

DNS解析失败分析方法综述

曾濛^{1,2}, 朱宇佳^{1,2}, 李白杨^{1,2}, 王志洋³, 陈闻宇³, 刘庆云^{1,2}

(1.中国科学院信息工程研究所, 北京 100085;

2.中国科学院大学网络空间安全学院, 北京 100049; 3.中国互联网络信息中心, 北京 100079)

摘要: 域名系统 (domain name system, DNS) 是互联网的核心基础设施, 其解析可靠性直接影响网络服务的可用性与用户体验。然而, 随着DNS的功能扩展与体系结构复杂度的增加, DNS解析失败日益频发。现有针对DNS解析失败的研究较为碎片化, 缺乏系统性的归纳与方法论支撑。鉴于此, 从协议实施缺陷、配置错误、域名滥用、网络与管理问题4个维度提出分类归因框架, 系统地刻画了DNS解析失败的成因与特征。基于该框架, 结合互联网工程任务组发布的请求评议标准与典型案例, 提出了协议一致性测试、自动化配置校验、域名信誉评分、高可用部署架构等缓解思路, 为DNS故障诊断和防护提供系统化的分析视角与实践参考。

关键词: DNS解析失败; 归因框架; 协议一致性; 配置校验; 域名滥用

中图分类号: TP393

文献标志码: A

DOI:10.11959/j.issn.2096-109x.2026002

Survey of DNS resolution failure analysis methods

Zeng Meng^{1,2}, Zhu Yujia^{1,2}, Li Baiyang^{1,2}, Wang Zhiyang³, Chen Wenyu³, Liu Qingyun^{1,2}

1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China

2. School of Cyberspace Security, University of Chinese Academy of Sciences, Beijing 100049, China

3. China Internet Network Information Center, Beijing 100079, China

Abstract: As the cornerstone of Internet infrastructure, the Domain Name System (DNS) underpins network availability and user experience. However, the continuous evolution of DNS functionality and its growing architectural complexity have significantly exacerbated the risk of resolution failures. Despite this, existing literature remained fragmented and lacked systematic synthesis or a robust methodological foundation. To address this gap, a four-dimensional attribution framework was proposed to systematically characterize the etiology and patterns of DNS failures, covering protocol implementation defects, configuration errors, domain abuse, and network management challenges. Based on this framework, mitigation strategies were further identified by integrating the request for comments (RFC) standards published by the internet engineering task force (IETF) with real-world case studies, including protocol compliance testing, automated configuration validation, domain reputation scoring, and high-availability deployment architecture. This work provides a comprehensive analytical perspective and practical guidelines for effective DNS failure diagnosis and resilience.

Keywords: DNS resolution failure, attribution framework, protocol compliance, configuration validation, domain abuse

收稿日期: 2025-07-16; 修回日期: 2025-10-19

通信作者: 朱宇佳, zhuyujia@iie.ac.cn

基金项目: 国家重点研发计划 (No.2024YFF1401304)

Foundation Item: The National key Research and Development Program of China (No.2024YFF1401304)

0 引言

域名系统 (domain name system, DNS) 作为互联网的关键基础设施, 负责实现域名与 IP 地址之间的映射, 是网络互联互通的基石。随着互联网规模的扩张与服务形态的演进, DNS 已从最初的简单地址解析机制, 逐步发展为涵盖安全扩展 (如 DNS 安全扩展 (DNSSEC))、智能调度 (如基于 DNS 的负载均衡) 和隐私保护 (如基于 HTTPS 的 DNS (DNS-over-HTTPS)、基于传输层安全协议的 DNS (DNS-over-TLS)) 功能的复杂系统。然而, 在用户规模爆炸式增长、新型网络架构广泛部署、攻防对抗加剧的背景下, DNS 解析失败现象愈发常见, 严重影响了网络服务的可用性与用户体验。

DNS 解析失败是指客户端发起域名查询后, 未收到查询域名的有效资源记录。其诱发因素复杂多样, 涉及协议实施缺陷、配置错误、域名滥用及网络与管理问题 4 个维度。DNS 解析失败对互联网生态的稳定运行构成了多重挑战: 在用户体验层面, DNS 解析失败直接导致服务不可达, 显著降低服务质量; 在服务可用性层面, DNS 解析失败可能引发大规模服务故障, 带来重大经济损失; 在网络安全层面, DNS 解析失败常被攻击者用于实施 DNS 缓存投毒、放大攻击等恶意活动。因此, 深入剖析 DNS 解析失败的成因机理与特征影响, 构建系统化的分析与归因框架, 对提升互联网基础设施的稳定性和安全性具有重要意义。

尽管学术界与工业界已在 DNS 解析失败领域进行了广泛探索, 但现有研究在系统性与通用性方面仍存在局限。一方面, 研究视角呈现碎片化特征, 多数工作集中于特定类型的解析失败 (如 DNSSEC 验证失败或缓存污染等), 缺乏对不同失败模式间内在关联的系统性剖析; 另一方面, 各种分析方法差异显著, 受数据采集方式 (被动测量或主动探测)、技术路径 (统计分析或机器学习) 及评估基准不一的影响, 不同研究得出的结论缺乏横向可比性。这些局限制约了 DNS 解析失败分析理论的完善和高效缓解措施的制定。

为此, 本文旨在建立一个多维度、系统化的 DNS 解析失败分析框架, 以整合现有碎片化研究成果, 为动态网络环境下的故障诊断与系统优化

提供理论支撑。具体而言, 本文从协议实施缺陷、配置错误、域名滥用及网络与管理问题 4 个维度搭建归因框架, 深入剖析各类解析失败的产生机理、演化特征与相互关联, 并在此基础上提出层次化的分析方法与缓解策略。该框架不仅有助于推动 DNS 解析失败研究的体系化发展, 还可以为工程实践中故障的快速定位与修复提供指导。

1 DNS 解析失败概述

作为互联网基础设施的关键枢纽, DNS 解析的可靠性和成功率直接影响着网络服务的可用性。解析失败不仅会导致目标资源无法访问, 还可能引发内容加载异常等级联故障, 严重影响用户体验与服务稳定性。图 1 展示了 DNS 解析失败及其应对措施的演进时间线。其中, 红色节点表示 DNS 解析失败引发的重大网络中断事件, 蓝色节点表示业界为应对此问题发布的请求评议 (request for comments, RFC), 绿色节点表示学术界围绕 DNS 解析失败开展的研究工作。

DNS 解析失败表现出多样化的状态特征。图 2 从客户端、递归解析器和权威服务器全链路视角, 揭示了不同失败模式的触发机理。具体而言, 当用户请求的域名未注册或在权威服务器中尚未配置时, 递归解析器会返回 NXDOMAIN (不存在的域名), 表明域名不存在或配置缺失; 若上游权威服务器响应异常、服务配置不完整或解析路径错误, 则递归解析器返回 SERVFAIL, 表示“服务器错误”; REFUSE 响应码表明服务器出于访问控制或安全策略原因, 实施了策略性拒绝。此外, 物理链路异常、服务器宕机等因素也会导致请求超时; 而报文格式错误、协议字段不兼容等问题则可能触发 FORMERR、NOTIMP 等响应码。虽然这些失败表面上均表现为无法解析出 IP 地址, 但其背后往往隐藏着协议实现缺陷、配置错误、域名滥用或网络攻击等深层次原因。由于同一响应码可能对应多种不同的归因路径, 因此有必要对现有的解析失败分析方法进行系统梳理。

