Computer Science and Application 计算机科学与应用, 2026, 16(4), 76-89
Published Online April 2026 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2026.164111

Hans汉斯

基于多关系异构谱图神经网络的财务报表欺诈检测

程福豪

重庆理工大学数学科学学院，重庆

收稿日期：2026年2月28日；录用日期：2026年3月27日；发布日期：2026年4月7日

摘　要

财务报表欺诈严重破坏资本市场的健康运行与资源配置，构建精准高效的欺诈检测模型具有重要的现实意义。随着图神经网络(GNN)的发展，基于企业关联网络的异常检测成为重要研究方向。然而，现有GNN模型多基于同质性假设(即相连节点具有相似特征或标签)，难以有效应对欺诈者为掩盖造假行为而刻意构建的大量异质性伪装连接。同时，传统方法往往忽略了企业间存在的供销、投资等多维复杂的网络关系。针对上述挑战，本文提出了一种基于多关系异构谱图神经网络特征提取的检测框架(M-RHGDF)。该框架首先通过边缘感知模块预测节点间的同质或异质关联，进而将原始的多关系图动态分裂为特定的正负子图。随后，引入基于谱图理论的可调Beta小波图神经网络(BWGNN)，针对不同子图进行特定频段的特征提取，有效分离代表正常模式的低频信号与揭示异常行为的高频信号。最后，通过聚合不同关系网络下的频域表征，实现对欺诈节点的精准分类。本文在经过数据预处理、字段脱敏且无时间依赖性的真实企业关联数据集FDCompCN上进行了详尽评估。实验结果表明，M-RHGDF模型在AUC、GMean、F1-macro及召回率等核心指标上均显著优于现有主流基线模型，充分证明了其在解决异构图欺诈检测问题中的优越性与鲁棒性。

关键词

财务报表，欺诈检测，图神经网络，谱图理论，异质图，特征提取

Financial Statement Fraud Detection Based on Multi-Relational Heterogeneous Spectral Graph Neural Networks

Fuhao Cheng

School of Mathematics and Statistics, Chongqing University of Technology, Chongqing

Received: February 28, 2026; accepted: March 27, 2026; published: April 7, 2026

文章引用: 程福豪. 基于多关系异构谱图神经网络的财务报表欺诈检测[J]. 计算机科学与应用, 2026, 16(4): 76-89.
DOI: 10.12677/csa.2026.164111

Abstract

Financial statement fraud poses a severe threat to the healthy operation and resource allocation of capital markets, making the development of accurate and efficient fraud detection models highly crucial. With the advancement of Graph Neural Networks (GNNs), anomaly detection based on corporate association networks has emerged as a promising research direction. However, most existing GNN models rely on the homophily assumption—which presumes that connected nodes share similar characteristics—and thus struggle to handle the extensive heterophilous connections deliberately forged by fraudsters for camouflage. Furthermore, traditional methods often overlook the multiplex, complex relations among enterprises, such as supply, distribution, and investment links. To tackle these challenges, this paper proposes a Multi-Relation Heterogeneous Graph Detection Framework (M-RHGDF) based on spectral graph feature extraction. Specifically, an edge-aware module is first utilized to predict whether the relations between nodes are homophilous or heterophilous, dynamically splitting the original multi-relation graph into specific positive and negative subgraphs. Subsequently, an adjustable Beta Wavelet Graph Neural Network (BWGNN) grounded in spectral graph theory is introduced to perform frequency-specific feature extraction on different subgraphs, effectively separating low-frequency signals that represent normal patterns from high-frequency signals indicative of anomalous behaviors. Finally, the spectral representations across various relational networks are aggregated to achieve a precise classification of fraudulent nodes. Extensive evaluations are conducted on FDCompCN, a real-world corporate association dataset characterized by rigorous pre-processing, anonymized fields, and temporal independence. Experimental results demonstrate that M-RHGDF significantly outperforms existing mainstream baseline models across core metrics including AUC, GMean, F1-macro, and Recall, thoroughly validating its superiority and robustness in addressing heterophilous graph fraud detection.

Keywords

Financial Statement, Fraud Detection, Graph Neural Network, Spectral Graph Theory, Heterogeneous Graph, Feature Extraction

1. 引言

财务报表欺诈严重威胁资本市场的健康运行与投资者信心。从安然事件到瑞幸咖啡财务造假，此类行为不仅导致涉事企业遭受巨额处罚甚至退市，更破坏了市场资源的有效配置，损害了广大投资者的利益[1] [2]。因此，构建准确、高效的财务报表欺诈检测模型，对于监管机构、审计师、投资者以及公司管理者而言，具有重要的理论价值和现实意义。

早期关于欺诈检测的研究主要依赖于计量经济模型和统计方法。研究者通常将财务报表欺诈视为二元变量，旨在建立欺诈与特定财务指标之间的因果关系。其中，由 Beneish [3]开发的 M-Score 模型和 Dechow 等人[4]开发的 F-Score 模型，通过一系列财务比率来评估公司的欺诈风险，在很长一段时间内被视为该领域的代表性模型。随着机器学习算法的进步和计算能力的提升，研究的重心逐渐从解释性统计模型转向预测性的机器学习模型，以期从海量数据中自动学习欺诈行为的复杂模式。例如，Cecchini 等人[5]使用基于财务比率的支持向量机(SVM)算法，成功识别了其研究样本中 80%的欺诈公司。Perols [6]通

过对比六种机器学习算法，发现逻辑回归和 SVM 在金融欺诈识别任务中表现最佳。除了数值型财务指标，Purda 和 Skillicorn [7]开始探索文本信息在欺诈检测中的应用，他们对财务报告的管理层讨论与分析(MD&A)部分进行文本分析，证明了非结构化文本数据蕴含了丰富的欺诈线索。此后，Bao 等人[8]采用 RusBoost 算法和原始财务变量，Brown 等人[9]引入主题模型分析财务报告的主题内容，Bertomeu 等人[10]采用梯度提升回归树(GBRT)并融合非财务因素，进一步提升了检测性能。这类基于传统机器学习的方法，其优势在于模型相对简单，具有较强的可解释性。然而，它们高度依赖领域知识进行手工特征工程，且其核心假设是样本独立同分布，因此无法捕捉公司之间存在的复杂关联网络，而这恰恰是财务欺诈行为滋生与传播的重要土壤。

