文章编号：2095-2163(2020)02-0245-05 中图分类号：TP393.08 文献标志码：A

基于循环神经网络模型的用户入侵行为检测与管控研究

唱姓嘉
(大连民族大学 计算机科学与工程学院，辽宁 大连 116650)

摘 要：本文研究并设计了一种针对网络用户入侵行为的智能化检测模块，共分为 3 个阶段。第一，检测阶段，将网络信息安全防御系统与深度学习理论结合，提出使用长短期记忆人工神经网络(LSTM)的算法解决入侵数据的检测问题，相对于卷积神经网络(CNN)在 ACC 值和 F_1 值上得到了明显的提升；第二，管控阶段，使用华为 eNSP 模拟器来模拟真实的华为网络设备，网络连接通过第一阶段后会产生检测结果，若检测结果表明网络连接携带了潜在的入侵行为信息，则会触发一个预先设置好的 Python 脚本程序，应用华为访问控制列表(ACL)技术，通过该脚本程序对华为设备下达最新配置命令，达到管控的效果，同时向设备管理人员发送电子邮件报警；第三，显示阶段，使用 Django 框架制作一个显示平台，将已经成功拦截的网络连接信息以列表的形式显示在该平台上，设备管理员可以登录此平台后，根据页面显示的被拦截网络连接的具体信息对网络连接作进一步分析和处理。

关键词：入侵行为检测；LSTM；华为设备管控；ACL

Research on user intrusion detection and control based on cyclic neural network model

CHANG Shenjia
(School of Computer Science and Engineering, Dalian Minzu University, Dalian Liaoning 116650, China)

【Abstract】 This paper studies and designs an intelligent detection module for network user intrusion behavior, which is divided into three stages. First, in the detection phase, the network information security defense system is combined with the deep learning theory, and a long-short-term memory artificial neural network (LSTM) algorithm is proposed to solve the detection problem of the intrusion data. Compared with the convolutional neural network (CNN), the ACC value and the F_1 value have been significantly improved; Second, in the management and control phase, the Huawei eNSP simulator is used to simulate the real Huawei network equipment. After the network connection passes the first stage, the detection result will be generated. If the detection result indicates that the network connection carries the potential intrusion behavior information, a pre-trigger will be triggered. Set up a Python script, apply Huawei Access Control List (ACL) technology, and use this script to issue the latest configuration commands to Huawei devices to achieve the effect of management and control, and send email alerts to device administrators; Third, in the display phase, a display platform is created using the Django framework, and the network connection information that has been successfully intercepted is displayed on the platform in the form of a list. The device administrator can log in to the platform, according to the blocked network connection displayed on the page, specific information is provided for further analysis and processing of network connections.

【Key words】 intrusion detection; LSTM; Huawei device management; ACL

0 引 言

随着人类社会的进步，互联网技术的发展也给人们带来了各种生机与活力[1]。然而任何事物在其发展的过程中都会存在双面性。互联网技术的迅猛发展，其最初所具备的开放性、共享性以及开放性协议等思想，尤其在当今大数据时代的背景下，互联网的特点连同众多种类的网络病毒对个人信息安全、甚至人身财产安全构成了严重的威胁。研究可知，人工智能(Artificial Intelligence，AI)日渐成为互联网技术的主流，将人工智能与网络信息安全防御技术相结合，是网络安全系统发展的重要方向。基于此，本文则旨在研究如何将传统的网络安全防护模式转变为网络安全智能化防护模式。因此着重使用了深度学习方法中的长短期记忆人工神经网络(Long Short-Term Memory，LSTM)，通过应用循环神经网络 LSTM 模型，构建网络用户入侵行为检测模型，实现对含有潜在入侵行为信息的网络连接检测的功能；通过应用华为访问控制列表(ACL)技术，将检测结果与网络设备管理结合使用，实现针对入侵行为的智能化管控功能。这样的模式可以确保网络用户在正常用网的前提下，能够对互联网中存在的异常行为进行实时的监管和控制，解放了大量人力

