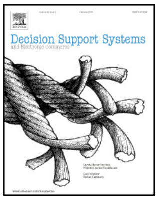
Decision Support Systems xxx (2016) xxx–xxx

Contents lists available at ScienceDirect

Decision Support Systems

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



Extracting and reasoning about implicit behavioral evidences for detecting fraudulent online transactions in e-Commerce

Jie Zhao [a], Raymond Y.K. Lau [b,*], Wenping Zhang [b], Kaihang Zhang [a], Xu Chen [a], Deyu Tang [c]

[a] *Department of Management Science and Engineering, School of Management, Guangdong University of Technology, Guangzhou 510520, China*
[b] *Department of Information Systems, College of Business, City University of Hong Kong, Hong Kong*
[c] *School of Medical Information and Engineering, Guangdong Pharmaceutical University, Guangzhou 510006, China*

ARTICLE INFO

Article history:
Received 12 August 2015
Received in revised form 9 April 2016
Accepted 9 April 2016
Available online xxxx

Keywords:
Theory of evidence
Evidence fusion
Fraud detection
Electronic Commerce

ABSTRACT

With the explosive growth of e-Commerce worldwide, there are also growing concerns about collusive fraudulent transaction attacks in e-Commerce. The main contribution of our research work is the design of a novel detection framework that can reason about implicit online user behavior for detecting collusive fraudulent transactions. Based on real transactional and user behavioral data collected from one of the largest e-Commerce platforms in the world, our experimental results confirm that the proposed detection framework can achieve an average true positive detection rate of 83% while the false alarm rate is kept at as low as 2.4%. To the best of our knowledge, this is one of the largest scale studies toward the detection of fraudulent transactions in e-Commerce. The managerial implication of our study is that administrators of e-Commerce platforms can apply our framework to detect and prevent fraudulent transaction attacks, and hence fair electronic trading is upheld in the ever expanding e-Commerce world.

1. Introduction

A recent study reveals that business-to-consumer (B2C) online sales worldwide have reached $1.5 trillion in 2014, with a growth rate of 20% over 2013.[1] Taobao, one of the largest e-Commerce platforms in the world, generated over 200 million online transactions and reached a peak rate of 205,000 transactions per minute just for its annual "singles' day" sales event taking place on 11 November 2013.[2] However, with the rapid growth of electronic commerce in the past two decades, so are the frequencies of various attacks to e-Commerce systems. The 2014 cybercrime report composed by the Center for Strategic and International Studies (CSIS) in the U.S. shows that the annual financial losses due to cybercrimes including the various attacks to e-Commerce systems may reach $600 billion.[3]

Among the different kinds of attacks to e-Commerce systems, collusive fraudulent transaction attack is the one that receives relatively less attention by researchers. In fact, there are strong financial incentives for cybercriminals (fraudsters) to generate fake online transactions. For instance, online reputation systems are widely adopted by e-Commerce sites (e.g., Taobao and eBay) so that buyers can indirectly evaluate the reliability of sellers by referring to their service ratings generated based on completed online transactions. To inflate these service ratings, a seller might pretend to be a buyer to purchase from her own online store, or employing a thirty-party attack agency to generate a large number of fake transactions and the corresponding service ratings. It is likely that inflated service ratings of sellers can boost their sales because buyers often rely on an online reputation system to determine from whom they should purchase in e-Commerce. For the study period from October 2008 to May 2009, the percentage of fraudulent transactions among all the consumer-to-consumer (C2C) online transactions conducted in China was found to be as high as 47% [1].

Nowadays, attacks against online transaction systems of e-Commerce sites are systematically managed by organized groups of cybercriminals (e.g., attack agencies). It is very difficult to detect collusive fraudulent transactions because these transactions may just look like legitimate transactions (e.g., having the same explicit features such as transaction amounts). Fig. 1 highlights a typical scenario of collusive fraudulent transaction attack in e-Commerce. The attack agency "C" is an organized group of cybercriminals. A dishonest seller "A" first approaches the agency "C" for generating fraudulent online transactions and inflated her ratings at an e-Commerce platform "D". The agency "C" accepts the attack requirements (e.g., number of fraudulent transactions and ratings generated in a certain period) posted by the dishonest seller "A" and starts to recruit some collusive buyers

[*] Corresponding author at: Department of Information Systems, City University of Hong Kong, Tat Chee Avenue, Kowloon, Hong Kong SAR.
E-mail addresses: zhaojie@gdut.edu.cn (J. Zhao), raylau@cityu.edu.hk (R.Y.K. Lau), wzhang23-c@cityu.edu.hk (W. Zhang).