金融数据天然具有社会属性，公司通过供应链、股权投资、高管关联等关系构成了复杂的网络结构。图神经网络(GNN)作为一种能够直接处理非结构化图数据的强大工具，为捕捉这种交互关联性提供了新的可能。基于图神经网络的欺诈检测方法依据其对数据的基本假设，可以分为基于同质性假设的方法和基于异质性假设的方法。早期的方法，如 Dou 等人[11]、Liu 等人[12]和 Liu 等人[13]的工作，通常基于同质性假设(Homophily)，即认为相连的节点具有相似的特征或标签，因此在信息聚合时主要采用低通滤波器，以强化这种相似性。然而，现实世界中的欺诈图往往呈现出异质性特征(Heterophily)，即相连节点间的特征或标签存在显著差异。为了隐藏自己，欺诈者会刻意与大量良性实体建立连接，例如垃圾邮件发送者利用正常用户账号进行扩散。这种伪装行为导致相连节点间(欺诈者与良性实体)的特征或标签差异巨大，严重违背了同质性假设。直接应用基于同质性假设的 GNN 会在欺诈节点的表征中引入大量噪声，从而弱化模型的检测性能。

为解决欺诈图中的这种异质性挑战，基于异质性假设的图神经网络方法被提出。解决思路主要有两种：一是通过图结构学习来减少异质连接，增加图的同质性，例如 Suresh 等人[14]的工作；二是设计新型的消息聚合策略，同时建模节点间的同质性与异质性，如 H2-FDetector 通过同时考虑节点间同质性和异质性的信息聚合策略取得了较好的结果。此后，Tang 等人[15]提出的 Beta 小波作为带通滤波器，可以同时提取图中的低频(同质)和高频(异质)信号，进一步提升了欺诈检测的性能。

尽管上述基于图神经网络的方法在处理异质性问题上取得了进展，但现有研究大多集中于单一类型的关系或特定场景。财务报表欺诈涉及投资关系、供销关系等多种关联，构成了典型的多关系异构图。如何在一个统一的框架内，有效处理这种多关系、强异质性的复杂网络结构，同时从谱域角度充分提取不同频段的特征信息，仍是亟待解决的问题。基于此，本文基于谱图理论，总结出一种适用于多关系异构图神经网络的检测范式(M-RHGDF)，并采用可以提取不同频域特征的 BWGNN 模块，对上市公司财务报表欺诈进行检测。通过在真实数据集 FDCompCN 上的实验[16]，旨在验证该方法在处理多关系异质性欺诈网络、提升欺诈样本召回率方面的有效性与优越性。

2. 模型介绍

2.1. 模型框架

本文提出的多关系异构谱图网络检测框架(M-RHGDF)如图 1，采用 BWGNN 模块提取不同频域特征，将其用于具有异质性欺诈图 FDCompCN 上进行节点分类。

M-RHGDF 包含 5 个模块，如图 1 所示，分别是节点嵌入、子图分裂、特征提取、特征聚合、节点分类，其中子图分裂模块内部可细分为两个子模块，分别是关系感知和分裂。

给定多关系图 $\mathcal{G}=\left\{V,X,\mathcal{E}_r\big|_{r=1}^{R},Y\right\}$，首先进入节点嵌入模块，得到节点嵌入特征 x_e，由关系感知子模块进行边类型的预测，即预测连接不同节点的边是异质边 $\mathcal{E}^-$ 还是同质边 $\mathcal{E}^+$，基于此关系类型 r，将整图

$\mathcal{G}$ 分裂为不同的关系整图 $\mathcal{G}_r$ 、关系正子图 $\mathcal{G}_r^+$ 和关系负子图 $\mathcal{G}_r^-$，并与整图 $\mathcal{G}$ 一起进入特征提取模块，针对不同的子图可以设计不同的特征提取网络，以提取相应频段的特征，最后在特征聚合模块中聚合来自不同子图的特征，再利用特征融合模块使聚合在一起的特征进行交互得到最终的节点表征。

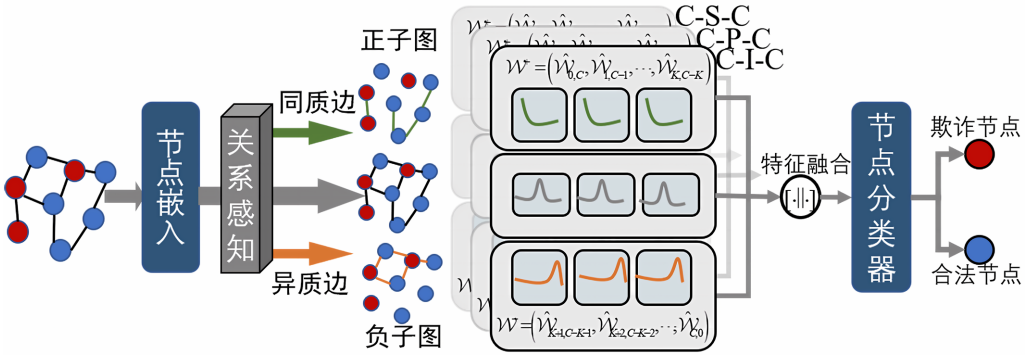

Figure 1. M-RHGDF overall detection framework
图 1. M-RHGDF 整体检测框架

针对 FDCompCN，上述符号中，V 是节点的集合，由 5317 个表示不同上市公司的节点构成；每个节点具有 57 维的特征 $x \in X$ ，x_e 表示节点嵌入特征；$\mathcal{E}_r = \{\mathcal{E}_r^+, \mathcal{E}_r^-\}$ 表示由关系 r 构成的边的集合，共 $R=3$ 种关系，分别是 C-I-C、C-P-C 和 C-S-C；$\mathcal{G}_r = \{V, X, \mathcal{E}_r, Y\}$，表示仅具有关系 r 的关系子图，正子图和负子图也称同质图或异质图，+,– 分别标识了边或图的同质性和异质性。其网络结构如表 1 所示。

Table 1. Models of the modules within the M-RHGDF framework in this paper
表 1. 本文 M-RHGDF 框架中各模块的模型

模块	网络
节点嵌入	Linear
关系感知	MLP
特征提取	BWGNN
特征聚合	Concatenatio [·‖·]
节点分类	MLP

节点嵌入模块可以用一个节点嵌入函数 E 来表示，经过节点嵌入后的特征可表示为 $h = E(x)$，该模型的节点嵌入是面向低维空间的一个线性投影(Linear)，如式(1)，也可以根据需要设计其它类型的模块：

$$h = E(x) = W_x x \tag{1}$$

其中 W_x 可训练的参数矩阵。

子图分裂模块中为了分割原始图，该模型构建了一个二元边分类器来预测每条边的类型。利用源节点 u 和目标节点 v 的特征以及它们的差 $\mathbf{h}_u - \mathbf{h}_v$ 来预测边的类型 ε_{uv}。边分类器由多层感知器(MLP)构建。

$$\begin{aligned} \psi_{uv} &= \tanh\left(W\left[\mathbf{h}_u \,\|\, \mathbf{h}_v \,\|\, \left(\mathbf{h}_u - \mathbf{h}_v\right)\right]\right) \\ \epsilon_{uv} &= \mathrm{SIGN}\left(\psi_{uv}\right) \end{aligned} \tag{2}$$

