软件学报 ISSN 1000-9825, CODEN RUXUEW
*Journal of Software*,2024,35(1):309−332 [doi: 10.13328/j.cnki.jos.006898]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

# DNS 信道传输加密技术: 现状、趋势和挑战*

张 曼, 姚健康, 李洪涛, 董科军, 延志伟

(中国互联网络信息中心, 北京 100190)

通信作者: 姚健康, E-mail: yaojk@cnnic.cn

**摘 要**: DNS 作为重要的互联网基础设施, 其明文传输的特点带来很多隐私安全风险. DoH、DoT、DoQ 等 DNS 信道传输加密技术致力于防止 DNS 数据被泄露或篡改, 并保证 DNS 消息来源的可靠性. 首先从 DNS 消息格式、数据存储和管理、系统架构和部署等 6 个方面分析明文 DNS 存在的隐私安全问题, 并对已有的相关技术和协议进行总结. 其次分析 DNS 信道传输加密技术的实现原理及应用现状, 进而基于多角度评测指标对各加密协议在不同网络条件下的性能表现进行讨论. 同时通过填充机制的局限性、加密流量识别和基于指纹的加密活动分析等方向探讨 DNS 信道传输加密技术的隐私保护效果. 此外从部署规范、恶意流量对加密技术的利用和攻击、隐私和网络安全管理之间的矛盾, 以及加密后影响隐私安全的其他因素等方面总结 DNS 信道传输加密技术存在的问题、挑战和相关解决方案. 最后总结加密 DNS 服务的发现、递归解析器到权威服务器之间的加密、服务器端的隐私保护、基于 HTTP/3 的 DNS 等后续需要着重关注的研究方向.

**关键词**: 隐私; 安全; QUIC; TLS 1.3; DoH; DoT; DoQ

**中图法分类号**: TP393

中文引用格式: 张曼, 姚健康, 李洪涛, 董科军, 延志伟. DNS信道传输加密技术: 现状、趋势和挑战. 软件学报, 2024, 35(1): 309–332. http://www.jos.org.cn/1000-9825/6898.htm

英文引用格式: Zhang M, Yao JK, Li HT, Dong KJ, Yan ZW. Encryption Technologies for DNS Channel Transmission: Status, Trends and Challenges. Ruan Jian Xue Bao/Journal of Software, 2024, 35(1): 309–332 (in Chinese). http://www.jos.org.cn/1000-9825/6898.htm

## Encryption Technologies for DNS Channel Transmission: Status, Trends and Challenges

ZHANG Man, YAO Jian-Kang, LI Hong-Tao, DONG Ke-Jun, YAN Zhi-Wei

(China Internet Network Information Center, Beijing 100190, China)

**Abstract**: As critical Internet infrastructure, DNS brings many privacy and security risks due to its plaintext transmission. Many encryption technologies for DNS channel transmission, such as DoH, DoT, and DoQ, are committed to preventing DNS data from leaking or tampering and ensuring the reliability of DNS message sources. Firstly, this study analyzes the privacy and security problems of plaintext DNS from six aspects, including the DNS message format, data storage and management, and system architecture and deployment, and then summarizes the existing related technologies and protocols. Secondly, the implementation principles and the application statuses of the encryption protocols for DNS channel transmission are analyzed, and the performance of each encryption protocol under different network conditions is discussed with multi-angle evaluation indicators. Meanwhile, it discusses the privacy protection effects of the encryption technologies for DNS channel transmission through the limitations of the padding mechanism, the encrypted traffic identification, and the fingerprint-based encryption activity analysis. In addition, the problems and challenges faced by encryption technologies for DNS channel transmission are summarized from the aspects of the deployment specifications, the illegal use of encryption technologies by malicious traffic and its attack on them, the contradiction between privacy and network security management, and other factors affecting privacy and security after encryption. Relevant solutions are also presented. Finally, it summarizes the highlights

* 基金项目: 北京市科技新星计划 (Z191100001119113)
收稿时间: 2022-08-02; 修改时间: 2022-09-16, 2022-11-26; 采用时间: 2023-01-05; jos 在线出版时间: 2023-06-28
CNKI 网络首发时间: 2023-06-29

of future research, such as the discovery of the encrypted DNS service, server-side privacy protection, the encryption between recursive resolvers and authoritative servers, and DNS over HTTP/3.

**Key words**: privacy; security; quick UDP Internet connection (QUIC); TLS 1.3; DNS over HTTPS (DoH); DNS over TLS (DoT); DNS over QUIC (DoQ)

## 1 引 言

DNS 协议在设计之初并未考虑到安全性和隐私性, 其明文通信及缺少认证的特点被网络攻击、消息窃听和用户活动分析等行为所利用. 根据安全公司 CrowdStrike 的报告, 广泛发生的 DNS 劫持事件使得多个行业的众多组织曾受到影响, 其中包括不同国家的政府机构, 以及医疗健康、保险、民用航空、互联网服务等领域的基础设施提供商[1]. 美国实施的通信监听计划包含大量 DNS 数据, 其通过收集个人网络社交活动中的日志文件及身份信息, 来进行数据挖掘和情报分析. 国际数据等公司发布的最新 DNS 威胁评估报告显示, 88% 的公司或组织曾遭遇过 DNS 攻击, 并且各类型攻击 (例如 DNS 隧道、DNS 网络钓鱼、基于 DNS 的恶意软件) 的发生频率也都有所增加[2]. DNS 攻击造成的应用及服务宕机、客户敏感信息泄露等给各业务方造成了严重损失. 疫情加速了教育、医疗、协同办公等不同领域的数字化转型进程, 但也为攻击者提供了新的目标和焦点, 根据报告显示在新冠疫情期间医疗保健行业遭受了 DNS 攻击的严重影响, 给人民的生命和财产安全造成巨大威胁[3]. 部署适当的 DNS 隐私安全解决方案对提升网络安全性具有重要作用.

DNS 信道传输加密技术的提出致力于增强 DNS 消息的隐私安全性, 本文从技术原理、实施现状、性能表现、隐私保护效果以及可能存在的问题和挑战等方面对 DNS 信道传输加密技术的研究工作进行分析总结. 第 2 节对 DNS 隐私安全问题和已有的相关研究进行分析. 第 3 节分析了 DNS 信道传输加密技术的技术实现原理. 第 4 节分别从当前应用现状、加密技术的性能影响、隐私保护效果等方面对 DNS 信道传输加密技术进行总结. 第 5 节讨论了 DNS 信道传输加密技术的问题和挑战. 第 6 节对未来的趋势和研究方向进行了展望. 最后第 7 节进行了全文总结.

## 2 背景知识

### 2.1 DNS 存在的隐私安全问题

DNS 隐私安全威胁产生于以下几个方面: DNS 查询数据本身带来的信息泄露、通信路径和 DNS 服务器端的数据隐私问题, 以及在数据存储和管理、系统架构和部署等方面存在的隐患, 具体分类如图 1 所示.

DNS 请求消息中包括的有关查询发起人和查询内容的数据会造成信息泄露, 如 QNAME 会泄露用户请求的域名, 并且该字段中可能嵌入了使用的应用软件等标识信息; 客户端与递归解析器通信请求中的源 IP 地址字段包含了用户自身地址; 客户端子网扩展则会泄露原始查询方的网络地址信息等.

在通信路径上中间攻击者可以监听、截获、篡改 DNS 消息, 一方面明文 DNS 消息中数据未加密, 路径中的第三方可进行偷窥, 造成数据泄露; 另一方面传统 DNS 通信过程中缺少身份认证机制, 客户端无法验证响应来源的真实性; 此外由于缺少数据完整性校验, DNS 消息可能面临被篡改的风险.

在服务器端同样存在隐私安全问题, 根据域名解析整体流程, DNS 服务器分为递归解析器、根域名服务器、顶级域名服务器以及权威 (域名) 服务器. 递归解析器可由互联网服务运营商提供, 此外一些网络公司也对外发布公共递归解析器, 以供用户选择. 基于网络活动中庞大的用户和查询体量, 递归解析器和权威服务器掌握大量 DNS 请求数据, 能够在此基础上进行信息观察、收集和分析处理, 或传输给第三方用于研究、安全分析和网络审查等.

在数据存储和管理方面, 注册数据的公开一定程度上造成了域名注册方的信息泄露; 明文区传送使攻击者有机会通过窃听网络连接来收集区内容; 美国封锁伊朗域名等事件也反映了在区文件的管理和修改权限设置机制方面存在一定的不合理性.

在系统架构和部署方面, 存在中心化、集中化、软件漏洞等问题. 虽然各级服务中设置了缓存机制, 但根服务器作为 DNS 系统的中枢, 依然成为重要攻击目标; 近年来针对根服务器的大规模 DDoS 等攻击时有发生, 如攻击者通过控制众多僵尸机器, 导致多个根服务器离线数小时[4]. 在网络安全领域, 攻击方可利用网络中的受感染设备获取攻击能力, 但防御方则需要付出数倍的成本来进行防范机制的部署, 虽然以往的攻击事件暂未导致大规模断网事故, 但随着物联网的发展, 网络中将存在大量易受感染的设备, 使得未来潜在的攻击能力会迅速增长, 针对 DNS 的物联网僵尸网络的规模和复杂性将大大增加[5]. 同时解析服务存在集中化问题, 头部的少数服务商占据了巨大的市场份额, 掌握大规模的用户通信数据, 此外 DNS 服务器软件自身或系统中的其他网络设备可能存在安全漏洞.

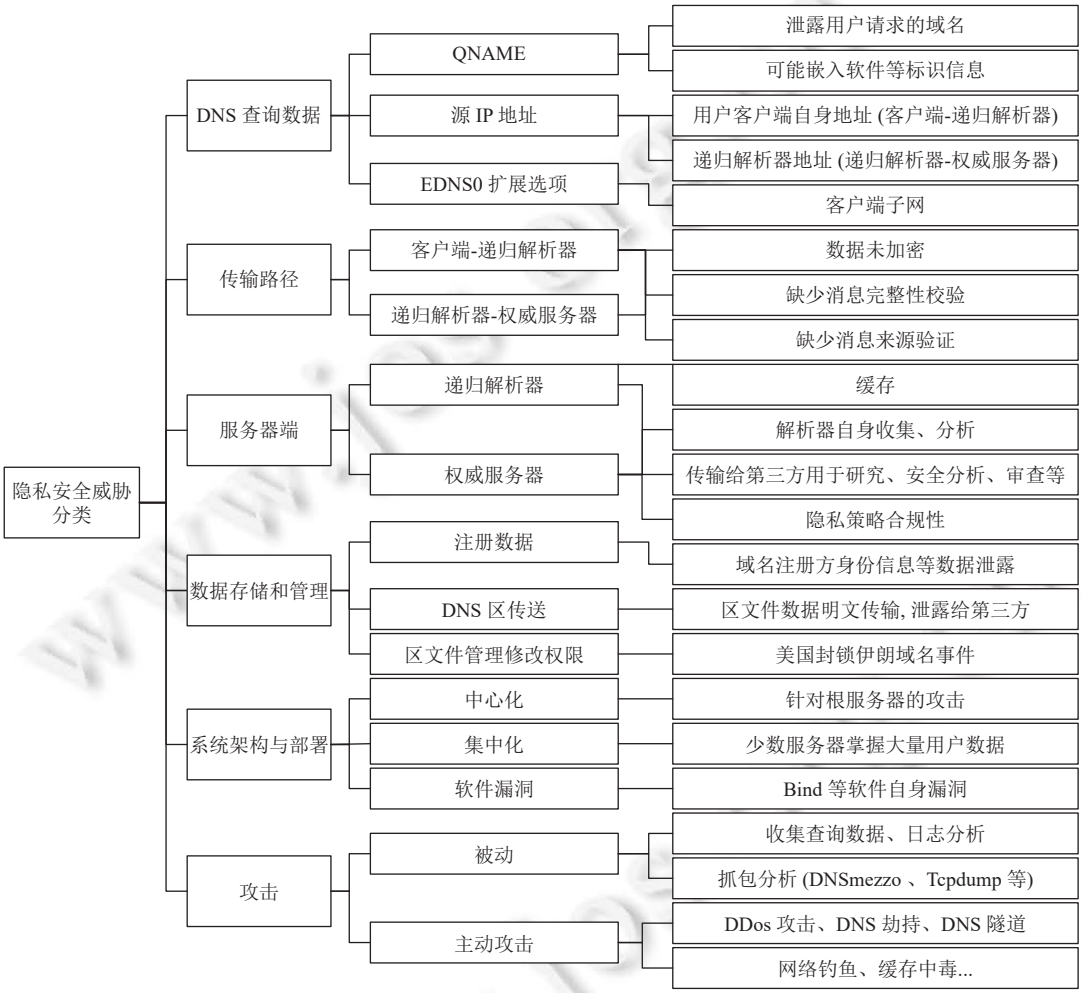


图 1 DNS 隐私安全问题分析

针对 DNS 的攻击分为被动攻击和主动攻击, 被动攻击可进行数据偷窥和分析, 包括查询数据及日志的收集, 抓包分析 (例如 DNSmezzo[6]、Tcpdump[7]) 等, 而主动攻击则可通过对查询请求过程进行直接的更改和破坏来实现攻击目的.

### 2.2 DNS 隐私安全增强相关研究

在 DNS 信道传输加密技术发布之前, 针对 DNS 存在的隐私安全问题 (参见第 2.1 节), 业内已开展了众多技术研究和方案设计[8,9]. 本节主要从解决的问题和技术架构实现等方面对已存在的技术协议进行分析和比较.

在增强通信路径上的隐私保护方面, DNSCrypt[10]和 DNSCurve[11]对 DNS 消息进行加密, 并在收到响应时进行来源验证, 保证 DNS 消息的机密性、真实性和完整性. DNSCurve 社区表示 DNSCurve 主要用于递归解析器和权威服务器之间, DNSCrypt 则多用于客户端和递归解析器之间, 二者除了采用的密钥交换和加密算法有差异外, 具体实现流程并无太大区别[11]. DNSCurve 基于 NS 资源记录进行公钥发布, 其密钥交换和加密算法分别为 Curve25519 和 XSalsa20-Poly1305, DNSCrypt 不同版本之间支持多种实现算法. DNSCrypt 和 DNSCurve 需要使用方进行密钥对的分发和管理, 部署成本较大, 并未被 IETF 标准化.

