An Agent based Approach to Secure Real Time Auction System using Trust Management Module with Image Encryption

Suhas R
M.Tech(CE) 4th Sem
Department of Computer Science and Engineering,
SJB Institute of Technology, Bangalore-60

***Abstract*: Agent based online auctions have not yet become popular because they are not trustable. One of the major concerns in agent based online auctions is the shilling behavior problem, which makes winners have to pay more than what they should pay for auctioned items. In this paper, we propose a real-time trust management module for agent based online auction systems using role-based access control mechanisms. The key components of the trust management module, a security agent can actively monitor online auctions in order to detect abnormal bidding behaviors in real-time. To illustrate the feasibility of our approach, we implemented a prototype real-time trust management module for agent-based online auction systems, and demonstrated how shill agents could be efficiently detected. The images in the auction system are encrypted by using various encryption schemes.**

I. INTRODUCTION

One of the most popular electronic commerce activities in recent years has been the use of online auction systems[1]. Among the various auction types, the English auction has emerged as the preferred form for online auction systems (e.g., eBay) due to its characteristics of multiple bids and ascending bidding price [1, 2]. As the number of users and products increases, more time is required for a user to search and bid for an auctioned item. To cope with this problem, agent based online markets have come into play. An agent based online auction system is a multi-agent system [3] that comprises software agents to handle tedious tasks on behalf of human users. Each agent is autonomous and capable of taking actions to fulfill its goal.

Thus, in an agent based online auction system, an agent can represent a user to search and bid for a product based on the constraints defined by the user. There is a pressing need for a trust management system to maintain trust among users as well as with the online auction system. By behaving in an undesirable or fraudulent manner, one party is able to gain at the expense of another. For example, bidders can use practices such as bid shielding and bid sniping to keep the price low[8]. Alternately, shill bidding is a strategy which a seller may pursue, to artificially inflate the auction price. In addition, siphoning is a tactic employed by an outsider, who is seeking to profit from an auction by offering bidders a cheaper, identical item. Finally, a seller might attempt to auction a non-existent or misrepresented item.

In this paper, we propose a real-time trust management model to establish trust for agent based online auction systems. In our proposed model, a security agent is responsible for keeping track of each transaction and detecting unusual activities, such as shill biddings; while an authorization module can update a user's role and access permissions dynamically. Due to real-time actions against any abnormal auction activities, our trust management model[1] can effectively maintain trust for agent based online auction systems.

The rest of this paper is organized as follows. Section 2 discusses about related work. Section 3 describes agent based online auction systems. Section 4 introduces a real-time trust management module integrated with a security agent. Section 5 presents an example to show how shill agents can be detected in real-time. Section 6 provides conclusions and our future work.

II. RELATED WORK

There are two main strands of work to which our research is related, i.e., work on agent-based online auction system and work on trust management in e-commerce. Ito and his colleagues proposed *BiddingBot* as a multi- agent system that supports co-operative bidding [5]. In their approach, bidding decisions are actually made by users rather agents. Ogston and Vassiliadis proposed a peer-to-peer agent-based auction system for continuous double auctions [6]. They found that peer-to-peer auctions are able to display price convergence behavior similar to that of centralized auctions. In Collins and his colleagues' work, a multi-agent system for contract negotiation was presented [7]. The system can be used as a testbed for online auctions; however, it may have problems with secrecy of bids, non-repudiation, and manipulation of bids. Although the above efforts are useful in justifying the feasibility of agent-based approach for online auctions, there are no attempts so far to provide security mechanisms to prevent an agent-based online auction system from being abused. Therefore, it is still hard to convince users to adopt the existing agent-based approaches for practical usage.

Figure 1 presents a high level software model for performing online auctions. There are two main parties: a bidder and an Auctioneer[2]. Theparties are joined by a communication link. There are two types of interface for a bidder. The first is the web interface. This is for a human bidder. The bidder interacts with the Auctioneer via a HTML browser. The second interface is for a software bidding agent. A bidding agent interacts with the Auctioneer using an application programming interface. The Auctioneer runs a web server (e.g., Apache) and a scripting language, in this case php. The entire auction is database driven. All state information (e.g., bids, timing, etc.) about the auction is contained in the database. When a client submits a bid or requests a price quote, a database transaction occurs. The database generates dynamic web pages in response to bidder activity using the scripting language.

