一种基于 LSTM 自动编码机的工业系统异常检测方法

沈潇军[1]，葛亚男[2]，沈志豪[1]，倪阳旦[1]，吕明琪[2]，翁正秋[3]
（1. 国网浙江省电力有限公司，浙江 杭州 310007；2. 浙江工业大学，浙江 杭州 310023；
3. 温州职业技术学院，浙江 温州 325035）

摘　要：在工业互联网的环境下，自动有效的异常检测方法对工业系统的安全、稳定生产具有重要的意义。传统的异常检测方法存在需要大量标注样本、不适应高维度时序数据等不足，提出一种基于 LSTM 自动编码机的工业系统异常检测方法。为克服现有方法依赖标注样本的不足，提出采用自动编码机，通过无监督的方式学习大量正常样本的特征和模式，在此基础上通过对样本进行重构和计算重构误差的方式进行异常检测。其次，为克服现有方法不适应高维度时序数据的不足，提出采用双向 LSTM 作为编码器，进而挖掘多维时序数据的潜在特征。基于一个真实造纸工业的数据集的实验表明，所提方法在各项指标上都对现有无监督异常检测方法有一定的提升，检测的总体精度达到了 93.4%。

关键词：异常检测；工业互联网；自动编码机；LSTM
中图分类号：TN929. 5
文献标识码：A
doi: 10.11959/j.issn.1000–0801.2020188

An LSTM auto-encoder based anomaly detection for industrial system

SHEN Xiaojun[1] ,GE Yanan[2], SHEN Zhihao[1], NI Yangdan[1], LV Mingqi[2], WENG Zhengqiu[3]
1. State Grid Zhejiang Electric Power Company, Hangzhou 310007, China
2. Zhejiang University of Technology, Hangzhou 310023, China
3. Wenzhou Polytechnics, Wenzhou 325035, China

Abstract: In the context of the industrial internet, automatic and effective anomaly detection methods are of great significance to the safe and stable production of industrial systems. Traditional anomaly detection methods have the disadvantages of requiring a large number of labeled samples, and not adapting to high-dimensional time series data. Aiming at these limitations, an industrial system anomaly detection method based on LSTM (long short-term memory)

收稿日期：2020–03–10；**修回日期**：2020–06–23
通信作者：翁正秋，derisweng@163.com
基金项目：国家自然科学基金资助项目（No.U1936215）；浙江省自然科学基金资助项目（No.LY18F020033）；工业和信息化部 2019 年工业互联网创新发展工程（No.TC190H3WN）；温州市 551 人才工程科研项目（温人社发〔2020〕61 号（No.5），温人社发〔2019〕55 号（No.17））；温州职业技术学院重大科研课题（No.WZY2020001）
Foundation Items: The National Natural Science Foundation of China (No. U1936215) ,The Natural Science Foundation of Zhejiang Province of China(No. LY18F020033), 2019 Industrial Internet Innovation and Development Project of the Ministry of Industry and Information Technology(No.TC190H3WN),Wenzhou Scientific Research Projects for 551 Talent Engineering Project (WenRenSheFa [2020]61(No.5), WenRenSheFa [2019] 55(No.17)), Major Scientific Research Projects of Wenzhou Polytechnics (No.WZY2020001)

auto-encoder was proposed. Firstly, to address the limitation of relying on labeled samples, an encoder used to learn the features and patterns of a large number of normal samples in an unsupervised manner. Then, anomaly detection was performed via reconstructing samples and calculating the reconstruction error. Secondly, to adapt to high-dimensional time series data, a BiLSTM (bidirectional LSTM) was used as an encoder, and then the potential characteristics of multi-dimensional time series data were mined. Experiments based on a real paper industry data set which demonstrate this method has improved the existing unsupervised anomaly detection methods in various indicators, and the overall accuracy of the detection has reached 93.4%.

Key words: abnormal detection, industrial internet, auto-encoder, LSTM

1　引言

近年，随着工业互联网（industrial internet）的快速发展，现代化工业制造系统通过传感器、控制器、智能仪表等监测设备，实现了对生产运行状态、环境和过程的感知和记录，积累了大量的工业数据[1]。工业互联网旨在实现更敏锐、更高效的工业制造系统的自动化控制和资源分配，同时提高智能工厂的能源效率。然而，由于工业互联网打破了网络世界和物理世界的边界，工业制造系统更容易受到外部恶意行为的侵袭[2]。此外，工业制造系统中不可避免地存在设备故障、性能下降、质量缺陷等生产问题[3]。如果工业生产中的入侵、故障等异常情况不能被及时检测出来，将可能给整个制造体系带来严重的损失。因此，异常检测是工业互联网的基本要求，对智能制造企业具有十分重要的意义[4]。

