TORCH：通过隧道观测刻画无效路由过滤

Renrui Tian清华大学，北京，中国

Yahui Li*清华大学，北京，中国

Xia Yin清华大学，北京，中国

Han Zhang清华大学，北京，中国

Xingang Shi清华大学，中国北京

Zhiliang Wang清华大学，中国北京

arXiv:2603.29207v1 [cs.NI] 31 Mar 2026

摘要

为缓解 BGP 前缀劫持，资源公钥基础设施（RPKI）通过路由起源验证（ROV）提供前缀起源认证。尽管针对 IPv4 已开展了大量测量工作，但 ROV 在 IPv6 中的防护效果尚未得到系统评估。现有方法对无效路由传播的可观测性有限：它们通常依赖少量受控前缀，或无法全面刻画真实网络环境中的 RPKI无效路由过滤情况，从而削弱了评估的准确性。此外，IPv6数据平面固有的不透明性，也加大了开展可扩展且可靠的主动测量的难度。

本文提出 TORCH，这是一种用于测量 IPv6 中无效路由过滤情况的新型框架。它将开放的 6in4 隧道端点重新用作分布广泛的观测点，以进行全球测量。其核心是我们开发的一种跨平面推断技术，无需目标做出响应即可确定可达性。该方法能够刻画在不同路由场景下流量是否以及如何被引导至无效起源，从而深入评估 ROV 在现实世界中的影响。

我们的测量结果显示，约 27% 的自治系统已实现近乎全面的路由起源验证保护。然而，仍有若干较为宽松的一级自治系统将流量中转至无效起源，因而保留了相当大的攻击面。通过以此前缀为中心的分析，我们首次提供了经验证据，表明同长度前缀过滤造成的附带损害可能影响全球互联网的很大一部分。我们的研究结果指出了路由起源验证部署中的根本性漏洞，并强调网络运营商亟须加快资源公钥基础设施的采用。我们公开了数据集。

CCS概念

• **安全与隐私 → 网络安全**。

关键词

资源公钥基础设施；路由起源验证；IPv6安全

1 引言

BGP 劫持。 互联网由数以万计相互连接的自治系统（ASes）组成，它们通过边界网关协议（BGP）交换可达性信息。在每个自治系统中，边界路由器会发出通告，声明如何到达其拥有的 IP前缀。然而，由于 BGP 本身不具备验证路由通告起源的机制，任何自治系统都可以谎称自己是其并未合法控制的前缀的起源，从而将发往该前缀的流量转移到自己的网络。这类事件被称为前缀劫持，在现实中时有发生 [13, 32, 36, 40, 50, 55, 56]。

基于 RPKI 的缓解措施。为缓解前缀劫持，IETF 对资源公钥基础设施（RPKI） [33],进行了标准化。该基础设施通过经加密签名的路由起源授权（ROA），将 IP前缀与其合法起源 AS 绑定。这些路由起源授权发布在全球可访问的 RPKI存储库中，并由依赖方（RP）验证器获取。要使 RPKI 提供有效保护，必须由路由器通过路由起源验证（ROV）主动使用已发布的路由起源授权。部署 ROV 的自治系统会配置其边界路由器，从 RP缓存获取已验证路由起源（VRP）载荷，并利用这些载荷对传入的 BGP 通告进行分类，丢弃未通过起源验证的路由。

ROV 部署有限。 RPKI 的有效性取决于正确签署的路由起源授权（ROA），以及各自治系统对路由起源验证（ROV）的一致执行。尽管近年来 ROA 的采用率快速增长，ROV 部署的推进却缓慢得多。这种有限的执行大幅削弱了 RPKI 的保护价值；要防止虚假通告传播，就必须由各自治系统一致地进行起源验证。近期测量结果 [30]表明，居住在会过滤 RPKI无效路由的网络中的用户地址不足 30 %。因此，全球路由基础设施中仍有相当一部分容易遭受潜在劫持，甚至受 ROA 保护的前缀

*Yahui Li 是本文的通讯作者。

仍可能被未实施 ROV 的网络错误路由。因此，了解 ROV 保护实际上在真实互联网的何处以及如何发挥作用至关重要。

ROV 测量中的缺口。准确评估某个自治系统的 ROV 状态并非易事，因为这需要根据外部观测推断其私有路由策略。此前的研究 [11, 28, 35, 49, 52]曾尝试推断 IPv4 中的 ROV 执行情况，但对 IPv6 中 ROV 状态的全面认识仍未实现。此外，这些研究存在固有局限，在迁移到 IPv6 时也面临重大障碍：

首先，现有方法受限于对无效路由传播的观测有限。它们通常依赖少量 RPKI 无效前缀，这些前缀要么由研究者自行托管 [14, 28, 30, 49, 52] ，要么是在实际网络中发现的 [11, 20, 35,58]。如此有限的一组无效前缀，无法涵盖无效通告可能经由哪些不同的上游提供商或对等互联关系到达待研究的自治系统，因此可能导致测量偏差，并对 ROV 保护作出错误评估。

其次，*IPv6*数据平面的固有不透明性阻碍了主动探测。庞大而稀疏的地址空间带来了严重的空间不透明性，使得难以在前缀内定位有响应的目标。即便发现了目标，它们也常因隐私扩展和临时寻址而转瞬即逝 [22, 43, 44]。这种时间不透明性会导致目标在探测步骤之间消失，从而增加测量工作量。此外，强制实施的 ICMPv6 速率限制 [26] 和显式过滤 [5, 16, 24] 会抑制响应，并导致跟踪中频繁出现缺失跳点 [1, 6]。这种拓扑不透明性阻碍了大规模高效测量。

贡献。随着 IPv6 流量迅速增长 [2, 18,23], ，评估整个 IPv6 互联网中的 BGP路由安全势在必行。我们认为，要准确刻画 IPv6 路由起源验证，必须满足三个基本要求：(1) 使用大规模观测点覆盖多样化的自治系统；(2) 充分了解无效路由传播，以全面描绘过滤行为；(3) 采用高效的测量技术，揭示不透明的 IPv6数据平面。为此，我们开发了 TORCH，这是一种用于测量 IPv6 中无效路由过滤的新型框架。具体而言，该框架利用开放的 6in4 隧道端点作为观测点，实现全球范围的测量。其核心是我们提出的一种跨平面可达性推断技术，该技术无需有响应的目标，并且能够抵御速率限制和过滤策略。借助该方法，我们能够刻画在各种路由场景中，流量是否以及如何被引导至无效起源，并捕获范围广泛的无效前缀。我们的主要贡献总结如下：

- **开放隧道的利用：**我们将开放的 6in4 隧道端点转化为能够执行 traceroute 测量的主动探测观测点，覆盖超过 2k 个网络。我们的工作为 IPv6 主动测量提供了全新的视角。
- **跨平面可达性推断：**我们推断可达性 - 通过将控制平面信息与数据平面轨迹相关联，推断前缀的可达性。这种方法无需在前缀内发现活跃目标，即使转发路径仅部分可见，也能进行稳健验证。该技术适用于 IPv4 和 IPv6 .
- **IPv6 路由起源验证的特征分析：**通过测量 200 多个活跃 RPKI 无效前缀的可达性，我们评估了 1,600 多个自治系统的 ROV 保护情况。研究结果表明，得到有效保护的自治系统不超过 27%，并量化了无效路由的实际传播情况，揭示了 IPv6 资源公钥基础设施部署中存在的显著不足。
- **RPKI 附带损害的证据：**我们首次提供了实证证据，表明相同长度前缀过滤造成的附带损害影响了全球互联网中的相当大一部分。为降低此类风险，我们强调有必要主动进行数据平面监控，以识别意外的可达性问题。

为便于复现并支持进一步研究，
我们将公开代码和数据集。

2 相关工作

2.1 被动测量

早期评估路由起源验证部署情况的工作主要依赖于对控制平面数据的被动分析。Gilad 等人 [20]证明，排名前 100 的互联网服务提供商几乎没有采用路由起源验证，这凸显出当核心网络不对无效路由进行过滤时，RPKI 的安全效益十分有限。后续研究 [57] 利用纵向 BGP 数据集评估 RPKI 注册的效益并追踪部署趋势，报告称无效路由过滤逐渐增加，尤其是在大型互联网服务提供商中。Du 等人 [17] 利用公共路由数据集，考察 MANRS 参与者是否遵循既定的路由安全要求。然而，Reuter 等人 [49] 提醒说，对控制平面的被动观测往往无法充分了解内部路由决策，可能导致错误识别启用路由起源验证的自治系统。

2.2 主动测量

为解决被动观测可见性有限的问题，后续研究转向主动测量，以主动测试资源公钥基础设施特定的路由行为。

通过受控前缀开展实验。一种主要的主动策略是，研究人员通告由其控制的前缀，同时故意注册相互冲突的路由起源授权（ROA），使其 BGP 通告无效。Reuter 等人 [49]

通过 PEERING 测试平台 [53],率先采用了这种方法，发现当时只有少数自治系统会持续执行过滤。后续研究 [27, 28, 52] 利用 RIPE Atlas 等分布式探测平台 [51], 将数据平面测量纳入其中。通过分析 traceroute 路径, 这些研究能够将过滤行为精细地归因于特定自治系统。

替代方案 [10, 14, 30]采用了更直接的方法：在数据平面测试其受控的 RPKI 无效前缀的可达性。Cloudflare 的 *Is BGPSafe Yet?* 项目 [14] 通过两个前缀提供网络资源，这两个前缀的路由属性完全相同，唯一区别在于其 RPKI 有效性。通过尝试获取这两项资源，该项目根据有效资源是否可访问而无效资源是否不可访问，识别基于 RPKI 的过滤。类似地，APNIC [30]通过在 Google Ads 中嵌入测量脚本，发起以用户为中心的测量。它引导最终用户的浏览器获取 RPKI 有效和 RPKI 无效信标，从而在全球范围内检测过滤行为。

利用真实网络环境中的无效前缀。为避免必须使用受控前缀，一些研究人员 [11,35] 利用互联网中的无效前缀。Chen 等人 [11] 收集了通往无效前缀的 traceroute 路径，并应用贝叶斯推断，估算数万个自治系统中的路由起源验证部署情况。Li 等人 [35] 利用 IP-ID 侧信道，在无需观测点的情况下推断远程主机到无效前缀的可达性，覆盖了超过 2.8 万个自治系统。

尽管取得了这些进展，现有测量对无效路由传播的观测仍然有限，因为它们依赖少量测试前缀，这也促使我们设计 TORCH。

3 概述

本节讨论在 IPv6 中实现大规模路由起源验证测量系统所面临的主要挑战，随后概述 TORCH 如何应对这些难题。具体而言，TORCH：（1）利用开放的 6in4 隧道端点作为观测点，实现大规模测量；（2）充分利用真实网络环境中的无效路由前缀，增强对无效路由传播的观测；（3）将数据平面观测与控制平面路由信息相关联，以准确推断前缀可达性。

