计算机科学
COMPUTER SCIENCE

基于图神经网络的银行交易欺诈检测方法

秦忠飘, 周亚同, 李哲

引用本文

秦忠飘, 周亚同, 李哲. 基于图神经网络的银行交易欺诈检测方法[J]. 计算机科学, 2024, 51(11A): 240200024-8.

QIN Zhongpiao, ZHOU Yatong, LI Zhe. Bank Transaction Fraud Detection Method Based on Graph Neural Network [J]. Computer Science, 2024, 51(11A): 240200024-8.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.240200024

基于图神经网络的银行交易欺诈检测方法

秦忠飘[1]　周亚同[1]　李　哲[2]
1 河北工业大学电子信息工程学院　天津 300401
2 河北工业大学数字经济产业研究院　石家庄 050000
(2678282628@qq.com)

摘　要　随着电子支付的迅速发展,欺诈问题日益增多。传统欺诈检测方法受限于规则和特征工程,难以捕获复杂的交易模式。相反,基于图的方法虽然强调了数据的关系性,但通常忽略了特征工程的重要性。为了解决这个问题,提出一种端到端的电信诈骗检测方法——基于图神经网络的银行交易欺诈检测方法。该方法设计了一个针对图数据的特征工程,并利用融合模型对其进行训练。具体来说,使用过采样和设置节点权重的方式对银行交易数据进行不平衡处理,然后采用改进的自适应相似度边和节点度权重融合策略,构建用户交易图数据并挖掘交易节点间的潜在关联信息,最后综合局部特征和全局特征通过模型融合来弥补单一分类器的不足。实验结果表明,在广西玉林银行的交易数据中,所提模型对于交易欺诈数据的检测在F1分数、召回率、AUC 3个指标上相比GraphSAGE分别提升1.65,1.36,4.2个百分点,图数据构建时间缩短了80%左右,与其他主流的检测算法相比也取得了更高的检测精度。

关键词:银行交易欺诈检测;特征工程;不平衡处理;相似度边;图神经网络
中图分类号　TP181;F830.49

Bank Transaction Fraud Detection Method Based on Graph Neural Network

QIN Zhongpiao[1],ZHOU Yatong[1] and LI Zhe[2]
1 School of Electronics and Information Engineering,Hebei University of Technology,Tianjin 300401,China
2 Institute of Digital Economy Industry Research,Hebei University of Technology,Shijiazhuang 050000,China

Abstract　With the rapid development of electronic payments,the fraud problem is increasing. Limited by rule and feature engineering,traditional fraud detection methods are difficult to capture complex transaction patterns. Conversely,graph-based methods often downplay the significance of feature engineering while highlighting the relational aspect of the data. In addition,few studies have examined the application of graph methods in the field of fraud detection for specific bank transaction data. To address this problem,this paper proposes an end-to-end telecom fraud detection method,a fraud detection method for banking transactions based on graph neural networks. The proposed method designs a feature engineering for graph models and trains it using a fusion model. Specifically,oversampling and node weighting are used to address the unbalanced dataset. Next,a user transaction graph model is built utilizing an adaptive similarity edge and node degree weight fusion technique to construct a user transaction graph model and mine potential correlation information between transaction nodes. Furthermore,model fusion is employed to merge local and global variables to overcome the constraints of separate classifiers. Experimental results show that in Guangxi Yulin Bank transaction data,the proposed model for the detection of transaction fraud data on the three indicators of F1 score,recall rate,and AUC is improved by 1.65%,1.36% and 4.2% compared to GraphSAGE,respectively. The model also achieves a reduction of approximately 80% in training time. In comparison to other mainstream detection algorithms,it exhibits higher detection accuracy.

Keywords　Bank transaction fraud detection,Feature engineering,Unbalanced treatment,Similarity edge,Graph neural network

近年来,随着通信技术的快速发展,电信诈骗一直危害不断[1-2],欺诈手段也不断升级,对个人和社会造成日益严重的损失。电信欺诈在实施过程中会在网络上留下各种各样的痕迹,例如在利用电子支付骗取用户资金时,资金流转记录就成为一种电信欺诈的有效痕迹。银行作为用户交易信息的拥有者,在近几年的电信欺诈中,同样遭受到了巨大的经济损失和信任危机。因此研究和开发高效准确的欺诈检测方法对于保护金融系统的安全和维护客户权益具有重要意义。

研究欺诈检测的方法主要可以分为两种。一种是基于规则和统计模型的传统欺诈检测方法。例如:Hila[3]通过构建

基金项目:京津冀基础研究合作专项(J210008,21JCZXJC00170,H2021202008);内蒙古自治区纪检监察大数据实验室开放课题(IMDBD202105)
This work was supported by the Special Foundation for Beijing Tianjin Hebei Basic Research Cooperation (J210008,21JCZXJC00170,H2021202008) and Inner Mongolia Discipline Inspection and Supervision Big Data Laboratory(IMDBD202105).
通信作者:周亚同(zyt@hebut.edu.cn)

专家系统的方式，结合相关专业知识和数据挖掘技术进行欺诈行为的检测。随着科技的不断发展，大规模高维度的交易数据逐渐成为欺诈检测的主要研究对象，同时也暴露出传统方法计算效率低下、费时费力等缺点。因此，出现了一种新的基于机器学习的欺诈检测方法。该类方法可以通过历史的交易记录自动学习其中的欺诈特征，节省大量人工操作，例如，Elm 等[4]在客户数据库中提取出 9 个特征并使用多层感知器进行欺诈检测；Zheng 等[5]根据受害者的大额转账信息，提出一种基于生成对抗网络的模型，来检测每次大额转账时欺诈的概率；Yang 等[6]针对用户话单数据提出了一种基于 3D 卷积神经网络的算法；Yang 等[7]对伪造语音进行研究，采用深度卷积神经网络（Convolutional Neural Network，CNN）进行检测。尽管上述方法取得一定的成果，但它们只关注局部特征，而忽略了数据中潜在的复杂结构。

