基于转发关系推断的公共解析器任播节点枚举方法

许成喜[1,2]，施凡[1,2]，张允义[1,3]，刘保君[3]，张先国[4]，李振汉[1]，王宇轩[1]
（1.国防科技大学电子对抗学院，安徽 合肥 230037；2.网络空间安全态势感知与评估安徽省重点实验室，安徽 合肥 230000；
3.清华大学网络科学与网络空间研究院，北京 100084；4.中电网络空间研究院有限公司，北京 100043）

摘　要：为了解决任播节点枚举所需测量资源多、成本高、召回率低等问题，针对采用任播技术部署的公共解析器，提出了一种基于转发关系推断的任播节点枚举方法。基于转发器与公共解析器之间存在内生转发关系的观察，将海量转发器转化成公共解析器任播节点测量的观测节点；然后，通过多轮次迭代执行转发关系测量、间接递归解析器聚合和转发器关联等步骤，推断转发器与公共解析器服务地址之间的转发关系，实现公共解析器任播节点的螺旋式枚举。以Google公共解析器公开数据为基准数据集，实验结果表明，所提方法仅需一台测量节点即可召回62.5%的Google公共解析器任播节点机场代码，与已有方法相比，在测量节点需求降低3~4个数量级的条件下，任播节点机场代码召回率提升了22.92个百分点。

关键词：公共解析器；任播节点枚举；转发关系；迭代算法；低成本
中图分类号：TP393.4
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024247

Enumerating anycast instances of public DNS resolver based on forwarding relationship inference

XU Chengxi[1,2], SHI Fan[1,2], ZHANG Yunyi[1,3], LIU Baojun[3],
ZHANG Xianguo[4], LI Zhenhan[1], WANG Yuxuan[1]
1. College of Electronic Engineering, National University of Defense Technology, Hefei 230037, China
2. Anhui Province Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, Hefei 230000, China
3. Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China
4.Cyberspace Institute Co., Ltd of China Electronics Technology Group Corporation, Beijing 100043, China

Abstract: In order to solve the problems of high measurement resources needed, high cost, and low recall rate for anycast enumeration, an anycast enumeration method based on forwarding relationship inference was proposed for anycast-based public DNS resolvers. Based on the observation of the endogenous forwarding relationship between open forwarders and public DNS resolvers, a massive number of open forwarders were transformed into vantage points in measuring public DNS resolvers' anycast instances; Then, through multiple iterations of forwarding relationship measurement, indirect resolver aggregation, and forwarder correlation, the forwarding relationship between forwarders and the DNS resolvers' service addresses was inferred, achieving a spiral enumeration of public parser anycast nodes. Using the publicly available data of Google Public DNS as the benchmark dataset, the experimental results show that the proposed method only requires one measurement machine to recall 62.5% of the airport codes of Google Public DNS's anycast instances. Compared with existing methods, the recall rate of anycast instance airport codes has increased by 22.92% under the condition of reducing the demand for measurement nodes by 3-4 orders of magnitude.

Keywords: public DNS resolver, anycast enumeration, forwarding relationship, iterative algorithm, low-cost

收稿日期：2024–08–21
通信作者：施凡，shifan17@nudt.edu.cn
基金项目：国家社会科学基金资助项目（No.2023-SKJJ-C-063）
Foundation Item: The National Social Science Foundation of China (No.2023-SKJJ-C-063)

0 引言

任播[1]是RFC 1546首次提出的一种特殊的网络通信方式，使用户可以访问同一个任播IP地址所标识的一组主机或服务中最近的任意一个。随着全球互联网的飞速发展，为了提升域名系统的抗攻击能力和域名解析效率，任播技术在域名系统领域得到广泛应用。域名系统运营机构面向用户提供统一的任播IP地址作为服务地址，而将实际执行递归域名解析流程的解析器部署在多个分散的地理位置上作为任播节点。任播技术的广泛应用催生出了公共解析器这一新兴的域名系统基础设施角色。自从2009年Google率先推出采用任播技术部署的公共解析器（服务IPv4地址为8.8.8.8和8.8.4.4）以来，基于任播技术的公共解析器市场得到蓬勃发展，先后涌现出了OpenDNS、Level3 DNS、Cloudflare DNS、114 DNS、AliDNS等诸多知名的公共解析器[2]。据测算，截至2022年11月，公共解析器在域名解析市场中的占有率已达到20%[3]。

公共解析器诞生后，公共解析器测量研究很快成为互联网测量领域研究的热点问题[4]。Randall等[5]对Google公共解析器、OpenDNS、Cloudflare和Quad9 DNS等4个主流公共解析器的缓存策略进行了推断与分析。Turgut等[6]利用RIPE Atlas节点对Google公共解析器的地理位置分布和缓存一致性进行了研究。Doan等[7]利用10 600个RIPE Atlas节点对公共解析器服务的流行度和性能进行了分析评估。Gamba等[8]利用10 000个RIPE探针研究了9个知名的任播公共解析器的基础设施、性能和可达性。

