Computer Science and Application 计算机科学与应用, 2022, 12(4), 1054-1060
Published Online April 2022 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2022.124108

Hans汉斯

基于时空残差网络的僵尸网络检测方法

陈飞健

广东工业大学，计算机学院，广东 广州

收稿日期：2022年3月16日；录用日期：2022年4月15日；发布日期：2022年4月22日

摘　要

僵尸网络是僵尸主机(botmaster)远程控制的受感染主机集群。传统的僵尸网络检测方法相对简单，主要来自网络数据包、结构等大量传入信息进行处理和预处理来实现的，可能存在较低的检测率，难以适应当前互联网的快速发展。针对僵尸网络检测问题，提出了一种基于时空残差特征的僵尸网络检测模型Res-1DCNN-LSTM。利用多层1DCNN和LSTM并行提取僵尸网络的空域和时序特征，然后在层与层之间引入捷径连接技术(shortcut connections)。实验结果表明，在公开数据集上，二分类和多分类的正确率可达98.89%和87.53%，在精度、召回率和F1值方面具有良好的性能。

关键词

僵尸网络检测，深度学习，时空特征

Botnet Detection Method Based on Spatial-Temporal Residual Network

Feijian Chen

School of Computer, Guangdong University of Technology, Guangzhou Guangdong

Received: Mar. 16th, 2022; accepted: Apr. 15th, 2022; published: Apr. 22nd, 2022

Abstract

Botnet is an infected host cluster remotely controlled by botmaster. The traditional botnet detection method is relatively simple, mainly from the processing and preprocessing of a large number of incoming information such as network packets and structures. It may have a low detection rate and is difficult to adapt to the rapid development of the current Internet. Aiming at the problem of botnet detection, a botnet detection model Res-1DCNN-LSTM based on Spatial-temporal residual features is proposed. Multi-layer 1DCNN and LSTM are used to extract the spatial and temporal characteristics of botnet in parallel, and then the shortcut connections are introduced between

文章引用: 陈飞健. 基于时空残差网络的僵尸网络检测方法[J]. 计算机科学与应用, 2022, 12(4): 1054-1060.
DOI: 10.12677/csa.2022.124108

layers. The experimental results show that the accuracy of binary and multi-classification can reach 98.89% and 87.53% on public datasets, and it has good performance in precision, recall and F1 value.

Keywords

Botnet Detection, Deep Learning, Spatial-Temporal Feature

1. 引言

随着 5G 技术、智能家居和其他移动设备的广泛应用，移动网络近年来已经成为电信的支柱。根据中国互联网络信息中心(CNNIC)统计，截至 2021 年 6 月，我国网民规模达 10.11 亿，较 2020 年 12 月增长 2175 万，互联网普及率达 71.6% [1]。物联网设备已被开发和应用于多个领域，包括智慧城市、智能电网、智能制造和维护、智能交通、安防和监控、精准农业、电力、水电等公用事业、供应链和库存优化等。但相对而言，网络上各种恶意行为层出不穷，网络安全正面临着越来越严重的威胁。基于 BaaS (僵尸网络即服务)的僵尸网络的规模也在逐渐增大，这种方式极大地提高了非分布式控制僵尸网络的难度[2]。全球范围内物联网的迅速增加为黑客利用僵尸网络来威胁网络安全和侵犯隐私提供了机会。

