Detecting Bad Moulthing Behavior in Reputation Systems
Kuan-Ta Chen (Chun-Yang Chen)\textsuperscript{1}, Cheng-Chun Lou\textsuperscript{2}, Polly Huang\textsuperscript{2}, and Ling-Jyh Chen\textsuperscript{1}
\textsuperscript{1}Academia Sinica, \textsuperscript{2}National Taiwan University

Background
- MMORPGs (Massively Multiplayer Online Role-Playing Games) have become extremely popular
- Game bots
  - Auto-playing game clients
  - One of the greatest threats of MMORPGs
- Detection of Game Bots
  - Manual detection (game master) \cite{1}
  - Traffic analysis approach \cite{2}
  - Voting-based system \cite{3}
  - Each player votes the suspicious player as a game bot

Motivation
- Problem in voting-based system
- Collusion
  - A secret agreement between two or more parties for a fraudulent, illegal, or deceitful purpose \cite{4}
  - Unfairly low ratings – bad moulthing
  - Unfairly high ratings – ballot stuffing
- Only can vote negatively (game bot)
  - This study focuses on bad-moulthing attacks

Problem Formulation
- Bad-Mouthing
  - A malicious group deliberately vote a legitimate player as a game bot
- Terms
  - Collusion Cluster: a bad-moulthing group
  - Victim: the legitimate players who are under bad-moulthing attacks
- Goal
  - To Detect the Collusion Clusters

Hypothesis
- The most voters of legitimate players are likely collusion cluster
- In case if a collusion cluster attacks for several times
  1. Collusion Cluster has more common voters than random voter cluster
  2. Victims have more common voters than random votee cluster
- Based-on
  - The voters \& votees id of each player
- Note
  - When not attack, a collusive player acts as a legitimate player

Voter-Based Collusion Cluster Detection
The relationship of collusion cluster is stronger than random votee cluster
Take the voters with more common voters between each other
- form the collusion cluster.

Voter-Voter-based Collusion Cluster Detection
The relationship of victim group is stronger than random votee cluster
First take the votes with more common voters
- form the victim group
Then take union of the voters of the victim group
- form the collusion cluster candidate

Performance Evaluation Results

<table>
<thead>
<tr>
<th># of Attack (Single CC or Multiple CC)</th>
<th>Voter-Based</th>
<th>Voter-Voter-Based</th>
<th>Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>More attacks</td>
<td></td>
<td></td>
<td>Voter-Voter &gt; Voter</td>
</tr>
<tr>
<td>Collusion Cluster Size</td>
<td></td>
<td>No influence</td>
<td>Need more than 3 high accuracy</td>
</tr>
<tr>
<td>Prob. of Collusive Player Attack</td>
<td></td>
<td>Higher Prob.</td>
<td>higher accuracy</td>
</tr>
<tr>
<td>Votee</td>
<td></td>
<td></td>
<td>Voter-Votee-Voter</td>
</tr>
</tbody>
</table>

Voter-Based scheme:
Robust to the size of collusion cluster
Voter-Votee-Based scheme:
Robust to the number of attacks

Conclusion
- Two mechanisms to detect the collusion cluster
  - Based on the voting history
  - Single cluster or multiple clusters
- Accuracy
  - Attack more than three times: 83%+
  - Attack more than five times: 97%+
- Adjust other experimental factors
  - Only collusion cluster size and prob. of collusive player attack vote have the obvious influence to the accuracy

Furture Work
Detecting players who participate in multiple collusion clusters

\cite{1} I. MacInnes and L. Hu, “Business models and operational issues in the chinese online game industry,” Telecommunications and Informatics, vol. 24, no. 2, pp. 130-144, 2007
\cite{3} Blizzard, http://www.blizzard.com/war3/
\cite{4} http://www.answers.com/collusion?cat=biz-fin