International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 16 (2017) pp. 6257-6266
© Research India Publications. http://www.ripublication.com

Security Boosted Online Auctions Using Group Cryptography

Jogi Priya P M
Research Scholar, Department of Computer Science Engineering,
KAHE, Karpagam University, Coimbatore, India

Dr. Joe Prathap P
Associate Professor, RMD Engineering College Chennai, India.

Abstract

Auctioning items through the Internet is a much prevalent and profit making industry. Auctioning through the Internet has numerous advantages over the traditional face to face offline auctioning systems, the most important being the flexibility offered to the buyers and sellers in terms of time and location. This advantage of online auctioning systems has often been exploited by both the parties to cheat each other. Buyers, who places the bid can trick or cheat by rejecting bids at a later stage, denying or declining payment, or making agreements with fellow bidders to generate negotiated price for the product. Besides, the sellers might decline or abort to deliver the products, or could work up with some manipulations with group of bidders. Duplicate bids or fake bids may also lead to serious problems in the entire online auctioning process. The objective of this paper is to introduce a novel and highly secure online auctions management system using group cryptography and remote supervision.

Keywords: Online auctions; group cryptography; remote supervision; security; secure auction management

INTRODUCTION

Over these years, auctions have been one of the most vital and profitable business in the world, selling different types of products and merchandize with fixed and varying prices (bids). Traditional auctions are restricted to certain locations where bidders and sellers meet physically for negotiations and business. These types of auctions are usually organized to sell unique and extremely rare products like painting, celebrity's properties etc. Physical location constraints have had negative impacts on the auction outcome over these years. Many bidders could not reach the location in time for the bid and many of them were not able to travel physically to the place of the auction. Sometimes, the sellers were unable to get good bids for their products due to this location constraint. The cost of arranging the place for the auction and cost incurred in conducting the auction were two other important issues in traditional auctions.

Since the birth of e-commerce through Internet, auctions online have become much popular, selling goods of all types ranging from eatables to buildings and properties. Online auctions have gained wide popularity with the participation of large number of sellers and buyers. The online auction model works in a very simple way, with the sellers placing the goods for sale through an intermediate online website and the buyers placing corresponding bids to the products they like to buy. The entire auction process is regulated by the intermediate online auction website software. The main thought behind online auctions is to enable the market to determine the exact price of a product. Also the bidders perceive that they have correctly evaluated the products they bid on, and sellers feel that they receive the highest price from the highest bid for the products they sell (Ba *et al*, 2003).

Advantages of online auctions

Online auctions offer numerous advantages compared to the traditional auctioning systems. They are considered more efficient (Albert, 2007) to its predecessor. The major advantages of online auctions are,

- Location flexibility: Buyers and sellers need not come physically to any location for the auctioning process. They can participate in the auction process from anywhere in the world through an Internet connection. This is the most important advantage of online auctions that have made them extremely popular within a short span of time. Buyers and Sellers could save money and time of travel to the place of auctions. A large number of items could be listed for auctions by the sellers from any location using the online software. The buyers could place their bids and obtain their desired product just sitting at home using an Internet connection with Wi-Fi or any wireless network. (Menon and Prathap, 2016; 2017). Many sellers usually offer free delivery of the products to the people who have won the bids. Also the products need not be transferred to any centralized destination, leading to reduced costs of the product.

- Flexibility in Time: Flexibility of time offered to both buyers and sellers is another major advantage of online auctioning system. Sellers are free to place the products for possible bids at any point of time. Usually the time of expiry of a bid is introduced by the seller. Buyers are free to search for similar products online and then have the option to compare with different websites and finally place a bid on the desired product before the time of expiry. This flexibility in time helps to attract a large number of bidders for the product.

- Increased number of bidders: With numerous advantages offered by online auctions, the number of bidders participating increases. People participate in the bidding process to obtain the product, to understand the pricing and sometimes just get the feel of the online auctioning process. Usually large number of bidders utilize the opportunity to place their bids and to participate in the bidding process.

- Increased number of sellers: Flexibility of time and location along with reduced costs attracts a very large number of sellers to introduce their products through online auctions. Reduced costs with minimum transportation and storage of the products is a major reason behind this increased number of sellers.

- Development of economy: With the increased number of customers, more and more sellers would start using the online auctioning systems. Increased number of sellers would in turn attract more customers and this leads to virtuous circle. This increases the overall trade flow leading to better economy and development.

Security Issues

One of the major area of concern in online auction is security of the entire auctioning system and the process. The major security requirements of the auctioning systems are given by Massias *et al.* (1999) and Mills *et al. (*2006). **Fairness** of the auctioning process is of high importance making sure that the highest bidder of the product wins and the corresponding bidder pays the amount decided by the bidding rules. It is also important to ensure that all the participating bidders have equal information about the bidding process. **Confidentiality** of bids is vital in the success of the entire auctioning process. It is very important to secretly maintain all the information related to bids to have an unbiased and efficient online auctioning process. In some cases, it is preferred to have **Anonymity** of bidders. **Mutual Trust** is a very important requirement in online auction system as the buyers and sellers does not come face to face.

Essentials for Secure Online Auctioning System

Secure online auction systems needs,

- **Monitoring**: A highly secure online auction system should have rigorous monitoring facility. Lack of proper monitoring facility can be catastrophic with increased cheating from both buyers and sellers (Avizienis *et al.* 2004). It is highly desirable to have a proper monitoring system to prevent and to detect cheating (Cramton 2005).

