小 型 微 型 计 算 机 系 统
Journal of Chinese Computer Systems
DOI:10.20009/j.cnki.21-1106/TP.2025-0194
2026 年 2 月 第 2 期
Vol.47 No.2 2026

面向主动学习的异常检测方法:现状与展望

赵海燕[1],吴思雨[1],曹 健[2],陈庆奎[1]

[1](上海理工大学 光电信息与计算机工程学院 上海市现代光学系统重点实验室 光学仪器与系统教育部工程研究中心,上海 200093)
[2](上海交通大学 计算机科学与技术系,上海 200030)
E-mail:cao-jian@sjtu.edu.cn

摘 要: 随着异常检测技术在网络安全、金融风控以及医疗诊断等众多领域的广泛应用,如何应对标注数据成本高昂以及误报率居高不下等问题,正变得愈发关键.在此背景下,主动异常检测应运而生,它借助交互学习框架,致力于降低误报率并提升检测性能.本文深入剖析了异常检测以及主动异常检测,系统阐释了主动异常检测的构成要素,并着重强调了其在削减数据标注成本以及减少误报发生频率方面的重要意义.此外,本文还从异常分类器、主动数据选择策略以及反馈信息的利用这三重视角,对主动异常检测方法进行了分类.最后,论文深入剖析了主动异常检测所面临的挑战,并为其未来的发展方向提出了研究方向和思路.

关 键 词: 主动异常检测;主动学习;深度学习;反馈信息
中图分类号: TP391 **文献标识码:** A **文 章 编 号:** 1000-1220(2026)02-0361-09

Active Anomaly Detection Approaches: Current Status and Prospects

ZHAO Haiyan[1], WU Siyu[1], CAO Jian[2], CHEN Qingkui[1]

[1](Shanghai Key Lab of Modern Optical System, Engineering Research Center of Optical Instrument and System, Ministry of Education, University of Shanghai for Science and Technology, Shanghai 200093, China)
[2](Department of Computer Science and Technology, Shanghai Jiao Tong University, Shanghai 200030, China)

Abstract: With the widespread application of anomaly detection technology in domains such as financial risk control, network security, and medical diagnosis, addressing issues like the high cost of labeled data and elevated false-positive rates has become increasingly crucial. In response to these challenges, active anomaly detection has emerged as an effective solution aimed at reducing false positive rates and enhancing detection performance through an intelligent interactive learning framework. This paper provides an in-depth exploration of anomaly detection and active anomaly detection, systematically elucidating the components of the latter and highlighting its significance in minimizing data labeling costs and the occurrence of false alarms. Furthermore, the paper categorizes active anomaly detection methods from three perspectives: anomaly classifiers, active data selection strategies, and the utilization of feedback information. Finally, the paper analyzes the challenges encountered in active anomaly detection and proposes innovative directions for its future progression.

Keywords: active anomaly detection; active learning; deep learning; feedback information

0 引 言

异常检测的目的是识别偏离预期行为的数据模式[1].一方面,传统异常检测技术通常依赖静态模型,导致其难以快速响应新出现的异常模式或数据漂移等变化.另一方面,在实际应用场景中获取完整的标注数据其成本往往过高且不切实际.

为解决这些问题,主动异常检测(Active Anomaly Discovery, AAD)[2]应运而生.其作为机器学习与异常检测交叉领域的重要分支,通过集成主动学习技术,优先标注数据集中信息量最大的样本融入专家反馈,不仅能够适应动态变化的数据环境,还能更精准地捕捉异常特征.主动异常检测其应用领域涵盖金融欺诈检测[3]、网络安全[4]、工业监测[5]、移动通信[6]和天文观测[7,8]等多个领域.相关研究[9-11]中主要关注于主动查询策略和深度主动学习异常检测.本文从传统模型和深度学习模型角度梳理其主动异常检测框架,分析主动查询策略如何协同专家反馈策略及反馈信息整合优化模型.

本文旨在先全面总结主动异常检测方法体系,然后系统梳理异常分类器、数据选择策略和反馈策略.最后剖析当前研究痛点并提出未来创新方向.

1 主动异常检测定义

主动异常检测源于机器学习与数据挖掘领域,旨在使用专家标记的少量标记样本通过增量学习迭代地提升模型性能[12].

收稿日期:2025-05-09 收修改稿日期:2025-06-11 基金项目:上海市科委创新计划项目(22DZ1100103)资助. 作者简介:**赵海燕**,女,1975 年生,博士,副教授,CCF 会员,研究方向为服务计算、数据挖掘、推荐系统;**吴思雨**,女,2001 年生,硕士研究生,研究方向为主动异常检测;**曹 健**,男,1972 年生,博士,教授,博士生导师,CCF 杰出会员,研究方向为智能数据分析、服务计算、协同计算、网络计算等;**陈庆奎**,男,1967 年生,博士,教授,博士生导师,CCF 会员,研究方向为计算机集群、并行数据库、并行理论、物联网等.

1.1 异常类型

“异常”在不同应用场景中具有差异性定义,通常指显著偏离主流模式的数据实例,常被称为离群点或新颖性检测[13].在主动异常检测领域,主要存在三类异常,如图 1 所示:点异常即单个数据点显著偏离数据集整体分布;上下文异常为特定情境下表现异常;集体异常为个体正常但群体模式异常.

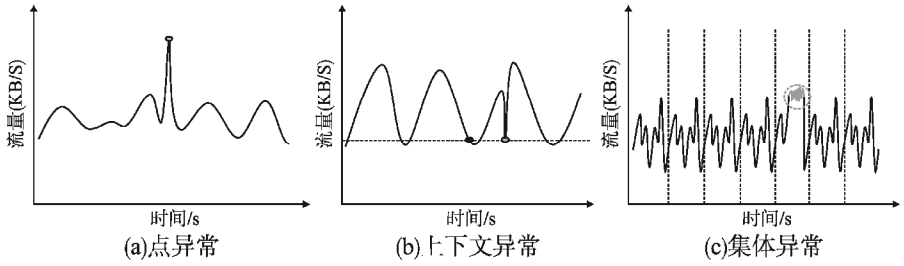

图 1 点异常、上下文异常、集体异常示例

Fig. 1 Examples of point anomaly, conditional anomaly, and collective anomaly

1.2 主动异常检测定义与模型

主动异常检测是一种融合主动学习框架的异常检测范式,其核心是通过主动学习方法来选择高信息量样本并利用反馈优化检测模型,实现在标注成本约束下异常检测精度与误报抑制效能的持续提升[14].如图 2 所示,展示了主动异常检测框架,其主动异常检测问题可以定义为:

1)训练数据:$D_{train}=\{X_i\}_{i=1}^{m}$,其中 $x_i\in\mathbb{R}^d$ 为原始特征向量.未标注样本集 u,少量标注样本 $S=\{X_k,y_k\}_{k=1}^{n}$,初始时 $n\ll m$,其中 $y_k\in\{0,1\}$(0 为正常,1 为异常).

