

ROV-GD: Improving the Measurement of ROV Deployment Using Graph Difference

Jun He*, Yahui Li*, Han Zhang*[†], Changqing An*, and Jilong Wang*[†]

*Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing, China

[†]Zhongguancun Laboratory, Beijing, China

Emails: he-j21@mails.tsinghua.edu.cn, liyahui_ego@126.com, zhhan@tsinghua.edu.cn, {acq, wjl}@cernet.edu.cn

Abstract—BGP has been threatened by prefix hijacking attacks due to the lack of authentication mechanisms. In recent years, many ASes have begun to participate in RPKI deployment to improve Internet security jointly. Some researchers have studied how to measure the actual deployment of ROV globally, but such works suffer from the shortcomings of small measurement coverage and insufficient accuracy. Therefore, we propose ROV-GD, a ROV measurement method based on graph difference. We collect routing path data from the control plane and data plane. Then, we rely on prefix reachability and propagation edges for ROV inference. The results show that about half of the tested ASes have ROV filtering behaviors. In addition, our method can be extended to the ROV measurement of IXPs. Through validation and analysis, we prove that our method leads to convincing results and, at the same time, has a broader coverage and better applicability than other existing methods.

Index Terms—BGP, RPKI, ROV, Measurement, Filtering, IXP

I. INTRODUCTION

Border Gateway Protocol (BGP), one of the most critical network protocols, is used to disseminate routing information about network prefixes between Autonomous Systems (ASes). However, BGP has no security guarantee, so an attacker AS can forge false routing information to propagate on the Internet and hijack normal traffic. This attack is known as prefix hijacking, which seriously affects network communication and may even cause substantial economic losses and security problems. In order to deal with this threat, IETF proposed the Resource Public Key Infrastructure (RPKI) [1] in 2008. RPKI prevents attackers from announcing prefix routes that do not belong to them through the cryptographic signature mechanism. The most essential concepts in RPKI are Route Origin Authorization (ROA) and Route Origin Validation (ROV). An ROA record indicates that an AS is designated by a prefix owner as the legal origin to announce routing information for the prefix. Furthermore, ROV is the corresponding authentication mechanism, which references trusted ROA records to verify the received BGP update messages.

In the more than ten years since RPKI came out, it has been recognized by more and more network workers. Its

popularity and deployment rate have been continuously increasing. Several works (e.g., [2], [3]) have studied the number of ROA records, their changes, and their coverage in the global routing table. Since ROA records are publicly available, studying and analyzing them is not technically complex. In contrast, whether an AS deploys ROV or not is often a private choice, so measurements on the actual deployment of ROV have always been a challenging topic. Although many methods [4]–[10] for ROV measurement have emerged in recent years, all of them currently have significant limitations. Specifically, measurements based on statistics and categorization are not sufficiently accurate and persuasive. Meanwhile, measurement methods based on logical inference have a small coverage scope. Moreover, none of the existing methods is suitable for inferring the ROV deployment of IXPs.

To address the shortcomings of existing research, we propose a ROV measurement method based on graph difference called ROV-GD. First, we select suitable prefixes from the global routing table as targets and perform the measurements from the control plane and data plane. Then, we utilize the differences of route propagation graphs and the known propagation edges for the inference of ROV filtering. In addition, our approach can be extended to measure the ROV adoption in IXPs. Finally, we compare our measurement results with existing datasets and perform manual validation to demonstrate the feasibility and accuracy of our approach.

Overall, we make the following contributions:

- We propose a new ROV measurement method based on graph difference that improves the accuracy and coverage scope.
- We measure the current ROV deployment of the Internet and find that nearly half of the tested ASes have filtering behaviors, indicating that RPKI is now better popularized.
- We extend our approach to discover the ROV adoption of an IXP remotely without sending elaborate update messages directly through it.

II. BACKGROUND

A. RPKI

RPKI is a public key infrastructure specialized to enhance Internet routing security. The five Regional Internet Registries (RIRs) are the trust anchors in the system and can issue CA

This work is partially supported by the National Science Foundation (No. 62102020) and Tsinghua University - Beijing Qihu Technology Co., Ltd Joint Research Center for Cyberspace Surveying and Mapping.

Yahui Li is the corresponding author.

certificates for their members. Prefix owners can register ROAs for their prefixes using the cryptographic signature algorithm with their private keys. A ROA record can be noted as $\{p, a, \text{max-length}\}$, which indicates that AS a is authorized to announce prefix p and its sub-prefixes as the origin, but the length of the announced prefix cannot be longer than max-length . All ROA records are centrally stored in RPKI repositories and are publicly accessible. Routers can periodically obtain ROAs and certificate data from RPKI repositories to keep them up-to-date. Furthermore, those ROAs with verified signatures can be converted to the corresponding Validated ROA Payloads (VRPs).

