) or not.

$$\varphi_i(p) = \begin{cases} 0 & \text{if } b_i < p, \\ 1 & \text{otherwise.} \end{cases}$$

Algorithm 1 Price Determination

Input: A set of elementary buyers N, a vector of bids $\vec{b}$.
Output: A vector of price $\vec{p^*}$.

1: $(G, \lambda) = Grouping(N)$.
2: **for all** $g_\kappa \in G$ **do**
3:     **for all** $p_j \in P_\kappa$ **do**
4:         $R_\kappa(p_j) = p_j \sum_{i \in g_\kappa} \varphi_i(p_j)$.
5:         $ER_\kappa(p_j) = exp(\epsilon R_\kappa(p_j))$.
6:     **end for**
7:     $Pr_\kappa^*(0) = 0$.
8:     **for all** $j \leq |g_\kappa|$ **do**
9:         $Pr_\kappa^*(j) = \sum_{\theta \leq j} \frac{ER_\kappa(p_\theta)}{\sum_{p \in P_\kappa} ER_\kappa(p)}$.
10:     **end for**
11:     $tmp = rand(0, 1)$.
12:     **for all** $p_j \in P_\kappa$ **do**
13:         **if** $Pr_\kappa^*(j) < tmp \leq Pr_\kappa^*(j + 1)$ **then**
14:             $p_\kappa^* = p_j$.
15:             $break$.
16:         **end if**
17:     **end for**
18: **end for**
19: **return** $\vec{p^*}$.

We define the function $q(g_\kappa, \vec{b}, p)$ to calculate the revenue of group κ when the price is p:

$$q(g_\kappa, \vec{b}, p) = p \sum_{i \in g_\kappa} \varphi_i(p). \tag{2}$$

Step 3: We determine the final price of each group κ.

A probabilistic mechanism is adopted to determine the final price of each group, which is denoted by M_q^ϵ:

$$M_q^\epsilon := Pr_\kappa(p) \propto e^{\epsilon q(g_\kappa, \vec{b}, p)}.$$

Intuitively, the probability of each price p being chosen increases exponentially with its corresponding revenue. But a single participant's bid change just have limited multiplicative influence on the probability of the relevatn price being chosen.

We choose p_κ^* as the final price for the winners in group κ, the revenue of this group will be

$$q(g_\kappa, \vec{b}, p_\kappa^*) = p_\kappa^* \sum_{i \in g_\kappa} \varphi_i(p_\kappa^*). \tag{3}$$

For all the buyer groups, we use the above three steps to determine the price for the winners. A vector $\vec{p^*}$ is used to indicate final prices determined for the λ groups:

$$\vec{p^*} = (p_1^*, p_2^*, \ldots, p_\lambda^*).$$

Algorithm 1 shows the pseudo code for the price determination process. R_κ indicates the set of all the potential revenues, where the prices is in the set P_κ:

$$R_\kappa = \{R_\kappa(p) | p \in P_\kappa\}.$$

Line 3-6 calculates all the potential group revenues for group g_κ. Line 7-10 calculates the probability of p being chosen.

Algorithm 2 Winner Selection

Input: A set of buyers N, a vector of bids $\vec{b}$, a set of the idle channels C, the number of idle channels m, a vector of price $\vec{p^*}$.

Output: A set of winners W, an allocated matrix of channels T.

1: $T = 0^{n,m}$.
2: $cnt = \min\{m, \lambda\}$.
3: $G' = Sort(G)$ based on group revenue.
4: **for all** $g'_\kappa \in G'$ **do**
5:    **if** $cnt \geq 0$ **then**
6:      $cnt = cnt - 1$.
7:      **for all** $i \in g'_\kappa$ **do**
8:        **if** $\varphi_i(p^*_\kappa) == 1$ **then**
9:          $T_{i\kappa} = 1$.
10:        **end if**
11:      **end for**
12:      $WS = g'_\kappa - \{i | i \in g_\kappa, \varphi_i(p^*_\kappa) = 0\}$.
13:      $W = W \cup WS$.
14:    **end if**
15: **end for**
16: **return** W and T.

Then, Line 11-16 determines the final price p^*_κ depending on a random variable.

According to the mechanism, we can see that the possibility of the price being chosen will enjoy a exponential growth with the increase of corresponding revenue. Intuitively, the mechanism achieves approximate revenue maximization, which will be proved in Section III-B.

Phase 3: Winner Selection

We now determine the winning groups and winners in each winning group. There are m idle channels to be leased out and λ groups waiting to lease channels.

