

基于多关系不平衡图的图神经网络欺诈检测

赵佳玉

西北师范大学数学与统计学院, 甘肃 兰州

收稿日期: 2023年10月23日; 录用日期: 2023年12月1日; 发布日期: 2023年12月13日

摘要

近年来, 为了挖掘图结构数据中包含的丰富的关系信息, 基于图神经网络的欺诈检测方法引起了人们的广泛关注。然而, 对于节点标签分布严重偏斜并且存在多种关系的图数据, 传统的图神经网络可能会表现不佳。为了解决多关系不平衡图上的欺诈检测问题, 本文提出了一种基于关系感知的图神经网络模型 (RA-GNN)。首先, 对目标节点进行基于节点相似度的Top-p邻居节点采样以改善节点标签分布不平衡问题; 其次, 在每种关系内部, 使用节点级注意力机制, 加强关键邻居节点对中心节点嵌入的影响, 聚合邻居信息得到每种关系下的邻居表示; 最后, 使用边级注意力机制自适应地学习每种关系下邻居表示的重要性, 实现关系感知的邻居信息聚合, 得到中心节点的嵌入向量并应用于欺诈检测任务。在真实欺诈检测数据集YelpChi和Amazon上的实验结果表明, 本文提出的RA-GNN模型与其他基于图神经网络的基线模型相比具有良好的欺诈检测性能, 并且所使用的核心模块有显著的增强效果。

关键词

欺诈检测, 多关系不平衡图, 图神经网络, 注意力机制

Graph Neural Network Fraud Detection Based on Multi-Relation Imbalanced Graph

Jiayu Zhao

College of Mathematics and Statistics, Northwest Normal University, Lanzhou Gansu

Received: Oct. 23rd, 2023; accepted: Dec. 1st, 2023; published: Dec. 13th, 2023

Abstract

In recent years, fraud detection methods based on graph neural networks have attracted much attention due to the rich relational information contained in graph-structured data. However, for graph data with severely skewed node label distribution and multiple relationships, traditional graph neural networks may perform poorly. In order to solve the fraud detection problem on mul-

ti-relationship unbalanced graphs, this paper proposes a relationship-aware graph neural network-based model (RA-GNN). First, Top-p neighbor node sampling based on node similarity is performed on target nodes to improve the problem of imbalanced node label distribution; second, within each relationship, a node-level attention mechanism is used to enhance the influence of key neighbor nodes on the central node embedding, and aggregate neighbor information to obtain neighbor representation under each relationship; Finally, an edge-level attention mechanism is used to adaptively learn the importance of the neighbor representation under each relationship to achieve relationship-awareness. Finally, using the edge-level attention mechanism to adaptively learn the importance of the neighbor representation under each relationship, the relationship-aware neighbor information is aggregated to obtain the embedding vector of the central node and applied to the fraud detection task. Experiments on both benchmark and real-world graph-based fraud detection tasks demonstrate that the proposed RA-GNN apparently outperforms other baselines.

Keywords

Fraud Detection, Multi- Relation Imbalanced Graph, Graph Neural Network, Attention Mechanism

Copyright © 2023 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

随着互联网的快速发展, 欺诈行为日益猖獗, 给个人、企业乃至整个社会带来了严重的经济损失和信誉风险。为了有效识别和预防欺诈行为, 研究者在金融[1] [2] [3] [4]、公共安全[5]、医疗[6] [7]等领域提出了各种各样的欺诈检测方法。由于欺诈行为具有多样性和复杂性, 使用图结构数据表示欺诈行为中包含的复杂关系, 能够更好的为欺诈检测提供有效的多角度信息。因此, 越来越多的研究人员开始使用图结构对现实世界中的欺诈行为关系进行建模, 构造基于图的欺诈检测模型[8] [9] [10] [11]。

一个欺诈检测的图数据集通常由良性节点、异常节点以及节点之间的关系边构成。基于图的欺诈检测旨在区分图数据中的异常节点和良性节点, 从本质上来说属于图上的半监督节点分类问题, 比如, 从信用卡交易数据中发现欺诈交易[12]、通过邮件发送信息确定垃圾邮件的发送者[13]、找出在线购物网站中发布的虚假评论[14]等。

随着图神经网络(Graph neural network, GNN)的发展, 如 GCN [15]、GAT [16]和 GraphSAGE [17]等。越来越多的 GNN 模型被广泛应用于欺诈检测任务, 如 SemiGNN [18]是一种半监督的异构图神经网络, 通过引入注意力机制及不同类型的损失函数来增强金融欺诈检测中的节点表示效果。GraphConsis [19]是一种解决欺诈检测中上下文不一致、特征不一致和关系不一致问题的异构图神经网络。NCI-GNN [20]是一种使用动态加权交叉熵损失函数和马尔科夫决策对邻域节点进行多层自适应聚合的图神经网络。CARE-GNN [21]是一个针对伪装的欺诈行为的图神经网络, 使用强化学习来增强 GNN 的聚合过程。基于 GNN 的欺诈检测模型先聚合邻居节点的信息, 为目标节点生成嵌入, 然后利用分类器检测节点嵌入是否存在异常。与传统的基于图的方法相比, 基于 GNN 的方法能够以端到端和半监督的方式进行训练, 节省大量的特征工程和数据标注成本[22]。

