Online Detection of Shill Bidding Fraud Based on Machine Learning Techniques

Conference Paper *in* Lecture Notes in Computer Science · June 2018

DOI: 10.1007/978-3-319-92058-0_29

Swati Ganguly
University of Regina
2 PUBLICATIONS 51 CITATIONS
SEE PROFILE

Samira Sadaoui
University of Regina
132 PUBLICATIONS 1,562 CITATIONS
SEE PROFILE

Online Detection of Shill Bidding Fraud Based on Machine Learning Techniques

Swati Ganguly and Samira Sadaoui(✉)

University of Regina, Regina, SK, Canada
{gangulys, sadaouis}@uregina.ca

Abstract. E-auctions have attracted serious fraud, such as Shill Bidding (SB), due to the large amount of money involved and anonymity of users. SB is difficult to detect given its similarity to normal bidding behavior. To this end, we develop an efficient SVM-based fraud classifier that enables auction companies to distinguish between legitimate and shill bidders. We introduce a robust approach to build offline the optimal SB classifier. To produce SB training data, we combine the hierarchical clustering and our own labelling strategy, and then utilize a hybrid data sampling method to solve the issue of highly imbalanced SB datasets. To avert financial loss in new auctions, the SB classifier is to be launched at the end of the bidding period and before auction finalization. Based on commercial auction data, we conduct experiments for offline and online SB detection. The classification results exhibit good detection accuracy and misclassification rate of shill bidders.

Keywords: Data clustering · Data labeling · Data sampling
Supervised learning · SVM · In-auction fraud · Shill bidding · Fraud detection

1 Introduction

E-auctions have greatly facilitated the selling and acquisition of goods and services. However, this industry, which involves millions of dollars, makes it attractive to fraudsters. Auctions are vulnerable to crimes committed by malicious moneymakers due to reasons like anonymity of users, flexibility of bidding, reduced legal policies against auction fraud and low costs of auction services. As per the Internet Crime Complaint Center (IC3), auction fraud is one of the most reported cybercrimes. In the IC3 report of 2015, a loss of 18 million USD has been recorded through 9,847 auction complaints. It is challenging to detect fraud occurring during the bidding process, called In-Auction Fraud (IAF), such as shill bidding, bid shielding and bid shading. In this study, we concentrate on Shill Bidding (SB) because it has been recognized as the most prevalent IAF and also the most difficult to detect due to its similarity to usual bidding behavior [6, 7, 22]. To improve his revenue, a seller may perform SB by creating fake accounts and/or colluding with other auction users. By considering the empirical studies of detecting shills, which experimented with data from different auction sites, this type of IAF occurred frequently [7, 19, 22]. Moreover, for many years, users complained about SB in various blogs and articles [14]. Contrary to eBay claim that only less than 0.1% of transactions are SB, it is estimated that the percentage

M. Mouhoub et al. (Eds.): IEA/AIE 2018, LNAI 10868, pp. 303–314, 2018.
https://doi.org/10.1007/978-3-319-92058-0_29

is actually 15%, 18% and 28% respectively for the three top selling categories: computer and networking, health and beauty, and eBay motors [13]. According to [5, 23], SB could lead to market failure. When caught, the guilty seller may be prosecuted. In 2001, three sellers were charged of SB worth a pay-off of $300,000 through 1100 auctions of art paintings [23]. The fraud was conducted on eBay with more than 40 fake accounts. In 2012, an auto-auction company was fined $70,000 for conducting SB fraud[1], and in 2014, a lawsuit was carried out against an auction company of real estate for committing SB[2].

The complexity of SB strategies makes their detection a difficult problem to solve. Additionally, to be successful, any SB detection model should address two important aspects: (1) dealing with the tremendous amount of auction data, including detailed information about bidders, sellers and auctions; and (2) learning from the characteristics of SB behavior to be able to detect SB accurately in new auctions. These requirements can be handled by Machine Learning Techniques (MLTs). Each MLT has its own pros and cons depending on the problem it is applied to. Numerous publications have showed the effectiveness of SVM across several classification and fraud detection applications. We select SVM to build our SB classifier because it possesses strong theoretical foundations, generalization capabilities, very good performance when learning with imbalanced training data (like SB data), and very fast execution when classifying new data (time is a critical requirement of e-auctions).

