计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2020,29(9):266−271 [doi: 10.15888/j.cnki.csa.007598]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于长短期记忆网络的工控网络异常流量检测①

田伟宏[1,2], 李喜旺[2], 司志坚[2,3]

[1](中国科学院大学, 北京 100049)
[2](中国科学院 沈阳计算技术研究所, 沈阳 110168)
[3](国网辽宁省电力有限公司, 沈阳 110004)
通讯作者: 田伟宏, E-mail: 296206234@qq.com

摘　要: 针对目前工控网络异常流量检测方法存在识别准确率不高和识别效率低的问题, 结合工控网络具有周期性的特点, 提出一种基于长短期记忆网络 (LSTM) 的时序预测的异常流量检测模型. 该模型以 LSTM 网络模型为核心, 用前 15 分钟的正常历史流量序列预测下一时刻的流量数据, 在测试集上准确率为 98.12% 的前提下, 可以认为模型的预测值即为正常值, 通过对比实际值和预测值来判断是否出现异常. 在不降低识别准确率的前提下, 由于提前计算出了预测值, 该方法大幅度提高了检测效率.

关键词: 长短期记忆网络; 时序预测; 工控网络; 异常流量检测; 流量序列

引用格式: 田伟宏,李喜旺,司志坚.基于长短期记忆网络的工控网络异常流量检测.计算机系统应用,2020,29(9):266–271. http://www.c-s-a.org.cn/1003-3254/7598.html

Detection of Abnormal Traffic in Industrial Control Network Based on LSTM Network

TIAN Wei-Hong[1,2], LI Xi-Wang[2], SI Zhi-Jian[2,3]

[1](University of Chinese Academy of Sciences, Beijing 100049, China)
[2](Shenyang Institute of Computing Technology, Chinese Academy of Sciences, Shenyang 110168, China)
[3](State Grid Liaoning Electric Power Co. Ltd., Shenyang 110004, China)

Abstract: Aiming at the problems of low recognition accuracy and low recognition efficiency in the current abnormal flow detection methods of industrial control network, combined with the periodic characteristics of industrial control networks, this study proposes an abnormal flow detection model based on Long-Short Term Memory network (LSTM) time series prediction. This model takes the LSTM network model as the core, and uses the normal historical traffic sequence of the first 15 minutes to predict the traffic data at the next moment. On the premise that the accuracy on the test set is 98.12%, the model's predicted value can be considered to be normal. By comparing the actual value with the predicted value, it is determined whether there is an abnormality. On the premise of not reducing the recognition accuracy rate, because the predicted value is calculated in advance, this method greatly improves the detection efficiency.

Key words: Long-Short Term Memory (LSTM) networks; timing prediction; industrial control networks; abnormal traffic detection; traffic sequence

在大力提倡"中国制造 2025", "工业 4.0"的大背景下, 我国工业得到了快速发展, 并且随着计算机技术在工控系统和工控网络中的应用, 逐渐打破了传统工控系统和网络的封闭性, 由于大多数工控网络协议在设计之初都没有考虑到安全问题, 使得工控系统的网络安全面临着严峻的考验[1]. 例如 2010 年的"震网"病毒

① 基金项目: 国家科技重大专项 (2017ZX01030-201)
Foundation item: National Science and Technology Major Program (2017ZX01030-201)
收稿时间: 2020-02-20; 修改时间: 2020-03-17; 采用时间: 2020-03-24; csa 在线出版时间: 2020-09-04

攻击伊朗核设施, 黑客渗透至工业内网后, 利用工业控制系统的安全漏洞, 改变相关设施的运行参数, 降低浓缩铀的成品浓度, 最终使得伊朗核工业陷入停滞; 2015 年的“Blackenergy”病毒造成了乌克兰的大面积停电; 2018 年俄罗斯黑客入侵美国电网; 2019 年委内瑞拉全国大面积停电. 从这些工控网络安全事件可以看出, 黑客已经将触角伸入到工业控制领域尤其是电网, 并且瘫痪对方的基础设施也成为了国与国之间的对抗手段, 工控网络已经成为了理想的攻击目标.

