# Reputation inflation detection in a Chinese C2C market

Weijia You [a,c], Lu Liu [a], Mu Xia [b,*], Chenggong Lv [a]

[a] School of Economics and Management, Beihang University, Beijing 100191, PR China
[b] Leavey School of Business, Santa Clara University, Santa Clara, CA 95053, USA
[c] School of Economics and Management, Beijing Forestry University, Beijing 100191, PR China

## ARTICLE INFO

## ABSTRACT

In consumer-to-consumer (C2C) markets, sellers can manipulate their reputation by employing a large number of puppet buyers who offer positive feedback on fake transactions. We present a conceptual framework to identify the characteristics of collusive transactions based on the *homo economicus* assumption. We hypothesize that transaction-related indicators including price, frequency, comment, and connectedness to the transaction network, and individual-related indicators including reputation and age can be used to identify collusive transactions. The model is empirically tested using a dataset from Taobao, the largest C2C market in China. The results show that the proposed indicators are effective in identifying collusive traders.

## 1. Introduction

Reputation systems are essential to consumer-to-consumer (C2C) e-commerce. Because of the separation of payment and delivery, transactions among geographically distant strangers are inherently risky (Hawes and Lumpkin 1986, Friedman and Resnick 2001). Reputation mechanisms (Tirole 1996), which report users' feedback on historical transactions, play crucial signaling and sanctioning roles (Dellarocas 2005). Designed to deter frauds by users, reputation systems are employed by the most popular online C2C shopping websites such as eBay, Amazon, Yahoo Auctions and Taobao. Indeed, numerous empirical studies have demonstrated that, in many cases, reputations systems are effective in predicting future performance of users and preventing online auction fraud (Resnick and Zeckhauser 2002, Macinnes et al. 2005, Gregg and Scott 2006).

Despite the widespread use of online reputation systems, a significant amount of online fraud has been reported. According to the 2009 Internet Crime Report (Internet Crime Complaint Center 2009), "non-delivered merchandise and/or payment" and "auction fraud" represented 30.2% of the 336,655 complaints filed in the US, accounting for US$559.7 million in losses. In China, according to the 2009 Online Shopping Report (iResearch 2009), 23.0% of the 21,657 complaints were online auction frauds. The increasing number of deceptions in online shopping can be attributed to weaknesses of current reputation systems, which include weak authentication resulting in easy re-registration (Neumann 1997,

Friedman and Resnick 2001, Dellarocas 2003), easily manipulated ratings and comments (Ba 2003), moral hazard of misusing reputation credits for pseudonyms on the Internet, and the tendency not to give negative feedback after completion of transaction (Baron 2002). Some scholars have noted these problems in reputation systems exist (Dellarocas 2000, Zacharia et al. 2000, Miller et al. 2002), and have proposed improvements (Dellarocas 2002, 2005, 2006; Dellarocas and Wood 2008). Josang et al. (2007) present an overview of existing and proposed systems for Internet transactions. Nevertheless, to date, there is no perfect solution that completely addresses all of the issues that have arisen related to reputation systems.

At the same time, much scholarly effort has been made on studying auction fraud, including the impact of forged sites (Grazioli and Jarvenpaa 2000), the types of fraud (Grazioli and Jarvenpaa 2003, Gregg and Scott 2008), the effects of online trading communities on fraud detection (Chua et al. 2007), and motivations behind fraud (Utz 2005). Various methods of fraud detection have been proposed, based on the classical classification methods of neural networks, fuzzy logic, genetic algorithms, support vector machines, regression, and decision trees. For a detailed overview of the methods for fraud detection, please refer to Laleh and Azgomi (2009). Nevertheless, only very limited attention has been paid to collusive behaviors among users, in spite of the fact that it undermines the reliability of reputation mechanisms.

This paper proposes a novel approach to identify users' collusive behavior. Using the *homo economicus* assumption, we analyzed the cost and benefit of each party involved in the collusion and obtained six indicators, which include both individual-related and transaction-related indicators. A detection model is also

* Corresponding author.
  E-mail address: mxia@scu.edu (M. Xia).

proposed to distinguish the collusive transactions from bona fide ones. A dataset from the largest online C2C market, Taobao.com, will be employed to illustrate the effectiveness of the proposed detection model. Our study's contributions have two aspects: (1) We offer a new way of identifying the characteristics of collusive behavior. The process of obtaining the indicators could be extended to other malicious behavior detection, such as smuggling, money laundering, tax evasion, and drug trafficking. (2) We also provide managerial implications on improving C2C websites.

The remainder of this paper is organized as follows. In the next section, we discuss the related literature. In Section 3, we describe the research context, and propose a number of corresponding hypotheses. Section 4 describes the dataset we will use in our empirical research. Section 5 presents the methodology and results. The last section discusses the research findings with their implications for practice, and proposes the future research possibilities.

## 2. Literature review

### 2.1. Collusion

Lian et al. (2007) defined *collusion* as a collaborative activity within groups of users that aim to generate group member benefits that are otherwise not available for individuals. It can be observed in a lot of systems. Collusion is often observed in the field of insurance, for instance. Little et al. (2002) quantitatively analyzed indicators of collusion in the United States Department of Agriculture's Risk Management Agency's national crop insurance program. Log linear modeling analysis and deviance statistics were applied to identify triplet and agent-producer doublets for possible collusion. Šubelj et al. (2011) proposed an expert system for detecting collaborating automobile insurance frauds. A novel assessment algorithm, called the iterative assessment algorithm, was proposed and demonstrated to be effective.

In the online context, researchers have also been working on detecting collusive behavior. Lian et al. (2007) studied user collusion that aims to gain unfair advantages over other users in Maze, a large-scale peer-to-peer (P2P) file-sharing system with a point-based incentive policy. By examining complete user logs, four types of collusion detectors are proposed. They also found that collusion patterns are similar to those found in Web spamming. Chau et al. (2006) and Zhang et al. (2008) adopted the idea behind outlier detection, and considered both user level and network level features for collusion detection in an electronic market. However, the detection model was limited to only scenarios in which fraudulent participants and their accomplices were created together and assigned different roles to play. Wang and Chiu (2005, 2008) adopted measurements from social network analysis and created a collaboration-based recommendation system to suggest risks of collusion associated with an account. However, *group purchasing behavior* makes a single $k$-core value insufficient to distinguish inflated-reputation accounts from legal ones. A group of buyers simultaneously buying from a set of sellers is a common phenomenon in group purchasing. This is because buyers in the group benefit from extra discounts (Marvel and Yang 2008). As a result, more relevant indicators need to be identified. Almendra and Schwabe (2009) advocated the use of human computation (crowdsourcing) to improve current fraud detection techniques. Yet before crowdsourcing can be employed, one has to first identify potential participants who may create fraud. This is the goal of our study.

### 2.2. Social network analysis

*Social network analysis* is the mapping and measuring of relationships and information ﬂows between people, groups, organizations, computers or other information processing entities (Hanneman and Riddle 2005). It quantitatively measures the interactions among members of community. As a research paradigm, it provides a new tool to understand the world. With the development of the Internet, two data issues in traditional social network analysis are being addressed, namely, difficulty in collecting large-scale data and bias in survey-based data. The availability of Web log data is facilitating the study on the structure and dynamics of social networks, behavior of individuals, and patterns of interaction (Albert and Barabasi 2001, Newman 2003).

Social network analysis focuses not on the attributes of individuals, but on relationships between individuals. The basic components are nodes and links. Nodes are abstractions for individuals, organizations, or communities (Borgatti et al. 1998). Links can be of various types of relationships based on contexts (Freeman 1979). After decades of efforts, measurements for describing networks on the global, subgroup, triad, dyad, and individual levels have been well developed (Wasserman and Faust 1994, Scott 2000). The relationship between the attributes of individuals and network structure has also been investigated (Grewal et al. 2006, Schilling and Phelps 2007, Sofiapereira and Soares 2007).

