基于流量时空特征的fast-flux僵尸网络检测方法

牛伟纳[①] 蒋天宇[①] 张小松[*①②] 谢 娇[①] 张俊哲[③] 赵振扉[①]

[①](电子科技大学计算机科学与工程学院/网络空间安全研究院 成都 611731)

[②](鹏城实验室网络空间安全研究中心 深圳 518040)

[③](四川大学网络空间安全学院 成都 610065)

摘 要：僵尸网络已成为网络空间安全的主要威胁之一，虽然目前可通过逆向工程等技术来对其进行检测，但是使用了诸如fast-flux等隐蔽技术的僵尸网络可以绕过现有的安全检测并继续存活。现有的fast-flux僵尸网络检测方法主要分为主动和被动两种，前者会造成较大的网络负载，后者存在特征值提取繁琐的问题。因此为了有效检测fast-flux僵尸网络并解决传统检测方法中存在的问题，该文结合卷积神经网络和循环神经网络，提出了基于流量时空特征的fast-flux僵尸网络检测方法。结合CTU-13和ISOT公开数据集的实验结果表明，该文所提检测方法和其他方法相比，准确率提升至98.3%，召回率提升至96.7%，精确度提升至97.5%。

关键词：僵尸网络；Fast-flux；卷积神经网络；循环神经网络

中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2020)08-1872-09

DOI: 10.11999/JEIT190724

Fast-flux Botnet Detection Method Based on Spatiotemporal Feature of Network Traffic

NIU Weina[①] JIANG Tianyu[①] ZHANG Xiaosong[①②] XIE Jiao[①]

ZHANG Junzhe[③] ZHAO Zhenfei[①]

[①](*Institute for Cyber Security*, *School of Computer Science and Engineering*, *University of Electronic Science and Technology of China*, *Chengdu* 611731, *China*)

[②](*Cyberspace Security Research Center*, *Peng Cheng Laboratory*, *Shenzhen* 518040, *China*)

[③](*College of Cybersecurity*, *Sichuan University*, *Chengdu* 610065, *China*)

Abstract: Botnets have become one of the main threats to cyberspace security. Although they can be detected by techniques such as reverse engineering, botnets using covert technologies such as fast-flux can successfully bypass existing security detection and continue to survive. The existing fast-flux botnet detection methods are mainly divided into active and passive, the former will cause a large network load, and the latter has the problem of cumbersome feature value extraction. In order to effectively detect fast-flux botnets and alleviate the problems in traditional detection methods, a fast-flux botnet detection method based on spatiotemporal features of network traffic is proposed, combined with convolutional neural networks and recurrent neural network models, the fast-flux botnet is detected from both spatial and temporal dimensions. Experiments performed on the CTU-13 and ISOT public data sets show that compared with other methods, the accuracy rate of the proposed method is 98.3%, the recall rate is 96.7%, and the accuracy is 97.5%.

Key words: Botnet; Fast-flux; Convolutional Neural Network (CNN); Recurrent Neural Network (RNN)

收稿日期：2019-09-19；改回日期：2020-04-18；网络出版：2020-05-12

*通信作者： 张小松 johnsonzxs@uestc.edu.cn

基金项目：国家重点研发计划(2016QY06X1205, 2018YFB0804050)，国家自然科学基金(61572115)

Foundation Items: The National Key Research and Development Program of China (2016QY06X1205, 2018YFB0804050), The National Natural Science Foundation of China (61572115)

1　引言

随着互联网技术的飞速发展，不法分子也开始利用网络来牟取非法利益，僵尸网络(botnet)便是犯罪分子经常采用的一种攻击手段。fast-flux技术是近年来僵尸网络使用的一种躲避检测的技术，2017年阿卡迈技术公司在其公布的白皮书中提到[1]，fast-flux僵尸网络包含一些分配在全球100强公司地址空间内的IP地址，这些地址可以被网络所有者用来进行欺诈行为。fast-flux僵尸网络危害巨大，可以用于执行恶意活动[2]，例如向用户传递恶意软件或窃取用户凭据。因此，如何有效检测出fast-flux僵尸网络已成为网络空间安全领域的热点研究方向之一。

目前研究人员已经针对fast-flux僵尸网络进行了大量研究，现有的fast-flux僵尸网络检测方法主要分为以下两种：

基于主动的检测方法：这种类型的检测方法主要通过主动收集垃圾邮件或者使用搜索引擎来获得域名，并通过查询域名系统(Domain Name System, DNS)进而获得相关的IP地址信息，从而生成fast-flux僵尸网络的恶意特征。这种检测方法往往会使用到域名分析或通过搜索引擎的返回结果来识别僵尸网络域名。Zang等人[3]提出了一种fast-flux僵尸网络检测方案，该方法可以识别由域生成算法生成的域组或代表不同僵尸网络的变量。Ai-Duwairi等人[4]提出一种基于搜索引擎的检测方法，通过查询包含了与可疑域名相关联的IP地址以及谷歌搜索引擎返回的结果页面，采用命中次数来判断fast-flux僵尸网络。但是这些基于主动的检测会耗用大量的内存，并且产生较大的网络负载，往往会产生较大的延迟。