ROV is the validation process in RPKI that references all VRPs to categorize a received routing update message into three states:

- 1) *Valid*: this update message matches a VRP record (the origin AS of this route is the AS specified in the VRP)
- 2) *Invalid*: this routing prefix is covered by some VRPs but does not match any of them
- 3) *Unknown*: this routing prefix is not covered by any VRPs.

The update messages classified as valid or unknown are usually accepted, and these two types of routes are collectively referred to as legitimate routes. Meanwhile, the invalid update messages are usually filtered.

B. ROV in IXPs

Currently, many ASes on the Internet establish peering connections through IXPs. In order to attract customers, many large IXPs provide good guarantees in terms of bandwidth, security, and reliability. With the development and popularization of RPKI, some IXPs have also started to deploy ROV on their route servers to filter invalid routes that may cause harm.

However, since the route servers are only responsible for forwarding routing update messages, they do not appear in the AS paths of the control plane. As a result, confusions arise when measuring the ROV deployment of ASes, wrongly attributing the filtering effect of the IXP to the downstream AS. So far, the existing methods have only considered sending the invalid routes directly through the IXP to reflect its ROV adoption. However, such a method can only measure a few directly connected IXPs. To measure the ROV deployment of more IXPs requires extensive IP path data and extending the inference method to multiple hops.

III. RELATED WORK

In this section, we introduce the existing related work on ROV measurement, analyzing the main ideas and limitations of different approaches.

Logical Inference. Reuter *et al.* [4] designed a verifiable controlled experiment to measure the ROV deployment of neighboring ASes by sending them valid and invalid routes. Their method is highly accurate and persuasive but only covers a small number of ASes. Rodday *et al.* [5] performed measurements from both the control plane and data plane, and extended the logical inference method to multi-hop cases. They

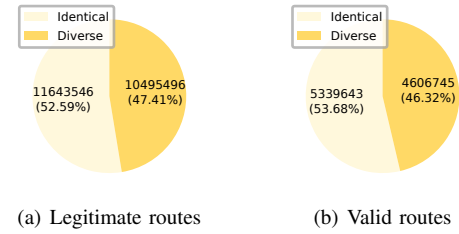


Fig. 1. Consistency analysis of routing paths between each pair of ASes.

considered starting with the origin AS and determining the ROV deployment for each AS on the path in turn. However, their method requires available probes in every AS on the route propagation path, resulting in a still limited number of ASs that can be measured. On the other hand, they use path differences as an indicator for ROV inference. We collected publicly available routing data using BGPStream [11] to analyze the routing paths between each pair (an origin AS and an observer AS) of ASes, and the results are shown in Fig. 1. We found that 47.41% of the AS pairs do not have identical AS paths between them for legitimate routes. Even considering only valid routes, 46.32% of AS pairs have multiple routing paths between them. It illustrates that ROV inference by path differences is not accurate enough.

Statistics and Classification. Hlavacek *et al.* [6], [7] considered announcing both valid and invalid routes by themselves and then collected the propagation paths from the control plane and data plane. Afterward, they categorized all observed ASes according to multiple statistical metrics. In this way, they identified ASes that are most likely to deploy ROV and those that do not. Nevertheless, since there is no solid logical correlation between the set metrics and ROV filtering, this kind of measurement method has a coarse granularity, thus lacking accuracy and persuasiveness.

Other Methods. Gilad *et al.* [8] first proposed a heuristic inference method for measuring ROV deployment. They set a counter for each AS to record the number of times it may have filtered the invalid routes. An AS is considered to have deployed ROV if its counter reaches three. Their method is straightforward but too much affected by data bias. Gray *et al.* [9] and Chen *et al.* [10] proposed ROV measurement methods based on machine learning. They converted the ROV inference problem into a Bayesian probabilistic model and then solved the model using MCMC and SVGD methods, respectively. Although both of their methods have extensive measurement coverage, like methods based on statistics and classification, they have high time complexity and low inference certainty compared to logical inference methods.