1 工控网络现状

目前工控网络的安全策略方法主要是边界防护, 包括使用网闸、工业防火墙、逻辑隔离等手段[2], 其主要特点是偏防御轻检测. 如平台硬件和软件加固、关键应用代码审计等; 强调集中监控, 依靠站内审计系统等. 主要不足之处表现为缺乏纵深防御, 一旦突破边界防护便很容易进行进一步的侵入.

工业控制系统 (Industrial Control System, ICS) 中, 电力行业应用最为广泛, 其中的变电站自动化约占整个 ICS 市场的 40%. 目前智能电网正在逐步取代传统的电力网络, 而智能变电站又是智能电网建设的重要环节, 是结合了比较先进并且具有高可靠性的智能设备组成的智能化变电站, 加强了变电站在无人值守、安全生产和远程监控等方面的综合管理水平. 网络和信息化技术的发展给电网的智能化提供了保障, 然而更多的研究和应用侧重于信息化引入新功能的实现, 对信息化和网络化背景下智能电网的安全性缺乏足够的考虑, 尤其是入侵检测方面的安全[3,4]. 目前, 建立有效的入侵检测方案是一项巨大的知识工程任务, 系统构建者依靠他们的直觉和经验选择异常检测的统计度量标准. 专家首先分析和分类工控网络的攻击场景和系统漏洞, 并手动编写相应的规则和模式用于检测入侵. 由于开发过程中的手动性和临时性, 这种入侵检测方案具有有限的可扩展性和适应性, 并且方案的更新既昂贵又缓慢.

随着机器学习的热度不断上升, 学术界在网络异常检测方面也提出过很多方法, 大致分为两种, 分别是传统的机器学习方法和近几年广泛使用的深度学习方法. 传统机器学习领域中, 具有代表性的方法有基于有监督的例如 SVM 的二分类方法[5] 和无监督的例如 K-Means 的聚类方法[6]. 有监督的方法例如 SVM 在训练模型时需要每个样本都有标签, 用于区分样本是否为攻击行为, 这种方法的局限性在于在工控网络中很难得到攻击类型完整的数据集; 无监督的检测方法以 K-means 聚类算法为例, 通过聚类算法来区分正常流量和异常流量. 这种方法的局限性表现为模型的稳定性不够好, 依赖训练数据集中正负样本的均衡性. 深度学习领域中具有代表性的方法有主题模型方法[7] 和卷积神经网络方法[8], 主题模型方法将数据包视为文档的词汇, 将网络异常行为视为文档的主题, 通过流量数据包的语义关系识别主题进而识别出网络异常, 这种方法的局限性在于工控网络应用领域广泛, 流量数据包即“词汇”也在源源不断的更新中, 很难学习到完整的语料库; 卷积神经网络方法将流量特征值映射为灰度图, 使卷积神经网络学习大量的流量特征灰度图, 达到识别异常流量的目的, 这种方法的优点是识别准确度高, 但是由于需要大量的点积运算, 所以识别效率并不高. 考虑到工控网络周期性强和流量数据包在时间维度上存在序列关系这两个特性, 所以本文提出基于时序预测的异常检测模型. 在机器学习领域中, 周期性的数据天然适合做时序预测, 并且当数据存在序列关系时, 连接数据的时间动态关系都比每个时间帧的内容更重要.

