Mind Your MANRS: Measuring the MANRS Ecosystem

Ben Du, Cecilia Testart, Romain Fontugne,
Gautam Akiwate, Alex C. Snoeren, kc claffy

Deepak Gouda
Esha Ashish Ponda
20th February, 2023

Background & Motivation

The Problem

- Border Gateway Protocol (BGP) - the interdomain routing protocol

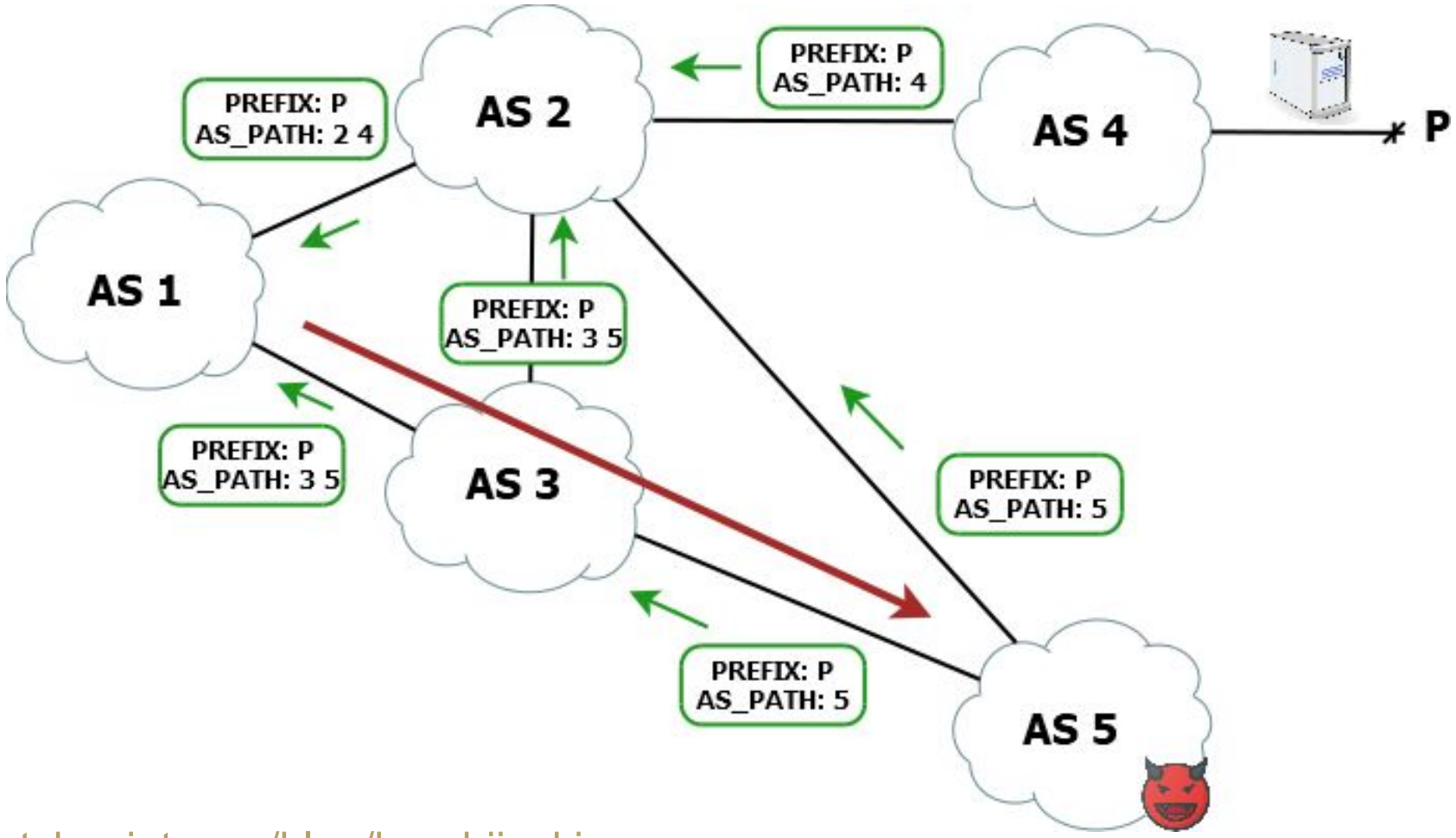
Source : https://dl.acm.org/doi/abs/10.1145/3517745.3561419