在缓解服务器端的数据收集方面, 应用较广泛的协议包括查询域名最小化 (query name minimization) 机制[12]. DNS 请求过程中, 递归解析器发至根服务器、顶级域名服务器及权威服务器的消息中都包括完整的请求域名, 查询域名最小化机制仅向各级服务器发送必要的信息 (例如在查询“www.example.com”时, 仅向根服务器发送“.com”域名信息), 以减少上级名称服务器获得的信息量. 该方案与原有 DNS 协议兼容, 部署较为方便, 但作用有限.

在保证 DNS 数据未经篡改且来源正确方面, IETF 推出了 DNS 安全扩展协议 (DNS security extensions, DNSSEC) 机制[13,14], 但它并未对消息进行加密. DNSSEC 利用非对称加密算法对 DNS 应答消息进行数字签名, 并通过父区对子区公钥做信任背书的机制, 在域名体系内逐级构建起信任链. DNSSEC 实现了 3 种功能, 包括为接收到的 DNS 响应消息提供来源认证、对 DNS 数据进行完整性校验, 以及对于不存在的名字和记录类型进行否定存在验证[13]. DNSSEC 定义了新的资源记录类型以实现上述功能, 分别为资源记录签名 (resource record signature, RRSIG)、DNS 公钥 (DNS public key, DNSKEY)、授权签名者 (delegation signer, DS)、NSEC (next secure). 其中 RRSIG 存放私钥对响应数据资源记录集的摘要信息进行签名后的结果. 在 DNS 区层次结构中, 每个区有一对公私钥, 区的公钥信息保存在 DNSKEY 资源记录中. 同时子区公钥的摘要信息会存储在父区的 DS 资源记录中, 用于逐级构建父区与子区之间的信任链. NSEC 通过指针方式对 DNS 区中存在的域名进行按序链接, 以证实某域名或数据类型不存在, NSEC3 则通过哈希机制来防止 NSEC 机制下的区遍历. 就部署情况而言, 虽然约 91% 的顶级域已部署 DNSSEC 验证服务, 但二级域部署率只占约 6%[15]; 此外虽然推出了 NSEC3, 但部分系统依旧部署先前的 NSEC, 存在区文件被遍历的风险.

为了确保服务器证书的合法性, 基于 DNS 的命名实体认证 (DNS-based authentication of named entities, DANE) 机制[16]被提出. DANE 实现的功能包括以下几个方面, 首先其能对 CA 机构进行限制, 允许客户端只接受特定 CA 机构签发的数字证书; 其次 DANE 能够对证书 (或公钥) 进行限制, 仅支持服务器使用特定的证书 (或公钥); 最后 DANE 支持信任锚点声明[16]. DANE 定义了 TLSA 资源记录类型, 其中包括 Cert.Usage (标识声明的类型)、选择符、匹配类型和证书关联数据 4 个选项字段. DANE 的实现需要依赖 DNSSEC 对其消息进行签名, DNSSEC 在二级域的低部署率对其推广应用产生了较大影响. 此外 DANE 会增加 TLS 连接过程的延时, 这也是阻碍其在高实时性业务中部署推广的因素.

在注册数据的隐私保护方面, 最初域名注册信息通过 WHOIS 协议[17]全部公开, 造成注册人敏感信息泄露, 改进的域名注册数据访问协议[18,19]中引入了多项安全机制. 首先, 其设立访问权限控制机制, 在匿名访问的基础上, 增加认证访问, 支持对客户端身份进行标识和验证, 同时对访问权限进行分级, 可根据用户身份和授权信息来实现数据的差异化或分层访问. 其次该协议增加了可靠性保障 (例如限制客户端特定时间内的查询频率等), 以及数据加密和完整性保护机制.

此外在新技术架构探索方面, 基于区块链的隐私安全机制也被用于名字空间领域. 它们利用区块链的合约、共识等特性对域名系统整体架构或其中一部分 (如根区管理) 进行改进, 或在区块链平台上构建去中心化、匿名性强的名字空间标识解析系统. 主要包括 Namecoin、Blockstack 名字系统、Handshake、以太坊名字服务等.

Namecoin[20]基于比特币链实现, 其采用键值对形式将数据存储在链上, 并定义了 NAME_NEW、NAME_FIRSTUPDATE、NAME_UPDATE 操作来完成域名注册流程, 其共识机制和挖矿算法设置与比特币类似. Namecoin 未开放顶级域申请, 仅支持“.bit”域下的域名注册. 它存在域名抢注等问题, 同时数据全部存储在链上, 对其性能和扩展性也带来一定的影响.

Blockstack 名字系统 (Blockstack name system, BNS)[21,22]将区块链底层实现、业务逻辑处理和数据存储进行

了解耦合, 底部区块链层负责存储基础的交易数据并实现共识等机制, 虚拟区块链层从底部区块链获取数据, 并进行业务逻辑的处理. BNS 设计去中心化的存储系统, 用户可以自由选择不同类型的存储服务商, 数据需加密存储并由所有者进行签名, 数据位置的指针和内容摘要信息保存在虚拟区块链层. 客户端发起访问请求后通过路由层进行数据查询, 并按照指针指示的存储位置进行数据读取, 此时需完成签名验证、摘要比对等校验, 以保证数据的安全和完整性. BNS 支持名字空间、各级子域的申请和注册, 但针对不同级别的域名, 其数据存储位置和管理机制存在差异.

Handshake[23]基于区块链架构实现 DNS 根域部分的管理, 它与 DNS 兼容, 不会替代现有 DNS 系统. Handshake 设计 Urkel 树进行数据存储索引, 并定义了拍卖、公示、资金退回、转移、更新等一系列智能合约来完成域名的拍卖注册和续签等流程. Handshake 支持个人注册顶级域名, 同时为了保持与现有 DNS 系统的兼容性, DNS 中已存在的顶级域以及部分公司和组织机构的域名被禁止注册.

以太坊名字服务 (Ethereum name service, ENS)[24,25]用可读性强的名字替代以太坊中原有的随机字符串, 来表示地址信息. 支持“.eth”顶级域下的域名注册管理, 同时 ENS 正在进行与 DNS 顶级域的集成, 集成完成后将支持其他顶级域下的域名注册.

对新系统架构的探索不止局限在区块链领域, GNU 名字系统[26,27]对 DNS 系统结构进行了重新设计, 致力于提供去中心化、抗审查和隐私增强的方案, 并能与当前 DNS 系统兼容. GNU 名字系统中每个区与加密密钥对一一对应, 密钥作为区的唯一标识; 同时其采用去中心化数据存储方式, 区内容经过加密和签名后以键值对的形式进行存储. GNU 名字系统新定义了一系列资源记录类型用于域解析授权、重定向等操作, 同时为了支持与 DNS 的互操作, 其定义了 GNS2DNS 资源记录, 以获取解析特定名字所需的 DNS 服务器信息.

上述技术的比较和总结如表 1 所示. 这些方案从不同方向对 DNS 隐私安全进行改进和探索, 部分协议由于推广部署成本较大暂未得到大规模应用. DNS 作为重要的互联网基础资源, 规模结构庞大, 直接进行新架构的切换难以实现, 基于区块链等的新架构研究也需要加强与现有 DNS 兼容整合的探索.

表 1　DNS 隐私安全增强相关技术

| 类别 | 特点 | 技术/协议 | 目标 | 描述 |
|---|---|---|---|---|
| 协议增强 | 未标准化 | DNSCrypt | 消息加密、利用签名验证服务器身份, 并防止消息篡改 | 用于DNS客户端和递归解析器之间, 推广部署成本较大, 未标准化 |
| | | DNSCurve | | 使用椭圆曲线加密算法, 基于NS资源记录进行密钥分发; 安全、运算速度较快; 推广部署成本较大, 未标准化 |
| | 标准化协议 | Query name minimization | 向各级服务器发送请求时仅提供当前步骤必需的域名标签集, 非必要情况下不发送完整域名信息 | 域名最终仍会暴露, 不能避免第三方窥探和权威服务器端的隐私泄露 |
| | | DNSSEC | 消息来源验证, 消息签名, 数据防篡改; 否定存在验证 | 数据未加密 |
| | | DANE | 限制或声明证书、CA机构、信任锚等的范围 | 定义TLSA资源记录, 依赖DNSSEC, DNSSEC在二级域上的低部署率对其推广应用影响较大 |
| 新架构探索 | 基于区块链的架构 | Namecoin | 基于区块链的名字标识解析系统 | 基于比特币链实现, 开放“.bit”域下域名注册, 不支持顶级域申请, 存在域名抢注等问题 |
| | | BNS | 致力于利用区块链技术架构来重构DNS | 底层链和Stacks链两层区块链结构, 数据不全部存储在链上; 支持名字空间及其下的子域申请, 并制定价格规则; 定义了去中心化存储系统 |
| | | Handshake | 不改变DNS架构, 仅对根区管理模块进行优化 | 基于区块链进行根区管理, 支持顶级域及子域申请, 与DNS兼容, 保留DNS中已有的域名 |
| | | ENS | 探索以太坊地址等资源标识解析 | ENS中正在添加对DNS中顶级域的支持 |
| | 其他 | GNS | 重新设计DNS架构, 构建去中心化、抗审查、提供隐私增强保护的名称系统 | 可与DNS集成和兼容, 建立于GNUnet之上, 每个区由区域键唯一标识, 定义了完整的密钥管理、加密、签名和域解析机制 |

## 3 DNS 信道传输加密技术原理

在第 2.1 节所述的威胁分类中, DNS 通信路径上的隐私安全保护具有比较重要的作用, 在客户端与递归解析器以及递归解析器与权威服务器之间的通信过程中, 对 DNS 消息实施监听、截获、篡改是多种攻击类型得以实现的落脚点. 即使 DNS 数据查询权限和结果本身是公开的, 但是用户的单个或一系列查询行为不应该公开[28]. 表 2 介绍了 DNS 隐私安全相关的国际标准制定情况, 为了增强传输路径上的隐私保护, IETF 先后制定了基于 HTTPS 的 DNS (DNS over HTTPS, DoH), 基于 TLS 的 DNS (DNS over TLS, DoT) 和基于 QUIC 的 DNS (DNS over QUIC, DoQ) 等 DNS 信道传输加密协议. DNS 信道传输加密旨在从隐私、身份认证、数据完整性等方面改善 DNS 数据安全并最大限度地减少网络运营商等对 DNS 流量的分析. 其中隐私部分防范 DNS 数据被偷窥或泄露, 身份认证机制确保数据在合法用户之间交互, 数据完整性验证防止消息被篡改.

表 2 DNS 隐私安全协议

| 条目 | 日期 | 描述 |
|---|---|---|
| RFC 7258 | 2014-05 | Pervasive monitoring is an attack |
| RFC 7816 | 2016-03 | QNAME minimization |
| RFC 7830 | 2016-05 | The EDNS(0) padding option |
| RFC 7858 | 2016-05 | DNS over TLS |
| RFC 7873 | 2016-05 | Domain name system (DNS) cookies |
| RFC 8094 | 2017-02 | DNS over DTLS |
| RFC 8310 | 2018-03 | Usage profiles for DNS over TLS and DNS over DTLS |
| RFC 8467 | 2018-10 | Padding policies for extension mechanisms for DNS (EDNS(0)) |
| RFC 8484 | 2018-10 | DNS over HTTPS |
| RFC 8932 | 2020-10 | Recommendations for DNS privacy service operators |
| RFC 9076 | 2021-07 | DNS privacy considerations |
| RFC 9103 | 2021-08 | DNS zone transfer over TLS |
| RFC 9114 | 2022-05 | HTTP/3 |
| RFC 9250 | 2022-05 | DNS over dedicated QUIC connections |

### 3.1 DoH 技术原理

RFC 8484[29]定义了 DoH 的技术规范, DoH 使用 HTTPS 协议进行 DNS 消息数据的传输, 所有 DNS 请求和响应都在 HTTP 数据包中进行编码, 其推荐的 HTTP 最低版本为 HTTP/2, 并使用 443 端口. DoH 中通过 HTTPS URL 发送 DNS 请求, 服务器需要支持一个或多个 URI 模板. 此外所有 DoH 服务器和客户端必须支持 application/dns-message 类型, 它本质上是 HTTPS 对 DNS 格式的封装. 另一种广泛支持的类型是 application/dns-json, 表示 JSON 格式的 DNS 消息, 但不强制要求服务器支持该格式.

在使用 DoH 时, 如果加密递归解析器的地址未知, 客户端与 DoH 服务器的通信过程将分为 URI 解析和双方通信两个阶段, URI 解析阶段浏览器通过发送非加密 DNS 请求来获取 DoH 服务器的 IP 地址信息, Do53 所面临的域名劫持等各种隐私安全风险在这个阶段同样存在. 双方通信阶段客户端与 DoH 服务器建立 TLS 连接, 通过 HTTPS 发送加密 DNS 查询请求.

DoH 不仅仅是基于 HTTP 的隧道, 其允许将 DNS 记录集成到具有缓存、重定向、代理、身份验证和压缩等机制的 HTTP 生态系统中, 例如扩展 DoH 功能支持从服务器推送 DNS 数据选项, 此外递归解析器的选择权转移到了 Web 浏览器等应用, 对底层操作系统透明. 一些公共服务器列表[30]汇总了当前已部署的 DoH 公共递归解析器, 用户可自行进行选择.

### 3.2 DoT 技术原理

DoT[31,32]是通过 TLS 连接发送 DNS 数据, 利用 TLS 实现 DNS 消息的加密和认证, 默认使用 853 端口. 由于数据包通过专用端口发送, 因此网络管理员比较容易实现针对 DoT 流量的识别、阻止或过滤, RFC 标准中允许其

使用 853 以外的端口. DTLS 在 UDP 之上实现, 基于 DTLS 的 DNS 能够避免 TCP 中的队头阻塞等问题, 已发布为实验性协议[33]. 此外, DNS 区传送原本以明文形式传输, 攻击者可通过窃听网络连接收集区文件内容; DNS TSIG (transaction signature, 事务签名) 机制将直接的区域传输对象限制为仅授权的客户端, 但其未增加数据机密性保护. 基于 TLS 的区传送使用 TLS 来防止对区传送的被动监控和数据收集[34].

