A Reverse Sealed-bid Auction System for Mobile Commerce

Mahendra Pratap Singh and Samrat Kella
Department of Computer Science and Engineering
National Institute of Technology Karnataka, Surathkal, India - 575025
{mahoo15, samrat.kella }@gmail.com

***Abstract* - In recent years, the demand for mobile commerce has increased. Due to this increased demand, mobile devices usage in internet auctions has also increased. In this paper, we propose a reverse sealed-bid auction model using collaborative mobile agents (MoRSAS) which can be used on mobile-based environment. We also proposed a new auction protocol using ECC (Elliptic Curve Cryptosystem) based signcryption scheme which reduces the computational load and communication overhead, providing high security with small key size. In our proposal, Trusted Dealer (TD) is the one who generates auction keys and key shares, also works like registration manager. Our method reduces the network load and executes the auction process efficiently. The proposed protocol satisfies the security requirements of sealed-bid auction protocol, like confidentiality, anonymity, bid privacy etc.**

Keywords - Anonymity, Bid privacy, Mobile agent, Mobile commerce, Reverse sealed-bid auction, Signcryption.

I. INTRODUCTION

With the advent of the Internet, auctions are nowadays widely used for electronic commerce. Many online auction protocols have been proposed for different auctions [1]. More and more auction sites are appearing, such as ebay.com, onsale.com, uBid.com etc. In general, auction protocols come under two categories: open auction and sealed-bid auction [2]. In open auction each participant is aware of others' bid values. English auction and Dutch auction are the auction protocols under open auction category. In sealed bid auctions each bidder is given just one chance to bid, and where he or she does not know the value of other bids. Sealed-bid auction can be divided into two types: First price auction and Second price auction (Vickrey auction). Use of agent technology in online auctions has got several advantages [3]. With the development of agent technology, several agent based online auction systems have been proposed.

Normally, auction can be a normal auction (one seller and many buyers) or a reverse auction (many sellers and one buyer). In normal auction, sellers take the lead in trades, while buyers have no authority except for estimating value. However, in the reverse auction a buyer puts up the request for their desired goods and along with a desired price, and sellers competitively decrease their price until a sale is made. Reverse auction gained much popularity with the emergence of Internet-based auctions. Many reverse auction sites are appearing such as Priceline.com, Youbid.com.au etc. Today, reverse auctions are used by large corporations to purchase raw materials, supplies and services like accounting and customer service. In this paper,
we set Reverse Sealed-bid auction as the target. MoRSAS caters to both first and second price (Vickrey) reverse auctions with full price flexibility.

Due to rapid growth in the usage of mobile phones, the demand for mobile commerce has increased. The consumers who are using their mobile devices to research and browse products and service have grown steadily. Because of this trend, we have proposed a reverse sealedbid auction agent model for mobile commerce using collaborative mobile agents. We also proposed a new auction protocol using ECC based signcryption which incurs much less computational as well as memory overhead compared to other conventional signcryption scheme. ECC can provide high security with small key size. In our protocol, we employed Shamir's threshold secret sharing scheme [4] to the achieve bid privacy. Our method makes the online auction system efficient and secure.

The remainder of this paper is as follow: Section II represents the previous approaches and section III presents the explanation of the different types of cryptographic schemes used. Section IV which focuses on the proposed Reserved Sealed-Bid Auction Model. Section V presents the security analysis of the proposed method and section VI presents the implementation and results. Section VII presents the conclusion.

II. RELATED WORK

In English auction, the bidder who places the highest bid is the winner and has to pay his/her bid value. At Dutch auction auctioneer sets a reserved price and then lowers the price until he gets a bid. In first price sealed-bid auction each bidder submits a single bid before a deadline without seeing others' bids. The highest bidder wins the auction and pays his/her bid. Similarly, in second price sealed-bid auction (Vickrey) the winner pays the price of second highest bid.

Many auction sites have solutions that offer a convenience to the users. eBay, for instance, uses a reserve-price auction method which allows the user to enter a reserve price. As long as the auction is open and the user's reserve price has not been reached, the agent bids the minimum amount necessary to become the highest bidder. However, this limits the user's choice of bidding strategy without bid privacy and may involve taking into account the effect of the 'winner's curse'. The winner's curse is the difference between the amount the winner paid and the next lower bid. If the bidder bids the perceived valuation of the item and wins, the bidder will know that he/she paid too much because others valued the item less. This problem can be solved using the agent allows the user to coordinate bids across multiple auctions automatically and select a bidding strategy [5]. Generally bid privacy is a desired property in

auction schemes. Franklin and Reiter [6] were among the first to address electronic auction with bid privacy. They achieved many basic requirements of auctions using combined cryptographic primitives such as secret sharing, digital cash and multicasts, and introduced their own primitive called ''verifiable signature sharing''. There are few publications which address the sealed-bid auctions.

Agents facilitate several auction types. Nomad [5], Magnet [7], MoCAAS [8], MoRAAS [9] and MoRVAM [10] are auction agent systems using a mobile agent mechanism. A mobile agent has the unique ability to transport itself from one system to another. This ability allows mobile agents to execute asynchronously and autonomously. Also, the mobile agents communicate with one another. Because of this ability, the auction agent using a mobile agent is smarter than the reserve auction agent. In agent based auction, bidder creates a bid agent to place bid. In case of open auctions bid agent places new bids according to the current bid price. Also the bid agents need to monitor the bidding period. But in case of sealed-bid auction bid agents has to place a single bid without the knowledge of others' bid. The bid agents need not to monitor bidding period as in open auction. So, bidder can directly place the bid rather than creating a bid agent for bidding which reduces infrastructure of the system. However, substituting auctioneer with a mobile agent is very useful in any type of auction. The above discussion remains same in case of reverse auctions also.

