软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, 2023,34(3):1512−1522 [doi: 10.13328/j.cnki.jos.006321]

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

地区网络边界发现方法*

朱金玉, 张 宇, 曾良伟, 张宏莉, 方滨兴

(哈尔滨工业大学 网络空间安全学院, 黑龙江 哈尔滨 150001)

通信作者: 张宇, E-mail: yuzhang@hit.edu.cn

摘 要: 地区网络边界刻画了现实世界国家和地区之间在网络空间中的拓扑界限. 提出了一种主被动结合的双阶段地区网络边界发现方法——RNB (regional network border). 第 1 阶段, 基于定向拓扑测量与地理定位方法发现目标地区网络边界片段; 第 2 阶段, 基于多源信息加权定位和双重 PING 定位在边界片段中精准发现网络边界. 实验以中国网络为对象, 与 CAIDA 数据集相比, 仅以 2.5%的探测代价新发现了 37%的边界节点, 共计 1 644 个. 经人工验证的一致率为 99.3%, 经某运营商验证的准确率为 75%.

关键词: 地区网络边界; IP 地理定位; 拓扑测量; 网络空间测绘

中图法分类号: TP393

中文引用格式: 朱金玉, 张宇, 曾良伟, 张宏莉, 方滨兴. 地区网络边界发现方法. 软件学报, 2023, 34(3): 1512–1522. http://www.jos.org.cn/1000-9825/6321.htm

英文引用格式: Zhu JY, Zhang Y, Zeng LW, Zhang HL, Fang BX. Method of Discovering Regional Network Border. Ruan Jian Xue Bao/Journal of Software, 2023, 34(3): 1512 –1522 (in Chinese). http://www.jos.org.cn/1000-9825/6321.htm

Method of Discovering Regional Network Border

ZHU Jin-Yu, ZHANG Yu, ZENG Liang-Wei, ZHANG Hong-Li, FANG Bin-Xing

(School of Cyberspace Science, Harbin Institute of Technology, Harbin 150001, China)

Abstract: The regional network border describes the topological border nodes in cyberspace among countries and regions in the real world. By combining active and passive measurement techniques, this study proposes a dual-stage method of discovering regional network border (RNB) nodes. The first stage is to discover the regional network border's candidate sets by using directed topology measurement and multi-source geolocation. The second stage is to accurately identify border nodes from the candidate sets by using multi-source information weighted geolocation and dual PING geolocation. The experiment took China as the target region and discovered 1 644 border nodes. Compared with the CAIDA data set, the proposed approach's results have 37% of exclusively discovered border nodes with only 2.5% of the measurement cost. The accuracy rate under manual verification is 99.3%, and that under the verification of an ISP operator is 75%.

Key words: regional network border (RNB); IP geolocation; topology measurement; cyberspace surveying and mapping

地区网络边界是指国家/地区之间在互联网中直接互连的网络层节点集合, 刻画了现实世界地区之间在网络空间中的拓扑界限. 其中, 地区指 ISO 3166“国际标准化组织(ISO)针对国家、地区、具特殊科学价值地点以及其子行政区(如省或州)名称的国际标准代码”中的 249 个国家/地区. 地区网络指在该地区部署的网络节点集合, 包括终端主机、路由器等. 一个地区网络边界是在该地区内且与地区外路由器直接连接的路由器接口 IP 地址集合.

发现地区网络边界是网络空间测绘中的关键任务之一, 其应用包括:

(1) 特定地区网络拓扑发现[1−3]. 例如 CAIDA Mapkit[4]项目指出, 其研究任务的挑战之一是难以识别目

* 基金项目: 国家重点研发计划(2016QY01W0103, 2016QY01W0105)
收稿时间: 2020-09-09; 修改时间: 2020-11-23, 2020-12-29; 采用时间: 2021-02-04; jos 在线出版时间: 2021-10-20

标地区网络范围. 地区网络边界发现研究直接解决上述挑战, 从拓扑测量结果中根据地区网络边界提取该地区的拓扑.

(2) 地区网络审计设备部署情况测量. 例如在 FilterMap[5]中, 需要尽量完整地发现过滤器. 过滤器通常部署在网络边界上, 地区网络边界发现可为该研究提供候选过滤器目标集.

(3) IP 地理定位数据修正[6]. 例如本文第 3 节地区网络边界发现的实验结果可作为地标, 用于修正商业 IP 地理定位库中地区级数据.

目前, 国内外尚未有针对地区网络边界发现的研究, 与其最相近研究是 AS (autonomous system, 自治域)边界推断. 两者的区别在于: 前者是国家级地理边界, 后者是运营商级逻辑边界. Tire1 AS 可能跨越多个地区, 一个地区内可能含有多个小型 AS. 因此, AS 级边界识别无法在上述应用中直接发挥作用.

地区网络边界发现的核心任务是地区网络边界推测, 即以标有地理信息的探测路径为输入, 发现每条路径中的边界节点. 输入数据来自两项数据准备子任务: (1) 定向网络拓扑发现, 以目标地区的 IP 地址为输入, 从地区外探测点测量目标, 使得每条探测路径均覆盖边界; (2) 拓扑节点地理定位, 以定向网络拓扑发现的结果为输入, 采用多种地理定位方法对节点位置标记为地区内或地区外.

地区网络边界发现面临的主要挑战在于:

(1) 难以获取完整覆盖目标地区网络边界的 IP 级拓扑数据. 拓扑数据的完整性决定地区网络边界发现的完整性. 现有公开 IP 级网络拓扑测量数据集, 例如 CAIDA ITDK[7], 并不针对地区网络边界, 完整性不足. 第三方开放探测资源, 例如 LookingGlass 服务器[8], 分布广泛但效率较低.