基于被动的检测方法：这种方法是通过收集网络上的流量，进而提取恶意数据的特征值。这也是目前主流的检测方法，既减轻了网络设备的负担，又能快速准确地实施检测。Alieyan等人[5]采用数据挖掘技术对fast-flux僵尸网络流量进行检测。该方法使用支持向量机(Support Vector Machine, SVM)算法来区分正常网络域名访问和fast-flux僵尸网络域名访问。Almomani等人[6]提出了fast-flux猎人(Fast-Flux Hunter, FFH)检测系统，FFH采用自适应演化模糊神经网络算法，其可作为监督学习和无监督学习的混合在线学习系统，不断学习收集到的fast-flux数据。此外，文献[7–15]也都是通过收集DNS流量，使用人工智能算法来检测fast-flux僵尸网络。

综合来看，目前对于fast-flux僵尸网络的研究方法主要是针对DNS流量进行的，fast-flux技术虽拥有庞大的IP地址池，但恶意域名服务器的数量较少，因此使用DNS流量进行检测能够拥有更好的效果。近几年学术界也侧重于运用机器学习的方法来检测fast-flux僵尸网络，然而基于机器学习的检测方法往往需要提取大量数据特征，如何合理地选取、处理特征值仍然是其需要面对的难题。因此，本文基于深度学习的方法，提出一种不依赖于特征值提取的检测方法，同时使用两种深度学习模型结合流量时空特征来对fast-flux僵尸网络进行检测。

本文针对目前主流检测方法的缺点，提出一种新的fast-flux僵尸网络检测方法，通过使用深度学习网络来结合空间和时序两种特征来检测fast-flux僵尸网络。此外，由于本文所提方法可以自动化提取特征，有效减少了人工主观提取特征值所带来的检测效果误差。本文的主要贡献如下：(1)进行fast-flux僵尸网络的空间特征的研究。使用卷积神经网络的方法来发现fast-flux僵尸网络的流量数据在空间层面上的特征，进而得到空间特征向量。(2)进行fast-flux僵尸网络的时序特征的研究。使用循环神经网络的方法来发现fast-flux僵尸网络的网络流量在时序层面上的特征，进而得到时序特征向量。(3)对空间和时序特征进行结合，得到时空特征，对fast-flux僵尸网络进行检测。

本文的总体组织结构安排如下。第2节：基于时空特征的fast-Flux僵尸网络检测方法，主要介绍本文方法的工作原理以及使用的模型技术。第3节：实验分析，主要介绍本文方法的检测效果以及与其他方法的对比结果情况。第4节：总结，主要对本文的检测方法进行归纳总结。

2　基于时空特征的Fast-Flux僵尸网络检测方法

本文所提基于时空特征的fast-flux僵尸网络检测方法总统架构如图1所示。首先对数据集进行预处理，将网络流数据转换为灰度图，再转化为符合空间特征模块输入要求的数据格式。在得到空间特征向量之后还需要将其输入到时间特征训练模块中来获得时空特征模型，最后将时空特征模型输入到softmax分类器中进行检测。接下来，将按照模块对所提方法进行具体介绍。

2.1　预处理模块

本文所使用的原始数据为流量数据，数据集的格式为pcap包。数据需经过预处理，转换数据格式，以匹配特征学习模型的输入格式，数据处理模块流程如图2所示。

本文所提方法主要是针对DNS数据响应包进行分析，因为响应包中包含了绝大部分请求数据包中

的有效信息。本文使用脚本工具将数据包的IP地址进行随机化操作以及清洗操作。此外本文截取每个数据流前1024 B的数据，如果某条数据流长度不够1024 B，则在末尾用0x00进行填充。

在对数据流进行统一化处理之后，需要将其转化为图片格式：对于本文统一化处理之后的数据(1024 B)，对每字节数据进行处理，将其变为8位的灰度像素，处理后的数据流转变为32×32的灰度图，可以观察的图片如图3所示。

从图3可知，正常的流量数据可视化之后的差别较为明显，但fast-flux僵尸网络的流量数据经可视化后却是相似的。因此可推测使用CNN对图片分类的方法来进行流量检测是有效的。

2.2 空间学习模块

本文的空间特征学习模型使用DenseNet网络，这种学习模型通过后面层与前面所有层建立密集连接来改进深度学习网络，减少了网络的参数量的同时可以提高学习效率。DenseNet的核心设计如图4所示。

在DenseNet模型中，第n层会和前面的n–1层都进行连接，并将结果作为下一层的输入。本文所使用的网络有5层，而5层的网络会包含15个连接(m层网络会有$m(m+1)/2$个连接)，这使得DenseNet网络变成了密集连接。DenseNet网络因为对所有层的特征图之间进行了连接，所以加强了特征的传递，能够更有效地利用特征，减轻了梯度

