一个自主开放的互联网根域名解析体系

张 宇[1], 夏重达[1], 方滨兴[1,2], 张宏莉[1]

[1]哈尔滨工业大学计算机科学与技术学院 计算机网络与信息安全技术研究中心, 哈尔滨 中国 150001
[2]东莞电子科技大学电子信息工程研究院, 东莞 中国 523808

摘要 域名系统(Domain Name System, DNS)的中心化根解析体系蕴含着权力滥用风险, 对互联网的开放与平等形成威胁。本文提出了一个新的自主开放根解析体系, 与现有 DNS 兼容的同时, 从结构和机制两方面对权力滥用予以威慑。首先, 针对域名唯一性与去中心化之间矛盾, 提出了授权与解析分离机制, 在保留单一根权威的条件下, 实现解析服务去中心化。接着, 针对中心式结构风险, 提出建立国家根与根联盟, 通过自治与合作实现权力制衡。然后, 分析了新体系防范风险的有效性以及在当前 DNS 基础之上的增量, 并讨论新体系所具有的自主、开放、平等、透明性质。最后, 对新体系的安全性进行分析并给出了一个原型系统。

关键词 域名系统; 根; 去中心化; 互联网治理
中图法分类号 TP393.4 **DOI 号** 10.19363/j.cnki.cn10-1380/tn.2017.10.005

An Autonomous Open Root Resolution Architecture for Domain Name System in the Internet

ZHANG Yu[1], XIA Zhongda[1], FANG Binxing[1,2], ZHANG Hongli[1]

[1] Research Center of Computer Network and Information Security Technology, Department of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China
[2] Institute of Electronic and Information Engineering in Dongguan, University of Electronic Science and Technology of China, Dongguan 523808, China

Abstract The current DNS (Domain Name System) root resolution architecture has the risk of power abuse which posts threats on the openness and equality of the Internet. This paper presents a new DNS-compatible autonomous open root resolution architecture to effectively prevent the power abuse from the perspectives of structure and mechanism. First, aiming at the dilemma between the name uniqueness and decentralization, we propose the separation of delegation and resolution to decentralize resolution service while keeping a single root authority. Then, to cope with the risk in the centralized structure, we propose a structure with country roots and inter-root to provide power balancing. We analyze the effectiveness of the new architecture against the abuse threats and the changes on current DNS. We discuss the autonomy, openness, equality and transparency of the new architecture. We also analyze the security of the new architecture and implement a prototype.

Key words Domain Name System; root; decentralization; Internet governance

1 引言

域名系统(Domain Name System, DNS)作为构建互联网的基石之一, 主要负责域名到IP地址的映射。DNS 体系结构包括四要素[1]: 1) 名字空间: 表示为一棵标签树, 树根所对应的区域, 称作根区。2) 一个分布式数据库: 由全体权威服务器及其区文件构成。负责根区解析的权威服务器, 为根服务器。3) 递归解析器: 互联网用户通过递归解析器实现域名解析, 递归解析器通过自顶向下的迭代查询来访问权威服务器。4) 解析协议: 系统各组件间通信协议。

DNS 名字空间结构、域名分配和解析过程都是严格层级化, 其中, 根区是名字空间的最高层, 根服务器提供根区解析服务。根解析体系作为域名解析起点和系统结构中心, 包括根区、根服务器及相关结构、协议、数据和服务。

通讯作者: 夏重达, 博士研究生, Email: xiazhongda@hit.edu.cn。
本课题得到广东省产学研合作项目“广东省健康云安全院士工作站”(No. 2016B090921001), 国家重点基础研究发展计划(“973”计划)(No.2011CB302605, No.2013CB329602), 国家自然科学基金(No.61202457, No.61402149)资助。
收稿日期: 2016-07-15; 修改日期: 2017-05-22; 定稿日期: 2017-08-23

目前, 域名、IP 地址、AS 号等关键互联网资源管理权属于美国商务部下属国家电信和信息管理局(National Telecommunications and Information Administration, NTIA)的互联网数字分配机构(Internet Assigned Numbers Authority, IANA)。NTIA 将 IANA 职能授权给美国互联网名称与数字地址分配机构(Internet Corporation for Assigned Names and Numbers, ICANN)。在政策上, IANA 职能被一分为二: ICANN 负责顶级域(Top Level Domain, TLD)注册和授权, 美国威瑞信公司(VeriSign)负责运维根区数据。TLD 运营商对根区的修改申请经 ICANN 同意与 NTIA 审批后, 由 VeriSign 对根区文件进行实际修改, 发布到 12 家根运营机构下的 13 个根服务器及其镜像。这一中心化结构通过域名系统安全扩展(DNS Security Extension, DNSSEC)[2]得到了密码学保护, 自 2010 年起部署的根密钥签名密钥(Key Signing Key, KSK)为信任锚。2014 年 NTIA 宣布有意将 IANA 职能移交给一个新的全球多利益攸关方组织。需要明确的是, IANA 职能移交并不改变当前根体系。

文献[3]中提出, DNS 根中心化结构蕴含权力滥用风险:

1) 消失性风险, 指从根区文件中删除特定顶级域名资源记录, 令网络用户无法访问该顶级域名下网站。若被删除的是一个国家的国家代码顶级域(country code Top Level Domain, ccTLD), 则该国域名下的域名体系也会跟着土崩瓦解, 这是一种“一国互联网被从国际互联网抹掉的风险”。

2) 致盲性风险, 只要根服务器及镜像拒绝为特定范围内递归服务器提供解析服务, 依赖相关递归服务器的用户就会因无法获得解析服务而无法上网。若针对一个国家, 则这是一种“一国网络用户被禁止互联网访问的风险”。

上述风险涉及对根区具有管理或操作权力的中心机构的信任问题。本文假设 IANA 发布的根区文件及根运维机构所提供的解析服务不可信。

根权力滥用风险严重危害互联网的开放与平等。首先, 开放的互联网应允许自由接入和通信, 但目前一国的域名解析需依赖于根权威, 国家间通信也绕不开根, 一旦根权威滥用权力, 将导致一国网络被关闭, 国家间通信中断。其次, 平等的互联网中各国网络应处于对等位置, 但根权威处于最高层级, 其他国家处于下一层级, 中心化根权威所具有的非对称能力令其凌驾于各国网络之上。因此, 为了互联网持续健康发展, 根权力滥用风险亟待解决。

在蓄意撤销域名或对特定用户拒绝服务的问题上仍存在争议, 已非单纯学术和技术问题, 涉及政治、经济、法律等多个领域, 极为复杂, 相关政策性讨论见文献[4,5], 非本文所研究内容。本文只从学术角度上剖析根问题, 希望对其他领域相关讨论提供有益输入。

本文针对上述问题提出一个新的根解析体系, 其核心思想是在于两点: 首先, 针对域名唯一性与去中心化两难问题, 提出了授权与解析分离机制, 在保留单一根权威的条件下, 实现解析服务去中心化; 其次, 针对中心式结构风险, 提出建立国家根与根联盟, 通过自治与合作来制衡权力, 实现开放平等互联。本文其余部分组织如下: 第 2 章分析相关工作; 第 3 章给出新体系设计目标; 第 4 章描述新体系设计; 第 5 章讨论新体系所具备性质; 第 6 章介绍试验系统; 最后总结本文。

2 相关工作

针对根解析体系中心性特征, 一类方案是对 DNS 根服务器去中心化。下面对 5 种该类方案按其技术特征来命名并介绍。

1) 递归根: 在递归解析器上直接做根区解析, 相当于建立一个本地根服务器。由 Google 推动, 用于其公开递归服务器 8.8.8.8, 以去掉递归到根服务器间延迟[6]。

