基于SAE-LSTM的工艺数据异常检测方法

尚文利[1],石 贺[2,3,4],赵剑明[2,3,4],曾 鹏[2,3,4]
(1. 广州大学电子与通信工程学院,广东广州 510006;2. 中国科学院沈阳自动化研究所,辽宁沈阳 110016;
3. 中国科学院大学,北京 100039;4. 中科院网络化控制系统重点实验室,辽宁沈阳 110016)

摘 要: 为解决工业网络安全防护中工艺数据异常检测误报率较高的问题,本文提出一种基于时间序列的异常检测方法.该方法对工艺数据进行相关性分析、向量映射等处理,再采用堆叠自编码神经网络(SAE)对工艺数据特征进行降维,根据工艺数据在传输序列间的相互关联性,设计基于长短期记忆神经网络(LSTM)的异常检测模型,最后进行工艺数据异常检测仿真实验验证分析.实验结果表明,基于时间序列的异常检测模型能有效提高工艺数据异常检测准确率,并且误报率要低于传统隐马尔可夫异常检测模型,同时获得较好的异常检测实时性.

关键词: 工业控制系统; 工控异常检测; 自编码神经网络; 长短期记忆神经网络
中图分类号: TP393.08;TP39 **文献标识码:** A **文章编号:** 0372-2112(2021)08-1561-08
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.12263/DZXB.20180015

An Anomaly Detection Method of Process Data Based on SAE-LSTM

SHANG Wen-li[1],SHI He[2,3,4],ZHAO Jian-ming[2,3,4],ZENG Peng[2,3,4]
(1. *School of Electronic and Communication Engineering, Guangzhou University, Guangzhou, Guangdong* 510006, *China*;
2. *Shenyang Institute of Automation, Chinese Academy of Science, Shenyang, Liaoning* 110016, *China*;
3. *University of Chinese Academy of Sciences, Beijing* 100039, *China*;
4. *Key Laboratory of Networked Control System, CAS , Shenyang, Liaoning* 110016, *China*)

Abstract: In order to solve the problem of high false alarm rate of abnormal detection of process data in industrial network security protection, this paper proposes an anomaly detection method based on time series. In this method, the process data is analyzed by association analysis and vector mapping, and the stacked auto-encoder neural network (SAE) is used to reduce the dimension of process data features. According to the correlation of process data in the transmission sequence, an anomaly detection model based on long and short term memory neural network (LSTM) is designed. Finally, the simulation analysis of abnormal detection of process data is carried out. The experimental results show that the anomaly detection model based on time series can greatly improve the accuracy of process data anomaly detection, and the false positive rate is lower than the traditional hidden Markov anomaly detection model, and at the same time get better real-time performance of anomaly detection.

Key words: industrial control system; industrial control anomaly detection system; auto-encoder neural network; long and short term memory neural network

1 引言

目前我国的工业控制系统已经广泛用于电力、水处理、石油化工、轨道交通、制造业等国计民生行业.早期的传统工业控制系统大部分以车间或厂区为单位,相互的车间在数据传输间是相对独立的,每个车间或厂区有各自独立的网络,数据间的传输和处理由审计员来完成,在小型企业所有厂区建立一套统一的局域网[1].但随着近几年工控网络的快速发展,IT办公网与工业控制网络深度融合,工业控制系统已经由传统的封闭、稳定的环境,变得更加开放、复杂.工业控制协议种类比传统IT行业更为多样,在物理层有RS232、RS485、Ethernet,数据链路层有CAN、ProfiBus等,应用层有ModBus和OPC等多种协议.各种木马、病毒等破坏程序也通过互联网的连接进入工业控制系统,由此

收稿日期:2018-12-29;修回日期:2021-05-31;责任编辑:郭游
基金项目:国家自然科学基金(No.61773368);之江实验室开放课题资助(No.2021KF0AB06)

工业数据安全问题受到学者的普遍关注[2~4].

异常检测作为入侵检测的一种重要手段,通过与正常行为间的匹配实现异常行为发现,无需预先了解攻击的特征形式,能有效地检测未知攻击. 异常检测系统利用的主要方法为统计学习、知识表示、机器学习,其中基于机器学习的异常检测方法能随着工业控制系统的数据积累不断地自主学习,降低入侵检测的误报率,提高检测的准确率和召回率,更适用于工业环境[5]. 目前国内外的工艺数据异常检测研究主要基于专家经验的模型构建;这些模型的构建都非常耗时,并且也不适合现在工业的工艺数据规模,对于复杂系统模型的建立,这种方法效果也不好. 基于机器学习的工业异常检测研究中国内外有使用经典支持向量机(SVM)的,如文献[6]使用SVM支持向量机的变种模型,对非时序数据处理效果尚可,但是在对时序数据特别是工业大数据的处理上,实时性和准确性都无法满足. 文献[7]使用马尔可夫模型,模型前期的数据维度处理采用主成分分析法降维和人为经验提取特征,这种方法没有很好地利用研究的数据本身特征,导致异常检测效果有限. 本文提出的多层堆叠自编码神经网络模型,极大地减少人为的干预,依靠深度学习网络深层次的迭代训练,自主地做到工艺数据降维提高异常检测模型的实时性.

