融合知识的多视图属性网络异常检测模型

杜航原 [1] 曹振武 [1] 王文剑 [1, 2] 白 亮 [2]

摘 要 属性网络异常检测在网络安全、电子商务和金融交易等领域中具有重要的理论与现实意义, 近年来受到了越来越多的关注. 大多数异常检测方法凭借网络有限的属性或结构信息进行决策生成, 往往难以对异常模式做出可靠的描述. 此外, 网络节点对应的实体往往关联着丰富的领域知识, 这些知识对于异常的识别具有重要的潜在价值. 针对上述情况, 提出一种融合知识的多视图网络异常检测模型, 在多视图学习模式下通过数据与知识的互补融合实现了对异常节点的有效识别. 首先, 使用 TransR 模型由领域知识图谱抽取知识向量表示, 并借助输入网络的拓扑关系构造其孪生网络. 接着, 在多视图学习框架下构建属性编码器和知识编码器, 分别将属性网络及其孪生网络嵌入到各自的表示空间, 并聚合为统一网络表示. 最后, 综合不同维度上的重构误差进行节点异常分数评价, 从而识别网络中的异常节点. 在真实网络数据集上的对比实验表明, 提出的模型能够实现对领域知识的有效融合, 并获得优于基线方法的异常检测性能.

关键词 属性网络, 异常检测, 图神经网络, 知识融合, 多视图学习

引用格式 杜航原, 曹振武, 王文剑, 白亮. 融合知识的多视图属性网络异常检测模型. 自动化学报, 2023, **49**(8): 1732−1744

DOI 10.16383/j.aas.c220629

Multi-view Outlier Detection for Attributed Network Based on Knowledge Fusion

DU Hang-Yuan[1] CAO Zhen-Wu[1] WANG Wen-Jian[1, 2] BAI Liang[2]

Abstract Outlier detection on attributed networks is of important theoretical and practical significance in the network security, ecommerce, financial transaction and many other fields, and receives more and more attentions in recent years. Most existing outlier detection methods usually generate decisions by pattern mining on the network structure or node attributes. However, it is difficult to make a reliable description for abnormal objects by just relying on the limited attribute and structure information directly available from given network data. Furthermore, the nodes in networks are usually associated with abundant domain knowledge in the real world, which has great potential value for outlier detection. To this end, this paper proposes a multi-view network outlier detection model based on knowledge fusion, which identifies the abnormal pattern effectively by complementary fusion of network data and associated knowledge under the multi-view learning mode. Firstly, the model applies TransR to extract knowledge vector representation from domain knowledge graph, and constructs a twin network with the topology structure of the input network. Then, the attribute encoder and the knowledge encoder are constructed under the multi-view learning framework to embed he attributed network and its twin network into their respective representation spaces separately. On this basis, the network embeddings in two views are integrated into a unified representation by the aggregator. Finally, the abnormal score of each node is evaluated by integrating the reconstruction errors in the two different dimensions, and the abnormal nodes in the network are then recognized. Extensive experiments on real network datasets demonstrate that the proposed model can realize effective fusion of domain knowledge and acquire better outlier detection performance than baseline approaches.

Key words Attributed networks, outlier detection, graph neural network, knowledge fusion, multi-view learning

Citation Du Hang-Yuan, Cao Zhen-Wu, Wang Wen-Jian, Bai Liang. Multi-view outlier detection for attributed network based on knowledge fusion. *Acta Automatica Sinica*, 2023, **49**(8): 1732−1744

属性网络[1] 作为一种包含丰富语义信息的数据组织形式, 在现实世界中普遍存在, 例如社交网络、生物信息网络、电商网络等. 这些网络中的节点除了彼此关联形成拓扑结构外, 往往还伴随一组丰富的特征或属性. 例如, 社交网络中的用户之间存在好友关系, 用户自身还具有兴趣标签、职业和年龄等重要属性. 电商网络中的商品可能与其他商品被

收稿日期 2022-08-08 录用日期 2023-01-18
Manuscript received August 8, 2022; accepted January 18, 2023
国家自然科学基金 (U21A20513, 62076154, 61902227, 62022052, 62276159), 山西省重点研发计划项目 (202202020101003)资助
Supported by National Natural Science Foundation of China (U21A20513, 62076154, 61902227, 62022052, 62276159) and the Key R&D Program of Shanxi Province (202202020101003)
本文责任编委 张敏灵
Recommended by Associate Editor ZHANG Min-Ling
1. 山西大学计算机与信息技术学院 太原 030006 2. 山西大学智能信息处理研究所 太原 030006
1. School of Computer and Information Technology, Shanxi University, Taiyuan 030006 2. Institute of Intelligent Information Processing, Shanxi University, Taiyuan 030006

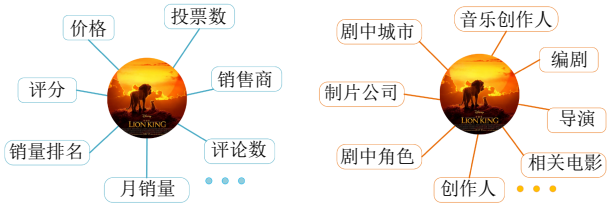
同一用户购买形成拓扑关系, 商品自身还具有价格、产地等属性信息. 属性网络具有建模现实世界复杂系统的强大能力, 近年来随着学术界和产业界的持续关注, 面向属性网络的异常检测问题也逐渐成为一个重要的研究领域.

属性网络异常检测的目标是识别与大多数节点具有显著差异的离群节点, 对于帮助决策者发现、管理和规避数据中的异常模式具有重要意义, 被广泛应用于诸多领域中. 例如, 对计算机网络中威胁网络安全的恶意软件或网络入侵的检测[2], 对电商网络中可能带给商家和客户巨大经济损失的欺诈行为的识别[3], 以及对社交媒体中恶意广告和垃圾邮件的过滤[4] 等.

由于获取异常标记的成本十分高昂, 目前大多数检测方法主要以无监督学习模式实现异常节点的识别. 这些方法大体上可以分为浅层学习方法和深度学习方法. 其中, 浅层方法通常采用异常度评价、残差分析或局部上下文分析等策略发现异常对象. 例如, LOF[5] 算法通过计算节点属性与其邻居的局部密度之间的距离, 在上下文中检测异常. Perozzi 等[6] 提出的 AMEN 方法, 基于邻域的内部相似性和外部分离性定义了 normality 指标, 将结构和属性结合起来量化属性邻域的质量, 将 normality 较低的低质量邻域识别为异常社区. Li 等[7] 构建了一种 Radar 框架, 该框架学习线性回归函数以拟合由网络结构正则化的节点属性, 回归函数的残差被用作衡量异常的分数. Gutierrez-Gomez 等[8] 提出一种能够在多个尺度进行网络异常检测的方法, 该方法利用信号平滑后节点存留的聚集性对异常节点进行刻画, 引入 Markov 稳定性框架进行社区发现, 以寻找异常所在的上下文结构.

受限于浅层学习机制对复杂分布和非线性问题有限的建模能力, 上述方法难以有效捕获网络中结构和属性不同信息模式之间的复杂交互关系. 深度学习模型凭借强大的表示学习能力和优秀的非线性决策能力, 能够在复杂的属性网络中为节点学习更为有效的表示. 为此, 一些研究尝试将深度神经网络用于解决属性网络上的异常检测问题. 例如, Chen 等[9] 设计了一种基于生成对抗属性网络的异常检测框架 GAAN, 利用生成器产生伪节点, 在编码器对真实和伪节点进行编码后, 使用鉴别器区分给定的两个连通节点来自原始网络还是生成数据, 并综合样本重构损失和判别损失构造异常检测的优化目标. Ding 等[10] 提出一种基于自编码器框架的深度异常检测模型 Dominant, 使用图卷积网络 (Graph convolutional network, GCN) 作为编码器将输入属性网络映射为低维嵌入. 解码器由网络嵌入重构拓扑结构和节点属性, 并通过重构误差来发现属性网络中的异常节点. Li 等[11] 提出一个基于谱卷积和反卷积的框架 SpecAE, 将属性网络嵌入到隐空间中, 利用拉普拉斯锐化来放大异常嵌入与正常节点嵌入之间的距离, 并结合密度估计模型来实现异常检测.

尽管上述方法在一些属性网络异常检测任务上获得了成功的应用, 然而由于异常样本的稀缺性以及先验信息的有限性, 仅仅依赖网络数据本身仍然难以对异常的分布特性做出准确可靠的描述. 在许多实际场景中, 在网络数据之外, 还以其他形式存在着关于网络系统的领域知识描述. 例如, 电商网络中的商品除了包含属性信息外, 还蕴含着现实世界中各类与其相关的知识信息, 如图 1 所示. 网络数据和领域知识源于对同一复杂系统在不同视角下的描述与刻画, 网络数据本身是数据生成机制作用下形成的一种表现形式, 而这些数据所属领域的知识则可能隐含着揭示网络数据形成和异常节点产生背后机理的有用信息. 因此, 如何对领域知识进行有效融合与利用, 进而提高网络异常检测的有效性, 将成为一个极具价值的问题.



