◆机器学习模型◆

基于改进 Transformer 和强化学习的僵尸网络 DGA 域名检测*

马永忠,夏保丽
(银川能源学院信息传媒学院,宁夏银川 750100)

摘要:针对现有僵尸网络检测方法检测精度不高和检测时间开销较大的问题,提出一种基于改进 Transformer 和强化学习的僵尸网络域名生成算法(Domain Generation Algorithm,DGA)的域名检测方法。首先,利用深度可分离卷积替换 ResNet 和 ResNeXt 网络中的卷积块,通过减少网络模型参数来降低模型的时间开销;其次,利用改进后的 ResNet 和 ResNeXt 网络将域名字符串映射到深度特征空间,构造多尺度特征,强化特征的表达能力;再次,利用长短期记忆神经网络(Long Short-Term Memory,LSTM)对 Transformer 网络进行改进,在保持字符间相对位置的同时,进一步建立上下文的长距离依赖编码,并在此基础上引入注意力机制,强化模型对关键特征的捕获能力;最后,引入强化学习对模型进行微调,提高 DGA 域名的检测精度。在多个 DGA 域名数据集上进行测试验证,结果表明该模型在保持检测时间开销较小的基础上,具有更高的检测精度。

关键词:僵尸网络 DGA 域名检测;深度可分离卷积;多尺度特征;Transformer;强化学习

中图分类号:TP393 **文献标识码**:A **文章编号**:1005-9164(2023)01-0139-10
DOI:10.13656/j.cnki.gxkx.20230308.016

互联网的快速发展给人们的日常生活和工作带来了众多便利,但与此同时,出于各种目的的网络恶意攻击事件也不断增多,如僵尸网络、点击欺诈和木马攻击等。该类攻击事件导致经济、信息等方面的安全损失不容小视。

域名生成算法(Domain Generation Algorithm,DGA)域名攻击事件中,攻击者首先向目标网络或主机中植入恶意软件,通过命令与控制(Command and Control,C&C)服务器建立与目标之间的联系[1],持续传输并控制攻击目标。此外,为达到隐匿性的效果,大多数攻击者采用 DGA、Fast-Flux、Domain-Flux 等域名变换技术随机大批量生成伪装域名[2,3],并在短时间内发起集群访问,造成目标网络瘫痪,影响合法用户的访问请求。因此,如何构建一种精确定位并识别 DGA 域名的模型成为网络安全领域的研究重点。

现有的 DGA 域名检测方法根据判定技术可以划分为基于历史流量的域名检测方法和基于字符级

收稿日期:2022-08-22 修回日期:2022-10-30
*银川能源学院校级科研项目(2022-KY-Z-9):"银川能源学院网络安全问题分析与防护对策研究"资助。
【第一作者简介】
马永忠(1982-),男,硕士,讲师,主要从事网络安全、深度学习、信息系统开发研究,E-mail:xiabl03@sina.com。
【引用本文】
马永忠,夏保丽.基于改进 Transformer 和强化学习的僵尸网络 DGA 域名检测[J].广西科学,2023,30(1):139-148.
MA Y Z,XIA B L. Botnet DGA Domain Name Detection Based on Improved Transformer and Reinforcement Learning [J]. Guangxi Sciences,2023,30(1):139-148.

特征的域名检测方法两大类[4]。其中,基于历史流量的域名检测方法大多依据攻击者的集群访问行为在短时间内的流量异常反应来快速判定待测域名的合法性。如 Stevanovic 等[5]提出一种域名系统(Domain Name System,DNS)流量分析的 DGA 域名检测方法,根据流经每个集群中主机的查询时间和频次,定位潜在恶意域名控制的 DNS 服务器,实现 DGA 域名的快速判定。张永斌等[6]提出一种基于域名组行为特征的恶意域名检测方法,通过对每个周期内域名解析请求的频次、失效域名集合等进行分析,并将请求同一组新域名的主机作为二次检测对象,进一步提高对恶意域名来源定位的准确性。韩春雨等[7]针对 Fast-Flux 产生的恶意域名隐蔽性强、难以检测的问题,提出一种基于 DNS 流量的 Fast-flux 恶意域名检测方法,从针对性和流量普适性等方面进一步提高了模型检测的性能。虽然上述基于历史流量的域名检测方法能够实现部分家族 DGA 域名的精确检测,但是该类模型主要通过恶意域名攻击所引起的流量异常给出待测域名合法或恶意的判断。然而,无论是从本地域名服务器还是其他域名服务器,流量数据采集的周期一般较长,导致系统检测时间开销较大,难以满足实际应用对检测实时性的高要求。

近年来,随着深度学习在计算机视觉和文本处理等方面的成功应用,利用深度学习和自然语言处理的相关技术解决网络安全中的恶意域名检测,成为网络安全领域新的热点研究课题[8-10]。

