

Poster: ERIS: Evaluating ROV via ICMPv6 Rate Limiting Side Channels

Renrui Tian
Tsinghua University
Beijing, China

Yahui Li*
Tsinghua University
Beijing, China

Han Zhang
Tsinghua University
Zhongguancun Laboratory
Beijing, China

Xinzhe Liu
Tsinghua University
Zhongguancun Laboratory
Beijing, China

Xia Yin
Tsinghua University
Zhongguancun Laboratory
Beijing, China

Xingang Shi
Tsinghua University
Zhongguancun Laboratory
Beijing, China

Zhiliang Wang
Tsinghua University
Zhongguancun Laboratory
Beijing, China

Jilong Wang
Tsinghua University
Zhongguancun Laboratory
Beijing, China

Abstract

The Resource Public Key Infrastructure (RPKI) plays a crucial role in securing BGP against prefix hijacking by enabling Route Origin Validation (ROV). However, the limited adoption of ROV in the real world undermines the effectiveness of RPKI. Hence, measuring ROV deployment in practice is essential for assessing the impact of RPKI. Existing measurement efforts either suffer from limited coverage and accuracy due to reliance on control-plane data, or require controlled IP prefixes or large-scale deployment of vantage points. Furthermore, most studies focused on IPv4, leaving ROV status in IPv6 largely underexplored.

To bridge this gap, we propose *ERIS*, the first measurement framework to evaluate ROV in IPv6 by leveraging ICMPv6 rate limiting side channels. *ERIS* does not require controlled prefixes or distributed vantage points, enabling scalable and accurate ROV measurements from a single vantage point.

CCS Concepts

• Security and privacy → Network security.

Keywords

RPKI; Route Origin Validation; ICMPv6 Rate Limiting Side Channel

ACM Reference Format:

Renrui Tian, Yahui Li, Han Zhang, Xinzhe Liu, Xia Yin, Xingang Shi, Zhiliang Wang, and Jilong Wang. 2025. Poster: ERIS: Evaluating ROV via ICMPv6 Rate Limiting Side Channels. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25)*, October 13–17, 2025, Taipei, Taiwan. ACM, New York, NY, USA, 3 pages. <https://doi.org/10.1145/3719027.3760707>

1 Introduction

The Resource Public Key Infrastructure (RPKI) is the most widely deployed security mechanism for mitigating BGP prefix hijacks.

*Yahui Li is the corresponding author of this paper.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
CCS '25, Taipei, Taiwan

© 2025 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1525-9/2025/10
<https://doi.org/10.1145/3719027.3760707>

It operates as a hierarchical and distributed system of Route Origin Authorizations (ROAs), which specify the ASes authorized to originate particular prefixes. By enforcing Route Origin Validation (ROV) on border routers, ASes can filter out invalid route announcements and thus prevent prefix hijacking. However, the limited adoption of ROV in practice undermines RPKI protection. Many ASes, discouraged by operational costs and insufficient incentives, choose not to implement ROV, leaving significant portions of the Internet exposed to threats. Therefore, measuring ROV is critical for evaluating the security impact of RPKI.

Prior efforts to measure ROV typically adopted control-plane or data-plane approaches, or both. Control-plane methods [3, 4, 6, 11] pinpoint ASes that announce or forward RPKI-invalid routes by analyzing routing information, but often struggle with low accuracy and incomplete coverage due to limited visibility from public BGP collectors into routing decisions [6, 11]. Data-plane approaches [1, 2, 5–7] generally rely on controlled IP prefixes or large-scale deployment of vantage points to launch scalable and elaborate measurements. Nonetheless, such methods demand significant resources and operational overhead. In response, [8] proposed a measurement framework that leverages IP-ID side channel to assess ROV status without requiring prefix ownership or recruiting vantage points. However, this technique cannot be extended to IPv6. Besides, existing studies mainly focused on measuring ROV enforcement in IPv4, leaving IPv6 largely underexplored.

To extend the strengths of [8] to ROV measurement in IPv6, we present *ERIS*, a pioneering framework that evaluates ROV status in IPv6 by exploiting ICMPv6 rate limiting side channels. Through carefully crafted probing techniques and inference strategies, *ERIS* enables extensive ROV measurements in IPv6 from a single vantage point without the need for controlled prefixes or distributed probe infrastructure. Our approach significantly lowers the barrier to large-scale measurements, offers a practical and resource-efficient alternative to existing techniques, and provides critical insights into the security landscape of the next-generation Internet.

