基于BILSTM与改进PSO算法的农业物联网入侵行为检测

李　昂

（九江职业大学信息工程学院，江西九江 332000）

【摘要】为了提升农业物联网的安全性，针对农业物联网的入侵行为特点，设计了基于BILSTM与改进粒子群优化算法的入侵检测方法。提出一种改进粒子群优化算法对BILSTM模型参数进行优化的算法，采用优化后的BILSTM模型对农业物联网网络入侵行为进行时间特征提取，使用Sofmax分类器进行分类。通过模拟实验，测试了农业物联网入侵行为检测方法的实际效果。实验表明，在入侵行为种类增加的情况下，该方法相比传统方法具有更高的检测率和更低的误检率，能够更加有效地针对农业物联网的入侵行为进行检测。

【关键词】双向长短期记忆；粒子群优化；农业物联网；入侵行为检测

【doi:10.3969/j.issn.2095-7661.2022.04.003】

【中图分类号】TN918　　【文献标识码】A　　【文章编号】2095-7661(2022)04-0009-03

Intrusion Detection Method of Agriculture IoT Based on Bidirectional LSTM and Improved PSO Algorithm

LI Ang

(College of Information Engineering, Jiujiang Vocational University, Jiujiang, Jiangxi, China 332000)

Abstract: To improve the security of agriculture Internet of Things, an intrusion detection method based on bidirectional LSTM and improved particle swarm optimization algorithm is designed according to the intrusion behavior characteristics of agriculture Internet of things. An improved particle swarm optimization algorithm is proposed to optimize the parameters of the bidirectional LSTM model. The bidirectional long-term and short-term memory neural network is used to extract the temporal characteristics of the intrusion behavior, and the sofmax classifier is used for classification. Through the simulation intrusion experiment, the detection effect of agriculture Internet of things intrusion detection method is tested. The experiment shows that the method in this paper has higher detection rate and lower false detection rate than traditional methods when the types of intrusion behaviors increase, and it can detect the intrusion behaviors of the agricultural Internet of Things more effectively.

Keywords:bidirectional LSTM; particle swarm optimization; agriculture IoT; intrusion detection

随着信息技术与物联网技术不断发展，农业物联网技术已成为实现农业智能化、网络化与自动化的重要技术手段。农业物联网能够为农作物生长的环境监测、农业设备远程控制与水产畜牧养殖提供有力的保障体系，提升农业数据监测传感器网络运行时的安全性与可监控性。农业物联网一旦遭受入侵将会产生难以估量的危险与经济损失，因此研究对农业物联网入侵行为的检测方法显得尤为必要。入侵检测技术一般分为基于特征的入侵检测与基于异常的入侵检测两种[1]，传统的检测方法有神经网络、主成分分析、支持向量机等统计学方法，这些方法需要对入侵行为的特征进行人工选择，在面临一些新的且复杂多变的入侵行为时存在误判率升高的现象。近年来，有许多关于物联网入侵检测方法的研究，有学者提出一种基于最小二乘支持向量机的物联网入侵检测方法[2]，以改进的K-means数据稀疏算法优化LSSVM分类器，能较好地适应较为苛刻的物联网资源环境。有学者提出一种单支持向量机检测算法[3]，使用二元粒子群优化算法对LightGBM算法进行优

[收稿日期] 2022-06-23

[作者简介] 李昂(1990—)，男，江西九江人，九江职业大学讲师，硕士，研究方向：机器学习、网络安全。

[基金项目] 2020年江西省教育厅科学技术研究项目“基于微服务架构的农业物联网云端数据监测系统研究”(项目编号：GJJ203910)。

化，对小样本数据有较高的准确性。有学者提出一种基于深度强化学习算法检测工业物联网中的入侵行为[4]，该方法基于LightGBM对工业物联网数据进行特征选择，使用PPO2算法构建入侵检测模型，采用ReLU进行分类，该方法能应对工业物联网中多种类型的网络攻击。文献[5]提出一种基于机器学习框架的入侵检测算法，采用贝叶斯优化算法与决策树分类模型相结合，能有效检测针对物联网设备的僵尸网络攻击。文献[6]以轻量级CNN为基础提出了一种Page-Net模型，可在布局网络参数时匹配流量特征分布的特点，能在小规模参数下检测物联网DDoS攻击并获得很好的检测效果。目前关于物联网入侵检测的研究主要集中于工业、智能家居等领域中，有关农业物联网入侵检测的研究较少。