3.1 关键挑战

我们的目标是通过推断自治系统针对无效路由的过滤行为，刻画其路由起源验证状态。为此，我们需要确定该自治系统是否仍能访问具有无效路由的前缀。然而，要开发稳健的测量框架，还需要应对以下几个关键挑战。

挑战一：缺乏大规模观测点。大规模测量面临的首要障碍是获取分布广泛的观测点。RIPE Atlas [51] 等平台虽然提供了宝贵的覆盖范围，但受基于积分的使用模型和严格配额的限制，导致测量吞吐量受到抑制。这些局限性削弱了在全球范围内生成无效路由过滤每日快照的可行性。

挑战 II：对无效传播的观测不足。现有测量仅依赖少量 RPKI 无效前缀，这些前缀要么是自托管的 [14, 28, 30, 49, 52] ，要么来自真实网络环境 [11, 20, 35, 58]。然而，如此有限的无效前缀集合只能让我们有限地了解无效路由传播，因为它无法涵盖其他无效通告可能经由哪些不同的上游网络或对等网络传播至受测自治系统。

为扩大可能路由路径的覆盖范围，RoVista [35] 利用真实网络环境中的无效前缀，而 APNIC [30] 则采用另一种方法，使用 Cloudflare 在其遍布全球的众多接入点运行的 RPKI信标。这两项工作都旨在减少上游过滤带来的测量偏差，并更全面地了解 ROV 保护情况。然而，RoVista 最近的测量显示，可用无效前缀的数量随着时间推移有所减少，通常不足五个，有时甚至仅剩两个。无效前缀如此稀缺，极大地削弱了 ROV评估的可靠性。

挑战 III：IPv6数据平面的不透明性。要确定通往目标前缀的可达性，一种直接的方法是在该前缀内找到一个活跃地址，并在数据平面上对其进行探测。然而，与 IPv4 不同，由于 IPv6 地址空间和网络拓扑本身具有不透明性，有效主动探测在 IPv6 中要困难得多。

缺乏可发现的活跃目标。由于地址空间庞大且人口稀少，IPv6 前缀内的可响应地址本就难以发现，这归因于其空间上的不透明性。对于仅包含无效路由的前缀，这一难题更加突出。由于一些中转网络如今已实施路由起源验证（ROV）并过滤无效通告，这些前缀获得的路由传播有限，因此可见性较低。因此，对于位于过滤网络之后的观测点而言，这些前缀在数据平面上基本无法到达，也就极难在其中找到可响应主机。

短暂且不稳定的地址。即使在某个前缀内识别出有响应的目标，它们也往往转瞬即逝，因为隐私扩展和临时地址的使用 [22, 43, 44]。这种时间上的不透明性 使这类目标不适合用于测量，也增加了

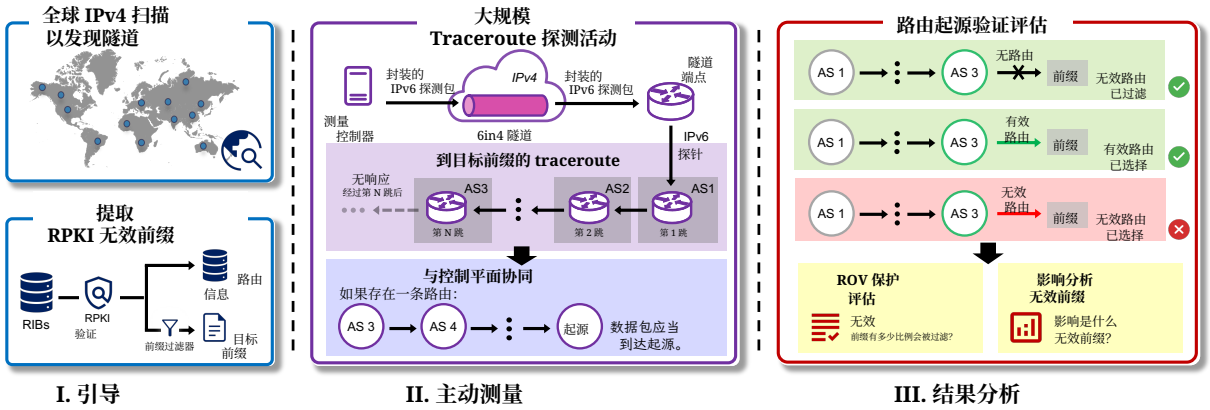


图 1：TORCH 概览。

发现可用活跃主机所需的工作量，因为目标可能会在测量步骤之间消失。

强制速率限制与 *ICMP* 过滤。 traceroute 等工具依赖 ICMP 错误消息逐跳解析转发路径。然而，强制速率限制 [26] 会抑制大量 ICMPv6 响应，并已被证实会导致追踪结果中频繁出现缺失跳点 [1, 6]，表现为拓扑不透明性。这带来了一个根本性的权衡：尽管大规模测量离不开较高的探测速率，但这会触发激进的速率限制，反而损害跳点的可见性。此外，网络运营商主动进行的 ICMP 过滤也加剧了路径透明性的缺失 [5, 16, 24]。

3.2 系统设计

为系统性地应对上述挑战，TORCH 纳入了三个核心设计组件。

设计 I：将宽松隧道重新用作观测点。 为解决观测点稀缺的问题，TORCH 策略性地利用开放的 6in4 隧道端点。我们识别出托管于缺乏出站源地址验证（SAV）的网络中的宽松端点，并利用其固有的转发能力注入测量探针。这种方法有效地将被动基础设施节点转变为主动的远程观测点。借助隧道的广泛分布，我们实现了覆盖 2k 多个自治系统的广泛范围。此外，我们的工作还确立了一种利用 6in4 隧道端点进行主动测量的有效实践。

设计 II：最大限度发挥互联网中无效前缀的效用。 TORCH 通过最大限度发挥互联网中无效前缀的效用，提升了对无效路由传播的可见性。我们大幅扩展了候选前缀的范围，纳入了先前研究通常认为不可用的无效前缀 [11, 35]。具体而言，TORCH 纳入了 (i) 无法发现任何可响应主机的完全无效前缀，(ii) 存在相互竞争的有效路由（即 MOAS 冲突）的无效前缀，以及 (iii) 被较不具体的有效路由覆盖的无效前缀。这使 TORCH 能够观测来自广泛无效起源的路由传播，从而全面刻画无效路由过滤。

设计 III：通过跨平面路径对齐推断可达性。 TORCH 首创了一种跨平面路径对齐策略，用于推断前缀可达性。TORCH 不会分别检查各个平面，而是协调数据平面探测与控制平面路由信息，促成二者协作。这种方法将验证从 IP 级响应能力提升到自治系统级路径可见性，并利用路由知识弥补数据平面上的观测缺口。这种协作式设计摆脱了对可发现活跃目标的依赖，使 TORCH 即使在只能部分观测到的跟踪记录中，也能稳健地刻画前缀可达性。

总之，TORCH 提出了一种用于刻画 IPv6 中无效路由过滤的框架，如图 1 所示。首先，它利用开放的 6in4 隧道端点作为全球观测点，并从路由信息库（RIB）数据中识别出一组多样化的 RPKI 无效前缀。接下来，TORCH 针对目标前缀开展大规模 Traceroute 探测活动，并运用跨平面推断来确定流量是否被传送到无效起源。最后，TORCH 支持对 ROV 保护进行以自治系统为中心的评估，并对无效前缀的现实影响开展前缀中心分析。

4 方法

本节详细介绍 TORCH 的实现。我们将阐述利用 6in4 隧道

端点的技术细节、跨平面可达性推断的机制，以及为最大限度地利用真实网络环境中的无效通告而采用的严谨策略。

4.1 利用 6in4 隧道

为了获得多样且分布广泛的测量观测点集合，我们利用了实际网络中可用的 6in4 隧道端点。具体而言，我们识别出托管在未实施 IPv6 出站 SAV [54],的网络中的端点，并将这些宽松的隧道节点重新用作观测点，以开展数据平面测量。

4.1.1 宽松的 *6in4* 隧道端点。6in4 协议 [21]是一种隧道机制，可将 IPv6 数据包封装在 IPv4 数据包中。收到封装数据包后，6in4 端点会移除外层 IPv4 首部，并根据其 IPv6 路由状态转发内层 IPv6 数据包。尽管随着原生 IPv6 部署的广泛普及，6in4 的实际作用有所降低，但以往的测量 [25, 31] 表明，许多开放的隧道节点仍在实际网络中保持活跃。

出站源地址验证旨在防止网络使用伪造的源地址发出数据包。尽管出站源地址验证能够有效缓解 IP 欺骗，但以往工作 [25]和我们的测量都表明，出站过滤普遍缺失：大多数检测到的 6in4 隧道都托管在缺乏出站源地址验证的网络中，这意味着它们可以转发源地址任意的 IPv6 数据包。这种宽松行为使我们能够构造用于主动测量的 IPv6 探测包，并通过 6in4 隧道发送这些探测包。

4.1.2 使用隧道端点进行 *traceroute*。已知一个缺乏出站源地址验证的 6in4 隧道端点后，我们可以利用其 IPv6 路由能力，从托管该端点的自治系统的视角执行 IPv6 路由跟踪。实际上，该端点会转发我们的探测包，就好像这些探测包是在本地发出的一样，使我们能够观察从其网络到任意目标的跟踪路径。

对于每个跳数限制，我们都会构造一个 ICMPv6 回显请求，将服务器的 IPv6 地址设为源地址，并将待测试目标设为目的地。然后，我们用 IPv4 首部封装 IPv6 数据包，将服务器的 IPv4 地址设为外层源地址，将端点的 IPv4 地址设为外层目的地址。端点收到数据包后，会剥除外层 IPv4 首部并转发内部的 IPv6 探测包，从而在其自治系统内部发起 traceroute。由于探测包的 IPv6 源地址设为我们的服务器，沿途生成的任何 ICMPv6 响应（例如 超时、目的地不可达或回显应答）都会直接返回给我们。这使我们能够重建从端点到目标的路由路径。

4.2 跨平面可达性推断

我们提出了跨平面可达性推断技术，这是一种路由-连通性混合方法，将控制平面的路由信息（路由）与数据平面轨迹（连通性）相结合。该技术使我们无需依赖可响应主机即可确定某个前缀的可达性，从而克服 IPv6数据平面的不透明性。我们的方法基于两个关键观察：

自治系统级可见性的韧性。首先，我们观察到，尽管 *IPv6* 路由跟踪经常因速率限制或过滤策略而出现缺失跳点，但自治系统级可见性的韧性相对更强。数据包穿越 transit AS 时，通常会由多个路由器依次转发。尽管个别路由器可能会抑制 ICMP 消息的生成，但仍很有可能收到来自该自治系统内部的至少一条回复。因此，即使跳级跟踪不完整，在自治系统层面观察到的转发路径仍具有更高的完整性。

