

## 缺失值场景下的多元时间序列异常检测算法

曾子辉, 李超洋, 廖清

### 引用本文

曾子辉, 李超洋, 廖清. 缺失值场景下的多元时间序列异常检测算法[J]. 计算机科学, 2024, 51(7): 108-115.

ZENG Zihui, LI Chaoyang, LIAO Qing. [Multivariate Time Series Anomaly Detection Algorithm in Missing Value Scenario](#) [J]. Computer Science, 2024, 51(7): 108-115.

---

### 相似文章推荐 (请使用火狐或 IE 浏览器查看文章)

#### Similar articles recommended (Please use Firefox or IE to view the article)

##### [针对系统调用的基于语义特征的多方面信息融合的主机异常检测框架](#)

Host Anomaly Detection Framework Based on Multifaceted Information Fusion of Semantic Features for System Calls

计算机科学, 2024, 51(7): 380-388. <https://doi.org/10.11896/jsjcx.230400023>

##### [基于深度确定性策略梯度与注意力Critic的多智能体协同清障算法](#)

Multi-agent Cooperative Algorithm for Obstacle Clearance Based on Deep Deterministic Policy Gradient and Attention Critic

计算机科学, 2024, 51(7): 319-326. <https://doi.org/10.11896/jsjcx.230600129>

##### [融合多图卷积与层级池化的文本分类模型](#)

Text Classification Method Based on Multi Graph Convolution and Hierarchical Pooling

计算机科学, 2024, 51(7): 303-309. <https://doi.org/10.11896/jsjcx.230400164>

##### [基于联合学习的语言粒度融合的重叠事件抽取方法](#)

Overlap Event Extraction Method with Language Granularity Fusion Based on Joint Learning

计算机科学, 2024, 51(7): 287-295. <https://doi.org/10.11896/jsjcx.230700118>

##### [轻量级深度神经网络模型适配边缘智能研究综述](#)

Lightweight Deep Neural Network Models for Edge Intelligence: A Survey

计算机科学, 2024, 51(7): 257-271. <https://doi.org/10.11896/jsjcx.240100045>

# 缺失值场景下的多元时间序列异常检测算法

曾子辉<sup>1</sup> 李超洋<sup>1,2</sup> 廖清<sup>1,2</sup>

1 哈尔滨工业大学(深圳)计算机科学与技术学院 广东 深圳 518055

2 鹏城实验室 广东 深圳 518055

(20S151144@stu.hit.edu.cn)

**摘要** 时间序列异常检测是工业界中一个重要的研究领域。当前的时间序列异常检测方法侧重于面向完整的时间序列数据进行异常检测,而没有考虑到包含工业场景中网络异常、传感器损坏等所导致的缺失值的时间序列异常检测任务。文中针对工业场景中更加常见的含缺失值的时间序列异常检测任务,提出了一种基于注意力重新表征的时间序列异常检测算法 MMAD (Missing Multivariate Time Series Anomaly Detection)。具体来说,MMAD 首先将包含缺失值的时间序列数据通过时间位置编码对时间序列中不同时间戳的空间关联进行建模,然后通过掩码注意力表征模块学习不同时间戳之间数据的关联关系并将其表征为一个高维的嵌入式编码矩阵,从而将包含缺失值的多元时间序列表示为不含缺失值的高维表征,最后引入条件标准化流对该表征进行重建,以重建概率作为异常评分,重建概率越小代表样本越异常。在 3 个经典时间序列数据集上进行实验,结果表明,相比其他基线方法,MMAD 性能平均提升了 11%,验证了 MMAD 在缺失值场景下进行多元时间序列异常检测的有效性。

**关键词:** 多元时间序列;异常检测;缺失值场景;注意力机制;神经网络

**中图分类号** TP389.1

## Multivariate Time Series Anomaly Detection Algorithm in Missing Value Scenario

ZENG Zihui<sup>1</sup>, LI Chaoyang<sup>1,2</sup> and LIAO Qing<sup>1,2</sup>

1 School of Computer Science and Technology, Harbin Institute of Technology (Shenzhen), Shenzhen, Guangdong 518055, China

2 Peng Cheng Laboratory, Shenzhen, Guangdong 518055, China

**Abstract** Time series anomaly detection is an important research field in industry. Current methods of time series anomaly detection focus on anomaly detection for complete time series data, without considering the time series anomaly detection task containing missing values caused by network anomaly and sensor damage in industrial scenarios. In this paper, we propose an attention representation-based time series anomaly detection algorithm MMAD (missing multivariate time series anomaly detection) for the more common time series anomaly detection tasks with missing values in industrial scenarios. Specifically, MMAD first models the spatial correlation of different time stamps in time series by time position coding. Then, we build an attention representation module to learn the relationships between different time stamps and represent them as an embedded high-dimensional coding matrix, thereby representing the multivariate time series with missing values as a high-dimensional representation without missing values. Finally, we design the conditional normalized flow to reconstruct the representation and use the reconstruction probability as the anomaly score, the lower the probability of reconstruction, the more abnormal the sample. Experiments on three classical time series datasets show that, the average performance of MMAD is improved by 11% comparing with other baseline methods, which verifies the efficacy of MMAD to achieve multivariate time series anomaly detection with missing values.

**Keywords** Multivariate time series, Anomaly detection, Missing-value scenario, Attention mechanism, Neural network

## 1 引言

在数据挖掘中,异常检测指对不符合预期模式的项目、事件或观测值的识别。异常检测已被应用于许多重要领域,

如视频监控、网络入侵检测、信用欺诈检测、电力行业和医疗保健<sup>[1]</sup>。

在信息工业快速发展的当代,互联设备和传感器的数量迅速增长,基于互联设备和传感器所组成的现实系统是

到稿日期:2023-04-16 返修日期:2023-08-25

基金项目:国家自然科学基金面上项目(U1711261);广东省基础与应用基础研究重大项目(2019B030302002)

This work was supported by the National Natural Science Foundation of China(General Program)(U1711261) and Guangdong Basic and Applied Basic Research Foundation(Major Program)(2019B030302002).