然而, 在欺诈检测任务中, 欺诈节点的数量远远少于良性节点。例如, 在 Yelp 网站上的真实评论数据集 YelpChi [23]中, 仅有 14.5%的评论是垃圾评论, 而其他评论为推荐评论, 那么预测结果将会很容易

被多数类样本主导，这也是 GNN 模型在类不平衡问题中性能较差的原因。近年来，人们致力于解决基于传统特征空间中的类不平衡问题，使用的主要方法可以分为重采样和重加权。重采样包括过采样和欠采样，过采样是通过重新抽样或生成新数据来增加少数类样本的数量，如人工少数类过采样(Synthetic Minority Over-Sampling Technique, SMOTE) [24]，自适应合成采样(Adaptive Synthetic Sampling, ADASYN) [25]等；欠采样是从多数类样本中选取一些剔除，使多数类和少数类样本数量相当，如 Easy Ensemble 算法[26]，但是欠采样可能会导致含有重要信息的样本丢失和过拟合的问题。重加权方法通过调整不同标签的权重来平衡节点标签的分布，如基于代价敏感的方法[27]或基于元学习的方法[28]。虽然传统特征空间中的类不平衡监督学习得到了很好的研究，但是用于处理图结构数据中的节点标签分布不平衡的图神经网络模型却没有得到充分的探索。

除此之外，在大规模异构图中，一个节点通常会与多种类型的关系相连，例如，在 Amazon [29]评论数据集中，两条评论可能由同一用户连接，也可能由同产品连接。假设一条评论存在异常，那么与这条评论通过共同的用户关系连接的另一条评论也可能是异常的，因为同一个欺诈用户往往会发布许多的欺诈评论。如果简单的平等对待异构图中的所有关系，即采用传统的拼接或平均操作来聚合所有关系下的节点[15] [16] [17] [30]，则无法从多个角度全面的获取邻居信息，使得异构图中包含的丰富语义信息无法被充分利用，从而限制图神经网络的表达能力。由此可见，在设计基于异构图的网络结构时，处理多关系下的邻居节点聚合问题是一个具有挑战性的任务。

为了解决上述两类问题，本文提出了一种适用于多关系类不平衡图的 GNN 欺诈检测模型(Relation-aware graph neural network, RA-GNN)。一方面，对于图中节点标签分布不平衡的问题，计算邻居节点与目标节点的相似度，使用 Top-p 采样得到与目标节点最相关的邻居节点集合；另一方面，对于多关系图的信息聚合问题，先后使用基于节点级和边级的注意力机制，自适应地学习每种关系下的权重，实现基于关系感知的信息聚合。本文在两个欺诈检测公开数据集上进行了大量实验，验证了所提模型 RA-GNN 的有效性。

2. 相关定义

2.1. 多关系不平衡图

给定一个图 $\mathcal{G}=(\mathcal{V},\mathcal{E},\mathcal{X},\mathcal{C})$ ，其中 $\mathcal{V}=\{v_1,\dots,v_n\}$ 表示节点集合， $\mathcal{E}=\{\mathcal{E}_1,\dots,\mathcal{E}_R\}$ 表示包含 R 种关系的边集合， $\mathcal{X}=\{x_1,\dots,x_N\}$ 表示节点的特征向量集合， \mathcal{C} 表示节点的标签集合。若在图 \mathcal{G} 中， \mathcal{C} 是包含两种类别的节点标签集合，其中多数类节点的数量与少数类节点的数量之比远大于 1，并且图中存在两种及以上的关系 R ，则称图 \mathcal{G} 为多关系不平衡图。

2.2. 基于图神经网络的欺诈检测

图神经网络是一种深度学习框架，通过邻域聚合的方式迭代更新图中节点的表示，在多关系不平衡图 \mathcal{G} 上，定义经过 l 次迭代后节点 v 的表示 $h_v^{(l)}$ 为：

$$h_v^{(l)} = \sigma \left(h_v^{(l-1)} \oplus \text{AGG}^{(l)} \left(\left\{ h_{u,r}^{(l-1)} : (v,u) \in \mathcal{E}_r^{(l)} \right\} \Big|_{r=1}^R \right) \right) \quad (1)$$

其中， $h_v^{(0)}$ 为节点 v 的原始输入特征， $h_v^{(l-1)}$ 为节点 v 在 $l-1$ 层的表示， $h_{u,r}^{(l-1)}$ 为节点 v 的邻居节点 u 在关系 r 下，第 $l-1$ 层的表示， $\mathcal{E}_r^{(l)}$ 为关系 r 在 $l-1$ 层的边集合， AGG 为聚合函数，如求和、均值或最大化聚合， σ 为激活函数， \oplus 表示向量结合的运算方式，如拼接或求和。

基于 GNN 的欺诈检测实质是一个在图上的节点分类任务，我们首先根据原始数据构造一个多关系不平衡图 \mathcal{G} ，图中每个节点都被标记为“欺诈”或“正常”，然后通过已知的节点信息来训练一个 GNN 检

