基于AAE的网络性能异常发现

王田丰,胡谷雨,王 睿,彭冬阳
(陆军工程大学 指挥控制工程学院,江苏 南京 210007)

摘 要:网络运维在充分发挥网络潜能方面有着不可替代的作用。其中,网络关键性能的监测和维护尤为重要。使用智能化的方法自动发现网络KPI的异常能够极大地减少运维人工成本,提升网络运维的效率。人工方法标注网络KPI中的异常,难度高,耗时长,因此无监督学习的异常检测正在成为解决此类问题的主要方法。提出一种基于对抗自编码器AAE的无监督检测模型AAE-AD,可以自动发现网络KPI中出现的异常,以便分析和排除网络故障。AAE-AD中使用了K最近邻算法进行缺失值的填充,交替训练自编码器网络和鉴别器网络来捕获正常数据的分布模式,结合自编码器网络的重构误差和鉴别器网络的鉴别能力计算出异常分值。实验表明,AAE-AD模型在最优F分数指标和AUC指标上均优于其他的无监督异常检测模型。

关键词:网络运维;时序序列;异常检测;对抗自编码器;生成对抗网络;K最近邻法
中图分类号:TP391 **文献标识码**:A **文章编号**:1673-629X(2021)07-0113-07
doi:10.3969/j.issn.1673-629X.2021.07.019

AAE-based Anomaly Detection for Network Performance

WANG Tian-feng, HU Gu-yu, WANG Rui, PENG Dong-yang
(School of Command and Control Engineering, Army Engineering University of PLA, Nanjing 210007, China)

Abstract: Network operation and maintenance plays an irreplaceable role in giving full play to the potential of network. The monitoring and maintenance of network critical performance is particularly important. Automatic detection of anomalies in network KPI by intelligent methods can greatly reduce the labor cost and improve the efficiency of network operation and maintenance. Manual methods to annotate anomalies in network KPIs are difficult and time-consuming, so unsupervised learning anomaly detection is becoming the main method to solve such problems. We propose an unsupervised detection model, AAE-AD, which is based on the adversarial autoencoder AAE, which can automatically detect the anomalies in network KPI, so as to analyze and troubleshoot network faults. In AAE-AD, the missing value is filled by the KNN, and the autoencoder network and the discriminator network are trained alternatively to capture the distribution pattern of normal data. The abnormal score is calculated by combining the reconstruction error of the autoencoder network and the discriminator network's discrimination ability. The experiment shows that the AAE-AD model is superior to other unsupervised anomaly detection models in terms of the optimal F score and AUC.

Key words: network operation and maintenance; temporal sequence; anomaly detection; AAE; GAN; KNN

0 引 言

为了确保良好的网络性能,需要对各个网络节点的吞吐量、延迟、丢包率等关键指标进行实时的监测和维护。这些指标在一定程度上反映了特定网络中用户的行为模式和网络的特性,具有动态性和周期性。网络中物理链路出现故障、网络遭受攻击导致故障等多方面的因素,都会导致网络出现异常,在这些监测的指标上也会有相应的异常体现。及时高效地发现网络指标的异常可以给网络运维人员赢得宝贵的时间来处理网络中出现的故障。

网络KPI(key performance indicator)异常检测(anomaly detection)问题可以抽象为时序序列异常检测问题,目的是为了发现不符合正常模式的序列段。有监督学习的方法[1-2]依赖准确的标注,而在实时的网络系统中,需要维护的指标数目多,并且数据都是实时产生的,数据量非常大,因此人工标注难以满足这一要求;无监督学习的方法不依赖于标注,在此问题上也有应用,但检测效果上仍不如人意。

为了解决这些困难,该文提出一种基于AAE[3](adversarial autoencoders)的无监督异常检测方法。目

收稿日期:2020-08-03 **修回日期**:2020-12-04
基金项目:装备预研基金项目(30501010301)
作者简介:王田丰(1997-),男,硕士,研究方向为网络管理、网络智能化;通讯作者:胡谷雨(1963-),男,博导,教授,研究方向为网络管理。

