Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2014, Article ID 314180, 11 pages
http://dx.doi.org/10.1155/2014/314180

Research Article

An Agent-Based Auction Protocol on Mobile Devices

Yu-Fang Chung,[1] Tzer-Long Chen,[2] Tzer-Shyong Chen,[3] Dai-Lun Chiang,[3] and Yu-Ting Chen[4]

[1] *Department of Electrical Engineering, Tunghai University, No. 1727, Section 4, Taiwan Boulevard, Xitun District, Taichung 40704, Taiwan*
[2] *Department of Technological Product Design, Lingtung University, Taiwan*
[3] *Department of Information Management, Tunghai University, Taichung, Taiwan*
[4] *Department of Computer Science and Engineering, National Chiao Tung University, Taiwan*

Correspondence should be addressed to Yu-Fang Chung; yfchung@thu.edu.tw

Received 14 October 2013; Revised 10 April 2014; Accepted 17 April 2014; Published 13 May 2014

Academic Editor: Li Weili

This paper proposes an English auction protocol to preserve a secure, fair, and effective online auction environment, where the operations are integrated with mobile agent technology for bidders participating in online auctions. The protocol consists of four participants, namely, registration manager, agent house, auction house, and bidder.

1. Introduction

With the popularization of the World Wide Web and its prompt adaptability to trends, traditional auction systems and business transactions have gradually transferred themselves to network platform transactions. Not only does online auction solve general problems like market price discrepancy due to asymmetric information, it also makes up for the time, space, and location constraints faced by traditional auctions and provides for transactions being conducted in conditions much freer and more public, allowing information much more transparency, and thus much fairer, and equal trading opportunities for the interested [1]. Therefore, online English auctions have successfully come to replace the offline traditional auctions, appearing more powerful and capable than the offline ones.

With the rapid development of mobile phones, the demand for mobile commerce has increased as a consequence. Based on market demand considerations, mobile service providers have begun launching mobile commerce services. To meet auction security demands in an environment of heterogeneous networks, an auction mechanism must satisfy both mobile and constraint needs. Under the analysis of various auction mechanisms in the study, a safe, fair, and efficient online auction environment was established by mobility and autonomy features of employing mobile agent.

Today, online auction protocols are applied over the Internet, including open auction and sealed-bid auction. Open auction can be subdivided into English auction and Dutch auction [1]. English auction is to have all participant bidders place their bidding prices on the basis of the reserve price that is preliminarily set by a host. After everything is in place, the host starts the bidding process. The bidding price soars gradually, the item going to the participant at the highest price. In Dutch auctions, bidders place their bids for lower prices. The auction will be closed when a bidder is willing to pay the final price [2]. Bidders in English auction can observe the bidding behaviors of their competitors during the entire auction process, so as to immediately adjust the bidding hereafter. Such a protocol is highly competitive because its game rule forces the bidding price to rise up. Thus, an item fetches highest price [3] at auction. As a result, the expected return on the goods in English auction protocol is usually higher than that in other protocols. Most auction-based websites, such as eBay and Yahoo! auctions, run the auction following English auction protocol, which are applied to the application of mobile commerce in the paper.

For the auction model on a mobile-based environment, [4] proposed a mobile auction agent model (MoAAM); bidders participate in online auctions through mobile agents. The protocol employed modular exponentiation operations which require a large computation amount, bringing a gradual degradation of performance in key generation, bidding, and verification phases. In contrast, the study runs the proposed protocol under the difficulty of solving discrete logarithm problem, leading to the positive improvement of performance in key generation, bidding, and verification phases. In terms of computation reduction on mobile devices and the workload of the connected server, the proposed system makes online auction systems much more convenient. A system should be endowed with the following features to maintain a fair and secure auction [5].

(1) Anonymity: during the course of an auction, no one is able to recognize the other bidders' identities.

(2) Traceability: the winner's real identity can be recognized at the end of the auction.

(3) No framing: the identities of all bidders remain independent. No one can falsely claim to be any other bidder who participates in the auction.

(4) Unforgeability: nobody is able to forge another one's valid bidding price.

(5) Nonrepudiation: the winning bidder is unable to deny the proposed bidding price after being announced.

(6) Fairness: all bidding must be conducted in an open and fair manner.

(7) Public verifiability: anyone can verify the identities and bidding prices of the participating bidders.

(8) Unlinkability among various auction rounds: nobody will know the same bidder's identity among different rounds of auction.

(9) Linkability within a single auction round: the bidders can repeatedly place new bidding prices within a single auction round and can be recognized by other bidders.

(10) Efficient bidding: in order to make the bidding efficient, computation complexity must be minimized.

(11) One-time registration: the bidder only needs to register once and then he/she can participate in all auctions that are opened.

(12) Easy revocation: the registration manager can easily revoke someone's right to bid.

The rest of this paper is organized as follows. Section 2 contains a review of related work on English auction protocol, the related cryptosystem concepts, and how the mobile auction agent model actually works in practice. The proposed protocol is shown in Section 3. In Section 4, the analyses of security and efficiency would be performed to examine the proposed protocol. The final conclusion and recommendations for further studies are given in Section 5.

2. Related Work

2.1. English Auction Protocol. Regarding English auction protocol research, the concept of bulletin board for verification was firstly applied to an English auction protocol in [6], satisfying various security concerns in the auction and successfully reducing computation and server load during the auction. The method was based on the concept in [7, 8], where group signature technology was utilized in English auction protocol to offer bidders higher security. Under the consideration of security, the protocol in [6] would not publish any bidders' information against the bidder privacy's risk, leading to loss of anonymity, fairness, and unlinkability among auction rounds, etc., as required by the English auction protocol. Later, [5] made improvements on the method in [6], allowing bidders' identities and information to be published, yet risking the unlinkability among auction rounds, for example, bidders' identities could not be identified through released information of previous auction rounds. In 2003, [9] proposed a much simpler and more effective method for the anonymity in English auction. However, it was shown to be insecure enough for bidders' privacy and rights by [10], as bidders were not allowed to verify whether the shared keys they possessed belonged to the same auctioneer during the auction. Subsequently, [11] utilized an alias for resolving the situation.

