基于多视角图神经网络的欺诈检测算法

陈卓，朱淼，杜军威
（青岛科技大学信息科学技术学院，山东 青岛 266061）

摘 要：针对欺诈检测领域样本标签不平衡、欺诈节点之间缺乏必要连接，导致欺诈检测任务不符合图神经网络同质性假设的问题，提出了基于多视角图神经网络的欺诈检测（MGFD）算法。首先，利用结构无关的编码器对网络中节点进行属性编码，以学习欺诈节点与正常节点之间的差异，使用层次注意力机制对网络中多视角信息进行融合，在学习差异的基础上充分利用网络中不同视角之间的交互信息对节点进行建模；然后，基于数据不平衡比采样子图，依据欺诈节点连接特性构建样本进行分类学习，解决样本标签不平衡的问题；最后，预测标签判别节点是否为欺诈节点。在公开数据集上的实验表明，MGFD 算法在基于图的欺诈检测领域检测效果优于对比方法。

关键词：欺诈检测；异常检测；注意力机制；图表示学习；不平衡学习
中图分类号：TP183
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2022221

Multi-view graph neural network for fraud detection algorithm

CHEN Zhuo, ZHU Miao, DU Junwei
School of Information Science and Technology, Qingdao University of Science and Technology, Qingdao 266061, China

Abstract: Aiming at the problem that in the field of fraud detection, imbalance labels and lack of necessary connections between fraud nodes, resulting in fraud detection tasks not conforming to the hypothesis of homogeneity of graph neural networks, multi-view graph neural network for fraud detection (MGFD) algorithm was proposed. First, A structure-independent encoder was used to encode the attributes of nodes in the network to learn the difference between the fraud node and the normal node. The hierarchical attention mechanism was designed to integrate the multi-view information in the network, and made full use of the interaction information between different perspectives in the network to model the nodes on the basis of learning differences. Then, based on the data imbalance ratio sampled subgraph, the sample was constructed according to the connection characteristics of fraud nodes for classification, which solved the problem of imbalance sample labels. Finally, the prediction label was used to identify whether a node is fraudulent. Experiments on real-world datasets have shown that the MGFD algorithm outperforms the comparison method in the field of graph-based fraud detection.

Keywords: fraud detection, anomaly detection, attention mechanism, graph representation learning, imbalance learning

0 引言

欺诈行为是指对事实错误的表达，是以使人发生错误认识为目的的故意行为。欺诈有多种类别，包括社交网络中的虚假信息、金融欺诈[1]、广告流量欺诈等，有效检测出欺诈行为对安全、金融等领域发展有着至关重要的作用。

由于图可以对现实世界中的关系进行良好建模，研究者将图神经网络（GNN, graph neural network）运用到欺诈检测中。基于图的异常检测方法是识别可疑

收稿日期：2022–07–25；**修回日期：**2022–09–30
基金项目：国家自然科学基金资助项目（No.62172249, No.61973180, No.62202253）；山东省自然科学基金资助项目（No.ZR2021MF092）
Foundation Items: The National Natural Science Foundation of China (No.62172249, No.61973180, No.62202253), The Natural Science Foundation of Shandong Province (No.ZR2021MF092)

行为最常用的技术之一[2]。

FRAUDER（fraud detection dual-resistant）[3]利用图结构无关的编码器学习欺诈节点和相邻正常节点不同的表示，从而判别欺诈节点和正常节点；而 semiGNN[4]从节点的多视角信息出发，利用层次注意力聚合节点不同视角之间的信息，学习了不同节点之间的交互以及不同视角之间的关系，以此进行分类。

然而，在欺诈检测任务中，欺诈者的数量远少于正常用户的数量，以 Amazon 数据集为例[5]，只有 9.5%的用户是欺诈者，而其他用户则是正常的。类不平衡问题使现有的欺诈检测算法在多数类中过拟合，忽略了少数类的特征，从而导致检测效果差。此外，在现实生活中，欺诈者通常连接大量的正常用户以实施欺诈行为，欺诈节点之间缺乏必要的连接，这可能导致欺诈者信息被隐藏在正常信息中，研究者将之称为欺诈者伪装行为。由于图神经网络的效果依赖于同质性假设，即距离相近的节点具有相似的信息，简单的图神经网络在聚合邻居节点信息后易掩盖其中的欺诈信息，难以识别欺诈节点，这也是欺诈检测任务的难点之一。现有研究[6-7]通过重采样的方法过滤掉欺诈节点相邻的正常节点以满足 GNN 的同质性假设。同时，利用重采样的方法对正常节点进行欠采样，对欺诈节点进行过采样也可以解决类不平衡问题。但图神经网络容易被一些微小的扰动迷惑[8]，特别是若某一层删减了过多的边，随着图结构的演化将会导致 GNN 过平滑。

针对上述问题，本文提出基于多视角图神经网络的欺诈检测（MGFD, multi-view graph neural network for fraud detection）算法，结合结构无关的编码器和层次注意力思想构建多视角特征嵌入模块，利用节点与子图对构建学习样本，并设计标签从而解决欺诈检测中的类不平衡问题，最终预测标签来判断节点是否为欺诈节点。本文的工作主要有以下几点。