本文提出一种基于时间序列的工艺数据异常检测方法,通过对工业数据库中工艺数据的编码、缺失值处理、特征关联分析、降维测试,使用自编码神经网络降维处理,构建基于循环神经网络RNN及其衍生类的异常检测模型,通过对工艺数据内容的异常行为判别,判定工业设备状态,检测工控异常的发生.

2 工艺数据特征提取

2.1 探索性工艺数据分析(Exploratory Data Analysis, EDA)

2.1.1 工艺数据采集

对工业数据进行异常检测要不断获取测试工艺数据集,本文中工艺数据采集方式为创建OPC采集器,配置指定工业数据库服务器的IP地址与密码,连接到工业库. 在SCADA(Supervisory Control And Data Acquisition)系统上对需要被访问的数据进行权限设置,通过OPC读取到SCADA数据[8,9].

通过对工艺数据的特征映射、编码、标准化处理,然后采用自编码神经网络进行数据降维. 本文使用的数据是某电厂的真实脱敏数据,在该电厂的发电控制流程中各种关键传感器的参数都会进入电厂的工控实时数据库,通过异常检测系统实时监控控制数据,检测结果返回给工控统一管控平台,实现实时的可视化展示. 本文所用数据即为流程中的各参数数据,本文提及的将自编码神经网络与长短期记忆神经网络等时序模型结合使用的检测方法普遍适用于制造业工艺参数的特征数据,这些工业控制检测环境状态不仅与此时刻的数据特征有关,又与此前一段时间内的目标状态有关. 本文使用的是非公开数据集,对于重复验证该实验效果可以使用天池大赛"智能制造质量预测"中的半导体制造行业真实的工艺数据,在此真实的公开数据集下本文模型也取得了良好的效果. 表1是在非公开数据集下经过数据处理得出数据集的基本描述,异常检测类别标签是一个二值型特征,初始样本有57个特征项,其中category类型特征有15项,数值型特征有26项,binary类型特征有17项,本文使用人为标定的训练数据集595212个样本,测试集892816个样本.

表1 工艺数据集描述

	Role	Level	Count
1	Input	Binary	17
2	Input	Category	15
3	Input	Float	10
4	Input	Int	16
5	Target	Binary	1

2.1.2 数值型特征相关性分析

多个线性特征会导致解空间不稳定,从而使得训练模型不易收敛,模型增加训练时间,对异常检测系统的实时性有影响[10]. 为避免给异常检测模型输送相关变量,本文通过计算数值型特征的相关系数矩阵$\boldsymbol{\rho}$,得到如图1所示的多维特征相关图. 图1中红色表示最大正相关,蓝色为最大负相关,图中最大正相关度为0.22,最大负相关度为-0.12,本文中设置的相关阈值为0.85,可以看出各个特征相关性较低,各个参数特征相关度没有超出阈值,不需要删除.

2.1.3 分类型特征分析

本文获取的分类型特征分为标志型变量(normal)和序列型变量(ordinary),标志型变量的大小不代表任何意义,仅仅表示一种类别,所以如果直接用来进行入侵检测模型训练会让模型认为是数值型变量,误导模型训练导致训练模型不准确. 另一类分类型特征属于序列型变量,就是虽然每个变量的数值指的是一种类型特征,但是每种类型间是有大小关系的. 对于第一种本文使用One-Hot编码,第二种情况采用映射方法,将分类变量转化为数值变量[11].