- **Accessibility:** Every person should be able to take part in the auctioning process. Sellers should be able to introduce their products for auction irrespective of place and time. Buyers should be able to place their bids irrespective of place and time. Online auctions should be possible without regard to time and location.

- **Management***:* A highly efficient management system for the entire auctioning process online is a major requirement for secure auctions. Online auction management includes product information setting, product information distribution, bidding value collection, database management and overall management of the rebidding process.

RELATED WORK

Syverson *et al.* (2003) introduced a novel auction management protocol which worked on the principle of digital signatures and required bidders to digitally sign and then publish their bids. The protocol extended the bid close time till an acceptable time of inactivity was observed. This was done to prevent the sniping attacks. To safeguard the fairness of the system, the authors presume the existence of a trusted notary and time stamping service. But this assumption is often unusable and invalid in many cases and this method had a number of flaws and could not be applied to present day scenarios. Another interesting method that used undeniable signatures for protection and security was proposed by Sakurai *et al.* (2001). A unique verification protocol was required to verify this signature in collaboration with the signer. The major merit of this system was that only the bid of the winning bidder was disclosed. Also there was no need for trust in the auctioneer since all bidders can verify the correctness of the protocol used. But the major issue with this system was the extensive computational and communications power that was required especially if the list of bidders or possible bid values were high. Due to this drawback this system was highly unsuitable for online auctions. Jung *et al.* (2009) proposed a more innovative and secure cryptographic mechanism for online auction management. A new method of electronic cash using revocable anonymity was introduced by this method and it enabled bidders to demonstrate that they have registered for the online auction in such a way that their identity can be revealed in the case of abuse. This helps to ensure proper auctioning process even when users did not cooperate. Josh Boyd (2007), suggested a technique known as verifiable signature sharing (VSS) that was used to share electronic coins amongst a distributed auctioneer. Reiter *et al.* (2003) proposed a sealed bid scheme for online auctions which hides the bids of all bidders by secret sharing amongst a set of auctioneers. The method used a highly scheme of polynomial secret sharing in combination with bitwise (or any other base) splitting of bids is used. But numerous computational overheads, complexity and added demerits prevented the implementation of these methods in real world scenarios. Harkavy *et al*. (2000) recently put forward an advanced management scheme for online auctions. The technique used the group encryption mechanism to introduce the required security in the entire system. But this method too heavy high computational cost and was highly inefficient. Another recently proposed method had a highly secure auction protocol with a supreme central manager to supervise all the information for the bidders. The major issue with this technique was regarding the trust maintained by the central manager.

Over these years very few works have focused on introducing detection and prevention systems aimed at online auction cheatings. Most of the proposed systems have been on checking and authenticating the identity of the bidders and in secure transfer of messages between them. Further the most recent methods use software's such as RainWorx and AJAuctionPro for online auctions. But these software's suffer from numerous security vulnerabilities and could compromise the secrecy of online auctions. Most of the existing techniques use only a username and a password for secure authentication. This authentication could be easily broken down by cheaters and hackers. Another recent method used Webcams to prevent cheating in online auctions by arbitrarily dispatching pictures of bidders during online auctions. But this method too was inefficient in detecting cheating in online auctions.

A highly efficient and practical approach is to use group protocols and group-mediated communications that would enable the members in the group to transfer messages between them securely. This would also consider different variations that include secure group composition, secure transfer of messages between the groups, and secure communication between the members within the group using the Diffie-Hellman key exchange and symmetric key (Feldman *et al.* 2000). This research paper proposes a Secure System for Online Auctions (SeOA) that adopts two groups for secure communication between distributed entities in the online auction system. In the proposed system the communication between the groups is protected through public key infrastructure (PKI), whereas communication between the group members uses several symmetric Diffie-Hellman keys. Collection of bidders in the entire system is represented as the "group" in this article.

THE SeOA SYSTEM

Architecture

The architecture of the proposed SeOA system is illustrated in figure 1.

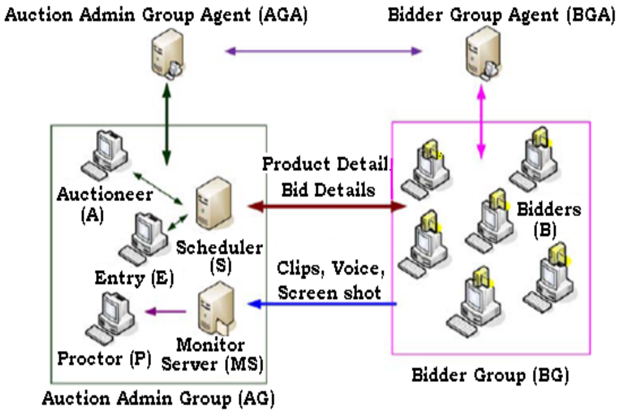


Figure 1. The system architecture of SeOA

Every object in the SeOA system work as members of AG or BG group. Scheduler S collects the problems and the account details from entry, and then dispenses the details and gathers the bid details from bidders. Bidders are observed through P using a proctor A with the data from MS. The group agents AGA and BGA create a set of private and public keys for every group (Sako 2000 and Sakurai 2002). This key collection is dispensed to all the associates of the group on every bid, and they interchange their public keys. Secure intergroup communications are ensured with the public key of each group. Symmetric keys generated by Diffie-Hellman key exchange method (Berry 2003 and Stuart 2000) is employed to enable secure transfer of messages between the members of the group.

