Combining ranking concept and social network analysis to detect collusive groups in online auctions

Shi-Jen Lin\textsuperscript{a}, Yi-Ying Jheng\textsuperscript{a}, Cheng-Hsien Yu\textsuperscript{a,b,*}

\textsuperscript{a} National Central University, Jhongli City, Taoyuan, Taiwan
\textsuperscript{b} China University of Technology, Hukou, Hsinchu, Taiwan

\textbf{A B S T R A C T}

Due to the popularity of online auction markets, auction fraud has become common. Typically, fraudsters will create many accounts and then transact among these accounts to get a higher rating score. This is easy to do because of the anonymity and low fees of the online auction platform. A literature review revealed that previous studies focused on detection of abnormal rating behaviors but did not provide a ranking method to evaluate how dangerous the fraudsters are. Therefore, we propose a process which can provide a method to detect collusive fraud groups in online auctions. First, we implement a Web crawling agent to collect real auction cases and identify potential collusive fraud groups based on the k-core clustering algorithm. Second, we define a data cleaning process to remove the unrelated data. Third, we use the Page-Rank algorithm to discover the critical accounts of the groups. Fourth, we developed a ranking method for auction fraud evaluation. This method is an extension of the standard Page-Rank algorithm and combines the concepts of Web structure and risk evaluation. Finally, we conduct experiments using the Adaptive Neuro-Fuzzy Inference System (ANFIS) neural network and verify the performance of our method by applying it to real auction cases. In summary, we find that the proposed ranking method is effective in identifying potential collusive fraud groups.

\textsuperscript{*} Corresponding author at: China University of Technology, Hukou, Hsinchu, Taiwan.

\textit{E-mail addresses: sjlin@mgt.ncu.edu.tw (S.-J. Lin), chyu@cute.edu.tw (C.-H. Yu).}

\textcopyright 2012 Elsevier Ltd. All rights reserved.

\textbf{1. Introduction}

Due to the popularity of the online auction markets, auction fraud has become common. According to an Internet Fraud Report (2003–2009) issued by the Internet Crime Complaint Center (IC3), a joint operation between the FBI and the National White Collar Crime Center (NW3C), the number of complaints about Internet fraud increased from 1400 per month in 2001 to 22,940 per month in 2008. From January 1, 2008 to December 31, 2008, IC3 received a total of 275,284 complaints, representing a 33.1% increase over the previous year. The total amount lost increased from $17 million in 2001 to $264 million in 2008. The total dollar loss linked to online fraud in 2008 was $264 million, about $25 million more than in 2007. Regarding the variety of fraud types, non-delivery of merchandise ranked number one (32.9%). Internet auction fraud was the second most reported offense (25.5%) (IC3, 2009). These figures indicate that online auction fraud causes significant losses.

This type of fraud is actually facilitated by the seller reputation rankings displayed on the most popular online auction sites, such as Yahoo and eBay. Because these rankings are based on a simple feedback mechanism, auctioneers can take advantage of the anonymity and the low online auction fees to create multiple accounts and increase their rating scores via sham transactions. In this way, they can deceive the buyer with their high rating score. Related studies also show that the most severe cases of Internet fraud, accounting for millions of dollars of loss, were reported by those who were misled by evaluation feedback (Griggs, 2003; Han, 2003; Wilke & Wingfield, 2003).

Despite these facts, previous studies on Internet auction fraud focused on the detection of abnormal rating behaviors of known auction fraud groups (Wang & Chiu, 2008) or focused on the classification of types of auction fraud (Pandit, Chau, Wang, & Faloutsos, 2007). Thus, they did not rank the degree of suspicion associated with each account of an auctioneer group. Furthermore, they did not provide an easy way for users to obtain the relevant information to evaluate collusive groups.

Therefore, we propose a process which can provide a ranking method to evaluate collusive fraud groups in online auctions. First, we implement a Web crawling agent to collect real auction cases and identify potential collusive fraud groups based on the k-core clustering algorithm. Second, we define a data cleaning process to remove the unrelated data. Third, we use the Page-Rank algorithm to discover the critical accounts of the groups. Fourth, we provide a ranking method for auction fraud evaluation. This method is extended from the standard Page-Rank algorithm and combines the concepts of Web structure and risk evaluation. Finally,
we conduct experiments using the Adaptive Neuro-Fuzzy Inference System (ANFIS) neural network and verify the performance of our method by applying it to real auction cases. In summary, we find that the proposed ranking method is effective in identifying a potential collusive fraud group.