1) 设计多视角特征嵌入模块，首先使用结构无关的编码器学习欺诈节点与正常节点之间的差异性表示，再利用层次注意力机制融合节点多视角信息，学习节点不同关系之间的信息，利用包含丰富信息的表示解决欺诈者伪装问题。

2) 构建节点与子图对，设计实例对标签以平衡数据的类别，通过学习正常节点与欺诈节点的差异使节点和子图对不断拟合标签，最终预测标签来判断节点类别，在不改变图结构的条件下解决类不平衡问题。

3) 在公开数据集中进行广泛的实验，验证算法检测欺诈节点的有效性。

1 问题的提出

1.1 相关定义和问题描述

本节首先给出不平衡比、多关系不平衡图、节点子图相关定义，然后给出针对图异常检测问题的形式化描述。

定义 1 不平衡比。给定标签集合 C，C_1、C_2 为 C 中的 2 个类别，C_1、C_2 不平衡比定义为 $\mathrm{IR}=\dfrac{|C_1|}{|C_2|}$，$\mathrm{IR}\in[0,+\infty)$。若 $\mathrm{IR}>1$，则 C_1 为多数类，C_2 为少数类；若 $\mathrm{IR}=1$，则 C 中的类别均衡。

定义 2 多关系不平衡图。给定图 $G=(V,\boldsymbol{\varepsilon},A,X,C)$，其中，$V=\{v_1,\cdots,v_N\}$ 是节点的集合，$\varepsilon=\{\varepsilon_1,\cdots,\varepsilon_R\}$ 是 R 种关系的边的集合，$A=\{\boldsymbol{A}_1,\cdots,\boldsymbol{A}_R\}$ 是 R 种关系对应的邻接矩阵集合。对于每个节点 $v_i\in V$，$\boldsymbol{x}_i\in X$ 是 d 维的特征向量，$c_i\in C$ 为节点 v_i 的标签。X和C 分别为节点特征集合和节点标签集合。如果 C 中的 2 个类别之间的不平衡比远大于 1，则称图 G 为多关系不平衡图。

定义 3 节点子图。给定节点 v_i，由游走算法得到节点 i 的第 k 个子图为 $g_i^k=(V_i^k,H_i^k)$。其中，$V_i^k=\{v_{i1}^k,v_{i2}^k,\cdots,v_{in}^k\}$ 为子图中的节点集合且 $|V_i^k|=n_i$；$\boldsymbol{H}_i^k\in R^{n_i\times d}$ 为节点表示矩阵，该矩阵行向量 $\boldsymbol{h}_{iw}^k\in R^d$ 为子图中第 w 个节点，d 为节点表示维度。

问题描述：基于图的欺诈检测。在多关系不平衡图 $G=(V,\varepsilon,A,X,C)$ 中，节点被标记为欺诈节点或正常节点。基于图的欺诈检测的目的是在多关系不平衡图 G 上发现欺诈节点与正常节点之间的显著差异，也可以表述为不平衡节点分类问题。

1.2 相关工作

下面，从基于图的欺诈检测和不平衡学习两方面介绍本文的相关工作。

1.2.1 基于图的欺诈检测

GraphRAD（graph-based risky account detection）[9]将图神经网络运用于欺诈检测任务，以欺诈节点为种子节点，向外发散生成局部社区，从而通过学习账户之间的关系图检测有潜在风险的账户。双向图卷积网络（Bi-GCN, bi-directional graph convolutional network）[10]使用图卷积网络检测社交网络中

的谣言，提出谣言源头和末端双向图模型，从而从深度和广度两方面检测谣言。文献[11]提供了一种新的异质信息网络节点聚合方法，针对用户节点、评论节点以及商品节点分别提出聚合器，聚合各自邻居节点的信息，同时通过评论之间的相似性，构建了一个同质的评论图，从而检测虚假的评论。这些方法结合数据特性利用图神经网络进行欺诈检测，但没有考虑到欺诈节点伪装以及样本不平衡问题。近期，部分工作针对欺诈者伪装以及类不平衡问题对网络进行改进，如 GraphConsis[6]提供了一种新的 GNN 框架用于解决欺诈者伪装问题，在聚合邻居节点时通过度量节点之间的一致性过滤不一致的节点，学习欺诈节点之间潜在的特征，从而对节点进行分类。CARE-GNN（camouflage resistance-GNN）[7]基于强化学习的方法学习节点的最优邻居节点数，利用标签相似度对邻居节点进行选择，以解决欺诈者的伪装问题。上述方法虽然可以在一定程度上解决欺诈者伪装问题，但检测效果仍受标签不平衡限制，且在相邻层网络中输入不同的图结构易使网络训练不稳定。