2.2. RSA Cryptosystem. RSA, developed by Rivest, Shamir, and Adleman, makes use of an expression with exponentials. It is the first algorithm known to be suitable for signing as well as encryption and is one of the first great advances in public-key cryptography. The RSA is one specific method of public-key cryptosystem utilizing two prime numbers as the key for encryption and decryption. The operations of RSA are listed below.

(1) Randomly select two large prime numbers p and q and calculate $N = pq$.

(2) Compute the least common multiple of two large prime numbers $\phi(N) = (p-1)(q-1)$.

(3) Compute the public key e, where e satisfies $\mathrm{GCD}(e, \phi(N)) = 1$.

(4) Compute the secret key d, where d satisfies $ed = 1 \bmod \phi(N)$.

(5) Publish (e, N) but keep the secret key d secretly. Since the security of RSA is based on calculating the prime factors p and q after publishing N the large prime numbers p and q should be carefully selected so that their factorization becomes impossible.

(6) The encryption and the decryption are presented as follows, where M is the plaintext and C is the ciphertext after the encryption.

$$\text{(Encryption) } C = M^e \bmod N.$$

$$\text{(Decryption) } M = C^d \bmod N.$$

The difficulty in factorizing large prime numbers determines the reliability of RSA algorithm. In other words,

the more difficulty the integer factorization presents, the more reliable the RSA algorithm is.

2.3. ElGamal Digital Signature. Putting digital signatures on a document aims to show the integrity and the nonrepudiation. Integrity refers to preventing the document from being tampered with in the transmission process, and the receiver can use the digital signature for verifying whether the document is tampered with or not. Since digital signature is calculated by the signer using his/her secret key, it could prevent the signer from denying the signature that he/she signed afterwards. This is considered to protect the receiver, as nonrepudiation. In numerous studies, many protocols were proposed for digital signatures, such as DSA, RSA, Schnorr, ElGamal [12], and ECDSS. The study applied the ElGamal algorithm to signature scheme, which is further introduced as follows.

(1) Choose a large prime number p, where $p-1$ has a large prime factor, and a primitive root g, where $g \in Z_p$.

(2) The signer chooses one integer x as his/her secret key satisfying $1 < x < p-1$.

(3) After computing his/her public key y using the following equation, the signer publishes it. Consider

$$y = g^x \bmod p. \tag{1}$$

(4) The signer randomly chooses an integer k satisfying $(k, p-1) = 1$.

(5) Compute the signature (r, s) of plaintext m. Consider

$$r = g^k \bmod p$$

$$m = xr + ks \bmod p-1 \quad \text{or} \quad s = k^{-1}(m - xr) \bmod p-1. \tag{2}$$

(6) The receiver verifies the legality after receiving the signature (r, s) as follows:

$$g^m = y^r r^s \bmod p. \tag{3}$$

If the equation holds, (r, s) is the legal signature of the plaintext m and vice versa.

The security of ElGamal depends on solving the difficulty of discrete logarithm problems p and g. An inappropriate selection of p and g would therefore result in the signature being forged.

2.4. Diffie-Hellman Key Exchange. Diffie-Hellman key exchange scheme allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communication channel [13]. The security is based on the difficulty of discrete logarithm problem (DLP). The operation of Diffie-Hellman key exchange is shown as follows.

(1) A selects one integer x as his/her secret key, which satisfies $1 < x < p-1$, where p is a prime number. Then, A uses the following equation for computing his/her public key X and publishes X:

$$X \equiv g^x \bmod p. \tag{4}$$

(2) B selects one integer y as his/her secret key, which satisfies $1 < y < p-1$, where p is a prime number. Then, B uses the following equation for computing his/her public key Y and publishes Y:

$$Y \equiv g^y \bmod p. \tag{5}$$

(3) Both A and B have the published public key and their own secret keys to calculate the shared secret key K_{ab} as follows:

$$K_{ab} \equiv Y^x \bmod p \quad \text{or} \quad K_{ba} \equiv X^y \bmod p. \tag{6}$$

(4) The last step is the verification, as follows:

$$K_{ab} \equiv Y^x \equiv (g^y)^x \equiv (g^x)^y \equiv X^y \equiv K_{ba} \bmod p. \tag{7}$$

There are two disadvantages to Diffie-Hellman scheme. First, the session key could merely be used between the two parties. When there are n users in a system, and one of them wants to communicate with any of the other users, the user will need to have $n-1$ session keys and the system will have to maintain $x(x-1)/2$ session keys. Second, the identities of the presently communicated objects are unknown; i.e., A and B would not recognize each other's actual identities.

2.5. Mobile Agent

2.5.1. Basic Concept of Mobile Agent. Recently, the application of mobile technology to network data transfer has received considerable attention. In information technology, the mobile agent is highly autonomous and is a mobile software that the users can capitalize to perform tasks in heterogeneous network environments. Since the mobile agent does not require constant online network connections, it also demonstrates significant improvement in the network performance.

The advantages of mobile agents include (1) low network loads, (2) high network latency resistance, (3) encapsulation of protocols, (4) asynchrony and autonomy, (5) dynamical adaptation, and (6) natural heterogeneity. The advantages of assigning tasks to mobile agents cannot be overemphasized. However, because it is entrusted with the user's private key and agent code at the time of task assignment, the data transfer management regarding agents' access management and control becomes particularly important.

Although this protocol can effectively solve data transmission insecurity, the efficiency can still be improved on. In Figure 1, the repetitious key storage in different agent codes not only results in the memory space consumption, it but also causes performance exhausted while computing keys.

