别名解析技术研究进展

王占丰[1]，程光[2]，胡超[3]，李晗[4]，翁年凤[5]，曹华平[4]

（1. 东南大学计算机科学与工程学院，江苏 南京 211189；2. 东南大学网络空间安全学院，江苏 南京 211189；
3. 解放军陆军工程大学指挥控制工程学院，江苏 南京 210007；4. 国家计算机网络应急技术处理协调中心，北京 100020；
5. 南京电讯技术研究所, 江苏 南京 210007）

摘 要：别名解析是发现位于同一台路由器上不同 IP 接口的技术，是网络拓扑推断的一个关键步骤，将因特网的逻辑拓扑转换为物理拓扑从而实现虚拟空间与现实世界映射重要方法。首先介绍了 IP 别名解析的概念，分析了 IP 别名关系的种类，然后对 IPv4 和 IPv6 的别名解析算法分别进行了详细论述，最后通过对所有算法的综合分析和对比，指出了在未来的研究中，特别是 IPv6 别名解析中，在别名目标集合筛选、指纹选择及推断方法中应注意的问题。

关键词：网络空间；测量；IP 别名解析；拓扑

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2019134

Research on the IP alias resolution technology

WANG Zhanfeng[1], CHENG Guang[2], HU Chao[3], LI Han[4], WENG Nianfeng[5], CAO Huaping[4]

1. School of Computer Science and Engineering, Southeast University, Nanjing 211189, China
2. College of Cyberspace Security, Southeast University, Nanjing 211189, China
3. College of Comannd Control Engineering, Army Engineering University of PLA, Nanjing 210007, China
4. National Computer Network Emergency Response Technique Team, Coordination Center of China, Beijing 100020, China
5. Nanjing Telecommunication Technology Research Institute, Nanjing 210007, China

Abstract: IP alias resolution, the procedure of identifying IP addresses belonging to the same router, is a critical step in Internet topology inference. It can convert the Internet logical topology into physical topology, and bridge the gap between the virtual world and real world. First the concept of IP alias resolution was introduced and the classical IP alias relationships were analyzed. Then the IPv4 alias resolution algorithms and the IPv6 alias resolution algorithms were discussed in detail separately. Finally, through the comprehensive analysis and comparison of all the algorithms, the research directions in the future especially in IPv6 alias resolution were pointed out in three folds such as alias target set selection, fingerprint selection and inference methods.

Key words: network space, measurement, IP alias resolution, topology

1 引言

当前，互联网已成为人类社会的基础设施，政治、经济、文化、科技、教育等无不因为互联网的出现而发生深刻革命[1]。伴随着接入技术的持续进步和硬件成本不断下降，网络深入到人类世界的任意角落，万物互联已成为现实。为了更好地使用和管控网络，人们迫切地希望了解网络拓扑结构[2-4]，

收稿日期：2018–09–07；**修回日期：**2019–05–05

通信作者：曹华平，caohuaping@cert.org.cn

基金项目：国家重点研发计划基金资助项目（No.2017YFB0801703）；国家自然科学基金资助项目（No.61602114）；赛尔网络下一代互联网技术创新基金资助项目（No.NGII20170406）；东南大学博士后创新人才培养资助基金资助项目（No.2242019R20024）

Foundation Items: The National Key Research and Development Program of China (No.2017YFB0801703), The National Natural Science Foundation of China (No.61602114), CERNET Innovation Project (No.NGII20170406), Foundation for Training Postdoctoral Innovative Talents in Southeast University (No.2242019R20024)

网络空间测绘与态势感知成为一个炙手可热的领域[5-9]，国内外一些知名企业纷纷开展相关研究，建立了许多态势感知平台和知识库，如 Zoomeye、Censys、Shodan、FOFA 等。

在网络态势分析中，只有将测量获得的逻辑拓扑与物理拓扑进行映射，才能将观测到的网络事件与网络设备进行关联[10-19]，这就需要采用别名解析技术。具体来说，别名解析技术就是从网络测量结果中找出属于同一设备的 IP 地址集合，该项技术广泛应用于路由器级拓扑发现、跟踪溯源和态势分析中。别名解析在 2000 年左右曾受到广泛关注，先后有 Mercator、iffinder、Ally 等著名的测量工具和平台被提出，但这些测量工具和平台存在测量开销较大和使用范围有限的问题[20-24]。由于 IPv4 地址在 2016 年已经耗尽，世界各国都在加紧推进 IPv6 网络的建设。由于 IPv4 和 IPv6 相互不兼容，针对 IPv4 的别名解析技术无法完全适应新的网络架构，从而涌现出一批新的研究成果。为了对别名解析技术形成较为全面的了解，通过 EI、SCI、知网、万方等文献检索工具对别名解析（alias resolution）、别名、IPID、时间戳等关键词的相关论文进行了检索。在论文检索过程中，以相关文献综述及重要的算法入手，并将所涉及的相关文献进行了拓展阅读，检索内容覆盖了国内外主要研究团队的最新成果。

别名解析方法从原理上大体分为基于测量的别名解析算法、基于推断的别名解析算法和综合方法 3 类。基于测量的别名解析算法向不同的 IP 地址发送探测分组，通过分析响应分组的内容或特征来判定 2 个或多个 IP 是否属于同一台路由器。基于推断的别名解析算法通过构建 IP 拓扑或 IP 接口名称来推断不同的 IP 地址是否属于同一台路由器。基于测量的别名解析方法更为准确，但是对于不响应测量或者响应不完整的网络设备，基于推断的别名解析算法也是一种补充。因此，综合方法是将几种别名解析方法组合起来从而进行更为全面和准确的判别[25]的一种方法。从技术发展过程看，别名解析方法逐渐从 IPv4 网络发展到 IPv6 网络，从小范围的网络扩展到整个 IP 地址空间。

2 IP 别名解析概述

2.1 典型的别名关系

路由器一般有多个接口，每个接口配有不同的 IP 地址，如果用一个接口的 IP 地址代表该路由器，则其他接口的 IP 地址称为别名[25]。别名关系推断是网络测量中的一个难题，该问题最早由 Pansiot 等[26]提出。如图 1(a)所示，2 个测量点 S_1 和 S_2 测量到目的主机 D 的路径时，得到的 IP 路径分别为 $S_1\rightarrow\cdots\rightarrow R_1^{\,1}\rightarrow R'^{\,1}_3\rightarrow R_4^{\,1}\rightarrow\cdots\rightarrow$D 和 $S_2\rightarrow\cdots\rightarrow R_2^{\,1}\rightarrow R_3^{\,1}\rightarrow R_4^{\,1}\rightarrow\cdots\rightarrow$D。如果不能推断路由器 R'_3 和路由器 R_3 为同一台路由器，则会得到图 1(b)所示的拓扑结构。图 1 中 $R_i^j\,(i=1,2,3,4,\ j=1,2,3)$ 表示路由器的接口。

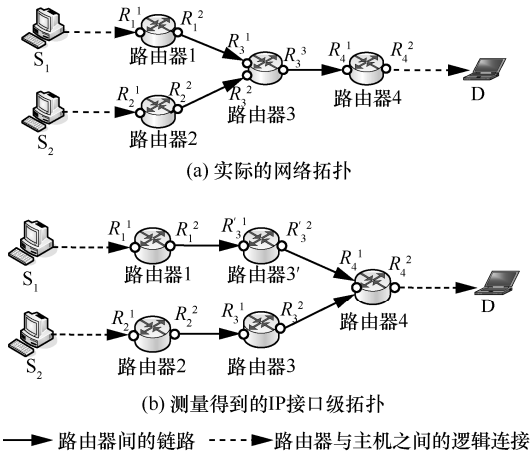


图 1 IP 别名关系示意

文献[27]将所有的 IP 别名关系分为 3 种情况。

1) 对称路由别名关系。从不同方向测量 2 条路径，如果在网络中 2 个 IP 处于对称位置，如图 2 中的接口 IP_{1y} 和 IP_{2y}、IP_{1z} 和 IP_{2z} 属于同一台路由器，且互为别名，这种互为别名的 IP 往往具有相同的 30 bit 网络标识。

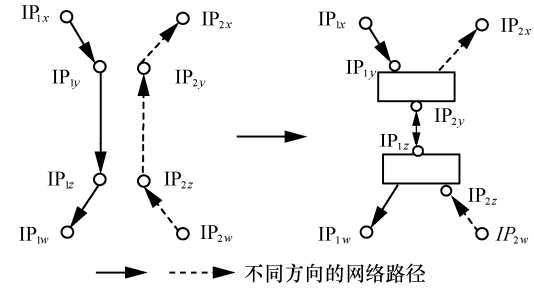


图 2 IP 路径中存在对称路段的别名关系

2) 相同后继别名关系。若测量发现的 IP 逻辑链路<IP_x，IP_y>和<IP_w，IP_y>具有相同的后继节点，则 IP_x 和 IP_w 互为别名，这种情况又称为三角别名，如图 3 所示。

3) 平行路径别名关系。如图 4 中的 2 条路径 L_1=$IP_{1x}\rightarrow\cdots\rightarrow IP_{1y}\rightarrow\cdots\rightarrow IP_{1z}$，$L_2$=$IP_{2x}\rightarrow\cdots\rightarrow IP_{2y}\rightarrow\cdots$

→IP_{2z}，若 IP_{1y} 和 IP_{2y} 属于同一台路由器，则这种情况称为平行别名。这种情况出现在从同一个方向进行探测，出现负载均衡，或者由不同的路由器策略造成。

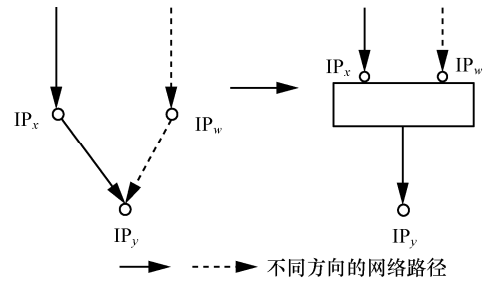


图 3　IP 路径中具有相同后继的别名关系

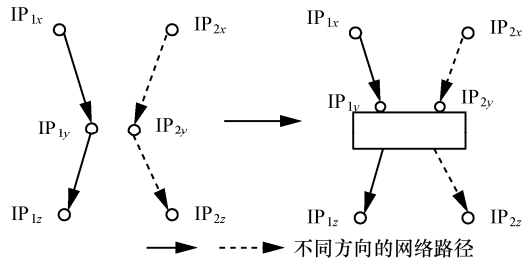


图 4　平行路径别名关系

2.2　别名解析基本思路

目前，别名解析算法已达 20 余种，然而从别名解析过程来看，所有别名解析算法主要分为 3 个环节：1) 别名集合筛选，2) 数据探测与分析，3) 别名判定，如图 5 所示。