2) 伪装根: 部分运营商将用户到根服务器查询引导到伪装的根镜像来进行根区解析, 以减少查询延迟和提高可靠性。

3) 开放根: 建立一组独立运作的根服务器, 平时采用 IANA 根区数据, 可不做删除操作, 但也无法保证获得最新数据,例如 ORSN (www.orsn.net), 我国机构参与面向 IPv6 的雪人计划 (www.yeti-dns.org)。ORSN 项目在欧洲发起, 其初衷是解决根服务器地理分布不均衡问题以及改变根区治理被一国垄断的格局, 该项目在欧洲各国部署根服务器, 由各国共同运营。雪人计划基于 IPv6 协议独立地提供根区解析服务, 提供了一个 DNS 试验平台。ORSN 和雪人计划均承诺所使用的根区数据与 IANA 保持一致, 不提供 TLD 注册服务, 也不创建新的名字空间。

4) 全球根: 中国互联网信息中心参与提出, 在当前 DNS 体系内添加一个称作全球任播根服务器(Universal Anycast Root Server, UARS)的逻辑根服务器, 任何组织都可以搭建一台 UARS 服务器, 利用任播技术实现对特定区域根区解析服务[7]。

5) 另类根: 建立一个完全独立于当前 IANA 体系的 DNS 系统, 相当于建立了一个另类名字空间,

这类域名通常称作“另类域名/山寨域名”, 如Public-Root (www.public-root.com)、Unifiedroot (www.unifiedroot.com)、ORSC(www.open-rsc.org), 此类方案不属于当前 DNS 体系, 不满足统一名字空间需求。

除另类根外, 上述方案都尽量保证与现有体系兼容。另类根则具有完全独立的名字空间。各方案与现有体系关系可参考图 1。

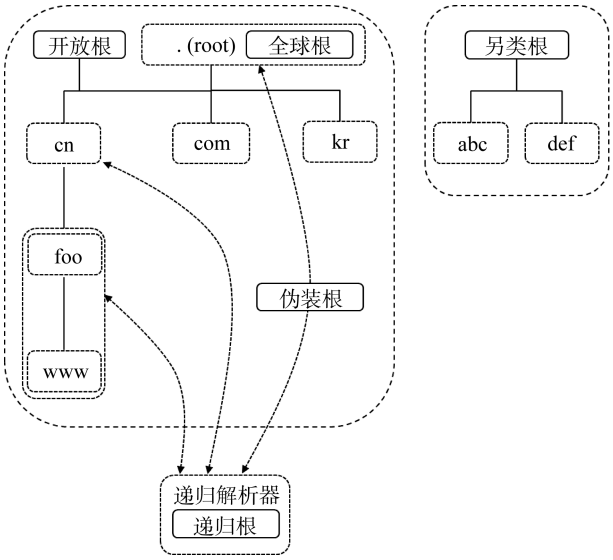

图 1 各根去中心化方案与现有体系关系

前四种方案从本质上是对根区解析服务去中心化, 递归根和伪装根不提供公开根区解析服务, 是一种性能优化方案, 开放根和全球根则建立独立的根服务器, 与原根共存。他们的一个共同点是, 根区数据依然来自 IANA, 并没有改变 DNS 根中心化结构, 权力滥用风险依然存在。

对等网思想也被应用于 DNS, 此类方案实现了部分 DNS 系统组件去中心化, 或针对解析功能[8-11], 或针对权威服务器[12], 但并未提出完整可替代的根解析体系, 因而对根权力滥用的遏制能力有限。

Namecoin[13]基于Bitcoin所采用的区块链技术实现分布式键值对数据库, 目前用于.bit 域名注册。该方案实现了域名注册与分配去中心化, 这种彻底无权威体系导致域名抢注问题并缺乏争议处理机制, 如何与当前 DNS 体系融合尚不清楚。

下面分析上述三类方案的优缺点, 并与本文所提方案进行比较。根去中心化方案本质上是一种“根镜像”, 能够做到与现有 DNS 体系兼容, 并一般要保证根区数据与 IANA 完全一致, 其优点是能直接应用到现有体系中, 并一定程度上提高根可用性, 缺点在于不能应对消失性风险; 对等网方案提出了分布式的域名信息存储和查询方案, 需要新的客户端和服务器软件支持, 其优点在于其大大提高了 DNS 解析体系的性能和健壮性, 缺点在于实施难度大, 为现有体系带来显著增量, 且同样不能应对消失性风险; Namecoin 则是一种完全去中心化体系, 优点在于完全去除了对根的依赖, 彻底消除权力滥用风险, 缺点在于不兼容当前 DNS 体系, 缺乏与 IANA 的一致性。

表 1 相关工作比较

方案	兼容性	一致性	应对风险	
			致盲性	消失性
根镜像	√	√	√	×
对等网	×	√	√	×
Namecoin	×	×	√	√

本文所提方案与以往工作的关系如下。首先, 不同于根镜像方案, 本文方案中根区数据来源不限于IANA, 通过TLD权威直接公开根区数据及国家根间根区数据交换实现了数据源头上的去中心化。其次, 不同于无中心的对等网和区块链方案, 本文方案保留 IANA 作为唯一顶级域授权管理者的角色, 从而保证了名字空间统一, 通过授权与解析分离机制, 实现了去中心化解析。

3 设计目标

新根解析体系设计的出发点来自于应对根权威权力滥用风险, 但这并不是设计新体系时所追求的最终目标, 而是三个更为重要目标的副产品。 这三个设计目标按重要程度排序如下:

3.1 域名空间统一与域名唯一性

统一的域名空间是互联网作为一个整体的关键, 而分裂的域名空间将极大阻碍互联互通, 增加新服务部署成本, 并提高域名仿冒风险。互联网体系结构委员会(Internet Architecture Board, IAB)给出 DNS 采用单根的理由在于, “为维护一个全球网络, 互联网需要一个全局唯一的公开名字空间。 DNS 名字空间是一个源自单个全局唯一根的层级结构名字空间。这是 DNS 设计中内在的技术限制” [14]。单信任锚意味着单数据源, 在保证了域名分配唯一性与数据一致性同时简化了信任模型。IAB 认为, DNSSEC 信任链与该层级结构一致具有很多优点, 通过广泛采纳单一信任锚可建立全局信任[15]。因此, 新体系必须确保 DNS 名字空间统一。

域名唯一性是 DNS 最基本的功能与安全属性。Zooko 三角猜想[16]提出, 任何命名体制只能在唯一性(或称安全性)、去中心化和有意义中三选二。唯一

性指的是一个名字所对应的对象是唯一的;去中心化指的是名字分配是去中心化的; 有意义指的是名字是人们可理解的、对用户来说具有意义。DNS 基本功能决定了需要具有唯一性, 同时要具有用户可理解性, 因此牺牲了非中心化; 牺牲唯一性的方案类似 QQ 昵称; 比特币地址采用公钥指纹为名字, 牺牲有意义。若 Zooko 三角猜想成立, 则任何对 DNS 域名分配去中心化的尝试都可能是徒劳的。

因此, 如何在保证域名空间统一与域名唯一性条件下, 实现域名解析体系去中心化是一个挑战。

3.2 域名解析的自主、开放与平等

自主域名解析是指一个国家或地区的域名解析不依赖于其他人, 能够独立保障本国范围内域名解析安全与可靠。当前 DNS 体系具备有限自主性, 顶级域权威可自主管理所在域, 但依赖于根权威将域名解析请求引导到顶级域权威服务器。自主性并不能通过单纯的建立一个新的根服务器或镜像来实现, 因为根区文件仍然来自于根权威。实现自主性是防范根权威权力滥用的基础, 或者说不能防范权力滥用, 则不具备自主性。