作者简介：唱姓嘉(1995-)，男，硕士研究生，主要研究方向：机器学习、计算机技术。

收稿日期：2019-11-15

的同时,也提高了网络安全防护的效率。

1 相关技术概述

1.1 卷积神经网络

近些年来深度学习中的卷积神经网络(CNN)技术迅猛发展,不仅在计算机视觉、语言识别等传统计算机领域有重大突破,还在医学研究领域[2]和自然气候研究领域[3]中也有着良好的表现。不同于一般的深度学习模型,CNN 模型的结构除了输入层和全连接层两个基本部分之外,还特别提出了卷积层与池化层两个新的概念,用于提取特征时对其进行卷积操作。值得一提的是,这 2 个新的结构层之间的节点并不需要全部连接,只需选取其中一部分的节点相连通即可。这样的结构可以使模型的多个节点共享权重值,进而将模型内部无用的参数清理干净。

CNN 模型的训练方式有 2 种,即:前向传播和方向传播。凭借其优异的内部结构,既可以提出数据中的多个局部特征,也能够挖掘数据深层次的隐含特征,现在 CNN 模型已经成为了深度学习方法中备注学界关注的算法模型。

1.2 循环神经网络

循环神经网络(RNN)[4]将时间的概念引入到了传统神经网络结构之中,在一个长度相同的时间段之中不断进行循环和递归操作,每一个当前时刻隐藏层的状态都由上一时刻隐藏层输出的状态和当前时刻输入的状态共同决定。这种独特的结构使 RNN 模型可以获取数据中的隐含特征,还能够对互相关联的特征进行挖掘。

长短期记忆人工神经网络模型(Long Short-Term Memory, LSTM)[5]是 RNN 的一种变体模型。最初提出是为了解决 RNN 模型无法处理长序列以及梯度爆炸的问题。LSTM 模型提出了神经元(cell)结构,在 RNN 模型的基础上设置了遗忘门、输入门以及输出门三个结构。通过设置门结构,有选择地保留或删除信息,在保留了对上下数据信息的记忆功能的基础上,增加了剔除无用数据信息的能力,LSTM 模型具体的内部结构如图 1 所示。

LSTM 模型的具体工作原理可以由以下公式来表示,即:

$$f_t = \sigma(W^f x_t + U^f h_{t-1}), \tag{1}$$

$$i_t = \sigma(W^i x_t + U^i h_{t-1}), \tag{2}$$

$$o_t = \sigma(W^o x_t + U^o h_{t-1}), \tag{3}$$

$$u_t = \tanh(W^u x_t + U^u h_{t-1}), \tag{4}$$

$$c_t = c_t \otimes u_t + f_t \otimes c_{t-1}, \tag{5}$$

$$h_t = o_t \otimes \tanh(c_t). \tag{6}$$

其中, W^f、W^i、W^o、W^u 是 4 个不同权重值; σ 和 tanh 表示门结构中 2 种激活函数;在某一时刻 t,x_t 表示当前的输入信息;h_{t-1} 表示上一时刻保留下的隐藏层的状态信息;$\otimes$ 表示元素点乘计算;遗忘门 f_t 用来控制剔除当前状态下的无用信息;输入门 i_t 用于引入需要处理的信息;输出信息则由输出门 o_t 负责控制;u_t 表示的是需要保留到下一时刻的状态信息;h_t 则是经过处理后最终输入到下一时刻的状态信息。

