Understanding Route Origin Validation (ROV) Deployment in the Real World and Why MANRS Action 1 Is Not Followed

Lancheng Qin, Li Chen, Dan Li, Honglin Ye, Yutian Wang

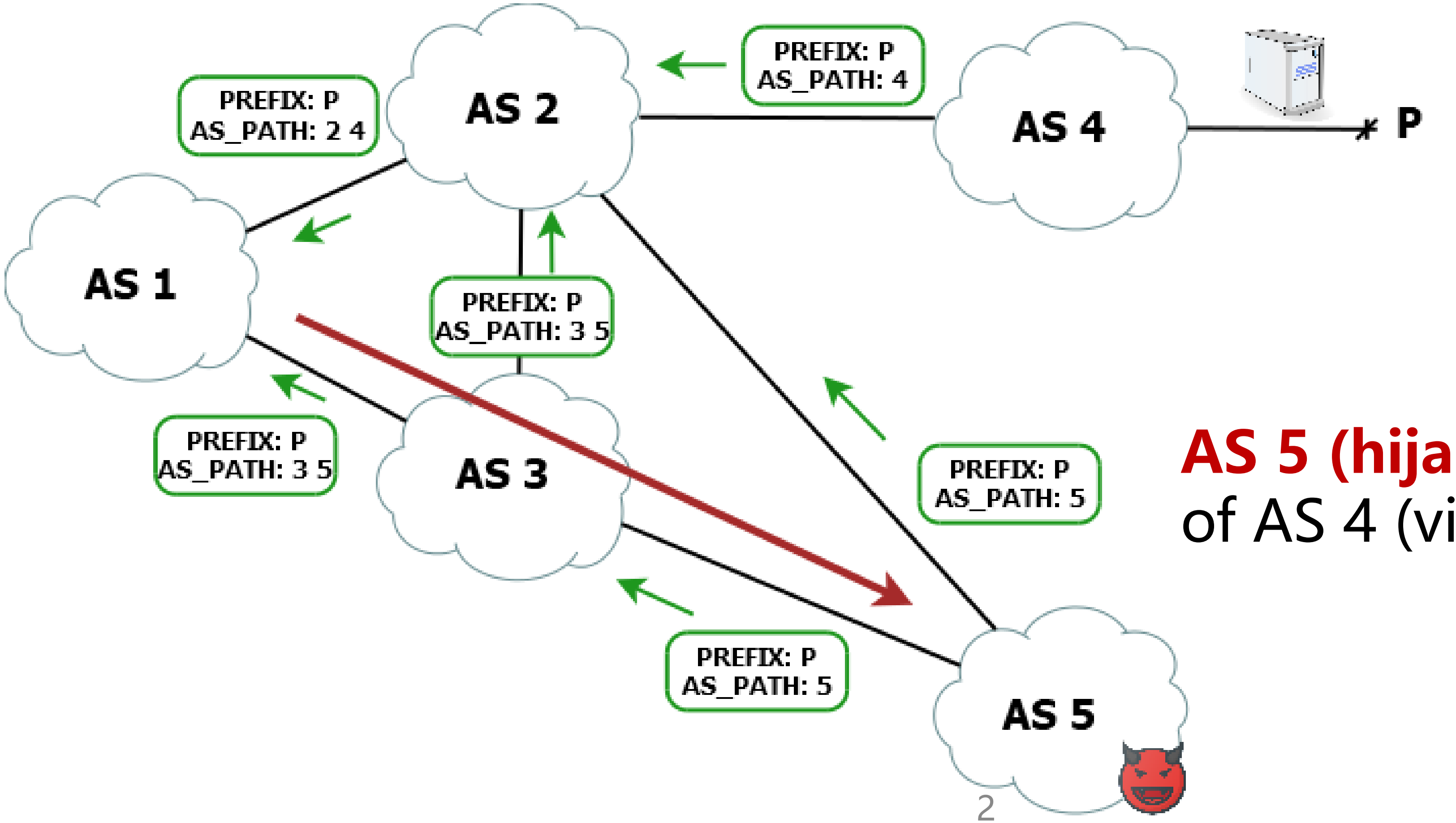
Tsinghua University

Zhongguancun Laboratory

BNRist

BGP Hijacking

BGP hijacking is one of the most important threats to today's Internet



AS 5 (hijacker) announces prefix P of AS 4 (victim) through BGP

MANRS

Mutually Agreed Norms for Routing Security (MANRS)

Action 1 (Mandatory)

Prevent the propagation of illegitimate BGP announcements from customers

Action 2 (Recommended)

Prevent traffic with spoofed source IP address

Action 3 (Mandatory)

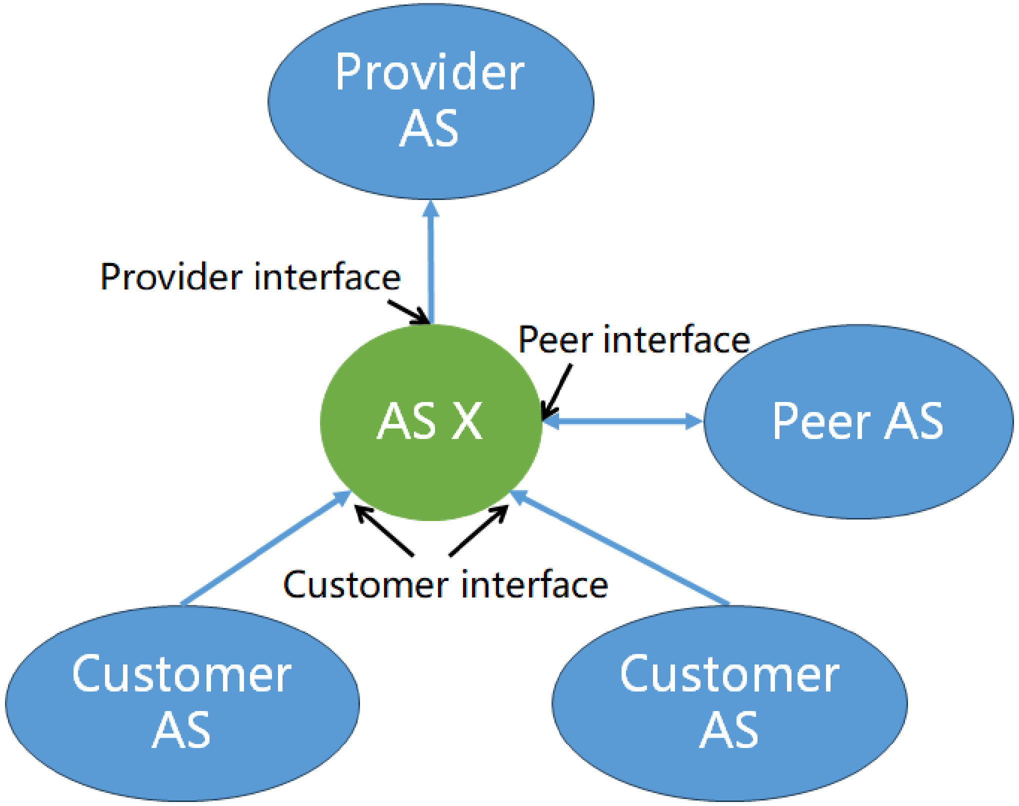
Enter contact information in IRRs or PeeringDB

