RWK-GNN:基于特征增强与子核分解的非平衡图欺诈检测算法

于浩淼,刘 炜,孟流畅,陈开睿,宋 友*
(北京航空航天大学软件学院,北京 100191)

摘 要: 金融欺诈对经济和社会稳定造成了严重的威胁,因此开发有效的欺诈检测算法对于保护金融系统的完整性至关重要. 目前已有多种基于图学习的欺诈检测算法应用于实际场景当中,这些方法或针对图的结构信息开展分类,或通过图卷积神经网络学习节点的嵌入式表示进行欺诈检测工作,关注角度相对单一,无法完备地在非平衡多关系图上开展欺诈检测分析. 针对以上问题,本论文提出了一种结合随机游走下的特征增强与子核分解的图神经网络欺诈检测算法(Random Walk feature enhancement and Kcore subkernel decomposition Graph Neural Network,RWK-GNN),该算法能够高效地挖掘出多关系不平衡图中节点层级与全局网络层级的拓扑信息,并通过子核分解算法优化图结构特征在社区演进角度上的传播与聚合,最终完成欺诈检测与识别. 为验证RWK-GNN算法性能,本文使用了图神经网络欺诈检测任务常用的公开数据集进行模型训练与测试. 实验结果表明,在同一评价指标下,该方法较相关机器学习算法与图神经网络算法有着较大提升,与CARE-GNN算法相比,该方法的AUC值提升了17%;与PC-GNN算法相比,该方法的AUC值提升了8%;与SIGN算法相比,该方法的AUC值提升了7%.

关键词: 深度学习;图表示学习;图神经网络;类不平衡;节点分类;金融欺诈检测
基金项目: 河北省重点研发计划(No.21310101D)
中图分类号: TP311.5;TP391.4 **文献标识码:** A **文章编号:** 0372-2112(2024)10-3382-10
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20240346

RWK-GNN: Fraud Detection for Imbalanced Graphs with Feature Enhancement and Subkernel Decomposition

YU Hao-miao, LIU Wei, MENG Liu-chang, CHEN Kai-rui, SONG You*
(*School of Software*, *Beihang University*, *Beijing* 100191, *China*)

Abstract: Financial fraud poses a serious threat to the economic and social stability, making the development of effective fraud detection algorithms crucial for safeguarding the integrity of the financial system. Currently, various graph-based fraud detection algorithms have been applied in practical scenarios. These methods either classify based on the structural information of graphs or utilize graph convolutional neural networks to learn embedded representations of nodes for fraud detection. However, these approaches have relatively narrow perspectives and cannot comprehensively analyze fraud detection on imbalanced multi-relational graphs. To address these issues, this paper proposes a RWK-GNN (Random Walk feature enhancement and Kcore subkernel decomposition Graph Neural Network), which efficiently extracts topological information at both the node level and the global network level in imbalanced graphs with multiple relationships. It optimizes the propagation and aggregation of graph structural features from the perspective of community evolution through subkernel decomposition algorithm, ultimately achieving fraud detection and identification. To validate the performance of the RWK-GNN algorithm, this study employs commonly used public datasets for graph neural network fraud detection tasks in model training and testing. Experimental results demonstrate significant improvements of this method over other machine learning algorithms and graph neural network algorithms in terms of the same evaluation metrics. Compared to the CARE-GNN algorithm, the proposed method achieves a 17% increase in AUC value. Compared to the PC-GNN algorithm, the proposed method achieves an 8% increase in AUC value. Moreover, compared to the SIGN algorithm, the proposed method achieves

收稿日期:2024-04-17;修回日期:2024-08-26;责任编辑:覃怀银
*通讯作者:宋友

a 7% increase in AUC value.

Key words: deep learning; graph representation learning; graph neural network; class imbalance; node classification; financial fraud detection

Foundation Item(s): Hebei Province National key Research and Development Program (No.21310101D)

1 引言

近年来,随着人工智能、大数据和深度学习等计算机技术的持续迭代和日益成熟,与数字技术紧密相关的金融领域也在快速发展,并推动着传统金融行业向线上模式发展. 逐步体系化的线上金融模式为企业和用户带来了便利,但同时也助长了欺诈行为的发生. 北京金融信息化研究所发布的《金融反欺诈与大数据风控研究报告(2023年)》[1]指出自2020年以来,我国电信网络诈骗案件数量不断增多,涉及财产损失不断增加,涉诈金额数量超过百亿. 金融欺诈不仅威胁着个体用户的财产安全,同时还严重损害了金融机构的信用程度与社会经济大环境,无论是在个人层面还是社会层面,都已成为了亟待解决的重要问题.

为了应对日益严峻的金融欺诈攻势,多种反欺诈算法被应用于实际业务场景,这些算法主要可以分为基于专家知识的欺诈检测算法,基于数据挖掘的欺诈检测算法和基于图的欺诈检测算法. 基于专家知识的欺诈检测算法依赖于专家经验规则的总结而展现出较高的业务可解释性,在检测欺诈行为的同时,该算法能够清晰地揭示判别欺诈风险的原因. 然而,该算法面临的一个显著问题是其难以适应业务场景的快速迭代,导致难以及时迁移和更新规则. 基于数据挖掘的欺诈检测算法则通过决策树、机器学习分类模型等方法对海量客户特征进行深入分析,从而完成欺诈风险的判别,这种算法能够随着业务场景的变迁灵活调整参数,展现出较高的灵活性和高效性. 基于图的欺诈检测算法依赖于人工神经网络来实现欺诈风险的检测,进一步提升了识别的准确率,但以上两种方法均缺乏足够的业务可解释性[2].

本文对以上的研究方法分析发现,现有的方法虽然能够通过神经网络模型利用数据当中的图结构信息,但仍然存在着一些不足,上述方法主要侧重于挖掘用户个体的特征信息,而对于社群内不同个体之间存在的多种复杂关联与交互信息的利用相对有限. 此外,在进行欺诈检测时,上述方法均未考虑欺诈行为和模式的复杂性和多变性. 实际上,随着社会的不断发展和技术的更新迭代,欺诈组织及其行为模式逐渐呈现出团伙化和隐蔽化的趋势,导致单一场景下的欺诈检测模型的分类与预测结果不佳.