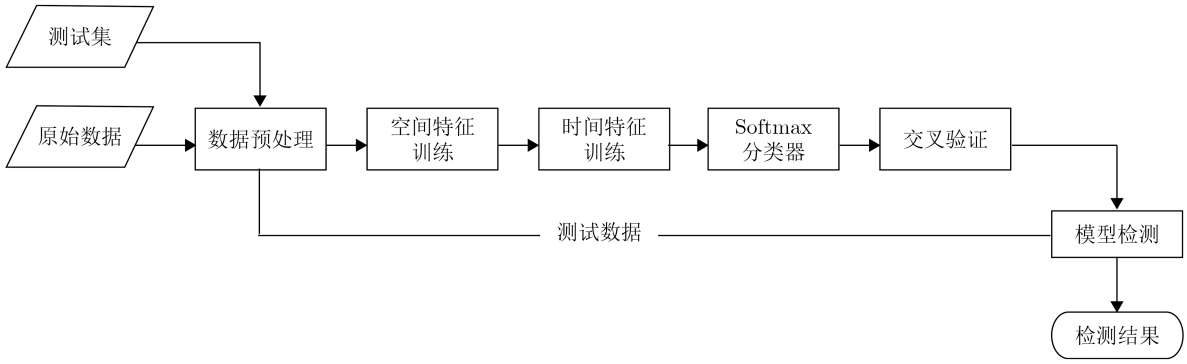


图 1 总体框架设计图

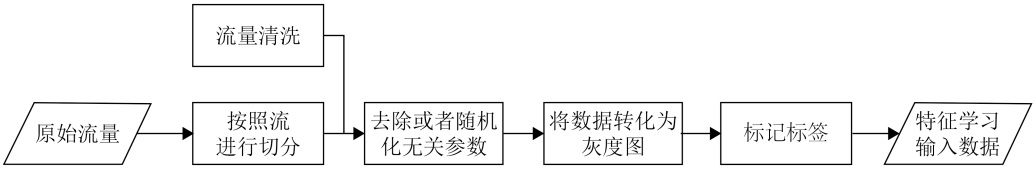
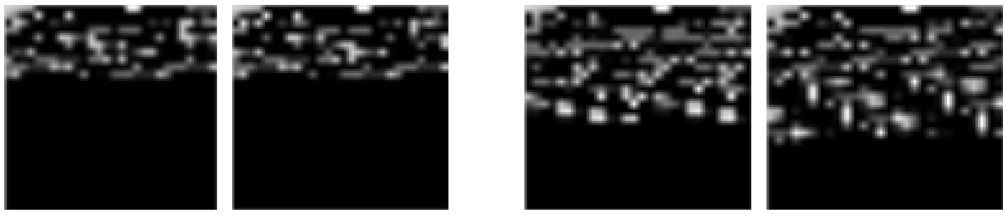


图 2 模块预处理流程图



(a) Fast-flux僵尸网络流量 (b) 正常网络流量

图 3 正常流量和fast-flux流量的可视化结果

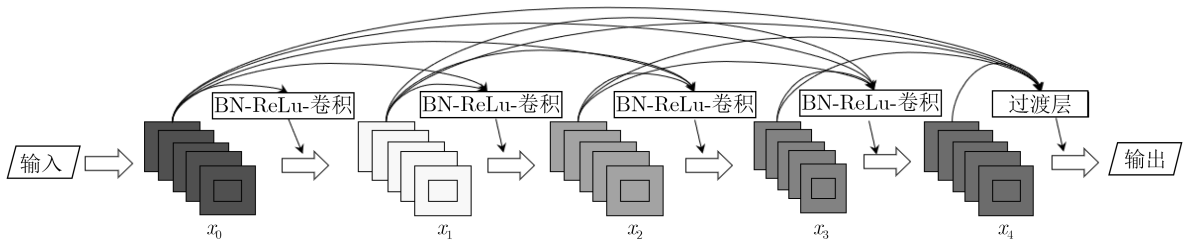


图 4 Dense block设计

消失的问题。结合fast-flux僵尸网络的特点，该网络相较于其他比较传统的方法有更好的上下文关联性，具体会在2.4节进行描述。这个过程用式(1)表示

$$x_l = H_l\left([x_0, x_1, \cdots, x_{l-1}]\right) \tag{1}$$

其中，$[x_0, x_1, \cdots, x_{l-1}]$表示对前面0到$l$–1层的输出特征图进行联级操作，对通道进行合并。$H_l$包括卷积、BN等操作。

空间特征获取算法的整体流程图如图5所示。

下面详细描述使用DenseNet模型来得到空间特征模型的流程。

(1) 卷积层C1：输入为32×32的原始数据，卷积步长为1，卷积核大小为3×3，卷积核数设置为16，最后得到16个大小为32×32的特征图。

(2) Dense block层D1：卷积层C1输出的32×32的特征图，经过该层12个1×1和3×3的卷积操作，其中前面5层的输出结合起来作为第6个子结构的输入，从而得到大小为32×32的特征图。

(3) 过渡层T1：连接两个dense block，对于上一个D1的输出通过1个1×1的卷积层和步长为2, 2×2的池化层的处理，输出16×16的特征图。

(4) Dense block层D2：对于T1层输出的16×16的特征图进行第2次密集卷积的操作，包括12个1×1和3×3的卷积操作，得到大小为16×16的特征图。

