



· 不确定性与知识获取 ·

基于图神经网络的时序信号异常检测方法

王婕婷¹, 张泽琰¹, 李飞江¹, 钱宇华^{1,2}

(1. 山西大学 大数据科学与产业研究院, 山西 太原 030006;

2. 山西大学 计算智能与中文信息处理教育部重点实验室, 山西 太原 030006)

摘要 高维时序数据异常检测是指从多元时间序列中识别出偏离整体模式或偏离预期行为的样本点的过程。在高维时序数据中,传感器间潜在的关联关系对于预测或检测任务的性能具有较大影响。图神经网络是一种基于节点的近邻关系学习节点表征的深度模型,能够有效建模传感器间的复杂关联。然而,现有基于图神经网络的异常检测方法大多依赖于单一的相似度度量来捕捉传感器间的关系,不能很好地学习传感器间的依赖关系。此外,在阈值选择时,现有方法使用正常数据中的最大异常得分作为切割阈值,限制了异常事件发生时的检测能力,从而造成较低的召回率。综上,提出了一种基于图神经网络的时序信号异常检测方法,根据传感器的特有特征使用多种相似度度量集成进行图结构学习;其次,将图结构学习方法与图神经网络相结合得到异常得分;最后,通过区间搜索法最优化 F -measure 指标寻找最优异常切割阈值。在两个真实传感器数据集上进行的实验表明,该方法比基准对比方法取得了较高的 F_1 值和召回率。

关键词 时序异常检测;图结构学习;注意力机制;相似度计算;区间搜索法

中图分类号: TP391 **DOI:** 10.16152/j.cnki.xdxbr.2025-02-011

A time series signal anomaly detection method based on graph neural network

WANG Jieting¹, ZHANG Zelong¹, LI Feijiang¹, QIAN Yuhua^{1,2}

(1. Institute of Big Data Science and Industry, Shanxi University, Taiyuan 030006, China;

2. Key Laboratory of Computational Intelligence and Chinese Information Processing,
Ministry of Education, Shanxi University, Taiyuan 030006, China)

Abstract Anomaly detection in high-dimensional time series data refers to the process of identifying sample points that deviate from the overall pattern or expected behavior from a multivariate time series. In high-dimensional time series data, the potential correlation between sensors has a significant impact on the performance of prediction or detection tasks. Graph neural networks are a deep model that learn node representations based on node proximity relationships, which can effectively model complex correlations between sensors. However, existing anomaly detection methods based on graph neural networks mostly rely on a single similarity measure to capture the relationships between variables and cannot learn the dependencies between variables well. In addition, when selecting thresholds, existing methods use the maximum anomaly score in normal data as the cut-

收稿日期: 2024-09-05

基金项目: 国家自然科学基金(62306170, 62106132); 山西省科技重大专项(202201020101006); 山西省基础研究计划(202103021223026, 20210302124271); 山西省科技创新人才团队专项(202304051001001)。

第一作者: 王婕婷, 女, 副教授, 硕士生导师, 从事统计机器学习和集成学习等研究, jtwang@sxu.edu.cn。

ting threshold, which limits the detection ability when abnormal events occur, resulting in lower recall rates. In summary, this paper proposes a temporal signal anomaly detection method based on graph neural networks, which integrates multiple similarity measures based on the unique features of sensors for graph structure learning. Then, the graph structure learning method is combined with the graph neural network to obtain anomaly scores. Finally, the interval search method was used to optimize the F -measure index and find the optimal anomaly cutting threshold. Experiments on two real sensor datasets showed that our method achieved higher F_1 values and recall compared to the benchmark comparison method.

Keywords temporal anomaly detection; graph structure learning; attention mechanism; similarity; interval search method

高维时序数据异常检测是指在多元时间序列中观察数据变化并检测其中异常行为的过程。这一技术广泛应用于多个行业领域。例如,在互联网领域实时监控并识别出异常行为;在制造业领域检测设备并识别异常故障等。

针对时序数据异常检测,研究者已经提出了多种方法,这些方法大致可以分为两大类:基于传统机器学习的方法和基于深度学习的方法。

传统方法主要依赖于设计的统计和算法策略,如主成分分析用于特征提取和异常点识别^[1];降维技术与基于密度的异常检测策略结合可以在高维空间中识别异常模式^[2];分析局部密度差异来精确定位异常点^[3];以及通过估计高维分布的支持域来识别远离该域的异常数据点^[4]。此外,还有利用时间序列的局部复发率和特性识别异常行为^[5]等。在深度学习方面,这些方法主要利用神经网络的强大表征学习能力,如针对具有季节性特征的多元时间序列,通过改进算法提高异常检测的准确性和鲁棒性^[6];引入随机性的循环神经网络更好地处理不确定性,从而提高异常检测的稳健性^[7];结合自编码器和生成对抗网络的优势实现快速且稳定的异常检测^[8];混合长短期记忆神经网络等先进结构预测单个家庭能源消耗实现对异常行为精确识别^[9],以及其他基于神经网络的方法^[10-14]。综上所述,时序异常检测领域的研究涵盖了从传统统计学习到现代深度学习的多种方法和技术。每种方法都有其独特的优势和适用场景。

然而,现有方法在处理时序数据时,往往忽视了传感器之间潜在的依赖关系,这在一定程度上限制了其预测和检测性能的进一步提升。上述方法在各自的领域内取得了显著成果,但在建模传感器间依赖关系方面的研究仍有待于进一步地探索和改进。

图神经网络(graph neural networks, GNNs)在建模多变量时间序列预测的图结构数据时,充分考虑了时间序列之间的依赖关系。在 GNNs 的框架下,每个时间序列被视作图中的一个节点,而时间序列间的依赖关系则被抽象为图中的边。这种设置允许节点的状态不仅受到其自身特征的影响,还受到其邻居节点状态的影响。然而,这些方法在模拟不同节点(即不同传感器)的行为时面临局限性,因为它们使用相同的模型参数来处理所有节点。例如,一种新的离散图结构学习方法旨在自动学习时间序列间的依赖关系^[15];一种时间图网络旨在针对动态图的深度学习框架^[16]以及通过引入 mask self-attention 层来克服现有图卷积方法的不足^[17]。综上所述,尽管 GNNs 在处理多变量时间序列预测的图结构数据时表现出强大的潜力,但仍需进一步研究和改进,以更好地模拟不同传感器的不同行为,并解决现有方法的局限性。其中最相关的工作是文献[11],该论文的核心是利用 GNNs 学习传感器间的关系图,并从这些模式中识别异常。该文提出了图结构学习的方法(GDN),该方法利用节点嵌入技术来捕捉图结构信息,并基于预测结果来检测异常。然而,该论文在图结构学习的过程中仅采用了一种相似度量,这可能无法全面捕捉传感器间的复杂依赖关系。此外,使用正常数据中的最大异常得分作为异常检测的阈值可能导致较低的召回率,因为验证集中可能包含因噪声、异常等因素导致的正常数据点。

