(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110865625 A
(43)申请公布日 2020.03.06

(21)申请号 201810985559.2

(22)申请日 2018.08.28

(71)申请人 中国科学院沈阳自动化研究所
地址 110016 辽宁省沈阳市沈河区南塔街114号

(72)发明人 尚文利 赵剑明 刘贤达 尹隆 陈春雨 曾鹏

(74)专利代理机构 沈阳科苑专利商标代理有限公司 21002
代理人 王倩

(51)Int.Cl.
G05B 23/02(2006.01)
G06N 3/04(2006.01)
G06N 3/08(2006.01)

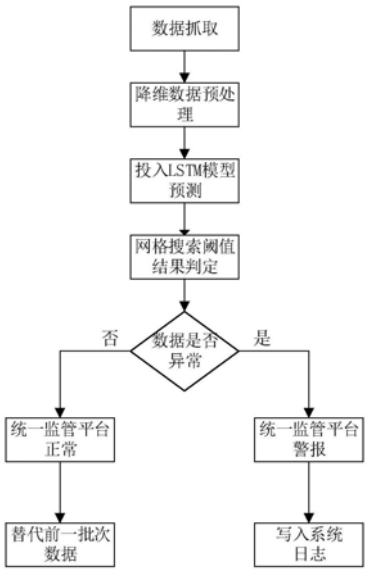
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种基于时间序列的工艺数据异常检测方法

(57)摘要

本发明涉及一种基于时间序列的工艺数据异常检测方法，通过自编码神经网络模型对工业数据进行降维处理，再通过LSTM神经网络模型进行工艺数据的检测，包括以下步骤：对工业数据进行预处理得到工业数据特征；根据工业数据特征构建自编码神经网络模型，进行工艺数据特征降维；根据降维后的工艺数据特征构建LSTM神经网络模型；通过LSTM神经网络模型进行工艺数据的异常检测。本发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异常检测模型。在不改变现有硬件设备架构的前提下，结合嵌入式设备自身特点，适合在各种设备中搭建平台。



CN 110865625 A

1.一种基于时间序列的工艺数据异常检测方法,其特征在于,通过自编码神经网络模型对工业数据进行降维处理,再通过LSTM神经网络模型进行工艺数据的检测,包括以下步骤:

对工业数据进行预处理得到工业数据特征;

根据工业数据特征构建自编码神经网络模型,进行工艺数据特征降维;

根据降维后的工艺数据特征构建LSTM神经网络模型;

通过LSTM神经网络模型进行工艺数据的异常检测。

2.根据权利要求1的一种基于时间序列的工艺数据异常检测方法,其特征在于,用于Lambda架构。

3.根据权利要求1所述的一种基于时间序列的工艺数据异常检测方法,所述预处理采用相关系数方法进行降维。

4.根据权利要求3所述的一种基于时间序列的工艺数据异常检测方法,所述相关系数方法中相关系数的取值区间在1到-1之间。

5.根据权利要求1所述的一种基于时间序列的工艺数据异常检测方法,所述根据工业数据特征构建自编码神经网络模型,进行工艺数据特征降维具体为:

将预处理后的工业数据特征作为自编码神经网络模型的输入,输出为降维后的工业数据特征,实现工艺数据特征降维。

6.根据权利要求1或5所述的一种基于时间序列的工艺数据异常检测方法,所述自编码神经网络模型为两层;第一层中间的隐藏层n由500神经元组成,使用随机梯度下降训练得到最小损失,再把结果作为第二层输入,第二层的中间隐藏层由125个神经元组成。

7.根据权利要求1或5所述的一种基于时间序列的工艺数据异常检测方法,在所述自编码神经网络模型第二层的隐藏层与输出的降维工艺数据特征之间引入Dropout层。

8.根据权利要求5所述的一种基于时间序列的工艺数据异常检测方法,所述根据降维后的工艺数据特征构建LSTM神经网络模型具体为:

将降维后的工艺数据特征作为LSTM神经网络模型的输入,输出为用于训练的异常工艺数据。

9.根据权利要求8所述的一种基于时间序列的工艺数据异常检测方法,所述LSTM神经网络模型选用交叉熵损失函数,采用随机梯度下降法更新网络参数;评估函数选用Adam自适应矩估计。

10.根据权利要求8所述的一种基于时间序列的工艺数据异常检测方法,构建LSTM神经网络模型时,通过使用动量的形式平滑网络训练的收敛曲线震荡。

一种基于时间序列的工艺数据异常检测方法

技术领域

[0001] 本发明涉及一种基于时间序列的工艺数据异常检测方法，其能确保工业数据在发生异常的情况下自动检测警报，属于工业系统的信息安全技术领域。

背景技术

[0002] 现阶段，工业控制系统已广泛应用于电力、轨道交通、石油化工、核设施等行业中，据统计，超过80％涉及国计民生的关键基础设施都依靠工业控制系统来实现自动化作业。近几年，针对工业控制系统的各种网络攻击与入侵事件屡见不鲜，根据美国国土安全部下属的工业控制系统网络应急响应小组(Industrial Control Systems Cyber Emergency Response Team，ICS-CERT) 连续三年的安全研究报告，针对工业控制系统的安全事件呈阶梯状增长态势，仅2015年该小组收集到全球工控安全漏洞数量就达到427个。

[0003] 工业控制系统的异常检测主要目的是在恶意攻击发生时进行实时监测与报警，是一种对工业控制系统局部关键区域进行安全检测的技术手段。然而，为了保障工业控制系统全方位的安全稳定运行，不仅需要攻击发生时的实时检测，同时更加需要对攻击即将发生时的有效预测，从整体角度感知整个工业控制系统的安全态势。因此，基于上述异常检测方法，需要进一步研究工业控制系统的安全感知理论，提供对未来一段时间内系统安全状况进行合理准确预测的能力。现阶段，针对工业控制系统的安全感知研究已经逐渐开始，但为数尚少。其中，论述了如何攻击智能电网，提出了智能电网环境下态势感知的具体要求；说明了电力系统中导致不充分态势感知的因素，并用马尔可夫模型评估不充分态势感知的影响；借助态势感知实现工控系统的自适应安全，辅助系统管理人员制定安全决策；结合完整性攻击研究，建立基于拜占庭将军问题的工控网络安全态势感知模型，判断系统中的恶意节点。上述研究工作表明安全感知理论已经在工业控制系统进行了初步探索，但在安全感知的工控独特要求及针对性方法设计方面还有待完善，主要原因在于：一方面，目前针对工业控制系统的信息安全需求及技术研究仍不成熟，工业控制系统的安全边界条件仍需进一步论证；另一方面，工业控制系统具有相对特殊的系统结构及通信特点，而信息安全研究人员难以从这些特点出发进行工业控制系统的安全感知研究。

发明内容

[0004] 针对上述提出的工控信息安全的要求，本发明的目的是一种基于SAE-LSTM 异常检测模型，本发明以工控系统中的工艺数据为检测对象，重点研究了如何在高维、复杂、大规模的工艺数据中将异常数据标识出来，以构建实时的工控信息安全异常检测模型。其中，SAE表示堆叠自编码神经网络模型，LSTM表示长短期记忆神经网络模型(Long Short-Term Memory)。

[0005] 本发明解决其技术问题所采用的技术方案是：一种基于时间序列的工艺数据异常检测方法，通过自编码神经网络模型对工业数据进行降维处理，再通过 LSTM神经网络模型进行工艺数据的检测，包括以下步骤：

