软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2021,32(1):167−193 [doi: 10.13328/j.cnki.jos.006100]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

面向图的异常检测研究综述*

李 忠[1,2], 靳小龙[1,2], 庄传志[1,2], 孙 智[1,2]

[1](网络数据科学与技术重点实验室(中国科学院 计算技术研究所),北京 100190)

[2](中国科学院大学 计算机与控制学院,北京 100049)

通讯作者: 靳小龙, E-mail: jinxiaolong@ict.ac.cn

摘 要: 近年来,随着Web 2.0的普及,使用图挖掘技术进行异常检测受到人们越来越多的关注.图异常检测在欺诈检测、入侵检测、虚假投票、僵尸粉丝分析等领域发挥着重要作用.在广泛调研国内外大量文献以及最新科研成果的基础上,按照数据表示形式将面向图的异常检测划分成静态图上的异常检测与动态图上的异常检测两大类,进一步按照异常类型将静态图上的异常分为孤立个体异常和群组异常检测两种类别,动态图上的异常分为孤立个体异常、群体异常以及事件异常这 3 种类型.对每一类异常检测方法当前的研究进展加以介绍,对每种异常检测算法的基本思想、优缺点进行分析、对比,总结面向图的异常检测的关键技术、常用框架、应用领域、常用数据集以及性能评估方法,并对未来可能的发展趋势进行展望.

关键词: 图异常检测;图数据挖掘;数据挖掘

中图法分类号: TP393

中文引用格式: 李忠,靳小龙,庄传志,孙智.面向图的异常检测研究综述.软件学报,2021,32(1):167−193. http://www.jos.org.cn/1000-9825/6100.htm

英文引用格式: Li Z, Jin XL, Zhuang CZ, Sun Z. Overview on graph based anomaly detection. Ruan Jian Xue Bao/Journal of Software, 2021,32(1):167−193 (in Chinese). http://www.jos.org.cn/1000-9825/6100.htm

Overview on Graph Based Anomaly Detection

LI Zhong[1,2], JIN Xiao-Long[1,2], ZHUANG Chuan-Zhi[1,2], SUN Zhi[1,2]

[1](Key Laboratory of Network Data Science and Technology (Institute of Computing Technology, Chinese Academy of Sciences), Beijing 100190, China)

[2](School of Computer and Control Engineering, University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: In recent years, with the popularization of Web 2.0, people pay more and more attentions to the graph anomaly detection. The graph anomaly detection plays an increasingly vital role in the field of fraud detection, intrusion detection, false voting, and zombie fan analysis. This paper presents a survey on existing approaches to address this problem and reviews the recent developed techniques to detect graph anomalies. The graph-oriented anomaly detection is divided into two types, the anomaly detection on static graph and the anomaly detection on dynamic graph. Existing work on static graph anomaly detection have identified two types of anomalies: One is individual anomaly that refers to the abnormal behaviors of individual entity, the other is group anomaly that occurs due to unusual patterns of groups. The anomaly on dynamic graph can be divided into three types: Isolated individual anomaly, group anomaly, and event anomaly. This paper introduces the current research progress of each kind of anomaly detection methods, and summarizes the key technologies, common frameworks, application fields, common data sets, and performance evaluation methods of graph-oriented anomaly detection. Finally, future research directions on graph anomaly detection are discussed.

Key words: graph anomaly detection; graph data mining; data mining

* 基金项目: 国家重点研发计划(2016QY02D0404); 国家自然科学基金(U1911401, 61772501, U1836206, 91646120)

Foundation item: National Key Research and Development Program of China (2016QY02D0404); National Natural Science Foundation of China (U1911401, 61772501, U1836206, 91646120)

收稿时间: 2019-07-01; 修改时间: 2019-11-30, 2020-04-11; 采用时间: 2020-06-16; jos 在线出版时间: 2020-07-27

1 研究背景

在互联网、物联网以及通信技术不断发展的大背景下,信息的交互、分析、协同变得越来越普遍.生活中的网络更随处可见,如电话通联网络、交通运输网络、电力网络等等.尤其随着社交网络的产生,人们有了更好的交流与协作平台,如微博、微信、QQ 等等.当人们享受网络带来的便捷性的同时,网络中的异常与欺诈行为也影响了社交网络的正常发展,如欺诈信息的传播、电信与信用卡欺诈、网络僵尸粉丝、购物网站恶意评价、网络扫描与网络入侵等.如何能够尽早并准确地检测到这些异常与欺诈行为,避免造成更多的危害变得尤为重要.区别于传统数据挖掘技术的面向图的异常检测技术,因其普适性和高效性,也受到学术界和工业界的广泛关注.

1.1 面向图的异常检测的定义

Hawkins 定义异常检测[1]就是发现那些和大部分对象不同的目标对象,以至于这些对象的分布或形成机制看起来与其他数据是不同的.面向图的异常检测是将原始问题使用图数据结构进行建模,并使用图数据挖掘技术和图论的相关理论知识,从图中找出分布、形成规律和大多数其他的实体不同的节点或者边.

1.1.1 传统的异常检测方法

传统的异常检测是数据挖掘中的一个重要应用,用来发现数据集中不同于其他数据的对象.离群点检测是异常检测的一种常用方法,传统的离群点检测的一般过程为:首先,根据已有的正常数据建立一个参考模型,对于新的观测数据,测试数据相似度是否在某个阈值之内,以此来判断数据是否是异常数据.传统的异常检测的方法也非常多,可以大致分为 4 类——基于统计的方法、基于距离的方法、基于偏差的方法、基于密度的方法.

(1) 基于统计的方法:假设数据分布符合一定的概率分布,如果数据和分布有差距,则认为是异常数据.但是现实数据有可能不符合任何一种理想的概率分布,或者符合的分布模式是未知的;
(2) 基于距离的方法:原理是正常的数据应该有足够多的邻居,异常数据则有很少的邻居;
(3) 基于偏差的方法:使用模型对数据进行预测,若预测值与实际值偏差超过一定的阈值则为异常数据;
(4) 基于密度的方法:基于距离的异常方法的改进,利用网格作 *K*NN 查询,可以查找局部异常因子.

1.1.2 面向图的异常检测方法

使用图数据表示网络具有得天独厚的优势.网络存在于我们生活的方方面面,图数据表示能力强,可以表示实体与实体之间的复杂关系.使用图模型表示网络数据,可使用图论的相关技术挖掘数据中有价值的信息.常用的图数据挖掘技术主要包括图聚类、图分类、图切割等.图异常检测技术是图数据挖掘技术的一种,如在社交网络中,将每个人作为一个点,人与人之间的互动关系是边,则在庞大的社交圈子中,不同人之间的互动联系就构成了庞大的社交关系图.在社交网络中,使用图异常检测技术可以识别网络中的异常账号、僵尸粉丝、广告推手等等.在计算机网络访问图中,使用图数据挖掘技术可以找出潜在的攻击者或入侵者.面向图异常检测可定义为:给定一个无权或有权的、静态的或动态的图数据模型,查找其中与大多数观测对象不一样的少量的边、节点或子图.

面向图异常检测不仅仅需要考虑对象与对象之间的相似度,还需要考虑对象与对象之间的关系信息.比如:通过交易网络图分析哪些交易是欺诈交易、通过通信网络数据图分析恐怖分子之间的联系网络、通过用户-商品网络数据分析水军或恶意评价之间的关系、通过关注者-被关注者网络分析网络僵尸粉丝的攻击方向等.

传统的图异常检测技术是异常检测技术和离群点检测技术在图数据挖掘中的应用,主要包括基于信息论的方法、基于偏差的方法、基于距离的方法以及基于社区的方法.近年来,神经网络是人工智能领域兴起的研究热点,随着研究工作的不断深入,神经网络在许多领域都取得了很大的进展,尤其是在模式识别、智能机器人、预测估计、自然语言处理等领域已成功地解决了许多现代计算机难以解决的实际问题,并表现出了良好的智能特性.随着神经网络的发展,近年来也有一些使用深度神经网络进行图异常检测的方法[2],主要分成两类.

(1) 基于有监督学习的方法,通过使用标签数据训练就可以得到非线性分类器,将异常检测问题作为分类问题来处理;
(2) 基于偏差的方法,通过使用编码器-解码器模型对数据进行重建,重建的误差超过阈值则认为是异常

数据.该方法通常适用于时间序列图.

本文在总结传统图异常检测技术的基础上,介绍了近年来采用神经网络以及张量分解等技术的图异常检测算法,最后对各类方法进行分析对比,说明其优缺点.

1.2 面向图的异常检测的分类

本文按照输入图的类型分为静态图异常检测与动态图异常检测两大类.给定一个问题,从是否将问题建模为动态图的角度出发,便于形成对问题的清晰的解决思路.此外,面向静态图的异常检测方法改进之后也可以应用于动态图的异常检测.因此,本文从静态图的异常检测到动态图的异常检测,形成递进逻辑,也便于读者理解相关模型与方法的优缺点.

- 面向静态图的异常检测

根据静态图是否包含属性,静态图异常检测可以分为两类——无权静态图异常检测以及有权静态图异常检测.

(1) 无权静态图异常检测:给定一个静态同质图,充分利用图的结构信息查找模式并识别异常节点.该类方法可以根据使用的模式进一步分为基于结构的模式和基于群体的模式这两类;

(2) 加权静态图异常检测:静态图的节点或者边具有属性,利用结构信息以及节点和边的属性信息进行异常检测.如社交网络中用户的兴趣、金融交易网络中的交易数量以及交易类型等等.

- 面向动态图的异常检测

给定一个无权图的序列或者加权图的序列,从中查找:(1) 对应一个事件或者改变对应的图;(2) 导致该改变或者事件的前 k 个节点/边/子图.

1.3 相关综述工作

近年来,由于社会各界对异常检测的关注,面向图的异常检测取得了很大的进展,有不少面向图异常检测的综述性文章陆续发表.Akoglu 等人[3]对面向图异常检测进行了综述,给出了异常检测分类的基础框架,将所有的算法分成了基于分类、统计、聚类以及信息论这 4 种类型,并对每种方法进行对比,给出面向图的异常检测在各个领域的应用.Gogoi 等人[4]按照使用技术,从基于距离的异常检测、基于密度的异常检测以及其他技术异常检测这 3 个方面进行综述,并将各种方法进行对比.Gupta 等人[5]针对时序数据的异常检测工作进行了总结和归纳,其中,时序数据包括空间时序数据、分布数据流、时序网络等.Ranshous 等人[6]将面向动态图异常检测分成了基于群体检测方法、基于 MDL 的方法、基于距离的方法、基于降维的方法、基于概率分布的方法等几类,并将每种类型方法中的主要算法进行对比.Yu 等人[7]关注于社交网络的异常检测,并从点异常和群体异常两个方面对社交网络异常检测研究进展进行概括和展望.

尽管已有上述众多的面向网络的异常检测综述,但大多都基于某一具体应用领域,目前仍然缺少对图异常检测研究进展进行系统、全面、深入地梳理和总结的工作.以往的工作或基于图的异常检测的具体某一应用进行归纳分析(如 Yu 等人[7]和 Zhang 等人[8]聚焦于社交网络中异常的账号检测以及异常群体检测,Mao 等人[9]关注于空间轨迹异常检测,Mo 等人[10]关注于网络水军检测),或只总结了传统的异常检测方法而没有涉及利用机器学习或者神经网络技术(如 Gogoi 等人[4]和 Gupta 等人[5]的工作).为此,本文对面向图的异常检测领域的传统方法以及最新的研究进展进行系统的归纳和分类总结,并展望未来的发展趋势.

本文首先按照输入图的类型将现有工作分为面向静态图的异常检测与面向动态图的异常检测两大类.在两类异常检测中,首先总结传统的、经典的方法,然后总结近年来利用机器学习技术与神经网络技术的一些方法.在第 4 节中,总结面向图异常检测的关键技术、常用框架、领域应用、实验数据以及评估方法.最后探讨该领域的所有方法的优缺点、当前图异常检测的挑战以及未来发展趋势.

2 面向静态图的异常检测

静态图的异常检测面对的图是静态的,也可以是变化网络在某一个时刻的快照,并根据整个图的结构信息

和节点信息,从中查找异常的实体,如节点、边、子图.

根据能够检测异常的实体之间的关系是否是相互独立的,静态图异常检测可以分为孤立个体异常检测和群体异常检测.

2.1 孤立个体异常检测

定义. 给定一个网络数据,从中查找异常的实体,若异常的实体和实体之间是相互独立的,则为孤立个体异常检测.

面向孤立个体的网络异常检测可以分为基于结构的方法、基于社团的方法、基于信息论的方法、基于降维的方法、基于子图的异常检测和基于神经网络的方法等.

2.1.1 基于结构的方法

基于结构的方法分为两类:基于结构特征的方法和基于结构相似度的方法:第 1 种方法是总结已有正常网络的特征,如节点出入度的分布规律或者子图中心度的规律等;第 2 种方法是通过图的结构计算节点临近度,并以此判断节点的异常性.

网络的特征可以按照特征粒度分为节点的特征和图的特征两部分.

- 节点的特征主要包括节点的出度、入度、中介中心度(betweenness centrality)、特征向量中心性(eigenvector centrality)、集中系数(clustering coefficient)等.Akoglu[11]提出了 egonet 特征,如节点所在的三角型数目、egonet 权重等等;
- 网络的图特征主要包括联通分量的个数、联通分量的分布、图的主特征值、最小生成树权重、平均节点深度、全局集中系数等.