前,AAE 被广泛应用在语音和图像生成领域,并取得很好的效果。在 KPI 异常检测场景下,用滑动窗把数据集切分成小样本,其中异常的窗口样本只占很小一部分。AAE 模型在训练中学习到的是正常样本的数据分布模式。因此在异常检测阶段,正常样本能够被很好地编解码,重构误差很小,并且编码器输出的特征向量也更有可能被鉴别器识别为“正常”,综合两者判断是“异常”的概率比较低;而异常样本不符合正常模式,不仅重构误差大,而且编码输出的特征向量也更容易被鉴别器判为“异常”,总体上被判为“异常”的概率比较高。

该文的创新点总结如下:

(1)针对网络性能异常问题,提出了基于 AAE 的无监督的检测方法;

(2)针对原始数据部分缺失问题,引入了 KNN 算法进行数据填充,进一步提高了模型的检测精度;

(3)实验结果表明,AAE-AD 在最优 F 分数指标,AUC 指标上均优于其他的无监督检测算法;

(4)AAE 和 VAE 两个模型理论上有一定的相似性,对于两个模型在检测性能上的差异,给出了合理的解释。

1 相关工作

通用异常检测技术的调研报告[4]给出了异常检测的定义和异常检测可遵循的原则,异常检测就是检测测试数据是否符合正常的数据分布,不符合正常数据分布的就被划分为异常,而且异常数据占比通常很小。许多新的方法被应用在网络异常检测领域[5],如集成学习[6]在网络异常检测中的运用解决了网络异常种类多、单一模型处理问题时局限性大的问题。

网络关键指标异常检测问题是网络异常检测问题的一个分支,属于时序序列异常检测。由于在网络监测系统中,记录的时序序列数据量非常庞大,人工难以给出满足有监督学习训练时需要的大量准确标注,因此这个问题往往在无监督学习范畴下解决比较合理。

自回归移动平均模型(autoregressive integrated moving average)是一种基于统计理论的无监督预测模型,结合了自回归模型(AR)和移动平均模型(MA)的优点,对于非平稳序列也能达到良好的预测效果。ARIMA 模型在异常检测领域[7]也有广泛的应用,如孙建树[8]等人将 ARIMA 运用到水文时间序列异常检测问题中,取得了良好效果。

RNN 和 LSTM 是最常用的两种深度时序序列预测模型,同时也是时序序列异常检测[9]的有效方法。一般在异常检测中,采用预测值与真实值差值的绝对值作为异常分值。其中,李洁等人[10]提出了基于 RNN 的多维时序序列预测算法;仇媛等人[11]提出了基于 LSTM 和滑动窗口的流数据异常检测方法。

生成模型是一种典型的无监督学习模型,在现在的图像和语音生成领域运用的非常广泛,在异常检测领域也衍生出一些可用的方法。变分自编码器(variational autoencoder, VAE)和生成式对抗网络(generative adversarial networks, GAN)是两种运用广泛且具有代表性的生成器模型。其中 VAE[12]使用了变分推断技术[13-14],通过不断优化证据下界(evidence lower bound, ELBO)来使得自编码器在得到训练的同时,模型生成的样本空间分布能不断靠近先验分布,这里的先验分布一般假设为混合高斯分布;而 GAN[15]模型分为生成器和鉴别器,通过交替训练生成器和鉴别器来使得生成器生成的样本越来越真实,同时鉴别器对于真假样本的鉴别能力越来越强,最终达到平衡。其中,VAE 与双向领域算法结合成一个混合模型[16],在 MNIST 和 CIFAR-10 数据集上取得了较好的异常检测效果。余广民等人[17]综合论述了基于 GAN 的异常检测算法,同时 GAN 也被应用到视频异常检测场景[18]中。

但是笔者发现上述方法中,传统的有监督模型的性能依赖于大量的人工标签,而现有的无监督模型 ARIMA、RNN、LSTM、VAE、GAN 在网络数据集上的异常检测效果仍然不够好,难以满足业务上的需求。为此,提出了一种新的基于 AAE 的异常检测模型 AAE-AD。这是一种无监督学习模型,适用于网络运维中人工标注困难的情境,该模型能够很好地学习到“正常”时序序列的特征空间分布,在针对网络 KPI 的异常检测中达到很好的效果。

