A Framework for Agent-Based Trust Management in Online Auctions

Prof. Haiping Xu
Computer and Information Science Department
University of Massachusetts Dartmouth
Email: hxu@umassd.edu

Acknowledgement

- Dr. Sol M. Shatz, Professor
  Concurrent Software Systems Laboratory
  Computer Science Department
  University of Illinois at Chicago

- Chris Bates, Graduate Student
  Concurrent Software Engineering Laboratory
  Computer and Information Science Department
  University of Massachusetts Dartmouth
Online Auctions

- Different types of auctions
  - Increase-price auction (English auction)
  - Decrease-price auction (Dutch auction)
  - Second-price sealed-bid auction (Vickrey auction)

- English auction has become the most popular one in online auction houses (e.g., eBay).
- However, it is time-consuming for a human user to search and place bids on an auctioned item.
- There is a pressing need to introduce agent technology into online auction systems.

Agent-Based Online Auctions

- It consists of an auction house and a number of clients.
- It is designed as a multi-agent system.
- The auction house is managed by auction house administrator.
- Agents at the client side work on behalf of human users.

Security agent monitors online auction transactions for any undesired bidding activities, e.g., shilling behaviors.
Shilling Behaviors

- A shill bidding is a deliberate activity of placing bids in order to artificially raise the price of an auctioned item.
- Although most of the online auction houses prohibit shilling behaviors, it is easy for malicious users to disguise themselves and put in shill bids in online auctions.
- In a recent research study at Carnegie Mellon University, dozens of probable fraudsters were detected at eBay using data mining techniques.
- It is vital to introduce a feasible trust management mechanism to prevent, detect and avoid trading frauds, such as shilling behaviors.

An Example

- We call this type of shilling behavior concurrent shilling.
- Other types of shilling behaviors include: reserve price shilling, competitive shilling etc.
- Shilling behaviors become much more severe in an agent-based online auction system because
  - Automatic detection of shill bidders in agent-based online auctions can be much more difficult.
  - Malicious users may set up bidding strategies and automatically initiate shilling activities.
Trust Management

- Trust management has been a promising approach to building trustworthiness in networked systems.
- Two major types of trust management approaches
  - Reputation-based trust management, e.g., in eBay,
    - It uses a very simple reputation based rating scheme for users
    - After each successful transaction, sellers and buyers are invited to rate each other on a 3-point scale, i.e., +1, 0, or -1.
    - The accumulative feedback score of a member represents how other members are satisfied with this member for doing business.
  - Policy-based trust management, e.g., in policyMaker,
    - Credentials and policies are fully programmable
    - Input \( (r, C, P) \) \( \rightarrow \) output whether the set \( C \) of credentials proves that the request \( r \) complies with the local security policy \( P \).
Our Role-Based Approach

- Our approach is a combined approach, which
  - Takes advantages of agent-based technologies.
  - Considers agent reputations stored in a history module.
  - Adopts role-based access control (RBAC) mechanism based on a set of policy rules.
- In an RBAC model, users are assigned roles with permissions
  - Results in reduced administrative costs as compared to associating users directly with permissions.
  - Most of the RBAC models follow the same basic structure of subject, role and privilege.
  - However, in a more sophisticated role-based access control model, access decisions also depend on other factors.
  - We use user’s real-time behaviors as factors in our RBAC model. Thus our approach supports dynamic role assignment and access control.

Agent-Based Trust Management (ATM)
Examples of Policy Rules

### Table 1. Examples of RA-Policy

<table>
<thead>
<tr>
<th>RA-Policy: A</th>
<th>RA-Policy: B</th>
</tr>
</thead>
<tbody>
<tr>
<td>assignRole(Requester, NeutralBidder) ← newUser(Requester), requestType(Requester, buy).</td>
<td>changeRole(Requester, UnTrustedBidder) ← currentRole(Requester, NeutralBidder), shillingScore(Requester, X, current), X ≥ 0.6, reputationScore(Requester, Y, oneMonth), Y ≤ 0.7.</td>
</tr>
</tbody>
</table>

### Table 2. Examples of AC-Policy

<table>
<thead>
<tr>
<th>AC-Policy: A</th>
<th>AC-Policy: B</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow(Requester, Bid) ← currentRole(Requester, TrustedBidder), shillingScore(Requester, X, current), X ≤ 0.3, reputationScore(Requester, Y, current), Y ≥ 0.6.</td>
<td>disallow(Requester, Bid, oneWeek) ← currentRole(Requester, UnTrustedBidder), shillingScore(Requester, X, current), X ≥ 0.6, reputationScore(Requester, Y, current), Y ≤ 0.7.</td>
</tr>
</tbody>
</table>

Auction Data Analysis

- The reputation score is simply an accumulative value of the rating scores from other users.
- The shilling score of a user can be calculated using an **S-Point** system.

\[
\text{point}(U, 0).
\text{point}(U, P + 1) :\text{positive-indication}(U, PF), \text{point}(U, P).
\text{point}(U, P - 1) :\text{negative-indication}(U, NF), \text{point}(U, P).
\]

*point(U, P)* is a predicate that denotes user *U*’s accumulated *S-Points* is *P*. 
*positive-indication(U, PF)* is a predicate that denotes user *U* is a possible shill according to temporal formula *PF*. 
*negative-indication(U, NF)* is a predicate that denotes user *U* is not likely a shill according to temporal formula *NF*. 

04/07/2008   CIS Dept., UMass Dartmouth
Model Checking Technology

A Predicate for Positive Indication: after "start of Auction 1" until "end of Auction 0", does "(User A bids in Auction 0 && Price is lower in Auction 1) or (User A bids in Auction 1 && Price is lower in Auction 0) become true?"

\[
\text{((S1 \&\& \neg E0 \Rightarrow (\neg E0 U(P \&\& \neg E0)))) \mid \mid ((S0 \&\& E0 \Rightarrow \neg E0 U(S \&\& \neg E0)))}
\]

Decision Making Process

- The security agent determines whether a shill suspect (detected by a monitoring agent) is an actual shill.
- We propose to use evidence-based theory, e.g., the Dempster-Shafer theory (D-S theory) to support the decision making process.
- Currently, we are working on a Bayesian network with multi-state nodes
  - Calculate the probability of being a shill or a normal user
  - Use additional evidence such as trading history, win-ratio etc.
- Build a feasible intention model for bidding agents to support evaluation of agent behaviors.
Agent Communication Language

- Use asynchronous message passing for agent communication.
- FIPA-ACL is an agent communication standard
  - is grounded in speech act theory.
  - defines a set of 22 communicative acts.

```
(INFORM
 :sender (agent-identifier :name MonAgent-2@PT502989:1099/JADE
 :addresses (sequence http://192.168.1.100:7778/acc)))
:receiver (set (agent-identifier :name SecurAgent@PT502989:1099/JADE
 :addresses (sequence http://192.168.1.100:7778/acc)))
:content "Suspicious shill B2 detected!"
:language "Plain English"
:ontology "Online Auctions"
:protocol "shill Detection Protocol"
:conversation-id inform-shill-suspects)
```

Agent Communication Protocol
The Security Agent Interface

The Sniffer Agent
Conclusions and Future Work

- We introduced a framework for agent-based trust management for online auctions
- We demonstrated that the agents in the ATM module can effectively communicate with each other
- For our future work, we plan to develop efficient and effective trust management mechanisms
- Formalize shill patterns (and normal bidding patterns), and implement the model checking approach for efficient analysis of auction data
- Develop a prototype trustworthy agent-based online auction systems.

Questions?

The slides for this talk can be downloaded from
http://www.cis.umassd.edu/~hxu