近年来,有许多关于异常检测相关性分析和基于图神经网络检测方法的工作。例如丁小欧等人挖掘分析序列的相关性,在此基础上提出基于相关性分析的异常检测算法,实现对隐性性强的异常数据进行有效识别处理^[18];卢光曦通过构建图状数据结构,利用图神经网络进行特征聚合与

提取,并结合目标检测算法进行物体的定位与分类等,为图神经网络在异常检测领域的应用提供了新的思路和方法^[19],这些工作推动了异常检测技术的发展。

针对上述问题,本文提出了一种基于图神经网络的时序信号异常检测方法。该方法通过集成多种相似度量来构建传感器间的图结构,以提高依赖关系建模的准确性。在异常检测任务中,可以将确定异常得分阈值的过程视为一个二分类问题。其目的是将异常检测任务转化为一个可优化的分类任务,从而便于使用机器学习方法进行处理。为了找到最佳阈值,Wang 等人提出了一种基于最大化纯准确度的区间搜索法来寻找最优的切割阈值^[20]。该方法通过最大化纯准确度的后验概率来指导阈值的选择,达到最佳的效果。该方法为异常检测任务提供了一种有效的阈值确定方法。因此,本文采用区间搜索法来寻找最优的异常检测阈值,避免了使用正常数据中的最大异常得分作为阈值所带来的局限性。在区间搜索过程中,利用 F -measure 损失值作为优化目标,以平衡精确率和召回率。在两个真实数据集上的实验结果表明,本文提出的方法相较于 GDN 方法具有更高的 F_1 值和召回率,从而验证了所提方法的有效性。

本文的主要贡献包括 3 个方面。

- 1) 针对传感器之间依赖关系的图学习,本文通过分析不同相似度量度的适用场景,提出了一个集成多种相似度量度的方法。这一创新点提高了传感器间依赖关系的准确性,为后续的异常检测任务奠定了坚实的基础。
- 2) 在阈值搜索阶段,本文摒弃了传统固定阈值的选择方法,而是利用自适应策略,根据现有数据的特点进行动态调整。通过引入基于最小化 F -measure 损失值的区间搜索法,找到一个更为合

理的固定阈值,从而更准确地判定异常点,这一改进提高了异常检测的准确性。

3) 为了验证本文方法的有效性,在两个具有真值异常的数据集上进行了实验。研究结果表明,本文提出的异常检测方法相较于基准对比方法具有更高的准确性。同时,实验结果也充分证明了相似度量度集成和区间搜索法在寻找最优阈值方面的有效性。

1 基于图神经网络的时序信号异常检测方法

1.1 问题描述

本文中,训练数据由 N 个传感器在 T_{train} 时间的数据组成,即 $\mathbf{s}_{\text{train}} = [\mathbf{s}_{\text{train}}^{(1)}, \mathbf{s}_{\text{train}}^{(2)}, \dots, \mathbf{s}_{\text{train}}^{(T_{\text{train}})}]$ 。每个时间点是 N 个传感器的值,即 $\mathbf{s}_{\text{train}}^{(T_{\text{train}})} \in \mathbf{R}^N$ 。时序异常检测通常被视为无监督学习任务,本文采用无监督异常检测框架来构建模型,假设训练数据仅由正常数据组成。

本文目标是检测测试集中的异常,测试集由来自与训练集相同的 N 个传感器在 T_{test} 个时间单位内的数据组成,即 $\mathbf{s}_{\text{test}} = [\mathbf{s}_{\text{test}}^{(1)}, \mathbf{s}_{\text{test}}^{(2)}, \dots, \mathbf{s}_{\text{test}}^{(T_{\text{test}})}]$,其中 $\mathbf{s}_{\text{test}}^{(T_{\text{test}})} \in \mathbf{R}^N$ 。算法的输出是一组在测试集上表示每个测试时间点是否有异常的二进制标签,即 $a(t) \in \{0, 1\}$,其中 $a(t) = 1$ 表示在 t 个时间点发生异常。

1.2 方法框架

本文所提出的方法主要包括两个核心阶段:模型训练与结果预测。

在模型训练阶段,本文采用如图 1 所示的方法框架,该框架融合了图结构学习与图注意力预测机制,旨在通过探索传感器间的复杂关联性预测时序数据。

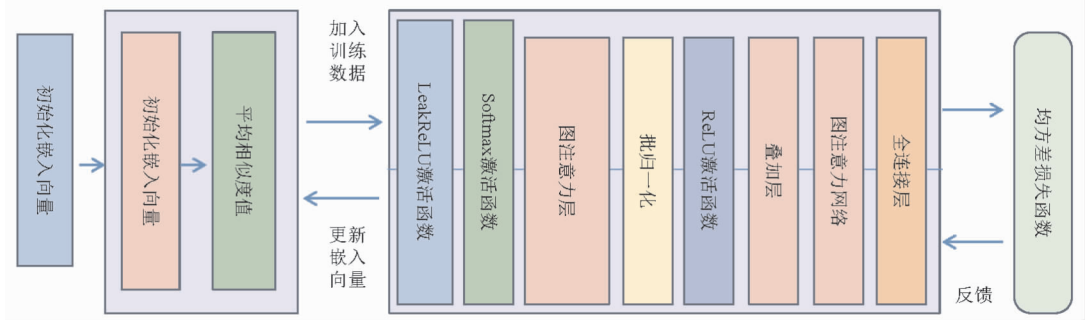


图 1 训练阶段框架图
Fig. 1 Framework diagram for the training phase

该框架首先初始化传感器节点并分配嵌入向量以捕捉潜在关系。随后,计算节点相似度并构建相似度矩阵,引入 Leaky ReLU 激活函数以增强非线性与防止梯度消失。在图注意力层中,利用相似度矩阵和节点特征计算注意力权重,以捕捉传感器间的复杂关联性。之后,通过批归一化和 ReLU 激活函数加速训练并增强泛化能力。为了捕获高阶信息,叠加多个图注意力层构建图注意力网络(GAT)。最终,通过全连接层映射节点表示到预测目标空间,并采用均方误差(MSE)作为损失函数优化预测结果。

在结果预测阶段,采用异常得分与阈值搜索相结合的策略,以有效地识别异常数据点。具体而言,通过计算异常得分能够准确识别测试数据集中的异常点。为了确立一个合适的异常阈值,用区间搜索法寻找一个能够准确区分正常数据与异常数据的固定阈值。该方法提升了异常检测的准确性。

1.3 图结构学习

考虑到不同传感器具有各自的特性,将每个传感器表示为低维向量 $\mathbf{v}_i \in \mathbf{R}^d, i \in \{1, 2, \dots, N\}$, 其中 N 为传感器的数量。如果两个传感器在原始数据中有相似性,那么它们的嵌入向量在嵌入空间中也具有相应的相似性,这些嵌入向量在初始阶段被随机赋值,并在模型的训练过程中与模型参数一同进行优化和更新。