[0006] 对工业数据进行预处理得到工业数据特征；

[0007] 根据工业数据特征构建自编码神经网络模型，进行工艺数据特征降维；

[0008] 根据降维后的工艺数据特征构建LSTM神经网络模型；

[0009] 通过LSTM神经网络模型进行工艺数据的异常检测。

[0010] 一种基于时间序列的工艺数据异常检测方法，用于Lambda架构。

[0011] 所述预处理采用相关系数方法进行降维。

[0012] 所述相关系数方法中相关系数的取值区间在1到-1之间。

[0013] 所述根据工业数据特征构建自编码神经网络模型，进行工艺数据特征降维具体为：

[0014] 将预处理后的工业数据特征作为自编码神经网络模型的输入，输出为降维后的工业数据特征，实现工艺数据特征降维。

[0015] 所述自编码神经网络模型为两层；第一层中间的隐藏层n由500神经元组成，使用随机梯度下降训练得到最小损失，再把结果作为第二层输入，第二层的中间隐藏层由125个神经元组成。

[0016] 在所述自编码神经网络模型第二层的隐藏层与输出的降维工艺数据特征之间引入Dropout层。

[0017] 所述根据降维后的工艺数据特征构建LSTM神经网络模型具体为：

[0018] 将降维后的工艺数据特征作为LSTM神经网络模型的输入，输出为用于训练的异常工艺数据。

[0019] 所述LSTM神经网络模型选用交叉熵损失函数，采用随机梯度下降法更新网络参数；评估函数选用Adam自适应矩估计。

[0020] 构建LSTM神经网络模型时，通过使用动量的形式平滑网络训练的收敛曲线震荡。

[0021] 本发明具有以下有益效果及优点：

[0022] 1.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异常检测模型。

[0023] 2.本发明在不改变现有硬件设备架构的前提下，结合嵌入式设备自身特点，适合在各种设备中搭建平台。

附图说明

[0024] 图1为本发明的基于SAE-LSTM异常检测系统的架构图。

[0025] 图2为本发明的基于LSTM的异常检测系统的神经网络结构图。

[0026] 图3为本发明的基于LSTM的异常检测系统运行架构示意图。

具体实施方式

[0027] 下面结合实施例对本发明做进一步的详细说明。

[0028] 一种基于时间序列的工艺数据异常检测方法，包括以下步骤：

[0029] 第一步：在模型搭建之前，设计整体实时异常检测架构；

[0030] 实时工艺数据异常检测模型的部署使用Lambda架构，分为实时响应、快速处理层和批处理层。

[0031] 收集数据阶段:程序从工业实时数据库中抓取最新1000个样本,使用非阻塞的异步写入接口,使用循环的检测程序不断抓取最新的数据库样本。

[0032] 数据处理消息源:由不同程序对抓取到的工业数据进行特征的预处理,再将数据发送到之后的消息处理单元,特征的处理选用特征相关系数方法,特征之间关系密切程度的统计指标,相关系数的取值区间在1到-1之间,去除相关度较高特征。

[0033] 消息存储单元:

[0034] 消息处理单元完成信息处理之后,将数据处理结果写入到Mysql数据库。

[0035] 第二步:构建堆叠自编码神经网络模型,设计神经网络结构,进行工艺数据降维;

[0036] 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。

[0037] 所述SAE神经网络模型使用两层的堆叠自编码神经网络,第一层中间的隐藏层n由500神经元组成,使用随机梯度下降训练得到最小损失,再把结果作为第二层输入,第二层的中间隐藏层由125个神经元组成。

[0038] 损失函数选择交叉熵损失,激活函数使用sigmoid非线性激活函数。

[0039] 为了增强模型的泛化性能和避免过拟合,引入Dropout层,Dropout参数选择0.5,选择随机丢弃一半的参数。

[0040] 第三步:构建LSTM神经网络模型,设计神经网络结构。

[0041] 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。评估函数选用Adam自适应矩估计。

[0042] 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。

[0043] 所述LSTM神经网络模型包括一层256维全连接层,两层28*256维lstm神经元,为了防止过拟合,Dropout层参数为0.6。

[0044] 所述LSTM神经网络时间步长大小timestep_size取3,实验验证此刻状态与之前三个状态相关联,预测效果最佳。

[0045] 针对时间序列的工艺数据异常检测平台,能够利用时间序列预测工控系统中被入侵感染的异常工艺数据,并及时发出警报,尽量降低实际工业现场损失,通过SAE神经网络达到数据降维效果,降低实时数据处理时间,使用LSTM神经网络作为异常检测主模型。

