Secure Transactions Using Mobile Agents with TTP

Song Han, Elizabeth Chang Member IEEE
School of Information Systems
Curtin Business School
Curtin University of Technology
GPO Box U1987 Perth, Western Australia 6845

Tharam Dillon, Fellow IEEE
Faculty of Information Technology
University of Technology Sydney
PO Box 123 Broadway NSW 2007 Australia

***Abstract*—Electronic commerce has pushed and benefitted from the development of mobile agents technology. One of the reasons is electronic commerce needs remote searching and negotiating between one customer and a number of E-shops. Mobile agents can travel over the Intranet or Internet. Therefore, mobile agents can help the customer or E-shops with remote searching and negotiating. However, because of the heterogeneousness of the networks the mobile agents migrate to, security issues should be tackled with cautions. This paper presents a new secure electronic commerce protocol. The underlying transactions are accomplished with mobile agents. A trusted third party (in fact, a trusted authority) is involved in the protocol.**

Keywords: Auditing, Electronic commerce, Fair identifiability, Mobile agent, Purchase plan.

I. Introduction

The mobile agent paradigm has been proposed as a promising solution to facilitate distributed computing over open and heterogeneous networks. Mobility, autonomy, and intelligence are identified as key features of mobile agent systems and enabling characteristics for the next-generation smart electronic commerce on the Internet. However, security and privacy in the mobile agent technology should be settled with cautions, since the mobile agents will migrate to the heterogeneous networks for the tasks of transactions.

We present an agent-based scenario for mobile commerce and discuss techniques using mobile agents with trusted third party that have been implemented to provide security in this scenario.

Consider such a scenario: There is a customer **C** who decides to buy flight tickets on the Internet. We look on this decision as a *current purchase plan*. For this purchase plan, **C** defines the *purchase requirement* (e.g. travel line, maximum price of ticket, arrival time, valid period of this purchase, etc.). And then, the customer arranges some mobile agents to search over the Internet (actually these mobile agents migrate to some E-Shops, i.e. some Travel Agents Servers). These E-shops will bid for this *purchase requirement* of the *current purchase plan*. Each E-shop wishes her own bidding will be successfully selected by the Customer as an optimal one. In order to make this *bid* confirmed and accepted by the Customer, each E-Shop will put a *legal signature* on the *bid*. This will not only help the underlying E-Shop improve the possibility of the Customer accepting this bid, but also help the Customer to verify whether this bid is really from the underlying E-Shop, as well as prevent this E-Shop from denying providing this bid for the purchase plan. In addition, other E-shops could not fabricate a valid bid to impersonate the *successful bidder*. Here the successful bidder is the E-shop, whose bid is accepted and paid by the customer. An additional state of this scenario is the underlying E-shop denies either bidding any purchase plan of the customer or receiving any money to her account.

In this paper we will propose a secure *transaction* protocol to address the above scenario. The underlying techniques are based on a new proxy signature scheme[4]. Han et al have presented another new proposal for secure transactions using mobile agents with agent broker. Their method is based on the concept of undetachable signatures [2].

Our protocol is designed to protect *financial situations or rights* of the customer. This is maintained through the signature on the bid from the corresponding E-shop. Therefore, it can not only help the Customer to verify whether this bid is really from the underlying E-Shop, but also prevent this E-Shop from denying providing this bid for the purchase plan.

Another issue is some previous solutions have the security flaw [5], [6], [8], [11], [14]. In detail, the customer can forge valid bid on behalf of the E-shops. consequently, the customer can blackmail the underlying E-shop by the fabricated bid [16]. Then, the financial situation of the E-shops will be spoiled by the customer. In our protocol, the customer is not able to forge any valid bid on behalf of any E-shop involved in the transactions.

In our protocol, a trusted third party is involved in the transaction. The trusted third party (TTP) in our paper satisfies two conditions: (1) The trusted third party does exactly what it is expected to do. This means (a) No less than it is supposed to do, so that TTP commits no acts of commission, such as, "Oh, I forgot to lock the door." and (b) No less than it is expected to do, so that TTP commits no acts of commission, such as, "Oh, I accidently made an extra key and gave it to Eve." (2) The trusted third party always adhere to the related security law and policy. Therefore, a reputable bank (or a legal and reputable association, etc.) is able to play the role of the trusted third party [16], [19]. Based on this point, the trusted third party in our paper is indeed a trusted authority.

The organization of the rest of our paper is as follows: Section 2 introduces the model of secure transactions using mobile agents with a trusted third party. Section 3 presents

0-7803-8971-9/05/$20.00 ©2005 IEEE

a new protocol according to the proposed model. Section 4 provides construction analysis, security analysis, and privacy analysis. The performance analysis is presented in section 5. The concluding remarks are provided in section 6.