基于节点的网络特征的异常检测方法的代表方法是 OddBall.OddBall[11]是一种基于特征的异常检测方法,通过观测基于 egonet 的特征分布规律,查找不符合该规律的 egonet,即可以找出图中的异常节点.自我网络(egonet)关注的不是网络整体,而是以个体节点为中心,通过收集以该个体所关联节点的信息,可以为个体构建一个局部网络.一个 egonet 是指以个体节点为中心的一跳范围内的所有邻居节点,以及这些节点之间的链接构成一个 egonet.如图 1 所示.

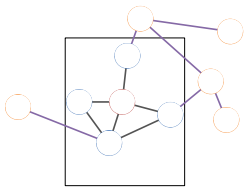


Fig.1 Egonet networks[11]

图 1 Egonet 示意图[11]

图 1 中红色节点为核心节点,蓝色节点为一跳邻居节点,方框中包含的节点和边组成了红色节点的 egonet.通过观测正常真实网络,Akoglu[11]提出如下基于 egonet 的特征的分布规律:给定一个图 G,节点 $i \in V(G)$,节点 i 的 egonet 为 g_i,满足:(1) g_i 中的节点数目 N_i 和边的数目 E_i 符合幂律分布 $E_i \propto N_i^{\alpha}$,$1 \leqslant \alpha \leqslant 2$;(2) g_i 中的权重 W_i 和边的数据 E_i 符合幂律分布 $W_i \propto E_i^{\beta}$,$\beta \geqslant 1$.真实的社交网络符合该幂律分布,根据基于 geonet 的分布规律,OddBall 使用节点值到拟合曲线的距离作为异常值,距离拟合曲线越远的点,异常值越高.算法使用的特征易于计算,可以用于大规模网络异常检测.但是,如果网络不符合幂律分布,则该算法将不起作用,且该算法只能适用于静态图.

2.1.2 基于社团的方法

基于社团方法的主要思路是:通过使用群体检测的方法,将距离比较近的节点归为一个群体,并查找那些连接各个群体却不属于各个群体的节点或者边,即,在网络中查找桥接节点或者桥接边.

该类方法一般分成两个步骤:(1) 通过给定的网络结构,利用节点的相似性或空间邻近性确定节点属于哪些群体;(2) 查找群体的桥接节点或者桥接边.

针对后文图 7 所示的 GLAD 模型图[12],步骤(1)可以基于节点的相似度,使用 *k*-means 聚类方法将节点聚为 *k* 个类.该方法需要借助上一节中提到的相似度的计算方法.步骤(1)也可以使用谱划分的方法,谱划分以谱图划分为理论基础,矩阵的谱就是矩阵的特征值和矩阵的特征向量,图划分问题转换成求解 Laplacian 矩阵的谱分解.算法的核心思想是:通过引入 Laplacican 矩阵,使用特征矩阵进行降维,再对低维的数据进行划分,极大地降低了运算量.

针对很多图划分方法以最大化群组内部边数为目标的方法,往往忽视了两种节点——一种是 hub 节点,另一种是异常节点,Xu 等人[13]提出了网络结构聚类的算法 SCAN.SCAN 算法将网络中的节点分成 3 种角色:一种是组内节点,这些节点属于某一些社团;另外一种是桥接节点,该类节点并不属于某一个社团,它们把不同的社团加以连接;最后一种是异常节点,该类节点只与很少几个特定团体之间有连接.如图 2 所示.

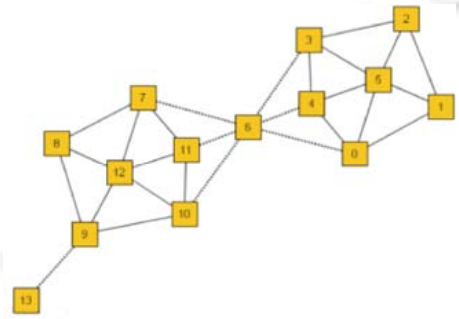


Fig.2 SCAN algorithm[13]

图 2 SCAN 算法示意图[13]

那些没有在高密度的连接块之内的节点则为异常节点.算法借助于 DBSCAN 算法确定超参数ε与μ.算法的时间复杂度为 $O(E)$,当图内边数较稠密时,时间复杂度很高.

网络群体检测还可以使用矩阵分解的方法,Tong 和 Lin[14]提出了使用矩阵分解进行群体检测和异常检测的方法 NrMF,对于一个图 G 的邻接矩阵 A,若一个秩为 r 的 A 的相似矩阵为 $\dot{A}$,那么对应的残差矩阵为 $R=A-\dot{A}$, 对于一个低维的矩阵的分解可以为 $A=\dot{A}+R=FG+R$, 其中,F 和 G 是一个维度为 r 的分解矩阵,R 是残差矩阵.F 和 G 能够自然地反映网络的群体结构信息,而对于残差矩阵,则对应着一个异常节点.实验证实了算法能够有效地识别出网络中的异常连接,可用于端口扫描检测以及 DDoS 攻击分析.

2.1.3 基于信任传播的方法

互联网上有不计其数的网页,用户信息获取的一个重要方式是通过搜索引擎.垃圾网页欺诈(Web spamming)是一种常用的攻击搜索引擎排序算法的行为.PageRank 和 HITS 算法认为:有很多重要的网页指向的网页是重要的网页,实际上是通过页面之间的超链接传播网页的重要性.Gyöngyi 等人[15]提出了针对垃圾网页的检测算法 TrustRank,该算法假设两个网页之间的连接表示两个网页的信任,比如网页 A 指向网页 B 表示网页 A 传递信任给网页 B.

TrustRank 由于种子网页列表的设置会有一定的偏差,使得与种子网站相关领域的网页信任值高,不同领域的信任值低.针对该问题,Wu 和 Goel[16]提出了改进算法 Topical TrustRank,使用话题划分种子网站列表,并提出不同的话题信息值合并的方法.

2.1.4 基于信息论的方法

利用信息论的方法进行异常检测一般使用信息论中的最小描述长度准则 MDL.对于给定的数据集合,使用模型和数据表示原有数据,正常数据使用的模型和描述数据占用空间最小,异常数据使得占用空间增大.MDL 模型具体介绍见第 4.2 节.针对以往的算法只能计算无权图,而真实世界的网络边往往是具有属性值的,如用户

产品打分网络,边上会有用户打分信息;社交网络中的边上会包含关系建立的时间;电话通联网络中会包含电话的持续时间等等.Shah 等人[17]提出了在加权图上利用网络结构和边的信息进行异常检测的方法 EdgeCentric,算法使用 MDL 检测具有异常行为的节点.算法支持同质网络与异质网络,并给出了网络中边的数据为多属性或单属性时节点的异常度量.

Chakrabarti[18]提出了基于图划分的异常边检测算法,算法可以检测出偏离网络大簇的异常的边.方法的核心思想是:如果移除一条边可以使网络更容易划分,那么移除边的两个连接节点则是异常节点.划分算法尝试寻找最好的划分数,使得 MDL 可以编码整个网络的空间使用最小.

2.1.5 基于神经网络的方法

近年来,深度神经网络因为具有较高的灵活性以及能够按照层级提取数据特征,从而在多个领域都取得了很好的性能.使用深度学习的方法解决图异常检测的方法也越来越多,并且通过实验表明,与一些传统方法相比都取得了不错的进步[19].

Chouiekh 等人[20]提出了使用有监督学习的方法,使用正常用户的数据训练神经网络,使用神经网络学习特征,并用于正常用户与异常用户的分类.方法使用电话通联网络用户通话详细信息(CDR),提取其中的通话事件信息,包括通联出度、入度、最大通话时间、每天通话数、每天 SMS 数量等信息,将两个月内用户每天的特征数据表示成一张图,然后使用交叉验证的方法,利用 7 层卷积神经网络进行训练,神经网络由 3 个卷积层、2 个池化层和 1 个全连接层组成.通过实验对比,这一算法比 SVM、随机森林和梯度提升算法取得的效果要好.

Alsheikh 等人[21]提出在 Spark 计算节点上使用深度学习提取特征的方法,解决了深度学习模型含有较多隐层以及海量参数、难以在集群上进行模型训练的问题.该工作用于电话通联网络产生的海量数据,使用 Spark 分布式计算框架提高海量数据的处理能力,是当前很多工业产品的主流做法.

图 3 为分层提取特征的深度学习模型图,第 1 层输入的数据为无标签数据,为了学习到输入数据的结构,每一层包含一个编码函数和解码函数,编码函数使用输入数据与当前层的参数生成一个新的特征集合,解码函数使用特征和参数重构数据,前一层的输入作为后面层的输出.最后,通过浅层特征的不断组合学习到复杂的特征.通过使用标签数据对每一层的参数进行微调,通过该方法可以实现网络的复杂特征提取,并采用 Chouiekh 等人[20]的思路进行模型训练与异常检测.

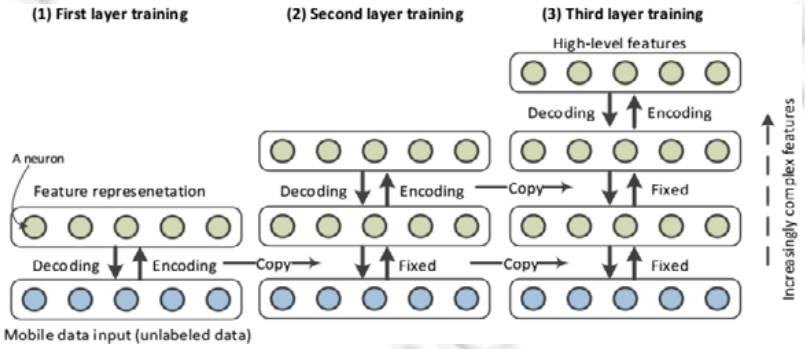


Fig.3 Layered feature extraction with deep learning model[21]

图 3 分层提取特征深度学习模型[21]

以上工作都是采用有监督的方法,有监督的方法需要有一定的标记数据,对于没有标记的数据,可以使用无监督的方法.传统的异常检测方法对数据降维的处理往往采用 PCA 的方法,但 PCA 方法假设系统是线性的,而在真实的环境中系统可能是非线性的[22].针对该问题,自学习编码器是一种无监督的模型训练方法,不需要用户提供标记数据.数据处理流程如图 4 所示.

Zhang 等人[23]提出了使用自编码器降维的方法,并将该自编码器用于社交网络谣言检测,通过使用自编码器,模型能够从原始数据中学习到更多的特征,并通过训练的模型识别正常的用户和谣言制造者.Zhang 等人[23]

的思路是:首先采集每个用户的原始数据,使用原始数据进行标准化处理;然后使用自编码器进行训练,输入和输出设置为相等,使用反向传播算法调整超参数;然后使用训练的模型,输入和输出差距较大的则为谣言信息.网络中的要素除了节点的信息之外,还包括节点的文本信息、用户行为信息等等.Zhang 等人[23]的工作还利用了节点的文本信息,以此来提取特征.

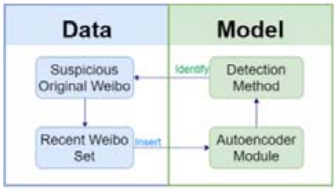


Fig.4 Flow chart for rumor detection using auto-encoder model[23]

图 4 使用自编码器进行谣言检测的流程图[23]

针对自动编码器鲁棒性弱的特点,出现了自动编码器的变种,降噪自动编码器 DA 是在自动编码器的基础上,训练数据加入噪声,所以自动编码器必须学习去除这种噪声而获得真正的没有被噪声污染过的输入[24].因此,这就迫使编码器去学习输入信号的更加鲁棒的表达,这也是它的泛化能力比一般编码器要更强的原因.Castellini 等人[25]提出了使用降噪自动编码器检测僵尸粉丝的方法,该算法针对监督学习的方法需用标签数据、而且标签数据需要覆盖各类异常特征的问题,提出了使用半监督的方法进行异常检测.该方法的总体思路和 Zhang 等人[23]提出的方法相同,使用真实的数据进行训练,得到原始数据的一个低维表示,并训练超参数使得重构数据尽量一致,重构差异较大的数据为异常数据.实验表明,算法的鲁棒性比自动编码器要好.

生成式对抗网络(generative adversarial network,简称 GAN)可以对现实世界复杂的高维数据进行建模,一些算法将 GAN 应用于网络异常检测领域.Zenati 等人[26]提出了使用 GAN 进行异常检测的方法,训练使用 BiGAN 模型,使模型同时学习一个编码器 E,将输入样本 x 映射到一个潜在的表示 z,同时学习一个生成器 G 和判别器 D.有别于普通 GAN 的判别器只考虑输入,这里的判别器同时需要考虑潜层表示.Zenati 等人[26]探索了不同的训练策略,使得 $E=G^{-1}$.通过在 KDD CUP 99 上的异常入侵检测数据集测试,算法取得了当前最高的准确度.

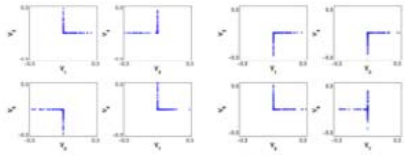
2.2 群体异常检测

给定一个网络数据,从其中查找异常的实体,异常的实体和实体之间存在一定的相互关系,通过异常检测算法检测出的为异常群体.

群体的网络异常检测可以分为基于谱分析的方法、基于稠密子图检测的方法、基于张量检测的方法和基于多层贝叶斯模型的方法等.