Social network analysis has been widely applied in data mining on crime and malicious behavior. Because criminals often develop networks to carry out various illegal activities, identifying subgroups and key members, and their interaction patterns are usually helpful in fighting crime (Chen et al. 2004). For example, Qin et al. (2005) collected information of members of Global Salafi Jihad network from multiple sources, and applied social network analysis to the network and obtained an authority derivation graph of the criminal network. Blume et al. (2006) used a dataset related to the information forecasting market for the soccer championship in Germany in 2005. This was also a context for the study of the effectiveness of his approach to search for malicious accounts. Ahmad et al. (2009) proposed another approach involving the use of network features of illicit behavior patterns to identify "gold farmers." They are users who accumulate virtual wealth or "gold" with the sole intention of selling it to other players. They also found that the network structure of "gold farmers" is similar to the network structure of drug traffickers. Šubelj et al. (2011) utilized four types of networks to represent the complex relationships among entities and proposed an expert system for automobile insurance collusion detection.

## 3. Research hypotheses

### 3.1. Research context

In this study, *collusion to inflate reputation* refers to the illegal business that some shady organizations undertake for profit. *Collusive seller* refers to the seller who wants to inflate his reputation through collusion. The term *puppet buyers* refers to accounts set up by illegal organizations for the sole purpose of conducting fake transactions with collusive sellers. The whole process of reputation inflation is presented in Fig. 1. After getting a payment from collusive seller, an illegal organization will employ a large number of puppet buyers who initiate multiple fake transactions (with no delivery of goods), and then will give positive ratings and comments. The theory of deception, proposed by Johnson et al. (2001), defines *deception* as "a cognitive interaction between two parties where one party, the deceiver, manipulates the environment of the other party, the target, so as to intentionally foster an incorrect cognitive representation of the target's situation and urge a desired action which the target would be unlikely to take without the manipulation." So collusive transactions that mislead potential buyers can be classified as undesirable instances of deception.
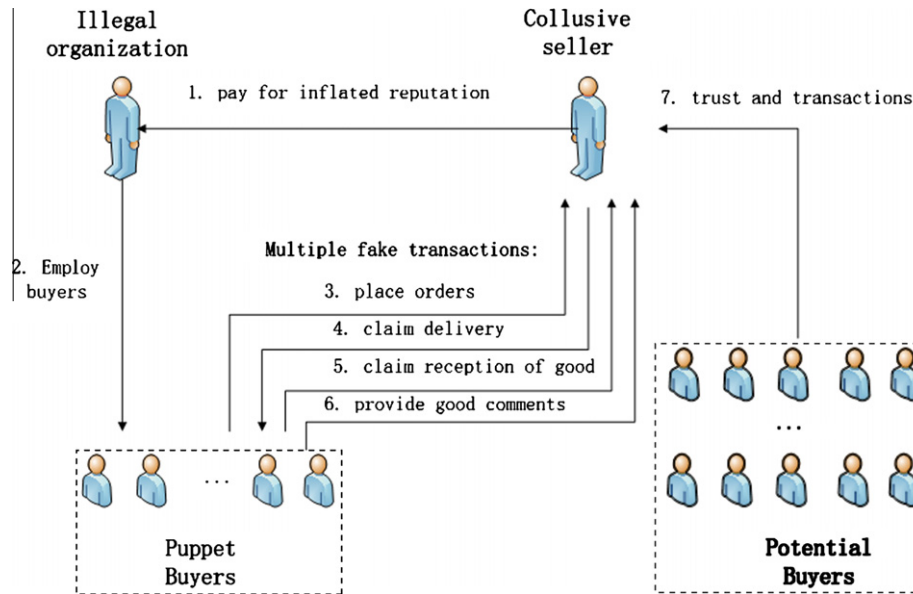
**Fig. 1.** Process of reputation inflation.

## 3.2. Cost-benefit analysis

*Homo economicus*, which depicts people as individualistic, opportunistic and self-serving, is a fundamental assumption of neo-classical economics. Sociologists criticized the pure *economic man* assumption and tried to reconcile *homo economicus* with *homo sociologicus* assumption (Ng and Tseng 2008). But most scholars agree that confined to certain aspects of life, such as business and politics, the *homo economicus* paradigm is crucial for survival and success (Randels 1998).

Neo-classical economist, Gary Becker, proposed that criminals make rational decisions (1968). In this view, criminals, as individuals who willingly commit crime, do so because from their perspective, the benefits of their crime outweigh the cost such as the probability of apprehension, conviction, and punishment. This theory helps to understand the deviant behaviors and provides some hints for prohibiting them. A similar idea can be found in Carl Shapiro's (1982) work too. He analyzed a monopolist's behavior weighed against the rewards of acting opportunistically when consumers cannot observe all the relevant attributes of the monopolist's product before purchase. In this study, collusion to inflate reputation is viewed as a specific crime in the context of e-business. Different from the electronic crimes resulting in financial loss and criminal prosecution, collusion here is limited to malicious behavior that violates public order and good morals. Based on the idea behind the economics of crime, which treats all behaviors as rational decisions, we will try to identify the features of collusive transactions.

### 3.2.1. Cost of inflating reputation

From the view of the puppet buyers, two types of costs are incurred in the process of collusion: behavioral costs and economic costs. *Behavioral costs* refer to the acts puppet buyers take to inflate a seller's reputation. As Verhallen (1984) suggested, behavior can be further categorized into goal acts and instrumental acts. *Goal acts* are defined as acts that lead to desirable outcomes, while *instrumental acts* are performed in order to reach a goal. In the C2C e-commerce context, registration is instrumental to becoming a puppet buyer. Efforts made to carry out the process involved in a malicious transaction, including selecting the merchandise, making the payment, rating, and providing comments, are the goal acts.

Buyer registration is usually simple. Typically a unique user name and a valid email address are the sole requirements to obtain a buyer identity. To set up an account, one is often required to activate the link that is sent by the online market to one's registered email box. The economic cost of becoming a buyer is close to zero due to the free email services provided by numerous websites. However, it takes time and effort to develop programs or to employ people to sign up for and maintain a sufficient number of email accounts from e-mail providers. The best way to minimize the cost in this step is to be an active trader, and conduct as many transactions as allowed by the market for each account. Activeness, as a characteristic of fraudsters, was also noticed in Blume et al. (2006)'s work. Thus, we propose our first hypothesis.

**Hypothesis 1** (*The Collusive Accounts Hypothesis*). *Collusive accounts are more active than bona fide accounts.*

The economic cost mainly refers to the time value of the money held by escrow services that authorize payments only after the buyer is satisfied. Escrow services provide institution-based trust, which facilitates transaction success and has been widely utilized in C2C markets (Pavlou and Gefen 2004). In collusive transactions, the payment (which actually pays for nothing) from the puppet buyer to the collusive seller has to be made through the escrow service. Therefore, taking the time spent on delivery and checking the merchandise into account, the payment is usually held by the escrow service for two to five days, or even longer. Hence, if the amount of money is large, the time value of money can be costly. In order to cut this cost, collusive transactions tend to involve cheap items. The less amount of money being held, the less it costs for buyer.

Another concern is cost per transaction. Transactions of low-value merchandise are more economical, as they are as effective as higher value ones in creating opportunities to inflate the reputations of collusive sellers. To gain as many positive ratings as possible with a certain amount of money, cheap items are the best choice.

