

基于多模态对抗学习的无监督时间序列异常检测

黄训华 张凤斌 樊好义 席 亮

(哈尔滨理工大学计算机科学与技术学院 哈尔滨 150000)
(1820410060@stu.hrbust.edu.cn)

Multimodal Adversarial Learning Based Unsupervised Time Series Anomaly Detection

Huang Xunhua, Zhang Fengbin, Fan Haoyi, and Xi Liang

(College of Computer Science and Technology, Harbin University of Science and Technology, Harbin 150000)

Abstract Time series anomaly detection is one of the most important research directions in machine learning, which aims to find the patterns that deviate significantly from the normal behavior of time series. However, most of the existing methods for anomaly detection of time series are based on single-modality feature learning, which ignores the relevance and complementarity of the characteristic distribution of time series in multi-modality space, and consequently fails to make full use of the existing information for learning. To alleviate the above problems, in this paper, we present a time series anomaly detection model based on multimodal adversarial learning. Firstly, we convert the original time series into the frequency domain to construct multi-modality time series representation. Then, based on the constructed multi-modality representation, we propose a multimodal generated adversarial network model to learn normal data's distributions in time domain and frequency domain jointly. Finally, by modeling the anomaly detection problem as the data reconstruction problem in time domain and frequency domain, we measure the anomaly score of time series from both the time domain and frequency domain perspectives. We verify the proposed method on the time series data sets of UCR and MIT-BIH. Experimental results on the 6 data sets of UCR and MIT-BIH show that, compared with the state-of-the-arts, the proposed method improves the AUC and AP metrics of anomaly detection performance by 12.50% and 21.59% respectively.

Key words time series; unsupervised anomaly detection; feature distribution; adversarial learning; multimodal

摘 要 时间序列异常检测旨在发现对应时序特征中不符合一般规律的特异性模式,是机器学习领域重要的研究方向之一.然而,现有的时序异常检测方法大多为单模态学习,忽略了时序信息在多模态空间上不同特征分布的关联性和互补性,不能充分利用已有信息进行有效地模式挖掘,从而造成检测效果差等问题.为此,提出了一种基于多模态对抗学习的无监督时间序列异常检测模型.首先,将原始时间序列转换至频域空间,构造多模态时间序列表示.其次,提出多模态生成对抗网络模型,针对多模态时间序列,实现正常时序信息关于时域和频域特征分布的无监督联合学习.最后,通过将异常检测问题转化为

收稿日期:2020-12-21;修回日期:2021-06-09

基金项目:国家自然科学基金项目(61172168)

This work was supported by the National Natural Science Foundation of China (61172168).

通信作者:张凤斌(zhangfb@hrbust.edu.cn)

时间序列在时域和频域空间的重构度量问题,从时域空间和频域空间 2 个方面度量时间序列的异常值,实现更有效的异常检测.在时间序列数据集 UCR 和 MIT-BIH 中的 6 个真实数据集的实验结果表明,在异常检测任务上相较于传统单模态异常检测方法,提出方法在 AUC 和 AP 这 2 个性能指标上最高分别提升了 12.50% 和 21.59%,证明了方法的有效性.

关键词 时间序列;无监督异常检测;特征分布;对抗学习;多模态

中图法分类号 TP391

时间序列(time series)是按照时间排序的一组随机变量,它通常是在相等间隔的时间段内依照给定的采样率对某种潜在过程进行观测的结果.视频、音频、轨迹图、心电图和动作捕捉都是常见的时序数据,对这些数据进行分析检测的关键是识别其中的模式、趋势和相关性^[1].时序数据的分析广泛地应用在科学、工程和商业领域中^[2-3],例如社交媒体^[4]、城市数据^[5]、电子交易^[6]和排名统计^[7]中.在这些领域中时序数据的分析需求主要包括特征提取、相关性分析和异常检测等.

异常检测的目的是找到某些观测值,它与其他观测值有很大的偏差,这样的偏差可能是由于不同的原因或机制所产生的^[8-9].在时序领域,现有的异常检测方法可分为有监督、半监督和无监督 3 类.其中,无监督方法在训练时不需要加注标签,通过密度估计的方式来检测异常.这种检测方式提供了良好的泛化能力,使模型不受限于数据的标签类型,是一种更适用于时间序列的检测方式^[8].而在众多的无监督异常检测方法中,基于生成对抗网络(generative adversarial network, GAN)^[10]的无监督异常检测算法因为优异的分布学习和特征重构能力得到了越来越多的关注.GAN 是一个强大的高维数据建模框架,常用来建模复杂高维的数据分布,它起初作为自然图像^[11-12]的生成模型已经获得了巨大成功,并且越来越多地用于时序信号^[13]和医学成像^[14]的异常检测领域.例如, Zhou 等人^[15]提出了一种基于 GAN 的心电数据异常检测模型,模型通过建模正常心电数据的分布来检测异常,并通过划分固定长度的心跳节拍将数据进行分段检测.这种划分时序周期的方法难以检测无明显周期的数据和长度可变的数据,更难以充分利用时序信息前后依赖的分布关联.为了利用时序依赖关系, Li 等人^[16]提出了一种基于 GAN 的多变量时间序列异常检测模型,此模型可以利用长短时记忆网络(long short-term memory, LSTM)^[17]来捕捉时间依赖关系,再使用 GAN 建模分布来实现异常检测.在此基础上, Geiger 等人^[18]

也提出了一种 GAN 与 LSTM 结合的时序异常检测方法,不同的是,该方法针对时序特征设计了多种重构误差计算和异常评分方法,进一步增强了模型的时序异常检测能力.上述方法都通过使用 GAN 学习特征分布的方式进行了异常检测,但是这些方法只在时序信息的时域特征上进行了分布学习,忽略了时序信息在多模态特征空间的分布关联,造成了对现有信息利用不足的问题.

如图 1 所示,在时序异常检测领域传统异常检测方法多采用原始时间序列直接进行单模态的检测,存在不能充分利用时序信息潜在分布关联的不足.作为对比,为解决传统方法单模态学习的不足,通过利用多模态特征空间的分布关联,本文提出了一个通用的无监督多模态对抗学习时间序列异常检测框架(multimodal GAN, MMGAN),旨在联合学习时间序列在时域空间和频域空间上的特征分布,增强模型分布建模能力.作为一个多模态对抗学习检测模型,MMGAN 能以生成对抗的方式捕捉时间序列在每个模态空间上的特征分布,并建立模态间的分布关联,再通过重构检测异常.具体地,MMGAN 主要有模态转换、多模态生成器和多模态判别器 3 部分组成.首先,模态转换模块负责时序特征从时域到频域的映射.其次,多模态生成器作为一个分布学习模块,由多模态自适应编码器和解码器组成,以 2 个模态信息为输入,通过模态间权重共享和低维

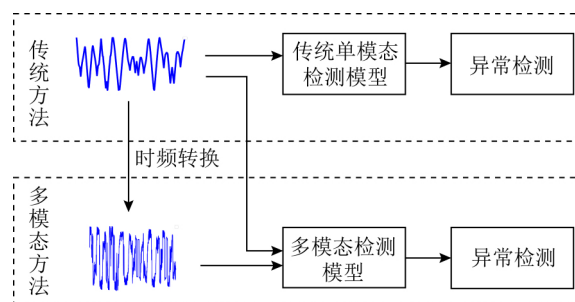


Fig. 1 Comparison of single modal and multimodal detection models

图 1 单模态与多模态检测模型对比

特征融合对时间序列进行多模态的分布关联学习和特征生成.然后,多模态判别器作为一个分布对齐模块,由多模态判别网络组成,以原始多模态信息和多模态生成器的生成特征为输入,通过多模态判别网络的判别进行分布对齐.最后,通过多模态生成器和多模态判别器的博弈对抗,多模态生成器学习到正常样本的特征分布,正常样本可以通过模型进行高质量的重构,而异常样本通过重构则会产生误差,发现异常.

