The Impact of False Negative Cost on the Performance of Cost Sensitive Learning Based on Bayes Minimum Risk: A Case Study in Detecting Fraudulent Transactions

Doaa Hassan
Computers and Systems Department, National Telecommunication Institute, Cairo, Egypt
E-mail: doaa@nti.sci.eg

Abstract—In this paper, we present a new investigation to the literature, where we study the impact of false negative (FN) cost on the performance of cost sensitive learning. The proposed investigation approach has been performed on cost sensitive classifiers developed using Bayes minimum risk as an example of an applied mechanism for making a classifier cost sensitive. We consider a case study in credit card fraud detection, where FN refers to the number of fraudulent transactions that are miss-detected and approved as legitimate ones, assuming the classifier predicts the fraudulent transaction. Our investigation approach relies on testing the performance of various complex cost sensitive classifiers from different categories developed using Bayes minimum risk at different costs of FN. Our results show that those classifiers behave differently at different costs of FN including the real and average amount of transaction, and a range of random constant costs that are greater or less than the average amount. However, in general the results show that the lower the costs of FN are, the better the classifier performances are. This leads to different conclusions from the one drawn in [1], which states that choosing the cost of FN to be equal to the amount of transaction leads to better performance of cost sensitive learning using Bayes minimum risk. The results of this paper are based on the real life anonymous and imbalanced UCSD transactional data set.

Index Terms—Cost sensitive learning; fraudulent transactions; Bayes minimum risk.

I. INTRODUCTION

As the use of debit and credit cards has increased rapidly in the last years, the detection of fraud transactions committed with them and hence ensuring a secure electronic transaction has become a great challenge to achieve. Recently there has been many research work done to use data mining and machine learning to address this challenge as a classification problem [2], [3], [4], [5]. The main objective of this research work is to identify the fraudulent transactions from the genuine ones using knowledge discovery from infrequent patterns derived from the gathered data in order to make a valid prediction. The classification mechanisms used in this research were evaluated using the classical evaluation measures such as accuracy, precision and recall [6].

However, the specialty of credit card fraud detection is that misclassifying a fraudulent transaction as legitimate (false negative (FN)) carries a significant different cost more than the inverse case (false positive (FP)) and hence the costs of false positive and false negative errors should be unequal and can differ from an example to another. Therefore there is a clear certain need to take the misclassification cost into account when applying the various data mining classification techniques for identifying credit card fraud in order to avoid the costliest of errors.

Recently various research methods have been developed in the literature on credit card fraud detection to differentiate between the cost of wrongly predicting a fraudulent transaction as legitimate from the cost of the inverse case [1], [7], [8], [15]. Some of these methods assume different constant costs for each type of both predictions [7]. Other methods assume the real financial cost of credit card fraud detection [1, 15], while [8] assuming a lower constant cost for predicting legitimate transactions as fraudulent ones.

To this end and due to the fact that misclassifying fraudulent transactions as legitimates ones may cause a huge waste of money, this paper investigates the impact of the cost of FN on the performance of various complex cost sensitive classifiers used for credit card fraud detection. The cost sensitive classifiers developed using Bayes minimum risk have been considered for the presented investigation in this paper. This technique was proposed in [1] as a method for making the classifier cost sensitive. The aim of the presented investigation is to determine the best cost of FN that leads to the best performance of classifier. Therefore, we evaluate the performance of different types of cost sensitive classifiers developed using Bayes Minimum Risk at different costs of FN including either the real or average amount of transaction in addition to a range of constant values that are greater or less than the average amount. This evaluation methodology considers an inequality between
the cost of FN and the cost of the FP (i.e., misclassifying legitimate transactions as fraudulent), where a lower administrative constant cost is assigned for FP. We have also considered a benefit cost for rightly detecting a fraudulent transaction. The “total cost” which is the summation of the misclassification and right classification costs of each test example of the entire test set of each classifier is used as a metric to evaluate the classifier performance. In this paper, the Bayes minimum risk classifier has been implemented and tested on different types of classifiers including support vector machine (SVM), decision trees (DT), random forest (RF), logistic regression (LR), neural network (NN) and Naïve Bayes [9]. As a result, various categories of cost sensitive classifiers have been obtained.

The structure of this paper is organized as follows: In Section II, we provide a background of cost sensitive learning and discuss the related work. In Section III, we introduce our investigation approach as well as the experimental settings. In Section IV, we present the performance evaluations. In Section V, we provide some discussions in view of the performance evaluation results. Finally we conclude the paper in Section VI with some directions for future work.

