文章编号:1674-2974(2020)08-0001-08 DOI:10.16339/j.cnki.hdxbzkb.2020.08.001

基于 ResNet 和双向 LSTM 融合的物联网入侵检测分类模型构建与优化研究

陈红松,陈京九†
(北京科技大学 计算机与通信工程学院,北京 100083)

摘 要: 为提高物联网入侵检测模型的综合性能, 将残差神经网络 (Residual Networks, ResNet)与双向长短时记忆(Long-Short Term Memory,LSTM)网络融合,构建物联网入侵检测分类模型.针对大规模物联网流量快速批量处理问题,在对原始数据进行清洗、转换等预处理基础上,提出将多条流量样本转换为灰度图,并利用基于 ResNet 和双向 LSTM 融合的深度学习方法构建物联网入侵检测分类模型.对分类模型的网络结构、可复用性进行综合优化实验,得到最终优化模型,分类准确率达到 96.77%,综合优化后的模型构建时间为 39.85 s.与其他机器学习算法结果相比,该优化方法在分类准确率和效率两个方面取得了很好的效果,综合性能优于传统的入侵检测分类模型.

关键词: 入侵检测;残差网络;双向 LSTM 网络;图像分类;物联网
中图分类号: TP183 **文献标志码:** A

Study on Construction of IOT Network Intrusion Detection Classification Model and Optimization Based on Combination of ResNet and Bidirectional LSTM Network

CHEN Hongsong, CHEN Jingjiu†
(School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China)

Abstract: In order to improve the performance of the Internet of Things (IOT) network intrusion detection model, Residual Networks (ResNet) and bidirectional Long-Short Term Memory (LSTM) networks were combined, and an IOT intrusion detection classification model was constructed. For the rapid and batch processing problem of large-scale IOT traffic, multiple traffic samples were converted into grayscale images. Then, the grayscale images were used to construct IOT intrusion detection and classification model which combined with ResNet and bidirectional LSTM network. The network structure and re-usability of the classification model were optimized experimentally, so the optimization model was obtained finally. The classification accuracy of the optimization model is 96.77%, and the running time after the model reuse optimization is 39.85 s. Compared with other machine learning algorithms, the proposed approach achieves good results in both classification accuracy and efficiency. The performance of the proposed model is better than that of traditional intrusion detection model.

Key words: intrusion detection; Residual Networks (ResNet); bidirectional Long-Short Term Memory (LSTM) networks; image classification; IOT (Internet of Things)

* **收稿日期:** 2019-07-22
基金项目: 国家社会科学基金资助项目(18BGJ071), National Social Science Foundation of China(18BGJ071)
作者简介: 陈红松(1977—),男,山东济宁人,北京科技大学教授,博士生导师
† 通讯联系人, E-mail: chenhs@ustb.edu.cn

随着网络的不断发展，人们对互联网的依赖也与日俱增. 互联网为人们的生产生活提供方便的同时,也滋生了越来越多的安全问题.尤其是在当前物与物相连的物联网时代，如何快速识别物联网中的入侵,成为网络安全领域亟待解决的问题之一.入侵检测系统(Intrusion Detection System,IDS)可对流经网络中的流量进行判别，以检测是否有入侵情况的发生.入侵检测的实质是一个分类问题,即判定当前流量记录正常与否,或判定流量所属攻击类别.

Sharafaldin 等[1]研发的 CICIDS2017 入侵检测数据集是一个公开数据集，该数据集基于真实环境采集得到. 数据集包含正常流量和最新的常见攻击流量,目前国内外有公司、研究机构与学校共计 196 所正在使用该数据集. Gharib 等[2]利用 B-Profile 系统基于 HTTP、HTTPS、FTP、SSH 和电子邮件协议构建了 25 个人类交互的抽象行为,用以生成正常背景流量. 实施的攻击包括暴力 FTP、暴力 SSH、DoS、Heartbleed、Web 攻击、渗透、僵尸网络和 DDoS 等.

孔令爽[3]利用将流量数据转换为图像的方法,把数据以灰度图的形式表示出来，使用图像中的纹理表征对入侵方式进行归类.徐温雅[4]提出利用改进的 K-means 算法对训练集中的样本进行数据筛选与预处理,通过基于 SVM 与神经网络的混合网络入侵检测模型对数据集进行分类. Vinayakumar 等[5]利用 CNN-RNN 网络构建入侵检测模型对 KDD CUP99数据集进行建模测试,准确率达到 98.7%,证明 CNN在提取图片高维特征时具有一定优势. Zhang 等[6]提出融合 LeNet5 和 LSTM 的方法构建入侵检测模型对 CICIDS2017 数据集进行建模测试，准确率达到 99.91%.Ustebay 等[7]提出深度多层感知机方法构建入侵检测模型,最终达到 91%的准确率. Dutta 等[8]利用 CNN-RNN 网络进行手写词语识别. Jain 等[9]利用 CNN-RNN 进行印度语单词识别，验证了 CNN-RNN 网络可以在提取图像特征的同时,学习时序相关特征.