基于深度学习的恶意域名检测技术,根据特征提取手段可以划分为手动提取特征和自动提取特征。其中 Yadav 等[11]使用 Kullback-Leibler (KL)距离、编辑距离(Edit distance)和 Jaccard 系数计算映射到同一组 IP 地址域名的相似性,根据计算结果判断其是否为 DGA 域名。马栋林等[12]利用改进的 Relief 计算已有字符特征权重,再用 C5.0 分类器进行合法域名与恶意域名的判定。相比而言,利用深度学习自动提取的域名字符级和词级特征,在强化决策能力的同时可以有效捕捉关键词或关键字符对域名的决策能力,进一步挖掘家族恶意域名特征,提高检测范围。吴涛等[9]提出一种基于 Convolutional Neural Network - Bi - directional Long Short - Term Memory (CNN-BiLSTM)迁移自反馈学习的小样本恶意域名检测方法,利用卷积神经网络(Convolutional Neural Network,CNN)和双向长短期记忆神经网络的串行模型实现合法域名与 DGA 域名的判定。Yang 等[13]提出一种基于深度学习的 DGA 域名检测算法,通过提取域名的解析特征、字符分布和 n-gram 分布等特征,并结合机器学习算法构建决策树模型,实现 DGA 域名的快速判定。张斌等[8]提出一种基于 CNN 与长短期记忆神经网络(Long Short-Term Memory,LSTM)相结合的 DGA 域名检测算法,通过将 CNN 提取的局部特征与 LSTM 提取的上下文序列特征相结合,构造 DGA 域名检测判定模型。Ai - Alyan 等[14]利用 CNN 并结合注意力机制的双向长短期记忆神经网络,快速学习域名序列的局部和全局信息。

上述基于深度学习的恶意域名检测方法主要通过分析域名字符串的结构和构词特征来实现合法域名与恶意域名的快速判断,可以有效缓解检测模型时间开销大的问题。然而,无论是基于自动提取特征还是手动提取特征的检测方法,域名字符串的上下文信息利用不充分成为该类模型的瓶颈问题之一。此外,对于新出现或新变种的 DGA 域名,由于没有先验知识,该类模型的检测精度不佳。为此,针对现有 DGA 域名检测方法检测精度不高和检测时间开销较大的问题,本研究在自动提取特征的基础上,利用 LSTM 改进 Transformer 的编码方式,进一步引入域名字符串字符和单词之间的上下文信息,提高域名中字符或单词位置编码信息的捕获能力。此外,引入 Policy Gradient 强化学习方法,提高模型对于合法域名与 DGA 域名的判定精度。

1 DGA 域名检测模型

图 1 给出了基于改进 Transformer 和强化学习的僵尸网络 DGA 域名检测模型的流程。主要包括数据预处理模块,用于域名数据的规整操作;特征提取模块,用于将域名映射到深度特征空间;特征编码模块,用于提取深度空间中域名字符向量的上下文编码特征;强化学习模块,用于端到端优化模型参数。

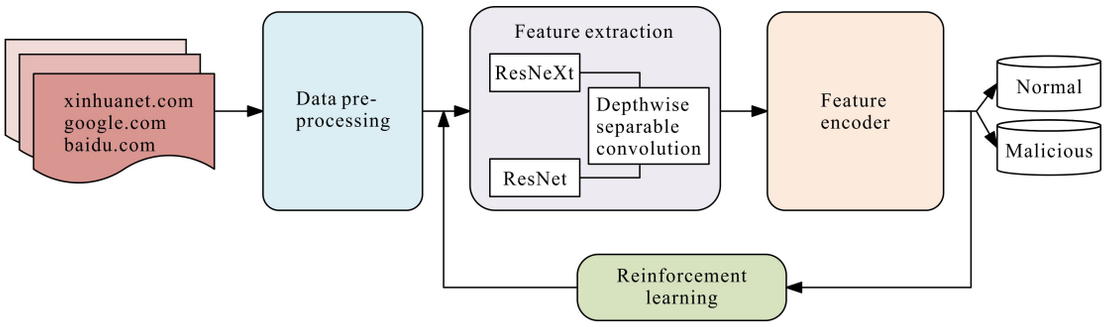

图 1　基于改进 Transformer 和强化学习的僵尸网络 DGA 域名检测模型流程图

Fig. 1　Flow chart of the botnet DGA domain name detection model based on improved Transformer and reinforcement learning

1.1　数据预处理

从 DGA Domain List、Alexa 和 Malware Domain List 等开源数据集,以及网络安全信息与动态周报等网页上收集整理合法域名和僵尸网络 DGA 域名,并去除域名中的顶级域名,提取二级、三级、四级等主体域名字符串,构造合法域名样本集和恶意域名样本集。

以"google.com"为例说明数据预处理过程。首先,删除顶级域名字符串".com",仅保留主体域名字符串"google",并为每个域名字符串添加标签,其中合法域名标记为 0,DGA 域名为 1;然后,将"google"域名字符串转换为序列{g,o,o,g,l,e},并将域名字符串统一为定长的 n,当域名字符串长度大于 n 时,对超出部分进行裁剪;当域名字符串长度不足 n 时,用 0 补齐。采集的域名数据集中主体域名长度 n 大部分小于 28 (图 2),因此,n 值设定为 28。字符串裁剪如公式(1)所示。

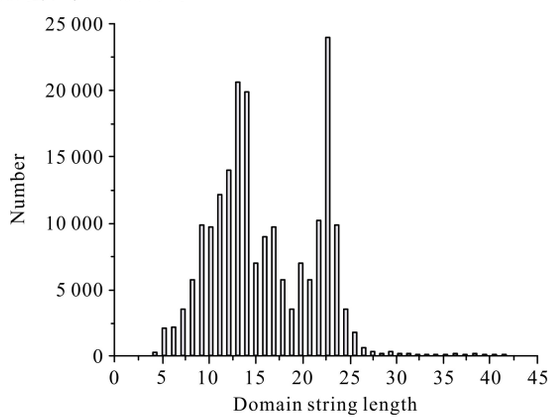

图 2　主体域名长度统计图

Fig. 2　Main domain name length statistics chart

$$s(str_i)=\begin{cases}0+str_i, l(str_i)<n\\ str_i, l(str_i)=n\\ str_i[0,n-1], l(str_i)>n\end{cases}, \quad (1)$$