2. Literature review

In this section, we survey the related approaches for online auction fraud detection and then review the social network analysis which is used to analyze the auctioneers' interactions. We also review the related work on the Page-Rank algorithm which will be applied to our Auction Fraud Rank algorithm.

2.1. Fraud detection in online auctions

According to the literature, fraud detection approaches can be classified into three kinds of methods: statistical methods, data mining techniques, and formal methods (Dong, Shatz, & Xu, 2009a). With regard to statistical methods, Rubin et al. (2005) propose a new reputation system for auction sites to help users protect their interests by warning them of the risk of auction fraud. The model uses three variables (average number of bids, average minimum starting bid, and bidders’ profiles) to identify whether an account shows activity typical of shill biddings (Rubin et al., 2005). Other researchers also use statistical methods to detect behaviors of fraudsters (Dong, Shatz, & Xu, 2009b; Trevathan & Wing, 1996). Use of a formal approach to detect shilling of software and hardware designs. Xu and Cheng (2007) and Clarke et al. (2007) propose the NetProbe approach, which models auctioneers with their transactions as a Markov Random Field to detect the fraudsters' suspicious patterns. It also constructs a belief propagation mechanism to detect similar fraudsters (Pandit et al., 2007). Formal notation and logic are used in mathematically rigorous techniques for the specification, development, and verification of software and hardware designs. Xu and Cheng (2007) and Clarke and Wing (1996) use a formal approach to detect shilling behaviors.

Recently, Wang and Chiu (2008) used social network analysis (SNA) indicators based on k-core and centered-weights algorithms to detect auction fraud groups because of the normal transactions do not have a complicated relationship. However, if collusive auctioneers are to manipulate their reputation, they must have transactions among themselves. Thus, collusive auctioneers' transactions have a complicated relationship and have the high-core characteristic in the transactional structure. Taking a structural perspective by focusing on the relationships between traders rather than their attribute values, Wang and Chiu used k-core and centered-weights algorithms to create a collaborative-based recommendation system that could suggest risks of collusion associated with an account (Wang & Chiu, 2005, 2008).

2.2. Page-Rank algorithm

Web mining is the application of data mining techniques to discover patterns from the Web. It also could be generalized into three different types: Web usage mining, Web content mining, and Web structure mining (Cooley, Mobasher, & Srivastava, 1997, 1999; Srivastava, Cooley, Deshpande, & Tan, 2000). Web usage mining ascertains user profiles and the users’ behaviors recorded inside the Web log file. Web content mining is the application of data mining techniques to unstructured or semi-structured data, usually HTML documents. Web content mining attempts to discover useful information from Web content. Web structure mining analyzes the hyperlink structure of the Web to discover relationships between Web pages. Based on the topology of the hyperlinks, Web structure mining categorizes Web pages and generates related patterns, such as the similarity and the relationships between different Web sites.

Recently, many researchers have applied social network analysis (SNA) combined with the Google’s Page-Rank algorithm, the Hyperlink-induced Topic Search (HITS) algorithm, or other pagerank algorithms to generate useful information for users (Jamali & Abolhassani, 2006; Mislove, Gummad, & Druschel, 2006; Pujol, Sangüesa, & Delgado, 2002). Thus, we also use SNA as the frame and combine ranking algorithms to evaluate the importance of an account in the transactional group.

The Page-Rank vector of citation ranking weight was introduced by Brin and Page (1998). The idea introduces a notion of page authority which is independent of the page content. Iterative graph-based ranking algorithms provide a way of deciding the importance of a vertex within a graph and of deciding the importance of a page on the Web. Page-Rank is defined as:

$$PR(u) = \frac{(1 - d)}{N} + d \sum_{v \in R(u)} \frac{PR(v)}{N_v}$$

where $u$ represents a web page; $d$ is a dampening factor that is usually set to 0.85; $R(u)$ is the set of pages that point to $u$; $PR(u)$ and $PR(v)$ are rank scores of page $u$ and $v$, respectively; $N_v$ denotes the number of outgoing links of page $v$; and $c$ is a factor used for normalization.