Action 4 (Mandatory)

Document intended routing announcements in IRRs or RPKI

MANRS Action 1

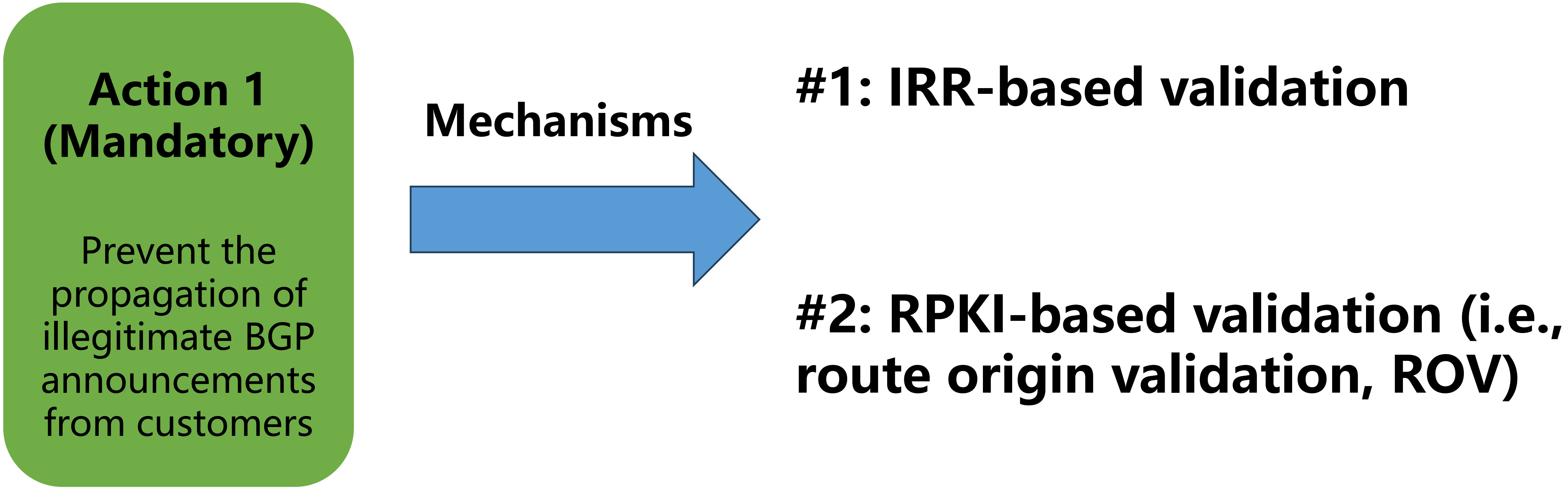
Mutually Agreed Norms for Routing Security (MANRS)



- □ Network operator must **check whether the announcements of their customers are correct**
  - ◆ At least deploying ROV at customer interfaces

MANRS Action 1

Mutually Agreed Norms for Routing Security (MANRS)



Action 1 (Mandatory)

Prevent the propagation of illegitimate BGP announcements from customers

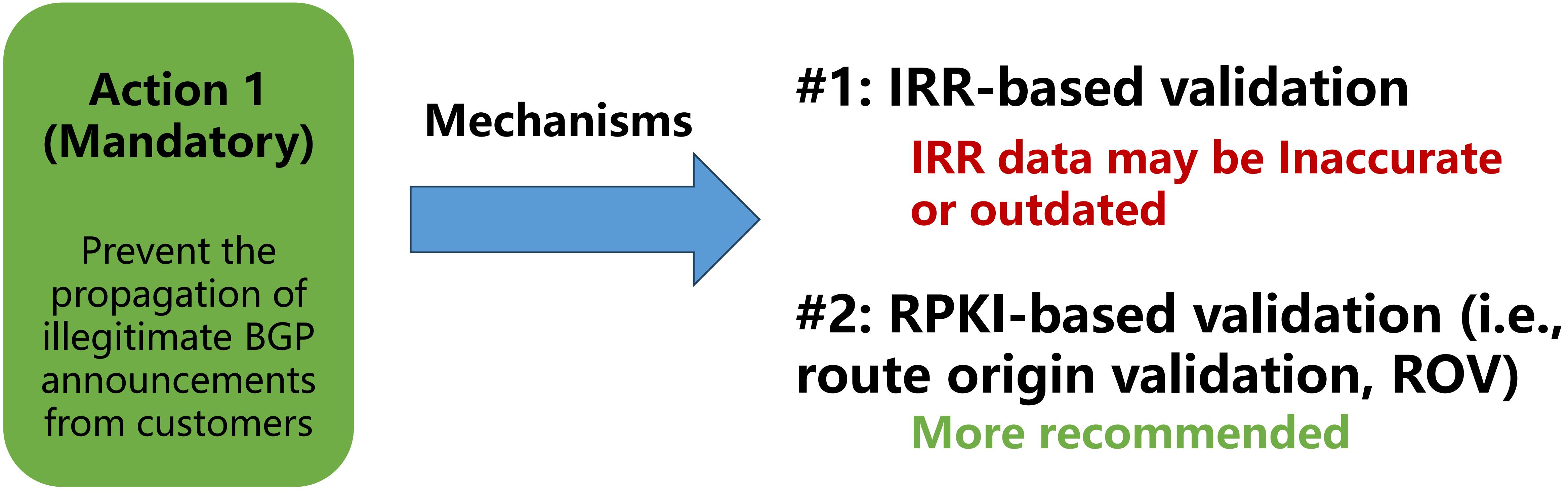
Mechanisms

#1: IRR-based validation

#2: RPKI-based validation (i.e., route origin validation, ROV)