测模型，最后使用该模型去预测未标记节点的标签类型，找出图中的“欺诈”节点。

3. 基于关系感知的 RA-GNN 欺诈检测模型

3.1. 模型概述

本文所提出的 RA-GNN 模型包括三个核心模块。首先，通过计算节点相似度进行邻居采样；其次，在每种关系内部，对中心节点的邻居特征采用节点级注意力聚合邻居信息；最后，对于每种关系下得到的邻居嵌入，使用边级注意力机制自适应地学习每种关系表示的重要性，整合得到中心节点的最终表示。

图 1 以两种关系的不平衡输入图为例展示了所提出的 RA-GNN 在第 l 层的主要框架。

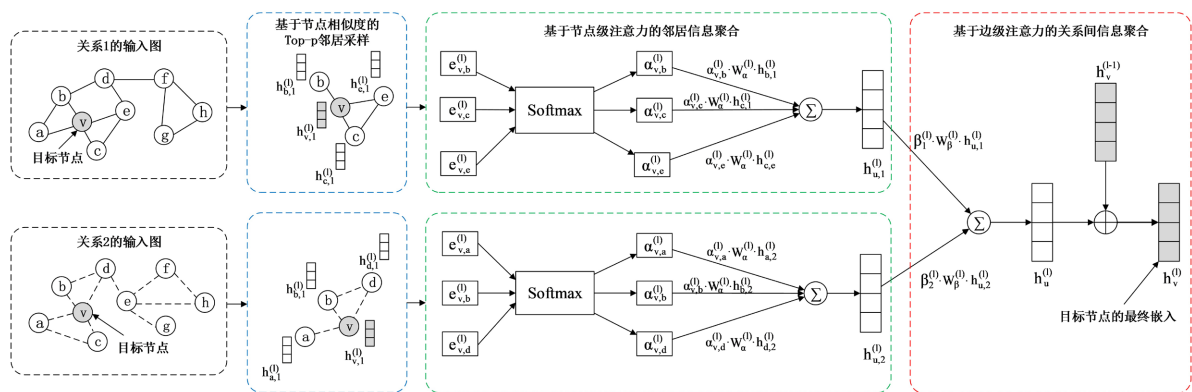


Figure 1. The framework of RA-GNN at layer l

图 1. RA-GNN 在第 l 层的主要框架图

3.2. 基于节点相似度的 Top-p 邻居采样

在大规模的多关系不平衡图中，正常节点的数量远多于欺诈节点的数量，若使用所有邻居信息聚合得到目标节点的表示，会使得模型训练时出现内存爆炸问题。受 GraphSAGE 的启发，本文对目标节点进行邻居采样，与 GraphSAGE 中固定采样规模不同，我们使用基于节点相似度的 Top-p 采样方法对每一层每个关系下的目标节点进行邻居采样。目标节点 v 在第 l 层，关系 r 下与其邻居节点 u 的相似性得分定义为：

$$S_r^{(l)}(v, u) = \exp\left(-\|h_{v,r}^{(l)} - h_{u,r}^{(l)}\|_2\right) \quad (2)$$

其中， $\|\cdot\|_2$ 表示向量的 l_2 正则化。计算得到目标节点与所有邻居节点的相似性得分之后，根据得分对邻居节点进行降序排列，定义采样阈值 $p_r^{(l)} \in (0, 1]$ ，则前 $p_r^{(l)} \cdot |S_r^{(l)}(v, u)|$ 个邻居为第 l 层所采样的邻居节点，将采样后在关系 r 下第 l 层得到邻居节点集合记为 $N_r^{(l)}$ 。

3.3. 基于节点级注意力机制的邻居聚合

在 3.2 中我们使用基于节点相似度的 Top-p 采样方法对中心节点进行邻居采样，接下来需要对中心节点的邻居信息进行聚合，得到中心节点的表示。传统的求和或平均聚合采用平等对待所有邻居节点的思想，无法区分邻居节点对中心节点的重要性程度，会忽略重要邻居节点对中心节点嵌入的影响，导致节点嵌入的准确性降低，从而对后续模型学习产生影响。为了充分利用不同程度的邻居信息，加强关键邻居节点对中心节点嵌入的影响。本文使用注意力机制为每个邻居节点计算注意力得分，为更重要的邻居节点分配更大的权重，并基于此进行邻居节点的关系内聚合。将注意力机制引入邻居节点的聚合是非

常有效的[3]，不仅可以通过并行计算提高运行效率，还能够容易地应用到归纳学习。在关系 r 下，计算中心节点 v 在第 l 层的邻居节点 u 重要性得分：

$$e_{v,u}^{(l)} = \text{LeakyReLU}\left(a^{(l)T} \left[W_{\alpha}^{(l)} h_{v,r}^{(l)} \parallel W_{\alpha}^{(l)} h_{u,r}^{(l)} \right]\right) \quad (3)$$