式中:$s(str_i)$ 表示经过裁剪后的定长向量,str_i 表示每一标准化的域名,$l(str_i)$ 表示域名 str_i 的长度。

1.2　特征提取

合法域名和 DGA 域名在构造方法和规则上形式相对自由,但在字符组成上仍存在上下文依赖关系[13]。然而,通过不断堆叠网络层数来提取更丰富的字符级和词级特征,极易导致模型出现梯度消失、性能衰退和梯度弥散等问题,因此,利用深度残差学习模块,通过堆叠层去拟合残差映射。残差网络结构设计如图 3 所示。

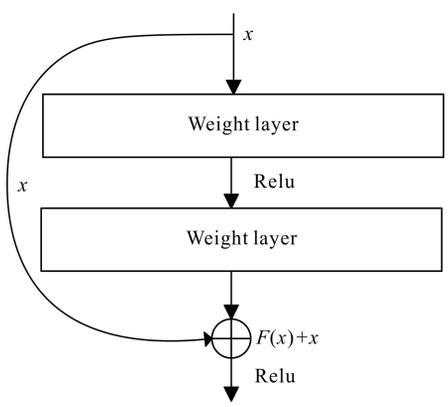

图 3　残差网络结构

Fig. 3　Residual network structure

网络层数的增加会导致模型计算复杂度增大,而 ResNeXt 网络能较好地解决该问题[15]。同时,ResNeXt 网络也具有处理上下文时序关系的能力。此外,充分考虑到深度网络对硬件设备性能的高需求,采用深度可分离卷积(Depthwise Separable Convolution,DSC)代替卷积操作对原始 ResNeXt 进行改进,通过降低参数量来加快模型推断的速度。DSC 神经网络结构如图 4 所示,首先,将域名字符向量经过一次卷积运算,生成 M 张特征图;然后,利用卷积核大小为 $n\times n$ 的多个卷积块将特征图沿着深度方向进行加权组合,得到输入字符向量在深度空间的特征映射;最后,在逐点卷积运算过程中,利用 1×1 的卷积核进行卷积滤波。因此,DSC 可以看作深度卷

积和逐点卷积的组合,该部分的验证见消融实验。

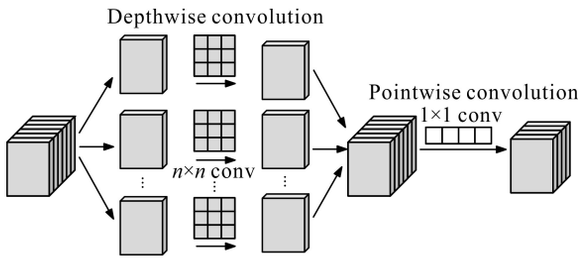

图 4 深度可分离卷积神经网络结构

Fig. 4 Depthwise separable convolution neural network structure

因域名字符长度短、字符单一,所包含信息局限,多尺度特征适用于特征局限等问题,故选用 ResNet 和 ResNeXt 网络作为主干网络,分别提取域名主体字符串的字符级和词级特征,利用多尺度特征强化特征的表征能力,结构如图 5 所示。计算如公式(2)、(3)和(4)所示。

$$R_1(str_i)=f_{\text{ResNet}}(str_i)\ , \tag{2}$$

$$R_2(str_i)=f_{\text{ResNeXt}}(str_i)\ , \tag{3}$$

$$R(str_i)=R_1(str_i)+R_2(str_i)\ , \tag{4}$$

式中:$R_1(str_i)$ 表示 ResNet 提取的字符级特征,$R_2(str_i)$ 表示 ResNeXt 提取的词级特征,$f(\cdot)$表示特征提取函数。

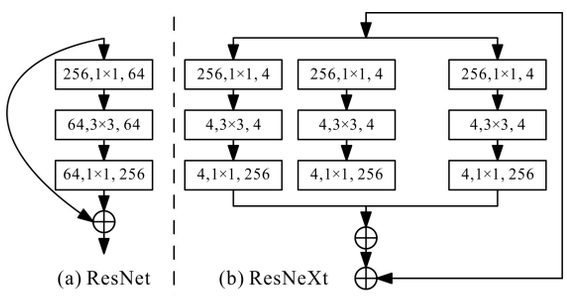

图 5 特征提取主干网络结构

Fig. 5 Feature extraction backbone network structure

1.3 特征编码

近年来,Transformer 广泛应用于自然语言处理和计算机视觉领域,并取得了突破性的进展[16]。因此,尝试利用 Transformer 作为域名字符深度特征的编码器,结构如图 6 所示。