In this paper, we propose an approach to build offline the optimal SVM-based SB detection model, which comprises of several steps: measurement, clustering, labeling and sampling of SB data, and SVM parameter tuning. Unlike other fraud datasets, SB data are lacking because they are difficult to obtain. To produce SB data, we first define metrics to measure the SB patterns, and then compute the metrics from raw auction data. To generate SB training data, we apply the Hierarchical Clustering and then our own labelling strategy. Fraud data are highly imbalanced in nature, and this class imbalance has been shown to decrease the performance of MLTs [8, 10]. Also, imbalanced data results in misclassifying the minority class because MLTs are often biased towards the majority class [12]. This is inappropriate in fraud detection applications since fraudulent instances tend to be classified as normal. To be effective in solving the imbalanced learning problem, we utilize a hybrid method of data over-sampling and under-sampling. The learned SVM model once online is to be launched at the end of the bidding period of each auction to detect suspicious bidders before processing payment. First for each participant, the SB features are calculated based on the bidding transactions. Subsequently, the fraud classifier is fed with the new SB instances in order to deduce their labels: normal or suspicious. We use "suspicious" as the finding requires confirmation. Indeed, further investigation is conducted to confirm or reject the suspicion. When suspected bidders are found to be actual shills, necessary actions are then taken by the auction admin, such as cancelling the infected auction to avert money loss for honest bidders, especially for high-priced products. To assess the performance of our SB classifier in both training and testing, we conduct

[1] https://www.trademe.co.nz/trust-safety/2012/9/29/shill-bidding.

[2] https://nypost.com/2014/12/25/lawsuit-targets-googles-auction-com.

several experiments based on the most adequate classification metrics for fraud data and imbalanced data.

Our work improves previous SB studies in several aspects, such as the offline process to build the fraud detection model. To train accurately the SB classifier, we utilize a collection of the most relevant strategies practised by shills rather than uncertain features (like feedback ratings) or general auction features (like transaction records). In spite of SB datasets being highly imbalanced, none of the past research on SB classification proposed a pre-processing phase to address this problem. Moreover, a SB classifier should be able to operate in real-life scenarios. Still, existing SB detection approaches did not implement any online detection strategy. In our work, thanks to the auction-wise classification features, we are able to cancel any auction infected by SB in order to avert money loss for the winners.

2 Related Works

SB detection studies are limited contrary to other fraud detection applications. There is only one study [15] where SVM has been deployed to classify SB. However, this work employed general auction features, like item price (11), user profiles (3) and transaction frequencies (15), and also uncertain features, like reputation feedback (12). These features are inappropriate to train accurately a SB classifier. Furthermore, this paper did not disclose any information about the preprocessing and learning steps. Another work [25] utilized 1-class SVM to determine outliers (abnormal behavior) according to the bidder history and feedback ratings, and then applied Decision Trees to find shills. Our approach is different from these two SB classifiers with respect to the classification features. For instance, as pointed out by [17], feedback ratings may not be fully trusted because they are not always honest and can bias the fraud classifier. At times, fake accounts can be created to accumulate positive ratings, and also users do not always provide feedback, which leads to insufficient information for assessing the behaviour of sellers and buyers. Moreover, the two previous systems focus only on learning SB behaviour. Nowadays, it is also important to develop an online SB detection approach, like ours, that is able to suspend an auction if it is infected by SB. There is another research on SB detection [7] but it differs from our work in the following aspects. This study developed an incremental Back-propagation ANN. But it is often found that ANN suffers from local minima and high computational cost, and also there are many ANN parameters to control. These are not issues for SVM. Feedback rating is used as one of the classification attributes but as mentioned earlier ratings are not reliable to assess shills. The classifier in [7] deals with bidder-wise classification features resulting in actions taken against fraudsters only. Actions if not taken against each infected auction cannot stop the financial loss from happening. More recently, in [9], the authors proposed prevention and detection methods of shill bidders. The prevention method regulates the creation of unauthorized user profiles by verifying certain legal parameters against an existing database. The detection method implements a 2-layered hybrid model. First, the authors applied the K-means clustering based on two features to partition bidders for the learning purpose. For the online phase, the authors employed Hidden Markov Model to compare each new bid with the learned bidding behaviour to determine if a bidder is a shill or not. Processing each bid negatively impacts the system performance. Moreover, using only two attributes does not provide sufficient information to classify shill bidders.