在当前工作的基础上,为了结合实际当中金融欺诈组织与模式的多样性,有效挖掘社群中个体间的关联信息,本文提出了基于特征增强与子核分解的非平衡图欺诈检测算法RWK-GNN(Random Walk feature enhance and Kcore subkernel decomposition Graph Neural Network). 该算法通过多关系特征集成方法对图节点特征进行挖掘,进而丰富节点嵌入表示,同时通过子核分解和邻域采样从社区演进和广度双视角出发深度挖掘图结构信息,并通过图神经网络完成采样后邻域节点信息向目标节点信息的聚合.

2 相关工作

2.1 基于专家知识的欺诈检测

基于专家知识的欺诈检测算法通过基于规则的专家系统架构开展在金融等领域方面的反欺诈工作. 该方法通过行业内专家人为集成若干反欺诈规则形成规则池,并使用逻辑关系运算对规则池当中的规则进行集成汇总. 20世纪90年代欺诈检测系统TRAP[3]是基于专家规则构建的典型系统代表,此类系统通过可重用的专业知识模型库,以规则匹配的方式从大量交易当中筛选出可疑交易,完成反欺诈工作.

随着时代和技术的不断发展,以及欺诈模式的不断变化,基于专家知识的欺诈检测算法所需规则数量也在不断增加. 为了更高效且精准地进行欺诈检测,Vatsa等[4]引入了博弈论等数学方法来提高欺诈检测系统的性能,将欺诈行为与检测系统设计为两个模型之间的相互重复博弈,以取得最大化收益. 现有基于专家知识的欺诈检测算法主要基于Liu等[5]提出的Rete算法,将规则池当中的专家规则编译为Rete网络来进行与事实的匹配. 此外,针对欺诈检测规则的管理问题,Gianini等[6]提出了一种基于Shapley值的规则量化原则,通过对规则的贡献程度开展排名来进行规则池的管理与规则评估工作.

2.2 基于数据挖掘的欺诈检测

在当前金融市场环境下,随着互联网大数据等信息技术的不断发展,研究人员提出了基于数据挖掘的欺诈检测算法. 相比于基于专家知识,基于数据挖掘的欺诈检测算法能够从大批量的历史数据当中自动捕获异常交易记录,同时挖掘暂未定义的新欺诈类型[7],能够更为高效地处理和筛选海量数据. 其中,Kokkinaki等[8]提出了采用决策树与布尔逻辑函数结合的方法对金融交易当中的消费行为进行分析,并通过聚类算法完成对欺诈行为的识别检测. Soemers等[9]将欺诈检测

设为奖励进行建模，通过增量回归树学习器创建具有与前者类似的预期奖励的交易集群，从而进行动态地检测信用卡欺诈行为.

2.3 基于图的欺诈检测

在金融服务当中用户间的互动十分丰富，且用户自身所展示的信息也非常多面，这些交互数据形成了一个大型的多视图网络，这些特质是上述方法无法充分利用的. 随着深度学习的不断发展以及图神经网络(Graph Nerual Network，GNN)的提出，研究人员在金融欺诈检测领域引入了相关方法，形成了基于图的欺诈检测算法. 此类算法能够针对用户、交易行为与交易方等共同构建形成的网络拓扑结构进行挖掘，进而构建相关的特征嵌入表示用于下游欺诈检测与交易行为分类.

在基于图结构数据的金融欺诈检测方面，Liu等[10]提出了GEM算法来自适应地从“帐户-设备”异构图中学习判别嵌入表示来进行恶意帐户检测. 随着注意力机制的出现与发展，部分金融欺诈模型引入该方法提升模型性能，Wang等[11]提出了一种半监督GNN模型Semi-GNN，并在模型当中引入了分层注意力机制，在更好地关联不同邻居和视图的同时使模型具有可解释性. 随着金融欺诈方式的发展，目前许多欺诈行为具有一定的伪装性，致使图数据出现关系特征与上下文不一致等情况，针对这些问题，Liu等[12]提出了GraphConsis模型，通过设计一致性评分来对不一致的邻居节点进行过滤，同时学习样本节点的关系注意力权重，从而应对图当中所存在的不一致问题；Li等[13]提出了NFE-GNN模型，该方法通过计算特征相似度对噪声信息进行过滤等方法增强欺诈类数据的特征信息，从而较好地应对数据噪声问题.

3 RWK-GNN方法

本文提出了在标签不平衡的情况下，基于多关系图特征集成与子核分解的RWK-GNN欺诈检测算法. 该算法模型主要包括多关系图特征集成层、子核分解层、节点邻域采样层以及特征信息聚合层四部分，具体算法架构如图1所示.