随着机器学习技术的发展和成熟，数据驱动模型成为异常检测的主流手段。一方面工业生产是一种持续的行为，另一方面工业生产的监测设备多样化程度高，积累的工业数据是一种典型的多维时序数据，因此基于多维时序数据的异常检测受到了工业互联网领域的高度重视。然而，面向工业互联网多维时序数据的异常检测是一项十分具有挑战的任务：首先，数据的不同维度之间存在潜在关联和相互影响，导致异常模式更难以检测和识别。其次，工业大数据具有体量大、多源异构、动态性强等一系列特点[5]，导致工业大数据的处理更加困难。

为应对上述挑战，本文提出了一种基于LSTM（long short-term memory）自动编码机的无监督异常检测模型，其主要思想为：首先，利用自动编码机学习大量正常样本，通过将正常样本映射到低维隐空间以学习正常样本的主要特征。在此基础上，基于隐空间的主要特征重构样本，并通过分析重构样本和原始样本之间的差异实现异常检测。自动编码机是一种无监督学习技术，且可通过设计自动编码机的网络结构处理多维非线性数据。其次，通过结合 LSTM 网络和自动编码机，并通过滑动窗口的方式分割样本，使自动编码机能够捕获多维时序数据中的时间依赖关系。与其他的无监督方法相比，提出的方法可以处理高维度时序数据，能够较好地适应实际工业互联网环境。

2　相关工作

大量现有研究表明，基于时序数据分析的异常检测是可行的手段。例如，Kanawaday 等[6]就从安装了多种传感器的生产设备中收集时序数据，并利用这些数据预测故障、优化制造过程。

传统的异常检测方法，如 KNN[7]、局部异常因子 LOF 算法[8]、基于连通性的异常点因子 COF 算法[9]等，利用样本之间的相似度区分正常与异常数据。然而，这些方法都有计算复杂度高、漏检率高，具有不适应高维数据的局限性。

为了应对这些问题，研究者们引入了有监督

机器学习的方法。例如，Griffin 等[10]提出了一种基于神经网络和决策树的异常检测方法，用于检测多个加工过程的异常情况。Nanduri 等[11]提出了使用递归神经网络检测可能降低飞行安全系数的异常事件。Janssens[12]提出了一种基于卷积神经网络的特征学习系统，用于检测旋转机械的故障状态。通过有监督学习方法，模型可以学习正常数据和异常数据之间模式的差异，可以有效提高异常检测的准确率。任何有监督方法都不可避免地需要数据有部分或全部的标注信息。然而，在实际应用中，一个常见的困难是，历史数据完全或大部分是没有标注的，特别是在工业互联网环境下，标注的代价太高。

为了解决这个难题，研究者们提出了一些无监督的异常检测方法。例如，Amruthnath 等[13]将几种无监督的学习方法应用于异常检测，如 K 均值、模糊 C 均值聚类等。这些方法的异常检测都可以定义为识别与标准行为有偏差的行为的过程，这也是无监督异常检测最常见的检测方式。Diez-Olivan 等[14]提出了一种基于 One-Class SVM 的异常检测方法，基于样本与分离超平面的距离得到异常分数，以此来检测传感器数据中的异常。Joshi 等[15]提出了基于隐马尔科夫模型（HMM）的异常检测，该模型通过提取特征并计算模型生成的状态序列中的异常概率建立 HMM。传统的无监督异常检测方法都需要解决的一个实际但基本的问题是确定其结构，即找到调整模型参数的方法，而目前没有较好的解决这个问题的方法。Feng 等[16]提出了一种动态自回归综合移动平均线模型（DARIMA），通过对时间序列数据之间的相关性建立预测模型，对预测结果按阈值判断异常，主要应用于短期预测，能够提取出数据中的短期时序依赖关系。Serdio 等[17]提出了一种基于不断学习的模糊模型和动态残差分析的发电厂煤厂异常检测方法，使用该模型无需异常标注。Kingma[18]应用了变分自动编码器（VAE），通过重建数据，分析重建数据和源数据的残差检测异常。Lu 等[19]提出了一种堆叠自动编码机，用来检测旋转机械组件的异常情况。堆叠自动编码机基于一系列自动编码器建立，以分层方式使用深层网络架构学习。以这种方式有利于获取复杂的感官信号的高阶特征表示，并且将这种高阶特征表示作为后续故障分类器的输入。通过无监督学习模型，可以应对现实情况中数据没有标注的情况，并且有利于提高异常检测系统的实时性。然而，传统的无监督学习方法在高维时序数据上的效果不佳，而在实际工业生产过程中，得到的数据大多具有高维度、高动态的特点。

