Electronic Commerce Research and Applications 13 (2014) 79–97

Contents lists available at ScienceDirect

Electronic Commerce Research and Applications

journal homepage: www.elsevier.com/locate/ecra

Analysis of fraudulent behavior strategies in online auctions for detecting latent fraudsters

Jau-Shien Chang [a,*], Wen-Hsi Chang [b]

[a] Department of Information Management, TamKang University, New Taipei City 25137, Taiwan, ROC
[b] Department of Management Sciences, TamKang University, New Taipei City 25137, Taiwan, ROC

ARTICLE INFO

Article history:
Received 20 October 2012
Received in revised form 28 August 2013
Accepted 28 October 2013
Available online 14 November 2013

Keywords:
Early fraud detection
Behavior fluctuation
Clustering
Online auction
E-commerce

ABSTRACT

Online auction fraudsters constantly monitor the contextual situations of the auction and change their behavior strategies accordingly to distract the attention of their targets. This flipping of behavior makes it difficult to identify fraudsters. Thus, legitimate traders need appropriate countermeasures to avoid becoming victimized. To help online auction users detect fraudsters as early as possible, this study develops a systematic method to discover the fraudulent strategies from proven cases of online auction fraud. First, according to the results of cluster analysis on the proven fraudsters, four typical types of fraud are identified, which are Aggressive, Classical, Luxury and Low-profiled. To provide better insight, a strategy is further represented by a series of status transitions. Hidden statuses of latent fraudsters are discovered by applying *X*-means clustering to the phased profiles of their transaction histories. As a result, various strategies can be extracted by such a systematic method and interesting characteristics are found in these strategies. For example, about 80% fraudsters in the Yahoo!Taiwan auction site flip their behavior no more than two times, which is not as complicated as expected originally. Based on these discovered fraudulent statuses, a high-resolution fraud detection method is performed to classify suspects into legitimate users or fraudsters in different statuses, potentially improving overall detection accuracy. A two-way monitoring procedure is then proposed to successively examine the statuses of a suspicious account. Analysis shows that the two-way monitoring method is promising for better detection of well-camouflaged fraudsters.

1. Introduction

Online auctions have become more profitable over the years, largely because such activities are not constrained by limited business hours and physical store locations. Moreover, the trading volume of online auctions increases as new trading opportunities emerge. For example, eBay, the largest worldwide auction site, posted US$ 11,651,654 in revenue for 2011 (eBay Inc. 2011), which significantly demonstrates the success of online auction business model. However, more trading disputes are inevitable with this higher trading volume, with fraud being the most threatening for users. With the anonymity and convenience that are part of the Internet environment, online auction fraudsters do not need to face target victims in person to complete their schemes. In addition, fraudsters often adjust their tricks as markets and situations change (Kaszuba et al. 2010, pp. 31–37), making it difficult for legitimate users to avoid fraudulent schemes. According to statistics of National White Collar Crime Center (NW3C) (2009, 2010), Internet auction fraud accounted for 25.5% of referred complaints in 2008, showing the seriousness of online auction fraud. While the number of reported complaints has declined in recent years, cases of online auction fraud are still listed among the top ten Internet complaints reported (NW3C 2011, 2012). The statistics imply that fraudsters now use fewer cases of schemes while increasing the dollar amount of the schemes and their success rate.

Fraudsters change their behavior statuses to perform specific tricks at particular moments to defraud innocent traders in online auctions. For example, a fraudster posing as a seller generally sells a large number of low-priced items in order to earn positive feedback at a minimal cost. After accumulating a high feedback score, he begins shelving high priced items. Once he sells one or more high-priced items and receives the transferred funds, the fraudster disappears immediately and never delivers the items. Obviously, online auction fraud is not a one-time act, resulting from a sequence of actions across the lifespan of a fraudster. In fact, after performing a given sequence of events, a fraudster may camouflage himself, staying in a particular status. For instance, a fraudster could complete a series of low-priced transactions to put himself in a status which contains high feedback scores, high trading density, and low average prices. In such a state, it may be easier to attract other members to trade with him. More complicated

* Corresponding author. Tel.: +886 223630386.
E-mail address: 090557@mail.tku.edu.tw (J.-S. Chang).

1567-4223/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.elerap.2013.10.004

fraudulent behavior can be formulated by a series of statuses, which is achieved through the use of a series of camouflaged actions. Obviously, legitimate traders would have more difficulty recognizing these cunning tricks.

To prevent fraud, most online auction houses implement simple reputation systems so that participants can evaluate potential trading partners. The reputation system used by eBay and Yahoo! Taiwan is a binary reputation system, which allows trading partners to leave positive rating or negative feedback ratings about the other trader after completing a transaction. The feedback received determines a member's accumulated score and his estimated reputation (or credibility) in the virtual society of the online auction site. In addition, the auction site will periodically report the backlist or suspended list to deter dishonest traders from committing fraud. And, general guidelines for fraud prevention will be announced for inexperienced traders. To enhance the reputation system, eBay further provides an extra-detailed rating mechanism to evaluate a seller (eBay Inc. 1995), which allows the buyer to leave feedback score for the obtained services such as 'item as described', 'communication', and 'shipping time'. In spite of these strong attempts by authorities of the auction sites, smart fraudsters constantly evolve their tricks to avoid detection.