MANRS Action 1

Mutually Agreed Norms for Routing Security (MANRS)



Action 1 (Mandatory)

Prevent the propagation of illegitimate BGP announcements from customers

Mechanisms

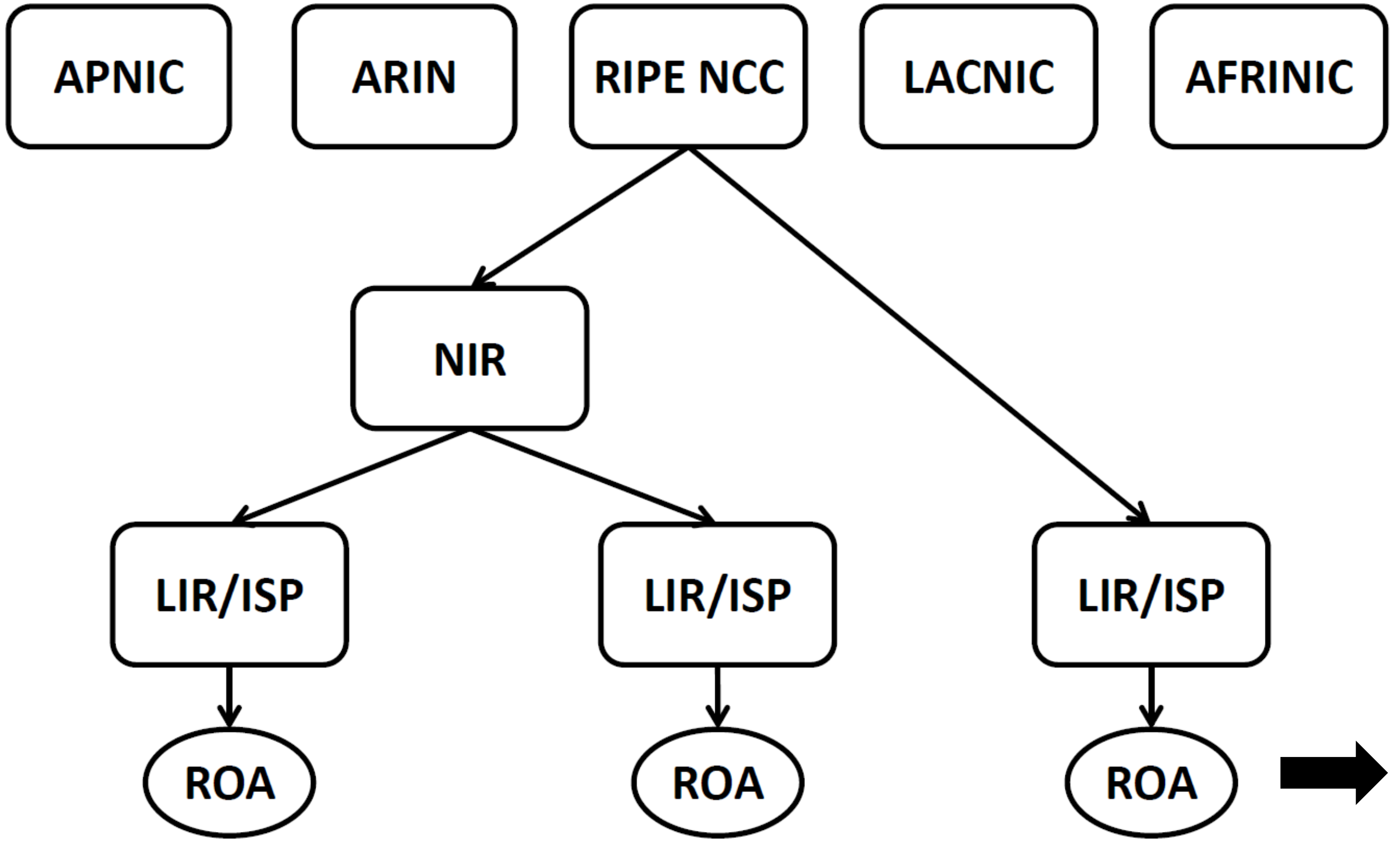
#1: IRR-based validation

IRR data may be Inaccurate or outdated

#2: RPKI-based validation (i.e., route origin validation, ROV)

More recommended

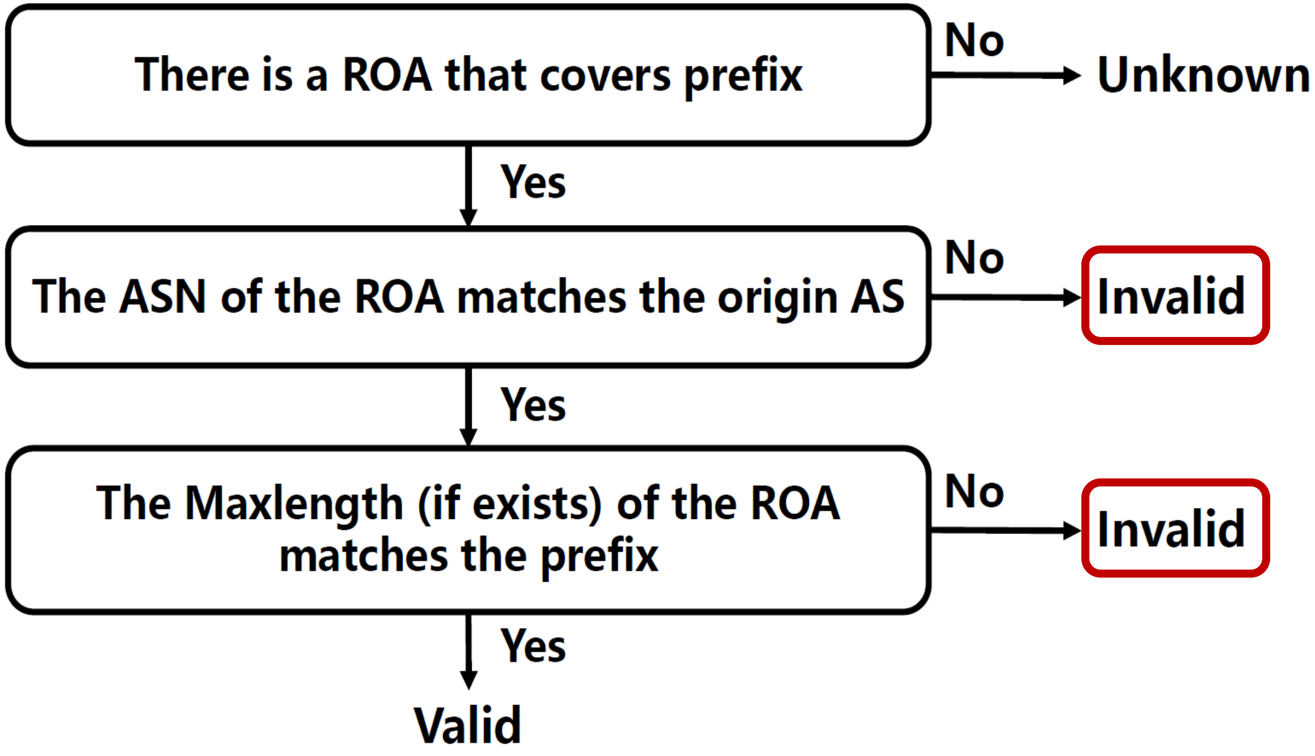
Resource Public Key Infrastructure (RPKI)