Another factor for the value of fake transactions is that the payment made by puppet buyers to the seller always comes from the seller himself in the form of an advance payment to the puppet buyers for the reputation inflation service. Collusion is illegal, so the rights of the seller who paid first are not protected by law. Only oral contracts between the seller and the puppet buyers, who are

conducting illegal activities, are involved. Therefore, the seller, to minimize his own risk, has an incentive to pay the lowest amount possible for the collusive transactions.

The observation of cheap items for inflating reputation is also mentioned in Chau et al. (2006). Taking all the above considerations into account, we propose:

**Hypothesis 2** (*The Collusive Transaction Merchandise Value Hypothesis*). *The average value of the merchandise in collusive transactions is lower than that in non-collusive transactions.*

Meanwhile, as the accounts were set up to solely conduct fake transactions, to decrease the risks of being detected from website operator, illegal organization regularly set up new accounts to enlarge the group of puppet buyers and use them right away, despite the behavioral cost of setting up accounts. Thus, we anticipate that newly-registered accounts are be more likely to be involved in collusive transactions. We further propose:

**Hypothesis 3** (*The Buyer's Short Account History Hypothesis*). *The shorter the history the buyer's account has, the more likely the transaction is related to collusion.*

### 3.2.2. Benefits of inflated reputation

The reasons why sellers in e-markets are pursuing high reputations lie in the correlation between high reputations and high profit. Resnick et al. (2000) conducted an experiment on eBay comparing sellers with high and low reputations selling the same products. They found that the difference in the willingness-to-pay of buyers was 8.1% of the selling price. Similar findings can be found for music CDs, computer modems, software, Canon digital camcorders, Harley-Davidson Barbie dolls among other studies (Ba and Pavlou 2002, Kalyanam and McIntyre 2001, McDonald and Slawson 2002). In addition, some researchers have found that a higher reputation brings higher sales volume (Livingston 2005). Li et al. (2008a) found that the good reputations of sellers have a positive impact on their sales volume, but the marginal impact decreases sharply. Through an empirical study on a dataset from eBay, Cabral and Hortaçsu (2010) found that when a seller first receives negative feedback, the seller's weekly sales rate drops from a positive 5% to a negative 8%.

Aside from the reputation score accumulated by positive, neutral, and negative ratings, the content of comments also contributes to the reputations of sellers. For example, spam review detection has been a hot topic in the data mining field (Hayati and Potdar 2009). Generally, the same positive rating has different meanings to potential buyers. For example, some buyers prefer sellers with quick delivery, whereas others may prefer sellers who patiently introduce to the merchandise. Viewing the comments provided by previous buyers provides more information to potential buyers than the reputation score itself. For potential buyers who want to purchase from specific sellers, detailed comments for the seller are more valuable than simple positive ratings. From our interviews with a number of buyers, we learned that in most cases, when a buyer is willing to take time to praise the seller, the seller must be good enough to be recommended. Therefore, for fake transactions to be effective in raising the reputation of the seller, buyers need to write informative comments. We infer that:

**Hypothesis 4** (*The Detailed Comments and Collusion Hypothesis*). *Collusion is positively related to the presence of detailed comments.*

Identifying the weaknesses of existing rating systems and improving them has been the focus of many researchers (Engelmann and Fischbacher 2009, Mathis et al. 2009, Fouss et al. 2010). According to the law of diminishing marginal utility (Culloch and Huston 1977), we infer that one-point increase on the reputation means differently to the sellers who own different reputations in this community. The sellers who already have high reputation should have less motivation to inflate their reputation while the new sellers who are eager to be noticed and trusted prefer a fast-growing reputation. That is to say, we hypothesize that fake transactions and related positive score are more desirable for new sellers than well-established ones. So the sellers with low reputation are more likely to be involved in collusion:

**Hypothesis 5** (*The Seller's Reputation and Collusion Hypothesis*). *The higher the reputation of the seller, the less likely the seller will participate in collusive transactions.*

Accordingly, the research model of this study is composed of both transaction-related indicators and individual-related indicators. Fig. 2 presents the research model that guides the empirical analysis.

## 4. Data

### 4.1. Data collection

Data for this study were collected from Taobao (www.taobao.com), the leading online C2C website in China in terms of market share, number of listed merchandise items, active users, and website traffic (Li et al. 2008b). Taobao was founded in May 2003. In 2005, Taobao became the leader in China's online shopping market. According to the Development Report on China Online Shopping Market conducted by iResearch (2010), the annual revenue in China's online shopping market reached US$38.7 billion (RMB263 billion) in 2009, with a growth rate of 105.2% over the previous year. Taobao had a 79.2% share of this market. We obtained data on fraudulent accounts specific to reputation inflation and related
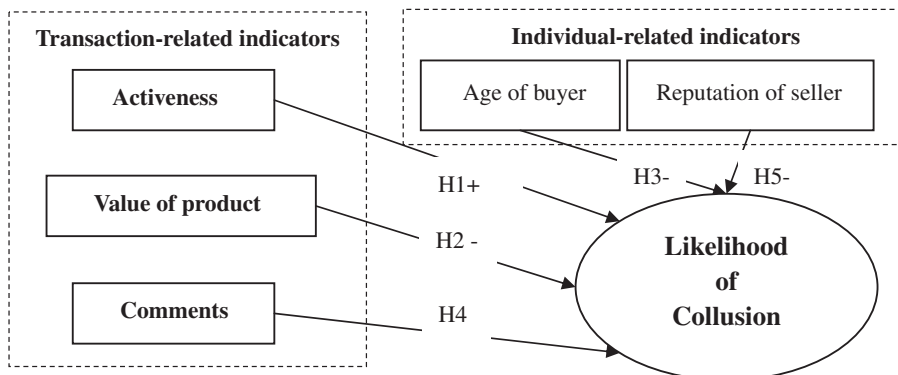


**Fig. 2.** Research Model.

collusive transaction records from Taobao under a non-disclosure agreement.

Taobao has made several efforts to detect collusion detection. In the first stage before July 2009, collusion detection was mainly complaint-driven. If complaints were filed about one specific seller, Taobao would investigate the seller, require information on past transactions, and look into reputation history, and registration information. This was to see if the seller engaged in reputation-inflation activities. The seller would be labeled as a *reputation-inflated account* if the seller could not provide enough evidence to explain the suspicious transactions. Between July and August 2009, with the emergence of shady organizations specializing in reputation inflation as a business, Taobao sifted through all the sellers and identified those whose reputation had grown rapidly and could not provide proof of their actual delivery of the merchandise. The dataset we obtained included collusive transactions that were the result of both the complaint-driven investigation and the all-seller investigations undertaken by Taobao.

In order to build a transaction network, we collected non-collusive transactions by a self-developed screen-scraping program, starting with the well-behaved buyers that had done business with the collusive sellers identified by Taobao. The program parsed the pages of these buyers to extract their transaction and evaluation records. In this manner, we obtained information on a large number of non-collusive accounts that have been confirmed as well-behaving by Taobao. The information includes the time of transaction, final price, rating, counterparty comments, and trader reputation.

The data collection was based on the users involved because the sellers usually sell merchandise in multiple categories. For example, we observed that a collusive seller who originally sold digital cameras as his main business also sold computer mouse cushions.

There were a total of 680,150 transactions, involving 816 collusive accounts and 23,434 non-collusive accounts from June 1, 2009 to June 30, 2009 that we used for analysis. This study uses the *user pair* (buyer and seller) as the unit of analysis. There were 20,400 user pairs in all, in which 991 were collusive user pairs and 19,049 were non-collusive user pairs.

## 4.2. Key variables

The dependent variable in our empirical analysis is whether the pair of traders (seller and buyer) is doing collusive transactions, where "1" stands for collusion and "0" stands for non-collusion. We employed the user pair as opposed to the transaction as the unit of analysis because a single transaction without context is insufficient for evaluating collusion.