任播节点识别与枚举也成为评估任播域名系统的域名解析效率、优化任播节点部署方案、提高任播域名系统韧性的重要途径。Calder等[9]提出一种基于ECS扩展的方法，实现了对Google的Web服务基础设施的枚举。Cicalese等[10-11]利用PlanetLab、RIPE等分布式测量平台提出一种协议无关的任播节点识别与枚举算法iGreedy，Sommese等[12]利用分布式测量平台实现了任播IPv4地址前缀的探测。

另一部分研究人员将公共解析器的任播节点看做解析器池。Alzoubi等[13]和Al-Dalky等[14]利用DNS协议中的CNAME链机制发现了公共解析器存在明显的解析器池现象。Huston等[3]利用RIPE分布式测量平台对公共解析器的解析器池进行了测量。不难发现，已有的任播节点枚举方法大多依赖于大规模测量平台，成本较高。例如，用户在使用RIPE Atlas分布式探针开展大规模测量之前，需通过赞助或共享自身节点的方式赚取足够的积分。

为了解决上述问题，本文提出一种轻量级的公共解析器任播节点快速枚举方法，利用可公开访问的转发器与公共解析器之间存在的内生转发关系，将海量的开放转发器转化成大规模分布式观测节点，使研究人员可以在单台主机上即可部署、触发完成公共解析器任播节点的测量与枚举，极大降低了公共解析器任播节点枚举研究与分析所需的测量资源。

1 研究背景

1.1 客户端域名系统基础设施

按照服务对象划分，互联网域名系统基础设施可分为服务端域名系统基础设施和客户端域名系统基础设施[15]。服务端域名系统基础设施主要是指权威域名服务器（ADNS, authoritative DNS），客户端域名系统基础设施主要由多种类型的解析器组成。随着互联网服务规模和终端用户规模的飞速发展，解析器架构从最初的分布式单服务器式设计逐渐进化到更加复杂的多层转发、多级缓存、多点备份的复杂架构，解析器分化为多种不同的角色。客户端域名系统基础设施因此呈现出更加复杂的结构，如图1所示。

图1中，箭头表示发送域名解析请求的方向。与客户端直接交互的解析器主要有开放解析器（ODNS, open DNS）和递归解析器系统（RDNSS, recursive DNS system）。递归解析器系统是指由域名解析服务提供商或ISP部署运营的复杂解析器系统，一般由解析器服务IP地址、隐藏解析器（HDNS, hidden DNS）和间接递归解析器（IRDNS, indirect recursive DNS）组成。其中，解析器服务IP地址为任播IP地址，用于面向终端用户提供域名解析服务，隐藏解析器主要用于递归解析器系统内部缓存和域名解析请求的分发调度，间接递归解析器主要作用是与权威域名服务器交互，执行实际的域名递归解析流程。开放解析器是指面向终端用户开放递归域名解析服务的解析器，主要包括转发器（FDNS, forwarder DNS）、直接递归解

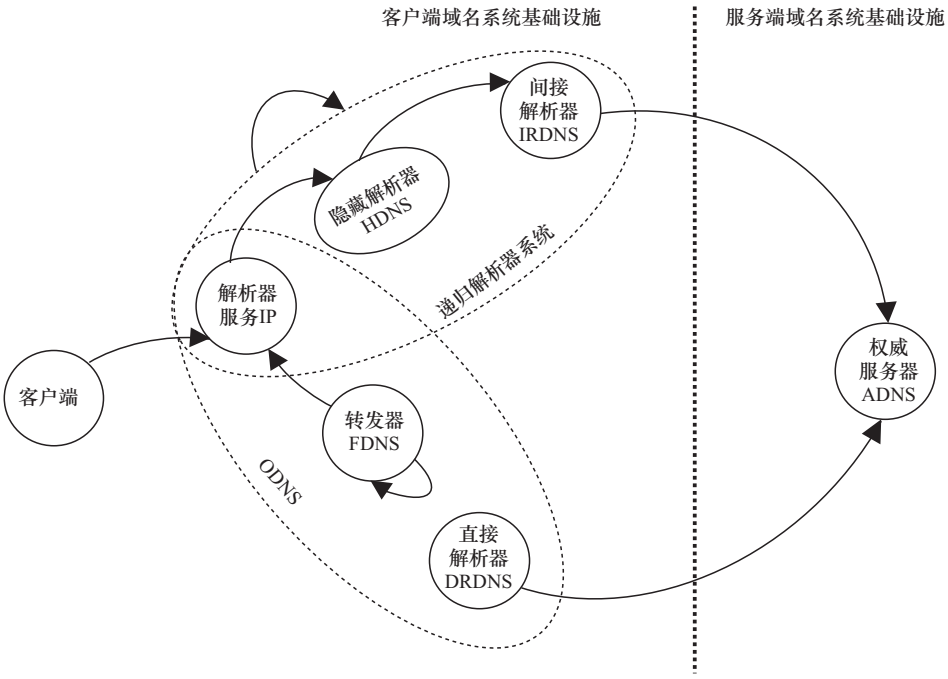


图1　客户端域名系统基础设施

析器（DRDNS, direct recursive DNS）等类型，从终端用户视角，解析器服务IP地址也与开放解析器体现出相同的开放递归服务的行为特征。综上所述，转发器、直接递归解析器和解析器服务IP等开放解析器接收终端用户的域名解析请求，间接递归解析器与权威域名系统直接交互，递归解析器系统通过一层或多层的隐藏解析器实现域名解析请求的高速分发和解析记录的高效缓存。客户端域名系统基础设施包含的解析器类型如表1所示。

