

# 属性网络中基于变分图自编码器的 异常节点检测方法

李 忠<sup>1,2</sup> 靳小龙<sup>1,2</sup> 王亚杰<sup>1,2</sup> 孟令宾<sup>1,2</sup> 庄传志<sup>1,2</sup> 孙 智<sup>1,2</sup>

**摘 要** 图神经网络为属性网络数据挖掘提供融合利用结构信息和属性信息的方法,但是在现阶段基于图自动编码器进行无监督属性网络异常节点检测时,常将正常节点子属性插值形成的节点误识别为异常节点,导致方法的假负率较高. 针对上述问题,文中提出基于变分图自编码器的异常节点检测方法. 模型包含两个编码器和一个解码器,利用一个编码器和一个解码器构成的变分自编码器模型,重建原始输入数据,再利用解码器和第二个编码器,使模型学习到不包含异常节点数据的网络隐层表达. 通过双变分自编码器学习正常节点子特征,并利用重建误差作为节点的异常度量,将由正常节点子特征构成的正常节点判别为正常节点. 在真实网络数据集上的实验表明,文中方法能有效进行属性网络异常节点检测.

**关键词** 异常节点检测, 属性网络, 变分自编码器, 重建误差, 无监督异常检测方法

**引用格式** 李 忠,靳小龙,王亚杰,孟令宾,庄传志,孙 智. 属性网络中基于变分图自编码器的异常节点检测方法. 模式识别与人工智能, 2022, 35(1): 17–25.

**DOI** 10.16451/j.cnki.issn1003-6059.202201002

**中图法分类号** TP 391

## Anomaly Node Detection Method Based on Variational Graph Auto-Encoders in Attribute Networks

LI Zhong<sup>1,2</sup>, JIN Xiaolong<sup>1,2</sup>, WANG Yajie<sup>1,2</sup>, MENG Lingbin<sup>1,2</sup>, ZHUANG Chuanzhi<sup>1,2</sup>, SUN Zhi<sup>1,2</sup>

**ABSTRACT** Graph neural network provides a method of combining structural information and attribute information for attribute network data mining. However, the current unsupervised attribute network anomaly node detection based on graph auto-encoder cannot capture the sub-features of normal nodes, and the false negative rate is high. Anomaly node detection method based on variational graph auto-encoders is proposed to detect abnormal nodes in attribute networks, containing two encoders and a decoder. A variational auto-encoder model consisting of an encoder and a decoder is designed to reconstruct the original input data. A decoder and the second encoder are utilized to learn the latent representation of the network without abnormal node data. The features of normal nodes are learned by the dual variational auto-encoder, and the reconstruction error is applied as the anomaly measure of nodes. Normal nodes composed of normal node features are identified as normal nodes by taking reconstruction error as the anomaly measurement of nodes. Experiments on real network datasets show that the proposed method is able to detect abnormal nodes in attribute networks effectively.

本文责任编辑 郝志峰

Recommended by Associate Editor HAO Zhifeng

1. 中国科学院 计算技术研究所 网络数据科学与技术重点实验室 北京 100190
2. 中国科学院大学 计算机与控制学院 北京 100049
1. Key Laboratory of Network Data Science and Technology, Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190
2. School of Computer and Control Engineering, University of Chinese Academy of Sciences, Beijing 100049

收稿日期:2021-09-09;录用日期:2021-12-17

Manuscript received September 9, 2021;

accepted December 17, 2021

国家重点研发计划项目(No. 2016QY02D0404)、国家自然科学基金项目(No. U1911401,61772501,U1836206,91646120)资助

Supported by National Key Research and Development Program of China(No. 2016QY02D0404), National Natural Science Foundation of China(No. U1911401,61772501,U1836206,91646120)

**Key Words** Anomaly Node Detection, Attribute Network, Variational Auto-encoder, Reconstruction Error, Unsupervised Anomaly Detection Method

**Citation** LI Z, JIN X L, WANG Y J, MENG L B, ZHUANG C Z, SUN Z. Anomaly Node Detection Method Based on Variational Graph Auto-Encoders in Attribute Networks. Pattern Recognition and Artificial Intelligence, 2021, 35(1): 17–25.

在大数据时代背景下,属性网络的结构复杂度与属性信息维度都具有相当大的规模,如何充分利用网络的结构信息和网络节点的属性信息进行网络数据挖掘获得学者们越来越多的注意力<sup>[1]</sup>. 属性网络中异常节点检测任务的目标是从属性网络中查找统计数据或分布规律和大多数正常节点不同的节点<sup>[2]</sup>,因此属性网络异常检测在网络分析与数据挖掘领域也受到学者们的关注<sup>[3]</sup>. 在现实的属性网络中,根据具体应用场景的不同,异常个体节点主要分为3类:结构异常<sup>[4-6]</sup>、属性上下文异常<sup>[7-9]</sup>、混合结构和属性信息异常.

近年来,图神经网络由于能结合网络结构信息和节点特征信息进行隐层特征学习,在很多图数据挖掘任务中表现出较优性能<sup>[10]</sup>. 但在实际的属性网络异常检测场景中,通常绝大多数样本是正常样本,异常样本数量占比极少,并在很多场景中,缺少真正可信的异常标注数据,因此有监督的属性网络异常检测算法普适性较差. 由于异常的原因和类型多种多样,而正常节点的结构和属性特征具有一定的规律,因此,可利用无监督方法学习正常节点的特征规律,结合重建误差以识别网络中的异常节点.

按照网络的节点是否包含属性信息,可将网络异常检测分为无属性网络异常节点检测和属性网络异常节点检测.

