퍼지 및 지능시스템학회 논문지 2004, Vol. 14, No. 6, pp. 678-686

단일 서버 기반의 안전한 봉인경매 기법

A Single Server-based Secure Electronic Sealed-Bid Auction Method

이건명, 김동호
Keon Myung Lee, Dong-Ho Kim

충북대학교 전기전자컴퓨터공학부, 컴퓨터정보통신연구소
School of Electric and Computer Engineering and RICIS, Chungbuk National University

Abstract

This paper presents a new method to securely conduct online sealed-bid auctions with a single auctioneer server. The sealed-bid auctions have several vulnerable security problems when they are performed on the Internet. One of such problems is the trust establishment between an auctioneer and bidders who participate in an auction. Several online sealed-bid auction methods have been developed to address this trust problem. The proposed method solves the security problems that would happen in the sealed-bid auction using a blind signature scheme and a contract signature protocol. It prevents the auctioneer from illegally manipulating the bidders' bidding information, repudiating the reception of some bid, manipulating the auction period, and illegally adding or deleting bids. In addition, it keeps the bidders from modifying the bidding information after issuing their bid and doing intentional mistake to invalidate their own bid. The method can be easily implemented using the multiagent architecture.

Key words : Sealed-bid auction, secure auction, security protocols, multiagent systems, electronic commerce

1. INTRODUCTION

The widespread accessibility to Internet has made various services developed in the online virtual space. One of the most popular services is the electronic commerce by which costumers and providers buy and sell goods and services without face-to-face interactions. Despite that state-of-the-state technologies are used in such Internet services, some problems are yet under struggling to resolve. Security is one of the crucial issues in the electronic commerce.

This paper is concerned with the security problems for online auctions that are one of electronic commerce services. Many auction web sites have been developed and have been being in service. Most of auction services on the B-to-C (business to customer) and B-to-B transactions are open-cry style auctions like English auction[1] in which all bidding information is available to other bidders during the bidding period. Meanwhile, online sealed-bid auctions are not so prevailing as open-cry auctions. This scarceness is partially caused by the trustworthiness problem on the auctioneer. Several security protocols have been proposed to enforce the trust to the auctioneer.[2-9] Those methods employ a trusted third party or multiple bidding managers sharing partial bidding information or a single server using security protocols to solve the trustworthiness problem. This paper proposes an online sealed-bid auction method with which auctions can be carried out in a trustworthy way between an auctioneer and multiple bidders without any third party and any assumptions on trust. The proposed method establishes the trust relationship between the auctioneer and bidders just through communications between them using a blind signature scheme and a contract signature protocol.

The remainder of this paper is organized as follows: Section 2 describes some auction protocols and some related works. Section 3 presents the proposed method for sealed-bid auctions. Section 4 shows how to design a sealed-bid auction system following the proposed method in terms of the multiagent paradigm. In final, Section 5 draws conclusions.

접수일자 : 2004년 8월 1일
완료일자 : 2004년 9월 8일
감사의 글 : 이 논문은 2004년도 충북대학교 학술연구지원사업의 연구비 지원에 의하여 연구되었음

2. RELATED WORKS

The first-price sealed-bid auction and the Vickrey auction are representative in the sealed-bid auctions. In the first-price sealed-bid auctions, each bidder submits its own bid without any information about the others' bids. The auctioneer awards the advertised item to the bidder who offered the highest price and the winning bidder pays its own bidding price. In the Vickrey (*second-price sealed-bid*) auctions, auctions are performed in a similar way to the first-price sealed-bid auction. The bidder who offered the highest price wins, but the clearing price is the second highest bidding price. It is known that in the Vickrey auctions the optimal strategy of bidders is to bid their true valuation of the advertised item.[7] Sealed-bid auctions are used, for example, in the auctioning of mineral rights to some government-owned land, in the sale of artwork and real estate, and in the auctioning of government procurement contracts.

In the off-line sealed-bid auctions, each bidder puts its own bidding price into an envelope, seals it up with some regulation stamp or signature, and submits it to the auctioneer. The bidders can get the confidence that their price is uncovered during the bidding period since they can check whether their envelope is illegally opened or not. It does not seem to be easy for bidders to get this kind of reassurance in the online sealed-bid auctions, since the bidding is electronically processed. If the auctioneer could see the bidders' prices, it might inform a colluding bidder of them to help the bidder win the auction. In the case of the Vickrey auctions, the auctioneer may put in some illegal bid to make more profit if it can see the bidding prices.