随着图理论的不断发展，机器学习可以作用到非欧几里得的数据上[8-10]。此外，电信网络所特有的拓扑结构，给欺诈检测带来了新的研究方向。Zhang 等[11]将用户通信关系转化为有向图，通过图卷积模块进行通信欺诈行为的捕捉。Liu 等[12]考虑节点属性提出一种基于注意力的图表示学习模型，并取得了良好的效果。目前图神经网络模型应用在金融欺诈[13-14]、网络欺诈[15]、跨域异常检测[16-17]任务中均取得了较好的性能。尽管如此，在欺诈检测领域仍存在以下挑战。

1）数据不平衡：在真实世界中，正常合法的交易或事件数量远远超过欺诈的数量，因此数据集中欺诈案例的数量相对较少。这种不平衡性会对训练模型产生影响，使得模型更倾向于检测样本数较多的类别，在罕见类别的检测上表现不佳。

2）欺诈伪装：缺少交易用户信息，在构建图数据时，节点多为无特征点；欺诈人员伪装自己，通过与正常用户交易，蒙蔽图模型的信息迭代，掩盖欺诈特征。

3）图数据构建时间长：因图数据结构复杂、局部连接性、不定大小、样本不均衡等各种原因，图数据结构的计算和构建过程相对耗时。

为了解决上述问题，本文提出一种基于图神经网络的银行交易欺诈检测（Bank Transaction Fraud Detection Method Based on Graph Neural Network，BTFD-GNN）模型。通过加入过采样和节点权重方法，使模型在训练过程中更注重少数样本的权重；为了识别欺诈行为，提出了一种基于欺诈领域知识的自适应边构建方法。该方法利用余弦相似度确定节点之间的边，以最大化连通子图和最小化平均度为目标确定边的阈值。同时，设计了一种节点度权重方法，以充分挖掘节点间潜在的欺诈关系；最后对 Graph Sample and Aggregated（GraphSAGE）[18]和 Graph Attention Network（GAT）[19]两种图神经网络模型的结果进行集成，以更好地捕捉到欺诈特征，提高泛化能力。基于所提方法进行实验，并与现有方法进行对比分析，证明了本文方法具有较好的性能。

1 图概念

图结构是一种描述实体之间关系的数据结构。在图中，节点表示实体，具有特征和属性，特征是节点的向量表示，属性包括标签、权重、度数等[20-21]。边表示实体之间的关联关系，附带权重、方向和类型等属性信息[22]。

在图的研究过程中，一般将图符号表示为 $G=(V,E,\boldsymbol{A},\boldsymbol{D},\boldsymbol{H},Y)$。其中，$V$ 表示节点的集合，即 $V=\{v_1,v_2,\cdots,v_s\}$，v_i 表示节点；E 表示边的集合，即 $E=\{e_1,e_2,\cdots,e_s\}$；e_i 表示边，其中 e_i 表示两个节点 v_{j_i} 和 v_{k_i} 的连接，即 $e_i=(v_{j_i},v_{k_i})\in E$，$v_{j_i},v_{k_i}\in V$；$\boldsymbol{A}$ 表示图 G 的邻接矩阵，是大小为 $s\times s$ 的方阵，其中 s 表示节点个数；在邻接矩阵 $\boldsymbol{A}$ 中存在元素 a_{ij}，表示节点 v_i 和 v_j 之间的边关系，$a_{ij}=1$ 表示节点 v_i 和 v_j 之间存在边关系，否则为 0[23]；$\boldsymbol{D}$ 表示图 G 的度矩阵，是表示节点度数的对角矩阵，一个节点的度表示为该节点与其他节点相连接的数量[24]。在度矩阵中，

$$\begin{cases}\boldsymbol{D}[i][j]=0, & i\neq j\\ \boldsymbol{D}[i][j]=d(i), & i=j\end{cases} \tag{1}$$

其中，$d(i)$表示节点 v_i 的度数；$\boldsymbol{H}$ 表示节点的特征矩阵，$\boldsymbol{H}=\{\boldsymbol{h}_1,\boldsymbol{h}_2,\cdots,\boldsymbol{h}_s\}$，每个节点 $v_i(1\leqslant i\leqslant s)$均对应一个维度为 d 的特征向量 $\boldsymbol{h}_i\in\boldsymbol{H}$；$Y$ 表示节点的标签信息集合，$Y=\{y_1,y_2,\cdots,y_s\}$，其中 $\boldsymbol{y}_i$ 表示节点 v_i 的标签，正常用户标签为 1，欺诈用户标签为 0。

2 BTFD-GNN 模型设计

2.1 总体思路

针对银行交易欺诈检测问题，本文提出的 BTFD-GNN 模型的流程图如图 1 所示，可分为 3 个模块：特征提取模块、图构建模块和模型训练模块。下面分别介绍这 3 个模块的具体实现。