The Page-Rank algorithm states that a page that is linked to many pages with high Page-Ranks receives a high rank itself. A popular page is often referred to by other pages and that an important web page contains a high number of out-links. Furthermore, the structure of collusive transactions conforms to the characteristics of the Page-Rank algorithm. An account that has many transactions in the collusive group is considered an important account; if a page has important links connected to it, its out-linking pages will also become important pages. Thus, the Page-Rank algorithm can be used to discover authoritative and important accounts. We will modify the Page-Rank algorithm to build our Auction Fraud Rank algorithm to find the potential risk of accounts in the group.

2.3. Social network analysis

SNA is the study of social relations among a set of actors, and actors can be individuals, organizations, or communities (Borgatti, 2010). It is used widely in the social and behavioral sciences, as well as in political science, economics, organizational science, and industrial engineering (Garton, Haythornthwaite, & Wellman, 1999; Wellman, 1996). The network perspective has proved fruitful in a wide range of social and behavioral science disciplines (Wasserman & Faust, 1994). The basic components of an SNA study are the actor or node and the connection or link (Borgatti, 2010). The nodes can be individual, corporate, or collective social units, and nodes are linked to one another by ties (Wasserman & Faust, 1994).

Divisions of actors into subgroups can be a very important aspect of social structure that can help explain how the network as a whole is likely to behave. A subgroup can be identified by the measurements of clique, k-plex, and k-cores (Everett, 1982; Everett & Borgatti, 1998; Hanneman & Riddle, 2005; Liu & Terzi, 2008; Wu, Xiao, Wang, He, & Wang, 2010; Zhou & Pei, 2008). The strongest possible clique is a given number of actors who have all possible ties present among themselves. A maximal complete sub-graph is such a grouping, expanded to include as many actors as possible (Johnson & Trick, 1996), as shown in Fig. 1.

$k$-Plex is an alternative way of relaxing the strong assumptions of the maximal complete sub-graph. $k$-Plex allows that actors may...
be members of a clique even if they have ties to all but k other members (Everett, 1982). In Fig. 2, the subgroup depicted, which includes \((a, b, c, d)\), is a 2-plex group.

K-Core is a maximal sub-graph in which each node is adjacent to at least k other points. It is also thought to be an essential complement to the measurement of density, which may not capture many of the features of the global network (Scott, 2002). The mathematical definition of k-core is:

Let \(G = (V, L)\) be a graph. \(V\) is the set of vertices and \(L\) is the set of lines (edges or arcs). We will denote \(n = |V|\) and \(m = |L|\). A subgraph \(H_k = (W, L(W))\) induced by the set \(W\) is a k-core or a core of order \(k\) iff \(\forall v \in W: \text{deg}_G(v) \geq k\), and \(H_k\) is the maximum subgraph with this property.

As shown in Fig. 3, the subgroup, which includes \((A, B, C, D, E, F)\), is a 2-core group.

In previous research (Wang & Chiu, 2005, 2008), the k-core indicator was used to reveal the cohesiveness of an account’s trading relationship as well as the reputation structures derived from transaction histories, since frequently engaged accounts will form subgroups that can be captured by the k-core indicators. Through use of the k-core indicator, malicious traders can be distinguished from the normal accounts. However, if we only use k-core to identify cohesive accounts, it will have high false negative and false positive results. As shown in Fig. 3, the subgroup, which includes \((A, B, C, D, E, F)\), is a 2-core subgroup. We assume that \((A, B, C, D, E, G)\) are collusive accounts and \(F\) is a normal account. \(G\) was only used to manipulate reputation one time, but it is not a member of the 2-core subgroup. Thus, \(F\) becomes a member of the 2-core subgroup. If we only use k-core to identify collusive accounts, we will falsely identify \(F\) as a member of the collusive accounts and \(G\) as a normal account. Using the approach of Wang et al., high false negative and false positive results would be derived because many members of the 2-core subgroup have possible links to the normal accounts and members of the 1-core subgroup have possible links to the collusive accounts. In order to solve the above problems, other indicators are needed. Furthermore, Wang et al.’s approach cannot fit all real-world cases. In fact, the 2-core subgroup will often appear in the real auction environment, but not all of the 2-core subgroups are collusive groups.