通信作者:廖清(liaoqing@hit.edu.cn)

现代生活的必要基础。例如车联网系统、电网系统、水处理厂、交通和通信网络等关键基础设施给人类生产生活提供了极大便利。现实系统中的传感器每时每刻都在产生大量的观测值,具备时刻信息的观测值序列被称为时间序列,一个时刻包含多个观测值的时间序列被称为多元时间序列。

针对多元时间序列数据,传统异常检测方式主要依靠数据专家进行人力排查<sup>[2-5]</sup>。然而,随着现实系统中传感器的数量增多,从系统中收集到的多元时间序列的维度也越来越高,不同指标之间的复杂性也越来越高,时间序列异常检测任务的难度越来越大,传统检测方式难以有效检测出时序异常。因此,如何自动化执行多元时间序列的异常检测任务已变得越来越重要<sup>[6-7]</sup>。

近年来,随着数据科学的进步以及人工智能技术的发展,基于数据挖掘和深度学习的异常检测方法得到了广泛研究<sup>[8]</sup>。根据异常检测方式的不同,多元时间序列异常检测方法主要分为基于预测的多元时间序列异常检测方法和基于重构的多元时间序列异常检测方法。

基于预测的多元时间序列异常检测方法指模型将最近时刻的数据或最近一段时间窗口的数据作为输入,来预测下一个时刻数据或未来一段时间的数据,并将预测值与实际值进行比较,从而确定输入时间序列的异常程度。通常将预测值与实际值的偏差作为异常分数。例如,Munir等<sup>[9]</sup>提出了DeepAnT(Deep Learning-based Anomaly Detection Approach)方法,DeepAnT包含两个模块,即时间序列预测器和异常检测器。其中时间序列预测器通过捕捉周期性和季节性时间序列来预测未来数据,异常检测器采用预测值与真实值误差的平方根作为异常值。Hundman等<sup>[10]</sup>提出了一种改进的LSTM模型LSTM-NDT(LSTMs and Nonparametric Dynamic Thresholding),通过从多元时间序列中提取历史信息来预测下一个时间步的数据;同时,他们还提出了一种非参数、动态和无监督的阈值搜索技术,用于评估真实值与预测值之间的残差。Su等<sup>[11]</sup>提出了OmniAnomaly,通过结合GRU(Gate Recurrent Unit)与VAE(Variational Auto-Encoder)并使用平面归一化流来描述潜在空间的非高斯分布,并基于非高斯分布对下一时刻值进行预测。Chen等<sup>[12]</sup>提出了GTA(Graph Structures with Transformer for Multivariate Time Series Anomaly Detection)模型,该模型首先融合多尺度扩张卷积和图卷积得到分层的时间上下文编码,并将改编码输入Transformer<sup>[13]</sup>模型中以建模和预测下一个时刻的序列。Deng等<sup>[14]</sup>提出了GDN(Graph Neural Network-Based Anomaly Detection),通过捕捉多个时间序列之间的关联关系,并通过一个全连接层对未来时刻的数据进行预测。虽然基于预测的时间序列异常检测方法能够预测时间序列的异常,但是当时间序列变化迅速且时间点数显著增加时,会产生较大的预测误差。

基于重建的多元时间序列异常检测方法指训练模型通过学习正常时间子序列的潜在表示来重建多元时间子序列并通过度量其与原始时间序列的差异来检测异常。例如,Zong等<sup>[15]</sup>提出了DAGMM(Deep Autoencoding Gaussian Mixture

Model)模型,该模型主要由一个压缩网络(Compression Network)和一个估计网络(Estimation Network)两部分组成,其中压缩网络利用自动编码器对输入样本进行降维,并重建样本,将重建样本与输入样本的重构误差输入估计网络,估计网络通过高斯混合模型计算样本能量,高样本能量代表高度异常。Dai等<sup>[16]</sup>提出了GANF(Graph-Augmented Normalizing Flows),该模型基于RNN(Recursive Neural Network)捕捉时间序列沿时间轴变化的趋势,同时引入贝叶斯网络捕捉不同时间序列之间的关系,最后采用基于标准化流重建的方式进行异常检测。Audibert等<sup>[17]</sup>提出了一种基于对抗性学习重建方法USAD(Unsupervised Anomaly Detection on Multivariate Time-series),该方法通过两个简单的自动编码器(Auto-Encoder,AE)进行对抗性学习来重建多元时间序列,并以重建序列与原始序列之间的差异作为异常分数进行异常检测。Chen等<sup>[18]</sup>提出了DAEMON模型,该模型由变分自编码器、生成器和两个生成判别器组成,并让子生成器之间相互约束,增强总体模型的重构能力。Li等<sup>[19]</sup>提出了MAD-GAN(Multivariate Anomaly Detection for Time-series Data with Generative Adversarial Networks)模型,该模型分别利用LSTM和RNN作为GAN的生成器和鉴别器来捕捉多元时间序列分布中的时间相关性,同时设计了一种融合判别误差以及真实样本与生成样本间的残差的异常分数,以此作为判断异常的标准。Chen等<sup>[20]</sup>提出了LSTM-GAN,融合GAN和Bi-LSTM(Bi-directional Long Short-Term Memory)实现了对多元时间序列的无监督重构和检测。

尽管上述工作在水厂治理异常检测、云服务异常检测等场景下取得了较好的效果,但这些工作均侧重于针对没有缺失值的多元时间序列数据进行异常检测。而在真实的监测场景中,传感器往往会因为各种客观因素而数据采集不全,例如,由于传输条件的限制和传感器的自然损坏而没有被及时更换等。