为了学习图结构,本文利用嵌入向量之间的相似关系。在这个图结构中,节点代表传感器,而边则反映了传感器间的依赖关系,使用邻接矩阵 $\mathbf{A}$ 来表示这个有向图结构,其中 $\mathbf{A}_{ij}$ 表示从节点 i 到节点 j 是否有有向边的存在。此外,引入 C_i 表示每个传感器 i 的先验信息,为除自身以外的所有传感器,即 $C_i \subseteq \{1, 2, \dots, N\} \setminus \{i\}$ 。为了确定传感器 i 的依赖关系,计算传感器 i 的嵌入向量与其候选关系 $j \in C_i$ 的多种相似度度量,包括归一化欧式距离相似度 e_{ji1} 、余弦相似度 e_{ji2} 、皮尔逊相关系数 e_{ji3} 。

$$e_{ji1} = \sqrt{\|\mathbf{v}_i - \mathbf{v}_j\|_2} \quad (1)$$

$$e_{ji1} = \frac{(1 - e_{ji1}) - \min(1 - e_{ji1})}{\max(1 - e_{ji1}) - \min(1 - e_{ji1})} \quad (2)$$

$$e_{ji2} = \frac{\mathbf{v}_i^T \mathbf{v}_j}{\|\mathbf{v}_i\| \cdot \|\mathbf{v}_j\|} \quad (3)$$

$$e_{ji3} = \frac{\text{cov}(\mathbf{v}_i, \mathbf{v}_j)}{\sigma_{v_i} \sigma_{v_j}} \quad (4)$$

其中: cov 为协方差; σ 为标准差。随后,为了综合考量 3 种不同方法所得到的相似度值,采用平均法对这些值进行汇总。通过计算这 3 种相似度值的平均数,期望得到一个更为稳健和全面的相似度度量,以更好地反映传感器之间的关联程度。

$$e_{ji} = (e_{ji1} + e_{ji2} + e_{ji3})/3 \quad (5)$$

该方法有助于在后续的图结构学习和异常检测任务中,提供更加准确和可靠的依据。

这 3 种相似度度量有不同的适用场景,如表 1 所示,通过对比 3 对模拟时序数据 $\sin(t)$ 与 $\cos(t)$ 、 $\sin(t)$ 与 $\sin(t) + 1$ 、 $\sin(t)$ 与 $2\sin(t) + 2$, 可以观察到不同相似度度量方式的表现。其中,第一列是相似度度量方式,分别对应式(1)~式(5)。这里向上的箭头表示值越高,样本之间的关联程度或相似性越强;向下的箭头表示值越低,样本之间的关联程度或相似性越强。从表 1 可以看出, $\sin(t)$ 和 $\sin(t) + 1$ 在图像上显示出最高的相似性;与 $\sin(t)$ 和 $\cos(t)$ 比较时,归一化欧式相似度值相同,但余弦相似度和皮尔逊相关系数却显示 $\sin(t)$ 与 $\cos(t)$ 之间的相似度更高,说明这种情况下余弦相似度和皮尔逊相关系数更能准确判断相似度的大小;与 $\sin(t)$ 和 $2\sin(t) + 2$ 比较时,余弦相似度和皮尔逊相关系数给出了相同的值,但归一化欧式相似度则显示 $\sin(t)$ 与 $\cos(t)$ 之间具有较高的相似度,表明这种情况下,归一化欧式相似度可能是判断相似度大小的更合适指标。通过计算平均相似度值,发现在 3 对不同时序数据的比较中,每个平均相似度值都是唯一的,且在第二组对比中达到最大。这验证了平均相似度在评估时序数据间相似度方面的有效性。

为了从 C_i 中筛选出真正存在依赖关系的传感器,本文选择前 K 个相似度值作为候选,

$$\mathbf{A}_{ji} = \mathbf{I} \{j \in \text{Top}K(\mathbf{e}_i; l \in C_i)\} \quad (6)$$

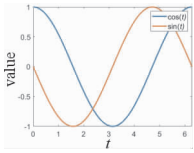
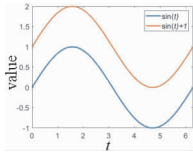
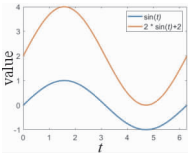
其中: l 为示性函数; K 值的选择取决于用户所需的稀疏度级别,从而实现了灵活且精确的依赖关系识别。

1.4 基于图注意力的预测

鉴于本文的主要焦点在于改进图结构学习和阈值搜索部分,采用了文献[11]中提出的基于图注意力的预测方法作为本节的框架。该方法的核心在于利用图注意力机制来预测每个传感器在特定时间点的预期行为,从而使用户能够轻松地识别出那些与其预期行为显著偏离的传感器。

表1 3种相似度量在不同场景下的对比

Tab.1 Comparison of three similarity measurements in different scenarios

相似度计算公式/ 时序数据			
欧式距离	25.079 9	25.079 9	53.199 2
归一化欧式相似度	1	1	-1
余弦相似度	0.000 003 451	0.577 14	0.577 14
皮尔逊相关系数	0.000 003 447	1	1
平均相似度	0.333 3	0.859 0	0.192 4

在 t 时刻,模型输入为 $\mathbf{x}^{(t)} = [\mathbf{s}^{(t-w)}, \mathbf{s}^{(t-w+1)}, \dots, \mathbf{s}^{(t-1)}]$, 其中 w 是滑动窗口大小, 预测的目标输出是当前时刻点的传感器数据 $\mathbf{s}^{(t)}$ 。为了有效地捕获传感器之间的复杂关系并做出准确预测, 引入了一个基于图注意力的特征提取器。这个特征提取器不仅能够捕捉传感器之间的相互作用, 还能通过全连接输出层来预测 t 时刻的传感器向量。

$$\mathbf{z}_i^{(t)} = \text{ReLU}(\alpha_{i,i} \mathbf{W} \mathbf{x}_i^{(t)} + \sum_{j \in N(i)} \alpha_{i,j} \mathbf{W} \mathbf{x}_j^{(t)}), \tag{7}$$

$$\mathbf{s}'^{(t)} = f_{\theta}(\mathbf{v}_1 \circ \mathbf{z}_1^{(t)}, \dots, \mathbf{v}_N \circ \mathbf{z}_N^{(t)}), \tag{8}$$

其中: $\mathbf{x}_i^{(t)}$ 为模型输入; $N(i) = \{j | A_{ji} > 0\}$; $\mathbf{W}$ 是训练得到的权重矩阵; $\circ$ 表示对应点乘; $\mathbf{s}'^{(t)}$ 为模型的预测输出; $\alpha_{i,j}$ 的计算公式为

$$\mathbf{g}_i^{(t)} = \mathbf{v}_i \oplus \mathbf{W} \mathbf{x}_i^{(t)} \tag{9}$$

$$\pi(i, j) = \text{Leaky ReLU}(\mathbf{a}^T (\mathbf{g}_i^{(t)} \oplus \mathbf{g}_j^{(t)})) \tag{10}$$

$$\alpha_{i,j} = \frac{\exp(\pi(i, j))}{\sum_{k \in N(i) \cup \{i\}} \exp(\pi(i, k))} \tag{11}$$