农业物联网系统较为复杂，系统的任何节点遭受入侵都会威胁整个物联网系统。农业物联网所处环境也与工业物联网或智能家居系统存在很大不同，常见的工业物联网或智能家居系统都处于密闭的环境中，而农业物联网的传感器节点经常出现在开放的空间内，如农业大田、林场以及畜牧场等，这使得农业物联网更容易遭受到入侵攻击。为了检测针对农业物联网系统的入侵行为，降低对农业物联网入侵的误判率，本文设计了一种基于双向LSTM与改进粒子群优化算法的入侵检测方法。使用改进粒子群优化算法对双向LSTM网络模型参数进行优化，利用双向LSTM来获取特征的前后关联与局部特性，提升了农业物联网入侵行为的检测准确率。

1 相关理论和方法

1.1 BILSTM

BILSTM（Bidirectional Long-term and Short-term Memory neural network，双向长短期记忆神经网络）是一种基于循环神经网络提出和改进的人工神经网络[7]，又名双向LSTM。LSTM通过增加输入门、遗忘门和输出门来改变自循环的权重，弥补了传统循环神经网络模型中梯度消失和梯度爆炸的缺陷[8]。此外，LSTM能够更好地处理非线性时间序列数据。LSTM模型的计算公式如公式(1)所示。

$$\begin{cases} i_t = \sigma(W_{xi}x_t + U_{hi}h_{t-1} + b_i) \\ g_t = \tanh(W_{xg}x_t + U_{hg}h_{t-1} + b_g) \\ f_t = \sigma(W_{xf}x_t + U_{hf}h_{t-1} + b_f) \\ O_t = \sigma(W_{xo}x_t + U_{ho}h_{t-1} + b_o) \\ c_t = f_t {}^{\mathrm{O}} c_{t-1} + i_t {}^{\mathrm{O}} g_t \\ h_t = \tanh(c_t) {}^{\mathrm{O}} q_t \end{cases} \tag{1}$$

式中i_t、f_t与O_t分别为输入、遗忘与输出门，g_t为输入更新值，b_i、b_g、b_f和b_o为每个门的偏差，W为前馈权重，U为循环权重。模型有两个激活单元，输入更新和输出激活，其中使用tanh激活函数具有更好的功能效果。

BILSTM由前向LSTM与后向LSTM两个序列构成，与单向LSTM相比具有更好的预测效果。BILSTM模型的计算公式如式(2)所示：

$$h_i = \left[\overrightarrow{h_i} \oplus \overleftarrow{h_i}\right] \tag{2}$$

$\overrightarrow{h_i}$表示前向LSTM序列的输出，$\overleftarrow{h_i}$表示后向LSTM序列的输出，h_i为双向LSTM输出。

1.2 粒子群优化算法改进

PSO（Particle Swarm Optimization，粒子群优化）算法具有很强的解决优化问题的能力，但是传统的PSO算法在处理优化问题时缺乏有效的参数控制。本文主要改进传统粒子群优化算法中惯性权重的选取分配与学习因子计算方法。常用的惯性权重分配策略采用线性递减的方式，即权重随着迭代次数线性下降。这种策略的不足之处在于，PSO的局部搜索能力会随着迭代次数的线性减少而降低，从而影响算法的优化性能。使用非线性递减分配方法可以改善这一点，改进后的惯性权重公式如式(3)所示：

$$W = W_{\max} - (W_{\max} - W_{\min})\sqrt{\frac{i}{num\_\max}} \tag{3}$$

式中$W_{\max}$和$W_{\min}$分别为最大惯性权重和最小惯性权重。i是当前的迭代次数，而$num_\max$是最大的迭代次数。

对学习因子进行改进，设置学习因子c_1和c_2，分别用于调整将移动到个体最佳位置和全局最佳位置的粒子步长。在实际应用中，随着迭代过程的推进，通常需要c_1的值从大到小，以在早期迭代中加快搜索速度，提高全局搜索能力。并且c_2的值需要从小到大改变，以方便迭代后期的局部细化搜索，同时提高精度。但是标准PSO通常设置$c_1=c_2=2$，这不能满足实际应用的要求。因此，引入正弦函数来改进学习因子，如下式所示：

$$\begin{cases} c_1 = 2\sqrt{1 - \sin\left(\frac{\pi}{2} * \frac{i}{num\_\max}\right)} \\ c_2 = 2\sqrt{\sin\left(\frac{\pi}{2} * \frac{i}{num\_\max}\right)} \end{cases} \tag{4}$$