(2) 难以兼顾效率与准确性的骨干路由器地理定位[9,10]. 地理定位的准确性决定地区网络边界发现的准确性. 现有的地理定位方法均存在一定的局限性: 主动测量定位方法[11−14]准确性较高, 但代价较高且依赖于地标点的准确性和规模; 被动推测定位方法[15,16]除基于域名的定位技术外, 通常以网段为定位粒度, 对骨干路由器定位准确性较低. 不同定位方法及商业定位数据库[17,18]的定位结果一致性存在问题.

(3) 网络部署实践与测量带来的复杂性. 与 AS 边界推断方法, 如 JBR[19]、BDRmap[20]、MAP-IT[21]、bdrmapIT[22]相同, 在测量数据中, 邻居地址、第三方地址、IXP 地址等问题同样将地区网络边界发现问题复杂化.

本文以地区网络边界发现为研究目标, 以当前拓扑测量和地理定位方法为研究基础, 提出一种主被动结合的双阶段地区网络边界发现方法——RNB. 第 1 阶段以边界发现的完整性为目标, 采用基于主动定向测量与被动推测定位相结合的方法, 在探测路径中提取包含地区网络边界节点的路径片段; 第 2 阶段以边界发现的准确性为目标, 采用基于多源信息加权定位与双重 PING 定位相结合的方法, 从路径片段中根据地理信息识别地区网络边界节点. 本文在地理定位问题上的创新点在于: 通过融合尽量广泛的被动定位地理数据源, 避免单一定位方法的局限性; 通过聚焦潜在的边界片段来降低主动测量定位的代价; 利用跨国边界节点间 RTT 高于国内节点间 RTT 这一特点提高准确性. 以中国网络为实验对象, 验证该方法.

本文第 1 节阐述地区网络边界发现的研究框架, 包括模型和方案概览. 第 2 节介绍地区网络边界发现的方法, 包括两个阶段的 4 个步骤. 第 3 节重点描述实验结果, 包括完整性评价和准确性评价. 第 4 节是总结.

1 研究框架

1.1 模型与问题

地区网络边界发现问题: 互联网 IP 级网络层拓扑为一个图 T. 一个目标地区的网络拓扑为 T 的子图 R 并且 R 是连通的, 即 R 内节点间通信不需要经过 R 外节点. R 的地区网络边界为其节点子集:

$$B=\{b\mid \exists(b,v), b\in R, v\in \overline{R}\},$$

其中, (b,v)表示以 b,v 为节点的边, 子图 $\overline{R}=T-R$ 为地区外网络拓扑. 如图 1 所示, IP 级网络拓扑层拓扑 T 由 R

和 $\bar{R}$ 组成，R 由绿色节点构成，其中包括地区边界节点和地区内拓扑节点；$\bar{R}$ 由红色地区外拓扑节点构成. R 通过 B 与 $\bar{R}$ 连通. 地区网络边界发现的目的是找到 B'并追求以下指标: (1) 完整性指标 $C=|B\cap B'|/|B|$; (2) 准确性指标 $P=|B\cap B'|/|B'|$.

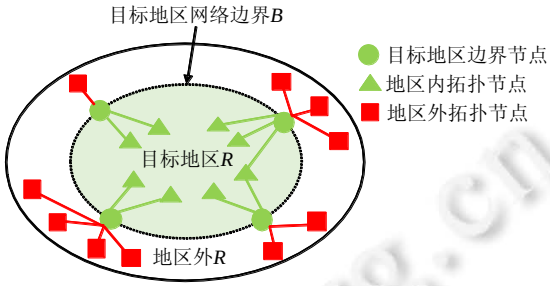

图 1　地区网络边界发现模型

1.2　方案概览

地区网络边界发现分两个阶段共 4 个步骤，如图 2 所示.

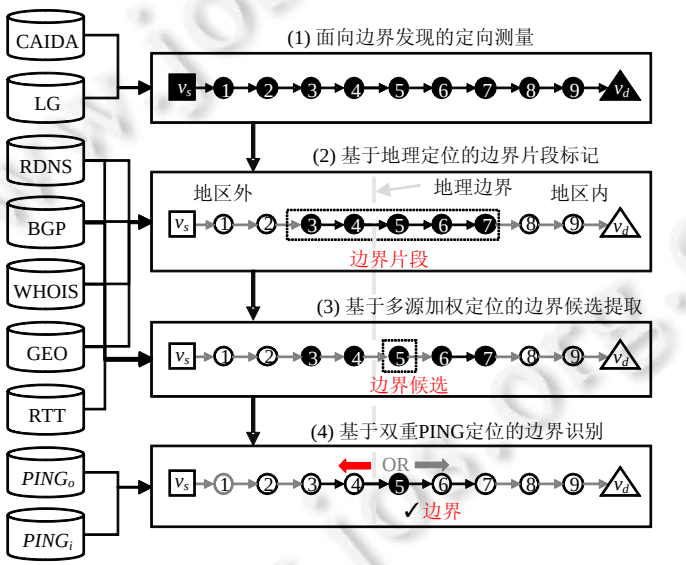

图 2　地区网络边界发现方法架构

- 阶段 1

(1) 面向边界发现的定向测量. 针对公开数据集缺乏针对性测量以及第三方开放平台效率低的问题，采用 LookingGlass 平台，有针对性地主动探测和 CAIDA 公开数据集共同建立地区网络拓扑图，从地区外探测点 v_s 对地区内探测目标 v_d 进行 traceroute 测量，详见第 2.1 节.

(2) 基于地理定位的边界片段标记. 针对主动测量定位方法代价大、花费时间久的问题，在保证完整性的前提下，采用被动推测定位方法缩小边界发现范围，基于 RDNS、BGP、WHOIS、GEODB 方法对拓扑数据进行地理定位，并提取与地区外相连接的边界片段，详见第 2.2 节.

- 阶段 2

(1) 基于多源加权定位的边界候选提取. 针对被动推测定位方法不准的问题，采用不同定位方法加权定位节点，基于 RTT、RDNS、BGP、GEODB、WHOIS 方法分别在边界片段中选择与地区外相连的节点,通过加权，将权值最大的节点作为边界候选，详见第 2.3 节.