2.2.1 基于谱分析的方法

图谱理论是应用图的相关矩阵的特征值和特征向量解决图的相关问题的方法[27],该类方法进行异常检测通常抽取具有相关性的用户群组或对象群组.谱分析中一个很重要的概念就是拉普拉斯矩阵,Von[28]给出了更多拉普拉斯矩阵的变种,如 L_{rw} 和 L_{sym},L_{rw} 可以用于 k=2 到 k=100 的网络划分.研究发现:该方法的网络划分可以检测出很多非常小的簇和一个非常大的核,并且簇内部缺乏相关性.针对该问题,Prakash[29]介绍了直接使用邻接矩阵进行划分的方法,同时发现了一些在大的稀疏网络中存在的规律.通过研究 18.6 万个节点和数百万条边的电话通联网络,发现图的单一向量在一条特定的轴上分布得很清晰,这种规律称为 EigenSpokes,由此算法可以进行检测可疑连接行为.EigenSpokes 基于 SVD 分解.该方法使用奇异值分解(singular value decomposition,简称 SVD)方法,通过对图的邻接矩阵进行分解查找相似的用户群.一般的工作都是通过分析左奇异矩阵 U_i 和 U_j 来发现存在的不同寻常的模式,如沿轴向分布、分布成类似珍珠的团等等.在图 5 所示的电话通联网络中,显示出不同时空域对应的 EigenSpokes 规律分布图.



(a) Region 2, Time 2 (b) Region 3, Time 3

Fig.5 Time and space distribution of telephone communication network[29]

图 5 电话通联网络中不同时空域对应的分布图[29]

2.2.2 基于稠密子图的方法

稠密子图挖掘一直是图数据挖掘的热点,一般地,基于稠密子图异常检测的步骤是:首先查找网络中最稠密的 k 个子图,然后进行异常检测.该类异常检测的定义根据场景的不同其使用方法也不尽相同.例如:社交网络中的所有节点应该都在一定的密度子图中,没有在稠密子图中的少量节点为异常节点;而在用户-商品构成的二部图中,欺诈账户往往因为有较高的一致性评价从而形成了稠密子图,而此时,在最稠密子图中心的节点往往是欺诈节点.

传统的用于稠密子图检测的方法一般是使用子图平均度度量,Charikar[30]提出使用子图的平均度定义子图的密度,对于一个图 $G=(V,E)$为一个无向图,其中,$S\subseteq V$,定义 $E(S)=\{i,j\in E:i\in S,j\in S\}$,定义子图的密度为 $f(S)=|E(S)|\div|S|$,即子图中边的个数与点的个数的比值.$2f(S)$是集合 S 的平均度,而稠密子图的问题则转化为计算函数 $f(S)$最大值的问题.求解该 $f(S)$的问题是一个线性规划问题,Charikar[30]给出了求解问题的精确算法.为了降低算法的复杂度,Charikar[30]提出了一种近似比为 2 的近似算法.

已有的利用检测子图最大平均度密度的方法存在一定的偏差,往往使检测出的结果包含大量的正常用户,准确率较低,增加了后期人为判断的难度.针对这一问题,Liu 等人[31]提出了 HoloScope 方法,基于“对比可疑度”的度量标准在 5 000 万条边的大图上,利用单机计算节点进行检测异常:(1) “对比可疑度”动态度量了异常用户和正常用户行为的对比性差异,包括连接拓扑、时间序列起伏、评分多样性等信息,有效地防止了对正常用户行为的误判;(2) 该检测方法鲁棒,并从理论上给出了对欺诈者攻击时间的屏障下界,增加了欺诈的时间成本;(3) 在仅利用拓扑结构和全部信息这两种实验条件下,该检测方法都比相应的基准方法在准确率上有较大的提升;(4) 算法的时间复杂度与大图的边数近似地呈线性关系,具有应用于大规模数据分析的能力.

2.2.3 基于张量分解的方法

谱分析方法一般使用邻接矩阵特征分解和 SVD 分解进行稠密子图的检测,EigenSpokes 算法用来在模式图中查找异常的模式,Jiang 等人[32]用于在社交网络中查找相同规律的关注者账号,Shah 等人[33]提出 fBox 用来在社交网络中查找小规模的异常攻击.

图或社交网络一般被建模为二维网络数据进行研究,但这样往往带来数据的缺失.近年来,人们使用多模数据(张量)对网络进行建模与分析,当模度为 2 时,可以建模社交网络的关注与被关注者的关系,如建模 Fasebook 上的谁和谁是朋友的关系;当模度为 3 时,可以建模以上网络是如何演进的或者商品评价时使用的是什么词组;当模度为 4 时,可以通过分析目标 IP、原始 IP、目标端口、时间戳等信息来追踪网络轨迹或者进行入侵检测.

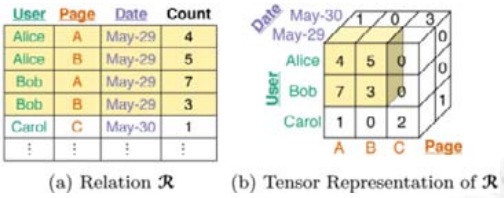
以维基百科修改历史数据集为例说明张量表示:存在关系 $R(user,page,date,count)$,每个元组(u,p,d,c)表示用户 u 在日期 d 修改了页面 p,次数为 c.关系中,前 3 个是属性,分别为 $user$、$page$ 和 $date$,最后一个是度量属性 $count$.

图 6 所示为关系的张量表示,底色为黄色的数据构成子块 B,在图 6(b)中,子块 B 对应着子张量 R.

针对基于 SVD 分解的方法以及张量分解的方法没有对多模稠密子图按照可疑度进行排序这一问题,Jiang 等人[34]提出了 CROSSSPOT 算法.该算法给出了在多模数据中进行稠密子图测量的度量公式,并提出了针对子向量或子张量进行可疑度计算的度量公式,并使用该度量在张量中查找稠密子图.

针对以往张量计算的算法计算速度较低、精确度也较低的问题,Shin 等人提出了一种灵活的、可调整的在张量中查找稠密子图的框架 M-Zoom[35].以往的算法在考虑子图密度时,使用的密度度量方式分为 3 种:基于算术的度量方式、基于空间的度量方式、基于可疑度的度量方式.M-Zoom 算法可以使用以上但不限于这 3 种度

量方式.M-Zoom 给出可以使用的子张量密度的定义为:如果两个块在某一个属性上有相同的基数,两个块的度量相等或者更高,则两个块的稠密度是相同的.算法可以用于在维基百科中查找冲突观点的用户之间的编辑战,也可以检测出维基百科中的攻击活动,如频繁的页码修改攻击.该算法也可以用来进行网络入侵检测,在网络AirForce 数据集上,该算法测试 AUC 为 0.98.



(a) Relation $\mathcal{R}$ (b) Tensor Representation of $\mathcal{R}$

Fig.6 Tensor representation of relations

图 6 关系的张量表示

2.2.4 基于多层贝叶斯模型的方法

层次贝叶斯模型是一个统计模型,用来为具有不同水平的问题进行建模,通过贝叶斯方法估计后验分布的参数.使用多层贝叶斯模型进行异常检测的方法多是使用概率分布创建一个数据的生成模型,并将那些相对不是模型生成的数据认为是异常数据.Xiong 等人[36]提出了两种层次贝叶斯模型,第 1 种就是隐含狄利克雷分布(latent Dirichlet allocation,简称 LDA)模型,文献[36]假设每一个单独的数据点属于几个话题,每一个群组是话题的联合分布,使用多元高斯分布来确定观测数据属于哪一个话题.Yu 等人提出了 GLAD 算法[12],GLAD 模型利用节点的特征信息和网络结构信息,自动推断群组的成员组成以及同时判断成员的角色.假设每一个成员为 p,一个群组为 G_p,一个角色为 R_p,G_p 表示考虑了网络信息相似性的聚类,R_p 表示节点特征值的归类.为简化起见,定义群组的个数为 M,角色的个数为 K,图 7 所示为 GLAD 的模型图.

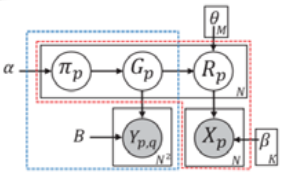


Fig.7 GLAD model[12]

图 7 GLAD 模型图[12]

GLAD 利用角色混合比例来定义群组的异常值,群组的异常值为 $-\sum_{p\in G}\langle \log p(R_p \mid \theta)\rangle_p$,分值越高,群组越异常.GLAD 的局限在于只能对静态图进行建模,无法建模动态图.除了群组的角色比例与其他正常群组不同之外,研究混合比例随网络演进的变化过程也是很有意义的.

2.3 小 结

本节主要对面向静态图异常检测的方法进行归类总结,并从个体异常检测以及群体的异常检测两个方面进行归纳,将个体的异常检测分成基于网络结构的异常检测、基于群体的异常检测、基于信任传播的异常检测和基于信息论的异常检测等几种类型.早期对于静态图异常检测的研究主要从图的特征提取、图结构划分以及信息压缩等方面进行,但对于大规模图数据异常检测而言,早期方法往往不能胜任.近年来,由于网络规模的提升以及计算能力的提升,图异常检测方法主要使用张量分解技术以及神经网络的相关技术.这两种技术都可以利用多模数据,异常检测也不是仅局限于网络结构特征,还可以融合考虑节点的内容信息、标签信息以及行为信息,并且应用越来越广泛.

静态图在对数据进行建模时没有考虑到时间维度,即:随着时间的变化,网络结构变化对应的图数据也发生了变化.因此,静态图异常检测也具有局限性.动态图异常检测技术在静态图异常检测的基础上发展而来.

3 面向动态图的异常检测

现实世界中的网络并不是一成不变的,而是随着时间的改变,网络的结构和网络节点的属性也在不断发生着变化,比如新的节点加入、个体之间新关系的增加或者消失、节点属性的改变等等.动态图的异常检测主要研究异常的节点、关系或者节点所处的某一个特殊的时刻.动态图异常检测主要是检测那些和大多数网络演进行为不同的异常情况,动态图异常检测在现实生活中有很多重要的应用,如生态失衡的研究、网络系统的入侵研究、社交网络中异常用户和事件的研究、社交网络用户舆情检测.虽然近几年来有很多用于静态图异常检测的方法,但是该类方法无法直接用于动态图,这是由于动态图异常检测和静态图异常检测模型不同所致.针对挑战和异常类型的不同,主要表现在如下几个方面.

(1) 图异常的种类不同:静态图中有异常点、异常关系、异常的子结构;动态图中同样包含以上几种异常,但是还包含图断层、图子结构消失或者偶尔出现的社交群体等等;
(2) 网络原型的变化有了时间的维度,需要同时存储时间维度并进行分析,每一个时间维度需要对原有图和增量图进行存储分析,原有静态图的分析方法还可以将所有数据加载在内存中进行计算,动态图中由于数据量太大将无法实现;
(3) 网络原型与时间的关联性具有多样性,如社交网络变化较快而基因网络变化较慢;
(4) 有些图异常会跨多个时间域,分析起来更加困难.

动态图的异常类型可以分为异常实体、关系、子结构和事件这 4 种.本文将异常分成个体异常检测、群体异常检测和事件异常检测这 3 部分.个体异常检测包括异常实体、关系以及事件的检测.最后根据异常检测采用的技术进行二次分类,主要包括基于社团检测的方法、基于压缩的方法、基于距离的方法、基于概率模型的方法等.

3.1 个体异常检测

动态图往往可以表示成为一个图和时间相关的序列.动态图中检测异常的个体之间是相互独立的,没有依存关系的为面向动态图异常个体检测,其中,异常的类型可以是异常的节点、异常的边、异常的时刻等等.主要使用的方法可以分为基于偏差的方法、基于谱的方法和基于降维的方法等几类.

3.1.1 基于偏差的方法

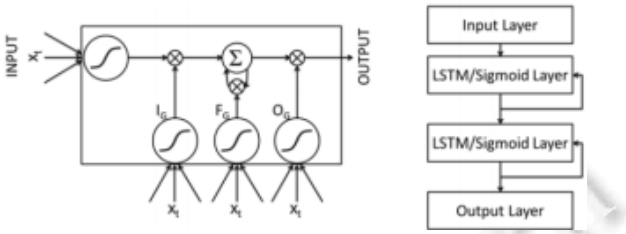
动态图异常检测最基本的方法就是构建每一个时刻网络对应的特征,然后进行异常分析.Pincombe[37]定义了图结构特征的距离来衡量两个连续时刻的图结构的差异,比如权重、边数、节点数、网络直径等.该工作用于网络异常演进时间节点检测.给定一个时间段以及度量方式,构建一个网络特征的序列.给定图 $G=\{V,E,W_V,W_E\}$,算法对每一种图的特征构建一个时间相关序列,每一个时间序列使用自回归滑动平均模型进行建模.自回归滑动平均模型(autoregressive moving average model,简称 ARMA 模型)是研究时间序列的重要方法,由自回归模型(简称 AR 模型)与移动平均模型(简称 MA 模型)为基础“混合”构成[38].

针对 ARMA 模型无法考虑一段时间内网络特征变化的特点,Malhotra 等人[39]提出了使用 LSTM(long short-term memory)进行异常检测的方法,LSTM 是长短期记忆网络,是一种时间递归神经网络,适合于处理和预测时间序列中间隔和延迟相对较长的重要事件.通过在 LSTM 中包含一定的循环隐层,可以令网络使用更稀疏的表示学习到更高层级的时序特征.算法通过使用不包含异常的数据进行训练,得到一个与时间相关的预测函数,预测结果的误差应该符合多元高斯分布,并以此进行异常检测.

