Research on Fincial Fraud Detection based on Deep Graph Neural Network

Ningxin Li *, Lidong Xu, Xuyang Zhang, Jianke Zou

Posted Date: 8 November 2024

doi: 10.20944/preprints202411.0609.v1

Keywords: Fincial fraud detection; Graph neural network; Graph attention network; Graph convolution

 doi:10.20944/preprints202411.0609.v1

Article

Research on Fincial Fraud Detection Based on Deep Graph Neural Network

Ningxin Li [1,*], Lidong Xu [2], Xuyang Zhang [3] and Jianke Zou [4]

[1] Fu Foundation School of Engineering and Applied Science, Columbia University, New York, USA
[2] Graziadio Business School, Pepperdine University, Malibu, CA; lidong.xu@alumnimail.pepperdine.edu
[3] Rackham School, University of Michigan-Ann Arbor, Ann Arbor, MI, USA; xuyangzh@umich.edu
[4] HSBC Business School, Department of Management, Peking University, Peking China; Zoujianke@pku.org.cn
* Correspondence: nl2735@columbia.edu

Abstract: Financial fraud refers to the act of obtaining financial benefits through dishonest means. Such acts not only disrupt the order of the financial market, but also harm social and economic development, and breed other illegal and criminal acts. With the proliferation of the internet and online payment methods, many fraudulent activities and money laundering have shifted from offline to online, posing a significant challenge for regulators. In this work, we proposed a novel detection model by utilizing the graph neural network. Specifically, the general model structure includes the combination of Graph Convolutional Network (GCN) and Graph Attention Network (GAT), which can effectively capture the complex relationships and features in the financial transaction network. By building a multilayer graph neural network, the model can perform deep learning on the implicit patterns between nodes, thereby improving the accuracy of fraud detection. Experimental analysis results show that the performance of the proposed method on multiple public datasets is better than that of traditional methods, showing its potential in practical application.

Keywords: fincial fraud detection; graph neural network; graph attention network; graph convolution

I. Introduction

Financial fraud is a far-reaching problem that affects not only the financial industry, the government and corporate sectors, but also the general consumer. Effective handling and detection of financial fraud requires the cooperation and efforts of banks and regulators. Fraud can have a huge negative impact on business and the functioning of society, with credit card fraud alone costing billions of dollars in lost revenue each year [1]. With the rapid development of the global economy and information technology, the scale of e-commerce and online transactions continues to expand, and the amount and scale of financial fraud are also increasing.

The fraud detection problem can be thought of as a classification problem. Traditional fraud detection methods can be divided into two categories: rule-based approaches and machine learning-based approaches. Although rule-based methods have been used in the financial industry for a long time, they also have some drawbacks [2]. Specifically, rule design is highly dependent on human prior knowledge, making it difficult to cope with complex patterns that are constantly changing. In addition, rule-based fraud detection strategies require a lot of manual labor on the part of financial domain experts, while non-domain experts require lengthy training to identify whether a transaction is fraudulent or not [3].

Financial fraud is a global problem that has caused huge financial losses and a crisis of confidence for financial institutions, businesses and consumers. With the rapid development of financial markets and the advancement of technology, fraud is becoming increasingly sophisticated

 doi:10.20944/preprints202411.0609.v1

and difficult to detect [4]. Financial fraud not only disrupts the normal order of the financial market, but also has a serious impact on social and economic development.

Traditional financial fraud detection methods rely heavily on rule-based systems that use expert knowledge to develop detection rules. However, these methods have significant limitations: rule design is highly dependent on human prior knowledge, difficult to adapt to complex and changing patterns, and requires extensive human intervention and lengthy training [5]. In addition, these methods are not as effective at detecting new and unknown frauds.

To overcome these limitations, machine learning-based methods are introduced into financial fraud detection. Most of these methods extract the statistical characteristics of users from different aspects and use these features for predictive classification [6]. However, these methods rarely take into account the interaction between users. Machine learning methods greatly improve the efficiency and accuracy of detection by analyzing historical data to automatically learn and identify potential fraud patterns. However, most machine learning methods mainly focus on the statistical characteristics of individual users and ignore the interaction between users, which limits their detection ability to a certain extent [7].