[0046] 为了对工业网络中工艺数据的安全防护,为工业实时数据库构建数据异常检测系统运行环境。参见图1,示出了本发明基于时序状态的LSTM异常检测系统架构,异常检测系统上层连接统一安全管控平台,下层连接从工业现场实时导入的工业实时数据库,参见图2,示出了LSTM的神经网络结构图,参见图3,示出了异常检测模型的流程图,从开始导入工艺数据到工艺数据的降维模型处理,经过长短期记忆神经网络异常检测模型得到异常值的概率,再根据训练结果使用网格搜索确定判定异常的阈值大小,最终输送给统一管理平台和日志记录。本发明的方法在具体实施时,工作主要流程如下:

[0047] 步骤一:从工业实时数据库获取数据进行前期的数据预处理。

[0048] 步骤二:在异常检测平台中搭建降噪自编码神经网络,通过最小化交叉熵损失函数,使用AdamOptimizer优化方法训练模型权重。

[0049] 步骤三:在异常检测平台中搭建长短期记忆神经网络,通过最小化交叉熵损失函

数,使用MomentumOptimizer动量优化方法,加快训练模型,训练模型权重,输出十维的异常指标,另外的模型参数为:

[0050] 确定每一层网络节点的丢弃比例Drop_out=0.6;

[0051] 确定LSTM的层数=2及时间窗口lookback=3;

[0052] 确定模型训练的数据轮询次数epoch=10和批次大小batch_size=200;

[0053] 步骤四:对输出的结构使用网格搜索交叉验证的方法,使用十折交叉验证寻找最优阈值,提高模型的灵敏度,平衡模型灵敏度与误报率。

[0054] 对所公开的实施例的上述说明,使本领域专业技术人员能够实现或使用本发明的实例开发出以上五个步骤,从而实现基于SAE-LSTM的异常检测系统构建。因此,本发明将不会被限制于本文所示的这些实施例,而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