算法的模型为:针对一个时间序列模型 $X=\{x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(n)}\}$,其中,对于每一个时刻 t 对应的 $x^{(t)}\in R^m$,是一个 m 维的向量 $\{x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(n)}\}$,每一个值对应一个输入变量.训练一个预测模型用来预测输入变量的值,训练使用交叉验证的方法,将正常的数据集分成 4 个部分:正常数据、正常验证数据 1、正常验证数据 2、正常测试数据.首先使用 LSTM 训练模型,然后计算预计错误的分布函数.图 8 所示为该算法 LSTM 的模块单位和层级结构.

LSTM 的网络架构为:使用 m 个维度中的一个作为输入,$d\times l$ 个单元作为输出,隐层的 LSTM 单元是循环网络的一个全连接网络,使用时间序列 S_N 进行训练,集合 V_{N1} 用来停止训练.使用 S_N 训练的模型计算验证数据集合

实验数据集中的每一个点对应的错误值的向量,错误向量的分布符合多元高斯分布 $N=N(\mu,\Sigma)$,使用最大似然估计的方法估计参数μ和Σ的值,在 t 时刻的相似度 p^t 通过 t 时间的错误向量进行计算,当 p^t 小于阈值τ时,任务在 t 时刻是异常数据;否则为正常数据.阈值τ可以通过最大化 $F_{\beta\text{-}score}$(异常数据为正样本,正常数据为负样本)计算得出.



(a) (b)

Fig.8 Units and hierarchies of LSTM[39]

图 8 LSTM 模块单位和层级结构[39]

基于偏差的方法也需要首先定义一个度量衡量两点之间的区别,偏差也可以认为是距离.异常节点和异常边的异常检测有些是基于距离度量的方法.衡量两个图的相似度一般使用网络的结构特征,如网络中节点的数目,不同的方法选择不同的度量方式,并用来计算异常值.

3.1.2 基于社区的方法

基于社区的方法追踪网络社区随着时间推进的社区变化情况以及社区组成节点的关系变化过程,同时进行异常检测.该类方法主要应用社区的网络结构,方法的不同体现在两个方面:(1) 对社区结构进行分析的方法不同,比如采用不同的社区检测方法;(2) 社区定义的方法不同,有的方法按照可能性认为节点可以隶属于多个社区,即有重叠的社区发现,而有些方法认为节点只能属于一个社区.

面向动态图的基于社区的孤立异常检测可以分为异常节点的检测和异常关系的检测.一个社区中的节点应该具有一定的相似性,如果一个节点在某一个时间段内新增大量的边,那么其他节点也应该新增大量的边.如果其他节点没有新增大量的边,那么该节点为异常节点.

针对动态图中社团演进模式难以发现以及存在很多干扰因素的问题,Gupta 等人[40]提出了一种有效的检测网络演进趋势异常的方法:首先对正常的网络社团演进行为使用潜在的模式挖掘进行建模,然后使用他们提出的通过计算节点演进与正常演进模式之间的距离来计算偏差.

Fu 等人提出了 dMMSB[41]模型以识别网络中角色以及角色随着时间变化的过程,但该模型需要用户指定一个超参数.Rossi 等人针对 dMMSB 模型需要超参数以及算法可扩展性差的问题,提出了一个可扩展的时序行为模型 DBMM[42],用来分析节点行为随时间变化的过程,学习一个预测模型估计节点行为,并可以检测异常的时序行为转移情况.

3.1.3 基于矩阵分解或张量分解的方法

该类方法一般是将网络表示成为张量,然后使用张量分解的方法或者其他降维的方法.动态图的异常检测首先需要对动态图进行建模,最简单且直接的方法是将时间作为一个维度,另外几个维度为其他感兴趣的因素.使用张量进行建模的优点是扩展性强,算法可以通过增加维度来考虑更多的信息,如属性信息.然后在整个图的张量的角度上,查找通用的模式并检测出异常的模式.静态图和动态图使用张量进行异常检测的方法是类似的,对于一个模度为 2 的张量,一般使用 SVD 分解的方法进行异常检测;在高维的张量上进行异常检测,则使用 SVD 的扩展方法 PARAFAC.

通过矩阵分解可以得到每一个节点的活动向量,如果一个节点的活动在一个连续的时间内变化较大,则认为该节点为异常节点.在静态图中,常使用主成分分析的方法进行降维,但在整个动态图中使用 PCA 降维,计算量会特别巨大.Yu 等人[43]认为,动态图的异常改变或者发生事件具有时间和空间上的局部性.因此,Yu 等人提出

在网络边结构上使用局部的 PCA 方法进行分析,局部的特征向量表示了边关联模型的相关信息,而局部的特征值则表示了网络边关联变化强弱的相对水平.

Yu 等人[43]算法的主要思路是:对每一个节点维持一个边连接矩阵 M,M 为 $n\times n$ 的矩阵,其中,n 为连接邻居的数目.对于每一个节点 i,值 $M(j,k)$表示边(i,j)和(i,k)的频率权重,频率权重采用衰减函数,随着时间的推迟而减弱.针对矩阵 M 使用 PCA 降维方法,最大的特征值和特征向量表示了关联边的变化活动情况,每个时间快照的特征值构成了一个时间序列.在阈值之外的特征值对应的时间节点为异常时间点,对应的节点 i 为异常节点.

3.1.4 异常边识别方法

以上方法都是从动态图中查找异常节点,还有一些方法是从网络中查找异常边.如 Heard 等人[44]认为:如果一个社交网络在某些方面进行了重要的改变,那么意味着在大多数情况下存在一些个体通联比以往更少或者更多,或者进行通联不同个体的数量比平时更多或更少.因此,他们提出一种在动态图中进行异常检测的两步骤方法:第 1 阶段清理数据库找到潜在的网络异常节点子数据集,第 2 步使用该子数据集构建一个子图.该算法可以完全并行执行.收敛到有问题的快照和节点对数据后,使用谱聚类的方法查找网络中的节点簇,收敛计算结果,提高准确性.

Li 等人[45]将交通网络视为一个边的权重随时间而变化的动态图,他们使用衰减函数计算随着时间的变化边权重的变化情况.算法将动态交通网络视为一个网络边的流,整个网络没有固定的拓扑结构,如果一条边在流中频繁出现,则该网络中该边会持续存在,关于边的持续函数计算是通过该边自从添加后持续的时间长度来表示的.异常度函数使用相似函数的变化总和表示,算法需要给定一个启发式参数 k,查找最异常的前 k 个边.Abello 等人[46]提出了基于集合偏差的异常模式检测方法 DND,该方法将图中的所有边标记上两个个体之间通信的时间,将整个动态图视为一个集合系统,这样可以使用组合差查看不同时间范围的变化情况,DND 的网络表示图如图 9 所示.

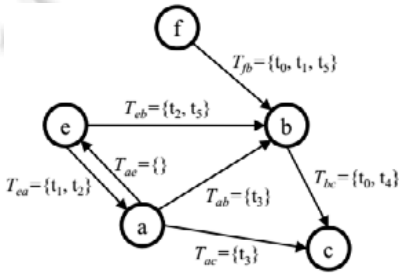


Fig.9 DND algorithm[46]

图 9 DND 算法[46]

DND 算法使用边集合偏差表示边的频率,当网络中存在一个新的边时,边的差通过与所有活跃的边的偏差的平均值进行计算而获得,如果该边的集合差超过一定的阈值,那么就认定边是异常的边.

3.2 异常群体检测

区别于动态图的孤立目标异常检测,动态图群体检测考虑到时间维度,难度更大.因为首先要根据给出的时间序列数据,提取出所有的社团信息,这需要使用社团发现的相关算法.而随着时间的改变,社团的组成结构是变化的,每个时间快照数据中的社团信息需要对应起来,这需要使用社团匹配的技术.Greene 等人[47]给出了追踪网络社团演进的一些方法,可用于社团匹配以及社团演进研究.当确定好匹配的社团之后,才可以使用异常检测的方法对社团的变化情况进行比较,如比较子图的边的权重、比较子图在相邻时间上的三角形数目的变化情况.在动态图中,异常子图主要是社团分解、社团合并、社团消失或者频繁再现等等不同于其他多数社团变化的子图和时间戳.动态图异常群体检测不同的领域,关注的异常群体的类型也不一样,如可以分析交通情况或者用于分析社交网络异常群体.

动态图异常群体的检测方法一般可以分为基于社团检测的方法、基于降维的方法和基于距离的方法等.

3.2.1 基于社团检测的方法

基于社团的方法首先将每一个时间的网络快照数据进行社团检测,然后分析社团的演进过程.

Chen 等人[48]提出一种基于社团的无参数的异常检测方法.Chen 等人认为,社团异常主要分为 6 种类型:社团的收缩、社团的增长、社团的合并、社团的切分、新社团的诞生和社团的消亡.算法使用社团代表集合,将临近时刻的社团代表集合进行比较,并将社团的变化情况归为 6 种异常中的一种.图 10 所示为社团增长和社团合并的示意图.

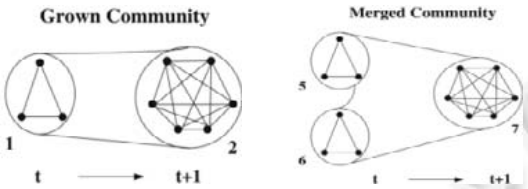


Fig.10 Community growth and community consolidation[48]

图 10 社团增长和社团合并示意图[48]

算法使用的是有重叠的社团检测技术,使用社团代表集合代表一个社团.一个社团的代表定义为在该社团中存在的且在其他社团中存在的次数最少的节点.通过使用代表集合,可有效降低算法的时间复杂度.

Araujo 等人[49]提出了一种基于增量张量分解的异常群体检测方法,可以发现临时的社团或者周期性不断出现的社团.算法使用 MDL 的方法进行社团分析,并使用张量分解的方法收敛计算结果集合.他们提出了一种近似算法,算法首先对每一个起点终点时间对给出一个打分,挑选出候选社团集合,使用得分值进行排序,查找重要的社团,使用 MDL 确定社团的大小,最后根据检测到的社团结合,再次使用张量分解多次迭代找到最优结果集合.

3.2.2 基于分解的方法

基于分解的方法是指使用矩阵分解或者张量分解的方法进行异常检测,张量分析是高维数据分析的一种有效工具.Koutra 等人[50]提出了一种基于 PARAFAC 的分解方法,可以检测出动态图中微小的团或者微小的改变,并进一步用于异常检测.

TENSORSPLAT 可以检测动态图中的改变,如在 DBLP 数据集中,可以检测经常转换研究领域的作者.另外,还可以检测随时间改变的异常情况,如可以在计算机连接网络或者社交网络交互中检测异常情况.算法还可以检测节点聚类信息,如研究领域相同的作者或者是相同的会议上发表论文的作者.

虽然已经有了成熟的张量分解的方法,但是很多现实的情况是数据量太大而无法加载到内存中.针对内存中无法加载超大张量的情况,Papalexakis 等人[51]提出了一种可并行执行并加速的张量分解的方法,算法可以提供运行速度 14 倍,并给出了分解结果正确的理论下限.

总而言之,使用分解的方法多是在静态图的基础上考虑时间维度信息,并使用张量分解的方法分析网络变化情况,以进行异常检测.

3.3 事件异常检测

不同于静态图,动态图除了有异常点、异常边、异常子图之外,还有一种类型是事件异常检测.通常情况下,事件异常检测是在时序数据中查找与其他大多数不同的时间点,再通过对时间点的网络结构数据使用静态图的异常检测方法深入研究异常发生的深层原因.

从时序数据中查找异常数据,需要将每一个时间快照的网络数据提取网络特征,临近的数据使用相似度的评估方法检测异常数据,如可以使用每个时间快照的节点的数目和连接边的数目变化情况,也可以提取每个时间快照的平均集聚系数,分析变化较大的时间点.

3.3.1 基于分解的方法

分解的方法主要是指矩阵分解或者张量分解的方法.基于分解的方法的主要思路有两种.

- 一种是使用数据降维,然后使用降维后得到的向量对原始数据进行重构还原.如果重建的误差高于一定的阈值,则认为对应的原始数据是异常数据,如 Sun 等人[52]提出的异常检测方法;
- 另一种思路是对每个时刻的图数据的特征值和特征向量进行计算,分析其变化趋势,变动较大的数据则为异常时间点.

低维度的数据往往可以直接采用 SVD 分解的方法或者 CUR 分解的方法,但是实际使用的数据是高维度稀疏的图数据,而稀疏的高维张量往往无法直接加载到内存中.Sun 等人[52]提出了一种压缩的矩阵分解方法,用于计算高维系数矩阵,并可以从动态图中检测事件异常.

Sun 等人[52]提出的异常检测思路是对于每一个时刻 t,使用提出的高维系数矩阵的压缩方法,计算出一个低维稠密的矩阵,并存储对应的列和行,存储近似差值 SSE,近似差值可以认为是使用压缩后的矩阵能够掌握的全局变化的信息量.在整个时间序列过程中,固定压缩比例和压缩后矩阵的大小,观测近似差值的变化情况.如果一个时刻的近似差较大或者一个时间段内近似差值变化较大,则在对应的时刻网络中有较大的变化或者事件,可以进一步采用静态图异常检测的方法进行研究.

以往的面向网络数据流的异常检测方法往往是基于数据源的方法,该类方法大多是在数据源嵌入一种检测算法,但该类方法无法找到异常的完整分布情况.针对该问题,Jiang 等人[53]提出了在完整网络数据流中使用稀疏 PCA 进行异常定位的方法,算法使用学习到的正常子空间进行异常检测.

3.3.2 基于距离的方法

基于距离的方法进行事件检测需要定义一个距离度量函数[54],计算一个时间序列数据中任意两个连续的时刻之间的图的距离;然后使用滑动窗口计算平均值或者查找前 k 个偏差比较大的值对应的时刻[55].

