综述

# DNS 攻击检测与安全防护研究综述

章坚武[1]，安彦军[1]，邓黄燕[2]
（1. 杭州电子科技大学，浙江 杭州 310018；2. 浙江宇视科技有限公司，浙江 杭州 310051）

**摘　要：**随着传统互联网逐渐向“互联网+”演变，域名系统（domain name system，DNS）从基础的地址解析向全面感知、可靠传输等新模式不断扩展。新场景下的 DNS 由于功能的多样性和覆盖领域的广泛性，一旦受到攻击会造成严重的后果，因此 DNS 攻击检测与安全防护方面的研究持续进行并越来越受到重视。首先介绍了几种常见的 DNS 攻击，包括 DNS 欺骗攻击、DNS 隐蔽信道攻击、DNS DDoS（distributed denial of service）攻击、DNS 反射放大攻击、恶意 DGA 域名；然后，从机器学习的角度出发对这些攻击的检测技术进行了系统性的分析和总结；接着，从 DNS 去中心化、DNS 加密认证、DNS 解析限制 3 个方面详细介绍了 DNS 的安全防护技术；最后，对未来的研究方向进行了展望。

**关键词：**域名系统；DNS 攻击检测；安全防护；机器学习
**中图分类号：**TP393
**文献标志码：**A
**doi:** 10.11959/j.issn.1000−0801.2022248

# A survey on DNS attack detection and security protection

ZHANG Jianwu[1], AN Yanjun[1], DENG Huangyan[2]
1. Hangzhou Dianzi University, Hangzhou 310018, China
2. Zhejiang Uniview Technologies Co., Ltd., Hangzhou 310051, China

**Abstract:** With the gradual evolution of the traditional Internet to “Internet+”, the domain name system (DNS) had been continuously expanding from basic address resolution to new models such as comprehensive perception and reliable transmission. Due to the diverse functions and the extensive coverage of DNS in the new scenario, it will cause serious consequences once attacked. Therefore, the research on DNS attack detection and security protection continues and attracts more and more attention. Firstly, several common DNS attacks were introduced, including DNS spoofing, DNS covert channel, DNS distributed denial of service (DDoS) attack, DNS reflection amplification attacks, and malicious DGA domain names. Subsequently, these DNS attack detection technologies were systematically analyzed and summarized from the machine learning perspective. Then, the DNS security protection technologies were sorted out in decentralization, authenticated encryption and limited resolution. Finally, some future research directions were proposed.

**Key words:** domain name system, DNS attack detection, security protection, machine learning

**收稿日期：**2021−11−12；**修回日期：**2022−08−25
**基金项目：**国家自然科学基金资助项目（No.U1866209，No.61772162）
**Foundation Items:** The National Natural Science Foundation of China (No.U1866209, No.61772162)

## 0 引言

随着物联网、AI、云技术的日益普及，传统互联网正向“互联网+物理设备”[1]、“互联网+AI”[2]和“互联网+云”[3]等“互联网+”逐渐演变，这些演变使连接人、物、应用和数据的网络迎来了一个全新的时代。2021 年互联网域名系统国家工程研究中心主任毛伟表示，“互联网发展至今，域名系统（domain name system，DNS）早已超越了简单的解析功能，成为涵盖‘网络空间’‘互联网关键基础资源’‘软硬件技术系统’在内的支撑全球互联网‘互联互通、共享共治’的重要基石”，并提出了下一代 DNS 的概念：从基础解析寻址向“全面感知、可靠传输、智能分析、精准决策”的新模式升级[4]。然而 DNS 的安全脆弱性[5]导致新模式下的 DNS 面临更加严峻的安全挑战。例如，随着万物互联的不断发展，智能医疗设备、穿戴设备涉及更多敏感隐私数据，攻击者通过 DNS 隐蔽信道不仅可以窃取其敏感数据，还可以通过恶意指令对数据进行更改，危害用户健康[6]。同时，DNS 面临大规模 DDoS（distributed denial of service）攻击的风险[7]。云环境中大量数据存储在云端，基于 DNS 欺骗和 DNS 隐蔽信道的数据泄露严重威胁云端数据安全，同时云环境下域名集中化管理，使云端 DNS 服务遭受 DDoS 攻击造成的损失更加严重[8]。新模式下的 DNS 涉及公共通信、信息服务、金融、电子政务、国防科技等重要领域，遭到攻击会丧失服务功能或者泄露重要数据，严重损害公共利益，甚至危害国民经济发展[9]。检测 DNS 攻击与加强 DNS 安全防护成为保障 DNS 平稳发展的必要手段。

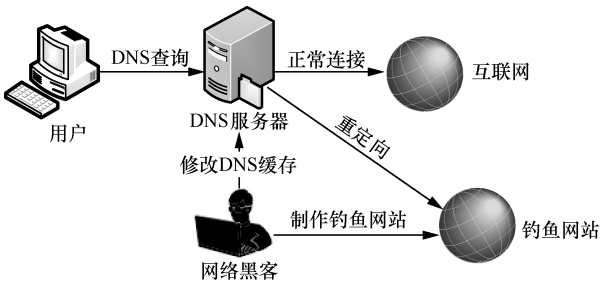
DNS 攻击检测与安全防护的研究意义在于：及时检测各种针对 DNS 的攻击，以保障 DNS 的正常运转；提升 DNS 自身安全的稳健性，以增强其对攻击的抵抗能力；有助于持续提升 DNS 在新模式下的功能多样性和覆盖领域广泛性。

在 DNS 攻击检测的研究过程中，研究人员通过引入机器学习技术，取得了较为显著的成就。机器学习在DNS攻击检测方面表现出不可比拟的优势。同时，为进一步提高 DNS 的安全性，大量相应的安全防护方案被提出，增强了 DNS 自身的稳健性。

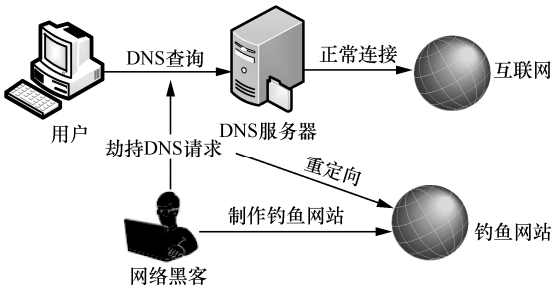
## 1 常见 DNS 攻击

### 1.1 DNS 欺骗

DNS 欺骗，亦称域名欺骗，可将用户合法请求对应的 IP 地址替换为一个虚假、恶意的 IP 地址，从而将用户导向至钓鱼网站，以窃取隐私信息。DNS 欺骗如图 1 所示，主要由两种方式组成：DNS 缓存中毒和 DNS 信息劫持[10]。




(a) DNS缓存中毒




(b) DNS信息劫持

图 1 DNS 欺骗

如图 1（a）所示，在 DNS 缓存中毒攻击中，攻击者非法修改 DNS 服务器的缓存记录，将域名原本对应的 IP 地址替换为恶意 IP 地址，从而将用户访问转移到钓鱼网站。DNS 缓存中毒极具传播性，如果其他DNS服务器从此处获得缓存信息，错误缓存将进一步扩散。与 DNS 缓存中毒不同，

DNS 信息劫持没有修改 DNS 服务器的缓存记录，而是在DNS服务器响应之前将用户请求导向恶意的 IP 地址，该过程如图 1（b）所示。在域名解析过程中，DNS 请求包与响应包通过序列号机制一一对应。攻击者通过监听用户和 DNS 服务器的通信过程，预测出 DNS 服务器响应包的序列号，并据此制作虚假响应包。该包在真实数据包到达之前返回给客户端，客户端解包，获得恶意的 IP 地址，从而将用户访问转移到钓鱼网站。

### 1.2　DNS 隐蔽信道

Lampson[11]首次提出隐蔽信道的概念，并将其定义为“信道被设计的本意并不是为了传输信息”的通信信道。隐蔽信道违反互联网通信协议的规则，使用网络信息载体（网络协议、协议数据）秘密传递信息[12]。由于传统的入侵检测系统和网络防火墙对这些载体的检测力度较小，隐蔽信道传输的数据难以被发现，因此隐蔽信道也是信息隐藏技术的一个分支。

DNS 隐蔽信道是一种报文封装技术，利用 DNS 数据包封装信息[13]。由于 DNS 原本并不是用于数据传输，人们总是忽视其也是恶意通信或数据泄露的潜在威胁[14]。此外，网络防火墙和入侵检测系统都会开放 DNS 服务，因为阻止 DNS 流量可能会导致合法的远程连接失败。因此，DNS 隐蔽信道逐渐成为攻击者手中理想的命令和控制（command and control，C&C）信道，被广泛用于秘密指令和数据的接收与发送。例如，发送恶意控制指令，窃取信用卡账号和登录密码或其他有价值的隐私信息等[15]。

