软件学报 ISSN 1000-9825, CODEN RUXUEW
2026,37(1):464−484 [doi: 10.13328/j.cnki.jos.007459] [CSTR: 32375.14.jos.007459]

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

RPKI 测量研究综述*

张泽源[1], 刘 翔[2], 张 宇[1,2], 张伟哲[1,2], 方滨兴[2,3]

[1](哈尔滨工业大学 网络空间安全学院, 黑龙江 哈尔滨 150001)

[2](鹏城实验室, 广东 深圳 518055)

[3](哈尔滨工业大学 (深圳), 广东 深圳 518055)

通信作者: 张宇, E-mail: yuzhang@hit.edu.cn

摘 要: RPKI 作为一项 BGP 安全增强的关键技术, 通过密码学验证路由中的起源真实性, 以防范 BGP 前缀劫持等攻击. RPKI 自 2012 年正式部署至今, 其部署规模日益增长, 目前互联网中一半以上的 IP 地址前缀已被 RPKI 覆盖. 为了解 RPKI 部署情况, RPKI 测量研究有助于更清晰地了解 RPKI 部署现状, 发现部署中存在的安全问题. 从 RPKI 数据对象测量、ROV 测量和 RPKI 基础设施测量这 3 个方向总结现有的 RPKI 测量工作. 对 RPKI 对象覆盖规模和 ROV 覆盖规模的测量结果进行总结, 展示了近年来 RPKI 部署的发展趋势, 并深入分析了不同 ROV 测量方案的优缺点. 还总结了 RPKI 的安全缺陷与 RPKI 的数据质量等问题, 最后给出了推动 RPKI 规模化安全部署的建议.

关键词: 边界网关协议安全; 资源公钥基础设施; 资源公钥基础设施测量

中图法分类号: TP309

中文引用格式: 张泽源, 刘翔, 张宇, 张伟哲, 方滨兴. RPKI测量研究综述. 软件学报, 2026, 37(1): 464–484. http://www.jos.org.cn/1000-9825/7459.htm

英文引用格式: Zhang ZY, Liu X, Zhang Y, Zhang WZ, Fang BX. Survey on RPKI Measurement Research. Ruan Jian Xue Bao/Journal of Software, 2026, 37(1): 464–484 (in Chinese). http://www.jos.org.cn/1000-9825/7459.htm

Survey on RPKI Measurement Research

ZHANG Ze-Yuan[1], LIU Xiang[2], ZHANG Yu[1,2], ZHANG Wei-Zhe[1,2], FANG Bin-Xing[2,3]

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

[2](Pengcheng Laboratory, Shenzhen 518055, China)

[3](Harbin Institute of Technology (Shenzhen), Shenzhen 518055, China)

Abstract: Resource public key infrastructure (RPKI) is a key technology for enhancing border gateway protocol (BGP) security, using cryptographic verification to prevent attacks such as prefix hijacking. Since its formal deployment in 2012, RPKI has grown to cover over half of Internet prefixes. Ongoing research on RPKI deployment helps to provide insights into current trends and identify security issues. This study reviews existing works on RPKI measurement from three perspectives: RPKI data object measurement, ROV measurement, and RPKI infrastructure measurement. It analyzes RPKI data object and ROV coverage metrics, deployment trends, and the effectiveness of different measurement approaches. Moreover, key security vulnerabilities and data quality issues are identified, and recommendations to promote large-scale RPKI deployment are proposed.

Key words: BGP security; resource pubic key infrastructure (RPKI); RPKI measurement

为了抵抗前缀劫持攻击, 增强 BGP 路由的安全性与稳定性, 互联网工程任务组 (Internet engineering task force, IETF) 于 2010 年开始推动资源公钥基础设施 (resource pubic key infrastructure, RPKI) 标准化[1]. RPKI 基于公钥基础设施 (public key infrastructure, PKI)[2]扩展, 使用资源证书 (resource certificate, RC)[3]认证互联网号码资源

* 基金项目: 国家重点研发计划 (2022YFB3104800); 鹏城实验室重大攻关基金 (PCL2023A05)
收稿时间: 2024-12-10; 修改时间: 2025-03-19; 采用时间: 2025-04-29; jos 在线出版时间: 2025-09-03
CNKI 网络首发时间: 2025-09-04

(Internet number resource, INR) 授权, 使用路由起源授权对象 (route origination authorization, ROA)[4]认证 IP 地址前缀和合法自治域 (autonomous system, AS) 的映射关系. 依赖方 (relying party, RP) 从发布点同步 ROA 数据, 并进行路由起源验证 (route origin validation, ROV)[5], 配置路由策略过滤与 ROA 冲突的路由信息, 来保护自己免受前缀劫持攻击.

RPKI 部署过程可分为 ROA 部署和 ROV 部署. 在 ROA 部署中, RPKI 参与者部署证书权威 (certificate authority, CA), 签发资源证书或者 ROA, 对资源的分配与授权关系进行认证. RPKI 签名对象会被上传到分布式资料库中. 在 ROV 部署中, RPKI 参与者部署 RP, 从 RPKI 资料库同步、验证资源证书、ROA 等数据, 利用有效 ROA 过滤前缀起源错误的路由信息.

作为新兴的互联网安全增强基础设施, 为了解 RPKI 的部署情况, 近年来对 RPKI 测量工作也在不断展开, 这些工作主要可分为以下几类.

(1) RPKI 功能测量: 对 RPKI 的主要功能进行测量, 测量工作按照 CA 侧功能和 RP 侧功能分为两类.

● RPKI 数据对象签发情况测量: 主要测量 RPKI 数据对象的签发情况, 包括对 ROA 覆盖规模、RPKI 数据质量的测量.

● ROV 测量: 主要测量互联网中实施 ROV 过滤的 AS, 即在域间路由中使用 ROV 来过滤无效路由信息的 AS.

(2) RPKI 基础设施测量: 对支撑 RPKI 功能所使用的底层组件如 CA、RP 等进行测量, 包括对软件的评估、对运行情况 (例如, 是否与最佳实践相符) 和部署弹性 (例如, 是否部署安全防范措施等) 的测量.

目前对 RPKI 研究已有一些综述性的工作. 文献 [6] 总结了 RPKI 存在的一些问题, 包括可扩展性, 资料库恶意操作, 资源重复分配等问题. 文献 [7] 总结了 RPKI 研究现状, 包括基于 RPKI 的应用和 RPKI 技术改进, 但未聚焦在 RPKI 测量方面. 在 RPKI 测量工作的综述方面, 文献 [8] 从 ROA 部署、ROV 部署以及 RPKI 弹性这 3 个方面对测量工作进行了详细综述, 但是缺失 ROV 部署测量方案分析, 也缺少 ROA 数据质量分析. 与上述工作对比, 本文全面梳理了 RPKI 测量工作并补充了方案对比分析.

本文第 1 节主要介绍 RPKI 的技术背景和发展现状. 第 2 节总结针对 RPKI 数据对象签发的测量工作, 包括对 ROA 规模和 RPKI 数据质量的测量. 第 3 节总结 ROV 测量工作, 分析现有 ROV 测量方案优缺点. 第 4 节从支撑 RPKI 功能的角度对 RPKI 基础设施测量工作进行梳理, 总结现有部署方案缺陷. 第 5 节总结分析 RPKI 在实际部署应用中遇到的问题与挑战, 并给出相应建议. 第 6 节对全文进行总结, 并简述未来研究趋势.

1 RPKI 技术背景与架构

1.1 RPKI 技术背景

由于在设计之初缺乏安全性考虑, 随着网络的发展, BGP 协议在安全上的脆弱性逐渐显露[9,10]. 前缀劫持是 BGP 面临的安全隐患之一, 其传播迅速, 严重影响了互联网的正常运行[11−15].

针对 BGP 协议的安全改进成为学术界和工业界的研究热点[16−22]. 2000 年, Kent 等人[20]提出第 1 个 BGP 安全增强技术 S-BGP, 利用密码学技术解决 BGP 协议的安全问题[23]. 但其设计过于理想化, 未考虑路由器现实性能的限制和互联网复杂的运行模式, 不适合实际部署使用[24].

2006 年, 互联网工程任务组成立了域间路由安全 (secure inter-domain routing, SIDR) 工作组, 开始对 RPKI 进行设计、开发, 并于 2010 年开展 RPKI 标准化工作. RPKI 继承了 S-BGP 的设计思想[25], 并简化了设计和功能以在互联网中实际部署. RPKI 利用数字证书体系认证互联网码号资源所有权, 保障路由起源信息的有效性. 2012 年 SIDR 工作组完成了 RPKI 整体技术框架和基础协议的标准化工作[25], 规范了 RPKI 的体系架构、资源管理模型、证书与签名对象结构、签名密钥与算法、路由起源验证流程等内容[1,3−5,26−35]. 同年, 全球 5 个地区性互联网注册机构 (regional Internet register, RIR) 牵头开始正式生产部署 RPKI.

2017 年, RPKI 标准化工作宣告完成, 同年 IETF 成立了域间路由安全操作 (secure inter-domain routing operations, SIDROPS) 工作组来解决 RPKI 部署和运维中发现的问题, 并进一步推动 RPKI 全球化部署. SIDR 工作组在完成使命后于 2018 年解散.

1.2 RPKI 技术架构

RPKI 以 PKI 体系为基础建立了层级化的互联网号码资源授权体系, 使得互联网号码资源授权关系可通过密码学验证. 图 1 给出了 RPKI 的架构图, 在 RPKI 体系中 5 大 RIR (APNIC、ARIN、RIPE NCC、AFRINIC 和 LACNIC) 作为信任锚点, 担任根 CA 的职能. 国家互联网注册机构 (national Internet register, NIR)、本地互联网注册机构 (local Internet register, LIR) 和互联网服务提供商 (Internet service provider, ISP) 等网络组织担任层级 CA 的职能, 为下级组织授权互联网号码资源的同时颁发 RC 认证. 资源拥有者可使用 RC 签发 IP 前缀和起源 AS 映射的密码学断言, 即 ROA, 保护路由起源安全. 路由参与者可以利用有效 ROA 来过滤与 ROA 不相符的路由来保护流量不被劫持.

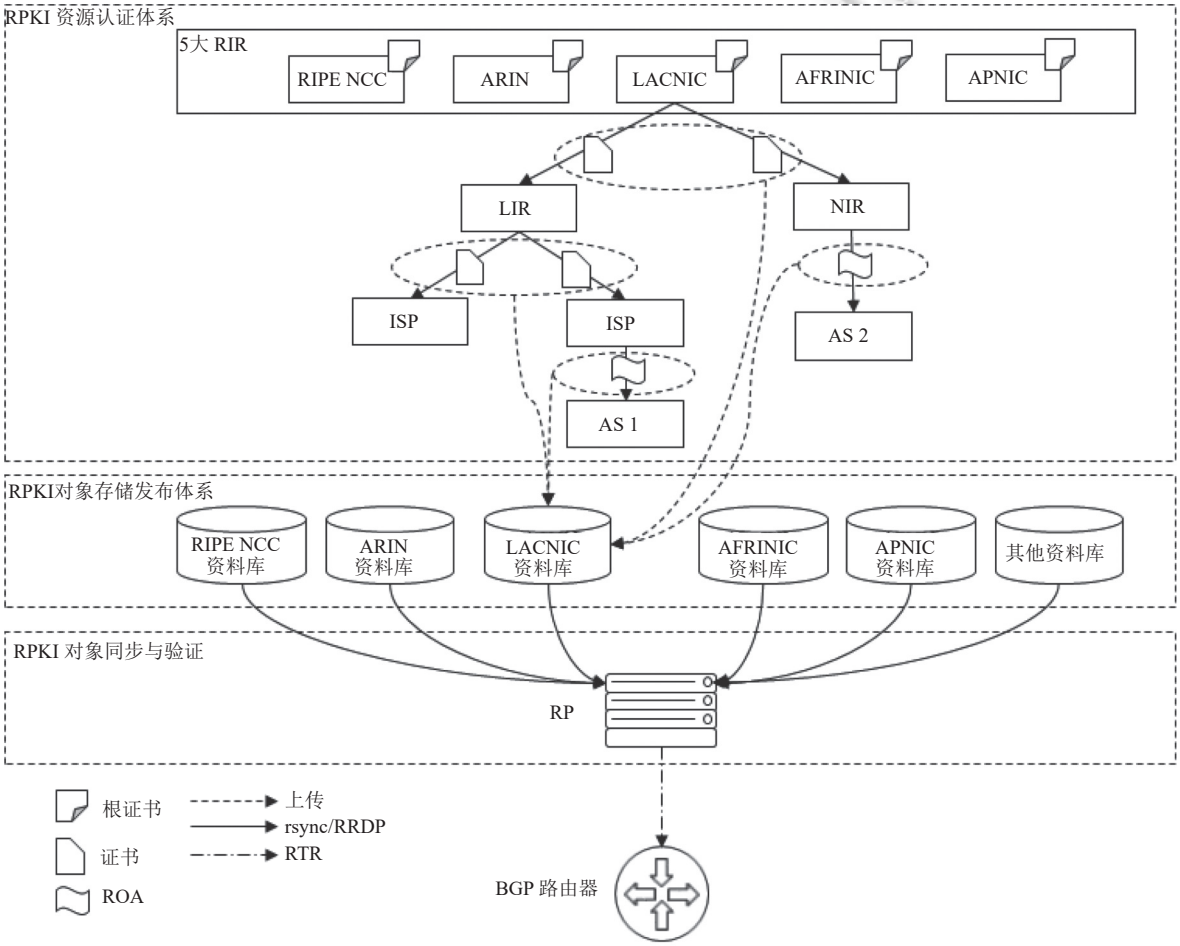


图 1 RPKI 架构图

RPKI 使用分布式资料库管理、存储、发布 RC 和 ROA 等 RPKI 对象, RPKI 允许两种模式的资料库——托管模式 (hosted model) 和授权模式 (delegated model). 在托管模式中, CA 将自己的 RC 和 ROA 委托给 RIR 存储和管理, 采用托管模式的 ISP 不需要自己部署维护 CA, 这对大多数缺少密码学经验的 ISP 来说节省了很多部署开销, 目前大多 ISP 选择托管资料库. 在授权模式中, CA 管理与发布分离, ISP 部署运营自己的 CA, 自主管理 RC 和 ROA, ISP 可以选择自己建立资料库 PP 或者委托给第三方如云服务提供商, 以提供更好的网络连接服务.

