山西大学学报(自然科学版)48(4):725—740,2025
Journal of Shanxi University(Nat. Sci. Ed.)

DOI:10.13451/j.sxu.ns.2025018

面向僵尸网络DGA攻击的智能检测技术与对抗策略研究

卫鸿婧[1],胡治国[2]

(1.中国移动通信集团山西有限公司,山西 太原 030032;
2.山西大学 大数据科学与产业研究院,山西 太原 030006)

摘 要:僵尸网络通过域名生成算法(Domain Generation Algorithms,DGA)能够动态生成大量难以预测的域名,从而规避传统静态监测机制,提升恶意活动的隐蔽性与持久性。随着DGA技术的不断演进,传统检测方法面临的挑战愈加严峻。如何高效识别与防范此类域名成为网络安全领域的关键问题。本文系统分析当前主流的DGA检测技术,涵盖基于统计特征、机器学习及深度学习的方法,深入探讨其工作原理、适用场景与性能表现,揭示现有研究在误报率、计算复杂度、数据集规模及新型DGA适应性等方面的不足。最后,本文提出深度学习优化与跨域协同检测的创新方向,并结合流量行为分析与生成规律阻断机制,构建多层次、综合性的DGA防御体系,为提升检测技术的有效性、准确性与适应性提供新思路。

关键词:僵尸网络;域名生成算法;域名检测;机器学习

中图分类号:TP393 **文献标志码**:A **文章编号**:0253-2395(2025)04-0725-16

The Research on Intelligent Detection Technology and Countermeasures for Botnet DGA Attacks

WEI Hongjing[1], HU ZhiGuo[2]

(1. *China Mobile Communications Group Shanxi Co, Ltd, Taiyuan* 030032*,China;*
2. *Institute of Big Data Science and Industry of China, Shanxi University, Taiyuan* 030006*, China*)

Abstract: Botnets can dynamically generate numerous unpredictable domains *via* Domain Generation Algorithms (DGA) to elude traditional static detection, enhancing the stealth and persistence of malicious activities. As DGA technology advances, traditional detection methods are facing growing challenges. Efficiently identifying and defending against these domains has become crucial in cybersecurity. This paper comprehensively analyzes mainstream DGA detection technologies, including those based on statistical features, machine learning, and deep learning. It delves into their principles, application scenarios, and performance, uncovering limitations in false positive rates, computational complexity, dataset size, and adaptability to new DGAs. Finally, the paper proposes innovative directions for deep learning-based detection and cross domain collaborative detection. Combined with traffic behavior analysis and generation-pattern blocking mechanisms, we build a multi-Layered, integrated DGA defense system, offering new ideas to improve detection effectiveness, accuracy, and adaptability.

Key words: botnet; domain generation algorithm; domain detection; machine learning

收稿日期:2025-02-15;**接受日期**:2025-03-24

基金项目:国家自然科学基金(61872226)

作者简介:卫鸿婧(1984—),女,山西太原人,硕士,高级工程师,研究方向为通信网络优化、网络安全。E-mail:13934666360@139.com

引文格式:卫鸿婧,胡治国.面向僵尸网络DGA攻击的智能检测技术与对抗策略研究[J].山西大学学报(自然科学版),2025,48(4):725-740. DOI:10.13451/j.sxu.ns.2025018.

0 引言

0.1 研究背景与问题

随着互联网技术的快速发展和恶意软件攻击方式的持续升级,僵尸网络(Botnet)已经构成全球网络安全领域中的一个重大隐患。僵尸网络由大量被恶意软件感染的设备组成,这些受控设备通过远程指令执行各种网络攻击,例如分布式拒绝服务(Distributed Denial of Service,DDoS)攻击、垃圾邮件传播和数据窃取等。为了规避基于固定IP地址或预设域名的传统检测策略,攻击者正逐渐转向更具隐蔽性和灵活性的通信手段。在这一背景下,域名生成算法(Domain Generation Algorithms, DGA)凭借自动批量地产生临时可用域名的能力,已成为僵尸网络指挥与控制C&C通信链条中的关键支撑技术[1-2]。

DGA技术通过自动化算法生成大量短期有效的域名,使得攻击者能够绕过传统基于静态域名黑名单或IP地址的防御系统。由于这些域名的高度动态性和随机性,传统的基于域名解析的检测方法往往难以有效识别和防范此类攻击。尤其是近年来,随着DGA生成技术不断演进,其域名生成模式愈趋复杂且难以预测,进一步提高了网络安全防护的难度[3-4]。尽管已有研究探索了针对DGA的检测技术,但现有方法在检测精度、实时性和计算资源利用等方面仍面临诸多挑战[5]。因此,如何在复杂多变的网络环境中高效捕捉并识别DGA域名,仍然是当下必须优先解决的关键难题。

在此背景下,本文旨在综述现有的DGA检测技术,分析其应用现状与发展趋势,并探讨面临的技术难题与未来研究方向。通过对DGA生成算法与检测方法的深入剖析探讨,本文希望为未来的防御策略提供理论依据和技术支持。

0.2 DGA的定义与重要性

DGA是一种用于自动生成大量域名的技术,这些域名通常具有高度的随机性和动态性,并且与真实合法域名难以区分。DGA生成的域名与传统静态域名不同,它们在生命周期内频繁变化,增加了检测难度。DGA的生成方法多样,包括基于字典的拼接、字符随机化以及基于熵值的生成等。这些策略使得DGA能够迅速产生大量域名,从而广泛应用于僵尸网络的指挥与控制(C&C)通信[6-7]。DGA在僵尸网络中充当着关键角色,它不仅使攻击者能够绕过基于静态黑名单和IP地址的传统检测机制,还能够在一定程度上保证C&C通信的稳定性与隐蔽性。攻击者通过DGA动态控制被感染设备,并指挥其执行恶意活动。由于DGA生成的域名会在短时间内频繁变化,传统的检测方法,如基于静态域名匹配和域名系统(Domain Name System,DNS)流量分析的检测,往往无法有效应对。随着生成算法的不断升级,攻击者能够根据网络环境和检测机制的变化实时调整生成规则,从而逃避检测。这一特点使得DGA成为当前网络安全防御中的重大挑战[8]。随着DGA技术的广泛应用,相关的检测技术手段也不断发展。目前,DGA检测方法大致可以分为基于统计特征、基于机器学习以及基于深度学习的检测方法[9-11]。然而,由于DGA的快速演化和高度不可预测性,现有检测方法面临诸多挑战,如过高的计算资源消耗、较高的误报率和实时性不足等问题。因此,如何有效地检测和防御DGA攻击,仍然是网络安全领域需要攻克的研究难题。

本文阐述了僵尸网络和DGA的基本概念及其背景,阐述了DGA在现代网络攻击中的关键作用及其对网络安全防护所带来的挑战。针对DGA检测技术的核心挑战,系统探讨了基于统计特征、机器学习、深度学习及区块链的方法,然后归纳了新兴检测技术与跨领域协同检测方法。最后在这些研究工作的基础上,我们基于网络流量分析与域名生成规律提出了一种动态防御框架,通过实时流量行为分析捕捉异常域名请求特征,结合生成规律阻断技术通过逆向分析恶意程序的DGA算法,建立规则库和分级拦截机制,实现对恶意域名的快速匹配和拦截。同时,采用域名信誉评估机制,对新生成域名进行评估,及时阻断或标记可疑域名,并与全球域名安全共享平台对接,实现跨域名系统的实时防护。以此构建出多层次、综合性的DGA攻击防御体系,以提高检测与拦截的整体效能。该体系通过特征层融合与决策层协同

优化,为应对动态化、智能化的僵尸网络DAG攻击提供了可扩展的技术范式。

1 僵尸网络与域名生成算法

1.1 僵尸网络的基本概念

僵尸网络(Botnet)是指由众多备受恶意软件感染的计算机构成的分布式网络,攻击者一般会使用远程指令进行控制,用于执行各种非法或恶意活动。作为网络攻击的主要工具之一,僵尸网络广泛应用于垃圾邮件传播、分布式拒绝服务攻击以及加密货币挖掘等领域。僵尸网络的高度分布式特性使其在规模、灵活性和隐蔽性方面远超传统的单点攻击方式,使得其成了亟须解决的核心威胁之一[12-13]。

从技术架构上看,僵尸网络通常包括三种主要组成部分:控制与指挥(C&C)服务器、僵尸主机以及攻击目标。C&C服务器是整个僵尸网络的中枢,负责向受控设备下达指令并接收执行结果;僵尸主机作为实际的攻击载体,在攻击者的控制下执行具体任务;而攻击目标通常是某个特定的网络系统、企业机构或个人用户。僵尸网络的运行依赖于高效的通信机制,域名解析在确保僵尸主机与控制服务器(C&C服务器)之间保持连接方面起着至关重要的作用[14]。

