文章编号：2096-1472(2022)-01-56-03
DOI:10.19644/j.cnki.issn2096-1472.2022.001.013

基于改进CNN-LSTM的网络入侵检测模型研究

葛继科，刘浩因，李青霞，陈祖琴

(重庆科技学院智能技术与工程学院，重庆 401331)
✉gjkweb@126.com; lhaoyin@qq.com; 690887086@qq.com; chenzuq81@163.com

摘　要：针对网络入侵检测模型特征提取算法复杂、训练参数过多、检测结果不理想等问题，提出一种改进卷积神经网络与长短期记忆网络结合的网络入侵检测方法(GCNN−LSTM)。首先，使用卷积神经网络对流量数据做特征选择，并选择全局池化层代替其中的全连接层；其次，结合长短期记忆网络强大的时间序列学习能力对改进卷积神经网络选择后的特征进行学习分类，以期在网络异常数据检测方面获得更好的效率和准确率。实验结果表明，提出的模型在UNSW−NB15数据集上有着较好的检测效果。在同等条件下，使用传统卷积神经网络的模型准确率为84.97%，训练时间为76.3 s；本模型准确率达到了88.96%，训练时间为61.1 s。

关键词：卷积神经网络；LSTM；全局池化；网络入侵检测
中图分类号：TP393.8　**文献标识码**：A

Research on Network Intrusion Detection Model based on Improved CNN-LSTM

GE Jike, LIU Haoyin, LI Qingxia, CHEN Zuqin

(*School of Intelligent Technology and Engineering*, *Chongqing University of Science and Technology*, *Chongqing* 401331, *China*)
✉gjkweb@126.com; lhaoyin@qq.com; 690887086@qq.com; chenzuq81@163.com

Abstract: Aiming at the problems of complex feature extraction algorithm, too many training parameters, and unsatisfactory detection results in the network intrusion detection model, this paper proposes a network intrusion detection method (GCNN-LSTM) combining improved convolutional neural network and long short-term memory (LSTM) network. Firstly, convolutional neural network is used to perform feature selection on the flow data, and its full connection layer is replaced by global pooling layer. Then, in view of its powerful time series learning ability, LSTM is used to learn and classify the features selected by the improved convolutional neural network, in order to obtain better efficiency and accuracy in network abnormal data detection. Experimental results show that the proposed model has a good detection effect on the UNSW−NB15 dataset. Under the same conditions, the accuracy of the model using the traditional convolutional neural network is 84.97%, and its raining time is 76.3 s, while the accuracy of the proposed model is 88.96%, and its training time is 61.1 s.

Keywords: convolutional neural network; LSTM; global pooling; network intrusion detection

1 引言(Introduction)

随着网络攻击手段的不断提升，基于浅层模型的网络入侵检测系统很难对复杂情况下的网络流量进行有效识别[1]。因此，网络入侵检测模型结构的优化已经成为当前安全研究领域的研究热点[2]。传统的入侵检测方法主要包括统计分析方法、阈值分析方法、特征分析方法等[3]。这些异常检测方法虽

基金项目：重庆科技学院研究生科技创新项目(YKJCX2020816)；重庆市高等教育教学改革研究项目(202078).

然能够对恶意流量进行识别，但只是对已经发现的恶意流量行为的总结，并不能适应当前互联网的海量数据和多变的网络攻击方式[4]。

深度学习能够直接从原始数据中提取特征，已逐渐被用于网络流量分类任务中。LSTM作为一种深度学习方法，由于具有保持长期记忆的能力，也逐渐被应用到各种网络入侵检测模型中。高忠石等[5]使用堆栈LSTM模型检测多维时间序列中的异常数据，并在ECG等四个数据集上进行验证，该模型在时间序列数据上有较好的验证结果。方圆等[6]提出了一种层次化的CNN−RNN模型，并在NSL−KDD与UNSW−NB15数据集上进行了分类实验。王毅等[7]使用CNN−LSTM方法构建入侵检测模型并在NSL−KDD数据集上进行分类实验。为提高模型性能，研究人员对传统CNN网络进行了改进，使用全局平均池化层代替全连接层[8]。

综合上述卷积神经网络在数据内部特征分析与长短期记忆网络在序列间关联提取方面的优势，本文提出一种基于改进卷积神经网络与长短期记忆网络相结合的网络入侵检测方法(GCNN−LSTM)，以期在网络异常数据检测方面获得更好的效率和准确率。

2　改进的CNN-LSTM模型构建(GCNN-LSTM model construction)

