计算机科学
COMPUTER SCIENCE

基于多模态生成对抗网络的多元时序数据异常检测

张仁斌, 左艺聪, 周泽林, 王龙, 崔宇航

引用本文

张仁斌, 左艺聪, 周泽林, 王龙, 崔宇航基于多模态生成对抗网络的多元时序数据异常检测[J]. 计算机科学, 2023, 50(5): 355-362.

ZHANG Renbin, ZUO Yicong, ZHOU Zelin, WANG Long, CUI Yuhang. Multimodal Generative Adversarial Networks Based Multivariate Time Series Anomaly Detection [J]. Computer Science, 2023, 50(5): 355-362.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220400221

基于多模态生成对抗网络的多元时序数据异常检测

张仁斌[1,2]　左艺聪[1]　周泽林[1]　王　龙[1]　崔宇航[1]
1 合肥工业大学计算机与信息学院　合肥 230601
2 工业安全与应急技术安徽省重点实验室　合肥 230601

摘　要　针对传统多元时序数据异常检测模型未考虑时空数据的多模态分布问题,提出了一种多模态生成对抗网络多元时序数据异常检测模型。利用滑动窗口分割时间序列并构造特征矩阵来捕获数据的多模态特征,将其与原始数据分别作为模态信息输入多模态编码器及多模态生成器中,输出具有时空信息的多模态特征矩阵,并将真实数据编码成特征矩阵,将两类特征矩阵作为判别器输入,利用梯度惩罚方法并拟合真实分布与生成分布之间的 Wasserstein 距离,取代二分类交叉熵损失训练判别器,结合生成器重构误差及判别器评分实现异常检测。基于安全水处理(SWaT)及水量分布(WADI)等数据集的测试结果表明,所提模型相比基准模型在 F1-分数性能指标上分别提升了 0.11 和 0.19,能够较好地识别多元时序数据异常,具有较好的鲁棒性以及泛化能力。

关键词:多元时间序列;异常检测;半监督学习;对抗学习;多模态
中图法分类号　TP311.13

Multimodal Generative Adversarial Networks Based Multivariate Time Series Anomaly Detection

ZHANG Renbin[1,2],ZUO Yicong[1],ZHOU Zelin[1],WANG Long[1] and CUI Yuhang[1]
1 School of Computer Science and Information Engineering,Hefei University of Technology,Hefei 230601,China
2 Anhui Province Key Laboratory of Industry Safety and Emergency Technology,Hefei 230601,China

Abstract　Aiming at the problem that the traditional anomaly detection model of multivariate time series data does not consider the multimodal distribution of spatio-temporal data,a multivariate time series data anomaly detection model based on multimodal generative adversarial networks is proposed. The sliding windows is used to segment the time series and construct feature matrices,so as to capture the multimodal features of the data. Feature matrix and raw data are fed into the multimodal encoder and multimodal generator as modal information respectively,then multimodal feature matrix with spatio-temporal information is outputted. The real data is encoded into feature matrices and the two types of feature matrices are utilized as discriminator inputs. In the proposed method,a gradient penalty method and the Wasserstein distance between the real and generated distributions to replace the binary cross-entropy loss are utilized to train the discriminator,then combining the generator reconstruction error and discriminator scores to detect anomalies. Experimental results based on the secure water treatment(SWaT) and the water distribution(WADI) datasets show that,compared with the baseline model,the proposed method improves the F1-score metrics by 0.11 and 0.19 respectively. The proposed method can identify multivariate time series data anomalies well,with good robustness and generalizability.

Keywords　Multivariate time series,Anomaly detection,Semi-supervised learning,Adversarial learning,Multimodal

1　引言

随着物联网和传感技术的发展,时序数据越来越庞大且变量之间的关系变得越来越复杂,基于时序数据的异常检测成为当前的热点和难点问题之一[1]。异常检测是检测序列中异于正常序列的序列,这种差异由不同的机制产生[2-4]。

现实系统中,网络传感器和执行器的普及生成了大量的多元时间序列数据,这些变量具有非线性的相关性。因现实系统的复杂性日益增加且人工标注数据成本较高,基于监督学习的多元时序数据异常检测的方法浪费了大量未标记数据,同时,为了提升监督学习方法的泛化能力,基于半监督学习的时序数据异常检测成为一类有效的检测方法。一方面,当今系统的动态复杂性,且监督学习方法由于缺乏标记数据而无法利用大量数据,导致传统的异常检测方法表现较差;

到稿日期:2022-04-22　返修日期:2022-09-11
基金项目:国家重点研发计划(2016YFC0801804,2016YFC0801405);中央高校基本科研业务费专项资金资助(PA2019GDPK0074)
This work was supported by the National Key Research and Development Projects of China(2016YFC0801804,2016YFC0801405) and Fundamental Research Funds for the Central Universities of China(PA2019GDPK0074).
通信作者:张仁斌(zhangrb@hfut.edu.cn)

另一方面，时序数据中多个变量(传感器/驱动器)之间是相互影响和依赖的，利用变量之间存在的大量信息对于检测模型的效果与性能也十分重要。然而基于时间单模态的自训练半监督异常检测模型存在以下问题：不能很好地处理时间相关性或者空间相关性的混合属性数据；忽略了时空数据的多模态分布，使得模型对数据集有依赖性，因此不能提供一个很好的多元时间序列异常检测范式。

为了有效地建立拟合时序关系以及变量之间的依赖性，同时为了解决对抗网络模型难以训练的问题，本文提出了一种基于多模态生成对抗网络(Generative Adversarial Networks，GAN)的多元时序数据异常检测模型，充分利用多元时序数据的时序关联性和特征相联性，构建混合模态生成器及混合模态编码器，用于学习并生成时序数据高维分布。本文的主要贡献如下：

(1)提出了一种通用的多模态编码器-多模态生成器-判别器框架，引入一种特征矩阵构造方式来获取时序数据的变量间的信息，通过编码器及生成器挖掘数据的时序特征分布，实现对时序数据异常的有效检测。

(2)提出了一种基于 GAN 的多元时间序列数据异常检测方法，该方法采用本文提出的多模态编码器-多模态生成器-判别器框架，实现正常时序信息关于时间和空间分布的联合学习，通过将异常检测问题转化为对序列进行重构和判别的问题，在这两个模态上度量时序数据的异常值。本文将由该方法形成的模型称为多模态生成对抗网络多元时序数据异常检测模型。实验证明，该方法能够很好地拟合时空中的非线性关系，从而实现时序信息的异常检测。

2 相关工作

传统统计算法用数据统计方式检测明显异于正常值的点，如整合移动平均自回归(Auto-Regressive Integrated Moving Average，ARIMA)模型[5]，其因对特征数据仅进行线性变换，使得模型存在特征之间及时序之间的非线性拟合性较低的问题。

现阶段除了传统统计算法之外，针对时序数据的异常检测研究还包括基于马尔可夫模型的方法[6]、基于距离检测的方法[7]等基于传统机器学习的方法，以及基于长短期记忆网络(Long Short Term Memory，LSTM)[8]、基于 Transformer[9]等深度学习方法。