3 Construction of Shill Bidding Dataset

3.1 Raw Auction Data

For our study, we utilize actual auction data that have been made public in the following link: www.modelingonlineauctions.com/datasets. The link displays auctions of three popular products extracted over a period of two months from eBay: Cartier wristwatches, Palm Pilot PDAs and Xbox game consoles. We select the PDA product because it attracted a large number of bidders, and according to eBay, today PDA belongs to the top 12 most sold item among 34 categories. Moreover, this product has a good price range and its auctions have a long duration (7 days). In fact, the higher the price, more a possibility of SB activities [6]. Also, shills have a better chance to imitate normal behavior in auctions with a long duration [5]. So based on these factors that encourage SB, our auction dataset is appropriate for SB learning. In Table 1, we conduct a statistical analysis of the PDA auction dataset.

Raw auction data are not always in a favourable condition, and thus require some cleansing. From the PDA set, we remove incomplete data, like records with a blank bidder ID, and noisy data, like auctions with less than three bids because they may bias the classification results. So, we delete 2.6% of auctions as shown in Table 1, and consequently we are left with 145 auctions.

3.2 SB Patterns and Weights

We choose eight SB patterns that have been found to be dominant across infected auctions [7, 19, 22]. These patterns represent the classification features that will decide whether a bidder is behaving suspiciously or normally (Table 2).

Afterwards, we assign weights (low, medium and high) to the SB patterns (Table 2). A weight denotes the relative importance of a pattern on the bidder's label, and the combination of all the weighted patterns influences the classification decision. Some of the patterns are similar to normal bidding behavior, thus making it difficult to differentiate between a normal and suspicious activity. E.g. we know that shills usually participate in auctions of some particular sellers. But there are situations where a normal bidder competes a lot for a certain seller due to reasons like the seller has an excellent reputation or he is the only one selling the item [22]. That is why we attach a medium weight to the 'Buyer Tendency' pattern. Furthermore, both 'Nibble Bidding' and 'Winning Ratio' indicate that some bidders, in spite of competing rigorously, hardly win. Both highly suggest shilling, and thus are assigned with a high weight. In fact, eBay has proclaimed in its buying guides that there are high chances that a bidder is performing SB when he nibbles with consecutive low increments but without winning the auction. For the experiments, we assign a value of 0.3 to the low weight, 0.5 to the medium weight, and 0.7 to the high weight [19].

Table 1. Statistics of source data

	PDA dataset
Total auctions	149
Total bidders (with unique ID)	1024
Total bids	3166
Average number of bidders per auction	7
Average number of bids per auction	21
Average winning price	$229.04
1-Bid auctions	NIL
2-Bid auctions	4

Table 2. Typical shill bidding strategies

Name	Description	Motive	Source	Weight
Starting price	Seller sets an unusually low starting price when compared to concurrent auctions (selling the same product)	To attract people to the auction	Auction	Low
Early bidding	Bidder submits a bid very early in the auction	To allure legitimate bidders to participate in that auction	Bid	Low
Bidding ratio	Bidder participates aggressively in the middle stage of the auction	To raise the auction price and attract higher bids from other participants	Bid	Medium
Nibble bidding	Bidder outbids oneself with consecutive small bids	To raise the auction price gradually	Bid	High
Last bidding	Bidder becomes inactive at the final stage of an auction	To prevent oneself from winning the auction	Bid	Medium
Winning ratio	Bidder competes aggressively in many auctions but hardy wins any auctions	The target is not to win the auction but to raise the price of the product	Bidder	High
Buyer tendency	Bidder participates exclusively in auctions of few sellers rather than a diversified lot	Collusive act involving the fraudulent seller and an accomplice who acts as a normal bidder to raise the price	Bidder	Medium
Auction bids	The number of bids in an auction with shilling is much more than that of concurrent auctions without shilling	To make the product appear more popular	Auction	Low

3.3 SB Measurement

To produce SB data, the eight SB patterns are measured for all the bidders of the 145 auctions. Based on the auction data source (organized with a total of 25 attributes), the patterns are computed against each bidder in each auction. As a result, we produce a SB dataset with a tally of 1639 instances. An instance, which represents the misbehavior of a bidder in an auction, is a vector of 10 fields: Auction ID, Bidder ID, and the eight fraud features. We measure most of these patterns based on the algorithms presented in [19] except for 'Nibble Bidding' and 'Starting Price' that we introduce in this paper. Each pattern is formulated in a way that the higher the value (normalized to [0, 1]), more the chances of fraud by the bidder. Next, we divide the SB dataset into two parts according to the start date of auctions: (1) 90% of data will be used for training the SVM classifier (offline SB detection). The resulting training set has a total of 1488 instances (130 auctions and 922 bidders); (2) 10% of more recent data will be used to test the SB classifier. The testing dataset contains 151 instances (15 auctions and 102 bidders).