Designated bidding is one form of reverse auction. In Designated bidding, auctioneer nominates a bidder based on the quality of their work. But this mechanism increases the probability of collusion, because the number of bid participants is restricted [11][12]. In theory the open bidding auction mechanism is better than the designated auction mechanism [13]. However, since buyers can solicit nominations via Internet, sellers can maintain collusion. Thus, we considered the designated auction mechanism in our protocol. The reverse extended vickrey auction (REV) protocol is one case of designated bid reverse auction. In REV auction [14] a buyer selects sellers who have substitute goods and the buyer's preferred goods. The nominated sellers submit sealed bids.

3. Cryptographic Schemes Used

Here, we explain the cryptographic schemes that we have employed in our protocol as follows.

3.1. Shamir's Threshold Cryptosystem

Threshold cryptosystem was first invented by Shamir [4] in 1976. In shamir's secret sharing scheme, a secret key S is shared among n participants such that

- S can be computed with the knowledge of any t or more shares.
- S cannot be determined with knowledge of t-1 or fewer shares.

In the Shamir's secret sharing scheme, a trusted dealer randomly selects (t-1) number of coefficients $a_1, a_2, ..., a_{t-1}$ from a finite field, F_p where p is a prime number and generates the polynomial $f(x)$ as

$$f(x) = s + \sum_{i=1}^{t-1} a_i \cdot x_i$$

where $f(0) = S$ is the secret key selected by the trusted dealer. The dealer computes the n shares $(x_1, y_1),....., (x_n, y_n)$ as $y_i = f(x_i)$ for unique x_i and (x_i, y_i) values are distributed to n participants. After receiving at least t shares $(x_1, y_1),...., (x_t, y_t)$, one can reconstruct the polynomial $f(x)$ by the Lagranges's interpolation formula as

$$f(x) = \sum_{i=1}^{t} y_i \left(\prod_{j=1, j\neq 1}^{t} \frac{x - x_j}{x_i - x_j} \right)$$

and recovers the secret key, S as $S=f(0)$

3.2. ECC based Signcrytion

In general, authenticity and confidentiality are achieved by digital signature followed by encryption. But the current method of signature then encryption consumes much computational power and the network bandwidth. As computational and communication overheads are becoming serious issues in today's various applications, a new paradigm called signcryption in public key cryptography has been evolved. It was first proposed by Zheng [15] in 1997. A signcryption scheme consists of two algorithms: (1) Signcryption algorithm, (2) Unsigncryption algorithm. Signcryption scheme fulfils the requirements of unforgeability, confidentiality, non-repudiation with lower cost compared to signature then encryption [16]. A signcryption scheme [17] has been implemented with elliptic curve cryptography where it has been shown that the scheme can save 58% in computational cost and 40% in communication overhead compared to signature then encryption scheme.

Elliptic Curve Cryptography (ECC) was first proposed by Neal Koblitz [18] and Victor Miller [19] in 1985. The ECC is able to improve the existing cryptogram systems in terms of having smaller public-key certificates, lower bandwidth usage, etc. [20]. It can provide high security with smaller key sizes. The security of ECC is based on Elliptic Curve Discrete Logarithm Problem (ECDLP) [21][22][23]. ECDLP can be defined as follows: given an elliptic curve E defined over F_p, a point P $\in$ (F_p) of order q, and a point Q$\in (F_p)$, determine the integer k, $0 \leq k \leq$ p- 2, such that Q = k.P , provided that such an integer exists. It is very difficult to find k; even the values of P and Q are known before.

Thus, we have used a simple ECC based signcryption scheme [24] in our proposed protocol. This scheme requires a trusted dealer TD which is resposible for generating parameters. TD choses a secure elliptic curve (E) over finite field F_p is chosen where p is a prime number and its base point is G of order q (where $q \geq$160 bits) . We consider that

Alice sends the message m to Bob through the signcryption scheme. Alice's private key d_A is chosen randomly from [1, $q-1$] and its corresponding public key is Q_A where $Q_A = d_A.G$ which is a point on E. Similarly, Bob's private key d_B is chosen randomly from [1, $q-1$] and its corresponding public key is Q_B where $Q_B = d_B.G$ which is a also point on E.

Signcryption algorithm:

Step-1 :

Alice chooses a random integer, $k \in [1, q-1]$ per each signcryption session and computes

$Y_A^1 = k.G = (x_1, y_1)$ and $Y_A^2 = k.Q_B = (x_2, y_2)$ where x_1, x_2 are the x−coodinates and y_1, y_2 are the y−coordinates of the corresponding points on E.

Step-2 :

Alice computes $r = m.x_2 \bmod q$ and $s = k - d_A.r \bmod q$.

Step-3 :

The signcrypted message (r, s, Y_A^1) is sent to Bob through public channel by Alice. It is evident that the parameter r includes the message m while the parameter s includes the signature of

the sender Alice.

Unsigncryption algorithm:

After receiving the message (r, s, Y_A^1), Bob verifies its validity and recovers the message m by following steps.

Step-1: He computes $Y_B^1 = r.Q_A + s.G = (x_3, y_3)$ and $Y_B^2 = d_B$. $Y_B^1 = (x_4, y_4)$ where x_3, x_4 are the x−coordinates and y_3, y_4 are the y−coordinates of the corresponding points on E.