本文以 ICS 中的典型代表电力系统网络作为研究对象, 变电站自动化以及调度自动化使用 IEC60870-5-104 远动通信规约 (Telecontrol equipment and systems - Part 5-104, IEC104) 控制协议[9,10]. 通过对东北电力公司某子网的交换机进行端口镜像, 采集一段时间内的流量并进行 104 规约的解析, 统计检测流量的特征, 包括从物理层到传输层的 TCP/IP 协议内容和应用层的应用规约控制信息 (Applying Protocol Control Information, APCI) 内容. 数据集采集完成后, 本文采用在时序预测领域使用最广泛且模型效果不错的长短时记忆网络 (Long-short Term Memory Network, LSTM) 进行流量时序预测并检测异常流量. LSTM 是一种改进之后的循环神经网络 (Recurrent Neural Network, RNN), 可以解决 RNN 无法处理长距离依赖的问题和训练模型时梯度消失的问题. 考虑到网络流量的派生属性中存在时间流量属性和机器流量属性, 其中机器流量属性是为了识别某种攻击, 例如探测漏洞行为, 需要考虑之前的若干个连接, 所以使用 LSTM可以更加全面和精准的识别出由多个连续数据包发起攻击引起的流量异常现象.

2 LSTM 网络模型设计

工控网络尤其是电力系统的网络使用场景单一, 在网络安全运行的情况下, 流量数据表现平稳, 并且具有周期性, 一旦网络发生异常, 流量就会产生较大的波动, 具体表现为流量各个维度的数值相较于历史数据发生突变, 不再符合周期性的特点. 基于工控网络流量平稳和周期性强的特点, 本文提出使用 LSTM 网络模型对工控网络的流量数据进行时序预测[11−14], 在网络正常运行的情况下, 可以认为模型的预测值为正常值, 当某一时刻的实际值偏离预测值较大, 即认为网络出现异常.

2.1 异常流量检测流程

检测流程分为两个阶段, 第一个阶段是解析流量数据包构建有效特征, 第二个阶段是 LSTM 网络模型的离线训练过程和在线检测过程. 第一阶段在电力 SCADA 系统中通过镜像端口的方式采集通信流量, 对采集到的数据包进行深度包解析, 针对 104 规约数据包, 除了要解析常规的源地址、目的地址、源端口、目的端口、标志位和连接时间等基本信息, 还要解析长度为 6 个字节的 APCI, 里面包含了控制电路的操作信息. 对解析到的字段进行整合并重新构造出模型输入需要的特征, 除了采集流量构造出的特征, 构建时序模型还需要加入滞后历史特征, 即模型需要用多长时间的输入去预测下一时刻的数值. 第二阶段在模型离线训练完成后, 即可部署线上环境, 对电力通信网络进行异常流量预测并实时报警.

2.2 特征构造

如图 1 所示, 第一阶段包含从流量中提取特征, 并构造有效特征两部分, 流量分为两部分, 第一部分是离线采集的流量, 主要用于模型训练, 第二部分是源源不断的在线流量. 从流量中解析出同 TCP/IP 协议一样的字段和 104 规约中的 APCI 字段. 解析字段分为 3 类, 第一类为 9 个内部属性, 这些属性是从网络数据包的头部中提取得到, 例如连接的持续时间 (duration), 连接的协议类型 (protocol_type), 包含 http、ftp、smtp 和 telnet 等 70 种网络服务类型 (service) 等; 第二类为内容属性, 这些属性是从网络数据包的内容区域中提取, 例如从应用规约数据单元中提取的信息体、数据单元标识和 104 规约报文变长帧中的 APCI; 第三类为派生属性, 这些属性的计算考虑了之前的连接, 细分为时间流量属性和机器流量属性, 时间流量属性考虑过去 2 秒内发生的连接, 例如到同一目标 IP 地址的点击总和 (count), 到同一目标端口号的连接总和 (srv_count) 等字段. 对以上 38 个字段构建时间统计特征, 构建方法分为计数 (count)、占比 (percent) 和均值 (average), 共构造出 12 个有效特征. 例如“相同主机”特征, 检查过去 2 秒内与当前连接具有相同目标主机的连接, 统计连接的数量, 再计算与当前连接具有相同服务的连接百分比、不同服务的百分比、SYN (泛洪) 的百分比以及 REJ(拒绝连接) 的百分比. 对于诸如报文内部属性中的网络服务类型等的非数值型特征, 需要对其进行独热编码 (one-hot) 转换为数值型特征用于模型的输入.