利用控制平面信息弥补可见性缺口。其次，我们利用一个关键洞见：控制平面路由信息能够有效弥补数据平面可见性方面的缺口。现在我们关注 AS 粒度，因此可以通过观察数据包是否进入起源自治系统来验证前缀可达性。然而，追踪路径中仍可能缺少某些自治系统，尤其是在高频测量活动期间，激进的探测可能触发更严格的速率限制。这意味着，来自某个自治系统的所有响应都可能被抑制，导致该自治系统未出现在路径中。当末端自治系统不响应时，这种不透明性尤其棘手，因为仅依赖数据平面视图，就无法区分真正的不可达与速率限制或过滤措施导致的无响应。幸运的是，我们注意到，公共 BGP 平台收集的路由数据有助于厘清这种模糊情况。我们的推断基于控制平面通告与数据平面转发之间的一致性。具体而言，如果观察到数据包进入某个自治系统，且该自治系统被观察到拥有通往目标前缀的路由，那么该数据包就属于该自治系统的主动转发逻辑，预计会被路由至目的地。因此，即使后续的数据平面路径不可见，控制平面仍能确认该自治系统有意愿且有能力将数据包路由至目的地。

基于上述见解，我们实现了一种协同推断机制，将数据平面中观察到的入口点与控制平面所保证的转发连续性 相关联。该过程分为两个阶段：

1. 数据平面锚定。 我们向目标前缀内的一个随机地址发起 traceroute 探测。我们不要求目标主机处于活动状态；相反，我们的目标是提取转发路径中可见的部分。通过将有响应的 IP 跳点映射到自治系统编号，我们重建经过的网络序列，并建立一个数据平面

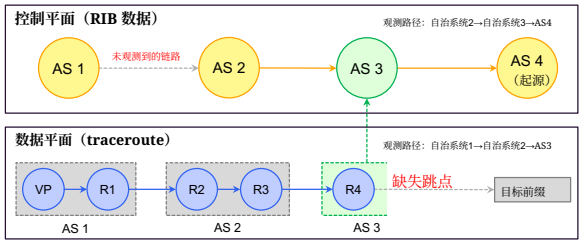


图2：跨平面可达性推断：将部分数据平面跟踪记录与控制平面路由路径相关联，以确定可达性。

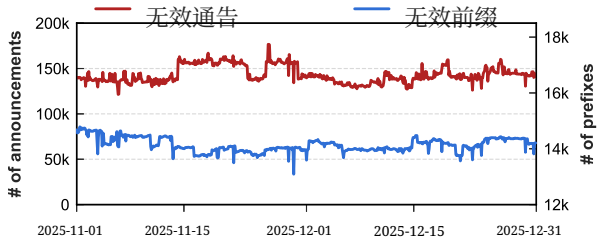


图3：无效前缀和无效通告的数量。

锚点， 以确认观测到的最远转发点。

2. 控制平面外推。 随后，我们通过将锚点与全球 BGP RIB 数据进行交叉比对来验证可达性。我们汇总控制平面通告的通往目标前缀的 AS 路径。如果数据平面锚点出现在任何控制平面路径中，就推断该前缀可达。这种对应关系表明，数据包已成功移交给承诺将其转发至目的地的自治系统，从而弥合了数据平面下游静默造成的差距。

图2展示了一个协作示例，我们在其中测试由 AS4 起源的前缀。我们从 AS1 的一个观测点向该前缀发起 traceroute，并将有响应的跳点映射到一条 AS路径。如图所示，由于存在缺失跳点，数据平面跟踪在 AS3 处提前终止，因此我们将 AS3 识别为锚点。通过查询控制平面，我们确认该锚点出现在一条有效的路由路径 AS2 AS3 AS4 上。确认数据包到达锚点，再结合控制平面所提供的下游连通性保证，足以支持可达性的推断。

值得注意的是，由于锚点之后的转发路径不可见，我们无意确定静默跳点中潜在的可达性问题（例如路由环路、黑洞或 ACL规则）。相反，我们的主要目标是验证源网络的转发意图，而这一推断为我们的研究提供了足够的粒度。

4.3 重新审视野外的无效前缀

为了全面评估无效路由过滤，我们尽可能利用真实网络环境中带有无效通告的前缀。图3显示，通告无效路由的起源自治系统数量保持稳定，对应的无效前缀数量也始终稳定。这种长期稳定性确保了我们的测量拥有可靠且一致的目标集。

4.3.1 仅限于有响应的无效前缀。使用 RPKI 无效前缀进行 ROV 测量时，若不

加以谨慎筛选，就可能引入显著偏差。正如先前研究所指出的 [11, 35], , 与无效路由相关联的前缀，如果存在替代有效路由，在实施 ROV 的自治系统中仍可能保持可达。这通常出现在两种情形下：

(1) 竞争性有效起源 *(MOAS)*：某个前缀可能同时由另一个拥有有效ROA的自治系统通告。这样，流量便可以通过有效路由转发至合法起源。(2) 覆盖性有效路由：合法起源会通告一个较不具体的前缀。如果更具体的无效路由被过滤，覆盖性有效路由便可提供备用转发路径，维持可达性。

在这些场景中，可达性观测会变得模糊：如果启用了路由起源验证（ROV），流量可能会通过有效路由转发至合法起源；如果无效路由被接受，流量则可能被送至未授权起源。因此，仅凭可达性无法区分这两种截然不同的转发行为。

为避免误解，先前的测量 [11,35, 58]将分析限制在仅由无效起源通告的前缀，并要求每个前缀内都存在可响应的目标，以便进行数据平面探测。然而，这两个限制大幅缩小了可用的测量范围。实际上，候选前缀池大幅缩减，因为许多完全无效前缀中没有任何可响应的目标。例如，近期的 RoVista 测量 [35] 在 IPv4 中的 1,098 个完全无效前缀里，仅能使用两个测试前缀。

4.3.2 迈向无效前缀的完整刻画。 我们认为，可用目标前缀稀缺，主要源于传统数据平面探测固有的局限性：它要求前缀内存在可响应主机，而且当有效路由和无效路由同时存在时，无法区分实际承载流量的是哪条路由。相比之下，我们的跨平面推断带来了显著优势，它将可达性与主机响应性分离，并提供足够的 AS 级可见性，以消除转发

路径的歧义。克服这些障碍后，我们便能充分利用仅无效前缀，并从此前被舍弃的复杂场景中重新找回可用前缀。我们将无效前缀分为三类：

类型 I：仅无效前缀。此类别由仅由无效起源通告、且既不存在并发有效通告也不存在有效覆盖前缀的前缀组成。由于不存在有效路由，在此情境下，可达性可作为不存在 ROV 过滤的确定性指标。通过采用跨平面推断机制，TORCH 无需发现活跃主机或开放端口，即可准确确定这些前缀的全部可达性。

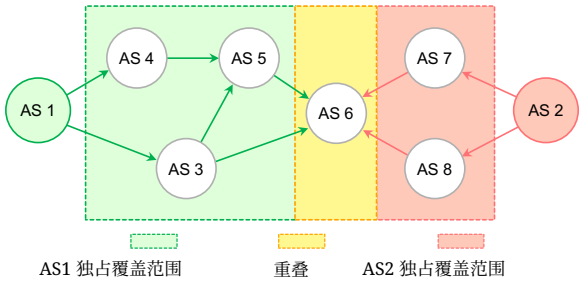


图 4：基于汇聚域消歧的示意图。仅当数据平面锚点位于未授权起源（AS2）的独占汇聚域（红色区域）内时，我们才推断其可达性；位于重叠区域（黄色区域）的锚点则被丢弃。

类型 II：具有相互竞争的有效起源的前缀。在这种情况下，无效通告与一个具有相同前缀长度的有效通告并存。简单的连通性测试无法区分探针到达的是合法起源还是未授权起源，因为二者通告的前缀完全相同。

TORCH 利用一项关键观察消除了这种歧义：相互竞争的起源通常会形成不同的覆盖区域（即基于 BGP 路径选择、选择并将流量转发至特定起源的一组自治系统）。我们通过汇总控制平面上的全球路由信息，明确划定覆盖区域及其对应的起源。为确定目的地，我们改进跨平面推断，以识别位于特定覆盖区域内的数据平面锚点。鉴于覆盖区域可能重叠，只有当该锚点能够被唯一归属于无效起源的覆盖区域时，我们才确认流量遵循了无效路径。这种保守的验证方式可确保探针遵循的是无效路由。

图 4 展示了这一过程。假设 AS1 是合法起源，AS2 是未经授权的起源。拓扑被划分为三个不同的区域：AS1 的独占汇聚域（绿色区域）、AS2 的独占汇聚域（红色区域）以及重叠区域（黄色区域）。为避免不确定性，我们仅在锚点位于无效起源的独占汇聚域（红色区域）内时，才推断其可达性。例如，位于 AS7 的锚点可作为到达 AS2 的确凿证据，而位于重叠区域内的 AS6 则会被舍弃。

类型 III：具有有效覆盖路由的前缀。在此情境下，具有无效路由的更具体前缀由具有有效路由的较不具体前缀覆盖。尽管根据最长前缀匹配，更具体的路由应优先处理，但如果两条路由共享相同的 AS 路径片段，有效覆盖路由的存在可能会掩盖无效路由。在这种情况下，沿无效路由转发的流量会经过与覆盖性有效路由相同的自治系统。这种拓扑重叠使得无法明确判定可达性是否由无效路由所致。

TORCH 采用三项约束，以确保归因严谨。首先，我们排除无效路由和有效覆盖路由的起源自治系统在拓扑或管理上相互关联的前缀（例如存在客户—提供商关系、共同上游，或属于同一组织）。其次，我们采用为类型 II 引入的基于覆盖区域的策略，仅在未观察到覆盖性有效路由的覆盖区域内推断无效路由。第三，如果观察到数据包经过较不具体前缀的起源自治系统，或该起源自治系统的直接上游提供商，我们便推断流量可能会先到达较不具体前缀的起源自治系统，再通过专用骨干网或其他互连网络传送至目的地。在这种情况下，观测到的可达性应归因于覆盖性有效路由。

通过采用这些精心设计的策略，TORCH 显著拓展了可测量的无效起源范围。这种可见性的提升，为更全面、准确地评估 ROV 过滤奠定了基础。

5 测量

本节介绍测量活动的端到端工作流程。我们详细说明如何构建基于隧道的观测点基础设施、选择包含无效路由的目标前缀，并启动大规模 traceroute 探测，以供后续分析。

5.1 获取隧道端点

为建立我们的观测点基础设施，我们遵循 [25]中确立的发现方法，并对整个 IPv4 地址空间进行全面扫描。此过程发现了 1,048,273 个宽松隧道端点，规模与 [25]相当。随后，我们分析这些端点的地理分布和 AS归属，从而评估观测点的覆盖范围和多样性。

