An Early Fraud Detection Mechanism for Online Auctions Based on Phased Modeling

[1]Jau-Shien Chang and [2]Wen-Hsi Chang

1Department of Information Management, TamKang University
[2]Graduate Institute of Management Sciences, TamKang University

[1]jschang@mail.im.tku.edu.tw
[2]wenhsi.chang@gmail.com

Abstract

Reputation systems provided by online auction sites are the only countermeasure available for buyers to evaluate a seller's credit. Unfortunately, feedback score mechanisms are too easily manipulated creating falsely overrated reputations. Therefore, developing an effective fraud detection method can assist the user in identifying cases of fraud. However, none of existing research addresses the most important issue of early fraud detection, which is, discovering a fraudster before he defrauds. For effective early fraud detection for online auctions, this paper proposes a novel phased detection framework to identify a potential fraudster as early as possible. To heighten precision in detection, different quantifiable behavioral features were extracted and integrated with regression model trees to build phased fraud behavior models. To demonstrate the effectiveness of the proposed method, real transaction data were collected from Taiwan's Yahoo!Kimo for training and testing. The experimental results with these models show that the recall rate of fraud detection is over 82%.

1. Introduction

Convenience and anonymity are two main distinguishing features of online auctions that also caused convenient loopholes for fraudsters. For instance, fraudsters can create multiple accounts which can be used to inflate the reputation of each other thereby increasing the odds to successfully deceive. Fraudsters can also collude with each other as in an accomplice syndicate, through which swift communication and connection enables easy defrauding. According to the Internet Crime Complaint Center, statistics showed that the total dollar loss of online auctions fraud being over $43m [1]. The statistic clearly shows effective fraud detection and prevention mechanisms for online auctions are critical.

Existing reputation systems estimate the reputation of a trader by accumulating quantifiable feedback score from trading partners. As a result, fraudster syndicates can always fabricate trading records to raise their reputations until accumulated scores are at satisfactory levels for their target victims at which point more expensive items are offered by the fraudster.

Referring to these features, a fraud detection model can be built by classification trees, regression analyses, Bayesian network construction or fuzzy inference [2]-[4]. However, we found that related literature do not address the more important fact that fraud detection models should be effective in discovering fraudsters before they defraud. Further, current models have difficulty detecting a fraudster's transaction behaviors during his non-criminal period as these actions mimic those of regular legitimate users. This paper proposes a novel phased detection framework to identify a potential fraudster as early as possible. Phased modeling is capable of representing the different stages of a fraudster's lifecycle and is used to distinguish latent fraudsters from legitimate accounts. To demonstrate the effectiveness of the proposed methods, real transaction data were collected from Taiwan's Yahoo!Kimo for training and testing. The results showed that the recall rate of fraud detection was over 82.6%.

The rest of this article is organized as follows: Section 2, the literature review, introduces existing reputation systems, the design of different detection indices, and discusses the relationship between regression analysis and fraud detection. The third section explains how transaction histories were segmented to simulate fraudulent behaviors in the early stages of a fraud. Section 4 describes how we induce the featured indices from our observations of

978-1-4244-5228-6/09/$26.00 ©2009 IEEE

fraudsters, and how to build detection models. Section 5 presents the experimental results. And finally, the conclusion and future research directions are presented in the last section.

2. Related Work

For the convenience of further discussion, the related research on reputation systems and regression trees is introduced in this section.

2.1. Reputation Systems of Online Auctions

The estimated reputation between the received feedback and the accumulated score can be represented by the following simple equation,

AccumScore = AccmScore+1, if positive feedback,
AccmScore -1, if negative feedback, Unchanged, if
neutral feedback,

However, several deficiencies exist in such a simple calculation method, which are often utilized by fraudsters. First, the score does not reflect the actual credit level of a member. For example, the score is not associated with the monetary value of a commodity. Fraudsters have taken advantage of this loophole and have learned to build their feedback scores through a large number of low-valued transactions. When their score is high enough, fraudsters will offer high-priced products to attract target victims [5], [6]. Secondly, negative feedback from one dissatisfied buyer does not reflect the seriousness of a victim's loss. Fraudsters can use fake personal information (or simply steal others') to create multiple accounts to form a criminal syndicate. These accomplice accounts then initiate false trades and highly rate one another over a very short period to accumulate high ratings [7].