通过对现状分析可知，深度学习构建入侵检测系统可以从原始数据中提取更高维度的特征，从而获得更加良好的分类模型. 本文提出一种基于 ResNet 与双向 LSTM 融合的网络入侵检测分类模型,并通过实验进行验证与优化.

1 物联网入侵检测数据预处理

本文提出基于 ResNet 和双向 LSTM 融合的物联网入侵检测分类模型构建与优化流程如图 1 所示.

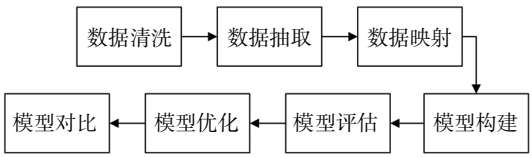


图 1 基于 ResNet 和双向 LSTM 融合的物联网入侵检测分类模型构建与优化流程图

Fig.1 Intrusion detection and classification model construction and optimization pipeline based on combination of ResNet and bidirectional LSTM network

由于流量数据具有时间相关性，为对大规模物联网流量进行批量、快速处理,提出将窗口内多条连续流量记录转换合成为图片并利用基于 ResNet 和双向 LSTM 融合的计算机视觉处理技术进行分类的方法.本文采用 CICIDS2017 数据集,对其进行数据清洗、数据抽取和数据映射等操作,将其转换为图像数据集.

1.1 数据清洗

通过对 CICIDS2017 数据集分析,发现该数据集存在缺失、乱码等问题,无法直接用于物联网入侵检测模型的构建. 为构建基于 ResNet 和双向 LSTM 融合的物联网入侵检测分类模型,利用数据清洗、数据变换等步骤需对原始数据集进行预处理.

“脏数据”是指不完整、含有噪声、不一致的数据,破坏了原始数据信息中的内部规律,导致数据分析和处理的运行效果不佳. 因此需要利用自定义的清洗规则,对“脏数据”进行数据清洗,手工或自动地将“脏数据”转换成满足数据质量要求的数据.

数据清洗面对的主要问题是空缺值、错误数据、孤立点和噪声，解决方案是利用相同的常数填补数据集缺失，将存在的特殊符号及乱码进行清空或替换处理. 由于 CICIDS2017 数据集存在的 78 个特征中,既有数值数据,又有字符数据,而深度神经网络的输入值应该是一个数值化矩阵，所以需要将数据标准化,数据变换时,对非数值化特征如“infinite”等转化为数值形式.

1.2 数据抽取

本文选用 CICIDS2017 中的 DDoS 和 Portscan 数据集,包含 225 255 条正常样本、128 027 条 DDoS 攻击样本和 158 930 条 Portscan 攻击样本.为增加不同类别样本之间的差异性,提高模型分类效果,本文提出数据抽取算法 SamExtract 对原始数据集进行预处

理.设样本空间 $T=\{T_1,T_2,\cdots,T_n\}$,当前样本为 T_t,样本类别 $i=\{0,1,2\}$ 分别代表正常、DDoS 攻击和 Portscan 攻击,SamExtract 算法伪代码如图 2 所示.

算法 1　基于窗口的数据抽取算法 SamExtract (D_A,w,α)

输入:CICIDS2017 数据集 D_A,窗口大小 w,抽取阈值 α
输出:抽取后数据集 D_B
(1)初始化样本计数器 $c_i=0\ (i=0,1,2),w,\alpha$
(2)for $k=1$ to $|D_A|/w$ do:
(3)　for t = kw to $(k+1)w$ do:
(4)　　if $T_t=i$ then:
(5)　　$c_i=c_i+1$
(6)　　if $c_i \geqslant w\alpha$ then:
(7)　　将当前窗口样本放入 D_B,并设定标签为 i
(8)　　end if
(9)　end if
(10)　$c_i=0$
(11)end for
(12)return D_B

图 2　SamExtract 伪代码

Fig.2　SamExtrace code

本文设定窗口大小 w=10,抽取阈值 α=0.9,抽取后得到的数据集 D_B 与数据集 D_A 对比如表 1 所示.

表 1　数据集 D_A,D_B 样本数对比

Tab.1　Dataset D_A,D_B sample number comparison

样本类型	D_A	D_B
正常样本数量	225 255	221 590
DDoS 攻击样本数量	128 027	127 890
Portscan 攻击样本数量	158 930	157 630

由表 1 可知抽取后得到的数据集 D_B 中正常样本、DDoS 攻击样本和 Portscan 攻击样本损失率分别为 1.63%、0.11%和 0.82%.由此可知,根据该方法抽取的数据集 D_B 仅损失了少量特征不明显的样本,保留了原始数据集 D_A 中的大部分样本,可证明该提取规则有效.