### 1.3　DNS DDoS 攻击

拒绝服务（denial of service，DoS）通过耗尽网络服务的资源和带宽，使服务器没有额外的能力处理外部请求，从而使网络服务崩溃、瘫痪。DoS 攻击是单一攻击者对单一对象发起的攻击，即一对一的攻击方式。DDoS 是升级版的 DoS 攻击，其攻击原理和攻击后果与 DoS 攻击相同，但其攻击方式变为更具有破坏性的多对一的攻击方式[16]。如图 2 所示，DDoS 攻击将成千上万个僵尸主机联合起来在同一时间内对同一目标发起攻击，这样的 DDoS 攻击流量可达到 1.2 TB/s[17]，大多数网络服务器没有能力应对如此规模的攻击流量，从而迅速崩溃。

与其他形式的 DDoS 攻击相比，DNS DDoS 攻击具有更强大的破坏力，这是因为 DNS 的分布式结构具有单点失效性，一旦某根域受到攻击，该根域下的整个网络便会瘫痪。此外，DNS DDoS 攻击还可以用来发起针对性的攻击，如 2016 年发生的 DNS DDoS 攻击事件[18]，其攻击目标是为 3 000 多

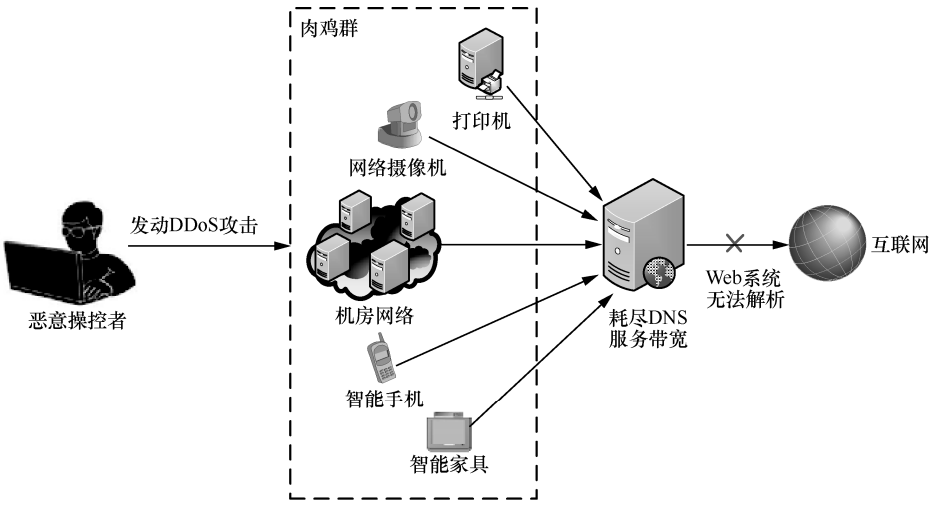



图 2　DNS DDoS 攻击

家企业提供DNS地址解析服务的权威名称服务提供商 Dyn，该攻击导致推特、亚马逊等知名网站在相当长一段时间内不可访问，造成巨大经济损失，Dyn 也因此丧失 8%的域名客户。

### 1.4 DNS 反射放大攻击

DNS 反射放大攻击利用 DNS 响应包比请求包大的特点，耗尽攻击目标的网络资源，本质上也属于 DDoS 攻击。DNS 反射放大攻击与常规 DNS DDoS 攻击的差别是，攻击者不是直接向目标发起攻击，而是通过伪造 IP 地址，向开放 DNS 服务器发送请求，此时服务器会将数倍于请求报文的响应报文发送到受害方，形成间接的 DDoS 攻击，该过程如图 3 所示。据统计，DNS 请求包的大小通常在 40～60 byte，而开放 DNS 服务器响应报文的大小却可以达到 4 000～6 000 byte，将攻击流量放大了近 100 倍。DNS 反射放大攻击使得攻击者控制少量的僵尸主机，就可以达到超大规模 DDoS 攻击的效果，在较短时间内使受害方网络崩溃、瘫痪。

### 1.5 恶意 DGA 域名

近年来，恶意软件的数量不断增加，对网络安全造成较为严重的破坏[19]。通常情况下，恶意软件有一个固定的 IP 地址和一个固定的域名，在该恶意软件的生存周期内，此对应关系不会发生变化。恶意软件通过域名与特定服务器通信以实现 C&C 通信，这样的域名被标识为恶意域名后，只需通过黑名单过滤就可以解决该恶意软件的威胁。近年来，恶意软件为了逃避检测，使用域名生成算法（domain generate algorithm，DGA）来不断更新域名。

DGA 是一种排序算法，用于定期生成大量的域名。在发动攻击时恶意软件使用 DGA 快速生产大量的恶意域名。此外，攻击者还配合使用速变 IP 技术不断变化 IP 地址，使域名和 IP 地址都处在动态的变化中。在这种方式下，黑名单无法起到过滤 DGA 域名的作用，这是因为黑名单的更新速度永远跟不上 DGA 的变化速度，并且防御者需找出所有的 DGA 域名才能切断与恶意软件的 C&C 通信。DGA 使恶意软件的检测变得更加困难，给网络安全造成了极大的威胁。

除上述 5 种常见的 DNS 攻击外，还存在一些特殊的 DNS 攻击。例如，漏洞攻击，攻击者利用 DNS 服务器缓存区溢出、访问权限等漏洞对 DNS 的安全性进行破坏[5]；域名渗透攻击，攻击者在合法的顶点域下注册恶意子域名，从而获得顶点域的信任，进行网络钓鱼和窃取重要信息[20]；蠕虫攻击，WannaCry 蠕虫病毒通过特定域名控制勒索病毒的传播，受感染主机的文件被非法加密，需要支付一定的费用才可解锁[21]。

表 1 对上述 DNS 攻击的原理以及攻击造成的后果进行了总结分析。

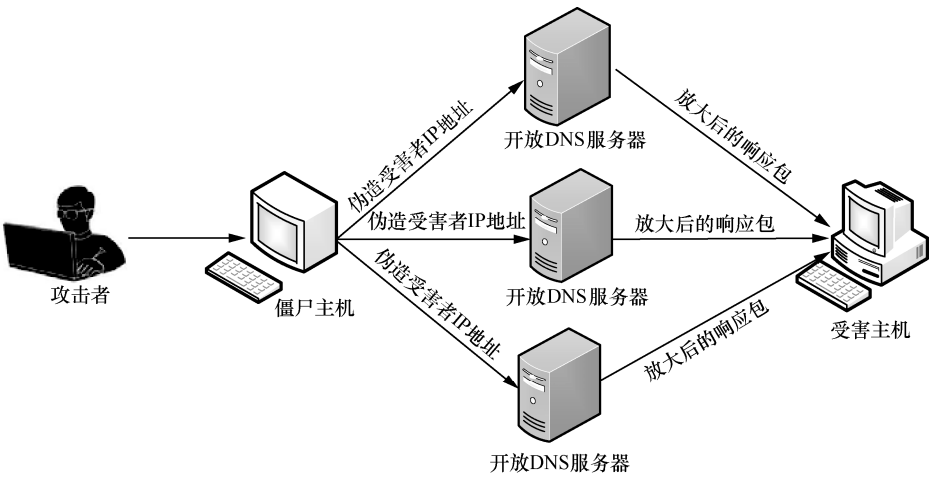



图 3 DNS 反射放大攻击过程

表 1　DNS 攻击对比分析

| 攻击方式 | 攻击原理 | 攻击后果 |
| --- | --- | --- |
| DNS 欺骗 | 修改 DNS 缓存或劫持 DNS 请求 | 网络钓鱼、信息窃取 |
| DNS 隐蔽信道 | 利用 DNS 数据包封装信息 | 发送恶意指令，窃取隐私信息 |
| DNS DDoS 攻击 | 直接耗尽服务器带宽资源 | 丧失网络服务能力，造成经济损失 |
| DNS 反射放大攻击 | 间接耗尽服务器带宽资源 | 丧失网络服务能力，造成经济损失 |
| 恶意 DGA 域名 | 使用 DGA 生成大量恶意域名 | 网络中存在大量恶意域名，破坏系统安全性能 |
| 漏洞攻击 | 利用缓存区溢出、访问权限等漏洞 | 破坏系统安全性能 |
| 域名渗透攻击 | 注册合法顶点域名的子域名 | 网络钓鱼、信息窃取 |
| 蠕虫攻击 | 基于各种木马病毒 | 传播计算机病毒、勒索病毒 |

## 2　常见 DNS 攻击检测技术

### 2.1　DNS 欺骗检测技术

DNS 欺骗的检测较为困难，这是因为 DNS 欺骗不会造成网络流量的明显变化，其数据包和普通的数据包在结构和内容上也极为相似。目前针对 DNS 欺骗的检测主要分为 3 种方式：被动监听检测技术、主动探测检测技术和交叉验证检测技术[10]。

（1）被动监听检测技术

被动监听检测技术通过统计 DNS 解析过程中每一个 DNS 请求包对应 DNS 响应包的数量来判断网络中是否发生 DNS 欺骗。通常情况下，一个 DNS 请求只会收到一个 DNS 应答，即便在一个域名对应多个 IP 地址的情况下也不会返回多个响应包，只是在应答报文中增加相应的应答域。但如果发生 DNS 欺骗，一个查询可能得到两个或者两个以上的响应包。被动监听检测的缺点是过于被动，不能积极主动地去发现一些隐藏的 DNS 欺骗。

