

A Multi-Tier Wireless Spectrum Sharing System Leveraging Secure Spectrum Auctions

Ahmed Abdelhadi, Haya Shajaiah, and Charles Clancy,

Abstract—Secure spectrum auctions can revolutionize the spectrum utilization of cellular networks and satisfy the ever increasing demand for resources. In this paper, a multi-tier dynamic spectrum sharing system is studied for efficient sharing of spectrum with commercial wireless system providers (WSPs), with an emphasis on federal spectrum sharing. The proposed spectrum sharing system optimizes usage of spectrum resources, manages intra-WSP and inter-WSP interference and provides essential level of security, privacy, and obfuscation to enable the most efficient and reliable usage of the shared spectrum. It features an intermediate spectrum auctioneer responsible for allocating resources to commercial WSPs by running secure spectrum auctions. The proposed secure spectrum auction, MTSSA, leverages Paillier cryptosystem to avoid possible fraud and bid-rigging. Numerical simulations are provided to compare the performance of MTSSA, in the considered spectrum sharing system, with other spectrum auction mechanisms for realistic cellular systems.

Index Terms—Multi-Tier Secure Spectrum Auction, Paillier Cryptosystem, Bid-rigging, Fraud

I. INTRODUCTION

Traditionally, radio spectrum management is controlled by a central government agency such as the Federal Communications Commission (FCC) in the United States. Such a centralized spectrum assignment mechanism predetermines static bands for specific usage without taking into consideration the service requirements and the dynamic nature of the radio spectrum. This results in an under-utilized pre-assigned spectrum bands while many of the commercial bands are overcrowded due to the rapid growth of wireless services. To address this limitation in the spectrum utilization, the FCC has legalized secondary markets for spectrum such that a primary spectrum licensee can lease its under-utilized spectrum to secondary incumbents [1]. Inspired by microeconomics mechanisms [2]–[4], spectrum auction seems to be a promising solution to release the under-utilized spectrum to potential secondary users [5]–[7]. There has been some previous work to deal with security issues in auction design. These works have focused on adding some new features to the auction design, such as confidentiality, fairness [8], [9] and anonymity.

Because of the reusability feature of the radio spectrum, traditional auctions can not be directly used in a spectrum auction design. Spectrum auctions should allow bidders, that are not within the interference radius of each other, to use the same frequency simultaneously. Therefore, the optimal spectrum allocation is considered NP-complete [10], [11] whereas

conventional auctions are based on optimal allocations [5]. In addition, a spectrum auction design is challenged by the effect of the back-room dealing, between insincere bidders and the auctioneer, to the whole network. A secure spectrum auction needs to avoid possible frauds of the auctioneer and bid-rigging between the bidders and the auctioneer.

In this paper, we design a secure spectrum auction that leverages Paillier cryptosystem, **MTSSA**, to avoid possible frauds and bid-riggings and provide a framework for a multi-tier spectrum sharing system to achieve an efficient utilization for the under-utilized spectrum.

A. Related Work

Most early works in spectrum auctions, such as [5], [7], have focused on single-seller multi-buyer auctions that deal with homogeneous channels. In [5], the authors have proposed **VERITAS**, a truthful mechanism that supports an eBay-like dynamic spectrum market. It is a good fit for short term and small regions based spectrum auction which is not the case in FCC required spectrum auction which is for long term and large geographical regions. To deal with interference between neighboring bidders, a conflict graph and a wireless spectrum auction framework have been proposed in [5]. Based on these concepts, a conflict graph is used to represent the interference relationship in **VERITAS** [5]. In a sealed secondary price and VCG auctions, the dominant strategy for certain bidder, when he has no information about other bidders' bids, is to bid with his true evaluation values [12]. The authors in [13] have showed that it is not always right to allocate spectrum bands to the bidder with the highest bid, as proposed in [5], if the sum of the neighbors bids is much higher than the highest bid. Their proposed solution is based on grouping nodes such that nodes with no interference are grouped together. However, their group partition approach is NP-complete under interference constraints [11].

The authors in [6] have proposed **TRUST**, a spectrum trading approach that satisfies some good properties. However, it achieves truthfulness while sacrificing one group of bidders, as it takes the group's bid as the clearing price. In [14], the authors have improved the idea of **TRUST** as they succeeded to achieve truthfulness by only sacrificing one buyer in each group. But, both works [6], [14] have inherited **McAfee** mechanism [15] which requires homogeneous channels. In [16], the proposed **TASC** mechanism was the first to consider heterogeneous channels. However, it can reduce the system efficiency as all channels are restricted to a unique clearing price. In [17], [18], **TASC** mechanism has been extended

A. Abdelhadi, H. Shajaiah, and C. Clancy are with the Hume Center for National Security and Technology, Virginia Tech, Arlington, VA, 22203 USA e-mail: {aabelhadi, hayajs, tcc}@vt.edu.

to consider spectrum reusability and diversity of channel characteristics. In [19], the authors have proposed a privacy preserving auction for spectrum trading. In [20], [21], an auction based framework is purposed. A third party leases its unused resources to service providers to provide dynamic cellular offloading.

In [5], [18], the authors have exploited frequency interference property. They used interference graph model that makes spectrum allocation, allows spectrum reuse and avoids interference. In [6], [14], the authors have utilized the reusability property by dividing buyers into groups such that buyers in the same group do not interfere with each other. Each group of buyers either wins or loses the same channel.

Most of existing works have failed to consider spectrum bands as non identical bands. Spectrum reusability in an auction design has been first addressed in [6]. In [22], the authors have modeled a spectrum auction based on spectrum reusability in a time-frequency division manner. The authors in [23] have also considered spectrum reusability in their auction design by assuming that each spectrum buyer is allowed to have multiple radios. The proposed **MTSSA** scheme also supports the frequency reusability property. Moreover, **MTSSA** supports the case of heterogeneous frequency bands.

Beside the properties of secondary price auctions that are beneficial to have in a spectrum auction, i.e. such as incentive compatibility, individual rationality and no positive transfers, it is important to secure the spectrum auction to avoid potential back room dealing. An ideal spectrum auction design would allow the auctioneer to find the best allocation of the frequency bands, determine the winners and their payments while the bidders keep their actual bidding values secret and unknown to the auctioneer. This can prevent frauds made by insincere auctioneers and bid rigging between the auctioneer and the bidders. There has been some previous works in secure spectrum auctions. The authors in [24]–[26], have used homomorphic encryption to secure traditional auction designs. In [27], the authors have considered frequency reuse in their secure spectrum auction design, and propose **THEMIS**. However, **THEMIS** does not support multi-tier spectrum sharing systems where spectrum reuse is possible among multiple service providers. In these systems a dynamic spectrum sharing approach is required to provide an efficient sharing of the spectrum among multiple service providers.

In this paper we design a truthful secure spectrum auction framework by considering the spectrum spatial reuse property and the heterogeneous propagation properties of different frequency bands. We propose **MTSSA**, a secure spectrum auction design that provides framework for a multi-tier dynamic spectrum sharing system and optimizes allocating the spectrum resources that are managed by a broker (i.e. the auctioneer). It allows the auctioneer to allocate its under-utilized frequency bands, leased from federal government, to commercial WSPs by running secure spectrum auction. By leveraging Paillier cryptosystem, **MTSSA** can prevent possible frauds and bid-rigging.

B. Our Contributions

The major contributions of the proposed spectrum auction are summarized as:

- **MTSSA** considers spectrum reusability and the case of heterogeneous frequency bands, e.g. commercial and federal bands.
- **MTSSA** provides a framework for a multi-tier dynamic spectrum sharing system that allows an efficient spectrum sharing of the under-utilized spectrum with commercial WSPs. The auctioneer allocates the under-utilized frequency bands to commercial WSPs' BSs by running a secure spectrum auction. **MTSSA** optimizes the usage of spectrum resources by managing intra-WSP and inter-WSP interference. In order to account for frequency reusability, the auctioneer divides the network into subnets and auctions the frequency bands in each of the subnets one after another. Each bidder (i.e. BS), maintains a conflict-table. The bidder updates the conflict-table and share his spectrum occupancy status with his neighbors when changes are made.
- **MTSSA** provides a truthful auction that is achieved when each bidder submits its true evaluation value. Truthfulness is a dominant strategy for **MTSSA** as it prevents manipulating the auction.
- **MTSSA** uses a payment method that satisfies some essential economic properties such as incentive compatibility, individual rationality and no positive transfers.
- **MTSSA** leverages Paillier cryptosystem [27]–[29] to create a ciphertext for the bidding values. Each BS submits its bidding values through a buffer that creates an encrypted version of the bidding values. While the actual bidding values are kept secret from the auctioneer, the auctioneer is still able to reveal the auction results and charge the bidders securely.
- **MTSSA** provides a secure spectrum auction that prevents frauds of insincere auctioneers and bid-rigging while achieving an efficient spectrum utilization, revenue and bidders' satisfaction.

