计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.250400085

基于知识图谱嵌入的异构图欺诈用户检测

吕舒琦[1]　张云峰[2]
1 山东开放大学直属学院　济南 250000
2 山东财经大学计算机科学与技术学院　济南 250000
(lvshuqi@sdou.edu.cn)

摘　要　在信用支付服务场景中,欺诈用户的检测问题一直是一个研究热点。在深度学习方法中,通常使用异质信息网络来建模不同类型的节点对象及其交互关系,如用节点表示支付服务场景中的用户及商家,用边来表示节点之间的交互关系,以充分利用图的结构信息。然而,已经提出的很多模型在捕捉节点特征信息时,往往只关注元路径端节点而忽略了元路径中间节点的信息,这将导致信息丢失的问题。因此,提出了一种基于知识图谱嵌入的异构图欺诈用户检测模型。首先,引入知识图谱嵌入方法作为元路径内部聚合编码器,与只关注元路径上端节点的方法不同,元路径内部聚合编码器在获取节点信息时会同时关注元路径中间节点,以聚集整条元路径上的节点信息,能够有效解决信息丢失的问题。除此之外,设计了一个多层融合注意力机制,从节点以及路径层面模拟用户对属性和元路径的偏好,并在全局层面以融合的角度分析特征的重要程度。在不同类型数据集上的实验结果表明,与现有的多种欺诈检测方法相比,所提模型取得了相对较好的结果。

关键词:欺诈检测;图神经网络;异构图;知识图谱嵌入;多层融合注意力机制
中图分类号　TP391

Fraud User Detection Based on Heterogeneous Information Network with Knowledge Graph Eembedding

LYU Shuqi[1] and ZHANG Yunfeng[2]
1 Directly Affiliated College,Shandong Open University,Jinan 250000,China
2 School of Computer Science and Technology,Shandong University of Finance and Economics,Jinan 250000,China

Abstract　In the scenario of credit payment service,the detection of fraudulent users has always been a research hotspot. In the deep learning method,heterogeneous information networks are usually used to model different types of node objects and their interaction relations. For example,nodes are used to represent users and merchants in the payment service scenario,and edges are used to represent the interaction relations between nodes,so as to make full use of the structural information of the graph. However,when capturing node feature information,many models that have been proposed often only focus on the end nodes of the meta path and ignore the information of the middle nodes of the meta path,which will lead to the problem of information loss. Therefore,this paper proposes a heterogeneous graph fraud user detection model based on knowledge graph embedding. Firstly,it introduces the knowledge graph embedding method as the meta path internal aggregation encoder. Different from the method of only focusing on the upper nodes of the meta path,the meta path internal aggregation coder will pay attention to the intermediate nodes of the meta path when obtaining the node information,so as to gather the node information on the whole meta path,which can effectively solve the problem of information loss. Moreover,it designs a multi-layer fusion attention mechanism to simulate users' preferences for attributes and meta paths from the node and path levels,and analyzes the importance of features from the perspective of fusion at the global level. The experimental results on different types of data sets show that the proposed model achieves relatively good results compared with many existing fraud detection methods.

Keywords　Fraud detection,Graph neural network,Heterogeneous graph,Knowledge map embedding,Multi-layer fusion attention mechanism

1　引言

当今,金融服务广泛应用于日常生活的许多方面,尤其是在线金融服务,给人们的生活带来了极大的便利,也给社会带来了巨大的经济效益。然而,随之出现的案件欺诈和套现欺诈等金融欺诈行为严重损害了用户和服务提供商的安全。套现欺诈是指没有实际物品交易,用户以各种方式将物品兑换成现金并用于其他目的,这会导致严重的金融风险。因此,如何进行套现欺诈用户的检测是一个需要研究的重要问题。

欺诈用户检测问题可以被视为分类问题[1-2],目的是预测目标用户在未来的交易中是否会有欺诈行为发生。传统方法中,基于规则的方法通过观察明显的欺诈信号来建立一套欺诈预测规则[3],然而,基于规则的方法容易受到攻击并且难以处理不断变化和复杂的模式。为了突破传统方法的局限性,

通信作者:张云峰(yfzhang@sdufe.edu.cn)

机器学习方法被提出，从数据中自动挖掘欺诈模式。大多数机器学习方法从不同方面提取用户的统计特征，根据特定用户的统计特征进行预测，并使用经典分类器如逻辑回归和神经网络来分类[4]。然而，这种方法很少考虑用户之间的交互。但事实上，在线金融交易场景中存在丰富的交互关系，为了能够充分利用金融场景中的交互关系，有大量研究者使用了图网络结构，其中节点表示对象，连接节点的边表示对象之间的关系。另外，现实世界的网络通常涉及多种节点类型和关系类型，即大量现实世界的图或网络本质上是异构的[5]。异构信息网络可以自然地集成不同类型的对象及其之间的交互，并在学习节点向量表示时保留异构结构和语义[6]。然而，传统的神经网络对所有节点一视同仁，无法对异构图中复杂的结构和语义信息进行建模。