● ROA. ROA 是记录 IP-AS 映射关系的签名对象, 语义上表示 AS 可以在 BGP 中作为起源 AS 声明的 IP 前

缀. ROA 包含以下信息: AS 号、前缀-maxLength, 其中 maxLength 属性用于限制路由前缀的最大长度. 例如, AS 999 123.1.0.0/20-24 表示 AS 999 可以在 BGP 中声明前缀 123.1.0.0/20 或其任意子前缀的路由, 但子前缀的长度不能超过 24.

● ROV. ROV 在 BGP 路由器上执行, 用于验证路由器接收路由的起源合法性. 如表 1 所示, ROV 的结果可被分为 3 类, 分别为 valid、invalid 和 not found. BGP 路由器可以使用不同的路由策略, 例如优先 valid 路由和 not found 路由, 较为谨慎的 AS 为了避免与目的地失去连接, 当仅有 invalid 路由时也会选择接受.

表 1　起源验证结果分类

结果	原因
valid	BGP路由的IP地址前缀和ASN (autonomous system number)与1个或多个ROA匹配, 并且宣告的前缀长度不超maxLength
invalid	BGP路由的IP地址前缀被一个或多个ROA覆盖, 但ASN不匹配或者路由的前缀长度超过ROA的maxLength
not found	BGP路由的IP地址前缀没有被ROA覆盖

● RP. RP 串联了 RPKI 与域间路由. 在 RPKI 侧, RP 根据信任锚位置 (trust anchor locator, TAL)[32]访问 RPKI 资料库, 使用 rsync 或者 RRDP[36]协议同步 RPKI 数据, 并执行从根证书到 ROA 的链式验证, 获取有效的 ROA 负载 (validated ROA payload, VRP). 在域间路由侧, RP 使用 RPKI 路由协议 (RPKI to router, RTR)[37]将 VRP 传输给 BGP 路由器. RP 的设计将密码学验证流程从路由器剥离, 降低了路由器性能和存储的负载压力, 减少了数据同步、验证的时间开销.

● RPKI 本地化管理. SLURM[38]机制增加了 RPKI 配置的灵活性. 如图 2 所示, SLURM 机制允许 RP 添加“本地过滤和断言”来创建本地路由认证视图. 过滤机制类似黑名单, 断言机制类似于白名单, RP 可以按需求增加、删除路由认证结果.

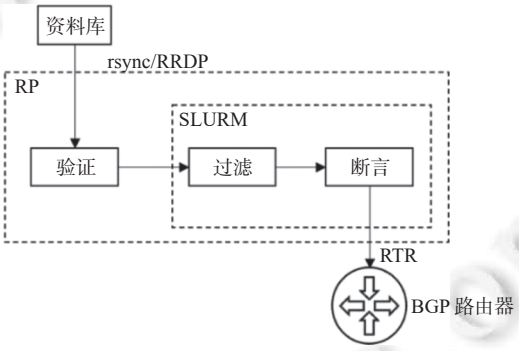


图 2　SLURM 机制

2　RPKI 数据对象签发情况测量

RPKI 数据对象签发情况的测量工作可分为以下两类.

● ROA 规模测量: 测量 ROA 覆盖规模, 包括签发 ROA 的 AS 数量、被 ROA 覆盖的 IP 前缀数量、被 ROA 覆盖的 IP 地址占全球 IP 地址空间的比例等.

● RPKI 数据质量测量: 对 RPKI 签名对象的数据质量问题进行测量, 包括 ROA 配置错误、maxLength 设置过长、资源授权冲突等.

2.1　ROA 规模测量

RPKI 的 ROA 覆盖规模可以从两个维度体现: 从 IP 地址的维度来看, ROA 规模可以用 ROA 覆盖路由前缀的

在互联网 IP 地址空间中的占比来表示; 从 AS 的维度来看, ROA 规模可以用签发 ROA 的 AS 数量表示. ROA 规模的测量方法比较简单, 一般包含 3 个步骤: ① 从 BGP 公开采集点下载路由数据, 提取出路由起源 AS 和 IP 前缀构成 AS-IP 对集. ② 从 RPKI 资料库同步 RPKI 数据, 进行层级验证得到有效 ROA 数据. ③ 利用有效 ROA 数据验证 AS-IP 对, invalid 和 valid 的 AS-IP 对的占比值和即可表示 ROA 覆盖规模.

Wählisch 等人[39]的测量工作发现, 截止到 2012 年 4 月互联网中仅 2% 的 IP 前缀被 ROA 覆盖, 其中 1.6% 的前缀路由验证结果为 valid, 剩余 0.4% 验证结果为 invalid. 对 invalid 路由产生的原因进一步分析发现, ROA 配置错误和 RPKI 测试导致相当多路由被验证为 invalid. 这表明在 RPKI 实际部署中, 仍然存在大量用户缺乏部署经验或最佳实践的指导.

Iamartino 等人[40]的测量从 2012 年 3 月持续到 2014 年 9 月, 期间 ROA 对 IP 前缀的覆盖率从 2.05% 增长到 5.41%. 测量末期发现 5 个 RIR 中 RIPE NCC 的部署最为活跃, 部署率达到了 15.68%, LACNIC 次之, APNIC 和 ARIN 的部署远落后于其他 3 个 RIR. 测量还发现约 80% 的 invalid 路由的前缀实际可达, 原因是这些前缀还被其他的 valid 和 not found 路由所覆盖, 即这些前缀同时被多个 AS 声明.

Wählisch 等人[41]将视角转向网站域名, 在 2015 年测量了 Alexa 的 top 1M sites 中网站域名所在 IP 前缀的 RPKI 覆盖率. 测量涵盖了 1 167 086 个 www 域名的 IP 地址和 1 154 170 个非 www 域名的 IP 地址, 分别映射到 1 369 030 和 1 334 957 个不同的前缀 AS 对, 其中仅 6% 的 Web 服务器前缀被 ROA 覆盖. 测量还发现内容分发网络 (content delivery network, CDN) 的 RPKI 部署率较低, 原因在于签发 ROA 会暴露运营商的业务信息. 此外, 部署收益低于部署成本也是运营商不愿意部署 RPKI 的一个原因.

Chung 等人[42]对 RPKI 在 IPv4 中的覆盖情况进行了长达 8 年的测量. 测量结果显示, 截至 2019 年已有 12.1% 的 IPv4 地址空间被覆盖. 在 5 个 RIR 中, RIPE NCC 的部署仍是最活跃的, 其管辖的 AS 中有 16.04% 都签发了至少 1 个 ROA, 而 LACNIC、APNIC、AFRINIC 和 ARIN 的这一数字仅分别为 9.33%、8.14%、3.30% 和 1.47%. 测量还发现 RPKI 的 ROA 部署规模在逐年增加, 特别是在 2017–2019 年间, 增长相较之前较为迅速.

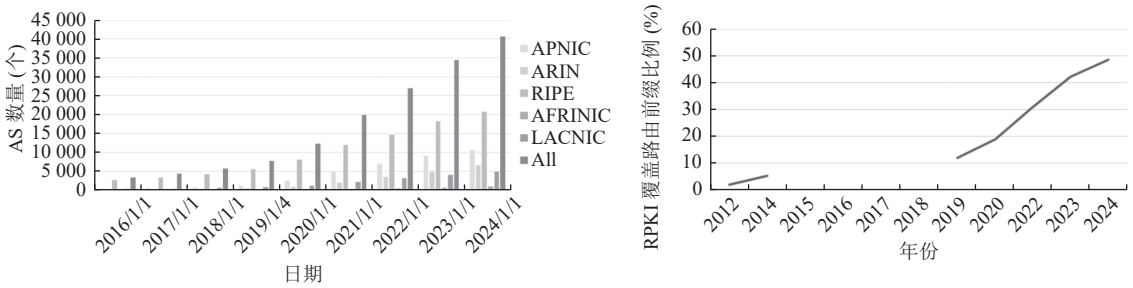
Hlavacek 等人[43]收集了 14 万个 ROA 的数据, 发现 39.3% 的 IPv4 前缀和 39.8% 的 IPv6 前缀被 ROA 覆盖. NIST RPKI 监控器[44]持续对 RPKI 的覆盖度进行测量, 发现截止到 2024 年 9 月 19 日, 53.52% 的 IPv4 前缀和 58.91% 的 IPv6 前缀被 ROA 所覆盖.

表 2 总结了自 2012 年来 ROA 部署规模测量工作的测量结果. RIPE NCC 按日存储了从 2011 年至今的 RPKI 历史数据, 图 3(a) 展示了 2016–2024 年每年的 1 月 1 日签署 ROA 的 AS 数量 (2019 年 1 月 1 日的数据缺失, 因此使用 1 月 4 日的数据代替), 图 3(b) 展示了 2012–2024 年 RPKI 对 IPv4 路由前缀覆盖率的变化, 数据来源于 NIST RPKI 监控器和文献 [39−42] (缺失 2015–2018 年的数据). 根据不同时期的测量结果可知, 在 RPKI 开始部署之初, 发展较为缓慢, 从 2012 年到 2019 年 ROA 的覆盖规模仅从 2% 增长到 12.1%. 自 2019 年起, RPKI 的发展速度加快, 如今 ROA 已覆盖全球超过一半的 IP 前缀[7]. 其原因在于, 自 2018 年起 RIR 开始全面推动 RPKI 部署, 各大型互联网服务提供商 ISP 和 CDN (如 Cloudflare、谷歌、亚马逊等) 开始支持和部署 RPKI[45], 推动 RPKI 迅速发展. 截止到 2024 年, 有超过一半的 IP 前缀进行了 RPKI 认证.

表 2　ROA 规模测量结果

文献	时间	覆盖率 (%)
Wählisch等人[39]	2012年4月	2.0
Iamartino等人[40]	2014年9月	5.4
Wählisch等人[41]	2015年	6.0*
Chung等人[42]	2019年	12.1 (IPv4)
Hlavacek等人[43]	2022年	39.3 (IPv4), 39.8 (IPv6)
NIST RPKI[44]	2024年9月19日	53.5 (IPv4), 58.9 (IPv6)

注: *仅测量网站域名的覆盖程度



(a) 部署 RPKI 的 AS 规模变化　　(b) RPKI 的 IP 覆盖规模变化趋势

图 3　RPKI 的 AS 和 IP 规模变化趋势

2.2　RPKI 数据质量测量

RPKI 数据质量直接影响着 RPKI 的可信度和声誉, 数据质量不佳也是阻碍 RPKI 发展的一个原因. 近年来有许多测量工作陆续发现了 RPKI 中存在的数据质量问题, 包括如下.

● ROA 与实际路由不一致: 由于人为失误、缺乏 BGP 专业知识、更新不及时等原因, 签发的 ROA 与实际路由信息存在冲突, 导致路由在 RPKI 起源验证中被验证为 invalid, 其后果是部署 RPKI 过滤的 AS 会与合法目的地断开连接.

● ROA maxLength 设置过长: maxLength 设置过长会导致 ROA 认证前缀范围比实际路由声明前缀范围大, 容易受到伪造起源子前缀劫持 (forged-origin subprefix hijack) 攻击[46].

● 互联网号码资源授权冲突: 互联网号码资源授权冲突指资源拥有者将同一个 IP 地址前缀或 AS 号码授权给不同的 ISP, 产生资源的重复授权或者资源拥有者将不属于自己的资源授权给 ISP.

(1) ROA 与实际路由不一致

Xu 等人[47]发现部分 AS 签发 ROA 时未考虑流量工程、前缀聚合失败或 IP 前缀所有权转移的情况, 导致声明的路由被验证为 invalid. 但这些路由实际应该是合法的. Xu 等人提出了 6 种容易出现 ROA 配置错误的场景. 经过 2018 年 2–5 月的测量, Xu 等人发现超过 60% 的 invalid 路由是由 ROA 配置错误导致, 实际应该是合法的路由. 此外, 他们还发现 ROA 配置错误导致的 invalid 路由都会长期存在, 与前缀劫持攻击持续时间短的特点不相符.