[1] http://www.emarketer.com/Article/Worldwide-Ecommerce-Sales-Increase-Nearly-20-2014/1011039.

[2] http://www.bloomberg.com/news/2013-11-11/alibaba-breaks-sales-record-on-china-singles-day-amid-discounts.html.

[3] http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

http://dx.doi.org/10.1016/j.dss.2016.04.003
0167-9236/© 2016 Elsevier B.V. All rights reserved.

Please cite this article as: J. Zhao, et al., Extracting and reasoning about implicit behavioral evidences for detecting fraudulent online transactions in e-Commerce, Decision Support Systems (2016), http://dx.doi.org/10.1016/j.dss.2016.04.003

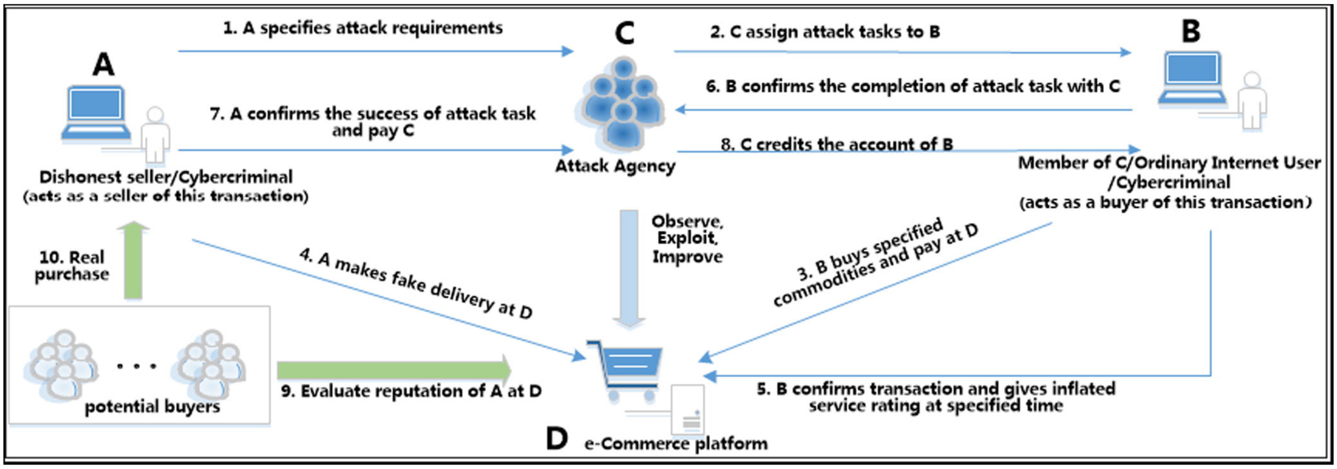

A
1. A specifies attack requirements
C
2. C assign attack tasks to B
B
6. B confirms the completion of attack task with C
7. A confirms the success of attack task and pay C
Attack Agency
8. C credits the account of B
Dishonest seller/Cybercriminal
(acts as a seller of this transaction)
Member of C/Ordinary Internet User /Cybercriminal
(acts as a buyer of this transaction)
10. Real purchase
4. A makes fake delivery at D
Observe, Exploit, Improve
3. B buys specified commodities and pay at D
potential buyers
9. Evaluate reputation of A at D
5. B confirms transaction and gives inflated service rating at specified time
D
e-Commerce platform

Fig. 1. A typical scenario of fraudulent transaction attack in e-Commerce.

such as “B”. A collusive buyer can be a professional cybercriminal (e.g., a member of the agency “C”) or just an ordinary Internet user. The agency “C” routes the attack requirements to “B”. Then, the collusive buyer “B” will purchase some commodities from “A” via the e-Commerce platform “D”. Upon receiving the online purchase from “B”, “A” will pretend to deliver commodities to “B”. After the online transaction is completed, “B” provides an untruthful (inflated) rating for the service quality of “A”. This cycle of fraudulent transaction generation is repeated by each of the recruited collusive buyers.