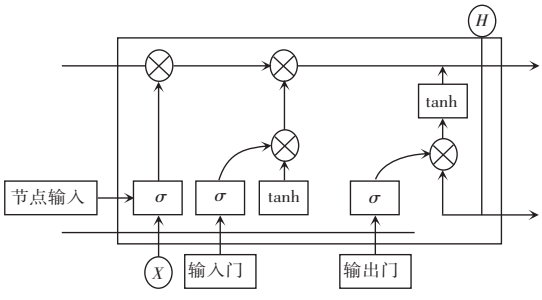

图 1 LSTM 模型的内部结构

Fig. 1 Internal structure of the LSTM model

1.3 华为访问控制列表技术

访问控制列表(ACL)技术[6]目前在控制网络资源的访问能力方面得到了广泛的应用,这是一种针对路由器设备基于包过滤的流量控制技术。通过输入一定的配置命令生成控制列表,把源地址、目的地址以及端口号作为数据包检查的基本元素,并可以设置一定规定,是否让符合条件的数据包通过路由器,进入到下一阶段网络,ACL 技术实例如图 2 所示。

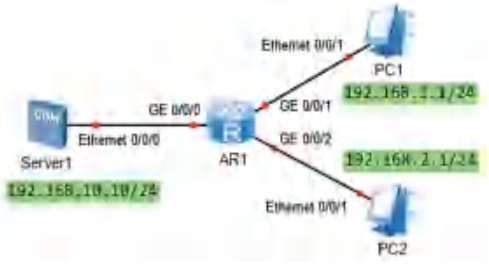

图 2 ACL 技术实例

Fig. 2 ACL technology example

配置华为标准的 acl,配置命令如下:

[R1]acl 2000

[R1-acl-basic-2000]rule 5 deny source 192.168.1.1 0

[R1-acl-basic-2000]rule 10 permit source any

此时在 R1 的 g0/0/1 的接口调用 acl2000,配置

命令如下：

[R1]interface g0/0/1

[R1 - GigabitEthernet0/0/1] traffic - filter inbound acl 2000

调用 acl2000 之后，再进行测试，发现 PC1 与服务器已经不通了，如图 3 所示。

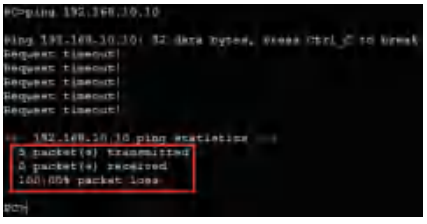

图 3　主机 PC1 的 Ping IP 界面

Fig. 3　Ping IP interface of host PC1

2　模型构建及实验准备工作

2.1　数据集

本文主要目标是针对网络用户入侵行为检测的研究，基于深度学习理论训练入侵行为检测模型，这就需要大量有效的实验数据，所以实验环节中，使用的数据集是 KDD-CUP99 的网络入侵检测数据集。KDD-CUP99 数据集是开源的，总共有 500 万条记录。此外，还分别提供了一个容量为 10%的训练子集和测试子集，在网络上可以下载到全套的 KDD-CUP99 数据集。

2.2　构造模型

在 KDD-CUP99 数据集中，有 8 个特征数据会受到时间因素的影响，分别是：'service'、'src_bytes'、'dst_host_diff_srv_rate'、'dst_host_rerror_rate'、'dst_bytes'、'hot'、'num_failed_logins'、'dst_host_srv_count'，可以用于构造符合时间序列的数据。由于 LSTM 模型在处理时间序列数据，并在预测结果方面表现得越来越好，所以本实验会基于 LSTM 模型对用户的入侵行为进行检测，详细的模型构造如图 4 所示。

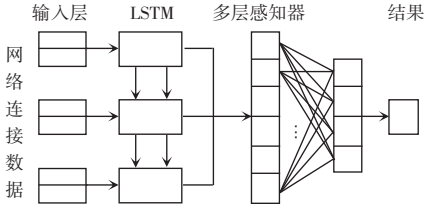

图 4　基于 LSTM 的用户的入侵行为进行检测模型

Fig. 4　LSTM-based user intrusion behavior detection model

本实验中，LSTM 模型的输入数据是 KDD-CUP99 原始数据集自带的容量为 10%的训练子集。LSTM 模型每次输入的数据长度为 T，输入样本选择的是某条网络连接的前 T s 的连接数据信息，标签也就是预测的行为标识，是第 $T+1$ s 的行为类别，这样就可以通过前 T s 的网络连接数据来预测第 $T+1$ s 的行为是正常行为、还是攻击行为。将该训练子集的数据信息输入到 LSTM 模型里面时，还需要满足输入层要求的维度，因此输入的 shape 是一个形如(samples, timesteps, input_dim)的 3D 张量。