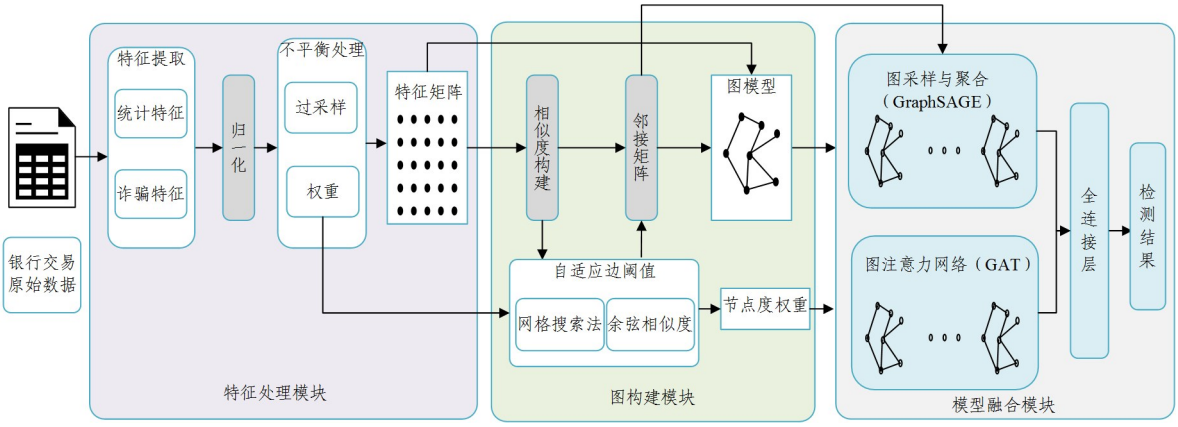


图 1 BTFD-GNN 流程图

Fig. 1 BTFD-GNN flowchart

2.2 特征提取模块

特征工程可以降低模型的复杂度，提高训练速度，在机器学习中扮演着重要角色。本研究设计与实现了如下特征提取模块，为下游模型训练奠定基础。

1）数据格式统一：本文使用的数据集包含 8 家银行的数据，为确保数据格式的一致性，将所有数据中的交易日期、交易金额、余额、交易类型等信息统一处理为元数据 D，其中包含日期、借方发生额、贷方发生额、摘要，以便于对银行交易数据进行后续分析。

2）特征提取：本文从统计特征和欺诈特征两个方面提取特征。统计特征包括借方发生额，贷方发生额的最大值、最小值、平均值等，以揭示用户在交易中的一般趋势。提取节点 v 在维度 n 上的对应统计特征，表示为：

$$h^n_{v,f}=f(D^n_v) \tag{2}$$

其中，函数 $f(\cdot)$ 为对元数据 D 进行统计特征采集的函数集合 F 中的一个元素，集合 F 中包括对数据进行统计特征提取的 sum(·)，max(·)，min(·)等元素，对节点 v 所提取出的 n 维统计特征表示为：

$$\boldsymbol{h}^n_{v,f}=(h^1_{v,f},h^2_{v,f_2},\cdots,h^n_{v,f_i}),\ \text{where}\ f_i\in F \tag{3}$$

欺诈特征包括试探性交易、转账类次数、转账占比等，用于发现欺诈策略和行为模式，其对应的特征表示为：

$$h^m_{v,fr}=fr(D^m_v) \tag{4}$$

其中，函数 $fr(\cdot)$ 为对元数据 D 进行欺诈特征采集的函数集合 Fr 中一个元素，集合 Fr 中包括上述欺诈特征的表示函数。该方式对节点 v 所提取出的 m 维统计特征表示为：

$$\boldsymbol{h}^m_{v,fr}=(f^1_{v,fr_1},f^2_{v,fr_2},\cdots,f^m_{v,fr_i}),\text{where}\ fr_i\in Fr \tag{5}$$

对应的特征矩阵表示为：

$$\boldsymbol{H}=\begin{bmatrix} h^1_{v_1,f_1} & h^1_{v_1,fr_1} & \cdots & \cdots & h^n_{v_1,f_{|F|}} & h^m_{v_1,fr_{|Fr|}} \\ h^1_{v_2,f_1} & h^1_{v_2,fr_1} & \cdots & \cdots & h^n_{v_2,f_{|F|}} & h^N_{v_2,fr_{|Fr|}} \\ \vdots & \vdots & h^i_{v,f} & h^i_{v,fr} & \vdots & \vdots \\ h^1_{v_s,f_1} & h^1_{v_s,fr_1} & \cdots & \cdots & h^n_{v_s,f_{|F|}} & h^m_{v_s,fr_{|Fr|}} \end{bmatrix}\in\mathbb{R}^{s\times d} \tag{6}$$

其中，$d=m+n$，最终提取特征在本文 4.2 节中展示。完成特征提取后对正负样本分别进行均值补充的异常值空缺值处理，提高模型的鲁棒性和准确性。

3）归一化处理：为了消除特征之间存在数量级差异，如用户的交易次数 40 与最大交易金额 40 000 在数量级上的差距非常大，导致模型过于关注较大数值特征的问题，本文将数量级压缩到－1 到 1 之间。根据特征的类型，本文选择了不同的归一化方法，包括最小-最大缩放、标准缩放、最大绝对值缩放和鲁棒性缩放等。根据特征类型选择不同的归一化处理方式，如表 1 所列。

表 1 归一化标准

Table 1 Normalization standards

特征类型	归一化方法
均值特征	标准缩放
标准差特征	标准缩放
最小最大值特征	最小-最大缩放
中位数特征	鲁棒性缩放
比例特征	标准缩放
计数特征	最小-最大缩放

4）不平衡处理：考虑到实际样本存在极不平衡问题，采用 1∶1 采样可能会出现过拟合现象，本文选择 1∶5 的采样比例，在平衡样本分布与保持数据多样性之间折中。之后对过采样后的节点进行权重处理，按比例对少数样本添加权重，权重 w 定义为：

$$w=\frac{N_{\text{majority}}}{N_{\text{oversampled}}} \tag{7}$$

其中，N_{minority} 表示少数类别标签的样本数量，$N_{\text{oversampled}}$ 表示过采样后的样本数量。通过上述方式，分两步对数据的不平衡进行处理，改善模型在少数类别数据上的检测性能，特征矩阵 $\boldsymbol{H}$ 转换成 $\boldsymbol{H}'=[h^{k\prime}_{v_1,f},h^{k\prime}_{v_1,fr},\cdots]$。

经过以上操作流程，得到特征矩阵，为后续的图构建和模型训练奠定数据基础。

2.3 图构建模块

鉴于目前欺诈的隐蔽性，本文采用节点相似度的方式进行边的构建，挖掘隐藏在交易特征中的欺诈信息，利用网格搜索法找到合适的相似度阈值，并结合银行数据背景提出节点度权重概念，输出邻接矩阵作为边权值。