On the other hand, legitimate buyers observe the inflated rating of “A” via the e-Commerce platform “D”, and eventually they will be lured to purchase from the dishonest seller “A”. It is extremely difficult to detect collusive fraudulent online transactions based on explicit transactional attributes such as prices of commodities, types of commodities, amounts of transactions, or even the ratings of buyers [5]. The reason is that a fraudulent transaction follows the normal transaction processing cycle at the e-Commerce platform D.

Common approaches for detecting attacks to e-Commerce systems include statistical methods [13,40] and machine learning methods [20,22,25,47–49]. However, these methods often rely on explicit features for detecting fraudulent entities (e.g., a bid in e-Auction). As discussed before, collusive fraudulent transactions may just look like legitimate transactions because they follow the same transaction processing cycle of legitimate transactions at an e-Commerce platform. As a result, existing detection methods that mainly rely on explicit transaction or commodity features may not be able to distinguish between fraudulent and legitimate online transactions. More recently, graph theoretic approaches have been proposed to detect attacks against e-Commerce systems [14–17]. However, these methods often assume that attackers are closely connected within a small social circle. Accordingly, these methods are not effective for detecting attackers who are loosely connected to each other via the global online community (e.g., an attack agency that recruits ordinary Internet users as collusive buyers). In fact, some recent studies show that collusive attackers can easily conceal their relationships with other attackers or attack agencies through a variety of identity hiding methods [9,17].

Accordingly, there is a pressing need to develop an effective method which can take into account both explicit features of transactions (e.g., commodity attributes) and implicit behavior of transacting parties (e.g., how long a buyer browses a product description page before making an online purchase) to tackle fraudulent transaction attacks in e-Commerce. To the best of our knowledge, our work represents one of the largest scale studies toward the detection of fraudulent transactions in e-Commerce. The main contributions of our research work are summarized as follows: (1) we develop a novel fraudulent transaction detection framework that exploits implicit online behavior of transacting parties for the detection of collusive fraudulent transactions in e-Commerce; (2) we extend the classical Dempster–Shafer (DS) uncertainty reasoning model by developing a novel evidence fusion method that can combine possibly conflicting evidences; and (3) we develop a genetic algorithm (GA)-based computational method that can continuously search for the near optimal parameters for dynamically constructing the belief functions of the extended DS model.

The rest of this paper is organized as follows. A discussion of related research work and a comparison of existing work with our approach are given in Section 2. The proposed DS reasoning-based framework for detecting collusive fraudulent transaction attack is highlighted in Section 3. The computational details of the proposed detection framework are illustrated in Section 4. The experimental procedures and result analysis are discussed in Section 5. Finally, we offer concluding remarks and highlight the directions of future research work.

2. Related work

2.1. Feature analysis for attack detection

Previous research examined different categories of features such as *transaction context*, *social relationship*, *time factor*, and *behavioral factor* for the detection of attacks against e-Commerce systems. Transaction context refers to transaction related features including explicit features such as prices of commodities [3,5,8,26,27], durations of transactions [3,5,26,27], service quality [3], reputation of buyers (sellers) [5,26,27], and product comments [5]. These features were applied to improve online reputation models [3,26,27] or develop attack detection model [5]. Explicit features such as seller ratings [21–23], starting auction price [19,21,23], bidding increments [11,19,21], and seller transaction history [23,24] were applied to detect shilling attacks in online auctions.

Social relationships among entities were explored to identify potential attacks. The measure of *k*-core was commonly used to quantify the strength of a relationship between entities [5,14]. Earlier attack prevention models such as Eigentrust [28] and PeerTrust [29] exploited the ratings [15] of entities to identify attacks against social networks. Time factor was also examined to compose high level features such as historical ratings. Online reputation systems such as SPORAS [30] compared the most recent ratings with historical ratings to identify reputation attacks. The dimension of time was applied to monitor traitors' attacks [26,31]. Behavioral factors were examined to build users' preference models in recommender systems [32], or developing attack detection systems [33,36,37]. More recently, fine-grained features such as types of browsers, browsing patterns, IP addresses, and so on have been applied to detect various kinds of frauds in E-commerce [34,35].