深入研究 DNS 解析失败问题, 不仅是保障关键信息基础设施稳定运行的前提, 也为网络安全防护与异常检测提供了重要的数据支撑。

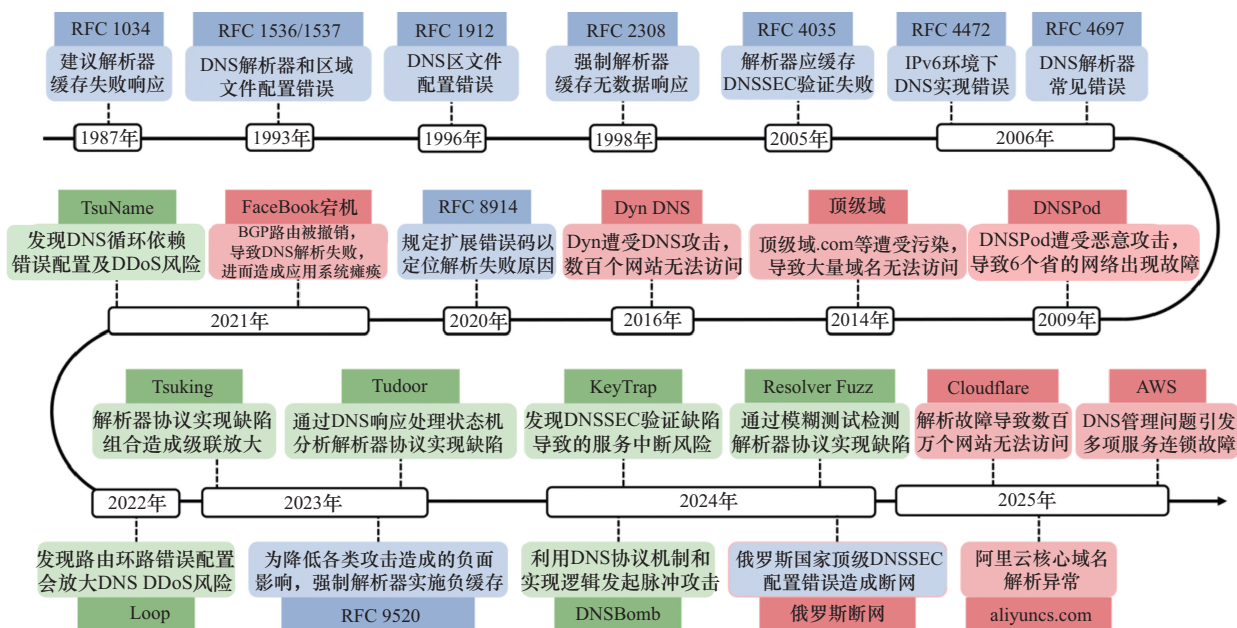


图1 DNS解析失败及其应对措施的演进时间线

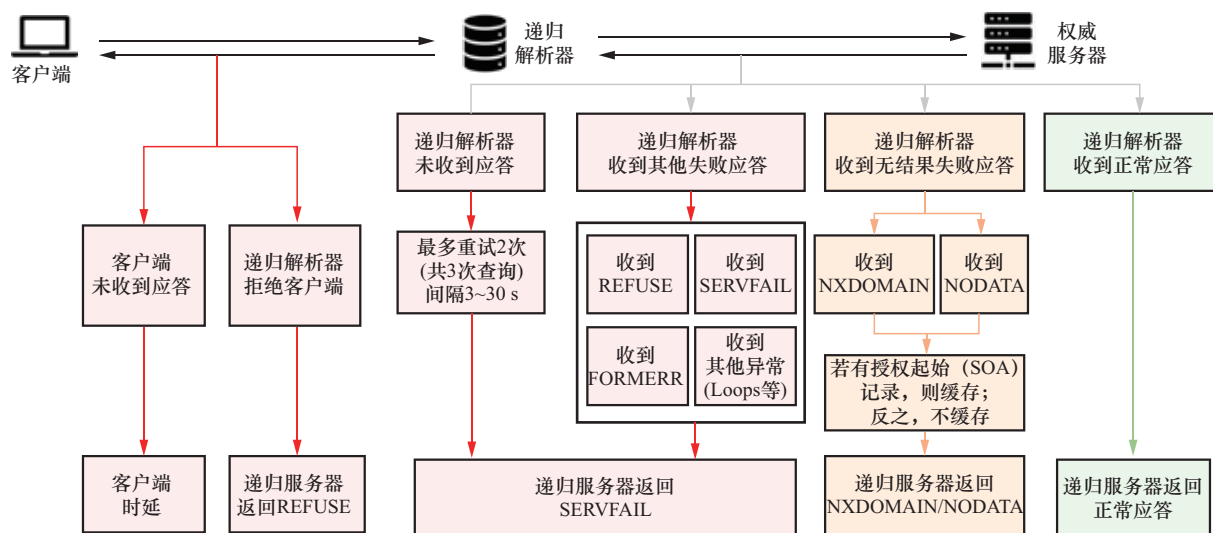


图2 全链路视角下的DNS解析失败模式触发机理

在网络运维层面，DNS解析失败请求的时空聚集特征可用于识别配置错误、服务异常及基础设施性能瓶颈，从而指导网络优化；在安全分析层面，DNS解析失败请求常与恶意扫描、域名生成算法（domain generation algorithm, DGA）流量、DNS隧道等攻击行为高度相关；在协议演进层面，大规模的解析失败流量往往反映出命名空间管理的混乱、协议部署一致性的缺失或新旧标准兼容性冲突。因此，系统地剖析DNS解析失败的原因、模式及特征，对增强DNS服务的韧性、提升网络空间安全的可观测性，以及支撑

协议演进与异常检测算法研究，具有重要的理论价值与现实意义。

2 DNS解析失败：分类与归因

DNS解析失败的成因复杂，涉及底层的协议实施缺陷、运行层面的配置疏漏、恶意的域名滥用行为和网络环境与管理约束。为系统化梳理现有研究成果，本文首先从技术、攻击和管理3个层面展开分析，在此基础上构建一个涵盖协议实施缺陷、配置错误、域名滥用及网络与管理问题的四维分类归因框架，如图3所示。

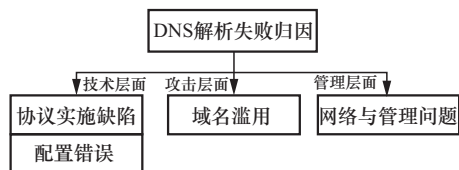


图3 DNS解析失败归因框架

从技术层面来看，DNS解析失败主要源于协议实施的缺陷或运行配置的错误，二者的核心差异体现在故障产生的生命周期阶段。其中，协议实现缺陷的责任主体为标准实现方，其根源在于开发阶段未严格遵循RFC标准或实现存在差异，这类问题通常会引发系统性故障。配置错误的责任主体为运行管理方。其本质是人为操作失误或缺乏有效的校验机制，集中表现为权威服务器或递归解析器的参数误配。此类故障大多呈现出局部性特征，但在级联效应下可能被放大。

从攻击层面来看，DNS解析失败主要由域名滥用行为触发。其责任主体为资源持有者或恶意攻击者，典型表现包括恶意抢注、过期域名复用、钓鱼攻击及DGA活动等，这些行为往往会导致大规模的NXDOMAIN响应或解析异常。

从管理层面来看，DNS解析失败主要归因为网络与管理问题。其责任主体多为外部环境提供方（如管理机构、网络运营商等）。此类故障的触发机制涉及网络拥塞、路由波动及策略性内容过滤等，通常具有地域性与策略相关性，影响范围可以跨越多个域。

2.1 协议实施缺陷

协议实施缺陷是指在DNS软件的开发和部署过程中，因未严格遵循相关协议标准而导致的解析异常。此类缺陷存在于解析器或权威服务器中，会使DNS报文处理逻辑偏离标准预期，进而引发解析失败甚至服务中断。

文献[1]的互联网全网测量结果表明，部分开放解析器在生成DNS响应时存在协议不一致问题。例如，错误标记递归可用（RA）或权威回答（AA）标志位，这种差异可能会导致解析异常。2024年1月，俄罗斯国家顶级域“.ru"在执行DNSSEC密钥轮转过程中，因未严格遵循协议规范配置相关资源记录而导致二级域名出现大规模解析失败，并引发区域性的网络中断。该事件凸显了协议实施缺陷潜藏的系统性风险与级联效

应，以及其可能造成的严重经济损失与社会影响。

协议实施缺陷不仅反映了技术实现层面的偏差，还暴露了标准落地过程中的薄弱环节，是影响DNS可靠性的关键因素之一。互联网工程任务组（internet engineering task force, IETF）发布的RFC文档系统定义了域名系统的基本结构、交互逻辑、安全机制以及实施规范，为DNS系统的稳健运行提供了明确的理论指引。因此，DNS软件开发者、注册管理机构及托管服务商等相关利益方应高度重视协议合规性，在软件编码、配置部署及版本迭代的全生命周期中强化标准遵循与一致性测试，最大程度地规避因实施偏差引发的解析故障。

2.2 配置错误

配置错误是指DNS参数设置不当或管理疏漏，导致解析逻辑偏离预期、引发服务不可达或中断的解析异常。配置错误广泛分布于客户端、递归解析器及权威服务器等环节。配置错误对DNS的稳定性构成严峻挑战，实证案例表明其破坏力巨大。在2020至2025年间，MasterCard的域名服务器（NS）记录被错误配置为“akam.ne”（正确配置应为“akam.net”），该配置错误不仅引发了大量无效委派查询，还带来了严重的域名劫持风险。

表1依据IETF发布的系列RFC文档，系统汇总了DNS中常见的配置错误类型。

表1 DNS错误配置相关的RFC文档

类别	RFC	内容
解析器配置错误	1536	如快速重传、递归循环等
	4697	如过度重传、无法处理多级委派
区域文件配置错误	1537	如授权起始（SOA）记录配置错误
	1912	如CNAME记录配置错误
IPv6 DNS错误	4472	如地址实现、服务配置错误

在解析器配置方面，现有标准重点关注实现逻辑的健壮性与资源效率。RFC 1536^[2]分析了早期解析器在实现上的典型缺陷，指出激进的快速重传机制可能引发不必要的重复查询，递归循环源于解析器未正确处理委派信息导致循环调用，

而对无数据响应 (NODATA) 处理不当则会误判域名不存在, 进而触发冗余查询。针对此类问题, 该文档建议增加重试间隔、引入增强递归逻辑的环路检测机制等, 为后续解析器实现提供了重要参考。RFC 4697^[3]总结了部署阶段的高频错误, 如针对失效服务器的持续无效查询、对根及顶级域 (TLD) 服务器的冗余请求及多级委派跟踪逻辑的缺失。这些行为显著增加了基础设施负载。据此, RFC 4697提出了引入缓存失效机制、智能选择上游服务器及改进委派跟踪逻辑等方法, 旨在减少无效流量的同时提升系统的健壮性。