无属性网络异常节点检测方法包括:1) 基于节点结构的方法,如权重图异常检测 (Spotting Anomalies in Weighted Graphs)<sup>[11]</sup>. 2) 基于社团的异常检测,使用群体检测方法<sup>[12-14]</sup>查找异常节点,此类算法可解释性较强,但效果依赖于不同的群体检测方法,只能检测固定类型的异常节点. 3) 基于图谱分析技术异常检测方法,如 EigenSpokes (Surprising Patterns and Scalable Community Chipping in Large Graphs)<sup>[15]</sup>, FRAUDAR (Bounding Graph Fraud in the Face of Camouflage)<sup>[16]</sup>, M-Zoom (Fast Dense-Block Detection in Tensors with Quality Guarantees)<sup>[17]</sup>, D-Cube (Dense-Block Detection in Terabyte-Scale Tensors)<sup>[18]</sup>, 此类算法计算效率较高,可扩展性较强,但检测结果存在较高偏差,异常数据中存在较多的正常数据. 由于网络表示学习技术可将高维度的网络

映射到一个低维的网络中,使用网络表示学习技术进行个体节点嵌入及群体嵌入,并结合分类技术,可查找影响结构稳定的异常节点<sup>[19-20]</sup>. 无属性网络异常节点检测方法通常只能利用网络的结构信息,无法利用网络节点属性信息,也无法利用网络隐层特征进行异常检测.

属性网络融合网络结构和节点属性信息,属性的多样性及结构与属性融合也给属性网络异常节点检测带来极大挑战. 传统的属性网络异常检测方法主要依赖特征选择方法,如基于属性相似度云模型的网络异常检测方法<sup>[21]</sup>.

为了充分利用网络结构和属性信息,研究者利用残差矩阵进行检测. Li 等<sup>[22]</sup>提出 RADAR (Residual Analysis for Anomaly Detection in Attributed Networks),利用网络和属性信息结合的残差矩阵进行异常检测. Peng 等<sup>[23]</sup>提出 ANOMALOUS (Joint Modeling Approach for Anomaly Detection on Attributed Networks),利用重建和残差矩阵分析进行异常检测.

随着卷积神经网络 (Convolutional Neural Network, CNN) 在计算机视觉方面的成功应用,学者们考虑将 CNN 应用于网络数据挖掘. 为了克服网络数据结构稀疏及网络结构为不规则的非欧氏空间的问题<sup>[10]</sup>,利用图卷积网络 (Graph Convolution Network, GCN) 进行节点分类检测异常的方法是有监督的机器学习方法,而异常节点检测通常没有可信标注数据,因此多使用无监督或半监督的方法. Ding 等<sup>[24]</sup>提出 DOMINANT (Deep Anomaly Detection on Attributed Networks),对原始训练数据依赖性较高,检测结果存在较大偏差.

针对极少数现实世界中可以以较小的成本获得异常标注数据的异常检测问题, Pang 等<sup>[25]</sup>提出弱监督异常检测算法,在建模期间还可使用有限数量的标记异常数据,使用标记的小规模异常数据进行学习,有助于识别感兴趣的异常并解决无监督异常检测中高误报率问题.

针对使用图训练机制学习目标发现异常但无法扩展,且无法连接到大型网络的问题, Liu 等<sup>[26]</sup>提出 CoLA (Contrastive Self-Supervised Learning Framework

for Anomaly Detection on Attributed Networks), 可用于大型网络, 但算法结果对于节点对的选择具有一定的依赖性.

因此, 本文提出基于图变分自编码器的异常节点检测方法 (Anomaly Node Detection Method Based on Variational Graph Auto-Encoders, VGAE), 通过重建误差判断节点是否为异常节点. 模型包含两个编码器和一个解码器, 利用一个编码器和一个解码器构成的变分自编码器模型重建原始输入数据, 再利用解码器和第二个编码器, 使模型学习到不包含异常节点数据的网络隐层表达. 通过双变分自编码器学习正常节点子特征, 并利用重建误差作为节点的异常度量, 将由正常节点子特征构成的正常节点判别为正常节点. 在真实网络数据集上的实验表明, 本文方法能有效进行属性网络异常节点检测. 本文方法源代码开源在 <https://github.com/lizhong2613/VGAE>.

## 1 问题定义

本文使用的标识符号和常用的网络定义符号相同, 具体如下.

**定义 1** 属性网络 定义一个属性网络  $\zeta = (V, \varepsilon, X)$  由, 其中,  $V = \{v_1, v_2, \dots, v_n\}$  表示网络中所有节点的集合, 网络中节点个数为  $n$ ,  $|V| = n$ .  $\varepsilon$  表示网络中所有节点连接边的集合, 其中  $|\varepsilon| = m$ .  $X$  为  $n \times d$  矩阵, 表示网络中所有节点属性组成的集合. 第  $i$  个节点的属性  $x_i \in \mathbf{R}^d, i = 1, 2, \dots, n$ . 连接矩阵  $A \in \mathbf{R}^{d \times d}$ , 表示网络节点和节点之间的连接关系, 如果节点  $i, j$  之间存在连接,  $A_{i,j} = 1$ , 否则  $A_{i,j} = 0$ . 对于一个有向连接网络, 连接矩阵  $A = \max(A, A^T)$ , 将有向网络转为无向网络进行处理.

**定义 2** 属性网络异常节点检测 给定一个属性网络  $\zeta = (V, \varepsilon, X)$ , 从该网络中检测一个异常节点集合  $O = \{o_1, o_2, \dots, o_k\}$ , 其中  $o_i, i = 1, 2, \dots, k$  的结构和属性分布规律和其它大多数节点不同.

## 2 基于变分图自编码器的异常节点检测方法

### 2.1 无监督的图神经网络异常节点检测

图神经网络类型开始主要为图卷积神经网络和图注意力网络, 后期其它神经网络迁移到图数据挖掘领域, 如图时空网络、图生成网络、图自编码器网

络. 图神经网络的本质是在图上对节点进行自动特征提取.

由于异常节点检测任务标注样本较少, 使得有监督的方法不适用于属性网络异常节点检测, 如利用图卷积神经网络和图注意力网络进行分类.