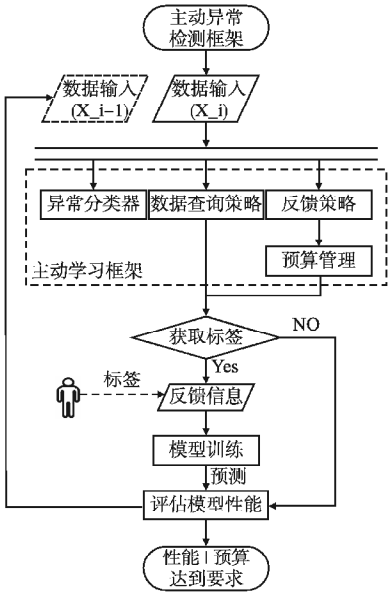

图 2 主动异常检测框架图

Fig. 2 Active anomaly detection framework diagram

2)模型定义:M_θ,通过学习参数 θ 使得异常样本被输出更高异常得分.

3)主动学习框架定义:B 为最大查询次数.每轮迭代选择信息量最大的样本 $X_t\in u$,$X_t=\arg\max_{X\in u}M_\theta(X)$.专家反馈标签 y_t,更新标注集合 $S\leftarrow S\cup\{(X_t,y_t)\}$.

4)损失函数:$L(S,M_\theta)$.

5)测试与评估:测试集为 $D_{test}=\{(X_j,y_j)\}_{j=1}^{n}$,$y_j$ 为样本标签.模型对测试集输出预测标签 $\hat{y}_j$,比较真实标签与预测标签进行评估模型性能.

主动学习系统包含两大核心组件:标注者和查询系统.标注者对查询提供响应,可能涉及专家反馈或其他标记方法.查询系统负责向标注者发起标签查询,面临选择数据实例进行标记的挑战,以优化学习性能和成本[15].

主动学习可以用于多种任务,其主要包含异常检测、多标签分类、图节点分类、流数据学习和多任务学习等.其中异常检测任务往往伴随着数据稀疏性、噪声敏感性和分布复杂性问题.为此,需采用查询策略通过结合半监督学习深度结合以应对标注不确定性.对比之下,多标签分类、图学习侧重于标签间复杂相关性和利用任务内在结构来优化样本选择.

文献[16]提出了一种半监督算法,将主动学习和子空间聚类相结合,并与专家用户交互以获取语义信息,从而识别相关的异常.其算法体现了初期主动异常检测框架的流程.文献[2]改进了其方法并首次提出主动异常检测.其引入了一种通过整合专家反馈来调整异常检测器的方法,以便更准确地识别与专家语义理解一致的异常实例.近年来,深度主动学习[17-19]因其在识别高维数据突出表现在异常检测领域崭露头角,它利用神经网络等深度学习模型捕捉空间关系,增强复杂数据集中异常的检测能力.

主动异常检测模型可根据数据标签的使用情况分为主要的 4 类,见图 3.监督模型利用标注数据学习正常与异常样本差异,构建分类器.但局限性为异常样本在训练集中通常占比不足,且获取精确标注成本高昂.半监督模型则使用少量标注正常数据与大量未标注数据.但是该模型假设未标注数据多为正常,当该假设不成立时,模型可能学习错误模式.与前者不同,无监督模型直接从原始数据检测异常,无需预标记数据集.值得注意的是若数据集含异常污染会干扰检测,且依赖"正常样本占多数"假设.混合模型则是融合多种学习范式,通过未标注数据提升泛化能力,但参数调优复杂度较高.

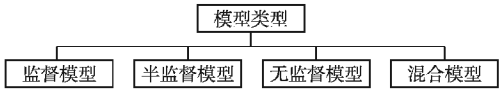

图 3 异常检测模型分类图

Fig. 3 Classification of anomaly detection models

1.3 主动异常检测面临的挑战

主动异常检测的核心问题在于如何在高不确定性、标注稀缺及动态数据环境中,通过交互策略最大化异常检测效能与标记成本的平衡.异常样本的稀疏性与主动学习的标注需求冲突.如网络入侵检测中,攻击模式动态演化,需实时捕捉新型异常而非已知变种,这就要求模型能通过少量标注快速识别异常模式的变化规律.但在动态数据流场景中,传统算法通常基于数据的静态假设,所以难以平衡高计算复杂度与实时响应需求.为此,需结合自适应策略优化模型更新效率,同时避免历史知识遗忘.另外,虽然深度学习模型能自动学习数据的高层次特征,但是其"黑箱"特性阻碍了专家对检测逻辑的理解,影响反馈质量与系统可信度.故专家反馈如果摄入标签噪声问题,错误标签会误导模型训练.

2　主动异常检测分类器

主动异常检测分类器主要用于初始异常判断,目的是为后续的主动学习提供异常候选集.故可以根据其底层算法主要分为两大类:基于传统方法和深度学习的方法.

2.1　传统方法

本小节将主要的传统异常检测技术分为如下几类:基于密度方法、树方法和域方法.参考文献中基于传统方法对比,见表 1.

基于密度方法其代表性的有局部离群因子(LOF),考虑到局部异常的数据分布特性,可以通过 k 近邻密度偏差进行检测.文献[20,21]将 LODA 做为动态调整权重的集成模型,其通过 M 个随机稀疏投影生成弱检测器,形成 M 维特征空间.在使用基于边界的不确定主动查询策略将样本反馈给专家后,采用近端梯度法来优化弱检测器权重.文献[22]针对光变曲线时间序列数据中瞬变体的异常标记成本高和稀有信号难以识别等问题,提出了一个无监督的主动学习异常检测框架.其新颖点在于首次将小波特征与主动学习结合用于射电瞬变检测,并将通过 Zooniverse 平台使志愿者标注数据动态优化异常排序.

基于树的分类器因其可解释性和计算效率而备受推崇.文献[14]提出了一种基于孤立森林的随机特征选择策略,其新颖点在于模型更新采用权重优化机制,专家反馈通过调整叶子节点颜色值直接修改异常评分.文献[24]提出的 A^3PF 基于先验知识的随机森林,创新性地利用网络攻击特征权重来构建树.其通过比较相邻批次中同一叶子节点实例数量的变化率来完成动态评分,进而量化不确定性.每次反馈给专家标记的标签信息则依赖于动态评分和不确定评分,随后结合伪标签数据更新森林的密度修正项,形成闭环优化.

基于域的方法围绕正常数据创建边界,将边界外的任何内容视为异常.这类别的代表性算法包括基于支持向量机(SVM),其变体包括基于支持向量数据描述(SVDD),旨在将正常数据封装在超球体内,将异常排除在外.另外,单类支持向量机(OC-SVM)通过最大化数据点到决策边界的距离来对异常进行分类,与 SVDD 相比,它更容易受到核函数和超参数选择的影响.

