我国互联网域名基础设施集中化程度测量研究

刘世明，李瑞烜，刘保君，段海新，孙东红
（清华大学网络科学与网络空间研究院，北京 100084）

摘　要：随着互联网商业模式的演变，最初基于分布式设计的域名基础设施呈现集中化趋势，可能造成大范围网络中断。聚焦于我国域名基础设施集中化，构建基于网页广告分发的递归解析器收集系统，结合大型被动域名解析日志主动测量中国国家和教育域名的权威服务器。测量结果表明，我国域名基础设施存在严重的集中化现象，但主要依赖于国内运营商和企业，与国外集中化节点存在显著差异。网络安全部门应加强对国内域名系统集中化节点的监测和风险预警。

关键词：域名系统；服务集中化；递归解析器；权威服务器；网络测量
中图分类号：TN915.08
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024261

Measurement study on the DNS centrality in China

LIU Shiming, LI Ruixuan, LIU Baojun, DUAN Haixin, SUN Donghong
Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China

Abstract: The Domain Name System (DNS) was initially designed with a distributed architecture to ensure availability. However, with the development of the Internet, the trend of centrality in the DNS has led to a series of potential single points of failure. Focusing on the centrality of China's DNS infrastructure, a passive recursive resolver data collection system based on Internet advertisement distribution was prompted. Combining passive DNS data with active domain authoritative resource record scanning, the authoritative servers for domain names of China and Chinese education were analyzed. The result indicates a high level of centrality, which primarily relies on Internet Service Providers (ISP) and local Internet companies, showing significant differences from the results abroad. Network authorities should strengthen the monitoring and warning mechanisms for centralized nodes in China's DNS infrastructure.

Keywords: domain name system, service centrality, recursive resolver, authoritative server, internet measurement

0　引言

作为互联网基础设施的神经中枢，域名系统（DNS, domain name system）可将用户友好的域名转化为机器可理解的IP地址。域名系统可保障上层网络服务和应用程序的正常运转，如电子邮件、网页浏览等，同时也可作为网络安全机制的信任基础，如数字证书签发以及邮件身份认证等。出于可靠性和健壮性的考量，域名系统的最初设计遵循分布式、去中心化的原则，依托于域名空间的树状结构对域名管辖区域逐层授权，从而避免单一节点成为域名解析的瓶颈。

然而，随着互联网商业模式的演变和云计算服务的飞速发展，最初基于分布式理念设计的域名基础设施已经逐步呈现出集中化趋势，即大量互联网用户和网络服务依赖于少量供应商的域名解析和授权服务。这导致域名系统衍生出大量潜在的单点故

收稿日期：2024–10–22
通信作者：刘保君，lbj@tsinghua.edu.cn
基金项目：国家重点研发计划基金资助项目（No.2023YFB3105600）
Foundation Item：The National Key Research and Development Project of China (No.2023YFB3105600)

障节点，导致众多真实的安全风险。在国际上，知名 DNS 服务提供商 Dyn 在 2016 年遭受 DDoS 攻击，造成大量流行网站在美国东部地区无法访问，如 Twitter、CNN 等[1]。在国内，重要域名解析服务提供商 DNSPod 在 2009 年发生单点故障问题，导致江苏、安徽等 6 个省市的电信服务器瘫痪 2 小时以上[2]。

域名基础设施可分为递归解析侧和权威服务侧两方面，众多研究工作表明它们均存在高度的集中化现象[3-9]。然而，先前研究都未针对中国的域名基础设施展开深入分析，我国域名系统服务的集中化程度还未得到全面揭示。具体来讲，先前针对递归解析侧集中化的测量方法，主要依托于谷歌广告平台来向用户分发测量脚本[3]，而该平台无法覆盖到国内用户。在权威服务侧，先前工作主要围绕全球流行域[4]，个别国家域名[5]的权威服务器展开集中化测量，缺乏对我国国家域名尤其是国内教育域名的评估。特别是由于教育行业的重要性，管理机构通常不会对外公开教育域名列表，这也为针对教育域名的研究工作带来巨大挑战。