(2) 基于双重 PING 定位的边界识别. 针对测量数据中邻居地址、第三方地址、IXP 地址问题和效率问题, 采用不同位置的测量点进行 PING 定位: 第 1 重, 基于全球多点 PING 定位边界候选和与其相连节点的位置发现边界; 第 2 重, 基于地区内多点 PING 定位检验边界的正误并修正, 详见第 2.4 节.

2 地区网络边界发现方法

2.1 面向边界发现的定向测量

定向测量的目标是: 通过选择探测点和探测目标, 使测量拓扑结果 T'尽可能完整地覆盖网络边界 B. 选择在地区外网络分布广泛的探测点对地区内地理位置和网络分布均匀的目标进行 traceroute 测量获得 T'. 一次目标可达的 traceroute 测量发现一条路径 $t=\{\{v_s,v_1,\ldots,v_b,\ldots y_d\}|v_s\in\bar{R}\ y_d\in R\}$, 其中, $\exists v_b\in B$.

从公开数据集 CAIDA 中提取中国网络拓扑, 其中, 中国香港、中国澳门和中国台湾的网络连接架构与中国内地网络不同, 为保证实验结果的严谨和可验证性, 本文以除港澳台外的中国内地网络为实验对象发现网络边界(后文中的中国网络特指中国内地的网络). CAIDA 作为网络拓扑测量平台的代表, 利用 traceroute 工具对整个 Internet 进行周期性扫描, 生成全球 IP 级拓扑数据. 从 2018 年 8 月 1 日–30 日的数据中, 提取中国网络拓扑共计 3 530 186 条路径, 其中有分布在 72 个 AS 的 92 个探测点、分布在 124 个 AS 的 74 205 个探测目标. 公开数据中特定区域拓扑数据与定向测量结果相比, 其发现的接口和链接完整性不足. 田野等人[23]基于中国互联网的独特性, 利用主要 ISP 层次结构和大量 IDC 数据中心, 仅使用 15 个探测点对中国网络进行拓扑测量, 与 iPlane 数据相比, 发现更多的接口和链接.

为进一步提高测量的完整性, 在 2018 年 10 月 19 日–2018 年 11 月 2 日, 在 LookingGlass 平台选择分布在 297 个 AS 的 983 个探测点对每个省份的每个运营商随机选择 3 个可达 IP 地址(分布在 26 个 AS 的 422 个探测目标)发起 traceroute 测量. 删除未到达探测目标和环形路径后, 获得 87 523 条路径.

2.2 基于地理定位的边界片段标记

边界片段标记的目标是: 通过被动推测定位方法, 从测量路径中提取包含网络边界 B 且节点数最少的连续片段. 采用一种地理定位方法或数据集来识别一个节点 v 是否在地区内, 可表示为一个函数 $g:v\to\{0,1,-1\}$, 其中, $\{0,1,-1\}$分别表示 v 定位在地区外、地区内或无法定位. 采用多种地理定位方法 $g_1,g_2,\ldots,g_m$ 分别对一条 traceroute 路径 $t=\{v_s,v_1,\ldots,v_b,\ldots,v_l,v_d\}$进行地理定位, 得到一个 l+2 行、m 列的矩阵 $G(t)=[g_j(v_i)]_{(l+2)\times m}$. 在 G(t)中, $\exists i\in l, j\in m$, 使 $g_j(v_i)=1$ 且 $g_j(v_{i-1})=0$, 其中, i 为符合条件的最小值, 标记节点 v_i. 当$\forall j\in m$, 使 $g_j(v_{i+2})=1$ 时, 提取边界片段为 $s=\{v_{i-2},v_{i-1},v_i,v_{i+1},v_{i+2}\}$; 否则, $\forall j\in m$, 使 $g_j(v_e)=1$, 其中, $e\in[i+2,l]$且为符合条件的最小值, 标记节点 v_e, 提取边界片段为 $s=\{v_{i-2},v_{i-1},v_i,v_{i+1},v_{i+2},\ldots,v_e\}$. 一个 e 行 m 列的边界片段矩阵 $G(s)=[g_j(v_i)]_{e\times m}$.

本文采用 RDNS、BGP、GEODB、WHOIS 被动推测定位方法定位拓扑数据. RDNS 方法通过反向解析 IP 地址的域名并提取包含的地理信息定位. DRoP[24]也采用这一方法定位. BGP 方法基于 BGP 路由数据和文献[25,26]所研究的工作实现 IP-to-AS 和 AS-to-GEO 两次映射定位. GeoCluster[27]验证了该方法可行性. WHOIS 方法通过查询 Whois 信息并提取注册者信息定位. NetGeo[28]通过查询 Whois 数据库推测主机位置信息. GEODB 方法查询 IP2Location 商业 IP 地址数据库. Gharaibeh 等人[29]评估了多种地理定位数据库在路由器定位的可靠性.

为了缩小边界发现范围, 并保留地区间连接关系, 基于被动推测定位结果在路径中标记边界片段. 被动推测定位方法均存在一定的局限性: 定位准确度不高、数据陈旧和完整性不高(例如, IP 地址无反向域名信息, 则 RDNS 方法无定位结果). 在路径中标记第 1 个与地区外相连的节点 v_i, 并提取其前后分别 2 跳节点为边界片段. 网络部署实践与测量有一定的复杂性, 可能出现位置交叉路径, 即路径中节点的位置依次为地区外-地区内-地区外-地区内的情况. 检验当 v_{i+2}的位置不是地区内时, 标记其后第 1 个所有定位方法均为地区内的节点 v_e, 边界片段为 v_i 前 2 跳节点至 v_e 的连续节点.