在区域文件配置方面, 数据的准确性直接决定解析结果的可信度。RFC 1537^[4]及其更新版 RFC 1912^[5]指出, 文件是 DNS 的核心组件, 其配置的准确性直接影响域名解析的正确性。常见的配置错误包括: SOA 记录中刷新 (Refresh) 与过期 (Expire) 参数设置不合理, 导致权威服务器同步失效; 冗余胶水记录的引入, 可能破坏解析一致性并扩大攻击面; 邮件交换记录的指向错误, 导致邮件通信失败。为此, 相关标准建议实施严格的格式校验与自动化一致性检测。

在 IPv6 DNS 配置方面, 随着双栈环境的普及, RFC 4472^[6]强调了地址空间管理的复杂性, 明确了运维人员在 AAAA 记录配置、反向解析域 (ip6.arpa) 设置、IPv6 特殊地址 (如 link-local、loopback 等地址) 处理等方面存在的误区。此外, 部分系统对 DNS64/NAT64 等过渡机制支持不足, 制约了纯 IPv6 (IPv6-only) 客户端的连通性。RFC 4472 建议通过精细化的地址类型规划与合理的资源记录配置, 提升 IPv6 DNS 服务的可用性与兼容性。

2.3 域名滥用

域名作为 DNS 解析体系的核心要素, 其状态与合规性直接决定解析服务的有效性。域名滥用不仅会破坏网络空间的信任基础, 还是诱发 DNS 解析失败与异常的关键因素之一。域名滥用形式多样, 包括恶意抢注、过期域名利用及域名劫持等。这些滥用行为常常作为网络钓鱼、恶意软件分发及 C2 通信等攻击活动的基础与载体。

实证案例揭示了域名滥用的危害。在 2024 年

10月12日发生的广东省教育厅短信平台入侵事件中, 攻击者混合使用了恶意抢注的近似域名、未清理的过期域名及被非法劫持的正常域名, 构建了复杂的恶意跳转链路, 导致解析流量异常波动, 并对公众数据安全与政府部门公信力造成损害。

针对这一挑战, 互联网名称与数字地址分配机构 (ICANN) 推出了域名滥用活动报告 (domain abuse activity reporting, DAAR) 项目, 旨在对顶级域中的滥用行为进行系统性的监测与量化分析, 为全球治理策略的制定提供数据支撑。因此, 梳理域名滥用的模式与特征, 对建立早期预警机制、减少 DNS 解析失败及实现主动防御具有重要的理论与实践意义。

2.4 网络与管理问题

网络与管理问题引发的解析失败, 特指网络监管政策、物理基础设施架构及网络传输环境等因素引发的解析异常。此类问题通常源于不同国家或地区在互联网治理策略、网络互联架构及基础设施部署上的差异。一方面, 宏观的互联网治理策略差异导致了解析边界的产生。随着俄罗斯 RuNet、欧盟 DNS4EU 等国家级或区域级 DNS 服务的兴起, 这些本地化的 DNS 系统在提升安全性的同时, 也会影响 DNS 解析结果, 导致解析失败或访问受限。另一方面, 微观的网络环境也会影响解析成功率。对其进行系统性研究, 有助于理解 DNS 解析失败的根本原因, 为提升 DNS 的鲁棒性和服务质量提供理论支持和实践指导。

3 DNS解析失败分析研究现状

基于前文提出的 DNS 解析失败归因框架, 本节从协议实施缺陷分析、配置错误分析、域名滥用检测及网络与管理问题分析 4 个方面, 系统梳理当前 DNS 解析失败分析的研究工作。

3.1 协议实施缺陷分析

攻击者常利用协议实施缺陷构造大量攻击流量, 导致 DNS 解析失败。Xu 等^[7]提出的 TsuKing 攻击, 通过协调多个解析器, 形成级联放大链, 实现超大规模的拒绝服务 (denial of service, DoS) 攻击。Li 等^[8]利用 DNS 解析器的超时机制、查询聚合与快速返回逻辑, 发起名为 DNSBomb 的高流量脉冲攻击, 触发服务过载和解析失败。Nosyk 等^[9]发现了路由环路可以被用于发起查询

环放大攻击的隐患,即使请求未达目的地,中间响应也能产生大量异常流量。Nawrocki 等^[10]系统分析了 DNS 放大攻击生态,揭示了反射器发现机制和查询构造策略如何导致大规模异常解析流量。这些研究表明,攻击者利用 DNS 协议的设计特性或中间系统行为制造流量异常,是间接或直接引发解析失败与服务中断的重要途径。

根据 DNS 解析器承担的功能,本文将解析器协议实施缺陷的相关研究划分为响应报文处理缺陷、缓存实施异常和安全措施缺陷 3 个类别进行介绍。解析器协议实施缺陷的相关研究见表 2。

3.1.1 响应报文处理缺陷

解析器需要具备完备的形式化解析方法,确保以系统化、标准化的方式对各类 DNS 响应报文进行准确解析,避免因报文格式差异、异常情况或潜在错误而导致的解析失败或误判,保障 DNS 查询过程的高效性和可靠性。

Li 等^[11]通过对各类开源 DNS 软件进行分析,确定了解析器在处理 DNS 响应时的一套形式化方法,并提出了 TuDoor 攻击。若解析器未按照相关形式化方法处理 DNS 响应包,则会导致各类解析失败异常。Lu 等^[12]通过分析被动流量并主动构建各类异常响应包,对开放 DNS 解析器返回的不符合规范的 DNS 响应进行识别和分类,指出这些不符合规范的 DNS 响应是造成响应报文解析失败的主要原因。

除 DNS 响应报文的字段内容外, DNS 响应报文的大小、截断、服务器端碎片化等也会干扰解析器的正常处理逻辑,并影响最终解析结果。Moura 等^[13]分析了荷兰国家顶级域(ccTLD)“.nl”的权威服务器的被动流量,评估了 DNS 响应的大小、截断及服务器端碎片化对解析结果的影响,为 DNS 解析失败分析提供了新的视角。

为更精准地定位 DNS 解析失败原因, IETF 制定并颁布了相关 RFC 标准,在该 RFC 标准中引入了 DNS 解析失败的扩展错误码机制(即在 DNS 响应报文的扩展字段中添加详细的错误信息)。Nosyk 等^[14]对公共解析器对该 RFC 标准的支持情况进行了测量分析,发现不同解析器在遵循和实现该标准方面存在较大差异。这种差异使得在实际故障排查中,利用扩展错误码定位根因面临不确定性,增加了排查复杂性。

3.1.2 缓存实施异常

在缓存实施异常方面,负缓存缺失与生存时间(TTL)配置和处理不当是两大主要因素。

1) 负缓存缺失:负缓存是减少失败流量的重要举措。负缓存是指递归解析器将查询失败的响应(如“域名不存在”NXDOMAIN)临时存储一段时间。在此期间,若收到对同一域名的重复查询,解析器将直接返回缓存的失败结果,而无须再次向权威服务器发起查询,从而减少查询时延和上游服务器的负载。随着互联网的发展和 DNS 的日益复杂, RFC 要求 DNS 解析器对所有

表 2 解析器协议实施缺陷的相关研究

类别	相关研究文献	研究内容
响应报文处理缺陷	文献[11]	若解析器不按形式化方法处理 DNS 响应包,则会导致各类解析失败
	文献[12]	不符合规范的 DNS 响应是导致解析失败的主要原因
	文献[13]	评估了 DNS 响应报文的大小、截断、服务器端碎片化对解析结果的影响
	文献[14]	发现不同解析器在遵循和实现协议方面存在较大差异
缓存实施异常	文献[15]	测量公共解析器对 NXDOMAIN 负缓存的实施情况
	文献[16]	测量开放解析器 NXDOMAIN 负缓存的实施情况
	文献[17]	对主流的公共解析器进行全面的负缓存测量
	文献[18]	父子域生存时间(time to live, TTL)值不一致可能增加解析失败风险
	文献[19]	部分 DNS 解析器会忽略 TTL 值并使用过期记录,影响解析准确性
安全措施缺陷	文献[20]	域名最小化(QMIN)的某些实现方式会导致解析失败率增加
	文献[21]	解析器在启用 QMIN 时的错误率仍较高
	文献[22]	在高时延和较差的网络条件下,加密 DNS 协议的性能明显低于传统的非加密 DNS 协议

类型的解析失败实施负缓存。未实施负缓存的解析器会产生大量的DNS解析失败流量，并面临攻击风险，影响DNS生态的健康。Afek等^[15]通过自建客户端和权威服务器、观察TTL值的变化，测量公共解析器对NXDOMAIN负缓存的实施情况。Shafir等^[16]使用类似方法测量开放解析器对NXDOMAIN负缓存的实施情况。Zeng等^[17]基于随机模拟的方法，首次对流行的公共解析器进行了全面的负缓存测量。

2) TTL配置和处理不当：TTL值的合理配置和正确处理直接影响DNS解析成功率和系统稳定性。Moura等^[18]指出，父域和子域TTL值不一致可能导致解析器缓存时长选择不当，增加解析失败风险。合理配置TTL值可减少DNS流量和时延，降低网络或服务器问题引发的解析失败频率。Schomp等^[19]发现部分DNS解析器会忽略TTL值而使用过期记录，进而影响解析准确性。