2.2. Frauds in Online Auctions

According to our observations, a fraudster's transaction history consists of both latency and execution periods. The latency period consists of planning and preparing for swindles and the execution period focuses on targeting victims. On the contrary, the transaction history of a legitimate account does not comprise obvious irregular behaviors as demarcations of different periods, and in practice, the transaction history of a legitimate user should remain consistent, regardless of its length,

2.3. Regression Analysis and Decision Tree Classification for Fraud Detection

Behavior modeling for fraud detection is one of the most popular applications of regression analysis. Mercer applied regression analysis to detect computer frauds by identifying the main characteristics of a computer fraud [8]. Brockett et al. also adopted regression analysis combined with specialists' expertise and experience to detect insurance claim fraud [9]. In addition, Kirkos validated the effectiveness of applying logistic regression to identify financial frauds [10]. Moreover, Kauffman and Wood used similar methods to predict reserve-price shilling in auctions [11].

In addition to regression analysis, decision trees have been applied to deal with fraud detection for decades as well. ID3 and C4.5 algorithms are the most commonly used algorithms for inducing decision trees [12]. Much of the research has demonstrated that decision tree classification is also a promising technique in modeling and identifying different kinds of fraudsters [13], [2], [3], [4]. Breiman proposed an approach that incorporated a decision tree inducer for discrete classes, and a scheme for inducing regression trees, called classification and regression trees (CART)[14]. Generally, regression is applicable in trend prediction and decision trees are able to transform a model into IF-THEN rules. The combination of the two notable characteristics of regression and decision trees of CART is quite successful in solving fraud detection problems [10]. Quinlan proposed another tree inducer, M5 using linear regression functions in the leaves. Frank used a simple transformation of the tree inducer M5′, based Quinlan's M5; a model tree induction technique which has proven successful in predicting continuous values [15], [16], [17]. When most attributes are numeric, the M5′ model tree generates more accurate classifiers than C5.0 [17]. So far, most research of online auction fraud detection applies decision tree-based classifiers, however, regression tree construction seems to have received far less attention in academia [18].

3. Phased Modeling Framework for Early Detection

Due to evidence-based principles, law enforcement agencies are only able to arrest a suspect as a result of an actual victim's testimony. This implies that without the presence of a victim, fraud cannot be identified meaning early detection or prevention of online fraud is much more difficult.

3.1. Lifespan of Fraudsters and Early Fraud Detection

A general procedure of online auction fraud detection can be divided into the following two phases: (1) Building models for fraudsters: the transaction histories of fraudsters are collected and are combined with those of normal traders to build a detection model (2) Fraud detection: the transaction history of a suspicious account will be fed into the detection model to determine whether this account is a fraudster or not.

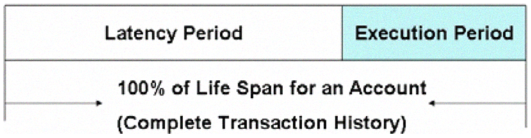
Latency Period
Execution Period
100% of Life Span for an Account
(Complete Transaction History)

Figure 1. Lifespan of a Fraudster

From our observation; a fraudster's lifespan can be divided into the latency period and the execution period (Shown as Figure1). The latency period is the stage of planning scams, in which preparation and developing high feedback scores are the main activities. The execution period is the stage where victims are targeted and scamming occurs. In practice, during the latency period a fraudster could appear to be behaving as a regular legitimate user. Though some fraudsters may exhibit sophisticated patterns during the latency period, these would be very difficult for most online auction users to detect. On the contrary, even novice buyers easily identify the behavior of a fraudster during the execution period. The previous discussion implies that if the fraud detection model relies solely on behavior during the execution period, it would be ineffective for early detection. We consider that well-designed fraud detection mechanisms should be capable of identifying not only potential fraudsters, but also when they might commit frauds.