边界片段示例如图 3 所示, 在路径中标记 v_i 后, 取其前 2 跳邻居 v_{i-1}, v_{i-2} 和其后 2 跳邻居 v_{i+1}, v_{i+2} 或其后

邻居至 v_e 构成边界片段. 其中, (v_{i-1},v_{i-2})组成有 2 类, 节点均为地区外如 *a*, 节点为地区外和匿名跳如 *b*. $(v_{i-1}, v_{i-2},\ldots,v_e)$组成分为 3 类, 标准如 1, 含匿名跳如 2–6, 位置交叉如 5–9. 其中, *a* 和 1 组成标准边界片段, *a*, *b* 和 2–4 组成含匿名跳的边界片段, *a*, *b* 和 7–9 组成位置交叉的边界片段, *a*, *b* 和 5, 6 组成既包含匿名跳又是位置交叉的边界片段. 当含匿名跳时, 该匿名跳以定位结果为–1 标记位置. 当位置交叉时, 边界片段中存在多个与地区外直接连接的节点, 这些节点均为边界.

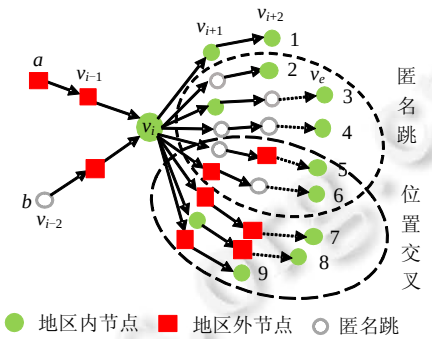

图 3 边界片段分类

在 CAIDA 和 LG 数据中, 分别提取边界片段 424 794 个和 45 095 个. 采用被动推测定位方法对 CAIDA 和 LG 拓扑数据和边界片段中 IP 地址分析见表 1: 与 LG 数据相比, IP 地址数量是 300 多倍, RDNS 条目数量是 97 倍, ASN 数量是 1.07 倍, WHOIS 数量是 25 倍, 城市数是 6 倍; 边界片段中, 片段数量约是 10 倍, IP 数量约是 3 倍, 城市数约是 2 倍, RDNS 数量、ASN 数量、WHOIS 组织数相近. CAIDA 中, 路径条数约是片段的 6 倍, 而 LG 仅约是 2 倍, CAIDA 数据存在大量冗余.

表 1 CAIDA 与 LG 拓扑测量数据分析

数据来源	路径条数	IP 数量	RDNS 数	ASN 数	WHOIS 注册者数	GEODB 城市数
CAIDA	3 530 186	3 706 679	427 703	517	32 193	3 222
LG	87 523	12 044	4 418	484	1 294	548
CAIDA_Candidate	424 794	14 374	1 373	156	712	499
LG_Candidate	45 095	5 301	1 159	181	520	261

2.3 基于多源加权定位的边界候选提取

边界候选提取的目标是, 对任意边界片段都能提取一个边界候选 v_c. 在边界片段矩阵 $G(s)=[g_j(v_i)]_{e\times m}$ 中, 每种方法 g_j 分别提取 v_i, 使 $g_j(v_i)=1$ 且 $g_j(v_{i-1})=0$. 根据权值 W_j 求和, $P(v)=\sum_j W_j g_j(v)$. 其中, $P(v)$最大时, 节点为边界候选 v_c.

分别采用 RTT、RDNS、BGP、GEODB、WHOIS 方法对边界片段中节点 IP 地址地理定位, 并提取边界. RTT 定位方法是基于时延-距离的相关性, 相邻 IP 地址间距离越远, 时延越大. 在边界片段中, 地区外与地区内相连的 IP 地址间距离应最远, 则提取时延差值最大的节点为边界. 被动推测定位方法通过查询各类数据库推测位置, 提取定位在地区内且其上一跳定位在地区外的节点为边界. RDNS 方法逐一解析 IP 地址域名, 利用域名中含有的国家或城市等信息定位; BGP、GEODB、WHOIS 方法通过 IP 地址所在网段对应的 AS 信息、地理位置信息和组织者信息提取地理信息. 在 CAIDA 和 LG 数据中, 不同定位方法提取边界的数量见表 2, 其中, RDNS 方法的完整性不高, 导致提取数量较少; RTT 方法中, 相邻 IP 地址的 RTT 值可能为负数, 且匿名跳影响导致部分边界片段无法提取边界, 并且由于时延测量误差, 同一 IP 地址可能在一片段中是边界, 在另一片段中未被提取为边界; BGP、GEODB 和 WHOIS 方法均提取边界数量较多, 以网段为定位粒度时, 可能在不同片段中将边界的邻居地址提取为边界.

表 2 各种定位方法提取边界节点数量

数据来源	RTT	RDNS	BGP	GEODB	WHOIS
CAIDA	1 887	378	2 509	2 215	2 124
LG	1 633	315	1 843	1 684	1 916

边界候选节点是单一路径通过不同方法定位数据加权获得, 而不是基于多路径信息, 避免了发现地区网络拓扑数据不完整性对边界发现的影响, 保证了方法的通用性. 采用多源加权定位方法对各种定位方法提取的边界结果分配不同权值, 在每个边界片段中, 选择权值最大的节点为边界候选节点. 如果多个节点权值相同, 则取节点序号最小的为边界候选节点. 其中, 权值分配的合理性采用两个指标评价.

(1) 边界候选节点数量反映了不同路径上边界候选的一致性, 数量越少, 一致性越高.

(2) 边界候选节点的召回率(即边界候选节点中包含的边界节点的数量除以边界候选节点总数)反映了边界候选节点提取的准确程度, 召回率越高越好.

分配权值是根据数据获取方法的可信性和 IP 地址块粒度, 采用“主动单 IP 地址优先”的加权方法, 权值从高到低分 3 档: (1) 主动测量单 IP 地址粒度, 权值为 2, 包括 RTT; (2) 被动推测单 IP 地址粒度, 权值为 1.5, 包括 RDNS; (3) 被动推测 IP 地址网段粒度, 权值为 1, 包括 BGP、GEODB 和 WHOIS.