3. Ranking method

3.1. Auction Fraud Rank algorithm

In this section, we will introduce our ranking method, the Auction Fraud Rank algorithm. We modify the standard Page-Rank algorithm to match the collusive structure. The Auction Fraud Rank algorithm is a combination of Web structure and potential risk perspectives. It is more suitable for use in identifying collusive subgroups than the standard Page-Rank algorithm. The Auction Fraud Rank is as follows:

\[
\text{AFR}(u) = \left(1 - d\right) + d \sum_{v \in B(u)} \frac{\text{PR}(v)}{N_v} + \frac{1}{\text{Date_Difference}} \times \frac{1}{\text{Credit}} + \text{Core}_i
\]

- \(\text{Date}_\text{Difference}\), represents days between the first transaction date of account and the average first transaction date of the group. If \(\text{Date}_\text{Difference}\) is 0, \(\text{Date}_\text{Difference}\) will be 1.
- \(\text{Credit}\), represents the account’s rating scores. If \(\text{Credit}\) is 0, \(\text{Credit}\) should equal to 1.
- \(\text{Core}\), represents the account’s core value. If the account is a member of a 1-core subgroup, \(\text{core}\) should equal to 0. If the account is a member of a 2-core subgroup, \(\text{core}\) should equal to 0.

If the Auction Fraud Rank value is close to 10, it means that the relevance between the account and the subgroup is very high; otherwise, if the value is equal to 0, the relevance is very low, so that the account might be ranked behind.

The mathematic definition of Date_Difference, is:

\[
\text{Date}_\text{Difference} = \text{Date}_i - \frac{1}{k} \sum_{j=1}^{k} \text{Date}_j/k
\]

- \(\text{Date}\), represents the date of the first transaction recorded for a user’s account (unit: day).
- \(\sum_{j=1}^{k} \text{Date}_j/k\) represents the average first transaction date of top-\(k\) accounts (unit: day).

In the real auction environment, the first transaction dates of the collusive group are very close, due to the fact that malicious
auctioneers create multiple accounts and manipulate their transactions in order to create high reputations in a short time. Thus, we add Date_Difference and Credit, to the Auction Fraud Rank algorithm. In order to calculate Date_Difference, we have to find the core accounts in the group. The Page-Rank algorithm can rank web pages according to ingoing and outgoing links. Wang and Chiu (2008) showed that collusive auctioneers have a complicated relationship and high core in the transaction structure. Thus, we will use the Page-Rank algorithm to discover each account's importance and find the core accounts in this group. If the account's ranking position is higher, it is possibly one of the core members. If this group is a collusive group, our method will identify those core accounts that very possibly are attributable to the primary fraudsters. After calculating the ranking position of accounts, we have to decide how many accounts (top-k) can represent core accounts in different groups. Because the user inputs different accounts, our system will collect related account numbers according to the transaction structure of the accounts so entered. We use the concept of SNA indicators, k-core, to decide k minimum. The minimum k is 3 because a group forms a 2-core subgroup from at least three accounts. If the group numbers increase every 10 accounts, k will add 1 in order to avoid only three accounts representing the first transaction date of the bigger subgroup. The account and k value are as shown in Table 1.

In the previous section, we did not determine all 2-core account to be core accounts because the normal accounts may be in the 2-core subgroup. If normal accounts are in the 2-core subgroup, the normal accounts' first transaction dates will be very different. This would influence the average of the first transaction date. On the other hand, we do not consider 3-core or 4-core accounts as core accounts because not every collusive group will have a transaction structure above 3-core. In the real auction environment, it is possible that collusive groups are the hub type. It is hard to decide k-core value. However, if we use the Page-Rank algorithm to calculate Page-Rank values and rank positions, we are not restricted by the transaction structure. Even though the execution time of Page-Rank is high, it does not require a lot of resources to implement in our system.