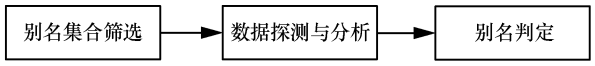


图 5　别名解析算法的一般流程

别名集合筛选主要指将那些可能互为别名的 IP 地址集从探测目标网络中过滤出来，从而减小搜索范围，也称为别名过滤技术[27-28]。这种别名过滤往往是通过分析潜在的别名关系或者 RFC 文档中关于路由器接口的分配规范来完成的，如 Palmtree 等算法在探测的目标集合构建时就考虑如何采用先验知识来减少测量开销。

数据探测与分析主要依据别名判定的原理进行数据测量与分析，如基于测量的别名解析算法通过测量获取的响应分组的 IPID[23]、路径信息[29]、时间戳[30]等信息，而基于推断的别名解析算法则分析网络的路径关系[31]和拓扑[32]来为别名判定做准备。

别名判定则是确定 2 个或多个 IP 是否为别名，主要依据是 RFC 文档或者路由器的配置规范。伴随着人工智能技术的发展和大数据技术的流行，一些基于机器学习的算法也逐步得到了应用，如 TreeNet 采用决策树的思想来进行别名关系的判定[25]；DisCarte 算法采用析取逻辑规划来进行别名判定[33]，AliasCluster 算法采用贝叶斯网络推断模型与链式推理逻辑来进行别名判定[34]。

某些别名解析算法对上述 3 个环节进行了简化，如 Mercator[20]、iffinder[21]、Passenger[29]、DisCarte[33]、Pamplona-traceroute[35]等算法将前 2 个环节合并为一个步骤，即从探测数据中获取可能的别名集合。本文将别名解析算法分为 IPv4 别名解析和 IPv6 别名解析两大类，再分别将两类算法进行细分，对典型算法的原理进行阐述。

3　IPv4 别名解析技术

3.1　基于测量的别名解析方法

3.1.1　基于同源地址的别名解析算法

基于同源地址的别名解析算法是最早的一类别名解析方法，由 Pansiot 等[26]提出，在网络拓扑测量工具 Mercator[20]及别名解析工具 iffinder[21]中均采用了该方法。这种方法通过主动探测来解析 IP 地址别名。根据 RFC1393[36]，向一个 IP 地址发送一个具有较高端口号、TTL 为 255 的分组，如果返回的“端口不可达”ICMP 分组源地址与目的地址不同，则说明该地址与被探测的目标地址是同一台路由器上的 2 个别名，如图 6 所示。对于 2 个可能互为别名的 IP 地址，若响应分组的原地址相同，也说明这 2 个 IP 地址互为别名。

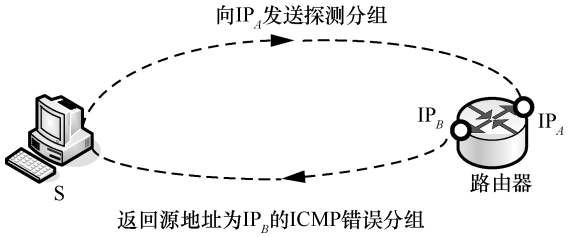


图 6　基于同源地址的别名解析算法原理示意

这种别名解析方法的优点在于不会产生误判，缺点是会受到路由器配置的影响，发现别名的完整性不高。在不考虑网络拥塞的情况下，当出现以下 2 种情况时，该算法无法发现别名[21]：1) 如果路由器被配置为“采用收到分组的目的地址作为响应分组的源地址”，那么通过响应分组将无法发现别名；2) 路由器不响应高端口的 ICMP 测量，据统计网络中约有 10%的核心路由器从来不响应未知

高端口的探测分组。

为了提高 IP 别名的识别率，使用该技术时可以通过以下 3 个方面进行优化[20-21]：

1) 可对同一个接口重复发送多个探测分组，因为不同时刻的响应分组会有所不同；

2) 改变分组的封装方式，因为不同系统在探测时返回的结果会有所不同；

3) 从不同的地理位置发起测量，因路由策略不同，从不同位置发起的探测响应情况会有所不同。

基于同源地址的别名解析算法虽然是为 IPv4 网络而设计，但是经改进后可以适用于 IPv6 网络中，适用的范围较广且准确度高。

3.1.2 基于 IPID 的别名解析算法

基于 IPID 的别名解析算法主要通过 IP 分组的标识变化来进行别名关系判别。在网络中，IP 分组是通过分组首部的标识字段（简称 IPID）来区别的，IPID 可以标识不同 IP 分组的多个分片从而进行重装。每个路由器都具有一个全局的计数器，每发送一个 IP 数据分组，IPID 加 1，全局计数器为路由器的多个网络接口所共享。由于 IPID 的值是单调递增的，那么由同一台路由器发出的连续分组应具有连续的 IPID 值，据此原理，当对同一台路由器的不同 IP 地址发送探测分组时，则返回分组的 IPID 值应该是连续或者相近的。这种方法不受路由器返回分组配置策略的影响。

1) Ally 算法

文献[23]在网络测量系统 Rocketfuel 中提出了基于 IPID 值进行别名解析的工具 Ally。Ally 是在 Mercator 的基础上提出的，该算法同时综合基于相同源地址的技术，分析路由器选择的 TTL 初始值及路由器对速率限制(rate limiting)情形来对别名关系进行判别。图 7 给出了 Ally 中使用 IPID 进行别名解析的基本过程。首先，对 2 个候选 IP 地址先后发送 2 个探测分组，从响应分组中获取的 IPID 分别为 x 和 y。然后，对上述 2 个 IP 再发送 2 个探测分组，获得的响应分组的 IPID 分别为 w 和 z。若返回的 IPID 满足关系 $x<y<w<z$，且 w 与 x 的值十分接近，则说明 2 个 IP 互为别名。在实际网络中，考虑分组的乱序等因素，只要 x 与 y 之差小于一定的阈值，仍可以认为 2 个 IP 为别名关系。Ally 算法受阈值的影响较大，一般阈值设置为 200，可以根据发送分组间隔长短进行调整。文献[23]的实验证实了这种技术存在错判和解析不完全的问题。同时，这种技术还有一个缺点，即效率比较低，需要 $O(n^2)$ 次的成对测试，在慢速网络和不响应的路由器较多的情况下，别名解析的耗时会很长。

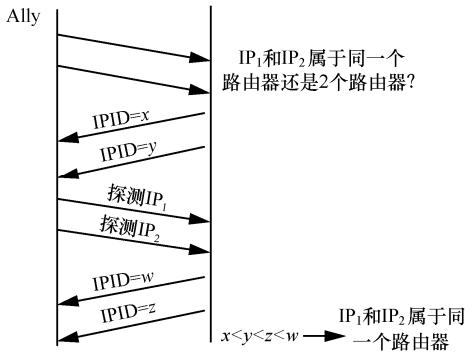


图 7 Ally 别名判别的原理

为了提高别名解析的效率，文献[23]对别名解析的范围采用启发式算法进行了限定：一是采用 DNS 系统中的层次化命名，对高度相似的域名进行别名判定，如 chi-sea-oc12.chicago.isp.net 与 chi-sfo-oc48.chicago.isp.net；二是对于返回的 TTL 值较为接近的 IP 进行别名关系判定；三是利用别名的传递关系进行判定，如若 IP_1 与 IP_2 互为别名，IP_2 与 IP_3 互为别名，则说明 IP_1 与 IP_3 互为别名。

Ally 算法的不足之处在于容易受到网络性能影响，从而导致分组乱序，其应用范围受到路由器是否采用共享 IPID 计数器的制约。

2) RadarGun 算法

Bender 等[37]发现共享一个 IPID 计数器的 2 个 IP 接口，在相近时间段内其响应分组的变化趋势十分接近，从而提出了算法 RadarGun。该算法不再对 IPID 值的连续性进行比较，而是为每个 IP 进行一组探测，分析不同 IP 响应结果构成的 IPID 时间序列变化趋势的近似性。若变化趋势一致，则认为 2 个 IP 互为别名，否则不是别名关系，如图 8 所示。RadarGun 具体做法如下。

① 首先，对于 n 个待判别的 IP 接口，不是针对每 2 个进行测量，而是针对每个 IP 进行一个序列的探测，从而得到不同的 IPID 序列。设存在 3 个 IP 地址 IP_a、IP_b、P_c，RadarGun 依次对 3 个 IP 进行测量，返回的 IPID 序列如下：A_1, B_1, C_1, A_2, B_2, C_2, …。如此，针对每个 IP 得到一个 IPID 序列，以 IP_a 为例，表示为 $\{t_i, A_i\}$，其中，t_i 表示第 i 时刻，A_i 表示第 i 时刻的 IPID，$0<i<N$，N 表示测量的次数。

② 为了保证算法的有效性，RadarGun 会过

滤一些无效的序列，如不响应的分组超过整个序列 25%的、IPID 为 0 或常数的、IPID 为非线性序列的[37]等序列。

③ 对任意 2 个有效的序列引入采样距离函数进行检验，具体如下。

对于任意 2 个序列$\{t_i, A_i\}$、$\{t_j, B_j\}$，若 $t_{A,i}<t_{B,j}<t_{A,i+1}$，采用线性插值法获得序列$\{t_i, A_i\}$在 $t_{B,j}$ 时刻的 IPID 估值 $\mathrm{ID}_{A,\mathrm{est}}$，然后计算 $\mathrm{ID}_{B,j}$ 与估值的距离 $\delta_{B,j}=|\mathrm{ID}_{A,\mathrm{est}}-\mathrm{ID}_{B,j}|$，采用同样的方法计算 $\delta_{A,j}$，最后计算 2 个序列的平均距离，如式(1)所示。

$$\Delta_{A,B}=\frac{\sum_i \delta_{A,i}+\sum_j \delta_{B,i}}{|A|+|B|} \tag{1}$$

④ 判别 2 个 IP 地址是否为别名。如果 $\Delta_{A,B}<200$，则 2 个 IP 互为别名；如果 $\Delta_{A,B}>1\,000$，则不是别名关系；如果 $200\leqslant\Delta_{A,B}\leqslant1\,000$，则需要进一步分析。