Chung 等人[42]探究了导致路由验证结果为 invalid 的原因. 他们发现原因之一是路由中前缀的长度超过了 ROA 中前缀的长度. 这类 invalid 路由的占比在 48.0%–51.5% 之间, 其中超过 90% 是因为 ROA 中未设置 maxLength 而非实际的前缀劫持. 另一个导致路由被验证为 invalid 的原因是路由的起源 AS 与 ROA 中 AS 不相符, 这类 invalid 路由更符合前缀劫持攻击的特点. 但 Chung 等人发现其中部分 invalid 路由是 ROA 配置错误而非前缀劫持导致的. 这些 ROA 配置错误包括: 1) AS 归属于同一 ISP, ISP 在两个 AS 都对同一前缀发布了路由但只对其中一个 AS 发布了 ROA; 2) AS 将子前缀分配给客户, 但没有更新 ROA; 3) AS 使用了 DDoS 防护, 在不同 AS 发布了同一前缀的路由, 但未及时更新 ROA. 与文献 [47] 类似, Chung 等人的测量也发现 ROA 配置错误导致的 invalid 路由存在时间相对较长的特点.

Hlavacek 等人[48,49]提出了区分 ROA 配置错误和实际前缀劫持的两个分类器. 第 1 个分类器使用 invalid 路由存在时间作为分类依据, 将持续时间较长的 invalid 路由分类为 ROA 配置错误导致的; 第 2 个分类器根据路由中起源 AS 与前缀的相关性进行分类, 若起源 AS 与前缀存在足够高的相关性, 则判断为是 ROA 配置错误而非前缀劫持, 其中相关性的证据可来自各种外部数据源, 例如 IRR 数据库、DNS 记录、whois 数据库等.

文献 [48,49] 对 2019 年 1 月的 89 730 起路由与 ROA 冲突进行识别并向相关运营商进行了核实, 分类器识别出 132 例冲突为 ROA 配置错误引起, 其中 123 例分类正确; 33 例冲突为劫持攻击引起, 其中 18 例分类正确.

(2) ROA maxLength 设置过长

Gilad 等人[50]在 2017 年发现 Loose ROA 的问题. Loose ROA 指 ROA 中包含的 maxLength 长度的子前缀未全部在 BGP 中宣告, 其原因在于 ROA 中 maxLength 设置过长. 例如 AS 999 仅声明 1 个/20 前缀——45.110.0.0/20

的路由, 但发布 maxLength 为 24 的 ROA:

45.110.0.0/20-24, AS 999.

发布 Loose ROA 的 AS 会面临伪造起源子前缀劫持攻击的威胁, 即攻击者可假装邻居伪造 AS 999 未宣告的/24 前缀的虚假 BGP 路由:

45.110.2.0/24, AS_PATH: 攻击者-AS 999.

该 BGP 路由的 RPKI 起源验证结果为 valid, 且由于最长前缀匹配机制, AS 会优先选择虚假路由而不是 45.110.0.0/20 的真实路由, 因此所有访问 45.110.2.0/24 的流量都会被攻击者劫持. Gilad 等人的测量发现互联网中约 30% 的 IP 前缀被 Loose ROA 覆盖.

同年, Gilad 等人[46]提出 AS 应该避免使用 maxLength 的部署建议, 因为使用 maxLength 可能会使发布的 ROA 不是 minimal ROA[51]. minimal ROA 中只包含 BGP 宣告的 IP 前缀, 因此不会受到伪造起源子前缀劫持攻击的威胁. Gilad 等人在 2017 年 6 月 1 日的测量发现 ROA 中有 4630 个前缀 (约 12%) 的 maxLength 长于前缀长度, 其中 84% 的前缀的 ROA 都是非 minimal ROA, 会受到伪造起源劫持攻击的影响. Gilad 等人对 maxLength 的使用建议已作为最佳实践写入 RPKI 标准化文档[52].

(3) 互联网号码资源授权冲突

Zou 等人[53]定义并测量了 RPKI 中的互联网号码资源授权冲突. 互联网号码资源拥有者可对 IP 地址前缀进行 3 种操作: 1) 自己使用; 2) 作为保留地址; 3) 分配给客户. 在 RPKI 中对应 3 种数据对象签发行为: 1) 为 IP 地址前缀发布 ROA; 2) 为 IP 地址前缀发布 AS 0 ROA; 3) 为客户签发 RC. 互联网号码资源拥有者对不属于自己的 IP 地址前缀进行操作或者对同一 IP 地址前缀同时进行多种操作就会造成互联网号码资源授权冲突. Zou 等人定义了 6 类资源分配或授权冲突 (如表 3 所示), 并采集了 2020 年 4 月 14 日的 RPKI 数据进行互联网号码资源冲突测量. 测量发现 2 起 B 类冲突, 5 起 C 类冲突, 4 起 E 类冲突. 测量还发现了 248 起潜在的 D 类冲突, 但无法判断是实际互联网号码资源冲突还是互联网号码资源转移后上级 CA 未及时撤销已发布的 ROA.

表 3　互联网号码资源授权冲突类型与测量结果[53]

冲突类型	冲突原因	测量结果 (起)
A类: 非法分配	CA分配了不属于自己的资源给客户	—
B类: 根CA重复分配	信任锚 (trust anchor, TA) CA分配了相同的资源给多个客户	2
C类: 中间CA重复分配	非信任锚CA分配了相同的资源给多个客户	5
D类: ROA (AS≠0) 与证书冲突	CA将使用的资源分配给客户	248 (潜在)
E类: ROA (AS=0) 与 ROA (AS≠0) 冲突	CA对保留的资源发布了ROA	4
F类: 证书与ROA (AS=0) 冲突	CA将保留的资源分配给了客户	—

表 4 总结了近年来数据质量测量工作. ROA 数据质量问题是现有 RPKI 体系无法解决的, 因为 RPKI 不保证 ROA 配置的正确性. 由于人为失误难以避免, 因此 ROA 数据质量问题难以根治, 目前可考虑以下几种减少影响的措施.

表 4　ROA 数据质量测量总结

测量目标	文献	测量时间	测量结果
ROA与实际路由不一致	[47]	2018年2–5月	超过60%的invalid路由由于ROA配置错误导致
	[42]	2011–2019年	(1) 超过90%前缀过长invalid路由是由于ROA未设置maxLength (2) 部分起源AS不符的invalid路由是由于ROA配置错误导致
	[48,49]	2019年1月	ROA配置错误导致138个路由被验证为invalid
ROA maxLength设置过长	[50]	2017年	约30%的IP前缀被Loose ROA覆盖
	[46]	2017年6月1日	ROA中有4630个前缀的maxLength长于前缀长度, 其中84%的前缀的ROA都是非minimal ROA
互联网号码资源授权冲突	[53]	2020年4月14日	发现11起互联网号码资源授权冲突, 248起潜在互联网号码资源授权冲突

(1) 对 RPKI 进行实时监控, 及时发现配置错误, 降低其带来的影响.

(2) 使用自动化配置代替人为配置, 例如使用文献 [46] 中给出的算法代替人工设置 maxLength.

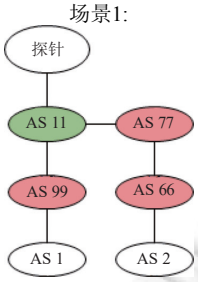
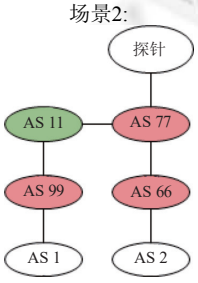
(3) 使用其他权威数据源检测资源配置, 利用 IRR、whois 等数据对 ROA 的 IP 资源进行检测, 及时发现资源键入错误.

3 ROV 测量

ROV 测量的主要目的是了解互联网中 AS 采用 ROV 技术过滤 invalid 路由的情况, 包括部署 ROV 的 AS 及其数量. 与 ROA 规模测量相比, ROV 测量更为困难. 因为判断一个 AS 是否部署 ROA, 可以简单地通过对比 RPKI 数据和 BGP 数据, 然而, 判断一个 AS 是否部署 ROV 则需要复杂的推测方法.

在 ROV 测量中, 推测一个 AS 部署 ROV 的基本依据是该 AS 接受起源验证有效的路由, 且可以过滤无效的路由. 表 5 给出了一种 ROV 测量方案示例. 测量者控制 AS 1 和 AS 2, 并让两个 AS 同时声明两个前缀的路由. 测量者使用两种 ROA 配置, 每种配置使一个 AS 的一个路由验证为 valid, 另一个路由验证为 invalid, 另一个 AS 的路由有效性相反. 然后使用网络探针对两个前缀进行 traceroute 获取连通性信息来推测 ROV 部署情况.

表 5 ROA 测量方案示例

实际测量场景	测量场景描述	ROA配置	traceroute结果	推测结果
场景1:  	AS 1和AS 2为测量者控制的自治域, 同时声明了前缀p1和p2的路由. AS 11部署了ROV过滤无效路由, 其他3个AS未部署ROV. 测量者在两种ROA配置下对p1和p2进行traceroute	测量者签发ROA: {(AS 1, p1), (AS 2, p2)}	对p1: 11-99-1 对p2: 11-77-66-2	在两种ROA配置中, traceroute总是路由到有效的起源自治域. traceroute路径总是在AS 11发生“改变”, 选择有效的路由, 说明AS 11大概率部署了ROV. 而其他AS是否部署ROV需要其他探针的traceroute结果来判断
		测量者签发ROA: {(AS 1, p2), (AS 2, p1)}	对p1: 11-77-66-2 对p2: 11-99-1	
场景2:  		测量者签发ROA: {(AS 1, p1), (AS 2, p2)}	对p1: 77-66-2 对p2: 77-66-2	在两种ROA配置中, AS 77和AS 66总是使用AS 2声明的路由, 无论路由的有效性, 说明AS 77和AS 66都没有部署ROV检测路由有效性
		测量者签发ROA: {(AS 1, p2), (AS 2, p1)}	对p1: 77-66-2 对p2: 77-66-2	

从表 5 场景 1 的测量结果可以发现 traceroute 到达了有效路由的起源自治域, 而 AS 11 是导致 traceroute 总是选择有效路由路径的关键 AS (traceroute 路径在该 AS 处发生分歧). 因此, 可以推测 AS 11 大概率部署了 ROV. 其他 AS 是否部署了 ROV 需要其他位置探针的 traceroute 结果才能判断.

从场景 2 的测量结果可以发现, 不管路由有效性如何, 探针的 traceroute 目的地总是到 AS 2. 这说明 AS 77 和 AS 66 无法识别路由的有效性, 因此可以推测 AS 77 和 AS 66 大概率没有部署 ROV.

在实际的 ROV 测量中, 测量方案需要解决 3 个主要问题.

(1) 如何排除非 ROV 过滤因素的影响. AS 路由过滤、防火墙等路由保护措施都可能对路由信息进行过滤, 与 ROV 过滤的功能在一定程度上类似. 这可能会导致测量者无法判断某一 AS 是否是因为部署了 ROV 才可以实现路由过滤效果, 在一定程度上会影响测量结果. 因此需要区分这些路由保护措施与 ROV 过滤.

(2) 如何排除附带收益 (collateral benefit)[50]的影响. 附带收益指因为上游 AS 部署了 ROV, 对无效路由起源宣

告进行过滤, 使得下游 AS 即使未部署 ROV 也可以不受到无效路由起源宣告的影响. 如图 4 所示, 部署了 ROV 的 AS 123 过滤了来自攻击者 AS 999 的无效路由起源宣告, 因此未部署 ROV 的下游 AS 124 也未受到无效路由的影响. 附带收益会使未部署 ROV 的 AS 也表现出 ROV 过滤的行为, 造成推测的假阳性.

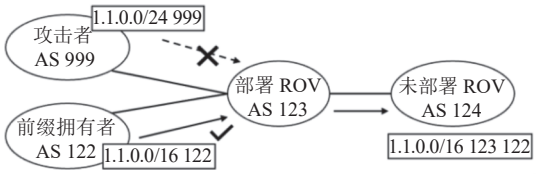


图 4 ROV 部署的附带收益

(3) 如何扩大 ROV 测量覆盖的范围. ROV 测量范围依赖于测量探针的可见性, 在不影响网络运行的情况下合理利用探针扩大测量范围, 有助于更好更清晰地了解全互联网的 ROV 部署情况.

近年来, 学术界、工业界针对全球 ROV 部署情况进行了多次测量工作. 这些测量工作可分为主动测量和被动测量两类. 在主动测量方案中, 测量者主动向待测 AS 发送协议数据包测量待测 AS 与目的 AS 的连通性, 常用的协议有 HTTP 协议、TCP 协议和 ICMP 协议. 在被动测量方案中, 测量者不主动发送数据包, 仅利用接入网络的测量探针测量待测 AS 与目的 AS 的连通性. 测量工作按照测量者是否能够控制 IP 地址前缀和 ROA 分为受控制测量和非受控测量.

Gilad 等人[50]在 2017 年首次提出一种被动 ROV 部署测量方案, 该方案在控制面上运行, 利用路由探针采集路由数据. 该方案首先找出一个既发布有效 BGP 路由起源宣告, 又发布无效 BGP 路由起源宣告的 AS, 然后判断在该 AS 和 BGP 收集器之间是否只存在一个转发 AS. 如果该转发 AS 满足以下两个条件, 则认为该 AS 部署了 ROV.

