RoVista: Measuring and Analyzing the Route Origin Validation (ROV) in RPKI

Weitong Li
Virginia Tech
USA

Zhexiao Lin
University of California, Berkeley
USA

Md. Ishtiaq Ashiq
Virginia Tech
USA

Emile Aben
RIPE NCC
Netherlands

Romain Fontugne
IIJ Research Lab
Japan

Amreesh Phokeer
Internet Society
USA

Taejoong Chung
Virginia Tech
USA

ABSTRACT

The Resource Public Key Infrastructure (RPKI) is a system to add security to the Internet routing. In recent years, the publication of Route Origin Authorization (ROA) objects, which bind IP prefixes to their legitimate origin ASN, has been rapidly increasing. However, ROAs are effective only if the routers use them to verify and filter invalid BGP announcements, a process called Route Origin Validation (ROV).

There are many proposed approaches to measure the status of ROV in the wild, but they are limited in scalability or accuracy. In this paper, we present RoVista, an ROV measurement framework that leverages IP-ID side channel and in-the-wild RPKI-invalid prefix. With over 20 months of longitudinal measurement, RoVista successfully covers more than 28K ASes where 63.8% of ASes have derived benefits from ROV, although the percentage of fully protected ASes remains relatively low at 12.3%. In order to validate our findings, we have also sought input from network operators.

We then evaluate the security impact of current ROV deployment and reveal misconfigurations that will weaken the protection of ROV. Lastly, we compare RoVista with other approaches and conclude with a discussion of our findings and limitations.

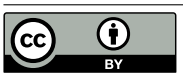
CCS CONCEPTS

• **Networks** → **Routing protocols**; Network measurement; • **Security and privacy** → **Security protocols**.

KEYWORDS

Resource Public Key Infrastructure, RPKI, Route Origin Validation, IP-ID Side Channel, Network Measurement

ACM Reference Format:
Weitong Li, Zhexiao Lin, Md. Ishtiaq Ashiq, Emile Aben, Romain Fontugne, Amreesh Phokeer, and Taejoong Chung. 2023. RoVista: Measuring and Analyzing the Route Origin Validation (ROV) in RPKI. In *Proceedings of the 2023 ACM Internet Measurement Conference (IMC '23), October 24–26, 2023, Montreal, QC, Canada.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3618257.3624806



IMC '23, October 24–26, 2023, Montreal, QC, Canada

ACM ISBN 979-8-4007-0382-9/23/10.
https://doi.org/10.1145/3618257.3624806

1 INTRODUCTION

The Border Gateway Protocol (BGP) is *the* mechanism by which routers exchange routing information across administrative domains. However, due to its reliance on trust, BGP is known to be vulnerable to attacks such as prefix hijacking [10, 45, 72, 82] and route leaks [42, 77]. To defend against these threats, many security extensions to BGP were introduced such as soBGP [81], S-BGP [38], BGPsec [31], and RPKI [8]; among them, RPKI has been the most popular, with RPKI objects covering more than 40% of the IPv4 prefixes being announced nowadays [65].

The Resource Public Key Infrastructure (RPKI) was introduced in 2008 [39]. At its core, RPKI is a hierarchical Public Key Infrastructure (PKI), which is rooted at the five Regional Internet Registries (RIRs).[1] RPKI uses a certificate to bind Internet Number Resources such as Autonomous Numbers (ASNs) and IP addresses to public keys via certificates. The corresponding private key is used to sign RPKI objects, such as Route Origin Authorization (ROA) objects which provide the legitimate origin Autonomous System Numbers (ASNs) of certain IP prefixes. Each of the five RIRs operates its own RPKI trust anchor and repository so that they can sign RPKI certificates and distribute RPKI objects such as ROA objects to the interested parties (e.g., routers). In recent few years, network resource owners (e.g., ISPs) have rapidly registered their prefixes in RPKI such as Comcast [36], Microsoft [51], or Netflix [52].

But, like any PKI, RPKI can only function correctly when routers (or ASes) also perform validation using ROA objects, which is called *Route Origin Validation* (ROV) [46]. Routers that do not perform ROV can still accept and propagate incorrect BGP announcements, letting attackers hijack IP prefixes *even if there is a ROA object that can verify such announcements.* Unfortunately, it is challenging to measure and identify the ROV status of an AS without access to its routers and hosts, so the overall state of deployment of ROV on the Internet is still not known in detail.

[1] APNIC, LACNIC, RIPE NCC, ARIN, and AFRINIC.

There has been a series of work that applies passive and active measurement techniques to understand the ROV status over networks [32, 34, 37, 50, 60, 75, 76]; one prominent example is `isBGPSafeYet.com` [37] that serves two contents, one of which is from a RPKI-valid IP address and the other one is from RPKI-invalid one. Thus, if the visitor can only fetch the content from the RPKI-valid IP address, it suggests that the AS is protected by ROV.

While these approaches successfully have measured the status of ROV of ASes, they often have a number of limitations. First, active-based measurements are usually done with a single or a couple of test IP prefixes making it hard to characterize the ROV policy of ASes [37, 59, 60]; for example, an AS that deploys ROV may choose not to do so for the IP prefixes announced from their customers. The same issue can arise when ASes are connected to multiple transit providers or peers.

Second, these approaches require a significant number of visitors or vantage points in order to measure numerous ASes; some prior works [18, 60, 76] use existing hardware such as RIPE Atlas [62], but this is often difficult to scale as users must deploy devices in their networks. For example, RIPE Atlas covers only 3,765 IPv4 ASNs at the time of writing [61].

In this paper, we explore an alternative approach to measure the ROV status of ASes, which allows us to characterize more than 28K ASes over 20 months without recruiting vantage points. This enables us to analyze how ROV has improved routing security over time. Coupled with the datasets, we also discuss the operational challenges of ROV.

In this paper, we make the following contributions:

- We present an ROV measurement technique called RoVista, which captures the ROV status of ASes without the need for IP prefixes or recruiting vantage points.
- We run RoVista for 20 months and analyze ROV policies for more than 28 K ASes; we find 10 K (36.2%) ASes that never perform ROV and 3,482 (12.3%) ASes that are perfectly protected by ROV.
- We cross-validate our findings with other trustworthy sources: from ISPs official announcement, survey of network operators, and personal communication.
- We show the impact and the challenge of ROV and compare our technique with other studies.

Our findings highlight the need for auditing of ROV policies of ASes for a better RPKI ecosystem. To this end, we release all of our code and datasets to the research community at

https://rovista.netsecurelab.org

for network operators, administrators, and researchers to reproduce and benefit from our work.

2 BACKGROUND AND RELATED WORK

2.1 BGP

Routers construct routing tables using Border Gateway Protocol (BGP). Briefly, BGP speakers announce *paths* towards the origin of IP prefixes through a series of ASes; for example, an example of a BGP route is like the following:

```
IP Prefix: 45.3.0.0/16
AS_PATH: AS3356 AS174 AS40220
```

In this route, we see that AS 40220 originates a route for an IP prefix of 45.3.0.0/16. Neighbors receive this route and use it in their routing tables, as well as forward it on to their neighbors according to its routing policy.

The BGP route selection process determines the optimal path for routing, usually based on factors like cost-efficiency and path length, when multiple announcements for the same IP prefix are received. When forwarding packets, routers utilize the most specific prefix available in their routing table.

Due to the missing security features in the original BGP protocol, interdomain routing is prone to many security attacks; first, an attacker can announce an IP prefix that it is not legitimately allowed to announce to intercept the traffic for that IP prefix to be sent; this is called *prefix hijacking*. Second, an attacker can perform *sub-prefix hijacking* by announcing a more specific IP prefix than the legitimate original prefix (e.g., announcing `45.3.96.16/20` in the above example.). Routers prioritize the most specific prefix, causing all traffic intended for the attacked prefix to be forwarded to the attacker.

These attacks have occurred frequently in practice, with significant effects on the original IP prefix holders [5, 7, 15].

2.2 RPKI

RPKI is a public key infrastructure that provides a cryptographically verifiable means of mapping IP prefixes to the origin ASes, which prevents both prefix hijacking and sub-prefix hijacking attacks. To do so, (1) network resource owners need to register RPKI objects to prevent their IP prefixes from being hijacked, and (2) network operators need to validate the BGP announcements with them to filter out the BGP announcements with RPKI-invalid IP prefixes.

Registering IP Prefixes: Network resource owners can authorize their IP prefixes by creating (at least) two objects;

(a) a CA certificate, which binds a set of Internet Number Resources (INRs) such as Autonomous System Numbers (ASNs) or IP Prefixes to a public key.

(b) a Route Origin Authorization (ROA), which authorizes an AS to announce IP prefixes; this object is ultimately signed by a CA certificate.

These objects must be published into public RPKI repositories operated by the five Regional Internet Registries (RIRs), each of which manages its own trust anchor. A trust anchor is equivalent to root certificates in other PKIs such as root stores in web PKI. In 2019, Chung et al. [17] reported that approximately 25% of ASes have published ROAs by analyzing the all of the RPKI objects present in the repositories.

Validating BGP announcements: RPKI validation software, called Relying Party (RP) software such as Routinator [71], fetches RPKI objects from the five repositories and performs cryptographic validation. Then, it produces a list of validated tuples (ASN, ROA prefix, prefix length), which is called Validated ROA Payloads (VRPs). The set of VRPs is provided to the AS's routers using the RP protocol [9] so that they can validate the incoming BGP announcements based on the standard [46], which is called *Route Origin Validation* (ROV).

When an RPKI-validating router receives a BGP announcement, it attempts to validate the announcement using the set of VRPs.

First, it determines whether the IP prefix in the BGP announcement is *covered* by any VRP. If so, it then determines if the BGP announcement exactly *matches* the VRP; a BGP announcement is said to match a VRP when (1) the VRP IP prefix covers the announced IP prefix, (2) the VRP AS matches the announced AS, and (3) the prefix length in VRP is greater than or equal to the announced prefix. Thus, we consider a BGP announcement to be *valid* if it is matched by a VRP, to be *invalid* if the IP prefix in the BGP announcement is covered, but no VRP matches the BGP announcement, and *unknown* if it is not covered by any VRP.

Unlike measuring the ROA deployment status across the network resource owners, *understanding how the Internet is currently benefits from ROV is known to be challenging* mainly due to the limited access to external routers (and ASes).

2.3 Efforts to measure ROV status

There have been a number of approaches to measure the ROV deployment across ASes.

Passive measurement approach: There has been a long thread of studies [23, 32, 50, 75] that mainly focused on the ASes who announce or forward RPKI-invalid BGP announcements by referring to the global BGP tables. These methods are straightforward, though it has been shown that passive measurements solely relying on control plane information may incorrectly identify ROV enabled ASes mainly due to limited visibility of routing decision [59].