在攻击初期或攻击过程中，网络安全管理员通常将僵尸网络视为普通流量。因此，及时有效的检测僵尸网络具有重要的现实意义，是保障网络安全的重要手段之一。僵尸网络的检测技术主要有两种：误用检测和异常检测。很多研究人员对基于异常网络的恶意行为[3]进行了研究，主要是提取正常流量行为的特征，并建立特征数据库。所有与特征库不匹配的行为都被判定为恶意行为。这种方法的优点是可以检测到未知的恶意类型，但其误报率相对较高。误用检测也称为特征检测。对 API 误用检测和 API 使用模式挖掘的研究集中在减少大量误报，即源自代码元素随机共现的模式(例如，方法调用)。这些误报可能会在 API 误用检测期间导致误报，从而阻碍此类自动检测器的实际应用[4]。针对这两种检测方法的局限性，近年来人们提出了许多与机器学习相关的动态方法并且获得了较高的准确率。在僵尸网络隐蔽技术迅速发展的今天，这些基于机器学习的方法在寻找合适的特征来训练分类模型方面存在一些困难。特征的数量和质量与给定数据集的模型的准确性高度相关[5]。本文方法利用深度学习进行僵尸网络的检测和多分类任务，能够很好地在未知恶意行为的发现能力和误报率之间取得良好的权衡。由于每个网络流都具有一定的空间结构，不同的信息构成一个完整的网络行为是具有时间依赖性的。因此，本文方法使用深层一维卷积神经网络(One Dimensional Convolutional Neural Network, 1D-CNN) [6]和长短期记忆网络(Long-Short Term Memory, LSTM) [7]并行提取空域特征信息和时序特征信息，然后用残差网络(Residual Networks, ResNet)来解决网络退化问题[8]。残差网络的捷径连接技术(shortcut connections)将融合的时空特征跨层传递，综合判断网络流是否为僵尸网络并对网络流进行多分类，以供后期研究使用。

2. 相关工作

当前随着僵尸网络隐蔽技术的不断增强，基于规则的误用检测已经不再适用。僵尸网络的检测和分类的研究主要集中于机器学习和深度学习两个领域。在机器学习方面：Yan 等人[9]提出了一种基于人工神经网络的僵尸网络检测模型，在检测 DDoS 攻击时采用数据重采样的方法。Nanthiya 等人[10]通过主成

分分析(PCA)对 DDoS 攻击数据包进行降维，然后训练和测试支持向量机、决策树和随机森林等机器学习算法进行分类。Nguyen 等人[11]提出了一种使用协同过滤和基于密度的聚类来检测 DGA 僵尸网络的方法。该方法使用聚类和分类算法去除噪声，并根据域名特征分布的相似性对相似域进行分组。

由于机器学习需要人工提取特征，对于数据集的特征依赖性较强，近年来深度学习的僵尸网络检测分类方法得到了广泛应用。Yerima [12]等人提出了一种基于卷积神经网络(CNN)的 Android 僵尸网络检测深度学习方法，该模型在 342 个静态应用程序特征上提取空间信息进行训练，以区分僵尸网络应用程序和普通应用程序，得到了较高的检测精度。Biswas 等人[13]通过 GRU 和 LSTM 从常规流量中识别出恶意僵尸网络流量，在 Bot-IoT 数据集上取得了高分类精度。Alkahtani [14]等人提出了 CNN-LSTM 算法来检测物联网僵尸网络攻击，改模型有效提取了僵尸网络的时空特征，在 N-BaIoT 数据集上得到了比较高的检测率。当前基于深度学习的僵尸网络检测方法很少使用深层网络，导致提取的特征不够丰富多样，而且比较少同时进行检测和多分类任务。因此，本文提出了 Res-1DCNN-LSTM 模型从时序和空域两个维度提取僵尸网络特征，并且引入捷径连接技术逐层连接时空特征，进而得到跟深层次的特征表达。