其中， $W_{\alpha}^{(l)}$ 为可训练的线性变换参数， $a^{(l)}$ 是将输入映射到 R 的权重向量， \parallel 表示向量拼接操作，使用 softmax 对重要性得分进行标准化得到邻居节点 u 的注意力系数为：

$$\alpha_{v,u}^{(l)} = \frac{\exp\left(e_{v,u}^{(l)}\right)}{\sum_{u \in N_r^{(l)}} \exp\left(e_{v,u}^{(l)}\right)} \quad (4)$$

则第 l 层，关系 r 下，邻居信息的最终嵌入为：

$$h_{u,r}^{(l)} = \sum_{u \in N_r^{(l)}} \alpha_{v,u}^{(l)} W_{\alpha}^{(l)} h_{u,r}^{(l)} \quad (5)$$

3.4. 基于边级注意力机制的关系间聚合

在一个多关系图中，节点之间的不同连接关系通常包含不同的语义信息，在得到每个关系内的节点表示之后，需要将不同关系下的邻居信息进行聚合，得到目标节点的最终表示。对于不同关系下的节点嵌入，若采用平均的方式聚合，将不可避免地削弱多关系图中关键连接所包含的重要信息，而采用拼接的方式聚合，则会提升计算复杂度并降低模型运行效率，从而限制图神经网络的表达能力。为了以更加高效的方式聚合邻居信息并且充分利用不同关系所包含的不同程度的语义信息，本文引入基于边级的注意力机制，对节点间存在的不同关系，实现关系感知的聚合策略，即通过注意力机制端到端的学习不同关系下的权重，通过对重要关系分配更高的权重，既能实现节点信息的有效利用，也有助于提高下游任务的预测准确性。

与 3.3 中计算注意力权重的思想相似，每个关系的注意力得分分为：

$$e_r^{(l)} = \text{LeakyReLU}\left(q^{(l)T} \left[W_{\beta}^{(l)} h_v^{(l)} \parallel W_{\beta}^{(l)} h_{u,r}^{(l)} \right]\right) \quad (6)$$

其中， $W_{\beta}^{(l)}$ 为可训练的线性变换参数， $q^{(l)}$ 是权重向量，对应的标准化注意力权重为：

$$\beta_r^{(l)} = \text{softmax}\left(e_r^{(l)}\right) = \frac{\exp\left(e_r^{(l)}\right)}{\sum_{r \in R} \exp\left(e_r^{(l)}\right)} \quad (7)$$

则中心节点的最终邻居向量可以由关系感知的注意力机制表示为：

$$h_u^{(l)} = \sum_{r \in R} \beta_r^{(l)} W_{\beta}^{(l)} h_{u,r}^{(l)} \quad (8)$$

可以看出，通过引入边级注意力机制能够聚合具有不同重要性程度的关系下的邻居信息，结合 3.3，则第 l 层中心节点的嵌入可以使用下式进行更新：

$$h_v^{(l)} = \sigma\left(h_v^{(l-1)} \parallel h_u^{(l)}\right) \quad (9)$$

3.5. 模型训练

本文在聚合过程之后，通过梯度下降和最小化交叉熵损失，进行模型训练和优化模型参数。对于节点 v ， $h_v^{(l)}$ 为最后一层的表示也是最终嵌入，则损失函数可以定义为：

$$\mathcal{L} = -\sum_{v \in V} [y_v \log p_v + (1 - y_v) \log(1 - p_v)]$$

$$p_v = MLP(h_v^{(L)})$$
(10)

由于模型学习到的参数可以被传递和共享，因此该模型支持在大规模的多关系不平衡图上进行关系感知的归纳学习。

4. 实验设计与分析

4.1. 实验设置

4.1.1. 数据集

本文选择了两个被广泛应用于欺诈检测的公开数据集进行实验。YelpChi [23]是从 Yelp 网站上获取的用户对酒店和餐馆的评论数据集。Amazon [29]收集了用户在亚马逊网站上购买乐器的产品评论数据集。上述两个数据集都是多关系不平衡图数据，其中，节点由 100 维特征表示，并且节点具有标签“0”或“1”，0 代表该节点是良性节点，1 代表该节点为欺诈节点。除此之外，节点之间都存在三种关系。这两个数据集的统计信息和三种关系的定义如下表 1 所示。

Table 1. The statistics of datasets

表 1. 数据集的统计信息

| 数据集 | 节点数 | 欺诈节点比例 | 边数 | 关系 | 关系数 |
|---------|--------|--------|-----------|-----------------------|-----------|
| YelpChi | 45,954 | 14.5% | 3,846,979 | R-U-R:同一用户发表的评论 | 49,315 |
| | | | | R-S-R:同一产品相同星级的评论 | 3,402,743 |
| | | | | R-T-R:同一产品在同月发表的评论 | 573,616 |
| Amazon | 11,944 | 9.5% | 4,398,392 | U-P-U:至少在一个相同产品评论的用户 | 175,608 |
| | | | | U-S-U:一周内至少有一个相同评级的用户 | 3,566,479 |
| | | | | U-V-U:互评文本相似度最高的5%用户 | 1,036,737 |

