资源公钥基础设施部署问题研究综述

杨国正[1,2],齐冬震[1,2],陈攀[1,2],沈照斌[1,2],尹鹏语[1],霍彦霖[1,2]
(1.国防科技大学电子对抗学院,安徽 合肥 230037;2.网络空间安全态势感知与评估安徽省重点实验室,安徽 合肥 230037)

摘 要: 资源公钥基础设施(RPKI)是保障边界网关协议(BGP)路由安全性的一项重要机制,通过路由源授权(ROA)和路由源验证(ROV)两项核心功能,实现对自治系统(AS)发布路由宣告的合法性验证。近年来,随着RPKI应用的持续拓展,研究者围绕ROA配置问题与ROV部署测量开展了大量工作,从不同维度刻画了RPKI在现实网络中的运行状态与防御能力。当前RPKI相关综述集中于对RPKI体系本身研究的阐述,着重强调RPKI体系的脆弱性,对于RPKI实际部署中遇到的关键问题及其相关研究并没有进行系统梳理和深入总结。首先,对近年来RPKI系统部署问题的相关研究进行了系统综述,重点梳理了ROA配置中常见错误类型,包括ROA良性冲突以及松散ROA展开系统性分析,揭示其成因及其对路由安全的影响;然后,对现有的ROV部署测量方法进行了综合归纳与对比分析,同时总结了对ROV验证有效性与路径传播影响的评估方法;最后,给出RPKI部署问题研究的未来发展方向,为后续在RPKI部署优化、安全评估与策略研究等方向提供了理论基础与方法参考,有利于促进RPKI体系的部署推广,有效防御BGP前缀劫持。

关键词: 路由安全;边界网关协议;前缀劫持;资源公钥基础设施;路由源授权;路由源验证
中图分类号: TP393 **文献标志码:** A **DOI:** 10.19678/j.issn.1000-3428.0252551

Review on Deployment Problems of Resource Public Key Infrastructure

YANG Guozheng[1,2], QI Dongzhen[1,2], CHEN Pan[1,2], SHEN Zhaobin[1,2], YIN Pengyu[1], HUO Yanlin[1,2]
(1.Electronic Countermeasure College, National University of Defense Technology, Hefei 230037, Anhui, China;
2.Cyberspace Security Situation Awareness and Evaluation Key Laboratory of Anhui Province, Hefei 230037, Anhui, China)

【Abstract】 Resource Public Key Infrastructure (RPKI) is an important mechanism for safeguarding Border Gateway Protocol (BGP) routing security, which verifies the legitimacy of BGP announcements through Route Origin Authorization (ROA) and Route Origin Validation (ROV). As RPKI continues to advance globally, its deployment status and defense effects have become prominent research hotspots. In recent years, researchers have extensively studied ROA configuration problems and ROV deployment measurements extensively, demonstrating the operational status and protection capability of RPKI in real networks from different dimensions. Current surveys mainly focus on theoretical research on RPKI systems, emphasizing architectural vulnerabilities without systematically organizing or summarizing the key challenges and related studies encountered in their actual deployment. This review systematically summarizes recent studies on the deployment issues of RPKI systems. First, it focuses on classifying common error types in ROA configurations, including benign ROA conflicts and loose ROA registrations, and analyses their causes and impacts on routing security systematically. Then, it comprehensively summarizes and compares existing ROV deployment measurement methods and reviews evaluation methods for assessing ROV validation effectiveness and its impact on path propagation. Finally, the review outlines future research directions to address RPKI deployment issues, providing a theoretical foundation and methodological reference for subsequent research on RPKI deployment optimization, security assessment, and strategy research. The findings can promote the widespread adoption of RPKI and enhance the defense against BGP prefix hijacking.

【Key words】 route security; Border Gateway Protocol (BGP); prefix hijacking; Resource Public Key Infrastructure (RPKI); Route Origin Authorization (ROA); Route Origin Validation (ROV)

0 引言

边界网关协议(BGP)作为互联网实际运行的域间路由协议,支撑着自治系统(AS)的路由宣告和路由选择[1]。然而,BGP在设计初期缺乏对路由源合法性的验证机制,导致其长期以来易受到前缀劫持

基金项目: 国家自然科学基金面上项目(62271496)。

作者简介: 杨国正,男,教授、博士,主研方向为网络空间测绘、态势感知;齐冬震,硕士研究生;陈攀(通信作者),博士研究生;沈照斌,硕士研究生;尹鹏语,本科生;霍彦霖,博士研究生。

收稿日期: 2025-06-04 **修回日期:** 2025-09-12 **E-mail:** cpan@nudt.edu.cn

等安全攻击的威胁,对全球网络的稳定性与数据安全构成了严峻挑战。

为了解决上述问题,研究人员提出了许多安全扩展机制,如 S-BGP[2]、soBGP[3]、BGPSec[4]等,还有研究人员设计了 BGP 协议的替代方案,如 SCION[5]等。但是,由于部署困难性,这些方案都没有得到广泛应用。2008 年,IETF 提出资源公钥基础设施(RPKI),其成为防御 BGP 劫持的最佳实践[6]。RPKI 包括两项核心机制:路由源授权(ROA)与路由源验证(ROV)。ROA 声明 AS 与前缀的合法绑定关系,ROV 使路由器能够对 BGP 路由宣告进行有效性认证,并根据认证结果采取优先级调整或丢弃无效宣告的策略进行处理。目前,ROA 的覆盖率已经突破 50%[7],ROV 的部署率也在逐步上升,RPKI 体系已经进入规模化部署阶段。

随着 RPKI 系统的应用推广,当前研究进一步发现 RPKI 防护机制在实际运行中会引入一些新的问题,主要体现在以下两个方面:

1)可靠性问题:在实际配置过程中,ROA 常因前缀长度设置不当、发布和撤销不及时等问题,导致合法的 BGP 宣告被误标为无效而丢弃,造成路由中断。这类问题被称为“良性冲突”问题,影响网络正常连通。出于运营灵活性或配置便利考虑,一些 ROA 使用了过宽的前缀授权,虽然避免了合法宣告被错误认证,却扩大了攻击面,导致未被使用的宣告可能被攻击者利用进行路径伪造。ROA 配置问题影响了 RPKI 系统的可靠性,降低了运营商对 RPKI 系统的信任和持续部署意愿。

2)有效性问题:ROV 的全球部署率虽然呈上升趋势,但依然存在覆盖率偏低且过滤策略不统一的问题。部分 AS 即使部署了 ROV,也没有对所有无效通告执行严格过滤。在实际运营环境中,攻击者仍可绕过验证节点,通过合法路径传播非法宣告,甚至导致已部署 ROV 的 AS 因邻接节点未执行验证而被错误引导至非法路径,造成防护失效。

针对上述问题,近年来研究人员提出了大量针对 RPKI 系统的测量和问题优化方案,尝试刻画该系统在现实网络环境中的运行状态和风险表现。

在 ROA 配置问题的相关研究中,早期工作聚焦于 RPKI 授权信息与实际 BGP 路由之间的一致性,通过大规模测量揭示常见配置问题的类型与比例,并评估其对路由可达性和验证准确性的潜在影响。随着问题认知的深化,后续研究逐步转向对配置问题的系统性缓解,从改进配置规范、优化 ROA 编码机制、设计具备配置问题识别能力的认证白名单机制等方面提升 RPKI 系统在面对动态网络环境时的可靠性。

在 ROV 部署测量方面,为准确刻画各 AS 对验证机制的实际部署情况与执行效果,现有方法主要从控制平面与数据平面两个角度开展研究。基于控制平面的方法通过收集和比较有效与无效宣告在路由传播路径上的差异,直接观察路径的 ROV 部署情况。基于数据平面的方法依托主动探测技术,测试不同网络到无效宣告前缀的可达性,间接反映 AS 受到 ROV 保护的程度。基于规则或统计概率模型的方法定位部署 ROV 的 AS。除了对部署状态的识别以外,研究人员也进一步关注验证机制的效能评估,即现有部署是否足以实现路径过滤、防御劫持等预期目标。ROV 部署状态的测量与评估在揭示 RPKI 系统实际运行表现、指导 RPKI 未来部署方面发挥了重要作用。

近年来,已有多篇综述对 RPKI 体系相关研究进行了梳理。苏莹莹等[8]从体系结构角度出发,重点分析了 RPKI 在可扩展性、证书链依赖等方面存在的结构性问题。秦超逸等[9]聚焦于 RPKI 中心化风险,从多个角度评述了去中心化方案的研究进展。这类综述主要从 RPKI 的架构脆弱性入手,强调其技术机制的局限性及改进方向。邹慧等[10]从更宏观的角度系统梳理了 RPKI 面临的风险挑战。RODDY 等[11]对 RPKI 的测量研究进行了回顾,内容涵盖较广。上述综述虽然内容全面,但并未聚焦于 RPKI 部署过程中的具体问题与技术障碍。

相较之下,本文与上述综述文献虽有交叉,但更侧重于 RPKI 在实际部署过程中面临的问题与挑战,重点围绕 ROA 配置问题、ROV 部署不足及其部署策略优化研究展开分析,系统总结已有研究成果的同时,剖析当前 RPKI 部署推进缓慢的深层次原因,以弥补现有综述对部署难题分析不足、前沿研究更新不及时等方面的缺陷,旨在为 RPKI 大规模部署提供理论参考与策略建议。