其中，**h** 是前述的节点嵌入特征。W 是可训练参数矩阵。$[\cdot\|\cdot]$ 是连接运算，将特征进行合并(Concatenation)。SIGN 函数用于将 tanh 的输出转换为二元结果 $\{-1,+1\}$。

根据原始图 $\mathcal{G}$ 中每条边的预测结果 ϵ_{uv}，将其分割为正子图 $\tilde{\mathcal{G}}^{+}$ 和负子图 $\tilde{\mathcal{G}}^{-}$。正子图 $\tilde{\mathcal{G}}^{+}$ 只包含预测的同质边，负子图 $\tilde{\mathcal{G}}^{-}$ 包含预测的异质边。

准确的边缘分类对后续步骤至关重要，它决定了分割子图的质量。为此采用一个辅助损失 $\mathcal{L}_E$ 来训练边分类器，如式(3)所示。该损失是根据构建的训练边缘 $\mathcal{E}_t$ 和预测结果计算得出的。损失函数定义为：

$$\mathcal{L}_E = \frac{1}{|\mathcal{E}_t|}\sum_{e_{uv}\in\mathcal{E}_t}\max\left(0,1-y_{e_{uv}}\psi_{uv}\right) \tag{3}$$

其中，$\mathcal{E}_t$ 是训练集中所有边构成的集合，$y_{e_{uv}}$ 是边 e_{uv} 的标签，如果边缘是同质边，标签值为 1；如果是异质边，标签值为−1。

由于模型需要关注不同类型子图中不同频率的信号，因此需要一个灵活的带通滤波器。而为分裂子图设计合适的图滤波器并非易事，目前的 GNN 主要使用低通滤波器。一些研究提出了通过多项式逼近或 Transformer 学习任意图滤波器的方法，如 BernNet [17]和 Specformer [18]。然而，这些方法并不适用于存在严重类不平衡问题的欺诈检测任务。欺诈节点只占图的一小部分。与高频信号相比，低频信号所占比例更高，经过训练的过滤器可能会优先关注低频信号。

因此，为了灵活地捕捉信号的特定和适当频率，该模型使用带通滤波器来捕捉特定频段，并引入可调节的 Beta 小波图神经网络(BWGNN) [15]。可调节的 Beta 小波使用 Beta 分布作为图的核函数。Beta 小波变换 $\mathcal{W}_{p,q}$ 的定义如式(4)：

$$\mathcal{W}_{p,q} = U\beta^{*}_{p,q}(\Lambda)U^{\mathrm{T}} = \beta^{*}_{p,q}(L) = \frac{(L/2)^{P}(I-L/2)^{q}}{2B(p+1,q+1)} \tag{4}$$

式(4)中，$p,q\in N^{+}$ 和 $B(p+1,q+1)=p!q!/(p+q+1)!$ 是一个常数。$\beta^{*}_{p,q}(w)$ 是一种 Beta 分布概率密度函数的转换，$\beta^{*}_{p,q}(w)=(1/2)\beta_{p,q}(\omega/2)$，$L$ 为图的拉普拉斯矩阵。

$$\beta_{p,q}(w) = \begin{cases}\dfrac{1}{B(p+1,q+1)}w^{p}(1-w)^{q} & \text{if } w\in[0,1]\\ 0 & \text{otherwise}\end{cases} \tag{5}$$

假设 $p+q=C$ 为常数，则会生成 $C+1$ 个 Beta 小波，从而构建变换 $\mathcal{W}$：

$$\mathcal{W} = \left(\mathcal{W}_{0,C},\mathcal{W}_{1,C-1},\cdots,\mathcal{W}_{C,0}\right) \tag{6}$$

通过设置式(7)中的超参数 K，我们可以将 $\mathcal{W}$ 分割为 $\mathcal{W}^{+}$ 和 $\mathcal{W}^{-}$，分别捕捉来自 $\tilde{\mathcal{G}}^{+}$ 和 $\tilde{\mathcal{G}}^{-}$ 的低频和高频信号。预测分裂图上的变换 $\hat{\mathcal{W}}_{p,q}$ 为：

$$\begin{aligned}\hat{\mathcal{W}}_{i,C-i} &= \begin{cases}\beta^{*}_{i,C-i}\left(\tilde{L}^{+}\right) & \text{if } i\in[0,K]\\ \beta^{*}_{i,C-i}\left(\tilde{L}^{-}\right) & \text{if } i\in[K+1,C]\end{cases}\\ \mathcal{W}^{+} &= \left(\hat{\mathcal{W}}_{0,C},\hat{\mathcal{W}}_{1,C-1},\cdots,\hat{\mathcal{W}}_{K,C-K}\right)\\ \mathcal{W}^{-} &= \left(\hat{\mathcal{W}}_{K+1,C-K-1},\hat{\mathcal{W}}_{K+2,C-K-2},\cdots,\hat{\mathcal{W}}_{C,0}\right)\end{aligned} \tag{7}$$

具体来说，式(8)定义了正子图和负子图中节点的聚合表征

$$\begin{aligned}\bar{\mathbf{h}}_i &= \hat{\mathcal{W}}_{i,C-i}(\mathbf{h})\\ \hat{\mathbf{h}}^{+} &= \left[\bar{\mathbf{h}}_0 \| \bar{\mathbf{h}}_1 \| \cdots \| \bar{\mathbf{h}}_K\right]\\ \hat{\mathbf{h}}^{-} &= \left[\bar{\mathbf{h}}_{K+1} \| \bar{\mathbf{h}}_{K+2} \| \cdots \| \bar{\mathbf{h}}_C\right]\\ \hat{\mathbf{h}} &= \sigma\left(W_s\left[\hat{\mathbf{h}}^{+} \| \hat{\mathbf{h}}^{-}\right]\right)\end{aligned} \tag{8}$$

式(8)中的W_s可训练权重矩阵，σ是非线性激活函数。

利用特征提取模块提取特征，在分割原始图形后，正子图表达更多的低频信号，负子图表达更多的高频信号。由于正负两个子图的结构并不完整，分割后的子图不再包含原始图形的所有结构信息。因此，为了增强整体语义，引入类似于卷积神经网络中的 ResNet 的残差连接变体，对原始图采用式(6)的 Beta 小波变换$\mathcal{W}$，并在后续聚合这些特征，使模型更具表现力，完整计算过程如式(9)和(10)。中W_o是一个可训练的权重矩阵。

$$\begin{aligned}\bar{\mathbf{h}}_i^{\circ} &= \mathcal{W}_{i,C-i}(\mathbf{h})\\ \hat{\mathbf{h}}^{\circ} &= \sigma\left(W_o\left[\bar{\mathbf{h}}_0^{\circ} \| \bar{\mathbf{h}}_1^{\circ} \| \cdots \| \bar{\mathbf{h}}_C\right]\right)\end{aligned} \tag{9}$$