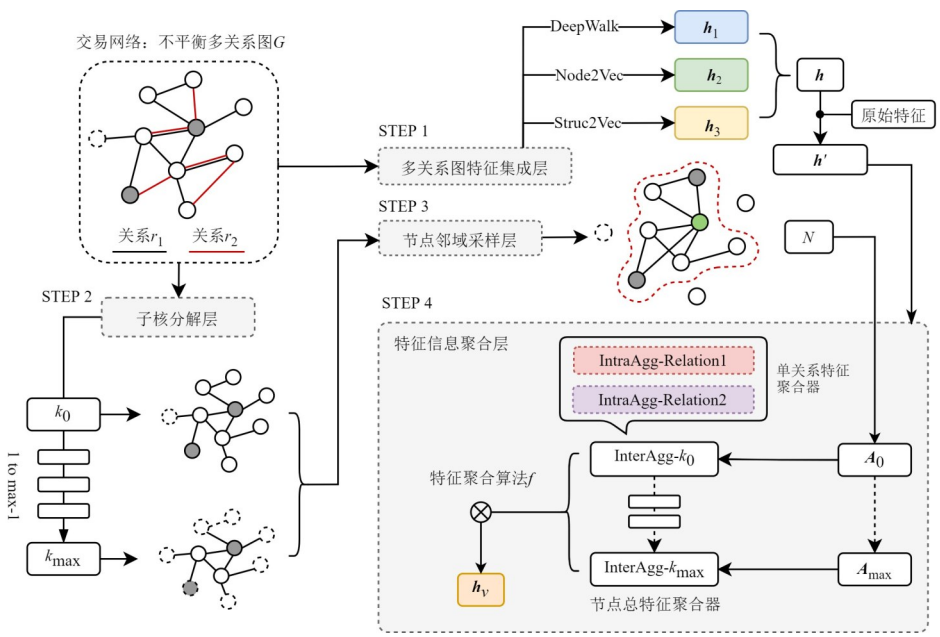


图1 RWK-GNN模型总体架构

其中多关系图特征集成层能较好解决数据集中手工提取的原始特征反馈信息匮乏、无法体现欺诈模式结构特征等问题；子核分解层从社区演进的角度出发，考虑图的稠密子图以及节点的连通性，将图按照节点的核心影响程度进行子图分解，通过边集迭代缩小的方式保留了节点的重要程度，用于后续特征信息的聚合；邻域节点采样层针对标签不平衡情况对节点的邻域进行过采样或欠采样，并引入节点特征空间上的相对距离，在相似的欺诈节点间构造新的邻域关系；特征信息聚合层通过构造特征聚合器完成深层次纵向特征信息的聚合，输出的节点嵌入表示结果用于下游的欺诈分类与检测等工作，完成对用户网络当中个体节点的欺诈风险判定.

3.1 多关系图特征集成层

在多关系图数据集中，各节点具有初始的特征信息，并使用嵌入向量表示. 大部分数据集的节点嵌入向量为手工提取特征，这些特征包含的信息倾向于反馈节点层面即用户个体的信息，而没有完备考虑图的复

杂结构特征信息. 针对该问题,本文提出了多关系图特征集成层来挖掘和集成多关系图当中各节点在个人角度和网络角度的综合特征信息. 多关系图特征集成层主要包括随机游走特征挖掘算法与多关系图特征集成方法,其中随机游走特征挖掘算法通过在关系图上构造随机游走序列的方式学习节点在图当中的嵌入表示,挖掘节点在网络层面上的特征信息;多关系图特征集成方法则考虑到异质图的多关系特点,将通过随机游走获得的各关系下的节点特征信息进行集成,用于后续模型的训练与学习.

3.1.1　随机游走特征挖掘算法

随机游走特征挖掘算法是一种通过学习图结构特征获取节点低纬嵌入向量表示的算法,该算法基于图中节点之间的随机游走过程,通过模拟节点之间的随机转移,挖掘出节点的特征信息. 在本文的特征挖掘过程当中,采用了三种随机游走算法,分别为DeepWalk算法[14]、Node2Vec算法[15]以及Struc2Vec算法[16].

(1) DeepWalk算法的核心步骤为构建游走序列和学习节点向量表示,该算法通过随机游走的方式采集若干节点序列,并基于SkipGram模型进行滑窗采样,完成对图中节点特征表示的学习. 该算法的优势在于能够从全局视图的角度出发针对于图的结构化信息进行学习,特别是在存在缺失信息的情况下.

(2) Node2Vec算法在随机游走的过程中引入节点转移概率的概念,针对DeepWalk算法的游走过程过于自由这一问题进行了调整和改进. 该算法设计了不同的参数用于计算节点的转移概率,从而控制游走方向在深度优先和广度优先之间的平衡程度. Node2Vec算法改进了随机游走序列的生成方式,采集到的节点序列能够反映深度优先和广度优先两种特性,进而增加单词嵌入的准确性,提高网络嵌入的效果. 此外,由于同时考虑到了图数据结构的两种维度特征,Node2Vec算法在社群类别的网络当中有着广泛的应用.

(3) Struc2Vec算法通过构建多层图进行结构特征的捕捉. 考虑到上述方法在随机游走过程中会对序列长度有所限制,该算法通过建立层次结构来描述节点之间的结构相似性,因此该算法不依赖于节点的相对距离来评估节点的相似性,且该层次结构对于结构相似性描述的严格程度逐层递增.

3.1.2　多关系图特征集成方法

DeepWalk、Node2Vec和Struc2Vec三种随机游走算法在游走方式上存在的差异使得这三种算法能够针对具有不同特点的图结构网络有着较好的表现. 本文考虑到金融交易场景的多样性以及欺诈行为的多变性与隐匿性,提出了适用于现实场景下的多关系图特征集成方法,该方法的框架图如图2所示.

该特征集成方法考虑到在实际场景当中往往无法第一时间感知到欺诈行为的具体模式这一问题,在单个关系图上采用多种游走方式,以便能够兼顾到不同的欺诈模式. 其中,DeepWalk算法适用于大部分简单欺诈模式,具有较好的泛用性,能够全面学习到个体节点所具有的嵌入表示和行为特征;Node2Vec算法则同时考虑到了图的广度与深度,能够通过调整参数对单个个体节点进行广度或深度模式下的游走,在具有特定特征的欺诈模式上有着较好的表现,例如传销式欺诈以及呈现链式行为模式的“单线欺诈结构”;Struc2Vec算法能够获取节点在不相邻空间上的结构相似性,适用于团伙性欺诈模式,例如具有“财务-中间人-实施人”结构的团伙作案行为.

通过三种方法学习到图中各节点在不同模式下的特征信息,并通过集成算法进行特征信息的整合,集成算法如式(1)所示:

$$\begin{aligned}\boldsymbol{E}_u &= f\left(\sum_r^R \boldsymbol{h}_{u,r}\right) \oplus f\left(\sum_r^R \boldsymbol{h}'_{u,r}\right) \oplus f\left(\sum_r^R \boldsymbol{h}''_{u,r}\right) \\ &= f\left(\sum_r^R \left(\boldsymbol{h}_{u,r} \oplus \boldsymbol{h}'_{u,r} \oplus \boldsymbol{h}''_{u,r}\right)\right)\end{aligned} \tag{1}$$

其中$\boldsymbol{E}_u$是点u的特征集成结果,为嵌入向量表示;f为集成方法,常用函数包括SUM、AVERAGE、MAX和MIN,本文采用AVERAGE作为集成方法函数.