IPv4 分布。 我们使用 RouteViews 前缀到自治系统映射数据集 [9]，将已识别的端点映射到 2,116 个不同的 IPv4 自治系统。通过斯坦福 ASdb 数据集 [60] 进一步分析发现，其中 1,828 个（86.4%）自治系统属于互联网服务提供商，这表明我们的观测点有效覆盖了隧道端点主要部署于其中的接入网络和用户侧网络。在地理特征分析方面，我们使用 MaxMind GeoLite2 数据库 [41]，发现这些隧道端点遍布全球 115 个国家（如图 10 所示），由此实现广泛的互联网覆盖，并支持后续测量捕获不同地区的异质路由行为。

IPv6 归属判定。由于隧道端点的 IPv4 和 IPv6 接口可能由不同的自治系统提供，直接将它们的 AS 归属视为相同可能导致归属错误 [25]。为避免这一问题，我们进行了主动测量，以推断为每个隧道端点提供连接的 IPv6 自治系统。通过结合直接发现 IPv6 地址与基于 traceroute 的推断（详见附录 A），我们成功将 777,667 个（74%）隧道端点归属到 1,349 个 IPv6 自治系统。

5.2 RPKI 无效前缀特征分析

我们从 RouteViews [47] 获取最新的 BGP RIB 快照，以构建候选前缀。首先，我们清理原始路由表，排除与保留或私有 ASN 及前缀相关的路由。随后，我们使用 Routinator [45] 进行验证，以识别无效通告。为过滤本地路由策略和临时配置造成的伪影，我们仅保留其无效路由被三个以上采集器观测到的前缀，以确保所选前缀具有足够的全球可见性。

如第 4.3 节所述，我们会应用额外的筛选条件，以获得可靠的目标。首先，我们找出不存在任何对应有效路由的完全无效前缀。其次，使用自治系统到组织映射数据集 [12]，移除无效和有效起源 AS 属于同一组织的前缀。第三，对于多起源自治系统前缀，如果无效和有效覆盖区域的重叠超过 20%，则舍弃这些情况，因为覆盖区域分离度有限会削弱推断的可靠性。最后，对于具有有效覆盖路由的前缀，我们排除无效和有效路由紧密耦合的情况。具体而言，我们移除满足以下条件的前缀

：一个通告的起源出现在另一个通告的 AS 路径中，或者两条路由均经由同一上游提供商传播。

如表 1 所示，截至 2025 年 11 月 30 日，我们从 164 个无效起源中获取了 328 个前缀。为了评估测量目标的多样性，我们进一步分析了其地理覆盖范围和网络属性。

类别	前缀	比例（%）	起源 AS
仅无效	284	86.6%	134
仅 MOAS	16	4.9%	13
仅覆盖	22	6.7%	20
MOAS 与覆盖	6	1.8%	5
总计	**328**	**100.0%**	**164**

表 1：截至2025年11月30日，目标前缀及其唯一起源自治系统的统计数据。

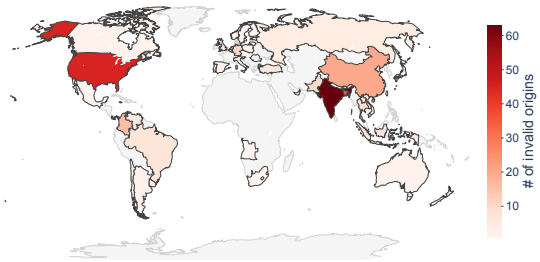


图 5：为目标前缀发布无效路由的自治系统的全球分布。

地理分布。如图 5 所示，无效起源遍布所有主要地区，呈现全球分布。值得注意的是，我们发现无效起源的密度与各地区 IPv6 部署程度相关。在印度、美国和中国等 IPv6 部署较为先进的国家，无效起源的集中度明显更高。相比之下，非洲地区的无效起源 AS 数量很少，该地区的 IPv6 发展总体上较为滞后。

网络特征。 我们根据网络类型和层级位置考察无效起源。利用斯坦福 ASdb 数据集 [60],，我们发现164个无效起源中有98个（60%）是互联网服务提供商。随后，我们使用 CAIDA AS Rank 数据集 [8]获取它们的排名。结果表明，这些自治系统覆盖了广泛的层级范围，从主要的一级和二级提供商，到规模较小的区域互联网服务提供商和末梢网络。

这种广泛的地理覆盖范围和层级多样性确保测量不会受到区域策略或网络层级的偏斜影响。通过面向多样化的起源，从大规模中转服务提供商到区域边缘网络，我们可以系统地刻画无效路由如何在异构网络中传播和被过滤。

5.3 大规模 traceroute 测量

我们从分布广泛的隧道端点向目标前缀开展大规模 traceroute 测量。尽管我们的跨平面可达性推断旨在具备韧性，但若直接

将来自数百万个源、面向数百个目的地的路由跟踪规模化，会产生难以承受的开销，并加剧速率限制，进而可能掩盖响应并使推断产生偏差。为在覆盖范围与探测效率之间取得平衡，我们通过策略性地选择目标前缀和观测点来优化测量设置。

目标聚类。我们将控制平面等效的候选前缀聚类，以减少冗余。具体而言，我们将所有路由收集器中 AS 路径均相同的前缀分组，并从每个簇中选取一个代表性前缀进行主动探测。这样可以避免冗余探针，并将探测预算集中用于不同的网络。

观测点采样。我们首先剔除会修改内层数据包首部的隧道节点（例如，重写源地址或重置跳数限制的节点），因为此类行为会破坏 traceroute 语义，并妨碍可靠的 ICMP 响应关联。随后，我们根据剩余节点的 IPv6 自治系统编号进行分层；也可以改用其 IPv4 自治系统编号或前缀进行分层，并从每组中随机抽取至多三个观测点。

最终，所得配置平均每天涉及 5,316 个隧道节点和 216 个目标前缀。

为了在限制探测开销的同时确保大规模推断的可靠性，我们精心安排了 traceroute 探测活动的执行。我们将 traceroute 探针的最大跳数限制设为 20；根据实测，这足以捕获大多数域间路由路径。为防止流量突发并缓解速率限制，我们对所有源与目的地组合采用轮询调度。最后，我们执行多轮探测，以加强跳点发现并缓解暂时性的网络问题。

5.4 评估 ROV 保护

与先前工作一致 [35], ，我们引入*ROV* 得分 ，用于量化针对无效路由的过滤效果。我们不推断某个自治系统是否明确部署了路由起源验证，而是评估其抵御能力 ，即抵御无效路由传播的能力。具体而言，ROV 得分定义为这样一部分目标前缀所占的比例：来自该自治系统的流量无法到达无效起源。得分越高，表示大多数前缀的无效起源均不可达，表明其保护能力强；无论这种保护是由自治系统在本地实施，还是继承自上游网络的过滤。反之，得分较低则表示流量仍可

被引导至许多前缀对应的无效起源，这表明转发路径上的过滤能力较弱或不一致。

6 结果

本节介绍我们于2025年12月17日至2025年12月27日期间开展的大规模 traceroute 测量活动结果。

6.1 ROV 全球状态

我们首先考察所测量 IPv6 网络中 ROV 保护的总体状态。在测量期间，TORCH 捕获了2,061个自治系统，其中包括承载隧道端点的网络，以及沿转发路径观测到的中间自治系统。对于中间自治系统，由于我们无法从这些网络发起探针，因此只能观测到那些相应 traceroute 恰好经过该网络的特定目标前缀。为确保推断结果稳健，并减轻采样不足造成的偏差，我们将分析范围限定为至少能够评估其到20个目标前缀可达性的自治系统。最后，我们重点分析由1,685个自治系统组成的整合数据集。

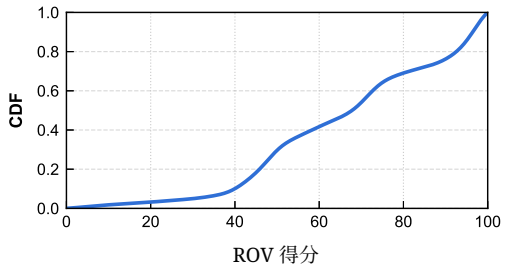


图 6：所有测量自治系统的 ROV 得分累积分布函数。

6.1.1 ROV 得分分布。图 6 展示了测量自治系统的 ROV 得分累积分布函数。26.9% 的自治系统获得了接近完全保护的得分（> 0.9），有效地丢弃了大多数目标前缀的无效路由。相比之下，30.4% 的自治系统表现出宽松的策略，得分低于 0.5。这些网络允许流量到达超过半数目标前缀的无效起源，因此极易受到 BGP 劫持威胁。其余自治系统则仅提供部分保护，这可能归因于上游过滤不一致或选择性执行。正如 [35],所述，此类行为往往源于基于关系的例外（例如，接受来自客户的无效路由）、本地覆盖（例如，SLURM [38]）或部署过程中遇到的运维挑战。

6.1.2 各大洲的 *ROV* 状态。我们研究了各大洲的 ROV 概况。如图 7 所示，各地区的 ROV 得分差异显著。北美洲和欧洲的得分偏高，表明保护措施总体上较为一致。亚洲和南美洲的得分分布则宽泛得多，整体保护水平中等。由于覆盖范围有限，大洋洲和非洲的结果应谨慎解读。在可测量的范围内，大洋洲往往呈现较高的 ROV 过滤水平，而非洲的保护水平则中等。总体而言，这些发现

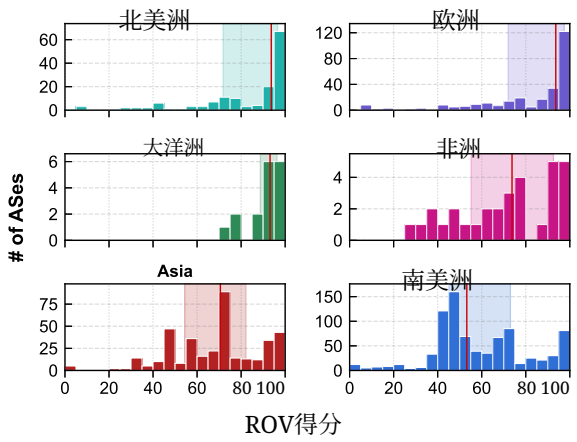


图 7：按大洲划分的路由起源验证得分分布。红线表示中位数，阴影区域表示各地区从第一四分位数（Q1）到第三四分位数（Q3）的范围。

证实全球 ROV 状态仍存在地域差异。

6.2 宽松的一级自治系统

一级自治系统构成互联网骨干网，对全球路由安全至关重要。先前的研究 [20, 28, 35]强调，资源公钥基础设施带来的安全效益主要源于核心网络中执行路由起源验证所产生的连带影响。作为通用的中转服务提供商，它们的过滤策略实际上决定了无效路由如何从核心网络传播至全球互联网。因此，我们评估了 17个一级自治系统中的路由起源验证效果。