无监督的图神经网络异常节点检测可利用原始无标注样本数据, 学习属性网络的低维表达, 并利用重建数据与原始数据误差, 检测异常节点. 自编码器是由多个编码函数和解码函数构成的可无监督学习的神经网络, 并在自然语言处理、计算机视觉及语音识别等领域存在广泛应用<sup>[27]</sup>. 图自编码器网络是将自编码器迁移至图数据上<sup>[28]</sup>. 目前图自编码器网络及其变种广泛应用于图节点表示, 图自编码器一般包含两部分: 图自编码器和图解码器. 图编码器将原始的网络数据表示为一个隐层表达, 图解码器根据隐层还原图的原始数据. 根据采用降维的目标函数的不同, 可分为  $L2$  重建、拉普拉斯特征映射、递归重建、排序、生成对抗网络 (Generative Adversarial Networks, GAN) 等, 其中部分方法可应用于属性网络<sup>[29]</sup>.

变分图自编码器 (Variational Graph Auto-Encoders, VGAE) 的隐层表示不是通过一个函数获得, 而是先通过一个 GCN, 确定一个多维高斯分布, 再计算均值向量和协方差矩阵, 即通过采样得到隐层表示:

$$\mu = GCN_{\mu}(X, A), \log_2 \sigma = GCN_{\sigma}(X, A),$$

其中用到的 2 个卷积层权重矩阵是不同的.

区别于自编码器通过提取特征建立输入输出之间的映射, 应用 VGAE 的目标是让模型学习属性图的隐层特征, 通过训练数据, 可得到正常数据子特征的分布, 而通过学习训练数据的分布, 可生成与训练数据相似的数据, 生成数据与真实的正样本数据极为相似, 而异常数据会与生成数据存在较大不同, 因此, 可利用生成式模型进行异常检测. 生成式模型 GAN 是一种学习范式, 并不特定于某种模型架构, 并且由于其存在 2 个模型互相博弈的特点, 理论的近似极限也无法确定. 本文尝试将变分自编码器 (Variational Auto-Encoders, VAE) 应用于属性网络, 利用隐变量模型, 推断真实分布的近似值, 取得较优效果.

### 2.2 方法框架

Ding 等<sup>[24]</sup> 提出 DOMINANT, 依赖原始训练数据, 以整个属性图作为输入, 只能从一个原始的输入属性图  $G$  得到对应的重构属性图  $\hat{G}$ , 如果输入的属性图中包含一定量的异常数据, 那么重构的属



性图中也会包含该异常节点,从而将异常样例识别为正常样例.原有属性图中正常节点的特征构成的新节点,如果在重构图中不存在,也会将正常样例识别为异常样例.总之,使用自编码器作为主框架重构原始属性图,无法生成新的正常样本,因为自编码器必须有有效输入,才能构造隐藏向量.

本文提出基于变分图自编码器的异常节点检测方法(VGAEE),框架采用图变分自编码器,在编码过程中增加一些限制,使生成的隐含向量能粗略遵循一个标准正态分布.

具体地,在编码器中,增加计算均值的网络和计算方差的网络.在计算均值的网络上施加高斯噪声,使解码器对噪声具有鲁棒性,增加一个KL散度损失函数,目的是让均值为0,方差为1.对应计算方差的网络用于动态调节噪声的强度.在解码器初始训练阶段,重构误差远大于KL散度损失,适当降低噪声,使结果容易拟合.在训练后期,重构误差小于KL散

度损失,增加噪声,增加重构误差,使用解码器提升它的生成能力.

利用均值网络和误差网络,结合隐层向量概率分布,使生成的结果包含由正常子特征构成的新样本,避免由于输入网络中不存在而被自编码器为主的方法判断为异常情况.

在DOMINANT<sup>[24]</sup>中,如果原始输入网络包含异常数据,重构的属性网络也包含异常数据,从而导致无法进行异常检测的问题.针对上述问题,本文方法使用两层编码器结构,使生成器可学习正常样本编码隐层特征.由于生成器和编码器都是为正常样本优化而设计,异常样本无法最小化输入和生成样本之间的距离,通过两层编码器,可增加异常样本和正常样本之间的距离,提高异常检测效果.

VGAEE框图如图1所示.整个模型的框架按顺序主要包含3个子网络:一个自编码器、一个解码器、一个自编码器.

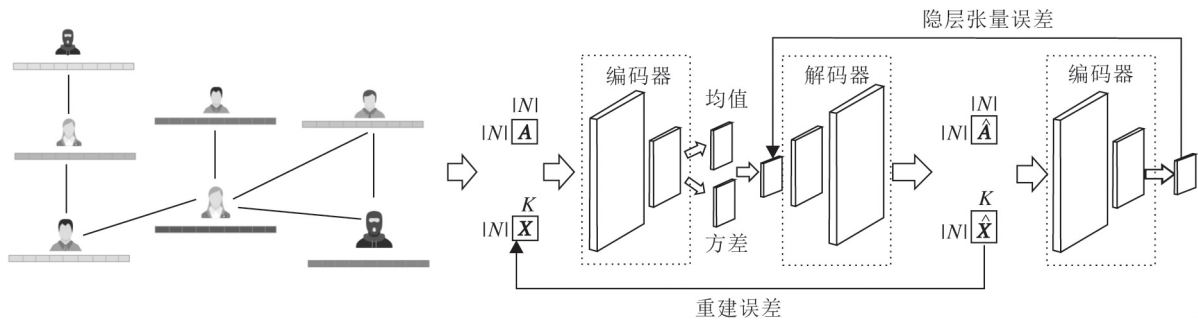


图1 本文方法框图

Fig.1 Sketch map of the proposed method

网络结构的自编码器和自解码器构成一个变分自动编码器结构,通过自编码器实现将输入的网络结构矩阵和网络属性矩阵进行降维,得到网络的隐层表示,并通过解码器重建.

