

Designing differentially private spectrum auction mechanisms

Chunchun Wu¹ · Zuying Wei¹ · Fan Wu¹ · Guihai Chen¹ · Shaojie Tang²

© Springer Science+Business Media New York 2015

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 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. Furthermore, we present an effective method to address the fairness issue in spectrum auctions. Results from extensive evaluations show that DIARY has substantial competitive advantages over existing mechanisms.

Keywords Mechanism design · Differential privacy · Fairness · Resource allocation

✉ Fan Wu
fwu@cs.sjtu.edu.cn
Chunchun Wu
bubble_chun@sjtu.edu.cn
Zuying Wei
zu_ying_hi@sjtu.edu.cn
Guihai Chen
gchen@cs.sjtu.edu.cn
Shaojie Tang
tangshaojie@gmail.com

¹ Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China

² Department of Information Systems, University of Texas at Dallas, Richardson, TX, USA

1 Introduction

Recent years have witnessed the fast development of wireless technology, which has brought a great increase in demand of spectrum resources. Spectrum is a scarce commodity controlled by governmental agencies (e.g., Federal Communications Commission (FCC) [9] in the 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 [20]. The current problem of spectrum allocation 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 (e.g., [5, 26, 31, 33]). Recently companies, such as Spectrum Bridge [1], have emerged to facilitate trading of idle spectrum, making dynamic spectrum redistribution no longer merely theoretical.

Auctions are well-studied protocols in economic theory for allocating scarce resources, and are attractive because of their well-defined notions for various objectives. A major difference between traditional 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 is that spectrum auctions are held repeatedly due to the dramatic changes of spectrum utilization. Most of previous studies on this issue neglect

the repeatability of spectrum auctions, and only greedily maximize one time revenue, resulting in a set of secondary users starving for spectrum. Such starvation not only abate victims' enthusiasm for participating in the auctions, which reduces long-term revenue of the primary users, but also may cause vindictive actions from secondary users who never have a chance to win [34]. Aiming at avoiding such negative influences, it is reasonable and desired to maintain a trade-off between revenue and fairness.

Furthermore, due to the repeatability of spectrum auctions, clues about others' private information may be revealed from historical records or previous rounds, so that spiteful secondary users can use such information to perform malicious manipulations, e.g., cheating and collusion. 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 (e.g., [16, 28]), which make participators bid truthfully in order to guarantee strategy-proofness or revenue maximization, obviously violate the bid privacy. The recent notion of *differential privacy* [6, 8], in addition with its own intrinsic virtue, can assure that participants have limited effect on the outcome of the mechanisms. Consequently, 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. However, designing such an auction mechanism has its own challenges:

- *Computational Complexity*: It has been shown that to find optimal solutions to the general problem of the channel allocation is NP-complete [4, 29], which means that 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, differentially private mechanisms belonging to the family of exponential mechanisms [15, 23] cannot be adopted directly.
- *Fairness*: Providing the guarantee of the fairness may sacrifice seller's total revenue. Therefore, the problem of balancing revenue maximization and fairness should be well studied.

In this paper, we propose DIARY, which is a Differentially private and Approximately Revenue maximizing auction mechanism for secondary spectrum markets. DIARY not only achieves approximate revenue maximization, but also guarantees bid privacy. 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. Then we extend DIARY to support multi-radio spectrum auction, and prove that the enhanced DAIRY also performs well.
- Third, We also do some simple but effective improvements to achieve fairness, which guarantee a minimum probability for every bidder to win the spectrum auction.
- Last but not least, we conduct extensive evaluations to compare the performance of DIARY with existing mechanisms RGTS [16], TSA [28], and PFR [11]. Evaluation results show that DIARY has substantial competitive advantages over existing mechanisms, especially when the competition for channels is intense.

The rest of this paper is organized as follows. In Sect. 2, we introduce our auction model and review some solution concepts. In Sect. 3, we show the design of our auction mechanism DIARY in a single-radio scenario, then we extend our mechanism to multi-radio scenario in Sect. 4. Section 5 presents the auction mechanism with fairness constraints. Extensive evaluations are demonstrated in Sect. 6 to compare the performance of the proposed mechanism with others. In Sect. 7, we discuss the related works. In the end, we draw our conclusion in Sect. 8.

2 Preliminaries

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

2.1 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 $C = \{c_1, c_2, \dots, c_m\}$. 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 $N = \{1, 2, \dots, n\}$. Each buyer is equipped with one or more radios, and can request one or more channels. The buyers' bids are represented as

$\mathbf{b} = (b_1, b_2, \dots, b_n)$. Each buyer has a per-channel valuation, which is private to himself, represented by $\mathbf{v} = (v_1, v_2, \dots, v_n)$. We use $\mathbf{r} = (r_1, r_2, \dots, r_n)$ 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 wishes 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 $f(\mathbf{b}, p)$:

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

2.2 Solution concepts

We review some solution concepts used in this paper about *differential privacy* here. Differential privacy has been studied extensively in the community of theoretical computer science. It guarantees that the probability distributions of possible outcomes are nearly identical, when the (input) data profiles are nearly identical. Formally,

Definition 1 (Differential Privacy [21]) A randomized function M gives ϵ -differential privacy if for any input vector $\mathbf{b} = (b_i, \mathbf{b}_{-i})$ and $\mathbf{b}' = (b'_i, \mathbf{b}_{-i})$ differing on a single item b_i , where \mathbf{b}_{-i} indicates the input vector of other users except i , and all $P' \subseteq P = \text{Range}(M)$,

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

Definition 2 (Af-Sensitivity [22]) For user i , when $b'_i \neq b_i = v_i$, let Δf be the difference of $f((b'_i, \mathbf{b}_{-i}), p)$ and $f((b_i, \mathbf{b}_{-i}), p)$ over all $p \in P$. If for all (b'_i, \mathbf{b}_{-i}) over all $p \in P$, the following inequality holds, we say that the objective function $f(\mathbf{b}, p)$ is *Af-Sensitivity*.

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

The solution concept of differential privacy is proposed by Dwork [6]. *Af-Sensitivity* guarantees that a single user's misreporting has limited effects on the output. If the objective function is *Af-Sensitivity*, Δf will

be a deterministic value, and it cannot be manipulated by the user.