2.2 基于堆叠自编码神经网络(Stacked Auto-Encoder, SAE)的特征提取

使用自编码神经网络将工艺数据进行压缩,由原始的n维压缩成m维,然后在需要还原数据的时候最小

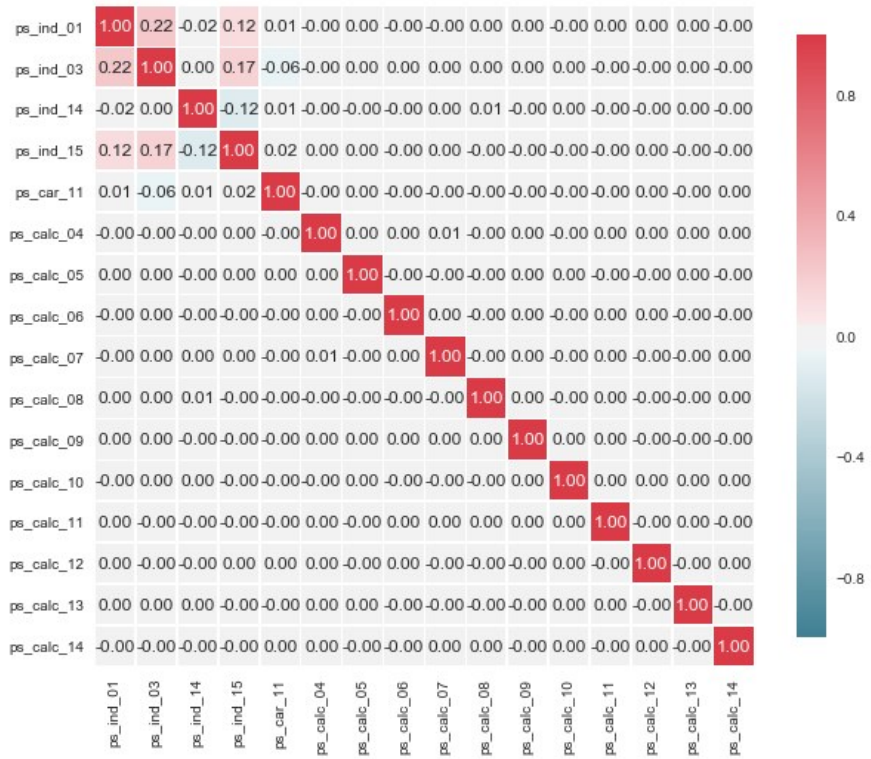

图1　数值型特征相关性图

化损失把数据恢复出来. 堆叠自编码神经网络是神经网络在数据特征提取上的一种非线性方法. 它是将自编码神经网络的输出状态 y 忽略,将隐层 h 作为原始信息,训练一个新的自编码器,这样经过层层堆叠,减小数据特征维数,又能保留数据关键信息[12,13],如图2所示.

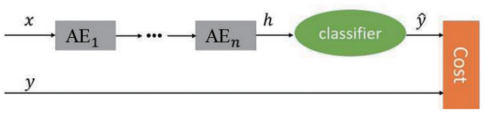

图2　堆叠自编码网络结构

假设, $\boldsymbol{X}$ 表示每个输入数据向量, 每个数据向量均为 n 维, $\boldsymbol{X} \in \mathbf{R}^n$, 每个隐层 H 的维度不同,则

$$H^{(1)} = f(\boldsymbol{W}^{(1)}\boldsymbol{X} + b^{(1)})$$

$$H^{(2)} = f(\boldsymbol{W}^{(2)}H^{(1)} + b^{(2)})$$

$$\vdots$$

$$\bar{y} = \text{softmax}\left(\boldsymbol{W}^{(n)}H^{(n-1)} + b^{(n-1)}\right)$$

$\boldsymbol{W}$ 是每个隐层的参数矩阵,经过层层迭代,最终通过 softmax 函数求得 y 维向量对应的概率大小[14~16]. 若 $H^{(1)}$ 为 m 维, $H^{(2)}$ 为 k 维,那么要训练一个 $n \to m \to k$ 结构的网络,实际上是先训练网络 $n \to m \to n$,得到 $n \to m$ 的变换,然后再训练 $m \to k \to m$ 网络,得到 $m \to k$ 的变换. 最终堆叠成 SAE,即为 $n \to m \to k$ 的结构.

本文使用 Google 的深度学习开源框架 Tensorflow,实现两层堆叠自编码器. Tensorflow 中最重要的结构就是计算图,计算图又称为有向图和数据流图,负责维护和更新状态. 数据流图用“节点”和“线”描述深度学习中的数学计算. “节点”表示施加的数学操作或数据输入输出,“线”表示“节点”间的关系. 图3为工艺数据基于自编码神经网络的降维数据流图,下方数据源 X_Origin 分别经过编码节点 Encoder 和解码节点 Decoder,最终进入损失节点 Loss 和汇总节点 Summaries,再由训练节点 Train 根据损失大小,经过循环迭代训练最小化节点损失,图中的编码节点或解码节点内都含两层全连接神经网络[17].

