MIDLG: Mutual Information based Dual Level GNN for Transaction Fraud Complaint Verification

Wen Zheng
Institute of Computing Technology, University of Chinese Academy of Sciences
Beijing, China
zhengwen20s@ict.ac.cn

Bingbing Xu
Institute of Computing Technology, Chinese Academy of Sciences
Beijing, China
xubingbing@ict.ac.cn

Emiao Lu
Wechat Pay, Tencent
Beijing, China
emiaolu@tencent.com

Yang Li
Qi Cao
Institute of Computing Technology, Chinese Academy of Sciences
Beijing, China
liyang21s,caoqi@ict.ac.cn

Xuan Zong
Wechat Pay, Tencent
Beijing, China
jasonzong@tencent.com

Huawei Shen
Institute of Computing Technology, Chinese Academy of Sciences
Beijing, China
shenhuawei@ict.ac.cn

ABSTRACT

"Transaction fraud" complaint verification, i.e., verifying whether a transaction corresponding to a complaint is fraudulent, is particularly critical to prevent economic loss. Compared with traditional fraud pre-transaction detection, complaint verification puts forward higher requirements: 1)an individual tends to exhibit different identities in different complaints, e.g., complainant or respondent, requiring the model to capture identity-related representations corresponding to the complaint; 2)the fraud ways evolve frequently to confront detection, requiring the model to perform stably under different fraud ways. Previous methods mainly focused on fraud pre-transaction detection, utilizing the historical information of users or conduct message passing based GNNs on relationship networks. However, they rarely consider capturing various identity-related representations and ignore the evolution of fraud ways, leading to failure in complaint verification. To address the above challenges, we propose the mutual information based dual level graph neural network, namely MIDLG, which defines a complaint as a super-node consisting of involved individuals, and characterizes the individual over node-level and super-node-level. Furthermore, the mutual information minimization objective is proposed based on "complaint verification-causal graph" to decouple the model prediction from relying on specific fraud ways, and thus achieve stability. MIDLG achieves SOTA results through extensive experiments in complaint verification on WeChat Finance, one online payment service serving more than 600 million users in China.

KDD '23, August 6–10, 2023, Long Beach, CA, USA.

ACM ISBN 979-8-4007-0103-0/23/08…$15.00
https://doi.org/10.1145/3580305.3599865

CCS CONCEPTS

• **Networks** → **Social media networks**; • **Information systems** → Social networks.

KEYWORDS

"transaction fraud" complaint verification; dual level propagation; "specific fraud" forget learning; graph neural networks

ACM Reference Format:
Wen Zheng, Bingbing Xu, Emiao Lu, Yang Li, Qi Cao, Xuan Zong, and Huawei Shen. 2023. MIDLG: Mutual Information based Dual Level GNN for Transaction Fraud Complaint Verification. In *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD '23), August 6–10, 2023, Long Beach, CA, USA.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3580305.3599865

1 INTRODUCTION

With the rapid development of Internet finance, online transaction fraud detection has become crucial, which can be divided into fraud pre-transaction detection and "transaction fraud" complaint verification. Fraud pre-transaction detection is designed to prevent suspicious transactions from occurring while "transaction fraud" complaint verification aims to verify whether a transaction corresponding to a complaint is fraudulent. Complaint verification can recover transaction losses or hand the complaint over to the police in serious cases to prevent possible future fraud. Therefore, it is critical to accurately verify complaints while the widespread fake complaints bring challenges.

Fig. 1 shows the process of complaint verification. As illustrated, a complaint generally involves multiple individuals with different identities, including the complainant, the respondent and the payee. Note that the respondent and payee are often not the same user, e.g., in gang fraud, the respondents are a large number of individuals who carry out fraudulent acts, but the payee is the leader of the gang. Compared with traditional fraud pre-transaction detection, complaint verification puts forward higher requirements: 1) an individual tends to exhibit different identities in different complaints, e.g., as Fig2 a) illustrated, a user acts complainant or respondent in

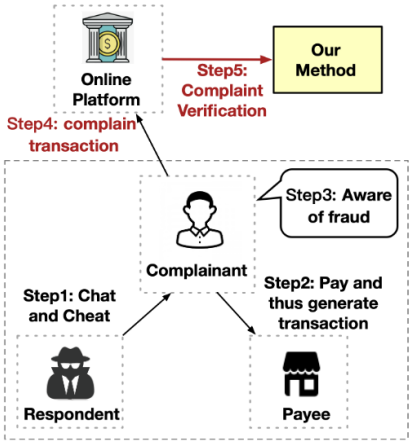

Figure 1: The process of complaint verification.

different complaints, requiring the model to capture identity-related representations corresponded with complaint; 2) the fraud ways evolve frequently to confront verification, e.g., as Fig2 b) shows, both the distribution of fraud ways and the specific patterns under a fraud way can change over time. Such phenomena require the model to perform stably under different fraud ways and patterns.

Previous methods mainly focused on fraud pre-transaction detection rather than complaint verification and they often leverage the attributes and historical behaviors of one transaction, e.g., SVM[13] models and neural networks[1]. Moreover, such methods do not consider the relations among different individuals. To model the relations, an intuitive idea is to combine the pending complaint and its related historical complaints to form a graph, where the nodes are all individuals involved in the above complaints, and the edges are the complaint or payment relations. Then leverage the current SOTA GNNs[9, 11, 15, 42] to model the above graph. However, the existed GNNs often rely on the homophily assumption[41] that connected nodes tend to have similar labels, which is not satisfied, e.g., connected nodes are usually complainants and respondents, and their labels are not consistent. What's worse, previous GNNs rarely consider to capture identity-related various representations and also ignore the evolution of fraud ways. Overfitting a model to a specific fraud way or pattern will lose its generalization to other fraud ways. The above problems lead to the failure of existed GNNs in complaint verification.

To address the above challenges, we propose the **m**utual **i**nformation based **d**ual **l**evel **g**raph neural network for complaint verification, namely MIDLG. Specifically, we define a super-node to represent a complaint which consists of its involved individuals, and characterizes the individual over node-level and super-node-level message passing. Such super-node-level message passing can significantly improve the homogeneity ratio and capture identity-related representations for individuals. To perform stably under the changes of fraud ways and patterns, the mutual information minimization objective is proposed based on "complaint verification-causal graph" to decouple the prediction results from relying on fraud patterns and ways. We implement the objective by the sophisticated fraud ways based adversarial forgetting and fraud patterns based invariant risk minimization respectively. Extensive experiments on WeChat Finance[1] show that our model achieves state-of-the-art results in "transaction fraud" complaint verification. Also, we provide ablation studies to evaluate the importance of each part.

Our contributions are summarized as follows:

- We investigate "transaction fraud" complaint verification, one important and realistic AI application problem. We propose the mutual information based dual level GNN for complaint verification, which defines a complaint as a super-node consisting of involved individuals, and characterizes the individual at node-level and super-node-level.
- We propose the "complaint verification-causal graph" and decouple the model prediction from relying on specific fraud patterns to achieve stability. Deriving from the mutual information minimization, we implement fraud ways-based adversarial forgetting and fraud patterns-based invariant risk minimization to achieve this goal.
- Our model achieves state-of-the-art results through extensive experiments in complaint verification on WeChat Finance, one online credit payment service serving more than 600 million users in China.

2 PRELIMINARY

In this section, we present the formalized definition of "transaction fraud" complaint verification and conduct detailed statistical analyzes of data.

