Detecting Cheating Behaviors in Cyber Competitions by Constructing Competition Network

Yuhong Liu and Yan (Lindsay) Sun
Department of Electrical, Computer and Biomedical Engineering, University of Rhode Island, Kingston, RI 02881
Emails: {yuhong, yansun}@ele.uri.edu

***Abstract*—Cyber Competition has been recognized as an efficient way to facilitate research and education in cyber security Cyber Competition has been recognized as an efficient way to facilitate research and education in cyber security field [1]–[3]. We have discovered that the participants (i.e. players) in cyber competitions can cheat in order to gain a higher rank or collect more prizes. In this work, we use data collected from the CANT competition to analyze such cheating behaviors and propose to build a competition social network to detect cheating behaviors in cyber competitions.**

I. Introduction

There is ample evidence that attackers insert unfair ratings into online rating systems, such as product rating at Amazon, hotel rating at Travelocity, and restaurant rating at Yelp, aiming to boost or downgrade the rating scores of certain products [4].

CANT is a cyber competition designed to collect real user attack data against online rating systems. In the competition, the normal rating data covered 300 products which were rated by 300 user IDs during 150 days. Players in the competition were required to control up to 30 user IDs, which are referred to as *malicious user IDs*, to downgrade the reputation score of a particular product.

The competition was launched on 05/12/2008 and lasted for 18 days. It successfully attracted more than 630 registered players and collected 826,980 valid submissions. Each submission contains a set of unfair ratings. The collected data set has been used to model human user attack behaviors and test attack-resistance properties of rating systems [5].

Cheating Behaviors in CANT: After the competition, we found an interesting cheating behavior. One participant (denoted by cheater C) registered 3 player IDs. These player IDs had taken the 2nd place, the 5th place, and the 32nd place respectively. The attack data submitted by these player IDs were similar. In the CANT competition, the top 19 players won cash prizes. By using pseudo player IDs, the cheater C increased his rewards.

Obviously, this type of cheating behaviors can happen in other cyber competitions. In many cyber competitions, the players submit different strategies and are rewarded according to how good their strategies are. If a cheater finds a good strategy, he can register extra pseudo player IDs and repeatedly submit the same/similar strategies, in order to defeat/discourage other players and obtain more rewards.

Proposed Solution Overview: A social network is a social structure described by network components, where "nodes" represent individuals and "edges" represent relationships among individuals. Social network is a powerful tool to model both individual behaviors and interactions of human players. We propose to understand and model the behavior patterns of cyber competition players from social networking point of view.

Existing social networks inherently describe collaboration among users. For example, Facebook users who are connected are friends. In this paper, we build a new type of social network called *competition social network*, in which two connected nodes represent two players who directly compete with each other in the cyber competition. Note that, the competition social network is a virtual concept, not a real social network such as Facebook.

II. Cheating in CANT Cyber Competition

Scoring method in the CANT competition: In the CANT competition, a player should register one and only one *player ID*. Each player ID can make many submissions. In a specific submission, the player can control up to U malicious user IDs, and insert up to R unfair ratings. All submissions are divided into groups according to: (1) the number of malicious user IDs and (2) the number of unfair ratings. Specifically, the group $G_{u,r}$ contains all submissions that use u malicious user IDs and r unfair ratings, where $0 < u \leq U$ and $0 < r \leq R$.

Within a group, the submission that yields the strongest attack (i.e. downgrading the reputation score of a specific product the most) is marked as the group winner. Note that there may be a tie, leading to multiple winners in one group. Let $W_{u,r}$ denote the set of submissions who are group winners of $G_{u,r}$. Let $s_{u,r}$ denote the size of $W_{u,r}$, i.e. the number of group winners in $G_{u,r}$.

In each group, the group winners equally split 1 point. If there is only one group winner in $G_{u,r}$ (i.e. $s_{u,r} = 1$) , the player who submits the group winner gains 1 point. If there are multiple group winners, each group winner will bring its player $1/s_{u,r}$ point. Specifically, assume that $k^P_{u,r}$ submissions in $W_{u,r}$ are submitted by player P. Then, the player P gain $k^P_{u,r}/s_{u,r}$ point in group $G_{u,r}$. The overall score of player P, denoted by S^P, is

$$S^P = \sum_{r=1}^{R} \sum_{u=1}^{U} \frac{k^P_{u,r}}{s_{u,r}}.$$

Consequence of cheating behavior: In many cyber competitions, the rewards are given to a few top players (e.g. top 19 players in CANT). Without pseudo IDs, a player can only win one prize. By sharing the winning strategies with a pseudo ID,

WIFS' 2011, November 29th-December 2nd, 2011, Foz do Iguaçu, Brazil.
This work is supported by NSF #0643532 and NSF #0931820.

the cheating player may win another prize and increase his/her "reward income". Only a few pseudo IDs can be sufficient to mess up the ranking and reward system. This is exactly what happened in the CANT competition. Therefore, new approaches to detect such cheating behaviors are on demand.