4 Clustering Shill Bidding Data

The most challenging task of constructing any training set is to label its data. To this end, we need first to cluster the SB training data. We choose Hierarchical Clustering since researchers have successfully utilized this clustering method for partitioning fraud data [16, 18]. This method is found to produce better quality of the generated clusters when compared to other clustering techniques. It does not require the number of clusters to be defined in advance by the user. Determining this number shouldn't be done randomly. In our case, instead of hard clustering the data directly into two groups, we want the clusters to be created systematically. We can then label the clusters as 'Normal' or 'Suspicious' according to their general behavioural property as explained in the next section. The computational complexity is high for Hierarchical Clustering [7]. Still given the fact that our training set is of average size, this clustering type will work fast. In addition, since the training phase is an offline and one-time operation, the time-efficiency is not an issue. More precisely, we utilize the centroid linkage as the similarity measure to partition our training dataset since it is less affected by outliers unlike single-link or complete-link [7]. After applying Hierarchical Clustering on our training dataset, we obtain eight clusters exposed in Table 3.

Table 3. Data clustering and labelling results

Cluster ID	Size (approx.)	Label
Cluster 1	78%	Normal
Cluster 3	14%	
Cluster 5	<1%	
Cluster 7	2%	
Cluster 2	2%	Suspicious
Cluster 4	1%	
Cluster 6	<1%	
Cluster 8	1%	

5 Labelling Shill Bidding Data

In each cluster, we categorize each fraud pattern into ‘low’ or ‘high’ behavioral property according to the average value of all the bidders in that particular cluster. Here, a cluster denotes the most prominent SB patterns. Table 4 provides two examples of cluster analysis and labelling. In ‘Cluster 1’, we found that except for ‘Starting Price’ (low weight), all the other shill patterns are low in property. This means the bidders in this cluster are behaving normally as most of the SB patterns are low in property. In ‘Cluster 2’, bidders have dominant shill patterns with high and medium weights. Among these, the presence of high-weight patterns, ‘Nibble Bidding’ and ‘Winning Ratio’, indicates that bidders in this cluster are most probably shills. This way, based on which fraud pattern of what weight falls in the high or low property category, we label the cluster as ‘Normal’ or ‘Suspicious’.

In Table 3, among the 8 generated clusters, 4 clusters with around 5% of instances show strong implication of SB because of the patterns dominating these clusters. In these 4 clusters, patterns with high weights mostly belong to the high property category, which implies that the values of these patterns are higher than average. Thus, we label them as suspicious. The remaining clusters with 95% of instances are labelled as normal because the patterns in the high property category are of low weight, and most of the patterns with high weights are in the low property category. In summary, we obtain a labelled training set with 95% of normal instances and 5% of suspicious instances. This set is a highly imbalanced dataset that requires sampling before the learning process can take place in order to build an efficient SB detection model.

Table 4. Clustering analysis

Cluster ID	Behavioural property	Label
Cluster 1	**Low Value:** Early Bidding (low weight) Auction Bids (low weight) Bidding Ratio (medium weight) Buying Tendency (medium weight) Last Bidding (medium weight) Winning Ratio (high weight) Nibble Bidding (high weight) **High Value:** Starting Price (low weight)	Normal
Cluster 2	**Low Value:** Auction Bids (low weight) Starting Price (low weight) **High Value:** Early Bidding (low weight) Bidding Ratio (medium weight) Buying Tendency (medium weight) Last Bidding (medium weight) Nibble Bidding (high weight) Winning Ratio (high weight)	Suspicious