The Problem

- Border Gateway Protocol (BGP) - the interdomain routing protocol
- BGP includes no mechanism to validate information exchanged between networks

Source : https://dl.acm.org/doi/abs/10.1145/3517745.3561419

The Problem



https://www.catchpoint.com/blog/bgp-hijacking

The Problem

- Border Gateway Protocol (BGP) - the interdomain routing protocol
- BGP includes no mechanism to validate information exchanged between networks
- Attackers can advertise IP address space without authorization (BGP hijacking)

Crypto Exchange KLAYswap Loses $1.9M After BGP Hijack

Hackers Performed Border Gateway Protocol Hack to Conduct Illegal Transactions

Prajeet Nair (@prajeetspeaks) • February 16, 2022

BORDER GATEWAY PROTOCOL INSECURITY —

How 3 hours of inaction from Amazon cost cryptocurrency holders $235,000

For 2nd time in 4 years, Amazon loses control of its IP space in BGP hijacking.

DAN GOODIN - 9/23/2022, 11:04 AM

Source : https://dl.acm.org/doi/abs/10.1145/3517745.3561419

Solution 1 - IRR (Internet Routing Registry)

IRR is a database system that allows network operators to publish and exchange information about their routing policies and interconnections.

Classifies BGP prefix origin as:

- ***Valid*** - At least one VRP with prefix, ASN and prefix length attributes matching the route
- ***Invalid*** - All VRPs with invalid ASNs
- **Invalid Length** - Correct ASN, invalid prefix length
- ***Not Found*** - No covering VRP

Solution 2 - RPKI (Resource Public Key Infrastructure)

A set of cryptographically attested databases containing authenticated prefix-origin information.

Classifies BGP prefix origin as:

- ***Valid*** - At least one VRP with prefix, ASN and max length attributes matching the route
- ***Invalid*** - All VRPs with invalid ASNs
- **Invalid Length** - Correct ASN, invalid max length
- ***Not Found*** - No covering VRP

The MANRS Initiative

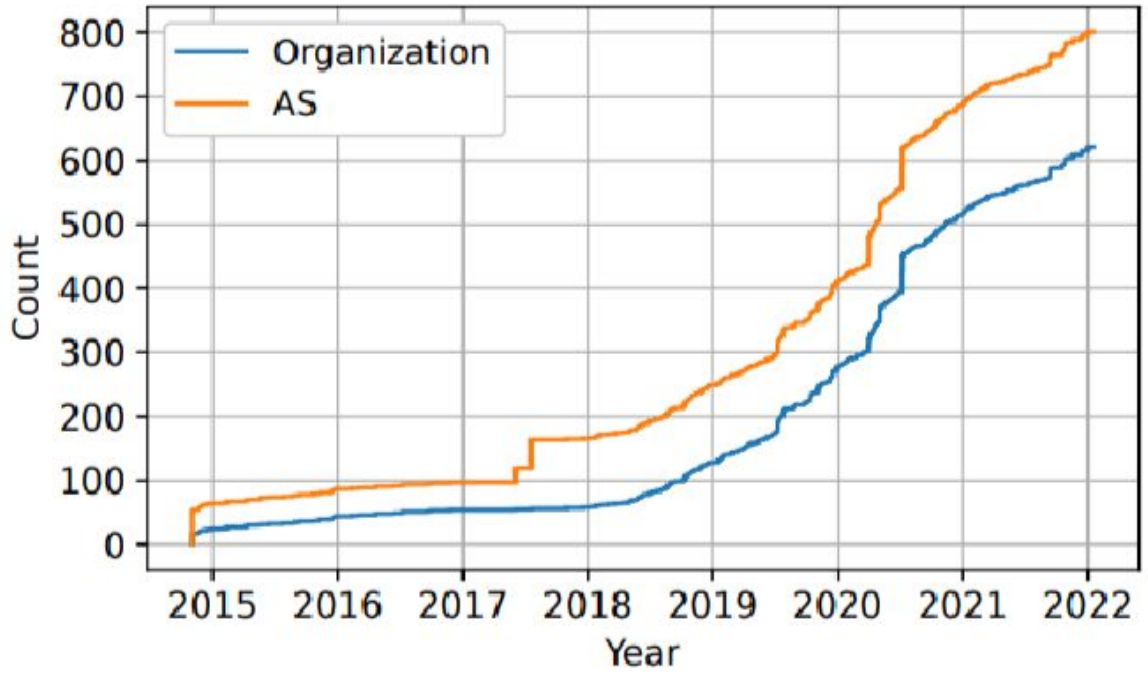
If we already have RPKI and IRR, why add MANRS also?