We use the example to explain the Auction Fraud Rank algorithm. As Fig. 4 shows, we suppose that A, B, C, D, E, F, G, J, K, W, X, Y, Z are collusion accounts and T, S, U, V are normal accounts. In the study of Pandit et al. (2007), the accounts in the collusion group are split into two categories: fraud and accomplice. It means that in the collusion group, most of the 1-core subgroup, which includes (B, G, F, E), is the accomplice and most of the 2-core subgroup, which includes (A, C, D, J, K), is the fraud. In addition, we consider that accomplices and fraudsters can behave like legitimate users and sometimes interact with other honest users to prevent the group being discovered as fraudulent. Why not directly use the standard Page-Rank algorithm to rank the position of collusion accounts? And why do we use these three parameters? The reasons are as follows:

1. If we use the standard Page-Rank algorithm to calculate the Page-Rank value of each account, the Page-Rank value of each account is the same among 1-core subgroups which include (B, G, F, E) and (T, S, U, V). Thus, the standard Page-Rank algorithm only can find which accounts are core accounts in the group but cannot determine the difference among 1-core accounts.

2. The Auction Fraud Rank algorithm which we adapted from the standard Page-Rank algorithm can reveal the underlying risk of the traders. If (B, E, F, G) are collusion members, their Date_Difference and Credit are less than those of normal accounts. Using the Auction Fraud Rank algorithm, their Date_Difference and Credit are small, and the Auction Fraud Rank value is relatively high. Meanwhile, Credit can lower the influence of Difference to the Auction Fraud Rank value. Because some collusion groups may stretch layout time to avoid being easily discovered, the first transaction date will not be so close, but the collusion groups’ reputation will still be small.

3. Core also plays an important role. If the account is one of the 2-core subgroup’s members, this account is more dangerous than the 1-core subgroup’s accounts. If this account is not a collusion account, we can use Date_Difference and Credit to lower the sensitivity of Core, to influence the Auction Fraud Rank value.

### Table 1

<table>
<thead>
<tr>
<th>Account numbers</th>
<th>Top-k value</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td>20</td>
<td>4</td>
</tr>
<tr>
<td>30</td>
<td>5</td>
</tr>
<tr>
<td>40</td>
<td>6</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Fig. 5. The black list of Yahoo auction site in Taiwan.
Yahoo Auction Site (http://www.tw.bid.yahoo.com) and Ruten Auction Site (http://www.ruten.com.tw) which are the biggest auction sites in Taiwan. As Figs. 5 and 6 shows, both of these two auction sites will publish the black list of accounts periodically. The six black accounts that have collusive fraud behaviors and in the black list were chosen by manual verified. The crawler will start crawling from these six black accounts to find out the black-related transaction network members and use to train our ranking method. Finally, the 259 related members were found in the six black-related networks. As Fig. 7 shows, the one of the black-related transaction networks has the 2-core topology. Details of the crawler implementation are as follows:

- We propose an Auction Crawler Agent algorithm that can unearth suspicious network patterns. We use the concept of a 2-core clustering algorithm to design our searching path for the Agent in order to capture the potential collusive group completely and immediately. First, the Auction Crawler Agent crawls the account data and record accounts that leave feedback in the listing in a breadth-first fashion. Second, the Auction Crawler Agent determines whether the current has 2-core accounts after searching the second layer. If the current structure has 2-core accounts, the Auction Crawler Agent will focus on them while searching the next layer. This step will loop until the Agent does not find 2-core accounts. Third, the Auction Crawler Agent will determine whether the 2-core accounts have listing feedbacks. If our record reveals listing feedbacks for 2-core accounts, the Auction Crawler Agent will focus on these accounts while searching the next layers and the system will go back to the second step. The stop condition of the Agent is that the transactional structure does not have a 2-core subgroup and our records do not include listing feedbacks of 2-core accounts or the system has been searching to the third layers.
- Auction Crawler Agent is developed by Java. Our system offers an interface to the user, whereby the user can simply input an account number.
- After the Auction Crawler Agent collects accounts, we can reconstruct the network graph of transactions between accounts.

We know that the 2-core indicator can determine the parts of a collusive group (Wang & Chiu, 2005, 2008), but if we only consider the 2-core indicator, it will bring the high false-negative results. In the data collection, we’ll make sure that the case is in the collusive fraud group. According to the definition of collusive fraud group, the malicious auctioneers create multiple accounts and manipulate their transactions to create reputations.