Transformer 网络由多个相同的层堆叠组成,每个编码器层由多头注意力机制和前馈网络组成,并用一个残差连接。其中,注意力机制用于强化关键词或关键字符的决策能力,可表示为公式(5)。

$$\text{attention}<Q,K,V>=\text{softmax}(QK^{\mathrm{T}})V, \tag{5}$$

式中:Q、K、V 分别表示查询、键和值的输入矩阵。此外,为了使模型能够同时关注提取的特征 $R(str_i)$

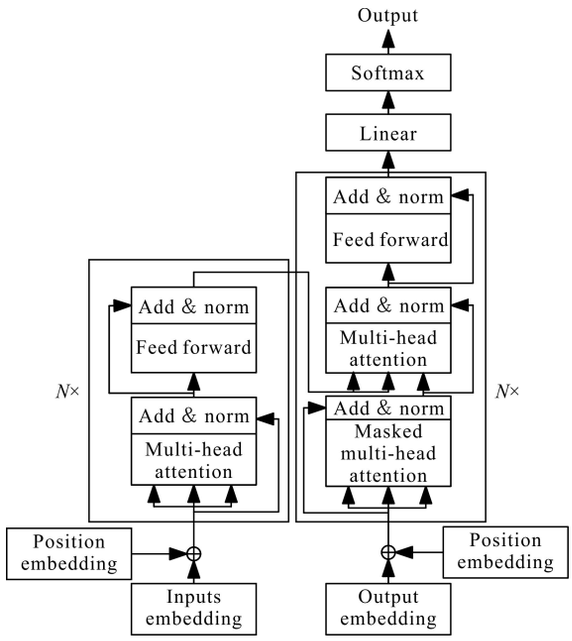

图 6 Transformer 网络特征编码流程

Fig. 6 Feature encoder process of the Transformer network

在不同空间位置处的深度特征信息,引入多头注意力机制。通过对输入的 Q、K 和 V 进行多次映射,得到多对注意力的结果值,表示为公式(6)。

$$\text{multi-head}(Q,K,V)=\text{concat}(\text{head}_1,\cdots,\text{head}_n)W', \tag{6}$$

式中:$\text{head}_i=\text{attention}(QW_i^Q,KW_i^K,VW_i^V)$表示第 i-head 的输出,n 为 head 的总数,W_i^Q、W_i^K、W_i^v 和 W' 为参数矩阵,均由模型学习获得。

此外,Transformer 网络虽然提供了位置编码,但是仅考虑了相对位置编码信息,与域名字符或单词无关,使得编码特征无法同时结合字符的上下文信息和相对位置编码信息。因此,首先借鉴 LSTM 对 Transformer 进行改进,即改进后的模型同时包含了字符级或单词级的上下文信息和 Transformer 提供的相对位置编码信息;其次,受残差网络的启发,赋予主干网络 ResNet 和 ResNeXt 提取的特征 $R(str_i)$ 不同比例的权重,并与引入 LSTM 的 Transformer 输出值进行点积计算,进一步强化字符级和词级特征的重要性;最后,利用改进后的模型对域名进行深度特征编码,并利用 softmax 层进行分类检测,快速给出待测域名的判定结果。改进后的 Transformer 模型结构如图 7 所示。

1.4 强化学习优化

为进一步提升模型对待测域名定位与识别的准确性,引入了策略梯度的强化学习[17]。在强化学习中将基准模型作为 Agent,域名主体字符序列作为

Environment。模型每间隔一个时间步,Agent 对应一个预测结果,并根据预测准确性,计算出奖励值,反馈至 Agent,模型优化流程如图 8 所示。

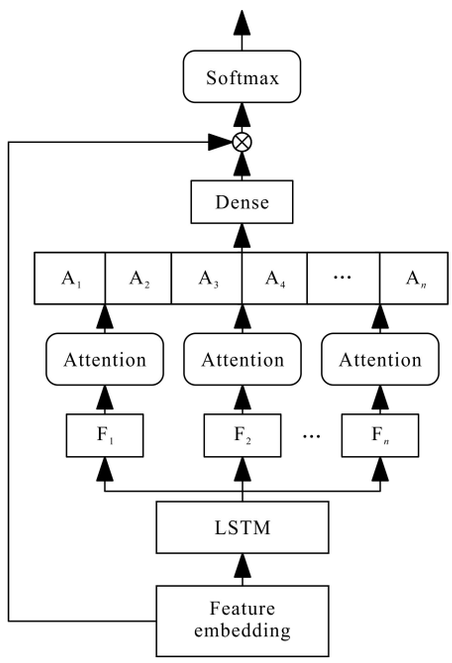

图 7 改进后的 Transformer 特征编码流程

Fig. 7 Improved transformer feature encoder process

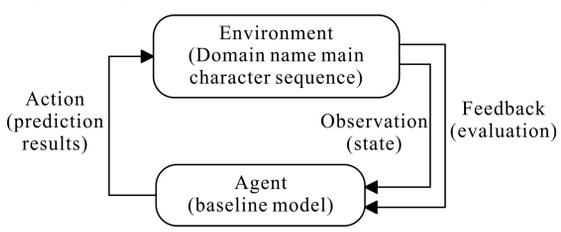

图 8 强化学习模型优化流程示意图

Fig. 8 Schematic diagram of the reinforcement learning model optimization process

