融合字符级滑动窗口和深度残差网络的僵尸网络DGA域名检测方法

刘小洋[1],刘加苗[1],刘 超[1],张宜浩[2]
(1. 重庆理工大学计算机科学与工程学院,重庆 400054; 2. 重庆理工大学人工智能学院,重庆 401135)

摘 要: 本文提出了一种基于字符级滑动窗口的深度残差网络(Sliding Window-Depth Residual Network,SW-DRN),首次将轻量级深度可分离式卷积应用于僵尸网络中DGA(Domain Generation Algorithm)域名检测. SW-DRN采用深度可分离式卷积,相比标准卷积减少了约56%的参数,增强了模型检测效率. 采集两种不同来源的数据,分别命名为Real-Dataset和Gen-Dataset. SW-DRN与对照组模型在两个数据集上进行实验,实验结果表明:SW-DRN模型在DGA域名二分类任务中的F-Score评估指标上分别取得了99.23%和97.81%的成绩;并且在少样本DGA域名家族以及域名字符串易混淆DGA域名情形下多分类任务中取得不错的成绩,相比目前已有的DGA域名分类模型在总体F-Score上提升了1.23%和1.01%的性能,增强了DGA域名家族之间的识别;同时还对所提出的模型在生成对抗模型产生域名进行测试,均能得到有效的识别.

关键词: 域名生成算法; 字符级向量; 残差网络; 深度可分离式卷积
中图分类号: TN915 **文献标识码:** A **文章编号:** 0372-2112(2022)01-0250-07
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20200619

Novel Botnet DGA Domain Detection Method Based on Character Level Sliding Window and Deep Residual Network

LIU Xiao-yang[1], LIU Jia-miao[1], LIU Chao[1], ZHANG Yi-hao[2]
(1. *School of Computer Science and Engineering, Chongqing University of Technology, Chongqing* 400054, *China*;
2. *School of Artificial Intelligence, Chongqing University of Technology, Chongqing* 401135, *China*)

Abstract: This paper proposed a character-level sliding window based deep residual network model SW-DRN (Sliding Window-Depth Residual Network), which was the first to apply light depthwise separable convolution to the DGA(Domain Generation Algorithm) domain name detection. In SW-DRN, the use of depthwise separable convolution reduced the number of model parameters by about 56% compared with standard convolution, which enhanced the efficiency of model detection. Collect data from two different sources, named Real-Dataset and Gen-Dataset. Finally, comparison experiments on the dataset with the proposed DGA domain name detection model by previous researchers. Experimental results on two datasets show that the proposed SW-DRN model has achieved good results of 99.23% and 97.81% on the F-Score evaluation indicator in the DGA domain name binary classification task. Compared with the existing DGA domain name classification model, the SW-DRN has made a 1.23% and 1.01% performance improvement on the F-Score, enhancing the DGA domain name family recognition. At the same time, the proposed model tests in the generative adversarial networks to generate domain names, and it can be effectively identified.

Key words: domain generation algorithm; character-level vector; residual network; depthwise separable convolution

1 前言

僵尸网络是指采用一种或多种传播手段,将大量主机感染bot程序病毒,从而使控制者和被感染主机之间形成一个可以一对多控制的网络. Internet用户的增多以及用户安全意识的缺乏,是导致僵尸网络产生的主要原因之一. 组建僵尸网络的僵尸程序被事先设计

收稿日期:2020-06-28;修回日期:2021-02-20;责任编辑:孙瑶
基金项目:国家社会科学基金(No.17XXW004)

好了DGA算法,利用该算法生成大量的DGA域名并周期性产生一个域名列表. 僵尸网络的控制者会注册某些域名作为该僵尸网络的命令控制服务器访问域名. 通过不断更改僵尸网络控制服务器的域名使僵尸网络保持运行的技术被称为domain flux[1]. 早期的DGA域名检测方式是黑名单、正则匹配等. 后来随着机器学习的兴起,利用大量的域名数据并做特征工程的域名检测的性能逐步提高. 随后基于深度学习自动特征提取的DGA域名检测方法也逐步得到发展.

本文的主要创新点:①提出了一种基于字符级滑动窗口的深度残差网络模型用于DGA域名的检测,使用区域卷积方式扩大卷积核感受野,然后精巧地设计了一种可变长式的深度可分离式卷积残差神经网络来提取特征;②提出的SW-DRN模型首次采用深度可分离式卷积设计,减少了模型的可训练参数以及训练成本,提升了模型的检测效率;③本文建立两个数据集,分别为Real-Dataset和Gen-Dataset,并且这两个数据集上的二分类和多分类任务均到达了目前领先的水平.