本文侧重于缺失值场景下的多元时间序列异常检测研究。为了验证已有时序异常检测方法在缺失值场景下的真实性能,本文在数据缺失场景下选取了4个最先进的多元时间异常检测模型进行异常检测评估,包括GDN(AAAI 2021)<sup>[14]</sup>, DAGMM(ICLR 2018)<sup>[15]</sup>,GANF(ICLR 2022)<sup>[16]</sup>,USAD(KDD 2020)<sup>[17]</sup>。实验通过随机删除数据集中的一部分数据来模拟缺失值场景。

图1展示了这些方法在完整数据集场景和缺失值场景下的性能表现,实验结果表明无论是基于预测的时间序列异常检测方法还是基于重建的时间序列异常检测方法,在存在缺失值的情况下性能均明显下降。例如,图中紫色曲线表示基于重建的时序异常检测GANF模型,当横坐标数据的缺失率从10%增至50%时,GANF模型在F1上的效果从0.74降至0.13;橙色曲线表示基于预测的时序异常检测GDN模型,当横坐标数据缺失率从10%增至50%时,GDN模型在F1上的效果从0.74降至0.56;当前多元时间序列异常检测模型在缺失值场景下性能会显著下降,无法满足真实存在的缺失值场景下的性能需求。因此,如何保证多元时间序列异常检测模型在存在缺失值的场景下

依然保证良好的性能具有重要的现实意义。

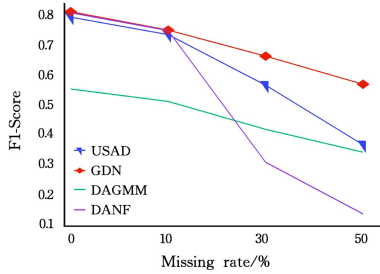


图1 多元时间异常检测方法在缺失值场景下的 F1 分数  
(电子版为彩图)

Fig. 1 F1-Score of multivariate time anomaly detection method in missing value scenario

本文的核心创新点如下：

(1)提出了一种面向缺失值的多元时间序列的异常检测算法(MMAD),该模型是一种基于重建的缺失值场景下的多元时间序列异常检测解决方案。

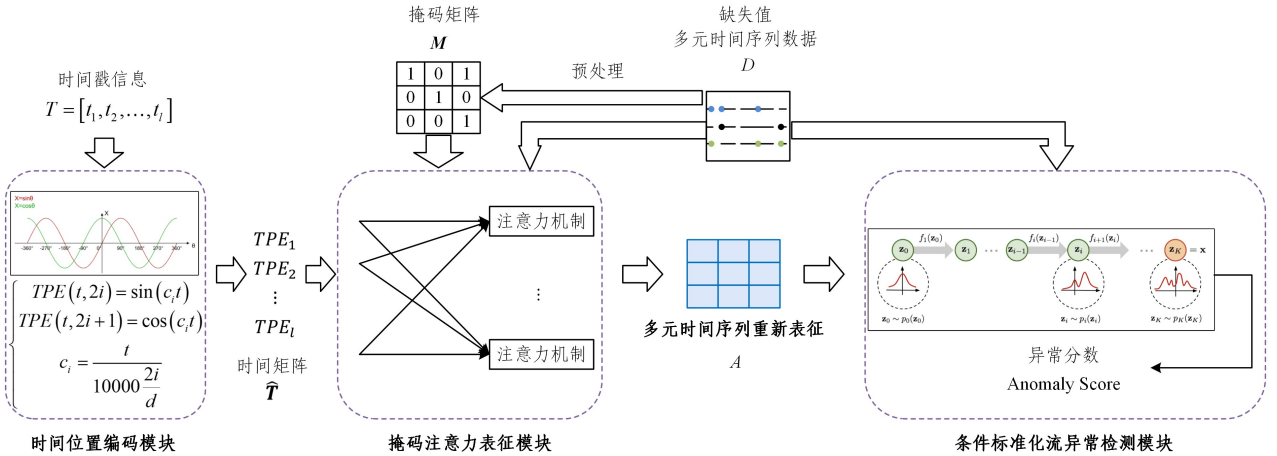


图2 MMAD 总体架构

Fig. 2 Overall architecture of MMAD

其中,时间位置编码模块的主要目的是将时间戳信息转化为时间位置编码,并输出基于时间位置编码组合成的时间矩阵,同时引入相对时间位置关系和绝对时间位置关系以充分挖掘时间戳中蕴含的空间关系。该模块输入时间戳信息  $T$ ,输出为时间矩阵  $\hat{T}$ 。

掩码注意力表征模块(MMAR)的主要目的是生成包含缺失值的多元时间序列数据的重新表征。具体地,构造掩码矩阵  $M$  来判断数据是否有缺失值, $M$  为一个与缺失值多元时间序列数据  $D$  大小相同的 0/1 矩阵,0 代表  $D$  中的数据缺失,1 代表数据没有缺失。掩码注意力表征模块输入为掩码矩阵  $M$ 、缺失值多元时间序列数据  $D$  和时间戳信息  $T$ ,输出为多元时间序列重新表征  $A$ 。

条件标准化流异常检测模块(CNF-AD)的目的是学习一个可逆变换函数以实现简单分布与真实分布近似之间的变换,通过该可逆变换函数与简单分布计算观测值在真实分布中的近似概率,并以该概率作为异常分数进行异常检测。条件标准化流异常检测模块输入为多元时间序列重新表征  $A$  和缺失值多元时间序列数据  $D$ ,输出为异常分数。

(2)提出了一种面向缺失值的掩码注意力机制(Missing Time Series Masked Attention Represent,MMAR),将包含缺失值的时间序列数据映射为完整的高维嵌入表征,该表征融合了时间信息、缺失值信息以及观测值信息;同时设计了一种基于条件标准化分布变换的异常检测模块(Conditional Normalizing Flow Anomaly Detection Module,CNF-AD),该模块计算真实分布与高维嵌入表征的概率密度,并以该概率密度作为异常分数进行异常检测。