为评估国内域名基础设施的集中化程度，本文系统测量国内用户的递归解析器配置和域名的权威服务器部署，使用赫芬达尔指数（HHI, Herfindahl-Hirschman index）作为衡量集中度的指标，其超过 25% 则表明高度集中化。在递归解析侧，本文借助支持高度定制化内容的国内网页广告分发商，构建递归解析器被动收集系统，通过无害化测量脚本在一周内收集了 53 988 个用户所配置的 4 529 个递归解析器，用户覆盖全国所有省级行政区。在权威服务侧，本文使用公开的 .cn 子域名列表[10]，通过域名授权资源主动扫描，收集了 3 073 282 个 .cn 子域名的 22 740 个权威服务器。特别地，针对中国教育网域名系统，本文从国内某大型域名服务商的被动域名解析日志中提取 2024 年内活跃的 2 543 个 .edu.cn 的子域名，并通过主动扫描域名授权资源记录，收集到 2 280 个权威服务器。

本文测量结果表明，国内的递归解析服务市场的 HHI 达到 36.5%，表现出高度的集中化。互联网服务提供商（ISP, Internet service provider）负责国内主要的递归解析服务，这与国外域名基础设施相似。具体来讲，90.4% 的国内用户使用 ISP 分配的递归解析器，其中，中国移动占 48.0%，中国电信占 27.3%。而在剩余的公共开放解析器市场，79.3% 的用户采用 114DNS，国际上主流的谷歌 DNS 只占 2.2%[3]。相较于互联网基础设施较为发达的省份，位于基础设施相对落后省份的用户的递归解析器供应商更为集中。

在权威服务器侧，.cn 子域名的权威服务器市场的 HHI 为 35.5%，同样表现出高度集中化现象。不同于亚马逊服务商作为全球流行域名的集中部署点[3]，57.6% 的 .cn 子域名部署于阿里云，89.5% 的 .edu.cn 子域名部署于中国教育和科研计算机网（CERNET）。

总之，我国域名基础设施呈现出高度集中化态势，少数国内运营商和企业占据了域名解析和授权服务的绝大部分市场份额。这一格局虽然有效防范了过度依赖境外域名服务导致的潜在网络中断风险，但也暴露出大量域名系统的单一故障节点。为提升我国互联网的整体安全性和可靠性，建议进一步优化域名基础设施布局，促进行业多元化发展，加强域名系统的流量负载均衡和关键数据备份。同时，网络安全部门应加强对域名基础设施的集中化节点的监测和风险预警，切实防范域名系统安全事故的发生。

1　域名系统集中化的演变与相关工作

1.1　域名系统的最初设计

在互联网发展早期，域名系统的运作主要依赖于由中心化机构分发的 Hosts 文件，来完成本地域名解析。为应对互联网主机数量的增长，Mockapetris 等[11-13]于 1983 年设计并实现了分布式的域名系统。依托于互联网域名空间的树状结构，根域名服务器将顶级域名（.cn）的管辖权授权给顶级域名服务器，顶级域名服务器将二级域名（.edu）的管辖权授权给权威域名服务器。图 1 展示了域名基础设施中互联网域名的解析流程。域名基础设施包括递归解析侧和权威服务侧两部分。用户首先将域名解析请求发给递归解析器，并由其依次查询根域名服务器、顶级域名服务器和权威服务器，来获取最终的域名解析结果。

域名基础设施中的权威服务器是公认的、全球规模最大的分布式数据库。分布式的理念一方面体现在域名空间采取层级授权关系，将域名解析的权限不断下放。另一方面，根据协议规范性要求[10]，

域名管理者需要配置多个权威服务器，并且应当满足地理位置和网络拓扑的多样性。该要求分布式的结构设计不仅减轻了域名解析的负载，同时保障了域名系统在遭遇单点故障时的健壮性。