2　相关工作

在僵尸网络的防御中,DGA域名检测起着重要的作用. 因此DGA域名检测成为网络安全领域中一个非常重要的研究点. 在2010年,Yadav等人[2]同时对DGA域名和非DGA域名集合1-gram与2-gram的分布提取特征进行了识别. Antonakakis等人[3]基于隐马尔科夫聚类发现了潜在的DGA域名家族. 在2016年,Woodbridge等人[4]首次将深度学习应用到DGA域名检测中,且该方法只使用域名字符串作为数据输入,利用深度学习自动提取字符串内的隐藏特征,使DGA域名检测的研究工作取得了飞跃性的突破. Vinayakumar等人[5]在不同深度学习框架上进行DGA域名检测实验,比较了多种卷积神经网络与循环神经网络. 吕品等人[6]使用双向多层的循环神经网络结构,对大规模DGA数据进行训练,最终得到的模型的DGA域名检测率为96%. Tran等人[7]提出了一种LSTM. MI算法,该算法结合了二分类和多类分类模型,并考虑了类别识别的重要性. Highnam等人[8]提出了一种新颖的混合神经网络,该模型对此类算法生成域的可能性进行了分析和评分. 杜鹏等人[9]提出一种混合词向量的DGA域名检测模型,并使用混合词向量CNN-LSTM和CNN-MWE模型做了实验对比. 从上述研究发现,基于深度学习的方法普遍优于基于人工特征的机器学习方法. 但是基于深度学习的DGA域名检测方法在DGA域名家族的二分和多分类任务上仍有很大的提升空间.

3　所提出的方法

本文提出的基于字符级滑动窗口的深度残差网络结构如图1所示. SW-DRN输入层接受固定长度为L的域名,且$L=48$. 对域名进行数值化处理,使用字符级词典把域名中的每个字符映射成one-hot编码向量. 嵌入层将one-hot的V_1维度向量映射成d维度,$d=16$. 于是开始特征提取,区域卷积部分采用标准卷积进行原始特征提取,采用多尺度的滑动窗口,选用3种一维卷积核,大小分别为1,3,5. 然后输入到深度可分离式卷积残差网络层进行更深层次的特征提取.

残差网络层的层数是可以根据图1中的深度可分离式卷积重复模块进行变化的,它的重复次数使用N来表示. 卷积重复模块的次数$N=4$,当N的值每增加1时,下一次卷积的滤波器数量n变为原来的2倍,于是滤波器的数量分别为64,128,256,512. 同时在深度可分离式卷积重复模块的尾部加上一个最大池化层,这

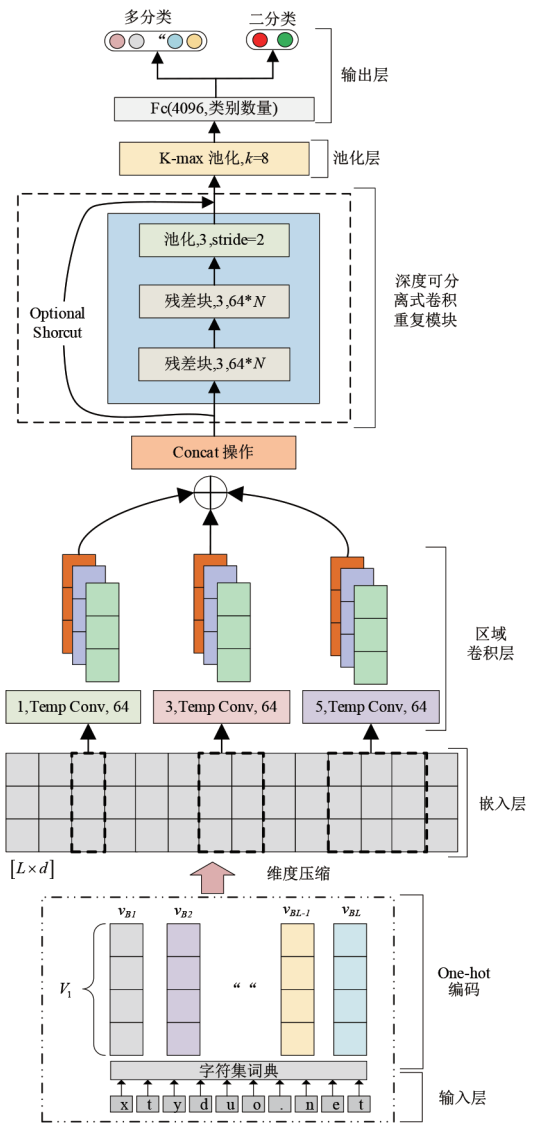

图1　SW-DRN模型架构

样每经过一个卷积重复模块时，特征图的长度变为原来的一半，其目的是在残差网络层中卷积核长度不变的情况下，通过减少长度L来增加对特征图的感受视野，这样可以提取DGA域名内不同位置字符之间的关系特征. 最后，需要对得到的特征图进行K-max池化采样，感受野$k=8$，目的是提取显著的特征，缓解模型的过拟合，增加模型的泛化能力. 输出层按照任务类型对输入的DGA样本进行类别预测.