其中: $\oplus$ 表示串联; $\mathbf{a}$ 是注意机制的学习系数向量。在训练过程中, 采用均方误差 (mean squared error, MSE) 作为损失函数, 以量化预测值 $\mathbf{s}'^{(t)}$ 与观测值 $\mathbf{s}^{(t)}$ 之间的偏差。具体的损失函数公式为

$$L_{\text{MSE}} = \frac{1}{T_{\text{train}} - w} \sum_{t=w+1}^{T_{\text{train}}} (\mathbf{s}'^{(t)} - \mathbf{s}^{(t)})^2 \tag{12}$$

通过最小化这个损失函数, 能够训练出一个既能够准确捕捉传感器间关系又能够预测传感器行为的模型。

1.5 图偏差得分

本文提出的模型独立地计算每个传感器的异常分数, 并将这些分数综合成每个时间点的单一异常分数。该方法使用户能够准确定位到哪些传

感器在何时出现了异常。

为了计算异常得分, 模型将每个时间点 t 的预期传感器数据与实际观测数据进行比较, 从而得出该时间点 t 和传感器 i 的绝对偏差 Err_i 。随后, 通过应用最大值函数 (max) 对各个传感器的错误值进行聚合, 得到时间点 t 的整体异常分数。这种聚合方法有助于突出显示在任何给定时间点最为异常的传感器, 从而为用户提供有关传感器状态的关键信息。

$$Err_i(t) = |\mathbf{s}_i^{(t)} - \mathbf{s}'_i(t)| \tag{13}$$

$$A(t) = \max_i (Err_i(t)) \tag{14}$$

得到每个时间点的偏差得分后, 模型的下一步骤是利用这些异常得分进行固定阈值搜索。

1.6 阈值搜索

本节旨在通过设置一个合适的阈值, 对传感器数据进行分类从而区分出正常和异常的数据点。首先, 给了一个定理表明当阈值为 $\frac{F_1}{2}$ 时, F -measure 的值达到最大, 从而使分类器的整体性能最优。

定理 1 最大化 F -measure 的分类器

$$h_{F_1}^*(x) = \arg \max_h F_1(h) = \begin{cases} 1, \eta(x) > \frac{F_1^*}{2}; \\ 0, \text{其他。} \end{cases} \tag{15}$$

其中: $F_1^* = F_1(h_{F_1}^*)$ 。

用定义1、定义2和引理1、引理2去证明定理1。

定义 1^[21] 如果一个度量随 FP 、 FN 不增加, 并且形式化为

$$\psi(FP, FN) = \frac{a_0 + a_1 FP + a_2 FN}{b_0 + b_1 FP + b_2 FN} \tag{16}$$

则该度量称为线性分数性能度量, 其中 $a_0, a_1, a_2, b_0, b_1, b_2 \in \mathbf{R}, b_0 + b_1 FP + b_2 FN \geq C_1 > 0$ 。

定义 2^[22] 代价敏感损失定义为

$$L_p(h) = \rho FP(h) + (1 - \rho) FN(h)$$

(17)

其中: $\rho \in (0,1)$ 。

$$\text{引理 1}^{[21]} \quad \text{当 } \rho = \frac{\Psi^* b_1 - a_1}{\Psi^* (b_1 + b_2) - (a_1 + a_2)}$$

时,关于线性分数性能指标 $\psi(FP, FN)$ 的损失值可以由关于 L_p^* 的损失值界定。

$$\psi^* - \psi(h) \leq C_2 (L_p(h) - L_p^*)$$

(18)

其中: $\psi^* = \max_h \psi(h)$; $L_p^* = \min_h L_p(h)$; $C_2 = \frac{1}{C_1} (\psi^* (b_1 + b_2) - (a_1 + a_2))$ 。

引理 2^[22] 最小化 L_p 的分类器是

$$h_{L_p}^* = \begin{cases} 1, & \eta(x) > \rho; \\ 0, & \text{其他。} \end{cases}$$

(19)

其中: $\eta(x) = P(Y = 1 | X = x)$ 。

根据表 2 的混淆矩阵,给出了精度(Pre)、召回率(Rec)和 F_1 -score (F_1) 的公式。

$$pre = \frac{TP}{TP + FP}$$

(20)

$$rec = \frac{TP}{TP + FN}$$

(21)

$$F_1 = \frac{2 \times pre \times rec}{pre + rec}$$

(22)

表 2 混淆矩阵

Tab. 2 Confusion matrix

$h(x)/Y$	$Y = 1$	$Y = 0$	Total(h)
$h(x) = 1$	TP	FP	$q(h)$
$h(x) = 0$	FN	TN	$1 - q(h)$
Total(Y)	p	$1 - p$	1

根据定义 1 和引理 1 可以得到 $F_1 = \frac{2p-2FN}{2p-FN+FP}$ 和 F_1 的损失值可以以 $\rho = \frac{F_1}{2}$ 的 L_p 为界,其中 $p = P(Y = 1)$ 。然后根据引理 2,得到了定理 1。因此合适的阈值利用区间搜索方法来优化 F -measure 损失值($FL = 1 - F_1$) 设定。

Naeasimhan 等人证明为一个后验概率估计分配一个经验阈值可以优化以 TP 、 TN 和 p 的函数表示的性能度量^[23]。本文指出 F -measure 可以表达为以 TP 、 TN 和 p 为变量的函数。因此将异常得分转化为概率形式,采用了 sigmoid 函数进行处理,得到了后验概率的表达式。

$$\gamma(t) = \frac{1}{1 + e^{-A(t)}}$$

(23)

Chong 等人证明区间搜索方法在寻找单峰函

数局部最小值方面具有显著效率^[24]。为了验证阈值与异常检测性能 FL 之间的关系,图 2 展示了在模拟数据集上的实验结果。在此实验中,随机生成了 1 000 个介于 0 和 1 之间的数值,并根据预设的规则对这些数值进行标签化,将大于 0.6 的数值标记为 +1(代表异常),否则标记为 0(代表正常)。随后,应用算法 1 中的区间搜索法来寻找最佳的阈值,并计算相应的 FL 。这一过程的目的是探索不同阈值设置下,异常检测算法的性能 FL 的表现。图 2 直观地展示了阈值与 FL 之间的关系,可以观察到 FL 随阈值变化呈现单峰特性。因此,本文用区间搜索法来优化 FL 的阈值。区间搜索法得到的最优阈值为 δ^* 。根据定理 1,有

$$\delta^* = \frac{F_1^*}{2} = \frac{1 - FL^*}{2}$$

(24)

其中: F_1^* 是 F -measure 的最大值; FL^* 是 F -measure 损失的最小值。然后将 plug-in 规则表示为

$$h_r(t) = \text{sign}(\gamma(t) - (1 - r)/2)$$

(25)

其中,sign 表示符号函数,并应用区间搜索方法来寻找最小化 $FL(h_r(x))$ 的最优 r 。实现区间搜索法优化 FL 阈值的具体算法如算法 1 所示,采用了间隔减少方法,每次迭代中,区间长度减少比率 $\zeta \in (0,0.5)$ 。该算法通过迭代搜索的方式,在指定的区间内寻找能够使 FL 达到最小值的阈值。

