2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT) | 978-1-6654-1296-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/AINIT54228.2021.00075

Fraud Detection Based on Graph Neural Networks with Self-attention

Min Li
Qilu University of Technology (Shandong Academy of Sciences)
Shandong Computer Science Center (National Supercomputing Center in Jinan)
Jinan, China

Mengjie Sun *
Qilu University of Technology (Shandong Academy of Sciences)
Shandong Computer Science Center (National Supercomputing Center in Jinan)
Jinan, China
* Corresponding author: 291708368@qq.com

Qianlong Liu
Qilu University of Technology (Shandong Academy of Sciences)
Shandong Computer Science Center (National Supercomputing Center in Jinan)
Jinan, China

Yumeng Zhang
Qilu University of Technology (Shandong Academy of Sciences)
Shandong Computer Science Center (National Supercomputing Center in Jinan)
Jinan, China

***Abstract*—With the rapid development of electronic payment, fraud cases occur frequently, and fraud detection is becoming more and more important. Traditional fraud detection model is not very good at processing information interaction between users. Furthermore, it could not handle the importance of each feature well. In order to solve this problem, this paper proposes a fraud detection model based on graph neural networks with self-attention mechanism. First of all, based on transaction data, the complex networks of interaction between user nodes and surrounding relationship nodes are reflected on the network modeling of social relationships between users. Second, by introducing graph neural networks model with self-attention mechanism based on node centrality structure characteristic index, a fraud detection model with coupling information of network characteristics and transaction characteristics is proposed. The experimental results show that this method can respond to fraud more accurately and improve the quality of judgment for the traditional fraud detection methods.**

Keywords-graph neural networks; fraud detection; deep learning; self-attention

I. INTRODUCTION

With the rapid development of Internet and e-commerce transaction services, electronic payment has become the most popular payment method. At the same time, fraud cases related to e-commerce transactions are also increasing. Fraud cases have severely impacted the stability of financial order and caused great social harm. As a result, fraud detection has become a high-profile topic. Fraud detection aims to predict whether an entity, which can be users or equipment or more, will participate in fraud in the future. Generally speaking, fraud detection problem can be thought of as classification problem. And its application direction includes financial fraud detection, water army recognition, etc. [1, 2,3]

Traditional fraud detection methods mostly use a variety of rule-based detection methods or manually identify many features to predict. The rule-based detection conducts fraud detection by observing whether the behavior activities conform to certain rules. The rule-based detection method has been used for a long time, but there exist shortcomings. The setting of rules is labor intensive and relies on the cognition of experts. Moreover, the rules are very vulnerable to the deceiver.

How to effectively use rules, reduce labor and time costs, and automatically detect fraud is of great significance to the development of Internet fraud model detection. At the same time, an automatic machine learning model is proposed. These models mainly predict according to the user's behavior, attributes and other characteristics, and use SVM, random forest and other methods to classify [4]. Xuan et al. (2018) [5] used random forests to train normal or fraud behavior characteristics. However, these fraud detection models using machine learning do not take into account information interaction between users, such as social relationships. In fact, these relationships may have a certain impact on fraud detection.

Recently, traditional graph learning is used for information interaction between users, but it also has the problem that the black box model cannot be explained [6]. Then, Gori et al. (2005) [7] first proposed a new neural networks model that can directly handle graphics --graph neural networks (GNN). Based on the intuitive idea of GNN, the nodes in the graph represent entities, and the edges represent the relationship between them. Compared with traditional graph learning, graph neural networks can not only learn the topology of graph networks, but also aggregate the characteristic information of neighborhood. Therefore, it can effectively learn various structures in graph networks, and plays a key role in the follow-up work. Park et al. (2019) [8] used the supervised neural networks model to estimate the importance of nodes in the graph. Meanwhile, node rich information, self-attention mechanism and centrality were flexibly used to adjust the model. For the graph neural networks of this paper, the method of self-attention mechanism is added to deal with the

The subject of Humanities and Social Sciences in Shandong Province in 2021 "Research on the mechanism of the level of digital economy, Inclusive Finance and high-quality development of manufacturing industry-- Based on the panel data of Shandong Province from 2011 to 2020" (NO. 2021-YYJJ-15).