2.1 Problem Definition

For "transaction fraud" complaint verification problem, we need to classify each transaction into binary classes: fraudulent or normal. The formal definition of the task is given as follows. Each complaint can be represented as a graph $\mathcal{G} = (V, E, X^v, X^e)$ which includes itself and its related historical complaints(the complaints that share at least one same individual with it). V denotes the individuals all involved in the above complaints with size N. E denotes the set of edges generated from the complaint or payment relations in involved complaints. $X^v \in \mathbb{R}^{N \times D^v}$ denotes the node attributes matrix, D^v is the dimension of input attributes. X^e denotes the edges attribute matrix. Label $y \in \{0, 1\}$ indicates whether a transaction corresponding to a complaint is fraudulent with $y = 1$ or normal with $y = 0$. Overall, We need to classify $\mathcal{G}$ into two classes: fraudulent or normal.

2.2 Data Analysis

In this subsection, we elaborate on why we propose dual level graph neural network for complaint verification and analyze the unstable distribution caused by changes of fraud ways and patterns.

2.2.1 Analysis of necessity of dual level propagation. In recent years, numerous graph neural networks, such as GCN[15], GAT[31], GraphSAGE[11] and MPNN[9], have achieved high performance by aggregating neighbors information to center nodes on both node

[1]Wechat Finance is Tencent's integrated business platform that provides mobile payment and financial services.

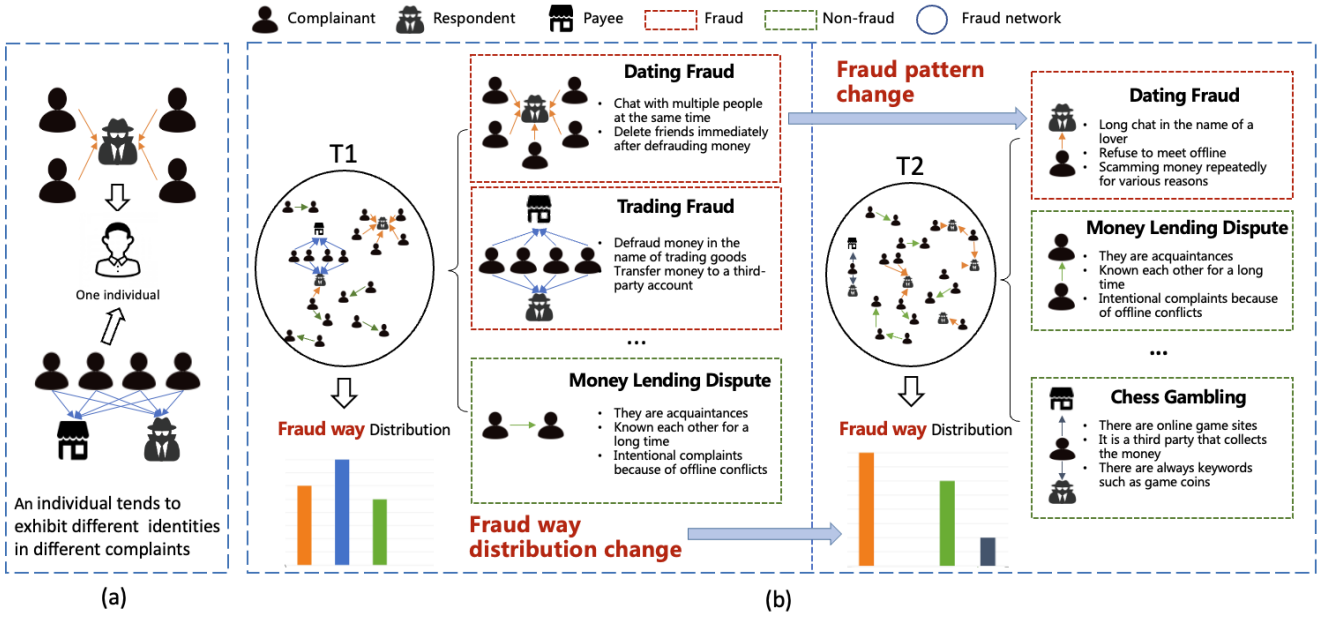

Figure 2: "Transaction fraud" complaint verification task description. Two challenges are given:(a) One individual may appear in different complaints with different identities. (b) Fraud patterns and fraud ways frequently change over time.

classification task and graph classification task. However, the traditional GNNs are not suitable for our "transaction fraud" complaint verification task. The reasons are as follows.

Firstly, an individual can play different identities in multiple complaints, e.g. complainant or respondent. So the model is expected to have the ability to take identity-related representation learning into consideration. Unfortunately, most current GNNs merely capture the single representation for one node which cannot characterize the different identities in multiple complaints for one individual precisely. Although there are several GNN-based studies that deliver different messages with diverse metapaths[34, 45], they finally learn one representation for an individual which cannot solve this dilemma effectively.

Additionally, the labels of two individuals connected by a complaint edge usually differ from each other. However, most graph neural networks follow the smoothness assumption proposed in [41], which leads to GNN models that only achieve great improvements on higher homogeneity ratio graphs. As a result, previous GNNs focusing on message passing at node level only cannot perform well. Instead, we define the complaint as a super-node and analyze the homogeneous ratios on the complaint based on the real data of WeChat Finance shown in Table 1. We extract 42,265 complaints from July and expand each of them into one graph by adding complaints that share at least one same individual with it. Note that the "Isolated-super-node" means no complaints sharing individual with the pending complaint. We figure out that the homogeneity ratio is still high for super-nodes, meaning the propagation at super-node level is promising and can facilitate tasks.

2.2.2 Analysis of necessity of stability design. To confront detection, fraud evolves frequently and often contains many different subtypes

Table 1: Homogeneous Ratio at Super-Node Level

Description	Value
Isolated-super-node Subgraph	22561
Multi-super-node Subgraph	19704
Homogeneous Ratio	0.9680

(fraud ways), such as dating fraud, non-delivery fraud, trading fraud, etc. As shown in Fig. 2, fraudsters will change their fraud ways and patterns for avoiding verification. Furthermore, the fraud data distribution fluctuates significantly on particular days, e.g., people tend to chat online shopping on crazy Friday, leading the number of trading fraud to increase.

To measure the fluctuation of fraud way distribution, we choose a day at the beginning of June and a day close to the 18th of June, which is the shopping spree day. We also pick two days in the mid and end of July to see how the distribution of the subtypes fluctuates over time. Fig. 3 demonstrates the distributions of five representative fraud subtypes. Taking trading fraud as an example, it is apparent that the quantity on June 21st is much lower than that on June 1st and the number of transaction frauds fluctuates significantly over time. Additionally, we also observe that there are some fraud subtypes such as pornography fraud and gambling fraud that occur every day but in a small number. However, ignoring these will still cause great economic losses.

This reveals that the distribution of fraud ways fluctuates greatly each day. Furthermore, different fraud subtypes also can present different patterns over time. As shown in Fig. 2, "Dating Fraud"

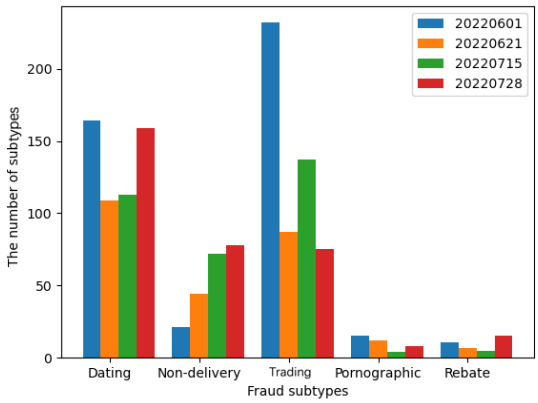

Figure 3: Analysis of change of the number of subtypes. The x-axis is the fraud subtypes, and the y-axis is the quantity of each subtype.

presents two completely different patterns at T1 and T2. This phenomenon requires the model not to fit into a specific fraud, but the commonalities of all fraud types, thus making stable predictions. In addition, the model should also pay much attention to the fraud subtypes that rarely occur.