首先，创建一个空的图对象 G，将特征矩阵加载到图中的每个节点上，然后计算所有节点特征间的相似度，作为边的权重保存在图中，构成图数据。常用的相似度度量方法包括欧氏距离[25]和余弦相似度[26]。余弦相似度度量向量间夹角的余弦值，可以更好地度量高维稀疏向量之间的相似性，更适合用于欺诈检测中的不平衡数据，因此本文以余弦相似度作为相似度度量指标。节点 v_i，v_j 之间的距离计算式如式(8)所示：

$$D(v_i,v_j)=\frac{\boldsymbol{h}_i\cdot\boldsymbol{h}_j}{\|\boldsymbol{h}_i\|\times\|\boldsymbol{h}_j\|} \tag{8}$$

根据式(8)定义节点之间的相似性，表示为：$Sim(v_i,v_j)=1-D(v_i,v_j)$。目前图中所有节点之间均存在连接边关系，即使是正负样本间也存在连接边的噪声情况，因此选择边阈值显得极为关键。为了确保图的连通性并降低计算复杂度，本研究采用网格搜索法来探究不同相似度阈值以寻求最佳解。在该方法中，首先创建一个副本图，去除在新阈值下权重低于阈值的边，并计算剩余图中最大连通分量的大小和平均节点度。最后，选择最大连通分量尺寸最大且平均节点度最小的阈值作为最优阈值。找到最优阈值后，将其应用于原始图中，移除权重低于阈值的边，完成图数据的构建。

为了进一步丰富节点表征，引入节点度权重 DW。节点度权重包含了节点的原始权重 w 和邻居节点的权重加权平均，通过这种方式关注到用户节点的密集成度，帮助模型更全面地捕捉节点在社交网络中的特征和行为。公式表达为：

$$DW(v_i)=w_i+\frac{1}{\boldsymbol{D}(v_i)}\sum_{v_j\in\mathcal{N}(v_i)}w_j\cdot Sim(v_i,v_j) \tag{9}$$

其中，w_i 代表节点 v_i 的原始权重，$\mathcal{N}(v_i)$ 表示节点 v_i 的邻居节点集合，$\boldsymbol{D}(v_i)$ 表示节点 v_i 的度。

基于上面流程，将数据集划分为训练、验证和测试子集，然后对每个子集构建数据子图。

总结来说，本节提出了一种基于相似度图的方法来表示欺诈检测中的高维稀疏数据，解决了欺诈伪装问题，并实现了图数据中边的降噪。这种方法有助于凸显与目标任务相关的信息，并且在特征工程阶段结合领域知识对图数据进行了构建，避免在图神经网络模型的训练阶段尝试不同阈值图数据

模型构建的时间，为后续的图神经网络模型提供更好的输入。

2.4 模型融合模块

从节点特征的局部信息和全局信息出发，本节将详细介绍针对欺诈检测任务的融合图神经网络模型。该模型结合GraphSAGE和GAT两种图卷积模型，由3层网络构成。

GraphSAGE层：用于捕捉局部邻域信息，通过对相邻节点的特征进行聚合，以及对相邻节点的均匀随机采样和均值池化进行聚合，学习当前节点的新特征表示。

$$\boldsymbol{h}_i^{(1)}=\sigma(\boldsymbol{W}_1\cdot[\boldsymbol{h}_i^{(0)}\parallel\{\boldsymbol{h}_u^{(0)},\forall u\in\mathcal{N}(v_i)\}]) \tag{10}$$

其中，$\boldsymbol{h}_i^{(1)}$是节点i在第一层的新特征表示，σ是激活函数，$\boldsymbol{W}_1$表示权重矩阵，$\boldsymbol{h}_u^{(0)}$是邻居节点u在第零层的特征表示，$[\cdot\parallel\cdot]$表示拼接操作，表示对节点i所有邻居节点聚合后与其特征$\boldsymbol{h}_i^{(0)}$一起进行更新。

GAT层：负责从全局角度捕捉连接关系，采用自注意力机制对所有邻居节点进行加权聚合，使模型能够自适应地确定各个邻居节点对当前节点的重要性，注意力权重和当前节点的新特征表示如下：

$$a_{i,u}=\frac{\exp(LeakyReLU(a^{\mathrm{T}}[W_2\cdot h_i^{(1)}\parallel W_2\cdot h_u^{(1)}])+\boldsymbol{DW}(v_i))}{\sum_{w\in\mathcal{N}(v_i)}\exp(LeakyReLU(\vec{a}^{\mathrm{T}}[W_2\cdot h_i^{(1)}\parallel W_2\cdot h_w^{(1)}])+\boldsymbol{DW}(v_i))} \tag{11}$$

$$\boldsymbol{h}_i^{(2)}=\sigma(\sum_{u\in\mathcal{N}(v_i)}\alpha_{u,v}\cdot(W_2\cdot\boldsymbol{h}_u^1)) \tag{12}$$

其中，$\boldsymbol{a}^{\mathrm{T}}$表示GAT层的注意力权重向量，$LeakyReLU(\cdot)$是激活函数，$\boldsymbol{W}_2$表示GAT层的权重矩阵。在对节点$i$和邻居节点$u$进行线性变换后拼接，通过注意力权重向量映射为实数，经过激活函数后，再进行归一化得到两个节点之间的注意力权重，最后进行节点的特征聚合。

全连接层：经过GraphSAGE和GAT两个图卷积层之后，将学到的节点特征进行拼接，利用全连接层得到最终的输出结果。

$$output=\sigma(\boldsymbol{W}_3\cdot[h_v^{(1)}\parallel h_v^{(2)}]+\boldsymbol{b}) \tag{13}$$