为了规避传统的检测与防御措施,现代僵尸网络逐渐从单一的C&C通信模式向更复杂的多层级通信模式转变。例如,采用点对点(P2P)通信架构能有效降低C&C服务器面临的集中化风险,提高僵尸网络的生存能力。此外,僵尸网络的多态性和模块化设计使其能够根据检测技术的变化快速演化,也为网络的检测与防御提出了更高的标准[15-16]。

僵尸网络的高隐蔽性和持续威胁特性对传统网络防护机制构成了巨大挑战(如图1所示)。特别是僵尸网络所采用的域名生成方式(如DGA),能够在极短时间内快速生成大量的动态域名,从而进一步加剧了网络防护的复杂性和难度。所以对僵尸网络的研究不仅需要从技术层面剖析其运行机制,还需在实际应用中探索有效的检测与防护策略,从而更好地对抗不断升级的网络攻击。

1.2 DGA的特点与生成机制

DGA的主要功能是使恶意软件能动态地创建众多域名,从而规避基于域名的检测和阻断拦截机制。通过DGA,攻击者可以在受感染主机和远程控制服务器之间建立通信链路,即使某些域名被封锁或注销,恶意软件仍然能够继续运作。DGA的主要特点、类型与主要算法如表1所示。

动态域名生成:DGA的关键特性在于其能够动态地产生域名。恶意软件在被感染的系统上,利用特定算法创造一系列看似无意义的域名。攻击者利用预设的算法来生成并操控域名,从而在攻击活动中保持通信的持续性。

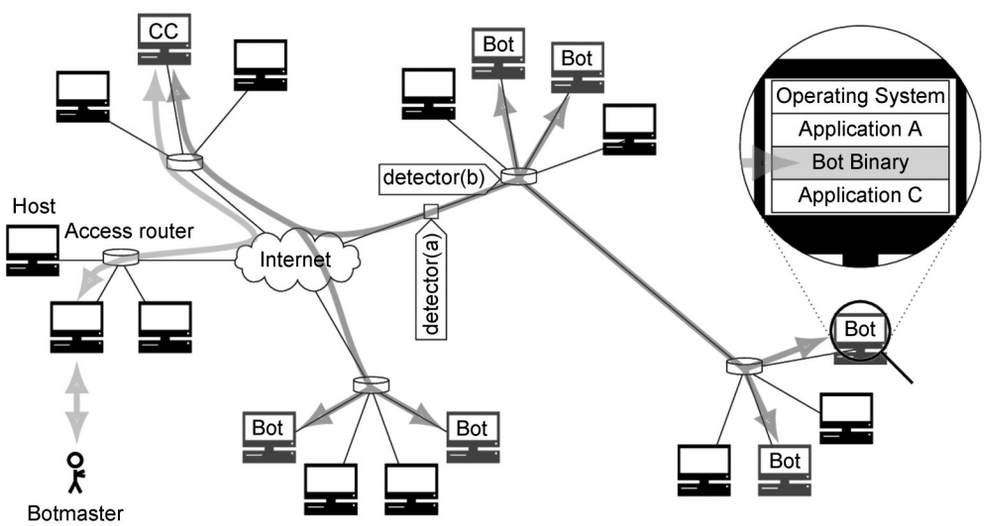

图1 僵尸网络示例[14]

Fig. 1 Example of botnet[14]

DGA生成的域名通常包含随机字符和无意义的组合,这使得它们难以被传统的黑名单防御机制识别。

表1 DGA的类型与生成机制

Table 1 Types and generation mechanisms of DGAs

DGA特点	DGA类型	DGA生成算法
动态生成	时间独立且确定性(TID)	算术型DGA
多样性	时间依赖且确定性(TDD)	哈希型DGA
适应性	时间依赖且非确定性(TDN)	单词表型DGA
难以追踪检测	时间独立且非确定性(TIN)	排列型DGA

多样性与适应性:DGA算法具有较强的适应性,能够根据时间、日期或其他外部因素调整生成的域名。例如,某些DGA会根据系统的时间戳生成域名,这使得每个感染设备生成的域名序列都可能不同,增加了检测的难度。DGA算法的多样性不仅能生成大量的域名,还能根据变化的环境保持对恶意服务器的访问。

防检测能力:由于DGA生成的域名具有较强的变异性,传统基于静态黑名单和规则的检测方式往往难以有效识别这些域名。即使一些域名被标记为恶意,新的、由相同算法生成的域名依旧能够继续用于恶意通信。这种特性使得DGA成为持续性攻击(如间谍软件、勒索软件和僵尸网络)中常用的技术。

Botmaster和Botnet之间通过共享相同的种子来“同步”生成域名。这些种子通常包括数值常量(如域名长度)或字符串(如字母表和顶级域名集合)。种子特性对DGA的生成过程有重要影响,主要体现在时间依赖性和确定性上[17]。

时间依赖性表明DGA使用时间源(如系统时间)来生成域名,因此这些域名在特定时间段内有效;确定性则意味着DGA的参数已知,从而可以预测生成的域名。部分DGA使用时间上的非确定性,例如恶意软件家族Schware和Bedep[18]采用欧盟中央银行每日发布的外汇汇率,Stone-Gross等[19]使用推特趋势作为种子。而Symantec报告中分析发现Jiripbot会提取一组系统属性[20],包括MAC地址和硬盘卷ID返回给攻击者。利用这些难以预测的数据来作为种子,增加了域名预测的难度。

从种子的时间性和确定性角度,DGA可分为四种类型:时间独立且确定性(TID)、时间依赖且确定性(TDD)、时间依赖且非确定性(TDN)和时间独立且非确定性(TIN)。这些特性决定了DGA的复杂度和防御难度。

从基于算法机制角度,Plohmann等[21]通过逆向工程,对43个基于DGA的恶意软件家族进行分析和扩展,将DGA分为四类:

算术型DGA:通过计算一系列值来生成域名。这些值可以直接转化为可用作域名名称的ASCII表示,或作为硬编码数组的索引来选取字母表中的字符。例如Conficker[22],这是一个典型的算术型DGA,它使用当前日期作为种子,每天生成50 000个域名,并分布在113个顶级域名(TLD)中。算术型DGA是最常见的类型之一,因其生成过程相对简单且计算高效。

哈希型DGA:利用哈希函数计算种子数据,并将其十六进制表示(hexdigest)用作域名的一部分。如Bamital[23]使用MD5哈希算法来生成域名,其同样是时间依赖的。Dyre[24]使用SHA256哈希生成域名,它还在生成的域名前加入一个随机前缀,增加了域名的伪装性。

单词表型DGA:通过从单词表中选取单词,并将选取的单词拼接成域名。单词表可以嵌入恶意软件中,或从公开资源获取。如Gozi[25]通过伪随机数生成器从公开的《美国独立宣言》中提取单词,并组合生成域名。其生成域名时可能截断单词,增加域名的随机性,例如amongpeaceknownlife.com或knownli.com。Suppobox[26]在恶意软件中嵌入了384个单词,随机选取两个单词进行组合以创建域名,并以“.net”作为其后缀,如brightfuture.net。

排列型DGA:从指定的初始域名出发,通过对域名组成部分进行多种排列组合,从而衍生出一系列潜在可用域名。以VolatileCedar[27]为例,其通过排列初始域名dotnetexplorer.net的二级部分生成域名,总计生成170个可能的域名。例如explorernetdot.net或dotexplorer.net。

综上总结DGA生成算法具体策略与特点如表2所示。

1.3 DGA在僵尸网络中的应用

在当代网络威胁格局中,僵尸网络的复杂性与隐蔽性日益增强,其中域名生成算法DGA

表2 DGA生成算法策略与特点

Table 2 Strategies and characteristics of generation algorithms of DAGs

DGA生成算法	算法策略	算法特点
算术型DGA	通过计算一系列值来生成域名	生成简单且计算高效
哈希型DGA	利用哈希函数计算种子数据	较高伪装性、防检测能力强
单词表型DGA	单词表中选取单词拼接成域名	通过截断单词增加随机性
排列型DGA	域名组成部分进行多种排列组合	通过排列组合生成衍生域名

扮演了关键角色。DGA通过动态生成域名,为僵尸网络的控制与指挥(C&C)通信提供了一种逃避静态分析和黑名单机制的手段。本文的主要目的是分析DGA在僵尸网络中的实际运用,并研究其对网络安全领域产生的具体影响。首先,DGA的核心价值在于其规避检测与追踪的能力。攻击者利用DGA生成的海量域名,大幅降低了单一域名被追踪或封禁的风险,确保僵尸网络即使在部分域名被识别的情况下,仍能通过其他域名维持与C&C服务器的通信。其次,DGA提高了僵尸网络的生存能力。由于DGA生成的域名具有动态更新的特性,僵尸网络能够在外部干扰或封禁措施下继续运作。这种动态性使得攻击者能够迅速切换C&C服务器,从而提升僵尸网络的鲁棒性。再者,DGA提升了僵尸网络的伪装效果。部分DGA生成的域名在语义或结构上与合法域名高度相似,模仿常见合法网站的格式,从而增加了网络安全设备和分析人员的检测难度。最后,DGA支持分布式通信。它为僵尸网络提供了分布式的域名生成机制,使得各僵尸主机能够独立生成域名从而与C&C服务器进行通信,降低了僵尸网络的集中化风险,增强了攻击的隐蔽性与灵活性。尽管DGA为僵尸网络提供了显著的优势,但其生成域名的规律和特征也为检测提供了潜在的切入点。研究人员通过分析DGA域名的统计特征、生成模式以及通信行为,已开发出更高效的检测算法。然而,面对DGA技术的持续演化,现有防御体系仍面临严峻挑战,亟须进一步优化以应对新型威胁[7,28-31]。