2.2　基于深度学习的方法

深度异常检测方法因为其的特征学习能力和处理复杂、高维数据的能力,在主动异常检测中崭露头角,考文献中基于深度学习方法对比,见表 2.

表 1　参考文献中基于传统方法对比

Table1　Comparison of traditional methods in the references

方法	算法	文献	目标问题	特点
基于密度	投影集成局部离群因子	AAD[20,21]	适用于动态高维数据	集成学习,反馈优化检测器权重
		文献[22]	分析光变曲线的特征来检测瞬变体	混合评分,标记密集区域依赖反馈,稀疏则依靠原异常分数
基于树	孤立森林	ALIF[14]	解决无监督模型无法捕捉领域特定异常的问题	标注结果映射叶子节点的颜色值,动态调整路径深度
	随机森林	文献[23]	环境监测中传感器数据检测	分析五种机器学习模型在主动学习框架下的性能
		A^3PF[24]	动态网络流量中的异常检测	结合自适应查询策略和标签增强更新
	随机空间划分树	ISPForest[25]	实时流式数据	利用轻量级增量学习机制,每次反馈后仅调整当前实例相关的树结构
	基于集成模型	IF-ADD[26,27]	调整集成权重以最大化异常发现率,处理漂移	使用孤立森林、半空间树等树模型作为基础检测器,提取叶子节点特征构建集成
基于域	支持向量机	文献[28]	深度集成异常检测	使用 LCD 采样策略,边缘节点协作选择样本训练模型
	单类支持向量机	OCSVM-AAD[29]	数据分布复杂,需核技巧处理非线性	专家反馈动态优化 OCSVM 的决策边界
		ALS-VDD[30]	大规模、高噪声工业数据	样本选择策略结合基于决策边界和局部密度,增量式优化模型

由于日志数据量大且数据标记成本高,因此无监督模型更适合处理日志异常检测任务.文献[31]提出的 AcLog 采用无监督 LSTM 模型,目的是学习正常时间序列进而检测异常.其新颖点在于样本选择策略基于窗口的"模糊"样本,但是这种策略容易陷入局部最优解.相比之下,文献[33]则更强调多维度的时序依赖,通过卷积层提取时空特征.AMAD 则采用集成的样本查询策略,其一关注异常比例动态调整不确定阈值,该阶段主要用于模型初期快速收敛.其二关注模型错误分类的样本,使用动态采样区间,模型后期依赖该策略精细化调整.

工业数据通常来自各种设备和传感器,具有数据量大、维度高和标记成本高的特点.文献[36]提出了多目标生成对抗主动学习,其新颖点在于采用隐式主动学习.其中判别器为生成器提供反馈信息以调整样本生成,而多个生成器生成多样

化的潜在异常. 该模型实现了完全无监督,其依赖于生成器与判别器的对抗平衡. 文献[37]引入了一种基于条件生成对抗网络的方法,重点关注生成多样化、信息丰富且具有代表性的异常样本,继承了多目标生成的思想. 文献[38]提出了基于集成的扩展条件生成对抗网络模型. 与之前的方法不同,它强调通过多判别器架构来纠正类别不平衡,每个判别器专注于纠正其他判别器的误分类,而不仅仅依赖生成器的多样性. 其中每个判别器包含两个分类器,通过集成判别器的平均输出选择基于边界的样本,模型训练则协同使用生成的平衡异常数据和少量的真实标注数据.

表 2 参考文献中基于深度学习方法对比

Table 2 Comparative analysis of deep learning-based methods in the references

方法	文献	目标问题	特点
长短期记忆网络	AcLog[31]	日志异常检测问题	利用滑动窗口生成子序列作为输入
	文献[32]	时间序列异常检测	获取反馈后进行增量训练
卷积神经网络	AMAD[33]	多元时间序列异常检测	使用 CNN 作为学习者模型
自编码器	文献[34]	网络入侵问题	针对数据流提出两种动态阈值方法(SATFF、AAT)
	GAAD[35]	工业异常检测问题	构建 K 近邻图表示样本间全局关系
生成对抗性网络	SO-GAAL/MO-GAA[36]	解决无标注问题	隐式生成潜在异常样本,适合无标记环境
	DIR-GAAL[37]	方向性敏感异常检测	半监督框架,分类器结合生成对抗和主动学习的双重优化
	EAL-GAN[38]	集成学习缓解类别不平衡	双分类器与集成判别器协同工作
混合模型	文献[39]	单变量时间序列	重采样技术与主动学习的协同
	EraseMTS[40]	打破 IID 假设限制和高净度要求	多粒度重构误差建模,边界定位协同动态扩展样本候选集
	IDEAL[41]	解决时间序列中自动调整窗口和可解释性	结合 LSTM-AE 重构误差和随机森林对进行异常解释
	Active-MTS-AD[42]	多变量时间序列	重构误差与 KL 散度的联合优化

在时间序列检测领域,混合模型不仅可以捕捉时间序列中的前向和后向依赖关系,还聚焦于模型可解释性为专家提供可参考的反馈信息. 文献[39]提出了一种 LSTM-AE 与主动学习结合的半监督异常检测框架. 其新颖点在于利用 LSTM-AE 编码后的低维特征训练分类器,通过边际不确定性采样选择分类置信度最低的样本进行专家标注. 在主动学习循环中集成重采样技术,缓解异常检测中的类别不平衡问题. 文献[41]提出了一种基于 LSTM-AE 的多变量时间序列异常检测模型. 其引入随机森林生成可解释的约束决策树,将异常模式转化为可解释的规则,作为专家反馈的桥梁. 随后,反馈结果用于进一步提升决策树规则的质量,其目的是形成解释性与检测精度的正向循环.

深度异常检测的优势包括自动特征提取,有效处理高维数据,以及随着数据规模的增加在性能上优于传统机器学习方法. 然而,深度学习模型在与主动学习结合时无法直观地给反馈专家提供判定异常规则. 比如对大型标记数据集的依赖以及在可解释性方面的挑战——特别是在医疗保健等领域,深度学习模型通常被视为黑箱. 故为了弥补这一方面的不足,可以将其与基于树的模型相结合,扩展模型的可解释性.

3 数据查询策略分类

主动学习通过选择信息量最大或最具代表性的未标注样本来提升模型性能[43]. 文献[9]中将数据查询策略分为 3 种类型:数据驱动、模型驱动和混合策略. 数据驱动聚焦于通过统计特征(如密度估计或不确定性度量)识别数据分布异常的实例;模型驱动策略则依据模型的预测行为选择样本,重点关注模型预测不确定性强的区域;混合策略综合前两者的优势,在统计洞察与模型行为间取得平衡. 参考文献中基于数据查询策略和反馈策略的对比,见表 3.