II. BACKGROUND

A. Cost Sensitive Learning Based on Bayes Minimum Risk

The accuracy of classifying a data set is commonly used in machine learning field as a metric to evaluate the performance of classifiers. However, some types of misclassifications may affect badly than others. For example, rejecting authorized access to a system may cause inconvenience while authorizing an illegitimate access may be more dangerous and cause very negative consequences. Here the role of cost sensitive learning appears, where the cost of every type of error is taken into account in order to avoid errors that lead to catastrophic situations [10].

In view of this, the goal of cost-sensitive learning is to use the cost matrix [10] to represent the cost of each type of misclassifications. In such a case, the cost matrix is considered as the dominant factor to find the border between the regions that divide optimally the example space. For example if misclassifying class i is more expensive relative to other classes then the region of class i must be expanded at the expense of other classes, even though there was no change in the class probabilities.

As for credit card fraud detection, let us consider the cost matrix shown in Table 1. The matrix is two dimensional matrix where the rows of the matrix represent the cost for the actual values of the class label (X_i) which has two possible values 1 for fraud or 0 for legitimate respectively. Similarly, the columns of the matrix represent the cost for the predicted values of the class label (y_j) which has also two possible values: 1 for fraud or 0 for legitimate respectively. The matrix entry C_{ij} is the cost of predicting the i\(->\)j class label when the i\(->\) class label is actually correct. Thus, the cost matrix has the following four entries:

- \(C_{ii}\) refers to the cost of predicting the credit card transaction as fraud and it is actually fraud.
- \(C_{ij}\) refers to the cost of predicting the credit card transaction as fraud and it is legitimate.
- \(C_{ji}\) refers to the cost of predicting the credit card transaction as legitimate and it is fraudulent.
- \(C_{jj}\) refers to the cost of predicting the credit card transaction as legitimate and it is actually legitimate.

In general, the correct prediction when \(j = i\) is cheaper than the incorrect prediction when \(j \neq i\). So in most cases, the entries \(C_{ii}\) and \(C_{jj}\) which are equivalent to the True Positive (TP) and True Negative (TN) in the confusion matrix of the classifier [11], along the main diagonal will all be zero. Using the cost matrix, the optimal prediction of an example x is the class j that minimizes a loss function L (i.e., the cost measure) defined for each j as the sum over the other alternative possibilities of the true class of x as follows:

\[
L(x, j) = \sum_{i} P(i|x)C_{ij}
\]

(1)

\[
P(p_i|x)C_{i1} + P(p_f|x)C_{11} \leq P(p_f|x)C_{10}
\]

(2)

where \(p_i|x\) and \(p_f|x\) represent the probabilities of a transaction being fraud and legitimate respectively and there is no cost for true negative (TN) due to predicting the legitimate transaction as legitimate (i.e., \(C_{ii}=0\)).

Equation (2) implements the Bayes minimum risk algorithm [12]. In this paper we develop various cost sensitive classifiers from different categories using the Bayes minimum risk algorithm. This is achieved by classifying each transaction in the testing set of each classifier as fraudulent or legitimate according to the

<table>
<thead>
<tr>
<th>Cost Matrix</th>
<th>Predicted Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual Class</td>
<td>Fraud</td>
</tr>
<tr>
<td>Fraud</td>
<td>(C_{ii})</td>
</tr>
<tr>
<td>Legitimate</td>
<td>(C_{ji})</td>
</tr>
</tbody>
</table>

Table 1. A cost matrix for credit card fraud detection
condition in (2).

B. Related Work

There have been some research attempts that investigated the cost sensitivity of classification to evaluate credit card fraud detection systems. For example, the work presented in [13] introduced a multi-classifier meta-learning approach to address the issues of skewed class distribution and nonuniform cost per error. The approach was applied to reduce the loss due to illegitimate transactions for the credit card fraud problem.

R.J. Bolton and D. J. Hand [14] reviewed the previous research that suggested a cost for Visa/MasterCard fraud and introduced a cost model to accompany the different classification outcomes in order to minimize the fraudulent loss.

Y. Shaia et al. [8] presented a cost sensitive decision tree approach for fraud detection that minimizes the sum of misclassification costs while selecting the splitting attribute at each non leaf node.

J. Wang et al. [27] developed cost-sensitive algorithms for solving the problem of an online cost-sensitive classification task. Their algorithms were designed to directly optimize the two widely known cost-sensitive measures, namely the maximization of weighted sum of sensitivity and specificity, and the minimization of weighted misclassification cost.