为验证该权值分配方案的合理性, 将其与另外 3 种权值分配方案做比较: (1) 无加权, 即权值均为 1; (2) 加权比扩大, 扩大了主动测量单个 IP 地址粒度数据的权值; (3) 被动网段优先, 被动推测网段粒度数据的权值大于主动测量数据.

在不同权值分配方案下, 获得边界候选节点数量见表 3. 主动单 IP 地址优先的权值分配方法获取边界候选节点数量最小. 无加权方法提取的边界候选节点更分散, 导致节点数量增加. 另外两种方案都导致某些定位方法提取的边界节点占比过高, 在加权比扩大方法中增加了只有 RTT 方法提取地边界候选节点; 在被动网段优先方法中增加了 BGP、GEODB、WHOIS 方法提取地边界候选节点.

表 3 在不同权值分配下获得边界候选节点数量

数据来源	主动单 IP 地址优先	无加权	加权比扩大	被动网段优先
	2, 1.5, 1, 1, 1	1, 1, 1, 1, 1	3, 2, 1, 1, 1	1, 1.5, 2, 2, 2
CAIDA	1 822	2 104	1 910	2 563
LG	1 573	1 789	1 606	1 949
总数	2 147	2 551	2 580	3 293

注: 不同权值分配方案中, RTT、RDNS、BGP、GEODB、WHOIS 定位方法的权值

2.4 基于主动双重PING定位的边界识别

该步骤的目标是, 用最少的 PING 测量次数准确识别边界 v_b. 采用 PING 测量结果来识别一个节点 v 是否在地区内, 可表示为一个函数 P:$v\to\{0,1,-1\}$, 其中, $\{0,1,-1\}$分别表示 v 定位在地区外、地区内或无法定位.

第 1 重采用全球多点 PING 定位边界片段 $s=\{v_{i-2},v_{i-1},v_i,\ldots,v_e\}$中的边界候选 $P_o(v_c)$, 根据定位结果分 3 种情况识别边界 v_b':

1. $P_o(v_c)=1$ 时, 则对 v_{c-k} 进行定位, 其中, $k\in[1,c-i+2]$, 直至 $P_o(v_{c-k})=0$, 识别 $v_b'=v_{c-k+1}$.
2. $P_o(v_c)=0$ 时, 则对 v_{c+k} 进行定位, 其中, $k\in[1,e-c]$, 直至 $P_o(v_{c+k})\neq 0$, 识别 $v_b'=v_{c+k}$.
3. $P_o(v_c)=-1$ 时, 则对 v_{c-1} 和 v_{c+1} 进行定位, 如果 $P_o(v_{c-1})=0$ 且 $P_o(v_{c+1})\neq 0$, 识别 $v_b'=v_c$; 否则, 以满足情况 1、情况 2 条件继续识别.

第 2 重采用地区内多点 PING 定位 p_i 检验全球多点 PING 定位识别边界正误. 当 $P_i(v_b')=1$时, $v_b=v_b'$; 否则, 继续定位至 $P_i(v_{b+k}')=1$, 其中, $k\in(1,e-b']$, 修正边界 $v_b=v_{b+k}'$. 同时检验边界片段中 P_o 与被动推测定位方法 g_m 定位结果, 如果$\forall j\in m$, $P_o(v)\neq g_j(v)=0$ 时, 采用 P_i 再次定位.

本文采用公开平台 CA App Synthetic Monitor[30]中的 PING 工具进行全球多点 PING 定位, 其探测点数量 63 个. 采用 PingPe[31]中的 PING 工具进行地区内多点 PING 定位, 其在中国 13 个省份部署了探测点. 通过平台上多个探测点对节点 v 进行 PING 测量, 取测量时延 $d(v)$最小的探测点的位置作为 v 的位置.

PING 定位方法存在一定局限性，当测量时延 $d(v)$最小的探测点与节点 v 地理位置相近但在不同国家或地区时，导致定位错误. 采用与多种被动推测定位结果比较和重复 PING 测量的方法降低错误率. 当第 1 重全球多点 PING 定位结果与多种被动推测定位结果均不一致时，采用第 2 重地区内多点 PING 再次定位修正结果. 如图 4 所示，在边界片段中，被动推测定位方法 g_m 对节点地理定位并提取与地区外相连的节点 7 为边界候选 v_c. 第 1 重 PING 定位 $P_o(v_c)$=0 则符合情况 2，对定位 $P_o(v_8)$=−1 则识别节点 8 为边界 v_b'. 第 2 重 PING 定位检验 g_m 和 P_o 定位不一致的节点 7，重复进行定位，得到 $P_i(v_7)$=1，则修正节点 7 为边界为 v_b.

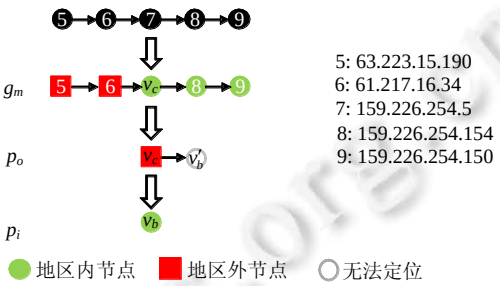

图 4 双重 PING 定位发现边界

在 CAIDA 和 LG 数据中，全球多点 PING 定位方法分别发现边界 1 245 个和 1 081 个. 地区内多点 PING 定位方法检验结果见表 4，其中，LG 比 CAIDA 新发现了 444 个边界.

表 4 采用第 2 重 PING 测量对边界发现结果检验

数据来源	中国	国外	无法定位
CAIDA	1 130	45	70
LG	940	42	99

3 实验结果

在 CAIDA 和 LG 数据中，RNB 方法分别发现边界 1 200 个和 1 039 个，其中，相同的边界有 595 个，不同的分别有 605 个和 444 个，合并去重后共计 1 644 个. 当分别采用单一定位方法发现边界片段中网络边界时，假设 RNB 方法发现边界为真，每种方法发现的召回率见表 5. RDNS 方法发现边界召回率高但发现数量少，RTT、BGP、GEO、WHOIS 方法发现正确数量多但召回率低.