2 AAE-AD 模型介绍

2.1 AAE-AD 数据预处理

网络监测器记录的网络数据往往长达数周。第一,不同时间段内的数值范围相差可能很大,并且往往带有噪声;第二,由于监测器故障或者人工操作失误,数据可能存在部分缺失。针对这两个问题,先对数据进行标准化处理,然后进行数据填充。数据标准化采用 z-score 方法,表示如下:

$$X' = \frac{X - \mu}{\sigma} \tag{1}$$

其中,μ 为观测值序列 X 的均值,σ 为 X 的均方差;数据标准化消除了奇异样本数据的影响,能够提高算法精度并加快算法的收敛速度。

缺失数据填充借鉴 KNN[19]算法思想,基本流程如以下伪代码所示:

算法 1:KNN 填充空数据。

输入:原始观测值序列 X';

输出:空值填充后的序列 X''。

1:设置近邻数量 k,计算空值区间集合 $M = \{(s_1,e_1),(s_2,e_2),\cdots,(s_q,e_q)\}$

2:for (s_i,e_i) in M

3:$j = 0$

4:while $s_i + j \leqslant e_i$ do

5:找到与下标 $(s_i + j)$ 最近的 k 个非空近邻下标,设为集合 G

6:计算各个近邻 n 对于目标空值的贡献比重 $w_n = \dfrac{\dfrac{1}{\mathrm{abs}(G_n - (s_i + j))}}{\sum_{l=0}^{|G|}\dfrac{1}{\mathrm{abs}(G_l - (s_i + j))}}$

7:计算 $X''[s_i + j] = \sum_{l=0}^{|G|} w_l * X'[G_l]$

8:$j = j + 1$

9:end while

10:end for

KNN 填充算法中,首先获取所有的空值区间 $M = \{(s_1,e_1),(s_2,e_2),\cdots,(s_q,e_q)\}$,$s$ 代表区间起始点,e 代表区间结束点,从 $X'[s]$ 到 $X'[e]$ 都是空值。算法的主要思想是利用坐标最近的 k 个点来计算填空值,其中邻居的影响与相隔的距离成反比,距离越近影响越大。算法第 6 行中,对各个邻居的影响力进行了归一化;第 7 行,对各个邻居的值进行加权求和,计算出填充值。

最后,采用滑动窗口方法将观测序列切分成固定长度的样本。模型训练中,每个长度为 W 的时间窗口为一个训练样本;异常检测中,也以时间窗口为基本单位。在实际的网络系统中,允许存在一定的时延,因此,只要选取合适的时间窗口,能够保证异常检测模型的实时性和实用性。

2.2　AAE-AD 模型训练

整个 AAE-AD 框架分为模型训练和异常检测两部分。如图 1 所示,训练过程包含了对编码器、解码器和鉴别器的训练。

编码器和解码器使用的是 CNN 网络,将一维数据变成二维数据使模型更好地学习到数据的空间分布特性,能够更好地进行特征提取和还原。编码器对训练样本进行特征提取产生特征向量,分别作为解码器和鉴别器的输入;解码器将特征还原后结合原始输入计算出重构损失,并对编码器和解码器参数进行更新;鉴别器结合编码器产生的特征向量和从混合高斯模型中采样出的向量计算出鉴别损失来更新鉴别器和编码器,这在提高鉴别器鉴别能力的同时,也使得编码器产生的特征向量越来越真实,最终能够达到混淆鉴别器的程度,两者达到一定的平衡。

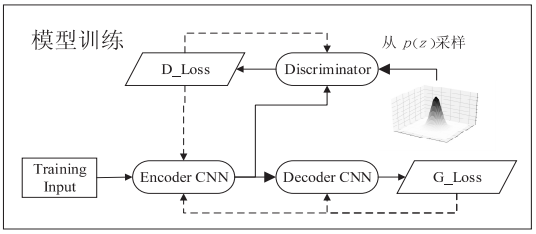

图 1　AAE-AD 模型的训练

2.2.1　自编码器网络的训练

自编码器网络实际上是一个信息压缩和还原的过程,编码器 G_1 将高维数据向量 x 压缩成低维特征向量 z,而解码器 G_2 负责将低维特征向量 z 尽量还原回去。在编解码的过程中存在信息损耗,信息损耗越大,重构效果越差。自编码器的训练就是通过最小化重构损失来增强网络的信息压缩与还原的能力。这里采用均方差损失,所以自编码器平均损失函数可以表示为:

$$\mathrm{Loss}_{G_1,G_2} = \frac{1}{n}\sum_{i=1}^{n}\mathrm{mse}(x_i, G_2(G_1(x_i))) \tag{2}$$