IV. METHODOLOGY

Of all the ROV measurement methods, those based on logical inference are more convincing. However, at present, the measurement coverage of such methods is small, while logical inference through path differences is not always accurate. To overcome the shortcomings of such methods, we propose

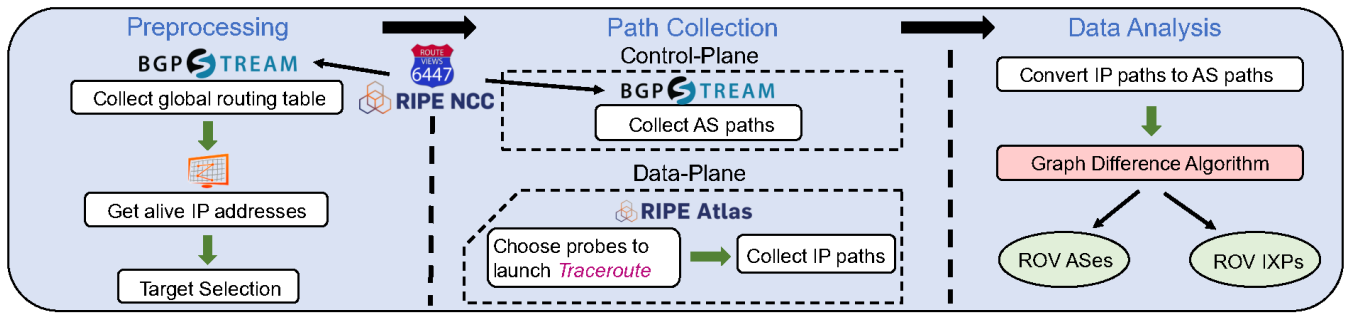


Fig. 2. Architecture and workflow of ROV-GD.

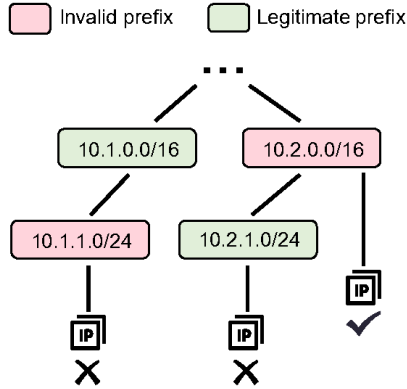


Fig. 3. Target selection of our data-plane measurement.

ROV-GD, a ROV measurement method based on graph difference. ROV-GD performs logical inference only through prefix reachability, which ensures the accuracy of the measurement. Moreover, to extend the measurement coverage, we choose invalid prefixes in the wild as detection targets and introduce the definition of *propagation edges*. In addition, our method can be extended to measure the ROV deployment of IXPs.

ROV-GD is divided into three phases (as shown in Fig. 2), which are the preprocessing phase, path collection phase, and data analysis phase. Firstly, in the preprocessing phase, we select suitable probing targets. Then, we perform passive measurement on the control plane and initiate active measurement on the data plane. Finally, we utilize the collected path information for AS ROV and IXP ROV inference using the graph difference algorithm. This section describes the flow and specific methods for each phase.

A. Preprocessing

As with all ROV measurement efforts, we need to infer the ROV deployment from the differences exhibited by invalid and legitimate routes. Specifically, we first need to find a target AS that announces both invalid and legitimate routes. Then, on the control plane, if an AS propagates the legitimate route of the target AS but does not propagate its invalid route, the AS is affected by ROV filtering (it has deployed ROV itself or its upstream AS has deployed ROV). On the data plane, when our active probing is reachable to the IP addresses in the legitimate

prefix but unreachable to the IP addresses in the invalid prefix, the existence of ROV can also be reflected.

Currently, there are two public route collector infrastructures globally (*i.e.*, RIPE RIS [12] and RouteViews [13]). These two platforms peer with some ASes through collectors and get BGP update messages from them. So, we can use BGPStream [11] to collect public routing data from these two platforms and build a global routing table. It allows us to know what prefix routes are being propagated throughout the Internet and by which ASes. Then, using the Routinator [14], we can get each route's RPKI validity (invalid or legitimate). All ASes announcing both invalid and legitimate routes constitute the target AS set for our control-plane measurements. The prefixes announced by these ASes are their corresponding target prefixes.

While on the data plane, packet forwarding follows the longest prefix matching principle. Therefore, we need to choose appropriate IP addresses to reflect the propagation paths and reachability of the target prefixes. In addition to propagating both invalid and legitimate routes, the target AS of data-plane measurement needs to satisfy two more requirements:

- 1) Both the invalid and legitimate prefixes have alive IP addresses that can respond to our probes.
- 2) Any legitimate prefix does not cover the selected invalid IP address.