RadarGun 虽然能够解决分组乱序所带来的问题，然而该算法仍然是基于阈值的，仍会受到网络性能等因素的影响。

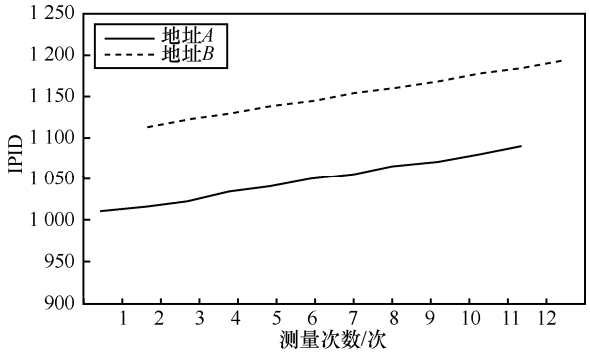


图 8　RadarGun 别名判别的原理

3) MIDAR

Ally 和 RadarGun 虽然在一定程度上能够提高别名的解析效率，但是要对整个 IP 地址空间或者大量 IP 地址进行解析，则需要做进一步优化。Keys 等[38]对 Ally 和 RadarGun 算法从 2 个方面进行了改进：① 如何对目标集进行测量，并对所有的 $O(N^2)$个别名关系进行判别；② 如何降低假阳率以提高别名解析的正确性。MIDAR（monotonic ID-based alias resolution tool）通过优化采样间隔，引入单调边界检验函数（MBT, the monotonic bounds test），采用多种探测方法来提高响应率，提出多个测量点协助测量及通过滑动平均窗口来提高算法的扩展性。

MIDAR 的工作原理较为复杂，实际上是一个复杂的别名解析系统，适用于大型网络测量平台及大规模的别名解析，总体分为 5 个阶段。

① 估计阶段（estimation stage）

估算阶段主要解决 2 个问题：一是对不同的目标主机选择合适的测量方法；二是确定采样时间间隔。测量时将所有待定的 IP 地址集合平均地分配到所有的测量点上，对每个目标 IP 采用所有的方法进行尝试。

② 发现阶段（discovery stage）

发现阶段主要判断 IP 地址是否采用同一个 IPID 计数器。根据估计阶段确定的测量速度来确定测量的滑动窗口，并采用最佳的测量方法对所有 IP 发起测量，对所有交叠时间序列进行检测。检测采用前文所述的 MBT 算法。

③ 消除阶段（elimination stage）

对可能是别名关系的 IP 地址对重复使用 MBT 函数计算从而减少假阳率。为了进一步减少探测分组，将所有的 IP 构建在一棵拓扑树上，对所有划分在同一棵子树的 IP 别名对进行探测，每棵子树探测 10 次，其中，每棵子树的间隔不超过整个树空间距离的 5%。实验表明这种探测仅多使用 15%的流量。

④ 验证阶段（corroboration stage）

验证阶段采用消除阶段的方法对所有的 IP 进行探测，但所验证的 IP 地址仅是消除阶段不能确定别名关系的 IP 地址集，因此输入集合更小。

⑤ 别名推断阶段（final alias inference）

前 3 个阶段对 IP 地址对进行了筛选，验证阶段仅对位于同一棵子树上的 IP 接口进行别名检验，而别名推断阶段将对所有别名的关系进行分析从而进行综合判定。如 *A* 和 *B* 互为别名，*B* 和 *C* 也互为别名，然而判定出 *A* 和 *C* 不是别名关系，则说明判定中存在误判，将这些可能存在误判的别名从集合中移除。

4) Pamplona-traceroute

基于 IPID 的别名解析算法研究分为 2 个方面，一方面是不断提高算法精度，另一方面是在控制预测精度的情况下，通过减少测量开销，提高算法效率。Pamplona-traceroute 在上述 2 个方面进行了尝试，将测量与推断隐含于 traceroute 测量过程，基于 IPID 的间隔和变化规律来进行别名关系推断[35]，具体分为 3 个阶段。

第一阶段进行测量，通过分析获取响应的 IP 地址、TTL、响应分组的 IPID 和响应分组的时间戳。该算法

支持 UDP、TCP 和 ICMP 等 3 种不同类型的探测，为了避免负载均衡的影响采用了成对的探测分组。

第二阶段将所有测量数据发送到一个测量服务器，从这些数据中筛选出采用共享 IPID 计数器的路由器。

第三阶段进行别名解析，将所有的分组中时间戳较为接近的 IP 地址对按照类似于 Ally 的方式进行分析，如 IPID 必须是单调增加的、IPID 必须小于一定的阈值、分组的时延小于一定的阈值等。

Pamplona-traceroute 算法将拓扑测量与别名解析进行了融合，并通过对 traceroute 进行了改造，从实验对比结果看该算法精度高于其他算法。但是该算法需要大规模的测量设施并需要节点间的协调，因此在实施过程中存在一定的困难。

相比基于相同源地址的别名判别算法，基于 IPID 的别名判别算法可以提高别名解析的完整性，同时具有较高准确度，但同样存在着漏判和误判的不足，主要原因如下：① 算法中阈值的选择受到网络性能和设备特征的影响，此外探测分组在中间路由器重新排队等因素都会对该阈值产生影响，如果阈值设置太大，解析的结果就会存在假阳，反之，就会漏报；② 一些路由器会将路由器的计数器设置为 0 或者不使用计数器，这种情况下此类算法失效；③ 有些路由器共享一个计数器但是为每个接口单独计数，这样互为别名的 2 个接口之间的 IPID 值就不再接近了；④ 存在与探测源跳数相同的 2 个不同路由器具有相近的 IPID 值的情况，虽然这种情形的概率很小。

3.1.3 基于时间戳字段的别名解析算法

IP 协议中包含一个预定义 IP 时间戳选项，启用此选项后，若分组经过路由器的 IP 包含在预定义 IP 地址集中，则该路由器会在分组中添加自己的时间戳。使用该选项时，预定义 IP 数不能超过 4 个，而且路由器会按照预先定义的次序逐一进行标记。据此可知，如果 2 个 IP 互为别名，所添加的时间戳应该相同。根据上述发现，Sherry 等[30]提出了一种基于时间戳的别名解析算法 Timestamp。

Timestamp 算法分为 4 步：首先向所有可能为别名的 IP 发送分组($A|AXXX$)排除那些会增加额外时间戳的分组，其中 X 表示一个不会出现在测量路径上的 IP 地址；然后针对可能互为别名的 2 个 IP 地址 A 和 B，从不同的测量点发送 2 个探测分组($A|ABAB$)和($B|BABA$)，每个探测点测量 5 次；所有出现 4 次时间戳的 IP 地址为别名。对出现 2 次时间戳的 2 个 IP 进行时钟测试，要求时间戳单调非减而且 90%的时间戳都是相同的，通过时钟测试后再判定其是否为循环路径，从而判定其是否为别名。

由于 Timestamp 采用了 ICMP 协议，而 ICMP 的端口不可达会引发错误直接插入探测载荷中，再发回测量主机。Marchetta 等[39]提出的 Pythia 算法采用 UDP 协议来构建分组，同时在一个测量过程中引入多个别名 IP，从而减小测量开销。Pythia 算法分为 2 个阶段：1) 预先准备阶段；2) 别名解析。在预先准备阶段采用与 Timestamp 相近的方式获得支持时间戳路由器及相关 IP 集合，对别名集合进行过滤。在别名解析阶段，具体分为 3 个步骤：① 从别名集合中选择一个 IP 地址 A 作为基准，然后提取可能和该 IP 互为别名的 IP 集合 β；② 从 IP 集合 β 中选择 4 个 IP 构成分组(A|ABCD)，然后通过返回的时间戳发现别名，如果 B 不是别名，将 B 从 IP 集合 β 中移除，否则加入别名集合，同时重新构建探测分组，如(A|ACDE)；③ 重复上述过程直到对所有 IP 都进行了别名解析。与其他别名解析算法相比，Pythia 算法一次可以最多测试 4 个 IP 地址的别名关系，提高了别名的发现效率。

Pythia 算法的不足是测试别名的关系数目有限，而且仅限于网络的前几跳，因此，这种算法适用于网络边缘靠近测量点的地方，对于距离测量点较远的路由器无法采用该方法进行探测，需部署大量测量节点才能得到较为全面的结果。

3.1.4 基于路由记录的别名解析算法

Sherwood 等[29]提了一种基于路由记录来推断别名的算法 Passenger，该算法在 traceroute 分组的报头中加入了路由记录（RR, record route）选项，路由器收到分组后会将路由器地址加入到分组头部中并更新头部的偏移量。实际上 traceroute 发现的路径与路由记录的路径并不重合。RR 记录的是路由器出向接口(outgoing interface)的地址，而 ICMP 分组记录的是进向接口(incoming interface)的地址，因此当 TTL=1 时，RR 中不会有任何记录，而当 TTL=2 时，RR 中记录的 IP 接口就是 TTL=1 时 ICMP 分组返回地址的别名，依次类推即可以进行别名推断，具体如图 9 所示。由于 IP 头部长度有限，RR 记录的路径长度最多不超过 9 跳。在 traceroute 测量中引入使用分组路由记录功能具有

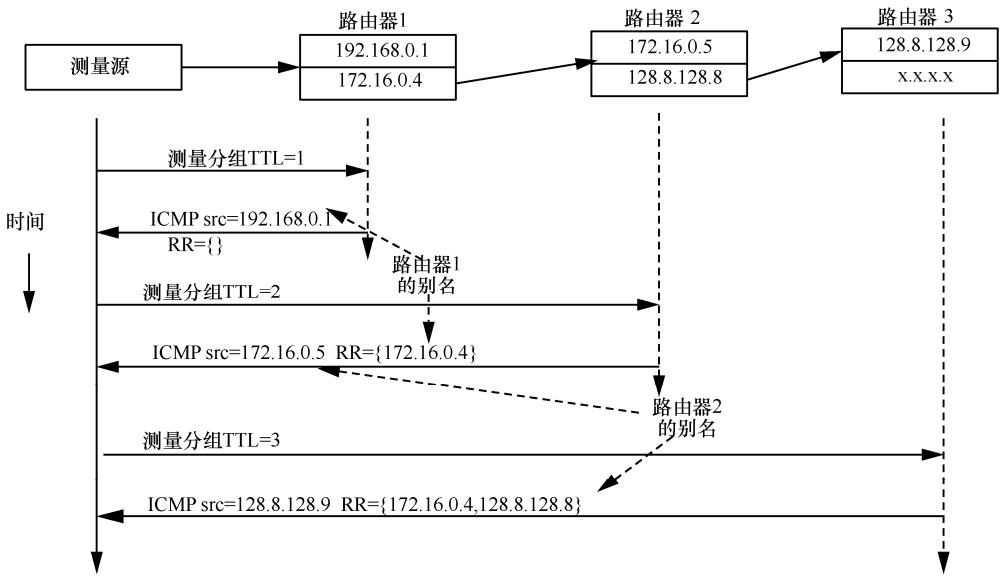


图 9　Passenger 算法原理

以下好处：1) 从某种程度上可以发现那些不响应 ICMP 测量的路由器；2) 可以发现隐藏的路由器；3)发现多连接的路由器；4) 发现中间路径中前 9 跳内路径的不稳定性。