3 METHOD

In this section, we present the details of mutual information based dual level graph neural network for complaint verification (MIDLG). Fig. 4 demonstrates the overall architecture of MIDLG which consists of a dual level propagation module(DLPM) and "specific fraud" forget learning module(SFFLM). DLPM motivated by subsection 2.2.1 aims to improve the homogeneity ratio and capture identity-related representations. SFFLM motivated by subsection 2.2.2 aims to decouple the prediction results from relying on specific fraud patterns and ways based on mutual information minimization to achieve stability. We will introduce each module respectively in the following sections.

3.1 Dual Level Propagation Module

The node level propagation in DLPM aims to capture the essential attributes of individuals. The super-node level propagation in DLPM can significantly improve the homogeneity ratio and capture identity-related representations. Next, we introduce representation learning at the node level and super-node level respectively.

3.1.1 Representation Learning at Node Level. In view that one individual may occur in multiple "transaction fraud" complaints, it will be involved in various relationships. To capture different relationships, we form relationship-related subgraphs to learn relationship-related representations at node level respectively. The types of relationships contain the complaint relationship (between a complainant and a respondent), the payment relationship (between a complainant and a payee) and the partnership relationship (between a respondent and a payee). Specifically, we construct the relationship-related subgraphs by filtering the edges of relationship r in $\mathcal{G}$ defined in Sec.2.1. Each subgraph is defined as $\mathcal{G}^r = (V^r, E^r, X^{rv}, X^{re})$ where E^r denotes the edges set under the relationship r. We apply the Laplacian matrix [15] to aggregate neighbors' information on each subgraph to reduce the parameters of the model. The embedding of nodes is updated in each layer as:

$$Z^r = \sigma(\tilde{D}^{r\,\frac{1}{2}} \tilde{A}^r \tilde{D}^{r\,-\frac{1}{2}} X^{rv} W^r) \tag{1}$$

Let D^r denotes the degree matrix. A^r denotes the adjacency matrix. I_N denotes the identity matrix. Note that $\tilde{A}^r = A^r + I_N$, $\tilde{D}^r_{ii} = \sum_j \tilde{A}_{ij}$. σ denotes the activation function and $W^r \in \mathbb{R}^{D^e \times D^h}$ is the parameters. $z^r_{v_i}$ is the representation of node v_i on the relation r. Finally, we concatenate the embedding of node v_i in different relations as its node-level representation:

$$z_{v_i} = \|_r^R z^r_{v_i} \tag{2}$$

where R is the set of relationship types.

3.1.2 Representation Learning at Super-Node Level. Generally, an individual tends to have different identities in different complaints. Therefore, we need to learn the identity-related representations to better characterize complaints after acquiring the node-level representations. To combat this challenge, we regard a complaint as a super-node that contains all the individuals involved in this complaint. By introducing the super-nodes, an individual will be involved in different super-nodes for identity-related representation learning. Meanwhile, two super-nodes are connected with an edge when they share at least one individual in a period of time so that the super-node-level GNN based model can pass messages between super-node. Based on this, the model can adaptively learn the different identity-related representations.

Specifically, we initialize the complaint-level embedding by combining node-level representations and the edge attributes of a complaint. For example, the embedding of the complaint j containing three nodes, denoted as v_1, v_2 and v_3, is initialized as:

$$h^0_j = [z_{v_1}, z_{v_2}, z_{v_3}, x^e_j], \tag{3}$$

where x^e_j denotes edge properties of complaint j and z_{v_i} is representation of v_i obtained from node level propagation. Different from node-level learning, attention mechanism is leveraged for super-node level propagation. We calculate the attention weight between two super-nodes at l-layer when two complaints share at least one same individual and appear within seven days as:

$$\alpha^l_{ij} = \frac{\exp(\text{LeakyReLU}((\vec{a}^l)^T [W^l \vec{h}^{l-1}_i \| W^l \vec{h}^{l-1}_j]))}{\sum_{k \in \mathcal{N}_i} \exp(\text{LeakyReLU}((\vec{a}^l)^T [W^l \vec{h}^{l-1}_i \| W^l \vec{h}^{l-1}_k]))}, \tag{4}$$

where $\mathcal{N}_i$ denotes the neighbour set of super-node i. Then we leverage the multi-headed attention mechanism to update the identity-related representation of complaint i in the first $L-1$ layers as:

$$\vec{h}^l_i = \|_{k=1}^K \text{ELU}(\sum_{j \in \mathcal{N}_i} \alpha^{lk}_{ij} W^{lk} \vec{h^{l-1}_j}), \tag{5}$$

where α^{lk}_{ij} denotes the attention parameters in the k-th attention head at l-th layer and W^{lk} is the weight matrix.

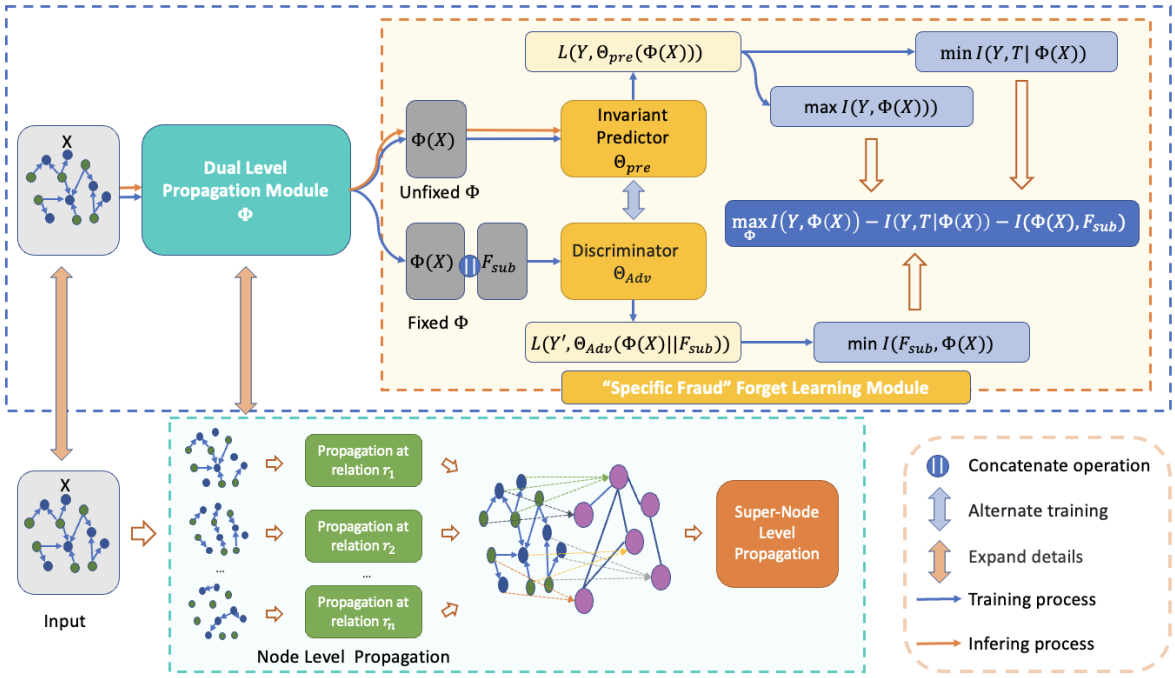

Figure 4: Overview of our MIDLG consists of dual level propagation module and "specific fraud" forget learning module.

