Poster: Towards Secure Spectrum Auction: Both Bids and Bidder Locations Matter

Zhili Chen[1], Lin Chen[2], Liusheng Huang[3], and Hong Zhong[1]
[1]School of Computer Science and Technology, Anhui University, 230601 Hefei, P. R. China
[2]Lab. Recherche Informatique (LRI-CNRS UMR 8623), Univ. Paris-Sud, 91405 Orsay, France
[3]School of Comput. Sci. and Tech., Univ. of Sci. and Tech. of China, 230027 Hefei, P. R. China
{zlchen3, lshuang}@ustc.edu.cn, chen@lri.fr, zhongh@mail.ustc.edu.cn

ABSTRACT

Truthful spectrum auctions make bidders reveal their true valuations for spectrum to maximize their utilities. However, disclosure of one's true value causes numerous security vulnerabilities. Moreover, as a distinguished property of spectrum auction compared to classical auctions, spectrum reutilisation requires that the bidder locations be disclosed to the auctioneer to run the auction. We investigate the impact of disclosing bidder locations and demonstrate that such disclosure can be exploited by a malicious auctioneer to gain extra profit and significantly degrade bidders' utility.

We then design a provably secure spectrum auction framework that does not leak any information on either bids or bidder locations other than the auction outcome. Technically, we leverage tools in garbled circuits and secret sharing, and design data-oblivious algorithms where the execution path does not depend on the input. We further implement our solution and theoretically and experimentally show that it incurs only limited computation and communication overhead.

CCS Concepts

•**Security and privacy** → **Security protocols;**

Keywords

Spectrum auction; security; privacy

1. INTRODUCTION

The deployment of millions of wireless mobile devices makes radio spectrum a precious resource. To alleviate spectrum scarcity, truthful spectrum auction is used as an efficient way to redistribute idle spectrum channels from primary to secondary spectrum users. Despite their economic robustness, truthful spectrum auctions are particularly vulnerable to various attacks because revealing one's true valuation naturally opens the door for many security vulnerabilities. For this reason, previous studies on secure spectrum auctions mainly focus on the protection of bid privacy of bidders.

MobiHoc'16 July 04-08, 2016, Paderborn, Germany

ACM ISBN 978-1-4503-4184-4/16/07.

DOI: http://dx.doi.org/10.1145/2942358.2947400

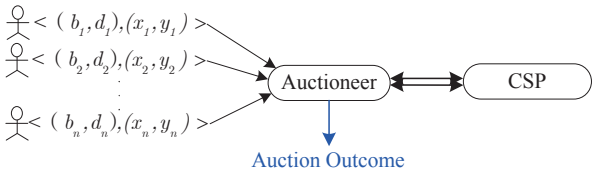


Figure 1: Secure spectrum auction architecture.

In this paper, for the first time to our knowledge, we show that disclosing bidder locations can be exploited by a malicious auctioneer to gain extra profit, tampering economic properties of the auction such as truthfulness and social efficiency. We then design a *cryptographical* secure spectrum auction protocol protecting *both* bid and location privacy of bidders, i.e. no participating party learns anything about the bids and bidder locations beyond the auction outcome. Experimental results show the efficiency of the protocol in both computation and communication overhead.

2. PROBLEM FORMULATION

We consider a dynamic spectrum auction setting exactly as studied in [1]. We aim at designing a secure auction protocol that do not leak any information to any entity other than the auction outcome. By auction outcome we mean the winner IDs, clearing prices, and channels allocated to the winners, which should be published after the auction. By entities we refer to auctioneer, crypto-service provider (CSP), bidders and other users not participating the auction.

Architecturally, our secure spectrum auction mechanism is depicted in Fig. 1: bidders want to keep their bids and locations private during the auction. They send secretly shared and encrypted bids and locations to an Auctioneer who runs the secure auction, with the intervention of a *crypto-service provider* (CSP), whose role is to enable secure computations in the auction. Specifically, the following security requirements should be satisfied in the auction: (1) No bidder can learn anything about the bids or the locations of other bidders, except the auction outcome of the current run; (2) Neither the auctioneer nor the CSP can learn anything about the bid or the location of any bidder, except the auction outcome of the current run; (3) Any user not participating the auction cannot learn anything about the bid or the location of any bidder, except the auction outcome of the current run.

In our work, we assume that the auctioneer and the CSP do not collude with each other. We focus on the *semi-honest* (or *honest but curious*) threat model where the auctioneer and the CSP follow the protocols we develop but may analyze protocol transcripts to infer additional information.

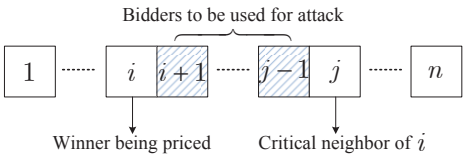


Figure 2: Bidders used for clearing price attacks in a bidder list sorted in descending order of b_i (i.e., $b_1 \geq b_2 \geq \cdots \geq b_n$). If the pseudo-bidder used for attack is located at $i+1$, bidder i suffers maximal utility lost; If it is located at $j-1$, then i suffers minimal utility lost.