II. Model of Transactions Using MA with TTP

In this section, we will propose a model for secure transactions using mobile agents (MAs) with the trusted third party (TTP). The motivation to propose this model is the needing of a universal framework for the E-commerce protocols of secure transactions using mobile agents as a mediate. This model integrates the serviceability of a trusted third party.

Model 1 (Model of Transactions Using MA with TTP) There are at least four participants involving in the model. They include: a customer, a trusted third party, an E-shop (at least one E-shop involving), and a mobile agent (at least one mobile agent involving). Besides these participants, there are seven procedures for the proposed model. These procedures deliver the specifications for the electronic commerce protocol using mobile agents with TTP. The followings provide the details for the model.

(1) System Setup: This procedure is a probabilistic polynomial time algorithm [16]. It generates *global parameters* as well as *local parameters* for the participants involving this procedure.

(2) Interaction between E-Shop and TTP: This procedure is a deterministic polynomial time algorithm. It generates the pseudonyms and partial private keys for the E-Shops, who plan to sell goods in the protocol.

(3) Preparing Mobile Agents: This procedure is a polynomial time algorithm. It involves the interactions between the customer and its mobile agents.

(4) Mobile Agents Migrating: This procedure is a deterministic polynomial time algorithm. In this procedure, the mobile agents are equipped with a *purchase request* (It includes the *purchase requirements* and some ciphertexts of partial secrets). And then, mobile agents migrate to some E-shops. E-shops will first check whether this purchase request is legal.

(5) Processing Transactions: This is a probabilistic polynomial time algorithm. The underlying E-shop first constructs the bidding key, by which this E-shop is able to make bidding for the purchase request. *The process of bidding for the purchase request* is, in fact, *the process of signing E-shops' bid.*

(6) Checking Transactions: This procedure is a deterministic polynomial time algorithm. The customer first checks whether the *returned purchase requirement* is still the one previously delivered by the mobile agents. In addition, the time-stamp is examined whether it is still valid. If the two items are both good, the customer will verify the signature on the bid. and also the bid is an optimal one, the customer will accept this

(7) Auditing E-Shop: This procedure is a probabilistic polynomial time algorithm. This procedure is usually off-line, except that the underlying E-shop does not take its duty in the transaction.

III. Proposed Protocol for Transactions Using MA with TTP

In this section we will propose a new protocol for transactions using mobile agents with a TTP. The proposed protocol is specified according to the new model given in section 2. Therefore, this protocol includes the following procedures: System Setup, Interaction between E-Shops and TTP, Preparing Mobile Agents, Mobile Agents Migrating, Processing Transactions, and Checking Transactions, as well as Auditing i-th E-Shop. A new proxy signature scheme [] is implied in the protocol. Its security is based on the security of DSS. Therefore, the proposed electronic commerce protocol has the same security level with the DSS. In addition, fair identifiability as a new security and privacy mechanism is maintained in the protocol.

A. System Setup

In this subsection, we will set up the system parameters for the proposed protocol. In the proposed protocol, there are at least four different participants: a Customer, a Trusted Third Party, an E-Shop, and the Mobile Agents (at least one Mobile Agent involving in the underlying transactions). The followings are the specifications of the global parameters as well as the the local parameters:

(1) **Choice of Global Parameters** There is a large prime p. Its bit-length is L, i.e. $2^{L-1} < p < 2^L$; where L is a multiple of 64, and $512 \leq L \leq 1024$. q is another large prime, where q divides $p-1$ and bit-length of q is 160. Let h be a primitive root modulo p $(1 < h < p-1)$ [3]. Set $g = h^{(p-1)/q} \bmod p$. Therefore, q is the order of g modulo p.

(2) **Choosing H()** $H()$ is a SHA hash function [16].

(3) **Private/Public Key Pair of Customer** Choosing a random number x_C, $x_C \in Z_q^*$, and computing $y_C = g^{x_C} \bmod p$. The private key of the Customer is x_C, the public key is y_C.

(4) **Identity of Customer** Denoting ID_C as the identity of the Customer. It is a bit-string that can identify the Customer.

(5) **Identity of E-Shop** Denoting ID_S as the identity of the E-Shop. It is a bit-string that can identify the E-Shop.

(6) **Private/Public Key Pair of TTP** Choosing a random number x_{TTP}, $x_{TTP} \in Z_q^*$, and computing $y_{TTP} = g^{x_{TTP}} \bmod p$. The private key of the Trusted Third Party is x_{TTP}, the public key is y_{TTP}.