1.3　数据映射

经过上述操作后,继续将数据集 D_B 中的数据映射为图像数据集. 由于本文设置窗口大小 w=10,CICIDS2017 数据集中特征数为 78 个, 所以将数据集 D_B 中尺寸为 10×78 的矩阵 $\boldsymbol{W}$ 映射为 10×78 大小的灰度图像. 图像中每一个像素对应矩阵中相应位置的数值.

但由于灰度图数值范围为[0,255],而原始矩阵 $\boldsymbol{W}$ 中数据区间较大,为保留更多特征细节,映射时需要对原始矩阵 $\boldsymbol{W}$ 进行归一化处理. 目前常用的归一化方法有均值方差归一化和最大最小归一化, 均值方差归一化处理后的数据符合标准正太分布,常用在一些通过距离得出相似度的聚类算法中, 计算公式为:

$$x=\frac{x-\bar{x}}{\sigma} \tag{1}$$

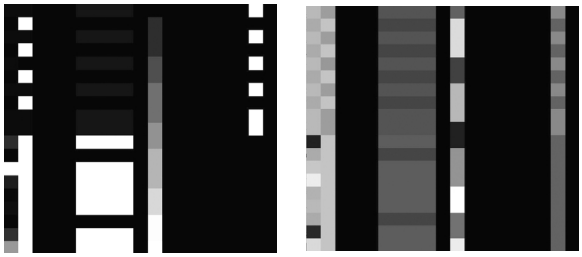
式中:x 为序列中某一数据当前值;$\bar{x}$为该序列中数据均值;σ 为该序列的标准差.

最大最小归一化的手段是一种线性的归一化方法,它的特点是不会对数据分布产生影响,但结果稳定性取决于数据集最大值、最小值的稳定性,常用于图像处理领域,计算公式为:

$$x=\frac{x-x_{\min}}{x_{\max}-x_{\min}} \tag{2}$$

式中:x 为序列中某一数据当前值;$x_{\min}$ 为序列中该数据最小值;$x_{\max}$ 为序列中该数据最大值.

通过归一化处理后的数值矩阵再次放缩到[0,255]区间,并将该值作为图像对应像素的灰度值,生成的局部流量图像如图 3 所示.



(a)最大最小归一化　　(b)均值方差归一化

图 3　不同归一化方法生成图片对比

Fig.3　Image comparison generated by different normalization methods

由图 3 可以看出,图 3(a)颜色区分更加鲜明,图 3(b)颜色区分不太明显,但是图 3(b)可以保留更多的信息. 其原因是均值方差归一化方法对数据的处理方式是把特征的样本均值变成 0, 标准差变成 1, 因此保留了更多特征, 而最大最小归一化方法对数据的处理方式是将样本数据根据最大值和最小值调整到一个区间内,这样会丢失更多的信息.因此本文图像映射采用均值方差归一化方法进行处理.

均值方差归一化处理后的正常流量、DDoS 攻击流量和 Portscan 攻击流量图像分别如图 4、图 5、图 6 所示.

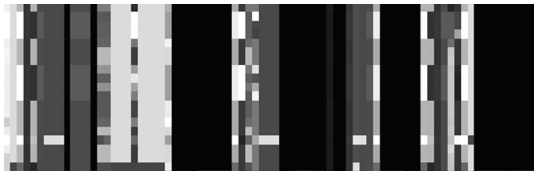


图 4 正常流量映射生成的图像

Fig.4 Image generated by normal traffic mapping

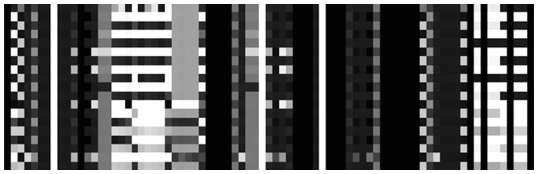


图 5 DDoS 攻击流量映射生成的图像

Fig.5 Image generated by DDoS attack traffic mapping

图 6 Portscan 攻击流量映射生成的图像

Fig.6 Image generated by Portscan attack traffic mapping

由图 4、图 5、图 6 可以看出,3 种不同类别流量映射图像差异较大,可证明该图像映射方法有效.因此本文后续根据该数据集进行建模与评估.

2 基于 ResNet 和双向 LSTM 融合的物联网入侵检测分类模型构建

本文提出的 ResNet+双向 LSTM 总体结构图如图 7 所示.

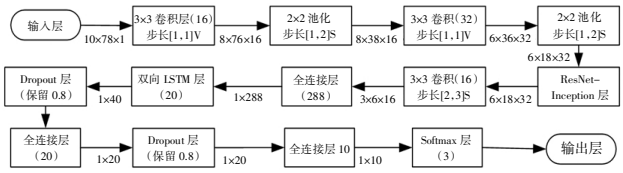


图 7 ResNet+双向 LSTM 总体结构图

Fig.7 ResNet+ bidirectional LSTM overall structure

图 7 中第一个卷积层中文字表示卷积核大小为 3×3,卷积核个数为 16 个,移动步长为[1,1],分别代表纵向移动 1 步以及横向移动 1 步,V 代表无填充,S 代表 0 填充, 第一个箭头下方数字代表当前张量高度为 10,宽度为 78,通道数为 1.其中输入层的结构图如图 8 所示.