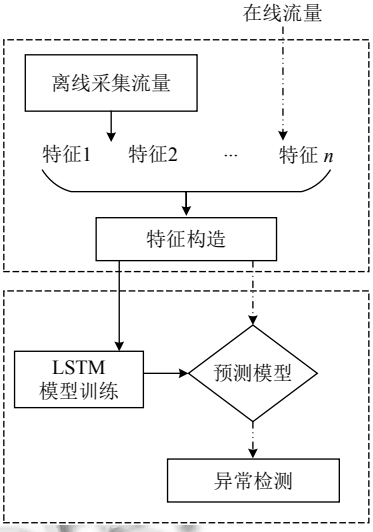

图 1 异常流量检测流程

2.3 模型训练

图 2 中的第二阶段为模型训练部分, 分为离线训练和在线检测两部分, 离线训练把构造好的特征输入到初始化的 LSTM 网络中进行模型训练, 训练好的预测模型输入以相同方式构造的特征样本进行异常流量检测, 如果模型检测到网络中的流量异常则发出警报.

3 LSTM 网络结构和参数更新

3.1 网络整体结构

LSTM 网络结构由 RNN 加入门控机制改进得到, RNN[15] 能够很好地处理不固定长度并且有序的输入序列. RNN 前向传播过程如图 3 所示, 网络参数权重的更新不仅仅依赖每一时刻t样本输入x_t对参数w的调整, 而且依赖t时刻之前计算并保存的隐含状态h_{t-1}对参

数的调整. 与传统的 RNN 相比, LSTM[16] 本质上还是基于t时刻的输入x_t和$t-1$时刻的隐状态h_{t-1}来计算t时刻的输出y_t和t时刻的隐状态h_t. 但是由于门控机制的加入, LSTM 网络更适合处理长依赖问题, 更加容易学习到工控网络周期性的规律, 并且容易识别由多个数据包共同作用引起的攻击类型.

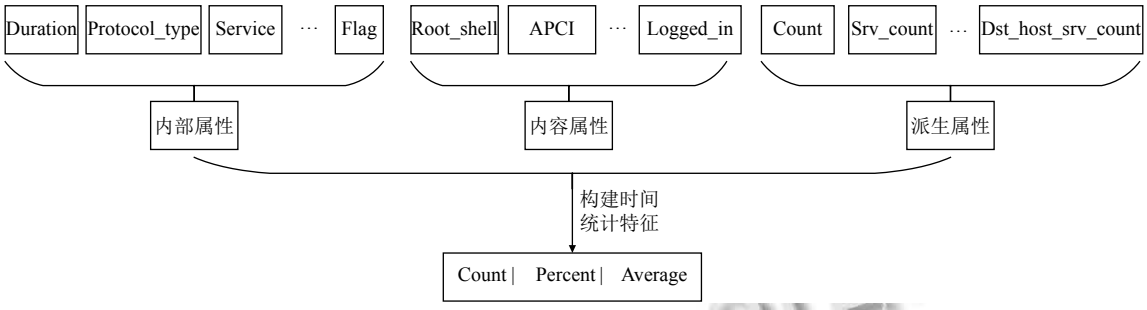

图 2 特征构造流程

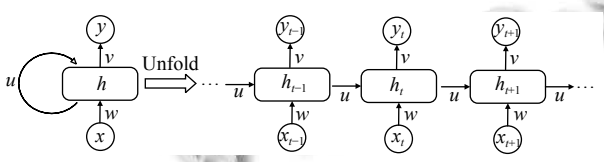

图 3 RNN 前向传播过程

本文提取数据包字段并构造了 12 个有效的时间统计特征, 网络模型在t时刻的结构为一个简单的前馈神经网络, 整体的网络结构如图 4 所示, 有 N 个前馈神经网络组成, 不同时刻的前馈神经网络通过隐藏层神经元传递依赖关系. 每层的前馈神经网络分为 3 层, 分别是包含 12 个神经元节点的输入层 (Input Layer), 含有 64 个神经元节点的隐藏层 (Hidden Layer), 含有 12 个神经元的输出层 (Output Layer), 在训练过程中, 前 N 个时刻的流量数据包用于预测 N+1 时刻的流量统计值, 即前 N 个时刻为样本特征, 第 N+1 个时刻为样本标签.