4.1.2. 对比模型

本文选择了几个先进的基于 GNN 的模型用于验证本文所提出的 RA-GNN 模型的有效性。

GCN [15]: 一个基于谱图卷积操作提取拓扑图中空间特征的图卷积神经网络。

GAT [16]: 一个基于注意力机制进行节点聚合的图注意力网络。

GraphSAGE [17]: 一个基于邻域采样器和平均聚合器的归纳图表示学习算法。

GraphConsis [20]: 一个用于解决欺诈检测中存在的非一致性的图神经网络。

CARE-GNN [21]: 一个用于解决欺诈检测中存在的伪装问题的图神经网络。

4.1.3. 实验环境

本文所有模型的实验环境配置如表 2 所示。

Table 2. Experimental environment configuration

表 2. 实验环境配置

| 实验环境 | 配置 |
|--------|-----------------|
| 操作系统 | Windows 11 64 位 |
| CPU | AMD Ryzen 7 |
| GPU | NVIDIA RTX3060 |
| 内存 | 16G |
| 编程语言 | python 3.8 |
| 深度学习框架 | Pytorch 1.12.0 |

4.1.4. 参数设置

本文所有模型使用的主要参数如表 3 所示。

Table 3. Experimental parameter setting
表 3. 实验参数设置

| 实验参数 | 定义 | 设置 |
|----------------|-----------|------|
| Batchsize | 批量大小 | 1024 |
| Epoch | 迭代次数 | 100 |
| Embedding size | 最终生成的嵌入维度 | 64 |
| Learning rate | 学习率 | 0.01 |
| Layer number | 图神经网络层数 | 1 |
| Optimizer | 优化器 | Adam |
| Test size | 测试数据比例 | 0.4 |

4.1.5. 评价指标

由于欺诈检测数据集存在明显的分布不平衡，因此所选的评价指标不应过分依赖多数类样本，而需要充分关注模型对少数类样本的分类能力。本文选取了四个基于混淆矩阵的评价指标来衡量模型的性能，它们分别是 *Recall*、*F1-score* 和 *AUC*。每个评价指标都可以由 *TP*、*FN*、*FP* 和 *TN* 计算得出，其中 *TP* 是真正类，*FN* 是假负类，*FP* 是假正类，*TN* 是真负类。此外，通过计算真正类率 *TPR* 和假负类率 *FPR*，并以 *FPR* 为横轴，以 *TPR* 为纵轴可以绘制出 *ROC* 曲线，曲线下的面积则代表 *AUC*。上述指标的计算见公式(11)-(14)。

$$Recall = \frac{TP}{TP + FN} \quad (11)$$

$$F1-score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (12)$$

$$TPR = \frac{TP}{TP + FN} \quad (13)$$

$$FPR = \frac{FP}{FP + TN} \quad (14)$$

4.2. 性能比较

本文在 YelpChi 和 Amazon 数据集上测试 RA-GNN 以及五个基于 GNN 的基线模型在欺诈检测任务中的性能。表 4 展示了所有模型在运行 100 个迭代周期后的评价指标。可以看出，本文所提出的 RA-GNN 在所有评价指标下都优于其他基线。

Table 4. The performance comparison on YelpChi and Amazon
表 4. 在 YelpChi 和 Amazon 数据集上的模型性能比较

| 模型 | YelpChi | | | Amazon | | |
|-------------|---------------|---------------|---------------|---------------|---------------|---------------|
| | F1 | AUC | Recall | F1 | AUC | Recall |
| GCN | 0.5533 | 0.5281 | 0.5211 | 0.6598 | 0.7478 | 0.6680 |
| GAT | 0.4649 | 0.5744 | 0.5386 | 0.6851 | 0.8102 | 0.6748 |
| GraphSAGE | 0.5471 | 0.5464 | 0.5266 | 0.6495 | 0.7635 | 0.7036 |
| GraphConsis | 0.6070 | 0.7285 | 0.6208 | 0.7837 | 0.8407 | 0.8450 |
| CARE-GNN | 0.6138 | 0.7705 | 0.7038 | 0.7857 | 0.8730 | 0.8367 |
| RA-GNN | 0.6616 | 0.7859 | 0.7077 | 0.8228 | 0.8862 | 0.8527 |

在所有基线模型中，GCN、GAT 和 GraphSAGE 仅能在同构图上运行，因此将数据集中的所有关系合并在一起进行测试。GCN、GAT 是传统的图神经网络方法，在不平衡的欺诈数据集中少数类的样本无法得到充分的训练，同时也忽略了节点之间包含的重要关系信息，因此他们的性能在所有对比模型中是最差的。GraphSAGE 是具有代表性的基于采样的方法，分别采用节点采样和图采样。但是 GraphSAGE 在采样时保持固定大小的邻域，对于邻域较大的节点，会造成信息丢失从而降低其性能。GraphConsis 和 CARE-GNN 是两种最先进的基于多关系图的欺诈检测方法，分别关注不一致性和伪装问题。而 CARE-GNN 比 GraphConsis 更好地采用了标签相似性度量和自适应采样阈值，因此显示出较好的性能。本文所提的 RA-GNN 在关系内对邻居节点使用节点级注意力聚合不同重要程度的邻居信息，在关系间使用边级注意力实现关系感知的信息聚合。在两个数据集上的实验结果都表明，RA-GNN 优于上述所有对比模型。