To support secure sealed-bid auctions on the Internet, several methods have been developed.[2-5] They can be classified into the following approaches: the trusted third party approach, the multiple auction server approach, and distributed encryption approach.

In the trusted third party approach, there is a third party which conducts auctions on behalf of an auctioneer in a trustworthy way. The auctioneer and the bidders are expected to have unconditional trust in the third party. Bidders encrypt their bidding information with the public key of the third party and send it to the third party. After the close of the bidding period, the third party determines the winning bid, and informs the auctioneer of the winning bid.[3] There is another method to use a third party called the auction issuer[4]. In this method, the bidders encrypt their bidding information with the public key of the auction issuer, and send the encrypted bidding information to the auctioneer. After the expiration of the bidding period, the auction issuer provides the auctioneer with some functions to determine the winning bid. In this method, the bidders do not need to directly communicate with the third party. In these third party-based methods, bidders are asked to believe that the third party does not collude with the auctioneer.

The multiple auction server approach allows to make multiple auction servers share partial bidding information to prevent bidding information from being revealed during the bidding period. In the approach, there is a method to use multiple bidding servers which conduct auctions.[5,13] The bidders encrypt their bidding information with each server's public key and then divide it and send such divided information to the bidding servers using (t,n)-threshold secret sharing protocol[5]. After the close of the bidding period, the bidding servers exchange the received bidding information each other, determine the winning bid and announce it. However, the method requires multiple bidding managers that work independently each other. It costs extra expense to implement such systems, and thus it is not suitable in small business applications.

In the distributed encryption approach, the auctioneer and the bidders conduct sealed-bid auctions using encrypted communication.[7,8,15] In this approach, the bidders gradually expose the bidding price information to the auctioneer through repetitive communication. Omote et al.[7]'s method represents bidders' bidding price in a binary number and hashes it bit by bid using hash chaining encryption[12], and sends it to the auctioneer. At the opening time, the bidders provide for the auctioneer pieces of information about their bidding price to be opened consecutively bit by bit from the most significant bit to the least significant bit provided that bit that is just opened is 1. In Prakobpol et al.'s method[8], bidding prices are represented by using a multi-dimensional hash chain, and bidders send their mobile agents holding the encrypted bidding prices to the auctioneer site. At the opening time, in the auctioneer site, the bidders' mobile agents communicate with the auctioneer server and they gradually expose the bidding prices to the auctioneer server. Even though the communication takes place in the auctioneer site during the opening phase, there remains yet concerns on security since the bidders' mobile agents reside in an insecure auctioneer site.

3. A SINGE SERVER-BASED SECURE SEALED-BID AUCTION METHOD

This section proposes a method that securely performs sealed-bid auctions with a single auctioneer server. The proposed method solves trust-related problems between the auctioneer and bidders using some security protocols.

3.1 Architecture and Entities

In the proposed auction system, there are two types of entities as follows:

Auctioneer It advertises an auction, receives the bids from the bidders, and determines the winning bidder and announces it after the end of the bidding period. The proposed method ensures that the auctioneer cannot uncover any information about the received bids until the bidding period ends and cannot illegally insert, delete, or modify the bidding information. In addition, it is guaranteed that the auctioneer determines the right winning bid and the right clear price.

Bidders They send an encrypted bid to the auctioneer if they are interested in the advertised item. At the end of the bidding period, they send to auctioneer their secret key used to encrypt their bid. The proposed method enables the bidders to verify whether the auctioneer determines the winner correctly. It is also ensured that the bidders cannot invalidate their bid illegally.

In the online sealed-bid auctions, usually there does not often exist the long-term relationship between bidders and the auctioneer or auctions may be run by many small-scale parties. Due to these reasons, we cannot expect any trust relationship between them. Therefore, it is very important to establish the trust relationship between the bidders and the auctioneer in the online sealed-bid auctions.