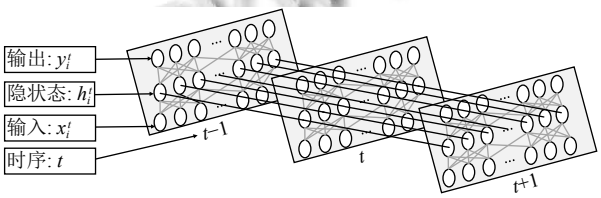

图 4 LSTM 神经网络时间展开图

3.2 参数更新过程

LSTM 网络相比 RNN 增加了存储单元用来存储长期记忆, 增加了输入门用来记忆 t 时刻的输入信息, 新来一个样本, 并不会完全学习记忆其中的特征, 而是自动学习除其中有多少有用信息可以用于 N+1 时刻的预测. 遗忘门用来选择性的忘记过去的某些信息, 起控制内部信息的作用. 输出门起控制输出信息的作用, 3 个门控单元的加入让 LSTM 网络在用梯度下降算法更新参数时不易于陷入梯度消失的问题, 3 个门的逻辑结构如图 5 所示.

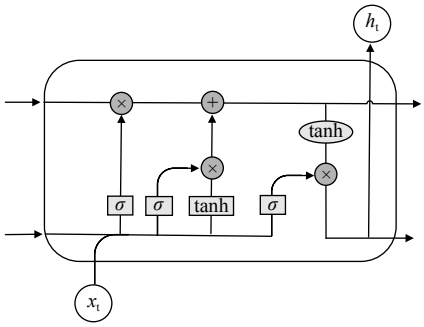

图 5 LSTM 网络门控机制

输入门输入 15 分钟以内 180 个样本的时间统计值, 15 分钟为滞后历史特征数值, 在训练过程中是一个超参数, 经过多组训练实验得到最优滞后历史特征, 对滞后历史特征数值的选择如表 1 所示, 可以发现, 当滞后历史特征为 15 分钟时, 模型在验证集上的损失最低, 表面用前 15 分钟的流量去预测下一时刻流量的时间统计特征最准确, 本文以 5 s 为最小单位, 在预测流量时, 预测下一时刻 (5 s 内) 的流量统计特性. 网络内部输入门的计算过程为

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

其中, σ为 Sigmoid 激活函数. 遗忘门、输出门和输入

门计算方式一样, 细胞状态C_t用于长期记忆, 更新过程为:

$$C_t = f_t * C_{t-1} + i_t * C_t \tag{2}$$

隐状态h_t用于短期记忆, 更新过程为:

$$h_t = o_t * \tanh(C_t) \tag{3}$$

其中, o_t为输出门的输出, tanh 为双曲正切激活函数.

表 1 滞后历史特征和隐藏层神经元节点数训练情况

滞后历史特征 (分钟)	隐藏层神经元节点数	Train_loss (训练误差)	Validation_loss (验证误差)
10	600	0.84	0.75
12	800	0.91	0.87
15	960	0.98	0.97
18	1100	0.98	0.95
20	1200	0.98	0.93

本文的隐藏层神经节点有 960 个, 网络输入的是一个三维向量 [640,180,12], 第一维 batch_size 的含义是一次性将 640 个样本序列, 输入到网络中进行训练, 使用梯度下降的方法完成一次误差反向传播和参数更新, 第二维 time_step 的含义是用前 180 个样本去预测下一时刻的流量值, 第三维 input_size 是单个样本的维度. 网络的输出是一个二维向量 [640×180, 12], 第一维代表输出 (预测) 的时刻流量值, 第二维代表单个样本的维度. 网络的输出为数值型数据, 所以损失函数采用均方误差损失函数[17], 定义为

$$MSE(y, y') = \frac{\sum_{i=1}^{n}(y_i - y_i')^2}{n} \tag{4}$$

其中, y为样本标签, y'为模型预测值, 输出值为 1×12 的向量, 图 6 为网络输出层的数据流图, 隐藏输出为输出层的输入, 经过 reshape 后和输出层权重进行点积运算, 加上偏置后得到 115 200 个样本的预测值.