1.2.2　不平衡学习

由于欺诈检测任务中欺诈节点远少于正常节点，欺诈检测涉及不平衡分类问题。现有的不平衡分类方法可分为重采样和重加权。重采样又可进一步分为过采样和欠采样。SMOTE（synthetic minority over-sampling technique）[12]是一种典型的重采样插值方法，通过对少数类过采样和多数类欠采样获得更好的分类结果。Wang 等[13]提出通过生成少数类样本以实现过采样。Chi 等[14]提出基于元学习的强化学习以学习欠采样。重加权算法可以通过成本敏感方法[15]和基于元学习的方法[16]实现。Cao 等[15]提出了感知标签分布的边缘损失，并将重加权与损失相结合以解决类不平衡问题。Hu 等[16]将监督学习和强化学习相结合，利用强化学习奖励动态调整数据加权。

目前，针对解决图数据中类不平衡问题的研究仍然较少。Shi 等[17]对图数据中类不平衡问题进行研究，提出了一种包含 2 种正则化的新型图卷积网络，训练所有未标记节点使其与训练良好的节点具有类似的数据分布从而促进不同类之间的平衡训练。该算法的局限性在于难以泛化到大规模图上。Zhao 等[18]提出通过生成节点和边进行过采样以平衡分类。由于不断生产新的图结构，这种方法有可能降低基于 GNN 方法的稳健性。

2　基于多视角图神经网络的欺诈检测

为了学习欺诈节点和正常节点之间显著差异并解决类不平衡问题，本文提出了 MGFD 算法，其由多视角特征嵌入、构建节点子图对标签、欺诈节点判别三部分组成，算法架构如图 1 所示。首先使用结构无关的编码器增强欺诈节点与正常节点之间的差异，基于层次注意力聚合节点得到包含节点多视角信息的差异化表示；然后，进行子图采样，基于不同类别的节点特性构建节点子图对标签，解决类不平衡问题并学习正常节点与欺诈节点之间的不一致信息；最后，判别标签得出节点是否为欺诈节点。

2.1　多视角特征嵌入

由于欺诈节点与正常节点具有不同的特征，但两者在拓扑结构上联系紧密，直接聚合邻居节点信息会平滑欺诈节点潜在的特征，因此在进行信息聚合之前，首先基于节点属性对节点进行结构无关编码，即在对节点属性进行编码时不考虑节点的结构信息，如式(1)所示。

$$h_i = \sigma(\boldsymbol{x}_i \boldsymbol{W}_e) \tag{1}$$

其中，$\boldsymbol{x}_i$ 为节点 v_i 的特征向量；σ 为非线性激活函数，对节点属性进行非线性变换；$\boldsymbol{W}_e$ 为可学习的权

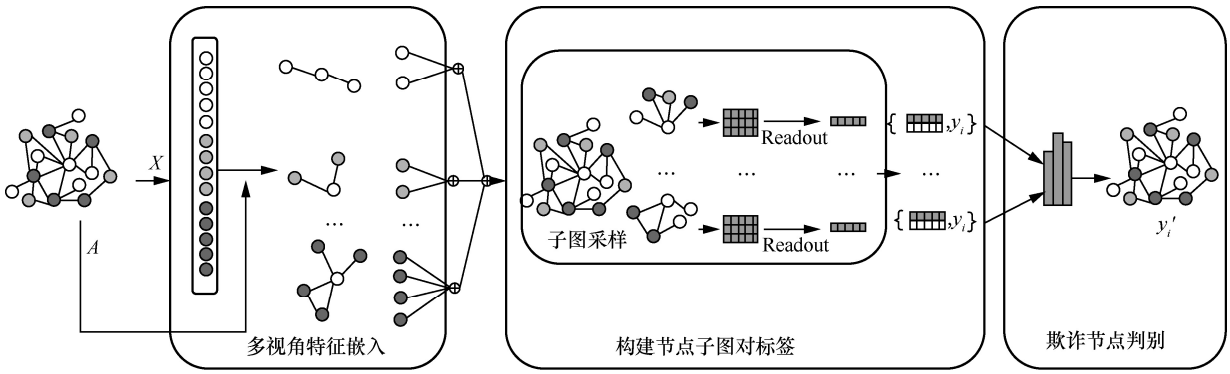


图 1　MGFD 算法架构

重矩阵；h_i 为学习到的节点 v_i 的第一层嵌入。

由于节点具有不同丰富的特征，为聚合不同视角下邻居节点的特征，使算法更易于区分欺诈节点和正常节点，减少对欺诈节点的错误判断，本文基于多层次的注意力机制分别对节点层和不同视角层进行信息融合，以学习不同关系下节点间的联系。

给定用户 v_j，v_{rj} 为用户 v_i 在视角 r 下的邻居，h_j 为节点 v_{rj} 的初始嵌入，利用节点 v_i 和 v_{rj} 之间的关系学习注意力系数 α_{ij}^r，如式(2)所示。

$$\alpha_{ij}^r = \frac{\exp(h_j \boldsymbol{W}_{ij}^r)}{\sum_{k \in N_i^r} \exp(h_k \boldsymbol{W}_{ik}^r)} \tag{2}$$

