文章编号:1671-4598(2026)04-0065-07 DOI:10.16526/j.cnki.11-4762/tp.2026.04.009 中图分类号:TP273 文献标识码:A

面向多维时间序列在线异常检测模型研究

张洪斌[1]，习从婷[2]，田 铮[1]，马雅洁[1]
(1.北京首都国际机场股份有限公司，北京 100621；
2.华北电力设计院有限公司，北京 100120)

摘要：在线多维时间序列异常检测是保障系统稳定性、预防故障和降低风险的核心技术需求，为了有效检测多维时间序列的异常，结合多维时间序列异常特性，提出了一种双层自适应多维时间序列异常检测模型（TAMAD)；TAMAD模型采用分层设计，融合了核密度估计与联合生存函数，实现了局部异常和总体异常识别；针对现实场景下阈值难以确定难题，基于极值理论（EVT)，构建动态阈值调整机制；实验结果表明了TAMAD模型综合性能最优，兼顾高精度与强召回能力，适用于对可靠性要求高的场景，模拟数据的结果说明TAMAD模型能够很好地定位异常，提供异常合理解释。

关键词：异常检测；多维时间序列；总体异常；可解释

Research on Online Anomaly Detection Models for Multivariate Time Series

ZHANG Hongbin[1], XI Congting[2], TIAN Zheng[1], MA Yajie[1]
(1. Capital Airports Holding Co., Ltd., Beijing 100621, China;
2. North China Electric Power Design Institute Co., Ltd., Beijing 100120, China)

Abstract: It is a core technical requirement for online multi-dimensional time series anomaly detection to ensure the system stability, prevent failures, and reduce risks. To effectively detect the anomalies in multidimensional time series, a two-layer adaptive multidimensional time series anomaly detection model (TAMAD) based on the characteristics of these anomalies is proposed, which employs a hierarchical design, integrating kernel density estimation with joint survival functions to identify both local and global anomalies. To address the challenge of threshold determination in real-world scenarios, a dynamic threshold adjustment mechanism based on extreme value theory (EVT) is developed. Experimental results demonstrate that the TAMAD model has optimal overall performance, balancing high precision with strong recall, making it suitable for reliability-critical scenarios. Simulation results further show that the model can effectively localize anomalies and provide reasonable explanations for the anomalies.

Keywords: anomaly detection; multivariate time series; global anomalies; reasonable explanations

0 引言

时间序列异常检测是流量分析、工业物联网、金融监测、医疗诊断等领域的关键技术[1]，异常检测是识别时间序列中偏离数据正常趋势的值或事件的过程。随着物联网（IoT)、工业互联网和智能监控系统的快速发展，海量多维时间序列数据如传感器数据、金融交易记录、服务器日志等，被实时采集并用于关键决策，海量多维时间序列异常检测不仅可以识别单个维度上的异常，也可以识别不同维度之间的异常关联等。在此背景下，在线多维时间序列异常检测成为保障系统稳定性、预防故障和降低风险的核心技术需求。

传统的时间序列异常检测的主要目标是识别单个时间序列中偏离正常模式的点，可以分为两大类，第一类是基于统计模型的方法，例如Z-Score检测、Grubbs检验以及Boxplot等，第二类是基于机器学习的方法，例如基于机器学习的方法[2-4]。但是该类方法对噪声敏感，可能误报正常波动为异常，而且假设数据分布已知，对

收稿日期:2025-10-26； **修回日期**:2025-11-12。
作者简介:张洪斌(1980-),男,博士,高级工程师。
引用格式:张洪斌,习从婷,田 铮,等.面向多维时间序列在线异常检测模型研究[J].计算机测量与控制,2026,34(4):65-71.

非正态分布的数据效果较差，更难以捕捉复杂的异常模式。基于机器学习的方法适合数据维度较高或模式复杂时，但是对样本有要求，在很多场景下异常数据非常稀疏且样本成本高。近年来，深度学习模型在异常检测中取得不少进展，相关研究[5-7]说明通过 GAN 可以学习和重构时间序列，结合判别损失和重建误差识别异常，该方法在工业时间序列异常检测中表现优异，且开源了多变量数据集。Transformer-GAN 混合模型[8-10]可以融合 Transformer 的序列建模能力和 GAN 的生成能力，有效捕捉多变量间依赖关系，在工业传感器、通信流量等数据中实现高精度检测。但是深度学习的模型计算成本较高，效率和可解释性不足。与传统单维时间序列不同，多维时间序列的异常可能表现为维度间的关联性破坏、局部模式突变或全局分布偏移，这使得检测任务更具挑战性[11]。传统的时间序列异常检测对于高维时间序列或者非平稳时间序列等，由于很难捕捉多元序列间的关系[12]，也很难对序列整体进行分析，所以效果不佳。图注意力网络（GAT）[13-16]可以用来构建维度之间的关系，利用注意力权重动态捕捉变量间相关性，在物联网设备监测中实现高精度多变量异常定位。结合序列模型和图模型[17-21]来学习维度关系，从而识别多维序列的时间也吸引了一些研究者的注意。但是图注意力网络类方法也存在效率和可解释性问题，另外图注意力网络类方法还难以刻画多维数据分布导致的序列整体异常。

