This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2011 proceedings.

Dealing with the Untrustworthy Auctioneer in Combinatorial Spectrum Auctions

Miao Pan*, Hongyan Li†, Pan Li‡ and Yuguang Fang*†
* Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611
† State Key Lab of Integrated Service Networks, Xidian University, Xi'an, China, 710071
‡ Department of Electrical and Computer Engineering, Mississippi State University, Mississippi State, MS 39762
Email: {miaopan@, fang@ece.}ufl.edu, hyli@xidian.edu.cn, li@ece.msstate.edu

***Abstract*—Spectrum auction is an enabling approach to drastically improving the spectrum utilization to satisfy the ever increasing service demands in wireless networks. However, the behaviors of the untrustworthy auctioneer (i.e., the frauds of the untrustworthy auctioneer and the bid-rigging between the greedy bidders and the insincere auctioneer) pose significant design challenges. In this paper, we propose a secure combinatorial spectrum auction (*SCSA*) by using homomorphic encryption to deal with the untrustworthy auctioneer. *SCSA* computes and reveals the results of spectrum auction while the actual bidding values are kept confidential. By taking frequency reuse and interference constraints into consideration, we also incorporate a corresponding procedure to implement the combinatorial spectrum auction. It has been shown that *SCSA* can effectively thwart the back-room dealing without much performance degradation.**

***Index Terms*—Security; spectrum auction; homomorphic encryption; cognitive radio networks.**

I. Introduction

In the last decade, more and more people rely on wireless services for their daily life and business. The accompanied dilemma between the booming growth of wireless services and the scarcity of radio spectrum has shoved the traditional fixed spectrum allocation off the edge, and resulted in numerous new techniques, which allow the opportunistic access to the under-utilized spectrum [1]. Inspired by the mechanisms in microeconomics, auction seems to be one of the most promising solutions to harvesting vacant spectrum resource for the potential unlicensed users [2], [3].

Although traditional auctions (e.g., Dutch auction, Vickrey-Clarke-Groves (VCG) auction, etc.) have desirable characteristics (e.g., incentive compatibility, Pareto efficiency, individual rationality, etc.) [4], they cannot be hammered into the spectrum auction design directly. Unlike common goods in conventional auctions, spectrum is reusable among bidders subject to the spatial interference constraints, i.e., bidders geographically far apart can use the same frequency simultaneously while bidders in close proximity cannot. To deal with the mutual interference between neighboring bidders, Gandhi et al. [5] has proposed the conflict graph and a general framework for wireless spectrum auctions. Based on these concepts, a truthfully bidding spectrum auction, *VERITAS*, is proposed by Zhou et al. in [2]. The notion of critical neighbor/value is proposed and employed to guarantee the auction strategy-proof. Zhou et al. [2] also provide an efficient allocation algorithm, which assigns bidders with spectrum bands sequentially from the bidder with the highest bid to the one with the lowest bid by considering the complex heterogeneous interference constraints. However, the validity of this algorithm is challenged by a special scenario in [3], which shows that it is not always right to allocate the spectrum bands to the bidder with the highest bid in case that the sum of the neighboring bids is much higher than the highest bid. In addition, the collusion among the bidders is described in [3]. As a possible solution, they group the nodes with negligible interference together as virtual bidders, trim the multi-winner spectrum auction [3] into a traditional single-winner auction and split the payment or revenue among the participating bidders using game theory. However, the issue of group partition itself is NP-complete with respect to the spatial reuse [5].

All aforementioned works assume that the auctioneer is trustworthy. In reality, this may not be the case. The auctioneer may overcharge the winning bidders with the forged price as shown in Fig. 1(a) or collude with greedy bidders to manipulate the auctions (e.g., bid-rigging) shown in Fig. 1(b). Thus, a secure spectrum auction design should also consider the frauds of the untrustworthy auctioneer. In this paper, with the consideration of interference constraints, we apply cryptographic techniques to design a novel secure spectrum auction scheme, called *SCSA*, to purge the possible frauds and bid-riggings. The contributions of the proposed auction are summarized as follows:

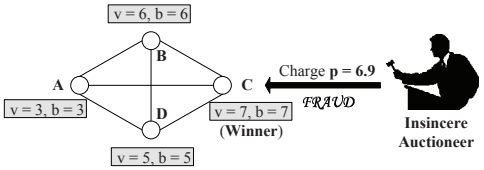
(i) *SCSA* supports combinatorial spectrum auction consisting of bands with diverse characteristics rather than the single-band spectrum auction consisting of bands only with uniform characteristics in previous works [2], [3], [5], [6].