特征聚合模块聚合不同关系和类型图的表征能力。对于一个图，节点的最终嵌入$\hat{h}^f$是来自原始图和预测正负子图表示的连接，并带有残余连接，如下，W_t是可训练的权重矩阵。

$$\hat{\mathbf{h}}^f = \left[\hat{\mathbf{h}} \| \hat{\mathbf{h}}^{\circ} \| W_t\mathbf{h}\right] \tag{10}$$

现实世界中的大多数欺诈图都包含多种类型的关系，及多关系图。为简单起见，省略前面公式中关系的表示。学习到每种关系下的表征后，该模型将不同关系下的节点表征聚合起来，构建节点的最终嵌入：

$$\mathbf{h}^f = AGG\left(\hat{\mathbf{h}}^f\big|_{r=1}, \hat{\mathbf{h}}^f\big|_{r=2}, \cdots, \hat{\mathbf{h}}^f\big|_{r=R}\right) \tag{11}$$

该模型使用合并作为聚合函数。这里也可以使用其他聚合函数，包括最大值、平均值、加权参数或注意力机制等。

节点分类模块利用前述模块提取到的图表特征进行节点分类任务，在该模型中节点分类模块采用一个 MLP 将节点映射到一个二元表示并通过 softmax 获得节点欺诈概率。

2.2. 模型训练

我们使用交叉熵损失进行节点分类的训练。给定训练节点集$\mathcal{V}_t$，节点v的最终嵌入为$\mathbf{h}_v^f$和v的标签y_v，损失函数定义如下：

$$\begin{aligned}\mathcal{L}_N &= -\sum_{v\in\mathcal{V}_t}\left[y_v \log\left(p_v\right) + \left(1-y_v\right)\log\left(1-p_v\right)\right]\\ p_v &= \mathrm{softmax}\left(\mathbf{h}_v^f\right)\end{aligned} \tag{12}$$

总体损失综合了边缘分类器和节点分类的损失。边缘分类器和 GNN 是联合训练的，并使用γ来控制两个任务的贡献。

$$\mathcal{L} = \mathcal{L}_N + \gamma\mathcal{L}_E \tag{13}$$

由于欺诈检测中的类不平衡问题，在计算损失时随机抽取了与欺诈节点数量相同的良性节点参与节点分类损失的计算，同样地，随机抽取与异质边数量相同的同质边参与边分类损失的计算。

3. 实验设计

3.1. 数据集与评估指标

本文使用公开的财务欺诈检据集 FDCompCN [16]，用于检测中国上市公司的财务报表欺诈。该数据收集了《中证行业分类 2016 年版》行业分类标准中在上海、深圳和北京证券交易所上市的 5317 家中国上市公司 2020 年至 2023 年间的样本。根据中国公司财务报表中披露的供应商、客户、股东和财务信息构建了一个多关系图谱。该图谱包含 5317 个节点和 10,059 个边，其中公司间投资关系边 C-I-C 具有 8505 个，客户关系边 C-P-C 具有 5944，供应商关系 C-S-C 边具有 6244 个。类别比例如图 2(a)所示，整个数据类别不平衡比约 9:1，图 2(b)为整个数据集的划分情况，类别分布保持一致。

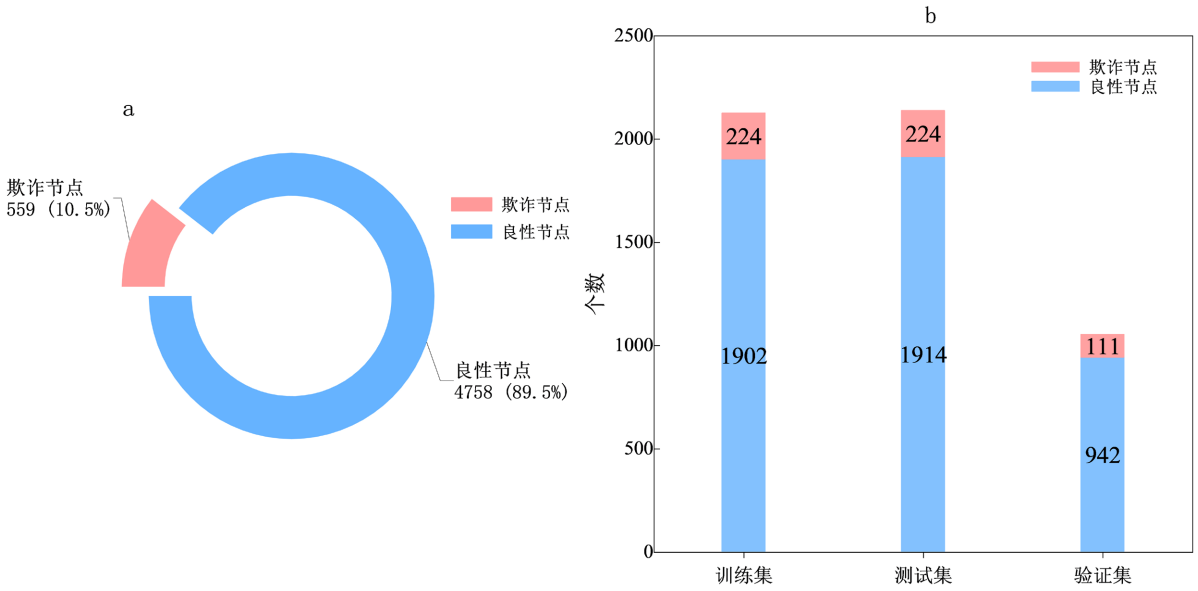

Figure 2. Distribution of data categories
图 2. 数据类别分布情况

为准确衡量欺诈图中与欺诈节点相关的边的异质性程度，本文引入欺诈节点边异质性 $\mathcal{H}_f$ 。由于欺诈节点在图中占比较小，只有约 10%的占比，全局边异质性无法有效反映欺诈节点邻域结构的真实异质程度。因此，我们仅考虑与欺诈节点有关的边中异质边的比例，并定义欺诈异质度 $\mathcal{H}_f$ 如下：

$$\mathcal{H}_f = \frac{\left|\left\{(v,u)\in\mathcal{E}:\left(y_v \neq y_u\right) \text{ and } \left(y_v = 1 \text{ or } y_u = 1\right)\right\}\right|}{\left|\left\{(v,u)\in\mathcal{E}: y_v = 1 \text{ or } y_u = 1\right\}\right|}$$