结合现有文献分析，由于深度学习模型复杂度较高，特别是多架构融合的模型，如 Transformer-GAN、GNN-自编码器混合模型，虽然兼顾时序依赖与数据分布建模，但是复杂度较高，难以在实践上使用。针对工业场景优化模型复杂度，设计可解释、轻量化的模型成为当前研究的趋势。针对多维时间序列异常检测的特性，提出一种双层自适应多维时间序列异常检测模型（TAMAD，two-layer adaptive multivariate time series anomaly detection model），模型基于滑动窗口实时更新统序列统计特征，无需预训练，可以适应数据分布变化。TAMAD 模型采用分层设计了 3 个关键模块，提高了模型的可解释性，首先是基于 KDE 模型检测单变量局部异常，基于核密度估计，构造条件度量的联合生存函数，采用概率学习融合局部异常和总体异常的识别，最后，为了适应数据的不断变化，基于极值理论（EVT），构建了动态阈值调整机制。TAMAD 属于无监督模型，无需标注数据，可以动态适应数据分布变化，可解释性强，可以实现异常定位和类型分析。

1 TAMAD 模型

与传统单维时间序列不同，多维时间序列的异常可能表现为维度间的关联性破坏、局部模式突变或全局分布偏移，这使得检测任务更具挑战性。另外，多维时间序列的维度高且可能存在冗余或噪声，传统的异常检测方法难以有效建模变量间的非线性关系，易导致误报或漏报。多维时间序列的异常检测模型需要满足下面的一些特性：1）低延迟处理，要求模型可以用流的方式动态接收数据流并实时输出检测结果；2）高维特征建模，要求模型能捕捉多维变量间的复杂依赖关系和分布特性；3）异常样本稀疏和多样性，要求模型能够在无监督学习或弱监督学习构建模型并且具有一定的可解释性。由于不同维度可能存在相关关系，因此多维时间序列异常检测需要捕捉单个维度序列特征的同时还需要建模不同维度的相关性。

交通流量、网络流量以及交易流量等是典型的多元时间序列，例如对于一个大型复杂的网络系统，流量分布在不同的路由设备上，路由设备的流量为一个多元时间序列数据流。类似的，在金融领域，例如股票市场，每个交易时间点上或产生所有上市公司的交易行情，也是多元时间序列数据流。这类多元时间序列数据流的异常检测首先需要考虑单个时间序列自身的变动异常。其次作为一个系统，这些多元序列变量之间存在关系，需要考虑不同变量之间的关系，检查数据在多元变量之间的分布特性发现异常。此外，如果多元时间序列的共同作用影响整体系统的稳定性，例如股票市场个股资金流会影响市场的整体资金流，则还需要考察多元序列的整体分布，检查总体异常。

基于上述分析，提出一种双层自适应多维时间序列异常检测模型（TAMAD，two-layer adaptive multivariate time series anomaly detection model），TAMAD 模型通过学习单个维度序列的分布特性，采用动态滑动窗口，构建高速的无监督检测，在获得异常的同时得到异常概率。考虑到多元序列变量作系统整体的输出，系统整体异常可能是单个维度之间的联合分布发生异常，所以接下来对个体异常概率进行联合分布建模，将整体异常建模为联合概率分布的异常。模型总体架构如图 1 所示。

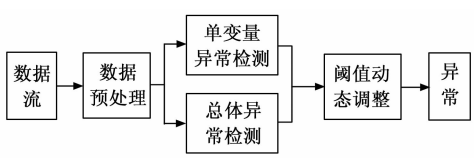


图 1 TAMAD 模型流程结构图

TAMAD 模型数据总体包含 4 个处理模块：1）预处理模块，主要进行标准化、去趋势和滑动窗口生成。2）2 个核心检测模块，分别是单变量异常检测模块，采用统计模型得到单变量的异常以及异常概率；总体异常检测模块分析系统总体异常程度，通过求解联合概率