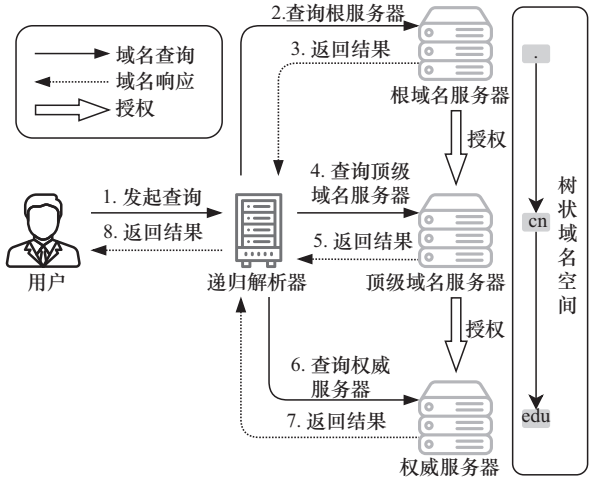

图1　域名基础设施中互联网域名的解析流程

1.2　域名系统的集中化趋势及危害

受到互联网商业模式变化的驱使和云计算的快速发展，域名基础设施的架构逐渐呈现集中化趋势，即大多数的域名解析和授权服务依赖于少数供应商。递归解析服务集中化现象产生的原因主要是用户为提高域名解析性能，偏向使用知名的公共递归解析器。对于域名授权服务，方便快捷的云上域名托管平台极大地降低了用户配置和管理域名的技术门槛，因此吸引了众多域名集中部署于大型权威服务器。

集中化趋势违背了域名系统最初的分布式设计理念，其危害性可表现在以下三方面。

破坏域名系统稳定性。大批量的域名查询请求会提高域名服务器的负载，一旦中心化节点服务器发生故障，就会造成大量用户无法正常进行域名解析。国内著名DNS供应商DNSPod，在2019年遭受黑客攻击，无法为国内十余万网站提供域名解析服务，导致本地ISP的DNS服务器流量过载，江苏、安徽等6个省市出现大面积断网[2]。

威胁用户隐私。域名系统的集中化会对用户隐私保护和域名服务稳定性均造成严重威胁。不道德的域名服务提供商可以更容易地收集和分析大量用户的域名解析请求，对用户行为进行画像，推断用户的爱好、工作、身体状况等用户隐私，从而实施定向广告投放，甚至是跨IP地址跟踪和个人信息贩卖。2021年美国联邦贸易委员会的报告中指出美国存在6家大型ISP收集大量DNS解析记录并向不可靠的第三方进行出售[14]。

破坏市场平衡。从递归解析器服务提供商和权威域名服务提供商考虑，集中化趋势还会加剧域名服务市场的垄断，破坏公平竞争的市场构成。

1.3　国内外相关研究工作及本文研究动机

大量研究工作[3-9]已经表明国外域名递归解析和授权服务均呈现出严重的集中化现象，但它们的测量结果都未能涵盖国内的域名基础设施。

对于递归解析服务，Huston等[3]通过在谷歌广告中嵌入递归解析器测量脚本，获取了互联网用户的递归解析器配置。他们发现65.0%的用户的递归解析器都由ISP分配，且谷歌DNS在开放递归解析器市场中占据绝大部分份额，达到68.7%。然而，谷歌广告平台几乎无法覆盖国内用户，因此无法评估我国递归解析服务的集中化。

在权威服务侧，研究人员大范围测量了流行域名和部分国家域名的权威服务器。文献[4]通过模拟DNS解析流程，使用排名前100万的流行域名，对权威服务器的集中化进行了测量，并指出超过50%的权威服务器同时为至少16个流行域名提供解析服务。Moura等[5]分析了2个国家顶级域名（.nl和.nz）服务器的被动流量。他们发现在对这2个国家顶级域名的所有域名查询中，有30%以上来自谷歌等五家知名云服务提供商的权威服务器。然而，已有研究都未针对我国国家域名和教育域名展开分析。

考虑到域名系统集中化的危害，针对国内域名基础设施集中化的大范围测量，可帮助安全监管部门和研究人员感知我国域名系统的发展状况，系统监测中心化节点的安全风险，具有显著的现实意义。

2　测量方法与数据集

本节首先定义域名基础设施集中化程度的衡量指标；然后，介绍基于网页广告分发的用户递归解析器配置测量方法；最后，介绍收集我国国家域名和教育域名的过程，以及主动探测域名授权资源记录的方法。此外，本节还提供了本文研究数据集的概况。