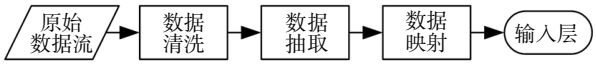


图 8 输入层结构图

Fig.8 Input layer structure

2.1 ResNet-Inception 层

图 7 中 ResNet-Inception 层是 Szegedy 等[10]基于 He 等[11] ResNet 融合了 GoogLeNet 中的 inception-v4 提出创新型结构. 具体结构如图 9 所示.

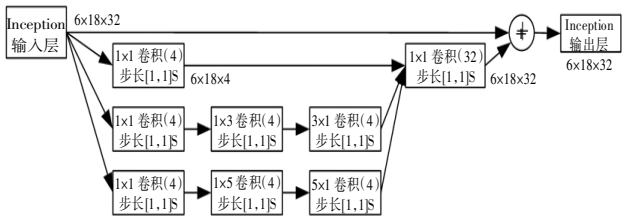


图 9 ResNet-Inception 层结构图

Fig.9 ResNet-Inception layer structure

由图 9 可以看出,ResNet-Inception 结构不仅在深度上进行扩展,还增加了网络的宽度. 在最右侧卷积层前有一个连接层, 把 3 个通道生成的不同类型但大小相同的特征图并排连接起来, 形成新的特征响应图. 数据在输出层之前经过了两条路线,一条是常规路线,另一条是捷径,直接实现单位映射的直接连接的路线. 两条路线得到的张量在输出层前进行了点加操作,最后将张量继续向网络下层传递.

2.2 双向 LSTM 层

长短时记忆网络 (Long-Short Term Memory, LSTM)[12] 是一种特殊的 RNN 类型, 其区别于普通 RNN 的地方,主要在于它在算法中放置了 3 扇门,分别叫做输入门(input gates)、遗忘门(forget gates)和输出门(output gates),通过门结构的设计来避免梯度消失问题. 门结构的存在可以让 LSTM 单元保存和获取长时间周期的上下文信息,LSTM 单元内部结构如图 10 所示.

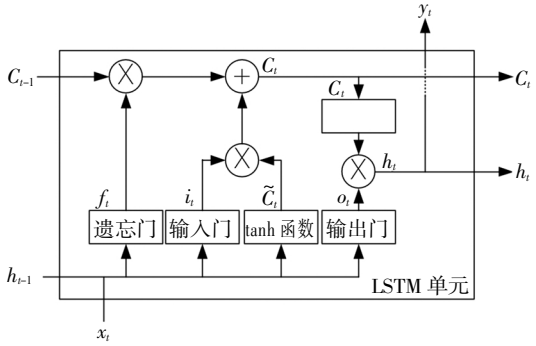


图 10 LSTM 单元内部结构图

Fig.10 LSTM unit architecture

图 10 中各参数计算公式如下:

$$f_t=\sigma(\boldsymbol{W}_{\mathrm{f}}\cdot[h_{t-1},\boldsymbol{x}_t]+b_{\mathrm{f}})$$
$$i_t=\sigma(\boldsymbol{W}_{\mathrm{i}}\cdot[h_{t-1},\boldsymbol{x}_t]+b_{\mathrm{i}})$$
$$\tilde{C}_t=\tanh(\boldsymbol{W}_{\mathrm{c}}\cdot[h_{t-1},\boldsymbol{x}_t]+b_{\mathrm{c}})$$
$$C_t=f_t*C_{t-1}+i_t*\tilde{C}_t$$
$$o_t=\sigma(\boldsymbol{W}_{\mathrm{o}}\cdot[h_{t-1},\boldsymbol{x}_t]+b_{\mathrm{o}})$$
$$h_t=o_t*\tanh(C_t)\qquad(3)$$

式中:σ 表示 sigmoid 函数;$\boldsymbol{W}_{\mathrm{f}}$、$\boldsymbol{W}_{\mathrm{i}}$、$\boldsymbol{W}_{\mathrm{c}}$、$\boldsymbol{W}_{\mathrm{o}}$ 分别为遗忘门、输入门、tanh 函数和输出门的权重矩阵;h_{t-1} 为隐藏层前一时刻输出;C_t 为当前 t 时刻 LSTM 单元的输出;o_t 为当前 t 时刻输出门的输出;h_t 为当前 t 时刻隐藏层的输出;$\boldsymbol{x}_t$ 为输入向量;b_{f}、b_{i}、b_{c}、b_{o} 分别为遗忘门、输入门、tanh 函数和输出门的偏置值.

双向 LSTM 网络中的每一个训练序列均由前向传播 LSTM 网络和反向传播 LSTM 网络组成,这两个 LSTM 网络同时连接一个输出层,为输出层中的每一个神经元提供完整的上下文信息. 具体双向 LSTM 网络结构如图 11 所示.