传统机器学习算法利用传统机器学习进行异常值筛选，如通过异常点 k 近邻距离远大于正常点近邻距离的理论来检测异常[10]，以及主成分分析(Principal Components Analysis，PCA)[11]通过改变原有的特征空间，根据数据投影在残差子空间的大小来检测异常，但该类方法均不能有效捕获时间信息，不适用于大数据集。Wilinski[12]利用图遍历和马尔可夫链进行相似矩阵转换来检测多元时序数据的异常，但因其需要异常状态的先验知识及各种状态变化概率，且需要假设时序数据稳定，因此不适用于现实系统中的长期预测。

由于基于无监督的深度学习算法在处理大量复杂数据时的有效性仍有待提升，以及现阶段时序数据标签的人工标注需要消耗大量人力成本，因此基于自训练的半监督深度学习时序异常分析算法研究成为时序数据异常检测的一种有效的检测方法[13-14]。自编码器(Autoencoder，AE)是一种优秀的表示学习方法[15]，可以有效解决生成数据分布模糊的问题。该类模型主要根据重构误差找到异常数据，近年来被证明在异常检测方面具有良好的性能[16]。Malhotra 等[17]采用长短期记忆自编码器(LSTM-autoencoder，LSTM-AE)生成时序数据，但该方法在高维、样本多样的数据集上建模难度较大，使得仅利用重构误差进行的异常评定效果较差。

GAN 最早由 Goodfellow 等[18]提出，因其在图像领域的异常检测具有一定的有效性，也逐渐成为时序数据异常检测的新方法之一。Esteban 等[19]构造了一种递归 GAN(Recurrent Generative Adversarial Networks，RGAN)，用于医学领域的时序数据生成。RGAN 成功生成了有用的时序数据，证明了对抗模式可以学习真实数据多模态分布的可能性。Li 等[20]提出 MAD-GAN(Multivariate Anomaly Detection-GAN)，并指明针对多元时序无须处理每个数据流，要从总体上考虑变量集捕获信息的方法论，试图利用滑动窗口捕获时序数据在时间和空间上的联合分布。然而，MAD-GAN 损失函数的设计导致其训练困难，使得在大多数情况下生成样本的多样性不足，且传统的基于二分类交叉熵损失的对抗网络可能会因生成器梯度消失而使得模型难以训练，必须谨慎调整生成器和判别器的训练参数。Geiger 等[21]针对标准对抗损失的原始公式存在梯度不稳定和模式崩溃的问题，采用带有梯度惩罚的损失以及一种周期一致的 GAN 结构，其针对一些数据集展现了有效的生成-判别模式，且模型训练相对来说更加容易，然而该模型没有很好地生成时序数据的多模态分布，不能有效表示高维信息的分布，因此模型没有很好的鲁棒性以及泛化能力。针对多元时序数据异常检测问题，对抗学习的方式已被证明在生成时间序列分布上比较成功[22]，如 Bashar 等[23]提出的 TAnoGAN(Time Series Anomaly Detection-GAN)。

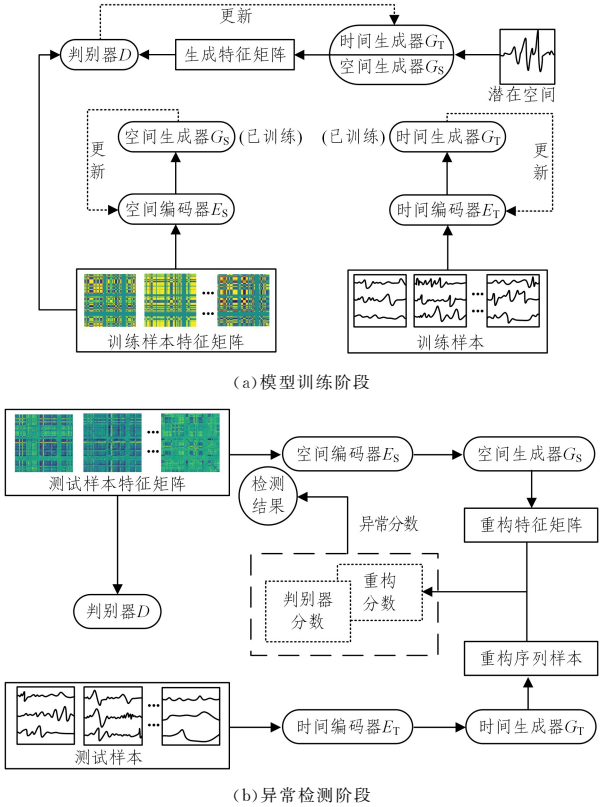
针对以上研究方法的不足，且为了拟合时序关系以及变量之间依赖性，同时为了解决传统 GAN 模型难以训练的问题，本文提出了多模态生成对抗网络多元时序数据异常检测模型。实验证明，本文模型可较好地解决这些问题。

因为系统中异常数据占比远远小于正常数据，在训练集没有标签的情况下，本文假设训练数据整体呈现正常数据分布，以此为前提，本文方法利用滑动窗口分割时间序列并构造特征矩阵来捕获数据的多模态特征，将其与原始数据共同作为模型的输入，基于多层 CNN(Convolutional Neural Networks)及 RNN(Recurrent Neural Network)构建多模态生成器及多模态编码器，并通过时序数据生成 2 个输出——单通道具有空间模态信息的特征矩阵 $\tilde{\boldsymbol{M}}_S$ 及单通道具有时间模态信息的特征矩阵 $\tilde{\boldsymbol{M}}_T$；再将 2 个模态特征矩阵进行有机结合，得到具有时空信息的多模态特征矩阵 $\tilde{\boldsymbol{M}}$；之后将真实数据分布根据不同特征间的关系编码构造一个特征矩阵 $\boldsymbol{M}$，将 $\tilde{\boldsymbol{M}}$ 及 $\boldsymbol{M}$ 作为判别器 D 的输入。训练判别器时通过限制判别器参数的改进梯度惩罚的方法并使用拟合真实分布与生成分布之间的 Wasserstein 距离的方式，来取代之前 GAN 异常检测

算法经常使用的判别器二分类交叉熵损失。最后模型结合重构分数及异常评分实现异常检测。滑动窗口及特征矩阵的具体构造方式将在 3.2 节中介绍。

3 多模态生成对抗网络框架

时间序列异常检测的基本任务是识别数据分布中的非一致点[24]。本文的多模态生成对抗网络多元时序数据异常检测模型框架如图 1 所示。



(a)模型训练阶段

(b)异常检测阶段

图 1 多模态生成对抗网络

Fig. 1 Multimodal generative adversarial networks

如图 1 所示，本文模型由多模态编码器 E、多模态生成器 G 和判别器 D 3 个模块组成。多模态生成器由时间模式生成器 G_T 和空间模式生成器 G_S 组成，在潜在空间中通过联合两者生成得到特征矩阵 $\widetilde{\boldsymbol{M}}$，并利用判别器 D 对真实分布形成的特征矩阵 $\boldsymbol{M}$ 和生成特征矩阵 $\widetilde{\boldsymbol{M}}$ 进行判别。与标准 GAN 框架一样，D 和 G 的参数根据 D 的输出进行更新，使其为真实序列和虚假序列分配正确的标签，训练生成器使其尽可能“欺骗”判别器(即误导 D 为虚假序列分配真实标签)。通过生成真实的样本，生成器 G 将捕获训练序列的隐藏多元分布，而且经过训练，判别器 D 也能以高灵敏度区分假数据(即异常数据)和真实数据(即正常数据)。