Figure 1 shows the schematic architecture of the proposed sealed-bid auction method that enforces trust on both the auctioneer and the bidders. When the auctioneer advertises an auction item, a bidder creates a secret key for itself and sends it to the auctioneer on which to get a digital signature, if it is interested in the item. When it sends the secret key, it uses the blind signature method[10] to prevent the auctioneer from uncovering the secret key information. The auctioneer signs on the secret key and keeps a copy of the signature in its database to use it to verity the bidders' secret keys later, and then sends the digital signature to the bidder. Then the bidder encrypts its bidding information, its digital signature on the secret key, and some supplementary information with its secret key and sends the encrypted message to the auctioneer. At the end of the auction period, the auctioneer asks the participating bidders to send back their secret key. The bidders send their secret key to the auctioneer so that it decrypts the received bidding information. Using the received secret keys, the auctioneer decrypts the bidding information and determines the winner according to some publicly known rule (e.g., the highest bidder wins). Based on the information provided by the auctioneer, the bidders can verify that the auctioneer determines the winning bid correctly. The proposed method can be used to support both the first-price sealed-bid auction and the Vickrey auction.

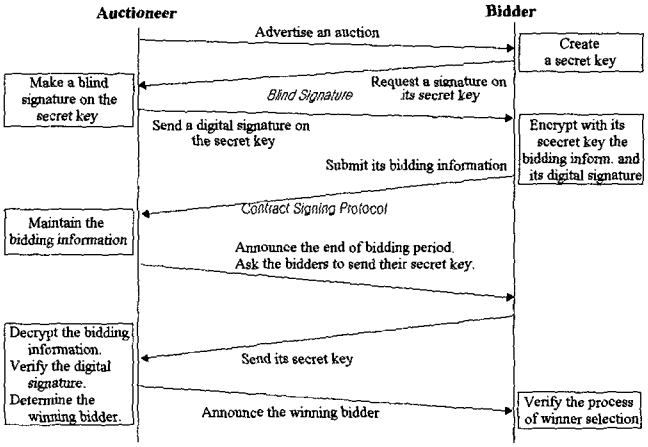

Figure 1. Schematic architecture of the proposed single server-based sealed-bid auction method

Figure 2 shows a sealed-bid auction scenario when the proposed method is employed. In the figure, each step performs the following operations:

① The auctioneer advertises an auction to bidders. On receiving the advertisement, a bidder who is interested in the auction item creates a secret key to be used in encrypting its bidding information.

② The bidder A sends its secret key that is processed by a blind function[10] in order to get a digital signature on the secret key.

③ The auctioneer signs on the blinded secret key and keeps a copy of the digital signature to verify the validity of secret keys later when it determines the winning bid. It also sends back a copy of the digital signature to the bidder.

④ Another bidder B sends its blinded secret key to the auctioneer in the same way as in step ②.

⑤ The bidder B gets back the signature on its secret key.

⑥ The bidder encrypts with the secret key its bidding price, digital signature on its secret key, and random value used in the blind function, and transfers it to the auctioneer using a contract signing protocol[11].

⑦ Each time the auctioneer receives a new bid, it delivers the received encrypted bidding information to all participating bidders later in order to enable them to monitor and verify the auction process. The auctioneer assigns a serial number to each received bid in an increasing order and distributes the received encrypted bidding information along with the assigned serial number to all participating bidders. On receiving such distributed bidding information, each bidder checks the serial number and may request the auctioneer to resend the missing bidding information, if any, that would have to be delivered before that.

⑧ Another bidder sends its bidding information in the same way as in ⑥.

⑨ The auctioneer sends the received bidding information to all participating bidders.

⑩ When the bidding period is expired, the auctioneer announces the close of the auction to all participating bidders.

⑪ The bidders send their own secret key to the auctioneer.

⑫ The auctioneer decrypts all bidding information using the received secret keys, and checks whether the right secrets are received by examining the digital signatures, the secret keys, and the random key values. Then it determines the winning bid and announces the winner to all participating bidders.

⑬ The auctioneer sends all bidders' secret keys to all participating bidders so that they can verify whether the auctioneer chose the right winner.