DoT 和基于 DTLS 的 DNS 支持两种隐私配置模式, 如表 3 所示: 严格模式和机会主义隐私模式, 严格模式要求加密和认证必须同时完成, 能够有效地防范主动和被动攻击者; 机会主义模式允许在加密和认证不能同时实现时支持不经过身份认证直接进行消息加密, 进一步支持回退到明文传输. 仅加密模式能够提供针对被动攻击的保护, 但并不能有效地防范主动攻击.

表 3 机会加密设置机制

| 配置模式 | 支持的操作类型 |
|---|---|
| 严格模式 | 加密并经过身份认证的传输 |
| 机会加密模式 | 加密并经过身份认证的传输<br>加密传输, 未经过身份认证<br>明文传输 |

### 3.3 DoQ 技术原理

TCP 协议应用非常广泛, 但也存在一些问题, 包括建立连接的握手延迟、队头阻塞等, 但是由于涉及操作系统内核层面, 同时网络中各种类型的设备需进行更新支持, 其功能改进和迭代都比较困难. HTTP/2 虽然通过多路复用机制解决了应用层的队头阻塞问题, 但在传输层 TCP 协议中该问题依然存在. TCP 虽然存在一些问题, 但是创建新的传输层协议并非易事, 牵一发而动全身, 需要网络系统中各方的支持, 涉及巨大的成本和工作量.

快速 UDP 网络连接 (quick UDP Internet connection, QUIC) 协议即在上述背景下提出, 一方面网络的场景和内容越来越复杂, 另一方面当前广泛使用的协议中几个由来已久的问题和矛盾变得越来越突出, QUIC 希望能更好地解决上面的问题, 进一步提升网络传输效率和响应速度. 它最初由 Google 提出, 该版本被称作 gQUIC, gQUIC 自定义了一套加密认证机制, 后在 IETF 进行整合改进. 2021 年 IETF 版本的 QUIC 发布为 RFC 9000, 并相继发布 QUIC 的丢包检测与拥塞控制、TLS 集成、头部压缩等系列标准[35–37]. 由于新建传输层协议部署困难太大, QUIC 在 UDP 基础上实现了加密可靠传输, 通过内部集成 TLS 保证数据安全. 此外基于 QUIC 的 HTTP 被命名为 HTTP/3, 并于 2022 年发布为 RFC 9114[38].

QUIC 将多路复用的机制下移到传输层, 定义流 (stream) 表示连接中传输有序字节的单向或双向通道, 每个连接同时支持多个流; 不同流之间相互独立, 一个数据包丢失仅会影响该包涉及的流, 不会对其他数据包中未涉及的流产生影响. 流是一种逻辑概念, 数据携带由不同类型的帧 (frame) 完成, 例如 CRYPTO 帧 (类型=0x06) 用于传输加密握手消息, STREAM 帧用来隐式的创建一条流并携带流数据发送. 同时帧会标识出自己属于哪个流, 多个帧可能归属于一个逻辑流. 帧包含在 QUIC 数据包中, QUIC 数据包封装在 UDP 数据报中, 单个 UDP 数据报可以封装一个或多个 QUIC 数据包, 其数据封装结构如图 2 所示. 同时 QUIC 设置了流和连接两个级别的流量控制机制, 通信双方可通过流量调节帧的交互, 动态的实现流量阈值管控的调整.

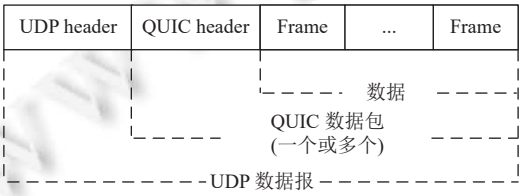


图 2 QUIC 数据传输结构

QUIC 连接基于连接 ID 进行标识, 而非地址端口信息, 不与网络路径进行绑定. 客户端在不同网络之间 (例如 Wi-Fi 和蜂窝网络) 进行切换时支持连接迁移, 无需重新建立连接. 由于集成了 TLS 1.3, QUIC 在首次连接时支持 1-RTT 握手, 并在后续连接中可实现 0-RTT 握手, 不过 0-RTT 可能存在重放攻击等安全风险.

相比于 TCP, QUIC 拥塞控制的算法和参数选择机制更加灵活, TCP 中重传数据包跟原始数据包的序列号一致, 接收端收到重传包后难以辨别该包是重传还是延迟过来的包, 造成往返时间 (round-trip time, RTT) 计算不准确. 而 QUIC 中数据包的编号单一递增, 丢包后重传包与原包号不一致. 同时 QUIC 中已经确认的数据包不支持取消确认, 并且支持更大的确认范围. 此外, TCP 中未计算接收端接收到数据包至发送确认之间的延迟时间, QUIC 中对这段时间进行了包含, 使得 RTT 计算更加准确.

基于 QUIC 的 DNS[39]把 DNS 请求和响应消息在 QUIC 中进行映射, 例如一个 DNS 请求响应映射到一个 QUIC 流中, 利用 QUIC 为 DNS 提供隐私保护功能. 为了避免与明文 DNS 混淆, DoQ 禁止使用 53 端口, 其默认端口为 853, 同时建议在客户端与递归解析器的通信中可协商使用 443 端口, 以避免基于端口号的流量拦截. 由于通信过程中可能会在一个 QUIC 数据包中传输多个包含不同 DNS 消息的 STREAM 帧, 在进行消息填充时应按照数据包粒度进行填充设置. 此外 QUIC 内部集成了 TLS, 如果 DoQ 连接建立失败, 它会首先尝试回退到 DoT, 如果还不行, 再回退到明文传输.

### 3.4 TLS 1.3

DoH、DOT 和 DoQ 都建立在 TLS 的基础上, 2008 年 TLS 1.2[40]发布, 成为目前广泛部署的 TLS 版本, 2018 年 RFC 8446[41]推出 TLS 1.3 版本. 与 TLS 1.2 相比, TLS 1.3 简化了密码协商模型并且规范了密钥协商的选项, 例如其将 Diffie-Hellman 算法的参数选择限制在已知的可选安全范围内, 客户端在发送第 1 条消息时便可以自己选择密钥参数, 而不用像 TLS 1.2 需要先等服务器确认其支持的选项, 节省协商交互时间. 同时由于 RSA 密钥交换不具有前向安全性, TLS 1.3 中已不再支持该算法. 此外 TLS 1.3 在密钥协商完成后即对后续握手消息和扩展选项进行加密, 并在非首次连接时支持 0-RTT 数据传输. 但是 0-RTT 可能带来一些问题, 一方面攻击者可以重放 0-RTT 数据, 并根据接收服务器的行为推测其内容; 另一方面是 0-RTT 机制依靠 TLS 恢复, TLS 恢复会使连续的客户端会话之间具有可链接性.

### 3.5 比较和总结

根据第 3.1–3.4 节中对各协议技术原理的分析, 在此基础上, 本节分别从架构层次、端口设置、流量隐蔽性、协议特点、DNS 服务选择权、适用场景等方面对 DNS 信道传输加密协议进行比较 (参见图 3 和表 4).

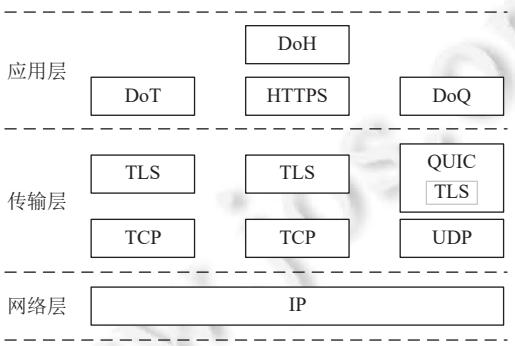


图 3 DoH、DoT、DoQ 框架图

图 3 为各协议的架构层次图, DoH 和 DoT 使用的传输层协议为 TCP, 而 DoQ 则在 UDP 基础上实现. 如表 4 所示, 由于 DoH 使用与 HTTPS 相同的端口号, 相对于 DoT 流量, 其具有更高的隐蔽性. 传统 DNS 递归解析器的选择在操作系统层面, DoH 将递归解析器的选择权转移到了浏览器等应用层面, 不同应用之间可以独立进行递归解析器选择, 互联网公司、ISP 等机构对特定技术的选择和支持一定程度上会从自身利益出发.

表 4 协议比较

| 协议 | DoH | DoT | DoQ |
|---|---|---|---|
| 默认端口 | 443 | 853 | 853 |
| 隐秘性 | 与HTTPS具有相同的端口号, 具有一定的隐蔽性 | 易被防火墙等屏蔽 | 易被防火墙等屏蔽(可协商使用443端口) |
| 特点 | 需要URL标识 | 相较DoH, 无需架构在HTTPS应用层之上 | 多路复用、拥塞控制、丢包检测等方面进行了优化 |
| DNS服务选择权 | 浏览器等应用 | 操作系统层面 | 操作系统层面 |
| 传输层协议 | TCP | TCP | UDP |
| 加密与身份认证 | TLS | TLS | TLS |
| 目前应用场景 | 客户端到递归解析器之间的通信路径 | 客户端到递归解析器之间的通信路径 | 客户端到递归解析器之间的通信路径 |
| 支持的场景 | 客户端到递归解析器之间的通信路径 | 递归解析器到权威服务器之间的通信路径、区传送等 | 递归解析器到权威服务器之间的通信路径、区传送等 |

DoH、DoT 和 DoQ 当前暂时多应用于 DNS 客户端和递归解析器之间的通信, 旨在防御路径上的攻击者, 并未解决 DNS 服务器端的隐私安全问题. 各服务器仍能看到所有请求, 用户应谨慎选择具有良好隐私策略的提供商. 此外 DoQ、DoT 等协议也支持递归解析器与权威服务器之间的通信保护.

## 4 DNS 信道传输加密技术分析

第 3 节总结了 DNS 信道传输加密技术的实现原理, 加密协议发布后引发关注的问题主要包括以下方面 (如图 4 所示).

首先各技术推出之后包括 DNS 解析服务商在内的网络基础设施和资源提供方的态度如何, 以及新协议当前的部署应用状态处于什么程度.

其次相对于传统 DNS, DoH 和 DoT 需要多次 TCP 及 TLS 握手来建立连接, 以保证安全可靠传输, 加密服务部署后性能表现如何, 与传统 DNS 相比, 是否会有较为明显的响应延迟问题. DoQ 虽然基于 QUIC 实现, 理论上从架构层面降低了握手等延迟, 那么相较于 DoH 和 DoT, DoQ 在实际表现中是否确实具有明显的优势.

此外加密协议致力于增强消息的机密性和安全性, 实际的隐私保护效果如何, 对加密消息的识别和分析是否存在可能.

基于上述问题, 本节主要从实施现状、性能影响、隐私保护效果等方面对 DNS 信道传输加密技术进行分析和讨论, 总体结构如后文图 4 所示.

### 4.1 现状分析

加密协议推出后其部署情况如何以及加密流量在网络中的占比也是研究者关注的方向. 2019 年初, Google 宣布在其公共递归解析器中支持 DoT[42]. 2020 年 2 月, Firefox[43]开始默认为美国用户推出 DoH 服务, 提供 Cloudflare (默认) 和 NextDNS 两个服务提供商. 随后 Chrome 浏览器[44]等应用、Apple[45]、Android[46]及 Windows 操作系统[47]相继添加了对加密解析的支持.

探测公共加密递归解析器部署情况可采用的方法主要分为几类 (如表 5 所示), 首先技术人员维护了一些公共加密服务器列表 (例如文献 [26]), 其中分类列举了已提供加密协议的厂商和对应的解析服务, 不过这些列表存在更新延迟和覆盖不全面等问题. URL 推测方法主要用于 DoH, 利用服务提供商的 DNS 递归解析器域名和 RFC 8484 中建议的 URL 字段设置的格式特征, 有针对性地进行加密协议的探测.

利用现有非加密服务器可用来发现原服务器中是否添加了对加密协议的支持, 跨协议探测则是发现加密服务器对其他协议的支持情况, 这两种方法都需要服务器通过特定机制 (如指定的资源记录等) 来发布自身属性信息, 并且通信双方就上述机制达成一致.

对加密服务部署情况的全面评估则多采用端口扫描法, 它基于加密协议的端口设置特征进行探测发现, 整体

步骤如表 6 所示. 例如 DoT 主要是在 853 端口上进行全网扫描, 而 DoH 则是在 IPv4 地址空间中扫描发现 443 端口打开的服务器, 同时借助反向 DNS 记录和被动 DNS 数据等得到递归解析器名等识别信息, 然后通过脚本对每个 IP 地址执行多个 DoH 请求, 并对答案进行评估, 以此为依据辨别哪些是真正的 DoH 服务器. 此外有研究者在请求步骤中同时设置了服务器名称标识 (server name indication, SNI) 字段值[48], 以便能够正确访问多托管服务器. 最后通过响应消息验证等来确认各个服务器支持的 DoH 协议功能和属性.