The Project of Shandong Provincial Natural Science Foundation "Research on the impact mechanism of government data opening on Regional Social Innovation" (No. ZR2020MG075)

978-1-6654-1296-4/21/$31.00 ©2021 IEEE
DOI 10.1109/AINIT54228.2021.00075

information interaction between users, solve the black box problem and detect fraud.

II. MODELING

A. Model Framework

Due to the repeated occurrence of fraud, which greatly threatens the normal operation of social life, how to detect fraud has become a common concern. In social relations, fraud is closely related to everyone's life, work and other aspects. Therefore, the user's historical transaction records have become an important research data for fraud detection.

This paper extracts transaction features through historical transaction records and uses complex network analysis to extract network features. Then the features are aggregated by a graph convolutional neural networks model with a self-attention mechanism.

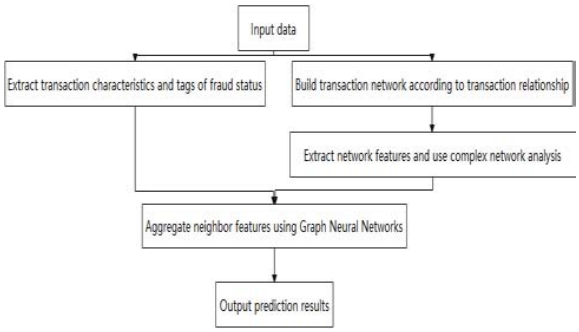

Figure 1. model structure framework

For a pair of directed graph G (V, E), V expresses the set of finite nodes with user characteristics and E expresses the edge set.

Based on the initial transaction, the transaction characteristics are extracted by integrating and calculating the data, and finally the following indicators are obtained: transaction amount, transaction product and time interval. Network characteristics are extracted based on complex networks analysis methods. And the importance and influence of different users in transactions are analyzed with the characteristics of degree centrality, betweenness centrality, and closeness centrality. In this paper, the graph convolution neural networks with self-attention mechanism in the graph neural networks are selected to aggregate neighbors, so as to construct the transaction fraud detection model.

B. Feature Extraction Algorithm

The data characteristics in this paper are divided into transaction characteristics and network characteristics. Transaction characteristics are based on the initial transaction. After calculation, the four transaction characteristics of transaction amount, transaction product, time interval, and buyer account can be obtained.

The extraction of network features is based on complex network analysis, and the use of node centricity recognition algorithm is as follows.

1) Degree Centrality: Set up a network G=(V，E) with no direction, N represents the total sum of nodes, and M represents the total sum of edges. Adjacency Matrix is $A=a_{ij}$.The degree of node v_i is written as k_i .Then the Degree Centrality of the node is described as:

$$DC(i) = \frac{k_i}{N-1} \quad (1)$$

2) Closeness Centrality: Closeness centrality measures the average distance between nodes and other nodes, which reflects the proximity of nodes in the network. Let d_{ij} be the shortest time path length of nodes v_i to v_j . Then the closeness centrality of the node is defined as:

$$CC(i) = \frac{N-1}{\sum_{j\neq i} d_{ij}} \quad (2)$$

3) Betweenness Centrality: Betweenness centrality is a measure of the criticality of a node by the number of the shortest path passing through a fixed node. It describes the level which nodes control information on the network. Betweenness Centrality is defined as:

$$BC(i) = \frac{2}{(N-1)(N-2)} \sum_{i\neq s, i\neq t, s\neq t} \frac{g_{st}^i}{g_{st}} \quad (3)$$

Where g_{st} is the number of the shortest path between nodes v_s and v_t, and g_{st}^i is the number of nodes v_i in the shortest path through v_s and v_t .