(3)实验结果表明 MMAD 在多维时间序列异常检测任务上有着良好的表现,尤其在包含缺失值的时间序列的异常检测任务上超越了当前最新的异常检测方法。

## 2 MMAD 整体框架

模型总图架构如图 2 所示,MMAD 模型主要由 3 个模块组成:时间位置编码模块(Time Position Encoding)、掩码注意力表征模块(MMAR)和条件标准化流异常检测模块(CNF-AD)。

## 3 方法实现

### 3.1 时间位置编码模块

时间位置编码模块旨在设计一种编码方法将原时间窗口中单个时间戳信息转换成时间位置编码,并引入绝对时间位置关系和相对时间位置关系来对时间信息进行建模。

受 Transformer<sup>[13]</sup>的启发,本文采用了和 Transformer 相同的编码方式。在 Transformer 中,该编码方式被用来表示句子中的单词位置,在 MMAD 中,我们用该编码表示时间戳信息。对于单个时间戳  $t$  进行时间位置编码得到  $z$  时间位置编码  $TPE$ ,如式(1)所示:

$$\begin{cases} TPE(t, 2i) = \sin(c_i t) \\ TPE(t, 2i + 1) = \cos(c_i t) \end{cases} \quad (1)$$

$$c_i = \frac{1}{10000 \frac{2i}{d}} \quad (2)$$

其中, $t$  代表时间戳, $i$  代表时间位置编码  $TPE$  中奇偶对的下标,其中  $i \in [0, \frac{d}{2})$ , $d$  代表时间位置编码  $TPE$  的长度。由式(1)可知,对于长度为  $d$  的时间位置编码,共有  $\frac{d}{2}$  个奇偶对,

其中奇数位置的元素值通过正弦函数计算得到,偶数位置的元素值通过余弦函数计算得到。

对于绝对时间间隔为  $p$  的两个不同时间位置的时间戳  $t_i$  和  $t_{i+p}$ ,由式(1)得到时间位置编码  $TPE_i$  和  $TPE_{i+p}$  如式(3)、式(4)所示:

$$TPE_i = [\dots, \sin(c_i t_i), \cos(c_i t_i), \dots] \quad (3)$$

$$TPE_{i+p} = [\dots, \sin(c_i t_{i+p}), \cos(c_i t_{i+p}), \dots] \quad (4)$$

其中,  $c_i$  为向量中第  $i$  个奇偶对的常量系数。

对于  $TPE_{i+p}$  中的每个元素,由于  $t_{i+p} = t_i + p$ ,因此,通过正余弦和式(5)、式(6)变换可得式(7)。其中,距离  $p$  为常数,则  $\sin(c_i p)$ ,  $\cos(c_i p)$  也为常数,即  $TPE_{i+p}$  可由  $TPE_i$  线性表示。

$$\sin(c_i t_{i+p}) = \sin(c_i t_i) \cos(c_i p) + \cos(c_i t_i) \sin(c_i p) \quad (5)$$

$$\cos(c_i t_{i+p}) = \cos(c_i t_i) \cos(c_i p) - \sin(c_i t_i) \sin(c_i p) \quad (6)$$

$$\begin{pmatrix} \sin(c_i t_{i+p}) \\ \cos(c_i t_{i+p}) \end{pmatrix} = \begin{pmatrix} u & v \\ -v & u \end{pmatrix} \begin{pmatrix} \sin(c_i t_i) \\ \cos(c_i t_i) \end{pmatrix} \quad (7)$$

$$u = \sin(c_i p) \quad (8)$$

$$v = \cos(c_i p) \quad (9)$$

为了充分捕捉不同时间间隔之间的关联特征,本文引入了绝对时间位置关系和相对时间位置关系。

绝对时间位置关系:如式(10)、式(11)所示,对于间隔为  $p$  的两个时间戳  $t_i$  和  $t_{i+p}$  的时间位置编码  $TPE_i$  和  $TPE_{i+p}$ ,存在线性表示关系。

$$TPE_{i+p} = (a, b) \cdot TPE_i \quad (10)$$

$$a = [u, -v]^T, b = [v, u]^T \quad (11)$$

相对时间位置关系:本文利用时间位置编码  $TPE_i$  和  $TPE_{i+p}$  之间的点积表示间隔为  $p$  的两个时间戳的相对时间位置关系,如式(12)所示:

$$TPE_i \cdot TPE_{i+p} = \sum_{i=0}^d \cos(c_i p) \quad (12)$$

相对时间位置关系是关于间隔  $p$  的余弦函数,与间隔  $p$  的大小成负相关,这表示时间间隔越大,相对时间位置关系越疏远。

在模型中,对于一个输入的包含缺失值的多元时间序列  $D \in R^{m \times l}$  ( $m$  是多元时间序列的维度,  $l$  为时间窗大小),  $T = [t_1, t_2, \dots, t_l]$  表示其中  $l$  个时间戳信息。对于  $T$  中第  $i$  个时间戳  $t_i$ ,经过时间位置编码后得到  $TPE_i$ ,并由  $TPE_i$  组成时间矩阵  $\hat{T}$ ,如式(13)所示:

$$\hat{T} = [TPE_1, TPE_2, \dots, TPE_l] \quad (13)$$

### 3.2 掩码注意力表征模块

掩码注意力模块旨在融合包含缺失值的多元时间序列中的有效信息,对包含缺失值的多元时间序列进行重新表征。

掩码注意力机制模块将  $T, D, M$  作为输入,基于注意力机制得到  $D$  的重新表征  $A \in R^{n \times d}$ ,如式(15)所示:

$$A = [A_1, A_2, \dots, A_d] \quad (14)$$

$$A_i = \sum_{j=0}^{d-1} att(i, j) V_j M_j \quad (15)$$

$$V = W_D D \quad (16)$$

其中,  $A_i$  为第  $i$  个时间戳的重新表征,其基于注意力机制融合其余  $j (j \in [0, d], j \neq i)$  时刻的信息得到。矩阵  $V$  是数据  $D$  经过权重矩阵  $W_D$  线性变换后得到的信息矩阵,  $V_j$  表示  $V$  矩阵在  $j$  时刻的信息向量,  $M_i$  表示  $i$  时刻的缺失信息,  $att(i, j)$  表示时刻  $i$  和时刻  $j$  之间的注意力权重。时刻  $i$  和时刻  $j$  之间的注意力权重由式(17)求得:

$$att(i, j) = \text{softmax}\left(\frac{Q_i K_j^T}{\sqrt{d_j}}\right) \quad (17)$$

$$Q = W_Q T \quad (18)$$

$$K = W_K T \quad (19)$$

其中,  $Q_i$  和  $K_i$  分别表示时刻  $i$  的查询信息以及时刻  $i$  的关键词信息;  $Q$  表示查询矩阵,由时间信息矩阵  $T$  经过权重矩阵  $W_Q$  线性变换得到;  $K$  表示查询矩阵,由时间信息矩阵  $T$  经过权重矩阵  $W_K$  线性变换得到。

### 3.3 条件标准化流异常检测模块

在经过掩码注意力表征模块之后,条件标准化流异常检测模块需要依据已有的信息完成对多元时间序列异常的判断。

MMAD 是一种基于重建的异常检测模型,传统基于重建的异常检测模型一般基于自动编码器(Auto Encoder)、变分自动编码器(Variational Autoencoder)等生成模型来捕获数据的分布。对于分布复杂的数据,仅依靠一个简单的模型直接模拟是非常困难的,标准化流<sup>[21]</sup>通过定义一系列可逆变换来进行不同分布之间的变换,基于流的方式,能够将一个简单的分布逐渐复杂化从而模拟一个复杂的分布。

设  $x \in R^m$  是一个  $m$  维的随机变量,  $x$  在其分布上的概率密度函数是  $p(x)$ 。标准化流指能够将  $x$  变换到标准分布的一种可逆变换  $f(x): R^m \rightarrow R^m$ ,这种分布通常是高斯分布或其他易于抽样且密度易于计算的分布。设标准分布上的随机变量  $z$  可以通过  $f$  变换得到  $z = f(x)$ ,且  $z$  的概率密度函数为  $q(z)$ ,根据变量替换式(20)、式(21):

$$p(x) = q(f(x)) * |\det Jf(x)| \quad (20)$$

$$q(z) = p(f^{-1}(z)) * |\det Jf^{-1}(z)| \quad (21)$$

可以计算得到真实数据的概率密度,如式(22)所示:

$$\log p(x) = \log q(f(x)) + \log |\det J \nabla_x f(x)| \quad (22)$$

在标准化流的基础上,为了更好地帮助模型学习简单分布到真实数据分布的变换,本文提出了一种条件标准化流,以掩码注意力机制的重新表征  $A$  作为先验条件,在该先验条件的限制下让模型学习简单分布到真实数据分布的变化。本文对标准化流做了如下改进,如式(23)所示:

$$\log p(D|A) = \log q(f(D; A)) + \log |\det J \nabla_D f(D; A)| \quad (23)$$

其中,  $D$  为原始数据,  $A$  为数据的掩码注意力重新表征。  $\log(D|A)$  将作为多元时间序列的异常分数。

## 4 实验及结果分析

实验主要包含 4 部分,第一部分为缺失值场景下的性能

对比实验,比较 MMAD 与当前多元时间序列异常检测方法在 3 种缺失值场景下的检测效果;第二部分为数据填充后的性能对比实验,在缺失值场景下,先对缺失数据集进行填充,然后比较 MMAD 与当前多元时间序列异常检测方法的性能表现;第三部分为参数敏感性实验,分析可能影响模型性能的因素;第四部分为消融实验,分析不同模块在完成异常检测任务过程中发挥的作用。

本章 4.1 节详细介绍实验所使用的数据集;4.2 节介绍本文所对比的异常检测方法以及实验评价指标;4.3 节介绍各异常检测方法在缺失值场景下进行多元时间序列异常检测的实验设置和结果;4.4 节介绍在填充缺失值数据之后,各异常检测方法的实验设置和结果;4.5 节展示不同参数对模型影响的效果;最后设计消融实验以验证模型各模块对异常检测效果的贡献。

#### 4.1 数据集介绍

SWaT(Secure Water Treatment)数据集<sup>[22]</sup>:源于与新加坡公用事业委员会协调的运行水处理试验台。该数据以 1 s 的频率收集持续 11 天 51 个传感器的记录。该数据集分为测试集和训练集,其中前 7 天为训练集,不包含异常或攻击行为,后 4 天为测试集,总共进行了 36 次攻击,其中大约 11% 的时间步为异常标签。

WADI(Water Distribution)数据集<sup>1)</sup>:是一个由大量供水管道组成的供水系统。因此,WADI 形成了一个更加完整和现实的水处理、存储和分配网络。数据集包含 14 天正常运行的数据,这些数据组成了训练集。在接下来的几天,以不同的时间间隔进行了许多受控的物理攻击,这与测试集中的异常情况对应。

SMD(Server Machine Dataset)数据集<sup>2)</sup>:从一家大型互联网公司收集的服务器机器数据集。数据集被分为两个等长的部分,其中前半部分为没有发生异常的数据集,可作为训练集;后半部分包含攻击行为,可作为测试集。

3 个数据集的详细信息如表 1 所列。

表 1 数据集统计信息  
Table 1 Statistics of datasets

数据集	训练集大小	测试集大小	传感器数量	异常占比/%
SWaT	99360	89984	51	11.99
WADI	241921	15701	123	7.09
SMD	708405	708420	38	4.16

#### 4.2 对比方法及性能评价指标

为了验证 MMAD 的性能,本文选取了以下对比方法。

GDN<sup>[14]</sup>(Deng 等,AAAI2021):基于预测的多元时间序列异常检测模型。其采用无监督异常检测,将结构学习方法与图形神经网络相结合,着重建模不同维度时间序列之间的关系,另外,使用注意力权重来解释检测到的异常。