分布计算整体流量的异常分数。3）阈值动态调整模型，单变量异常检测模块和总体异常检测模块输出异常概率，通过阈值判别是否异常。阈值动态调整模型基于极值理论构建动态阈值，实现序列中去趋势化和去季节化，避免误差信号的干扰，输出最终异常类型与分数。TAMAD 模型采用分层模块化设计，将单变量异常检测、整体异常检测进行分解和集成，提高了模型的可解释性，支持复杂场景，能够同时检测单变量突变、整体流量波动和分配比例偏移。TAMAD 模型在智能个体异常检测中引入核密度估计（KDE），直接建模多维比例分布，更精准地捕捉多变量间的复杂依赖关系，尤其在高维数据中表现优异。

为了形式化地讨论模型，首先，给出相关符号和定义，由于预处理模块主要用于处理序列的读取、对齐等任务，所以主要分析讨论 TAMAD 模型的 3 个核心模块。

1）符号定义与基本假设：

设一个多元时间序列数据流为：$\boldsymbol{X}^t = \{X_1^t, X_2^t, \cdots, X_n^t\}$，其中 X_i^t 为第 i 个变量的时间序列。

设模型对单个变量的异常测度称为单变量局部异常分数，记做：$S_i^{\text{local}} = F_{\text{local}}(X_i^t)$，多元序列代表的系统整体的异常程度称为全局异常分数，记作 $S^{\text{global}} = F_{\text{global}}(\boldsymbol{X}^t)$。

由于异常是否发生是一个概率测度，所以定义概率转换函数：

单变量正常概率密度：$p_i^{\text{local}}(s) = P(S_i^{\text{local}} = s \mid \text{正常})$；

全局正常概率密度：$p^{\text{global}}(s) = P(S^{\text{global}} = s \mid \text{正常})$。

对于大型系统的多元时间序列数据流，每个节点产生的信号变量是独立的，如果不独立，则可以通过依赖关系去除相关变量，所以我们假设：

（1）单变量异常与全局异常在正常状态下服从独立生成过程；

（2）异常状态下至少存在一个维度（单变量或全局）的生成过程发生显著偏移。

2）TAMAD 模型：

为了实现高维多元时间序列在线异常检测，我们构建了双层自适应多维时间序列异常检测模型，模型包含 3 个核心模块：

（1）单变量异常检测：

首先采用动态滑动窗口，构建高速的无监督检测。算法流程如下：

算法 1：单变量异常检测

输入：时间序列 $\boldsymbol{X}^t$

输出：时间序列中每个维度的异常得分 $\boldsymbol{S}_i^{\text{local}}$

对变量 $\boldsymbol{X}_i^t$，其滑动窗口 $\boldsymbol{W}(\boldsymbol{X}_i^t) = (x_i^{t-w+1}, \cdots, x_i^{t-1})$，长度 $\boldsymbol{W}$。

计算中位数 $m_i = median[\boldsymbol{W}(\boldsymbol{X}_i^t)]$，记 $\sigma(m_i) = MAD[\boldsymbol{W}(\boldsymbol{X}_i^t)]$

计算偏差：$\boldsymbol{Z}_i^t = \sigma(m_i) \times (\boldsymbol{X}_i^t - m_i)$

单变量的异常分数为：$\boldsymbol{S}_i^{\text{local}} = \max(\boldsymbol{Z}_i^t)$

return(S_i^{local})

算法 1 中，动态滑动窗口划分的基本依据是时间序列的特性，如果序列具有周期性，窗口长度设置为周期的 3 倍，否则采用交叉验证评估不同窗口长度下的统计量显著性得到。

基于算法 1 的单变量异常得分，单变量异常检测模块通过阈值比较来判别异常状态。

（2）总体异常检测：

为了测度系统总体异常，我们主要将通过个体异常概率进行联合分布建模，将总体异常用联合概率表达，然后设置阈值，通过阈值比较来判别异常状态。总体异常模型的详细逻辑如下：

首先，建立正常状态下的联合分布，对每个单变量异常概率 S_i^{local} 和全局异常概率 S^{global}，通过核密度估计（KDE）建模其边缘分布：

$$p_i^{\text{local}}(s) = \frac{1}{Nh_i} \sum_{k=1}^{N} K\left(\frac{s - S_i^{(k)}}{h_i}\right) \tag{1}$$

$$p^{\text{global}}(s) = \frac{1}{Nh_g} \sum_{k=1}^{N} K\left(\frac{s - S_{\text{global}}^{(k)}}{h_g}\right) \tag{2}$$