To identify a premeditated fraudster during the latency period, a phased modeling framework is proposed for early detection. In the proposed framework, aside from the entire transaction history of a fraudster (100%), the behaviors in different phases of the fraudster's lifespan (e.g., 80% and 90% of the lifespan) are also used to build detection models respectively. According to our observations, a transaction history that includes fraud(s) can easily be identified by the 100% detection model, which means the fraud has already occurred. In addition, the 100% model implies the transaction history contains the fraud execution point somewhere close to the end of the lifecycle. Therefore, it stands to reason that even if the end of the fraudster's lifecycle has not been reached, the behaviors of the potential fraudster should match those of the 100% fraud detection models. During the latency period, the 100% detection model would fail to identify a fraudster because no criminal behavioral traits are present. In such a case, other detection models built by using different phases of a fraudsters' lifespan could then be used to test the suspicious target.

For phased modeling, the transaction history of a trader is partitioned by the accumulated ratings. Given an account u and transaction history TH(u)= {tr1, tr2, ⋯, trn}, the r% lifespan of u is denoted as TH(u,r%)={ tr1, tr2, ⋯, trd}, and $d=\lceil n*r\% \rceil$. For example, if n=50, then TH(u, 80%) would be { tr1, tr2, ⋯, tr40 }. We use M(r%) for behavior model in r% phase, or the model for r% of lifespan.

3.2. Procedures for Early Detection

When an account is judged as not currently committing fraud, it implies a fraud will occur sometime after the checkpoint of our phased models. In our approach, we exclude all impossible points to narrow the range of a fraud occurrence. Though this approach might affect the precision rate slightly, it will still be suitable for sending warning messages. False predictions would cause extreme money loss, especially misidentifying a fraudster as a legitimate seller. Therefore, we created a conceptual strainer that is analogous to hybrid-phased models (Figure 2). Conceptually the strainer works with transaction behavior as it does with other material; a large-holed strainer is used first to filter fraudsters and legitimate accounts. In this way, all accounts matching phase 80%-100% will be filtered out. Next a smaller-holed strainer filters phase 85%-100% fraudulent behaviors, and another finer strainer is used to filter out fraudsters in phase 90%-100%, and then to deal with phase 95%-100%. Finally, we apply the finest-holed strainer to eliminate phase 100%, so as to accomplish early online auction fraud detection.

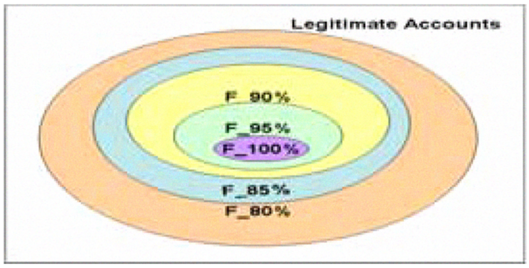

Figure 2. Conceptual Strainers for Phased Models

4. Construction of the Fraud Detection Model

The quality of a constructed tree is closely related to the selected attributes in classification.

4.1. Online Auction Fraud Detection Measuring Factors

Most previous related work related to the statistics generated using open transaction information of online auction sites for factors measuring fraudulent behavior, such as percentage of positive and negative feedback ratings, average, standard deviation and median commodity prices within a specific time range, and so on [2], [3], [19] In addition to numerical values (such as the starting bid) and Boolean values for denoting particular status (such as being a shop owner) [7], there are other more sophisticated attributes, such as using K-core in a transaction network which is helpful for detecting reputation inflation [3], [4], [19], [20]. Even though many factors for fraud detection have been proposed, few take the time-dependent behaviors of a fraudster into consideration. For example, if an account suddenly obtains many positive ratings within a short time, it could be inferred that the seller is suspect of artificially raising feedback scores. To further take into account the time-dependent behaviors of fraudsters, 7 measuring factors in numeric have been developed for constructing decision trees for online auction fraud detection. Two have been commonly used in the previous work and five of them have been newly developed in this work (Refer to Table 1).