The complexity and volatility of financial markets make graphs built on financial data often heterogeneous or time-changing, which poses challenges to modeling techniques. Financial data is complex and diverse, and is usually presented in the form of graph data, but traditional financial fraud detection methods cannot effectively process this kind of graph data [8]. The advent of graph neural networks (GNNs) solves this problem well. Graph neural networks are a deep learning method that operates on graph domains and are often designed for tasks such as node classification, edge prediction, and graph classification. Due to its ability to deal with complex graph structures and good performance, graph neural networks have been widely studied and applied in financial tasks such as anti-money laundering and credit card fraud detection.

II. Related Work

Over the past few decades, the operating model based on embedded rules has become very popular in the financial community. Because these rules are simple and easy to code, they are often developed by consultants and domain experts who apply their own work experience to automated decision-making processes. Roldán-García et al. [9] proposed a rule-based expert system whose main purpose is to check and manage anti-fraud rule datasets to avoid semantic conflicts that lead to erroneous execution of the underlying expert system. An expert system is defined as a computing system that is capable of representation and reasoning within a specific domain of knowledge in order to solve problems and provide recommendations.

In the field of fraud detection, one of the traditional machine learning methods is Support Vector Machine (SVM) [10], which has been widely used in the field of fraud detection and anti-money laundering. Although SVMs can achieve good detection results, they take a long time to train. To address data imbalances and long training times, SVMs can be optimized using hyperparameter tuning and random sampling, a combination of which can compensate for the shortcomings of a single approach. Bayesian classifiers [11] are also one of the machine learning methods commonly used for fraud detection. In fraud detection, logical operators and if-else conditions can be used to analyze the relationships between attributes in a dataset, while Bayesian classifiers can effectively identify and find money laundering activities.

Le et al. [12] proposed a method that combines clustering with multilayer perceptron (MP) to detect suspected money laundering cases. The technique uses a simple center-based clustering technique that uses the frequency and number of transactions as input to the multilayer perceptron training process. The principle of the unsupervised detection algorithm is to predict outliers by searching for outliers. However, these algorithms are often criticized for their high false-positive and false-negative rates in real-world deployments. To solve this problem, Shubhomoy et al. [13] proposed an active anomaly discovery method combined with expert feedback, by adjusting the anomaly detector to make the outliers it finds more in line with the experts' semantic understanding of the anomaly.

 doi:10.20944/preprints202411.0609.v1

In recent years, cryptocurrencies have become a haven for money laundering activities, however, existing unsupervised anomaly detection methods are insufficient in detecting real Bitcoin transactions. To solve this problem, Joana et al. [14] proposed an active learning solution based on a real Bitcoin transaction dataset that can match the performance of a supervised baseline algorithm with only 5% labels.

III. Methodologies

III.This paper proposes a financial fraud detection method based on Deep Graph Neural Network (DGNN). The specific model approach includes the following parts: data preprocessing, graph construction, graph neural network modeling, and fraud detection.

A. Notions

Initially, we summarize the primary used parameters and its functions in following Table 1.

Table 1. Primary Notions.

Symbols	Functions
$G = (V, E)$	Preprocessed graph data
$\tilde{A}$	Adjacency matrix plus the self-loop
$\widetilde{D}$	Degree matrix
$H^{(l)}$	Node feature matrix
$W^{(l)}$	Weight matrix
σ	Activation function
$h_j^{(l)}$	Eigenvector
$a^{(l)}$	Attention weight vector
$[\cdot \,\|\|\, \cdot]$	Splicing operation of the vector
y	Prediction result

B. Graph embedding

Firstly, the features are extracted from the financial transaction records and the data structures of nodes and edges are constructed. Nodes represent transaction entities (e.g., users, accounts, transactions), and edges represent relationships between entities (e.g., transaction behavior, money flow). Each node and edge is accompanied by an eigenvector that represents its properties and relationship information.

The preprocessed data is constructed into a graph $G = (V, E)$, where V represents the node set and E represents the edge set. Each node $v_i \in V$ corresponds to an eigenvector x_i, and each edge $e_{ij} \in E$ corresponds to an eigenvector e_{ij}.