3. 时空残差网络模型

本文提出的时空残差网络模型 Res-1DCNN-LSTM 由 1DCNN、LSTM 和 ResNet 残差连接组成。模型总体架构如下图 1 所示：

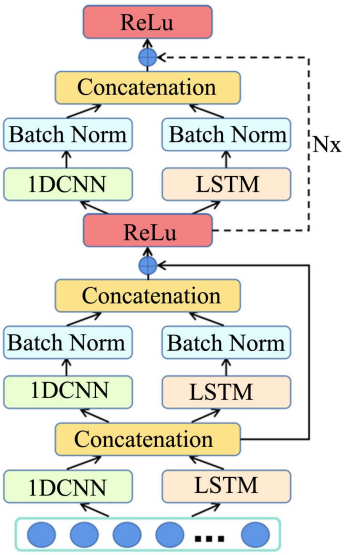

Figure 1. Overall architecture diagram of Res-1DCNN-LSTM
图 1. Res-1DCNN-LSTM

3.1. 一维卷积神经网络

由于网络流量是一组按网络层次组合的一维字节序列，因此选择一维卷积神经网络作为空间特征提取器比二维卷积神经网络更适合[15]。所设计的 1D-CNN (一维卷积神经网络)由输入层、一维卷积层、一维最大池化层和输出层构成。一维卷积的计算过程如下：

$$s_i = f\left(\omega_i \otimes s_{i-1} + b_i\right)$$

获得每个样本的一维卷积特征后，进行最大池化计算，其大小由核尺寸 k、步长 i 和填充大小 p 决定，计算过程如下所示：

$$s_i' = \max\{k, i, p, s_i\}$$

3.2. 长短期记忆网络

循环神经网络(RNN)算法通常用于处理具有时间特性的序列。然而在实际应用中RNN容易梯度消失。为了解决这一问题，LSTM 引入记忆单元来处理长短期时序特征。LSTM 由遗忘门、输入门和输出门构成，其计算过程如下所示：

$$\begin{aligned}
f_t &= \sigma\left(\omega_f\left[h_{t-1}, x_t\right] + b_f\right)\\
i_t &= \sigma\left(\omega_i\left[h_{t-1}, x_t\right] + b_i\right)\\
\tilde{C}_t &= \tanh\left(\omega_C\left[h_{t-1}, x_t\right] + b_C\right)\\
C_t &= f_t * C_{t-1} + i_t * \tilde{C}_t\\
o_t &= \sigma\left(\omega_o\left[h_{t-1}, x_t\right] + b_o\right)\\
h_t &= o_t * \tanh\left(C_t\right)
\end{aligned}$$

经过 1D-CNN 和 LSTM 提取的特征输入到批量归一化层(Batch Normalization)。训练网络模型的时候，Batch Normalization 保持每个 batch 的均值和方差不变。其中偏移和缩放为可学习参数，能够让网络权重保持规整，。在某种程度上加速网络训练收敛，提高模型泛化能力。Batch Normalization 的计算过程如下所示：

$$\begin{aligned}
\mu_B &= \frac{1}{|B|}\sum_{i\in B} x_i\\
\sigma_B^2 &= \frac{1}{|B|}\sum_{i\in B}\left(x_i - \mu_B\right)^2 + \varepsilon\\
x_{i+1} &= \gamma\frac{x_i - \mu_B}{\sigma_B} + \beta
\end{aligned}$$

每层网络计算完的 CNN 和 RNN 特征进行拼接，然后输入到 ReLU 非线性激活函数中。ReLU 的计算过程如下所示：

$$\mathrm{ReLU}(x) = \begin{cases} 0, & x \le 0 \\ x, & x > 0 \end{cases}$$

3.3. 残差网络

残差网络能够将神经网络变得更深而不会梯度消失，能够解决网络退化问题，在计算机视觉任务中取得了非常好的成绩，今年来也逐渐被应用与 NLP 任务中。多层 1D-CNN 和 LSTM 并行提取僵尸网络的空间和时间特征，融合成多层时序特征，同时在层与层之间引入残差网络的捷径连接(shortcut connections)，让网络变得更深，学习到更多深层特征。残差网络的计算过程如下所示：

$$f(x) = x + g(x)$$

本文所提出的 Res-1DCNN-LSTM 方法，包括两种残差网络块，记为 block1 和 block2。由于僵尸网络数据维度较小，在 block1 中，CNN 和 RNN 不改变输入维度，然后将两个特征向量进行拼接，进而扩大特征维度，并且能最大程度保留原始数据特征。对于 block2，CNN 和 RNN 不断深入学习特征，特征维度不断减小，而通道数不断增加。最终提取的时空特征输入到 softmax 层进行二分类和多分类。