作为一种用来处理图数据的神经网络，图神经网络(GNN)[7]能够在沿着图的结构计算图数据的同时保留图的结构信息。此外，元路径是连接两个实体的特定路径，可以被视为挖掘节点之间的潜在关系的一种方式，能够描述相关节点类型之间的一致关系。基于元路径的方法[8-9]可以充分且直观地利用图形的网络结构，然而，尽管基于元路径的嵌入方法在许多任务上优于许多传统的网络嵌入方法，但在现有的许多基于元路径的方法中，通常只考虑了目标节点所在元路径上的端节点信息，而忽略了元路径上所有中间节点的信息，导致信息的丢失[10]。因此，我们需要找到一种方法，在能够建模和利用异构图中多种关系模式的同时，也能将元路径中间节点连同端节点的信息一起聚合进来。知识图谱嵌入(KGE)[11]是知识图谱领域的一个重要研究分支，在金融、推荐系统等领域有着广泛的应用，通常被认为是解决多关系类型问题的有效方法。

此外，大量研究人员在以往的欺诈检测工作中使用了注意力机制来给对最后的特定任务贡献最大的特征赋予较高的权重。然而，以往的研究主要的关注点集中在节点和路径层面。一些研究人员利用注意力机制编码邻居节点的重要性[12]。近年来，还有许多研究人员使用了包括节点和路径级别[13-14]的分层注意机制。然而，很少有文献从融合的角度综合考虑节点和路径级特征的重要性。

考虑到以上因素，本文提出了一种基于知识图嵌入的异构信息网络欺诈用户检测模型。基于知识图嵌入在建模多种关系类型问题上的优势，我们将其作为元路径内部聚合编码器，用于对元路径中间节点的信息进行聚合，有效地解决了由于只关注端节点而导致的信息丢失问题。此外，本文建立了一个多层融合注意机制，从节点、路径和全局3个层次有效地获取用户的特征表示。节点级注意机制用于权衡不同元路径实例对目标节点的贡献程度，路径级注意机制为不同的元路径分配权重，以表征不同元路径的重要性，全局注意机制从融合的角度关注权重，同时考虑节点和路径的重要性，以获得更有效的节点特征表达。

总之，本文有以下贡献：

1)受MAGNN[15]的启发，提出一种元路径的内部聚合编码器，该编码器引入知识图嵌入方法来整合包括中间节点在内的整条元路径上的节点信息，以解决信息丢失的问题，这是该方法首次应用于金融欺诈用户检测领域；

2)为了获得全局用户特征表示，提出了一种多层融合注意机制，该机制自动模拟用户对节点属性和元路径的偏好，以融合的角度获得更有效的全局特征表达；

3)在不同类型数据集上的结果表明，与以往提出的方法相比，本文提出的欺诈用户检测模型取得了更好的预测结果。

2 相关工作

2.1 异构图欺诈检测

在图结构化数据中，每个数据样本(节点)都有与之相关联的边，该信息可用于捕获实例之间的相互依赖关系。图神经网络作为一种挖掘图数据的有效方法，被广泛应用于异构图的欺诈检测工作中。

在金融欺诈检测领域[16-17]，Wang等[18]开发了一个半监督图注意力网络模型SemiGNN，将有标签部分与无标签部分分开处理，并使用了注意力机制，达到了检测金融欺诈的目的；Liu等[19]提出一种自适应感知路径的图神经网络GeniePath，自动学习对目标节点贡献大的邻居进行传播；针对恶意账户设备和行为聚集性，Liu等提出了GEM(Graph Embeddings for Malicious accounts)[20]系统，构建账户-设备异构网络，以拓扑结构和行为特征作为输入，直接学习图神经网络模型。在其他领域，如意见欺诈方面，通过提取review的内容特征以及评论者身上的主要特征进行分类，基于GCN的模型FdGars[21]能够检测出高风险的reviewer；GAS[22]提出了一种基于GCN的高度可扩展的反垃圾邮件方法，其在满足效率要求的同时，显著地识别出了更多的垃圾评论，减轻了对抗行为的影响。Player2Vec[23]首先将构建的属性异构信息网络(AHIN)映射到一个由多个单视图属性图构成的多视图网络，由元路径描述用户之间的关系，然后利用GCN模型学习每个单视图属性图的嵌入；最后利用注意力机制融合基于不同单视图属性图的不同嵌入，以获得最终表示。Hu等[14]利用属性异构信息网络对信用支付服务场景中不同类型的对象及其丰富的属性和交互关系进行建模，研究了套现用户检测问题，基于元路径方法，提出了一种层次注意机制的套现用户检测模型HACUD。然而，HACUD在元路径聚合过程中，只考虑了一条元路径的端节点信息，而忽略了所有中间节点的结构和语义信息。HERec[24]基于元路径的邻居将异构图转换为基于多条元路径的同构图，并应用DeepWalk模型来学习目标类型的节点嵌入。同样地，该方法在元路径聚合过程中也存在忽略中间节点信息的问题，而此类问题的出现将影响最终的分类效果。

上述基于元路径的模型(如SemiGNN，HACUD和HERec)中普遍存在着信息丢失问题；另外，上述使用注意机制的模型仅从节点以及路径级别独立考虑特征的重要性，并没有从融合角度考虑全局。