表 5 单一方法发现边界结果

	RTT	RDNS	BGP	GEODB	WHOIS
发现正确	1 397	494	1 587	1 572	1 565
发现总数	2 857	548	3 206	2 946	3 347
召回率(%)	48.90	90.15	49.50	53.36	46.76

为进一步考察多源加权定位方法中权值分配方案的合理性，对最终发现边界集在不同权值分配方案所提取边界候选集上的召回率进行比较，见表 6. 召回率为边界候选节点中包含的边界节点的数量除以边界候选节点总数. 主动单 IP 地址优先方法的召回率为 70.98%，大于其他权值分配的结果，再次证明其合理性.

表 6 在不同权值分配下的边界候选节点召回率

	主动单 IP 地址优先	无加权	加权比扩大	被动网段优先
	2, 1.5, 1, 1, 1	1, 1, 1, 1, 1	3, 2, 1, 1, 1	1, 1.5, 2, 2, 2
边界候选与边界交集	1 524	1 458	1 363	1 499
召回率(%)	70.98	57.15	52.83	45.52

图 5 展示了部分中国网络边界，从 27 个国外探测点测量中国目的 IP 地址 1.192.0.1 的网络拓扑路径实例图. 利用 IP2location 商业地址库对拓扑节点定位，以不同颜色区分不同国家，其中，绿色代表中国，其他颜色

代表其他国家. 中国边界应为绿色节点, 且其左侧区域为中国节点, 右侧区域为地区外节点.在图中, 并非所有节点颜色与实际相符, 其中, 边界和左侧区域非绿色节点以及右侧区域绿色节点在商业地址定位库中定位错误. 基于此规律, 利用边界发现结果可修正 IP 地址在商业定位库中的位置信息.

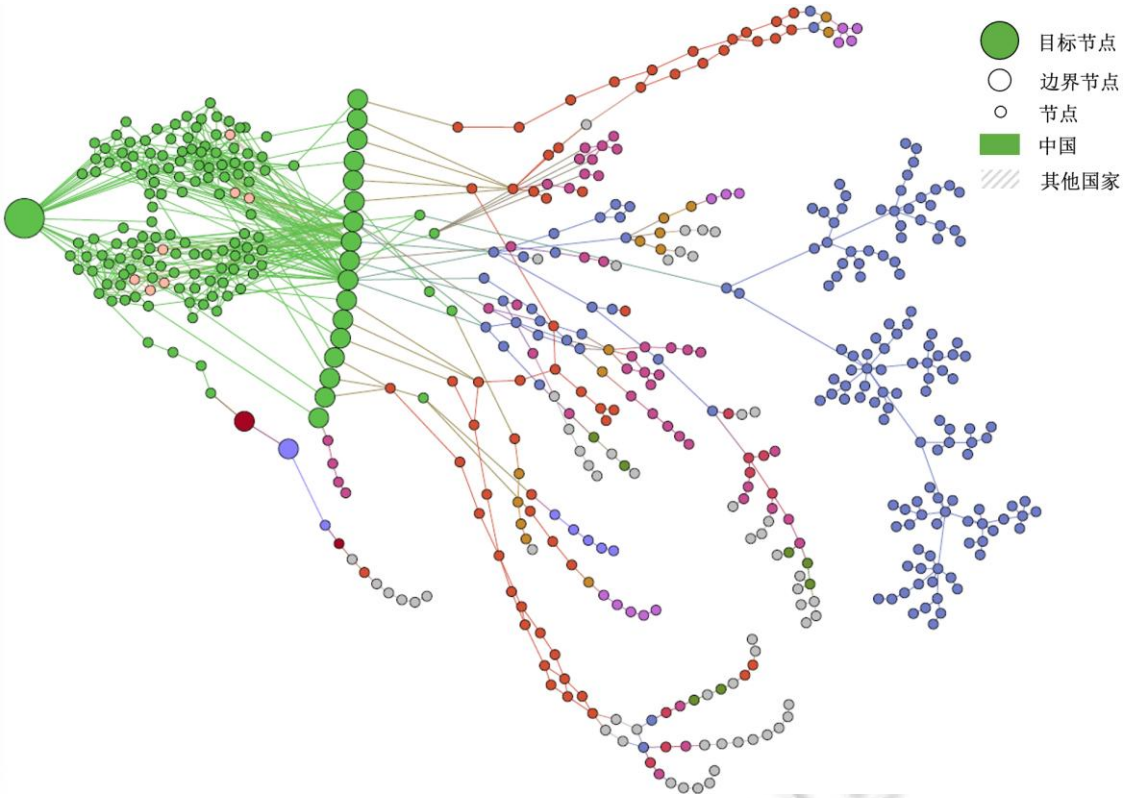

图 5 中国网络边界部分实例图

3.1 完整性评价

我们采用基于LG平台的面向边界发现的定向测量所得到的数据, 与CAIDA的公开拓扑测量数据集相比, 以不及2.5%的探测代价(87523/3530186)新发现了37.0%的边界(444/1200), 将完整率提高了27.0% (444/1644).

3.2 准确性评价

目前我们没有检索到中国网络边界的真实公开数据集. 在无法基于Groundtruth直接验证算法准确性的前提下, 采用两种方法间接验证 RNB 方法准确性. 本文提出人工验证和某运营商匿名检验方法间接评价准确性.

3.2.1 人工验证

选择对地区网络边界识别问题有初步理解的人员, 对基于 LG 平台的测量数据进行人工验证观察的数据涵盖 RTT、RDNS、BGP、GEODB、WHOIS 和双重 PING 定位的 IP 地理数据. 将包含同一边界 IP 地址的不同边界片段作为一组一起观察. 验证人员依据对地区网络边界的理解和地理信息识别边界 IP 地址. 耗时约 140 个小时, 检验 45 095 个边界片段中的 1 039 个边界 IP 地址, 人工验证与 RNB 方法发现边界一致率为 99.3%, 其中有 7 个边界 IP 地址不一致.

