Deep Learning Techniques in Financial Fraud Detection

Kuangyi Gu
Fudan University, Mathematical and Scientific College, Shanghai, China, 18300180054@fudan.edu.cn, Corresponding author

ABSTRACT

Nowadays, the rapid development of information technology brings great convenience to people and the financial industry. However, hidden fraud risks emerge at the same time. We can find increasing financial fraud easily. A typical example is credit card fraud, and it will cause the loss of billions of dollars for financial companies and institutions every year. In the process of solving these new types of financial frauds, some traditional statistical and machine learning methods don't perform well. As a result, lots of experts devote themselves to designing some new machine learning methods, and they do have found some great new methods. This paper gives a comprehensive review of new statistics and machine learning methods in detecting financial fraud. The review summarizes and introduces the core idea of these new methods. It provides a good reference source in guiding the detection of financial fraud for both academic and practical fields with useful information on the statistic and machine learning fields.

CCS CONCEPTS

• **Information systems** → Information systems applications; Computing platforms.

KEYWORDS

Deep Learning, Machine Learning, Fraud Detection, Graph Neural Network

ACM Reference Format:
Kuangyi Gu. 2022. Deep Learning Techniques in Financial Fraud Detection. In *7th International Conference on Cyber Security and Information Engineering (ICCSIE2022), September 23–25, 2022, Brisbane, QLD, Australia.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3558819.3565093

1 INTRODUCTION

In recent years, some new information technologies have been applied in the financial field, and they have changed people's consumption behavior and model of the financial industry a lot, especially e-commerce and money transfer. People enjoy the convenience brought by new technology. However, hidden fraud risks emerge at the same time. Since e-commerce allows most individuals and companies to perform their transactions online, the adoption of an electronic payment system is more common. But with the complexity of the Internet and concealment of the network, electronic payment systems provide a breeding gourd for financial fraud, such as credit card fraud. The explosive growth of electronic transaction information makes it more difficult to detect and classify financial fraud, which will cause the loss of billions of dollars for financial companies and institutions every year. As a result, the rule-based expert must find some new methods to detect and prevent these new types of financial fraud.

Most experts focus on the statistic and machine learning field. Because of the explosion of online transaction information, it is too difficult for people to detect financial fraud manually. As the online environment develops quickly, new fraud methods appear successively. A fixed detection model won't perform well in the detection field, and its previous performance has proven it. So we need a more complex and reasonable model to deal with financial fraud. Moreover, several surveys have been conducted in the US and the UK. The studies show that financial fraud made a loss of $400 billion every year while 1.6 pounds to insurers in the UK [1].

Experts and scholars have tried lots of new statistics and machine learning methods to detect financial fraud. For example, Zhou et al. [2] proposed an intelligent and distributed Big Data approach for Internet financial fraud [2]. This algorithm is called 'Node2Vec', which can learn and represent the topological features in the financial network graphs into low-dimensional vectors. Moreover, Liu et al.proposed a new model named Pick and Choose Graph Neural Network(PC-GNN) [3]. It can solve some thorny problems which traditional GNN-based methods can't solve very well. Forough et al. focus on credit card fraud [4]. They proposed a new model that utilizes Long Short-term Memory (LSTM) and Gated Recurrent Unit(GRU) as its base classifiers and uses a novel voting mechanism based on Artificial Neural Network (ANN) on the top of that. Li et al. noticed that the number of illegitimate transactions is much less than that of normal transactions, so it's meaningful to address the problem of class imbalance, which occurs when the sample sizes of different datasets have a large gap [5]. As a result, the author proposed a hybrid method with a Dynamic Weighted Entropy measurement for improving the efficiency of the whole model learning, and the divide-and-conquer idea is used. Moreover, Błaszczyński et al. focus on auto loan fraud [6]. Comparing the concept of auto loan fraud with credit card fraud, the author thought that they have some similarities. So this paper tried a new technique that has not been employed in financial fraud detection yet. It is named Dominance-based Rough Set Balanced Rule Ensemble(DRSA-BRE), and it does have some advantages compared with traditional methods. Carcillo et al.present a new hybrid technique that combines supervised learning and unsupervised learning together [7]. They found supervised learning performs not very well in the detection of financial fraud. So they tried the combination of supervised learning and unsupervised learning. The fact proves that the combination does improve the accuracy of prediction. The main objective of this paper is to review the work of some experts who employ