其中，$\boldsymbol{W}_3$是全连接层权重矩阵，$\boldsymbol{b}$是偏置向量。

通过融合GraphSAGE和GAT两种GNN模型，BTFD-GNN模型能更好地学习节点之间的关系，从而提高欺诈检测的准确性。

3 实验与结果分析

3.1 数据集描述

本实验所使用的数据集来自广西玉林银行交易欺诈检测项目，该数据集是由广西玉林公安提供，包含了8家银行的欺诈嫌疑人真实交易数据和少量正常用户的交易数据，其中诈骗用户1460人，正常用户29人。正常样本数量较少的原因主要有3点。首先，欺诈用户的行为更具有研究价值。在欺诈检测领域，研究人员通常更加关注于识别欺诈特征和行为，因此对欺诈样本的需求较大。其次，由于银行对用户信息的严格保护，公安机关更容易获取诈骗用户的交易数据。这一因素使得诈骗样本相对容易获取，进而影响了正常样本数量的相对稀缺性。最后，在实际应用中数据常常呈不平衡分布，这对于改进算法学习如何区分欺诈交易与正常交易具有一定的促进作用。本数据涵盖了借方发生额、贷方发生额、余额、摘要等用户信息，如图2所示，按照特征工程提取出的特征如表2所列。

广西****银行对账明细

网点号：1111111　　起止日期：2021-06-03至2021-12-03　　币种：CNY|人民币

账号：12345678　　户名：*****

日期	账号序列号	户名	币种	借方发生额	贷方发生额	余额	交易对手账号	交易对手名称	摘要
2021-09-29	1	*****	CNY	0.00	200.00	200.00	#####	0	微信零钱提现,微信零钱提现,网联支付
2021-10-09	1	*****	CNY	0.00	49,999.00	50,199.00	000000000	###	超网贷记来帐入账,,超级网银-转入
2021-10-09	1	*****	CNY	0.00	49,999.00	100,198.00	000000000	###	超网贷记来帐入账,,超级网银-转入
2021-10-09	1	*****	CNY	0.00	49,999.00	150,197.00	000000000	###	超网贷记来帐入账,,超级网银-转入
2021-10-09	1	*****	CNY	0.00	49,999.00	200,196.00	000000000	###	超网贷记来帐入账,,超级网银-转入
2021-10-09	1	*****	CNY	35,733.00	0.00	164,463.00	11111111	！！！	超网跨行转账,手机转账,超级网银记账-转出
2021-10-09	1	*****	CNY	10,001.00	0.00	154,462.00	22222222	aaa	超网跨行转账,手机转账,超级网银记账-转出

图2 原始数据展示

Fig. 2 Raw data display

表2 特征展示

Table 2 Feature display

变量	特征
日期	num_trade_days,num_trade_months,monthly_count,daily_count,total_trades,avg_daily_trades,avg_monthly_trades
借方发生额	num_lt_1,outAccouts_mean,outAccouts_std,outAccouts_min,outAccouts_max,outAccouts_median,dayInTimes_outAcc_max,dayInTimes_outAcc_min,dayInTimes_outAcc_std,dayInTimes_outAcc_mean,dayInTimes_outAcc_50,n_100_out_accouts,zhanbi_100_out
贷方发生额	incomeAccins_mean,incomeAccins_std,incomeAccins_min,incomeAccins_max,incomeAccins_median,dayInTimes_income_max,dayInTimes_income_min
摘要	zhanbi_jiefang,dayInTimes_jiefang_zhuanzhanbi_max,dayInTimes_jiefang_zhuanzhanbi_mean,jiefang_zhuan_max,jiefang_zhuan_mean,dayInTimes_huofang_zhuanzhanbi_max,dayInTimes_huofang_zhuanzhanbi_mean,huofang_zhuan_max,huofang_zhuan_mean

阈值选择和图数据的构建时间如表3所列，可以看出，余弦相似度最佳阈值为0.7，对应最大连通子图为1752，且较小平均节点度为1052.93，图数据构建时间为89.02 s。按照8∶1∶1的比例划分训练集、验证集、测试集后，数据集维度如表4所列，通过图构建模块得到的3个数据子图如图3所示。

表3　阈值信息以及图构建时间

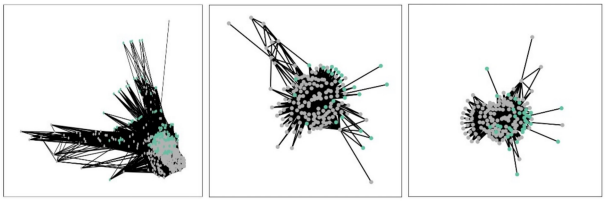
Table 3　Threshold information and graph construction time

阈值	最大连通子图	平均节点度	图构建时间
0.600	1752	1285.048	89.02
0.650	1752	1178.341	
0.700	1752	1052.927	
0.750	1751	911.169	
0.800	1751	759.932	
0.850	1746	594.611	
0.900	1719	400.661	
0.950	1629	174.698	

表4　银行交易数据子集维度展示

Table 4　Dimension display of bank transaction data subsets

变量	节点数	节点特征维度	边数
训练集 train	1401	50	596068
验证集 val	175	50	8934
测试集 test	176	50	8451



(a)训练集　(b)验证集　(c)测试集

注：灰色：欺诈用户；绿色：正常用户。

图3　银行交易数据展示

Fig. 3　Bank transaction data display

3.2　实验设置

3.2.1　实验环境

本实验所有实验基于Pytorch框架，使用PyTorch Geometric库进行图数据的保存以及图神经网络的搭建，采用NVIDIA GeForce RTX 3090进行模型训练。

3.2.2　评价指标

在欺诈检测中，最重要的是识别出欺诈用户即召回率(Recall)，同时也要防止模型过于激进，将正常误判为欺诈的情况即精确率(Precision)。F_1值是这两个指标的综合考量，计算式如下：

$$F_1=\frac{2\times precison\times recall}{precison+recall} \tag{14}$$

此外，AUC(ROC曲线下的面积)适合在数据不平衡的情况下评估模型性能。因此使用召回率、F1和AUC作为评价指标来衡量模型性能。

3.2.3　模型训练超参数

为了优化模型性能，提高泛化能力，在实验进行前，需要对其中的超参数进行选择。根据相关论文和实验经验，本文选择表5中的27组超参数进行多次实验后，选取AUC平均值最高的一组。根据表5所列，在超参数组合{隐藏层大小为128，隐藏层数量为1，学习率为0.001}时，AUC score取值最高为0.8949。