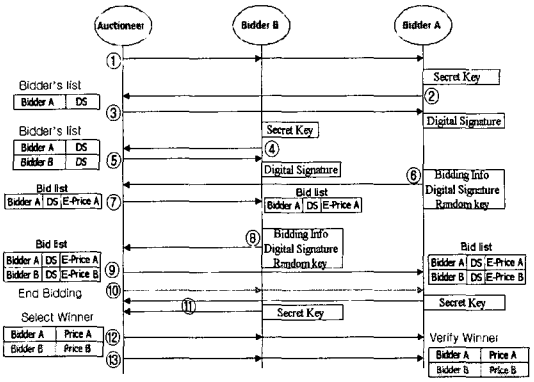

Figure 2. Auction scenario using the proposed method

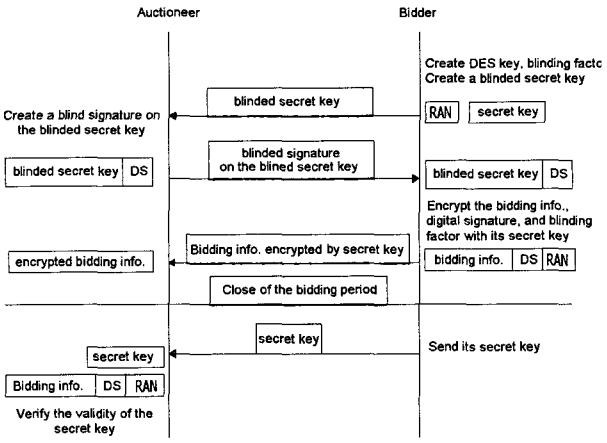

Figure 3. Maintaining secret keys

3.2 Maintaining Secret Keys

In the proposed method, the bidders send the encrypted bidding information to the auctioneer and provide the secret key to uncover the encrypted bidding information after the bid period is expired. There is a pitfall in this scheme. Some bidder may try to invalidate its bid by sending a wrong secret key to the auctioneer. To prevent such misbehaviors, the proposed method asks the bidders to get a digital signature on their secret key. The digital signatures are used to verify the validity of the secret keys when the auctioneer determines the winning bid.

The bidders must send their secret key to the auctioneer to get a digital signature on their key. However, they do not want the auctioneer to learn about their secret key until the end of the bidding period. To get a digital signature on their key, the bidders use the blind signature scheme. In the blind signature scheme [10], a bidder applies a blind function to its secret key with a random number, and it sends the blinded secret key to the auctioneer. The auctioneer cannot derive any useful information from the blinded secret key. The auctioneer signs on the blinded secret key and sends back it to the bidder. Then, the bidder can obtain the true digital signature on its secret from the digital signature on the blinded secret key and the random number used in the blinding function.

When a bidder issues a bid to the auctioneer, it encrypts the following information with its secret key into a message: its bidding information, the digital signature on its secret key, the random number used as the blind factor in the blind signature scheme. The encrypted information can be decrypted by the same secret key. The bidders provide their secret keys to the auctioneer at the time it determines the winning bid. With the secret keys, the auctioneer open all bidding

information and check whether the received secret key is valid or not by checking their digital signature and their corresponding random value.

3.3 Transferring Bidding Information

When a bidder issues a bid to the auctioneer, it wants to receive a certificate on its bid to prevent the auctioneer from repudiating the reception of its bid within the bidding period. To support this non-repudiation service, the proposed method uses a contract signing protocol when each bidder sends its bidding information to the auctioneer.

In the cryptography literature, there are several contract signing protocols[5]. The contract signing protocols are asked to satisfy the following requirements:

- Fairness If one party decides to abort the contract signing protocol, the other party should know that the protocol is over.
- Completeness The protocol should be robust against adversaries attempting to cause it to abort without the consent of either party.
- Non-Repudiation The protocol should not allow parties to arbitrarily decide to withdraw their support from a contract after the protocol is over.
- Efficiency Signing a contract should require a minimum of messages and computation time.

These protocols usually require heavy message exchanges between contractors, thus a large communication bandwidth and high computing power are usually needed in their implementation.