新体系应维护和促进互联网开放。首先, 新体系的设计与标准的制定都应该是开放性的, 经过广泛参与和充分讨论的。其次, 新体系应面向全世界开放, 能够自由加入和退出, 不存在壁垒。另外, 新体系中解析服务也应面向整个互联网, 不存在地域性。

新体系应遵循平等原则, 各成员处于同一层级, 或通过协商形成上下层级。不能在去除原体系中最高权威同时, 又以其他形式树立出一个新权威。当然, 平等要建立在域名空间统一与域名唯一性的基础之上, 以避免域名空间分裂与混乱。

3.3 最小化设计、开发与部署成本

新体系的定位是对当前 DNS 系统的改进, 并非一个全新的域名系统。鉴于作为 DNS 扩展的 DNSSEC 的设计、开发与部署所经历的漫长过程, 在一个成功体系上建立新体系极为困难。为了新体系不只是纸上谈兵, 其成本不仅包括人力与物力, 还包括系统复杂性, 与原系统软硬件兼容性, 部署动机以及新体系所带来变化所产生的社会成本。

从技术角度来看, 当前 DNS 中心式层级式体系设计简单且高效, DNS 的成功也证明其技术的有效性与先进性。新体系应通过最大化继承当前 DNS 体系, 充分利用现有系统和技术, 在避免“重新发明轮子”的同时, 继承 DNS 的分布、高效、可靠等优点。以不影响当前 DNS 系统为前提, 为最小化部署成本, 应尽量与当前 DNS 体系兼容, 以现有 DNS 软件为基础、利用当前 DNS 基础设施, 追求渐进部署。新体系设计应紧密围绕在根解析本身, 不涉及其他 DNS 功能和性能问题。

4 新体系设计

以上述目标为设计方向, 为实现自主与开放的新体系, 从两个方面打破当前单中心的根解析体系。首先, 针对域名空间统一与去中心化两难问题, 提出域名授权与域名解析分离的思想, 在保持域名空间统一与域名唯一性的同时, 将根区解析服务独立出来, 实现权威数据与解析服务分离, 在承认 IANA 为根权威的前提下建立多根解析体系; 接着, 针对中心式结构风险, 从根区管理的角度出发, 设计一种新的多根结构, 打破当前的中心化根区管理体系, 体现 TLD 权威在根区管理体系中的权力, 在一定程度上规避中心式结构中权力滥用风险。

4.1 核心思想

新体系的核心思想是将 TLD 的分配与解析相分离。新体系与当前 DNS 体系示意图如图 2 所示。当前 DNS 体系中, TLD 由 IANA 分配给 TLD 权威机构, TLD 权威机构将权威服务器 IP 地址提交给 IANA, 由 IANA 写入根区文件并提供解析。在新体系中, 依旧由 IANA 负责 TLD 分配, 但由一个新根联盟(后面具体阐述)负责域名解析。新体系与当前 DNS 相同点在于, 仍然是 IANA 负责 TLD 分配, 不同之处在于, TLD 权威通过根联盟发布包括其域名权威服务器 IP 地址在内的 TLD 权威信息。

通过 TLD 的分配与解析相分离, 一方面保证了域名空间统一与域名唯一性。在新体系下, IANA 仍然是域名空间中唯一的根管理者, 以此保证名字分配公正与唯一。所有 TLD 注册机构仍然需要向 IANA 实体申请域名或提交根区修改申请, 之后由 IANA 来授权。另一方面, 由于当前根服务器与根联盟体系并存, 域名解析已摆脱完全依赖于单一权威的现状, 从而实现了解析服务的去中心化。上述两方面一起使得新体系在满足了统一域名空间与名字唯一性需求的同时, 实现了对根权威权力的制衡。

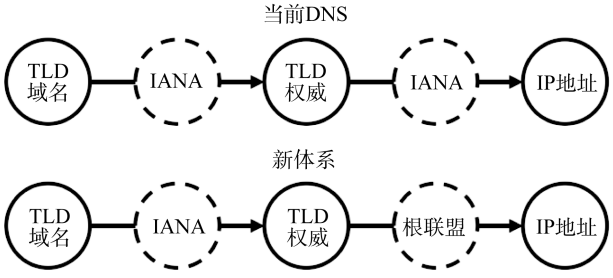

图 2 新旧根解析体系示意图

上述思想在两个层面上具有重要的意义。在根区解析服务的层面, 新的体系将授权与解析分离, 由根联盟中各国家根节点独立提供根区解析服务, 与目前的根服务器共存; 在根区管理层面, 新体系在承认 IANA 的 TLD 分配权威地位同时, 在根联盟内, 同时体现 TLD 权威对域名的直接所有权和控制权, 匹配当前互联网开放平等的治理结构, 从一定程度上规避根权威权力滥用风险。

4.2 体系结构

基于上述思想设计的新体系包括两个核心组件:

1) 国家根: 国家运维的根服务器, 与当前 DNS 下 13 个根服务器以及其他类型根服务器并存, 不存在任何独占性或者冲突; 国家根提供包括根解析在内的解析服务, 同时能够与其他国家根对等地进行数据交换; 在新体系中, 国家根是本国 ccTLD 及其他本国 TLD 的权威。

2) 根联盟: 多个国家根基于对等协议组成根联盟, 联盟内成员自愿交换包括本国 ccTLD 及其他可信域名在内的信息, 从而使得根解析系统结构与互联网开放平等的治理结构相匹配。如图 3 所示, 假设中国与韩国分别建立了国家根, 两个国家根之间形成联盟, 并交换彼此掌握的根区信息, 主要包括本国 TLD 信息。同时, 每个国家根可自主决定对交换所得信息的信任度及用途。例如, 承认某国家根是其国家 ccTLD 的绝对权威, 并当交换所得信息与来自 IANA 的信息出现冲突时, 采用来自国家根的信息。

国家根及根联盟与原根并存, 同时提供根区解析服务, 递归解析器可以自主选择使用根联盟内的国家根还是原根作为根服务器, 或以原根为主、根联盟为辅。

基于上述描述, 在新的体系中, 国家根扮演两个主要角色:

1) 根区解析服务提供者: 从 IANA, 本国 TLD 等源获取根区信息, 对不同来源的数据进行合并, 处理信息冲突, 生成根区数据, 并使用生成的根区数据提供可靠的根区解析服务。这实现了根区信息的授权与解析相分离, 以及解析服务去中心化。同时, 每个国家代表了根区管理体系中的主要利益攸关方, 其独立提供的根区解析服务能最大保证本国 TLD 的解析安全。

2) 根联盟中的对等节点: 与根联盟中的其他国家根形成对等关系, 交换包括 ccTLD 在内的 TLD 信息。每个国家根都是本国 ccTLD 的绝对权威, 实现了互联网分治, 对于其他国家根来说, 是本国 ccTLD 的权威数据源。同时, 可以直接为联盟中其他节点直接提供递归解析服务, 作为一种应急措施, 提升根联盟整体的 DNS 解析健壮性。

国家根的建立符合 DNS 设计之初的基本原则之一, 即域名管理结构与域名解析结构一致。当前 DNS 解析的单根逻辑结构已经难以满足如今的互联网治理需求, 缺乏对开放互联与多方共治的结构性支撑。国家根体现了国家这一互联网治理主体在 DNS 体系中角色, 实现了多根解析结构, 同时又不破坏域名空间的统一性。