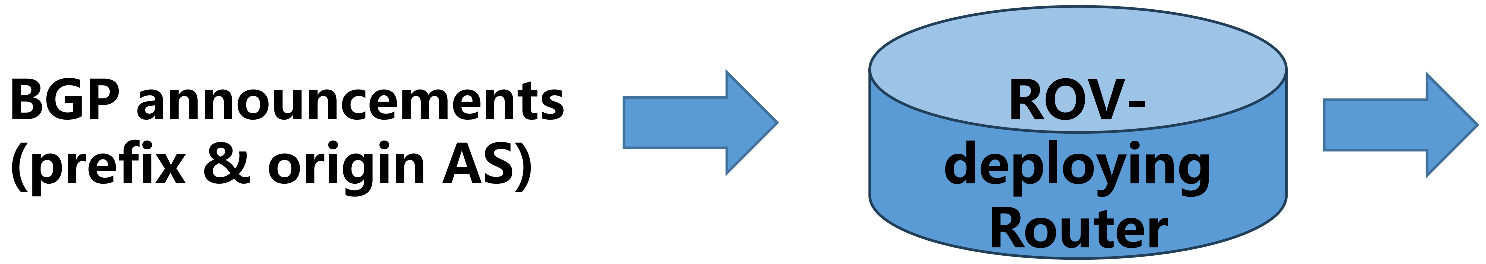


Example

Prefix: 45.89.248.0/24
Max Length: /24
ASN: 3356
Emitted: Thu, 24 Aug 2023 17:08:53 GMT
Validity: Thu, 24 Aug 2023 17:03:53 GMT - Thu, 22 Aug 2024 17:08:53 GMT
Trust Anchor: RIPE

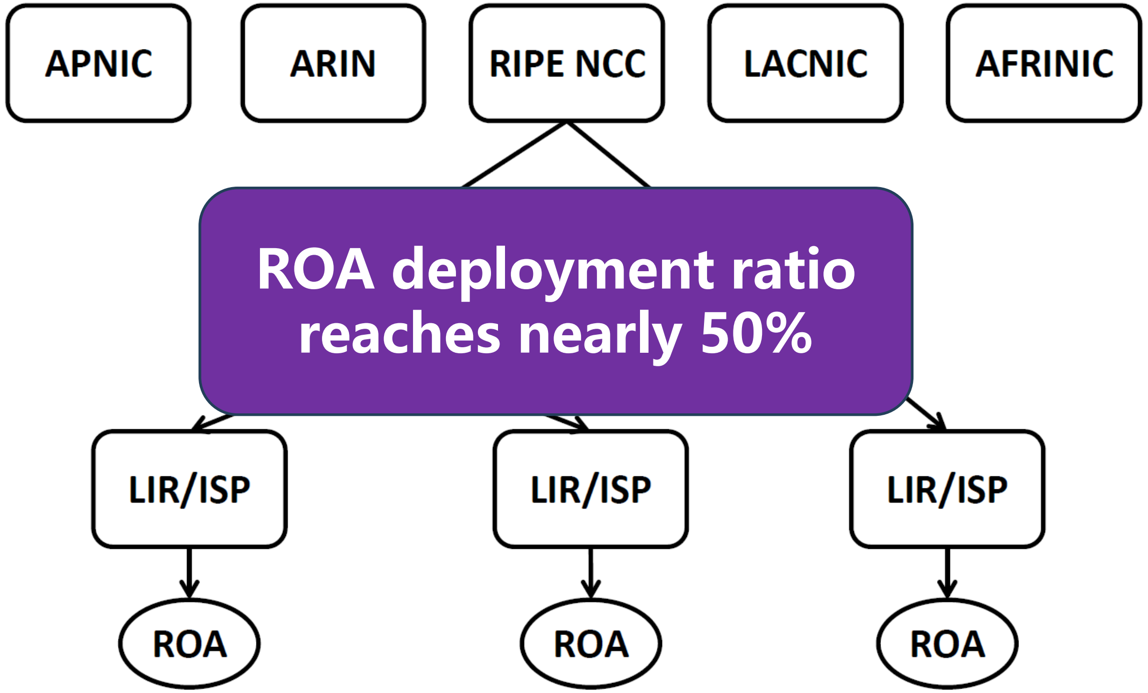
Route Origin Validation (ROV)


There is a ROA that covers prefix
No
Unknown
Yes
The ASN of the ROA matches the origin AS
No
Invalid
Yes
The Maxlength (if exists) of the ROA matches the prefix
No
Invalid
Yes
Valid