基于传统的堆叠自动编码器能够处理高维数据，但是在时序数据上的效果不佳，而 LSTM 网络能够有效提取出数据的时序特征，本文结合自动编码器和 LSTM 网络的特点，采用基于 LSTM 的自动编码器的无监督检测模型。自动编码器的网络体系结构可以处理多维非线性数据，且学习无标记数据集的正常行为。本文的方法通过结合 LSTM 网络和自动编码器，并通过滑动窗口的方式分割数据集样本，使 LSTM 单元能够捕获多变量传感器中的时间依赖关系。同时模型在 LSTM 网络中结合了 BiLSTM 网络，可以更好地利用数据中的长期依赖关系，并且相较于简单 LSTM 网络，它还能提取异常时刻前后数据对其的影响。经过实验验证，本文的方法在处理高容量、高维度、无标签，并且与时间相关的不平衡数据上有较好的效果，能够较好地适应实际工业环境。

3 异常检测模型

3.1 模型构建

在实际工业生产过程中，得到的数据大多具有高容量、高复杂、时序性的特点，并且大部分数据存在无标注或标注不全的问题，这就导致了传统的无监督方法无法有效地处理这类数据。

本文所要解决的问题就是如何检测无标注的

复杂时序数据中的异常数据。

3.2　LSTM 自动编码机

循环神经网络（RNN）是一种用于处理时序数据的深度神经网络。它将上一步的输出和当前的输入级联到一起，利用 tanh 函数控制两者的输出权重，因此可有效地从时序数据中学习特征。然而，面对长度过长的时序数据，标准的 RNN 会因为梯度消失或梯度爆炸的问题而无法捕捉长期依赖。为了学习长期依赖关系，提出了 LSTM 网络[20]。LSTM 在 RNN 的基础上改进了隐藏层单元，通过添加存储单元克服 RNN 的梯度消失问题。这些存储单元包括遗忘门、输入门、输出门，增加了对过去状态的过滤，可以选择哪些状态对当前更有影响，而不是简单地选择最近状态。

自动编码机是一种无监督的神经网络模型，它包括两个阶段：编码和解码。编码器可以通过将原始数据映射到低维空间学习到输入数据的主要特征和模式。解码器可以从低维空间重构原始输入数据。

本文结合 LSTM 网络和自动编码机，在编码器中使用两层 LSTM 用于提取时序数据的特征，在解码器中同样使用两层 LSTM 从特征中重构样本。

3.3　双向 LSTM

在时序数据中某一时刻发生的异常，不但这一时刻之前的数据会与异常存在潜在关联，更重要的是该异常会显著影响这一时刻之后的数据。因此，异常时刻的过去和未来的数据都可用于检测异常。然而，LSTM 网络只使用某一时刻之前的输入信息抽取特征。为了同时考虑异常时刻的过去和未来数据，本文使用双向 LSTM 网络作为编码器。双向 LSTM 的网络结构如图 1 所示，双向 LSTM 网络由两个独立的 LSTM 网络组成，双向 LSTM 具有两个独立的隐藏层，这两个隐藏层除了方向外，内部结构完全一致。第一层 LSTM 计算当前时间点的正向信息，第二层反向读取相同的序列，计算当前时间点的反向信息。两个隐藏层独立计算当前时间点的状态和输出，并前馈到相同的输出层，双向 LSTM 网络在当前时间点的输出由这两个隐藏层共同决定。在训练时，由于两个网络无互相作用，因此可以作为一个通用的前馈网络，其反向传播过程也与 LSTM 类似，唯一的不同是传播到输出层后，返回给两个隐藏层以不同的方向传播，完成对权重的更新。

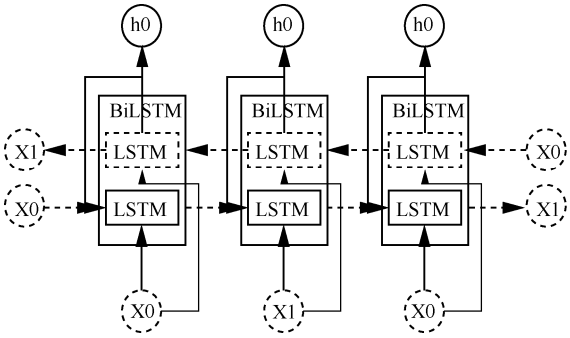


图 1　双向 LSTM 的网络结构

本文结合双向 LSTM 网络和 LSTM 网络的优点，在编码器中，标准的 LSTM 网络前增加一层双向 LSTM 网络，综合当前时间点过去和未来的信息对时间序列提取特征。由于双向 LSTM 网络会增加数据的维度，所以本文在其后接上一层 LSTM 网络对提取的特征降维，将其映射到低维空间。

值得注意的是，双向 LSTM 需要使用目标时刻未来的数据用于异常检测，这在一定程度上会降低系统的实时性（即未来一定时间内的数据获取后才能实施异常检测），因此在系统实际部署的过程中需要权衡考虑。