ICCSIE2022, September 23–25, 2022, Brisbane, QLD, Australia
© 2022 Association for Computing Machinery.
ACM ISBN 978-1-4503-9741-4/22/09…$15.00
https://doi.org/10.1145/3558819.3565093

new statistics and machine learning techniques in financial fraud detection. So the contributions of this paper are as follows:

This paper focuses on the recent paper which introduces some new statistics and machine learning techniques and gives a summary of this research. It includes some new techniques which were not mentioned in the previous review.

This paper introduces the concept of some common types of financial fraud. And to each specific financial, this paper will give one or more new presented statistics and machine learning techniques to solve the problem.

This paper summarizes the advantages, disadvantages, and realistic applications of the new statistic and machine learning techniques. If someone wants to make use of the method mentioned above, this paper is a good reference.

This paper begins with an introduction that includes recent surveys, the contribution of this paper, and the organization of this paper. Section2 will introduce the common types of financial fraud. The definition and the description of different types of financial fraud are both introduced in this section. Section3 introduces the new neural network techniques which are used in statistic and machine learning areas. Section4 is the literature review of some newly emerging techniques. And section5 is the conclusion.

2 TYPES OF FINANCIAL FRAUD

Due to the development of the financial industry, there are many types of financial fraud, including credit card fraud, mortgage fraud, embezzlement, insurance fraud, health care fraud, and so on. Given that some readers don't understand the meaning of these words, this paper will introduce the definition of financial fraud nouns in the next section, and these types of financial fraud are the common types of financial fraud.

2.1 Credit Card Fraud

A credit card fraud occurs when a customer is using a payment card, such as a credit card or a debit card (mainly the former one). It appears with the development of e-commerce. People are allowed to perform transactions without physical money. Fraudsters utilize this character of credit cards to commit crimes.

Credit card fraud can be split into two categories: Online and Offline fraud. On Online fraud, fraudsters perform the transaction in an online environment through the Internet. In contrast, in offline fraud, fraudsters always use a fake or stolen credit card to perform the online transaction. Credit card fraud causes billions of dollars of loss to financial companies and institutions every year.

2.2 Mortgage

Mortgage fraud occurs when a person wants to take out a loan from a bank. He may modify the information during the process of loan application in a mortgage. Moreover, a person is using his estate as a guarantee to get the loan, but he falsely estimates the original value of his property to gain more loans from the financial institution. It is another type of mortgage fraud.

2.3 Embezzlement

Embezzlement means the appropriation of assets. The assets belong to other people, or it is used for some other purposes initially. But you convert the assets to your account in an illegal way. This is embezzlement. A common example is that a husband or a wife embezzles funds from a bank account jointly held with the spouse.

2.4 Health Care Fraud

Health care fraud refers to a person who wants to gain illegal benefits from government health care programs. These people usually circumvent the law and utilize the flaw of the initial law and regulation to fulfill their purpose.

2.5 Insurance Fraud

Insurance fraud is any act committed to defraud an insurance process. It occurs when a claimant makes some accidents deliberately to gain some benefit from the insurers. But if the insurer knows the deliberate behavior of the claimant, he will deny the requirement of the claimant.

3 NEURAL NETWORKS FOR FRAUD DETECTION

This part is meant to introduce two new statistic and machine learning techniques that can be used in the financial fraud detection area.

3.1 Graph Attention Network

Graph Attention Network(GAT) is a variant of Graph Neural Network(GNN). It uses Multi-head Attention Mechanism to aggregate the representation of neighbor nodes and iteratively update the representation of each node. After that, GAT can realize the self-adaption distribution of the weight of different neighbor nodes.