- If $\lambda \leq m$, then all the groups are winning groups.
- If $\lambda > m$, we sort the groups in non-increasing order according to the group revenue, denoted by G'. In case of a tie, we break it randomly.

$$G' : g'_1 \geq g'_2 \geq \ldots \geq g'_\kappa \geq \ldots \geq g'_\lambda.$$

We choose the first m groups with higher revenue as the winning groups in group set G'.

In each winning group g'_κ, buyers whose bid is higher than the final price are winners. Algorithm 2 shows the pseudo code for the winner selection process.

At the end of the auction, the seller collects all the payments as his revenue. To illustrate clearly, we define $Q(G, \vec{b})$ as the final revenue:

$$Q(G, \vec{b}) = \sum_{\kappa=1}^{\min\{m,\lambda\}} q(g_\kappa, \vec{b}, p^*_\kappa). \qquad (4)$$

B. Analysis

Now we are going to prove that DIARY achieves differential privacy and approximate revenue maximization.

Differential Privacy

We assume that for any group g_κ, a single buyer's bid change in $\vec{b}$ can change $q(g_\kappa, \vec{b}, p)$ by Δq, which means that the objective function $q(g_\kappa, \vec{b}, p)$ is $\Delta q - sensitivity$.

Lemma 1: When there is at most one spiteful bidder, M^ϵ_q gives $(2\epsilon\Delta q)$-differential privacy.

Proof: When there is one spiteful bidder, he just can belong to one group. Without loss of generality, we assume the spiteful bidder belongs to group g_κ. Here,

$$P'_\kappa = \{b_1, b_2, \ldots, b'_i, \ldots, b_n\}.$$

Assume a buyer i misreports his bid b_i as b'_i, for any $p \in P_\kappa$, the density of M^ϵ_q at p is equal to

$$\frac{e^{\epsilon q(g_\kappa, (b_i, \vec{b}_{-i}), p)}}{\sum_{p \in P_\kappa} e^{\epsilon q(g_\kappa, (b_i, \vec{b}_{-i}), p)}}$$
$$\leq \frac{e^{\epsilon\Delta q} \cdot e^{\epsilon q(g_\kappa, (b'_i, \vec{b}_{-i}), p')}}{e^{-\epsilon\Delta q} \cdot \sum_{p' \in P'_\kappa} e^{\epsilon q(g_\kappa, (b'_i, \vec{b}_{-i}), p')}} \qquad (5)$$
$$= e^{2\epsilon\Delta q} \cdot \frac{e^{\epsilon q(g_\kappa, (b'_i, \vec{b}_{-i}), p')}}{\sum_{p' \in P'_\kappa} e^{\epsilon q(g_\kappa, (b'_i, \vec{b}_{-i}), p')}}.$$

This gives a factor of at most $e^{\epsilon\Delta q}$ in the numerator and at least $e^{-\epsilon\Delta q}$ in the denominator, giving $e^{2\epsilon\Delta q}$ in total. Intuitively, M^ϵ_q gives $(2\epsilon\Delta q)$-differential privacy. ∎

Lemma 2: When there are at most τ spiteful bidders, M^ϵ_q gives $(2\epsilon\tau\Delta q)$-differential privacy.

Proof: The bid change of a single buyer can change q by Δq. When there are at most τ spiteful bidders, we assume that k buyers will be divided into one group. A single buyer's bid change in a group can change the revenue by Δq, then $k(k \geq 1)$ bidders' bid changes in a group can change q by $k\Delta q$. Then, no matter how the τ buyers will be divided, τ buyers' bid change can change the revenue by at most $\tau\Delta q$. Here, $\vec{b'} = (b_1, b_2, \ldots, b'_i, \ldots, b'_{i+\tau-1}, \ldots, b_n)$ and the price set P'_κ is:

$$P'_\kappa = \{b_1, b_2, \ldots, b'_i, \ldots, b'_{i+\tau-1}, \ldots, b_n\}.$$

Using Theorem 1, for any $p \in P_\kappa$, we can get that:

$$\frac{e^{\epsilon q(g_\kappa, \vec{b}, p)}}{\sum_{p \in P_\kappa} e^{\epsilon q(g_\kappa, \vec{b}, p)}}$$
$$\leq \frac{e^{\tau\epsilon\Delta q} \cdot e^{\epsilon q(g_\kappa, \vec{b'}, p)}}{e^{-\tau\epsilon\Delta q} \cdot \sum_{p' \in P'_\kappa} e^{\epsilon q(g_\kappa, \vec{b'}, p')}} \qquad (6)$$
$$= e^{2\tau\epsilon\Delta q} \cdot \frac{e^{\epsilon q(g_\kappa, \vec{b'}, p)}}{\sum_{p' \in P'_\kappa} e^{\epsilon q(g_\kappa, \vec{b}, p')}}.$$

So $(2\epsilon\tau\Delta q)$-differential privacy have been guaranteed. ∎

We can get the following theorem according to the Lemma 1 and Lemma 2:

Theorem 1: DIARY achieves ϵ^*-differential privacy.