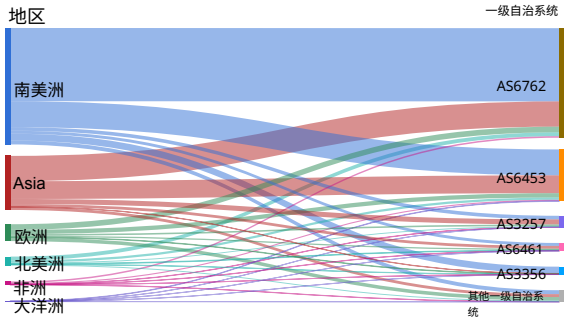


图8：多个宽松的一级自治系统将来自不同地区的流量中转至无效起源，使无效起源在其服务地区内保持可达。

6.2.1 一级自治系统之间的 *ROV* 执行并不一致。表2总结了 TORCH 测得的 17 个一级网络的 ROV 状态。少数一级自治系统几乎全面执行 ROV。例如，德国电信（AS3320）、Verizon（AS701）和 AT&T（AS7018）会过滤掉几乎所有无效路由。然而，这种严格的保护并未普遍存在于一级网络中。许多运营商仍然采用宽松的过滤策略。值得注意的是，观测发现 Level 3（AS3356）会将流量转向无效起源，涉及超过一半的目标前缀。

互联网核心网络中路由起源验证执行情况不一致，给全球路由安全带来了系统性风险。如图8所示，若干宽松的一级自治系统负责将流量从各大洲转发至无效起源。由于未严格采用路由起源验证，这些网络仍能保持对无效起源的可达性，并使这种可达性扩散至其广泛的服务区域。默认路由的普遍使用 [7, 35]进一步加剧了这一漏洞：即使某个自治系统在本地执行路由起源验证，流量仍可能通过默认路由被导向不进行验证的上游提供商，进而削弱本地过滤的效益。

Rank	自治系统编号	组织	得分
1	3356	Level 3 母公司 , LLC	40.2%
2	1299	Arelion Sweden AB	50.0%
3	174	Cogent Communications	73.6%
4	3257	GTTCommunications Inc.	70.6%
5	2914	NTT America, Inc.	90.8%
6	6939	Hurricane Electric LLC	52.4%
7	6453	TATA Communications	71.4%
8	6461	Zayo Bandwidth	92.4%
9	6762	Telecom Italia Sparkle	59.6%
11	3491	PCCW Global , Inc.	69.6%
12	5511	Orange S.A.	96.4%
14	12956	TELXIUS Cable	89.0%
20	3320	德国电信股份公司	99.1%
30	6830	Liberty Global	95.7%
31	7018	AT&T Enterprises, LLC	98.7%
33	701	Verizon	98.7%
101	209	CenturyLink Communications, LLC	97.6%

表2：一级自治系统的 ROV 分数。其中一些自治系统的 ROV 保护水平异常低。

6.2.2 与 *IPv4* 的比较。 为更好地理解我们的发现，我们将 IPv6 测量结果与近期关于 IPv4 路由起源验证（ROV）测量的研究进行比较。RoVista [35] 报告称，17个一级自治系统中有16个展现出较强的 ROV 保护，对 IPv4 核心网络给出了乐观的评估。然而，我们的发现更接近 [28], 的保守评估：该研究仅在

15个一级网络中的9个发现了明确的 ROV 执行证据。这表明，RoVista 可能高估了 IPv4 ROV 的成熟度，这或许归因于其使用的测试前缀有限。借助数量更多的无效前缀，TORCH 揭示了更严峻的情况：无效路由过滤部署不一致，使 IPv6 骨干网整体上仍易于接受无效路由，因而容易遭受前缀劫持。

6.3 结果验证

现有的路由起源验证测量研究主要关注 IPv4。对于 IPv6，我们发现 APNIC 测量项目 [30]提供了路由起源验证过滤的纵向基准数据。因此，我们使用 APNIC 的结果来验证我们的发现。

6.3.1 一级自治系统的验证。我们首先针对拥有充足 APNIC 样本的一级自治系统评估 TORCH。对于过滤率稳定在 99% 以上的网络（ AS3320 、 AS7018 、 AS701 和 AS6830 ），TORCH 始终给出较高的路由起源验证得分。对于过滤情况波动较大、且多次观测结果远低于 90% 的网络（AS174、AS3356 和 AS1299），TORCH 能准确识别出这些网络的保护并不完善。

由于 IPv6 的 APNIC 采样较为稀疏，我们尝试参考 APNIC 的 IPv4 基准数据。AS3257、AS3491、AS6453 和 AS6762 中观察到的 IPv4 过滤不稳定或过滤率较低，这表明它们在 IPv6 中可能也部署了不完善的路由起源验证。相反，对于 AS12956 和 AS5511，其 IPv4 过滤始终完整，可间接证明它们严格执行路由起源验证。对于这些网络，TORCH 弥补了一个关键的测量缺口，为其 IPv6 路由起源验证状态提供了稳定的评估。

我们的发现与 APNIC 基准数据之间存在若干差异，这凸显了基于单个前缀进行测量的局限性：这类测量通常只能局部反映 ROV 保护情况。相比之下，TORCH 通过评估对多种无效起源的可达性，能够更全面、准确地评估 ROV 实践。一个典型案例是 AS6939：APNIC 报告显示，其 IPv6 过滤率大多处于 90% 至 100% 之间，过去两个月中仅有一次降至 80%。然而，我们的 traceroute 结果显示，在 18% 的测量日中，AS6939 能够到达 Cloudflare 的无效前缀。这表明，APNIC 的评估可能受到其依赖 Cloudflare 运营的单个无效前缀这一做法的偏倚。类似地，我们持续观察到 AS6461 和 AS2914 能够到达 Cloudflare 的前缀，尽管它们会过滤大多数其他无效路由。对于 AS209，APNIC 报告的 IPv6 过滤率大幅波动，范围为 50% 至 90%；而 TORCH 观察到，在大多数情况下，过滤均有效。鉴于 AS209 在 IPv4 中始终保持较高的过滤率，我们推断其在 IPv6 中也实施了 ROV，但部分接口似乎不会过滤 Cloudflare 的前缀。

6.3.2 大规模验证。我们将验证范围扩大到 686 个自治系统，每个自治系统至少有 10 个 APNIC 样本。采用 90% 的 ROV 得分和 APNIC 过滤率阈值，我们将每个自治系统划分为完全或不完全受保护，并评估两组标签的一致性。结果显示，TORCH 与 APNIC 对 586 个自治系统（85.4%）的判定一致，其中包括 518 个被正确识别为未受保护的自治系统，以及 68 个经确认严格执行 ROV 的自治系统。

其余 100 个差异（14.6%）凸显了 APNIC 评估的局限性。在 83 个案例中，TORCH 识别出正在执行 ROV 的自治系统，而 APNIC 却将其标记为未受保护。详细调查 traceroute 结果后，我们发现，这些自治系统中有 71 个（85.5%）没有过滤 Cloudflare 的无效前缀，尽管它们成功阻止了其他测试前缀。此外，APNIC 显示有 17 个自治系统正在执行 ROV，但 TORCH 的测量结果表明其过滤并不完整。这些结果表明，基于单个前缀的测量可能会高估或低估 ROV 保护程度，而 TORCH 能够更稳健、全面地刻画 ROV 过滤情况。

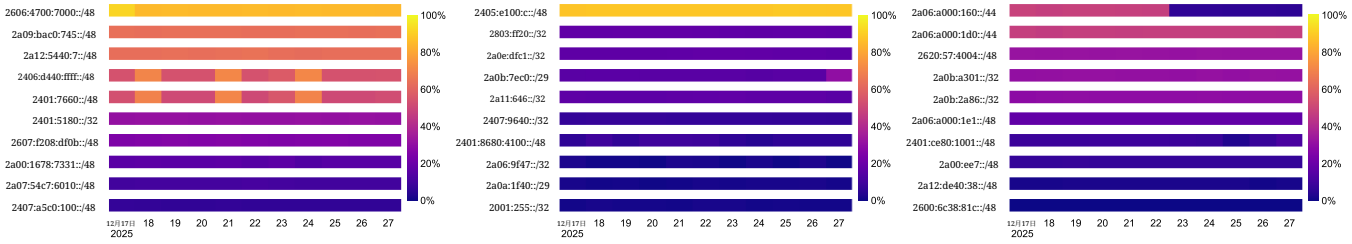
7 无效起源可达性

本节将进行前缀中心分析，以评估 ROV 过滤对 RPKI 无效前缀可达性的影响。为此，我们引入一个前缀级指标 无效可达性，用于刻画流量最终被送达无效起源的程度。具体而言，对于每个前缀，我们将无效可达性计算为数据包被转发至无效起源的自治系统所占的比例。

7.1 无效可达性的特征分析

如第 4.3 节所述，我们分析了三类 RPKI 无效前缀：(i) 仅无效前缀；(ii) 存在竞争起源的 MOAS 前缀；以及 (iii) 有较不具体的有效路由覆盖的前缀。对于每一类，我们随机抽取 10 个在测量期间始终可观测的代表性前缀。图 9 展示了这些前缀在测量期间的无效可达性。值得注意的是，若干前缀的可达性会随时间变化，我们在附录 B 中对此进行了详细分析。

7.1.1 完全无效前缀。完全无效前缀呈现出高度多样的无效可达性。如图 9a 所示，其可达性从完全隔离到全球范围内高度可达不等。低可达性可能表明，无效起源的上游提供商实施了 ROV 过滤；而许多其他前缀的高可达性则揭示了全球互联网普遍缺乏严格的 ROV 执行。例如，Cloudflare 从全球数百个接入点通告无效前缀 2606:4700:7000::/48。



(a) 完全无效前缀 **(b) 多起源自治系统前缀** **(c) 有效路由覆盖前缀**

图 9：三个类别中采样前缀的无效可达性热图。颜色表示随时间变化的、能够到达每个前缀无效起源的自治系统比例，揭示了不同前缀类型之间的显著模式。

（PoP） [48]。该前缀的无效可达性始终超过 84%，这意味着许多网络和互联网交换点（IXP）未能丢弃无效路由，使 BGP 劫持仍有很大的攻击面。

7.1.2 多起源自治系统前缀。图 9b 显示，多起源自治系统前缀的无效可达性通常低于 20%，仅有一个例外（2405:e100:c::/48）。这一结果可归因于 ROV 过滤，以及有效起源与无效起源之间的路由竞争。具体而言，即使某个自治系统不对无效路由进行过滤，其本地 BGP 决策流程仍可能优先选择合法路由（例如，由于本地优先级较高或 AS 路径较短），从而将流量导向有效起源。

7.1.3 有效路由覆盖前缀。对于被有效的较短前缀路由覆盖的无效前缀，我们观察到整体无效可达性处于中等水平（图 9c），高于多起源自治系统前缀。这是因为更具体的无效路由无需与相同长度的路由竞争，因而能够传播得更广，并且在转发过程中优先于较短的有效路由。

一个典型案例是前缀 2620:57:4004::/48。我们观察到，全球中转服务提供商 AS37468（Angola Cables）既接受了由 AS38345 发起、指向 2620:57:4004::/48 的无效路由，也接受了由 AS62831 发起、指向 2620:57:4000::/40 的有效路由。我们的测量还显示，AS37468 将来自 242 个下游自治系统的流量中转至无效起源，占所有观测到的发往该前缀的流量的 17.8%。此案例也凸显了核心中转网络中的路由起源验证实施缺口如何显著加剧子前缀劫持的影响，即使被劫持的前缀表面上受到 ROA 保护。

7.2 附带损害的真实影响是什么?