2.1　集中化程度衡量指标

域名基础设施的集中化指的是大量互联网用户和域名的解析和授权服务由少数供应商掌控。为直观地表示互联网基础设施的集中化程度，本文采用HHI指标对递归解析器和权威服务器的供应商市场进行评估。HHI是衡量产业集中度的常用指标，数值越大代表市场越接近垄断[15-16]。HHI的计算式为

$$\mathrm{HHI} = \sum_{i=1}^{n} S_i^2$$

其中，S_i为公司市场份额的百分比。HHI超过10%代表中等的集中化程度，超过25%则表明出现了高度的集中化。为计算HHI指标，需要获取国内递归解析器供应商和权威服务器供应商的服务用户和域名数量，本文将在下面逐一介绍测量方法。

2.2　国内互联网用户递归解析器地址测量

2.2.1　基于广告分发的递归解析器地址测量方法

由于用户所配置的递归解析器通常不会暴露在外，因此很难直接主动探测到它们。一种可行的测量方法是，通过让用户向受控域名发送HTTP请求，使得用户配置的递归解析主动查询受控域名的权威服务器。如此一来，Web服务器的访问日志中就会保存用户信息，而权威服务器的访问日志中会保存用户的递归解析器。

基于广告JavaScript触发HTTP请求的递归解析器测量方法。为了让用户向受控域名发送HTTP请求，本文借鉴Huston等的测量方法，通过网页广告平台向用户分发测量脚本。为满足本文测量需求，网页广告平台需能涵盖国内用户，并支持高度定制化的网页广告。本文最终采用要发广告联盟作为广告分发商，其能够针对性地向国内主流网站投放广告，且支持用户自定义的HTML脚本。本文所定制的网页广告中包含一段无恶意的JavaScript代码，其可实现当用户浏览包含广告的网页时，自动向本文的受控域名发送HTTP请求。

基于权威服务器错误响应的全量递归解析器IP地址获取方法。对于用户主机，当产生域名解析的需求时，使用配置的首选解析器发起查询请求。当该解析器未能将域名解析为IP地址时，用户主机会逐一选择配置中剩余的解析器依次发起查询请求，直到正常返回结果。因此，为了获取用户所配置的全部递归解析器，受控权威服务器可通过返回SERVFAIL的方式让用户配置的所有递归解析器逐一访问受控权威服务器。

图2为基于网页广告分发的递归解析器配置测量平台的运行过程，主要包含下面5个步骤。

1) 用户访问携带广告的网页，JavaScript脚本向用户分配唯一标识符（UUID），并随后触发客户端向受控Web服务器发送携带UUID的URL的HTTP请求。