SeOA Requirements and System Software

The initial requirements in the implementation of the proposed method include microphones and Webcams in the computers of the bidders. High quality webcams need to be installed in bidder's computers to assist monitoring. The software used to implement the systems is divided into two parts, server side and client side. The OS of the bidder's and proctor's computer are presumed to be Windows 2000 or XP. The system and APIs are developed to support Linux systems too. We further discuss the server side and client side implementations of the software.

Server Side

- First Scheduler (S)

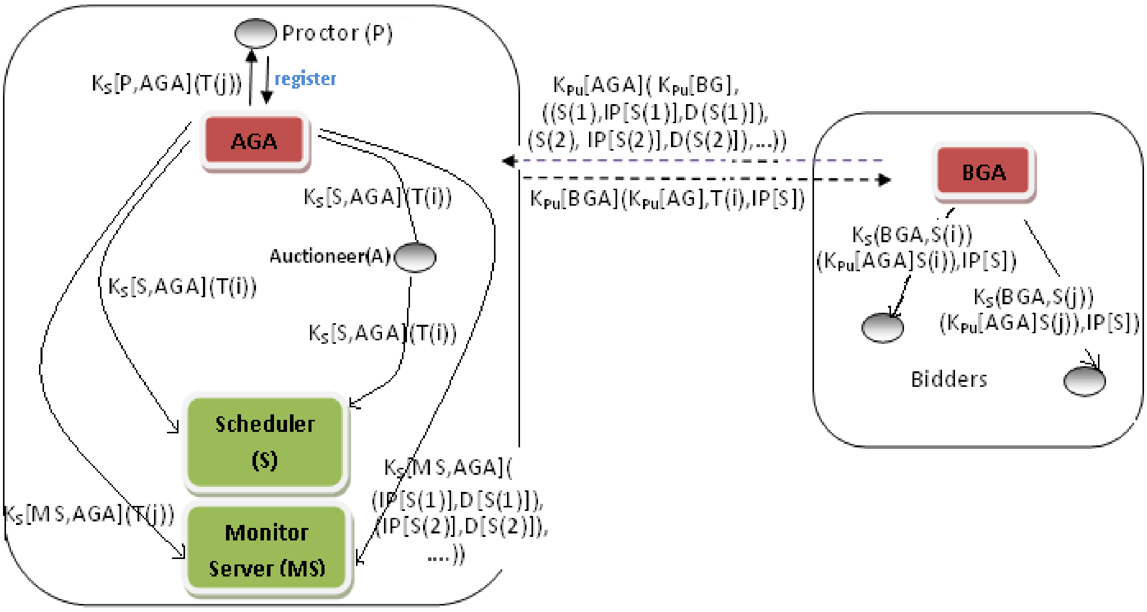

Proctor (P)
$K_S[P,AGA](T(j))$
register
AGA
$K_S[S,AGA](T(i))$
Auctioneer(A)
$K_S[S,AGA](T(i))$
$K_S[S,AGA](T(i))$
Scheduler (S)
Monitor Server (MS)
$K_S[MS,AGA](T(j))$
$K_S[MS,AGA]((IP[S(1)],D[S(1)]), (IP[S(2)],D[S(2)]), ...))$
$K_{Pu}[AGA](K_{Pu}[BG], ((S(1),IP[S(1)],D(S(1)]), (S(2), IP[S(2)],D(S(2)]),...))$
$K_{Pu}[BGA](K_{Pu}[AG],T(i),IP[S])$
BGA
$K_S(BGA,S(i)) (K_{Pu}[AGA]S(i)),IP[S])$
$K_S(BGA,S(j)) (K_{Pu}[AGA]S(j)),IP[S])$
Bidders