（2）主动探测检测技术

主动探测技术是 DNS 主机自主发出 DNS 请求探测数据包，试探网络中是否有 DNS 欺骗发生。探测主机向非 DNS 服务方发送请求，理论上不会收到任何响应。而攻击者往往不会拒绝任何一个 DNS 请求，也不会检查数据包的有效性，从而返回一个欺骗响应包给探测主机。主动探测检测技术的缺点是需要发出大量的探测包，浪费带宽资源，加重网络负担；另外，DNS 欺骗通常针对特定的域名，而 DNS 服务器中解析的域名有很多，因此该技术的检测效率往往较低。

（3）交叉验证检测技术

交叉验证技术基于 DNS 的反向查询功能。DNS 主机首先通过域名查询获得 IP 地址，然后据此 IP 地址反向查询域名，如果二者匹配，说明没有发生 DNS 欺骗，否则说明欺骗攻击存在。但并不是所有的 DNS 服务器都支持反向查询的功能，该检测方法应用受限。

### 2.2　DNS 隐蔽信道检测技术

目前国内外研究将 DNS 隐蔽信道的检测技术分为两大类：基于载荷特征的检测技术和基于流量特征的检测技术。由于 DNS 隐蔽信道利用 DNS 协议的载荷内容封装信息，载荷分析通过判断捕获的 DNS 报文特征和标准 DNS 报文特征是否存在差异来识别隐蔽信道。载荷分析的优点是原理简单，缺点是难以检测报文特征接近正常的隐蔽信道。

基于流量特征的检测技术通过宏观分析 DNS 流量的异常行为来检测隐蔽信道。隐蔽信道的报文特征可以造假，但流量特征是无法更改的，如某个 IP 地址下的 DNS 流量突然增多、大量 DNS 流量流向未知区域等。流量分析的优点是不受隐蔽信道构建技术的影响，通用性较好，缺点是需要对大规模的流量进行统计分析，是一项耗时、烦琐的任务。Farnham 等[14]对常用的载荷特征和流量特征进行了总结，见表 2。

表 2 DNS 隐蔽信道常用检测特征

| 特征 | | 描述 |
|---|---|---|
| 载荷特征 | DNS 请求/响应的大小 | 隐蔽信道通常在请求和响应中放入尽可能多的数据导致长域名 |
| | 主机名的熵 | 隐蔽域名无意义表现为每个字符的均匀使用，具有较高的熵 |
| | 域名中数字字符所占百分比 | 合法域名很少使用数字，经过编码的域名会含有大量的数字 |
| | 最长有意义字符串百分比 | 合法域名通常具有一定含义，隐蔽信道域名随机性强、无意义 |
| | 域名中不同字符个数 | 域名中不同字符过多时通常存在隐蔽信道 |
| | 字符频率 | 合法域名是通用语言的体现，遵循齐普夫定律，字符会集中到高频字符 |
| | 连续的辅音字母 | 合法域名为了方便发音不会使用连续的辅音字母 |
| | 不常用资源记录类型 | 正常信道一般没有 TXT 记录，DNS 隐蔽信道可能会存在大量的 TXT 记录 |
| 流量特征 | 每个 IP 地址的 DNS 流量总量 | 特定客户端 IP 地址由于轮询服务器产生大量流量 |
| | 每个域名的 DNS 流量总量 | DNS 隐蔽信道通过特定受控的域名传输数据，造成该域名流量较大 |
| | DNS 服务器的地理位置 | 大量的 DNS 流量流向无关未知区域，很可能是隐蔽信道造成的 |
| | 历史域名信息 | 隐蔽信道域名通常是最近生成的，造成最近添加的未知的 NS/A 记录 |
| | 孤独的 DNS 请求 | DNS 请求通常在另一个请求之前发出，例如通过 HTTP 的 Web 页面请求 |

随着机器学习技术的发展，目前 DNS 隐蔽信道检测大多综合使用载荷特征和流量特征训练机器学习模型，因此上述分类方法已经不太适用。本文从机器学习的角度出发，对近年来 DNS 隐蔽信道检测技术进行全面的分类和总结，并将其分为两大类：无监督学习和监督学习。监督学习又分为传统的机器学习技术和深度学习技术，深度学习又分为基于特征工程的深度学习检测技术和基于非特征工程的深度学习检测技术。最后按照分类结果的维度将每一项技术归为二分类或者多分类。

2.2.1 无监督学习

无监督学习主要通过DNS报文的载荷特征来检测隐蔽信道，并且主要的无监督学习方式是聚类。如 Das 等[22]提出一种基于 TXT 资源记录聚类的检测方法：首先从 TXT 记录中提取 8 维特征，例如字符串的熵、长度、字符比率、大小写字母的比率、数字比率等；然后对正常通信、隐蔽信道通信下的特征进行统计分析，得到每种特征的分布规律；最后依据此规律将正常流量和隧道流量聚类成不同的两部分。此方法的优点是，当样本差别较大时，不仅可以检测DNS隐蔽信道流量，还可以将不同的隐蔽信道进行分类；其缺点是，过程比较复杂，需要提前手动分析各个特征在正常流量中和隐蔽信道流量中的分布规律。除此之外，人工分析难免会发生各种误差，导致聚类的结果不理想，不能很好地达到检测的目的。因此无监督学习在 DNS 隐蔽信道检测上的应用不是很多。

2.2.2 监督学习

（1）传统的机器学习技术

在过去的十几年中，使用传统的机器学习技术检测DNS隐蔽信道[23-26]是非常热门的研究。如，Aiello 等[23]提出了一种基于传统支持向量机（support vector machine，SVM）的检测方法，提取DNS查询和响应的数据包大小和时间间隔的统计值（如平均值、方差、偏度和峰度）作为特征，训练 SVM 分类器检测隐蔽信道流量；Almusawi 等[24]改进了传统的 SVM，并提出了一种多标签的分类器 Multi-SVM，Multi-SVM 不仅可以区分正常流量和隐蔽信道流量，还可以对不同的隐蔽信道流量进行分类。除 SVM 外，应用于 DNS 隐蔽信道检测的传统机器学习方法还包括随机森林（random forest，RF）[25]、决策树（decision tree，DT）[26]等。这些方法只是在分类器的选择上存在差异，训练模型使用的特征大同小异，因此不对这些传统模型展开详细叙述。

为了进一步提高传统机器学习模型的准确性，Yang 等[27]提出了一种堆叠模型，该模型将 *k*-近邻（*k*-nearest neighbor，KNN）、SVM 和 RF 结合起来生成了一个更加强大的分类器。实验结果表明，与单个 KNN、SVM、RF 相比，堆叠模型具有更好的准确率。堆叠模型是未来研究的一个重点方向，因为堆叠模型可以更好地学习数据集中的有效特性，从而提升检测准确度。

（2）深度学习技术

传统机器学习技术的一个共同缺点是不适用于大规模的数据集，检测精度会随着数据集的扩大而降低。深度学习可以有效地弥补传统机器学习的不足，近年来使用深度学习技术来检测 DNS 隐蔽信道已成为一种趋势[28-32]。本文将基于深度学习的 DNS 隐蔽信道检测技术分为两类：基于特征工程的深度学习检测技术和基于非特征工程的深度学习检测技术。

基于特征工程的深度学习检测技术[28-30]需要从数据集中提取感兴趣的特征并进行预处理，然后训练检测模型；而基于非特征工程的深度学习检测技术[31-32]无须人工提取特征，将数据集直接输入模型进行训练。卷积神经网络（convolutional neural network，CNN）在 DNS 隐蔽信道检测中被广泛使用。Bubnov[28]提出了一种多标签的 CNN 检测模型，并提取 DNS 资源记录和域名熵作为训练特征，对不同类型的 DNS 隐蔽信道进行检测。该模型具有非常简单的架构，仅使用单尺度卷积的 CNN 构建模型，检测精度不是特别理想。之后，Palua 等[29]提出了一种多尺度卷积神经网络（multi-class convolutional network，MC-CNN）检测模型。与 Bubnov[28]的模型相比，MC-CNN 设计了不同尺寸的卷积核，可以从多个维度感知目标的特征，从而有效地提高检测精度。张猛等[30]提出了一种将 DNS 隐蔽信道检测与图像识别相结合的全新方法，首先将数据集中的特征输入灰度图像中，然后构建基于 CNN 的 Lenet-5 模型进行图像识别，从而达到检测隐蔽信道的目的。该方法开辟了一个全新的检测方向，突破了现有 DNS 隐蔽信道检测技术上的局限性。该方法的一个主要缺点是将隐蔽信道特征嵌入灰度图像时需要耗费大量的人力资源，增加了额外的工作量。

Bubnov[28]、Palua 等[29]、张猛等[30]的方法都需要人工提取特征来训练模型，属于基于特征工程的检测技术。如今深度学习的数据量都非常大，提取特征并进行预处理是极其耗时的任务，而基于非特征工程的深度学习检测技术可以避免这一工作，有效地节省人力资源，所以该检测技术是最近的研究热点。