1) 该 AS 转发源 AS 发布的有效 BGP 起源宣告, 并且丢弃源 AS 发布的无效的 BGP 起源宣告.

2) 该 AS 的上述行为被至少 3 个起源 AS 观测到.

该方案测量于 2016 年 7 月进行, 覆盖了规模前 100 的 ISP, 发现 9 个 ISP 部署了 ROV, 78 个 ISP 未部署 ROV, 剩余 13 个 ISP 无法判断. 该方案较为简单, 难以判断过滤无效路由的行为是否由 ROV 引起, 要求待测 AS 是路径中唯一表现出过滤无效路由行为的 AS, 这降低了附带收益的影响, 但同时也减少了测量覆盖的范围.

Reuter 等人[54]复现了 Gilad 等人的测量工作, 并且发现其是非受控的, 且测量结果高度依赖于路由收集器集合的选取. 针对此问题, Reuter 等人提出了一种在控制面运行的受控测量方案, 测量者能够主动声明路由信息且发布 ROA. 该方案需要待测 AS 满足两个前提假设.

1) 连接假设: 待测 AS 需要与测量者控制的 AS 直连.

2) 可见性假设: 待测 AS 的路由信息可被观测.

在该方案中, 测量者控制 AS 发布两个不同前缀的路由—对照前缀和实验前缀, 且交替使用两种 ROA 配置. 测量中对照前缀的路由始终保持 valid 状态, 而实验前缀的路由有效性在 valid 和 invalid 之间切换. 如果实验前缀的路由从 valid 变为 invalid 时, 待测 AS 过滤了实验前缀的路由或待测 AS 到达实验前缀的路由与对照前缀的路由不同, 则推测待测 AS 部署了 ROV. 测量分别在 2017 年的 2 月、5 月和 8 月进行, 覆盖了 730 个 AS, 但满足连接假设和可见性假设的 AS 仅有 68 个, 发现 3 个 AS 部署了 ROV. 该方案采用受控的测量方案, 引入对照前缀, 降低了其他非 ROV 过滤因素的影响. 同时该方案的连接假设排除了上游 AS 部署 ROV 带来的附带收益影响, 但连接假设和可见性假设的引入也限制了测量覆盖的范围.

Hlavacek 等人[55]重复了控制平面的测量, 并且进一步提出了数据平面的测量方案. 该方案采用了受控制的测量方案, 在前缀发布上与文献 [54] 略有不同. 在两个 AS 分别都发布两个前缀路由并设置两种 ROA 配置, 每种配置都使一个 AS 的一个前缀的路由有效, 另一个前缀的路由无效, 而另一个 AS 的前缀有效性相反. 在数据平面上的测量方案有两种, 一种是使用 RIPE Atlas 的探针在两种 ROA 配置下分别对两个前缀进行 traceroute, 然后将 IP 路径映射为 AS 路径; 另一种是向 top 1.25M Alexa 网站服务器发送 TCP SYN 数据包, 通过接收服务器的回复情

况来判断服务器 IP 是否受到保护. 在数据分析上, 将 AS 分为 4 类: 1) 第 1 类 AS 未部署 ROV, 这类 AS 出现在无效路由的路径上; 2) 第 2 类 AS 包含所有可能部署 ROV 的 AS, 这类 AS 仅出现在有效路由的路径上; 3) 第 3 类 AS 部署了 ROV 的概率较高, 这类 AS 在两种 ROA 配置下都出现在通往两个前缀的有效路由路径中; 4) 第 4 类 AS 为第 3 类的超集, 这类 AS 在两种 ROA 配置下至少出现在一个前缀的有效路由路径中, 这类 AS 部署了 ROV 的概率较低. 测量在 2017 年 2–6 月进行, 在控制面测量中, 发现 4 个 AS 可能部署了 ROV; 在数据面测量中, 发现了 12 个 AS 可能部署了 ROV, 其中 2 个 AS 部署了 ROV 的概率较高. 该方案在多个 AS 宣告了路由, 一定程度上降低了附带收益的影响, 但是其仅靠 AS 是否出现在有效、无效路由路径上来判断 AS 是否部署 ROV 的分析方式容易产生假阳性. 值得借鉴的是, 该方案利用数据平面上的测量扩充了探针的数量从而扩大了测量范围, 使得测量的 AS 由数百增加到数千个.

文献 [56,57] 利用 ICMP 协议在数据平面上进行了受控制的测量. 方案设置了两种探针, 一类配置有效前缀下的 IP 地址, 另一类配置无效前缀下的 IP 地址. 测量先使用有效 IP 地址探针向整个 IPv4 地址空间发送 ICMP 数据包, 然后利用无效 IP 地址探针向回复的 IP 地址发送 ICMP 数据包. 推测仅回复有效 IP 地址探针的 ISP 部署了 ROV, 而对两种探针均回复的 ISP 未部署 ROV. 该方案利用全地址空间扫描扩大了测量范围, 给出了 58 000 多个 AS 的测量结果. 但该方案无法确定 ICMP 数据包是由于 ROV 被过滤还是被 ICMP 过滤器过滤, 因此存在假阳性的可能; 该方案无法解决附带收益的问题.

RPKI WebTest[58]和 Cloudflare[59]提供了相似的实时测量服务, 在无效前缀路由和有效前缀路由下分别部署了网站, 若用户能够访问无效前缀下的网站, 说明所在 ISP 或者 ISP 上游未部署 ROV 防护.

Testart 等人[60]提出了一种利用统计方法粗略估计 ROV 部署情况的测量方案. 该方案基于一种启发式思想, 认为如果一个自治域将接收到的路由中的大部分都发送给邻居 AS, 且其中不包含无效路由信息, 则推测该自治域部署了 ROV 过滤. 基于此, 该方案提出了 full-feeder 的概念: 如果路由收集器的一个邻居 AS (peer) 发送给路由收集器的前缀起源对 (prefix-origin pairs) 数量大于全部前缀起源对的 75%, 则认为这个 AS 是一个 full-feeder. 如果一个 full-feeder 发送给路由收集器的无效前缀起源对少于所有前缀起源对的 20%, 则推测该 full-feeder 部署了 ROV. 测量了 2017 年 4 月–2020 年 1 月的 ROV 部署情况, 发现 ROV 部署呈上升趋势, 在 2017 年 4 月少于 2% 的 full-feeder 进行 ROV 过滤 (IPv4 中 219 个 full-feeder 仅有 3 个部署, IPv6 中 176 个 full-feeder 有 2 个部署), 到 2020 年 1 月下旬, IPv4 中 11% 的 full-feeder 部署 ROV (290 个中的 30 个), 而 IPv6 中有 10% (246 个中的 23 个). 该方案基于启发式的思路, 无法排除非 ROV 因素过滤的影响, 缺乏对 AS 过滤无效路由的直接验证, 且路由探针的可见性直接影响 AS 是否满足 full-feeder 的条件, 限制测量覆盖范围.

Huston 等人[61]提出了一种针对末端用户受 ROV 保护情况的测量方案. 与文献 [60] 类似, 方案不精确测量部署 ROV 的 AS, 而是测量现有 ROV 部署能保护多少用户. 方案在 DFZ (default-free zone) 中声明了一个路由, DFZ 指使用全路由表的互联网核心 AS 集合[62], 交替以 12 h 和 36 h 为间隔更改路由的有效性. 然后在路由前缀下配置了一个 Web 服务器, 在不同路由有效性下让用户访问 Web 服务器, 统计用户对服务器的可达性. 2020 年 6 月的测量显示约 17% 的用户受到了 ROV 过滤的保护.

Rodday 等人[63]的方案在文献 [54,55] 的基础上做了 3 点改进, 使得测量能够: 1) 放宽连接假设; 2) 区分 ROV 完全过滤和部分过滤; 3) 识别 IXP 过滤. 测量设置与文献 [55] 类似, 使用 RIPE Atlas 探针对对照前缀和实验前缀进行 traceroute, 并在此基础上额外发布了前缀路由进行测量以探究 IXP 中路由服务器的 ROV 部署情况. 方案的改进体现在数据分析部分. 待测 AS 按照是否满足连接假设分为两类: 1) 当待测 AS 满足连接假设时, 分析方法与文献 [54] 相同; 2) 当待测 AS 不满足连接假设时, 当待测 AS 是唯一过滤无效路由的 AS 时才能推测该 AS 部署了 ROV. 为区分 ROV 完全过滤和部分过滤, 该方案引入包含列表 (including list), 接受无效路由的 AS 会被加入包含列表中, 若推测部署 ROV 的 AS 出现在包含列表中, 则推测该 AS 进行部分过滤. 对路由服务器的测量让方案能够区分 IXP 过滤和 AS 过滤. 测量在 2021 年 7 月 2 日–7 月 19 日进行, 在 3 694 个 AS 中选择了 5 537 个探针, 推测 206 个 AS 部署了 ROV, 10 个为强置信度, 12 个为弱置信度, 184 个是通过 IXP 路由服务器过滤. 这 206 个 AS 中 146 个为全部过滤, 60 个为部分过滤. 该方案细化了 AS 分类, 首次识别了 ROV 完全过滤和部分过滤, 放宽连

接假设, 扩大了测量范围. 为防止放宽连接假设带来的假阳性, 方案加强了在不满足连接假设的情况下推测 AS 部署 ROV 的要求: 需要验证路径中的其他 AS 均没有进行 ROV 过滤, 因此这些 AS 中都需要部署有探针.

Gray 等人[64]和 Chen 等人[65]使用贝叶斯方法推断 AS 是否部署 ROV. 在贝叶斯模型中, AS 的 ROV 部署与否用概率表示, 即 AS 有多少概率部署 ROV 过滤. Chen 等人将互联网中发布有效路由和无效路由的 AS 作为目标 AS, 使用 RIPE Atlas 和 perfSONAR 的探针对这些 AS 的路由前缀进行 traceroute, 从而扩大了测量覆盖的范围. traceroute 路径通过 IP-AS 映射转化为 AS 路径, 获得 AS 路径和 AS 路径有效性 (即路径上目的 AS 是否是合法的起源 AS) 的二元数据集合. 通过贝叶斯公式, ROV 部署推断问题转化为求解每个 AS 部署 ROV 的概率为多少, 才能使观测到的数据集与实际测量得到数据集最相符. Gray 等人和 Chen 等人分别使用马尔可夫链蒙特卡罗 (Markov-chain Monte Carlo, MCMC) 和变分梯度下降 (Stein variational gradient descent, SVGD) 方法求解出每个 AS 部署 ROV 的概率分布, 使用概率分布的平均值和最高密度区间 (highest density interval, HDI) 为指标按阈值将 AS 的 ROV 部署情况分为 4 类: 完全部署、未部署、部分部署和未知. 测量于 2021 年 6 月 1 日–6 月 7 日进行, 测量覆盖 11 074 个 AS. 推测算法共发现 3 107 个 AS (28%) 完全部署了 ROV, 4 716 个 AS (43%) 未部署 ROV, 357 个 AS (3%) 部分部署了 ROV, 剩余 2 894 个 AS (26%) 无法推测. Chen 等人的方案利用互联网中的 AS 发布的有效无效路由对作为 traceroute 目标, 扩大了测量的范围, 方案使用概率推断, 无须考虑上游 AS 的影响. 在推断准确性上, 测量使用 is-bgp-safe-yet 为验证集进行了验证, 准确率达到 100%, 推断部署 ROV 的 AS 占实际部署 ROV 的 AS 的比例, 即召回率达到 92.98%.

Hlavacek 等人[66]的测量方案以文献 [54] 和文献 [63] 为基础, 测量设置两个相邻的/24 前缀并以文献 [63] 的方案使用两个 AS 宣告并设置两个 ROA 配置. 为了降低文献 [54] 方案的假阳性以及文献 [63] 推断不满足连接假设的 AS 是否部署 ROV 对探针的高要求, 引入了分歧点 (divergence point) 和更为详细的 AS 分类. 分歧点指总是选择有效前缀路由的 AS, 两个目的前缀相邻降低了分歧由其他路由因素过滤导致的可能性, 路径分歧很可能是因为分歧点部署 ROV 引起的. AS 根据所在路径有效性情况以及是否是分歧点进行分类, 共分为 7 类, 分歧点提供 ROV 部署的正面证据, 仅出现在有效路径或是偶尔出现在无效路径上区分完全过滤还是部分过滤. 测量在 2022 年 6 月 8 日和 10 日进行, 共测量 2 325 个 AS, 97 个 AS (约 4%) 部署 ROV 且部分过滤, 554 个 AS (约 24%) 部署 ROV 且完全过滤, 995 个 AS (约 43%) 没有部署 ROV, 剩余的 AS 无法判断. 分歧点的引入, 增加了判断不满足连接假设的 AS 是否部署 ROV 的依据, 也降低了上游 AS 过滤的影响.