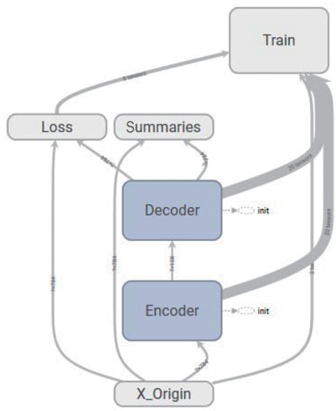

图3　自编码网络数据流图

3 基于长短期记忆神经网络的工艺数据异常检测方法

3.1 长短期记忆网络模型(LSTM)

长短期记忆网络(Long Short Term Memory Networks,LSTM)是循环神经网络RNN的一种优化模型,与RNN相比,LSTM模型增加了三个门,分别为遗忘门、传入门和输出门.这些门的作用是控制之前隐藏状态需要记忆、需要遗忘、需要输出的部分[18~20].图4为LSTM内部结构.

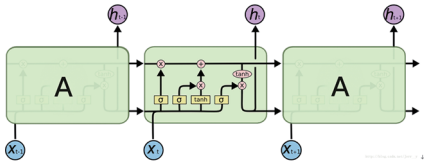

图4 LSTM内部结构

遗忘门(forget gates)输入是h_{t-1}和x_t,输出是每个数值都在0~1之间长度与cell状态向量长度相同的向量,决定哪些有用信息通过这个cell.

$$f_t = \sigma\left(w_f \cdot \left[h_{t-1}, x_t\right] + b_f\right)$$

传入门输入和遗忘门相同,用来决定让哪些新的信息加入cell状态.这个功能分两部分完成,Sigmoid层决定哪些信息更新,再加权tanh层决定隐层哪些信息加入状态.

$$i_t = \sigma\left(w_i \cdot \left[h_{t-1}, x_t\right] + b_i\right)$$

$$\tilde{C}_t = \tanh\left(w_C \cdot \left[h_{t-1}, x_t\right] + b_C\right)$$

这样就把新的状态添加到cell状态中,并且替换掉了旧的状态.

$$C_t = f_t * C_{t-1} + i_t * \tilde{C}_t$$

输出门用来决定输出什么隐藏信息.这个功能实现也分为两部分,Sigmoid层决定哪些信息需要输出,再加权tanh层得到最终输出值.

激活函数:$\dfrac{1}{1+e^{-z}}$

tanh激活函数:$2*\mathrm{Sigmoid}(2x) - 1$

使用激活函数是使神经元模型具有非线性,一个两层的神经网络就可以逼近任何函数.激活函数还可以使输出结果在一定的范围内,使输出具有可微性、单调性,这样在随机梯度下降优化时初始化参数将更加容易.tanh激活函数是Sigmoid的变形,与Sigmoid不同的是tanh激活函数是0均值的,在实际应用中,tanh比Sigmoid的效果更好,并且Sigmoid在输入非常大或非常小时,神经网络的训练梯度接近于0,模型学习接近停止[21~25].

3.2 LSTM多层神经网络的结构设计及训练过程

3.2.1 数据采集

本文采集工艺流程数据,训练数据使用前期在历史数据库中得到的60万个左右数据集,测试数据每三分钟计算一次这段时间进入数据库中的数据作为神经网络的输入.

3.2.2 输入数据的预处理

本文输入数据的降维方法是基于堆叠自编码神经网络SAE的特征提取,原始工艺数据57维特征经过归一化处理输入到含有两层的自编码神经网络,在保证最小损失的情况下,选择输出数据为28维.

3.2.3 LSTM网络节点数选择

因为每个时刻的输入特征是28维,输入到模型中的每一行是一个样本,代表一个时序状态,所以时序长度为1.

本文LSTM神经网络模型的隐层神经元结构参考了已经成熟的LSTM模型,另外采用试值法,测试隐层节点数对异常检测模型的影响,最终试验确定每层节点数为256个,层数为两层.为了细化工艺数据的异常程度,本文把异常检测模型输出设计成十分类,异常检测模型输出分为0到9十个等级的异常指标,指标数值越大代表这条样本的异常程度越高.经过第二个hidden_size层,LSTM部分的输出会是一个[hidden_size]维度的tensor,为了得到一个分类结果还需要接一个Softmax层,输出结果为十个不同异常程度指标的概率,之后在十分类值后加入阈值,通过阈值调整可以快速地调节模型,在出现误报率较高的情况下,提高模型的阈值可以降低检测模型的敏感度,避免了模型只能离线校准的局限性.图5为本文使用的完整LSTM网络结构图.