III. Competition Social Network

Social networks are traditionally used to describe and facilitate collaboration. Can social network concept be used in a competition environment, in which nodes (i.e. players) have to defeat one another to achieve their goals? In this work, we define a competition network, in which the nodes' behaviors are dramatically different from these in collaborative social networks. In the context of CANT competition, we introduce the following concepts.

- **Competition relationship** exists and only exists between two player IDs when they have submissions belonging to the same $W_{u,r}$ (i.e. group winners of $G_{u,r}$).
- **Competition value** is computed for each pair of players with competition relationship. Assume $t^i_{u,r}$ denote the points obtained by player P_i in group $G_{u,r}$. If we define $H^{i,j}_{u,r} = \begin{cases} 0 & \text{if } t^i_{u,r} \cdot t^j_{u,r} = 0 \\ 1 & \text{if } t^i_{u,r} \cdot t^j_{u,r} \neq 0 \end{cases}$, the competition value from P_i to P_j is
$$V_{p_i->p_j} = \sum_{u=1}^{U} \sum_{r=1}^{R} t^i_{u,r} \cdot H^{i,j}_{u,r},$$
and similarly, the competition value from P_j to P_i is
$$V_{p_j->p_i} = \sum_{u=1}^{U} \sum_{r=1}^{R} t^j_{u,r} \cdot H^{i,j}_{u,r}.$$
- The **competition degree** of a node is the number of links connected to this node in the competition network.

Although we focus on the CANT competition in this paper, the concept of competition network can be extended to other cyber competitions as long as one can define quantitative competition value between two players.

We divide the overall time of the competition into $N = 36$ equal time frames, where one frame roughly represents half day. The competition network is updated at the end of each frame.

IV. Detection of Cheating Behaviors

We refer to the main ID controlled by the cheater as the original ID, and the other IDs controlled by the cheater as the *pseudo IDs*. We have made three major observations. *First*, the pseudo IDs often submit a large amount of winning submissions within a short time, leading to a sudden increase in the competition degree. *Second*, since a pseudo ID uses the similar attack strategies as the original ID, they always compete with each other. The competition value from the pseudo ID to the original ID is much larger than the competition value from the pseudo ID to other player IDs. *Third*, as the competition goes on, a normal player will compete with more and more players, leading to a larger and larger competition degree. The pseudo IDs, however, tends to have a smaller competition degree.

We then detect the cheating players in three steps.

	Ground Truth	The proposed scheme	Score based scheme
Pseudo ID	5, 32	5, 20, 32	5
Original ID	2	2, 1	None

TABLE I: Comparison result summary

1. At the end of the competition, if a player ID's competition degree is much smaller than the average competition degree of other players, this player ID is marked as a pseudo player ID.
2. If a player ID experiences sudden increase in the competition degree, this player ID is marked as a pseudo player ID.
3. If the competition value between a player ID and an identified pseudo player ID is much higher than the average competition value, this player ID is marked as the original ID of the cheater.

V. Results

After the competition, the players reported a cheater (original ID 2, pseudo ID 5 and 32). We have confirmed this cheating behavior through offline investigation. This serves as the ground truth in our experiments. It is important to point out that our ground truth is not complete. In other words, we know there is one cheater for sure, but do not know whether there are other cheaters.

With the proposed scheme, we detect 3 player IDs: player ID 5, 20 and 32 as pseudo player IDs. Among them, player 5 and 20 experience sudden increase in their competition degrees. Player 32 has a very low competition degree (< 4) during the whole competition, whereas other players' degrees are at least 13 at the final stages. Furthermore, we identify that player 5 is the pseudo ID of player 2, and player 20 is the pseudo ID of player 1.

We compare the proposed detection scheme with a simple score-based scheme. In the score-based scheme, a player is considered as pseudo player if his/her score suddenly increases. With simple score based scheme, we can detect player ID 5 as a pseudo player ID. The original player ID that is associated with the pseudo player ID cannot be determined. The detailed results are shown in Table I.

Obviously, the proposed scheme, compared with the score-based scheme, has two advantages: (1) more accurate detection results and (2) capable of identifying the original ID of the cheater.

References

[1] M. Gomez, J. Sabater-Mir, J. Carbo, and G. Muller, "Improving the art-testbed, thoughts and reflections," in *Workshop on Competitive agents in Agent Reputation and Trust Testbed*, Salamanca, 2008, pp. 1–15.

[2] J. Werther, M. Zhivich, T. Leek, and N. Zeldovich, "Experiences in cyber security education: The mit lincoln laboratory capture-the-flag exercise," in *Cyber Security Experimentation And Test*, 8 August 2011.

[3] *CANT*, http://www.ele.uri.edu/nest/cant.html.

[4] C. Dellarocas, "Strategic manipulation of internet opinion forums: Implications for consumers and firms," *Management Science*, vol. 52, no. 10, pp. 1577–1593, Oct 2006.

[5] Y. Liu and Y. Sun, "Anomaly detection in feedback-based reputation systems through temporal and correlation analysis," in *Proc. of 2nd IEEE Int. Conf. on Social Computing*, Aug 2010.