Berlingerio 等人[56]提出了一种基于距离的评价网络相似度的方法 NetSimile,给定两组节点集合,使用 NetSimile 算法可以计算两组网络之间的相似度,且网络之间可以没有共有节点.算法可以使用在迁移学习中或者是网络节点更换身份之后的重新识别.算法的主要思路是:针对每一个图 G,从众多的特征之中提取出能够表示网络结构和网络结构特征分布规律的特征.两个图之间的相似度就是两个图的指纹特征向量的相似度.

计算两个图之间相似度的方法多种多样,Soundarajan 等人[57]对常见的计算两个图距离的方法进行对比,通过实验对比近 20 种网络相似度的方法后发现:不同的网络相似度的计算方法具有惊人的相关性,一些复杂的计算网络相似度的方法可以使用简单的方法近似计算,并且带重启的随机游走方法和 NetSimile 方法取得的结果排序是一致的.

3.3.3 基于神经网络的异常事件检测方法

时序数据分析的传统方法采用基于统计的方法居多,近年来,随着深度神经网络的发展,尤其是长短期记忆网络的发展,由于其具有存储长期记忆的能力,对处理未知长度的序列数据非常有用.LSTM 内部的循环隐层使得神经网络能够学习到更高层的时序特征.

Malhotra 等人[39]提出了使用 LSTM 进行异常检测的方法,通过使用 LSTM 网络建模正常数据,可以准确地检测出没有预处理过的异常.实验结果表明:LSTM 的 sigmoid 的神经层可以捕获时间序列的结构信息,并可以从不同的时间范围处理时间序列信息.该方法已在第 3.1.1 节中进行了详细介绍.

真实的数据中往往已经包含了异常的数据和变化的数据,这些数据使得训练的模型偏离了潜在的模式,尤其是实时在线系统.Guo 等人[58]提出了一种鲁棒性更高的自适应梯度方法的 LSTM 神经网络,以预测时序数据中的异常和变化的点数据.算法通过时序网络局部的特征来设置损失的梯度,以适应于新的实时的观测数据.算法使用 LSTM 对时间数据建模,并采用随机梯度下降的方法从时间序列数据中学习模型,一个新的观测数据到达后,模型的参数根据新的可用数据损失的梯度进行更新,如果新的观测数据是可能的异常数据,则与常规模式的数据不同,其对应的梯度将会下调,从而避免在线模型突然偏离正常的模式.该方法定义了一个变化点和前后的时间差距较大的点.如果一个新的观测数据为一个变化点,则对应的梯度将会被限制在一个较高的值并引导模型适应新的数据.算法根据局部数据的分布特征构建一个权重函数,权重由可疑度和局部数据偏差构成,使得模型学习过程更具有鲁棒性.

Malhotra 等人[39]提出的方法认为:异常是一个孤立的时间点,并且每个点之间是相互独立的,异常检测的模型并没有利用以往的数据或者事件来评估当前点的能力.在一些应用场景中,如 DOS 攻击,事件通常会持续一段时间,并且异常是由一个连续的时间点集合来表示的,单独一个点的访问失败是正常的,但当很多点同时访问失败就不正常了.为了检测这种攻击,异常检测的模型需要能够捕获并记住以往的一些事件,Bontemps 等人[59]针对以往的方法仅针对孤立点进行异常检测,提出了使用 LSTM 网络查找群体异常的方法,并将该方法应用于网络入侵检测.在文献[59]中,当前的事件依赖于以往的事件和当前的事件,模型通过一个循环数据监测群体异常,循环数据中使用模型预测指定的时间之后的结果,如果预测误差超过了一定的阈值并且持续了一段时间,则认为是一段群体异常.

Malhotra 等人[60]认为:时间序列数据往往会受到外部因素的干扰,如人为操作因素或者外界环境因素,而且可能不会被时间序列数值感应器接收到,数据噪声和异常数据同时存在,因此对时间序列的预测是困难的.Malhotra 等人[60]提出了使用编码-解码器的 LSTM 神经网络,使用模型重建正常的时间序列,使用重建误差检测异常.编码器学习一个向量表示一个时间序列,而一个解码器则表示重建一个时间序列,该模型的训练只能使用正常的时间序列数据.该方法可以适用于多传感器的时间序列数据,当给出一个异常序列之后,原有的模型不能很好地重建数据,这样会导致较高的重建误差,以此来判定异常数据.图 11 所示为序列数据的推断模型.

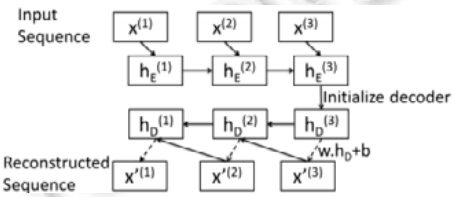


Fig.11 Model to predict $\{x'^{(1)},x'^{(2)},x'^{(3)}\}$ with $\{x^{(1)},x^{(2)},x^{(3)}\}$[60]

图 11 使用序列数据$\{x^{(1)},x^{(2)},x^{(3)}\}$预测$\{x'^{(1)},x'^{(2)},x'^{(3)}\}$的模型[60]

生成式对抗网络(generative adversarial network,简称 GAN)可以对现实世界复杂的高维数据进行建模,一些算法将 GAN 应用于网络异常检测领域.当前的时间序列数据都是多元数据,即,在同一个时间点同时有多个感应器检测到的数据.Li 等人[61]提出了使用 GAN 和 LSTM 相结合的方法进行异常检测,算法将多元数据同时进行考虑,针对很多有监督的异常检测算法采用的是线性映射和转换的无监督的异常检测算法,算法使用非线性转换的方法综合考虑多个时间序列.图 12 所示为模型架构图.

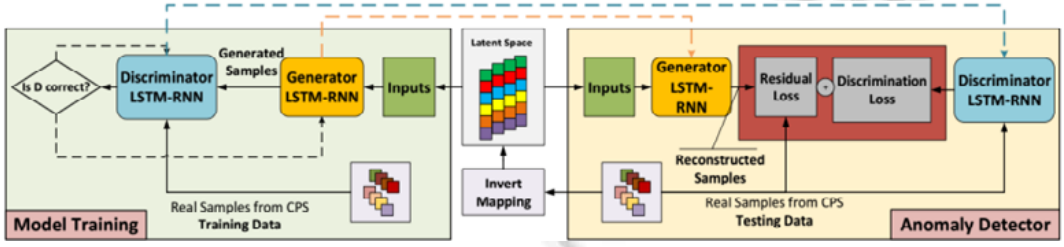


Fig.12 An anomaly detection model based on GAN[61]

图 12 基于 GAN 的异常检测模型[61]

图 12 左面部分是一个典型的 GAN,生成器从一个指定的潜在空间生成一个假的样本,并传递给判别器.判别器区分生成样本的真实与否,根据生成的结果更新判别器和生成器的参数,使得判别器更好地区分数据的真实性.生成器则被训练得尽量能够骗过判别器,即让判别器认为假的样本为真.通过足够多轮的迭代,生成器能够找到训练序列的潜在分布,判别器则能够区分真和假的数据.图 12 右侧的框架是利用 GAN 的生成器与判别器进行异常检测,生成器用来计算重建的样本和真实数据之间的残差,判别器用来计算判别差.通过实验验证,

算法可有效检测出网络攻击.

3.4 小 结

动态图异常检测是异常检测的一个重要领域,本节将面向动态图异常检测的异常类型分成了 3 种类型:孤立点或孤立边的异常检测、异常群体的检测、事件的异常检测.动态图异常检测问题常常为任务驱动,不同的应用目标可以使用不同的方法.如在社交网络中,查询异常的账号或用户行为需要使用个体异常检测;金融欺诈中查找异常的时间节点,需要使用事件异常检测的方法.

4 面向图的异常检测技术框架与应用

4.1 面向图的异常检测的关键技术

图是一种常用的数据结构,用来描述实体和实体之间的相互关系.近年来,随着社交网络以及知识图谱的推动,图数据挖掘与图异常检测受到广泛关注,面向图的异常检测也出现了很多新的方法,总体来说会涉及以下几个关键技术之一.

(1) 降维.降维技术是图异常检测的常用技术之一,这是因为降维技术解决了图异常检测中的两大问题:正常数据模式提取问题以及高维数据计算复杂度高的问题.在面向图的异常检测中,使用降维技术提取数据的主成分,正常数据可以使用主成分加以表示而异常数据无法做到,这是使用降维技术解决该类问题的一种常用思路,如利用自编码器模型进行数据重建、使用重建误差进行异常检测的方法和 NMF 方法等等.随着网络规模的快速膨胀,降维技术还能提高算法执行效率,有利于降低原始数据计算复杂度.降维技术主要应用于无监督异常检测中.基于矩阵分解的方法和基于张量分解的方法的本质都是降维,传统的降维方法包括 MDL 方法与 PCA 方法.网络嵌入技术以及当前火热的图神经网络技术,也是将高维抽象空间的数据映射到低维具象的空间.如利用节点内容相似度进行异常检测,可使用 node2vec、LINE、GraRep;利用节点的结构进行异常检测,可使用 struct2ve;利用节点的附加信息,可使用 CANE、CENE 方法;

(2) 深度神经网络模型.该类方法受神经网络在其他领域取得的成功的启发,利用了神经网络和数据集训练识别器.该类方法不需要提取特征,模型会学习数据的低维特征和高维特征,并进行识别.图卷积神经网络可以直接端到端地分类或回归.该技术主要分为两类:一种是谱图卷积,在傅里叶域进行卷积变换;另一种是空间域卷积,直接在网络上进行卷积.该类方法主要应用于有监督的异常检测中;

(3) 预测模型.该类方法是前面两种关键技术的结合:首先,通过将原始的真实数据输入到神经网络中,然后使用神经网络模型学习正常数据的潜在规律,使用学习到的模型预测未来的数据,并利用预测误差的分布规律或使用判别器判断异常,如使用 LSTM 或 GAN 模型进行预测.该类方法主要用于图异常事件检测.

4.2 面向图的异常检测的常用框架

从给定的原始数据中是否包含标注数据的角度,面向图的异常检测可以分为有监督的异常检测方法和无监督的异常检测方法.有监督的异常检测算法的一般框架如图 13 所示.

在有监督的图异常检测算法中,使用的特征包括数据本身的属性信息(如社交网络中节点的信用等级、是否认证等等)以及图的特征信息(如节点的出度、入度、中介中心度等等).

对于没有可靠标注的数据集,使用无监督的图异常检测技术,算法的一般框架如图 14 所示.

无监督的图异常检测技术常使用降维技术,对原始数据降维表示,并使用降维之后的模型表示原始数据,利用重建误差进行图异常检测.常用的图降维技术有:

(1) Network embedding 技术.网络嵌入技术的目标是学习网络中节点的低纬度潜在表示,学习到的特征表示可以结合聚类技术,用于图异常检测;

(2) MDL 技术.最小描述长度(MDL)准则是 Rissane 在研究通用编码时提出来的,其基本原理是:对于一组

给定的实例数据 D,如果要对其进行保存,为了节省存储空间,一般采用某种模型对其进行编码压缩,然后再保存压缩后的数据.所以需要保存的数据长度(比特数)等于这些实例数据进行编码压缩后的长度加上保存模型所需数据长度,将该数据长度称为总描述长度.最小描述长度(MDL)原理就是要求选择总描述长度最小的模型.不失一般性,如果一个数据可以使用一个模型很好地进行压缩,则为正常数据,异常数据则是那些使得最小描述长度变长的个体,如 Shah 等人[17]的算法使用 MDL 检测具有异常行为的节点,算法支持同质网络与异质网络.Chakrabarti[18]提出了划分算法尝试寻找最好的划分数,使得 MDL 编码整个网络占用存储空间最小.MDL 技术能够用于异常检测技术,原因是该技术能够压缩表示原始数据,而异常数据的表示需要较高的成本,以此进行异常检测;

(3) 图谱论相关技术.使用拉普拉斯矩阵表示图,利用使用特征值和特征向量表示对原有图进行表示,使用前 k 个特征值和特征向量对原始数据降维表示;

(4) 张量分解.将一个张量表示成有限个秩-张量之和,达到数据降维的目标;

(5) 编码器-解码器模型.该模型包含两部分内容:编码器的作用是将高维的原始数据降到低维的结构上表示,解码器是编码器的逆过程.编码器与解码器之间的隐层是该模型的核心,能够反映高维原始数据的本质规律,确定原始数据的维数;

(6) PCA 降维.经过特征工程之后的数据,有很多特征存在线性相关性,PCA 方法的原理是查找原始数据在某一个维度或者方向上的投影,从而使数据在这些方向上投影的方差最大.这些方向包含了更多信息量,从而进行数据压缩以及异常数据挖掘.PCA 降维的缺点是只能线性降维.

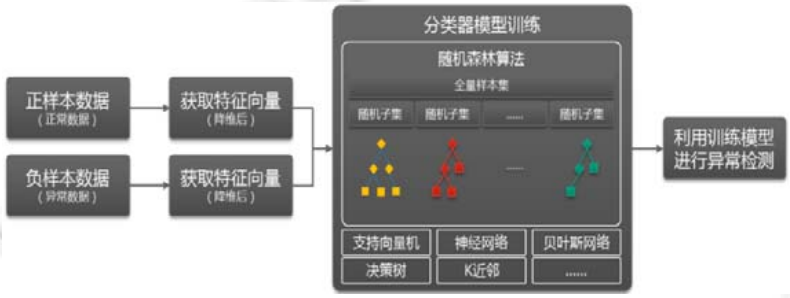


Fig.13 Supervised graph anomaly detection algorithm framework

图 13 有监督的图异常检测算法框架图

Fig.14 Unsupervised graph anomaly detection algorithm framework

图 14 无监督的图异常检测算法框架图

4.3 面向图异常检测的应用

随着信息化技术的发展,人们越来越重视信息安全,异常检测尤其是面向图的异常检测一直是学术界和工业界研究的热点.面向图的异常检测可以应用于社会生活的各个领域,如金融、互联网安全、社交关系挖掘、电信诈骗检测等等.面向图的异常检测的应用领域主要如下所列.