C. Graph convolution and attention networks

The basic idea of a graph convolutional neural network is to aggregate information from neighbor nodes by performing convolution operations through adjacency matrices. Specifically, the hierarchical update of the graph convolutional neural network is shown in Equation 1:

$$H^{(l+1)} = \sigma\left(\widetilde{D}^{-\frac{1}{2}}\tilde{A}\widetilde{D}^{-\frac{1}{2}}H^{(l)}W^{(l)}\right) \tag{1}$$

where $\tilde{A} = A + I$ denotes the adjacency matrix plus the self-loop, $\widetilde{D}$ is the degree matrix of $\tilde{A}$, $H^{(l)}$ is the node feature matrix of the l layer, $W^{(l)}$ is the weight matrix of the l layer, and σ is the activation function.

 doi:10.20944/preprints202411.0609.v1

Additionally, the graph attention network introduces an attention mechanism that aggregates information by assigning different weights to different neighbor nodes. The updated calculation is expressed as following Equation 2.

$$h_i^{(l+1)} = \sigma\left(\sum_{j\in N(i)} \alpha_{ij}^{(l)} W^{(l)} h_j^{(l)}\right), \tag{2}$$

Where $W^{(l)}$ represents the weight matrix for layer l. The eigenvector is expressed as $h_j^{(l)}$ node j at the l-layer. The $\alpha_{ij}^{(l)}$ is the attention coefficient, which is calculated by the following Equation 3.

$$\alpha_{ij}^{(l)} = \frac{\exp\left(LeakyReLU(a^{(l)T}\left[W^{(l)}h_i^{(l)}||W^{(l)}h_j^{(l)}\right])\right)}{\sum_{k\in N(i)}\exp\left(LeakyReLU\left(a^{(l)T}\left[W^{(l)}h_i^{(l)}||W^{(l)}h_k^{(l)}\right]\right)\right)}, \tag{3}$$

Where $a^{(l)}$ represents the attention weight vector of layer l. $a^{(l)T}$ transpose of the attention weight vector at the level l. The eigenvector of the $W^{(l)}h_i^{(l)}$ node i after being transformed by the weight matrix at level l. The eigenvector of the $W^{(l)}h_j^{(l)}$ node j after being transformed by the weight matrix at the l layer. Operation function $[\cdot||\cdot]$ represents the splicing operation of the vector. $LeakyReLU$ activation function, Leaky ReLU is a variant of ReLU that is used to calculate attention weights. $\sum_{k\in N(i)}(\cdot)$ normalize all neighbor k of node i.

In above method, the graph attention network can effectively aggregate the neighbor information of nodes and assign different weights according to the similarity between nodes, so as to better capture the complex graph structure information.

Finally, we input the output eigenvectors of the graph neural network into a fully connected layer and classify them through the Softmax function to detect fraud, which is expressed as following Equation 4.

$$y = Softmax(W_o\, h_i + b_o), \tag{2}$$

Where W_o and b_o are the weights and biases of the output layer, and y is the prediction result.

IV. Experiments

A. Experimental Setups

In this experiment, open-source datasets from Yelp and Amazon were used to verify the effectiveness of the proposed ER-GNN model in fraud detection. The Yelp dataset focuses on spam comment detection and contains three main relationships: reviews posted by the same user (R-U-R), reviews under the same product with the same star rating (R-T-R), and reviews published by the same product in the same month (R-S-R). Amazon datasets also have a similar ternary relationship structure that helps identify potential fraud in reviews. These datasets are represented in the form of graphs, with nodes representing comments and edges representing relationships between comments.

Due to the large number of dataset nodes, the mini-batch training method was used to train ER-GNN and other baseline algorithms. AT-GCN uses the Adam optimizer and the learning rate is set to 0.01. In ER-GNN, the number of training rounds is 50, the number of layers is 1, the regularization parameter is 2, and the action step size for reinforcement learning is 0.02. In the Yelp dataset, the model has a batch size of 1024 and a learning rate of 0.01, and in the Amazon dataset, the batch size is 256 and a learning rate of 0.005. These settings ensure training efficiency and model performance when working with large-scale data.

B. Experimental Analysis

In financial fraud detection, Accuracy is an important evaluation metric, which measures the model's ability to correctly classify all samples, including fraud and non-fraud samples. Accuracy is

 doi:10.20944/preprints202411.0609.v1

defined as the number of samples correctly classified as a proportion of the total sample size. Following Figure 1 demonstrates the detection accuracy with existing methods.

