doi:10.11887/j.cn.202503004 http://journal.nudt.edu.cn

面向缺失多元时间序列的图神经网络异常检测算法

高 杨[1],王新宇[1],贺 达[2],宋明黎[1],周春燕[3*]
(1. 浙江大学 计算机科学与技术学院,浙江 杭州 310027;2. 浙江大学 软件学院,浙江 宁波 315048;
3. 浙江省平安建设大数据重点实验室,浙江 杭州 310016)

摘 要:针对真实物联网环境中的缺失多元时间序列异常检测难题,提出一种融合缺失信息图嵌入的多元时间序列异常检测算法;基于预插值与异常检测任务融合的联合学习框架,设计一个基于时序高斯核函数的图神经网络(graph neural network, GNN)预插值模块,实现了预插值与异常检测任务的共同优化;提出一种时间序列数据缺失信息嵌入的图结构学习方法,采用图注意力机制融合缺失信息掩蔽矩阵和时空特征向量,有效建模多元时间序列缺失数据分布的潜在联系。在真实物联网传感器数据集上验证了提出算法的性能,实验结果表明,该方法在缺失多元时间序列异常检测任务上显著优于主流两阶段方法,预插值模块对比实验部分充分证明了基于高斯核函数的GNN预插值层的有效性。

关键词:多元时间序列;异常检测;图神经网络;预插值
中图分类号:TP183 **文献标志码**:A **文章编号**:1001-2486(2025)03-032-09

论文拓展

Anomaly detection algorithm based on graph neural network for missing multivariate time series

GAO Yang[1], *WANG Xinyu*[1], *HE Da*[2], *SONG Mingli*[1], *ZHOU Chunyan*[3*]
(1. College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China;
2. School of Software Technology, Zhejiang University, Ningbo 315048, China;
3. Zhejiang Provincial Key Laboratory of Social Security Governance Big Data, Hangzhou 310016, China)

Abstract: Addressing the issue of anomaly detection on missing multivariate time series data in real IoT(Internet of things) environments, a novel method on multivariate time series anomaly detection algorithm intergrated with graph embedding of missing information was proposed. Using a joint learning framework of pre-interpolation and anomaly detection task fusion, a GNN(graph neural network) pre-interpolation module based on time series Gaussian kernel function was designed to realize the joint optimization of pre-interpolation and anomaly detection task. A graph structure learning method for embedding missing information in time series data was proposed, using graph attention mechanism to fuse missing information masking matrix and spatiotemporal feature vectors, effectively modeling the potential connections of missing data distribution in multivariate time series. The performance of the algorithm was verified on real IoT sensor datasets. Experimental results prove that the proposed method significantly outperform the mainstream two-stage methods on the task of missing multivariate time series anomaly detection. The comparative experiment of the pre-interpolation module fully prove the effectiveness of the GNN pre-interpolation layer based on the Gaussian kernel function.

Keywords: multivariate time series; anomaly detection; graph neural network; pre-interpolation

时间序列异常检测是数据挖掘领域的重要研究方向,在传感器故障检测[1]、临床诊断[2]、网络入侵检测[3]和企业财务预测[4]等场景有着广泛的应用。随着物联网、大数据与人工智能技术的快速发展,车联网、工业物联网和数据中心也逐渐推广开来,具有复杂耦合关系的传感器设备产生了大量多元时间序列数据,这些时间序列数据之间普遍存在联系,对时间序列异常检测任务带来了新的挑战。除此以外,在真实物联网环境中,传感器缺陷和网络通信故障情况普遍存在,时常会

收稿日期:2023-12-03
基金项目:浙江省"领雁"研发攻关计划资助项目(2024C01114);国家自然科学基金联合基金重点资助项目(U20B2066)
第一作者:高杨(1991—),男,江苏扬州人,博士研究生,E-mail:roygao@zju.edu.cn
***通信作者**:周春燕(1972—),女,浙江诸暨人,正高级工程师,硕士,E-mail:hzgazcy@163.com
引用格式:高杨,王新宇,贺达,等. 面向缺失多元时间序列的图神经网络异常检测算法[J]. 国防科技大学学报, 2025, 47(3): 32-40.
Citation: GAO Y, WANG X Y, HE D, et al. Anomaly detection algorithm based on graph neural network for missing multivariate time series[J]. Journal of National University of Defense Technology, 2025, 47(3): 32-40.

导致数据在采集、传输过程中出现缺失[5],如何在部分数据缺失的情况下进行多元时间序列异常检测是非常值得研究的问题。

在早期的科研工作中,因为异常样本标记数据的缺乏,研究者普遍采用无监督的统计学习方法来进行异常检测,比如高斯混合模型[6]、基于距离的聚类方法[7]和单分类支持向量机[8](one-class support vector machine, one-class SVM)等。这类方法通常基于整体的数据分布来识别异常,并没有充分考虑时间序列的上下文关联性和传感器数据的高维特性,极大地影响了异常检测任务的性能[9]。伴随着深度学习技术的快速发展,许多深度模型被提出并应用到了时间序列异常检测问题上,这些方法通常可以被分为两大类:基于重构误差的方法和基于预测的方法[10]。前者的典型方法是自动编码器(autoencoder, AE)[11],它使用重构误差来度量样本间的异常程度;后者的典型方法是长短期记忆(long short-term memory, LSTM)网络[12],它采用独特的门设计,可以有效建模时间序列中的上下文信息。但是这些方法都是为单一时间序列设计的,忽视了多元时间序列之间的空间联系,无法有效建模不同时间序列间的关联关系,在复杂耦合传感器互联网络中的应用受到了限制。