4.3.1 网络入侵检测

互联网将世界上任意角落的两个人通过网络连接起来,在为人们提供交流工具、为企业提供合作平台的同时,也为网络攻击者提供了攻击便利.利用图异常检测技术,对正常的网络行为和访问方式建模,可以高效地识别并阻止网络或者系统攻击(如攻击者通过 0day 漏洞攻击、DDoS 攻击、系统提权攻击、数据访问恶意攻击、未授权访问系统或者恶意软件等等).Animesh 等人[3]对使用异常检测方法检测网络入侵的类型、检测框架、方法分类等等进行了总结归纳.Akoglu 等人[62]使用基于图的异常检测技术查找电子邮件通联网络中的重要节点与可疑节点.Tong 和 Lin[14]的工作可以应用于端口扫描检测以及 DDoS 攻击分析.Yu 等人[63]提出了基于随机游走的 SybilGuard 算法,可以用于女巫攻击检测.Liu[64]等人使用异常检测技术检测软件漏洞.在点到点网络中,女巫攻击是一种常见的网络问题,一个女巫恶意节点声称自己具有多重身份,可以使存储在多个节点上的文件最后仅存储在一个节点上,节点的退出导致文件存储失效.在网络中,恶意节点有很多女巫身份,网络中会存在最小商割,即一部分边(攻击者和信任者之间的关系)的移除,使得网络的大部分节点和剩余节点是不连通的,而正常的网络中不存在这种割.SybilGuard 使用一种随机游走的变种算法,在信任节点上多次重复执行随机游走算法,多个游走路径的交点到起点之间的节点是可信任的.这是因为,通过信任节点构成的路径会以较大的概率还在信任区内,最后可以找到所有的信任区节点,从而进行女巫攻击检测.

4.3.2 电信网络异常检测

对电信服务提供者来说,使用基于图的异常检测技术,可以对电信网络节点异常流量进行检测和管理,同时提高电信网络的鲁棒性和抗攻击性,避免骨干节点的瘫痪而导致整个网络的通信中断.对电信服务使用者来说,图异常检测技术可以识别通联网络中的广告推手、电信网络欺诈,查找异常的通联时间节点以及异常的电话通联群组.如:Akoglu 等人[39]使用动态图异常检测技术,基于短信收发网络,研究个体异常的时间周期(如短信接收规律的改变);Prakash 等人[29]使用谱分析技术识别电信网络中的群组的变化;Chouiekh 等人[20]使用有监督学习的方法,利用电话通联网络中用户通话的详细信息进行正常用户与异常用户的分类;Prakash[29]使用邻接矩阵划分的方法检测可疑电话行为.

4.3.3 社交网络异常检测

社交网络中存在很多通过软件批量生成的僵尸账号以及垃圾信息传播账号,该类账号可以模拟正常的用户行为,如发消息、关注可信账号等.该类账号可为某些账号提供增粉、广告推销、活动推广、虚假商品评论等等服务,为攻击者赚取巨大利益,并给正常用户的账户隐私、使用体验等造成威胁.使用图异常检测技术识别社交网络中的异常账号,是当前学术界和工业界一直关注的热点问题.

对于社交网络中的异常账号,Aggarwal[65]提出的 CatchSync 算法利用节点的结构相似度来加以检测.CatchSync 的主要思想是:社交网络中的异常账号有很多同步的行为,如这些可疑节点需要同时执行某些任务,必须关注某些指定的账号.同时,这些节点的连接特点也不同于网络的其他节点.CatchSync 提出了同步度量和正常度度量方法,然后根据每一个节点计算节点的同步度与正常度,最后将整个网络图的同步度和正常度采用图表方式加以展示.使用基于距离的方法,将偏离大部分节点的具有较高同步度和较低正常度的节点认定为异常节点.Henderson 提出的 Rolx[66]根据节点的结构信息给节点确定一个角色,如团体成员节点、外围节点等,为节点的分类和节点相似性计算提供了新的计量方法,该方法可用于社交网络任务角色分类.

针对虚假评论检测,图异常检测也有很多应用.一般商品评论使用二部图进行网络建模,Hooi 等人[67]提出了在二部图上进行异常检测的算法 Fraudar,该算法给出了一个新的可疑度度量,并给出了在图中无法检测异常的理论上限.Akoglu[68]针对以往的启发式算法需要先验知识的缺点提出无监督的方法 FRAUDEAGLE,该算法可以用于用户商品评价欺诈检测,同时还可以使用网络评论的评分信息和感情信息.算法包含两个步骤:对用户进行打分和欺诈检测.算法不使用评价的文本语义,只使用评价的情感信息,如评价是正面的还是负面的,以此将观点欺诈问题转换为网络分类问题而加以解决.

图异常检测技术还可用于社交网络谣言的检测,如 Zhang 等人[23]通过训练的模型来识别正常的用户和谣言制造者.

4.3.4 金融异常检测

金融异常主要是指金融欺诈,主要包括如下几种类型:(1) 伪造身份信息,获取不当利益,或者享受免费服务,如使用伪造的标识信息、认证信息、地址信息等办理银行卡或信息卡,违规获取利益;(2) 克隆他人信息,获取他人财产或享受他人应有的服务;(3) 捏造信息,通过相关途径使非法利益合法,如洗钱行为.图异常检测技术在金融领域有着大量的应用,如通过图中回路识别洗钱行为、通过图的对应关系检测冒用行为.如:NetProbe 算法[69]使用马尔可夫随机场(MRF)对用户和交易进行建模并查找欺诈用户,同时使用信任传播算法检测欺诈者.

本文将图异常检测技术应用进行了分类汇总,见表 1.

Table 1 Summary table of graph anomaly detection technologys' application

表 1 图异常检测技术应用分类汇总表

应用领域	相关工作
网络入侵检测	Refs.[3,4,14,35,55,64,70−72]
电信网络异常检测	Refs.[29,39,44,49,71,73,74]
社交网络异常检测	Refs.[12,13,18,23,33,46,62,63,69,75−83]
金融异常检测	Refs.[84,85]

4.4 面向图的异常检测的数据集与评估方法

4.4.1 面向图的异常检测数据集类型

面向图的异常检测方法需要对应的数据集来验证方法的有效性和方法的性能,而在当前的研究中,绝大多数数据集都没有可信的数据标签,而且在进行异常标注任务时也具有一定的挑战性,有监督的机器学习算法也难以使用标注数据进行训练.因此,当前异常检测方法数据集按照生成方式主要分为如下 3 类:(1) 按照分布规律生成的模拟数据;(2) 真实的数据以及模拟数据形成的合成数据;(3) 真实的带标注的数据.

对于全部模拟数据集,一般使用模拟分布与随机生成相结合的方法,模拟分布规律形成的数据为正常数据(如模拟社交网络数据需要满足幂律分布规律),随机生成的数据为异常数据.Kagan 等人在文献[86]中的算法 2 提出了模拟真实数据分布的算法过程,SNAP 平台中也有模拟生成数据的具体算法实现.

半合成数据集使用真实数据作为正常数据,使用随机生成策略生成数据作为异常数据.真实带标注的数据分为两种类型:第 1 种数据类型中包含是否是正常数据的标识,如信用卡欺诈检测数据集;第 2 种数据类型为数据可通过服务接口获取数据是否正常的信息,如在社交网络异常检测中,可以通过网络爬虫获取用户当前状态,如果用户主页无法访问则用户为异常用户,Twitter 和新浪微博的数据集都可以采用该方法来进行检测.由于面向图的异常检测数据集比较多,且很多数据集节点附加数据很少,因此我们将常用的图异常检测数据集的名称、类型、图说明信息、节点数目、边数据等信息进行了总结,并将 Twitter 和新浪微博异常账号验证代码一起开源在了 https://github. com/lizhong2613/GraphAnomalyDetectionDatasets 上.

图异常检测技术应用于不同的领域,所面临的图数据的模型是不同的,原始数据按照模型组成可以分为两种类型:同质网络数据集与异质网络数据集.异质网络将原始问题抽象成由不同类型的节点和不同类型的链接构成的网络,同质网络中节点的类型和链接的类型是相同的.如在 Twitter 社交网络中,节点都对应于一个用户账户,节点之间的关系是关注关系;而在 Yelp 数据集中,节点包含了商品和用户账号两种类型,账号和商品之间的关系是评论关系.

在以往工作中,常用的同质网络数据集主要包括 Twitter、新浪微博、Academia.edu、Boys' Friendship、ArXiv、DBLP 数据集.常用的异质网络数据集有 Flixster、Yelp、douban 等.

4.4.2 面向图的异常检测算法性能评估方法

面向图的异常检测算法的目标是,从给定的数据集中查找出异常数据.传统的图异常检测方法侧重于算法的有效性以及算法的时间复杂度.由于近年来计算机算力的提升以及云计算等技术的出现,图异常检测更加注重算法识别效果(尤其是神经网络类算法训练过程需要大量时间不断迭代优化模型).一般情况下,算法会给出一个异常度的定义,每个节点或边按照分类器或可疑度计算公式获得可疑度,在用户给定阈值的情况下,按照降

序给出数据集中的异常数据.当前,图的异常检测算法的评估利用二分类算法的评估方法说明算法的性能,主要采用如下指标.

(1) TPR:在所有实际为正的样本中,被正确地判断为正样本的比率,该指标越高越好;

(2) FPR:在所有实际为负的样本中,被错误地判断为正样本的比率,该指标越低越好;

(3) Precision:原本为正例的样本占预测为正样本的比率,该指标越高越好;

(4) AUC:AUC 指标为 ROC 曲线下面积,ROC 曲线由 TPR 和 FPR 计算得到,该指标越高越好.

4.5 小 结

本节从图异常检测算法的关键技术、常用框架分类、详细应用领域、常用数据集以及评估方法等几个角度出发,对图异常检测进行归纳整理,便于读者对图异常检测问题有全面和详细的了解.

5 总结与展望

面向图的异常检测是对图数据进行数据挖掘的一个主要应用,也一直是学者们的研究热点.随着互联网的发展,图规模越来越大,复杂性越来越高,新技术的发展也为面向图的异常检测提供了理论基础,如张量分解技术、网络嵌入技术以及图卷积技术等.然而,异常类型的不同,使用的方法也不同,达到的效果也不同,本节将对面向图的异常检测技术进行总结,并对未来的发展方向加以展望.

5.1 面向图的异常检测方法分类对比

异常检测方法的分类汇总可见表 2.

Table 2 Classification summary table of graph anomaly detection technology

表 2 异常检测方法分类汇总表

类别	子类	方法种类	方法描述	方法优点	方法缺点
静态图	孤立个体异常检测	基于结构的方法	利用网络结构特征的方法和基于结构相似度的方法:第 1 种方法是总结已有正常网络的特征;第 2 种方法是通过图的结构计算节点的临近度,并以此判断节点的异常性	利用网络的结构特征,便于计算,可解释性强	没有考虑节点本身属性信息,只能应用于同质网络,难以总结高维特征
		基于社团的方法	使用群体检测的方法,将距离比较近的节点归为一个群体,那些连接各个群体却不属于各个群体的节点或者边为异常个体	可解释性强,可利用不同的社团检测算法	网络规模大,变化快,社团检测结果变化快
		基于信任传播的方法	每个节点的重要性和可靠性不同,并通过边进行传播	可扩展性强,可以找到前 k 个重要节点	一般需要先验知识
		基于信息论的方法	利用 MDL 检测导致编码长度异常增加的个体	可解释性强	无应用于群体异常和动态图异常检测的工作
		基于神经网络的方法	有监督的方法使用标签数据训练分类器,利用分类器进行判断;无监督的方法使用编码器与解码器模型,使用重建误差进行异常检测	自动化特征工程,不需要提取特征	可解释性差,计算复杂度高
静态图	群体异常检测	基于谱分析的方法	利用图谱理论,利用特征值和特征向量表示数据	利用谱分析进行降维	需先计算特征值和特征向量,需确定主特征个数
		基于稠密子图的方法	查找网络中最稠密的前 k 个子图	时间复杂度低,可扩展性强	结果存在偏差,异常数据中存在正常数据

Table 2 Classification summary table of graph anomaly detection technology (Continued)

表 2 异常检测方法分类汇总表(续)