3.1 不确定性策略

不确定性原则是主动学习的核心准则. 如下是基于不确定性的典型度量方法.

3.1.1 基于局部密度

基于局部密度的不确定性度量是主动异常检测的常用方法. 在局部离群因子假设中,正常数据通常分布于高密度区域且与邻域样本密度相似,而异常样本则位于密度骤降区域. 对于基于树的异常分类器来说可通过分析树路径中的密度变化及叶节点的稀疏分布来评估不确定性[24]. 具体而言,孤立森林通过路径长度计算异常分数,路径越短表明样本越可能异常.

3.1.2 基于高置信度

高置信度策略基于模型驱动根据预测结果选择样本,关注模型非常确定的实例,这有助于加强已知的决策边界. 文献[21]验证了主动学习中广泛使用的 Top-N 策略的有效性. 该策略在主动异常检测中数据选择方法中广泛使用.

文献[25]提出量化每棵树的不确定性基于历史反馈计算当前区域的异常比. 其通过动态计算局部区域的异常比例,衡量单棵树预测与历史反馈的偏离程度,多棵树平均后得到全局不确定性. 不同于基于信息熵或边界的主动学习,该方法通过模型与历史反馈的一致性直接量化不确定性. 相较于 IF-AAD 等依赖累积反馈的方法,ISPForest 实现了单样本驱动的在线更新. 文献[41]通过计算时间序列窗口的自相关系数,

并与正常模式的自相关分布进行对比. 选择那些偏离正常范围最大的样本(如通过 KL 散度或马氏距离衡量差异)作为反馈候选.

表 3　参考文献中基于数据查询策略和反馈策略的对比

Table 3 Comparative of data query strategies and feedback strategies in the references

文献	数据查询策略	反馈策略	特点
LogALST[4]	不确定性策略(基于熵)	标注后样本重新训练学生模型	针对日志数据新增时,熵策略优先标注使模型适应变化
B-ALIF[5]	不确定性策略(决策边界、高置信度)	反馈触发贝叶斯推断,调整叶子节点的 Beta 分布参数	将标注数据作为贝叶斯先验,直接修正模型内部结构的置信度
文献[7]	个性化混合策略(基于用户反馈的异常分数重排序)	用户兴趣标签 + 异常置信度融合	个性化推荐,用户兴趣驱动的异常发现
AMAD[33]	根据模型收敛情况采用自适应查询策略	通过重训练直接优化决策边界	真实系统中异常样本稀少,初期捕捉更多误判异常,后期捕捉漏检的真实异常
GAAD[35]	图传播混合策略(K 近邻图传播不确定性与代表性)	标签传播 + 密度感知	工业质检等高维数据、需快速响应新异常类型
DIR-GAAL [37]	混合策略(不确定性、方向性、多样性)	协同样本方向性和异常增强生成器的对抗强度	方向性敏感场景
文献[39]	不确定性策略(边际不确定性)	结合过采样和欠采样平衡数据	适合静态时间序列
Active-MTS-AD [42]	混合策略(Top-k、阈值附近、区间随机采样)	分母惩罚、负惩罚、度量学习	适合动态数据分布,处理概念漂移
文献[44]	代表性策略	用户标注的节点作为初始聚类中心	结合用户标注的全局聚类中心和 SOINN 生成的局部拓扑关系
Pineforest[45]	不确定性策略	淘汰低质量树,保留符合专家预期的森林(隐式反馈)	强调轻量级调整,间接优化模型结构,适合高维数据
EBDALM [46]	不确定性采样(设计多层感知机学习多模型的动态权重)	集成模型权重调整(正样本迫使接近参考分布、异常样本强制远离正常分布)	多源异构数据融合场景

3.1.3　基于边界

基于边界策略与基于高置信度策略的目标相反,选择模型对其预测最不确定的样本,由于其可解释性和易于实现,因此受到关注. 其假设所选样本通常位于决策边界附近,其代表性的方法有基于重构误差、基于熵、基于距离的最小置信度(LCD)和最小间隔(SM).

基于重建误差的策略其本质是标注靠近隐式决策边界的样本,这些样本的重构值值与阈值的差异最小,模型对其分类最不确定. 这与主动学习中基于决策边界的不确定性抽样(如 SVM 的间隔采样)高度相似. 文献[34]针对网络数据流中的异常检测,提出了一种新颖的基于重构误差距离的阈值策略. 通过衰减因子计算历史重构误差 RE 差异的均值和标准差,该方法选择低于均值一定标准差范围的样本进行标注,旨在通过标注边界样本来优化模型决策,如式(1)和式(2)所示:

$$RE = \frac{1}{n}\sum_{i=1}^{n}(T'_i - T_i)^2 \tag{1}$$

$$\mathrm{E} = (\phi - RE)^2 \tag{2}$$

其中 n 为总窗口数,T_i 和 T'_i 表示第 i^{th} 个网络的输入与输出,ϕ 表示预设置阈值,E 表示不确定性度量.

文献[40]提出了一种基于边缘异常候选集的迭代式主动多元时序异常检测算法. 其新颖点在于基于多粒度重构误差的异常置信度建模,即结合序列内和序列间局部/全局依赖关系. 在主动学习阶段选择最接近阈值 ϕ 的样本作为中心点,再向该样本时间轴前后各扩展 j 个样本,定位并覆盖分类边界附近的"高信息量"样本. 这种设计的核心目的是实现主动学习中"以最小标注成本换取最大模型增益". 然而,对于时间序列数据使用固定阈值 ϕ 可能无法适应数据分布的变化.

基于熵的不确定性策略[47]选择熵值最高的样本,即模型预测概率分布最接近均匀分布的样本. 这类样本通常位于分类边界附近,标注后能最大程度减少模型的泛化误差. 文献[4]提出了一种结合主动学习和自训练的半监督日志异常检测技术. 模型对未标记的日志数据集进行预测,生成概率矩阵并计算熵值 C_x,如式(3)和式(4)所示:

$$C_x = -\sum_{j=1}^{c} p_j \cdot \log(p_j) \tag{3}$$

$$H(x) = 1 - C_x \tag{4}$$

其中,p_j 表示样本 x 属于类别 j 的概率,c 表示总类别数. $H(x)$ 为模型确定置信度分数.

3.2　代表性策略

代表性(多样性)策略强调选择能够捕捉数据集整体分布特征的数据点. 在选择代表性策略时,通常考虑其多样性,最简单的方法是随机采样来扩展样本候选集.