The remainder of this paper is organized as follows. In Section II, the spectrum trading architecture is described and the system model for the Multi-Tier spectrum sharing secure auction **MTSSA** is outlined. In Section III, design considerations are presented. We describe the payment method for the proposed auction in Section III-A, prove its satisfaction of some desired economic properties in Section III-B and describe the design challenges in III-C. In Section IV, we present the frequency bands allocation procedure and the encryption design using Paillier cryptosystem for the proposed **MTSSA**. Simulation set up and performance analysis are discussed in Section V. Section VI concludes the paper.

II. SYSTEM MODEL

A. Spectrum Trading Architecture

We consider a spectrum trading scenario where the spectrum owner is a federal regulatory agency that leases its under-utilized spectrum on a long-term basis to a broker which manages spectrum assets and plays the role of a middleman

for the spectrum owner of the under-utilized spectrum, e.g. federal government, and the WSPs. The architecture of this spectrum assignments is represented through a spectrum pyramid as shown in Figure 1. At the top of this pyramid, is the spectrum owner that leases the under-utilized frequency bands to a spectrum broker under certain rules [1], [30], [31]. The broker represents a secondary market place that auctions these frequency bands to WSPs. At the bottom of the pyramid, are the end users devices (i.e. users equipments (UEs)) that are assigned spectrum by the WSPs base stations (BSs). In this paper we focus on designing a secure spectrum auction between the broker (i.e. the auctioneer) and the WSPs base stations to allocate the under-utilized frequency bands.

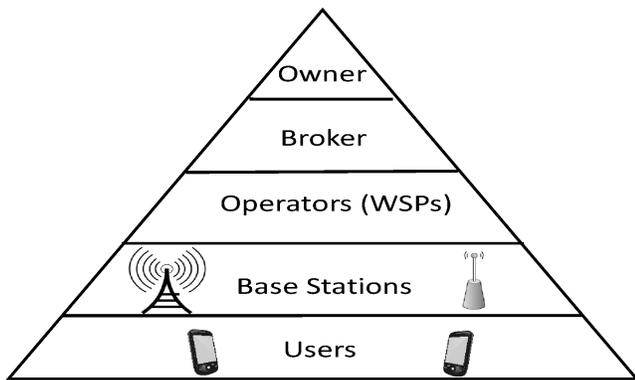


Fig. 1. A spectrum pyramid that represents an architecture for the under-utilized spectrum assignments.

B. Spectrum Auction Model

Consider a spectrum auction setting, where one auctioneer (i.e. the broker in Figure 1) auctions a set of frequency bands $\mathcal{M} = \{1, 2, \dots, M\}$ to $\mathcal{N} = \{1, 2, \dots, N\}$ bidders (i.e. nodes representing BSs) located in the same geographical region where \mathcal{N} represents a set of all bidders that belong to different WSPs. Let L be the number of WSPs where each WSP has a coverage area within the auction's geographical region. Each WSP (i.e. the l^{th} WSP) provides a mobile wireless service over multiple cellular cells. Its cellular network consists of macro cells and small cells. Within the coverage area of some macro cells, there exist one or more small cells with pico/femto BSs, see Figure 2. Let \mathcal{N}^l be the set of all of macro cells and small cells BSs that belong to the l^{th} WSP and let \mathcal{N} be a set of all nodes that belong to the L WSPs where $\mathcal{N} = \mathcal{N}^1 \cup \mathcal{N}^2 \cup \dots \cup \mathcal{N}^L$ and $N = |\mathcal{N}|$.

In this paper, we consider a multi-band spectrum auction where each node can bid for a single or multiple frequency bands from the set of available frequency bands \mathcal{M} based on its demand. Once the broker leases the spectrum owner's unused frequency bands in \mathcal{M} for a time duration T , the broker becomes the owner of the spectrum bands in \mathcal{M} . Meanwhile, the interested WSPs submit their bids to the broker. Let the allocation set $\mathcal{K} = \{\alpha^1, \alpha^2, \dots\}$ denotes the set of all possible allocations of the frequency bands \mathcal{M} . For example, given that $\mathcal{M} = \{1, 2\}$ and $\mathcal{N} = \{1, 2\}$, we have $\mathcal{K} = \{\alpha^1 = (\{1, 2\}, \{\}), \alpha^2 = (\{1\}, \{2\}), \alpha^3 =$

$(\{2\}, \{1\}), \alpha^4 = (\{\}, \{1, 2\})\}$, where $(\alpha^1 = (\{1, 2\}, \{\}))$ denotes that frequency bands 1 and 2 are allocated to bidder 1 and nothing to bidder 2. Each node submits its sealed bids $\mathbf{b}_n = [b_n(\alpha^1), b_n(\alpha^2), \dots]$, e.g. $\mathbf{b}_1 = [2, 1, 1, 0]$ indicates that node 1 bids 2 for allocation α^1 , 1 for allocation α^2 , 1 for allocation α^3 and 0 for allocation α^4 . For certain allocation $\alpha = \alpha_n$, each node n has a true evaluation value $v_n(\alpha)$. Let $\mathbf{v}_n = [v_n(\alpha^1), v_n(\alpha^2), \dots]$ be the true evaluation vector for node n . Let p_n represents the price that is charged by the auctioneer to bidder n for allocating the frequency bands. The utility of bidder n , denoted by U_n , is defined as the difference between the bidder's true evaluation value and the actual price it pays to the auctioneer p_i , $U_n = v_n(\alpha) - p_n$, for a specific allocation α . The Auctioneer's revenue from the spectrum sales is defined as $R = \sum_{n=1}^N p_n$. We assume that bidders can submit different bids for different combinations of the frequency bands. Table I summarizes some of the notations used in the design.

TABLE I
KEY SYMBOLS IN THIS PAPER

\mathcal{M}	Frequency bands set
\mathcal{N}^l	Bidders set for all bidders that belong to WSP l
\mathcal{N}	Bidders set of all nodes that belong to the L WSPs, $\mathcal{N} = \mathcal{N}^1 \cup \mathcal{N}^2 \cup \dots \cup \mathcal{N}^L$
\mathcal{K}	Allocation set $\mathcal{K} = \{\alpha^1, \alpha^2, \dots, \alpha^i\}$
\mathbf{b}_n	Node n sealed bids vector for the allocation set \mathcal{K}
\mathbf{v}_n	True evaluation vector of BS n
p_n	Price charged by the auctioneer to BS n
U_n	Bidder's utility, $U_n = v_n(\alpha) - p_n$
R	Auctioneer's revenue, $R = \sum_{n=1}^N p_n$

In Figure 2, we show two WSPs (i.e. $L = 2$) providing service in the same geographical region where the broker performs its spectrum auction. Both WSPs are interested in the auctioneer's frequency bands \mathcal{M} . Therefore, both of them participate in the spectrum auction. In the coverage area of each WSP there exists multiple macro cells and small cells managed by that WSP. BSs requesting additional frequency bands submit sealed bidding vectors to the auctioneer via an intermediate secure gateway to participate in the auction of the under-utilized federal spectrum bands. Considering the frequency reuse property [6], [11], each BS has certain coverage radius (i.e. assume it is equivalent to the cell's radius). Within the coverage radius of the n^{th} BS, non of the interfering BSs can simultaneously use any of the frequency bands that the n^{th} BS is using. However, a non-interfering BS can use the same frequency band that is simultaneously used by a BS located outside its coverage radius without causing interference, i.e. frequency reuse is utilized in our model. The auctioneer constructs an interference conflict graph for all the BSs that are participating in the auction. In Figure 3, we show the frequency conflict graph with all bidders/BSs that belong to the two WSPs, each BS is connected with other BSs located within its coverage radius (i.e. bidder n is connected with all BSs that must not simultaneously use same frequency bands due to interference between them) where the edges represent mutual interference between the

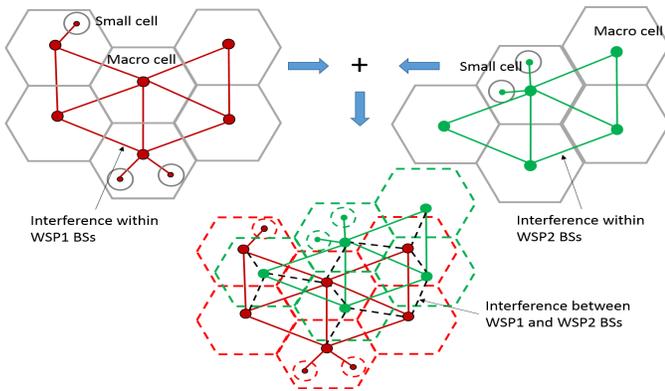


Fig. 2. Two WSPs with a coverage area within the geographical region where the auction takes place. In each WSP's macro cells and small cells, all the BSs that are interested in the auctioneer's under-utilized frequency bands are part of the interference conflict graph.