先前研究 [20, 34, 42] 已指出路由起源验证实践中的附带损害。这种情况发生在某个自治系统在控制平面上正确丢弃无效路由，但由于其上游提供商未实施路由起源验证，其流量仍被路由至无效起源。问题源于控制平面的路由选择与数据平面转发行为之间不一致。即使某个自治系统选择了有效路由，其上游仍可能依据本地路由策略（例如更具体的路由、本地优先级或 AS 路径长度）将流量转发至无效目的地。由于这种流量偏转发生在下一跳之后，且上游提供商的内部路由策略通常不透明，因此附带损害构成了一个隐蔽的攻击面，在控制平面上基本不可见。

为降低这种风险，现有研究 [34, 42] 通过检查上游网络的自治系统是否传播无效路由或实施路由起源验证，推断是否存在附带损害，并据此选择更安全的上游网络。然而，如果某个上游网络仅部分部署了路由起源验证，或只向邻居通告有效路由，同时在内部维持无效转发路径，这些研究就无法察觉。

重要的是，TORCH 能够细致地实证刻画流量是否以及如何被引导至无效起源，从而揭示控制平面观测无法发现的潜在附带损害。我们通过两个案例研究展示其在现实世界中的影响，并指出背后的原因。

7.2.1 案例研究 *I*：同长度 *MOAS* 前缀。我们调查了一个持续存在的 MOAS 异常，该异常涉及前缀 2405:e100:c::/48，其无效可达性始终超过 88%。该前缀由 AS137085（有效）和 AS132116（无效）同时通告。人工检查表明，这两个自治系统很可能由同一组织运营，而这一关系未被 [12] 识别。尽管

这种情况并无恶意，但它揭示了控制平面与数据平面之间的不一致如何助长隐蔽的同长度前缀劫持。

TORCH 发现，观测到的流量中有 67.9% 经由一级互联网服务提供商 AS6453 转发至无效起源。通过分析 RouteViews 的 RIB 数据 [47], , 我们发现 AS6453 广泛传播有效路由和无效路由：有效路由 P_v (AS6453 AS4755 AS137085) 经由 AS4755 到达有效起源，而无效路由 P_i (AS6453 AS9498 AS132116) 则经过 AS9498。我们的 traceroute 结果显示，收集到的大多数轨迹都与这两条路由一致：89.1% 的流量经由 AS9498 转发，而只有 10.5% 经由 AS4755 转发。其余流量（不足 0.5%）对应缺失跳点或其他路由。

为了解这一异常的普遍影响，我们将分析扩展至另外 15 个可测量的一级网络。我们发现，这些网络最终都会沿着 P_i 转发流量，其中包括 8 个几乎全面实施路由起源验证保护的网络；沿该路径转发的流量占它们发往该前缀的中转流量的 96.5%。然而，观测发现其中 14 个网络在控制平面上只有有效路由。这些发现表明发生了附带损害。为佐证这一观察，我们进一步考察 AS1299（Arelion）。通过其公开的 Looking Glass [59], , 我们确认纽约的一台路由器在其 RIB 中选择了 P_v，但来自同一台路由器的路由跟踪探测却沿着 P_i 转发，这与我们的测量结果一致。

我们的 traceroute 结果使我们能够量化附带损害的影响。我们总共发现了这些一级自治系统中 845 个受影响的下游网络。关键的是，鉴于我们的观测受隧道节点分布的限制，实际影响范围可能更广，甚至可能涉及这些一级提供商的整个客户锥。尽管如此，我们的发现足以证明其对全球造成了重大影响，这也凸显出，单个关键一级自治系统缺乏 ROV，便可能削弱整个互联网的集体验证工作。

总之，此案例展示了真实互联网中针对等长前缀的隐蔽劫持，并凸显了其安全影响：如果上游提供商同时维护有效和无效路由，执行 *ROV* 的自治系统仍容易受到攻击；宽松上游网络的内部路由策略可能会将数据包引向一个通往无效源站的出口点，从而削弱下游 *ROV* 过滤的效果。更重要的是，它首次证明了此类附带损害可能影响互联网的相当大一部分。

7.2.2 案例研究 *II*：被有效路由覆盖的更具体前缀。在本案例中，我们聚焦于前缀 2a06:a000:1d0::/44；在我们的测量期间，该前缀的无效可达性超过 46%。该前缀起源于 AS142594（无效），而其父前缀 2a06:a000::/32 起源于 AS58212（有效）。

我们发现 AS16117 和 AS18001 是附带损害的两个受害者。在 TORCH 和 APNIC 的评估中，这两个自治系统都表现出强有力的 ROV 过滤证据；而它们的提供商 AS12552 和 AS8966 则分别表现出不一致或较弱的过滤，这表明缺乏 ROV 执行。我们的分析证实，仅靠本地 ROV 工作不足以防止附带损害。

由于我们无法直接访问它们的路由表，因此通过从其隧道端点执行 traceroute 来推断它们的路由选择。具体而言，我们采用差分探测策略，分别探测无效 /44 前缀内的一个地址，以及有效 /32 父前缀（不包括 /44 范围）内的另一个地址。对于 AS16117，针对 /44 的探针经过 AS16117 AS12552 AS60800 AS142594，而针对 /32 的探针则经过 AS16117 AS12552 AS31027 AS58212。这表明 AS12552 是这两个前缀的传输服务提供商。我们还通过 NLNOG Looking Glass [46], 进一步验证，AS12552 接受并传播了无效路由。这些观察结果有力地证明了附带损害：对于 /44 前缀，尽管 AS16117 将流量转发至其上游网络，并预期流量会沿有效的覆盖 /32 路由转发，但 AS12552 接受并优先选择无效的 /44 路由，导致流量被导向无效起源。类似地，对于 AS18001，我们观察到几乎相同的附带损害模式。针对无效 /44 前缀的探针经过 AS18001 AS8966 AS60800 AS142594，而针对有效覆盖前缀 /32 的探针则经过 AS18001 AS8966 AS58212。

通过两个案例研究，我们展示了附带损害在真实互联网中的严重影响。除现有的防御方案外， [34, 42], 我们建议网络运营商对可能的异常前缀进行主动探测，并采用我们的可达性推断技术，主动评估无效起源造成的数据平面暴露。一旦发现未经授权的可达性，运营商即可及时采取措施，减轻其不利影响。

8 讨论

局限性。 尽管 TORCH 效果显著，但仍存在两个主要局限。首先，我们的分析依赖于前缀到 AS 以及 AS 到组织映射数据集的准确性 [9, 12]。这些数据源可能过时或存在错误，进而导致少量归属判断不准确。其次，traceroute 路径可能受到负载均衡和路由动态的影响而发生偏差。先前的研究 [3, 15, 19] 讨论过这些挑战，并提出了缓解技术，以提高路径重建的准确性。

超越先前工作。 回顾性分析表明，我们跨平面可达性推断背后的直觉，与早期一项网络可达性研究中探讨的观点相呼应 [37]。然而，我们在

推断范围和复杂程度方面都取得了重大进展。具体而言，[37] 中的方法受到保守启发式方法的限制，只检查最后两跳来进行推断。相比之下，我们的方法采用了更积极的策略，考虑所有拥有通往该前缀路由的自治系统。此外，我们还明确处理复杂路由场景（例如，多起源自治系统前缀）中的可达性推断，从而实现更精细、更稳健的消歧。

通用性和可扩展性。本文提出的跨平面可达性推断方法独立于特定的测量基础设施或网络协议。虽然我们使用开放的 6in4 隧道端点实例化了 TORCH，但其底层推断逻辑同样适用于从其他测量平台（如 RIPE Atlas [51]）获取的 traceroute 数据。此外，该方法与协议无关，可轻松扩展至 IPv4。通过运行 IPv4 路由跟踪，可以采用相同的分析原则评估 IPv4 中的 ROV 状态。此外，我们的方法为网络运营商提供了数据平面诊断能力，使其能够通过检查流量是否被转发至无效起源，及时识别前缀劫持。

9 结论

本文介绍了 TORCH，这是一种用于表征 IPv6 中无效路由过滤的测量框架。我们利用 6in4 隧道端点作为分布式观测点，并采用跨平面推断技术，对 IPv6 中的 ROV 保护进行了系统评估。

我们的测量显示，只有约 27% 的自治系统实现了近乎全面的防护，而若干宽松的 Tier-1 网络仍会中转流量至无效起源，保留了相当大的攻击面。此外，我们首次提供了实证证据，表明在采用相同长度前缀过滤时，附带损害可能影响全球互联网中相当大的一部分。为降低这些风险，我们敦促运营商实施主动的数据平面监控，以检测此类非预期的可达性问题。

综合来看，我们的发现揭示了当前 ROV 部署中的关键安全漏洞和非预期不利影响。这些见解凸显了加快资源公钥基础设施采用，以及实施更严格、协调一致的过滤实践，从而保障全球 BGP 路由系统安全的迫切必要性。