从图1中域名解析请求处理流向可以看出，只有直接递归解析器和间接递归解析器直接与权威域名服务器交互，转发器只是将域名解析请求转发至另一个转发器或者递归解析器系统。据研究，至少有20%的转发器将域名解析请求转发至公共解析器等递归解析器系统[3]。

1.2　问题描述

公共解析器任播节点枚举问题可描述为：给定基于任播部署的公共解析器服务IP地址$RDNSS_{target}$，枚举解析器服务IP地址背后的任播实例及其IP地址。对应到图1中，则是已知递归解析器系统的服务IP，求解该解析器系统中部署的间接递归解析器集合。因此，本文研究的公共解析器任播节点枚举与特定递归解析器系统的解析器池发现具有相同的语义。

直觉上，观测节点的数量及地理分布是公共解析器任播节点枚举的关键所在，观测节点数量越多，地理分布越广泛，可召回的任播节点数量越多。这也是研究人员开展此类研究高度依赖于RIPE Atlas和PlanetLab等分布式测量平台的原因。然而，此类平台部署和使用成本较高，限制了大多

表1　　**客户端域名系统基础设施解析器类型**

解析器类型	简称	主要特征
转发器	FDNS	开启递归,接受公开访问,只将域名解析请求转发给上游解析器
直接递归解析器	DRDNS	开启递归,接受公开访问,实际执行域名递归解析过程
间接递归解析器	IRDNS	不接受公开访问,实际执行域名递归解析过程
隐藏解析器	HDNS	不接受公开访问,对外界透明,主要用于域名解析请求的高速分发和解析结果的高效缓存
递归解析器系统	RDNSS	开启递归,接受公开访问,本身具有较复杂的结构
递归解析器系统服务IP	Service IP	开启递归,接受公开访问,将域名解析请求分发给递归解析器系统中的其他解析器

数研究团队针对公共解析器任播节点开展持续的枚举分析。为此，根据大量转发器将域名解析请求转发至公共解析器这一观察，本文提出一种基于转发关系推断的公共解析器任播节点枚举方法。

2 方法设计

基于转发关系推断的公共解析器任播节点枚举的基本思想是利用转发器与公共解析器之间存在的内生转发关系，将海量转发器转化成为公共解析器任播节点枚举的观测节点，重复执行转发关系测量、间接递归解析器聚合和转发器关联等步骤，迭代地枚举公共解析器的任播节点。基于转发关系推断的公共解析器任播节点枚举方法总体架构如图2所示。

具体而言，首先在少量已有全网转发关系测量数据（如一个轮次）的基础上，采用实时探测的方法，首先向待测解析器系统$\mathrm{RDNSS}_{\mathrm{target}}$发送多次查询请求，获得初始间接递归解析器集合$\mathrm{IPI}_0=\{\mathrm{ipi}_1,\cdots\mathrm{ipi}_i,\cdots,\mathrm{ipi}_n\}$。然后，根据$\mathrm{IPI}_0$在已有转发关系测量数据$(\mathrm{IPF}_{\mathrm{in}},\mathrm{IPI}_{\mathrm{out}})$筛选出待测解析器系统$\mathrm{RDNSS}_{\mathrm{target}}$所服务的初始转发器集合$\mathrm{IPF}_0=\{\mathrm{ipf}_1,\cdots\mathrm{ipf}_i,\cdots,\mathrm{ipf}_m\}$。令$\mathrm{IPI}_{\mathrm{RDNSS}_{\mathrm{target}}}=\mathrm{IPI}_0$，$\mathrm{IPF}_{\mathrm{RDNSS}_{\mathrm{target}}}=\mathrm{IPF}_0$。接下来，通过实时探测的方法迭代地更新$\mathrm{IPI}_{\mathrm{RDNSS}_{\mathrm{target}}}$和$\mathrm{IPF}_{\mathrm{RDNSS}_{\mathrm{target}}}$。具体地，向转发器集合$\mathrm{IPF}_{\mathrm{RDNSS}_{\mathrm{target}}}$发送转发关系查询请求。由于转发器设置的转发关系具有内生性和确定性，在短时间内不会频繁改变。因而，可以推测这些查询请求经过一次或多次转发，将到达待测解析器系统$\mathrm{RDNSS}_{\mathrm{target}}$，进而分发至某个间接递归解析器，完成最终的域名解析过程。考虑到转发器可能设置了多个上游解析器系统，引入间接递归解析器扩展策略，即通过自治系统组织机构（ASO, autonomous system organization）信息来过滤非同一待测解析器系统$\mathrm{RDNSS}_{\mathrm{target}}$的间接递归解析器进入间接递归解析器集合$\mathrm{IPI}_{\mathrm{RDNSS}_{\mathrm{target}}}$。若后续查找中的候选间接递归解析器$\mathrm{ipi}_c$的ASO信息与当前$\mathrm{IPI}_{\mathrm{RDNSS}_{\mathrm{target}}}$中的ASO信息一致，则将候选间接递归解析器$\mathrm{ipi}_c$添加到$\mathrm{IPI}_{\mathrm{RDNSS}_{\mathrm{target}}}$中。然后，根据实时探测到的转发关系数据和已有的转发关系数据更新$\mathrm{IPF}_{\mathrm{RDNSS}_{\mathrm{target}}}$。迭代地执行上述过程，直到$\mathrm{IPI}_{\mathrm{RDNSS}_{\mathrm{target}}}$达到一个稳定的状态，其中的节点数量不再增多。算法的伪代码描述如算法1所示。

