Framework for Online Auction Fraud Detection

S.MD.HAROON

M.Tech, PG Scholar.

D.KHADAR HUSSAIN

M.Tech(CSE Dept), Research Scholar,

JNTU College of Engineering, Anantapuramu-515002.A.P.

ABSTRACT

As the internet becomes more pervasive in all areas of human activity, attackers can use theanonymity of the cyberspace to commit crimes and compromise the IT organization. As presently there isno generally implemented authentication technology we have to monitor the contents and relations ofmessages and internet traffic to detect infringements. Online shopping and online auction have achieved more and more recognition due to theemergence of the world wide open and the problem of building online machine-learned models for identifying auction deception in e-commerce web sites is considered. As people are enjoying the advantages from online trading (exchange), traitors (defectors) are also taking benefits to accomplish deceptive activities against candid parties to obtain dishonest income. To detect and prevent such dishonest (illegal) and deceptive activities proactive fraud-detection moderation systems are commonly applied in practice. Machine-learned models (prototype) which are learned online are capable to catch deceptive more proficiently and quickly than human-tuned rule-based systems. An online probity model framework is proposed in this paper that takes online feature scope, co-efficient limits from human associate and numerous instances learning into account concurrently. We show that this model can probably differentiate more deceptions and extensively decrease customer complaints which are based on a real-world online auction fraud detection data compared to several baseline models and the human-tuned rule-based system.

Keywords:**WWW (World Wide Web), Online shopping, Fraud Detection, Online Probity Model, Auction.**

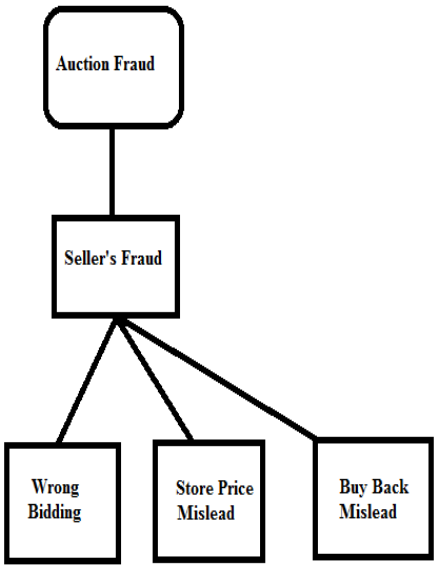
1. INTRODUCTION

Nowadays various websites are allowing Internet users to purchase and trade products which profits everyone in terms of effortlessness and effectiveness [1, 2]. People are enjoying the advantages from online trading; traitors are also taking advantages to accomplish deceptive activities against candid parties to obtain false profit. Online auction however is a diverse business model by which items are sold through price bidding [3]. Usually there is a starting price and finishing time which is mentioned by the sellers. Possible buyers bid against each other once the auction creates, and the winner gets the article (item) with their maximum winning bid [4-6]. Online auction attracts criminals to commit fraud relating to any platform supporting financial relationships. The unreliable types of auction fraud are as follows. Products obtained by the buyer are not distributed by the seller. The sent products do not match the portrayals that were posted by sellers [7, 8]. The nasty sellers may even post non accessible items with fake description to mislead buyers [9, 10] which is shown in Fig 1, and ask for payments to be wired directly to them via bank-to-

ISSN: 2278 – 1323

bank wire transfer. To providesome guarantee against deception, Electronic-commerce sites often give insurance to fraud victims to cover their loss up to a certain amount.

Fig 1: Online Auction Fraud



2. APPROACHES TO PREVENT FRAUD

In order to lessen the amount of recompenses and to improve their online reputation, ecommerce providers often implement the following approaches to control and prevent (avoid) fraud. The identities of registered users are authenticated through email, SMS, or phone verifications [11, 12]. A rating system where buyers offer feedbacks is commonly used in ecommerce sites so that deceptive sellers can be caught immediately after the first wave of buyer opposition. In addition, to manually review distrustful sellers or buyers, proactive control systems are built for allowing human experts. There are still many outstanding and challenging cases to fight frauds with a moderation system even the e-commerce sites spend a big (large) budget (financial plan). Traitors (defectors) and deceptive sellers regularly change their accounts and IP addresses to evade being caught [13]. It is usually infeasible for human experts to inspect every buyer and seller to decide if they are committing deception, especially when the ecommerce site attracts a lot of traffic. The designs of deceptive sellers frequently alter constantly to take the benefits of material trends. For example, deceptive sellers sell the "newest" products at the time to attract more potential victims [14]. Also, when they find a loophole (gap) in the fraud detection structure, they will immediately leverage the weakness.

3. ONLINE AUCTION FRAUD RELATED WORK

Online auction deception is always renowned as an essential issue. There are articles on websites to teach people how to avoid online auction fraud (deception) [15,16]. Auction fraud is measured into fewkinds and proposes methodologies to contest them. To detect auction frauds, standard systems are used broadly by websites even though many of them use naive approaches. To elicit user feedback it is summarized by several key properties of a good reputation system and also the challenges for the modern reputation systems. A Markov random field model is introduced with a belief propagation algorithm for the user reputation as other representative work connecting reputation systems with online auction fraud detectioninvolved. Other than reputation systems, for monitoring and detecting fraud machine learned models have been useful to moderation systems. We treat the fraud detection problem as a binary classification problem in this paper. The most frequently used models for binary classification include logistic regression, probity regression, support vector machine (SVM) and resolve trees. When getting a batch (lot) of input the typical has to be updated according to the data and make predictions and servings for the next batch as online modeling considers the scenario that the input is given one piece at a time. The concept of online modeling has been applied to various areas, such as stock price fore-casting, web content optimization, and web spam recognition. Online education usually requires much lighter computation and memory load compared to offline models; hence it can be extensively used in real-time systems with uninterrupted support of inputs.