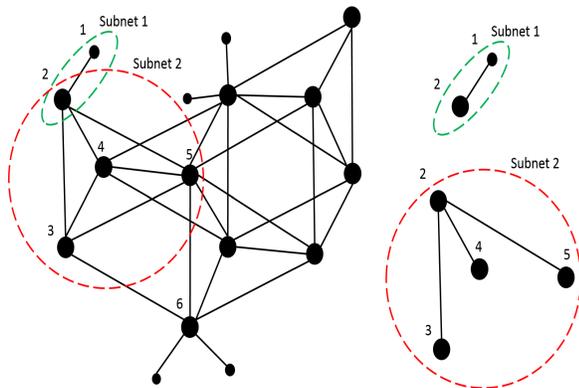


Fig. 3. Frequency conflict graph for all BSs that belong to the two WSPs shown in Figure 2. Each node represents one BS and the edges represent mutual interference between the end points (i.e. BSs). Subnet 1 consists of the small cell's BS (i.e. BS 1), which represents the root BS for the subnet, and the macro cell's BS (i.e. BS 2). Subnet 2 consists of BSs 2, 3, 4 and 5 where BS 2 is the root BS.

corresponding BSs. The interference conflict graph can be constructed using physical or protocol channel model [32]. It is assumed that there exists a pilot channel, like the one in [33], to exchange information between the auctioneer and the BSs or simply by sending that unsecured information with the bids. Furthermore, the proposed spectrum auction is executed in one subnet after another where a subnet is defined to be a group of BSs that includes one root BS, i.e. BS n , and all other BSs that are connected to it through interference edges (i.e. the BSs that have mutual interference with BS n) but not previously considered root BSs. Figure 3 shows two subnets in the frequency conflict graph of the two WSPs. In Figure 4, we show the spectrum auction model for **MTSSA** for two WSPs' participate in the spectrum auction. First, all BSs submit their encrypted bidding vectors via an intermediate gateway that is operated by federal government. The auctioneer then carries out a secure spectrum auction in one subnet after another. It then allocates the winning BSs frequency bands and charges them for the allocated resources.

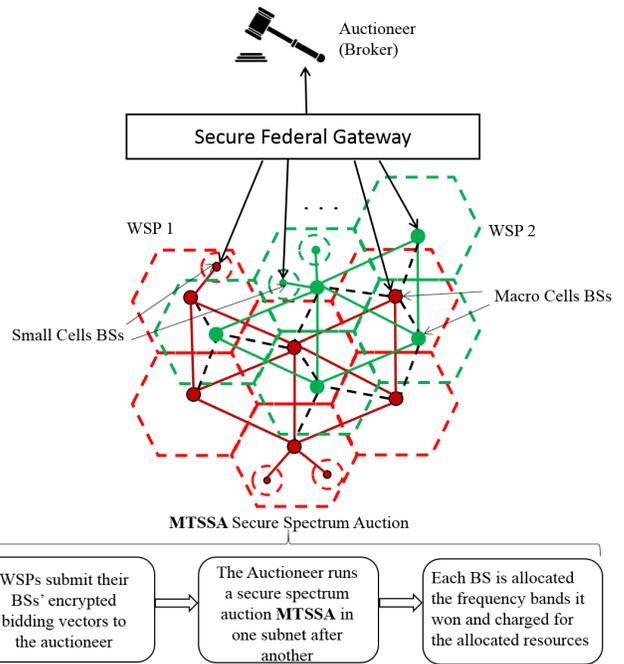


Fig. 4. Spectrum auction model for the proposed **MTSSA** with two WSPs' BSs participating in the auction.

III. DESIGN CONSIDERATIONS

In this section, we present the payment method for the proposed auction. We also discuss some economic properties that need to be considered in the design and prove that by using a VCG based auction approach some desired economic properties can be satisfied.

A. The Payment Method

Our goal is to use a payment rule that satisfies some of the required economic properties, such as incentive compatibility, individual rationality and no positive transfers. In addition, it is important for the payment rule to provide a satisfactory revenue for the auctioneer. Under certain assumptions, it has been proven that VCG auction satisfies these three economic properties while maximizing the auctioneer's revenue [34]. VCG auction is also proven to be Pareto efficient [35]. In VCG, each bidder submits its true evaluation values regardless of the bidding values that other bidders submit. This is a dominant strategy for the bidder to maximize its utility and win the auction. In our design, we use a payment method that is based on VCG mechanism with Clarke pivot payments [36]. Using this payment rule, each bidder pays the difference between the social welfare with and without his participation (i.e. bidder n pays the externality he causes). Consider the same system setup as described in Section II. Each bidder n submits its sealed bidding vector \mathbf{b}_n for the allocation set \mathcal{K} . The auctioneer selects a Pareto efficient allocation $\alpha^* \in \mathcal{K}$ where α^* is defined as

$$\alpha^* = \arg \max_{\alpha \in \mathcal{K}} \sum_n b_n(\alpha). \quad (1)$$

With truthful bidding values, the auctioneer assigns its frequency bands \mathcal{M} based on α^* allocation. Furthermore, let

$\alpha_{-n}^* \in \mathcal{K}$ be an allocation without node n participating that is defined as

$$\alpha_{-n}^* = \arg \max_{\alpha \in \mathcal{K}} \sum_{k \neq n} b_k(\alpha). \quad (2)$$

The auctioneer charges bidder n a payment p_n that is equivalent to

$$p_n = \sum_{k \neq n} b_k(\alpha_{-n}^*) - \sum_{k \neq n} b_k(\alpha^*). \quad (3)$$

Then, the utility of bidder n can be expressed as

$$\begin{aligned} U_n &= v_n(\alpha^*) - p_n \\ &= v_n(\alpha^*) - \left(\sum_{k \neq n} b_k(\alpha_{-n}^*) - \sum_{k \neq n} b_k(\alpha^*) \right) \\ &= [v_n(\alpha^*) + \sum_{k \neq n} b_k(\alpha^*)] - \sum_{k \neq n} b_k(\alpha_{-n}^*). \end{aligned} \quad (4)$$

B. Desired Economic Auction Properties

It is essential for an auction to have certain economic properties. First, we discuss these economic properties and then we prove that by using a VCG based auction approach these properties can be satisfied.

- 1) **Incentive Compatibility (truthfulness):** An auction is incentive compatible if non of the bidders can get higher utility by not reporting its true evaluation vector. Based on this property, a dominant strategy for any bidder is to declare its true evaluation value regardless of what the other bidders do.
- 2) **Individual Rationality:** An auction is individually rational if the utility U_n for each bidder n is greater or equal zero (i.e. $U_n \geq 0$). Meaning that the winning bidders obtain non-negative utility (i.e. bidders do not pay more than their evaluation values) from the auction and no one suffer as a result of participating in the auction.
- 3) **No Positive Transfers:** In auctions with no positive transfers, the payment of any bidder n must be greater or equal zero (i.e. $p_n \geq 0$). This prevents situations when the auctioneer has to pay the bidders.

In Lemma III.1, Lemma III.2 and Lemma III.3, we show that by using the payment method and the VCG based auction approach discussed above, the aforementioned desired economic properties can be satisfied.