When integrating differential privacy with an auction mechanism, the input data would be buyers' bid vectors, and two neighbouring profiles differ in only one bid (added, removed or changed). A differentially private mechanism M can address the concern of personal input leakage. In an auction, any change in a buyer's bid won't bring significant changes to the outcome, and thus, the others cannot infer information of this particular buyer just from the outcomes.

A powerful tool in the literature of differential privacy is the exponential mechanism proposed by McSherry and Talwar [21]. The goal of a privacy mechanism is to map, randomly, a set of n inputs each from a domain D to some output in a range P .

Definition 3 (Exponential Mechanism [21]) Given a range P , a data profile \mathbf{b} , an objective function q , and a small constant ϵ , the exponential mechanism M_q^ϵ chooses an outcome p from the range P with probability

$$\Pr[M_q^\epsilon(\mathbf{b}) = p] \propto e^{\epsilon q(\mathbf{b}, p)}.$$

Intuitively, a small additive change to $q(\mathbf{b}, p)$ as might be caused by a single participant, has a limited multiplicative influence on the density of any output, guaranteeing differential privacy. Nonetheless, the probability associated with an output p increases exponentially with its score on the input \mathbf{b} , substantially biasing the distribution towards high scoring outputs and bringing the expected score close to the optimum.

3 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. We will consider the extended model in which buyers are equipped with multiple radios and bid for multiple channels in Sect. 4.

3.1 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.

As the channel has spatial reusability, we can model the conflict 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 conflict. In other words, the two buyers linked by an edge cannot work on the same channel simultaneously. With the method proposed in [32], 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., [25]). The λ groups are denoted by $G = \{g_1, g_2, \dots, g_\lambda\}$.

Figure 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 divide 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 $g_3 = \{D, G\}$.

3.1.1 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.

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

As for the reason why the optimal price would certainly be one of the bids is because if the price is not one of bids, we can increase the price slightly (not exceeding any higher bids), then the number of winners who can afford the price will not change but the total revenue increases.

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 bid) or not.

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

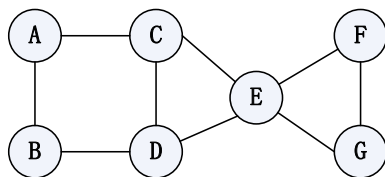


Fig. 1 A simple conflict graph, in which there are seven buyers A, B, C, D, E, F and G. The link between two buyers indicates a confliction

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

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

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^e :

$$M_q^e := Pr_\kappa(p) \propto e^{eq(g_\kappa, \mathbf{b}, p)}.$$

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 relevant price being chosen.

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

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

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

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

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. 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 Sect. 3.2. What's more, a small change in bid vector \mathbf{b} (maybe a single buyer's bid change) will not give much difference to the possibility of corresponding p_κ and revenue, which also can be seen in Sect. 3.2.

3.1.2 Phase 3: Winner selection

In Phase 2, we have determined the price for the winners of each winning group. 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.

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

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 $Q(G, \mathbf{b})$ as the final revenue:

$$Q(G, \mathbf{b}) = \sum_{\kappa=1}^{\min\{m, \lambda\}} q(g_\kappa, \mathbf{b}, p_\kappa^*). \quad (4)$$

3.2 Analysis

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

ALGORITHM 1: Price Determination

Input: A set of elementary buyers N , a vector of bids \mathbf{b} .

Output: A vector of price \mathbf{p}^* .

```

1:  $(G, \lambda) = \text{Grouping}(N)$ .
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:      $ER_\kappa(p_j) = \text{exp}(\epsilon R_\kappa(p_j))$ .
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:   $tmp = \text{rand}(0, 1)$ .
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  $\mathbf{p}^*$ .
```

ALGORITHM 2: Winner Selection

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

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

```

1:  $T = 0^{n, m}$ .
2:  $cnt = \min\{m, \lambda\}$ .
3:  $G' = \text{Sort}(G)$  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  $T$ .
```

3.2.1 Differential Privacy

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

Lemma 1 When each buyer is equipped with a single radio and there is at most one spiteful bidder, M_q^ϵ 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,

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

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

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

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

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_q^ϵ gives $(2\epsilon\Delta q)$ -differential privacy. \square

Lemma 2 When each buyer is equipped with a single radio and there are at most τ spiteful bidders, M_q^ϵ gives $(2\epsilon\tau\Delta q)$ -differential privacy.

Proof The bid change of a single buyer, who is equipped with a single radio, 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, $\mathbf{b}' = (b_1, b_2, \dots, b'_i, \dots, b'_{i+\tau-1}, \dots, b_n)$ and the price set P'_κ is:

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

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

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

$$= e^{2\tau\epsilon\Delta q} \cdot \frac{e^{\epsilon q(g_\kappa, \mathbf{b}', p)}}{\sum_{p' \in P'_\kappa} e^{\epsilon q(g_\kappa, \mathbf{b}, p')}}.$$

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 When each buyer is equipped with a single radio, DIARY achieves ϵ^* -differential privacy.

3.2.2 Approximate Revenue Maximization

In this subsection, we will prove that our channel auction mechanism DIARY achieves approximate revenue maximization. Without loss of generality, we first prove that the group revenue $q(g_\kappa, \mathbf{b}, p)$ of group g_κ can achieve the approximate revenue maximization when DIARY is used.

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

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

$$M_q^\epsilon(\hat{p}) = \frac{e^{\epsilon q(g_\kappa, \mathbf{b}, \hat{p})}}{\sum_{p \in P_\kappa} e^{\epsilon q(g_\kappa, \mathbf{b}, p)}} \leq \frac{e^{\epsilon(\max_p q(g_\kappa, \mathbf{b}, p) - \delta)}}{e^{\epsilon \max_p q(g_\kappa, \mathbf{b}, p)}} = e^{-\epsilon\delta}.$$

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

$$\begin{aligned} E_{M_q^\epsilon}[q(g_\kappa, \mathbf{b}, p)] &\geq (\max_p q(g_\kappa, \mathbf{b}, p) - \delta) M_q^\epsilon(P_\kappa \setminus \hat{P}_\kappa) \\ &\geq (\max_p q(g_\kappa, \mathbf{b}, p) - \delta) (1 - |g_\kappa| e^{-\epsilon\delta}). \end{aligned}$$

We substitute for δ , then we get:

$$\begin{aligned} E_{M_q^\epsilon}[q(g_\kappa, \mathbf{b}, p)] &\geq (\max_p q(g_\kappa, \mathbf{b}, p) - \delta) (1 - \epsilon) \\ &\geq (1 - \epsilon) \max_p q(g_\kappa, \mathbf{b}, p) - \delta \end{aligned}$$