本文贡献如下:

1) 提出了一种通用的多模态时间序列的无监督异常检测框架.通过挖掘正常时序信息在不同模态上的特征分布,实现异常时序信息的有效检测.

2) 提出了一种基于对抗学习的多模态时间序列异常检测方法.该方法提出一个多模态生成对抗网络模型,实现正常时序信息关于时域特征分布和频域特征分布的联合学习,通过将异常检测问题转化为时序信息在时域和频域空间的重构度量问题,从时域空间和频域空间 2 个方面度量时间序列的异常值,实现更有效的异常检测.

在多个真实时序信息数据集上做了充分的实验,结果表明:相比最新的基准方法,本文提出的方法在 AUC 和 AP 这 2 个性能指标上实现了最高分别 12.50% 和 21.59% 的提升.

1 相关工作

1.1 基于 GAN 的无监督异常检测方法

异常检测在众多领域已经得到了非常广泛的研究^[19-21].无监督的异常检测方法由于训练不需要标签而更贴近实际应用场景,是一种更理想的检测方法^[8].具体的无监督检测算法包括基于聚类和基于重构的算法等.

基于聚类的方法通过学习正常数据周围的分类边界来划分异常,如单类支持向量机(one-class SVM, OCSVM)^[22]等.基于重构的方法一般先学习数据的潜在低维表示,再通过重构误差^[19]的方式来确定样本是否异常,例如:主成分分析方法(principal component analysis, PCA)及其一些变体^[23],但这些方法只能进行线性重构.而且,这些算法都是基于离群值不像正态数据集中分布的假设,无法正确检测密度较高的组异常.为表征非线性变换,解决传统重构方法的缺陷,基于深度学习的自动编码器(auto encoder, AE)^[24]、递归自编码器(recurrent neural network

auto-encoder, RNNAE)^[25]、长短时自编码器(long short-term memory auto-encoder, LSTM AE)^[26]和变分自编码器(variational auto-encoder, VAE)^[27]相继出现.但是,如果没有适当的正则化,这些重构方式容易出现过拟合,进而导致检测精度降低.

另一种基于重构的无监督异常检测方法是基于 GAN 的, GAN 可以通过生成器(generator, G)和判别器(discriminator, D)的博弈对抗来学习特征分布,生成高质量的重构特征.例如, Schlegl 等人^[14]提出了一种通过 GAN 建模正常图像分布进行异常检测的方法.这是 GAN 在异常检测方向的开山之作,然而,该方法在测试时需要为每个样例解决一个优化问题,以找到一个潜在的表示,然后使用这个潜在表示来计算异常,这极大增加了该方法的时间复杂度,降低了检测效率.在此基础上, Zenati 等人^[28]提出了一种基于双向 GAN 的异常检测模型.此模型采用多个判别器来稳定 GAN 的训练,提高了检测性能的同时减少了时间复杂度.但是此模型较为复杂的结构擅长处理高维特征,在低维小数据集上处理太过冗余,导致效率低下. Akcay 等人^[29]提出一种使用多个编解码网络的 GAN 进行异常检测的方法,该模型针对图像做了多种约束,在视觉领域得到了广泛认可.但是这种针对性的模型设计也限制了该方法在其他领域的应用.而在时序领域, Zhou 等人^[15]提出一种基于 GAN 的心电异常检测模型,此模型通过重构心电数据进行异常检测,但是该方法仅限于周期性的数据,分段检测方法也难以充分利用时序信息的潜在关联.为了利用时序依赖的同时进行异常检测, Li 等人^[16]提出了一种基于 GAN 的多变量时间序列异常检测模型,通过在 GAN 中嵌入 LSTM 的方式,此模型可以利用特征的时序依赖进行分布学习和特征重构.但是,由于 LSTM 网络无法并行、训练慢和难以处理长序列的特点导致了此模型应用有限.通过以上现状可以看出,基于 GAN 的无监督异常检测算法在不同应用领域都取得了成效,但是在时序领域,面对复杂多变的时序信息,已有的检测方法仅是在时域空间上进行特征学习,不能充分利用时间序列在多个空间上的特征.受此启发,可以设计一种多模态的检测方法,利用多个空间特征分布的联合学习提高模型对时序数据分布的建模能力,执行更高效的异常检测.

1.2 时间序列的时频模态

时间序列可以利用时频联合域分析将自身的时域特征映射到频域空间形成多模态特征.多模态

特征可以为异常检测提供时域与频域的联合分布信息,解决了以往单一的时域或者频域分析的缺陷,为时序检测提供了更多的角度.而现有的检测方法却忽略了这种多模态特征的学习方式.

能进行时序模态转换的时频分析工具有很多,比如,傅里叶变换(Fourier transform, FT)、短时傅里叶变换(short-term Fourier transform, STFT)和小波变换(wavelet transform, WT)等.在异常检测领域, Gothwal 等人^[30]提出了一种利用 FT 对心电信号进行异常检测的方法,该方法首先通过 FT 对心电峰值进行分析,然后利用神经网络对心脏疾病进行检测,但是因为傅里叶变换无法应对非平稳信号的缺陷,该方法对某些非平稳异常类型识别较差. Cocconcelli 等人^[31]提出了一种电机损伤检测方法,该方法利用 STFT 对电机运行进行周期性的特征提取,再进行时频平均以增强故障特征.但是由于短时傅里叶变换的“窗口”尺寸需要手动设定,所以该方法难以高效利用时序特征,也难以应对突发载荷.

WT 继承和发展了 STFT 局部化的思想,通过提供一个随频率改变的“时间-频率窗口”弥补了“窗口”大小不随频率变化的不足,是进行信号时频分析和处理的理想工具. WT 通过变换能够突出问题某些方面的特征,能进行时间(空间)频率的局部化分析,并能通过伸缩平移对信号逐步进行多尺度细化,最终达到高频处时间细分、低频处频率细分、自动适应时频信号分析的要求,从而可聚焦到信号的任意细节,解决了 FT 的缺陷. WT 在应用领域,特别是在图像处理^[32]和信号检测^[33]以及众多非线性科学领域得到了广泛的应用.多模态方法可以利用 WT 的这种多分辨率特性挖掘频域空间上的分布信息,充分利用时序信息的时频关联.

基于以上 2 部分的相关研究现状,在时序异常检测领域,现有的检测方法只能在时间序列的单个特征空间上进行特征学习,忽略了时间序列在多个特征空间上的分布关联.而时频分析方法可以将时域特征映射到频域,为检测提供多个模态空间上的特征.因此,本文提出了一种多模态对抗学习时序异常检测框架,通过小波变换将时间序列映射到频域形成多模态特征,并利用 GAN 出色的分布学习能力来捕捉这种多模态特征分布关联,以此实现多模态的时序异常检测.

2 多模态对抗学习异常检测方法

MMGAN 是一个基于多模态对抗学习的无监督时间序列异常检测模型,模型框架如图 2 所示,由模态转换、多模态生成器 G 和多模态判别器 D 这 3 个模块组成.具体地,模态转换模块实现时序特征的时频转换,利用小波变换将特征 x_i^T 从时域空间映射到频域空间形成频域特征 x_i^F ;多模态生成器 G 中有自适应编码器 G_E 和解码器 G_D , G_E 将特征 x_i^T 和 x_i^F 编码为 z^T 和 z^F ,然后将得到的各个模态的低维表示融合为 z^+ ,解码器 G_D 将融合特征 z^+ 重构为 $x_i^{T'}$ 和 $x_i^{F'}$;多模态判别器 D 对原始特征和重构特征进行判别.多模态生成器中编码网络和多模态判别器的判别网络根据模态进行权重共享.整个模型通过学习正常数据的分布和特征重构来发现异常.从分布角度上:

定义 1. $p_{\text{data}}(x_i^T)$ 和 $p_{\text{data}}(x_i^F)$ 为每个样本 x 在其时域和频域特征空间上的分布.