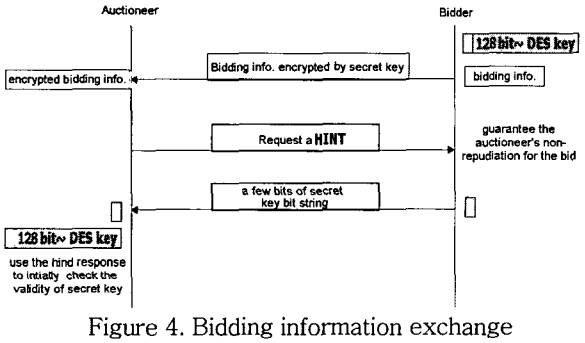

Figure 4. Bidding information exchange

The proposed method uses a variant of Ralph Merkel's puzzle protocol[6] which is a kind of contract signing protocols. The puzzle protocol exchanges a message in the following way to prevent a receiver from repudiating the reception of the message: The sender creates a puzzle by encrypting the signed contract with a very long, randomly chosen key in a symmetric algorithm. It sends the puzzle to the receiver and asks the receiver to send a return receipt for the puzzle. If the sender receives a return receipt, it sends to the receiver a "hint" for the puzzle. This hint helps the sender solve the puzzle, but does not reveal the entire message. The sender asks the receiver for a return receipt for the hint. If there is no more return receipt, the sender does not send any hint to the receiver and the contract is invalidated. The protocol continues until the sender has received a return receipt from enough hints such that solving the puzzle becomes trivial. Now the sender knows that the receiver has the message.

When a bidder submits bidding information to the auctioneer, a variant of Ralph Merkel's puzzle is used to prevent the auctioneer from repudiating the reception of the bidding. In the proposed method, the following mechanism is employed that is similar to the puzzle protocol: A bidder sends to the auctioneer the bidding information encrypted in its secret key, where the encrypted bidding information has the similar role of a puzzle in the puzzle protocol. On receiving the bidding information, the auctioneer sends back to the bidder a hint request that contains the time information when the bids was received and is signed by the auctioneer's private key. That received hint request message can be used as the certificate to show the bidding information is received by the auctioneer in time. As a hint to the hint request, the bidder sends several bits from its secret key bit string to the auctioneer. The hint bit strings can be used to pre-verify the bidders' secret key when the bidders send their secret keys just after the bidding period is expired. In the traditional puzzle protocol, a sequence of hint request and its response is carried out to make sure that the sender and its corresponding receiver have the confidence in the contract signing. But in the proposed method, they exchange only one hint request and one hint response to minimize the communication traffic. If the auctioneer does not send a hint request to the bidder, the bidder may resend its bidding information or checks the time and complains it to the auctioneer in an off-line way. If the auctioneer does not receive the hint from the bidder, it resends the hint request to the bidder. If the bidder does not answer to the request at the end of the bidding period, it considers that the bidder gives up the bidding. Figure 4 shows how the bidding information is exchanged using a variant of the puzzle protocol.

3.4 Verifying the Auction Results

By making the bidding information unreadable until the end of the bidding period, we can prevent the auctioneer from colluding with a bidder to award the auction item to

the bidder since there is no way to get the bidding prices. But there are other vulnerability in online sealed-bid auctions: At the end of the bidding period, when the auctioneer uncovers the bidding price, it may put a counterfeit bid to give the item to some specific party or to increase the clear price by adding a new second-price bidding price in a Vickrey auction. To prevent this kind of misbehaviors, the proposed method provides a validation mechanism as follows: Each time the auctioneer receives a new encrypted bid, it sends a copy of it to all participating bidders and new bidders are received all encrypted bidding information the auctioneer has received so far at that time they join in the auction. After the bidding period, the auctioneer receives the secret keys from all participating bidders, verifies the validity of the keys, determines the winning bid, and announces it to all participating bidders. After that, the auctioneer sends all bidders' secret keys to the participating bidders. Then each bidder performs the same operations as done in the auctioneer to verify that the auction has been carried out in a right way.

3.5 Maintaining Trust

In online sealed-bid auctions, the trust between the auctioneer and bidders is a crucial issue. The bidders want to make sure that the auctioneer does a fair deal, and the auctioneer wants to find out any misbehavior of bidders. The proposed method solves such trust problems by employing secret key encryption in bidding, contract signing protocol in bidding information transmission, blind signature technique, and an auction result validation mechanism.

3.5.1 Trust on the Auctioneer

The bidders may be worried about what if the auctioneer illegally manipulates their bids, what if it repudiates the reception of their bids, what if it insists that their bids did not arrive within the bidding period, what if it illegally adds or deletes some bids, or what if it determines a false winning bid. All these vulnerabilities are overcome by the proposed method as follows:

Illegal manipulation of bidding information The bidders send to the auctioneer their bidding information that is encrypted with their secret key. The secret keys are not available to the auctioneer until the bidding period closes. Therefore, there is no chance for the auctioneer to illegally manipulate the bidding information.