在人工验证中, 主要有以下几种情况, 如图 6 所示. 边界片段数据中包含多种被动推测方法 g_m, 双重 PING 测量 P_o 和 P_i 定位结果. 实例(1)中, g_m 和 P_i 定位结果相同, 验证人员以 v_5 为边界, 与 RNB 方法结果一致; 实例(2)中, g_m 和 P_i 定位 v_6 位置不同, 验证人员以 P_i 定位结果为正确, 验证 v_7 为边界, 与 RNB 方法结果一致;

实例(3)中, P_i 无法定位 v_6 和 v_7, 验证人员以 g_m 定位结果为正确, 验证 v_7 为边界, 与 RNB 方法结果不同; 实例(4)中, 边界片段的位置出现交叉情况, 验证人员认为存在两个边界 v_6 和 v_8, 验证结果之一与 RNB 方法结果一致, 为 v_8.

图 6 人工验证边界发现实例

RNB 方法在一条路径中只发现一个边界, 然而在人工检验过程中发现: 除位置交叉路径外, 在一条路径中存在多个 IP 地址被发现为边界; 同时, 这些边界分别在另外路径中仍是唯一的边界. 如图 7 所示(图中箭头连线不同代表不同路径, 图中包括 1-3-5, 2-4-7, 1-3-4-8, 2-4-3-6 路径), 节点 3、节点 4 均为边界, 在路径 1-3-5 和 2-4-7 中为唯一边界, 在路径 1-3-4-8 和 2-4-3-6 中为多边界. 这一现象可能导致边界发现不完整.

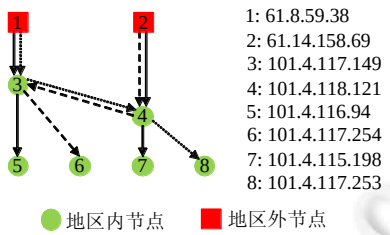

图 7 路径中出现多个网络边界节点实例

3.2.2 运营商验证

在寻求运营商验证数据时, 由于边界数据的敏感性, 仅一家移动网络运营商给予帮助. 根据 WHOIS 信息从边界数据中提取属于该运营商的 28 个边界 IP 地址, 提交该运营商验证. 该运营商给出一次实验结果的验证, 反馈一个正确的边界 IP 地址总数, 无具体的 IP 地址列表. 验证正确个数为 21, 准确率为 75%. 运营商验证的方法本身存在局限性, 其潜在原因包括两点.

(1) 网络拓扑变化: 验证时间 2019 年 4 月, 与测量时间间隔 6 个月, 网络边界可能变化.

(2) 对边界概念理解的差异: 运营商验证人员理解的中国网络边界与本文有出入.

在未来的工作中, 将与更多运营商进一步合作, 提高验证质量, 最终改进地区网络边界方法.

4 总 结

本文构建了地区网络边界发现模型, 采用地理位置信息将 IP 级网络拓扑区分为地区内和地区外, 从而提出了一种地区网络边界发现的方法——RNB. 在针对中国网络的实验中, 以 CAIDA 和 LG 平台获得的定向拓扑数据保证了方法的完整性, 以被动推测的地理定位方法获得边界片段保证了方法的高效性, 以主动测量的定位方法发现边界保证了方法的准确性.

References:

[1] Zhang Y, Fang BX, Zhang HL. Chinese IP-level network topology measurement and analysis. Journal of Communications, 2007, 28(12): 96−101 (in Chinese with English abstract). [doi: 10.3321/j.issn:1000-436x.2007.12.016]

[2] Zhang Y, Zhang HL, Fang BX. A survey on Internet topology modeling. Ruan Jian Xue Bao/Journal of Software, 2004, 15(8): 1220−1226 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15/1220.htm

[3] Zhang HL, Fang BX, Hu MZ, Jiang Y, Zhan CY, Zhang SF. A survey on Internet measurement and analysis. Ruan Jian Xue Bao/Journal of Software, 2003, 14(1): 110−116 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/110.htm

[4] Dainotti A. Mapkit: Investigating the susceptibility of the Internet topology to country-level connectivity disruption and manipulation. 2017. https://www.caida.org/funding/satc-mapkit/satc-mapkit_proposal.xml

[5] Raman RS, Stoll A, Dalek J, Dalek J, Sarabi A, Ramesh R, Scott W, Ensafi R. Measuring the deployment of network censorship filters at global scale. In: Proc. of the Network and Distributed System Security. 2020. https://dx.doi.org/10.14722/ndss.2020.23099

[6] Poese I, Uhlig S, Gueye B. IP geolocation databases: Unreliable? ACM SIGCOMM Computer Communication Review, 2011, 41(2): 53−56. [doi: 10.1145/1971162.1971171]

[7] CAIDA. Macroscopic topology measurements project and the archipelago measurement infrastructure. 2006. https://www.caida.org/projects/macroscopic/

[8] Giotsas V, Dhamdhere A, Claffy KC. Periscope: Unifying looking glass querying. In: Proc. of the Passive and Active Network Measurement Conf. Workshop. 2016. 177−189.

[9] Wang ZF, Feng J, Xing CY, Zhang GM, Xu B. Research on the IP geolocation technology. Ruan Jian Xue Bao/Journal of Software, 2014, 25(7): 1527−1540 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4621.htm [doi: 10.13328/j.cnki.jos.004621]

[10] Zhu JY, Zhang Y, Zeng LW, Yu ZX, Zhang HL. Geolocation for multi-interface routers. Journal of Cyber Security, 2018, 3(4): 15−24 (in Chinese with English abstract). [doi: 10.19363/J.cnki.cn10-1380/tn.2018.07.02]

[11] Katz-Bassett E, John JP, Krishnamurthy A, Wetheerall D. Towards IP geolocation using delay and topology measurements. In: Proc. of the Internet Measurement Conf. 2006. 71−84.