其中,x_i 是来自原始数据的样本。

2.2.2　对抗网络的训练

AAE 中对抗训练的思想来自于 GAN,可以看成一个两者博弈的过程。这里就是编码器部分 G_1 与鉴别器 D 的博弈[20],训练的目标就是能够使 G_1 编码结果越来越接近“真实分布”,即预设的先验分布 $p(z)$,同时使得鉴别器能够更好地区分特征向量到底是来自于编码器输出的特征向量还是采样自“真实分布”的向量。先验分布假设为混合高斯分布,因为混合高斯分布经过神经网络投射可以拟合任意的分布。总体优化目标可以作如下表示:

$$\min_{G_1}\max_{D} V(D,G_1) = E_{z\sim p(z)}[\log D(z)] + E_{x\sim p_{data}(x)}[\log(1 - D(G_1(x)))] \tag{3}$$

鉴别器优化目标表示为:

$$\min -\frac{1}{n}\sum_{i=1}^{n}[\log D(z_i) + \log(1 - D(G_1(x_i)))] \tag{4}$$

编码器优化目标表示为:

$$\min \frac{1}{n}\sum_{i=1}^{n}[\log(1 - D(G_1(x_i)))] \tag{5}$$

其中,z_i 是采样自先验分布的向量,x_i 是来自原始数据的样本,n 为样本数。

自编码器网络和对抗网络交替训练,训练过程如以下伪代码所示:

算法 2:AAE-AD 模型训练。

输入:训练样本集 X;

输出:模型 G_1,G_2,D。

1:对训练样本集 X 进行预处理,产生输入样本 $\{x_1,x_2,\cdots,x_n\}$

2:for the q^{th} epoch do

3:for the i^{th} sample do

4:将 x_i 输入 AAE-AD 模型,产生编码器输出 $G_1(x_i)$,解码器输出 $G_2(G_1(x_i))$,鉴别器输出 $D(G_1(x_i))$

5:计算 $\text{loss}_A = \text{mse}(x_i, G_2(G_1(x_i)))$,使用 Adam[21] 优化器更新编码器和解码器参数

6:从混合高斯分布中采样出向量 z_i,产生鉴别器输出 $D(z_i)$

7:计算 $\text{loss}_D = -\log D(z_i) - \log(1 - D(G_1(x_i)))$,使用 Adam 优化器更新鉴别器参数

8:计算 $\text{loss}_{G_1} = \log(1 - D(G_1(x_i)))$,使用 Adam 优化器更新编码器参数

9:end for

10:end for

2.3 AAE-AD 异常检测

在网络训练结束后,模型中自编码器和鉴别器有相对独立的异常判断机制,如图 2 所示,模型的异常检测是将测试样本输入模型,结合模型的自编码器部分产生的重构误差和鉴别器部分产生的鉴别分值来对样本做异常判断的过程。

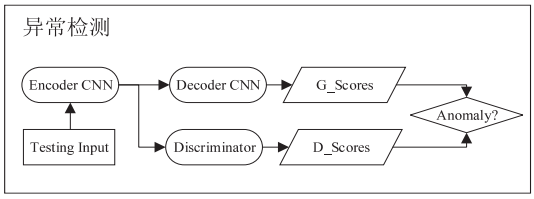

图 2 AAE-AD 模型的异常检测

在异常检测中,AAE-AD 模型的判断依据是测试样本是否符合正常模式。自编码器通过训练学习到了样本空间 X 到特征空间 Z 的投射函数 $q_\varphi(z \mid x)$ 和特征空间 Z 到样本空间 X 的投射函数 $h_\varphi(x \mid z)$,能够对符合正常模式的样本进行很好的编解码。因此,对于正常样本来说,经过自编码器网络计算出的重构误差较小,而异常样本的重构误差较大。对抗网络经过训练,编码器 G_1 能够将符合正常分布的样本编码成能够混淆鉴别器 D 的特征向量,鉴别器 D 也往往认为这是“真的”;而异常样本难以被很好地编码,其编码出的特征向量会被鉴别器 D 判为“假的”。结合这两者给出的结果计算测试样本的异常分值,如果异常分值大于设定的阈值则被判为异常。