残差网络[10]的设计是为了防止当网络层数加深时，模型在训练中出现梯度爆炸和梯度消失. 考虑到残差块中若使用标准卷积会导致模型计算量增加并降低模型的检测效率，于是在DGA域名检测中本文在设计残差块时首次应用深度可分离式卷积[11]. 图2为SW-DRN中残差块的内部结构. 为了增加模型训练的稳定性，引入批标准化(Batch Norm). 残差块的数据流方向如式(1)所示：

$$x_l = x'_{l-1} + H(x_{l-1}) \tag{1}$$

其中，x_{l-1}为残差块的输入；x_l为残差块输出.

本文为了探索网络模型的深度对DGA域名检测的影响，使用SW-DRN模型分别在深度层数为9，17，29，49的情况下进行相应的训练并测试，所得对比结果在实验部分展示.

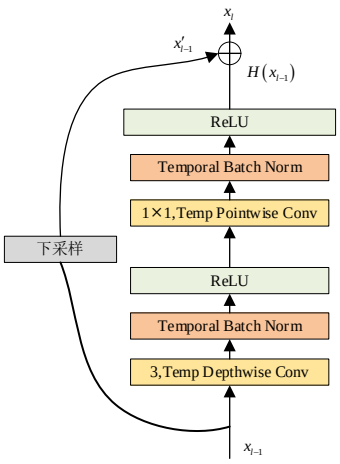

图2 深度可分离式卷积残差块

4 实验与结果分析

4.1 实验超参数

SW-DRN模型的超参数：初始化学习率为0.01；每32 Epoch的学习率调整成原来的1/2；优化器为Adam；Epoch为128；B(Batch size)=512.

4.2 Real-Dataset 和 Gen-Dataset

Real-Dataset数据集由2部分组成：一部分是合法的域名样本，来自Alexa访问量全球排名前一百万的网站域名；另一部分用360 Netlab DGA公开数据. Real-Dataset数据集包含21种DGA家族数据集，同时为了减缓数据不平衡问题，本文对该数据集进行欠采样.

本文不仅收集真实网络环境下的DGA域名样本，同时还用域名生成算法产生DGA域名样本并和Alexa中的域名一起作为合法域名构成数据集Gen-Dataset. 本文从Internet中收集了主流的域名生成算法，然后根据不同域名的生成算法，按满足条件不同，生成了33种不同家族的DGA域名，且每个类数量均为20 000.

4.3 模型性能衡量指标

SW-DRN模型具有二分类和多分类的任务. 表1是分类混淆矩阵.

表1 分类结果混淆矩阵

实际类	预测类	
	DGA域名	合法域名
DGA域名	TP	FN
合法域名	FP	TN

准确率：

$$\mathrm{Acc} = \frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN}} \tag{2}$$

查准率：

$$\mathrm{precision} = \frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FP}} \tag{3}$$

检测率(Detection Rate，DR)：

$$\mathrm{DR} = \frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \tag{4}$$

误报率(False Positive Rate，FPR)：

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}} \tag{5}$$

$$\mathrm{F\text{-}score} = \frac{2\cdot\mathrm{precision}\cdot\mathrm{recall}}{\mathrm{precision}+\mathrm{recall}} \tag{6}$$

考虑到实验中Real-Dataset存在数据不平衡的问题，因此采用“macro”方式计算F-score比较合适.

4.4 模型对比实验分析

在Real-Dataset数据集和Gen-Dataset数据集上进行的二分类和多分类的实验，采用的对比实验模型分别是LSTM[12]、GRU[13]、Shallow-CNN[13]、CNN-LSTM[14]和LSTM-Attention[15].

在Real-Dataset数据集上的二分类结果如表2所示. 从表2中可知，本文所提出的SW-DRN模型和对比模型在5个评估指标上都取得了不错的成绩，说明深度学习模型在DGA域名检测中具有非常不错的性能. 由于Real-Dataset数据集中DGA合法域名的特征相对容易区分，且各个性能指标几乎都超过99%，SW-DRN与其他模型对比，在二分类任务上取得了微弱的领先. 表3展示了各个模型在Gen-Dataset数据集上的评估结果. SW-DRN模型在5个性能指标上都领先于对比模

型. 但SW-DRN模型在Gen-Dataset数据集上并没有达到Real-Dataset数据集上一样的识别率,主要原因是Gen-Dataset数据集中的DGA家族数量更多,增加了识别的难度.