3.2　子核分解层

在图深度学习当中,大部分模型在特征聚合阶段均考虑到了图的平面视角,也即邻域节点特征,但忽略了图的社区视角. 从社区演进的角度出发,不同的节点在图当中的核心程度存在较大差异,如图3所示. 对于一个存在大量交易行为的网络,存在大量边缘节点以及少数核心节点,核心节点当中的非欺诈节点代表了行业当中的核心业务,欺诈节点则代表了交易当中存在的严重风险行为,两类核心节点的影响力和重要程度随着子图分解程度的加深而不断增加,其特征信息在欺诈检测等下游任务当中具有重要价值.

本文在子核分解层引入了Kcore算法来完成对多关系图中节点具有的社区演进特征的挖掘,其在模型当中承担识别和分析图中核心节点的重要功能,该算法通过迭代分解图结构的方式挖掘出图中紧密连接的部分. 在特征聚合时采用合适的子核分解结果参与聚合过程可提升图核心节点特征信息的相应权重,有助于图神经网络更好地理解图具有的社区结构,提高图学习任务的性能和效率.

3.3　节点邻域采样层

在图神经网络当中,节点通过多种网络层将其邻域的节点所持有的特征通过某种方式进行聚合,以平均聚合方法和图卷积网络为例:

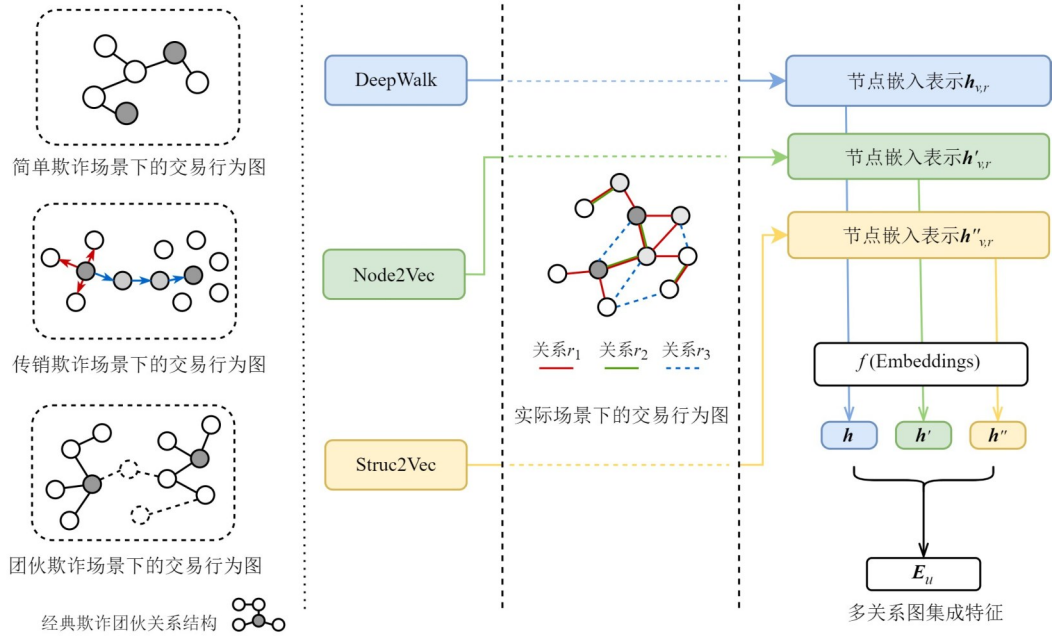


图2 多关系图特征集成方法

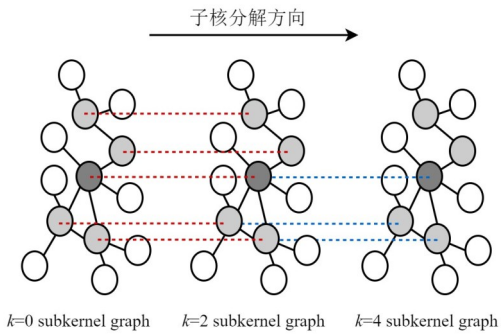


图3 社区演进视角下的图子核分解

(1)平均聚合:通过平均的思想来对节点及附近节点的信息进行表达,对于节点u的聚合特征$\boldsymbol{h}$如式(2)所示:

$$\boldsymbol{h}_u^{l+1}=\sigma(\boldsymbol{W}(\boldsymbol{h}_u^l+\frac{1}{|N|}\sum_{j\in N}\boldsymbol{h}_j^l)) \tag{2}$$

其中,σ为激活函数,$\boldsymbol{W}$为参数矩阵,N为节点u的邻居节点集,l为当前所在网络层. 可以看出,平均聚合方法是一种迭代算法,节点特征嵌入表示在经过一轮计算后会扩展一圈聚合范围,随着层数的增加,单个节点的感知域也会越大.

(2)图卷积网络:引入节点度的概念,通过卷积计算的方式对节点及附近节点的信息进行表达,聚合特征$\boldsymbol{H}$如式(3)所示:

$$\boldsymbol{H}^{l+1}=\sigma(\hat{\boldsymbol{D}}^{-\frac{1}{2}}\hat{\boldsymbol{A}}\hat{\boldsymbol{D}}^{-\frac{1}{2}}\boldsymbol{H}^l\boldsymbol{W}^l) \tag{3}$$

其中,σ为激活函数,$\hat{\boldsymbol{A}}$为添加了自环的邻接矩阵,$\hat{\boldsymbol{D}}$为与$\hat{\boldsymbol{A}}$相对应的节点度矩阵,$\boldsymbol{W}$为参数矩阵. 可以看出,在图卷积神经网络当中考虑到了在卷积计算的过程当中包含节点自身的特征,且通过度表示节点邻域的大小能够对特征进行更准确的刻画.

对于平均聚合方法,存在节点对其邻域节点过分依赖的问题,若节点的某个邻居节点度远大于节点本身,则邻居节点聚合得到的特征信息在该节点特征计算的过程当中实际价值较低. 图卷积网络在此基础上引入了节点度的概念,较好地解决了对邻居过分依赖的问题,但随着卷积层的增加,各个节点所感知到的信息也在不断接近,容易出现过平滑(over-smoothing)的问题.