参考文献

[1] Pablo Alvarez、Florin Oprea 和 John Rula。2017。IPv6 路由跟踪的速率限制十分普遍：测量与缓解。（2017）。[2] APNIC Labs。2025年。各国 IPv6 支持率。https://stats.labs. apnic.net/ipv6/。访问日期：2026年1月4日。[3] Brice Augustin、Xavier Cuvellier、Benjamin Orgogozo、Fabien Viger、Timur Friedman、Matthieu Latapy、Clémence Magnien 和 Renata Teixeira。2006。使用 Paris traceroute 避免 traceroute 异常。发表于第*6*届*ACM SIGCOMM*互联网测量会议论文集（巴西里约热内卢）（*IMC '06*）。计算机协会，纽约州纽约市，美国，153 158 10 1145 1177080 1177100 – 。doi: 。/。[4] Michael Bailey、David Dittrich、Erin Kenneally 和 Doug Maughan。2012年。《门洛报告》。*IEEE*《安全与隐私》10, 2（2012年），71–75。[5] Shehar Bano、Philipp Richter、Mobin Javed、Srikanth Sundaresan、Zakir Durumeric、Steven J. Murdoch、Richard Mortier 和 Vern Paxson。2018年。扫描互联网以检测存活性。*SIGCOMM*计算机通信评论 48, 2 2018 2 9 10 1145 3213232 3213234（5月），–。doi: 。/。[6] Robert Beverly、Ramakrishnan Durairajan、David Plonka 和 Justin P. Rohrer。2018年。观察者眼中的IP：主动发现IPv6拓扑的策略。载于*2018*年互联网测量会议论文集（美国马萨诸塞州波士顿）（*IMC '18*）。计算机协会，纽约州纽约市，美国，308 321 10 1145 3278532 3278559 –。doi: 。/。[7] Randy Bush、Olaf Maennel、Matthew Roughan 和 Steve Uhlig。2009年。互联网视力检查：评估互联网可达性中损坏的眼镜。载于第*9*届*ACM SIGCOMM*互联网测量会议论文集（美国伊利诺伊州芝加哥）（*IMC '09*）。计算机协会，纽约州纽约市，美国，242–253。doi:10.1145/1644893.1644923[8] CAIDA。2025年。AS 排名。https://asrank.caida.org/。访问日期：2025年11月17日。[9] CAIDA。2025年。IPv4和IPv6的Routeviews 前缀到 AS 映射数据集。https://www.caida.org/catalog/datasets/routeviews-prefix2as/ 访问日期：2025年11月17日。[10] Ben Cartwright-Cox。2018年。BGP的安全功能现在能正常工作了吗?https://blog.benjojo.co.uk/post/are-bgps-security-features-working-yet-rpki[11] Wenqi Chen、Zhiliang Wang、Dongqi Han、Chenxin Duan、Xia Yin、Jiahai Yang 和 Xingang Shi。2022年。ROV-MI：大规模、准确且高效的ROV部署测量。载于*NDSS*。[12] Zhiyi Chen、Zachary S. Bischof、Cecilia Testart 和 Alberto Dainotti。2023年。改进兄弟自治系统的推断。载于被动与主动测量：第*24*届国际会议，*PAM 2023*，线上会议，*2023*年*3*月*21*日至*23*日，论文集。施普林格出版社，柏林，海德堡，345–372。doi:10.1007/978-3-031-28486-1_15[13] Shinyoung Cho、Romain Fontugne、Kenjiro Cho、Alberto Dainotti 和 Phillipa Gill。2019年。BGP 劫持分类。载于*2019*年网络流量测量与分析会议（*TMA*）。25–32。doi:10.23919/TMA.2019.8784511[14] Cloudflare。2020年。Is BGP Safe Yet? https://isbgpsafeyet.com/。访问日期：2025年11月17日。[15] Italo Cunha、Renata Teixeira、Darryl Veitch 和 Christophe Diot。2011年。预测和跟踪互联网路径变化。*SIGCOMM*计算机通信评论 41, 4 2011 122 133 10 1145 2043164 2018451（8月），–。[16] 2007 doi: 。/。Elwyn B. Davies 和 János Mohácsi。。《防火墙中ICMPv6消息过滤建议》。RFC 4890。doi:10.17487/RFC4890[17] Ben Du、Cecilia Testart、Romain Fontugne、Gautam Akiwate、Alex C. Snoeren 和 kc claffy。2022年。谨慎对待MANRS：测量MANRS生态系统。载于第*22*届*ACM*互联网测量会议论文集（法国尼斯）（*IMC '22*）。计算机协会，纽约州纽约市，美国，716–729。doi:10.1145/3517745. 3561419[18] Facebook。2025年。IPv6 总体采用率。https://www.facebook.com/ipv6/?tab=ipv6_total_adoption。访问日期：2026年1月4日。[19] Elverton Fazzion、Giancarlo Teixeira、Darryl Veitch、Christophe Diot、Renata Teixeira 和 Ítalo Cunha。2025年。RemapRoute：互联网路径变化的局部重新映射。载于*2025*年*ACM*互联网测量会议论文集（美国）（*IMC '25*）。计算机协会，纽约州纽约市，美国，185–191。doi:10.1145/3730567.3732923

[20] Yossi Gilad、Avichai Cohen、Amir Herzberg、Michael Schapira 和 Haya Shulman。2016年。我们已经到达目标了吗？关于资源公钥基础设施的部署与安全。密码学电子预印本档案（2016年）。[21] Robert E. Gilligan 和 Erik Nordmark。2005年。IPv6主机和路由器的基本过渡机制。RFC 4213。doi:10.17487/RFC4213[22] Fernando Gont、Suresh Krishnan、Dr. Thomas Narten 和 Richard P. Draves。2021年。无状态地址自动配置的临时地址扩展。RFC 。doi: 。/RFC 谷歌。。IPv统计数据。https://www.google.com/intl/en/ipv6/statistics.html。访问日期：2026年1月4日。[24] Mehmet H. Gunes 和 Kamil Sarac。2009年。分析路由器对主动测量探针的响应能力。载于被动与主动网络测量，Sue B. Moon、Renata Teixeira 和 Steve Uhlig（编）。Springer Berlin Heidelberg，柏林，海德堡，23–32。[25] Jiaxing Guo、Lin He、Daguo Cheng、Xingang Shi 和 Ying Liu。2025年。让旧工具焕发新生：利用6in4 隧道测量源地址验证部署。载于*2025*年*IEEE/ACM*第*33*届服务质量国际研讨会（*IWQoS*）。1–10。doi:10.1109/IWQoS 65803 2025 11143432 。Mukesh Gupta 和 [26] Alex Conta。2006年。互联网协议版本6（IPv6）规范的互联网控制消息协议（ICMPv6）。RFC 4443。doi:10.17487/RFC4443[27] Tomas Hlavacek、Amir Herzberg、Haya Shulman 和 Michael Waidner。2018年。实践经验：测量路由起源验证的方法。载于*2018*年第*48*届*IEEE/IFIP*年度国际可靠系统与网络会议（*DSN*）。634–641。doi:10.1109/DSN. 2018.00070[28] Tomas Hlavacek、Haya Shulman、Niklas Vogel 和 Michael Waidner。2023年。亲近朋友，更要亲近路由服务器：洞察互联网中的资源公钥基础设施验证。载于第*32*届*USENIX*安全研讨会（*USENIX Security 23*）。USENIX协会，阿纳海姆，加利福尼亚州，4841–4858。
h
t
t
p
s://
www.usenix.org/conference/usenixsecurity23/presentation/hlavacek [29] Hurricane Electric。2026年。AS49544 的 Looking Glass。https://bgp.he.net/lg/49544。访问日期：2026年1月4日。[30] Geoff Huston。2021年。测量路由起源授权和ROV。https://stats.labs.apnic.net/rpki[31] John Kristoff、Mohammad Ghasemisharif、Chris Kanich 和 Jason Polakis。2021年。隧道尽头的困境：实际环境中的传统IPv6过渡机制。载于被动与主动测量：第*22*届国际会议，*PAM 2021*，线上会议，*2021*年*3*月*29*日至*4*月*1*日，论文集（德国科特布斯）。施普林格出版社，柏林，海德堡，390 405 10 1007 978 3 030 72582 2_23 –。doi: 。/ - - - - [32] Mohit Lad、Ricardo Oliveira、Beichuan Zhang 和 Lixia Zhang。2007年。理解互联网拓扑抵御前缀劫持攻击的韧性。载于第*37*届*IEEE/IFIP*国际可靠系统与网络会议（*DSN*）论文集。IEEE，368–377。doi:10.1109/DSN.2007.95[33] Matt Lepinski 和 Stephen Kent。2012年。支持安全互联网路由的基础设施。RFC 6480 10 17487 6480 。doi: 。/RFC 2025 [34] Weitong Li、Yuze Li 和 Taejoong Chung。。{ImpROV}：测量并实际缓解{资源公钥基础设施}路由起源验证中的{附带损害}。载于第*34*届*USENIX*安全研讨会（*USENIX Security 25*）。3631–3647。[35] Weitong Li、Zhexiao Lin、Md. Ishtiaq Ashiq、Emile Aben、Romain Fontugne、Amreesh Phokeer 和 Taejoong Chung。2023年。RoVista：测量并分析资源公钥基础设施中的路由起源验证（ROV）。载于*2023*年*ACM*互联网测量会议论文集（加拿大魁北克省蒙特利尔）（*IMC '23*）。计算机协会，纽约州纽约市，美国，73–88。doi:10.1145/3618257.3624806

[36] Pat Litke 和 Joe Stewart。2014年。为加密货币获利而进行的 BGP 劫持。Dell SecureWorks 反威胁部门研究简报。可访问：https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit。[37] Andra Lutu、Marcelo Bagnulo、Cristel Pelsser 和 Olaf Maennel。2014年。了解 IPv6 有限可见性前缀的可达性。载于第*15*届被动与主动测量国际会议论文集——第*8362*卷（美国加利福尼亚州洛杉矶）（*PAM 2014*）。施普林格出版社，柏林，海德堡，163–172。doi:10.1007/978-3-319- 04918-2 16_[38] Di Ma、David Mandelberg 和 Tim Bruijnzeels。2018年。基于 RPKI 的简化本地互联网号码资源管理（SLURM）。RFC 8416。doi:10.17487/RFC8416[39] Macarne。2026年。Looking Glass。https://lg.macarne.com/。访问日期：2026年1月4日。[40] Doug Madory。2023年。互联网重大 BGP 事件简史。Kentik 博客。可访问：https://www.kentik.com/blog/a-brief-history-of-the-internets-biggest-bgp-incidents/。[41] MaxMind。2025年。GeoLite2 免费地理定位数据。https://dev.maxmind.com/geoip/geolite2-free-geolocation-data 访问日期：2025- 11-17。[42] Reynaldo Morillo、Justin Furuness、Cameron Morris、James Breslin、Amir Herzberg 和 Bing Wang。2021年。路由起源验证++：针对 BGP 劫持的改进型可部署防御措施。。载于*NDSS*。[43] Thomas Narten 博士、Richard P. Draves 和 Suresh Krishnan。2007年。IPv6 无状态地址自动配置隐私扩展。RFC 4941。doi:10.17487/RFC4941[44] Thomas Narten 博士、Tatsuya Jinmei 和 Susan Thomson 博士。2007年。IPv6 无状态地址自动配置。RFC 4862。doi:10.17487/ RFC4862[45] NLnet Labs。2025年。Routinator。https://nlnetlabs.nl/projects/routing/ routinator/[46] NLNOG。2026年。NLNOG Looking Glass。https://lg.ring.nlnog.net/。访问日期：2026年1月4日。[47] 俄勒冈大学。2025年。俄勒冈大学 RouteViews 项目。https://www.routeviews.org/routeviews/ 访问日期：2025-11-17。[48] Louis Poinsignon。2020年。Is BGP Safe Yet? 还没有，但我们正在密切跟踪。https://blog.cloudflare.com/is-bgp-safe-yet-rpki-routing- security-initiative/。Cloudflare 博客。访问日期：2026-01-05。[49] Andreas Reuter、Randy Bush、Italo Cunha、Ethan Katz-Bassett、Thomas C. Schmidt 和 Matthias Wählisch。2018年。迈向严谨的 RPKI 路由验证与过滤采用情况测量方法。*SIGCOMM* 计算机通信评论48，1（2018年4月），19–27。doi:10.1145/3211852.3211856[50] RIPE NCC。2008年。YouTube 劫持：RIPE NCC RIS 案例研究。RIPE NCC 新闻。可访问：https://www.ripe.net/about-us/youtube-hijacking-a-ripe-ncc-ris-case-study/。[51] RIPE NCC。2025年。RIPE Atlas。https://atlas.ripe.net/ 访问日期：2025- 11-17。[52] Nils Rodday、Ítalo Cunha、Randy Bush、Ethan Katz-Bassett、Gabi D Rodosek、Thomas C Schmidt 和 Matthias Wählisch。2021年。在数据平面重新审视 RPKI 路由起源验证。载于网络流量测量与分析会议（*TMA*，*IFIP*）论文集。[53] Brandon Schlinker、Kyriakos Zarifis、Italo Cunha、Nick Feamster 和 Ethan Katz-Bassett。2014年。PEERING：为我们服务的自治系统。载于第*13*届 *ACM* 网络热点研讨会论文集（美国加利福尼亚州洛杉矶）（*HotNets-XIII*）。计算机协会，美国纽约州纽约，1–7。doi:10.1145/2670518.2673887[54] Daniel Senie 和 Paul Ferguson。2000年。网络入口过滤：防御利用 IP 源地址欺骗的拒绝服务攻击。RFC 2827。doi:10.17487/RFC2827