(ii) *SCSA* provides an effective procedure to auction the spectrum bands under the interference constraints. To address the NP-completeness of spectrum allocation in view of the frequency reuse, *SCSA* decomposes the whole network into small subnetworks according to the number of bidders, and auctions the spectrum bands in subnetworks one by one.

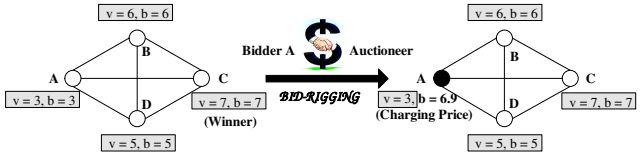
(iii) *SCSA* leverages homomorphic encryption [7] to mask the bidding values with a vector of ciphertexts, which enables the auctioneer to find the maximum bidding value and charge the bidders securely. By employing a variant of VCG (V^2CG) auction [4] in the subnetworks, the auctioneer could compute and reveal the results of spectrum auction, while the actual bidding values are kept secret from both the other bidders and

This work was partially supported by the U.S. National Science Foundation under grants CNS-0721744 and CNS-0916391, and the China 111 Project under Grant B08038.

978-1-4244-9268-8/11/$26.00 ©2011 IEEE



(a) Frauds of the insincere auctioneer



(b) Bid-rigging between the auctioneer and the bidders

Fig. 1. Challenges to secure spectrum auction design

the auctioneer.

(iv) *SCSA* secures the spectrum auction against frauds and bid-riggings with relatively low communication and computational complexity. We show that *SCSA* is more efficient than existing secure auction designs, and achieves similar performance in terms of spectrum utilization compared with existing auction designs when the auctioneer is assumed trustworthy.

II. Network Model and Preliminaries

A. System Overview

We consider a typical spectrum auction setting, where the auctioneer auctions his unutilized spectrum bands $\mathcal{S} = \{1, 2, \cdots, s\}$ to $\mathcal{N} = \{1, 2, \cdots, n\}$ nodes/bidders. The available $\mathcal{S}$ spectrum bands are supposed to have different characteristics to different nodes (in the sequel, we use the words nodes and bidders interchangeably) in terms of the frequency of the available band, the segment type of the band (i.e., contiguous segment or discontinuous one), the location of the bidders, etc., so that bidders may submit different bids for different combinations of the spectrum bands. Considering the frequency reuse [5], i.e., adjacent nodes must not use the same bands simultaneously while geographically well-separated ones can, we represent the interference relationship among bidders by a conflict graph, which can be constructed from either physical model or protocol model [2], [3], [5], [8]. Moreover, we assume that spectrum auctions take place periodically[1], the bidders are static in each period, and there is a common channel for necessary information exchanges between the auctioneer and bidders. The main notations and definitions related to the spectrum auction are summarized as follows:

- *A Feasible Allocation* – $\boldsymbol{\lambda} = \big(\lambda(1), \lambda(2), \cdots, \lambda(n)\big)$ denotes a feasible allocation for a set of spectrum bands $\mathcal{S}$, where $\lambda(i)$ represents the bunch of bands allocated to bidder i with the following conditions holding: $\bigcup_i \lambda(i) \subseteq \mathcal{S}$, and for all $i \neq j$, $\lambda(i) \cap \lambda(j) = \emptyset$.
- *Allocation Set* – $\mathcal{N}^{\mathcal{S}} = \{\boldsymbol{\lambda} : \mathcal{S} \rightarrow \mathcal{N}\}$ denotes the set of allocations of spectrum bands $\mathcal{S}$ to bidders $\mathcal{N}$.
- *Bidding Values* – $b_i(\lambda(i))$ indicates the bidding values of node i for the bunch of spectrum bands $\lambda(i)$.
- *Evaluation Values* – $v_i(\lambda(i))$ represents the true evaluation values of node i for for the bunch of spectrum bands $\lambda(i)$. In case that the auction is incentive compatible, v_i equals to b_i.
- *Charging Price* – p_i is the price charged by the auctioneer for allocating the spectrum bands to winning bidder i.
- *Bidder's Utility* – u_i stands for the utility of bidder i. It is defined as $u_i(\lambda(i)) = v_i(\lambda(i)) - p_i$ for the bunch of spectrum bands $\lambda(i)$.