Then we draw the conclusion that

$$E_{M_q^\epsilon}[q(g_\kappa, \mathbf{b}, p)] \geq (1 - \epsilon) \max_p q(g_\kappa, \mathbf{b}, p) - \delta. \tag{7}$$

We use Eq. 7 to all winning groups, which gives

$$\begin{aligned} E_{M_q^\epsilon} \sum_{\kappa=1}^{\min(m, \lambda)} [q(g_\kappa, \mathbf{b}, p)] &\geq \sum_{\kappa=1}^{\min(m, \lambda)} (1 - \epsilon) \max_p q(g_\kappa, \mathbf{b}, p) - \delta \\ &= (1 - \epsilon) \max_p Q(G, \mathbf{b}) - \sum_{\kappa=1}^{\min(m, \lambda)} \delta. \end{aligned}$$

We can draw the following theorem according to Lemma 3:

Theorem 2 DIARY achieves revenue approximate maximization.

4 Extending DIARY to multi-radio scenario

In the previous section, we considered the scenario in which each buyer only has a single radio. In reality, some access points may be equipped with multiple radios. In this section,

we will extend our mechanism DIARY to the multi-radio buyer scenario.

4.1 Design of DIARY in multi-radio scenario

In multi-radio buyer scenario, each buyer is equipped with one or more radios, and can request one or more channels in the auction. Note that, all channels are homogeneous except for their identify number. In other words, the utility of a buyer for receiving any channel is equal. Hence, we assume that buyer bids equally for each channel he requests.

When buyer i is equipped with r_i radios, we use r_i elementary buyers to represent buyer i in the conflict graph. Actually, a buyer who is equipped with only one radio is an elementary buyer himself. We use N' to denote the set of elementary buyers. Since the elementary buyers, who indicate the radios belonging to the same buyer, cannot work on the same channel, we link them by an edge in the conflict graph. We also use an edge to link the elementary buyers who inherit the confliction condition of their parents. We make an assumption that the buyer who request multiple channels can do part of his work if his demands are semi-satisfied.

For example, in Fig. 2, Buyer A , B and C is equipped with 3, 2 and 1 radio, respectively. So totally there are 6 elementary buyers in the conflict graph. Note that elementary buyers A^1 , A^2 and A^3 represent the three radios equipped by buyer A , which mutually conflict with each other. Similarly, elementary buyers B^1 and B^2 represent the two radios equipped by buyer B and elementary buyer C is the buyer C himself.

After using elementary buyers to indicate the radios equipped by multi-radio buyers, DIARY can be directly applied in multi-radio buyer scenario.

4.2 Analysis

In this subsection, we prove that when DIARY is used in multi-radio buyer scenario, DIARY still achieves

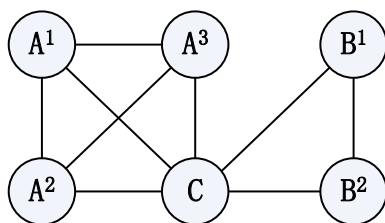


Fig. 2 A simple conflict graph, in which there are three buyers A , B and C . Buyer A , B and C is equipped with 3, 2 and a single radio respectively. The node represents an elementary buyer and the link between two elementary buyers indicates the confliction

differential privacy. Actually in multi-radio buyer scenario, an elementary buyer is equal to a buyer in single radio buyer scenario. Therefore, DIARY achieves differential privacy and approximate revenue maximization.

Lemma 4 When each buyer is equipped with r radios and there is at most one spiteful bidders, M_q^ϵ gives $(2\epsilon r \Delta q)$ -differential privacy.

Lemma 5 When each buyer is equipped with r radios and there is at most τ spiteful bidders, M_q^ϵ gives $(2\epsilon r \tau \Delta q)$ -differential privacy.

The proof is similar to the single-radio scenario. Due to the space limit, we will not give the proof here. If you are interested, feel free to contact us for details. We can get the following theorem according to Lemma 4, and Lemma 5:

Theorem 3 When DIARY is used, mechanism M_q^ϵ achieves ϵ^* -differential privacy.

5 Fairness in DIARY

In Sect. 3, we have shown the design of DIARY which aims to maximize the revenue via differential privacy. However, DIARY doesn't take fairness into account, which may cause a series of negative influence. Due to the fact that buyers in losing groups are all disqualified in current round (they even have no chance to be treated unfairly), we consider the fairness to provide a minimum service guarantee in each winning group.

5.1 Design of DIARY-with-fairness

We make some simple but effective improvements to DIARY to achieve fairness. Our fairness constraints are designed to ensure a minimum probability vector \mathbf{t} of getting the spectrum resource for buyers in each winning group.

Intuitively, in a winning group, the buyer with the lowest bid may have the lowest probability to get spectrum. We assume that buyers in a winning group are numbered in non-decreasing order of bid:

$$\hat{b} = (b_1, b_2, \dots, b_{|g_\kappa|}).$$

Let $Pr_\kappa(b_i)$ denote the probability of b_i being chosen as the final price in group g_κ . For every buyer i , the probability of getting what he wants is the sum of probabilities of all bids lower than b_i to be chosen as the final price. Formally, the probability of buyer i to win in the auction is:

$$Pr'_\kappa(b_i) = \sum_{j=1}^i Pr_\kappa(b_j).$$

Clearly, the probability of buyer with the lowest bid to win is the lowest, and is equal to the probability to be chosen as the final price. Only when the price is exactly his own bid, he can afford to buy the channels and carry out his work.

Our goal of considering fairness is improving the bidders' lowest probabilities to get channels without violating the rule that, the probability of prices being chosen is positive correlative with the corresponding revenues.