(a) 影片及其属性信息
(a) The movie and its attribute information

(b) 影片及其领域知识
(b) The movie and its domain knowledge

图 1　电商网络中的属性信息与知识
Fig. 1　Attribute information and knowledge in the e-commerce network

本文提出了一种融合领域知识的多视图异常检测 (Multi-view outlier detection based on knowledge fusion, MOD-KF) 模型. 该模型首先利用领域知识为属性网络构造孪生网络, 形成对该网络的多视图描述. 接着在多视图模式下学习网络的低维表示, 通过视图聚合将领域知识融入到节点的统一表示中. 最后从网络拓扑和节点特征两个维度进行网络的解码重构, 依据重构误差计算节点的异常得分, 实现对异常节点的识别. 通过对领域知识的融合, 该模型可以使网络表示中保留更多有助于下游决策生成的关键信息, 进而改善可用数据较少的情况下异常检测的决策有效性.

本文的主要贡献如下:

1) 设计了一个多视图决策框架, 将属性网络以及相关领域知识构建的孪生网络作为复杂系统在不同视图下的信息形式表现. 借助图神经网络学习二者的网络表示, 并通过视图聚合操作实现了网络数据和领域知识在决策生成中的有效融合.

2) 提出了一种融合领域知识的属性网络异常检测模型 MOD-KF, 在图自编码器框架下, 以多视图的方式并行学习输入网络和孪生网络的表示, 丰富和完善了对网络中对象的描述, 使异常检测的有效性和可靠性得到提升.

3) 在真实网络数据集上对 MOD-KF 和几种异常检测基线方法进行了比较分析, 实验结果验证了该模型的有效性.

本文的结构组织如下: 第 1 节对相关工作进行了简要介绍; 第 2 节给出了问题定义; 第 3 节详细阐述了 MOD-KF 模型的构成及原理; 第 4 节通过实验对提出模型的有效性进行了验证; 第 5 节对本文的工作进行了总结和展望.

1 相关工作

目前, 较少有工作探讨在网络异常检测中融合领域知识, 这里着重对以下几个相关领域的工作进行简要介绍, 包括网络异常检测、图神经网络和知识图谱嵌入.

1.1 网络异常检测

近年来, 越来越多的业务场景中不断生成以图或网络结构表示的复杂的、相互关联的数据. 在这些复杂网络中, 往往存在部分和其他大多数对象具有明显不同行为表现的异常对象. 它们常表现为与网络中其余部分具有不同连接模式的单个节点, 或者是彼此之间频繁交互, 形成密集联系的团体. 为了识别这些异常对象, 一些研究工作借助网络数据中的拓扑结构, 对不同节点间的交互行为和依赖关系加以分析, 进行网络异常的识别. 例如, Fraudar 算法[12] 定义了一个表示节点平均可疑度的全局度量, 通过逐步移除二部图中可疑度最低的节点, 使得剩余网络结构的全局平均可疑度达到最大, 从而找到异常子网络. SCAN 算法[13] 根据节点的结构和连通性进行聚类, 基于节点在结构上的相似性度量同时检测网络中的簇、桥节点和离群点. NetWalk 模型[14] 利用游走机制将网络分解为一系列团组, 通过团组嵌入的方式学习网络表示, 并使用蓄水池采样策略在网络的动态变化中对学习到的表示进行更新, 在此基础上采用动态聚类模型检测网络中的异常.

除了结构信息外, 网络数据中还常常具备描述节点特征的属性信息. 将结构与属性信息进行融合, 有助于提升异常检测的有效性. 这些检测方法可分为如下几类: 1) 从社区分析或测量自我中心网络的角度上发现异常, 例如 AMEN[6] 从每个节点的自我中心网络信息发现属性网络上的异常邻居; 2) 通过对节点特征子空间进行选择, 然后在子空间中发现异常, 例如 Sanchez 等[15] 提出了一种统计选择全等子空间的方法 ConSub 来捕获节点属性和图结构之间的依赖关系, 将其应用于社区离群点检测; 3) 基于残差分析的方法[7], 认为异常节点无法通过其他参考节点进行近似替代; 4) 基于属性网络重构损失的方法, 例如 Dominant[10] 通过图自编码器和图卷积神经网络的协同作用, 利用 GCN 学习到的节点表示对属性网络进行重构, 根据结构和属性两方面的重构损失评估节点的异常水平. Chen 等[9] 构建了基于生成对抗网络的检测模型, 训练以高斯噪声为输入的生成器借助先验数据分布进行数据生成, 通过鉴别器对编码器产生的真实节点和生成数据的成对嵌入进行判别, 并由节点属性重构误差和判别损失共同产生节点的异常分数.

1.2 图神经网络

图神经网络[16−17] 是一种利用图结构对节点属性和连接关系进行建模和学习, 并从网络数据中实现特征提取与表示的神经网络模型. 近年来, 随着网络数据在真实世界中大量涌现, 图神经网络在网络数据的分析处理中受到广泛关注, 取得了大量研究成果, 并在网络表示学习、图分类、链路预测和社区发现等各类任务中获得成功应用.

图卷积网络[18] 是一类被广泛使用的图神经网络模型, 根据特征提取方式的不同可以分为频域模型和空域模型两类. 前者从图信号处理的角度, 将图卷积层定义为一个滤波器, 使用图傅里叶变换及其扩展形式将节点表示转换至频谱域来执行卷积操作, 相当于通过滤波器从网络数据中过滤特定频带的信号. 后者从网络节点的空间关系出发, 通过邻域信息聚合机制迭代更新节点表示来定义卷积算子. 这类模型通常由邻域聚合函数、节点更新函数以及读出函数组成. 在邻域信息聚合的过程中, 考虑到各节点对当前节点状态更新的重要性可能存在差异, 图注意力网络 (Graph attention network, GAT)[19] 将图卷积和注意力机制相结合, 根据每个节点和邻居节点的属性信息, 在节点状态更新时依据自注意力机制计算各邻居节点的贡献度, 据此在信息聚合过程中给予各节点不同程度的关注, 提高模型的学习效率.

面向网络数据的无监督学习任务, 自编码器也经常被用作信息传播框架构建图神经网络. 例如, Hou 等[20] 设计了一种对抗属性自编码器 A3Graph, 由编码器将节点属性编码为低维隐空间中的低维表示, 并通过解码器将节点表示映射到由正值点互信息矩阵 (Positive pointwise mutual information, PPMI) 和属性矩阵组成的聚合矩阵, 再借助对抗式学习模式为编码器的输出施以先验分布来提高表示学习的稳定性. Wang 等[21] 提出了一种图卷积编码器框架 GASN, 首先使用改进的 GCN 对图结构和隐空间中的节点属性进行编码, 在此基础上设计了一种高通图解码器重构节点属性, 接着利用内积层重构网络结构关系, 最后构建统一优化框架对编码器和两个子解码器进行联合优化.

1.3 知识图谱嵌入

网络中的异常除了反映在拓扑结构和节点属性两个维度外, 还可以通过挖掘其领域知识描述进行识别. 作为一种常见的知识组织形式, 知识图谱[22] 以图的形式描述了客观世界中的实体及其之间的多种关系. 其中, 实体表示真实存在的对象或抽象概念, 关系记录了实体间的某种联系. 知识图谱作为丰富且易获取的重要知识来源, 在图像分类和推荐系统[23−26] 等各种应用中展现出重要价值, 受到人们的广泛关注. 近年来, 一些大型知识图谱数据库如 Freebase、WordNet 和 DBpedia[27] 等相继问世.

为了获取和在学习模型中使用知识图谱中的知识, 需要通过嵌入方法[28] 将知识图谱中的实体和关系映射到低维向量空间, 在保留知识图谱结构信息的同时获得知识的表示. 知识图谱嵌入方法可大致分为 3 类: 1) 基于距离的模型[29], 将关系建模为从头实体到尾实体的距离变换, 通过最小化变换后两个实体间的距离误差, 将知识图谱中的实体和关系类型分别映射到低维空间; 2) 基于语义匹配的模型[30], 利用相似度评分函数构建实体和关系嵌入向量之间的交互关系, 通过匹配不同实体和关系类型的潜在语义, 在度量事实合理性的过程中学习知识嵌入; 3) 基于神经网络的模型[31], 凭借神经网络对非线性复杂关系的表达能力, 通过对输入数据特征分布的空间转换, 学习知识图谱中的结构特征和语义特征, 在结构和关系建模方面提升知识图谱嵌入的性能.