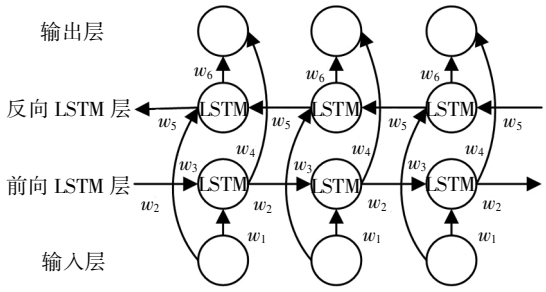


图 11　双向 LSTM 网络结构图

Fig.11　Bidirectional LSTM network architecture

由图 11 可知,每一个输出神经元的输入都包含前向 LSTM 层输出与反向 LSTM 层输出. 输出神经元的计算公式如下:

$$h_t=f(w_1\boldsymbol{x}_t+w_2h_{t-1})$$
$$h_t'=f(w_3\boldsymbol{x}_t+w_5h_{t-1}')$$
$$o_t=g(w_4h_t+w_6h_t')\qquad(4)$$

3　基于 ResNet 和双向 LSTM 融合的物联网入侵检测分类模型评估与优化

3.1　模型评估

本文采用 TensorFlow 开源机器学习框架，将第 1 节生成的数据集按照时间维度分割为训练集与测试集,构造并验证基于 ResNet 和双向 LSTM 融合的物联网入侵检测分类模型的有效性. 数据集类别分布如表 2 所示.

表 2　图像数据集类别分布

Tab.2　Image dataset sample category distribution

样本类型	训练集	测试集
正常样本数量	13 014	9 145
DDoS 攻击样本数量	7 219	5 570
Portscan 攻击样本数量	5 394	10 369

使用卷积层与最大池化层构造 ResNet-Inception 结构，双向 LSTM 网络参数为 288 个输入节点，中间隐藏层为 1 层，隐藏层节点 20 个，学习率为 0.001.利用图像训练集对网络进行训练,共训练 100 轮,取最佳效果如表 3 所示.

表 3　基于 ResNet 和双向 LSTM 融合模型分类预测实验结果

Tab.3　Experimental results of ResNet and bidirectional LSTM model

类别	准确率/%	召回率/%	F 度量/%	样本数
正常流量	91.32	93.53	92.41	9 145
DDoS 攻击流量	94.22	98.06	96.10	5 570
Portscan 攻击流量	97.05	92.85	94.90	10 369

该网络结构在 64 轮时获得最佳结果,准确率为 94.26%，训练耗时 1 488.87 s. 其中 F 度量为综合了准确率与召回率参数的指标,计算公式如下:

$$F=\frac{2\times P\times R}{P+R}\qquad(5)$$

式中:P 为准确率;R 为召回率.

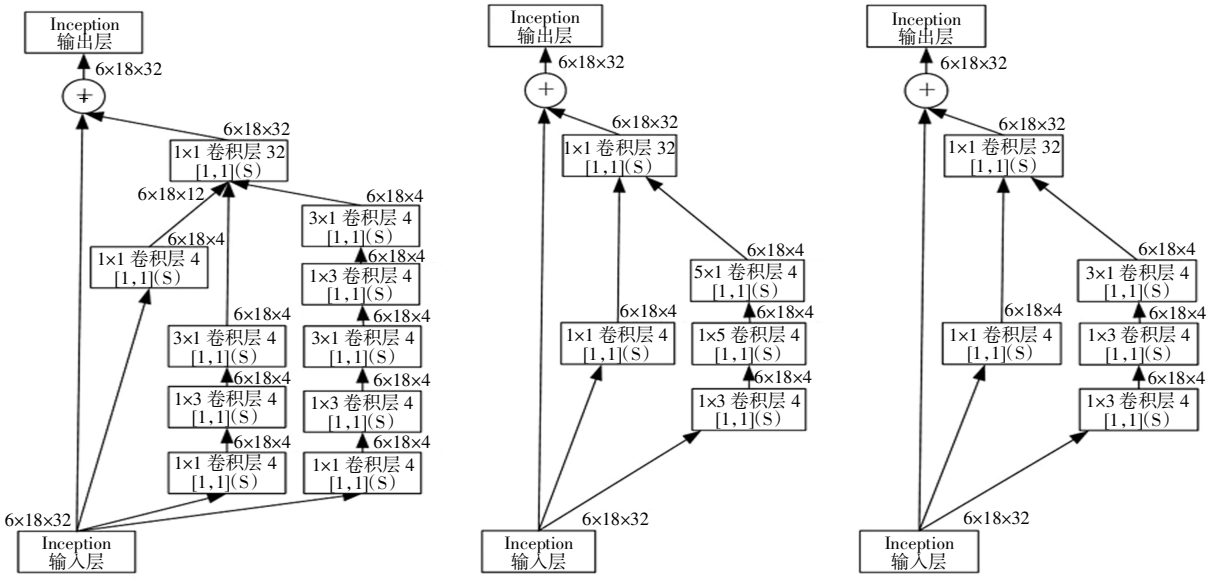
ResNet-Inception 结构解决了深层网络的梯度消失问题，长短时记忆单元特有的门结构解决了传统循环神经网络时间维度的梯度消失问题，实现较大范围的上下文信息的保存与传输，提高了 LSTM 单元对具有长时间间隔相关性特点的序列信息的处理能力.

