International Journal of Current Engineering and Technology
©2021 INPRESSCO®, All Rights Reserved

E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Privacy-Preserving and Truthful Online Spectrum Allocation for Bidding

Shadanan Dani Prof. Vandana Navale.

Department of Computer Engineering Dhole Patil College of Engineering,

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

The notoriety of the Internet, the reconciliation administrations have slowly changed individuals every day life, for example, web based business exercises on exchanges, transportation, etc. The E-sell off, one of the famous online business exercises, enables bidders to legitimately offer the items over the Internet. With respect to fixed offer, the additional exchange cost is required for the middle people in light of the fact that the outsider is the significant job between the purchasers and the merchants help to exchange both during the bartering. Bidders frequently feel tested when searching for the best offering techniques to exceed expectations in the focused condition of numerous and concurrent online sales for same or comparable things. Bidders face muddled issues for choosing which closeout to take part in, regardless of whether to offer early or late, and the amount to offer. In this framework, we present the plan of offering techniques which intend to conjecture the offer sums for purchasers at a specific minute in time dependent on their offering conduct and their valuation of an unloaded thing. The operator builds up an exhaustive philosophy for definite value estimation which structures offering techniques to address purchasers' distinctive offering practices utilizing two approaches: Mamdani strategy with Regression Analysis and Negotiation Decision Functions. The exploratory outcomes demonstrate that the operators who pursue dissuading relapse approach beat other existing specialists in many settings as far as their prosperity rate and anticipated utility. Like SCO device give most noteworthy need to utilizing rating for government contractual worker.

Keywords: *E-auction, Public Bid, Sealed Bid, Smart Contract, Government Contract.*

Introduction

To achieve truthfulness and improve spectrum utilization, auction mechanisms tend to stimulate bidders to bid their true valuations of the spectrum, and to disclose their geo-location information for spectrum reuse. In an online spectrum auction, bidders are further required to specify their request of timeslots to determine spectrum occupancy. However, one's true spectrum valuation, geo-location and request of time-slots are sensitive and private information that should be shielded from the non-trustworthy auctioneer and other rival bidders. For example, bidders' true valuations of the spectrum may be commercial secrets closely related to bidder's economic situation and the profits of winning the spectrum. By leveraging historical bidding values, the auctioneer may rig the auction, and rival bidders may manipulate their bids to increase their own utility, violating the truthfulness of the original auction mechanism.

A Privacy-pReserving and truthful Online double auction mechanism for Spectrum allocaTion, referred to as PROST. PROST provides a comprehensive protection for bid values, bid ranking order, geo-location and request of time-slots of bidders as well as reserving the truthfulness of the auction mechanism. To provide privacy guarantees for users' sensitive information, we utilize the Paillier cryptosystem to encrypt sensitive data locally before outsourcing. With a clever use of garbled circuits and oblivious transfer protocol, we develop a series of building blocks that support various arithmetics over encrypted real numbers, including addition, subtraction, multiplication, comparison and selection. Based on these carefully-designed building blocks, we have established secure protocols for every step of the auction, making sure that nothing will be leaked but the final auction results including winners, clearing prices and allocated time-slots.

The rise of programming operator innovation has made an imaginative system for creating on the web closeout components. As a result of their exceptional versatile abilities and trainability, programming operators have turned into a basic segment of web based exchanging frameworks for purchasing and selling merchandise. Programming operators can perform different errands like examining the present market to foresee future patterns, choosing offer sums at a specific minute in time, assessing diverse sale parameters and checking closeout progress, just as some more. These arranging specialists outflank their human partners in light of the efficient methodology they take to overseeing complex basic leadership circumstances adequately. This makes more open doors for master bidders and merchants to boost fulfillment and benefit. 1) We are the first to propose an exhaustive security safeguarding system for online twofold auctions, ensuring the protection of offer qualities, offer positioning request, geo-area and solicitation of schedule vacancies. Plus, we structure a novel security safeguarding purchaser gathering convention for spectrum reuse, which extraordinarily improves the assignment proficiency without uncovering any private data.

2) We build up a progression of building squares to help different mathematics over encoded genuine numbers, including expansion, subtraction, increase, correlation and determination, which can be promptly applied to security safeguarding of other spectrum auctions. Besides, we achieve a request for extent decrease in both calculation what's more, correspondence costs by utilizing information pressing and simultaneous figuring strategies.