4. 实验与分析

4.1. 实验环境

使用 pytorch1.8.0 作为深度学习实验框架。电脑配置：11th Gen Intel(R) Core(TM) i5-11400H @ 2.70GHz 处理器、16.0 GB 虚拟内存、Ubuntu16.04 操作系统和 NVIDIA GeForce RTX 3060Ti 显卡。

4.2. 数据集和评估指标

本文用基于物联网网络的僵尸网络数据集 N-BaIoT [16]。由 115 个特征的数据样本组成。数据集通过物联网设备的端口镜像收集。在设置网络确保数据为良性后，立即捕获良性数据。对于两种类型的包大小(只有出站/同时出站和入站)、包计数和包抖动，每个统计值提取包到达之间的时间。在 5 个时间窗口(100 ms、500 ms、1.5 s、10 s 和 1 min)中，每个时间窗口共提取了 23 个特征，共 115 个特征。我们使用了框架中的所有 115 个特性。本文按源数据集同比例取样 5%，得到 353,130 条数据集，合计 11 个类别，其中包括 10 个僵尸网络和一个正常流量。提取的数据集各个类别占比分布如下图 2 所示：

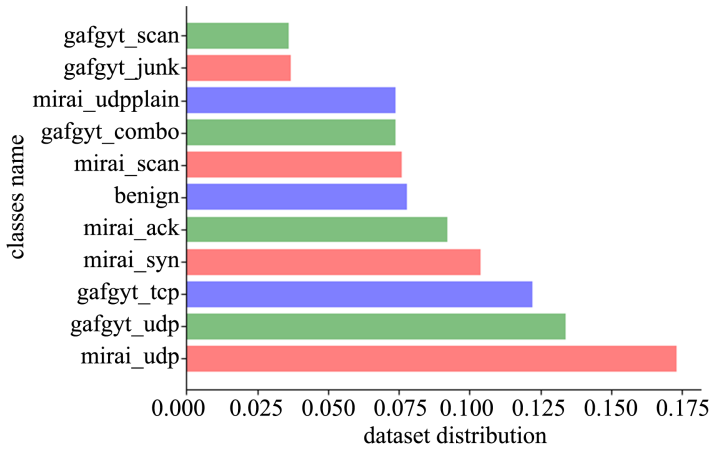

Figure 2. Dataset distribution of the proportion of each category
图 2. 数据集各类别占比分布

对于僵尸网络的检测和多分类任务，本文评估指标为准确率(ACC)和 F1 值。

4.3. 对比实验与结果分析

为了评估和检查所提出的基于时空残差网络的僵尸网络检测和分类性能，本人做了几组对比实验。模型学习率为 0.001，epoch 为 30，batchsize 为 512。训练和验证准确率和损失如下图 3 所示。

僵尸网络的危害性和快速变化性，导致其被检测的难度增加。因此设计准确率高，误报率低的检测算法至关重要。除此之外，僵尸网络的多分类任务能够区分出所有僵尸网络类别和正常网络流，识别出的多种僵尸网络类别可供后续研究它们之间的区别，追踪僵尸网络的变化。由于当前对 N-BaIoT 数据集的研究文献很少同时使用所有 11 个类别进行二分类和多分类。因此，本文设计两组分类任务，将将本文提出的 Res-1DCNN-LSTM 模型和其他模型进行对照实验，如表 1 所示。

有上图两组对比实验可知，本文方法 Res-1DCNN-LSTM 在多种模型中综合性能最强。在二分类任务中：除了 Dense，其他模型都获得了较高的准确率和 F1 值，其中本文方法和 CNN-LSTM 准确率最高。在多分类任务中：CNN-LSTM 的准确率好于单独使用 CNN 和 RNN 模型，本文方法取得了最高 F1 值，可见深层的神经网络可以学习到更多的特征来学习多种类别。