RoVista[67]利用 IP-ID 侧通道技术测量 ROV 部署情况. 利用使用全局递增的 IP-ID 的主机作为虚拟探针 (vVP, virtual vantage point). 不被其他有效路由前缀覆盖的无效路由前缀称为测试 IP 前缀 (test IP prefix), 测试 IP 前缀下的测试主机为 tNode (test node). 在测量中向 tNode 发送多个以 vVP 为源地址的 TCP SYN 数据包, tNode 会回复 TCP ACK 数据包给 vVP, 导致 vVP 的 IP-ID 增长, 根据 vVP 的 IP-ID 增长模式能够判断 tNode 和 vVP 之间的连通性从而推断 ROV 部署. 与前面利用数据平面端到端协议的测量方案[54−59,61]相似, 该方案无法排除上游 AS 过滤的影响. 因此 RoVista 以 ROV 受保护分数衡量 AS, 而不是精确测量 AS 是否部署 ROV. 一个 AS 的 ROV 保护分数为被 ROV 过滤导致无法访问该 AS 内任一 vVP 的 tNode 的占比. 测量从 2021 年 12 月 24 日持续到 2023 年 9 月 12 日, 使用 1 396 407 个 vVP, 共覆盖 28 314 个 AS, 其中 10 249 个 AS (36.2%) 的 ROV 保护分数为 0, 即自身和上游未部署 ROV; 3 482 个 AS (12.3%) 的 ROV 保护分数为 1, 即自身或者所有上游 AS 部署了 ROV; 14 583 个 AS (51.5%) 的 ROV 的保护分数在 0–1 之间, 即表现出部分部署. RoVista 利用全局 IP-ID 主机作为探针, 极大地扩展了测量范围, 但其无法区分自身部署还是上游 AS 部署, 并且具有全局 IP-ID 特性的主机在逐渐被淘汰[66], 对后续的测量会产生影响.

表 6 总结了现有的 ROV 测量工作. ROV 测量方案在不断优化, 测量覆盖的范围在不断增加. ROV 测量存在的一个问题是难以验证测量结果. Cloudflare 的 is-bgp-safe-yet 项目依靠网络运营商的贡献提供 AS 的 RPKI 部署状态, 但截至 2024 年 8 月, 仅包含 427 个 AS 的 RPKI 部署情况且大多 AS 都是属于大型运营商, 难以满足验证需求. Rodday 等人[68]提出基于 Mininet 自动生成网络拓扑的框架来帮助验证 ROV 测量结果, 目前能够支持 4 000 个节点的仿真, 为解决 ROV 测量结果验证问题提供了一个思路.

表 6 ROV 测量工作总结

测量工作	测量方法	判定依据	测量时间	重要结论
Gilad等人[50]	● 非受控测量 ● 公开路由表采集	待测AS是否过滤相邻AS的无效路由而接受其有效路由	2016年7月	测量覆盖前100的ISP, 其中9个ISP部署了ROV, 78个未部署
Reuter等人[54]	● 受控测量 ● 公开路由表采集	在满足连接假设和可见性假设的前提下, 待测AS是否过滤受控AS的无效路由而接受其有效路由	2017年2月20–27日, 2017年5月11–17日, 2017年8月1–7日	1) 测量覆盖730个AS, 发现3个AS部署了ROV 2) 首次引入对照前缀, 提出连接假设和可见性假设, 提高了测量的可信度
Hlavacek等人[55]	● 受控测量 ● 公开路由表采集、traceroute、基于TCP的连通性检测	待测AS所在AS路径的有效性	2017年2月–6月	1) 测量覆盖了2092个AS, 12个AS可能部署了ROV 2) 使用数据面测量, 扩大测量范围
文献[56,57]	● 受控测量 ● ICMP扫描	待测AS内主机回复路由的有效性	2018和2019年	测量覆盖了5万多个AS
RPKI WebTest[58]	● 受控测量 ● 基于HTTP的连通性检测	待测AS内的用户是否无法访问无效路由下的Web服务器而能够访问有效路由下的Web服务器	在线	—
Cloudflare Inc[59]	● 受控测量 ● 基于HTTP的连通性检测	待测AS内的用户是否能够访问无效路由覆盖的Web服务器	在线	380个AS提供了ROV配置信息
Testart等人[60]	● 非受控测量 ● 公开路由表采集	待测AS是否将大部分路由发送给邻居AS且同时只将少部分无效路由发送给邻居AS	2017年4月–2020年1月	测量覆盖了536个AS, 53个AS部署了ROV
Huston等人[61]	● 受控测量 ● 基于HTTP的连通性检测	—	2020年6月	2020年6月, RPKI过滤影响到约17%的互联网用户
Rodday等人[63]	● 受控测量 ● traceroute	待测AS是否过滤受控AS的无效路由而接受其有效路由	2021年7月2–19日	测量覆盖了3694个AS. 发现206个AS部署了ROV, 其中184个AS是由于IXP的ROV保护. 146个AS过滤所有无效路由
Chen等人[65]	● 非受控测量 ● traceroute	待测AS部署ROV的概率分布, 用贝叶斯方法计算得到	2021年6月1–7日	测量覆盖了11074个AS, 发现3107个AS部署了ROV, 4716个AS未部署ROV, 357个AS部署ROV过滤部分无效路由, 剩余2894个AS无法判断
Hlavacek等人[66]	● 受控测量 ● 公开路由表采集、traceroute	待测AS是否是分歧点、所在AS路径的有效性	2020年6月8日, 2020年6月10日	测量覆盖了2325个AS, 其中约24%的AS部署ROV并严格过滤无效路由, 约43%的AS没有部署ROV
RoVista[67]	● 非受控测量 ● IP-ID测通道技术、基于TCP的连通性检测	vVP的IP-ID增长模式	2021年12月24日–2023年9月12日	测量覆盖了28314个AS, 其中10249个AS自身和上游未部署ROV; 3482个AS自身或者所有上游AS部署了ROV; 14583个AS的自身或者上游AS部分部署了ROV

4 RPKI 基础设施测量

如图 5 所示, RPKI 基础设施主要包括 CA、RPKI 资料库和 RP. CA 负责资源认证、签发 RPKI 数据对象. RPKI 资料库负责公开 CA 签发的 RPKI 数据. RP 用于同步、验证 RPKI 数据对象, 得到 VRP. 路由器使用 RTR 协议从 RP 同步 VRP 数据执行 ROV. 此外, RPKI 的运行还需要相应的域名服务器、解析器来连通 RP 和 RPKI 资料库.

对 RPK 基础设施的测量可以了解实际 RPKI 底层软硬件的部署情况, 有助于获取部署经验, 发现部署缺陷.

近年来的测量工作针对 RPKI 基础设施展开, 这些测量工作按照支撑的 RPKI 功能可分为两类: 1) 资源认证与数据发布; 2) 数据同步与验证.

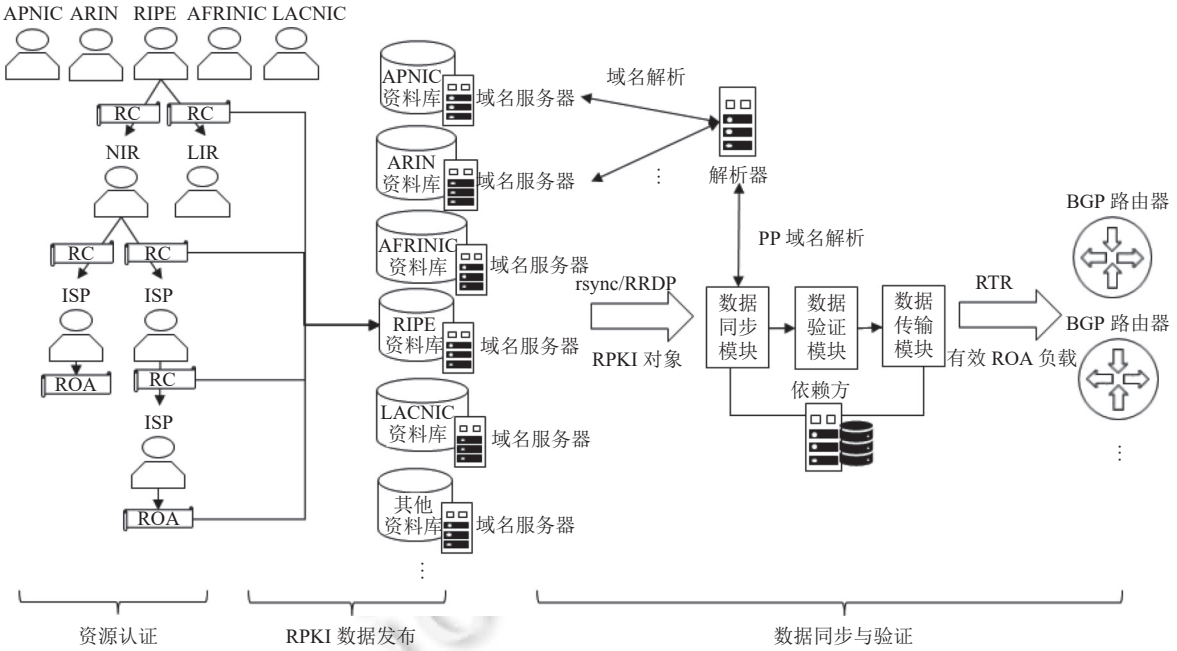


图 5 RPKI 系统基础设施

4.1 资源认证与数据发布

支撑资源认证与数据发布功能的 RPKI 基础设施主要是 CA 和 RPKI 资料库. CA 负责认证互联网码号资源并签署对应的 RC、ROA 等 RPKI 对象. 资料库负责存储、公开 CA 签发的 RPKI 对象. 现有的 RPKI CA 软件集成了 CA 和资料库的功能, 目前公开的 CA 软件有 Krill 和 rpki.net[69], 见表 7. 此外, 域名服务器负责存储 RPKI 资料库的域名记录. 本节的测量工作可分为 CA 操作延迟测量和资料库部署弹性测量两类.

表 7 RPKI CA 软件总结

名称	开发语言	开发团队	状态
Krill	Rust	NLnet Labs	仍在维护
rpki.net	Python	Dragon Research Labs	停止维护

● 操作延迟测量: Fontugne 等人[70]测量了 5 个 RIR 在进行 IPv4/IPv6 资源签署、发布以及撤销 ROA 等操作的延迟, 延迟中位数结果见表 8. 测量发现 APNIC 的 CA 每 20 min 对用户的创建、删除请求进行批量处理, 其他 4 个 RIR 在收到用户的创建或删除请求后立即执行, 因此 APNIC 签署和撤销 ROA 的操作相较于其他 RIR 有 10 min 的平均延迟. ARIN 和 LACNIC 设置的 ROA 签名时间晚于实际发布时间使得 ROA 在发布一段时间内无法通过有效性验证, 导致测量的 ROA 发布时间偏长, ARIN 之后修复了这个问题.

表 8 各 RIR 对 ROA 的操作时延 (IPv4/IPv6)[70] (min)

RIR	签署ROA	发布ROA	撤销ROA
AFRINIC	0/0	3/2	0/0
APNIC	10/13	4/3	10/12
LACNIC	0/0	54/32	0/0
RIPE NCC	0/0	4/4	0/0
ARIN	—/—	8/9	0/0

● 部署弹性测量: Su 等人[71]测量了资料库部署的弹性情况, 测量结果表明截至 2023 年 4 月 1 日, 资料库的数量从最初的 5 个增长到了 61 个, 但仅有 8 个资料库部署在 CDN 中以提供弹性服务; 58 个资料库的所有服务器均在单一 AS 中, 存在单点故障的风险; 仅有 14 个资料库发布了 ROA, 其余的资料库都面临着前缀劫持的威胁. 这表明现有资料库部署存在脆弱性.

4.2 数据同步与验证

支撑数据同步与验证功能的 RPKI 基础设施主要是 RP. RP 定期从各资料库同步验证 RPKI 数据, 获取有效 ROA 数据负载. RP 还需要域名解析器的支持来访问资料库. 本节的测量工作可分为 RP 软件评估、RP 同步行为测量和 RP 部署弹性测量 3 类.

目前实际部署中使用的主流 RP 软件包括 Routinator、rpki-client、OctoRPKI、Fort, 其他 RP 软件也有使用, 但占比较少[72]. 表 9 总结了现有的一些 RP 软件的信息及常用的标准. 在功能上, 各 RP 软件都支持 RPKI 数据同步和验证的基本功能, 部分 RP 软件例如 rpki-client、OctoRPKI 需要额外的工具支持 RTR 协议. 在文档丰富度上, Routinator, rpki-client, Fort 的文档较为丰富, 给出了下载安装方法、用法说明、支持功能等各方面的详细说明. Fort 的文档还提供了软件漏洞的信息, rpki-prover 的文档缺少了用法说明部分的内容, 其余 RP 软件的文档只给出了下载安装方法和生成有效 ROA 数据结果的方法, 缺少支持功能和详细的用法说明.

表 9 RP 软件总结

RP软件	开发语言	状态	功能支持					
			rsync	RRDP	RTR	BGPsec	SLURM	ASPA
Routinator	Rust	维护中	√	√	√	√	√	√
rpki-client	C	维护中	√	√	×	√	—	√
OctoRPKI	Go	维护中	√	√	×	—	√	—
Fort	C	维护中	√	√	√	√	√	—
RPSTIR2	Go	维护中	√	√	√	—	—	—
RIPE Validator	Java	停止维护	√	√	√	×	√	×
rpki.net	Python/C	停止维护	√	√	√	√	—	×
rpki-prover	Haskell	维护中	√	√	√	√	√	√

● 软件评估: Friedemann 等人[73]从安装易用性、性能、结果一致性、代码质量、应用性以及功能丰富性这 6 个维度对 7 款主流 RP 软件 RPKI Validator、RPSTIR2、OctoRPKI、Routinator、FORT-Validator、rpki-client 和 rpki-prover 进行了量化评分, 量化的结果见表 10. Routinator 在各方面表现都较为优秀, 推荐在实际部署中使用.