在实际金融交易场景下,一个交易网络当中的欺诈行为存在的数量往往较少,对应的图中欺诈节点与普通节点数量的比值远小于1,因此会存在严重的节点标签不平衡情况,且目标对象(欺诈节点)为标签分类当中的少数类(minority,公式中记作M). 若将标签不平衡的数据输入图神经网络当中,会导致欺诈节点的特征信息被多数类(majority)稀释,无法进行准确的欺诈行为分类与预测. 针对此问题,本文设计了节点邻域采样层,对少数类进行过采样,对多数类进行欠采样,通过平衡采样的方式解决因标签不平衡导致的稀释问题. 样本选择与节点邻居采样方法如式(4)~(7):

$$P(v,r)=\frac{\text{Degree}(v,r)}{\text{ClassFrequency}(v,r)} \tag{4}$$

$$N_{v,r}^{\text{under}}=\{u\in V|A_r(v,u)>0\text{ and }D(v,u)<\rho\} \tag{5}$$

$$N_{v,r}^{\text{over}}=\{u\in V|u,v\in M\text{ and }D(v,u)<\rho\} \tag{6}$$

$$N_{v,r}=N_{v,r}^{\text{under}}\bigcup N_{v,r}^{\text{over}} \tag{7}$$

其中,$P(v,r)$为关系图r采样时节点v被选择的概率,$N_{v,r}$为采样结果,ρ为采样筛选阈值. 该方法引入节点度和

标签频率综合考虑节点在图当中的重要程度,并增加采样时少数类别节点被采样的概率,且随着节点度数越高,被采样的可能性越大,能够确保采样时不会破坏图的结构特征. 此外,由于存在标签不平衡的情况,本文对样本当中节点进行邻域构造时采用欠采样方法,通过计算点与点间的曼哈顿距离对邻居节点进行选择;针对少数类节点,则通过过采样的方法,在邻域构造的过程当中添加虚构边连接空间上相似的同类别节点来补充邻域元素.

3.4 特征聚合层

结合子核分解层与节点邻域采样层,本文设计了RWK-GNN模型的节点特征聚合层. 该方法在当前网络层的子核分解邻域样本的基础上,对单关系下邻居节点的当前层特征信息进行聚合,接着将多个关系下的特征信息再次聚合,得到节点在当前层的特征聚合结果. 聚合过程如式(8)~(10)所示:

$$\boldsymbol{h}_{v,r}^{l+1}=\mathrm{ReLU}(\boldsymbol{W}_r^{l+1}(\boldsymbol{h}_{v,r}^{l}\oplus\Theta(l,r,v))) \tag{8}$$

$$\Theta(l,r,v)=\mathrm{AGG}\{\boldsymbol{h}_{u,r,k}^{l},u\in N_{r,k}^{l+1}(v)\} \tag{9}$$

$$\boldsymbol{h}_{v}^{l+1}=\mathrm{ReLU}(\boldsymbol{W}^{l+1}(\boldsymbol{h}_{v}^{l}\oplus\bigcup_{r}^{R}\boldsymbol{h}_{v,r}^{l})) \tag{10}$$

其中$\boldsymbol{h}_{v,r}^{l}$为第l层网络中关系r下节点v的特征嵌入表示,$\boldsymbol{W}$为权重矩阵,Θ为特征平均聚合函数,ReLU为模型激活函数.

本文提出的RWK-GNN方法结合随机游走下的特征增强与子核分解算法,相较于现有的图表示学习模型,针对多数方法未考虑到的实际场景下欺诈组织与行为特点进行创新. 首先本文方法针对普通欺诈、传销欺诈与团伙欺诈等不同诈骗组织的结构特征,通过Node2Vec方法适配差异化场景,在考虑到多维度节点特征信息的前提下生成嵌入向量表示. 同时,该模型的不同模块在方法的优化思路上相对应,在进行特征增强与临域采样的过程当中,考虑图数据中可能存在的欺诈伪装行为,通过Struc2Vec方法与特征空间中的点间相对距离,保留了图数据的结构特征,抽取欺诈节点间的隐式关系,进一步提高模型的预测准确度. 此外,本模型引入Kcore子核分解算法,通过迭代分解图结构的方式挖掘出图中紧密连接的部分,结合社区演进概念,对不同核心度的子图进行特征聚合,更加充分地利用了图的特征结构信息,提升模型的整体性能.

4 实验结果与分析

本文实验采用Python3.8及Pytorch2.2.1深度学习框架进行模型搭建,并使用AUC(Area Under Curve,AUC)和F_1-macro值作为模型性能评价指标,在图神经网络欺诈检测任务常用的公开数据集YelpChi以及中国公司财务报表欺诈公开数据集FDCompCN上进行实验探究与验证. 在实验阶段,模型的邻域采样层相关参数ρ值为0.5,数据集按照40%,20%和40%的比例划分为训练集、验证集和测试集. 其中训练集与测试集的划分基于Scikit-learn[17]提供的分层采样方法,确保划分所得两个集合的不平衡率一致.

4.1 数据集介绍

本文实验采用YelpChi评论欺诈数据集[18]与中国公司财务报表欺诈的数据集FDCompCN[19]作为训练数据集. 两数据集具体信息如表1所示.

表1　数据集具体信息

数据集	关系类别	不平衡比率	关系描述	关系图边数
YelpChi	R-U-R	0.145	同一用户发布的评论	49 315
	R-T-R		同一产品在某星级下的评论	573 616
	R-S-R		同一时间发布的某产品下的评论	3 402 743
FDCompCN	C-I-C	0.105	存在投资关系的公司	5 686
	C-P-C		同一客户下的公司	760
	C-S-C		同一上游供应商下的公司	1 043

4.1.1 YelpChi数据集

YelpChi数据集是基于美国最大的点评网站Yelp的一个行为图数据集,该数据集以稀疏矩阵的形式存储了相关的个体特征与图结构化特征,并提取了32个手工特征作为节点的原始特征. 该数据集拥有45 954个节点.

4.1.2 FDCompCN数据集

FDCompCN数据集是以中国公司财务报表欺诈为主要内容的公开数据集,其数据来自中国股票市场和会计研究(CSMAR)数据库,该数据集包含2020年至2023年间中国企业财务报表中展示的供应商、客户、股东和财务信息,其中包括5 317家中国上市公司.