3.3　对比方法

为了验证本文所提模型的有效性，将其与以下模型进行对比。其中SVM使用未进行平衡处理的原始数据进行实验，GCN，GIN，GraphSAGE，GAT，PC-GNN，BW-GNN，BTFD-GNN均在本文图数据构建后的子图基础上进行实验，最后两种GNN模型使用强化学习方式利用邻域采样器构建图数据，进行图数据构建时间的对比。

Support Vector Machine(SVM)[27]：一种线性分类器，根据监督学习对数据进行二值分类。

GCN[28]：一种图卷积的GNN模型。

Graph Isomorphism Network(GIN)[29]：一种捕捉节点特征相互作用的GCN模型。

GraphSAGE：聚合邻居节点的GNN模型。

GAT：一种注意力机制的GNN模型。

BW-GNN[30]：基于小波变换的GNN模型。

PC-GNN[31]：一种标签平衡采样器的GNN模型。

Augmented-GNN[32]：一种强化学习进行图数据构建的GNN模型。

CARE-GNN[33]：对抗伪装欺诈的GNN模型。

表5　超参数组合以及得分情况

Table 5　Hyperparameter combinations and scores

隐藏层大小	隐藏层数量	学习率	*AUC*
32	1	0.001	0.8883
		0.005	0.8902
		0.010	0.8620
	2	0.001	0.8373
		0.005	0.8407
		0.010	0.8570
	3	0.001	0.7576
		0.005	0.7622
		0.010	0.7547
64	1	0.001	0.8732
		0.005	0.8877
		0.010	0.8571
	2	0.001	0.8122
		0.005	0.8172
		0.010	0.8503
	3	0.001	0.7807
		0.005	0.7532
		0.010	0.7668
128	1	0.001	**0.8949**
		0.005	0.8675
		0.010	0.8139
	2	0.001	0.8367
		0.005	0.8672
		0.010	0.8557
	3	0.001	0.8006
		0.005	0.8133
		0.010	0.7997

3.4　性能评估

图4展示了GCN，GIN，GraphSAGE，GAT，PC-GNN，BW-GNN，CARE-GNN，BTFD-GNN训练过程中的F_1，recall以及AUC变化曲线。可以看出，经过80轮迭代后，BTFD-GNN模型展现出了更好的性能，相较于其他模型，在3个指标上获得了更高的得分。同时，在整个训练过程中，随着训练轮数的增加，BTFD-GNN模型的性能稳步上升，并逐渐趋于稳定。其他模型如GIN可能由于局部最小值、不稳定梯度更新等，在训练中性能会出现上下波动的情况，也随着轮数增加

逐渐趋于稳定。表 6 列出了对比实验结果得分和模型训练时间。

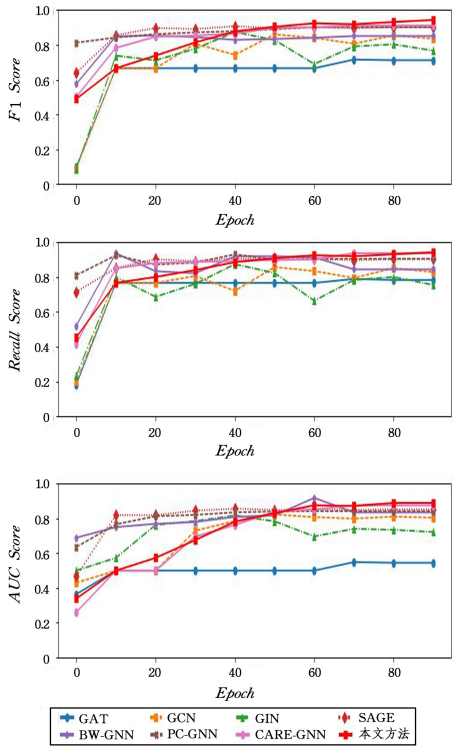


图 4 训练过程中的 F1, recall, AUC 变化曲线

Fig. 4 F1, recall, and AUC variation curves during training

表 6 不同模型下的欺诈检测结果性能比较

Table 6 Performance comparison of fraud detection results of different models

变量	F_1	*Recall*	*AUC*	训练时间
SVM	0.9217	1.0000	0.5000	0.2320
GCN	0.8319	0.8438	0.7360	0.6515
GIN	0.8283	0.8233	0.7872	0.3998
GraphSAGE	0.9065	0.9097	0.8469	**0.3485**
GAT	0.8314	0.8500	0.7468	0.8449
PC-GNN	0.9019	0.9057	0.8417	0.4122
BW-GNN	0.8512	0.8449	0.8344	1.5422
CARE-GNN	0.9115	0.9295	0.8751	0.7289
BTFD-GNN	**0.9230**	0.9233	**0.8889**	0.9148

由表 6 所列数据可以得出以下结论：

1)平衡处理表现：对比 SVM, PC-GNN, BW-GNN 和 BTFD-GNN 的结果，尽管 BTFD-GNN 在 Recall 指标上略低 AUC 一些，但其整体性能仍优于 SVM, PC-GNN 和 BW-GNN，在 AUC 方面具有突出表现。SVM 由于缺乏不平衡处理，对少数样本的识别效果不佳；PC-GNN 相比 GCN 在 AUC 上提升 10.57%，说明标签平衡采样器对不平衡数据有着显著效果；BW-GNN 相比 GCN 在 AUC 上提升 9.84%，说明该方法对不平衡数据有着显著效果，但与本文提出的 BTFD-GNN 方法相比，在应对不平衡数据上略逊一筹。