DAGMM<sup>[15]</sup>(Zong 等,ICLR 2018):基于重建的多元

时间序列异常检测模型。其采用无监督异常检测,结合降噪自编码器和密度估计进行端到端的训练,有效避免了模型局部最优。最后模型采用欧氏距离和余弦相似度两种度量方式计算重构误差。

GANF<sup>[16]</sup>(Dai 等,ICLR2022):基于重建的多元时间序列异常检测模型。其采用无监督异常检测,通过贝叶斯网络建模因果关系的有向无环图,通过 RNN 建模时间序列;引入条件概率作为检测异常分数。

USAD<sup>[17]</sup>(Audibert 等,KDD2020):基于重建的多元时间序列异常检测模型。其采用无监督异常检测,在两阶段训练方案下训练两个自动编码器,包括一个共享编码器和两个单独的解码器(自动编码器训练阶段和对抗训练阶段)。

多元时间序列异常检测模型一般采用精确率 Precision、召回率 Recall,F1 分数作为性能评价指标。其中精确率 Precision 是检测出某类特征的数量与检测出的所有特征数量之间的比率,用于衡量模型的查准率;召回率 Recall 指检测出的某类特征的数量和数据集中所有该类特征数量的比率,用于衡量检索系统的查全率。综合评价指标(F1 分数)是准确率和召回率的调和平均值。精确率 Precision、召回率 Recall 和 F1 分数的计算式如下:

$$Precision = \frac{TP}{TP + FP} \quad (24)$$

$$Recall = \frac{TP}{TP + FN} \quad (25)$$

$$F1 = \frac{2TP}{2TP + FP + FN} \quad (26)$$

#### 4.3 缺失值场景下的性能对比实验

为了测试不同缺失率下删除数据后异常检测算法的性能表现,实验设计了 3 种缺失值场景:缺失率 10%、缺失率 30%、缺失率 50%。

由于传统多元时间序列异常检测模型只能在不包含缺失值的数据集上执行异常检测任务,因此,保证传统多元时间序列异常检测模型在包含缺失值的数据集上正常运行必须先对缺失值进行填充。在真实的场景中,数据收集系统往往会将缺失值标记为 NaN(Not a Number)。为了模拟这种场景,本文选取一个在数据集中不存在的值,并以固定值填充方法代替 NaN,例如 -1。

表 2—表 4 列出了各算法在 SWaT,SMD,WADI 数据集上、不同缺失率下的检测效果。在 SWAT 数据集上,MMAD 在缺失率为 50% 的情况下表现最好,相比次优方法(GDN)效果提升了 21%,在缺失率为 10% 的场景下表现最差,相比次优方法(GDN)提升了 0.2%,在 3 种缺失值场景下平均提升 8%。在 SMD 数据集以及 WADI 数据集上,MMAD 在 3 种缺失值场景下均展现了最优的效果,在 SMD 数据集上平均提升了 10%,在 WADI 数据集上平均提升了 15%。由实验结果可以发现,MMAD 在 3 个数据集的 3 种缺失值场景下均展现出了最优的性能,同时,在缺失率逐渐提高的情况下,性能衰减最少。

<sup>1)</sup>itrust.sutd.edu.sg/itrust-labs\_datasets/dataset\_info/

<sup>2)</sup>github.com/NetManAIOps/OmniAnomaly

表2 SWaT数据集上不同缺失值场景下的检测效果对比

Table 2 Comparison of detection effects under the scenario of different missing values on SWaT dataset

方法	缺失率=10%			缺失率=30%			缺失率=50%		
	F1	Precision	Recall	F1	Precision	Recall	F1	Precision	Recall
USAD	0.7331	0.9063	0.6155	0.5635	0.4238	0.8408	0.3636	0.2456	0.7003
GDN	0.7483	0.9140	0.6335	0.6609	0.8167	0.5550	0.5666	0.7271	0.4641
DAGMM	0.5089	0.4319	0.6193	0.4152	0.3455	0.5202	0.3386	0.2764	0.4370
GANF	0.7468	0.9101	0.6331	0.3048	0.2025	0.6154	0.1314	0.0703	1.0000
MMAD	<b>0.7504</b>	0.9889	0.6046	<b>0.6886</b>	0.8106	0.5986	<b>0.6869</b>	0.7840	0.6112

表3 SMD数据集上不同缺失值场景下的检测效果对比

Table 3 Comparison of detection effects under the scenario of different missing values on SMD dataset

方法	缺失率=10%			缺失率=30%			缺失率=50%		
	F1	Precision	Recall	F1	Precision	Recall	F1	Precision	Recall
USAD	0.7040	0.4949	0.9991	0.6142	0.4713	0.8815	0.5818	0.4392	0.8617
GDN	0.7040	0.6253	0.8054	0.4141	0.5955	0.3174	0.3517	0.2364	0.6871
DAGMM	0.6823	0.6235	0.7062	0.5793	0.5938	0.5655	0.5781	0.4643	0.7658
GANF	0.6098	0.5018	0.7770	0.5810	0.4779	0.7409	0.5808	0.4247	0.9185
MMAD	<b>0.7377</b>	0.7735	0.7050	<b>0.7025</b>	0.7367	0.6714	<b>0.6491</b>	0.5881	0.7243

表4 WADI数据集上不同缺失值场景下的检测效果对比

Table 4 Comparison of detection effects under the scenario of different missing values on WADI dataset