Therefore, [14] proposed two schemes in the application of mobile agent. The first method applied the tree-structure

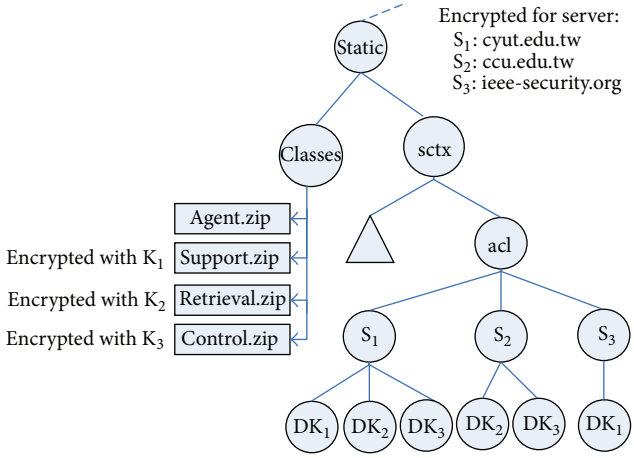
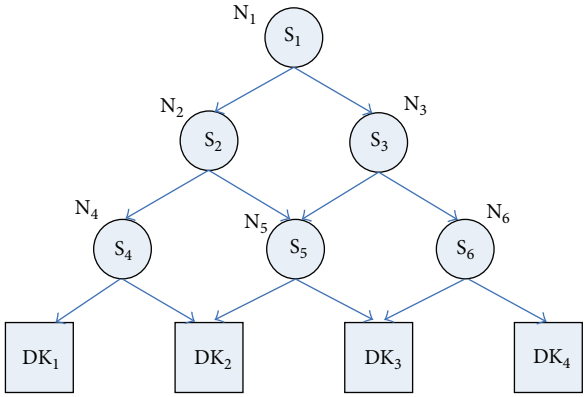


Figure 1: Tree-based structure of key management and access control.



DK: decryption key

Figure 2: Hierarchical structure of key management and access control.

of Akl and Taylor into the agent management, integrating the keys of lower successive tiers as one. The server could thus use its own key and through mathematical computation obtain successive private keys that could restore confidential documents. This security is based on the difficulty of solving elliptic curve discrete logarithm problem. The second scheme, in its attempt to improve mobile agent's computation efficiency, applied the cryptosystem based on the difficulty of discrete logarithm problem to reduce the public parameter size without compromising security. Their approach used the hierarchical structure for managing mobile agent's access control to users' keys, at the same time protecting data transmission when the access permission differed from user to user as shown in Figure 2.

During the task execution, the mobile agent roams between various hosts in a network. In the process to carry out message exchanges, it may also be required to connect with other mobile agents, which, thus, imposes security concerns arising out of insecure connections [15], malicious modifications by unauthorized external users, or even deliberate attacks by internal users. Therefore, mobile agent security is an important issue that needs to be overcome to effect into its successful application.

The mobile agent might face the following threats during the task execution.

(1) Unauthorized users access to the related information of servers:

(1.1) causing deliberate system paralysis and breakdown in a nonauthorization situation,

(1.2) unauthorized access to data or resource from server by forging as authorized agents.

(2) Attacks on mobile agent by other agents:

(2.1) forging identity codes of other agents for authorization access to services and resources, thereby avoiding the responsibility and breaching other users' trust on the legal mobile agent,

(2.2) paralyzing the legal agent by sending repetitious messages.

(3) Attacks on mobile agent by other malicious servers:

(3.1) deceiving and threatening the mobile agent through the abuse of trusted third party servers' identification codes,

(3.2) ignoring the mobile agent's requests deliberately,

(3.3) deceiving negotiating mobile agents by tampering with their data field.

(4) Attacks on server by other malicious servers or mobile agents:

(4.1) deliberate delayed response to mobile agent's request: such common attacks intend to cut off the requests or lower the mobile agent's efficiency by making the mobile agent wait for responses, resulting in repeated requests and hence lowering the system efficiency. Abnormal or abrupt task termination of mobile agents results from deadlock state where other mobile agent continue to wait for responses,

(4.2) deterring the mobile agents from task completion deliberately, resulting in a live-locked.

2.5.2. Mobile Auction Agent Model. Mobile auction agent model [4], called MoAAM, is designed to enable users to use their mobile devices to participate in online auctions. MoAAM consists of four agents, namely, (1) personal agent, (2) customer agent, (3) auctioneer agent, and (4) broker agent. How these agents communicate with each other in MoAAM through a web server is shown in Figure 3.

Inside the mobile device, there is an interactive interface, called personal agent, which would connect with an agent

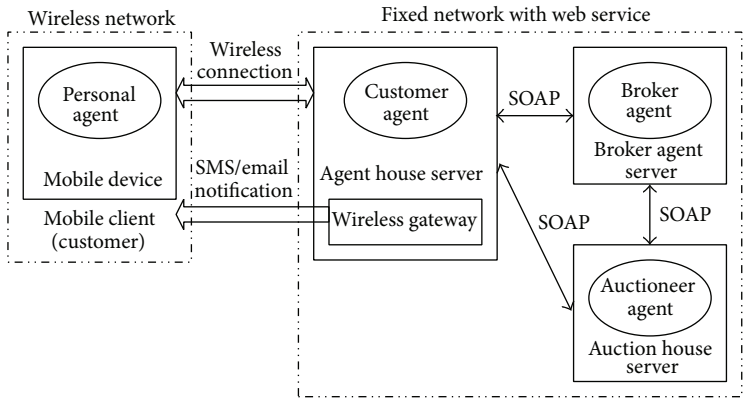


Figure 3: Communication in MoAAM.