(5) 过渡层T2：对于上一个D2的输出通过1个1×1的卷积层和步长为2, 2×2的池化层，输出8×8的中间特征图。

(6) Dense block层D3：对于T2层输出的8×8的特征图进行第3次密集卷积的操作，其中包括24个1×1和3×3的卷积操作，得到大小为8×8的特征图。

2.3 时序特征学习模块

为了进一步提高对fast-flux僵尸网络流量的检测效果，还需要对流量数据在时间层面上的表现特征进行学习，因此本文采用循环神经网络(Recurrent Neural Network, RNN)中的长短期记忆(Long Short-Term Memory, LSTM)网络进行时间特征的学习检测。在fast-flux僵尸网络所产生的流量数据中，当前的分组数据可能和前面的分组数据之间有着关联关系，因此与其他RNN网络相比，使用LSTM网络会更贴合检测fast-flux僵尸网络的应用场景。

为了应对实际网络和僵尸网络的通信情况，更准确地获得时序特征，本文使用了双向LSTM网络(Bi-directional LSTM, BiLSTM)，并对层数进行了修改：先使用经过空间特征训练学习的数据中的字节序列作为输入，然后将数据分组训练得到数据包特征向量，再将得到的数据包特征向量序列作为下一层的输入，这样依次共经过4层分组训练，最后会得到整个数据组特征向量，即时间维度特征。整个时序特征的结构图如图6所示。

BiLSTM的模型具体训练过程如下：

(1) LSTM层L1：由128个单元构成，输入为经过空间特征训练后的字节序列，输出为128个256维向量。

(2) 全连接层D1：由256个神经元构成，输出为256维向量。

(3) LSTM层L2：由64个单元构成，输入为D1层处理之后的字节特征数据，输出为64个256维向量。

(4) 全连接层D2：由128个神经元构成，输出为128维向量。

(5) LSTM层L3：由32个单元构成，输入为D2层处理之后包特征数据，输出为32个256维向量。

(6) 全连接层D3：由64个神经元构成，输出为64维向量。

(7) LSTM层L4：由16个单元构成，输入为

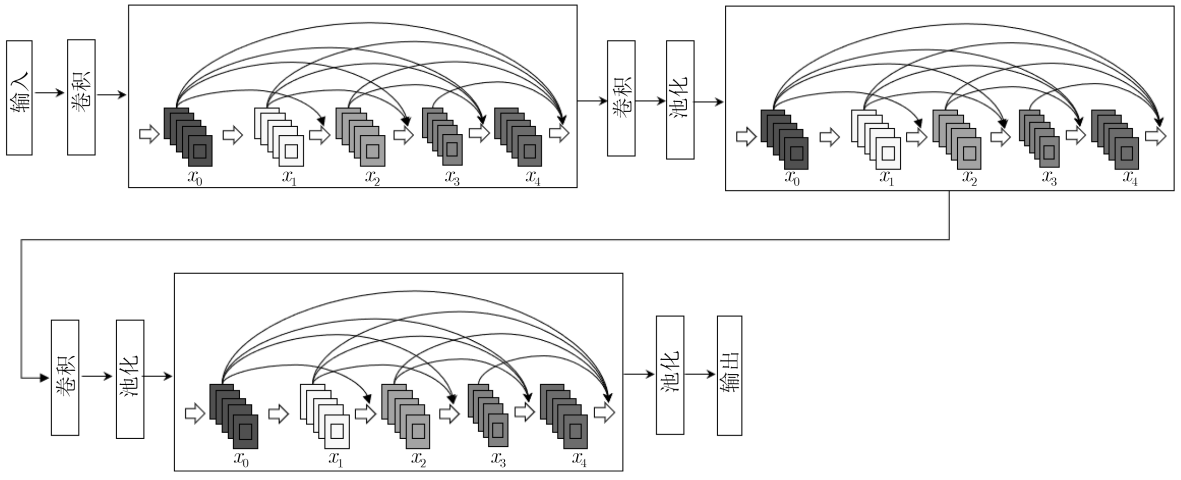


图 5 DenseNet模型整体结构

D3层处理之后的流特征数据，输出为16个256维向量。

(8) 全连接层D4：由8个神经元构成，输出为8维向量。

2.4 特征融合验证

本文之所以选择这两种深度学习网络，除了模型训练的高效性以外，还由僵尸网络本身的通信特征决定的。使用fast-flux技术的僵尸网络，其访问的IP地址是不断变化的，但是当IP地址发生变化的时候，控制主机需要通知僵尸网络的其他主机和组件发生了变化，即主机发出了某条指令之后，访问的IP都会发生变化，这样僵尸网络的通信流量会出现明显的上下文关联特征。如果使用的是预设好的规则，在IP池中循环改变IP地址的方法，那么IP地址的变换也会有一定规律，即会按照一定的顺序访问这些IP主机，产生的通信流量的上下文也是有关联的，不像正常访问流量一样，上下文流量没有明显的联系。