To examine our proposed hypotheses, we constructed measurements based on the context of this empirical study, Taobao.com. The reputation system at Taobao is very similar to other C2C websites, in that users can rate their trading partner after a transaction. There is one notable difference: only buyers who pay through Alipay, a payment system owned by the same parent company of Taobao, can provide feedback to the seller. Alipay is similar to Paypal (www.paypal.com) and Escrow (www.escrow.com), where a third party authorizes payment only after the buyer receives and approves the merchandise (Hu et al. 2004). However, Alipay has a distinctive feature that sets it apart from traditional escrow services: it is free for all traders on Taobao.

In Taobao, each user's profile consists of two scores, the reputation as a buyer, and the reputation as a seller. A positive, neutral, and negative feedback will add 1, 0 and −1 to the reputation score, respectively. According to a Taobao rule, within a period of fourteen days, a member can only rate another member at most six times for six different transactions. The more positive ratings users receive from other users, the higher the reputation score.

### 4.2.1. Activeness

Illegal organizations conduct collusions as a business, for which establishing new accounts is a significant cost. Therefore, they maximize the activities of each account to the extent allowed by the site. We can observe the overall activeness level of each account through the number of transactions in a given time window. *Activeness* with one single seller can be measured by pair-wise transaction frequency. Puppet buyers often buy a lot of different kinds of merchandise from a seller within a short period. Limited by the Taobao rule of not more than six ratings in fourteen days between any pair of users, a puppet buyer would have no motivation to buy more than six items from a particular seller within any fourteen-day window. If a number of buyers are set up to help inflate the reputation of some specific sellers, we can observe them purchasing from the same set of sellers simultaneously.

The best measure to identify the situation that a group of puppet buyers purchase from a group of sellers simultaneously is an indicator named *k-core*. The idea behind *k-core* was first proposed by Seidman (1983). The formal definition is as follows (Batagelj and Zaversnik 2003).

Let $G = (V, L)$ be a graph, where $V$ is the set of vertices and $L$ is the set of edges. We denote $n = |V|$, $m = |L|$, and introduce a subgraph $H = (W, L/W)$ $W$ is a *k-core* or *a core of order k* if $\forall v \in W$: $\deg_H(v) \geqslant k$, and $H$ is the maximal sub-graph with this property. The term $L|W$ denotes the edges related to the node set of $W$. The *degree function* $\deg_H(v)$ can be in-degree, out-degree, or in-degree and out-degree, depending on the research need. Here, we focus on linkages between traders, so both *in-degree* and *out-degree* are considered. The *k-core* measure is frequently used to differentiate strong ties among subgroups.

A transaction network is constructed by taking each account as a node and the transactions between a buyer and a seller as a link between the two nodes. The directed arrow from the buyer to the seller means that the buyer purchases one or more items from the seller. The two-core graph of part of the collusive transactions network at Taobao is shown in Fig. 3. Each account is marked by a user ID for our purpose (not the real ID at Taobao). Obviously, it is highly likely that a large group of buyers (marked by blue circles) are employed to serve the two sellers in the middle (marked by red squares). Meanwhile, part of those buyers on the left also colluded with thirteen other sellers simultaneously. Since players repeat transactions but rarely with the same player in C2C market (Resnick and Zeckhauser 2002), especially in one-month time window, it is very unlikely that a group of buyers all bought from exactly the same set of sellers in the same month. Hence, suspicious sellers and buyers can be identified at the same time visually from the figures like Fig. 3, or, equivalently, by the higher *k-core* value of each user in the transaction network we constructed.

### 4.2.2. Rating and comments

There are three options when a buyer rates a seller at Taobao: positive, neutral, and negative, which add 1, 0 and −1 to reputation scores, respectively. In addition, one can also include detailed text comments. In this study, from the view of benefit of sellers, we used information of both ratings and comments as indicators. We first differentiate three types of ratings, and then further divide the positive rating into three subclasses according to Taobao rules. First, if no rating is provided by a buyer after 15 days since the seller evaluated the buyer (indicating that the transaction should be closed), there will be a positive rating with the text "no comment is good comment" appearing in the seller's evaluation history, assuming the buyer has nothing bad to say about the transaction. We name this kind of situation as "no comment is a good comment." Second, if the buyer does not have specific comments for evaluating the seller, the buyer can simply click the button for "good" for comments and we will see "good!" in the evaluation
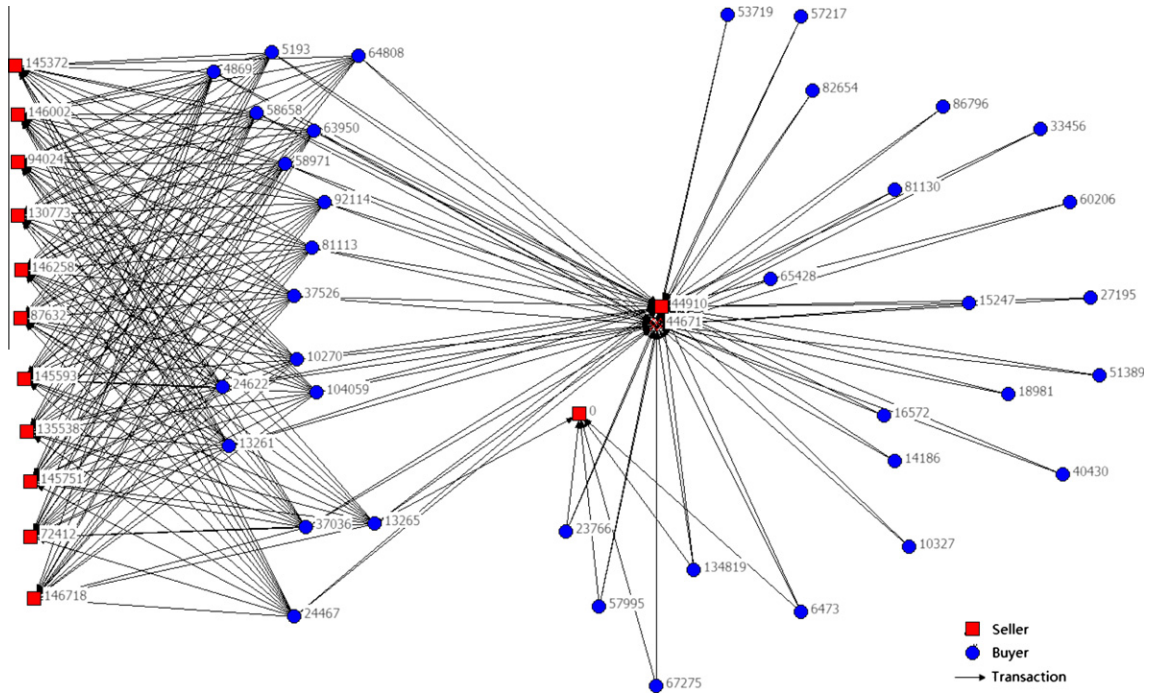
**Fig. 3.** Two-core subgraph of some collusive transactions.

history of the seller. We call this "one-click good comment." Third, if user both provides positive rating and writes detailed comments for the seller, we name it as "specific comments for the transaction." To sum up, we classify the evaluation part of each transaction (rating and comments) into five groups (Table 1).

Recall that user-written comments are helpful for potential buyers, thus, we assume that five types of comments add different values to the reputation of sellers as follows: E < D < C < B < A.