类别	子类	方法种类	方法描述	方法优点	方法缺点
静态图	群体异常检测	基于张量检测的方法	利用多模数据进行建模,具有更高的信息表示能力,并结合张量分解技术进行降维和异常检测	可以处理高维的数据	需占用较多的内存空间
		基于多层贝叶斯模型的方法	使用概率分布创建一个数据的生成模型,并将那些相对不是模型生成的数据认为是异常数据	生成方法灵活,可进行聚合运算	模型假设分布为多维高斯分布,其他分布不适用
动态图	孤立个体异常检测	基于偏差的方法	定义距离的度量方式,使用聚类方法查找偏差较大的数据	便于计算,距离具有可解释性	结果依赖于距离的定义公式的好坏
		基于社区的方法	追踪网络社区随着时间的推进社区变化以及社区组成节点的关系变化的过程,查找和大多数个体不同的个体	根据变化的社区查找异常个体	算法结果依赖于不同时刻的社团对应方法
		基于分解的方法	利用张量分解对高维数据进行分析	可处理高维数据	需要指定分解张量的阶,检测结果依赖于选择的阶
	异常群体检测	基于社团检测的方法	追踪社团的变化,识别没有保持稳定性的社团	根据社团变化情况查找异常群体,可解释性强	算法结果依赖于不同时刻的社团对应方法
		基于分解的方法	利用张量分解对高维数据进行分析	可处理高维数据,对噪声鲁棒,不破坏原数据的空间结构	需要指定分解张量的阶,检测结果依赖于选择的阶
	事件异常检测	基于分解的方法	利用张量分解对高维数据进行分析	可处理高维数据	需要指定分解张量的阶
		基于距离的方法	定义一个距离度量函数,利用滑动窗口计算平均值或者查找前 k 个偏差比较大的值对应的时刻	可解释性强,定义距离后可集合多种方法进行异常检测	算法结果的好坏依赖于距离的定义方法
		基于神经网络的异常事件检测方法	利用历史数据进行训练,利用预测数据与真实数据之间的偏差进行异常检测	可处理时间序列数据	可解释性差

5.2 面向图的异常检测的挑战

近年来,面向图的异常检测受到了越来越多学者的关注,尽管新的研究方法和研究成果不断涌现,当前的异常检测研究还处于学术研究阶段,面向图的异常检测仍然面临很多挑战,主要如下:

(1) 真实的异常数据不够全面、规范.很多异常算法能够查找出与其他大多数生成形式不同的数据,但是在诸多应用中,很少有确定的异常数据,并且有标注的数据少之又少.异常数据和噪声数据同时存在于原始数据中,不能有效地使用有监督的机器学习方法进行模型训练,检测模型训练难,结果验证难度大,识别结果存在偏差;

(2) 算法有效性与算法可扩展性的结合较为困难.随着通信技术以及计算机技术的发展,当前网络的规模越来越大,网络中的节点数以亿计,优化结果搜索空间大;并且随着网络的变化,搜索空间呈指数级增长,网络变化频率快,异常业务场景也具有动态性.如在金融欺诈和网络欺诈中,算法并不是一成不变的,随着模型的升级,欺诈者也会针对模型进行攻击,导致模型需要不断更新,一些传统的方法无法应用于大规模网络,甚至于节点关系的邻接矩阵无法加载到内存中.算法除了有效性,必须有较好的可扩展性和经济性,可用于大规模图计算;

(3) 网络内容属性与结构属性的结合应用.除了网络的规模较大以及变化频率快的特点,网络中内容的信息也越来越多元化,如社交网络中用户评论的内容、用户的兴趣、用户的个人信息、发表的观点、所处的地理位置等等,充分利用网络的多元信息进行异常检测充满挑战;

(4) 异常检测的可解释性.异常检测模型难以给出异常实例的根本原因以及异常产生的原因,使用直观性高、交互性强的工具进行辅助,如使用图表、动画的形式进行研判,这方面的工作更少.

5.3 展 望

综上所述,图异常检测问题的建模与应用得到了学术界和工业界的广泛关注,随着云计算、神经网络的蓬勃发展,利用强大的计算能力,全面考虑网络的结构性信息和内容性信息,构建智能化的异常检测模型的需求越来越强烈.尤其是异常检测根据不同的应用领域,采用的模型和方法差异性大、业务导向性强、模型不确定性强等诸多挑战将推动异常检测的研究向纵深方向不断发展.未来的研究方向主要包括以下几个方面.

(1) 结合自然语言处理技术,全面融合网络的结构信息、标签信息和内容信息,构建充分利用多维度信息的异常检测方法.当前的异常检测方法主要利用了节点或边的结构信息和属性信息,只是利用了部分特征信息,但只有很少的工作会考虑内容信息.如随着社交网络、电商平台的发展,网络承载的观点也越来越多.如何充分利用内容信息,结合越来越成熟的自然语言处理技术,或者是图神经网络技术,将是未来的发展方向;

(2) 自动化特征提取技术与异常检测的结合.现有的一些异常检测方法利用专家知识,通过大量的数据分析提取网络特征,分析研判异常数据与正常数据的特征实现异常检测.该方法规范性差,效率低.利用深度神经网络,自动提取网络低维度特征与高维特征,构建识别器或者异常检测辅助工具,将是未来的发展方向;

(3) 图异常检测的可解释性研究.目前,对各种异常检测方法的可解释性工作是相当少的,除了以往基于特征的异常检测方法外,其他方法侧重于算法的高效性和可扩展性上的比较;而且实际生活中,真正的异常数据本来就很难获取.未来的研究可以利用更加泛化的异常描述方法,解释异常实例的特殊性成因,并结合可视化技术,让分析结果更加清晰;

(4) 模型训练优化以及预测结果优化.未来的异常检测模型能够利用的特征与信息会很多,结果的准确率也会越来越高,模型训练和模型调参的时间成本将会不断增加.如何利用精简模型获取较高的模型性能,或者利用网络压缩的方法提高算法的效率,是下一步的研究方向.

References:

[1] Moonesinghe HDK, Tan PN. Outrank: A graph-based outlier detection framework using random walk. Int'l Journal on Artificial Intelligence Tools, 2008,17(1):19−36.

[2] Guo JY, Li RH, Zhang Y, Wang GR. Graph neural network based anomaly detection in dynamic networks. Ruan Jian Xue Bao/Journal of Software, 2020,31(3):748−762 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5903.htm [doi: 10.13328/j.cnki.jos.005903]

[3] Akoglu L, Tong H, Koutra D. Graph based anomaly detection and description: A survey. Data Mining and Knowledge Discovery, 2015,29(3):626−688.

[4] Gogoi P, Bhattacharyya DK, Borah B, *et al*. A survey of outlier detection methods in network anomaly identification. The Computer Journal, 2011,54(4):570−588.

[5] Gupta M, Gao J, Aggarwal CC, *et al*. Outlier detection for temporal data: A survey. IEEE Trans. on Knowledge and Data Engineering, 2014,26(9):2250−2267.

[6] Ranshous S, Shen S, Koutra D, *et al*. Anomaly detection in dynamic networks: A survey. Wiley Interdisciplinary Reviews: Computational Statistics, 2015,7(3):223−247.

[7] Yu R, Qiu H, Wen Z, *et al*. A survey on social media anomaly detection. ACM SIGKDD Explorations Newsletter, 2016,18(1):1−14.

[8] Zhang YQ, Lv SQ, Fan D. Anomaly detection in online social networks. Chinese Journal of Computers, 2015,10:2011−2027 (in Chinese with English abstract).

[9] Mao JL, JinCQ, Zhang ZG, Zhou AY. Anomaly detection for trajectory big data: Advancements and framework. Ruan Jian Xue Bao/Journal of Software, 2017,28(1):17−34 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5151.htm [doi: 10.13328/j.cnki.jos.005151]

[10] Mo Q, Yang K. Overview of Web spammer detection. Ruan Jian Xue Bao/Journal of Software, 2014,25(7):1505−1526 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4617.htm [doi: 10.13328/j.cnki.jos.004617]

[11] Akoglu L, McGlohon M, Faloutsos C. Oddball: Spotting anomalies in weighted graphs. In: Proc. of the Pacific-Asia Conf. on Knowledge Discovery and Data Mining. Berlin, Heidelberg: Springer-Verlag, 2010. 410−421.

[12] Yu R, He X, Liu Y. Glad: Group anomaly detection in social media analysis. ACM Trans. on Knowledge Discovery from Data (TKDD), 2015,10(2):18.

[13] Xu X, Yuruk N, Feng Z, *et al*. Scan: A structural clustering algorithm for networks. In: Proc. of the 13th ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining. ACM, 2007. 824−833.

[14] Tong H, Lin CY. Non-negative residual matrix factorization with application to graph anomaly detection. In: Proc. of the 2011 SIAM Int'l Conf. on Data Mining. Society for Industrial and Applied Mathematics, 2011. 143−153.

[15] Gyöngyi Z, Garcia-Molina H, Pedersen J. Combating Web Spam with trustrank. In: Proc. of the 30th Int'l Conf. on Very Large Data Bases, Vol. 30. VLDB Endowment, 2004. 576−587.

[16] Wu B, Goel V, Davison BD. Topical trustrank: Using topicality to combat Web Spam. In: Proc. of the 15th Int'l Conf. on World Wide Web. ACM, 2006. 63−72.

[17] Shah N, Beutel A, Hooi B, *et al*. Edgecentric: Anomaly detection in edge-attributed networks. In: Proc. of the 16th IEEE Int'l Conf. on Data Mining Workshops (ICDMW). IEEE, 2016. 327−334.

[18] Chakrabarti D. Autopart: Parameter-free graph partitioning and outlier detection. In: Proc. of the European Conf. on Principles of Data Mining and Knowledge Discovery. Berlin, Heidelberg: Springer-Verlag, 2004. 112−124.

[19] Li HP, Hu ZY, Wu YH, Wu FC. Behavior modeling and abnormality detection based on semi-supervised learning method. Ruan Jian Xue Bao/Journal of Software, 2007,18(3):527−537 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/527.htm [doi: 10.1360/jos180527]

[20] Chouiekh A, Haj ELHIEL. ConvNets for fraud detection analysis. Procedia Computer Science, 2018,127:133−138.

[21] Alsheikh MA, Niyato D, Lin S, *et al*. Mobile big data analytics using deep learning and apache spark. IEEE Network, 2016,30(3):22−29.

[22] Cai RC, Xie WH, Hao ZF, Wang LJ, Wen W. Abnormal crowd detection based on multi-scale recurrent neural network. Ruan Jian Xue Bao/Journal of Software, 2015,26(11):2884−2896 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4893.htm [doi: 10.13328/j.cnki.jos.004893]

[23] Zhang Y, Chen W, Yeo CK, *et al*. Detecting rumors on online social networks using multi-layer autoencoder. In: Proc. of the 2017 IEEE Technology & Engineering Management Conf. (TEMSCON). IEEE, 2017. 437−441.

[24] Guan SP, JinXL, Jia YT, Wang YZ, Cheng XQ. Knowledge reasoning over knowledge graph: A survey. Ruan Jian Xue Bao/Journal of Software, 2018,29(10):2966−2994 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5551.htm [doi: 10. 13328/j.cnki.jos.005551]

[25] Castellini J, Poggioni V, Sorbi G. Fake Twitter followers detection by denoising autoencoder. In: Proc. of the Int'l Conf. on Web Intelligence. ACM, 2017. 195−202.

[26] Zenati H, Foo CS, Lecouat B, *et al*. Efficient GAN-based anomaly detection. arXiv Preprint arXiv: 1802.06222, 2018.

[27] Zou BY, Li CP, Tan LW, Chen H, Wang SQ. Social recommendations based on user trust and tensor factorization. Ruan Jian Xue Bao/Journal of Software, 2014,25(12):2852−2864 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4725.htm [doi: 10.13328/j.cnki.jos.004725]

[28] Von Luxburg U. A tutorial on spectral clustering. Statistics and Computing, 2007,17(4):395−416.

[29] Prakash BA, Sridharan A, Seshadri M, *et al*. Eigenspokes: Surprising patterns and scalable community chipping in large graphs. In: Proc. of the Pacific-Asia Conf. on Knowledge Discovery and Data Mining. Berlin, Heidelberg: Springer-Verlag, 2010. 435−448.

[30] Charikar M. Greedy approximation algorithms for finding dense components in a graph. In: Proc. of the Int'l Workshop on Approximation Algorithms for Combinatorial Optimization. Berlin, Heidelberg: Springer-Verlag, 2000. 84−95.

[31] Liu S, Hooi B, Faloutsos C. Holoscope: Topology-and-spike aware fraud detection. In: Proc. of the 2017 ACM on Conf. on Information and Knowledge Management. ACM, 2017. 1539−1548.

[32] Jiang M, Cui P, Beutel A, *et al*. Inferring strange behavior from connectivity pattern in social networks. In: Proc. of the Pacific-Asia Conf. on Knowledge Discovery and Data Mining. Cham: Springer-Verlag, 2014. 126−138.

[33] Shah N, Beutel A, Gallagher B, *et al*. Spotting suspicious link behavior with fbox: An adversarial perspective. In: Proc. of the 2014 IEEE Int'l Conf. on Data Mining (ICDM). IEEE, 2014. 959−964.

[34] Jiang M, Beutel A, Cui P, *et al*. A general suspiciousness metric for dense blocks in multimodal data. In: Proc. of the 2015 IEEE Int'l Conf. on Data Mining (ICDM). IEEE, 2015. 781−786.

[35] Shin K, Hooi B, Faloutsos C. M-Zoom: Fast dense-block detection in tensors with quality guarantees. In: Proc. of the Joint European Conf. on Machine Learning and Knowledge Discovery in Databases. Cham: Springer-Verlag, 2016. 264−280.

[36] Xiong L, Póczos B, Schneider J, *et al*. Hierarchical probabilistic models for group anomaly detection. In: Proc. of the 14th Int'l Conf. on Artificial Intelligence and Statistics. 2011. 789−797.

[37] Pincombe B. Anomaly detection in time series of graphs using arma processes. Asor Bulletin, 2005,24(4):2.

[38] Chen L, Zhu PS, Qian TY, Zhu H, Zhou J. Edge sampling based network embedding model. Ruan Jian Xue Bao/Journal of Software, 2018,29(3):756−771 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5435.htm [doi: 10.13328/j.cnki.jos.005435]

[39] Malhotra P, Vig L, Shroff G, *et al*. Long Short Term Memory Networks for Anomaly Detection in Time Series. Presses Universitaires de Louvain, 2015. 89.