从2.1节中可以直观地看到，fast-flux僵尸网络在灰度图中具有很明显的特征，这种从数据流量转化的图片上面可以学习到的特征可以被认为是“空间特征”，它反映了数据流量本身的特征。但是考虑到上面所提到的fast-flux僵尸网络本身的特点，本文所提方法在获得空间特征之后，还需要学习时间维度上的特征，包括周期性、上下文关联性等等。因此考虑这些因素，在对比了其他僵尸网络检测方法(如FFH等)，本文选择了DenseNet和BiLSTM这两种深度学习网络。DenseNet通过采用密集连接以及concat的方式，充分利用之前各层的特征信息，从而可以更好地学习流量之间的关联特征信息，可以输出存在前后依赖关系的特征，有着良好的上下文信息优势。而BiLSTM网络本身被广泛用于上下文关联学习[16]，可以进一步加强DenseNet的训练结果，并且本文对BiLSTM进行了改进，可以更好地来发掘和利用数据流量的特征。因此再加上综合了这些方面的特征之后，本文提出的方法可以更加准确地检测使用fast-flux的僵尸网络。

为了验证本文所采取方法的效果，本文通过设置对比试验，即(1)只使用CNN网络；(2)只使用RNN网络；(3)使用本文所提方法进行对比，来展示本文所提方法的提升效果。试验效果如图7和8所示。

从图7和图8的实验结果可以看出，本文所提时空特征模型在准确率和精确度上面都使用有了明显的提升。因此，本文所提方法能够通过串联CNN和RNN网络学习到流量特征的时间和空间特性，从而更精确地检测到fast-flux僵尸网络。

2.5 分类模块

(1) 分类器选择：本文使用softmax分类器来检测网络流量为正常流量还是fast-flux僵尸网络流

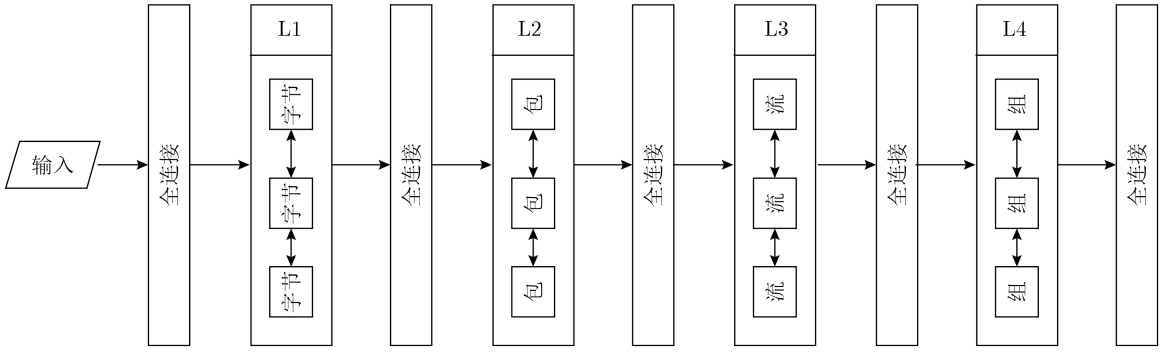


图 6 BiLSTM模型整体结构

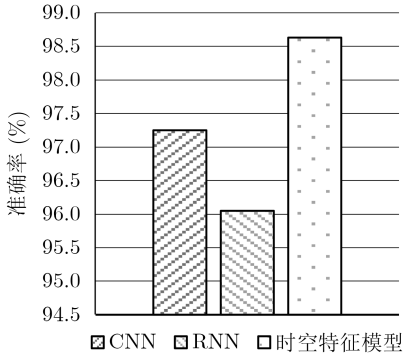


图 7 效果准确率对比

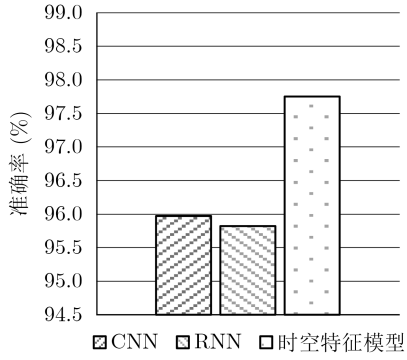


图 8 效果精确率对比

量。softmax分类器是目前人工智能网络中最常用的分类器之一。对于一个数组S来说，其每个元素的softmax值就是

$$\text{softmax}\left(s_i\right)=\frac{\mathrm{e}^{s_i}}{\sum_{j=1}^{N}\mathrm{e}^{s_j}},\ i=1,2,\cdots,N \tag{2}$$

其中，S_i表示模型对输入x在第i个类别上的评分值。本文最后的输出结果为两类。

(2) 损失函数：模型训练时，本文使用交叉熵作为损失函数来避免均方误差损失函数学习速率降低的问题。公式为

$$\begin{aligned}J\left(\theta\right)=&-\frac{1}{m}\sum_{i=1}^{m}y^{(i)}\lg\left(\boldsymbol{h}_\theta\left(x^{(i)}\right)\right)\\&+\left(1-y^{(i)}\right)\lg\left(1-\boldsymbol{h}_\theta\left(x^{(i)}\right)\right)\end{aligned} \tag{3}$$

其中，$\boldsymbol{h}$为权值矩阵，$x(i)$为样本输入，y为真实标签结果，m为样本个数。

3　实验分析

3.1　实验环境

由于本实验注重高速网络环境中fast-flux僵尸网络的检测，需要对流经系统的流量进行实时的处理判断，所以系统需具备良好的运算和高效的读写性能。硬件配置如表1所示，软件环境配置如表2所示。