[55] Pavlos Sermpezis、Vasileios Kotronis、Alberto Dainotti 和 Xeno - fontas A. Dimitropoulos。2018年。《网络运营商关于BGP前缀劫持的调查》。*ACM SIGCOMM*计算机通信评论48, 1（2018年），64–69。doi:10.1145/3211852.3211862
[56] Aftab Siddiqui。2018年。《发生了什么？Amazon Route 53 BGP劫持如何接管以太坊加密货币钱包》。互联网协会博客。网址：https://www.internetsociety.org/blog/2018/ 04/amazons-route-53-bgp-hijack/。

[57] Cecilia Testart、Philipp Richter、Alistair King、Alberto Dainotti 和 David Clark。2020年。《要不要过滤：衡量当下注册资源公钥基础设施的益处》。载于被动与主动网络测量国际会议。施普林格，71–87。[58] Renrui Tian、Yahui Li、Han Zhang、XinZhe Liu、Xia Yin、Xingang Shi、Zhiliang Wang 和 Jilong Wang。2025年。《海报：ERIS：通过ICMPv6速率限制侧信道评估路由起源验证》。载于*2025*年*ACM SIGSAC*计算机与通信安全会议（台北，台湾）（*CCS '25*）。计算机协会，纽约，美国，4731–4733。doi:10.1145/3719027.3760707[59] Twelve99。2026年。AS1299路由观察站。https://lg.twelve99.net/。访问日期：2026年1月4日。[60] Maya Ziv、Liz Izhikevich、Kimberly Ruth、Katherine Izhikevich 和 Zakir Durumeric。2021年。《ASdb：一个用于对自治系统所有者进行分类的系统》。载于第*21*届*ACM*互联网测量会议论文集（线上会议）（*IMC '21*）。计算机协会，纽约，美国，703–719。doi:10.1145/3487552. 3487853

伦理考量

为尽量减少对网络运营和第三方基础设施的潜在影响，我们依据 [4]设计并执行了测量。具体而言，我们的探测严格限制为低速率路由跟踪数据包，不会出于任何无关目的生成其他流量。我们严格实施每端点速率限制，以确保带宽消耗可忽略不计，并避免干扰合法的隧道流量。除这些探针外，我们严格避免任何可能助长基础设施滥用的操作，例如诱发放大效应或探测内部网络资产。为进一步减轻对任何单一网络的测量负担，我们通过观测点采样和目标去重来减少探测开销。

我们还限制了路由跟踪的最大跳数，并采用轮询调度策略以防止流量突发。最后，为降低基础设施暴露相关的安全与隐私风险，我们对数据集中的所有敏感 IP 地址进行匿名化处理。这包括隧道节点的公共 IPv4 接口，以及内部网络中的所有非公共 IPv6 地址。

A 隧道地理定位与 AS 归属判定

本节补充说明已发现的 6in4 隧道端点的地理分布，以及用于 IPv6 AS 归属判定的启发式方法的技术实现。

A.1 地理分布

图 10 展示了根据 IPv4 地址确定的 1,048,273 个隧道端点的全球分布。这些端点遍布 115 个国家，其中中国和澳大利亚的集群尤为密集。巴西、印度和美国也有显著的集中分布。

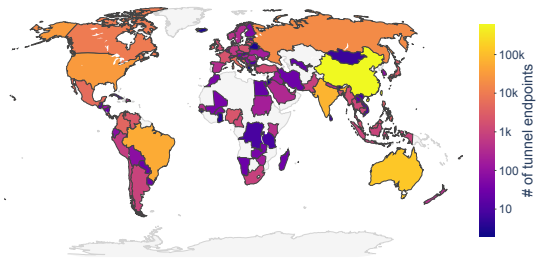


图 10：发现的 6in4 隧道端点的全球地理分布。

A.2 IPv6 归属判定

我们通过主动测量来推断并验证隧道端点的 IPv6 AS 归属。为此，我们首先尝试使用 [25] 中描述的方法直接获取 IPv6 地址。对于每个端点，我们发送一个封装的 ICMPv6回显请求，并将内层跳数限制设为 1。端点收到数据包后，会对外层 IPv4 首部进行解封装，并像往常一样处理内层 IPv6 数据包。由于跳数限制递减至零，端点将回复一条 ICMPv6 超时消息，从而暴露其 IPv6 地址。利用这一技术，我们获取了 175,559 个端点（17%）的 IPv6 地址，这些端点分布在 242 个自治系统中。

对于其余端点，我们采用两种基于 traceroute 的启发式方法，以验证其 IPv4 和 IPv6 连通性是否由同一自治系统提供。这两种方法都利用第 4.1 节中描述的方法，从隧道端点发起路由跟踪探测。

跨自治系统追踪。首先，我们从每个隧道端点向一级自治系统中的稳定目标执行 IPv6 路由跟踪，这些目标预计位于端点的本地网络之外。通过将流量导向高连接性服务提供商，我们迫使路径穿越网络边界。因此，第一个响应的跃点通常对应本地网关或直接相连的上游路由器。随后，如果该跃点的 IPv6 地址映射到与端点 IPv4 地址相同的自治系统，我们便确认这一归属。

自治系统内追踪。如果跨自治系统追踪未能找到匹配的自治系统，我们就继续测试该端点在拓扑上是否与其托管自治系统的原生 IPv6 基础设施相邻

所在的 IPv4 自治系统。为此，我们首先从全球 BGP 路由信息库中提取该端点的 IPv4 自治系统编号所通告的所有 IPv6 前缀，以确定目标 IPv6 地址空间 [47]。在每个前缀内，我们通过附加常见的接口标识符（例如 ::1、::FFFF）来构造潜在的活跃目标。由于这些目标代表严格位于托管自治系统内部的目的地，因此来自本地端点的流量不应流出到公共互联网，而应经过该自治系统的内部网络架构。我们对这些目标执行 IPv6 路由跟踪；如果前两跳中的任何一个路由器映射到托管端点的 IPv4 自治系统，我们便将这种邻接关系视为确认 AS 归属的依据。

最后，我们成功将 777,667 个隧道端点（74%）归属到 1,349 个 IPv6 自治系统。

B 可达性动态

在测量期间，若干前缀表现出显著的可达性动态，如图 9 所示。我们调查了这些动态背后的原因。

B.1 案例 1：路由起源验证实施中的操作漏洞

我们观察到，Cloudflare 的 RPKI 信标 2606:4700:7000::/48 的可达性在 2025年12月17日略有上升，这表明某些自治系统在这一天接受了 RPKI无效路由。例如，AS4538（CERNET）通常没有通往该前缀的路由，却意外地通过将流量路由至位于 Equinix 香港的 Cloudflare 的接入点而获得了可达性。然而，公开路由信息库快照 [47] 未显示与该事件相对应的变化，这表明此类无效路由传播可能仅局限于局部，因此无法被公开路由收集器观测到。

类似地，AS6939（Hurricane Electric）的可达性也出现了显著波动。TORCH 的持续监测显示，AS6939 于 2026 年 1 月 8 日和 9 日短暂恢复了对该前缀的访问。在此期间，来自 AS4538 的 traceroute 探测先后经过 AS23911（CNGI-6IX）和 AS6939，最终到达 Cloudflare 位于 Equinix 苏黎世的入口点。这表明，无效路由最初由 AS6939 接受，随后向下游传播至 AS23911 和 AS4538。同时，RIB 数据 [47] 显示，在测量窗口内，AS6939 确实传播了无效路由，从而损害了其下游客户锥的路由完整性。值得注意的是，APNIC 的测量结果 [30],也进一步印证了我们的发现：同一时期，AS6939 的 ROV 过滤率显著下降。

总体而言，这些可达性异常表明，ROV 部署受影响的自治系统时可能存在潜在的实现缺陷或配置错误。此外，我们对12月17日事件的调查表明，由于可见性有限，控制平面监测可能会忽略局部路由变化。这凸显了主动数据平面测量的必要性，只有这样才能全面捕捉路由动态。

B.2 案例 2：一级自治系统在无效路由传播中的关键作用

三个 RPKI 无效前缀的可达性变化与 AS6762（Telecom Italia Sparkle）的控制平面可见性密切相关。具体而言，前缀 2406:d440:ffff::/48 和 2401:7660::/48 均由 AS4837（中国联通）的客户自治系统起源，并经其 transit 网络传播，在整个观测窗口内均出现反复的可见性波动。对可达性激增前后的路由数据进行比较分析后发现，这些异常源于 AS4837 将这些无效客户路由导出至 AS6762。AS6762 接受这些路由后，又将其传播至其庞大的客户锥，从而使这两个前缀的全球可达性大幅提升。

相比之下，前缀 2a06:a000:160::/44 在 2025年12月23日之后可达性骤降，同时相应的 RIB 条目也大幅减少。我们注意到，在可达性下降之前，AS64289 和 AS6762 这两个关键自治系统频繁出现在观测到的传播路径中——该路由由 AS64289 传播至 AS6762——但之后便不再出现 [47]。对 AS64289 [39] 的 Looking Glass 查询证实，该前缀仍保留在其本地路由表中，这表明可达性下降并非由 AS64289 丢失该路由所致（例如，由于上游撤销）。相反，更有可能是 AS6762 过滤了来自 AS64289 的通告，或未能收到该通告。为区分这两种可能性，我们查询了 AS49544 [29]（AS64289 的另一个对等体）的 Looking Glass，发现其路由表中也同样没有该路由。两个对等体的路由表中均缺少该路由，因此我们可以更有把握地将可达性下降归因于 AS64289 导出策略的变化，而非 AS6762 的局部过滤。

总而言之，这些发现凸显了一级自治系统在全球路由传播中的关键作用。前缀的全球可见性取决于一级网络的中转和导出决策，因此，在这一层级严格执行路由起源验证，能为互联网范围的路由安全带来显著的附带收益。