Active measurement approach: To overcome the limitation of passive measurement techniques, an extensive series of successful studies [34, 37, 59, 60, 69, 76] examined the ROV status of ASes by *announcing RPKI-invalid prefixes themselves*. More specifically, they register ROAs for their IP prefix but with *a different AS that they would announce* to make their BGP announcement invalid. For example, Rueter et al. [59] conducted a controlled experiment by announcing RPKI-invalid prefixes from their own AS to infer the ASes that deployed ROV by comparing their prefix visibility measured from RouteViews [70] and RIPE RIS [63]. Similarly, other studies [34, 37, 60, 69, 76] also published their ROAs, but they use a data-plane based approach such as traceroute [60, 76] or HTTP requests [34, 37, 69] to infer the connectivity from a host towards RPKI-invalid prefixes. They used Google Ads network [34] or dedicated hardware (e.g., RIPE Atlas [18, 60, 76, 76]), or relied on volunteers [37, 69] to recruit vantage points.

Other studies [19, 76] present a methodology that does not require volunteers by performing ICMP [19] or TCP [76] scans of the entire IPv4 space to measure the connectivity towards RPKI-invalid hosts; however, it is often inaccurate as it introduces an inconsistency depending on the chosen measurement location. Recently, Chen et al. [18] applied a machine learning technique to infer the ROV policy of ASes, which tried to infer ROV policies of 8 K ASes using RIPE Atlas.

3 ROVISTA: SYSTEM DESIGN

3.1 Design Goals

As introduced in §2.3, there are considerable works that measure ROV status of ASes by (1) announcing an RPKI-invalid IP prefix that they control and (2) recruiting remote hosts that send a probe

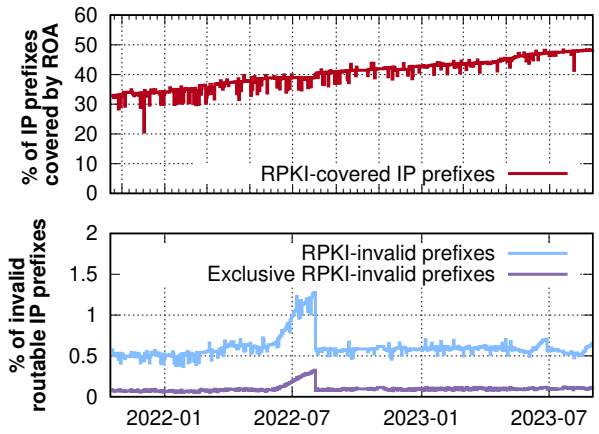


Figure 1: The coverage of ROA and the percentage of invalid IP prefixes routed through a single origin are shown. The surge of RPKI-invalid prefixes was caused by AS 23674 and 62240, which announced 434 invalid prefixes between May 27th and August 3rd, 2022.

(e.g., HTTP requests [37]) to test their reachability towards such RPKI-invalid prefix. However, we argue that these approaches have two limitations. First of all, the ROV policy of an AS is not uniform across all IP prefixes; for example, we find that even ROV ASes can still accept RPKI-invalid announcements when they are routed from their customers because filtering the RPKI-invalid prefixes forwarded from their customers could potentially harm their profit. Thus, we have to use multiple RPKI-invalid IP prefixes to accurately understand the ROV policy of ASes. Second, measuring the ROV policy of ASes at scale is difficult when it requires cooperation of vantage points (e.g., RIPE Atlas) or volunteers (e.g., isbgpsafeyet.com) in a variety of networks across the globe.

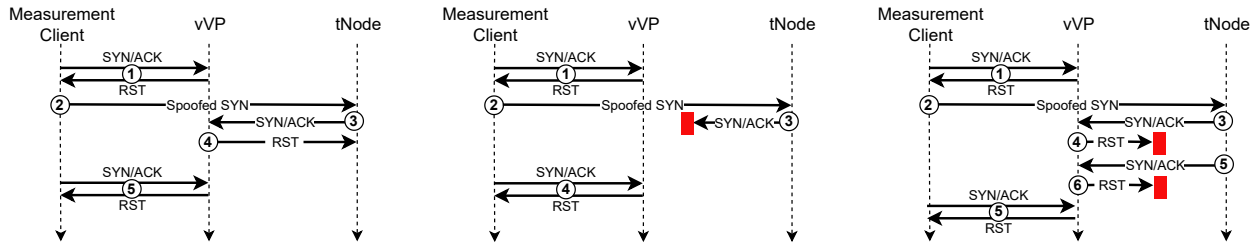
RoVista tries to overcome such limitation; it does not require any IP prefixes to control and volunteers or vantage points that can run the experiment. Specifically, we (1) leverage in-the-wild RPKI-invalid prefixes and (2) use IP-ID side-channel technique to conjecture the reachability from a remote end host to another host under in-the-wild RPKI-invalid prefixes.

3.2 In-the-wild RPKI-invalid prefixes

Network resource owners have rapidly registered their prefixes in RPKI by publishing ROAs such as Comcast [36] and Microsoft [51]; Figure 1 (top) shows the portion of IP prefixes covered by at least one VRP from December 24th, 2021 to September 12th, 2023 captured at RouteViews [70]. We find a steady growth of RPKI deployment; for example, 48.2% of IPv4 prefixes are RPKI-covered in our latest snapshot.

However, when validating BGP announcements in the wild against ROAs, they are not always valid; as shown in Figure 1 (bottom), there were 6,782 (0.7%) RPKI-invalid prefixes in the latest snapshot, *which should be filtered by the ASes that implement ROV*.

Thus, we could infer the ROV status of an AS if we have (1) well-distributed presence of such prefixes across networks, and (2)



(a) No filtering (b) Inbound filtering (c) Outbound filtering

Figure 2: Timeline of our methodology to detect the ROV-policy of a vVP's AS by leveraging the IP-ID side-channel.

a reliable method that can measure the directional connectivity from the AS towards RPKI-invalid prefixes; for example, if multiple hosts within an AS cannot reach to many RPKI-invalid prefixes it may indicate that the AS is protected by ROV.

However, we cannot blindly use all RPKI-invalid prefixes for our measurement. This is because a prefix that is announced by an incorrect AS (thus being RPKI-invalid) may still be reachable from ROV ASes if the same prefix is also announced by the legitimate AS. In such cases, the traffic will be directed to the legitimate AS, potentially leading to a mistaken identification that the AS can reach RPKI-invalid prefixes and therefore not implementing ROV. Thus, we must selectively choose RPKI-invalid prefixes that are not announced by their legitimate AS, by comparing them with other BGP announcements. Figure 1 (bottom) shows the percentage of RPKI-invalid prefixes that are exclusively announced by wrong ASNs; we observe 1,362 prefixes during our measurement period, which we call *test IP prefixes*. We also call the hosts under test IP prefixes, *test nodes, or tNodes*.

3.3 Measuring ROV status with IP-ID side-channel

We now try to infer the reachability between two remote end hosts using a technique called IP-ID side-channel, which has been used in other areas for detecting censorship [57], measuring packet drop [28] and ingress filtering [25].

The IP-ID is a 16 bits field in the IPv4 header [56] and was originally designed to assist packet fragmentation and reassembly by assigning a unique identifier for each packet. There are multiple methods to assign the IP-ID for each packet by managing a *counter*, which is mainly determined by the implementation of the Operating System (OS). We specifically focus on the *Global counter*, which increments the IP-ID by 1 unit whenever it sends a new packet regardless of its destination; this is used in early versions of Windows (e.g., Windows XP) or FreeBSD [48]. We refer to hosts with a global counter as *virtual vantage points* (vVPs) and use them *to infer the connectivity of a host towards tNodes*.

At a high-level, we keep monitoring how the vVP's IP-ID grows by sending TCP SYN packets to the vVP from our measurement client so that we can record its IP-ID in the corresponding ACK packets. At the same time, we send *spoofed* TCP SYN packets to a tNode to let it send TCP SYN/ACK packets to the vVP. Depending on the reachability between the VRP and the tNode, we can observe three possible IP-ID growth patterns as illustrated in Figure 2;

(a) No filtering between the tNode and the vVP (i.e., the vVP's AS does not perform ROV); in such case, we see the bursty IP-ID growth (between ① and ④) by the number of spoofed packets that we have generated.

(b) Inbound filtering; this is due to either egress filtering of the tNode's AS or ingress filter of the vVP's AS; in this case, we do not see any IP-ID growth between the step ① and ④ other than the RST packets to our measurement client in the step ④.

(c) Outbound filtering; this could be due to (1) the ROV on the vVP's AS or its upstream AS or (2) ingress filtering of the tNode (thus, false positive); such false positives can be eliminated as we test multiple vVPs in the same AS with *many tNodes*. Similar to the 'No Filtering' case, we can observe the IP-ID growth by the number of the SYN/ACK packets from the tNode; however, since the RST packets cannot reach the tNode, it will trigger the tNode's Retransmission Timeout (RTO) after a certain period (usually 3 seconds [58]) making the tNode send another SYN/ACK packets. In return, vVP will also send additional RST packets letting us detect an additional bursty growth of IP-IDs.

4 ROVISTA: IMPLEMENTATION

4.1 Obtaining tNodes

Every 4 hours, we collect and validate RouteView datasets with all RPKI objects collected from all of the five RPKI repositories to obtain test IP prefixes. We then scan them using ZMap [26] to find tNodes that open popular TCP port numbers [68] so that we can send TCP SYN packets. For each tNode, we confirm whether it responds to our spoofed SYN packets and implements RTO correctly; to this end, we set up two measurement clients in two different ASes, and we let one client send SYN packets to a tNode with the spoofed source IP address to the other measurement client. We then check whether it satisfies all the following conditions:

(a) It must respond to our spoofed SYN packets with proper SYN/ACK packets.

(b) It must start retransmission if it does not receive any ACK or RST packet from the destination within 1 ~ 3 seconds.

(c) It must not perform retransmission when receiving RST packets. Otherwise, we cannot distinguish between the no filtering and outbound filtering case.

Removing false tNodes: Due to the incomplete view of the routing table in RouteViews, there can be tNodes that remain reachable through alternative routes. Thus, we take additional steps to minimize such erroneous tNodes; First, to avoid RPKI-invalid announcement changes during our measurement period, we ensure that the validity of the tNodes IP prefix remains unchanged for each measurement round by validating BGP announcements before and after the experiment. Second, we use RIPE Atlas probes and choose probes from the 10 ASes that we confirmed their ROV deployment through personal communication [6, 22] or their official announcements [27, 41, 78].[2] We then only consider the tNodes where more than 90% of the probes in ROV ASes cannot reach *and* more than 90% of the probes in non-ROV ASes can reach them; we can find, on average, 31 tNodes (with a minimum of 10 tNodes) during our measurement process.

4.2 Obtaining Virtual Vantage Points (vVPs)

We use ZMap to obtain a set of vVP candidates, which respond to our TCP SYN/ACK scans with a RST packet so that we can track their IP-ID values. At first glance, identifying a host with a global counter seems trivial: we could just send several packets from our machine to see if the IP-IDs in the RST packets continuously grow. However, this approach cannot distinguish between the hosts with a global counter and a local counter, which manages a unique counter for each destination IP address. Thus, we send TCP SYN/ACK packets from different source IP addresses to let it generate RST packets to each of them as background traffic during our measurement period;

(a) To mitigate any potential harm to clients, we send only *five* TCP SYN packets, each of which is from a different port number. To minimize the chance of our packets being out-of-ordered, we set the interval between each packet to a second.