Given a dependency graph that has N nodes. We suppose that the corresponding eigenvector of node I in ith GAT is $\boldsymbol{h}_i^{l+1}$, $\boldsymbol{h}_i^{l+1} \in R^{Kd^{l+1}}$. K is the number of head of the graph attention, and d^{l+1} represents the dimension of eigenvector output by GAT when K equals 1. The updating formulas are:

$$\boldsymbol{h}_i^{l+1} ||_{k=1}^{K} \sigma\left(\sum_{j\in N(i)} a_{ij}^{lk} \boldsymbol{W}^{lk} \boldsymbol{h}_j^l\right) \tag{1}$$

$$a_{ij}^{lk} = \frac{exp\left(LeakyReLU\left(\boldsymbol{a}_{lk}^T\left[\boldsymbol{W}^{lk}\boldsymbol{h}_i^l \parallel \boldsymbol{W}^{lk}\boldsymbol{h}_j^l\right]\right)\right)}{\sum_{u\in N(i)} exp\left(LeakyReLU\left(\boldsymbol{a}_{lk}^T\left[\boldsymbol{W}^{lk}\boldsymbol{h}_i^l \parallel \boldsymbol{W}^{lk}\boldsymbol{h}_u^l\right]\right)\right)} \tag{2}$$

In the formulas, || represents the joint operation, *N(i)* represents the neighbor nodes of the node *i*, a_{ij}^{lk} represents the weight coefficient calculated by the kth attention head in lth GAT, $\boldsymbol{W}^{lk} \in R^{d^{l+1}\times d^l}$ and $\boldsymbol{a}_{lk}^T \in R^{2d^{l+1}}$ are weight coefficients, $\boldsymbol{h}_j^l \in R^{d^l}$ represents the hidden state vector of neighbor nodes, and LeakyReLU represents the activation function.

3.2 Graph Convolutional Network

Nowadays, the GCN form presented by Kipf et al. is accepted generally [8]. It is presented as a local first-order approximation of spectral graph convolution, and it's a very easy and efficient graph neural network. In fact, GCN is a multi-layer neural network, as is showed in Figure 1, which can be used on the graph directly.

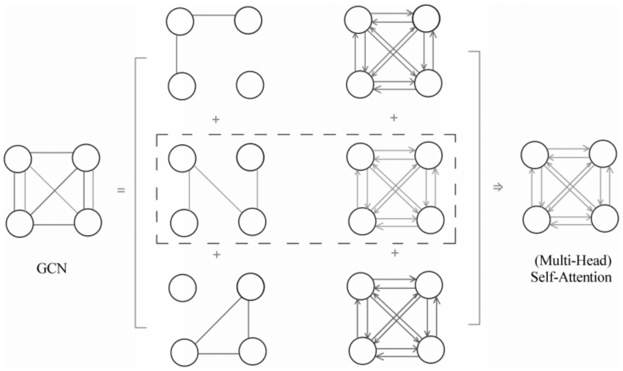

Figure 1: The structure of the GCN

It is based on the neighbor nodes of each node to generate the embedded vector representation of this node, and this embedded vector representation can code the local graph structure and the characteristic information of neighbor nodes in the GCN.

Considering graph G which includes n nodes. Each node has a side connected to itself. The adjacent matrix of graph G is $\boldsymbol{A}$. Due to the self-connected side, the diagonal elements in $\boldsymbol{A}$ equal to 1. The computational formula of degree matrix $\boldsymbol{D}$ is as formula(3):

$$\boldsymbol{D}_{ii} = \sum\nolimits_j \boldsymbol{A}_{ij} \tag{3}$$

Setting $\boldsymbol{X} \in R^{n\times m}$ is eigenmatrix, and m is the dimension of eigenvector.

If using a one-layer convolutional operation, GCN could only acquire the information of its direct neighbor nodes. However, if we use a multi-layer graph convolutional network, we can acquire the information in a larger area. For one-layer GCN, new eigenmatrix $\boldsymbol{H}^{(l+1)} \in R^{n\times k}$ can be obtained by formula(4):

$$\boldsymbol{H}^{(l+1)} = \tilde{\boldsymbol{A}}\boldsymbol{H}^{(l)}\boldsymbol{W}^{(l)} \tag{4}$$