2 域名生成算法检测方法

2.1 基于统计分析的检测方法

基于统计分析的方法所利用的信息可分为两个部分。(1)只使用域名自身信息,如域名长度、字符频率、n-gram分布、KL距离、Jaccard系数;(2)配合使用域名附属信息,如DNS信息[恶意域名的生存时间(Time To Live,TTL)值往往较低、DGA域名通常有高比例的不存在的域名(Non-Existent Domain,NXDOMAIN)记录、IP地址分布等]、域名注册信息查询协议(WHOIS)信息(例如短期注册域名或频繁更换注册人信息的域名可能具有恶意特征、同一注册人名下的多个域名可能属于同一攻击者)、域名历史信息等。

Yadav等[32]通过使用距离分析DGA域名特性。其后续工作[33]通过建模成功域名与失败域名的时间相关性和信息熵检测DGA。Antonakakis等[34]使用聚类方法分析域名的长度、随机性水平和字符频率分布,并结合隐马尔可夫模型进行分类。Zhang等[35]分析域名的字符组成、词汇层次结构以检测DGA域名。Wang等[36]使用分词技术提取域名的词语特征,并结合字符数量和数字数量等特征进行检测。Grill等[37]则提出一种基于NetFlow流量分析的识别方案,通过深入挖掘DNS流量特征从而定位潜在的DGA域名。Zang等[38]使用IP、TTL地址分布、WHOIS信息和域名历史信息等网络特征进行检测。这些基于统计检测的方法通常具有较强的可解释性,在部分实际部署中表现突出。

2.2 基于机器学习的检测方法

机器学习模型通过接受人工传入的特征来实现更加可靠的分类(二分类仅识别正常/异常域名,而多分类要求识别具体的DGA模式,难度更大)。基于机器学习的方法和统计分析的方法之间的界限并不是泾渭分明的,因为机器学习也需要通过人工选择和处理的特征来进行检测。

2.2.1 支持向量机(SVM)算法

支持向量机(Support Vector Machine,SVM)[39]是一种常用的二分类算法,广泛应用

于DGA检测任务。SVM工作原理是通过寻找一个最优超平面,从而最大限度地划分开各类别的样本,完成分类任务[40]。给定训练集$\{(\boldsymbol{x}_i,y_i)\}$,其中$\boldsymbol{x}_i\in i^n$为特征向量,$y_i\in\{-1,1\}$为类别标签,SVM的目标是通过优化以下目标函数找到最优超平面:

$$\min\frac{1}{2}/\!/\boldsymbol{w}/\!/^2 \text{ subject to } y_i(w^{\mathrm{T}}x_i+b)\geqslant 1,\forall i \tag{1}$$

其中$\boldsymbol{w}$为法向量,b为偏置。Dahal等[41]利用自编码器(autoencoder)生成16位域名表示,然后使用SVM对域名进行分类。Davuth等[42]对他们收集的150万个域名字符串进行了统计分析,同时依据良性域名与恶意域名在统计特性上的不同,采用了双字母(Bi-gram)特征提取方法,即将字符串中相邻的两个字符视为一个单元进行特征抽取,之后利用支持向量机对这些双字母特征进行分类。在其测试集中删除与训练集相同的共同特征后,准确率(Accuracy,ACC)由92.81%提升至95.28%。实验结果表明,双字母特征结合SVM分类器显著提高了恶意域名识别的准确性。

2.2.2 树集成算法

树集成方法是数据科学家最常用的DGA算法之一,可以很好地扩展到大规模数据集,Bilge等[43]开发出的EXPOSURE系统提取了15个域名特征,同时利用J48决策树进行分类。Schüppen等[44]基于随机森林(Random Forest,RF)算法,从DNS流量中提取了包含7个语言特征、12个结构特征和2项统计性指标,用以对NXDomain类型的域名进行分类。Sivaguru等[45]训练了三种随机森林(B-RF、M-RF、OVA-RF)应用于DGA检测,主要通过提取域名的多种特征,如字符熵、n-gram中位数等,来训练模型来进行多分类。其在Cryptolocker-Flashback,dyre,locky等时间依赖的数据集和banjori,tinba,ramnit等时间不变的数据集上的结果显示,M-RF和OVA-RF的加权宏平均$F1$分数在0.94左右,而深度学习模型达到0.97以上。Nie等[46]提出了一种基于游戏理论的对抗性域名生成算法DGA检测方法,使用多级增量随机森林MIRF模型来提高检测的准确性和鲁棒性。通过交替运行对抗性DGA和增量域名检测器,MIRF模型能够有效识别并应对对抗性DGA生成的恶意域名,解决了传统检测方法在增量训练和灾难性遗忘方面的问题。尽管随机森林在检测时间依赖的DGA家族方面表现良好,但在面对时间不变的DGA家族时,其鲁棒性较差。此外,将这些模型应用于实际流量数据时,许多域名被错误地标记为恶意,这暴露了仅依赖标准白名单(数据集Alexa)进行训练的DGA检测系统的局限性。

2.2.3 聚类算法

聚类算法通过判别各个域名在空间中的分布情况来对其进行分类判别。Yadav等[32]聚焦于域名与IP的解析关系,通过二分图的连接分量分析实现聚类。其后续进一步加入了NXDomain流量的聚类分析[33]。

Zhou等[47]基于NXDomain流量,通过域名的二级域(2LD)或解析IP地址进行分组,并通过计算访问模式和活动时间分布的相似性来聚类。Schiavoni等[48]研发了Phoenix系统,该系统结合了域名字符串特征和IP地址特征,并依据基于密度的空间聚类算法(Density-based Spatial Clustering of Applications with Noise,DBSCAN)聚类算法的结果来做出判断。Antonakakis等[49]提出了Pleiades,该算法分为两个模块:DGA发现模块和DGA分类和C&C检测模块(如图2所示)。DGA发现模块通过分析DNS查询失败的响应,使用字符串特征和主机查询重叠度进行聚类,准确发现新的DGA并构建新模型,而DGA分类和C&C检测模块则通过多类分类器和隐马尔可夫模型对新发现的域名进行分类和识别,提高了C&C域名的识别精度并减少误报。基于聚类的DGA检测属于“回溯检测模式”,即只能离线检测,这意味着检测存在时间延迟。而相比其他监督方法的“实时检测模式”,聚类算法的优点是无监督且可处理大批量数据。

2.3 基于深度学习的DGA检测方法

深度学习方法利用神经网络模型对域名进行端到端的学习,自动提取有效特征。并针对不同域名设计不同的特征提取方法,实现了对不同长度DGA域名的有效检测[50]。相较于传

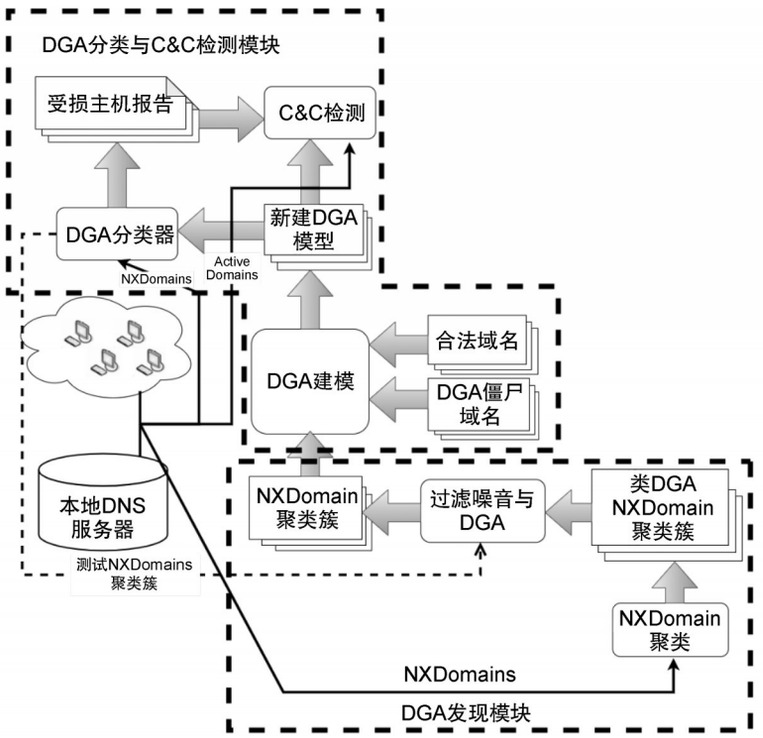

图2 Pleiades方法检测DGA[17]