The work presented in this paper is inspired by the work introduced in [1], where the Bayes’ risk classifier is used in combination with the cost matrix to build RF and LR cost sensitive classifiers. The work proposed in [1] assigns a real financial cost for wrongly classifying a fraudulent transaction as legitimate one (FN) and a lower constant cost for the inverse case (FP). Our approach extends this work by assigning a negative administrative cost (i.e., benefit) for rightly detecting fraudulent transactions. Moreover, we investigate the impact of FN cost on the performance of various common cost sensitive classifiers developed using Bayes minimum risk by testing their performance at different costs of FN and determine which cost of FN leads to the best performance of the classifier.

III. Basic Approach

We study the effect of the cost of FN that it has on the performance of cost sensitive classifiers developed using Bayes minimum risk in order to detect the fraudulent transactions. Since the concept of cost sensitive learning relies on assigning a cost for misclassifying fraudulent transaction as legitimate one and the inverse case, therefore the first step in our approach is to assign values for the four entries in the cost matrix shown Table 1 as follows:

- We assign the cost of false positive (FP) (i.e., classifying a legitimate transaction as a fraudulent one) administratively as a result for analyzing the transaction and wrongly contacting the card holder. Hence we assign a value of \( C_{02} \) to \( C_{01} \).
- We assign the cost of false negative (i.e., classifying a fraudulent transaction as a legitimate one) to be equal initially to the real amount of the transaction (i.e., the amount of money stolen by this transaction) following the approach in [1]. Hence we assign the real value of transaction to \( C_{10} \).
- We assume that there is no cost for true negative (TN) (i.e., correctly classifying legitimate transactions and hence we assign a zero value to \( C_{00} \).
- We repeat the procedure in the previous steps, but with assigning the average amount of transactions to the cost of FN (\( C_{10} \) in the cost matrix in Table 1), then change it to other different random values that are either greater or less than the average amount of transactions.

Table 2 shows the new generated cost matrix after assigning values to its four entries. As shown in the table, we refer to the cost of FN for a transaction \( i \) with a variable \( F_{N,C} \), that takes different values including the real, average amount of transactions and a range of random constant costs that are greater or less than the average amount. Using this cost matrix, the cost measure is defined as follows:

\[
C = \sum_{i=1}^{n} x_i (p_i * C_{A1} + (1-p_i) * F_{N,C}) + (1-x_i) * p_i * C_{A2} \tag{3}
\]

where \( n \) is the number of samples/transactions, \( C \) is the sum of costs of all elements of the cost matrix for \( n \) transactions (i.e., the total cost), \( x_i \) is the actual class label of \( i \)th transaction and \( p_i \) is the predicted class label for the same \( i \)th transaction. In the paper experiment \( CA_1 \) is set to -1 dollar (i.e., the bank customer will be charged one dollar by the bank when detecting a fraudulent transaction) as it is considered a benefit to identify a fraudulent transaction, while \( CA_2 \) is set to +1 dollar, due to incorrectly contacting the credit card holder.

Table 2. Setting values for the entries in the cost matrix.

<table>
<thead>
<tr>
<th>Cost Matrix</th>
<th>Predicted Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual Class</td>
<td></td>
</tr>
<tr>
<td>Fraud</td>
<td>( C_{01} )</td>
</tr>
<tr>
<td>Legitimate</td>
<td>( C_{02} )</td>
</tr>
</tbody>
</table>

The second step in our approach is to develop cost sensitive classifiers from different categories based on Bayes minimum risk by re-expressing/re-implementing the condition specified by (2), according to the values of cost matrix entries shown in Table 2. Formally, this can be expressed as follows:
\[ P(p_i | x)C_{A_1} + P(p_f | x)C_{A_2} \leq P(p_f | x)FN_{C_i} \]  

(4)

Finally, the last step in our approach is to test the performance of each classifier in terms of the total cost for each value of FN_C in order to figure out which cost of FN leads to the best classifier performance.

A. Experimental Environment

We have run our approach for investigating the influence of FN cost on the performance of cost sensitive learning based on Bayes minimum risk on a windows laptop machine with 2.6 GHZ processor Intel core (TM) i5 and 4 G Memory Rams. We have used Weka [15], a free open source software data mining tool to generate different classifiers from different categories and train them on the experimental data set. The choice of Weka is ideal for our experiment since it allows us to easily solve the imbalanced data set problem [16] using Weka filters [17] to create a balanced subsample of the data set as we will see in the next two subsections. Moreover, it allows us to obtain the probabilities of a transaction being fraud or legitimate that we need for developing cost sensitive classifiers based on Bayes minimum risk as expressed by (2). Next we implement the Bayes minimum risk algorithm in python and test it on the testing sets of all classifiers generated by Weka and calculating the total cost in each case.