2.2 知识图谱嵌入

知识图谱嵌入是知识库中实体和关系的嵌入表示，是知识图谱领域的一项重要研究工作，在语义检索、知识问答和推荐系统等许多应用中被广泛使用。

知识图谱嵌入模型通常可分为：翻译模型(TransE，TransH和TransR等)[25-27]，双线性模型(RESCAL和DistMult等)[28-29]，双曲几何模型(Poincare和MuRE等)，神经网络(Conv和CapsE等)[30-31]，以及旋转模型(RotatE，QuatE和DihEdral等)[32-34]等。

根据现有文献，图结构中有 3 种重要关系：对称、反转和合成。基于异构图的复杂节点和边类型，我们希望找到一种方法可以对多种类型的关系模式进行建模和推断，以便从由多个节点类型组成的元路径中有效提取关键信息，为金融用户欺诈检测工作提供服务。然而，翻译模型和双线性模型等只捕获部分关系模式，无法对上述所有模式进行建模和推断。例如，TransE[25]将每个关系表示为源实体和目标实体之间的双射，因此能够隐式建模反转和反转关系的复合；ComplEx[35]通过引入复杂的嵌入来扩展 DistMult[29]，以便更好地建模，但它无法推断合成模式。受欧拉分解的启发，为了找到一个能够对上述 3 种关系进行建模和推断的关系模型，Sun 等提出了 RotatE[32]模型。具体来说，旋转模型将实体和关系映射到复杂的向量空间，并将每个关系定义为头部实体和尾部实体之间的旋转。文献中的结果表明，旋转模型能够有效地推断和建模各种关系模式。

基于以上分析，我们知道一些模型（如转换模型和双线性模型等）并不能有效地分析和建模各种关系类型，在异构图中可能无法发挥良好的作用。

因此，基于旋转模型在推断和建模多个关系模式方面的优势，本文在模型中使用旋转模型作为元路径的内部聚合编码器，以帮助获取元路径中间节点的信息。此外，提出了一个多层注意融合机制，以获取全面的特征信息。在此基础上，文中提出了一种基于知识图嵌入的异构信息网络欺诈用户检测模型。

3 模型

结合知识图谱嵌入的用户欺诈模型由 4 个主要模块组成：节点投影、路径内聚合、路径间聚合和预测层。模型总体框架如图 1 所示，4 个模块在图中分别用(a)(b)(c)(d)表示。

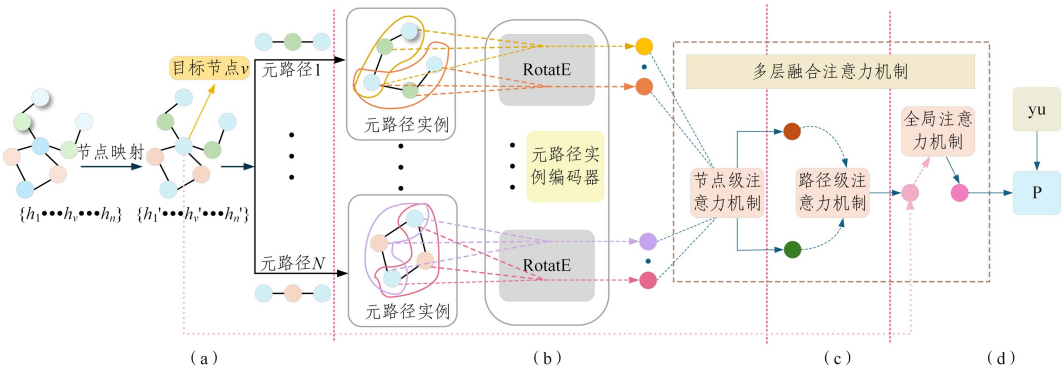

图 1 模型总体架构

Fig. 1 Overall architecture of the model

3.1 节点映射

在线金融交易场景中存在不同类型的节点，而不同类型的节点特征向量具有不同的维度，或者具有相同的向量维度但位于不同的特征空间，这使得在统一的框架中处理不同维度的特征向量非常困难，因此我们首先使用不同的全连接层将不同类型的节点特征投影到相同的潜在向量空间。

$$h_v' = M_{\rho v} \cdot h_v \tag{1}$$

其中，h_v 表示原始特征向量，h_v' 是节点 v 的投影潜在向量，$M_{\rho v}$ 表示节点的参数权重矩阵。

将节点投影到同一个向量空间后，所有节点的投影特征共享相同的维度，解决了源于节点内容特征的图的异构性。

3.2 元路径内部聚合

元路径内部聚合模块对元路径实例进行编码，学习嵌入在目标节点、目标节点基于元路径的邻居以及它们之间的上下文中的结构和语义信息。对于欺诈用户检测问题，在线金融交易中往往存在以下常见情况：在一条元路径 U-U(User-User)中，用户 U1 与用户 U2 之间有交互信息，而在元路径 U-M-U 中，用户 U1 通过商家 M1 与用户 U3 间接存在交互，如果用户 U3 有欺诈行为，即 U3 属于欺诈用户，那用户 U1 发生欺诈行为的可能性会大大增加；另外，商家 M1 很有可能与其他欺诈用户有交互关系，如果我们只考虑一条元路径的首末端节点，其他的信息很难被挖掘出来，对于目标用户是否会发生欺诈行为的预测也会产生偏差。因此，将元路径的中间节点信息考虑在内是非常有必要的。