针对传统CNN中全连接层产生参数比重过大导致的过拟合问题，本文提出一种优化的网络检测模型GCNN−LSTM。该模型采用全局池化层代替全连接层的方式对CNN进行改进；并结合LSTM算法强大的时间序列学习能力对特征选择后的数据进行训练；最后采用Sigmoid激活函数对训练结果作二分类预测。GCNN−LSTM模型结构如图1所示。

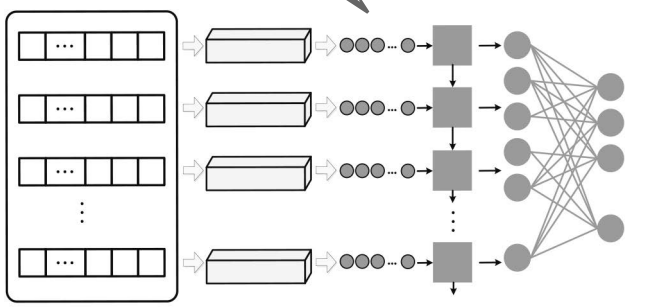


图1 GCNN−LSTM模型结构

Fig.1 GCNN−LSTM model structure

2.1　改进的卷积神经网络

卷积神经网络(Convolutional Neural Network，CNN)是一种重要的深度学习算法，在空间特征提取方面有着很好的效果，常用于信号处理及图像分类当中。典型的CNN结构如图2所示，由卷积层、池化层、全连接层交叉堆叠组成。其中，卷积层通过控制卷积核大小提取样本数据的局部特征。池化层一般处于卷积层下一层，主要用于特征选择，减少原始数据的特征维数，防止过拟合。全连接层负责对前面提取的局部特征进行整合，再把处理后的输出值传输到分类器。全连接层的输出数据通过紧随其后的非线性激活函数(tanh、Sigmoid、rectifier等)生成特征映射。

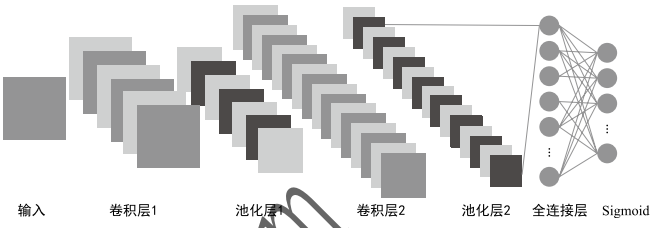


图2 卷积神经网络基本结构

Fig.2 Basic structure of CNN

但常用的CNN直接应用在入侵检测数据中的特征选择时，并不能很好地对关键特征进行提取，主要是因为传统CNN模型中的全连接层产生的参数占总模型参数比重过大，导致迭代时的计算量增加，且容易引起过拟合，影响整个模型的泛化能力。使用全局池化代替全连接层对CNN进行优化能有效解决该问题。

全局池化相比于普通池化，将整张特征图输出为一个值，使得输出数量等同于最后一层的通道数。假设模型的最后一个卷积层为m×n×4的特征图，全连接与全局池化的结构如图3(a)、图3(b)所示。

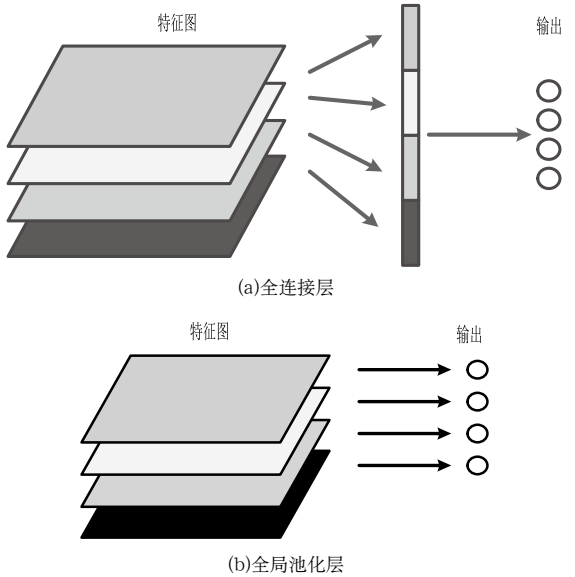


图3 全连接与全局池化结构图

Fig.3 Structure diagram of full connection and global pooling

全局池化分为全局最大池化与全局平均池化，特征图对应输出的特征值公式分别如式(1)、式(2)所示。

$$y^{l}=\max[x_{ij}^{(l)}] \tag{1}$$

$$y^{(l)}=\frac{1}{m\cdot n}[\sum_{i=0}^{m}\sum_{j=0}^{n}x_{ij}^{(l)}] \tag{2}$$

其中，式(1)表示全局最大池化，式(2)表示全局平均池化，$m\cdot n$表示特征图大小，$x_{ij}^{(l)}$表示第l张特征图的值。

2.2 长短期记忆网络

CNN主要是对单个数据包内部的特征进行分析，缺乏对序列之间关联的提取分析，因此与长短期记忆网络(Long Short Term Memory Networks，LSTM)结合构建的模型在网络入侵检测方面会有更好的训练效果。LSTM作为一种深度学习方法，由于具有保持长期记忆的能力，逐渐被应用在各种网络入侵检测模型中。LSTM通过三个“门”保持对过长数据的记忆能力，分别为遗忘门、输入门、输出门，详细计算方法如式(3)—式(6)所示。