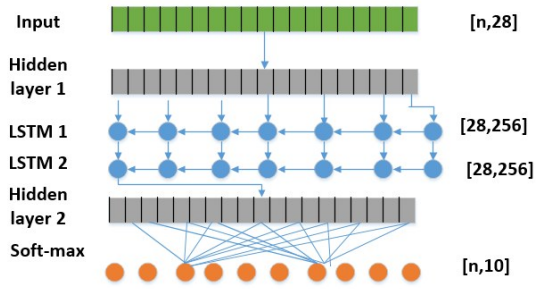

图5 LSTM网络结构

3.2.4 损失函数和评估函数选择

对于工艺数据的异常检测是一个二分类问题,选用交叉熵损失函数,用于LSTM网络的随机梯度下降法更新网络参数.评估函数本文选用Tensorflow提供的AdamOptimizer函数,AdamOptimizer可以通过使用动量

的形式来平滑网络训练的收敛曲线震荡,改善传统梯度下降,促进超参数动态调整. 我们可以通过创建标签错误率的摘要标量来跟踪丢失和错误率.

3.2.5 LSTM 神经网络的训练过程

在训练和测试两个阶段,本文采用不同的投放大小,所以batch_size采用占位符的方式. 另外定义输入输出占位符.

步骤1 LSTM 的输入shape = (batch_size, timestep_size, input_size).

步骤2 调用Tensorflow 提供的rnn. LSTMCell函数,创建LSTM神经网络单元.

步骤3 调用 MultiRNNCell 函数来实现多层LSTM.

步骤4 用全零来初始化state 参数,当time_major ==False 时,outputs. shape = [batch_size, timestep_size, hidden_size].

步骤5 调用 dynamic_rnn 函数让构建好的网络能够动态运行.

步骤6 创建会话Session,初始化全局变量,设置训练集每次投入1000个训练样本,循环600次训练过程,6万个样本都能训练一遍. 在训练过程中每隔20次,也就是每输入2万个样本输出一次模型评估入侵检测的准确率和auc得分.

4 实验对比分析

为了验证本文提出的SAE-LSTM神经网络模型对未知工艺数据的判断准确率,以及在实际工业异常检测系统中配置后的效果,利用课题组现有的工控安全防护仿真实验室,在异常检测系统中部署SAE-LSTM模型,实验室配备机架式服务器、工控主机、工业防火墙、异常检测系统、工业网闸等,可以满足本实验的要求. 在仿真服务器的数据库中投入电厂所得的实际数据,实际数据中的异常数据远远少于正常的数据样本,属于imbalance数据,采用分层交叉验证的方式进行仿真实验,即在验证集和训练集中的正负样本比例一致,验证集的平均得分能很好地反映出模型对未知数据的预测效果. 图6为仿真实验交叉验证模型使用3种不同激活函数的损失曲线图,CV设为10折,交叉验证得分设为交叉熵损失得分. X轴为训练批次,每批次1000个样本,Y轴为模型损失总和. 综上本文选取最优的ReLU激活函数,仿真实验表明SAE-LSTM模型误报率较低,训练后期效果明显.

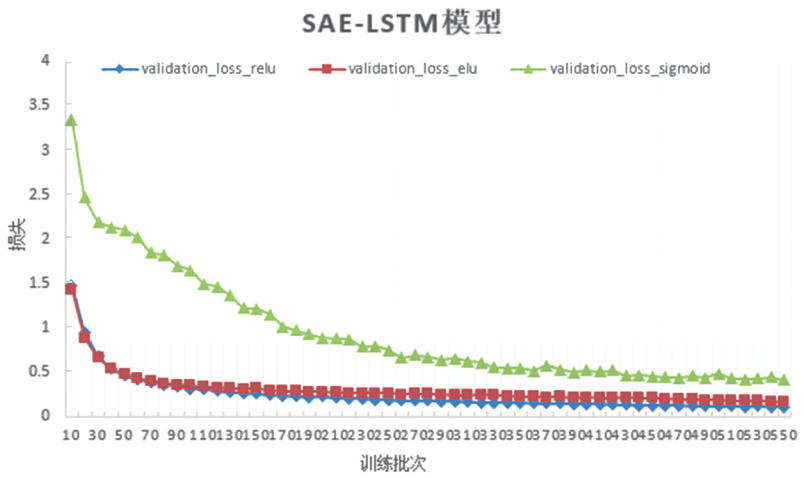

图6　SAE-LSTM模型激活函数对比

为了进一步验证基于时间序列的SAE-LSTM神经网络在对工艺数据的异常检测中的效果,仿真实验另配置时序模型:隐马尔可夫模型(Hidden Markov Model, HMM),非时序模型:SVM模型、XGboost模型、随机森林模型(Random Forest, RF)、梯度提升模型(GDBT)进行对比试验. 试验指标对照为准确率和误报率,结果如图7~8和表2.