Approximate Revenue Maximization

Lemma 3: Let $q(g_\kappa, \vec{b}, p)$ be a $\Delta q - sensitivity$ objective function and $p \in P_\kappa$. Then for any $\vec{b}$ and $0 < \epsilon < 1$, $E_{M_q^\epsilon}[q(g_\kappa, \vec{b}, p)] \geq (1 - \epsilon) \max_p q(g_\kappa, \vec{b}, p) - \delta$, where $\delta = \frac{1}{\epsilon} \ln(\frac{1}{\epsilon} |g_\kappa|)$.

Proof: For a fixed vector of bids $\vec{b}$, we denote by $\hat{P}_\kappa = \{\hat{p} \in P_\kappa : q(g_\kappa, \vec{b}, \hat{p}) < \max_p q(g_\kappa, \vec{b}, p) - \delta\}$. Then, for any $\hat{p} \in \hat{P}_\kappa$, the following holds:

$$M_q^\epsilon(\hat{p}) = \frac{e^{\epsilon q(g_\kappa, \vec{b}, \hat{p})}}{\sum_{p \in P_\kappa} e^{\epsilon q(g_\kappa, \vec{b}, p)}}$$

$$\leq \frac{e^{\epsilon(\max_p q(g_\kappa, \vec{b}, p) - \delta)}}{e^{\epsilon \max_p q(g_\kappa, \vec{b}, p)}}$$

$$= e^{-\epsilon \delta}.$$

Then we can get that $M_q^\epsilon(\hat{P}_\kappa) = \sum_{\hat{p} \in \hat{P}_\kappa} M_q^\epsilon(\hat{p}) \leq |\hat{P}_\kappa| e^{-\epsilon \delta} \leq |g_\kappa| e^{-\epsilon \delta}$. What's more, $M_q^\epsilon(P_\kappa \backslash \hat{P}_\kappa) \geq 1 - |g_\kappa| e^{-\epsilon \delta}$. The above calculation results imply:

$$\underset{M_q^\epsilon}{E}[q(g_\kappa, \vec{b}, p)]$$

$$\geq (\max_p q(g_\kappa, \vec{b}, p) - \delta) M_q^\epsilon(P_\kappa \backslash \hat{P}_\kappa)$$

$$\geq (\max_p q(g_\kappa, \vec{b}, p) - \delta)(1 - |g_\kappa| e^{-\epsilon \delta}).$$

We substitute for δ, then we get:

$$\underset{M_q^\epsilon}{E}[q(g_\kappa, \vec{b}, p)]$$

$$\geq (\max_p q(g_\kappa, \vec{b}, p) - \delta)(1 - \epsilon)$$

$$\geq (1 - \epsilon) \max_p q(g_\kappa, \vec{b}, p) - \delta.$$

Then we draw the conclusion that

$$\underset{M_q^\epsilon}{E}[q(g_\kappa, \vec{b}, p)] \geq (1 - \epsilon) \max_p q(g_\kappa, \vec{b}, p) - \delta. \quad (7)$$

∎

We use Equation 7 to all winning groups, which gives

$$\underset{M_q^\epsilon}{E} \sum_{\kappa=1}^{\min(m, \lambda)} [q(g_\kappa, \vec{b}, p)]$$

$$\geq \sum_{\kappa=1}^{\min(m, \lambda)} (1 - \epsilon) \max_p q(g_\kappa, \vec{b}, p) - \delta)$$

$$= (1 - \epsilon) \max_p Q(G, \vec{b}) - \sum_{\kappa=1}^{\min(m, \lambda)} \delta.$$

We can draw the following theorem according to Lemma 3:

Theorem 2: DIARY achieves revenue approximate maximization.

IV. NUMERICAL RESULTS

In this section, we do extensive experiments to compare the performance of DIARY with the existing mechanisms.