4　方法设计

4.1　方法概述

本文提出的异常检测方法的步骤如图 2 所示，包含如下 3 个步骤。

（1）利用滑动窗口对样本进行划分，并对其进行标准化等预处理。

（2）采用自动编码机对样本进行特征提取和

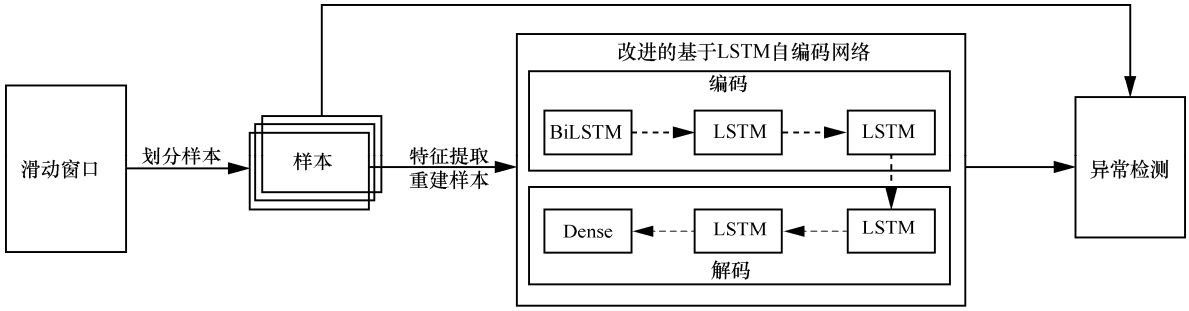


图 2　本文提出的异常检测方法的步骤

样本重构。针对样本的时序特性，自动编码机采用 LSTM 作为编码器和解码器。

（3）基于原样本和重构样本的差异进行异常检测。

4.2　数据预处理

4.2.1　滑动窗口

在实际工业环境中，由于工业设备是持续运行的，因此从工业设备传感器中采集到的数据是容量巨大的时序数据。为了分析这样的数据，异常检测模型必须一方面对时间敏感（即精确检测到异常发生的时间点），另一方面保持数据的时间关联性（即时序数据在时间轴上存在邻近性、周期性等关联）。因此，采用滑动窗口方法分割原始数据。

对于原始数据 $X=\{I\times F\}$，I 是数据容量，F 是数据维度，基于滑动窗口的方法主要分为 2 个步骤：首先，确定窗口宽度 W 和滑动步长 S。然后，根据窗口宽度和滑动步长将 X 划分成由多个样本组成的样本集 X'（$I'\times W\times F$）。其中，I'为划分后样本的个数。

对于基于滑动窗口的时序数据样本划分方法，窗口宽度 W 是最重要的参数。设置较大的窗口宽度可以较好地挖掘样本内部时序数据的时间依赖关系，但是会造成检测精度的下降（即异常可能只占样本的其中一小部分）。而设置较小的窗口宽度可以更好地把异常部分独立出来，但是也容易破坏时序数据的时间依赖关联，导致自动编码机难以学习到正常样本的主要特征和模式。综合考虑上述因素，基于实验探索，将窗口宽度设定为滑动步长的 1~5 倍。

4.2.2　标准化

大多情况下，不同传感器产生的数据的尺度会有很大差异，如果直接使用，容易使模型产生偏见。因此，利用 Z-score 方法对数据进行标准化操作，具体计算方法如式（1）：

$$X'=\frac{X-\bar{X}}{\sigma(X)} \tag{1}$$

其中，$\bar{X}$ 为样本的平均值，$\sigma(\cdot)$ 为样本的标准差。该操作就是通过计算样本的均值和标准差，对每个特征进行居中和缩放，使每个变量在每个窗口中均值为 0，标准差为 1，将不同维度的数据变换到同一尺度。

4.3　特征学习

得到样本集后，接下来需要建立模型对样本集进行学习。然而，在无监督的条件下，模型缺少学习的目标。针对此问题，自动编码机将模型的学习目标设置为样本本身，并通过将样本映射到一个维度较低的特征空间以学习样本的主要特征和模式，则学习过后的模型可基于主要特征将样本重构出来。其中，将样本映射到低维特征空间的模块为编码器，而基于主要特征重构样本的模块为解码器。

基于 LSTM 的自动编码机网络结构如图 3 所示，为适应工业数据的时序特性，提出了一种基于 LSTM 的自动编码机，其本质上是一个深度神经网络，包括编码器和解码器两部分。其中，编码器融合了双向 LSTM 网络，RepeatVector 层和