与许多将时序数据进行序列化处理的 GAN 模型[19-21,23]的做法不同，本文模型不是独立处理单个数据点，而是考虑局部数据集来捕获序列多模态，具体做法是将多元时间序列按滑动时间窗口的方式进行序列预划分。如图 1(b)所示，经过有效训练之后，在异常检测阶段，模型通过编码器 E 和生成器 G 重构原始序列，以原始序列及其特征矩阵和重构序列及其特征矩阵的残差为重构分数，再将多元时间序列按滑动时间窗口的方式进行序列预划分，将每个时间窗口映射到特征矩阵，构成检测矩阵序列 $\boldsymbol{P}=(\boldsymbol{M}_1,\boldsymbol{M}_2,\cdots,\boldsymbol{M}_n)$，使检测矩阵序列 $\boldsymbol{P}$ 通过训练好的判别器 D 得到判别评分，最后由融合重构误差和判别评分得到序列的异常评分，最终设定异常范围阈值，得到检测结果。

3.1 问题定义

多元时间序列 $\boldsymbol{T}$ 代表由连续 N 个时间戳的各种不同变量在某一时刻联合形成的序列向量集合 $\boldsymbol{T}=\{\boldsymbol{t}_1,\boldsymbol{t}_2,\boldsymbol{t}_3,\cdots,\boldsymbol{t}_N\}$，其中 $\boldsymbol{t}_i(i=1,2,3,\cdots,N)$ 表示第 i 个时间戳的序列向量。$\boldsymbol{T}$ 用矩阵的形式表示为：

$$\begin{matrix}\boldsymbol{t}_1\\ \vdots\\ \boldsymbol{t}_N\end{matrix}\begin{bmatrix}x_{11} & \cdots & x_{1H}\\ \vdots & \ddots & \vdots\\ x_{N1} & \cdots & x_{NH}\end{bmatrix} \tag{1}$$

其中，横向的每个向量 $\boldsymbol{t}_i=(x_{i1},x_{i2},\cdots,x_{iH})$ 为第 i 个时间戳的 H 个变量的信息，H 为特征数。令纵向的每个向量 $\boldsymbol{s}_j=(x_{1j},x_{2j},\cdots,x_{Nj})$ 表示第 j 个特征的时间序列向量，其中 $j=1,2,\cdots,H$。$\boldsymbol{t}_i$ 之间具有时间关联性，$\boldsymbol{s}_j$ 之间具有特征之间的相联信息，本文称之为空间关联性。对于 $\boldsymbol{T}=\{\boldsymbol{t}_1,\boldsymbol{t}_2,\boldsymbol{t}_3,\cdots,\boldsymbol{t}_N\}$，确定滑动窗口的大小为 W，步长为 S，从而得到多元时间序列的 n 个子序列，即 $\boldsymbol{T}=\{\boldsymbol{x}_{wi},i=1,2,\cdots,n\}$，其中 n 为窗口个数。通过滑动窗口生成固定长度的输入。多元时间序列异常检测的任务是对 $\boldsymbol{T}$ 产生一个输出向量 $\boldsymbol{l}=\{Lable^1_{\text{pre}},Lable^2_{\text{pre}},\cdots,Lable^n_{\text{pre}}\}$，其中 $Lable^i_{\text{pre}}\in\{0,1\}$ 表示第 i 个时间窗口是否为异常。滑动窗口具体方法将在 3.2 节介绍，异常检测具体方法将在 3.4 节介绍。

3.2 时间序列多模态学习建模

现有研究指出不同时间序列之间的相关性是表征系统状态的关键[25-26]，多模态时空间存在 $\boldsymbol{s}_j$ 之间的关联信息，这些信息是多元系统中不可忽略的一部分。为此，本文采用一种滑动时间窗口及特征矩阵的方式，以便充分表征时空模态。

对于多元时间序列向量集 $\{\boldsymbol{t}_1,\boldsymbol{t}_2,\boldsymbol{t}_3,\cdots,\boldsymbol{t}_N\}$，每一刻的序列向量 $\boldsymbol{t}_i$ 都对应一个区分正常和异常的标签 l_i，且确定滑动窗口的大小为 W，步长为 S，从而得到多元时间序列的 n 个子序列 $\boldsymbol{T}=\{\boldsymbol{x}_{wi},i=1,2,\cdots,n\}$，$n$ 为窗口的个数。由以上的定义可得：$n=\left\lceil\dfrac{N-W}{S}\right\rceil+1$。对于每个窗口子序列 $\boldsymbol{x}_{wi}$ 来说都有 H 个变量特征，本文定义在 $\boldsymbol{x}_{wi}$ 窗口中的第 η 个特征的时间序列为 $\boldsymbol{x}^{\eta}_{wi}$，则 $\boldsymbol{x}_{wi}$ 可以被看成是由 H 个时间序列向量构成，即 $\boldsymbol{x}_{wi}=\{\boldsymbol{x}^1_{wi},\boldsymbol{x}^2_{wi},\cdots,\boldsymbol{x}^H_{wi}\}$，$\boldsymbol{x}^{\eta}_{wi}(\eta=1,2,\cdots,H)$ 为一个时间序列向量。

本文模型以特征矩阵 $\boldsymbol{M}$ 记录时间序列两两之间的相关性。受文献[26]启发，利用向量之间的余弦相关性可以很好地表示两个向量之间的联系的特性。对于一个时间序列窗口 $\boldsymbol{x}_{wi}$ 以及 $\boldsymbol{M}$ 中的一个值 $m_{\eta\zeta}\in\boldsymbol{M}$，本文中 $\boldsymbol{M}$ 的构造方法如式(2)所示：

$$m_{\eta\zeta}=\cos\langle\boldsymbol{x}^{\eta}_{wi},\boldsymbol{x}^{\zeta}_{wi}\rangle \tag{2}$$

其中，$0<\eta,\zeta<H$，$-1\leqslant m_{\eta\zeta}\leqslant 1$。本文构造矩阵 $\boldsymbol{M}$ 具有以下两个特征：