Step-2: Bob verifies whether Y_A^1 matches with Y_B^1 or not. If it matches, the signcrypted message (r, s, Y_A^1) is valid, otherwise it is invalid.

Step-3: If the signcryption message is valid, then Bob recovers the message m by $m = r.(x_4)^{-1} \bmod q$.

It can be proved that

$Y_B^1 = r.Q_A + s.G = r.(d_A.G) + (k - d_A.r).G = k.G = Y_A^1$.

Thus the validity of the signcrypted message (r, s, Y_A^1) can be verified by the condition

$Y_A^1 = Y_B^1$. Again, it can be shown that

$Y_B^2 = d_B.Y_B^1 = d_B.Y_A^1 = d_B.(k.G) = k.(d_B.G) = k.Q_B = Y_A^2 = (x_2, y_2) = (x_4, y_4)$

Now, we know that $r = m.x_2 \bmod q = m.x_4 \bmod q$. So, the message $m = r.(x_4)^{-1} \bmod q$.

This signcryption scheme preserves the security features properly like unforgeability, confidentiality, non-repudiation and forward secrecy.

4. Proposed Reverse Sealed-bid Auction Model

In order to achieve the auctioneer's (buyer) mobility on interment auction, our system is inherited and proposed from MoCAAS [8]. Proposed model consists of four main components: (1) Trusted Dealer (TD) (2) Buyer agent (3) Broker agent and (4) Seller (Mobile Device). TD is certified by Certification Authority (CA). TD is responsible for generating auction keys and key shares, also works like registration manager. Anyone who wants to participate in the auction or conduct an auction has to register with TD. TD verifies registration details and assigns a unique identification number (UID). After successful registration, he/she can participate in auction or conduct an auction. Any mobile user who wants to participate in the auction or conduct an auction has to register with TD. TD verifies registration details and assigns a unique identification number (UID). After successful registration, he/she can participate in auction or conduct an auction. A mobile user who wants to make purchase connects to a BuyApplication which is hosted in a server in the fixed network and sends information about the product, which the user wants, like its features, the desired price and the maximum price to offer. A mobile user who wants to sell goods connects to a SellApplication which is hosted in a server in the fixed network and registers with broker agent. As soon as buyer agents have been created, they negotiate with the selected sellers which are recommended by the broker agent. At the end of auction, buyer agent sends the auction results to the user.

The architecture of MoRSAS is shown in Figure 1. The buyer-agent offer interfaces for specifying agents, querying the broker-agent. An interface for specifying agents sends a request for a generated buyer-agent to the buyer agent creator. The buyer-agent creator creates the buyer-agent from a template and registers the buyer-agent with the broker-agent. An interface for querying broker-agent shows the recommended sellers list and the expected goods.

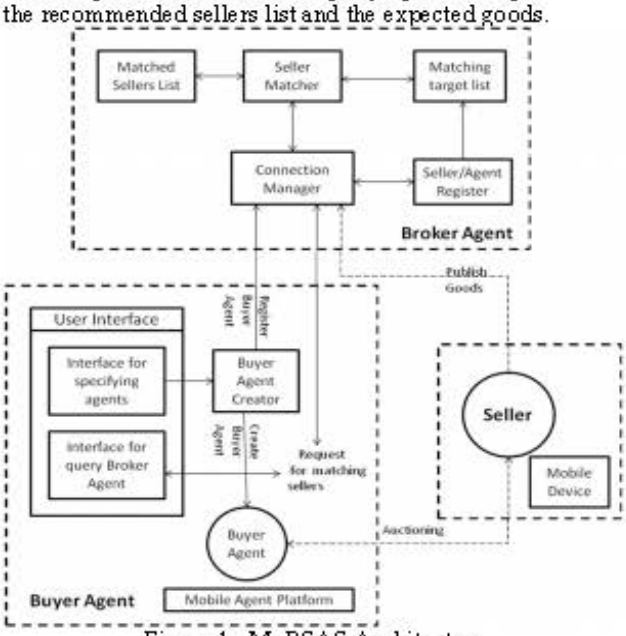

Figure 1. MoRSAS Architecture

The broker-agent matches the buyers and the sellers. A connection manager forwards messages to an agent/seller register or a seller matcher. If the message comes from the buyer agent and the message is a query for recommending the sellers, the connection manager forwards the message to the seller matcher. If the message comes from the buyer-agent or the seller and the message is a request for registration, the connection manager forwards the message to the agent/seller register. The agent register registers agents with the matching target list. The agent/seller register registers agents or sellers with the matching target list. The agent matcher matches a buyer-agent and seller. It inserts a matched pair into the matched pair list. Finally, buyer agent requests the designated sellers to participate in the auction.

The buyer agent and sellers collaborate with each other in order to execute an auction. Figure 2 presents entire workflow of MoRSAS. When a new is auction created, (1) a seller must publish his/her goods by registering it with a broker agent. (2) Buyer agent submits the data received from the buyer to the broker agent. (3) The buyer agent requests the broker agent for matching sellers. (4) Then the broker agent searches for a recommendable sellers and returns the results to the buyer agent. (5) The buyer agent informs the buyer, buyer selects sellers recommended by the broker agent. (6) The buyer agent requests all the designated sellers for bidding. (7) The sellers grant the request of the buyer agent. (8) Finally, buyer agent starts an auction process which will take place with our proposed auction protocol.