We follow Chen's method [10] by first scanning the IPv4 address space using Zmap [15] to obtain all alive IP addresses that are responsive to probing. Then, based on our filtering method, we can obtain the target ASes and corresponding IP pairs that can be used for our data-plane measurement. Note that our second requirement is more stringent than before. Chen's method only requires that any legitimate prefix does not cover the invalid prefix. However, we consider the selected invalid IP address. As shown in Fig. 3, assume that *10.1.1.0/24* is an invalid prefix covered by a less specific legitimate prefix *10.1.0.0/16*. In such a case, both Chen's and our filtering methods will exclude this invalid prefix. Meanwhile, *10.2.0.0/16* is an invalid prefix not covered by other legitimate prefixes. We found many alive IP addresses in the invalid prefix, but some are covered by another more specific legitimate prefix *10.2.1.0/24*, which we will also exclude. It ensures that the selected invalid IP address truly represents this invalid prefix. Unlike the control plane, we only select a pair of target IPs for each eligible AS

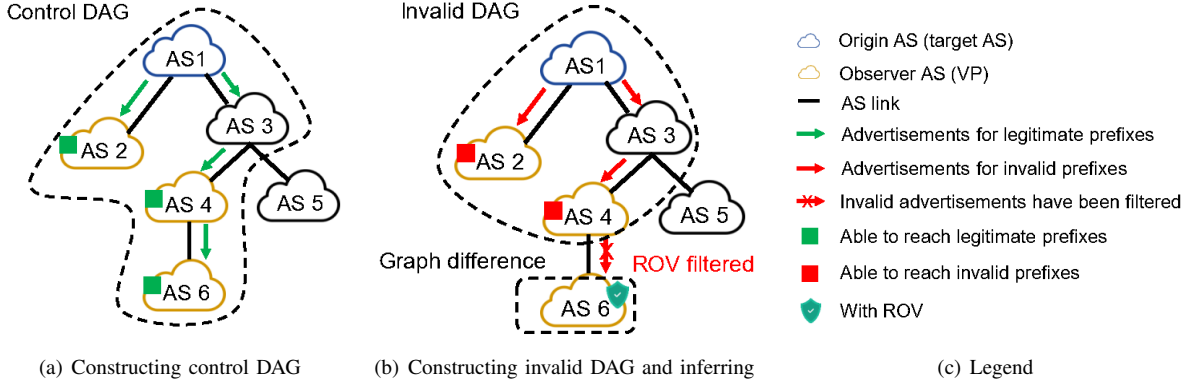


Fig. 4. Illustration of graph difference algorithm.

due to traffic and resource constraints on the data plane.

B. Path Collection

After selecting measurement targets, we can start measuring and collecting results. On the control plane, we still use BGPStream to collect the routing information related to the target AS. Specifically, we extract from the RIB dumps to get the AS paths from each peering AS to all target prefixes.

On the data plane, we perform active probing through RIPE Atlas [16]. By January 2024, RIPE Atlas has more than 12,000 probes available worldwide, constituting the largest Internet measurement network. To make our probing results cover a broader scope of the Internet, we choose probes from as many different ASes as possible. For probes belonging to the same AS, we select only one representative probe from each country (note that an AS may span multiple countries). Using these selected probes, we launch *traceroute* measurements to our target IP pairs. After excluding the failed probings, we can obtain the set of IP paths that respond to our probes.

C. Data Analysis

The AS paths obtained from our control-plane passive measurement directly reflect how routes propagate between ASes, so no additional processing is required. In contrast, IP paths obtained from our data-plane measurement should be converted to AS paths. We can use MaxMind's GeoLite2 ASN dataset [17] and CAIDA's IXPs dataset [18] to map IP addresses to corresponding AS numbers while marking the passing IXPs.

Graph Difference Algorithm. We can start our inference algorithm after getting all the AS path data. As shown in Fig. 4, for a target AS (AS 1), we use the corresponding legitimate paths to construct the control DAG [19]. Moreover, we use the invalid paths to construct the invalid DAG. ASes in the control DAG but not in the invalid DAG (we call this set the *graph difference*) are the potential ROV deployers. However, for each AS in the graph difference, there are two things we cannot determine:

- 1) The reachability of the AS to a particular invalid prefix.
- 2) Did the AS actually receive that invalid route?

When we have a probe in that AS, we can solve the first problem from the probing results. To solve the second problem, we introduce the concept of *propagation edges*. If an edge propagates a legitimate route announced by the target AS, then we define this edge as a propagation edge. According to the basic routing model [20], an AS usually does not intentionally hide part of the routes it receives from a particular neighbor as it propagates outward. So when an AS's upstream AS learns a particular invalid route (as evidenced by its presence in the invalid paths) and there is a propagation edge between them, the downstream AS will also receive that invalid route (whether it will be filtered or not). Suppose an AS behaves as unreachable to a particular invalid prefix even after receiving the corresponding invalid route. In that case, we infer that the AS has deployed ROV. As shown in Fig. 4(b), AS 6 belongs to the graph difference and is unreachable to one invalid prefix, while AS 4 is reachable for the invalid prefix. Because there is a propagation edge between them, we are able to find out that AS 6 has deployed ROV using our inference algorithm.