Fig. 2 Pleiades method for detecting DGA[17]

统机器学习方法,深度学习模型具备处理更高复杂度的域名模式,尤其是在面对变种复杂的DGA时,具有更强的适应性。

2.3.1 卷积神经网络(CNN)

卷积神经网络(Convolutional Neural Network,CNN)通过滑动窗口操作提取域名中的局部特征,在DGA域名的识别中表现出色。CNN的关键在于通过卷积层和池化层的层叠结构,捕获域名中的重要模式。卷积操作如下:

$$z_{i,j}=\sum_{m,n} w_{m,n}x_{i+m,j+n}+b, \qquad (2)$$

其中 $w_{m,n}$ 为卷积核,$x_{i,j}$ 为输入数据,b 为偏置项。CNN+LSTM(Long Short-term Memory)的混合范式被广泛使用来检测DGA:Yu等[51]研究了CNN和LSTM架构在检测DGA域名中的性能。这些模型均在字符级操作,仅使用域名字符串作为输入,无需上下文信息。文献[52-55]同样采用了类似的组合架构来检测DGA。Aravena等[56]结合词嵌入和CNN来捕捉语义关系。Liang等[50]结合了卷积神经网络在特征提取方面和n-gram模型在语义表征方面的优势,提出了一种新颖的基于n-gram的组合特征域名分类模型HDGAetector(如图3所示)。其在DGArchive和Net-lab360数据集上构建了基于长度的平衡数据集,研究发现指标受样品长度的影响较小,在超短数据集DS_{3_6}、中等长度数据集DS_{7_10}和超长数据集DS_{21_63}上的$F1$分数达到了91.64%、94.44%、98.76%。

2.3.2 词向量(Word2Vec)

Word2Vec[57]是一种神经网络模型,用于生成词向量嵌入,它通过学习单词的分布式表征来揭示和捕捉词汇之间的语义关联,通常用于文本分类[58]、情感分析[59]等。Word2Vec模型主要有两种架构:连续词袋模型(Continuous Bag-of-Words,CBOW)和跳跃模型(Skip-gram)。Koh等[60]提出了一种方法,结合预训练的上下文敏感词嵌入模型ELMo和一个简单的全连接分类器,基于词级信息对域名进行分类。Aravena等[56]采用词向量模型(Word2Vec)技术来生成域名的词嵌入来捕捉域名中字符的语义关系。通过将这些嵌入作为输入特征,提出的DeepD2V方法采用了深度学习模型,利用CNN技术以实现DGA域名的识别与分类。通过25-DGA数据集上的实验评估,证明了DeepD2V显著优于当前基于浅学习和词典分析

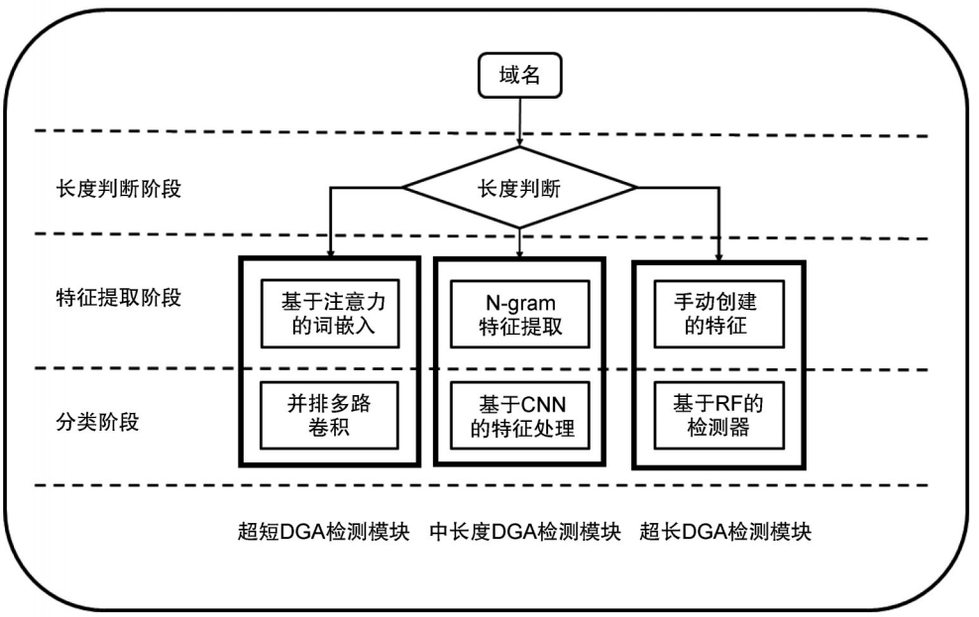

图3 HDGAetector模型的体系结构[23]

Fig. 3 Architecture of HDGAetector model[23]

的DGA检测和分析方法,实现了97%以上的准确率和召回率。

2.3.3 循环神经网络(RNN)

循环神经网络(Recurrent Neural Network,RNN)[61]因其在处理序列数据方面的优异表现,在DGA检测领域得到了广泛应用,(如图4所示)。特别是通过引入记忆单元和门控机制长短期记忆网络(LSTM),有效提升了对域名中长期依赖关系的捕捉能力。Woodbridge等[62]率先提出基于LSTM的DGA检测模型,成功利用域名的时序特征进行检测。随后,Tran等[63]在此基础上开发了LSTM.MI,通过成本敏感学习方法有效解决了多分类任务中的类别不平衡问题,显著提升了检测性能。后续研究进一步探索了不同RNN变体的应用。Shahzad等[64]对GRU、LSTM和双向LSTM(BiLSTM)在DGA检测中的性能进行了对比,并在Alexa Top 1M、OSIN、Cisco Umbrella以及Netlab 360提供的DGA域名数据集上进行了测试,发现各架构在性能上差异不大,平均ACC约为87%,真阳率(True Positive Rate,TPR)为81%,曲线下方面积(Area Under Curve,AUC)为0.98。Namgung等[65]将BiLSTM与CNN结合,通过多模态特征融合,进一步提升了检测准确率。

近年来,注意力机制的引入为RNN模型赋予了更强的特征提取能力。Chen等[66]在LSTM模型中集成注意力机制,因此在词嵌入过程中模型能够集中于更具判别力的特征,显

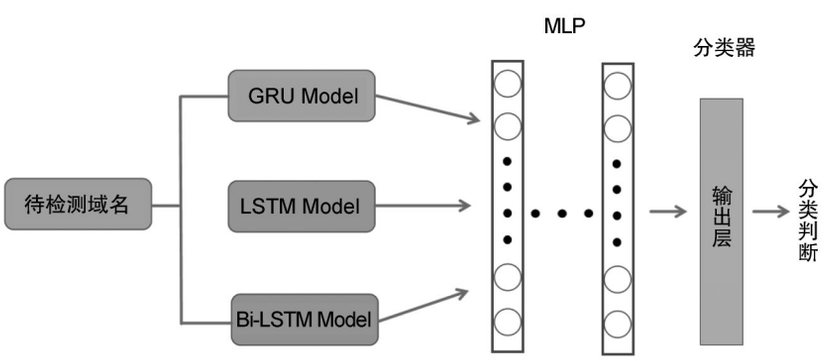

图4 循环神经网络判别DGA[7]

Fig. 4 Discriminate DGA with recurrent neural network[7]

著提升了检测效果。此外,集成多种深度学习模型的方法也逐渐兴起,如郎波等[67]利用图卷积网络(Graph Convolutional Network,GCN)、BiLSTM和多层感知机(Multilayer Perceptron,MLP)模块的特征融合,大幅提升了检测效果。

2.3.4 其他深度模型

Gao等[68]提出了一种基于深度信念网络(Deep Belief Network,DBN)的网络入侵检测模型,使用KDD CUP 1999数据集中的特征进行三阶段训练。Anderson等[69]从不同角度制定了对抗性生成网络(Generative Adversarial Network,GAN)的方法,用于生成对抗性DGA域名,依照这种方法尝试去欺骗分类器。结果表明,该方法成功达成目标。随后,将GAN生成的域名添加到训练集中,改进了DGA检测性能。

Zhai[70]等提出了一种基于生成对抗网络(GAN)的可控域名生成算法,通过Wasserstein GAN(WGAN)生成域名,确保生成的域名具有强大的反检测能力。该方法利用自然语言处理技术控制生成的域名符合域名规则且无重复,通过时间依赖的种子动态生成域名,增强了域名生成算法的隐蔽性和有效性。实验结果表明,可控域名生成算法(Controllable Domain Generation Algorithm,CDGA)在反检测能力、重复率和冲突率方面均优于现有的其他DGA算法。