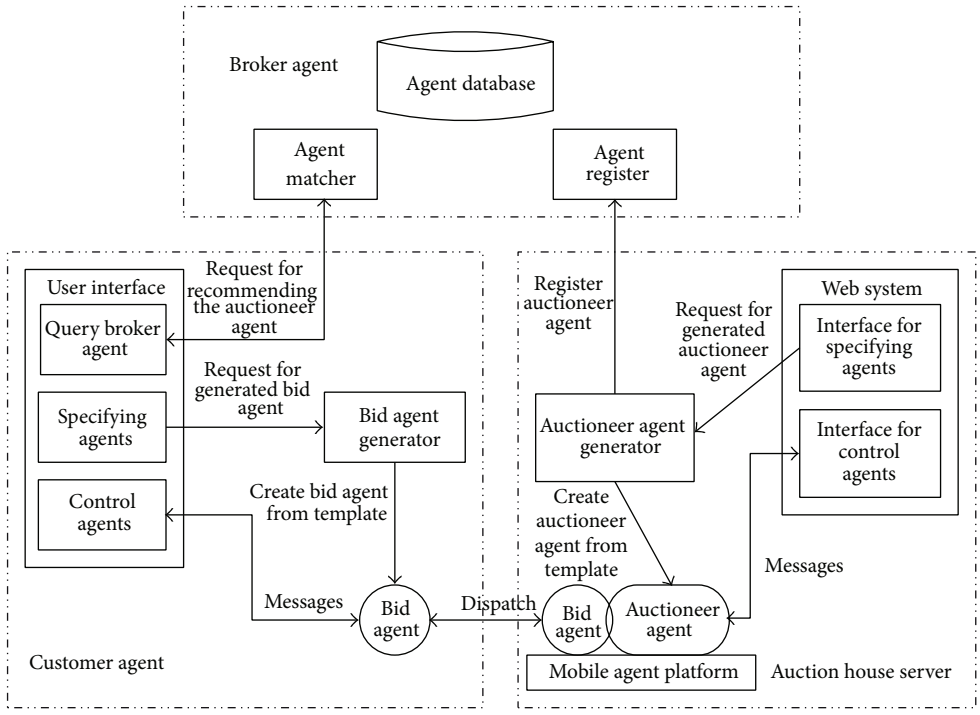


Figure 4: Architecture of MoAAM.

house server via the wireless network. In a few words, a personal agent is a preset agent that operates on the mobile device and provides an interface to allow users to communicate with the agent house server. The customer agent, the auctioneer agent, and the broker agent all operate in the fixed network. The personal agent connects to the customer agent when a mobile network user wants to buy a specific product. Then, the person agent sends the description of desired products and price information to the customer agent. On the other hand, an auctioneer registers the information of products to the broker agent. After the broker agent receives the user's request, an auction list, which meets the user's needs, will be generated and sent back to the user. If the user decides to purchase the auction items from the received list, a bid agent will be created by the customer agent and be dispatched to an auction house server to participate in the bidding.

The architecture of MoAAM [4] is shown in Figure 4 and how it works is described as follows.

(1) Primary participants in the MoAAM:

(1.1) broker agent: it is responsible for pairing up bidders and auctioneers. Moreover, it generates auction item lists and provides bidding price information for the users,

(1.2) bid agent: an individual user would use it for participating in auctions and placing the bids,

(1.3) auctioneer agent: auctioneers use it as their representative for managing the items they are selling,

(1.4) auction house server: a platform where online auctions take place.

(2) The running of customer agent.
The customer agent provides an interface with three different functions for the user:

(2.1) query the broker agent: know what kind of auction items the broker agent so far has registered and the bidding prices for these items,

(2.2) specify the bid agent: a user sends his/her request and bidding information to the bid agent generator. The generator will create a bid agent from a template,

(2.3) control the bid agent: this function allows the user to communicate with the bid agent and control the behavior of a bid agent.

(3) The running of broker agent.
First, the auctioneer needs to register his/her agent with the broker agent, and then the broker agent will store the auctioneer's information in the database. When the customer agent sends a request for item information, the broker agent would reply with a list of recommended items to the customer agent.

(4) The running of auction house.
The auction house server offers a web interface to allow the auctioneers to execute the following functions:

(4.1) specify the auctioneer agent: an auctioneer sends his/her request and auction information to the auctioneer agent generator. The generator will create an auctioneer agent from a template. The newly created agent and auction information would be registered with the broker agent,

(4.2) the management of the auctioneer agent: this interface allows the auctioneer to communicate with the auctioneer agent and control the auctioneer agent's behavior.

(5) Mobile agent platform.
The mobile agent platform is where the bid agent and the auctioneer agent would be sent to as the auction starts.

3. Proposed Protocol

The proposed system includes six phases of (1) initialization, (2) registration, (3) generation of transaction public key, (4) signature, (5) auction bidding, and (6) winner announcement. The whole process flow is shown in Figure 5. In the process, there are four main participants, which are registration manager (RM), agent house (AH), auction house (AUH), and bidder (B). What the participants do is described as follows.

(1) Registration Manager (RM):

(1.1) it is a unit for bidders applying for the registration. All bidders only require registering once. After that, they can participate in multiple auctions and no more registration is needed,

(1.2) to be in charge of storing bidders' identity information and corresponding secret parameters,

(1.3) to manage and maintain the bulletin board, which is called BBRM. On the bulletin board, two types of information would be published. One is the registration key and identity information of a bidder and another is a pseudonym that a bidder uses in a single auction round. The published information would be supplied to anyone for the identification verification, and only the RM has the authority to write and update the bulletin board.

(2) Agent House (AH):

(i) to be in charge of communicating with the broker agent and create bid agents,

(ii) to manage and maintain a bulletin board, which is called BB_{AH}. The bulletin board would provide the bidder's transaction public key for the verification purpose, and only the AH has the authority to write and update the bulletin board.

(3) Auction House (AUH):

(3.1) to provide the auction place, to maintain the operations, and to host the auctions,

(3.2) to manage and maintain a bulletin board, which is called BB_{AUH}. On this bulletin board, the published information would be the bidding information of bidders and the winning bidder's information. All the published information can be used for verifying one's identity, and only the AUH has the authority to write and update the bulletin board.

(4) Bidder (B):

(i) it is the one who participates and places bids in the auction.

The system using modular exponentiation in the English auction protocol is presented as follows. The given system parameters are shown in Table 1.

In the following are the auction processes.