表 10 RPKI RP 软件评分[73]

RP软件	安装易用性 (满分55)	性能 (满分80)	结果一致性 (满分25)	代码质量 (满分15)	应用性 (满分30)	功能丰满度 (满分65)	总分 (满分270)
RPKI Validator	46	56	**25**	9	20	41	197
RPSTIR2	17	24	7	7	21	28	104
OctoRPKI	47	58	**25**	11	21	45	207
Routinator	**53**	69	21	**14**	**30**	**63**	**250**
FORT-Validator	51	55	**25**	10	23	57	221
rpki-client	37	63	23	13	19	26	181
rpki-prover	40	**72**	19	**14**	23	33	201

注: 最高分数用加粗显示

● RP 行为测量: Kristoff 等人[74]在 2019 年和 2020 年对互联网中 RP 从数据完整性、更新间隔、资料库同步协议等 3 个维度进行测量, 测量结果表明如下.

1) 在数据完整性上, 约 20% 的 RP 获得的 RPKI 数据不完整, 原因在于这些 RP 不访问 5 个 RIR 资料库下的子资料库.

2) 在更新间隔上, 约 20% 的 RP 设置的更新间隔较长, 每天更新低于 20 次, 这些 RP 获取的 RPKI 数据会落后于 RPKI 资料库的最新版本.

3) 在资料库同步协议方面, 约 95% 的 RP 同时支持 rsync 和 RRDP 协议访问资料库, 但约 90% 的 RP 在 RRDP 协议访问失败后无法切换至 rsync 协议访问. 当资料库 RRDP 服务失效时, 这些 RP 将无法获取 RPKI 更新.

Fontugne 等人[70]的测量估计 RP 将 VRP 发送给路由器的延迟不超过 2 min.

● 部署弹性测量: Mirdita 等人[72]测量了互联网中 RP 的安全漏洞情况, 发现 56% 的 RP 都存在至少一个安全漏洞, 易受到拒绝服务 (denial of service, DoS)、RPKI 缓存中毒[75]、RPKI 降级[76]等攻击, 其原因在于实际部署中使用的 RP 软件存在如下问题: 1) 未修补漏洞; 2) 版本过旧; 3) 已停止维护.

Hlavacek 等人[77]在 2022 年 4 月和 9 月对 RP 的域名解析器弹性情况进行了测量, 发现部分域名解析器存在以下问题.

1) 存在单点故障: 部署多个 RP 的 AS 中有 42.8% 仅使用一个递归解析器解析 RPKI 发布点, 82.9% 的 RP 使用的递归解析器位于单一 AS 中, 对单一解析器或者单一 AS 的攻击会导致一个 AS 所有的 RP 失效, 详细结果见表 11.

表 11 域名解析器的 AS 分布情况[77]

解析器位置	使用单一RP的AS (%)	使用多个RP的AS (%)	RP数量 (个)
解析器位于单一AS	46.15	18.85	2 163
解析器位于多个AS	16.80	18.20	447

(2) 未部署 DNSSEC: 38% 的 AS 使用的 DNS 解析器不验证 DNSSEC, 24% 的 AS 使用了无法接收 DNSSEC 签名回复的解析器, 易受到 DNS 缓存中毒攻击.

(3) 未部署 RPKI: 24% 的 RP 解析器、10 个根域名服务器和 50 个发布点的域名没有受到 RPKI 保护, 容易成为路由前缀劫持的攻击目标. 综上, 解析器是数据同步中较为脆弱的一环.

4.3 总 结

表 12 对 RPKI 基础设施测量工作进行总结. 在资源认证与数据发布组件的测量方面, 文献 [70] 发现 ARIN 和 LACNIC 的 CA 在证书有效时间设置上存在问题, 导致证书在颁发一段时间内无效, 证书拥有者的前缀无法及时受到保护. 文献 [71] 发现部分资料库部署存在单点故障、前缀劫持等安全风险, 对单一 AS 的前缀劫持等攻击会导致资料库无法被访问, RP 无法同步资料库的更新数据. 在数据同步与验证的组件的测量方面, 文献 [74] 发现 RP 存在同步数据不完整、更新间隔设置过长、访问协议设置缺少健壮性的问题, 可能导致 RP 同步数据不完全, 同步数据陈旧或者无法访问资料库. 文献 [72] 发现 AS 部署时使用停止更新或者版本陈旧的 RP 软件, 这些 RP 存在安全漏洞, 易受到 DoS、RPKI 降级等攻击导致无法同步 RPKI 数据. 在解析器的测量方面, 文献 [78] 发现 RP 使用的递归解析器存在单点故障、未部署 DNSSEC 和 RPKI 的问题, 导致 DNS 解析成为防御脆弱的环节.

表 12 RPKI 基础设施测量总结

支撑功能	测量对象	文献	测量时间	测量工作
资源认证与数据发布	CA	[70]	2021年11月1日–2022年10月6日	ROA签署、发布延迟
	资料库	[71]	2023年4月1日	部署弹性
	域名服务器	[77]	2021年4月、9月	受RPKI保护情况
数据同步与验证	RP	[73]	—	软件评估
		[74]	2019年3月–2020年4月, 2020年5月6–17日	数据完整性、更新间隔、同步协议
		[72]	2023年12月	安全漏洞
		[70]	2021年11月1日–2022年10月6日	VRP传输延迟
	域名解析器	[77]	2021年4月、9月	部署弹性和健壮性

5 RPKI 部署挑战与建议

5.1 RPKI 部署中的挑战

如前所述, 虽然 RPKI 经过 10 余年的发展, 其部署率较初期有了大幅度的增长, 但是互联网中仍有将近一半的路由没有被 RPKI 覆盖. 近年来对 RPKI 的测量表明仍有诸多因素阻碍着 RPKI 部署的发展.

(1) 数据质量问题: 由于 RPKI 并不遵循“do no harm”的基本原则[78], 低质量的 RPKI 数据会阻碍网络的正常运行: 错误的 ROA 配置会降低网络的连通性; Loose ROA 让网络更容易受到攻击. 虽然近年来的测量表明, 从部署初期开始, RPKI 标准不断成熟, 数据质量在不断改善[42], 但人工失误难以避免, RPKI 数据质量问题难以根治.

(2) 缺乏部署激励[78,79]: 当部署率较低时, RPKI 增量部署带来的边际效益低. 当多数 AS 都部署了 ROV 时, AS 签发 ROA 才有较高的收益; 同样地, 当多数 AS 都签发了 ROA 时, AS 部署 ROV 才有较高的收益. 目前的测量表明超过 50% 的路由前缀被 ROA 覆盖, 而仅约 27% 的 AS 部署了 ROV[66], ROA 和 ROV 的部署还不够完善, 导致大多部署者, 尤其是小型运营商因收益不足呈观望态度, 阻碍了 RPKI 部署的发展.

(3) 部署依赖[7]: RPKI 的部署依赖在 ROA 和 ROV 上都有体现: 1) ROA 部署上: 资源层级认证的结构使得 ROA 部署需要从上而下完成, 当上级网络完成资源认证, 具备签发资源证书能力之后, 下级网络才能部署, 因此 RPKI 的部署严重依赖于互联网核心网络. 2) ROV 部署上: 若上游 AS 未部署 ROV, 部署 ROV 的 AS 发送的数据包可能被上游 AS 转发到错误的目的地, 导致 ROV 无法发挥作用, 阻碍 ROV 部署的发展. 文献 [63] 对 ROV 的测量中也发现这一问题.

(4) RPKI 服务的脆弱性: 对 RPKI 组件的测量反映出目前已有的 RPKI 部署缺乏安全考虑, 具体表现为: 1) 存在单点故障: RPKI 部署者仅使用单一服务器或者多个位于同一 AS 的服务器提供资料库或依赖方服务. 2) 存在安全漏洞: 使用存在安全漏洞的依赖方软件. 3) 缺乏安全措施: 未部署 DNSSEC 和 RPKI, 容易受到 DNS 缓存中毒、前缀劫持等攻击. 这意味着部分 RPKI 设施无法提供可靠的服务, 降低了 RPKI 的可信度.

此外, RPKI 的中心化风险[69,80]和法律层面的顾虑[81]也使得网络运营商降低了部署 RPKI 的兴趣.

5.2 RPKI 部署的建议

针对上述 RPKI 部署挑战, 本文认为 RPKI 部署的推广可从以下几个角度考虑.

(1) 提高 RPKI 数据质量和可信度: 一方面, 学术界和工业界需要不断完善 RPKI 的相关标准, 明确操作规范. 网络运营商遵循标准部署、使用 RPKI. 另一方面, RPKI 低质量数据多来源于人为失误或缺乏专业知识, 可考虑开发 RPKI 自动化工具进行自动化配置, 降低人为操作失误风险, 提高 RPKI 体系整体的可信度和声誉.

(2) 加强部署激励[7]: 以 5 大 RIR 推动, 大型网络运营商带头部署 RPKI, 签发 ROA 并使用 ROV 过滤无效路由, 增加 ROA 和 ROV 的部署收益, 激励其他网络部署 RPKI. 同时, 核心网络的部署也能使因上层部署依赖而无法部署 RPKI 的网络完成部署.

(3) 简化 RPKI 部署: RPKI 是一个较为复杂的体系, 无论是部署还是后期的运维, 都需要较高的密码学知识和路由知识, 一些网络不具备这些专业知识, 导致其难以部署 RPKI. 因此, 可以从技术层面上降低 RPKI 部署、管理的复杂度, 使其易于运行、维护、配置, 降低部署和运维压力.

(4) 加强组件部署安全性: 目前的测量工作表明无论是 CA 侧还是 RP 侧, 在部署中都缺乏安全性考虑, 提供的 RPKI 服务缺乏可靠性. 因此在实际部署中要加强组件的安全性: 1) 增强弹性部署, 在多 AS 部署多 PP 或 RP 服务器, 消除单点故障. 2) 为 PP 和 RP 服务器及相应的权威服务器和解析器签发 ROA, 并部署 DNSSEC, 缓解缓存中毒、前缀劫持的影响. 3) 采用最新版本 RP 或 CA 软件并及时更新, 缓解软件安全漏洞对 RPKI 数据同步或发布的影响.

目前还有一些研究利用区块链扁平结构代替现有 RPKI 层级结构来改善 RPKI 的中心化层级架构, 以求从根本上解决中心化风险, 同时使用区块链收益作为部署激励推动 RPKI 部署发展[82−93].

6 总 结

近年来对 RPKI 的测量工作显示 RPKI 的规模在逐渐增加, 无论是 ROA 部署规模还是 ROV 部署规模, RPKI

的数据质量虽然在不断改善[42], 但总体进展较为缓慢. 已有的 RPKI 部署中也存在一些问题: RPKI 组件部署集中、安全性较差, 一些关键组件例如资料库服务器和依赖方服务器, 或集中在单一 AS, 或依赖单一其他组件, 存在单点故障隐患; 此外, RPKI 组件本身未部署 DNSSEC 和 RPKI, 难以提供可靠服务. 虽然 RPKI 存在一些问题, 但 RPKI 无疑是目前解决路由劫持的最佳方案, 显著增强了域间路由安全[72,94].

在可预见的未来, RPKI 将会在技术完善和部署安全上做出努力, 其应用范围也会不断扩大, RPKI 测量研究仍会是网络测量领域的一个重要方向. 未来的 RPKI 测量工作可从以下两个方面展开.

● RPKI 应用的测量: RPKI 的应用场景不断增加, 例如, RPKI 签名清单 (RPKI signed checklist, RSC)[95]使得资源拥有者可以使用互联网码号资源签名任意数字对象; 映射源授权 (mapping origin authorization, MOA)[96]用于验证 IPv6 单栈网络中地址映射规则的安全性, 保证 IPv6 单栈网络中 IPv4 业务的正常运行. 未来对于新的 RPKI 应用的测量值得研究.

● RPKI 异常识别: 人工失误、上级 CA 的单边操作等会导致 CA、ROA 的数据异常, 影响路由的起源验证结果, 且难以与正常数据区分. 未来可结合机器学习技术, 实现 RPKI 异常的快速、准确的识别.