领域知识在网络数据之外的另一个视角为下游任务的决策生成提供了重要信息依据. 为此, 本文借助知识图谱嵌入在知识视图中为输入网络构造孪生网络, 并通过对数据视图和知识视图中网络表示的聚合实现对异常节点的识别, 提高异常检测的有效性.

2 问题定义

定义 1. 属性网络: 给定一个网络 $\mathcal{G} = (V, E, X)$, 其中, $V = \{v_i | i = 1, 2, \cdots, n\}$表示网络中 n个节点构成的集合, 每个节点具有 d 个属性, $x_i \in X(i = 1, 2, \cdots, n)$表示节点 v_i 的属性向量, $X \in \mathbf{R}^{n\times d}$表示所有节点的属性向量组成的矩阵. $E = \{e(i, j) | v_i \in V, v_j \in V\}$是网络中所有边构成的集合, $e(i, j)$表示节点 v_i 和 v_j之间的边, 共 $|E| = m$ 条边. 此外, 通过邻接矩阵 $A \in \mathbf{R}^{n\times n}$ 表示属性网络的拓扑结构, 若节点 v_i 和 v_j 之间存在边, 则 $A_{ij} = 1$, 否则 $A_{ij} = 0$.

定义 2. 领域知识图谱: 通常被表示为 $\mathcal{T} = (N, R, T)$, 其中, N 为实体构成的集合, R 表示关系的集合, 集合中的关系 $\boldsymbol{r}$ 连接两个实体构成三元组 $(\boldsymbol{h}, \boldsymbol{r}, \boldsymbol{t}) \in T$, $\boldsymbol{h} \in N$ 为头实体, $\boldsymbol{t} \in N$ 为尾实体, T 表示三元组构成的集合. 知识图谱以三元组形式描述了相关对象的概念及联系, 例如三元组 (狮子王, 制片公司, 迪士尼), 表述了“电影《狮子王》的制片公司是迪士尼”这一事实.

定义 3. 融合领域知识的多视图异常检测: 给定属性网络 $\mathcal{G}$ 和领域知识图谱 $\mathcal{T}$, 该任务的目标是学习一个异常检测模型 $\mathcal{F}(\mathcal{G}, \mathcal{T})$: $V \to \mathbf{R}^n$, 获得属性网络中各节点的异常得分, 进而衡量其异常程度.

3 MOD-KF 模型

针对属性网络在有限信息来源下难以对异常对象做出可靠描述的问题, 提出了一种异常检测模型 —— MOD-KF. 该模型的总体架构如图 2 所示, 以图自编码器为信息处理框架, 由 4 个基本组件构成: 1) 孪生网络构造模块, 使用 TransR 模型学习属性网络对应的领域知识图谱嵌入, 并依据网络的拓扑关系构造其知识视图下的孪生网络; 2) 多视图编码器, 在数据视图和知识视图下通过两组并行的 GAT 分别构造属性编码器和知识编码器, 学习属性网络和孪生网络的嵌入; 3) 聚合器, 将不同视图下的网络嵌入聚合为统一表示; 4) 解码器, 由节点的统一表示对网络的拓扑结构和节点特征进行重构, 借助这两个维度上的重构误差建立模型的优化目标, 并输出网络节点异常评分.

3.1 孪生网络构造模块

孪生网络具有和输入网络相同的拓扑结构, 与后者使用属性信息进行节点描述不同, 孪生网络将领域知识作为另一个视角下对节点的特性描述.

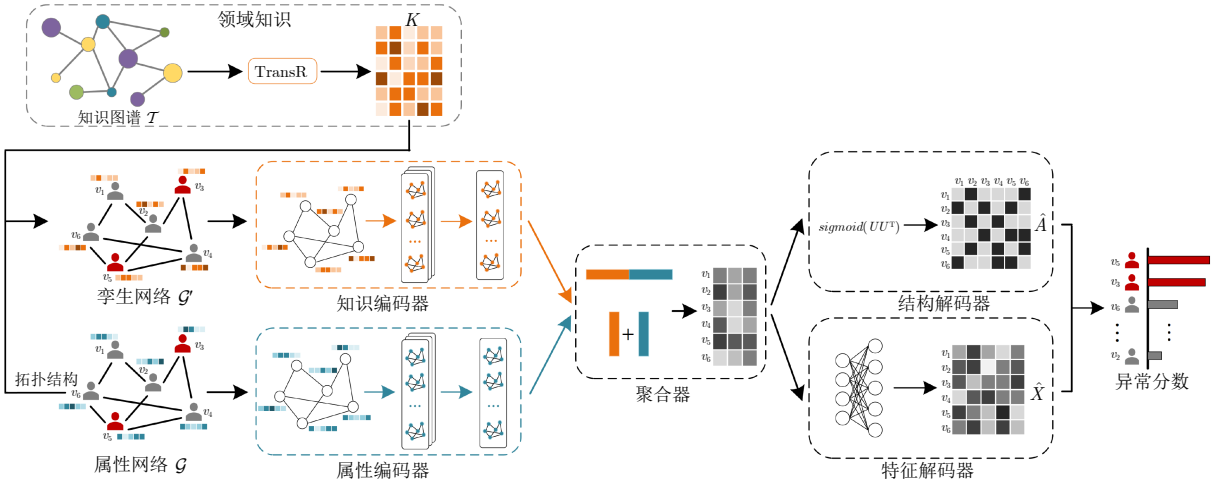


图 2 MOD-KF 模型总体框架

Fig. 2 The overall framework of the MOD-KF model

对于属性网络 $\mathcal{G}=(V, E, X)$, 其孪生网络的构造包含两个步骤: 首先, 使用 TransR 模型对其相关的领域知识图谱进行嵌入学习, 以获得节点知识的向量表示; 接着依据网络的拓扑结构将这些知识表示进行关联, 完成孪生网络构造. 在知识图谱中, 每个实体通常会通过不同的关系连接到其他实体上, 这些关系从多个方面对实体的特性进行刻画. TransR 模型在实体空间和关系空间分别对实体和关系进行建模, 并通过在相应关系空间中投影实体间转换来学习实体和关系的嵌入.

具体来说, 对于一个三元组 $(\boldsymbol{h}, \boldsymbol{r}, \boldsymbol{t})$, 将头实体与尾实体的嵌入分别记作 $\boldsymbol{h}$ 和 $\boldsymbol{t}$, 令 $\boldsymbol{r}$ 表示实体间关系的嵌入. 通过为关系 $\boldsymbol{r}$ 设置一个映射矩阵 M_r, 可以将实体由实体空间投影到相应的关系空间, 分别获得头实体投影向量 $\boldsymbol{h}_r$ 和尾实体投影向量 $\boldsymbol{t}_r$ 如式 (1) 所示:

$$\boldsymbol{h}_r=\boldsymbol{h}M_r, \quad \boldsymbol{t}_r=\boldsymbol{t}M_r \tag{1}$$

随后, 在投影实体之间建立转换, 通过式 (2) 的得分函数计算头尾实体投影向量之间的距离, 以此来衡量事实成立的可能性:

$$f_r(\boldsymbol{h}, \boldsymbol{t})=\|\boldsymbol{h}_r+\boldsymbol{r}-\boldsymbol{t}_r\|_2^2 \tag{2}$$

特定关系的投影可以使那些实际具有这种关系的头尾实体彼此靠近, 否则使它们相互远离.

使用式 (1) 和式 (2) 以迭代方式对三元组的嵌入表示不断更新, 从表示结果中抽取与各网络节点相关的知识向量表示, 构建输入网络的知识矩阵, 记作 $K\in\mathbf{R}^{n\times d}$, 该矩阵的每一行记录了各节点的知识特征. 在此基础上, 基于属性网络 $\mathcal{G}=(V, E, X)$ 的拓扑结构构造其孪生网络, 记作 $\mathcal{G}'=(V, E, K)$.

3.2 多视图编码器

多视图编码器由属性编码器和知识编码器构成, 分别用于在不同视图下对属性网络和孪生网络进行编码, 学习节点在低维隐空间中的相应表示. 属性网络中的节点是对现实世界相应实体的抽象表达, 在实际场景中, 实体的不同邻居通常对其有着不同程度的影响, 为此本文使用两组并行的 GAT 网络构成多视图编码器. 通过自注意力机制对节点权重进行自适应匹配, 在对邻域信息进行聚合的过程中, 将节点之间的关联关系更好地融合到节点表示中.