3.1. Initialization. The RM and AH establish system parameters and the steps are as follows.

(1) Registration Manager

Step 1. Set up a read-only bulletin board (BB_{RM}) and post two kinds of information. One is the registration key and identity information of all bidders. Another is pseudonyms used by

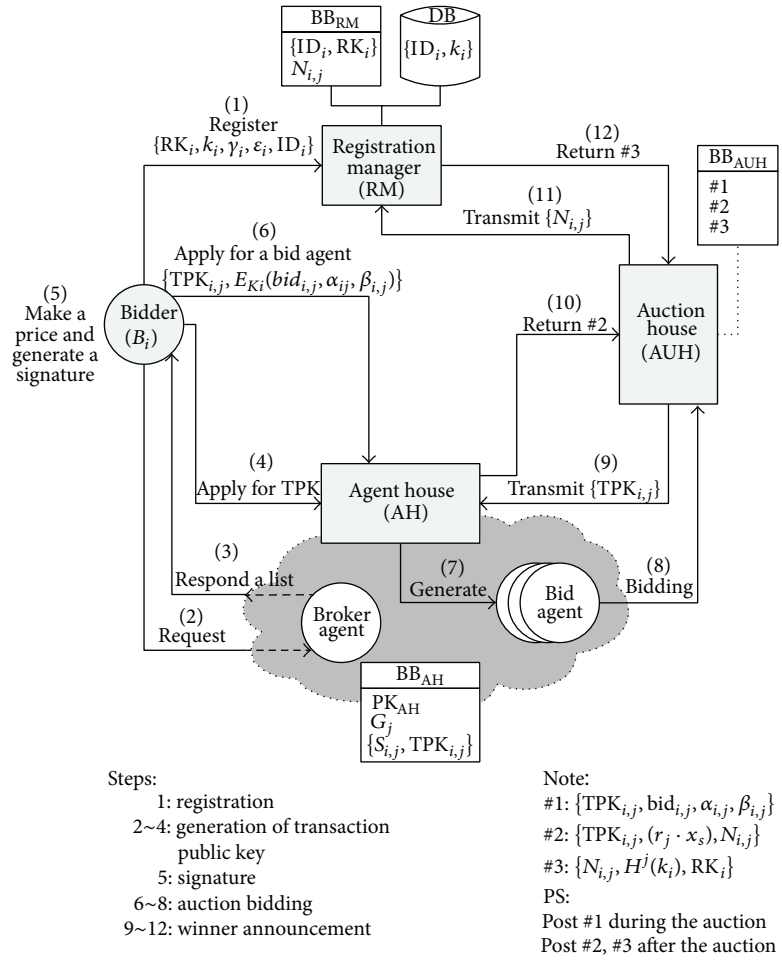


Figure 5: Flow chart of proposed system.

the bidders in the jth round of auction. The RM is the only one who can write and update the bulletin board.

Step 2. Declare p, q, g, $H(x)$ publicly.

(2) Auction House

Step 1. Set up a read-only bulletin board ($\mathrm{BB_{AH}}$) and publish the transaction public key and related information of all bidders on the bulletin board. AH is the only one authorized to write and update the bulletin board.

Step 2. Randomly select an integer $\mathrm{SK_{AH}} \in [1, q-1]$ as the private key to calculate the corresponding public key $\mathrm{PK_{AH}}$. The equation is as follows:

$$\mathrm{PK_{AH}} = g^{\mathrm{SK_{AH}}} \bmod p. \tag{8}$$

Step 3. Post $\mathrm{PK_{AH}}$ on $\mathrm{BB_{AH}}$.

3.2. Registration. As a new bidder (B_i) joins in an auction; B_i must apply for the registration with the RM at the very beginning. After the registration is completed, the RM would generate pseudonyms, which can only be used one time for B_i in the jth round of auction.

B_i should first calculate all relevant parameters before registering with the RM. The registration process is shown as follows.

Step 1. B_i randomly selects an integer $\mathrm{SK}_i \in [1, q-1]$ as the private key and computes a corresponding registration key RK_i. The equation is given as follows:

$$\mathrm{RK}_i = g^{\mathrm{SK}_i} \bmod p. \tag{9}$$

Step 2. B_i randomly selects an integer $k_i \in [1, q-1]$ as a secret parameter.

Step 3. B_i randomly selects an integer $t_{1,i} \in [1, q-1]$ and computes the verification information $(\gamma_i, \varepsilon_i)$. The computation steps are given as follows:

$$\begin{aligned} \gamma_i &= H\left(g^{t_{1,i}} \bmod p\right) \\ \varepsilon_i &= \left(t_{1,i} + \gamma_i \cdot \mathrm{SK}_i\right) \bmod q. \end{aligned} \tag{10}$$

Step 4. B_i sends the information $\{\mathrm{RK}_i, k_i, \gamma_i, \varepsilon_i\}$ and the identity information (ID_i) through a secure channel to the

Table 1: Parameters for modular exponentiation system.

p, q	Two big prime numbers, satisfying $q \mid p-1$
g	A generator with order q in Z_p
$E_K(m)$	A symmetric encryption method of message m with the key K (K is the shared key between Bi and AM)
$H(x)$	A one-way hash function, satisfying $H^j(x) = H(x, H^{j-1}(x))$ and $H^0(x) = x$
SK_{AH}	AH's private key
PK_{AH}	AH's public key
B_i	The ith bidder
$bid_{i,j}$	A bidding price that is placed by Bi in the jth round of auction
SK_i	Bi's private key
RK_i	Bi's registration key
$k_i, t_{1,i}, t_{2,i}$	Three secret parameters chosen by Bi
$N_{i,j}$	A pseudonym, RM creates only for Bi in the jth round of auction
r_j	A random number chosen by AH in the jth round of auction
G_j	The public information published by AH in the jth round of auction
$TPK_{i,j}$	A transaction public key, AH generates only for Bi in the jth round of auction

RM. After the RM receives the information transmitted by B_i, the registration would proceed.

Step 5. The RM authenticates the validity of $\{RK_i, k_i, \gamma_i, \varepsilon_i\}$ by the following equations:

$$\gamma_i' = H\left(g^{\varepsilon_i} \cdot RK_i^{-\gamma_i} \bmod p\right) \tag{11}$$

$$\gamma_i' \stackrel{?}{=} \gamma_i. \tag{12}$$

If (12) holds, $\{RK_i, k_i, \gamma_i, \varepsilon_i\}$ is valid. This proves SK_i and RK_i corresponding to each other. In contrast, RM would refuse to take the registration application from B_i if the received information is forged.