References

[1] Lepinski M, Kent S. RFC 6480: An infrastructure to support secure Internet routing. 2012. https://www.rfc-editor.org/rfc/pdfrfc/rfc6480.txt.pdf [doi: 10.17487/RFC6480]

[2] Cooper D, Santesson S, Farrell S, Boeyen S, Housley R, Polk W. RFC 5280: Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile. 2008. https://www.rfc-editor.org/rfc/pdfrfc/rfc5280.txt.pdf [doi: 10.17487/RFC5280]

[3] Huston G, Michaelson G, Loomans R. RFC 6487: A profile for X.509 PKIX resource certificates. 2012. https://www.rfc-editor.org/rfc/pdfrfc/rfc6487.txt.pdf [doi: 10.17487/RFC6487]

[4] Lepinski M, Kent S, Kong D. RFC 6482: A profile for route origin authorizations (ROAs). 2012. https://www.rfc-editor.org/rfc/pdfrfc/rfc6482.txt.pdf [doi: 10.17487/RFC6482]

[5] Huston G, Michaelson G. RFC 6483: Validation of route origination using the resource certificate public key infrastructure (PKI) and route origin authorizations (ROAs). 2012. https://www.rfc-editor.org/rfc/rfc6483 [doi: 10.17487/RFC6483]

[6] Su YY, Li D, Ye HL. Resource public key infrastructure RPKI: Status and problems. Telecommunications Science, 2021, 37(3): 75–89 (in Chinese with English abstract). [doi: 10.11959/j.issn.1000-0801.2021050]

[7] Zou H, Ma D, Shao Q, Mao W. A survey of the resource public key infrastructure. Chinese Journal of Computers, 2022, 45(5): 1100–1132 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2022.01100]

[8] Rodday N, Cunha Í, Bush R, Katz-Bassett E, Rodosek GD, Schmidt TC, Wählisch M. The resource public key infrastructure (RPKI): A survey on measurements and future prospects. IEEE Trans. on Network and Service Management, 2024, 21(2): 2353–2373. [doi: 10.1109/TNSM.2023.3327455]

[9] Rekhter Y, Li T, Hares S. RFC 4271: A border gateway protocol 4 (BGP-4). 2006. https://www.rfc-editor.org/rfc/pdfrfc/rfc4271.txt.pdf [doi: 10.17487/RFC4271]

[10] Butler K, Farley TR, McDaniel P, Rexford J. A survey of BGP security issues and solutions. Proc. of the IEEE, 2010, 98(1): 100–122. [doi: 10.1109/JPROC.2009.2034031]

[11] Al-Musawi B, Branch P, Armitage G. BGP anomaly detection techniques: A survey. IEEE Communications Surveys & Tutorials, 2017, 19(1): 377–396. [doi: 10.1109/COMST.2016.2622240]

[12] Heilman E, Cooper D, Reyzin L, Goldberg S. From the consent of the routed: Improving the transparency of the RPKI. ACM SIGCOMM Computer Communication Review, 2014, 44(4): 51–62. [doi: 10.1145/2740070.2626293]

[13] Hiran R, Carlsson N, Gill P. Characterizing large-scale routing anomalies: A case study of the China Telecom incident. In: Proc. of the 14th Int'l Conf. on Passive and Active Measurement. Hong Kong: Springer, 2013. 229–238. [doi: 10.1007/978-3-642-36516-4_23]

[14] Siddiqui A. KlaySwap-another BGP hijack targeting crypto wallets. 2022. https://manrs.org/2022/02/klayswap-another-bgp-hijack-targeting-crypto-wallets/

[15] Bryton H, Mingwei Z, Tanner R. Cloudflare 1.1.1.1 incident on June 27, 2024—The Cloudflare blog. 2024. https://www.resource.dnsafrica.org/2025/01/14/cloudflare-1-1-1-1-incident-on-june-27-2024-the-cloudflare-blog/

[16] Lad M, Massey D, Pei D, Wu YG, Zhang BC, Zhang LX. PHAS: A prefix hijack alert system. In: Proc. of the 15th Conf. on USENIX Security Symp. Vancouver: USENIX Association, 2006. 11.

[17] Shi XG, Xiang Y, Wang ZL, Yin X, Wu JP. Detecting prefix hijackings in the Internet with argus. In: Proc. of the 2012 Internet Measurement Conf. Boston: ACM, 2012. 15–28. [doi: 10.1145/2398776.2398779]

[18] Sermpezis P, Kotronis V, Gigis P, Dimitropoulos X, Cicalese D, King A, Dainotti A. ARTEMIS: Neutralizing BGP hijacking within a minute. IEEE/ACM Trans. on Networking, 2018, 26(6): 2471–2486. [doi: 10.1109/TNET.2018.2869798]

[19] Schlamp J, Holz R, Jacquemart Q, Carle G, Biersack EW. HEAP: Reliable assessment of BGP hijacking attacks. IEEE Journal on Selected Areas in Communications, 2016, 34(6): 1849–1861. [doi: 10.1109/JSAC.2016.2558978]

[20] Kent S, Lynn C, Seo K. Secure border gateway protocol (S-BGP). IEEE Journal on Selected Areas in Communications, 2000, 18(4): 582–592. [doi: 10.1109/49.839934]

[21] White R. Securing BGP through secure origin BGP (soBGP). Business Communications Review, 2003, 33(5): 47–53.

[22] Lepinski M, Sriram K. RFC 8205: BGPsec protocol specification. 2017. https://www.rfc-editor.org/rfc/pdfrfc/rfc8205.txt.pdf [doi: 10.17487/RFC8205]

[23] Li S, Zhuge JW, Li X. Study on BGP security. Ruan Jian Xue Bao/Journal of Software, 2013, 24(1): 121–138 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4346.htm [doi: 10.3724/SP.J.1001.2013.04346]

[24] Wang Q, Li FJ, Ni XL, Xia LL, Ma Z. Research on blockchain-based inter-domain routing security enhancement. Journal of Frontiers of Computer Science and Technology, 2024, 18(12): 3144–3174 (in Chinese with English abstract). [doi: 10.3778/j.issn.1673-9418.2407065]

[25] Ma D. Scaling RPKI relying party system. ZTE Technology Journal, 2023, 29(1): 40–44 (in Chinese with English abstract). [doi: 10.12142/ZTETJ.202301008]

[26] Huston G, Loomans R, Michaelson G. RFC 6481: A profile for resource certificate repository structure. 2012. https://www.rfc-editor.org/rfc/pdfrfc/rfc6481.txt.pdf [doi: 10.17487/RFC6481]

[27] Kent S, Kong D, Seo K, Watro R. RFC 6484: Certificate policy (CP) for the resource public key infrastructure (RPKI). 2012. https://www.rfc-editor.org/rfc/pdfrfc/rfc6484.txt.pdf [doi: 10.17487/RFC6484]

[28] Huston G. RFC 6485: The profile for algorithms and key sizes for use in the resource public key infrastructure (RPKI). 2012. https://www.rfc-editor.org/rfc/pdfrfc/rfc6485.txt.pdf [doi: 10.17487/RFC6485]

[29] Austein R, Huston G, Kent S, Lepinski M. RFC 6486: Manifests for the resource public key infrastructure (RPKI). 2012. https://www.rfc-editor.org/rfc/pdfrfc/rfc6486.txt.pdf [doi: 10.17487/RFC6486]

[30] Lepinski M, Chi A, Kent S. RFC 6488: Signed object template for the resource public key infrastructure (RPKI). 2012. https://www.rfc-editor.org/rfc/pdfrfc/rfc6488.txt.pdf [doi: 10.17487/RFC6488]

[31] Huston G, Michaelson G, Kent S. RFC 6489: Certification authority (CA) key rollover in the resource public key infrastructure (RPKI). 2012. https://www.rfc-editor.org/rfc/pdfrfc/rfc6489.txt.pdf [doi: 10.17487/RFC6489]

[32] Huston G, Weiler S, Michaelson G, Kent S. RFC 6490: Resource public key infrastructure (RPKI) trust anchor locator. 2012. https://www.rfc-editor.org/rfc/pdfrfc/rfc6490.txt.pdf [doi: 10.17487/RFC6490]

[33] Manderson T, Vegoda L, Kent S. RFC 6491: Resource public key infrastructure (RPKI) objects issued by IANA. 2012. https://www.rfc-editor.org/rfc/pdfrfc/rfc6491.txt.pdf [doi: 10.17487/RFC6491]

[34] Huston G, Loomans R, Ellacott B, Austein R. RFC 6492: A protocol for provisioning resource certificates. 2012. https://www.rfc-editor.org/rfc/pdfrfc/rfc6492.txt.pdf [doi: 10.17487/RFC6492]

[35] Bush R. RFC 6493: The resource public key infrastructure (RPKI) ghostbusters record. 2012. https://www.rfc-editor.org/rfc/pdfrfc/rfc6493.txt.pdf [doi: 10.17487/RFC6493]

[36] Bruijnzeels T, Muravskiy O, Weber B, Austein R. RFC 8182: The RPKI repository delta protocol (RRDP). 2017. https://www.rfc-editor.org/rfc/pdfrfc/rfc8182.txt.pdf [doi: 10.17487/RFC8182]

[37] Bush R, Austein R. RFC 8210: The resource public key infrastructure (RPKI) to router protocol, Version 1. 2017. https://www.rfc-editor.org/rfc/pdfrfc/rfc8210.txt.pdf [doi: 10.17487/RFC8210]

[38] Ma D, Mandelberg D, Bruijnzeels T. RFC 8416: Simplified local Internet number resource management with the RPKI (SLURM). 2018. https://www.rfc-editor.org/rfc/pdfrfc/rfc8416.txt.pdf [doi: 10.17487/RFC8416]

[39] Wählisch M, Maennel O, Schmidt TC. Towards detecting BGP route hijacking using the RPKI. ACM SIGCOMM Computer Communication Review, 2012, 42(4): 103–104. [doi: 10.1145/2377677.2377702]

[40] Iamartino D, Pelsser C, Bush R. Measuring BGP route origin registration and validation. In: Proc. of the 16th Int'l Conf. on Passive and Active Measurement. New York: Springer, 2015. 28–40. [doi: 10.1007/978-3-319-15509-8_3]

[41] Wählisch M, Schmidt R, Schmidt TC, Maennel O, Uhlig S, Tyson G. RiPKI: The tragic story of RPKI deployment in the Web ecosystem. In: Proc. of the 14th ACM Workshop on Hot Topics in Networks. Philadelphia: ACM, 2015. 11. [doi: 10.1145/2834050.2834102]

[42] Chung T, Aben E, Bruijnzeels T, Chandrasekaran B, Choffnes D, Levin D, Maggs BM, Mislove A, van Rijswijk-Deij R, Rula J, Sullivan N.

RPKI is coming of age: A longitudinal study of RPKI deployment and invalid route origins. In: Proc. of the 2019 Internet Measurement Conf. Amsterdam: ACM, 2019. 406–419. [doi: 10.1145/3355369.3355596]

[43] Hlavacek T, Jeitner P, Mirdita D, Shulman H, Waidner M. Beyond limits: How to disable validators in secure networks. In: Proc. of the 2023 ACM SIGCOMM Conf. New York: ACM, 2023. 950–966. [doi: 10.1145/3603269.3604861]

[44] NIST. NIST RPKI deployment monitor. 2021. https://www.nist.gov/services-resources/software/nist-rpki-deployment-monitor

[45] Schulmann H, Vogel N, Waidner M. RPKI: Not perfect but good enough. arXiv:2409.14518, 2024.

[46] Gilad Y, Sagga O, Goldberg S. MaxLength considered harmful to the RPKI. In: Proc. of the 13th Int'l Conf. on Emerging Networking Experiments and Technologies. Incheon: ACM, 2017. 101–107. [doi: 10.1145/3143361.3143363]

[47] Xu WJ, Chang DL, Li X. On the classification and false alarm of invalid prefixes in RPKI based BGP route origin validation. In: Proc. of the 2019 IFIP/IEEE Symp. on Integrated Network and Service Management (IM). Arlington: IEEE, 2019. 654–658.

[48] Hlavacek T, Shulman H, Waidner M. Not all conflicts are created equal: Automated error resolution in RPKI deployments. In: Proc. of the 2021 IEEE INFOCOM Conf. on Computer Communications Workshops. Vancouver: IEEE, 2021. 1–2. [doi: 10.1109/INFOCOMWKSHPS51825.2021.9484607]

[49] Hlavacek T, Shulman H, Waidner M. Smart RPKI validation: Avoiding errors and preventing hijacks. In: Proc. of the 27th European Symp. on Research in Computer Security. Copenhagen: Springer, 2022. 509–530. [doi: 10.1007/978-3-031-17140-6_25]

[50] Gilad Y, Cohen A, Herzberg A, Schapira M, Shulman H. Are we there yet? On RPKI's deployment and security. In: Proc. of the 2017 Network and Distributed System Security Symp. San Diego: Internet Society, 2017. 1–15.

[51] Bush R. RFC 7115: Origin validation operation based on the resource public key infrastructure (RPKI). 2014. https://www.rfc-editor.org/rfc/pdfrfc/rfc7115.txt.pdf [doi: 10.17487/RFC7115]

[52] Gilad Y, Goldberg S, Sriram K, Snijders J, Maddison B. RFC 9319: The use of maxLength in the resource public key infrastructure (RPKI). 2018. https://www.rfc-editor.org/rfc/pdfrfc/rfc9319.txt.pdf [doi: 10.17487/RFC9319]

[53] Zou H, Ma D, Shao Q, Mao W. The horizontal INR conflict-detection algorithm: Revealing INR reallocation and reauthorization in RPKI. In: Proc. of the 2021 IFIP/IEEE Int'l Symp. on Integrated Network Management. Bordeaux: IEEE, 2021. 459–465.