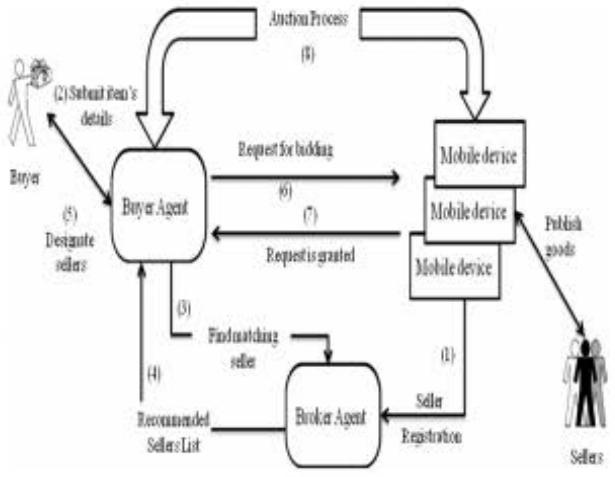

Figure 2. MoRSAS workflow

In our model, we have proposed a new auction protocol which includes five phases: Setup Phase, Auction Initialization Phase, Bidding phase, Opening Phase, Winner announcement Phase. The three participants in the protocol are Trusted Dealer, Buyer (Auctioneer), and Seller. It manages and maintains the bulletin board, which is called BB_{TD}. Only the TD has the authority to write and update the board. Buyer agent (Auctioneer) also maintains a bulletin board, which is called BB_A. Only the buyer agent has the authority to write and update the board. Every auction holds a unique identification number AUC_{id}.

4.1. System Parameters

The system parameters of MoRSAS are given in Table 1.

Table 1. System Parameters.

p	A big prime number;
q	A big prime number; q is the order of a generative point on an elliptic curve and its value is within $(p+1+2\sqrt{p}, p+1-2\sqrt{p})$;
E	Elliptic curve equation $y^2 = x^3+ax+b(mod\ p)$, where a, b are real numbers and satisfy $4a^3+27b^2\ mod\ p \neq 0$;
G	A generative point on an elliptic curve with order as q;
P	A point on an elliptic curve;
x_1	The value of the x coordinate of point P on the elliptic curve;
y_1	The value of the y coordinate of point P on the elliptic curve;
$H(x)$	A cryptographic one-way hash function;
Q_{TD}, d_{TD}	TD's public key and private key,
S_i	The i^{th} seller;
$bid_{i,j}$	A bid value that is placed by S_i in j^{th} round of auction ;
$Q_{A,j}$, $d_{A,j}$	Auction public key and private key in j^{th} round of auction;
$Q_{s,j}$, $d_{s,j}$	Seller's Public and Private key shares in j^{th} round of auction;
$Q_{b,j}$, $d_{b,j}$	Buyer agent's Public and Private key shares in j^{th} round of auction;
S_{id}, A_{id}	Unique Identification Number assigned by TD;
k_i	Secret parameter selected by S_i;
$Y_{i,j}$	A pseudonym generated by TD for S_i in j^{th} round of auction;

4.2. Setup Phase

Step1: TD chooses a secure elliptic curve E over finite field Fp where p is a prime number, base point G of order q (where $q \geq 160$bits).

Step2: TD chooses its private key $d_{TD} \in [1, q-1]$ and corresponding public key $Q_{TD} = d_{TD} \cdot G$.

Step3: TD publishes p, q, G, Q_{TD}.

4.3. Auction Initialization Phase

Buyer chooses, through buyer agent, n sellers. Buyer agent notifies TD that n members take place in this auction. TD chooses a threshold value t based on n value. Before auction

starts, TD posts the AUC_{id} and auction rule on BB_{TD}. TD generates pseudonym, auction keys and key shares for each auction round.

4.3.1 Pseudonym Generation

Before j^{th} round of auction starts, TD would generate a pseudonym ($Y_{i,j}$) for every bidder S_i. All pseudonyms would be posted on BB_{TD}.

Step1: Seller randomly selects an integer $k_i \in [1, q-1]$ as secret parameter and computes the verification information as follows.

$$P = k_i \cdot G = (x, y)$$
$$h = H(x \| y)$$

Step1: Seller sends the information $\{k_i, h\}$ through a secure channel to TD.

Step2: TD checks the validity of $\{k_i, h\}$ by the following equation.

$$P_i = k_i \cdot G = (x_i, y_i)$$
$$h_i = H(x_i \| y_i)$$
$$h_i \stackrel{?}{=} h$$

Step3: TD stores the k_i and generates a pseudonym for S_i using the following equation.

$$Y_{i,j} = H(k_i \| AUC_{id} \oplus S_{i,id} \| j)$$

The pseudonyms would be posted on BB_{TD}. S_i can verify his pseudonym using above equation. If S_i dose not find his/her pseudonym on BB_{TD}, he/she can appeal to TD.

4.3.2 Generation of Auction Keys and Key Shares

TD generates auction keys and key shares for j^{th} round of auction as shown below:

Step1: TD generates auction public key $Q_{A,j}$ and private key $d_{A,j}$. It chooses random integer $d_{A,j}$ from [1, q-1] and computes corresponding public key $Q_{A,j} = d_{A,j} \cdot G$.

Step2: It chooses a temporary UID (t_{id}) and generate a unique ID $id_{i,j}$ for each bidder S_i as $id_{i,j} = (S_{i,id} \oplus t_{id})$. TD uses $id_{i,j}$ for generating the key share of each S_i.

Step3: It generates a (t -1) degree secret polynomial as $f(x) = a_0 + a_1 \cdot x + \ldots + a_{t-1} \cdot x^{t-1}$ where $a_0 = f(0) = d_{A,j}$. The coefficients $a_1, a_2, \ldots, a_{t-1}$ are randomly selected from finite field Fp.