依据此定义，分别计算各关系子图下的欺诈节点同质性，数据集各项统计结果如表所示。其中同构图表示不区分边的关系类型，统计结果如表 2 显示，3 种关系子图以及它们诱导的同构图的欺诈同质度均处于较低水平(≤12%)。

在欺诈检测研究中，欺诈检测数据集高度不平衡，模型性能的评估需兼顾对少数类(欺诈样本)的识别能力以及整体分类效果。以下常用的几个指标，可以综合评估模型性能：AUC-ROC (AUC)、GMean、F1-macro 和 Recall。

Recall：召回率是一个重要的评价指标，用于衡量模型对所有实际正例(欺诈样本)的正确预测能力，其计算公式如下：

$$\text{Recall} = \frac{TP}{TP + FN} \tag{14}$$

其中，TP (True Positives)为正确识别的欺诈样本数，FN (False Negatives)为被误判为正常的欺诈样本数。

Table 2. Statistics of the FDCompCN
表 2. 欺诈图统计结果

总节点数量	欺诈比例	关系类型	欺诈同质度($1-\mathcal{H}_l$)
5317	10.5%	C-I-C	11.2%
		C-P-C	4.3%
		C-S-C	3.6%
		同构图	8.6%

F1-macro：精确率(Precision)与召回率的调和平均，宏平均 F1 是对每个类别分别计算 F1 后取算术平均，适用于欺诈检测这类不平衡数据集，能够综合评估模型在所有类别上的表现。对于二分类问题，宏平均 F1 定义为：

$$\begin{aligned} F_{Macro} &= \frac{1}{n}\sum_{i=1}^{n} F_1^{(i)} \\ F_1^{(i)} &= \frac{2 \times \text{Precision}^{(i)} \times \text{Recall}^{(i)}}{\text{Precision}^{(i)} + \text{Precision}^{(i)}} \end{aligned} \tag{15}$$

其中第 i 个类别的精确率 $\text{Precision}^{(i)} = TP^{(i)} \Big/ \left(TP^{(i)} + FP^{(i)}\right)$，召回率 $\text{Recall}^{(i)} = TP^{(i)} \Big/ \left(TP^{(i)} + FN^{(i)}\right)$。

AUC (Area under the Receiver Operating Characteristic Curve)是 ROC 曲线下的面积，度量模型在不同阈值下区分正负类的能力。该指标不受分类阈值影响，能全面反映模型的排序性能。AUC 值越接近 1，模型区分欺诈的能力越强。

$$\text{AUC} = \int_0^1 \text{TPR}(t)\,\text{dFPR}(t) \tag{16}$$

其中，$\text{TPR}(t)$ 为阈值 t 下的真正例率(召回率)，$\text{FPR}(t)$ 为假正例率 $\left(FP \Big/ \left(FP + TN\right)\right)$。在实际计算中，通常采用梯形法对离散的 ROC 点进行积分。

GMean 是几何平均(Geometric Mean)，常用于评估类别不平衡任务，同时考虑召回率和特异度(Specificity，对负类的识别)。

$$\text{GMean} = \sqrt{\text{Recall} \times \text{Specificity}} = \sqrt{\frac{TP}{TP + FN} \times \frac{TN}{TN + FP}} \tag{17}$$

3.2. 实验环境

实验的软硬件环境见表 3，硬件方面采用 Intel(R)Core(TM) i9-10850KCPU@3.60GHz，配备 24 GB DDR4 内存。图形计算由 NVIDIA GeForce RTX 3090 显卡(24 GB 显存)提供支持。软件环境基于 Ubuntu 20.04 LTS 操作系统，使用 Python 3.9.13 进行编程，深度学习模型基于 PyTorch 1.12.1 框架构建，并利用 CUDA 11.6 进行 GPU 加速。

参数的设置及其含义见表 4，具体设定为 Beta 小波多项式的阶数 $C = 4$，正负子图不同频段频率分割阶数 $K = 2$，控制边分类损失对整体损失贡献的系数 $\gamma = 0.8$，初始学习率 $lr = 0.002$，权重衰减系数

weight_decay = 6e−05，最大迭代次数为 3000 次，并利用早停机制监控训练过程，连续 100 次迭代，模型在验证集上性能没有提升即停止训练过程，保存训练过程中最优模型。

Table 3. Experimental environment details
表 3. 实验环境详情

软硬件	配置/版本
CPU	Intel(R) Core(TM) i9-10850K @ 3.60 GHz
内存	24 GB DDR4
显卡	NVIDIA GeForce RTX 3090 (24 GB 显存)
操作系统	Ubuntu 20.04 LTS
编程语言	Python 3.9.13
深度学习框架	PyTorch 1.12.1
CUDA 版本	11.6

Table 4. Experimental parameter settings and meanings
表 4. 实验参数设置及其含义

参数名称	参数值	参数含义
Beta 小波多项式阶数(C)	4	控制 Beta 小波滤波器的多项式阶数，决定感受野大小。
频段频率分割阶数(K)	2	决定正负子图在不同频段上的分割粒度，用于提取多频特征。
边分类损失贡献系数(γ)	0.8	平衡边分类损失 $\mathcal{L}_E$ 与节点分类损失 $\mathcal{L}_N$ 在总损失中的权重。
初始学习率 lr	0.002	优化器的初始步长，影响收敛速度与稳定性。
权重衰减系数	6e−05	L2 正则化系数，用于抑制过拟合，提升泛化能力。
最大迭代次数	3000	训练过程允许的最大轮数，确保模型充分收敛。
早停耐心值	100	验证集性能连续 100 次迭代无提升时终止训练，防止过拟合。

4. 实验

4.1. 对比实验

为全面评估所提多关系异构谱图检测框架(M-RHGDF)的有效性，本文在真实的财务报表欺诈检测数据集 FDCompCN 上进行了广泛的对比实验。基线方法涵盖了传统机器学习模型、通用图神经网络、针对异质图优化的图模型以及专用的异常检测图模型。具体的性能表现如表 5 和图 3 所示。

实验结果表明，仅依赖节点特征的 XGBoost 和 MLP 在 AUC (分别为 0.6067 与 0.5732)和 F1-macro 等综合评价指标上表现欠佳。这表明了在高度复杂的金融网络中，单纯依赖孤立的财务指标不足以全面刻画欺诈行为，网络拓扑结构的缺失严重制约了模型的判别能力。然而，当引入经典的通用图神经网络(如 GCN 和 GAT)时，模型的 AUC 指标不仅没有提升，反而下降至 0.5238 和 0.5235，性能甚至不及多层感知机(MLP)。这一反直觉现象的本质在于：传统 GNN 的核心机制是基于同质性假设的低通滤波，倾向

