Detecting Bad Mouthing 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) [1]
  - Traffic analysis approach [2]
  - Voting-based system [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 [4]
    - Only can vote negatively (game bot)
    - This study focuses on bad-mouthing attacks

Problem Formulation

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

Hypothesis

- The most votes of legitimate players are likely collusion clusters
- In case if a collusion cluster attacks for several times
  1. Collusion Cluster has more common votes than random voter cluster
  2. Victims have more common votes than random votee cluster
- Based on
  - The voters & votees id of each player
  - 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 voter cluster

1. Take the voters with more common votes between each other
   - form the collusion cluster.

Votee-Voter-based Collusion Cluster Detection

The relationship of victim group is stronger than random votee cluster

1. 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

- # of Attack (Single CC or Multiple CC) More attacks > higher accuracy
- Collusion Cluster Size No influence > high accuracy
- Need more than 3 > high accuracy
- Prob. of Collusive Player Attack Vote Higher Prob. > higher accuracy

Conclusions

- 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