The Problem (again?)

- There was no guidance or methodology on how to adopt IRR and RPKI to improve the security posture of organizations and ASes
- To encourage collective action among ASes and organizations in adoption of routing security best practices MANRS was launched

MANRS - Mutually Agreed Norms on Routing Security

MANRS (Mutually Agreed Norms for Routing Security) initiative was launched in 2014 by a group of networks to advocate for set of security best practices.



Paper Objectives

- Characterize new networks which joined after inception of MANRS
- Analysis of difference in implementations of security best practices (actions) between MANRS and non-MANRS networks. The level of deployment per network and the conformance is considered.
- Study of the impact of MANRS networks on the whole Internet in terms of RPKI registration and Route Origin Validation deployment.

Datasets

IHR Data

	timebin	prefix	hege	visibility	rpki_status	irr_status	asn_id	originasn_id
0	2023-02-01 00:00:00+00	2610:a1:3092::/48	0.033333	12.162162	NotFound	Valid	397224	397224
1	2023-02-01 00:00:00+00	2610:a1:1079::/48	0.041667	12.837838	NotFound	Valid	12008	397224
2	2023-02-01 00:00:00+00	2610:a1:1079::/48	0.041667	12.837838	NotFound	Valid	397224	397224
3	2023-02-01 00:00:00+00	2610:a1:1013::/48	0.016667	10.810811	NotFound	Valid	12008	397224
4	2023-02-01 00:00:00+00	2610:a1:1013::/48	0.016667	10.810811	NotFound	Valid	397224	397224
5	2023-02-01 00:00:00+00	2610:a1:1009::/48	0.041667	12.837838	NotFound	Valid	12008	397224
6	2023-02-01 00:00:00+00	2610:a1:1009::/48	0.041667	12.837838	NotFound	Valid	397224	397224
7	2023-02-01 00:00:00+00	2001:dcd:3::/48	0.025000	11.486486	Valid	Valid	12008	397224
8	2023-02-01 00:00:00+00	2001:dcd:3::/48	0.025000	11.486486	Valid	Valid	397224	397224
9	2023-02-01 00:00:00+00	2610:a1:1007::/48	0.016667	10.810811	NotFound	Valid	12008	397224

In this paper, IHR prefix origin datasets and transit dataset were used for certain calculations