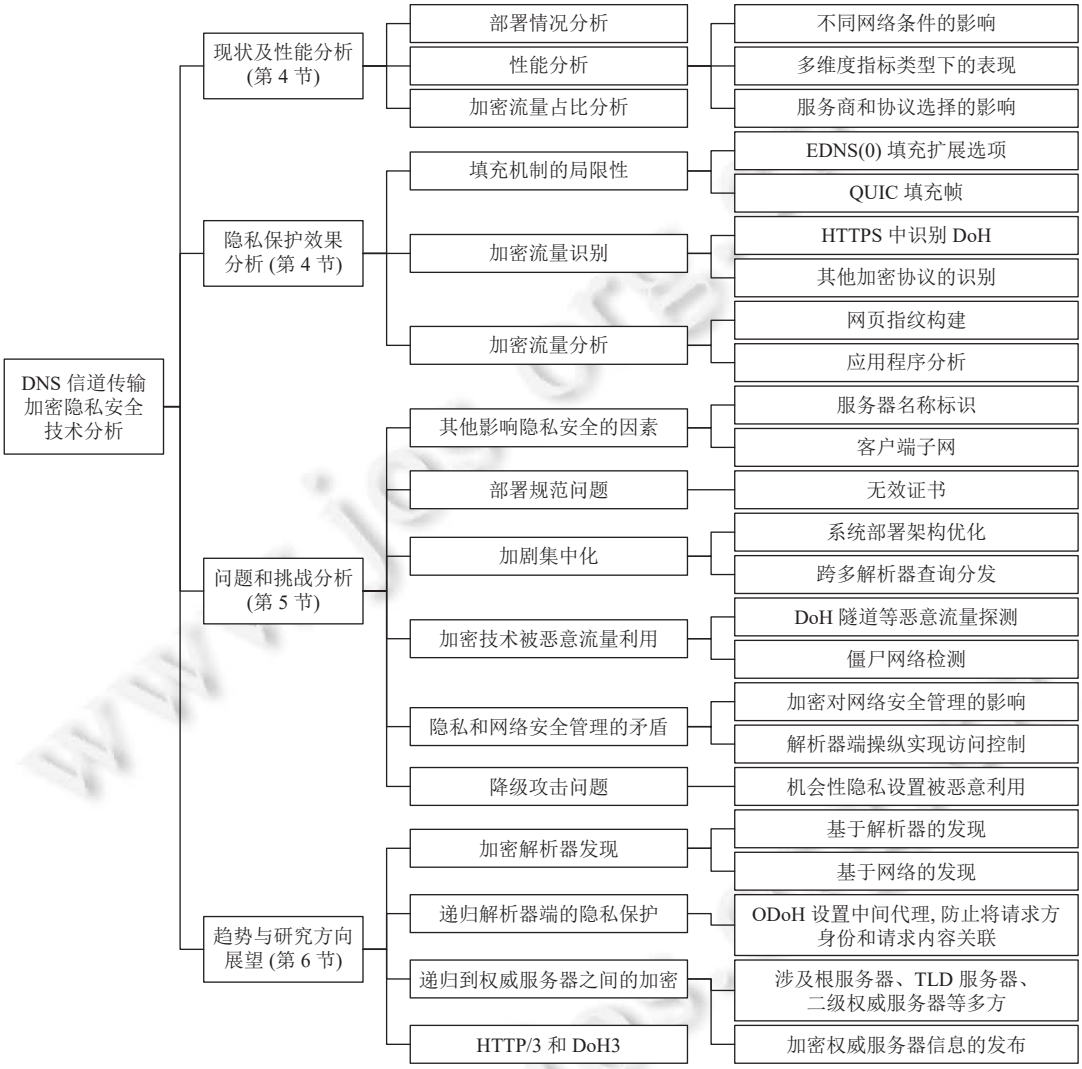


图 4 DNS 信道传输加密技术分析框架图

表 5 公共加密 DNS 服务器探测方法分类

| 方法 | 描述 |
|---|---|
| 公共服务器列表 | 例如文献[26] |
| URL推测 (DoH) | 基于URL探测网络中加密递归解析器和流量 |
| 根据现有非加密服务器信息探测加密服务器信息 | 服务器通过通信双方协商好的机制 (如指定的资源记录)将自身属性信息发布给客户端 |
| 已部署的加密服务器探测其他协议支持情况 | |
| 端口扫描后发送加密请求 | 见表6 |

表 6 端口扫描探测公共加密递归解析器流程

| 步骤 | 描述 |
|---|---|
| 端口扫描 | IPv4地址空间内用默认端口进行全网扫描 |
| 反向解析 | 根据扫描得到的IP地址, 通过反向解析等方法得到对应域名信息 |
| 发送加密DNS请求 | 向端口扫描得到的IP地址发送加密DNS请求 |
| 加入SNI字段 | 发送请求时加入域名信息至SNI字段[48] |
| 响应信息验证 | 对接收到的响应消息进行资源记录、证书等的校验 |

Lu 等人[49]发现 2019–2020 年一年多的时间里 DoT 递归解析器的数目由 2 000 增至约 7 800, 分属 1 200 多家服务提供商, 在此期间 DoH 服务提供商的数目也增加了一倍多. García 等人[50]通过全网扫描发现的 DoH 服务器比目前公共服务器列表中记录的多出近 4 倍 (按 IP 地址计算, 实际不同的 IP 可能对应同一个递归解析器名).

Luo 等人[48]在开放递归解析器的探测过程中, 通过端口扫描向潜在 IP 地址发送加密 DNS 请求, 并在请求中将上述 IP 对应的域名信息加入 SNI 字段中, 结果共发现 5.7k 个 DoH 递归解析器和 9.6k 个 DoT 递归解析器, 但约 30% 的解析器不能得到正确响应. Kosek 等人[51]从 2021 年中到 2022 年初探测到 DoQ 递归解析器的数目增长了 46%, 达到 1 217, 同时由于 QUIC 协议的 RFC 发布前历经众多版本的改进, 因此在探测期间服务的迭代和更新波动比较频繁.

加密流量在整个网络中的占比方面, 2019 年 Cloudflare 公布其公共递归解析器上加密流量的占比为 8%. 有研究者测量欧洲大型 ISP 服务商、大学、全球安全公司中的 DoH、DoT、DoQ 流量情况及分布, 发现上述 3 个组织中 Do53 流量至少比加密 DNS 流量多 3 个数量级, 探测结果很少发现 DoQ 流量[50].

在对公共加密递归解析器的评估及其支持的功能集方面, 虽然 DoH 中未强制要求使用特定的 URL 路径, 但从服务运营商的选择趋势变化上, 大家更趋向于选择统一的基准路径段, 以避免太多的 URL 令人困惑并可能产生配置错误[52].

### 4.2 DNS 信道传输加密技术性能分析

DoT 和 DoH 都基于 TCP 和 TLS 运行, 需要多次握手协商, 此外加密协议需要 DNS 服务器对查询消息进行解密, 并对待发出的响应消息进行加密, 这进一步增加了 DNS 服务器的开销. DNS 信道传输加密技术会对性能、服务器负载和用户体验产生怎样的影响是值得关注的问题.

2018 年, Mozilla 基于真实浏览器用户数据对 Firefox 的 DoH 响应时间进行了大规模测量, 发现大多数查询 DoH 比 Do53 慢 6 ms[53]. 但是 Mozilla 的测试只是关于 Cloudflare 的 DoH 递归解析器, 未包括网络延迟、吞吐量等因素对加密服务器性能影响的探索.

为了更加全面地对加密协议的性能特点进行分析, 研究者[49,51−56]在网络环境选择方面覆盖了大学网络、代理网络、云数据中心、家庭网路, 以及蜂窝网络和有损网路等. 性能分析指标分为传输数据量、加密协议连接建立时间、DNS 查询的响应时间、网页加载时间等. 在实际的分析测试过程中, 连接重用的使用程度, 厂商和协议选择之间的差异, 及测量时的网络状态等因素也会对性能结果产生一定的影响.

#### 4.2.1 加密协议对响应时间和页面加载时间的影响

本节从数据包和传输字节的开销、队头阻塞问题的影响、解析响应时间及页面加载时间等方面分析评估加密协议的属性特征和性能表现情况, 如表 7 所示.

在数据包和传输字节开销对比方面, Böttger 等人[52]通过大学网络测试发现通常情况下访问网页时发送的总 DNS 查询数目是网页数量的 20 多倍, 单个 DoH 交换消耗的字节数是 Do53 的 30 倍以上, 数据包的数量大约是 Do53 的 15 倍左右. 连接复用情况下 DoH 消耗的字节和数据包数量仍约是传统 DNS 的 4 倍多.

通过分析研究者发现队头阻塞问题会为各协议带来一定的影响[52], DoH 推荐的 HTTP 最低版本为 HTTP/2, 相比于 HTTP/1.1, HTTP/2 解决了应用层的队头阻塞, 但由于在传输层 TCP 协议感知不到上层协议的多路复用机

制, 该问题并未彻底解决. 同时虽然不经常发生, 队头阻塞问题也存在于 TLS 中, QUIC 协议将多路复用机制下移到传输层, 并将 TLS 的加密粒度改为按包加密, 以缓解上述问题.

表 7 性能分析

| 指标 | 条件 | 分析 |
|---|---|---|
| 数据包和传输字节开销 | 大学网络, Alexa全球排名前100 000的网页 | 字节数、数据包数目加密流量为Do53的十几倍至几十倍; 连接复用情况下降至约4倍多 |
| 队头阻塞的影响 | DoH、DoT、Do53全球多点部署 | HTTP/1.1受影响较大; HTTP/2、QUIC进行了改进 |
| DNS响应时间 | | 由于建立连接、消息加解密等, DoH、DoT高于Do53 |
| 页面加载时间 | | 通过连接重用、技术优化等DoH、DoT与Do53页面加载时间的差异不太明显 |
| 网络条件的影响 | 模拟蜂窝4G网络、有损蜂窝4G网络及3G网络; 美国家庭网络 | 随着网络吞吐量的下降和损耗增加, DoT和DoH的性能表现有明显的下降; 有损网络条件下DoH具有更高的失败率和错误率 |
| 不同提供商、协议的影响 | Cloudflare、Google、Quad9; Do53、DoT、DoH | 不同服务商之间以及同一服务商提供的不同协议的服务之间可能存在较大性能差异; 同时性能表现存在明显的地区差异 |
| DoQ与其他协议对比 | DoQ、DoH、DoT往返时间和握手时间 | 约20%需要1-RTT, 40%需要2个以上的RTT、相较DoT和DoH仍有较大优势 |

研究者发现由于建立连接、加密等的开销, DoH、DoT 的解析响应时间高于 Do53, 例如 Doan 等人[55]发现包含完整握手的 DoT 响应约比明文 DNS 慢 100 ms. 但在网页加载时间方面的差别并不明显, 在网络条件正常并选择合适递归解析器的情况下, DoH 等在提供隐私保护的同时, 并不会使用户感知到明显的页面加载效率上的牺牲[49,52,54,56]. 这一方面是由于长连接机制可以一定程度上降低单个查询响应的连接开销, 另一方面提供商和应用厂商在实现加密协议部署时会进行相应的技术优化, 例如 Firefox 可以一次并行解析多个域名, 其 Do53 和 DoT 中使用了线程池进行同步解析, 而 DoH 实现是异步的, 并对 HTTP/2 协议进行了优化, 避免因为响应时间的延迟而过多影响页面加载性能[56]. 此外 Deccio 等人[57]发现 TCP 快速打开 (TCP fast open, TFO) 在 DoH 和 DoT 递归解析器中具有很低的支持率.

Kosek 等人[51]通过比较 DoQ 和其他协议的往返时间和握手时间, 发现大约 20% 测量结果需要 1-RTT, 40% 的结果需要 2 个以上的 RTT, 虽然 DoQ 的性能表现不如预期, 但相较于 DoH 和 DoT, DoQ 仍表现出了较大的优势.

#### 4.2.2 网络条件对不同协议性能的影响

在不同网络条件带来的影响方面, 通过在模拟的蜂窝 4G 网络、有损蜂窝 4G 网络及 3G 网络中的测量, Hounsel 等人[56]发现在页面加载方面, 有损 4G 网络上 DoT 和 DoH 比 Do53 稍快, 他们分析原因是 TCP 和 UDP 之间处理 DNS 超时的差异. 对于 DoT 和 DoH, 由于 TCP 的缘故 DNS 数据包会在 2 倍往返时间的延迟后重传, 当往返时间在数百毫秒数量级时, DoT 和 DoH 将比 Do53 更快地重传丢弃的数据包. 但是随着网络吞吐量的下降和损耗增加, DoT 和 DoH 的性能表现有明显的下降, 这是由于加密协议发送的字节数更高, 导致大多数网站链接饱和, 而且高延迟和随机丢包会进一步加剧对 TCP 的性能影响. 此外在有损网络条件下, DoH 具有更高的失败率和错误率; 在对家庭网络的测量中, 随着递归解析器延迟的增加, 研究者也得到了相同的结果[54].

#### 4.2.3 服务商的选择对性能的影响

不同服务商之间以及同一服务商提供的不同协议之间可能存在很大的性能差异. 在页面加载时间方面, 对于 Cloudflare, 3 种协议的平均表现相似, 但是研究者发现 Google 的 DoH 和 Quad9 的 DoT 性能却明显较低, 这可能跟缓存机制设置或连接到权威名称服务器失败后通过 Do53 触发重试有关[56]. 同时由于较高比例的用户配置使用 Cloudflare Do53 和 Google Do53, 使得它们缓存了大量的热门域名, 二者的页面加载时间中位数比本地 Do53 递归更短. 在针对美国两千多个家庭网络中应用的加密协议和传统 DNS 的性能测试实验中, 通过分析不同递归解析器中 DoH、DoT 和传统 DNS 的连接建立时间开销、DNS 响应时间, 以及网络延迟和提供商选择对查询速率的影

响, 研究者也得出了相同的结论, 发现不同递归解析器之间的性能差异较大[54,58]. 此外在全球不同位置访问时, 部分解析器性能表现出了明显的地区差异[55]. DNS 客户端应定期进行延迟和响应时间测试, 以确定应选择哪种协议和提供商, 没有单一的协议或服务能够在所有的客户端上表现最佳.

### 4.3 DNS 信道传输加密技术隐私保护效果分析

加密协议部署后其隐私保护效果如何, 对加密流量的识别和分析是否存在可能, 是值得关注的问题. 消息加密后建议进一步通过填充机制来隐藏数据的真实属性信息 (参见第 4.3.1 节), 但填充机制也存在一定的局限性, 第 4.3.2 节探讨了对加密流量识别和分析的进展, 第 4.3.3 节对现有方案的不足进行了总结.