Step 6. The RM keeps B_i's identity information ID_i and the corresponding secret parameter k_i in its own database.

Step 7. The RM posts B_i's identity information ID_i and registration key RK_i on BB_{RM}.

Step 8. Before the jth round of auction starts, the RM would generate a pseudonym ($N_{i,j}$) for every bidder B_i. The order of all pseudonyms would be randomly arranged and posted on BB_{RM}. The equation is shown as follows:

$$N_{i,j} = RK_i^{H^j(k_i)} \bmod p. \tag{13}$$

Step 9. B_i can use (13) for computing his/her own pseudonym and verify that his/her pseudonym matches with the one posted on BB_{RM}. If B_i dose not find his/her pseudonym on BB_{RM}, he/she can appeal to the RM.

3.3. Generation of Transaction Public Key. In the jth round of auction, B_i can obtain the auction information through the AH who could ask the broker agent to supply the information about currently open auctions. The broker agent would prepare an auction house list that matches the needs of B_i and send the list back to the AH for B_i to review. When B_i decides which auction he/she wants to participate in, B_i would have to apply for a transaction public key ($TPK_{i,j}$), which is managed by the AH. The AH would generate $TPK_{i,j}$ with B_i's pseudonym on BB_{RM} for the bidder. The steps are given as follows.

Step 1. The AH randomly selects an integer $r_j \in [1, q-1]$ and computes the public information G_j. Then, the AH would post G_j on BB_{AH}. The equation is shown as follows:

$$G_j = g^{r_j} \bmod p. \tag{14}$$

Step 2. The AH would use $N_{i,j}$ and its own private key SK_{AH} for generating a parameter $S_{i,j}$ and $TPK_{i,j}$ for each B_i and post the generated information on BB_{AH}. The equation is shown as follows:

$$S_{i,j} = N_{i,j}^{SK_{AH}} \bmod p \tag{15}$$

$$TPK_{i,j} = N_{i,j}^{r_j \cdot S_{i,j}} \bmod p. \tag{16}$$

3.4. Signature. Before B_i starts to participate in the auction, B_i must verify $TPK_{i,j}$ given by the AH on BB_{AH}. If the key is valid, B_i would calculate the corresponding signature with the bidding price and related information. Subsequently, B_i can start participating in the bidding. The steps are stated as follows.

Step 1. B_i uses the AH's public key PK_{AH} for computing a parameter $S_{i,j}'$, as follows:

$$S_{i,j}' = PK_{AH}^{H^j(k_i) \cdot SK_i} \bmod p. \tag{17}$$

Step 2. B_i combines his/her private key SK_i and parameter $S_{i,j}'$ to generate $TPK_{i,j}'$, as follows:

$$TPK_{i,j}' = G_j^{H^j(k_i) \cdot S_{i,j}' \cdot SK_i} \bmod p. \tag{18}$$

$S_{i,j}'$ and $TPK_{i,j}'$ must verify that they are matched with the information posted on BB_{AH}; if not, B_i can appeal to AH.

Step 3. B_i randomly selects an integer $t_{2,i} \in [1, q-1]$ and decides a bidding price $bid_{i,j}$. Afterwards, a corresponding signature $\{\alpha_{i,j}, \beta_{i,j}\}$ is created, shown as follows:

$$\alpha_{i,j} = G_j^{t_{2,i}} \bmod p$$

$$\beta_{i,j} = \left(t_{2,i} + H^j(k_i) \cdot S_{i,j} \cdot SK_i \cdot H\left(bid_{i,j} \,||\, \alpha_{i,j}\right)\right) \bmod q. \tag{19}$$

Step 4. B_i uses the AH's public key PK_{AH} for computing the shared key K_i, shown as follows:

$$K_i = PK_{AH}^{H^j(k_i) \cdot S_{i,j} \cdot SK_i} \bmod p. \tag{20}$$

Table 2: Definition of the notation.

T_{MUL}	The time cost for modulus multiplication operation
T_{EXP}	The time cost for modulus exponentiation operation
T_H	The time cost for one-way hash function operation

Step 5. B_i used K_i for encrypting the bid $\text{bid}_{i,j}$ and the signature $\{\alpha_{i,j}, \beta_{i,j}\}$ to obtain the ciphertext $E_{K_i}(\text{bid}_{i,j}, \alpha_{i,j}, \beta_{i,j})$.

3.5. Auction Bidding. Before the auction starts, B_i needs to obtain a bid agent from the AH. After a bid agent is acquired, B_i, then, is allowed to bid. The auction bidding process is stated as follows.

Step 1. B_i should first send out the data tuple $\{\text{TPK}_{i,j}, E_{K_i}(\text{bid}_{i,j}, \alpha_{i,j}, \beta_{i,j})\}$ to the AH and apply for a bid agent.

Step 2. After the AH receives the data from B_i, the AH must compute the shared key K_i to decrypt the ciphertext $E_{K_i}(\text{bid}_{i,j}, \alpha_{i,j}, \beta_{i,j})$ and authenticate the validity of $\{\text{TPK}_{i,j}, E_{K_i}(\text{bid}_{i,j}, \alpha_{i,j}, \beta_{i,j})\}$. The equations for verification are shown as follows:

$$K_i = \text{TPK}_{i,j}^{\text{SK}_{\text{AH}} \cdot r_j^{-1}} \bmod p \tag{21}$$

$$G_j^{\beta_{i,j}} \stackrel{?}{=} \text{TPK}_{i,j}^{H(\text{bid}_{i,j} \| \alpha_{i,j})} \cdot \alpha_{i,j} \bmod p. \tag{22}$$

If (22) holds, this proves that $\{\text{TPK}_{i,j}, E_{K_i}(\text{bid}_{i,j}, \alpha_{i,j}, \beta_{i,j})\}$ is valid, and vice versa. The AH can reject the bidding request from B_i if the received information is false.