A. Evaluation Setup

In our evaluation setup, we assume that bidders are deployed in a large geographic area randomly, and then apply a distance-based interference model to produce the corresponding conflict graph. In our experiment, we choose 2000×2000 meters as default terrain. Any two bidders within 425 meters are supposed to conflict with each other. We assume that all bidders' true valuation is uniformly distributed over $(0, 1]$. The results are averaged over 200 runs to obtain expected results.
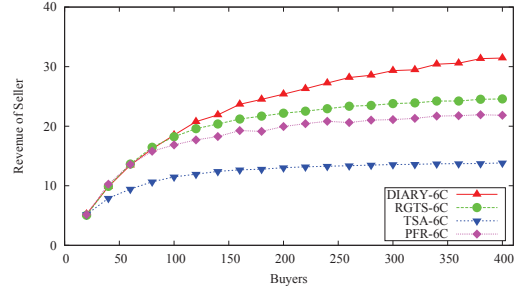
(a) There are 6 channels available.
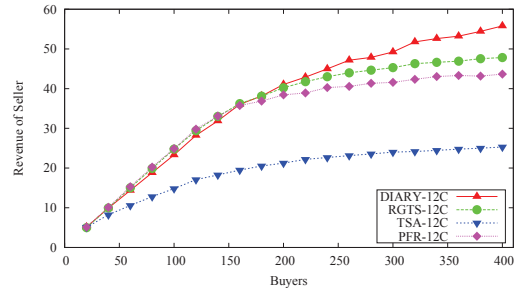
(b) There are 12 channels available.
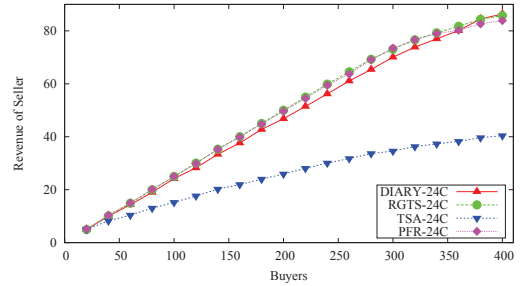
(c) There are 24 channels available.

Fig. 2. Revenue of DIARY, RGTS, TSA and PFA

B. Evaluation Results

In our first set of experimental results, we compare the revenue of DIARY with existing mechanism RGTS [11], TSA [19] and PFR [8]. In RGTS [11], the valuation of bidder is replaced by virtual valuation. We use the normal distribution here. In TSA [19], bidders are grouped into several cells, adjacent cells conflict with each other. In PFR [8], an iterative algorithm is used to determine the winner and the price.

As shown in Fig.2, DIARY outperforms other mechanisms in most cases. Fig.2 Also shows that when the number

of buyers is very small or channels are sufficient, DIARY achieves similar revenue with RGTS and PFR. We can see that the more fierce the competition is, the better performance DIARY gets.
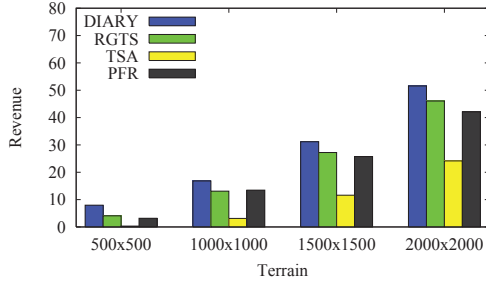

Fig. 3.   Revenue of DIARY, RGTS, TSA, PFR in different terrains

Then we compare the performance of DIARY with existing auction mechanisms in different terrains. The terrains range from 500×500 meters to 2000×2000 meters while remaining the density of bidder. We assume that there are 20, 80, 180 and 320 buyers in 500×500, 1000×1000, 1500×1500 and 2000×2000 meters respectively. The result is shown in Fig.3. DIARY produces better performance than other mechanisms in different terrain areas. As the terrain area increases or the competition gets more fierce, DIARY's advantages over RGTS, TSA and PFR become more significant.

V. RELATED WORKS

In this section, we review related works on channel allocation schemes mechanism design via differential privacy.

Recently, dynamic mechanisms of spectrum auctions has been widely concerned, especially in aspect of strategy-proof [6], [17], [21], [23] and revenue maximization [5], [11], [19]. However, the existing revenue maximization mechanisms all lose sight of the importance of bid privacy, which may cause a series of negative influence. Only a handful of work [9] guarantee the privacy of bidders, but compromising the revenue unfortunately.