6 Sampling Shill Bidding Data

Handling screwed class distribution is a constant area of study in machine learning. A training dataset is imbalanced if the occurrence of positive instances (the minority class) is much less than the occurrence of negative instances (the majority class). In this situation, the classifiers are biased towards the negative class, which means that positive instances tend to be classified as negatives ones. This is inappropriate in fraud detection problems because once fraudulent transactions are labelled as normal and authenticated as legitimate, they can never be tracked thereafter. Moreover, as demonstrated in [8], classifiers suffer from low performance when dealing with highly imbalanced data. There are two ways for addressing the imbalanced learning problem: data sampling or cost-sensitive learning. We choose data sampling because it performs with similar effectiveness, if not better than that of cost-sensitive learning, and for moderate size of training sets, like ours, cost-sensitive learning algorithms do not work well [24]. In our study, we apply two intelligent over-sampling and under-sampling schemes: (1) SMOTE [3], which generates new positive instances and randomly places them between positive instances and their neighbors. When compared to other over-sampling techniques, SMOTE is more useful in creating a generalized decision region [2], and relatively achieves better results than any other random sampling and probabilistic estimation methods [4]; (2) SpreadSubsample [11], which produces a random subsample of the negative class based on the spread frequency (user defined) between the positive and negative class. For example, a spread frequency of 10 implies that for 10 positive instances, this method keeps 1 negative instance. Our labelled SB training set is highly imbalanced with a ratio equal to 19:1. Since SVM is efficient with moderately screwed class imbalance, therefore we need to perform data sampling by achieving the balancing ratio of 2:1. We try three methods, SMOTE only, SpreadSubsample only, and hybrid of both, to determine which one works the best for our particular SB training set. The experimental results showed that the hybrid method is more efficient. Indeed, we have achieved an AUC value of 86% for hybrid, 80% with SMOTE only, and 71% with SpreadSubsample only.

7 SVM Classification of Shill Bidding

SVM has been proved to be an efficient classifier in several fraud application problems [20], such as telecommunication, credit card, insurance and power utility. We chose SVM for the SB classification task for the following important facts:

- It is almost impossible to linearly separate auction data because of the evolving nature of the bidding process on one hand, and the distinctive features of SB fraud on the other hand [7]. This is where the kernel functions of SVM come into play to deal with no linearly separable auction data.
- According to a well-cited research [2] (cited 950 times), SVM is very efficient with moderately imbalanced data. Another work [21] showed that once sampling is performed on the training set, SVM outperforms major classifiers, like K-Nearest Neighbour, Decision Tree and Logistic Regression. In terms of the minority class,

SVM has been found to be superior to Naive Bayes and Decision Tree on several imbalanced benchmark datasets [26].

To build the optimal SB classifier, we need to select the best kernel and tune efficiently the SVM parameters. Since auction data are non-linearly separable, we need to use the non-linear kernel RBF shown to be effective in many classification and fraud detection problems [26]. Also, when the number of features is small and the number of instances is comparatively much higher, like our training set, RBF is the most suitable for classification. Next, we search for the best values of the cost parameter C and the free kernel parameter Υ. This is accomplished with the help of the K-fold Cross-Validation (CV) process that tries various pairs of C and Υ until the best performance is attained. The range that we define for C is [0.01, 10.0] and for Υ is [0.01, 0.9] as done in many past studies. Table 5 exposes the performance results for 5-fold and 10-fold CV. We can see that when the value of K is 10, the SVM model performs better since it achieves an AUC of 86% contrary to 82% when K is 5. There are several classification metrics but not all are suitable to assess the performance of fraud data and imbalanced data. In fraud detection problems, we are more concerned about suspicious bidders rather than normal bidders. So, here we focus on the detection accuracy and misclassification rate of the positive class. In Table 5, the Recall rate of 0.77 and Precision rate of 0.72 indicate that the SVM classifier does a good justice to the fraud class with acceptable detection rates. The SB classifier exhibits a very good overall performance of 0.86.

Table 5. Cross-validation

K = 5					
C	Υ	Precision	Recall	F-measure	AUC
1.5	0.1	0.692	0.310	0.429	0.654
1.5	0.9	0.708	0.586	0.642	0.791
2.3	0.1	0.760	0.655	0.704	0.826
2.3	0.9	0.680	0.586	0.630	0.791
2.5	0.1	0.760	0.655	0.704	0.826
3.0	0.1	0.731	0.655	0.691	0.825
K = 10					
C	Υ	Precision	Recall	F-measure	AUC
1.5	0.1	0.778	0.483	0.596	0.740
1.5	0.9	0.773	0.586	0.667	0.791
2.3	0.1	0.792	0.665	0.717	0.826
2.3	0.9	0.696	0.552	0.615	0.774
2.5	**0.1**	**0.778**	**0.724**	**0.750**	**0.860**
3.0	0.1	0.769	0.690	0.727	0.843