基于聚类的策略是数据驱动的查询策略. 这些方法首先使用聚类算法将数据分为聚类,然后在每个聚类中选择最具代表性的样本. 通常,最具代表性的样本是距离聚类中心最近或在聚类分布中最居中的样本. 这确保了标记数据捕捉到了每个聚类的基本特征. 文献[44]使用自编码器进行特征压缩,自组织增量神经网络来学习网络行为模式,以及模糊 C 均值(FCM)算法对异常进行分类. 与传统的 K 均值不同,模糊 C 均值 基于对聚类中心的距离对模式进行分类,强调聚类影响力和交互式探索. 其核心思想是优先标注聚类中心或代表性节点,以快速定义正常或异常模式.

但当数据分布不均匀时,基于聚类的策略可能会忽略数据中的局部细节. 基于距离的代表性策略可以通过计算样本与所有其他样本之间的距离来捕捉这些局部细节,从而评估

样本在数据集中的局部密度. 文献[37]通过密度估计选择能代表整体分布的样本,确保标注的样本能反映数据集的全局特性. 样本的密度越高,它在整个数据集中就越具有代表性. 这种策略也可以描述为选择对周围数据分布影响最大的实例.

3.3 混合策略

在主动异常检测中,如果仅仅考虑基于不确定性的数据选择策略会忽略样本分布的多样性,结果可能导致聚类效应. 混合策略通过整合基于不确定性的策略与代表性(多样性)策略.

文献[7]提出一种结合数据相关性评分与异常评分的主动学习策略,通过专家反馈调整推荐结果,使其更符合专家兴趣需求. 该策略能有效过滤无关样本并提升标注效率,同时体现了相关性概念的主动性. 文献[27]指出之前的研究关于 Select-Top 策略(Top-k)可能缺乏多样性,并提出 Select-Diverse 混合策略. 该方法利用树结构划分数据空间,计算子空间相关性并选择紧凑子空间集表征实例群,融合了 Select-Top 与多样性驱动的查询选择机制.

文献[30]通过将基于距离决策边界的样本筛选与局部密度指导的关键区域相结合,在减少标注需求的同时有效抑制噪声干扰. 文献[35]提出的 GAAD 方法通过编码器-解码器模型重构误差衡量不确定性,并通过样本与近邻距离之和表征代表性. 在主动学习初期采用重构误差作为不确定性策略标注样本,若在预设预算内未发现新异常样本,则切换至基于聚类的代表性策略,若连续选择一定数量正常样本,则重新启用不确定性策略. 样本 x 的信息量 $E(x)$ 定义如公式(5)所示:

$$E(x)=\alpha\cdot\|x-\text{Decoder}(\text{Encoder}(x))\|^2+(1-\alpha)\cdot(-\sum_{x'\in NN_k(x)}\|x-x'\|^2) \tag{5}$$

其中,α 用于平衡不确定性与代表性权重,x 为当前样本,x'表示其 k 近邻样本.

综上,混合策略通过协同不确定性驱动与代表性驱动机制,在主动异常检测中发挥关键作用. 基于不确定性的策略聚焦模型置信度低的模糊样本以提升检测敏感度,代表性策略则通过捕获数据整体分布确保泛化能力. 二者的动态平衡可适应复杂动态环境,近年来已成为提升检测效能的核心研究方向[48].

4 反馈策略分类

与传统异常检测方法不同,主动异常检测不仅旨在提升异常识别的数量,更通过最大化异常检测器的性能以增强检测精度与异常定位能力. 因此,反馈机制在主动异常检测的有效性中起着决定性作用.

4.1 反馈形式与预算管理

在反馈阶段,专家对实例进行审查并提供反馈. 最常见的反馈形式包括类别标签和置信度分数. 类别标签是标准的反馈类型. 相反,置信度分数反映了专家对其标签正确性的确定程度,为模型优化提供了更细致的信息.

预算是指算法在主动学习过程中可以向专家提出的查询的最大次数,旨在最小化对专家标记的依赖,同时提高学习效率. 一个简单的方法是使用固定的查询次数 B. 在最近的研究中更加关注预算管理策略根据模型的学习进度和积累的知识调整查询频率. 例如,在早期阶段频繁查询可以加速学习,而后期减少查询可以巩固知识. 此外,异常分布影响查询模式. 聚集的异常可能导致更频繁的查询,而稀疏的异常需要更少的查询.

4.2 负惩罚与正惩罚

负惩罚调整模型以最小化假阳性(将正常实例错误分类为异常的情况). 相反,正惩罚侧重于减少假阴性,即未检测到真实异常.

文献[8]提出该模型的主要目标是通过调整决策树权重,使标记为“正常”的样本在未来的推荐中排名更低,从而减少假阳性. 文献[29]中利用专家反馈来优化 OCSVM 的边界,其引入了三类惩罚项,其分别为未标记数据、标记为正常的误报、标记为异常的漏报. 对标记为正的 FP 施加惩罚,强制这些点位于决策边界内. 而对于对标记为异常的 FN 则使用相反的目的,即强制这些点位于决策边界外. 在后续的主动学习的迭代中,获取的反馈逐步修正模型的错误认知,使边界更贴合真实数据分布.

文献[33]针对 Top-N 策略在低异常评分区间漏报累积的缺陷. 其提双惩罚机制选择误分类样本进行动态优化模型决策边界.

$$u_{FP}^{*}=\arg\max_{u\in U}(P(\hat{y}|u)-f(u)) \tag{6}$$

$$u_{FN}^{*}=\arg\max_{u\in U}-(P(\hat{y}|u)-f(u)) \tag{7}$$

其中,u 表示未标注数据点,$P_M(\hat{y}|u)$为模型预测 u 为异常的概率,$f(u)$为模型置信度指示函数.

公式(6)根据 FP 样本的分布,更新决策边界阈值,进行边界收缩. 公式(7)根据 FN 样本调整阈值下限,进行边界扩展.

4.3 正向奖励机制

正向奖励源自强化学习,通过激励智能体执行有益动作以优化长期收益. 在主动异常检测中,成功识别异常可触发正向奖励,从而强化模型的良性行为模式[49].

文献[7]使用随机森林回归来预测未标记和标记数据之间的相关性. 通过专家标记反馈,被标记为“相关”的样本在未来的推荐中排名更高,从而实现正向强化. 文献[12]将奖励机制分为外部和内在奖励. 外部奖励针对标记数据,对正确分类给予奖励,反之对错误分类施加惩罚. 内在奖励利用未标记数据的潜力,例如鼓励正确识别正常数据以减少对异常的过度敏感性,并根据潜在异常的无监督异常分数授予奖励,从而促进发现更多异常. 这两种机制的结合有效平衡标记数据的利用和未标记数据的探索,提高模型的性能和鲁棒性.

4.4 特征空间优化

特征空间优化不仅影响单个样本的分类,还全局调整特征空间的分布,使决策边界能够根据更新的特征分布进行校准.