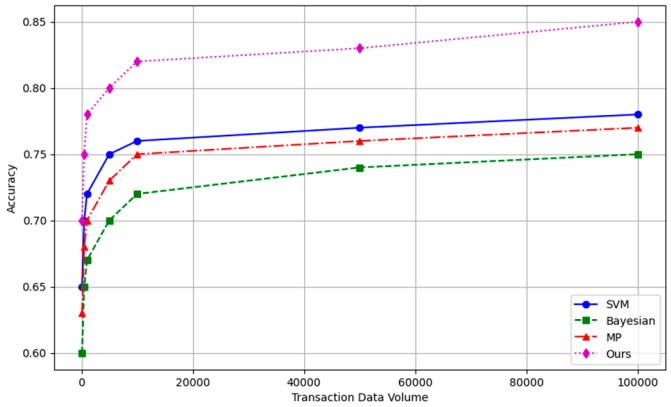

Figure 1. Accuracy Comparison of Different Methods.

In financial fraud detection, the impact of different parameter settings on model performance is crucial. In order to verify the robustness of our proposed method, we conducted parameter sensitivity experiments on the dataset, focusing on the influence of different loss function weights on the performance of the model. To verify the robustness of our method, we conducted parameter sensitivity experiments on the Elliptic dataset to investigate the impact of different loss function weights on model performance. In the experiment, the weight of the normal node gradually increases from 0.1 to 0.9, and the weight of the fraudulent node decreases accordingly.

Additionally, following Figure 2 shows the impact of different loss function weights on the performance of each method model on the dataset. The abscissa is the weight assigned to the normal node, and the ordinate is the accuracy of the model. Methods of comparison include SVM, Bayesian, MP, and our method (purple dotted line). As you can see, our method achieves the highest accuracy when the weight of the normal node is 0.35 (corresponding to the weight of the rogue node is 0.65). Through this parameter sensitivity experiment, the robustness of each model under different parameters can be verified, and the optimal parameter configuration can be found to improve the model performance.

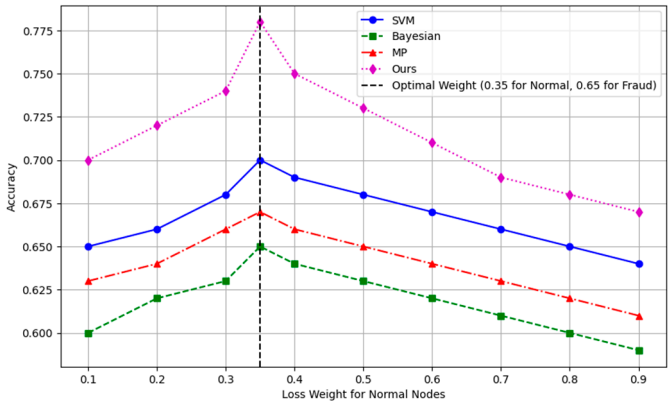

Figure 2. Model Performance with Different Loss Weights.

Recall is the proportion of actual fraud that the model successfully detects. It reflects the model's ability to catch fraud. High recall rates mean that the model is able to detect the majority of fraud, reducing the risk of undetected fraud, reducing potential financial losses, and enhancing trust between users and institutions. Following Figure 3 compares the average recall comparison results among different model.

 doi:10.20944/preprints202411.0609.v1

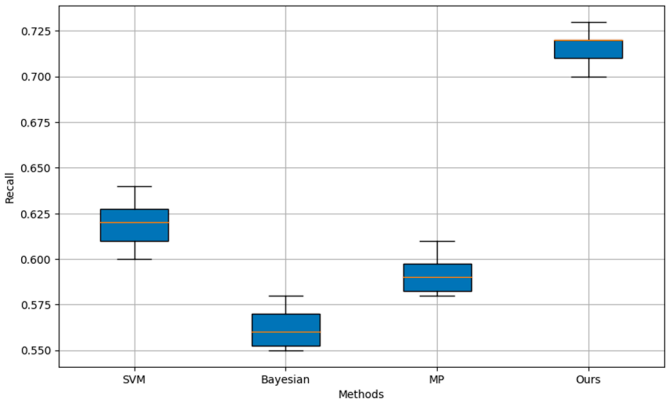

Figure 3. Recall Comparison of Different Methods.