异常检测过程如以下伪代码表示:

算法 3:AAE 的异常检测。

输入:测试样本集 X;

输出:测试样本异常分值 S。

1:对测试样本集 X 进行预处理,产生输入样本 $\{x_1, x_2, \cdots, x_n\}$

2:for the i^{th} sample do

3:将 x_i 输入自编码器网络,输出 $G_2(G_1(x_i))$,计算 $s_1 = \text{mse}(x_i, G_2(G_1(x_i)))$

4:将 x_i 输入对抗网络,输出 $D(G_1(x_i))$,记为 $s_2 = \log(1 - D(G_1(x_i)))$

5:计算样本 x_i 的总异常分值 $s = \lambda s_1 + (1 - \lambda)s_2$

6:end for

3 实验验证

3.1 实验数据集

实验数据集选自 2018 年 AIOps 的 KPI 异常检测竞赛中的 8 组 KPI 数据。网络监测设备的数据采样间隔单位是分钟,这 8 组数据的异常点已经由专业网络管理人员标出,因此这 8 组数据可以在实验中用来比较不同算法间的性能。表 1 中列出了各组数据的检测点数量、异常点数量和缺失点数量,其中 F,G,H 三组数据不包含缺失点。

表 1 实验数据集

数据集	检测点总量	异常点数量	缺失点数量
A	216 000	16 113	1 116
B	131 795	7 396	2 923
C	131 795	6 822	3 011
D	131 785	105	2 998
E	131 795	8 222	2 749
F	17 568	209	0
G	17 568	103	0
H	17 568	67	0

3.2 评价指标

F_1 分数是一种用来衡量分类模型性能的指标,兼顾了分类模型的精确率(precision)和召回率(recall),计算公式如下:

$$F_1 = 2 * \frac{\text{precision} * \text{recall}}{\text{precision} + \text{recall}} \tag{6}$$

F_1 分数值越大表明分类性能越好,最优 F_1 分数指的是取不同分类阈值时,数值最大的 F_1 分数。

ROC 曲线是根据一系列不同分类阈值,以真正例率(true positive rate,TPR)为纵坐标,假正例率(false positive rate,FPR)为横坐标绘制的曲线。AUC(area under curve)为 ROC 曲线下面积,AUC 越大代表分类模型效果越好。

在实验中,异常检测的单位是窗口,每个窗口用该窗口中最后一个点作为记录点。数据集中已经给出真实的异常点,记包含异常点或者丢失点的窗口为“真实异常窗口”。预测结束以后,记异常分值大于阈值或者包含丢失点的窗口为“预测异常窗口”。通过改变异常判断的阈值,可以计算出最优 F_1 分数并且绘制出 ROC 曲线,进而计算出 AUC 值。

3.3 实验参数设置

把每一个数据集都划分为三部分,前 50% 用于训练,中间 30% 用于验证模型损失,后 20% 用于异常检测。K 代表了模型的特征空间维度,在训练中也是一个

重要的参数。K 取值太小会导致不同维度之间的相关性太高,特征空间的表示能力会变差,同时模型的训练也更容易过拟合。在经过反复的实验后,选取 $K=10$。滑动窗口是训练和检测的基本单位,窗口长度 W 设置太大会增加过拟合的风险,设置过小会导致模型难以学习到数据的正常分布模式,在反复的实验中发现窗口大小 W 设置 120 较为合适。异常检测中,异常分值由自编码器和鉴别器的输出共同决定,设置 λ 为 0.8,这也是在反复实验中获得的经验值,λ 如何取值能够使得模型性能最佳也是后续的一项工作。