4.3. 消融研究

为了验证 RA-GNN 中两个关键步骤，即聚合邻居信息的节点级注意力和关系感知的边级注意力，通过分别移除这两个模块来验证其有效性。将移除节点级注意力的模型记为 $RA-GNN_{\setminus A}$ ，将移除关系感知注意力的模型记为 $RA-GNN_{\setminus R}$ ，在图 2 中展示了在 YelpChi 和 Amazon 数据集上进行的模型消融研究结果。从图中我们可以观察到，与去除两个关键步骤的变体模型相比，RA-GNN 在三个评价指标上均具有最佳表现，说明这两个模块能够有效提升模型检测效果。从 YelpChi 数据集上的实验结果中可以发现，两种变体模型在移除关键步骤后，图神经网络的性能明显下降。除此之外，在 Amazon 数据集中能够更清楚地看出 $RA-GNN_{\setminus R}$ 在移除关系感知注意力后，损失了不同关系的重要性及语义信息，导致模型在多关系图中的表现不佳。由此可以得出结论，引入聚合邻居信息的节点级注意力和关系感知的边级注意力，能够有效提升图神经网络在多关系图上的欺诈检测性能。

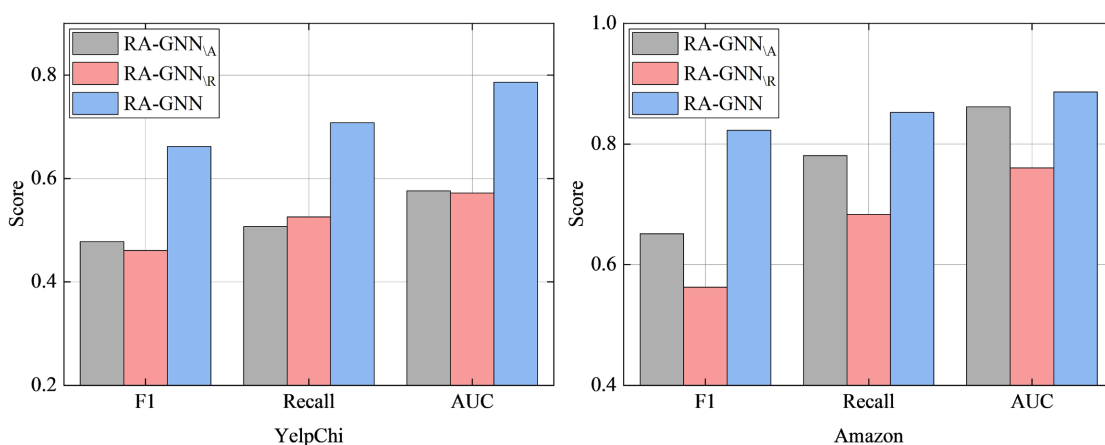


Figure 2. The ablation study results on YelpChi and Amazon

图 2. 在 YelpChi 和 Amazon 数据集上的消融研究结果

4.4. 参数敏感性分析

为了评估 RA-GNN 在不同训练参数下的性能，本文选取四个主要的模型超参数，在 YelpChi 数据集上进行了参数敏感性实验。图 3 展示了 RA-GNN 在 YelpChi 数据集上关于四个超参数的测试性能。从图 3(a)中，我们观察到增加批量大小会提升 F1 和 Recall，而对 AUC 的影响不是很明显；图 3(b)展示了不同的最终嵌入维度下模型的性能，可以发现维度在 64 时，模型能体现出较好的性能；从图 3(c)中可以发现，

迭代次数为 40, 60 和 80 时, 模型性能没有较为明显的变化, 说明迭代次数的增加并不会显著提升模型性能; 图 3(d)说明学习率不宜设置太小或太大, 当学习率设置为 0.01 时有更好的预测结果。