最终,如果某个时间刻度 t 的异常得分超过了预设的固定阈值,则该时间刻度将被标记为异常。

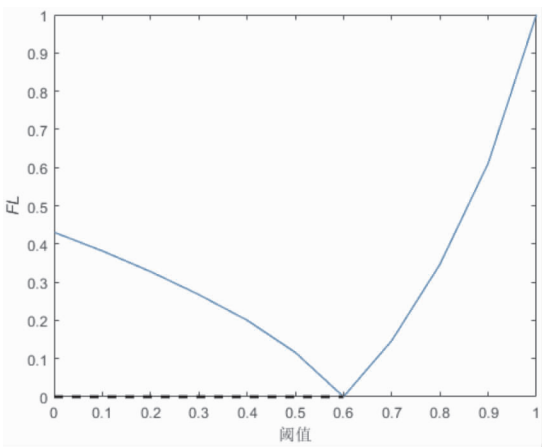


图 2 阈值与 FL 的关系图

Fig. 2 The relationship graph between threshold and FL

算法 1 最小化 FL 的区间搜索算法。

输入:后验概率 $\gamma(t)$;验证集 S_N

令 $a = 0, b = 1, \zeta$ 为区间长度减少比率, v 停

止条件,sign 是符号函数。

输出:最优阈值 δ^*

① 令 $\lambda = a + \zeta(b - a), \mu = b - \zeta(b - a)$

② $h_\lambda(t) = \text{sign}(\gamma(t) - (1 - \lambda)/2), h_\mu(t) = \text{sign}(\gamma(t) - (1 - \mu)/2)$

③ 在 S_N 上计算 $FL(h_\lambda, Y)$ 和 $FL(h_\mu, Y)$

④ while $b - a > v$, do

⑤ if $FL(h_\lambda, Y) < = FL(h_\mu, Y)$

⑥ $b = \mu$

⑦ else

⑧ $a = \lambda$

⑨ end if

⑩ $\lambda = a + \zeta(b - a), \mu = b - \zeta(b - a)$

⑪ 在 S_N 上计算 $FL(h_\lambda, Y)$ 和 $FL(h_\mu, Y)$

⑫ $\delta = (1 - \lambda)/2$

⑬ end while

2 实验分析

本节将在 2 个公开数据集上进行 3 个实验来全面分析本文提出的异常检测方法的有效性。

实验一:将本文方法与多种主流的异常检测算法进行比较,评估其在 Pre 、 Rec 和 F_1 指标上的表现。

实验二:为了验证相似度度量集成的有效性,将从集成相似度度量的角度出发,将本文方法与 GDN 方法进行对比。

实验三:为了验证区间阈值搜索策略的有效性,用不同阈值搜索方法进行比较,评估其在 Pre 、 Rec 和 F_1 指标上的表现。

接下来将详细介绍基于图神经网络的时序信号异常检测方法进行实验的内容。

2.1 数据集

实验中使用了 2 个基于水处理物理试验台系统的传感器数据集(见表 3): SWAT^[25] (secure water treatment) 和 WADI^[26] (water distribution)。本实验将数据集划分为训练集、验证集和测试集,比例为 3: 5: 2。训练集仅包含正常状态下的数据,而验证集和测试集则包含正常与异常状态数据,以全面评估模型性能。鉴于数据采集频率与计算效率考量,实施了降采样策略,每 10 s 选取一次测量值作为样本。在确定样本标签时,依据 10 s 内出现频率最高的标签作为该时间段的代表。为保持与已有研究的一致性,剔除了 2 个

数据集的前 2 160 个样本。这些预处理步骤旨在提升数据集的质量和模型的性能。

表 3 两个数据集的描述

Tab. 3 Description of two datasets

数据集	特征数	训练集个数	验证集个数	测试集个数	异常比例/%
SWAT	50	28 506	45 996	17 994	11.97
WADI	127	40 821	68 035	27 214	5.99

2.2 实验设置

模型使用 Adam 优化器学习率为 1×10^{-3} 进行训练; epoch 为 50, 使用 10 的早期停止, 具体为在连续 10 个 epoch 内模型性能未有明显提升时停止训练。对于 WADI 和 SWAT 数据集, 嵌入向量长度为 128 和 64, k 为 30 和 15, 神经元的隐藏层为 128 和 64, BATCH SIZE 为 32 和 16, 滑动窗口大小 w 都为 5。为了与 GDN 方法进行公平比较, 本实验在参数设置上尽量保持与 GDN 方法一致, 以确保实验结果的可靠性和有效性。

2.3 评价指标

实验使用测试数据集上的 Pre 、 Rec 和 F_1 作为评估指标, 如式(19) ~ 式(21)所示, 全面评价本文提出的异常检测方法以及基准对比方法的性能。同时, 还通过比较使用不同阈值搜索方法的实验结果, 来探究阈值搜索策略对模型性能的影响。

2.4 本文方法与主流异常检测算法的性能对比

为了评估本文提出的异常检测方法的性能表现, 选择了 8 种当前流行的异常检测算法作为基准对比方法。这些算法包括: USAD^[27], ADD^[28], AE^[29], DAGMM^[30], IF^[31], LSTM-VAE^[32], LSTM-GAN^[33], GDN^[11]。

在表 4 中展示了在 SWAT 和 WADI 数据集上, 本文方法和基准对比方法在 Pre 、 Rec 和 F_1 3 个评价指标的异常检测结果。为了更清晰地呈现结果, 在表中将每个评价指标下的最高值进行了加粗处理。

因为 F_1 是 Pre 和 Rec 的加权平均值, 它能够全面反映模型的整体性能表现, 因此在比较不同模型性能时, 主要侧重于对 F_1 的分析。从表 4 的实验结果来看, 本文提出的方法在 2 个数据集上的 F_1 均超过了基准方法, 同时在精度和召回率方面也取得了较高的数值。值得注意的是, SWAT

和 WADI 数据集均为高维度且不平衡的数据集,如表 3 所示,这种特性在实际应用中尤为常见。本文方法在高维度及不平衡数据场景下依然表现出色,充分证明了其在实际应用中的有效性和实用性。

表 4 SWAT 和 WADI 数据集上与基准方法对比结果
Tab. 4 Comparison results with baseline methods on the SWAT and WADI datasets

SWAT			
方法	F_1	Pre	Rec
DAGMM	0.393 7	0.274 6	0.695 2
IF	0.493 3	0.803 0	0.356
AE	0.610 3	0.726 3	0.526 3
LSTM-VAE	0.738 5	0.962 4	0.599 1
ADD	0.769 9	0.980 0	0.634 0
LSTM-GAN	0.775 4	0.989 7	0.637 4
GDN	0.796 9	0.992 4	0.665 8
USAD	0.834 0	0.979 0	0.727 0
本文方法	0.871 8	0.829 0	0.919 2