通过使用元路径实例编码器，将沿元路径实例的所有节点特征转换为单个向量。

$$h_{\rho(v,n)} = f(\rho(v,n)) = f(h_v', h_n', h_{im}', \forall_{im} \in \rho(v,n)_{im}) \tag{2}$$

其中，$\rho(v,n)$ 表示单个实例，h_{im} 表示中间节点的特征向量，$h_{\rho(v,n)}$ 表示元路径实例的所有节点特征。

基于 RotatE 在处理多关系问题上的优越性，我们将其作为元路径实例编码器，以充分利用嵌入在元路径顺序结构中的信息。给定一条元路径 $\rho(u,v)=(t_0,t_1,\cdots,t_n)$，其中 $t_0=u$，$t_n=v$，设 R_i 为节点 t 和节点 t_i 之间的关系，r_i 为 R_i 的关系向量，则 RotatE 编码器公式如下：

$$O_0 = h_{t0}' = h_u' \tag{3}$$

$$O_i = h_{ti}' + O_{i-1} \odot r_i \tag{4}$$

$$h_{p(v,u)} = \frac{O_n}{n+1} \tag{5}$$

其中，h_{ti}' 和 r_i 都是复向量，$\odot$ 为元素积。通过将向量的前半部分视为实部，并将后半部分作为虚部，可以将 d' 维的实向量视作 $d'/2$ 维的复向量。在该过程中，每个目标节点从元路径实例所连接的基于元路径邻居节点中提取并组合信息。通过这种方式，从两个相邻节点和它们之间的元路径上下文中捕获异构图的结构和语义信息，也就是说，在聚合目标用户节点信息时充分考虑用户与其他用户以及商家之间的交互信息。

基于不同元路径实例对目标节点表示的贡献不同，本文使用图注意机制来加权与目标节点 v 相关的元路径实例的总和；此外，为了减少图异质性造成的高方差、稳定学习过程，使用了多头注意力机制。我们学习每个元路径实例的标准化权重，并对所有实例的总和进行加权，然后使用 softmax 函数进行归一化。

$$e_{vn}^{\rho}=LeakyRelu(a_{\rho}^{\mathrm{T}}\cdot[h_v'\parallel h_{\rho(v,n)}]) \tag{6}$$

$$\alpha=\frac{\exp(e_{vn}^{\rho})}{\sum_{i\in N_v^{\rho}}\exp(e_{vn}^{\rho})} \tag{7}$$

$$h_v^{\rho}=\Big\|_{k=1}^{K}\sigma\Big(\sum_{n\in N_v^{\rho}}[\alpha]_k\cdot h_{\rho(v,n)}\Big) \tag{8}$$

其中，a_{ρ} 是元路径的参数化注意向量，$\|$ 表示向量拼接算子，e_{vn}^{ρ} 表示元路径实例 $\rho(v,n)$ 对节点 v 的重要性。

3.3 元路径聚合

获得每条元路径中所有节点的聚合信息后，使用元路径间的聚合模块来组合所有元路径的语义信息。在异构图中，不同元路径的重要性不同。例如，针对金融欺诈用户检测场景，U-U 与 U-M-U 元路径对于最终预测任务的贡献程度是不同的，因此我们使用图注意力机制为不同的元路径分配不同的权重，以便于在聚合用户信息时从更为重要的路径中提取更多的有效信息，更为准确地判断目标用户是否为欺诈用户。

首先，通过对所有元路径的特定节点向量求平均值，我们总结了每条元路径 $\rho_i\in\rho_A$，然后使用注意机制融合 v 的元路径特定节点向量，如下所示：

$$e_{\rho i}=\frac{1}{|V_A|}\sum_{v\in V_A}q_A^{\mathrm{T}}\tanh(W_A\cdot h_v^{\rho i}+b_A) \tag{9}$$

$$\beta=\frac{\exp(e_{\rho i})}{\exp(e_{\rho})} \tag{10}$$

$$h_v^{\rho A}=\sum_{\rho\in\rho_A}\beta\cdot h_v^{\rho} \tag{11}$$

其中，$\rho_A\in R_{dm}$ 是节点类型 A 的参数化注意向量，β 可以解释为元路径对节点的相对重要性，ρ_i 最后对节点 v 的所有元路径特定节点向量进行加权求和。