3.4　神经网络设置

模型分为三个子网络,分别是编码器网络、解码器网络、鉴别器网络。编码器网络中使用了 4 层神经网络,第一层为包含 144 个节点的全连接网络;第二层为通道数 32,5 * 5 卷积核的卷积层,使用 LeakyReLU 做激活;第三层为通道数 64,5 * 5 卷积核的卷积层,使用 LeakyReLU 做激活;第四层为节点数 $2K$(K 为特征维度)的全连接层。编码器输出为特征向量 z 的均值和标准差,使用重参数化技巧采样出特征向量 z,分别作为解码器和鉴别器的输入。解码器使用 4 层神经网络,第一层为包含 576 个节点的全连接层;第二层为通道数 64,5 * 5 卷积核的反卷积层,使用 LeakyReLU 做激活;第三层为通道数为 32,5 * 5 卷积核的反卷积层,使用 LeakyReLU 做激活;第四层为节点数为 W 的全连接层。鉴别器使用三层全连接网络,节点数分别为 128,128,1。优化器选择上,三个网络都使用了 Adam 优化器。

3.5　结果分析

3.5.1　模型间性能对比

如表 2 所示,在最优 F 分数指标上,AAE-AD 模型("0"值填充)在数据集 A,B,C,E,F,G,H 上都优于其他的无监督检测模型,性能提升分别为 3.31%,14.06%,14.48%,13.58%,112.67%,356.19%,454.34%。可以看到,在 F,G,H 数据集上,异常点比较少,对于模型检测的精确度要求非常高,其他无监督算法的 F 分数普遍在 0.2 以下,效果非常不理想;而 AAE-AD 在这几个数据集上依然能保持良好的检测精度。在数据集 D 上,RNN,LSTM 模型性能超过了其他的无监督模型,F 分数分别为 0.966 和 0.936。除了 AAE-AD 之外,VAE 的性能在 A,B,C,E 数据集上普遍优于其他无监督模型,总体来说是一种次优的方案。ARIMA 优点是不需要训练模型,能达到一定的精度,可见在对精确度要求不是很严格的应用场景中,可以采用 ARIMA 模型。

表 2　最优 F 分数指标对比

模型	A	B	C	D	E	F	G	H
ARIMA	0.703	0.644	0.645	0.925	0.462	0.221	0.098	0.100
RNN	0.746	0.813	0.812	0.966	0.371	0.179	0.194	0.138
LSTM	0.747	0.813	0.809	0.936	0.451	0.179	0.156	0.173
GAN	0.748	0.858	0.555	0.832	0.303	0.192	0.114	0.145
VAE	0.785	0.868	0.863	0.832	0.854	0.174	0.118	0.147
AAE	0.811	0.990	0.988	0.913	0.970	0.470	0.885	0.959
KNN-AAE	0.811	0.983	0.990	0.941	0.989			

如表 3 所示,在 AUC 指标上,AAE-AD 模型("0"值填充)在 B,C,E,F,G,H 数据集上都优于其他无监督检测模型,性能提升分别为 3.21%,2.78%,1.43%,59.09%,50%,64.29%。在数据集 A 上,GAN 模型表现最佳,AUC 值为 0.844;在数据集 D 上,RNN 和 LSTM 模型超过了其他方法,AUC 值分别为 0.978 和 0.970。与最优 F 指标类似,VAE 仅次于 AAE 方法。

表 3　AUC 指标对比

模型	A	B	C	D	E	F	G	H
ARIMA	0.760	0.724	0.683	0.939	0.567	0.528	0.528	0.451
RNN	0.804	0.861	0.868	0.978	0.620	0.514	0.656	0.496
LSTM	0.799	0.851	0.857	0.970	0.600	0.481	0.590	0.602
GAN	0.844	0.845	0.812	0.875	0.605	0.477	0.382	0.453
VAE	0.843	0.967	0.972	0.844	0.982	0.473	0.603	0.564
AAE	0.826	0.998	0.999	0.956	0.996	0.840	0.984	0.989
KNN-AAE	0.826	0.992	0.999	0.980	0.996			

3.5.2 KNN 填充与“0 值填充”

因为数据集 F,G,H 不包含缺失值,所以仅在 A ~ E 数据集上对比了 KNN 填充与“0”值填充的性能差异。在最优 F 指标上,KNN 填充方法在 C,D,E 三个数据集上提升了检测精度,在数据集 A 上没有变化,在数据集 B 上降了 0.71% 的精度;在 AUC 指标上,KNN 填充方法在数据集 D 上提升了 2.51% 精度,在数据集 B 上降了 0.60% 的精度,其他三个数据集不变。由此,可以发现,KNN 填充方法可以在一定程度上提高 AAE-AD 模型的检测精度,是一种有效的缺失值填充方法。