(b) We next send additional five bursty packets each of which has *a different spoofed source IP address.*

(c) Finally, we repeat the first step.

After these steps, we determine it as a vVP when we see a continuous growth (including the wraparound) at least by the number of packets we sent in total of IP-IDs. It is worth noting that scanning for IPv4 and identifying hosts with the global counter is more time-consuming than locating tNodes. As a result, we collect vVPs daily.

4.3 Detecting Outbound filtering

For each pair of vVPs and tNodes, we experiment as follows:

(a) We first send a SYN/ACK packet to a vVP every 0.5 seconds for 5 seconds to measure its background traffic from its IP-ID.

(b) Next, we send 10 spoofed SYN packets to a tNode within ϵ seconds, which only takes a few milliseconds.

[2]The ROV policy of ASes may be updated over time. Thus, we continuously update the list by monitoring their reachability to tNodes.

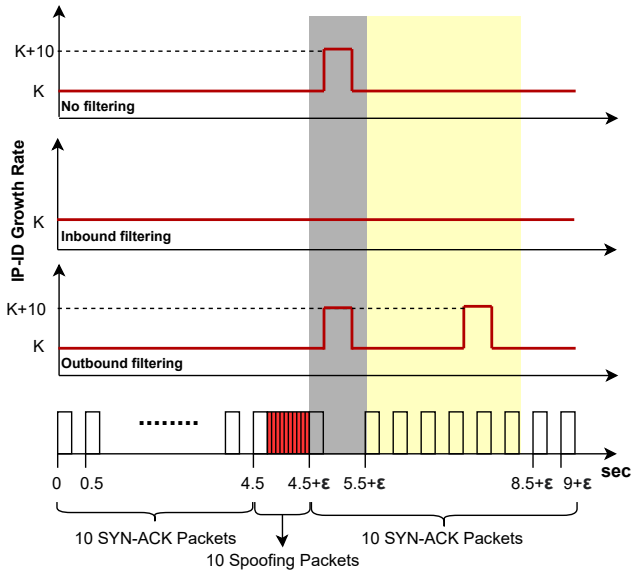


Figure 3: The packet sequence of our experiment and the IP-ID growth pattern that we expect to observe depending on the reachability between a vVP and a target.

(c) We wait for one second[3] and repeat the first step to measure its traffic again.

We next analyze the IP-ID growth pattern to detect the ROV. Assuming there are K packets per second constantly generated from the vVP, we can expect different IP-ID growth patterns depending on the ROV status of the vVP's AS as illustrated in Figure 3.

(a) No filtering between the tNode and the vVP: we can observe the constant IP-ID growth rate of K packets/sec until we send 10 spoofed packets. After then, we observe one *spike* (around $K + 10$) between $4.5 + \epsilon$ and $5.5 + \epsilon$.

(b) Inbound filtering: the IP-ID growth rate will be the same as K since the vVP will not send any RST packets.

(c) Outbound filtering: we observe one spike after sending 10 spoofed packets similar to (a). Due to the outbound filtering, however, the 10 RST packets from the vVP cannot reach the tNode. This triggers the tNode to raise Retransmission Timeout (RTO) [58] and send additional 10 SYN/ACK packets to the vVP. In return, vVP sends additional 10 RST packets to the tNode, allowing us to observe an additional spike of the IP-ID growth.

Since RoVista generates a time series data (i.e., IP-ID values), we can use statistical detection methods to accurately detect the spike. There has been a number of studies [28, 57] that model IP-ID patterns to detect such spikes so that we can utilize. However, these methods typically gain more accuracy as they collect more data (e.g., 500 spoofed packets [28]) or they run lengthy measurements over the same node (e.g., 47 trials in 17 days [57]).

Since our focus is to detect a collective behavior of vVPs in the same AS not an individual vVP's behavior [28] while limiting the

[3]We assume that all 10 SYN/ACK packets from the tNode have arrived at the vVP within one second.

number of spoofing packets to 10 to minimize the potential harm to vVPs, we take an alternative approach:

Similar to prior work [28], we initially employ the Autoregressive Moving Average (ARMA) model [11] to model each time series. However, it is important to note that the ARMA model is applicable only to stationary time series, where statistical properties such as mean remain constant over time. Hence, the ARMA model may not perform well when dealing with time series that exhibit changing statistical properties, such as those with trends or seasonality. Thus, we also utilize the *Autoregressive Integrated Moving Average* (ARIMA) [11] model instead when the IP-ID pattern is identified as a *nonstationary time series* using the Augmented Dickey-Fuller (ADF) test [29]. We then apply one-tailed hypothesis testing on observed IP-ID pattern to detect a spike.[4]

5 ETHICS

Our methodology could bring up a few ethical measurement issues. Below, we discuss the key ethical concerns related to our experiments.

To identify vVPs and tNodes, we perform Internet-wide scans using ZMap, which introduces additional network load on both sides and may raise concerns. To address these concerns, we adhere to the ethical scanning guidelines outlined in [26]. We inform local network administrators to mitigate risks and handle any inquiries that may arise. Additionally, we ensure that our scans do not overwhelm the upstream provider by limiting the scanning bandwidth to 100Mbps. Furthermore, we generate only the necessary amount of traffic required for our research objectives, minimizing any excessive network load.

The (spoofed) TCP packets that we send also raise concerns on network loads and privacy concerns. We acknowledge that we have not asked for any explicit consent to such vVPs, which may violate one of the four principles of the Menlo Report [24], "Respect for Persons"; unfortunately, it is practically impossible for us to obtain an informed consent from all owners of vVPs.

However, it is important to note that the inability to obtain informed consent does not imply a disregard for respect towards individuals [73]. To ensure to follow the guidelines by the Menlo report [24], we note that (1) our methodology only sends TCP packets *without* any payload, (2) for each vVP, we only send less than 51 TCP SYN/ACK packets in 10 seconds with a maximum rate of 12 packet/sec. Additionally, we make sure that the IP addresses of tNodes are not in block lists (Spamhaus [79] and FeodoTracker [1]), thus mitigating any potential harm to operators of vVPs. We also spread out our experiments according to a random permutation of each pair of IP address and port number to minimize potential negative impacts on a host.

We believe that our methodology carefully balances the potential harm to the ASes of vVPs with the scientific benefit of our results.

[4]Given that the accuracy might be influenced by the volume of background traffic, which is beyond our control, we filter out the vVPs for which we cannot draw any inference from the 10 packets. For detailed models and detection methodology, please refer to Appendix A.

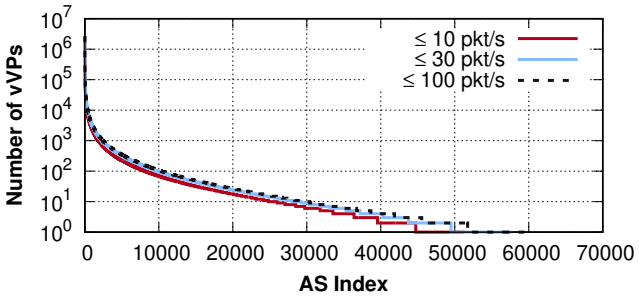


Figure 4: The distribution of the number of vVPs for each ASN from our scan with their background traffic.

6 MEASUREMENT RESULTS

We run RoVista from December 24, 2021 to September 12th, 2023 on a daily basis to measure vVPs and tNodes, and ultimately assess the level of ROV protection for each AS.

6.1 Measurement coverage

vVPs: RoVista has found 43,627,201 vVPs that cover more than 60,000 ASes. However, we intentionally exclude experiments where the background traffic exceeds 10 packets per second to enhance the likelihood of detecting a spike. As a result, we focus on analyzing 1,396,070 (3.2%) vVPs, which correspond to 34,708 (55.2%) ASes. Additionally, we specifically examine ASes for which we have a minimum of 10 vVPs available, which enables us to draw robust conclusions regarding the ROV status of ASes, leaving us with a dataset of 1,396,407 vVPs that cover 28,314 ASes registered in 231 countries.

Due to our restriction to vVPs with low background traffic (i.e., $\leq$ 10 packets), it is possible that we could have measured a greater number of ASes if we had relaxed this limit. The distribution of the number of unique ASes covered by vVPs based on their background traffic is illustrated in Figure 4. Notably, if we had considered vVPs generating background traffic of 30 or 100 packets per second, we could have potentially measured an additional 14,052 and 18,639 ASes, respectively. However, this would require a significant increase in the number of bursty spoofed packets sent to tNodes, resulting in a heightened negative impact on both vVPs and tNodes. Therefore, we choose to use vVPs with low background traffic in order to effectively measure the ROV policy of numerous ASes while minimizing the generation of excessive unsolicited traffic to vVPs. For an extended discussion of the ethics of using vVPs, please see §5.

tNodes: We proceed to assess the diversity of IP prefixes associated with these tNodes and discover that they have been routed through 2,902 unique IP prefixes, which belong to 466 ASes registered in 51 countries. Furthermore, the ROAs that invalidate these IP prefixes are evenly distributed across all Regional Internet Registries (RIRs): 1,317 tNodes in APNIC, 402 tNodes in RIPE NCC, 690 tNodes in ARIN, 198 tNodes in AFRINIC, and 295 tNodes in LACNIC. The broad distribution of tNodes across different geographical locations and networks allows us to gain a comprehensive understanding of the ROV status of ASes on the Internet.

6.2 Determining the Level of ROV Protection

For each pair of vVPs and tNodes, we apply our model to determine if the vVP is unable to reach the tNode. To minimize the false positive arose from the client-side (i.e., vVP) errors, we only consider the tNodes if all vVPs within an AS unanimously agree on their reachability. Since the ROV policy of an AS is not specific to individual clients, if one client cannot reach a tNode due to ROV, all other vVPs within the same AS should also be unable to reach the tNode. On average, we find that 95.1% of tNodes demonstrate consistent reachability across all vVPs within an AS.

Next, we calculate the *ROV protection score*, which represents the percentage of tNodes that are inaccessible from any of the vVPs within the same AS due to outbound filtering. It is important to note that the ROV protection score measures the extent to which an AS is protected by ROV, rather than determining whether it actively deploys ROV itself; the score can be 1.0 if an AS has implemented ROV internally or if all of its upstream providers have implemented ROV, indicating full protection. Conversely, a ROV protection score of zero may indicate that an AS has never deployed ROV. Nevertheless, we believe that the ROV protection score can serve as an indicator of the level of protection provided by RPKI for an AS. Throughout the paper, we use the terms ROV score and ROV protection score interchangeably for brevity.

6.3 Cross-validation

The evaluation of RoVista poses a significant challenge due to the limited transparency surrounding network operators' policies. Obtaining ground truth regarding which ASNs have actually implemented ROV is not a straightforward task.