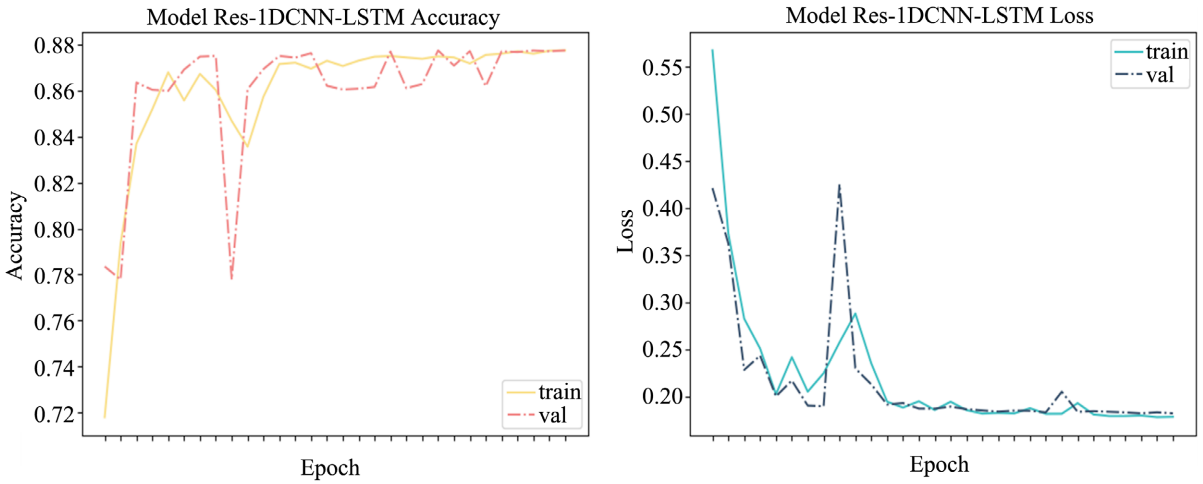

Figure 3. Accuracy and loss
图 3. 准确率和损失

Table 1. Experimental results of different models
表 1. 不同模型实验结果

模型	二分类		多分类	
	Accuracy (%)	F1 (%)	Accuracy (%)	F1 (%)
Dense	96.32	95.76	82.45	79.89
GRU	98.57	98.34	85.56	84.94
1DCNN	98.62	98.24	85.73	84.38
CNN-LSTM	98.91	98.71	86.98	87.23
本文方法	98.89	99.32	87.53	88.56

5. 总结

本文提出一种新的僵尸网络检测方法，针对于僵尸网络存在空间和时间二维特征，使用CNN和LSTM提取时空特征。然后在深层次的时空特征之间引入残差网络的残差连接来综合检测网络流和僵尸网络，以供后期研究使用。该模型在在二分类任务中表现出色，准确率和F1均达到了98%以上，在多分类任务中F1值最高，可见Res-1DCNN-LSTM能够为每个类别提取出足够多准确的特征向量。在后续的研究中，本人将研究Bert模型对于僵尸网络检测的有效性并且深入理解僵尸网络的传播原理。

参考文献

[1] 张保淑. 中国网民规模超 10 亿[N]. 人民日报海外版, 2021-08-28(002). https://doi.org/10.28656/n.cnki.nrmrh.2021.002645

[2] Alieyan, K., Almomani, A., Manasrah, A. and Kadhum, M.M. (2017) A Survey of Botnet Detection Based on DNS. *Neural Computing and Applications*, **28**, 1541-1558. https://doi.org/10.1007/s00521-015-2128-0

[3] Oza, A., Ross, K., Low, R.M. and Stamp, M. (2014) HTTP Attack Detection Using *N*-Gram Analysis. *Computers & Security*, **45**, 242-254. https://doi.org/10.1016/j.cose.2014.06.002