as2Org (CAIDA)

```
# format:aut|changed|aut_name|org_id|opaque_id|source
1|20180220|LVLT-1|LPL-141-ARIN|e5e3b9c13678dfc483fb1f819d70883c_ARIN|ARIN
2|20120621|UDEL-DCN|UNIVER-19-ARIN|c3a16289a7ed6fb75fec2e256e5b5101_ARIN|ARIN
3|20100927|MIT-GATEWAYS|MIT-2-ARIN|d98c567cda2db06e693f2b574eafe848_ARIN|ARIN
4|20120313|ISI-AS|USC-32-ARIN|8c3f2df306a67e97a7abb5a2a0335865_ARIN|ARIN
5|20200723|SYMBOLICS|WGL-117-ARIN|481404355c401f2604c57a0fda4ee68f_ARIN|ARIN
6|20210121|BULL-HN|ATOS-Z-ARIN|61457436058bce0a6be1a923532a3255_ARIN|ARIN
7||DSTL|ORG-TDSA4-RIPE||RIPE
8|19971110|RICE-AS|RICEUN-ARIN|5f676a1dae02fc7cb708558c3ff1d122_ARIN|ARIN
9|20120402|CMU-ROUTER|CARNEG-Z-ARIN|859ff8395a142b506a4aa4425d450e1d_ARIN|ARIN
10|20000418|CSNET-EXT-AS|CCICC-ARIN|3fa2e5aa48f205a7696ea6fbcd437cff_ARIN|ARIN
11|20190812|HARVARD|HARVAR-ARIN|88e9e1a9f78221c5b97e72d580642205_ARIN|ARIN
12|20111010|NYU-DOMAIN|NYU-ARIN|b6fb8bb4720cd209413bd2838531ca56_ARIN|ARIN
13|20110802|DNIC-AS-00013|HEADQU-3-ARIN|c096bf755fee3dfb7b9046461595ebd0_ARIN|ARIN
14|20100628|COLUMBIA-GW|COLUMB-ARIN|148b369d3a54363bcd99798b25c1dc23_ARIN|ARIN
```

AS relationship dataset

```
206676|41529|-1
207381|203903|-1
210765|3557|-1
211834|3557|-1
212679|211627|-1
393672|30673|-1
397064|400830|-1
32035|8359|0
32035|16552|0
32035|37680|0
32035|7713|0
32035|398493|0
32035|28917|0
32035|63920|0
```

AS rank dataset

AS Rank ▲	AS Number ▽	Organization		cone size (ASes) ▽
1	3356	Level 3 Parent, LLC		48838
2	1299	Telia Company AB		38639
3	174	Cogent Communications		34689
4	2914	NTT America, Inc.		19219
5	6939	Hurricane Electric LLC		19144
6	6762	TELECOM ITALIA SPARKLE S.p.A.		17901
7	3257	GTT Communications Inc.		17898
8	6461	Zayo Bandwidth		17341
9	6453	TATA COMMUNICATIONS (AMERICA) INC		16999
10	3491	PCCW Global, Inc.		11363

https://asrank.caida.org/

Historical MANRS dataset

Not available publicly - was requested by authors

MANRS Actions

What does MANRS do?

Security best practices = actions

Actions for Network Operators (ISPs)

849 participants
3 mandatory actions, 1 recommended

- **Action 1** : Prevent propagation of incorrect routing information by checking the correctness of their customer's BGP announcements

- **Action 4** : Register 90% intended BGP announcements in IRR or RPKI

Actions for Cloud Providers and CDNs

21 participants

5 mandatory actions, 1 recommended

- **Action 1** : Implement ingress filtering on peers and customers by checking prefix origin validity whenever feasible

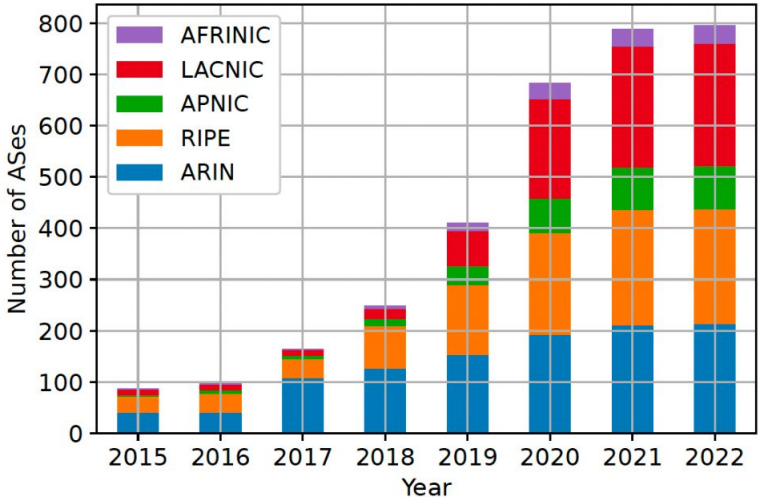
- **Action 4** : Register ALL intended BGP announcements to external parties in IRR or RPKI