方法	缺失率=10%			缺失率=30%			缺失率=50%		
	F1	Precision	Recall	F1	Precision	Recall	F1	Precision	Recall
USAD	0.2167	0.2679	0.1930	0.1879	0.2551	0.1838	0.1866	0.1897	0.1836
GDN	0.1870	0.0842	0.5436	0.1185	0.0802	0.5177	0.1092	0.1092	1.0000
DAGMM	0.0913	0.0463	0.9732	0.0715	0.0441	0.9269	0.0643	0.0333	0.9286
GANF	0.2825	0.1466	0.5863	0.2228	0.1396	0.5584	0.1739	0.1667	0.1818
MMAD	<b>0.2963</b>	0.2207	0.4500	<b>0.2821</b>	0.2102	0.4286	0.2179	<b>0.2179</b>	0.5844

4.4 数据填充后的性能对比实验

由于对比方法都是面向完整数据集所设计的模型,为了更加公平地与对比方法进行比较,本文还设计了一组先填充数据集再进行性能对比的实验。填充使用均值(Mean)填充和中位数(Median)填充两种方法。

图3—图5分别展示了在SWaT, WADI, SMD数据集上的对比结果。

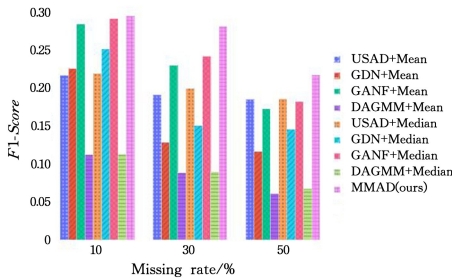


图3 SWaT数据集上有填充的检测效果对比结果

Fig. 3 Comparisons results of detection effects with populated data on SWaT data sets

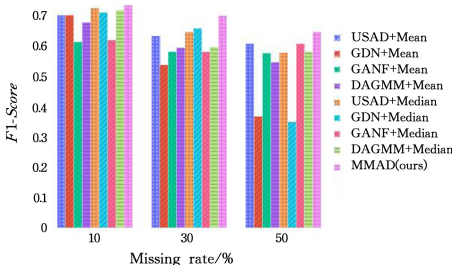


图4 WADI数据集上有填充的检测效果对比结果

Fig. 4 Comparisons results of detection effects with populated data on WADI dataset

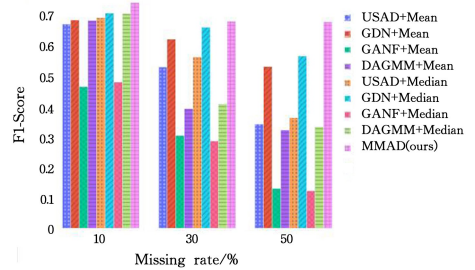


图5 SMD数据集上有填充的检测效果对比结果

Fig. 5 Comparisons results of detection effects with populated data on SMD dataset

在缺失率为10%的场景下,MMAD在WADI数据集上相比次优方法的F1-Score提升了24%,在SWaT数据集上相比次优方法提升了2%;在缺失率为30%的场景下,MMAD在WADI数据集上表现最好,相比次优方法的F1-Score提升了20%,在SWaT数据集上相比次优方法提升了5%;在缺失率为50%的场景下,模型在SMD数据集上相比次优方法的F1-Score提升了6%,在SWaT数据集上相比次优方法提升了4%。

本文在3个数据集上与多种方法在填充场景下的性能进行对比,结果表明,所提方法的性能结果均得到了提升,验证了所提方法的有效性。

4.5 消融实验

为了验证各模块对模型性能的贡献,在原有模型的基础上通过删除MMAR模块(W/O MMAR)和CNF-AD模块(W/O CNF-AD)与完整模型进行对比,实验场景为缺失率30%与缺失率50%,实验数据集选用SWaT数据集。

删除MMAR模块即删除模型的时间位置编码模块以及

掩码注意力表征模块,直接将数据通过 CNF-AD 模块进行异常检测任务;删除 CNF-AD 模块即删除模型的条件标准化流检测模块,由于删除该模块后模型无法通过条件标准化流来执行异常检测任务,故本文使用一个全连接层来替代 CNF-AD 模块,全连接层输出正常/异常标签。

通过消融实验结果发现,删除 MMAR 模块后,模型在缺失率 30%与 50%的情况下性能分别下降 27%和 49%,表明 MMAR 模块在缺失率 30%与 50%的场景下对数据建模起到了重要的作用。删除 CNF-AD 模块后模型在缺失率 30%和 50%的情况下性能分别下降了 34%与 38%,这表明 CNF-AD 能够有效识别异常。

#### 4.6 参数敏感性分析

窗口大小:数据集中存在不同的异常类型,有的异常类型持续时间较长,较大的窗口大小有助于模型发现异常;有的异常类型持续时间较短,较小的窗口大小有助于模型发现异常。为了验证 MMAD 对窗口大小的敏感性,实验对比了本模型在 SWaT 数据集上、缺失率为 30%的场景下不同窗口大小的性能,窗口大小为 5,10,20,50,100。表 5 列出了不同窗口大小的对比实验结果,模型在窗口大小为 10 的情况下 F1 分数达到最优。

表 5 窗口大小对比实验结果

Table 5 Experiment results of window size comparison

窗口大小	F1	Precision	Recall
5	0.5165	0.6080	0.4490
10	<b>0.6886</b>	<b>0.8106</b>	<b>0.5986</b>
20	0.6198	0.7295	0.5387
50	0.6680	0.7863	0.5806
100	0.5819	0.6850	0.5058

隐空间大小:掩码注意力表征模块将包含缺失值的时序数据进行重新表征,隐空间太小可能会导致信息的损失,隐空间过大可能会导致过拟合。

本实验选取模型在 SWaT 数据集上、缺失率为 30%、隐空间大小为 32,64,128,256,512 的对比结果。表 6 列出了对比实验结果,可以发现,隐空间大小为 256 的情况下 F1 分数表现最好。

表 6 隐空间大小对比实验结果

Table 6 Experiment results of hidden size comparison

隐空间大小	F1	Precision	Recall
32	0.6060	0.7133	0.5268
64	0.6198	0.7295	0.5387
128	0.6542	0.7701	0.5687
256	<b>0.6887</b>	<b>0.8106</b>	<b>0.5986</b>
512	0.5991	0.7052	0.5208