In this subsection, we first evaluate the accuracy of our IP-ID model using RIPE Atlas and we proceed to evaluate the derived ROV status obtained from three reliable sources: (1) official announcements from network operators, (2) surveys conducted with network operators, and (3) personal communications with network operators.

6.3.1 Evaluating the IP-ID model: traceroute. To validate the reachability between ASes and tNodes, we utilize RIPE-Atlas [62]. We focus on the ASes that can be measured by both RoVista and probes and proceed as follows:

(a) For each tNode, we select 10 probes from an AS with a zero ROV score according to RoVista. TCP traceroutes are executed towards the tNode using the same port number employed by RoVista to ensure a response from the tNode. This process is repeated for all tNodes.

(b) If the last hop in the traceroute result corresponds to the tNode, we consider the probe to have reached the tNode. Otherwise, we consider it unreachable.

By employing this methodology, we gather a total of 168,642 traceroute measurements towards 27 tNodes. These measurements are conducted using 6,296 probes, covering 2,768 ASes, on April 4th, 2022. To eliminate potential errors stemming from the RIPE Atlas API, we exclude traceroute results where different probes within the same AS yield diverse traceroute outcomes for the same tNode. This step allows us to retain 167,392 (99.2%) reliable traceroute results for analysis. We observe that all probes within the same AS exhibit consistent reachability towards a tNode. Consequently, we can confirm that the results are not specific to individual probes. This enables us to construct a dependable list of tuples (AS, tNode, reachability).

We then compare this list with the RoVista measurement results obtained on the same date. Remarkably, we find that all tuples exhibit *a perfect match*, indicating compelling evidence that RoVista accurately identifies the reachability from vVPs to tNodes; this supports the feasibility of measuring the ROV score of ASes using the IP-ID model of RoVista.

6.3.2 Evaluating ROV protection score. Network operators often refrain from disclosing their routing policies due to various reasons such as business relationships, such as peering arrangements [30], or security concerns, such as BGP blackholing [44]. As a result, previous studies that assess ROV status have not cross-validated their findings with network operators.[5] We now attempt to validate our results with four difference sources.

Network operators' official announcements: We observe that certain network operators publicly announce their ROV deployment through channels such as social media platforms (e.g., Twitter), official blog posts, or mailing lists (e.g., nanog). To gather this information, we utilize the archive of the nanog mailing list and engage with network operators on the RPKI community discord channel [64]. As a result, we collect information from 40 ASes, including 38 ASes that have announced their implementation of ROV and 2 ASes that have announced their non-implementation of ROV. The complete list can be found in Appendix B.

Comparing these announcements with the corresponding ROV scores obtained from RoVista in our latest scan, we make several observations. Firstly, we discovered that among the 38 ASes claiming ROV deployment, 34 of them achieved a perfect ROV score of 100%. Additionally, one AS achieved a ROV score of 92.5%. However, it is important to note that not all of these ASes consistently maintain a 100% score throughout our measurement period; for instance, RETN (AS 9002) experiences variations in its ROV score We revisit them in §7.6 to discuss the challenges associated with their ROV implementation.

Secondly, interestingly, we observe that the ROV scores of the remaining three ASes claiming ROV deployment, BIT (AS 12859), Gigabit ApS (AS 60876), and Dhiraagu (AS 7642), are consistently zero.

To understand this discrepancy, we reached out to the network operators; unfortunately, we received only one response from BIT [14], who informed us that although they initially enabled ROV in early 2018 [2], they encountered an outage in the same year due to a bug in Juniper routers [3]. The bug caused the routing protocol daemon (RPD) to crash during ROV implementation, leading them to retract ROV from their entire network. This suggests that network operators may face challenges in implementing ROV due to equipment issues, which we will further investigate in §7.6.

Lastly, for the two ASes that claim non-deployment of ROV, we confirm that their ROV score is indeed zero.

[5] A recent study [18] attempted to validate their results using Cloudflare's list, which we have identified as inaccurate. We will discuss this further in Section 8.

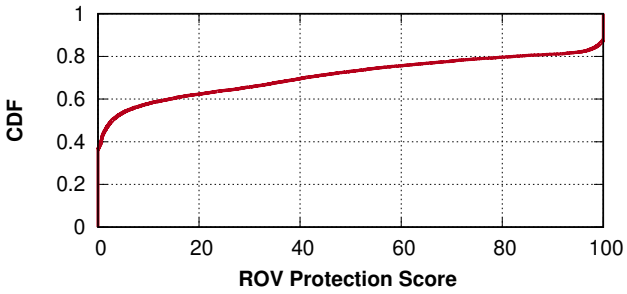


Figure 5: CDF of the percentage of the latest ROV score of ASes captured by RoVista.

Network Operators Survey: We collaborated with Mutually Agreed Norms for Routing Security (MANRS) [49] to conduct surveys of participants.Out of the 31 network operators that we received responses from, RoVista captured 22 (71.0%) of them. Among the captured operators, 13 (37.2%) confirmed deploying ROV and achieved a perfect ROV score on RoVista. For the 4 network operators who were uncertain about their ROV deployment, three had a ROV score of 0% while one scored 100%. Five network operators stated that they have not deployed ROV; four of their ROV scores are zero, but interestingly, RoVista finds that one of them (AS 1403) achieves 100% ROV score. Upon investigating their providers, AS 1403 is found to have two providers (AS 6453 and 174), both of which had a 100% ROV score. This suggests that they may not be reaching RPKI-invalid prefixes, as these prefixes are likely being filtered by the providers. We will delve into this phenomenon in detail in the upcoming section.

Personal communication: We launched our website (https://rovista.netsecurelab.org/) that publishes the ROV score for ASes on a daily basis. We have been contacted by 10 network operators[6] through email and RPKI Discord channel. Among the contacted network operators, only one, Charter (AS11351), reported an inconsistency. They claimed to have deployed ROV, while RoVista indicated a ROV score lower than 50%; upon further investigation, we provided them with the details of the tested tNodes and vVPs, and they acknowledged that they had missed ROV deployment for some of their peering routers.

For the remaining 9 network operators, they confirmed our findings; among them 7 operators claimed to have deployed ROV and RoVista finds that 5 network operators consistently achieved a 100% ROV score during our measurement period. For the other two network operators, NTT (AS 2914) and AT&T (AS 7018) whose ROV scores were not always at 100%, we will discuss these cases in detail in §7.6.

6.4 Limitation

RoVista has several limitations. We wish to discuss them explicitly before presenting our analysis. First of all, RoVista is unable to measure the ROV protection score of Internet exchange points (IXPs) such as DE-CIX [12] since it is not feasible to find vVPs within IXPs. Second, RoVista relies on hosts that announce RPKI-invalid prefixes (i.e., tNodes), which are collected from public BGP collectors (e.g., RouteViews [70]), which known as having a limited coverage [80]. Third, as ROV deployment becomes more widespread, the number of observable tNodes is likely to decrease; this can pose challenges in utilizing our approach effectively. Lastly, the ROV protection score of an AS does not directly indicate the ROV *deployment* status of that AS. This is primarily due to the methodology employed by RoVista, which relies on data plane measurements using TCP packets, while the actual ROV decision is made in the control plane. Thus, it is possible that an AS that has deployed ROV may exhibit a relatively low ROV protection score due to the nature of complex BGP routing such as collateral damage [32], default route problems, or prefer-valid policies, which will be discussed later.

[6]ATT (AS7018), Comcast (AS7922), Seacom (AS37100), Colt (AS8820), IIJ (AS2497), NTT (AS2914), Swisscom (AS3303), Charter (AS11351), BIT (AS12859), and ZAYO (AS6461)

7 ANALYSIS

7.1 The state of ROV

In this subsection, we analyze the current state of ROV and its evolution over time. In Figure 5, we present the distribution of latest ROV scores for all ASes captured by RoVista. We make a number of observations; Firstly, we notice that out of 28,314 ASes, 10,249 (36.2%) consistently have a 0% ROV score, indicating that they do not *implement* ROV and are therefore more vulnerable to BGP hijacking attacks. Conversely, we find that 3,482 (12.3%) consistently achieve a 100% ROV score, indicating full ROV protection.

Interestingly, the remaining 14,583 (51.5%) fall into the category of reaching some, but not all, tNodes, which could be due to two reasons; firstly, the ROV policy can be applied differently depending on the source of BGP announcements, determined by AS relationships. For instance, some ASes accept RPKI-invalid route announcements from their customers [35]. Moreover, customized lists like SLURM [43] can be used to define ROV policies that allow routes even if they are RPKI invalid. Additionally, certain ASes may encounter challenges in their ROV deployments due to equipment issues [16], which will be further examined in the following section.

Rank	ASN	ISP	ROV ratio
1	3356	Level 3 Parent, LLC	100.00%
2	1299	Telia Company AB	100.00%
3	174	Cogent Communications	100.00%
4	3257	GTT Communications Inc.	100.00%
6	2914	NTT America, Inc.	100.00%
8	6461	Zayo Bandwidth	100.00%
9	6453	TATA Communications	100.00%
10	3491	PCCW Global, Inc.	100.00%
14	5511	Orange S.A.	100.00%
15	12956	Telefonica Global Solutions	100.00%
18	701	Verizon	94.44%
21	7018	AT&T Services, Inc.	100.00%
22	3320	Deutsche Telekom AG	0.00%
31	6830	Liberty Global B.V.	100.00%
32	1239	Sprint	100.00%
36	209	CenturyLink Communications, LLC	100.00%
72	2828	Verizon	94.44%

Table 1: The ROV ratio for 17 Tier-1 ASes as of September 12th, 2023.

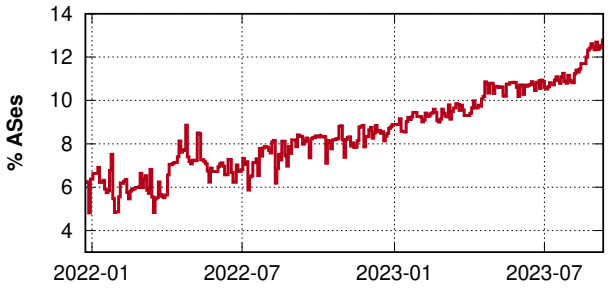


Figure 6: The overall percentage of ASes with an ROV score of 100% over time.

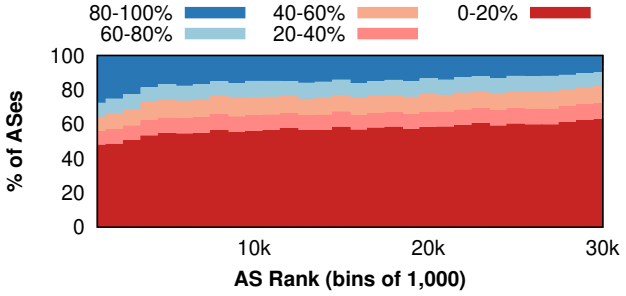


Figure 7: Higher ranked ASes tend to have higher ROV scores.