(7) **Identity of TTP** Denoting ID_{TTP} as the identity of the Trusted Third Party (TTP). It is a bit-string that is held by the Trusted Third Party.

B. Interaction between E-Shop and TTP

This procedure can be accomplished through "off-line" with respect to the underlying transactions. That is to say, the interaction is processed (by some E-Shops and a Trusted Third Party) earlier than the coming transactions. In this algorithm, the Trusted Third Party will issue a pseudonym and a secret key for every E-Shop (ES_1, ES_2, …, ES_n), by which the E-Shops can take part in the underlying transactions. The details are the followings:

(1) **Registration** Each E-Shop ES_i $(1 \leq i \leq n)$ registers her/his identity $ID_S^{(i)}$ $(1 \leq i \leq n)$ and a request R_i $(1 \leq i \leq n)$ to the Trusted Third Party, respectively.

(2) **Creating Pseudonym** The Trusted Third Party chooses two different random numbers $k_{TTP_i} \in Z_q^*$ and $k_S^{(i)} \in Z_p$ for each E-Shop ES_i $(1 \leq i \leq n)$, respectively. And he/she then computes r_{TTP_i},

$$r_{TTP_i} = g^{k_{TTP_i}} \text{mod } p \tag{1}$$

and

$$n_S^{(i)} = H(ID_S^{(i)}, R_i, k_S^{(i)}). \tag{2}$$

The $n_S^{(i)}$ will play the role of the pseudonym for each E-Shop ES_i $(1 \leq i \leq n)$, respectively. From the computation of $n_S^{(i)}$, we know that this pseudonym is linked to the identity of the corresponding E-Shop ES_i $(1 \leq i \leq n)$, respectively.

(3) **Sending Messages** The Trusted Third Party computes $s_{TTP}^{(i)}$,

$$s_{TTP}^{(i)} = x_{TTP} H(n_S^{(i)}), r_{TTP_i}) + k_{TTP_i} \text{mod } q \tag{3}$$

and then sends the tuple $\{n_S^{(i)}, s_{TTP}^{(i)}, r_{TTP_i}\}$ to each E-Shop ES_i $(1 \leq i \leq n)$ through a secure channel, respectively. $s_{TTP}^{(i)}$ will be a partial private key of the corresponding E-Shop.

(4) **Checking Partial Private Key** After each E-Shop ES_i $(1 \leq i \leq n)$ receives the above tuple, she/he will check whether the tuple satisfies the following equation

$$y_{TTP}^{H(n_S^{(i)}, r_{TTP_i})} = g^{s_{TTP}^{(i)}}. \tag{4}$$

If it holds, the E-Shop ES_i $(1 \leq i \leq n)$ will have $s_{TTP}^{(i)}$ as a partial private key, and $n_S^{(i)}$ as the pseudonym which is linked to her/his idnetity $ID_S^{(i)}$. Therefore, this E-Shop keeps $s_{TTP}^{(i)}$ secret, and makes $n_S^{(i)}$ as well as r_{TTP_i} public. If the equation does not hold, this E-Shop will register to the Trusted Third Party with another request R_i'.

C. Preparing Mobile Agents

As soon as the Customer initializes any purchase, she/he will prepare some mobile agents $MA_1, MA_2, \ldots, MA_n$ and arrange them to some E-Shops ES_i $(1 \leq i \leq n)$ for the purchase plan; where $n > 1$ is a positive integer. The details are the followings:

(1) **Constructing Public Parameters** The Customer chooses random numbers $k_C^{(1)} \in Z_q^*$, $k_C^{(2)} \in Z_q^*$, $\ldots$, $k_C^{(n)} \in Z_q^*$, and computes

$$r_C^{(1)} = g^{k_C^{(1)}} \text{mod } p, \tag{5}$$

$$r_C^{(2)} = g^{k_C^{(2)}} \text{mod } p, \tag{6}$$

$$\ldots,$$

$$r_C^{(n)} = g^{k_C^{(n)}} \text{mod } p. \tag{7}$$

These parameters will be involved in the forthcoming transactions.