Usually, we need activation function σ as well: $\boldsymbol{H}^{(l+1)} := \sigma(\boldsymbol{H}^{(l+1)})$. In this formula, $\boldsymbol{W}^{(l)} \in R^{(m\times k)}$ is the matrix which transforms the eigenmatrix $\boldsymbol{H}^{(l)}$ linearly. l represents the number of layers. The input eigenmatrix of the network is the initial eigenmatrix which is as formula(5):

$$\boldsymbol{H}^{(0)} = \boldsymbol{X} \tag{5}$$

And adjacent matrix $\tilde{\boldsymbol{A}}$ is the symmetric convention normalization of initial adjacent matrix $\boldsymbol{A}$. It is as follows:

$$\tilde{\boldsymbol{A}} = \boldsymbol{D}^{-\frac{1}{2}}\boldsymbol{A}\boldsymbol{D}^{-\frac{1}{2}} \tag{6}$$

We can find that degree matrix $\boldsymbol{D}$ can be calculated out by initial adjacent matrix $\boldsymbol{A}$, and initial adjacent matrix $\boldsymbol{A}$ in GCN has always been given before the training. As a result, before each section of GCN, such as training, debugging, and testing, we can calculate the symmetric convention normalization matrix $\tilde{\boldsymbol{A}}$ and save it to save time and resources, instead of recalculating to obtain the same value.

Moreover, to allow GCN to solve some more complicated graph structures which include grammar, Marcheggiani et al.introduce a new mechanism to solve the direction of connecting-side and the categories of labels for GCN [9]. Due to their contribution, the eigenvector of a new node v can be represented as follows:

$$h_v^{(l+1)} = \sigma\left(\sum\nolimits_{u\in N(v)} \boldsymbol{W}_{L(u,v)}^{(l)} h_u^{(l)} + b_{L(u,v)}^{(l)}\right) \tag{7}$$

In formula(7), the *N(v)* represents the set of the neighbor nodes of node v. $\boldsymbol{W}^{(l)}$and $b^{(l)}$represent the parameter matrix or the parameter that can be learned. *L(u,v)* is the function that returns the direction of the side connecting node u and v. Compared with $\boldsymbol{W}^{(l)}$ in formula(4), the connecting sides with different directions and categories can be represented by different learning parameters. Similarly, if we aggregate the representation of all the neighbor nodes after transformation, we can get the new eigenvector of this node.

4 LITERATURE REVIEW

There are lots of literature focusing on utilizing different types of stochastic and machine learning methods to perform financial fraud detection. There exist some papers that summarize the state-of-the-art framework in this area, such as GCN, GNN, and so on. In this paper, I mean to deliver some improvement of the state-of-the-art framework. Some of the new methods may be based on the existing framework and the others may be brand new. But above all, these new methods all perform better in datasets provided by huge online transaction companies like Amazon and Taobao.

4.1 Sub Graph Neural Network

When it comes to detecting financial fraud on built user-item graphs, lots of existing methods still use manually designed methods, such as label propagation and dense block assumption. Although these two methods have proved effective in practice, they have some drawbacks. Most significantly, the success of these two methods is based on their instinctive inductive property, which makes sure that they can detect the new users and items directly. Moreover, they are both heuristics and rely on human design. These drawbacks limit the performance of manually designed methods.

Besides manually designed methods, another broadly accepted method is learning-based techniques, such as graph representation learning and graph neural networks(GNNs). These methods have become mature in recent years and they have been utilized in financial fraud detection by some experts. They do perform better than heuristic methods in some areas. However, they still have some drawbacks. Learning-based techniques rely on content features that can't always be available or need to train node ID embedding, while in practice there are usually many behaviors on new users and items with untrained ID embeddings.

Song et. al. propose a subgraph-based method that can be utilized when only structural information is available [10]. For each candidate user-item edge, we extract the subgraph around it. Then we mark the nodes with new label IDs on the subgraph. At last, we design a powerful relational graph isomorphism network(R-GIN) which has a strong expression ability. Due to the advantage of the design of SubGNN, SubGNN can learn complicated knowledge reasoning rules on the relabelled heterogeneous subgraphs and detect fraud detection precisely.