表2 Real-Dataset数据集二分类结果/%

模型名	Acc	precision	recall	F-score
LSTM	99. 14	99. 14	99. 12	99. 13
GRU	98. 82	98. 80	98. 81	98. 80
CNN-LSTM	99. 09	99. 08	99. 07	99. 07
Shallow-CNN	98. 66	98. 66	98. 62	98. 64
LSTM- Attention	99. 15	99. 14	99. 14	99. 14
SW-DRN	99. 24	99. 25	99. 21	99. 23

模型在Real-Dataset数据集上的多分类实验结果如表4所示. 根据实验结果可以发现,SW-DRN模型在多分类整体评估指标F - score上,比最优对照模型高出了1. 23%. 且SW-DRN在gameover和virut等5个家族上的误报率均为0,在多个DGA家族上取得了领先的成绩,即使在一些DGA家族上未能超越对比模型,但也紧随其后. 同样从表5中的数据不难发现,SW-DRN模型比对照模型在整体多分类指标上F-score提升了1. 01%,且在多个DGA域名家族上领先于其他模型. 但同上述SW-DRN模型在Real-Dataset数据集上的测试结果相比,Gen-Dataset数据集中的DGA域名家族种类更多,对各个家族的识别难度也越大. 还发现,在dircrypt、pros-likefan和dnschanger等一些家族上,其域名之间具有高较高相似性,使得识别率低于其他家族.

表3 Gen-Dataset数据集二分类结果对比/%

模型名	Acc	precision	recall	F-score
LSTM	97. 35	97. 36	97. 36	97. 35
GRU	96. 14	96. 19	96. 17	96. 14
CNN-LSTM	97. 21	97. 21	97. 22	97. 21
Shallow-CNN	96. 92	96. 93	96. 93	96. 92
LSTM- Attention	92. 42	92. 45	92. 44	92. 42
SW-DRN	97. 81	97. 81	97. 82	97. 81

表4 Real-Dataset 多分类结果/%

模型名	LSTM			GRU			LSTM-Attention			Shallow-CNN			CNN-LSTM			SW-DRN		
类别	DR	FPR	F-score	DR	FPR	F-score	DR	FPR	F-score	DR	FPR	F-score	DR	FPR	F-score	DR	FPR	F-score
banjori	100	0. 01	99. 95	99. 6	0. 078	99. 43	100	0. 013	99. 94	99. 98	0. 029	99. 85	100	0. 018	99. 91	100	0. 016	99. 93
emotet	100	0. 034	99. 84	99. 88	0. 029	99. 8	100	0. 031	99. 85	100	0. 026	99. 88	100	0. 029	99. 86	99. 98	0. 026	99. 86
rovnix	99. 8	0. 037	99. 73	97. 98	0. 243	97. 83	99. 68	0. 021	99. 74	99. 82	0. 013	99. 85	99. 7	0. 039	99. 66	99. 8	0. 013	99. 84
tinba	96. 82	0. 51	96. 01	90. 62	0. 899	90. 98	97. 35	0. 478	96. 42	99. 78	0. 708	96. 61	99. 65	0. 661	96. 76	98. 88	0. 541	96. 91
pykspa_v1	99. 98	0. 01	99. 94	98. 98	0. 136	98. 84	99. 95	0. 029	99. 84	99. 88	0. 039	99. 75	99. 92	0. 013	99. 9	99. 88	0. 01	99. 89
simda	99. 18	0. 01	99. 54	99. 65	0. 091	99. 39	100	0. 031	99. 85	99. 95	0. 037	99. 8	99. 95	0. 034	99. 81	99. 98	0. 031	99. 84
ramnit	90. 96	1. 275	89. 43	79. 67	2. 29	78. 87	90. 14	1. 098	89. 75	91. 09	1. 025	90. 59	90. 96	1. 015	90. 57	93. 17	1. 119	91. 3
gameover	99. 71	0. 003	99. 83	98. 54	0. 025	99. 06	99. 67	0. 018	99. 69	99. 71	0. 003	99. 83	99. 75	0. 03	99. 63	99. 71	0	99. 85
ranbyus	90. 97	0. 276	92. 68	88. 23	0. 547	88. 77	91. 79	0. 314	92. 79	92. 56	0. 301	93. 32	92. 17	0. 177	94. 25	92. 36	0. 124	94. 85
virut	100	0	100	100	0	100	99. 9	0. 005	99. 9	100	0	100	100	0	100	100	0	100
murofet	86. 62	0. 387	88. 48	80. 08	0. 833	80. 15	91. 82	0. 528	89. 88	90. 77	0. 427	90. 38	90. 48	0. 439	90. 08	91	0. 385	90. 95
necurs	87. 95	0. 423	88. 53	70. 39	1. 075	71. 22	86. 95	0. 317	89. 17	84. 13	0. 408	86. 51	88. 32	0. 325	89. 86	88. 57	0. 145	92. 14
shiotob	96. 61	0. 076	97. 31	78. 78	0. 816	78. 93	97. 55	0. 052	98. 11	94. 85	0. 14	95. 6	95. 29	0. 12	96. 08	96. 42	0. 054	97. 49
symmi	100	0. 002	99. 94	99. 76	0. 012	99. 59	100	0	100	100	0	100	100	0	100	100	0	100
shifu	99. 02	0. 081	96. 27	94. 69	0. 024	96. 3	98. 23	0. 01	98. 71	98. 62	0. 007	99. 01	98. 43	0. 01	98. 81	98. 82	0. 007	99. 11
suppobox	99. 53	0. 045	97. 56	94. 55	0. 081	93. 33	100	0. 012	99. 41	98. 82	0. 048	97. 09	99. 29	0. 029	98. 24	100	0. 014	99. 29
qadars	98. 75	0. 021	98. 26	79. 25	0. 232	77. 89	99. 5	0. 002	99. 62	89. 5	0. 043	92. 27	96	0. 053	95. 29	99. 75	0	99. 87
locky	54. 98	0. 207	57. 08	25. 11	0. 407	25. 22	56. 28	0. 169	60. 19	29. 87	0. 088	40. 95	39. 39	0. 086	50. 84	58. 87	0. 09	67. 16
chinad	98. 5	0. 002	98. 99	83. 5	0. 031	87. 89	98	0. 002	98. 74	98. 5	0. 005	98. 75	97. 5	0. 002	98. 48	99	0. 007	98. 75
cryptolocker	40. 5	0. 204	44. 14	23	0. 349	23. 41	48	0. 147	53. 63	43	0. 107	51. 96	52. 5	0. 088	61. 4	60. 5	0. 145	63. 35
dyre	100	0. 002	99. 75	99. 5	0. 005	99. 25	100	0. 005	99. 5	100	0. 002	99. 75	100	0	100	100	0	100
macro	92. 38	-	92. 53	84. 85	-	85. 05	93. 09	-	93. 55	90. 99	-	91. 98	92. 34	-	93. 3	94. 13	-	94. 78