其中，$\boldsymbol{W}_{ij}^r$ 和 $\boldsymbol{W}_{ik}^r$ 为可学习的注意力参数矩阵，N_i^r 表示节点 v_i 在视角 r 下包含自身的邻居节点集合。由注意力系数作为邻居节点的权重，结合邻居节点自身表示，得到节点 v_i 在视角 r 下的表示为

$$h_i^r = \sum_{k \in N_i^r} \alpha_{ik}^r h_k \tag{3}$$

为了获得节点更全面的信息，需要融合不同视角的信息，以获得高阶的语义信息。由于不同视角得到的节点表示位于不同的空间域，直接融合难以在低维空间中捕获不同视角之间的相关性[4]。因此在融合多视角信息前，使用多层感知器（MLP, multilayer perceptron）将特定视角的节点表示映射到高维的空间中，第 l 层的表示为

$$h_i^{r(l)} = \mathrm{MLP}(h_i^{r(l-1)}) \tag{4}$$

不同视角表示对欺诈检测任务具有不同的贡献，因此本文提出视角级的注意力机制。同理，视角级注意力系数 β_i^r 的计算式为

$$\beta_i^r = \frac{\exp(h_i^{r(l)} \boldsymbol{\varphi}_i^r)}{\sum_{k \in \{1,\cdots,m\}} \exp(h_i^{k(l)} \boldsymbol{\varphi}_i^k)}, r \in \{1,\cdots,m\} \tag{5}$$

其中，$\boldsymbol{\varphi}_i^r$ 为可学习的视角权重向量。

得到不同视角的权重向量后，结合不同视角的嵌入得到节点的多视角特征嵌入，如式(6)所示。

$$h_i = \Big\|_{r=1}^{m} (\beta_i^r h_i^{r(l)}) \tag{6}$$

其中，$\|$ 表示拼接操作，拼接不同视角下节点表示。

2.2 构建节点子图对标签

在欺诈检测任务中，由于欺诈者通常连接正常用户以伪装自己，且欺诈节点远少于正常节点，直接聚合邻居节点易使欺诈者特征被掩盖。本文基于节点子图对构建平衡标签以解决上述问题。由于正常节点与欺诈节点具有不同的行为模式和特征，本文利用节点子图作为新的学习样本，通过构建节点与其子图对，学习判别节点与其子图不同的交互模式，将欺诈节点与其子图对称为负样本，正常节点与其子图对称为正样本。为解决样本不均衡问题，将不平衡比作为少数类节点和多数类节点的子图采样轮数之比，以平衡正负样本数，使分类器充分学习到负样本的特征，避免算法在多数类上过拟合，忽略负样本的信息。

由多视角特征嵌入模块得到节点的表示后，首先确定目标节点，子图为从目标节点采样的局部子图，利用带重启的随机游走（RWR, random walk with restart）算法[19]得到节点的多个子图。RWR 算法表示在游走时有一定概率回到起点，如式(7)所示。

$$\vec{\boldsymbol{r}} = c \boldsymbol{W}_{i,j} \vec{\boldsymbol{r}} + (1-c) \vec{\boldsymbol{o}} \tag{7}$$

其中，$\vec{\boldsymbol{o}}$ 是起点向量；$\vec{\boldsymbol{r}}$ 是终点向量；$\boldsymbol{W}_{i,j}$ 表示图中边的权重，即从节点 i 到节点 j 的概率，在本文中为邻接矩阵；c 为重启概率，当 c =0 时游走回起点。对于正常节点，由游走得到 K 个子图，g_i^k 为第 k 个子图，G_i^k 为节点 i 的第 k 个子图表示，对于欺诈节点，由游走得到 $\tilde{k}$ 个子图 $g_i^{\tilde{k}}$，其中 $\frac{\tilde{k}}{k} = \mathrm{IR}$，利用平均池化作为读出函数 Readout(·) 融合节点表示，具体如式(8)和式(9)所示。

$$G_i^k = \mathrm{Readout}(g_i^k) = \sum_{w=1}^{n_i} \frac{h_{iw}^k}{n_i} \tag{8}$$

$$G_i^{\tilde{k}} = \mathrm{Readout}(g_i^{\tilde{k}}) = \sum_{w=1}^{n_i} \frac{h_{iw}^{\tilde{k}}}{n_i} \tag{9}$$

为度量节点与其子图的一致性，采用双线性映射函数 Bilinear(·) 计算其相似度，对于正常节点，节点与子图对即正样本的分数为

$$s_i^k = \mathrm{Bilinear}(h_i, G_i^k) = \sigma(h_i \boldsymbol{W}_S G_i^{kT}) \tag{10}$$

其中，$\boldsymbol{W}_S$ 为可学习参数矩阵。对于欺诈节点，节点与子图对即负样本的分数为

$$\tilde{s}_i^{\tilde{k}} = \mathrm{Bilinear}(h_i, G_i^{\tilde{k}}) = \sigma(h_i \boldsymbol{W}_P G_i^{\tilde{k}T}) \tag{11}$$