LSTM 模型接收网络连接的数据，经历 15 个隐藏层的计算之后把数据输入到全连接层，最后得到网络连接数据的特征向量；将得到的特征向量输入到新的全连接网络模型中，并使用 Dropout 方法来防止模型出现过拟合问题。

本实验中的 LSTM 模型输入层具有 8 个特征，共 78 个维度，输出层具有 1 个标签，共 40 个维度，使用的激活函数为 Sigmoid 函数，在模型的最后加入一个用 100 个神经元构成的全连接层深度网络，以此作为模型最后预测结果的输出。

3　用户行为检测实验及设备应用实现

3.1　实验环境

神经网络模型的搭建对于实验设备的硬件要求较高，具体的实验环境配置见表 1。

表 1　硬件环境配置

Tab. 1　Hardware environment configuration

配置项	配置内容
操作系统	Windows 10
处理器	Intel(R) Core(TM) i7-8750H CPU @ 2.20 GHz 2.21 GHz
显卡	NVIDIA GeForce GTX 1060 6 GB
硬盘	SSD 512 GB
内存	16.0 GB

3.2　评价指标

对于用户入侵行为检测实验，典型评价指标主要有：准确率 ACC、漏报率 FNR、误报率 FPR[7] 和精确率及召回率的调和均值 $F_1-score$，若要计算 $F_1-score$(F_1 值)，还需要引入 2 个中间值即精确率 PRE 和召回率 REC。准确率、漏报率、误报率、精确率、召回率和精确率及召回率的调和均值的定义可由下面的公式来表示，即：

$$ACC=\frac{TP+TN}{TP+FN+FP+TN},\tag{7}$$

$$FNR=\frac{FN}{TP+FN},\tag{8}$$

$$FPR=\frac{FP}{FP+TN},\tag{9}$$

$$PRE=\frac{TP}{TP+FP},\tag{10}$$

$$REC = \frac{TP}{TP + FN}, \tag{11}$$

$$F_1 = \frac{2 * (REC * PRE)}{REC + PRE} = \frac{2TP}{2TP + FP + FN}. \tag{12}$$

3.3 实验流程

使用卷积和循环神经网络模型进行网络用户入侵行为检测的实验流程如下：

(1)对 KDD-CUP99 数据集提供的训练子集进行预处理操作,共分为 6 步,分别是添加列标签、对数据集进行统计、数据标准化、行为标识分类、符号特征数值化和数据归一化。

(2)将预处理完成的训练子集输入到 LSTM 模型中,设置初始参数见表 2,开始训练网络用户入侵行为检测模型。

表 2 实验详细参数

Tab. 2 Experimental detailed parameters

配置参数	参数值
迭代次数	10
每层神经元个数	160
隐藏层个数	15
激活函数	Sigmoid
初始学习率	0.001
Dropout	0.7
样本批次大小	128

(3)设置 2 类对照实验,分别为:基于 LSTM 模型的不同网络层数对用户入侵行为检测的影响和基于不同深度学习模型对用户入侵行为检测的影响。

3.4 实验结果

按照上述实验流程进行实验和对照实验后,生成的实验结果见表 3、表 4。

表 3 不同网络层数实验结果

Tab. 3 Experimental results of different network layers

LSTM 层数	*ACC*/%	*FNR*/%	*FPR*/%	F_1 - *score*/%	平均时间/s
12	97.2	2.77	2.87	91.8	56.34
15	98.3	2.69	2.37	93.5	68.75
18	96.5	2.92	2.88	89.7	79.26

表 4 不同网络模型实验结果

Tab. 4 Experimental results of different network model

	ACC/%	*FNR*/%	*FPR*/%	F_1 - *score*/%	平均时间/s
CNN	91.9	3.81	4.06	87.6	95.60
LSTM	98.3	2.69	2.37	93.5	68.75