Figure 2. Auction arrangement

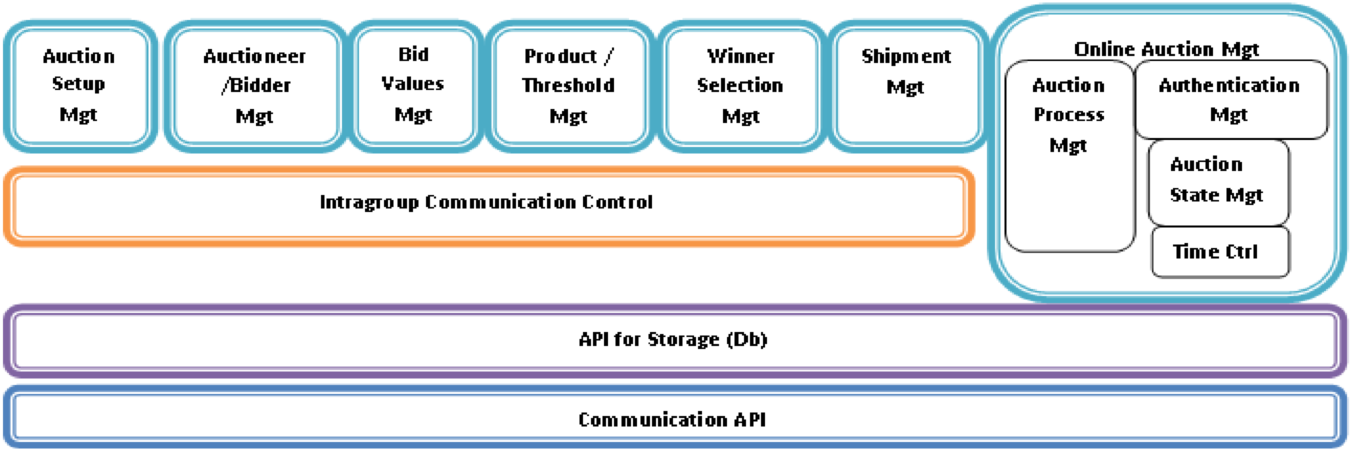


Figure 3. Scheduler structural design

As illustrated in the figures 2 and 3, as soon as the online auction system is set up, Scheduler S acquires the temporary identity of the auctioneer T(i) from AGA straight via the Auctioneer Management Module (AMM). The identity obtained from the auctioneer T(i) is encrypted using the symmetric key $K_s[S, AGA]$ that is shared between S and AGA. To input the details of the bidding process that include the product descriptions, bidding timeline, the auctioneer is checked via A with T(i) by the Auction Setup Management module in S. Using the product module, details of various products, values of bids, and the time allotted to the online bidding activity are stored in database (Db), which is acquired only by Scheduler. When B[S(i)] binds to S with its identity, S(i) and its IP, IP[S(i)], the ABMM forwards to AGA and demands the checking of the auctioneer. As S(i) is encrypted with $K_{Pu}[AGA]$, B[S(i)] will not be able to know its identity and S thus will not be able to check the bidder. After the checking, S saves S(i) and IP[S(i)] in the Db and forwards IP[S(i)] to MS. It then forwards the information and the time allocated to bidding to B[S(i)] via the Auction Process Management module.

With the proposed Secure System for Online Auctions (SeOA) system, the bids presented by the bidders are supplied to the AMM, which stores the bids to Db and then the Bid

Value Module (BVM) signs them with the accurate bids given by B. The winning bid entries are stored in Db. The bids signed by S can be referenced by E via the BVMM when additional details are inserted in the product and bid descriptions. Once all the bidders have presented their bids, the winning bids are distributed to the Bidders. The Time Control module is introduced to manage the time involved in bidding, and the Auction State module checks the states of all B's. This is illustrated in figure 4.

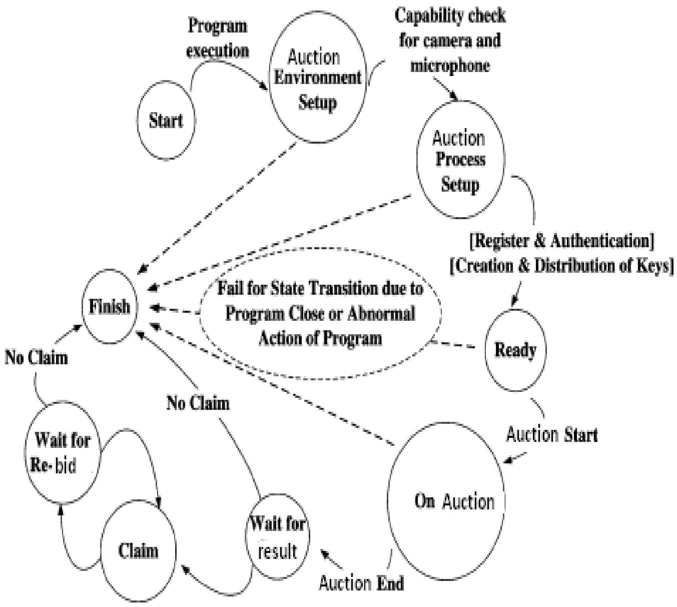

Program execution
Auction Environment Setup
Capability check for camera and microphone
Start
Auction Process Setup
[Register & Authentication]
[Creation & Distribution of Keys]
Finish
Fail for State Transition due to Program Close or Abnormal Action of Program
Ready
No Claim
No Claim
Auction Start
Wait for Re-bid
On Auction
Wait for result
Claim
Auction End

Figure 4. Online auction client state transition diagram

The integrity of the different messages used in communication is verified using an Authentication Management module. The enquiries from the bidders are stored in the Db first so that auctioneer can dispense the replies one by one. This process is managed by an Auction Shipment Module.

- Monitor Server (MS)

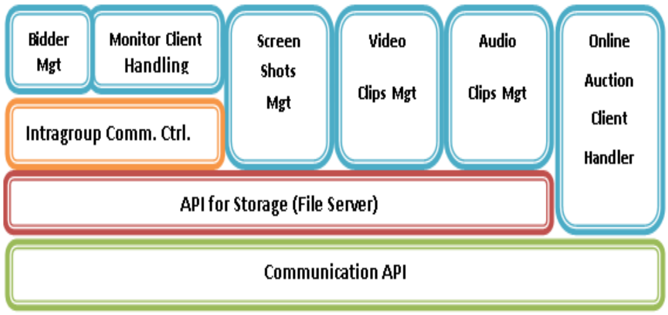


Figure 5. Monitor server architecture.

As illustrated in Figure 5, when the ABM in MS obtains bidder's IP from S, it constructs a directory in the server system to store the data obtained in monitoring. As illustrated in Figure 2, the module also checks the bidder by examining in contrast the IP with that from AGA. The data obtained from monitoring is saved with the reference photos for the bidders obtained from AGA; the photos were captured when BGA authenticated the bidders. A proctor connecting MS via P can check a bidder by comparing the saved reference photo and the monitor data during or after the completion of the bidding process. The Auction Client Handler reports the ports to which video, audio, and screen captures of bidders are sent.

- Bidder Group Agent (BGA)

Two set keys, (K_{Pu}[BG], K_{Pr}[BG]) and (K_{Pu}[BGA],K_{Pr}[BGA]) are generated by BGA when BG is established. The first key is for BG and the second one is for BGA itself. After the verification of the bidders, BGA sends one-time identities to the BG group entities.