B. Homomorphic Encryption

Homomorphic encryption is a probabilistic[2] asymmetric public key encryption. The special features of homomorphic encryption includes homomorphic addition/multiplication, indistinguishability, and self-blinding [7]:

- **Homomorphic addition/multiplication.** Given $\mathscr{E}$ is the homomorphic encryption of a message M, $\mathscr{E}(\cdot)$ is additive homomorphic, i.e., $\mathscr{E}(M_1 + M_2) = \mathscr{E}(M_1)\mathscr{E}(M_2)$ (e.g., Paillier cryptosystem and Benaloh cryptosystem)/multiplicative homomorphic, i.e., $\mathscr{E}(M_1 M_2) = \mathscr{E}(M_1)\mathscr{E}(M_2)$ (e.g., ElGamal encryption).
- **Indistinguishability.** $\mathscr{E}(\cdot)$ is considered indistinguishable if the same plaintext M is encrypted twice, these two ciphertexts are totally different, and no one can succeed in distinguishing the corresponding original plaintexts with a probability significantly greater than $1/2$ (i.e., random guessing) unless he decrypts the ciphertexts.
- **Self-blinding.** Any ciphertext can be publicly changed into another one without affecting the plaintext, which means a different randomized ciphertext $\mathscr{E}'(M)$ can be computed from the ciphertext $\mathscr{E}(M)$ without knowing either the decryption key or the original plaintext.

III. Multi-hop Spectrum Auction Procedure

To deal with the back-room dealing, the proposed *SCSA* leverages homomorphic encryption to mask the bidding values and enable the auctioneer to charge the winners without leaking the information about bidding values. In parallel with the encryption design, *SCSA* also provides a supporting conflict-table-driven auction procedure to implement the spectrum auction. In this section, we describe the multi-hop spectrum auction procedure. Then, we elaborate the encryption design of the proposed *SCSA* in the next section.

The detailed procedure of *SCSA* is presented as follows.

Preparation: Each bidder sets up two tables, a conflict-table for storing the nodes causing mutual interference and a price-charged table for storing a series of charging prices for the bands he won. Bidders fill in the conflict-table with current interfering neighbors and initialize the price-charged table with zeros. For any bidder $i \in \mathcal{N}$, he encloses his identity, location information and his own bidding values b_i for the bunches of bands in which he is interested in his bid. The identity and location information of bidder i are public to the auctioneer for

[1]The auction period should not be too long (e.g., months or years) to make dynamic spectrum allocation infeasible, and it should not be too short (e.g., seconds or minutes) to incur overwhelming overhead in spectrum trading. The typical duration is hours or days as shown in [9]. In the rest of paper, we assume that all the spectrum auctions are of fixed duration, so that the time parameter is not included, and we only need to focus on a specific period for the design of secure spectrum auction.

[2]The term "probabilistic encryption" is typically used in reference to public key encryption algorithms. Probabilistic encryption uses the randomness in an encryption algorithm, so that when encrypting the same plaintext for several times, it will yield different ciphertexts.

subnetwork division, allocating spectrum bands and charging prices, but b_i is masked using homomorphic encryption. Then, bidders submit their bids to the auctioneer.

Start-up: Due to the NP-completeness of spectrum allocation, there is no optimal choice for the auctioneer to start the subnetwork spectrum auctions with a designated bidder in order to maximize his revenue. Therefore, the auctioneer can initiate the subnetwork auctions with a randomly chosen bidder, say node i, where bidder i is regarded as the center of the current subnetwork, and his interference range is set to be the radius of the subnetwork.

Bidder Indexing: The auctioneer sorts the bidders within the subnetwork according to their Euclidean distances from the center i. The closer to the center, the smaller index the bidder is labeled. The auctioneer stores the index information in a distance vector $\mathcal{D}$, whose element d_j denotes the j-th node away from the center i in terms of distance.

Subnetwork Auction: After indexing the bidders, the auctioneer collects the bids and carries out the secure combinatorial spectrum auction within the subnetwork by using homomorphic encryption. The results of the subnetwork auction, i.e., the set of winners and corresponding charging prices, are published. Details of encryption design for the secure subnetwork spectrum auction are elaborated in Section IV.