度量学习是一种学习样本之间距离度量的技术,旨在将同一类别的样本在特征空间中更紧密地聚集,同时将不同类别的样本推得更远. 文献[25]通过区域调整和异常分数更新

优化模型. 如果一个区域大多被标记为正常,则进行“合并”操作以降低其异常分数. 如果该区域同时包含正常和异常实例,则应用“终端扩展”以更好地区分它们,降低假阴性. 由文献[42]提出的基于伪标签度量学习的反馈策略结合类内损失和类间损失,通过潜在空间特征约束实现了小样本下的异常模式适应. 类内损失 L_{intra},惩罚同一类别样本之间的较大距离,确保相似样本在特征空间中更紧密地聚集. 类似地,类间损失 L_{inter} 鼓励不同类别样本之间的较大距离,帮助模型建立清晰的类别边界. 式(8)和式(9)这两个损失函数共同优化模型区分正常和异常实例的能力.

$$L_{\text{intra}}=\frac{2}{|S_n|^2-|S_n|}\sum_{x,x'\in S_n,x<x'}D(r_x,r_{x'})+\frac{2}{|S_a|^2-|S_a|}\sum_{x,x'\in S_a,x<x'}D(r_x,r_{x'}) \tag{8}$$

$$L_{\text{inter}}=\frac{1}{|S_n|\cdot|S_a|}\sum_{x\in S_n,x'\in S_a}\max\{0,M-D(r_x,r_{x'})\} \tag{9}$$

其中,S_n 与 S_a 分别表示正常、异常样本集合,$D(\cdot)$ 为潜在空间特征距离度量,M 为异类最小间距约束,如果不同类别样本之间的特征距离大于 M,则损失为零.

文献[50]通过动态调整边界优化策略. 如果标记的异常样本比例较高,边界向内移动,将异常与中心推远. 如果比例较低,边界向外移动,将正常样本拉近. 这种动态调整使正常样本更紧凑,将异常推得更远,增强模型的辨别能力.

4.5　标签增强

在主动异常检测中,标签增强是为查询实例的邻近未标注样本生成伪标签,其依赖假设邻近样本类别一致. 标签增强的一个关键优势在于,它通过整合“专家”提供的标签和从数据间关系得出的标签,提高了预测一致性.

伪标签增强策略是一种半监督学习技术,利用训练有素的模型预测未标记数据的标签,生成伪标签. 文献[31]提出在获取专家注释信息后,复制正常数据以增强模型对远程请求流中此类正常向量的记忆. 同时,对于异常数据,识别类似的异常数据,并应用随机丢弃策略以减少误报. 文献[35]提出结合 K 近邻图扩展标签传播范围,以表示样本之间的关系. 其核心在于标记数据的不确定性与类似未标记数据呈正相关,而代表性则呈负相关. 另外,其结合动态平衡策略,在异常边界探索与分布覆盖间取得平衡,避免漏检.

文献[44]提出通过计算标记实例后隶属矩阵的变化来量化数据的影响. 影响力越大的实例能够更有效地传播标签信息,特别是在数据分布的密集区域,标记这些实例可以更有效地传播标签信息. 由文献[51]提出的异常分数相似性策略结合类似于伪标签的反馈机制以提高模型的有效性. 该策略首先根据异常分数的分布选择和标记数据点,然后基于此反馈为具有相似异常分数的邻近数据点分配标签. SAS 策略通过过滤误标记的异常数据有效清理重放缓冲区,降低异常污染的风险.

反馈策略的选择与异常分类器和数据结构密不可分. 负/正惩罚机制通过权衡误报与漏报优化检测精度. 正向奖励机制激励模型持续提升异常识别能力. 特征空间优化重构特征空间的全局分布以增强判别边界适应性. 标签增强则通过扩展数据多样性提升模型泛化能力. 多策略协同使主动异常检测系统能有效应对动态环境中的复杂数据模式.

5　挑战与展望

尽管主动异常检测在解决标注数据稀缺和类别不平衡方面取得了显著进展,但在实际应用中仍面临诸多挑战. 本节系统分析当前存在的关键问题,并展望未来研究方向.

5.1　实时异常检测

对于像传感器、交易和日志这类持续产生大规模数据的应用来说,实时检测异常的能力至关重要. 实时系统需要高效处理高速数据流,但传统算法由于计算复杂且需多次处理数据,难以应对. 主动异常检测通过利用反馈机制动态选择最有价值的样本进行标记,从而优化实时检测.

增量学习[52]提供了一种有前景的解决方案,使模型能够随着数据的流入不断更新,而无需完全重新训练. 这种方法有助于保留先前获得的知识,同时检测不断演变的异常. 另外,经验回放通过存储历史交互并在后续训练中随机抽取它们,增强了学习过程,从而减轻了数据点之间的时序相关性,提高了模型的稳定性和效率. 自适应策略越来越受欢迎,它们利用专家反馈动态调整检测阈值以优化边界,从而减少假阳性和假阴性.

5.2　可解释性

在主动异常检测中,可解释性对于使专家能够理解模型决策过程至关重要. 这有助于更好的验证,并促进公平性和鲁棒性. 传统主动异常检测通过专家反馈调整模型权重,但缺乏对调整过程的解释,导致用户无法理解权重变化的逻辑. 文献[53]引入集成可解释性机制(AWS)特征重要性指标,量化每个特征对异常得分的贡献,提供后反馈的透明解释. 在 AWS 的基础上,将 AAD 调整后的权重归一化并与原始 AWS 得分结合,使得专家反馈不仅改变模型输出,还通过特征重要性解释调整逻辑.

紧凑描述通过异常实例的简明特征摘要揭示潜在模式,提供对多种异常模式的见解. 然而,平衡可解释性与模型性能存在显著挑战. 例如,复杂模型可能优先考虑准确性而牺牲结果的可解释性,导致系统输出的可信度降低. 另外,缺乏标准化评估标准进一步加剧了评估难度. 后续的研究应聚焦于开发定制化可解释性指标和自适应解释技术,根据用户需求动态调整解释粒度. 构建面向领域专家的可视化解释框架,增强模型与专家的双向交互. 探索可解释性对标注反馈质量的增强机制,通过改进反馈闭环提升系统有效性.

5.3　标注噪声容忍

精准的样本标注对主动异常检测至关重要,然而获取领域专家的高质量标注耗时且成本高昂. 实际应用中,非专业标注者提供的标签往往存在噪声. 故在缺乏充足专家反馈的情况下,验证这些标注的准确性极具挑战,导致模型训练过程复杂化.

传统主动学习默认标注完全可靠,但这一假设在现实场景中难以成立. 针对此问题,文献[54]提出基于黄金标准实例的标注者评估与训练策略,根据标准表现将标注者分为三类:专家、学徒和不合格. 通过迭代培训和任务再分配,标签准确性逐步提高. 未来的研究应不仅需要开发鲁棒算法降低噪

声标签对模型性能的影响并且还需要对标注质量控制设计半自动验证工具辅助人工审核.