- Auction Admin Group Agent (AGA)

Similar to the BGA, AGA creates (K_{Pu}[AG], K_{Pr}[AG]) and (K_{Pu}[AGA], K_{Pr}[AGA]) when A registers itself to AGA. AGA also introduces one-time identities for the members of its group after verifying them. As illustrated in Figure 2, AGA forwards the identity of A and the IP of S to BGA and also forwards the identity of the auctioneer T(i) to Scheduler, S.

- Proctor (P)

The Proctor, P connects to MS to monitor the auction using the data obtained in supervision during the auction. The system works in a way that P should register with AGA first and then be verified with a temporary identity T(j) while linking to MS via P.

Client Side

- First Online auction client

The system introduces enhanced security in client side with application B by blocking all message transfers except those related to the auction by terminating all the ports that are irrelevant to the auction using a filter-hook driver (Pinker 2003).

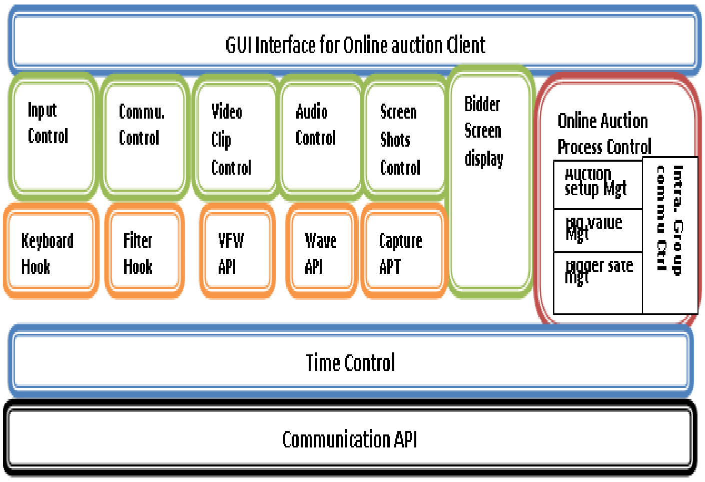


Figure 6. Online auction client architecture

Also as illustrated in Figure 6, all other applications on the bidder's computer, except B, are barred from starting up by a keyboard-hook (Stefan 2005). The VFW and WAVE APIs are used to catch the video of the bidder. H.263 is used to compress the Video from the webcam and it is and sent to MS (McAfee 2000). Because of the smaller size, the audio data generated with the microphone is forwarded to MS without any compression of data. In order to reduce the size and resolution the snapshot of the screen is processed via the Capture API and then forwarded to MS. The entire online auction system is controlled by the Auction Process Control module. The details and the values of the winning bids are allocated to the bidders via the Problem Management and Bid Value Modules.

Here the bidder application, B presents the bids to S via the Bid Management module, and the bid time is governed by the Time Control module. A request is forwarded to S via the Bid Value Module. The Auction Setup Module obtains the temporary identity of B and IP of S from BGA. The transfer of messages between B and BGA are done via the Intragroup Communication Control module. The Auction State Module in B maintains the states of B as illustrated in Figure 4.

Improved security in online auction process

Setup for the Auction Environment

The setup of the proposed system requires all the bidders to download and install B on their systems. The systems presume one monitor for each bidder. Application B runs as a full screen program and terminates all ports except those required for the auction and verifies the Webcam and microphone. Once the auction environment is set up, the bidder is authenticated and the details of the products are given. B opens the details for the bidder after receiving the message from S to start bidding.

Setup of an Online Auction

Figure 2 illustrates the configuration of the online auction system started by A, which binds itself to AGA and obtains its temporary identity T(i) as KS[S, AGA](T(i)). When a bidder registers with BGA via B, the bidder receives S(i) in the form of K_{Pu}[AGA](S(i)) from BGA as a member of BG and IP[S].

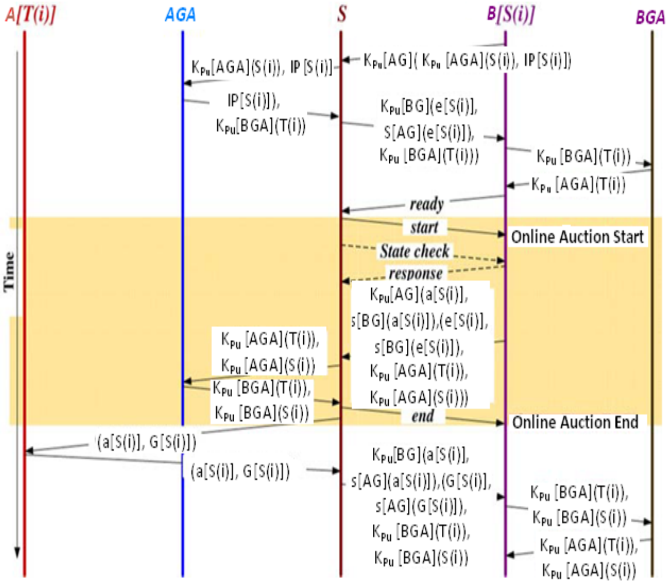


Figure 7. A secure online auction process.

Further as illustrated in Figure 7, B links to S and requests its verification by forwarding K_{Pu}[AGA](S(i)) and IP[S(i)].

After B registers with BGA, BGA sends S(i), IP[S(i)], and D[S(i)] for B to AGA. In order to act as an evidence in detecting cheating AGA sends IP[S(i)], and D[S(i)] to MS. When S notifies MS of IP[S(i)], MS verifies if the IP is in the IP list of the bidder from AGA. If valid, MS requests the transmission tests of the monitor data for the bidder.