于平滑相连节点的特征。而在真实的财务欺诈网络中，欺诈者为掩饰违规行为，往往会刻意与大量正常公司建立异质性关联。这种高频的异质性结构噪声在低通滤波器的作用下被放大，导致节点表征严重混淆(过度平滑)，从而使通用 GNN 在欺诈检测任务中失效。

Table 5. Comparative experiments of different models
表 5. 不同模型的对比实验

Metric	AUC	GMean	F1-macro	Recall
XGBoost	0.6067	0.6089	0.5036	0.5786
MLP	0.5732	0.5437	0.4245	0.5776
---	---	---	---	---
GCN	0.5238	0.5467	0.4057	0.6274
GAT	0.5235	0.5201	0.3769	0.6215
GPRGNN	0.6678	0.6124	0.5047	0.5769
FAGCN	0.6816	0.6350	0.5137	0.625
---	---	---	---	---
H^2-FDetector	0.6483	0.6178	0.5004	0.6347
BWGNN	0.6293	0.5897	0.5017	0.5386
---	---	---	---	---
M-RHGDF	0.6867	0.6437	0.5201	0.6469

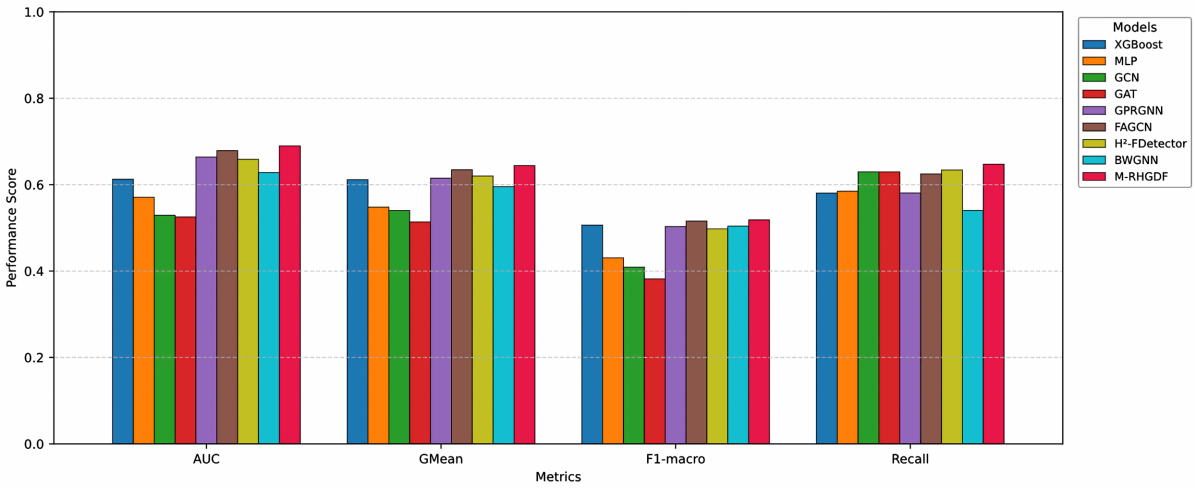

Figure 3. Model performance comparison
图 3. 模型性能对比

相较于传统 GNN，专门针对异质图设计的模型(如 GPRGNN [19]、FAGCN [20]和 H^2-FDetector)性能有显著回升。例如，FAGCN 和 H^2-FDetector 的 AUC 分别达到了 0.6816 和 0.6483，并且在召回率(Recall)上表现优异(分别为 0.6250 和 0.6347)。这说明自适应地融合高频信号和利用异质性边缘，能够有效剥离

欺诈节点伪装，挖掘出更多潜在的财务造假样本。纯 BWGNN 模型虽然引入了 Beta 小波以捕获高频异常信号，但由于缺乏对复杂图结构的显式解耦，其 AUC 仅为 0.6293，性能提升受限。

本文提出的 M-RHGDF 模型在所有评估指标上均取得了不错的性能：AUC 达到 0.6867，GMean 为 0.6437，F1-macro 提升至 0.5201，召回率高达 0.6469。相较于表现最好的基线模型 FAGCN，M-RHGDF 的 AUC 和召回率分别实现了约 0.75%和 3.5%的提升。同时，如表 2 所示，各关系子图的欺诈节点边同质度分别为：C-I-C 关系 11.2%、C-P-C 关系 4.3%、C-S-C 关系 3.6%。这些数值表明，欺诈节点在绝大多数情况下与正常节点相连，形成了极强的异质性结构，即欺诈者倾向于通过伪装行为隐藏自身，大量连接正常节点以逃避检测。这种高度异质性的图结构对基于同质性假设的传统 GNN 构成了严峻挑战。从表 5 的实验结果可以看出，GCN 和 GAT 在 FDCompCN 上的 AUC 仅为 0.5238 和 0.5235，显著低于其他方法，原因在于它们本质上执行低通滤波，聚合邻居信息时会受到大量正常节点特征的干扰，从而淹没了欺诈节点的异常信号。

相比之下，本文提出的 M-RHGDF 在 FDCompCN 上取得了最佳性能，这与其对图异质性的针对性设计密切相关。首先，M-RHGDF 通过边分类器将原始图拆分为多关系正(同质边)负(异质边)子图，使得高频信号(主要集中于异质边上)得以在负子图中被单独提取。其次，采用可调 Beta 小波作为带通滤波器，能够灵活聚焦于不同频段，尤其在高异质性关系(如 C-P-C 和 C-S-C)上，滤波器可有效放大高频能量，从而突出欺诈节点与正常节点之间的差异。最后，多关系聚合机制进一步融合了不同关系下的异质信号，使模型能够综合利用各关系中的伪装线索。因此，M-RHGDF 在高度异质的 FDCompCN 数据集上展现出最强的欺诈识别能力，验证了其设计对于处理欺诈图中异质性的有效性。

4.2. 消融实验

为进一步验证 M-RHGDF 框架中各个核心组件的有效性，本文设计了针对图分裂模块、频域滤波器类型以及多关系融合机制的三组消融实验。实验结果详见表 6。

Table 6. Ablation experiments using different modules
表 6. 采用不同模块的消融实验

Metric	AUC	GMean	F1-macro	Recall
pure-BWGNN	0.6293	0.5897	0.5017	0.5386
M-RHGDF + GCN	0.5532	0.5348	0.4203	0.571
M-RHGDF + BernNet	0.6023	0.5779	0.4650	0.5832
M-RHGDF*	0.5528	0.5364	0.4378	0.5462
M-RHGDF	0.6867	0.6437	0.5201	0.6469