图7和图8是交叉验证训练模型,经过550个训练批次后所得的在每个批次上的准确率和损失曲线对比图,通过对比可知SAE-LSTM模型无论在对工艺数据入侵检测的准确率还是误报率方面性能要好于其他模型,对比模型中效果较好的还有隐马尔可夫模型,但训

表2　分层采样交叉验证实验结果

模型	分层交叉验证得分			
	准确率	训练批次	误报率	训练批次
SVM	0. 56	530	0. 45	530
RF	0. 54	530	0. 51	530
XGboost	0. 71	490	0. 35	490
HMM	0. 95	330	0. 08	330
SAE-LSTM	0. 97	250	0. 03	250

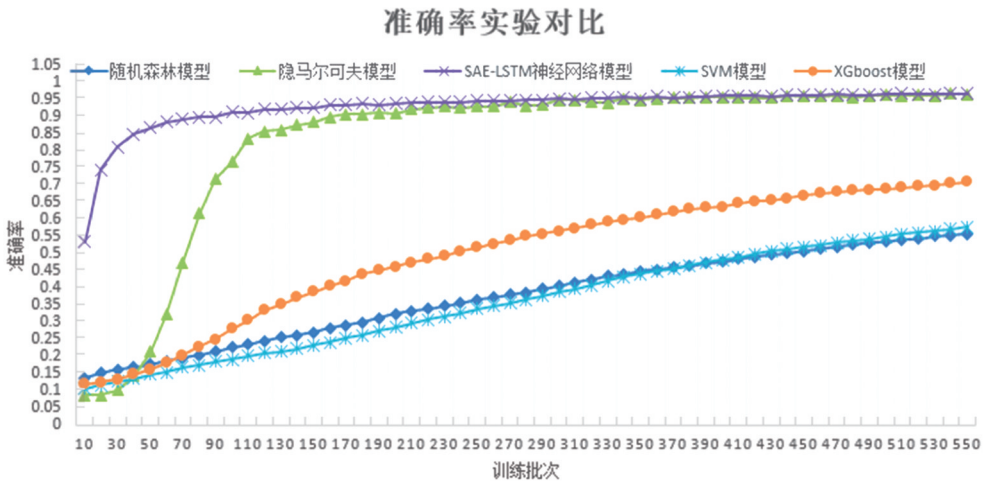

图7 不同模型的准确率实验对比

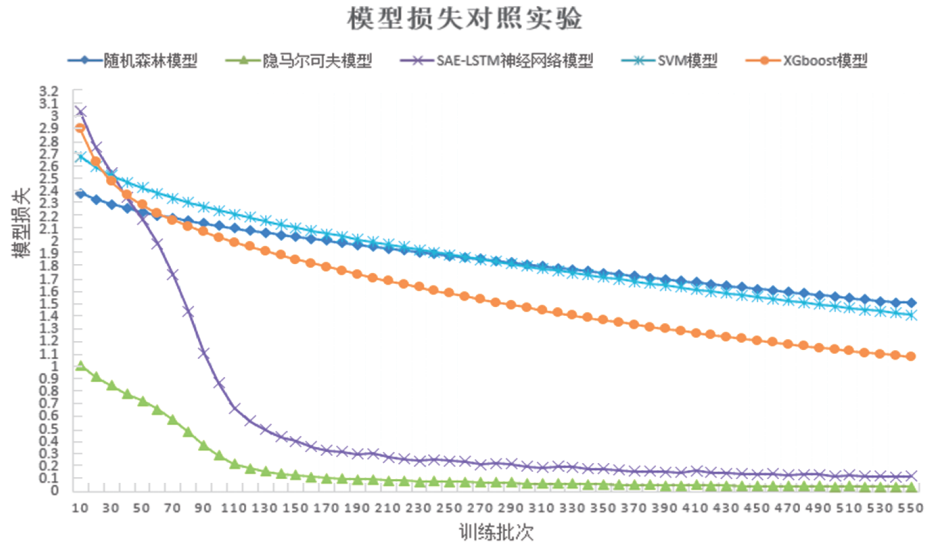

图8 不同模型的交叉熵损失实验对比

练模型收敛所用时间为SAE-LSTM模型的两倍. 在非时序模型中,XGboost模型效果要好于其他非时序模型. 实验表明,工艺数据异常行为的预测与时序影响效果明显.

