计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2023,32(2):274−280 [doi: 10.15888/j.cnki.csa.008989]

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

基于深度学习的网络流量异常识别与检测①

邓华伟[1,2], 李喜旺[1,3]

[1](中国科学院 沈阳计算技术研究所, 沈阳 110168)
[2](中国科学院大学, 北京 100049)
[3](辽宁省智能电网云计算专业技术创新中心, 沈阳 110168)
通信作者: 李喜旺, E-mail: lixw@sict.ac.cn

摘　要: 针对传统的工控网络流量数据在复杂网络环境下特征维度高, 特征处理复杂度高, 模型检测效率低等问题, 本文使用了一种基于随机森林 (random forest, RF) 和长短期记忆网络 (long short-term memory, LSTM) 结合的流量异常识别与检测方法. 首先使用随机森林算法计算流量特征的重要度评分, 筛选出重要特征, 剔除冗余特征, 然后使用 LSTM 进行异常流量的识别与检测. 为了评估模型的有效性与优越性, 本文使用准确率、精确率、召回率和 *F*1-score 进行模型评价, 并与传统的机器学习方法 Naive Bayes、QDA、KNN 算法进行对比. 实验结果表明, 在公开数据集 CIC-IDS-2017 中, 异常流量识别的总体准确率达 99%. 与传统的机器学习算法相比, 该方法有效地提高了复杂网络环境下异常检测的准确性和效率, 在工业控制网络安全和异常检测方面具有实际应用价值.

关键词: 异常检测; 随机森林; 特征选择; 深度学习; 长短期记忆网络

引用格式: 邓华伟,李喜旺.基于深度学习的网络流量异常识别与检测.计算机系统应用,2023,32(2):274–280. http://www.c-s-a.org.cn/1003-3254/8989.html

Abnormal Network Flow Identification and Detection Based on Deep Learning

DENG Hua-Wei[1,2], LI Xi-Wang[1,3]

[1](Shenyang Institute of Computing Technology, Chinese Academy of Sciences, Shenyang 110168, China)
[2](University of Chinese Academy of Sciences, Beijing 100049, China)
[3](Liaoning Smart Grid Cloud Computing Technology Innovation Center, Shenyang 110168, China)

Abstract: Aiming at the problems of the high dimension of features, high complexity of feature processing, and low efficiency of model detection of traditional industrial control network traffic data in complex network environments, this study uses an abnormal network flow identification and detection method based on random forest (RF) and long short-term memory (LSTM) network. Firstly, the random forest algorithm is used to calculate the importance score of flow characteristics, screen out important features, and eliminate redundant features. Then, LSTM is adopted to identify and detect abnormal flows. In order to evaluate the effectiveness and superiority of the model, the accuracy, precision, recall, and *F*1-score are used in this study to evaluate the model, and the model is compared with traditional machine learning methods including Naive Bayes, QDA, and KNN algorithms. The experimental results show that the overall accuracy of abnormal flow identification reaches 99% on the CIC-IDS-2017 public data set. In addition, compared with traditional machine learning algorithms, the proposed method has effectively improved the accuracy and efficiency of anomaly detection in complex network environments, and it has practical application value in industrial control network security and anomaly detection.

Key words: anomaly detection; random forest (RF); feature selection; deep learning; long short-term memory (LSTM) network

① 基金项目: 辽宁省“兴辽英才计划”(XLYC2019019)
收稿时间: 2022-06-04; 修改时间: 2022-08-15; 采用时间: 2022-09-28; csa 在线出版时间: 2022-11-16
CNKI 网络首发时间: 2022-11-18

工业互联网在经济发展和国家发展中具有重要的战略地位. 随着信息化的发展普及, 传统的工业互联网的暴露程度不断增加. 随着近年来网络攻击的泛滥, 网络攻击呈现多样化、复杂化、高强度的趋势发展. 2021 年 7 月份, 国家互联网应急中心 (CNCERT) 发布《2021 年上半年我国互联网网络安全检测数据分析报告》指出, 2021 年上半年, 恶意程序样本捕获数量约 2 307 万个, 日均传播次数达 582 万余次, 我国境内感染计算机恶意程序的主机数量约 446 万台, 同比增长 46.8%, 境内目标遭受大量的 DDoS 攻击, 网页仿冒、网站后门、网页篡改等安全事件依旧频发, 煤炭、石油、电力、城市轨道交通等重点行业存在高危漏洞, 工业互联网设备面临诸多安全威胁[1].