单纯建立国家根本身不能实现彻底去中心化, 因为根区文件来源仍然是根区管理者 IANA。为此, 建立根联盟的目的就是实现根区信息交换, 解决根区信息来源单一的问题。每个 ccTLD 权威或者新兴 TLD 权威向所在国家根进行报备。这样, 对于一个 ccTLD 就需要将自己的注册信息提交到两个地方, 同时也具有了两个指向自己的胶水记录。联盟内各国家根以全连接的方式对等接入互联体系中, 每个国家都可以与其他国家签订协议进行数据交换, 从而达到信息来源的去中心化。由此, 根联盟中国家根扮演了根区信息交换点的角色, 对于根联盟中其他国家根来说, 是对等节点, 也是根区数据来源之一, 而通过签订对等协议而实现互连的国家根则组成根联盟, 各国 TLD 信息将由各国家根在根联盟内传播。

4.3 根联盟互联体系

国家根是根联盟中的对等节点, 节点间存在着多种互联关系, 节点及节点间的对等互联关系构成了本节所述的根联盟互联体系。

当前体系中, 国家根节点间主要存在以下两种互联关系:

1) 根区数据交换: 国家根设置根区数据交换点, 用来发布本国 ccTLD 等 TLD 的信息, 并从其他国家根获取其发布的信息, 各国是本国 TLD 的权威数据源。

2) 对等解析: 通过设置对等解析点, 国家根间可以将递归 DNS 解析请求互相转发。应急态下, 如部分网络连接被切断, 可以通过对等解析点将不可解析请求全部转发给别国。

下面对两种互联关系进行详细说明。

4.3.1 根区数据交换

所述“交换”实际包含两个独立的过程: 1) 发布本国 TLD 信息供其他节点获取; 2) 从其他节点获取 TLD 信息。所获信息将被按照某种策略合并入最终的根区数据。

根区数据交换涉及以下主要元素:

1) 数据源(Source): 数据的提供方, 负责提供数据及验证数据所需凭据。

2) 获取方(Retriever): 数据的获取者, 从数据源获取数据并根据凭据验证数据是否真实有效。

3) 被交换数据(Exchange Data): 所涉 TLD(一般为 ccTLD)的相关信息(NS 记录及对应的胶水记录等)。

4) 交换协议(Exchange Protocol): 在根区交换过程中应遵循的一系列规则, 包括通信方法、数据格式、数据生成流程、数据认证流程、相关技术标准等。交换协议是根区数据交换的核心。

根联盟中, 各国家根节点部署有根区交换点, 其既是数据源也是获取方, 根区交换点间基于交换协议进行通信互联, 实现根区数据交换。

在已实现的试验系统中, 设计了一种基于 DNSSEC 协议的根区数据交换方案。作为数据源, 每个国家根基于非对称密码学技术产生一对公私钥, 并将公钥公开, 告知其他国家根。作为数据源, 将 TLD 信息按照区文件格式存储并签名。最后, 按照协议, 通过某种途径发布签名后区文件。获取方按照交换协议从数据源获取数据, 并使用其公钥对数据进行验证, 验证过程主要基于 DNSSEC 协议完成。

上述过程涉及通信、密钥生成、数据生成、数据验证等问题, 这些关键细节属于交换协议范畴, 并在交换协议中被明确定义。

交换协议主要内容如下:

1) 通信方法: 通信使用 DNS 协议, 获取方向指定 IP 地址和端口逐域、逐条获取 DNS 资源记录。数据源需要提供支持 DNSSEC 认证的标准 DNS 解析服务。

2) 数据格式: 数据源应生成包含其欲发布信息、符合区文件格式要求的区文件并签名。因为不直接传输区文件, 对数据格式的要求不体现在通信过程中, 而体现在为了通过 DNS 服务发布信息, 数据源需要生成满足格式要求的签名后区文件。

3) 数据生成流程: 将欲发布的 TLD 信息按照区文件格式存储, 并添加用于建立解析链的辅助信息, 最终将整个文件按域分割并对分割后文件进行签名。

4) 数据验证流程: 使用通信对方的公钥作为信任锚, 基于标准 DNSSEC 协议对获得的 DNS 记录进行认证, 通过认证则认为数据有效并录入数据库, 反之则无效并记录异常。

5) 相关标准及软件版本: 使用 BIND 9.4 提供标准 DNS 权威解析服务(非递归)。所使用密码学技术和相关工具遵从 DNSSEC 最新 RFC 标准。

4.3.2 对等解析

对等解析涉及以下主要元素:

1) 请求方(Requester): 请求方对 DNS 请求进行转发, 一般使用标准 DNS 协议转发给互联节点。DNS 请求一般来自国内的应急响应系统或 DNS 递归解析器。请求方负责将 DNS 响应返回给原请求者, 帮助其完成 DNS 解析。

2) 响应方(Responder): 响应方一般提供标准 DNS 递归解析服务, 并只允许与之互联的节点使用。响应方可以直接提供递归解析服务, 也可以继续转发请求到国内 DNS 递归解析器。

3) 请求数据(Request Data): 一般为标准的 DNS 请求, 由请求方转发至响应方。

4) 响应数据(Response Data): 一般为标准 DNS 响应。

5) 对等解析协议(Peering Protocol): 包括通信方式、数据传输格式等。

4.4 互联协议

为了实现国家根互联, 国家根的实际运营者, 即主权国家间, 需协商“国家根互联协议”。这份协议至少要包含以下内容:

1) 国家根信息: 如国家根服务器的 IP 地址, 可公开的技术细节等(如所使用 DNS 服务器软件版本, 是否使用 Anycast 进行多点部署)。

2) 本国权威 TLD 列表: 包括本国 ccTLD 在内全部本国 TLD 列表, 宣称对这些 TLD 的权威地位。根区交换过程中, 国家根会在根区数据交换点上发布本国权威 TLD 的权威信息, 互联节点会按照互联协议中 TLD 列表获取 TLD 相关信息, 通信和验证过程遵从根区数据交换协议约定。

3) 根区数据交换协议: 根区数据交换方案及技术细节。包括本国根区数据交换点的地址、端口号、交换方案、数据验证方法等。这一协议应在双方协商后, 达成一致, 以实现对等交换。对于实际交换方案, 可以由根联盟全体成员共同协商, 提出若干种安全可靠的公开技术方案, 供各国间自主选择。在原型试验系统中, 已实现一种基于 DNSSEC 的根区数据交换方案, 实现了两个国家根间对等根区数据交换, 并使用国家根公钥对数据真实性和完整性进行验证。

4) 提供的其他接口: 为对方开放的其他服务及服务的协议, 如前文中提到的对等解析服务。这些接口可以帮助提升根联盟整体健壮性。

同时, 协议中还可以加入保证或承诺相关内容, 例如保证本国所提供根区文件中完整且准确地包含了对方权威 TLD 信息, 作为对联盟关系的巩固与约束。

互联协议是国家根之间签订的契约, 也是国家根之间建立互联关系的基础, 是根联盟中互联体系

的形式化定义。

4.5 根区数据与解析服务

国家根提供根区解析服务的数据源有三个, 如图 3 所示: 1) 根权威 IANA 的根区数据; 2) TLD 权威向国家根报备根区数据; 3) 根联盟中国家根之间根区交换。数据来源的多样性确保了信息流上不被单一权威所控制, 从根本上实现了对根权威的权力制衡, 同时又不会创造出新的权力垄断。数据源多样性程度依赖于联盟规模, 越多国家建立国家根并形成统一根联盟, 则整个体系越健壮。