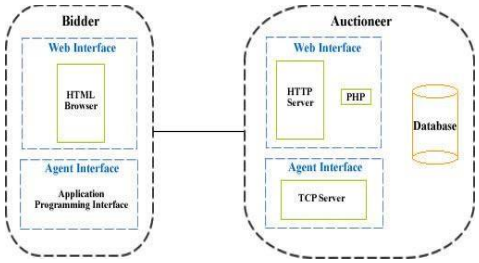

Figure 1. Online Auction Software Model

In this paper, we propose a real-time trust management model for agent based online auction systems. Our proposed model can be used to establish and maintain trust among agents based on both agents' history information and real-time state information. To

monitor and detect any undesired behaviors such as shilling behaviors in an agent based online auction system, a security agent is designed and implemented. In addition, we isolate various security related policies in different modules, so the policies can be updated dynamically.

III. AGENT BASED ONLINE AUCTION SYSTEM

An agent based online auction system is a multi-agent system that facilitates online auction activities on behalf of human users to make users' life much easier. We have developed a prototype agent based online auction system using the JADE agent development framework [14]. Figure 1 shows a client-server architecture of our agent based online auction system, which consists of various types of software agents, such as search agent, bidding agent, and auction agent. In particular, a security agent is introduced to provide security mechanisms for detection of undesired biddingbehaviors.

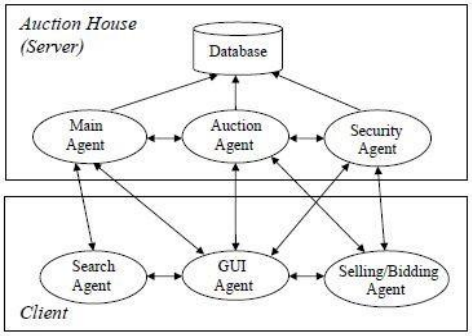

Figure 2. Architecture of agent based auction systems

The agent based online auction system is managed by an auction house administrator and used by various sellers and buyers. The auction house is implemented at the sever side with three major types of agents, namely the main agent, the auction agent, and the security agent. The main agent works as a controller for the auction house, and is responsible for creating new accounts for users, creating auction agents, and also responding to queries for items or auctions from agents at the client side. For each new auction, a corresponding auction agent is created to handle its auction related activities such as posting bids. While an auction is running, an agent representing a user can put bids on auctioned items; meanwhile, the corresponding auction agent is responsible for updating bidding activities for all involved agents. At the end of an auction,the auction agent notifies the winner of the auction, and passes the control back to the main agent. As a major component for security, the security agent monitors all online auction transactions performed by bidding agents.

The agents that work on behalf of human users are implemented at the client side, which involves three major types of agents, namely the search agent, the selling/ bidding agent, and the GUI agent. A GUI agent receives commands from a user, and updates the user interface when messages are sent and received. A search agent can automatically search and join an auction on behalf of a user. Finally, a selling/bidding agent is responsible for initiating auctions or automatically placing bids on behalf of a user according to user defined bidding strategies. Note that a user can be a seller and a bidder at the same time.

In the agent based online auction system, a user can configure a bidding agent by providing auction related information, such as the type of items they are interested in, maximum value for that item, and bidding strategies for how to put bids during an auction. A configured bidding agent will run autonomously, and make decisions on behalf of the user during the bidding process.

IV. IMPLEMENTION

Trust Management Module

The trust management module (TMM) defined in Figure 2 is a key component in an agent based online auction system for trust maintenance, which can be further refined as shown in Figure 3. From the figure, we can see that the trust management module consists of a number of sub-modules

such as authentication, authorization, state and history modules. As one of the major features of our TMM module, the security agent works closely with other modules of the TMM to maintain trust among agents in real-time. The authorization module, the access control module, and the security agent have their own policy rules defined by the auction administrator. Each set of policy rules are modularized in a corresponding database that can be updated dynamically without shutting down the agent-based online auction system.

Figure 2 is an overview of our proposed trust management module in an agent based online auction system. From the figure, we can see that a human user can configure an agent to initiate an auction as a seller or put bids on an auctioned item as a buyer. Before an agent starts to work, it must go through atrust management module for security purpose. The agent needs to send a digital certificate or user credentials to the trust management module for authentication and authorization. Once the user configured agent is authenticated and authorized, it will be allowed to place requests for auction related activities. During the auction process, a configured agent can check current status or ratings of other configured agents in order to make proper decisions on choosing the right auction. Meanwhile, a security agent is designed for monitoring auction transactions for any suspicious bidding behaviors.