1) 属性编码器. 由两个注意力层堆叠而成, 在数据视图下对属性网络 $\mathcal{G}=(V, E, X)$ 进行编码. 其中, 第一层使用多头注意力机制, 第二层使用单头注意力机制, 属性编码器输出如式 (3) 所示:

$$Z_{\mathcal{G}}=f(f(X, A), A) \tag{3}$$

其中, $Z_{\mathcal{G}}\in\mathbf{R}^{n\times d'}$ 为属性编码器输出的节点表示, 函数 $f(X, A)$ 表示图注意力层. 在进行节点邻域信息聚合的过程中, 图注意力机制对邻域内各节点赋予了不同的注意力系数. 节点与其邻居节点之间的注意力系数由式 (4) 计算:

$$e_{ij}=LeakyReLU\left(\boldsymbol{c}^{\mathrm{T}}\left([W_{\mathrm{enc}}\boldsymbol{x}_i \parallel W_{\mathrm{enc}}\boldsymbol{x}_j]\right)\right) \tag{4}$$

式中, e_{ij} 是节点 v_i 和节点 v_j 之间的注意力系数, 表示节点 v_j 对于节点 v_i 的重要程度, $v_j\in\mathcal{N}_i$, $\mathcal{N}_i$ 为节点 v_i 的一阶邻居节点集合. $W_{\mathrm{enc}}\in\mathbf{R}^{h'\times d}$ 是作用到每个节点上的可学习权重矩阵. $\parallel$ 表示拼接操作, $\boldsymbol{c}\in\mathbf{R}^{2h'}$ 为权重向量.

为了使节点之间的注意力系数易于比较, 通过式 (5) 对注意力系数进行归一化:

$$\alpha_{ij}=\frac{\exp\left(e_{ij}\right)}{\sum\limits_{v_j\in\mathcal{N}_i}\exp\left(e_{ij}\right)} \tag{5}$$

利用归一化注意力系数对邻居节点进行聚合, 如式 (6) 所示:

$$\boldsymbol{x}_i'=\sigma\left(\sum_{v_j\in\mathcal{N}_i}\alpha_{ij}W_{\text{enc}}\boldsymbol{x}_j\right) \tag{6}$$

其中, $\sigma(\cdot)$ 为激活函数, 实现对数据的非线性变换.

以上步骤通过单头注意力机制聚合邻域信息对节点表示进行了更新. 进一步地, 为了增强模型泛化能力, 在图注意力层中引入多头注意力机制, 通过多个相互独立的单头注意力网络分别计算出一组注意力系数, 再通过式 (7) 将多个表示结果进行拼接, 得到节点 v_i 的表示输出:

$$\boldsymbol{x}_i'=\|_{p=1}^{P}\ \sigma\left(\sum_{v_j\in\mathcal{N}_i}\alpha_{ij}^{p}W_{\text{enc}}^{p}\boldsymbol{x}_j\right) \tag{7}$$

其中, P 表示单头注意力网络的数量, α_{ij}^{p} 表示第 p 个注意力网络计算得到的注意力系数, W_{enc}^{p} 表示第 p 个注意力网络的权重矩阵.

2) 知识编码器. 知识视图下的编码器具有和属性编码器完全相同的结构, 用于学习孪生网络 $\mathcal{G}'=(V, E, K)$ 的表示, 其构成如式 (8) 所示:

$$Z_{\mathcal{G}'}=f\left(f\left(K, A\right), A\right) \tag{8}$$

其中, $Z_{\mathcal{G}'}\in\mathbf{R}^{n\times d'}$ 为知识编码器输出的孪生网络的节点表示.

3.3 聚合器

原始属性网络及其孪生网络是对不同视角下同一复杂系统的信息描述, 二者的网络表示在模型决策过程中能为彼此提供互补信息. 为了提高模型决策的有效性, 本文利用聚合器对不同视图下的网络表示进行融合, 进而获得网络节点的多视图统一表示. 我们采用了两种视图聚合策略, 具体如下:

1) 拼接聚合器 (Concat): 对两个视图的节点向量表示进行纵向拼接, 形成一个维度更高的向量, 如式 (9) 所示:

$$U=concat\left(Z_{\mathcal{G}}, Z_{\mathcal{G}'}\right) \tag{9}$$

其中, $concat(\cdot)$ 表示纵向拼接操作, $U\in\mathbf{R}^{n\times(2d')}$ 表示拼接聚合后形成的多视图统一表示.

2) 加和聚合器 (Add): 由两个视图的节点向量表示按照对应元素相加的方式, 获得一个同维度的新向量, 如式 (10) 所示:

$$U=Z_{\mathcal{G}}+Z_{\mathcal{G}'} \tag{10}$$

其中, $U\in\mathbf{R}^{n\times d'}$ 为使用加和聚合器获得的多视图统一表示.

3.4 解码器

解码器包含结构解码器和特征解码器两个部分, 依据节点统一表示分别对网络的拓扑结构和节点特征进行重构.

1) 结构解码器, 通过计算节点统一表示间的内积实现对网络拓扑的重构, 如式 (11) 所示:

$$\hat{A}=sigmoid\left(UU^{\mathrm{T}}\right) \tag{11}$$

其中, $\hat{A}$ 表示重构后的网络拓扑结构.

2) 特征解码器, 使用两层全连接网络实现对节点特征的重构, 如式 (12) 所示:

$$\hat{X}=\left(\left(UW_{\text{dec}}^{(0)}+\boldsymbol{b}^{(0)}\right)W_{\text{dec}}^{(1)}+\boldsymbol{b}^{(l)}\right) \tag{12}$$

其中, $\hat{X}$ 为节点的重构特征信息, $\boldsymbol{b}^{(l)}$ 表示第 l 个全连接层的偏置向量. 特征解码器的输出是对网络的节点属性和领域知识两类信息在同一特征空间中的重构.

在上述框架中, 经过对属性网络和孪生网络的多视图编码、聚合以及重构过程, 实现了领域知识和属性网络在低维表示中的有效融合, 丰富和完善了学习模型的信息来源和决策依据, 对于提升模型决策的有效性和可靠性具有积极作用.

3.5 优化模型及异常评分

MOD-KF 模型的优化目标由两部分组成, 如式 (13) 所示:

$$\mathcal{L}=\lambda\mathcal{L}_f+(1-\lambda)\mathcal{L}_s \tag{13}$$

其中 $\mathcal{L}_f$ 为特征重构误差, 使用 F-范数由式 (14) 定义:

$$\mathcal{L}_f=\left\|X+K-\hat{X}\right\|_{\text{F}}^{2} \tag{14}$$

由于解码器的输入为聚合后的节点统一表示, 因此在计算特征重构误差时将原始网络与孪生网络中的属性作为共同参照. $\mathcal{L}_s$ 为结构重构误差, 由式 (15) 定义:

$$\mathcal{L}_s=\left\|A-\hat{A}\right\|_{\text{F}}^{2} \tag{15}$$

$\lambda\in[0, 1]$ 为平衡系数, 用于调整两种重构误差间的权重.

网络中的异常节点通常与其他节点存在某种数据模式上的显著差异, 因而本文将节点重构误差作为评价节点异常分数的重要手段, 并给出节点异常评分函数如式 (16) 所示:

$$score\,(v_i) = \lambda \left\| \boldsymbol{x}_i + \boldsymbol{k}_i - \hat{\boldsymbol{x}}_i \right\|_2^2 + (1-\lambda) \left\| \boldsymbol{a}_i - \hat{\boldsymbol{a}}_i \right\|_2^2 \tag{16}$$

式中 $score\,(v_i)$ 为节点 v_i 的异常分数, 用于反映该节点的异常程度, 取值越大表明节点的异常程度越高.

综上, MOD-KF 模型的算法实施流程总结为算法 1.

算法 1. 属性网络异常检测算法 MOD-KF

输入. 属性网络 $\mathcal{G} = (V, E, X)$, 领域知识图谱 $\mathcal{T} = (N, R, T)$, 平衡系数 λ, 注意力头数 P, 最大迭代次数 L.

输出. 节点异常评分: $score\,(v_i)$.

1) 随机初始化头实体 $\boldsymbol{h}$, 尾实体 $\boldsymbol{t}$, 关系 $\boldsymbol{r}$, 映射矩阵 M_r, 可训练参数矩阵 W_{enc}, W_{dec}, 权重向量 $\boldsymbol{c}$ 和偏置向量 $\boldsymbol{b}$;

2) $i \leftarrow 0$;

3) while $i < L$ do

4) 根据式 (1) 计算 $\boldsymbol{h}$ 和 $\boldsymbol{t}$ 在映射矩阵下的投影向量;

5) 根据式 (2) 计算三元组的得分;

6) 反向传播更新 $\boldsymbol{h}$, $\boldsymbol{r}$, $\boldsymbol{t}$ 和 M_r;

7) end while

8) 基于领域知识矩阵 K 构造孪生网络 $\mathcal{G}'$;

9) while $i < L$ do

10) 根据式 (4) 和式 (5) 分别计算 $\mathcal{G}$ 和 $\mathcal{G}'$ 中所有节点和其邻居节点之间的注意力系数 e, 并归一化;

11) 根据式 (6) 和式 (7) 计算属性编码器的输出 $Z_{\mathcal{G}}$ 和知识编码器的输出 $Z_{\mathcal{G}'}$;

12) 使用式 (9) 或式 (10) 对 $Z_{\mathcal{G}}$ 和 $Z_{\mathcal{G}'}$ 进行聚合, 获得多视图统一表示;

13) 根据式 (11) 和式 (12) 进行拓扑重构及特征重构;

14) 根据式 (13) 计算损失 $\mathcal{L}$;

15) 反向传播更新所有可训练参数 W_{enc}, W_{dec}, $\boldsymbol{c}$ 和 $\boldsymbol{b}$;

16) end while

17) Return $score\,(v_i)$.