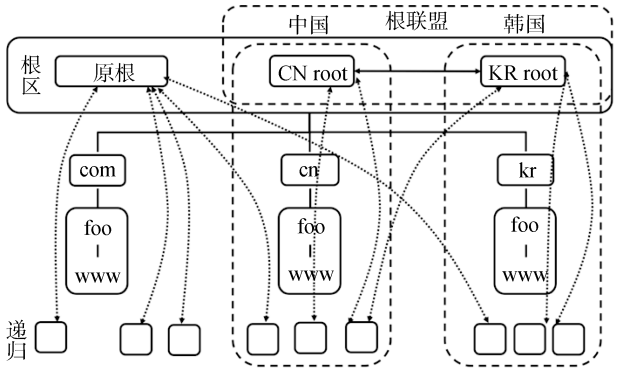

图 3 新体系下 DNS 结构

从根区治理的角度来说, 当 TLD 权威能够直接发布自身信息时, 相当于提升了 TLD 权威地位。这对 IANA 和根联盟形成一种威慑, 因为一旦 IANA 或根联盟滥用权力, 则其与 TLD 权威间互信将被破坏, TLD 权威将通过其他通道发布信息, 降低了相关恶意权威的信誉和地位。这可以看作是一种底层对上层的权力制衡机制。

从根区解析服务的角度来说, 根联盟的每一个国家根成员会优先保证本国 TLD 可以正确地被解析, 每一个国家根都提供根区解析服务, 则其至少为本国的 TLD 负责, 与当前由 IANA 实际控制全部根区解析服务相比, 主要 TLD(例如 ccTLD)的主体也成为了根区解析服务的提供者。对于用户或递归解析器来说, 在掌握了根联盟内各国家根的根区解析服务的使用方法(如国家根服务器的 IP 地址)后, 可以十分灵活地制定本地信任策略, 最大程度地保障 DNS 解析安全。

多数据源所带来的一个负面问题是信息冲突, 即不同来源的同一 TLD 数据不一致, 原因可能是无意的配置错误或蓄意攻击。解决方案有两种: 一种是建立数据源可信度优先级, 例如 TLD 权威高于根联盟, 根联盟高于 IANA。这一优先级排序的理由在于, TLD 权威是真实信息的最大受益者, 在无利害关系时根联盟中真实信息承载国家声誉, IANA 则需维护其根区管理者权威。其中, 切身利益大于国家声誉, 国家声誉大于管理权威。另一种方案是 TLD 权威采用类似 DNSSEC 的密码学手段, 首先将自身的公钥通过多种途径公开, 之后通过数字签名来保证信息的完整性与真实性。以此将其他数据源作为单纯的信息发布渠道, 将多数据源转化为单数据源, 从而避免了信息冲突。

在新的体系中, 处理上述信息冲突的手段是灵活的、非全局的, 每个国家根都可以自行确定根据多数据源获取的根区数据生成根区文件的规则, 而不影响与其他国家根节点的互连以及对外提供的根区解析服务的行为。为了保证信息的透明性, 国家根可以公布每一份根区数据生成过程, 包括可认证的、来自各数据源的全部原始数据, 生成根区数据所用合并规则, 具体的信息冲突, 冲突消解规则及最终结果。

为了保持与当前 DNS 解析体系在功能上的一致性, 也提升解析服务安全性, 新体系需要对 DNSSEC 协议予以支持。DNSSEC 协议是当前已经被广泛部署并长期使用的 DNS 安全协议, 可以有效地对 DNS 解析的过程加以保护。DNSSEC 协议中的信任锚是 DNSSEC 安全验证的起点, 是其信任模型的唯一顶点。对于 DNSSEC 中信任锚问题, 由于 DNSSEC 是对信任的一种密码技术保护, 采用谁的公钥相当于信任谁。新体系中, 国家根具有独立的公钥, 作为一个独立的 DNSSEC 信任锚。国家根对根区数据重新用自己的区签名公钥来签名。递归解析器若启用了 DNSSEC 验证, 并选择使用国家根作为根服务器, 只需将其信任锚设为国家根的公钥, 即可正常进行 DNSSEC 验证。这样, 新体系下, DNSSEC 依旧保护信息的真实性与完整性, 信任谁由递归解析器自主选择。

5 新体系分析

本章分析根联盟体系应对权力滥用风险的方案, 新体系相对于当前 DNS 的增量, 新体系是否满足之前设定的设计目标, 新体系所具有的其他性质, 以及新体系的安全性。

5.1 滥用风险防范

在新体系下, 假设相关 TLD 信息已经被成功发布到国家根, 并且国家根本身是安全可靠的, 只有原根存在滥用问题。常态下, 体系内的域名解析过程与原 DNS 中的过程相同, 只是对于使用了根联盟作为根的递归解析服务器来说, 根服务器不再是原根,

而是一个国家根。下面对各种风险发生时, 应急态下解析过程进行说明。

对于消失性风险, 如图 4 所示, 假定我国的.cn 域被从原根抹去, 韩国的递归解析器将无法从原根处得到其信息。如果递归解析器将根指向了韩国国家根, 韩国与中国为根联盟中盟友, 则两国国家根已经交换过各自授权 ccTLD 信息, 此时韩国递归服务器就仍可以得到.cn 域信息, 顺利访问.cn 域下域名。这样根联盟中盟友, 中国的 ccTLD 并没有消失。迭代解析过程与常态下类似。

对于致盲性风险, 如图 5 所示, 假定原根拒绝对中国提供服务, 对于配置了中国国家根的递归服务器, 要解析盟国 ccTLD 下域名, 类似上述“消失性风险”中解析过程, 依然可以得到 ccTLD 信息。中国国家根服务器中有交换得来的韩国 ccTLD 信息, 递归解析器也就可以进行解析。