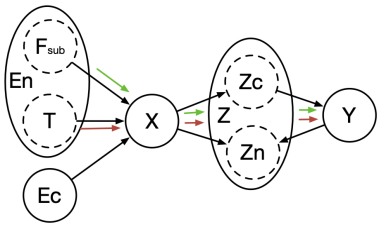

Figure 5: The complaint verification-causal graph. X are the attributes. Time T and subtypes of complaints F_{sub} cause fluctuations. Z_a and Z_c are the representation learned by the model. Y is the output.

With the identity-related representation h_i^l learned at super-node level, we map h_i^l to a 2-dimensional output to classify i as:

$$\vec{h}_i^L = \text{ELU}(\sum_{j \in \mathcal{N}_i} \alpha_{ij}^L W \vec{h}_j^{L-1}), \tag{6}$$

3.2 "Specific Fraud" Forget Learning Module

In this part, we first describe why traditional models are unstable from a causal perspective. Then we propose to constrain the model via mutual information minimization to forget the specific fraud ways and patterns and thus improve model stability.

3.2.1 Complaint verification-causal graph. We know fraudulent ways and patterns change over time. As shown in Fig5, the training data X are generated due to a number of factors, which can be divided into two parts: E_c and E_n. E_c is the casual environment variable that shows the constant impact on fraud. E_n is the non-causal environment variable which shows the unstable impact. In our scenario, time (containing the change of fraud patterns) and fraud subtypes (fraud ways) can be regarded as E_n. We hope our model to learn complaint embedding that only contains the causal factors, such as paying behaviors. The representation learned by the model is also divided by us into two parts: non-causal component Z_n and casual component Z_c. Z_c is the causal representation, which can leads to a stable prediction. Z_n is the non-causal part of Z, which contains the unstable factors with model output Y. Thus constraining the representation Z including Zc only can make the stable prediction. So we need to break the red and green paths.

Based on the above analysis, improving the stability when time and fraud subtypes distribution change requires the model not to fit non-causal variables. Ideally, it is desired that the predicted Y does not fluctuate drastically over time and subtypes.

To forget time T and subtype F_{sub} in Y, here are two directions:

(1) The ideal way is to make Y and F_{sub} (or T) independent when given Z_c. However, it is almost impossible to distinguish Z_c and Z_n from the representation Z. Thus when conditioned on Z, we can minimize the mutual information $I(F_{sub}, Y|Z)$ and $I(T, Y|Z)$ to constrain the model not to capture Z_n, which is non-causal variable but affected by T and F_{sub}.

(2) We can directly reduce the mutual information $I(Z, T)$ and $I(Z, F_{sub})$ to break the red path and the green path.

In the following sections, we explain how to determine the directions in forgetting T and F_{sub} respectively, and how to design a model to achieve our goals.

3.2.2 Forget the effect of time on Y. As time is futuristic, it is difficult to directly decrease the mutual information between Z and T. So we consider the first approach, i.e., eliminating the spurious environmental feature Z_n in Z by seeking the causal feature Z_c that can make Y stable over T. Therefore, the ideal representation $Z = \Phi(X)$ has the following two merits: (1) Z does not change among different T for the same Y, hence achieving the conditional invariance of $Y \perp T \| Z$; (2) Z should be informative of the class label Y. The above two conditions coincide with the objective of invariant risk minimization[2] method, and the learning objective is[16]:

$$\max_{\Phi} I(\Phi(X), Y) - \lambda I(Y, T|\Phi(X)) \tag{7}$$

where T is used to divide the dataset into different environments, e.g., the dataset collected in Time $T = 20220618$ can be seen as an environment. The objective function corresponding to our complaint causal graph is to reduce non-causal Z_n in Z.

We split the dataset into multiple environments by day. The model includes two parts: data representation learner and predictor. Based on invariant risk minimization, we find a representation Φ to learn causal connections rather than statistical associations by constraining the optimal predictor is simultaneously Bayes optimal in all environments. The main objective is stated as:

$$\begin{aligned} &\min_{\substack{\Phi:\mathcal{X}\to\mathcal{H} \\ w:\mathcal{H}\to\mathcal{Y}}} \sum_{e\in\mathcal{E}_{\text{tr}}} R^e(w \circ \Phi(\mathcal{X})) \\ &\text{s.t.} \quad w \in \arg\min_{\bar{w}:\mathcal{H}\to\mathcal{Y}} R^e(\bar{w} \circ \Phi), \text{for all } e \in \mathcal{E}_{\text{tr}} \end{aligned} \tag{8}$$

where w is the predictor, $\mathcal{X}, \mathcal{H}, \mathcal{Y}$ are input, hidden representations, and output representations respectively, $\mathcal{E}_{tr}$ is the environment set, Φ is the data representation learner and R^e is the loss function, which is the cross-entropy loss in complaint verification task. It restricts the optimal predictors based on $\Phi(\mathcal{X})$ in all environments are the same and thus reduces $I(Y, T|\Phi(X))$. We follow the equivalent IRMv1[2] to achieve it.

3.2.3 Forget the effect of subtype on Y. Although the above approach reduces mutual information(MI) between T and prediction label Y given representation, it is insufficient in reducing MI between subtypes and Y. Specifically, subtypes are highly correlated with the label Y, and even some subtypes are all fraudulent. The environment partition based on subtypes will result in some environments containing only one type of label Y, which can not guide the model training. Therefore, we directly minimize the mutual information between the representation and subtype F_{sub}:

$$\min_{Z} I(Z, F_{sub}) = \min_{Z} D_{KL}(P(Z, F_{sub}) \| P(Z)P(F_{sub})) \tag{9}$$

where Z is the representation learned by the model. Minimizing the mutual information equals minimizing the KL divergence[27].

We implement it via GAN which can minimize the KL divergence [36]. Specifically, we take the representation of each complaint (obtained by the above dual level propagation module) concatenate with its real subtype as a positive example $y_i^{adv} = 1$, and concatenate the representation with a random subtype as a negative example $y_i^{adv} = 0$. A discriminator is proposed to classify the above examples. Let Φ denote the dual level propagation module, then we get:

$$H = \Phi(V, E, X^{node}, X^{edge}) \tag{10}$$

where the representation of complaint i is the i-th row of H. Then we put the representation into the discriminator:

$$\hat{y}_i^{adv} = \sigma(W_2(\sigma(W_1[h_i \| F_{sub}]))) \tag{11}$$

where W_1 and W_2 are parameters and σ is activation function. The discriminator fixes the parameters in Φ and maximizes the accuracy of subtypes prediction by optimizing W_1 and W_2. The optimization objective of the discriminator is to minimize:

$$\mathcal{L}^{Adv} = \frac{1}{N'} \sum_{i=1}^{N'} y_i^{adv} \log \hat{y}_i^{adv} + (1 - y_i^{adv}) \log(1 - \hat{y}_i^{adv}) \tag{12}$$

where N' is the number of samples. To achieve Eq.9, we constrain the Φ to forget the F_{sub}. Specifically, we fix W_1 and W_2 and train Φ to maximize $\mathcal{L}^{Adv}$. Such adversarial forgetting makes the discriminator unable to distinguish between positive and negative samples, thus constraining the representation not relying on subtypes.