Extension of Inference. By processing the results of our data plane measurement, we get some AS paths marked with IXPs. Using these data, we can infer the ROV deployment of those IXPs by extending our inference method. The essence of the graph difference algorithm is to discover the filtering behaviors after passing through some propagation edges. However, if an IXP is present on the propagation edge, we can not determine whether the filtering happened in the passing IXP, the downstream AS, or both. However, if the downstream AS is reachable to some invalid prefixes, we can infer that it is the IXP that performed the filtering. Considering Fig. 5 as an example, AS 1 receives two prefixes (*i.e.*, P_1 and P_2) with different RPKI validity from a target AS and propagates them to AS 3 via an IXP. Then, our graph difference algorithm shows that P_2 is filtered. At the same time, AS 3 is reachable to another invalid prefix, P_3 , so we infer that the passing IXP has deployed ROV and filtered P_2 .

V. RESULTS

In this section, we first show the preliminary results of control-plane and data-plane measurements. Using these results,

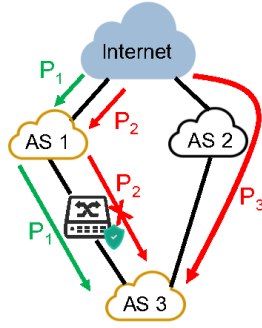


Fig. 5. Extending our inference algorithm to IXP scenarios.

we perform the inference of AS ROV filtering using our proposed inference algorithm. After that, we give the inference results for IXP ROV filtering, which are obtained using our extended inference method. Finally, we validate the above inference results and prove the effectiveness and accuracy of our method.

A. Preliminary Results

Control-plane. We used BGPStream to collect routing information provided by all RIPE RIS and RouteViews peering ASes on January 7, 2024. After obtaining the complete Internet routing table, we checked the RPKI validity of each route using Routinator. In this way, we found 1290 ASes as the origin, announcing both invalid and legitimate routes. Using these 1290 ASes as target ASes and 832 peering ASes as vantage points (VPs), we collected 584,042 invalid and 79,309,477 legitimate AS paths (note that one target AS may announce multiple invalid or legitimate prefix routes).

Data-plane. As previously described, we need to select suitable target ASes from the 1290 candidate ASes discovered by our control-plane measurement. First, we scanned the IPv4 address space using Zmap to obtain alive IP addresses in these 1290 ASes that can be used as *traceroute* targets. Then, through our target filtering method, we obtained 72 pairs of target IPs belonging to different ASes, respectively. In each pair, one is covered by only one invalid prefix route, and the other is covered by some legitimate routes. After that, we eliminated the IP pairs with unstable RPKI validity as well as relatively poor IP address responsiveness by manually checking and finally selected 66 target IP pairs.

We selected 4149 probes from the RIPE Atlas platform with significant geographic distribution differences to broaden the measurement coverage, covering 3777 ASes (VPs of the data plane). We then initiated *traceroute* measurements from each probe to all 66 pairs of target IP addresses and obtained a large number of IP paths that responded to our measurements. After that, we converted the IP paths to AS paths and labeled the passing IXPs. Ultimately, we obtained 79,574 invalid and 258,969 legitimate AS paths.

TABLE I
RESULTS OF ROV INFERENCE [# ASes]

	Control-plane	Data-plane	Total unique
Strictly filtering	20	294	263*
Partially filtering	458	1349	1772

*If an AS is inferred to be strictly filtering and partially filtering in two measurements, then we categorize it as partially filtering.

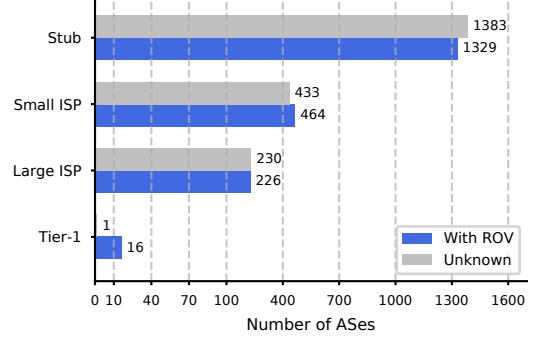


Fig. 6. ROV inference results of ASes at different levels.