4.2 对比算法介绍

为了检验本文提出的RWK-GNN方法的有效性,我们比较了9个图神经网络模型及其改进算法:GCN,MLP,GraphSAGE[20],CARE-GNN[21],PC-GNN[22],SAGN[23],SIGN[24],DAGNN[25]以及AO-GNN[26].

4.3 实验分析

4.3.1 子核分解算法有效性分析

为验证子核分解算法的有效性,本文基于GraphSAGE、CARE-GNN以及PC-GNN三种针对多关系不平

衡图的GNN模型设计对照实验，结果如表2所示．实验结果表明，在基础模型中增加子核分解层，能够考虑到图的社区演进角度，进而提高在欺诈分类与检测方面的性能与表现．

表2 子核分解算法有效性验证

模型方法	Model Baseline				增加子核分解层			
	YelpChi		FDCompCN		YelpChi		FDCompCN	
	F_1-macro	AUC	F_1-macro	AUC	F_1-macro	AUC	F_1-macro	AUC
GraphSAGE	0.454 3	0.750 5	0.505 9	0.649 1	0.565 2	**0.759 2**	0.511 8	**0.654 7**
CARE-GNN	0.578 4	0.741 4	0.490 0	0.651 8	0.630 5	**0.803 4**	0.503 7	**0.664 3**
PC-GNN	0.643 5	0.837 7	0.518 7	0.667 4	0.677 4	**0.841 3**	0.528 5	**0.673 2**

4.3.2 随机游走特征增强算法有效性分析

为验证随机游走特征增强算法的有效性，本文基于GCN、MLP等七组对比算法设计了对照实验，结果如表3所示．

实验结果表明，添加了特征增强层的模型性能均优于模型的基础性能，其中DeepWalk算法对大部分模型的提升性能高于另外两种游走算法，侧面验证了前文提到的DeepWalk算法的普适性．

表3 随机游走特征增强算法有效性验证

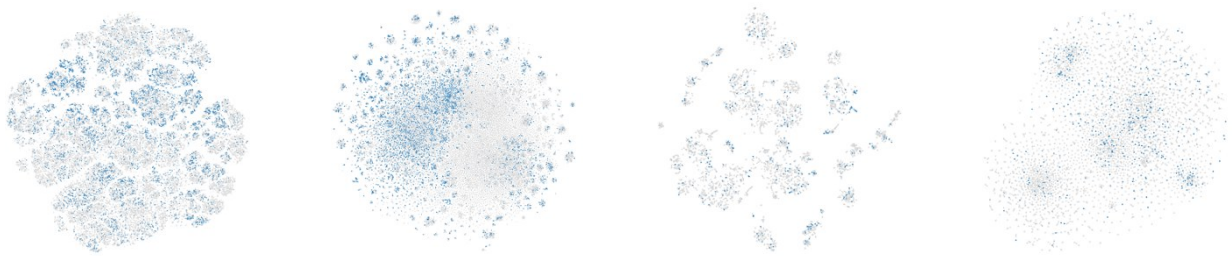
模型方法	Model Baseline				增加DeepWalk			
	YelpChi		FDCompCN		YelpChi		FDCompCN	
	F_1-macro	AUC	F_1-macro	AUC	F_1-macro	AUC	F_1-macro	AUC
GCN	0.440 7	0.567 7	0.408 9	0.529 2	0.499 9	0.588 2	0.427 1	0.535 1
MLP	0.494 1	0.759 8	0.430 6	0.570 8	0.460 8	0.770 1	0.438 8	0.576 9
GraphSAGE	0.454 3	0.750 5	0.505 9	0.649 1	0.722 8	**0.864 0**	0.524 5	0.656 4
CARE-GNN	0.578 4	0.741 4	0.490 0	0.651 8	0.716 1	**0.882 6**	0.507 1	0.663 6
PC-GNN	0.643 5	0.837 7	0.518 7	0.667 4	0.725 6	0.882 0	0.531 0	**0.684 3**
SAGN	0.685 5	0.832 1	0.504 4	0.651 3	0.747 9	**0.892 2**	0.520 2	**0.669 2**
SIGN	0.702 9	0.832 7	0.513 2	0.660 5	0.708 5	**0.890 1**	0.521 5	**0.679 0**
模型方法	增加Node2Vec				增加Struc2Vec			
	YelpChi		FDCompCN		YelpChi		FDCompCN	
	F_1-macro	AUC	F_1-macro	AUC	F_1-macro	AUC	F_1-macro	AUC
GCN	0.544 8	**0.696 7**	0.428 2	**0.549 2**	0.464 3	0.628 8	0.425 1	0.545 7
MLP	0.483 1	**0.861 7**	0.441 2	**0.586 9**	0.480 4	0.842 8	0.447 1	0.582 5
GraphSAGE	0.614 2	0.784 4	0.516 6	0.662 0	0.636 1	0.844 8	0.519 3	**0.663 5**
CARE-GNN	0.630 9	0.798 4	0.501 7	**0.666 2**	0.668 5	0.852 0	0.507 8	0.665 1
PC-GNN	0.716 6	0.873 8	0.529 2	0.681 3	0.637 9	**0.845 8**	0.529 8	0.680 0
SAGN	0.791 9	0.861 9	0.518 7	0.666 6	0.891 3	0.754 7	0.519 5	0.668 7
SIGN	0.599 2	0.895 1	0.530 4	0.673 6	0.881 7	0.747 3	0.527 9	0.672 1

此外，本文针对YelpChi数据集与FDCompCN数据集当中手工提取的原始节点特征和本文的多关系图特征集成方法所得特征进行特征数据降维与可视化，结果如图4(a)~(d)所示．根据降维后的特征分布情况来看，YelpChi数据集与FDCompCN数据集当中的原始特征能够在一定程度上体现节点类别的差异，但仍然存在特征模糊和差异不明显的情况，而经过本文的多关系特征集成方法处理后得到的特征在降维后相比于前者出现了明显的类别分离效果，进一步证明了本文方法的有效性．