Liu 等[31]提出一种 BYTE-CNN 检测模型，并将整个 DNS 数据包作为模型的输入。该模型的优点是没有依赖具体的检测特征，而是学习整个 DNS 数据包的结构信息，具有较高的检测灵活性。BYTE-CNN 的缺点是当 DNS 数据包混杂过量无关信息时，检测性能难以保证。Chen 等[32]提出了一种基于长短期记忆（long short-term memory，LSTM）网络的检测模型，识别 DNS 隐蔽信道域名。该模型同样没有依赖具体的检测特征，而是直接将域名输入 LSTM 进行训练。以上基于非特征工程的深度学习检测技术除可以节省人力资源外，另一个优点是模型的泛化性能好，因为没有依赖具体的特征，当攻击者修改编码机制时，可以避免重新训练一个检测模型。表 3 对上述基于监督学习的 DNS 隐蔽信道检测技术进行了对比分析。

### 2.3　DNS DDoS 攻击检测技术

关于 DNS DDoS 攻击，研究人员不仅关心攻击的检测，也将研究重点放在如何缓解此攻击上。因为 DNS DDoS 攻击往往能造成严重的经济损失，缓解一部分攻击可以有效降低一些损失。本节按照 DNS DDoS 攻击的检测和缓解两个部分展开叙述。

表 3　基于监督学习的 DNS 隐蔽信道检测技术

| 机器学习类型 | 文献 | 所用算法 | 分类方式 | 依赖特征提取 |
|---|---|---|---|---|
| 传统机器学习 | 文献[23] | SVM | 二分类 | 是 |
| | 文献[24] | Multi-SVM | 多分类 | 是 |
| | 文献[25] | RF | 二分类 | 是 |
| | 文献[26] | DT | 二分类 | 是 |
| | 文献[27] | KNN、SVM、RF | 二分类 | 是 |
| 深度学习 | 文献[28] | CNN | 多分类 | 是 |
| | 文献[24] | MC-CNN | 二分类 | 是 |
| | 文献[30] | Letnet-5 | 二分类 | 是 |
| | 文献[31] | BYTE-CNN | 二分类 | 否 |
| | 文献[32] | LSTM | 二分类 | 否 |

#### 2.3.1　DNS DDoS 攻击的检测技术

DNS DDoS 攻击的检测技术可以分为两类：离线检测[33-34]和在线检测[35]。离线检测通过提取攻击期间的 DNS 数据包特征与正常 DNS 数据包特征训练机器学习分类器，将检测问题转换为分类问题。例如，Takeuchi 等[33]通过训练贝叶斯分类器、Chen 等[34]通过训练 RF 分类器对 DDoS 流量和正常流量进行分类。虽然这种方式可以识别 DNS DDoS 攻击，但是实际意义不是很大，因为 DDoS 攻击持续时间不是很长，攻击结束后再去进行分类也就失去了意义。

在线检测是近年来研究的重点方向，检测到攻击流量时，会设置报警信号提醒服务器采取相应的应对措施，在一定程度上降低损失。在线检测基于对流量的监控，即通过监控某一时间段内流量的变化情况来识别 DDoS 攻击。Trejo 等[35]提出了一种 KNN 在线动态检测模型，将当前时刻的流量、与当前时刻在同 1 h 内的流量以及过去 3 h 内的流量作为一组训练数据。如果 3 个部分的流量都是相似的，则被认为是正常 DNS 流量，否则认为出现异常情况。在线检测的关键在于识别流量的异常变化，而真实网络环境中的正常流量也是时刻变化的，所以在线检测技术必须设置某种标准来区分流量的正常变化和异常变化。

#### 2.3.2　DNS DDoS 攻击的缓解技术

（1）响应缓存技术

响应缓存技术[36-38]利用服务器在受到攻击时可以为自己缓存中的域提供服务的特性，保证在 DDoS 攻击期间，部分服务可以正常运行。Ballani 等[36]和 Wei 等[37]提出 DNS 解析器不要完全清除已过期的 TTL（time to live）记录，而是将其转存在一个单独的“过期缓存”列表中。当 DNS 权威名称服务器受到攻击，其相应的解析器收不到任何响应时，DNS 解析器从“过期缓存”的 TTL 记录中响应查询。Ballani 等[36]提出的方法的局限是，该“过期缓存”列表是不更新的，长时间不访问该服务的记录仍保留在缓存中，导致“过期缓存”的响应效率较低。Mahjabin 等[38]在“过期缓存”中引入一种更新机制，不断去除一些陈旧的访问记录，使“过期缓存”列表保持动态更新，大大提高 DDoS 攻击期间“过期缓存”机制的接入效率。

（2）负载均衡技术

负载均衡技术[38-40]基于合作的思想，在若干服务器之间共享资源。在攻击期间，受到攻击的服务器将资源解析任务转移到没有受到攻击的服务器上，有效缓解 DDoS 攻击的威胁。Anycast[39]是一种被广泛应用的网络路由方式，允许位于不同地域的一组服务器使用相同的 IP 地址。当 DDoS 攻击被发起时，攻击流量被发送到与它最近

的 DNS 服务器，使攻击流量被分散，网络中不会出现单点瓶颈，从而有效缓解 DDoS 攻击。

Mahjabin 等[38]提出了一种动态负载均衡解决方案，在 DDoS 攻击之前只有 1～2 个服务器为单一域名提供服务，在攻击期间其他服务器根据资源占用情况决定是否为该域名提供解析服务。这种方式下 DNS 服务器的数量不是固定的，可以随着攻击量的变化而变化，动态负载均衡技术极大提高了资源的利用率，节约了服务器成本。Wang[40]提出一种基于域重定向的负载均衡技术，其核心思想是将 DNS 查询重定向到备用服务器，从而防止 DNS 服务器过载。该技术首先将若干 DNS 服务器组成一个重定向链，当链中的某一个节点被大量查询流量淹没时，会通过 DNAME 记录（将属于某一个域的查询转移到另一个域，即跨域重定向），将查询流量重定向到其他相关的服务器上，从而实现重定向链中节点之间的流量被重新分配，有效缓解了 DNS 服务器流量过载的情况。

（3）其他通用技术

近年来，研究人员都致力于研究与开发一些防御 DDoS 攻击的通用技术，如软件定义网络（software defined network）[41]、网络功能虚拟化（network function virtualization）[42]和信息中心网络（information-centric networking）[43]，这些技术也通过检查攻击流量和资源共享来缓解 DDoS 攻击。

### 2.4　DNS 反射放大攻击检测技术

DNS 反射放大攻击的本质也是 DDoS 攻击，其检测方式与上述 DNS DDoS 攻击检测方式相似，此处不再赘述。本节介绍 DNS 反射放大攻击的缓解策略，包括对开放 DNS 服务器的保护，过滤伪造源 IP 数据包以及稀释和清洗攻击流量[44]。

（1）对开放 DNS 服务器的保护

开放 DNS 服务器极容易被攻击者利用，充当攻击过程中的流量放大器，因此加强对开放 DNS 服务器的保护可以有效缓解 DNS 反射放大攻击。首先，可以考虑关闭一些不必要的 DNS 服务，同时加强请求服务的鉴权和认证；其次，加强防火墙、路由器的管控力度，判断流量的源 IP 地址，对不属于内部子网的 IP 地址进行阻断；最后，按照数据包大小对来自外部的 DNS 响应包进行过滤，并将超大的数据包直接丢弃。

（2）过滤伪造源 IP 数据包

反射攻击的源头是攻击者发送的伪造 DNS 请求数据包，如果互联网服务提供商可以检查数据包的合法性，对伪造数据包进行过滤，就可以限制 DNS 反射放大攻击。RFC2827/BCP38 规则中建议使用数据包入口过滤技术，以避免攻击者构建虚假的伪 IP 数据包发起 DNS 反射放大攻击。但出于成本考虑，遵守这一建议的网络服务提供商较少，导致该方法没有被广泛应用，DNS 仍面临虚假 IP 数据包的严峻挑战。

（3）稀释和清洗攻击流量

稀释、清洗 DNS 反射放大攻击的流量主要用到 Anycast 技术。在攻击期间，反射放大流量被发送到最近的 Anycast 数据清洗中心进行流量清洗过滤，将大规模的反射放大流量进行稀释、分散，从而有效防御反射放大攻击。

### 2.5　恶意 DGA 域名检测技术

#### 2.5.1　基于黑名单的检测技术

黑名单技术在网络安全领域被广泛使用，将恶意域名列入黑名单是早期 DGA 域名研究中最常用的方法。另一种类似于黑名单的技术是使用逆向工程，即通过研究 DGA 的规律，在攻击之前提前抢注域名并列入黑名单，以阻止与恶意域名通信。但 DGA 域名通常在攻击发起时临时产生，在攻击结束时消亡，生命周期很短，将这样的域名列入黑名单是无效的。另外，网络安全人员必须不断更新黑名单以应对 DGA 域名的不断更新，所以黑名单技术需要耗费大量的人力资源，应用比较受限。