(1)特征矩阵是多维空间的向量两两作用的结果，而且夹角余弦可以有效地表示两个时间序列向量之间的关系，因此

特征矩阵装载时间序列空间模态上大部分的信息，并且由于窗口 W 的存在，特征矩阵也带有少量的时间模态信息。

(2)特征矩阵中的每一个元素的取值范围均在−1～1之间，越接近−1代表向量之间越呈负相关，越接近1代表向量之间越呈正相关，这种性质使得特征矩阵方便参与计算，无须再进行进一步的数据预处理。

在训练模型阶段模拟生成潜在空间 $\boldsymbol{Z}$ 中的数据 $\boldsymbol{z}$，$\boldsymbol{z}$ 服从高斯分布，即 $\boldsymbol{z}\sim N(0,1)$ 可以保证潜在空间的随机性及标准性，故可将多元时间序列 $\boldsymbol{T}$ 和 $\boldsymbol{Z}$ 放入模型中进行训练。

训练时通过时间序列窗口的方式输入数据，将 $\boldsymbol{Z}$ 输入多模态生成器 G 中，G 由时间模式生成器 G_{T} 及空间模式生成器 G_{S} 组成。G_{T} 旨在从潜在空间中生成原始的时间序列 $\tilde{\boldsymbol{x}}_{wi}$，通过对生成的 $\tilde{\boldsymbol{x}}_{wi}$ 进行特征矩阵操作得到具有时间模态信息的特征矩阵 $\widetilde{\boldsymbol{M}}_{\mathrm{T}}$。$G_{\mathrm{S}}$ 则直接从潜在空间中生成特征矩阵 $\widetilde{\boldsymbol{M}}_{\mathrm{S}}$ 以拟合真实数据分布的空间模态，即变量之间的相联性，并且确定一个时空融合参数 α 以融合时间特征矩阵 $\widetilde{\boldsymbol{M}}_{\mathrm{T}}$ 和空间特征矩阵 $\widetilde{\boldsymbol{M}}_{\mathrm{S}}$，得到具有多模态时空信息的特征矩阵 $\widetilde{\boldsymbol{M}}$，并且有：

$$\widetilde{\boldsymbol{M}}=\alpha\widetilde{\boldsymbol{M}}_{\mathrm{S}}+(1-\alpha)\widetilde{\boldsymbol{M}}_{\mathrm{T}} \tag{3}$$

其中，$0\leqslant\alpha\leqslant1$，当时序数据的特征变量间联系较紧密时，$\alpha$ 应更接近1，反之，则更接近0。得到 $\widetilde{\boldsymbol{M}}$ 之后，将 $\widetilde{\boldsymbol{M}}$ 和真实序列对应的特征矩阵 $\boldsymbol{M}$ 输入判别器中进行生成器 G 和判别器 D 的对抗训练。因特征矩阵的计算包括了特征间的信息以及时序信息，所以 $\boldsymbol{M}$ 中包含了真实数据多模态时空信息，这对应了生成器 G 的两个模态叠加形式。

3.3 梯度惩罚网络训练

大多数用于时序数据异常检测的 GAN 模型训练判别器 D 采用的都是传统的 GAN 损失。传统的 GAN 判别器采用最大化式(4)的损失函数来尽量将真实样本分为正例以及将生成样本分为负例。

$$L=E_{x\sim P_r}[\log D(x)]+E_{x\sim P_g}[\log(1-D(x))] \tag{4}$$

其中，P_r 代表真实样本分布，P_g 代表生成样本分布。Arjovsky 等[27]已经证明，当判别器近似最优时，训练生成器需要最小化的式(4)可以改写为式(5)：

$$L=2JS(P_r\parallel P_g)-2\log 2 \tag{5}$$

其中，$JS()$ 代表求两个分布的 Jensen-Shannon 散度(Jensen-Shannon Divergence)。当 P_r 与 P_g 的支撑集(Support)是高维空间中的低维流形(Manifold)时，P_r 与 P_g 重叠部分测度(Measure)为0的概率为1，且因 P_r 和 P_g 没有重叠或者重叠部分可忽略时，式(5)则为某一固定常数，从而导致该损失函数形式可能带来生成器梯度消失的问题[27-28]。并且这种损失函数形式也会造成生成器模式崩坏的问题，具体表现为：当判别器被训练得非常好时，生成器表现出宁可生成一些重复的样本来保证评分，也不会生成多样性的样本。

可以采用一种 WGAN(Wasserstein-GAN)[28-30]的方法，用近似真实分布与生成分布之间的 Wasserstein 距离来训练生成器和判别器，如式(6)所示，以此避免不易训练的问题。

$$\min(G)\max(D)V(G,D)=E_{x\sim P_X}[D(x)]-E_{z\sim P_z}[D(G(z))] \tag{6}$$

本文判别器损失函数采用文献[29]的方式，类似于WGAN-GP(WGAN-gradient penalty)[30]的方法，而且为了满足判别器网络参数的利普希兹(Lipschitz)连续[28]，利用了更加平滑的判别器损失函数，如式(7)所示：

$$L_D=-E_{x\sim P_X}[D(x)]+E_{z\sim P_z}[D(G(z))]+\lambda_{gp}E_{x\sim\hat{X}}[\max(0,\parallel\nabla_xD(x)\parallel_p-1)]^2 \tag{7}$$

其中，X 代表真实数据分布，$\hat{X}$ 是真实数据及生成数据的一次插值分布，λ_{gp} 代表梯度惩罚的系数，实验部分采用 $p=2$ 代表2范数。Geiger 等[21]在利用 GAN 做时序数据异常检测时的模型训练采用 $E_{x\sim\hat{X}}[\parallel\nabla_xD(x)\parallel_p-1]^2$ 来做梯度惩罚项以满足 Lipschitz 连续。本文则采用文献[29]的方式，因为 $E_{x\sim\hat{X}}[\max(0,\parallel\nabla_xD(x)\parallel_p-1)]^2$ 项可以让判别网络参数的变化更加平滑且 $\parallel\nabla_xD(x)\parallel_p$ 项不是单调地靠近1，而是选择比1大的部分做出惩罚[29]。相应地，生成器的损失函数如式(8)所示：

$$L_G=-E_{z\sim P_z}[D(G(z))] \tag{8}$$

使用这种方式可有效解决生成器梯度消失的问题[29]，使得模型比之前的对抗模型更加容易训练且 Wasserstein 距离更小，对抗模型训练得越好。理论上，经过足够多次的生成器与判别器博弈训练，先固定生成器 G 再训练多模态编码器 E，多模态编码器能够有效提取真实分布多模态信息并将其映射到低维潜在空间中，多模态生成器能够提取潜在空间到真实分布的映射关系。因此可利用编码器及生成器重构真实样本，理想情况下，异常样本无法进行有效重构，并且因判别器可抓捕到多模态特征，利用真实样本构造特征矩阵并由判别器评分，同样地，异常样本无法得到和正常样本同样分布的评分，因此该模型基于联合判别评分和重构误差来鉴别异常，详细方法将在3.4节中说明。