1 相关背景

1.1 BGP 劫持

BGP 是互联网的核心路由协议,主要作用于骨干网络,负责在不同 AS 之间传播路由信息并选择流量转发路径。BGP 基于路径矢量机制,允许 AS 能够基于商业关系优先选择路由转发路径,通过 AS 属性有效避免路径环路,采取仅传播路由变化信息的增量更新机制降低网络开销。BGP 的特性提升了互联网的可扩展性和灵活性,截至 2025 年

2 月，已经有超过 10 万个 AS 和 100 万条路由的通信依赖 BGP 路由协议[12]。

AS 通过发布 BGP 路由宣告来声明其对特定网络的所有权，或者宣告到达特定前缀的 AS 级路径。然而，由于 BGP 协议在设计之初缺乏验证机制，AS 可以宣告其他 AS 的路由前缀对前往该网络的流量进行劫持，造成网络中断、数据泄露等恶劣影响，这类攻击被称为 BGP 前缀劫持。BGP 前缀劫持严重破坏了互联网的稳定性，历史上发生过许多大规模的 BGP 前缀劫持事件。2008 年，巴基斯坦电信(AS17557)错误发布前缀 208.65.153.0/24，对 YouTube 流量实现了重定向[13]；2017 年，巴西 SECW 电信劫持了 Cloudflare、谷歌和 BancoBrazil 的前缀，造成网络服务中断[14]；2024 年，Cloudflare 的公共 DNS 服务 1.1.1.1 遭遇 BGP 劫持，部分流量被错误引导至巴西的自治系统 AS267613，导致全球用户访问延迟和连接中断[15]。

BGP 劫持主要包括前缀劫持和子前缀劫持两类，前缀劫持是指攻击者在 BGP 宣告中将其他 AS 号的前缀宣告成自身所有，利用路由转发最短路径优先原则实现劫持；子前缀劫持是指攻击者直接宣告目标子前缀的所有权，利用路由转发的最长前缀匹配原则，诱导流量转发至特定 AS。两种 BGP 劫持场景如图 1 所示。

图 1(a)为正常场景下 AS1 宣告 1.1.1.1/20 网络的所有权，AS2 接收到路由宣告后，向 AS3 发布前往网络 1.1.1.1/20 的 AS 路径信息，AS3 在与该网络进行通信时会通过 AS 路径 2-1 进行转发。当存在前缀劫持时，如图 1(b)所示，攻击者 AS4 同样宣告网络 1.1.1.1/20 的所有权，此时 AS3 会根据最短路径优先的原则将前往该网络的流量转发至 AS4。如果 AS4 发布比 1.1.1.1/20 更详细的网络 1.1.1.1/24，如图 1(c)所示，此时不仅 AS3 的路由信息受到污染，AS2 也会由于最长前缀匹配原则将前往网络 1.1.1.1/24 的流量全部转发至 AS4。

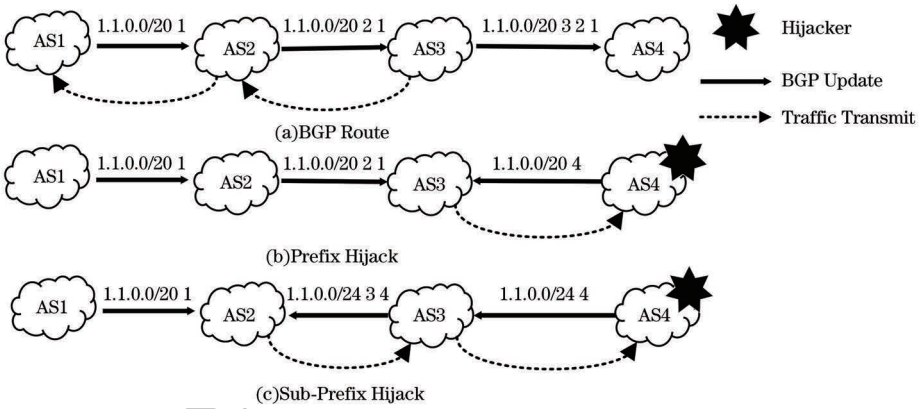

图 1 BGP 劫持示意图

Fig. 1 BGP hijacking diagram

1.2 RPKI

RPKI 是一种提供对 BGP 宣告加密验证方案的公钥基础设施，通过将 IP 前缀和 AS 绑定发布到经过认证的数据库中，使 BGP 路由器能够验证接收到的路由宣告的合法性，从而实现对 BGP 劫持的防御。RPKI 包括证书签发、证书存储和数据验证 3 个部分，整体框架如图 2 所示。

证书签发体系将所有的证书颁发机构(CA)分层，由上至下逐级发布证书对 RPKI 资源进行授权，体系末端的互联网服务提供商(ISP)发布 ROA 宣告 AS 对于前缀的所有权。其中，五大互联网注册机构(RIR)维护自身的信任锚，其他各级 CA 拥有上级 CA 颁发的证书，可以通过发布证书对其拥有的资源进行重新分配。最终由 ISP 注册 ROA 以(Prefix，Max-Length，ASN)的形式将 AS 与 IP 前缀进行绑定，其中，Prefix 和 ASN 对前缀的归属权进行认证，Max-Length 规定了可以进行路由宣告的最大掩码长度。

CA 和 ISP 各自拥有一个发布点(PP)，发布的证书和注册的 ROA 都会上传到 PP 中，所有的 PP 构成证书存储体系。在证书验证体系中，依赖方(RP)软件通过 RRDP 协议或者 rsync 同步 PP 中所有的证书和 ROA，验证后从有效的 ROA 中生成认证 RPKI 前缀(VRP)，通过 RTR 协议发送给路由器。

ROV 是 RPKI 系统的具体应用。当接收到来自其他 AS 的 BGP 宣告时，部署了 ROV 的路由器会基于最长前缀匹配原则在有效 ROA 中进行搜索。如果宣告前缀与 ROA 相匹配，包括 ASN 和前缀长度，该宣告被认证为有效(Valid)；如果 ROA 包括该宣告中的前缀，但ASN不匹配，或者前缀长度

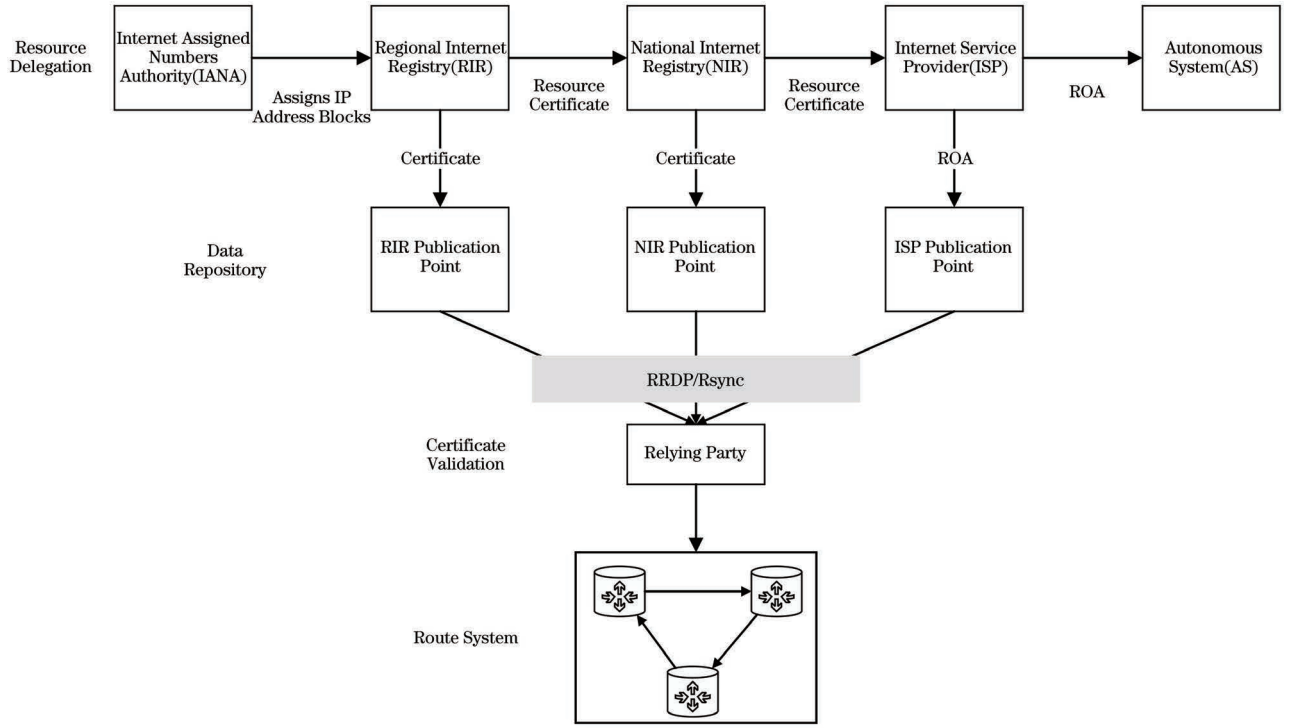

图 2 RPKI 整体架构

Fig. 2 Overall RPKI architecture

与 Max-Length 不匹配，该宣告被认证为无效(Invalid)；如果没有 ROA 覆盖该宣告中的前缀，则该宣告认证结果为未知(Unknown)。路由器根据认证结果设置 BGP 宣告的优先级，例如 Valid 优先于 Unknown，Unknown 优先于 Invalid 等。ROV 验证流程如图 3 所示。