Repudiation of the reception of some bid To prevent the auctioneer from repudiating the reception of some bid, the proposed method uses a variant of the puzzle method which is a contract signing protocol. At the transmission of a bidding information, if the auctioneer receives an encrypted bidding information, it sends back a hint request message to the corresponding bidder. The hint request message contains some information about the time when the encrypted bidding information arrived at the auctioneer. This hint request message has the role of a proof of the bid participation and thus the auctioneer cannot repudiate the reception of some bid.

Illegal manipulation of bidding period The auctioneer may try to close the bidding period earlier than the time announced to keep some other bidders from participating in the advertised auction. This kind of misbehavior can be detected by the puzzle protocol used in bidding information transmission. Within the bidding period, the auctioneer has to receive any bid and respond with the hint request for such a bid. If the auctioneer responds with the message 'the bidding period is expired' within the bidding period, the bidder can tell whether the auctioneer is illegally manipulating the bidding period since the auctioneer's responses contain the information of timestamp at which they are created.

Illegal addition and deletion of bids To prevent the auctioneer from adding or deleting bidding information, the auctioneer is asked to distribute all encrypted bidding information to all participating bidders each time it receives a new bid. Therefore, after the close of bidding period, the auctioneer cannot add or delete any bidding information to affect the auction. That is because the winner bid and the second highest bid, which is used in Vickrey auction, must be in the list of bidding information received by all participating bidders.

Dishonesty in selection of the winner To make sure the auctioneer selects the right winner, the proposed method provides a verification mechanism. After the announcement of the winning bid, it gives all the participating bidders all secret keys of bidding information they have received during the bidding period Thus the bidders can verify whether the winner selection is properly made, using the bidding information and secret keys.

3.5.2 Trust on Bidders

The bidders participate in an auction to get the advertised item at the beginning. But later some bidders may change their mind and try to invalidate their bid in a

way other than making a legal withdrawal. One of invalidating attempts is to send a wrong secret key to the auctioneer after the close of bidding period. Sometimes, an unauthorized bidder may participate in the auction to make troubles. The proposed method solves these problems using the blind signature technique.

Intentional invalidation of bids To prevent the bidders from invalidating their bidding information, the proposed method asks the bidders to get their digital signature on their secret key using the blind signature technique, and asks them to include their digital signature in their bidding information and to submit their secret key along with their digital signature on the key just after the close of the bidding period. With this information of digital signature, the auctioneer can verify that the bidders sent a correct secret key. If the auctioneer finds out some bidders who sent a wrong secret key, it may ask them to resend their secret key or impose some constraints on the right to bid or some penalties on them.

Unauthorized bids To prevent some unauthorized bidders from joining in an auction, the proposed method asks every bidder to acquire a digital signature on its secret key. During the process, the auctioneer checks the identification of bidders and their qualification. Because the digital signature on secret keys are required each time they participate in an auction and the validity of bidding information is checked later, unauthorized bidders cannot participate in an auction.

3.6 Performance Analysis

The performance of the proposed sealed-bid auction method depends on the number of messages exchanged between the auctioneer and the bidders. The following shows the number of exchanged messages at each step when the auction takes place according to the method described in Figure 2: Let n be the number of potential bidders and m the number of participating bidders ($m \leq n$).

Step ① (auction announcement) : n

Step ②, ③, ④, ⑤ (blind signature processing) : $2m$

Step ⑥, ⑧ (bidding) : m

Step ⑦, ⑨ (multicast the encrypted bids to the participating bidders) : $m(m+1)/2$

Step ⑩ (announce the end of bidding) : n

Step ⑪ (report secret keys of bidders) : m

Step ⑫, ⑬ (award winner) : m

Therefore, the total number of exchanged messages is $m^2/2 + 11/2m + 2n$. Since $m \leq n$, the number of messages is $O(n^2)$. As the number of bidders increases, the message exchange increases by a square factor. This would be an obstacle to apply the proposed method to a sealed-bid auction with many bidders.

However, if the auctioneer delays the multicast of the encrypted bids at Steps ⑦ and ⑨, and multicasts all the encrypted bids at the end of Step ⑩ all at once, then the scalability can be largely improved. In that case, each time a bidder bids to the auctioneer, the auctioneer should send back so-called the receipt, containing the bidding information along with the bidding time stamp, which is encrypted with the auctioneer's private key. This prevents the auctioneer from intentionally leaving out some bidder's bid because the bidders can prove their bidding made within the bidding time with the receipt. In this modified method, the number of messages becomes $2n+6m$. Therefore this modified version can be applied to the situations in which there are many bidders.