其中，$\boldsymbol{W}_P$ 为可学习参数矩阵。

通过以上模型训练，每一个对比实例对都可以得到一个预测标签值 s_i。最终，模型的对比目标使 s 与标签 y_i 尽可能接近。本文使用标准交叉熵损失目标函数，即

$$L = -\sum_{i=1}^{N} y_i \log(s_i) + (1-y_i) \log(1-s_i) \tag{12}$$

2.3 欺诈节点判别

将节点输入训练好的对比模型后，模型对其进行子图采样，将样本输入分类器中，由 J 个子图得到 $\left[s_i^1, s_i^2, \cdots, s_i^j\right]$。将判别值表示为样本节点子图对预测标签平均值，即

$$S_i = \sum_{j=1}^{J} \frac{s_i^j}{J} \tag{13}$$

正常节点分数趋于 0，欺诈节点分数趋于 1，相较于正常节点，欺诈节点具有较大的判别分数，因此节点是否为欺诈节点的概率为

$$y_i' = \text{sigmoid}(S_i) \tag{14}$$

基于以上论述，基于多视角图神经网络的欺诈检测算法的伪代码过程如算法 1 所示。

算法 1　基于多视角图神经网络的欺诈检测算法

输入　多关系不平衡图 $G=(V,\varepsilon,A,X,C)$，训练集 V_{train}，训练轮数 epoch，训练批次大小 batch_size

输出　节点 i 的欺诈预测标签 s_i

1) 随机初始化编码器参数 $\boldsymbol{W}_e$，注意力参数 $\boldsymbol{W}^r$，$\boldsymbol{\varphi}^r$，子图学习参数 $\boldsymbol{W}_S$，$\boldsymbol{W}_P$

2) for e in epoch do

3)　for b in batch_size do

4)　　for r in R do

5)　　利用拓扑无关的编码器对节点进行属性编码，得到初始嵌入 h_i；

6)　　选取节点 v_i 的邻居节点 v_j；

7)　　基于节点级注意力机制融合邻居节点嵌入 h_j 得到节点嵌入 h_i^r；

8)　　end for

9)　　基于关系级注意力机制融合节点嵌入 h_i^r 得到高维空间节点嵌入 h_i；

10)　　if $c_i == 0$ do

11)　　for k in K

12)　　依据式(7)随机游走获取节点子图

13)　　end for

14)　　else

15)　　for k in int(KIR)

16)　　随机游走获得节点子图；

17)　　end for

18)　　依据式(8)～式(11)学习节点及其子图对

19)　　依据判别器判别节点是否为欺诈节点

20)　end for

21) end for

3 实验与分析

3.1 实验数据集

本文在广泛使用的公开数据集上进行对比实验，分别为 Yelpchi 数据集[20]和 Amazon 数据集[5]。Yelpchi 数据集收集了 Yelp 网站的酒店和餐厅评论。Yelpchi 数据集中的节点是具有 100 维特征的评论，包含以下 3 个关系：1) R-U-R 连接同一用户发布的评论；2) R-S-R 连接同一产品下的评论，具有相同的星级评级；3) R-T-R 连接当月发布的同一产品下的评论。Amazon 数据集包括了 Amazon 网站乐器类别下的产品评论。Amazon 数据集中图的节点是具有 100 维特征的用户，包含以下 3 个关系：1) U-P-U 连接至少查看过同一个产品的用户；2) U-S-U 连接在一周内拥有至少一个相同评级的用户；3) U-V-U 连接具有前 5%的 TF-IDF（term frequency inverse document frequency）相似性的用户。这 2 个数据集的统计数据如表 1 所示，其中标签相似度为欺诈节点与其一阶邻居节点标签平均相似度。从表 1 可以看出，除了 Yelpchi 数据集中的 R-U-R 关系外，其他关系下欺诈节点与其邻居节点的标签相似度都很低，说明图中的欺诈节点与正常节点普遍的连接性以及欺诈节点之间缺乏必要连接的数据特性。

表 1　　**数据集统计数据**

数据集	节点数	不平衡率	关系	关系边数	标签相似度
Yelpchi	45 954	5.9	R-U-R	49 315	0.908 9
			R-S-R	3 402 743	0.176 4
			R-T-R	573 616	0.185 7
Amazon	11 944	13.5	U-P-U	175 608	0.167 3
			U-S-U	3 566 479	0.055 8
			U-V-U	1 036 737	0.053 2

3.2 实验对比方法

为了评估模型欺诈检测性能，本文选取了 GCN 以及几种先进方法进行对比实验。

GCN[21]。图卷积网络对空间域中的节点嵌入进行卷积操作，即聚合邻居的信息来表示节点。

FdGars[22]。该方法基于 GCN 对虚假评论账户进行检测，针对评论的语义特点设计特征，并通过 GCN 对节点特征进一步编码。

GraphConsis[6]。该方法通过邻居节点距离及标签信息均衡采样，解决欺诈检测领域不一致即欺诈者伪装问题。

CARE-GNN[7]。该方法针对欺诈者伪装问题，利用强化学习思想设计自适应的阈值用来筛选邻居节点。

FRAUDER[3]。该方法是一种基于图神经网络的欺诈检测算法，通过设计节点信息聚合机制以及损失函数，实现对图不一致和类不平衡问题的双重抵抗能力。

3.3 评价指标

由于欺诈检测类不平衡问题，本文选用 3 个被广泛使用的对类无偏差的度量指标：AUC、Recall-macro 和 F1-macro。AUC 为受试者操作特征（ROC, receiver operator characteristic）曲线的下面积，AUC 表示随机选择一个欺诈节点，其排名高于正常节点的预测概率。Recall-macro 评估检测到的欺诈节点和正常节点占实际数量的比例的未加权平均值。F1 分数是召回率和精度之间的权衡，而 F1-macro 是正常节点和欺诈节点 F1 分数的未加权平均值。

