Variable Bid Fee: An Online Auction Shill Bidding Prevention Methodology

Dhanmeet Kaur
Department of Computer Science and Engineering
Thapar University
Patiala, India
dhanmeetk16@gmail.com

Deepak Garg
Department of Computer Science and Engineering
Thapar University
Patiala, India
dgarg@thapar.edu

***Abstract*— A highly accelerated growth of e-market has lead to a well flourished online auctions scenario. Along with the attraction of numerous users world-wide, the online auctions have also allured in multiple frauds, periodically changing in nature and strategy to accustom to the proposed fraud detection and prevention approaches. As per the Internet Crime Complaint Center report 2013, auction fraud is enlisted as the topmost fraud accounting for drastic monetary losses. Amongst the online auctions frauds, shill bidding seems to be the most prominent fraud. In this paper, we present a variable bid fee methodology as a prevention technique for shill bidders. A bidder is charged for each of his bid based on the amount he bids. The winner of an auction wins back the charges he paid as bid fee; he gains an additional benefit to recover the bid fee he paid for the auctions he earlier lost in. This maintains the competitive spirit of an auction. On the contrary, the inherent nature of a shill bidder of frequently bidding in an auction and never winning one, will cause him perpetual monetary losses. We proposed this methodology based on the idea that the risk of losing money will reduce the tendency to exhibit shill behavior.**

Keywords—auction; fraud; bid-fee;

I. Introduction

E-commerce has taken the business to an altogether new level with auction market sprawling its firm hold in the e-market. Besides providing ease, comfort and convenient trade, this significant online auction market attracts umpteen fraudsters. As per the crime report by IC3 (Internet Crime Complaint Center, the auction fraud has drastically increased from being at ninth position in 'the top most common IC3 categories' with 5.7% complaints registered to being the topmost complaint category as 'auto-auction fraud' in 2013 report with a total of 14,169 registered complaints accounting for a loss of $51,581,511 [9].

An auction scenario involves a user, who registers as a seller and puts up items for auction on websites which may or may not include an initial starting price. Multiple users registered as buyers compete amongst themselves to obtain the item. Different auction sites are based on different auction protocols, the most common one being the English auction in which a minimum price is set. The highest bidder wins. Each auction has a limited lifetime but the bidders can bid anytime of the day or night as opposed to real life auctions that were constrained by the physical presence of sellers and buyers at a location restricted over a small duration of the day. Ebay, the pioneer and leading auction site has an intelligent recommendation system to help buyers bid smartly and stay in the competition. Most of the auction sites have a feedback mechanism with -1, 0 and 1 scores for unsatisfied, average and satisfied online trade. The feedback score is a reflection of the reputation of a user and also a potential area of fraud.

The minimal auction fee charges and the anonymity of participants lures in fraudulent groups. All types of frauds are difficult to define and hence hard to identify as well. Moreover, the types of frauds keep evolving with the changing online auction market. Some of the most common identified auction frauds are:

- *Non-Delivery of goods:* The buyer doesn't receive the good he has won in an auction and has already paid for in case of immediate payment schemes.
- *Misinterpretation:* The goods won in an auction are not as described by the seller on the auction site. The seller may have tactfully described the good or used Photoshop to enhance the product quality in the uploaded image on the site.
- *Fee-Stacking:* The seller increments the price of the good as determined at the end of the auction by applying additional charges such as shipping and handling charges which were not mentioned of during or prior to the auction process.
- *Triangulation:* It involves three actors – a buyer, a seller and a fraudster. The fraudster acts as a normal buyer to buy a commodity from a seller but uses fake credit card numbers for payment. The same fraudster acts as a seller to sell the product to a naïve buyer and immediately receives payment from him. The buyer becomes the victim of stolen product investigation.
- *Bid Shielding:* The buyer, through a fake account, hikes the price of an item beyond it's worth thus driving away potential buyers. The buyer withdraws this bid at the last moment and the second highest bid wins which is the buyer's

original account's bid or another buyer cooperating in the fraud.