Table 1. Measuring Factors

Factor	Description
DensityOfPos	Density of obtaining positive ratings
DensityOfNeg	Density of obtaining negative ratings
EndCloseToPos	Density of obtaining positive ratings after closing bid
RatioOfSToS	Given being a seller, the ratio of positive ratings from other sellers to all positive ratings
LastNegCloseToCur	Time difference from the last negative rating to the current time
RatioOfPos	Ratio of positive ratings to total feedback count
RatioOfNeg	Ratio of negative ratings to total feedback count

4.2 Building Fraudster Models Based on Model Trees

Both regression trees and model trees incorporate the characteristics of decision trees and regression analyses. An online auction fraud case could potentially be discovered through different combinations of multiple irregular behaviors. Thus, it seems that constructing a single model, which could identify all types of fraud, would be impossible. Since construction model trees inherently contain multiple regression models, they are especially effective in providing a solution to this problem. There are various kinds of regression techniques and decision trees which can be integrated for classification in most cases. For the sake of simplicity, we focus on model trees with linear regression equations in which linear regression equations are the decision criteria in transforming multiple linear regression models for classification. One regression model was built for each class value based on the concept of Classification via Regression [17]. In this work, the ClassificationViaRegression classifier has been used in Weka3.6.0 which implements base routines for generating M5' model trees and rules to identify fraudsters.

5. Experimental Results

5.1 Evaluation Metrics and Data Set

To show the effectiveness of our approach, the following parameters were adopted as the metrics for comparison and evaluation (Shown as Table 2), In this context, a Positive case is one corresponding to a fraud; on the other hand, Negative stands for a non-fraud case.

Table 2. Evaluation Metrics

Metric	Definition
TP Rate	TP/(TP+FN)
FP Rate	FP/(FP+TN)
Precision	TP/(TP+FP)
Recall	TP/(TP+FN)
F-Measure	2 ×Recall ×Precision/(Recall+ Precision)

T=True F=False P= Positive N=Negative

To prepare a data set for testing, we collected the transaction histories of 1,467 accounts from Taiwan's Yahoo!Kimo auction site, comprising of 236 fraudsters and 1231 legal traders. The transaction history of each account is segmented into 5 different phases (phase 80%, 85%, 90%, 95% and 100%) in order to extract phased behavioral features respectively. We randomly select 312 legitimate accounts and 156 fraudsters as a training set. The results of all extracted features were combined to form a data set consisting of 2,340 phased behavior profiles with 7 factors. The data of the training set was then used to build hybrid phased models (Refer to Figure 3) applying Adaboost with ClassificationViaRegression classifier in Weka3.6.0. In addition to the training sets, we randomly selected 156 legitimate accounts and 78 fraudsters from the remaining data to generate 1,170 phased profiles were reserved for testing.

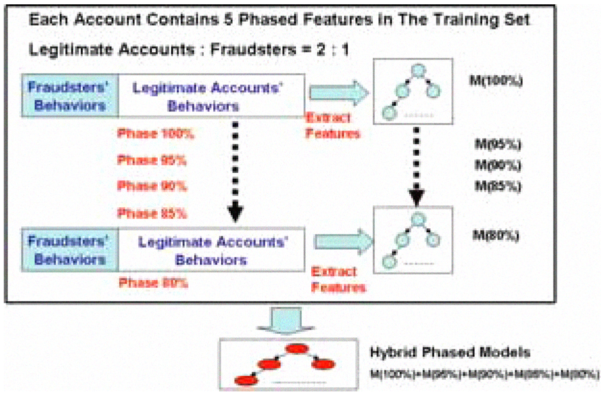
Each Account Contains 5 Phased Features in The Training Set
Legitimate Accounts : Fraudsters = 2 : 1
Fraudsters' Behaviors
Legitimate Accounts' Behaviors
Extract Features
M(100%)
Phase 100%
Phase 95%
Phase 90%
Phase 85%
M(95%)
M(90%)
M(85%)
Fraudsters' Behaviors
Legitimate Accounts' Behaviors
Phase 80%
Extract Features
M(80%)
Hybrid Phased Models
M(100%)+M(95%)+M(90%)+M(85%)+M(80%)

Figure 3. Hybrid Phased Models

5.2 Experimental Results of Classification of Phased Models

The experimental results of classification of phased models are presented as table 2.