为更进一步证明SW-DRN的性能,针对当前生成对抗网络产生的DGA域名来测试基于深度学习的DGA域名检测器. 本文选择3个有关对抗样本的域名生成模型,分别为DeepDGA[16]、MaskDGA[17]和CharBot[18]. 表6是SW-DRN分别在这3种生成域名的测试集上的结果. SW-DRN在DeepDGA、MaskDGA和CharBot这3种生成域名的识别上均取得了不错的效果,但由于CharBot是直接对合法域名字符的个别位置上的字符随机替换,

表5 Gen-Dataset多分类结果/%

模型名	LSTM			GRU			LSTM-Attention			Shallow-CNN			CNN-LSTM			SW-DRN		
类别	DR	FPR	F-score	DR	FPR	F-score	DR	FPR	F-score	DR	FPR	F-score	DR	FPR	F-score	DR	FPR	F-score
pitou	100	0.007	99.9	99.93	0.006	99.88	99.98	0.023	99.67	100	0.004	99.94	99.68	0.013	99.65	100	0.005	99.93
zloader	99.55	0.153	97.67	100	0.159	97.81	100	0.156	97.85	100	0.156	97.85	99.82	0.156	97.76	100	0.154	97.88
locky	79.7	0.986	76.83	72.55	0.549	77.17	70.48	0.397	77.59	66.8	0.703	71.6	71.8	0.502	77.23	76.85	0.508	80.41
newgoz	99.98	0.001	99.97	99.95	0	99.97	99.98	0	99.99	99.95	0	99.97	99.92	0.003	99.92	99.98	0	99.99
dircrypt	69.45	0.839	71.94	69.58	0.973	70.63	76.18	1.064	73.9	73.88	1.349	69.73	72.1	0.885	73.19	74.82	0.846	75.33
padcrypt	100	0.002	99.98	99.92	0.006	99.88	99.95	0	99.97	100	0.004	99.94	99.95	0.009	99.85	100	0.001	99.99
symmi	99.98	0	99.99	100	0.004	99.94	99.92	0	99.96	100	0	100	100	0.004	99.95	100	0	100
murofet	99.98	0	99.99	100	0	100	100	0	100	100	0	100	99.95	0.001	99.96	100	0	100
proslikefan	61.4	0.768	67.09	55.82	1.01	60.59	62.6	0.673	68.95	51.62	0.721	60.05	60.85	0.662	67.8	66.62	0.821	70.22
reconyc	95.7	0.068	96.85	93.6	0.001	96.68	96.05	0.05	97.29	94.7	0.038	96.74	95.08	0.039	96.93	95.52	0.032	97.26
ranbyus	96.48	0.241	94.92	98.68	0.268	95.7	98.3	0.235	95.94	98.1	0.265	95.44	98.68	0.287	95.45	99.98	0.257	96.49
dnschanger	52.42	2.223	48.76	68.25	2.834	55.02	34.98	1.571	39.03	48.15	2.004	47.07	53.42	2.213	49.52	40.72	1.681	43.3
shiotob	92.88	0.132	94.48	92.42	0.043	95.46	92.35	0.018	95.77	92.7	0.06	95.37	92.55	0.116	94.52	92.3	0.022	95.68
fobber	46.78	1.979	46.19	33.15	1.372	38.59	65.4	2.604	54.78	53.52	2.265	49.25	46.45	2.005	45.77	59.05	2.513	51.38
qadars	99.98	0.004	99.93	99.45	0	99.72	99.72	0	99.86	99.58	0.021	99.49	98.22	0.003	99.07	100	0.003	99.96
ramdo	100	0	100	100	0.002	99.98	100	0	100	100	0.002	99.98	100	0.002	99.98	100	0	100