3.7 Comparisons to other Single Server-based methods

Omote et al.[7]'s method and Prakobpol et al.'s method[8] provides sealed-bid auctions with a single auctioneer server. Their methods have an advantage in that the bidding prices other than the winner's are not disclosed during the opening phase.

Omote at al.'s method encodes the bidding prices in binary numbers and asks bidders to send pieces of bidding information as many times as up to the bit string length of the bidding prices in synchronized manner across all the bidders during the opening phase. The number of exchanged messages depends on the range of bidding prices as well as the number of bidders. It is also burdensome to synchronize the message exchanges multiple times. The proposed method, especially the modified version, is advantageous in that the number of exchanged messages depends on only the number of bidders and there is no special synchronization burden.

Prakobpol et al.'s method uses bidder mobile agents who contain bidding information and reside in the auctioneer's site. Therefore, in terms of communication overhead, Prakobpol et al.'s method is efficient since the communication between the auctioneer and the bidder agents take place in a single server. However, if a hacker gains a control of the auctioneer's site, the method has some risk for the bidding information to be leaked. Compared to this method, the proposed method sends the encrypted bidding information to the auctioneer. It keeps the bidding information in secret on the auctioneer site as far as the employed encryption system is strong enough.

4. DESIGN OF A MULTIAGENT-BASED SEALED-BID AUCTION SYSTEM

The proposed auction method requires multiple message exchanges between the auctioneer and bidders. Once an auction is opened by an auctioneer of the auction site, the role of auctioneer can be conducted by a software system without any intervention of human operators. Bidders can participate in online auctions through bidder clients that get bid prices from bidders, and exchange some messages with the auctioneer server. An auction system with this kind of an auctioneer and bidders can be efficiently implemented with a multiagent system. The auctioneer server and the bidder clients do not require much interaction with an auctioneer and bidders, and can work autonomously according to the predefined protocols. This kind of characteristics fits well with the agent paradigm[13].

The client-server architecture consisting of an auctioneer server and bidder clients can be seamlessly mapped into a multiagent architecture. We can build an auction system by assigning an agent to the auctioneer server and each bidder client, respectively. Each agent is supposed to have a communication module to find counterparts and exchange messages. The auctioneer agent plays the role of conducting an auction. It receives encrypted bidding information, announces the end of bidding period, and then gets the secret key information and determines the winner. It also has some cryptographic capabilities such as key authentication, digital signature generation, and so on. The bidder client agents are implemented in a form of daemon process that is a program always working on. Once it receives a bid price from the user, it generates a secret key and gets a blind signature on it from the auctioneer server agent, and then submits the encrypted bidding information containing the bid price and digital signature on the secret key. It waits until the auctioneer server agent tells the close of bidding period or provides encrypted bidding information that happens during the auction. Upon the announcement of the end of bidding period, it sends the secret key information and then waits the auctioneer server agent to announce the winner along with some information for verification.

Based on this design, we implemented a prototype auction system that supports both the first price sealed-bid auction and the Vickrey auction. The system is implemented using Java language and JCE(Java Cryptography Extension) library. The system is executable on any platform with a Java virtual machine. It is observed that the implemented system works successfully as it is expected.

5. CONCLUSIONS

This paper proposed a secure online sealed-bid auction method to use only an auctioneer. The proposed method establishes the trust relationship between the auctioneer and bidders by using blind signature and contract signing protocol. With the communications between the auctioneer and bidders, it enables both of counterparts not to cheat each other.

The key idea of the proposed method is not to reveal the bidding information until the end of biding period to the auctioneer. To do this, the bidders send bidding information encrypted by their own secret key and the auctioneer announces all encrypted bid information to all participating bidders. At the end of bidding period, the bidders provide their secret keys to the auctioneer.

The proposed method solves the trust-related problems that would happen in the online sealed-bid auctions like this. It prevents the auctioneer from illegally manipulating bidding information, repudiating the reception of some bids, illegally adding or deleting some bidding information, and determining a false winning bid. In addition, it prevents the bidders from illegally invalidating their bid and prevents unauthorized bidders from participating in an auction.

To support the proposed sealed-bid auction method, several cryptographic techniques are employed. Symmetric cryptographic system and asymmetric cryptographic system are used in encrypting and decrypting bidding information and in signing hint request messages. Blind signature technique is used in signing on secret keys. Contract signing protocol is used in transferring bidding information.