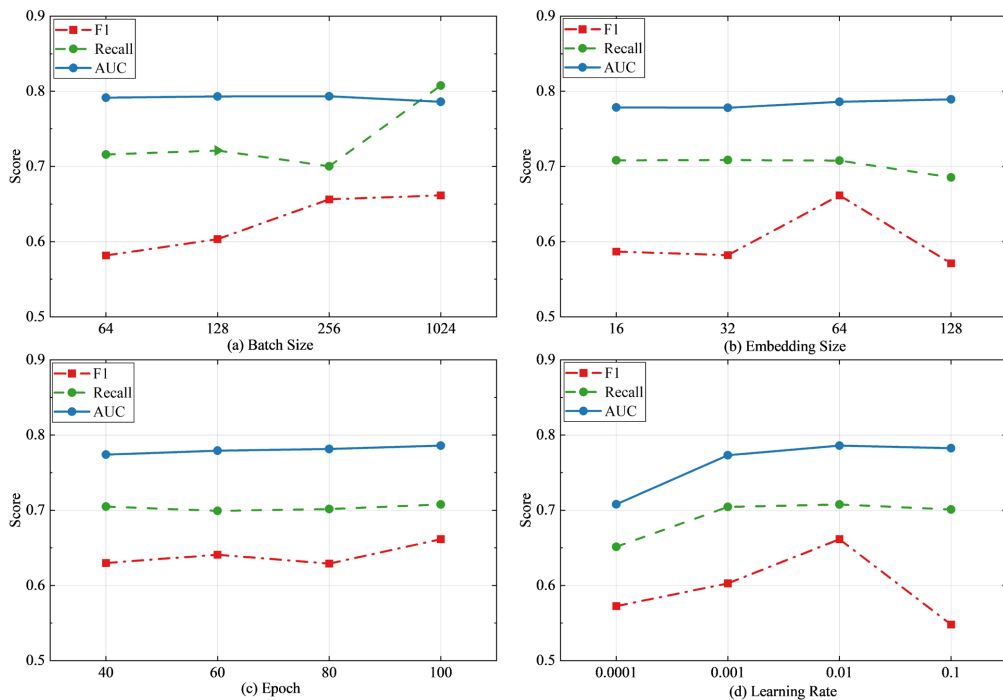


Figure 3. The parameter sensitivity analysis on YelpChi
图 3. YelpChi 数据集上的参数敏感性分析

5. 结论

为了提升图神经网络在多关系不平衡图中的欺诈检测性能, 本文提出一种基于关系感知的图神经网络欺诈检测模型 RA-GNN。首先, 针对不平衡图中存在的正负样本数量差异较大的问题, 对目标节点进行基于节点相似度的 Top-p 邻居节点采样; 其次, 对于关系图中包含的每种关系内部, 使用节点级注意力机制聚合邻居信息, 通过为不同重要性程度的邻居节点分配不同的权重, 加强关键邻居节点对中心节点嵌入的影响; 最后, 将每种关系下得到的邻居嵌入, 使用边级注意力机制自适应地学习每种关系表示的重要性, 整合得到中心节点的最终嵌入向量应用到下游的欺诈检测任务。本文在真实欺诈检测数据集 YelpChi 和 Amazon 上进行了广泛实验, 实验结果表明, 所提出的 RA-GNN 模型与其他基线相比具有良好的欺诈检测性能, 并且所使用的核心模块有显著的增强效果。下一步将尝试把 RA-GNN 应用到其他基于多关系不平衡图的任务中, 同时将探索欺诈检测任务中存在的时空模式。

参考文献

- [1] Carcillo, F., Borgne, Y.L., Caelen, O., *et al.* (2021) Combining Unsupervised and Supervised Learning in Credit Card Fraud Detection. *Information Sciences*, **557**, 317-331. <https://doi.org/10.1016/j.ins.2019.05.042>
- [2] Liu, C., Zhong, Q.W., Ao, X., *et al.* (2020) Fraud Transactions Detection via Behavior Tree with Local Intention Calibration. *Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Diego, 23-27 August 2020, 3035-3043. <https://doi.org/10.1145/3394486.3403354>
- [3] Wu, J.F., Yao, M.F., Wu, D., *et al.* (2023) DEDGAT: Dual Embedding of Directed Graph Attention Networks for Detecting Financial Risk.