5 结论

本文主要研究基于时间序列的工艺数据异常检测,提出了一种堆叠自编码神经网络对数据特征提取与长短期记忆神经网络建模相结合的工艺数据异常检测模型(SAE-LSTM),利用这一方法可以有效地判别工艺数据是否存在异常,根据异常反应频率,工控网络安全人员可以更好地实施安全防护手段. 工艺数据按照时间序列采集与存储,使用时序模型对此类数据进行异常检测,与非时序模型(SVM、RF等模型)对比,根据实验结果来看效果更佳.

本文模型后续实验增加了在真实的半导体制造行业复杂工艺数据下的模型效果测试,利用本文模型也取得了很好的效果. 通过分析可知,由于LSTM的三个门的结构在时序序列中能有效提取模型的输入特征,又能通过不断的训练,调整之前目标状态对此刻预测的影响;在非时序的数据中,模型不断调整forget gates参数,直到输出向量模很小,这会使此前时刻目标状态对此刻预测状态影响降到很低,而使用自编码神经网络又能在大部分高维复杂数据降维中取得不错效果. 与传统的时序模型HMM相比,使用该模型可以有效地提高异常检测的准确率降低误报率,而且异常检测的实时性有所提高,更加有利于对工艺数据的实时检测. 此外,本文的LSTM网络模型结构还有一定的提高空

间,在模型结构的设计方面还有很多值得研究的地方,以后会在这一方面进行深入研究.

参考文献

[1] 赖英旭, 刘增辉, 蔡晓田, 等. 工业控制系统入侵检测研究综述[J]. 通信学报, 2017, 38(2): 143 – 156.
Lai Y X, Liu Z H, Cai X T, et al. Research on intrusion detection of industrial control system[J]. Journal on Communications, 2017, 38(2): 143 – 156. (in Chinese)

[2] 张凯一, 陈铁明, 严春. 工业控制系统安全及异常检测研究进展[J]. 信息安全研究, 2017, 3(7): 624 – 632.
Zhang K Y, Chen T M, Yan C. Research survey on industrial control systems security and intrusion detection[J]. Journal of Information Security Research, 2017, 3(7): 624 – 632. (in Chinese)

[3] 毕战科, 许胜礼. 入侵检测技术的研究现状及其发展[J]. 软件导刊, 2010, 9(11): 152 – 154.
Bi Z K, Xu S L. Actuality and development trend of intrusion detection technology[J]. Software Guide, 2010, 9(11): 152 – 154. (in Chinese)

[4] Yim K, Castiglione A, Yi J H, et al. Cyber threats to industrial control systems[A]. Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats[C]. New York, NY, USA: ACM, 2015. 79 – 81.

[5] Cheminod M, Durante L, Valenzano A. Review of security issues in industrial networks[J]. IEEE Transactions on Industrial Informatics, 2013, 9(1): 277 – 293.

[6] 尚文利, 张盛山, 万明, 等. 基于PSO- SVM的Modbus TCP通讯的异常检测方法[J]. 电子学报, 2014, 42(11): 2314 – 2320.
Shang W L, Zhang S S, Wan M, et al. Modbus/TCP communication anomaly detection algorithm based on PSO-SVM[J]. Acta Electronica Sinica, 2014, 42(11): 2314 – 2320. (in Chinese)

[7] 张响亮, 王伟, 管晓宏. 基于隐马尔可夫模型的程序行为异常检测[J]. 西安交通大学学报, 2005, 39(10): 1056 – 1059.
Zhang X L, Wang W, Guan X H. Detection of anomalous program behaviors based on hidden Markov models[J]. Journal of Xi'an Jiaotong University, 2005, 39(10): 1056 – 1059. (in Chinese)

[8] 谢柏林, 余顺争. 基于关键事件序列的应用层异常检测机制[J]. 小型微型计算机系统, 2010, 31(2): 249 – 253.
Xie B L, Yu S Z. Application level anomaly detection based on series of events[J]. Journal of Chinese Computer Systems, 2010, 31(2): 249 – 253. (in Chinese)

[9] 张云贵, 赵华, 王丽娜. 基于工业控制模型的非参数CUSUM入侵检测方法[J]. 东南大学学报(自然科学版), 2012, 42(S1): 55 – 59.
Zhang Y G, Zhao H, Wang L N. A non- parametric CUSUM intrusion detection method based on industrial control model[J]. Journal of Southeast University (Natural Science Edition), 2012, 42(S1): 55 – 59. (in Chinese)

[10] 钱叶魁, 陈鸣, 叶立新, 等. 基于多尺度主成分分析的全网络异常检测方法[J]. 软件学报, 2012, 23(2): 361 – 377.
Qian Y K, Chen M, Ye L X, et al. Network- wide anomaly detection method based on multiscale principal component analysis[J]. Journal of Software, 2012, 23(2): 361 – 377. (in Chinese)

[11] Hinton G E. Reducing the dimensionality of data with neural networks[J]. Science, 2006, 313(5786): 504 – 507.