利用强化学习对模型进行优化时,设待测域名字符串在 t 时刻预测的状态、结果和奖励所组成的序列为 $\tau_t=\{s_1,a_1,r_1,\cdots,s_t,a_t,r_t\}$,其中 s_t 表示 Environment 在 t 时刻的状态;a_t 表示在 t 时刻所预测的结果;r_t 表示奖励值。最后,通过使用损失值和奖励值计算损失函数梯度,并根据梯度值整体优化模型参数,计算如公式(7)和(8)所示。

$$L(\theta)=-\frac{1}{N}\sum_{\tau_t}R(\tau_t)\log\pi_\theta(\tau_t)=-E_{\tau_t\sim\pi_\theta}[R(\tau_t)],\tag{7}$$

$$\nabla_\theta L(\theta)=-E_{\tau_t\sim\pi_\theta}[R(\tau_t)\cdot\nabla\log\pi_\theta(\tau_t)],\tag{8}$$

式中:$L(\theta)$ 表示损失值,N 表示环境中的样本个数,$R(\tau_t)$ 表示 τ_t 的总奖励值,$E_{\tau_t\sim\pi_\theta}$ 表示奖励的期望值。$\nabla_\theta(\cdot)$ 表示导函数;π_θ 表示策略梯度。

2 实验与结果分析

2.1 数据集

从公开数据集和网络安全信息与动态周报等网页中收集整理获得 500 000 条合法域名和 200 000 条恶意域名。其中合法域名主要来源于 Alexa 和思科收集的合法域名白名单;DGA 域名主要来源于 Malware Domain List 和 360 网络安全实验室收集的 22 种经典家族 DGA 恶意域名,并按照 7∶3 的比例划分为训练数据和测试数据。样本详细数据如表 1 所示。

表 1 数据集描述

Table 1 Description of the dataset

类型 Types		描述 Description	数量(万) Quantities (ten thousand)
Legal domain names		Alexa,domain whitelists from Cisco	50
Malicious domain names	Malware Domain List (MD)	http://www.malwaredomainlist.com/	5
	360Netlab	Virut, Bamital, Cleaner, Emotet, Corebot, Fobber, Gspy, Madmax, Matsnu, Bigviktor, Conficker, Enviserv, Feodo, Mirai, Padcrypt, Mydoom, Nymaim, Qadars, Tinynuke, Tofsee, Vawtrak, Xshellghost	15

2.2 实验环境与评价指标

实验环境为 64 位联想 P15,8 核 16 线程 i9-10885H 1T SSD,模型采用 Pytorch 深度学习框架,开发环境为 Anaconda 3.5.7,Python 版本为 3.7,显卡为英伟达 GTX3060Ti。优化器采用 Adam,初始学习率为 0.000 1。此外,为防止模型过拟合,采用 dropout=0.5,batch_size=128。

图 9 给出了模型训练准确率(Accuracy)、损失值

(Loss)与迭代次数(Epoch)之间的对应曲线。可以看出,在 Epoch 为 90 时,训练和测试阶段的 Accuracy 和 Loss 曲线区域平稳,因此,设定 Epoch 为 90。

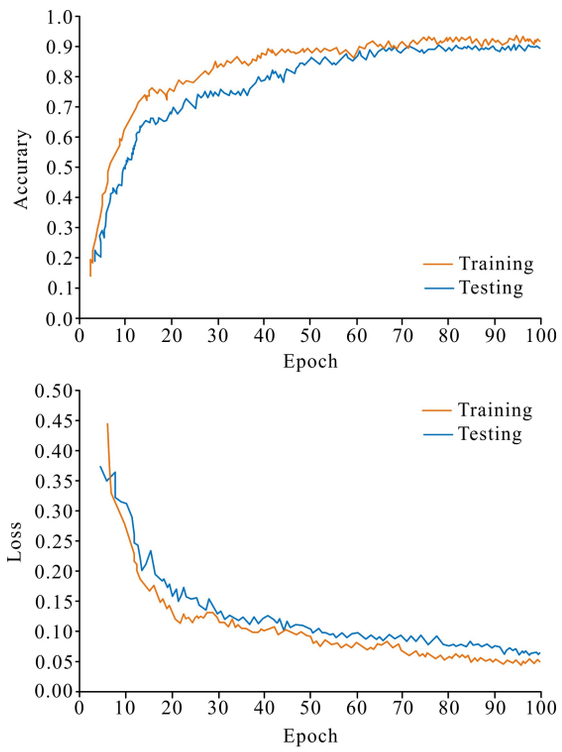

图 9　准确率、损失与训练轮次对应曲线

Fig. 9　Correspondence curves of the accuracy, loss and training epoch

实验结果评价指标采用准确率(Accuracy)、精准率(Precision)、召回率(Recall)和 $F1$ 等,计算如公式(9)所示。

$$\begin{cases} \text{Accuracy}=\dfrac{T_{m\to m}+T_{n\to n}}{T_{m\to m}+F_{m\to n}+T_{n\to n}+F_{n\to m}} \\ \text{Precision}=\dfrac{T_{m\to m}}{T_{m\to m}+F_{n\to m}} \\ \text{Recall}=\dfrac{T_{m\to m}}{T_{m\to m}+F_{m\to n}} \\ F1=\dfrac{2\times\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}} \end{cases}, \tag{9}$$

式中:$T_{m\to m}$ 表示准确检测出的 DGA 域名总数,$F_{m\to n}$ 表示将 DGA 域名误报为合法域名的个数,$F_{n\to m}$ 表示将合法域名误报为 DGA 域名的个数,$T_{n\to n}$ 表示被算法准确检测出的 DGA 域名总数。