We must make sure that, no matter how we choose t_κ , we will not violate the original rule. We consider a case where $q(g_\kappa, \mathbf{b}, b_{min})$ is the lowest revenue. The highest probability of b_{min} to be chosen must be lower than $\frac{1}{|g_\kappa|}$. In other words, no matter how we choose t_κ , t_κ cannot be higher than $\frac{1}{|g_\kappa|}$. Therefore, we set the adjustment range of t_κ as:

$$0 < t_\kappa < \frac{1}{|g_\kappa|}. \tag{8}$$

Let b_{min} denote the lowest bid. We can calculate $Pr_\kappa(b_{min})$ as:

$$Pr_\kappa(b_{min}) = \frac{e^{\epsilon q(g_\kappa, \mathbf{b}, b_{min})}}{\sum_{p \in P_\kappa} e^{\epsilon q(g_\kappa, \mathbf{b}, p)}}.$$

To achieve fairness, we make a simple, but effective change to the probabilistic mechanism, for any $p \in P_\kappa$:

$$\hat{M}_q^\epsilon := \hat{Pr}_\kappa(p) \propto e^{\epsilon q(g_\kappa, \mathbf{b}, p)} + \gamma_\kappa.$$

To guarantee the probability $\hat{Pr}_\kappa(p) \geq 0$, we add the constraint:

$$\gamma_\kappa \geq - \min_{p \in P_\kappa} e^{\epsilon q(g_\kappa, \mathbf{b}, p)}.$$

What's more, when $Pr_\kappa(b_{min}) \geq t_\kappa$, the lowest probability of being satisfied in group g_κ is higher than t_κ , so it's not necessary for us to consider fairness. Then, when $Pr_\kappa(b_{min}) \geq t_\kappa$, we set $\gamma_\kappa = 0$.

Now what we need to do is to ensure the buyer with lowest bid in winning group g_κ having at least probability t_κ to win.

$$\begin{aligned} \hat{Pr}_\kappa(b_{min}) &= \frac{e^{\epsilon q(g_\kappa, \mathbf{b}, b_{min})} + \gamma_\kappa}{\sum_{p \in P_\kappa} (e^{\epsilon q(g_\kappa, \mathbf{b}, p)} + \gamma_\kappa)} \\ &= \frac{e^{\epsilon q(g_\kappa, \mathbf{b}, b_{min})} + \gamma_\kappa}{\sum_{p \in P_\kappa} e^{\epsilon q(g_\kappa, \mathbf{b}, p)} + |g_\kappa| \gamma_\kappa} \\ &\geq t_\kappa \end{aligned}$$

Here, $0 < t_\kappa < \frac{1}{|g_\kappa|}$, and $\gamma_\kappa \geq - \min_{p \in P_\kappa} e^{\epsilon q(g_\kappa, \mathbf{b}, p)}$. γ_κ is a adjustable parameter depending on t_κ .

$$\gamma_\kappa \geq \frac{\sum_{p \in P_\kappa} e^{\epsilon q(g_\kappa, \mathbf{b}, p)} t_\kappa - e^{\epsilon q(g_\kappa, \mathbf{b}, b_{min})}}{1 - |g_\kappa| t_\kappa} \tag{9}$$

According to the range of t_κ , we can get that $\gamma_\kappa > 0$. When γ_κ subjects to the constraint (9), DIARY-with-Fairness achieves the fairness, which means buyers are guaranteed a minimum probability of getting service.

5.2 Analysis

In this section, we prove that DIARY-with-Fairness achieves differential privacy and approximate revenue maximization.

5.2.1 Differential Privacy

Lemma 6 When each buyer is equipped with a single radio and there is at most one spiteful bidder, \hat{M}_q^ϵ gives $(2\epsilon\Delta q)$ -differential privacy.

Proof Similar with Lemma 1, we assume a buyer i mis-reporting his bid b_i as b'_i , then P_κ will be:

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

Then for any $p \in P_\kappa$, the density of \hat{M}_q^ϵ at p is equal to

$$\begin{aligned} &\frac{e^{\epsilon q(g_\kappa, (b_i, \mathbf{b}_{-i}), p)} + \gamma_\kappa}{\sum_{p \in P_\kappa} (e^{\epsilon q(g_\kappa, (b_i, \mathbf{b}_{-i}), p)} + \gamma_\kappa)} \\ &\leq \frac{e^{\epsilon\Delta q} \cdot e^{\epsilon q(g_\kappa, (b'_i, \mathbf{b}_{-i}), p)} + \gamma_\kappa}{e^{-\epsilon\Delta q} \cdot \sum_{p' \in P'_\kappa} e^{\epsilon q(g_\kappa, (b'_i, \mathbf{b}_{-i}), p')} + |g_\kappa| \gamma_\kappa} \tag{10} \\ &\leq e^{2\epsilon\Delta q} \cdot \frac{e^{\epsilon q(g_\kappa, (b'_i, \mathbf{b}_{-i}), p)} + \gamma_\kappa}{\sum_{p' \in P'_\kappa} (e^{\epsilon q(g_\kappa, (b'_i, \mathbf{b}_{-i}), p')} + \gamma_\kappa)}. \end{aligned}$$

We can see from Eq. 10, M_q^ϵ gives $(2\epsilon\Delta q)$ -differential privacy.

When each buyer is equipped with multiple radios and at most τ buyers misreport in the auction, we can get similar results. Due to space limit, we will not give the proof. According to Theorems 1, and 3, we can get the following theorem:

Theorem 4 DIARY-with-Fairness achieves ϵ^* -differential privacy.

5.2.1.1 Approximate revenue maximization

Lemma 7 Let $q(g_\kappa, \mathbf{b}, p)$ be a Δq -sensitivity objective function and $p \in P_\kappa$. Then for any \mathbf{b} and $0 < \epsilon < 1$, $E_{M_q^\epsilon}[q(g_\kappa, \mathbf{b}, p)] \geq (1 - \epsilon - |g_\kappa| \eta) \max_p q(g_\kappa, \mathbf{b}, p) - \delta$, where $\eta = \frac{\gamma_\kappa}{e^{\max_p q(g_\kappa, \mathbf{b}, p)} + |g_\kappa| \gamma_\kappa}$ and $\delta = \frac{1}{\epsilon} \ln(\frac{1}{\epsilon} |g_\kappa|)$.