Type C comments should be particularly noticed because of the Taobao rule. As we mentioned earlier, the seller cannot obtain payment until the buyer approves. Type C comments only appear when the buyer does not approve in fifteen days after the seller has confirmed his delivery of the merchandise and has evaluated the buyer. The rule is set to protect the seller in the situation where the buyer who has received the merchandise is too busy to log in and click the approval button. If the transaction is closed in this way, the money is held by Alipay for a significantly longer time than usual. Hence, still thinking about the time value of money held by the escrow service, the collusive buyer would comment on the seller as early as possible, that is, Type C comments should rarely appear from collusive transactions. Thus, the indicators about comment could be specified as "the percentage of each type of comment".

To sum up, the major independent variables are about the transaction pattern of each pair of traders, including the number of different items bought and sold during the month (transaction frequency), the average price of items bought and sold, comments for the seller, and connectedness to the transaction network. Aside

from transaction-related indicators, two individual-related indicators are also involved, seller reputation and buyer age. Table 2 presents definitions of the variables and explanation of measurement.

### 4.3. Descriptive statistics

We start our analysis with descriptive statistics that provide a first glimpse of the patterns of relationships. There are four transaction-related indicators of interest: average price, number of transactions during the month (frequency), comments, and connectedness. There are five types of comments presented in Table 1, and four dummy variables are involved. The type E comment is the base type for comparison. The descriptive statistics of the variables are presented in Table 3. The column "Mean" shows the average value of the each variable. For example, the average price of the goods sold in this month is RMB 74.81, and the most expensive goods is sold at the price RMB 5200. (See the column "Max.") The column "S.D." shows the standard deviation of the variable in this dataset.

## 5. Empirical methodology and results

### 5.1. Empirical model

Logistic regression is suitable for building a fraud detection model because the dependent variable is dichotomous (Gregg and Scott 2006). Logistic regression does not assume a linear relationship between the dependent variable and the independent variables, and has been used in predicting collusion (Abarca and Armstrong 2000, Macinnes et al. 2005). It has been widely applied in fraud detection in various areas (Matsumura and Tucker 1992, Grazioli and Jarvenpaa 2000, 2003).

We employ a logit regression to test the proposed indicators. The variables seller reputation score, buyer age, seller and buyer $k$-core, price, and number of transactions during the month were all transformed to their logarithmic equivalents. The transformations were necessary because of considerable skewness. The model is as follows:

**Table 1**
Types of comments.

| Type of rating | Type of comment | Class |
|---|---|---|
| Positive | Specific comments for the transaction | A |
| | One-Click good comment | B |
| | "No comment is a good comment" | C |
| Neutral | | D |
| Negative | | E |

**Table 2**
Data description.

| Variable name | Description | Code |
|---|---|---|
| *Transaction-related indicators:* | | |
| Transactions frequency | Number of transactions between a pair of seller and buyer during a month. | Integer number |
| Connectedness | Measured by the k-core value (see 4.2 for details) | Integer number |
| Comment type | Comment type was constructed by the rating information and text reviews. It reveals satisfaction with the transaction counterpart. | A = positive rating with user-written comments |
| | | B = positive rating with "one click good comment" |
| | | C = positive rating with "no comment is good comment" |
| | | D = neutral rating |
| | | E = negative rating |
| Average price | Average price was constructed by dividing the sum of the value of all the items sold/bought between a pair of seller and buyer by the number of items. | Real number |
| *Individual-related indicators:* | | |
| Reputation | Reputation at Taobao is represented by the accumulated positive(+1), neutral(0) and negative(−1) ratings for sellers and buyers. The higher the reputation is, the more positive ratings the user receives. Each user has two parts of reputation, One is the reputation as a buyer, and the other is the reputation as a seller | Integer number |
| Age | Number of days from user registration at Taobao | Integer number |

**Table 3**
Descriptive statistics of key variables for collusive and non-collusive pairs.

| | Mean | S.D. | Min | Max |
|---|---|---|---|---|
| Frequency | 1.71 | 1.1 | 1 | 13 |
| Price | 74.81 | 162.03 | 0.01 | 5200 |
| buyer_age | 601.43 | 497.82 | 7 | 2243 |
| buyer_k_core | 1.39 | 1.75 | 1 | 19 |
| seller_reputation | 20067.07 | 69175.9 | 5 | 13,04,256 |
| seller_k_core | 6.89 | 3.88 | 1 | 22 |
| comment_A | 0.36 | 0.48 | 0 | 1 |
| comment_B | 0.42 | 0.49 | 0 | 1 |
| comment_C | 0.21 | 0.41 | 0 | 1 |
| comment_D | 0.01 | 0.08 | 0 | 1 |

$$\begin{aligned} Likelihood\ of\ collusion = {} & \beta_0 + \beta_1 \cdot \ln Price + \beta_2 \cdot \ln Frequency \\ & + \beta_3 \cdot \ln Comments + \beta_4 \cdot \ln Seller's\ k\_core \\ & + \beta_5 \cdot \ln Buyer's\ k\_core \\ & + \beta_6 \cdot \ln Seller's\ Reputation \\ & + \beta_7 \cdot \ln Buyer's\ Age. \end{aligned}$$

A formal multicollinearity test was conducted before the regression analysis. The results showed a tolerance value above the threshold of 0.1 (Hair et al. 1995), which means that we can proceed with further analysis without the concern about multicollinearity.

## 5.2. Estimation results

The results of the estimation (shown in Table 4) exhibit a satisfactory fit with pseudo $R^2$ = 0.676. The proposed indicators are all significant at the 0.01 level. The positive coefficient of the variable "frequency" (0.618) and "k-core value" of seller and buyer (1.085 and 2.071) indicate that activeness we discussed earlier is one of the characteristics of collusion. Also, it validates the fact that puppet buyer is active both with one seller and multiple sellers. The result supports the Collusive Accounts Hypothesis (H1). Similarly, the negative sign associated with price and the likelihood of collusion indicates that the Collusive Transaction Merchandise Value Hypothesis (H2) is supported. It means that cheap items are more involved in collusive transactions. The coefficient (−0.708) quantitatively measured the impact of price increase on the possibility of collusive user pair. As to the relationship between comments and likelihood of collusion, the type A comment, positive rating with user-written comments, also significantly affects the likelihood of collusion. It supports The Detailed Comments and Collusion Hypothesis (H4). Meanwhile, the individual-related indicators are also effective in this model. Consistent with our expectation, the puppet buyer accounts are newly created. To minimize their costs of collusion, these puppet buyers often immediately started their collusion efforts after registration as a new user. Thus, the Buyer's Short Account History Hypothesis (H3) is supported. Likewise, the sellers with lower reputation are more involved in collusion, which is a support to the Seller's Reputation and Collusion Hypothesis (H5). To sum up, all the five hypotheses presented in Fig. 2 are all supported in this empirical study, which is to say that the cost and benefit analysis helped us to identify the effective indicators of collusive transactions.