corebot	100	0.001	99.99	99.88	0	99.94	100	0.002	99.98	100	0	100	99.98	0.001	99.97	100	0	100
qakbot	58.25	0.453	68.13	61.8	0.718	67.9	65.8	0.639	71.6	57.12	0.385	68.02	59.12	0.462	68.69	62.85	0.443	71.7
nymaim	85.88	1.495	75.33	53	2.241	49.05	78.62	1.288	73.17	47.18	2.465	43.55	84.12	1.664	72.84	90.62	1.543	77.42
necurs	81.75	0.211	87.11	79.25	0.029	88.02	80.85	0.055	88.65	70.25	0.288	78.77	79.18	0.203	85.64	81.05	0.02	89.26
simda	100	0	100	100	0	100	100	0	100	100	0	100	100	0	100	100	0	100
suppobox	95.38	0.322	93.3	97.55	1.213	84.19	90.92	0.07	94.27	85.75	0.303	88.28	92.7	0.503	89.62	92.55	0.041	95.56
pykspa	72.15	1.414	68.07	76.25	2.155	64.35	84.58	2.405	67.04	68.42	2.36	58.25	80.22	1.823	69.29	79.1	1.49	71.56
mydoom	100	0.004	99.94	100	0.025	99.65	99.85	0.004	99.86	100	0.006	99.91	99.78	0.028	99.5	100	0.001	99.99
vawtrak	99.95	0.006	99.89	100	0.036	99.48	99.97	0.004	99.92	100	0.028	99.6	99.72	0.027	99.48	100	0.003	99.96
nymaim2	98.03	0.038	98.45	95.22	0.041	96.96	97.64	0.02	98.51	95.56	0.124	95.95	95.98	0.095	96.58	98.78	0.024	99.04
pizd	89.38	0.161	91.69	65.36	0.116	77.18	98.81	0.326	94.06	93.16	0.528	88.12	85.44	0.258	87.91	99.02	0.265	95.13
banjori	100	0	100	100	0	100	100	0	100	100	0	100	100	0	100	100	0	100
tinba	98.5	0.337	92.36	96.35	0.399	90.12	97.19	0.332	91.8	96.93	0.436	89.73	97.66	0.41	90.57	97.85	0.186	95
tempedreve	72.92	0.428	72.19	64.87	0.429	66.87	60.38	0.216	68.99	71.85	0.702	65.45	69.49	0.383	71.06	73.68	0.371	74.08
kraken	50.71	0.225	59.94	49.71	0.145	61.51	46.21	0.058	61.21	49.21	0.153	60.84	50.21	0.16	61.45	49.79	0.118	62.43
monerodownloader	100	0	100	100	0	100	100	0	100	100	0	100	100	0.001	99.9	100	0	100
chinad	99.67	0.001	99.67	99.67	0.001	99.67	97.07	0.001	98.35	99.35	0.001	99.51	98.05	0.002	98.69	99.67	0.001	99.67
macro	87.78	-	87.89	85.52	-	85.81	87.69	-	88.04	85.26	-	85.4	87.27	-	87.5	88.81	-	89.05

因此评估指标相比其他2种域名稍差一些.

表6 SW-DRN模型在生成域名上测试结果/%

模型名	Acc	precision	recall	F-score
DeepDGA	99.97	99.97	99.98	99.97
CharBot	96.86	96.88	96.87	96.87
MaskDGA	98.19	97.51	98.50	97.98

4.5 模型的参数量

为了评估模型的参数量,选择参数量在9层的SW-DRN模型进行实验. 实验结果如表7所示,SW-DRN模型使用深度可分离式卷积比标准卷积减少了约56%的参数.