Step4: Finally, TD computes the private key shares for every seller Si and buyer agent from the above polynomial.

- For S_i, $d_{i,j} = f(id_{i,j})$ and corresponding public key share $Q_{i,j} = d_{i,j} \cdot G$.
- For Buyer agent, $d_{b,j} = f(A_{id})$ and corresponding public key share $Q_{b,j} = d_{b,j} \cdot G$.

TD sends the private key shares securely and posts the $Q_{A,j}$ and public key shares on BB_{TD}.

4.4. Bidding phase

In j^{th} round of auction, each S_i submits the bid through signcryption [16].

Step1: Each seller prepares the bidding information $\{Y_{i,j}, bid_{i,j}\}$. Seller submits bidding information to the buyer agent through signcryption.

Step2: Buyer agent checks the validity of the bids by using the public key shares of the bidders. And, it posts the bidding information on BB_A.

4.5. Opening Phase

In the opening phase, buyer agent constructs the private key and determines the winner for j^{th} round of auction.

Step1: Each seller submits his/her private key share $\{id_{i,j}, d_{i,j}\}$ to the buyer agent through signcryption.

Step2: After receiving more than (t-1) number of shares from the bidders, buyer agent constructs the private key using Lagrange's interpolation formula as described in Section 3.1. The private key is posted on BB_A.

Step3: The buyer agent decrypts the bids and determines the winner according to the auction rule.

4.6 Winner announcement Phase

When j^{th} round of auction ends, buyer agent announces the winner.

Step1: Buyer agent posts the winner's bidding information ($Y_{i,j}$, $bid_{i,j}$) on BB_A.

Step2: If it is last round of the auction, buyer agent sends the $Y_{i,j}$ of the winner to TD through signcryption and gets the details of the winner.

Figure 3 illustrates the proposed auction protocol.

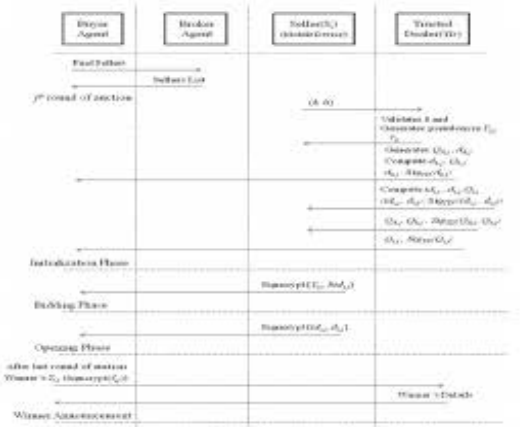

Figure 3. Procedure of proposed auction protocol

4.7 Dispute

If S_i cheats or simply crashes, buyer agent invokes the dispute protocol, which is two-party protocol between buyer agent and trusted dealer. Buyer agent sends the signcrypted message received from the S_i to TD. TD validates the message and conforms the S_i's deviation. If the conformation is true, TD sends of the key share of the bidder in the j^{th} round of auction. As a result, auctioneer excludes the S_i from bidder's list and can continue the opening phase.

As ECC based signcryption incurs much less computational overhead and able to provide high security with smaller key sizes, the proposed auction protocol makes the online auction efficient and secure. Moreover, the proposed model needs less infrastructure compared to MoRAAS [9], and MoRVAM [10]. As shown in the architecture, Sellers need not create a bid agent in fixed network. Sellers can submit their signcrypted bids from the mobile device itself. The implementation details of the ECC based signcryption scheme are discussed in Section 6.

5. Security Analyses

The desired properties that are required by any electronic sealed-bid auction protocol [25][26] are examined as follows.

1. Correctness: The winning price and winner that are determined according to auction rules should be correct, assuming every party acts honestly.

   Correctness is guaranteed by the buyer agent acting honestly. An honest seller S_i submits his secret share $d_{i,j}$ to buyer agent. After receiving more than (t -1) number of shares, buyer agent constructs the secret key and determines the winner according to the predefined auction rule.

2. Bid-Confidentiality: Bids are not revealed to anybody until auction closes.

   Bids are encrypted using auction public key. Bids are not revealed until the end of the auction. Buyer agent can construct the secret key only after receiving the shares from the sellers.

3. Fairness: The submitted bids cannot be modified. Bidder is unable to deny his bid, after he submits it.

   Bid-Confidentiality is maintained and sellers sign the bids using their private key shares. Non-repudiation is also maintained. No one can change or disclose the bids until the bidding period is closed.

4. Bidder-Anonymity: The bidder's identity cannot be disclosed to anybody throughout the auction.

   Seller submits the bid using his/her pseudonym ($Y_{i,j}$). Buyer agent knows the only $Y_{i,j}$ of the bidder. Buyer agent cannot derive any relationship between the pseudonyms of the same bidder in different rounds. Because, the round number j changes in the calculation of $Y_{i,j}$.

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

   Seller's signature cannot be forged. Even though attacker gets the public key, it will be very difficult to him to obtain secret key, because of the Elliptic Curve Discrete Logarithm Problem (ECDLP).

6. Non-forgeability: No one can forge another one's valid bid price.

   Attackers cannot forge any valid bid information. Because, bidding information is signcrypted with the seller's secret key. Attackers cannot produce a valid signcryption without seller's secret key.

7. Bid-Privacy: The losing bids are not revealed until end of the auction even to the auctioneer. Nobody can access the bids until the end of auction except buyer agent.