3.2.4 Overall view on "specific fraud" forget learning. We consider the respective properties of time and subtypes, and keep knowledge in Z by maximizing $I(Y, Z)$. The final objective is as:

$$\max_{Z} I(Y, Z) - I(Y, T|Z) - I(Z, F_{sub}) \tag{13}$$

where the symbols correspond to the meaning in Fig5.

3.3 Model Optimization

After the propagation at the super-node level, the i-th complaint representation h_i is fed into a softmax activation function as:

$$\hat{y}_i = \text{softmax}(h_i). \tag{14}$$

For the classification task, we compute the cross-entropy loss:

$$\mathcal{L}^{BCE} = \frac{1}{N} \sum_{i=1}^{N} y_i \cdot \log \hat{y}_i + (1 - y_i) \cdot \log(1 - \hat{y}_i) \tag{15}$$

where y_i is the ground truth label and $\hat{y}_i$ is the prediction of complaint i. Combining $\mathcal{L}^{BCE}$, $\mathcal{L}^{IRM}$ and $\mathcal{L}^{Adv}$, we obtain the final loss of the main model:

$$\mathcal{L}^{M} = \mathcal{L}^{BCE} + \lambda_1 \mathcal{L}^{IRM} - \lambda_2 \mathcal{L}^{Adv} \tag{16}$$

where λ_1 and λ_2 are hyper-parameters to control the weights of $\mathcal{L}^{IRM}$ and $\mathcal{L}^{Adv}$ .For the adversarial discriminator, the optimization objective is:

$$\mathcal{L}^{A} = \mathcal{L}^{Adv} \tag{17}$$

We train the parameters of the discriminator and the main model alternately until the model converges.

4 EXPERIMENTS

In this section, we validate MIDLG by comparing it with other representative models in a realistic "transaction fraud" complaint dataset on WeChat Finance.

Table 2: Details of the Dataset

Description	Value
Number of Complaints	189,034
Number of Individuals	223,598
Number of subtypes	46
Dimension of Individual Attributes	95
Dimension of Relation Attributes	6

4.1 Dataset

The dataset is collected from a real "transaction fraud" complaint verification scenario in WeChat Finance. In detail, the complaints are extracted from July 15th, 2022, to August 31th, 2022. A complaint record is generated when a user reports to the online complain platform on account of suffering transaction fraud. Taking each complaint as a sample, the input information is its $\mathcal{G} = (V, E, X^v, X^e)$ defined in Sec 2.1, which includes its attribute information of involved individuals and the relations. Detailed information is shown in Table 2.

We divide the dataset according to time to prevent data leakage and test our model stability in a real scenario, meaning that the training data precedes the test data. Specifically, the training set is from July 15th to July 24th, the validation set is from July 25th to July 27th. To better investigate the effect of the model when the data distribution changes, we construct three test sets, called July data(JD), August data(AD), and Manual data(MD). JD is collected from July 28 to July 30 whose distribution is nearly consistent with the training and validation set. AD and MD are sampled from the complaints in August, and the MD is manipulated to increase the distribution, i.e., reducing the frequency of subtypes that appear more frequently in the training set. As shown in Fig6, the subtype distribution shift with respect to the training set is getting more and more drastic in the three test sets. To maintain consistency with reality, we constrain the proportion of positive and negative samples and only alter the distribution of subtypes. The size of training set, validation set, JD, AD, and MD are 98169, 32048, 29018, 4556, and 6603 respectively.

4.2 Baselines

We consider several representative methods for complaint verification, divided into two types: (1) Attribute leveraged only. We use SVM (Suykens and Vandewalle 1999) and MLP as our baselines. However, attributes include some structural features, proposed by experts for convenient manual review. (2) Attribute and structure both are leveraged. GNNs are designed for such graph-related tasks. However, it is full of challenges to leverage the existing GNN into our task directly since complaint verification is a new task. Specifically, the challenges are as follows: 1) Since an individual may appear in different complaints under different identities, we leverage the information of the latest appearance on the baseline methods. 2) Since the edge attributes and different relations existed in our task, we add an MLP in GNN baselines to capture the edge relations for fairness. Based on the above processing, we take two representative GNNs (GCN [15] and GAT [31]) and state-of-the-art GNN model (DAGNN [19]) to demonstrate the superiority of MIDLG model

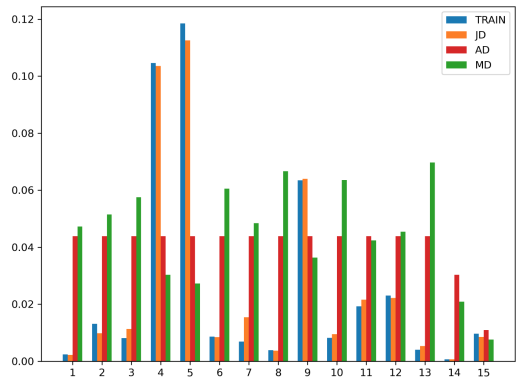

Figure 6: The subtype distribution of the training set and the three test sets(JD, AD, MD)

Furthermore, we design three ablation studies to verify the effect of each part. DLPM only includes dual level propagation part. We add IRM and adversarial module to dual level propagation module separately, named MIDLG$\backslash_{Adv}$ and MIDLG$\backslash_{IRM}$.

4.3 Experiment Settings and Configurations

We present details of our experiment setup and super parameters setup in this section.

4.3.1 Experiment Settings. To conduct the experiments, we construct the N-hop subgraphs by extracting historical information related to the users' identities in complaint relations on node-level representation learning. We adopt the node attributes in the last complaint as the node-level representations uniformly to solve the attribute conflict problem. Specifically, 1) it is hard to load the whole graph into memory once because of the large number of users. We adopt the node sampling method and set the sampled neighbor order N to 2. 2) The unbalanced number of fraud-transaction and normal-transaction complaints urges us to adopt negative sampling on the training dataset for equalizing negative and positive samples. 3) On account of the different scales between the different dimensions of an attribute, we perform the min-max normalization for the node and edge attributes.

4.3.2 Experiment Configurations. Generally, there are many hyperparameters in the model. The Adam optimizer[14] is applied for all models' optimization. For a fair comparison, the hidden dimension of all models is searched in the space of $\{8, 16, 32\}$ and we choose the number of training epochs from the space of $\{500, 700, 1000\}$, learning rate in $\{1e^{-2}, 5e^{-3}, 1e^{-3}, 5e^{-4}, 1e^{-4}\}$, and the coefficient of $\mathcal{L}^{IRM}$ and $\mathcal{L}^{Adv}$ in $\{1.0, 0.5, 0.1, 0.05\}$. The weight decay is fixed with $1e^{-4}$. Then we set the number of propagation layers in GNNs to 2 for both the node-level and super-node-level in our model.Furthermore, we adopt iterative training for the adversarial part and main model. We choose 5:1 among the training ratios of epoch between adversarial module and main model in

Table 3: Results(%) of models on real-world "transaction fraud" complaint verification dataset on WeChat Finance.