Measurements and Findings

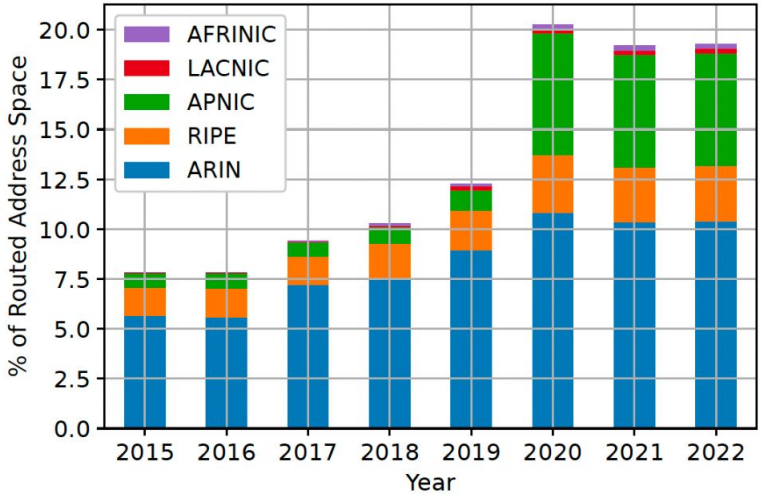
Research Questions focused on

Participation	Conformance	Impact
Growth of the MANRS ecosystem	What percentage of members conform the the MANRS Actions	Are MANRS networks more likely to filter invalid announcements?

Participation



(a) MANRS ASes over time. Brazil (in LACNIC region) added 90 small ASes in 2020 due to local outreach efforts.



(b) Percentage of MANRS routed IPv4 address space. MANRS ASes in the ARIN region announce the most address space.

AS Customer Degree

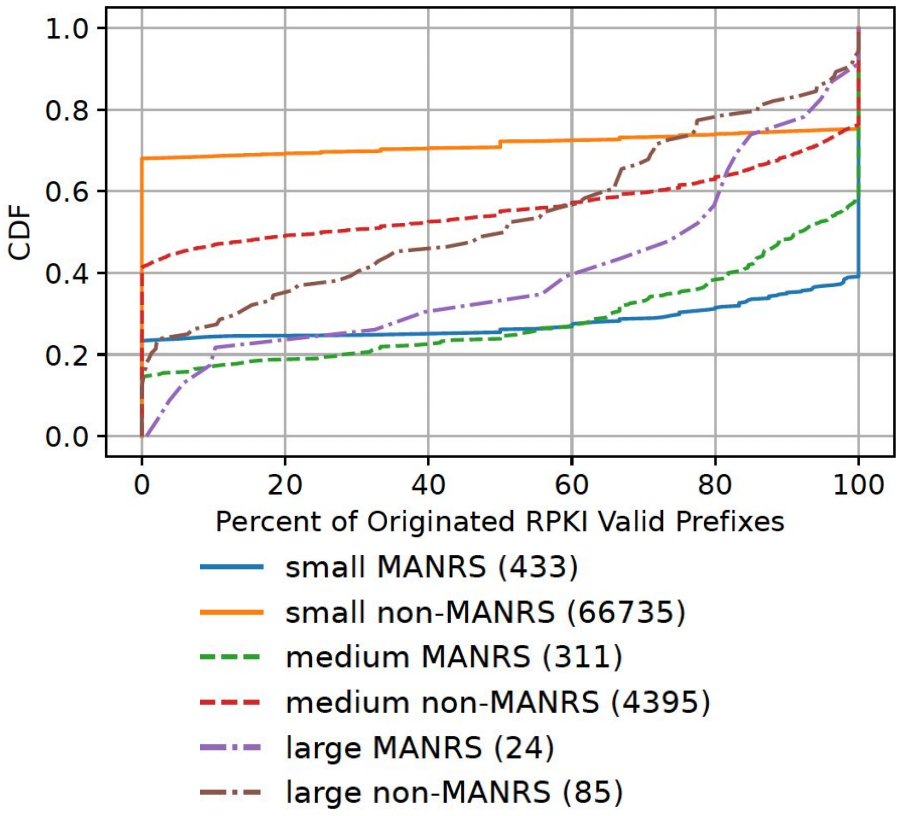
- **Small Networks:** *Customer degree* ≤ 2
- **Medium Networks:** 2 ≤ *Customer degree* ≤ 180
- **Large Networks:** *Customer degree* > 180