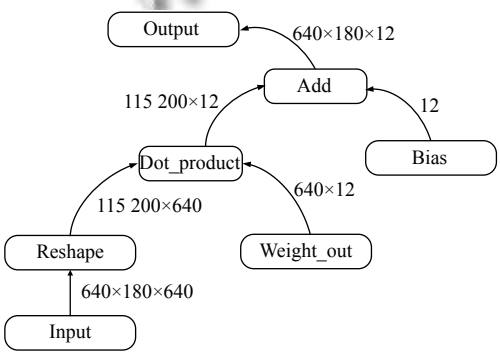

图 6 网络输出层数据流图

4 实验设计与结果分析

本文训练模型所用的数据采集自东北电力公司某子网, 利用 C++库函数 libpcap 对数据包进行捕获和深度解析, 对捕获到的数据包在时间维度上进行整合, 对时间间隔为 5 s (慢速攻击标准) 内的流量报文构造统计特征生成一个样本, 数据集的大小为 4.26 GB, 将数据集按照采集时间分为训练集和验证集, 训练集和数据集的比例为 70%:30%, 由于时间序列的原因, 划分数据集不能随机打乱, 而是按照采集流量的时间线, 把前 70% 的数据包划分为训练集, 后 30% 的数据包划分为验证集, 供模型训练和验证其有效性[18].

4.1 模型训练过程

模型训练过程中, 网络参数可以由训练得到, 滞后历史特征和隐藏层神经节点个数两个超参数通过网格调参的方式选取最优组合, 通过多轮训练的结果, 如表 1 所示, 可以发现, 最优组合为滞后历史特征的值为 15 分钟, 隐藏层的神经元节点数的值为 960 个. 模型每更新 500 次参数后计算一次训练误差和验证误差, 在迭代到第 19 轮时, validation_loss (验证误差) 达到最小, 在最优组合的超参数下, 模型在验证集上的准确率可以达到 97%, 图 7 为模型的 validation_loss 下降过程, 从图 7 中可以看出, 从第 19 次迭代后, 模型的 validation_loss 不再下降.

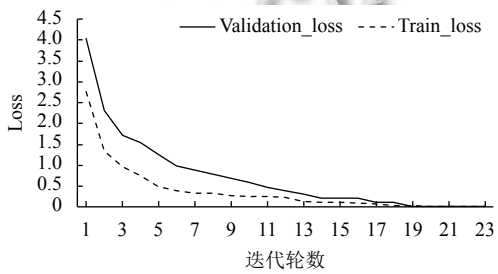

图 7 训练和验证损失

4.2 实验结果对比

表 2 列举出了多种主流算法对工控网络异常流量的识别率、误报率和识别效率, 可以发现, 本文算法在识别率和识别效率均优于半监督的 K-means 算法、单类支持向量机 (One Class Support Vector Machine, OCSVM) 和 BP 神经网络, 相比卷积神经网络方法, 本文算法误报率稍高, 但是识别效率却快了几倍. 总体而言, 本文算法结合工控网络周期性强和流量报文具有时序的特点, 使用 LSTM 模型取得了较好的效果.