2.5.2 基于语言特征的检测技术

DGA 域名一般比正常域名要长很多，所以长域名是 DGA 域名的一个关键特征，以长度检测为中心的研究也是之前的热点[45]，而基于黑名单的检测方法难以检测长度较短的 DGA 域名。为此，基于语言特征的检测方法被提出。人为设计的域名通常具有一定的意义，而 DGA 域名是随机生成的，不具有实际意义，也难以发音与记忆。Ahluwalia 等[46]根据词汇特性和语言特征，计算了域名的信息论度量，从而检测出长短不同的 DGA 域名。Agyepong 等[47]通过查看域名中单个字符（unigram）以及双字符（bigram）的分布情况，计算 KL 距离、编辑距离和 Jaccard 系数来检测恶意域名。随着编码技术的发展，许多 DGA 域名与正常域名已体现出很大的相似性，仅分析域名的结构特征很难达到准确的检测效果，且容易被对手规避。

2.5.3 基于流量分析的检测技术

DGA 域名在一定程度上会造成 DNS 流量出现异常情况，例如，使域名解析器生成大量的域名不存在（non-existent domain，NXDOMAIN）流量。NXDOMAIN 流量表明解析器没有该请求域名的相关记录。Antonakakis 等[48]基于这一原理提出了一种利用 NXDOMAIN 流量检测 DGA 域名的方法。Zhou 等[49]发现同一 DGA 域组中的每个域名具有类似的查询风格，如果能够确定某个域名为 DGA 域名，然后在 DNS 流量中寻找与该域名类似的流量，可以同时过滤掉同一恶意软件生成的 DGA 域组。

基于流量分析的检测技术虽可以达到较好的检测效果，但是在实际研究中这种方法并不常用，因为 DNS 报文中包含太多与所需信息无关的内容，分析流量规律是一项极其耗费时间的任务，导致检测效率较低。

2.5.4 基于机器学习的检测技术

基于机器学习的 DGA 域名检测技术是近年来的研究热点，其相关检测技术与 DNS 隐蔽信道检测相似，唯一的差别在于，DGA 域名检测中涉及了数据样本不平衡时的解决方案，即代价敏感（考虑了数据不平衡问题）和非代价敏感的检测技术（没有考虑数据不平衡问题）。

在无监督学习中，DGA 域名检测主要使用聚类算法，利用正常域名和 DGA 域名在语义特性和结构特性上的差异进行聚类，最常用的聚类算法为 *K*-means 聚类[50-51]。

在监督学习中，利用传统机器学习技术检测 DGA 域名的通用方法是提取域名的结构特征，如域名长度、熵、元音字符、辅音字符、数字字符的比率等，然后训练 RF[52-53]、DT[54-55]、KNN[56]、SVM[57]等分类器达到检测目的。传统的机器学习技术依赖于特征提取，检测的灵活性较差。

在监督学习中，利用深度学习技术检测 DGA 域名的优势是不依赖具体的人工提取特征，有效提高了检测的准确性和灵活性。LSTM 具备长期学习能力以及优秀的文本特征学习能力，是 DGA 域名检测中最受欢迎的神经网络。但是 Woodbridge 等[58]发现了 LSTM 在多分类任务中对数据不平衡非常敏感，很难检测出域名结构特殊且样本数量较少的 DGA 域名。之后 Tran 等[59]、Chen 等[60]针对这一问题，提出了一种代价敏感的解决方案，其核心思想是通过分配动态权重，提高特殊样本在分类中所占的权重，从而提升特殊样本的检测率。循环神经网络（recurrent neural network，RNN）[61]、生成对抗网络（generative adversarial network，GAN）[62]也是 DGA 域名检测中较为常用的检测网络。王媛媛等[63]总结了 RNN、LSTM、GAN 在 DGA 域名检测中的优势与缺陷，具体见表 4。最后将上述 DGA 域名检测技术进行总结，见表 5。

## 3 DNS 安全防护

基于 DNS 可发起多种类型的攻击，单纯的检测防御难以有效抵御各种 DNS 风险，因此多种提

表 4　RNN、LSTM、GAN 优缺点对比

| 网络 | 优点 | 缺点 |
| --- | --- | --- |
| RNN | 具有一定记忆能力，对序列特征学习具有一定优势 | 只有短期记忆能力，容易出现梯度消失、梯度爆炸现象，且对随机性低的域名产生较高的误报 |
| LSTM | 相比 RNN 具有长期学习能力，在文本学习和自然语言处理等领域被广泛应用 | 对随机性低的域名产生较高的误报 |
| GAN | 通过对生成对抗样本的训练，具有一定预测未来 DGA 变体域名的能力 | 处理离散序列数据存在生成器难以传递梯度更新，判别器难以评估完整的序列数据的缺陷 |

表 5　基于监督学习的 DGA 域名检测技术

| 学习方式 | 机器学习类型 | 文献 | 所用算法 | 分类方式 | 依赖特征提取 | 代价敏感 |
| --- | --- | --- | --- | --- | --- | --- |
| 无监督学习 | | 文献[50] | *K*-means | 二分类 | 是 | 否 |
| | | 文献[51] | *K*-means | 二分类 | 是 | 否 |
| 监督学习 | 传统机器学习 | 文献[52] | RF | 多分类 | 是 | 否 |
| | | 文献[53] | RF | 二分类 | 是 | 否 |
| | | 文献[54] | DT RF | 二分类 | 是 | 否 |
| | | 文献[55] | DT | 二分类 | 是 | 否 |
| | | 文献[56] | SVM KNN | 二分类 | 是 | 否 |
| | | 文献[57] | SVM | 多分类 | 是 | 否 |
| | 深度学习 | 文献[58] | LSTM | 多分类 | 否 | 否 |
| | | 文献[59] | LSTM | 多分类 | 否 | 是 |
| | | 文献[60] | LSTM | 多分类 | 否 | 是 |
| | | 文献[61] | RNN | 二分类 | 否 | 否 |
| | | 文献[62] | GAN | 二分类 | 否 | 否 |

高 DNS 自身稳健性的安全防护方案被提出。本节从 DNS 去中心化、DNS 加密认证、DNS 解析限制 3 个方面对近年来的 DNS 安全防护方案进行总结与分析。

### 3.1　DNS 去中心化

DNS 的树状分布结构以及根域管理模式，导致其具有单点失效的问题。有效加强 DNS 安全稳健性的方法之一是改变其中心化的拓扑结构。目前关于 DNS 去中心化的技术方案主要包含以下 3 个方面。

（1）基于 P2P 网络的 DNS 去中心化

基于 P2P（peer to peer）网络负载均衡的特点，研究人员提出 P2P 模式下的 DNS 解析系统。P2P 网络中不存在中心节点，每个节点相互平等，网络资源和服务分散在每一个节点上，没有单点失效问题，对 DDoS 攻击具有高弹性，如基于 Chord 的动态域名服务（dynamic domain name service，DDNS）网络[64]、基于 Kademlia 的 P-DONAS 网络[65]。在 DDNS 和 P-DONAS 网络中，DNS 域名记录的存储和检索利用分布式哈希表（distributed Hash table，DHT）完成，所以这两种网络继承了 DHT 的良好容错特性，即 DHT 上的一个 DNS 服务器受到攻击宕机时，其数据会自动向相邻服务器转移，只有当所有服务器都瘫痪时，数据才会丢失，造成 DNS 解析失败。

基于 P2P 的 DNS 去中心化方案虽然能有效解决 DNS 单点失效的问题，但是也存在一些局限性。

- 数据延迟，P2P 网络的数据需多次转发才能到达所有节点，当网络波动时，一条 DNS 查询可能在多个大时延的 P2P 网络节点上进行传输，DNS 解析效率明显下降。
- 数据伪造，P2P 网络缺乏验证数据真实性的机制，容易遭受 DNS 欺骗攻击。
- 数据冗余，P2P 网络的每个节点都要进行

数据的转发，同一节点会多次收到同样的数据，造成数据冗余。

（2）基于区块链的 DNS 去中心化

区块链是在不可靠环境下提供可靠决策的分布式账簿技术，具有去中心化、防篡改等特点[66]。区块链去中心化的特性使 DNS 可以有效抵御 DDoS 攻击；防篡改的特性保证 DNS 记录难以被篡改，从而有效抵御 DNS 欺骗攻击。目前较为流行的基于区块链去中心化的 DNS 是基于 Bitcoin 开发的 Namecoin[67]和 Blockstack[68]。Namecoin 是 Bitcoin 的第一个衍生系统，使用虚拟顶级域名.bit 提供 DNS 服务。Namecoin 保留了 Bitcoin 的绝大多数功能和特性，只是将 Bitcoin 链上存储的交易数据替换为.bit 和 IP 地址的对应关系，该对应关系被永久写入区块链，保证相应的域名可以一直被访问。然而，Namecoin 将域名记录信息和控制信息都存储在链上，整个系统面临的数据存储压力很大，导致其在扩展性上存在一定的局限性。为了解决这一问题，将域名信息和控制信息分层存储的 Blockstack 系统被提出。Blockstack 在区块链中仅保存少量的控制信息用于协议注册、创建域名、哈希绑定和密钥绑定，大量的域名记录信息存储在外部数据库中，实现了数据平面和控制平面的分离，提高了区块链 DNS 的扩展性。