[12] Vincent P, Larochelle H, Bengio Y, et al. Extracting and composing robust features with denoising autoencoders [A]. Proceedings of the 25th International Conference on Machine Learning(ICML'08) [C]. New York, NY, USA: ACM, 2008. 1096 – 1103.

[13] Vincent P, Larochelle H, Lajoie I, et al. Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion[J]. Journal of Machine Learning Research, 2010, 11: 3371 – 3408.

[14] Rifai S, Vincent P, Muller X, et al. Contractive auto-encoders: Explicit invariance during feature extraction[A]. Proceedings of the 28th International Conference on International Conference on Machine Learning(ICML' 11)[C]. New York, NY, USA: ACM, 2011. 833 – 840

[15] Chen M M, Xu Z X, Weinberger K Q, et al. Marginalized denoising autoencoders for domain adaptation[A]. Proceedings of the 29th International Coference on International Conference on Machine Learning(ICML' 12) [C]. New York, NY, USA: ACM, 2012. 1627 – 1634.

[16] Bengio Y. Learning deep architectures for AI[J]. Foundations and Trends ® in Machine Learning, 2009, 2(1): 1 – 127.

[17] Liu S J, Yang N, Li M, et al. A recursive recurrent neural network for statistical machine translation[A]. Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers) [C]. Stroudsburg, PA, USA: Association for Computational Linguistics, 2014. 1491 – 1500.

[18] Biswas A, Karunakaran S. Cybernetic modeling of industrial control systems: Towards threat analysis of criti-

cal infrastructure[EB/OL]. https://www.researchgate.net/publication/282652007_Cybernetic_modeling_of_Industrial_Control_Systems_Towards_threat_analysis_of_critical_infrastructure, 2021.

[19] Soelaiman R, Martoyo A, Purwananto Y, et al. Implementation of recurrent neural network and boosting method for time-series forecasting[A]. International Conference on Instrumentation, Communication, Information Technology, and Biomedical Engineering[C]. Bandung, Indonesia: IEEE, 2009. 1 – 8.

[20] Ren H R, Ye Z X, Li Z W. Anomaly detection based on a dynamic Markov model[J]. Information Sciences, 2017, 411: 52 – 65.

[21] Tsai C L, Chang A Y, Chen C J, et al. Dynamic intrusion detection system based on feature extraction and multidimensional hidden Markov model analysis[A]. International Carnahan Conference on Security Technology[C]. Zurich, Switzerland: IEEE, 2009. 85 – 88.

[22] Marchi E, Vesperini F, Eyben F, et al. A novel approach for automatic acoustic novelty detection using a denoising autoencoder with bidirectional LSTM neural networks [A]. IEEE International Conference on Acoustics, Speech and Signal Processing[C]. South Brisbane, QLD, Australia: IEEE, 2015. 1996 – 2000.

[23] Marchi E, Ferroni G, Eyben F, et al. Multi-resolution linear prediction based features for audio onset detection with bidirectional LSTM neural networks[A]. IEEE International Conference on Acoustics, Speech and Signal Processing[C]. Florence, Italy: IEEE, 2014. 2164 – 2168.

[24] 梁辰, 李成海, 周来恩. PCA-BP神经网络入侵检测方法[J]. 空军工程大学学报(自然科学版), 2016, 17(6): 93 – 98.
Liang C, Li C H, Zhou L E. A PCA-BP neural network-based intrusion detection method[J]. Journal of Air Force Engineering University (Natural Science Edition), 2016, 17(6): 93 – 98. (in Chinese)

[25] 杨雅辉, 黄海珍, 沈晴霓, 等. 基于增量式GHSOM神经网络模型的入侵检测研究[J]. 计算机学报, 2014, 37(5): 1216 – 1224.
Yang Y H, Huang H Z, Shen Q N, et al. Research on intrusion detection based on incremental GHSOM[J]. Chinese Journal of Computers, 2014, 37(5): 1216 – 1224. (in Chinese)

作者简介

尚文利 男,1974年生于黑龙江省望奎县.博士,研究员,博士生导师.现为广州大学“百人计划”学科带头人,原中国科学院沈阳自动化研究所工业控制系统信息安全方向学术带头人.主要研究方向为工业控制系统信息安全、计算智能与机器学习、边缘计算.
E-mail:shangwl@gzhu.edu.cn

石 贺 男,1993年生于辽宁省沈阳市.中国科学院大学硕士研究生.研究方向为机器学习、数据挖掘、工业控制系统信息安全.
E-mail:shihe@sia.cn