3.6 复杂度分析

MOD-KF 模型由多视图编码器、聚合器和解码器 3 个主要模块构成. 在多视图编码器中, 两层图注意力层的计算复杂度可以表示为 $\mathrm{O}(nd'H + md')$, 其中, $H = \max(d', d)$, d' 为编码器的嵌入维度, n 为网络中节点的个数, m 为网络邻接矩阵 A 中非零元素的数量. 聚合器的时间复杂度为 $\mathrm{O}(2nd')$, 解码器中结构和特征重构的复杂度分别为 $\mathrm{O}(n^2d')$ 和 $\mathrm{O}(nd'H)$. 由于 n 一般远大于 2, 因此, 模型的总体时间复杂度为 $\mathrm{O}(nd'H + md' + n^2d')$.

4 实验及分析

4.1 实验数据

仿真实验使用了 3 个由真实信息网络采集获得的属性网络数据集, 同时构造了这些数据集所涉领域的知识图谱形成对属性网络的知识描述. 为确保实验数据的有效性, 我们在数据集的构造过程中考虑了以下问题: 1) 确保数据集具备一定规模, 以充分表现出研究对象应该具备的特征; 2) 当实验数据来自超大规模原始数据集的采样时, 确保数据采样尽可能保留原有数据的分布特性.

AmazonBooks. 图书评分数据集, 来自商品评价数据集 Amazon Review Dataset 中的图书品类, 由用户对 290 余万种图书的超过 5 000 万条评论构成, 包含了商品信息和用户评论两部分. 我们将图书商品作为节点, 利用用户与商品间的共同购买关系构建网络.

MovieLens. 电影评分数据集, 由电影信息、用户信息、评分信息 3 部分构成, 记录了 6 040 位用户对 3 900 部电影的约 100 万条评分数据. 我们将影片作为网络节点, 每个节点包含了影片类型、评价得分和上映时间等 20 个属性, 将用户对影片的共同评价关系作为节点间连边.

Last.FM. 由在线音乐网站 Last.FM 采集的音乐收听记录数据集, 由用户信息、歌曲信息和收听记录构成. 在该数据集中, 歌曲信息包含名称、ID、演唱者、流派、风格等特征. 我们将歌曲作为节点, 以用户对歌曲的共同收听关系作为节点间连边.

为了保证数据质量, 我们依据 10-core 原则从上述数据集中抽取至少存在 10 个交互关系的用户和项目, 借助交互关系构建网络数据集. 在此基础上, 通过异常注入[32−33] 的方式向上述数据集分别注入结构异常和属性异常, 进而产生异常节点作为检测目标. 具体而言, 在注入结构异常时, 设置 AmazonBooks 和 Last.FM 数据集中的小集团规模为 20, 数量为 10; 设置 MovieLens 数据集中的小集团规模为 10, 数量为 5. 在注入属性异常时, 每个数据集在随机抽取的 100 个节点范围内选取差异最大的两个节点进行属性交叉. 在领域知识描述方面, 使用由 DBpedia 和 Freebase 中抽取的与上述数据集相关的三元组, 构建其领域知识图谱. 实验所用数据集的具体统计信息如表 1 所示.

4.2 实验设置

1) 基线方法

本文选取 5 种异常检测算法作为基线方法与本文提出的 MOD-KF 模型进行比较, 这些方法涵盖了属性网络异常检测的经典算法和最新成果, 并且涉及深度学习和多视图学习等不同策略. 具体包括: Radar[7], GAAN[9], Dominant[10], SpecAE[11], ALA-

表 1　实验数据集统计信息
Table 1　Statistics of datasets in experiment

数据集	网络特性				领域知识		
	节点	属性	边	异常率	实体	关系	三元组
AmazonBooks	24 915	28	128 742	0.0247	124 320	93	541 853
MoviesLens	2 182	20	31 573	0.0522	50 875	52	181 639
Last.FM	23 566	8	187 472	0.0258	47 986	12	325 147

RM[34]. 其中, Radar 是一种基于残差分析的无监督异常检测模型, 通过学习属性信息的残差及其与网络结构的一致性来检测异常节点; GAAN 是一种基于生成对抗性网络的异常检测方法, 依据能否在生成器的潜在空间中找到样本的适当表示实现对异常节点的识别; Dominant 认为网络中的异常节点由网络的拓扑结构和节点属性共同决定, 在 Autoencoder 框架下利用重构损失识别网络中的异常节点; SpecAE 是一个基于谱卷积和反卷积的框架, 利用拉普拉斯锐化来放大异常表示和其他节点表示之间的距离, 将重构误差与密度估计模型结合起来实现异常节点检测; ALARM 是一个多视图异常检测模型, 通过多个并行的图编码器学习节点在不同数据视图下的表示, 再依据多视图聚合结果的解码情况进行异常节点的识别.

2) 评估指标

在实验中使用以下 3 个异常检测的常用指标对各方法的性能进行评价.

ROC-AUC. 作为异常检测方法中广泛使用的评估手段, ROC 图是根据真实异常分布和异常检测结果绘制的真阳性率与假阳性率相关性曲线. AUC 值是 ROC 图中曲线下的面积, 直观上表示模型能够对网络中任意一对异常节点和正常节点进行正确划分的概率. AUC 取值越接近 1, 表示模型的异常检测性能越好.

Precision@K. 表示由异常检测模型产生的前 K 个检测结果中真实异常节点所占比例, 这一结果是对模型异常检测精度的反映.

Recall@K. 表示由异常检测模型产生的前 K 个检测结果中真实异常节点在异常总数中所占的比例, 该指标取值越接近 1 表示异常检测结果的有效性越高.

3) 实验参数设置

为了避免随机性对实验结果产生的影响, 每种算法随机运行 50 次, 取其结果的平均值进行比较. 在实验中, 将所有算法编码器的节点嵌入维度设为 128. MOD-KF 模型使用 Adam 优化器进行训练, 学习率设为 0.006, 平衡系数设为 $\lambda = 0.5$, 注意力头数设为 5. 根据 MOD-KF 聚合器的实现方式不同, 将其分为两种方法进行实验比较, 即使用加和聚合器的 MOD-KF_Add 和使用拼接聚合器的 MOD-KF_Concat. 各基线方法依据其作者给出的建议设置参数.

4.3　实验结果与分析

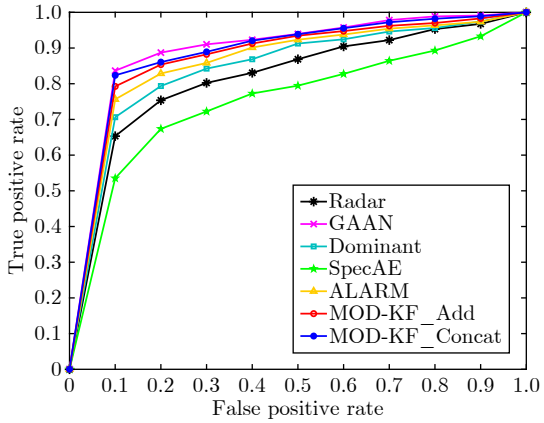
4.3.1　检测性能比较

表 2 给出了不同异常检测方法在 3 个数据集上获得的 AUC 值, 相应的 ROC 曲线如图 3 所示.