为了解决这些问题,Yan 等[13]提出了图神经网络(graph neural network, GNN),它是一种可以利用深度学习方法直接对图结构数据学习的框架,对于多元关系的建模表现出了优异的性能。鉴于 GNN 的成功,研究者基于 GNN 提出了一系列新的算法,比如引入卷积层设计的图卷积神经网络[14](graph convolution neural networks, GCNs)、加入注意力机制的图注意力神经网络(graph attention neural networks, GATs)等[15,9]。然而这类方法也存在不足,由于在建模过程中没有考虑到真实物联网环境中广泛存在的数据缺失问题,在实际应用时通常会采用先进行缺失值插值再异常检测的两阶段方法[16]。因为插值阶段和异常检测阶段的优化目标并不相同,插值结果会极大地影响异常检测的最终效果。除此以外,先插值再异常检测的两阶段方法对于深度学习模型的训练、部署和决策等运维过程也带来了更多的成本开销。

综上所述,现有算法在部分数据缺失情况下进行多元时间序列异常检测时,会出现时空信息建模不充分、插值过程影响异常检测任务性能等问题。针对这些不足,本文提出一种融合缺失信息图嵌入的多元时间序列异常检测算法:基于预插值与异常检测任务融合的联合学习框架,在补全缺失时间序列信息的同时,保证预插值与异常检测任务共同优化;采用时间序列数据缺失信息嵌入的图结构学习方法,充分建模邻域传感器缺失数据分布的潜在关联;最后,模型基于学习到的多元时间序列时空嵌入向量进行预测,基于预测偏差值进行异常检测。

1　融合缺失信息图嵌入的多元时间序列异常检测

1.1　问题背景

在工业物联网环境中,为了高效地运维管理各类生产设施,通常部署着许多传感器设备。这些传感器设备按照预设的采样频率持续监控采集各种系统环境数据,会产出多组按照时间排序的随机变量,即多元时间序列[5]。这些传感器在物理空间或者信息空间可能存在着某种复杂、非线性的关联关系,例如温度变化会导致气压变化,多元时间序列也存在着内部潜在关联。由于真实物联网环境的复杂性,传感器缺陷和网络通信故障不可避免,产生的多元时间序列往往存在数据缺失现象,这给面向多元时间序列的异常检测任务带来了巨大的挑战。

1.1.1　多元时间序列异常检测

通过对多元时间序列进行异常检测,可以有效地识别异常数据背后隐含的设备故障问题,帮助运维人员尽快诊断和排除风险。传统的传感器监测系统通常由系统专家为每个监控信号设定正常响应的阈值区间,如果信号响应超过了专家定义的阈值,就会被系统判定为异常。

典型的多元时间序列异常检测场景如图 1 所示,3 个位移传感器位于相邻区域,所产生的时间序列也表现出相似的数据分布,并没有发生数据缺失。图中红色虚线表示系统专家为传感器 3 设定的正常响应区间。传感器 3 在 2 s 时的信号响

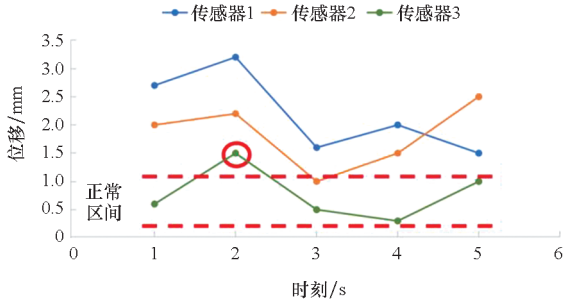

图 1　多元时间序列异常检测

Fig. 1　Anomaly detection of multivariate time series

应超出了该区间,红色圆圈表示的异常点可以被有效识别。

1.1.2 缺失多元时间序列异常检测

在真实物联网环境中,考虑到网络通信故障、传感器缺陷等原因,多元时间序列在采集、传输、加载过程中不可避免会出现数据缺失问题,传统方法通常会基于缺失时间序列的数据分布信息进行插值填补缺失数据,再进行异常检测。

如图 2 所示,传感器 3 在 2 s 时的异常数据出现了缺失,传统方法会基于传感器 3 自身的单一时间序列信息插值填补再检测异常,但由于填补数据处于正常响应区间内,缺失的异常点并不能被有效识别,潜在风险会被忽视。

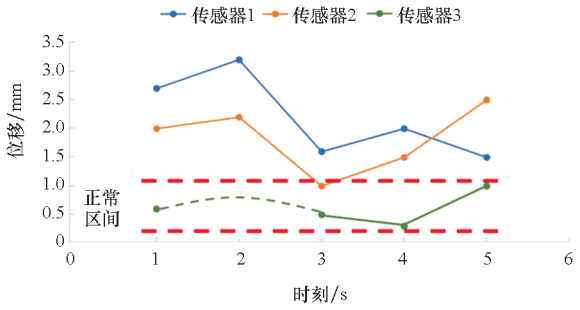

图 2 基于时序信息插值的异常检测

Fig. 2 Anomaly detection based on temporal information interpolation

传感器 3 与传感器 1、2 在空间区域中距离接近,因此其信号响应在时间轴上会表现出相似的数据分布。如图 3 所示,3 个传感器在 2 s 时的响应值都偏高,融合多元时间序列的时序信息和空间信息进行插值,能够极大提高填补数据的精准度,有效缓解数据缺失对最终异常检测任务的影响,识别出潜在风险。