Allocation & Payment: Determined by both subnetwork auction results and location of the winners, the allocation of spectrum bands and the payment are different in three cases:

Case 1: If the current center, bidder i, is not one of the winners, the auctioneer needs to check the elements in the winner set $\mathcal{W}$, choose the winning bidder with the smallest index to be the next center, and set his interference range as the radius of the next subnetwork. According to the results of current subnetwork auction, all the winning bidders store the spectrum bands they won and the corresponding charging prices into their price-charged tables. After that, current center, bidder i, is deleted from the conflict-tables of his neighbors. The subnetwork spectrum auction centered at node i ends, and the auction goes to ***Bidder Indexing*** of the next center for the next subnetwork auction.

Case 2: If the center, bidder i, is the only winner of the auction, and he is charged at p_i for the bunch of bands λ, he will compare the current charging price p_i with the previous charging prices stored in his price-charged table and pay the highest one of all the prices for the bunch of spectrum bands[3]. Then, the center node broadcasts his spectrum occupancy information and his neighbors eliminate him from their conflict-tables. After that, the auctioneer sets the node with the smallest index as the next center. The auction goes to ***Bidder Indexing*** for the next subnetwork auction.

Case 3: Provided that there are more winners than the current center i, the process is the same as in *Case 2*, except that the auctioneer would rather take the node with the smallest index in the winning set $\mathcal{W}$ as the next center for the consideration of computational efficiency.

[3]Paying the highest price in the price-charged table is to guarantee the center, bidder i, to beat other competitors in the previous subnetwork auctions, where i is not the center.

IV. Design of Secure Subnetwork Auction

Now, the only problem left is how to securely carry out the spectrum auction in each subnetwork. Since VCG auction has been proved to be incentive-compatible from the bidder side, we can modify it with cryptographic tools to prevent the insincere behaviors from the auctioneer side and apply it to spectrum auctions of the subnetworks.

A. V^2CG Auction: An Equivalent Variant of VCG Auction

In this section, we develop a variant of VCG auction that can achieve the same outcome as the VCG auction. In this protocol, as in the standard VCG, for each bunch $\mathcal{G}$, bidder i declares his bidding value $b_i(\mathcal{G})$. Note that the declared bidding value is not necessarily the same as the true evaluation value $v_i(\mathcal{G})$.

To simplify the protocol description, we introduce the following notation. For a set of goods $\mathcal{G} \subseteq \mathcal{S}$ and a set of bidders $\mathcal{M}$, we define $B^*(\mathcal{G}, \mathcal{M})$ as the sum of the evaluation values of $\mathcal{M}$ when $\mathcal{G}$ is allocated optimally among $\mathcal{M}$. To be precise, let us represent the set of all feasible allocations of a set of goods $\mathcal{G}$ as $\mathcal{M}^{\mathcal{G}}$, where for each $\boldsymbol{\lambda} = (\lambda(1), \lambda(2), \cdots, \lambda(m)) \in \mathcal{M}^{\mathcal{G}}$, $\bigcup_{i \in \mathcal{M}} \lambda(i) \subseteq \mathcal{G}$ and for all $i \neq j$, $\lambda(i) \cap \lambda(j) = \emptyset$ holds. $B^*(\mathcal{G}, \mathcal{M})$ is defined as follows.

$$B^*(\mathcal{G}, \mathcal{M}) = \max_{\boldsymbol{\lambda} \in \mathcal{M}^{\mathcal{G}}} \sum_{j \in \mathcal{M}} b_j\big(\lambda(j)\big). \tag{1}$$

In this protocol, instead of determining the allocation, we first determine the price of each bunch of bands $\mathcal{G}$ for each bidder i is defined as follows.

$$p_{i,\mathcal{G}} = B^*(\mathcal{S}, \mathcal{N}\backslash\{i\}) - B^*(\mathcal{S}\backslash\mathcal{G}, \mathcal{N}\backslash\{i\}). \tag{2}$$

Next, each bidder i chooses a bunch that maximizes his utility based on the prices, i.e., he chooses $\mathcal{G}^*$, where $\mathcal{G}^* = \operatorname{argmax}_{\mathcal{G} \subseteq \mathcal{S}} v_i(\mathcal{G}) - p_{i,\mathcal{G}}$. Note that each bidder can choose a bunch of bands that maximizes his utility independently from the choices of other bidders. To be more precise, if there exist multiple bunches that maximize his utility, then the protocol performs some adjustment so that the choices are consistent, but each bidder is still guaranteed to obtain one bunch that maximizes his utility.

The proposed variant of auction is equivalent to VCG auction. The following theorems hold.

