2011 Second International Conference on Emerging Applications of Information Technology

A New Secure Protocol for Multi-Attribute Multi-round e-Reverse Auction using Online Trusted Third Party

T. R. Srinath, Samrat Kella
Dept. of Computer Science and Engineering
National Institute of Technology Karnataka
Surathkal 575025, India
Email:(talari.srinath,samrat.kella)@gmail.com

Mamata Jenamani
Dept. of Industrial Engineering and Management
Indian Institute of Technology
Kharagpur 721302, India
Email: mamatajenamani@yahoo.co.in

***Abstract*—We develop a secure protocol for multi-attribute multi-round reverse auction. The scheme comprises of three interactive parties: the Online Trusted Third Party (TTP), the Auctioneer and the Bidder. Online TTP is the one who gets certified from Certification Authority (CA), Auctioneer is the buyer and bidders are the sellers. The TTP confirms and authenticates the identities of bidders and the auctioneer; the auctioneer issues the bidding keys to bidders and schedules the auction rounds. Encryption and Decryption of bids is done by combined key made from public and secret shares of TTP and auctioneer using ElGamal cryptosystem. TTP Combines the keys and gives to auctioneer at appropriate time. TTP generates pseudonym for bidder which is used as unique identifier and makes the bidder anonymous to auctioneer till last round. The scheme developed here can effectively reduce the computational load on the auctioneer and bidders. It provides the following security features anonymity, non-repudiation, bid privacy, easy revocation, no framing, data integrity and single registration. The proposed scheme can assure a secure bidding environment for the sellers.**

***Index Terms*—Anonymity; Certification Authority (CA); Non-Repudiation; Bid privacy**

I. Introduction

Electronic reverse auctions have been adopted by many companies for organizational procurement. It is a market mechanism involving a single buyer and multiple sellers to induce competition for price reduction. Besides purchase cost reduction the other benefits that e-reverse auction brings in includes cycle time reduction, decrease in administrative cost and exploration of unknown supplier base. Reverse auctions introduce market competition and put a downward pressure on price [1] . Such auctions have well defined structure and rules which make the procurement process transparent and, at least in theory, and discover a competitive market price.

The inability of the price-only auctions to capture the potential of the suppliers led to the use of multi-attribute reverse auctions. These auctions include multiple non-price attributes such as product quality, lead time, and production capacity etc. besides price. It has been observed through experimental studies that increasing the number of attributes better specifies the potential of a supplier and thus generate more utility for the buyer. In single round case all the bidders submit the multi attribute bid only once, whereas in multi-round case they get a feedback on the winning bid and get a chance to revise their bid a number of times. In case of a price only auction the winner is the bidder with lowest price whereas in case of multi attribute auction a buyer has to design a scoring function combining all the attributes and the winner is the bidder with highest score. We give a brief overview of the mechanism latter in the paper. The more details about multi attribute reverse auction are explained in [2][3].

In a reverse auction the sellers submit the bids online and the buyer determines the winner by comparing the bids. The security concerns here are that a bidder would like to ensure that her personal and bid details are not revealed to their competitors before the specified time even when somebody at the buyer's end collude with her competitor. Though many efforts have been made in the past to solve this problem for price only and single round auctions [4][5], not many have been working in the context of multi-attribute and multi round auctions.

We proposed a scheme to conduct secure multi-attribute and multi-round auction with the help of an online Trusted Third Party (TTP). The security concerns of the bidders in such auction are twofold: Firstly, in each round the bid details must not be revealed and secondly, the winning score must be revealed without revealing the identity. The buyers concern is that even if she evaluates the anonymous bids, the bidders must not repudiate about the ownership of their own bid. More formally, the security concern must address the issues of confidentiality, data integrity and non-repudiation along with anonymity. We propose to use ElGamal cryptosystem to address these security concerns

Koutarou and Makoto [6] address the security issues in Multi-attribute Procurement Auction. A secure protocol for the multi-item auction is proposed in [7]. The paper uses verifiable technique of shared key chain to find the winners without revealing the losing bids and unnecessary information. Some authors introduce the concept of trusted third party to ease the security process. For example, [8] and [5] introduce a separate

978-0-7695-4329-1/11 $26.00 © 2011 IEEE
DOI 10.1109/EAIT.2011.83

party called registration manager to store bidder's details and assumption is that there is no collusion with the auctioneer. This leads us to introduce online TTP to make our protocol more secure and efficient with less computation.