Sherwood 等[33]又对 Passenger 算法进行了改进，提出了 DisCarte 算法，在原有算法上引入了析取逻辑规划（DLP, disjunctive logic programming）对别名推断过程进行形式化表示。DisCarte 算法的求解过程十分复杂，大致分为 2 个阶段：1) 数据预处理，根据不同厂商对于路由记录协议的实现对数据进行分析；2) DLP 求解，也就是将所有的判别转换为逻辑表达式，然后进行求解。

基于路由器记录的别名解析算法虽然引入了新的别名解析思路，但也存在一些不足：1) 采用 RR 选项的分组会引起路由器的过滤，或被入侵检测系统视为入侵流量；2) 不同的路由器厂商对于 RFC791[40]的实现规则不尽相同，需要对不同厂商的协议实现细节进行分析，要考虑循环路由、防火墙、协议实现、隐匿节点、路径长度等众多因素。此类算法对路由器的要求较高，可以作为一种辅助的别名解析方法，用于提高解析的正确率。

3.1.5　基于 IGMP 的路由器别名解析方法

随着多播技术被广泛地应用于视频、音频等领域，越来越多的路由器开始支持网际组管理协议（IGMP, internet group management protocol）。高歌等[41]提出了一种基于 IGMP 的路由器别名解析方法，其工作原理是向目标路由器发送 IGMP 组播分组中的 Ask_Neighbors 分组，目标路由器收到探测分组后会返回给源地址一个 Neighbors_Reply 分组。根据协议，目标路由器会将其接口信息、邻居接口的信息及该路由器接口的相关属性信息放入返回的分组中。以图 10 为例，测量节点对目标路由器 R1 发起探测，路由器 R1 收到探测分组后发送一个响应分组，此分组信息包含路由器 R1 的接口地址和接口属性信息，以及与其相连的邻居路由器 R2~R4 的接口地址和部分接口属性信息。在某些情况下，分组返回的所有信息并不完整，可能是部分接口信息，因此需要对不同的端口进行探测从而保证完信息的整性。

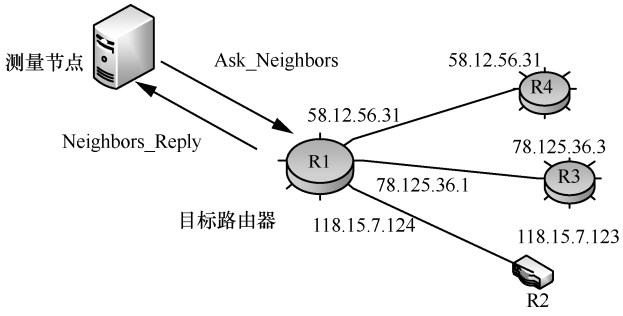


图 10　基于 IGMP 的别名解析过程实例

高歌等[41]提出的算法是在 mrinfo 工具上改进而来的，原始的 mrinfo 收到一个响应分组后就停止接收，当同时对多个目标进行探测时会导致数据丢失。为了避免上述情况的发生，改进后 mrinfo+按照 IP 地址对收到分组进行比对，如果收到来自相同

源地址的分组则丢弃，否则进行处理提取接口作为别名。在测试环境中，此算法探测的效率和准确性方面要高于其他别名解析算法，但是其受到路由器是否支持 IGMP 协议的限制。根据文献[41]对 94 280 个 IP 地址的探测结果表明，仅有 9 797 个目标地址响应探测，然而在实际网络中这个响应比例可能会更低，并且大量的路由器会对 IGMP 探测进行过滤[42]。

此算法由于探测分组会被过滤而导致算法的可用程度大幅下降，仅可作为一种补充性的测量方法，无法在网络中普遍使用。

3.2 基于推断的别名解析算法

3.2.1 基于 DNS 域名的别名推断算法

基于 DNS 域名的别名解析算法(DASAR, DNS based alias resolution)是对 IP 地址的域名进行 DNS 反向查询，然后通过域名的语义分析来推断域名的别名关系[32]。其基本思想是，对路由器的多个接口地址做反向 DNS 地址查询，将域名划分为不同的段，然后按照逆序进行对比。例如，sl-bb21-lon-14-0.sprintlink.net 和 sl-bb21-lon-8-0.sprintlink.net 所对应的 IP 地址是别名，根据“lon”可以猜测 2 个域名属于同一台伦敦的主干路由器，而“14-0”“8-0”可能对应于路由器上的端口。

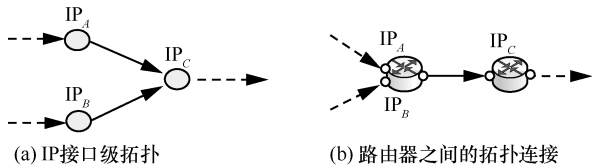
基于 DNS 域名的别名推断算法的准确性依赖于域名命名方式，不同 ISP 可能采用不同的命名方式，因此对于不同 ISP 需要设计不同的推理规则，同时域名信息更新的及时性和命名的范围都会影响算法的使用范围。这种算法虽然简单，但是其准确性和使用范围都有限。赵洪华等[28]对中国、日本、韩国等国家的路由器分析表明，路由器端口采用域名进行标注的在所有路由器端口中的比例很低，因此，这种算法无法大规模使用，可作为一种补充性的解析方法。

3.2.2 基于拓扑的别名推断算法

基于拓扑的别名推断算法利用 IP 地址的连接关系和约束对 IP 的别名关系进行推断，其基本方法如下：对可能是别名关系的 IP 地址对采用 traceroute 测量路径信息，然后将这些信息构建成一张有向图，其中，节点为路由器接口的 IP 地址，边表示 2 个 IP 地址间是否存在一条链路，方向是从测量源到目的地址的测量方向。Spring 等[32]总结出 2 条规则来进行别名关系分析，具体如下。

1) 具有相同直接后继的 IP 地址可能互为别名

一般路由器之间的连接为点对点方式，在这种情况下具有相同直接后继的 IP 地址可能互为是别名。通过拓扑测量获得 IP_A、IP_B、IP_C 的连接关系如图 11(a)所示，其中 IP_C 为 IP_A 和 IP_B 相同后继，如果路由器之间是点对点连接，则它们之间路由器拓扑如图 11(b)所示。



(a) IP接口级拓扑 (b) 路由器之间的拓扑连接

图 11 具有相同后继的 IP 地址是别名

2) 在同一条 traceroute 路径中出现的 IP 地址不是别名

这条规则的前提是网络中不存在循环路径，对于采用多路访问技术或交换网络连接路由器的情形，这种方法就会产生误判。实际上这一规则并不用于判断别名关系，而是用于排除不可能为别名关系的 IP 地址对，从而减少测量和判别的 IP 地址对的数目，对于一个长度为 n 的路径，此规则就可以减少 Cn^2 次判别计算。

基于以上原则，一些利用网络拓扑结构来进行别名关系推测的算法被提出，如 AAR[31]、APAR[43]、Kapar[44]等。

1) AAR 别名解析算法

基于上述规定，Gunes 等[31]提出了 AAR (analytical alias resolution)别名解析算法，其基本思想是对任意一条网络路径从 2 个方向进行测量，获得该路径上所有路由器两侧的 IP 地址，然后通过比较分析判定往返路径中同一跳的 IP 是否满足“/30”和“/31”的情况，对称路由如图 12 所示。

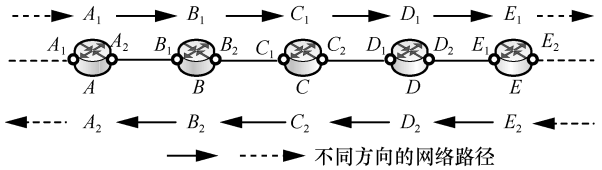


图 12 对称路由示意

Gunes 等[31]对南卫理公会大学（SMU, Southern Methodist University）和耶鲁大学（Yale University）之间的往返路径采用 traceroute 进行了测量，得到的路径如表 1 所示。通过检验，可以发现从第 2 行到第 10 行中往返 2 个方向上的 IP 地址均满足属于“/30”或“/31”的同一个子网，如 129.119.0.249 和 206.223.141.90 互为别名，

206.223.141.89 和 206.223.141.69 互为别名。由此，可以得到 SMU 和耶鲁大学（表 1 和图 13 中简写为 Yale）的网络连接拓扑，如图 13 所示。

表 1　trcaceroute 双向测量获得的网络路径

跳数	SMU 到 Yale（正向路径）	Yale 到 SMU 到（反向路径）
1	129.119.39.1	129.119.223.249
2	129.119.0.249	129.119.0.250
3	206.223.141.89	206.223.141.90
4	206.223.141.70	206.223.141.69
5	198.32.8.34	198.32.8.33
6	198.32.8.66	198.32.8.65
7	198.32.8.84	198.32.8.85
8	192.5.89.9	192.5.89.10
9	192.5.89.33	192.5.89.34
10	192.5.89.70	192.5.89.69
11	130.132.1.19	130.132.1.100
12	130.132.252.244	130.132.23.1

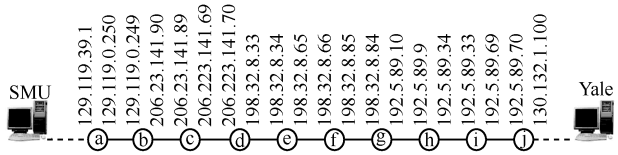


图 13　SMU 和耶鲁大学的网络连接拓扑

Gunes 等[13]在 Abilene 网络中对 AAR 别名解析算法进行了测试，与其他算法相比，该算法在开销和完整性方面具有很大优势。然而，这种算法在实际应用中存在着很大的局限性，因为其数据采集必须是端到端的双向测量。为获得这样的数据，必须进行端与端之间 2 个方向的协作，因此在大规模网络中，这种方法难以实施。