实际上，数据的绝对情况难以获取，且异常数据点也较少，因此本文假设训练集的数据都是正常的。定义 GAN 的生成器 G 由时间模式生成器 G_{T} 和空间模式生成器 G_{S} 构成。G_{T} 由长短期递归神经网络(LSTM-Recurrent Neural Network，LSTM-RNN)组成，G_{S} 及判别器 D 均由卷积神经网络(Convolutional Neural Ntworks，CNN)组成。经过有限轮次的迭代后，为了在异常检测时可以重构真实分布，我们将训练好的生成器 G 单独提取出来以训练多模态编码器 E，目标是让 E 将真实时间序列分布完美地映射到低维的潜在空间。编码器 E 分为时间编码器 E_{T} 和空间编码器 E_{S}。E_{T} 由 LSTM-RNN 构成，E_{S} 则由 CNN 构成，这是因为基于 RNN 的网络擅长捕获时序数据的时间依赖，基于 CNN 的网络擅长捕获特征之间的关系。理论上，成功的编码器 E 可以提取多模态时空序列的各种有效信息，并将其压缩至低维空间。

训练编码器 E 时将训练好的生成器 G 参数固定，将原始时间序列 $\boldsymbol{x}_{wi}(i=1,2,\cdots)$ 依次放入编码器网络，得到的低维数据再由生成器 G 还原得到 $\hat{\boldsymbol{x}}_{wi}$，由两者的 L2 范数差异构成损失进行编码器网络参数迭代。因此，为了能够训练好编码器，本文模型中编码器 E 的损失函数如式(9)所示：

$$L_E=E_{x\sim P_X}\parallel x,\hat{x}\parallel_2 \tag{9}$$

其中，E 可以为 E_{T} 或 E_{S}，训练 E_{T} 时以 G_{T} 来重构数据；训练 E_{S} 时则以 G_{S} 来重构数据的特征矩阵。在训练好编码器 E 之后，

便可用训练好的整个网络以一个联合判别器判别及生成器编码器重构的方式获取联合的异常分数，用于检测数据中的异常。

3.4 时序数据异常检测

在模型检测阶段，也将测试集进行滑动时间窗口划分成多个子序列，再将这些时间序列窗口分成两种模态：一种是原始时序数据，即主要为时间模态；另一种是将序列窗口变换成特征矩阵，即主要为空间模态。通过重构原始时序数据得到重构分数 Rec_Score1，通过重构特征矩阵得到重构分数 Rec_Score2，将两者有机结合得到 Rec_Score，如式(10)所示：

$$Rec\_Score=\theta Rec\_Score1+(1-\theta)Rec\_Score2 \tag{10}$$

其中，$\theta\in[0,1]$。

将特征矩阵输入到训练好的判别器中得到判别分数 Dis_Score，并组合两种分数得到最后用于检测异常的异常分数 Ano_Score。定义对序列进行的预测标记为 $Lable_{pre}$。对于异常分数 Ano_Score，以式(11)或式(12)的方式对序列进行标记，它们的情况正好相反，具体的选择需要根据实际情况确定，其中 1 代表预测为异常，0 则代表预测为正常，τ_1 和 τ_2 分别代表预定义阈值，用于划分异常和正常数据的界限。

$$Lable_{pre}=\begin{cases}1, & \tau_1<Ano\_Score<\tau_2\\ 0, & \text{othercase}\end{cases} \tag{11}$$

$$Lable_{pre}=\begin{cases}0, & \tau_1<Ano\_Score<\tau_2\\ 1, & \text{othercase}\end{cases} \tag{12}$$

本文基于多模态生成对抗网络的多元时序数据异常检测包括重构阶段和判别阶段。

(1) 判别阶段：将原始时序数据序列窗口 $\boldsymbol{X}_{test}$ 进行特征矩阵的变换，得到原始特征矩阵 $\boldsymbol{M}_{test}$，最后的判别分数 Ano_Score 为 $D(\boldsymbol{M}_{test})$。

(2)重构阶段：将原始数据序列窗口 $\boldsymbol{X}_{test}$ 和原始特征矩阵 $\boldsymbol{M}_{test}$ 分别输入到训练好的编码器 E_T 和 E_S 中并映射到潜在空间，得到低维的 $E_T(\boldsymbol{X}_{test})$ 和 $E_S(\boldsymbol{M}_{test})$，再通过训练好的生成器 G_T 和 G_S 还原得到 $\hat{\boldsymbol{X}}_{test}$ 和 $\hat{\boldsymbol{M}}_{test}$，以此可以得到重构分数 Rec_Score：

$$Rec\_Score=\theta MSE(\boldsymbol{X}_{test},\hat{\boldsymbol{X}}_{test})+(1-\theta)MSE(\boldsymbol{M}_{test},\hat{\boldsymbol{M}}_{test}) \tag{13}$$

融合两种分数得到最终的异常分数的计算式，如式(14)所示：

$$Ano\_Score=\lambda Dis\_Score+(1-\lambda)Rec\_Score \tag{14}$$

式(13)中，MSE 代表均方误差(Mean Square Error，MSE)。式(14)中，λ 的取值范围为 $0<\lambda<1$，由此得到联合判别和重构的异常分数。

本文的多模态生成对抗网络多元时序数据异常检测算法如算法 1 所示，其中 n 和 m 分别代表训练集和测试集的样本数；n_d 代表每一个轮次(epoch)训练判别器的次数，本文默认为 5。函数 $M()$ 代表对时间序列窗口进行特征矩阵变换；α 和 θ 都是一个具体的值，取值范围为 $[0,1]$；β 不是一个具体值，而是一系列与输入窗口维度一样的随机数，β 中每一个值都是独立且随机的，取值范围均为 $[0,1]$；b 为 batch_size 的大小，本文设置默认为 64。

算法 1 多模态 GAN 多元时序数据异常检测

Input：原始数据 $\mathbf{X}$ 和 $\mathbf{X}_{test}$，潜在空间数据 $\mathbf{Z}$

Output：异常评分 Ano_Score

Train：

1. for each epoch do
2. for d=0,1…,n_d do
3. 从真实数据 $\mathbf{X}$ 中提取训练数据滑动窗口 $\{\mathbf{x}_{wi},i=1,2,\cdots,n\}$
4. 从潜在空间 $\mathbf{Z}$ 中提取一维向量 $\{\mathbf{z}_i,i=1,2,\cdots,n\}$，其中 $z_i\sim N(0,1)$
5. $G(\mathbf{z}_i)=\alpha\cdot G_S(\mathbf{z}_i)+(1-\alpha)\cdot M(G_T(\mathbf{z}_i))$
6. $\varphi_i=\beta\cdot M(\mathbf{x}_{wi})+(1-\beta)\cdot G(\mathbf{z}_i)$
7. 通过最小化 L_D 更新判别器 D：
8. $L_D=-D(M(\mathbf{x}_{wi}))+D(G(\mathbf{z}_i))+\lambda_{gp}\cdot \max\{0,\|\nabla_{\varphi_i}D(\varphi_i)\|-1\}^2$
9. end
10. 通过最小化 L_{G_T} 更新时间模态生成器(G_T)：
11. $L_{G_T}=-\frac{1}{b}\sum_{i=1}^{b}D(M(G_T(\mathbf{z}_i)))$
12. 通过最小化 L_{G_S} 更新空间模态生成器(G_S)：
13. $L_{G_S}=-\frac{1}{b}\sum_{i=1}^{b}D(G_S(\mathbf{z}_i))$
14. end
15. 保存 G_S，G_T 以及 D 的参数
16. for each epoch_encoder do
17. 从真实数据中提取训练数据滑动窗口 $\{\mathbf{x}_{wi},i=1,2,\cdots,n\}$
18. 通过最小化 L_E 分别更新时间模态编码器及空间模态编码器：
19. $L_E=MSE(G_T(E_T(\mathbf{x}_{wi})),\mathbf{x}_{wi})$
20. $L_E=MSE(G_S(E_S(M(\mathbf{x}_{wi}))),M(\mathbf{x}_{wi}))$
21. end
22. 保存 E_T 及 E_S 的参数