Secondly, even ASes that do not directly implement ROV might be fully protected if all their transit providers have deployed ROV [47]; this phenomenon, known as collateral benefit, arises when ROV-deployed ASes filter out RPKI-invalid prefixes and prevent the propagation of such BGP announcements to their customers [32]. Thus, it is crucial for large network operators, including tier-1 ASes to perform ROV. Table 1 shows the ROV score for 17 tier-1 ASes[7] and we observe that 16 (94.1%) of them have a 100% ROV score. These networks are the most central in interdomain routing, so a large deployment here is important for the state of ROV of the Internet as a whole.

Figure 6 shows the percentage of ASes of which ROV score is 100% during our measurement period. One key observation is that ROV protection is not rare anymore: at the beginning of our measurement, we find that 6.3% of ASes is ROV protected in December 2021, and it increased to 12.3% in September 2023. This is encouraging compared to other proposed routing security protocols that suffered from their low deployment rate such as BGPsec [31].

7.2 ROV score vs. ASRank

Now we examine the relationship between the ROV score and the ranking of ASes, which is determined by its customer cone size [40]. Figure 7 shows the fraction of ASes with a different range of ROV scores for top 30K ASes. First, we immediately notice that bigger ASes are more likely to have a higher ROV score, which is encouraging; for example, 25% of the 1,000 biggest ASes can filter more than 80% of tNodes. In contrast, we see more ASes with low ROV scores (i.e., 0 – 20%) as their rankings decrease. We believe these the ASes with such low ROV scores do not implement ROV themselves; considering that they are still able to filter some RPKI-invalid prefixes, it suggests that such filtering could be due to their providers who implement ROV (i.e., collateral benefit).

We will dig deeper and attempt to measure the impact and challenges of collateral benefit in the following section.

7.3 Case study: collateral benefit

As mentioned earlier, the deployment of ROV by ASes can provide benefits to their customers or peers through in-path filtering. However, measuring the actual impact of this filtering in a real-world setting is challenging as it requires longitudinal measurements of ROV across numerous ASes.

Using RoVista, we identify 92 ASes whose ROV protection scores jumped from 0% to 100% on 17 different dates simultaneously. Interestingly, among each of the ASNs that exhibit synchronous behavior on a given date, we discover that 17 of them serve as a provider for some of the other ASes, which may suggest that the customer ASes are RPKI-protected as a result of their provider ASes' ROV deployment.

Among them, we find two large ASes for which we are able to cross-validate their ROV deployment: Orange (AS 5511) [55] and KPN (AS 1136) [67].

Orange (AS 5511): Orange announced its ROV deployment on June 27th, 2022 [55]. However, RoVista identifies that Orange (AS 5511) has been a 100% score since June 6th, 2022, which may suggest that they may have deployed and tested ROV prior to making the official announcement. We observe that the ROV scores of 20 other ASes, who are Orange's customers, also jumped up to 100% on the same date.

KPN (AS 1136): KPN (AS 1136), a large dutch ISP, announced its ROV deployment [67] on March 16th, 2022, but RoVista finds that the ROV score of KPN jumps up from 0% to 100% on March 14th, 2022 before its announcements. During our measurement period, RoVista captured the ROV score of KPN and its six customers as shown in Figure 8. However, we discovered that not all of them benefited from KPN's ROV deployment. Four of their customers (AS 8694, 8737, 21286, and 28685) also simultaneously achieved a 100% ROV score while the remaining two customers (AS 3573 and 15466) did not experience any change in their ROV scores. Analyzing their connections to other ASes using BGP datasets and AS relationships, we made several observations.

Firstly, the four ASes that exhibited synchronized behavior are stub networks without any upstream links other than KPN, which explains their consistent ROV score alignment. Secondly, AS 3573 is connected to 41 other providers, out of which 23 had a 0% ROV score. This may have enbled AS 3573 to reroute through these providers, bypassing the ROV deployment of KPN, and maintain its original ROV score.

Similarly, AS 15466 had an additional provider, AS 5400, whose ROV score remained consistently at 0% throughout the measurement period. This allowed AS 15466 to continue reaching tNodes through AS 5400, unaffected by the ROV deployment of its primary

[7] We refer to them as the ones that are connected to each other (i.e., clique) and transit free [40].

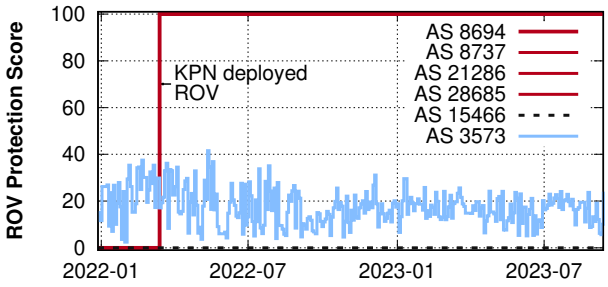


Figure 8: ROV scores of KPN and its customers

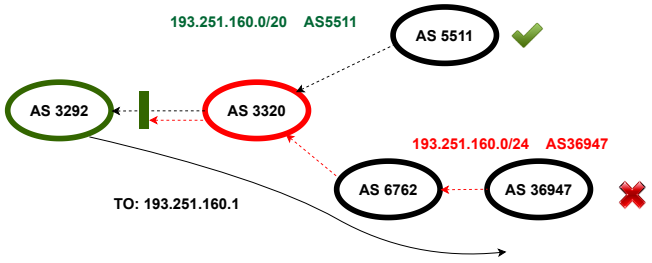


Figure 9: Collateral damage on AS 3292; ROV scores of AS 3292 and 3320 are 92.1% and 0% respectively.

AS (KPN). It is noteworthy that AS 8694, which demonstrated synchronized behavior, has an additional provider, AS 36332, with a 100% ROV score. This allowed AS 8694 to reach tNodes through KPN until the deployment of ROV by KPN.

These findings emphasize that networks with multiple upstreams may not gain collateral benefit if some of these upstreams do not perform ROV.

7.4 Case study: collateral damage

We have seen that a provider AS that deploys ROV can yield collateral benefit to its customers. However, less obviously, a provider AS that does not deploy ROV can cause collateral damage to its customers even if they do.

For example, AS 3292 (TDC A/S) announced their ROV deployment on February 21st, 2021 [84]; however, RoVista finds that they can constantly reach three tNodes, making their ROV score be 92.1%. To deep investigate this phenomenon, we utilize the traceroute results discussed in §6.3.1 to gain insights into the paths taken to reach the three tNodes. Our observations shed light on the situation.

First, we find that all of their traceroute results other than three tNodes are terminated internally, making them unable to reach the tNodes, which confirms their ROV deployment. *Secondly*, among the successful traceroute results to the tNodes, two of them are forwarded to AS 3320 (Deutsche Telekom), *which has a 0% ROV score.* To understand this behavior, we examine the corresponding BGP announcements in RouteViews and analyzed why TDC (AS 3292) still has a route towards these tNodes. Figure 9 summarizes our findings; first, we notice that AS 3320 receives two announcements, one of which is 193.251.160.0/24 originated from AS 36947 (RPKI-invalid), and the other is 193.251.160.0/20 originated from AS 5511 (RPKI-valid). Since it does not perform ROV, it will add both entries to its routing table and also forward them to AS 3292:

```
193.251.160.0/20 AS5511
193.251.160.0/24 AS6762, AS36947
```

AS 3292 filters RPKI-invalid announcement, thus it only keeps the valid one and adds it to its BGP table.

```
193.251.160.0/20 AS3320, AS5511
```

When a probe in AS 3292 sends a packet to 193.251.160.1, the AS finds the matched entry, 193.251.160.0/20, and forwards it to AS 3320. However, AS 3320 finds two matches in its BGP table, thus it chooses the *most specific* entry, 193.251.160.0/24, which is RPKI-invalid, ultimately letting AS 3292 reach to the invalid origin.

This observation highlights that even ASes that deploy ROV can remain vulnerable to BGP hijacking attacks when their transit providers or peers do not implement ROV. Therefore, it is crucial for larger ASNs to consider deploying ROV not only for their own networks but also to protect the interests of their customers. To systematically identify ASes exposed to collateral damages, we conduct the following steps along with traceroute experiments:

(a) We examine whether all successful traceroute results of an AS passed through an AS with a 0% ROV score as the next hop.
(b) We find if there are RPKI-valid or unknown IP prefixes available in the RouteViews BGP table datasets that cover the IP prefixes of tNodes.
(c) We then check whether the IP prefixes are announced through the AS.

By following this procedure, we discover six ASes[8] and find that their ROV score is greater than 90% but can reach some RPKI-invalid prefixes.

Considering that the collateral damage can occur *even to ASes that correctly deploy ROV*. This presents a significant challenge for these ASes since it is more challenging from them to notice and fix it because it totally depends on the ROV policy of their upstream ASes.

7.5 Case study: BGPStream

We now evaluate the impact of ROV using historical BGP hijacking reports collected from BGPStream [13], which detects hijacking attempts [54] by monitoring the real time BGP announcements from multiple datasets such as RouteViews [70] or RIPE RIS [63]. We utilize the APIs of BGP hijack detection systems to collect reports on BGP hijacking attacks during our measurement period. These reports provide valuable information, including the time of detection, hijacked IP prefixes, authorized AS to announce them, and the attacking AS.

With a total of 1,277 collected IPv4 hijack reports, we perform the following analysis. First, we match the reports with BGP announcements from RouteViews to obtain the routing path using the `AS-PATH` attribute. Next, we check if the announced IP prefixes are covered by at least one VRP.

[8] IUCC (AS 378), Compass (AS 9245), NTS workspace (AS 15576), TrustPower (AS 55850), SGN (AS 12778), ARSAT (AS 52361)

Out of the 1,277 reports, we find that 179 (14%) are RPKI-covered. Among these reports, we are able to capture the ROV score of at least one AS on the AS-PATH in 161 (89.9%) reports, and all ASes in 124 (69.2%) reports.

Among the 124 reports with complete ROV score information, *only 5 (4.0%) involve ASes with a ROV score higher than 90%*. Remarkably, all of these 5 reports are due to the customers of those ASes forwarding invalid BGP announcements to them, indicating that these ASes do not filter RPKI-invalid prefixes propagated by their customers. On the other hand, all ASes in the remaining 119 reports have a zero ROV score, suggesting that the attacks may not have occured if these ASes had deployed ROV.

For the other 1,098 hijacked prefixes not covered by ROAs, we capture the ROV scores of all ASes on the AS-PATH for 884 (80.5%) of them. Surprisingly, 204 of these prefixes (23.1%) involve at least one AS with a ROV score higher than 90%. *This suggests that these attacks could have been prevented if the owners of the prefixes had registered ROAs.*

Taken together, our findings highlight that network operators should consider deploying ROV and registering ROAs for their IP prefixes. Despite a previous study showing a lack of interest in deploying both ROAs and ROV among network practitioners [32], our results emphasize the importance of these measures in enhancing the security of BGP routing.