#### 4.3.1 填充机制分析

即使 DNS 查询和响应消息都已加密, 但仍然可以使用元数据对这些消息进行识别和关联, 进而影响加密的隐私效果, 例如加密 DNS 消息的大小和时间信息可以用来与递归解析器上游的未加密 DNS 请求相关联. DoH、DoT 和 DoQ 都建议使用 RFC 7830[59]中定义的 EDNS(0) 填充扩展选项 (其结构如图 5 所示), 以允许客户端和服务器通过可变长度的填充字节来手动增加 DNS 消息的长度, 如表 8 所示. 填充字节应设为 0x00, 但如果担心填充部分在加密前被压缩可设为其他值. RFC 8467[60]进一步提出了填充数据的设置策略, 填充选项应放在 EDNS(0) 选项空间的最后, 同时需要考虑填充消息大小和资源消耗的权衡, 以及不同传输协议的影响等. 其中列举了块长度填充、最大长度填充、随机长度填充和随机块长度填充等填充机制, 并推荐使用块长度填充机制, 此外建议客户端应将查询消息填充至最接近的 128 字节的倍数, 服务器端响应消息的填充块长度建议为 468 字节的倍数. 除 RFC 7830 中定义的填充选项外, QUIC 协议中定义了专门的填充帧, 使得 DoQ 还可以从数据包层面进行填充设置.

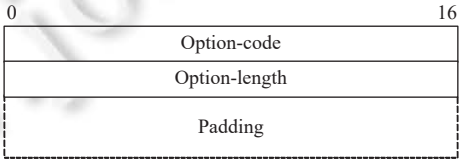


图 5 EDNS(0) 填充扩展选项结构图

表 8 填充机制

| 填充机制 | 描述 | 适用协议 |
|---|---|---|
| EDNS(0)填充扩展选项 | 通过填充字节手动增加消息长度<br>填充数据的设置策略: 推荐块长度填充机制 | DoH、DoT、DoQ |
| 填充帧 | QUIC中填充(PADDING)帧 | DoQ |

#### 4.3.2 加密流量的识别和分析

影响加密协议隐私保护效果的关键因素是它们能否防止被识别和分析. 识别分为对正常和恶意加密流量的识别, 例如从 HTTPS 流量中区分出哪些是 DoH, 识别隐藏在加密流量中的恶意活动等; 分析是在识别的基础上进一步对用户活动细节进行探索, 例如对用户访问的网站、使用的客户端及具体应用进行破解.

填充机制虽然对加密流量的识别具有一定的抑制作用, 但其效果有限, 并不能完全避免对加密数据的分析[61−64]. 此外通过用一个递归解析器上的训练数据对另一个解析器上的流量进行识别, 研究者发现使用推荐的填充策略增加了不同递归解析器之间流量的相似性[61]. 同时通过测试发现有很高比例的 DoH 和 DoT 服务不支持填充功能.

从 HTTPS 流量中识别 DoH 数据这方面的研究主要基于二者的特征差异进行分析. 研究者发现相较于 HTTPS 流量, 单个 DoH 请求和响应至少包含多个数据包, 除重新连接及变更 DoH 服务器等特殊情况外, 浏览器跟 DoH 服务器建立连接后会保持更长时间[65]. 虽然文件下载、视频流传输时也会产生长连接, 但相比之下这些类型的连接会在更短的时间内传输更多的数据.

Vekshin 等人[65]利用 AdaBoost 决策树等 5 种机器学习算法从普通 HTTPS 流量中检测区分 DoH 通信, 并通

过网络流量的行为特征来识别特定客户端. 他们用基尼指数计算后选取的 DoH 识别最重要的特征是流的持续时间和平均包间延迟, 此外还包括响应数据包大小的方差、传入和传出数据量的对称性等. 在识别 DoH 客户端时选取的主要特征是传入数据包大小的差异, 但是其能够很好分离客户端的原因在于不同浏览器对 EDNS 填充功能的支持情况不同.

在对用户访问的网站进行识别方面, 主要方法是基于加密 DNS 信息构建网页指纹. Bushart 等人[63]对 DNS 序列进行建模, 通过请求间的依赖关系同时结合数据包大小和时间间隔等信息来识别用户访问的网站. 但他们的方法也有一定的局限性, 在用户建模方面, 其未考虑特定网站加载时可能同步进行的其他 DNS 流量, 并且未考虑 DNS 和浏览器缓存的影响, 同时 DNS 消息可能在多个 TLS 记录中传输, 这种情况会影响消息大小提取的精确度. Houser 等人[64]对 DoT 的信息泄露进行评估, 其方法基于随机森林和 AdaBoost 分类器实现, 特征集由 DNS 消息的时间序列构建, 包含时间戳、加密消息的长度和流量方向等, 并从中提取更高级别的特征, 例如查询或响应长度、数据包总数、时间间隔或每秒查询数等, 进一步在此基础上计算一系列统计数据作为分类器参数. 孟德超等人[66]利用长短期记忆网络 (long short-term memory, LSTM) 对用户网站访问痕迹进行分析, 并且效果优于 Siby 等人[67]的方法.

Hoang 等人[68]提出一种基于 IP 的网站指纹技术. 在指纹生成阶段, 选取共 220k 个热门网站和敏感网站, 分别建立其主域名和从域名 (例如获取页面中的引用资源所涉及的域名) 集合, 以及对应的主从 IP 地址集合. 虽然访问网页时部分域名请求顺序没有绝对固定的先后关系, 但根据浏览器的关键渲染路径, 某些域名请求之间仍会存在依赖关系. Hoang 等人选取 domLoading、domContentLoaded 和 domComplete 这 3 个事件将域名和对应的 IP 地址划分到 3 个不同的阶段以构建加强指纹. 在进行匹配时对于给定的 IP 地址序列, 先将主 IP 与所有指纹进行匹配, 获得候选集, 然后基于各个连接的时间序列利用 K-means 方法将其余 IP 进行聚类, 将分类后 3 个阶段的集合与候选者集合分别取交集, 并计算信息熵, 值高者为最终结果. 最终识别的综合准确率为 91%, 未成功匹配的网站中有不少候选域名都指向同一网站, 如同一公司在不同 TLD 下注册的域名或同一公司的不同名字. 上述部分方案的比较如表 9 所示.

表 9　加密流量的分析

| 方向 | 协议 | 方法 | 特征 |
|---|---|---|---|
| 通过指纹构建分析用户访问的网站 | DoT[64]、DoH[63] | 随机森林、AdaBoost分类器等 | 查询和响应长度及数目、查询和响应的累积字节数、数据包之间时间间隔、总传输时间、连续的查询或响应组、单个TLS记录中的DNS消息数、每秒查询数、接收前*N*字节的时间以及以上特征的统计值 |
| | DoH、DoT | 基于IP构建网站指纹[68] | 构建域名集合和IP集的对应关系, 并根据浏览器渲染事件的逻辑关系进行阶段分类构建指纹 |
| 应用/客户端分析 | DoH、DoT | 随机森林等[61] | TLS记录大小频率分布、DNS序列的距离、N-grams等 |

#### 4.3.3　现有研究方案的局限和不足

之前已有较多网页指纹相关的研究, 但多是基于 HTTPS 进行构建, 相比之下利用 DNS 信息构建网站指纹可能存在流量较小及消息大小区分度不明显等问题. 网页加载时会发送多个 HTTP 请求获取页面的所有对象, 由于多个对象可能存储在同一主机上, 因此该过程中发送的 DNS 查询数目可能明显低于 HTTP 消息的数目; 另一方面 HTTP 请求中字段设置更加多样化, 同时网页上不同资源对象大小差异较大, 可进一步增强其区分度.

此外网页指纹识别的准确率、稳定性、健壮性受到诸多方面因素的影响. 首先, 浏览器缓存会影响指纹识别的准确率, 虽然较小的 TTL 值和浏览器的缓存分区策略使该影响有所减弱. 其次网站引用资源元素的改变或者域名和 IP 映射关系的改变等因素会影响指纹的稳定性. 有研究者建议弱化网站的差异性, 如隐藏数据交换的数量、为一组页面发送相同数目的查询或响应以及引入无关数据包调整时间间隔等, 但这可能会增加额外的网络负担[64]. 网站所有者和托管服务商可以从减小第三方资源的引用、增强网站内容的动态变化、广告拦截、增强域名和 IP 对应关系的变化等方面加强网站的隐私防护.

上述相关研究都对实验环境和威胁模型等条件进行了限制, 并且都在相对封闭的场景中进行指纹模型训练和验证, 由于网站域名数据量巨大, 在完全开放的环境中进行域名识别比较困难. 此外主动攻击者在流量分析的基础上可能会进一步创建有利于自身攻击的条件, 如通过发送 DNS 请求影响缓存等, 进一步增加加密流量被识别和分析的风险. 当前研究在构建威胁模型时并未考虑将不同协议之间进行关联的场景, 主要基于加密 DNS 流量自身构建网站指纹. 在 DNS 信道传输加密技术推出之前, 基于网站指纹已开展了大量的研究, 但主要关注 HTTPS 等协议, 利用不同协议之间的数据关联能否创建更加准确的网站指纹是后续的一个探索方向.

## 5 DNS 信道传输加密技术的问题和挑战

本节主要对 DNS 信道传输加密技术可能存在的问题和挑战进行分析.

### 5.1 传输路径上其他影响隐私安全的因素

流量加密后仍存在其他可能泄露隐私的因素, 例如有研究者评估了使用加密解析代替明文传输能否避免路径上的审查机制, 但单纯替换加密协议并没有取得理想效果[69]. 因此加密协议需要与其他技术相互配合, 以更好地保护隐私安全. 消息加密后仍存在隐私泄露的地方包括服务器名称标识 (第 5.1.1 节) 和客户端子网信息 (第 5.1.2 节) 等.

#### 5.1.1 服务器名称标识

基于名称的虚拟主机是一种用于在单个服务器上托管多个域的方法, 因此在 TLS 握手完成之前服务器需要一种机制来获取用户打算访问哪个域名, 以便提供正确的证书, 服务器名称标识 (server name indication, SNI) 扩展被引入以解决上述问题. 由于当前 TLS 握手期间 SNI 扩展未加密, 路径上的观察者可以通过窃听 TLS 握手流量来探测用户访问的域名. 加密 SNI (encrypted SNI, ESNI) 的草案[70]正在推进, 以使 TLS 1.3 版本中支持 ESNI.

同时研究者对 DNS 信道传输加密技术和 ESNI 的部署能在多大程度上保护用户隐私进行了评估[71], SNI 加密后攻击者可以利用目标 IP 地址来推断用户访问的站点, 他们使用共同托管导致的 $k$ 匿名度和 IP 地址变化的动态程度两个指标来量化 ESNI 为不同托管和 CDN 服务商提供的隐私增益. 如表 10 所示, 通过在全球 9 个位置进行测试, 发现部署加密 DNS 和 ESNI 后, 其选取的域中有约 20% 由于独占一个或多个 IP 地址从而不会获得任何隐私优势, 约 30% 的 $k$ 值大于 100 的域将获得显著的隐私优势, 隐私得到明显改善的域远不那么受欢迎. 同时约 81% 的多主机域共同托管在 30% 的 IP 地址上, 通过分析域名对应的 IP 地址的动态变化程度, 发现其中只有 7.7% 以天粒度更改托管的 IP 地址. 但是他们的测试结果中不考虑共同托管网站之间的可区分性 (例如人气排名、网站敏感度和网络流量模式等), 以及利用特定于页面的属性构建的网页指纹等信息, 实际攻击者可以基于上述信息做进一步分析.

表 10 加密机制和 ESNI 部署后域名获得的隐私保护效果分析

| 域分类 | 特点 | 域名占比 | 占有IP的比例 | 属性 | 隐私增益效果 |
|---|---|---|---|---|---|
| 单一托管域 | 单个域名独占一个或多个IP | 约20% | 70% | 热门域名 | 未获得隐私增强 |
| 多托管域 | 域名对应的IP托管域名数目大于1且小于100 | 约50% | 共30% | 非热门域名 | 获得一定程度的隐私增强 |
| | 域名对应的IP托管域名数目大于100 | 约30% | | 非热门域名 | 获得较明显的隐私增强 |

#### 5.1.2 客户端子网

许多权威名称服务器根据感知的用户拓扑位置返回不同的响应, 然而递归解析器发送的源地址一般是其自身地址, 并且很多递归解析器在拓扑上并不接近真实的用户查询源. ECS (EDNS client subnet, 客户端子网扩展) 选项扩展[72]使得递归解析器能够在请求中加入查询来源的原始地址信息. 递归与权威服务器通信时的源 IP 地址一定程度上隐藏了真实的用户, 但客户端子网 EDNS0 选项则会暴露用户信息.

Poitrey[73]认为 ECS 的主要问题是隐私泄露和 DNS 缓存碎片, 同时发现排名前 100 万的支持 ECS 的域名中有超过一半从不同位置的子网查询时都会返回相同的结果, 但却要按子网存储多个相同结果的副本. 他们提出的解

决方案包括子网聚合后进行重新映射和建立白名单机制. 根据 GeoIP 将客户端原始的子网映射到基于位置的编码块 (格式为 ASN:Country[:Metro Code]), 并以此作为 key, 相同的 key 映射到同一个随机选择的子网上, 以替代原来的子网信息. 该机制避免客户端子网信息泄露, 同时一定程度上提升了缓存利用率.

### 5.2 部署规范和集中化加剧问题

递归解析器在部署时使用无效证书的问题较为突出, 2020 年的扫描中发现使用无效证书的 DoT 服务占比近 29%, 其中大部分为自签名证书, 除此之外还包括证书过期和信任链不完整等[49]. 文献 [48] 发现 10.2% 的开放 DoH 递归解析器和 60.7% 的开放 DoT 递归解析器使用无效证书. 同时有较高比例的 DoH 和 DoT 服务不支持填充功能.

递归解析器部署方面的另一问题是集中化, DNS 服务的集中化问题一直存在, 根据分析 5 个大型的云服务商负责荷兰和新西兰两个 TLD 的 30% 的请求[74]. 相较于传统 DNS, DoH 将递归解析器选择控制权转移到浏览器供应商或其他应用提供商, 少数头部公司在服务器数目和流量占比上占有主导地位, 同时由于其在 Do53 中积累下大量数据和用户优势, 更容易获得用户的选择. 部署集中化问题进一步对递归解析器端的用户数据隐私保护提出了挑战.

美国电信协会等组织抗议谷歌在其浏览器和安卓系统中支持 DoH, 他们认为由于 Chrome 浏览器和安卓系统具有强大的用户占有率, 谷歌对加密协议的部署将加剧 DNS 的集中化, 使得一个公司拥有大量的 DNS 数据, 损害了广告和其他行业的竞争公平性[75].