表7 SW-DRN可训练参数量对比/百万

模型名	SW-DRN（标准卷积）	SW-DRN（深度可分离式卷积）
参数量	1.85	0.81

4.6 模型深度的探索

本文把SW-DRN模型的层数设定为9,17,29,49,

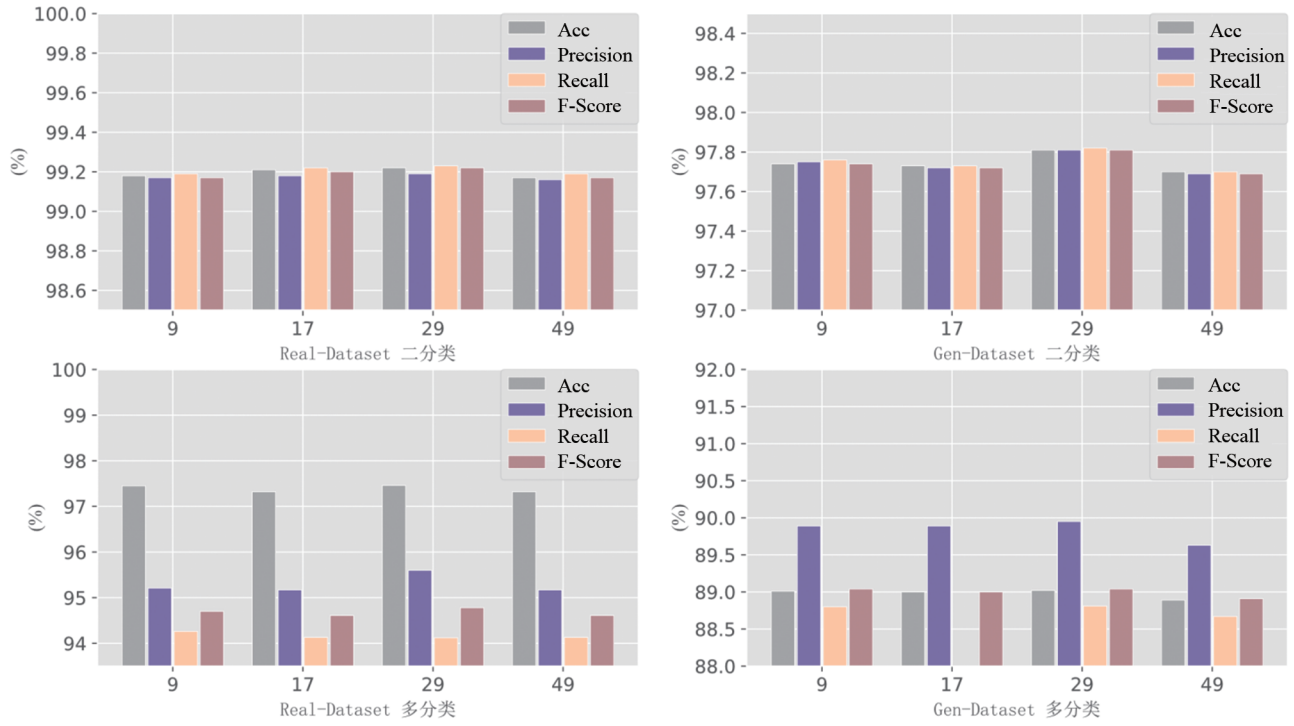

图3　SW-DRN的不同深度性能

并在Real-Dataset数据集和Gen-Dataset数据集上分别进行二分类和多分类实验,结果如图3所示. 当SW-DRN模型为9层时,已经取得了不错的性能,且随着模型的层数逐渐加深,模型的性能并无明显提升. 当模型为49层时,模型因拟合能力太强而出现过拟合现象,导致泛化能力下降. 对SW-DRN模型进行更深层数的探索,得到更深层次的网络模型,并不能更好地提升模型在DGA域名上的检测性能.

5　结束语

本文提出了一种基于字符级滑动窗口的深度残差神经网络模型. 实验证明,SW-DRN模型不仅在二分类任务上优于对比模型,而且在多分类任务中取得了当前最优异的成绩. 针对少样本DGA域名家族进行识别以及对高随机性、易混淆的DGA域名之间进行识别,相比当前已有的DGA域名分类模型,SW-DRN模型取得了更进一步的提升. 本文还对SW-DRN模型进一步实验,通过可变长的深度可分离式卷积残差模块实现对SW-DRN不同深度的探索,同时还对模型的检测效率进行了对比,实验证明,深度可分离式卷积能够有效地降低模型的可训练参数量.