5.4 多模态数据融合

在主动异常检测中,多模态数据融合对实时监控和响应至关重要,特别是在应对复杂攻击时能显著提升识别能力.通过整合多模态数据,系统可捕获互补信息以增强对复杂模式和异常的检测能力.然而,多模态的有效融合面临信息干扰或丢失等挑战,可能影响检测性能.

一种常见的方法是将多个模态的特征向量连接起来,但这可能导致见解被稀释.元特征提取使模型能够在数据集中提取一致的特征,允许训练有素的元策略直接应用于新的未标记数据,而无需进一步调整,这对于保持特征表示的一致性至关重要.此外,决策层融合通过在决策阶段整合信息来缓解这些问题,保留特定模态的特征,并增强检测的鲁棒性.总体而言,多模态数据融合有望提高主动异常检测系统的有效性和鲁棒性,但需平衡模态互补性与信息冗余,避免决策冲突.

5.5 概念漂移

概念漂移指数据分布随时间动态变化的现象,是动态环境中异常检测的核心挑战.在金融欺诈检测领域需要应对欺诈手段的快速演变,在工业物联网领域需要处理设备状态漂移导致的异常误报.噪声的干扰可能会掩盖真实漂移,使区分真正的漂移和短期波动变得复杂.像集成方法通过结合多个模型的预测,可以帮助减轻漂移对单个模型的影响.在线学习允许随着新数据的增加而进行模型更新,确保对分布变化的响应能力.此外,迁移学习和模型复用促进了预训练模型对新环境的适应,增强了检测新出现的漂移模式的能力.

6 总 结

本文从主动异常检测的定义出发,系统分析了其框架与流程,并从3个核心维度对现有研究进行了总结.异常分类器涵盖传统统计方法与深度学习方法.数据选择策略分析了基于不确定性与代表性的混合查询机制.反馈利用机制分析了通过正/负惩罚优化模型、正向反馈机制、结合特征空间重构与标签增强提升检测精度.针对动态环境下的实时检测、概念漂移、多模态融合等挑战,论文进一步探讨了当前主动异常检测领域仍存在的挑战,并对未来研究方向进行展望.

References:

[1] Nassif A B, Talib M A, Nasir Q, et al. Machine learning for anomaly detection: a systematic review[J]. IEEE Access, 2021, 9: 78658-78700, doi: 10.1109/ACCESS.2021.3083060.

[2] Das S, Wong W K, Dietterich T, et al. Incorporating expert feedback into active anomaly discovery[C]//IEEE 16th International Conference on Data Mining (ICDM), 2016: 853-858.

[3] Cunha L L, Brito M A, Oliveira D F, et al. Active learning in the detection of anomalies in cryptocurrency transactions[J]. Machine Learning and Knowledge Extraction, 2023, 5(4): 1717-1745.

[4] Wang R, Wu Z, Li Y, et al. A semi-supervised log anomaly detection method based on active learning and self-training[C]//International Conference on Computer Application and Information Security, 2024: 671-679.

[5] Sartor D, Barbariol T, Susto G A. Bayesian active learning isolation forest (B-ALIF): a weakly supervised strategy for anomaly detection[J]. Engineering Applications of Artificial Intelligence, 2024, 130: 107671, doi: 10.1016/j.engappai.2023.107671.

[6] Trujillo J A, de-la-Bandera I, Burgueño J, et al. Active learning methodology for expert-assisted anomaly detection in mobile communications [J]. Sensors, 2022, 23 (1): 126, doi: 10.3390/s23010126.

[7] Lochner M, Bassett B A. ASTRONOMALY: personalised active anomaly detection in astronomical data[J]. Astronomy and Computing, 2021, 36: 100481, doi: 10.1016/j.ascom.2021.100481.

[8] Ishida E E O, Kornilov M V, Malanchev K L, et al. Active anomaly detection for time-domain discoveries[J]. Astronomy & Astrophysics, 2021, 650: A195, doi: 10.1051/0004-6361/202037709.

[9] Trittenbach H, Englhardt A, Böhm K. An overview and a benchmark of active learning for outlier detection with one-class classifiers[J]. Expert Systems with Applications, 2021, 168: 114372, doi: 10.1016/j.eswa.2020.114372.

[10] Zamanzadeh Darban Z, Webb G I, Pan S, et al. Deep learning for time series anomaly detection: a survey[J]. ACM Computing Surveys, 2025, 57(1): 1-42.

[11] Yang X, Qi X, Zhou X. Deep learning technologies for time series anomaly detection in healthcare: a review[J]. IEEE Access, 2023, 11: 117788-117799, doi: 10.1109/ACCESS.2023.3325896.

[12] Chen C, Wang D, Mao F, et al. Deep anomaly detection via active anomaly search[C]//Proceedings of the 23rd International Conference on Autonomous Agents and Multiagent Systems, 2024: 308-316.

[13] Pang G, Shen C, Cao L, et al. Deep learning for anomaly detection: a review[J]. ACM Computing Surveys, 2021, 54(2): 1-38.

[14] Marcelli E, Barbariol T, Sartor D, et al. Active learning-based isolation forest (ALIF): enhancing anomaly detection with expert feedback[J]. Information Sciences, 2024, 678: 121012, doi: 10.1016/j.ins.2024.121012.

[15] Aggarwal C C, Kong X, Gu Q, et al. Active learning: a survey[J]. Data Classification: Algorithms and Applications, 2014: 571-605, doi: 10.1201/b17320.

[16] Pichara K, Soto A. Active learning and subspace clustering for anomaly detection [J]. Intelligent Data Analysis, 2011, 15 (2): 151-171.

[17] Li Y, Wang Y, Ma X, et al. A graph-based method for active outlier detection with limited expert feedback[J]. IEEE Access, 2019, 7: 152267-152277, doi: 10.1109/ACCESS.2019.2947736.

[18] Liu Y, Li Z, Zhou C, et al. Generative adversarial active learning for unsupervised outlier detection [J]. IEEE Transactions on Knowledge and Data Engineering, 2019, 32(8): 1517-1528.

[19] Pimentel T, Monteiro M, Veloso A, et al. Deep active learning for anomaly detection[C]//International Joint Conference on Neural Networks, 2020: 1-8.

[20] Das S, Wong W K, Dietterich T, et al. Incorporating expert feedback into active anomaly discovery[C]//IEEE 16th International Conference on Data Mining, 2016: 853-858.

[21] Das S, Wong W K, Dietterich T, et al. Discovering anomalies by incorporating feedback from an expert[J]. ACM Transactions on Knowledge Discovery from Data, 2020, 14(4): 1-32.

[22] Andersson A, Lintott C, Fender R, et al. Finding radio transients with anomaly detection and active learning based on volunteer classifications[J]. Monthly Notices of the Royal Astronomical Society, 2025, 538(3): 1397-1414.