Dense（全连接）层是为了使重建样本与原样本具有同样的维度。其中，RepeatVector 层的原理是将输入重复若干次后输出。

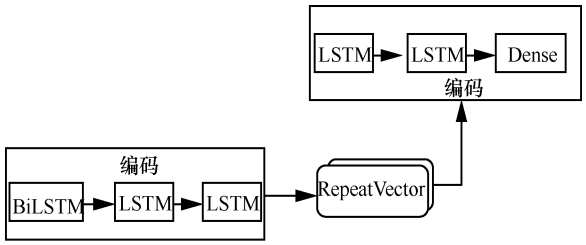


图 3　基于 LSTM 的自动编码机网络结构

4.4　异常检测模块

自动编码机在对编码后的特征进行解码重构样本的过程中，会产生误差。训练自动编码机的原理是使用反向传播的方式最小化重构误差。在训练阶段，向自动编码机中输入正常数据，自动编码机通过减小重构样本和原始样本的均方误差学习正常数据的隐含特征和模式。所以在测试阶段，正常样本的重构误差比较小，而异常样本的重构误差比较大（由于模型没有学习到异常样本的隐含特征和模式）。因此，本文将重构误差作为该样本的异常分数。

异常检测算法的步骤如图 4 所示。首先，由于每个原始样本都被表示为一个 $W\times F$ 的矩阵（W 为窗口宽度，F 为时序数据维度），则重构样本也可表示为一个 $W\times F$ 的矩阵。然后，当 W 较大时，窗口可能包含多个时刻，不同时刻可能存在异常标注冲突（即窗口中某些时刻可能被标注为异常，而某些时刻可能被标注为正常），因此本文取样本中心时刻的标注作为样本的标注。为适应这个设置，取原始样本和重构样本的中心时刻向量，并计算这两个向量的均方误差作为异常分数。最后，若异常分数超过预先设定的阈值，则判定该样本发生了异常。

5　实验结果与分析

5.1　数据集

本文基于一个来自工业造纸流水线的真实数据集[21]进行实验。造纸是一个连续的工业生产过程，在这个过程中有可能发生各种异常（如纸张断裂）。

数据集包含从生产线上多个传感器采集到的数据，采集频率为 0.5 Hz。因此，采集到的传感器数据是一个多维时序数据，包含 18 398 个采样。此外，数据集提供了异常事件的标注信息，包含 124 个时刻被标注了异常。数据的字段具体如下。

- t：时间戳，代表数据的采集时间。
- y：数据标注，$y=1$ 代表异常，$y=0$ 代表正常。数据标注针对每个单独的采样，而多个连续的标注均为 $y=1$ 代表异常持续一定时间。
- x_1~x_{61}：是特征变量，代表从不同传感器中采集到的读数，包括设备状态（如转速、

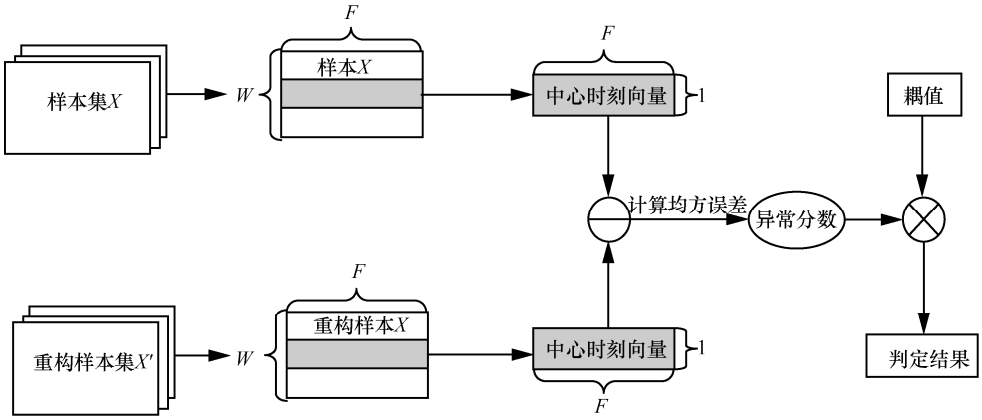


图 4　异常检测算法的步骤

真空度等）和材料状态（如纸浆纤维指标、化学品数量等）。其中，x_{28} 和 x_{61} 只用于标注生产的纸张类型，与生产过程无关，在实验过程中删掉这两个特征变量。

5.2 评价指标

由于对异常检测而言，异常事件的识别率和误判率是其关注的重点，所以本文使用如下的指标来评判模型的优劣。

（1）异常事件的识别率：

$$\mathrm{TPR}=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \tag{2}$$

（2）正常情况的识别率：

$$\mathrm{TNR}=\frac{\mathrm{TN}}{\mathrm{FP}+\mathrm{TN}} \tag{3}$$

（3）异常事件的误判率：

$$\mathrm{FPR}=\frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}} \tag{4}$$

（4）总体精度：

$$\mathrm{Accuracy}=\frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{FP}+\mathrm{TN}+\mathrm{FN}} \tag{5}$$