- *Bid Shilling:* The seller creates fake accounts to act as buyers which increase the bidding price by small amounts during the auction thereby resulting in the further increment of the bid amount by the genuine rival buyers. This eventually leads to the product getting sold at a higher price.
- *Accumulation Fraud:* The seller establishes a good reputation through legal feedbacks by selling commodities of lower cost initially. A high positive feedback wins the trust of buyers. At this stage the seller puts a high priced item for auction with an immediate payment requirement. The seller gets the payment and doesn't deliver the product.
- *Ballot Stuffing:* The seller creates fake accounts that win the seller's auctions and provide him with a positive feedback. The seller's reputation gets enhanced based on the manipulated increment of the feedback score [1].

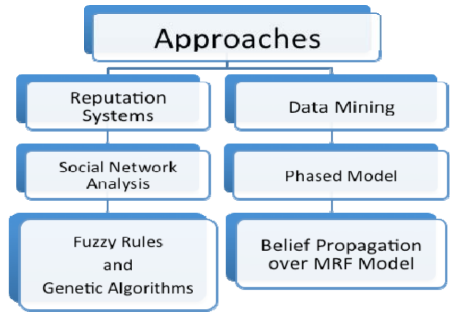
- *Buy and Switch:* The buyer receives a good quality product, replaces it with an inferior one and claims a replacement or the price paid.

By closely observing the behavior of the buyers and the sellers individually, the various frauds can be looked into but fraud detection becomes complex when multiple frauds occur simultaneously as in the current online auction fraud scenario. Nowadays, the fraudsters don't get involved in a fraud directly. Instead an additional group of accounts called 'accomplice' are involved. Fraudsters are not directly linked to the honest buyers. Accomplice forms an intermediate layer linking to fraudsters and protecting their identity on one end and simultaneously manipulating the honest buyers. The strategies of fraud keep changing as numerous fraud countermeasures evolve.

II. Literature Survey

Multiple approaches have been proposed and experimented to control the immense losses incurred due to auction frauds. Over a period of time, the scope of research has shifted from fraud detection to fraud prediction. Reputation systems, social network analysis, data mining, phased model, belief propagation over MRF model and a combination of fuzzy logic and genetic algorithms are the major areas that have made significant contribution in milestone achievements in the exploration of efficient techniques for fraud detection and prediction in online auctions.

Fraud Dealing Approaches:



A. *Reputation Systems*

The most basic and initially proposed countermeasure for online auction fraud was an integration of reputation system to the auction sites. It is based on the feedback mechanism. When an auction is over both the seller and the buyer can leave feedback for each other in terms of rating or comments which get accumulated in their respective profiles.

This simple approach has a few drawbacks. The feedback can be obtained by unfair means. A seller may create multiple accounts, participate and win its own auctions to rate itself positively. Also, an honest user may refrain itself from sending a negative feedback in fear of receiving a negative one in contempt [12]. Thus, both positive and negative ratings can be tampered with. Moreover, the comments do not add up to the final rating displayed on the user's profile. Though the content analysis on textual feedback may reveal additional information yet it is avoided on account of the amount of processing time involved. As is the case with the feedback scores, even the comments can be manipulated.

Inspite of its noticeable flaws, many auction sites use the reputation system because of its simplicity and comprehensibility by a layman.

Mikolaj Morzy proposed algorithms for the enhancement of reputation system by the incorporation of two factors- credibility and density, derived from introspection of interaction amongst the users. These factors help us to judge the users involved in an auction in a better way than the reputation systems based on mere feedback score [1].

B. *Social Network Analysis*

Social network analysis (SNA) is the mathematical and behavioral study of interactions amongst people or groups. SNA finds application in fraud detection in online auctions based on the observation that accounts involved in collusive groups tend to have a complicated relationship amongst them.

Google's Page Rank algorithm and HITS (hyperlink induced topic search) algorithm are the leading algorithms to rate the importance of a webpage on the internet. SNA along with the Page Rank algorithm has been explored to discover and rate the important accounts in a subgroup. Page rank algorithm rates the web pages based on the page rank of the pages pointing to the given page and the number of links leaving from those pages. The webpage with numerous inbound links from higher rated webpages will be an important webpage and thus will have a higher rating as well.

To detect collusive groups, initially SNA is utilized to detect a suspicious subgroup based on the chosen characteristics of graph such as clique, k-core or k-plex. A web crawler based on the chosen clustering parameter, helps capture potential fraudulent groups. Once the suspicious subgroup is identified, each node is assigned a score based on the modified page rank algorithm called Auction Fraud Rank algorithm which characterizes each node with a certain degree of suspiciousness parameter. The algorithm incorporates three additional parameters to the original page rank algorithm [2].