基于区块链的 DNS 去中心化方案也存在一些局限性。与传统 DNS 不兼容，用户必须安装特定的解析插件才能与实际的 DNS 通信；面临 51%攻击的风险，基于区块链的 DNS，如果被控制了整个系统 51%的算力，即超过一半的 DNS 记录可以被恶意更改，整个系统的安全性将无法保证。

（3）基于根联盟的 DNS 根去中心化

庞大的互联网系统仅包含 13 个根服务器，网络的接入和通信都以这些根为中心。DNS 根中心化蕴含权力滥用的风险，可以通过 DNS 根区对特定的群体、组织、甚至国家发起针对性攻击，因此研究人员提出 DNS 根域去中心化的方案。基于根联盟的 DNS 根去中心化的方式主要包括如下 4 种[69]：递归根，在本地递归解析服务器上直接进行根域解析，相当于在本地建立一个根服务器；伪装根，将部分根域的查询导向到该根域的伪装镜像进行解析，以降低根域的解析垄断性；开放根，建立独立运作的根服务器，打破根服务器地理分布不均衡以及根区管理被少数国家操纵的现状；全球根，添加根服务器的数量，将 13 个根服务器扩增到更大规模，通过 Anycast 技术实现对特定根区的解析。

基于根联盟的DNS根去中心化的本质是削弱根的权威性，将根服务器的解析权限分散到各个子根，在一定程度上可以缓解针对特定域的攻击。该方案的缺点是没有达到完全的 DNS 去中心化，根区数据仍来源于互联网数字分配机构（Internet Assigned Numbers Authority，IANA），根权力滥用的风险只是被降低，仍然存在。

### 3.2 DNS 加密认证

传统开放式的DNS解析过程缺乏对数据真实性的验证和对完整性的保护，导致 DNS 容易遭受欺骗攻击。随着密码技术的发展，将加密技术引入DNS来保障数据传输过程的真实性和完整性受到广泛关注。目前 DNS 加密认证技术主要包括如下几种方式。

（1）DNSSEC 加密认证

国际因特网工程任务组（Internet Engineering Task Force，IETF）提出基于数字签名和密钥加密认证的 DNSSEC（domain name system security extensions）方案[70]以确保DNS解析结果的真实性。DNSSEC 为 DNS 根域名添加存储密钥和验证密钥是否有效的安全记录，并且从最高级别的根域名开始逐级为域名提供签名认证，从而建立一条从根区开始逐级认证的信任链。在 DNS 解析过程中，DNSSEC 沿着信任链自顶向下解析，通过签名认证每一级子域的数据都真实可靠，从而保证 DNS 解析的结果难以被篡改，有效抵御 DNS 欺骗攻击。

（2）DNSCurve 加密认证

DNSSEC 并不对 DNS 数据本身进行加密，只是通过签名验证 DNS 数据的真实性，如果 DNS 报文被恶意抓取，会造成严重的信息泄露。为了保证 DNS 数据包在传输过程中的保密性，研究人员提出一种基于椭圆曲线加密算法的 DNSCurve 系统[71]为 DNS 提供链路层的安全防护。DNSCurve 保证 DNS 请求被正确解析的机制与 DNSSEC 类似，差别在于 DNSCurve 在验证 DNS 数据包的真实性后还需对数据包进行加密。因此即使 DNSCurve 系统下的 DNS 数据包被恶意分析，但由于加密算法的保护，攻击者仍难以获取有效信息。

（3）协议加密认证

传统 DNS 基于用户数据报协议（user datagram protocol，UDP）传输数据，UDP 在网络上明文传输，无法保证数据的安全性。此外，UDP 是无连接的协议，通信双方无法验证对方的身份，容易遭受欺骗攻击。因此对 DNS 传输层协议进行安全增强来提升 DNS 安全性的方式受到广泛研究。目前最安全有效的方式是 DOT（DNS over TLS）和 DOH（DNS over HTTPS）方案。DOT 使用传输控制协议（transmission control protocol，TCP）和传输层安全（transport layer security，TLS）协议传输数据，数据传输前 DNS 解析器和服务器建立 TCP 连接验证双方的身份，防止虚假数据包入侵；数据传输过程中使用 TLS 协议对 DNS 数据进行加密，防止数据内容被篡改和泄露。DOH 的原理与 DOT 类似，区别在于 DOH 基于超文本传输安全协议（hypertext transfer protocol secure，HTTPS）进行封装，格式更加通用。

### 3.3　DNS 解析限制

（1）设置开放服务器查询权限

开放 DNS 服务器提供响应外部资源请求的功能，但是网络防火墙和入侵检测系统对开放 DNS 服务器的保护力度不足，导致其容易被攻击者利用，实施 DNS 反射放大攻击、DNS 信息劫持、DNS 缓存中毒等恶意攻击。因此研究人员提出对开放 DNS 服务器设置接入权限[5]，以减少网络中恶意 DNS 请求的数量。

（2）设置权威服务器响应速率

权威域名服务器可以统计相同来源 DNS 查询的频次，据此可以设置一个响应计数阈值来限制响应的数量。在一定的时间段内，DNS 响应次数达到设定的阈值，权威域名服务器停止响应，以降低其遭受 DDoS 攻击和反射放大攻击的风险。

## 4　未来研究方向

### 4.1　DNS 攻击检测方面

随着攻击技术的发展，检测技术也需不断改进，目前 DNS 攻击检测技术存在如下局限性待解决。

（1）检测模型的更新往往落后于攻击技术的变化，难以应对变型攻击。如恶意 DGA 域名的检测技术往往落后于 DGA 域名变化的速度[72]，导致恶意域名不能被及时发现，造成安全隐患。

（2）缺乏对特殊攻击的深入研究。目前大多数检测技术缺乏对特殊攻击的深入研究，如低吞吐量下的 DNS 隐蔽信道，此类型的 DNS 隐蔽信道虽然降低了信息泄露的速率，但即便一个 DNS 数据包只泄露 1 bit 的信息，在一年后泄露的信息量可以达到 26 GB[73]。特殊类型的攻击应引起足够的重视。

（3）检测的时效性难以满足。目前多数检测系统只关注检测的准确性和鲁棒性等指标，然而检测效率对检测系统同样重要。隐私泄露、DNS 欺骗、DDoS 攻击等具有严重后果的攻击如果不能及时被发现，会造成严重的后果，因此未来的检测系统需不断提高检测的时效性。

### 4.2　DNS 安全方面

针对 DNS 安全问题，目前已经涌现了大量研究成果，但是 DNS 攻击事件仍不断发生，这是由 DNS 自身安全脆弱性造成的，检测与缓解技术难以应对各种攻击方式。因此未来研究应重点提升 DNS 自身的稳健性来降低遭受攻击的风险，未来 DNS 安全防护可以关注以下几个方面。

（1）加大去中心化 DNS 研究力度。基于区块链的 DNS 可以有效兼容区块链技术的各项优点，是未来 DNS 去中心化的重要研究方向。目前基于区块链的 DNS 设计面临如下挑战。

- 兼容性有待提高。基于区块链的系统与 DNS 是各自独立的两部分，兼容性差[74]，需要安装特定的解析插件才能访问域名系统，只有不断提高两者的兼容性，才能使基于区块链的 DNS 被广泛部署。
- 共识算法的效率有待提高。DNS 的数据需要不断更新和维护，数据需要在整个链上达成共识一致更新。然而目前主要的共识算法的效率较低，难以满足 DNS 数据实时更新的需要[75]，如工作量证明、权益证明等，因此结合 DNS 场景需求设计高效的共识算法是基于区块链DNS去中心化的重要课题。

（2）提高 DNS 加密方案部署覆盖率。基于加密技术和签名认证技术实现了对DNS资源记录完整性和可靠性的保护，可以有效地解决 DNS 欺骗攻击，保护 DNS 的安全，然而该技术的部署覆盖率却不是很高，如 DNSSEC 在顶级域的部署率为 89%，而在二级域的部署率仅为 3%，这是因为目前大多数 DNS 加密方案普遍存在如下问题。

- 兼容性差。目前绝大多数的加密方案需要对 DNS 协议进行修改，且难以与 DNS 兼容运行，造成这些研究成果难以在实际中被广泛推广，如何提高加密防护方案与 DNS 的兼容性是未来 DNS 加密技术研究的首要方向。
- 网络资源开销大。基于加密技术的DNS中，DNS 数据包会携带大量的数字签名消息，耗费额外的网络带宽资源。这一特点一旦被攻击者利用，会增加 DNS 受到放大攻击的风险[69]。因此需要进一步地研究 DNS 加密技术的安全性与资源消耗的平衡。

### 4.3 云环境下的 DNS 安全

云服务的蓬勃发展使DNS服务逐渐向云端迁移，云环境相较于传统的互联网更加复杂，云安全面临更加严峻的挑战。据调查，在云服务对象中，有 42%的组织受到了来自 DNS 云应用的宕机攻击，云环境下的 DNS 安全同样面临严峻的挑战[76]。