(2) **Constructing Purchase Requirements** According to the current purchase plan, the Customer will construct the corresponding purchase requirements. These purchase requirements will be assigned to the corresponding mobile agents in order to seek an optimal transaction. The Customer constructs the purchase requirements as follows:

$$J_1 = Req_C^{(1)}, \tag{8}$$

$$J_2 = Req_C^{(2)}, \tag{9}$$

$$\ldots,$$

$$J_t = Req_C^{(n)}. \tag{10}$$

Since these Mobile Agents are prepared for the same purchase plan, the purchase requirements are all equal, i.e.

$$J_1 = J_2 = \ldots = J_t = J_C, \tag{11}$$

where J_C is defined as the current purchase requirement. It includes: (1) *the description of a desired product*; (2) *an expiration date and time-stamp, that implies the valid purchase period*; (3) *the maximum price that is accepted to the Customer*; (4) *a due date for the delivery of the product*; and (5) *an address for the delivery of the product.*

(3) **Constructing Partial Secrets** The Customer will construct some partial secrets, that will be used by some E-Shop in the forthcoming transactions. The details are the followings: The Customer computes

$$\begin{aligned} s_C^{(1)} &= x_C H(J_1, r_C^{(1)}) + k_C^{(1)} \\ &= x_C H(J_C, r_C^{(1)}) + k_C^{(1)} \text{mod } q; \end{aligned} \tag{12}$$

$$\begin{aligned} s_C^{(2)} &= x_C H(J_2, r_C^{(2)}) + k_C^{(2)} \\ &= x_C H(J_C, r_C^{(2)}) + k_C^{(2)} \text{mod } q; \end{aligned} \tag{13}$$

$$\ldots$$

$$\begin{aligned} s_C^{(n)} &= x_C H(J_n, r_C^{(n)}) + k_C^{(n)} \\ &= x_C H(J_C, r_C^{(n)}) + k_C^{(n)} \text{mod } q. \end{aligned} \tag{14}$$

(4) **Equipping Mobile Agents** The Customer will equip these mobile agents with the above public parameters and partial secrets. In detail, the Customer provides each Mobile Agent MA_j $(1 \leq j \leq n)$ with the corresponding tuple

$$\{J_C, E_j(s_C^{(j)}), r_C^j, E_j(ID_C)\}, \tag{15}$$

respectively. Here, $E_j(s_C^{(j)})$ is the ciphertext of the $j-th$ partial private key $s_C^{(j)}$, and $E_j()$ is a specific public key cryptosystem of an E-Shop, to whom the $j-th$ Mobile Agent MA_j will migrate for the purchase plan of the Customer.

D. Mobile Agents Migrating

As soon as the Mobile Agents are equipped with the corresponding tuple defined as Equation (*), the different Mobile Agent will migrate to the different E-Shop to search an optimal purchase. Without loss of generality, we may assume that the i-th Mobile Agent MA_i migrates to the i-th E-Shop ES_i, where $1 \leq i \leq n$. The followings are the details:

(1) **Migrating** The i-th Mobile Agent MA_i migrates with the tuple

$$\{J_C, E_i(s_C^{(i)}), r_C^i, E_i(ID_C)\} \tag{16}$$

to the i-th E-Shop ES_i; where $E_i()$ is the public key encryption algorithm of ES_i; and $E_i(s_C^{(i)})$ is the ciphertext of the i-th partial private key $s_C^{(i)}$ under the public key encryption algorithm $E_i()$ of the i-th E-Shop ES_i.

(2) **Checking Time-stamp** After the Mobile Agent MA_i arrives at the ES_i, the E-Shop ES_i gets the tuple

$$\{J_C, E_i(s_C^{(i)}), r_C^i, E_i(ID_C)\} \tag{17}$$

and checks whether the *purchase requirement* J_C is *legal* or not. That is, the i-th E-Shop will examine whether the time-stamp on J_C is valid. If it is not valid, this E-Shop will stop, since this *purchase request* is out of date. If it is valid, this E-Shop will go on the next step.

(3) **Obtaining Partial Secret** After the Mobile Agent MA_i arrives at the ES_i, the E-Shop ES_i gets the tuple $\{J_C, E_i(s_C^{(i)}), r_C^i, E_i(ID_C)\}$ and decrypts $E_i(s_C^{(i)})$ and $E_i(ID_C)$ by using her/his private key corresponding to the encryption algorithm $E_i()$. Consequently, the E-Shop obtains the partial secret $s_C^{(i)}$. She/he will keep $s_C^{(i)}$ secret while making $r_C^{(i)}$ public.

(4) **Checking** The E-Shop ES_i will check whether the partial secret $s_C^{(i)}$ is valid with respect to the corresponding public parameter $r_C^{(i)}$. She/he checks whether

$$y_C^{H(J_C, r_C^{(i)})} r_C^{(i)} = g^{s_C^{(i)}}. \tag{18}$$

If it is not valid, this E-Shop will stop, since the current purchase plan may be spoiled. If it is valid, this E-Shop will take part in the bidding for the purchase plan of the Customer.