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

$$\begin{aligned}
 M_q^\epsilon(\hat{p}) &= \frac{e^{\epsilon q(g_\kappa, \mathbf{b}, \hat{p})} + \gamma_\kappa}{\sum_{p \in P_\kappa} (e^{\epsilon q(g_\kappa, \mathbf{b}, p)} + \gamma_\kappa)} \\
 &\leq \frac{e^{\epsilon(\max_p q(g_\kappa, \mathbf{b}, p) - \delta)} + \gamma_\kappa}{e^{\epsilon \max_p q(g_\kappa, \mathbf{b}, p)} + |g_\kappa| \gamma_\kappa} \\
 &\leq e^{-\epsilon \delta} + \frac{\gamma_\kappa}{e^{\epsilon \max_p q(g_\kappa, \mathbf{b}, p)} + |g_\kappa| \gamma_\kappa} \\
 &= e^{-\epsilon \delta} + \eta.
 \end{aligned}$$

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

$$\begin{aligned}
 E_{M_q^\epsilon} [q(g_\kappa, \mathbf{b}, p)] &\geq (\max_p q(g_\kappa, \mathbf{b}, p) - \delta) M_q^\epsilon(P_\kappa \setminus \hat{P}_\kappa) \\
 &\geq (\max_p q(g_\kappa, \mathbf{b}, p) - \delta) (1 - |g_\kappa| (e^{-\epsilon \delta} + \eta)).
 \end{aligned}$$

We substitute for δ , then we get:

$$\begin{aligned}
 E_{M_q^\epsilon} [q(g_\kappa, \mathbf{b}, p)] &\geq (\max_p q(g_\kappa, \mathbf{b}, p) - \delta) (1 - \epsilon - |g_\kappa| \eta) \\
 &= (1 - \epsilon - |g_\kappa| \eta) (\max_p q(g_\kappa, \mathbf{b}, p) - \delta) \\
 &\geq (1 - \epsilon - |g_\kappa| \eta) \max_p q(g_\kappa, \mathbf{b}, p) - \delta.
 \end{aligned}$$

Then we draw the conclusion that

$$E_{M_q^\epsilon} [q(g_\kappa, \mathbf{b}, p)] \geq (1 - \epsilon - |g_\kappa| \eta) \max_p q(g_\kappa, \mathbf{b}, p) - \delta. \tag{11}$$

We use Eq. 11 to all the winning groups, which gives

$$\begin{aligned}
 E_{M_q^\epsilon} \sum_{\kappa=1}^{\min(m, \lambda)} [q(g_\kappa, \mathbf{b}, p)] &\geq \sum_{\kappa=1}^{\min(m, \lambda)} ((1 - \epsilon - |g_\kappa| \eta) \max_p q(g_\kappa, \mathbf{b}, p) - \delta) \\
 &\geq \sum_{\kappa=1}^{\min(m, \lambda)} ((1 - \epsilon - \max(|g_\kappa|) \cdot \eta) \max_p q(g_\kappa, \mathbf{b}, p) - \delta) \\
 &= (1 - \epsilon - \max(|g_\kappa|) \cdot \eta) \max_p Q(G, \mathbf{b}) - \sum_{\kappa=1}^{\min(m, \lambda)} \delta.
 \end{aligned}$$

We can draw the following theorem according to Lemma 7:

Theorem 5 When mechanism \hat{M}_q^ϵ is used, DIARY-with-Fairness achieves approximate revenue maximization.

6 Numerical results

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

6.1 Evaluation setup

In our evaluation setup, we assume that there are 6, 12, or 24 idle channels available and evaluate the cases in which each buyer is equipped with a single radio or 3 radios. We also 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 evaluation, we choose 2000×2000 square meters as default terrain. Any two bidders within 425 meters are supposed to conflict with each other, i.e., they can not share the same channel. We assume that all bidders' true valuation is uniformly distributed over $(0, 1]$. The results are averaged over 200 runs to obtain expected results. In the evaluation results of DIARY with Fairness, we set the range of t_κ of each group g_κ as $(0, \frac{1}{|g_\kappa|})$ (Eq. 8). To illustrate clearly, we use u and v to denote $Pr_\kappa(b_{min})$ and $\frac{1}{|g_\kappa|}$ in each group g_κ , respectively.

6.2 Evaluation results

In our first set of evaluation results, we compare the revenue of DIARY with existing mechanisms RGTS [16], TSA [28] and PFR [11]. In RGTS [16], the valuation of bidder is replaced by virtual valuation. We use the normal distribution here. In TSA [28], bidders are grouped into several cells, adjacent cells conflict with each other. In PFR [11], an iterative algorithm is used to determine the winner and the price.

As shown in Fig. 3, DIARY outperforms other mechanisms in most cases. Figure 3 Also shows that when the number of buyers is very small or channels are sufficient, DIARY achieves similar revenue with RGTS and PFR. When each buyer is equipped with 3 radios, the number of elementary buyer is three times larger than the number of buyers in single-radio scenario. Figure 4(a)–(c) show the evaluation results when there are 6, 12 and 24 channels available and each buyer is equipped with three radios. We can see that the intenser the competition is, the better performance DIARY gets.

Then we compare the performance of DIARY with existing auction mechanisms in different terrains. The terrains range from 500×500 square meters to 2000×2000 square meters while remaining the density of buyers. We assume that there are 20, 80, 180 and 320 buyers in 500×500 , 1000×1000 , 1500×1500 and 2000×2000 square meters respectively.

The result is shown in Fig. 5. DIARY produces better performance than other mechanisms in different terrain areas. We can see from Fig. 5(a), (b) that as the terrain area increases or the competition gets intenser, DIARY's advantages over RGTS, TSA and PFR become more significant.