Table 2. Experimental Results

TP Rate	FP Rate	Preci sion	Recal l	F-Measure	Class
0.873	0.173	0.909	0.873	0.89	Legit
0.826	0.126	0.765	0.826	0.794	Fraud

The behavioral features of a fraudster with a complete (phase 100%) transaction history were found to be unlikely during the latency period. Therefore, to screen behavioral changes during the latency period, we segmented the transaction history into different phases in order to emulate the early stage movements. From this, behavioral models were built respectively. In our experimental observations, some fraudsters in phase 80%-85% carried out legitimate trades in order to lure expected potential victim responses. When fraudsters advanced to phase 90%, their behaviors were similar to phase 80% in terms of time. Therefore, differentiating phases 80% and 90% proved difficult. However, behaviors in phase 80% differed from phase 100% in which behaviors were more aggressive in order to obtain results. The changes in behavior were analogous to our conceptual strainer theory for refinement. First, we categorized fraudsters into phase 100%, then phase 95%, and so on. Successively, we predicted which period the categorized fraudsters were approximately. We use a set of consecutive conceptual strainers for identifying the phase of a fraudster with individual phased models respectively (Shown as Figure 4, Fr% stands for fraudsters in phase r%.)

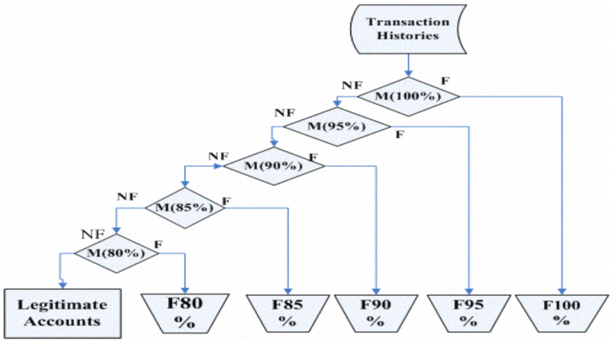

Figure 4. Fraudster's Phase Identification

6. Conclusion and Future Work

Under the current conditions, it is more practical to continue using existing reputation systems to enhance the capability of early detection of online auction fraud. Our experimental results show that Recall rate of detection current and potential fraudsters by the phased behavior models is 82.6%. The results not only demonstrate the effectiveness of the factors we have devised and the feasibility of our early detection theory, but also reflect behavior combinations of fraudsters in the real world. Even though our findings have demonstrated practicality in online auctions, some shortcomings require improvement in the future: (1) Our approach cannot grapple with identity theft. Because the transaction history we used did not belong to a thief, accounts always enter the execution period directly without any preparation. (2) It is difficult to identify the exact reasons sellers obtain negative ratings. Certain personal dissatisfaction or other non-criminal reasons may cause negative ratings, which might lower the dependability and lead to misjudging a legitimate seller as a fraudster. (3) Shorter lifespan trends of fraudsters reduce users' response time. (4) The devised behavioral models are ineffective in the very early period of the transaction history. Particularly, it is not useful in building an effective detection model for behavior before phase 80%.

References

[1] Internet Fraud Complaint Center, "2008 Internet Crime Report – January 1- December 31," National White Collar Crime and the Federal Bureau Investigation, Apr. 2009; http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf

[2] D. H. Chau, and C. Faloutsos, "Fraud Detection in Electronic Auction," *in Proceedings of European Web Mining Forum (*EWMF 2005) at ECML/PKDD, Oct. 3-7, 2005.