C. The Selection Of Graph Neural Networks Model

Graph convolution neural networks (GCN) can be regarded as a feature extractor with graph data. The core idea is to use the edge information to aggregate the node information and add and average the neighbor nodes, so as to generate a new node representation. Bruna et al. [9] proposed a graph Laplacian method based on spectral domain, which extended the convolutional neural networks to non-Euclidean data. For low dimensional graphs, we can learn the convolution layer of multiple parameters independent of the input size, so as to form an efficient deep structure. Kipf et al. [10] proposed a semi supervised learning method based on effective convolution neural networks. The graph convolution neural networks used in this paper use its proposed method to work directly on the graph. We use the first-order local approximation of spectral convolution to stimulate the selection of our convolution structure. Our model scales the edges of the graph linearly and learns the hidden layer representation, which codes both the local graph structure and the characteristics of the nodes. The above domain-based method simplifies the improved first-order graph convolution neural networks model and uses semi-supervised method to classify user nodes on the transaction network. Based on the spectral decomposition of the Laplacian matrix, the following graph volumes are adopted by GCN:

$$H^{l+1} = \sigma\left(\tilde{D}^{-\frac{1}{2}}\tilde{A}\tilde{D}^{-\frac{1}{2}}H^l W^l\right) \quad (4)$$

In equation 4, H^l represents the input of the initial eigenvector of the node, H^{l+1} represents the output of the updated state vector of the node (the output of the l layer), $\sigma(\cdot)$represents the non-linear activation function, $\tilde{A}$ represents the degree matrix of the self-connected matrix $\tilde{A} = A + I$, $\tilde{D}$

represents the degree matrix of the self-connected matrix, I represents the unit matrix, A represents the adjacency matrix, and W^{l}represents the linear transformation matrix.

The loss functions of this paper are as follows:

$$L = -\sum_{i\in Y}\sum_{k=1}^{K} t_{ik} \ln h_{ik}^{(L)} \quad (5)$$

Where Y represents the index data collection of nodes, $h_{ik}^{(L)}$ represents the kth with node marked in layer L, and t_{ik} represents the true information label.

In order to model the nodes and relationship edges of a transactional social network, multiple convolution layers need to be overlaid to learn the internal hidden representation of each node in the graph and to complete the information fusion of behavior content or social relationships.

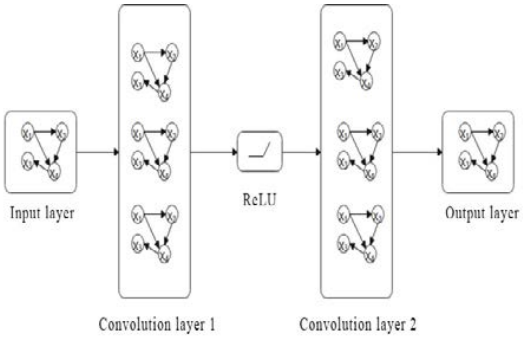

Figure 2. GNN schematic diagram

The GNN diagram is shown above. The graph convolution layer of GNN is stacked by two layers with each layer sharing parameters. The neighbors of each node perform a convolution operation, update the node with the result of the convolution, and then update the hidden state of the node through the activation function Rectified Linear Unit (ReLU).

III. EXPERIMENT

A. Dataset

This data comes from the real-world e-commerce transactions of Vesta, a pioneer in guaranteeing e-commerce payment solutions. Dataset has 73838 customers (credit cards), with at least two or more transactions. Of these, 71575 (96.9%) had no fraudulent transactions and 2134 (2.9%) always had fraudulent transactions. Only 129 (0.2%) were a mixture of fraudsters and non-fraudsters. The distribution of the products traded is shown in the figure.

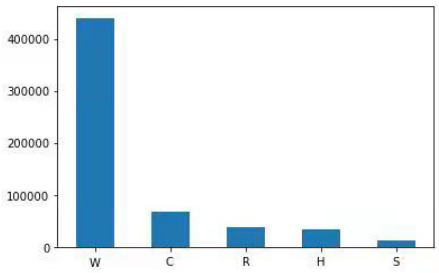

Figure 3. The distribution of products

The training set included 569877 people who were not involved in fraud and 20663 people who were involved in fraud. The data set is highly unbalanced, and the distribution of fraud and non-fraud is shown in the figure.

```
train_transaction.isFraud.value_counts()

0    569877
1     20663
Name: isFraud, dtype: int64
```

Figure 4. Data distribution. The isFraud attribute name indicates whether the user is a fraudster, 0 is a non-fraudster, and 1 is a fraudster.