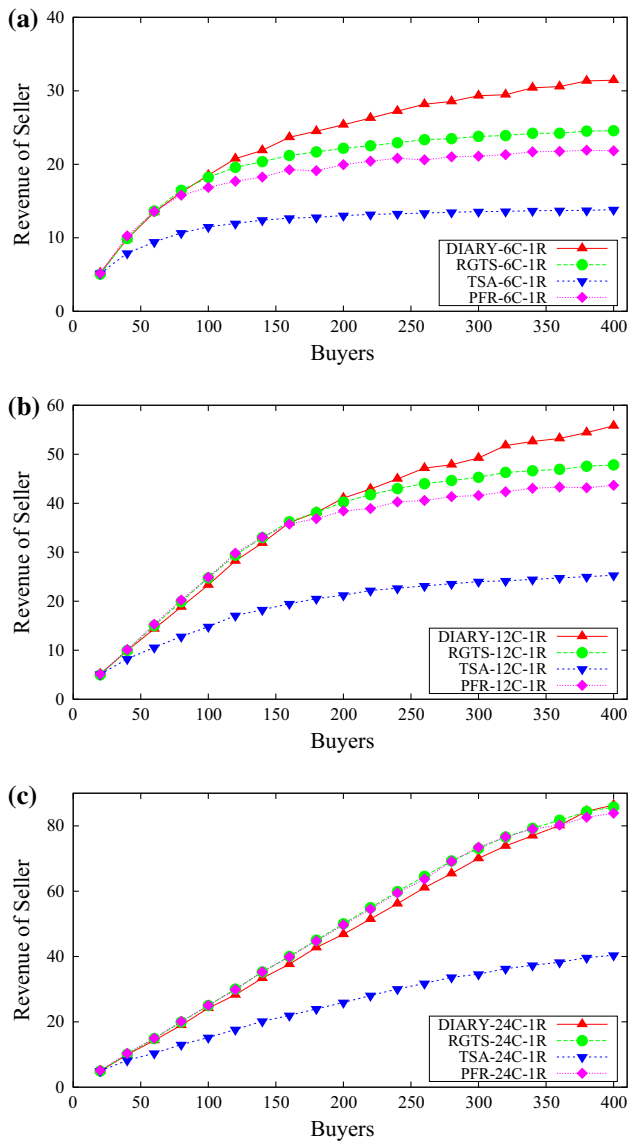


Fig. 3 Revenue of DIARY, RGTS, TSA and PFA with single radio. **a** 6 Channels available with single radio. **b** 12 Channels available with single radio. **c** 24 Channels available with single radio

In our third set of evaluation results, we change the t_κ of each group g_κ continuously. Then we choose $t_\kappa = \frac{d}{2}$ to observe the tradeoff between fairness and revenue, where $d = \frac{v-u}{4}$. Figure 6 shows the revenue changes according to different t_κ . We can see from Fig. 6 that, when we change t_κ in $(0, v)$, DIARY and DIARY-with-Fairness achieve the same revenue. The reason for this phenomenon is that when $t_\kappa \leq Pr_\kappa(b_{min})$, $\gamma_\kappa = 0$, which means there is no need to make any adjustment for fairness. When $t_\kappa \geq Pr_\kappa(b_{min})$, DIARY-with-Fairness conducts a little lower performance than DIARY. No matter how many radios each buyer is equipped with, we can achieve fairness without sacrificing the revenue severely.

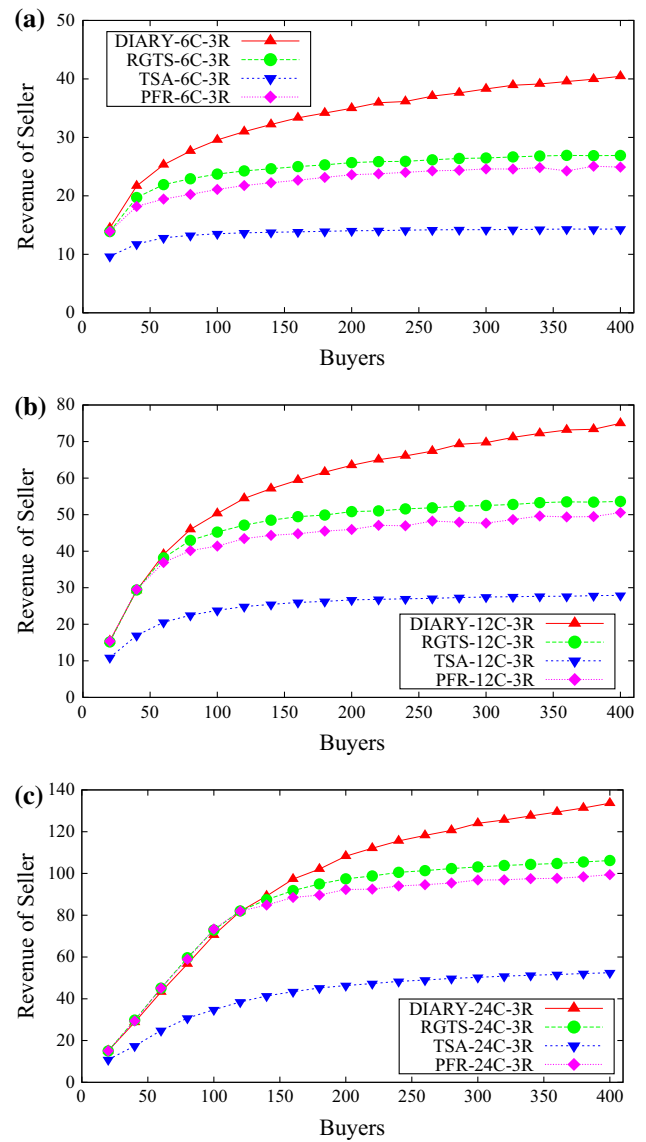


Fig. 4 Revenue of DIARY, RGTS, TSA and PFA with multi radio. **a** 6 Channels available with multi radio. **b** 12 Channels available with multi radio. **c** 24 Channels available with multi radio

Figure 7 shows the difference of revenue between DIARY and DIARY-with-Fairness when the number of bidders grows. We can see from Fig. 7 that no matter each buyer is equipped with a single or three radios, fairness has very limited effect on the revenue. The biggest difference between DIARY and DIARY-with-Fairness is less than 4.

7 Related works

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

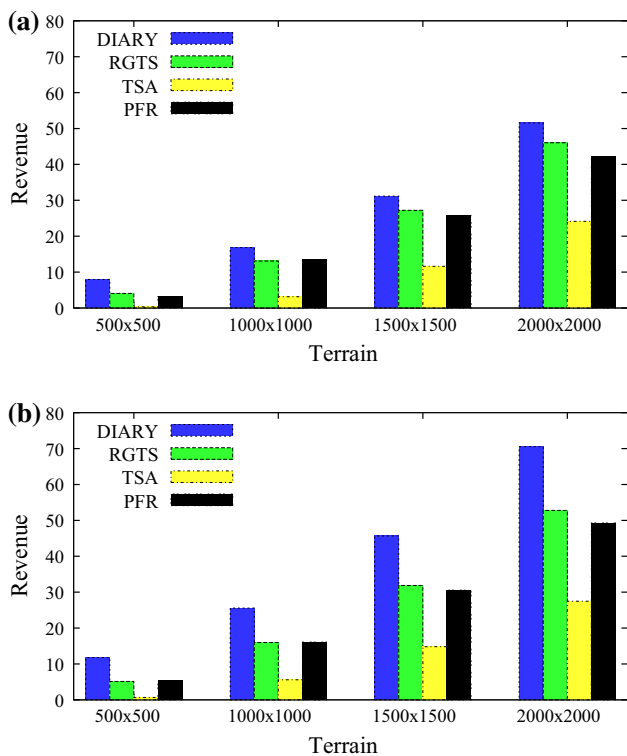


Fig. 5 Revenue of DIARY, RGTS, TSA, PFR in different terrains. **a** Single radio scenario. **b** Multi radio scenario.