3.2　数据集

本文的实验数据集由僵尸网络流量和正常网络流量两个部分组成。其中，僵尸网络流量一部分取自于布拉格捷克理工大学(Czech Technical University, CTU)大学收集并公开的数据，主要来源为CTU-13数据集[17]。除此之外，僵尸网络数据集还加入了ISOT 2010数据集[18]中的fast-flux僵尸网络流量。

表 1　实验硬件环境参数表

硬件	具体参数
服务器	戴尔PowerEdge R730XD
内存	4个金士顿16 GB
处理器	2个英特尔E5-2630
硬盘	东芝2 TB

表 2　实验软件环境参数表

软件	版本
操作系统	Cenos7
编译器	IntelliJ Idea
GCC	5.2.1
TensorFlow	1.1.1

正常流量取自于CTU数据集中所收集的正常流量，除此之外，为了保证测试数据集的准确性，本文还加入了自己所收集的正常DNS流量。其中，fast-flux流量和正常流量以1:1的比例进行训练和测试，具体的数据情况如表3。

3.3　评估方法

本文选择以下标准评价提出的方法：准确率(accuracy)，召回率(recall)和精确率(precision)。

准确率(ACCuracy)计算公式为

$$\text{ACC}=\frac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FP}+\text{FN}} \tag{4}$$

召回率(recall)计算公式为

$$\text{recall}=\frac{\text{TP}}{\text{TP}+\text{FN}} \tag{5}$$

精确度(P)计算公式为

$$P=\frac{\text{TP}}{\text{TP}+\text{FP}} \tag{6}$$

其中各参数的来源：假阴性(False Negative, FN)：被判定为正常流量，但是事实上是fast-flux僵尸网络流量；假阳性(False Positive, FP)：被判定为fast-flux僵尸网络流量，但事实上是正常流量；真阴性(True Negative, TN)：被判定为正常流量，事实上也是正常流量；真阳性(True Positive, TP)：被判定为fast-flux僵尸网络流量，事实上也是fast-flux僵尸网络流量。

3.4　实验数据

3.4.1　对比试验

对比实验本文采用了基于被动检测FFH[6]，基于统计的检测方法[19]，基于主动的检测方法Gflux[4]以及传统的机器学习方法随机森林算法[20]。其中FFH和Gflux已经在第1节进行了介绍。

基于随机森林的检测方法是一种重要的基于Bagging的集成学习方法，通过引入随机性来减少过拟合和提高抗噪声能力。为了验证其效果，采取和FFH相同的特征值进行训练。

而基于统计的检测方法是一种基于被动的DNS流量检测方法。主要通过分析网络中的流量，根据特征值分析来检测fast-flux僵尸网络攻击。该方法基于静态和历史这两种指标进行检测。

3.4.2　参数选择

第3节中提到，在对流量进行特征学习之前，

表 3　数据集组成表

数据类型	CTU-13	ISOT数据集	自收集
良性DNS流量	5133	0	2874
Fast-FluxDNS流量	4229	4003	0

需要对数据集进行预处理。为了方便选择合适的参数，本文针对会话切分的方式和数据流截取大小这两个参数进行试验验证，以确定较好的训练参数。

在对DNS流量数据进行切分时分别采用了会话切分(保留了请求和响应数据包)和流切分(保留DNS的响应数据包)，对以上两种方式的训练数据分别进行训练，结果如图9和10所示。实验结果显示，采用会话切分对于训练结果并没有提升。DNS响应数据包中已经包含了训练需要的特征值中绝大部分参数。

对于空间特征学习模块，本文分别构造了22×22, 23×23, …, 32×32, 35×35的图片训练集，训练结果如图11所示。结果表明当图像大于1024 Byte后，训练的准确率不会进一步提升，通过对数据的进一步分析发现98%以上的输入训练样本长度小于1024字节，因此本文选择32×32的图像进行训练。

3.4.3 实验对比结果

本文使用3.3节提到的3个指标，将本文所提方法和FFH[6]、统计方法[19]、GFlux[4]和随机森林[20]方法进行对比试验，结果图12、图13和图14所示。

可以看出，本文所提方法在准确率，召回率和精确度上面和对比方法相比都有提升，说明本文所用到的空间特征和时间特征相结合的检测方法可以更加有效地反映网络流量特性。经过25轮训练后准