#### 5.2.1 系统部署架构优化

Hounsel 等人[76]认为 DNS 信道传输加密协议的部署在某些情况下加剧了 DNS 的集中化, 其对 DNS 递归解析器架构的设计和实现进行重构, 提出去中心化的名称解析. 他们增加了额外的分发策略, 并将名称解析决策的控制权从单个应用程序中转移出来, 设计支持基于规则的 DNS 服务选择策略 (例如匹配客户端 MAC 或 IP 地址等), 同时测试了基于 HASH 的分发、随机分发、循环分发等几种查询分发策略.

Hoang 等人[77]提出一种 K-resolver DNS 解析机制, 利用桶哈希机制将 DNS 查询分散到多个 DoH 递归解析器中, 避免单个递归解析器了解用户的整个 Web 浏览记录后构建完整的用户档案. 在性能方面, 由于所选 DoH 服务器的地理位置原因, K-resolver 机制对 DNS 解析时间和网页加载时间有一些影响, 当有完善的任播服务器时, 该方法产生的额外开销可大幅降低.

跨多个服务器分发 DNS 查询是改善互联网用户隐私的一个研究方向. 但在制定具体的分发策略时还有很多问题需要注意, 单纯的循环、随机分发等并不能起到隐私保护的效果, 同时需要关注其对性能的影响, 以及是否会对 CDN 本地化产生负面影响等. 此外访问特定网页时由于第三方资源引用等产生的多个域名查询请求能够被用作网页指纹, DNS 预取也会向递归解析器泄露用户后续可能要访问的网页的域名, 制定分发策略时也需要将上述因素考虑在内.

### 5.3 恶意流量对加密技术的利用和攻击

#### 5.3.1 加密技术被恶意流量利用

加密技术在给合法用户提供隐私安全的同时其数据加密的特性也为恶意软件及攻击者提供了可乘之机. 例如安全公司发现恶意软件 Godlua 利用 DoH, 把非法服务器 URL 存储在特定资源记录中, 并将该资源记录的获取过程进行隐藏[78]; 伊朗黑客组织 Oilrig 利用 DoH 防止其盗取数据的传输过程被监测[79]. 流量加密使得原有针对明文 DNS 的检测方法中使用的特征被隐藏[80].

Patsakis 等人[81]研究了如果恶意软件使用保护隐私的 DNS 服务来解析其 C&C 服务器是否会绕过当前的安全机制, 并讨论了 DNS 信道传输加密对 DGA 检测带来的影响. 他们分析了不同数据集的响应数据包大小分布的范围、标准差, 发现 DGA 生成静态长度或长度变化差异较小的域时, 基于数据包的流量分析可实现高准确率的恶意流量区分. 进一步的他们将僵尸网络流量构建成时间序列变量, 使用 Hodrick-Prescott 过滤器去除流量噪声影响, 在此基础上进行趋势和自相关性分析, 并利用自回归滑动平均模型系数来构建失陷指标, 结果表明该方法可以

识别异常活动并标记僵尸网络感染, 但无法有效地将攻击归因于特定的僵尸程序. 张千帆等人[82]选取时间序列等特征, 通过 KNN 设计了在 DoH 中检测 DGA 流量的方法, 准确率为 79%.

Banadaki 等人[83]构建一种两层模型来检测恶意 DNS 流量, 首先将 DoH 流量和非 DoH 流量进行分类, 在此基础上在第 2 层进行恶意 DoH 和良性 DoH 的识别, 在该方法中选取源 IP、目的 IP 及数据包长度中位数等 34 种特征, 并采用 XGBoost 等 6 种算法. MontazeriShatoori 等人[84]同样基于两层模型构建分类器进行 DNS 隧道检测. Singh 等人[85]与 Banadaki 选用了相同的数据集, 但在算法的选择上有所不同, 其选择梯度提升树、随机森林等 4 种算法. Kwan 等人[86]对一个支持加密 DNS 隧道的原型工具的抗审查性进行了评估, 并基于数据包大小、吞吐量等特征构建基于阈值的 DNS 隧道检测机制.

Zhan 等人[87]通过客户端 TLS 指纹并基于流特征构建分类器来进行 DoH 隧道检测, 他们选取的特征分为 TLS 记录长度和时间间隔两大类, TLS 记录长度可以间接的反映域名长度信息, 同时相较 DNS 隧道流量, 正常 DNS 发送的请求随机性更高, 并且由于缓存机制收到响应的平均时间间隔更短. 上述两类特征分别包括查询、响应和流上所有数据包的 TLS 记录长度, 以及两个连续查询/响应之间的时间间隔、相邻一对查询和响应之间的时间间隔和对应的统计值. 通过对准确率、精确率、召回率、*F*1-score 等方面的评估, 上述方法取得了较好的实验结果. 由于机器学习方法中特征的提取和构建复杂度高, Ding 等人[88]利用变分自编码器和双向 GRU 网络来构建能够自动进行特征学习的 DNS 隧道检测方法, Nguyen 等人[89]在企业网络中构建基于 Transformer 的 DoH 隧道攻击检测系统. 上述方法的比较和总结如表 11 所示.

表 11　加密流量识别

| 方向 | 协议 | 方法 | 特征 |
|---|---|---|---|
| HTTP流量中检测DoH | DoH | AdaBoost决策树、C4.5决策树等5种机器学习算法[65] | 流的持续时间、平均包间延迟、响应数据包大小的方差、传入和传出数据量的对称性等 |
| 恶意流量识别 | 恶意DoH检测 | 两层模型; XGBoost、LightGBM、梯度提升树、随机森林等[83,85] | 源IP、目的IP、端口、数据包长度、时间戳、持续时间、发送和接收字节量、方差标准差等统计指标 |
| | | Boosting决策树、随机森林、逻辑回归[87] | 查询、响应流上所有数据包的TLS记录长度; 两个连续查询/响应之间的时间间隔; 相邻一对查询和响应之间的时间间隔; 每个流级特征的最小值、最大值、平均值、标准差 |
| | | 变分自编码器和双向GRU网络[88]; 基于Transformer构建DNS隧道检测系统[89] | 特征自学习; 连接时长、发送接收字节数及速率、数据包长度及响应时间差异等统计指标 |

### 5.3.2　降级攻击问题

DNS 信道传输加密技术各协议都支持机会主义隐私设置方案, 浏览器等应用在采用加密 DNS 解析时大多默认开启了该机制. 机会主义隐私设置的初衷是允许在某些隐私性要求不高或条件不具备的场景下能正常为用户提供服务, 但是为了规避加密协议提供的保护, 攻击者可能利用该机制对加密服务进行降级. 如第 3.1 节所述, DoH 通信过程中, 在 URI 解析阶段攻击者可以对 DNS 消息进行过滤和拦截, 或通过缓存中毒的方法使用虚假 IP 地址替换目标 DoH 服务器的 IP 地址, 进而影响后续客户端与 DoH 递归解析器的正常连接. 双方通信阶段攻击者可以通过 TCP 流量数据拦截或篡改等使 DoH 回退到传统 DNS. 攻击者可获取 TCP 报头中的序列号和确认号, 并向受害者或 DoH 递归解析器发送伪造的 TCP 重置数据包, 以诱使他们切断 TCP 连接[90].

Huang 等人[90]对 DoH 的降级攻击进行了分析, 他们选取了 Chrome 等 6 款常用的浏览器, 并选用连续请求周期、请求间隔时间设置、最大时间间隔 3 个属性测试面对不同攻击方法时各浏览器的反应. 发生降级后没有任何浏览器会尝试通知用户, 部分浏览器需要很长时间才能恢复到 DoH.

## 5.4　隐私和网络安全管理的矛盾

章坚武等人[91]和胡宁等人[92]对 DNS 各种攻击类型和检测技术进行了总结和分析, 当前家长控制、企业防火墙、病毒防护等安全软件都依赖未加密的 DNS 通信来过滤流量或实施安全防护策略, 加密协议的应用使得网络

管理员和技术团队对网络安全的精准管控变得困难. 隐私和网络安全的平衡位置应在哪里各方持不同态度, 完全加密的机制对网络安全管理造成了一定的负面影响.

部分研究者建议设置代理系统作为中间人解密 HTTPS 流量, 以对流量执行深度数据包检查, 但是该方法同样面临一些问题, 首先涉及开放网络中的证书部署及身份认证信息的管理, 此外 TLS 会话密钥等数据的存储及会话解密将消耗大量的存储和计算资源, 同时对性能也会产生一定的影响[80].

此外信道传输加密协议对客户端到递归解析器之间的通信过程进行加密, 但递归解析器端仍可对响应进行查看甚至修改, 以实现访问控制和安全管理. Jin 等人[69]通过大规模的测试来评估加密协议中 DNS 操纵的情况. 研究者基于数千个递归解析器及 740 万次 DNS 查询测试, 发现 1.66% 的 DoT 响应和 1.42% 的 DoH 响应进行了 DNS 操纵. 最严重的 DoT 递归解析器操纵了 728 个域名的响应. 并且被操纵的响应来自超过 2/3 的 DoT 和 DoH 递归解析器, 与之前研究 11% 的测试结果[93]相比, DNS 操纵在加密协议中比在传统 DNS 更普遍. 同时同一提供商下不同递归解析器审查域的数量可能存在很大的差异. 对 DNS 信道传输加密技术存在的问题和挑战的分类总结如表 12 所示.

表 12 DNS 信道传输加密技术的问题和挑战

| 问题和挑战 | 表现 | 相关研究/改进方案 |
|---|---|---|
| 加密后其他影响隐私安全的因素 | 服务器名称标识泄露目标服务器名字 | 对服务器名称标识进行加密; SNI加密后共同托管的匿名度和IP地址动态变化对隐私增益的影响[71] |
| | 客户端子网 | 客户端子网信息进行重新映射, 缓解信息泄露[73] |
| 部署规范问题 | 无效证书的问题; 部分不支持填充机制 | 存在自签名证书、证书过期、信任链不完整等[49,48] |
| 部署集中化问题 | 递归解析器的选择配置权限转移等因素加剧集中化 | 跨递归解析器进行DNS查询的分发[76,77] |
| 恶意流量对加密技术的利用和攻击 | 恶意流量利用加密技术隐藏自身的攻击行为 | 对利用加密协议进行隐蔽通信的僵尸网络(例如利用加密协议隐藏与C&C服务器的通信等)、DGA等进行检测[81]; 机器学习、神经网络等方法识别恶意加密DNS流量[83−88], 恶意流量检测两层模型(首先识别DoH流量, 进而区分良性和恶意DoH流量)[83,84] |
| | 降级攻击 | 机会主义隐私配置支持仅加密无身份认证, 或退至明文传输, 机会加密配置被攻击者利用[90] |
| 隐私和网络安全管理的矛盾 | 加密对网络安全防护技术提出了新的要求 | 加密技术部署后攻击检测技术、安全监管和网络管理机制需要进行改进; 加密协议部署后递归解析器端的DNS操纵[69] |

## 6 趋势与研究方向展望

DNS 信道传输加密协议推出后, 未来待解决的问题和后续其他研究方向主要包括以下方面.

### 6.1 加密 DNS 服务器发现

由于明文 DNS 传输已广泛部署多年, 加密协议推出后如何在当前传统递归解析器广泛部署的环境下进行过渡和转换是需要解决的问题. 首先客户端如何发现支持加密机制的 DNS 递归解析器, 以及上述解析器的参数信息如何传递给客户端用于其选择决策. 其次非加密递归解析器升级或服务商推出了新的加密递归解析器后, 用户如何能够及时地发现并更换使用新的加密服务. 同时某些应用软件或 APP 厂商, 以及一些公司可能希望用户通过特定的加密递归解析器来访问自己的应用或域名. 最后通过其他协议或公共列表获取到加密递归解析器名字后, 用户需要能够获取该解析器更加详细的信息, 并对其进行身份验证. 此外权威服务器支持加密后也面临如何进行信息发布的问题.

加密递归解析器发现的相关研究包括两个方向, 基于递归解析器的发现和基于网络的发现. Pauly 等人[94]提出一种利用 SVCB 资源记录来发现 DNS 信道传输加密配置的机制, 该方法支持从非加密递归解析器探测对应的加密递归解析器, 同时可以发现和选择该解析器支持的多种加密协议, 其适用于非加密和对应的加密递归解析器

由同一实体管理的场景. Boucadair 等人[95]通过定义新的 DHCP、DHCPv6 和 IPv6 路由通告选项来发现加密 DNS 递归服务器, 定义的选项扩展字段中包括加密递归解析器的完整域名、IPv6 地址及一些服务参数信息. 针对当前提出的加密递归解析器发现机制不支持客户端通过本地转发器与上层解析器进行通信的场景, Schwartz 等人[96]提出本地转发器通过私有 IP 地址指定时, 采用基于加密 DNS 的机会隐私配置来执行宽松的验证策略, 去除证书校验过程. 同时某些 DNS 转发器会起到阻止访问恶意软件或其他威胁域的作用, 并在学校、公司等环境下对提供特定服务的域进行禁止, 应确保此服务不会因跨转发器升级到对应的加密解析服务而丢失[96].

### 6.2 递归解析器到权威服务器之间的加密

虽然 DoQ 等协议也支持递归解析器到权威服务器之间的隐私安全保护, 但相较于客户端到递归解析器的通信路径, 递归解析器和权威服务器之间信道传输加密技术的应用面临更多困难, 也是未来值得关注和研究的方向. 一方面 DNS 解析时若未命中缓存, 递归解析器会依次向根服务器、顶级域服务器、二级域权威服务器发送查询请求, 为增强隐私保护防止消息 (例如查询的目标域名等) 泄露, 上述路径都需要实现加密机制, 同时隐私保护效果跟权威服务器服务域名的数目有关. 另一方面由于下一级查询依赖于上一级查询的响应, 如果当前路径未部署加密认证机制, 若遭受攻击导致响应被篡改为攻击者服务器, 则下游路径即便已部署加密协议其安全性也无法保证. 上级路径未部署时缺少相应的机制来向下游通信路径传达自身响应的可信性证明.