具体流程为:对于一个属性网络,编码器首先读取网络的邻接矩阵  $A \in \mathbf{R}^{n \times k}$  和属性矩阵  $X \in \mathbf{R}^{n \times n}$ ,将数据前向传播至编码器网络  $G_E$ .  $G_E$  由两层 GCN 组成,采用批量标准化 (BatchNorm) 加速神经网络训练过程,使用线性整流函数 (Rectified Linear Unit, ReLU) 作为激活函数.通过  $G_E$  进行特征提取,将原始的输入数据压缩至一个隐层表示  $z \in \mathbf{R}^d$ ,其中  $d$  为  $z$  能保存网络特征的最小维度.然后隐层网络信息传输给解码器网络  $G_D$ ,解码器网络针对网络结构和网络属性分别进行重建.  $X$  采用两层卷积网络进行重建,使用 ReLU 作为激活函数.  $A$  采用一层卷积层进行解码,再采用内积操作进行重建.通过解

码器  $G_D$  重建得到的邻接矩阵和属性矩阵与原始数据的维度相同.该过程可表示为

$$(\hat{A}, \hat{X}) = G_D(z), z = G_E(A, X).$$

方法第2部分是一个编码器网络  $E$ ,使用不同的参数将重建得到的  $\hat{A}, \hat{X}$  再次压缩,网络结构和  $G_E$  相同,编码器网络  $E$  将  $\hat{A}, \hat{X}$  压缩至和  $z$  相同大小,得到  $\hat{z}$ ,通过参数化学习最小化隐层向量之间的表示.

VGAEE 中添加一个额外的自编码器,这是因为一个编码器和一个解码器可构成自编码器模型,模型目标是为了重建原始输入数据,而原始输入数据中包含异常数据.通过第一个解码器之后重建的网络数据是可能包含少量异常数据的结果数据集,再次使用编码器网络,得到的  $\hat{z}$  基本不包含异常数据.通过不断学习最小化隐层向量  $z$  和  $\hat{z}$  之间的表示,使网络的隐层向量  $z$  是正常数据的隐层表示,而不是

包含异常数据的隐层表示,从而更有效地检测异常数据。

### 2.3 目标函数

给定一个属性网络数据  $G$ , 包含异常个体节点数据, 尽管  $G_E$  尽量将所有的网络结构信息和网络属性信息包含在隐层表示  $z$  内, 但  $G_D$  无法通过  $z$  对异常节点进行重建。这是因为在训练和调参的过程中, VGAE 只能捕获正常数据, 并根据正常数据获取数据的高维特征, 而异常数据因为数据量较少, 且不具备正常子特征, 因此在降维过程中, 对应信息不包含在隐层  $z$  中。

在通过变分自编码器得到的还原  $\hat{A}, \hat{X}$  中, 不包含异常数据, 通过  $E$  将  $\hat{A}, \hat{X}$  映射到的潜在表示  $\hat{z}$  中不会包含异常节点的特征表示, 因此  $z$  和  $\hat{z}$  存在偏差。VGAE 目标如下: 通过不断训练使输出的  $\hat{A}, \hat{X}$  中只包含正常数据, 需要使  $\hat{A}, \hat{X}$  与  $A, X$  尽量接近,  $z$  与  $\hat{z}$  尽量接近。因此设置 2 种目标函数: 编码损失函数与重建损失函数。

重建损失函数和自编码器是相同的, 重建损失函数的目标是使通过解码器还原的数据和原始输入数据尽量接近。

通过重建损失函数, 本文方法能学习属性网络的上下文信息, 为了能尽量学习到正常的子特征, 忽略其它非重要及非正常的子特征, 重建损失函数采用  $L_1$  正则化范式计算原始数据与重建数据之间的重建误差:

$$L_{\text{rec}} = \alpha \|X - \hat{X}\|_1 + (1 - \alpha) \|A - \hat{A}\|_1,$$

其中  $\alpha$  表示属性矩阵重建误差和邻接矩阵重建误差之间的加权值。

$L_{\text{rec}}$  使解码器生成的数据尽量和原始数据接近, 可能会包含部分噪声数据。因此本文模型包含另外一个编码器  $E$ , 编码损失函数  $L_{\text{enc}}$  的目标是使通过编码器  $G_E$  得到的中间变量  $z$  和重建变量经过编码器  $E$  之后的隐层表示尽量接近。  $L_{\text{enc}}$  定义如下:

$$L_{\text{enc}} = \|G_E(A, X) - E(\hat{A}, \hat{X})\|_2,$$

其中,  $G_E(A, X)$  表示通过编码器得到的中间隐层变量  $z$ ,  $E(\hat{A}, \hat{X})$  表示通过第二部分编码器得到的隐层表示。编码器  $E$  表示生成的属性网络学习隐层编码特征。

整个方法的损失函数通过重建损失函数和编码损失函数加权求得:

$$L = \beta L_{\text{rec}} + (1 - \beta) L_{\text{enc}},$$

$\beta$  表示两部分的相对权重。

使用样本数据不断训练, 多次迭代, 通过梯度下降法不断优化权重矩阵, 变分自编码器使目标函数不断减小, 并最终收敛。利用最终的隐层进行数据重建, 对每个节点利用重建误差作为衡量节点异常的度量值。对网络中每个节点的异常度定义如下:

$$\text{score}(v_i) = \alpha (x_i - \hat{x}_i) + (1 - \alpha) (a_i - \hat{a}_i),$$

其中,  $x_i$  表示原始节点  $i$  的属性向量,  $\hat{x}_i$  表示重建节点的属性向量,  $a_i$  表示节点  $i$  的连接向量,  $\hat{a}_i$  表示重建  $i$  的连接向量。