当移除子图分裂模块，使框架退化为纯 Beta 小波图网络(pure-BWGNN)时，模型的 AUC 大幅下降了 8.36% (从 0.6867 降至 0.6293)。这有力地表明在进行谱特征提取之前，预先通过边缘分类器分离同质与异质子图是极其关键的步骤。未经结构净化的原始图中混杂了大量的伪装连接，直接进行波普变换容易导致特征模糊，而显式的图分裂为后续的定向频段提取提供了清晰的结构基础。

本文探讨了不同图滤波器对检测性能的影响。当采用 GCN 替换 BWGNN 模块(M-RHGDF + GCN)时，模型退化为纯低通滤波机制，导致 AUC 断崖式下跌至 0.5532。这再次印证了高频信号在揭示异常节点中的核心地位。另一方面，采用可学习任意频段的 BernNet (M-RHGDF + BernNet)时，AUC 回升至 0.6031，

但仍明显低于本文最终方案。其原因在于欺诈检测数据集存在严重的类别不平衡(欺诈节点占比极小)。在这种数据分布下,无约束的可学习滤波器(如 BernNet)在优化过程中极易被占主导地位的正常节点“带偏”,错误地将权重向低频区间倾斜。相反，M-RHGDF 中采用的可调 Beta 小波能够以先验的数学形式稳定地提取并强化高频特征，对不平衡数据表现出更强的鲁棒性。

实验中的 M-RHGDF*变体移除了对多关系子图的处理，将供应链、股权投资等多种关系混合为单一的同质化连接网络。结果显示，这种忽略关系异质性的做法导致 AUC 骤降至 0.5528。这表明，在复杂的商业环境中，不同类型的业务关联(如 C-I-C、C-P-C、C-S-C)蕴含着截然不同的语义维度。M-RHGDF 通过保留并聚合这些多维关系网络的信息，显著丰富了节点表征的层次，提升了模型对隐蔽财务欺诈手段的判别能力。

4.3. 案例分析

为更直观地揭示 M-RHGDF 模型的实际检测机制，本节从 FDCompCN 测试集中筛选出被基线模型漏判、但被 M-RHGDF 成功识别的典型欺诈节点，进行详细的案例分析。本文从中选取具有伪装策略的代表性案例，以阐明图结构信息在欺诈检测中不可替代的作用。

枢纽型伪装节点#3717 是一个在企业关联网络中具有显著伪装性的欺诈公司，它通过 C-I-C (投资关系)和 C-P-C (客户关系)两种关系与 10 个邻居节点建立了紧密联系。如图 4 所示，其邻域呈现出典型的“混合伪装”结构——10 个直接邻居中有 5 个为正常公司、5 个为欺诈公司。该节点的局部异质性比例为 50%，远高于全图平均水平(约 10.5%)，表明该区域是欺诈行为高度集聚的“灰色地带”。

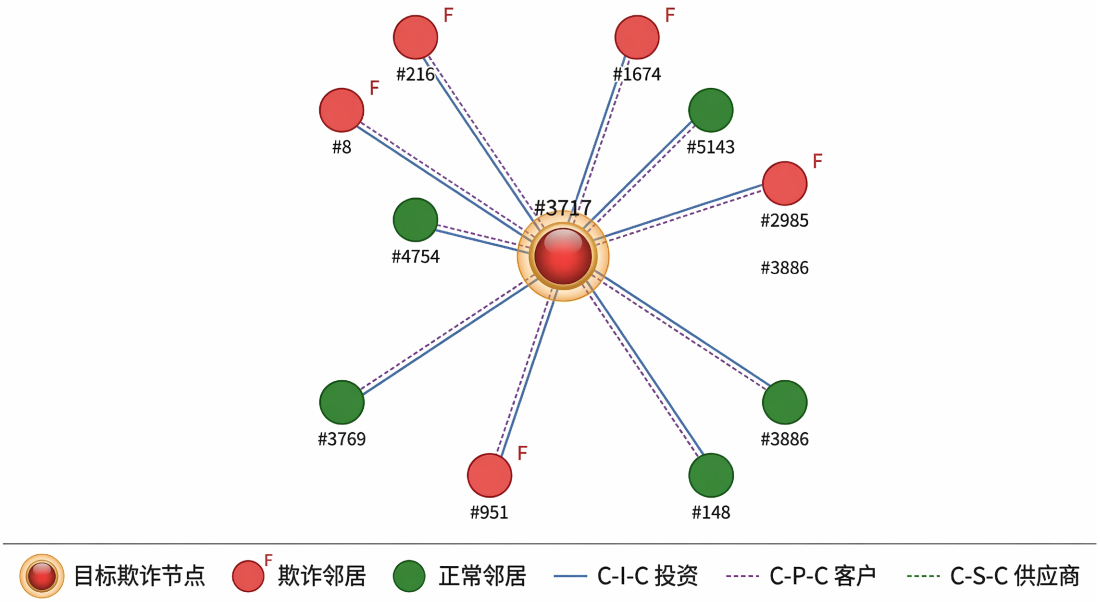

Figure 4. Local neighborhood structure of node #3717
图 4. 节点#3717 局部邻居结构

从特征空间的角度分析，节点#3717 在多个关键财务指标上展现出显著的“特征压缩”现象：其中 F55 和 F51 两个判别性最强的特征维度均为 0.00，而其正常邻居在这两个维度上的均值分别高达 0.60。这种“关键维度清零”的特征模式使得该节点在纯特征空间中与正常公司的分布高度重叠。如表 5 所示，MLP、GCN 和 GAT 三个基线模型给出的欺诈概率分别仅为 0.3638、0.4006 和 0.4174，均未达到 0.5 的

判别阈值，导致其被一致误判为正常公司。

然而，M-RHGDF 模型通过其核心设计成功识别了该节点。具体而言：首先，边缘感知模块预测出该节点连接的多条异质边，将其邻域分裂为正子图(同质连接)和负子图(异质连接)。在负子图中，该节点与 5 个正常邻居之间的异质边被显式提取。随后，可调 Beta 小波在负子图上有效放大了高频信号——尽管节点#3717 自身特征“伪装”良好，但它与正常邻居之间在 F55、F51、F40 等维度上 0.37~0.60 的特征差异构成了强烈的高频异常信号。此外，多关系聚合机制将 C-I-C 和 C-P-C 两种关系网络中提取的异质信号进行融合，进一步增强了模型对该欺诈节点的判别信度，最终给出 0.72 的欺诈概率，实现了成功检出。