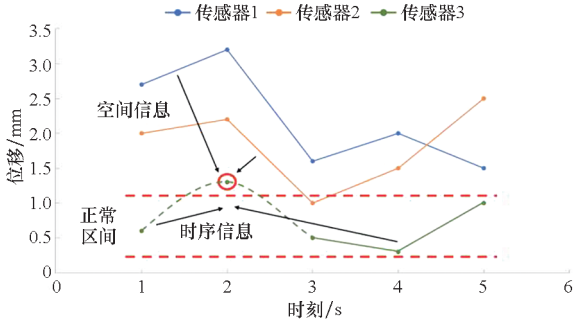

图 3 基于时空信息插值的异常检测

Fig. 3 Anomaly detection based on spatio-temporal information interpolation

针对上述问题,研究了部分数据缺失情况下的多元时间序列异常检测问题,本文提出一种融合缺失信息图嵌入的图神经网络算法。该算法采用预插值与异常检测任务融合的联合学习框架,融合多元时间序列数据缺失信息进行图结构学习,与当前两阶段的图异常检测方法相比,能够充分建模缺失多元时间序列的时空关联信息,减少插值过程对异常检测任务的负面影响。

1.2 数学模型

融合缺失信息图嵌入的多元时间序列异常检测算法能够利用多元时间序列的时空信息和缺失信息,检测出多元时间序列中潜在的异常值。对该算法的输入、输出定义如下:

定义 1 $\boldsymbol{X}_{1:n}$ 为一个长度为 n 的多元时间序列,表示为:

$$\boldsymbol{X}_{1:n}=(\boldsymbol{X}_1,\cdots,\boldsymbol{X}_t,\cdots,\boldsymbol{X}_n)\in\mathbb{R}^{l\times n} \tag{1}$$

式中,$\boldsymbol{X}_t=(x_t^1,\cdots,x_t^l)\in\mathbb{R}^l$ 为时刻 t 的时间序列特征向量,x_t^i 是 $\boldsymbol{X}_t$ 的第 i 个变量,l 是变量的个数。

定义 2 $\boldsymbol{m}_{1:n}$ 为多元时间序列缺失情况的掩蔽矩阵,表示为:

$$\boldsymbol{m}_{1:n}=(\boldsymbol{m}_1,\cdots,\boldsymbol{m}_t,\cdots,\boldsymbol{m}_n)\in\{0,1\}^{l\times n} \tag{2}$$

式中,$\boldsymbol{m}_t=(m_t^1,\cdots,m_t^l)\in\{0,1\}^l$ 是表示时刻 t 的数据点是否可观测的掩蔽向量,其中 $m_t^i=1$ 表示 x_t^i 可以被观测到,反之 $m_t^i=0$ 表示 x_t^i 缺失。

定义 3 $\boldsymbol{a}_{1:n}$ 为多元时间序列的异常结果,表示为:

$$\boldsymbol{a}_{1:n}=(\boldsymbol{a}_1,\cdots,\boldsymbol{a}_t,\cdots,\boldsymbol{a}_n)\in\{0,1\}^{l\times n} \tag{3}$$

式中,$\boldsymbol{a}_t=(a_t^1,\cdots,a_t^l)\in\{0,1\}^l$ 表示时刻 t 数据点的异常分数,其中 $a_t^i=1$ 表示 x_t^i 为异常值。任务目标为检测出多元时间序列中的异常值。

1.3 预插值与异常检测任务融合的联合学习框架

预插值与异常检测任务融合的联合学习框架如图 4 所示,包含预插值层、图结构学习层和异常检测模块 3 个主要组件,将多元时间序列间的关系建模成图,学习缺失多元时间序列的时间、空间关联,补全缺失数据,有效识别异常值。各主要组件作用如下:

1)基于高斯核函数的 GNN 预插值:采用图神经网络建模多元时间序列间的空间关系,嵌入高斯核函数所表征的时序特征对缺失时间序列预插值。

2)缺失信息融合的图结构学习:输入预插值后的多元时间序列嵌入向量和多元时间序列缺失信息,利用图注意力机制融合缺失时间序列的时空信息预测未来的时间序列。

3)基于预测的异常检测:输入预测值,计算和真实值的偏差,通过归一化偏差值识别出异常值。

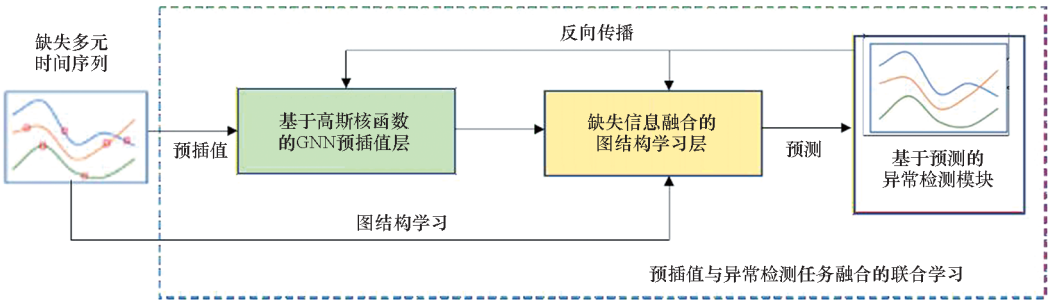

图 4　一种预插值与异常检测任务融合的联合学习框架

Fig. 4　A joint learning framework for pre-interpolation and anomaly detection

1.3.1　基于高斯核函数的 GNN 预插值

基于高斯核函数的预插值层输入为多元时间序列 $\boldsymbol{X}_{1:n}$和缺失信息掩蔽矩阵 $\boldsymbol{m}_{1:n}$。与 Shukla[17] 类似,对于 t^* 时刻第 i 个时序变量,采用高斯核函数 $k(t^*,t;\alpha_i)=\mathrm{e}^{-\alpha_i(t^*-t)^2}$来度量时刻 $t(1\leqslant t\leqslant n)$ 对时刻 t^* 的时序影响,定义时刻 t^* 的观测密度函数为 $\lambda(t^*,m^i;\alpha_i)=\sum_{t=1}^{n}m_t^i k(t^*,t;\alpha_i)m_t^i x_t^i$,其中 α_i 是可学习的参数。根据上述定义,可以推导出时序预测值 $\bar{\boldsymbol{x}}_{t^*}^i$ 的表达式为:

$$\bar{\boldsymbol{x}}_{t^*}^i=\frac{1}{\lambda(t^*,m^i;\alpha_i)}\sum_{t=1}^{n}k(t^*,t;\alpha_i)m_t^i x_t^i \tag{4}$$