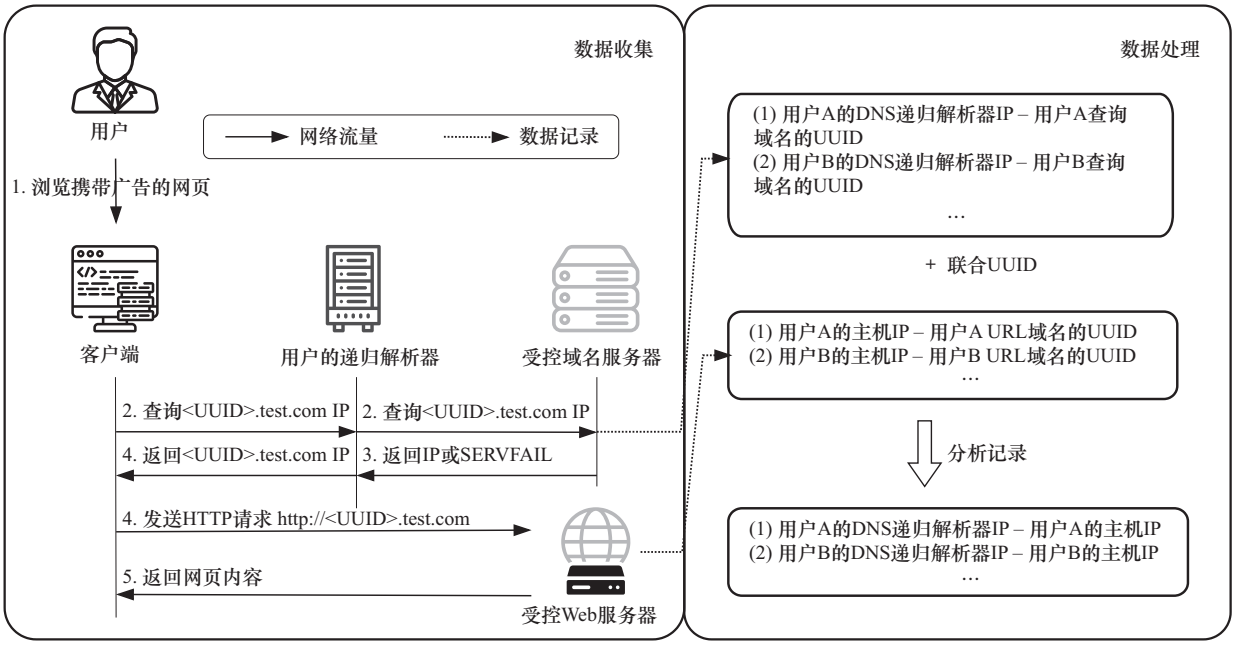

图2　基于广告分发的递归解析器地址测量平台的运行过程

2) 为完成HTTP请求，用户的客户端会向递归解析器查询受控域名的IP地址。之后，递归解析器向受控的权威服务器发送域名解析请求。权威服务器会记录递归解析器的IP地址和嵌在查询域名内的UUID。

3) 受控权威域名服务器向递归解析器返回域名的IP地址或者SERVFAIL，来获取用户配置的首选和所有递归解析器。

4) 递归解析器将受控域名的IP地址返回给客户端。之后，客户端向受控的Web服务器发送携带UUID的HTTP查询请求，受控的Web服务器记录访问用户的IP以及对应的UUID。

5) 受控的Web服务器做出HTTP应答，针对该用户的数据收集结束。

最后，本文使用UUID对HTTP查询和域名解析查询进行关联，就可以获得用户所配置的首选递归解析器和全部递归解析器。

2.2.2 递归解析器数据集概览

测量任务共持续7天，收集了345 539条广告流量。经过数据去重，共覆盖国内53 988个用户IP地址以及4 529个递归解析器IP地址。

为计算递归解析器市场的HHI，需要获取递归解析器的供应商。本文首先采用先前测量研究工作[17]中使用的开放的IP地理数据库IP-API，获取所有IP地址的组织信息和地理信息。为了更加准确地识别递归解析器的所属组织，本文还使用大型供应商公开的递归解析器列表对IP地址的组织信息进行了核实和修正，包括在先前工作[18]中使用的公共递归解析器IP列表，例如谷歌DNS和Cloudflare DNS。结果表明，递归解析器共属于177个供应商，用户和递归解析器的地理位置覆盖了全国34个省级行政区，用户分布在238个自治系统（AS, autonomous system），递归解析器分布在235个AS。

2.3 基于主动收集的权威服务器测量方法

权威域名服务器的集中化测量需要就国内域名，探查其依赖的权威域名服务器。为保证所探测的域名由国内用户注册，本文选取顶级域.cn的子域名作为权威服务器测量的域名数据集，因其在申请注册时需进行身份证明。该数据集可通过相关测量工作[19]中使用的公共DNS查询工具ViewDNS.info收集的域名列表获取。

特别地，为了研究中国教育域名系统，选取了.edu.cn的子域名进行研究。其并没有公开渠道可获取。因此，本文通过从国内某大型域名服务商的被动域名解析流量中提取顶级域为edu.cn的二级域名，来构造中国教育域名列表。为保证收集到的域名处于活跃状态，本文仅保留在2024年可正常解析且累积被查询次数超过50次的域名。

探测上述两类域名的权威服务器测量数据集如表1所示。此外，本文同样使用IP-API[17]来获取权威服务器的所属组织。

表1 权威服务器测量数据集

域名类型	活跃域名数量	权威服务器数量	权威覆盖AS数量
.cn子域名	3 073 282	22 740	2 253
.edu.cn子域名	2 543	2 280	66

2.4 测量实验伦理道德问题考量

为了避免测量实验对互联网造成影响，本文严格遵守伦理道德要求，对测量过程进行了严格的把控。本文的递归解析器测量平台仅收集了国内用户的IP地址和其使用的递归解析器，并未记录用户的浏览偏好和隐私信息，测量实验结束后会立即断开与用户的任何交互。测量实验中使用的域名和服务器都为专用的受控服务器，并且为服务器部署在线网页，说明实验意图和联系方式。在对权威域名服务器测量的过程中，本文严格控制网络扫描的流量和并发度，防止对解析器和扫描目标造成过大负载。