3.2　模型优化

3.2.1　ResNet-Inception 层结构优化

初始 ResNet-Inception 层结构如图 8 所示,不同的 ResNet-Inception 结构对于不同数据集拟合情况不同. 因此本文尝试调整 ResNet-Inception 结构对模型进行进一步优化. 优化后的 v_1、v_2 和 v_3 结构如图 12 所示.

在保持其他参数不变的情况下,仅更改 ResNet-Inception 层的结构，训练 100 轮，得到不同的 ResNet-Inception 结构效果对比如表 4 所示.



(a)v_1 (b)v_2 (c)v_3

图 12 不同 ResNet–Inception 层结构对比

Fig.12 Different ResNet–Inception layer comparison

表 4 不同 ResNet–Inception 结构效果对比

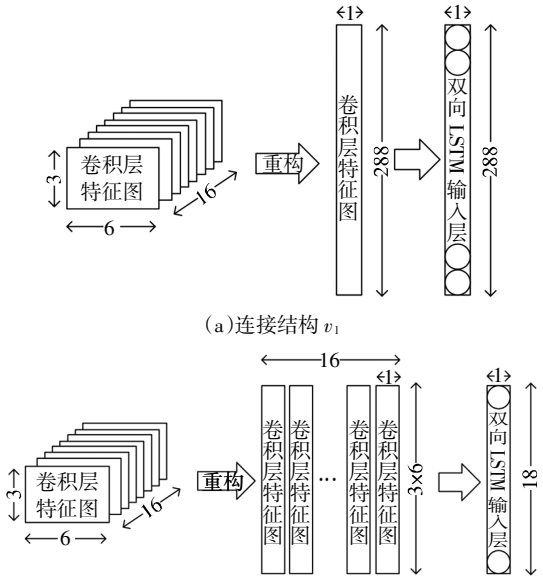
Tab.4 Results comparison of different ResNet–Inception architecture

ResNet–Inception 结构	迭代轮数	训练时间/s	准确率/%
v_1	57	1 422.37	93.84
v_2	94	3 077.07	94.75
v_3	77	1 840.17	94.84

由图 12 可知,ResNet–Inception v_1 结构最为复杂有 3 个平行分支,v_2、v_3 结构比 v_1 结构少一个平行分支. 由表 4 可知, 采用 ResNet–Inception v_3 结构的分类模型在 77 轮时获得最佳结果, 准确率为 94.84%,训练耗时 1 840.17 s,效果强于 v_1 和 v_2 结构. 因此下文针对 ResNet–Inception v_3 结构继续进行优化.

3.2.2 ResNet 与双向 LSTM 层间连接结构优化

本文当前 ResNet 层与双向 LSTM 层间连接方式是将 16 个 3×6 大小的特征图全部展开成为 1×288 的向量作为双向 LSTM 层的输入,此时双向 LSTM 层的输入节点数为 288,时间序列长度为 1.而文献[6]中将全连接层后的 1×1 600 的向量重构为 10×160 的向量获得了较好的效果, 因此本文尝试改进 ResNet 与双向 LSTM 层间的连接层结构,将 16 个特征图作为双向 LSTM 层的不同时间序列, 此时双向 LSTM 层的输入节点数为 18,时间序列长度为 16. 两种不同连接结构对比图如图 13 所示.



(a)连接结构 v_1

(b)连接结构 v_2

图 13 不同连接结构对比

Fig.13 Different link architecture comparison

本文在 3.2.1 节网络结构基础上,保持其他网络参数不变, 分别采用不同连接结构对模型进行分类测试,得到对比结果如表 5 所示.

表 5 不同连接结构效果对比

Tab.5 Results comparison of different link architecture

连接结构	迭代轮数	训练时间/s	准确率/%
v_1	77	1 840.17	94.84
v_2	75	1 883.36	93.38

由表 5 可知, 在连接层结构为 v_1 时取得最佳效

果,且由实验结果可知,在连接层结构为 v_2 时,模型的稳定性受到影响，分类结果在 66.70%~93.38%之间波动.因此文本后续实验基于连接结构 v_1 进行优化.

3.2.3　双向 LSTM 层结构优化

门控循环单元（Gate Recurrent Unit,GRU)[10]是一种对 LSTM 精简后的变体,将 LSTM 中的遗忘门和输入门合并为更新门(update gates),因此 GRU 的结构只有两个门组成,结构更为简单,计算量也随之降低.本文尝试将 LSTM 单元更换为 GRU 与 RNN(Recurrent Neural Networks)单元,同时调整双向 LSTM 层结构以达到更佳分类效果. 模型优化效果对比如表 6 所示.