[23] Russo S, Lürig M, Hao W, et al. Active learning for anomaly detection in environmental data[J]. Environmental Modelling & Soft-

ware,2020,134:104869,doi:10.1016/j.envsoft.2020.104869.
[24] Li B,Wang Y,Cheng L. Adaptive and augmented active anomaly detection on dynamic network traffic streams[J]. Frontiers of Information Technology & Electronic Engineering,2024,25(3):446-460.
[25] Li Q,Yu Z,Xu H,et al. Human-machine interactive streaming anomaly detection by online self-adaptive forest[J]. Frontiers of Computer Science,2023,17(2):172317,doi:10.1007/s11704-022-1270-y.
[26] Das S,Islam M R,Jayakodi N K,et al. Active anomaly detection via ensembles[J]. arXiv preprint arXiv:1809.06477,2018.
[27] Das S,Islam M R,Jayakodi N K,et al. Effectiveness of tree-based ensembles for anomaly discovery:insights,batch and streaming active learning[J]. Journal of Artificial Intelligence Research,2024,80:127-170,doi:10.1613/jair.1.14741.
[28] Cai H,Hua C,Xu W. Design of active learning framework for collaborative anomaly detection[C]//11th International Conference on Wireless Communications and Signal Processing, IEEE,2019:1-7.
[29] Lesouple J,Tourneret J Y. Incorporating user feedback into one-class support vector machines for anomaly detection[C]//28th European Signal Processing Conference,IEEE,2021:1608-1612.
[30] Yin L,Wang H,Fan W. Active learning based support vector data description method for robust novelty detection[J]. Knowledge-Based Systems,2018,153:40-52,doi:10.1016/j.knosys.2018.04.020.
[31] Duan C,Jia T,Li Y,et al. Aclog:an approach to detecting anomalies from system logs with active learning[C]//IEEE International Conference on Web Services,2023:436-443.
[32] Wang C,Huang T,Li M,et al. A Bayesian LSTM based active anomaly detection service for large online systems[C]//Proceedings of the 15th Asia-Pacific Symposium on Internetware,2024:407-416.
[33] Yu R,Wang Y,Wang W. AMAD:active learning-based multivariate time series anomaly detection for large-scale IT systems[J]. Computers & Security,2024,137:103603,doi:10.1016/j.cose.2023.103603.
[34] Nixon C,Sedky M,Champion J,et al. SALAD:a split active learning based unsupervised network data stream anomaly detection method using autoencoders[J]. Expert Systems with Applications,2024,248:123439,doi:10.1016/j.eswa.2024.123439.
[35] Xiao K,Cao J,Zeng Z,et al. Graph-based active learning with uncertainty and representativeness for industrial anomaly detection[J]. IEEE Transactions on Instrumentation and Measurement,2023,72:1-14,doi:10.1109/TIM.2023.3279422.
[36] Liu Y,Li Z,Zhou C,et al. Generative adversarial active learning for unsupervised outlier detection[J]. IEEE Transactions on Knowledge and Data Engineering,2019,32(8):1517-1528.
[37] Bah M J,Zhang J,Yu T,et al. A generative adversarial active learning method for effective outlier detection[C]//IEEE 34th International Conference on Tools with Artificial Intelligence,2022:131-139.
[38] Chen Z,Duan J,Kang L,et al. Supervised anomaly detection via conditional generative adversarial network and ensemble active learning[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence,2022,45(6):7781-7798.
[39] Sabata T,Holena M. Active learning for LSTM-autoencoder-based anomaly detection in electrocar-diogram readings[C]//IAL@ PKDD/ECML,2020:72-77.
[40] MENG F,YANG Q L,HUO J,et al. EraseMTS:iterative active multivariable time series anomaly detection algorithm based on margin anomaly candidate set[J]. Journal of Computer Applications,2024,44(5):1458-1463.
[41] Homayouni H,Ghosh S,Ray I,et al. An autocorrelation-based LSTM-autoencoder for anomaly detection on time-series data[C]//IEEE International Conference on Big Data,2020:5068-5077.
[42] Wang W,Chen P,Xu Y,et al. Active-MTSAD:multivariate time series anomaly detection with active learning[C]//52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks,2022:263-274.
[43] Li X,Wang X,Chen X,et al. Unlabeled data selection for active learning in image classification[J]. Scientific Reports,2024,14(1):424,doi:10.1038/s41598-023-50598-z.
[44] Fan X,Li C,Yuan X,et al. An interactive visual analytics approach for network anomaly detection through smart labeling[J]. Journal of Visualization,2019,22:955-971,doi:10.1007/s12650-019-00580-7.
[45] Kornilov M V,Korolev V S,Malanchev K L,et al. Coniferest:a complete active anomaly detection framework[J]. Astronomy and Computing,2025,52:100960,doi:10.1016/j.ascom.2025.100960.
[46] Tang X,Astle Y S,Freeman C. Deep anomaly detection with ensemble-based active learning[C]//IEEE International Conference on Big Data,2020:1663-1670.
[47] Zakariah M,Almazyad A S. Anomaly detection for IoT systems using active learning[J]. Applied Sciences,2023,13(21):12029,doi:10.3390/app132112029.
[48] Li W,Qian W,Chen L,et al. Sample diversity selection strategy based on label distribution morphology for active label distribution learning[J]. Pattern Recognition,2024,150:110322,doi:10.1016/j.patcog.2024.110322.
[49] Zha D,Lai K H,Wan M,et al. Meta-AAD:active anomaly detection with deep reinforcement learning[C]//IEEE International Conference on Data Mining,2020:771-780.
[50] Kim M,Kim J,Yu J,et al. Active anomaly detection based on deep one-class classification[J]. Pattern Recognition Letters,2023,167:18-24,doi:10.1016/j.patrec.2022.12.009.
[51] Faber K,Corizzo R,Sniezynski B,et al. Active lifelong anomaly detection with experience replay[C]//IEEE 9th International Conference on Data Science and Advanced Analytics,2022:1-10.
[52] Jin W,Guo F,Zhu L. ISSTAD:incremental self-supervised learning based on transformer for anomaly detection and localization[J]. arXiv preprint arXiv:2303.17354,2023,doi:10.48550/arxiv.2303.17354.
[53] Kopljar D,Drvar V,Babic J,et al. xAAD-post-feedback explainability for active anomaly discovery[J]. IEEE Access,2024,12:181914-181924,doi:10.1109/ACCESS.2024.3510233.
[54] Zhu Y,Yang K. Tripartite active learning for interactive anomaly discovery[J]. IEEE Access,2019,7:63195-63203,doi:10.1109/ACCESS.2019.2915388.

附中文参考文献:

[40] 孟　凡,杨群力,霍　静,等. 基于边缘异常候选集的迭代式主动多元时序异常检测算法[J]. 计算机应用,2024,44(5):1458-1463.