The proposed method can be easily implemented in a multi-agent architecture. The functions of an auctioneer and bidders can be easily modeled in the agent paradigm An auctioneer has well-established functionality and thus it can be successfully implemented in an agent. Due to the characteristics of bidders to wait some messages from the auctioneer and responds to them, the agents that work autonomously and independently are appropriate to the sealed-bid auction systems with the proposed protocol. We implemented a sealed-bid online-auction system based on the proposed method. It works in an expected way and does not require so many resources since the auctioneer server can be implemented in a single computer.

In the proposed system, to provide the non-repudiation service the auctioneer distributes to the participating bidders all bidding information that is encrypted with the bidder's secret key. There might be some risk that a bidder discovers other bidders' bidding information. If a bidder uses a supercomputer to decipher the received bidding information, it may succeed in uncovering the contents of some bidding information although its possibility is very low. If the auction item is very valuable, we can improve the security level by asking the auctioneer to encrypt the received bidding information with its own secret key before it distributes it to the participating bidders.

The proposed method requires frequent message exchanges between the auctioneer and bidders. Therefore, it would have some communication bottleneck at the auctioneer server side. But in small-scale online sealed-bid auctions, such a problem would not happen. In addition, the modified version of the proposed method enables the communication overhead to increase just by a factor linear to the number of bidders by using an additional public-key mechanism.

References

[1] P. Garcia, E. Gimenez, L. Godo, J. A. Rodriguez-Aguilar, "Bidding Strategies for Trading Agents in Auction-based Tournaments", in *Agent Mediated Electronic Commerce*(P. Noriega, C. Sierra, eds), pp.151-165, Springer, 1999.

[2] M. K. Franklin, M. K. Reiter, "Fair exchange with a semi-trusted third party", *Proc. of the 4th ACM Conf. on Computer and Communication Security*, pp.1-6, 1997.

[3] A. Asokan, V. Shoup, M. Waidner, "Asynchronous protocols for optimistic fair exchange", *Proc. of the IEEE Symp. On Research in Security and Privac,,* pp.86-99, 1998.

[4] M. Naor, B. Pinkas, and O. Reingold. "Privacy preserving auctions and mechanism design", *Proc. 1st ACM Conference on Electronic Commerce,* October 1999.

[5] M. K. Franklin, M. K. Reiter. "The design and implementation of secure auction server", *IEEE Trans. On Software Engineering*, Vol.22, No.5, pp.302-312, 1996.

[6] David Molnar, "Signing Electronic Contracts", *ACM Crossroads.* Available at http://www.acm.org/ crossroads/ xrds7-1/contract.html

[7] T. W. Sandholm, "Distributed Relation Decision Making", in *Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence* (G. Weiss, eds.), The MIT Press, pp.259-298, 1999.

[8] K. Omote, A. Miyaji, An Anonymous Sealed-bid Auction with a Feature of Enterntainment, Transaction of Information Processing Society of Japna, Vol.42, No.8, Aug. 2001.

[9] N. Prakobpol, Y. Permpoontanalarp, Multi-dimensional Hash Chain For Sealed-Bid Auction, *Lecture Notes in Computer Science*, Vol.2908, 2003.

[10] T. Okamoto, H. Yamamoto, *Modern Cryptography*, Industry Books, 1997.

[11] C. P. Pfleeger, *Security in Computing*, Prentice-Hall, 1997.

[12] W. Stallings, Cryptography and Network Security: Principle and Practice, Prentice-Hall, 1999.

[13] G. Weiss, *Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence*, The MIT Press, 1998.

[14] A. Juels and M.Szydlo. A Two-Server Sealed-Bid Auction Protocol, *Proc. of Financial Cryptography 2002*, 2002.

[15] K. Suzuki, K. Kobayashi, H. Morita, Efficient Sealed-bid Auction Using Hash Chain, *Proc. of 3rd International Conference on Information Security and Cryptology*, pp.183-191, 2000.

저 자 소 개

이건명(Keon Myung Lee)
14권 5호 참조

김동호(Dong-Ho Kim)
2000 : 충북대학교 컴퓨터과학과(학사)
2002 : 충북대학교 전자계산학과(석사)
현재 LG전자 정보통신사업부
관심분야 : 보안, 인공지능