Tuan等[71]提出的基于LSTM和注意力层的深度学习模型,首先将域名转换为字符序列并进行编码处理,然后利用LSTM网络学习域名中的时间序列特征。在此基础上,应用注意力机制识别域名中的关键字符或子域名,进一步提高分类能力。模型在区分恶意域名和正常域名识别恶意域名所属的DGA家族均表现出色,尤其在AADR数据集上,模型分类识别的准确率达到很好的结果。

Hu等[72]基于Siamese网络的DGA检测方法,通过对比学习和Siamese网络框架,利用有限的训练样本来提取域名字符串中字符的隐含关系信息,然后基于提取的神经特征向量训练机器学习分类器来识别恶意域名。实验结果表明,DGAD-SN在小规模DGA家族和新兴DGA变种检测中的准确性和鲁棒性优于现有方法。

基于深度学习方法可以自动学习数据中的复杂模式,减少人工特征设计的依赖,其对于复杂的DGA和未知的生成算法具有较强的适应能力。然而基于深度学习方法训练过程需要大量的计算资源,尤其是在大规模数据集上,模型复杂度高,可解释性较差。而且对训练数据质量要求较高,低质量的数据可能影响模型的泛化能力。

2.4 基于区块链的DGA检测方法

Gao等[73]利用区块链构建可信的数据交换环境,将DNS解析流量数据上传至区块链网络,借助其分布式账本特性防止数据被恶意篡改,确保数据的真实性与完整性,同时实现各节点间的安全数据共享与协作;运用区块链维护可信的黑白名单,及时更新并管理黑名单和白名单,新检测到的DGA域名可快速更新至区块链黑名单中,且由于区块链的共识机制,各节点能同步获取最新名单,确保检测的及时性和准确性,同时有效防止名单被篡改。

3 DGA检测技术潜在瓶颈

3.1 DGA的演化与检测难度

随着攻击者在生成域名方面的技术不断进步,DGA检测面临着越来越复杂的挑战。最初,DGA的生成算法多为简单的字符随机化或基于字典的生成方式,这些方法生成的域名通常具有较为显著的统计特征,如高熵值和无意义的字符组合。因此,基于统计分析或简单规则的检测方法可以有效识别此类域名。

然而,随着技术的发展,攻击者开始采用更加复杂的生成算法,这些算法能够模仿正常域名的特征,甚至加入一定的语义规则,从而降低了DGA与正常域名之间的可区分性。例如,近年来出现了基于Markov链、LSTM(长短期记忆网络)等生成方法,这些方法通过模拟自然语言的字符序列,提高了DGA的语言特性和规律性,减少了其随机性[74]。因此,传统的依赖于统计特征的方法,特别是依赖于熵值和字符频率的检测手段,已经难以适应当前的检测需求。

此外,攻击者还通过不断更新和变种生成算法,使得DGA的生成方式多样化并具有较高

的适应性。例如,通过动态调整生成规则、混合不同生成策略,以及引入加密或变种机制,使得DGA能够躲避现有检测算法[70,74-75]。这种演化导致了DGA的特征不再稳定,使得检测系统在面对不断变化的生成算法时,容易出现误报或漏报。因此,DGA检测技术必须不断迭代,以应对日益复杂的生成模式和攻击手段。

3.2 实时性与计算开销的权衡

在大规模网络环境下,DGA的检测不仅要求高准确性,还必须具备足够的实时性。DGA生成机制的变化速度和网络流量的膨胀,使得实时检测成为一项巨大的挑战。现有的DGA检测方法,尤其是基于机器学习和深度学习的模型,通常需要在海量数据中快速提取和分析特征,判断域名是否为DGA。对于基于统计特征的方法,虽然计算复杂度较低,但当域名数量庞大时,特征计算仍然需要大量时间和资源。尤其是在处理跨区域的网络流量时,延迟可能影响检测的实时性。基于机器学习的方法通过特征提取和模型训练,通常需要较长的计算时间,尤其是当涉及复杂的多维度特征时,训练和推理过程的计算成本剧增。深度学习模型,特别是CNN和RNN等,尽管能给出相当准确的结果,但其训练和推理阶段的计算开销极高,尤其是在大规模数据集上应用时,模型推理可能需要使用专门的硬件加速器(如GPU),这进一步加大了成本和实时处理的难度。此外,深度学习模型的存储需求也较为庞大,尤其是在模型训练过程中,需要大量的训练数据和高效的存储设备,以便存储训练过程中的中间结果和优化参数。因此,如何在保证准确性的同时降低计算开销、提高实时性,成为DGA检测中的核心问题。

3.3 假阳性与假阴性现象

在DGA检测中,假阳性(False Positive)和假阴性(False Negative)问题严重影响检测系统的有效性和可靠性。假阳性指的是正常域名被误判为DGA,而假阴性则是DGA未能被检测出来,仍然被误判为正常域名。这两类误判不仅降低了检测系统的准确性,还可能导致安全风险和运维成本的增加。假阳性问题常见于统计特征相似的域名,尤其是当DGA采用更为复杂的生成机制,模仿正常域名时。例如,使用基于词典或预定义规则生成的DGA往往具有与正常域名相似的字符组合或语义结构,这使得基于统计特征的检测方法容易将其误判为正常域名。这种误判会导致不必要的警报产生,迫使网络管理员频繁核查,浪费时间和资源。在大规模网络环境中,假阳性的积累可能会淹没真正的安全事件,从而影响检测系统的实际效果。假阴性问题则更加严重,因为它意味着恶意DGA域名未能被及时发现,攻击者可能利用这些域名进行网络钓鱼、恶意软件传播或其他类型的攻击。例如,某些DGA域名生成算法可能通过对字典域名的扰动、加密或使用特定的字符混排,来规避现有检测系统的识别。这类DGA的隐蔽性使得现有的检测方法难以完全识别,导致假阴性的发生。假阴性的存在直接威胁到网络的安全性,因为它使得恶意活动得以在网络中悄然进行,造成数据泄露、系统入侵等严重后果[76]。

4 DGA检测技术路线与对抗防御策略设计

4.1 DGA检测技术的设计

4.1.1 新兴检测技术的应用

深度学习,尤其是CNN和Transformer模型等在DGA检测中的应用,已显示出较为显著的优势。与传统机器学习方法相比,深度学习无须手动提取特征,能够自动学习到数据的深层次特征,尤其在面对多样化、复杂的DGA生成模式时,能够实现较高的检测精度[31,77]。然而,深度学习模型在训练时往往需要大量的标注数据以及高性能计算资源,这也成为其推广应用中的一大挑战。

图神经网络(GNN)作为一种新兴的图数据处理方法,近年来逐渐被应用于网络安全领域。由于DGA生成的域名常常存在一定的结构性或关系性,GNN能够通过学习域名之间的关联性,发现潜在的生成模式。GNN的图结构学习特性使其能够处理DGA域名生成过程中潜在的图状依赖关系,为DGA检测提供了新的视角。

迁移学习(Transfer Learning)作为一种通过借用源领域知识来加速目标领域学习的技术,

也可被应用于DGA检测中。在DGA检测任务中,迁移学习能够有效利用已有的域名数据集进行预训练,缩短模型的训练时间并提高检测效果。这在面对数据量不足、标注困难的情况下,尤其具有优势。此外,大语言模型也有望进一步提升DGA检测的性能和灵活性,推动DGA检测从传统的规则匹配向智能化、自动化转变[78]。

4.1.2 跨领域协同检测方法

单一的检测技术往往难以应对复杂的DGA攻击场景,尤其是面对新的生成算法和复杂的攻击模式时。因此,跨领域协同检测方法将成为未来DGA检测研究的重要发展方向。跨领域协同检测旨在通过多种技术手段的结合,综合利用网络流量分析、行为检测、语义分析等多维度信息,以提高DGA检测的准确性和鲁棒性。

具体来说,跨领域协同检测方法将结合传统的基于统计特征的检测、机器学习、深度学习等技术,与基于网络流量、DNS请求模式、主机行为分析等信息源相结合。例如,基于网络流量的检测方法通过分析域名解析请求的频率、分布模式和时序特征,可以辅助传统检测方法发现异常行为。结合DNS流量的模式识别,可以揭示出潜在的恶意DGA域名,而这些信息在单一的特征检测中难以捕捉到。

此外,行为分析技术也能够通过检测域名解析请求背后的网络行为特征,为DGA检测提供支持。例如,恶意DGA域名通常会伴随异常的访问模式或高频率的请求,这些行为特征能够与其他方法的结果相结合,为最终决策提供更为全面的支持。通过融合多个领域的数据和方法,跨领域协同检测能够提高检测系统的容错性,减少误报和漏报,从而提升了系统在错综复杂的环境下的适应能力。

4.2 新型DGA攻击的对抗防御策略设计

目前DGA被广泛应用于恶意软件中,用于生成随机化的域名,以躲避传统的基于静态黑名单的防护机制。针对这一威胁,本文提出了两大类有效的对抗防御策略:基于流量行为分析的检测与响应策略和基于域名生成规律的阻断策略。