***Theorem** 1:* A bunch of spectrum bands $\mathcal{G}$ maximizes bidder i's utility if and only if for some $\boldsymbol{\lambda}^*$, $\lambda^*(i) = \mathcal{G}$ holds.

Proof: For the detailed proof and examples, please check the report posted at http://plaza.ufl.edu/miaopan/TR-SSA.pdf. ■

***Theorem** 2:* If $\mathcal{G}$ maximizes bidder i's utility, then $p_i = p_{i,\mathcal{G}}$ holds.

Proof: For the detailed proof and examples, please check the report posted at http://plaza.ufl.edu/miaopan/TR-SSA.pdf. ■

B. Encrypted Representation of Bidding Values

We use homomorphic additive cryptosystem [7] to mask the bidding values. Assuming k ($1 \leq k \leq q$) is the bidding value

for a bunch of spectrum bands λ (i.e., $k = b(\lambda)$), k can be represented by a vector $\mathbf{e}(k)$ of ciphertexts

$$\mathbf{e}(k) = (e^1, \cdots, e^q) = (\underbrace{\mathscr{E}(x), \cdots, \mathscr{E}(x)}_{k}, \underbrace{\mathscr{E}(0), \cdots, \mathscr{E}(0)}_{q-k}), \quad (3)$$

where $\mathscr{E}(0)$ and $\mathscr{E}(x)$ account for the homomorphic encryption of 0 and the common public element x ($x \neq 0$), respectively. Here, q is a number large enough to cover all the possible bidding values for any bunch of available spectrum bands. For instance, assuming $q = 3$ and $k = 2$ for the given bunch of bands λ, $\mathbf{e}(k) = \mathbf{e}(2) = \big(\mathscr{E}(x), \mathscr{E}(x), \mathscr{E}(0)\big)$.

Because of the self-blinding property of $\mathscr{E}$, k cannot be determined without decrypting each element in the vector $\mathbf{e}(k)$.

The maximum of encrypted bidding value, $\mathbf{e}(k_i) = (e_i^1, ..., e_i^q)$, can be found without leaking information about any other bidding value, $\mathbf{e}(k_j) = (e_j^1, ..., e_j^q), j \neq i$, as follows. Let us consider the product of all the bidding vectors for certain spectrum allocation λ,

$$\prod_i \mathbf{e}(k_i) = (\prod_i e_i^1, \cdots, \prod_i e_i^q). \quad (4)$$

By the property of homomorphic addition, the j-th component of the vector above can be denoted as

$$y_j = \prod_i e_i^j = \mathscr{E}^{c(j)}(x) = \mathscr{E}(c(j)x), \quad (5)$$

where $c(j) = |\{i | j \leq k_i\}|$ indicates the number of values that are equal to or greater than j. It is obvious that $c(j)$ monotonically decreases when j increases, which gives us some hints to solving the maximum value selection problem. To find the maximum of these bidding values, we decrypt y_j and check whether decryption $\mathscr{E}^{-1}(y_j)$ is equal to 0 or not from $j = q$ down to $j = 1$ until we find the largest j subject to $\mathscr{E}^{-1}(y_j) \neq 0$. This j is equal to $\max\{k_i\}$, i.e., the maximum of the bidding values for the bunch λ.

C. Payment Calculation via Dynamic Programming

In this section, we illustrate how the auctioneer[4] calculates the payment of bidder i in the V^{2}CG auction via dynamic programming [11]. Let $\mathbf{e}[\cdot]$ represent the encrypted value. Based on the homomorphic encryption and formula of payment in (2), assume each bidder j (except i) declares his encrypted bidding value $\mathbf{e}[b_j(\mathcal{G})]$[5] for each bunch of bands $\mathcal{G}$ in which he is interested. If bidder j has substitutable choice of band-bunch, e.g., bidder j wants either $\mathcal{G}_1$ or $\mathcal{G}_2$ but not both at the same time, we introduce a dummy good d to solve the problem. Specifically, if bidder j is interested in both $\mathcal{G}_1 \cup \{d\}$ and $\mathcal{G}_2 \cup \{d\}$, it can be avoided that both $\mathcal{G}_1$ and $\mathcal{G}_2$ are allocated to bidder j at the same time since $\mathcal{G}_1 \cup \{d\} \bigcap \mathcal{G}_2 \cup \{d\} = \{d\}$.