4.2 Pick and Choose Graph Neural Network

In reality, GNN-based algorithms seldom succeed because of the class imbalance problem. Class imbalance means that the sample sizes of different have a large difference: because compared with normal legitimate transactions, the number of fraudulent transactions is much fewer.

For previous work, there are there main challenges for GNN methods. The first challenge is the redundant link information. In reality, the fraudsters will leave no stone unturned to intimate the legitimate users. As a result, there is much more legitimate link information than illegal transaction information. The second challenge is the lack of necessary link information between fraudsters. Fraudsters always avoid meeting another fraudster. When we find an existing fraudster, it is very difficult for us to find another fraudster by the link between the found fraudster and other nodes. The third challenge is the message aggregation of GNNs.

To amend the class imbalance problem, Liu et. al.propose a Pick and Choose Graph Neural Network(PC-GNN) for imbalanced supervised learning on graphs [3].

For the algorithm side, we design a label-balanced sampler to pick nodes and edges to train. For the application side, we propose a neighborhood sampler to choose neighbors with a learnable parameterized distance function. For the fraud target node, the redundant links could be filtered by choosing neighbors that are gar from the neighbor set. Since the keyword of the solving process is ‘pick’ and ‘choose’, we call this method Pick and Choose Graph Neural Network(PC-GNN).

4.3 Node2Vec

Zhou et. al.proposed Node2Vec in their paper. Node2Vec is a distributed data approach, which is designed to learn and represent the topological features in the financial network graph into low-dimensional dense vectors[2].

4.4 Dynamic Weighted Entropy

In previous financial fraud detection, lots of experts focus on the problem of class imbalance. However, they don’t mention the problem of overlapping. Overlap refers to the problem that in the same data space region, there exist different kinds of samples. It considerably increases the difficulty of constructing a classifier to distinguish the samples in the overlapping areas. As fraudsters always try their best to intimate the behavior of legitimate transactions, it is obvious that fraudulent transactions and legitimate transactions could be mixed in some data areas, and this is called overlapping.

Firstly, Li et. al. proposed a Divide-and-Conquer method to solve the class imbalance problem [5]. This method has two steps: Divide and Conquer. In Divide-step, the detection uses some existing efficient models, such as One-Class SVM(OCSVM), isolation Forest, and Auto-Encoder(AE), to learn the principle profile of the fraud transactions (because it is the minority sample). With the help of the profile, we can find the overlapping subset and the non-overlapping subset. And then in the Conquer-step, we deal with the overlapping subset and the non-overlapping subset severally. Since few of the fraud transaction samples are categorized into the non-overlapping subset, they can be viewed as the majority ones for simplicity. For overlapping subsets, we can make use of some powerful supervised classifiers, such as Random Forest(RF) and Artificial Neural Network(ANN). Dynamic Weighted Entropy(DWE) considers both the number of excluded anomalies of minority samples and the Imbalance Ratio of the overlapping subset. With the help of DWE, it is more efficient to choose the optimal hyperparameters of the financial fraud detection model, and it can also reduce the strategic decision-making entropy.

4.5 Deep Sequential Model

When we want to build a supervised machine learning model to detect financial fraud, we always face some challenges, including skewness of data, concept drift, the short-time response of the system, and so on. Lots of work have been done to solve these problems, and they do be proved effective in practice, such as Artificial Neural Network(ANN), support vector machines, decision tree, and so on. During these methods, we find methods that use contextual and sequential models, such as RNNs, can perform better than other models by reviewing recent research in the financial fraud detection area. However, the most significant problem of simple RNNs is their vanish gradient. Due to the problem, it is harder for the model to update the weight parameters in the learning process, and it may slow down or even stop the learning process. Although LSTM is proposed to solve this problem, it still has its drawback: computational complexity.

Based on the previous reasons, Forough et. al.wants to take the advantage of the two approaches and combine them to get better performance [4]. In their paper, they proposed a novel ensemble model that takes the positive sides of LSTM and GRU networks as its base classifiers and utilizes a novel voting mode based on ANN on top of that. Moreover, they proposed to learn from the output of its base classifiers, and they make final inference based on the learned patterns of base classifiers’ prediction through a Feed-Forward Neural Network(FFNN). It is a brand new attempt, and it does perform better than the state-of-the-art models.