4.2.1 基于流量行为分析的检测与响应策略

流量行为分析是识别DGA攻击的一种关键防御手段,尤其在不依赖于域名解析的异常检测机制的情况下。DGA域名通常具有以下特点:首先,生成的域名包含随机字符,且与正常域名结构差异较大;其次,恶意程序会定期更换控制域名,导致频繁的域名请求和连接。基于这些特点,安全防御系统可以通过以下几种方式对DGA行为进行识别和响应。

流量模式分析:通过对网络流量进行深度分析,识别出异常的请求模式。例如,若某一IP地址或网络节点频繁向不同的域名发送请求,且域名请求没有明显的地理位置或时域规律,则可能是DGA攻击的表现。此外,若DNS请求在短时间内聚集在某一时段或高频次地请求新生成的域名,这也可能是DGA行为的指示。

DNS请求异常检测:虽然不涉及域名解析的异常检测,但仍可以对DNS请求进行其他类型的监控。例如,可以监测某些特定IP发送的大量DNS请求,并结合流量的分布特征,判断是否存在DGA攻击。若某一时间窗口内,有大量请求指向不常见的域名,且这些域名的生成时间规律性强,则可能是DGA攻击信号。

反应与封锁:一旦检测到潜在的DGA攻击,防御系统可以通过临时封锁可疑的域名或IP地址,防止恶意流量的进一步传播,同时向安全响应团队发出警报,便于及时采取应对措施。

4.2.2 基于域名生成规律的阻断策略

与基于流量的分析不同,另一类对抗策略侧重于识别DGA域名的生成规律,进而阻断恶意流量。DGA域名的生成通常遵循一定的算法或模式,攻击者虽然可以频繁更换域名,但这些生成的域名依然存在一些共同的特征。通过逆向分析恶意程序的DGA算法,可以构建如下对抗策略。

规则库与算法映射:通过对已知DGA类型的逆向分析,提取生成域名的算法特征,建立对应的规则库。一旦检测到新生成的域名符合某些已知的算法特征,可以迅速判断该域名为恶意域名,并进行阻断。

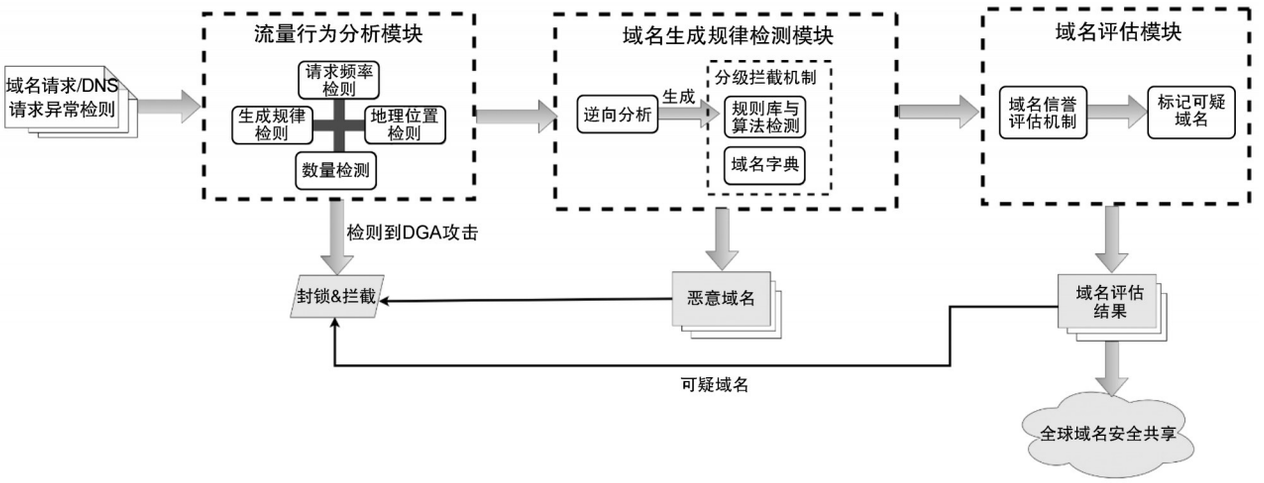

图5 多层次防御体系图

Fig. 5 Diagram of the multi-layered defense system

分级拦截机制:结合DGA生成算法的已知规律,构建基于域名字典和算法预测的分级拦截机制。对于某些常见的DGA算法,可以实现快速匹配和拦截;而对于较为复杂或未知的DGA,防御系统可以采用动态生成和实时分析的方式进行识别和阻断。

域名信誉评估:采用域名信誉评估机制,评估新生成的域名是否为恶意域名。对于高度怀疑的域名,可以立即阻断或标记,防止其对系统造成进一步威胁。同时,评估结果可以与全球域名安全共享平台进行对接,以实现跨域名系统的实时防护。

综上所述,针对新型DGA攻击,防御策略应当结合流量行为分析与基于生成规律的域名拦截机制,形成多层次、综合性的防御体系如图5所示,以提高对DGA攻击的防护效果。

5 结论

本文系统评估了当前主流的DGA检测技术,包括基于统计特征、机器学习和深度学习的方法,探讨了不同方法的优势与局限性。统计特征方法解释性强,但难以应对复杂DGA生成模式;机器学习模型依赖人工特征设计,存在泛化性和实时性瓶颈;深度学习能够捕捉复杂域名模式,但其高计算开销与低可解释性限制了实际部署。此外,现有技术普遍面临高误报率、数据稀缺性以及对新型DGA的适应性差等问题。为应对这些挑战,本文提出了几种优化策略:首先,通过深度学习模型优化(如注意力机制与多模态融合)提升性能;其次,结合跨域协同检测(流量行为分析与生成规律挖掘)增强系统鲁棒性;再次,采用多层次防御策略(动态拦截与信誉评估机制)提高检测能力。未来研究可探索轻量化深度学习架构与边缘计算结合、利用迁移学习和联邦学习缓解数据孤岛问题、结合大语言模型与GAN提升对未知DGA的预测能力,并推动跨机构、跨领域的威胁情报共享,促进主动防御。通过技术与机制的协同创新,提供更有效的DGA攻防对抗方案。

参考文献:

[1] XU X L, ZHOU Y L, LI Q S. Domain Algorithmically Generated Botnet Detection and Analysis[C]//International Conference on Security and Privacy in Communication Networks. Cham: Springer International Publishing, 2015: 530-534. DOI: 10.1007/978-3-319-23829-6_38.

[2] 张维维, 龚俭, 刘茜, 等. 基于词素特征的轻量级域名检测算法[J]. 软件学报, 2016, **27**(9): 2348-2364. DOI: 10.13328/j.cnki.jos.004913.
ZHANG W W, GONG J, LIU Q, *et al*. Lightweight Domain Name Detection Algorithm Based on Morpheme Features[J]. *J Softw*, 2016, **27**(9): 2348-2364. DOI: 10.13328/j.cnki.jos.004913.

[3] 王宇, 王祖朝, 潘瑞. 基于字符特征的DGA域名检测方法研究综述[J]. 计算机科学, 2023, **50**(8): 251-259. DOI: 10.11896/jsjkx.220700277.
WANG Y, WANG Z C, PAN R. Survey of DGA Domain

Name Detection Based on Character Feature[J]. *Comput Sci*, 2023, **50**(8): 251−259. DOI: 10.11896/jsjkx.220700277.

[4] 汪绪先, 黄缙华, 翟优, 等. 域名生成算法检测技术综述[J]. 计算机科学, 2024, **51**(8): 371−378. DOI: 10.11896/jsjkx.230700189.
WANG X X, HUANG J H, ZHAI Y, *et al*. Survey of Detection Techniques for Domain Generation Algorithm [J]. *Comput Sci*, 2024, **51**(8): 371−378. DOI: 10.11896/jsjkx.230700189.

[5] SAEED A M H, WANG D H, ALNEDHARI H A M, *et al*. A Survey of Machine Learning and Deep Learning Based DGA Detection Techniques[M]//Smart Computing and Communication. Cham: Springer International Publishing, 2022: 133−143. DOI: 10.1007/978-3-030-97774-0_12.

[6] CHEN Y J, PANG B, SHAO G L, *et al*. DGA-based Botnet Detection Toward Imbalanced Multiclass Learning [J]. *Tsinghua Sci Technol*, 2021, **26**(4): 387−402. DOI: 10.26599/TST.2020.9010021.

[7] NIE L H, SHAN X Y, ZHAO L P, *et al*. PKDGA: A Partial Knowledge-based Domain Generation Algorithm for Botnets[J]. *IEEE Trans Inf Forensics Secur*, 2023, **18**: 4854−4869. DOI:10.1109/TIFS.2023.3298229.

[8] ALQAHTANI H, KUMAR G. Advances in Artificial Intelligence for Detecting Algorithmically Generated Domains: Current Trends and Future Prospects[J]. *Eng Appl Artif Intell*, 2024, **138**: 109410. DOI:10.1016/j.engappai.2024.109410.