Lemma III.1. *Let \mathbf{v}_n and $\mathbf{v}'_n \neq \mathbf{v}_n$ be the n^{th} bidder bidding vector when it is equivalent to its true evaluation values and any other values, respectively, and let α^* and $\alpha^{*'} be the allocations that maximize the social welfare when \mathbf{v}_n and \mathbf{v}'_n are declared, respectively. Then, for the n^{th} bidder, the utility $U_n \geq U'_n$.$*

Proof: Using the utility definition and payment method in Section III-A, the utility of bidder n is $U_n = v_n(\alpha^*) + \sum_{k \neq n} v_k(\alpha^*) - \sum_{k \neq n} v_k(\alpha_{-n}^*)$ when declaring \mathbf{v}_n whereas the utility of bidder n is $U'_n = v_n(\alpha^{*'}) + \sum_{k \neq n} v_k(\alpha^{*'}) - \sum_{k \neq n} v_k(\alpha_{-n}^*)$ when declaring \mathbf{v}'_n . Since α^* is the allocation that maximizes the social welfare, we have the following inequality:

$$\sum_n v_n(\alpha^*) \geq \sum_n v_n(\alpha^{*'}). \quad (5)$$

Now, by subtracting the term $\sum_{k \neq n} v_k(\alpha_{-n}^*)$ from both sides of equation (5), we get $U_n \geq U'_n$ which is the incentive compatibility property. ■

Lemma III.2. *Let α^* and α_{-n}^* be the allocations that maximize the social welfare with and without node n 's participation, respectively, with the assumption that each bidder submits its true evaluation values. Then each bidder n do not suffer as a result of participating in the auction and the auction's winners do not pay more than their evaluation values (i.e. $U_n \geq 0$).*

Proof: To show individual rationality, consider the utility of node n :

$$\begin{aligned} U_n &= v_n(\alpha^*) + \sum_{k \neq n} v_k(\alpha^*) - \sum_{k \neq n} v_k(\alpha_{-n}^*) \\ &\geq \sum_j v_j(\alpha^*) - \sum_j v_j(\alpha_{-n}^*) \\ &\geq 0. \end{aligned}$$

The first inequality holds since $v_n(\alpha^*) + \sum_{k \neq n} v_k(\alpha^*) = \sum_j v_j(\alpha^*)$, $\sum_j v_j(\alpha_{-n}^*) \geq \sum_{k \neq n} v_k(\alpha_{-n}^*)$ and $\sum_j v_j(\alpha_{-n}^*) \geq 0$. The second inequality holds because α^* is the allocation that maximizes the social welfare, $\sum_j v_j(\alpha^*)$. ■

Lemma III.3. *As a result of using the payment method in Section III-A, the auction has no positive transfers (i.e. $p_n \geq 0$ for each bidder n).*

Proof: From equation (3), we have $p_n = \sum_{k \neq n} b_k(\alpha_{-n}^*) - \sum_{k \neq n} b_k(\alpha^*) \geq 0$, since α_{-n}^* is the allocation that maximizes the social welfare without the n^{th} bidder participation, $\sum_{k \neq n} b_k(\alpha_{-n}^*)$. ■

C. Design Challenges

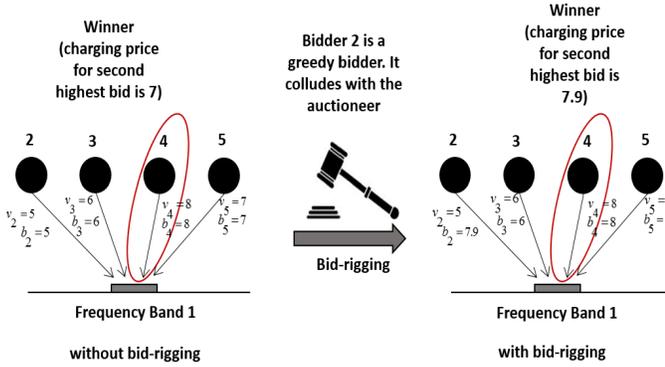
Truthfulness is one of the important properties that needs to be taking into consideration when designing a spectrum auction. Sealed secondary price auction and VCG auction are very preferable as they guarantee that bidders submit their true evaluation values. As mentioned before, VCG auction has many properties that are essential to have in a spectrum auction. However, VCG requires finding an optimal allocation which is NP-complete because of the spectrum spatial reusability property. In addition, VCG is vulnerable to frauds of the auctioneer and bid-rigging between the insincere auctioneer and greedy bidders [27]. Therefore, VCG auction can not be used in a spectrum auction without countermeasures for fraud and bid-rigging.

Bid-rigging between a greedy bidder and an auctioneer can occur for the benefit of both. Since the auctioneer is aware of all bidders' bidding values, he can collude with a greedy bidder and reveal the winning bid value to him. In Figure 5, we show an example of a spectrum auction where the auctioneer auctions one frequency band $|\mathcal{M}| = 1$ to four BSs (i.e. subnet 2 of the frequency conflict graph that is shown in Figure 3). The auctioneer runs a VCG auction that is equivalent to a sealed secondary price auction for one frequency band auction. In Figure 5(a), we show an example of bid-rigging. Bidder 4 is

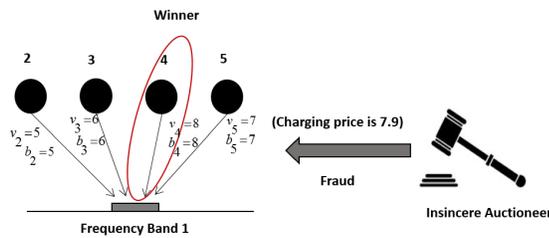
the winner and bidder 2 is a greedy bidder who colludes with the auctioneer and learns about the highest bid. As a result, bidder 2 bids a value that is higher than his true evaluation but a little bit less than the highest bid. By doing so, the auctioneer considers the bidding value of bidder 2 to be the charging price for the winner (i.e. bidder 4). By such a bid-rigging action, the auctioneer can make more profit and share the spoils with bidder 2.

On the other hand, a fraud occurs when an insincere auctioneer overcharges the winner in order to increase his own profit. This results in an unexpected bad utility for the winner. In Figure 5(b), bidder 4 is the winner and the charging price should be 7 which is equivalent to the second highest bid. However, the insincere auctioneer charges bidder 4 at 7.9 to obtain higher revenue. This is possible since all bidding values are sealed and bidders do not know about the bidding values of each other.

To avoid possible bid-rigging and frauds, a successful spectrum auction design needs to take into consideration securing the auction by making the auctioneer able to decide how to allocate the frequency bands while keeping the bidders' actual bidding values unknown to the auctioneer. This is essential to avoid possible back-room dealing and ensure a secure spectrum auction.



(a) Bid-rigging between an insincere auctioneer and a greedy bidder



(b) Frauds of an insincere auctioneer

Fig. 5. Examples of bid-rigging and frauds in an unsecured spectrum auction of one frequency band and four BSs.

IV. MTSSA: SECURE SPECTRUM AUCTION DESIGN

In order to enable an efficient usage of the under-utilized shared spectrum managed by a broker. It is important to design a secure spectrum auction that allows the broker to provide a sufficient level of security, privacy and obfuscation

to enable a reliable and efficient usage of the shared spectrum. In order to thwart back-room dealing, it is essential to have a mechanism that allows the auctioneer to find the maximum bid among all bidders without knowing their actual bids. The proposed **MTSSA** leverages Paillier cryptosystem to avoid possible frauds and bid-rigging. In this section, we first describe Paillier cryptosystem and point out its special features. We then discuss **MTSSA** frequency bands allocation procedure. Finally, we present the security part of **MTSSA**.

A. Paillier Cryptosystem

Some of Paillier cryptosystem properties are essential for our secure spectrum auction design. Paillier cryptosystem [27]–[29] is a probabilistic public key encryption system, i.e. the term probabilistic encryption indicates that when encrypting the same plaintext for multiple times it yields different ciphertexts, that satisfies special features such as homomorphic addition, indistinguishability and self blinding.

The homomorphic properties of Paillier cryptosystem provide it with a notable feature. As the encryption function of a message m , is given by $C(m)$, is additively homomorphic, i.e. $C(m_1 + m_2) = C(m_1)C(m_2)$. On the other hand, with the indistinguishability property of Paillier cryptosystem, if the plaintext m is encrypted twice, the two created ciphertexts are different from each other and no one can distinguish the original plaintexts, except by random guessing, unless decrypting the original ciphertexts. The self blinding property allows changing the ciphertext publicly without affecting the plaintext. Therefore, from the ciphertext $C(m)$, it is possible to compute a different randomized ciphertext $C'(m)$ without knowing the decryption key or the original plaintext.

B. Frequency Bands Allocation Procedure

All BSs that are interested in the auction and belong to the WSPs within the geographical region of the auction submit their bidding values to participate in the auction. Based on the location of these BSs and which WSPs they belong to, the auctioneer creates an interference conflict graph (i.e. like the one in Figure 3). The auctioneer executes the auction in one subnet at a time. For each subnet, the auctioneer selects a random BS $n \in \mathcal{N}$ to be the current root BS and considers its corresponding subnet, i.e. connected nodes/BSs. After solving for the current subnet, the auctioneer selects a new BS, that has not been a root BS before, to be the new root BS and excludes any previous root BS from its subnet along with the allocated frequency bands to these BSs. Following the same procedure, the auctioneer continues to execute the auction in one subnet after another until each BS has participated in the auction. Based on the subnet auction results, the auctioneer allocates the corresponding root node the frequency bands and charges it for the allocated resources. Each Bidder that is participating in the auction maintains a local conflict-table, i.e. as in [13]. The bidder updates his bidding values if any BS within his interference range (i.e. connected to him in the interference conflict graph) wins frequency bands.