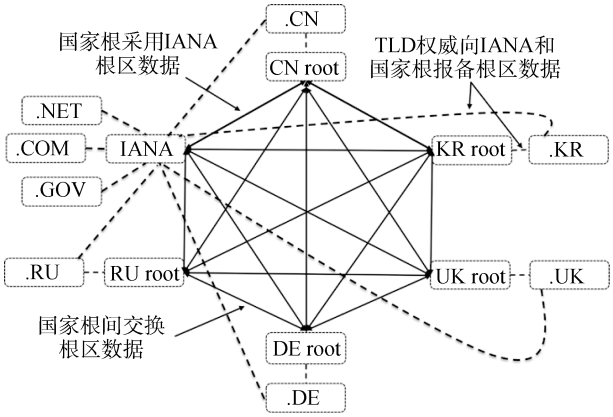

图 4　根联盟内根区信息交换

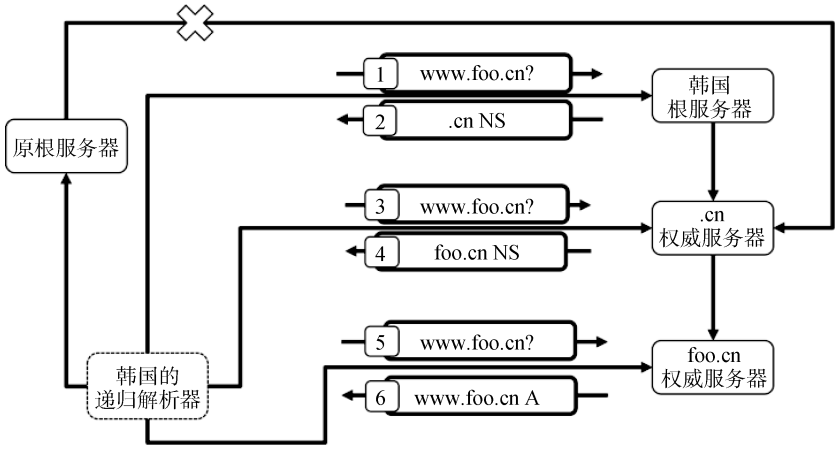

图 5　新体系在消失性风险下的解析过程

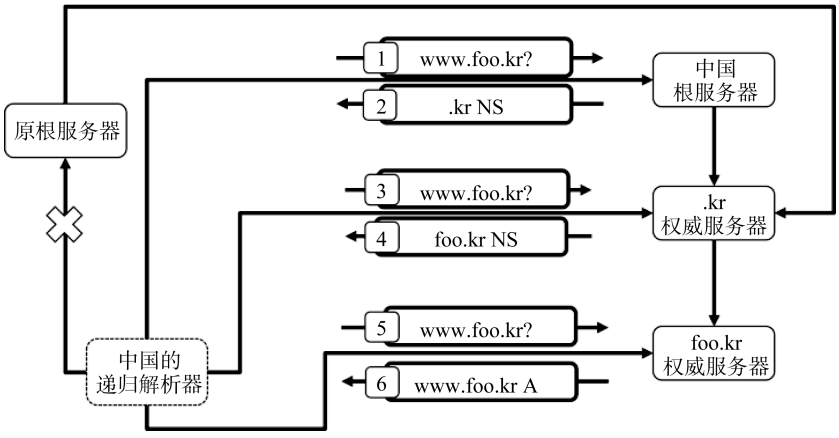

图 6　新体系在致盲性风险下的解析过程

可见, 新体系可以防范根权威权力滥用问题, 而新体系自身的威胁和风险将在后文进行分析。

5.2　新体系增量

通过新老 DNS 根系统运作模式对比可以发现, 新体系相对于原体系增量很小, 具体到 DNS 体系中四要素如下:

1) 域名空间: 原本域名空间不变, 仍保持单根树结构。新体系中 TLD 授权分配不变, TLD 发布信息的渠道除了通过根权威, 还新增了根联盟。

2) 权威服务器: 原权威服务器(包括根服务器)

功能不变, 新增加的国家根服务器将会与原根服务器并存。本国 ccTLD 及其他 TLD(自愿)只需将在 IANA 注册信息向国家根管理机构报备即可。

3) 递归解析器: 采用国家根的递归解析器需要将缺省的 Root Hint 配置设定为国家根服务器 IP 地址。对于 DNSSEC, 递归解析器需将信任锚配置为相应根服务器的 KSK。

4) 解析协议: 不变。

由此可见, 新体系对当前 DNS 改进主要在于根解析结构和 TLD 信息流, 不改变 DNS 协议及其行为。这保证了最小化设计、开发与部署成本。

5.3 新体系性质

新体系具有以下性质:

1) 域名空间统一与域名唯一性: 分析设计方案在 Zooko 三角猜想方面性质, 来回答之前提出的问题: DNS 必须牺牲去中心化, 但新体系结构需要去中心化, 该如何解决这对矛盾? 新体系通过分离域名分配与域名解析, 令问题从一个三角转化为两个三角。域名分配三角满足唯一性与用户可理解(牺牲去中心化), 域名解析三角满足去中心化与用户可理解(牺牲唯一性)。在本方案维持 IANA 作为唯一域名空间管理机构的现状, 因此名字空间结构在逻辑上与当前 DNS 一致, 都满足唯一性和用户可理解, 牺牲去中心化。本方案所提出的根联盟体系中不存在单个中心。当某个根中数据被篡改, 其他根数据可能将保持之前正确状态, 此时不同根上的根区数据可能不一致。因此, 本方案解析结构满足去中心化和用户可理解, 牺牲了数据一致性, 而这正是防范威胁的必然结果。

2) 自主性: 由国家根承担的根区解析服务完全自主, 不依赖 IANA。递归解析器及其用户自主选择原根或某个国家根, 若选择国家根, 则受到国家根及根联盟在根解析上保障。向国家根报备的 TLD 也得到了根联盟保障, 如之前所分析的, TLD 地位通过根联盟得到了提升, 增加了自主性。

3) 开放与平等: 所有国家自愿加入和退出根联盟, 不存在壁垒。同时根联盟将会面向互联网上所有递归解析器开放, 即向所有互联网用户开放。新体系中根联盟成员之间关系平等, 不存在层级关系。国家根与原根共存, 其实际作用范围, 依赖于递归解析器和用户的自主选择。新体系与当前体系的区别可以类比为“联合国”与“某一国”的区别。

4) 透明性: 整个系统与现有的 DNS 系统互不冲突; 新体系只涉及域名解析, 对当前 IANA 域名授权管理透明; 根联盟体系对除采用国家根的递归解析器外其他 DNS 组件透明; 新体系无需对当前 DNS 服务器软件做任何改动, 对 DNS 协议本身透明。

5) 渐进部署: 新体系作为 DNS 体系的一种改进, 可实现渐进部署。根联盟随着国家根的建立逐渐形成, 同时新体系覆盖用户随着递归解析器采用国家根而逐渐增加。部署激励来自于提高所部署国家根解析的自主性。新体系也可作为一种应急响应方案, 常态下无需对互联网用户提供服务, 因而部署过程可从小范围测试开始, 逐渐扩大部署范围。实际部署中所面临挑战已不是单纯学术问题。

6) 健壮性: 新体系中的根联盟将国家根组织成一个整体, 在联盟内实现互联互通, 一方面通过根区数据交换获取彼此的权威 TLD 信息, 最大程度确保联盟内成员掌握来自权威真实可靠的 TLD 信息; 另一方面通过提供对等的递归解析服务提高 DNS 解析服务的可用性。同时, 每个国家根独立提供根区解析服务, 整个根联盟形成一个平等多根解析体系, 与现有单根解析体系相比, 更为健壮, 也更为合理。

5.4 安全性分析

引入国家根和根联盟后, 新的体系结构不再具有严格的中心化特征, 弱化了根权力滥用风险, 同时, 国家根也可能遭受与与原根服务器类似的攻击。

5.4.1 威胁模型

假定攻击者从外部试图攻击国家根系统, 典型的攻击者可能具有如下能力:

1) C1 阻塞网络: 攻击者可实施 DDoS 攻击;

2) C3 劫持系统: 攻击者利用系统漏洞, 造成系统、软件崩溃, 甚至获得系统控制权;

3) C2 密码学攻击: 攻击者将能够解密加密内容, 或伪造消息。

具有上述能力的攻击者对国家根实施攻击所造成的威胁包括:

1) 通讯中断: C1 攻击者令国家根所处网络环境被阻塞或破坏, 导致不能正常提供服务及与其他国家根互联;

2) 系统瘫痪: C2 攻击者令国家根系统瘫痪, 导致不能正常提供服务及与其他国家根互联;

3) 伪造数据: C3 攻击者伪造用于交换的根区数据, 并或伪装成国家根提供基于伪造数据的根区解析服务。

国家根本身提供根区解析服务, 如果拒绝服务或使用伪造的根区数据, 将会影响 DNS 解析安全; 由于国家根间存在互联关系, 不可信根会影响与之互联国家根的根区数据, 由于存在根区数据交换, 可信根的根区数据中将可能包含来自不可信根的伪

造数据。

综上, 新的体系主要面临以下两种安全风险: 根失效, 根欺骗。

5.4.2 根失效

若国家根不能正常对外提供服务, 例如遭受拒绝服务攻击, 或出现网络、系统故障, 将会影响其用户及与之互联的其他国家根, 称为根失效风险, 不能正常对外提供服务的国家根称为失效根。

下面从 DNS 解析和根联盟两个角度分析根失效风险所带来的威胁。

从 DNS 解析的角度, 失效根的用户将不能进行域名解析, 这与致盲性风险是相同的, 本质上是根拒绝服务。递归服务器可以将原根或其他国家根作为备选根服务器, 及时进行切换。