2) APAR

为了克服 AAR 算法的不足，Gunes 等[43]又提出一种基于分析和探测的别名解析器（APAR, analytic and probe-based alias resolver）。APAR 不仅考虑了路由器之间的点对点连接的情况，还考虑了多个连接的情况，这就意味着必须拓展子网的范围。该算法共分为 2 个步骤：① 从收集的路径信息中提取可能是别名集合的数据集；② 使用别名子网对别名进行解析。

在子网段提取阶段，APAR 在 traceroute 探测到的大量地址中推断子网信息。首先，将所有的 IP 地址中具有相同“/22”前缀的地址划分为一个子网（或子集）。然后，检验这些地址是否满足正确性约束、完整性及处理次序 3 个约束条件，其中准确性约束是指若这个子网中的任何一个广播地址出现在 traceroute 数据中，则该子网不为真；完整性约束是指在 traceroute 路径中至少发现一半的子网地址；处理次序是指首先对完整率高的先处理，对于完整率相同的则处理涉及路径较多的子集。

在形成子集后，对子集的判定又有 3 个规则，分别为：无循环路径、相同邻居节点和距离测度[45]。无循环路径是指所有可能为别名的任意 2 个 IP 不能出现在同一跳路径上。相同邻居节点是指 2 个互为别名的 IP 具有相同的前继节点或后继节点，或者这些节点互为别名。距离测度是指从一个测量点到互为别名关系的 IP 测量获得路径长度应该相同或者接近。其中，最后一个规则是个可选条件，在可以进行测量时使用。

3) Kapar 算法

APAR 具有更高的准确性，同时考虑了路由器多连接的情况。Keys 等[44]对 APAR 进行了改进和优化，提出了 Kapar 算法，该算法避免了将所有的路径信息存储到内存中，提高了算法性能。与 APAR 相反，Kapar 算法在测量数据上通过一个检测合并使用最少的信息，具体如下。

① Kapar 将所有的路径数据划分为 3 跳分段数据。

② 通过分析路径文件生成不可能存在别名关系的子网的列表，子网长度在 24 位以上。

③ 为每个路径分配一个 ID，存储所有的 IP 信息，根据这些信息可以分析是否存在循环路径。

此外，Kapar 还从其他几个方面改进了 APAR 算法，具体如下。

① 可以使用其他来源的别名集合，如通过指纹解析获得的别名集合。

② 在子网信息阶段，采用了更加严格的算法来判定点到点的子网。

③ 在别名推测阶段，对邻接关系采用了更加严格的判定算法。

④ 综合使用多个观测点获得 TTL 数据来降低别名解析假阳率。

总体而言，基于推断的别名解析算法在原理上更加复杂，这些方法大多借助网络的拓扑结构进行推断，为了获取全面的网络拓扑地址信息，

必须进行分布式测量，从而导致算法实现起来较为困难。因此，此类算法在有测量数据集或者分布式平台的情况下才能更好地得到应用。

3.2.3 基于机器学习的别名推断算法

在前期研究的结果上，AliasCluster 算法[34]将机器学习的方法引入到别名解析中，试图仅采用 traceroute 而不增加测量开销来实现别名解析。该算法分为 2 个阶段，具体如下。

阶段 1 通过 traceroute 测量收集数据，分析获得的 3 个数据特征（IP 子网、出入度、跳数等），采用贝叶斯网络推断模型推断 2 个 IP 互为别名的概率。

阶段 2 考虑到一个路由器可能具有多个别名地址或者缺乏足够推断信息，引入链式推理方法将 2 个 IP 地址视为一个聚类，如果 2 个聚类的相似性较为接近就进行合并，从而通过推断发现新的 IP 地址别名关系。

AliasCluster 算法采用了机器学习的方式，精度受到参数设置影响，但是为设计新的解析算法指明了方向，特别是在缺乏足够探测信息的网络条件下。

除了 AliasCluster 算法外，Grailet 等[25]提出 TreeNet 和 Sherwood 等[33]提出的 DisCarte 算法也引入了机器学习的思想和方法，本文分别在 3.3.2 节和 3.1.4 节进行详述。

综上所述，机器学习方法的引入使别名解析过程中可以使用多种探测数据和指纹信息，采取更加复杂的逻辑推理，从而提高别名解析效率，因此如何更好地使用机器学习方法来进行别名解析将成为新的研究方向之一。

3.3 综合测量法

实际上随着基于测量和基于推断两类算法研究的不断深入，为了减少测量复杂度，提高测量精度，一些综合性的别名探测算法被提出，如 Palmtree 算法[46]、TreeNet 算法[25]。

3.3.1 Palmtree 算法

Tozal 等[46]综合考虑路由器接口 IP 地址的分配方案与同源地址 IP 别名解析的原理，在此基础上提出了 Palmtree 算法，该算法的基本思想如下。

1) 首先探测目标的 IP 地址是否活跃。

2) 如果探测的目标 IP 是活跃的，则分析探测节点到目标 IP 的跳数。

3) 根据 RFC 4632 中路由器接口的分配方案，对“/31”或“/30”的子网中的 IP 地址进行探测，然后采用同源地址的方法判断别名关系。

该算法声称可以将探测的复杂度降低到线性复杂度，实际上在缺乏全局先验知识的情况下，其探测复杂度也是较大的。因此，该算法可以适用于对特定网络的别名判定。

3.3.2 TreeNet 算法

Grailet 等[25]提出了一种综合各种测量方法的别名解析算法 TreeNet，该算法分为 3 个步骤：首先，通过拓扑测量将所有的 IP 别名划分为小的集合，从而避免了大规模探测，划分时所有 IP 节点的路径跳数不能超过 1 跳，拓扑探测中采用 ExploreNET 算法[47]；然后，采集所有别名的指纹信息，主要包括 TTL 值、端口不可达分组源地址、IPID、DNS 的解析结果及时间戳信息；最后，将上述采集的信息，按照指纹信息的可信度进行分类，依次为 UDP 探测的响应、IPID 序号、DNS 解析结果等，从而进行综合的别名解析。TreeNet 算法可以看做是 iffinder、Kapar 等算法的结合体，实验证明该算法可以采用较少的探测分组实现与 MIDAR、Kapar 类似的精度。

TreeNet 算法需要集合多种别名解析工具，实现方法较为复杂，但其精度和准确度都是较高的，适用于大规模的别名解析。

4 IPv6 别名解析技术

IPv6 协议不仅扩展了 IPv4 地址空间的范围，而且对 IP 分组的分组格式等方面也做了修改[48]，如 IPv6 网络层不再支持大数据分组的再分组与重装，而是由应用层负责完成，同时 IPv6 增强了对组播和流控制的支持、自动配置及更高的安全性和较小的路由表。由于种种原因，IPv6 标准虽然已经提出了 20 多年，但是仍然没有得到广泛的部署和使用，仅在部分骨干网络和试验网络中得到了应用[40]。随着 IPv4 地址的耗尽，IPv6 的部署进度不断加快。据统计，全球 IPv6 的 BGP（border gateway protocol）前缀通告呈现出指数级增长，超过 6 000 个 AS（autonomous system）宣告了 IPv6 可达，约占所有 AS 数的 15%，因此，研究 IPv6 的网络拓扑及别名解析正变得更加紧迫[49]。

由于 IPv6 网络与 IPv4 网络设计上的差异，许多可以用于 IPv4 网络的别名解析技术无法应用于 IPv6 网络。先后有一些研究者提出了基于源路由、诱发式 IPID 的 IPv6 别名解析技术和基于前缀的别

名解析算法，如 Atlas[50]、RMP[51]、TBT[52]、Speedtrap[53]、UAv6[54]等算法。

4.1　基于源路由的别名解析算法

路由器在检查分组跳数限制之前通常会先处理路由扩展头部。Atlas 对 2 个可能互为别名关系的 IP 地址对(x,y)，将向 y 发送跳数限制设置为到 x 跳数的 UDP 分组。如果 2 个 IP 互为别名，则会收到“跳数超出限制”和“端口不可达”的响应分组。文献[51]发现在所有响应分组中，“跳数超出限制”的响应分组主要是由路由器的注入端口产生。因此，要发现 y 的别名，必须将分组的超时限制设置为 y 的跳数，从测量点 V 通过 x 和 y 向目标地址 D 发起测量，才会收到来自于 y 的超时响应分组，这样就需要一个足够大的地址集，来寻找互为别名的 IP 地址。Qian 等[55]又提出在 IPv6 分组的头部加入一个乱序的比特序列，从而通过多个测量点发起测量捕获别名关系。

基于源路由的别名解析算法不足在于：1) 路由器是否支持源路由，若不支持则方法无效；2) 上述算法采用 UDP 协议，如果不支持 UDP 协议则方法无效。因此，基于源路由的别名解析算法只适用于部分路由器。

4.2　基于诱发式 IPID 的别名解析算法

4.2.1　TBT 算法

Robert 等[52]利用 IPv6 的特点提出了一种诱发式 IPID 的别名解析算法（TBT, too-big trick），其基本过程如下。首先，测量点发送一个 1 300 B 的数据分组，这个分组超过了 IPv6 协议 MTU 的 1 280 B 限制，同时又小于 IPv4 协议的 MTU 限制的 1 500 B，因此当接收者收到该数据分组时会将数据分组返回给发送者。此时，测量点再根据 IPv6 协议发出一个“Too Big”分组，探测目标收到此分组会将发送缓存设为 1 280 B。然后，测量点再发送一个 1 300 B 的测量分组，探测目标会将分组拆分为 2 个分组进行发送并加入分段 ID。此后，测量点发送的分组都会进行类似拆分，而同一个路由器不同端口发送的分组的 ID 必然相近，因此可以判定出别名关系。TBT 算法如图 14 所示。这种诱发式的别名探测方法准确率十分高，而且减少了测量数据。

TBT 算法虽然具有较高的准确性，但是探测的数据量相对于 IPv4 的 IPID 方法的数据量要大很多，同时探测的次数随着别名数的增加迅速增加，会带来较大的网络负载。