针对工业互联网中重要的业务系统进行异常流量的检测, 提前进行预防与研判, 对工业互联网的攻击防御具有重要的作用. 基于业务系统的流量特征, 对业务系统中的异常流量行为进行入侵检测, 不仅可以增强系统的防御能力, 而且可以在恶意行为潜藏或发生时及时发现并对进一步采取防御措施提供帮助. 此外, 流量异常检测能够发掘出业务系统的网络流量发展趋势, 使得相关部门能够网络规划和网络资源进行优化更新, 进而有效防御网络威胁.

1 流量异常识别与检测

在工控系统中, 异常识别与检测是一种主动的安全防御技术, 可以弥补防火墙等传统防御技术的不足, 保证重要业务系统的安全. 近年来, 异常检测的方法主要有以下几种.

基于传统机器学习的方法. 机器学习模型方法包括 LightGBM[2]、XGBoost[3]、K-means 等, 这类方法一般将时序问题转换为监督学习, 通过特征工程和机器学习方法进行异常检测. 传统的机器学习方法在异常流量的检测方面取得了一定的效果. 王智慧等人[4] 为了解决传统攻击检测漏检率、误检率高的问题, 提出了基于 LightGBM 的异常流量检测模型, 该模型首先使用 KPCA 提取异常流量的关键特征, 将高维度的数据进行降维, 而后使用 LightGBM 模型进行异常流量的检测, 经验证该方法可以有效地实现工控系统异常流量的动态检测. 但该模型泛化能力不足, 无法检测未知的异常攻击流量. Jiang 等人[5] 提出了 PSO-XGBoost 模型, 模型利用 PSO (粒子群算法) 良好的搜索能力, 对 XGBoost 相关参数进行自适应优化, 可以有效提高网络入侵检测的效率与准确率. 但是粒子群算法波动较大, 粒子数量或者迭代次数对算法影响较大, 若设置不合理会产生局部最优解或者寻优时间过长的问题. 在入侵检测方面, K-means 是最常用也是最为经典的基于划分的聚类算法. 其思想是在空间中按照一定策略选择 k 个点作为簇的初始中心, 然后基于这 k 个点对数据进行划分, 不断迭代, 更新每个簇的中心点, 不断重新划分, 直至到达最大迭代次数或者到最好的聚类结果[6]. 王胜等人[7] 针对 IEC61850 智能变电站专有协议, 使用了一种基于信息熵的特征选取方法, 而后利用 K-means 聚类算法完成了对异常流量的检测分析集相关分析. 虽然 K-means 算法原理简单, 但是存在收敛速度慢、算法时间复杂度较高的问题, 且对噪声和离群点非常敏感. 传统的机器学习方法是浅层学习方法[8], 难以捕捉到重要信息, 局限性较大, 无法充分挖掘数据之间的特征与关联, 泛化能力较弱, 十分有限.

基于深度学习的方法. 深度学习算法能够充分挖掘和提取数据之间的潜在特征, 可以做复杂的非线性映射, 具备强大的表征学习能力[9]. 在流量异常检测、电力负荷预测等领域广泛使用且表现出良好的性能以及准确率. 深度学习模型方法, 包括 LSTM/GRU、wavenet、1D-CNN、Transformer 等. 深度学习中的 LSTM/GRU 模型, 就是专门为解决时间序列问题而设计的, 但是 CNN 模型是本来解决图像问题的, 但是经过演变和发展也可以用来很好地解决时间序列问题. Transformer 是 2017 年被提出的时序模型, 该模型基于 multi-head attention 结构具备同时建模长期和短期时序特征的能力. 工控网络流量信息具有周期性和时序性的特性, 针对这一特性, 田伟宏等人[10] 提出了一种基于 LSTM 的异常流量识别与检测的模型, 该方法提前对流量数据值进行预测, 在保证识别率较高的情况下, 有效提高了模型的检测效率. 但是该方法需要依赖于人工的特征提取, 特征处理较为复杂, 对模型效果影响较大. 杜浩良等人[11] 提出了一种融合 CNN 和 LSTM 的混合异常检测模型, 该模型使用 CNN 提取数据空间特征, LSTM 提取数据时序特征, 充分挖掘流量数据的结构化特点和时空特征, 有效提高了模型的准确率, 但是 CNN 具有较多的权值、阈值, 参数对模型影响较大, 选择不当容易导致陷入局部极小值解. 杨月麟等人[12] 基于 Transformer 提出一种流量异常检测模型, 该模型

很好地解决了网络数据流量远程依赖以及数据样本不平衡的问题. 经验证该模型在准确率以及检测时间方面均有优异的表现. 李梅等人[13] 在 CNN 和 LSTM 的基础上融入了注意力机制, 在 CNN 中加入注意力机制可以抽取重要细粒度特征, 然后经由 LSTM 抽取时序规律的粗粒度特征. 但是这种方法使得模型更为复杂, 使得模型时间复杂度高, 训练时间较长[14].