此外,为了进一步评价模型的整体检测性能,利用 AUC 表示 ROC 曲线下的区域,其中,ROC 曲线是以 FPR 为 X 轴,TPR 为 Y 轴绘制的曲线,计算如公式(10)所示。

$$\text{AUC}=\int(\text{TPR})d(\text{FPR})\ 。 \tag{10}$$

2.3　结果与分析

①经典 DGA 家族恶意域名检测。

表 2 给出了模型对 360 网络安全实验室收集的 22 种经典 DGA 家族恶意域名的检测性能。可以看出,模型对 22 种 DGA 家族恶意域名的平均检测准确率为 95.72%,其中 5 种家族恶意域名检测精度超过 97%,10 种家族恶意域名检测精度超过 96%,16 种家族恶意域名检测精度超过 95%,仅 Fobber、Madmax 和 Mydoom 家族检测精度不足 94%,但仍可以达到 93.58%及以上的准确率。此外,模型在保持较高检测精度的基础上,可以识别出多家族多种类型的恶意域名,具有更广泛的检测范围。

②对比实验。

为了验证模型的有效性,在相同的评价指标下,与当前主流模型进行对比,包括文献[8,18-24]中的模型,实验结果如表 3 所示。由表 3 可知,模型可实现平均检测 Accuracy 为 97.59%、Precision 为 96.81%、Recall 为 96.94%、F1 为 95.82%,检测时间开销(Time Overhead,TO)为 9.76 s,相比所有对比模型,优势明显。本研究的主要目的是尽可能地检测出 DGA 域名以及最大限度地降低 DGA 域名漏报为合法域名的可能,Recall 值验证了模型的设计初衷。与合法域名误报为 DGA 域名的实际代价相比,DGA 域名漏报为合法域名的代价更大[25],这进一步证实了模型的实际应用价值。

表 2　多家族 DGA 域名检测(%)

Table 2　Multi-family DGA domain name detection (%)

类型 Types	准确率 Accuracy	精准率 Precision	召回率 Recall	$F1$	类型 Types	准确率 Accuracy	精准率 Precision	召回率 Recall	$F1$
Virut	96.30	94.63	94.12	95.02	Enviserv	95.68	95.41	94.86	94.04
Bamital	95.84	97.01	96.20	94.09	Feodo	96.39	96.65	95.23	94.51
Ccleaner	94.86	92.42	93.39	93.88	Mirai	95.22	96.08	95.36	94.27
Emotet	97.15	96.25	96.22	95.24	Padcrypt	97.29	96.25	96.09	95.36

续表

Continued table

类型 Types	准确率 Accuracy	精准率 Precision	召回率 Recall	*F*1	类型 Types	准确率 Accuracy	精准率 Precision	召回率 Recall	*F*1
Corebot	97.34	96.62	96.26	96.08	Mydoom	93.58	93.10	93.64	93.79
Fobber	93.79	94.06	93.67	94.44	Nymaim	95.36	94.59	94.14	94.62
Gspy	96.16	96.60	97.22	96.39	Qadars	97.01	97.08	96.19	95.15
Madmax	93.77	93.10	94.49	94.17	Tinynuke	95.66	96.03	95.53	96.56
Matsnu	95.38	94.76	94.23	94.09	Tofsee	94.69	93.82	94.55	94.03
Bigviktor	97.46	96.59	96.01	95.80	Vawtrak	94.39	95.03	95.14	94.62
Conficker	96.15	95.88	95.50	95.61	Xshellghost	96.28	96.29	95.87	94.73

表 3　本研究模型与当前主流模型的性能对比

Table 3　Performance comparison of the proposed method with current mainstream models

方法 Methods	准确率（%） Accuracy（%）	精准率（%） Precision（%）	召回率（%） Recall（%）	*F*1（%）	TO（s）
Zhang et al[8]	95.10	95.42	93.91	94.66	12.67
Huang et al[18]	97.46	96.51	96.75	95.73	13.64
Zhu et al[19]	94.71	94.09	94.32	94.76	11.65
Selvi et al[20]	96.18	96.30	96.79	95.80	15.40
Yang et al[21]	95.26	94.92	95.01	94.17	19.21
Zhang et al[22]	94.52	96.49	96.27	94.13	46.38
Wang et al[23]	95.28	94.39	95.08	95.38	112.00
Li et al [24]	94.38	93.25	95.43	94.32	21.08
Ours	97.59	96.81	96.94	95.82	9.76

此外，图 10 给出了不同模型之间的 ROC 曲线对比结果，AUC 面积越大，表明模型的预测效果越好，可以看出，相比其余对比模型，本研究模型的 AUC 值最大，即预测效果最好。

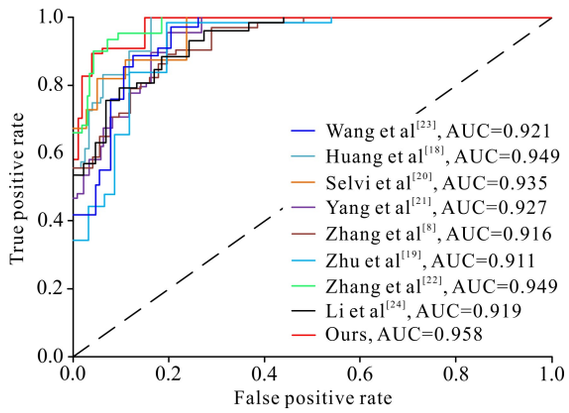

图 10　本研究模型与当前主流模型的 ROC 曲线对比

Fig. 10　ROC curves comparison of the proposed method with current mainstream models