4.2. Experiment design

In the experiment, we apply the ANFIS to evaluate the risk of each account in the group. Fig. 8 shows the model used in this research for fraud data identification. The ANFIS takes three inputs (Date_difference, Credit, Auction Fraud Rank value) and has one output (the account’s risk). To realize this, we developed an ANFIS with five layers. The ANFIS approach uses Gaussian functions for fuzzy sets, Takagi and Sugeno’s fuzzy algorithm, and singleton fuzzy rule for the if-then rules. The initial parameters of the network are the mean and standard deviation of the membership functions (antecedent...
parameters) and consequent parameters. The output of each rule is a constant term. The final output is the weighted average of each rule's output, and it represents the risk of the account. The ANFIS learning algorithm is used to obtain and adjust the parameters of the fuzzy terms and consequent output. The rule parameters are recursively updated until an acceptable error is reached. We apply the back-propagation and hybrid algorithm separately to compare which algorithm will have the better accuracy. The output error is defined as follows:

\[ E = \sum_j (d_j - y_j)^2 \]  

where \( d_j \) represents the real value (if the account \( j \) is a collusive fraud account, the value is equal to be 1; otherwise, if the account, is a normal account, the value is equal to be 1) and \( y_j \) is the system output value.

In the experimental design, we collected collusive fraud group cases in advance. We randomly chose two cases as testing data and others as training data. We used training data to train rules and parameters of ANFIS and used testing data to validate the system effectiveness. We repeated this experiment three times. Then we predicted whether the account is a collusive account when the output of system is higher than the threshold. We used mean value (the dangerous mean of the training data) – standard deviation (the dangerous standard deviation of the training data) as the threshold to contain most of the collusive accounts. Table 2 is a confusion matrix that summarizes the number of instances predicted correctly or incorrectly by such a classification model.

5. Results and discussion

5.1. System performance

In this section, we will discuss the performance of our AFR ranking method in the learning algorithms. Compare the precision and recall rates between the back-propagation learning algorithm and hybrid algorithm, it shows the results in Tables 3 and 4. We found that the recall rate of our system on average is 98.3% and the average F-measure is 92.2%. These results show that our approach is effective for collusive group detection in online auctions.

5.2. Comparison with other studies

For comparison with other studies, we applied Wang and Chiu (2005) approach to our collected data. The results are shown in Table 5.

As we can see in Table 5, the precision rate is above 70%, but the recall rate is not stable in some data. The reason is that if we only use 2-core accounts to detect fraudsters, we will miss 1-core accounts. On the other hand, 1-core accounts are possible as potential collusive accounts. Thus, the Wang et al. approach will have high false-negative results.

In order to improve the precision rate, Wang and Chiu (2008) use the robbery algorithm to find central accounts of the SNA map. The robbery algorithm is as follows:

- The center measurement starts with one account's linking degrees as initial weights or starts with initial weights 1.

<table>
<thead>
<tr>
<th>Table 2</th>
<th>A confusion matrix for a binary classification problem.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual class</td>
<td>Collusive account</td>
</tr>
<tr>
<td>Predicted class</td>
<td>tp (true positive)</td>
</tr>
</tbody>
</table>

Precision = TP/TP + FP  
Recall = TP/TP + FN  

\[ F - \text{measure} = 2/(1/\text{precision rate} + 1/\text{recall rate}) \]  

Fig. 8. ANFIS model of fuzzy interference.
rithm to evaluate our test data. The result of Wang et al.'s approach
Chiu (2008). On the other hand, we also applied the robbery algo-
 centered degree weights greater than zero and is identified as
tered degree weight drop down to zero. The other group has the
Precision rate and recall rate of Wang et al.'s approach.
Table 6
<table>
<thead>
<tr>
<th>Data set</th>
<th>Precision rate (%)</th>
<th>Recall rate (%)</th>
<th>F-measure (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. 1</td>
<td>80</td>
<td>100</td>
<td>89</td>
</tr>
<tr>
<td>No. 2</td>
<td>94.12</td>
<td>100</td>
<td>96.97</td>
</tr>
<tr>
<td>No. 3</td>
<td>90.91</td>
<td>100</td>
<td>95.24</td>
</tr>
<tr>
<td>No. 4</td>
<td>90.91</td>
<td>100</td>
<td>95.24</td>
</tr>
<tr>
<td>No. 5</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>No. 6</td>
<td>50</td>
<td>50</td>
<td>50</td>
</tr>
</tbody>
</table>