## 5.3. Detection model

Logistic regression is a good classification algorithm with respect to mean error, mean rank of error rate and training time (Lim et al. 2000). Thus, in this study, the logit model can also be applied as a collusion detection model. A *receiver operating characteristics* (ROC) *graph*, first used by Spackman (1989), is a useful technique for visualizing the performance of a classifier that decouples classifier performance from class skew and error costs (Fawcett 2006). In Fig. 4, the *y*-axis "sensitivity" means the *true positive rate* (also called *recall*) and the *x*-axis "1-specificity" means the *false positive rate* (also called *false alarm rate*). The diagonal line

**Table 4**
Likelihood of collusion: Logit regression estimation results.

| Variables | Collusion |
|---|---|
| ln(*price*) | −0.708[***] |
| | (0.0336) |
| ln(*frequency*) | 0.618[***] |
| | (0.107) |
| ln(*buyer_kcore*) | 2.071[***] |
| | (0.0969) |
| ln(*seller_kcore*) | 1.085[***] |
| | (0.113) |
| *comment_A* | 1.084[***] |
| | (0.118) |
| ln(*seller_reputation*) | −0.286[***] |
| | (0.0403) |
| ln(*buyer_age*) | −0.601[***] |
| | (0.0586) |
| Observations | 20,040 |

Standard errors in parentheses.
LR   chi2(9) = 5331.83;   Prob > chi2 = 0.000;   Pseudo R2 = 0.6756.
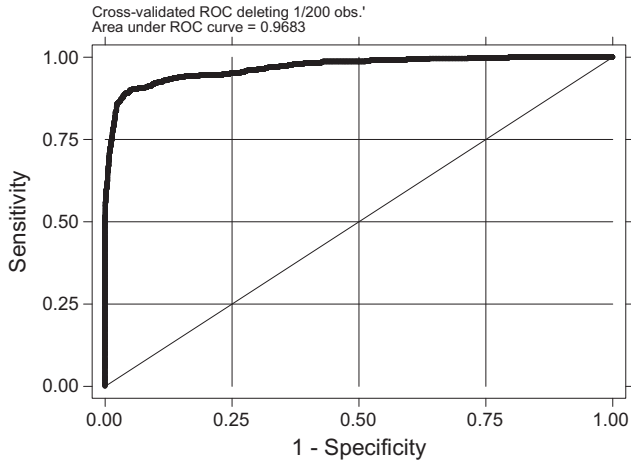[***] $p < 0.01$.

**Fig. 4.** Cross-validated ROC curve for the detection model.

$y = x$ represents the strategy of randomly guessing a class. Logistic regression yields an instance probability that represents the degree to which an instance is a member of a class. Each threshold produces a different point in the ROC space. The *area under the ROC curve* (AUC) is calculated to measure the performance of the classifier (Bradley et al. 1997). The result of cross validation (Fig. 4) shows that the AUC of this logit model approaches 0.968 which means that it is an effective model for collusion detection.

## 6. Discussion, limitations and future research

### 6.1. Conclusion

Table 5 shows the key findings of this study by summarizing the empirical results and providing some explanation to result we obtained. The initial goal of this paper was to present a framework to obtain the features of collusive behavior in C2C markets. Based on the labeled data from Taobao, the empirical study shows that the indicators, both transaction-related and individual-related, are effective in detecting the collusion. The malicious users are significantly different from bona fide ones. The process of obtaining these indicators can be extended to other malicious behavior such as smuggling and tax evasion.

### 6.2. Implications for system designs

The results of this research provide some implications for C2C online market designs. Reputation has been found to facilitate transactions between stranger, and it becomes more reliable when reputation-inflated traders can be identified promptly. The following strategies are suggested to reduce reputation inflation.

First, raise the cost of entry. The simple email address requirement for registration as a buyer is far from a costly procedure. Combining the real world identity with the virtual one in an online shopping website can raise the cost of setting up a new account, while increasing the trustworthiness of sellers. Although the strategy may drive away some potential users to other competing sites due to the increased behavioral cost, the users in this community are better protected. More in-depth requirements of registration and authorization have been increasingly accepted as an understandable cost to maintain a well-mannered community.

Second, raise the cost of each reputation score. In current systems, no matter how much the merchandise costs and no matter who is providing the rating, one point can be added to the reputation of the seller after a transaction, motivating fake transactions involving cheap items by new entrants. The value of items bought and sold, the reputation of the buyer, and decay with time should all be taken into account when generating seller reputation (Wu et al. 2008). Likewise, the transactions involving tangible goods, as compared to digital goods, require more product delivery effort on the part of sellers. Hence, the nature of the goods should also be considered in a reputation mechanism.

Third, raise the cost of risk, which refers to losses if collusive transactions are identified. E-business websites, such as Taobao, should pay more attention to collusion detection, which could increase the perceived risk for perpetrators. Meanwhile, more severe punishments that make the costs far outweigh the benefits are also necessary to deter would-be perpetrators.

Fourth, lower the benefits that reputation scores alone bring to sellers. In current systems, sellers pursue higher reputation scores mainly for the chances of being noticed and trusted by potential buyers. A web site can promote alternative ways of establishing trustworthiness. For example, the seller with low reputation can participate in a consumer assurance program. If the consumer is not satisfied with a flawed product bought from the sellers in this program, Taobao will pay back the buyer and subsequently punish the seller.

**Table 5**
Key findings.

| Independent Variable | Empirical results | Explanation |
|---|---|---|
| Average price | As hypothesized, value of merchandise is an indicator for collusion detection. The lower the price is, the greater is the likelihood of collusion is. (The Collusive Transaction Merchandise Value Hypothesis, H2) | As the price decreases, the same amount of money paid to the shady organization brings back more positive ratings. It also decreases the risk of pre-paid collusive seller |
| Transactions frequency | The pair with frequent transactions is more likely to be collusive. (The Collusive Accounts Hypothesis, H1) | Being active with the same counterpart decreases the behavioral cost |
| Comment type | As expected, comment types are related to collusion. And presence of Type A comment (positive rating with detailed praise) increases the likelihood of collusion. (The Detailed Comments and Collusion Hypothesis, H4) | Comment of type A (positive rating with detailed praise) brings greater benefits to collusive sellers than the comments of other types |
| Connectedness | The more connected the traders are to the collusion clique, the greater is the likelihood of collusion. (The Collusive Accounts Hypothesis, H1) | A group of buyers employed by shady organizations did fake transactions with numerous collusive sellers simultaneously. The behavior forms a clique and increases the k-core value of the traders involved |
| Seller reputation | As expected, the higher seller reputation is, the less likely the seller will participate the collusion (The Seller's Reputation and Collusion Hypothesis, H5) | Sellers with higher reputation are established and cherish the reputation it has gained, thus are less motivated to participate the collusion |
| Buyer age | Newly-registered accounts are more likely to be involved in collusion. (The Buyer's Short Account History Hypothesis, H3) | Illegal organization employed puppet buyers and start the collusion right after the registration |

## 6.3. Limitations and future research

The study has a few limitations. First is the scope of data collection. There might be some collusive accounts that survived in the investigation conducted by Taobao. This kind of limitation is shared across studies in all forms of deviant behavior, and it is commonly accepted (Grazioli and Jarvenpaa 2003). Second, the detection model of collusive transactions presented in this study is based on the regulations of Taobao. Although Taobao shares some similarities with eBay, there are still some differences on specific regulations (Li et al. 2008b). Hence, for other online shopping sites with different regulations, the indicators might not all be applicable, such as when the maximum positive points that a buyer can give a single seller is only one regardless of the number of transactions. For example, at eBay, the frequency of transactions between a pair of traders is not indicative of collusive trading. Although the reputation inflation detection model is only currently effective for Taobao, the cost-and-benefit analysis procedure can be generalized to other online C2C shopping sites. Third, the dataset for the empirical study is limited to a one-month time window, so we are not able to capture the whole process of reputation inflation. Panel data covering all the transactions of each account since its registration will provide more information for collusion detection.

Further research should focus on the generalizability of the method and detection model we proposed. More empirical data need to be collected from other popular C2C markets to investigate the cost and benefit of collusion in those settings and to test the effectiveness of the model. Meanwhile, as the perpetrators of fraud evolve their capabilities to fight the detection efforts of Taobao, a more adaptive detection model might also be required. It will be one of the directions of our further research.

## References

Abarca, J., and Armstrong, E. P. How to use multiple logistic regression in retrospective database analyses. *Formulary*, 35, 10, 2000, 832–841.

Ahmad, M., Keegan, B., Srivastava, J., Williams, D., and Contractor, N. S. Mining for gold farmers: automatic detection of deviant players in MMOGs. In J. Vigo-Aguiar (ed.). *Proceedings of the 2009 International Conference on Computational Science and Engineering, Vancouver, BC, Canada, August 29–31, 2009.*, IEEE Computer Society, Los Alamitos, CA, 2009, 340–345.