   Buyer agent has access to all bids during opening phase of the auction. Thus, Weak bid privacy is achieved.

8. Public verifiability: Anybody can verify the auction outcome.

   All the information required to decide the auction result is posted on the bulletin board (BB_A). Anybody can verify the bidder identity, bid validity and winning bid details using this information.

9. Linkability within a single auction round: In a single auction round, the bidders can repeatedly place new bid and can be recognized by other bidders.

   Within a single auction round, S_i holds the same $d_{s,j}$ to place the bid. Seller's identity and how many times the seller placed the bids can be traced.

10. Unlinkability among various auction rounds: No one will be able to know the same bidder's identity that among different rounds of auction.

    The pseudonym and private key share are different for each auction round. Nobody can know the S_i's relationship with various auction rounds.

11. Efficiency: The protocol has to reduce computation and communication cost for making efficient bidding.

    In our protocol, ECC based signcryption effectively reduces the computation and communication cost of online bidding.

12. One-time Registration: The bidders need to register once and then they can participate in all auctions.

Seller uses his pseudonym to participate in auction. Hence, seller needs to register once with TD.

13. Easy Revocation: Trusted Dealer can easily revoke someone's right to bid.

    TD can easily delete the seller's details from database. Once the information is removed, the seller loses the right to participate in the auction.

14. Robustness: Malicious behaviour of anybody cannot compromise the system. Correctness should be ensured in any case.

    Nobody can pretend to be another bidder due to their signatures and the property of the bulletin board. Corrupt behavior by any participant cannot produce an incorrect outcome. Buyer agent can eliminate the cheating bidders through the execution of dispute protocol. Cheaters cannot make any corruption.

15. Price flexibility: Bidders can bid any value within a range of minimum and maximum biddable prices.

    Bidders can bid on any price. There is no set of prices.

16. Rule flexibility: The protocol is independent of the auction rules.

    Auction can be first-price or second-price auction. Winner and winning price are determined according to the predefined auction rule.

6. Implementation and Results

We have developed the BuyApplication and SellApplication in a J2ME wireless tool kit 2.5.1 [27]. Figure 4 shows the working of these two applications. A buyer submits the item details and desired features through BuyApplication. BuyApplication sends the submitted data to fixed network in order to create the Buyer agent. A seller who is requested to participate in auction starts the SellApplication. Seller gets his/her pseudonym and required keys from TD. Then the seller submits his bid which will be signcrypted and submitted to the buyer agent. After the bidding period, sellers submit their key shares to the buyer agent to continue the opening phase. At the end of auction, buyer agent sends the winner's details to the buyer and 'win' or 'fail' message to the each seller.

The key pair generation, signcryption and unsigncryption algorithms are successfully implemented using random elliptic curve over finite prime field (160 bit & 192 bit) in the J2ME. Table 2 and Table 3 show the performance measurement for key pair generation, signcryption and unsigncryption algorithms on J2ME wireless toolkit 2.5.1.

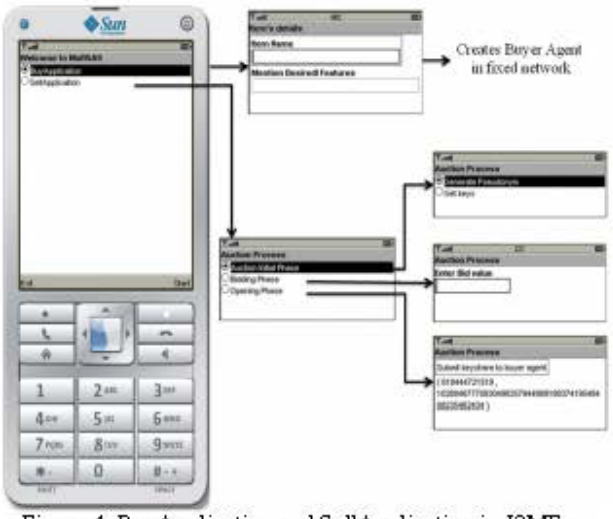

Figure 4. BuyApplication and SellApplication in J2ME.

Table 2. Performance Results (160 bit).

Algorithm	Time Measured in Wireless Toolkit 2.5.1(in milliseconds) for different speeds(bytes code/millisecond)					
	1000	802	600	401	203	100
Key pair Generation	6250	7813	10390	15594	30797	62547
Signcryption	13641	17000	22750	34047	67250	136500
Unsigncryption	50844	63390	84703	126797	250344	508250

Table 3. Performance Results (192 bit).

Algorithm	Time Measured in Wireless Toolkit 2.5.1(in milliseconds) for different speeds(bytes code/millisecond)					
	1000	802	600	401	203	100
Key pair Generation	8110	10156	13547	20250	40047	81230
Signcryption	17703	22000	29453	44047	87578	176500
Unsigncryption	75297	93890	125500	187797	371922	752938

In our implementation, we have taken the standard elliptic curve domain parameters from [28]. The following figures show the performance measurement for key generation, signcryption and unsigncryption algorithms on J2ME wireless toolkit 2.5.1.