2 农业物联网入侵行为检测模型

利用改进PSO算法优化后的BILSTM网络模型进行提取特征，通过分类器对特征进行分类，从

而实现农业物联网入侵行为检测，具体步骤如图1所示。

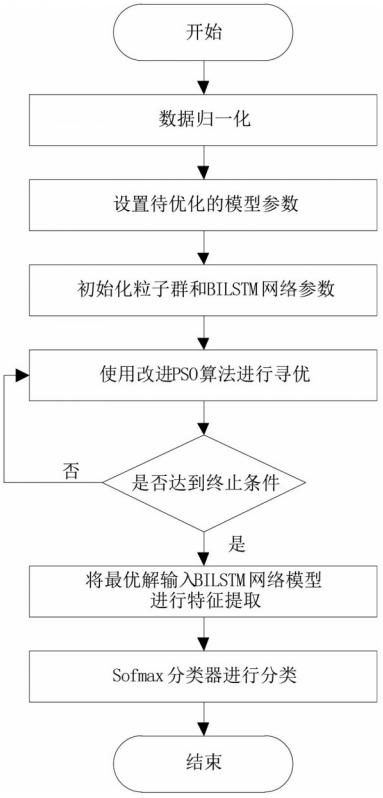

图1　农业物联网入侵检测模型图

模型算法实现流程：

1）数据预处理，对经过清洗的数据进行归一化处理。归一化采用min-max标准化方法，计算公式如式（5）所示。

$$Z = \frac{Z - Z_{\max}}{Z_{\max} - Z_{\min}} \tag{5}$$

2）对准备优化的模型参数进行初始化，确定种群大小、粒子维度、迭代次数、学习因子、惯性权重，定义待优化参数的区间。

3）随机生成粒子，初始化粒子的位置与速度。设置粒子的适应度函数，计算公式如式（6）所示。式中N代表验证样本的数量，x_t代表验证样本的实际值，$\hat{x}_t$代表验证样本的拟合值。选择获得的双向LSTM模型验证数据的均方根误差作为个体适应度函数，并以最小适应度值作为PSO算法的迭代目标。利用1.2节所述的改进的PSO算法来选择最优的参数。

$$F = \sqrt{\frac{1}{N}\sum_{t=1}^{N}(x_t - \hat{x}_t)^2} \tag{6}$$

4）更新粒子的速度和位置，计算每个粒子的适应度值，确定个体最优适应度值和群体最优适应度值。在迭代过程中，粒子的速度与位置根据这两个最优值进行持续更新。

5）将经过改进PSO算法优化后所得到的参数值代入双向LSTM神经网络模型，将测试样本输入模型进行特征提取。

6）使用Sofmax分类器[9]进行分类，检测出异常入侵行为。

3　实验结果与分析

本文实验数据来源于正常与模拟入侵环境下农业物联网系统的网络流量数据。将数据集的60%划分为训练集、剩余的40%划分为验证集与测试集，验证集与测试集各20%。通过将SVM、LSTM、BILSTM与本文方法的对比实验来验证检测性能。由表1的数据可以看出，本文所提方法的检测准确率达到91.6%，在准确率、精确率与召回率方面均优于传统方法，验证了本文所提算法的有效性。

表1　四种检测方法的实验结果对比表

方法	评价指标		
	准确率（%）	精确率（%）	召回率（%）
SVM	82.4	85.6	80.3
LSTM	87.7	88.5	86.5
BILSTM	90.4	92.3	94.2
本文方法	91.6	93.7	95.4

图2为四种不同方法检测多种入侵行为的误检率对比。在农业物联网中，入侵行为包含DDoS攻击、DoS攻击、操作系统服务扫描攻击、漏洞利用攻击和数据过滤攻击等。从实验结果中可以发现，随着入侵行为种类数量的增加，本文所提方法的误检率变化相对较为平稳，最高误检率为6.3%。而其他方法的误检率随着入侵行为种类的增加而大幅增加，最高可达到19.8%。由此可见，本文所提方法对于多种入侵行为的检测具有较低的误检率，能够更好地提升农业物联网的安全性。