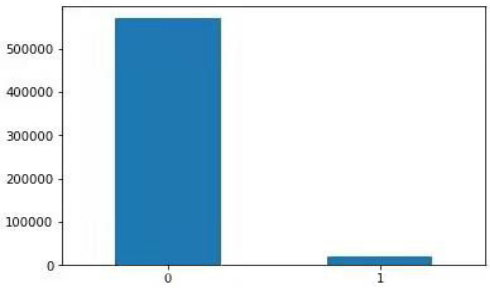

Figure 5. Data distribution histogram

B. The Experimental Setup

For the data set, the transaction and network characteristics are selected to construct the user characteristics of the calculation graph, as shown in the table I.

In the GAT structure, there are 32 hidden units in the first convolution layer and 16 hidden units in the second convolution layer. To prevent overfitting, a learning rate is set to 0.01, and the dimension of the hidden variable Zi is 16. The experiment used Adam optimizer to train 100 epochs. The model is used for performance evaluation experiments with accuracy, loss rate, AUC and other indicators.

TABLE I. SELECT FEATURES

Features	Describe
Transaction AMT	Transaction amount
Product CD	Trading products
Transaction DT	The time interval
DC	Degree of centricity
CC	Close to the centra
BC	Betweenness centrality

C. An Optimization Method

The optimization of the algorithm uses forward and reverse propagation in common neural networks. The graph convolution neural networks are expanded into the common networks structure shown in the following figure. The connection between layers is determined by the connection relationship of the original graph. The whole model is trained by forward propagation from left to right, and then back propagation according to the loss. First, the predicted value and loss function are calculated based on the input image and label, and the initial gradient is set to 0, then the current gradient is calculated by back propagation. Finally, the parameters in the network are updated according to the gradient.

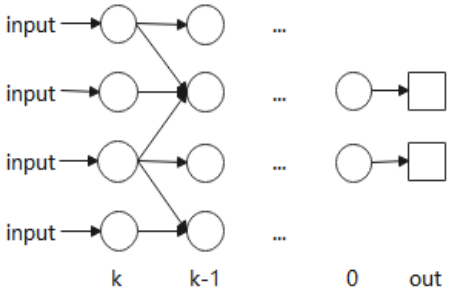

Figure 6. Neural networks expansion plan

D. Baseline Methods

Comparing models of various algorithms used in the experiment include:

- Random forest: A classifier that uses multiple trees to train and predict data. The transaction characteristics of users are used as input for the model.
- Support Vector Machine (SVM): A classifier that uses supervised learning to classify data. The transaction characteristics of users are used as input for the model.
- GCN: A feature extractor that allows us to process the data characteristics of these graphs. The transaction characteristics of users with social relationships are used as input for the model.
- GAT: A graphical convolution neural networks with self-attention mechanism are added, which is the graphical convolution neural networks used in this paper.

Accuracy and AUC are used to assess the performance of each fraud detection model.

E. Experimental Analysis

Based on the analysis above, the transaction fraud detection model is used to predict and evaluate the data. The loss values of training set results and the accuracy of test set results are shown in the following figure. The results show that the model predicts very inaccurately at the beginning, and the accuracy is similar to that of random guess, or even less than that of guess. As the number of training sessions increases, the accuracy of the model increases and the loss function decreases. After the model training is stable, the highest accuracy rate reaches 99.3%.