B. AS ROV Filtering

After obtaining the AS paths from the control-plane and data-plane measurements, we can infer the ROV deployment of these VP ASes using our inference method. As shown in Tab. I, among all 4082 ASes to be tested, we infer a total of 2035(49.85%) ASes with ROV filtering behavior. Among them, 263 ASes adopt strict ROV filtering policies and do not propagate a single invalid route (*strictly filtering*). In contrast, 1772 ASes exhibit filtering characteristics but still propagate some invalid routes (*partially filtering*). It may be because these ASes only filter routes from particular neighbors or not all routers in the AS deploy ROV.

Based on the widely used UCLA classification [21], we further analyze the hierarchy of these ASes. It is worth mentioning that we only determine whether an AS has ROV filtering behavior. When we do not find that an AS has filtering behavior, we cannot be sure that this AS must not have deployed ROV (due to the limitations of measurement resources). So, we define the ASes that do not show signs of ROV as *Unknown*. From the results in Fig. 6, we can see that most of the Tier-1 ASes, large ISPs, and small ISPs, as the core part of the Internet, have shown signs of ROV deployment. In addition, the previous study by Hlavacek *et al.* [7] showed that stub ASes rarely show evidence of ROV filtering. They found that these stub ASes are generally protected by the filtering effects of upstream ASes or are vulnerable to invalid routes. However, our results show that about half of the tested stub ASes exhibit signs of filtering. This may indicate that more and more stub ASes are also trying to deploy ROV in recent years.

C. IXP ROV Filtering

Among all the IP paths obtained from our data-plane measurements, we flagged 340 IXPs at different locations. Fol-

lowing our extended inference method, we found that 207 IXPs exhibited filtering behavior at least once. In AS ROV inference, we found that ASes with a high number of filtering behaviors, even if they propagate invalid routes, will have a relatively low number. It implies that the probability or area of ROV deployment for that AS is more significant, which is intuitive. Nevertheless, we found that even if an IXP has many filtering behaviors, it is still likely to propagate plenty of invalid routes simultaneously. Similarly, Hlavacek *et al.* [7] found that many IXPs propagate invalid routes, including some large IXPs explicitly stating that they have deployed ROV. They think that even if an IXP's route servers deploy ROV, other direct peering sessions in the IXP may still propagate invalid routes. Our inference results also corroborate this view.

D. Validation

AS ROV Validation. There is no large-scale ground truth dataset available on ROV deployment of ASes. However, several well-known organizations have made their ROV measurement results publicly available, and we can validate our results by referring to these datasets.

The largest available dataset on ROV measurement comes from APNIC Labs [22]. It covers most ASes around the world with a large number of probe samples. At the same time, it reduces the impact of upstream filtering effects through anycast network. So, their dataset roughly reflects the extent of ROV deployment per AS. We only focus on ASes with a sample number greater than 1000 in the dataset (to reduce the error) and compare our results with them. Of the 2035 ASes with ROV filtering behavior in our results, 361 overlapped with their dataset. For 52 of these ASes classified as *strictly filtering*, the APNIC dataset suggests that filtering is present in all of them. Moreover, 43 ASes have higher than 90% filtering rates, indicating that these ASes deploy ROVs extensively. For the other 309 ASes classified as *partially filtering*, 292 of them also have filtering behavior in the APNIC dataset.

Cloudflare [23] collected some data on AS ROV deployment through ASes' Twitter announcements and operator mailing lists. Since an AS making an official announcement generally implies strict deployment, we compared the ASes we inferred to be *strictly filtering* with their dataset. The results show that of the 32 overlapping ASes, 27 are confirmed to deploy ROV filtering by the Cloudflare dataset. The other five conflicting ASes, which we manually inspected, revealed that two were also officially declared to have deployed ROV. Overall, our AS ROV inference results are broadly consistent with these public datasets.

IXP ROV Validation. Many IXPs deploy ROV filtering on their route servers, but no relevant public dataset exists. We validate this by manually investigating IXPs' websites and searching Google for IXP names with RPKI-related keywords. On the one hand, we manually verified the 10 IXPs with the most filtering behaviors (even though several propagated massive invalid routes), and all declared that they had deployed ROV. On the other hand, we verified the 10 IXPs that propagate the highest number of invalid routes and have not been detected

with filtering behaviors. In seven of them, we did not find any declarations about ROV deployment. Two of them (*i.e.*, Netnod and EdgeNXT) declared the deployment of ROV but were not detected by our inference. In addition, JKT-IX indicates that ROV is currently enabled on only one of its seven route servers. As with previous AS ROV inference, our inference only attempts to discover filtering behaviors and cannot determine that a particular IXP must not have deployed ROV. However, the above validation results indicate that our method does help to discover the ROV deployment in IXPs.