算法1 基于转发关系推断的任播节点枚举算法

给定以解析器服务IP地址形式给定待测公共解析器$\mathrm{RDNSS}_{\mathrm{target}}$，和基础转发关系测量数据$(\mathrm{IPF}_{\mathrm{in}},\mathrm{IPI}_{\mathrm{out}})$。

1) 生成初始集合：$\mathrm{IPI}_0=\{\mathrm{ipi}_1,\cdots\mathrm{ipi}_i,\cdots,\mathrm{ipi}_n\}$，$\mathrm{IPF}_0=\{\mathrm{ipf}_1,\cdots\mathrm{ipf}_i,\cdots,\mathrm{ipf}_m\}$，$\mathrm{ASO}_{\mathrm{IPI}}\leftarrow\mathrm{get\_aso}(\mathrm{IPI}_0)$。$\mathrm{IPI}_{\mathrm{RDNSS}_{\mathrm{target}}}=\mathrm{IPI}_0$，$\mathrm{IPF}_{\mathrm{RDNSS}_{\mathrm{target}}}=\mathrm{IPF}_0$，$\mathrm{Len}_{\mathrm{RDNSS}_{\mathrm{target}}}(0)=\mathrm{Len}(\mathrm{IPI}_0)$。

2) 循环

3) 向$\mathrm{IPF}_{\mathrm{RDNSS}_{\mathrm{target}}}$发送转发关系测量报文，收集转发关系测量数据，生成候选转发关系$(\mathrm{IPF}_c,\mathrm{IPI}_c)$；

4) for ipi_{ci} in IPI_c

5) if $\mathrm{ASO}_{\mathrm{ipi}_{ci}}\in\mathrm{ASO}_{\mathrm{IPI}}$

6) $\mathrm{IPI}_{\mathrm{RDNSS}_{\mathrm{target}}}=\mathrm{IPI}_{\mathrm{RDNSS}_{\mathrm{target}}}\cup\{\mathrm{ipi}_{ci}\}$；

7) $\mathrm{IPF}_{\mathrm{RDNSS}_{\mathrm{target}}}=\mathrm{IPF}_{\mathrm{RDNSS}_{\mathrm{target}}}\cup\mathrm{IPF}_{\mathrm{ipi}_{ci}}$；

8) $\mathrm{Len}_{\mathrm{RDNSS}_{\mathrm{target}}}(i)=\mathrm{Len}(\mathrm{IPI}_{\mathrm{RDNSS}_{\mathrm{target}}})$；

9) end if

10) end for

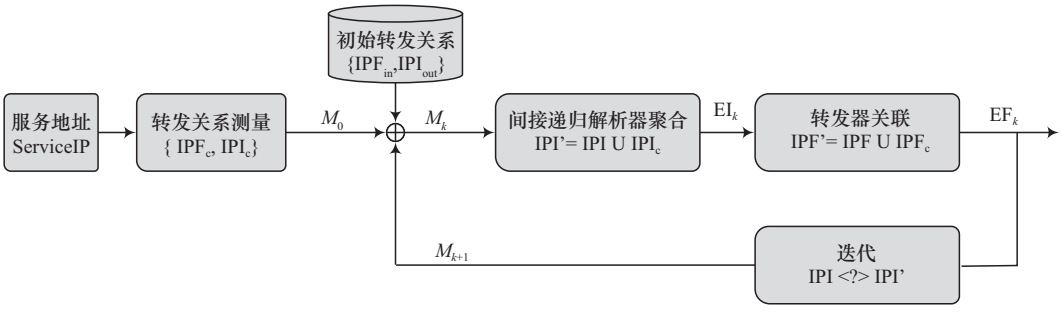


图2 基于转发关系推断的公共解析器任播节点枚举方法总体架构

11) until $Len_{RDNSS_{target}}(i)$收敛，即$Len_{RDNSS_{target}}(i+1)=Len_{RDNSS_{target}}(i)$。

2.1　转发关系测量

转发是指用户域名解析请求在到达权威服务器之前在多个解析器中流转的现象。当域名解析请求从一个解析器流转至另一个解析器时，则称两者之间存在转发关系。一个转发器可能会将解析请求转发至另一个转发器，一个递归解析器系统也可能将解析请求转发至另一个递归解析器系统。更为一般地，当解析器之间存在转发关系时，则形式化描述为R1 → R2，此时，称R2为R1的上游解析器。这里的解析器可能是转发器，也可能是递归解析器系统，如公共解析器。