参考文献

[1] ANTONAKAKIS M, PERDISCI R, LEE W, et al. Detecting malware domains at the upper dns hierarchy. USENIX security symposium[C]//Proceedings of the 20th USENIX conference on Security. San Francisco, USA: ACM, 2011: 1-16.

[2] YADAV S, REDDY A K K, REDDY A L N, et al. Detecting algorithmically generated domain-flux attacks with DNS traffic analysis[J]. IEEE/ACM Transactions on Networking, 2012, 20(5): 1663-1677.

[3] ANTONAKAKIS M, PERDISCI R, NADJI Y, et al. From throw-away traffic to bots: Detecting the rise of DGA-based malware[C]//Proceedings of the 21st USENIX Conference on Security Symposium. Washington, USA: ACM, 2012: 491-506.

[4] WOODBRIDGE J, ANDERSON H S, AHUJA A, et al. Predicting domain generation algorithms with long short-term memory networks[J]. [2020]. https://arxiv.org/abs/1611.00791.

[5] VINAYAKUMAR R, SOMAN K P, POORNACHANDRAN P, et al. Evaluating deep learning approaches to characterize and classify the DGAs at scale[J]. Journal of Intelligent & Fuzzy Systems, 2018, 34(3): 1265-1276.

[6] 吕品, 李全刚, 柳厅文, 等. 基于双向LSTM的误植域名滥用检测方法[J]. 电子学报, 2018, 46(9): 2081-2086.
LU P, LI Q G, LIU T W, et al. Towards typosquatting abuse detection using bi-directional LSTM[J]. Acta Electronica Sinica, 2018, 46(9): 2081-2086. (in Chinese)

[7] TRAN D, MAC H, TONG V, et al. A LSTM based frame-

work for handling multiclass imbalance in DGA botnet detection[J]. Neurocomputing, 2018, 275: 2401-2413.
[8] HIGHNAM K, PUZIO D, LUO S, et al. Real-time detection of dictionary DGA network traffic using deep learning [J]. SN Computer Science, 2021, 2(2): 1-17.
[9] 杜鹏, 丁世飞. 基于混合词向量深度学习模型的DGA域名检测方法[J]. 计算机研究与发展, 2020, 57(2): 433-446.
DU P, DING S F. A DGA domain name detection method based on deep learning models with mixed word embedding[J]. Journal of Computer Research and Development, 2020, 57(2): 433-446. (in Chinese)
[10] HE K M, ZHANG X Y, REN S Q, et al. Deep residual learning for image recognition[C]//2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Las Vegas, USA: IEEE, 2016: 770-778.
[11] HOWARD A G, ZHU M L, CHEN B, et al. MobileNets: Efficient convolutional neural networks for mobile vision applications[EB/OL]. (2017) [2020]. https://arxiv. org/abs/1704.04861.
[12] TRAN D, MAC H, TONG V, et al. A LSTM based framework for handling multiclass imbalance in DGA botnet detection[J]. Neurocomputing, 2018, 275: 2401-2413.
[13] VINAYAKUMAR R, SOMAN K P, POORNACHANDRAN P, et al. DBD: Deep Learning DGA-based Botnet Detection[M]//Deep Learning Applications for Cyber Security. Cham: Springer International Publishing, 2019: 127-149.
[14] YU B, PAN J, HU J M, et al. Character level based detection of DGA domain names[C]//2018 International Joint Conference on Neural Networks (IJCNN). Rio, Brazil: IEEE, 2018: 1-8.
[15] QIAO Y C, ZHANG B, ZHANG W Z, et al. DGA domain name classification method based on long short-term memory with attention mechanism[J]. Applied Sciences, 2019, 9(20): 4205.
[16] ANDERSON H S, WOODBRIDGE J, FILAR B. DeepDGA: Adversarially-tuned domain generation and detection [C]//Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security. New York, USA: ACM, 2016: 13-21.
[17] SIDI L, NADLER A, SHABTAI A. MaskDGA: A black-box evasion technique against DGA classifiers and adversarial defenses[EB/OL]. (2019) [2020]. https://arxiv. org/abs/1902.08909.
[18] PECK J, NIE C, SIVAGURU R, et al. CharBot: A simple and effective method for evading DGA classifiers[J]. IEEE Access, 2019, 7: 91759-91771.

作者简介

刘小洋 男,1980年出生,安徽安庆人. 博士后. 现为重庆理工大学计算机科学与工程学院教授、硕士生导师. 主要从事社交网络分析、人工智能、网络安全与数据挖掘等方面的研究工作.
E-mail:lxy3103@163.com

刘加苗(通信作者) 男,1994年出生,重庆渝北人. 现为重庆理工大学计算机科学与工程学院硕士研究生. 主要从事网络安全、恶意流量检测与域名分析等方面的研究工作.
E-mail:jiamiaoliu@126.com