3.4 参数选择

在多视角特征嵌入模块，节点表示维度对后续欺诈检测的影响如图 2～图 4 所示。节点表示维度超过 64 维时，欺诈检测效果在 3 个评价指标上都呈下降趋势，因此选择输出节点表示维度为 64 维。

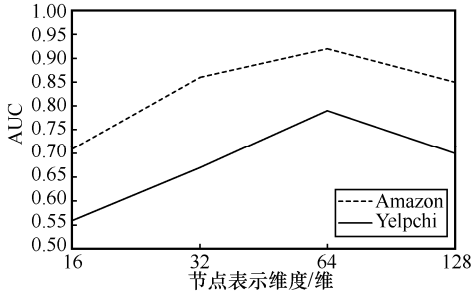


图 2 参数选择 AUC 指标结果

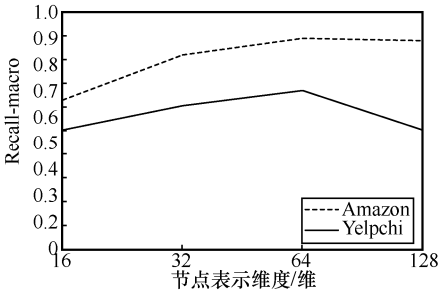


图 3 参数选择 Recall-macro 指标结果

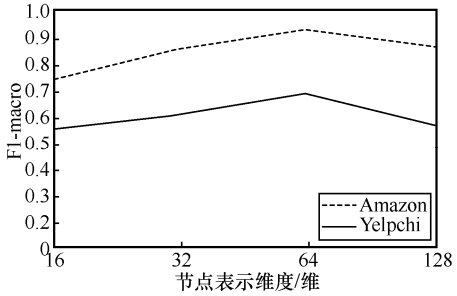


图 4 参数选择 F1-macro 指标结果

3.5 对比实验

MGFD 算法与对比方法在不同数据集上的对比实验结果如表 2 所示。由表 2 可以看出，在给定评价指标上，MGFD 算法均取得了最好的检测效果。

表 2 对比实验结果

方法	Yelpchi			Amazon		
	AUC	Recall-macro	F1-macro	AUC	Recall-macro	F1-macro
GCN	0.598 3	0.500 0	0.562 0	0.779 4	0.5000	0.648 6
FdGars	0.653 6	0.500 0	0.553 2	0.818 5	0.718 6	0.614 5
GraphConsis	0.698 3	0.610 0	0.585 7	0.874 1	0.851 2	0.751 2
CARE-GNN	0.765 7	0.664 6	0.633 2	0.906 7	0.834 7	0.899 0
FRAUDER	0.772 2	0.677 2	0.591 2	0.925 3	0.881 6	0.866 7
MGFD	**0.791 0**	**0.678 1**	**0.654 1**	**0.925 6**	**0.891 0**	**0.924 1**

1) MGFD 算法在 2 个数据集上都取得了最好的效果，这说明 MGFD 算法能够有效解决欺诈检测任务中节点不一致以及类不平衡问题，并学习到欺诈节点潜在的学习模式。MGFD 算法效果好于 FRAUDER 说明多视角的特征嵌入增强了节点自身与其他节点之间的不一致信息以便识别欺诈节点。

2) GCN 表现不好的原因在于其对于分类任务的有效性依赖于同质性假设，即节点与其邻居节点具有相似的特征，但这一假设在欺诈检测任务中并不成立。因此 GCN 在欺诈检测任务中效果不好。

3.6 消融实验

为验证 MGFD 算法多视角嵌入模块以及构建节点子图对标签的有效性，本文对以上 2 个模块进行消融实验，实验结果如图 5～图 7 所示，其中，without MV 表示不进行多角度的特征嵌入，对节点进行简单的卷积得到嵌入；without IL 表示不构建节点子图对标签；MGFD-ALL 表示完整的算法。