Rest of the paper is organized as follows. Section II describes the winner determination in multi-attribute multi-round Reverse Auction. We describe security requirements in Section III. Section IV describes the cryptographic algorithms used in our scheme. We describes the phases involved in this scheme and steps to execute those phases securely in Section V. We discussed security analysis in Section VI. Finally we present our conclusions in Section VII.

II. Winner Determination in Multi-attribute Multi-Round Reverse Auction

Winner determination is the process of selecting the right bidder to award the business. A buyer in multi-attribute reverse auction tries to minimize the price while maximizing the other quality related attributes during the winner determination. In other words she tries to maximize her utility defined through a scoring function [9], [10] . A scoring function combines the attributes to determine a score for each multi-attribute bid. A typical scoring function takes the following form:

$$S = \sum_{r=1}^{K} w_r \cdot f_r(x_r) - P$$

Where, K is the number of non-price attributes considered by the buyer, x_r is the value of the r^{th} attribute submitted by the supplier, w_r is the weight indicating the importance given to the attribute, $f_r(\cdot)$ is the valuation function associated with the attribute, and P is the bid price. The summation term inside S is also called the aggregate value function. The buyer maximizes the scoring function to selecting the supplier.

III. Security Requirements in Multi-round Reverse Auction

Security Requirements for multi-round reverse auction are as follows:

A. *Anonymity* :
No chance of leaking lost bidders details in auction. No one shall be able to identify the bidder during the auction.

B. *Bid privacy* :
No auction bid is revealed except winning bid.

C. *Non-Repudiation* :
No bidders can deny their bids submission.

D. *Integrity* :
Each bidder needs to register before bidding, and each bid is signed by an authenticated bidder. In the transmission phase, the tender is not modified.

E. *No framing* :
The identities of all bidders remain independent. No one can falsely claim to be any other bidder who participated in the auction.

F. *One-time Registration* :
The bidder only needs to register once and then she can participate in all auctions.

G. *Easy revocation* :
TTP can easily revoke someone's right to bid. Once the information is removed from the data base, the bidder loses the right to participate in the auction.

IV. Cryptographic algorithms used in the proposed scheme

Our scheme achieves security features by using cryptographic algorithms: ElGamal encryption and decryption algorithm, signature generation and verification algorithm [11], shared keychain algorithm [7] and pseudonym generation algorithm [12]. All the algorithms are explained as follows:

A. *ElGamal cryptosystem* :

ElGamal cryptosystem is a public key cryptosystem which is based on the difficulty of a problem called the "Discrete Logarithm Problem (DLP)". In order to achieve the strong security in our scheme we have used the ElGamal cryptosystem for encryption, decryption and signature generation and verification [11].

B. *Shared key chain technique based on ElGamal cryptosystem* :

The technique called shared key chain based on DLP [7] extended to ElGamal cryptosystem; is used in our scheme in order to achieve the bid privacy in the auction. ElGamal shared key chain is explained as follows:
Assume that x_1 and x_2 are the two private keys in ElGamal cryptosystem and their corresponding public keys are y_1 and y_2. By using two pairs $(y_1,\ x_1)$ (y_2, x_2), a new key pair (y_3, x_3) can be generate for the same cryptosystem as in Eqn. 1.

$$y_3 = y_1 * y_2 \tag{1}$$

The corresponding private key for y_3 can be determined only by adding x_1 and x_2 as in Eqn. 2.

$$x_3 = x_1 + x_2 \tag{2}$$

Similarly for each round TTP will generate encryption and decryption keys by using auctioneer's and his public and private key shares.

C. *Pseudonym generation algorithm* :

Pseudonyms are identifiers of subjects. The subject that may be identified by the pseudonym is the holder of the pseudonym. From the technical point of view, a pseudonym is a bit string which is unique as identifier and suitable to be used to authenticate the holder and his data.
In order to generate unique pseudonym, our scheme uses the algorithm proposed by Peter and Martin [12]. In the following algorithm (Table I) UID is unique identifier, Data is bidder's data. (e, n) and (d, n) are public and private keys of RSA. $E_e(m)$ represents the encryption of message m with the public key (e, n) and PAD represents padding bits, PseudoID represents pseudonym.