Since the revenue maximization is well-studied, the novel idea of our work is that we achieve bid privacy via differential privacy. So here we focus on the related works about differential privacy. Dwork [2] proposed the solution concept of differential privacy for the first time, then McSherry and Talwar [13] combined the differential privacy and mechanism design, and gave a general method to deal with revenue maximization in unlimited supply auction, attribute auctions and constrained pricing problems. Dwork [4] introduced the definition of differential privacy and two basic techniques for achieving differential privacy, meanwhile showed some interesting applications of the techniques. Recently, Xiao [18] argued that the study of privacy must be coupled with the study of incentives, and introduced a model combining differential privacy with truthfulness and efficiency. Nissim et al. [15] designed an general approximately optimal mechanism via differential privacy. Nissim et al. [14] also modeled the privacy-aware agents and designed a privacy-aware mechanism via differential privacy.

VI. CONCLUSION

In this paper, we have designed DIARY, which is a differentially private and approximately revenue maximizing auction mechanism for secondary spectrum markets. We have proven that DIARY not only achieves differential privacy but also achieves approximate revenue maximization. The experimental results have shown that DIARY outperforms the existing mechanisms.

REFERENCES

[1] "Spectrum bridge," http://www.spectrumbridge.com.
[2] C. Dwork, "Differential privacy," in *Automata, languages and programming*, 2006.
[3] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography*, 2006.
[4] C. Dwork, "Differential privacy: A survey of results," in *Theory and Applications of Models of Computation*, 2008.
[5] S. Gandhi, C. Buragohain, L. Cao, H. Zheng, and S. Suri, "A general framework for wireless spectrum auctions," in *DySPAN*, 2007.
[6] L. Gao, X. Wang, Y. Xu, and Q. Zhang, "Spectrum trading in cognitive radio networks: A contract-theoretic modeling approach," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 843–855, 2011.
[7] L. Gao, Y. Xu, and X. Wang, "Map: Multiauctioneer progressive auction for dynamic spectrum access," *IEEE Transactions on Mobile Computing*, vol. 10, no. 8, pp. 1144–1161, 2011.
[8] A. Gopinathan and Z. Li, "A prior-free revenue maximizing auction for secondary spectrum access," in *INFOCOM*, 2011.
[9] Q. Huang, Y. Tao, and F. Wu, "Spring: A strategy-proof and privacy preserving spectrum auction mechanism," in *INFOCOM*, 2013.
[10] Z. Huang and S. Kannan, "The exponential mechanism for social welfare: Private, truthful, and nearly optimal," in *FOCS*, 2012.
[11] J. Jia, Q. Zhang, Q. Zhang, and M. Liu, "Revenue generation for truthful spectrum auction in dynamic spectrum access," in *MobiHoc*, 2009.
[12] M. A. McHenry, P. A. Tenhula, D. McCloskey, D. A. Roberson, and C. S. Hood, "Chicago spectrum occupancy measurements & analysis and a long-term studies proposal," in *Proceedings of the first international workshop on Technology and policy for accessing spectrum*, 2006.
[13] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *FOCS*, 2007.
[14] K. Nissim, C. Orlandi, and R. Smorodinsky, "Privacy-aware mechanism design," in *EC*, 2012.
[15] K. Nissim, R. Smorodinsky, and M. Tennenholtz, "Approximately optimal mechanism design via differential privacy," in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, 2012.
[16] D. B. West, *Introduction to Graph Theory, Second edition*. Prentice Hall, 1996.
[17] F. Wu and N. Vaidya, "Small: A strategy-proof mechanism for radio spectrum allocation," in *INFOCOM*, 2011.
[18] D. Xiao, "Is privacy compatible with truthfulness?" *IACR Cryptology ePrint Archive*, vol. 2011, p. 5, 2011.
[19] D. Yang, X. Fang, and G. Xue, "Truthful auction for cooperative communications with revenue maximization," in *ICC*, 2012.
[20] W. Yue, "Analytical methods to calculate the performance of a cellular mobile radio communication system with hybrid channel assignment," *IEEE transactions on vehicular technology*, vol. 40, no. 2, pp. 453–460, 1991.
[21] X. Zhou, S. Gandhi, S. Suri, and H. Zheng, "ebay in the sky: strategy-proof wireless spectrum auctions," in *MOBICOM*, 2008.
[22] X. Zhou, Z. Zhang, G. Wang, X. Yu, B. Y. Zhao, and H. Zheng, "Practical conflict graphs for dynamic spectrum distribution," in *SIGMETRICS*, 2013.
[23] X. Zhou and H. Zheng, "Trust: A general framework for truthful double spectrum auctions," in *INFOCOM*, 2009.
[24] Y. Zhou and R. Lukose, "Vindictive bidding in keyword auctions." in *EC*, 2007.