考虑到不同时序变量存在的潜在空间关联,采用图神经网络在预插值层中嵌入时空信息。输入为每个时序变量预测值,为了获得输入特征的高维空间有效表达,定义权重矩阵 $\boldsymbol{H}\in\mathbb{R}^{l\times l}$进行自注意力变换到每个时序变量上:

$$h_{ij}=attention(\boldsymbol{W}\bar{\boldsymbol{x}}_{t^*}^i,\boldsymbol{W}\bar{\boldsymbol{x}}_{t^*}^j) \tag{5}$$

$$\beta_{ij}=\mathrm{softmax}_j(h_{ij}) \tag{6}$$

其中,$attention(\cdot)$表示注意力函数[15],$\boldsymbol{W}$ 表示对每个节点进行共享线性交换的可训练权重矩阵,β_{ij}是时序预测值的注意力系数。根据计算好的注意力系数将特征加权求和,扩展到多头注意力机制[18]进行加强,如式(7)所示,其中 K 为多头注意力机制的超参数,$\hat{\boldsymbol{x}}_{t^*}^i$ 为输入图结构学习层的预插值嵌入向量。

$$\hat{\boldsymbol{x}}_{t^*}^i=\sigma\left(\frac{1}{K}\sum_{k=1}^{K}\sum_{j=1}^{l}\beta_{ij}^k\boldsymbol{W}^k\hat{\boldsymbol{x}}_{t^*}^j\right) \tag{7}$$

其中,$\sigma(\cdot)$表示 LeakyReLU 非线性激活函数。

基于高斯核函数的 GNN 预插值层如图 5 所示,包括高斯核函数时序插值和图神经网络空域插值等 2 个主要模块,分别建模缺失多元时间序列的时空信息,为图结构学习层提供预插值嵌入向量。其中,α_i 和 β_{ij}在后续的图结构学习层中会参与联合训练,将插值任务和异常检测任务的优化目标进行对齐。

1.3.2　缺失信息融合的图结构学习

图结构学习层的目标是从图结构视角建模缺失多元时间序列间的关联关系。以物联网场景为例,传感器之间具有复杂耦合关系,空间距离、传感器类型、网络拓扑都有可能影响传感器之间的联系,很难获得充分的先验知识来定义传感器间

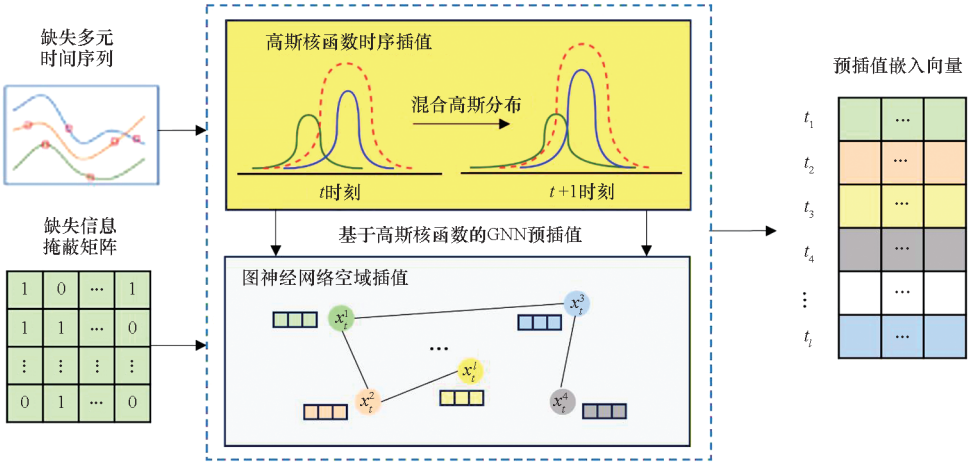

图 5　基于高斯核函数的 GNN 预插值架构

Fig. 5　Architecture of GNN pre-interpolation layer based on Gaussian kernel function

的图结构[9]。针对该问题,定义邻接矩阵 $\boldsymbol{D}$ 来表示多元时间序列间的关系,其中 D_{ij} 度量了时间序列 i 和时间序列 j 间的潜在联系。

考虑到在真实场景中先验知识对多元时间序列关系建模的有效性,定义与时间序列 i 潜在联系的集合 E_i 如式(8)所示,如果没有先验知识,集合 E_i 包含除时间序列 i 以外的所有时间序列。

$$E_i \subseteq \{1,2,\cdots,l\} \setminus \{i\} \tag{8}$$

为了计算出与时间序列 i 联系的时间序列,如式(9)、式(10)所示,先计算出多元时间序列嵌入向量 $\boldsymbol{u}_i$ 间的相似度,再选择前 p 个时间序列作为存在关系序列。其中,p 为超参数,可以用来调整邻接矩阵 $\boldsymbol{D}$ 的稀疏性;$\boldsymbol{u}_i$ 是门控循环单元(gated recurrent unit, GRU)基本单元所抽取的多元时间序列嵌入向量。

$$\boldsymbol{e}_{ji} = \frac{\boldsymbol{u}_i^{\mathrm{T}} \boldsymbol{u}_j}{\|\boldsymbol{u}_i\| \cdot \|\boldsymbol{u}_j\|},\ j \in E_i \tag{9}$$

$$D_{ji} = 1\{j \in \mathrm{TopP}(\{\boldsymbol{e}_{ji}; p \in E_i\})\} \tag{10}$$