Test：

23. $\mathbf{X}_{test}=\{\mathbf{x}_{wi}^{test},i=1,2,\cdots,m\}$
24. for i=1,2,…,m do
25. $\hat{\mathbf{x}}_i=G_T(E(\mathbf{x}_{wi}^{test}))$
26. $\hat{\mathbf{m}}_i=G_S(E(M(\mathbf{x}_{wi}^{test})))$
27. $Rec\_Score=\theta MSE(\mathbf{x}_{wi}^{test},\hat{\mathbf{x}}_i)+(1-\theta)MSE(M(\mathbf{x}_{wi}^{test}),\hat{\mathbf{m}}_i)$
28. $Dis\_Score=D(M(\mathbf{x}_{wi}^{test}))$
29. $Ano\_Score=\lambda Dis\_Score+(1-\lambda)Rec\_Score$
30. end

在算法 1 中，第 1－22 行是模型的训练阶段，具体地，第 1－14 行是时间模态生成器、空间模态生成器与判别器的训练，一直重复这两个循环直到逐渐收敛逼近纳什均衡；第 16－21 行是时间模态编码器及空间模态编码器的训练，采用已训练的两个生成器辅助进行重构，通过最小化编码器损失函数更新两个编码器参数直到收敛。第 23－30 行是根据训练好的模型计算异常评分。

综上所述，多模态生成对抗网络多元时序数据异常检测方法从多元时序数据多个模态信息出发，采用基于重构及判别的混合策略，对异常的评估取决于生成样本与原始样本的距离以及判别生成样本为正常样本的可能性，具体实现在于生成器从多模态时空学习特征分布的能力，判别器从样本的高维分布上进行鉴别。

4 实验设置和结果

为了对所提模型的可行性进行验证，将其与其他半监督时序数据异常检测方法在精确率、召回率和 F1-分数这 3 个评价指标上进行对比，实验基于 Windows 10 环境，使用 Python3.8.5 下 Pytorch 框架进行模型搭建。平台主要硬件参数为 CPU Intel Core i7-9750HF，内存 16GB，GPU NVIDIA GeForce GTX 1660 Ti，6GB 显存。

本文的模型评估采用运行监控情况的水分布数据集(Water Distribution，WADI)[31]以及安全水处理模型(Secure Water Treatment，SWaT)数据集[32]。

本文实验采用的两种数据集的统计信息如表 1 所列，其中异常率(Anomaly)指测试集中数据集的异常占比。

表 1 数据集的统计信息

Table 1 Statistical information of datasets

Dataset	Features	Train	Test	Anomaly/%
SWaT	51	99360	89984	11.99
WADI	123	241921	15701	7.09

4.1 实验设置

在整个实验的训练测试阶段，都是在时间序列起始处取滑动时间窗口，实验所采用的窗口大小 $W=100$，滑动步长为 50，因此在序列的最后可能会无法获得完整的长度为 100 的时间窗口，默认将此部分窗口剔除。因为舍去此部分时序数据相比整个时间序列的时间跨度是微乎其微的，所以是完全可以接受的。

实际应用中，异常往往会持续一段时间形成连续的异常段，因此，对于适当大小异常段内的任何观测，模型检测到异常警报是可以接受的。这种观点亦在文献[33]中被提出，并且被广泛应用于异常检测任务的评估。因此时间序列窗口的标签可以表示为只要有异常则为异常，反之则代表该窗口是正常的。

在神经网络的训练上，选择单向 LSTM 及多个卷积网络层的 CNN 分别作为时间模态编码器 E_T 和空间模态编码器 E_S，时间模态生成器 G_T 亦使用了单向 LSTM 网络，空间模态生成器 G_S 则使用了多层反卷积的 CNN。对于判别器，采用多层卷积层的 CNN。根据经验，训练的策略采用每训练 1 次生成器，即训练 5 次判别器，依此方式对正常数据集进行 100 次迭代。对于编码器，固定训练好的生成器 G 以训练编码器 E，在正常数据上迭代 200 次。所有神经网络的训练中设定 batch_size 大小为 64，网络参数优化器选择 Adam，优化器的起始学习率为 0.00001，优化器的衰减速率参数为(0，0.9)，优化器其他参数采用默认值。

在评价指标上，采用最常用的精确率、召回率及 F1-分数。精确率指标签为正类占所有预测为正类的比例；召回率指正确预测为正类占数据标签为正类的比例；F1-分数则为精确率和召回率的调和平均数。数据的真实标签以及预测的标签一共有 4 种类别：TP 代表数据标签为正类预测标签也为正类；TN 代表数据标签为负类预测标签也为负类；FP 代表数据标签为负类预测标签为正类；FN 代表数据标签为正类预测标签为负类。精确率、召回率和 F1-分数和计算式分别如式(15)－式(17)所示：

$$Precision=\frac{TP}{TP+FP} \tag{15}$$

$$Recall=\frac{TP}{TP+FN} \tag{16}$$

$$F1\text{-}Score=2\cdot\frac{Precision\cdot Recall}{Precision+Recall} \tag{17}$$

为了减少假阳性率(FP)、提高模型的精确率，本文在异常检测的预测标签后还采用一种单异常裁剪的策略。在真实系统中，异常往往在连续的时间段出现[33]，因此在预测标签连续的情况下，当预测标签的前一个标签和后一个标签都是正常时，预测的标签为异常很有可能是假异常(FP)，因此采取单异常裁剪策略，即出现单个时间窗的异常时，将其预测变更为正常标签。此做法可以降低假阳性率。