Step 3. The AH uses the bidding information $\{\text{TPK}_{i,j}, \text{bid}_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$ for creating a new bid agent for B_i, and then the AH would send this agent to the selected AUH to represent B_i participating in the auction.

Steps 1, 2, and 3 can be skipped if the bid is placed more than once. Only the bidding information would be verified.

Step 4. When the bid agent arrives at the AUH, it has to be verified that $\text{TPK}_{i,j}$ is the same as on BB_{AH}. If not, the AUH can reject B_i's application.

Step 5. The AUH verifies the bidding information $\{\text{TPK}_{i,j}, \text{bid}_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$ using (22). If (22) holds, it means that $\{\text{TPK}_{i,j}, \text{bid}_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$ is valid.

Step 6. The AUH posts the bidding information $\{\text{TPK}_{i,j}, \text{bid}_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$ on BB_{AUH}. Anyone can use (22) for verifying the bidding information of B_i.

3.6. Winner Announcement. When the jth round of auction ends, the one who places the highest bidding price would be announced as the winner. Then, the AUH would take the winner's $\text{TPK}_{i,j}$ to reconfirm the winner's information $N_{i,j}$ and RK_i with the AH and RM. Afterwards, the result would be published on BB_{AUH} and can be obtained by anyone to verify. The steps are stated as follows.

Step 1. The AUH takes the winner's $\text{TPK}_{i,j}$ to the AH and asks for the pseudonym $N_{i,j}$ used by the winner.

Step 2. The AH returns the information $\{\text{TPK}_{i,j}, (r_j \cdot S_{i,j}), N_{i,j}\}$ back to the AUH.

Step 3. The AUH can use (16) for confirming the relationship between $\text{TPK}_{i,j}$ and $N_{i,j}$.

Step 4. The AUH takes the winner's $N_{i,j}$ to the RM and asks for the winner's RK_i.

Step 5. The RM returns the information $\{N_{i,j}, H^j(k_i), \text{RK}_i\}$ back to the AUH.

Step 6. The AUH can use (13) for confirming the relationship between $N_{i,j}$ and RK_i.

Step 7. The AUH will post the winner's information, $\{\text{TPK}_{i,j}, (r_j \cdot S_{i,j}), N_{i,j}\}$ and $\{N_{i,j}, H^j(k_i), \text{RK}_i\}$, on BB_{AUH}. The winner's information on BB_{AUH} can be obtained by anyone to verify again according to (13) and (16).

4. Security and Efficiency Analysis

The proposed cryptosystem applied the ElGamal algorithm, it having two advantages: (1) not keeping secret parameters, as all system parameters can be public, and (2) different ciphertexts formed from the same plaintext at distinct time by one same user. The ElGamal parameters are generally used in each phase of this system. The security is established on the difficulty of solving discrete logarithm problem, for example, giving g, p, and S_{KAH}; the attempt of guessing or deciphering P_{KAH} is computationally infeasible. Regarding the above-mentioned security features, the proposed protocol is discussed as follows.

(1) Anonymity. Except RM and AH working together to reveal the identity during the auction, nobody can find out who the bidder is. The anonymity of bidders can be analyzed from the perspectives of RM, AH, and AUH.

(1.1) For the AUH, it is only authorized to obtain the bidding information, $\{\text{TPK}_{i,j}, \text{bid}_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$ and $\{\alpha_{i,j}, \beta_{i,j}\}$, is the signature for $\text{bid}_{i,j}$, where $\text{TPK}_{i,j}$ is a key for the verification. Thus, the AUH is just allowed to use $\text{TPK}_{i,j}$ for verifying the signature and comparing $\text{TPK}_{i,j}$ to the one posted on BB_{AH}. Still, who the bidder is will never be known.

(1.2) For the AH, it merely knows the relationship between $N_{i,j}$ and $\text{TPK}_{i,j}$; thus, it does not have enough information to recognize who the bidder is.

(1.3) For the RM, it cannot derive from $\text{TPK}_{i,j}$ to obtain the corresponding $N_{i,j}$, even if the RM has the bidder's identity information.

Table 3: Analysis of computation complexity

Phase	[4]	The proposed system
Registration	$5nT_{\text{EXP}} + 1nT_{\text{MUL}} + 2nT_H$	$5nT_{\text{EXP}} + 2nT_{\text{MUL}} + 3nT_H$
Generation of transaction public key	$7nT_{\text{EXP}} + 5nT_{\text{MUL}} + 1nT_H$	$(2n+1)T_{\text{EXP}} + 1nT_{\text{MUL}}$
Signature	$3T_{\text{EXP}} + 5T_{\text{MUL}} + 1T_H$	$4T_{\text{EXP}} + 8T_{\text{MUL}} + 2T_H$
Auction bidding	$3T_{\text{EXP}} + 3T_{\text{MUL}} + 2T_H$	$3T_{\text{EXP}} + 2T_{\text{MUL}} + 1T_H$
Winner announcement	$2T_{\text{EXP}} + 1T_{\text{MUL}} + 1T_H$	$2T_{\text{EXP}} + 1T_{\text{MUL}} + 1T_H$

As seen in the comparison table, the computation amount of this system is much lower than [4], especially in the generation phase of transaction public key.

(2) Traceability. Anyone can get $\{\text{TPK}_{i,j}, (r_j \cdot x_{S_{i,j}}), N_{i,j}\}$ and $\{N_{i,j}, H^j(k_i), \text{RK}_i\}$ from BB_{AUH} and use (13) and (16) for verifying the winning bidder's identity.

(3) No Framing. Unless attackers get B_i's SK_i, B_i's signature cannot be forged. Even if attackers get RK_i and intend to derive SK_i from RK_i, it will be difficult for him/her to obtain SK_i, because of the security based on the DLP.

(4) Unforgeability. Attackers will be unable to calculate the transaction public key by using the equation $\text{TPK}_{i,j} = G_j^{H^j(k_i)\cdot S_{i,j}\cdot \text{SK}_i}$ (in modular exponentiation system) or $\text{TPK}_{i,j} = (H^j(k_i) \cdot x_{S'_{i,j}} \cdot \text{SK}_i)G_j$ or to forge any valid bidding information $\{\text{TPK}_{i,j}, \text{bid}_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$. The reason can be explained in three aspects.