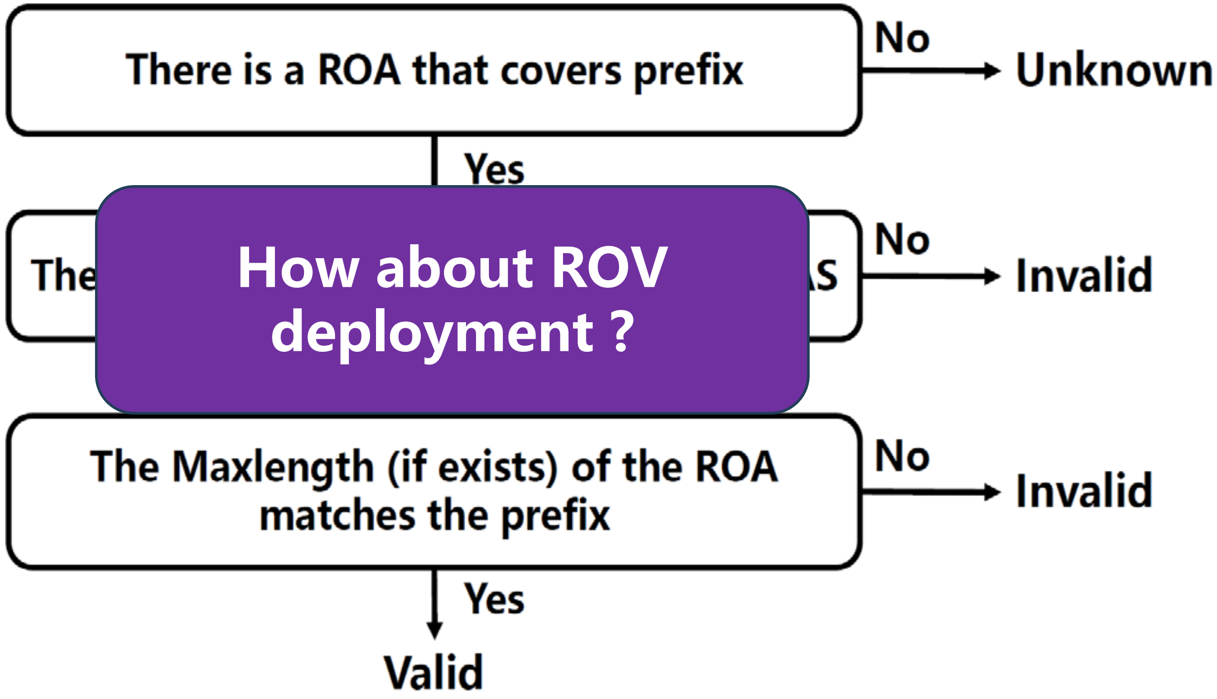


- □ RPKI-valid and RPKI-unknown prefixes will be propagated
- □ RPKI-invalid prefixes should be dropped

RPKI Deployment



ROA deployment ratio reaches nearly 50%


There is a ROA that covers prefix
No
Unknown
Yes
The
S
No
Invalid
The Maxlength (if exists) of the ROA matches the prefix
No
Invalid
Yes
Valid

How about ROV deployment ?

Questions

□ How about ROV deployment in real world and network operators' compliance to MANRS Action 1?

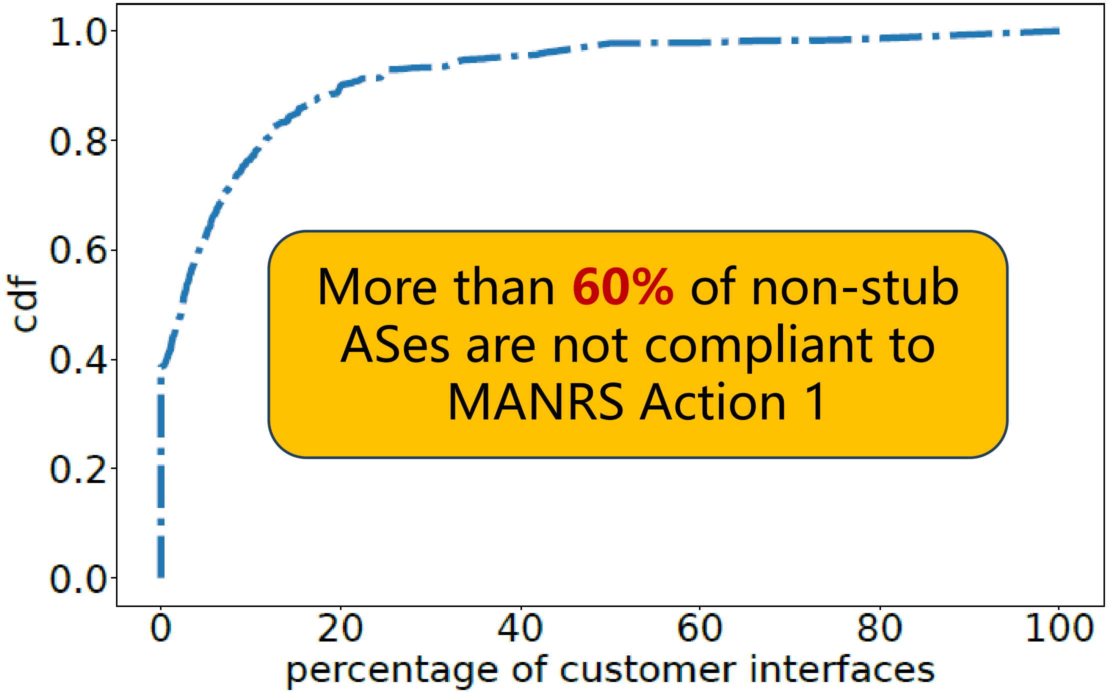
□ Why are network operators not following MANRS Action 1?

□ How to promote further deployment of ROV?

Measurement

We measure the **prevalence of RPKI-invalid prefixes** that propagated through each AS

- □ BGP data: RouteViews and RIPE RIS
- □ AS relationship: CAIDA
- □ We finally identify **1,012 ASes (117 stub ASes and 895 non-stub ASes) that have propagated RPKI-invalid prefixes**

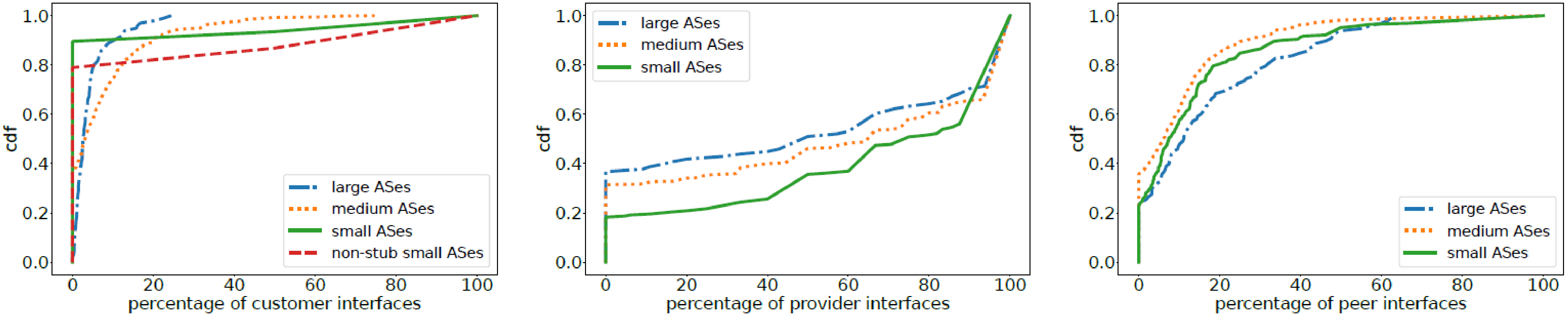


More than **60%** of non-stub ASes are not compliant to MANRS Action 1

Figure 3: Percentage of customer interfaces that accept RPKI-invalid prefixes for non-stub ASes. More than 60% of non-stub ASes are not compliant to MANRS Action 1.