3.1.3 安全措施缺陷

在DNS协议运行过程中，各类安全措施（如域名查询最小化、加密DNS等）的配置与实施的合理性也会影响DNS解析的成功率。

QMIN作为一种隐私保护技术，通过仅向权威服务器发送最小化信息，有效减少了DNS查询过程中的信息泄露。然而，其配置和实现方式对解析成功率产生了显著影响。De Vries等^[20]采用主动测量的方法，首次研究了QMIN在互联网中的部署情况，发现某些实现方式（如严格模式）可能导致解析失败率显著提升。在此基础上，Magnusson等^[21]扩展了相关研究，通过主动与被动测量方法分析了QMIN的采用情况，发现尽管错误率有所下降，但部分解析器在启用QMIN时的错误率仍较高。

在加密DNS的部署使用方面，Mbewe等^[22]研究了在非洲地区采用加密DNS协议对用户体验的影响。研究发现，在时延大、网络条件较差的场景下，采用加密DNS协议的系统在性能上明显低于采用非加密DNS（Do53）协议的系统，导致解析失败率显著提升。

DNSSEC作为DNS安全增强扩展，其自身存在的设计缺陷同样可能引发解析失败。Heftrig^[23]等揭示的DNSSEC协议中的KeyTrap攻击正是此类设计缺陷的典型体现。该攻击利用DNSSEC协议中的漏洞，使DNS解析器在验证签名时陷入算法复杂性攻击，进而引发DoS并产生大量解析失败流量。

除设计漏洞外，DNSSEC在配置与实施层面的问题也是导致DNS解析失败的重要原因。文献[24-27]的相关研究（汇总于表3）表明，DNSSEC记录缺失或错误、使用弱密钥、签名过期、信任链断裂等问题，以及解析器未正确验证或不支持相关机制，均可能引发安全降级或解析失败，这凸显了正确部署与严格遵循标准的重要性。刘林晖等^[28]通过设置8种DNSSEC错误配置，发现尽管大多数递归解析器能够识别错误，但仍广泛存在错误识别不完整或返回错误码不准确的情况。这表明DNSSEC协议在实际部署中存在实施不一致的问题，这种实施上的差异直接导致了DNS解析失败的发生。

3.2 配置错误分析

配置错误广泛存在于客户端、递归解析器及权威服务器等环节。这类错误配置所形成的安全缺陷极易被恶意攻击者利用，用于发起DNS放大攻击、域名劫持等，进而可能诱发大规模的解析失败或服务瘫痪事件。

Zhang等^[29]通过模糊测试发现缓存污染、内

表3 DNSSEC错误配置相关研究

相关研究文献	记录缺失或错误	使用弱密钥	错误签名
文献[24]	30%的域名缺失DNSSEC记录	39%的域名使用不安全的密钥签名密钥（KSK）、90%的域名使用不安全的区域签名密钥（ZSK）	0.6%的域名提供错误的资源记录签名（RRSIG）
文献[25]	4%的域名存在配置错误	—	—
文献[26]	19%的Alexa域名无法建立信任链	52%的二级域名使用1 024位或更短的RSA密钥	—
文献[27]	0.45%的域名配置错误导致验证失败	1 024位RSA密钥在二级域名中大量使用，且512位密钥数量增加	1 799个域名的签名过期

存破坏、资源耗尽等解析器漏洞，这些漏洞会导致系统不稳定，降低解析成功率。Li 等^[11]分析了 DNS 响应预处理流程中的逻辑漏洞，指出解析器在处理畸形响应时容易触发重试机制甚至崩溃。解析器和权威服务器在实现上存在安全边界缺失或异常处理机制不当等问题，使其在面对恶意构造或非标准的输入时，也会产生 DNS 解析失败。本节将依据配置错误产生的具体位置，对其成因展开系统性分析。

3.2.1 客户端配置错误分析

客户端的本地配置问题（如查询参数配置错误^[30]、本地解析器配置错误^[31]等）是导致 DNS 解析失败的重要因素之一。奇安信的研究指出，某品牌手机的一款应用在进行 DNS 解析时，错误地为查询域名自动添加了“ll”或“null”后缀，此类畸形查询产生了大量无效的解析失败流量。此外，部分客户端将专用于本地网络的域名（如“.local”和“.localdomain”）的查询请求发送给公共递归解析器，这类查询因在公共域名空间中不存在对应记录而必然失败。Yang 等^[30]通过对被动 DNS 流量进行上下文信息的统计，发现不同的解析器对同一域名的解析成功率存在差异。这一发现表明，客户端应选择更合适的解析器，从而降低解析失败流量占比。

3.2.2 解析器配置错误分析

解析器在配置管理层面的缺陷不仅是解析失败的直接诱因，还因为掩盖了失败的根本原因而显著增加了故障排查和系统优化的难度。具体而言，解析器的软件版本选择、负载均衡策略及缓

存配置均可能引入解析行为的不确定性，进而影响 DNS 解析结果。

在软件版本选择方面，Takano 等^[32]通过对互联网上开放解析器和 DNS 服务器版本分布的大规模测量，发现许多 DNS 服务器仍在运行过时的软件版本。这些版本通常存在已知安全漏洞，并且可能缺乏对现代 DNS 功能的支持，这不仅易导致解析失败，也为攻击者提供了可乘之机。在负载均衡策略方面，Müller 等^[33]对递归解析器选择权威服务器的行为进行了深入研究，揭示了选择机制的缺陷，即解析器未充分评估目标服务器的时延、实时负载和可用性。这种选择机制的缺陷，容易导致解析请求被发送给响应缓慢或已不可用的服务器，进而增加了解析失败的风险。

在缓存配置方面，Ager 等^[34]比较了本地解析器与公共解析器的性能，指出 DNS 缓存的效率对解析性能和失败率有着直接影响。若 DNS 缓存被污染或未正确更新，则可能导致解析失败；若缓存机制未能有效识别和保护重要域名，导致高频域名被误淘汰，则会显著增加上游查询压力和解析失败风险。为解决此问题，郝逸航等^[35]提出了一种基于 Sketch 技术的域名缓存管理方法，以实现域名缓存的动态规划管理。

3.2.3 权威服务器配置错误分析

权威服务器的配置管理缺陷主要集中在委派记录（NS 记录）上，这些缺陷可以划分为悬挂域名、错误委派和循环依赖 3 类，相关研究见表 4。

表 4 权威服务器配置管理缺陷相关研究

缺陷类别	相关研究文献	研究内容
悬挂域名	文献[36]	识别 3 类悬挂域名，并提出相应的防御机制
	文献[37]	提出 Hosting Checker 风险识别框架
错误委派	文献[38]	测量研究错误委派与冗余配置不足的后果
	文献[39]	量化错误委派的普遍性和持久性
	文献[40]	分析父域与子域委派记录不一致问题
	文献[41]	分析胶水记录缺乏有效验证机制等问题
循环依赖	文献[42]	通过大规模流量分析，指出循环依赖是引发解析失败的主要根源之一
	文献[43]	即时少量 NS 记录配置错误引发的循环依赖，也可能造成大量解析失败

(1) 悬挂域名

悬挂域名是指DNS委派记录所指向的服务器资源已不存在、失效或被释放,导致解析失败并引发安全风险。Liu等^[36]揭示了悬挂DNS记录带来的安全威胁,即DNS记录仍存在但其指向资源已失效。该研究识别了云平台IP地址重用、被弃用的第三方服务和过期域名3种攻击向量,并提出了相应的防御机制。为识别悬挂域名,Zhang等^[37]提出了Hosting Checker框架。该框架通过被动收集并重建依赖链,能够有效发现潜在的悬挂配置,帮助管理员及时修复相关配置问题,从而减少由此引发的解析失败和安全事件。

(2) 错误委派

错误委派是指父域设置的NS记录指向了无法对该子域提供权威解析的服务器。Pappas等^[38]指出,错误委派会使查询响应时间延长30倍,且由于缺乏足够的服务器冗余,相关区域在网络出现波动时极易完全失效。Akiwate等^[39]量化了错误委派的普遍性和持久性,指出错误委派是造成解析失败直接且常见的原因。Sommese等^[40]分析了父域与子域NS记录不一致问题及其对解析时延及解析失败的影响,并评估了解析器在处理不一致NS记录时的表现差异。此外,未及时更新的陈旧胶水记录指向已废弃的IP地址,也是导致解析失败的潜在隐患。文献[41]指出,多数DNS软件在处理胶水记录时缺乏主动验证,解析器容易缓存这些无效记录。