3) We present a careful hypothetical investigation of PROST regarding both security and proficiency. To further show its proficiency and reasonableness, we direct exploratory assessments and contrast and non-private saving online auction component. The test results affirm that PROST accomplishes pleasant spectrum allotment effectiveness with light calculation and correspondence costs, making PROST a down to earth online auction model for dynamic spectrum portion.

Literature Survey

Online auctions became a pervasive transaction mechanism for e-commerce. As the largest online market within the worldwide, eBay is a good study that permits the study of online auctions using data connecting real societies and transactions. They present an in depth examination and analysis of many online auction assets including: consumer surplus, sniping, bidding strategy and their cross affairs. Our goal is to gauge the theoretical foundations of online auctions and find out patterns and behaviors hidden thanks to the shortage of real and extensive transaction data. we uncover a critical connection among sniping and high surplus ratios, which means the uncertainty of true value during a competitive environment. The key issue is the wrong assumption that bidder's valuations are independent from each other, which leads to inefficient auctions. In order to deal with the inefficiencies of current online formats we introduce a declining price auction model customized for online transactions. Conceptually, this model ought to deal with the complexities of competition in an online environment while maximizing social welfare. [1]

In recent years, the proliferation of the planet Wide Web has cause a rise within the number of public auctions on the web . One of the characteristics of online auctions is that a successful implementation requires a high volume of buyers and sellers at its website. Consequently, auction sites which have a high volume of traffic have a plus over those during which the quantity is restricted . This leads to even greater polarization of buyers and sellers towards a specific site. This is often mentioned because the network effect during a sort of web and telecommunication applications involving interactions among an outsized number of entities. Though this consequence has qualitatively been known to rise the value of the total web, its effect has not ever been calculated thoroughly. In this paper, we construct a Markov Model to analyse the network effect within the case of web auctions. We show that the network effect is extremely powerful for the case of web auctions and may end in a situation during which one auction can quickly overwhelm its competing sites. This leads to a situation during which the natural stable equilibrium is that of one online auction seller for a given product and geographical locality. While one player structure is unlikely due to some approximation assumptions within the model, the trend seems to point out the likely existence of single dominant player within the web auction space. [2]

Academic interest within the popularity and success of online auctions has been increasing. Although much research has been administered in an effort to know online auctions, little effort has been made to integrate the findings of previous research and evaluate the status of the research in this area. The unbiased of this exercise is to discover the intellectual development of consumer conduct in online auction research through a meta-analysis of the issued auction research. The findings of this study are supported an analysis of 83 articles on this subject published mainly in information systems (IS) journals between 1998 and 2007. The outcomes specify that the buyer behavior research on online auctions are often categorized into three major areas facilitating factors, consumer behavior and auction consequences. Based on this instructions for upcoming investigation on e-auction consumer behavior are discussed, including potential new constructs, unexplored relationships and new definitions and measurements, and suggestions for methodological improvements are made. [3]

This study seeks to the solution the question of how a private would trade off between listing fee (i.e., cost of listing an auction item) and transaction probability (i.e., the chance that a product will be sold). Applying the exchange off dynamic worldview into the bartering setting, we look at a vender's decision of online closeout outlet and consequent beginning value techniques when confronting the exchange off between exchange likelihood and posting expense. Results from a gathering of research facility tests propose that a merchant would acquire a significant expense in return for a superior exchange prospect. Besides, if the normal exchange likelihood is high, a dealer is bound to line a high beginning cost in spite of acquiring a high posting charge. The suggestions for hypothesis and practice are examined. [4]

Online closeout is turning out to be increasingly more well known in electronic business (EC). It has become the standard exchanging techniques customer to buyer (C2C), like eBay. The consistent coordinated effort field and normal idea of trade might be shaped in the participation of the Multi-Agent framework (MAS), and afterward the operators will have such a lot of basic information so as to finish the errands. The individual from MAS has both collaboration and personal circumstance. In view of the examination of the collaboration and rivalry of the participators inside the online closeout, the idea of additional time and history data is presented. As existing fragmented data, the proficiency of the closeout is low without think about the history data. This paper recommends a MAS stream casing and arrangement calculations that cause the bidders of the closeout to take an interest inside the exchange sincerely and effectively. Both the effectiveness and straightforwardness among the participators have been improved. [5]