C. Data Mining Approach

Another basic approach to deal with detection of online auction fraud involves two steps namely, detecting outliers and building a decision tree.

Based on a set of certain attributes that contribute in analyzing and probable detection of a fraud, a dataset is created from the online auctions. The selection of attributes plays a major role in the proposed fraud detection system. The size and quality of the dataset of attributes directly affects the cost, accuracy and efficiency of the detection model being proposed. Wen-Hsi Chang and Jau-Shien Chang have categorized the attributes into three major groups – price related attributes, rating related attributes and item related attributes [3]. A major related issue is that not the whole history of users is available. Even if made available, it would lead to intensive computation and time consumption. Thus, the main focus should be on the selection of a small and relevant set of attributes that don't degrade the system performance by exhausting the available system resources as the system has to deal with the numerous auctions occurring at any real time instance. The need of the scenario being an efficient fraud detection system, the careful selection of attributes plays a vital role in determining the success factor of the proposed system.

Once the dataset has been created, the next step is to analyze the behavior of the users involved in the auction based upon the selected attributes and detect the outliers. The behavior of fraudsters differs from the behavior of normal users in some or the other aspect. Therefore, detection of outliers corresponds to the detection of potential fraudsters. Multiple methods have been proposed for the detection of outliers – an unsupervised learning technique such as a one class SVM being one of them [4]. This approach works well where shill bidding is involved.

Social network analysis on a set of user IDs is another technique to obtain a set of potential fraudsters [5]. Sometimes the normal users too might behave in a manner similar to that of the outliers or the potential fraudsters. To differentiate between the normal buyers and the cheats, data mining technique approach is incorporated. Usually C4.5, a decision tree learning method is used. Based on the pool of potential fraudsters identified in the previous step, C4.5 builds a decision tree. Each node of the tree gives a rule. Thus, these set of rules become prediction rules for the identification of fraudsters in future.

D. Phased Model Approach

Phased model approach is a predictive fraud detection approach. The available transaction history of the users is partitioned into smaller sections for an in-depth examination. The transaction history of a fraudulent account can be considered divided into two major portions – prior to the occurrence of the fraud know as the latency period of the account and during the occurrence of the fraud, known as the execution period. A phased model proposes analyzing the account at a few p% stages from the starting. For example, 30% phased model implies the analysis of the first 30% of the transaction history of the total lifespan of the account. Other than the timeline, even the rating can be considered as the basis for the phased model construction such as positive, negative and neutral rating phases of an account. At each phase, a learning algorithm is employed to explore the selected attributes that determine the behavior of a user. W.H Chang and J.S Chang suggested a modified wrapper approach [3]. They even suggested HCM, a hybrid complement phased model aimed to improve the accuracy of the detection system considering the fact that the latter part of the transaction history of lifespan of an account reveals more information wherein p% phase model implies the last p% of the transaction history of the account. The study of the phased model can be considered analogous to the study of the fraud development because a fraudulent account will be characterized by a noticeable change in its behavior over its transactional lifespan from its initial imitation of an honest user's activities to the execution of a well manipulated fraud. A general behavioral pattern of a fraudster can be concluded which forms the basis for prediction of similar frauds in future.

E. Belief Propagation over a Markov Random Field Model

2LFS, 2-Level Fraud Spotting, is a technique that combines both the bidder history as well as its interactions with other users to detect a fraud prior to its occurrence. The features in combination help detect fraud patterns. The problem is designed in form of the Markov Random Field Model, followed by the application of a belief propagation algorithm to yield the results [6].

A further modification of 2LFS has been presented as an algorithm named SPAN, Score Propagation over an Auction Network, to deal with the shrewdly planned collusive frauds in online auctions [7]. This algorithm inspects various graphs based on different selected feature sets of both sellers and buyers, to calculate a score which is combined to obtain a final anomaly score. The calculated anomaly score is transmitted using a modified belief propagation algorithm. A significant change was the modification of the update rule to include the level of interaction amongst users.