转发关系是客户端域名系统基础设施中普遍存在的基本关系，客户端域名基础设施正是靠着解析器间的转发关系实现了全球互联网用户域名解析流量的分发、转发与汇聚。解析器转发关系测量的过程中常常伴随着解析器组件的识别，其目标是识别出客户端域名系统基础设施中各类型解析器，区别其在域名解析过程中扮演的角色作用。已有研究中，研究人员的常规实践是使用A类型的资源记录来发现开放解析器。具体来说，研究人员注册测试用户并部署该域名的权威服务器，配置特定的A类型资源记录。然后在测试端发起精心设计的查询请求，如在子域中嵌入目标测试IP，以将测量流量与其他流量区分开来。然后收集相应记录，根据一定的规则，对解析器角色加以识别。研究人员主要采取两种数据收集方法：一是从权威名称服务器获取查询日志[13,16]；二是从测量节点（VP, vantage point）收集固定或特定信息编码的响应[17]。

现有解析器转发关系测量及解析器组件识别研究中存在测量报文的应答报文容易被篡改、抗篡改能力差的问题。已有研究均采用查询A记录的测量报文，而A记录的应答记录很容易在域名解析过程中经过中间网络设备时被篡改，导致这种方法探测转发关系的准确性无法保证。

为应对上述问题，本文对现有的测量方法进行了扩展，设计实现了基于TXT记录的测量方法，其核心思想在于：1) 测量报文中采用TXT类型查询请求替代A类型查询请求，TXT记录为可变长度字符串，能够支持在应答报文中嵌入定制化的响应信息，因而，可以用来规避、识别解析器篡改记录的行为；2) 对权威DNS服务器进行定制化修改，使其在收到特定的TXT类型查询时，自动返回定制化的动态响应信息。

基于TXT记录的转发关系测量方法流程如图3所示。测量节点首先向IPv4地址空间中的待测IP地址（如IP1）发送转发关系测量报文Q1，查询IP1.mydomain.com域名的TXT记录。若IP1为解析器，则接受测量报文的查询请求，触发域名解析流程，通过IP2向预设的权威DNS服务器发送与测量报文相同的查询请求Q2。权威DNS服务器自动将间接递归解析器IP地址、查询端口及时间戳等动态信息封装在应答报文中的TXT记录中，构建形如“timestamp#IP2#srcport#”的TXT应答记录，并沿着测量报文解析路径返回至测量节点。如此一来，仅需在测量节点上收集R2，即可得到转发关系数据。

图3中，Q2为权威DNS服务器收到的测量请求，R2为测量节点收到的数据。Q2意味着转发关系测量请求触发了解析器的域名解析流程，R2意味着解析器对转发关系测量域名查询请求做出了响应并返回了应答报文。

基于转发关系推断的公共解析器任播节点枚举方法中需要进行多轮次的转发关系测量。首先，在算法执行初始化阶段，进行一次全网的转发关系测量，作为已知间接递归解析器与转发器关联的数据依据。然后，在每轮次迭代过程中，针对关联得到的转发器集合进行一次转发关系测量，将更多转发器转化成为任播节点枚举的观测节点。

2.2　间接递归解析器聚合

基于转发关系推断的公共解析器任播节点枚举

图3　基于TXT记录的转发关系测量方法流程

的基本思路是将$IPF_{RDNSS_{target}}$作为分布式测量节点，利用$IPF_{RDNSS_{target}}$与待测公共解析器$RDNSS_{target}$服务IP地址之间存在的转发关系，在一个单一的测量发起节点上向大量$IPF_{RDNSS_{target}}$发送转发关系测量报文并接收应答报文，提取并构建候选的间接递归解析器集合IPI_c。通过比对间接递归解析器的IP地址ASO信息，判断是否更新待待测公共解析器$RDNSS_{target}$的间接递归解析器池集合$IPI_{RDNSS_{target}}$。选择ASO信息作为间接递归解析器聚合条件是因为Google、Cloudflare、OpenDNS等公共解析器服务提供商倾向于使用其构建的全球云基础设施部署其运营的公共解析器的任播节点。

2.3 转发器关联

在更新间接递归解析器池集合$IPI_{RDNSS_{target}}$的同时，利用全网的转发关系数据，更新转发器集合$IPF_{RDNSS_{target}}$，作为观测节点用于下一轮次的转发关系测量。具体地，在全网转发关系数据中，将所有与更新后的间接递归解析器池$IPI_{RDNSS_{target}}$存在转发关系的转发器筛选出来。在算法1执行迭代过程中，由于新的间接递归解析器节点的加入，在全网转发关系数据中必定会关联到更多的转发器。同时，根据任播协议语义，在同一个节点上多次访问，可能会访问到不同的任播节点，因此，论文采取将关联得到的全量转发器均参与下一轮次的转发关系测量的策略，用以加速算法收敛。