其中:TopP(·)函数输出时间序列相似度排前 P 的时间序列索引,P 为超参数;$1\{\cdot\}$ 表示如果时间序列 j 满足 TopP(·)函数,则将邻接矩阵对应的元素 D_{ij} 设置为 1。

为了学习缺失多元时间序列间的潜在联系,设计了缺失信息融合的图注意力特征提取模块。与传统的图注意力机制不同,该方法先采用 GRU 基本单元抽取了多元时间序列的时序特征,再对多元时间序列间的空间联系和数据缺失关联进行建模,如式(11)~(14)所示。

$$\boldsymbol{z}_i^{(t)} = \mathrm{ReLU}\left(\boldsymbol{\gamma}_{i,i}\boldsymbol{Q}\hat{\boldsymbol{x}}_{t*}^{i} + \sum_{j \in \psi(i)} \boldsymbol{\gamma}_{i,j}\boldsymbol{Q}\hat{\boldsymbol{x}}_{t*}^{j}\right) \tag{11}$$

$$\boldsymbol{g}_{t*}^{i} = \boldsymbol{u}_i \oplus \boldsymbol{Q}(\hat{\boldsymbol{x}}_{t*}^{i} \| \boldsymbol{m}_{t*}^{i}) \tag{12}$$

$$\boldsymbol{\pi}(i,j) = \mathrm{ReLU}(attention(\boldsymbol{g}_{t*}^{i} \oplus \boldsymbol{g}_{t*}^{j})) \tag{13}$$

$$\boldsymbol{\gamma}_{i,j} = \mathrm{softmax}_j(\boldsymbol{\pi}(i,j)) \tag{14}$$

其中,预插值嵌入向量 $\hat{\boldsymbol{x}}_{t*}^{i} \in \mathbb{R}^{n}$ 是时间序列 i 的输入特征,$\psi(i) = \{j/D_{ji} > 0\}$ 是时间序列 i 根据邻接矩阵 $\boldsymbol{D}$ 得到的关联序列集合,$\boldsymbol{Q} \in \mathbb{R}^{l \times n}$ 是可学习的权重矩阵对每一个时间序列节点进行共享参数的线性变换;$\boldsymbol{g}_{t*}^{i}$ 连接多元时间序列嵌入向量 $\boldsymbol{u}_i$ 和预插值变换特征 $\boldsymbol{Q}\hat{\boldsymbol{x}}_{t*}^{i}$,并融合了缺失信息掩蔽矩阵 $\boldsymbol{m}_{1:n}$;$\boldsymbol{\gamma}_{i,j}$ 是通过图注意力机制学习的关联系数;$\boldsymbol{z}_i^{(t)}$ 是最终输入异常检测层的多元时间序列变量的聚合表征。

缺失信息融合的图结构学习架构如图 6 所示,基于先验知识定义多元时间序列间的邻接矩阵,采用图注意力机制融合多元时间序列数据缺失的关联性,学习多元时间序列的时空特征对多元时间序列进行预测。

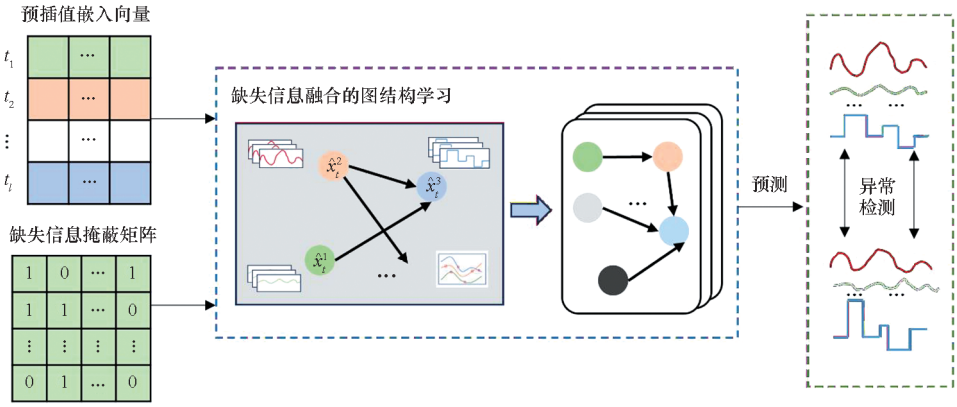

图 6 缺失信息融合的图结构学习架构

Fig. 6 Architecture of graph structure learning with missing information fusion

1.3.3 基于预测的异常检测

在异常检测模块,采用全连接层设计,基于多元时间序列聚合表征 $\boldsymbol{z}_i^{(t)}$ 和多元时间序列嵌入向量 $\boldsymbol{u}_i$ 计算出多元时间序列预测值 $\boldsymbol{y}_{t*}^{i}$,如式(15)所示:

$$\boldsymbol{y}_{t*}^{i} = f_\theta([\boldsymbol{u}_1 \circ \boldsymbol{z}_{t*}^{1}, \cdots, \boldsymbol{u}_l \circ \boldsymbol{z}_{t*}^{l}]) \tag{15}$$

式中,"∘"是向量连接运算。使用均方根误差来度量多元时间序列观测值和预测值之间的偏差并作为损失函数进行优化,如式(16)所示。

$$L_{\mathrm{MSE}} = \frac{1}{T_{\mathrm{train}} - \omega} \sum_{t*=\omega+1}^{T_{\mathrm{train}}} \|\hat{\boldsymbol{y}}_{t*} - \boldsymbol{y}_{t*}\|_2^2 \tag{16}$$