AS Customer Degree

- **Small Networks:** *Customer degree* ≤ 2
- **Medium Networks:** 2 ≤ *Customer degree* ≤ 180
- **Large Networks:** *Customer degree* > 180

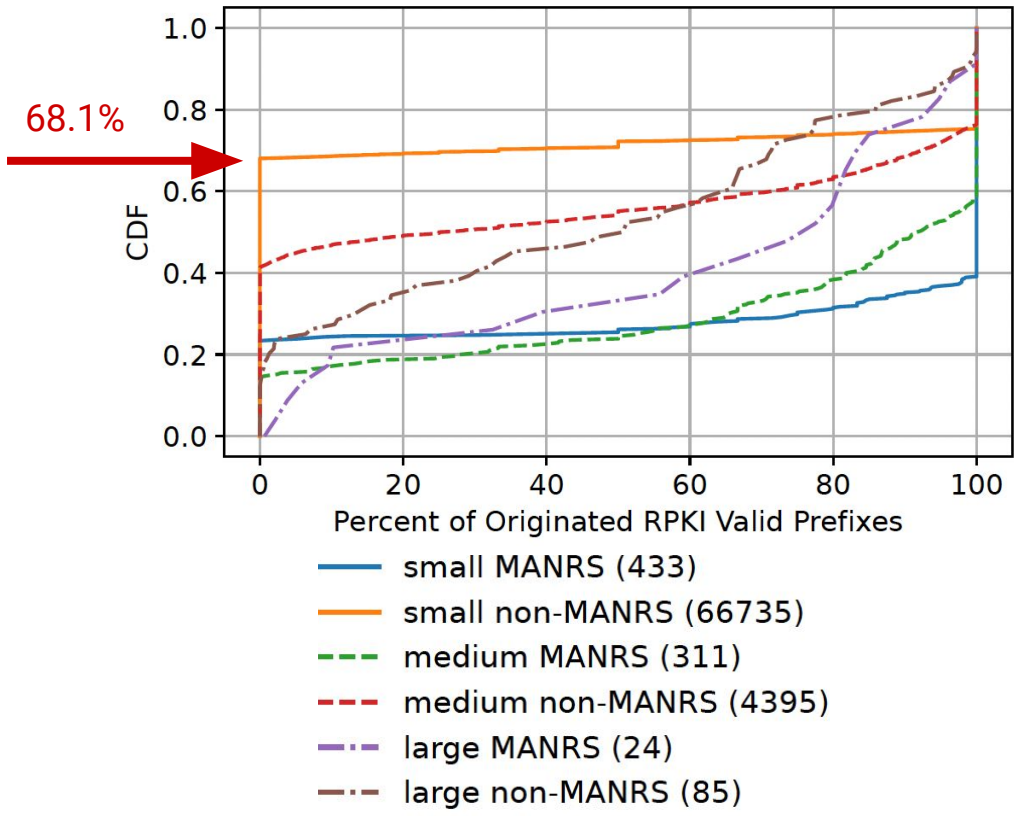
Classification metrics derived from Dhamdhere et. al - *Twelve Years in the Evolution of the Internet Ecosystem*