Note that we usually do not compare our results with those of other measurement methods because of the time-sensitive nature of ROV deployment and the difficulty of replicating the measurement conditions of other methods.

VI. DISCUSSION

In this section, we discuss several remaining problems in ROV measurements and analyze the advantages of ROV-GD.

A. Remaining Problems

Lack of VPs. If ROV measurements are to be performed based on logical inference, current methods require at least one VP (*i.e.*, probe of the data plane or peering site of the control plane) in the AS under test. Otherwise, we cannot know the reachability of that AS to the invalid prefix. To the disadvantage of researchers, there are only a small number of ASes with available VPs. So, the coverage of ROV measurement based on logical inference is limited. However, suppose there are available probes in the target invalid prefix. In that case, we can consider reverse probing to reflect the reachability of each AS to the invalid prefix by whether the reply arrives or not.

Measurement Bias. Currently, many ASes have large geographical spans and complex network architectures, and it often takes time to deploy a security mechanism fully. In addition, the VPs in an AS sometimes only reflect the situation of part of the network but not the overall AS. Even if we find that ROV is deployed in the subnet where a VP is located, it does not mean that the whole AS has fully deployed ROV. Our measurement results also show this, as many ASes still propagate invalid routes while exhibiting filtering behaviors. However, this situation will be improved with the popularization of RPKI.

Inaccuracy of Measurement. Since the VPs of the control plane are mainly distributed in the core area of the Internet, we have to rely on data-plane measurements to get a broader measurement coverage. However, the *traceroute* probing has many missing results (not responding or responding with private IP addresses), not to mention the errors in converting IP paths to AS paths. So, inaccurate results are a common problem in all data-plane measurements.

B. Our Strengths

Less Resource-demanding. On the control plane, our approach requires only passive data collection. On the data plane, we only need to scan for active IP addresses and utilize public platforms to launch measurements to a small number of target IPs. Many related works utilize specialized network prefixes

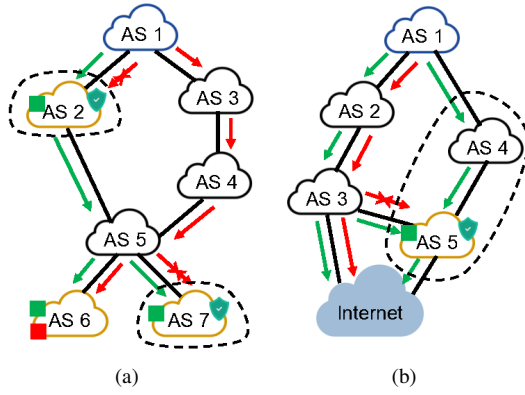


Fig. 7. Two possible cases in the measurements.

and AS numbers to initiate announcements over the Internet to create targets for observation. In contrast, our approach is less demanding, more straightforward, and more feasible.

More precise and broader coverage. We present explicit logical inference conditions rather than rely on quantitative statistics for approximate categorization. Moreover, we only consider reachability as the most critical judgment criterion, so our inference is more rigorous and precise. At the same time, our measurement has a broader measurement coverage (found more than 2000 ROV ASes) than other measurements based on logical inference ([4], [5] found three and about 200 ASes that have deployed ROV, respectively).

Strong applicability. Rodday *et al.* [5] previously extended the logical inference method to the multi-hop case. However, they required that none of the upstream ASes of the AS to be tested have deployed ROV and that there are available VPs in each AS on the path. As shown in Fig. 7(a), AS 2 has deployed ROV, and there is no available VP in AS 5, so their method could not determine whether AS 7 has deployed ROV. In contrast, our method can be successfully applied to this case. In addition, McDaniel *et al.* [19] and Smith *et al.* [24] used *min/max inference* to infer the deployment of filtering mechanisms. However, they simply infer that all ASes in the graph difference have deployed filtration or that only the root of each weakly connected component has deployed filtration. In the case of Fig. 7(b), using *min/max inference*, one would incorrectly infer that both AS 4 and AS 5 are filtering or only AS 4 is filtering. However, our method correctly infers that only AS 5 is filtering. To summarize, our method is more applicable.

Highly Extensible. Since we focus on which propagation edge the filtering behavior occurs on, our method can also be extended to the inference of other filtering mechanisms. We just need to collect the propagation paths of normal routes and routes that would be filtered. After that, we can follow the graph difference algorithm for inference.