综上所述, 复杂多变的网络环境使得网络流量数据朝着高维度发展, 在面对高维度的特征数据时, 深度学习模型无法有效处理高维度数据, 导致模型效率低. 因此剔除冗余特征进行特征筛选, 是提高模型效率的重要方式. 综上本文提出了一种结合随机森林算法与 LSTM 模型的异常流量检测方法, 首先使用随机森林算法, 对网络流量的特征进行重要度评分, 选取相关性最高的特征, 充分提取流量信息的关键特征, 使用 LSTM 模型充分挖掘流量特征之间的关系, 进行流量异常的检测与识别, 提高系统异常检测的效率.

2 研究方法

2.1 随机森林

随机森林 (random forest, RF) 模型[15] 中包含很多决策树, 采用 Bootstrap 重抽样技术随机从数据集中采样以构造、训练模型中的每棵决策树, 最终将每个决策树进行组合, 然后通过投票方式得出最终结果. RF 对异常值和噪声具有较强的容忍度, 在面对海量高维的数据时, 能够在数据分析的同时得到特征的重要性评分 (variable importance measures, VIM)[16].

本文使用随机森林对流量特征进行重要度评分, 计算每个特征在随机森林中每个决策树上所做的贡献量, 即求解该特征在某个节点上, 分枝前后的基尼指数 (*Gini*) 差值, 对数据中包含的所有特征进行求解. 将单个特征基尼指数差值除以所有特征基尼指数差值, 得到某个特征归一化后的贡献量, 获得每个特征的重要性权重, 对特征之间的重要性权重进行比较、排序. *Gini* 指数的计算方法[17] 为:

$$Gini(p)=\sum_{k=1}^{K}p_k(1-p_k)=1-\sum_{k=1}^{k}p_k^2 \tag{1}$$

其中, K 表示有 K 个类别, p_k 表示第 k 个类型的权重.

每个特征 j 在节点 m 的基尼指数变化值使用 VIM_{jm} 表示, 其计算方法为:

$$VIM_{jm}^{Gini}=GI_m-GI_l-GI_r \tag{2}$$

其中, GI_l 和 GI_r 表示节点 m 分支后, 新产生的两个结点的基尼指数.

最后, 将特征 j 贡献量做归一化处理, 记为特征 j 的重要性评分:

$$VIM_j^{Gini}=\frac{VIM_j^{Gini}}{\sum_{i=1}^{c}VIM_i^{Gini}} \tag{3}$$

其中, VIM_j^{Gini} 是特征 j 的基尼指数 $\sum_{i=1}^{c}VIM_i^{Gini}$ 是所有特征的基尼指数差之和.

2.2 LSTM 模型

长短期记忆网络 (LSTM)[18] 于 1997 年由 Hochreiter 和 Schmidhuber 提出, 是一种改进的时间循环神经网络, 由于其特殊的网络结构, 适用于处理时序型数据. 传统的 RNN 中, 当连续数据的序列变长时, 会使展开时间步过长, 在反向传播更新参数的时候, 梯度要按时间步长连续相乘, 会导致梯度消失的问题. LSTM 中遗忘门、输入门等门控制单元的提出, 将短期记忆和长期记忆进行结合, 控制特征的流通与损失, 可以在一定程度上解决 RNN 无法处理长距离依赖导致的梯度消失问题. LSTM 包含 3 个门单元, 分别是输入门 i_t、遗忘门 f_t、以及输出门 o_t. 其中最重要的是遗忘门, 用于判断上一时刻中哪些记忆信息需要保留与丢失, 输入门判断此刻需要的记忆信息, 输出门用于决定输出的内容. 相关计算公式如式 (4)–式 (9) 所示:

$$i_t=\sigma(W_i\cdot[h_{t-1},x_t]+b_i) \tag{4}$$

$$f_t=\sigma(W_f\cdot[h_{t-1},x_t]+b_f) \tag{5}$$

$$o_t=\sigma(W_o\cdot[h_{t-1},x_t]+b_o) \tag{6}$$

$$C_t=(f_t*C_{t-1}+i_t*\tilde{C}_t) \tag{7}$$

$$h_t=o_t*\tanh(C_t) \tag{8}$$

$$\tilde{C}_t=\tanh(W_c\cdot[h_{t-1},x_t]+b_c) \tag{9}$$

其中, 式 (4) 表示输入门, 式 (5) 表示遗忘门, 式 (6) 表示输出门, 式 (7) 表示细胞态 (长期记忆), 式 (8) 表示记忆体 (短期记忆), 式 (9) 表示候选态 (新知识), W_i、W_f、W_o 为权重矩阵, b_i、b_f、b_o 为偏置项, x_t 为 t 时刻的输入信息, h_t 表示中间输出, tanh 表示双曲正切激活函数, σ 表示 Sigmoid 激活函数, LSTM 神经网络结构图如图 1 所示.

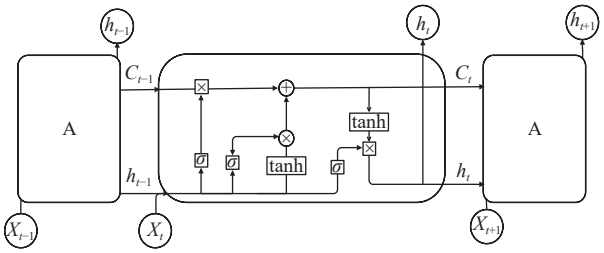

图 1 LSTM 网络结构

2.3 异常检测模型

综合随机森林与 LSTM 神经网络的特点, 以及工控网络流量的时序性和周期性特点, 本文尝试使用随机森林与 LSTM 进行入侵检测的识别. 本文模型主要有两部分组成, 其中随机森林部分负责特征提取, LSTM 网络部分作为流量分类器进行学习和分类, 进行异常流量的检测与分类. 本模型在面对高维度的数据特征时, 可以选择出重要度评分较高的相关特征以便更高效的用于异常流量的检测. 与现有的 CNN 相比, 两者均可用于特征提取, 但是 CNN 是一种反向传播算法, 对数据量的需求大, 且池化层的存在会导致许多有价值信息的丢失, 在面对高维数据时存在效率低等问题, 而随机森林实现简单, 能够处理高维度数据和平衡一些属性权重带来的误差[19], 模型的泛化能力强.

模型中首先使用随机森林, 针对高维度的流量特征进行特征选择, 根据不同阶段选择出最能体现流量特点的特征, 最终融合阶段特征使得选择的特征更具有代表性[20], 特征选择包括针对单个攻击类型的特征选择以及所有攻击类型汇总的特征选择, 重要度评分较高的特征作为返回向量包传送到 LSTM 系统, 作为 LSTM 的输入信息, LSTM 系统由 LSTM 层、Dense 层 (全连接层)、输出层组成, 对提取的特征向量包进行学习、处理, 计算属于每一类的概率, 最终得到分类结果. 为了防止过拟合, 可以使用 Dropout 舍弃一定概率的神经网络单元. 本模型异常检测的全流程如图 2 所示.

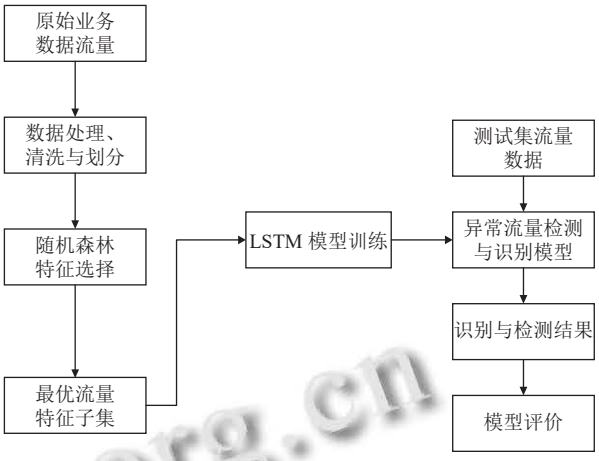

图 2 异常检测流程图

3 实验分析

3.1 实验环境

本文使用的软硬件环境为: Windows 10 操作系统, 基于 Python 3.7 的 TensorFlow 2.1 和 Keras 2.3.1 软件框架, AMD Ryzen 7 5800H@3.20 GHz CPU, 16 GB 内存, NVIDIA GeForce GTX 1650 显卡.