表 6　双向 LSTM 层结构优化效果对比

Tab.6　Results comparison of bidirectional LSTM layer architecture

神经元结构	隐藏层数	节点数	迭代轮数	时间/s	准确率/%
LSTM	1	15	66	1 577.07	93.65
LSTM	1	20	77	1 840.17	94.84
LSTM	1	25	85	1 923.28	94.57
GRU	1	20	61	1 427.13	93.62
RNN	1	20	56	1 109.67	93.28
LSTM	2	20	63	1 471.05	95.43
LSTM	3	20	96	2 276.22	94.85

由表 6 可知,RNN 与 GRU 单元结构较为简单,构建模型所需训练时间较短，但准确率较 LSTM 单元有所下降. 因此下文继续基于 LSTM 单元进行优化.而 LSTM 层在隐藏层数为 2 层,隐藏层节点为 20 个时，在不影响分类器准确率的同时达到了效率的提升. 因此本文后续将基于当前结构进行进一步优化.

3.3　模型复用

由于模型训练花费时间较长,且具有随机性,导致模型无法保证每次均能得到最佳结果. 因此 tensorflow 框架针对这一问题设计提供了 saver 函数,利用 tensorflow 中的 saver 函数可以将任意轮次训练中的相关模型参数保存至 checkpoints 文件中. 本文设定初始准确率阈值 α 为 0.8,判断当前迭代轮次模型准确率是否高于当前准确率阈值，若高于当前准确率阈值,则利用 saver 函数保存当前模型参数并更新准确率阈值为当前模型准确率，反之则进行下一轮训练. 设模型迭代总轮次为 w,当前轮次模型为 M_i($0<i<w$),本文所用最佳模型保存算法 BestSaver 伪代码如图 14 所示.

算法 2 最佳模型保存算法 BestSaver (M_i,w,α)

输入:当前轮次模型 M_i,模型迭代总轮次 w,准确率阈值 α
输出:最佳模型 M_B
(1)初始化 $w=1\,000$,$\alpha=0.8$
(2)for i = 1 to w do:
(3)　if eval(M_i) > α then:
(4)　　M_B = saver(M_i)
(5)　　α = eval(M_i)
(6)　end if
(7) end for
(8) return M_B

图 14　最佳模型保存算法 BestSaver 伪代码

Fig.14　BestSaver code of best model save algorithm

经过图 14 的 BestSaver 算法后得到最佳模型 M_B,利用 restore 函数可以将 M_B 恢复,再对图像测试集进行测试,依然可以达到最优效果,为模型的迁移复用提供了便利. 利用 3.2 节最优网络结构参数,对图像数据集进行 1 000 轮的训练测试,发现第 903 轮循环时得到了最优的模型结果，准确率达 96.77%,模型训练共耗时 13 968.88 s. 利用 BestSaver 算法将其模型保存后，利用 restore 方法读取最佳模型参数并对全部图像测试集进行预测，准确率依然达到 96.77%,但模型构建所耗费的时间缩短为 39.85 s,大大提高了模型检测效率，为大规模物联网流量入侵检测提供可行方案.

4　物联网入侵检测分类模型对比

本文利用第 1 节处理后的图像数据集对于目前主流机器学习方法进行了训练测试，分类模型效果对比如表 7 所示.

由表 7 可知,在其他机器学习算法中,ResNet 神经网络分类模型获得了最高的准确率 96.08%,模型构建耗时 9 698.51 s,而支持向量机(Support Vector Machine,SVM)算法准确率最低为 36.46%,耗时 3 758.84 s. 其余的算法如 LeNet5 神经网络、AlexNet 神经网络、VGGNet 神经网络、GoogLeNet 神经网络、朴素贝叶斯(Naive Bayes,NB)、支持向量机(Support Vector Machine,SVM)、随机森林（Random Forest Classifier,RFC)、决策树(Decesion Tree,DT)、梯度提升(Gradient Boosting,GB)、AdaBoost 算法,分别获得了 67.95%到 95.52%之间不等的准确率,模型构建耗费时间跨度也从 0.42 s 到 8 794.45 s. 与以上方法对比，本文所提 ResNet-双向 LSTM 算法获得了

96.77%的准确率,模型构建时间为 13 968.88 s.但利用保存好的模型进行模型重构,模型构建时间可以缩短到 40 s 以内,效果好于其他机器学习模型.