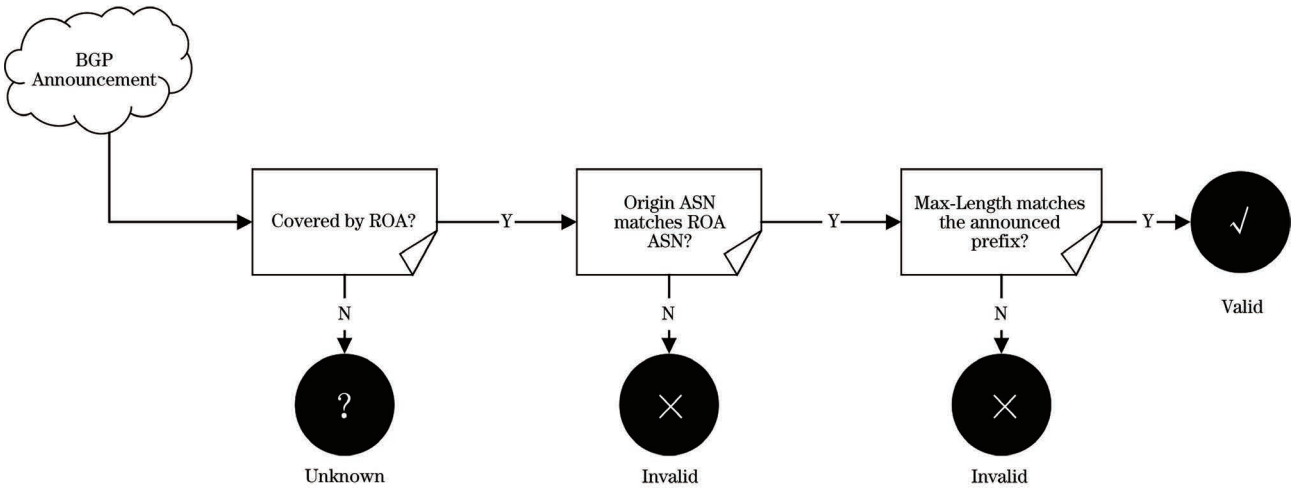

图 3 ROV 示意图

Fig. 3 ROV diagram

ROA 和 ROV 共同构成 RPKI 系统，ROA 用于保障前缀所有权声明的合法性，ROV 基于 ROA 验证 BGP 宣告，协同阻止未经授权的前缀公告，从而有效应对 BGP 劫持。

2 ROA 配置问题研究

随着 RPKI 系统的持续部署，ROA 作为其核心组成之一，在提升 BGP 路由起源认证能力方面发挥了关键作用。然而，现实网络中的 ROA 配置实践并不总是规范或准确的，诸如前缀长度设置不当、ROA 发布和撤销不及时等问题普遍存在。目前，针对 ROA 配置问题的测量分析主要包括两方面：一是 ROA 良性冲突问题，该问题会导致合法宣告被丢弃影响网络性能；二是 Loose ROA 问题，即 ROA 注册的前缀没有被合法的自治域完全宣告，导致 BGP 路由容易受到子前缀路径伪造攻击的现象。

2.1 配置问题

2012 年,WÄHLISCH 等[16]首次针对 ROA 配置情况开展了分析研究,通过整合 RPKI 数据库和 RIPE RIS[17]、RouteViews[18]数据源的 BGP 信息,量化评估了 RPKI 的部署现状,ROA 仅覆盖了 2%的 BGP 路由宣告,其中 20%被标记为无效宣告。在无效宣告中,又有超过 40%的路径中至少包含一个有效的 AS,这一发现首次说明 ROA 配置存在错误问题。WÄHLISCH 等[16]进一步归纳了 3 种主要的配置问题:1)服务提供商将前缀分配给客户,但没有为客户 AS 正确注册 ROA,导致认证失败;2)ROA 记录的 AS 与 BGP 宣告的 AS 匹配,但由于 Max-Length 设置不当,使得实际宣告的前缀比 ROA 允许的更具体,最终认证无效;3)属于同一组织的多个 AS 仅有部分注册了 ROA,导致其他 AS 的合法宣告被标记为无效。

为了量化研究 ROA 配置准确性问题,IAMARTINO 等[19]对 2012—2014 年的 ROA 和 BGP 数据进行了系统分析,发现 ROA 覆盖率从 2.05%逐步提升至 5.41%,Max-Length 设置错误占比从 61.01%降至 54.51%,无效 ASN 从 24%降至 18%,但在无效 ASN 相关错误中,57.36%～83.23%的路径中包含正确 AS。该研究为表征 RPKI 部署初期的配置准确性问题特征提供了重要的实证基础。

CHUNG 等[20]通过分析 2011—2019 年的历史数据,揭示 ROA 部署问题的长期变化趋势。将 BGP 宣告与 ROA 记录进行匹配后发现,无效 BGP 宣告的比例从 48.92%下降至 2.25%～5.39%,但其中约 50%的无效宣告是由于 Max-Length 设置不当。ROA 配置不准确呈现时间持续性特征,约有 10%持续时间超过 1 年。截至 2019 年,全球 IPv4 地址空间 ROA 覆盖率已达到 12.4%,但覆盖范围存在区域差异。RIPE NCC 的地址空间 ROA 覆盖率已达到 30%,而 ARIN 的覆盖率不到 3%。

WÄHLISCH 等[21]在 2015 年对 Web 服务 RPKI 部署的研究也揭示了显著的不均衡现象:排名前 100 的域名中仅 4%受 RPKI 保护,而排名靠后的 10 万个网站部署率为 5.5%,这种现象主要源于内容传递网络(CDN)运营商极低的参与度,199 个 CDN 运营 AS 中仅 4 个注册 ROA,而大多数高流量网站依赖 CDN 进行托管。

HLAVACEK 等[22-23]深入分析了全球 BGP 宣告和 ROA 之间的冲突,发现在路由验证结果无效的结果中存在一定比例的良性冲突。研究进一步对常见的 ROA 错误配置场景进行了分类,包括错误的 AS 绑定、错误的前缀长度和过时的 ROA 等,这些问题可能导致合法前缀的 BGP 宣告被 ROV 拦截,影响网络连通性。为了量化 ROA 良性冲突的影响,HLAVACEK 等[22-23]从欧洲的 IXP 节点处获取 2 Tb/s 的数据流,使用 NetFlow/sFlow 统计被 ROV 过滤的流量,结果发现错误配置的 ROA 导致的良性冲突造成了大量合法流量被丢弃。

2022 年,ROA 覆盖率呈现显著增长态势,LI 等[24]提出的新型 ROA 编码方案研究中显示全球 ROA 覆盖率已达 35%,这一数据与 OLIVER 等[25]同年的研究结果相互印证。2025 年,NIST RPKI Monitor[7]发布的最新监测数据表明:当前全球地址空间的 ROA 覆盖率已进一步提升至 50%,标志着 RPKI 部署进入新阶段。

本文对收集的 2025 年 4 月 28 日的 BGP 宣告和 RPKI 数据进行分析,发现认证无效的宣告比例约为 1.19%,其中,Max-Length 导致的无效占比为 48.87%,宣告中 AS 与 ROA 记录中 AS 存在商业关系的宣告占 30.54%。

除了良性冲突以外,GALID 等[26]发现 ROA 的配置还会引发新的安全风险。如果 ROA 的 Max-Length 设置不当,导致 ROA 覆盖的所有子前缀中包含没有被单独宣告的子前缀,攻击者可以利用没有被宣告的子前缀伪造路径实现流量劫持。例如,AS1 发布 ROA(1.1.0.0/20,24,AS1),但只宣告 1.1.0.0/20 单个前缀,没有宣告 1.1.0.0/21～24 中的其他子前缀,假设攻击者为 AS2,针对上述 Loose ROA,AS2 可以发布 BGP 宣告 1.1.0.0/24,AS2 AS1。由于宣告源是 AS1,ROV 认证结果为 Valid,不会被 RPKI 体系过滤,但此时没有其他 AS 宣告 1.1.0.0/24,通往该子网的所有流量将被重定向至 AS2。这种容易受到伪造子前缀路径劫持攻击的 ROA 被称为 Loose ROA。

2.2 配置优化

ROA 配置不当作为 RPKI 部署过程中最常见的问题之一,其根本原因不只局限于操作失误或规则不明,本质上还是 RPKI 设计模型的灵活程度与现实网络运营的复杂性不匹配。无论是 Max-Length 设置不当,还是 ASN 不一致所导致的良性冲突,其背后均体现了资源使用方式灵活性与 ROA 配置方式静态性之间的矛盾。

以 Max-Length 问题为例,RPKI 认证模型要求资源拥有者为每个前缀设定精确的最大可宣告长度。但在实际网络中,运营商需要根据负载、故障等

情况灵活调整前缀粒度，而这一动态变化很难通过静态 ROA 及时同步。出于对连通性的考虑，运营商倾向于设置较宽的 Max-Length，但又会引入伪造子前缀劫持风险，形成灵活性与安全性的冲突。