3.4 预测层

经过以上过程，可获得目标用户的聚集表示 $h_v^{\rho A}$，该聚集表示包含了相关邻居节点的信息。我们建立了一个全局注意力机制，从融合的角度分析节点级和路径级特征的重要性，以提高分类精度。仍然使用 softmax 对注意力分数进行标准化，获得特征的最终表示：

$$m_{v,v_{\rho}}=Relu(k^{\mathrm{T}}\cdot[h_v'\parallel h_v^{\rho A}]) \tag{12}$$

$$\gamma=\frac{\exp(m_i)}{\sum_{i\in v,v_{\rho}}\exp(m_{v,v_{\rho}})} \tag{13}$$

$$\tilde{h_v}=\sum_{\rho\in\rho_A}\gamma\cdot h_v^{\rho A} \tag{14}$$

其中，k 是全局的参数化注意向量。我们将得到的最终表示输入到几个完全连接的神经网络中，如下所示：

$$Z_u=Relu(W_l\cdots Relu(W_1\tilde{h_v}+b_1)+b_l) \tag{15}$$

其中，W 和 b 表示权重矩阵和偏差向量。

通过使用带有 sigmod 单位的回归层，我们可以获得给定类别的预测概率：

$$p_u=sigmod(W_p^{\mathrm{T}}Z_u+b_p) \tag{16}$$

使用交叉熵损失函数来建模目标函数：

$$L=-\sum_{v\in V_L}\sum_{t=1}^{T}y_v[t]\cdot p_v[t] \tag{17}$$

其中，T 是类别数，V_L 是带有标签的节点集，y_v 是节点 v 的一个独热编码向量，p_v 是节点 v 的预测概率。

4 实验

4.1 数据集

本研究使用了来自不同领域的两个数据集。需要说明的是，由于金融交易固有的私密性，在欺诈检测领域进行的研究没有公开可用的数据集，我们仅找到 Synthetic Financial Datasets 这一个适用于金融欺诈用户检测问题的数据集。为了保证实验的完整性，考虑到金融用户欺诈检测问题本身属于分类问题，我们使用了参考模型 MAGNN 中用于验证节点分类效果时使用的 DBLP 数据集来验证我们模型的有效性。

(1)DBLP。DBLP 是一个计算机科学书目网站。经过数据预处理后，我们采用了 DBLP 的一个子集，其中包含 4 057 位作者、14 328 篇论文、7 723 个术语和 20 个出版社。作者分为 4 个研究领域(数据库、数据挖掘、人工智能和信息检索)。作者节点分为 400 个训练集、验证集和测试集。

(2)Synthetic Financial Datasets。金融欺诈检测数据集对在线金融交易领域的研究人员来说非常重要，然而，金融交易数据特殊的私密性，导致在欺诈检测领域没有公开披露可用的数据集。Synthetic Financial Datasets 是由模拟器 PaySim 生成的复合数据集，使用私有数据集中的聚合数据生成类似于事务正常操作的复合数据集并注入恶意欺诈行为，以便用于检测欺诈行为的方法研究之中。

4.2 评估指标

实验中，使用 F1 分数和准确率(Accuracy)对模型进行评估，这是分类任务的常用评估标准。F1 分数是统计学中用来衡量分类模型精确度的一种指标，它同时兼顾了分类模型的准确率和召回率，可以被看作是模型准确率和召回率的一种加权平均，最大值是 1，最小值是 0，值越大意味着模型越好。F1 分数定义如下：

$$F1=2\times\frac{precision\times recall}{precision+recall} \tag{18}$$

准确率(Accuracy)代表正确预测占总样本的比例，定义如下：

$$Acc=\frac{TP+TN}{TP+TN+FP+FN} \tag{19}$$

其中，TP(正确识别)表示被检索到正样本，实际也是正样本；FP(一类错误识别)表示被检索到正样本，实际是负样本；TN(正确识别)表示未被检索到正样本，实际也是负样本；FN(二类错误识别)表示未被检索到正样本，实际是正样本。准确率越高，分类器越好。

4.3 训练细节

我们基于 Python3.6，调用 DGL，NetworkX 和 NumPy 等包实现了提出的模型，使用 xavier 初始值设定项随机初始化模型参数。将节点隐藏状态的维度设置为 64 维，采样的邻居数默认值为 100。此外，将 epoch 设置为 100，batch-size 设置为 8，学习率设置为 0.002。对于其他比较方法，我们根据文献对其参数进行了优化。此外，对于所有基线方法，

我们均根据原文献代码提供的数据处理方法对数据集进行处理。

4.4 对比实验

4.4.1 基线方法

为了验证欺诈检测模型的有效性,将其与以下几类基线模型进行比较,包括使用简单图卷积网络的模型、使用元路径概念以及单层注意力机制的模型、使用权重参数而非注意力机制来捕捉重要性的模型,以及使用多层注意力机制和元路径概念但未考虑元路径中间节点信息的模型。

Fdgars:该模型是最早研究使用 GCN 进行意见欺诈检测的模型之一,使用经典的 GCN 对节点特征进行编码,分析腾讯应用商店水军的行为和语义特征。模型中使用了经典的共同评论关系,即如果两个客户评价了同一个应用程序,那么他们的节点之间会有一条边存在。

Player2Vec:该模型使用异构信息网络来模拟网络论坛,使用元路径模拟同质节点的异构关系,不同的元路径类似于不同的关系;使用 GCN 编码同一元路径下的节点构成的同质图,并使用注意机制来学习不同元路径的重要性。