Metric	Test Set	SVM	DNN	GNN	GAT	DAGNN	MIDLG
AUC	JD	76.07 ± 0.12	74.97 ± 0.18	74.29 ± 0.36	75.00 ± 0.04	76.05 ± 0.91	**76.67 ± 0.29**
	AD	73.96 ± 0.10	69.25 ± 1.10	73.27 ± 0.54	72.93 ± 0.37	74.01 ± 1.00	**76.67 ± 0.77**
	MD	71.34 ± 0.29	71.92 ± 0.61	70.72 ± 0.40	71.21 ± 0.33	72.16 ± 0.91	**73.71 ± 0.76**
ACC@Top40%	JD	98.48 ± 0.05	98.27 ± 0.06	98.35 ± 0.05	98.32 ± 0.02	98.50 ± 0.21	**98.51 ± 0.09**
	AD	95.20 ± 0.16	95.02 ± 0.24	94.80 ± 0.26	94.62 ± 0.21	95.20 ± 0.44	**96.59 ± 0.43**
	MD	94.76 ± 0.15	94.99 ± 0.30	94.49 ± 0.20	94.67 ± 0.16	95.20 ± 0.39	**96.16 ± 0.32**
ACC@Top60%	JD	97.88 ± 0.03	97.70 ± 0.10	97.71 ± 0.09	97.85 ± 0.03	97.82 ± 0.06	**97.90 ± 0.13**
	AD	93.84 ± 0.04	93.84 ± 0.23	93.84 ± 0.25	93.62 ± 0.15	93.64 ± 0.27	**94.23 ± 0.27**
	MD	94.17 ± 0.07	94.15 ± 0.07	93.84 ± 0.25	93.62 ± 0.15	93.87 ± 0.20	**94.28 ± 0.25**

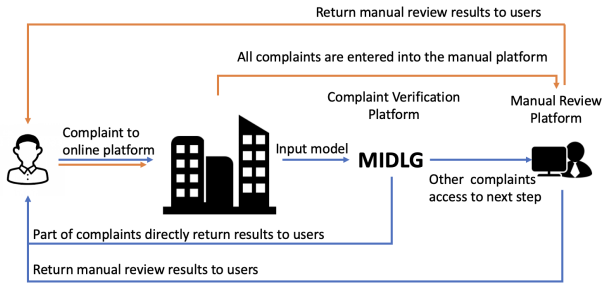

Figure 7: Complaint flow chart of the company. (1)The orange line indicates the manual review process used currently. (2) The blue line shows the whole process under MIDLG. Part of the complaint will be verified by the model.

{1:10, 1:5, 5:1, 10:1}. All models are implemented in Python with pytorch version.

4.4 Metric

Due to complaint verification being a new and complex problem, most companies hire people to review complaints directly, which needs expensive human resources. Considering the difficulty of the task, our goal is to reduce human input through models rather than completely replacing humans. Therefore, we hope the model can tag a subset of complaints very accurately and thus can remove them from manual review, as shown in Fig7.

For practical reasons, companies often want to minimize labor costs, such as reducing labor by 40% or 60%. Since part of the model's output is returned directly to the user, we require the output to be very accurate. To make our metric consistent with the task, we propose a task-oriented metric to only consider the output with high confidence(the output returned directly to the user) as follows:

$$\textbf{ACC@Topk\%} = \frac{C_k}{N_k} \tag{18}$$

We rank the confidence of samples according to the output of the model. N_k indicates the number of samples in the first k percent and C_k means the number of correctly predicted samples in N_k. Due to the imbalance of positive and negative samples in the Tencent WeChat dataset, the metric AUC(the area enclosed by the coordinate axis under the ROC curve) which is widely used to evaluate the effect of the model under unbalanced data is added to comprehensive evaluate our model.

Table 4: Results(%) of models on MD set.

Model	ACC@Top40%	ACC@Top60%	AUC
DLPM	95.56 ± 0.41	94.16 ± 0.14	72.79 ± 0.54
MIDLG$\backslash_{Adv}$	95.94 ± 0.39	94.23 ± 0.13	73.31 ± 0.66
MIDLG$\backslash_{IRM}$	95.83 ± 0.14	94.25 ± 0.05	72.90 ± 0.42
MIDLG	**96.16 ± 0.32**	**94.28 ± 0.25**	**73.71 ± 0.76**

4.5 Main Results

The main results of different models are shown in Table 3, from which we can draw two main conclusions from the experimental outcomes.

Precision Analysis. We observe that the ACC@Topk% of our model is consistently higher than that of traditional machine learning models and GNN-based models in AD and MD. At the same time, AUC metric improves significantly, up to 2.5% difference compared to DAGNN.

Stability Analysis. We validate the performance under distribution changes. The prediction results show that SVM, DNN, GAT and DAGNN show varying degrees of decline in effectiveness when the distribution distance is farther away in the AUC metric especially, while our model achieves almost identical performance in AD and MD, and outperforms other methods by 2-3% in AD and more than 1% in MD. Meanwhile, our model improves significantly on data AD and MD with large distribution changes.

4.6 Ablation Studies

Furthermore, we conduct extensive ablation studies to verify the effectiveness of each module in our model demonstrated in Table 4. To intuitively show the effectiveness of each module, we verify the performance in MD with the most distribution shift. We first demonstrate the significance of the dual level propagation module(DLPM). Also, we added the IRM and Adv modules to MIDLG$\backslash_{SFFLM}$ respectively. The results show that MIDLG has achieved improvements over other models, indicating that each module is effective.

Table 5: Results(%) of models on non-graph dataset.

Model	ACC@Top40%	ACC@Top60%	AUC
SVM	96.71 ± 0.10	96.34 ± 0.04	66.36 ± 0.49
MIDLG	**98.31 ± 0.07**	**96.93 ± 0.98**	**74.20 ± 0.34**

In order to verify the importance of GNNs in the task, we delete the graph feature in JD, and re-run MIDLG and SVM. As shown in Fig5, the AUC and ACC@Topk% have been significantly improved, up to 7.5% improvements in AUC especially. In the future, we hope to manually extract graph features, so graph models is necessary "in transaction fraud" complaint verification.

4.7 Visualization Analysis

The proposed SFFLM aims to forget the specific fraud patterns and thus achieve stability. To intuitively show the effect of SFFLM, we visualize the representation in learned by DLPM and MIDLG on MD in Fig8 via TSNE. Red circles represent fraud samples, and blue circles represent non-fraud samples. It can be observed that the representations learned by the model without "specific fraud" forget learning module are separated on each subtype, as indicated by the yellow triangle. Differently, the representations learned by MIDLG are mixed over different subtypes. Thus SFFLM allows the model to learn the commonalities to distinguish fraud from non-fraud, rather than the specific pattern of one subtype, which can handle the distribution shift under confrontation.

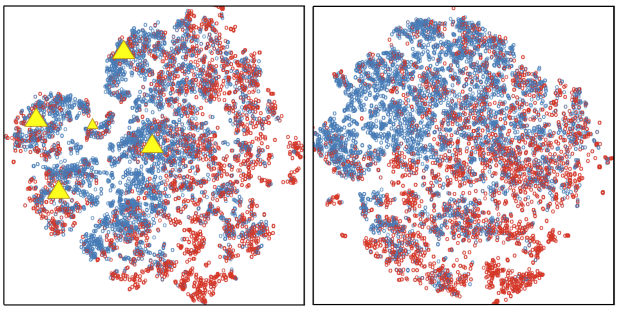

Figure 8: (a) The representations learned by DLPM, which are separate over different subtypes (yellow triangles). (b) The representations learned by MIDLG are mixed.