其中，TP 为异常事件被准确识别，FP 为正常情况被判断为异常事件，TN 为正常情况被准确识别，FN 为异常事件被误判成正常情况。

在二分类问题中，ROC（receiver operating characteristic）曲线和 AUC（area under the curve）值常被用来评价一个二值分类器（binary classifier）的优劣。

（1）ROC 曲线

ROC 曲线是以 FPR 为横轴，以 TPR 为纵轴，随阈值的移动而形成的一条连续曲线。

（2）AUC

AUC 值代表 ROC 曲线下的面积，介于 0.1 和 1 之间。AUC 数值可以直观的评价模型的好坏，值越大越好。

5.3 建模训练及测试实验

首先，基于对数据集中异常标注的分析，发现异常事件的持续时间基本在 4 s 以内（即异常事件一般覆盖不超过 2 个采样）。因此，设置滑动窗口的窗口宽度 W 为 5，这个数值可以确保在异常样本的窗口宽度内可以包含整个异常事件。

然后，本文设置滑动步长 S 为 1，对数据 X 进行样本划分，得到样本集 X'（$I'\times W\times F$），I' 为划分后的样本个数，W 为窗口宽度（W = 5），F 是样本特征的维度（F=59）。最后，对样本进行训练集、验证集、测试集的划分。训练集、验证集和测试集中样本数量的分布见表 1。

表 1 样本数量分布

标签类型	训练集	验证集	测试集
正常（y=0）	11 692	2 926	3 650
异常（y=1）	0	17	29

本文的 LSTM 自动编码机的各层参数见表 2，前 3 层为编码器，后 3 层为解码器（结构如图 2 所示）。BiLSTM 层包含 2 个 LSTM 隐藏层，每个 LSTM 层的单元数量为 32，输出层级联两个 LSTM 层的输出，所以得到的输出维度为 64。第三层 LSTM 输出的是最后的隐藏层状态而不是全部序列状态，其维度为（1，16），因此为了使其和原样本具有一致的时间维度，在其后加上了一个 RepeatVector 层，重复 5 次最后的隐层状态，RepeatVector 层的输出维度为（5，16）。

表 2 LSTM 自动编码机各层参数

网络层		单元数	输出维度	参数个数/个
编码器	BiLSTM	32	（5，64）	23 552
	LSTM	32	（5，32）	12 416
	LSTM	16	（1，16）	3 136
	RepeatVector	—	（5，16）	0
解码器	LSTM	16	（5，16）	2 112
	LSTM	32	（5，32）	6 272
	Dense	59	（5，59）	1 947

在实验中还有一个重要参数就是阈值，通过 GridSearch 实验发现阈值为 0.3 时模型性能最佳。此外，本文选择均方误差（mean squared error，MSE）作为 LSTM 自编码器的损失函数，并采用 Adam 优化器来更新网络参数，从而最小化损失函数。

对本文提出方法的实验的部分结果如图 5、图 6 和图 7 所示。其中，图 5 显示了重构正常样本和重构异常样本的均方误差分布。可以看出，异常样本和正常样本的重构误差是有一定区分度的。异常样本的重构误差普遍较大。图 6 展示了本文提出的方法的检测结果的混淆矩阵。可以看出，本文提出的方法的异常检测的准确率 TPR 为 55.2%，总体精度 ACC 为 93.4%。图 7 展示了本文提出的方法的 ROC 曲线，其 AUC 值达到 88.9%。