2.4 迭代收敛条件

基于转发关系推断的公共解析器任播节点枚举通过迭代执行转发关系测量、间接递归解析器聚合和转发器关联等步骤，实现公共解析器任播节点的螺旋式枚举。显然，本文的迭代算法是收敛的，极限情况为枚举出全部任播节点。当上述迭代过程无法发现新的间接递归解析器时，可认为算法应当停止。因此，算法1的迭代停止条件为相邻2个轮次得到的间接递归解析器数量没有发生变化，即$Len_{RDNSS_{target}}(i+1) = Len_{RDNSS_{target}}(i)$。

3 实验分析

为了证明所提任播节点枚举方法的有效性，论文对基于分布式测量平台、基于CNAME链、基于NS链和基于转发关系的等四类方法的成本与性能进行了测量与对比分析。

3.1 基准数据

虽然任播技术在公共解析器市场领域十分流行，然而，除Google之外，鲜有DNS服务提供商公开他们的任播节点或解析器池列表。Google在其官方页面上公开了其运营的公共解析器服务所依赖的IP地址段，根据Google公布的数据[18]，Google公共解析器的任播节点分布在全球的292个大小不等的IP地址段，IP前缀在/24到/26之间，Google将这些IP地址段编码成48个唯一的地理位置，用临近的机场代码进行标识（即GeoCode）。因此，选择Google公开的数据作为基准数据。

3.2 度量指标

为了定量度量任播节点枚举方法的能力，定义了任播节点的召回率指标，即算法发现的任播节点IP地址数量占待测公共解析器公布的任播节点总数的百分比，计算式为

$$\mathrm{recall}_{\mathrm{irdns}} = \frac{\mathrm{sum}(\mathrm{irdns}_{\mathrm{dis}})}{\mathrm{sum}(\mathrm{irdns}_{\mathrm{all}})} \times 100\% \tag{1}$$

其中，$\mathrm{sum}(\mathrm{irdns}_{\mathrm{dis}})$为算法发现的公共解析器任播节点数量，$\mathrm{sum}(\mathrm{irdns}_{\mathrm{all}})$为官方公开的任播节点数量。需要注意的是，虽然Google公开了其任播节点的IP地址范围，但没有公开具体的任播节点数量。因此，实验中仍然无法计算准确的$\mathrm{recall}_{\mathrm{irdns}}$指标。为此，本文利用同步序列编号（SYN）扫描的方法，对Google公布的292个IP地址段的IP地址进行了存活性探测，共发现7048个存活主机。实验中，以上述数值作为Google公布的任播节点数量的近似值。

此外，为了与iGreedy等方法进行比较，参照任播节点召回率指标定义了任播节点IP地址段召回率$\mathrm{recall}_{\mathrm{irdnsrange}}$、任播节点机场代码召回率$\mathrm{recall}_{\mathrm{irdnsgeocode}}$等可计算的度量指标，用于评价任播节点枚举方法对任播节点IP地址段和任播节点相邻机场代码的召回率。

$$\mathrm{recall}_{\mathrm{irdnsrange}} = \frac{\mathrm{sum}(\mathrm{irdnsrange}_{\mathrm{dis}})}{\mathrm{sum}(\mathrm{irdnsrange}_{\mathrm{all}})} \times 100\% \tag{2}$$

$$\mathrm{recall}_{\mathrm{irdnsgeocode}} = \frac{\mathrm{sum}(\mathrm{irdnsgeocode}_{\mathrm{dis}})}{\mathrm{sum}(\mathrm{irdnsgeocode}_{\mathrm{all}})} \times 100\% \tag{3}$$

3.3 实验设置

实验采用扩展的Zmap[19]进行迭代的转发关系探测。实验使用了一条中国电信的互联网专线，上下行对等带宽为100Mbit/s。测量主机为一台普通

的商用台式机，安装的操作系统为Linux Kali2 5.2.0。待测公共解析器设置为Google公共解析器，其公开的IPv4服务地址为8.8.8.8和8.8.4.4。

3.4　实验结果

表2展示了分布式测量平台[10]、CNAME链[14]、NS链[20]、转发关系等4种解析器池发现方法的性能。其中，由于Google只公开了部署解析器池的IP地址段，并未公开具体解析器节点IP地址及数量，因此，在进行算法比较时，计算了各种算法的3种类型的召回率指标，即$\text{recall}_{\text{irdns}}$、$\text{recall}_{\text{irdnsrange}}$及$\text{recall}_{\text{irdnsgeocode}}$，如表2所示。

表2　　任播节点枚举实验结果

方法	$\text{recall}_{\text{irdns}}$	$\text{recall}_{\text{irdnsrange}}$	$\text{recall}_{\text{irdnsgeocode}}$
iGreedy[10]（分布式测量平台）	N/A	N/A	39.58%
CNAME链[14]	4.50%	N/A	N/A
NS链[20]	7.19%	29.79%	45.83%
转发关系	33.29%	58.22%	62.5%