ASN 不一致问题同样如此。RPKI 要求前缀所有者注册 ROA 时绑定特定的 AS 号，但在网络实际运行中，路由宣告可能由其他 AS 代为发出，无论是上游代理、中间托管，还是组织内部多个 AS 的业务划分，都会导致 ROA 未能覆盖实际宣告。这种资源管理权与宣告权的不一致现象在网络运营过程中十分常见，但在 RPKI 当前模型下无法被表达或验证。

虽然理论上，资源持有者可以通过更细粒度、更全面地注册 ROA 来覆盖所有潜在的合法宣告路径，从而避免认证误判，但这一方式在实际运营中存在明显局限。全面注册 ROA 会导致 ROA 数量急剧增长，增加 RPKI 系统在内存、同步、传输等方面的负担，带来显著的性能开销。此外，在多组织协作、委托代理等场景下，协调成本高、信任关系复杂、管理职责模糊等因素也严重阻碍了细粒度 ROA 的实际落地。因此，ROA 配置问题难以完全通过规范化操作或工具自动化加以根除。

针对上述挑战，当前研究主要从两个方向展开探索：一方面，提升 RPKI 系统的性能与结构效率，通过优化 ROA 的表达方式以降低系统负担；另一方面，增强 RPKI 的鲁棒性与容错能力，以适应多样化、动态化的运营需求，缓解因配置错误引发的连通性中断。下文将围绕这两类优化路径，系统介绍相关研究工作与技术方案。

2.2.1 RPKI 性能优化

在发现 Loose ROA 现象后，GALID 等[27]对该问题进行了深入研究。ROA 中的 Max-Length 字段用于约束被授权 AS 可通告前缀的最大长度，从而限制前缀粒度并提高路由宣告的可控性，能够为 ROA 的发布提供灵活性，但是安全风险远大于便利性。通过测量发现，12% 的 ROA 设置的 Max-Length 值比前缀更大，容易受到伪造子前缀路径攻击，因此 GALID 等[27]建议使用 Minimal ROA[28]方案。Minimal ROA 与 BGP 宣告的前缀一一对应，不再使用 Max-Length 字段，从而有效降低路径劫持的风险。然而，Minimal ROA 也带来了 ROA 数量及由此产生的 RTR 协议数据单元(PDU)数量的增长，增加了系统开销。为了解决这一问题，GALID 等[27]提出 Compress-ROA 对 Minimal ROA 覆盖的前缀进行合并，在保证安全性的同时降低了 ROA 的数量。实验表明，在 2017 年的 RPKI 环境下，Compress-ROA 的压缩率达到 15.9%。

2022 年，LI 等[24]提出了基于位图的 ROA 编码方案 Hanging ROA。该方案首先将 IPv4 地址空间构造为一棵完全二叉树，然后将该地址树拆分为若干棵子树，使用子树的根节点作为标识，对于每棵子树，采用层次遍历方式，将其映射为一个位图，若某一前缀被 ROA 覆盖，则在位图上对应位置标记为“1”，否则为“0”。通过该压缩方案，Hanging ROA 可在不丢失前缀粒度信息的前提下，实现高效压缩与组织。相较于 Minimal ROA 方案，Hanging ROA 降低了 26.7%的 RRDP PDU 数量和 44.5%～64.7% 的 AS 路由器 RTR 全局同步成本。

2.2.2 RPKI 鲁棒性优化

为应对 ROA 配置问题导致的路径误判问题，提升 RPKI 系统的灵活性，已有研究从提升系统灵活性的角度提出了两类代表性机制：一类以 DISCO[29]为代表，优化 ROA 注册流程，基于实际控制权动态生成授权信息；另一类通过路径验证阶段的容错机制识别良性冲突，如 SROV[22]和 LOV[30]通过行为分析或机器学习手段，将被误判的合法路径动态纳入白名单，缓解认证过严引发的网络中断风险。

DISCO[29]系统旨在缓解 RPKI 静态授权模型与网络实际运营之间的矛盾，构建一种支持动态授权的补充机制。与传统 RPKI 依赖资源持有者预先注册 ROA、绑定“合法 AS”的方式不同，DISCO 引入“实际控制权”作为信任基础，即根据当前实际宣告该前缀的 AS 行为动态建立短周期证书，从而更好地适应现实中多组织协作与宣告权委托的复杂场景。

具体而言，DISCO 在 BGP 路由通告中嵌入发布 AS 的公钥，并通过全球分布式观测点对路径进行验证。当足够数量的观测点在一定时间窗口内观测到某 AS 对某前缀的稳定宣告时，即可视为该 AS 具备该前缀的“实际控制权”。系统随后自动为该路径签发短周期 ROA，并存入公共存储库，实现无需人工介入的动态授权。实验表明，DISCO 可自动覆盖 97%以上的合法 BGP 路径，显著减少因 ROA 缺失或配置错误导致的连通性问题。

除了从注册阶段入手提升授权的动态性以外，另一类研究则着眼于路径验证阶段，通过识别和容忍由配置不当引发的良性冲突，进一步增强 RPKI 系统对复杂现实场景的适应能力。

GALID 等[26]提出 ROAlert，ROAlert 周期性

从 RPKI 发布点获取 ROA 数据，将其与 RouteViews 中的 BGP 宣告进行比较，基于常见的配置问题找出问题 ROA，然后通过邮件或者网页向网络管理员发送预警。

2022 年，HLAVACEK 等[22]进一步提出一种启发式认证方法，该方法基于时间和聚合多源数据对良性冲突进行识别，并集成到 RP 中，形成 SROV 框架。由于 ROA 良性冲突与实际劫持时间的持续时间存在明显差异，因此基于冲突持续时间可以区分大部分良性冲突，但同时为避免单纯基于时间方案的白名单漏报现象，采用聚合多源数据对 AS 与前缀的合法性进行验证，通过评分系统量化关联性。实验结果表明，结合聚合数据分类方法后，SROV 误判率显著降低。

基于冲突持续时间的方法所需时间成本较高，且分类过程存在滞后性。因此，SCHULMANN 等[30]提出了一种名为 LOV（Learning Origin Validation）的机制。LOV 通过机器学习分类器、后分析器和隔离机制，识别被 RPKI 判别无效但实际合法的路由，将其列为 ROV 的白名单。具体而言，LOV 利用多个特征量化路由的合法性，并通过随机森林等机器学习模型对 ROA 冲突事件进行分类。后分析器基于 AS 在路径中的可见性变化对分类器得到的潜在劫持事件进行二次确认，没有被确定为劫持事件的冲突被传递到隔离区，隔离区计算分类器时使用特征的加权和，当加权和超过某个阈值时，该冲突被加入白名单。对于没有在后分析器中被证实的劫持事件，隔离区会分析其持续性时间，将持续时间超过阈值的冲突加入白名单。在为期 6 个月的测量中，LOV 成功识别 52 846 条良性冲突。

2.3 测量结果

本文根据研究的时间顺序形成 ROA 测量结果如表 1 所示，其中“—”表示原文献中没有该指标值，下同。

表 1 各阶段 ROA 测量结果对比

Table 1 Comparison of ROA measurement results across stages

Research team	Time	ROA coverage rate/%	Proportion of Invalid routes/%	Configuration issues
WÄHLISCH et al.[16]	2012	2	20	Invalid paths containing Valid ASes (40%)
IAMARTINO et al.[19]	2012—2014	2.05→5.41	—	Max-Length inappropriate settings (61.01%→54.51%), Invalid paths containing legitimate ASes (57.36%→83.23%)
GILAD et al.[26]	2017	6.55	8.43	ROA-covered prefixes contain undeclared sub-prefixes (30%)
CHUANG et al.[20]	2011—2019	12.4 (2019)	48.92→2.25	Max-Length misconfiguration (50%)
LI et al.[24]	2022	35	—	—
OLIVER et al.[25]	2022	35	—	—
Ours	2025	About 50	1.19	Max-Length inappropriate settings (48.87%), commercial relationship exists between the announcing AS and the AS in the ROA (30.54%)

3 ROV 部署测量研究

在发布 ROA 的基础上，需要进一步在 AS 的 BGP 路由器上部署 ROV 机制，通过验证 BGP 路由宣告的合法性来防止前缀劫持等攻击。因此，ROV 的部署程度也是影响全球互联网路由系统安全性的重要因素。当前，部署 ROV 的 AS 比例仍然有限。为分析评估 ROV 的当前态势和推动 ROV 的部署发展，研究人员从控制平面和数据平面两个层面提出了多种测量方法。前者主要通过开源项目提供的收集器收集 BGP 路由宣告，分析前缀在控制平面的传播情况，推断路径上的 AS 是否部署 ROV；后者分析探测数据包在数据平面的转发情况，通过对无效宣告前缀的可达性间接反映 AS 对无效宣告的过滤情况。

3.1 控制平面测量

2017 年，GLIAD 等[26]对 ROV 部署情况开展了测量研究。该团队从控制平面收集 BGP 宣告，筛选其中传播了无效宣告的路径，认为这些路径上的 AS 没有部署 ROV，或者至少不是对所有的前缀都进行了 ROV 过滤。对于源 AS 同时存在有效宣告和无效宣告的情况，如果 AS 只出现在有效宣告的路径中，而不在无效宣告的路径中，当达到一定数量时则认为其部署了 ROV。结果显示，Top 20 的 AS 只有 1 个部署了 ROV，Top 100 的 AS 只有 9 个部署了 ROV。该团队向超过 100 个网络管理人员发送了匿名调查，其中约 5.68%的受访 AS 按照严格丢弃无效路由的策略部署 ROV，约 10%受访 AS 称采取降低优先级的策略部署 ROV。该团队还揭示了 ROV 部署的附带利益和附带损害现象：附带利