WADI			
方法	F_1	Pre	Rec
DAGMM	0.360 9	0.544 4	0.269 9
IF	0.387 9	0.993 0	0.241 0
AE	0.343 5	0.343 5	0.343 5
LSTM-VAE	0.248 2	0.877 9	0.144 5
ADD	0.554 8	0.890 0	0.403 0
LSTM-GAN	0.373 0	0.414 4	0.339 2
GDN	0.459 2	0.645 2	0.356 4
USAD	0.423 0	0.644 0	0.316 0
本文方法	0.580 8	0.565 9	0.596 5

注:表中部分结果来自文献[11,34]。

2.5 相似度量集成有效性验证

为了验证集成相似度量在异常检测中的有效性,对本文提出的方法与 GDN 方法在 SWAT 和 WADI 数据集上进行了比较,特别关注了仅包含正常数据的验证集的预测结果。如图 3 和图 4 所示,在 SWAT 和 WADI 数据集上展示了部分传感器在相似度量集成前后的观测与预测数据。(a)~(d)展示了使用单一相似度度量的预测结

果,即 GDN 方法。在这些子图中,蓝色曲线表示观测数据,红色曲线表示预测数据。横轴代表时间点,纵轴表示传感器在 t 时刻的值。相应地,(e)~(h)展示了使用 3 种相似度量集成后的预测结果,即本文的方法。值得注意的是,(a)(e)、(b)(f)、(c)(g)和(d)(h)分别对应相同的传感器。通过比较(a)~(d)与(e)~(h)中的红色和蓝色曲线,可以观察到集成相似度量后的预测结果与观测结果更为接近。此外,集成后的异常得分明显较低,这进一步验证了集成相似度量在异常检测中的有效性。

图 5 则展示了在仅包含正常数据的验证集上,所有传感器在整个验证集时间范围内的相似度量集成前后的总体异常得分。横轴代表传感器,纵轴代表传感器的异常得分。其中,蓝色表示相似度量集成后的结果,红色表示使用单一相似度度量的结果。

对图 5 的分析显示,在图 5(a)中,总共有 50 个柱状图,其中蓝色柱状图(代表集成后的结果)低于红色柱状图(代表单一相似度度量的结果)的数量为 37。类似地,在图 5(b)中,总共有 128 个柱状图,其中蓝色柱状图低于红色柱状图的数量为 79。结果表明,在大多数情况下,相似度量集成后的总体异常得分低于单一相似度度量的得分,从而验证了集成方法在异常检测中的优势。

图 3~图 5 所展示的结果充分证实了相似度量集成在降低整体异常得分、提升模型预测能力以及优化模型预测效果方面的有效性。通过集成多种相似度量,能够实现更为准确的异常检测,从而增强模型在复杂环境下的适应性。

2.6 不同阈值搜索方法对本文方法性能的影响

为了探究区间搜索法在异常检测中的性能表现,将其与 GDN 方法、大津法和二分查找法 3 种阈值选择方法进行对比。GDN^[11]方法是 将正常数据最高偏差得分作为阈值;大津法^[35]是一种基于类间方差最大化的阈值选择方法,它将数据分为两类,一类大于等于阈值,一类小于阈值,通过最大化两类之间的方差来确定最优阈值;二分查找法则是一种经典的搜索算法,它从数据集的中间元素开始搜索,根据中间元素与目标值的比较结果,在相应的数据子集中继续搜索,重复这一过程直到找到目标元素。

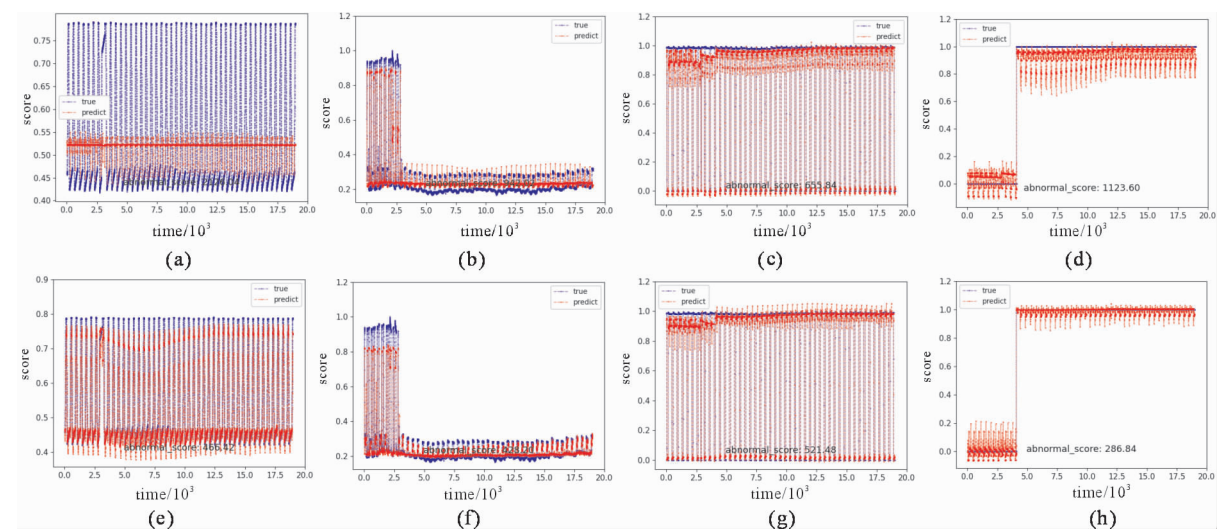


图 3 SWAT 数据集部分传感器相似度量集成前后的观测与预测数据

Fig. 3 Observation and prediction data before and after sensor similarity integration in the SWAT dataset

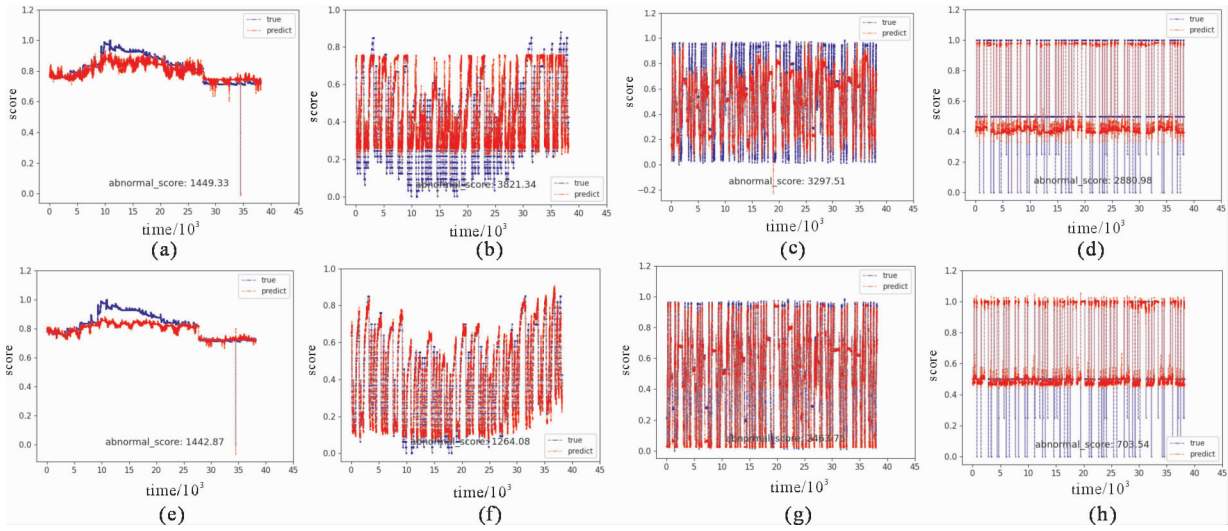


图 4 WADI 数据集部分传感器相似度量集成前后的观测与预测数据

Fig. 4 Observation and prediction data before and after sensor similarity integration in the WADI dataset