F. *Shill Score Algorithm*

Another significant contribution to the fraud detection techniques is the proposition of SSA, Shill Score Algorithm, by Jarrod Trevanthan and Wayne Read [8]. Its main focus is on detection of shill bidding. Based on the analysis of the behavior of an individual shill bidder or a collusive shill bidding techniques, formulae have been devised to calculate the shill score that assists in the identification of shill bidding accounts.

Fuzzy logic and genetic algorithms haven been together experimented with, to present an altogether different approach for fraud detection in online auctions. Fuzzy rules depict the fraud detection rules followed by the basic genetic algorithm functions to optimize the rules [10].

Another variant of a fraud detection mechanism is the architecture approach wherein a model for the online auction scenario is suggested to provide better security against frauds [11].

III. Variable Bid Fee: An Online Auction Shill Bidding Prevention Methodology

We propose this model to deal with the most prominent fraud in an online auction- shill bidding.

Shill bidding is an online auction fraud technique in which the seller tries to manipulate bidders into bidding more than they would have in a normal auction scenario. Thus, eventually increasing the selling price of the item. A shill bidder manipulates the honest bidders by bidding higher than them. An honest bidder, unaware of the fact that the increased bid was by another honest bidder or by a shill bidder, bids more and thus is trapped in a vicious cycle of bids in order to win the auction. The seller may achieve this by creating fake accounts or by colluding with other sellers to form a group. A group of shill bidders is formed in order to avoid easy detection of shill bidding. On the contrary, a single shill bidder account may catch even the naïve bidder's attention if the bid history is analyzed carefully.

The major characteristics of shill bidders are:

1) Minimum increment in the bid price: A shill bidder's main aim is to instigate the honest bidders to bid higher. Thus, if it raises the current bidding price by an appreciable higher bid amount, it might never get outbid by the honest bidders. Therefore, a shill bidder bids an amount barely enough to surpass the current highest bid.
2) A shill bidder avoids winning an auction which would mean the item on auction being returned to the seller himself. This is another reason that the shill bidder increments the highest bid by as little as possible. Also this makes shill bidders more active during the initial phase of an auction rather than towards the end. Shill bidding close to the auction termination time increases the risk of shill bidder winning the auction.
3) Minimum inter-bid interval time: It is characteristic of a shill bidder to bid as soon as possible after a bid by an honest bidder in an attempt to buy more time for the honest bidders to bid further.
4) Two prominent factors that can jointly be observed to indicate a potential shill bidder from the bid history are a high bid frequency and a high interaction with the seller.

Our proposed methodology for dealing with shill bidding stems from the fact that the two major factors responsible for the encouragement of shill bidding in online auctions are: ease of multiple accounts creation and negligible or minimal participation fee.

Stringent account registration conditions must be applied to deal with the first factor such as linking the user's ids to a phone number. Not that the individuals don't own multiple phone numbers but it can limit the multiple accounts creation on auctioning websites upto a certain extent. One Time Passwords (OTPs) help link a user account to a phone number.

The main idea of our proposed methodology, in an attempt to abate the shill bidding fraud, is the introduction of a variable auction participation fee. Each bidder pays a bidding fee, for every bid he places, proportional to the bidding amount. The bidding fee is kept low so as not to discourage bidders but on the same time dissuades a single or a group of shill bidders colluding together to bid frequently in order to increase the selling price of the item. As the number of shill bids by shill accounts increase, so does the bidding fee. The risk of losing money reduces the tendency to exhibit shill behavior. To keep up the spirit of an auction, the bidding fee scenario is so designed that the winner gets exempted from paying the auction fee. The winner's bidding charges are adjusted in the final winning bid once he confirms to buy the item he has won the auction for.

To account for the situations where an honest bidder exhibits a behavior similar to that of a shill bidder, a provisional is provided to win back the bidding charges of a previous auction. The winner of an auction gets a dual benefit. Along with concession of the bidding fee of the current auction he won, he gets to avail the opportunity to redeem the same amount of money lost in the previous auctions he didn't win. A shill bidder who doesn't aim to win an auction won't be able to recover the bidding charges of auctions. In an attempt to retrieve the lost amount, even if a shill bidder wins an auction that would imply a seller getting back his own item that was auctioned and eventually putting the seller at a loss. On the other hand, an honest bidder is motivated in order to win an auction to recover the prior losses if any due to a loss in an auction.