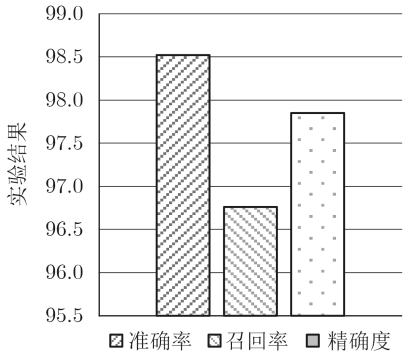


图 9 会话切割试验效果图

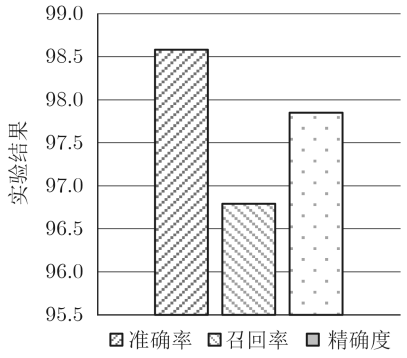


图 10 流切割试验效果图

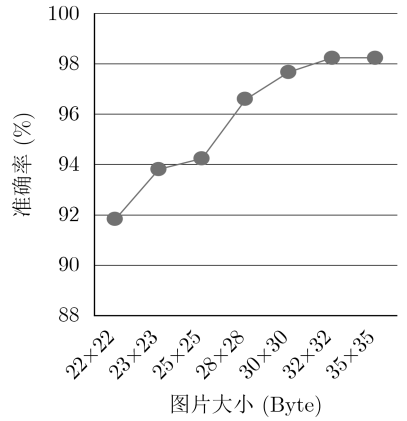


图 11 图片大小试验结果

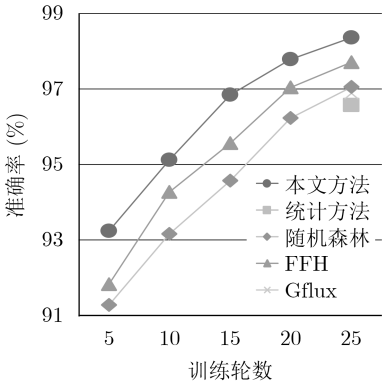


图 12 准确率对比图

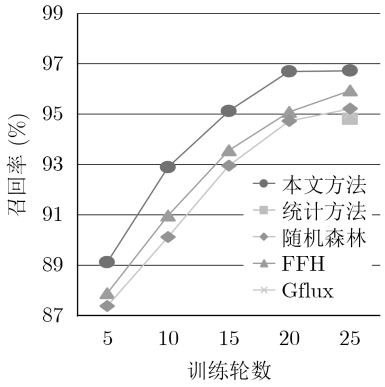


图 13 召回率对比图

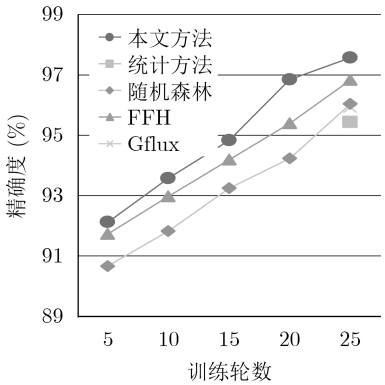


图 14 精确度对比图

确率值达到98.36%，相比较统计方法为96.57%，Gflux为96.88%，随机森林为97.05%，FFH为97.71%；召回率达到96.72%，统计方法为94.81%，Gflux为95.03%，随机森林为95.21%，FFH为95.95%；精确度达到97.57%，统计方法为95.43%，Gflux为95.91%，随机森林为96.04%，FFH为96.83%。本文方法使用了更适合fast-flux僵尸网络的深度学习模型，而随机森林、GFlux和FFH由于主要关注了数据流量本身的特性，较少考虑到流量传输时的前后关联。本文所采用的方法由于使用了CNN和RNN两种深度学习模型来提取的时间和空间特征，相比其他算法有着更好的准确率、召回率和精确度，也不需要人工提取特征值。

4　结论

随着fast-flux僵尸网络隐蔽技术和控制手段的不断发展，传统的基于机器学习的fast-flux僵尸网络检测方法已经越来越难以应对，而且还存在着人工提取、处理特征繁琐困难等一系列问题。为此，本文提出了一种使用深度学习网络的检测方法，本文的方法通过使用CNN和RNN两种深度学习网络，可以自动地从fast-flux僵尸网络流量中学习时间与空间两个维度上的特征。在获取空间特征时通过将网络流量转化为灰度图的方法，利用DenseNet网络来高效快速地完成训练；在获取时间特征后，再将从空间特征得到的特征数据作为输入，使用双向LSTM网络来进一步强化训练结果，从而得到完整的fast-flux僵尸网络时空特征。

本文的方法通过结合空间和时序特征对网络流量进行检测，将两种深度学习网络串联起来进行学习。本文的方法不需要人工提取特征选择，避免了繁琐的数据处理，减少了人工参与选择的误差。实验证明，相比于使用单一维度的机器学习检测方法具有更高的准确率以及精确度。

参 考 文 献

[1] OR K, RAVIV P, and GUY M. Digging deeper-an in-depth analysis of a fast flux network[EB/OL]. https://www.akamai.com/cn/zh/multimedia/documents/white-paper/digging-deeper-in-depth-analysis-of-fast-flux-network.pdf, 2017.

[2] 蒋鸿玲, 邵秀丽, 李耀芳. 基于MapReduce的僵尸网络在线检测算法[J]. 电子与信息学报, 2013, 35(7): 1732–1738.
JIANG Hongling, SHAO Xiuli, and LI Yaofang. Online botnet detection algorithm using MapReduce[J]. *Journal of Electronics & Information Technology*, 2013, 35(7): 1732–1738.