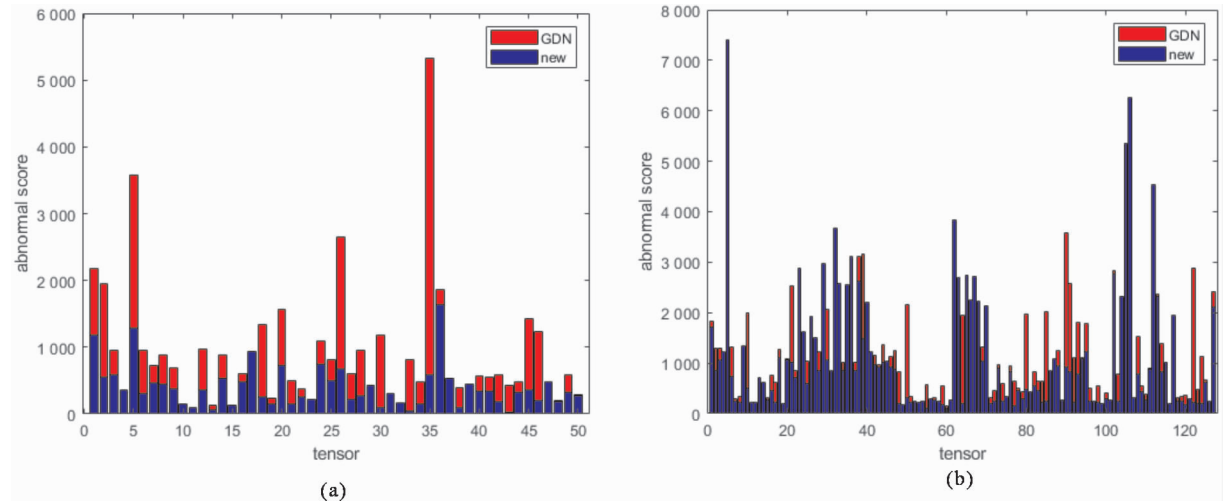


图 5 SWAT 和 WADI 数据集全部传感器相似度量集成前后的异常得分

Fig. 5 Anomaly scores before and after integrating the similarity of all sensors in the SWAT and WADI datasets

表 5 中展示了在 SWAT 和 WADI 2 个数据集上,分别使用上述 4 种方法来确定最优阈值,并基于该阈值计算了 Pre 、 Rec 和 F_1 3 个评价指标的异常检测结果。为了更直观地展示性能差异,将每个指标下的最高值进行了加粗处理。

表 5 SWAT 和 WADI 数据集上寻找阈值不同方法对比结果

Tab. 5 Comparison of different methods for finding thresholds on SWAT and WADI datasets

SWAT			
方法	F_1	Pre	Rec
GDN 方法	0.796 9	0.992 4	0.665 8
二分查找法	0.838 5	0.772 4	0.917 0
大津法	0.846 5	0.793 4	0.907 3
区间搜索法	0.871 8	0.829 0	0.919 2

WADI			
方法	F_1	Pre	Rec
GDN 方法	0.459 2	0.645 2	0.356 4
二分查找法	0.577 0	0.558 8	0.596 5
大津法	0.578 9	0.620 9	0.542 2
区间搜索法	0.580 8	0.565 9	0.596 5

从表 5 的实验结果可以看出,本文提出的异常检测方法在 F_1 上,无论是在 SWAT 还是 WADI 数据集上,均优于 GDN 方法、大津法和二分查找法。同时,在精度和召回率方面,本文方法也取得了较高的数值。这些结果充分证明了区间阈值搜索策略的有效性。

3 结语

本文深入探讨了高维时序数据中的异常检测问题,特别是在多元时间序列背景下,如何有效识别那些偏离整体模式或预期行为的样本点。在高维时序数据的分析中,传感器间的潜在关联关系对于预测和异常检测任务的性能具有决定性作用。针对这一挑战,本文提出了一种基于图神经网络的时序信号异常检测方法。

首先,现有基于图神经网络的异常检测方法在捕捉多变量间复杂关系时存在局限性,尤其是它们往往依赖于单一的相似度量。为了克服这一局限,本文提出的方法结合传感器的特有特征,采用多种相似度量集成的方式来进行图结构学

习。该方法能够更全面地捕获传感器间的复杂依赖关系,从而为后续的图神经网络学习提供更为丰富和准确的信息。

其次,本文将图结构学习方法与图神经网络模型相结合,旨在通过图神经网络在处理复杂关系数据方面的优势,实现对时序信号行为的精确预测,并基于预测结果构建出高效的异常评分机制。这一步骤不仅显著提升了异常检测的准确性,还增强了模型对异常事件的敏感性。

最后,为了克服传统方法中固定阈值的局限性,本文采用了区间搜索法来最优化 F -measure 指标,从而自适应地确定最优的异常切割阈值。该方法能够根据数据的实际情况灵活调整阈值,有效提高了异常检测的召回率。

在两个真实传感器数据集上进行的实验表明,本文所提出的方法在 F_1 值和召回率方面均取得了显著的提升。与基准对比方法相比,本文方法在指标上表现出色,充分证明了多种相似度量集成和区间搜索法寻找阈值的有效性。

综上所述,本文的研究为高维时序数据的异常检测提供了一种新的视角和方法,并展示了图神经网络在处理复杂关系数据时的能力。文中相似度集成主要采用了简单的算术平均方法,而未来工作将探索加权平均等更先进的融合方法。此外,本文在运用区间搜索法确定最优阈值时,考虑的是阈值与异常检测性能之间的单峰关系。当面向复杂的现实应用场景时,异常的出现可能呈现多模式特性,导致阈值与异常检测性能之间的关系呈现多峰状态,本文方法可能无法准确识别在多峰情况下的异常。因此,未来的研究将探索更为先进的方法,以识别并适应可能出现的多峰性能,进而提升异常检测算法在多模态异常场景中的应用潜力。

参考文献

[1] SHYU M, CHEN S, SARINNAPAKORN K, et al. A novel anomaly detection scheme based on principal component classifier [C] // Proc Icdm Foundation & New Direction of Data Mining Workshop. Melbourne, FL, USA: IEEE, 2003: 353-365.

[2] ANGIULLI F, PIZZUTI C. Fast outlier detection in high dimensional spaces[C] // Principles of Data Mining and Knowledge Discovery. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002: 15-27.