2 Reachability Inference via ICMPv6 Rate Limiting Side Channels

ROV status and network reachability. As demonstrated in [1, 7], a straightforward approach to measuring the ROV status of an AS is to test whether remote hosts within the target AS can reach an RPKI-invalid prefix. Building upon this idea, [8] leveraged IP-ID

side channel to eliminate the need for vantage points, though their method is limited to IPv4. To extend ROV side-channel measurement to IPv6, we develop a reachability inference technique that exploits ICMPv6 rate limiting side channels.

Prior work. [10] was the first to introduce the use of ICMPv6 rate limiting side channels for measuring network reachability. However, this method faces two critical limitations. First, it relies on accurate estimation of round-trip time (RTT) between two remote hosts, which is difficult to obtain at a feasible cost and undermines the robustness of the reachability conclusions. Second, it uses a fixed number of probe packets for all routers, without accounting for variations in their rate limiting parameters and implementations. For most routers, this results in excessive probing that depletes their token buckets unnecessarily. The prolonged refill time that follows delays subsequent measurements, thereby reducing the efficiency of repeated probing for individual routers.

Our approach. To overcome these limitations, we propose two major improvements. We first eliminate the need for RTT estimation by *extending the timing for detecting the router's rate-limiting state*. By continuously sending probe packets and carefully controlling the rate of reflected responses, we are able to maintain the rate-limited state if the target router is reachable, thereby enabling robust and RTT-insensitive detection. In addition, we implement *a lightweight yet effective calibration that dynamically determines the minimum probe rate required to trigger ICMPv6 rate limiting* for each individual router. By adapting the probe rate to each router's specific rate limiting threshold, this approach reduces token bucket refill delays and substantially improves both measurement efficiency and scalability. The improved reachability measurement operates as follows:

(1) *Setup.* Given two remote routers A and B , along with an unassigned address T within the subnet routed by B , our objective is to infer whether A can reach B without requiring control over either device.

(2) *Rate calibration.* To ensure robust and accurate detection, we first employ an adaptive calibration mechanism to determine the minimum probe rate necessary to trigger ICMPv6 rate limiting at router B . This calibration begins with a slow start phase, where the probe rate is doubled in each step. Starting from a low initial rate, we send probe packets (e.g., ICMPv6 Echo Requests) to T , eliciting ICMPv6 Destination Unreachable messages from B . We then monitor the number of responses received: if the number of responses matches the number of probes sent, we infer that rate limiting has not yet been triggered; otherwise, if the response count falls below the number of sent probes, we conclude that the rate-limiting threshold has been exceeded. Subsequently, we perform a binary search between the last non-limiting rate and the first limiting rate to pinpoint the minimum probe rate that reliably triggers rate limiting. This adaptive procedure tailors the probe rate to each router's specific threshold and reduces the impact of token bucket refill delays.

(3) *Reachability inference.* Once the minimum rate-limiting threshold of B is established, we proceed with the reachability measurement. We send ICMPv6 Echo Requests to A at the calibrated rate, with a spoofed source address T . This prompts A to send ICMPv6 Echo Replies back to T at the same rate. If A can reach the prefix routed by B , these replies will be transmitted to B , and B will

generate ICMPv6 Destination Unreachable messages. By tuning the probe rate to trigger rate limiting, we can maintain B in a rate-limited state over an extended period. This prolonged timing allows for accurate observation of rate-limiting behavior and significantly improves the robustness of the detection. Finally, we send a small number of normal ICMPv6 Echo Requests to T . By comparing the expected and observed number of error messages received, we can reliably determine whether B is rate-limited, thereby inferring the reachability from A to B .

Practical considerations. While our approach enables robust and scalable reachability inference via ICMPv6 rate limiting, its applicability is subject to several conditions:

- (1) *Source address spoofing.* The measurement host must support IPv6 source address spoofing, which may be blocked by source address validation (SAV). In practice, many vantage points without strict SAV enforcement remain usable.
- (2) *Sufficient reflected response rate.* Router A must respond to spoofed probes at a sufficiently high rate to trigger rate limiting at B . To satisfy this, we only select routers with loose rate limiting for measurement.
- (3) *Global rate limiting.* We assume that router B enforces global ICMPv6 rate limiting across all incoming traffic. To ensure this, we conduct a supplemental test to filter out routers that apply per-source rate limiting.
- (4) *ICMPv6 filtering.* Intermediate networks or end routers may apply ICMPv6 filtering and thus drop reflected ICMPv6 messages from A , which may hinder the observation of rate-limiting behavior. To mitigate this issue, we can use alternative reflection-based protocols such as TCP packets or UDP-based DNS queries. For example, spoofed DNS requests sent to a DNS resolver A' can induce it to send responses to B , which can similarly trigger rate limiting and thus serve the same purpose as ICMPv6 in our measurement.