- [4] 刘华玲, 刘雅欣, 许珺怡, 等. 图异常检测在金融反欺诈中的应用研究进展[J]. 计算机工程与应用, 2022, 58(22): 41-53.
- [5] Karami, A. (2018) An Anomaly-Based Intrusion Detection System in Presence of Benign Outliers with Visualization Capabilities. *Expert Systems with Applications*, **108**, 36-60. <https://doi.org/10.1016/j.eswa.2018.04.038>
- [6] 易东义, 邓根强, 董超雄, 等. 基于图卷积神经网络的医保欺诈检测算法[J]. 计算机应用, 2020, 40(5): 1272-1277.
- [7] Kumar, M., Ghani, R. and Mei, Z.S. (2010) Data Mining to Predict and Prevent Errors in Health Insurance Claims Processing. *Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Washington DC, 25-28 July 2010, 65-74. <https://doi.org/10.1145/1835804.1835816>
- [8] Wang, H.R., Dou, Y.T., Chen, C.Y., et al. (2023) Attacking Fake News Detectors via Manipulating News Social Engagement. *Proceedings of the ACM Web Conference*, Austin, 30 April-4 May 2023, 3978-3986. <https://doi.org/10.1145/3543507.3583868>
- [9] Zhao, L., Sawlani, S., Srinivasan, A. and Akoglu, L. (2022) Graph Anomaly Detection with Unsupervised GNNs.
- [10] Boniol, P., Palpanas, T., Meftah, M. and Remy, E. (2020) GraphAn: Graph-Based Subsequence Anomaly Detection. *Proceedings of the VLDB Endowment*, **13**, 2941-2944. <https://doi.org/10.14778/3415478.3415514>
- [11] Pourhabibi, A., Ong, K.L., Kam, B.H. and Boo, Y.L. (2020) Fraud Detection: A Systematic Literature Review of Graph-Based Anomaly Detection Approaches. *Decision Support Systems*, **133**, Article ID: 113303. <https://doi.org/10.1016/j.dss.2020.113303>
- [12] Xiang, S., Zhu, M.Z., Cheng, D.W., et al. (2023) Semi-Supervised Credit Card Fraud Detection via Attribute-Driven Graph Representation. *Proceedings of the AAAI Conference on Artificial Intelligence*, **37**, 14557-14565. <https://doi.org/10.1609/aaai.v37i12.26702>
- [13] Alam, A.Z., Faris, H., Alqatawna, J., et al. (2018) Evolving Support Vector Machines Using Whale Optimization Algorithm for Spam Profiles Detection on Online Social Networks in Different Lingual Contexts. *Knowledge-Based Systems*, **153**, 91-104. <https://doi.org/10.1016/j.knsys.2018.04.025>
- [14] Nguyen, T.T., Phan, T.C., Pham, H.T., et al. (2023) Example-Based Explanations for Streaming Fraud Detection on Graphs. *Information Sciences*, **621**, 319-340. <https://doi.org/10.1016/j.ins.2022.11.119>
- [15] Defferrard, M., Bresson, X.V. and Ergheynst, P. (2016) Convolutional Neural Networks on Graphs with Fast Localized Spectral Filtering. *Proceedings of the 30th International Conference on Neural Information Processing Systems*, Barcelona, 5-10 December 2016, 3844-3852.
- [16] Veličković, P., Cucurull, G., Casanova, A., et al. (2018) Graph Attention Networks. *International Conference on Learning Representations*, Vancouver, 30 April-3 May 2018, 1-12.
- [17] Hamilton, W., Ying, Z. and Leskovec, J. (2017) Inductive Representation Learning on Large Graphs. *Proceedings of the 31st International Conference on Neural Information Processing Systems*, Long Beach, 4-9 December 2017, 1025-1035.
- [18] Wang, D., Lin, J., Cui, P., et al. (2019) A Semi-Supervised Graph Attentive Network for Financial Fraud Detection. *IEEE International Conference on Data Mining*, Beijing, 8-11 November 2019, 598-607. <https://doi.org/10.1109/ICDM.2019.00070>
- [19] 陈安琪, 陈睿, 邝祝芳, 等. 基于图神经网络的不平衡欺诈检测研究[J]. 计算机工程, 2023, 49(11): 150-159.
- [20] Liu, Z., Dou, Y., Yu, P.S., et al. (2020) Alleviating the Inconsistency Problem of Applying Graph Neural Network to Fraud Detection. *Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval*, 25-30 July 2020, 1569-1572. <https://doi.org/10.1145/3397271.3401253>
- [21] Dou, Y., Liu, Z., Sun, L., et al. (2020) Enhancing Graph Neural Network-based Fraud Detectors against Camouflaged Fraudsters. *Proceedings of the 29th ACM International Conference on Information and Knowledge Management*, 19-23 October 2020, 315-324. <https://doi.org/10.1145/3340531.3411903>
- [22] 段福先. 基于异构图神经网络的欺诈检测研究[D]: [硕士学位论文]. 南昌: 华东交通大学, 2022.
- [23] Rayana, S. and Akoglu, L. (2015) Collective Opinion Spam Detection: Bridging Review Networks and Metadata. *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Sydney, 10-13 August 2015, 985-994. <https://doi.org/10.1145/2783258.2783370>
- [24] Chawla, N., Bowyer, K., Hall, L., et al. (2002) SMOTE: Synthetic Minority Over-Sampling Technique. *Journal of Artificial Intelligence Research*, **16**, 321-357. <https://doi.org/10.1613/jair.953>
- [25] He, H.B., Bai, Y., et al. (2008) ADASYN: Adaptive Synthetic Sampling Approach for Imbalanced Learning. *IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence)*, Hong Kong, 1-8 June 2008, 1322-1328.

-
- [26] Liu, X.Y., Wu, J.X., Zhou, Z.H., *et al.* (2008) Exploratory Under-Sampling for Class-Imbalance Learning. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, **39**, 539-550. <https://doi.org/10.1109/TSMCB.2008.2007853>
- [27] Li, X.Y., Sun, X., Meng, Y.X., *et al.* (2020) Dice Loss for Data-Imbalanced NLP Tasks. *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*, 5-10 July 2020, 465-476. <https://doi.org/10.18653/v1/2020.acl-main.45>
- [28] Shu, J., Xie, Q. and Yi, L.X. (2019) Meta-Weight-Net: Learning an Explicit Mapping for Sample Weighting. *Proceedings of the 33rd International Conference on Neural Information Processing Systems*, Vancouver, 8-14 December 2019, 1919-1930.
- [29] Mcauley, J.J. and Leskovec, J. (2013) From Amateurs to Connoisseurs: Modeling the Evolution of User Expertise through Online Reviews. *Proceedings of the 22nd International Conference on World Wide Web*, Rio de Janeiro, 13-17 May 2013, 897-908. <https://doi.org/10.1145/2488388.2488466>
- [30] Wang, X., Zhu, M.Q., Bo, D.Y., *et al.* (2020) AMGCN: Adaptive Multi-Channel Graph Convolutional Networks. *Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 23-27 August 2020, 1243-1253. <https://doi.org/10.1145/3394486.3403177>