GEM:该模型在支付宝中检测恶意账户,其节点为账户和设备,账户节点和设备节点之间的交互由边表示。在收集信息时,对于账户节点,首先在同一设备子图下聚合其邻居,然后从不同子图中聚合信息,使用权重参数来编码不同设备子图的重要性,而不是使用注意机制。

HACUD:该模型是一个基于分层注意力机制的套现用户检测模型,使用属性异构信息网络对信用支付服务场景中不同类型的对象及其丰富的属性和交互进行建模。通过利用 AHIN 中结构信息的不同方面,结合基于元路径的邻域来增强对象的特征表示,精心设计了分层注意机制,以模拟用户对属性和元路径的偏好。

4.4.2 实验结果

为了验证模型的有效性,我们在两种不同类型的数据集上进行了实验。需要说明的是,由于在金融交易中欺诈用户的数量远远低于正常用户,所以金融数据集 Synthetic Financial Datasets 中的正负样本数量极不平衡,在这一情况下使用 Accuracy 作为评价指标意义不大,因此在数据集 Synthetic Financial Datasets 上的实验仅使用 F1-Score 作为评价指标。

在数据集 DBLP 上的结果如表 1 与图 2 所示。我们的模型在 F1-Score 和准确率方面的指标均优于基准模型,与 HACUD 相比,*F1-Score* 提高了 1.75 个百分点,*Accuracy* 提高了 1.30 个百分点,这是因为 RotatE 作为元路径编码器能够将元路径中间节点的信息也利用起来,有效地帮助模型获取到更多有用的信息,以此来帮助进行预测。我们还发现,相比于未使用注意力机制的模型,使用了注意力机制的模型能够取得更好的结果,这证明了注意力机制的有效性。另外,我们在模型中使用了一种多层融合注意力机制,该机制从融合的角度分析节点级和路径级的特征在全局层面的重要程度,比 GEM 中应用的自注意力机制和 HACUD 中应用的双层注意力机制(包括节点级和路径级)更有效,这也是我们的模型能够获得更好分类精度的原因之一。

表 1 在 DBLP 数据集上的实验结果

Table 1 Experimental results on DBLP

(%)

Model	*F1-Score*	*Accuracy*
FdGars	88.40	89.01
Player2Vec	88.74	89.27
GEM	82.36	87.40
HACUD	92.07	93.02
Ours	**93.82**	**94.32**

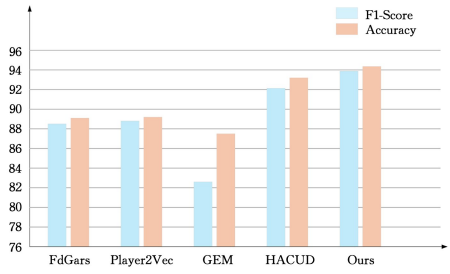

图 2 DBLP 上的实验结果

Fig. 2 Experimental results on DBLP

在金融数据集 Synthetic Financial Dataset 上的结果如表 2 及图 3 所示。与基线模型相比,我们提出的方法仍然取得了更好的分类结果。此外,值得一提的是,在金融数据集上得到的结果明显低于文本数据集 DBLP 上的结果。这是因为受欺诈检测金融数据集数据私密性的限制,合成金融数据集 Synthetic Financial Dataset 上的元路径数量以及数据信息量要少于 DBLP,这将对模型的实验效果造成影响。

表 2 在 Synthetic Financial Dataset 上的实验结果

Table 2 Experimental results on Synthetic Financial Dataset

Model	*F1-Score*/%
FdGars	69.10
Player2Vec	69.75
GEM	68.51
HACUD	70.76
Ours	**71.22**

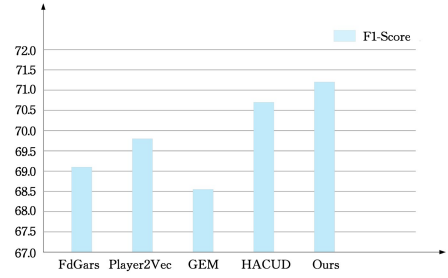

图 3 Synthetic Financial Dataset 上的实验结果

Fig. 3 Experimental results on Synthetic Financial Dataset

4.5 消融实验

为了验证我们所采用的元路径编码器和多层融合注意力机制的有效性,我们设计了以下消融实验。其中 $\text{Ours}_{\text{feat}}$ 表示没有使用节点内容信息,Ours_{nb} 表示只考虑基于元路径的邻居,Ours_{sm} 表示只使用来自单个最佳元路径的信息,Ours_{gl} 表示不使用全局注意力机制。

如表 3 及图 4 所示,当分别去除 4 个对比模块时,模型的实验结果在一定程度上均有所降低。在不考虑节点内容信息、只考虑节点的相邻节点信息、仅使用单一最佳元路径以及没有使用全局注意力机制时,模型的 F1-Score 分别降低了

0.08 个百分点、0.13 个百分点、0.05 个百分点、0.02 个百分点，*Accuracy* 分别降低了 0.12 个百分点、0.16 个百分点、0.07 个百分点、0.02 个百分点。类似地，如表 4、图 5 所示，在数据集 Synthetic Financial Dataset 上的实验结果有着与 DBLP 数据集上相似的趋势。