定义 2. $p_z(z^T)$ 和 $p_z(z^F)$ 是原始模态分布在低

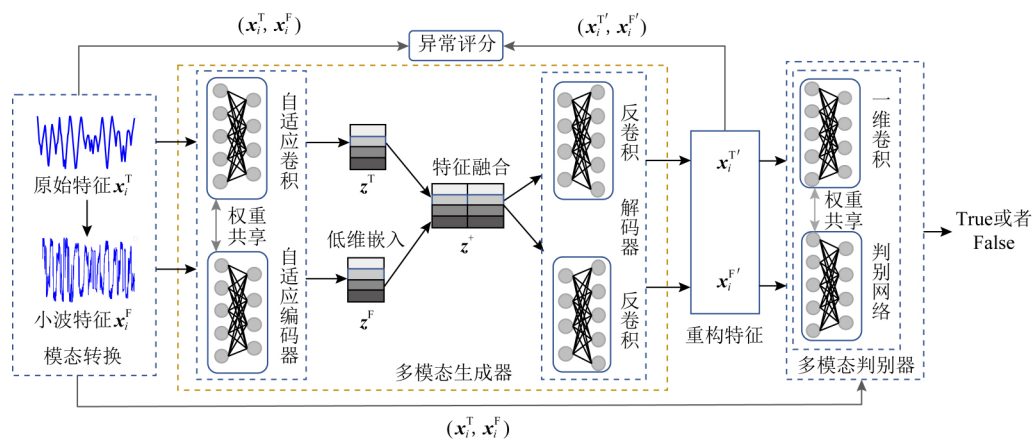


Fig. 2 Multimodal generation adversarial model

图 2 多模态生成对抗模型

维空间 Z 上的映射, $p_Z(z^+)$ 是空间 Z 上 2 个低维分布的融合。

定义 3. $p_g(x_i^T)$ 和 $p_g(x_i^F)$ 为时域和频域特征空间上生成特征的分布。

根据分布定义,多模态生成对抗网络的目标函数为

$$\min_G \max_D V(D, G) = E_{x \sim p_{\text{data}}(x^T)} [\lg D(x_i^T)] + E_{x \sim p_{\text{data}}(x^F)} [\lg D(x_i^F)] + E_{z \sim p_z(z^+)} [\lg(1 - D(G(z^+)))]. \quad (1)$$

根据式(1),对于给定的多模态生成器 G ,最佳的多模态判别器为

$$\max_D V(D, G) = \max_D D_G^*(x_i) = \frac{p_{\text{data}}(x_i^T)}{p_{\text{data}}(x_i^T) + p_g(x_i^T)} + \frac{p_{\text{data}}(x_i^F)}{p_{\text{data}}(x_i^F) + p_g(x_i^F)}. \quad (2)$$

对于最佳的多模态判别器 $\max_D V(D, G)$, 博弈公式可以重新表述为 $C(G) = \max_D V(G, D)$, $C(G)$ 推导如下:

$$\begin{aligned} C(G) &= \max_D V(G, D) = \\ &E_{x \sim p_{\text{data}}(x^T)} [\lg D_G^*(x_i^T)] + \\ &E_{x \sim p_{\text{data}}(x^F)} [\lg D_G^*(x_i^F)] + \\ &E_{z \sim p_z(z^+)} [\lg(1 - D_G^*(G(z^+)))] = \\ &E_{x \sim p_{\text{data}}(x^T)} [\lg D_G^*(x_i^T)] + \\ &E_{x \sim p_{\text{data}}(x^F)} [\lg D_G^*(x_i^F)] + \\ &E_{x \sim p_g(x^T)} [\lg(1 - D_G^*(x_i^T))] + \\ &E_{x \sim p_g(x^F)} [\lg(1 - D_G^*(x_i^F))] = \\ &E_{x \sim p_{\text{data}}(x^T)} \left[\lg \frac{p_{\text{data}}(x_i^T)}{p_{\text{data}}(x_i^T) + p_g(x_i^T)} \right] + \\ &E_{x \sim p_{\text{data}}(x^F)} \left[\lg \frac{p_{\text{data}}(x_i^F)}{p_{\text{data}}(x_i^F) + p_g(x_i^F)} \right] + \\ &E_{x \sim p_g(x^T)} \left[\lg \frac{p_g(x_i^T)}{p_{\text{data}}(x_i^T) + p_g(x_i^T)} \right] + \\ &E_{x \sim p_g(x^F)} \left[\lg \frac{p_g(x_i^F)}{p_{\text{data}}(x_i^F) + p_g(x_i^F)} \right]. \end{aligned}$$

如上可见,对于 $C(G)$, 当且仅当 $p_{\text{data}}(x_i^T) = p_g(x_i^T)$, $p_{\text{data}}(x_i^F) = p_g(x_i^F)$ 时达到全局最小. 此时多模态判别器无法识别真实样本和生成样本. 所以, 对于多模态对抗学习模型, 每个模态的 $p_{\text{data}}(x) = p_g(x)$ 时, 算法达到纳什均衡^[10], 即全局最优. MMGAN 可以通过多模态分布的联合学习来更好地逼近全局最优。

2.1 模态时频转换

模态之间通过小波变换进行 x_i^T 到 x_i^F 的变换. 这种变换将一个离散时间信号分解为一个离散小波

表示. 形式上, 给定时间序列 $x = (t_0, t_1, \dots, t_{N-1})^T$ 代表一个长度为 N 的离散时间序列, 基函数为 $\varphi = (\varphi_0, \varphi_1, \dots, \varphi_{N-1})^T$ 和 $\psi = (\psi_0, \psi_1, \dots, \psi_{N-1})^T$, 那么每个尺度层(j_0 或 j)中每个平移(以 k 为索引)的系数就是信号在每个基函数上的投影:

$$w_\varphi[j_0, k] = (x, \varphi_{j_0, k}) = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} X[m] \varphi_{j_0, k}[m], \quad (3)$$

$$w_\psi[j, k] = (x, \psi_{j, k}) = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} X[m] \psi_{j, k}[m]. \quad (4)$$

在式(3)和式(4)中 $w_\varphi[j_0, k]$ 被称为近似系数, $w_\psi[j, k]$ 被称为细节系数. 不同层次上的细节系数反映了信号在不同尺度上的方差, 而近似系数则反映了信号在该尺度上的平滑平均. 离散小波变换的一个重要性质是每一层的细节系数是正交的, 对于任何一对不在同一层的细节系数, 如式(5), 其内积为 0:

$$w_\psi[j, *] \cdot w_\psi[j', *] = 0. \quad (5)$$

因此, 可以将细节系数解释为信号的加性分解, 即多分辨率分析. 小波变换利用这种多分辨率特性能在非平稳时间序列上进行时频分析, 使异常检测模型对非平稳时间序列信息也具有高效的检测能力。

2.2 生成器和判别器

MMGAN 的生成对抗部分主要由多模态生成器和多模态判别器 2 部分组成。

2.2.1 多模态生成器

为了充分利用多模态时序信息的同时解决模态特征维度变换带来的参数敏感性问题, MMGAN 的多模态生成器采用了一种覆盖所有尺度的自适应卷积架构(omni-scale CNN, OSCNN)^[34]. 这个架构在学习过程中会自适应选择最优卷积核大小, 避免过大或过小卷积核带来的时序特征表示损失和噪声问题^[34], 辅助多模态方法进行更好的特征学习. 如图 3 所示, MMGAN 使用的自适应卷积架构由输入数据、自动设置卷积核、拼接、激活函数和输出 5 个基本部分构成. 卷积核的大小为 1 到 N 的质数, 卷积核的数量为 1 到 N 的质数个数, N 的大小与每个模态特征的维度正相关. 在最后一层卷积中, 只有大小为 1 和 2 的卷积核, 通过这种卷积架构, 卷积的接受域可以覆盖所有尺度的时序样本, 保证时序特征得到高效学习。