[12] Gueye B, Ziviani A, Crovella M, Fdida S. Constraint-based geolocation of Internet hosts. IEEE/ACM Trans. on Networking, 2006, 14(6): 1219−1232. [doi: 10.1109/TNET.2006.886332]

[13] Wong B, Stoyanov I, Sirer EG. Octant: A comprehensive framework for the geolocalization of Internet hosts. In: Proc. of the Networked Systems Design & Implementation. USENIX Association, 2007. 313−326.

[14] Dong Z, Perera RDW, Chandramouli R, Subbalakshmi KP. Network measurement based modeling and optimization for IP geolocation. Computer Networks the Int'l Journal of Computer & Telecommunications Networking, 2011, 56(1): 85−98. [doi: 10.1016/j.comnet.2011.08.011]

[15] Vixie VD, Goodwin P, Dickinson T. A Means for Expressing Location Information in the Domain Name System. RFC1876, IERF, 1996.

[16] Chabarek J, Barford P. What's in a name? Decoding router interface names. In: Proc. of the Hotplanet, ACM Workshop. 2013. 3−8.

[17] MaxMind. https://www.maxmind.com

[18] IP2Location. https://www.ip2location.com/

[19] Wei ZH, Chen M, Zhao HH, Ji L. Deducing AS borders from IP path information. Ruan Jian Xue Bao/Journal of Software, 2010, 21(9): 2387−2394 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3741.htm [doi: 10.3724/SP.J.1001.2010.03741]

[20] Luckie M, Dhamdhere A, Huffaker B, Clark D, Claffy KC. BDRmap: Inference of borders between IP networks. In: Proc. of the Internet Measurement Conf. 2016. 381−396.

[21] Marder A, Smith JM. MAP-IT: Multipass accurate passive inferences from traceroute. In: Proc. of the Internet Measurement Conf. 2016. 397−411.

[22] Marder A, Luckie M, Dhamdhere A, Huffaker B, Claffy KC, Smith JM. Pushing the boundaries with BDRmapIT: Mapping router ownership at Internet scale. In: Proc. of the Internet Measurement Conf. 2018. 56−69.

[23] Ye T, Dey R, Liu Y, Ross KW. Topology mapping and geolocating for China's Internet. IEEE Trans. on Parallel & Distributed Systems, 2012, 24(9): 1908−1917. [doi: 10.1109/TPDS.2012.271].

[24] Huffaker B, Fomenkov M, Claffy K. DRoP: DNS-based router positioning. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 5−13. [doi: 10.1145/2656877.2656879]

[25] CIDR report. http://www.cidr-report.org/as2.0/

[26] Freedman MJ, Vutukuru M, Feamster N, Balakrishnan H. Geographic locality of IP prefixes. In: Proc. of the Internet Measurement Conf. 2005.

[27] Padmanabhan VN, Subramanian L. An investigation of geographic mapping techniques for Internet hosts. ACM SIGCOMM Computer Communication Review, 2001, 31(4): 173−185. [doi: 10.1145/964723.383073]

[28] Moore D, Periakaruppan R, Donohoe J, Claff K. Where in the world is netgeo.caida.org? In: Proc. of the Int'l Networking Conf. 2000.

[29] Gharaibeh M, Shah A, Huffaker B, Zhang H, Ensafi R, Papadopoulos C. A look at router geolocation in public and commercial databases. In: Proc. of the Internet Measurement Conf. 2017. 463−469.

[30] CA app synthetic monitor. https://asm.ca.com

[31] PingPe. http://ping.pe/

附中文参考文献:

[1] 张宇, 方滨兴, 张宏莉. 中国 IP 级网络拓扑测量与分析. 通信学报, 2007, 28(12): 96−101. [doi: 10.3321/j.issn:1000-436x.2007.12.016]

[2] 张宇, 张宏莉, 方滨兴. Internet 拓扑建模综述. 软件学报, 2004, 15(8): 1220−1226. http://www.jos.org.cn/1000-9825/15/1220.htm

[3] 张宏莉, 方滨兴, 胡铭曾, 姜誉, 詹春燕, 张树峰. Internet 测量与分析综述. 软件学报, 2003, 14(1): 110−116. http://www.jos.org.cn/1000-9825/14/110.htm

[9] 王占丰, 冯径, 邢长友, 张国敏, 许博. IP 定位技术的研究. 软件学报, 2014, 25(7): 1527−1540. http://www.jos.org.cn/1000-9825/4621.htm [doi: 10.13328/j.cnki.jos.004621]

[10] 朱金玉, 张宇, 曾良伟, 余卓勋, 张宏莉. 一种多接口路由器地理定位方法. 信息安全学报, 2018, 3(4): 15−24. [doi: 10.19363/J.cnki.cn10-1380/tn.2018.07.02]

[19] 魏镇韩, 陈鸣, 赵洪华, 吉梁. 从 IP 路径信息中推导 AS 边界. 软件学报, 2010, 21(9): 2387−2394. http://www.jos.org.cn/1000-9825/3741.htm [doi: 10.3724/SP.J.1001.2010.03741]

朱金玉(1993－), 女, 博士生, 主要研究领域为互联网关键资源安全, IP 地理定位.

张宇(1979－), 男, 博士, 副教授, CCF 高级会员, 主要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.

曾良伟(1995－), 男, 硕士, 主要研究领域为互联网关键资源安全.

张宏莉(1973－), 女, 博士, 教授, 博士生导师, CCF 专业会员, 主要研究领域为网络安全, 网络测量和网络计算.

方滨兴(1960－), 男, 博士, 教授, 博士生导师, CCF 会士, 主要研究领域为网络信息安全, 信息内容安全.