（1）云环境下基于 DNS 的数据泄露。云服务伴随着数据的海量存储，越来越多的数据在 Internet 上传输，传输的信息越重要，发生泄露后造成的影响越大，如利用 DNS 隐蔽信道进行隐私数据的传输和窃取[5]。云环境下基于 DNS 的数据泄露需引起高度关注。

（2）云环境下的 DNS 欺骗。网络钓鱼和恶意软件欺诈在云环境中依然有效[77]，缓解云环境下的 DNS 欺骗是一个重要的研究方向。

（3）云环境下的拒绝服务攻击。云环境下域名解析服务集中到少数云服务提供商。文献[78]表明 91%～93%的二级域共享同一个权威名称解析服务器，因此云环境下的 DDoS 攻击一旦成功，会造成更加严重的后果。云环境下 DNS 服务的集中化发展已成趋势，如何有效检测 DDoS 攻击和缓解集中化后遭受 DDoS 攻击的风险，亟待进一步研究。

## 5 结束语

DNS 功能的多样性使其遭受攻击时造成的后果愈发严重，因此提高 DNS 攻击检测能力与加强 DNS 安全防护是保障 DNS 功能扩展的必要前提。本文详细介绍了常见DNS攻击的检测技术以及增强 DNS 安全性能的防护方法，并对未来 DNS 安全的研究方向进行了展望。希望本文可以为相关领域的研究人员提供一定的参考。

## 参考文献：

[1] KHANNA A, KAUR S. Internet of things (IoT), applications and challenges: a comprehensive review[J]. Wireless Personal Communications, 2020, 114(2): 1687-1762.

[2] LIU Y, XIAO F. Intelligent monitoring system of residential environment based on cloud computing and Internet of things[J]. IEEE Access, 2021(99): 58378-58389.

[3] ZENG Z, QI L. “Internet + artificial intelligence” human resource information management system construction innovation and research[J]. Mathematical Problems in Engineering, 2021, 2021(6): 1-11.

[4] 倪思洁. 互联网域名系统国家工程研究中心主任毛伟：网络根基恐被“卡脖子”，下一步往哪走[N]. 中国科学报, 2022-01-06(3).
NI S J. Director of the National Engineering Research Center for the Internet Domain Name System: the foundation of the Internet may be stuck, where to go next[N]. China Science Daily, 2022-01-06(3).

[5] 王文通, 胡宁, 刘波, 等. DNS 安全防护技术研究综述[J]. 软件学报, 2020, 31(7): 2205-2220.
WANG W T, HU N, LIU B, et al. Survey on technology of security enhancement for DNS[J]. Journal of Software, 2020, 31(7): 2205-2220.

[6] VACCARI I, NARTENI S, AIELLO M, et al. Exploiting Internet of things protocols for malicious data exfiltration activities[J]. IEEE Access, 2021(9): 104261-104280.

[7] TUSHIR B, DALAL Y, DEZFOULI B, et al. A quantitative study of DDoS and E-DDoS attacks on Wi-Fi smart home devices[J]. IEEE Internet of Things Journal, 2020, 8(8): 6282-6292.

[8] ABHISHTA A, VAN R, NIEUWENHUIS L J M. Measuring the impact of a successful DDoS attack on the customer behaviour of managed DNS service providers[J]. ACM SIGCOMM Computer Communication Review, 2019, 48(5): 70-76.

[9] 域名国家工程研究中心. 下一代 DNS，牢筑关键信息基础设施安全[EB]. 2022.
Domain Name National Engineering Research Center. Next-generation DNS, strengthening the security of critical information infrastructure[EB]. 2022.

[10] 李杰. DNS 欺骗和缓存中毒攻击的检测[D]. 成都: 电子科技大学, 2015.
LI J. The detection of DNS spoofing and cache poisoning attack[D]. Chengdu: University of electronic science and technology of China, 2015.

[11] LAMPSON B W. A note on the confinement problem[J]. Communications of the ACM, 1973, 16(10): 613-615.

[12] 李彦峰, 丁丽萍, 吴敬征, 等. 网络隐蔽信道关键技术研究综述[J]. 软件学报, 2019, 30(8): 2470-2490.
LI Y F, DING L P, WU J Z, et al. Survey on key issues in networks covert channel[J]. Journal of Software, 2019, 30(8): 2470-2490.

[13] WANY Y, ZHOU A, LIAO S, et al. A comprehensive survey on DNS tunnel detection[J]. Computer Networks, 2021(197): 108322.

[14] FARNHAM G, ATLASIS A. Detecting DNS tunneling[J]. SANS Institute InfoSec Reading Room, 2013(9): 1-32.

[15] AHMED J, GHARAKHEILI H H, RAZA Q, et al. Monitoring enterprise DNS queries for detecting data exfiltration from internal hosts[J]. IEEE Transactions on Network and Service Management, 2019, 17(1): 265-279.

[16] KOLIAS C, KAMBOURAKIS G, STAVROU A, et al. DDoS in the IoT: Mirai and other botnets[J]. Computer, 2017, 50(7): 80-84.

[17] JOW J, XIAO Y, HAN W. A survey of intrusion detection systems in smart grid[J]. International Journal of Sensor Networks, 2017, 23(3): 170-186.

[18] GREENSTEIN S. The aftermath of the Dyn DDoS attack[J]. IEEE Micro, 2019, 39(4): 66-68.

[19] PATSAKIS C,CASINO F, KATOS V. Encrypted and covert DNS queries for botnets: challenges and countermeasures[J]. Computers & Security, 2020(88): 101614.

[20] 王浩. 基于机器学习的异常 DNS 流量检测研究[D]. 南京: 南京邮电大学, 2019.
WANG H. Research on machine learning based abnormal DNS traffic detection[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2019.

[21] 戴云伟, 沈春苗. DNS 的 RPZ 安全防护系统的构建配置与验证[J]. 计算机系统应用, 2022, 31(3): 129-135.
DAI Y W, SHEN C M. Construction, configuration and verification of DNS RPZ protection system[J]. Computer Systems & Applications,2022, 31(3): 129-135.

[22] DAS A, SHEN M Y, SHASHANKA M, et al. Detection of exfiltration and tunneling over DNS[C]//Proceedings of 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA). Piscataway: IEEE Press, 2017: 737-742.

[23] AIELLO M, MONGELLI M, PAPALEO G. Basic classifiers for DNS tunneling detection[C]//Proceedings of 2013 IEEE Symposium on Computers and Communications (ISCC). Piscataway: IEEE Press, 2013: 880-885.

[24] ALMUSAWI A, AMINTOOSI H. DNS tunneling detection method based on multilabel support vector machine[J]. Security and Communication Networks, 2018.

[25] BUCZAK A L, HANKE P A, CANCRO G J, et al. Detection of tunnels in PCAP data by random forests[C]//Proceedings of the 11th Annual Cyber and Information Security Research Conference. [S.l.:s.n.], 2016: 1-4.

[26] 章思宇, 邹福泰, 王鲁华, 等. 基于 DNS 的隐蔽通道流量检测[J]. 通信学报, 2013, 34(5): 143-151.
ZHANG S Y, ZOU F T, WANG L H, et al. Detecting DNS-based covert channel on live traffic[J]. Journal on Communications, 2013, 34(5): 143-151.

[27] YANG P, LI Y, ZHANG Y. Detecting DNS covert channels using stacking model[J]. China Communications, 2020, 17(10): 183-194.

[28] BUBNOV Y. DNS tunneling detection using feed forward neural network[J]. European Journal of Engineering and Technology Research, 2018, 3(11): 16-19.

[29] PALAU F, CATANIA C, GUERRA J, et al. Detecting DNS threats: a deep learning model to rule them all[C]//Proceedings of Simposio Argentino de Inteligencia Artificial. [S.l.:s.n.], 2019: 1-12.

[30] 张猛, 孙昊良, 杨鹏. 基于改进卷积神经网络识别 DNS 隐蔽信道[J]. 通信学报, 2020, 41(1): 169-179.
ZHANG M, SUN H L, YANG P. Identification of DNS covert channel based on improved convolutional neural network[J]. Journal on Communications, 2020, 41(1): 169-179.

[31] LIU C, DAI L, CUI W, et al. A byte-level CNN method to detect DNS tunnels[C]//Proceedings of 2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC). Piscataway: IEEE Press, 2019: 1-8.

[32] CHEN S, LANG B, LIU H, et al. DNS covert channel detection method using the LSTM model[J]. Computers & Security, 2021 (104): 102095.

[33] TAKEUCHI Y, YOSHIDA T, KOBAYASHI R, et al. Detection of the DNS water torture attack by analyzing features of the subdomain name[J]. Journal of Information Processing, 2016, 24(5): 793-801.

[34] CHEN L, ZHANG Y, ZHAO Q, et al. Detection of DNS DDoS attacks with random forest algorithm on spark[J]. Procedia Computer Science, 2018(134): 310-315.

[35] TREJO L A, FERMAN V, MEDINA M A, et al. DNS-ADVP: a machine learning anomaly detection and visual platform to protect top-level domain name servers against DDoS attacks[J]. IEEE Access, 2019(7): 116358-116369.