Measurement

Percentage of **different classes of interfaces** (i.e., customer interface, provider interface, peer interface) that accept RPKI-invalid prefixes



(a) Percentage of customer interfaces that accept RPKI-invalid prefixes.

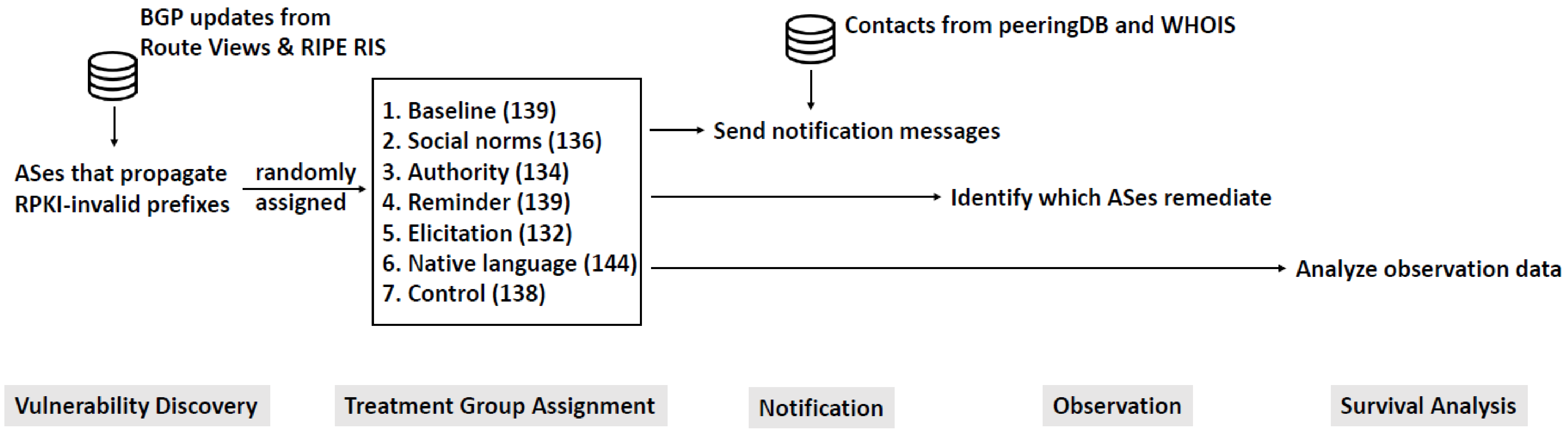
(b) Percentage of provider interfaces that accept RPKI-invalid prefixes.

(c) Percentage of peer interfaces that accept RPKI-invalid prefixes.

Figure 4: Percentage of different classes of interfaces that accept RPKI-invalid prefixes.

Notification Experiment

We present the first notification experiment to evaluate
the impact of different notification on ROV remediation



BGP updates from
Route Views & RIPE RIS

ASes that propagate
RPKI-invalid prefixes

randomly
assigned

1. Baseline (139)
2. Social norms (136)
3. Authority (134)
4. Reminder (139)
5. Elicitation (132)
6. Native language (144)
7. Control (138)

Contacts from peeringDB and WHOIS

Send notification messages

Identify which ASes remediate

Analyze observation data

Vulnerability Discovery

Treatment Group Assignment

Notification

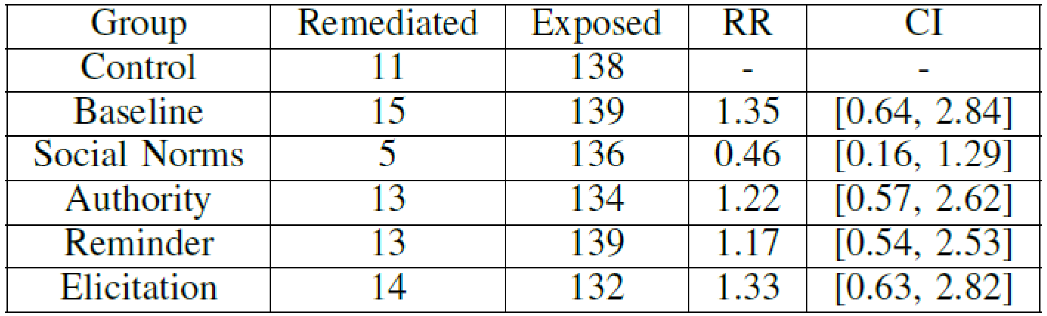
Observation

Survival Analysis

Notification Experiment

None of the treatments can significantly improve the remediation rate of ROV compared to the control group

Table I: Relative risk ratios for different nudge treatments compared to the control group.



Group	Remediated	Exposed	RR	CI
Control	11	138	-	-
Baseline	15	139	1.35	[0.64, 2.84]
Social Norms	5	136	0.46	[0.16, 1.29]
Authority	13	134	1.22	[0.57, 2.62]
Reminder	13	139	1.17	[0.54, 2.53]
Elicitation	14	132	1.33	[0.63, 2.82]