5 RELATED WORK

In this section, we review traditional graph neural network methods, and the research on model stability. Also, we briefly introduce GNN-based financial fraud detection methods.

Research on Graph Representation Learning. Graph neural networks(GNNs)[9, 11, 15, 19, 24, 31, 37, 39, 42, 43] enrich node representation by aggregating neighbors information. The most central problem of GNN is how to design convolution operator(aggregation function), which is used to construct correlation between nodes relationships. Graph Convolution Network(GCN)[15] is based on the Laplace matrix to construct aggregation function, passing between nodes without parameter learning. GAT[31] adopts attention mechanism to learn importance between neighboring nodes when passing messages. GraphSAGE[11] proposes random neighbor sampling since graphs in reality is always huge. MoNet[24] and MPNN[9] offer people general frameworks for designing GNN-based methods. HAN[34] defines different meta-path to solve the problem of diverse node types and edge types in graphs. However, most graph methods are designed without considering model instability in specific problem scenarios.

Research on Model Stability. Existing methods to improve model stability fall into three main categories: adversarial training techniques, data randomization techniques, and stable learning techniques. Adversarial training techniques[4, 5, 8, 10, 23, 25, 40] add imperceptible perturbations to the samples (e.g., changing the values of a few pixels on the image) and constrain model to adapt to such changes[10, 28, 46]. Data randomization techniques are implemented by doing random transformations on the training data, such as resizing and filling images[38] or adding noise to the training data[20, 32]. Stable learning techniques[2, 20, 29, 30, 44] often base on cause and effect rather than correlations by introducing prior information. LaCIM[30] defines the cause-and-effect graph on the animal picture classification task to eliminate the influence of the environment on the classification results.

Research on Financial Fraud Detection. Financial fraud detection was initially based on machine learning methods, such as SVM[13], Bayesian networks[7], and neural networks[1]. People bring in the graph methods to model complex relational data in fraud detection scenarios[3, 6, 12, 17, 18, 21, 22, 26, 33, 35, 47]. For example, [35] introduce GNN methods to detect money laundering fraud and [26] take dynamics into account in the fraud detection task. [6] study the problem of disguise in fraud. To our knowledge, there are no models that consider stability in the platform-based financial fraud detection tasks.

6 CONCLUSION

In this paper, we propose MIDLG to solve two main challenges in complaint verification:1) the states of an individual in different complaints may be different. 2) fraud ways constantly change requiring models to fit commonality in diverse frauds. For the first challenge, we design dual level graph neural network to capture the node-level information and super-node-level information. To address the instability challenge, we propose the optimization objective of minimizing mutual information from the perspective of causal graphs, then adopt invariant risk minimization and adversarial forgetting methods to remove the effect of time as well as fraud subtypes respectively. Extensive experiments demonstrate that our model achieves SOTA results. In the future, we will apply our model system to immediate fraud detection tasks, which have higher requirements for stability and immediacy.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grant No.U21B2046, No.62202448), the 2022 Tencent Wechat Rhino-Bird Focused Research Program and China Postdoctoral Science Foundation(2022M713208).

REFERENCES

[1] Emin Aleskerov, Bernd Freisleben, and Bharat Rao. 1997. Cardwatch: A neural network based database mining system for credit card fraud detection. In *Proceedings of the IEEE/IAFE 1997 computational intelligence for financial engineering (CIFEr)*. IEEE, 220–226.

[2] Martin Arjovsky, Léon Bottou, Ishaan Gulrajani, and David Lopez-Paz. 2019. Invariant risk minimization. *arXiv preprint arXiv:1907.02893* (2019).

[3] Wendong Bi, Bingbing Xu, Xiaoqian Sun, Zidong Wang, Huawei Shen, and Xueqi Cheng. 2022. Company-as-Tribe: Company Financial Risk Assessment on Tribe-Style Graph with Hierarchical Graph Neural Networks. In *Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*. 2712–2720.

[4] Nicholas Carlini and David Wagner. 2017. Towards evaluating the robustness of neural networks. In *2017 ieee symposium on security and privacy (sp)*. Ieee, 39–57.

[5] Quanyu Dai, Xiao Shen, Liang Zhang, Qiang Li, and Dan Wang. 2019. Adversarial Training Methods for Network Embedding. In *Proceedings of The Web Conference 2019 (WWW '19)*. 329–339.

[6] Yingtong Dou, Zhiwei Liu, Li Sun, Yutong Deng, Hao Peng, and Philip S Yu. 2020. Enhancing graph neural network-based fraud detectors against camouflaged fraudsters. In *Proceedings of the 29th ACM International Conference on Information & Knowledge Management*. 315–324.

[7] Kazuo J Ezawa and Steven W Norton. 1996. Constructing Bayesian networks to predict uncollectible telecommunications accounts. *IEEE Expert* 11, 5 (1996), 45–51.

[8] Fuli Feng, Xiangnan He, Jie Tang, and Tat-Seng Chua. 2019. Graph adversarial training: Dynamically regularizing based on graph structure. *IEEE Transactions on Knowledge and Data Engineering* (2019).

[9] Justin Gilmer, Samuel S Schoenholz, Patrick F Riley, Oriol Vinyals, and George E Dahl. 2017. Neural message passing for quantum chemistry. In *International conference on machine learning*. PMLR, 1263–1272.

[10] Ian J Goodfellow, Jonathon Shlens, and Christian Szegedy. 2014. Explaining and harnessing adversarial examples. *arXiv preprint arXiv:1412.6572* (2014).

[11] Will Hamilton, Zhitao Ying, and Jure Leskovec. 2017. Inductive representation learning on large graphs. *Advances in neural information processing systems* 30 (2017).

[12] Bryan Hooi, Hyun Ah Song, Alex Beutel, Neil Shah, Kijung Shin, and Christos Faloutsos. 2016. Fraudar: Bounding graph fraud in the face of camouflage. In *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining*. 895–904.

[13] Hyun-Chul Kim, Shaoning Pang, Hong-Mo Je, Daijin Kim, and Sung Yang Bang. 2003. Constructing support vector machine ensemble. *Pattern recognition* 36, 12 (2003), 2757–2767.

[14] Diederik P Kingma and Jimmy Ba. 2014. Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980* (2014).

[15] Thomas N Kipf and Max Welling. 2016. Semi-supervised classification with graph convolutional networks. *arXiv preprint arXiv:1609.02907* (2016).

[16] Bo Li, Yifei Shen, Yezhen Wang, Wenzhen Zhu, Dongsheng Li, Kurt Keutzer, and Han Zhao. 2022. Invariant information bottleneck for domain generalization. In *Proceedings of the AAAI Conference on Artificial Intelligence*, Vol. 36. 7399–7407.

[17] Zhao Li, Haishuai Wang, Peng Zhang, Pengrui Hui, Jiaming Huang, Jian Liao, Ji Zhang, and Jiajun Bu. 2021. Live-streaming fraud detection: a heterogeneous graph neural network approach. In *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining*. 3670–3678.

[18] Chen Liang, Ziqi Liu, Bin Liu, Jun Zhou, Xiaolong Li, Shuang Yang, and Yuan Qi. 2019. Uncovering insurance fraud conspiracy with network learning. In *Proceedings of the 42nd international ACM SIGIR conference on research and development in information retrieval*. 1181–1184.

[19] Meng Liu, Hongyang Gao, and Shuiwang Ji. 2020. Towards deeper graph neural networks. In *Proceedings of the 26th ACM SIGKDD international conference on knowledge discovery & data mining*. 338–348.