Albert, R., and Barabasi, A. Statistical mechanics of complex networks. *Reviews of Modern Physics*, 74, 1, 2001, 47–97.

Almendra, V., and Schwabe, D. Fraud detection by human agents: a pilot study. In T. D. Noia and F. Buccafurri (eds.). *E-Commerce and Web Technologies, 10th International Conference, Linz, Austria, September 1–4, 2009*, Springer, New York, NY, 2009, 300–311.

Ba, S. Building trust in online auction markets through an economic incentive mechanism. *Decision Support Systems*, 35, 3, 2003, 273–286.

Ba, S., and Pavlou, P. Evidence of the effect of trust building technology in electronic markets: price premiums and buyer behavior. *MIS Quarterly*, 26, 3, 2002, 243–268.

Baron, D. P. Private ordering on the Internet: the eBay community of traders. *Business and Politics*, 4, 3, 2002, 274–275.

Batagelj, V., and Zaversnik, M. An O (m) algorithm for cores decomposition of networks. Working paper: *Arxiv preprint cs.DS/0310049*, 2003.

Becker, G. Crime and punishment: an economic approach. *Journal of Political Economy*, 76, 2, 1968, 169–217.

Blume, M., Weinhardt, C., and Seese, D. Using network analysis for fraud detection in electronic markets. In T. Dreier, R. Studer, and C. Weinhardt (eds.). *Information Management and Market Engineering, Volume 4 of Studies on eOrganisation and Market Engineering*, vol. 4, University Atsverlag Karlsruhe, Germany, 2006, 101–112.

Borgatti, S., Jones, C., and Everett, G. Network measures of social capital. *Connections*, 21, 2, 1998, 27–36.

Bradley, P. S., Mangasarian, O. L., and Street, W. N. Clustering via concave minimization. In M. C. Mozer, M. I. Jordan, and T. Petsche (eds.), *Advances in Neural Information Processing Systems*, MIT Press, Cambridge, MA, 1997, 368–374.

Cabral, L., and Hortaçsu, A. The dynamics of seller reputation: evidence from eBay. *The Journal of Industrial Economics*, 58, 1, 2010, 54–78.

Chau, D., Pandit, S., and Faloutsos, C. Detecting fraudulent personalities in networks of online auctioneers. In J. Fürnkranz, T. Scheffer, and M. Spiliopoulou (eds.). *10th European Conference on Principles and Practice of Knowledge Discovery in Databases, Berlin, Germany, September 18–22, 2006*, Springer, New York, NY, 2006, 103–114.

Chen, H., Chung, W., Xu, J. J., Wang, G., Qin, Y., and Chau, M. Crime data mining: a general framework and some examples. *Computer*, 37, 4, 2004, 50–56.

Chua, C. E., Wareham, J., and Robey, D. The role of online trading communities in managing Internet auction fraud. *MIS Quarterly*, 31, 4, 2007, 759–781.

Culloch, M., and Huston, J. The Austrian theory of the marginal use and of ordinal marginal utility. *Journal of Economics*, 37, 4, 1977, 249–280.

Dellarocas, C. Immunizing on-line reputation reporting systems against unfair ratings and discriminatory behavior. In *Proceedings of the 2nd ACM Conference on Electronic Commerce, Minneapolis, MN, October 17–20, 2000*, ACM, New York, NY, 2000, 150–157.

Dellarocas, C. Goodwill hunting: An economically efficient online feedback mechanism for environments with variable product quality. In J. Padget, O. Shehory, D. Parkes, N. Sadeh, and W. Walsh (eds.). *Agent-Mediated Electronic Commerce IV. Designing Mechanisms and Systems, AAMAS 2002 Workshop on Agent-Mediated Electronic Commerce, Bologna, Italy, July 16, 2002*, Springer, New York, NY, 2002, 238–252.

Dellarocas, C. The digitization of word of mouth: promise and challenges of online feedback mechanisms. *Management Science*, 49, 10, 2003, 1407–1424.

Dellarocas, C. Reputation mechanism design in online trading environments with pure moral hazard. *Information Systems Research*, 16, 2, 2005, 209–230.

Dellarocas, C. Research note—how often should reputation mechanisms update a trader's reputation profile? *Information Systems Research*, 17, 3, 2006, 271–285.

Dellarocas, C., and Wood, C. The sound of silence in online feedback: estimating trading risks in the presence of reporting bias. *Management Science*, 54, 3, 2008, 460–476.

Engelmann, D., and Fischbacher, U. Indirect reciprocity and strategic reputation building in an experimental helping game. *Games and Economic Behavior*, 67, 2, 2009, 399–407.

Fawcett, T. An introduction to ROC analysis. *Pattern Recognition Letters*, 27, 8, 2006, 861–874.

Fouss, F., Achbany, Y., and Saerens, M. A probabilistic reputation model based on transaction ratings. *Information Sciences*, 180, 11, 2010, 2095–2123.

Freeman, L. Centrality in social networks conceptual clarification. *Social Networks*, 1, 3, 1979, 215–239.

Friedman, E. J., and Resnick, P. The social cost of cheap pseudonyms. *Journal of Economics & Management Strategy*, 10, 2, 2001, 173–199.

Grazioli, S., and Jarvenpaa, S. Perils of Internet fraud: an empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 30, 4, 2000, 395–410.

Grazioli, S., and Jarvenpaa, S. Consumer and business deception on the Internet: content analysis of documentary. *International Journal of Electronic Commerce*, 7, 4, 2003, 93–118.

Gregg, D., and Scott, J. The role of reputation systems in reducing on-line auction fraud. *International Journal of Electronic Commerce*, 10, 3, 2006, 95–120.

Gregg, D., and Scott, J. A typology of complaints about eBay sellers. *Communications of the ACM*, 51, 4, 2008, 69–74.

Grewal, R., Lilien, G., and Mallapragada, G. Location, location, location: how network embeddedness affects project success in open source systems. *Management Science*, 52, 7, 2006, 1043–1056.

Hair, J., Anderson, R., Tatham, R., and Black, W. *Multivariate Data Analysis*, 4th edition. Prentice Hall, Englewood Cliffs, NJ, 1995.

Hanneman, R. A., and Riddle, M. *Introduction to Social Network Methods*. University of California, Riverside, CA, 2005.

Hawes, J. M., and Lumpkin, J. R. Perceived risk and the selection of a retail patronage mode. *Journal of the Academy of Marketing Science*, 14, 4, 1986, 37–42.

Hayati, P., and Potdar, V. Toward spam 2.0: An evaluation of Web 2.0 anti-spam methods. In 7th IEEE International Conference on Industrial Informatics, Cardiff, Wales, UK, June 23–26, 2009, 875–880.

Hu, X., Lin, Z., Whinston, A. B., and Zhang, H. Hope or hype: on the viability of escrow services as trusted third parties in online auction environments. *Information Systems Research*, 15, 3, 2004, 236–249.

Internet Crime Complaint Center, 2009 IC3 annual report. Available at www.ic3.gov/media/annualreports.aspx. iResearch, 2009 online shopping industry, statistical analysis of complaints. (2009年度网络购物行业统计分析报告). Available at http://www.news.c2cc.cn/wgx/data/201003/469970.htm. Translated from a Chinese language news source.

iResearch, Report of 2009–2010 Chinese online shopping industry (艾瑞咨询: 2009 年中国网络购物交易规模达2630亿元 电子商务影响加深) (April 9, 2010). <news. iresearch.cn/viewpoints/112343.shtml>. Translated from a Chinese language news source.