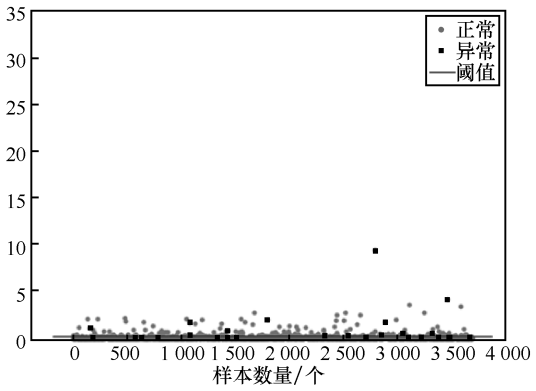


图 5　重构正常样本和重构异常样本的均方误差分布

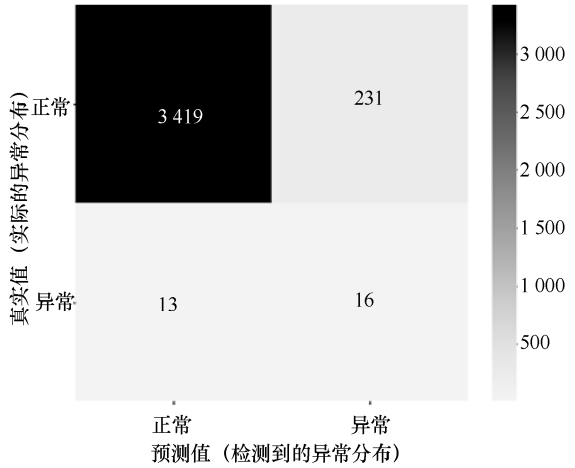


图 6　本文提出的方法的检测结果的混淆矩阵

本文提出的方法（称为 BiLSTM-AE）是一种面向时序数据的无监督异常检测方法。因此，将其与现有的无监督异常检测基线方法进行对比，包括基于距离度量的异常检测方法 OC-SVM、基于模型融合的异常检测方法 iForest、现有基于自动编码机的异常检测方法 LSTM-AE。基线方法具体描述如下。

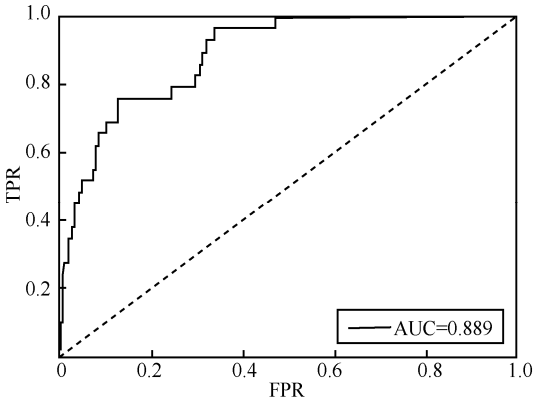


图 7　本文提出的方法的 ROC 曲线

- OC-SVM：OC-SVM[22]是通过从训练集学习一个能将正常样本划分且与零点最远的超平面来检测异常。检测时，在超平面内的样本为正常样本，在超平面外的样本为异常样本。需要注意的是，OC-SVM 检测得到的是二进制的检测结果而不是概率分数，所以 OC-SVM 方法无法画出 ROC 曲线。
- iForest：iForest[23]的算法思想是重复从不同的维度对数据集进行切分。与正常数据相比，异常数据只需要更少的切分次数就可以被分离出来。若样本的切分次数低于阈值，则为异常样本。
- LSTM-AE：LSTM-AE[24]是在编码器中使用 LSTM 用于提取时序数据的特征，在解码器中同样使用 LSTM 从特征中重构样本。模型通过比较重构误差检测异常。

实验结果见表 3。可以看出，BiLSTM-AE 明显优于 OC-SVM，而与 iForest 比较，BiLSTM-AE 虽然在总体精度上略优于 iForest，但是在异常的

识别率和AUC值上要明显优于iForest。LSTM-AE虽然在异常识别率和AUC值上优于OC-SVM和iForest，但同时误判率也有增高，导致ACC略有下降。BiLSTM-AE通过引入双向LSTM网络改进了LSTM-AE，因此BiLSTM-AE较LSTM-AE在TPR、ACC、AUC 3个指标上都有提高。这说明本方法能更好地发现高容量、高维度的时序数据中的潜在特征和模式，因此更容易发现潜在的异常。

表3 不同方法的异常检测结果对比

模型	TPR	ACC	AUC
BiLSTM-AE	55.2%	93.4%	88.9%
iForest	31%	92.7%	72.1%
OC-SVM	24.1%	92.4%	-
LSTM-AE	48%	90.4%	81%

6 结束语

为应对工业系统对自动故障检测的需求，本文提出了一种基于LSTM自动编码机的无监督异常检测方法。本方法采用“双向LSTM+自动编码机”的架构，实现了对工控系统的异常检测。其中，双向LSTM可有效捕捉高维时序数据的特征，提高了异常检测的准确度；自动编码机可自动学习正常数据的模式，实现了无监督的异常检测。基于真实工控数据的实验，表明本方法在对实际工业环境产生的高维度时序数据的异常检测上有良好的效果，模型对异常样本和正常样本的最终分类准确率达到了93.4%，并在各项指标上优于现有无监督异常检测方法。

参考文献：

[1] ZHOU L Y, GUO H Q. Anomaly detection methods for IoT Networks[C]//Proceedings of 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI). Piscataway: IEEE Press, 2018: 214-219.

[2] GENGE B, PIROSKA H, CALIN E. Anomaly detection in aging industrial internet of things[J]. IEEE Access, 2019(99): 1.

[3] WONG T, LUO Z. Recurrent auto-encoder model for large-scale industrial sensor signal analysis[C]//Proceedings of International Conference on Engineering Applications of Neural Networks. Berlin: Springer, 2018: 203-216

[4] HUANG H K. Real-time fault-detection for IoT facilities using GBRBM-based DNN[J]. IEEE Internet of Things Journal, 2019(10): 1-1.