使用自适应卷积网络的多模态生成器模块如图 2 所示. 具体地, 在多模态生成器 G 中, 由 2 个共享

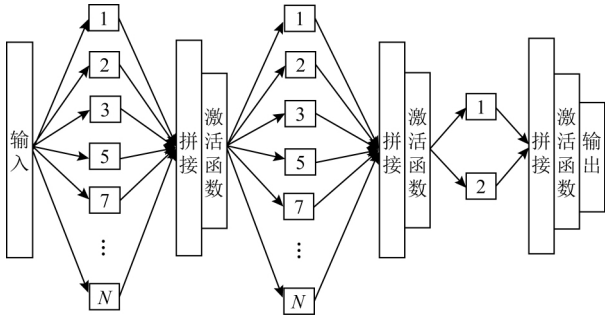


Fig. 3 Adaptive convolution

图3 自适应卷积

权重的自适应卷积网络组成的自适应编码器 G_E 将时域和频域空间上的原始数据分布 $p_{data}(x_i^T)$ 和 $p_{data}(x_i^F)$ 映射到低维空间 $p_z(z^T)$ 和 $p_z(z^F)$ 上, 并对 x_i^T 和 x_i^F 进行特征提取得到低维嵌入 z^T 和 z^F , 映射函数为

$$\begin{aligned} p_z(z^T) &= p_{data}(z^T | x_i^T), \\ p_z(z^F) &= p_{data}(z^F | x_i^F), \end{aligned} \quad (6)$$

低维嵌入函数为

$$z^T, z^F = G_E(x_i^T, x_i^F), \quad (7)$$

生成器 G 再将 z^T 和 z^F 融合为 z^+ , 融合公式为

$$z^+ = fusion(z^T, z^F) = z^T \oplus z^F, \quad (8)$$

其中, \oplus 符号代表特征按照指定维数 concat 的操作.

G 通过特征融合的方式建立潜在空间的时频分布关联. 融合特征 z^+ 进入包含 2 个反卷积网络的解码器 G_D , G_D 将低维分布映射到 2 个模态的生成空间 $p_g(x_i^T)$ 和 $p_g(x_i^F)$ 上, 并生成 2 个重构特征 $x_i^{T'}$ 和 $x_i^{F'}$, 高维映射函数为

$$\begin{aligned} p_g(x_i^F) &= p_z(x_i^F | z^+), \\ p_g(x_i^T) &= p_z(x_i^T | z^+), \end{aligned} \quad (9)$$

特征重构函数为

$$x_i^{T'}, x_i^{F'} = G_D(z^+). \quad (10)$$

多模态生成器通过编解码方式建立了时序特征分布的映射关系, 并通过网络权重共享和低维特征融合建立时序特征的时频分布关联, 充分利用时序信息多模态分布关联的同时解决参数敏感性问题, 使多模态时序特征得到高效学习, 增强模型特征重构能力.

2.2.2 多模态判别器

多模态判别器模块如图 2 所示, 主要由 2 个权重共享的卷积网络组成, 它们负责对多模态的原始特征和生成特征进行判别. 通过让原始特征的 $p_{data}(x_i^T)$ 和 $p_{data}(x_i^F)$ 判别为 True, 让生成特征的 $p_g(x_i^T)$ 和 $p_g(x_i^F)$ 判别为 False, 使多模态生成器生成越来越

逼近原始分布的特征, 即不断逼近全局最优解 $p_{data}(x_i^T) = p_g(x_i^T)$, $p_{data}(x_i^F) = p_g(x_i^F)$, 以此来对齐分布.

2.3 损失函数

多模态生成器 G 由 2 个组件构成: 自适应编码器 G_E 和解码器 G_D . 多模态特征重构公式为 $x_i^{T'}$, $x_i^{F'} = G_D(z^+)$. 根据式 (1), 多模态判别器的损失函数为

$$\begin{aligned} L_D &= E_{x \sim p_{data}(x^T)} [\lg D(x_i^T)] + \\ &E_{x \sim p_{data}(x^F)} [\lg D(x_i^F)] + \\ &E_{z \sim p_z(z^+)} [\lg (1 - D(G(z^+)))] = \\ &E_{x \sim p_{data}(x^T)} [\lg D(x_i^T)] + E_{x \sim p_{data}(x^F)} [\lg D(x_i^F)] + \\ &E_{x \sim p_g(x^T)} [\lg (1 - D(x_i^T))] + \\ &E_{x \sim p_g(x^F)} [\lg (1 - D(x_i^F))]. \end{aligned} \quad (11)$$

在多模态生成器 G 中, 损失函数采用重构误差损失和成对特征匹配损失的组合, 以此来最小化原始时序数据和经过判别网络隐藏层学习到的时序特征的误差, 提高判别网络的性能. f_D 为判别网络某一隐藏层上的激活函数, 多模态重构误差损失和多模态成对特征匹配损失函数分别为

$$L_r = \|x_i^T - x_i^{T'}\|_2^2 + \|x_i^F - x_i^{F'}\|_2^2, \quad (12)$$

$$\begin{aligned} L_{pf} &= \|f_D(x_i^T) - f_D(x_i^{T'})\|_2^2 + \\ &\|f_D(x_i^F) - f_D(x_i^{F'})\|_2^2. \end{aligned} \quad (13)$$

所以, 多模态生成器损失函数为

$$\begin{aligned} L_G &= \|x_i^T - x_i^{T'}\|_2^2 + \|x_i^F - x_i^{F'}\|_2^2 + \\ &\|f_D(x_i^T) - f_D(x_i^{T'})\|_2^2 + \|f_D(x_i^F) - f_D(x_i^{F'})\|_2^2. \end{aligned} \quad (14)$$

2.4 异常检测

多模态生成器 G 和多模态判别器 D 经过博弈学习, 利用式 (1) 逐渐逼近最优解 $p_{data}(x_i^T) = p_g(x_i^T)$, $p_{data}(x_i^F) = p_g(x_i^F)$. 此时的多模态生成器具有最优的特征生成能力, 即能从潜在空间高质量重构正常样本. 反之, 异常样本的重构会有误差, 以此发掘异常. 多模态检测框架异常评分公式为

$$F_s = \lambda_T (\|x_i^T - x_i^{T'}\|_2^2) + \lambda_F (\|x_i^F - x_i^{F'}\|_2^2), \quad (15)$$

其中 λ_T 和 λ_F 为每个模态评分的权重, 计算为

$$\begin{aligned} \lambda_T &= \frac{size(x^T)}{size(x^T) + size(x^F)}, \\ \lambda_F &= \frac{size(x^F)}{size(x^T) + size(x^F)}, \end{aligned} \quad (16)$$

其中 $size()$ 为模态特征维度.

2.5 算法实现

综合以上, MMGAN 的时序异常检测具体过程如算法 1:

算法 1. 多模态异常检测算法.

输入: 输入时序样本矩阵 $T = (x_1, x_2, \dots, x_N)$,

N 为样本数量;

输出: 异常评分.