Then, the auctioneer creates a virtual state $(\mathcal{G}, |\mathcal{G}|)$ for each bunch $\mathcal{G} \subseteq \mathcal{S}$, where $|\mathcal{G}|$ denotes the number of available spectrum bands included in $\mathcal{G}$. Meanwhile, the auctioneer creates the following directed, weighted links for each bunch of bands $\mathcal{G}$ which bidder j is interested in.

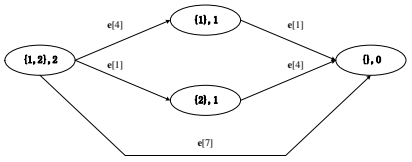
- For a link from state $(\mathcal{G}, |\mathcal{G}|)$ to state $(\{\}, 0)$, the weight $w((\mathcal{G}, |\mathcal{G}|), (\{\}, 0))$ is $\mathbf{e}[b_j(\mathcal{G})]$ (also equal to $\mathbf{e}[v_j(\mathcal{G})]$).
- For any $\mathcal{G}^{'}, \mathcal{G}^{''} \subseteq \mathcal{S}$, where $\mathcal{G}^{''} \subset \mathcal{G}^{'}$, $\mathcal{G}^{'} \backslash \mathcal{G}^{''} = \mathcal{G}$, and $|\mathcal{G}^{''}| \geq |\mathcal{G}^{'}|/2$, the weight $w((\mathcal{G}^{'}, |\mathcal{G}^{'}|), (\mathcal{G}^{''}, |\mathcal{G}^{''}|))$ for a link from state $(\mathcal{G}^{'}, |\mathcal{G}^{'}|)$ to state $(\mathcal{G}^{''}, |\mathcal{G}^{''}|)$ is $\mathbf{e}[v_j(\mathcal{G})]$.

We present a graph of state diagram and corresponding weighted links with $\mathcal{G} = \{1, 2\}$ in Fig. 2. In this figure, the length of the longest path from initial state $(\mathcal{G}, |\mathcal{G}|)$ to terminal state $(\{\}, 0)$ represents the sum of the encrypted bidding values when allocating a bunch of spectrum bands $\mathcal{G}$ optimally to bidders other than i, i.e., $\mathbf{e}[B^*(\mathcal{G}, \mathcal{N}\backslash\{i\})]$. Let $\Omega\big((\mathcal{G}, |\mathcal{G}|)\big)$ denote the length of the longest path from $(\mathcal{G}, |\mathcal{G}|)$ to $(\{\}, 0)$. Then, $\mathbf{e}[\Omega\big((\mathcal{G}, |\mathcal{G}|)\big)]$ can be calculated by the following recurrence process.

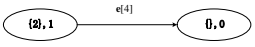
- $\mathbf{e}[\Omega\big((\{\}, 0)\big)] = \mathbf{e}[0]$
- $\mathbf{e}[\Omega\big((\mathcal{G}, |\mathcal{G}|)\big)] = \max_{((\mathcal{G}, |\mathcal{G}|), (\mathcal{G}', |\mathcal{G}'|))} \mathbf{e}[w\big((\mathcal{G}, |\mathcal{G}|), (\mathcal{G}^{'}, |\mathcal{G}^{'}|)\big) + \Omega\big((\mathcal{G}^{'}, |\mathcal{G}^{'}|)\big)]$.

Using this approach, we can obtain $\Omega\big((\mathcal{G}, |\mathcal{G}|)\big)$ by starting from a state that has a smaller bunch of spectrum bands. From (2), the price of bidder i for bunch $\mathcal{G}$, i.e., $p_{i,\mathcal{G}}$, is given as $B^*(\mathcal{S}, \mathcal{N}\backslash\{i\}) - B^*(\mathcal{S}\backslash\mathcal{G}, \mathcal{N}\backslash\{i\})$. Therefore, $p_{i,\mathcal{G}}$ is

$$p_{i,\mathcal{G}} = \Omega\big((\mathcal{S}, |\mathcal{S}|)\big) - \Omega\big((\mathcal{S}\backslash\mathcal{G}, |\mathcal{S}\backslash\mathcal{G}|)\big). \quad (6)$$



(a) The illustrative graph for $\Omega((\{1, 2\}, 2))$ calculation.



(b) The illustrative graph for $\Omega((\{2\}, 1))$ calculation.

Fig. 2. An example of state diagram for dynamic programming in the case that bidder 1 is interested in $\mathcal{G} = \{1\}$.