The above Figure 3 shows an experimental comparison of different methods on recall. The abscissa is for different methods, including SVM, Bayesian, MP, and ours (Ours), and the ordinate is the recall. The boxplot clearly shows the distribution of recall for each method, and it can be seen that our method (Ours) is significantly better than the other methods in terms of recall, showing a higher median and a smaller range of fluctuations.

V. Conclusions

In conclusion, a financial fraud detection method based on Deep Graph Neural Network (D-GNN) is proposed, and its effectiveness is verified by experiments. Through experimental comparisons on multiple open-source datasets such as Yelp and Amazon datasets, it was found that our method significantly outperformed traditional methods (such as SVM, Bayesian classifiers, and MP algorithms) in terms of accuracy and recall. The parameter sensitivity experiment further proves that the appropriate parameter setting can significantly improve the performance of the model, and verifies the robustness and practicability of the model. In general, the financial fraud detection method based on deep graph neural network shows a wide prospect in practical application and provides strong technical support for financial security. Future work will further optimize the model structure and explore more graph neural network variants to improve detection performance and apply it to more real-world scenarios.

References

1. Ali, Abdulalem, et al. "Financial fraud detection based on machine learning: a systematic literature review." Applied Sciences 12.19 (2022): 9637.
2. Shoetan, Philip Olaseni, et al. "Reviewing the role of big data analytics in financial fraud detection." Finance & Accounting Research Journal 6.3 (2024): 384-394.
3. Li, Ranran, et al. "Internet financial fraud detection based on graph learning." Ieee Transactions on Computational Social Systems (2022).
4. Zhou, Hangjun, et al. "Internet financial fraud detection based on a distributed big data approach with node2vec." IEEE Access 9 (2021): 43378-43386.
5. Gupta, Amit, M. C. Lohani, and Mahesh Manchanda. "Financial fraud detection using naive bayes algorithm in highly imbalance data set." Journal of Discrete Mathematical Sciences and Cryptography 24.5 (2021): 1559-1572.
6. Mao, Xuting, et al. "Financial fraud detection using the related-party transaction knowledge graph." Procedia Computer Science 199 (2022): 733-740.
7. Innan, Nouhaila, Muhammad Al-Zafar Khan, and Mohamed Bennai. "Financial fraud detection: a comparative study of quantum machine learning models." International Journal of Quantum Information 22.02 (2024): 2350044.
8. Awosika, Tomisin, Raj Mani Shukla, and Bernardi Pranggono. "Transparency and privacy: the role of explainable ai and federated learning in financial fraud detection." IEEE Access (2024).

 doi:10.20944/preprints202411.0609.v1

9. del Mar Roldán-García, María, José García-Nieto, and José F. Aldana-Montes. "Enhancing semantic consistency in anti-fraud rule-based expert systems." Expert Systems with Applications 90 (2017): 332-343.
10. Pambudi, Bayu Nur, Indriana Hidayah, and Silmi Fauziati. "Improving money laundering detection using optimized support vector machine." 2019 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI). IEEE, 2019.
11. Kumar, Ashwini, Sanjoy Das, and Vishu Tyagi. "Anti money laundering detection using Naïve Bayes classifier." 2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON). IEEE, 2020.
12. Le-Khac, Nhien-An, Sammer Markos, and Mohand-Tahar Kechadi. "Towards a new data mining-based approach for anti-money laundering in an international investment bank." Digital Forensics and Cyber Crime: First International ICST Conference, ICDF2C 2009, Albany, NY, USA, September 30-October 2, 2009, Revised Selected Papers 1. Springer Berlin Heidelberg, 2010.
13. Das, Shubhomoy, et al. "Incorporating expert feedback into active anomaly discovery." 2016 IEEE 16th International Conference on Data Mining (ICDM). IEEE, 2016.
14. Lorenz, Joana, et al. "Machine learning methods to detect money laundering in the bitcoin blockchain in the presence of label scarcity." Proceedings of the first ACM international conference on AI in finance. 2020.