其中：h_i，h_g 为带宽参数，$K(\cdot)$ 为核函数，采用高斯核。带宽参数 h 的选择会影响 KDE 模型的敏感性和鲁棒性，为了平衡计算代价和模型的效果，我们采用了自适应带宽（Adaptive Bandwidth）技术，根据数据点的局部密度动态调整带宽，计算方法为：

$$h_i = h_0 \cdot f(x_i)^{-1/2} \tag{3}$$

其中：h_0 为全局带宽，$f(x_i)$ 为局部密度，自适应带宽能够更好地捕捉局部异常。

计算全局异常概率，单变量异常概率定义为当前观测值的概率密度在正常分布中的生存函数：

$$P_i^{\text{local}} = 1 - \int_{(-\infty)}^{s_i} p_i^{\text{local}}(u)du = 1 - F_i^{\text{local}}(s_i) \tag{4}$$

同理，有全局异常概率：

$$P^{\text{global}} = 1 - F^{\text{global}}(s_{\text{global}}) \tag{5}$$

全局异常概率的计算需要联合分布，在独立性假设下，正常状态的联合生存函数为：

$$P(\text{正常}) = \prod_{i=1}^{n}(1 - P_i^{\text{local}}) \cdot (1 - P^{\text{global}}) \tag{6}$$

所以，总体异常概率的定义为：

$$P^{\text{total}} = 1 - P(\text{正常}) =$$

$$1 - \left[\prod_{i=1}^{n}(1 - P_i^{\text{local}})\right] \cdot (1 - P^{\text{global}}) \tag{7}$$

为降低计算复杂度，我们采用最大单变量异常概率近似计算总体异常概率：

$$P^{\text{total}} \approx 1 - (1 - \max_i P_i^{\text{local}}) \cdot (1 - P^{\text{global}}) \tag{8}$$

3）基于极值理论（EVT）动态阈值调整：

单变量异常检测和总体异常检测都需要设置阈值，对于流量异常检测，不仅需要快速检测，更重要的数据流随着业务和设备的发展，异常阈值会随着变化，所以需要构建动态阈值，实现异常检测的自适应性。我们基于极值理论构建动态阈值。算法主要过程，首先对异常分数序列 S_t 进行去趋势化和去季节化，提取残差序列 R_t，其次用平均超额函数法确定初始阈值，并极大似然估计拟合广义帕累托分布（GPD），最后用滑动窗口进行分位数阈值选择。

阈值选择：使用平均超额函数法确定初始阈值 u：

$$E(u)=\frac{\sum_{R_t>u}(R_t-u)}{N_u},$$

$$N_u=\text{满足 } R_t>u \text{ 的数据量} \tag{9}$$

选择 u 使得当 $R_t>u$ 时，$E(u)$ 近似线性增长。

拟合 GPD 分布，对超过阈值 u 的极端值 $\{R_t-u \mid R_t>u\}$，用极大似然估计拟合 GPD：

$$\mathrm{GPD}(x;\xi,\sigma)=1-\left(1+\frac{\xi x}{\sigma}\right)^{-1/\xi} \tag{10}$$

其中：ξ 为形状参数，σ 为尺度参数

动态阈值计算：首先设定容忍风险水平 α，计算分位数阈值如下：

$$\theta_t=u+\frac{\sigma}{\xi}\left\{\left[\frac{n_u}{N}(1-\alpha)\right]^{-\xi}-1\right\} \tag{11}$$

其中：n_u 是超过 u 的样本数，N 为总样本数。实践上通常设定 $\alpha=0.99$。

在真实场景下新的数据会产生统计量漂移，所以需要在线更新参数。结合历史数据，模型可以实现参数 u，ξ，σ 的进行自动更新，主要采用滑动窗口定期重新估计。

2 实验设计与结果分析

为了衡量 TAMAD 模型的有效性，我们选择了多个模型在不同的数据集上进行了大量实验。由于目前多数模型是带监督的，为了合理的分析和对比模型，我们在实验中采用了有监督的训练方法，用样本进行模型参数训练。

2.1 实验设置

为了客观评价模型的效果，对比模型我们分别从传统统计模型、机器学习模型以及深度学习模型选择了主要的代表性模型，这些模型可以适用于不同场景，具有较好的效果，具体如表 1 所示。

为了全面地对比不同模型的效果，我们首先将无监督的异常检测转化为有监督的对比，然后采用主要的分类评估指标，评估指标具体含义和计算说明如表 2 所示。

表 1 对比模型

模型类型	典型算法	适用场景
传统统计模型	KDE	数据分布稳定、低噪声场景
机器学习模型	Isolation Forest	中等维度、可解释性要求高
深度学习模型	LSTM-VAE、MSCRED、GANomaly	高维复杂模式、时序依赖强