- ① 初始化 G 和 D , 定义 $p_{\text{data}}(x_i^T)$ 和 $p_{\text{data}}(x_i^F)$.
- ② FOR i IN $\{1, 2, \dots, N\}$ DO:
- ③ 时域 x_i^T 通过式(3)(4)生成频域 x_i^F ;
- ④ $p_{\text{data}}(x_i^T)$ 和 $p_{\text{data}}(x_i^F)$ 通过式(6)进行分布低维映射;
- ⑤ x_i^T 和 x_i^F 通过式(7)进行特征嵌入;
- ⑥ z^T 和 z^F 通过式(8)进行融合;
- ⑦ $p_z(z^+)$ 通过式(9)进行分布高维映射;
- ⑧ z^+ 通过式(10)进行重构;
- ⑨ D 通过式(11)进行损失计算, 梯度下降更新模型;
- ⑩ G 通过式(14)进行损失计算, 梯度下降更新模型;
- ⑪ G 和 D 根据训练代数重复步骤④~⑩, 式(1)逐渐逼近最优解;
- ⑫ END FOR
- ⑬ G 通过式(15)计算异常评分.

结合算法 1, 时间序列的多模态异常检测过程为:

- 1) 原始时域时序特征通过步骤③生成频域特征.
- 2) 在多模态生成器中, 2 个模态数据依次通过步骤④~⑧学习关联分布并重构出 2 个特征. 生成器通过步骤⑩进行更新.

3) 在多模态判别器中, 通过步骤⑨对生成特征和原始特征进行判别, 以对齐原始分布和生成分布, 并更新自身.

4) 通过步骤⑪逐渐收敛逼近纳什均衡.

5) 通过步骤⑬检测异常.

综上所述, MMGAN 是一个基于重构的异常检测方法, 异常的评估取决于生成样本与原始样本的距离, 即生成器从潜在空间学习特征分布的能力. 而 MMGAN 的多模态思想可以在时域和频域 2 个空间上对特征分布进行联合学习, 增强模型的分布建模和特征重构能力, 从而提高检测性能.

3 实验结果分析

本节从对比实验、消融实验和可视化实验 3 个角度分析论证多模态异常检测框架的检测性能.

3.1 环境和数据集

实验基于 Ubuntu 环境, 使用 Pytorch 框架进

行模型搭建. 平台主要硬件参数为 CPU Inter Core i7-9700, 内存 64 GB, GPU NVIDIA 2070, 8 GB 显存.

实验使用的数据集为:

1) MIT-BIH 心电图数据集. MIT-BIH 心律失常数据集包含了来自 Beth Israel 医院的 48 个试验对象的心电图记录. 标签由 2 个或更多独立的心脏病专家在每一次心跳的波峰上注释, 指出每一次心跳的位置和类型. 根据 AAMI 推荐, 正常节拍包括标注为 N, L 和 R4 的节拍, 而命名为 102, 104, 107 和 218 的记录由于信号质量不够而被删除. 数据集总共包含 97 568 次心跳节拍和 2 860 万个时间点. 实验时, 本文采用和文献[15]相同的数据处理方式, 即把 ECG 数据按周期切割成相同的心跳节拍进行检测.

2) UCR 时间序列数据集^[35]. 该数据集于 2002 年推出, 经过数十年发展已经成为时间序列领域的重要资源, 至少有 1 000 篇发表的论文使用了该数据集. UCR 已经成为时间信号处理领域的基准数据. 该数据集一直在经历周期性的扩展. 在本文使用时, UCR 已经拓展为 128 个数据集. 实验时, 从中取部分标签种类或者特征长度不同的 5 个数据集, 相关数据集统计如表 1 所示:

Table 1 Data Set Statistics

表 1 数据集统计信息

数据集	维度	数据条数	类别
CBF	128	930	3
MixedShapesSmallTrain	1 024	2 525	5
UCR FreezerSmallTrain	301	2 878	2
TwoPatterns	128	5 000	4
ElectricDevices	96	16 637	7
MIT-BIH Arrhythmia	320	97 568	2

3.2 评价指标

由于数据的处理方式和训练方式存在样本不平衡的特性, 本文使用 AP(average precision)和 AUC(area under curve)指标来衡量模型性能, 相较于其他直接基于混淆矩阵的评价方式, AP 和 AUC 的计算方法同时考虑了模型对于正例和负例的分类能力. 更重要的是, 在数据样本正负类不平衡而且随着时间变化的情况下, 它们依然能够对分类器做出合理的评价. AP 和 AUC 的计算结果分别来源于 PR(precision-recall)曲线和 ROC(receiver operating characteristic curve)曲线, 其最根本的统计来源为异常检测的分类混淆矩阵, 如表 2 所示:

Table 2 Classification Confusion Matrix for Anomaly Detection

表 2 异常检测分类混淆矩阵

真实类别	检测正常	检测异常
正常类	TP	FN
异常类	FP	TN

计算 AP 的 PR 曲线如图 4 所示,其中横轴为召回率(*Recall*, 或 *TPR*),反映了分类器对正例的覆盖能力.而纵轴为精确度(*Precision*),反映了分类器预测正例的准确程度.PR 曲线反映了分类器对正例的识别准确程度和对正例的覆盖能力之间的权衡.样本中每个类别可以绘制出一条 PR 曲线,曲线中为依次改变置信度为 10%~100%得到一组由精确度和召回率组成的坐标,连接这些值就是 PR 曲线.

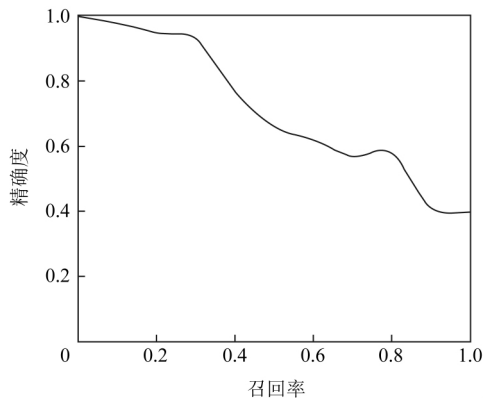


Fig. 4 PR curve graph

图 4 PR 曲线图

精确度体现了预测为正且实际为正的实例占有所有预测为正的样本比例,计算方法为

$$Precision = \frac{TP}{TP + FP} \quad (17)$$

召回率体现了预测为正且实际为正的实例占有所有正类样本的比例,计算方法为

$$Recall = \frac{TP}{TP + FN} \quad (18)$$

计算 AUC 的 ROC 曲线是以假阳率 (false positive rate, FPR) 为横轴、召回率为纵轴,衡量二分类系统性能的曲线,反映了分类器对正例的覆盖能力和对负例的覆盖能力之间的权衡.同样依次取置信度 10%~100%,会得到一组不同的假阳率、召回率组成的坐标,连接两者就能得到 ROC 曲线,ROC 曲线与 X 轴围成的图形面积可以作为一个综合衡量指标,即 AUC.

FPR 表示预测为正但实际为负的实例占有所有负样本的比例,计算方法为

$$FPR = \frac{FP}{FP + TN} \quad (19)$$

3.3 实验设置和实验参数

为了验证本文方法的有效性,本文的实验过程将进行 5 个模型在 6 个数据集上的对比实验、消融实验和数据可视化实验.实验时采用“one VS all”的训练方式,依次将一类时序特征处理为正常,将其余种类的特征处理为异常.对每个标签重复训练 10 次,以保证结果的可信性和稳定性.对于每个数据集,实验中用 80% 的官方数据集进行训练,保持剩余的 20% 作为测试组,进一步从训练集挑选 25% 作为验证集,然后从训练集中丢弃异常样本.

实验基本参数:训练迭代次数为 200,批大小 $batchsize=64$,学习率 $lr=0.001$.为了体现本文的自适应方法可以克服参数敏感性,面对不同的数据集和不同模态的特征维度,模型的网络参数均相同.使用 Leaky Relu 激活函数并设置斜率为 0.2,编码潜在向量的维度由自适应编码网络自己学得.网络的具体参数表 3 所示,其中 $Conv(k, s, p)$ 为一维卷积, $ConvT(k, s, p)$ 为一维反卷积,卷积网络中, k 代表 $kernel_size$, s 代表 $stride$, p 代表 $padding$.