式中,T_{train} 表示输入训练数据的最终时刻,ω 表示批式训练中时间窗口的大小。

在异常检测阶段中,首先计算出时刻 t 的多元时间序列 i 的预测值 $\boldsymbol{y}_{t*}^{i}$,然后度量预测值和观测值间的偏差并进行归一化,如式(17)~(18)所示:

$$Err_i(t) = |\hat{\boldsymbol{y}}_t^i - \boldsymbol{y}_t^i| \tag{17}$$

$$b_i(t) = \frac{Err_i(t) - \tilde{\mu}_i}{\tilde{\sigma}_i} \tag{18}$$

其中,$\tilde{\mu}_i$ 和 $\tilde{\sigma}_i$ 是偏差值的期望和标准差。最后将标准化后偏差值最大变量标记为异常,如式(19)所示。

$$B(t) = \max_i b_i(t) \tag{19}$$

在真实物联网场景中,可以结合设置固定阈值的方式来降低异常值的报警率[19],在后续实验部分将验证集中的最大偏差设置为了阈值。

2　实验结果与分析

实验采用了安全水处理(secure water treatment, SWaT[20])和水分配(water distribution, WADI[21])数据集,二者都是从水处理物理试验台系统中采集的传感器多元时间序列数据,科研人员模拟了真实世界中的攻击场景,构造了数据集中的异常样本。

2.1　实验数据

SWaT 数据集与 WADI 数据集是从新加坡公共事业局运行的水处理物理试验台系统中采集构建的,后者在前者水处理系统的基础上添加了水分配系统,形成了一个完整而现实的水处理、储存和分配网络,二者分别包含 51 个传感器 11 d 内的连续监测信号和 127 个传感器 16 d 内的连续监测信号。研究人员模拟了真实世界中的攻击模式,包括通过通信网络传输的网络攻击和对水泵、水箱等硬件设备的物理攻击,以不同的时间间隔对单个或者多个设备进行单次或者多轮次的受控攻击,这些攻击对应于测试集中的异常标记。图 7是水处理物理试验台系统传感器设备拓扑关系图,上述数据集因为传感器关联复杂,攻击模式多样,被研究者们广泛用于多元时间序列异常检测算法的效果评估。因为水处理物理试验台系统首次启动需要 5 ~ 6 h 才能达到稳定[21],两个数据集中的前 2 160 个样本被剔除了。考虑训练效率的原因,对原始数据以 10 s 为时间窗口进行下采样,生成的标签是该时间窗口中数量最多的标签。此外,由于 SWaT 和 WADI 数据集缺失数据较少,基于缺失数据的原始分布随机扩充了占比为 10% 的缺失数据,模拟了真实场景下数据缺失的情况。如表 1 所示,SWaT 的训练集包含采样后前 6 d 的 47 515 条数据,都是正常样本,测试集包含后 5 d 的 44 986 条数据,存在异常样本,占比为 11.97%;WADI 的训练集包含采样后前 14 d 的118 795条数据,都是正常样本,测试集包含后 2 d 的 17 257 条数据,存在异常样本,占比为 5.99%。

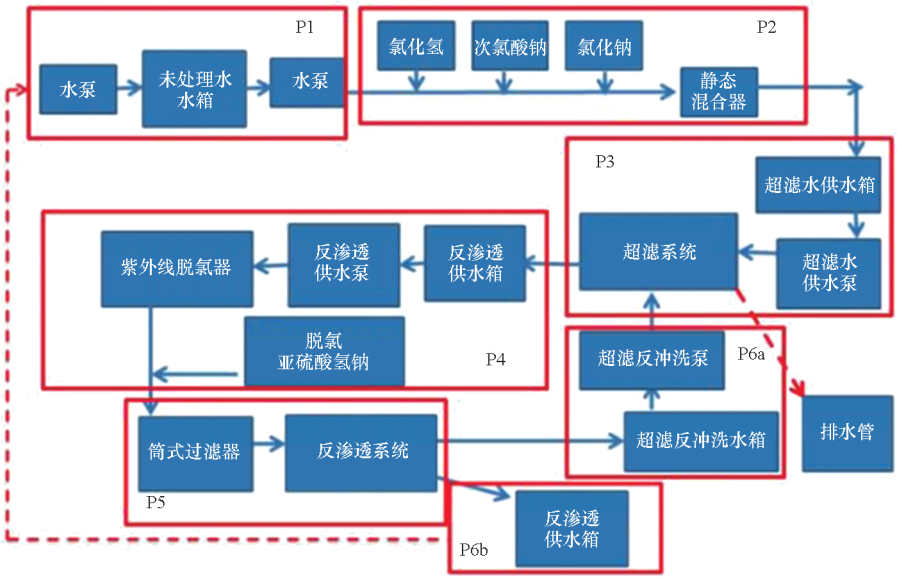

图 7　水处理物理试验台系统传感器设备拓扑结构

Fig. 7　Topological structure of sensors device in water treatment physical test bench system

表 1　实验数据集统计指标

Tab. 1　Statistics index of experimental dataset

数据集名称	传感器数量	训练集样本数	测试集样本数	异常比例/%
SWaT	51	47 515	44 986	11.97
WADI	127	118 795	17 257	5.99

2.2　评价指标

这一部分的评价指标测试了融合缺失信息图嵌入的多元时间序列异常检测算法和其他基准方法的性能。使用在异常检测任务中常用的指标对相关算法进行评估:准确率(Precision)、召回率(Recall)和 F1 分数(F1-Score),其定义如式(20) ~ (22)所示。

$$Precision = \frac{TP}{TP + FP} \tag{20}$$

$$Recall = \frac{TP}{TP + FN} \tag{21}$$

$$F1\text{-}Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{22}$$

在实验过程中,正例表示识别为异常样本,而负例表示识别为正常样本;真正例(true positive, TP)表示被正确检测为异常的异常样本;假正例(false positive,FP)表示错误地将正常样本标记为异常;假负例(false negative,FN)表示错误地将异常样本标记为正常。