从根联盟的角度, 与失效根互联的国家根将不能通过根区交换获取该国的 TLD 信息, 其仍可从 IANA 获取, 但可能与失效根所提供数据不一致。失效根不会显著地影响其他国家根的根区数据完整性, 但会导致本国 TLD 信息不能在根联盟内传播, 本国 TLD 解析安全也就得不到保证。其他国家根可以根据实际情况选择继续使用历史数据或改为从 IANA 获取。

值得一提的是, 若国家根仍提供服务, 但行为异常, 例如数据不能通过认证, 或未遵守互联协议约定, 也是失效的, 因为用户或者其他国家根能够发现这些异常并拒绝使用其提供的服务。

5.4.3 根欺骗

根区 KSK 和根区交换时所使用的公钥等可以用来验证国家根所提供信息的真实性。存在这样一种风险, 恶意第三方能够伪造出可通过验证的信息并伪装成国家根将其发布, 或国家根的管理者恶意篡改信息, 称为根欺骗风险, 信息被伪造或存在欺骗行为的国家根称为欺骗根。

下面从 DNS 解析和根联盟两个角度分析。

从 DNS 解析的角度, 攻击者能够决定任意域名的解析结果。如果国家根被完全控制, 或根区 KSK 对应的私钥泄露, 则 DNSSEC 也不能发现此类攻击。

从根联盟的角度, 当国家根与欺骗根互联, 其根区数据中就可能包含来自不可信根的不真实、恶意信息, 进而影响其提供的根区解析服务。不过由于根区交换中不存在传递机制, 欺骗根只能影响与之互联的国家根, 且受影响 TLD 范围也受根区数据交换协议中约定限制。另外, 这些恶意信息是否能够进入根区数据还取决于根区数据合并策略。合并策略由各国家根的管理者自主制定, 与国家间信任关系、TLD 重要性等因素有关。

综上, 新体系中, 欺骗根有能力篡改其他国家根的根区数据, 但仅限于其本国 TLD 范围, 且受多种因素限制。另外, 国家根间协同作恶不能增加其成功率和危害。而受影响的国家根可以从合并策略入手, 降低风险, 例如加入人工审核机制。

5.4.4 小结

由于国家根本身也是根服务器, 所以不论是根失效风险还是根欺骗风险, 从 DNS 解析的角度, 国家根和根联盟并没有带来新威胁。实际上, 新体系提供了原根以外的备选根区解析方案, 总体上增加了 DNS 解析体系健壮性。在根联盟中, 国家根互联仅限于数据交换, 攻击者一般只能影响其他国家根的根区数据, 而不能借助互联关系危害国家根本身, 且信息交换不传递, 恶意信息不会不可控地扩散。合理的根区数据合并策略和人工审核机制是防范根欺骗风险的关键。

6 验证性系统

下面介绍基于本文所提出体系实现的一个试验系统。

如图 7 所示, 一个国家根节点由三个功能模块组成。数据采集模块从多个数据源采集根区数据, 并在数据管理模块中被合并生成一份根区数据, 由解析服务模块使用这份数据对外提供根区解析服务。国家根节点对外提供根区解析服务, 并通过根区交换点与其他节点交换根区数据。国家根节点间通过根区交换和对等解析等实现互联, 组成根联盟。

试验系统已经在全国四个城市进行部署, 每个城市部署有一个国家根节点, 并扮演一个国家的角色, 节点互联组成根联盟。每个国家根节点都对外提供根区解析服务, 并以应急响应接口的形式提供递归解析服务, 同时通过根区交换点和对等解析点与其他节点互联。目前部署情况如表 2 所示。

试用国家根提供的根区解析服务可以将递归服务器的 Root Hint 指向国家根的根服务器, 或者普通用户可以直接使用各节点部署的递归服务器(即国家根的应急响应接口)。每个国家根上都配置了用于测试的特殊 TLD, 可通过访问测试网址来验证国家根使用情况。这些特殊网址包括: 1) www.root: 如果使用了国家根, 则会看到国家根信息页面, 其中包括国家信息; 2) www.<ccTLD>-root: 各国国家根信息页面。<ccTLD>-root 属于被交换的 TLD, 所以该域名还可以用来发现所使用国家根与哪些国家根互联。

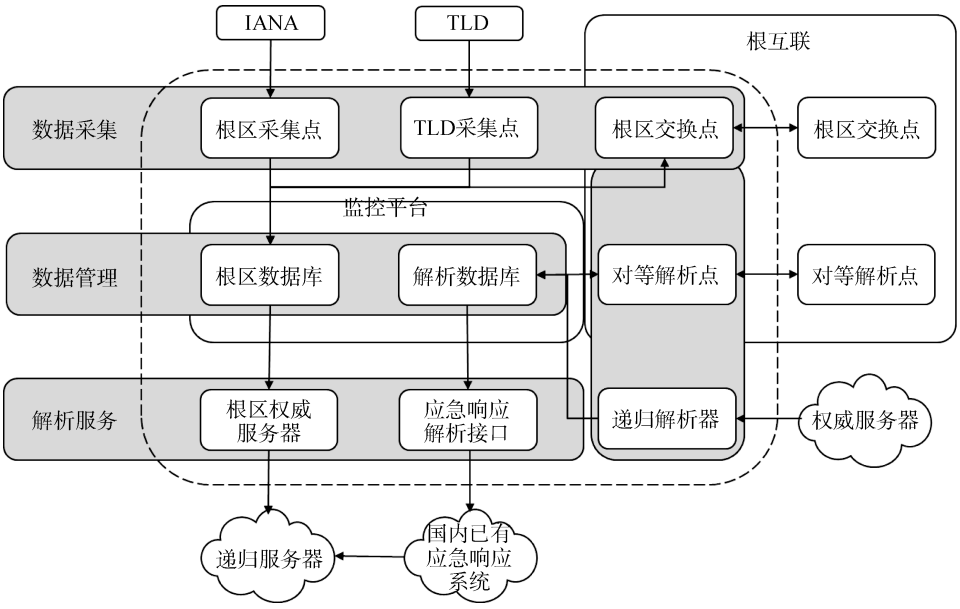

图 7　系统模块图

表 2　原型系统部署信息(2017 年 5 月 22 日)

城市	国家	本国 TLD	根服务器	递归服务器	测试 URL
北京	中国	cn. cn-root.	49.5.3.4	49.5.3.6	http://www.cn-root
哈尔滨	俄罗斯	ru. ru-root.	202.118.236.229	202.118.236.220	http://www.ru-root
威海	韩国	kr. kr-root.	221.2.160.226	221.2.160.228	http://www.kr-root:8888
长沙	巴基斯坦	pk. pk-root.	119.39.5.27	119.39.5.29	http://www.pk-root

由于上述域名的 TLD 不存在于 IANA 的根区中, 浏览器可能不会将其当作网址处理, 所以访问时需加上 HTTP 协议标识, 例如 http://www.root。哈尔滨节点目前处在教育网环境中, 部分运营商网络中可能无法连通。

另外, 目前系统已经完成根区解析服务性能测试, 测试结果表明, 若网络条件良好, 国家根提供的根区解析服务能够单机处理 20 万次/秒的 DNS 请求并稳定运行。测试环境参考了 Knot DNS[17]软件所使用的 DISTEL[18]测试方案, 具体环境如图 8 所示。