[36] BALLANI H, FRANCIS P. Mitigating DNSDoS attacks[C]// Proceedings of the 15th ACM Conference on Computer and Communications Security. New York: ACM Press, 2008: 189-198.

[37] WEI M L, LU Y C, ZHEN M L. Alleviating the impact of DNS DDoS attacks[C]//Proceedings of 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing. Piscataway: IEEE Press, 2010: 240-243.

[38] MAHJABIN T, XIAO Y, LI T, et al. Load distributed and benign-bot mitigation methods for IoT DNS flood attacks[J]. IEEE Internet of Things Journal, 2019, 7(2): 986-1000.

[39] JARI A, AVOKH A. PSO-based sink placement and load-balanced anycast routing in multi-sink WSNs considering compressive sensing theory[J]. Engineering Applications of Artificial Intelligence, 2021(100): 104164.

[40] WANG Z. An elastic and resiliency defense against DDoS attacks on the critical DNS authoritative infrastructure[J]. Journal of Computer and System Sciences, 2019(99): 1-26.

[41] YIN D, ZHANG L, YANG K. A DDoS attack detection and mitigation with software-defined Internet of Things framework[J]. IEEE Access, 2018(6): 24694-24705.

[42] LAL S, TALEB T, DUTTA A. NFV: Security threats and best practices[J]. IEEE Communications Magazine, 2017, 55(8): 211-217.

[43] TOURANI R, MISRA S, Mick T, et al. Security, privacy, and access control in information-centric networking: a survey[J]. IEEE communications surveys & tutorials, 2017, 20(1): 566-600.

[44] 陶乃勇. DDoS 放大攻击原理及防护方法[J]. 电信网技术, 2017(10): 89-93.
TAO N Y. The principle and protection methods of DDoS amplification attack[J]. Telecommunications Network Technology, 2017(10):89-93.

[45] MOWBRAY M, HAGEN J. Finding domain-generation algorithms by looking at length distribution[C]//Proceedings of 2014 IEEE International Symposium on Software Reliability Engineering Workshops. Piscataway: IEEE Press, 2014: 395-400.

[46] AHLUWALIA A, TRAORE I, GANAME K, et al. Detecting broad length algorithmically generated domains[C]//Procee dings of International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments. [S.l.:s.n.], 2017: 19-34.

[47] AGYEPONG E, BUCHANAN W J, JONES K. Detection of algorithmically generated malicious domain[C]//Proceedings of 6th International Conference of Advanced Computer Science & Information Technology. [S.l.:s.n.], 2018.

[48] ANTONAKAKIS M, PERDISCI R, NADJI Y, et al. From throw-away traffic to bots: detecting the rise of DGA-based malware[C]//Proceedings of 21st Security Symposium. [S.l.:s.n.], 2012: 491-506.

[49] 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.

[50] BISIO F, SAELI S, LOMBARDO P, et al. Real-time behavioral DGA detection through machine learning[C]//Proceedings of 2017 International Carnahan Conference on Security Technology (ICCST). Piscataway: IEEE Press, 2017: 1-6.

[51] PU Y, CHEN X, PU Y, et al. A clustering approach for detecting auto-generated Botnet domains[C]//Proceedings of International Conference on Applications and Techniques in Information Security. [S.l.:s.n.], 2015: 269-279.

[52] LUO X, WANG L, XU Z, et al. DGAsensor: fast detection for DGA-based malwares[C]//Proceedings of the 5th International Conference on Communications and Broadband Networking. [S.l.:s.n.], 2017: 47-53.

[53] XU S, LI S Q, MENG K, et al. An adaptive malicious domain detection mechanism with DNS traffic[C]//Proceedings of the 2017 VI International Conference on Network, Communication and Computing. [S.l.:s.n.], 2017: 86-91.

[54] STEVANOVIC M, PEDERSEN J M, ALCONZO a, et al. A method for identifying compromised clients based on DNS traffic analysis[J]. International Journal of Information Security, 2017, 16(2): 115-132.

[55] BILGE L, SEN S, BALZAROTTI D, et al. Exposure: A passive DNS analysis service to detect and report malicious domains[J]. ACM Transactions on Information and System Security, 2014, 16(4): 1-28.

[56] BARUCH M, DAVID G. Domain generation algorithm detection using machine learning methods[M]. Cyber security: power and technology. [S.l.:s.n.], 2018: 133-161.

[57] MAC H, TRAN D, TONG V, et al. DGA botnet detection using supervised learning methods[C]//Proceedings of the Eighth In-

ternational Symposium on Information and Communication Technology. [S.l.:s.n.], 2017: 211-218.
[58] WOODBRIDGE J, ANDERSON H S, AHUJA A, et al. Predicting domain generation algorithms with long short-term memory networks[J]. arXiv preprint, 2016, arXiv:1611.00791.
[59] 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.
[60] CHEN Y, PANG B, SHAO G, et al. DGA-based botnet detection toward imbalanced multiclass learning[J]. Tsinghua Science and Technology, 2021, 26(4): 387-402.
[61] 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.
[62] 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 Press, 2016: 13-21.
[63] 王媛媛, 吴春江, 刘启和, 等. 恶意域名检测研究与应用综述[J]. 计算机应用与软件, 2019, 36(9): 310-316.
WANG Y Y, WU C J, LIU Q H, et al. Overview of malicious domain Name detection and application[J]. Computer Applications and Software, 2019, 36(9): 310-316.
[64] BENSHOOF B, ROSEN A, BOURGEOIS A G, et al. Distributed decentralized domain name service[C]//Proceedings of 2016 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW). Piscataway: IEEE Press, 2016: 1279-1287.
[65] YIN S, TENG Y, HU N, et al. Decentralization of DNS: old problems and new challenges[C]//Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies. [S.l.:s.n.], 2020: 335-341.
[66] 陈烨, 许冬瑾, 肖亮. 基于区块链的网络安全技术综述[J]. 电信科学, 2018, 34(3): 10-16.
CHEN Y, XU D J, XIAO L. Survey on network security based on blockchain[J]. Telecommunications Science, 2018, 34(3): 10-16.
[67] KIM J Y. A comparative study of block chain: Bitcoin· Namecoin· MediBloc[J]. Journal of Science and Technology Studies, 2018, 18(3): 217-255.
[68] ALI M, NELSON J, SHEA R, et al. Blockstack: a global naming and storage system secured by blockchains[C]//Proceedings of 2016 USENIX Annual Technical Conference (USENIX ATC 16). [S.l.:s.n.], 2016: 181-194.
[69] 胡宁, 邓文平, 姚苏. 互联网 DNS 安全研究现状与挑战[J]. 网络与信息安全学报, 2017, 3(3): 13-21.
HU N, DENG W P, YAO S. Issues and challenges of Internet DNS security[J]. Chinese Journal of Network and Information Security, 2017,3(3):13-21
[70] CHUNG T, VAN R, CHOFFNES D, et al. Understanding the role of registrars in DNSSEC deployment[C]//Proceedings of the 2017 Internet Measurement Conference. [S.l.:s.n.], 2017: 369-383.
[71] ZOU F, ZHANG S, PEI B, et al. Survey on domain name system security[C]//Proceedings of 2016 IEEE First International Conference on Data Science in Cyberspace (DSC). Piscataway: IEEE Press, 2016: 602-607.
[72] YU L, ZHANG W, WANG J, et al. Seqgan: sequence generative adversarial nets with policy gradient[C]//Proceedings of the AAAI Conference on Artificial Intelligence. [S.l.:s.n.], 2017, 31(1).
[73] NADLER A, AMINOV A, SHABTAI A. Detection of malicious and low throughput data exfiltration over the DNS protocol[J]. Computers & Security, 2019, 80: 36-53.
[74] ZHUANG T, LIU W F, DONG L I. DNS root domain name analysis system based on block chain[J]. Telecommunications Science, 2018, 34(3): 17.
[75] ZARRIN J, PHANG H W, SAHEER L B, et al. Blockchain for decentralization of internet: prospects, trends and challenges[J]. Cluster Computing, 2021: 1-26.
[76] MISHRA S, TRIPATHY N, MISHRA B K, et al. Analysis of security issues in cloud environment[J]. Security Designs for the Cloud, IoT, and Social Networking, 2019: 19-41.
[77] POPLI M. A survey on cloud security issues and challenges[C]// Proceedings of 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom). Piscataway: IEEE Press, 2019: 230-235.
[78] ALLMAN M. Comments on DNS robustness[C]//Proceedings of the Internet Measurement Conference 2018. [S.l.:s.n.], 2018: 84-90.

[作者简介]

**章坚武**（1961– ），男，博士，杭州电子科技大学通信工程学院教授、博士生导师，中国电子学会、中国通信学会高级会员，浙江省通信学会常务理事，主要研究方向为移动通信、多媒体信号处理与人工智能、通信网络与信息安全。

**安彦军**（1996– ），男，杭州电子科技大学通信工程学院硕士生，主要研究方向为网络安全、人工智能。

**邓黄燕**（1987– ），女，浙江宇视科技有限公司高级工程师、公共事务总监，主要研究方向为人工智能、物联网等。