表 3 在 DBLP 数据集上的消融实验结果

Table 3 Ablation experimental results on DBLP

(%)

Model	*F1-Score*	*Accuracy*
$Ours_{feat}$	93.74	94.20
$Ours_{nb}$	93.69	94.16
$Ours_{sm}$	93.77	94.25
$Ours_{gl}$	93.80	94.30
Ours	**93.82**	**94.32**

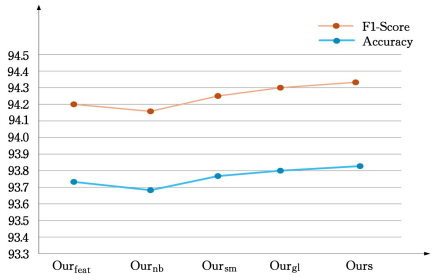

图 4 DBLP 上的消融实验结果

Fig. 4 Ablation experimental results on DBLP

表 4 在 Synthetic Financial Dataset 上的消融实验结果

Table 4 Ablation Experimental results on Synthetic Financial Dataset

Model	*F1-Score*/%
$Ours_{feat}$	71.08
$Ours_{nb}$	71.05
$Ours_{sm}$	71.11
$Ours_{gl}$	71.15
Ours	**71.22**

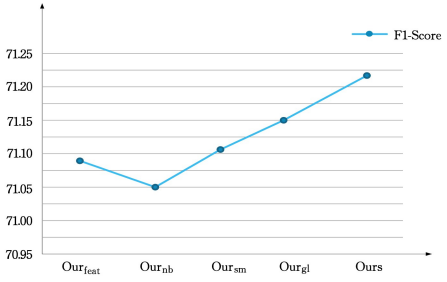

图 5 Synthetic Financial Dataset 上的消融实验结果

Fig. 5 Ablation experimental results on Synthetic Financial Dataset

进一步分析实验结果，通过利用节点内容特征，完整的模型相比 $Ours_{feat}$ 有显著的性能改进，这表明了应用节点内容转换来整合节点特征的必要性。将 $Ours_{nb}$ 与完整模型 Ours 进行比较，我们发现相比于仅考虑基于元路径的邻居，聚合元路径实例上所有节点信息(包括中间节点)的做法可以有效提高性能，这验证了我们在模型中使用知识图谱嵌入方法 RotatE 对中间节点信息进行内部聚合的有效性。$Ours_{sm}$ 与完整模型结果之间的差异表明了多条元路径的信息聚合也是一个关键步骤。在 $Ours_{gl}$ 与 Ours 结果比较中，我们发现全局注意力机制确实在模型的工作过程中发挥了一定的正向作用。

结束语 本文研究了基于图神经网络的金融欺诈用户检测问题。该模型在异构图框架中引入了知识图谱嵌入的概念，采用知识图嵌入方法 RotatE 作为元路径内部编码器，解决了现有基于元路径的研究中节点信息丢失的问题。此外，本文还设计了一种多层融合注意力机制来模拟用户对属性和元路径的偏好，从全局出发，以融合的角度分析特征用于最终的分类任务，以达到检测欺诈用户的目的。在多种公共数据集上的结果表明，我们提出的模型相比于基准模型能够获得更好的分类结果。

然而，由于金融数据具有高度敏感性、商业保密性和监管合规要求等特殊性，当前公开可用的高质量金融欺诈检测数据集存在显著稀缺性。本研究受限于数据获取渠道的合规边界，实验部分仅能基于少量数据集开展，这在一定程度上制约了模型训练的充分性和结论的普适性。针对当前数据稀缺性挑战，我们将在未来的工作中探索更有效的数据获取与增强策略，提升数据集的规模和质量，从而支撑更可靠的模型训练与评估，提高模型检测的准确率。

参 考 文 献

[1] HILAL W, ANDREW S, GADSDEN, et al. Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances [J]. Expert Systems with Applications, 2022, 193: 1.

[2] KAIDI L, TIANMENG Y, MIN Z, et al. SEFraud: Graph-based Self-Explainable Fraud Detection via Interpretative Mask Learning[C]// Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD'24). Association for Computing Machinery, New York, NY, USA, 2024: 5329-5338.

[3] 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. IEEE, 1997: 107-113.

[4] AGARWAL A, BARHAM P, BREVDO E, et al. Ten-sorflow: A system for large-scale machine learning[C]// Proceedings of the 12th USENIX Conference on Operating Systems Design and Implementation. USENIX Association, 2016.

[5] KHEMANI B, PATIL S, KOTECHA K T S. A review of graph neural networks: concepts, architectures, techniques, challenges, datasets, applications, and future directions[J]. Journal of Big Data, 2024, 11(1).

[6] WANG X, BO D, SHI C, et al. A Survey on Heterogeneous Graph Embedding: Methods, Techniques, Applications and Sources[J]. IEEE Transactions on Big Data, 2023, 9(2): 415-436.

[7] 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.

[8] ZHANG M, HE T T, DONG M. Meta-path reasoning of knowledge graph for commonsense question answering[J]. Frontiers of Computer Science, 2024, 18(1): 181303.