3 国内递归解析服务的集中化程度分析

3.1 国内递归解析服务市场概览

本文测量结果表明国内用户的首选递归解析器的市场HHI为36.5%，属于高度集中化。递归解析器市场通常可以分为本地ISP和公共的开放递归解析服务商。图3展示了国内用户配置的首选递归解析器的分布情况，可以看到国内运营商占据了主要的市场份额，中国移动、中国电信、中国网通和中国联通为国内88.7%的国内用户提供递归解析服务。中国移动的用户市场是最庞大的，占据了48.0%。本地ISP的递归解析服务通常位于离用户网络较近的地方，测量结果表明44 357个用户（82.2%）与其配置的递归解析器在同一省市，

45 679 个用户（84.6%）与其配置的递归解析器在同一 AS 下。此外，先前研究工作[3]表明全球三分之二的用户使用本地 ISP 分配的递归解析器，这一比例要低于国内。主要原因在于公共递归解析器在国外更受欢迎，特别是谷歌 DNS[3]。

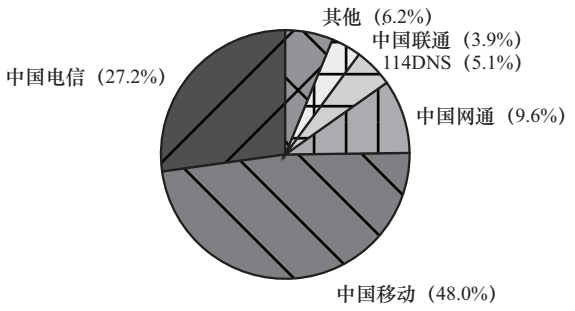

图3　用户配置的首选递归解析器的分布情况

对于知名公共解析器，本文选取了 114DNS、阿里云 DNS、腾讯 DNSPod、百度 DNS、谷歌 DNS、OpenDNS 等作为分析对象。知名公共解析器的用户有 3 450 个（6.4%），其中 114DNS 的用户数量最多，达到了 2 737 个（79.3%）。然而，在国外用户市场份额可占到 14.0% 的谷歌 DNS[3]，在国内仅有 0.2% 的用户在使用。此外，国内的开放递归解析器市场 HHI 为 49%，同样属于高度集中化。

对于用户配置的全部递归解析器市场，本文计算得到的 HHI 为 24.1%，体现出的集中化程度要低于首选递归解析器市场。这主要是由于用户在除去首选配置的 ISP 递归解析器外，通常还会配置公共的开放递归解析器作为候选。

3.2　国内不同地区用户的递归解析器配置

本节对国内不同地区的递归解析器配置情况进行分析，通过不同地区的递归解析器的服务提供商的占比计算相应的 HHI 值。表 2 展示了用户首选递归解析器市场 HHI 前三名和后三名的情况。

用户的首选递归解析器市场的 HHI 平均值为 40.6%，这表示大部分地区的用户所使用的递归解析器都集中于少量供应商。递归解析器市场集中度高的地区主要为互联网基础设施相对落后的地区，它们的 HHI 均超过了 50%。对于基础设施较为发达的地区，它们的 HHI 值均小于 35%。此外，用户全部递归解析器市场的 HHI 平均值比为 29.9%，低于首选递归市场，但集中度较高的地区与首选递归市场相似。

表 2　用户首选递归解析器市场 HHI 排名

排名	省级行政区	HHI
1	西藏	68.0%
2	青海	58.3%
3	甘肃	51.9%
32	陕西	30.8%
33	上海	29.0%
34	北京	21.4%

4　国内域名权威服务的集中化程度分析

4.1　.cn 子域名的权威服务器部署

本节分析 .cn 子域名的权威服务器的集中化情况。该部分域名的权威服务器市场的 HHI 为 35.5%，而之前研究工作表明全球流行域名的权威服务器市场的 HHI 为 15%。因此，我国域名的权威服务的集中化程度相对全球域名更为突出。