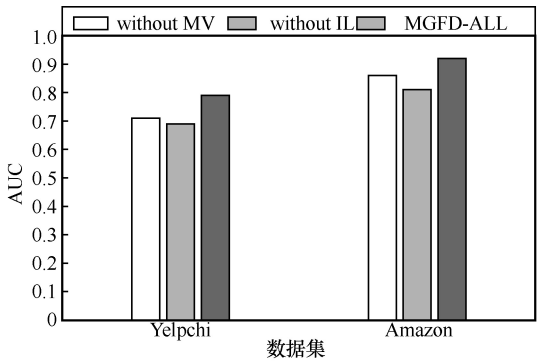


图 5 消融实验 AUC 结果

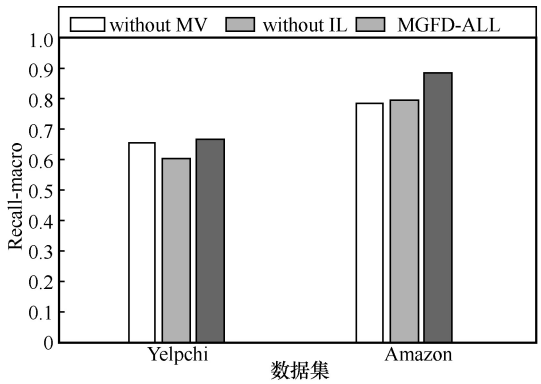


图 6　消融实验 Recall-macro 指标结果

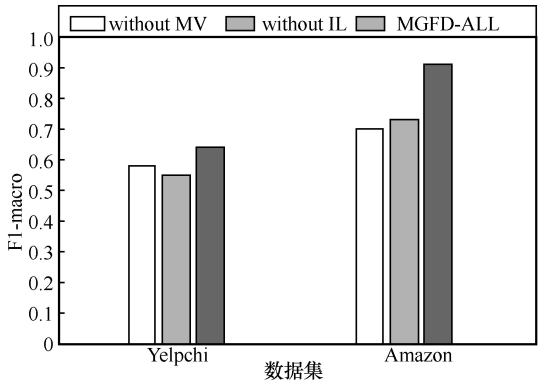


图 7　消融实验 F1-macro 指标结果

从图 5～图 7 可以看出，多视角特征嵌入模块和构建节点子图对标签均对检测效果具有正面的影响，其中由于构建节点子图对标签针对欺诈节点伪装以及类不平衡问题，其对检查效果具有更重要的影响。

3.7　节点特征嵌入相似性分析

为验证多视角特征嵌入模块可以学习到正常节点和欺诈节点的差异性表示，本文设计实验评估相邻节点之间的相似度，表 3 和表 4 分别展示了所选数据集上正常节点和欺诈节点与其一阶邻居节点在不同关系下的平均余弦相似度，其中初始嵌入即节点属性，P_1 表示节点经过结构无关的属性编码器后的输出，P_2 表示经过层次注意力机制聚合的节点表示。

表 3　　Amazon 数据集实验结果

节点	关系	平均余弦相似度		
		初始嵌入	P_1	P_2
欺诈节点	U-P-U	0.690 7	0.069 0	0.069 1
	U-S-U	0.594 7	0.062 1	0.062 3
	U-V-U	0.507 1	0.063 9	0.064 5
正常节点	U-P-U	0.679 4	0.618 1	0.618 5
	U-S-U	0.594 4	0.533 0	0.562 0
	U-V-U	0.513 1	0.567 1	0.601 2

表 4　　Yelpchi 数据集实验结果

节点	关系	平均余弦相似度		
		初始嵌入	P_1	P_2
欺诈节点	R-U-R	0.951 1	0.302 3	0.351 0
	R-T-R	0.871 7	0.101 9	0.101 6
	R-S-R	0.863 4	0.101 9	0.101 9
正常节点	R-U-R	0.981 1	0.865 3	0.865 6
	R-T-R	0.863 6	0.885 2	0.885 3
	R-S-R	0.855 6	0.829 0	0.829 0

以 Amazon 数据集在关系 U-P-U 下为例，当欺诈节点连接正常节点伪装自己时，欺诈节点与其一阶邻居节点之间的相似度高达 0.690 7，但经过模型训练后，P_1 和 P_2 分别降低到 0.069 0 和 0.069 1，而正常节点相似度则变化不明显，可见 MGFD 算法有效地学习了欺诈节点与其正常邻居节点之间的差异化表示，为后续的欺诈检测提供了有力支撑。在 Yelpchi 数据集的 R-U-R 关系下，训练后的 P_1 和 P_2 相较于其他关系略高，这是由于在此关系下，欺诈节点与其一阶邻居节点的标签相似度为 0.951 1，即欺诈节点与欺诈节点连接较多，但是由于欺诈节点行为不稳定，欺诈节点之间也可以学习到差异性表示，训练过后其与一阶邻居节点的相似度也有一定程度的降低。

4　结束语

针对现有图欺诈检测任务中欺诈节点伪装问题以及类不平衡问题，本文多视角特征嵌入机制面向多种关系学习节点表示，针对伪装问题学习节点的一致与不一致信息，并利用采样策略解决类不平衡问题，从而对图中的欺诈节点进行检测。在公共图数据集上的相关实验验证了本文算法具有较好的欺诈检测效果。后续研究将针对现实世界中特定领域数据中的异常信息，设计预处理步骤，从而加强领域异常信息的发掘以提升欺诈检测的效果。

参考文献：

[1] 朱会娟, 陈锦富, 李致远, 等. 基于多特征自适应融合的区块链异常交易检测方法[J]. 通信学报, 2021, 42(5): 41-50.
ZHU H J, CHEN J F, LI Z Y, et al. Block-chain abnormal transaction detection method based on adaptive multi-feature fusion[J]. Journal on Communications, 2021, 42(5): 41-50.