Table 4
<table>
<thead>
<tr>
<th>Data set</th>
<th>Precision rate (%)</th>
<th>Recall rate (%)</th>
<th>F-measure (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. 1</td>
<td>72.73</td>
<td>100</td>
<td>84.21</td>
</tr>
<tr>
<td>No. 2</td>
<td>94.12</td>
<td>100</td>
<td>96.97</td>
</tr>
<tr>
<td>No. 3</td>
<td>81.82</td>
<td>90</td>
<td>85.71</td>
</tr>
<tr>
<td>No. 4</td>
<td>90.91</td>
<td>100</td>
<td>95.24</td>
</tr>
<tr>
<td>No. 5</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>No. 6</td>
<td>83.33</td>
<td>100</td>
<td>90.9</td>
</tr>
</tbody>
</table>

Table 5
<table>
<thead>
<tr>
<th>Data set</th>
<th>Precision rate (%)</th>
<th>Recall rate (%)</th>
<th>F-measure (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. 1</td>
<td>78</td>
<td>78</td>
<td>78</td>
</tr>
<tr>
<td>No. 2</td>
<td>84.61</td>
<td>75</td>
<td>78.57</td>
</tr>
<tr>
<td>No. 3</td>
<td>72.7</td>
<td>100</td>
<td>84.21</td>
</tr>
<tr>
<td>No. 4</td>
<td>100</td>
<td>42.11</td>
<td>57.14</td>
</tr>
<tr>
<td>No. 5</td>
<td>100</td>
<td>85.71</td>
<td>92.31</td>
</tr>
<tr>
<td>No. 6</td>
<td>100</td>
<td>40</td>
<td>57.14</td>
</tr>
</tbody>
</table>

- If an account has higher degree (is stronger) than its neighbors, it will steal all degrees from neighbors. All the weights originally associated with the “weak” nodes in the graph/network will be reduced to zero.

This center algorithm generates two groups of accounts from our testing data; one group of accounts was “robbed” to have centered degree weight drop down to zero. The other group has the centered degree weights greater than zero and is identified as potentially suspicious accounts using the method of Wang and Chiu (2008). On the other hand, we also applied the robbery algorithm to evaluate our test data. The result of Wang et al.’s approach with centers is shown as Table 6.

As we can see in Table 6, the robbery algorithm can help to improve precision rate, but the recall rate drops dramatically. The reason is that accounts which are bigger than zero are almost 2–3 accounts. Although we can correctly identify fraudulent accounts, the false positive rate is too high. In data set no. 3, we used the robbery algorithm to detect malicious accounts, and the result is that only one account’s value is bigger than zero and this account is not a collusive account. Therefore, the precision rate and recall rate of this data set are both zero.

Table 6
<table>
<thead>
<tr>
<th>Data set</th>
<th>Precision rate (%)</th>
<th>Recall rate (%)</th>
<th>F-measure (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. 1</td>
<td>100</td>
<td>33.33</td>
<td>50</td>
</tr>
<tr>
<td>No. 2</td>
<td>100</td>
<td>11.76</td>
<td>21</td>
</tr>
<tr>
<td>No. 3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>No. 4</td>
<td>100</td>
<td>18.18</td>
<td>30.77</td>
</tr>
<tr>
<td>No. 5</td>
<td>100</td>
<td>14.29</td>
<td>25</td>
</tr>
<tr>
<td>No. 6</td>
<td>100</td>
<td>11.11</td>
<td>20</td>
</tr>
</tbody>
</table>

Finally, we compared the approach of Wang and Chiu (2008) to ours. The performance of F-measures is shown as Fig. 9. According to the figure, we can find the performance of our approach is higher than that of the approach of Wang et al. Both of the back-propagation and hybrid learning algorithms have good performance in detecting the fraudster accounts. The back-propagation learning algorithm is recommended to use to build the model. In addition, the hybrid learning algorithm has a good performance too.

6. Conclusions
In summary, we propose a new ranking method for collusive group detection in online auctions and applied it to a real-world online auction site. The ranking method includes new indicators that are the Date Difference and the AFR value more than previous studies (Wang and Chiu (2008)), so this method can provide better performance than the previous approaches. In future work, we will expand the data sets and add more indicators and learning algorithms to fit the fraudsters’ fast-changing behaviors.

References