[9] DONG Y, CHAWLA N V, SWAMI A. metapath2vec: Scalable representation learning for heterogeneous networks[C]// Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2017: 135-144.

[10] FU X, ZHANG J, MENG Z, et al. Magnn: Metapath aggregated graph neural network for heterogeneous graph embedding[C]// Proceedings of The Web Conference 2020. 2020: 2331-2341.

[11] ZHANG Y,KONG X,SHEN Z,et al. A survey on temporal knowledge graph embedding: Models and applications[J]. Knowledge-Based Systems,2024,304.

[12] GUANGSHANG G. Review of Research on Neural Network Combined with Attention Mechanism in Recommendation System[J]. Journal of Computer Engineering & Applications,2024,60(10).

[13] WANG X,JI H,SHI C,et al. Heterogeneous graph attention network[C]// The World Wide Web Conference. 2019:2022-2032.

[14] HU B,ZHANG Z,SHI C,et al. Cash-out user detection based on attributed heterogeneous information network with a hierarchical attention mechanism[C]// Proceedings of the AAAI Conference on Artificial Intelligence. 2019:946-953.

[15] FU X,ZHANG J,MENG Z,et al. MAGNN:Metapath Aggregated Graph Neural Network for Heterogeneous Graph Embedding[C]// Proceedings of the Web Conference 2020. 2020:2331-2341.

[16] CHENG D,ZOU Y,XIANG S,et al. Graph neural networks for financial fraud detection:a review[J]. Frontiers of Computers Science,2025,19(9):199609.

[17] KHODABANDEHLOU S,GOLPAYEGANI A H. FiFrauD:Unsupervised Financial Fraud Detection in Dynamic Graph Streams[J]. ACM Transactions on Knowledge Discovery from Data,2024,18(5):29.

[18] WANG D,LIN J,CUI P,et al. A Semi-supervised Graph Attentive Network for Financial Fraud Detection[C]// ICDM. IEEE,2019:598-607.

[19] LIU Z,CHEN C,LI L,et al. GeniePath:Graph Neural Networks with Adaptive Receptive Paths[C]// Proceedings of the AAAI Conference on Artificial Intelligence. 2018.

[20] LIU Z,CHEEN C,YANG X,et al. Heterogeneous Graph Neural Networks for Malicious Account Detection[C]// Proceedings of the 27th ACM International Conference on Information and Knowledge Management. 2018:2077-2085.

[21] WANG J,WEN R,WU C,et al. FdGars:Fraudster Detection via Graph Convolutional Networks in Online App Review System[C]// Companion The 2019 World Wide Web Conference. 2019.

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

[23] ZHANGY,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. 2019:549-558.

[24] SHI C,HU B,ZHAO W X,et al. Heterogeneous information network embedding for recommendation[J]. IEEE Transactions on Knowledge and Data Engineering,2018,31(2):357-370.

[25] BORDES A,USUNIER N,GARCIA-DURAN A,et al. Translating embeddings for modeling multi-relational data[J]. Advances in Neural Information Processing Systems,2013,26.

[26] WANG Z,ZHANG J,FENG J,et al. Knowledge graph embedding by translating on hyperplanes[C]// Proceedings of the AAAI Conference on Artificial Intelligence. 2014.

[27] LIN Y,LIU Z,SUN M,et al. Learning entity and relation embeddings for knowledge graph completion[C]// Twenty-ninth AAAI Conference on Artificial Intelligence. 2015.

[28] NICKEL M,TRESP V,KRIEGEL H P. A three-way model for collective learning on multi-relational data[C]// ICML. 2011.

[29] YANG B,YI H W,HE X,et al. Embedding entities and relations for learning and inference in knowledge bases[J]. arXiv:1412.6575,2014.

[30] DETTMERS T,MINERXINI P,STENETORP P,et al. Convolutional 2d knowledge graph embeddings[C]// Thirty-second AAAI Conference on Artificial Intelligence. 2018.

[31] VU T,NGUYEN T D,NGUYEN D Q,et al. A capsule network-based embedding model for knowledge graph completion and search personalization[C]// Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics:Human Language Technologies,Volume 1(Long and Short Papers). 2019:2180-2189.

[32] SUN Z,DENG Z H,NIE J Y,et al. Rotate:Knowledge graph embedding by relational rotation in complex space[J]. arXiv:1902.10197,2019.

[33] ZHANG S,TAY Y,YAO L,et al. Quaternion knowledge graph embeddings[J]. arXiv:1904.10281,2019.

[34] XU C,LI R. Relation embedding with dihedral group in knowledge graph[J]. arXiv:1906.00687,2019.

[35] TROUILLON T,WELLBL J,RIEDEL S,et al. Complex embeddings for simple link prediction[C]// International Conference on Machine Learning. PMLR,2016:2071-2080.

LYU Shuqi, born in 1996, postgraduate. Her main research interests include knowledge graph and graph neural network.

ZHANG Yunfeng, born in 1977, Ph.D, professor, Ph.D supervisor, is a member of CCF (No. 29888M). His main research interests include the theory and application of image and video data analysis and visualization.