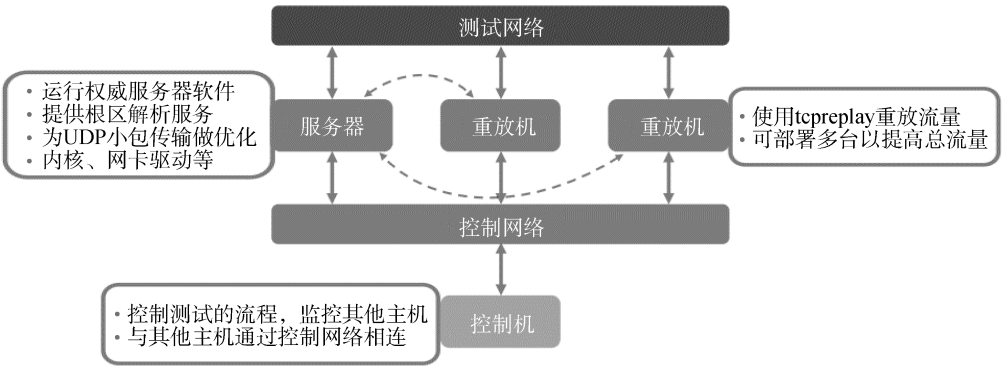

图 8　性能测试环境

处理 DNS 请求的服务器配置如下:

• CPU: Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz(6 × 2 = 12 cores)

• 内存: 32GB DDR3

• 网卡: Intel Corporation I350 Gigabit Network Connection

• 系统: Ubuntu Server 15.04 (Kernel 3.19.0-15-generic)

测试中以不同的速率向服务器重放 DNS 请求流量, 并统计服务器返回的 DNS 响应数, 计算响应率。测试结果如图 9 所示, 在 20 万次/秒的流量下, 响应率接近 98%。

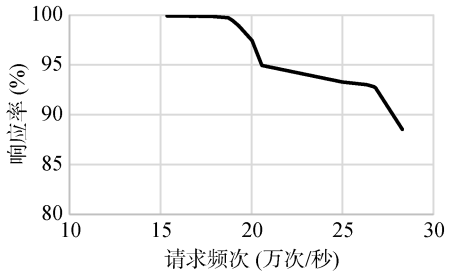

图 9　性能测试结果

上述测试结果为单机性能, 考虑到抵御 DDoS 等攻击带来的超大流量, 也对启用负载均衡机制后的性能提升进行了测试。经测试, 双机负载均衡可以得到 1.9 倍的性能提升。由于 DNS 流量多为无状态的 UDP 流量, 仅需使用简单的调度策略, 多机负载均衡就可以带来接近线性的性能增长。

后续工作会模拟根权力滥用风险被利用情景, 验证新体系有效性, 并在实际网络环境中用真实流量对系统进行压力测试, 评估系统健壮性。

7　结论

随着互联网从当初的一个试验系统发展成为如今的"第五疆域", DNS 所涉及问题逐渐从工程技术领域延伸到政治经济领域。这一趋势主要表现为技术与政策的耦合程度加深, 极大增加了互联网系统安全复杂性。本文针对 DNS 根解析中潜在的权力滥用问题, 提出了一种新的根解析体系。该体系通过将顶级域名分配与域名解析相分离, 并建立国家根和根联盟, 在保证域名空间统一和域名唯一性的同时, 实现了去中心化、自主、开放、平等、透明、可渐进部署的根解析体系。

一个原型系统已经被实现与试验, 未来工作主要包括三个方面: 1) 继续研究根权力滥用对策与去中心化理论, 为根联盟体系奠定更坚实的理论基础; 2) 开展更大规模试验, 以验证新体系理论的正确性以及实际系统实现的有效性与可靠性; 3) 开展更大范围研讨, 起草相关协议标准, 促进根问题早日解决。

致谢　感谢实验室的苏申、刘文峰、康宁、李秉睿、秦超逸、余卓勋同学在原型系统研发中的贡献。

参考文献

[1] P. V. Mockapetris, K. J. Dunlap, "Development of the Domain Name System", *Computer Communication Review*, vol. 18, no. 4, pp. 123-133, 1988.

[2] G. Ateniese, S. Mangard, "A new approach to DNS security (DNSSEC)", in *Proceedings of the 8th ACM conference on Computer and Communications Security*, pp. 86-95, 2001.

[3] B.X. Fang, "Country Autonomous Root Domain Name Resolution Architecture from the Perfective of Country Cyber Sovereignty", *Information Security and Communication Privacy*, no. 12, pp. 35-38(in Chinese), 2014.
(方滨兴, "从"国家网络主权"谈基于国家联盟的自治根域名解析体系", *信息安全与通信保密*, 2014, (12): 35-38。)

[4] B. Kuerbis, and M. Mueller, "Negotiating a new governance hierarchy: An analysis of the conflicting incentives to secure internet routing", *Communications and Strategies*, no. 81, pp. 125-142, 2011.

[5] M. Mueller, A. Schmidt, and B. Kuerbis, "Internet security and networked governance in international relations", *International Studies Review*, vol. 15, no. 1, pp. 86–104, 2013.

[6] W. Kumari, P. Hoffman, "Decreasing Access Time to Root Servers by Running One on Loopback", RFC7706.

[7] Xiaodong Lee, Vixie Paul, Zhiwei Yan, "How to scale the DNS root system?", Internet draft, 2015.

[8] R. Cox, A. Muthitacharoen, and R. Morris, "Serving DNS Using a Peer-to-Peer Lookup Service", in I*nternational Workshop on Peer-To-Peer Systems*. (*IPTPS'02*), pp. 155-165, 2002.

[9] M. Freeman, E. Freudenthal, and D. Mazieres, "Democratizing Content Publication with Coral", in *Symposium on Networked Systems Design and Implementation*. (*NSDI'04*), vol. 4, pp. 18-18, 2004.

[10] K. Parker, Z. Wang, V. Pai, and L. Peterson, "CoDNS: Improving DNS Performance and Reliability via Cooperative Lookups", in *Symposium on Operating Systems Design and Implementation*. (*OSDI'04*), vol. 4, pp. 14-14, 2004.

[11] V. Ramasubramanian, and E. G. Sirer, "The design and implementation of a next generation name service for the internet", in *ACM SIGCOMM 2004*, pp. 385-386, 2004.

[12] C. Cachin, and A. Samar, "Secure distributed DNS", in *IEEE International Conference on Dependable Systems and Networks 2004*, pp. 423-432, 2004.

[13] "Namecoin", http://namecoin.info.

[14] Internet Architecture Board, "IAB Technical Comment on the Unique DNS Root", RFC2826, 2010.

[15] "The IAB's correspondence with NTIA on DNSSEC deployment at the root", https://www.iab.org/documents/correspondence-reports-documents/docs2008/2008-11-18-dnssecdeployment-at-the-root/, 2008.

[16] "Names: Distributed, Secure, Human-Readable: Choose Two", http://web.archive.org/web/20011020191610/http://

zooko.com/distnames.html, Oct, 2001.
[17] “Knot DNS”, https://www.knot-dns.cz.
[18] “NSD An Authoritative Nameserver” pp. 28-28, https://www.dns-oarc.net/files/dnsops-2006/Kolkman-NSD.pdf.

张宇 于 2009 年在哈尔滨工业大学计算机系统结构专业获得博士学位。现任哈尔滨工业大学计算机网络与信息安全技术研究中心副教授。研究领域为互联网关键资源安全，网络拓扑测量，未来网络体系结构。Email: yuzhang@hit.edu.cn

夏重达 于 2013 年在哈尔滨工业大学信息安全专业获得学士学位。现在哈尔滨工业大学计算机科学与技术专业攻读博士学位。研究领域为互联网关键资源安全、未来网络体系结构。研究兴趣包括: NDN 网络移动性支持、软件定义网络、区块链技术。
Email: xiazhongda@hit.edu.cn

方滨兴 男，中国工程院院士，哈尔滨工业大学计算机科学与技术学院教授、博士生导师，研究方向为网络与信息安全、并行计算和分布式系统。

张宏莉 女，博士，哈尔滨工业大学计算机科学与技术学院教授、博士生导师，研究方向为网络安全、网络测量和网络计算。