表 2 各类算法测试结果对比

指标	K-means 聚类	OCSVN	BP神经网络	卷积神经网络	本文算法
识别率(%)	87.01	88.62	92.37	97.88	97.67
误报率(%)	12.99	10.67	8.05	3.39	9.37
识别用时(s)	21	18	24	26	6

5 总结

本文以工控网络中的电力系统网络为研究对象, 使用 LSTM 算法识别工控网络流量异常, 结合工控网络场景相较单一和周期性的特点, 采集流量后对解析的数据包字段解析重构时间统计特征, 采用时序预测的方式识别流量异常, 通过实验可以发现, 能有效识别出异于正常情况的网络波动, 由于提前预测出正常流量的特征值, 算法在异常流量的识别效率上优于传统识别方法, 有利于技术人员尽早发现异常做出相应的安全防护措施, 提高工控网络在入侵检测方面的安全性. 本文提出的时序预测模型虽然在识别准确率和识别效率相较其它算法有所提升, 但是时序预测模型要求流量数据具有周期性这一特点, 并且模型的最终效果非常依赖训练前期的特征构造, 目前特征构造中使用计数、百分比和均值统计指标, 后续为了进一步提高模型的识别率, 降低模型的误报率, 会在特征构造中加入其它的统计指标.

参考文献

1 周民军. 工控网络现状与安全分析. 现代工业经济和信息化, 2017, (15): 61–62.

2 吴震生. 基于工控协议防火墙的脆弱性研究. 自动化与仪表, 2019, 34(8): 105–108.

3 崔秀帅. 智能变电站报文安全及其实时性研究 [硕士学位论文]. 哈尔滨: 哈尔滨工业大学, 2016.

4 倪震. 电力工控网络安全风险分析与预测关键技术研究 [博士学位论文]. 南京: 南京理工大学, 2018.

5 安攀峰. 基于 SVM 的工业控制网络入侵检测方法应用研究. 电子世界, 2017, (1): 154, 156.

6 刘进, 卢安文, 陈家佳. 基于模糊聚类算法的工控网络控制故障检测方法研究. 计算机测量与控制, 2015, 23(3): 681–684. [doi: 10.3969/j.issn.1671-4598.2015.03.002]

7 祝士祥. 基于深度学习的工控网络异常检测研究和实现 [硕士学位论文]. 北京: 北京邮电大学, 2017.

8 张艳升, 李喜旺, 李丹, 等. 基于卷积神经网络的工控网络异常流量检测. 计算机应用, 2019, 39(5): 1512–1517. [doi: 10.11772/j.issn.1001-9081.2018091928]

9 张望妮, 牛瑞. 利用 IEC104 远动规约解决实际问题. 电子技术与软件工程, 2018, (21): 159–160.

10 江泽鑫. IEC60870-5-104 规约安全性分析及攻击实验. 信息技术与网络安全, 2018, 37(10): 1–4, 14.

11 张照宇. 时序事件分析与研究 [硕士学位论文]. 西安: 西安电子科技大学, 2019.

12 曾豪. 基于 LSTM 的环境污染时间序列预测模型的研究 [硕士学位论文]. 武汉: 华中科技大学, 2019.

13 王伟. 基于深度学习的网络流量分类及异常检测方法研究 [博士学位论文]. 合肥: 中国科学技术大学, 2018.

14 卜国卿. 网络流量异常检测技术研究与实现 [硕士学位论文]. 成都: 电子科技大学, 2018.

15 Liu RR. Short-term traffic flow prediction based on deep circulation neural network. Proceedings of the 2nd International Seminar on Artificial Intelligence, Networking and Information Technology(ANIT 2018). Shanghai, China. 2018. 580–583.

16 Navares R, Aznarte JL. Predicting air quality with deep learning LSTM: Towards comprehensive models. Ecological Informatics, 2020, 55: 101019. [doi: 10.1016/j.ecoinf.2019.101019]

17 董巧玲. 不同误差影响模型下总体最小二乘法在多元线性回归中的应用研究 [硕士学位论文]. 太原: 太原理工大学, 2016.

18 陈凯. 深度学习模型的高效训练算法研究 [博士学位论文]. 合肥: 中国科学技术大学, 2016.