The **MTSSA** procedure is presented in the following steps:

1. **Each BS $n \in \mathcal{N}$ sets up its conflict-table and submits its encrypted version of bidding values \mathbf{b}_n :** Each WSP l within the auctioneer's geographical region creates a set of all BSs \mathcal{N}^l that are interested in bidding for the auctioneer's under-utilized frequency bands. Each BS $n \in \mathcal{N}^l$ creates a conflict-table with all the interfering BSs denoted by \mathcal{I}_n (i.e. \mathcal{I}_n is a set of all BSs that are located within the coverage area of BS n). Each WSP l provides an update to each BS $n \in \mathcal{N}^l$ regarding its interfering BSs \mathcal{I}_n^1 . Each $n \in \mathcal{N}^l$ creates its bidding vector \mathbf{b}_n that will be an input to a buffer that encrypts the bidding values. The encrypted bids are then submitted to federal gateway for randomization, see Section IV-C, then sent to auctioneer, see Figure 4. Neither the auctioneer nor the other bidders know the actual bidding values \mathbf{b}_n that BS n has submitted. We show in Section IV-C1 the procedure of encrypting the bidding values using Paillier encryption.

2. **Start with a random BS $n \in \mathcal{N}$ and consider its corresponding subnet:** The auctioneer does not have an optimal choice regarding which subnet it starts the auction from in order to maximize his revenue. Therefore, the auctioneer selects a random bidder n from the set \mathcal{N} and considers its corresponding subnet (i.e. a subnet consists of a root BS n and all other BSs connected to BS n in the interference conflict graph except BSs that have been previously considered root BSs).

3. **The auctioneer carries out a secure spectrum auction in the subnet of the selected BS n :** The auctioneer performs a secure spectrum auction procedure (detailed in Section IV-C) in the current subnet under consideration.

4. **Allocate frequency bands and charge price:** Based on the subnet auction's results, the auctioneer allocates the root BS frequency bands and charges it for the allocated resources. The allocation and the payment vary based on the location of root BS and its relative bid with respect to neighboring BSs. Each winning BS stores its allocated frequency bands and its charging price in the conflict-table.

5. **Proceed to next root BS:** A new root BS is selected based on a random selection done by auctioneer and the corresponding subnet secure bids are sent to auctioneer and the process is repeated starting from step 2.

Algorithm IV.1 summarizes **MTSSA** spectrum auction procedure.

C. Secure Spectrum Auction Using Paillier Cryptosystem

In order for **MTSSA** to ensure a secure auction, it is important to design **MTSSA** such that no way for the auctioneer to manipulate the auction. VCG auction is proven to have the incentive compatibility property from the bidders side which is essential for our design. In order for **MTSSA** to prevent the auctioneer from conducting any frauds or bid-rigging [27], it is important to limit the auctioneer's capability by making him only able to exploit the winners and their payments without knowing the actual bidding values. So, by leveraging Paillier

¹It is assumed that each WSP l is aware of all BSs in its coverage area within the auction's geographical region, whether they belong to it or to other WSPs. Therefore, the set of interfering BSs \mathcal{I}_n includes all BSs within the coverage area of BS n that belong to WSP l as well as BSs that belong to other WSPs.

Algorithm IV.1 MTSSA Frequency Bands Allocation

```

 $\mathcal{N} = \mathcal{N}^1 \cup \mathcal{N}^2 \dots \cup \mathcal{N}^L$  {i.e.  $\mathcal{N}$  is the set of all BSs in the
interference conflict graph}
 $\mathcal{N}_0 = \mathcal{N}$ 
Auctioneer generates his private and public keys of Paillier
cryptosystem
Auctioneer sends public key and element  $x$  to all BSs via
pilot channel
while  $\mathcal{N} \neq \emptyset$  do
   $n = \text{random}(\mathcal{N})$  {Auctioneer selects a random BS}
   $\mathcal{N}_n = \text{include\_conflict}(n)$  {Auctioneer adds BSs that
form the  $n^{\text{th}}$  subnet from conflict-table of  $n^{\text{th}}$  BS as root}

   $\mathcal{N}_- = (\mathcal{N}_0 \setminus \mathcal{N}) \cap \mathcal{N}_n$  { $\mathcal{N}_-$  is set of previous root BSs
in the  $n^{\text{th}}$  subnet}
   $\mathcal{N}_n = \mathcal{N}_n \setminus \mathcal{N}_-$  {Auctioneer removes from  $\mathcal{N}_n$  previous
root BSs}
   $\mathcal{M}_- = \text{include\_alloc}(\mathcal{N}_-)$  { $\mathcal{M}_-$  is set of freq. bands
allocated to  $\mathcal{N}_-$ }
   $\mathcal{M}_n = \mathcal{M} \setminus \mathcal{M}_-$  {Auctioneer removes from  $\mathcal{M}$  freq.
bands allocated to  $\mathcal{N}_-$ }
   $\mathcal{K}_n = \text{alloc\_vect}(\mathcal{N}_n, \mathcal{M}_n)$  {Auctioneer forms alloca-
tion vector  $\mathcal{K}_n$  and sends to  $\mathcal{N}_n$ }
  BSs  $\in \mathcal{N}_n$  send encrypted bids to federal gateway
  Federal gateway randomizes bids and forward to auction-
eer
  Auctioneer selects the highest allocation  $\alpha^*$ 
  Auctioneer charges price  $p_n$  to BS  $n$ 
   $\mathcal{N} = \mathcal{N} \setminus \{n\}$ 
end while

```

cryptosystem in our design, **MTSSA** can ensure a secure spectrum auction. Next we discuss in details how both the bidders and the auctioneer need to collaborate in order to carry out a secure spectrum auction.

1) *Impact of Paillier Cryptosystem on the Bidding Values:* **Encrypting the Bidding Values:** Each bidder submits its bidding values through a buffer that uses Paillier cryptosystem to encrypt the bidding values and create a vector of ciphertexts for each bidding value. Let s be a number that any actual bidding value does not exceed and let $z = b(\alpha)$ be the actual bidding value for allocation α such that $1 \leq z \leq s$. Let the vector of ciphertexts for z be $\mathbf{c}(z)$ that is given by

$$\begin{aligned} \mathbf{c}(z) &= (c^1, \dots, c^s) \\ &= (\underbrace{C(x), \dots, C(x)}_z, \underbrace{C(0), \dots, C(0)}_{s-z}), \end{aligned} \quad (6)$$

where $C(x)$ is the Paillier encryption of the public element x (i.e. $x \neq 0$) and $C(0)$ is the Paillier encryption of 0. As mentioned before, C has a self blinding property which makes z undeterminable without decrypting the elements in $\mathbf{c}(z)$.

Selecting the Maximum Bidding Value: The auctioneer can determine the bidder with the maximum bidding value from the encrypted bidding values without knowing their

actual values. Let $\mathbf{c}(z_j) = (c_j^1, \dots, c_j^s)$ be the encrypted bidding vector of bidder n for certain allocation α . First, consider the product of all encrypted bidding vectors for allocation α ,

$$\prod_j \mathbf{c}(z_j) = (Q_1, \dots, Q_s) = \left(\prod_j c_j^1, \dots, \prod_j c_j^s \right). \quad (7)$$

Due to the homomorphic addition property of Paillier cryptosystem, Q_i (i.e. $1 \leq i \leq s$ and $i \neq j$) is equivalent to

$$Q_i = \prod_j c_j^i = C^{\gamma(i)}(x) = C(\gamma(i)x), \quad (8)$$

where $\gamma(i)$ represents the number of values that are equal to or greater than i , i.e. $\gamma(i) = |\{j : z_j \geq i\}|$. Given that $\gamma(i)$ monotonically decreases when i increases, one way to find the maximum of these bidding values is to decrypt Q_i and check whether the decrypted value $C^{-1}(Q_i)$ equals 0 or not for i changing from $s \rightarrow 1$. Once the largest i with a decrypted value $C^{-1}(Q_i) \neq 0$ is found, then the maximum bidding value for the allocation α is determined to be i (i.e. $i = \max\{z_j\}$).