(3) 循环依赖

循环依赖是指解析一个域名所必须查询的权威服务器,其自身的地址解析又反过来依赖于该域名,致使整个解析过程陷入逻辑死循环。图4展示了典型的DNS区域循环依赖。

文献[44]和文献[45]分别从图模型和协议形式模型角度研究了DNS中的名称依赖问题。前者通过构建区域依赖图,直观展示解析过程中区域间的依赖关系,帮助定位失败源并评估依赖链的复杂性,从而预测潜在风险;后者基于协议标准构建了名称依赖的形式模型,揭示父域配置错误、NS目标地址解析异常等可能导致失败的关键因素,同时分析了缓存行为对解析稳定性的影响,为优化DNS配置提供了理论支持。Jung等^[42]通过大规模流量追踪,发现循环依赖、查询超时和配置错误等均为导致解析失败的主要原因。Bojović等^[43]提出的方法能够对配置错误进行分类与量化,其研究表明,即便少量NS记录配置错误,也可能会影响大量域名的可用性。通过识别错误配置问题(如非权威定义、解析过程循环、区域传输等),可显著提升DNS的性能与安全性。

键因素,同时分析了缓存行为对解析稳定性的影响,为优化DNS配置提供了理论支持。Jung等^[42]通过大规模流量追踪,发现循环依赖、查询超时和配置错误等均为导致解析失败的主要原因。Bojović等^[43]提出的方法能够对配置错误进行分类与量化,其研究表明,即便少量NS记录配置错误,也可能会影响大量域名的可用性。通过识别错误配置问题(如非权威定义、解析过程循环、区域传输等),可显著提升DNS的性能与安全性。

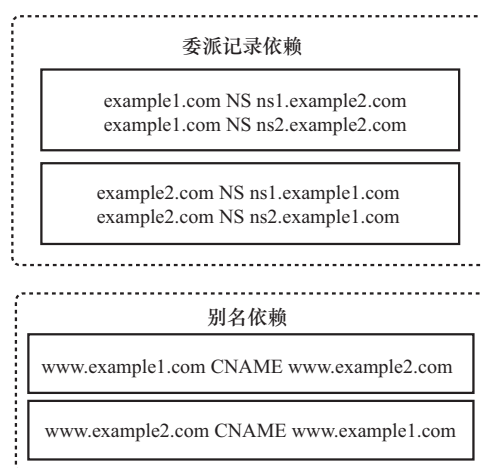


图4 典型的DNS区域循环依赖

3.3 域名滥用检测

域名滥用的研究范围广泛,本节重点关注那些直接导致大量解析失败请求的滥用行为(包括域名抢注、过期域名滥用及恶意域名活动)的检测研究。

3.3.1 域名抢注

表5总结了域名抢注相关研究。Nikiforakis等^[46]探讨了攻击者注册与目标域名仅1 bit之差的域名,用于劫持流量。Kintis等^[47]分析了商标与短语组合域名的大规模滥用,攻击者利用这些域名发起钓鱼或高级持续性威胁攻击,其影响广泛且持续时间长。Agten等^[48]研究了拼写错误域名抢注现象,发现大多数品牌未主动防御域名抢注。Wang等^[49]揭示了点位误输类型域名的系统化注册和广告变现机制。Vissers等^[50]从域名服务器角度研究了配置错误和比特翻转导致的域名劫持与DNS解析失败问题。

表5 域名抢注相关研究

域名抢注类型	说明
Bitsquatting ^[46]	比特翻转造成的域名抢注
Combosquatting ^[47]	商标+短语类型的域名抢注
Typosquatting ^[48]	输入错误类型的域名抢注
Dotsquatting ^[49]	点位错误的域名抢注
Homosquatting ^[50]	相似字符的域名抢注

3.3.2 过期域名

域名过期将导致域名处于不可解析状态，域名生命周期阶段发生变化会带来相应的解析失败风险与安全隐患。表6总结了过期域名相关研究。Lauinger等^[51]研究了域名到期后被重新注册的现象，指出所有权的频繁变更会造成解析不稳定与高失败率，这反映出解析系统在面对突发并发请求时的脆弱性。Lauinger等^[52]还指出，域名查询工具WHOIS数据的不一致性和注册过程的复杂性增加了域名状态判断的难度，从而影响解析准确性和故障排查效率。Lever等^[53]揭示了攻击者重新注册已过期的可信域名并加以滥用（如邮件劫持、恶意软件投递）的行为，并提出Alembic算法。该算法利用被动DNS数据识别域名所有权变更，从而预防解析失败与恶意解析。Moore等^[54]针对美国关闭银行遗留域名的再利用问题展开分析，发现部分此类域名被用于广告、搜索引擎优化或恶意活动。Hao等^[55]研究了垃圾邮件发送者的域名注册行为，发现其偏好批量注册并重复利用过期域名，且活动集中于少数注册商，这类行为容易引发解析指向恶意内容的失败事件。

表6 过期域名相关研究

相关研究文献	研究内容
文献[51]	域名所有权频繁变更导致解析高失败率
文献[52]	WHOIS信息准确性影响解析失败故障排查
文献[53]	过期域名的重新注册被滥用
文献[54]	金融行业过期域名存在较高的滥用风险
文献[55]	批量注册过期域名用于发送垃圾邮件的行为

3.3.3 恶意域名

恶意域名是DNS解析失败的重要诱因，准确识别恶意域名对提升DNS故障诊断与安全防护能力至关重要。马永征等^[56]指出，DGA、Fast-Flux等恶意域名技术会生成大量随机域名或频繁更换解析IP，从而导致DNS返回大量NXDOMAIN响应或出现异常解析行为。这类域名滥用引发的解析失败，严重扰乱了DNS的正常解析秩序。本节将恶意域名检测相关研究划分为4类，即基于网络图与关系建模的方法、基于DNS查询响应行为的异常识别方法、基于机器学习的自动化检测方法和基于注册行为与生命周期建模的方法。恶意域名相关研究见表7。

（1）基于网络图与关系建模的方法

基于网络图与关系建模的方法利用域名之间的解析、解析器、IP地址或其他上下游组件之间的交互关系，构建图结构或依赖网络，实现对潜在恶意域名的识别。Khalil等^[57]提出了一种基于图推理的检测框架，用于识别缓存投毒导致的隐蔽恶意域名。Kountouras等^[58]设计的Thales系统采用主动探测的方式构建大规模的域名—响应关系图，通过分析潜在的恶意域名传播路径实现早

表7 恶意域名相关研究

方法类型	相关研究文献	研究内容
基于网络图与关系建模的方法	文献[57]	基于图推理的框架识别隐蔽恶意域名
	文献[58]	主动探测潜在的恶意域名
基于DNS查询响应行为的异常识别方法	文献[59]	使用NXDOMAIN响应观测恶意活动
	文献[30]	DNS基础设施对恶意域名识别的影响
	文献[60]	分析异常查询请求类型，为DNS解析失败与恶意行为关联提供关键线索
	文献[61-62]	利用反向DNS查询模式和客户端异常活动揭示潜在的恶意行为
基于机器学习的自动化检测方法	文献[63]	采用机器学习模型识别DGA构造的恶意域名
基于注册行为与生命周期建模的方法	文献[64]	分析新注册域名的行为特征，发现恶意域名的异常行为
	文献[65]	建立恶意域名声誉评分模型

期的检测与响应。与被动监测相比,主动采集能够提供更广泛的覆盖范围,从而有效提升了恶意域名识别的前瞻性。

(2) 基于DNS查询响应行为的异常识别方法

基于DNS查询响应行为的异常识别方法关注DNS查询及其响应特征,尤其是NXDOMAIN响应的异常分布与模式,据此分析恶意行为对DNS的影响。Liu等^[59]分析了Farsight数据库中超过1 460亿条NXDOMAIN记录,发现大量失败查询与DGA域名、域名抢注及黑名单域名密切相关,表明NXDOMAIN响应可以作为恶意活动的重要观测窗口。Yang等^[30]通过对30亿条DNS查询进行统计分析,揭示了不同解析器、新通用顶级域(gTLD)和国际化域名(IDN)在解析失败率上的显著差异,反映了DNS基础设施本身对恶意域名识别产生的复杂影响。Gao等^[60]深入研究了A-for-A查询、无效TLD等异常请求类型,为DNS解析失败与恶意行为之间的关联提供了关键线索。此外,反向DNS查询模式^[61]和客户端异常活动^[62](如网络扫描和垃圾邮件传播)也可以作为辅助特征,帮助揭示由客户端发起的潜在恶意行为。

(3) 基于机器学习的自动化检测方法

随着恶意域名技术手段的不断演化,传统特征工程难以应对新型威胁,研究者转向利用机器学习模型进行特征自动提取与分类建模。FANCI系统^[63]提取DNS流量中NXDOMAIN响应的语言、统计和结构特征,并采用随机森林和支持向量机等模型识别由DGA构造的恶意域名。

(4) 基于注册行为与生命周期建模的方法

该方法利用域名在注册阶段的行为特征及其生命周期轨迹(如注册时间窗口、使用频次和DNS解析行为等)来预测其潜在风险。Hao等^[64]通过分析新注册域名的行为特征,结合垃圾邮件陷阱与Verisign的DNS数据,发现恶意域名在注册初期即表现出可以观测的异常行为(如生命周期极短、解析请求瞬时爆发等),从而支持在攻击发生前进行早期预警。Notos系统^[65]通过整合域名的网络属性与历史行为数据,构建了动态声誉评分模型,为潜在恶意域名赋予动态风险标