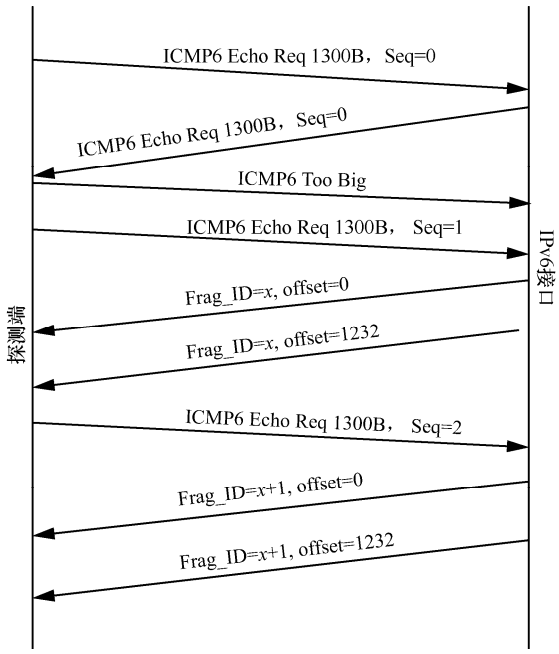


图 14　TBT 别名解析算法原理

4.2.2　Speedtrap

Luckie[53]将诱发式的 IPID 探测技术与 IPv4 别名解析中的单调边界测试函数相结合，提出了 IPv6 的别名解析工具 Speedtrap，从而可以进行整个网络范围内的数据 IP 别名解析。Speedtrap 别名解析的基本过程如下。

1) 通过测量确定响应分组中带有 IPID 的网络接口集合，目的是过滤掉那些不响应测量和采用随机计数器的路由器。实际上除了 Jupiter 路由器外，华为、思科、惠普等多数路由器都响应测量。

2) 确定哪些接口可能共享一个计数器，即哪些 IP 位于同一台路由器上。将响应网络接口的 IPID 按照时间划分为不同的组，然后对不同的 2 个接口地址进行探测，形成备选的别名关系集合。

3) 将不同路由器上的计数器进行区分，对可能是别名的 IP 进行反复测量，这样使不位于同一台路由器的接口返回的 IPID 差距变大，若 IPID 不再满足 MBT 约束则将其从别名集合中删除。

4) 对 IP 别名进行探测和确认。对还在别名集合中的任意 2 个接口进行测量，检测其是否满足 MBT 条件，从而进一步确认其别名关系。

采用 Speedtrap 对 52 969 个 IP 接口进行了测量和分析，共耗时 9 h，其中 5.5 h 用于确定接口的响应分组是否包含 IPID。实验表明有 17 002 个接口响应测量，发现了 11 181 台路由器。探测时间较长的原因是：为了诱发路由器对 IPv6 分组进行分

组，需要发射的分组要比IPv4大46倍（至少1 280 B），由于数据量较大，故探测时间较长。在真实网络的训练集中测试发现，Speedtrap 的正确性可以达到 99%以上。

相对于 TBT 算法，Speedtrap 的效率得到了提升，但是 TBT 算法和 Speedtrap 算法都需要接口共享计数器才能实现。统计表明，在实际部署的路由器中，仅有 32%的路由器采用共享的计数器[53]，因此，这类算法只能适用于部分路由器。

4.3 基于前缀的别名解析算法

Padmanabhan 等[54]通过对 IPv6 端到端的 IP 地址配置方式进行了研究，发现在 IPv6 中采用了与 IPv4 相似的配置方式，多数采用“/126”前缀。基于此提出了 UAv6 算法，该算法分为 2 个阶段，具体如下。

1) 进行可能的别名集合探测。对一个 IP 的“/126”子网进行探测，如果该前缀所包括的 4 个 IP 地址均能响应 ICMPv6 的探测，则不会出现任何别名，当有 2 个 IP 地址响应时才能出现别名，设不响应的地址为 X_1、X_2，返回的源地址为 Y，将其记录下来。

2) 对于可能的别名集合进行检测。为了检验是否为别名，采用 traceroute 或路径的最大传输单元来进行检测。如果某个 X_1 位于 Y 的路径上后一跳，则说明 X_1 不可能为别名，反之亦然。

UAv6 算法提出了一种新的别名解析方法，但是该算法的复杂度较高，同时与 IPv4 中的相同源地址方法原理基本相似，不受路由器计数器及源路由的影响，可以与其他 IPv6 别名解析算法进行互补，从而提高解析的全面性。

5 算法对比与分析

5.1 算法综合分析

别名解析算法设计原理各异，适用于不同网络环境。下面从算法的准确性、完整性、开销、易用性、使用范围等几个不同的角度对这些算法进行综合对比，从而发现别名解析算法研究趋势，如表 2 所示。

准确性：推断的别名关系是否正确。

完整性：对别名是否能够发现测量范围内的所有别名关系。

开销：用于探测别名所用探测分组的数量。当需要发送分组越多时，网络流量和时间越多，效率越低，反之，效率就越高。

简易性：算法使用是否简易，是否需要很多外部条件支持，即算法实现的难易程度。

协议：算法适用的 IP 协议，包括 IPv4 和 IPv6。

适用场景：算法的部署方式以及范围。

时间：论文发表时间。

实际上在各种别名解析算法中，主要有 3 个影响算法使用的因素：适用范围、准确性和效率。众所周知，如果算法能够集中部署，则大规模应用较为容易；如果需要分布式测量往往不易实现。基于探测的算法中，如基于同源地址的 Mercator[24]、iffinder[25]、Alas[50]算法，基于 IPID 的 Ally[23]、RadarGun[37]、MIDAR[38]、TBT[52]、Speedtrap[53]等均可以通过集中部署的方式来实现，而基于图论或拓扑的算法往往需要大规模的分布式测量来实现，在实际操作中难以实现，因此，这些算法往往借助于 Ark、PlanetLab 等大型测量项目才可以部署。

为了对算法的准确性和效率有个全面的认识，对典型算法的精度和时间效率进行了对比，结果如图 15 所示，该结果综合了 Garcia-Jimenez[35]、Padmanabhan[54]等实验结果。考虑到实验的差别，本文参照相关论文进行了定性对比。从图中可以发现基于同源地址的算法最为准确，而采用 IPID 的算法次之，基于网络拓扑的推断算法则需要较大的开销，同时无法保证算法准确性，在以后的算法设计中应充分考虑上述因素。

为了进一步说明算法的演化过程理清研究思路，采用图形进行了展示，具体如图 16 所示。从算法的演化过程可以发现，基于 IPID 及拓扑的算法最多，也是发展最为迅速的研究方向，同时新的算法综合考虑了各种要素，综合运用各种别名指纹，而采用时间戳、路由记录字段的算法则研究的较少。此外，可以发现针对 IPv6 的别名解析算法由于 IPv6 的快速部署而受到重视，成为这几年研究的热点。但 IPv6 别名解析算法主要集中在 IPID 或者是同源地址的方法，而采用拓扑推断的算法较少。这主要是因为 IPv6 在近几年才得到了大规模部署，其测量数据较少，缺乏必要的数据支撑。

5.2 未来研究方向

通过前文分析可以发现 IPv4 别名解析研究比较成熟，而针对 IPv6 的研究则处于起步阶段，为此结合别名解析中的 3 个阶段提出如下建议。

表 2　　别名解析技术对比

算法名称	原理	准确性	完整性	开销	简易性	协议	适用场景	发布时间
Mercator[20]	同源地址	高	较低	$O(n^2)$	容易	IPv4	集中，全网络	2000
iffinder[21]	同源地址	高	较低	$O(n^2)$	容易	IPv4	集中，全网络	2001
Alas[50]	同源地址	高	较低	$O(n^2)$	容易	IPv4+IPv6	集中，全网络	2001
Ally[23]	同源地址+IPID	中	较低	$O(n^2)$	较容易	IPv4	集中，全网络	2002
DASAR[32]	DNS 解析	高	较低	$O(n^2)$	容易	IPv4	集中，全网络	2004
AAR[31]	图论	中	高	$O(n^2)$	难	IPv4	分布式，全网络	2006
Passenger[29]	RR	中	中	$O(n^2)$	难	IPv4	集中，网络边缘	2006
RadarGun[37]	IPID	中	中	$CO(n)$	较容易	IPv4	集中，全网络	2008
DisCarte[33]	RR	高	中	$O(n^2)$	难	IPv4	集中，网络边缘	2008
APAR[43]	图论	中	高	$O(n^2)$	难	IPv4	分布式，全网络	2009
Kapar[44]	图论	中	高	$O(n^2)$	难	IPv4	分布式，全网络络	2010
Timestamp[49]	时间戳	高	低	$O(n^2)$	简单	IPv4	分布式，网络边缘	2010
Palmtree[46]	综合	高	低	$O(n)$	简单	IPv4	集中，整个网络	2011
Pythia[39]	时间戳	高	低	$O(n^2)$	简单	IPv4	分布式，网络边缘	2013
MIDAR[38]	IPID	中	中	$CO(n^2)$	较容易	IPv4	集中，部分网络	2013
AliasCluster[34]	图论	中	中	$CO(n^2)$	容易	IPv4	分布式，全网络	2013
Pamplona-traceroute[35]	IPID	高	高	$Cn+O(n^2)$	难	IPv4	分布式，全网络	2013
TreeNet[25]	综合	高	低	$Cn+O(n^2)$	复杂	IPv4	集中，部分网络	2017
RMP[51]	同源地址	中	较低	$O(n^2)$	容易	IPv4+IPv6	集中，部分网络	2010
Mrinfo+[41]	IGMP	高	低	$O(n)$	简单	IPv4+IPv6	集中，部分网络	2012
TBT[52]	IPID	高	高	$CO(n^2)$	难	IPv6	集中，部分网络	2013
Speedtrap[53]	IPID	高	高	$CO(n^2)$	难	IPv6	集中，部分网络	2013
UAv6[54]	ICMP	高	中	$CO(n)$	简单	IPv6	分布式，部分网络	2015

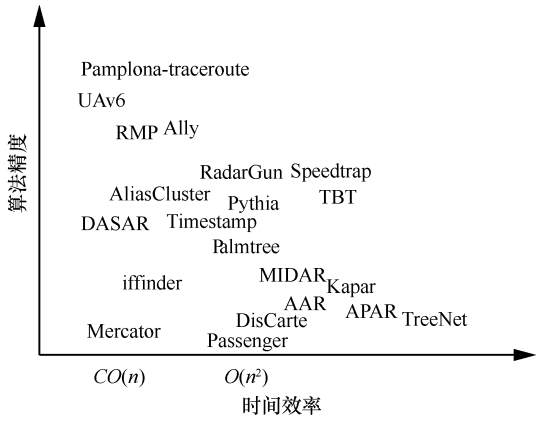


图 15　不同算法精度和复杂度的对比

1) 别名空间的选择

别名空间选择目的在于缩小可能互为别名的 IP 地址范围，从而减少探测开销，提高解析效率。在 IPv4 空间中，由于地址空间有限，随着计算能力的提高和网络带宽的扩展，一些快速扫描技术如 Zmap[56]、Masscan[57]等可以在很短时间内实现对网络空间的扫描，从而为 IPv4 的别名解析提供数据支撑。但是，IPv6 地址空间十分巨大，按照现有的扫描速度需要 10^{30} 年才能扫描结束[58]。在如此稀疏的 IP 地址空间中要想缩小别名的搜索范围有 2 种方法，一是挖掘路由器别名分配规律，二是通过全量测量发现所有活跃 IP 地址。