Proposed Methodology

As shown in Fig. 1, our model consists of three parties: a set of bidders including sellers and buyers, an auctioneer and an auction agent. The auction agent, who cooperates with the auctioneer to facilitate the running of privacy-preserving auction mechanism, is introduced following existing literature [11], [12], [14], [15]. The agent and the auctioneer are both semihonest, meaning that they will faithfully follow the protocol, but attempt to learn information besides the output [14]. Before the auction starts, the agent generates the key pair of Paillier cryptosystem [26]. Then, the auctioneer cooperates with the agent to determine the winners, clearing prices and allocated time-slots based on encrypted data received from bidders, and finally returns the auction results to bidders. We consider an online double auction for homogenous spectrum. Suppose there is a set S = {s1, s2, ..., sM} of M sellers, each of whom owns one channel to sublease during the time interval [0, T]. We assume that the channels are identical and the time is slotted (discrete). We use si to represent both the seller and her channel without confusion. Let v s i denote

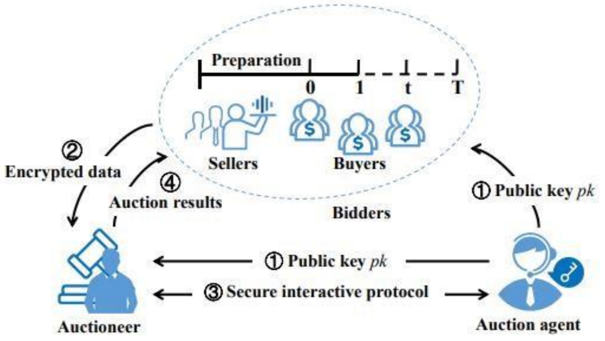


Fig 1. System Architecture

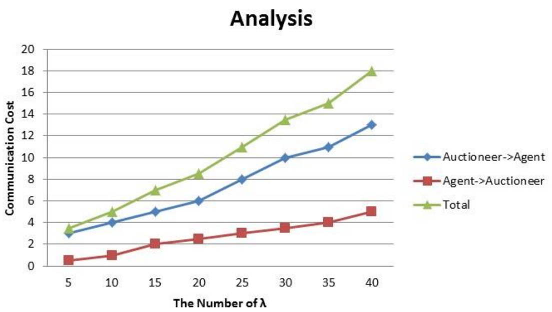
The fixed asking price of si for subleasing the channel for one time slot. Buyers arrive in an online fashion. Suppose there is a set B = {b1, b2, ..., bK} of K buyers coming at time t (0 ≤ t < T), each requesting for one channel. The request information of buyer bj is (v b j , tb j , xj , yj , rj), in which v b j is the bid for one channel per time slot, t b j is the request of time-slots, (xj , yj) is the location, and rj is the conflict radius. Conflict free buyers can reuse the same channel simultaneously.

Algorithm

A. Parallel Convert of data which is send For that generate two k-bit random number.
Obtain garbled value. Compute and send.
B. Select Value to encrypt and decrypt at the other end.
C. Create grouping of buyers for bidding.
D. Find Maximum Independent Set(MIS) from grouping which shows the maximum bidders for that bidding.
E. Take Auction with privacy to the auctioneer.
F. Provide Winning buyer to all bidders for that bidding.

Results

The communication cost (for online execution) increases quadratically with λ for reasons similar to those for the computation costs. Besides, it is shown that the auctioneer→agent communication cost is much larger than that of agent→auctioneer communication cost.



Conclusions

We have presented PROST, the first privacy preserving and truthful online double auction mechanism for spectrum allocation. PROST provides a comprehensive privacy protection for bidders, including bid values, bid ranking order, geo-location and time dynamics. PROST is constructed based on our carefully-designed security building blocks, which are well applicable in other spectrum auctions. We have conducted rigorous security analysis to prove that PROST is secure against semi-honest adversaries. The experimental results have demonstrated that PROST achieves strong privacy protection and nice spectrum allocation efficiency with light computation and communication costs.

Acknowledgment

I would like to thank my project guide ||Prof. Vandana Navale|| who always being with presence and constant, constructive criticism to made this paper. I would also like to thank all the staff of Computer Department for their valuable guidance, suggestions and support through the paper work, who has given co-operation for the project with personal attention. At the last I thankful to my friends, colleagues for the inspirational help provided to me through a paper work.

References

[1]. Q. Wang, M. Du, X. Chen, Y. Chen, P. Zhou, X. Chen, and X. Huang, —Privacy-preserving collaborative model learning: The case of word vector training,|| IEEE Transactions on Knowledge and Data Engineering, vol. PP, pp. 1–1, DOI: 10.1109/TKDE.2018.2 819 673, 2018.