[2] POURHABIBI T, ONG K L, KAM B H, et al. Fraud detection: a systematic literature review of graph-based anomaly detection approaches[J]. Decision Support Systems, 2020, 133: 113303.

[3] ZHANG G, WU J, YANG J, et al. FRAUDRE: fraud detection dual-resistant to graph inconsistency and imbalance[C]//Proceedings of IEEE International Conference on Data Mining. Piscataway: IEEE Press, 2021: 867-876.

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

[5] MCAULEY J J, LESKOVEC J. From amateurs to connoisseurs: modeling the evolution of user expertise through online reviews[C]//Proceedings of the 22nd International Conference on World Wide Web. New York: ACM Press, 2013: 897-908.

[6] LIU Z, DOU Y, 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 Press, 2020: 1569-1572.

[7] 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 Press, 2020: 315-324.

[8] 陈晋音, 张敦杰, 黄国瀚, 等. 面向图神经网络的对抗攻击与防御综述[J]. 网络与信息安全学报, 2021, 7(3):28.
CHEN J Y, ZHANG D J, HUANG G H, et al. Adversarial attack and defense on graph neural networks: a survey[J]. Chinese Journal of Network and Information Security, 2021, 7(3):28.

[9] MA J, ZHANG D, WANG Y, et al. GraphRAD: a graph-based risky account detection system[C]//Proceedings of ACM SIGKDD Conference. New York: ACM Press, 2018: 9

[10] BIAN T, XIAO X, XU T, et al. Rumor detection on social media with bi-directional graph convolutional networks[C]//Proceedings of the AAAI Conference on Artificial Intelligence. Palo Alto: AAAI Press, 2020: 549-556.

[11] LI A, QIN Z, LIU R S, et al. Spam review detection with graph convolutional networks[C]//Proceedings of the 28th ACM International Conference on Information and Knowledge Management. New York: ACM Press, 2019: 2703-2711.

[12] CHAWLA N V, BOWYER K W, HALL L O, et al. SMOTE: synthetic minority over-sampling technique[J]. Journal of Artificial Intelligence Research, 2002, 16: 321-357.

[13] WANG W, WANG S, FAN W, et al. Global-and-local aware data generation for the class imbalance problem[C]//Proceedings of the 2020 SIAM International Conference on Data Mining. Philadelphia: Society for Industrial and Applied Mathematics, 2020: 307-315.

[14] CHI J F, ZENG G X, ZHONG Q W, et al. Learning to undersampling for class imbalanced credit risk forecasting[C]//Proceedings of IEEE International Conference on Data Mining. Piscataway: IEEE Press, 2020: 72-81.

[15] CAO K, WEI C, GAIDON A, et al. Learning imbalanced datasets with label-distribution-aware margin loss[C]//Proceedings of the 33rd International Conference on Neural Information Processing Systems. Massachusetts: MIT Press, 2019: 1567-1578.

[16] HU Z, TAN B, SALAKHUTDINOV R R, et al. Learning data manipulation for augmentation and weighting[C]//Proceedings of the 33rd International Conference on Neural Information Processing Systems. Massachusetts: MIT Press, 2019: 32.

[17] SHI M, TANG Y F, ZHU X Q, et al. Multi-class imbalanced graph convolutional network learning[C]//Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence. San Francisco: Margan Kaufmann, 2020: 2879-2885.

[18] ZHAO T X, ZHANG X, WANG S H. GraphSMOTE: imbalanced node classification on graphs with graph neural networks[C]//Proceedings of the 14th ACM International Conference on Web Search and Data Mining. New York: ACM Press, 2021: 833-841.

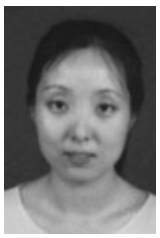
[19] TONG H H, FALOUTSOS C, PAN J Y. Fast random walk with restart and its applications[C]//Proceedings of the Sixth International Conference on Data Mining. Piscataway: IEEE Press, 2006: 613-622.

[20] 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 Press, 2015: 985-994.

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

[22] WANG J Y, WEN R, WU C M, et al. FDGars: fraudster detection via graph convolutional networks in online APP review system[C]//Proceedings of the 22nd International Conference on World Wide Web. New York: ACM Press, 2019: 310-316.

[作者简介]



陈卓（1978− ），女，山东青岛人，博士，青岛科技大学副教授、硕士生导师，主要研究方向为自然语言处理、推荐系统等。

朱淼（1998− ），女，安徽六安人，青岛科技大学硕士生，主要研究方向为图神经网络、异常检测等。

杜军威（1974−），男，山东威海人，博士，青岛科技大学教授、博士生导师，主要研究方向为数据挖掘、知识图谱与知识工程等。