8 Simulation

This phase consists of applying the SB classifier to the unlabelled testing dataset (15 PDA auctions) to detect potential fraudsters. We represent the classification results with the confusion matrix (Table 6). The actual numbers of normal and suspicious instances are found to be 139 and 12 respect. We can see that out of 139 normal instances, 132 have been correctly classified but 7 incorrectly classified. On the other hand, out of the 12 suspicious instances, 8 are correctly predicted but 4 remained undetected. Since we are dealing with fraud data, it is far more important to minimize the number of False Negatives (suspicious bidders incorrectly classified as normal) than that of False Positives (normal bidders incorrectly classified as suspicious). Indeed, bidders belonging to the False Positive category can be further investigated and then cleared of the accusation [17]. However, instances in the False Negative category, once labelled as normal and authenticated as legitimate transactions, can never be tracked thereafter.

Table 6. Testing results – confusion matrix

		Predicted class	
		Normal	Suspicious
Actual class	Normal	132 (TN)	7 (FP)
	Suspicious	4 (FN)	8 (TP)

In this study, we focus on the detection accuracy (Recall) and misclassification rate (False Negative Rate) of fraudulent bidders. The second metric denotes the percentage of fraudulent instances incorrectly identified as normal.

- Recall = TP/(TP + FN) = 8/(8 + 4) = 0.66
- False Negative Rate = FN/(FN + TP) = 4/(8 + 4) = 0.34

As per the Recall value, we can state that our model has detected 66% of shill bidders correctly. The remaining 34% of bidders have been incorrectly labelled as normal, which is the False Negative Rate. The graphical representation of AUC is depicted in the left-hand graph of Fig. 1 whereas the ideal ROC curve (when AUC = 1) is seen in the right hand. An AUC of 80% is achieved during testing, which is very good.

It is critical for any fraud detection model to return the classification results of new data as fast as possible. In e-auctions, the response time is a critical requirement. The time report for SB training is 294 s (1488 instances) and testing is 4 (151 instances). Time is not an issue when training the SVM model since it is done offline and conducted only once. In real-life situations, we launch our classifier at each auction where the number of instances (bidders) hardly exceeds 50. Thus, we can claim that the fraud classifier has no time-efficiency issue when testing unseen bidding data.

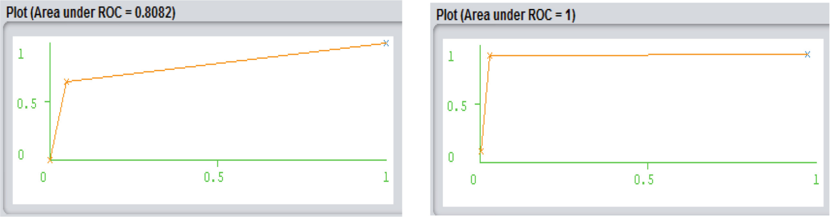

Fig. 1. Testing results – area under ROC

9 Conclusion

Detecting SB before finalizing the auction deal is necessary to avoid money loss for the winners. For this purpose, we have devised an online SVM-based SB detection system. There is a lack in SB classification studies because SB data are difficult to obtain. We have applied clustering and labelling techniques to label SB data and sampling to solve the imbalanced learning issue. Once the bidding transactions of an auction are available, we analyze them all at once to detect more accurately fraud in each auction, and take actions if the auction is infected. The SB classifier has exhibited a very good performance in both training and testing. Since time is a critical requirement of e-auctions, we can fully automate the verification of suspicious bidders by using the trust management framework defined in [1].