表 7 消融实验结果(SWAT 数据集)

Table 7 Ablation experiment results(SWAT dataset)

场景	缺失率 30%	缺失率 50%
W/O MMAR	0.5734	0.3405
W/O CNF-AD	0.4578	0.4958
MMAD	<b>0.6886</b>	<b>0.6869</b>

**结束语** 本文针对工业场景中更加常见的含缺失值的时间序列异常检测任务,提出了一种基于注意力重新表征的时间序列异常检测算法。该算法首先将包含缺失值的时间序列

数据通过时间位置编码对时间序列中不同时间戳关联性进行建模;然后通过掩码注意力表征模块学习不同时间戳之间数据的关联关系并将其表征为一个高维的嵌入式编码矩阵;最后引入条件标准化流对数据进行重建,以重建概率作为数据异常评分;最后本文通过实验分析了模型在不同缺失值场景下的性能表现、参数敏感性以及模型各模块的贡献。

下一步将考虑以下研究方向:1)改进掩码注意力表征模块,使模块不仅能够学习不同时刻的信息,还能够学习同一时刻不同指标之间的关联关系;2)在其他领域的多元时间序列异常检测任务上验证 MMAD 的有效性。

## 参考文献

- [1] CHOI K, YI J, PARK C, et al. Deep Learning for Anomaly Detection in Time-series Data: Review, Analysis, and Guidelines [J]. IEEE Access, 2021, 9: 120043-120065.
- [2] SUN Y, LI S H, CUI C, et al. Outlier Detection Method Based on Gauss Calibration Function for Power User Data [J]. Grid Technology, 2018, 42(5): 1595-1606.
- [3] PENG C, WANG L W, HU W L. Electromagnetic Spectrum Anomaly Detection Algorithm Based on Depth Feature Fusion [J]. Journal of Electronics, 2022, 50(6): 1359-1369.
- [4] SUN C F, LU W M, DAI H D, et al. A Small Sample Data Augmentation Method Based on Time GAN and OCSVM for Multivariate Degenerated Equipment [J]. Journal of Electronics, 2022, 50(11): 2678-2687.
- [5] ZHANG R B, ZUO Y C, ZHOU Z L, et al. Multimodal Generative Adversarial Networks Based Multivariate Time Series Anomaly Detection [J]. Computer Science, 2023, 50(5): 355-362.
- [6] ZHANG J E, WU D, BOULET B. Time Series Anomaly Detection for Smart Grids: A Survey [C] // 2021 IEEE Electrical Power and Energy Conference (EPEC). IEEE, 2021: 125-130.
- [7] PANG G, SHEN C, CAO L, et al. Deep Learning for Anomaly Detection: A Review [J]. ACM Computing Surveys (CSUR), 2021, 54(2): 1-38.
- [8] WENING P, SCHMIDL S, PAPPENBROCK T. TIMEEVAL: A Benchmarking Toolkit for Time Series Anomaly Detection Algorithms [J]. Proceedings of the VLDB Endowment, 2022, 15(12): 3678-3681.
- [9] MUNIR M, SIDDIQUI S A, DENGEL A, et al. DEEPANT: A Deep Learning Approach for Unsupervised Anomaly Detection in Time Series [J]. IEEE Access, 2018, 7: 1991-2005.
- [10] HUNDMAN K, CONSTANTINOU V, LAPORTE C, et al. Detecting Spacecraft Anomalies Using LSTMs and Nonparametric Dynamic Thresholding [C] // Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 2018: 387-395.
- [11] SU Y, ZHAO Y, NIU C, 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, 2019: 2828-2837.

- [12] CHEN Z, CHEN D, ZHANG X, et al. Learning Graph Structures with Transformer for Multivariate Time-Series Anomaly Detection in IOT[J]. IEEE Internet of Things Journal, 2021, 9(12):9179-9189.
- [13] VASWANI A, SHAZEER N, PARMAR N, et al. Attention is All You Need[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems, 2017:6000-6010.
- [14] DENG A, HOOI B. Graph NeuralNetwork-Based Anomaly Detection in Multivariate Time Series[C]//Proceedings of the AAAI Conference on Artificial Intelligence, 2021:4027-4035.
- [15] 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.
- [16] DAI E Y, CHEN J. Graph-Augmented Normalizing Flows for Anomaly Detection of Multiple Time Series[C]//International Conference on Learning Representations, 2022.
- [17] 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, 2020:3395-3404.
- [18] CHEN X, DENG L, HUANG F, et al. DAEMON: Unsupervised Anomaly Detection and Interpretation for Multivariate Time Series[C]//2021 IEEE 37th International Conference on Data Engineering (ICDE), IEEE, 2021:2225-2230.
- [19] LI D, CHEN D, JIN B, et al. MAD-GAN: Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks[C]//Artificial Neural Networks and Machine Learning—ICANN, 2019:703-716.
- [20] CHEN S W, LI J, XUAN J X, et al. LSTM-GAN: Unsupervised Anomaly Detection for Time Series Fusion of GAN and Bi-LSTM[J]. Journal of Chinese Computer Systems, 2024, 45(1):123-131.
- [21] REZENDE D, MOHAMED S. Variational Inference with Normalizing Flows [C] // International Conference on Machine Learning, PMLR, 2015:1530-1538.
- [22] GOH J, ADEPU S, JUNEJO K N, et al. A Dataset to Support Research in The Design of Secure Water Treatment Systems [C]//International Conference on Critical Information Infrastructures Security, Springer, 2016:88-99.



**ZENG Zihui**, born in 1997, postgraduate. His main research interests include artificial intelligence and anomaly detection.



**LIAO Qing**, born in 1988, Ph.D, professor, Ph.D supervisor. Her main research interests include artificial intelligence and data mining.

(责任编辑:何杨)