2)注意力机制的影响：相比 GCN, GraphSAGE, GAT 和 GIN 模型，BTFD-GNN 在欺诈检测任务上有良好的表现，说明了所提模型的自适应相似度边构建策略在深入挖掘潜在联系方面发挥了重要作用，相比 GraphSAGE 模型在 F_1, *Recall* 和 *AUC* 上分别提升了 1.7%, 1.56%和 4.2%，说明添加注意力机制在不平衡的欺诈检测任务中可以更好地注意到少数样本，但由于注意力机制的参数众多，在训练时间上有所欠缺。同样对比 BTFD-GNN 模型与 GAT 可以看出，二者在训练时间上相差不多。

图神经网络的模型训练时间一般分为两个部分，一是图数据构建时间，二是模型训练时间。表 6 列出了图模型的训练时间，下面对图数据构建时间进行讨论。

表 7 列出了强化学习方式下的阈值、*F1*, *AUC*, *Loss* 以及图构建时间，表示 CARE-GNN 和 Augmented-GNN 的两种方式对经过特征矩阵进行强化学习选择最优阈值构建图数据的部分，可以看出阈值为 0.5 时，*Loss* 最低，其对应的 F_1, *Recall* 和 *AUC* 为 0.9180, 0.9333, 0.9138，时间为 432.62 s。对比表 3 的 89.02 s，可以看出 BTFD-GNN 的图构建时间约为强化学习方式选择阈值进行图构建时间的 1/5，原因是强化学习模型对应阈值的 0.5，表示从 0 到 0.5 进行 5 次图模型构建和训练的时间，时间复杂度表示为 $O(\theta - min\_threshold) * (V+E)$)，而 BTFD-GNN 模型的时间复杂度表示为 $O(V+E)$。最后 Augmented-GNN 和 CAER-GNN 两个模型比基础 GCN 在各个指标上分别均提升了 6%以上，这也说明两种强化学习方式在检测结果上具有良好表现。

表 7 强化学习方式下的阈值信息以及图构建时间

Table 7 Threshold information and graph construction time in reinforcement learning

阈值	*F1*	*AUC*	*Loss*	图构建时间/s
0.1	0.9216	0.8792	0.4593	
0.2	0.9216	0.8368	0.4590	
0.3	0.9216	0.5000	0.4590	
0.4	0.9216	0.8932	0.4218	
0.5	0.9180	**0.9138**	**0.3476**	432.62
0.6	0.9183	0.8900	0.3842	
0.7	0.9235	0.8996	0.3717	
0.8	0.9252	0.9047	0.3686	
0.9	0.9216	0.8875	0.4045	

图 5 给出了 BTFD-GNN 模型在训练集和验证集上的得分情况，以评估其拟合能力和泛化能力。

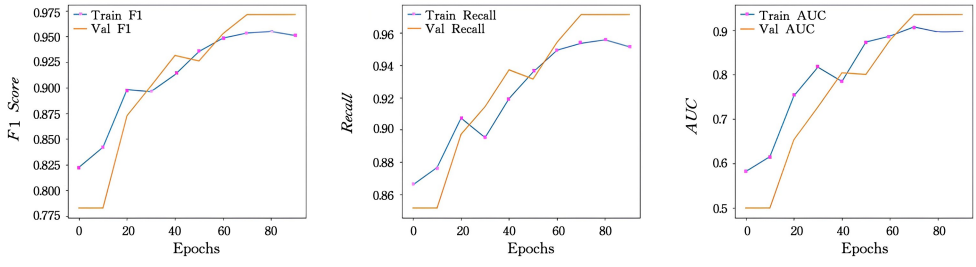
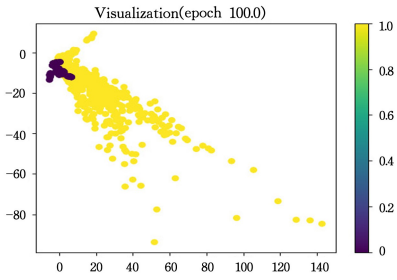


图 5 BTFD-GNN 训练、验证得分情况

Fig. 5 BTFD-GNN training and verification scores

横轴表示训练轮数(epoch)，可以观察到训练集和验证集的得分曲线相互交错，这表明模型在训练过程中存在噪声影响，原因可能是在图构建模块中存在正负样本间互相连接的噪声边情况。但是随着训练的进行，训练集和验证集的得分逐渐提高，这说明该模型是具备较好的拟合能力和泛化能力。图 6 给出了模型训练后得到的正负样本节点分布。可以看出，正常样本的节点聚集在零点附近，说明数据存在不平衡性，模型更倾向于学习多数样本，反映在图中的分布和正常用户有明显区别，这也表明模型对于欺诈用户与正常用户的分类也比较成功。



注：黄色代表欺诈用户；黑色代表正常用户。

图 6　模型测试集分类情况

Fig. 6　Classification of model test sets

结束语　本文致力于解决欺诈检测中的样本不平衡和欺诈挖掘问题。总体而言，在特征提取部分，使用过采样和节点度权重策略，使模型能够更好地关注少数类别样本；在图构建模块，采用自适应边构建和节点度权重方法，有效挖掘节点间的潜在欺诈关系，缩短图数据构建时间；在模型融合部分，通过两个模型的融合，关注节点的局部特征和全局特征。最后与多种机器学习经典模型进行对比，证明了本文所提模型的有效性，为相关领域的研究和应用提供有价值的参考。

未来的研究可以从以下几个方面进行拓展：首先，可以进一步探索更多的特征工程方法和模型结构，以提升欺诈检测的性能；其次，可以考虑引入更多的数据预处理和增强方法，以进一步优化数据的表示和模型的训练过程；此外，可以尝试将其他领域的知识和技术应用于欺诈检测任务，以探索更多的创新解决方案。

参 考 文 献

[1] BECKER R A, VOLINSKY C, WILKS A R. Fraud Detection in Telecommunications: History and Lessons Learned [J]. Technometrics, 2010, 52(1): 20-33.