In the literature, dynamic mechanisms of spectrum auctions has been widely concerned, especially in aspect of strategy-proofness [26, 31, 33] and revenue maximization [10, 16, 28]. Also various kinds of auction forms are explored [17, 19, 24, 30]. Nevertheless, 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 [3, 14, 18] guarantee the privacy of bidders, but compromise 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 [6] proposed the solution concept of differential privacy for the first time, then McSherry and Talwar [21] 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 [7] introduced the definition of differential privacy and two basic techniques for achieving differential privacy, meanwhile showed some interesting applications of the techniques. Recently, Xiao [27] 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. [23] designed an general approximately optimal mechanism via differential privacy. Nissim

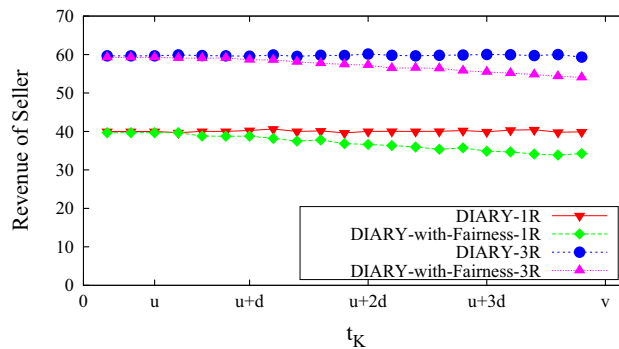


Fig. 6 Revenue of DIARY and DIARY-with-Fairness, when we set t_k in $[u, v)$. There are 12 channels available and each buyer is equipped with one radio or three radios

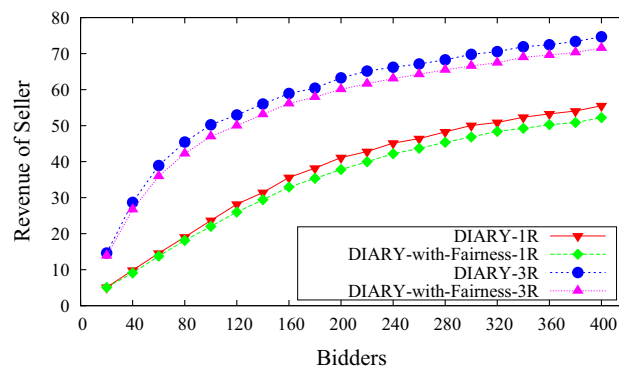


Fig. 7 Revenue of DIARY and DIARY-with-Fairness, when we set $t_k = \frac{d}{2}$. There are 12 channels available and each buyer is equipped with one radio or three radios

et al. [22] also modeled the privacy-aware agents and designed a privacy-aware mechanism via differential privacy. There are also works extending the properties [2, 15] and applications [12, 13] of differential privacy.

However, it's worth mentioning that there dose exist some work considering the joint problem of designing both approximately revenue maximizing and privacy preserving auction mechanism for secondary spectrum markets just recently [35, 36]. But the mechanism proposed in this paper is more intuitive and easily understood. More importantly, we are the first to locate the crucial issue of fairness in privacy preserving auction mechanisms for spectrum redistribution.

8 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. We also make some simple but effective improvements to address the fairness issue in spectrum auctions, so that buyers are guaranteed a minimum probability of getting service. The evaluation results have shown that DIARY outperforms the existing mechanisms.