4.6 Combination of Supervised Learning and Unsupervised Learning

In the previous content, we have mentioned some credit card detection machine learning models, some of them are supervised learning models, and some of them are unsupervised learning models. However, solo supervised learning models or solo unsupervised learning models have their drawbacks.

For supervised learning techniques, it depends on the set of past transactions for which the label of the transaction is known. In another word, they are based on the assumption that fraudulent patterns can be learned from the analysis of past transactions. However, labels are not always available immediately.

For unsupervised learning techniques, they rely on the assumption that outliers of the transaction distribution are frauds. However, it is worthy of nothing when their use also extends to clustering and compression algorithms.

Carcillo et.al. think that supervised learning approaches and unsupervised learning approaches are complementary: supervised techniques learn from past fraudulent transactions, while unsupervised techniques aim to detect the new kinds of fraudulent transactions [7]. Their paper concerns the integration of unsupervised techniques with supervised detection classifiers. They present a number of criteria to compute outlier scores at the different granularity and we assess their added value in terms of accuracy once integrated as features in a supervised learning strategy. Their adoption of this principle is new in the credit card fraud detection area.

4.7 Auto Loan Problem

When it comes to financial fraud, the first impression of most people is credit card fraud, and lots of experts devote themselves to detecting credit card fraud. However, with the development of information technology, some newly emerging financial fraud should also be paid attention to. One of them is auto loan fraud, and it didn't obtain too much attention or be explored. Compared with a credit card, an auto loan is a type of secured credit product. Although this kind is more difficult to commit, fraudsters will gain much more illegal profit if they succeed.

Considering such situation, Błaszczyński et al.propose the Dominance-based Rough Set Balance Rule Ensemble (DRSA-BRE) predict the auto loan fraud [6]. The characterization of DRAS-BRE begins with a short reminder of the DRSA. It is followed by the description of a method designed for analysis of data with imbalanced decision classes and used to build up an ensemble classifier called BRE. So it is called DRSA-BRE.

5 CONCLUSION

Nowadays, Although financial fraud detection techniques becomes mature, financial fraud still causes large quantities of financial loss. Among different types of financial frauds, such as credit card fraud, mortgage, auto loan fraud, and so on, some of them have been having been studied intensively, some of them are still not been explored. But it is obvious that we will do better and better with the development of stochastic and machine learning techniques. This paper summarizes some new exploration in the financial fraud detection area, and I hope this paper will be meaningful for some others who want to learn some newly emerging techniques in this area.

REFERENCES

[1] S., M., *et al.* Fraud Analysis Approaches in the Age of Big Data - A Review of State of the Art. in 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS*W). 2017.

[2] H., Z., *et al.*, Internet Financial Fraud Detection Based on a Distributed Big Data Approach With Node2vec. IEEE Access, 2021. 9: p. 43378-43386.

[3] Y, Liu., *et al.*, Pick and Choose: A GNN-based Imbalanced Learning Approach for Fraud Detection. 2021.

[4] Forough, J. and S. Momtazi, Ensemble of deep sequential models for credit card fraud detection. Applied Soft Computing, 2021. 99: p. 106883.

[5] Li, Z., *et al.*, A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection. Expert Systems with Applications, 2021. 175: p. 114750.

[6] Błaszczyński, J., *et al.*, Auto loan fraud detection using dominance-based rough set approach versus machine learning methods. Expert Systems with Applications, 2021. 163: p. 113740.

[7] Carcillo, F., *et al.*, Combining unsupervised and supervised learning in credit card fraud detection. Information Sciences, 2021. 557: p. 317-331.

[8] Thomas N. Kipf, M.W., SEMI-SUPERVISED CLASSIFICATION WITH GRAPH CONVOLUTIONAL NETWORKS, in ICLR. 2017.

[9] Marcheggiani, D. and I. Titov, Encoding Sentences with Graph Convolutional Networks for Semantic Role Labeling. 2017.

[10] Song, J., *et al.*, A subgraph-based knowledge reasoning method for collective fraud detection in E-commerce. Neurocomputing, 2021. 461: p. 587-597.