3.2 数据集预处理

为验证模型的有效性, 本文使用公开的 IDS 数据集 CIC-IDS-2017, 该数据集由加拿大通信安全机构 (CSE) 和网络安全研究院 (CIC) 合作公布. 相较于经典的 KDD99 数据集, 该数据集来源于真实世界, 使用的协议更加丰富, 包括 FTP、HTTP、SSH、Email 以及 HTTPS 协议[21], 共计 200 万余个标记流. 此外, 每个标记流包含 70 余条特征, 使用标签对正常流量或者攻击类型进行标注, 包含 DDoS、Port Scan、SSH-Patator 等 14 种攻击类型. 数据集中有些攻击类型数量较少, 不具备训练基础, 本文对一些攻击类型以及异常数据进行剔除. 采用文献 [22] 中的方式进行数据预处理, 将文本类型转换为数值类型. 为了解决数据不平衡的问题以及测试模型对单个攻击类型的效果, 本文针对每种攻击类型构造自己的数据集. 首先, 将原始数据集中周一至周五的流量信息进行预处理、汇总, 从汇总文件中提取出每种攻击类型, 选取正常标签数据对每种攻击类型数据进行补充完善, 使得正常类型: 攻击类型的比例在 7:3 左右, 数据集划分后攻击类型数量如表 1 所示. 为了验证模型总体识别的效果, 文中将所有异常攻击类型统一划分标签而后生成数据集, 并使用模型进行异常识别, 对模型总体效果进行验证.

本文针对每种攻击类型, 使用随机森林算法分别计算该攻击类型流量特征的重要度评分, 每个攻击类型选取 7 个重要度评分最高的特征, 对数据进行特征降维, 表 2 中表示每种攻击类型重要度评分最高的前 7 个特征. 其次, 为了验证模型的整体效果, 本文将所有正常类型以及所有异常类型分别进行编码, 使

用随机森林算法进行特征选择, 选取评分度最高的 8 个特征作为 LSTM 系统的输入, 重要性权重如图 3 所示.

表 1 数据集划分

类型	攻击类型数量	正常类型数量	总量
All Data	469 274	2 203 723	2 672 997
Bot	1 966	4 276	6 242
DDoS	41 835	92 295	134 130
DoS GoldenEye	10 293	22 291	32 584
DoS Hulk	231 073	551 149	782 222
DoS Slowhttptest	5 499	12 260	17 759
DoS Slowloris	5 796	12 457	18 253
FTP-Patator	7 938	17 262	25 200
PortScan	158 930	368 180	527 110
SSH-Patator	5 897	12 734	18 631

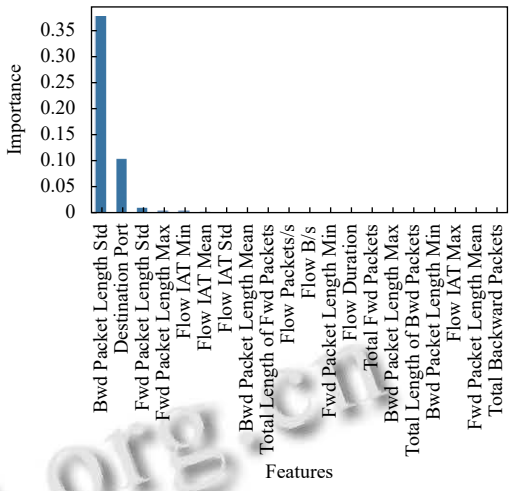

图 3 重要度评分

表 2 攻击类型特征选择

攻击类型	Bot	DDoS	DoS GoldenEye	DoS Hulk	DoS Slowhttptest
特征选择	Bwd Packet Length Mean Flow IAT Max Flow IAT Std Flow Duration Flow IAT Mean Flow IAT Min Flow B/s	Bwd Packet Length Std Total Backward Packets Fwd IAT Total Flow Duration Total Length of Fwd Packets Flow IAT Min Flow IAT Std	Flow IAT Max Total Backward Packets Flow IAT Min Fwd Packet Length Min Bwd Packet Length Std Fwd Packet Length Max Bwd Packet Length Mean	Flow IAT Max Total Backward Packets Flow IAT Min Fwd Packet Length Min Bwd Packet Length Std Fwd Packet Length Max Bwd Packet Length Mean	Flow IAT Mean Fwd Packet Length Min Bwd Packet Length Mean Fwd Packet Length Std Fwd Packet Length Mean Bwd Packet Length Std Total Length of Bwd Packets
攻击类型	DoS Slowloris	FTP-Patator	PortScan	SSH-Patator	—
特征选择	Flow IAT Mean Bwd Packet Length Mean Total Fwd Packets Fwd IAT Total Total Length of Bwd Packets Flow IAT Std Fwd Packet Length Min	Fwd Packet Length Max Fwd Packet Length Std Fwd Packet Length Mean Bwd Packet Length Mean Flow IAT Min Total Length of Bwd Packets Flow Duration	Total Length of Fwd Packets Flow B/s Flow IAT Max Flow Duration Fwd IAT Total Flow IAT Mean Fwd Packet Length Max	Flow B/s Flow IAT Mean Flow Packets/s Fwd Packet Length Max Flow Duration Flow IAT Max Total Length of Fwd Packets	—