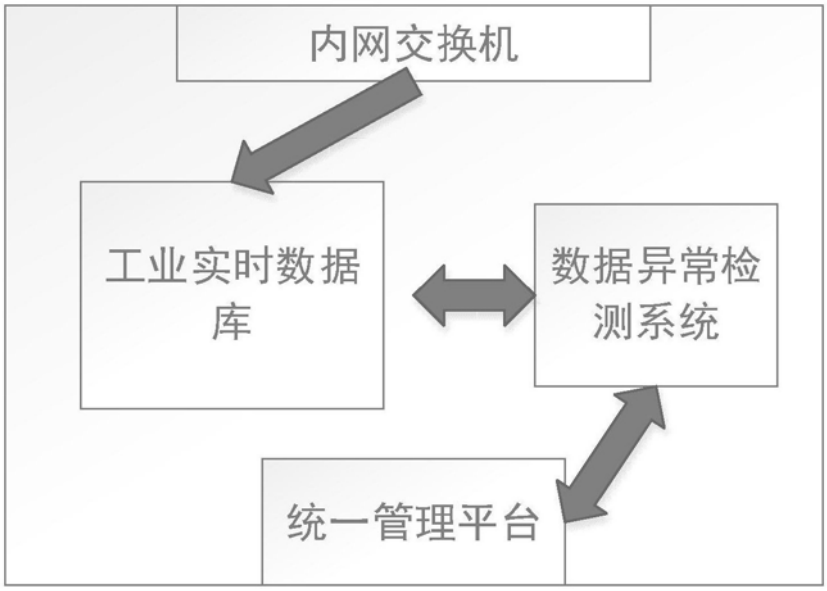

内网交换机
工业实时数据库
数据异常检测系统
统一管理平台

图1

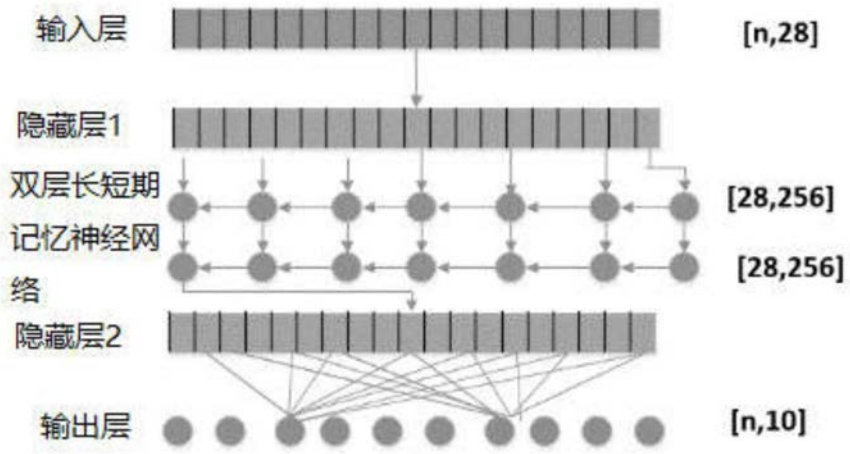

输入层
[n,28]
隐藏层1
双层长短期记忆神经网络
[28,256]
[28,256]
隐藏层2
输出层
[n,10]

图2

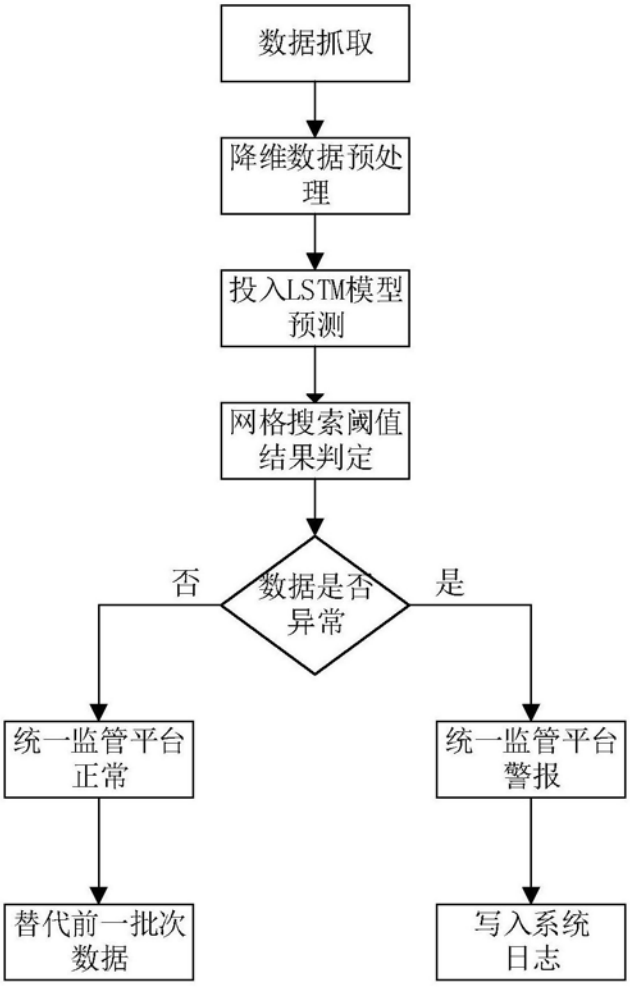

数据抓取
降维数据预处理
投入LSTM模型预测
网格搜索阈值结果判定
数据是否异常
否
是
统一监管平台正常
统一监管平台警报
替代前一批次数据
写入系统日志

图3