[3] D. H. Chau, S. Pandit and C. Faloutsos, "Detecting Fraudulent Personalities in Networks of Online Auctioneers," *in Proceedings of PKDD 2006(LNAI 4*213), pp. 103-114, Sep. 18-22, 2006.

[4] Y. Ku, Y. Chen and C. Chiu, "A Proposed Data Mining Approach for Internet Auction Fraud Detection," *Lecture Notes in Computer Science 4430 Springer,* pp. 238-243, Apr. 11-12, 2007.

[5] S. Curry, "Online Auctions: The Bizarre Bazaar," *Internet Scambuster*, vol. 43, no.1, 2001, p.p. 1-43.

[6] R. J Kauffman and C. A. Wood, "Irregular Bidding from Opportunism: An Exploration of Shilling in Online Auctions," *Information Systems Research*, vol. VV, 2007, pp. 1-36.

[7] J. Wang and C.Q. Chiu, "Detecting Online Auction Inflated-Reputation Behaviors using Social Network Analysis," *in NAACSOS Conference 2005 Proceedings*, Jun. 26-28, 2005.

[8] L. Mercer, "Fraud Detection via Regression Analysis," *Computers and Security*, no. 9, 1990, pp. 331-338.

[9] P. Brockett, R. Derrig, L. Golden, A. Levine and M. Alpert, "Fraud Classification using Principal Component Analysis of RIDITs," *Journal of Risk and Insurance,* vol. 69, no.3, 2002, pp. 341-371.

[10] E. Kirkos, C. Spathis, and Y. Manolopoulos, "Data Mining Techniques for the Detection of Fraudulent Financial Statements," *Expert Systems with Applications*, vol. 32, issue 4, 2007, pp. 995-1003.

[11] R. J. Kauffman, and C. Wood, "A Running up the Bid: Detecting, Predicting, and Preventing Reserve Price Shilling in Online Auctions." *In International Conference on Electronic Commerce*, Pittsburgh, PA, 2003.

[12] T. Mitchell, *Machine learning*, Singapore: McGraw-Hill, 1997, pp. 65-69.

[13] H. Shao, H. Zhao and G. Chang, "Applying Data Mining to Detect Fraud Behavior in Customs Declaration," *in Proceedings of the First International Conference on Machine Learning and Cybernetics,* pp. 1241-1244, Nov. 2002.

[14] E. Breiman, J. Friedman, R. Olshen and C. Stone, "Classification and Regression Trees," Belmont, CA: Wadsworth International Group, 1984, pp.8-15

[15] J. R. Quinlan, "Learning with Continuous Classes," *in 5th Australian Joint Conference on Artificial Intelligence*, Singapore, 1992, pp. 343-348

[16] Y. Wang and I. H. Witten, "Induction of model trees for predicting continuous classes," *in Poster papers of the 9th European Conference on Machine Learning*, University of Economics, Faculty of Informatics and Statistics, Prague, 1997.

[17] E. Frank, Y. Wang, S. Inglis, G. Holmes and I. H. Witten, "Using Model Trees for Classification," *Machine Learning,* 1998, vol. 32, no.1, pp. 63-76.

[18] A. Dobra and J. Gehrke, "SECRET: A Scalable Linear Regression Tree Algorithm," *In Proc SIGKDD'02 Edmonton,* Alberta, Canada, 2002.

[19] S. Pandit,, D. H. Chau,, S.Wang, and C. Faloutsos, "NetProbe: A Fast and Scalable System for Fraud Detection in Online Auction Networks," *in Proceedings of the 16th international conference on World Wide Web*, pp.201-210, May. 2007.

[20] M. Kobayahi, and T. Ito, "An Approach to Implement A Trading Network Visualization System for Internet Auctions," *in Proceedings of the Second International Conference on Knowledge, Information and Creativity Support Systems*, Ishikawa, Japan: (KICSS 2007), Nov. 5-7, 2007.