E. Processing Transactions

In this procedure, the i-th E-Shop will first construct her/his own bidding key s_{bid}, by which this E-Shop can bid for the purchase plan initialised by the Customer. She/he will then construct the bidding of her/his goods to this purchase. And then, the i-th Mobile Agent will be equipped with this bidding and return to its owner, i.e. the Customer. Note that the bidding key is kept secret by this E-Shop. The details of this procedure is as follows:

(1) **Constructing Bidding Key** So far, the i-th E-Shop holds some parameters produced by the Trusted Third Party as well as the Customer. This E-Shop will first computes her/his bidding key as s_{bid},

$$s_{bid} = s_C^{(i)} H(s_{TTP}^{(i)}, ID_c) + s_{TTP}^{(I)} \text{mod } q. \tag{19}$$

And then, she/he computes y_{bid},

$$\begin{aligned} y_{bid} &= g^{s_{bid}} \text{mod } p \\ &= g^{s_C^{(i)} H(s_{TTP}^{(i)})} g^{s_{TTP}^{(i)}} \text{mod } p. \end{aligned} \tag{20}$$

In the end, the i-th E-Shop makes y_{bid} public while keeping s_{bid} secret.

(2) **Proposing the Bid** According to the purchase requirement J_C, the i-th E-Shop proposes the corresponding bid for J_C. This bid is defined as B_{bid}. And B_{bid} includes: (1) the description of the i-th E-Shop's goods; (2) the minimum price that will be acceptable to the i-th E-Shop; (3) a due date for the delivery of the goods; (4) a bank account number provided by the i-th E-Shop; (5) a due date for transferring money into the bank account; (6) an expiration date and time-stamp, that implies the valid period of the bid B_{bid}.

(3) **Signing the Bid** In order to make this bid confirmed and accepted by the Customer, the i-th E-Shop will put a legal signature on the bid B_{bid}. This will not only help the i-th E-Shop improve the possibility of the Customer accepting this bid, but also help the Customer to verify whether this bid is really from the i-th E-Shop, as well as prevent the i-th E-Shop from denying providing this bid for the purchase plan. The details of this procedure is as follows:

- The i-th E-Shop computes m,

$$m = H(B_{bid}, ID_C, n_S^{(i)}); \tag{21}$$

- The i-th E-Shop chooses a random number k, $k \in Z_q^*$, and sets

$$\alpha = (g^k \text{mod } p) \text{mod } q; \tag{22}$$

- The i-th E-Shop computes β,

$$\beta = k^{-1}(H(m, \alpha, n_S^i) + s_{bid}\alpha) \text{mod } q. \tag{23}$$

Therefore, the signature on the bid B_{bid} is $\{\alpha, \beta\}$.

(4) **Arranging MA to Return** The i-th E-Shop equips the i-th Mobile Agent MA_i with the tuple:

$$B_{bid}, r_C^{(i)}, n_S^{(i)}, ID_C, J_i, \alpha, \beta. \tag{24}$$

This tuple represents the whole transaction. The i-th Mobile Agent then returns to its owner, i.e. the Customer.

F. Checking Transactions

As soon as the i-th Mobile Agent returns to the Customer, the Customer first checks the transaction tuple, and then decides whether to accept this bid. The followings are the details:

(1) The Customer first checks whether $J_i = J_C$. If it holds, she/he continues the next steps. Otherwise, she/he will arrange the j-th Mobile Agent MA_j (where $1 \leq j \leq n$ and $j \neq i$) to seek an optimal bid for the current purchase plan.

(2) The Customer computes $r_1 = H(m, n_S^{(i)}, \alpha)\beta^{-1} \text{mod } q$.

(3) The Customer computes $r_2 = \alpha\beta^{-1} \text{mod } q$.

(4) The Customer verifies whether the following equation holds

$$(g^{r_1} y_{bid}^{r_2} \text{mod } p) \text{mod } q = \alpha.$$

If it holds, the Customer accepts this bid as valid. If it does not hold, the Customer will arrange the j-th Mobile Agent MA_j (where $1 \leq j \leq n$ and $j \neq i$) to seek an optimal bid for the current purchase plan.

G. Auditing i-th E-Shop

The following scenario may take place: After verifying the transaction tuple, the Customer accepts the bid B_{bid} as an optimal bid. Therefore, she transfers some money as the price listed in the bid. However, the i-th E-Shop denies ever receiving any money and sending any bid. How can we deal with this situation? Who will audit the i-th E-Shop? The details given below provides a solution to this scenario.

(1) The Customer sends the tuple $\{\alpha, n_S^{(i)}, \beta\}$ (which is from the whole transaction tuple $B_{bid}, r_C^{(i)}, n_S^{(i)}, ID_C, J_i, \alpha, \beta$.) to the Trusted Third Party.