Conformance - RPKI



CDF of ASes vs percentage of originated RPKI valid prefixes

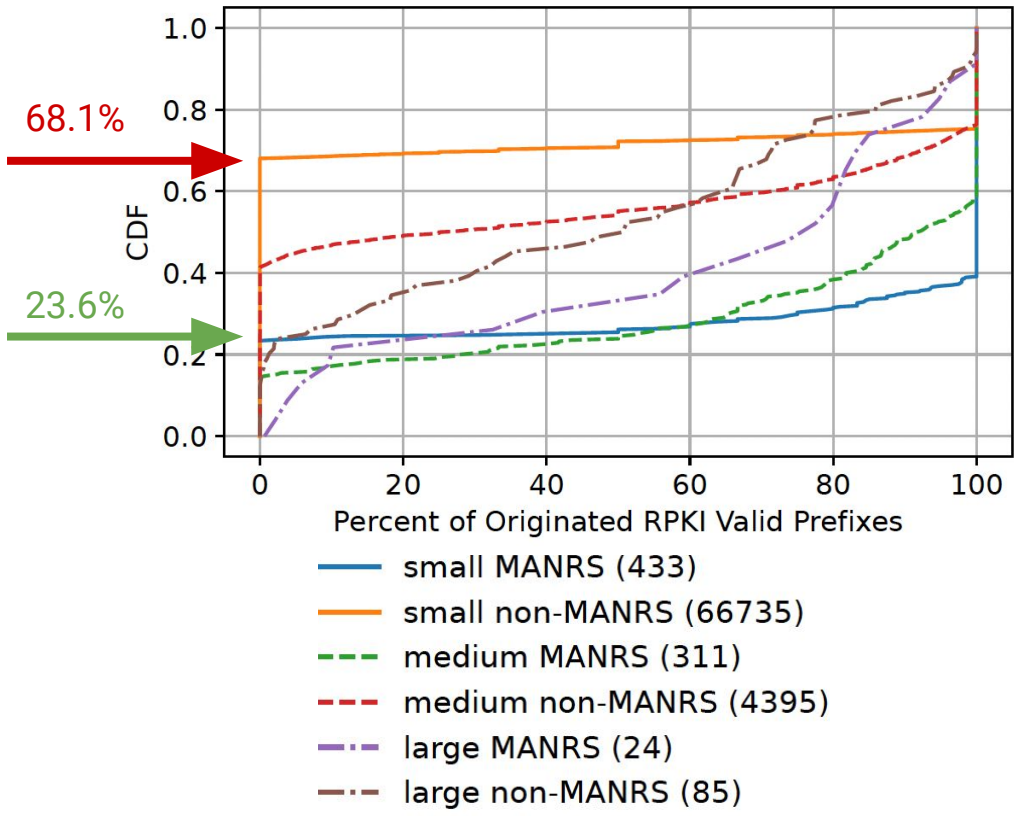
Conformance - RPKI



Percentage of ASes generating only Valid prefixes

- ***Small ASes :*** *24.7% vs 60.1%*
- ***Medium ASes :*** *23.8% vs 41.5%*

Conformance - RPKI



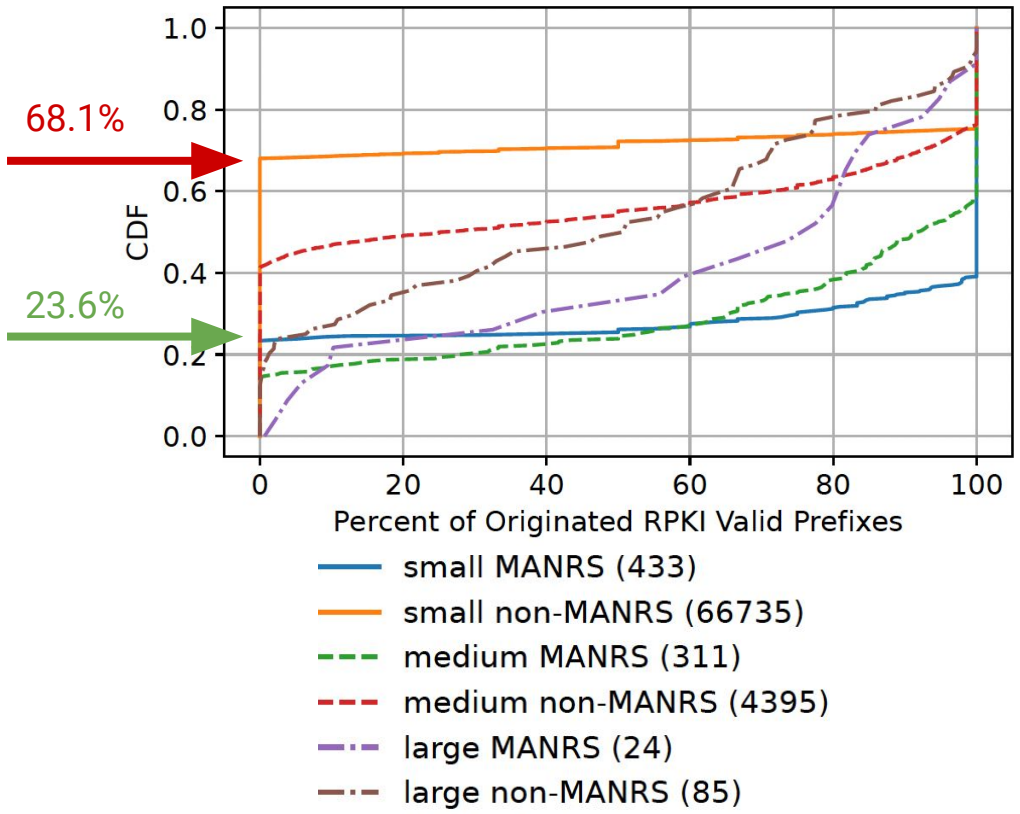
Percentage of ASes generating only Valid prefixes

- ***Small ASes :*** *24.7% vs 60.1%*
- ***Medium ASes :*** *23.8% vs 41.5%*

MANRS *network*

- *twice as likely to originate only RPKI valid prefixes*
- *less likely to originate RPKI invalid prefixes*