[3] ZANG Xiaodong, GONG Jian, MO Shaohuang, *et al*. Identifying fast-flux botnet with AGD names at the upper DNS hierarchy[J]. *IEEE Access*, 2018, 6: 69713–69727. doi: 10.1109/ACCESS.2018.2880884.

[4] AL-DUWAIRI B, AL-HAMMOURI A, ALDWAIRI M, *et al*. GFlux: A google-based system for Fast Flux detection[C]. 2015 IEEE Conference on Communications and Network Security (CNS), Florence, Italy, 2015: 755–756. doi: 10.1109/CNS.2015.7346920.

[5] ALIEYAN K, ANBAR M, ALMOMANI A, *et al*. Botnets detecting attack based on DNS features[C]. 2018 International Arab Conference on Information Technology (ACIT), Werdanye, Lebanon, 2018: 1–4. doi: 10.1109/ACIT.2018.8672582.

[6] ALMOMANI A. Fast-flux hunter: A system for filtering online fast-flux botnet[J]. *Neural Computing and Applications*, 2018, 29(7): 483–493. doi: 10.1007/s00521-016-2531-1.

[7] Al NAWASRAH A. Fast flux botnet detection based on adaptive dynamic evolving spiking neural network[D]. [Ph.D. dissertation], University of Salford, 2018.

[8] JIANG Cibin and LI J S. Exploring global IP-usage patterns in fast-flux service networks[J]. *Journal of Computers*, 2017, 12(4): 371–380.

[9] WANG Zhi, QIN Meilin, CHEN Mengqi, *et al*. Hiding fast flux botnet in plain email sight[C]. SecureComm 2017 International Workshops on Security and Privacy in Communication Networks, Niagara Falls, Canada, 2017: 182–197.

[10] REIMERS A C, BRUGGEMAN F J, OLIVIER B G, *et al*. Fast flux module detection using matroid theory[J]. *Journal of Computational Biology*, 2015, 22(5): 414–424. doi: 10.1089/cmb.2014.0141.

[11] ERQUIAGA M J, CATANIA C, and GARCÍA S. Detecting DGA malware traffic through behavioral models[C]. 2016 IEEE Biennial Congress of Argentina (ARGENCON), Buenos Aires, Argentina, 2016: 1–6. doi: 10.1109/ARGENCON.2016.7585238.

[12] TORABI S, BOUKHTOUTA A, ASSI C, *et al*. Detecting internet abuse by analyzing passive DNS traffic: A survey of implemented systems[J]. *IEEE Communications Surveys & Tutorials*, 2018, 20(4): 3389–3415. doi: 10.1109/COMST.2018.2849614.

[13] HSU F H, WANG C S, HSU C H, *et al*. Detect fast-flux domains through response time differences[J]. *IEEE Journal on Selected Areas in Communications*, 2014, 32(10): 1947–1956. doi: 10.1109/JSAC.2014.2358814.

[14] CELIK Z B and MCDANIEL P. Extending detection with privileged information via generalized distillation[C]. 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, USA, 2018: 83–88. doi: 10.1109/SPW.2018.00021.

[15] CHEN Wenlin, CHEN Yixin, and WEINBERGER K Q.

Fast flux discriminant for large-scale sparse nonlinear classification[C]. The 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, New York, 2014: 621–630.

[16] 田生伟, 周兴发, 禹龙, 等. 基于双向LSTM的维吾尔语事件因果关系抽取[J]. 电子与信息学报, 2018, 40(1): 200–208. doi: 10.11999/JEIT170402.
TIAN Shengwei, ZHOU Xingfa, YU Long, *et al*. Causal relation extraction of Uyghur events based on bidirectional Long Short-term Memory model[J]. *Journal of Electronics & Information Technology*, 2018, 40(1): 200–208. doi: 10.11999/JEIT170402.

[17] CTU University. MCFP Dataset-Malware Capture facility project[EB/OL]. https://mcfp.weebly.com/mcfp-dataset.html, 2018.

[18] University of Victoria. ISOT Botnet dataset[EB/OL]. https://www.uvic.ca/engineering/ece/isot/datasets/index.php, 2010.

[19] LOMBARDO P, SAELI S, BISIO F, *et al*. Fast flux service network detection via data mining on passive DNS traffic[C]. The 21st International Conference on Information Security, Guildford, UK, 2018: 463–480. doi: 10.1007/978-3-319-99136-8_25.

[20] CHAHAL P S and KHURANA S S. TempR: Application of stricture dependent intelligent classifier for fast flux domain detection[J]. *International Journal of Computer Network and Information Security*, 2016, 8(10): 37–44. doi: 10.5815/ijcnis.2016.10.05.

牛伟纳：女，1990年生，博士，讲师，研究方向为网络安全、软件安全、AI在网络安全安全中的应用.

蒋天宇：男，1995年生，硕士生，研究方向为网络安全、网络攻击检测.

张小松：男，1968年生，博士，教授，研究方向为大数据应用及安全、人工智能的应用与安全、移动计算安全、网络攻击的追踪溯源.

谢 娇：女，1996年生，硕士生，研究方向为网络安全、网络攻击检测.

赵振扉：男，1991年生，硕士生，研究方向为网络安全、网络攻击检测.

责任编辑：余 蓉