References

1. Spectrum bridge. <http://www.spectrumbridge.com>
2. Chen, Y., Chong, S., Kash, I. A., Moran, T., & Vadhan, S. (2013). Truthful mechanisms for agents that value privacy. In *Proceedings of the 14th ACM conference on electronic commerce, EC*.
3. Chen, Z., Huang, L., & Chen, L. (2015). Itsec: An information-theoretically secure framework for truthful spectrum auctions. In *INFOCOM*.
4. Cox, D. C., & Reudink, D. O. (1971). Dynamic channel assignment in high capacity mobile communication system. *Bell System Technical Journal*, 50(6), 1833–1857.
5. Cramton, P. (2002). *Spectrum auctions*.
6. Dwork, C. (2006). Differential privacy. In *Automata, languages and programming*.
7. Dwork, C. (2008). Differential privacy: A survey of results. In *Theory and applications of models of computation*.
8. Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography*.
9. Federal Communications Commission (FCC): <http://www.fcc.gov/>.
10. Gandhi, S., Buragohain, C., Cao, L., Zheng, H., & Suri, S. (2007). A general framework for wireless spectrum auctions. In: *New frontiers in dynamic spectrum access networks, DySPAN*
11. Gopinathan, A., & Li, Z. (2011). A prior-free revenue maximizing auction for secondary spectrum access. In *INFOCOM*.
12. He, K., & Mu, X. (2014). Differentially private and incentive compatible recommendation system for the adoption of network goods. In *Proceedings of the 15th ACM conference on economics and computation, EC*.
13. Hua, J., Gao, Y., & Zhong, S. (2015). Differentially private publication of general time-serial trajectory data. In *INFOCOM*.
14. Huang, Q., Tao, Y., & Wu, F. (2013). Spring: A strategy-proof and privacy preserving spectrum auction mechanism. In *INFOCOM*.
15. Huang, Z., & Kannan, S. (2012). The exponential mechanism for social welfare: Private, truthful, and nearly optimal. In *Foundations of computer science, FOCS*.
16. Jia, J., Zhang, Q., Zhang, Q., & Liu, M. (2009). Revenue generation for truthful spectrum auction in dynamic spectrum access. In *Mobile ad hoc networking and computing, MobiHoc*.
17. Li, H., Wu, C., & Li, Z. (2015). Socially-optimal online spectrum auctions for secondary wireless communication. In *INFOCOM*.
18. Li, M., Li, P., Guo, L., & Huang, X. (2015). Pper: Privacy-preserving economic-robust spectrum auction in wireless networks. In *INFOCOM*.
19. Li, W., Cheng, X., Bie, R., & Zhao, F. (2014). An extensible and flexible truthful auction framework for heterogeneous spectrum markets. In *Proceedings of the 15th ACM international symposium on mobile ad hoc networking and computing*.
20. McHenry, M. A., Tenhula, P. A., McCloskey, D., Roberson, D. A., & Hood, C. S. (2006). Chicago spectrum occupancy measurements and analysis and a long-term studies proposal. In *Proceedings of the first international workshop on technology and policy for accessing spectrum*.
21. McSherry, F., & Talwar, K. (2007). Mechanism design via differential privacy. In *Foundations of computer science, FOCS*.
22. Nissim, K., Orlandi, C., & Smorodinsky, R. (2012). Privacy-aware mechanism design. In *Electronic commerce, EC*.
23. Nissim, K., Smorodinsky, R., & Tennenholtz, M. (2012). Approximately optimal mechanism design via differential privacy. In *Proceedings of the 3rd innovations in theoretical computer science conference*.
24. Peng, D., Yang, S., Wu, F., Chen, G., & Luo, T. (2015). Resisting three-dimensional manipulations in distributed wireless spectrum auctions. In *INFOCOM*.
25. West, D. B. (1996). *Introduction to graph theory* (2nd ed.). New Jersey: Prentice Hall.
26. Wu, F., & Vaidya, N. (2011). Small: A strategy-proof mechanism for radio spectrum allocation. In *INFOCOM*.
27. Xiao, D. (2011). Is privacy compatible with truthfulness? *IACR Cryptology ePrint Archive, 2011, 5*.
28. Yang, D., Fang, X., & Xue, G. (2012). Truthful auction for cooperative communications with revenue maximization. In *International conference on communications, ICC*.
29. Yue, W. (1991). Analytical methods to calculate the performance of a cellular mobile radio communication system with hybrid channel assignment. *IEEE Transactions on Vehicular Technology*, 40(2), 453–460.
30. Zheng, Z., Wu, F., Tang, S., & Chen, G. (2014). Unknown combinatorial auction mechanisms for heterogeneous spectrum redistribution. In *Proceedings of the 15th ACM international symposium on mobile ad hoc networking and computing*.
31. Zhou, X., Gandhi, S., Suri, S., & Zheng, H. (2008). ebay in the sky: Strategy-proof wireless spectrum auctions. In *ACM/IEEE international conference on mobile computing and networking, MOBICOM*.
32. Zhou, X., Zhang, Z., Wang, G., Yu, X., Zhao, B. Y., & Zheng, H. (2013). Practical conflict graphs for dynamic spectrum distribution. In *Measurement and modeling of computer systems, SIGMETRICS*.
33. Zhou, X., & Zheng, H. (2009). Trust: A general framework for truthful double spectrum auctions. In *INFOCOM*.
34. Zhou, Y., & Lukose, R. (2007). Vindictive bidding in keyword auctions. In *Electronic commerce, EC*.
35. Zhu, R., Li, Z., Wu, F., Shin, K., & Chen, G. (2014). Differentially private spectrum auction with approximate revenue maximization. In *Proceedings of the 15th ACM international symposium on mobile ad hoc networking and computing*.
36. Zhu, R., & Shin, K. G. (2015). Differentially private and strategy-proof spectrum auction with approximate revenue maximization. In *INFOCOM*.



Chunchun Wu is a graduate student in the Department of Computer Science and Engineering at Shanghai Jiao Tong University. She received her B.S. degree from Nanjing University in 2013. Her research interests lie in game theory, mechanism design and resource management in wireless networks.



Zuying Wei obtained her M.S. degree from the department of Computer Science and Engineering at Shanghai Jiao Tong University, P. R. China. She is interested in the research of spectrum resource management in wireless networks and the combination of game theory and resource management.



Fan Wu is an associate professor in the Department of Computer Science and Engineering, Shanghai Jiao Tong University. He received his B.S. in Computer Science from Nanjing University in 2004, and Ph.D. in Computer Science and Engineering from the State University of New York at Buffalo in 2009. He has visited the University of Illinois at Urbana-Champaign (UIUC) as a Post Doc Research Associate. His research interests include

wireless networking and mobile computing, algorithmic game theory and its applications, and privacy preservation. He has published more than 80 peer-reviewed papers in leading technical journals and conference proceedings. He is a receipt of China National Natural Science Fund for Outstanding Young Scientists, CCF-Intel Young Faculty Researcher Program Award, CCF-Tencent Rhinoceros bird Open Fund, and Pujiang Scholar. He has served as the chair of CCF YOCSEF Shanghai, on the editorial board of Elsevier Computer Communications, and as the member of technical program committees of more than 40 academic conferences. For more information, please visit <http://www.cs.sjtu.edu.cn/~fwu/>.



Guihai Chen earned his B.S. degree from Nanjing University in 1984, M.E. degree from Southeast University in 1987, and Ph.D. degree from the University of Hong Kong in 1997. He is a distinguished professor of Shanghai Jiaotong University, China. He had been invited as a visiting professor by many universities including Kyushu Institute of Technology, Japan in 1998, University of Queensland, Australia in 2000, and Wayne State University,

USA during September 2001 to August 2003. He has a wide range of

research interests with focus on sensor networks, peer-to-peer computing, high-performance computer architecture and combinatorics. He has published more than 200 peer-reviewed papers, and more than 120 of them are in well-archived international journals such as IEEE Transactions on Parallel and Distributed Systems, Journal of Parallel and Distributed Computing, Wireless Networks, The Computer Journal, International Journal of Foundations of Computer Science, and Performance Evaluation, and also in well-known conference proceedings such as HPCA, MOBIHOC, INFOCOM, ICNP, ICPP, IPDPS and ICDCS.



Shaojie Tang is currently an assistant professor of Naveen Jindal School of Management at University of Texas at Dallas. He received his Ph.D. in computer science from Illinois Institute of Technology in 2012. His research interest includes social networks, mobile commerce, game theory, e-business and optimization. He received the Best Paper Awards in ACM MobiHoc 2014 and IEEE MASS 2013. He also received the ACM SIGMobile service

award in 2014. Tang served in various positions (as chairs and TPC members) at numerous conferences, including ACM MobiHoc, IEEE INFOCOM, IEEE ICDCS and IEEE ICNP. He is an editor for Elsevier Information Processing in the Agriculture and International Journal of Distributed Sensor Networks.