Online Auction Control

After the online auction is set up, S forwards the required details E[S(i)], its digital signature s[AG](E[S(i)]) signed by AG , and identity of the auctioneer K_{Pu}[BGA](T(i)) to B[S(i)] as illustrated in Figure 7. B[S(i)] checks the integrity of E[S(i)] with s[AG](E[S(i)]) and appeal checking of the auctioneer by forwarding K_{Pu}[BGA](T(i)) to BGA. After checking that no anomalies exist in the descriptions, B forwards the ready message to S. When S receives the ready message from all the bidders, it forwards the start message to all the B's. At that point, B lets bidders see the details one by one. The monitor data for all bidders are transmitted to the monitor server until the auction ends. B[S(i)] sends s[BG](a[S(i)]), e[S(i)], s[AG](e[S(i)]), K_{Pu}[AGA](T(i)),

K_{Pu}[AGA][S(i)], as well as its bid details, a[S(i)] to S. S requests the verification of B[S(i)] to AGA and checks the integrity of the product and the bid value.

Winner Selection

As illustrated in Figure 7, after B[S(i)] submits a[S(i)], and B[S(i)] is verified by AGA, S imprints the received bids with correct threshold given by A and calculate the winning bid.

ANALYSIS

Security confirmation for SeOA and E-monitoring

System Model

In the proposed Secure Online Auctioning system, online auction has been represented with the same rules that pertain to traditional face to face offline auctions. In the proposed system, the person setting the auction can provide the required details and valid threshold bid values via the auctioneer A. The bidder can then enter via the entry E. Using the proctor, the bidders can be easily supervised with the real time monitor data stored in the server. The scheduler S governs and manages the descriptions of the products, their right threshold values, and the bid values from bidders. The authentication, which was based only on a username and password in the existing system, is boosted by group management.

Security is further strengthened by verification using Webcam. Further, temporary identities are issued for every auction. Thus it becomes impossible for any entity to capture all details and real identities and the shared keys in the auctioning system. This enhances the security of the system and prevents the chances for system compromise that might be caused due to the breakdown of a single object from any external attack.

Achievement of Security Requirements

In the proposed SeOA system, any cheating could be found out using the data from monitoring stored on the MS. The security measures for the system is administered via the intergroup communication based on PKI, the intragroup communication using symmetric keys and the temporary identity. For every auction, the systems set the auction administrative group and the bidder group. All the entities in the online auction is a part of one of this group. Temporary identities are issues by the selected agents of each group to the corresponding group members. The agents as well as the group members are unaware of the identities of other members. Further, member in the corresponding group is unaware of their temporary identity. This is achieved by issuing the temporary identity in an encrypted form and protected by the public key of the verifier, the other group agent. These identities are then exchanged by the group agents.

Cheating avoidance and discovery Through E-monitoring

The proposed SeOA system uses five unique methods to avoid and detect cheating in online auctions. Initially, a Webcam is used to verify the identities of all the entities in the system. Further, the reference photos taken during the verification process are stored, to be used for authentication during the auction process. Secondly, the data obtained during the supervision of different bidders are saved and stored during the auction process. With this continuous recording of video and audio during the auction rather than isolated images, a proctor can easily determine the bidders involved in cheating. Another method is using the screen shots saved in parallel with videos of a bidder. Using these screen shots, a proctor can easily understand what operation is the bidder really performing with their computer. The next major technique put forward by the proposed method is to eliminate all the communication by the bidders, except for those required for the online auction via port control. All ports except those required for the online auction are disabled and the ports used can be chosen randomly for each bidder. This eliminates the cheating via a fixed port. Finally, all application programs except the online auction client are disabled by controlling the inputs of the bidders.

Overhead

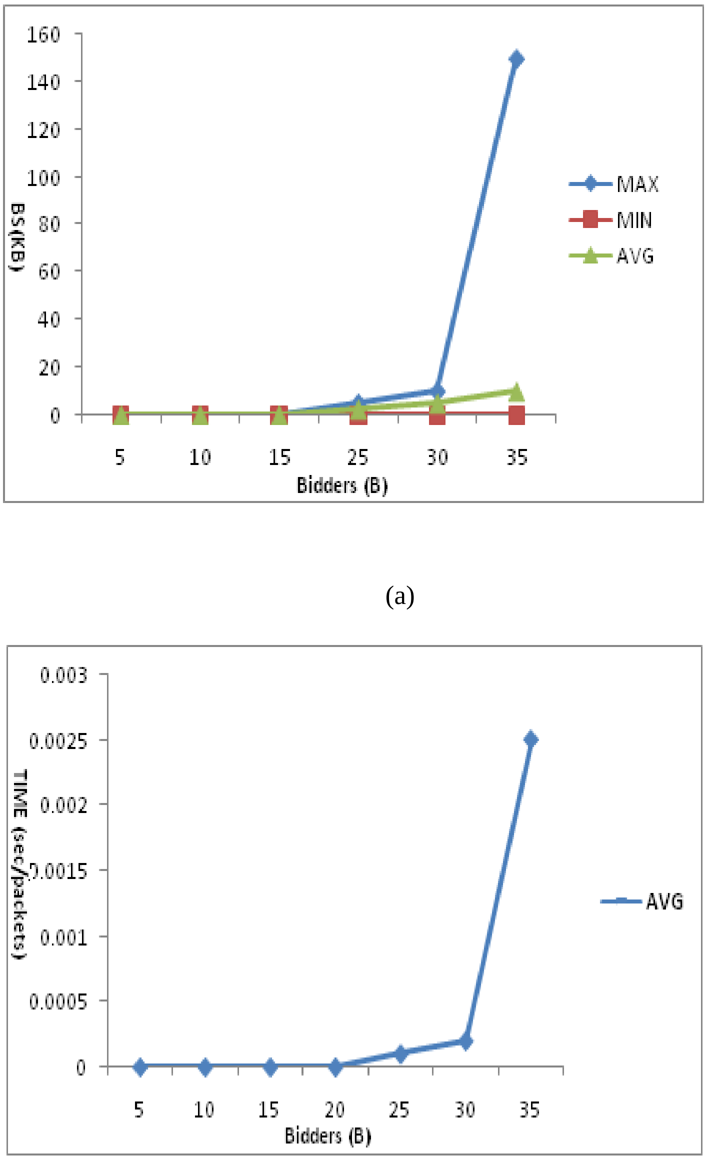
This section discusses the overhead incurred by the proposed system in detecting and preventing cheating in online auctions. The overhead is mainly generated from the storage and transmission delay with the monitor data. To evaluate the overhead, a prototype of the SeOA system was developed. Quantity of data generated every second in the auction process was then measured. The Webcam used was A4Tech PK-835MJ Webcam which had a built in Mic. The online auction client application was then installed on Pentium IV computer with Windows XP OS. The system used a 2 GB RAM with 3.00 GHz CPU. The frame rate was set to 15 for the incoming video data and the maximum allowed drop rate was set at 50%. H.263 was used for compressing the video data.. For an hour auction, 720 MB of data was saved on the MS for each bidder.