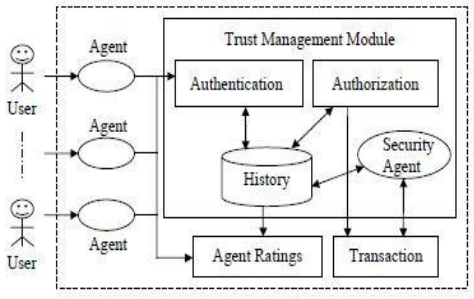

Figure 3. Trust management module

The role assignment process assigns a role to the configured agent dynamically by applying role assignment policies, called *RA Policies* based on gathered information related to the corresponding user. The access control process grants or restricts the access to auction related activities for the user configured agent based on access control policies, called *AC Policies*. The access control mechanism also determines how frequently the security agent should monitor a configured agent's auction transaction activities. After being authorized, the configured agent can start to make requests for auction related activities with certain permissions. Meanwhile, the security agent continuously monitors auction related activities in the auction system according to security agent policies called *SA Policies*. Once the security agent detects any shilling behaviors, the security agent determines the severe level of the shilling behaviors, and updates the current state information of the shill bidder. Furthermore, the security agent notifies all participating configured agents about the shilling behavior of the shill bidder in the corresponding auction.

History Module and State Module

The history module stores information about users' previous auction activities over a certain period of time. Examples of such information include previously assigned roles,access information, shilling behaviors, and feedback information. After each successful transaction of a configured agent, the information in the history module is updated, and is ready to be accessed by the security agent and the trust management module for decision making.

The state module stores information related to the configured agents and their current activities, which includes currently assigned agent roles, granted resource access information, and possible shilling behaviors. The state module information is used along with the history module information to determine a configured agent's next dynamic role assignment by the role assignment module.

Authorization Module

In our proposed agent-based auction system, all requests made by an agent are controlled by the authorization module (Figure 3). In other words, in order to perform any auction related activities, an agent must first get an appropriate role and access permissions from the authorization module. We now describe in more details for the two major components in the authorization module, i.e., the role assignment module and the access control module, as follows.

Role Assignment Dynamic role assignment is performed according to predefined *RA Policies* stored in a role assignment database. The needed information for the computation includes the following: (1) the configured agent's history information, number of positive and negative feedbacks, and feedback status from the history module; (2) the user's current role and shilling behavior information from the state module. According to the *RA* policies, an agent can be assigned to one of the following five types of roles: *most trusted*, *trusted*, *average*, *untrusted*, and *most untrusted* for both sellers and buyers. As an example of role assignment rules, the following policy written in Prolog defines the conditions for assigning the *most trusted* buyer (*mtb*) role to an agent.

According to the above rule, an *mtb* role is assigned to a bidding agent when the agent satisfies requirements such as having more than 1000 positive feedbacks, having less than 100 negative responses, not doing shilling in the last transaction, and taking a role of either *most trusted* buyer (*mtb*) or *trusted* buyer (*tb*)currently.

Access Control The access control module grants or denies an agent the access to resources requested by the agent. It may also restrict a bidding agent to perform certainauction activities for a period of time, if the agent has any shilling behaviors in its previous history.

A newly registered agent, which starts by getting a role of *average* buyer, is assumed to be trustable, so it shall have the privilege to perform auction activities. During the auction time, if an agent's role is downgraded (e.g., from a role of *average* buyer to a role of *untrusted.* buyer), it signifies that undesired activities have been done by the agent. In this case, the access control module may give warnings to the agent or

restrict the agent to perform further activities for a certain period of time. If an agent is restricted to participate in any auction related activities for a certain period of time, the access control module sets the penalty status as *active* for the agent, and will deny all requests by that agent. The following is an example of *AC Policy* in Prolog that defines how different penalties can be applied and how different security levels will be set according to different situations of role changes.

Security Agent

To make online auction system trustworthy and to ensure the bidding process reliable, we should prevent and minimize undesired bidding behaviors. Since it is not feasible to monitor every activity of each agent in details, we decrease the load of the security agent by defining different security levels such that the depth of checking is directly proportional to the level of distrust in the user. For example, a bidding agent with security level of 1 will receive the most careful monitoring.