(4.1) Attackers cannot obtain B_i's SK_i, k_i, and $S_{i,j}$.

(4.2) Attackers have to spend a great deal of time on resolving the DLP, even if $H^j(k_i) \cdot S_{i,j} \cdot \text{SK}_i$ or $(H^j(k_i) \cdot x_{S'_{i,j}} \cdot \text{SK}_i)$ is captured.

(4.3) Because $H^j(k_i)$ is different in each round of auction, the bidder's pseudonym $N_{i,j}$ and transaction public key $\text{TPK}_{i,j}$ would be different in each round of auction.

(5) Nonrepudiation. A signature is hidden inside the bidding information and it has the characteristic of no framing. Therefore, the winning bidder of the auction round cannot deny his/her signature.

(6) Fairness. All bidders use pseudonyms to join in the auction. The AUH will post the valid bidding information BB_{AUH}. If B_i does not find his/her bidding information, he/she could appeal to the AUH. Like this, the AUH can fairly handle all bidders' information.

(7) Public Verifiability. Anyone can confirm the validity of the bidder, the validity of a bid, and the winning bidder's real identities.

(8) Unlinkability among Various Auction Rounds. In each auction, the pseudonym generated by the RM and the transaction public key generated by the AH are different. Except the RM and AH sharing these keys with each other, no one will know the relationship about B_i among various auction rounds.

(9) Linkability within a Single Auction Round. Within a single round of the auction, B_i holds the same $\text{TPK}_{i,j}$ to place a bid in the auction. It is traceable to know how many times the bidder places the bid and who places the bid.

(10) Efficiency of Bidding. The efficiency of bidding shall be explained later.

(11) One-Time Registration. A bidder uses a pseudonym $N_{i,j}$ for participating in the auction. Hence, B_i only needs to register once with the RM.

(12) Easy Revocation. It is easy for the RM to revoke a bidder's identification and secret parameters from the database. Once the information is removed from the database, the bidder loses the right to participate in the auction.

The following is the performance comparison between [4] and the proposed protocol. The notation used is defined as shown as Tables 2 and 3.

Due to modulus addition and subtraction operation amount being low, they can be omitted.

The analysis of computation complexity related to these two systems is described below following the above information.

As seen in the comparison table, the computation amount of this system is much lower than [4], especially in the generation phase of transaction public key.

5. Conclusion

This paper puts forward an agent-based English auction protocol to allow bidders to obtain information and participate in auctions through an agent. Based upon the proposal, it clearly satisfies all of the security requirements for online auction protocols, such as anonymity, traceability, fairness, and so on. Because the mobile devices are identified with inherently weaker computation capability, this protocol is employed on the mobile agent to achieve lower computation amount and to reduce the time cost consumed by verification and computation. This is a means to make the online auction on mobile devices become more efficient and convenient. As wireless networks continue to become extensively used, the proposed system for wireless data exchange has just met the minimum for the security purpose. In the future, the key

point would be focused on enhancing the auction-related data protection.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported partially by National Science Council, Taiwan, under Grant NSC 102-2221-E-029-008.

References

[1] Z. X. Huang, *Applying data mining to analyze online auction market [M.S. thesis]*, Chaoyang University of Technology, Taichung, China, 2003.

[2] F. M. Lee, J. P. Chen, and J. W. Hung, "Applying software agent on internet auction and bargaining system," *Institute of Information & Computing Machinery*, vol. 3, no. 2, pp. 67–80, 2000.

[3] F. C. Peng, C. O. Chang, and M. C. Chen, "A study of influence of different auction mechanism to no-performing assets," *Sun Yat-Sen Management Review*, vol. 16, no. 3, pp. 401–428, 2008.

[4] K. H. Huang, *A study on mobile computing applications to secure transaction models [Doctoral Dissertation]*, National Taiwan University, Taipei, China, 2008.

[5] K. K. Lee and J. Ma, "Efficient public auction with one-time registration and public Verifiability," in *Proceedings of the 2nd International Conference on Cryptology in India (INDOCRYPT '01)*, pp. 162–174, Chennai, India, December 16-20, 2001.

[6] K. Omote and A. Miyaji, "A practical English auction with one-time registration," in *Proceedings of the 6th Australasian Conference on Information Security and Privacy*, pp. 221–234, Sydney, Australia, July 2001.

[7] K. Q. Nguyen and J. Traore, "An online public auction protocol protecting bidder privacy," in *Proceedings of the 5th Australasian Conference on Information Security and Privacy*, pp. 427–442, Brisbane, Australia, July 2000.

[8] T. C. Wu, K. Y. Chen, and Z. Y. Lin, "An English auction mechanism for internet environment," in *Proceedings of the Information Security Conference (ISC '02)*, pp. 331–337.

[9] C.-C. Chang and Y.-F. Chang, "Efficient anonymous auction protocols with freewheeling bids," *Computers and Security*, vol. 22, no. 8, pp. 728–734, 2003.

[10] R. Jiang, L. Pan, and J.-H. Li, "An improvement on efficient anonymous auction protocols," *Computers and Security*, vol. 24, no. 2, pp. 169–174, 2005.

[11] Y.-F. Chang and C.-C. Chang, "Enhanced anonymous auction protocols with freewheeling bids," in *Proceedings of the 20th International Conference on Advanced Information Networking and Applications*, pp. 353–358, Vienna, Austria, April 2006.

[12] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[13] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[14] K.-H. Huang, Y.-F. Chung, C.-H. Liu, F. Lai, and T.-S. Chen, "Efficient migration for mobile computing in distributed networks," *Computer Standards and Interfaces*, vol. 31, no. 1, pp. 40–47, 2009.

[15] I.-C. Lin, H.-H. Ou, and M.-S. Hwang, "Efficient access control and key management schemes for mobile agents," *Computer Standards and Interfaces*, vol. 26, no. 5, pp. 423–433, 2004.