4.3.3 各模型性能比较

表4给出了本文提出的RWK-GNN与所有对比方法的检测性能，从中可以看出RWK-GNN的性能优于所有对比方法，证明了其有效性．此外，通过实验我们得出以下结论：

(1)相比于MLP、GCN和GraphSAGE等已有算法模型，RWK-GNN有着明显的提升，主要原因是由于这些模型没有考虑到实际当中欺诈行为的复杂性和多样性．其中，MLP是一种相对简单的神经网络结构，其处理复杂图结构数据的能力有限，而交易行为网络关系复杂，MLP可能无法充分捕获这些复杂模式；GCN模型在进行特征聚合时容易出现过平滑问题，使得图中节点的特征信息趋于相似，影响后续的分类与检测任务；GraphSAGE在构造节点邻域时会按照固定数量进行不



(a) YelpChi原始特征　(b) YelpChi集成后特征　(c) FDCompCN原始特征　(d) FDCompCN集成后特征

图4　特征降维可视化对比结果

恰当采样,可能会导致节点类别的不平衡程度进一步加剧,甚至出现少数类被完全过滤从而导致检测性能更差的情况.

(2)对于CARE-GNN和PC-GNN等针对多关系图的算法模型,由于考虑到图结构复杂程度,其性能与经典方法相比略有升高,但弱于本文提出的RWK-GNN方法.其中CARE-GNN算法考虑到了数据当中可能存在伪装与噪声而对节点进行选择性过滤,PC-GNN考虑到欺诈数据当中存在的类不平衡情况而对节点进行针对性采样.本文方法在以上方法的基础上引入子核分解概念,从社区演进视角出发对节点的特征进行挖掘,进一步提升聚合后特征的信息价值,进而提升模型性能.

表4　本文RWK-GNN方法与现有模型的检测性能比较

类别	模型方法	YelpChi		FDCompCN	
		F_1-macro	AUC	F_1-macro	AUC
已有方法	GCN	0.440 7	0.567 7	0.408 9	0.529 2
	MLP	0.494 1	0.759 8	0.430 6	0.570 8
	GraphSAGE	0.454 3	0.750 5	0.505 9	0.649 1
	CARE-GNN	0.578 4	0.741 4	0.490 0	0.651 8
	PC-GNN	0.643 5	0.837 7	0.518 7	0.667 4
	SAGN	0.685 5	0.832 1	0.504 4	0.651 3
	SIGN	0.702 9	0.832 7	0.513 2	0.660 5
	DAGNN	0.706 1	0.877 9	0.511 4	0.685 6
	AO-GNN	0.709 3	0.881 3	0.527 9	0.690 1
本文方法	RWK-GNN	**0.746 9**	**0.913 3**	**0.560 8**	**0.703 7**

(3) SIGN方法通过不同大小的图卷积滤波器来避免对图采样的需求,提升了模型在大图上的训练效率;SAGN方法可以自适应地收集不同跳点之间的邻域信息,采用了结构感知的注意力机制来代替SIGN中的串联操作.这两种方法在性能上均高于经典方法,但弱于本文方法.本文提出的RWK-GNN方法能够通过合适的随机游走算法对特定欺诈场景下的节点特征进行深度挖掘,通过多关系图特征集成层丰富节点特征,提升模型整体性能.

(4)AO-GNN方法引入了标签分布不敏感的最大化AUC方法来处理数据集当中存在的标签不平衡问题,DAGNN方法则考虑到了真实数据当中可能存在的伪装行为与噪声问题,通过降低噪声干扰与扩展通道等方式优化GNN模型,在性能上较之前的方法都有所提升,但均弱于本文提出的RWK-GNN方法.本文模型通过子核分解算法挖掘节点间的紧密关系,能够在一定程度上规避伪装与噪声带来的负面影响,从而进一步提升模型在欺诈检测当中的精确度.

4.4　消融实验

本文通过设计消融实验来验证RWK-GNN方法当中两个关键模块的有效性,构造2个变体方法如下:

(1)RWK-GNN/r:在完整方法RWK-GNN中,只使用多关系图特征集成组件和邻域节点采样组件,而不使用子核分解组件.

(2)RWK-GNN/k:在完整方法RWK-GNN中,只使用子核分解组件和邻域节点采样组件,而不使用多关系图特征集成组件.

实验结果如表5所示.从结果中可以看出,由于RWK-GNN/r方法仅依赖多关系图特征集成组件和邻域节点采样组件,忽略了子核分解组件,这导致在训练过程中模型未充分考虑图的社区演进特性,无法充分学习到特定模式下的节点特征.

另一方面,与完整方法相比,RWK-GNN/k方法的性能评估指标有所降低.这一结果说明,缺乏多关系图特征集成组件的处理,使得数据集的原始节点特征无法有效地反映节点的实际信息.相比之下,通过多关系图特征集成方法对节点嵌入表示进行拓展,能够更精确地捕捉节点的复杂特性,从而有效地提升模型的检测性能.

表5 RWK-GNN方法及其2个变体方法的检测性能

类别	方法名称	YelpChi		FDCompCN	
		F_1-macro	AUC	F_1-macro	AUC
变体方法	RWK-GNN/r	0.686 1	0.856 5	0.506 2	0.672 5
	RWK-GNN/k	0.697 5	0.824 2	0.482 9	0.668 4
完整方法	RWK-GNN	**0.746 9**	**0.913 3**	**0.560 8**	**0.703 7**

5 结论

现有图神经网络欺诈检测方法很少考虑实际欺诈模式的多样性以及多关系不平衡图的社区演进特征，导致模型检测性能不理想，本文提出了一种结合随机游走和子核分解的图神经网络欺诈检测算法，通过挖掘图结构增强节点特征，丰富嵌入表示信息，在考虑图社区演进特征的基础上构造节点邻域，完成从邻居节点到目标节点的特征聚合．在公开数据集YelpChi与FDCompCN上通过实验验证了RWK-GNN方法的有效性．

参考文献

[1] 北京金融信息化研究所．金融反欺诈与大数据风控研究报告 [EB/OL]. (2023-12-26) [2024-04-10]. https://www.docin.com/p-4571244234.html.

[2] MOTIE S, RAAHEMI B. Financial fraud detection using graph neural networks: A systematic review[J]. Expert Systems with Applications, 2024, 240: 122156.

[3] PORTER D. Reusable analysis and design components for knowledge-based system development[M]//Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992: 373-391.