签。该方法可作为防御缓存投毒的组成部分,为异常域名检测提供依据。

3.4 网络与管理问题分析

网络监管政策及跨域访问限制等因素同样是引发DNS解析失败的重要原因。依据问题来源和影响机制,可以将相关研究归纳为以下3类。

(1) 政策监管导致的解析失败

国家或地区出于网络安全、内容治理等目的实施的互联网管理政策,常直接影响DNS解析过程。

(2) 运营商配置与策略引发的解析失败

网络运营商的网络配置策略和DNS服务部署直接影响终端用户的解析体验。配置不当或特定管控策略(如本地DNS劫持、解析器策略性过滤或重定向、网络拥塞与QoS限制、最大传输单元与分片问题等)会引入额外的失败点。

(3) 基础设施与跨域访问问题

全球网络基础设施的部署差异、连通性问题及特定技术方案的局限性也会导致解析失败。例如,内容分发网络部署不当、路由异常与网络分区、IPv6/IPv4双栈兼容性问题、Anycast节点分布不均等均可能导致解析失败。

网络与管理问题作为DNS解析所依赖的外部环境,受运营商策略执行、基础设施条件等的制约,其影响范围广、根因复杂且往往具有地域特征。文献^[66]通过集成多种测量技术构建了覆盖全球的测量平台,其大规模测量数据和时间序列分析能力有助于识别解析失败的时空特征,并区分配置错误与技术故障等原因。Siby等^[67]揭示了加密DNS(如DNS-over-HTTPS、DNS-over-TLS)在流量分析下仍存在的隐私泄露风险,提出的特征集与分析方法有助于识别加密流量中由攻击或识别错误而导致的解析失败,并对现有防护手段的局限性提供了参考。Pearce等^[68]提出通过可验证性指标,可以识别不同解析器返回结果的不一致,从而有效发现解析失败现象。Feal等^[69]对开源过滤列表生态进行了系统性分析,指出其结构不一致、标签混乱与更新频率不稳定可能引发误判,进而影响解析行为的准确性。Niaki等^[70]利用虚拟专用网络(virtual private network, VPN)节点构建了一个全球化监测平台,

其长期观测与聚类分析为识别异常解析行为及解析失败的潜在原因提供了支持。Kogan 等^[71]提出了基于私有信息检索的阻断列表查询机制,在保护用户隐私的同时提升了查询效率,降低了系统性能瓶颈导致的解析失败风险。

总体而言,上述研究从多个维度丰富了 DNS 解析失败的诊断工具和研究视角,推动了对解析失败现象背后机制的深入理解。

4 DNS 解析失败缓解措施

为降低 DNS 解析失败造成的影响,定位 DNS 解析失败原因,IETF 颁布了 RFC 8914^[72],该标准定义了扩展 DNS 错误(EDE)码,允许 DNS 服务器在错误响应中附加详细的失败原因信息。这一机制在不改变现有响应码(response code, RCODE)的处理方式的前提下,通过携带额外的错误码与说明文本,帮助解析器和应用程序更准确地理解错误原因。RFC 8914 还定义了系列初始错误码,并创建了一个由因特网编号分配机构(IANA)维护的注册表,以支持未来的扩展。该机制有助于提升 DNSSEC 验证失败等场景下的错误处理透明度与诊断能力。RFC 8914 定义的典型扩展 DNS 错误码见表 8。

表 8 RFC 8914 定义的典型扩展 DNS 错误码

EDE 码	含义	说明
2	Unsupported DS Digest Type	不支持的 DS 记录哈希算法
7	Signature Expired	资源记录集合签名(RRSIG)记录过期
14	Not Ready	区域未准备就绪
15	Blocked	因内部策略无法响应
21	Not Supported	不支持的查询
22	No Reachable Authority	无法连接到任何权威服务器
23	Network Error	网络错误
30	Invalid Query Type	无效的请求类型

通过引入 EDE 码, RFC 8914 显著增强了 DNS 错误处理的表达能力,使解析器和应用程序能够更准确地识别和处理各类 DNS 解析失败。特别是在 DNSSEC 验证、网络故障和安全策略相关的场景中, EDE 码提供了更多的上下文信

息,有助于运维人员和开发者快速诊断和解决问题。此外, RFC 8914 强调了扩展错误信息潜在的安全风险,建议用户在未经验证的情况下不应完全采信,从而避免潜在的攻击或信息泄露。

除 EDE 码外,针对前文梳理的各类解析失败归因及其分析方法,应采取相应的措施。

4.1 协议一致性测试

第 3.1 节分析的协议实施缺陷(如解析器响应处理缺陷、缓存实施异常、安全措施缺陷、权威服务器的区域依赖和 DNSSEC 缺陷),其根源在于对协议规范不完全遵循、不同实现之间的兼容性差异和对边缘情况处理的不一致。基于文献[11-14]提出的形式化方法、异常响应识别和协议一致性测量等手段,可以通过开发和使用协议一致性测试工具进行缓解。例如,利用符号执行、模糊测试等技术对主流 DNS 软件(如解析器、权威服务器的软件)进行自动化检测,从而识别潜在缺陷。此外,应当推动社区对 DNS 协议更新内容的统一理解和落实,如通过官方测试套件、标准遵循认证等方式促进实现规范化。在实际部署中,运营方应当参考第 3.1.2 节关于缓存实施异常(文献[15-19])和第 3.1.3 节关于 DNSSEC 缺陷(文献[24-27])的分析结论,定期对解析器和权威服务器进行升级和行为验证,从而降低历史实现问题引发的故障风险。

与传统针对单一漏洞的修补方式不同,本文提出的缓解措施强调系统性与前瞻性,旨在通过形式化分析、一致性测试和主动验证提升整体鲁棒性。传统方法通常是反应式的,即在问题暴露后进行修补,且聚焦于特定点(如修复某个 SERVFAIL 错误)。而本文框架指导的方法强调前瞻性和全面性,基于对协议栈合规性的整体形式化分析与测试评估,推动生态层面的标准化以减少兼容性问题并通过对缓存、DNSSEC 等关键机制的持续主动验证来减少潜在故障。这种方法力求从根源上提升协议实现的整体鲁棒性,而非仅解决已出现的个例问题。

4.2 自动化配置校验

DNS 的配置逻辑复杂且管理职责分散,常导致区域配置错误、权限设置不当等问题。为应对第 3.2 节揭示的配置错误导致的解析失败,当前

较为有效的策略是引入自动化的配置生成与校验机制,在上线前对配置文件进行语法和逻辑上的系统审查。现有的一些校验工具(如DNSViz、ZoneCheck、ZLint等)能够辅助实现文献[36-39]、文献[41-43]等提出的针对悬挂域名、错误委派和循环依赖的检测。此外,DNS配置应采用可追踪、版本化的方式进行管理,借助基础设施即代码(infrastructure as code, IaC)方法提升配置的可审计性与一致性。结合文献[32-34]关于解析器配置缺陷的分析,以及文献[73-74]通过建设统一的监控与告警系统,可以实现对配置变更导致的解析失败的实时发现与快速响应。

配置错误缓解策略的核心优势在于整合性和预防性。相较于传统主要依赖人工逐项检查配置或仅在故障发生后进行排查的方法,上线前的系统性预防能够动态感知和快速定位由环境变化或隐性配置错误引发的故障。

4.3 域名信誉评分

域名滥用是导致DNS解析失败的重要原因,如第3.3节所述。针对不同类型的域名滥用,信誉评分机制可作为统一的检测与决策支撑框架,实现从被动响应到主动评估的转变。

针对域名抢注,可以通过部署的机器学习模型,针对拼写错误、组合抢注等特征进行模式识别,实现对抢注域名的分类识别与拦截。

针对过期域名滥用,可以通过在系统层面引入信誉评分机制(如Notos系统^[65]),辅助解析器决策是否尝试解析可疑域名;同时,利用生命周期建模算法(如Alembic^[53])加强注册机构对域名过期状态和所有权变更的监控。

针对恶意域名,通过构建多维检测防御体系,综合运用网络图关系建模^[57-58]、DNS查询响应行为异常识别^[30,59-60]、机器学习自动化检测^[63]和注册行为与生命周期建模^[64-65]等技术手段。此外,建立跨域的恶意情报共享机制,是打破信息孤岛、提升整体防御效能的关键路径。

综上,基于对域名滥用形态的系统分类,采用针对性检测技术以实现精准识别,引入动态信誉评分机制以支持灵活决策,并通过统一归因框架促进情报共享与协同防御,可应对域名滥用形式的多样性与关联性。

4.4 高可用部署架构

针对第3.4节分析的网络与管理问题,本文提出以下多维度的缓解策略。

1) 架构冗余与容错:建议DNS采用多路径、多上游服务器的架构设计,提升系统的容错与冗余能力。

2) 协议加密与隐私防护:基于Censored Planet^[66]、Iris^[68]、ICLab^[70]等平台提供的全球测量数据,针对解析路径干扰风险,可以部署DNS-over-HTTPS、DNS-over-TLS等加密协议来构建安全通道。同时,须关注加密DNS流量可能存在的侧信道分析风险^[67]并采取相应的流量混淆措施。

3) 广域调度与主动感知:在全球范围内部署Anycast技术可以显著提升解析服务的可达性与响应效率。文献[69]和[71]的研究启示我们,面向大规模分布式系统,可借鉴其关于全球部署架构与动态监测的思路,通过主动探测与被动监测手段及时发现网络异常,并优化策略的准确性和时效性。