2.4　消融实验

2.4.1　多头注意力分析

Transformer 中注意力头 head 数量在测试集上的准确率曲线如图 11 所示。可以看出，随着 head 的增加，准确率上升趋势明显；当 head 达到 12 时，增加 head 数，曲线趋于平稳。因此，设定注意力头 head 的值为 12。

2.4.2　改进的 Transformer 性能测试

为验证改进后 Transformer 的检测性能，分别构造原始 Transformer、仅利用 LSTM 改进的 Transformer 模型、利用 LSTM 与残差权值计算（Residual Weights Calculation，RWC）改进的 Transformer 以及最终模型。此外，进一步验证了强化学习对模型检测性能提升的影响，并在测试集上进行验证。实验结果如表 4 所示。

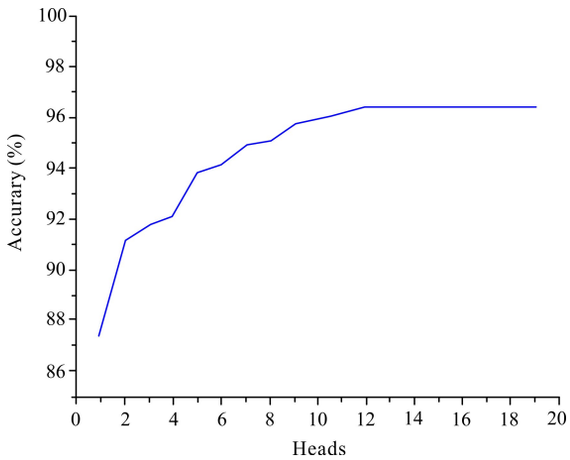

图 11　注意力头 head 的个数与准确率之间的关联曲线

Fig. 11　Correlation curve between the number of attention head and accuracy

由表 4 可知,利用原始 Transformer 进行特征编码时,虽然可以实现 93.76%的平均检测准确率,但是通过 LSTM 改进的 Transformer,同时考虑了字符的上下文信息和相对位置编码信息,平均检测准确率提升了 1.52%;此外,利用残差网络的原理,进一步提升了模型检测性能,提升效果显著;最后,利用强化学习进一步微调模型,平均检测准确率为 97.59%。上述结果验证了模型设计的高效性。

2.4.3　深度可分离卷积

DSC 将标准卷积过程分解为多个等效的深度卷积和逐点卷积,在卷积运算过程中通过分解滤波器来降低参数量,在识别性能变化可接受的范围内尽可能通过减少模型参数量来降低模型的训练时间开销。表 5 给出了引入 DSC 对模型整体检测性能的影响。可以看出,相比未引入 DSC 的基准模型,引入 DSC 的模型虽然其检测准确率下降了 0.12%,但其检测时间开销降低了 36.54%。考虑到恶意攻击检测的实时性要求,检测精度下降比例在可接受范围之内,上述实验结果进一步验证了采用 DSC 代替标准卷积进行特征提取的有效性。

表 4　消融实验(%)

Table 4　Ablation experiments (%)

方法 Methods	准确率 Accuracy	精准率 Precision	召回率 Recall	*F*1
Transformer	93.76	93.25	92.86	92.93
LSTM + Transformer	95.28	95.37	94.94	94.89
LSTM + Transformer + RWC	95.91	95.86	95.05	94.90
LSTM + Transformer + RWC + Reinforcement learning	97.59	96.81	96.94	95.82

表 5　深度可分离卷积消融实验

Table 5　Ablation experiments of depthwise separable convolution

方法 Methods	准确率(%) Accuracy (%)	精准率(%) Precision (%)	召回率(%) Recall (%)	*F*1 (%)	TO (s)
LSTM + Transformer + RWC + Reinforcement learning	96.38	96.11	96.94	95.82	15.38
DSC + LSTM + Transformer + RWC + Reinforcement learning	96.26	96.08	96.82	95.79	9.76

3　结束语

本研究提出了一种新的 DGA 域名检测算法,通过利用 DSC 代替传统卷积,缓解了模型运行时间较长的问题;此外,尝试将 Transformer 应用到 DGA 域名检测领域,在原始 Transformer 的基础上,利用 LSTM 进行编码方式改进,同时考虑了相对位置编码和上下文语义信息;受残差网络的启发,将改进编码方式的 Transformer 的输出值与原始提取的特征进行点积计算,进一步强化了字符级和词级特征的重要性;最后,利用强化学习从数据样本中获取奖励值来优化模型参数,提升模型的检测性能。通过在测试集上进行测试,验证了所提出模型具有较低的时间开销、较高的检测精度和较广的检测范围,为实时定位木马、僵尸网络等的攻击提供了一种新思路,丰富了 DGA 域名的检测手段。

参考文献

[1]　赵宏,常兆斌,王乐. 基于词法特征的恶意域名快速检测算法[J]. 计算机应用,2019,39(1):227-231.

[2]　彭成维,云晓春,张永铮,等. 一种基于域名请求伴随关

系的恶意域名检测方法[J].计算机研究与发展,2019,56(6):1263-1274.

[3] YAN X D,XU Y,CUI B J. Learning URL embedding for malicious website detection [J]. IEEE Transactions on Industrial Informatics,2020,16(10):6673-6681.