[4] Nielebock, S., Heumüller, R., Schott, K.M. and Ortmeier, F. (2021) Guided Pattern Mining for API Misuse Detection by Change-Based Code Analysis. *Automated Software Engineering*, **28**, Article No. 15. https://doi.org/10.1007/s10515-021-00294-x

[5] Shi, W.C. and Sun, H.M. (2020) DeepBot: A Time-Based BotNet Detection with Deep Learning. *Soft Computing*, **24**, 16605-16616. https://doi.org/10.1007/s00500-020-04963-z

[6] Lecun, Y., Bottou, L., Bengio, Y. and Haffner, P. (1998) Gradient-Based Learning Applied to Document Recognition. *Proceedings of the IEEE*, **86**, 2278-2324. https://doi.org/10.1109/5.726791

[7] Hochreiter, S. and Schmidhuber, J. (1997) Long Short-Term Memory. *Neural Computation*, **9**, 1735-1780. https://doi.org/10.1162/neco.1997.9.8.1735

[8] He, K., Zhang, X., Ren, S. and Sun, J. (2016) Deep Residual Learning for Image Recognition. 2016 *IEEE Conference on Computer Vision and Pattern Recognition* (*CVPR*), Las Vegas, 27-30 June 2016, 770-778. https://doi.org/10.1109/CVPR.2016.90

[9] Soe, Y.N., Santosa, P.I. and Hartanto, R. (2019) DDoS Attack Detection Based on Simple ANN with SMOTE for IoT Environment. 2019 4*th International Conference on Informatics and Computing* (*ICIC*), Semarang, 16-17 October 2019, 1-5. https://doi.org/10.1109/ICIC47613.2019.8985853

[10] Nanthiya, D., Keerthika, P., Gopal, S.B., Kayalvizhi, S.B., Raja, T. and Priya, R.S. (2021) SVM Based DDoS Attack Detection in IoT Using Iot-23 BotNet Dataset. 2021 *Innovations in Power and Advanced Computing Technologies* (*i-PACT*), Kuala Lumpur, 27-29 November 2021, 1-7. https://doi.org/10.1109/i-PACT52855.2021.9696569

[11] Nguyen, T.D., Cao, T.D. and Nguyen, L.G. (2015) DGA Botnet Detection Using Collaborative Filtering and Density-Based Clustering. *Proceedings of the* 6*th International Symposium on Information and Communication Technology*, Hue City, December 2015, 203-209. https://doi.org/10.1145/2833258.2833310

[12] Yerima, S.Y. and Alzaylaee, M.K. (2020) Mobile Botnet Detection: A Deep Learning Approach Using Convolutional Neural Networks. 2020 *International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (*CyberSA*), Dublin, 15-19 June 2020, 1-8. https://doi.org/10.1109/CyberSA49311.2020.9139664

[13] Biswas, R. and Roy, S. (2021) Botnet Traffic Identification Using Neural Networks. *Multimedia Tools and Applications*, **80**, 24147-24171. https://doi.org/10.1007/s11042-021-10765-8

[14] Alkahtani, H. and Aldhyani, T.H.H. (2021) Botnet Attack Detection by Using CNN-LSTM Model for Internet of Things Applications. *Security and Communication Networks*, **2021**, Article ID: 3806459. https://doi.org/10.1155/2021/3806459

[15] Li, C., Zhang, Y., Wang, W., Liao, Z. and Feng, F. (2022) Botnet Detection with Deep Neural Networks Using Feature Fusion. 2022 *International Seminar on Computer Science and Engineering Technology* (*SCSET*), Indianapolis, 8-9 January 2022, 255-258. https://doi.org/10.1109/SCSET55041.2022.00066

[16] Meidan, Y., Bohadana, M., Mathov, Y., *et al*. (2018) N-baiot—Network-Based Detection of Iot Botnet Attacks Using Deep Autoencoders. *IEEE Pervasive Computing*, **17**, 12-22.