4. DATA MINING TECHNIQUES FOR PREVENTING FRAUDS

4.1) Detection of new fraud cases of a known fraud pattern. When a new case of fraud is detected, the goalof fraud detection is not only to stop and prosecute this particular instance of fraud, e.g., by dismissing anemployee who was involved in procurement fraud, but also to prevent similar cases of fraud from arising, example, by finding indicators that facilitate the identification of such cases earlier and with higher confidence. Supervisedlearning can be used to find these indicators by generalizing the single cases into high-quality rules, and preventthe same type of fraud from happening again.

4.2) Detection of new fraud patterns. It is safe to assume that new types of fraud are being developed all thetime. Hence, fraud detection cannot only rely on tracing known types of fraud, but must also incorporatemethods to find new fraud patterns. In order to do this, one cannot rely on known fraud labels, but must identifyunusual patterns based on other

ISSN: 2278 – 1323

properties of the data. Once a statistical significant abnormality is found, the patterncan then be reported back to a fraud officer for investigation. An example might be that a certain type of doctorspends much more money per patient than the rest. While it can be statistically confirmed that such a deviation inthe budget is indeed significant and not random, one can usually not decide from the given data whether there isa valid reason for the higher spending (e.g., the doctor treating a special group of high-risk patients that requiremore expensive treatment) or whether this is a sign of fraud. This makes unsupervised fraud detection morechallenging, because it needs to combine high statistical significance of the found patterns with interpretability,such that the experts can understand and judge the validity of the patterns.

5. CONCLUSION

Due to increasing usage of internet, online shopping and online auction has taken a major concern in e-commerce today. Now-days its gaining importance and this lead to frauds taking place and an innocent victim suffers without notice.

We present recent research on internet threats aiming at fraud or hampering critical information infrastructure. One approach concentrates on the rapid detection of phishing email, designed to make it next impossible for attackers to obtain financial resources or commit identity theft in this way.

Then we addressonline models for the auction deception restraint and discovery system. We show that our proposed online probity model framework is based on a real word online auction fraud uncovering data, which combines online features collection, clearingmeasurements from proficient knowledge and several instance learning and can extensively develop over baselines and the human-tuned model.

We presented how data mining techniques can be used to prevent fraud with fake auction goods, and online auction system. In future research we can incorporate other data mining techniques which could greatly improve the effectiveness of the whole detection process.

References

[1] Agarwal D, Chen B, Elango P. Spatio-temporal models for estimating click-through rate. In Proceedings of the 18th international conference on World Wide Web ACM 2009; 21-30.

[2] Andrews S, Tsochantaridis I, Hofmann T. Support vector machines for multiple-instance learning. Advances in Neural Information Processing Systems 2003; 577-584.

[3] Bliss C. The calculation of the dosage-mortality curve. Annals of Applied Biology 1935; 22(1):134–167.

[4] Borodin A, El-Yaniv R. Online computation and competitive analysis, Cambridge University Press New York, 1998.

[5] Breiman L. Random forests. Machine learning 2001; 45(1):5–32.

[6] Brent R. Algorithms for minimization without derivatives. Dover Pubns, 2002.

[7] Chau D, Fallouts C. Fraud detection in electronic auction. In European Web Mining Forum EWMF 2005; 87.

[8] Chipman H, George E, McCulloch R. Bart: Bayesian additive regression trees. The Annals of Applied Statistics 2010; 4(1): 266–298.

[9] Chu W, Zinkevich M, Li L, Thomas A, Tseng B. Unbiased online active learning in data streams. In Proceedings of the 17th ACM SIGK DDinternational conference on Knowledge discovery and data mining ACM, 2011; 195–203.

[10] Chua C, Wareham J. Fighting internet auction fraud: An assessment and proposal. Computer 2004; 37(10): 31–37.

[11] Collins R, Liu Y, Leordeanu M. Online selection of discriminative tracking features. IEEE Transactions on Pattern Analysis and Machine Intelligence 2005; 1631-1643.

[12] Cristianini N, Shawe-Taylor J. An introduction to support Vector Machines: and other kernel-based learning methods. Cambridge university press, 2006.

[13] Dietterich T, Lathrop R, Lozano-P´erez T. solving the multiple instance problems with axis-parallel rectangles. Artificial Intelligence 1997; 89(1-2): 31–71.

[14] Zhang L, Yang J, Tseng B. Online Modeling of Proactive Moderation System for Auction Fraud Detection.

[15] Federal Trade Commission. Internet auctions: A guide for buyers and sellers. http://www.ftc.gov/bcp/ conline/pubs/online/auctions.htm, 2004.

[16] Ku Y, Chen Y, Chiu C. A proposed data mining approach for internet auction fraud detection. Intelligence and Security Informatics 2007; 238–243.

ISSN: 2278 – 1323