3.3 实验分析与评价

本文使用随机森林算法进行特征提取后, 使用 LSTM 网络进行异常检测与识别. 在随机森林部分, 将随机森林中的决策树的数目设置为 250, 将随机种子 random_state 设置为 0, 选取的特征子集中特征的个数的 max_features 参数设置为 auto. 在 LSTM 部分, 由一个 LSTM 层组成, 其神经元个数为 128, 优化函数使用 Adadelt, 损失函数使用 categorical_crossentropy, metrics 参数为 accuracy, 为了缓解过拟合, 在全连接层加入 dropout, 比例为 0.5. 另外, 模型中还引入了 early stopping 机制, 借助 Keras 中的 EarlyStopping 类, 当训练模型在测试集上的性能不再增加的时候就停止训练, 从而达到充分训练的作用, 又避免过拟合, 提高模型的泛化能力, 加速目标函数的收敛, 并将训练过程中最好的模型保存下来.

本文使用准确率 (accuracy, *ACC*)、召回率 (recall, *RE*)、精确率 (precision, *PR*) 以及分类器精度得分 (*F*1-score, *F*1) 对模型进行评价, 计算公式如下:

$$ACC = \frac{TP+TN}{TP+FP+FN+TN} \tag{10}$$

$$RE = \frac{TP}{TP+FN} \tag{11}$$

$$PR = \frac{TP}{TP+FP} \tag{12}$$

$$F1 = \frac{2}{\frac{1}{PR}+\frac{1}{RE}} \tag{13}$$

其中, *TP* 表示将攻击类型检测为攻击类型, *TN* 表示将正常类型检测为正常类, *FP* 表示将正常类型检测为攻击类型, *FN* 表示为将攻击类型检测为正常类型. 其混淆矩阵可表示为表 3.

表 3 混淆矩阵

真实类型	预测类型	
	Attack	Normal
Attack	*TP*	*FN*
Normal	*FP*	*TN*

实验过程中, 模型的准确率与损失函数变化如图 4 和图 5 所示. 在训练过程中, 随着迭代的进行, 模型不断收敛, 在迭代到第 20 次左右的时候, 模型的准确率 *ACC* 和损失函数 Loss 趋于稳定.