Queuing theory and simulations were used to estimate the load for MS with multiple bidders. Simulation was used to determine the number of MS to be given and the delay in transmission. It was presumed that the arrival rate at the MS was based on the Poisson distribution. Performance of the model was calculated using the value of T_M, which is the average time for a packet to stay in the MS, and BS, which is the size of the packet buffer in the gateway at the MS to avoid dropping packets above the probability P_{drop} as (1). B is the count of bidders; λ_P is the arrival rate at P. The service rate in the monitor server μ_{MS} can be derived as (2) where $1/\mu_{FS}$ is the time required to copy one packet of the monitor data.

$$T_M = \frac{1}{\lambda_{MS} - \mu_{MS}} P_{drop} > \frac{(1-\rho)^{BS}}{1-\rho^{BS+1}} \qquad (1)$$

$$\lambda_{MS} = \sum \lambda B * B\mu_{MS} = \frac{1}{\left(\frac{1}{\mu_{FS}}\right)+\left(\frac{1}{\mu_G}\right)} \qquad (2)$$

When the distpensation of packet lengths is presumed to be exponential with 515 bits/packet and the link capacity is fixed as 100Mb/s, the 1/μG is given as 5.15μs/p. The copy time is calculated on a Pentium IV 3.0 GHz computer with 2 GB RAM. The values of $1/\mu_{FS}$ and λ_B were 4.25μs/packet and 4 packets/s, averaged over 1000 trials. To obtain BS, the drop ratio bound Pdrop was set to 10-6. Figure 8(a) shows the maximum (MAX), average (AVG), and minimum (MIN) buffer requirements of BS at the gateways of nodes for the given P_{drop}. In Figure 8(b), the delay per packet in a node affects the delay of the monitor data delivered to the MS. As the number of bidder increases, the total volume of the monitor data also increases.



(a)

(b)

Figure 8. The performance of monitor data delivery (a) MAX, AVG, and MIN buffer requirements at the gateways of nodes. (b) Node delay per packet.

CONCLUSIONS AND FUTURE WORK

This research paper proposed a novel and highly secure online auctions management system using group cryptography with remote supervision. The paper initially discussed the advantages of the online auction process over the traditional face to face auction process. Further the paper discussed the issues and challenges involved in maintaining security of the online auctioning systems. The paper discussed previous works done on introducing the secure online auction systems. The paper introduced a new secure online auction management system that targeted towards auctions administered via the Internet at a fixed time with one problem set, but without any restriction on the bidder location. The proposed Secure Online Auction Approach (SeOA) approach is applied to online auction administered at different times and provide with a secure and easy and automated auction process. Using the proposed e-monitoring method, the bidders can be observed, just like the traditional face to face auction system. Any cheating that went unobserved during the time of auction can be found out using the monitor data saved in the server. The improved security for the online auction is controlled through the intergroup communication based on PKI, the intragroup communication using symmetric keys and the temporary identity. Future research should be targeted at detecting malicious entries in the system and in preventing frauds in online auctioning system.

REFERENCES

[1] Albert, M. R. (2007) 'E-buyer Beware: Why Online Auction Fraud Should Be Regulated', *American Business Law Journal,* Vol. 39, No. 4, pp.575-643.

[2] Auction Watch (2006). Available at: http://www.auctionwatch.com (accessed 1, June, 2010).

[3] Avizienis, J.C. Laprie, B. Randell, and C. E. Landwehr (2004) 'Basic concepts and taxonomy of dependable and secure computing', *IEEE Trans. Dependable Sec. Comput.,* Vol. 1, No.1, pp. 11–33.

[4] Ba, S., Whinston, A. B. and Zhang, H. (2003) 'Building trust in online auction markets through an economic incentive mechanism', *Decision Support Systems,* Vol.35, No.3, pp.273-286.