Johnson, P. E., Grazioli, S., Jamal, K., and Berryman, G. Detecting deception: adversarial problem solving in a low base rate world. *Cognitive Science*, 25, 3, 2001, 355–392.

Josang, A., Ismail, R., and Boyd, C. A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43, 2, 2007, 618–644.

Kalyanam, K. and McIntyre, S. Returns to reputation in online auction markets. Working paper W-RW01-02, Santa Clara University, Saint Clara, CA, 2001.

Laleh, N., and Azgomi, M. A taxonomy of frauds and fraud detection techniques. In S. K. Prasad, S. Routray, R. Khurana, and S. Sahni (eds.). *Information Systems, Technology and Management, Third International Conference on Information Systems, Technology and Management, Ghaziabad, India, March 12–13, 2009*, Springer, New York, NY, 2009, 256–267.

Li, W., Wu, D., and Xu, H. Reputation in China's online auction market: evidence from Taobao.com. *Frontiers of Business Research in China*, 2, 3, 2008a, 323–338.

Li, D., Li, J., and Lin, Z. Online consumer-to-consumer market in China – a comparative study of Taobao and eBay. *Electronic Commerce Research and Applications*, 7, 1, 2008b, 55–67.

Lian, Q., Zhang, Z., Yang, M., Zhao, B., Dai, Y., and Li, X. An empirical study of collusion behavior in the Maze P2P file-sharing system. In *27th IEEE International Conference on Distributed Computing Systems, June 25–29, 2007, Toronto, Ontario, Canada*, IEEE Computer Society Press, Washington, DC, 2007, 56–65.

Lim, T., Loh, W., and Shih, Y. A comparison of prediction accuracy, complexity, and training time of thirty-three old and new classification algorithms. *Machine Learning*, 40, 3, 2000, 203–228.

Little, B., Johnston, W., Lovell, A., Rejesus, R., and Steed, S. Collusion in the US crop insurance program: Applied data mining. In D. Hand, D. Keim, and R. Ng (eds.). *Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Edmonton, Alberta, Canada, July 23–26, 2002*, ACM Press, New York, NY, 2002, 594–598.

Livingston, J. How valuable is a good reputation? A sample selection model of internet auctions. *Review of Economics and Statistics*, 87, 3, 2005, 453–465.

Macinnes, I., Li, Y., and Yurcik, W. Reputation and dispute in eBay transactions. *International Journal of Electronic Commerce*, 10, 1, 2005, 27–54.

Marvel, H., and Yang, H. Group purchasing, nonlinear tariffs, and oligopoly. *International Journal of Industrial Organization*, 26, 5, 2008, 1090–1105.

Mathis, J., McAndrews, J., and Rochet, J. Rating the raters: are reputation concerns powerful enough to discipline rating agencies? *Journal of Monetary Economics*, 56, 5, 2009, 657–674.

Matsumura, E., and Tucker, R. Fraud detection: a theoretical foundation. *Accounting Review*, 67, 4, 1992, 753–782.

McDonald, C. G., and Slawson, V. C. Reputation in an Internet auction market. *Economic Inquiry*, 40, 4, 2002, 633–650.

Miller, N., Resnick, P., and Zeckhauser, R. Eliciting honest feedback in electronic markets. Working paper, Kennedy School of Government, Harvard University, Cambridge, MA, 2002.

Neumann, P. Identity-related misuse. *Communications of the ACM*, 40, 7, 1997, 112.

Newman, M. The structure and function of complex networks. *SIAM Review*, 45, 2, 2003, 167–256.

Ng, I. C. L., and Tseng, L. M. Learning to be sociable: the evolution of homo economicus. *American Journal of Economics and Sociology*, 67, 2, 2008, 265–286.

Pavlou, P. A., and Gefen, D. Building effective online marketplaces with institution-based trust. *Information Systems Research*, 15, 1, 2004, 35–53.

Qin, J., Xu, J., Hu, D., Sageman, M., and Chen, H. Analyzing terrorist networks: A case study of the global Salafi Jihad network. In P. Kantor, G. Muresan, F. Roberts, D. D. Zeng, F. Y. Wang, H. Chen, and R. C. Merkle (eds.). *Intelligence and Security Informatics, IEEE International Conference on Intelligence and Security Informatics (ISI 2005), Atlanta, GA, USA, May 19–20, 2005*, Springer, New York, NY, 2005, 287–304.

Randels, G. D. The contingency of business: narrative, metaphor, and ethics. *Ethics*, 17, 12, 1998, 1299–1310.

Resnick, P., and Zeckhauser, R. Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system. In M. R. Baye (ed.). *The Economics of the Internet and E-Commerce (Advances in Applied Microeconomics*, vol. 11, JAI Press, Greenwich, CT, 2002, 127–157.

Resnick, P., Zeckhauser, R., Friedman, E., and Kuwabara, K. Reputation systems. *Communications of the ACM*, 43, 12, 2000, 45–48.

Schilling, M., and Phelps, C. Interfirm collaboration networks: the impact of large-scale network structure on firm innovation. *Management Science*, 53, 7, 2007, 1113–1126.

Scott, J. *Social Network Analysis: A Handbook*, 2nd edition. Sage, London, UK, 2000.

Seidman, S. Network structure and minimum degree. *Social Networks*, 5, 3, 1983, 269–287.

Shapiro, C. Consumer information, product quality, and seller reputation. *The Bell Journal of Economics*, 13, 1, 1982, 20–35.

Sofiapereira, C., and Soares, A. Improving the quality of collaboration requirements for information management through social networks analysis. *International Journal of Information Management*, 27, 2, 2007, 86–103.

Spackman, K. A. Signal detection theory: Valuable tools for evaluating inductive learning. In A. M. Segre (ed.). *Proceeding of the Sixth International Workshop on Machine Learning, Morgan Kaufman, San Mateo, CA, June 26–27, 1989*, Morgan Kaufmann, San Mateo, CA, 1989, 160–163.

Šubelj, L., Furlan, S., and Bajec, M. An expert system for detecting automobile insurance fraud using social network analysis. *Expert Systems with Applications*, 38, 1, 2011, 1039–1052.

Tirole, J. A theory of collective reputations (with applications to the persistence of corruption and to firm quality). *Review of Economic Studies*, 63, 1, 1996, 1–22.

Utz, S. Types of deception and underlying motivation: what people think. *Social Science Computer Review*, 23, 1, 2005, 49–56.

Verhallen, T. Attitude theory and behavioral costs. *Journal of Economic Psychology*, 5, 3, 1984, 223–249.

Wang, J., and Chiu, C. Detecting online auction inflated-reputation behaviors using social network analysis. Presentation, North American Association for Computational Social and Organizational Science, Notre Dame, IN, June 26–28, 2005.

Wang, J., and Chiu, C. Recommending trusted online auction sellers using social network analysis. *Expert Systems with Applications*, 34, 3, 2008, 1666–1679.

Wasserman, S., and Faust, K. *Social Network Analysis: Methods and Applications*. Cambridge University Press, Cambridge, 1994.

Wu, F., Li, H. H., and Kuo, Y. H. Reputation evaluation for choosing a trustworthy counterparty in C2C e-commerce. *Electronic Commerce Research and Applications*, 7, 1, 2008, 55–67.

Zacharia, G., Moukas, A., and Maes, P. Collaborative reputation mechanisms in electronic marketplaces. *Decision Support Systems*, 29, 4, 2000, 371–388.

Zhang, B., Zhou, Y., and Faloutsos, C. Toward a comprehensive model in Internet auction fraud detection. In R. H. Sprague (ed.). *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), Waikoloa, HI, Jan 7–10, 2008*, IEEE Computer Society, Los Angeles, CA, 2008, 79–87.