综上所述,本文通过多路径容错与全球智能调度主动构建系统韧性,利用加密DNS抵御干扰与隐私风险,并借鉴全球测量方法论建立主动监控体系,从而为在复杂多变的全球网络环境中维持DNS解析的稳定性提供了系统化的解决途径。

4.5 小结

本节提出的缓解措施构成了针对不同DNS解析失败原因的分层防控体系。在协议实施层面,强调利用形式化分析、一致性测试和主动验证,确保解析器与权威服务器严格遵循标准并保持兼容性,从根源上减少故障风险。在配置管理层面,引入自动化配置生成与校验、版本化管理和实时监控,预防和快速定位人为失误或隐性配置错误引发的解析失败。在安全防御层面,针对域名滥用问题,结合模式识别、信誉评分、生命周期建模及威胁情报共享,实现精准识别与阻断。面对新型攻击行为,则通过负缓存机制、增强请求随机性、及时修补漏洞与流量异常检测等手段降低其影响。在网络环境与设施层面,对于网络与管理问题,建议采用多路径冗余、Any-

cast 部署、加密 DNS 及全球测量与主动监控相结合的方式, 提高解析的可达性与抗干扰能力。该体系兼具前瞻性与协同性, 既注重源头治理, 又强化动态防御, 从而系统性提升 DNS 解析的稳定性与安全性。

5 结束语

展望未来, 相关研究仍需在多个层面持续深化。在方法层面, 可以通过长期、跨域的数据测量与因果建模, 探索更具普适性和可验证性的分析框架。在实践层面, 应推动干预措施与验证机制的结合 (如借助真实网络部署或 A/B 测试等方法评估各项缓解措施的有效性)。在应用场景方面, 加密 DNS 的普及、IPv6 规模部署和物联网的快速发展, 将对解析失败治理提出新的挑战, 亟须发展实时异常检测、跨域信任机制和标准化诊断工具。

综上所述, 本文提出的分类框架与 DNS 解析失败缓解思路, 为 DNS 故障诊断和防护提供了系统化的分析视角与实践参考。

参考文献:

- [1] Park J, Khormali A, Mohaisen M, et al. Where are you taking me? behavioral analysis of open DNS resolvers[C]//Proceedings of the 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Piscataway: IEEE Press, 2019: 493-504.
- [2] Internet Engineering Task Force. Common DNS implementation errors and suggested Fixes : RFC1536[S]. 1993.
- [3] Internet Engineering Task Force. Observed DNS resolution misbehavior: RFC 4697 [S]. 2006.
- [4] Internet Engineering Task Force. Common DNS data file configuration errors: RFC 1537 [S]. 1993.
- [5] Internet Engineering Task Force. Common DNS operational and configuration errors: RFC 1912 [S]. 1996.
- [6] Internet Engineering Task Force. Operational considerations and issues with IPv6 DNS: RFC 4472[S]. 2006.
- [7] Xu W, Li X, Lu C Y, et al. TsuKing: coordinating DNS resolvers and queries into potent DoS amplifiers[C]//Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2023: 311-325.
- [8] Li X, Wu D S, Duan H X, et al. DNSBomb: a new practical-and-powerful pulsing DoS attack exploiting DNS queries-and-responses[C]//Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2024: 4478-4496.
- [9] Nosyk Y, Korczyński M, Duda A. Routing loops asMega amplifiers for DNS-based DDoS attacks[C]//Proceedings of Passive and Active Measurement. Cham: Springer, 2022: 629-644.
- [10] Nawrocki M, Jonker M, Schmidt T C, et al. The far side of DNS amplification: tracing the DDoS attack ecosystem from the Internet core[C]//Proceedings of the 21st ACM Internet Measurement Conference. New York: ACM, 2021: 419-434.
- [11] Li X, Xu W, Liu B J, et al. TuDoor attack: systematically exploring and exploiting logic vulnerabilities in DNS response pre-processing with malformed packets[C]//Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2024: 4459-4477.
- [12] Lu K Y, Chai T T, Xu H Y, et al. Research on unexpected DNS response from open DNS resolvers[J]. The Computer Journal, 2022, 65(9): 2276-2298.
- [13] Moura G C M, Müller M, Davids M, et al. Fragmentation, truncation, and timeouts: are large DNS messages falling to bits? [C]//Passive and Active Measurement. Cham: Springer, 2021: 460-477.
- [14] Nosyk Y, Korczyński M, Duda A. Extended DNS errors: unlocking the full potential of DNS troubleshooting[C]//Proceedings of the 2023 ACM on Internet Measurement Conference. New York: ACM, 2023: 213-221.
- [15] Afek Y, Bremner-Barr A, Peleg N. Poster: measuring open resolvers negative caching[J]. 2021.
- [16] Shafir L, Afek Y, Bremner-Barr A, et al. DNS negative caching in the wild[C]//Proceedings of the ACM SIGCOMM 2019 Conference Posters and Demos. New York: ACM, 2019: 143-145.
- [17] Zeng M, Zhu Y J, Li B Y, et al. Failed yet stored: a first look at DNS negative caching[C]//Proceedings of the 2024 IEEE International Performance, Computing, and Communications Conference (IPCCC). Piscataway: IEEE Press, 2025: 1-10.
- [18] Moura G C M, Heidemann J, De O Schmidt R, et al. Cache me if you can: effects of DNS time-to-live[C]//Proceedings of the Internet Measurement Conference. New York: ACM, 2019: 101-115.
- [19] Schomp K, Callahan T, Rabinovich M, et al. On measuring the client-side DNS infrastructure[C]//Proceedings of the 2013 Conference on Internet Measurement Conference. New York: ACM, 2013: 77-90.
- [20] De Vries W B, Scheitle Q, Müller M, et al. A first look at QNAME minimization in the domain name system[C]//Passive and Active Measurement. Cham: Springer, 2019: 147-160.
- [21] Magnusson J, Müller M, Brunstrom A, et al. A second look at DNS QNAME minimization[C]//Proceedings of the 24th International Conference on Passive and Active Measurement. Cham: Springer, 2023: 496-521.
- [22] Mbeve E S, Chavula J. On QoE impact of DoH and DoT in Africa: why a user's DNS choice matters[C]//Proceedings of International Conference on Towards new e-Infrastructure and e-Services for Developing Countries. Cham: Springer, 2021: 289-304.
- [23] Heftrig E, Schulmann H, Vogel N, et al. The harder you try, the harder you fail: the KeyTrap denial-of-service algorithmic complex-