Randomizing the Encrypted bidding Values: Without knowing z , the federal gateway adds a constant t to the encrypted vector $\mathbf{c}(z)$ and randomizes the rest of its elements. This results in the following vector

$$\mathbf{c}'(z+t) = \underbrace{(C(x), \dots, C(x))}_z, c'_1, \dots, c'_{s-z}, \quad (9)$$

where t can not be obtained from either $\mathbf{c}(z)$ or $\mathbf{c}'(z+t)$ because of the self blinding property of Paillier cryptosystem. In addition, t can not be figured out by comparing $\mathbf{c}(z)$ and $\mathbf{c}(z+t)$ during the shifting and randomizing process.

2) *Securing the MTSSA Subnet Auction:* By using Paillier cryptosystem as discussed in Section IV-C1, with encrypted bidding values it is still possible to find the maximum bid and the encrypted bidding vectors are randomized without knowing their actual values. This makes it possible to apply a VCG based auction in each subnet. As mentioned before, the proposed MTSSA auction is carried out in one subnet after another. In certain subnet, MTSSA auction is performed as follows:

1. The auctioneer generates his private and public keys of Paillier cryptosystem and publishes his public key and element x over the pilot channel.

2. Each BS submits its sealed bidding vector $\mathbf{b}_n = \mathbf{v}_n$ (i.e. its true evaluation values since we consider a VCG based auction). The auctioneer creates representing vectors $\mathbf{C}_T = \mathbf{C}(O)$, $\mathbf{C}_1 = \mathbf{C}(O), \dots, \mathbf{C}_N = \mathbf{C}(O)$ where N is the number of bidders (i.e. BSs), the initial $O(\alpha)$ equals 0 and the size of vector \mathbf{C} equals $|\mathcal{K}|$. In order for bidder z to keep his bidding value b_z secret, he adds his encrypted bidding value to all of the representing vectors except \mathbf{C}_z . Once all bidders are done performing this addition, the auctioneer obtains

$$\mathbf{C}_T = \left(\prod_n \mathbf{c}(b_n(\alpha_1)), \dots, \prod_n \mathbf{c}(b_n(\alpha_{|\mathcal{K}|})) \right). \quad (10)$$

Due to the homomorphic addition property of Paillier cryptosystem, equation (10) is equivalent to

$$\mathbf{C}_T = \left(\mathbf{c}\left(\sum_n b_n(\alpha_1)\right), \dots, \mathbf{c}\left(\sum_n b_n(\alpha_{|\mathcal{K}|})\right) \right) = \mathbf{C}\left(\sum_z b_z\right), \quad (11)$$

and

$$\mathbf{C}_z = \mathbf{C}\left(\sum_{n \neq z} b_n\right) \quad 1 \leq z \leq N. \quad (12)$$

3. Federal gateway adds $\theta(\alpha) = t$ to $\mathbf{C}_T, \mathbf{C}_1, \dots, \mathbf{C}_N$ to obtain $\mathbf{C}(\sum_n b_n + \theta)$ and $\mathbf{C}(\sum_{n \neq z} b_n + \theta) \forall z$. It sends these randomized encrypted bids to auctioneer.

4. In order for the auctioneer to select an allocation for the current subnet and find its corresponding charging price, it finds the maximum sum value

$$\begin{aligned} g &= \arg \max_{\alpha \in \mathcal{K}} \left(\sum_n b_n(\alpha) + \theta(\alpha) \right) \\ &= \arg \max_{\alpha \in \mathcal{K}} \left(\sum_n b_n(\alpha) \right) + t, \end{aligned} \quad (13)$$

which can be determined by the auctioneer by taking the product of all the encrypted elements in \mathbf{C}_T , i.e. as discussed in Section IV-C1, which is equivalent to $\prod_{i=1}^{|\mathcal{K}|} \mathbf{c}(\sum_{n=1}^N b_n(\alpha_i) + t)$. The auctioneer determines the maximum element in that product which is equivalent to g in (13).

5. For each allocation α , the auctioneer decrypts the g^{th} element of vector $\mathbf{c}(\sum_n b_n(\alpha) + \theta(\alpha))$ in \mathbf{C}_T and finds whether it equals 0 or x . If it equals x at allocation α^* , then the auctioneer selects α^* to be the allocation that maximizes $\sum_n b_n$ in the current subnet and considers its corresponding BSs.

6. To find the charging price for the root BS, the auctioneer decrypts $\mathbf{c}(\sum_{n \neq z} b_n(\alpha^*) + \theta)$ of \mathbf{C}_z and finds the masked value $(\sum_{n \neq z} b_n(\alpha^*) + \theta)$.

7. The auctioneer then finds the maximum masked bid of the product of the encrypted elements $\max_{\alpha \in \mathcal{K}} (\sum_{n \neq z} b_n(\alpha) + t)$, similar to Step 4, which is equivalent to $(\sum_{n \neq z} b_n(\alpha_{-z}^*) + t)$.

8. The auctioneer then finds the charging price for root BS of allocation α^* that is given by

$$p_z = \left(\sum_{n \neq z} b_n(\alpha_{-z}^*) + t \right) - \left(\sum_{n \neq z} b_n(\alpha^*) + t \right). \quad (14)$$

V. SIMULATION AND ANALYSIS

In this section, we first evaluate the performance of the proposed MTSSA spectrum auction and compare it with the performance of other spectrum auction mechanisms. Three performance metrics are considered: spectrum utilization, auctioneer's revenue and bidders' satisfaction. These are the most important performance metrics that need to be maximized in a successful spectrum auction. In addition, we analyze the security strategy of the proposed secure spectrum auction MTSSA that makes it able to avoid possible frauds and bid-rigging.

A. Performance Analysis

We consider a spectrum auction hosted by the auctioneer (the broker) in a $A * A m^2$ square geographical region with two cellular networks located within the same region where the auction takes place. Each cellular network belongs to different WSP, i.e. there exists two WSPs $L = 2$ that are interested in participating in the spectrum auction. Each WSP has certain number of BSs, located in macro cells or small cells, that are interested in bidding for the auctioneer's under-utilized frequency bands. The BSs are randomly placed in the auction's geographical area. Suppose that the frequency mutual interference between any two BSs is based on the distance between them. Any two macro cells' BSs located within a distance of $0.4A$ can not be allocated the same frequency bands and these BSs are connected together in the frequency conflict graph. Also, any small cell's BS can not be allocated the same frequency bands of any other BS located within a distance of $0.05A$ from it. In our simulation setup, bids are selected randomly with bidding per frequency band is monotonically decreasing, i.e the BS's bid for first frequency band is higher than second frequency band and second frequency band is higher than third frequency band and so on, see [37]–[39].

Based on the frequency assignment policy, three spectrum auction mechanisms are considered in our simulation as described in the following three cases:

- *Case 1* : Conventional spectrum leasing (**CSL**) case where the government directly leases the under-utilized spectrum to each WSP with heist bid. Once the WSP is assigned certain frequency bands, it then allocates these resources internally to its BSs.
- *Case 2* : **MTSSA** where each WSP directly submits all of its BSs' encrypted bids to the auctioneer. The auctioneer decides the frequency bands allocation to each BS whereas the WSP has no control on the resources allocation process. By using **MTSSA** frequency assignment process, each BS can be allocated any number of frequency bands between zero and all of the auctioneer's under-utilized frequency bands.
- *Case 3* : **MTSSA** with fixed limit (**MTSSA-FL**) is a special case of the proposed **MTSSA** where the frequency bands allocation policy is similar to the proposed **MTSSA** but is restricted in the number of frequency bands that each BS can bid for. Each BS bids for a fixed number of frequency bands and it can be allocated any number of frequency bands between zero and that fixed number of frequency bands it submitted the bids for.

We ran Monte Carlo Simulation, for the three cases described above, and the results are averaged over 25 independent runs in which the location and the bidding values of the BSs are generated randomly and the performance metrics are evaluated. We consider the network setup described above with different number of macro cells and small cells' BSs that belong to the two WSPs. First, we consider 8 BSs, i.e. 4 macro cells' BSs and 4 small cells' BSs. Second, we consider 12 BSs, i.e. 6 macro cells' BSs and 6 small cells' BSs. Third, we consider 16 BSs, i.e. 8 macro cells' BSs and 8 small cells'

BSs.