Table 3 Network Parameters

表 3 网络参数

模块	编码网络	解码网络
生成器	自适应最大层数为 3, 自适应最大卷积核为 89	ConvT(10,1,0)
		ConvT(4,2,1)
		ConvT(4,2,1)
		ConvT(4,2,1)
判别器	pooling	linear
		Conv(4,2,1)
		Conv(4,2,1)
		Conv(4,2,1)
		Conv(4,2,1)

3.4 对比方法

MMGAN 将与 4 种传统单模态异常检测方法进行对比.

1) AnoGAN^[14] 是一个基于 WGAN 的生成对抗模型,在训练阶段,仅使用正常样本无监督地学习一个潜在空间中的流形分布.测试时,对于测试样本,定义一个损失函数进行多次反向传播以求得一个样本的潜在空间表示.生成器利用这个潜在表示生成一个新的数据,使用这个生成和原始样本进行异常检测. AnoGAN 是生成对抗思想在异常检测的

开山之作.然而,在测试时,该方法需要为每个例子解决一个优化问题,以找到一个潜在的表示 z ,然后使用这个 z 来计算示例的异常值,这使得该方法在大型高维数据集或实时应用中不切实际.

2) ALAD^[28]是一个基于双向 GAN 的异常检测模型.模型训练时,从一个数据 x 的原始特征空间中经过编码得到一个潜在向量 z ,同时从某个分布中采样得到 z' ,解码 z' 得到 x' ,最后将 (x, z) 和 (x', z') 送入判别器进行判别,以此稳定对抗训练.最后模型使用重构误差来确定数据样本是否异常. ALAD 擅长处理高维特征,但是在低维小数据集上处理太过复杂,导致效率低下.

3) Ganomaly^[29]是一个针对图像的生成对抗异常检测方法.不同于一般基于自编码器的方法, Ganomaly 使用了一个编码器(encoder 1)—解码器(decoder)—编码器(encoder 2)的网络结构,同时学习原图、重建图和原图的编码、重建图的编码 2 个映射关系.该方法不仅对生成的图片外观做了约束,对图片内容也做了约束,在视觉领域得到了广泛认可.但是这种针对图像的设计使得该模型在时序领域表现欠佳.

4) BeatGAN^[15]是一个应用在时序上的生成对抗模型,该方法以划分固定心跳节拍的方式对 ECG 数据进行了异常检测,模型也采用编码器的方式得到样本的潜在表示.不同的是, BeatGAN 在判别网络中采用对抗正则的方式对编码中间特征进行了约束,一定程度上解决了梯度消失和爆炸问题.但是该方法由于采用划分周期的方法,所以难以高效处理

无明显周期或者特征长度可变的时序特征,更难以充分利用时间序列的关联关系,应用有限.

综合以上分析可以看出:传统单模态异常检测算法因为各自的局限性,并不能在时序领域建立一个通用的检测模型对时间序列进行高效的利用.本文提出的多模态检测方法可以充分利用时序信息在多模态空间上的特征分布关系,解决传统方法带来的问题.

3.5 实验结果分析

3.5.1 对比实验

5 个模型在 6 个数据集的对比实验结果如表 4 所示.从表中可以看出,在 UCR 的 5 个数据集上, MMGAN 在网络参数固定的情况下在 AUC 和 AP 这 2 个指标上实现了对传统最优单模态方法最高 12.50%和 21.59%的超越,证明 MMGAN 的自适应网络帮助模型在多模态空间上学习到了更好的特征分布.在 CBF 这个小数据量的数据集上, MMGAN 相较于传统单模态检测方法在 2 个指标上实现了 12.50%和 21.59%的最高提升,证明在小数据量的数据集上多模态思想充分利用已有信息的优势愈发明显.在 MIT-BIH 的 Arrhythmia 数据集上,面对具有明显周期的 ECG 数据, MMGAN 在 2 个指标上分别实现了对传统最优单模态方法的 1.20%和 1.02%提升,证明多模态方法针对大数据量的周期性数据也能进行高质量的分布学习.综上,本文提出的 MMGAN 能有效学习时间序列在不同模态上的分布关联实现更高效的异常检测,弥补了传统单模态方法只能利用单一空间数据进行学习的缺陷.

Table 4 Abnormal Detection Results

表 4 异常检测结果

方法	数据集											
	CBF		MixedShapes-SmallTrain		FreezerSmall-Train		Two-Patterns		Electric-Devices		Arrhythmia	
	AUC	AP	AUC	AP	AUC	AP	AUC	AP	AUC	AP	AUC	AP
AnoGAN ^[14]	0.664 9	0.596 4	0.722 1	0.818 9	0.688 0	0.730 5	0.598 0	0.599 9	0.659 1	0.624 7	0.904 3	0.865 6
ALAD ^[28]	0.761 0	0.717 7	0.789 1	0.761 6	0.764 1	0.777 0	0.658 7	0.582 0	0.751 0	0.771 6	0.864 2	0.803 5
Ganomaly ^[29]	0.791 7	0.699 1	0.767 3	0.754 8	0.753 4	0.621 6	0.651 8	0.545 4	0.848 9	0.822 9	0.908 3	0.870 1
BeatGAN ^[15]	0.816 5	0.735 1	0.888 5	0.811 2	0.857 0	0.724 8	0.625 3	0.478 3	0.716 4	0.579 9	0.944 7	0.910 8
MMGAN	0.918 6	0.893 8	0.918 3	0.844 9	0.895 0	0.817 0	0.726 1	0.615 0	0.893 4	0.882 3	0.956 0	0.920 1

注:黑体数字为指标最高值.

3.5.2 消融实验

为了验证模型中各部分的有效性,本节将在 UCR 的 ElectricDevices 数据集上进行 MMGAN 的消融实验.4 种模型结构分别为:

1) GAN 模型.单模态生成对抗模型,生成器和判别器使用最基本的卷积和反卷积作为网络编解码结构.

2) MMGAN w/o(without) M 模型.在生成对抗

模型中使用单模态自适应编码器作为编码模块,未添加多模态结构.

3) MMGAN w/o(without) OS 模型.使用多模态结构,但是多模态生成器使用基本卷积网络和反卷积网络作为编码和解码器,未添加自适应卷积结构.

4) MMGAN 模型.本文最终模型,使用多模态框架并添加自适应编码器作为框架的编码部分.

以上 4 种模型在 ElectricDevices 数据集上的 AUC 和 AP 指标如表 5 所示:

Table 5 Ablation Experiments on ElectricDevices Dataset
表 5 ElectricDevices 数据集消融实验

模型	AUC	AP
GAN	0.716 4	0.579 9
MMGAN w/o M	0.882 3	0.823 4
MMGAN w/o OS	0.773 6	0.756 5
MMGAN	0.893 4	0.882 3

注:黑体数字为指标最高值.

从表 5 中可见,加入自适应结构的生成对抗模型(MMGAN w/o M)较只使用普通卷积结构的 GAN,在 AUC 和 AP 这 2 个性能指标上分别提高了 23.16%和 41.99%,证明自适应卷积较传统卷积方法能在时序特征上学到更好的特征.而加入多模

态结构的生成对抗模型(MMGAN w/o OS)较 GAN 在 2 个指标上分别提高了 7.98%和 30.45%,证明多模态思想帮助模型学到了多空间的联合分布,比单模态方法执行了更高效的异常检测.而最终的模型比只使用自适应结构的模型(MMGAN w/o M)在 2 个指标上分别提高了 1.26%和 7.15%;比只使用多模态思想的模型(MMGAN w/o OS)在 2 个性能指标上分别提高了 15.49%和 16.63%;比只使用普通卷积的模型(GAN)在 2 个性能指标上分别提高了 24.71%和 52.15%;证明自适应结构与多模态方法的结合使得 MMGAN 在多模态特征空间上学到了更好的特征分布,在 AUC 和 AP 上实现了检测性能的超越.