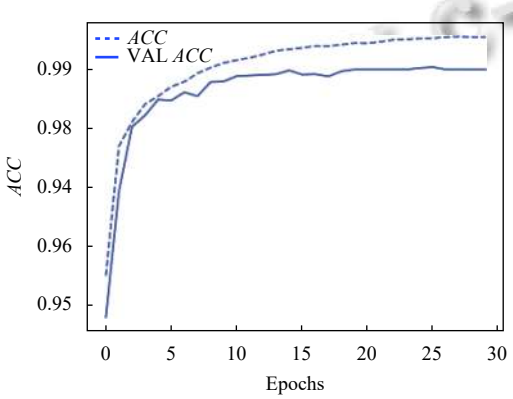

图 4 训练过程 *ACC* 变化

为了验证本文方法在异常流量检测方面的优越性, 针对每种攻击类型以及所有攻击类型汇总的流量数据分别使用常见的机器学习算法进行实验对比, 如朴素贝叶斯 (naive Bayes)、二次判别分析 (QDA)、K 近邻 (KNN), 使用准确率 (*ACC*)、召回率 (*RE*)、精确率 (*PR*)、和 *F*1-score 作为评价指标. 不同算法之间的性能比较如表 4 所示. 从结果中可以看出, 攻击类型 FTP-Patator 以及 PortScan 具有较高的检测效率, 这可能是因为这两种攻击类型具有较为明显的识别特征.在结果中可以看出, LSTM 模型在各种攻击类型的识别检测上具有良好的表现, 本文算法有效提高了 Bot、DDos、DoS GoldenEye、DoS Hulk 攻击流量识别以及整体的识别准确率. 除 DoS Slowhttptest、DoS Slowloris 攻击外, 本文算法准确率均高于或者等于对比算法的准确率. 此外, 本文算法重要优势是对整体攻击类型识别的准确率在训练集上最终达到 99%. 最后, 为了验证模型的有效性, 本文对汇总数据集进行随机取样, 选取部分数据作为数据集验证, 使用本文方法 (RF-LSTM) 与未使用随机森林进行特征提取的 LSTM 方法作比较, 结果如表 5.

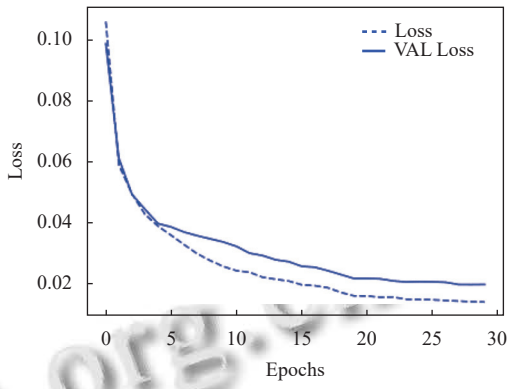

图 5 训练过程 Loss 变化

表 4 机器学习算法对比

Parameter	Naive Bayes				QDA				KNN				本文方法			
	ACC	*RE*	*PR*	*F*1	*ACC*	*RE*	*PR*	*F*1	*ACC*	*RE*	*PR*	*F*1	*ACC*	*RE*	*PR*	*F*1
Bot	0.56	0.69	0.70	0.56	0.68	0.77	0.74	0.68	0.94	0.95	0.92	0.93	0.97	0.97	0.96	0.96
DDoS	0.34	0.52	0.66	0.28	0.79	0.85	0.80	0.78	0.96	0.96	0.95	0.95	0.97	0.97	0.96	0.96
DoS GoldenEye	0.88	0.84	0.87	0.85	0.73	0.82	0.87	0.82	0.81	0.98	0.97	0.97	0.99	0.99	0.98	0.98
DoS Hulk	0.81	0.77	0.77	0.77	0.47	0.62	0.68	0.46	0.97	0.97	0.96	0.97	0.98	0.98	0.97	0.97
DoS Slowhttptest	0.43	0.57	0.62	0.41	0.70	0.77	0.73	0.70	0.99	0.99	0.98	0.98	0.98	0.98	0.97	0.98
DoS Slowloris	0.40	0.56	0.67	0.36	0.49	0.62	0.66	0.49	0.99	0.99	0.99	0.99	0.98	0.98	0.97	0.97
FTP-Patator	0.55	0.67	0.70	0.54	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
PortScan	0.44	0.60	0.67	0.43	0.84	0.88	0.82	0.83	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
SSH-Patator	0.68	0.76	0.75	0.68	0.79	0.84	0.80	0.79	0.96	0.96	0.95	0.95	0.96	0.97	0.95.	0.96
All Data	0.84	0.69	0.74	0.71	0.82	0.68	0.71	0.69	0.98	0.98	0.97	0.98	0.99	0.98	0.98	0.98

表 5 LSTM 模型与 RF-LSTM 模型对比结果

模型	*ACC*	*RE*	*PR*	*F*1	Time (s)
LSTM	0.99	0.99	0.99	0.99	7005
RF-LSTM	0.99	0.98	0.98	0.98	3346

结果表明, 本文方法在准确率、召回率、精确率等评价指标损失很小的情况下, 将模型的训练时间大大缩短, 提高了模型检测的效率, 节省了计算机资源,

具有实际的应用价值.

4 结论

针对传统的工控网络流量数据在复杂网络环境下特征维度高, 模型检测效率低的问题, 提出了一种基于随机森林 (RF) 和长短期记忆网络 (LSTM) 的算法, 从高维度流量数据特征中提取出关键流量特征, 剔除冗余特征, 通过 LSTM 算法充分挖掘网络流量特征之间的关系, 进行网络异常流量的识别与检测. 实验结果表明, 本文算法在 CIC-IDS-2017 数据集上总体准确率达到 99%, 与 Naive Bayes、QDA、KNN 机器学习算法相比, 本文算法在绝大多数攻击类型的识别准确率上优于或者等于对比算法, 且与单独的 LSTM 算法做对比, 本文方法在保证准确率损耗极小的情况下, 大大提高了模型的检测效率, 在工控网络异常检测方面具有实际的应用价值.