We consider three performance metrics to compare between **CSL**, **MTSSA**, and **MTSSA-FL**. These performance metrics are:

- **Spectrum Utilization**: It is represented by the sum of the frequency bands that are allocated by the auctioneer to the winning BSs.
- **Auctioneer's Revenue**: It is given by the sum of all BSs' payments, i.e $R = \sum_{n=1}^{n=N} p_n$.
- **Bidders' Satisfaction**: It is represented by the sum of all winning BSs' utilities divided by the sum of all BSs' evaluation values, i.e. $\sum_{n \in \mathcal{A}} U_n / \sum_{n \in \mathcal{N}} v_n$, where \mathcal{A} is the set of BSs that are allocated frequency bands.

In Figure 6, we compare the performance of the proposed **MTSSA** and its special case **MTSSA-FL** with that of a **CSL** based auction. We plot the spectrum utilization, auctioneers revenue and BSs satisfaction of the three auction designs with different number of BSs, i.e. 8 BSs, 12 BSs and 16 BSs as mentioned before.

Figure 6(a) shows the spectrum utilization versus the number of available under-utilized frequency bands. As the number of frequency bands increases, the spectrum utilization, which is represented by the number of the allocated frequency bands, also increases for each of the three auction mechanisms. For certain number of frequency bands, each of the three mechanisms shows higher utilization when the number of BSs (bidders) increases. However, it is not surprising that the performance in terms of utilization for **CSL** is lower than that for the other two mechanisms. This is because in **CSL**, the auctioneer assigns each WSP different frequency bands and the frequency bands assigned to each WSP are then auctioned among BSs that belong to that WSP. In the case of **CSL**, the auctioneer considers one frequency conflict graph for each WSP and frequency reusability is not applicable among BSs that belong to different WSPs, i.e. BSs that belong to different WSPs and are not within the interference range of each other are not allowed to use the same frequency bands. Moreover, the utilization in the cases of **MTSSA** and **MTSSA-FL** is almost the same when the number of available frequency bands is low and is slightly higher for **MTSSA** than that for **MTSSA-FL** when the number of available frequency bands is higher.

Figure 6(b) shows that for each of the three mechanisms, the auctioneer's revenue increases when the number of BSs increases. This is expected as the auctioneer's revenue increases with more bidders requesting more resources. However, for certain number of BSs, the auctioneer's revenue for **MTSSA-FL** is higher than that for **MTSSA** and **CSL** and as expected the auctioneer's revenue is the lowest in the case of **CSL**. The bump of **MTSSA** over **CSL** is from the payments received from winning BSs that belong to different WSPs, and not located within the interference range of each other, but are allocated similar frequency bands.

We show in Figure 6(c) that as the number of frequency bands increases, the bidders' satisfaction also increases until it saturates when each bidder is allocated the number of frequency bands he bids for. On the other hand, the bidders satisfaction for **CSL** is higher than that for **MTSSA** and **MTSSA-FL** due to the less number of BSs competing for

resources as all the frequency bands are allocated to one WSP. Therefore, the bidders who belong to the winning WSP get their requested frequency bands while paying less.

The comparison between the three mechanisms in Figure 6 shows that **MTSSA** behaves well in terms of performance and proves to be better than the conventional spectrum leasing mechanism as it considers spectrum reusability and in the same time it guarantees a secure spectrum auction.

B. MTSSA Security Analysis

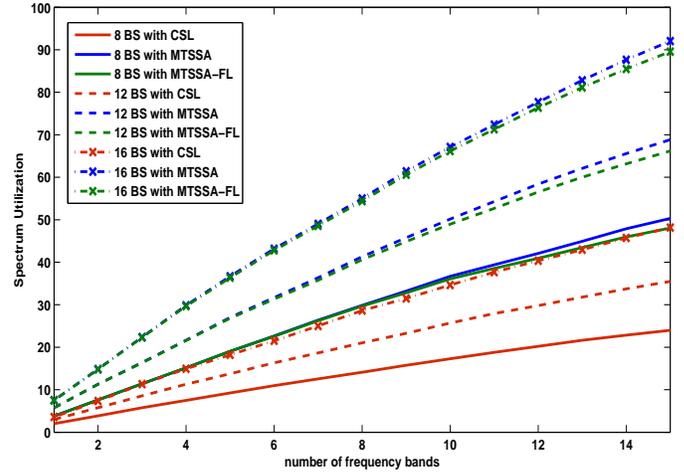
As discussed before, our proposed **MTSSA** leverages Paillier cryptosystem in order to ensure that the BSs' bidding values are kept unknown to the auctioneer while the auctioneer is still able to find the winners and charges them their corresponding payments. This is possible because of the indistinguishability property of Paillier cryptosystem, i.e. it is not possible to know the value of z without decrypting each element in $c(z)$, and the self blinding property that makes it impossible to find a mapping function from $c(t)$ to $c^{-1}(z+t)$ [27]–[29]. In order to prevent an insincere auctioneer from performing any frauds, we consider a secure gateway that is operated by federal government. Its main function is to randomize the encrypted bids by the random constant t . So auctioneer can determine the winning allocation and assign secondary price without any knowledge of the original bidding values of BSs. This way **MTSSA** can avoid bid-rigging between an insincere auctioneer and a greedy bidder. This can be guaranteed because even if certain bidder colludes with auctioneer, he can not find out about the bidding values as federal gateway randomized it. Therefore, all BSs that belong to different WSPs are treated equally by the proposed **MTSSA** and their bidding values are kept secret from the auctioneer who is only able to determine the winners and their corresponding charged price.

VI. CONCLUSION

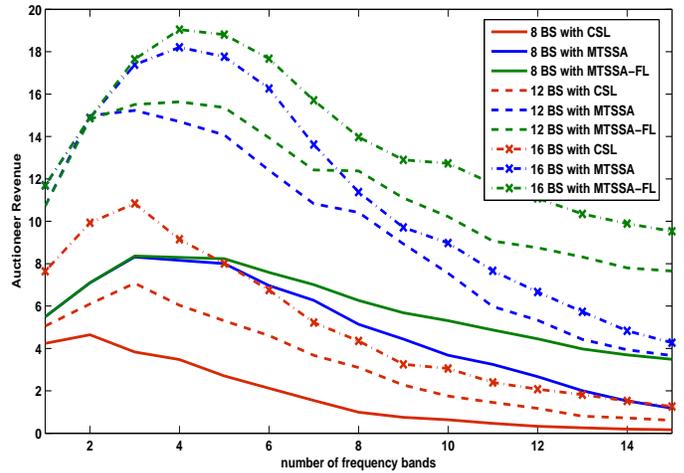
In this paper, we propose a secure spectrum auction **MTSSA** for a multi-tier dynamic spectrum sharing system. By considering the spectrum reusability property, **MTSSA** enables an efficient sharing of the under-utilized frequency bands with commercial WSPs. In order to allow spectrum reuse among multiple WSPs, the frequency conflict graph that is considered by **MTSSA** includes all BSs that belong to multiple WSPs and the auction is carried out in one subnet after another. **MTSSA** leverages Paillier cryptosystem and a federal gateway to keep the BSs' bidding values unknown to the auctioneer. The auctioneer uses the additive homomorphic property of Paillier cryptosystem to find the winning bidders and their charging prices. This prevents possible frauds and bid-rigging between an insincere auctioneer and greedy bidders. Compared with conventional spectrum leasing mechanism, **MTSSA** has shown better performance while providing a secure spectrum auction against possible back room dealings.

REFERENCES

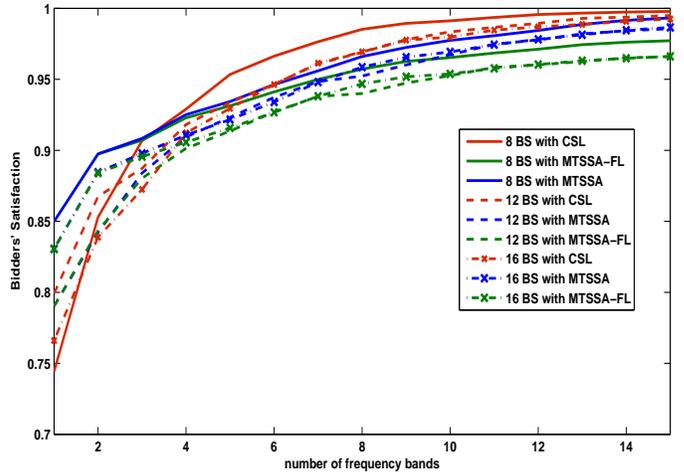
[1] FCC (2004), "Second report and order: Promoting efficient use of spectrum through elimination of barrier to the development of secondary markets," Tech. rep., FCC 04-167.



(a) Spectrum Utilization



(b) Auctioneer's Revenue



(c) Bidders' Satisfaction

Fig. 6. Performance comparison of **MTSSA**, **MTSSA-FL** and **CSL**.