3.5.3 数据嵌入可视化

为了探索学习过程中数据嵌入的质量,本节实验对不同方法的样本嵌入进行可视化比较.具体而言,从 ElectricDevices 的测试集中选择 1 674 个数据样本.在此数据集上本文方法与 Ganomaly 和 AnoGAN 进行比较,将这 3 个方法的样本嵌入作为 t-SNE 工具的输入,然后生成二维空间的样本嵌入可视化.结果如图 5 所示,其中蓝色对应于正常类别,红色对应于异常类别.模型从左至右分别是 AnoGAN, Ganomaly 和 MMGAN.

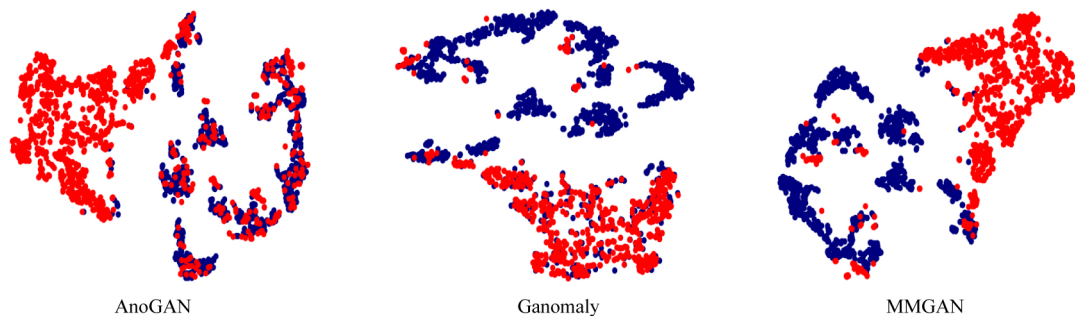


Fig. 5 Feature embedding

图 5 特征嵌入

在 MMGAN 的可视化结果中,正常数据和异常数据分布在不同的空间范围内,正常和异常数据都进行了有效聚集,而且边缘分界明显.证明多模态框架帮助模型学习到了更好的时序特征分布,充分利用了时序特征在多个模态上的分布关联,将样本进行了更好的分离.对比 Ganomaly 和 AnoGAN,这 2 种方法的嵌入较本文方法在可视化上有明显差距, Ganomaly 分界尚为明显但是重叠样本较多, AnoGAN 分界不明显的同时重合样本点也很多,嵌入效果差.

3.5.4 异常分布可视化

为了探索模型对异常数据的检测能力,本节实验对不同方法的异常评分分布进行了可视化实验.具体而言,本文方法与 Ganomaly 和 AnoGAN 在 ElectricDevices 的测试集上分别进行异常评分计算,然后将评分生成柱状图.结果如图 6 所示.

在 MMGAN 的异常评分分布结果中,评分中的正常和异常分布边界(异常阈值)清晰明显,重合分布很少,正负样本的评分都进行了有效聚集.证明多模态检测框架学习到了高质量的特征分布,从而

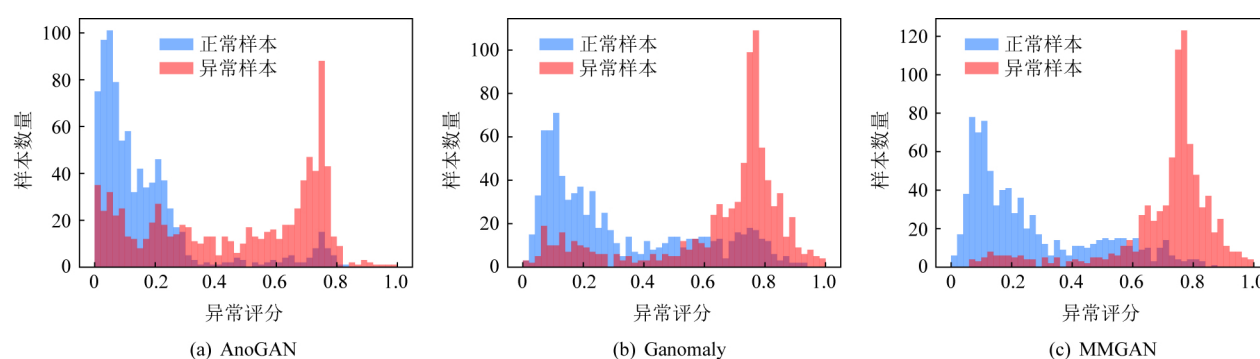


Fig. 6 Anomaly score distribution

图6 异常评分分布

给出了更准确的异常评分.对比 Ganomaly 和 AnoGAN,这 2 种方法的异常评分分布较本文方法在可视化上有明显差距,Ganomaly 正负评分的样本重合分布较多,AnoGAN 则更甚,大量正常样本被预测为异常.

综合以上所有实验结果,异常检测对比实验证明本文模型在 AUC 和 AP 这 2 个指标上实现了检测性能的提升;消融实验证明了本文各个思想对于时序异常检测的有效性;数据嵌入可视化体现了多模态检测思想帮助模型在时间序列上提取到了更好的嵌入特征;异常评分分布可视化证明了本方法更好地完成了正负样本评分的分离.可以得出结论:本文方法相较于传统单模态模型在时间序列的异常检测上表现出了更优异的检测性能.

4 总结与展望

当前,在时间序列异常检测领域,传统的单模态检测方法只能在单个数据空间上进行特征分布学习,从而造成了对现有信息利用不足、检测效率低等问题.然而多模态方法可以利用多模态空间上的特征分布关联解决传统单模态方法的缺陷.据此,本文提出了多模态生成对抗检测模型,通过“生成+对抗”的方式发掘时间序列在多个模态空间上的特征分布关联,充分利用时序信息进行分布建模,以此提高检测能力.另外,采用自适应卷积的编码器可以针对时序特征建立最优的特征提取方式.整个模型在充分利用时序信息分布的同时解决了参数敏感性问题,提高异常检测效率.

本文在 6 个数据集上进行了大量的实验,结果验证了本文思想的有效性,多模态方法可以通过学

习时序特征在多个特征空间上的分布关联来充分利用已有信息提高异常检测效率.下一阶段我们将考虑将更多的模态加入到这种方法以期达到对时序信息更高效的利用.

参 考 文 献

- [1] Keim D A, Nietzschmann T, Schelwies N, et al. Spectral visualization system for analyzing financial time series data [C] //Proc of Eurographics/IEEE TCVG Symp on Visualization. Aire-la-Ville, Switzerland: Eurographics Association, 2006: 195–202
- [2] McLachlan P, Munzner T, Koutsofios E, et al. LiveRAC: Interactive visual exploration of system management time series data [C] //Proc of the ACM SIGCHI Conf on Human Factors in Computing Systems. New York: ACM, 2008: 1483–1492
- [3] Weber M, Alexa M, Muller W. Visualizing time-series on spirals [C] //Proc of the 2011 IEEE Symp on Information Visualization. Los Alamitos, CA: IEEE Computer Society, 2011: 7–14
- [4] Kumar P, Sinha A. Real-time analysis and visualization of onlinesocial media dynamics [C] //Proc of the 2nd Int Conf on Next Generation Computing Technologies. Piscataway, NJ: IEEE, 2016: 362–367
- [5] Chen Wei, Huang Zhaosong, Wu Feiran, et al. VAUD: A visual analysis approach for exploring spatio-temporal urban data [J]. IEEE Transactions on Visualization and Computer Graphics, 2018, 24(9): 2636–2648
- [6] Xie Cong, Chen Wei, Huang Xinxin, et al. Vaet: A visual analytics approach for e-transactions time-series [J]. IEEE Transactions on Visualization and Computer Graphics, 2014, 20(12): 1743–1752
- [7] Xia Jing, Hou Yumeng, Chen Y V, et al. Visualizing rank timeseries of Wikipedia top viewed pages [J]. IEEE Computer Graphics and Applications, 2017, 37(2): 42–53