[9] ALAEIYAN M, PARSA S, VINOD P, *et al*. Detection of Algorithmically-generated Domains: An Adversarial Machine Learning Approach[J]. *Comput Commun*, 2020, **160**: 661−673. DOI:10.1016/j.comcom.2020.04.033.

[10] XIONG W, JIANG H Y, GUAN H T, *et al*. DSQNet: Domain SeQuence Based Deep Neural Network for AGDs Detection[C]//2021 IEEE Symposium on Computers and Communications (ISCC). New York: IEEE, 2021: 1−7. DOI:10.1109/ISCC53001.2021.9631503.

[11] DING L, LI L J, HAN J H, *et al*. Detecting Domain Generation Algorithms with Bi-LSTM[J]. *Comput Mater Continua*, 2019, **61**(3): 1285−1304. DOI: 10.32604/cmc.2019.06160.

[12] AMINI P, ARAGHIZADEH M A, AZMI R. A Survey on Botnet: Classification, Detection and Defense [C]//2015 International Electronics Symposium (IES). New York: IEEE, 2015: 233−238. DOI: 10.1109/ELECSYM.2015.7380847.

[13] MAHMOUD M, NIR M, MATRAWY A. A Survey on Botnet Architectures, Detection and Defences[J]. *Int J Netw Secur*, 2014, **17**(3): 272−289.

[14] VORMAYR G, ZSEBY T, FABINI J. Botnet Communication Patterns[J]. *IEEE Commun Surv Tutor*, 2017, **19**(4): 2768−2796. DOI:10.1109/COMST.2017.2749442.

[15] HAMMOODI HASAN KABLA A, ANBAR M, MANICKAM S, *et al*. Monitoring Peer-to-peer Botnets: Requirements, Challenges, and Future Works[J]. *Comput Mater Continua*, 2023, **75**(2): 3375−3398. DOI: 10.32604/cmc.2023.036587.

[16] GAO H Y, LI L X, LEI H, *et al*. One IOTA of Countless Legions: A Next-generation Botnet Premises Design Substrated on Blockchain and Internet of Things[J]. *IEEE Internet Things J*, 2024, **11**(5): 9107−9126. DOI: 10.1109/JIOT.2023.3322716.

[17] BARABOSCH T, WICHMANN A, LEDER F, *et al*. Automatic Extraction of Domain Name Generation Algorithms From Current Malware[C]//Proc. NATO Symposium IST−111 on Information Assurance and Cyber Defense. Koblenz, Germany: NATO STO, 2012.

[18] SCHWARZ D, BEDEP'S D G A. Trading Foreign Exchange for Malware Domains, 2015[EB/OL]. https://asert. arbornetworks. com/bedeps−dgatrading−foreign−exchange−for−malware−domains.

[19] STONE-GROSS B, COVA M, CAVALLARO L, *et al*. Your Botnet Is My Botnet: Analysis of a Botnet Takeover [C]//Proceedings of the 16th ACM Conference on Computer and Communications Security. New York: ACM, 2009: 1635−647. DOI:10.1145/1653662.1653738.

[20] SECURITY RESPONSE. Butterfly: Corporate Spies out for Financial Gain. Tech. rep[R]. Tempe, A2, USA: Symantec, 2015.

[21] PLOHMANN D, YAKDAN K, KLATT M, *et al*. A Comprehensive Measurement Study of Domain Generating Malware[C]//25th USENIX Security Symposium (USENIX Security 16). Austin, TX, USA: USENIX Association, 2016: 263−278. DOI: 10.5555/3241094.

[22] LEDER F, WERNER T. Know Your Enemy: Containing Conficker[R]. Germany: University of Bonn, 2009.

[23] KRYSIUK P, THAKUR V. Trojan.Bamital[R]. California: Symantec, 2013. https://docs. broadcom. com/doc/trojan-bamital-13-en.

[24] Chasing Cybercrime: Network Insights of Dyre and Dridex Trojan bankers[R]. Barcelona, Spain: Blueliv, 2015.

[25] 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): 110. DOI: 10.1007/s42979-021-00507-w.

[26] ALEXA. Top Sites on the Web[EB/OL]. (2015)[2025-03-29]. http://www.alexa.com/topsites.

[27] BAUMGARTNER K, RAIU C. Sinkholing Volatile Cedar DGA Infrastructure[EB/OL]. (2015)[2025-04-10]. https:urelist.com/blog/research/69421/sinkholingvolatile-cedar-dga-infrastructure/.

[28] VISHVAKARMA D K, BHATIA A, RIHA Z. Detection of Algorithmically Generated Domain Names in Botnets [M]//Advanced Information Networking and Applications. Cham: Springer International Publishing, 2019: 1279-1290. DOI:10.1007/978-3-030-15032-7_107.

[29] KUMAR V, KUMAR S, GUPTA A K. Real-time Detection of Botnet Behavior in Cloud Using Domain Generation Algorithm[C]//Proceedings of the International Conference on Advances in Information Communication Technology & Computing - AICTC '16. New York: ACM, 2016: 1-3. DOI:10.1145/2979779.2979848.

[30] SAROJINI S, ASHA S. Detection for Domain Generation Algorithm (DGA) Domain Botnet Based on Neural Network with Multi-head Self-attention Mechanisms [J]. *Int J Syst Assur Eng Manag*, 2022: 1-16. DOI: 10.1007/s13198-022-01713-2.

[31] ZANG X D, CAO J B, ZHANG X C, *et al*. BotDetector: a System for Identifying DGA-based Botnet with CNN-LSTM[J]. *Telecommun Syst*, 2024, **85**(2): 207-223. DOI:10.1007/s11235-023-01073-7.

[32] YADAV S, REDDY A K K, NARASIMHA REDDY A L, *et al*. Detecting Algorithmically Generated Malicious Domain Names[C]//Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement. New York: ACM, 2010: 10.1145/1879141.1879148. DOI: 10.1145/1879141.1879148.

[33] YADAV S, REDDY A K K, NARASIMHA REDDY A L, *et al*. Detecting Algorithmically Generated Domain-flux Attacks with DNS Traffic Analysis[J]. *IEEE/ACM Trans Netw*, 2012, **20**(5): 1663-1677. DOI: 10.1109/TNET.2012.2184552.

[34] ANTONAKAKIS M, PERDISCI R, DAGON D, *et al*. Building a Dynamic Reputation System for DNS[J]. *Proc 19th USENIX Secur Symp*, 2010: 273-289.

[35] ZHANG Y, ZHANG Y Z, XIAO J. Detecting the DGA-based Malicious Domain Names[M]//Trustworthy Computing and Services. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014: 130-137. DOI: 10.1007/978-3-662-43908-1_17.

[36] WANG W, SHIRLEY K. Breaking Bad: Detecting Malicious Domains Using Word Segmentation[EB/OL]. (2015-06-12)[2025-04-10]. https://arxiv.org/abs/1506.04111.

[37] GRILL M, NIKOLAEV I, VALEROS V, *et al*. Detecting DGA Malware Using Net Flow[C]//2015 IFIP/IEEE International Symposium on Integrated Network Management (IM). New York: IEEE, 2015: 1304-1309. DOI:10.1109/INM.2015.7140486.

[38] ZANG X, GONG J, HU X. Detecting Malicious Domain Name Based on AGD[J]. *Journal on Communications*, 2018, **39**(7): 15-25. DOI: 10.11959/j. issn. 1000-436x.2018116.

[39] CORTES C, VAPNIK V. Support-vector Networks[J]. *Mach Learn*, 1995, **20**(3): 273-297. DOI: 10.1007/BF00994018.

[40] SCHÖLKOPF B, SMOLA A J. Learning with kernels: support vector machines, regularization, optimization, and beyond[M]. Cambridge, Mass.: MIT Press, 2002.

[41] DAHAL B, KIM Y. AutoEncoded Domains with Mean Activation for DGA Botnet Detection[C]//2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3). New York: IEEE, 2019: 208-212. DOI:10.1109/icgs3.2019.8688037.

[42] DAVUTH N, KIM S R. Classification of Malicious Domain Names Using Support Vector Machine and Bigram Method[J]. *International Journal of Security and Its Applications*, 2013,**7**(1): 51-58.

[43] BILGE L, KIRDA E, KRUEGEL C, *et al*. EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis[C]//Ndss. San Diego, USA: The Internet Society. 2011: 1-17.

[44] SCHÜPPEN S, TEUBERT D, HERRMANN P, *et al*. FANCI: Feature-based Automated NXDomain Classification and Intelligence[C]//USENIX. Baltimore, MD, USA: USENIX Association. 2018: 1165-1181. DOI: 10.5555/3277203.3277290.

[45] SIVAGURU R, CHOUDHARY C, YU B, *et al*. An Evaluation of DGA Classifiers[C]//2018 IEEE International Conference on Big Data (Big Data). New York: IEEE, 2018: 5058-5067. DOI:10.1109/BigData.2018.8621875.