5. 实验总结

本文聚焦于资本市场中财务报表欺诈行为的隐蔽性与复杂性，指出现有基于同质性假设的图神经网络在处理该类任务时存在严重的高频信号损失问题。为此，本文提出并验证了 M-RHGDF 多关系异构谱图检测框架。通过在经过严格预处理、字段含义隐去且剔除了时间依赖特性的 FDCompCN 公开数据集上进行广泛实验，得出以下结论：第一，欺诈节点刻意构建的伪装连接导致图网络呈现强异质性，传统的低通 GNN 模型在此场景下往往失效；第二，采用边缘分类器对图结构进行同质与异质拆解，是提升谱图网络特征提取纯度的有效前提；第三，结合多关系聚合机制与 Beta 小波带通滤波技术，能够兼顾多维度的商业语义与特定频段的异常突变，在类别极度不平衡的环境下依然具备强大的识别能力。综合而言，M-RHGDF 框架不仅在各项检测指标上实现了基线模型的超越，也为后续基于图谱理论的金融风控研究提供了参考。

参考文献

[1] Duan, W., Hu, N. and Xue, F. (2024) The Information Content of Financial Statement Fraud Risk: An Ensemble Learning Approach. *Decision Support Systems*, **182**, Article 114231. https://doi.org/10.1016/j.dss.2024.114231

[2] Shahana, T., Lavanya, V. and Bhat, A.R. (2023) State of the Art in Financial Statement Fraud Detection: A Systematic Review. *Technological Forecasting and Social Change*, **192**, Article 122527. https://doi.org/10.1016/j.techfore.2023.122527

[3] Beneish, M.D. (1999) Incentives and Penalties Related to Earnings Overstatements That Violate GAAP. *The Accounting Review*, **74**, 425-457. https://doi.org/10.2308/accr.1999.74.4.425

[4] Dechow, P.M., Ge, W., Larson, C.R. and Sloan, R.G. (2011) Predicting Material Accounting Misstatements. *Contemporary Accounting Research*, **28**, 17-82. https://doi.org/10.1111/j.1911-3846.2010.01041.x

[5] Cecchini, M., Aytug, H., Koehler, G.J. and Pathak, P. (2010) Detecting Management Fraud in Public Companies. *Management Science*, **56**, 1146-1160. https://doi.org/10.1287/mnsc.1100.1174

[6] Perols, J. (2011) Financial Statement Fraud Detection: An Analysis of Statistical and Machine Learning Algorithms. *Auditing*: *A Journal of Practice & Theory*, **30**, 19-50. https://doi.org/10.2308/ajpt-50009

[7] Purda, L. and Skillicorn, D. (2014) Accounting Variables, Deception, and a Bag of Words: Assessing the Tools of Fraud Detection. *Contemporary Accounting Research*, **32**, 1193-1223. https://doi.org/10.1111/1911-3846.12089

[8] Bao, Y., Ke, B., Li, B., Yu, Y.J. and Zhang, J. (2020) Detecting Accounting Fraud in Publicly Traded U.S. Firms Using a Machine Learning Approach. *Journal of Accounting Research*, **58**, 199-235. https://doi.org/10.1111/1475-679x.12292

[9] Brown, N.C., Crowley, R.M. and Elliott, W.B. (2020) What Are You Saying? Using *Topic* to Detect Financial Misreporting. *Journal of Accounting Research*, **58**, 237-291. https://doi.org/10.1111/1475-679x.12294

[10] Bertomeu, J., Cheynel, E., Floyd, E. and Pan, W. (2020) Using Machine Learning to Detect Misstatements. *Review of Accounting Studies*, **26**, 468-519. https://doi.org/10.1007/s11142-020-09563-8

[11] Dou, Y., Liu, Z., Sun, L., Deng, Y., Peng, H. and Yu, P.S. (2020) Enhancing Graph Neural Network-Based Fraud Detectors against Camouflaged Fraudsters. *Proceedings of the* 29*th ACM International Conference on Information & Knowledge Management*, Virtual Event, 19-23 October 2020, 315-324. https://doi.org/10.1145/3340531.3411903

[12] Liu, Y., Ao, X., Qin, Z., Chi, J., Feng, J., Yang, H., *et al*. (2021) Pick and Choose: A GNN-Based Imbalanced Learning Approach for Fraud Detection. *Proceedings of the Web Conference* 2021, Ljubljana, 19-23 April 2021, 3168-3177.

https://doi.org/10.1145/3442381.3449989

[13] Liu, Z., Dou, Y., Yu, P.S., Deng, Y. and Peng, H. (2020) Alleviating the Inconsistency Problem of Applying Graph Neural Network to Fraud Detection. *Proceedings of the* 43*rd International ACM SIGIR Conference on Research and Development in Information Retrieval*, Virtual Event, 25-30 July 2020, 1569-1572. https://doi.org/10.1145/3397271.3401253

[14] Suresh, S., Budde, V., Neville, J., Li, P. and Ma, J. (2021) Breaking the Limit of Graph Neural Networks by Improving the Assortativity of Graphs with Local Mixing Patterns. *Proceedings of the* 27*th ACM SIGKDD Conference on Knowledge Discovery & Data Mining*, Virtual Event, 14-18 August 2021, 1541-1551. https://doi.org/10.1145/3447548.3467373

[15] Tang, J., Li, J., Gao, Z., *et al*. (2022) Rethinking Graph Neural Networks for Anomaly Detection. *Proceedings of the* 39*th International Conference on Machine Learning*, Baltimore, 21076-21089. https://proceedings.mlr.press/v162/tang22b/tang22b.pdf

[16] Wu, B., Yao, X., Zhang, B., Chao, K. and Li, Y. (2023) SplitGNN: Spectral Graph Neural Network for Fraud Detection against Heterophily. *Proceedings of the* 32*nd ACM International Conference on Information and Knowledge Management*, Birmingham, 21-25 October 2023, 2737-2746. https://doi.org/10.1145/3583780.3615067

[17] Bo, D., Shi, C., Wang, L., *et al*. (2022) Specformer: Spectral Graph Neural Networks Meet Transformers. *The Eleventh International Conference on Learning Representations*, Kigali, 1-5 May 2023. https://openreview.net/forum?id=0pdSt3oyJa1

[18] He, M., Wei, Z., Huang, Z., *et al*. (2021) BernNet: Learning Arbitrary Graph Spectral Filters via Bernstein Approximation. *Proceedings of the* 35*th International Conference on Neural Information Processing Systems*, Red Hook, 6-14 December 2021, 14239-14251.

[19] Chien, E., Peng, J., Li, P., *et al*. (2021) Adaptive Universal Generalized PageRank Graph Neural Network. *International Conference on Learning Representations*. https://openreview.net/forum?id=n6jl7fLxrP

[20] Bo, D., Wang, X., Shi, C. and Shen, H. (2021) Beyond Low-Frequency Information in Graph Convolutional Networks. *Proceedings of the AAAI Conference on Artificial Intelligence*, **35**, 3950-3957. https://doi.org/10.1609/aaai.v35i5.16514