[54] Reuter A, Bush R, Cunha I, Katz-Bassett E, Schmidt TC, Wählisch M. Towards a rigorous methodology for measuring adoption of RPKI route validation and filtering. ACM SIGCOMM Computer Communication Review, 2018, 48(1): 19–27. [doi: 10.1145/3211852.3211856]

[55] Hlavacek T, Herzberg A, Shulman H, Waidner M. Practical experience: Methodologies for measuring route origin validation. In: Proc. of the 48th Annual IEEE/IFIP Int'l Conf. on Dependable Systems and Networks. Luxembourg: IEEE, 2018. 634–641. [doi: 10.1109/DSN.2018.00070]

[56] Are BGPs security features working yet? 2018. https://blog.benjojo.co.uk/post/are-bgps-security-features-working-yet-rpki

[57] The year of RPKI on the control plane. 2019. https://blog.benjojo.co.uk/post/the-year-of-rpki-on-the-control-plane

[58] Trenaman N, Aben E, den Hertog J, Snijders J. RPKI test. 2019. https://labs.ripe.net/author/nathalie_nathalie/rpki-test/

[59] Cloudflare Inc. Is BGP safe yet? 2022. https://isbgpsafeyet.com/

[60] Testart C, Richter P, King A, Dainotti A, Clark D. To filter or not to filter: Measuring the benefits of registering in the RPKI today. In: Proc. of the 21st Int'l Conf. on Passive and Active Measurement. Eugene: Springer, 2020. 71–87. [doi: 10.1007/978-3-030-44081-7_5]

[61] Huston G, Damas J. Measuring route origin validation. 2020. https://www.potaroo.net/ispcol/2020-06/rov.html

[62] Gutiérrez PAA. A simplified Internet routing architecture: Removing traffic engineering and security artifacts from the Internet's default free zone. Mobile Networks and Applications, 2011, 16(4): 433–445. [doi: 10.1007/s11036-011-0320-8]

[63] Rodday N, Cunha ÍS, Bush R, Katz-Bassett E, Rodosek GD, Schmidt TC, Wählisch M. Revisiting RPKI route origin validation on the data plane. In: Proc. of 5th Network Traffic Measurement and Analysis Conf. IFIP, 2021.

[64] Gray C, Mosig C, Bush R, Pelsser C, Roughan M, Schmidt TC, Wahlisch M. BGP beacons, network tomography, and Bayesian computation to locate route flap damping. In: Proc. of the 2020 ACM Internet Measurement Conf. ACM, 2020. 492–505. [doi: 10.1145/3419394.3423624]

[65] Chen WQ, Wang ZL, Han DQ, Duan CX, Yin X, Yang JH, Shi XG. ROV-MI: Large-scale, accurate and efficient measurement of ROV deployment. In: Proc. of the 2022 Network and Distributed Systems Security (NDSS) Symp. San Diego: 2022. [doi: 10.14722/ndss.2022.23214]

[66] Hlavacek T, Shulman H, Vogel N, Waidner M. Keep your friends close, but your routeservers closer: Insights into RPKI validation in the Internet. In: Proc. of the 32nd USENIX Conf. on Security Symp. Anaheim: USENIX Association, 2023. 4841–4858.

[67] Li WT, Lin ZX, Ashiq MI, Aben E, Fontugne R, Phokeer A, Chung T. RoVista: Measuring and analyzing the route origin validation (ROV) in RPKI. In: Proc. of the 2023 ACM on Internet Measurement Conf. Montreal: ACM, 2023. 73–88. [doi: 10.1145/3618257.

3624806]

[68] Rodday N, van Baaren R, Hendriks L, van Rijswijk-Deij R, Pras A, Dreo G. Evaluating RPKI ROV identification methodologies in automatically generated Mininet topologies. In: Proc. of the 16th Int'l Conf. on Emerging Networking Experiments and Technologies. Barcelona: ACM, 2020. 530–531. [doi: 10.1145/3386367.3431669]

[69] Qin CY, Zhang Y, Fang BX. Survey on decentralized security-enhanced technologies for RPKI. Journal on Communications, 2024, 45(7): 196–205 (in Chinese with English abstract). [doi: 10.11959/j.issn.1000-436x.2024102]

[70] Fontugne R, Phokeer A, Pelsser C, Vermeulen K, Bush R. RPKI time-of-flight: Tracking delays in the management, control, and data planes. In: Proc. of the 24th Int'l Conf. on Passive and Active Measurement. Springer, 2023. 429–457. [doi: 10.1007/978-3-031-28486-1_18]

[71] Su YY, Li D, Chen L, Li Q, Ling ST. dRR: A decentralized, scalable, and auditable architecture for RPKI repository. In: Proc. of the 31st Annual Network and Distributed System Security Symp. San Diego: Internet Society, 2024. [doi: 10.14722/ndss.2024.24368]

[72] Mirdita D, Schulmann H, Waidner M. SoK: An introspective analysis of RPKI security. arXiv:2408.12359, 2024.

[73] Friedemann PH, Rodday N, Rodosek GD. Assessing the RPKI validator ecosystem. In: Proc. of the 13th Int'l Conf. on Ubiquitous and Future Networks. Barcelona: IEEE, 2022. 295–300. [doi: 10.1109/ICUFN55119.2022.9829712]

[74] Kristoff J, Bush R, Kanich C, Michaelson G, Phokeer A, Schmidt TC, Wählisch M. On measuring RPKI relying parties. In: Proc. of the 2020 ACM Internet Measurement Conf. ACM, 2020. 484–491. [doi: 10.1145/3419394.3423622]

[75] Mirdita D, Schulmann H, Vogel N, Waidner M. The CURE to vulnerabilities in RPKI validation. In: Proc. of the 31st Annual Network and Distributed System Security Symp. San Diego: Internet Society, 2024. [doi: 10.14722/ndss.2024.241093]

[76] Hlavacek T, Jeitner P, Mirdita D, Shulman H, Waidner M. Stalloris: RPKI downgrade attack. In: Proc. of the 31st USENIX Security Symp. 2022. 4455–4471.

[77] Hlavacek T, Jeitner P, Mirdita D, Shulman H, Waidner M. Behind the scenes of RPKI. In: Proc. of the 2022 ACM SIGSAC Conf. on Computer and Communications Security. Los Angeles: ACM, 2022. 1413–1426. [doi: 10.1145/3548606.3560645]

[78] Hlavacek T, Cunha I, Gilad Y, Herzberg A, Katz-Bassett E, Schapira M, Shulman H. DISCO: Sidestepping RPKI's deployment barriers. In: Proc. of the 2020 Network and Distributed Systems Security Symp. San Diego: Internet Society, 2020. 1–17. [doi: 10.14722/ndss.2020.2435]

[79] Gilad Y, Hlavacek T, Herzberg A, Schapira M, Shulman H. Perfect is the enemy of good: Setting realistic goals for BGP security. In: Proc. of the 17th ACM Workshop on Hot Topics in Networks. Redmond: ACM, 2018. 57–63. [doi: 10.1145/3286062.3286071]

[80] Cooper D, Heilman E, Brogle K, Reyzin L, Goldberg S. On the risk of misbehaving RPKI authorities. In: Proc. of the 12th ACM Workshop on Hot Topics in Networks. College Park: ACM, 2013. 16. [doi: 10.1145/2535771.2535787]

[81] Yoo CS, Wishnick DA. Lowering legal barriers to RPKI adoption. 2019. https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3308619#

[82] Hari A, Lakshman TV. The Internet blockchain: A distributed, tamper-resistant transaction framework for the Internet. In: Proc. of the 15th ACM Workshop on Hot Topics in Networks. Atlanta: ACM, 2016. 204–210. [doi: 10.1145/3005745.3005771]

[83] Xing QQ, Wang BS, Wang XF. BGPcoin: Blockchain-based Internet number resource authority and BGP security solution. Symmetry, 2018, 10(9): 408. [doi: 10.3390/sym10090408]

[84] Paillisse J, Manrique J, Bonet G, Rodriguez-Natal A, Maino F, Cabellos A. Decentralized trust in the inter-domain routing infrastructure. IEEE Access, 2019, 7: 166896–166905. [doi: 10.1109/ACCESS.2019.2954096]

[85] Liu S, Yang F, Li DD, Bagnulo M, Liu BY, Huang XH. The trusted and decentralized network resource management. In: Proc. of the 29th Int'l Conf. on Computer Communications and Networks. Honolulu: IEEE, 2020. 1–7. [doi: 10.1109/ICCCN49398.2020.9209590]

[86] Angieri S, García-martínez A, Liu BY, Yan ZW, Wang C, Bagnulo M. A distributed autonomous organization for Internet address management. IEEE Trans. on Engineering Management, 2020, 67(4): 1459–1475. [doi: 10.1109/TEM.2019.2924737]

[87] Angieri S, Bagnulo M, García-martínez A, Liu BY, Wei XP. InBlock4: Blockchain-based route origin validation. In: Proc. of the 2020 IEEE INFOCOM Conf. on Computer Communications Workshops. Toronto: IEEE, 2020. 291–296. [doi: 10.1109/INFOCOMWKSHPS50562.2020.9162879]

[88] García-martínez A, Angieri S, Liu BY, Yang F, Bagnulo M. Design and implementation of InBlock—A distributed IP address registration system. IEEE Systems Journal, 2021, 15(3): 3528–3539. [doi: 10.1109/JSYST.2020.3003526]

[89] Lu HM, Tang Y, Sun Y. DRRS-BC: Decentralized routing registration system based on blockchain. IEEE/CAA Journal of Automatica Sinica, 2021, 8(12): 1868–1876. [doi: 10.1109/JAS.2021.1004204]

[90] He GB, Su W, Gao S, Yue JR, Das SK. ROAchain: Securing route origin authorization with blockchain for inter-domain routing. IEEE Trans. on Network and Service Management, 2021, 18(2): 1690–1705. [doi: 10.1109/TNSM.2020.3015557]

[91] Saad M, Anwar A, Ahmad A, Alasmary H, Yuksel M, Mohaisen D. RouteChain: Towards blockchain-based secure and efficient BGP routing. Computer Networks, 2022, 217: 109362. [doi: 10.1016/J.COMNET.2022.109362]

[92] Podili P, Cherupally SR, Boga S, KataoKa K. Inter-domain prefix and route validation using fast and scalable DAG based distributed ledger for secure BGP routing. Journal of Network and Systems Management, 2022, 30(4): 55. [doi: 10.1007/s10922-022-09668-2]

[93] Li J, X MW, Cao JH, Meng ZL, Zhang GQ. Decentralized Internet number resource management system based on blockchain technology. Journal of Tsinghua University (Science and Technology), 2023, 63(9): 1366–1379 (in Chinese with English abstract). [doi: 10.16511/j.cnki.qhdxxb.2023.21.016]

[94] Madory D. RPKI ROV deployment reaches major milestone. 2024. https://blog.apnic.net/2024/05/08/rpki-rov-deployment-reaches-major-milestone/

[95] Snijders J, Harrison T, Maddison B. RFC 9323: A profile for RPKI signed checklists (RSCs). 2022. https://www.rfc-editor.org/rfc/pdfrfc/rfc9323.txt.pdf [doi: 10.17487/RFC9323]

[96] Xie CF, Dong GZ, Li X, Huston G, Ma D. A profile for mapping origin authorizations (MOAs). 2024. https://www.ietf.org/archive/id/draft-xie-sidrops-moa-profile-00.html

附中文参考文献

[6] 苏莹莹, 李丹, 叶洪琳. 资源公钥基础设施 RPKI: 现状与问题. 电信科学, 2021, 37(3): 75–89. [doi: 10.11959/j.issn.1000-0801.2021050]

[7] 邹慧, 马迪, 邵晴, 毛伟. 互联网码号资源公钥基础设施 (RPKI) 研究综述. 计算机学报, 2022, 45(5): 1100–1132. [doi: 10.11897/SP.J.1016.2022.01100]

[23] 黎松, 诸葛建伟, 李星. BGP 安全研究. 软件学报, 2013, 24(1): 121–138. http://www.jos.org.cn/1000-9825/4346.htm [doi: 10.3724/SP.J.1001.2013.04346]

[24] 王群, 李馥娟, 倪雪莉, 夏玲玲, 马卓. 域间路由安全增强及区块链技术的应用研究. 计算机科学与探索, 2024, 18(12): 3144–3174. [doi: 10.3778/j.issn.1673-9418.2407065]

[25] 马迪. 构建可扩展的 RPKI 依赖方系统部署机制. 中兴通讯技术, 2023, 29(1): 40–44. [doi: 10.12142/ZTETJ.202301008]

[69] 秦超逸, 张宇, 方滨兴. RPKI 去中心化安全增强技术综述. 通信学报, 2024, 45(7): 196–205. [doi: 10.11959/j.issn.1000-436x.2024102]

[93] 李江, 徐明伟, 曹家浩, 孟子立, 张国强. 基于区块链技术的去中心化互联网号码资源管理系统. 清华大学学报 (自然科学版), 2023, 63(9): 1366–1379. [doi: 10.16511/j.cnki.qhdxxb.2023.21.016]

作者简介

张泽源, 博士生, 主要研究领域为网络空间安全.

刘翔, 博士, 助理研究员, 主要研究领域为密码学, 互联网基础设施, 路由安全.

张宇, 博士, 教授, 博士生导师, CCF 高级会员, 主要研究领域为互联网基础设施安全, 互联网体系结构, 互联网测量.

张伟哲, 博士, 教授, 博士生导师, CCF 杰出会员, 主要研究领域为信息安全, 系统结构.

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