在数据预处理方面，采用 z-score 标准化，即对于每一个特征所对应的一元时间序列，对每个数据进行处理，如式(18)所示：

$$data_i=\frac{data_i-mean(data)}{std(data)+\delta} \tag{18}$$

其中，$data$ 表示一个单独特征的时间序列数据集，δ 代表一个远远小于真实数据的数，这样可以方便真实数据 $data_i$ 的标准化。

4.2 测试结果

将本文模型与多种半监督时间序列异常检测方法进行对比，传统方法中的对比模型有主成分分析法(PCA)和基于距离的 KNN 方法。在基于自编码器的对比方法中，本文将与基于自编码器的 LSTM-AE 方法，以及同样基于对抗网络的 MAD-GAN[20]模型和 Tad-GAN(Time Series Anomaly Detection-GAN)[21]模型进行精确率、召回率及 F1-分数 3 个指标的对比，如表 2 所列。

表 2 不同模型在不同数据集的检测指标

Table 2 Detection metrics of different models on different datasets

Dataset	Methods	*Precision*/%	*Recall*/%	*F1-Score*
WADI	PCA	6.41	41.96	0.11
	KNN	39.23	37.65	0.38
	LSTM-AE	40.91	37.50	0.39
	MAD-GAN	41.44	33.92	0.37
	Tad-GAN	42.11	33.33	0.37
	本文模型	**48.48**	**66.67**	**0.56**
SWaT	PCA	34.58	58.33	0.43
	KNN	26.01	**91.54**	0.41
	LSTM-AE	47.22	70.91	0.57
	MAD-GAN	**98.97**	63.74	**0.77**
	Tad-GAN	91.45	50.55	0.65
	本文模型	96.07	62.18	0.76

表 2 列出了不同模型在 WADI 和 SWaT 数据集上的实验结果。在数据集 WADI 中，本文方法取得了 48.48%的精确率及 66.67%的召回率；在数据集 SWaT 中，本文方法取得了 96.07%的精确率及 62.82%的召回率。本文模型相比各种半监督时序异常检测方法有较大的性能提升，表明多模态 GAN 充分挖掘了多元时序数据的多维特征，有效提高了模型的准确性，且本文方法与同样基于 GAN 框架的 Tad-GAN 相比，在 WADI 和 SWaT 数据集上的 F1-分数分别提升了 0.19 和 0.11，在表征能力不等的其他基线模型中 F1-分数均有

稳定的提升，这说明本文模型具备良好的泛化性能。

针对判别异常检测策略是否具有良好性能的问题，本文还评估了模型在异常检测时的多种策略。采用单独使用判别分数和重构分数的策略作为一个选项，以及是否增加单异常裁剪策略作为另一个选项。实验结果如表 3 所列。

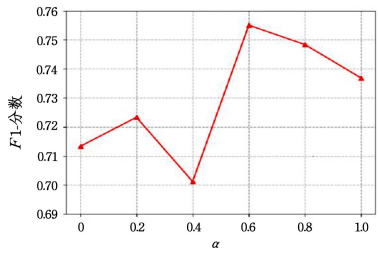
表 3 本文模型在不同策略下不同数据集的 F1-分数

Table 3 F1-score of the proposed model on different datasets under different strategies

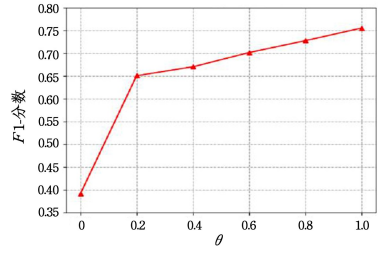
Dataset	Detection strategy	*F1-Score*
WADI	仅用判别分数(无单异常裁剪)	0.30
	仅用判别分数(有单异常裁剪)	0.23
	仅有重构分数(无单异常裁剪)	0.48
	仅有重构分数(有单异常裁剪)	0.52
	联合异常分数(无单异常裁剪)	0.51
	联合异常分数(有单异常裁剪)	0.56
SWaT	仅用判别分数(无单异常裁剪)	0.34
	仅用判别分数(有单异常裁剪)	0.37
	仅有重构分数(无单异常裁剪)	0.69
	仅有重构分数(有单异常裁剪)	0.69
	联合异常分数(无单异常裁剪)	0.74
	联合异常分数(有单异常裁剪)	0.76

表 3 实验结果表明，总体上联合异常分数的检测稳定性及鲁棒性更好，而且在这些现实系统的数据中采用单异常裁剪策略是一种有效的方法，这验证了本文的假设一定程度上的正确性。实验结果表明，现实系统中异常往往是以一段不可忽略的连续时间的形式出现，模型检测到一个窗口的异常时，很有可能是预测标签 FP(假阳性)，将这种单一出现的异常重新标以正常标签，可以很好地降低假阳性率，以此提高模型在现实系统中的精确率及 F1-分数。

为了探究多模态生成对抗网络多元时序数据异常检测模型中重要参数 α 及 θ 的影响，针对所提模型在 SWaT 数据集上进行了超参数敏感分析实验。实验结果如图 2 所示，可以看出 2 个参数都对算法性能产生了影响，其中测试 θ 利用的是 α 为 0.6 时已经训练好的模型。



(a)参数 α 的影响



(b)参数 θ 的影响

图 2 超参数对模型性能的影响

Fig. 2 Effect of hyperparameters on model performance

由图 2(a)可知，参数 α 对性能的影响分别在值为 0.2 及 0.6 处产生了极大值，其中 α 取 0.6 时针对 SWaT 数据集的检测效果最好，且 α 在整个取值区间内对 F1-分数的影响总体较小。另外由图 2(b)可知，F1-分数与 θ 成一个正相关的映射关系，在 θ 取值为 1 时，F1-分数最大，这说明针对 SWaT 数据集不宜利用空间相关性进行重构，且 α 为 0.6 的训练方式导致空间模态生成器没有很好地学习，但随着 θ 的增大，其对性能的影响也越来越小。实验结果表明，本文方法对于参数 α 的选择敏感度较低；参数 θ 则需针对具体数据集及具体网络模型进行取值，本文模型针对参数 θ 的选择敏感度较高。本文针对 SWaT 数据集所采用的超参数取值分别为 $\alpha=0.6$，$\theta=1.0$。

此外，模型时间窗口 W 的大小设置是一个值得关注的问题，W 不能太大也不能太小。如果时间窗口过大，在现实系统中检测就会失去实际意义；反之如果窗口过小，则会导致窗口序列的时间相关性很小，失去了很多时间模态信息[34]。因此需要一个恰当的窗口大小，在保证预测精确率和召回率的同时，也能符合实际检测需求。例如在 WADI 数据集中，系统每秒都会采集一次数据，对于这种运转比较快的现实系统，本文的窗口大小设置为 100，但对于其他没有进行实验的数据集，窗口大小的设置应当服从怎样的规则，这是今后工作需要思考的问题。

结束语 本文主要针对现有研究忽略了时空数据的多模态分布问题，提出了一种基于生成对抗网络的多元时序数据的异常检测模型。本文模型充分利用时序数据的多模态分布，在多模态生成器及多模态编码器充分学习时序数据的时空相关性的基础上，利用基于 GAN 的对抗学习方式训练判别器，并在异常检测时利用联合重构分数和判别分数的方法进行异常检测，另外通过一种单异常检测策略提高了模型的精确率。同时针对以往对抗网络不易训练且容易造成模式崩溃的问题，采用一种改进的梯度惩罚方式进行模型训练。模型验证测试结果表明，该模型相较于各种基于自训练的半监督时序数据异常检测方法，在精确率和召回率以及 F1-分数的指标上表现更好，验证了本文模型的有效性。未来将考虑基于多模态编码器-多模态生成器-判别器框架采用其他网络模型的方面展开工作。

参 考 文 献

[1] WANG L, LIN Y, WU Y, et al. Forecast-based Multi-aspect Framework for Multivariate Time-series Anomaly Detection [C]// 2021 IEEE International Conference on Big Data (Big Data). Orlando, 2021: 938-947.