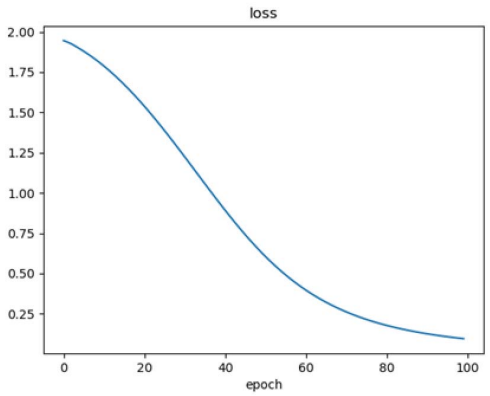

Figure 7. Training set loss function

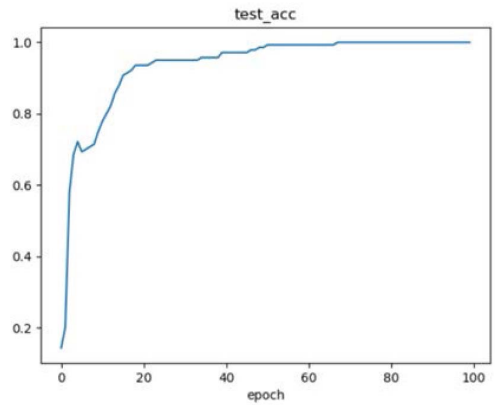

Figure 8. The accuracy of the test set

Random forest and Support Vector Machine (SVM) are widely used and the main algorithms for classification problems. GCN is the most popular neural networks model at present, and the model in this paper is also a graph neural networks model based on it. This model is compared with the random forest and the support vector machine model in

machine learning and the graph neural networks model. The prediction accuracy of the different models is shown in the following figure. GAT model has better recognition ability than other models. Moreover, its AUC is 7.1% higher than the random forest in traditional machine learning model, 5.7% higher than the support vector machine, and 2.1% higher than the traditional GCN.

Therefore, the model has a better accuracy for fraud detection of transaction data with social relationship.

TABLE II. THE CLASSIFICATION RESULTS OF THE MODEL

The model's name	acc	AUC
RF	0.913	0.915
SVM	0.922	0.929
GCN	0.978	0.965
GAT	0.993	0.986

IV. CONCLUSION & FUTURE WORK

This paper presents a fraud detection method based on graph neural networks with self-attention mechanism. Based on complex networks analysis and graph neural networks algorithm, the transaction characteristics and network characteristics of users are analyzed and evaluated, and a fraud detection model is built. This paper evaluates GAT model through a real data set. By comparing the calculated results with the actual results, it can be found that this model has good prediction results for fraud detection. That is, it can reduce fraud and risk loss to some extent. In the future, the graph neural networks will be further applied to the real-time system to achieve the real-time interception of fraud detection.

ACKNOWLEDGMENT

This paper is supported by the subject of Humanities and Social Sciences in Shandong Province in 2021"Research on the mechanism of the level of digital economy, Inclusive Finance and high-quality development of manufacturing industry--Based on the panel data of Shandong Province from 2011 to 2020" (NO. 2021-YYJJ-15), and the project of Shandong Provincial Natural Science Foundation "Research on the impact mechanism of government data opening on Regional Social Innovation" (No. ZR2020MG075).

REFERENCES

[1] Sungkono, K.R. and R. Sarno. "Patterns of fraud detection using coupled Hidden Markov Model." in 2017 3rd International Conference on Science in Information Technology (ICSITech). 2017. IEEE.

[2] Huang, D., et al., "CoDetect: Financial fraud detection with anomaly feature detection. "IEEE Access, 2018. 6: p. 19161-19174.

[3] Yong-qiang, et al. "Network Malicious Action Hazard Assessment Based on Game Model and Grey Clustering." in 2014 International Conference on Computer,Network Security and Communication Engineering(CNSCE 2014).

[4] Hejazi, M. and Y.P. Singh, "One-class support vector machines approach to anomaly detection." Applied Artificial Intelligence, 2013. 27(5): p. 351-366.

[5] Xuan, S., et al. "Random forest for credit card fraud detection." in 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC). 2018. IEEE.

[6] Liu, Z., et al. "Heterogeneous graph neural networks for malicious account detection." in Proceedings of the 27th ACM International Conference on Information and Knowledge Management. 2018.

[7] Gori, M., G. Monfardini, and F. Scarselli. "A new model for learning in graph domains. in Proceedings." 2005 IEEE International Joint Conference on Neural Networks, 2005. 2005. IEEE.

[8] Park, N., et al. "Estimating node importance in knowledge graphs using graph neural networks." in Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. 2019.

[9] Bruna, J., et al., "Spectral networks and locally connected networks on graphs." arXiv preprint arXiv:1312.6203, 2013.

[10] Kipf, T.N. and M. Welling, "Semi-supervised classification with graph convolutional networks." arXiv preprint arXiv:1609.02907, 2016.