V. Performance Comparison

A. Simulation Setup

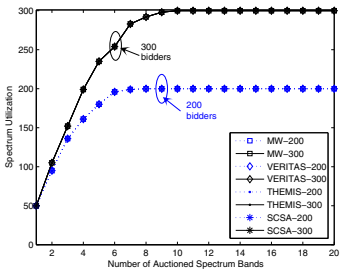
We assume the spectrum auction hosted by the auctioneer is deployed in a 1*1 square area, where nodes are uniformly distributed and connected [12]. Suppose the wireless mutual interference is simply distance-based, and any two bidders within 0.1 distance conflict with each other and cannot be allocated with the same spectrum bands. The bidding values of different bidders over different bands are supposed to be i.i.d random variables uniformly distributed over $(0, 10]$. To be simple, for every bidder, we let the bidding value for a bunch of bands be the sum of bidding values for the bands, which constitute the spectrum bunch.

B. Results and Analysis

1) Spectrum Utilization: We compare the spectrum utilization of *SCSA* with that of *M-W* [3], *VERITAS* [2] and *THEMIS* [6] with 200 and 300 bidders, respectively. In Fig. 3(a), as the number of bands increases, the spectrum utilization also increases until it saturates (i.e., every bidder is allocated a band) in all four auctions. It is not surprising that the performance results of *M-W*, *VERITAS*, *THEMIS* and *SCSA* are the same in terms of spectrum utilization, because they mainly differ in their price charging and security designs.

[4]The auctioneer distributes the key $\mathscr{E}$ for decrypting bidding values among plural servers by using secret sharing technique. A lot of secret sharing or group decryption mechanisms can be employed to effectively prevent the distributed servers from colluding with each other to reveal the bids. Please refer to [10] for the details about secret sharing algorithms.

[5]Since V^{2}CG auction is the variant of VCG auction and keeps the property of incentive compatibility, each bidder bids truthfully and the bidding value for any bunch of spectrum bands is equal to the evaluation value.



(a) Spectrum utilization comparison.

TABLE I
THE COMPARISON OF COMMUNICATION COMPLEXITY BETWEEN *THEMIS* AND *SCSA*

Spectrum Auction Designs	**THEMIS**		**SCSA**	
pattern	**round**	**volume**	**round**	**volume**
the bidders $\leftrightarrow$ the auctioneer	$\mathcal{O}(n \log n)$	$\mathcal{O}\big(n \log n \times (\log n)^s \times q \log n\big)$	$\mathcal{O}(n \log n)$	$\mathcal{O}\big(n \log n \times 2^s \times q \log n\big)$
the bidder $\leftrightarrow$ neighbor bidders	$\mathcal{O}(\log n)$	$\mathcal{O}(\log n)$	$\mathcal{O}(\log n)$	$\mathcal{O}(\log n)$

TABLE II
THE COMPARISON OF COMPUTATIONAL COMPLEXITY BETWEEN *THEMIS* AND *SCSA*

Spectrum Auction Designs	**THEMIS**	**SCSA**
pattern	**computational complexity**	**computational complexity**
the bidder	$\mathcal{O}\big(n \log n \times (\log n)^s \times q \log n\big)$	$\mathcal{O}\big(n \log n \times 2^s \times q \log n\big)$
the auctioneer	$\mathcal{O}\big(t \times n \log n \times (\log n)^s \times q \log n\big)$	$\mathcal{O}\big(t \times n \log n \times 2^s \times q \log n\big)$

(b) Complexity comparison in terms of communication and computation.

Fig. 3. (i) Spectrum utilization comparison among *M-W*, *VERITAS*, *THEMIS* and *SCSA*. (ii) Complexity comparison between *THEMIS* and *SCSA*.

2) Security Analysis: To prevent an untrustworthy auctioneer from learning the bids and manipulating the auction by frauds, the auctioneer must employ l servers for encryption/decryption in *SCSA*. The decryption to determine the maximum of truthful bidding values is performed in a distributed manner by these servers. By using *SCSA*, for bidder i, the payment-calculator consisting of t servers learns $B^*(\mathcal{G}, \mathcal{N}\backslash\{i\})$ for each state $(\mathcal{G}, |\mathcal{G}|)$. However, note that $B^*(\mathcal{G}, \mathcal{N}\backslash\{i\})$ is obtained by aggregating many truthful bidding values of bidders, so that it is difficult to estimate each bidding value from $B^*(\mathcal{G}, \mathcal{N}\backslash\{i\})$. Unless t, $t < l$ (or more than t) servers collude, the auctioneer cannot decrypt vectors representing the bidding values of bidders illegally. Similarly, the bid-rigging between the bidders and the auctioneer becomes meaningless because the individual server itself knows nothing more than the winners and their payments in *SCSA*. Even if a certain bidder could collude with a number of servers composing the auctioneer, he cannot find out any information about the bids if only the number is less than t.