表 2 实验评估指标

指标	公式/定义	说明
P	$TP/(FP+TP)$	准确率 P，关注误报率
R	$TP/(TP+FN)$	召回率 R，关注漏报率
F_1	$2\times[P\times R/(P+R)]$	平衡精确率与召回率
AUC-ROC	ROC 曲线下的面积	类别不平衡场景

为了综合全面地对比不同模型的性能，我们选择了目前公开领域的主要数据集进行实验，实验数据的特性、具体含义和说明如表 3 所示。数据集涵盖了工业领域、网络流量以及互联网行为等领域，具有较好的代表性。

表 3 实验数据集说明

数据集	维度	异常类型	典型应用领域
NASA PCoE	27	设备退化、传感器故障	工业设备监控
SWaT	51	攻击注入、物理故障	关键基础设施安全
Yahoo A1	5	网络流量突变、服务异常	IT 运维监控
KDD Cup 2018	20	能源消耗异常	智能电网
NAB	30	点异常、上下文异常	通用基准测试

2.2 实验结果与分析

我们首先对各模型在不同数据集上的性能表现进行了分析，图 2 给出了不同模型在不同数据上的 P 的结果。由于 MSCRED 模型训练原因，我们没有在 Yahoo A1 和 NAB 数据集上得到结果。图 3 给出了不同模型在不同数据上的 R 的结果。

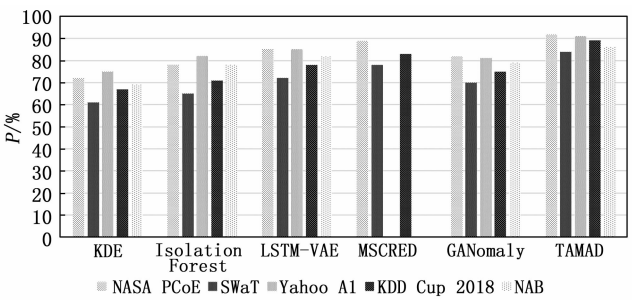


图 2 不同模型在不同数据上的 P 的结果

从图 2 和图 3 可以看出，TAMAD 比其他模型都获得了较好的效果，特别是对于维度较高的数据集 SWaT 和 NAB，TAMAD 模型都超过其他模型。例如，MSCRED 模型的性能也比较均衡。对于高维数据，如 SWaT，深度学习模型因捕捉空间－时间相关性表现优

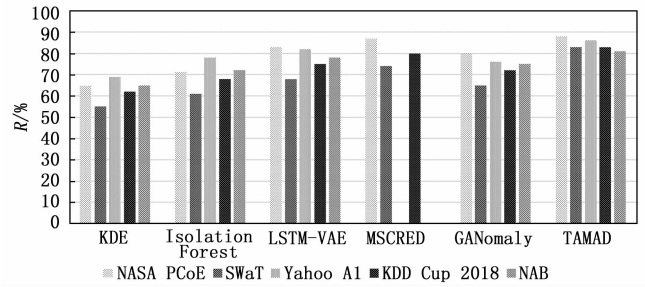


图 3　不同模型在不同数据上的 Recall 的结果

异。而传统模型，如 KDE 因维度灾难性能显著下降。在低维数据上，Isolation Forest 表现良好，因其计算效率高且对低维数据鲁棒。

从各模型在不同数据集上的表现来看，TAMAD 在绝大多数指标上都领先，尤其在 P 和 R 的平衡性上表现突出，如 NASA PCoE 中 P 92%/R 88%，SWaT 中 P 84%/R 83%，都超出了其它模型的结果。这表明其在复杂时序数据中捕捉异常模式的能力较强。MSCRED 在部分数据集（如 NASA PCoE 和 KDD Cup 2018）中表现接近 TAMAD，但存在数据缺失问题（如 Yahoo A1 和 NAB 中无结果），可能受限于模型对特定数据结构的适应性。LSTM-VAE 和 GANomaly 作为生成模型，整体优于传统方法（如 KDE 和 Isolation Forest），但略逊于 TAMAD，反映其在复杂场景中仍有优化空间。传统方法中，Isolation Forest 表现稳定但平庸，而 KDE 在多数场景中表现最弱，说明基于密度估计的方法在时序异常检测中存在局限性。