益指的是若上游 AS 执行 ROV，则下游 AS 可以从过滤中受益，并且不会成为劫持攻击的受害者；附带损害是指上游没有部署 ROV 的 AS 可能会导致下游部署 ROV 的 AS 无法连接受害者 AS，甚至将流量转发给攻击者 AS。

GLIAD 等[26]的测量结果受限于收集器的选择，且采取被动收集方法难以控制实验变量，测量结果容易受到其他路由策略的影响。为此，REUTER 等[31]在 GLIAD 等[26]测量方案的基础上，进一步分析了收集器对测量结果的影响，发现若仅采用部分 VP 进行实验，可能导致 ROV 的测量结果缺少数据支撑，极有可能引起误分类。该团队定义了非受控和受控实验两种实验方法：非受控实验是指传统被动收集方法；受控实验允许改变单一变量（如路由有效性），同时控制其他变量不变，以观察并测量 AS 的路由选择行为。

为了提高测量准确性，REUTER 等[31]使用 PEERING[32]测试平台进行受控实验。首先，从同一个源 AS 发布两个均在 ROA 注册的不同前缀宣告，然后修改 ROA 令其中一个宣告无效，查看 VP 路径选择的情况，VP 要求与 PEERING 存在连接关系，且能够访问其路由选择情况。如果 VP 对于无效宣告存在不同的路径或不存在路径，则认为其部署了 ROV。该方法已应用于一个实时监测系统[33]，并于 2021 年 3 月识别出 118 个 AS 部署 ROV。

2020 年，TESTART 等[34]通过构造 AS 散点图研究了与收集器直连的 AS 的 ROV 部署情况。该团队从控制平面获取 BGP 宣告，将宣告路径上与收集器直连的 AS 定义为 Feeder，前缀传播总数达到阈值的 Feeder 被定义为 Full-feeder，当 Full-feeder 传播无效前缀的数量小于阈值时，判定其部署 ROV，阈值通过构造 Feeder-AS 关于无效前缀传播数量和前缀传播总数的散点图分析得到。该团队通过分析从 2017 年 4 月至 2020 年 1 月期间的全球路由表和 RPKI 记录，发现最初只有少数 AS 过滤不符合 RPKI 的宣告，但随着时间的推移而不断增加，截至 2020 年 1 月约有 10%的 Full-feeder 在其路由器上配置了 ROV。

2024 年，QIN 等[35]从控制平面角度探究了 MANRS Action 1 的执行情况。MANRS Action 1 要求网络运营商过滤来自客户 AS 的非法 BGP 宣告。该团队测量了 AS 对无效前缀的传播情况，发现 1 012 个 AS 允许 RPKI 无效前缀通过，进一步分析不同规模 AS 对无效前缀的传播情况，得到 895 个非终端 AS 中有 61.3%的 AS 传播了从客户接收的无效前缀，从而证明了有 61.3%的 AS 没有遵循 MANRS Action 1。针对该现象，该团队与 5 家网络运营商进行访谈交流，了解到商业利益是他们执行 Action 1 的最大阻碍之一，有些客户明确要求供应商不得丢弃其网络宣告。根据访谈结果，为了获取 ROV 的具体部署情况，该团队设计问卷对 82 个运营商进行了调研，结果发现 37.8%的受访者完全执行了 RPKI 无效过滤，17.1%的受访者执行了部分过滤，而 45.1%的受访者尚未执行 RPKI 无效过滤。该工作的重心在于社会工程学与调研方案设计，但与 ISP 等 AS 机构联系较为困难，导致样本较少，且难以复现，无法全面刻画当前 ROV 的部署态势。

2025 年，LI 等[36]对 RPKI 中的“附带损害”问题进行了深入研究，通过真实网络测量发现，大量 Invalid 通告可能绕过现有的 ROV 部署，导致路径被错误引导。为此，该团队提出了一种轻量级的缓解方案 ImpROV，该方案通过识别不安全的下一跳并构造本地路由规避策略，提升了 ROV 部署的整体防护能力。实验证明，该方案在性能开销可控的前提下，可有效降低前缀劫持的成功率，为当前 RPKI 体系中的安全缺口提供了切实可行的缓解方案。

3.2 数据平面测量

2018 年，CARTWRIGHT-COX[37]首次提出了一种基于数据平面的 ROV 部署率测量方法：从 RPKI 验证状态分别为有效与无效的前缀中选取探测点向目标地址发送 ICMP Ping 请求，根据其响应情况的差异对 ROV 部署范围进行推断。如果目标地址响应来自有效前缀的请求但不响应来自无效前缀的请求，则可推测目标地址所在的网络实施了基于 ROV 的无效前缀过滤策略。

同年，HLAVACEK 等[38]在借鉴控制平面测量方法[31]的基础上设计了两种新的数据平面测量方法，分别基于 Traceroute 和 TCP SYN 报文：1）基于 Traceroute 的测量方法通过 RIPE Atlas[39]向有效和无效前缀发送路径探测报文，并结合 CAIDA[40]数据集将 IP 级路径映射为 AS 级路径，采取与控制平面相同的分类方案对 AS 的 ROV 部署情况进行分类，如果 AS 出现在无效宣告的路径上，则认为其没有部署 ROV，如果 AS 仅出现在优先宣告的路径上，且在不同 ROA 条件下至少出现在一个有效宣告的路径上，则认为其可能部署了 ROV，在具体实验中将 AS 分为不验证（97.0%）、可能验证（2.3%）、已验证（0.1%）和大概率验证（0.5%）

4 类；2）基于 TCP SYN 的测量方法与 CARTWRIGHT-COX[37]和王志强等[41]的思路类似，分别从 RPKI 认证有效和无效前缀下的主机向 Alexa 排名前 125 万的网站服务器发送 TCP SYN 请求，根据响应情况评估这些网站是否受 ROV 保护，实验得出未受 ROV 保护(93.30%)、可能受保护(0.03%)和无法解析(6.66%)3 类结果。上述两种方法均发现：数据平面测得的 ROV 部署率远低于控制平面得到的结果。

由于 HLAVACEK 等[22-23]提出的测量方案没有考虑当前 AS 会受到上游部署 ROV 的 AS 保护的情况，因此存在识别不准确的问题。2021 年，RODDAY 等[42]提出了更为严格的部署 ROV 的 AS 识别方案。该团队借助 PEERING 平台在 IXP 上的 POP 点发布 BGP 前缀，并通过 CA 注册对应 ROA。实验设置了对照组与实验组：前者始终保持 ROA 有效，后者则周期性变换 ROA 有效性。通过 RIPE Atlas 在同一周期内对两个前缀分别进行 Traceroute 探测，依据路径情况推断 AS 是否部署 ROV。若目标 AS 与发布源直接相连：在 ROA 有效与无效时均可达，则未部署 ROV；仅在有效状态下可达，则表明其丢弃无效前缀；路径在状态变化时发生变化但仍可达，则可能执行了部分过滤。若为非直连情形，则要求路径上的 AS 都托管探针，只有路径上的其他 AS 确定没有部署 ROV，则该 AS 才可能确定部署 ROV。

RODDAY 等[42]通过严格的条件区分减少了假阳性的情况，但同一路径上可能有多个 AS 部署 ROV，且难以让所有路径中的 AS 托管探针，研究又引入了假阴性的问题。因此，2023 年，HLAVACEK 等[43]在前期研究的基础上更新了其测量方法，结合控制平面(使用 RouteViews 与 RIPE RIS)与数据平面(改进 RIPE Atlas 采集与分析流程)进行更细粒度的分类。控制平面采用 C1～C4 4 类分类，数据平面测量则引入“分散点”概念将分类结果扩展为 C1～C7 7 类，分类粒度更细。实验表明：控制平面中存在负面证据的 AS(C1)占比 54.6%，具有强证据证明部署 ROV 的 AS 比例(C3)为 29.9%；数据平面中明确未部署的 AS(C1)为 42.8%，明确部署的 AS(C6/C7)有 24%。测量结果与 Cloudflare 测量结果[44]存在 75%的重叠度间接说明了测量结果的有效性。

在数据平面上也有工作进行非受控的测量，该类研究直接利用互联网本身存在的无效宣告进行测量。2022 年，CHEN 等[45]提出 ROV-MI 框架，该框架首先利用 BGPStream[46]与 Routinator[47]对 BGP 宣告进行验证与筛选，剔除 MOAS 或被覆盖前缀等干扰项，然后结合 ZMap[48]与 RIPE Atlas 探针，对无效与有效前缀中的存活 IP 执行 Traceroute 测量，将 IP 路径映射为 AS 级后，标记部署和未部署 ROV 的路径，最后引入基于贝叶斯推断的 SVGD 算法，实现高维条件下 ROV 部署状态的高效推理。与以往受限于 PEERING 平台前缀数量的研究相比，ROV-MI 利用实际网络中的 RPKI 无效前缀开展测量，扩展了覆盖范围。