[3] BREUNIG M M, KRIEGEL H P, NG R T, et al.

- LOF: Identifying density-based local outliers [J]. ACM SIGMOD Record, 2000, 29(2): 93-104.
- [4] SCHÖLKOPF B, PLATT J C, SHAWE-TAYLOR J, et al. Estimating the support of a high-dimensional distribution[J]. Neural Computation, 2001, 13(7): 1443-1471.
- [5] HU M, FENG X W, JI Z W, et al. A novel computational approach for discord search with local recurrence rates in multivariate time series[J]. Information Sciences, 2019, 477: 220-233.
- [6] KHOSHNEVISAN F, FAN Z W, CARVALHO V R. Improving robustness on seasonality-heavy multivariate time series anomaly detection[EB/OL]. (2020-07-25) [2024-05-10]. <https://arxiv.org/abs/2007.14254v1>.
- [7] SU Y, ZHAO Y J, NIU C H, et al. Robust anomaly detection for multivariate time series through stochastic recurrent neural network[C]//Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. Anchorage AK USA:ACM, 2019: 2828-2837.
- [8] ZHANG Z J, LI W Z, DING W X, et al. STADGAN: Unsupervised anomaly detection on multivariate time series with self-training generative adversarial networks[J]. ACM Transactions on Knowledge Discovery from Data, 2023, 17(5): 1-18.
- [9] YAN K, LI W, JI Z W, et al. A hybrid LSTM neural network for energy consumption forecasting of individual households[J]. IEEE Access, 2019, 7: 157633-157642.
- [10] CHEN Z K, CHEN D S, ZHANG X, et al. Learning graph structures with transformer for multivariate time-series anomaly detection in IoT[J]. IEEE Internet of Things Journal, 2022, 9(12): 9179-9189.
- [11] DENG A L, HOOI B. Graph neural network-based anomaly detection in multivariate time series[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2021, 35(5): 4027-4035.
- [12] SHEN L, LI Z, KWOK J. Timeseries anomaly detection using temporal hierarchical one-class network[J]. Neural Information Processing Systems, 2020, 33: 13016-13026.
- [13] HE Y D, ZHAO J B. Temporal convolutional networks for anomaly detection in time series[J]. Journal of Physics: Conference Series, 2019, 1213(4): 042050.
- [14] DING N, GAO H B, BU H Y, et al. RADM: Real-time anomaly detection in multivariate time series based on Bayesian network[C]//2018 IEEE International Conference on Smart Internet of Things. Xi'an, China: IEEE, 2018: 129-134.
- [15] SHANG C, CHEN J, BI J B. Discrete graph structure learning for forecasting multiple time series[EB/OL]. (2021-04-21) [2024-05-10]. <https://arxiv.org/abs/2101.06861v3>.
- [16] ROSSI E, CHAMBERLAIN B, FRASCA F, et al. Temporal graph networks for deep learning on dynamic graph[EB/OL]. (2020-10-09) [2024-05-10] <https://arxiv.org/abs/2006.10637v3>.
- [17] VELICKOVIC P, CUCURULL G, CASANOVA A, et al. Graph attention networks[EB/OL]. (2018-02-04) [2024-05-10]. <https://arxiv.org/abs/1710.10903v3>.
- [18] 丁小欧, 于晟健, 王沐贤, 等. 基于相关性分析的工业时序数据异常检测[J]. 软件学报, 2020, 31(3): 726-747.
- DING X O, YU S J, WANG M X, et al. Abnormal detection of industrial time-series data based on correlation analysis[J]. Journal of Software, 2020, 31(3): 726-747.
- [19] 卢光曦. 基于图神经网络的目标检测与识别算法研究[D]. 西安:西安电子科技大学, 2022.
- [20] WANG J T, QIAN Y H, LI F J. Learning with mitigating random consistency from the accuracy measure[J]. Machine Learning, 2020, 109(12): 2247-2281.
- [21] KOTŁOWSKI W, DEMBCEZYŃSKI K. Surrogate regret bounds for generalized classification performance metrics[J]. Machine Learning, 2017, 106(4): 549-572.
- [22] ELKAN C. The foundations of cost-sensitive learning[J]. Proceedings of the International Joint Conference on Artificial Intelligence, 2001, 17: 973-978.
- [23] NAEASIMHAN H, VAISH R, AGARWAL S. On the statistical consistency of plug-in classifiers for non-decomposable performance measures[J]. In Proceedings of the 27th International Conference on Neural Information Processing Systems, 2014, 1: 1493-1501.
- [24] CHONG E K P, ZAK S H. An introduction to optimization. 3rd ed[M]. New York: Wiley, 2011.
- [25] MATHUR A P, TIPPENHAUER N O. SWAT: A water treatment testbed for research and training on ICS security[C]//2016 International Workshop on Cyber-physical Systems for Smart Water Networks. Vienna, Austria. IEEE, 2016: 31-36.
- [26] AHMED C M, PALLETI V R, MATHUR A P. WADI: A water distribution testbed for research in the design of secure cyber physical systems[C]//Proceedings of the 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks. Pittsburgh

- Pennsylvania: ACM, 2017: 25-28.
- [27] AUDIBERT J, MICHIARDI P, GUYARD F, et al. USAD: Unsupervised anomaly detection on multivariate time series [C] // Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. Virtual Event CA USA: ACM, 2020: 3395-3404.
- [28] DAS S, WONG W K, DIETTERICH T, et al. Incorporating expert feedback into active anomaly discovery [C] // 2016 IEEE 16th International Conference on Data Mining. Barcelona, Spain: IEEE, 2016: 853-858.
- [29] FERNANDO B. Outlier analysis [J]. Computing reviews, 2014: 55-10.
- [30] ZONG B, SONG Q, MIN M R, et al. Deep autoencoding gaussian mixture model for unsupervised anomaly detection [C] // International Conference on Learning Representations, 2018: 1-19.
- [31] LIU F T, TING K M, ZHOU Z H. Isolation forest [C] // 2008 Eighth IEEE International Conference on Data Mining. Pisa, Italy: IEEE, 2008: 413-422.
- [32] PARK D, HOSHI Y, KEMP C C. A multimodal anomaly detector for robot-assisted feeding using an LSTM-based variational autoencoder [J]. IEEE Robotics and Automation Letters, 2018, 3(3): 1544-1551.
- [33] LI D, CHEN D C, JIN B H, et al. MAD-GAN: Multivariate anomaly detection for time series data with generative adversarial networks [C] // Artificial Neural Networks and Machine Learning, ICANN 2019: Text and Time Series. Cham: Springer International Publishing, 2019: 703-716.
- [34] ZHANG W Q, ZHANG C, TSUNG F. GRELEN: Multivariate time series anomaly detection from the perspective of graph relational learning [C] // Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence. Vienna, Austria: International Joint Conferences on Artificial Intelligence Organization, 2022: 2390-2397.
- [35] LI F J, QIAN Y H, WANG J T, et al. Clustering ensemble based on sample's stability [J]. Artificial Intelligence, 2019, 273: 37-55.

(编辑 张欢)