To detect shilling, the security agent is configured to perform different types of security checks. At the lowest level (level 4), only the distance in locations of a buyer and a seller are checked according to their IP addresses. At level 3, we check if a buyer is participating in concurrent auctions with identical auctioned items. Note that concurrent shilling, where a bidding agent places bids on an auction item with higher auction price rather than on the auctioned item with lower auction price, is a strong indication of shilling behaviors. At level 2, the security agent analyses the bidding style of a buyer against common shill patterns. In many cases, it has been found that a shilling agent does aggressive biddings at the beginning, and stops bidding towards the end of the auction to avoid winning the auction. Finally, at the highest security level (level 1), the security agent performs all above checks coupled with ananalysis of the bidding agent's history. The security agent derives a shill factor by applying different security rules on the agent's current and previous behaviors. If the shill factor is high enough, the agent's bidding status will be set as *shilling*, and the state module will be updated. The updated information stored in the state module will be used by the role assignment module when the shill bidder makes a new bidding request.

Encryption

The image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. Image encryption, video encryption, chaos based encryption have applications in many fields. The images need to be encrypted in the auction system. Encryption will be defined as the conversion of plain message into a form called a cipher text that cannot be read by any people without decrypting the encrypted text. Decryption is the reverse process of encryption which is the process of converting the encrypted text into its original plain text, so that it can be read.

VI. CONCLUSION

In order to build a trustworthy agent- based online auction system, we introduced a real-time trust management module (TMM) to restrict and prevent undesired bidding behaviors such as shilling behaviors in online auctions. Based on an agent's current and previous behaviors in agent-based online auctions, the real-time trust management module can assign agent roles dynamically, and grant or deny an agent for varying levels of access to auction related resources and activities. Meanwhile, any undesirable bidding behaviors performed by a bidding agent can be automatically detected by a security agent. We have defined different policy rules in Prolog for dynamic role assignment, access control mechanisms, and undesirable bidding behavior detection.

VI. REFERENCES

[1] R. Patel, H. Xu, and A. Goel, "Real-Time Trust Management in Agent Based Online Auction Systems," In *Proceedings of the* *th*

[2] Jarrod Trevathan, Wayne Read and Rodel Balingit, "*Online Auction Software Fundamentals*", 2009 International Conference on Computer Engineering and Applications IPCSIT, vol.2, pp. 254-259, 2011.

[3] Katia Sycara, "MultiAgent Systems," *AI Magazine*, Vol. 19, No. 2, Summer 1998, pp. 79-92.

[4] Haiping Xu, Sol M. Shatz, and Christopher K.Bates, "*A Framework for Agent-Based TrustManagement in Online Auctions*," IEEE Computer Society, 2008.

[5] T. Ito, N. Fukuta, T. Shintani, K. Sycara, "BiddingBot: A Multiagent Support System for Cooperative Bidding in Multiple Auctions," In *Proceedings of the Fourth International Conference on MultiAgent Systems*, July, 2000, pp. 399- 400.

[6] Hemanta Kumar P., Gautam Barua, "*Design of a Real-Time Auction System*", 4th International Conference on Electronic Commerce Research, Dallas, Texas, USA, pp. 683-692, 2001.

[7] Radheshyam Nanduri, Sai Krishna.G, Sandeep Kumar. D, Sathyamoorthy. E, and Dr.N.Ch.S. N. Iyengar, "*A Framework for Secure and Scalable Agent Based E-Auctions*", Special Issue of the International Journal of the Computer, the Internet and Management, Vol.17 No. SP1, March, 2009.

[8] J. Trevathan and W. Read, "Undesirable and Fraudulent Behaviour in Online Auctions," In *Proceedings of the International Conference on Security and Cryptography*, 2006, pp.450-458.

[9] D. H. Chau, S. Pandit and C. Faloutsos, "Detecting Fraudulent Personalities in Networks of Online Auctioneers," *PKDD 2006*, Berlin Germany.

[10] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-Based Access Control Models," *IEEE Computer*, 29(2):38-47, 1996.

19 International Conference on Software Engineering and Knowledge Engineering (SEKE'07), Boston, USA, July 2007, pp. 244-250.