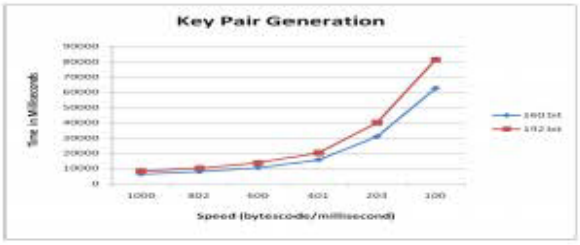

Figure 5. Performance measurement for Key pair generation

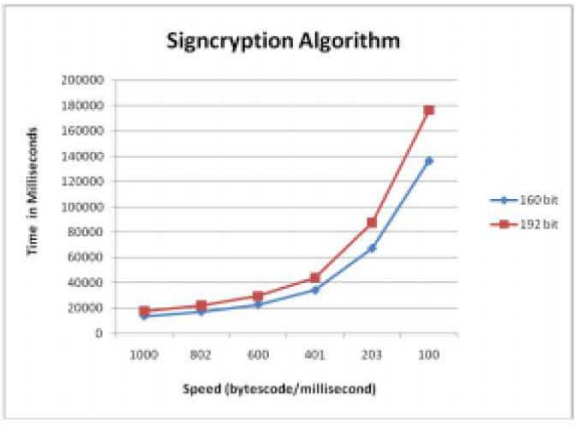

Figure 6. Performance measurement for signcryption.

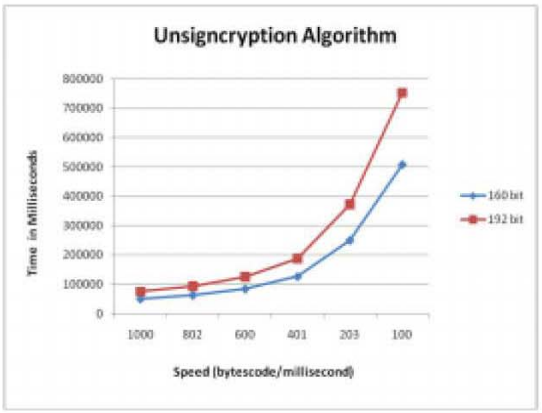

Figure 7. Performance measurement for Unsigncryption.

In f^{th} round of auction, TD generates a secret polynomial of chosen threshold value. From the polynomial, TD computes the shares for the sellers and the buyer agent is shown in Figure 8.

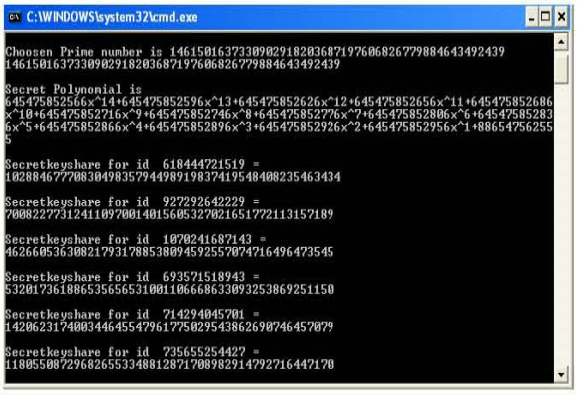

Figure 8. Key shares generation

In the opening phase of the auction, buyer agent has to construct the secrete key using the key shares submitted by the sellers. Buyer agent runs the Lagrange's Interpolation formula in order to construct the secret key. Secret construction is shown in Figure 9.

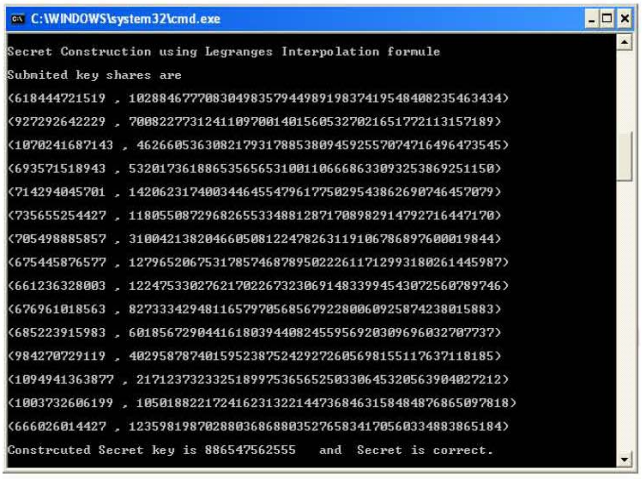

Figure 9. Secret Construction.

7. Conclusions

In this paper, we proposed a reverse sealed-bid auction agent system. A mobile agent mechanism reduces the user operations and network load. Buyer agent efficiently substituted for buyer (auctioneer). Buyer need not to be connected always during the auction. A new auction protocol is proposed using ECC based signcryption scheme which reduces the computational load and communication overhead. We have employed Shamir's threshold secret sharing scheme in our protocol to achieve bid privacy. In the protocol, dishonest bidders can be identified and they are excluded from the auction. The auction protocol makes the online auction secure and efficient on mobile devices.

In our model, buyer side all the compuation is performed in fixed nertwork, by the buyer agent and do not overload the buyer's mobile device. Sellers submit their bids from the mobile device without creating the bidding agent in the fixed network because bids are signcrypted with in mobile device itself. As ECC able to provide high security with small key size, it does not overload the communication channel between the mobile device and the fixed network. Thus, our model needs less infrastructure and excutes the auction process efficiently. The protocol satisfies all the desired properties of sealed-bid auction protocol like anonymity, fairness, bid privacy etc. Furthermore, signcryption and unsigncryption algorithms are implemented on J2ME wireless tool kit 2.5.1. In the future, we would focus on achieving strong bid privacy.

REFERENCES

[1] Passch,Carsten., Song, William., Kou, Weidong., and Tanl,Chung-Jen, (2001) "Online Auction Protocols: A Comparative Study", ELECTRONICS COMMERCE TECHNOLOGIES, LNCS, Vol. 2040, pp. 170-186. Springer, Heidelberg.