表 7 分类模型效果对比

Tab.7 Results comparison of different classification model

算法名称	准确率/%	构建时间/s
KNN	95.45	1 373.65
SVM	36.46	3 758.84
NB	91.67	0.42
RFC	70.66	1.27
DT	69.91	6.02
AdaBoost	90.85	14.57
GB	67.95	77.23
LeNet5	88.51	397.07
AlexNet	84.89	895.51
VGGNet	72.40	2 699.06
GoogLeNet	95.52	8 794.45
ResNet	96.08	9 698.51
ResNet-双向 LSTM	96.77	13 968.88
ResNet-双向 LSTM(复用优化) (模型重构时间)	96.77	39.85

本文所用 Portscan 攻击数据仅为 2017 年 7 月 7 日 13:55-14:35 共 40 min 采集到的流量数据,而 DDoS 攻击数据仅为 2017 年 7 月 7 日 15:56-16:16 共 20 min 采集到的流量数据,其样本数量已足够训练本文所提模型.而在实际应用时,由于现实网络环境中攻击流量与正常流量的数据量巨大,且采集时间没有限制,所以样本量将更加庞大.因此实际应用时的样本量远大于本文训练时所用样本量,足以训练本文所提模型.因此本文所提模型对真实物联网环境下大规模入侵检测分类模型构建及优化具有一定参考价值.

5 结 论

针对大规模物联网流量批量快速处理问题,本文提出 SamExtract 算法将窗口内多条连续流量记录转换合成为图片,并利用基于 ResNet 和双向 LSTM 融合的深度学习方法构建物联网入侵检测分类模型.本文提出的基于 ResNet 和双向 LSTM 融合的网络结构,在空间维度上,利用卷积层提取图像有效特征,利用 ResNet-Inception 层解决深层次网络梯度消失难以训练的问题;在时间维度上,利用双向 LSTM 网络学习网络流量间的潜在时间特征.通过进一步优化 ResNet-Inception 层结构、连接层结构、双向 LSTM 网络和复用分类模型,使优化后的分类模型在提高准确率的同时提高分类器执行效率.采用生成的图像测试集对优化后的分类模型进行测试,模型分类预测的准确率达到了 96.77%,模型构建时间为 39.85 s,综合性能优于其他分类模型.本文所提 SamExtract 算法、网络结构优化、模型复用等优化方法对物联网环境下大规模入侵检测分类模型构建及优化具有一定参考价值.

参考文献

[1] SHARAFALDIN I,LASHKARI A H,GHORBANI A A. Toward generating a new intrusion detection dataset and intrusion traffic characterization [C]// International Conference on Information Systems Security and Privacy. Berlin:Springer,2018:108—116.

[2] GHARIB A,SHARAFALDIN I,LASHKARI A H,*et al*. An evaluation framework for intrusion detection dataset [C]// International Conference on Information Science and Security. Washington D C:IEEE Computer Society,2016:1—6.

[3] 孔令爽. 基于深度学习和迁移学习的入侵检测研究[D].青岛:山东大学信息科学与工程学院,2018:1—10.
KONG L S. Research on intrusion detection based on deep learning and transfer learning [D]. Qingdao:School of Information Science and Engineering,Shandong University,2018:1—10. (In Chinese)

[4] 徐温雅. 基于机器学习的网络入侵检测研究[D]. 北京:北京交通大学计算机与信息技术学院,2018:2—16.
XU W Y. Research on network intrusion detection based on machine learning [D]. Beijing:School of Computer and Information Technology,Beijing Jiao Tong University,2018:2—16. (In Chinese)

[5] VINAYAKUMAR R,SOMAN K P,POORNACHANDRAN P. Applying convolutional neural network for network intrusion detection[C]// International Conference on Advances in Computing,Communications and Informatics. Washington D C:IEEE Computer Society,2017:1107—1110.

[6] ZHANG Y,CHEN X,JIN L,*et al*. Network Intrusion detection:based on deep hierarchical network and original flow data [J]. IEEE Access,2019,7(1):37004—37016.

[7] USTEBAY S,TURGUT Z,AYDIN M A. Intrusion detection system with recursive feature elimination by using random forest and deep learning classifier [C]// International Congress on Big Data,Deep Learning and Fighting Cyber Terrorism. Washington D C:IEEE Computer Society,2018:71—76.

[8] DUTTA K,KRISHNAN P,MATHEW M,*et al*. Improving CNN-RNN hybrid networks for handwriting recognition[C]// International Conference on Frontiers in Handwriting Recognition. Washington D C:IEEE Computer Society,2018:80—85.

[9] JAIN M,MATHEW M,JAWAHAR C V. Unconstrained OCR for Urdu using deep CNN-RNN hybrid networks [C]// IAPR Asian Conference on Pattern Recognition. Washington D C:IEEE Computer Society,2017:747—752.

[10] SZEGEDY C,IOFFE S,VANHOUCKE V. Inception-v4,inception-ResNet and the impact of residual connections on learning [C]// AAAI Conference on Artificial Intelligence. Palo Alto:AAAI Press,2016:4278—4284.

[11] HE K M,ZHANG X Y,REN S Q,*et al*. Deep residual learning for image recognition [C]// IEEE Conference on Computer Vision and Pattern Recognition. Washington D C:IEEE Computer Society,2016:770—778.

[12] KIM J,KIM J,THU H L T,*et al*. Long short term memory recurrent neural network classifier for intrusion detection [C]// IEEE International Conference on Platform Technology and Service. Washington D C:IEEE Computer Society,2016:1—5.