[5] RIEGER T. Fast predictive maintenance in industrial internet of things (IIoT) with deep learning (DL): a review[C]//Proceedings of 2019 Collaborative European Research Conference (CERC2019). [S.l.:s.n.], 2019: 69-79.

[6] KANAWADAY A , SANE A. Machine learning for predictive maintenance of industrial machines using IoT sensor data[C]//Proceedings of 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS). Piscataway: IEEE Press, 2017: 107-110.

[7] ABU A, HANEEN A. Effects of distance measure choice on *K*-nearest neighbor classifier performance: a review[J]. Big Data, 2019(7): 221-248.

[8] BREUNING M. LOF: identifying density-based local outliers[C]//Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data. New York: ACM Press，2000, 29(2): 93-104.

[9] TANG J. Enhancing effectiveness of outlier detections for low density patterns[C]//Proceedings of Pacific-Asia Conference on Knowledge Discovery and Data Mining. Berlin: Springer, 2002.

[10] GRIFFIN J M, DOBERTI A J, VALBORT H, et al. Multiple classification of the force and acceleration signals extracted during multiple machine processes: part 1 intelligent classification from an anomaly perspective[J]. International Journal of Advanced Manufacturing Technology, 2017(93): 1-13.

[11] NANDURI A, SHERRY L. Anomaly detection in aircraft data using recurrent neural networks (RNN)[C]//Proceedings of 2016 Integrated Communications Navigation and Surveillance (ICNS). Piscataway: IEEE Press, 2016.

[12] JANSSENS O. Convolutional neural network based fault detection for rotating machinery[J]. Journal of Sound and Vibration, 2016(377): 331-345.

[13] AMRUTHNATH N, TARUN G. A research study on unsupervised machine learning algorithms for early fault detection in predictive maintenance[C]//Proceedings of 2018 5th International Conference on Industrial Engineering and Applications (ICIEA). Piscataway: IEEE Press, 2018: 355-361.

[14] DIEZ-OLIVAN A, RUBIO J A P. Kernel-based support vector machines for automated health status assessment in monitoring sensor data[J]. The International Journal of Advanced Manufacturing Technology, 2018, 95(1-4): 327-340.

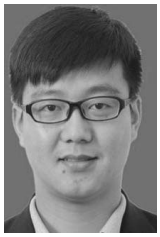
[15] JOSHI S, PHOHA V. Investigating hidden Markov models

capabilities in anomaly detection[C]//Proceedings of the 43rd Annual Southeast Regional Conference. New York: ACM Press, 2005: 98-103.
[16] FENG T Z, DU Z H, SUN Y K, et al. Real-time anomaly detection of short-time-scale gwac survey light curves[C]//Proceedings of 2017 IEEE International Congress on Big Data (BigData Congress). Piscataway: IEEE Press, 2017: 224-231.
[17] SERDIO F, LUGHOFER E, PICHLER K, et al. Residual-based fault detection using soft computing techniques for condition monitoring at rolling mills[J]. Information Sciences, 2014(259): 304-320.
[18] KINGMA D P. Auto-encoding variational bayes[J]. arXiv: 1312.6114. 2013.
[19] LU C, WANG Z Y, QIN W L, et al. Fault diagnosis of rotary machinery components using a stacked denoising autoencoder-based health state identification[J]. Signal Processing, 2016(130): 377-388.
[20] HOCHREITER S, SCHMIDHUBER J. Long short-term memory[J]. Neural computation, 1997(9): 1735-1780.
[21] RANJAN C. Dataset: rare event classification in multivariate time series[J]. arXiv: 1809.10717. 2018.
[22] SCHOLKOPF B, WILLIAMSONET R, et al. Support vector method for novelty detection[C]//Proceedings of the 12th International Conference on Neural Information Processing Systems. Cambridge: MIT Press,1999: 582-588.
[23] LIU F T, TING K M, ZHOU Z H. Isolation-based anomaly detection[J]. ACM Transactions on Knowledge Discovery from Data (TKDD), 2012, 6(1): 1-39.
[24] MALHOTRA P. LSTM-based encoder-decoder for multi-sensor anomaly detection[J]. arXiv: 1607. 00148. 2016.

[作者简介]

沈潇军（1975– ），男，国网浙江省电力有限公司高级工程师，主要研究方向为电力信息化技术及信息管理。

葛亚男（1994– ），女，浙江工业大学研究生，主要研究方向为网络安全。



沈志豪（1986– ），男，国网浙江省电力有限公司高级工程师，主要研究方向为电力系统信息化运维。

倪阳旦（1986– ），男，国网浙江省电力有限公司高级工程师，主要研究方向为电力信息技术。

吕明琪（1981– ），男，浙江工业大学副教授，主要研究方向为网络安全、移动安全、系统安全。

翁正秋（1981– ），女，温州职业技术学院副教授，主要研究方向为数据安全与大数据技术。