此外在加密权威服务器的属性等信息如何告知递归解析器方面, 可通过服务端发布或递归解析器端主动查询等方式, 但都存在实际的问题, 虽然已定义了服务绑定资源记录, 但 EPP 等协议暂未提供对其的支持, 一定程度上阻碍了加密协议的应用部署进程.

2021 年根服务器运营商在针对加密机制发布的声明[97]中表述了对加密、连接状态维护等带来的性能影响和可能引发的新型拒绝服务攻击的担忧, 同时表示根服务器运营商不愿成为加密机制的早期实践方, 并建议可采用其他机制 (例如维护本地根区副本[98]) 提高隐私保护.

基于上述问题, Gillmor 等人[99]提出递归解析器和权威服务器通信时使用单边部署支持机会加密配置, 由于 DoH 中需要知道服务器的 URL, 目前暂未有机制使得客户端能单方面探测到 DoH 权威服务器, 因此研究者选用了 DoT 和 DoQ 协议.

### 6.3 DNS 服务器端的隐私保护

DoH、DoT 和 DoQ 避免了路径上的窥探和数据篡改, 但是主要的加密递归解析器掌握在少数几家服务提供商 (例如 Cloudflare、Google、Quad9 等) 手中, 部署的集中化使得服务器掌握大量数据, 能够方便地进行数据收集和分析, 进而挖掘用户的敏感信息. 递归解析器端隐私泄露问题的一种解决途径是建立数据管理维护的规范和机制, 例如 Mozilla 围绕数据保留、汇总、销售或转让等操作定义了一套限制条件, 要求浏览器的 DoH 递归解析器遵守他们制定的可信递归解析器策略文档[100]中概述的隐私要求. 这种方法以政策和合约等为基础建立信任机制, 但它们难以验证且缺乏执行手段, 探索有效的协议和机制来加强递归解析器和权威服务器端的隐私保护也是未来的研究方向.

ODoH[101,102]在 DoH 的基础上进行了扩展, 通过增加代理来避免任何一方同时掌握客户端 IP 地址以及对应的 DNS 请求和响应的内容, 防止递归解析器利用信息关联进行用户活动分析. ODoH 中引入了目标对象的概念, 它表示递归解析器或转发器. 客户端将 DNS 查询用 HTTP POST 请求形式发送给代理, 其中通过定义的目标主机和目标路径两个字段指示将消息发送至哪个目标对象. 代理收到客户端发来的请求后根据上述信息与目标对象建立连接. 客户端通过代理发送给目标对象的 DNS 查询消息由公钥进行加密, 确保只有指定的目标对象才能解析客户端的请求内容. 目标对象发送的响应也通过代理返回给客户端, 整个过程中代理不应将可能会泄露客户端身份的有关信息发送给目标对象. 同时有研究者提出 DoHoT (DNS over HTTPS over Tor, 基于 Tor 的 DoH), 但其在 DNS 响应时间和网页加载时间等方面对性能有较大的影响[103].

### 6.4 HTTP/3 和 DoH3

DoH 协议提出时 HTTP/3 尚未发布, HTTP/3 基于 QUIC 和 UDP 实现, QUIC 致力于替代 TCP 协议并且发展

迅速, 目前已被国内外众多公司部署应用, 例如其在 Facebook 中的流量占比已超过 75%[104], 并在音视频、直播、图文下载及不稳定的网络环境下明显的改善错误率和卡顿率等指标. NextDNS 已尝试推出 DoH3 服务, 今年 7 月 Google 宣布在 Android 平台支持 DoH3[105]. 但由于 HTTP/3 刚正式发布, 大部分服务提供商暂未提供对 DoH3 功能的支持. 未来 QUIC 协议及 HTTP/3 的发展是否会在一定程度上推动 DoQ 和 DoH3 的部署, 以及其性能和隐私安全表现及优化等也是值得关注的方向.

## 7 总 结

对明文 DNS 的隐私和安全保护机制一直在迭代探索中发展, DNS 信道传输加密协议自发布后得到了广泛的关注和大规模的应用部署. 本文分析了 DNS 信道传输加密协议的技术原理及应用现状, 并从不同的指标、网络设施环境等方向对性能影响进行讨论; 进而对信道传输加密技术的隐私保护效果进行分析, 最后从传输路径上其他影响隐私安全的因素、部署规范和集中化加剧、恶意流量对加密技术的利用和攻击、隐私和网络安全管理的矛盾等方面分析总结了 DNS 信道传输加密技术所面临的问题和挑战及对应的解决方案, 并从加密解析器发现、递归解析器端的隐私保护、递归解析器到权威服务器之间的加密等方面对未来的趋势和研究方向进行展望.

**References:**


[1] CrowdStrike. Widespread DNS hijacking activity targets multiple sectors. 2019. https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/

[2] Fouchereau R. IDC 2022 global DNS threat report. 2022. https://www.efficientip.com/resources/idc-dns-threat-report-2022/

[3] Help Net Security. Healthcare suffering from DNS attacks more than other industries. 2021. https://www.helpnetsecurity.com/2021/07/15/healthcare-dns-attacks/

[4] McCarthy K. Internet's root servers take hit in DDoS attack. 2015. https://www.theregister.com/2015/12/08/internet_root_servers_ddos/

[5] Hesselman C, Kaeo M, Chapin L, Claffy K, Seiden M, Mcpherson D, Piscitello D, Mcconachie A, April T, Latour J, Rasmussen R. The DNS in IoT: Opportunities, risks, and challenges. IEEE Internet Computing, 2020, 24(4): 23–32. [doi: 10.1109/MIC.2020.3005388]

[6] DNSmezzo. DNSmezzo form AFNIC project DNSwitness. 2022. https://github.com/dsutto/DNSmezzo

[7] The Tcpdump Group. Tcpdump. 2021. https://www.tcpdump.org/

[8] Wang WT, Hu N, Liu B, Liu X, Li SD. Survey on technology of security enhancement for DNS. Ruan Jian Xue Bao/Journal of Software, 2020, 31(7): 2205–2220 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6046.htm [doi: 10.13328/j.cnki.jos.006046]

[9] Huang K, Kong N. Research on status of DNS privacy. Computer Engineering and Applications, 2018, 54(9): 28–36 (in Chinese with English abstract). [doi: 10.3778/j.issn.1002-8331.1801-0101]

[10] DNSCrypt. 2021. https://dnscrypt.info/

[11] DNSCurve: Usable security for DNS. 2021. https://dnscurve.org/

[12] Bortzmeyer S. RFC 7816 DNS query name minimisation to improve privacy. 2016. https://www.rfc-editor.org/info/rfc7816

[13] Arends R, Austein R, Larson M, Massey D, Rose S. RFC 4033 DNS security introduction and requirements. 2005. https://www.rfc-editor.org/info/rfc4033

[14] Arends R, Austein R, Larson M, Massey D, Rose S. RFC 4034 Resource records for the DNS security extensions. 2005. https://www.rfc-editor.org/info/rfc4034

[15] DNSSEC deployment report. 2023. https://rick.eng.br/dnssecstat/

[16] Hoffman P, Schlyter J. RFC 6698 The DNS-based authentication of named entities (DANE) transport layer security (TLS) protocol: TLSA. 2012. https://www.rfc-editor.org/info/rfc6698

[17] Daigle L. RFC 3912 WHOIS protocol specification. 2004. https://www.rfc-editor.org/info/rfc3912

[18] Newton A, Ellacott B, Kong N. RFC 7480 HTTP usage in the registration data access protocol (RDAP). 2015. https://www.rfc-editor.org/info/rfc7480

[19] Hollenbeck S, Kong N. RFC 7481 Security services for the registration data access protocol (RDAP). 2015. https://www.rfc-editor.org/info/rfc7481

[20] Loibl A. Namecoin. In: Proc. of the 2014 Seminars FI/IITM SS Network Architectures and Services. 2014. 107–113. [doi: 10.2313/NET-2014-08-1_14]

[21] Ali M, Nelson J, Shea R, Freedman MJ. Blockstack: A global naming and storage system secured by blockchains. In: Proc. of the 2016 USENIX Annual Technical Conf. Denver: USENIX Association, 2016. 181–194.
[22] Bloackstack name service. 2021. https://docs.blockstack.org/core/naming/introduction.html
[23] Handshake. 2021. https://handshake.org/files/handshake.txt
[24] Ethereum Name Service Document. 2021. https://docs.ens.domains/
[25] The Ethereum Name Service Constitution. 2021. https://ensdao.eth.limo/constitution.pdf
[26] Schanzenbach M, Grothoff C, Fix B. The GNU name system. 2022. https://datatracker.ietf.org/doc/html/draft-schanzen-gns-19
[27] The GNU name system. 2022. https://www.gnunet.org/en/gns.html
[28] Wicinski T. RFC 9076 DNS privacy considerations. 2021. https://www.rfc-editor.org/info/rfc9076
[29] Hoffman P, McManus P. RFC 8484 DNS Queries over HTTPS (DoH). 2018. https://www.rfc-editor.org/info/rfc8484
[30] Curl. Publicly available servers. 2021. https://github.com/curl/curl/wiki/DNS-over-HTTPS
[31] Hu Z, Zhu L, Heidemann J, Mankin A, Wessels D, Hoffman P. RFC 7858 specification for DNS over transport layer security (TLS). 2016. https://www.rfc-editor.org/info/rfc7858
[32] Dickinson S, Gillmor D, Reddy T. RFC 8310 usage profiles for DNS over TLS and DNS over DTLS. 2018. https://www.rfc-editor.org/info/rfc8310
[33] Reddy T, Wing D, Patil P. RFC 8094 DNS over datagram transport layer security (DTLS). 2017. https://www.rfc-editor.org/info/rfc8094
[34] Toorop W, Dickinson S, Sahib S, Aras P, Mankin A. RFC 9103 DNS zone transfer over TLS. 2021. https://www.rfc-editor.org/info/rfc9103
[35] Iyengar J, Thomson M. RFC 9000 QUIC: A UDP-based multiplexed and secure transport. 2021. https://www.rfc-editor.org/info/rfc9000
[36] Thomson M, Turner S. RFC 9001 using TLS to secure QUIC. 2021. https://www.rfc-editor.org/info/rfc9001
[37] Iyengar J, Swett I. RFC 9002 QUIC loss detection and congestion control. 2021. https://www.rfc-editor.org/info/rfc9002
[38] Bishop M. RFC 9114 HTTP/3. 2022. https://www.rfc-editor.org/info/rfc9114
[39] Huitema C, Dickinson S, Mankin A. RFC 9250 DNS over dedicated QUIC connections. 2022. https://www.rfc-editor.org/info/rfc9250
[40] Dierks T, Rescorla E. RFC 5246 The transport layer security (TLS) protocol version 1.2. 2008. https://www.rfc-editor.org/info/rfc5246
[41] Rescorla E. RFC 8446 The transport layer security (TLS) protocol version 1.3. 2018. https://www.rfc-editor.org/info/rfc8446
[42] Duckett C. Google public DNS gets DNS-over-TLS treatment. 2019. https://www.zdnet.com/article/google-public-dns-gets-dns-over-tls-treatment/
[43] Deckelmann S. Firefox continues push to bring DNS over HTTPS by default for US users. 2020. https://blog.mozilla.org/blog/2020/02/25/firefox-continues-push-to-bring-dns-over-https-by-default-for-us-users/
[44] Chromium blog: A safer and more private browsing experience with secure DNS. 2020. https://blog.chromium.org/2020/05/a-safer-and-more-private-browsing-DoH.html
[45] Apple enable encrypted DNS. 2020. https://developer.apple.com/videos/play/wwdc2020/10047/
[46] DNS over TLS support in Android developer preview. 2018. https://android-developers.googleblog.com/2018/04/dns-over-tls-support-in-android-p.html
[47] Improving DNS configuration in Settings. 2020. https://blogs.windows.com/windows-insider/2020/08/05/announcing-windows-10-insider-preview-build-20185/
[48] Luo M, Yao YP, Xin LL, Jiang ZW, Wang QY, Shi WC. Measurement for encrypted open resolvers: Applications and security. Computer Networks, 2022, 213: 109081. [doi: 10.1016/j.comnet.2022.109081]
[49] Lu CY, Liu BJ, Li Z, Hao S, Duan HX, Zhang MM, Leng CY, Liu Y, Zhang ZF, Wu JP. An end-to-end, large-scale measurement of DNS-over-encryption: How far have we come? In: Proc. of the 2019 Internet Measurement Conf. Amsterdam: ACM, 2019. 22–35. [doi: 10.1145/3355369.3355580]
[50] García S, Hynek K, Vekshin D, Čejka T, Wasicek A. Large scale measurement on the adoption of encrypted DNS. arXiv:2107.04436, 2021.
[51] Kosek M, Doan TV, Granderath M, Bajpai V. One to rule them all? A first look at DNS over QUIC. In: Proc. of the 23rd Int'l Conf. on Passive and Active Network Measurement. Springer, 2022. 537–551. [doi: 10.1007/978-3-030-98785-5_24]
[52] Böttger T, Cuadrado F, Antichi G, Fernandes EL, Tyson G, Castro I, Uhlig S. An empirical study of the cost of DNS-over-HTTPS. In: Proc. of the 2019 Internet Measurement Conf. Amsterdam: ACM, 2019. 15–21. [doi: 10.1145/3355369.3355575]
[53] Firefox nightly secure DNS experimental results. 2018. https://blog.nightly.mozilla.org/2018/08/28/firefox-nightly-secure-dns-experimental-results/

[54] Hounsel A, Schmitt P, Borgolte K, Feamster N. Can encrypted DNS be fast? In: Proc. of the 22nd Int'l Conf. on Passive and Active Network Measurement. Springer, 2021. 444–459. [doi: 10.1007/978-3-030-72582-2_26]

[55] Doan TV, Tsareva I, Bajpai V. Measuring DNS over TLS from the edge: Adoption, reliability, and response times. In: Proc. of the 22nd Int'l Conf. on Passive and Active Network Measurement. Springer, 2021. 192–209. [doi: 10.1007/978-3-030-72582-2_12]

[56] Hounsel A, Borgolte K, Schmitt P, Holland J, Feamster N. Comparing the effects of DNS, DoT, and DoH on Web performance. In: Proc. of the 2020 Web Conf. Taipei: ACM, 2020. 562–572. [doi: 10.1145/3366423.3380139]

[57] Deccio C, Davis J. DNS privacy in practice and preparation. In: Proc. of the 15th Int'l Conf. on Emerging Networking Experiments and Technologies. Orlando: ACM, 2019. 138–143. [doi: 10.1145/3359989.3365435]

[58] Borgolte K, Chattopadhyay T, Feamster N, Feamster N, Kshirsagar M, Holland J, Hounsel A, Schmitt P. How DNS over HTTPS is reshaping privacy, performance, and policy in the Internet ecosystem. In: Proc. of the 47th Research Conf. on Communications, Information and Internet Policy. 2019. [doi: 10.2139/ssrn.3427563]

[59] Mayrhofer A. RFC 7830 The EDNS(0) padding option. 2016. https://www.rfc-editor.org/info/rfc7830

[60] Mayrhofer A. RFC 8467 Padding policies for extension mechanisms for DNS (EDNS(0)). 2018. https://www.rfc-editor.org/info/rfc8467

[61] Mühlhauser M, Pridöhl H, Herrmann D. How private is Android's private DNS setting? Identifying apps by encrypted DNS traffic. In: Proc. of the 16th Int'l Conf. on Availability, Reliability and Security. New York: ACM, 2021. 1–10. [doi: 10.1145/3465481.3465764]

[62] Hynek K, Cejka T. Privacy illusion: Beware of unpadded DoH. In: Proc. of the 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conf. Vancouver: IEEE, 2020. 621–628. . [doi: 10.1109/IEMCON51383.2020.9284864]

[63] Bushart J, Rossow C. Padding ain't enough: Assessing the privacy guarantees of encrypted DNS. In: Proc. of the 10th USENIX Workshop on Free and Open Communications on the Internet. Santa Clara: USENIX Association, 2020.