由于有些数据的类别不平衡，如 KDD Cup，所以我们单独把各个模型的 AUC-ROC 结果列在表 4 中。因 P 和 R 受异常比例影响较大，而 *AUC-ROC* 可以较好地表示不同类上总体的效果，这也是深度学习模型通常在 R 上表现更好，但 P 可能略低，如 GANomaly 的原因。从 AUC-ROC 分析，LSTM-VAE、MSCRED 在所有数据集上均取得较高 AUC-ROC 值。传统模型（如 KDE）在低维数据上表现尚可，但在高维数据上表现较差。TAMAD 模型在所有的数据集上都取得了最好效果，说明 TAMAD 模型在不同类型的数据集上都可以很好

表 4　不同模型在不同数据上的 AUC-ROC 结果　%

模型	NASA PCoE	SWaT	Yahoo A1	KDD Cup 2018	NAB
KDE	78	68	78	71	75
Isolation Forest	82	71	85	75	80
LSTM-VAE	89	78	89	82	85
MSCRED	92	84	—	87	—
GANomaly	86	75	84	80	83
TAMAD	95	89	92	91	89

地完成检测任务，对于类不平衡的时间序列，模型也可以很好地检测出来异常。

为了分析单变量异常检测时，窗口对结果的影响，我们对比分析了不同窗口长度在 NASA PCoE 数据集上的性能表现，结果如表 5 所示。从表中可以看出，模型随着窗口的变化性能会有一定的波动，在窗口长度为 100 时，性能达到最佳。虽然性能有波动，但是总体而言，模型的 AUC-ROC 具有较好的结果。窗口变长时，统计量过于平滑，模型对近期变化的敏感性下降（Recall 降低）。根据性能分析，实践上采用了窗口为 100。

表 5　不同窗口长度在 NASA PCoE 数据集的表现　%

窗口长度/w	P	R	*AUC-ROC*
30	75	80	82
50	78	82	85
100	82	85	89
200	80	83	87
500	77	81	84

2.3　模拟实验结果与分析

为了深入分析 TAMAD 模型的性能和探索结果的可解释性，我们构造了一个模拟数据，采用人工添加不同类型的异常，基于模型的检测结果，对照检测出来的异常点以及异常决策逻辑来分析异常的合理性和可解释性。

首先，基于多元高斯分布生成正常数据，数据值以 0 均值。这样构造一个维度为 3 的多维时间序列，然后在序列的不同的维度和时间点注入异常，分别注入 4 个不同类型的异常，形成 4 个样本。人工异常的类型分别是单变量联合异常、单变量异常、单变量异常＋全局异常、单变量正常但全局值低。这些异常分别反映了个体和整体异常，以便观察模型是否可以有效识别不同类型的异常。异常分布的样本值为：

样本 1：[3.2，2.9，3.1]，＃单变量联合异常

样本 2：[0.1，－0.5，4.0]，＃单变量异常＋全局异常

样本 3：[－2.0，－3.0，－1.5]，＃正常（但全局值低）

样本 4：[2.5，2.0，5.0] ＃明显异常

图 4 给出了异常点在不同维度的分布情况，其中横坐标为样本观测值的大小，纵坐标为观测值的发生概率，从图 4 可以看出，有两个异常点（异常点 3、4）在维度 0 处于分位数较高的位置，但是异常点 0、1 处于分位数的中间。类似的，4 个异常点在维度 1 和维度 2 上很难通过分数值区分，这为一般的异常检测方法带来很大的挑战。

用 TAMAD 模型检测样本后的结果如表 6 所示，

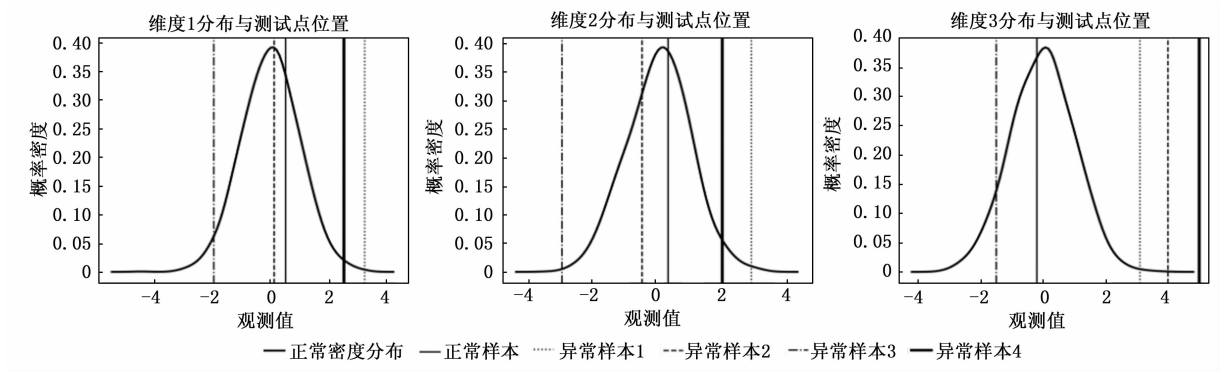


图 4 异常在不同维度的分布情况

从表上可以看出，模型检测到 5 个异常点，分别标记为样本 0～4。其中样本 1～4 分别和模拟数据中注入的异常样本 1－样本 4 对应，而样本 0 则是系统发现的新的异常。模型检测到的样本 1－样本 4 的异常类型、异常值以及主要异常维度和注入的异常一致，说明 TAMAD 模型不仅具有良好的性能，还具有准确的异常点定位功能。