3) Efficiency Analysis: Here, we assume the network in the auction area is connected, which implies that the node density of the subnetworks is on the order of $\mathcal{O}(\log n)$ [12].

Table I shows the communication pattern, the order of communication rounds and the communication volume for bidders in both *THEMIS* and *SCSA*. In *THEMIS*, the bidder must declare his evaluation values over all $\mathcal{O}((\log n)^s)$ possible allocations in the subnetwork auction. But in the subnetwork auction of *SCSA*, the bidder only declares his evaluation values for the spectrum bunch that he is interested in, where the number of states for those bunches is in the order of $\mathcal{O}(2^s)$. Compared with *THEMIS*, it effectively reduces the communication overhead, especially for the case that the network density is high. Compared with conventional secure auction designs [11], there is also additional communication complexity incurred by the subnetwork decomposition. But this overhead is unavoidable when we take frequency reuse into consideration.

Table II shows the computational complexity for the auctioneer and a bidder in both *THEMIS* and *SCSA*. Similar to the analysis of communication cost, *SCSA* is more efficient than *THEMIS*. The computational complexity of bidders and the auctioneer is also related to the subnetwork composition, linear to the number of possible bidding values q and exponential to available spectrum bands s, which are inevitable but limited.

VI. CONCLUSION

To purge the frauds and bid-riggings caused by the untrustworthy auctioneer, we have applied cryptographic technique to the spectrum auction design and proposed *SCSA*, a secure combinatorial spectrum auction scheme based on homomorphic encryption. Considering frequency reuse, we have divided the whole network into small subnetworks and allowed the bidders to mask the bidding values with homomorphic ciphertexts. Using homomorphic encryption, *SCSA* enables the auctioneer to find the maximum bid and calculate the charging prices for each bunch of spectrum bands securely in the subnetwork auction without knowing the actual bidding values. We have shown that *SCSA* is much more efficient than previously proposed scheme *THEMIS* without too much performance degradation in terms of spectrum utilization.

REFERENCES

[1] FCC, "Spectrum policy task force report," Report of Federal Communications Commission, Et docket No. 02-135, Nov. 2002.
[2] X. Zhou, S. Gandhi, S. Suri, and H. Zheng, "ebay in the sky: strategy-proof wireless spectrum auctions," in *Proc. of Mobile Computing and Networking, Mobicom '08*, San Francisco, CA, Sep. 2008.
[3] Y. Wu, B. Wang, K. J. Liu, and T. Clancy, "A multi-winner cognitive spectrum auction framework with collusion-resistant mechanisms," in *Proc. of IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN '08*, Chicago, IL, Oct. 2008.
[4] V. Krishna, *Auction Theory*. Academic Press, 2002.
[5] S. Gandhi, C. Buragohain, L. Cao, H. Zheng, and S. Suri, "A general framework for wireless spectrum auctions," in *Proc. of IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN '07*, Dublin, Ireland, Apr. 2007.
[6] M. Pan, J. Sun, and Y. Fang, "Purging the back-room dealing: Secure spectrum auction leveraging Paillier Cryptosystem," *IEEE Journal on Selected Areas in Communications*, to appear, Technical Report. [Online]. Available: http://winet.ece.ufl.edu/~miaopan/file/Themis.pdf
[7] E. Goh, "Encryption schemes from bilinear maps," Ph.D. Thesis, Stanford University, USA, Sep. 2007.
[8] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 388–404, March 2000.
[9] L. Giupponi, R. Agusti, J. Perez-Romero, and O. S. Roig, "A novel approach for joint radio resource management based on fuzzy neural methodology," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 3, pp. 1789–1805, May 2008.
[10] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[11] K. Suzuki and M. Yokoo, "Secure combinatorial auctions by dynamic programming with polynomial secret sharing," in *Proc. of the Financial Cryptography Conference FC '02*, Southampton, Bermuda, March 2002.
[12] C. Bettstetter, "On the minimum node degree and connectivity of a wireless multihop network," in *Proc. of ACM international symposium on Mobile ad hoc networking and computing, Mobihoc '02*, Lausanne, Switzerland, Jun. 2002.