由表 3 和表 4 分析发现,基于 LSTM 模型并且将网络层数设置为 15 层的时候,实验的效果是最好的,即入侵行为检测的准确度是最高的。

3.5 设备应用实现

设计出一个网络拓扑图,用于网络用户入侵行为检测模型与华为设备结合应用的实验,网络拓扑如图 5 所示。

图 5 设备应用实验网络拓扑

Fig. 5 Device application experiment network topology

通过已经训练好的模型对网络连接进行检测,根据检测的结果来对华为设备进行管控,使模型具有实用价值。华为 eNSP 模拟器负责模拟真实的实验设备环境,网络用户入侵行为检测与华为设备相结合的应用具体实现步骤如下：

(1)配置 Telnet 服务。Telnet 协议[8]是 TCP/IP 协议族中的一部分,也是远程登录服务的标准协议和主要手段,为用户提供了在本地计算机上完成远程主机工作的能力。

(2)设备云与本机网卡实现对连。华为云设备(Cloud)可以与本机的网卡对连,实现使用本机就可以控制虚拟设备的功能。华为 eNSP 模拟器是一个模拟虚拟化设备的软件,并不像真实的设备一样。为了能够使得操作设备更加简便,eNSP 模拟器提供了一种云设备,可以使本地计算机轻松地访问这些虚拟设备,方便对其进行配置。

(3)通过 Python 脚本程序对设备进行配置。对华为设备的具体配置操作,可以通过预置一个 Python 脚本程序来实现。通过使用 Python 语言第三方程序库中的 Paramiko 模块,来实现远程登录华为设备并处理简单的配置命令。Paramiko 模块是对 SSHv2 协议的 Python 实现,提供了客户端与服务器功能,而其本身是一个围绕 SSH 网络概念的 Python 接口,有了该接口以后,就可以在 Python 代码中直接用 SSH 协议对远程服务器执行操作。

4 用户入侵行为分析结果管理功能实现

实现用户入侵行为分析结果管理功能主要是为了展示检测实验的效果,用于显示被拦截网络连接的基本信息,包括设别名称、设备端口、源 IP 地址和目的 IP 地址,同时还显示网络连接被拦截的时间、

处理状态、处理人和处理时间。设备管理员可以通过删除操作，来删除已经被误拦截的网络连接，保证正常的网络连接准确地到达用户主机。

导入 Python 第三方程序库中的 socket 模块、flask. request 模块。在用户入侵行为分析结果管理功能中的“analysis.py”文件中编写 get_request_ip( ) 函数和 get_my_ip( ) 函数，分别用来获取源主机的 IP 地址和目标主机的 IP 地址；编写 net_del( ) 函数实现删除网络连接的操作，入侵行为分析结果管理页面如图 6 所示。

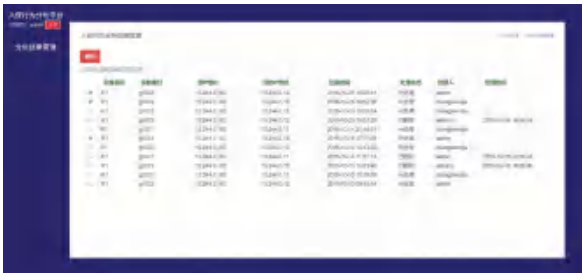

图 6　分析结果管理页面

Fig. 6　Analysis result management page

5　结束语

虽然本文提出的网络用户入侵行为智能化检测模块在检测入侵行为时取得了一定的效果，但是还是存在一些亟待解决的问题，详述如下。

(1)训练模型时没有与机器学习的算法作对照实验，同时也没有与混合模型作对照试验，只是与卷积神经网络(CNN)的实验结果进行了对比。仅仅使用 LSTM 模型，检测的准确率为 98.3%，在理论上依旧存在误检测的问题。下一步则要和其他算法、模型进行对比，确定使用一个检测准确率最高的方法。