表2中的iGreedy算法由Cicalese等[10]提出，用于对任播系统的任播实例进行枚举和定位，iGreedy算法基于时延测量，利用时间不一致性思想和贪婪算法实现了任播节点的枚举。根据其网站公开的结果，iGreedy算法能够枚举19个Google公共DNS的任播实例，即对应于Google公布数据中的机场代码数量，召回率为39.58%。由于iGreedy算法基于时延测量，无法准确获知解析器IP地址，因此无法对任播实例的IP地址或IP地址范围进行精细的分析。根据Schomp等2018年的测量结果，基于CNAME链的解析器池发现方法发现的最大的解析器池即Google的解析器池，包含317个间接递归解析器[14]，这意味着该方法任播节点的召回率仅为4.5%，由于文中仅说明这些解析器来自5个IPv4 /24 CIDR网段，并未给出具体的解析器IP地址范围，无法进行$\text{recall}_{\text{irdnsrange}}$和$\text{recall}_{\text{irdnsgeocode}}$的计算分析。

综合来看，论文基于转发关系的任播节点枚举方法在$\text{recall}_{\text{irdns}}$、$\text{recall}_{\text{irdnsrange}}$和$\text{recall}_{\text{irdnsgeocode}}$等3个召回率度量指标上均明显高于已有方法。基于NS链的方法的任播节点召回率$\text{recall}_{\text{irdns}}$是基于CNAME链的方法的1.6倍，然而其能力受限于特征解析器（RD=1）的规模和分布。相比较而言，基于转发关系的方法将海量转发器转化成观测节点，其任播节点召回能力是基于CNAME链的7.4倍，是基于NS链的4.6倍，任播节点相邻机场代码召回率达到62.5%，在iGreedy算法召回率基础上提升了22.92个百分点，是iGreedy算法的1.58倍。

3.5　分析讨论

表3从依赖的探测资源、所能获得的观测节点数量和召回率3个方面比较了现有的公共解析器任播节点枚举方法。

3.4节已经对召回率指标进行了对比分析，本节主要对各种方法所能利用的观测节点规模进行对比分析。iGreedy算法依赖于分布式测量平台。知名的测量平台可在全球广泛部署其观测节点，如RIPE Atlas在全球103个国家和地区的542个城市部署了约10 000个观测节点，PlanetLab在全球48个国家的717个地理位置部署了1 300个测量节点。然而，平台测量节点的部署受到诸多因素的影响，包括地缘政治、用户习惯和市场份额，以上偏置将导致依赖这些平台开展的测量存在难以量化的视域限制。另一方面，由于分布式测量平台的部署成本高，大多数分布式测量平台并不能免费使用，获得平台使用授权也并不容易，往往需要支付赞助费用或者共享自己的节点，加入分布式测量平台中。基于CNAME链、NS链和转发关系的任播节点枚举方法均可以直接采用单台测量主机进行测量，大幅降低测量门槛，然而，这3种方法所能获得的实际

表3　　任播节点枚举方法分析比较

方法	依赖探测资源	节点规模（$\times 10^3$）	召回率
iGreedy	分布式测量平台	1~10	N/A, N/A, 39.58%
CNAME链	单台测量主机	0.1	4.50%, N/A, N/A
NS链	单台测量主机	1.5	7.19%, 29.79%, 45.83%
转发关系	单台测量主机	10~100	33.29%, 58.22%, 62.5%

观测节点的规模却存在较大差异，其中，基于CNAME链的方法通过控制CNAME链长度、CNAME记录等参数，最多可获得上百个观测节点的观测效果。然而，文献指出该方法的使用存在较大的局限性；基于NS链的方法可将满足一定特性的解析器转化成观测节点，这些解析器与大多数解析器的不同之处在于经其流转后的域名解析查询中请求递归（RD, recursion desired）标志仍然置位。该方法可获得分布于18个国家地区的约1500个可用于测量的开放解析器；基于转发关系的方法可将与待测公共解析器存在转发关系的开放转发器转化成为观测节点，其优势在于转发器规模基数庞大，且大量转发器与公共解析器之间存在内生的转发关系。由此关联得到可用于观测节点的转发器规模可达数万到数十万。以Google公共解析器为例，这样的转发器数量约有10.8万个，节点规模远超现有的分布式测量平台和其他方法。

综上所述，基于转发关系的公共解析器任播节点枚举方法借助于与公共解析器存在转发关系的转发器，将其转化成为任播节点枚举的观测节点。本文所提方法对测量节点的需求仅为基于分布式测量平台的方法的1‰~1‰，显著降低了依赖探测资源，同时在多个召回率指标上明显优于现有方法。

4 结束语

本文对基于转发关系推断的公共解析器任播节点枚举方法进行了研究。基于转发器与公共解析器之间存在内生转发关系的观察，通过重复执行转发关系测量、间接递归解析器聚合和转发器关联等步骤，将海量转发器转化成公共解析器任播节点枚举的观测节点，迭代实现了公共解析器任播节点的轻量级枚举，使研究人员仅需一台联网观测节点即可完成公共解析器任播节点枚举。实验结果表明，与已有方法相比，本文方法具有实施成本低和任播节点召回率高的优点。

参考文献：

[1] PARTRIDGE C, MENDEZ T, MILLIKEN W. Host anycasting service [J]. RFC, 1993, 1546: 1-9.