[46] NIE L H, ZHAO L P, LI K Q, *et al*. A Game-based Adversarial DGA Detection Scheme Using Multi-level Incremental Random Forest[J]. *IEEE Trans Netw Sci Eng*, 2023, **11**(1): 779-792. DOI:10.1109/TNSE.2023.3308126.

[47] ZHOU Y, LI Q, MIAO Q, *et al*. DGA-Based Botnet Detection Using DNS Traffic[J]. *Journal of Internet Services and Information Security*, 2013, **3**(3/4): 116-123. DOI:10.22667/JISIS.2013.11.31.116.

[48] SCHIAVONI S, MAGGI F, CAVALLARO L, *et al*. Phoenix: DGA-based Botnet Tracking and Intelligence [M]//Detection of Intrusions and Malware, and Vulner-

ability Assessment. Cham: Springer International Publishing, 2014: 192−211. DOI:10.1007/978-3-319-08509-8_11.

[49] ANTONAKAKIS M, PERDISCI R, NADJI Y, *et al*. From Throw-away Traffic to Bots: Detecting the Rise of DGA-based Malware[C]//21st USENIX Security Symposium (USENIX Security 12). Bellevue, WA, USA: USENIX Association. 2012: 491−506.

[50] LIANG J B, CHEN S H, WEI Z L, *et al*. HAGDetector: Heterogeneous DGA Domain Name Detection Model [J]. *Comput Secur*, 2022, **120**: 102803. DOI: 10.1016/j.cose.2022.102803.

[51] YU B, GRAY D L, PAN J, *et al*. Inline DGA Detection with Deep Networks[C]//2017 IEEE International Conference on Data Mining Workshops (ICDMW). New York: IEEE, 2017: 683−692. DOI:10.1109/ICDMW.2017.96.

[52] 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). New York: IEEE, 2018: 1−8. DOI:10.1109/IJCNN.2018.8489147.

[53] CHEN G B, YE D H, XING Z C, *et al*. Ensemble Application of Convolutional and Recurrent Neural Networks for Multi-label Text Categorization[C]//2017 International Joint Conference on Neural Networks (IJCNN). New York: IEEE, 2017: 2377−2383. DOI: 10.1109/IJCNN.2017.7966144.

[54] KIM Y, JERNITE Y, SONTAG D, *et al*. Character-aware Neural Language Models[J]. *Proc AAAI Conf Artif Intell*, 2016, **30**(1): 2714−2749. DOI: 10.1609/aaai.v30i1.10362

[55] MOHAN V S, R V, KP S, *et al*. S. P. O. O. F Net: Syntactic Patterns for Identification of Ominous Online Factors[C]//2018 IEEE Security and Privacy Workshops (SPW). New York: IEEE, 2018: 258−263. DOI:10.1109/SPW.2018.00041.

[56] ARAVENA L T, CASAS P, BUSTOS-JIMÉNEZ J, *et al*. DeepD2V - Deep Learning and Domain Word Embeddings for DGA Based Malware Detection[C]//2024 IEEE International Conference on Machine Learning for Communication and Networking (ICMLCN). New York: IEEE, 2024: 164−170. DOI: 10.1109/ICMLCN59089.2024.10624693.

[57] MIKOLOV T, CHEN K, CORRADO G, *et al*. Efficient Estimation of Word Representations in Vector Space [EB/OL]. (2013−09−07)[2025−04−10]. https://arxiv.org/abs/1301.3781.

[58] SUN G Y, CHENG Y N, ZHANG Z X, *et al*. Text Classification with Improved Word Embedding and Adaptive Segmentation[J]. *Expert Syst Appl*, 2024, **238**: 121852. DOI:10.1016/j.eswa.2023.121852.

[59] KHINE A H, WETTAYAPRASIT W, DUANGSUWAN J. A New Word Embedding Model Integrated with Medical Knowledge for Deep Learning-based Sentiment Classification[J]. *Artif Intell Med*, 2024, **148**: 102758. DOI:10.1016/j.artmed.2023.102758.

[60] KOH J J, RHODES B. Inline Detection of Domain Generation Algorithms with Context-sensitive Word Embeddings[C]//2018 IEEE International Conference on Big Data (Big Data). New York: IEEE, 2018: 2966−2971. DOI:10.1109/BigData.2018.8622066.

[61] HOCHREITER S, SCHMIDHUBER J. Long Short-term Memory[J]. *Neural Comput*, 1997, **9**(8): 1735−1780. DOI:10.1162/neco.1997.9.8.1735.

[62] WOODBRIDGE J, ANDERSON H S, AHUJA A, *et al*. Predicting Domain Generation Algorithms with Long Short-term Memory Networks[EB/OL]. (2016-11-02)[2025-01-10]. https://arxiv.org/abs/1611.00791.

[63] 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. DOI:10.1016/j.neucom.2017.11.018.

[64] SHAHZAD H, SATTAR A R, SKANDARANIYAM J. DGA Domain Detection Using Deep Learning[C]//2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP). New York: IEEE, 2021: 139−143. DOI:10.1109/CSP51677.2021.9357591.

[65] NAMGUNG J, SON S, MOON Y S. Efficient Deep Learning Models for DGA Domain Detection[J]. *Secur Commun Netw*, 2021, **2021**(1): 8887881. DOI: 10.1155/2021/8887881.

[66] CHEN Y, ZHANG S, LIU J, *et al*. Towards a Deep Learning Approach for Detecting Malicious Domains [C]//2018 IEEE International Conference on Smart Cloud (SmartCloud). New York: IEEE, 2018: 190−195. DOI:10.1109/SmartCloud.2018.00039.

[67] 郎波, 谢冲, 陈少杰, 等. 基于多模态特征融合的Fast-Flux恶意域名检测方法[J]. 信息网络安全, 2022(4): 20−29. DOI: 10.3969/j.issn.1671-1122.2022.04.003.
LANG B, XIE C, CHEN S J, *et al*. Fast-flux Malicious Domain Name Detection Method Based on Multimodal Feature Fusion[J]. *Netinfo Secur*, 2022(4): 20−29. DOI: 10.3969/j.issn.1671-1122.2022.04.003.

[68] GAO N, GAO L, GAO Q L, *et al*. An Intrusion Detection Model Based on Deep Belief Networks[C]//2014 Second International Conference on Advanced Cloud and Big Data. New York: IEEE, 2014: 247−252. DOI:

10.1109/CBD.2014.41.

[69] 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: ACM, 2016: 13−21. DOI:10.1145/2996758.2996767.

[70] ZHAI Y, YANG J, WANG Z X, *et al*. Cdga: a GAN-based Controllable Domain Generation Algorithm[C]//2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). New York: IEEE, 2022: 352−360. DOI:10.1109/TrustCom56396.2022.00056.

[71] TUAN T A, LONG H V, TANIAR D. On Detecting and Classifying DGA Botnets and Their Families[J]. *Comput Secur*, 2022, **113**: 102549. DOI: 10.1016/j.cose.2021.102549.

[72] HU X Y, LI M, CHENG G, *et al*. Towards Accurate DGA Detection Based on Siamese Network with Insufficient Training Samples[C]//ICC 2022−IEEE International Conference on Communications. New York: IEEE, 2022: 2670−2675. DOI:10.1109/ICC45855.2022.9838409.

[73] GAO F, HAN W B, OU W. BotHunter: Distributed Malicious Domain Name Detection Model Based on Deep Learning and Blockchain[M]//Intelligent Computing Technology and Automation. 2024: 903−913. Amsterdam: IOS Press, DOI:10.3233/atde231270.

[74] GRAVES A, SCHMIDHUBER J. Framewise Phoneme Classification with Bidirectional LSTM and Other Neural Network Architectures[J]. *Neural Netw*, 2005, **18**(5/6): 602−610. DOI:10.1016/j.neunet.2005.06.042.

[75] HU X Y, CHEN H, LI M, *et al*. ReplaceDGA: BiLSTM-based Adversarial DGA with High Anti-detection Ability[J]. *IEEE Trans Inf Forensics Secur*, 2023, **18**: 4406−4421. DOI:10.1109/TIFS.2023.3293956.

[76] LEE H J, KIM H K. Mitigating False Positives in DGA Detection for Non-English Domain Names[C]//2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks−Supplemental Volume (DSN−S). New York: IEEE, 2024: 150−151. DOI: 10.1109/DSN-S60304.2024.00042.

[77] 余子丞, 凌捷. 基于Transformer和多特征融合的DGA域名检测方法[J]. 计算机工程与科学, 2023, **45**(8): 1416−1423. DOI: 10.3969/j. issn. 1007-130X. 2023.08.010.

YU Z C, LING J. A DGA Domain Name Detection Method Based on Transformer and Multi-feature Fusion [J]. *Comput Eng Sci*, 2023, **45**(8): 1416−1423. DOI: 10.3969/j.issn.1007-130X.2023.08.010.

[78] REYNIER LA O, CATANIA C A, PARLANTI T. LLMS for Domain Generation Algorithm Detection[EB/OL]. (2024−11−6) [2025−04−10]. https://arxiv. org/abs/2411.03307.