B. UCSD transactional data set

The basic experiment of this paper has been performed on UCSD transactional data set [18]. This data set was used before for detecting odd e-commerce transactions as presented in [19], [20]. It has 94682 examples of real e-commerce transactions, where 92,588 of them are legitimate transactions and the remaining 2094 transactions are fraudulent with a fraud ratio of 2.2%. The data set has 19 attributes/features, 8 of them are nominal while the remaining 11 features are numerical in addition to a class attribute. Since the data set is large and imbalanced (i.e., there is a class imbalance, where the number of fraudulent transaction is too small in comparison to the number of legitimate ones), our experiment is done with under-sampling [21] the data set by selecting smaller subset of transactions (sub-ample) of the data set for training and testing the generated classifiers. The sub-sample contains 4690 instances, where 2345 of them are legitimate transactions and the remaining are fraudulent with a fraud ratio of 50.0%. We have used all transactions in the sub-sample as training and test data, where we split the sub-sample into training (66.67%) and testing (33.33%). The training sub-sample has 3126 transactions where 1565 are legitimate and the remaining 1561 transactions are fraudulent with a fraud ratio of 49.94%. The testing sub-sample has 1564 instances, where 780 instances are legitimate and the remaining 784 transactions are fraudulent with a fraud ratio 50.13%. In order to make the test data set reflects the real fraud distribution of 2.2 as % in the original data set, we have resampled the test data set sub-sample again and get a new testing sub-sample with 797 transactions, where 780 of them are legitimate and 17 are fraudulent with a fraud ratio of 2.13%. The weka.filters package [22] has been used to resample the data set.

C. Experimental Procedure

The experimental procedure of our approach has the following steps:

- Generating various classifiers from different categories including DT, SVM, NN, NB, LR, and RF. More precisely the J48, SMO, MultilayerPerceptron, Naivebayes, Logistic, and RandomForest implementations respectively in Weka. We train those classifiers on the experimental training sub-sample of UCSD data set. By generating and training the classifiers using Weka, we can get the probabilities of a transaction being either fraud or legitimate.
- Developing cost sensitive classifiers from different categories based on the Bayes minimum risk algorithm specified by (4) using the cost matrix shown in Table 2 and the obtained probabilities in the previous step for each trained classifier.
- Testing all the developed cost sensitive classifiers by predicting each instance (i.e., transaction) in the UCSD testing set sub-sample for each classifier as fraud or legitimate according to the condition given in (4).
- Calculating the total cost for each cost sensitive classifier created in the previous step based on the cost measure given in (3) and for each value of FN_C in the cost matrix shown in Table 2. FN_C takes the values of either the real or the average amount of transaction in addition to a range of values that are greater or less than the average amount of transaction.
- Evaluating the performance of each classifier in terms of the total cost, for each value of FN_C.

IV. PERFORMANCE EVALUATION AND RESULTS

We have tested the impact of FN cost on the performance of cost sensitive learning using Bayes minimum risk for detecting credit card fraud by reporting about the performance of each classifier, for each value of FN in terms of the total cost as presented in (3). Table 3 shows the results of performance evaluation of each classifier when the cost of FN is equal to the real and average amount of transactions, or when it has a random constant cost greater than or less the average amount of transaction (e.g., 100, 50, 10, 7, 5, and 2 respectively). From the results shown in Table 3, we have noticed the following:

- When the cost of FN is equal to either the real or average amount of transaction, we found that SVM is the best as it achieves the most saving, while DT is the worst among all developed
complex cost sensitive classifiers. Moreover, we found that SVM also achieves the best accuracy, while DT has the worst accuracy among all complex classifiers. Fig. 1. and 2. show the misclassification cost and accuracy for each classifier in each case.

- The performance of all classifiers is improved by achieving a lower cost (i.e., more saving) when the cost of FN resulting from predicting the fraudulent transaction as legitimate one decreases as shown in Fig. 3.

Table 3. The performance of cost sensitive classifiers in terms of total cost in dollar with different costs of FN.