为了精确定位部署 ROV 的 AS，ROV-MI 不再基于规则进行分类，而是优化了 GRAY 等[49]提出的用于推断 AS 内部的路由策略的贝叶斯网络属性推断算法框架。该团队利用马尔可夫蒙特卡罗(MCMC)算法求解后验概率，但 MCMC 算法采取随机采样的方式模拟 AS 部署概率，在 AS 节点数量较多时，收敛速度较慢。ROV-MI 利用变分梯度下降(SVGD)算法进行求解，SVGD 给出了更新样本的梯度方向的解析解。基于这个梯度，ROV-MI 可以使用确定性梯度下降法对粒子进行迭代更新，有效提高优化的速度和效率。实验结果表明，在传播有效 RPKI 声明的 11 074 个 AS 中，约 28%已部署 ROV、43%未部署 ROV、3%部分部署 ROV、26%状态不明确。在进行 ROV 部署 AS 定位时，基于条件概率建模的方法相对于基于规则的方法具有更强的可解释性，但在实际数据中存在覆盖路径稀疏与不均衡现象。条件概率采样方法对于仅有少量路径覆盖的低频 AS 推断结果不稳定。

2023 年，LI 等[50]提出 RoVista，同样采用非受控方式，相对于 ROV-MI，RoVista 结合 IPID 侧信道技术对 ROV 部署状态进行端到端测量。该方法克服了传统方法在 VP 部署数量不足及商业政策影响下的局限性，通过筛选非法 AS 宣告的无效前缀，构建测试节点(tNodes)与虚拟视点(vVP)，并分析 vVP 的 IPID 增长模式判断路由是否被过滤，进一步分析 vVP 所属 AS 受 ROV 保护的情况，给出了 ROV 保护评分，量化了互联网 ROV 的部署效果。该工作能够实现 ROV 部署状态的大规模测量，但仅局限于分析 AS 受 ROV 的保护情况，无法对部署 ROV 的 AS 实现精确定位。

3.3 控制平面与数据平面

当前 ROV 部署测量的核心思路是通过观测网络中对有效与无效 BGP 宣告的传播情况，推断路径上 AS 的 ROV 部署状态。这类方法本质上依赖路径行为的差异进行间接判断，因此容易受到其他路

由策略的干扰。例如，AS 选择有效宣告可能并非其执行 ROV 过滤了无效宣告，而只是因为有效宣告的优先级更高，从而无法准确反映其 ROV 部署状态。因此，亟需一种能够直接体现 ROV 实际过滤行为的测量方式。

在现有方法中，控制平面测量通过分析 BGP 路由表或更新信息，识别不同状态宣告的传播路径，其优点是路径结构清晰，受网络噪声影响较小，但其主要局限在于依赖公开观测点的数据整体覆盖范围有限，影响部署态势的全面刻画。

数据平面测量通过发送探测包判断路径可达性，进而推断路径节点对不同宣告的选择行为，具备更广泛的测量覆盖能力。然而，该方法存在多方面局限。一方面，测量结果需从 IP 级路径映射至 AS 级，严重依赖开源数据集，而这些数据集中常包含 BGP 劫持等异常路径，易造成结果污染。另一方面，受“附带损害”影响，即使某节点已部署 ROV，其探测包仍可能被转发至未部署 ROV 的上游，最终到达无效宣告源，从而在路径上误标为“未部署”，导致假阴性结果。

本文对现有方法从测量平面、测量方案和分类方案方面进行了对比，如表 2 所示。

表 2 各 ROV 测量方法的分析比较

Table 2 Analysis and comparison of various ROV measurement methods

Research team	Time	Measurement plane	Controlled	Measurement methodology	Classification scheme	Defects
GALID et al.[26]	2017	Control	N	BGP announcement path analysis	Heuristic classification	Limited number of vantage points, restricted coverage; non-controlled method affected by routing policies
REUTER et al.[31]	2018	Control	Y	Controlled experiments on the PEERING platform	Valid/Invalid path differentiation	Limited nodes available to observe routing decisions
TESTART et al.[34]	2020	Control	N	Feeder path analysis	Full feeder prefix propagation threshold classification	Focused on feeder nodes, limited coverage
GRAY et al.[49]	2020	Control	—	—	Bayesian inference framework	Large number of ASes, wide sampling space
QIN et al.[35]	2024	Control	N	Analysis of MANRS compliance and Invalid path propagation	Whether Invalid paths are propagated	Focused on social engineering and surveys, small sample size
HLAVACEK et al.[38]	2018	Control & Data	Y	ICMP Ping, Traceroute, TCP SYN	Rule-based classification	Unable to identify upstream protection scenarios; classification rules not rigorous
RODDY et al.[42]	2022	Data	Y	Traceroute	Rule-based classification of single-hop and multi-hop ASes	Difficult to deploy probes in all ASes along the path
CHEN et al.[45]	2022	Data	N	ROV-MI framework	SVGD	Poor inference for ASes with sparse path coverage
HLAVACEK et al.[43]	2023	Control & Data	Y	Enhanced Atlas probing and distributed-point path analysis	Four categories (control), seven categories (data) rule-based classification	Classification relies on rules, lacks theoretical foundation
LI et al.[50]	2023	Data	N	IP-ID side channel	IPID growth patterns and ROV protection scoring	Unable to localize ROV-deployed ASes

3.4 部署效果评估

早期工作主要通过 CAIDA 数据集的 AS 连接数据库构造 AS 级网络，基于 ROV 测量结果分析不同 ROV 部署条件下对于 BGP 劫持的防御效果。GALID 等[26]通过随机选择 AS 模拟部署 ROV，评估了在 ROV 部分部署条件下“附带收益”、“覆盖损害”以及“组织间依赖”对于 BGP 安全性的影响。HLAVACEK 等[38]在测量 ROV 部署现状后，基于当时部署情况，对 ROV 防御效果进行了评估。

然而，上述评估方案缺乏一个基准网络用于验证，导致其结果难以精确衡量和比较。为了解决使用不同的实验环境、前缀公告位置等因素而导致难以直接比较的问题，RODDAY 等[51]提出了一种新的框架，该框架能够利用从 RouteViews 和 RIPE RIS 等公共 BGP 收集器项目中获取的数据自动提取 AS 及其关系生成 Mininet 拓扑，为开展 ROV 部署评估研究提供了可控实验环境。

2023 年，HLAVACEK 等[43]又提出基于图分析的 ROV 部署评估方法，重点比较了在 IXP 与

Tier-1 运营商上部署 ROV 的影响差异。使用数据平面的测量结果构建 AS 级网络，去除部署 ROV 的 AS 相邻边，模拟不同部署场景下的无效路径传播情况，研究发现 Tier-1 等核心 AS 的 ROV 部署可显著降低网络连通性并限制攻击传播范围，而仅在 IXP 路由服务器上部署 ROV 的效果有限，因大量直连会话仍可绕过验证路径传播无效通告。该工作验证了部署位置对安全防护效果的差异性影响，为 ROV 部署策略优化提供了方法指导。

同年，DU 等[52]从控制平面出发，提出了一种用于评估 ROV 部署有效性与优先级优化的轻量级方法。为量化中转 AS 对无效通告的“倾向程度”，该团队引入 AS hegemony 指标，评估各 AS 在 Valid 与 Invalid 路径中的影响力差异，并据此识别出一批更倾向于传播 Invalid 通告的 AS，这些 AS 的 ROV 部署潜力更高，对提升全网 RPKI 防御能力具有更大的价值。该研究不仅揭示了当前 ROV 部署的不完整性，也为后续部署推进策略提供了重要的量化评估手段。

2024 年，ZENG 等[53]从演化博弈论视角出发，系统建模并分析了 RPKI 部署中长期存在的 ROA 发布与 ROV 部署的循环依赖问题：如果 AS 不能得到足够的保护，例如 ROA 覆盖的地址空间比例低，AS 使用 ROV 进行过滤的意愿也就不强烈；ROV 过滤比例低反过来又会影响 AS 注册 ROA 的积极性。AS 采取 ROA 和 ROV 的策略选择受到其他 AS 的策略影响，而这个选择是不断发生变化的。该团队构建了一个演化博弈模型，将 AS 视为博弈参与者，模拟了 AS 的策略选择和试错表现的演化过程，通过分析演化均衡的演化和稳定过程，可以获得 ROA 注册率和 ROV 部署率的取值范围。当两者的数值进入该范围时，演化可以以更快的速度达到理想状态。模型引入 ROA 注册与 ROV 过滤的部署概率变量(γ, θ)，并根据收益矩阵与复制动态方程推导系统演化的平衡态。结果表明，该系统具有两个稳定状态：完全部署(1,1)与完全不部署(0,0)，而内部平衡点(θ^*,γ^*)的具体位置决定了系统演化的最终走向。为了降低 RPKI 演化达成理想部署状态所需的最低初始部署率，该团队提出 RPKIN 机制：引入一种邻居间的“过滤通知”服务，当部署过滤策略的 AS 发现无效通告时，主动通知其邻居，帮助其识别并丢弃错误路径。该机制能够显著增加部署过滤与注册策略的收益，从而有效降低达到理想状态的最低部署率(θ^*,γ^*)，提升全网达成完全部署状态的可能性。

3.5 部署障碍分析

尽管 ROV 作为 RPKI 体系中的核心验证机制，具备显著的安全防护能力，但根据现有测量结果来看，ROV 在全球范围内的部署比例仍处于较低水平，且部署进展缓慢。结合现有研究与实际网络运营现状，可以将制约 ROV 部署推广的核心因素归纳为以下 3 个方面：