7.6 Challenges to achieving a 100% ROV protection score

As shown in Figure 5, we observe that 1,592 ASes (5.8%) where their ROV score is greater than 90%, but not 100%. To gain insights into this phenomenon, we leverage RIPE Atlas probes located within these ASes and analyze the traceroute results towards each tNode obtained from 6.3. Additionally, we also reach out to network operators through MANRS [49], RIPE NCC, and the RPKI community discord channel [64] to better understand their ROV policy. Through these efforts, we have identified three key challenges to achieving a 100% ROV score:

ROV exemption for the routes from customers: Certain ASes choose not to implement ROV for routes received from their customers. This decision is often driven by the concern that filtering RPKI-invalid prefixes forwarded by their customers could have a negative impact on their profitability.

We first identify these ASes by using traceroute results; among the 3,523 ASes of which ROV score is greater than 90%, we are able to measure 362 ASes from RIPE Atlas probes. Among these, we focus on the ASes that have at least one successful traceroute result towards tNodes, leaving us with 73 ASes. We then identify the ASes where all of the first hops in the traceroutes belong to their customers by analyzing the CAIDA AS relationship datasets, which reveals four ASes: AT&T (AS 7018), Cogent (AS 174), ARNES (AS 2107), and Forthnet (AS 1241); among them, we are able to confirm our findings through communication with AT&T [4].

Default route: ASes that have implemented ROV can still reach RPKI-invalid prefixes if they have set a default route to a non-validating network. This means that all traffic destined for RPKI-invalid prefixes can be forwarded to the default route, which points to an AS that does not deploy ROV. To identify such ASes, we also analyze the ASes with a ROV score higher than 90% and specifically look for ASes where all successful traceroutes towards tNodes are routed through a single AS as their first hop, which is not their customer.

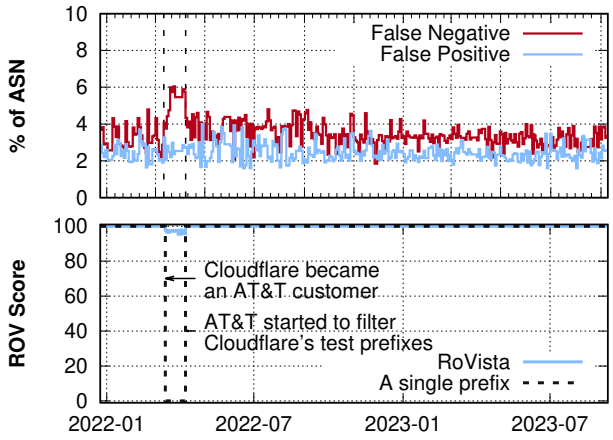


Figure 10: The false positive and negative ratio of a single RPKI-invalid prefix based measurement (top) and the ROV score of AT&T over time (bottom).

We discover 5 ASes that fulfill these conditions: Swisscom (AS 3320), Telenet BVBA (AS 3303) to AS 6830, Pe3nyNet (AS 48926), Planetel SPA (AS 47217), Libatech (AS 60999), all of which first hops towards the tNodes are Deutsche Telekom (AS 3320), Liberty Global (AS 6830), Quantcom (AS 29208), Aruba (AS 31034), and Orange (AS 5511), respectively. We reached out to Swisscom (AS 3303) [74] and confirmed that this issue arose from a misconfigured default route due to on-ramp tunnels for DDoS mitigation [20], which enabled reachability for invalid prefixes while they were dropped at the edge routers. They fixed the issue after our report.

Equipment and other technical issues: Through the communication with network operators, we have learned that some of them have disabled ROV due to their hardware issues; for example, we find that NTT (AS 2914) shows 94.7% of ROV score on average during our measurement period. From the conversation, we were informed that NTT deployed ROV in their network in March 2021, but still propagates a number of RPKI-invalid prefixes due to the router vendors that do not appropriately support ROV due to the routers that do not support ROV causing approximately 900 RPKI-invalid being propagated through them [53].

8 COMPARISON WITH OTHER APPROACHES

In this section, we compare RoVista with other popular approaches that measure the ROV status of ASes.

Single RPKI-invalid prefix based measurement: As discussed in §2.3, there have been many studies that measure ROV status of ASes by using RPKI-invalid test prefixes such as Cloudflare's `isbgpsafeyet.com`. While this approach is simple and effective, it may be inaccurate when an AS performs ROV differently depending on IP prefixes.

To explore the discrepancy between a single-prefix based approach and RoVista, we use Cloudflare's test RPKI-invalid prefix, `103.21.244.0/24` to simulate their results. We begin by confirming that two tNodes share the same IP addresses as those used in `isbgpsafeyet.com` so that we can simulate their results. Similar to how `isbgpsafeyet.com` determines the ROV status of an AS, we define an AS as `safe` if all vVPs within the AS cannot reach both tNodes, and `unsafe` if all vVPs within the AS can reach them; All vVPs within the same AS consistently exhibit reachability towards both tNodes.

We then classify an AS as a false negative when the single-prefix measurement labels it as `unsafe`, but RoVista determines its ROV score to be above 90% to ensure a conservative threshold. We also consider an AS to be a false positive if it is classified as `safe` but RoVista identifies its ROV score as 0%. We apply this throughout the measurement period and Figure 10 (top) presents the results. We notice that there is an average of 2.5% false positives and 3.8% false negatives, with a rapid increase occurring after March 14th, 2022. This is mainly because of AT&T (AS 7018), one of the tier-1 ASes, of which ROV score decreases from 100% to 97.8% on the same date (bottom). Upon contacting AT&T [4], we learned that (1) AT&T does not filter RPKI-invalid prefixes on customer connections, and (2) Cloudflare became a customer of AT&T in March 2022, resulting in their test IP prefix not being filtered by AT&T.

As a consequence, all ASes connected to AT&T became capable of reaching the Cloudflare's test prefix, leading to their classification as `unsafe`.

APNIC RPKI dashboard: APNIC maintains a RPKI dashboard [34] that shows the ROV status of ASes. Their approach is similar to Cloudflare's `isbgpsafeyet.com`, in which they run two prefixes, one of which is the Cloudflare's RPKI-invalid IP prefix. However, APNIC leverages the Google advertisement network to recruit vantage points.

The dashboard calculates the *ROV filtering percentage*, which represents the percentage of *clients* unable to fetch content served from the RPKI-invalid prefix. In contrast, our RoVista's ROV protection score measures the fraction of RPKI-invalid prefixes that an AS cannot reach, making a direct comparison challenging. Although the APNIC dashboard covers 45,372 ASes, including those with only one client measured, we find that 22,169 ASes can be captured by RoVista. Consequently, we discovered that the APNIC dashboard also encounters the same issue we described earlier; we observed that the *ROV filtering percentage* of AT&T dropped to 0% on March 14th; we promptly informed APNIC and AT&T of our findings on April 4th, 2022 [66], leading AT&T to begin filtering Cloudflare's test IP prefixes on April 20th, 2022, in order to avoid such misclassifications.

Nevertheless, these results show that relying on a single or two IP prefixes to assess an AS's RPKI status can result in incorrect determinations. Consequently, concerns about the accuracy of these methods have been raised in several reports [21, 83].

Cloudflare's list: Cloudflare also manages a crowdsourced list of network operators and their ROV status [33]. This allows anyone to contribute by submitting a pull request that includes an AS number, the ROV status (classified as `safe`, `partially safe`, or `unsafe`), and a reference (e.g., a screenshot from isbgpsafeyet.com or a news article). At the time of writing, the list contains 402 ASes, 327 (81.3%) of which are captured by RoVista; Among them, 78 are marked as `safe`, 52 as `partially safe`, and 208 as `unsafe`. We now compare each of them with the ROV scores. Figure 11 shows their distribution and we make a number of observations.

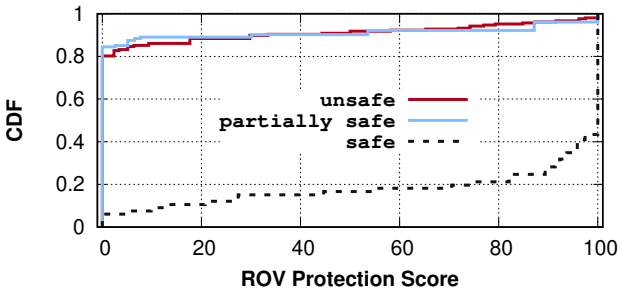


Figure 11: ROV scores of ASes in Cloudflare's list.

First, among the 67 `safe` ASes, 36 of them (53%) have a 100% ROV score. This includes seven tier-1 ASes in Table 1. However, it is worth noting that there are still 11 (16%) ASes with a ROV score below 50%, such as BIT (AS 12859) and Swisscom (AS 3303) that we have discussed in §7.6.

166 (80%) of the `unsafe` ASes have a zero ROV score, which is expected; however, there are also ASes with a 100% ROV score within the `unsafe` category, such as KPN (AS 1136) and Orange (AS 5511), which have recently enabled ROV. We also find that 44 (88%) of the `partially safe` ASes have a ROV score of zero.

We believe the disparities largely stem from (1) outdated reports, as seen with BIT (AS 12859), and (2) the limitations of measuring a single IP prefix. Overall, our results highlight the challenges of accurately measuring and tracking the ROV status of network operators.

rpki.exposed spreadsheet: `rpki.exposed` [67] is a spreadsheet that network operators collectively manage. It lists a number of network operators that has deployed ROV along with their ASN; 24 ISPs identify themselves as performing ROV as of the writing. Among them, RoVista can capture the ROV policy of 19 (79.1%) ASes; 18 ASes have a ROV score higher than 90%. The other inconsistent AS is BIT (AS 12859) that retracted ROV deployment in early 2018 as described in §6.3; this also highlights a challenge of crowd-sourced lists, which may not always be promptly updated.

9 CONCLUSION

In this paper, we introduced RoVista, a scalable measurement platform that assesses the ROV protection status of ASes without requiring IP prefixes for control or recruiting vantage points. We observed that ASes with a perfect ROV protection score is not rare anymore, currently accounting for more than 12.3% of ASes. However, this number is growing over time, especially among higher-ranked ASes.

Through our longitudinal measurement, we discovered empirical evidences of both collateral benefits and damages associated with ROV deployment. We emphasize the importance of higher-ranked

ASes adopting ROV to have a larger global impact (collateral benefit), while also cautioning network operators to implement ROV to protect against collateral damages. Furthermore, we highlighted the challenges faced by network operators in managing ROV correctly. We compared RoVista with several popular ROV measurement platforms and discussed their limitations.

Our findings underscore the necessity of continuous auditing of ROV deployments and the importance of effective management by network operators.