2.3 实验设置

实验环境是一台 PC 服务器,其 CPU 为 11th Gen Intel(R) Core(TM) i7 - 1165G7 @ 2.80 GHz, GPU 是 NVIDIA GeForce RTX 3070,以 PyTorch 和 PyTorch Geometric 库为基本框架,在 Python3.8.3 中搭建深度神经网络进行训练。模型的参数设置如下:滑动时间窗口大小为 8;drop out 参数为 0.2;优化器选择 Adam;初始学习率为 0.01;训练轮数上限为 40。

为了证明融合缺失信息图嵌入的多元时间序列异常检测算法的总体性能,实验过程将其与 6 种无监督方法进行了比较。这些方法包括:主成分分析(principal component analysis, PCA)、AE、基于长短期记忆网络的差分自编码器[22](long short-term memory networks-variational auto-encoder, LSTM-VAE)、基于生成对抗网络的多元时间序列异常检测[23](multivariate anomaly detection for time series data with generative adversarial networks, MAD-GAN)、深度自编码高斯混合模型[24](deep autoencoding Gaussian mixture model, DAGMM)和图差分网络[5](graph deviation network, GDN)。因为并非所有用于比较的基准方法都提供了选择异常阈值的机制,在计算评价指标时测试了每个算法的可能异常阈值,并登记了与最高 F1 分数相关的结果。

2.4 结果分析

2.4.1 SWaT 数据集实验结果

SWaT 数据集的实验结果如表 2 所示,可以看到,相较于基准方法,本文提出的方法能达到更好的效果,其中 F1 分数达到了 0.79,准确率和召回率分别达到了 95.31% 和 67.59%,均显著领先于基准方法。图 8 展示了融合缺失信息图嵌入的多元时间序列异常检测算法在 SWaT 数据集上的训练损失函数收敛曲线。因为 GNN 预插值层的网络结构比较复杂,传播过程的计算复杂度更高,可以明显发现采用期望预插值层收敛速度会更快,但两者最终都会收敛到接近的合理区间。

表 2 SWaT 数据集上的实验结果

Tab. 2 Experimental result on SWaT dataset

方法名称	准确率/%	召回率/%	F1 分数
PCA	20.20	21.03	0.20
AE	65.62	49.31	0.56
LSTM-VAE	67.72	61.63	0.64
MAD-GAN	90.22	57.32	0.70
DAGMM	30.21	67.25	0.42
GDN	92.35	62.66	0.74
本文方法	95.31	67.59	0.79

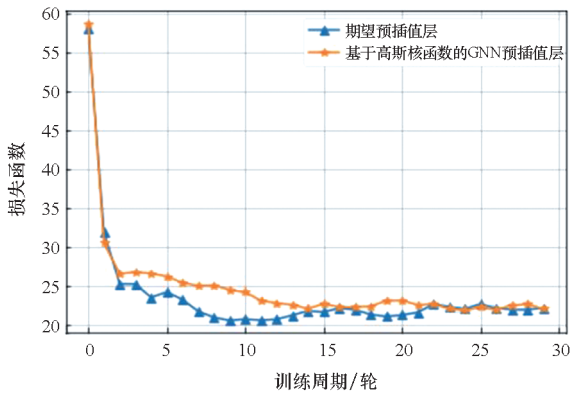

图 8 SWaT 数据集上损失函数收敛曲线

Fig. 8 Convergence curve of loss function on SWaT dataset

2.4.2 WADI 数据集实验结果

WADI 数据集的实验结果如表 3 所示,由于 WADI 数据集的复杂度高于 SWaT 数据集,相关方法异常检测效果均有所下降,尤其是在召回率指标上。由于传感器间的关联关系复杂度上升,多元时间序列间的空间特征信息抽取更加重要,基于图神经网络的方法明显好于传统方法。尽管如此,与基准方法相比,本文提出的融合缺失信息图嵌入的多元时间序列异常检测算法效果依旧领先,其中准确率达到了 92.38%,召回率达到了 41.81%,F1 分数达到了 0.57。图 9 展示了融合缺失信息图嵌入的多元时间序列异常检测算法在 WADI 数据集上的训练损失函数收敛曲线,整体趋势和 SWaT 数据集上的情况基本一致。考虑到 WADI 数据集包含更多的传感器多元时间序列特征和更少的异常样本,损失函数收敛速度要快于 SWaT 数据集。

表 3　WADI 数据集上的实验结果

Tab. 3　Experimental result on WADI dataset

方法名称	准确率/%	召回率/%	F1 分数
PCA	31.21	5.05	0.08
AE	32.86	33.92	0.33
LSTM-VAE	77.61	14.30	0.24
MAD-GAN	40.32	32.81	0.36
DAGMM	53.22	25.44	0.34
GDN	92.12	36.82	0.50
本文方法	92.38	41.81	0.57

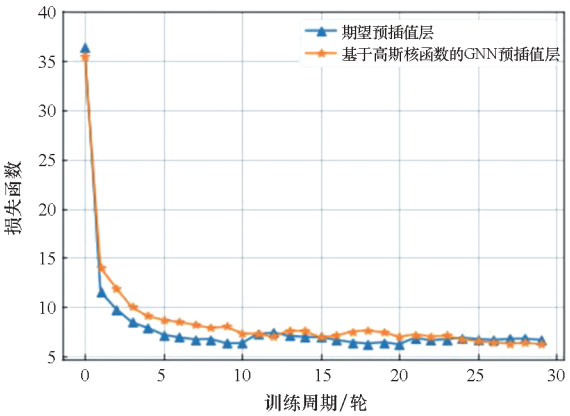

图 9　WADI 数据集上损失函数收敛曲线

Fig. 9　Convergence curve of loss function on WADI dataset

2.4.3　预插值模块对比实验

为了验证基于高斯核函数的 GNN 预插值模块的有效性,设计了预插值模块对比实验,将 GNN 预插值层替换为期望平滑,算法框架和其他实验环境参数保持不变,在 WADI 数据集下进行了验证,最终的实验结果如表 4 所示。