[4] VATSA V, SURAL S, MAJUMDAR A K. A game-theoretic approach to credit card fraud detection[M]//Lecture Notes in Computer Science. Berlin: Springer Berlin Heidelberg, 2005: 263-276.

[5] LIU D, GU T, XUE J P. Rule engine based on improvement rete algorithm[C]//The 2010 International Conference on Apperceiving Computing and Intelligence Analysis Proceeding. Piscataway: IEEE, 2010: 346-349.

[6] GIANINI G, FOSSI L G, MIO C, et al. Managing a pool of rules for credit card fraud detection by a Game Theory based approach[J]. Future Generation Computer Systems, 2020, 102: 549-561.

[7] ABDALLAH A, MAAROF M A, ZAINAL A. Fraud detection system: A survey[J]. Journal of Network and Computer Applications, 2016, 68: 90-113.

[8] KOKKINAKI A I. On atypical database transactions: identification of probable frauds using machine learning for user profiling[C]//Proceedings 1997 IEEE Knowledge and Data Engineering Exchange Workshop. Piscataway: IEEE, 1997: 107-113.

[9] SOEMERS D, BRYS T, DRIESSENS K, et al. Adapting to concept drift in credit card transaction data streams using contextual bandits and decision trees[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2018, 32 (1): 7831-7836.

[10] LIU Z Q, CHEN C C, YANG X X, et al. Heterogeneous graph neural networks for malicious account detection [C]//Proceedings of the 27th ACM International Conference on Information and Knowledge Management. New York: ACM, 2018: 2077-2085.

[11] WANG D X, LIN J B, CUI P, et al. A semi-supervised graph attentive network for financial fraud detection[C]// 2019 IEEE International Conference on Data Mining (ICDM). Piscataway: IEEE, 2019: 598-607.

[12] LIU Z W, DOU Y T, YU P S, et al. Alleviating the inconsistency problem of applying graph neural network to fraud detection[C]//Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval. New York: ACM, 2020: 1569-1572.

[13] 李康和, 黄震华．基于噪声过滤与特征增强的图神经网络欺诈检测方法[J]. 电子学报, 2023, 51(11): 3053-3060.
LI K H, HUANG Z H. Noise filtering and feature enhancement based graph neural network method for fraud detection[J]. Acta Electronica Sinica, 2023, 51(11): 3053-3060. (in Chinese)

[14] PEROZZI B, AL-RFOU R, SKIENA S. DeepWalk: Online learning of social representations[C]//Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM, 2014: 701-710.

[15] GROVER A, LESKOVEC J. Node2vec: Scalable feature learning for networks[J]. KDD: Proceedings. International Conference on Knowledge Discovery & Data Mining, 2016, 2016: 855-864.

[16] RIBEIRO L F R, SAVERESE P H P, FIGUEIREDO D R. Struc2vec: Learning node representations from structural identity[C]//Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM, 2017: 385-394.

[17] PEDREGOSA F, VAROQUAUX G, GRAMFORT A, et al. Scikit-learn: Machine learning in Python[EB/OL]. (2012-01-02)[2024-04-10]. https://arxiv.org/abs/1201.0490.

[18] RAYANA S, AKOGLU L. Collective opinion spam detection: Bridging review networks and metadata[C]//Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM, 2015: 985-994.

[19] WU B, YAO X Y, ZHANG B Y, et al. SplitGNN: Spectral graph neural network for fraud detection against heterophily[C]//Proceedings of the 32nd ACM International Conference on Information and Knowledge Management. New York: ACM, 2023: 2737-2746.

[20] HAMILTON W L, YING R, LESKOVEC J. Inductive representation learning on large graphs[EB/OL]. (2017-06-07)[2024-04-10]. http://arxiv.org/abs/1706.02216

[21] DOU Y T, LIU Z W, 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. New York: ACM, 2020: 315-324

[22] LIU Y, AO X, QIN Z D, et al. Pick and choose: A GNN-based imbalanced learning approach for fraud detection [C]//Proceedings of the Web Conference 2021. New York: ACM, 2021: 3168-3177.

[23] SUN C, GU H, HU J. Scalable and adaptive graph neural networks with self-label-enhanced training[EB/OL]. (2021-04-19)[2024-04-10]. https://arxiv.org/abs/2104.09376.

[24] FRASCA F, ROSSI E, EYNARD D, et al. SIGN: Scalable inception graph neural networks[EB/OL]. (2020-04-23)[2024-04-10]. https://arxiv.org/abs/2004.11198.

[25] LI Q T, HE Y S, XU C, et al. Dual-augment graph neural network for fraud detection[C]//Proceedings of the 31st ACM International Conference on Information & Knowledge Management. New York: ACM, 2022: 4188-4192.

[26] HUANG M, LIU Y, AO X, et al. Auc-oriented graph neural network for fraud detection[C]//Proceedings of the ACM Web Conference 2022. New York: ACM, 2022: 1311-1321.

作者简介

于浩淼　男,2000年3月出生于河南省周口市. 现为北京航空航天大学软件学院硕士研究生. 主要研究方向为图神经网络与欺诈检测.
E-mail: yuhaomiao@buaa.edu.cn

刘　炜　男,1998年12月出生于内蒙古自治区呼和浩特市,现为北京航空航天大学软件学院硕士研究生,主要研究方向为图神经网络、机器学习与欺诈检测等.
E-mail: buaaliuwei@buaa.edu.cn

孟流畅　女,2002年4月出生于山东省德州市,现为北京航空航天大学软件学院硕士研究生,主要研究方向为射电望远镜数据处理、图像处理、图神经网络等.
E-mail: SY2321112@buaa.edu.cn

陈开睿　男,2000年8月出生于广东省珠海市,现为北京航空航天大学软件学院硕士研究生,主要研究方向为智能软件工程、代码翻译、持续学习等.
E-mail: SY2221103@buaa.edu.cn

宋　友　男,1973年8月出生于四川省乐山市. 现为北京航空航天大学软件学院教授、博士生导师. 主要研究方向为大数据分析、人机交互、科技金融、人工智能等. 中国电子学会会员编号:E190161439M.
E-mail: songyou@buaa.edu.cn