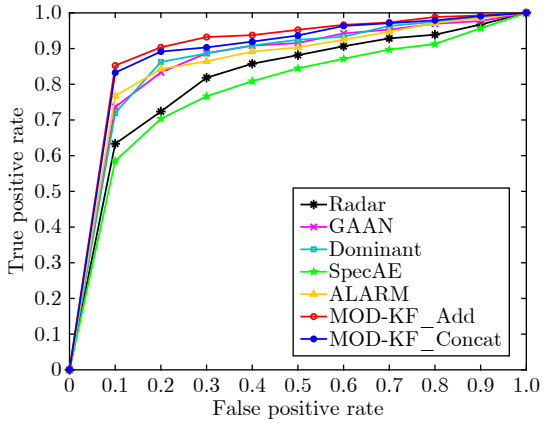
表 2　各方法在不同数据集上的 AUC 值
Table 2　AUC values of each method on different datasets

方法	AmazonBooks	MovieLens	Last.FM
Radar	0.7205	0.7586	0.6891
GAAN	**0.8436**	0.8203	0.7504
Dominant	0.7585	0.8246	0.7331
SpecAE	0.6824	0.7348	0.6706
ALARM	0.7643	0.8165	0.7729
MOD-KF_Add	0.8230	**0.8852**	0.8106
MOD-KF_Concat	0.8364	0.8743	**0.8213**

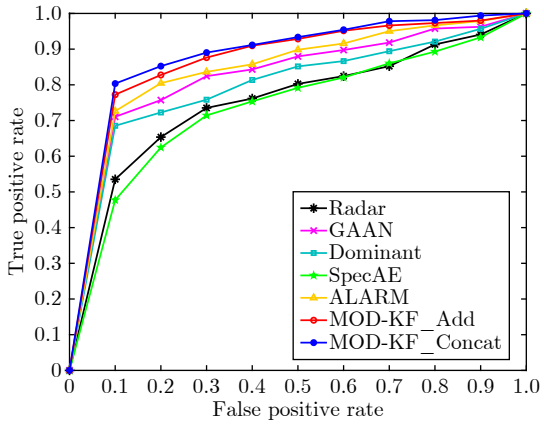
总体来看, MOD-KF 模型在使用两种聚合策略时都可以在 3 个实验数据集上获得较为优秀的异常检测性能. SpecAE 算法利用谱自编码器分别学习节点属性和网络结构的向量表示, 并利用属性重构误差实现全局异常节点的实现. 由于网络异常是在属性与结构的共同影响下产生的, SpecAE 算法在学习网络表示与设计优化目标时将二者作为独立的因素处理, 因而在 3 个数据集上的检测结果 AUC 最低. Radar 算法通过学习和分析残差来识别网络中属性和结构异于其他部分的少数节点, 受限于其浅层机制, 算法处理网络稀疏性、数据非线性和复杂交互的能力不足, 因而难以获得令人满意的检测结果. Dominant 算法借助深度神经网络为网络节点学习有效的低维表示, 其异常检测结果的 AUC 值相比 SpecAE 和 Radar 有较为明显的提高. ALARM 算法将节点属性划分为若干视图, 在不同视图下学习节点低维表示, 基于多视图融合结果实现异常的



(a) AmazonBooks 数据集上的 ROC 曲线
(a) ROC curves on AmazonBooks dataset



(b) MovieLens 数据集上的 ROC 曲线
(b) ROC curves on MovieLens dataset



(c) Last.FM 数据集上的 ROC 曲线
(c) ROC curves on Last.FM dataset

图 3 各方法在不同数据集上的 ROC 曲线

Fig. 3 ROC curves of each method on different datasets

识别, 有利于挖掘异常模式在不同视图下的潜在特性, 一定程度上提升了模型的检测性能, 但是该算法在进行视图划分时可能面临多维属性耦合产生的不利影响. GAAN 算法在 AmazonBooks 数据集上获得了最优检测结果, 这主要是由于该算法具有一定的生成能力, 从而在训练数据较为有限的情况下改善了模型对于异常模式分布特性的捕捉能力. 同时, 由于 GAAN 的生成器需要使用特定分布的噪声产生负样本, 当网络数据的分布特性和异常模式较为复杂时, 模型的性能受到一定影响, 因而在 MovieLens 和 Last.FM 数据集上表现一般. 本文提出的 MOD-KF 模型利用领域知识生成待检测网络的孪生网络, 将领域知识作为对网络数据的有效补充, 从知识视图和数据视图共同形成对网络异常的识别决策. 在 MovieLens 和 Last.FM 数据集上, MOD-KF_Add 和 MOD-KF_Concat 的检测结果分别获得最优 AUC 值, 在 AmazonBooks 数据集上, 这两种算法相比最优的 GAAN 算法非常接近. 这表明在多视图框架下融合领域知识对于提高模型在属性网络异常检测任务中的决策能力是可行且有效的.

表 3 和表 4 分别给出了不同异常检测算法在 3 个数据集上获得的 Precision@K 和 Recall@K 评估结果. 其中, 对于规模较小的 MovieLens 数据集, K 的取值依次设为 5, 10, 50, 100; 在另外两个数据集上, K 的取值依次设为 50, 100, 200, 500.

从这些结果可以观察到, MOD-KF 在大多数情况下相比其他算法能够识别更多真实的异常节点. 值得注意的是, 在 AmazonBooks 数据集上, GAAN 获得了最高的 Precision@200 和 Precision@500 值, 而 MOD-KF_Add 则获得了更具优势的 Precision@50 和 Precision@100 结果. 这表明, 在排名较高的检测结果中, MOD-KF_Add 的决策更加可靠, 这对于一些需要识别关键异常的场景具有重要意义. 在 MovieLens 数据集上, ALARM 算法获得了最优的 Recall@5 结果, 但随着 K 的增大, MOD-KF_Add 和 MOD-KF_Concat 逐渐表现出优势. 这些实验结果表明, MOD-KF 模型在不同尺度范围内都能够获得对网络异常节点较高的查准率和查全率.

此外, 通过实验结果还可以发现, MOD-KF 模型在使用两种基础聚合策略时都获得了可靠性较高的异常检测结果, 这表明在该框架下加和策略和拼接策略都能够实现领域知识和网络数据的有效融合, 进而提高模型的异常检测性能.

4.3.2 消融实验

为了考察 MOD-KF 模型不同构件在异常检测中发挥的作用和对模型的影响, 我们仅保留 MOD-KF 中知识视图的处理环节, 将算法记作 MOD-KF_1, 仅保留 MOD-KF 中数据视图的处理环节, 将算法记作 MOD-KF_2. 在 3 个数据集上将它们与 MOD-KF_Add 和 MOD-KF_Concat 进行比

表 3 不同算法的 Precision@K 结果

Table 3 Results of different algorithms in terms of Precision@K

数据集	K	异常检测方法						
		Radar	GAAN	Dominant	SpecAE	ALARM	MOD-KF_Add	MOD-KF_Concat
AmazonBooks	50	0.8236	0.9008	0.8412	0.7784	0.8431	**0.9248**	0.9183
	100	0.8393	0.9078	0.7927	0.8069	0.8113	**0.9194**	0.9146
	200	0.7543	**0.8851**	0.7329	0.7208	0.7840	0.8742	0.8616
	500	0.7340	**0.8633**	0.7624	0.6905	0.7517	0.8526	0.8519
MovieLens	5	0.8040	0.7960	**0.9840**	0.7920	0.9680	0.9800	0.9720
	10	0.8420	0.8540	0.8940	0.8180	0.8960	**0.9540**	0.9440
	50	0.7194	0.8405	0.8368	0.8177	0.8526	**0.9357**	0.9022
	100	0.7271	0.8111	0.8224	0.7670	0.8365	0.8978	**0.9095**
Last.FM	50	0.8174	0.7579	0.8148	0.7392	0.8384	**0.9002**	0.8886
	100	0.7855	0.7413	0.7969	0.7132	0.8085	0.8826	**0.8871**
	200	0.7247	0.7554	0.7331	0.6807	0.7948	**0.9053**	0.8966
	500	0.6716	0.7525	0.7143	0.6365	0.7743	0.8623	**0.8704**

表 4 不同算法的 Recall@K 结果

Table 4 Results of different algorithms in terms of Recall@K

数据集	K	异常检测方法						
		Radar	GAAN	Dominant	SpecAE	ALARM	MOD-KF_Add	MOD-KF_Concat
AmazonBooks	50	0.0631	0.0728	0.0662	0.0618	0.0660	**0.0746**	0.0743
	100	0.1319	0.1471	0.1353	0.1185	0.1304	0.1486	**0.1506**
	200	0.2425	**0.2839**	0.2495	0.2311	0.2351	0.2792	0.2805
	500	0.5880	0.6810	0.6063	0.5211	0.5903	0.6776	**0.6846**
MovieLens	5	0.0322	0.0356	0.0353	0.0296	**0.0423**	0.0420	0.0416
	10	0.0684	0.0752	0.0781	0.0654	0.0733	0.0813	**0.0852**
	50	0.3238	0.3228	0.3611	0.3141	0.3599	**0.4040**	0.3961
	100	0.6359	0.7041	0.7098	0.5811	0.7118	**0.7862**	0.7770
Last.FM	50	0.0659	0.0609	0.0644	0.0610	0.0656	0.0712	**0.0724**
	100	0.1074	0.1086	0.1164	0.1034	0.1121	0.1221	**0.1257**
	200	0.2291	0.2380	0.2475	0.2231	0.2420	**0.2788**	0.2771
	500	0.5467	0.5990	0.5957	0.5131	0.6340	0.6931	**0.7022**

较, 各算法异常检测结果的 AUC 值如图 4 所示.