(2)检测只有正常行为和攻击行为这两种结果，并没有将攻击行为中的 4 种攻击方式细分开来，所以无法提炼出详细的预防和检测入侵行为的策略。下一步则要按照不同的攻击方式，总结出不同的预防和防范策略。

总结来说，本文提出的网络用户入侵行为智能化检测模块有一定的实用价值，能够解放大量的人力，通过“人机合作”的模式，保障用户上网安全。在网络安全形势日益严峻的背景下，本课题的深入探讨研究则有着重要的现实意义。

参考文献

[1] 汤沁泉. 基于网络行为分析的网络安全预警系统设计与实现[D]. 南京：南京理工大学，2015.

[2] WALLACH I，DZAMBA M，HEIFETS A. AtomNet：A Deep Convolutional Neural Network for bioactivity prediction in structure-based drug discovery[J]. Mathematische Zeitschrift，2015，47(1)：34.

[3] LIU Yuejie，RACAH E，PRABHAT，et al. Application of deep Convolutional Neural Networks for detecting extreme weather in climate datasets[J]. arXiv preprint arXiv：1605.01156，2016.

[4] MIKOLOV T，KOMBRINK S，BURGET L，et al. Exentsions of recurrent Neural network language model[C]// 2011 IEEE International Conference on Acoustics，Speech and Signal Processing (ICASSP). Praha：IEEE，2011：5528.

[5] GRAVES A. Supervised sequence labelling with Recurrent Neural Networks[M]. Berlin/ Heidelberg：Springer-Verlag ，2011.

[6] 梁娟娟，廖翔. 论访问控制列表 ACL 在校园网中的应用[J]. 计算机产品与流通，2018(2)：211.

[7] AMBUSAIDI M A，HE Xiangjian，NANDA P，et al. Building an intrusion detection system using a filter-based feature selection algorithm[J]. IEEE Transactions on Computers，2016，65(10)：2986.

[8] 李彪，陈勋. 局域网组网技术[M]. 哈尔滨：哈尔滨工程大学出版社，2010.

(上接第 244 页)

[4] 熊仕勇，陈春俊，王锋，等. 一种新的轨距动态检测方法研究[J]. 铁道科学与工程学报，2018，15(7)：1825.

[5] 康飞. 基于机器视觉的轨道检测系统研究[D]. 兰州：兰州交通大学，2014.

[6] 闵永智，王红霞，康飞，等. 基于图像式传感器的铁路轨距检测系统研究[J]. 激光技术，2015，39(3)：344.

[7] 邓丽华，孙福强，刘宇，等. 非接触式位移传感器在动响应测试中的应用研究[J]. 电子技术与软件工程，2014(12)：265.

[8] CIFUENTES C A，FRIZERA A，CARELLI R，et al. Human-robot interaction based on wearable IMU sensor and laser range finder[J]. Robotics and Autonomous Systems，2014，62(10)：1425.

[9] 李龙民. 基于 FPGA 的激光测距系统的研究[D]. 长春：长春理工大学，2017.

[10] 王振宇，李烨，郁丰，等. 一种激光三角测量的标定方法及误差分析[J]. 激光技术，2017，41(4)：521.

[11] 朱旭芳，朱小芳. 24 位模数转换器 AD7190 原理及应用[J]. 软件导刊，2015，14(3)：24.

[12] 晁元德. 高精度 24 位模数转换器 AD7176-2 的原理及应用[J]. 自动化与仪器仪表，2014(8)：79.

[13] 周海涛，董全林，周卫宁. ADS1256 在多路高精度加速度计数据采集中的应用[J]. 航空电子技术，2009，40(4)：15.

[14] 陈雨彤. 基于最小二乘法的线性回归方程推导与应用分析[J]. 中国新通信，2018，20(24)：206-208.

[15] 张丽丽. 最小二乘问题的算法与应用研究[D]. 北京：华北电力大学(北京)，2017.