1)部署行为缺乏可观测性。ROV 的部署状态与验证策略完全由 AS 本地自主决定，而运营商通常不会公开相关配置。尽管近年来已提出多种控制平面与数据平面测量方法，用以识别某些 AS 是否启用了 ROV，但这类研究主要聚焦于“是否部署”的粗粒度判断，在具体策略层面(如只丢弃无效路由、接受部分异常路径等)缺乏测量能力。与此同时，现有部署识别方法本身仍存在显著局限，主要表现为可测路径覆盖率低、推断过程依赖间接观测存在误差、缺乏对实时变化的响应能力。这种部署行为与策略双重不可见的状态，不仅限制了研究者对 ROV 体系效能的系统性分析，也使运营商难以量化自身部署可能带来的收益与风险，降低了实际部署的意愿。

2)部署过程缺少有效指导。目前，ROV 部署高度依赖运营商的自发行为，缺乏明确的优先级建议、成本评估与收益模型支撑。现有的工作尝试通过博弈模型或部署模拟进行收益评估，但往往忽略了网络结构、路径依赖等多维因素，难以为不同 AS 类型提供可行、可落地的部署参考。此外，在 ROV 部署尚未形成大规模协同效应的初期阶段，运营商若选择率先部署，往往需独自承担配置复杂度上升、潜在的路由流量损失等多重不确定成本。然而，现有研究中普遍缺乏对“早期部署者”所面临风险的识别、建模与缓解机制，也缺少相应的激励或保障策略。这种缺位使得运营商更倾向于“观望而非行动”，等待他人先行部署，从而陷入集体部署意愿低迷的困境，进一步拖慢了 ROV 在全球范围内的推广进程。

3)ROA 配置错误引发信任障碍。ROA 配置不当造成的良性冲突导致合法 BGP 路径被误判为无效并被 ROV 丢弃，造成网络中断、网络连通性降低等损害。虽然已有 LOV、SROV 等检测机制进行误判缓解，但当前尚无法彻底消除这类误伤风险。这种由配置误差引发的信任问题，直接影响运营商对 RPKI 体系稳定性的信心，成为部署意愿进一步下降的重要因素。

4 未来展望

尽管 RPKI 体系理论上为 BGP 提供了完备的

认证框架，但整体部署仍旧进展缓慢，严重限制了其在实际网络中的防御能力。近年来，ROA 的覆盖率已经超过 50%，RPKI 的部署瓶颈逐步由资源注册转向验证机制。相比之下，ROV 部署比例仍旧较低，且推进速度缓慢。ROV 作为 RPKI 防御生效的关键环节，其部署水平直接决定了认证体系的实效性。因此，深入分析制约 ROV 部署的关键挑战，探索具有针对性的解决路径，将成为推动 RPKI 体系全面部署的核心突破口。下面围绕当前 ROV 部署过程中存在的三大核心障碍，对未来可展开的研究进行展望。

4.1 高精度 ROV 测量体系

ROV 部署状态的可见性不足，是当前制约 RPKI 部署推广的重要瓶颈之一。现有测量方法主要依赖对有效与无效 BGP 路径的观测差异进行间接推断，无法真正反映 AS 是否执行了 ROV 过滤行为，导致测量结果存在较大误差与歧义。

在测量方法层面，亟需设计能够观测到 ROV 实际过滤行为的测量机制，增强对过滤动作本身的检测能力，从而提升部署状态识别的精度与可验证性。在策略识别层面，ROV 部署并非简单的二元状态，不同 AS 可能在验证对象（是否过滤下游宣告）、验证方案（是否引入白名单或额外验证机制）、过滤策略（丢弃或降权无效路由）等环节存在多样化差异。因此，未来可通过引入路径行为建模、策略分类框架等方法，对 AS 的验证行为进行结构化解析，实现对 ROV 部署策略的细粒度识别与动态分析，为部署评估与协同优化提供更具操作性的决策依据。

4.2 ROV 部署策略引导与协同激励机制

当前 ROV 部署仍主要依赖运营商的自发决策，缺乏部署优先级评估、协同收益分析与激励机制支持，导致部署过程分散、保守，难以形成有效推进。未来研究可从两个关键方向入手：一方面，构建面向不同网络角色的部署优先级评估体系，结合 AS 等级、路径依赖、连接关系等多维特征，识别在保障连通性、提升安全性方面影响更大的关键节点，为其提供定制化的部署建议与成本收益评估模型；另一方面，考虑到 ROV 尚处于部署初期，协同收益尚未显现，早期部署者往往需独自承担额外的配置、维护与连通性风险，因此更需设计面向“先行者”的激励与补偿机制。从机制设计角度探索具有局部激励效应的部署策略，例如构建区域性互惠协议、基于信誉的资源交换模型，或引入监管引导与政策激励，从而在部署初期形成正向收益反馈，打破观望博弈，推动 ROV 部署走出冷启动困境。

4.3 ROA 配置容错机制

尽管已有研究提出了多种 ROA 配置错误的检测和缓解方案，如基于静态规则匹配的 ROAlert、启发式分析的 SROV 和机器学习分类的 LOV 等，但这些方法多数建立在对既有特征的静态提取与经验规则的预设之上，缺乏对动态网络环境中 ROA 与路径合法性之间关系的深入建模，尤其在 AS 关系频繁演化、路径多样性突出的背景下，现有方法的准确性与鲁棒性均受到较大的挑战。

未来研究应进一步关注如何精准刻画“合法但被判无效”这一类特殊路径的行为特征，识别其与恶意路径之间的本质差异。在方法上，可以融合 AS 商业关系、组织结构、历史 ROA 切片信息和地理位置等多源异构信息，通过神经网络建模 AS 间拓扑与关系特征，结合时间序列建模方法刻画路径的演化趋势，构建更加智能和具备泛化能力的冲突识别机制。此外，为提升模型的可解释性与部署适应性，可引入注意力机制识别影响判定结果的关键要素，配合动态白名单机制缓解误伤带来的连通性损害。这一方向不仅有望有效提升 ROA 配置错误检测的覆盖率和准确率，也将推动构建更具弹性与容错能力的路由验证系统。

5 结束语

随着 RPKI 体系在全球范围内持续部署，其部署状态、安全防御效果和引入问题缓解方面成为新的研究方向。现有研究围绕 RPKI 系统的两个关键机制开展了大量测量与分析工作。一方面，研究人员通过对 ROA 记录与 BGP 通告的比对，识别并分类了常见的配置错误，评估其对路由可靠性与前缀一致性的影响；另一方面，研究人员从控制平面与数据平面出发，提出了针对 ROV 的多种测量方法，用以刻画其部署状态、执行行为及对无效路径传播的实际抑制能力。随着研究的深入，越来越多的工作开始关注路径过滤策略差异、部署位置影响与系统性评估方法，推动 RPKI 从基础部署测量向更全面的安全效能评估方向发展。

参考文献

[1] LOUGHEED K, REKHTER Y. Border Gateway Protocol 3 (BGP-3): RFC 1267[R]. T. J. Watson Research Center, IBM Corp., 1991.

[2] KENT S, LYNN C, SEO K. Secure Border Gateway Protocol (S-BGP)[J]. IEEE Journal on Selected Areas in Communications, 2000, 18(4): 582-592.

[3] WHITE R. Securing BGP through secure origin BGP (soBGP)[J]. Business Communications Review, 2003, 33(5): 47-53.

[4] GEORGE W, MURPHY S. BGPSec considerations for autonomous system (as) migration: RFC 8206[R]. PARSONS, Inc., 2017.

[5] ZHANG X, HSIAO H C, HASKER G, et al. SCION: scalability, control, and isolation on next-generation networks[C]// Proceedings of the IEEE Symposium on Security and Privacy. Washington D.C., USA: IEEE Press, 2011: 212-227.

[6] LEPINSKI M, KENT S. An infrastructure to support secure internet routing: RFC 6480[R]. BBN Technologies, 2012.

[7] MONITOR N R. NIST RPKI monitor[EB/OL]. [2025-05-07]. https://www.nist.gov/services-resources/software/nist-rpki-deployment-monitor.

[8] 苏莹莹, 李丹, 叶洪琳. 资源公钥基础设施 RPKI: 现状与问题[J]. 电信科学, 2021, 37(3): 75-89.
SU Y Y, LI D, YE H L. Resource public key infrastructure RPKI: status and problems[J]. Telecommunications Science, 2021, 37(3): 75-89. (in Chinese)

[9] 秦超逸, 张宇, 方滨兴. RPKI 去中心化安全增强技术综述[J]. 通信学报, 2024, 45(7): 196-205.
QIN C Y, ZHANG Y, FANG B X. Survey on decentralized security-enhanced technologies for RPKI[J]. Journal on Communications, 2024, 45(7): 196-205. (in Chinese)

[10] 邹慧, 马迪, 邵晴, 等. 互联网码号资源公钥基础设施(RPKI)研究综述[J]. 计算机学报, 2022, 45(5): 1100-1132.
ZOU H, MA D, SHAO Q, et al. A survey of the resource public key infrastructure[J]. Chinese Journal of Computers, 2022, 45(5): 1100-1132. (in Chinese)

[11] RODDAY N, CUNHA I, BUSH R, et al. The Resource Public Key Infrastructure (RPKI): a survey on measurements and future prospects[J]. IEEE Transactions on Network and Service Management, 2024, 21(2): 2353-2373.

[12] CIDR Report for 20 Feb 25[EB/OL]. [2025-05-07]. https://www.cidr-report.org/as2.0/.