[2] S. Sengupta and M. Chatterjee, "An Economic Framework for Dynamic Spectrum Access and Service Pricing," *Networking, IEEE/ACM Transactions on*, vol. 17, pp. 1200–1213, Aug 2009.

[3] M. Pan, F. Chen, X. Yin, and Y. Fang, "Fair Profit Allocation in the Spectrum Auction Using the Shapley Value," in *Global Telecommunications*

- Conference, 2009. *GLOBECOM 2009. IEEE*, pp. 1–6, Nov 2009.
- [4] J. Zhang and Q. Zhang, “Stackelberg Game for Utility-based Cooperative Cognitive radio Networks,” *MobiHoc ’09*, (New York, NY, USA), pp. 23–32, ACM, 2009.
 - [5] X. Zhou, S. Gandhi, S. Suri, and H. Zheng, “eBay in the Sky: Strategy-proof Wireless Spectrum Auctions,” *MobiCom ’08*, (New York, NY, USA), pp. 2–13, ACM, 2008.
 - [6] X. Zhou and H. Zheng, “TRUST: A General Framework for Truthful Double Spectrum Auctions,” in *INFOCOM 2009, IEEE*, pp. 999–1007, April 2009.
 - [7] J. Jia, Q. Zhang, Q. Zhang, and M. Liu, “Revenue Generation for Truthful Spectrum Auction in Dynamic Spectrum Access,” *MobiHoc ’09*, (New York, NY, USA), pp. 3–12, ACM, 2009.
 - [8] C.-C. Wu, C.-C. Chang, and I.-C. Lin, “New Sealed-Bid Electronic Auction with Fairness, Security and Efficiency,” *J. Comput. Sci. Technol.*, vol. 23, no. 2, pp. 253–264, 2008.
 - [9] K. Peng, C. Boyd, and E. Dawson, “Batch Verification of Validity of Bids in Homomorphic e-Auction,” *Comput. Commun.*, vol. 29, pp. 2798–2805, Sept. 2006.
 - [10] S. Gandhi, C. Buragohain, L. Cao, H. Zheng, and S. Suri, “A General Framework for Wireless Spectrum Auctions,” in *DySPAN 2007*, pp. 22–33, April 2007.
 - [11] K. Jain, J. Padhye, V. N. Padmanabhan, and L. Qiu, “Impact of Interference on Multi-hop Wireless Network Performance,” *MobiCom ’03*, (New York, NY, USA), pp. 66–80, ACM, 2003.
 - [12] R. Weber, “Auction Theory: By Vijay Krishna. Academic Press, 2002,” *Games and Economic Behavior*, vol. 45, no. 2, pp. 488–497, 2003.
 - [13] Y. Wu, B. Wang, K. Liu, and T. Clancy, “A multi-winner cognitive spectrum auction framework with collusion-resistant mechanisms,” in *DySPAN 2008*, pp. 1–9, Oct 2008.
 - [14] F. Wu and N. Vaidya, “A Strategy-Proof Radio Spectrum Auction Mechanism in Noncooperative Wireless Networks,” *Mobile Computing, IEEE Transactions on*, vol. 12, pp. 885–894, May 2013.
 - [15] R. McAfee, “A dominant strategy double auction,” *Journal of Economic Theory*, vol. 56, no. 2, pp. 434 – 450, 1992.
 - [16] D. Yang, X. Fang, and G. Xue, “Truthful Auction for Cooperative Communications,” *MobiHoc ’11*, (New York, NY, USA), pp. 9:1–9:10, ACM, 2011.
 - [17] X. Feng, Y. Chen, J. Zhang, Q. Zhang, and B. Li, “TAHES: A Truthful Double Auction Mechanism for Heterogeneous Spectrums,” *Wireless Communications, IEEE Transactions on*, vol. 11, pp. 4038–4047, November 2012.
 - [18] Y. Chen, J. Zhang, K. Wu, and Q. Zhang, “TAMES: A Truthful Auction Mechanism for heterogeneous spectrum allocation,” in *INFOCOM, 2013 Proceedings IEEE*, pp. 180–184, April 2013.
 - [19] Q. Huang, Y. Tao, and F. Wu, “SPRING: A Strategy-proof and Privacy preserving spectrum auction mechanism,” in *INFOCOM, 2013 Proceedings IEEE*, pp. 827–835, April 2013.
 - [20] W. Dong, S. Rallapalli, R. Jana, L. Qiu, K. Ramakrishnan, L. Razoumov, Y. Zhang, and T. W. Cho, “iDEAL: Incentivized dynamic cellular offloading via auctions,” in *INFOCOM, 2013 Proceedings IEEE*, pp. 755–763, April 2013.
 - [21] X. Zhuo, W. Gao, G. Cao, and Y. Dai, “Win-Coupon: An incentive framework for 3G traffic offloading,” in *Network Protocols (ICNP), 2011 19th IEEE International Conference on*, pp. 206–215, Oct 2011.
 - [22] M. Dong, G. Sun, X. Wang, and Q. Zhang, “Combinatorial auction with time-frequency flexibility in cognitive radio networks,” in *INFOCOM, 2012 Proceedings IEEE*, pp. 2282–2290, March 2012.
 - [23] F. Wu and N. Vaidya, “SMALL: A Strategy-proof Mechanism for radio spectrum allocation,” in *INFOCOM, 2011 Proceedings IEEE*, pp. 81–85, April 2011.
 - [24] M. Yokoo and K. Suzuki, “Secure Multi-agent Dynamic Programming Based on Homomorphic Encryption and Its Application to Combinatorial Auctions,” in *Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems: Part 1, AAMAS ’02*, (New York, NY, USA), pp. 112–119, ACM, 2002.
 - [25] K. Suzuki and M. Yokoo, “Secure Generalized Vickrey Auction Using Homomorphic Encryption,” in *Financial Cryptography* (R. N. Wright, ed.), vol. 2742 of *Lecture Notes in Computer Science*, pp. 239–249, Springer, 2003.
 - [26] M. Yokoo and K. Suzuki, “Secure Generalized Vickrey Auction without Third-party Servers,” in *Financial Cryptography* (A. Juels, ed.), vol. 3110 of *Lecture Notes in Computer Science*, pp. 132–146, Springer, 2004.
 - [27] 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*, vol. 29, no. 4, pp. 866–876, 2011.
 - [28] P. Paillier, “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes,” vol. 1592, pp. 223–238, 1999.
 - [29] P. Paillier and D. Pointcheval, “Efficient Public-Key Cryptosystems Provably Secure Against Active Adversaries,” in *Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security: Advances in Cryptology, ASIACRYPT ’99*, (London, UK, UK), pp. 165–179, Springer-Verlag, 1999.
 - [30] FCC (2003), “The development of secondary markets-Report and Order and further notice of proposed rule marketing,” Tech. rep., FCC 03-113.
 - [31] FCC (2010), “Unlicensed Operations in the TV Broadcast Bands, Second Memorandum Opinion and Order,” Tech. rep., FCC 10-174.
 - [32] J. Jose, A. Abdel-Hadi, P. Gupta, and S. Vishwanath, “On the impact of mobility on multicast capacity of wireless networks,” in *INFOCOM, 2010 Proceedings IEEE*, pp. 1–5, March 2010.
 - [33] H. Shajiaiah, A. Khawar, A. Abdel-Hadi, and C. Clancy, “Resource allocation with carrier aggregation in LTE Advanced cellular system sharing spectrum with S-band radar,” in *DYSPAN*, pp. 34–37, April 2014.
 - [34] T. Groves, “Incentives in teams,” *Econometrica*, vol. 41, 1973.
 - [35] W. Vickrey, “Counterspeculation, Auctions and Competitive Sealed Tenders,” *Journal of Finance*, pp. 8–37, 1961.
 - [36] N. Nisan, T. Roughgarden, É. Tardos, and V. V. Vazirani, *Algorithmic Game Theory*. New York, NY, USA: Cambridge University Press, 2007.
 - [37] A. Abdel-Hadi and C. Clancy, “A Utility Proportional Fairness Approach for Resource Allocation in 4G-LTE,” in *ICNC Workshop CNC*, 2014.
 - [38] A. Abdel-Hadi and C. Clancy, “A Robust Optimal Rate Allocation Algorithm and Pricing Policy for Hybrid Traffic in 4G-LTE,” in *PIMRC*, 2013.
 - [39] H. Shajiaiah, A. Abdel-Hadi, and C. Clancy, “Utility proportional fairness resource allocation with carrier aggregation in 4G-lte,” *Milcom*, 2013.