The algorithmic form of our methodology is presented further. LA_i, Locked Account, is a data structure proposed for each bidder i. It stores the amount, which is the bid fee corresponding to the auction id of the auction the bidder is currently participating in.

Consider the following bidding scenario for auction 'watch_sale'. Each entry in LA_i corresponds to a bid by bidder i. Amount specifies the bid fee charged on each bid which is 2% of the bid price by bidder i as per the proposed algorithm. A bidder may participate in multiple auctions. Therefore, auction_id identifies the bid fee entries corresponding to an auction. $Recoverable\_amount_i$ is the sum of bid fee entries of an auction that bidder i has lost. This is the amount which the bidder can retrieve on winning any further auction he participates in. In the following example, bidder b4 wins the auction and hence is privileged to retrieve the total bid fee he paid in this auction. Thus, only for bidder b4 the Recoverable_amount is transferred to the Recovered_amount. For the losing bidders, the Recovered_amount remains nil.

TABLE I. An online auction scenario

Bidder id	Price	Time	Bid_fee
b1	100	0.10	2.00
b2	125	0.20	2.50
b1	127	0.21	2.54
b3	150	0.26	3.00
b2	170	0.40	3.40
b1	172	0.43	3.44
b4	175	0.55	3.50

Bidder 1 seems a potential shill bidder as it exhibited the major characteristics of potential shill bidders.

LA_{b1}	
Amount	**auction_id**
2.00	watch_sale
2.54	watch_sale
3.44	watch_sale

$Recoverable\_amount_{b1}$
7.98

For bidder b2:

LA_{b2}	
Amount	**auction_id**
2.50	watch_sale
3.40	watch_sale

Let bidder b2 be an honest bidder and wins an auction in due time, he'll be able to recover the amount in contrast to the shill bidder b1 who won't win an auction and thus unable to regain any of his bidding charges back.

$Recoverable\_amount_{b2}$
5.90

For bidder b3:

LA_{b3}	
Amount	**Amount**
3.00	3.00

$Recoverable\_amount_{b3}$
3.00

For the winning bidder b4:

LA_{b4}	
Amount	**Amount**
3.50	3.50

$Recoverable\_amount_{b4}$
0.00

$Recovered\_amount_{b4}$
3.50

```
1.  Begin auction
2.      auction_time_left = auction.end.time - current_time
3.      while(auction_time_left)
4.          if bidder i wants to bid
5.              Input bid_amount from bidder
6.              bid_fee = 2% of bid_amount
7.              if bid_amount > current highest bid
8.                  Send for payment
9.                  if bid_fee is paid
10.                     bid = valid
11.                     LA_i: amount = bid_fee
12.                     LA_i: auction_id = id of the auction bidder i currently bid on
13.     winning_bid = highest valid bid
14.     winner = bidder of winning_bid
15.     if winner wants to pay
16.         amount_to_pay = winning_bid - ∑(bid_fee) for current auction_id – amount he
                wants to retrieve from total_recovered_amount
17.         if payment made
18.             item_purchased = true
19.             for bidder = winner and auction_id = winning auction id
20.                 benefit = ∑ LA_i: amount
21.             clear LA_winner entries whereauction_id = winning auction id
22.             for each bidder j where j ≠ winner
23.                 Recoverable_amount_j = ∑ (LA_j: amount) where auction_id = id of
                        auction bidder j lost
24.         goto 15
25.     else
26.         for each bid of declared winner i
27.             bid = invalid
```

```
            Recoverable_amount_i = ∑ (LA_i: amount) where auction_id = winning auction id
        goto 13
        if benefit > recoverable_amount_{i = winner}
            Recovered_amount_{i winner} = recoverable_amount_{i = winner}
        else
            Recovered_amount_{i = winner} = benefit
        Recoverable_amount_{i = winner}= Recoverable_amount_{i = winner} – Recovered_amount_{i = winner}
        total_retrieved_amount_{i = winner} = total_retrieved_amount_{i = winner} +
                    Recovered_amount_{i = winner}

End
```