表 3 为 .cn 子域名的权威服务器市场中，排名前 10 的提供商分布。阿里云为 .cn 子域名的主要权威服务供应商，占到了 57.6%。而对于全球流行域名主要依赖的国外权威服务供应商[3]，如亚马逊云、Cloudflare 等，.cn 子域名很少将授权服务托管给它们。

表 3　cn 子域名权威服务器服务提供商分布

排名	提供商	占比	累积占比
1	阿里云	57.6%	57.6%
2	中国移动	8.1%	65.7%
3	中国电信	6.0%	71.7%
4	Cloudflare	5.6%	77.3%
5	帝恩思	5.0%	82.3%
6	唯一网络	4.9%	87.2%
7	腾讯云	4.9%	92.1%
8	中国联通	4.5%	96.6%
9	Godaddy	1.2%	97.8%
10	华为云	0.5%	98.3%

本文还对 .cn 子域名的权威服务器所在的 IP 地址网段进行了分析。结果表明排名前四的地址段均属于阿里云，分别为 39.96.153.32/27 地址段，47.118.199.192/27 地址段，120.76.107.32/27 地址段和 139.224.142.96/27 地址段，它们一共占据全部权威域名服务器的 57.0%。

4.2 .edu.cn子域名的权威服务器部署

本节对.edu.cn子域名的权威服务器部署进行分析，表4列举了排名前4的权威服务提供商。结果表明89.5%的.edu.cn子域名的权威服务器部署在CERNET网络中，权威服务器部署高度集中。这有利于教育网管理员监管和保护教育领域的关键域名基础设施，确保教育域名的解析服务可靠性，但是并不符合规范中对于权威服务器部署应满足网络拓扑多样性的要求[10]。这同时对教育网的域名授权服务提出了更高的要求，一旦出现故障将严重影响我国教育行业的网络服务运转。

表4 edu.cn子域名权威服务器服务提供商分布

排名	提供商	占比	累积占比
1	CERNET	89.5%	89.5%
2	中国电信	5.0%	94.5%
3	中国联通	0.9%	95.4%
4	阿里云	0.7%	96.1%

图4为.edu.cn子域名的权威服务器所在的IP地址网段的分布占比。从图4可以发现，相较于.cn子域名，.edu.cn子域名的权威服务器的IP地址分布较为分散。28.4%的权威服务器部署在属于CERNET的202.112.4.0/23网络地址段中，而其余IP地址段中的权威服务器数量都较少。具体来讲，39.2%的IP地址段中的权威服务器数量少于或等于两台。

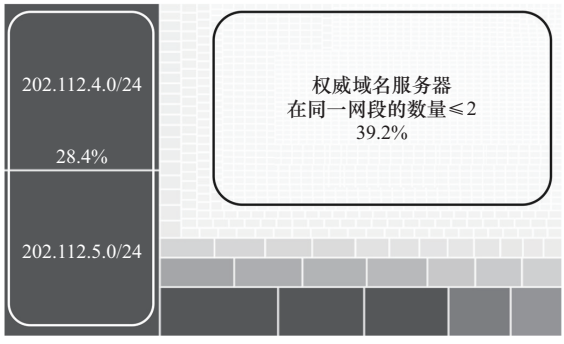

图4 .edu.cn子域名权威服务器IP地址段统计

5 结束语

本文针对国内域名基础设施的集中化程度展开研究，基于网页广告平台大范围测量国内用户的递归解析器配置，结合大型域名解析日志和再主动扫描测量.cn子域名特别是.edu.cn子域名的权威服务器部署。测量结果表明国内域名基础设施呈现高度集中化，大量域名递归解析和授权服务依赖于少数国内运营商和企业。ISP是国内主要的递归解析服务供应商，占用户市场的90.4%。国内用户使用的公共开放递归解析器主要为114DNS，而非在国外更为流行的谷歌DNS。.cn子域名的权威服务器集中部署于阿里云，而.edu.cn子域名权威服务器集中部署于CERNET。总之，我国域名基础设施存在大量潜在的单一故障节点，域名解析和授权服务供应商应加强对自身服务器的性能、灾备能力、防御措施的严格要求，做好流量负载均衡以及数据备份。网络安全部门应加强对集中化节点的安全风险监测和预警，防止单点故障的发生导致大面积的互联网服务中断。

参考文献：

[1] WOOLF N. DDoS attack that disrupted internet was largest of its kind in history[EB/OL]. (2016)[2024-10-22].