[20] Xuanqing Liu, Minhao Cheng, Huan Zhang, and Cho-Jui Hsieh. 2018. Towards robust neural networks via random self-ensemble. In *Proceedings of the European Conference on Computer Vision (ECCV)*. 369–385.

[21] Ziqi Liu, Chaochao Chen, Xinxing Yang, Jun Zhou, Xiaolong Li, and Le Song. 2018. Heterogeneous graph neural networks for malicious account detection. In *Proceedings of the 27th ACM international conference on information and knowledge management*. 2077–2085.

[22] Zhiwei Liu, Yingtong Dou, Philip S Yu, Yutong Deng, and Hao Peng. 2020. Alleviating the inconsistency problem of applying graph neural network to fraud detection. In *Proceedings of the 43rd international ACM SIGIR conference on research and development in information retrieval*. 1569–1572.

[23] Aleksander Madry, Aleksandar Makelov, Ludwig Schmidt, Dimitris Tsipras, and Adrian Vladu. 2017. Towards deep learning models resistant to adversarial attacks. *arXiv preprint arXiv:1706.06083* (2017).

[24] Federico Monti, Davide Boscaini, Jonathan Masci, Emanuele Rodola, Jan Svoboda, and Michael M Bronstein. 2017. Geometric deep learning on graphs and manifolds using mixture model cnns. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. 5115–5124.

[25] Nicolas Papernot, Patrick McDaniel, Somesh Jha, Matt Fredrikson, Z Berkay Celik, and Ananthram Swami. 2016. The limitations of deep learning in adversarial settings. In *2016 IEEE European symposium on security and privacy (EuroS&P)*. IEEE, 372–387.

[26] Aldo Pareja, Giacomo Domeniconi, Jie Chen, Tengfei Ma, Toyotaro Suzumura, Hiroki Kanezashi, Tim Kaler, Tao Schardl, and Charles Leiserson. 2020. Evolvegcn: Evolving graph convolutional networks for dynamic graphs. In *Proceedings of the AAAI Conference on Artificial Intelligence*, Vol. 34. 5363–5370.

[27] Ali Lotfi Rezaabad and Sriram Vishwanath. 2020. Learning representations by maximizing mutual information in variational autoencoders. In *2020 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2729–2734.

[28] Ali Shafahi, Mahyar Najibi, Mohammad Amin Ghiasi, Zheng Xu, John Dickerson, Christoph Studer, Larry S Davis, Gavin Taylor, and Tom Goldstein. 2019. Adversarial training for free! *Advances in Neural Information Processing Systems* 32 (2019).

[29] Zheyan Shen, Peng Cui, Jiashuo Liu, Tong Zhang, Bo Li, and Zhitang Chen. 2020. Stable learning via differentiated variable decorrelation. In *Proceedings of the 26th ACM SIGKDD international conference on knowledge discovery & data mining*. 2185–2193.

[30] Xinwei Sun, Botong Wu, Xiangyu Zheng, Chang Liu, Wei Chen, Tao Qin, and Tie-yan Liu. 2020. Latent causal invariant model. *arXiv preprint arXiv:2011.02203* (2020).

[31] Petar Veličković, Guillem Cucurull, Arantxa Casanova, Adriana Romero, Pietro Lio, and Yoshua Bengio. 2017. Graph attention networks. *arXiv preprint arXiv:1710.10903* (2017).

[32] Pascal Vincent, Hugo Larochelle, Yoshua Bengio, and Pierre-Antoine Manzagol. 2008. Extracting and composing robust features with denoising autoencoders. In *Proceedings of the 25th international conference on Machine learning*. 1096–1103.

[33] Daixin Wang, Jianbin Lin, Peng Cui, Quanhui Jia, Zhen Wang, Yanming Fang, Quan Yu, Jun Zhou, Shuang Yang, and Yuan Qi. 2019. A semi-supervised graph attentive network for financial fraud detection. In *2019 IEEE International Conference on Data Mining (ICDM)*. IEEE, 598–607.

[34] Xiao Wang, Houye Ji, Chuan Shi, Bai Wang, Yanfang Ye, Peng Cui, and Philip S Yu. 2019. Heterogeneous graph attention network. In *The world wide web conference*. 2022–2032.

[35] Mark Weber, Jie Chen, Toyotaro Suzumura, Aldo Pareja, Tengfei Ma, Hiroki Kanezashi, Tim Kaler, Charles E Leiserson, and Tao B Schardl. 2018. Scalable graph learning for anti-money laundering: A first look. *arXiv preprint arXiv:1812.00076* (2018).

[36] Lilian Weng. 2019. From gan to wgan. *arXiv preprint arXiv:1904.08994* (2019).

[37] Felix Wu, Amauri Souza, Tianyi Zhang, Christopher Fifty, Tao Yu, and Kilian Weinberger. 2019. Simplifying graph convolutional networks. In *International conference on machine learning*. PMLR, 6861–6871.

[38] Cihang Xie, Jianyu Wang, Zhishuai Zhang, Zhou Ren, and Alan Yuille. 2017. Mitigating adversarial effects through randomization. *arXiv preprint arXiv:1711.01991* (2017).

[39] Bingbing Xu, Keyan Cen, Junjie Huang, Huawei Shen, and Xueqi Cheng. 2020. A survey on graph convolutional neural network. *Chinese Journal of Computers* 43, 5 (2020), 755–780.

[40] Bingbing Xu, Junjie Huang, Liang Hou, Huawei Shen, Jinhua Gao, and Xueqi Cheng. 2020. Label-consistency based graph neural networks for semi-supervised node classification. In *Proceedings of the 43rd International ACM SIGIR conference on research and development in Information Retrieval*. 1897–1900.

[41] Bingbing Xu, Huawei Shen, Qi Cao, Keting Cen, and Xueqi Cheng. 2020. Graph convolutional networks using heat kernel for semi-supervised learning. *arXiv preprint arXiv:2007.16002* (2020).

[42] Bingbing Xu, Huawei Shen, Qi Cao, Yunqi Qiu, and Xueqi Cheng. 2019. Graph wavelet neural network. *arXiv preprint arXiv:1904.07785* (2019).

[43] Keyulu Xu, Chengtao Li, Yonglong Tian, Tomohiro Sonobe, Ken-ichi Kawarabayashi, and Stefanie Jegelka. 2018. Representation learning on graphs with jumping knowledge networks. In *International conference on machine learning*. PMLR, 5453–5462.

[44] Mengyue Yang, Furui Liu, Zhitang Chen, Xinwei Shen, Jianye Hao, and Jun Wang. 2021. CausalVAE: Disentangled representation learning via neural structural causal models. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 9593–9602.

[45] Chuxu Zhang, Dongjin Song, Chao Huang, Ananthram Swami, and Nitesh V Chawla. 2019. Heterogeneous graph neural network. In *Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining*. 793–803.

[46] Dinghuai Zhang, Tianyuan Zhang, Yiping Lu, Zhanxing Zhu, and Bin Dong. 2019. You only propagate once: Accelerating adversarial training via maximal principle. *Advances in Neural Information Processing Systems* 32 (2019).

[47] Shijie Zhang, Hongzhi Yin, Tong Chen, Quoc Viet Nguyen Hung, Zi Huang, and Lizhen Cui. 2020. Gcn-based user representation learning for unifying robust recommendation and fraudster detection. In *Proceedings of the 43rd international ACM SIGIR conference on research and development in information retrieval*. 689–698.