节点的重建误差越大, 说明节点的异常度越高。因此可通过计算节点的异常重建误差, 按照节点的重建误差进行排序, 最后得到网络中异常节点的排序。按照给定的阈值, 最终得到满足阈值的前  $k$  个异常节点的集合  $O = \{o_1, o_2, \dots, o_k\}$ 。

## 3 实验及结果分析

### 3.1 实验数据集

本节选择使用较多的 BlogCatalog、ACM、Flickr 数据集进行对比实验。

1) BlogCatalog 数据集。从 BlogCatalog 社交博客网站上爬取的数据, 在该博客社交网络中, 用户可关注另外一位用户形成朋友关系, 每位用户都具有有一些描述标签, 该标签整理之后形成节点的属性信息。

2) ACM 数据集。ACM 学术文章发表的一个引文网络, 网络中的每个节点都是一篇文章, 节点和节点之间的引用形成一条连接边, 每个节点的属性信息为该文章的摘要信息和关键词信息。

3) Flickr 数据集。从 Flickr 网站爬取的社交网络数据。用户可在该网站上分享照片, 网络中每个节点对应一位用户, 节点的属性信息是用户的标签信息, 主要包括用户的兴趣爱好等。

以往的属性网络异常检测方法对上述三个数据集中插入一定数量的异常节点, 为了便于对比, 本文使用的数据集和以往的工作数据集相同, 3 个数据集的具体信息如表 1 所示。

表 1 实验数据集的详细情况

Table 1 Details of experimental datasets

名称	节点	连接边	属性维度	异常节点
BlogCatalog	5196	171743	8189	300
ACM	16484	71980	8337	600
Flickr	7575	239738	12047	450

### 3.2 对比方法

本文选择近年来具有代表性的属性网络异常检测方法作为基线方法进行对比。

1) LOF (Local Outlier Factor)<sup>[30]</sup>. LOF 基于距离的异常检测算法, 可直接对矩阵检测离群点. 对于属性网络, 可直接将属性矩阵应用 LOF, 或针对网络特征可结合节点属性矩阵直接进行拼接, 再应用 LOF. 本文采取第 1 种方法, 直接对属性矩阵采用 LOF.

2) SCAN (Structural Clustering Algorithm for Networks)<sup>[6]</sup>. 该方法利用网络结构信息进行网络社团发现, 并将不属于任何社团的孤立节点作为异常节点, 时间复杂度较低, 可扩展性较强. 本文直接利用 SCAN, 输入网络邻接矩阵计算异常节点.

3) RADAR<sup>[22]</sup>. 该方法利用网络属性信息和网络结构信息的残差矩阵, 查找属性网络孤立异常节点.

3) ANOMALOUS<sup>[23]</sup>. 该方法是利用降维和残差矩阵分析的属性网络异常检测方法.

4) DOMINANT<sup>[10]</sup>. 该方法是基于自编码器的属性网络异常检测方法, 利用 CNN 进行特征提取, 利用重建误差进行异常节点检测.

5) AMEN (Anomaly Mining of Entity Neighborhoods)<sup>[7]</sup>. 该方法是基于自我网络结构特征的异常检测方法, 统计属性网络中自我网络的属性分布规律, 判断节点是否为异常节点.

6) CoLA<sup>[26]</sup>. 该方法是基于自编码器的属性网络异常检测方法, 利用 CNN 进行特征提取, 利用重建误差进行异常节点检测.

7) DGI (Deep Graph Infomax)<sup>[31]</sup>. 该方法是使用非监督方式学习节点嵌入表示的方法, 通过最大化局部特征与全局特征的互信息, 将属性网络的两者相关性用于分类任务, 进行正常节点与异常节点的分类.

### 3.3 度量标准

异常检测问题可认为是从给定的样本中进行分类, 识别正负例, 本节使用分类问题中常用评价指标, 具体如下.

1) Recall@K. 在前面 Top K 个查询结果中, 正确结果数量与所有正确结果数量的比率, 也叫查全率.

2) ROC-AUC. 对于分类问题, 一般会设置一个阈值, 控制检索结果中正例和负例的不同权重. 阈值越低, 较多的样本会被识别为正例, 虽然提高识别率, 但更多的负例会被识别为正例. 根据不同的阈值设置, 横坐标由假正率, 纵坐标由真正率构成的分类

结果的曲线成为受试者工作特征 (Receiver Operating Characteristic, ROC) 曲线. ROC 曲线下的面积 (Area Under Curve, AUC) 越大, 算法效果越优.

3) 对于异常检测模型, 结果预测为正例或负例, 可使用二分类的评价指标说明模型的优劣. 常用的二分类评价指标有真阳性 (True Positive Rate, TPR)、真阴性 (True Negative Rate, FPR)、假阳性 (False Positive Rate, FPR)、假阴性 (False Negative Rate, FNR). TPR 为所有正例中被预测为正例的比率, 也叫召回率或查全率. FRP 为所有反例中被预测为正例的比率. TNR 为所有反例中被预测为反例的比率. FNR 为所有正例中被预测为反例的比率. TPR 越高, FRP 越低, 说明模型性能越优.

### 3.4 参数设置

由于自适应矩估计 (Adaptive Moment Estimation, Adam) 优化器可利用动量和自适应学习率, 替代梯度下降实现权重寻优, 因此在实验中使用 Adam 优化器加速神经网络收敛. 设置迭代次数为 200. 实验中设置学习率为 0.001, 隐层维度分别设置为 8, 16, 32, 64, 128, 256, 512, 1 024, 采用网格搜索交叉验证 (Grid Search Cross Validation, gridSearchCV), 确定最优参数.

在对比实验中, SCAN 的邻居阈值  $\varepsilon$  设置为 0.7, 邻居数量  $\mu$  设置为 1. Radar 中超参数  $\alpha = 0.1$ ,  $\beta = 0.01$ ,  $\gamma = 0.1$ , 在第 17 次迭代收敛, 因此设置迭代次数为 20. LOF 中设置邻居数量为 20. DOMINANT 中, 设置  $\alpha = 0.7$ , 迭代次数为 300, 图自编码器隐层的维度设置为 128.