- [8] Chandola V, Banerjee A, Kumar V. Anomaly detection: A survey [J]. *ACM Computing Surveys*, 2009, 41(3): 1–58
- [9] Breunig M M, Kriegel H P, Ng R T, et al. LOF: Identifying density-based local outliers [C] // *Proc of the ACM SIGMOD Record*. New York: ACM, 2000: 93–104
- [10] Goodfellow I, Pouget-Abadie J, Mirza M, et al. Generative adversarial nets [C] // *Advances in Neural Information Processing Systems*. Montreal, CA: NIPS, 2014: 2672–2680
- [11] Radford A, Metz L, Chintala S. Unsupervised representation learning with deep convolutional generative adversarial networks [J]. *arXiv preprint, arXiv:1511.06434*, 2015
- [12] Creswell A, White T, Dumoulin V, et al. Generative adversarial networks: An overview [J]. *IEEE Signal Processing Magazine*, 2018, 35(1): 53–65
- [13] Lee H, Tsao Y. Generative adversarial network and its applications to speech signal and natural language processing [C] // *Proc of IEEE Int Conf on Acoustics, Speech and Signal Processing*. Piscataway, NJ: IEEE, 2018: 1–7
- [14] Schlegl T, Seeböck P, Waldstein S M, et al. Unsupervised anomaly detection with generative adversarial networks to guide marker discovery [C] // *Proc of the Int Conf on Information Processing in Medical Imaging*. Berlin: Springer, 2017: 146–157
- [15] Zhou Bin, Liu Shenghua, Hooi B. BeatGAN anomalous rhythm detection using adversarially generated time series [C] // *Proc of the 28th Int Joint Conf on Artificial Intelligence*. California: IJCAI, 2019: 4433–4439
- [16] Li Dan, Chen Dacheng, Jin Baihong, et al. MAD-GAN: Multivariate anomaly detection for time series data with generative adversarial networks [C] // *Proc of the Int Conf on Artificial Neural Networks*. Berlin: Springer, 2019: 703–716
- [17] Hochreiter S, Schmidhuber J. Long short-term memory [J]. *Neural Computation*, 1997, 9(8): 1735–1780
- [18] Geiger A, Liu Dongyu, Alnegheimish S, et al. TadGAN: Time series anomaly detection using generative adversarial networks [C] // *Proc of 2020 IEEE Int Conf on Big Data*. Piscataway, NJ: IEEE, 2020: 33–43
- [19] Amarasinghe K, Kenney K, Manic M. Toward explainable deep neural network based anomaly detection [C] // *Proc of 2018 11th Int Conf on Human System Interaction*. Piscataway, NJ: IEEE, 2018: 311–317
- [20] O'Shea T J, Clancy T C, McGwier R W. Recurrent neural radio anomaly detection [J]. *arXiv preprint, arXiv:1611.00301*, 2016
- [21] Chauhan S, Vig L. Anomaly detection in ECG time signals via deep long short-term memory networks [C] // *Proc of 2015 IEEE Int Conf on Data Science and Advanced Analytics*. Piscataway, NJ: IEEE, 2015: 1–7
- [22] Schölkopf B, Williamson R C, Smola A, et al. Support vector method for novelty detection [J]. *Advances in Neural Information Processing Systems*, 1999, 12(1): 582–588
- [23] Candès E J, Li Xiaodong, Ma Yi, et al. Robust principal component analysis? [J]. *Journal of the ACM*, 2011, 58(3): 1–37
- [24] Zhou Chong, Paffenroth R C. Anomaly detection with robust deep autoencoders [C] // *Proc of the 23rd ACM SIGKDD Int Conf on Knowledge Discovery and Data Mining*. Halifax, CA: ASSOC, 2017: 665–674
- [25] Cho K, Van Merriënboer B, Gulcehre C, et al. Learning phrase representations using RNN encoder-decoder for statistical machine translation [C] // *Proc of the Conf on Empirical Methods in Natural Language Processing*. ACL, 2014: 1724–1734
- [26] Malhotra P, Ramakrishnan A, Anand G, et al. LSTM-based encoder-decoder for multi-sensor anomaly detection [J]. *arXiv preprint, arXiv:1607.00148*, 2016
- [27] Kingma D P, Welling M. Auto-encoding variational Bayes [J]. *arXiv preprint, arXiv:1312.6114*, 2013
- [28] Zenati H, Romain M, Foo C S, et al. Adversarially learned anomaly detection [C] // *Proc of 2018 IEEE Int Conf on Data Mining*. Piscataway, NJ: IEEE, 2018: 727–736
- [29] Akcay S, Atapour-Abarghouei A, Breckon T P. Ganomaly: Semi-supervised anomaly detection via adversarial training [C] // *Proc of Asian Conf on Computer Vision*. Berlin: Springer, 2018: 622–637
- [30] Gothwal H, Kedawat S, Kumar R. Cardiac Arrhythmias detection in an ECG beat signal using fast fourier transform and artificial neural network [J]. *Journal of Biomedical Science and Engineering*, 2011, 4(4): 289–296
- [31] Cocconcelli M, Zimroz R, Rubini R, et al. STFT based approach for ball bearing fault detection in a varying speed motor [M] // *Condition Monitoring of Machinery in Non-Stationary Operations*. Berlin: Springer, 2012: 41–50
- [32] Ma Ling, Zhang Xiaohui. Characteristic of color images with watermark based on the relationship between non-void subspaces of inner space [J]. *Chinese Journal of Computers*, 2017, 40(5): 1203–1217 (in Chinese)
(马玲, 张晓辉. 基于内积空间非空子空间变换关系的含水印彩色图像特征分析 [J]. *计算机学报*, 2017, 40(5): 1203–1217)
- [33] Su Weixing, Zhu Yunlong, Liu Fang, et al. Outliers and change-points detection algorithm for time series [J]. *Journal of Computer Research and Development*, 2014, 51(4): 781–788 (in Chinese)
(苏卫星, 朱云龙, 刘芳, 等. 时间序列异常点及突变点的检测算法 [J]. *计算机研究与发展*, 2014, 51(4): 781–788)

- [34] Tang Wensi, Long Guodong, Liu Lu, et al. Rethinking 1D-CNN for time series classification: A stronger baseline [J]. arXiv preprint, arXiv: 2002.10061, 2020
- [35] Dau H A, Bagnall A, Kamgar K, et al. The UCR time series archive [J]. IEEE/CAA Journal of Automatica Sinica, 2019, 6(6): 1293–1305



Huang Xunhua, born in 1995. PhD candidate. His main research interests include information security and anomaly detection.

黄训华, 1995 年生. 博士研究生. 主要研究方向为信息安全与异常检测.



Zhang Fengbin, born in 1965. PhD, professor and PhD supervisor. Senior member of CCF. His main research interests include network and information security.

张凤斌, 1965 年生. 博士, 教授, 博士生导师. CCF 高级会员. 主要研究方向为网络与信息安全.



Fan Haoyi, born in 1994. PhD candidate. His main research interests include network embedding, anomaly detection, time series signal analysis and deep learning.

樊好义, 1994 年生. 博士研究生. 主要研究方向为网络嵌入、异常检测、时间序列信号分析和深度学习等.



Xi Liang, born in 1983. PhD, associate professor, master supervisor. His main research interests include artificial intelligence and its application, network and information security, machine learning, etc.

席亮, 1983 年生. 博士, 副教授, 硕士生导师. 主要研究方向为人工智能及其应用、网络和信息安全、机器学习等.