Variable Bid Fee Algorithm

IV. Comparison of our proposed Variable Bid Fee Methodology with the prior proposed techniques

TABLE II. Comparison

	Requirements of a fraud detection/ prevention methodology		
	Bid History	***Data Mining***	***Fraud Calculation Parameter***
Auction Fraud Rank Algorithm	Required (Transactional dates of accounts involved)	Required (2-core clustering algorithm)	Auction Fraud Rank
Shill Bidder Detection for Online Auctions	Required (Bidder attributes)	Required (Outlier detection - SVM)	Rules derived from decision tree
Detecting Collusive Shill Bidding	Required (Bid and previous auction statistics)	Not Required	Shill Score
Variable Bid Fee Methodology	Not Required (Based on current bids in an auction)	Not Required	No complex calculations required. (Risk of financial loss reduces fraud)

In contrast to the other proposed collusive fraud detection techniques, our Variable Fee Bid methodology requires no bid history, data mining or complicated fraud parameter calculations. Due to these major differences our methodology is a faster and easier preventive measure of shill bidding. A consistent shill bidder or collusive shill bidding groups will eventually be at a loss. But our proposed methodology might dissuade one time bidders from bidding because they won't get a chance to recover the bid fee charges once they have lost the only auction they have participated in.

V. Conclusion

This paper proposes a variable bidding fee price methodology that targets shill bidding, the most dominant fraud strategy; in an e-auction market. It is a shill bidding prevention technique as collusive groups and individual shill bidder accounts will eventually be at a loss thereby dissuading sellers to continue with this fraud practice. We cater for the honest ferocious bidder behavior by providing them an opportunity to recover bid fee charges of their prior auctions on winning. An additional benefit to the winner is the exemption of the bidding charges.

The major benefit of our proposed methodology over other fraud detection and prevention techniques is that our methodology works on the current active auctions of the users. It does not require the bid history and bid attributes of bidders which increase the storage requirements as well as the calculation complexity.

VI. Future Work

We charged 2% of the bidding price as the bidding fee. Different pricing schemes can be explored to improve the effectiveness of our shill bidding prevention mechanism.

References

[1] Morzy, Mikołaj. "New algorithms for mining the reputation of participants of online auctions." [Algorithmica 52.1 (2008): 95-112].

[2] Lin, Shi-Jen, Yi-Ying Jheng, and Cheng-Hsien Yu. "Combining ranking concept and social network analysis to detect collusive groups in online auctions."[Expert Systems with Applications 39.10 (2012): 9079-9086].

[3] Chang, Wen-Hsi, and Jau-Shien Chang. "An effective early fraud detection method for online auctions." [Electronic Commerce Research and Applications11.4 (2012): 346-360].

[4] Yoshida, Tsuyoshi, and Hayato Ohwada. "Shill bidder detection for online auctions." PRICAI 2010: Trends in Artificial Intelligence. [Springer Berlin Heidelberg, 2010. 351-358].

[5] Ku, Yungchang, Yuchi Chen, and Chaochang Chiu. "A proposed data mining approach for internet auction fraud detection." Intelligence and Security Informatics. [Springer Berlin Heidelberg, 2007. 238-243].

[6] Chau, Duen Horng, Shashank Pandit, and Christos Faloutsos. "Detecting fraudulent personalities in networks of online auctioneers." Knowledge Discovery in Databases: PKDD 2006. [Springer Berlin Heidelberg, 2006. 103-114].

[7] Tsang, Sidney, et al. "SPAN: Finding collaborative frauds in online auctions." [Knowledge-Based Systems 71 (2014): 389-408].

[8] Trevathan, Jarrod, and Wayne Read. "Detecting collusive shill bidding."Information Technology, 2007. ITNG'07. Fourth International Conference on. IEEE, 2007.

[9] Internet Crime Complaint Center (2014), 2013 Internet crime report.

[10] Yu, Cheng-Hsien, and Shi-Jen Lin. "Fuzzy rule optimization for online auction frauds detection based on genetic algorithm." [Electronic Commerce Research13.2 (2013): 169-182].

[11] Ghasemi, Hamid-Reza, and Gholam-Reza Mohammadi. "Architecture-oriented approach for detecting fraud in the online auction." e-Commerce in Developing Countries: With Focus on e-Trust (ECDC), 2014 8th International Conference on. IEEE, 2014.

[12] Zhang, Bin, Yi Zhou, and Christos Faloutsos. "Toward a comprehensive model in internet auction fraud detection." Hawaii International Conference on System Sciences, Proceedings of the 41st Annual. IEEE, 2008.