针对如何发现路由器别名的分配规律，文献[38]对 IPv4 别名进行了分析。图 17 是 22 515 对 IP 别名中 2 个 IP 地址的距离的累计分布概率，即 2 个互为别名的 IP 地址如果将其转换为整数后的差异。从图中可以发现在一个“/24”（即 IP 之间的差小于

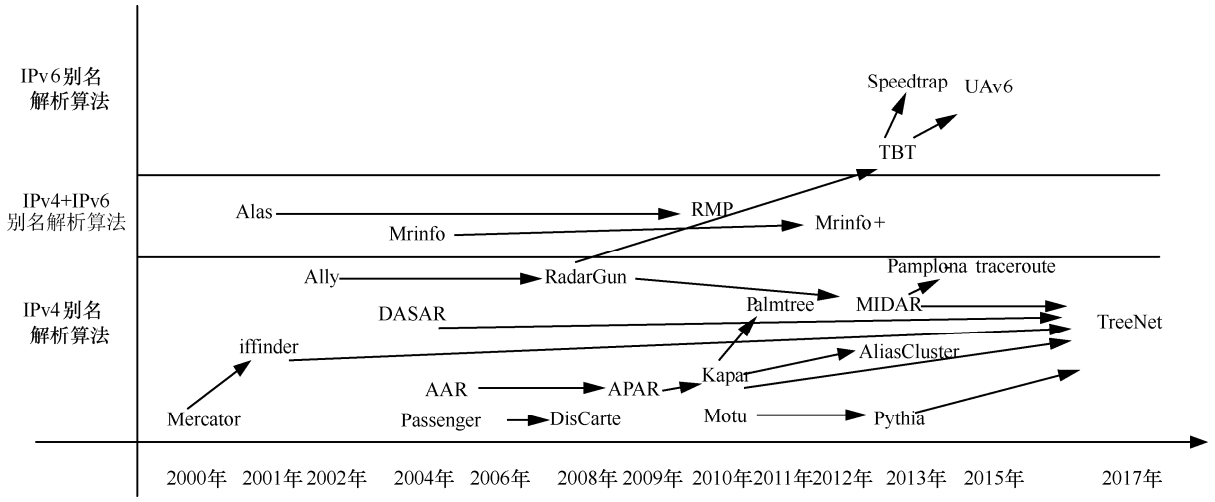


图 16　别名解析算法演化过程

128）位 IP 子网内互为别名的 IP 地址不足 30%，而一个“/16”（即 IP 之间的差小于 65 536）位子网中互为别名的 IP 地址约为 50%，这说明即便在密度很高的 IPv4 网络中，IP 地址别名的距离也较大。在 IPv6 网络中，IP 地址资源更为丰富，因此试图发现路由器的别名的分配规律来缩小别名的探测范围变得更加困难。

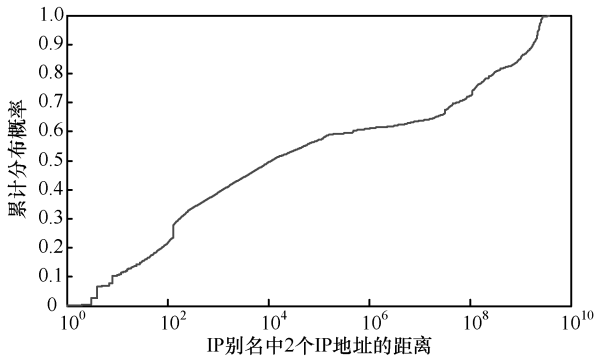


图 17　IP 别名之间的距离累计分布函数

针对如何发现所有活跃 IP 地址的问题，解决方案为实现对 IPv6 空间的快速探测，从而根据 IPv6 的接口分布规律来进行别名关系搜索。关于 IPv6 地址空间的快速探测研究有很多[59]，如 DNS 解析、被动流量解析、traceroute 测量等方法。据统计，在国外 IPv6 网络较为普及，如美国、印度等超过 50%的流量为 IPv6 流量，而探测发现的活跃 IPv6 地址仅有 5×10^7 个[60]，仅为一小部分，因此未来如何快速探测活跃 IP 地址是影响 IP 别名解析效率的关键。

2) 算法指纹特征的选取

在进行别名解析算法的设计过程中，最主要的是设计别名识别的指纹特征。图 16 给出了主要别名解析算法的演化过程，这些算法大致可以分为 3 类，即基于 IPID 的算法、基于拓扑推断的算法及其他算法。其中前两类算法由于得到了多数路由器的支持而得到了广泛的应用，而基于路由记录、IGMP 协议的算法由于多数路由器不支持甚至禁用，很难进一步研究。因此，在算法的指纹选择时，要选择更加具有代表性的指纹特征才能使算法在更加广泛的范围中应用。实际上，目前算法采用的很多指纹特征并没有得到广泛的支持。

Salutari 等[61]通过大规模测量研究了路由器采用 IPID 的情况，发现大多数路由器或主机采用常数 IPID（39%）或局部计数器（34%），采用全局计数器的约占 18%，无规律的约占 7%和采用随机数 IPID 的约占 2%。在五类 IPID 中，只有采用全局模式的路由器才能用于定位，这一测量结果说明采用 IPID 进行大规模的别名解析并不具有普适性。同时，Marchetta 等[62]对 1 400 多个 AS 中 32.7 万个目标进行了测量，经分析发现有 32.4%的路由器支持时间戳字段。这说明目前作为 IP 别名解析的主要方向的基于 IPID 的方法仅能发现较小一部分的别名，而要提高 IP 别名解析的准确性，则要借助于全面的指纹特征。特别是针对 IPv6 协议进行深入分析，发现其在路由记录、组播协议、时间戳等方面的特征，丰富别名判别的指纹特征集合。

3) 基于机器学习的判定方法

别名解析本质上是一个判别问题，即判定 2 个或者多个 IP 是否互为别名，其判别依据是 IP 的域名、TTL、拓扑位置、IPID 连续性、出入度等，然而由于网络中情况十分复杂，无法采用一种方式进行全面的分类，或者无法获得完整的数据，必须采用多种指纹相结合的方式。在机器学习中，有很多基于多特征分类或判别的方法，或者实现复杂推理的算法，机器学习技术的引入应重点考虑以下 2 个方面。

① 不再借助于一个单独的特征而是多个指纹特征，因此需要构建全面的推理过程，如算法 DisCarte 中采用了析取逻辑规划[33]，用以进行复杂逻辑的推理，从而提高算法判别的全面性。

② 在算法中应当考虑不完全信息的处理，比如在拓扑分析中往往需要借助于大规模分布测量，但是现实中无法实现，如 AliasCluster 算法中采用的链式推理逻辑，就可以避免信息不完全所带来的别名误判。因此，在推理中采用不确定性决策、灰色理论、贝叶斯网络、决策树等方法来构建完善的推理过程。

6 结束语

别名解析技术是实现网络空间从逻辑拓扑到物理拓扑映射的关键步骤，同时也是网络空间测量领域的技术难题。由于缺乏大规模的数据验证，别名解析技术的准确性一直受到质疑。然而由于网络空间安全战略的需要，必须进一步提高别名解析算法的性能。别名解析不仅需要深入了解网络协议细节、IP 地址分配规律和网络拓扑知识，还需要借助于大规模网络测量基础设施进行数据测量、收集及分析。特别是随着 IPv6 的广泛部署，在测量和分析上出现了许多新的问题，如在 IPv6 网络空间中实现别名集合快速获取，低开销的快速测量、别名关系的准确推断等。要解决这些新问题就必须采用新的方法，在算法的设计中应当采用多种特征信息，引入机器学习的方法，从而提高别名解析的准确性和完整性，为网络空间拓扑构建、态势感知、追踪溯源等业务应用提供数据支撑。

参考文献：

[1] CLAFFY K, CLARK D. Workshop on Internet economics (WIE2014) report [J]. ACM SIGCOMM Computer Communication Review, 2015, 45(3):43-48.

[2] WILLINGER W, ROUGHAN M. Internet topology research redux [M]. ACM SIGCOMM eBook: Recent Advances in Networking, 2013.

[3] DONNET B, FRIEDMAN T. Internet topology discovery: a survey [J]. IEEE Communications Surveys and Tutorials, 2007, 9(4): 2-15.

[4] LUCKIE M, DHAMDHERE A, HUFFAKER B, et al. Bdrmap: inference of borders between IP networks [C]// ACM SIGCOMM Conference on Internet Measurement. ACM, 2016:381-396.

[5] GIOTSAS V, DHAMDHERE A, CLAFFY K. Periscope: unifying looking glass querying [C]// Passive and Active Measurement Conference. Springer, 2016: 177-189.

[6] CHANDRASEKARAN B, SMARAGDAKIS G, BERGER A, et al., A server-to-server view of the Internet[C]// ACM International Conference on emerging Networking EXperiments and Technologies. ACM, 2015:1-13.

[7] GIOTSAS V, LUCKIE M, HUFFAKER B, et al. Inferring complex AS relationships [C]// ACM SIGCOMM Conference on Internet Measurement. ACM, 2014:23-30.

[8] HUFFAKER B, FOMENKOV M, CLAFFY K. DRoP: DNS-based router positioning [J]. ACM SIGCOMM Computer Communication Review, 2014, 44(3):5-13.

[9] KING A, HUFFAKER B, DAINOTTI A, et al. A coordinated view of the temporal evolution of large-scale Internet events [J]. Computing, 2014, 96(1):53-65.

[10] GIOTSAS V, ZHOU S, LUCKIE M, et al. Inferring multilateral peering[C]// ACM SIGCOMM Conference on Emerging Networking Experiments and Technologies. ACM, 2013:247-258.

[11] GIOTSAS V, SMARAGDAKIS G, HUFFAKER B, et al. Mapping peering interconnections to a facility[C]// ACM International Conference on Emerging Networking Experiments and Technologies. ACM, 2015:1-13.

[12] AGER B, MÜHLBAUER W, SMARAGDAKIS G, et al. Web content cartography[C]//ACM SIGCOMM Conference on Internet Measurement Conference. ACM, 2011: 585-600.

[13] CASTRO I, CARDONA J C, GORINSKY S, et al. Remote peering: more peering without internet flattening[C]// ACM International Conference on Emerging Networking Experiments and Technologies. ACM, 2014: 185-198.