[64] Houser R, Li Z, Cotton C, Wang HN. An investigation on information leakage of DNS over TLS. In: Proc. of the 15th Int'l Conf. on Emerging Networking Experiments and Technologies. Orlando: ACM, 2019. 123–137. [doi: 10.1145/3359989.3365429]

[65] Vekshin D, Hynek K, Cejka T. DoH insight: Detecting DNS over HTTPS by machine learning. In: Proc. of the 15th Int'l Conf. on Availability, Reliability and Security. ACM, 2020. 87. [doi: 10.1145/3407023.3409192]

[66] Meng DC, Zou FT. DNS privacy protection security analysis. Communications Technology, 2020, 53(2): 445–449 (in Chinese with English abstract). [doi: 10.3969/j.issn.1002-0802.2020.02.028]

[67] Siby S, Juarez M, Diaz C, Vallina-Rodriguez N, Troncoso C. Encrypted DNS→privacy? A traffic analysis perspective. In: Proc. of the 27th Annual Network and Distributed System Security Symp. San Diego: The Internet Society, 2020. [doi: 10.14722/ndss.2020.24301]

[68] Hoang NP, Niaki AA, Gill P, Polychronakis M. Domain name encryption is not enough: Privacy leakage via IP-based website fingerprinting. Proc. on Privacy Enhancing Technologies, 2021, 2021(4): 420–440. [doi: 10.2478/popets-2021-0078]

[69] Jin L, Hao S, Wang HN, Cotton C. Understanding the impact of encrypted DNS on internet censorship. In: Proc. of the 2021 Web Conf. Ljubljana: ACM, 2021. 484–495. [doi: 10.1145/3442381.3450084]

[70] Rescorla E, Oku K, Sullivan N, Wood CA. TLS encrypted client hello. 2022. https://datatracker.ietf.org/doc/html/draft-ietf-tls-esni-14

[71] Hoang NP, Niaki AA, Borisov N, Gill P, Polychronakis M. Assessing the privacy benefits of domain name encryption. In: Proc. of the 15th ACM Asia Conf. on Computer and Communications Security. Taipei: ACM, 2020. 290–304. [doi: 10.1145/3320269.3384728]

[72] Contavalli C, van der Gaast W, Lawrence D, Kumari W. RFC 7871 client subnet in DNS queries. 2016. https://www.rfc-editor.org/info/rfc7871

[73] How we made DNS both fast and private with ECS. 2021. https://medium.com/nextdns/how-we-made-dns-both-fast-and-private-with-ecs-4970d70401e5

[74] Moura GCM, Castro S, Hardaker W, Wullink M, Hesselman C. Clouding up the Internet: How centralized is DNS traffic becoming? In: Proc. of the 2020 ACM Internet Measurement Conf. ACM, 2020. 42–49. [doi: 10.1145/3419394.3423625]

[75] Final DoH letter. 2019. https://www.ncta.com/sites/default/files/2019-09/Final%20DOH%20LETTER%209-19-19.pdf

[76] Hounsel A, Schmitt P, Borgolte K, Feamster N. Encryption without centralization: Distributing DNS queries across recursive resolvers. In: Proc. of the 2021 Applied Networking Research Workshop. ACM, 2021. 62–68. [doi: 10.1145/3472305.3472318]

[77] Hoang NP, Lin I, Ghavamnia S, Polychronakis M. K-resolver: Towards decentralizing encrypted DNS resolution. In: Proc. of the 2020 NDSS Workshop on Measurements, Attacks, and Defenses for the Web. San Diego: Internet Society. 2020. [doi: 10.14722/madweb.2020.23009]

[78] Turing A, Ye GS. An analysis of Godlua backdoor. 2019. https://blog.netlab.360.com/an-analysis-of-godlua-backdoor-en/

[79] Cimpanu C. Iranian hacker group becomes first known APT to weaponize DNS-over-HTTPS (DoH). 2020. https://www.zdnet.com/article/iranian-hacker-group-becomes-first-known-apt-to-weaponize-dns-over-https-doh/

[80] Bumanglag K, Kettani H. On the impact of DNS over HTTPS paradigm on cyber systems. In: Proc. of the 3rd Int'l Conf. on Information

and Computer Technologies. San Jose: IEEE, 2020. 494–499. [doi: 10.1109/ICICT50521.2020.00085]

[81] Patsakis C, Casino F, Katos V. Encrypted and covert DNS queries for botnets: Challenges and countermeasures. Computers & Security, 2020, 88: 101614. [doi: 10.1016/j.cose.2019.101614]

[82] Zhang QF, Guo XJ, Zhou PJ. DGA identification method based on DoH traffic. Computer Technology and Development, 2021, 31(12): 122–127 (in Chinese with English abstract). [doi: 10.3969/j.issn.1673-629X.2021.12.021]

[83] Banadaki YM. Detecting malicious DNS over HTTPS traffic in domain name system using machine learning classifiers. Journal of Computer Sciences and Applications, 2020, 8(2): 46–55. [doi: 10.12691/jcsa-8-2-2]

[84] MontazeriShatoori M, Davidson L, Kaur G, Lashkari AH. Detection of DoH tunnels using time-series classification of encrypted traffic. In: Proc. of the 2020 IEEE Int'l Conf. on Dependable, Autonomic and Secure Computing, Int'l Conf. on Pervasive Intelligence and Computing, Int'l Conf. on Cloud and Big Data Computing, Int'l Conf. on Cyber Science and Technology Congress. Calgary: IEEE, 2020. 63–70. [doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00026]

[85] Singh SK, Roy PK. Detecting malicious DNS over HTTPS traffic using machine learning. In: Proc. of the 2020 Int'l Conf. on Innovation and Intelligence for Informatics, Computing and Technologies. Sakheer: IEEE, 2020. 1–6. [doi: 10.1109/3ICT51146.2020.9312004]

[86] Kwan C, Janiszewski P, Qiu SL, Wang C, Bocovich C. Exploring simple detection techniques for DNS-over-HTTPS tunnels. In: Proc. of the 2021 ACM SIGCOMM Workshop on Free and Open Communications on the Internet. New York: Association for Computing Machinery, 2021. 37–42. [doi: 10.1145/3473604.3474563]

[87] Zhan MQ, Li Y, Yu GX, Li B, Wang WP. Detecting DNS over HTTPS based data exfiltration. Computer Networks, 2022, 209: 108919. [doi: 10.1016/j.comnet.2022.108919]

[88] Ding S, Zhang DQ, Ge JG, Yuan XW, Du XH. Encrypt DNS traffic: Automated feature learning method for detecting DNS tunnels. In: Proc. of the 2021 IEEE Int'l Conf. on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking. New York: IEEE, 2021. 352–359. [doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00056]

[89] Nguyen TA, Park M. DoH tunneling detection system for enterprise network using deep learning technique. Applied Sciences, 2022, 12(5): 2416. [doi: 10.3390/app12052416]

[90] Huang Q, Chang DL, Li Z. A comprehensive study of DNS-over-HTTPS downgrade attack. In: Proc. of the 10th USENIX Workshop on Free and Open Communications on the Internet. USENIX Association, 2020. 1–8.

[91] Zhang JW, An YJ, Deng HY. A survey on DNS attack detection and security protection. Telecommunications Science, 2022, 38(9): 1–17 (in Chinese with English abstract). [doi: 10.11959/j.issn.1000-0801.2022248]

[92] Hu N, Deng WP, Yao S. Issues and challenges of Internet DNS security. Chinese Journal of Network and Information Security, 2017, 3(3): 13–21 (in Chinese with English abstract). [doi: 10.11959/j.issn.2096-109x.2017.00154]

[93] Pearce P, Jones B, Li F, Ensafi R, Feamster N, Weaver N, Paxson V. Global measurement of DNS manipulation. In: Proc. of the 26th USENIX Conf. on Security Symp. Vancouver: USENIX Association, 2017. 307–323.

[94] Pauly T, Kinnear E, Wood CA, McManus P, Jensen T. Discovery of designated resolvers. 2022. https://www.ietf.org/archive/id/draft-ietf-add-ddr-10.html

[95] Boucadair M, Reddy T, Wing D, Cook N, Jensen T. DHCP and router advertisement options for the discovery of network-designated resolvers. 2023. https://www.ietf.org/archive/id/draft-ietf-add-dnr-16.html

[96] Schwartz B, Box C. Discovery of designated resolvers in the presence of legacy forwarders. 2021. https://www.ietf.org/archive/id/draft-schwartz-add-ddr-forwarders-01.html

[97] Statement on DNS Encryption. 2021. https://root-servers.org/media/news/Statement_on_DNS_Encryption.pdf

[98] Kumari W, Hoffman P. RFC 8806 running a root server local to a resolver. 2020. https://www.rfc-editor.org/info/rfc8806

[99] Gillmor DK, Salazar J, Hoffman P. Unilateral opportunistic deployment of encrypted recursive-to-authoritative DNS. 2023. https://www.ietf.org/archive/id/draft-ietf-dprive-unilateral-probing-06.html

[100] Security/DoH-resolver-policy. 2021. https://wiki.mozilla.org/Security/DOH-resolver-policy

[101] Kinnear E, McManus P, Pauly T, Verma T, Wood CA. RFC 9230 oblivious DNS over HTTPS. 2022. https://www.rfc-editor.org/info/rfc9230

[102] Singanamalla S, Chunhapanya S, Hoyland J, Vavruša M, Verma T, Wu P, Fayed M, Heimerl K, Sullivan N, Wood C. Oblivious DNS over HTTPS (ODoH): A practical privacy enhancement to DNS. Proc. on Privacy Enhancing Technologies, 2021, 2021(4): 575–592. [doi: 10.2478/popets-2021-0085]

[103] Alecmuffett. Dohot: Making practical use of DNS over HTTPS over Tor. 2020. https://github.com/alecmuffett/dohot/blob/master/papers/

no-port-53-who-dis-paper-3.1.pdf
[104] How Facebook is bringing QUIC to billions. 2020. https://engineering.fb.com/2020/10/21/networking-traffic/how-facebook-is-bringing-quic-to-billions/
[105] DNS over HTTP3 in Android. 2022. https://security.googleblog.com/2022/07/dns-over-http3-in-android.html

**附中文参考文献**:

[8] 王文通, 胡宁, 刘波, 刘欣, 李树栋. DNS安全防护技术研究综述. 软件学报, 2020, 31(7): 2205–2220. http://www.jos.org.cn/1000-9825/6046.htm [doi: 10.13328/j.cnki.jos.006046]
[9] 黄锴, 孔宁. DNS隐私问题现状的研究. 计算机工程与应用, 2018, 54(9): 28–36. [doi: 10.3778/j.issn.1002-8331.1801-0101]
[66] 孟德超, 邹福泰. DNS隐私保护安全性分析. 通信技术, 2020, 53(2): 445–449. [doi: 10.3969/j.issn.1002-0802.2020.02.028]
[82] 张千帆, 郭晓军, 周鹏举. 基于DoH流量的DGA识别方法. 计算机技术与发展, 2021, 31(12): 122–127. [doi: 10.3969/j.issn.1673-629X.2021.12.021]
[91] 章坚武, 安彦军, 邓黄燕. DNS攻击检测与安全防护研究综述. 电信科学, 2022, 38(9): 1–17. [doi: 10.11959/j.issn.1000-0801.2022248]
[92] 胡宁, 邓文平, 姚苏. 互联网DNS安全研究现状与挑战. 网络与信息安全学报, 2017, 3(3): 13–21. [doi: 10.11959/j.issn.2096-109x.2017.00154]

**张曼**(1992－), 女, 工程师, 主要研究领域为互联网基础资源治理, 网络安全.

**董科军**(1977－), 男, 博士, 正高级工程师, CCF 高级会员, 主要研究领域为互联网基础资源管理, 云计算, 分布式系统, 网络协同技术.

**姚健康**(1978－), 男, 博士, 研究员, CCF 专业会员, 主要研究领域为 DNS 等互联网基础技术资源, 网络安全, 互联网治理.

**延志伟**(1985－), 男, 博士, 研究员, CCF 专业会员, 主要研究领域为互联网名址协议, 网络安全, 下一代网络架构.

**李洪涛**(1977－), 男, 正高级工程师, CCF 高级会员, 主要研究领域为计算机应用技术, 下一代互联网架构, 互联网基础资源新型解析技术, 大数据分析.