### 3.5 实验结果

各方法在 3 个数据集上的 AUC 值对比如表 2 所示, 对于 CoLA<sup>[26]</sup> 与 DGI<sup>[33]</sup>, 由于未找到可复现的代码, 本文直接使用文献[26]中 AUC 指标进行对比.

表 2 各方法在 3 个数据集上的 AUC 值对比

Table 2 AUC value comparison of different methods on 3 datasets

方法	BlogCatalog	ACM	Flickr
CoLA	0.7854	0.8237	0.7513
DGI	0.5827	0.6240	0.6237
DOMINANT	0.7494	0.7813	0.7490
ANOMALYOUS	0.7038	0.7237	0.7434
AMEN	0.5626	0.6392	0.6573
SCAN	0.5010	0.3094	0.4539
RADAR	0.1912	0.1707	0.2480
LOF	0.3780	0.3221	0.4881
VGAE	0.8135	0.8967	0.8167



由表2可见,VGAEE的AUC值最高,LOF、RADAR、SCAN由于只能使用网络的结构或节点的属性信息,AUC值均低于0.5.

各方法在3个数据集上的Recall@K值对比如图2所示.

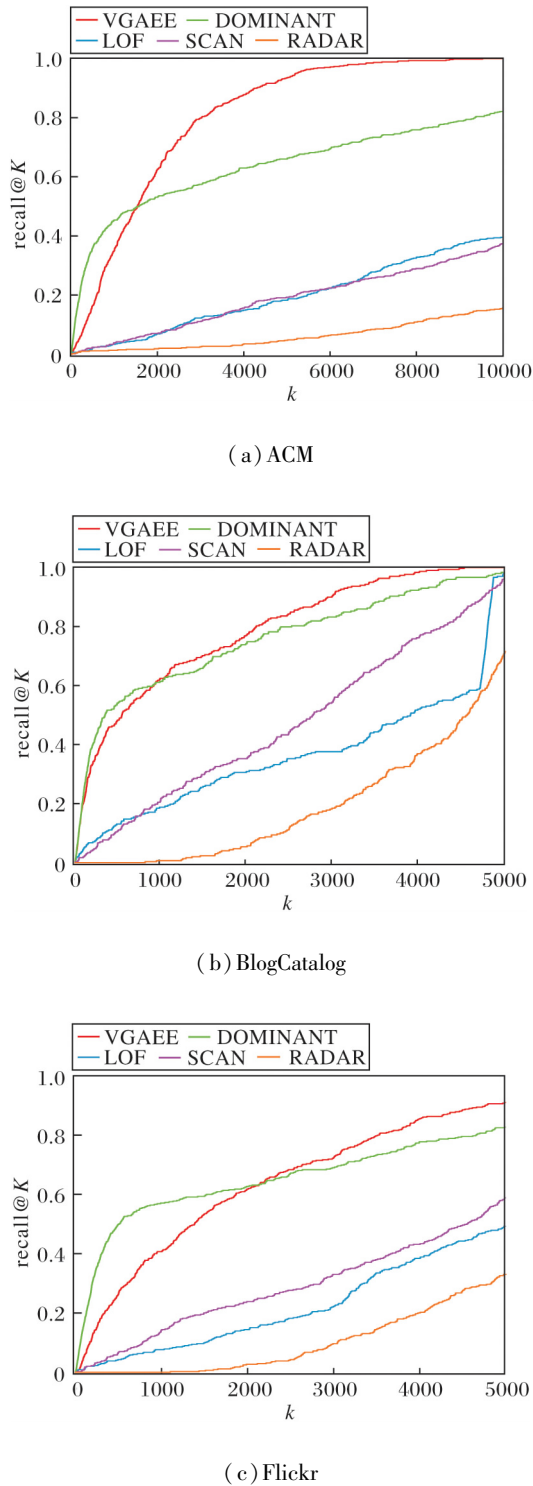


图2 各方法在3个数据集上的Recall@K值对比  
Fig.2 Recall@K value comparison of different methods on 3 datasets

由图2可看到,在3个数据集上,DOMINANT和VGAEE优于仅使用网络结构信息或仅使用节点属性的方法. DOMINANT能捕获异常程度较大的节点,之后性能下降,无法捕获异常节点的隐层子特征,存在偏差,会将正常节点判定为异常节点,召回率随着K的增大,无法识别更多的异常节点,而VGAEE的召回率迅速增加,识别更多的异常节点.

在ACM、BlogCatalog数据集上不同参数对实验结果的影响如图3所示.