[4] VAN CAN N,TU D N,TUAN T A,et al. A new method to classify malicious domain name using Neutrosophic sets in DGA botnet detection [J]. Journal of Intelligent & Fuzzy Systems,2020,38(4):4223-1236.

[5] STEVANOVIC M,PEDERSEN J M,D'ALCONZO A,et al. On the ground truth problem of malicious DNS traffic analysis [J]. Computing and Security,2015,55(11):142-158.

[6] 张永斌,陆寅,张艳宁.基于组行为特征的恶意域名检测[J].计算机科学,2013,40(8):146-148,185.

[7] 韩春雨,张永铮,张玉. Fast-flucos:基于 DNS 流量的 Fast-flux 恶意域名检测方法[J].通信学报,2020,41(5):37-47.

[8] 张斌,廖仁杰.基于 CNN 与 LSTM 相结合的恶意域名检测模型[J].电子与信息学报,2021,43(10):2944-2951.

[9] 吴涛,王占海,张健,等.基于 CNN-BilSTM 迁移自反馈学习的小样本恶意域名检测[J/OL].小型微型计算机系统,2022(2022-01-12)[2022-02-13]. https://doi.org/10.20009/j.cnki.21-1106/TP.2021-0580.

[10] FANG L M,YUN X Y,YIN C C,et al. ANCS:automatic NXDomain classification system based on incremental fuzzy rough sets machine learning [J]. IEEE Transactions on Fuzzy Systems,2020,5(7):742-756.

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

[12] 马栋林,张澍寰,赵宏.改进 Relief-C5.0 的恶意域名检测算法[J].计算机工程与应用,2022,58(11):100-106.

[13] YANG P,ZHEN G,ZENG P. Phishing website detection based on multidimensional features driven by deep learning [J]. IEEE Access,2019,7:15196-15209.

[14] AI-ALYAN A,AI-AHMADI S. Robust URL phishing detection based on deep learning [J]. Ksii Transactions on Internet and Information Systems,2020,14(7):2752-2768.

[15] SU A,HE X L,ZHAO X F. JPEG steganalysis based on ResNeXt with Gauss partial derivative filters [J]. Multimedia Tools and Applications,2021,80:3349-3366.

[16] YANG C,LU T L,YAN S Y,et al. N-Trans:parallel detection algorithm for DGA domain names [J]. Future Internet,2022,14(7):209.

[17] SUBRAMANIAN A,CHITLANGIA S,BATHS V. Reinforcement learning and its connections with neuroscience and psychology [J]. Neural Networks,2021,145:271-287.

[18] 黄蔚秋,欧毓毅,凌捷.基于 APCNN 和 BiGRU-Att 的单词 DGA 域名检测方法[J].计算机应用研究,2021,39(5):1541-1545.

[19] ZHU J L,PENG G H,WANG D W. Dual-domain-based adversarial defense with conditional VAE and bayesian network [J]. IEEE Transactions on Industrial Informatics,2021,17(1):596-605.

[20] SELVI J,RODRIGUEZ R J,SORIA-OLIVAS E. Detection of algorithmically generated malicious domain names using masked N-grams [J]. Expert Systems with Applications,2019,124:156-163.

[21] 杨路辉,白惠文,刘光杰,等.基于可分离卷积的轻量级恶意域名检测模型[J].网络与信息安全学报,2020,6(6):112-120.

[22] 张凤,张微,魏金花.基于 BERT 和层次化 Attention 的恶意域名检测[J].中国电子科学研究院学报,2022,17(3):290-296.

[23] 王甜甜,刘雄飞.一种分阶段的恶意域名检测算法[J].小型微型计算机系统,2022,43(10):2046-2050.

[24] 李晓冬,李育强,宋元凤,等.新的基于融合向量的 DGA 域名检测方法[J].计算机应用研究,2022,39(6):1834-1837,1844.

[25] ZHAO H,CHANG Z B,WANG W J,et al. Malicious domain names detection algorithm based on lexical analysis and feature quantification [J]. IEEE Access,2019,7:128990-128999.

Botnet DGA Domain Name Detection Based on Improved Transformer and Reinforcement Learning

MA Yongzhong, XIA Baoli
(School of Information Media, Yinchuan University of Energy, Yinchuan, Ningxia, 750100, China)

Abstract: Aiming at the problems of low detection accuracy and large detection time overhead of existing botnet detection methods, a domain name detection method based on improved Transformer and reinforcement learning Domain Generation Algorithm (DGA) is proposed. Firstly, the deep separable convolution is used to replace the convolution blocks in ResNet and ResNeXt networks, and the time overhead of the model is reduced by reducing the network model parameters. Secondly, the improved ResNet and ResNeXt networks are used to map domain name strings into the deep feature space to construct multi-scale features, which is helpful for enhancing the ability of the feature expression. Thirdly, the Transformer network is improved by using the Long Short-Term Memory (LSTM) neural network. While maintaining the relative position between characters, the long-distance dependent coding of context is further established. On this basis, the attention mechanism is introduced to strengthen the model's ability to capture key features. Finally, reinforcement learning is introduced to fine-tune the model to improve the detection accuracy of DGA domain name. Through testing and verification on multiple DGA domain data sets, the results show that the model has higher detection accuracy while maintaining less detection time overhead.

Key words: Botnet DGA domain name detection; depthwise separable convolution; multi-scale feature; Transformer; reinforcement learning

责任编辑:陆　雁