TABLE I
ALGORITHM TO GENERATE PSEUDONYM

```
Input: UID, Data
Output: PseudoID
1. Generate two random primes $p,\ q\ \epsilon_R$ IP.
2. Generate a random public key $e$ with
    $((p-1)(q-1), e) = 1$
3. Compute the private key $d = e^{-1}$ MOD $(p-1)(q-1)$.
4. Generate the pseudonym
    $P = E_e$(UID||Data||PAD)||e||n)

5. Return PseudoID.
```

TABLE II
PROPOSED SYSTEM PARAMETERS

$CERT_t$	Certificate of TTP
PK_t, SK_t	Public and secret keys of TTP
ElGamal public parameters	q is a prime (where $q \geq$ 1024 bits) $p = 2^k q + 1$ is a prime (where q $\geq$ 1024 bits, k is positive integer constant) g: generator of GF(p) (where g $\geq$ 1024 bits)
y_i, x_i	Public and Secret shares of TTP which are used in encrypting and decrypting bid details of bidder.
PK_a, SK_a	Public and Secret shares of Auctioneer which are used in encrypting and decrypting bid details of bidder.
PseudoID	Pseudonym generated for the bidder.
Y_i, X_i	Encryption key for round i: $Y_i = y_i * PK_a$ Decryption key for round i: $X_i = x_i * SK_a$
E(bid ,Y_i)	ElGamal Encryption of bid details using Y_i
H()	Collision Resistant hash function
Sig()	ElGamal based signature

V. THE PROPOSED SYSTEM

The proposed scheme consists of four phases: Initialization phase, Bidding phase, Opening phase and Winner determination phase. Three participants in the scheme are: the Online Trusted Third Party (TTP), the Auctioneer (A) and the Bidder (B). The system parameters explained in Table II.

Phases and steps in it are as follows:

A. *Initialization phase:*

Step 1: Certification from CA

TTP gets right to manage and provide trust to auctioneers and bidders, only when he is certified from CA.

Step 2: Registration

In this phase registration of auctioneer and bidders are done by TTP after examining their submission details.

Step 3: Key Generation

Based on ElGamal public parameters auctioneer generates his shared key pair and TTP generates his own shared key pairs for multi-round. TTP generates key pair for bidder to generate signature on their bids. All the three participants contain public keys shares of others.

Step 4: Bidder Authentication in Auctioneer's site

Auctioneer queries the TTP and get minimum details of bidder for allowing him to bid based on those details.

Step 5: Encryption Key for bidding in multi-rounds

TTP combines his and auctioneer's public key shares using shared keychain algorithm to get the encryption key for each round. TTP sends this key to auctioneer.

B. *Bidding phase*

Step 1: Bidder logs on to Auctioneer's site based on the details with they already registered with TTP. Auctioneer sends the encryption key for corresponding round that he gets from TTP to bidder for encrypting the bid.

Step 2: Bidder bids and signs it only in particular time period mentioned by Auctioneer.

C. *Opening phase*

Step 1: Signature Validation

Auctioneer checks validity of the signature by using public key of bidder sent by TTP.

Step 2: Decryption Key

TTP generates decryption key using shared keychain algorithm by combining TTP's and auctioneer's secret key share. Different encryption keys and corresponding decryption keys are generated for different rounds.

D. *Winner Determination phase*

Step 1: Auctioneer decrypts the bid and compute scores of bids. She finds the winner who maximizes the score and publishes her PseudoID and score.

Step 2: Auctioneer for further process to takes place she gets details from TTP through PseudoID but TTP will send details only after last round to maintain anonymity.

VI. SECURITY ANALYSIS

Security analysis for multi-round sealed bid Reverse auction is explained as follows:

A. *Anonymity* :

Bidder is identified only by his PseudoID. Auctioneer knows only the PseudoID of winner even after the final round. TTP will reveal only the details of the last round winner to Auctioneer.

B. *Bid privacy* :

Bid privacy achieved here is weak because auctioneer knows all the bid details during opening phase of each round.