表 6 TAMAD 模型检测模拟样本的结果

样本	异常维度	维度异常值	全局	决策逻辑
样本 0	维度 0	0.5	0.60（否）	多维度轻微异常叠加
样本 1	维度 0	3.2	9.20（是）	维度 0 出现极端值(3.2) ＋ 总流量显著偏离常态
样本 2	维度 2	4	3.60（是）	维度 2 出现极端值(4.0) ＋ 总流量显著偏离常态
样本 3	维度 1	－3	－6.50（是）	维度 1 出现极端值(－3.0) ＋ 总流量显著偏离常态
样本 4	维度 2	5	9.50（是）	维度 2 出现极端值(5.0) ＋ 总流量显著偏离常态

从检测异常的决策逻辑分析，模型给出了明确的异常逻辑和异常类型说明，例如样本 1 和样本 4，不仅单个维度检测出来异常，也检测出总体流量也存在异常，说明模型检测的异常结果具有合理的逻辑和判别条件。

我们把用 TAMAD 模型检测到的异常样本投影到 3 维空间中，给出异常点分布的图，如图 5 所示，其中维度 1，维度 2 以及维度 3 为样本观测值的大小。从图 5 可以看出，模型检测到异常点样本 1 到样本 4 分布在 3 维空间的分布都可以较好的和正常数据分离。样本 0 虽然和正常数据分离度交差，虽然概率较低，但模型还是检测到弱的整体异常。

3 结束语

针对复杂的多维时间序列异常检测问题，结合多维时间序列的分布特征、异常类型等特性，提出一种双层

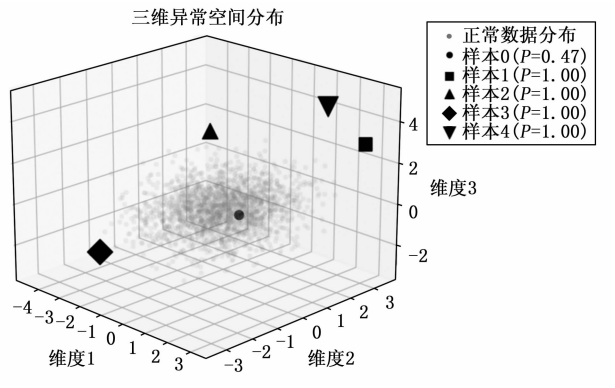


图 5 异常在不同维度的分布情况

自适应多维时间序列异常检测模型 TAMAD，模型基于滑动窗口实时更新系统序列统计特征，可以较好地发现多维时间序列中的异常，可以动态适应数据分布变化，可以实现异常定位和类型分析。从真实数据和模拟数据进行大量实验对比，选择了目前主要的方法作为基准。实验结果表明 TAMAD 模型综合性能最优，兼顾高精度与强召回能力，适用于对可靠性要求高的场景，深度模型在复杂时序模式挖掘中优势明显，适合多维、长序列数据。模拟数据的结果说明 TAMAD 模型能够很好地定位异常，提供异常合理解释。

由于复杂社会和工业场景中，时间序列的维度和频率都特别高，超高维数据会导致“维度灾难”，使得 KDE 难以有效捕捉变量间的依赖关系。另外，在实时性要求高的场景，如工业监控、金融交易等，需要毫秒级响应，而复杂模型通常计算开销大，TAMAD 模型虽然比较了复杂矩阵的计算开销，但是计算全局分布时依然代价较高。在实际应用中，时间序列也可能会有大量的缺失，导致数据稀疏，稀疏数据会显著影响统计量的估计。针对这些实际应用场景，未来，面临超高维数据时，可以探索使用主成分分析、t-SNE 或自编码器（Autoencoder）将高维数据投影到低维空间或者开发稀疏核密度估计方法，如 Sparse KDE 等，减少对无关变量的依赖。面临实时要求和海量高频数据，可以探索利

用分布式框架并行处理高频数据流或者使用 GPU/TPU 加速深度学习模型推理，或开发专用硬件（如 FPGA）实现高效计算。面临数据中的稀疏特性时，可以探索使用生成对抗网络或变分自编码器填补稀疏区域的数据。

参考文献：

[1] ETSI Technical Committee. SynSig：anomaly-aware synthetic signal generation using conditional GANs [R]. TR 103 582. European Telecommunications Standards Institute，2022.