ACKNOWLEDGMENT

We extend our heartfelt gratitude to the anonymous reviewers and our shepherd, Stephen McQuistin, for their invaluable insights. We also deeply appreciate the contributions of Ties de Kock and Robbie Mitchell. Special thanks to Tony Tauber (Comcast), Martin Mckee (Verizon), Blake Willis (Zayo), and Rob Robertson (Zayo), as well as the network operators who took part in our survey, lending further credibility to our findings. We are indebted to the Internet Society and the MANRS Mentors and Ambassador program for their constructive feedback and unwavering support. Lastly, our appreciation is directed to RIPE NCC for the generous provision of RIPE Atlas probe credits. This research was supported in part by NSF grant CNS-2247306, Comcast Innovation Fund, and Commonwealth Cyber Initiative.

REFERENCES

[1] Abuse.ch Feodo Tracker. https://feodotracker.abuse.ch/.
[2] Registratie van RPKI-informatie voor een veilige routering. https://www.bit.nl/news/2081/88/Registratie-van-RPKI-informatie-voor-een-veilige-routering.
[3] 16.2R2-S9: Software Release Notification for Junos Software Service Release version 16.2R2-S9. https://supportportal.juniper.net/s/article/16-2R2-S9-Software-Release-Notification-for-Junos-Software-Service-Release-version-16-2R2-S9?language=en_US.
[4] AT&T (AS 7018). Personal Communication.
[5] H. Ballani, P. Francis, and X. Zhang. A study of prefix hijacking and interception in the internet. *SIGCOMM*, 2007.
[6] J. Borkenhagen. AT&T/AS 7018 Now Drops Invalid Prefixes from Peers. https://mailman.nanog.org/pipermail/nanog/2019-February/099501.html, 2019.
[7] K. Butler, T. R. Farley, P. McDaniel, and J. Rexford. A survey of BGP security issues and solutions. *Proceedings of the IEEE*, 98(1), IEEE, 2010.
[8] R. Bush and R. Austein. The Resource Public Key Infrastructure (RPKI) to Router Protocol. RFC 6810, IETF, 2013.
[9] R. Bush and R. Austein. https://tools.ietf.org/html/rfc8210. RFC 8210, IETF, 2017.
[10] R. Brandom. Hackers emptied Ethereum wallets by breaking the basic infrastructure of the internet. 2018. https://www.theverge.com/2018/4/24/17275982/myetherwallet-hack-bgp-dns-hijacking-stolen-ethereum.
[11] S. Bisgaard and M. Kulahci. *Time Series Analysis and Forecasting by Example*. Wiley, 2011.
[12] BGP Announcement Filtering – Extract from the route server guides. https://www.de-cix.net/en/about-de-cix/news/insights-how-and-what-the-de-cix-route-servers-filter.
[13] BGPStream. https://bgpstream.com/.
[14] BIT (AS12859). Personal Communication.
[15] J. Cowie. China's 18-Minute Mystery. 2010. https://dyn.com/blog/chinas-18-minute-mystery/.
[16] M. Candela. A One-Year Review of RPKI Operations. https://ripe84.ripe.net/archives/video/741/.
[17] T. Chung, E. Aben, T. Bruijnzeels, B. Chandrasekaran, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, R. van Rijswijk-Deij, J. P. Rula, and N. Sullivan. RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins. *IMC*, 2019.
[18] W. Chen, Z. Wang, D. Han, C. Duan, X. Yin, J. Yang, and X. Shi. ROV-MI: Large-Scale, Accurate and Efficient Measurement of ROV Deployment. *NDSS*, 2022.
[19] B. Cartwright-Cox. Measuring RPKI Adoption via the data-plane. NLNOG Day 2018. https://nlnog.net/static/nlnogday2018/8_Measuring_RPKI_ben_NLNOG_2018.pdf.
[20] Chapter: Implementing Cisco ASR 9000 vDDoS Mitigation. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-5/system-security/configuration/guide/b-system-security-cg-asr9000-65x/b-system-security-cg-asr9000-65x_chapter_01110.html.
[21] Cogent RPKI invalid filtering. https://lists.archive.carbon60.com/nanog/users/216856.
[22] Comcast (AS 7922). Personal Communication.
[23] B. DU, C. Testart, R. Fontugne, G. Akiwate, A. C. Snoeren, and K. Claffy. Mind your MANRS: measuring the MANRS ecosystem. *Proceedings of the 22nd ACM Internet Measurement Conference*, 2022.
[24] D. Dittrich and E. Kenneally. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. 2012. https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf.
[25] T. Dai and H. Shulman. SMap: Internet-wide Scanning for Spoofing. *ACSAC*, IEEE Computer Society, 2021.
[26] Z. Durumeric, E. Wustrow, and J. A. Halderman. ZMap: Fast Internet-Wide Scanning and its Security Applications. *USENIX Security*, 2013.
[27] Deutsche Telekom Non-ROV. https://twitter.com/deutschetelekom/status/1252177058555473920.
[28] R. Ensafi, J. Knockel, G. Alexander, and J. R. Crandall. Detecting Intentional Packet Drops on the Internet via TCP/IP Side Channels. *PAM*, 2014.
[29] W. A. Fuller. *Introduction to statistical time series*. John Wiley & Sons, 2009.
[30] L. Gao. On inferring autonomous system relationships in the Internet. *IEEE/ACM Transactions on networking*, 9(6), IEEE, 2001.
[31] W. George and S. Murphy. https://tools.ietf.org/html/rfc8206. RFC 8206, IETF, 2017.
[32] Y. Gilad, A. Cohen, A. Herzberg, M. Schapira, and H. Shulman. Are We There Yet? On RPKI's Deployment and Security. *NDSS*, 2017.
[33] Github: Cloudflare repository. https://github.com/cloudflare/isbgpsafeyet.com/tree/master/data.
[34] G. Huston and J. Damas. Measuring Route Origin Validation. 2020. https://www.potaroo.net/ispcol/2020-06/rov.html.
[35] T. Hori. IIJ's Efforts with RPKI. https://www.iij.ad.jp/en/dev/iir/pdf/iir_vol50_focus1_EN.pdf.
[36] Improved BGP Routing Security Adds Another Important Layer of Protection to Online Networks. https://corporate.comcast.com/stories/improved-bgp-routing-security-adds-another-layer-of-protection-to-network.
[37] Is BGP Safe Yet? https://isbgpsafeyet.com/.

[38] C. Lynn, J. Mikkelson, and K. Seo. Secure BGP (S-BGP). IETF, 2003.
[39] M. Lepinski and S. Kent. An Infrastructure to Support Secure Internet Routing. RFC 6480, IETF, 2012.
[40] M. Luckie, B. Huffaker, K. Claffy, A. Dhamdhere, and V. Giotsas. AS Relationships, Customer Cones, and Validation. *IMC*, 2013.
[41] Level3. Level3/AS 7018 Now Drops Invalid Prefixes from Peers and Customers. https://twitter.com/lumentechco/status/1374035675742412800, 2021.
[42] A. Medina. CenturyLink / Level 3 Outage Analysis. 2020. https://www.thousandeyes.com/blog/centurylink-level-3-outage-analysis.
[43] D. Ma, D. Mandelberg, and T. Bruijnzeels. Simplified Local Internet Number Resource Management with the RPKI (SLURM). IETF, 2018.
[44] L. Miller and C. Pelsser. A taxonomy of attacks using bgp blackholing. *European Symposium on Research in Computer Security*, 2019.
[45] O. Moll. Border Gateway Protocol Hijacking - Examples and Solutions. 2020. https://www.anapaya.net/blog/border-gateway-protocol-hijacking-examples-and-solutions.
[46] P. Mohapatra, J. Scudder, D. Ward, R. Bush, and R. Austein. BGP Prefix Origin Validation. RFC 6811, IETF, 2013.
[47] R. Morillo, J. Furuness, C. Morris, J. Breslin, A. Herzberg, and B. Wang. ROV++: Improved Deployable Defense against BGP Hijacking. *NDSS*, 2021.
[48] S. Mongkolluksamee, K. Fukuda, and P. Pongpaibool. Counting NATted hosts by observing TCP/IP field behaviors. *IEEE ICC*, 2012.
[49] MANRS for Network Operators. 2021. https://www.manrs.org/netops/network-operator-actions/.
[50] MANRS. MANRS Observatory. https://observatory.manrs.org/.
[51] Microsoft introduces steps to improve internet routing security. https://azure.microsoft.com/en-us/blog/microsoft-introduces-steps-to-improve-internet-routing-security/.
[52] Netflix (AS2906) Route Object Authorization. https://bgp.he.net/AS2906#_prefixes.
[53] NTT. Routing Registry. https://www.gin.ntt.net/support-center/policies-procedures/routing-registry/#RPKI.
[54] C. Orsini, A. King, D. Giordano, V. Giotsas, and A. Dainotti. BGPStream: A Software Framework for Live and Historical BGP Data Analysis. *IMC*, 2016.
[55] Orange International Carriers — RPKI validation. https://twitter.com/OrangeIC/status/1541436188241891328.
[56] J. Postel. Internet Protocol. RFC 791, IETF, 1981.
[57] P. Pearce, R. Ensafi, F. Li, N. Feamster, and V. Paxson. Augur: Internet-Wide Detection of Connectivity Disruptions. *IEEE S&P*, 2017.
[58] V. Paxson, M. Allman, J. Chu, and M. Sargent. Computing TCP's Retransmission Timer. RFC 6298, IETF, 2011. http://www.ietf.org/rfc/rfc6298.txt.
[59] A. Reuter, R. Bush, I. Cunha, E. Katz-Bassett, T. C. Schmidt, and M. Whlisch. Towards a Rigorous Methodology for Measuring Adoption of RPKI Route Validation and Filtering. *CCR*, 48(1), 2018.
[60] N. Rodday, I. Cunha, R. Bush, E. Katz-Bassett, G. D. Rodosek, T. C. Schmidt, and M. Wählisch. Revisiting RPKI Route Origin Validation on the Data Plane. *TMA*, 2021.
[61] RIPE Atlas. https://atlas.ripe.net/.
[62] RIPE NCC Annual Report 2015. https://www.ripe.net/publications/docs/ripe-665.
[63] RIPE Routing Information Service (RIS). http://www.ripe.net/projects/ris/rawdata.html.
[64] RPKI Community Discord. https://discord.gg/WaPgs8vEKy.
[65] RPKI Deployment Monitor. https://rpki-monitor.antd.nist.gov.
[66] RPKI I-ROV Per-Country filtering for AS7018: ATT-INTERNET4, United States of America (US). https://stats.labs.apnic.net/rpki/AS7018.
[67] RPKI deployment state: rpki.exposed. https://docs.google.com/spreadsheets/d/1qduCCF_p-czzFr9N-5STh3-NNAxyrYjECRwtgULR2c0.
[68] Rapid7 SSL Certificate Scans. https://scans.io/study/sonar.ssl.
[69] RIPE. RPKI Test. https://www.ripe.net/s/rpki-test/.
[70] University of Oregon RouteViews project. http://www.routeviews.org/.
[71] Routinator. https://nlnetlabs.nl/projects/rpki/routinator/.
[72] A. Siddiqui. A Major BGP Hijack by AS55410-Vodafone Idea Ltd. 2020. https://www.manrs.org/2021/04/a-major-bgp-hijack-by-as55410-vodafone-idea-ltd/.
[73] M. Salganik. Bit by Bit: Social Research for the Digital Age. 2016.
[74] Swisscomm (AS3033). Personal Communication.
[75] C. Testart, P. Richter, A. King, A. Dainotti, and D. Clark. To Filter or not to Filter: Measuring the Benefits of Registering in the RPKI Today. *PAM*, 2018.
[76] H. Tomas, H. Amir, S. Haya, and W. Michael. Practical experience: Methodologies for measuring route origin validation. *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2018.
[77] L. Tung. iCloud goes down: Apple joins the Google, Facebook, Cloudflare cloud outage club. 2019. https://www.zdnet.com/article/icloud-goes-down-apple-joins-the-google-facebook-cloudflare-cloud-outage-club/.
[78] Telia (AS1299) announced ROV on June 10, 2021. https://www.arelion.com/our-network/bgp-routing/routing-security.html.
[79] The Spamhaus Project. https://www.spamhaus.org/.
[80] F. Wohlfart, N. Chatzis, C. Dabanoglu, G. Carle, and W. Willinger. Leveraging Interconnections for Performance: The Serving Infrastructure of a Large CDN. *SIGCOMM*, 2018.
[81] R. White. Architecture and Deployment Considerations for Secure Origin BGP (soBGP). IETF, 2006.
[82] YouTube Hijacking: A RIPE NCC RIS case study. 2008. https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study.
[83] "Is BGP safe yet?" test. https://seclists.org/nanog/2020/Apr/257.
[84] nielsfc: Rejecting invalids was fully implemented throughout the network February 24th 2021. https://github.com/cloudflare/isbgpsafeyet.com/pull/523.