[2] McAfee, R. P. and McMillan, J. (1987) "Auctions and Bidding", Journal of Economic Literature, Vol. 25, pp. 699-738.

[3] Guttman, R.H., Moukas, A. G. and Maes, P. (1998) "Agent-mediated electronic commerce: a survey", Knowledge Engineering Review, Vol. 13, No. 2, pp. 147-159.

[4] Shamir,A. (1979) "How to share a secret", Communications of the ACM, Vol. 22, pp. 612-613.

[5] Sandholm, T., and Huai, Q. (2000) "Nomad: mobile-agent system for an internet-based auction house", IEEE Internet Computing, pp. 80-86.

[6] Franklin, M. K., and Reiter, M. K. (1996) "The design and implementation of a secure auction service", IEEE Transactions on Software Engineering, Vol. 22(5), pp. 302–312.

[7] Steinmetz, E., Collins, J., Jamison, S., Sundarewara, R., Mobasher, B., and Gini, M. (1998) "Bid evaluation and selection in the MAGNET automated contracting system", First International Workshop on Agent Mediated Electronic Trading AMET-98, pp. 105-125.

[8] Lee, K. Y., Yun, J. S., and Jo, G. S. (2003) "MoCAAS: auction agent system using a collaborative mobile agent in electronic commerce", Expert systems with applications, pp. 183-187.

[9] Shiha, Dong-Her., Huanga,Shin-Yi., YenA,David C. (2005) "new reverse auction agent system for m-commerce using mobile agents", Computer Standards & Interfaces, Vol. 27, pp. 383-395.

[10] Shiha, Dong-Her., Linb, Binshan., and Huanga,Shin-Yi., (May, 2007) "MoRVAM: A reverse Vickrey auction system for mobile commerce", Expert Systems with Applications, Vol.32, pp. 1113–1123.

[11] McMillan, J. (1991) "Japan's Price-Fixing Conspiracy, Economics and Politics", Vol.3, pp. 201- 218.

[12] Saijo T., Une M., and Yamaguchi T. (1994) "Dango experiments", forth coming in Journal of the Japanese and International Economics.

[13] Baba, Y. Mineika no ookushon(in Japanese) (2000), "Financial Review", Policy Research Institute of the Ministry of Finance Japan.

[14] Matsuo, Tokuro. & Ito, Takayuki. (2002) "A Designated Bid Reverse Auction for Agent-Based Electronic Commerce", Developments in Applied Artificial Intelligence, LNAI, Vol. 2358, pp. 460–469, Springer, Heidelberg.

[15] Zheng, Y. (1998) "Signcryption and its applications in efficient public key solutions", Proceedings of Information Security Workshop (ISW'97), LNCS, Vol. 1397, pp. 291-312, Springer, Heidelberg.

[16] Zheng, Y. (1997) "Digital signcryption or how to achieve cost (signature&encryption) ≤ cost (signature) +cost (encryption)", Advances in Cryptology-Crypto '97 Proceedings, Vol. 1294, pp.165–179. Springer, Heidelberg.

[17] Zheng, Y. and Imai,H. (1998) "How to construct efficient signcryption schemes on elliptic curves", Information Processing Letters, Vol. 68, pp. 227-233.

[18] Koblitz, N. (1987) "Elliptic Curve Cryptosystems. Mathematics of Computation", Vol. 48(177), pp.203–209.

[19] Miller, V.S. (1986) "Use of Elliptic Curves in Cryptography", Williams, H.C. (ed.) CRYPTO 1985, LNCS, Vol. 218, pp. 417–426. Springer, Heidelberg.

[20] Wu, S.T. (2005) "Authentication and Group Secure Communications Using Elliptic Curve Cryptography", Doctoral Dissertation, National Taiwan University of Science and Technology, Taipei.

[21] Scott A. Vanstone. (1997) "Elliptic curve cryptosystem -the answer to strong, fast public key cryptography for securing constrained environments", Information Security Technical Report, Vol. 2(2), pp. 78 -87.

[22] Toorani, M. and Shirazi, A. A. B. (2009) "An elliptic curve-based signcryption scheme with forward secrecy." Journal of Applied Sciences, Vol. 9(6), pp. 1025-1035.

[23] Tan, C. H. (2006) "Analysis of improved signcryption scheme with key privacy", *Information Processing Letters*, Vol. 99(4), pp.135-138.

[24] Changgen, Peng., Xiang,Li., (1998) "Threshold Signcryption Scheme Based on Elliptic Curve Cryptosystem and Verifiable Secret Sharing", *Information Processing Letters*, Vol. 68, p.227-233.

[25] Peng, K., Boyd, C., Dawson, E., and Viswanathan, K. (2003) "Five sealed-bid auction models", *Proceedings of the ustralasian information Security Workshop Conference (AISW 2003)*,Vol 21.

[26] Lee, B., Kim, K., and Ma, J. (2001) "Efficient Public Auction ith One-time Registration and Public Verifiability", Pandu Rangan, C., Ding, C. (eds.*) INDOCRYPT 2001*, LNCS, Vol. 2247, pp.162-174. Springer, Heidelberg.

[27] "Sun Java Wireless Toolkit 2.5.1 for CLDC Download", http://www.oracle.com/technetwork/java/downloa d-2-5-1-138417.html

[28] Certicom, (2000) "Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters", http://www.secg.org/download/aid-386/sec2_final.pdf.