References

1. Abedinzadeh, S., Sadaoui, S.: A rough sets-based agent trust management framework. Int. J. Intell. Syst. Appl. **5**(4), 1–9 (2013)
2. Akbani, R., Kwek, S., Japkowicz, N.: Applying support vector machines to imbalanced datasets. In: Boulicaut, J.-F., Esposito, F., Giannotti, F., Pedreschi, D. (eds.) ECML 2004. LNCS (LNAI), vol. 3201, pp. 39–50. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-30115-8_7
3. Chawla, N.V., et al.: SMOTE: synthetic minority over-sampling technique. J. Artif. Intell. Res. **16**, 321–357 (2002)
4. Chawla, N.V.: C4.5 and imbalanced data sets: investigating the effect of sampling method, probabilistic estimate, and decision tree structure. In: International Conference on Machine Learning (2003)
5. Dong, F., Shatz, S., Xu, H.: Combating online in-auction frauds: clues, techniques and challenges. Comput. Sci. Rev. **3**(4), 245–258 (2009)
6. Dong, F., Shatz, S.M., Xu, H., Majumdar, D.: Price comparison: a reliable approach to identifying SB in online auctions? Electron. Commer. Res. Appl. **11**(2), 171–179 (2012)
7. Ford, B.J., Haiping, X., Valova, I.: A real-time self-adaptive classifier for identifying suspicious bidders in online auctions. Comput. J. **56**(5), 646–663 (2013)
8. Ganguly, S., Sadaoui, S.: Classification of imbalanced auction fraud data. In: Mouhoub, M., Langlais, P. (eds.) AI 2017. LNCS (LNAI), vol. 10233, pp. 84–89. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-57351-9_11

9. Gupta, P., Mundra, A.: Online in-auction fraud detection using online hybrid model. In: International Conference on Computing, Communication & Automation (2015)
10. He, H., Garcia, E.A.: Learning from imbalanced data. IEEE Trans. Knowl. Data Eng. **21**(9), 1263–1284 (2009)
11. Hernandez, J., Carrasco-Ochoa, J.A., Martínez-Trinidad, J.F.: An empirical study of oversampling and undersampling for instance selection methods on imbalance datasets. In: Ruiz-Shulcloper, J., Sanniti di Baja, G. (eds.) CIARP 2013. LNCS, vol. 8258, pp. 262–269. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41822-8_33
12. Köknar-Tezel, S., Latecki, L.J.: Improving SVM classification on imbalanced data sets in distance spaces. In: IEEE International Conference on Data Mining, pp. 259–269 (2009)
13. Nikitkov, A., Bay, D.: Online auction fraud: ethical perspective. J. Bus. Ethics **79**(3), 235–244 (2008)
14. Nikitkov, A., Bay, D.: SB: empirical evidence of its effectiveness and likelihood of detection in online auction systems. Int. J. Account. Inf. Syst. **16**, 42–54 (2015)
15. Ochaeta, K.: Fraud Detection for Internet Auctions. “A Data Mining Approach”, Master’s Thesis, College of Technology Management, National Tsing-Hua University, Hsinchu, Taiwan (2008)
16. Phua, C., et al.: A comprehensive survey of data mining-based fraud detection research. arXiv preprint arXiv:1009.6119 (2010)
17. Resnick, P., et al.: Reputation systems. Commun. ACM **43**(12), 45–48 (2000)
18. Sabau, A.S.: Survey of clustering based financial fraud detection research. Informatica Economica **16**(1), 110 (2012)
19. Sadaoui, S., Wang, X.: A dynamic stage-based fraud monitoring framework of multiple live auctions. Appl. Intell. (2016). https://doi.org/10.1007/s10489-016-0818-7
20. Sallehuddin, R., Ibrahim, S., Elmi, A.H.: Classification of SIM box fraud detection using support vector machine and artificial neural network. Int. J. Innov. Comput. **4**(2), 19–27 (2014)
21. Seiffert, C., et al.: An empirical study of the classification performance of learners on imbalanced and noisy software quality data. Inf. Sci. **259**, 571–595 (2014)
22. Trevathan, J., Read, W.: Detecting SB in online English auctions. In: Handbook of Research on Social and Organizational Liabilities in Information Security, p. 446 (2008)
23. Trevathan, J.: Getting into the mind of an “in-auction” fraud perpetrator. Comput. Sci. Rev. **27**, 1–15 (2018)
24. Weiss, G.M., McCarthy, K., Zabar, B.: Cost-sensitive learning vs. sampling: which is best for handling unbalanced classes with unequal error costs? In: International Conference on Data Mining, pp. 35–41 (2007)
25. Yoshida, T., Ohwada, H.: Shill bidder detection for online auctions. In: Zhang, B.-T., Orgun, M.A. (eds.) PRICAI 2010. LNCS (LNAI), vol. 6230, pp. 351–358. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-15246-7_33
26. Zhang, S., Sadaoui, S., Mouhoub, M.: An empirical analysis of imbalanced data classification. Comput. Inf. Sci. **8**(1), 151 (2015)