Several deficiencies exist in such a simple reputation calculation method. For example, fraudsters can use fake personal information (or simply steal others' identities) to create multiple accounts to form a criminal syndicate. These accomplice accounts then initiate false trades and leave positive ratings for one another to accumulate high ratings during a very short period of time (Wang and Chiu 2005). In general, it is difficult to recognize a potential fraud through instinct only, especially if one is considering an account with a high reputation score. As a result, a less experienced trader can easily become a victim in spite of the reputation system. Therefore, researchers propose different methods of detecting online auction fraud to assist traders identify suspicious accounts (Pandit et al. 2007, Ku et al. 2007, Chang and Chang 2009).

To develop an effective fraud detection method, an appropriate measured attribute set is needed to describe or extract the characteristics of traders' behavior. In addition, a suitable learning method is also needed to build the detection model from the extracted data. Chau and Faloutsos (2005) proposed a set of price-related attributes and applied classification trees to construct their fraud detection method. In a different approach, Chang and Chang (2011, pp. 11251–11252)adopted several feedback-related attributes and incorporated them with classification and instance-based learning methods to improve fraud detection accuracy. To consider early fraud detection, Chang and Chang (2009, pp. 744–745) also proposed a hybrid-phased modeling method to detect latent fraudsters. In the case of organized fraud, social network analysis can be applied to extract the relationships among traders and help identify accomplices (Wang and Chiu 2005, Ku et al. 2007). Kobayashi and Ito (2007a, 2007b, 2008) visualized the networking relations using graphs theory to help users identify unusual partner relationships.

Even though these proposed fraud detection methods provide some degree of satisfaction, problems still remain. First, these detection methods produce a binary result, fraudulent or legitimate. However, fraud detection systems are often prone to misjudgment and may miss schemed and camouflaged fraudsters. This is because fraud is not just a result but a process. Examining the final (accumulated) status of a suspicious trader at a particular moment is not enough to detect a well-camouflaged fraudster. The behavior flipping of suspicious traders needs to be carefully investigated to identify these cunning fraudsters and increase the overall accuracy of detection processes. Second, behavior granularity and resolution also need to be improved in fraud detection outcomes. At present, when cases are erroneously classified (i.e., a legitimate trader is misjudged as a fraudster and vice versa), the developers of detection methods do not have enough information to deal with these missed targets. Finally, for the purpose of fraud prevention, it is more important to discover a latent fraudster before the fraud is activated. That is, it would be better to report potential fraud before legitimate traders are victimized. For this purpose, the suspect could be continuously monitored and not just looked at as part of a one-time detection process.

Based on the above discussions, it can be seen that a more elaborate and effective mechanism is needed to uncover fraudulent strategies and detect online auction fraudsters as early as possible. To this end, this study identifies four typical types of fraudsters by applying cluster analysis to the proven fraudsters, which are Aggressive, Classical, Luxury and Low-profiled. To provide better insight, the fraudulent strategies are extracted by examining the transaction histories of proven fraudsters.[1] A fraudulent strategy is defined by a series of status transitions, in which hidden statuses of latent fraudsters are induced by applying *X*-means clustering to their phased profiles. This process extracts 29 sequences and identifies several interesting characteristics. For example, about 80% fraudsters in the Yahoo!Taiwan flip their behavior no more than two times, which is not as complicated as expected originally. Furthermore, most fraudsters will keep their initial status at the end of their frauds, even after flipping their behavior several times. Based on these discovered fraudulent statuses, a higher-resolution fraud detection method can be performed, which classifies latent fraudsters into different groups and potentially improves the detection of specific types of fraudsters. Subsequently, for well-camouflaged fraudsters, a two-way status monitoring procedure is proposed to successively examine the statuses of a suspicious account. Analysis shows that the monitoring method is promising for better detecting well-camouflaged fraudsters.

The rest of this paper is organized as follows: preliminary information and a literature review are presented in the second section. The third section presents how to observe fraudulent flipping behavior using clustering techniques. Analyses of fraudulent behavior are discussed in the fourth section. The fifth section presents the experimental results of a new early fraud detection method using behavior statuses identification. The final section offers conclusions and suggestions for future work.

2. Preliminary and literature review

The concepts and techniques related to this study are introduced in this section. First, the features of online auction fraud are depicted. Next, the measured attributes of fraudulent behavior identification applied are discussed. Subsequently, the phased profiling technique is introduced to simplify the discussions in the rest of the article. Finally, we introduce the *X*-means clustering technique used in this study.

2.1. Online auction fraud

To handle transaction disputes and prevent fraud, the online auction sites have developed their own reputation systems to assist their members in selecting proper trading partners. In general, these reputation systems can provide some degree of protection for trading partners. However, cunning fraudsters can always find various ways to attack the reputation systems. Jøsang and Golbeck (2009) summarized nine different types of attacks and stressed the necessarity of designing a robust reputation system. Hoffman et al.

[1] These proven fraudsters in this study were gathered from the official announcement, known as the blacklist, of the online auction site of Yahoo!Taiwan.