(2) The Trusted Third Party replies the tuple $\{ID_S^{(i)}, k_S^{(i)}\}$ to the Customer.

(3) The Trusted Third Party audits the i-th E-Shop by using the following equation:

$$H(ID_S^{(i)}, R_i, k_S^{(i)}) = n_S^{(i)}.$$

Since the Trusted Third Party holds $n_S^{(i)}$ and $k_S^{(i)}$, the i-th E-Shop will be identified and audited.

IV. Construction Analysis and Security Proofs

This paper has presented a new electronic commerce protocol for transactions using mobile agents. And a trusted third party is involved in the proposed protocol. It is interesting to analyze how the protocol works. Most importantly, security of the protocol should be maintained, since the transactions are initiated over the Internet. And Internet is a site where there exist a number of attacks, from passive attacks to active attacks, from external attacks to internal attacks [16], [19].

A. Construction Analysis

Generally speaking, construction analysis serves as a functional deloyment from the construction, operationability, and functioning points of view. This subsection will provide a deployment for the proposed transaction protocol.

In our protocol, we have introduced a customer, a trusted third party, an E-shop, and a number of mobile agents. However, in a virtual electronic commerce environment, there will be more than one customer as well as more than one E-shop. For the complex scenario, it is easy to extend the proposed protocol to a multiple level of electronic commerce transactions protocol. Therefore, in the following we only deploy the protocol from the simple and concise perspective.

(1) Role of the Customer: The customer first proposes a *purchase plan*. Around the purchase plan, she constructs the purchase requirements

$$J_1 = J_2 = \ldots = J_t = J_C, \tag{25}$$

which direct the underlying E-shops to bid for the purchase plan. Here, J_C includes: (1) *the description of a desired product*; (2) *an expiration date and time-stamp, that implies the valid purchase period*; (3) *the maximum price that is accepted to the Customer*; (4) *a due date for the delivery of the product*; and (5) *an address for the delivery of the product*.

Also, the customer constructs mobile codes

$$\{J_C, E_j(s_C^{(j)}), r_C^j, E_j(ID_C)\}, \tag{26}$$

for the mobile agents. Note that a valid signature on the bid includes J_C. That is, *J_C is used to restrict the context of the bidding taken by the E-shops*. Other parts of the mobile code, i.e.

$$\{E_j(s_C^{(j)}), r_C^j, E_j(ID_C)\}$$

is used to generate the bidding key for the E-shops.

Another duty of the customer is she will verify the bids

$$B_{bid}, r_C^{(i)}, n_S^{(i)}, ID_C, J_i, \alpha, \beta. \tag{27}$$

returned by the mobile agents. If it is valid, she will transfer some money to the E-shop's bank account.

(2) Functioning of the Mobile Agents: The main duty of the mobile agents is to help its owner accomplish the purchase plan. They actually interact with their owner and the E-shops, respectively. (As noted in Remark 1, We know that the E-shops are also some mobile agents.) For the interaction between the mobile agents and their owner, the mobile agents are equipped with some mobile codes:

$$\{J_C, E_j(s_C^{(j)}), r_C^j, E_j(ID_C)\}, \tag{28}$$

where $1 \leq j \leq n$. For the interaction with the E-shops, the mobile agents transport some bids:

$$B_{bid}, r_C^{(i)}, n_S^{(i)}, ID_C, J_i, \alpha, \beta. \tag{29}$$

(3) Role of the TTP: A trusted third party is involved in the protocol. TTP has two different roles: one is to record the registration of the E-shops, and help the E-shops generate the bidding keys . In order to fulfil this, the TTP sends the tuple

$$\{n_S^{(i)}, s_{TTP}^{(i)}, r_{TTP_i}\}$$

to each E-Shop ES_i $(1 \leq i \leq n)$ through a secure channel, respectively. Here, $s_{TTP}^{(i)}$,

$$s_{TTP}^{(i)} = x_{TTP}H(n_S^{(i)}), r_{TTP_i}) + k_{TTP_i}\text{mod } q. \tag{30}$$

The other role of TTP is to audit the E-shops during the course of the transactions. This service is accomplished using the following equation:

$$H(ID_S^{(i)}, R_i, k_S^{(i)}) = n_S^{(i)}.$$

(4) Role of the E-shops: The E-shops take part in bidding for the purchase initiated by the customer. Therefore, The E-shops need to have bidding private key and public key: s_{bid} and y_{bid},

$$s_{bid} = s_C^{(i)}H(s_{TTP}^{(i)}, ID_c) + s_{TTP}^{(I)}\text{mod } q. \tag{31}$$

and

$$\begin{aligned} y_{bid} &= g^{s_{bid}}\text{mod } p \\ &= g^{s_C^{(i)}H(s_{TTP}^{(i)})}g^{s_{TTP}^{(i)}}\text{mod } p. \end{aligned} \tag{32}$$