表 4　预插值模块对比实验结果

Tab. 4　Comparative experimental result of pre-interpolation module

方法名称	准确率/%	召回率/%	F1 分数
期望平滑	85.72	37.49	0.52
基于高斯核函数的 GNN 预插值	92.38	41.81	0.57

从实验结果可以看出,基于高斯核函数的 GNN 预插值模块对最终的异常检测效果有着非常大的提升,当将预插值模块替换为期望平滑后,准确率、召回率出现了明显的下降。

3　结论

提出了融合缺失信息图嵌入的多元时间序列异常检测算法,设计预插值与异常检测任务融合的联合学习框架,克服了传统两阶段方法的不足,能够有效缓解缺失数据对多元时间序列异常检测任务的影响;设计了缺失信息融合的图结构学习模块,采用图注意力机制融合缺失信息掩蔽矩阵和时空特征向量,兼顾了多元时间序列的时空特征和缺失数据的潜在联系。在真实物联网传感器数据集对提出算法进行了实验,与基准方法相比,提出算法在缺失多元时间序列异常检测任务上更有优势,预插值模块对比实验结果证明了基于高斯核函数的 GNN 预插值层设计的有效性。

参考文献(References)

[1] 刘学, 孙翱, 李冬. 参照化流形空间融合学习的敏感特征提取与异常检测方法[J]. 国防科技大学学报, 2020, 42(6): 47 – 55.
LIU X, SUN A, LI D. Sensitive feature extraction and anomaly detection method based on referenced manifold spatial fusion learning[J]. Journal of National University of Defense Technology, 2020, 42(6): 47 – 55. (in Chinese)

[2] SUNNY J S, PATRO C P K, KARNANI K, et al. Anomaly detection framework for wearables data: a perspective review on data concepts, data analysis algorithms and prospects[J]. Sensors, 2022, 22(3): 756.

[3] 王意洁, 程力, 马行空. 运用警报关联的威胁行为检测技术综述[J]. 国防科技大学学报, 2017, 39(5): 128 – 138.
WANG Y J, CHENG L, MA X K. Survey of alert-correlation based on network threat detection techniques[J]. Journal of National University of Defense Technology, 2017, 39(5): 128 – 138. (in Chinese)

[4] CRÉPEY S, LEHDILI N, MADHAR N, et al. Anomaly detection in financial time series by principal component analysis and neural networks[J]. Algorithms, 2022, 15(10): 385.

[5] SHI X, HAO K R, CHEN L, et al. Multivariate time series prediction of complex systems based on graph neural networks with location embedding graph structure learning[J]. Advanced Engineering Informatics, 2022, 54: 101810.

[6] HANSEN L K, SIGURDSSON S, KOLENDA T, et al. Modeling text with generalizable Gaussian mixtures[C]// Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, 2020: 3494 – 3497.

[7] 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.

[8] 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.

[9] 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.

[10] LI T Y, COMER M L, DELP E J, et al. Anomaly scoring for prediction-based anomaly detection in time series [C]// Proceedings of the IEEE Aerospace Conference, 2020: 1 – 7.

[11] SOUIDEN I, OMRI M N, BRAHMI Z. A survey of outlier detection in high dimensional data streams [J]. Computer Science Review, 2022, 44: 100463.

[12] FAN J, ZHANG K, HUANG Y P, et al. Parallel spatio-temporal attention-based TCN for multivariate time series prediction[J]. Neural Computing and Applications, 2023, 35(18): 13109 – 13118.

[13] YAN Y J, HASHEMI M, SWERSKY K, et al. Two sides of the same coin: heterophily and oversmoothing in graph convolutional neural networks[C]//Proceedings of the IEEE International Conference on Data Mining (ICDM), 2022: 1287 – 1292.

[14] KIPF T, WELLING M. Semi-supervised classification with graph convolutional networks [C]//Proceedings of the International Conference on Learning Representations, 2017.

[15] VELIČKOVIĆ P, CUCURULL G, CASANOVA A, et al. Graph attention networks [C]//Proceedings of the International Conference on Learning Representations, 2018.

[16] KREINDLER D M, LUMSDEN C J. The effects of the irregular sample and missing data in time series analysis[J]. Nonlinear Dynamics, Psychology, and Life Sciences, 2006, 10(2): 187 – 214.

[17] CHALLU C, OLIVARES K G, ORESHKIN B N, et al. NHITS: neural hierarchical interpolation for time series forecasting[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2023, 37(6): 6989 – 6997.

[18] HOSHEN Y. VAIN: attentional multi-agent predictive modeling [C]//Proceedings of the Thirty-First Annual Conference on Neural Information Processing Systems, 2017.

[19] SIFFER A, FOUQUE P A, TERMIER A, et al. Anomaly detection in streams with extreme value theory [C]// Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2017: 1067 – 1075.

[20] MATHUR A P, TIPPENHAUER N O. SWaT: a water treatment testbed for research and training on ICS security[C]// Proceedings of the International Workshop on Cyber-Physical Systems for Smart Water Networks (CySWater), 2016: 31 – 36.

[21] 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, 2017: 25 – 28.

[22] 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.

[23] LI D, CHEN D C, JIN B H, et al. MAD-GAN: multivariate anomaly detection for time series data with generative adversarial networks [C]//Proceedings of the Internet Corporation for Assigned Names and Numbers, 2019: 703 – 716.

[24] ZONG B, SONG Q, MIN M R, et al. Deep autoencoding Gaussian mixture model for unsupervised anomaly detection[C]//Proceedings of the International Conference on Learning Representations, 2018.