[40] Gupta M, Gao J, Sun Y, *et al*. Community trend outlier detection using soft temporal pattern mining. In: Proc. of the Joint European Conf. on Machine Learning and Knowledge Discovery in Databases. Berlin, Heidelberg: Springer-Verlag, 2012. 692−708.

[41] Fu W, Song L, Xing EP. Dynamic mixed membership blockmodel for evolving networks. In: Proc. of the 26th Annual Int'l Conf. on Machine Learning. ACM, 2009. 329−336.

[42] Rossi RA, Gallagher B, Neville J, *et al*. Modeling dynamic behavior in large evolving graphs. In: Proc. of the 6th ACM Int'l Conf. on Web Search and Data Mining. ACM, 2013. 667−676.

[43] Yu W, Aggarwal CC, Ma S, *et al*. On anomalous hotspot discovery in graph streams. In: Proc. of the 13th IEEE Int'l Conf. on Data Mining (ICDM). IEEE, 2013. 1271−1276.

[44] Heard NA, Weston DJ, Platanioti K, *et al*. Bayesian anomaly detection methods for social networks. The Annals of Applied Statistics, 2010,4(2):645−662.

[45] Li X, Li Z, Han J, *et al*. Temporal outlier detection in vehicle traffic data. In: Proc. of the IEEE Int'l Conf. on Data Engineering. IEEE, 2009. 1319−1322.

[46] Abello J, Eliassi-Rad T, Devanur N. Detecting novel discrepancies in communication networks. In: Proc. of the 10th IEEE Int'l Conf. on Data Mining (ICDM). IEEE, 2010. 8−17.

[47] Greene D, Doyle D, Cunningham P. Tracking the evolution of communities in dynamic social networks. In: Proc. of the 2010 Int'l Conf. on Advances in Social Networks Analysis and Mining (ASONAM). IEEE, 2010. 176−183.

[48] Chen Z, Hendrix W, Samatova NF. Community-based anomaly detection in evolutionary networks. Journal of Intelligent Information Systems, 2012,39(1):59−85.

[49] Araujo M, Papadimitriou S, Günnemann S, *et al*. Com2: Fast automatic discovery of temporal ('comet') communities. In: Proc. of the Pacific-Asia Conf. on Knowledge Discovery and Data Mining. Cham: Springer-Verlag, 2014. 271−283.

[50] Koutra D, Papalexakis EE, Faloutsos C. Tensorsplat: Spotting latent anomalies in time. In: Proc. of the 16th Panhellenic Conf. on Informatics (PCI). IEEE, 2012. 144−149.

[51] Papalexakis EE, Faloutsos C, Sidiropoulos ND. Parcube: Sparse parallelizable tensor decompositions. In: Proc. of the Joint European Conf. on Machine Learning and Knowledge Discovery in Databases. Berlin, Heidelberg: Springer-Verlag, 2012. 521−536.

[52] Sun J, Xie Y, Zhang H, *et al*. Less is more: Compact matrix decomposition for large sparse graphs. In: Proc. of the 2007 SIAM Int'l Conf. on Data Mining. Society for Industrial and Applied Mathematics, 2007. 366−377.

[53] Jiang R, Fei H, Huan J. Anomaly localization for network data streams with graph joint sparse PCA. In: Proc. of the 17th ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining. ACM, 2011. 886−894.

[54] Zhu YW, Yang JH, Zhang JX. Anomaly detection based on traffic information structure. Ruan Jian Xue Bao/Journal of Software, 2010,21(10):2573−2583 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3698.htm [doi: 10.3724/SP.J.1001.2010.03698]

[55] Fu PG, Hu XH. Anomaly detection algorithm based on the local distance of density-based sampling data. Ruan Jian Xue Bao/Journal of Software, 2017,28(10):2625−2639 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5134.htm [doi: 10.13328/j.cnki.jos.005134]

[56] Berlingerio M, Koutra D, Eliassi-Rad T, *et al*. Netsimile: A scalable approach to size-independent network similarity. arXiv Preprint arXiv: 1209.2684, 2012.

[57] Soundarajan S, Eliassi-Rad T, Gallagher B. Which network similarity measure should you choose: An empirical study. In: Proc. of the Workshop on Information in Networks. New York, 2013.

[58] Guo T, Xu Z, Yao X, *et al*. Robust online time series prediction with recurrent neural networks. In: Proc. of the 2016 IEEE Int'l Conf. on Data Science and Advanced Analytics (DSAA). IEEE, 2016. 816−825.

[59] Bontemps L, McDermott J, Le-Khac NA. Collective anomaly detection based on long short-term memory recurrent neural networks. In: Proc. of the Int'l Conf. on Future Data and Security Engineering. Cham: Springer-Verlag, 2016. 141−152.

[60] Malhotra P, Ramakrishnan A, Anand G, *et al*. LSTM-based encoder-decoder for multi-sensor anomaly detection. arXiv Preprint arXiv: 1607.00148, 2016.

[61] Li D, Chen D, Goh J, *et al*. Anomaly detection with generative adversarial networks for multivariate time series. arXiv Preprint arXiv: 1809.04758, 2018.

[62] Akoglu L, Tong H, Vreeken J, *et al*. Fast and reliable anomaly detection in categorical data. In: Proc. of the 21st ACM Int'l Conf. on Information and Knowledge Management. ACM, 2012. 415−424.

[63] Yu H, Kaminsky M, Gibbons PB, *et al*. Sybilguard: Defending against Sybil attacks via social networks. ACM SIGCOMM Computer Communication Review, 2006,36(4):267−278.

[64] Liu C, Yan X, Yu H, *et al*. Mining behavior graphs for "backtrace" of noncrashing bugs. In: Proc. of the 2005 SIAM Int'l Conf. on Data Mining. Society for Industrial and Applied Mathematics, 2005. 286−297.

[65] Aggarwal CC. Outlier detection in graphs and networks. In: Proc. of the Outlier Analysis. Cham: Springer-Verlag, 2017. 369−397.

[66] Henderson K, Gallagher B, Eliassi-Rad T, *et al*. Rolx: Structural role extraction & mining in large graphs. In: Proc. of the 18th ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining. ACM, 2012. 1231−1239.

[67] Hooi B, Song HA, Beutel A, *et al*. Fraudar: Bounding graph fraud in the face of camouflage. In: Proc. of the 22nd ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining. ACM, 2016. 895−904.

[68] Akoglu L, Chandy R, Faloutsos C. Opinion fraud detection in online reviews by network effects. ICWSM, 2013,13:2−11.

[69] Pandit S, Chau DH, Wang S, *et al*. Netprobe: A fast and scalable system for fraud detection in online auction networks. In: Proc. of the 16th Int'l Conf. on World Wide Web. ACM, 2007. 201−210.

[70] Yu H, Gibbons PB, Kaminsky M, *et al*. Sybillimit: A near-optimal social network defense against Sybil attacks. In: Proc. of the 2008 IEEE Symp. on Security and Privacy (SP 2008). IEEE, 2008. 3−17.

[71] Sun J, Faloutsos C, Faloutsos C, *et al*. Graphscope: Parameter-free mining of large time-evolving graphs. In: Proc. of the 13th ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining. ACM, 2007. 687−696.

[72] Noble CC, Cook DJ. Graph-based anomaly detection. In: Proc. of the 9th ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining. ACM, 2003. 631−636.

[73] De Melo POSV, Akoglu L, Faloutsos C, *et al*. Surprising patterns for the call duration distribution of mobile phone users. In: Proc. of the Joint European Conf. on Machine Learning and Knowledge Discovery in Databases. Berlin, Heidelberg: Springer-Verlag, 2010. 354−369.

[74] Fischer G. Communities of interest: Learning through the interaction of multiple knowledge systems. In: Proc. of the 24th IRIS Conf. 2001. 1−13.

[75] Hooi B, Shah N, Beutel A, *et al*. Birdnest: Bayesian inference for ratings-fraud detection. In: Proc. of the 2016 SIAM Int'l Conf. on Data Mining. Society for Industrial and Applied Mathematics, 2016. 495−503.

[76] Sun H, Huang J, Han J, *et al*. Gskeletonclu: Density-based network clustering via structure-connected tree division or agglomeration. In: Proc. of the 10th IEEE Int'l Conf. on Data Mining (ICDM). IEEE, 2010. 481−490.

[77] Rattigan MJ, Jensen D. The case for anomalous link discovery. ACM SIGKDD Explorations Newsletter, 2005,7(2):41−47.

[78] Aggarwal CC, Zhao Y, Philip SY. Outlier detection in graph streams. 2011. [doi: 10.1109/ICDE.2011.5767885]

[79] Shiokawa H, Fujiwara Y, Onizuka M. SCAN++: Efficient algorithm for finding clusters, hubs and outliers on large-scale graphs. Proc. of the VLDB Endowment, 2015,8(11):1178−1189.

[80] Gupta M, Gao J, Sun Y, *et al*. Integrating community matching and outlier detection for mining evolutionary community outliers. In: Proc. of the 18th ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining. ACM, 2012. 859−867.

[81] Cao Q, Sirivianos M, Yang X, *et al*. Aiding the detection of fake accounts in large scale social online services. In: Proc. of the 9th USENIX Conf. on Networked Systems Design and Implementation. USENIX Association, 2012. 15.

[82] Jiang M, Cui P, Beutel A, *et al*. Catching synchronized behaviors in large networks: A graph mining approach. ACM Trans. on Knowledge Discovery from Data (TKDD), 2016,10(4):35.

[83] Akhter MI, Ahamad MG. Detecting telecommunication fraud using neural networks through data mining. Int'l Journal of Scientific and Engineering Research, 2012,3(3):601−606.

[84] Boden B, Günnemann S, Hoffmann H, *et al*. RMiCS: A robust approach for mining coherent subgraphs in edge-labeled multi-layer graphs. In: Proc. of the 25th Int'l Conf. on Scientific and Statistical Database Management. ACM, 2013. 23.

[85] Yang B, Cao J, Ni R, *et al*. Anomaly detection in moving crowds through spatiotemporal autoencoding and additional attention. In: Proc. of the Advances in Multimedia. 2018.

[86] Kagan D, Elovichi Y, Fire M. Generic anomalous vertices detection utilizing a link prediction algorithm. Social Network Analysis and Mining, 2018,8(1):27.

附中文参考文献:

[2] 郭嘉琰,李荣华,张岩,王国仁.基于图神经网络的动态网络异常检测算法.软件学报,2020,31(3):748−762. http://www.jos.org.cn/1000-9825/5903.htm [doi: 10. 13328/j.cnki.jos.005903]

[8] 张玉清,吕少卿,范丹.在线社交网络中异常帐号检测方法研究.计算机学报,2015,10:2011−2027.

[9] 毛嘉莉,金澈清,章志刚,周傲英.轨迹大数据异常检测:研究进展及系统框架.软件学报,2017,28(1):17−34. http://www.jos.org.cn/1000-9825/5151.htm [doi: 10.13328/j.cnki.jos.005151]

[10] 莫倩,杨珂.网络水军识别研究.软件学报,2014,25(7):1505−1526. http://www.jos.org.cn/1000-9825/4617.htm [doi: 10.13328/j.cnki.jos.004617]

[19] 李和平,胡占义,吴毅红,吴福朝.基于半监督学习的行为建模与异常检测.软件学报,2007,18(3):527−537. http://www.jos.org.cn/1000-9825/18/527.htm [doi: 10.1360/jos180527]

[22] 蔡瑞初,谢伟浩,郝志峰,王丽娟,温雯.基于多尺度时间递归神经网络的人群异常检测.软件学报,2015,26(11):2884−2896. http://www.jos.org.cn/1000-9825/4893.htm [doi: 10.13328/j.cnki.jos.004893]

[24] 官赛萍,靳小龙,贾岩涛,王元卓,程学旗.面向知识图谱的知识推理研究进展.软件学报,2018,29(10):2966−2994. http://www.jos.org.cn/1000-9825/5551.htm [doi: 10. 13328/j.cnki.jos.005551]

[27] 邹本友,李翠平,谭力文,陈红,王绍卿.基于用户信任和张量分解的社会网络推荐.软件学报,2014,25(12):2852−2864. http://www.jos.org.cn/1000-9825/4725.htm [doi: 10.13328/j.cnki.jos.004725]

[38] 陈丽,朱裴松,钱铁云,朱辉,周静.基于边采样的网络表示学习模型.软件学报,2018,29(3):756−771. http://www.jos.org.cn/1000-9825/5435.htm [doi: 10.13328/j.cnki.jos.005435]

[56] 朱应武,杨家海,张金祥.基于流量信息结构的异常检测.软件学报,2010,21(10):2573−2583. http://www.jos.org.cn/1000-9825/3698.htm [doi: 10.3724/SP.J.1001.2010.03698]

[57] 付培国,胡晓惠.基于密度偏倚抽样的局部距离异常检测方法.软件学报,2017,28(10):2625−2639. http://www.jos.org.cn/1000-9825/5134.htm [doi: 10.13328/j.cnki.jos.005134]

李忠(1987－),男,博士生,工程师,主要研究领域为社交网络计算,网络异常检测,知识图谱.

庄传志(1985－),男,博士生,工程师,CCF学生会员,主要研究领域为自然语言处理,知识图谱.

靳小龙(1976－),男,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为知识图谱,社会计算,大数据.

孙智(1985－),男,博士生,主要研究领域为图异常检测,知识图谱.