VII. CONCLUSION

To understand the current state of ROV deployment on the Internet, we propose a ROV measurement method based on graph difference. Specifically, we initiated measurements

from the control plane and data plane. Then, we collected propagation paths for ROV inference. The results showed that about half of all tested ASes had filtering behaviors. Compared to other similar works, our method has a broader measurement coverage and is verified to be highly accurate. In addition, our work is the first to propose a generalized method for inferring the ROV deployment of IXPs. In the future, we intend to conduct regular measurements to follow the global trend of RPKI deployment.

ACKNOWLEDGMENT

We would like to thank RIPE Atlas for offering us sufficient user credits and properly loosening our measurement quotas.

REFERENCES

- [1] M. Lepinski and S. Kent, "An Infrastructure to Support Secure Internet Routing," RFC 6480, February 2012.
- [2] T. Chung *et al.*, "RPKI is coming of age: A longitudinal study of RPKI deployment and invalid route origins," in *Proceedings of the Internet Measurement Conference*, 2019, pp. 406-419.
- [3] R. Fontugne, A. Phokeer, C. Pelsser, K. Vermeulen, and R. Bush, "RPKI Time-of-Flight: Tracking Delays in the Management, Control, and Data Planes," in *International Conference on Passive and Active Network Measurement*, 2023, pp. 429-457.
- [4] A. Reuter *et al.*, "Towards a rigorous methodology for measuring adoption of RPKI route validation and filtering," *ACM SIGCOMM Computer Communication Review*, vol. 48, no. 1, pp. 19-27, 2018.
- [5] N. Rodday *et al.*, "Revisiting rpk route origin validation on the data plane," in *Proceedings of Network Traffic Measurement and Analysis Conference*, 2021.
- [6] T. Hlavacek, A. Herzberg, H. Shulman, and M. Waidner, "Practical experience: Methodologies for measuring route origin validation," in *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2018, pp. 634-641.
- [7] T. Hlavacek, H. Shulman, N. Vogel, and M. Waidner, "Keep Your Friends Close, but Your Routers Closer: Insights into RPKI Validation in the Internet," in *32nd USENIX Security Symposium*, 2023, pp. 4841-4858.
- [8] Y. Gilad, A. Cohen, A. Herzberg, M. Schapira, and H. Shulman, "Are we there yet? On RPKI's deployment and security," in *NDSS*, 2017.
- [9] C. Gray *et al.*, "BGP beacons, network tomography, and Bayesian computation to locate route flap damping," in *Proceedings of the ACM Internet Measurement Conference*, 2020, pp. 492-505.
- [10] W. Chen *et al.*, "ROV-MI: Large-Scale, Accurate and Efficient Measurement of ROV Deployment," in *NDSS*, 2022.
- [11] CAIDA, "BGPStream," <https://bgpstream.caida.org/>, 2021.
- [12] RIPE NCC, "Routing Information Service (RIS)," <https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris>, 2024.
- [13] University of Oregon, "RouteViews Project," <http://www.routeviews.org/routeviews/>, 2024.
- [14] NLnetLabs, "Routinator," <https://github.com/NLnetLabs/routinator>, 2024.
- [15] The Zmap Team, "The ZMap Project," <https://zmap.io/>, 2022.
- [16] RIPE NCC, "RIPE Atlas," <https://atlas.ripe.net/>, 2024.
- [17] MaxMind, "GeoLite2 ASN Database," <https://dev.maxmind.com/geoip/docs/databases/asn>, 2024.
- [18] CAIDA, "IXPs Dataset," <https://www.caida.org/catalog/datasets/ixps/>, 2024.
- [19] T. McDaniel, J. M. Smith, and M. Schuchard, "Flexsealing BGP against route leaks: peerlock active measurement and analysis," in *NDSS*, 2021.
- [20] L. Gao and J. Rexford, "Stable Internet routing without global coordination," *IEEE/ACM Transactions on Networking*, vol. 9, no. 6, pp. 681-692, 2001.
- [21] R. Oliveira, D. Pei, W. Willinger, B. Zhang, and L. Zhang, "The (in) completeness of the observed Internet AS-level structure," *IEEE/ACM Transactions on Networking*, vol. 18, no. 1, pp. 109-122, 2009.
- [22] APNIC Labs, "RPKI I-ROV Filtering World Map," <https://stats.labs.apnic.net/rpki>, 2024.
- [23] Cloudflare, "Is BGP safe yet?," <https://isbgpsafeyet.com/>, 2021.
- [24] J. M. Smith, K. Birkeland, T. McDaniel, and M. Schuchard, "Withdrawing the BGP re-routing curtain: Understanding the security impact of BGP poisoning via real-world measurements," in *NDSS*, 2020.