B. Security Proofs

This subsection, we will prove that the proposed transaction protocol satisfy the following security properties: (1) strong unforgeability of any bid of the underlying E-shops. This property is valid with respect to the customer. (2) *fair identifiability* of the underlying E-shops. This property is valid with respect to the E-shops. (3) verifiability of the bid of the underlying E-shops. This property is valid with respect to any one who holds the related public parameters. (4) strong undeniability of the bid in the transactions. This property is valid with respect to the E-shops. The details are the followings:

(1) Strong unforgeability of any bid of the underlying E-shops. This property is valid with respect to the customer. This means that the customer is not able to forge valid any bid on behalf of any underlying E-shop. From Equation (3) and (31), we have

$$\begin{aligned} s_{bid} &= s_C^{(i)}H(s_{TTP}^{(i)}, ID_c) + s_{TTP}^{(I)}\text{mod } q \\ &= (s_C^{(i)}H(s_{TTP}^{(i)}, ID_c) + x_{TTP}H(n_S^{(i)}), r_{TTP_i}) + k_{TTP_i})\text{mod } q. \end{aligned} \tag{33}$$

It is difficult to figure out the value of s_{bid}, since k_{TTP_i} and x_{TTP} are two random and private elements of Z_q^*. If the customer tries to tackle Equation (20), she will need to solve the discrete logarithm problem [16]. On the other hand, from Equation (22) and (23), the underlying bidding signature is based on the DSS [18]. Therefore, the strong unforgeability is maintained.

(2) *Fair Identifiability* of the underlying E-shops. This property is valid with respect to the E-shops. Fair identifiability means that no one is able to identify the underlying E-shop whose bid is accepted by the customer. An exceptional situation is the trusted third party can identify the underlying E-shop through the pseudonym. This only takes place when the E-shop denies ever bidding and receiving money in the transactions. In fact, from the signature generated by the E-shop

$$B_{bid}, r_C^{(i)}, n_S^{(i)}, ID_C, J_i, \alpha, \beta,$$

any one except cannot identify the underlying E-shop. This is because: (a) B_{bid} ={the description of the underlying E-Shop's goods; the minimum price that will be acceptable to the underlying E-Shop; a due date for the delivery of the goods; a bank account number provided by the underlyinig E-Shop; a due date for transferring money into the bank account; an expiration date and time-stamp.} It does not leak any information of the identity for the underlying E-shop. and (b) $n_S^{(i)} = H(ID_S^{(i)}, R_i, k_S^{(i)})$. Therefore, ID_S^i is mapped using a hash function.

(3) Verifiability of the bid of the underlying E-shops. This property is valid with respect to any one who holds the related public parameters. Verifiability means that any one who holds the related public parameters can check whether a bid is valid. It is easy to conclude this point from the process of Checking Transactions (see Section 3. F).

(4) Undeniability of the bid in the transactions. This property is valid with respect to the E-shops. Undeniability means that the underlying E-shop cannot deny she ever generated a valid signature on the bid. In fact, from Equation (29) we know that n_S^i is theoretically linked to this E-shop. More importantly, the verifying equation $(g^{r_1}y_{bid}^{r_2}\text{mod } p)\text{mod } q = \alpha$ implies this E-shop ever generated the signature on the bid. This point is derived from the procedure of Processing Transactions as well as Checking Transactions.

V. Performance Analysis

The performance of the proposed electronic commerce protocol can be discussed from two aspects: off-line workloads and on-line workloads.

The off-line workloads mainly include the computation cost. The procedures of System Setup, Preparing Mobile Agents, and Processing Transactions can be all dealt with through tne off-line mode. The computation cost is discussed with respect to one customer with one E-shop. The underlying computation costs are dominated by one modular exponentiation computation, one hash function computation, and two encryption computations for the procedure of System Setup; one modular multiplication, one modular exponentiation, one hash function evaluation for the procedure of Preparing Mobile Agents; one modular exponentiation, one modular inversion, one hash function evaluation, one modular multiplication for the procedure of Processing Transactions.