[13] RIPE NCC. YouTube hijacking a ripe NCC RIS case study[EB/OL]. [2025-05-07]. http://www.ripe.net/news/study-youtube-hijacking.html.

[14] ROBACHEVSKY A. 14, 000 Incidents: a 2017 routing security year in review[EB/OL]. [2025-05-07]. https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/.

[15] HERDES B, ZHANG M, RYAN T. Cloudflare 1.1.1.1 incident on june 27, 2024[EB/OL]. [2025-05-07]. https://blog.cloudflare.com/cloudflare-1111-incident-on-june-27-2024.

[16] WÄHLISCH M, MAENNEL O, SCHMIDT T C. Towards detecting BGP route hijacking using the RPKI[J]. ACM SIGCOMM Computer Communication Review, 2012, 42(4): 103-104.

[17] RIPE Routing Information Service (RIS)[EB/OL]. [2025-05-07]. https://www.ripe.net/analyse/internet-measure.

[18] The route views project[EB/OL]. [2025-05-07]. http://www.routeviews.org/routeviews/. ments/routing-information-service-ris/ris-raw-data.

[19] IAMARTINO D, PELSSER C, BUSH R. Measuring BGP route origin registration and validation[C]// Proceedings of International Conference on Passive and Active Network Measurement. Berlin, Germany: Springer, 2015: 28-40.

[20] CHUNG T, ABEN E, BRUIJNZEELS T, et al. RPKI is coming of age: a longitudinal study of RPKI deployment and invalid route origins[C]// Proceedings of the Internet Measurement Conference. New York, USA: ACM Press, 2019: 406-419.

[21] WÄHLISCH M, SCHMIDT R, SCHMIDT T C, et al. RiPKI: the tragic story of RPKI deployment in the Web ecosystem[C]// Proceedings of the 14th ACM Workshop on Hot Topics in Networks. New York, USA: ACM Press, 2015: 1-7.

[22] HLAVACEK T, SHULMAN H, WAIDNER M. Smart RPKI validation: avoiding errors and preventing hijacks[C]// Proceedings of ESORICS'22. Berlin, Germany: Springer, 2022: 509-530.

[23] HLAVACEK T, SHULMAN H, WAIDNER M. Not all conflicts are created equal: automated error resolution in RPKI deployments[C]//Proceedings of the IEEE Conference on Computer Communications Workshops. Washington D.C., USA: IEEE Press, 2021: 1-2.

[24] LI Y B, ZOU H, CHEN Y X, et al. The hanging ROA: a secure and scalable encoding scheme for route origin authorization[C]// Proceedings of the IEEE Conference on Computer Communications. Washington D.C., USA: IEEE Press, 2022: 21-30.

[25] OLIVER L, AKIWATE G, LUCKIE M, et al. Stop, DROP, and ROA: effectiveness of defenses through the lens of DROP[C]// Proceedings of the 22nd ACM Internet Measurement Conference. New York, USA: ACM Press, 2022: 730-737.

[26] GILAD Y, COHEN A, HERZBERG A, et al. Are we there yet? On RPKI's deployment and security[C]//Proceedings of 2017 Network and Distributed System Security Symposium. San Diego, USA: Internet Society, 2017: 1-10.

[27] GILAD Y, SAGGA O, GOLDBERG S. MaxLength considered harmful to the RPKI[C]//Proceedings of the 13th International Conference on Emerging Networking EXperiments and Technologies. New York, USA: ACM Press, 2017: 101-107.

[28] BUSH R. Origin validation operation based on the Resource Public Key Infrastructure (RPKI): RFC 7115[R]. Internet Engineering Task Force (IETF), 2014.

[29] HLAVACEK T, CUNHA I, GILAD Y, et al. DISCO: sidestepping RPKI's deployment barriers[C]//Proceedings of 2020 Network and Distributed System Security Symposium. San Diego, USA: Internet Society, 2020: 1-12.

[30] SCHULMANN H, ZHAO S J. Learning to identify conflicts in RPKI[EB/OL]. [2025-05-07]. https://arxiv.org/abs/2502.03378.

[31] REUTER A, BUSH R, CUNHA I, et al. Towards a rigorous methodology for measuring adoption of RPKI route validation and filtering[J]. ACM SIGCOMM Computer Communication Review, 2018, 48(1): 19-27.

[32] SCHLINKER B, ZARIFIS K, CUNHA I, et al. PEERING: an as for us[C]//Proceedings of the 13th ACM Workshop on Hot Topics in Networks. New York, USA: ACM Press, 2014: 1-7.

[33] REUTER A, BUSH R, CUNHA I, et al. Measuring RPKI route origin validation deployment[Z]. 2016.

[34] TESTART C, RICHTER P, KING A, et al. To filter or not to filter: measuring the benefits of registering in the RPKI today[C]//Proceedings of the 21st International Conference Passive and Active Measurement. Berlin, Germany: Springer, 2020: 71-87.

[35] QIN L C, CHEN L, LI D, et al. Understanding Route Origin Validation (ROV) deployment in the real world and why MANRS action 1 is not followed[C]//Proceedings of the Network and Distributed System Security Symposium. Washington D.C., USA: IEEE Press, 2024: 1-13.

[36] LI W, LI Y, CHUNG T. ImpROV: measurement and practical mitigation of collateral damage in RPKI route origin validation[C]// Proceedings of the USENIX Security Symposium. [S.l.]: USENIX, 2025: 1-15.

[37] CARTWRIGHT-COX B. Are BGPs security features working yet? [EB/OL]. [2025-05-07]. https://benjojo.co.uk/u/benjojo.

[38] HLAVACEK T, HERZBERG A, SHULMAN H, et al. Practical experience: methodologies for measuring route origin validation[C]//Proceedings of the 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Washington D. C., USA: IEEE Press, 2018: 634-641.

[39] What is RIPE Atlas? [EB/OL]. [2025-05-07]. https://atlas.ripe.net/about/.

[40] CAIDA. Prefix to as mapping [EB/OL]. [2025-05-07]. https://www.caida.org/catalog/datasets/routeviews-prefix2as/.

[41] 王志强, 陈力园, 代蛟. 基于 WTGWO 的无线传感器网络三维部署优化方法[J]. 吉林大学学报(理学版), 2024, 62(2): 410-416.
WANG Z Q, CHEN L Y, DAI J. Three-dimensional deployment optimization method of wireless sensor network based on WTGWO[J]. Journal of Jilin University (Science Edition), 2024, 62(2): 410-416. (in Chinese)

[42] RODDAY N, CUNHA F S, BUSH R, et al. Revisiting RPKI route origin validation on the data plane[EB/OL]. [2025-05-07]. https://www.semanticscholar.org/paper/Revisiting-RPKI-Route-Origin-Validation-on-the-Data-Rodday-Cunha/363018c6f2e36d6d0b82c0a2c7cb6fcf1edb2f20/figure/3.

[43] HLAVACEK T, SCHULMANN H, VOGEL N, et al. Keep your friends close, but your routeservers closer: insights into RPKI validation in the Internet[C]//Proceedings of the 32nd USENIX Security Symposium. [S. l.]: USENIX, 2023: 4841-4858.

[44] Is BGP safe yet? No[EB/OL]. [2025-05-07]. https://isbgpsafeyet.com/.

[45] CHEN W Q, WANG Z L, HAN D Q, et al. ROV-MI: large-scale, accurate and efficient measurement of ROV deployment[C]//Proceedings of the 2022 Network and Distributed System Security Symposium. San Diego, USA: Internet Society, 2022: 1-17.

[46] ORSINI C, KING A, GIORDANO D, et al. BGPStream: a software framework for live and historical BGP data analysis[C]//Proceedings of the 2016 Internet Measurement Conference. New York, USA: ACM Press, 2016: 429-444.

[47] NLnetLabs. Routinator[EB/OL]. [2025-05-07]. https://github.com/NLnetLabs/routinator.

[48] DURUMERIC Z, WUSTROW E, HALDERMAN J A. ZMap: fast Internet-wide scanning and its security applications[C]//Proceedings of the USENIX Security Symposium. [S. l.]: USENIX, 2013: 605-620.

[49] GRAY C, MOSIG C, BUSH R, et al. BGP beacons, network tomography, and Bayesian computation to locate route flap damping[C]//Proceedings of the ACM Internet Measurement Conference. New York, USA: ACM Press, 2020: 492-505.

[50] LI W T, LIN Z X, ASHIQ M I, et al. RoVista: measuring and analyzing the Route Origin Validation (ROV) in RPKI[C]//Proceedings of the 2023 ACM on Internet Measurement Conference. New York, USA: ACM Press, 2023: 73-88.

[51] RODDAY N, VAN BAAREN R, HENDRIKS L, et al. Evaluating RPKI ROV identification methodologies in automatically generated mininet topologies[C]//Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies. New York, USA: ACM Press, 2020: 530-531.

[52] DU B, TESTART C, FONTUGNE R, et al. Poster: taking the low road: how RPKI invalids propagate[C]//Proceedings of the ACM SIGCOMM 2023 Conference. New York, USA: ACM Press, 2023: 1144-1146.

[53] ZENG M, HUANG X H, ZHANG P, et al. Improving prefix hijacking defense of RPKI from an evolutionary game perspective[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(6): 5170-5184.

文字编辑 陆燕菲
栏目编辑 赖玉玲