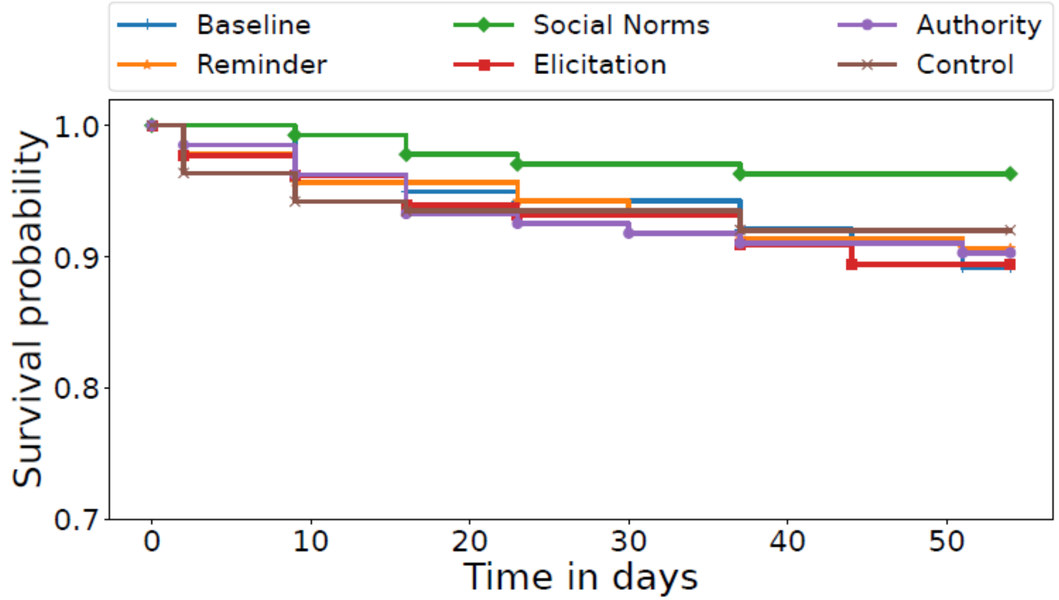
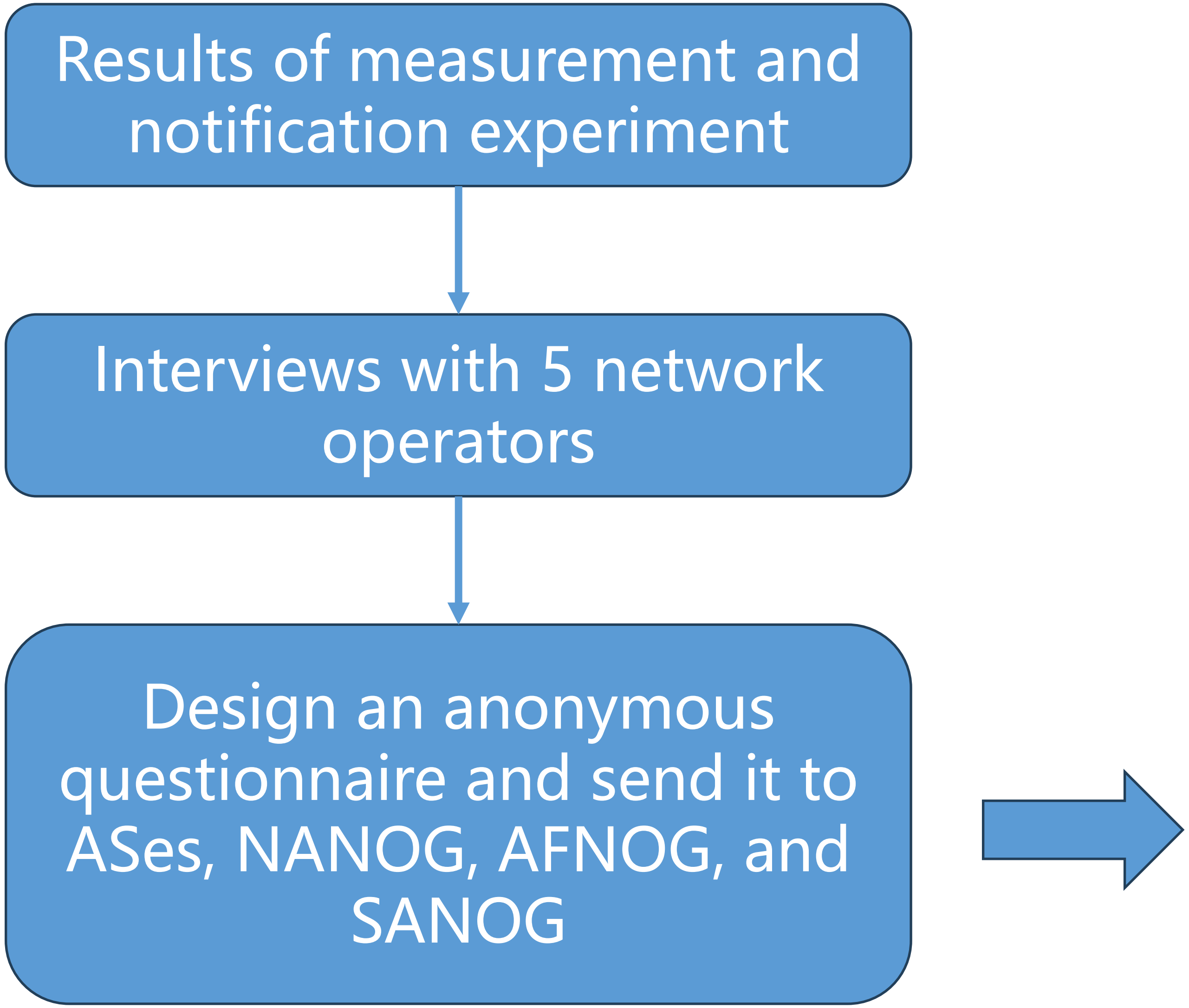


Figure 6: Survival curves for different nudge treatments and the control group.

Questions

- □ How about ROV deployment in real world and network operators' compliance to MANRS Action 1?
- □ Why are network operators not following MANRS Action 1?
- □ How to promote further deployment of ROV?

Survey



Results of measurement and notification experiment

Interviews with 5 network operators

Design an anonymous questionnaire and send it to ASes, NANOG, AFNOG, and SANOG

1. Do you deploy or intend to deploy ROV at provider interfaces, customer interfaces, or peer interfaces?
2. What are your reasons for not intending to deploy ROV at different classes of interfaces?
3. Have you encountered any problems when operating ROV?
4. Does the implementation guide provided by MANRS initiative provide effective assistance?
5. What do you think are the priorities of deploying ROV at different classes of interfaces?
6. What are your valuable experiences or suggestions for implementing or operating ROV?