$$f_t=\sigma\left(W_f\cdot[h_{t-1},x_t]+b_f\right) \tag{3}$$

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

$$\widetilde{C_t}=\tanh(W_c\cdot[h_{t-1},x_t]+b_c) \tag{5}$$

$$C_t=f_t\cdot C_{t-1}+i_t\cdot\widetilde{C_t} \tag{6}$$

其中，f、i、$\widetilde{C}$、C表示遗忘门、输入门、单元状态与输出门，W、b分别表示权重与偏置。

遗忘门使用Sigmoid函数决定当前时间会丢弃多少信息，使得LSTM可以在保留上下文信息的基础上，会“遗忘”一部分信息；输入门主要对输入信息进行筛选，以此来更新单元状态；输出门根据单元状态确定输出值。最后将输出数据放入分类器进行分类处理，本文采用Sigmoid函数作为激活函数对输出数据作二分类，该激活函数的公式如式(7)所示。

$$S(x)=\frac{1}{1+e^{-x}} \tag{7}$$

3 实验设计与分析(Experimental setup and analysis)

3.1 评估指标

实验采用四种常用评价指标对提出的入侵检测模型进行评估：准确率(Accuracy)、召回率(Recall)、精确度(Precision)及F1值(F1-score)。计算公式如式(8)—式(11)所示。

$$ACC=\frac{TP+TN}{TP+FP+FN+TN} \tag{8}$$

$$Recall=\frac{TP}{TP+FN} \tag{9}$$

$$Precision=\frac{TP}{TP+FP} \tag{10}$$

$$F1=\frac{2\times Precision\times Recall}{Precision+Recall} \tag{11}$$

其中，关于每种评价指标的参数TP、TN、FP和FN的定义如表1所示。

表1 混淆矩阵

Tab.1 Confusion matrix

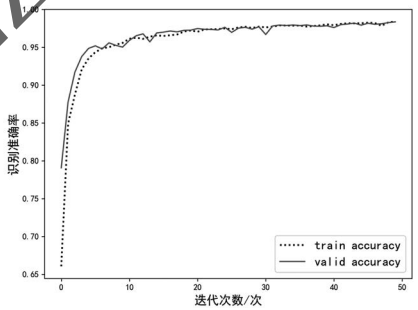
预测结果	真实正类	真实负类
预测为正类	TP	FP
预测为负类	FN	TN

3.2 实验数据

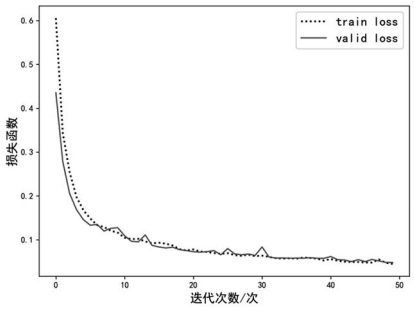
实验使用澳大利亚网络安全中心(ACCS)于2015 年建立的入侵检测数据集UNSW-NB15。该数据集共有82,332 条样本数据，包含除正常情况外的模糊测试、渗透分析、漏洞利用、DoS、泛型攻击、后门、侦察、shellcode、蠕虫等九种攻击方式。每条样本数据包含45 维特征，其中前35 维数据是从报头数据包中收集的综合信息，包括流量特征、基础特征、内容特征和时间特征；36—43 维特征表示其他生成特征；最后两维是标签数据。由于本文是对异常数据进行识别，因此只需要对标签数据进行二分类。

3.3 实验结果与分析

使用全局池化改进的CNN-LSTM网络模型在UNSW-NB15数据集上训练，得到的识别准确率与损失函数变化如图4(a)、图4(b)所示。



(a)识别准确率



(b)损失函数

图4 UNSW-NB15数据集上训练过程曲线图

Fig.4 Training process curve on UNSW-NB15 dataset

为了更加全面地验证模型在测试集上的预测效果，将GCNN-LSTM模型与传统模型进行对比实验。模型激活函数设置为Sigmoid，学习率为0.01。实验结果如表2所示，可以看出这两种优化后的模型在准确率与训练时间上都比传统模型有更好的效果。

(下转第55页)