可以看出, 无论是单独利用知识视图的 MOD-KF_1 还是单独利用数据视图的 MOD-KF_2, 它们的异常检测性能相比 MOD-KF_Add 和 MOD-KF_Concat 都存在较为显著的差距. 这一结果表明, 对网络数据和领域知识的挖掘都为异常检测的决策生成提供了可用依据, 同时二者形成的关于异常节点分布特性的描述都存在局限性. 通过对知识表示和数据表示进行简单的“加和”或“拼接”使得异常检测性能得到显著提升, 一方面验证了 MOD-KF 模型的有效性, 另一方面也反映出知识视图和数据视图在描述网络数据分布特性方面存在一定的一致性和互补性.

4.3.3 参数分析

为了探究平衡系数 λ、注意力头数以及嵌入维度等参数对 MOD-KF 模型性能的影响, 我们对这些参数取不同值时模型的 AUC 值进行比较. 由于模型的两个版本获得的异常检测结果较为接近, 我们在参数分析实验中使用了 MOD-KF_Add 方法.

1) 平衡系数

平衡系数 λ 用于调节模型优化目标的内部构成, 当 $\lambda = 0$ 时, 模型将属性图和知识图聚合表示的结构重构误差作为优化目标, 完全依据结构特性进行异常的识别; 当 $\lambda = 1$ 时, 模型将聚合表示的特征重构误差作为优化目标, 依赖节点属性和领域知识判断节点是否异常. λ 取值在此区间内时, 结构特

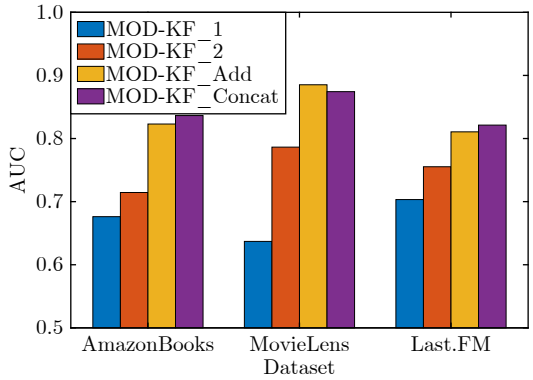


图 4 消融实验结果

Fig. 4 Detection results of ablation experiment

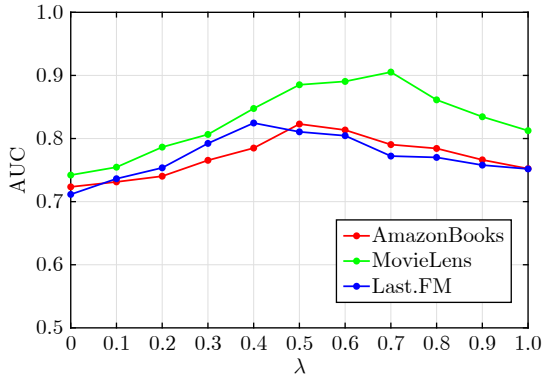


图 5 不同 λ 值对检测结果的影响

Fig. 5 Impact of different λ values on detection result

性和节点特征以一定比例共同作为识别网络异常的决策依据. 固定其他两个参数的取值, 将平衡系数的取值范围设为 [0, 1], MOD-KF_Add 获得的异常检测结果随 λ 取值的变化情况如图 5 所示. 可以看出, λ 取值为 0 或 1 时, 模型都无法获得最优结果, 随着 λ 在这一区间内变化, 检测结果的 AUC 值会随之产生一定程度的改变. 在不同数据集上, 当 λ 取某一特定值时, 模型能够获得最优检测结果. 例如, 在 MovieLens 数据集上, 当 λ 取值在 0.7 附近时, 异常检测结果的 AUC 达到最高水平; 在 Last.FM 和 AmazonBooks 数据集上, λ 取值分别在 0.4 和 0.5 附近时模型获得最优检测结果. 这一结果与各数据集自身的数据分布以及异常模式有一定联系. 因此, 聚合后的统一表示在结构描述和属性描述两个方面将对异常检测过程中的决策生成产生不同程度的影响.

2) 嵌入维度

图 6 显示了嵌入维度分别为 {2, 4, 8, 16, 32, 64, 128, 256, 512} 时模型异常检测结果的 AUC 变化情况. 由图中可以看出, 当嵌入维度处于较低水平时, 模型在不同数据集上的检测性能都随着嵌入维度的增加得到比较显著的提升. 这是由于较高的嵌入维度能保留对网络更加完整和全面的信息描述, 使模型获得可靠的检测结果. 当嵌入维度达到一定水平后, 维度的增加对模型性能的提升变得十分有限. 尤其是在 MovieLens 数据集上, 当嵌入维度由 256 增加到 512 时, 检测结果反而出现了一定程度的下滑. 这是由于嵌入维度过高时, 一些与异常检测决策生成无关的冗余信息也被保留, 甚至会对决策过程产生不利影响. 在上述实验中, 嵌入维度达到 32 后检测模型就可以获得较为可靠的检测结果, 这有利于控制下游异常检测任务的计算规模.

3) 注意力头数

此外, 我们通过对两个视图编码器中的注意力

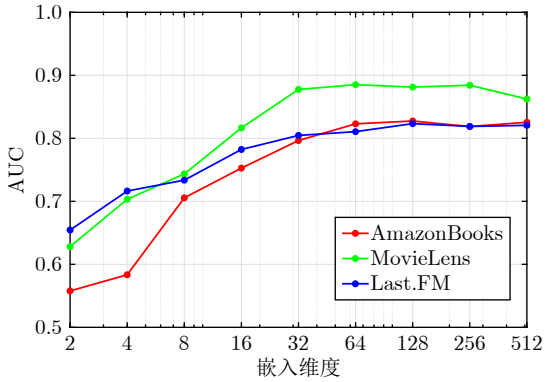


图 6 嵌入维度对检测结果的影响

Fig. 6 Impact of different embedding dimensions on detection result

头数进行调整, 讨论其对模型性能的影响, 实验结果如图 7 所示. 总体来看, 在不同的注意力头数下, 模型的检测性能所受影响较小, 整体上维持在较高水平. 在实验使用的 3 个数据集上, 将注意力头数设为 5 可以兼顾计算效率与异常检测性能.

5 结论

针对网络异常检测中存在的有效信息不足、难以生成可靠决策的问题, 提出了一种融合领域知识的多视图属性网络异常检测模型 MOD-KF. 该模型基于领域知识构造属性网络的孪生网络, 并通过多视图学习模式并行地学习属性网络与孪生网络的低维表示. 在对不同视图下网络表示进行聚合的基础上, 根据网络的重构误差建立异常评分机制实现对网络中异常节点的识别. 在真实属性网络数据集上的实验表明, MOD-KF 模型能够实现异常检测性能的显著提升. 本文为网络数据的异常检测问题提供了一种新的研究视角, 在 MOD-KF 提供的框架下, 大量知识表示、编码网络、解码策略以及信息

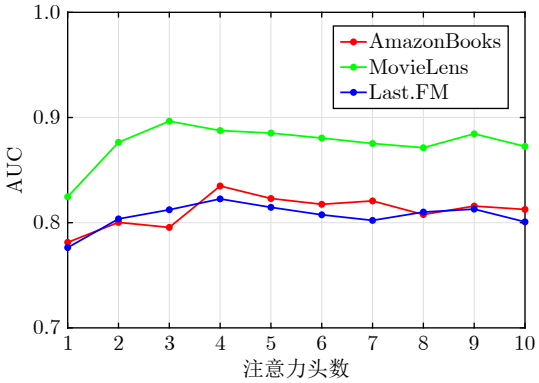


图 7 不同注意力头数对检测结果的影响

Fig. 7 Impact of different attention heads on detection result

融合的相关成果都可用于该框架, 构建出符合需要的异常检测算法. 特别是, 通过设计融合交互机制、一体化优化目标以及相应的训练策略等, 提出的孪生网络构造方法可视作一种元知识抽取, 用作改善其他现有异常检测方法的性能.

在未来工作中, 我们将围绕以下问题进一步探索领域知识在网络异常检测中的应用: 1) 探寻领域知识与网络数据间的互作用机制, 进而解释网络数据形成与演化机理; 2) 领域知识与网络数据间一致性和互补性的量化分析, 这将有利于提升异常检测分析的有效性; 3) 借助领域知识进行模型决策解释, 以及构建解释性更佳的模型, 这将有利于揭示异常产生的机理, 形成对网络异常的根本性认知.