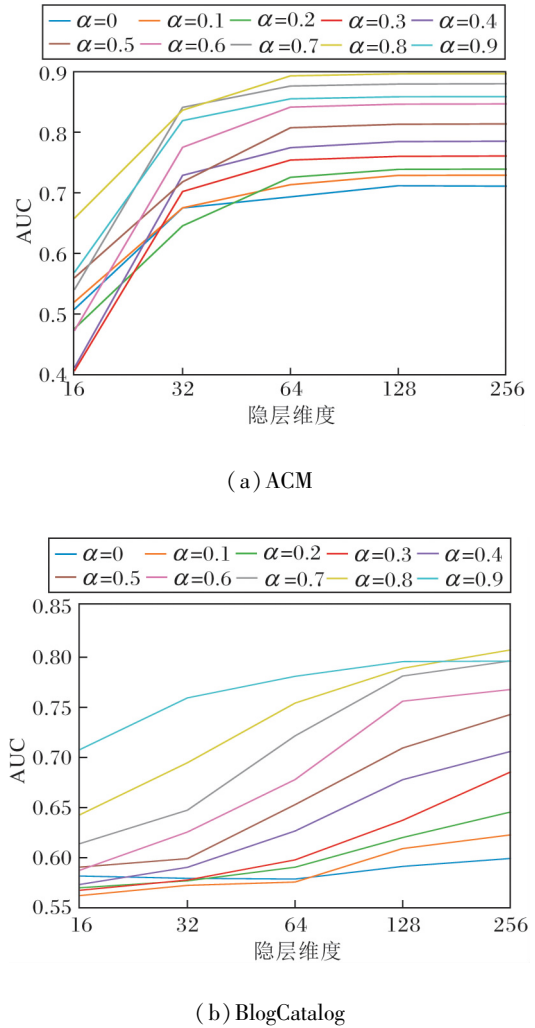


图3  $\alpha$  对 AUC 值的影响  
Fig.3 Influence of different  $\alpha$  on AUC values

由图3(a)可看出,当仅采用网络结构信息( $\alpha=1.0$ )时,AUC值最低,说明仅采用单一因素进行异常检测效果不理想,而当 $\alpha=0.8$ 时AUC值最优,说明结构信息和节点的属性信息在异常检测上权重不同,节点的属性信息占比更大.在ACM数据集上,随着隐层维度的增大,检测结果更优,而在隐层维度达到128维之后,AUC值基本达到最优,在维度达

到 256 时,无更好提升.

由图 3(b)可知,在 BlogCatalog 数据集上, $\alpha=0.9$  时 AUC 值最优,隐层维度在 256 时达到最优.该结果说明不同数据集上,节点的属性信息对于异常检测比网络结构更重要,但不同的数据集节点属性对异常节点检测的重要性不同,并且网络隐层维度在达到 128 或 256 时能更好地提取网络的深层特征.

## 4 结 束 语

本文提出基于变分图自编码器的异常节点检测方法,可充分利用网络结构信息和节点属性信息进行异常节点检测.利用变分自编码器获取正常节点深度子特征,并识别由正常子特征构成的节点为正常节点,减少预测误差,提升系统的召回率.通过两层编码器,充分学习属性网络隐层特征,并利用重建误差进行属性网络异常检测.实验表明,本文方法优于仅利用网络结构信息或属性信息进行异常检测的方法,并且优于使用自编码器的网络模型,能有效地从属性网络中检测出异常节点.今后可考虑使用变分自编码器的改进算法,如基于流模型的算法,以提高检测效果,也可在大规模网络上预训练模型并迁移至其它网络上进行异常检测,降低时间成本,提高检测效率.异常检测的可解释性也是今后的一个研究方向.

## 参 考 文 献

- [1] AKOGLU L, TONG H H, KOUTRA D. Graph Based Anomaly Detection and Description: A Survey. *Data Mining and Knowledge Discovery*, 2015, 29(3): 626–688.
- [2] DING K Z, LI J D, LIU H. Interactive Anomaly Detection on Attributed Networks // *Proc of the 20th ACM International Conference on Web Search and Data Mining*. New York, USA: ACM, 2019: 357–365.
- [3] CAO S S, LU W, XU Q K. Deep Neural Networks for Learning Graph Representations // *Proc of the 30th AAAI Conference on Artificial Intelligence*. Palo Alto, USA: AAAI, 2016: 1145–1152.
- [4] GAO J, LIANG F, FAN W, *et al.* On Community Outliers and Their Efficient Detection in Information Networks // *Proc of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. New York, USA: ACM, 2010: 813–822.
- [5] PEROZZI B, AKOGLU L, SÁNCHEZ P I, *et al.* Focused Clustering and Outlier Detection in Large Attributed Graphs // *Proc of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. New York, USA: ACM, 2014: 1346–1355.
- [6] XU X W, YURUK N, FENG Z D, *et al.* SCAN: A Structural Clustering Algorithm for Networks // *Proc of the 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. New York, USA: ACM, 2007: 824–833.
- [7] PEROZZI B, AKOGLU L. Scalable Anomaly Ranking of Attributed Neighborhoods // *Proc of the 16th SIAM International Conference on Data Mining*. Philadelphia, USA: SIAM, 2016: 207–215.
- [8] LUO M N, NIE F P, CHANG X J, *et al.* Adaptive Unsupervised Feature Selection with Structure Regularization. *IEEE Transactions on Neural Networks and Learning Systems*, 2018, 29(4): 944–956.
- [9] ZHAO X, WU Y H, LEE D L, *et al.* iForest: Interpreting Random Forests via Visual Analytics. *IEEE Transactions on Visualization and Computer Graphics*, 2019, 25(1): 407–416.
- [10] KIPF T N, WELING M. Semi-supervised Classification with Graph Convolutional Networks[C/OL]. [2021–08–20]. <https://arxiv.org/pdf/1609.02907.pdf>.
- [11] AKOGLU L, MCGLOHON M, FALOUTSOS C. Oddball: Spotting Anomalies in Weighted Graphs // *Proc of the Pacific-Asia Conference on Knowledge Discovery and Data Mining*. Berlin, Germany: Springer, 2010: 410–421.
- [12] ROSSI R A, GALLAGHER B, NEVILLE J, *et al.* Modeling Dynamic Behavior in Large Evolving Graphs // *Proc of the 6th ACM International Conference on Web Search and Data Mining*. New York, USA: ACM, 2013: 667–676.
- [13] TONG H H, LIN C Y. Non-negative Residual Matrix Factorization with Application to Graph Anomaly Detection // *Proc of the 11th SIAM International Conference on Data Mining*. Philadelphia, USA: SIAM, 2011: 143–153.
- [14] HENDERSON K, GALLAGHER B, ELIASSI-RAD T, *et al.* Rol-X: Structural Role Extraction & Mining in Large Graphs // *Proc of the 18th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. New York, USA: ACM, 2012: 1231–1239.
- [15] PRAKASH B A, SRIDHARAN A, SESHADRI M, *et al.* EigenSpokes: Surprising Patterns and Scalable Community Chipping in Large Graphs // *Proc of the Pacific-Asia Conference on Knowledge Discovery and Data Mining*. Berlin, Germany: Springer, 2010: 435–448.
- [16] HOOI B, SONG H A, BEUTEL A, *et al.* FRAUDAR: Bounding Graph Fraud in the Face of Camouflage // *Proc of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. New York, USA: ACM, 2016: 895–904.
- [17] SHIN K, HOOI B, FALOUTSOS C. M-Zoom: Fast Dense-Block Detection in Tensors with Quality Guarantees // *Proc of the Joint European Conference on Machine Learning and Knowledge Discovery in Databases*. Berlin, Germany: Springer, 2016: 264–280.
- [18] SHIN K, HOOI B, KIM J, *et al.* D-Cube: Dense-Block Detection in Terabyte-Scale Tensors // *Proc of the 10th ACM International*