[14] BREITBART Y, GAROFALAKIS M, MARTIN C, et al. Topology discovery in heterogeneous IP networks[C]// IEEE International Conference on Computer Communications. IEEE, 2000: 265-274.

[15] BEJERANO Y. Taking the skelons out of the closets: a simple and efficient topology discovery scheme for large Ethernet [J]. ACM/IEEE Transactions on Networking, 2009, 17(5): 1385-1398.

[16] HADDADI H, RIO M, IANNACCONE G, et al. Network topologies: inference, modeling and generation [J]. IEEE Communication Surveys Tutorials, 2008, 10(2):48-69.

[17] DONNET B, FRIEDMAN T. Internet topology discovery: a survey [J]. IEEE Communications Surveys and Tutorials, 2007, 9(4): 2-15.

[18] SPRING N, MAHAJAN R, WETHERALL D, et al. Measuring ISP topologies with rocketfuel [J]. IEEE/ACM Transactions on Networking, 2004, 12(1): 2-16.

[19] CLAFFY K C. Internet tomography [EB]. Nature, Web Matter, 1999.

[20] GOVINDAN R, TANGMUNARUNKIT H. Heuristics for Internet map discovery[C]// IEEE International Conference on Computer

Communications. IEEE. 2000: 1371-1380.

[21] PANSIOT J, GRAD D. On routes and multicast trees in the Internet [J]. ACM SIGCOMM Computer Communication Review, 1998, 28(1):41-50.

[22] SPRING N, WETHERALL D, ANDERSON T. ScrIPtroute: a public Internet measurement facility [C]// USENIX Symposium on Internet Technologies and Systems. USENIX, 2003: 225-238.

[23] SPRING N, MAHAJAN R, WETHERALL D. Measuring ISP topologies with rocketfuel [J]. ACM SIGCOMM Computer Communication Review, 2002, 32(4):133-145.

[24] KEYS K. IP alias resolution techniques: technical report[R]. Cooperative Association for Internet Data Analysis, [2009−01−19].

[25] GRAILET J F, DONNET B. Towards a renewed alias resolution with space search reduction and IP fingerprinting [C]// Network Traffic Measurement and Analysis Conference. IEEE, 2017:1-9.

[26] PANSIOT J, GRAD D. On routes and multicast trees in the internet [J]. ACM SIGCOMM Computer Communication Review, 1998, 28(1): 41-50.

[27] 赵洪华, 白华利, 陈鸣, 等. 路由器级拓扑发现中的别名过滤算法[J]. 西安电子科技大学学报, 2009, 36(1):177-182.
ZHAO H H, BAI H L, CHEN M, et al. Alias filter algorithm in router level topology discovery [J]. Journal of Xi'dian University, 2009, 36(1):177-182.

[28] 赵洪华, 白华利, 陈鸣, 等. 别名解析中的别名过滤技术[J]. 软件学报, 2009, 20(8):2280-2288.
ZHAO H H, BAI H L, CHEN M, et al. Alias filtering technique in alias resolution [J]. Journal of Software, 2009, 20(8):2280-2288.

[29] SHERWOOD R, SPRING N. Touring the Internet in a TCP sidecar [C]//ACM SIGCOMM Conference on Internet Measurement. ACM, 2006: 339-344.

[30] SHERRY J, KATZ-BASSETT E, PIMENOVA M, et al. Resolving IP aliases with prespecified timestamps[C]//ACM SIGCOMM Conference on Internet Measurement. ACM, 2010:172-178.

[31] GUNES M H, SARAC K. Analytical IP alias resolution [C]//IEEE International Conference on Conference.IEEE, 2006:459-464.

[32] SPRING N, DONTCHEVA M, RODRIG M, et al. How to resolve IP aliases [R]. The University of Washington: Department of Computer Science and Engineering, 2004.

[33] SHERWOOD R, BENDER A, SPRING N. Discarte: a disjunctive Internet cartographer [C]// ACM SIGCOMM Conference on Data Communication. ACM, 2008:303-314.

[34] SPINELLI L, CROVELLA M, ERIKSSON B. AliasCluster: a lightweight approach to interface disambiguation[C]// IEEE International Conference on Computer Communications. IEEE, 2013: 3333-3338.

[35] GARCIA-JIMENEZ S, MAGANA E, MORATO D, et al. Pamplona-traceroute: topology discovery and alias resolution to build router level Internet maps[C]// Global Information Infrastructure Symposium. GIIS, 2013:1-8.

[36] MALKIN G. Traceroute using an IP option[R]. RFC1393, (1993−02−02) [2018−09−07].

[37] BENDER A, SHERWOOD R, SPRING N. Fixing Ally's growing pains with velocity modeling [C]// ACM SIGCOMM Conference on Internet Measurement. ACM, 2008:337-342.

[38] KEYS K, HYUN Y, LUCKIE M, et al. Internet-scale IPv4 alias resolution with MIDAR [J]. IEEE/ACM Transactions on Networking, 2013, 21(2):383-399.

[39] MARCHETTA P, PERSICO V. Pythia: yet another active probing technique for alias resolution [C]//ACM Conference on Emerging Networking Experiments and Technologies. ACM, 2013:229-234.

[40] POSTEL J. DARPA Internet program protocol specification[R]. RFC 791, (1981−09−01)[2018−09−07].

[41] 高歌. 路由器别名解析方法研究[D]. 哈尔滨:黑龙江大学, 2012.
GAO G. Research on router alias resolution method [D]. Harbin: Heilongjiang University, 2012.

[42] MARCHETTA P, MERINDOL P, DONNET B, et al. Quantifying and mitigating IGMP filtering in topology discovery[C]// Global Communications Conference. IEEE, 2012:1871-1876.

[43] GUNES M, SARAC K. Resolving IP aliases in building traceroute-based internet maps [J]. IEEE/ACM Transactions on Networking, 2009, 17(6):1738-1751.

[44] KEYS K. Internet-scale IP alias resolution techniques [J]. ACM SIGCOMM Computer Communication Review, 2010, 40(1):50-55.

[45] LONE Q, LUCKIE M, KORCZYŃSKI M, et al. Using loops observed in traceroute to infer the ability to spoof [C]// International Conference on Passive & Active Network Measurement. Springer, 2017:229-241.

[46] TOZAL M E, SARAC K. Palmtree: an IP alias resolution algorithm with linear probing complexity[J]. Computer Communications, 2011, 34(5):658-669.

[47] TOZAL M. E, SARAC K. Subnet level network topology mapping[C]//IEEE International Performance Computing and Communications Conference. IEEE, 2011:1-8.

[48] BONICA R, KUMARI W, BUSH R, et al. IPv6 fragment header deprecated Internet draft [S]. (2013−07−01)[2018−09−07].

[49] ORSINI C, KING A, GIORDANO D, et al. BGPStream: a software framework for live and historical BGP data analysis[C]//ACM SIGCOMM Conference on Internet Measurement. ACM, 2016:429-444.

[50] WADDINGTON D G, CHANG F, VISWANATHAN R, et al. Topology discovery for public IPv6 networks [J]. ACM SIGCOMM Computer Communication Review, 2003, 33(3): 59-68.

[51] QIAN S, WANG Y, XU K. Utilizing destination options header to resolve IPv6 alias resolution [C]// The Global Communications Conference. IEEE, 2010:1-6.

[52] BEVERLY R, BRINKMEYER W, LUCKIE M, et al. IPv6 alias resolution via induced fragmentation[C]//International Conference on Passive & Active Network Measurement. IEEE, 2013:155-165.

[53] LUCKIE M, BEVERLY R, BRINKMEYER W, et al. Speedtrap: Internet-scale IPv6 alias resolution [C]// ACM SIGCOMM on Internet Measurement Conference. ACM, 2013:119-126.

[54] PADMANABHAN R, LI Z, LEVIN D, et al. UAv6: alias resolution in IPv6 using unused addresses[C]// International Conference on Passive & Active Network Measurement. Springer. 2015:136-148.

[55] QIAN S, XU M, QIAO Z, et al. Route positional method for IPv6 alias resolution [C]// International Conference on Computer Communications & Networks. Springer, 2010:1-6.

[56] DURUMERIC Z, WUSTROW E, HALDERMAN J A. ZMap: fast internet-wide scanning and its security applications[C]// USENIX Conference on Security. USENIX Association, 2013:605-620.

[57] GRAHAM R D. MASSCAN: Mass IP port scanner[R]. GitHub, (2016−06−06) [2018−09−07].

[58] MURDOCK A, LI F, BRAMSEN P, et al. Target generation for internet-wide IPv6 scanning[C]// ACM Internet Measurement Conference.

ACM, 2017:242-253.

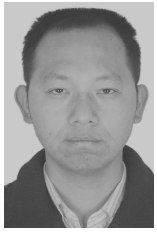
[59] MURDOCK A, LI F, BRAMSEN P, et al.Target generation for Internet-wide IPv6 scanning[C]// ACM Internet Measurement Conference. ACM, 2017:242-253.

[60] FIEBIG T, BORGOLTE K, HAO S, et al. Something from nothing (there): collecting global IPv6 datasets from DNS[C]// International Conference on Passive & Active Network Measurement. Springer, 2017:30-43.

[61] SALUTARI F, CICALESE D, ROSSI D J. A closer look at IPID behavior in the wild[C]// International Conference on Passive & Active Network Measurement. Springer, 2018:243-254.

[62] MARCHETTA P, DE DONATO W, PESCAPÉ A. Detecting third-party addresses in traceroute traces with IP timestamp option[C]// International Conference on Passive & Active Network Measurement .Springer, 2013:21-30.

[作者简介]



王占丰（1982− ），男，河北临城人，博士，东南大学在站博士后，主要研究方向为网络测量、网络性能分析与建模、网络安全。

程光（1973− ），男，安徽黄山人，博士，东南大学教授、博士生导师，主要研究方向为网络安全、网络测量与行为学及未来网络安全。

胡超（1984− ），男，江西吉安人，博士，解放军陆军工程大学讲师，主要研究方向为网络测量、SDN、网络空间安全等。

李晗（1986− ），男，四川成都人，博士，国家计算机网络应急技术处理协调中心高级工程师，主要研究方向为网络空间测量、网络基础资源管理。

翁年凤（1983− ），男，安徽天长人，博士，南京电讯技术研究所工程师，主要研究方向为数据工程、Web 深度挖掘。

曹华平（1976− ），男，北京人，国家计算机网络应急技术处理协调中心高级工程师，主要研究方向为网络信息安全、互联网基础资源管理、可信网络等。