[2] 王左利, 魏亮. 揭秘5·19断网风暴 剖析断网事件[EB/OL]. (2009)[2024-10-22].
WANG Z L, WEI L. Unveiling the May 19th Internet Outage: Analyzing the Network Disruption Event[EB/OL]. (2009)[2024-10-22].

[3] HUSTON G. Looking at centrality in the DNS[EB/OL]. (2022)[2024-10-22].

[4] 刘文峰. 域名系统安全自主根区管理与解析关键技术研究[D]. 哈尔滨: 哈尔滨工业大学, 2022.
LIU W F. Research on key technologies of domain name system security autonomous root zone management and resolution[D]. Harbin: Harbin Institute of Technology, 2022.

[5] MOURA G C M, CASTRO S, HARDAKER W, et al. Clouding up the Internet: how centralized is DNS traffic becoming? [C]//Proceedings of the ACM Internet Measurement Conference. New York: ACM Press, 2020: 42-49.

[6] RADU R, HAUSDING M. Consolidation in the DNS resolver market – how much, how fast, how dangerous?[J]. Journal of Cyber Policy, 2020, 5(1): 46-64.

[7] SHUE C A, KALAFUT A J, GUPTA M. The web is smaller than it seems[C]//Proceedings of the 7th ACM SIGCOMM conference on Internet measurement. New York: ACM Press, 2007: 123-128.

[8] ALLMAN M. Comments on DNS robustness[C]//Proceedings of the Internet Measurement Conference 2018. 2018: 84-90.

[9] KASHAF A, SEKAR V, AGARWAL Y. Analyzing third party service dependencies in modern web services: have we learned from the mirai-dyn incident? [C]//Proceedings of the ACM Internet Measurement Conference. New York: ACM Press, 2020: 634-647.

[10] ELZ R, BUSH R, BRADNER S, et al. RFC 2182: Selection and Operation of Secondary DNS Servers[R]. 1997.

[11] LOTTOR M K. Domain administrators operations guide[J]. RFC,

1987, 1033: 1-22.
[12] MOCKAPETRIS P. RFC 1034: Domain names - concepts and facilities [R]. 1987.
[13] MOCKAPETRIS P. Domain names - implementation and specification [R]. 1987
[14] FTC. A look at what isps know about you: examining the privacy practices of six major internet service providers [R]. 2021.
[15] LEYDESDORFF L, RAFOLS I. Indicators of the interdisciplinarity of journals: diversity, centrality, and citations[J]. Journal of Informetrics, 2011, 5(1): 87-100.
[16] ROTUNDO G, D'ARCANGELIS A M. Network of companies: an analysis of market concentration in the Italian stock market[J]. Quality & Quantity, 2014, 48(4): 1893-1910.
[17] LI R, LIU B, LU C, et al. A Worldwide view on the reachability of encrypted DNS services[C]//Proceedings of the ACM on Web Conference 2024. New York: ACM Press, 2024: 1193-1202.
[18] HUANG C, MALTZ D A, LI J, et al. Public DNS system and global traffic management[C]//Proceedings of IEEE INFOCOM. Piscataway: IEEE Press, 2011: 2615-2623.
[19] HOLZ R, AMANN J, RAZAGHPANAH A, et al. The era of TLS 1.3: measuring deployment and use with active and passive methods[J]. arXiv Preprint, arXiv:1907.12762, 2019.

[作者简介]

刘世明（2000– ），男，山东平度人，清华大学硕士生，主要研究方向为网络安全、网络测量。

李瑞烜（1999– ），男，山西忻州人，清华大学工程师，主要研究方向为网络测量、域名安全、邮件安全等。

刘保君（1994– ），男，安徽宿州人，博士，清华大学助理教授、博士生导师，主要研究方向为网络安全、网络测量、网络犯罪检测等。

段海新（1972– ），男，山东济宁人，博士，清华大学教授、博士生导师，主要研究方向为网络和系统安全。

孙东红（1974– ），女，黑龙江哈尔滨人，博士，清华大学副研究员，主要研究方向为网络与信息安全。