References

1 Wu L C, Wang D L, Song K S, Feng S, Zhang Y F, Yu G. Dual-view hypergraph neural networks for attributed graph learning. *Knowledge-Based Systems*, 2021, **227**: Article No. 107185

2 Yang Z, Liu X D, Li T, Wu D, Wang J J, Zhao Y W, et al. A systematic literature review of methods and datasets for anomaly-based network intrusion detection. *Computers & Security*, 2022, **116**: Article No. 102675

3 Song J S, Qu X R, Hu Z H, Li Z, Gao J, Zhang J. A subgraph-based knowledge reasoning method for collective fraud detection in E-commerce. *Neurocomputing*, 2021, **461**: 587−597

4 Wang Z Y, Wei W, Mao X L, Guo G B, Zhou P, Jiang S. User-based network embedding for opinion spammer detection. *Pattern Recognition*, 2022, **125**: Article No. 108512

5 Breunig M M, Kriegel H P, Ng R T, Sander J. LOF: Identifying density-based local outliers. *SIGMOD Record*, 2000, **29**(2): 93−104

6 Perozzi B, Akoglu L. Scalable anomaly ranking of attributed neighborhoods. In: Proceedings of the SIAM International Conference on Data Mining (SDM). Miami, Florida, USA: SIAM, 2016. 207−215

7 Li J D, Dani H, Hu X, Liu H. Radar: Residual analysis for anomaly detection in attributed networks. In: Proceedings of the 26th International Joint Conference on Artificial Intelligence. Melbourne, Australia: IJCAI, 2017. 2152−2158

8 Gutierrez-Gomez L, Bovet A, Delvenne J C. Multi-scale anomaly detection on attributed networks. In: Proceedings of the 34th AAAI Conference on Artificial Intelligence. New York, USA: AAAI, 2020. 678−685

9 Chen Z X, Liu B, Wang M Q, Dai P, Lv J, Bo L F. Generative adversarial attributed network anomaly detection. In: Proceedings of the 29th ACM International Conference on Information and Knowledge Management. Ireland: ACM, 2020. 1989−1992

10 Ding K Z, Li J D, Bhanushali R, Liu H. Deep anomaly detection on attributed networks. In: Proceedings of the 19th SIAM International Conference on Data Mining. Calgary, Alberta, Canada: SIAM, 2019. 594−602

11 Li Y N, Huang X, Li J D, Du M N, Zou N. SpecAE: Spectral autoencoder for anomaly detection in attributed networks. In: Proceedings of the 28th ACM International Conference on Information and Knowledge Management. Beijing, China: ACM, 2019. 2233−2236

12 Hooi B, Song H A, Beutel A, Shah N, Shin K, Faloutsos C. Fraudar: Bounding graph fraud in the face of camouflage. In: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. San Francisco, USA: ACM, 2016. 895−904

13 Xu X W, Yuruk N, Feng Z D, Schweiger T A J. Scan: A structural clustering algorithm for networks. In: Proceedings of the 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. San Jose, California, USA: ACM, 2007. 824−833

14 Yu W C, Cheng W, Aggarwal C C, Zhang K, Chen H F, Wang W. NetWalk: A flexible deep embedding approach for anomaly detection in dynamic networks. In: Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. London, UK: ACM, 2018. 2672−2681

15 Sanchez P I, Muller E, Laforet F, Keller F, Bohm K. Statistical selection of congruent subspaces for mining attributed graphs. In: Proceedings of the IEEE 13th International Conference on Data Mining (ICDM). Dallas, TX, USA: IEEE, 2013. 647−656

16 Oloulade B M, Gao J L, Chen J M, Lyu T F, Al-Sabri R. Graph neural architecture search: A survey. *Tsinghua Science and Technology*, 2022, **27**(4): 692−708

17 Fan S H, Wang X, Shi C, Kuang K, Liu N, Wang B. Debiased graph neural networks with agnostic label selection bias. *IEEE Transactions on Neural Networks and Learning Systems*, 2022

18 Hong X B, Zhang T, Cui Z, Yang J. Variational gridded graph convolution network for node classification. *IEEE/CAA Journal of Automatica Sinica*, 2021, **8**(10): 1697−1708

19 Velickovic P, Cucurull G, Casanova A, Romero A, Liò P, Bengio Y. Graph attention networks. In: Proceedings of the 6th International Conference on Learning Representations. Vancouver, BC, Canada: ICLR, 2017.

20 Hou M L, Wang L, Liu J Y, Kong X J, Xia F. A3Graph: Adversarial attributed autoencoder for graph representation learning. In: Proceedings of the 36th Annual ACM Symposium on Applied Computing. South Korea: ACM, 2021. 1697−1704

21 Wang J, Liang J Y, Yao K X, Liang J Q, Wang D H. Graph convolutional autoencoders with co-learning of graph structure and node attributes. *Pattern Recognition*, 2022, **121**: Article No. 108215

22 Abu-Salih B. Domain-specific knowledge graphs: A survey. *Journal of Network and Computer Applications*, 2021, **185**: Article No. 103076

23 Li Y S, Kong D Y, Zhang Y J, Tan Y H, Chen L. Robust deep alignment network with remote sensing knowledge graph for zero-shot and generalized zero-shot remote sensing image scene classification. *ISPRS Journal of Photogrammetry and Remote Sensing*, 2021, **179**: 145−158

24 Castellano G, Digeno V, Sansaro G, Vessio G. Leveraging knowledge graphs and deep learning for automatic art analysis. *Knowledge-Based Systems*, 2022, **248**: Article No. 108859

25 Rao Zi-Yun, Zhang Yi, Liu Jun-Tao, Cao Wan-Hua. Recommendation methods and systems using knowledge graph. *Acta Automatica Sinica*, 2021, **47**(9): 2061−2077
(饶子昀, 张毅, 刘俊涛, 曹万华. 应用知识图谱的推荐方法与系统. 自动化学报, 2021, **47**(9): 2061−2077)

26 Chen Y, Mensah S, Ma F, Wang H, Jiang Z A. Collaborative filtering grounded on knowledge graphs. *Pattern Recognition Letters*, 2021, **151**: 55−61

27 Du Y, Ranwez S, Sutton-Charani N, Ranwez V. Post-hoc recommendation explanations through an efficient exploitation of the DBpedia category hierarchy. *Knowledge-Based Systems*, 2022, **245**: Article No. 108560

28 Ji S X, Pan S R, Cambria E, Marttinen P, Yu P S. A survey on knowledge graphs: Representation, acquisition, and applications. *IEEE Transactions on Neural Networks and Learning Systems*, 2022, **33**(2): 494−514

29 Lin Y K, Liu Z Y, Sun M S, Liu Y, Zhu X. Learning entity and relation embeddings for knowledge graph completion. In: Proceedings of the 29th AAAI Conference on Artificial Intelligence. Austin, Texas, USA: AAAI, 2015. 2181−2187

30 Balazevic I, Allen C, Hospedales T M. TuckER: Tensor factorization for knowledge graph completion. In: Proceedings of the Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing. Hong Kong, China: Association for Computational Linguistics, 2019. 5184−5193

31 Shang C, Tang Y, Huang J, Bi J B, He X D, Zhou B W. End-to-end structure-aware convolutional networks for knowledge base completion. In: Proceedings of the 33rd AAAI Conference on Artificial Intelligence. Honolulu, Hawaii, USA: AAAI, 2019. 3060−3067

32 Ding K Z, Li J D, Liu H. Interactive anomaly detection on attributed networks. In: Proceedings of the 12th ACM International Conference on Web Search and Data Mining. Melbourne, Australia: ACM, 2019. 357−365

33 Song X Y, Wu M X, Jermaine C, Ranka S. Conditional anomaly detection. *IEEE Transactions on Knowledge & Data Engineering*, 2007, **19**(5): 631−645

34 Peng Z, Luo M N, Li J D, Xue L G, Zheng Q H. A deep multi-view framework for anomaly detection on attributed networks. *IEEE Transactions on Knowledge & Data Engineering*, 2022, **34**(6): 2539−2552

杜航原 山西大学计算机与信息技术学院副教授. 主要研究方向为数据挖掘和机器学习. 本文通信作者.
E-mail: duhangyuan@sxu.edu.cn
(**DU Hang-Yuan** Associate professor at the School of Computer and Information Technology, Shanxi University. His research interest covers data mining and machine learning. Corresponding author of this paper.)

曹振武 山西大学计算机与信息技术学院硕士研究生. 主要研究方向为数据挖掘和机器学习.
E-mail: caozhenwu_sxu@126.com
(**CAO Zhen-Wu** Master student at the School of Computer and Information Technology, Shanxi University. His research interest covers data mining and machine learning.)

王文剑 山西大学计算机与信息技术学院教授. 主要研究方向为机器学习, 数据挖掘和人工智能.
E-mail: wjwang@sxu.edu.cn
(**WANG Wen-Jian** Professor at the School of Computer and Information Technology, Shanxi University. Her research interest covers machine learning, data mining and artificial intelligence.)

白 亮 山西大学智能信息处理研究所教授. 主要研究方向为机器学习, 数据挖掘和数据科学与大数据计算.
E-mail: bailiang@sxu.edu.cn
(**BAI Liang** Professor at the Institute of Intelligent Information Processing, Shanxi University. His research interest covers machine learning, data mining, data science and big data computing.)