- Conference on Web Search and Data Mining. New York, USA; ACM, 2017: 681–689.
- [19] HU R J, AGGARWAL C C, MA S, *et al.* An Embedding Approach to Anomaly Detection // Proc of the 32nd IEEE International Conference on Data Engineering. Washington, USA; IEEE, 2016: 385–396.
- [20] YU W C, CHENG W, AGGARWAL C C, *et al.* NetWalk: A Flexible Deep Embedding Approach for Anomaly Detection in Dynamic Networks // Proc of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York, USA; ACM, 2018: 2672–2681.
- [21] 张君, 张国英, 刘玉树. 基于属性相似度云模型的网络异常检测. 吉林大学学报(工学版), 2006, 36(6): 954–957. (ZHANG J, ZHANG G Y, LIU Y S. Network Anomaly Detection Based on Attributes Similarity and Cloud Model. Journal of Jilin University(Engineering and Technology Edition), 2006, 36(6): 954–957.)
- [22] LI J D, DANI H, HU X, *et al.* RADAR: Residual Analysis for Anomaly Detection in Attributed Networks // Proc of the 26th International Joint Conference on Artificial Intelligence. New York, USA; ACM, 2017: 2152–2158.
- [23] PENG Z, LUO M N, LI J D, *et al.* ANOMALOUS: A Joint Modeling Approach for Anomaly Detection on Attributed Networks // Proc of the 27th International Joint Conference on Artificial Intelligence. New York, USA; ACM, 2018: 3513–3519.
- [24] DING K, LI J D, BHANUSHALI R, *et al.* Deep Anomaly Detection on Attributed Networks // Proc of the 19th SIAM International Conference on Data Mining. Philadelphia, USA; SIAM, 2019: 594–602.
- [25] PANG G S, SHEN C H D, JIN H, *et al.* Deep Weakly Supervised Anomaly Detection [C/OL]. [2021–08–20]. <https://arxiv.org/pdf/1910.13601.pdf>.
- [26] LIU Y X, LI Z, PAN S R, *et al.* Anomaly Detection on Attributed Networks via Contrastive Self-Supervised Learning. IEEE Transactions on Neural Networks and Learning Systems, 2021. DOI: 10.1109/TNNLS.2021.3068344.
- [27] AKCAY S, ATAPOUR-ABARGHOUEI A, BRECKON T P. GANomaly: Semi-supervised Anomaly Detection via Adversarial Training // Proc of the Asian Conference on Computer Vision. Berlin, Germany: Springer, 2018: 622–637.
- [28] 李忠, 靳小龙, 庄传志, 等. 面向图的异常检测研究综述. 软件学报, 2021, 32(1): 167–193. (LI Z, JIN X L, ZHUANG C Z, *et al.* Overview on Graph Based Anomaly Detection. Journal of Software, 2021, 32(1): 167–193.)
- [29] LI Z, JIN X L, ZHUANG C Z, *et al.* Content-Aware Anomaly Detection with Network Representation Learning // Proc of the International Conference on Algorithms and Architectures for Parallel Processing. Berlin, Germany: Springer, 2020: 50–64.
- [30] BREUNIG M M, KRIEGEL H P, NG R T, *et al.* LOF: Identifying Density-Based Local Outliers. ACM SIGMOD Record, 2000, 29(2): 93–104.
- [31] VELIČKOVIĆ P, FEDUS W, HAMILTON W L, *et al.* Deep Graph Infomax [C/OL]. [2021–08–20]. <http://export.arxiv.org/pdf/1809.10341>.

## 作者简介



李忠(通信作者), 博士研究生, 主要研究方向为网络异常检测. E-mail: lizhong17b@ict.ac.cn.

(LI Zhong (Corresponding author), Ph. D. candidate. His research interests include network anomaly detection.)



靳小龙, 博士, 研究员, 主要研究方向为知识图谱、社交网络计算. E-mail: jinxiaolong@ict.ac.cn.

(JIN Xiaolong, Ph. D., professor. His research interests include knowledge graph and social network computing.)



王亚杰, 博士研究生, 主要研究方向为信息抽取. E-mail: wangyajie18b@ict.ac.cn.

(WANG Yajie, Ph. D. candidate. His research interests include information extraction.)



孟令宾, 博士研究生, 主要研究方向为知识图谱. E-mail: menglingbin19b@ict.ac.cn.

(MEMG Lingbin, Ph. D. candidate. His research interests include knowledge graph.)



庄传志, 博士研究生, 主要研究方向为关系抽取、自然语言处理. E-mail: zhuangcz@ict.ac.cn.

(ZHUANG Chuanzhi, Ph. D. candidate. His research interests include relation extraction and natural language processing.)



孙智, 博士研究生, 主要研究方向为知识图谱、异常检测. E-mail: Sunzhi17b@ict.ac.cn.

(SUN Zhi, Ph. D. candidate. His research interests include knowledge graph and anomaly detection.)