C. *Non-Repudiation* :

All bidders produce their signatures Sig(bid), on the commitment to their bids. Therefore, the submission of their bids is undeniable due to their signatures.

D. *Integrity* :

Each bidder must register before bidding, and each bid should signed by an authenticated bidder. In the transmission phase auctioneer can check tender modification by validating the bidder's signature.

E. *No framing* :

PseudoID and Sig (E(bid, Yi)) uniquely identifies the bidder. No one can falsely claim to be any other bidder who participated in the auction.

F. *One-time Registration* :

The bidder only needs to register once and then he can participate in all auction items

G. *Easy revocation* :

TTP can easily revoke someone's right to bid. It is easy for TTP to delete the bidder's identification and secret parameters from the database. Once the information is removed from the database, TTP informs auctioneer immediately to update. Then the bidder loses the right to participate in the auction. If bidder bids some false bids (bid shilling) dispute can be solved by TTP, when auctioneer provides PseudoID of bidder.

VII. Conclusions

This work developed here satisfies security requirements like anonymity, bid privacy, non-repudiation and data integrity in multi-round multi attribute reverse auctions by using online TTP (Certified member of CA) and cryptographic algorithms; shared keychain algorithm, pseudonym generation algorithm and ElGamal based signature algorithm. This scheme is the first one in dealing with security issues in multi-round multi attribute reverse auctions. Use of online TTP is an innovative idea and is never been put forward in this field. The scheme developed here can effectively reduce the computational load on the auctioneer and bidders. The proposed scheme can assure a secure bidding environment for the sellers. This scheme improves bidding efficiency, effectiveness and convenience of the auction.

References

[1] S. Beall *et al.*, "The role of reverse auctions in strategic sourcing," Center for Advanced Purchasing Studies, Temple, AZ, USA, Tech. Rep., 2003.

[2] G. Z. Bupt, S. Sangwan, and S. Tingjie, "Mechanism design of online multi-attribute reverse auction," in *42nd Hawaii International Conference on System Sciences*, Jan., pp. 1–7. [Online]. Available: 10.1109/HICSS.2009.306

[3] S. Talluria, R. Narasimhana, and S. Viswanathana, "Information technologies for procurement decisions: a decision support system for multi-attribute e-reverse auctions," *International Journal of Production Research*, pp. 2615–2628, 2007. [Online]. Available: 10.1080/00207540601020585

[4] L. Shengli, W. Changjie, and W. Yumin, "A secure multi-round electronic auction scheme,," in *EUROCOMM 2000, Information Systems for Enhanced public Safety and Security*, 2000, p. 330 334. [Online]. Available: 10.1109/EURCOM.2000.874827

[5] *An Agent-Based English Auction Protocol Using Elliptic Curve Cryptosystem for Mobile Commerce*, ser. Algorithms and Architectures for Parallel Processing. Springer Verlag, 2009, vol. 5574. [Online]. Available: 10.1007/978-3-642-03095-622

[6] *Secure Multi-attribute Procurement Auction.* Springer-Verlag, 2006. [Online]. Available: 10.1007/1160493824.

[7] D.-H. Shih, C.-H. Cheng, and J.-C. Shen, "A secure protocol of reverse discriminatory auction with bid privacy," in *Sixth International Conference on the Management of Mobile Business*, pp. 52–52. [Online]. Available: 10.1109/ICMB.2007.3.

[8] Y. F. Chung *et al.*, "Bidder-anonymous english auction scheme with privacy and public verifiability," *Journal of Systems and Software*, p. 113119, Jan. 2008. [Online]. Available: doi:10.1016/j.jss.2007.03.029

[9] E. David, R. Azoulay-Schwartz, and S. Kraus, "Bidding in sealed-bid and english multi-attribute auctions," *Decision Support Systems*, pp. 527–556, 2006. [Online]. Available: 10.1016/j.dss.2005.02.007.

[10] J. E. Teich *et al.*, "A multi-attribute e-auction mechanism for procurement: Theoretical foundation," *European Journal of Operational Research*, pp. 90–100, 2006. [Online]. Available: 10.1016/j.ejor.2005.04.023

[11] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, pp. 469–472, 1985.

[12] *Unique User-Generated Digital Pseudonyms.* Springer-Verlag, 2005. [Online]. Available: 10.1007/1156032615