[2] SHIN Y，LEE S，TARIQ S，et al. ITAD：integrative tensor-based anomaly detection system for reducing false positives of satellite systems [C] // Proceedings of the 29th ACM International Conference on Information & Knowledge Management，New York：Association for Computing Machinery，2020：2733－2740.

[3] BREUNIG M M，KRIEGEL HP，NG R T，et al. LOF：identifying density-based local outliers [C] // Proceedings of ACM SIGMOD International Conference on Management of Data，New York：Association for Computing Machinery，2000：93－104.

[4] MA J，PERKINS S. Time-series novelty detection using one-class support vector machines [C] // Proceedings of the International Joint Conference on Neural Networks. Piscataway，NJ：IEEE Press，2003：1741－1745.

[5] LI D，CHEN D，JIN B，et al. MAD-GAN：Multivariate anomaly detection for time series data with generative adversarial networks [C] // Proceedings of the 28th International Conference on Artificial Neural Networks，Springer，2019：703－716.

[6] ZHANG Y，LI X，WANG Z. Real-time anomaly detection in crowdsourcing data streams via dynamic attention GAN [J]. IEEE Transactions on Knowledge and Data Engineering，2021，34 (8)：3894－3905.

[7] CHEN W，TIAN L，CHEN B，et al. Deep variational graph convolutional recurrent network for multivariate time series anomaly detection [C] // Proceedings of the 2022 International Conference on Machine Learning，Maryland：PMLR，2022：3621－3633.

[8] HUO W，ZHANG Q，LIU Y. Random transformer for nonlinear temporal dependency modeling in communication networks [J]. IEEE Transactions on Network Science and Engineering，2022，9 (3)：1241－1253.

[9] CHEN J，XU R. Cross-dimensional attention fusion network for ECG anomaly detection [J]. Medical Image Analysis，2023，85：102732.

[10] XU J，WU H，WANG J，et al. Anomaly transformer：time series anomaly detection with association discrepancy [C] //Proceedings of the 10th International Conference on Learning Representations（ICLR 2022），2022：1－10.

[11] ZHANG C X，SONG D J，CHEN Y C，et al. A deep neural network for unsupervised anomaly detection and diagnosis in multivariate time series data [C] // Proceedings of the 33rd AAAI Conference on Artificial Intelligence，Palo Alto，CA：AAAI Press，2019：1409－1418.

[12] 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.

[13] ZHAO H，WANG Y，DUAN J，et al. Multivariate time-series anomaly detection via graph attention network [J]. IEEE Internet of Things Journal，2020，7 (9)：8167－8181.

[14] LIANG L，LI F. Spatial-temporal graph convolutional networks for traffic anomaly detection [J]. Transportation Research Part C：Emerging Technologies，2021，129：103214.

[15] WANG S B，GUO Y，HUANG S H，et al. A deep graph neural network-based link prediction model for proactive anomaly detection in discrete manufacturing workshop [J]. Journal of Manufacturing Systems，2025，79：301－317.

[16] LI S，LI W，COOK C. Hierarchical metric-temporal graph embedding for cloud cluster monitoring [C] // Proceedings of the 37th AAAI Conference on Artificial Intelligence，AAAI Press，2023：4567－4575.

[17] WANG X，LI J. SPD autoencoder with multiscale trend analysis for mine disaster monitoring [J]. IEEE Sensors Journal，2021，21 (15)：17102－17112.

[18] KIM S，PARK H. Frequency-enhanced LSTM autoencoder for stealthy anomaly detection [J]. Expert Systems with Applications，2022，198：116856.

[19] ZHANG T，YU H. Adversarial reconstruction autoencoder for concept drift adaptation in smart meters [J]. IEEE Transactions on Smart Grid，2020，11 (5)：4321－4332.

[20] DEMPSTER A，PETITJEAN F，WEBB G I. ROCKET：Exceptionally fast and accurate time series classification using random convolutional Kernels [J]. Data Mining and Knowledge Discovery，2020，34 (5)：1454－1495.

[21] PARK J，LEE K. Dynamic pattern library updating for financial transaction anomaly detection [J]. ACM Transactions on Knowledge Discovery from Data，2023，17 (3)：1－25.