Survey Results

Non-compliant networks are mainly due to **economical and technical reasons**

Economical reasons

- □ Lack of time and effort
- □ Business conflict
  - ◆ Customer ASes do not want their announcements to be dropped
- □ Limited router capability
- □ High operational overhead

Technical reasons

- □ Technical bugs in RIR servers or router software
- □ Technical limitations of ROV mechanism
  - ◆ Drop legitimate BGP announcements due to incomplete or inaccurate ROA
  - ◆ Depend on upstream filtering
  - ◆ Vulnerable to BGP path hijacking

Questions

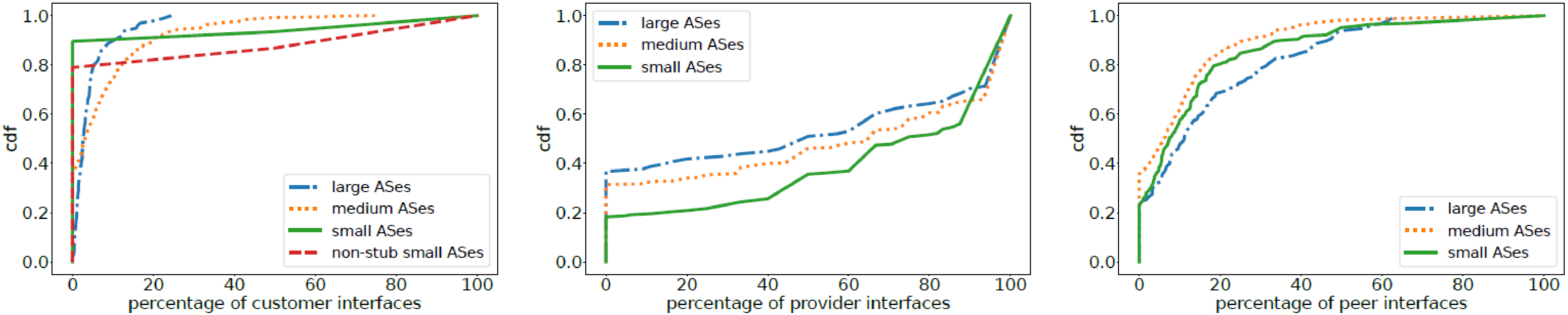
□ How about ROV deployment in real world and network operators' compliance to MANRS Action 1?

□ Why are network operators not following MANRS Action 1?

□ How to promote further deployment of ROV?

Recommendation on Deployment Strategy

- Since it is difficult to perform RPKI-invalid filtering at all classes of interfaces simultaneously, partial filtering is common in the early days of ROV deployment
  - What is the best deployment strategy?



(a) Percentage of customer interfaces that accept RPKI-invalid prefixes.

(b) Percentage of provider interfaces that accept RPKI-invalid prefixes.

(c) Percentage of peer interfaces that accept RPKI-invalid prefixes.

Figure 4: Percentage of different classes of interfaces that accept RPKI-invalid prefixes.

Recommendation on Deployment Strategy

- ROV at provider interfaces can **work better in preventing the propagation of RPKI-invalid prefixes** than ROV at customer or peer interfaces

- For transit networks, deploying ROV at provider interfaces **will not conflict with the business requirements of their customers**

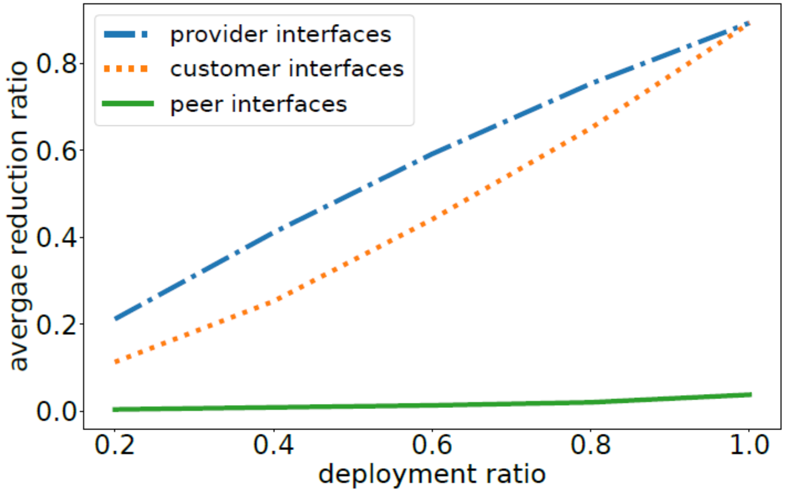


Figure 8: The average reduction ratio of polluted ASes of deploying ROV at provider interfaces, at customer interfaces, or at peer interfaces over different deployment ratios.

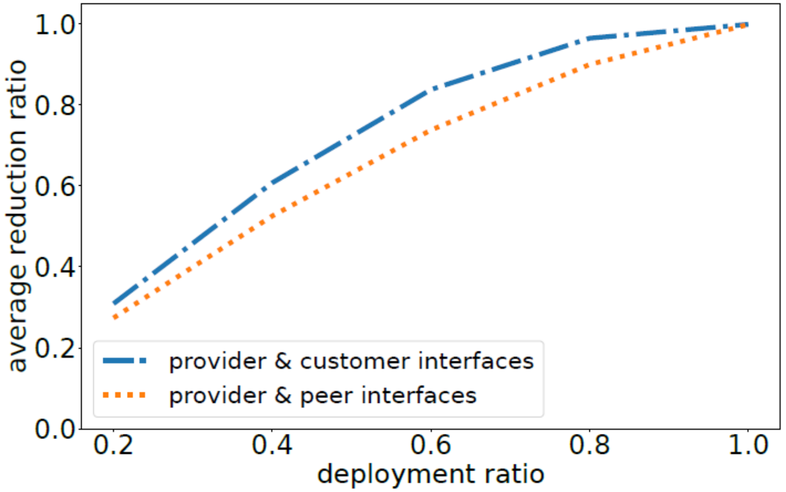


Figure 9: The average reduction ratio of polluted ASes of deploying ROV at provider and customer interfaces, or at provider and peer interfaces over different deployment ratios.

Provider interface

>

Customer interface

>

Peer interface

Recommendation for Backup and Purchasing

□ Increase the geographic diversity and software diversity of ROV deployment

◆Deploy to two different data centers or use two different code-bases

□ Market research

◆Arista, Arrcus, Cisco, Extreme Networks, Huawei, H3C, Juniper, MikroTik, and Nokia have supported ROV in their routers

Thank you!

Lancheng Qin

qlc19@mails.tsinghua.edu.cn

Acknowledgement: Deng Feng Fund