此外, 本文还存在以下问题. 本文提前将不平衡的数据集进行平衡化处理, 在处理现实世界中数据集不平衡的问题, 还需要引入其他方法, 对数据进行清洗, 比如考虑引入类型权重等方法减小数据不平衡对模型的影响或者采用 GAN 等方法生产相关样本数据. 另外, 模型在面对新的异常时, 可能存在泛化能力不足的问题, 下一步将采用性能更好的模型如 Transformer 等.

参考文献

1 国家互联网应急中心 (CNCERT). 2021 年上半年我国互联网网络安全监测数据分析报告. https://www.cert.org.cn/publish/main/upload/File/first-half%20%20year%20cyberseurity%20report%202021.pdf. (2021-07-31).

2 Ke GL, Meng Q, Finley T, *et al*. LightGBM: A highly efficient gradient boosting decision tree. Proceedings of the 31st International Conference on Neural Information Processing Systems. Long Beach: ACM, 2017. 3149–3157.

3 Chen TQ, Guestrin C. XGBoost: A scalable tree boosting system. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. San Francisco: ACM, 2016. 785–794.

4 王智慧, 王静, 方蓬勃, 等. 基于 LightGBM 的电力工控系统异常流量检测方法. 电力信息与通信技术, 2021, 19(11): 69–77.

5 Jiang H, He Z, Ye G, *et al*. Network intrusion detection based on PSO-XGBoost model. IEEE Access, 2020, 8: 58392–58401.

6 刘奇旭, 陈艳辉, 尼杰硕, 等. 基于机器学习的工业互联网入侵检测综述. 计算机研究与发展, 2022, 59(5): 994–1014.

7 王胜, 唐超, 张凌浩, 等. 面向 IEC61850 智能变电站的网络安全异常流量分析方法. 重庆大学学报, 2022, 45(1): 1–8.

8 石乐义, 朱红强, 刘祎豪, 等. 基于相关信息熵和 CNN-BiLSTM 的工业控制系统入侵检测. 计算机研究与发展, 2019, 56(11): 2330–2338.

9 蹇诗婕, 卢志刚, 杜丹, 等. 网络入侵检测技术综述. 信息安全学报, 2020, 5(4): 96–122.

10 田伟宏. 智能变电站网络异常检测方法的研究与实现 [硕士学位论文]. 沈阳: 中国科学院大学 (中国科学院沈阳计算技术研究所), 2020.

11 杜浩良, 孔飘红, 金学奇, 等. 基于深度学习的电力信息网络流量异常检测. 浙江电力, 2021, 40(12): 117–123.

12 杨月麟, 毕宗泽. 基于深度学习的网络流量异常检测. 计算机科学, 2021, 48(S2): 540–546.

13 李梅, 宁德军, 郭佳程. 基于注意力机制的 CNN-LSTM 模型及其应用. 计算机工程与应用, 2019, 55(13): 20–27.

14 舒豪, 王晨, 史峄. 基于 BiLSTM 和注意力机制的入侵检测. 计算机工程与设计, 2020, 41(11): 3042–3046.

15 Breiman L. Random forests. Machine Learning, 2001, 45(1): 5–32.

16 李光华, 李俊清, 张亮, 等. 一种融合蚁群算法和随机森林的特征选择方法. 计算机科学, 2019, 46(11A): 212–215.

17 陈卓, 吕娜. 基于随机森林和 XGBoost 的网络入侵检测模型. 信号处理, 2020, 36(7): 1055–1064.

18 Hochreiter S, Schmidhuber J. Long short-term memory. Neural Computation, 1997, 9(8): 1735–1780.

19 韦泽鲲, 夏靖波, 张晓燕, 等. 基于随机森林的流量多特征提取与分类研究. 传感器与微系统, 2016, 35(12): 55–59.

20 佟欣欣. 基于深度学习的加密流量识别研究 [硕士学位论文]. 合肥: 中国科学技术大学, 2021.

21 陈解元. 基于 LSTM 的卷积神经网络异常流量检测方法. 信息技术与网络安全, 2021, 40(7): 42–46.

22 Kostas K. Anomaly detection in networks using machine learning [Master's thesis]. Edinburgh: Heriot-Watt University, 2018.

(校对责编: 牛欣悦)