3 ROV Measurement with ERIS

In this section, we present how *ERIS* infers ROV status by leveraging ICMPv6 rate limiting side channels described in Section 2. As shown in Figure 1, *ERIS* first identifies IPv6 addresses within globally routed prefixes and RPKI-invalid prefixes. This yields two sets of responsive addresses: those located within ASes (referred to as *probes*), and those located within RPKI-invalid prefixes (referred to as *targets*). *ERIS* then performs reachability measurements for each pair of *probes* and *targets*. Finally, it aggregates the measurement results at the AS-prefix level to assess the ROV status.

Discovery of probes and targets. We use the RouteViews [9] dataset to extract global IPv6 prefixes, and validate the latest BGP updates to select the prefixes exclusively covered by RPKI-invalid announcements, ensuring that *packets sent to these prefixes can only be routed to an illegitimate AS* [8]. We then apply the strategy described in [10] to obtain active router addresses as *probes* and *targets* from the corresponding prefixes. For each prefix, we iterate over its /64 sub-prefixes and randomize lower bits to construct a probe address. Due to the sparsity of the IPv6 address space, sending an echo request to such an address typically elicits an ICMPv6 Destination Unreachable message from a periphery router, which reveals the router address and an unreachable IPv6 address

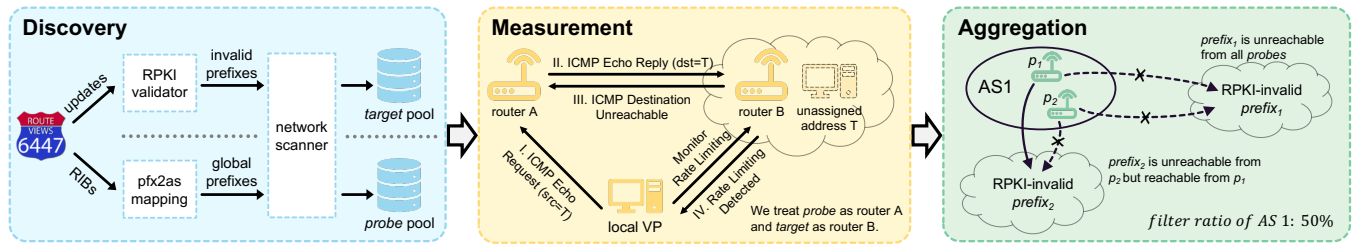


Figure 1: The framework of ERIS.

within its subnet. To ensure availability, we further select *probes* that can promptly respond to frequent requests and *targets* with global rate limiting.

Reachability measurement. We filter out ASes that do not have sufficient number of identified *probes* to improve the confidence of subsequent measurements. For each remaining AS, we measure the reachability from each of its *probes* to each *target* as described in Section 2. To mitigate transient network jitter, we conduct multiple rounds of measurement and draw reachability conclusions only if consistent results are observed.

Result aggregation. We aggregate the results at AS-prefix level to infer ROV status. Inspired by [8], we define a filter ratio to evaluate the extent of RPKI-based protection. Specifically, the filter ratio represents the proportion of RPKI-invalid prefixes that are unreachable from all *probes* within a given AS. A higher ratio indicates better protection, as more invalid prefixes are filtered—either due to the AS’s own ROV deployment or collateral benefit derived from its upstream providers.

4 Preliminary Results

We implemented a prototype framework (about 4.5K lines of code) and conducted a preliminary experiment that covers 5,440 ASes. Based on a simple assumption that ASes with a filter ratio below 50% have not deployed ROV, we found that 43.66% of them have not implemented ROV. For example, we observed that a Tier-1 provider AS6762 has not deployed ROV, which aligns with its behavior in IPv4, as reported by [8]. Compared to APNIC [7], ERIS achieves over 89% recall within the top 10, top 100, and top 1,000 AS rankings. However, a minor yet non-negligible portion of our results shows inconsistencies with APNIC, primarily because we use a fixed threshold for classification while the filter ratios measured by both methods are inherently sensitive to variations in vantage point sampling, which can lead to discrepancies in classification outcomes. In future work, we plan to enhance the measurement framework to improve its accuracy and robustness, and to perform a more comprehensive analysis of the measurement results. We also intend to regularly release updated datasets to support ongoing research in the community.