[2] BARSON P, FIELD S, DAVEY N, et al. The detection of fraud in mobile phone networks [J]. Neural Network World, 1996, 6(4): 477-484.

[3] HILAS C S. Designing an expert system for fraud detection in private telecommunications networks [J]. Expert Systems with Applications, 2009, 36(9): 11559-69.

[4] ELMI A H, IBRAHIM S, SALLEHUDDIN R. Detecting SIM Box Fraud Using Neural Network[C]// Proceedings of the IT Convergence and Security. 2012.

[5] ZHENG Y J, ZHOU X H, SHENG W G, et al. Generative adversarial network based telecom fraud detection at the receiving bank [J]. Neural Networks, 2018, 102: 78-86.

[6] YANG H B, MA Y C, LI J L. Telecommunication Fraud Identification System Based on Convolutional neural network [J]. Telecommunications Technology, 2019, (6): 60-63, 68.

[7] YANG H T, WANG H P, CHU X T, et al. Fake speech detection based on deep Convolutional neural network [J]. Police Technology, 2022, 190(1): 3336.

[8] LIU S, JI X, LIU C, et al. Extended resource allocation index for link prediction of complex network [J]. Physica A: Statistical Mechanics and its Applications, 2017, 479: 174-183.

[9] ZHENG Q Z, XU P F. Structure Learning of Gaussian Graphical Models with Latent Variables Based on Adaptive Penalties [J]. Journal of Jilin University (Scinence Edition), 2023, 61(5): 1056-1062.

[10] WEST D B. Introduction to graph theory [M]. Prentice hall Upper Saddle River, 2001.

[11] ZHANG J J, TANG Y C, JI S Y, et al, A telecom fraud identification method based on graph neural network [J]. Electronics Science Technology and Application, 2021, 47(6): 25-29, 34.

[12] LIU M, LIAO J, WANG J, et al. AGRM: attention-based graph representation model for telecom fraud detection [C] // 2019 IEEE International Conference on Communications (ICC 2019). IEEE. 2019.

[13] XU B, SHEN H, SUN B, et al. Towards consumer loan fraud detection: Graph neural networks with role-constrained conditional random field[C]// Proceedings of the AAAI Conference on Artificial Intelligence. 2021.

[14] LIANG T, ZENG G, ZHONG Q, et al. Credit risk and limits forecasting in e-commerce consumer lending service via multi-view-aware mixture-of-experts nets [C] // Proceedings of the 14th ACM international Conference on Web Search and Data Mining. 2021.

[15] ZHANG Y, FAN Y, YE Y, et al. Key player identification in underground forums over attributed heterogeneous information network embedding framework [C] // Proceedings of the 28th ACM International Conference on Information and Knowledge Management. 2019.

[16] DING K, ZHOU Q, TONG H, et al. Few-shot network anomaly detection via cross-network meta-learning [C] // Proceedings of the Web Conference. 2021.

[17] DING K, SHU K, SHAN X, et al. Cross-domain graph anomaly detection [J]. IEEE Transactions on Neural Networks and Learning Systems, 2021, 33(6): 2406-2415.

[18] HAMILTON W, YING Z, LESKOVEC J. Inductive representation learning on large graphs [J]. Advances in Neural Information Processing Systems, 2017, 30.

[19] VELIČKOVIĆ P, CUCURULL G, CASANOVA A, et al. Graph attention networks [J]. arXiv: 171010903, 2017.

[20] WU Z, PAN S, CHEN F, et al. A comprehensive survey on graph neural networks [J]. IEEE Transactions on Neural Networks and Learning Systems, 2020, 32(1): 4-24.

[21] HAMILTON W L, YING R, LESKOVEC J. Representation learning on graphs: Methods and applications [J]. arXiv: 170905584, 2017.

[22] ZHOU J, CUI G, HU S, et al. Graph neural networks: Areview of methods and applications [J]. AI Open, 2020, 1: 57-81.

[23] FISCHER A, BOTERO J F, BECK M T, et al. Virtual network embedding: A survey [J]. IEEE Communications Surveys & Tutorials, 2013, 15(4): 1888-1906.

[24] WU Z, PAN S, CHEN F, et al. A Comprehensive Survey on Graph Neural Networks [J]. IEEE Transactions on Neural Networks and Learning Systems, 2021, 32(1): 4-24.

[25] KANG J M. Distance Metrics [M]// Encyclopedia of GIS. Cham; Springer International Publishing. 2017: 483-484.

[26] CHOWDHURY G G. Introduction to modern information retrieval [M]. Facet Publishing, 2010.

[27] CORTES C, VAPNIK V. Support-vector networks [J]. Machine Learning, 1995, 20: 273-97.

[28] KIPF T N, WELLING M. Semi-supervised classification with graph convolutional networks [J]. arXiv: 1609. 02907, 2016.

[29] XU K, HU W, LESKOVEC J, et al. How powerful are graph neural networks? [J]. arXiv: 1810. 00826, 2018.

[30] TANG J, LI J, GAO Z, et al. Rethinking graph neural networks for anomaly detection [C] // Proceedings of the International Conference on Machine Learning. PMLR, 2022.

[31] LIU Y, AO X, QIN Z, et al. Pick and choose: a GNN-based imbalanced learning approach for fraud detection[C]// Proceedings of the Web Conference. 2021.

[32] HU X, CHEN H, CHEN H, et al. Mining Mobile Network Fraudsters with Augmented Graph Neural Networks [J]. Entropy, 2023, 25(1): 150.

[33] DOU Y, LIU Z, SUN L, et al. Enhancing graph neural network-based fraud detectors against camouflaged fraudsters[C]// Proceedings of the 29th ACM International Conference on Information & Knowledge Management. 2020.

QIN Zhongpiao, born in 1999, postgraduate, is a member of CCF (No. P6799G). His main research interest is fraud detection.

ZHOU Yatong, born in 1973, Ph.D, professor. His main research interests include pattern recognition and machine learning.