[5] Berry Schoenmakers, (2003) 'A simple publicly verifiable secret sharing scheme and its application to electronic voting', *Journal of Advances in Cryptology,* Vol.4, No.1, pp. 148-164.

[6] Cramton, P. (2005). 'Ascending auctions, European', *Economic Review,* Vol.42, No.5, pp.745-756.

[7] Hong Liu, Shouhong Wang and Fei Teng, (2002) 'Real-time multi-auctions and the agent support', *Journal of Electronic Commerce Research,* Vol.1, No.4, pp. 615-630.

[8] Josh Boyd, (2007) 'Safety on the auction block', *Information Security.* Available at: http://www.infosecuritymag.com (accessed 13, June, 2010).

[9] Jung Im Y. and Heon Y. Yeom, (2009) 'Enhanced Security for Online Exams Using Group Cryptography', *IEEE Transactions on Education,* Vol. 52, No. 3, pp. 340-349.

[10] Kapali Viswanathan, Colin Boyd, And Ed Dawson, (2000) 'A three phased scheme for sealed bid auction system design', *Journal of* Information *Security and Privacy* Vol.2, No. 2, pp. 267-273.

[11] Kazue Sako (2000) An auction scheme which hides the bids of losers *(Springer-Verlag, 2000).*

[12] Kouichi Sakurai and Shingo Miyazaki, (2002) *A bulletin-board based digital auction scheme with bidding down strategy* (City University of Hong Kong Press, 2002).

[13] Manoj Kumar and Stuart Feldman, I. (2000) 'Internet auctions', *Journal on Electronic Commerce,* Vol.4, No.1, pp.132-151.

[14] Massias, H. Serret Avila, X. And Quisquater, J.J. (1999) 'Timestamps: main issues on their use and implementation', *International Journal on Enabling Technologies: Infrastructure for Collaborative Enterprises,* Vol. 10, No. 1, pp.178–183.

[15] Matthew Franklin, K. And Michael Reiter, K., (2003) The design and implementation of a secure auction service', *IEEE Transaction on Software Engineering,* Vol. 22, No. 5, pp. 302-312.

[16] Mcafee, John, Preston R. & Mcmillan, (2000) 'Auctions and Bidding', *Journal of Economic Literature, American Economic Association,* Vol. 25, No. 2, pp. 699-738.

[17] Menon V. G, Jogi Priya P M, Joe Prathap P M, (2013). 'Analyzing the behavior and performance of greedy perimeter stateless routing protocol in highly dynamic mobile ad hoc networks', *Life Science Journal,* vol. 10, no.2, pp 1601-1605.

[18] Menon V. G. and Joe Prathap P M, (2016). 'Comparative Analysis of Opportunistic Routing Protocols for Underwater Acoustic Sensor Networks', *Proceedings of the IEEE International Conference on Emerging Technological Trends [ICETT],* Kerala, India.

[19] Menon V. G. and Joe Prathap P M, (2016). 'Routing in Highly Dynamic Ad Hoc Networks: Issues and Challenges' *International Journal of Computer Science*

and Engineering, vol.8, no. 4, pp.112-116.

[20] Menon V. G. and Joe Prathap P M, (2017). 'Towards Optimal Data Delivery in Highly Mobile Wireless Ad Hoc Networks", *International Journal of Computer Science and Engineering*, vol.9, no. 1, pp.1-6.

[21] Menon V. G. and Joe Prathap P.M, (2016). 'Analyzing the Behavior and Performance of Opportunistic Routing Protocols in Highly Mobile Wireless Ad Hoc Networks', *International Journal of Engineering and Technology*, vol. 8, no. 5, pp. 1916-1924.

[22] Menon V G and Joe Prathap P M (2016). "A Review on Efficient Opportunistic Forwarding Techniques used to Handle Communication Voids in Underwater Wireless Sensor Networks", Advances in Wireless and Mobile Communications, Vol. 10,No.5, pp. 1059-1066

[23] Michael Harkavy, J.D., Tygar, And Hiroaki Kikuchi, (2000) 'Electronic auctions with private bids', Journal *on Electronic Commerce*, Vol.4, No.1, pp. 61-83.

[24] Michael Wellman P. And Peter Wurman, R. (2001) 'Real time issues for internet auctions'. In: *DARE-98: First IEEE Workshop on Dependable and Real- Time Ecommerce Systems*, (New York, 2001).

[25] Mills, D. L. (2006) *Computer Network Time Synchronization: The Network Time Protocol*. (CRC Press, Inc., Boca Raton, FL, USA)

[26] Pinker, E.J. Seidman, A. And Vakrat, Y. (2003) 'Managing Online Auctions: Current Business and Research Issues', *Management Science*, Vol. 49, No. 11, pp. 1457-1484.

[27] Sakurai, Mihir Bellare, Juan Garay, A., And Tal Rabin, (2001), 'Fast batch verification for modular exponentiation and digital signatures', *Advances in Cryptology*, Vol. 2, No.1, pp. 236-250.

[28] Stefan Klein, (2005) 'Introduction to Electronic Auctions', *Electronic Markets*, Vol. 7, No. 4, pp. 13-26.

[29] Stuart G. Stubblebine and Paul Syverson, F., Fair, (2000). *on-line auctions without special trusted parties* (Springer-Verlag, 2000).

[30] Syverson, R., Deering, S., Estrin, D., Farinacci, D., Jacobson, V., Liu, C.G. And Wei, L., (2003) 'The PIM architecture for wide-area multicast routing', IEEE*/ACM Transactions on Networking*, Vol. 4, No. 2, pp. 153-162.