<table>
<thead>
<tr>
<th>Cost of FN</th>
<th>DT</th>
<th>SVM</th>
<th>NN</th>
<th>NB</th>
<th>LR</th>
<th>RF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real amount</td>
<td>673</td>
<td>165.75</td>
<td>207</td>
<td>455</td>
<td>560</td>
<td>594</td>
</tr>
<tr>
<td>AVG=24.48</td>
<td>673</td>
<td>174.43</td>
<td>205</td>
<td>464</td>
<td>588</td>
<td>629</td>
</tr>
<tr>
<td>100</td>
<td>715</td>
<td>401</td>
<td>240</td>
<td>644</td>
<td>736</td>
<td>736</td>
</tr>
<tr>
<td>50</td>
<td>673</td>
<td>251</td>
<td>220</td>
<td>558</td>
<td>682</td>
<td>691</td>
</tr>
<tr>
<td>10</td>
<td>673</td>
<td>131</td>
<td>190</td>
<td>335</td>
<td>455</td>
<td>494</td>
</tr>
<tr>
<td>7</td>
<td>350</td>
<td>122</td>
<td>176</td>
<td>296</td>
<td>396</td>
<td>443</td>
</tr>
<tr>
<td>5</td>
<td>334</td>
<td>116</td>
<td>163</td>
<td>268</td>
<td>342</td>
<td>389</td>
</tr>
<tr>
<td>2</td>
<td>158</td>
<td>107</td>
<td>144</td>
<td>187</td>
<td>222</td>
<td>253</td>
</tr>
</tbody>
</table>

Fig.3. The performance of cost sensitive classifiers when the cost of FN =100 or 50 or 10 or 7 or 5 or 2.

V. DISCUSSION

In the following, we discuss some remarks about the effect of FN cost on the performance of cost sensitive learning algorithms developed using Bayes minimum risk for identifying the credit card fraud. In view of the evaluation results that we have obtained in the previous section, we can conclude the following:

- The performance of the cost-sensitive learning using Bayes minimum risk is related to cost of FN, where the former is inversely proportional to the later.
- The learning algorithms that have been made cost sensitive based on Bayes minimum risk and which were presented in [1, 26] in order to identify credit card fraud, namely logistic regression (LR) and random forest (RF) are not the best in performance among all tested complex classifiers. SVM, NN and Naive Bayes outperform those classifiers by achieving more cost saving as shown in Fig. 1, 2. and 3.
- The performance of all classifiers when the cost of FN is equal to the real amount of transaction is much closed or similar to the performance of those classifiers when the cost of FN has a constant value that is equal to the average amount of transaction as Fig. 1 and 2 show respectively.
- Assigning the real amount of transaction to FN does not lead all the time to the best performance by achieving the lowest cost with all complex classifiers categories as illustrated in Table 3. This contradicts what is mentioned in [1] regarding the positive effect of assigning the real cost of transaction to the cost of FN on improving the performance cost sensitive classifiers developed based on Bayes minimum risk.
VI. CONCLUSIONS

In this paper, we have conducted a new study on the impact of assigning different costs for false negative (FN) in the cost matrix on the performance of various cost-sensitive classifiers. We have considered the Bayes minimum risk as a method for developing cost sensitive classifiers. Moreover, the credit card fraud detection has been considered as a case of study, where FN refers to misclassifying the fraudulent transaction as legitimate. We have evaluated the performance of those classifiers in terms of the total cost which is the summation of the misclassification and right classification costs of each test example in the entire test set. We have tried various costs for FN starting from the real amount of transactions up to small administrative constant cost values, where there is a small constant difference between the costs of FN and FP. Our results show that though assigning a high cost for FN should be considered for detecting credit card fraud, there is always a tradeoff between the cost of FN and the performance of the cost-sensitive classifier, where the lower the costs of FN are, the better the classifier performances are. Therefore, the choice of the best cost of FN that leads to the best performance of cost sensitive classifier remains a challenge.

As a future work, we are planning to apply our approach for investigating the influence of assigning different costs for FN on the performance of various cost sensitive classifiers developed using other techniques different from Bayes minimum risk such as MetaCost [23], threshold optimization [24] and those presented in [25]. Also we are looking forward to applying our investigation approach to other case studies different from credit fraud detection such as unauthorized access detection.

ACKNOWLEDGMENT

I am so grateful to Predrag Radivojac at Indiana University- Bloomington for his significant contribution to this work and for various discussions and suggestions. Also I would like to thank the reviewers of this paper for their insightful comments.

REFERENCES

The Impact of False Negative Cost on the Performance of Cost Sensitive Learning Based on Bayes Minimum Risk: A Case Study in Detecting Fraudulent Transactions


Authors’ Profiles

Doaa Hassan earned her Ph.D. in 2012 from Computer and Systems Engineering Department at Faculty of Engineering at Zagazig University - Egypt. As a part of her PhD, she also spent more than one year and half as Ph.D. candidate at Computer Science Department at Eindhoven University of Technology in the Netherlands. Currently, she is affiliated as an Assistant Professor at Computers and Systems Department at National and Telecommunication Institute in Cairo- Egypt. She has been also a visiting research associate at School of Informatics and Computing at Indiana University - Bloomington. Her research interest focuses on using machine learning and data mining techniques for automatic detection of network intrusions and applications malware, and enforcing information flow policies.