3. DESIGN CHALLENGE: PROTECTING BIDS ONLY IS NOT ENOUGH

In this section, we illustrate the challenges in securing VERITAS. We first show that protecting only bid privacy in VERITAS is insecure and the vulnerabilities can be exploited by the auctioneer to get extra profit. We then conduct a quantitative experiment to investigate how much extra profit the auctioneer can get.

Clearing Price Attack. A natural idea to secure VERITAS is to protect the privacy of per-channel bids b_i (or bids (b_i, d_i)). In the following, we show that protecting only per-channel bid privacy is not enough (the case of protecting only (b_i, d_i) can be similarly analyzed, with appropriate inference of d_i values.).

If only per-channel bids are protected in VERITAS, the misbehaved auctioneer can conduct the following attack to increase its profit:

- Learning the bidder locations, the auctioneer can compute the conflict graph, identify each bidder by its location and obtain its per-channel bid ranking from the auction execution.
- With the knowledge of conflict graph, per-channel bid ranking and the auction outcome, the auctioneer can establish the correspondence between certain winners and their critical neighbors using the same method as used in VERITAS (Note that running VERITAS does not need the exact per-channel bid values).
- The auctioneer then raises the clearing price of each winner to the bid of a bidder between the winner and its critical neighbor in the bidder list sorted in descending order of b_i, as shown in Fig. 2.

Quantitative Experimentation. A practical way to launch the clearing price attack is to let some pseudo-bidders participate the auction and use them to increase the clearing price of the real bidders (cf. Fig. 2). In the following, we perform a quantitative experiment to evaluate the impact of this attack. We simulate a network where 100 bidders are randomly distributed in a $1000m \times 1000m$ square with a conflict distance $100m$. We repeat the experiment with 100 random network topologies to study the extra profit obtained by the auctioneer. We find that the maximal increase of the auctioneer's revenue is 57%, the minimal is 2%, the average is 29%. We further examine the max/min/average utility loss of each attacked winner after the clearing price attack, and find that in the worst case, the attacked winners lose nearly all their utility, with an average loss of 50%.

4. SECURE SPECTRUM AUCTION DESIGN

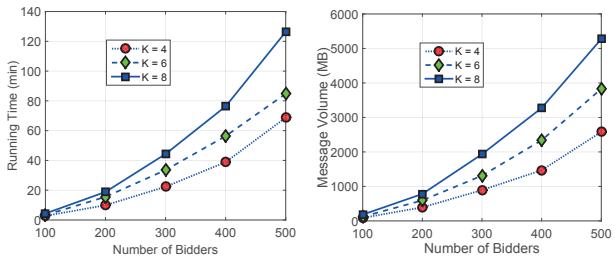
Motivated by the observation in Sec. 3, we design a secure spectrum auction protocol preserving both bid and bidder location privacy. The framework of our secure spectrum auction framework is illustrated in Fig. 1.

To allow the auctioneer to execute the auction while neither the auctioneer nor the CSP can learn anything about bids and bidder locations except what can be revealed from the auction outcome, we apply a hybrid approach in our design by combining garbled circuits with secret sharing. Specifically, our design rationale is as follows.

- First, each bidder splits its ID, bid and location using XOR secret sharing into two shares. It then encrypts one share with the auctioneer's public key, and the other share with the CSP's public key, and submits both encrypted shares to the auctioneer anonymously.
- Next, the auctioneer collects its encrypted shares of all the bidders' IDs, bids and locations, and forwards the other encrypted shares to the CSP. Both the auctioneer and CSP then decrypt and get their respective shares.
- Using the boolean circuit computing the auction, the CSP generates a garbled circuit with secretly shared input and sends it to the auctioneer.
- The auctioneer obtains the garbled values corresponding to all input shares to the auction and then executes the garbled circuit to get the auction outcome in the clear.

5. EXPERIMENTAL RESULTS

In this section, we carry out experiments to evaluate the performance of our secure spectrum auction protocol. We implement our protocol (denoted by SEC) on top of FastGC [2]. We evaluate the efficiency of SEC in term of running time and communication overhead. We fix the number of channels auctioned ($K = 4$, $K = 6$ and $K = 8$), and vary the number of bidders (N) from 100 to 500. From Fig. 3, we see that all running times are roughly within 2 hours, and all communication overheads are within 6 GB, which is acceptable for practical applications.



(a) Running Time (b) Communication Overhead

Figure 3: Performance Evaluation of SEC in term of Running Time and and Communication Overhead.

Acknowledgment

The work is supported by the Natural Science Foundation of China under Grant Nos. 61572031, 61572001 & 61202407, and the Natural Science Foundation of Anhui Province under Grant No. 201508085QF132.

6. REFERENCES

[1] X. Zhou, S. Gandhi, S. Suri, and H. Zheng. ebay in the sky: Strategyproof wireless spectrum auctions. In *Proc. of MobiCom*, pages 2–13, 2008.

[2] Y. Huang, D. Evans, J. Katz, and L. Malka. Faster secure two-party computation using garbled circuits. In *Proc. USENIX Security*, 2011.