APPENDIX

A MODELING IP-ID PATTERNS

IP-ID model: Similar to prior work [28], we model each time series using ARMA model. However, ARMA model can only be applied to stationary time series, where its statistical properties (e.g., mean) do not change over time. Thus ARMA model may not work well when the statistical properties of background traffic change over time. For time series with trend or with seasonality (e.g., the background

traffic that shows a specific pattern), we use ARIMA model instead, which suits for *nonstationary time series*.

To determine whether the observed time series traffic is stationary or not, we first apply Augmented Dickey Fuller (ADF) test [29] and then use ARMA model for stationary and ARIMA model for nonstationary time series. When a time series of observed background traffic before we send spoofing packet, $x_1, \ldots, x_t$, is determined as stationary, we can fit by ARMA(p, q) as

$$x_t = c + \sum_{t=1}^{p} \phi_t x_{t-p} + w_t + \sum_{t=1}^{q} \theta_t w_{t-q}$$

where w_t is the white noise, and $\phi_p, \theta_q \neq 0$ are constant parameters. On the other hand, when the time series is not stationary, it can be regarded as a combination of a nonstationary trend component and a zero-mean stationary component; then differencing the times series may lead to a stationary time series. Thus, we fit $x_1, \ldots, x_t$ by ARIMA(p, d, q), which is ARMA(p, q) by taking difference as:

$$(1-B)^d x_t = (1-B)^{d-1}(x_t - x_{t-1}) = \cdots$$

where B is the backshift operator (i.e., $B^k x_t = x_{t-k}$ for any positive integer k).

Detecting a spike: From the first 10 IP-ID values $x_1, \ldots, x_{10}$ from probing packets, we can predict the future background, $\hat{x}_{t+1}, \ldots, \hat{x}_{t+m}$, and estimate the variance of the noise at each time point as $\hat{\sigma}^2_{t+1}, \ldots, \hat{\sigma}^2_{t+m}$, where $t+m$ is the end time of the experiment. To detect the spike, we apply one-tailed hypothesis testing on observed IP-ID pattern $x_{t+1}, \ldots, x_{t+m}$ and detects a spike at time $t+k$ if the observed x_{t+k} is *significant larger than the predict background noise* $\hat{x}_{t+k}$.

To detect the spike, we consider the Z-score at time point $t+k$ defined as:

$$z_{t+k} := \frac{x_{t+k} - \hat{x}_{t+k}}{\hat{\sigma}_{t+k}},$$

for $k = 1, 2, \ldots, m$.

Since the spike can only increase the background traffic, we apply one-tailed hypothesis testing: for any confidence level $\alpha \in (0, 1)$, we consider the $1-\alpha$ quantile of the standard normal distribution and denote by t_α. For any $k = 1, 2, \ldots, m$, we reject the null hypothesis and conclude that there is a spike at time $t+k$ if $z_{t+k} > t_\alpha$. We then determine the filtering scenario based on what we mentioned in §4.3.

False positive and negative: Since we use Z-score and one-tailed hypothesis testing with a confidence level $\alpha \in (0, 1)$, the false positive rate is smaller than α asymptotically as long as the model assumptions hold; we use $\alpha = 0.05$ as typically chosen.

On the other hand, false negative (FN) happens when model failed detecting a spike. Let σ^2_{t+k} be the variance of x_{t+k} given data $x_1, \ldots, x_t$ and s be the actual value of the spike, the asymptotic false negative rate under the model assumptions will be:

$$\mathrm{P}(z_{t+k} \leq t_\alpha \mid s) = \mathrm{P}(N(0,1) + s/\sigma^2_{t+k} \leq t_\alpha) = \Phi(t_\alpha - s/\sigma^2_{t+k}),$$

where $N(0, 1)$ is the standard normal distribution and Φ is its cumulative distribution function. As it shows, the false negative rate depends on the confidence level α in hypothesis testing, and signal to noise ratio s/σ^2_{t+k}. Since the measured spike can be smaller than 10 packets, we assume that the spike follows a normal distribution of $N(10, \sigma^2_s)$ where σ^2_s is the variance of actual spoofed packets, making the asymptotic FN rate be $\int \Phi(t_\alpha - s/\sigma^2_{t+k}) f_s(s)\mathrm{d}s$.

Thus, we exclude vVPs if their estimated FP or FN are higher than the confidence level α, which is chosen as 0.05 from our analysis. Moreover, we only consider an AS where we can have at least 10 vVPs, all of which exhibit the same behavior; thus, the probability that all vVPs in the same AS experience FP or FN will become negligible.

B OFFICIAL SOURCES FOR ROV STATUS

Table 2 and Table 3 list (1) ASNs, (2) their announced ROV policy, and (3) references.

ISP	ASN	Source	ROV Ratio from RoVista
HEANet	1213	https://twitter.com/natural20/status/1366385420360155144	100%
Telstra	1221	https://lists.ausnog.net/pipermail/ausnog/2020-July/044367.html	100%
Sprint / T-Mobile	1239	https://www.sprint.net/policies/bgp-aggregation-and-filtering	100%
Telia	1299	https://www.teliacarrier.com/Our-Network/BGP-Routing/Routing-Security.html	100%
EBOX	1403	https://whois.arin.net/rest/asn/AS1403/pft?s=AS1403	100%
IIJ	2497	https://www.iij.ad.jp/en/dev/iir/pdf/iir_vol50_focus1_EN.pdf	100%
Belnet	2611	https://belnet.be/en/belnet-has-successfully-implemented-rpki	100%
NTT	2914	https://www.gin.ntt.net/support/policy/rr.cfm#RPKI	100%
TDC	3292	https://github.com/cloudflare/isbgpsafeyet.com/pull/523	100%
Swisscom	3303	https://twitter.com/swisscom_csirt/status/1300666695959244800	100%
Level3	3356	https://twitter.com/lumentechco/status/1374035675742412800	100%
Telstra	4637	https://www.zdnet.com/article/telstra-to-roll-out-rpki-routing-security-from-june-2020/	100%
Vocus	4826	https://blog.apnic.net/2021/05/13/vocus-rpki-implementation/	100%
Orange	5511	https://twitter.com/OrangeIC/status/1541436188241891328	100%
Cyta	6866	https://blog.daknob.net/rpki-deployment-greece-feb-19/	100%
Hurricane Electric	6939	https://mailman.nanog.org/pipermail/nanog/2020-June/108277.html	100%
AT&T	7018	https://mailman.nanog.org/pipermail/nanog/2019-February/099501.html	100%
Dhiraagu	7642	https://twitter.com/isseykun/status/1261758917467668481	0%
Comcast	7922	https://corporate.comcast.com/stories/improved-bgp-routing-security-adds-another-layer-of-protection-to-network	100%
ColoClue	8283	https://github.com/coloclue/kees	100%
Atom86	8455	https://www.linkedin.com/pulse/atom86-leveraging-rpki-make-internet-safer-place-ralph-dirkse/	100%
RETN	9002	https://twitter.com/RETNnet/status/1333735456408793089	92.5%
BIT	12859	https://www.bit.nl/news/2081/88/Registratie-van-RPKI-informatie-voor-een-veilige-routering-informatie-voor-een-veilige-routering	0%
Amazon	16509	https://aws.amazon.com/blogs/networking-and-content-delivery/how-aws-is-helping-to-secure-internet-routing/	100%
ASERGO	30736	https://twitter.com/asergogroup/status/1258377169526546432	100%
Jaguar	30781	https://twitter.com/JDescoux/status/1253344721201696768	100%
Seacom	37100	https://www.ripe.net/participate/mail/forum/routing-wg/PDZlMzAzMzhhLWVhOTAtNzIxOC1lMzI0LTBjZjMyOGI1Y2NkM0BzZWFjb20ubXU+	
NAPAfrica	37195	https://www.napafrica.net/technical/rpki-handy-hints/	100%
Workonline	37271	https://as37271.fyi/routing-policy/	100%
Freethought	41000	https://twitter.com/freethoughtnet/status/1222841548771090432	100%
Fiber Telecom	41327	https://www.peeringdb.com/asn/41327	100%
HOPUS	44530	https://twitter.com/afenioux/status/1305430383345971201	100%
NAP.EC	52482	https://www.aeprovi.org.ec/es/implementacion-de-rpki-y-validacion-de-origen-bgp-en-ecuador	100%
Scaleway	54265	https://mailman.nanog.org/pipermail/nanog/2020-April/107295.html	100%
Terrahost	56655	https://twitter.com/TerraHost/status/1259311449073168384	100%
KAPSI	57692	https://twitter.com/atonkyra/status/1253609926221496322	100%
Fusix	57866	https://fusix.nl/deploying-rpki/	100%
Gigabit ApS	60876	https://mailman.nanog.org/pipermail/nanog/2020-April/107295.html	0%
Tuxis	197731	https://twitter.com/Tuxis_IE/status/1105060034873049091	100%

Table 2: The list of official sources that network operators announced performing ROV; the shaded rows represent discrepant results from RoVista as of April 1st, 2023.

ISP	ASN	Source	ROV Ratio from RoVista
Deutsche Telekom	3320	https://twitter.com/deutschetelekom/status/1252177058555473920	0%
Worldstream	49981	https://twitter.com/worldstream/status/1257670396461166593	0%

Table 3: The list of official sources that network operators announced not performing ROV.