3.5.3 AAE 与 VAE 性能差异分析

AAE 模型与 VAE 模型在模型训练中存在一定的相似性。其中 AAE 通过对抗训练的方式来约束特征空间的向量分布;而 VAE 通过 KL 散度的约束来实现这一点。在图像分类任务中,VAE 的特征空间分布存在空隙[3],而 AAE 的特征空间结合非常紧密;在本实验中也发现了类似的现象。为了使特征空间更直观可见,将特征维度设为 2,在其他训练参数相同的情况下,两者的特征空间如图 3 所示。

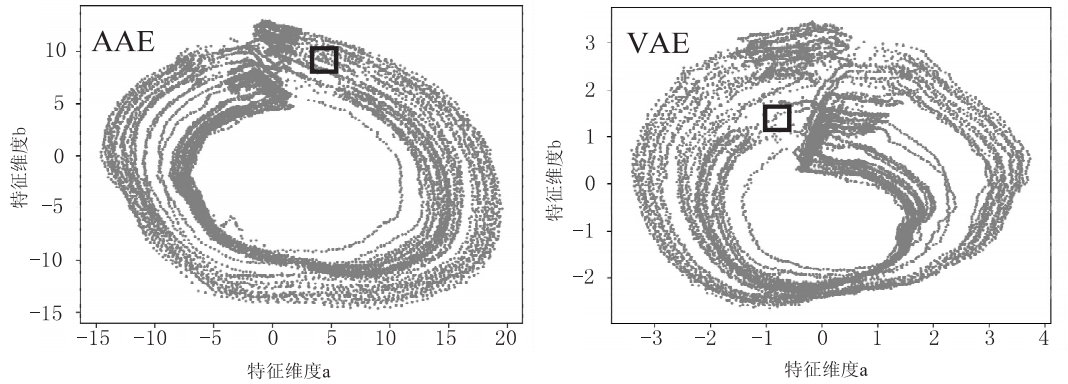

图 3 AAE 与 VAE 特征空间对比

其中两图中黑框区域为相同时间区域对应的特征空间,AAE 中此区域点分布密集而均匀,而 VAE 在此区域的分布较为零散;采样了其中的一个点,分别用 AAE 和 VAE 进行编码解码,结果如图 4 所示。可见,在特征空间离散区域,VAE 对样本的重构效果并不好,容易把正常点判成异常点,从而影响整体的检测精度,这也是 VAE 检测性能低于 AAE 的主要原因。

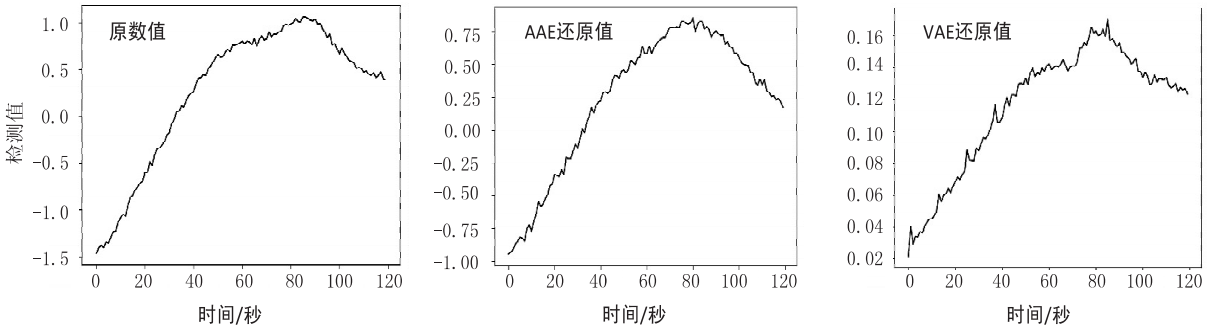

图 4 AAE 与 VAE 重构效果对比

4 结束语

针对网络性能异常发现任务中检测精度不够高的问题,提出了 AAE-AD 模型,其中使用了 KNN 作为缺失值填充的方法。实验结果表明,AAE-AD 模型在异常发现任务中性能普遍优于现有的其他无监督检测模型;其中 KNN 缺失值填充技术能进一步提升 AAE-AD 的性能。