5 Ethics

We have made extensive efforts to minimize the impact on network devices. We limit the total scanning bandwidth to 100 Mbps and the maximum bandwidth per prefix to 1 Kbps during the discovery phase. In reachability measurements, we use the minimum rates to conserve bandwidth on both *probes* and *targets*. With a probing

rate of 100 pps and a packet size of 70 bytes, we ensure that the peak bandwidth usage is limited to approximately 14 KB/s, and the process completes within 5 seconds.

6 Acknowledgment

This research is supported by the National Natural Science Foundation of China (No. 62102020, 62394322).

References

- [1] Ben Cartwright-Cox. 2018. Are BGP’s security features working yet? <https://blog.benjojo.co.uk/post/are-bgps-security-features-working-yet-rpki>
- [2] Wenqi Chen, Zhiliang Wang, Dongqi Han, Chenxin Duan, Xia Yin, Jiahai Yang, and Xingang Shi. 2022. ROV-MI: Large-Scale, Accurate and Efficient Measurement of ROV Deployment. In *29th Annual Network and Distributed System Security Symposium, NDSS 2022, San Diego, California, USA, April 24-28, 2022*. The Internet Society. <https://www.ndss-symposium.org/ndss-paper/auto-draft-183/>
- [3] Yossi Gilad, Avichai Cohen, Amir Herzberg, Michael Schapira, and Haya Schulmann. 2017. Are We There Yet? On RPKI’s Deployment and Security. In *24th Annual Network and Distributed System Security Symposium, NDSS 2017, San Diego, California, USA, February 26 - March 1, 2017*. The Internet Society. <https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/are-we-there-yet-rpkis-deployment-and-security/>
- [4] Caitlin Gray, Clemens Mosig, Randy Bush, Cristel Pelsser, Matthew Roughan, Thomas C. Schmidt, and Matthias Wahlisch. 2020. BGP Beacons, Network Tomography, and Bayesian Computation to Locate Route Flap Damping. In *Proceedings of the ACM Internet Measurement Conference (Virtual Event, USA) (IMC '20)*. Association for Computing Machinery, New York, NY, USA, 492–505. <https://doi.org/10.1145/3419394.3423624>
- [5] Tomas Hlavacek, Amir Herzberg, Haya Shulman, and Michael Waidner. 2018. Practical Experience: Methodologies for Measuring Route Origin Validation. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. 634–641. <https://doi.org/10.1109/DSN.2018.00070>
- [6] Tomas Hlavacek, Haya Shulman, Niklas Vogel, and Michael Waidner. 2023. Keep Your Friends Close, but Your Routers Closer: Insights into RPKI Validation in the Internet. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 4841–4858. <https://www.usenix.org/conference/usenixsecurity23/presentation/hlavacek>
- [7] Geoff Huston. 2021. Measuring ROAs and ROV. <https://blog.apnic.net/2021/03/24/measuring-roas-and-rov>
- [8] Weitong Li, Zhexiong Lin, Md. Ishtiaq Ashiq, Emile Aben, Romain Fontugne, Amresh Phokeer, and Taejoong Chung. 2023. RoVista: Measuring and Analyzing the Route Origin Validation (ROV) in RPKI. In *Proceedings of the 2023 ACM on Internet Measurement Conference (Montreal QC, Canada) (IMC '23)*. Association for Computing Machinery, New York, NY, USA, 73–88. <https://doi.org/10.1145/3618257.3624806>
- [9] University of Oregon. 2024. University of Oregon RouteViews Project. <https://www.routeviews.org/routeviews/>
- [10] Long Pan, Jiahai Yang, Lin He, Zhiliang Wang, Leyao Nie, Guanglei Song, and Yaozhong Liu. 2023. Your Router is My Prober: Measuring IPv6 Networks via ICMP Rate Limiting Side Channels. In *30th Annual Network and Distributed System Security Symposium, NDSS 2023, San Diego, California, USA, February 27 - March 3, 2023*. The Internet Society. <https://www.ndss-symposium.org/ndss-paper/your-router-is-my-prober-measuring-ipv6-networks-via-icmp-rate-limiting-side-channels/>
- [11] Andreas Reuter, Randy Bush, Italo Cunha, Ethan Katz-Bassett, Thomas C. Schmidt, and Matthias Wahlisch. 2018. Towards a Rigorous Methodology for Measuring Adoption of RPKI Route Validation and Filtering. *SIGCOMM Comput. Commun. Rev.* 48, 1 (apr 2018), 19–27. <https://doi.org/10.1145/3211852.3211856>