[2] CHANDOLA V, BANERJEE A, KUMAR V. Anomaly detection: A survey [J]. ACM Computing Surveys (CSUR), 2009, 41(3): 1-58.

[3] BREUNIG M M, KRIEGEL H P, NG R T, et al. LOF: identifying density-based local outliers [C]// Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data. DallasS, 2000: 93-104.

[4] LI C N, FENG G W, LIU R Y, et al. Traffic Trajectory Anomaly Detection Method Based on Reconstruction Error [J]. Computer Science, 2022, 49(2): 149-155.

[5] JARQUE C M, BERA A K. Efficient tests for normality, ho-

moscedasticity and serial independence of regression residuals [J]. Economics Letters, 1980, 6(3): 255-259.
[6] LI J, PEDRYCZ W, JAMAL I. Multivariate time series anomaly detection: A framework of Hidden Markov Models[J]. Applied Soft Computing, 2017, 60: 229-240.
[7] BURNAEV E, ISHIMTSEV V. Conformalized density-and distance-based anomaly detection in time-series data[J]. arXiv: 1608.04585, 2016.
[8] KARAAHMETOGLU O, ILHAN F, BALABAN I, et al. Unsupervised Online Anomaly Detection On Irregularly Sampled Or Missing Valued Time-Series Data Using LSTM Networks[J]. arXiv: 2005.12005, 2020.
[9] LIM B, ARIK S O, LOEFF N, et al. Temporal fusion transformers for interpretable multi-horizon time series forecasting[J]. arXiv: 1912.09363, 2019.
[10] ANGIULLI F, PIZZUTI C. Fast outlier detection in high dimensional spaces[C]// European Conference on Principles of Data Mining and Knowledge Discovery. Berlin, 2002: 15-27.
[11] RINGBERG H, SOULE A, REXFORD J, et al. Sensitivity of PCA for traffic anomaly detection[C]// Proceedings of the 2007 ACM SIGMETRICS International Conference on Measurement and Modeling of computer Systems. San Diego, 2007: 109-120.
[12] WILINSKI A. Time series modeling and forecasting based on a Markov chain with changing transition matrices[J]. Expert Systems with Applications, 2019, 133: 163-172.
[13] CHEN H, LIU H, CHU X, et al. Anomaly detection and critical SCADA parameters identification for wind turbines based on LSTM-AE neural network[J]. Renewable Energy, 2021, 172: 829-840.
[14] ZHAO H, WANG Y, DUAN J, et al. Multivariate time-series anomaly detection via graph attention network[C]// 2020 IEEE International Conference on Data Mining (ICDM). Sorrento, 2020: 841-850.
[15] AN J, CHO S. Variational autoencoder based anomaly detection using reconstruction probability[J]. Special Lecture on IE, 2015, 2(1): 1-18.
[16] LI L, YAN J, WANG H, et al. Anomaly detection of time series with smoothness-inducing sequential variational auto-encoder [J]. IEEE Transactionson Neural Networks and Learning Systems, 2020, 32(3): 1177-1191.
[17] MALHOTRA P, TV V, RAMAKRISHNAN A, et al. Multi-sensor prognostics using an unsupervised health index based on LSTM encoder-decoder[J]. arXiv: 1608.06154, 2016.
[18] GOODFELLOW I J, POUGET A J, MIRZA M, et al. Generative Adversarial Networks[J]. Advances in Neural Information Processing Systems, 2014, 3: 2672-2680.
[19] ESTEBAN C, HYLAND S L, RÄTSCH G. Real-valued (medical) time series generation with recurrent conditional gans[J]. arXiv: 1706.02633, 2017.
[20] LI D, CHEN D, JIN B, et al. MAD-GAN: Multivariate anomaly detection for time series data with generative adversarial networks[C]// International Conference on Artificial Neural Networks. Cham, 2019: 703-716.
[21] GEIGER A, LIU D, ALNEGHEIMISH S, et al. TadGAN: Time series anomaly detection using generative adversarial networks [C]// 2020 IEEE International Conference on Big Data (Big Data). Atlanta, 2020: 33-43.
[22] NHO Y H, RYU S, KWON D S. UI-GAN: Generative adversarial network-based anomaly detection using user initial information for wearable devices[J]. IEEE Sensors Journal, 2021, 21(8): 9949-9958.
[23] BASHAR M A, NAYAK R. TAnoGAN: time series anomaly detection with generative adversarial networks[C]// 2020 IEEE Symposium Series on Computational Intelligence (SSCI). Canberra, 2020: 1778-1785.
[24] WANG S, LI C, LIM A. A model for non-stationary time series and its applications in filtering and anomaly detection[J]. IEEE Transactions on Instrumentation and Measurement, 2021, 70: 1-11.
[25] HALLAC D, VARE S, BOYD S, et al. Toeplitz inverse covariance-based clustering of multivariate time series data[C]// Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. Halifax, 2017: 215-223.
[26] ZHANG C, SONG D, CHEN Y, et al. A deep neural network for unsupervised anomaly detection and diagnosis in multivariate time series data[J]. arXiv: 1811.08055, 2018.
[27] ARJOVSKY M, BOTTOU L. Towards principled methods for training generative adversarial networks[J]. arXiv: 1701.04862, 2017.
[28] ARJOVSKY M, CHINTALA S, BOTTOU L. Wasserstein generative adversarial networks[C]// International Conference on Machine Learning. Sydney, 2017: 214-223.
[29] PETZKA H, FISCHER A, LUKOVNICOV D. On the regularization of wasserstein gans[J]. arXiv: 1709.08894, 2017.
[30] GULRAJANI I, AHMED F, ARJOVSKY M, et al. Improved training of wasserstein gans[C]// Advances in Neural Information Processing Systems. Long Beach, 2017: 5767-5777.
[31] 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. Cham, 2016: 88-99.
[32] 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 (CySWater). Vienna, 2016: 31-36.
[33] XU H, CHEN W, ZHAO N, et al. Unsupervised Anomaly Detection via Variational Auto-Encoder for Seasonal KPIs in Web Applications[C]// Proceedings of the 2018 World Wide Web Conference. Lyon, 2018: 187-196.
[34] 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.

ZHANG Renbin, born in 1971, Ph.D, associate professor. His main research interests include industrial Internet security and artificial intelligence.

(责任编辑:杨雪敏)