- ity attacks on DNSSEC[C]//Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2024: 497-510.
- [24] Chung T, Rijswijk-Deij R V, Chandrasekaran B, et al. A longitudinal, end-to-end view of the DNSSEC ecosystem[C]//Proceedings of the 26th USENIX Security Symposium. Berkeley: USENIX Association, 2017: 1307-1322.
- [25] Van Adrichem N L M, Blenn N, Lúa A R, et al. A measurement study of DNSSEC misconfigurations[J]. Security Informatics, 2015, 4(8): 1-14.
- [26] Dai T X, Shulman H, Waidner M. DNSSEC misconfigurations in popular domains[C]//Proceedings of International Conference on Cryptology and Network Security. Cham: Springer, 2016: 651-660.
- [27] Wander M. Measurement survey of server-side DNSSEC adoption[C]//Proceedings of the 2017 Network Traffic Measurement and Analysis Conference (TMA). Piscataway: IEEE Press, 2017: 1-9.
- [28] 刘林晖, 涂菲帆, 陈勇, 等. 递归侧DNSSEC错误配置检测能力大规模探测分析[J]. 2024, 10(5): 81-94.
- Liu L H, Tu F F, Chen Y, et al. Large-scale measurement and analysis on misconfigurations of DNSSEC from recursive side[J]. Chinese Journal of Network and Information Security, 2024, 10(5): 81-94.
- [29] Zhang Q, Bai X, Li X, et al. ResolverFuzz: automated discovery of DNS resolver vulnerabilities with query-response fuzzing[C]//Proceedings of the 33rd USENIX Security Symposium. Berkeley: USENIX Association, 2024: 4729-4746.
- [30] Yang D H, Li Z Y, Jiang H Y, et al. A deep dive into DNS behavior and query failures[J]. Computer Networks, 2022, 214: 109131.
- [31] Lyu M Z, Gharakheili H H, Russell C, et al. Analyzing enterprise DNS traffic to classify assets and track cyber-health[J]. arXiv: 2201.07352, 2022.
- [32] Takano Y, Ando R, Takahashi T, et al. A measurement study of open resolvers and DNS server version[C]//Internet Conference (IEICE). 2013.
- [33] Müller M, Moura G C M, De O Schmidt R, et al. Recursives in the wild: engineering authoritative DNS servers[C]//Proceedings of the 2017 Internet Measurement Conference. New York: ACM, 2017: 489-495.
- [34] Ager B, Mühlbauer W, Smaragdakis G, et al. Comparing DNS resolvers in the wild[C]//Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement. New York: ACM, 2010: 15-21.
- [35] 郝逸航, 刘紫千, 常力元, 等. 基于Sketch的重要DNS查询缓存方法[J]. 网络与信息安全学报, 2024, 10(5): 95-106.
- Hao Y H, Liu Z Q, Chang L Y, et al. Sketch-based caching method for significant DNS queries[J]. Chinese Journal of Network and Information Security, 2024, 10(5): 95-106.
- [36] Liu D P, Hao S, Wang H N. All your DNS records point to us: understanding the security threats of dangling DNS records[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 1414-1425.
- [37] Zhang M M, Li X, Liu B J, et al. Detecting and measuring security risks of hosting-based dangling domains[J]. Proceedings of the ACM on Measurement and Analysis of Computing Systems, 2023, 7(1): 1-28.
- [38] Pappas V, Xu Z G, Lu S W, et al. Impact of configuration errors on DNS robustness[C]//Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications. 2004: 319-330.
- [39] Akiwate G, Jonker M, Sommesse R, et al. Unresolved issues: prevalence, persistence, and perils of lame delegations[C]//Proceedings of the ACM Internet Measurement Conference. New York: ACM, 2020: 281-294.
- [40] Sommesse R, Moura G C M, Jonker M, et al. When parents and children disagree: diving into DNS delegation inconsistency[C]//Passive and Active Measurement. Cham: Springer, 2020: 175-189.
- [41] Zhang Y Y, Liu B J, Duan H X, et al. Rethinking the security threats of stale DNS glue records[C]//Proceedings of the 33rd USENIX Security Symposium. Berkeley: USENIX Association, 2024: 1261-1277.
- [42] Jung J, Sit E, Balakrishnan H, et al. DNS performance and the effectiveness of caching[C]//Proceedings of the IEEE/ACM Transactions on Networking. Piscataway: IEEE Press, 2002, 10(5): 589-603.
- [43] Bojović P D, Gajin S. An approach to evaluation of common DNS misconfigurations[J]. arXiv:1711.05696, 2017.
- [44] Jiang J, Zhang J, Duan H X, et al. Analysis and measurement of zone dependency in the domain name system[C]//Proceedings of the 2018 IEEE International Conference on Communications (ICC). Piscataway: IEEE Press, 2018: 1-7.
- [45] Deccio C, Chen C C, Mohapatra P, et al. Quality of name resolution in the domain name system[C]//Proceedings of the 2009 17th IEEE International Conference on Network Protocols. Piscataway: IEEE Press, 2009: 113-122.
- [46] Nikiforakis N, Van Acker S, Meert W, et al. Bitsquatting: exploiting bit-flips for fun, or profit? [C]//Proceedings of the 22nd International Conference on World Wide Web. New York: ACM, 2013: 989-998.
- [47] Kintis P, Miramirkhani N, Lever C, et al. Hiding in plain sight: a longitudinal study of combosquatting abuse[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2017: 569-586.
- [48] Agten P, Joosen W, Piessens F, et al. Seven months' worth of mistakes: a longitudinal study of typosquatting abuse[C]//Proceedings 2015 Network and Distributed System Security Symposium. Internet Society, 2015.
- [49] Wang Y M, Beck D, Wang J, et al. Strider typo-patrol: discovery and analysis of systematic typo-squatting[J]. SRUTI, 2006.
- [50] Vissers T, Barron T, Van Goethem T, et al. The wolf of name street: hijacking domains through their nameservers[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2017: 957-970.
- [51] Lauinger T, Chaabane A, Buyukkayhan A S, et al. Game of regis-

- trars: an empirical analysis of post-expiration domain name take-overs[C]//Proceedings of the 26th USENIX Security Symposium. Berkeley: USENIX Association, 2017: 865-880.
- [52] Lauinger T, Onarlioglu K, Chaabane A, et al. WHOIS lost in translation: (mis)understanding domain name expiration and re-registration[C]//Proceedings of the 2016 Internet Measurement Conference. New York: ACM, 2016: 247-253.
- [53] Lever C, Walls R, Nadjji Y, et al. Domain-Z: 28 registrations later measuring the exploitation of residual trust in domains[C]//Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2016: 691-706.
- [54] Moore T, Clayton R. The ghosts of banking past: empirical analysis of closed bank websites[M]//Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2014: 33-48.
- [55] Hao S, Thomas M, Paxson V, et al. Understanding the domain registration behavior of spammers[C]//Proceedings of the 2013 Conference on Internet Measurement Conference. New York: ACM, 2013: 63-76.
- [56] 马永征, 李洪涛, 马中胜, 等. 防护性DNS服务关键技术研究综述[J]. 网络与信息安全学报, 2024, 10(5): 39-55.
Ma Y Z, Li H T, Ma Z S, et al. Survey on key technologies for protective DNS service [J]. Chinese Journal of Network and Information Security, 2024, 10(5): 39-55.
- [57] Khalil I M, Guan B, Nabeel M, et al. A domain is only as good as its buddies: detecting stealthy malicious domains via graph inference[C]//Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. New York: ACM, 2018: 330-341.
- [58] Kountouras A, Kintis P, Lever C, et al. Enabling network security through active DNS datasets[C]//Proceedings of Research in Attacks, Intrusions, and Defenses. Cham: Springer, 2016: 188-208.
- [59] Liu G N, Jin L, Hao S, et al. Dial “N” for NXDomain: the scale, origin, and security implications of DNS queries to non-existent domains[C]//Proceedings of the 2023 ACM on Internet Measurement Conference. New York: ACM, 2023: 198-212.
- [60] Gao H Y, Yegneswaran V, Chen Y, et al. An empirical reexamination of global DNS behavior[C]//Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM. New York: ACM, 2013: 267-278.
- [61] Fukuda K, Heidemann J. Detecting malicious activity with DNS backscatter[C]//Proceedings of the 2015 Internet Measurement Conference. New York: ACM, 2015: 197-210.
- [62] Qu J, Ma X B, Liu W M. Who is DNS serving for a human-software perspective of modeling DNS services[J]. Knowledge-Based Systems, 2023, 263: 110279.
- [63] Schuppen S, Teubert D, Herrmann P, et al. FANCI: feature-based automated NXDomain classification and intelligence[C]//Proceedings of the 27th USENIX Security Symposium. Berkeley: USENIX Association, 2018: 1165-1181.
- [64] Hao S, Feamster N, Pandrangi R. Monitoring the initial DNS behavior of malicious domains[C]//Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference. New York: ACM, 2011: 269-278.
- [65] Antonakakis M, Perdisci R, Dagon D, et al. Building a dynamic reputation system for DNS[C]//Proceedings of the 19th USENIX Security Symposium. Berkeley: USENIX Association, 2010.
- [66] Raman R S, Shenoy P, Kohls K, et al. Censored planet: an Internet-wide, longitudinal censorship observatory[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2020: 49-66.
- [67] Siby S, Juarez M, Diaz C, et al. Encrypted DNS $\Rightarrow$ privacy a traffic analysis perspective[J]. arXiv:1906.09682, 2019.
- [68] Pearce P, Jones B, Li F, et al. Global measurement of DNS manipulation[C]//Proceedings of the 26th USENIX Security Symposium. Berkeley: USENIX Association, 2017: 307-323.
- [69] Feal á, Vallina P, Gamba J, et al. Blocklist babel: on the transparency and dynamics of open source blocklisting[J]. IEEE Transactions on Network and Service Management, 2021, 18(2): 1334-1349.
- [70] Niaki A A, Cho S, Weinberg Z, et al. ICLab: a global, longitudinal Internet censorship measurement platform[C]//Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2020: 135-151.
- [71] Kogan D, Corrigan-Gibbs H. Private blocklist lookups with checklist[C]//Proceedings of the 30th USENIX security symposium. Berkeley: USENIX Association, 2021: 875-892.
- [72] Internet Engineering Task Force. Extended DNS errors: RFC 8914[S]. 2020.
- [73] Hendriks L, De Boer P T, Pras A. IPv6-specific misconfigurations in the DNS[C]//Proceedings of the 2017 13th International Conference on Network and Service Management (CNSM). Piscataway: IEEE Press, 2017: 1-5.
- [74] Liao X, Xu J, Zhang Q, et al. A comprehensive study of DNS operational issues by mining DNS forums[J]. IEEE Access, 2022, 10: 110807-110820.

[作者简介]



曾濛 (1998-), 男, 山东淄博人, 中国科学院信息工程研究所硕士生, 主要研究方向为网络空间测绘。



朱宇佳 (1984-), 女, 江苏无锡人, 博士, 中国科学院信息工程研究所副研究员, 主要研究方向为网络空间测绘、域名安全、网络大数据分析。



李白杨（1995-），男，河南平顶山人，中国科学院信息工程研究所工程师，主要研究方向为网络空间测绘、域名体系安全。



陈闻宇（1980-），男，江苏无锡人，博士，中国互联网络信息中心高级工程师，主要研究方向为互联网基础资源、网络安全、大数据和区块链技术。



王志洋（1984-），男，安徽枞阳人，中国互联网络信息中心高级工程师，主要研究方向为智能信息处理和互联网基础资源管理。



刘庆云（1980-），男，河北衡水人，博士，中国科学院信息工程研究所正研级高级工程师、博士生导师，主要研究方向为网络空间测绘、网络空间安全。