The on-line workloads also mainly include the communication cost and the computation cost. The procedures of Interaction between E-shops and TTP, Mobile Agents Migrating, and Checking Transactions as well as Auditing i-th E-shop can be all dealt with through the on-line mode. We discuss the on-line workloads with respect to one-time successful transaction between the customer and the underlying E-shop. The communication cost is one round of communication between the E-shop and the TTP, one round of communication between the underlying mobile agent and the E-shop (resp. the Customer), and one round of communication between the customer and the TTP. The corresponding computation costs are dominated by one modular exponentiation, one hash function evaluation, one hash evaluation, one modular multiplication, two modular exponentiations for the procedure of Interaction between E-shops and TTP; two modular exponentiations for the procedure of Mobile Agents Migrating; one modular inversion evaluation, one hash function evaluation, three modular multiplications, two modular exponentiations for the procedure of Checking Transactions; one hash function evaluation for the procedure of Auditing i-th E-shop.

VI. Conclusion

This paper has proposed a new electronic commerce protocol. The proposed protocol integrates mobile agents with the underlying transactions. The mobile agents help to accomplish the purchase plan initiated by the customer. A trusted authority is integrated and plays two important different roles: one is help the E-shops register; the other is help to maintain the fair privacy. We have provided proofs for construction and security.

Acknowledgment

The authors would like to thank the anonymous reviewers.

References

[1] W. Farmer, J. Gutmann and V. Swarup, *Security for Mobile Agents: Authentication and State Appraisal.* Proc. of the European Symposium on Research in Computer Security (ESORICS), LNCS 1146, Springer-Verlag, pp.118-130, 1996.

[2] S. Han, E. Chang and T. Dillon, *Secure e-Transactions using Mobile Agents with Agent Broker* To appear in the Proceedings of IEEE ICSSSM.

[3] Jon C. Graff, *Cryptograhpy and E-commerce,* A Wiley Tech Brief, Wiley Computer Publishing, 2001.

[4] S. Han and E. Chang, *A secure strong proxy signature scheme based on DSS* To appear in the Proceedings of HPCC.

[5] P. Kotzanikolaous, M. Burmester and V. Chrissikopoulos, *Secure Transactions with Mobile Agents in Hostile Environments.* ACISP 2000, LNCS 1841, Springer-Verlag, pp.289-297, 2000.

[6] P. Kotzanikolaous, G. Katsirelos and V. Chrissikopoulos, *Mobile Agents for Secure Electronic Transactions.* Recent Advances in Signal Processing and Communications, World Scientific and Engineering Society Press, pp.363-368, 1999.

[7] S. Kim, S. Park, and D. Won, *Proxy Signatures, Revisited.* Proc. of ICICS'97, Y. Han et al(Eds.), LNCS 1334, Springer-Verlag, pp. 223-232, 1997.

[8] B. Lee, H. Kim and K. Kim, *Secure Mobile Agent Using Strong Non-designated Proxy Signature.* ACISP 2001, Springer-verlag, LNCS 2119, pp.474-486, 2001

[9] B. Lee, H. Kim and K. Kim, *Strong Proxy Signature and its Applications.* Proc. of SCIS2001, pp. 603-608, 2001.

[10] S. Loureio and R. Molva, *Privacy for Mobile Code.* Proc. of Distributed Object Security Workshop OOPSLA'99, 1999.

[11] J. Merwe and S.H. Solms, *Electronic Commerce with Secure Intelligent Trade Agents,* Proc. of ICICS'97, Y. Han et al(Eds.), LNCS 1334, Springer-Verlag, pp.452-462, 1997.

[12] R. Otomura, M. Soshi, and A. Miyaji, *On Digital Signature Schemes for Mobile Agents,* Proc. of SCIS2001, pp. 851-855, 2001.

[13] H. Petersen and P. Horster, *Self-certified Keys - Concepts and Applications,* Proc. Communications and Multimedia Security'97, pp. 102 - 116, Chapman & Hall, 1997.

[14] T. Sander and C. F. Tschudin, *Protecting Mobile Agents Against Malicious Hosts,* Mobile Agent Security, LNCS 1419, Springer-Verlag, pp.44-60, 1997.

[15] D. Singelee and B. Prehneel, *Secure e-Commerce using Mobile Agents on untrusted hosts,* COSIC Internal Report 2004.

[16] A.Menezes, P.C.van Oorschot and S.A.Vanstone, *Handbook of applied cryptography,* CRC Press, Boca Raton, 1997.

[17] N. Y. Lee and M. F. Lee, *The security of a stong proxy signature scheme with proxy signer privacy protection,* Applied Mathematics and Computation 161, (2005) pp. 807-812.

[18] The Digital Signature Standard, NIST, 1994.

[19] M. E. Whitman and H. J. Mattord, *Principles of Inforamtion Security,* Second Edition, Thomson Course Technology, 2005.
IEEE Wireless Communications Magazine, IEEE Press, February 2004.