[2] 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.

[3] Huston G. Looking at centrality in the DNS[EB/OL]. 2022.

[4] 刘文峰, 张宇, 张宏莉, 等. 域名系统测量研究综述[J]. 软件学报, 2022, 33(1): 211-232.
LIU W F, ZHANG Y, ZHANG H L, et al. Survey on domain name system measurement research[J]. Journal of Software, 2022, 33(1): 211-232.

[5] RANDALL A, LIU E Z, AKIWATE G, et al. Trufflehunter: cache snooping rare domains at large public DNS resolvers[C]//Proceedings of the ACM Internet Measurement Conference. New York: ACM Press, 2020: 50-64.

[6] TURGUT T. Peeling the Google public DNS onion[D]. Amsterdam: University of Amsterdam, 2015.

[7] DOAN T V, FRIES J, BAJPAI V. Evaluating public DNS services in the wake of increasing centralization of DNS[C]//Proceedings of the 2021 IFIP Networking Conference (IFIP Networking). Piscataway: IEEE Press, 2021: 1-9.

[8] GAMBA J, FEAL´A, VALLINA-RODRIGUEZ N, et al. Exploring anycast-based public DNS resolvers[C]//Proceedings of the 18th ACM Internet Measurement Conference. New York: ACM Press, 2018:1.

[9] CALDER M, FAN X, HU Z, et al. Mapping the expansion of google's serving infrastructure[C]//Proceedings of the 2013 conference on Internet measurement conference. New York: ACM Press, 2013: 313-326.

[10] CICALESE D, JOUMBLATT D, ROSSI D, et al. A fistful of pings: Accurate and lightweight anycast enumeration and geolocation[C]// Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM). Piscataway: IEEE Press, 2015: 2776-2784.

[11] CICALESE D, AUGÉ J, JOUMBLATT D, et al. Characterizing IPv4 anycast adoption and deployment[C]//Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies. New York: ACM Press, 2015: 1-13.

[12] SOMMESE R, BERTHOLDO L, AKIWATE G, et al. MAnycast2: using anycast to measure anycast[C]//Proceedings of the ACM Internet Measurement Conference. New York: ACM Press, 2020: 456-463.

[13] ALZOUBI H A, RABINOVICH M, SPATSCHECK O. The anatomy of LDNS clusters: findings and implications for web content delivery [C]//Proceedings of the 22nd international conference on World Wide Web. New York: ACM Press, 2013: 83-94.

[14] AL-DALKY R, SCHOMP K. Characterization of collaborative resolution in recursive DNS resolvers[M]. Cham: Springer International Publishing, 2018.

[15] SCHOMP K, CALLAHAN T, RABINOVICH M, et al. On measuring the client-side DNS infrastructure[C]//Proceedings of the 2013 conference on Internet measurement conference. New York: ACM Press, 2013: 77-90.

[16] PARK J, KHORMALI A, MOHAISEN M, et al. Where are you taking me? behavioral analysis of open DNS resolvers[C]//Proceedings of the 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Piscataway: IEEE Press, 2019: 493-504.

[17] KÜHRER M, HUPPERICH T, BUSHART J, et al. Going wild: large-scale classification of open DNS resolvers[C]//Proceedings of the 2015 Internet Measurement Conference. New York: ACM Press, 2015: 355-368.

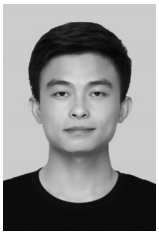
[18] Google. Locations of IP address ranges google public DNS[EB/OL]. 2023.

[19] DURUMERIC Z, WUSTROW E, HALDERMAN J A. Fast internet-wide scanning and its security applications[C]//Proceedings of the 22nd USENIX Security Symposium. Berkeley: USENIX Association, 2013: 605-620.
[20] XU C, ZHANG Y, SHI F, et al. Measuring the centrality of DNS infrastructure in the wild[J]. Applied Sciences, 2023, 13(9): 5739.

[作者简介]

许成喜（1989– ），男，安徽潜山人，博士，国防科技大学讲师，主要研究方向为互联网基础设施安全和网络空间测绘。

施凡（1983– ），男，安徽庐江人，博士，国防科技大学副教授，主要研究方向为网络空间测绘和网络空间测量。

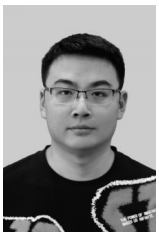


张允义（1996– ），男，山东巨野人，国防科技大学博士生，主要研究方向为互联网基础设施安全、互联网测量、DNS 协议安全分析和新型网络犯罪技术的检测与对抗。

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。

张先国（1981– ），男，安徽合肥人，中电网络空间研究院有限公司正高级工程师，主要研究方向为网络空间安全和网络攻防。

李振汉（1989– ），男，安徽怀宁人，国防科技大学讲师，主要研究方向网络空间测绘与大数据分析。



王宇轩（2000– ），男，河北保定人，国防科技大学博士生，主要研究方向为DNS 协议安全分析。