后续工作包括两方面,一是 AAE-AD 模型对参数敏感,如窗口大小 W,特征空间维度 K,异常分数计算系数 λ,需要进一步探讨参数变化和模型性能的定性关系来提高模型训练的效率;二是尝试将 AAE-AD 模型运用在多维时序序列异常检测中,以提升它的实用性。

参考文献:

[1] LIU D,ZHAO Y,XU H,et al. Opprentice:towards practical and automatic anomaly detection through machine learning [C]//Proceedings of the 2015 internet measurement conference. Tokyo,Japan:ACM,2015:211-224.

[2] LAPTEV N,AMIZADEH S,FLINT I. Generic and scalable framework for automated time - series anomaly detection [C]//Proceedings of the 21th ACM SIGKDD international conference on knowledge discovery and data mining. Sydney,NSW,Australia:ACM,2015:1929-1947.

[3] MAKHZANI A, SHLENS J, JAITLY N, et al. Adversarial autoencoders[C]//International conference on learning representations. San Juan, Puerto Rico: [s. n.], 2016.

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

[5] AHMED M, MAHMOOD A N, HU J. A survey of network anomaly detection techniques [J]. Journal of Network and Computer Applications, 2015, 60: 19-31.

[6] VANERIO J, CASAS P. Ensemble-learning approaches for network security and anomaly detection[C]//Proceedings of the workshop on big data analytics and machine learning for data communication networks. Los Angeles: ACM, 2017: 1-6.

[7] 熊志斌. 基于 ARIMA 与神经网络集成的 GDP 时间序列预测研究[J]. 数理统计与管理, 2011, 30(2): 306-314.

[8] 孙建树, 娄渊胜, 陈裕俊. 基于 ARIMA-SVR 的水文时间序列异常值检测[J]. 计算机与数字工程, 2018, 46(2): 225-230.

[9] 张金磊. 时间序列数据异常检测及预测应用研究[D]. 桂林: 广西师范大学, 2019.

[10] 李　洁, 林永峰. 基于多时间尺度 RNN 的时序数据预测[J]. 计算机应用与软件, 2018, 35(7): 33-37.

[11] 仇　媛, 常相茂, 仇　倩, 等. 基于长短期记忆网络和滑动窗口的流数据异常检测方法[J]. 计算机应用, 2020, 40(5): 1335-1339.

[12] KINGMA D P, WELLING M. Auto-encoding variational Bayes[C]//International conference on learning representations. [s. l.]: [s. n.], 2014.

[13] SOELCH M, BAYER J, LUDERSDORFER M, et al. Variational inference for online anomaly detection in high dimensional time series[C]//International conference on learning representations. [s. l.]: [s. n.], 2016.

[14] REZENDE D J, MOHAMED S, WIERSTRA D. Stochastic backpropagation and approximate inference in deep generative models[C]//Proceedings of the 31st international conference on machine learning research. Beijing: PMLR, 2014: 1278-1286.

[15] GOODFELLOW I J, POUGET-ABADIE J, MIRZA M, et al. Generative adversarial networks[C]//Neural information processing systems. Montreal: NIPS, 2014: 2672-2680.

[16] 刘晓明. 基于深度变分学习的异常检测模型研究[D]. 保定: 河北大学, 2020.

[17] 余广民, 林金堂, 姚剑敏, 等. 基于 GAN 网络的异常检测算法研究[J]. 广播电视网络, 2020(4): 101-107.

[18] 雷　正. 基于生成式模型的视频异常场景检测研究与实现[D]. 北京: 北京邮电大学, 2019.

[19] GOU J, DU L, ZHANG Y, et al. A new distance-weighted k-nearest neighbor classifier [J]. Journal of Information and Computational Science, 2012, 9(6): 1429-1436.

[20] SALIMANS T, GOODFELLOW I J, ZAREMBA W, et al. Improved techniques for training GANs[C]//Advances in neural information processing systems, Barcelona: NIPS, 2016: 2234-2242.

[21] KINGMA D, BA J. Adam: a method for stochastic optimization[C]//International conference on learning representations. San Diego, CA: NIPS, 2015.