[2]. Y. Chen, X. Yin, and J. Zhang, —A reverse auction framework for hybrid access in femtocell network,|| Journal of Computer Science and Technology, vol. 32, no. 6, pp. 1250–1264, 2017.

[3]. Q. Wang, M. He, M. Du, S. S. M. Chow, R. W. F. Lai, and Q. Zou, —Searchable encryption over feature-rich data,|| IEEE Transactions on Dependable and Secure Computing, vol. 15, pp. 496–510, 2016.

[4]. S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, —Securing sift: Privacy-preserving outsourcing computation of feature extractions over encrypted image data,|| IEEE Transactions on Image Processing, vol. 25, no. 7, pp. 3411–3425, 2016.

[5]. R. Zhu and K. G. Shin, —Differentially private and strategyproof spectrum auction with approximate revenue maximization,|| in Proc. of INFOCOM'15. IEEE, 2015, pp. 918–926.

[6]. F. Wu, Q. Huang, Y. Tao, and G. Chen, —Towards privacy preservation in strategy-proof spectrum auction mechanisms for noncooperative wireless networks,|| IEEE/ACM Transactions on Networking, vol. 23, no. 4, pp. 1271–1285, 2015.

[7]. Q. Huang, Y. Gui, F. Wu, and G. Chen, —A general privacypreserving auction mechanism for secondary spectrum markets,|| IEEE/ACM Transactions on Networking, vol. 24, no. 3, pp. 1881–1893, 2015.

[8]. M. Hoefer, T. Kesselheim, and B. Vocking, —Approximation algorithms ¨ for secondary spectrum auctions,|| ACM Transactions on Internet Technology, vol. 14, no. 2-3, p. 16, 2014.

[9]. Z. Chen, L. Huang, L. Li, W. Yang, H. Miao, M. Tian, and F. Wang, —PSTRUST: Provably secure solution for truthful double spectrum auctions,|| in Proc. of INFOCOM'14. IEEE, 2014, pp. 1249–1257.

[10]. Y. Chen, P. Lin, and Q. Zhang, —LOTUS: Location-aware online truthful double auction for dynamic spectrum access,|| in Proc. of DYSPAN'14. IEEE, pp. 510–518.

[11]. H. Huang, X. Li, Y. Sun, and H. Xu, —PPS: Privacypreserving strategyproof social-efficient spectrum auction mechanisms,|| IEEE/ACM Transactions on Networking, vol. 26, no. 5, pp. 1393–1404, 2013.

[12]. X. Feng, Y. Chen, J. Zhang, Q. Zhang, and B. Li, —TAHES: Truthful double auction for heterogeneous spectrums,|| IEEE Transactions on Wireless Communications, no. 11, pp. 3076–3080, 2012.

[13]. P. Xu, X.-Y. Li, and S. Tang, —Efficient and strategyproof spectrum allocations in multichannel wireless networks,|| IEEE Transactions on Computers, vol. 60, no. 4, pp. 580–

[14]. 593, 2011.

[15]. P. Xu, X. Xu, S. Tang, and X.-Y. Li, —Truthful online spectrum allocation and auction in multi-channel wireless networks,|| in Proc. of INFOCOM'11. IEEE, 2011, pp. 26–

[16]. 30.

[17]. P. Xu and X.-Y. Li, —TOFU: Semi-truthful online frequency allocation mechanism for wireless networks,|| IEEE/ACM

[18]. Transactions on Networking, vol. 19, no. 2, pp. 433–446, 2011.

[19]. 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.

[20]. S. Wang, P. Xu, X. Xu, S. Tang, X. Li, and X. Liu, —TODA: Truthful online double auction for spectrum allocation in wireless networks,|| in Proc. of DySPAN'10. IEEE, 2010, pp. 1–10.

[21]. P. Xu, S. Wang, and X.-Y. Li, —SALSA: Strategyproof online spectrum admissions for wireless networks,|| IEEE

[22]. Transactions on Computers, vol. 59, no. 12, pp. 1691–1702, 2010.

[23]. X. Zhou and H. Zheng, —TRUST: A general framework for truthful double spectrum auctions,|| in Proc. of INFOCOM'09. IEEE, 2009, pp. 999–1007.

[24]. X. Zhou, S. Gandhi, S. Suri, and H. Zheng, —eBay in the sky: Strategyproof wireless spectrum auctions,|| in Proc. of MOBICOM'08. ACM, 2008, pp. 2–13.