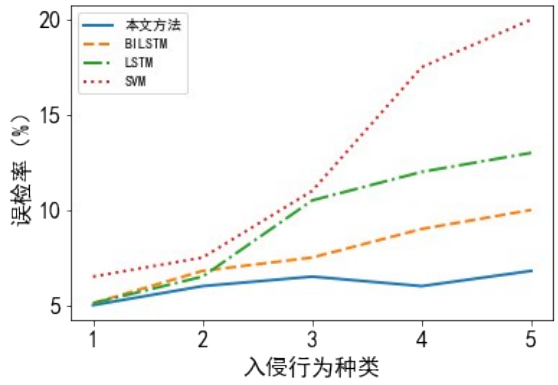

图2　不同方法对于五种入侵行为的误检率

4　结语

本文针对农业物联网的入侵行为特点进行研究，设计了基于双向LSTM与

（下转第46页）

丝不苟、追求卓越。

2.4 充分利用新媒体，弘扬优秀传统文化

大众传媒信息量大、传播速度快、覆盖面广、吸引力强，生动的画面、动人的故事，往往更容易引起学生的共鸣，进而达到既定的教育目标。通过重温红色经典影视剧，对学生进行优秀传统文化教育，是弘扬优秀传统文化的有效手段。例如，定期组织学生观看《开国大典》《亮剑》等历史题材的经典影视剧，有助于学生树立正确的价值观与人生观，增强自身的文化素养，丰富学生精神生活，陶冶身心、提升个人道德修养。新媒体传播方式更加主动、灵活和自由，学生可以利用碎片时间随时浏览，实现快速获取和更新。学校可以通过官网、公众号等新媒体方式，定期投放传统文化建设专栏，利用碎片化的时间加强学生对传统文化的了解，提高家长对学生学习的关注，把有意义的事做得更有意思，让正能量更强劲、更生动[5]。

3 结语

班级建设对于提高班级管理水平和促进学生发展十分重要，将中华优秀传统文化融入职业院校班级管理，开展传统文化浸润教育，不但有利于优秀传统文化传承与发展，更能增强学生的民族意识，培养学生良好的道德品质、职业精神以及社会主义核心价值观，使学生真正成为德智体美劳全面发展的社会主义建设者和接班人。

【参考文献】

[1]刘小炼.习近平关于传统文化重要论述研究[D].重庆:西南大学,2019.

[2]黄冬梅.中华优秀传统文化融入中职艺校班级管理探究[J].广西教育,2021(18):93-94.

[3]丁秀荣.中华传统文化:班级文化建设的根基[J].现代教育科学,2019(2):26-29.

[4]黄水莲.经典文学作品的思想政治教育功能研究[J].湖南邮电职业技术学院学报,2020(1):112-114.

[5]宋璐.积极心理学视角下的班级建设[J].速读(下旬),2020(2):241.

（上接第11页）

改进粒子群优化算法的入侵检测方法。提出一种改进粒子群优化算法对双向LSTM模型参数进行优化，采用双向LSTM来检测农业物联网网络异常。实验表明，本农业物联网入侵检测方法具备较优的检测效果，能使农业物联网的安全性得到提升，未来将进一步优化算法模型以提升检测效率。

【参考文献】

[1]王振东,张林,李大海.基于机器学习的物联网入侵检测系统综述[J].计算机工程与应用,2021(4):18-27.

[2]魏琴芳,吕博文,胡向东.基于稀疏化LSSVM的物联网轻量级入侵检测方法[J].重庆邮电大学学报(自然科学版),2021(3):475-481.

[3]刘靖宇.基于支持向量机的工业物联网入侵检测研究[D].沈阳:中国科学院大学(中国科学院沈阳计算技术研究所),2021.

[4]李贝贝,宋佳芮,杜卿芸,何俊江.DRL-IDS:基于深度强化学习的工业物联网入侵检测系统[J].计算机科学,2021(7):47-54.

[5]Injadat M N, Moubayed A, Shami A. Detecting Botnet Attacks in IoT Environments: An Optimized Machine Learning Approach[C]. 2020 32nd International Conference on Microelectronics (ICM),2020.

[6]韩长江.基于深度学习的物联网DDoS攻击流量检测算法设计与实现[D].济南:山东大学,2020.

[7]麻文刚,张亚东,郭进.基于LSTM与改进残差网络优化的异常流量检测方法[J].通信学报,2021(5):23-40.

[8]陈解元.基于LSTM的卷积神经网络异常流量检测方法[J].信息技术与网络安全,2021(7):42-46.

[9]龙浩,张书奎,张力.群智感知中基于维诺单元的隐私保护方法[J].计算机工程,2020(5):181-186,192.