Conformance - RPKI



Percentage of ASes generating only Valid prefixes

- ***Small ASes :*** *24.7% vs 60.1%*
- ***Medium ASes :*** *23.8% vs 41.5%*

MANRS *network*

- *twice as likely to originate only RPKI valid prefixes*
- *less likely to originate RPKI invalid prefixes*

Finding : MANRS networks are more likely to register in RPKI !

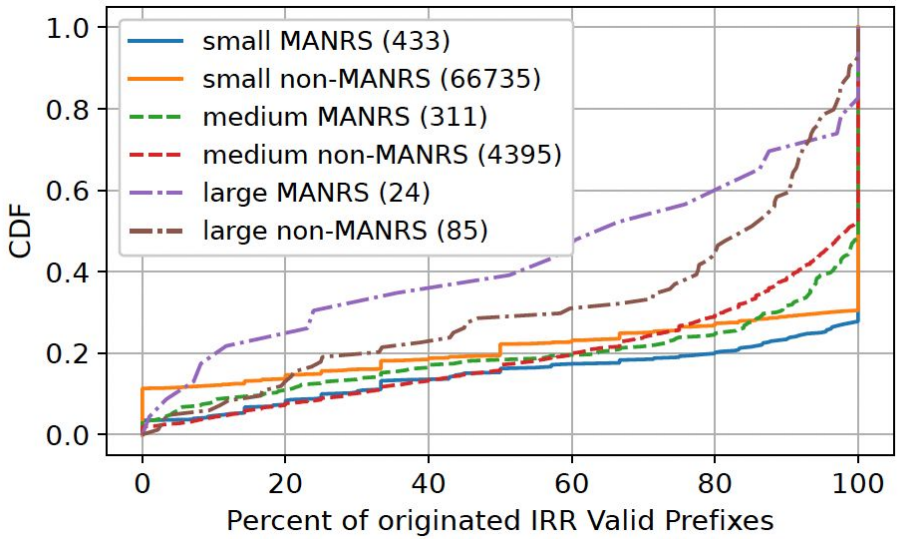
Question

- *Why do we observe a bimodal distribution in small ASes?*

Question

- *Why do we observe a bimodal distribution in small ASes?*
- *“Small MANRS ASes were about 2.5 times more likely to register ROAs.” Why?*

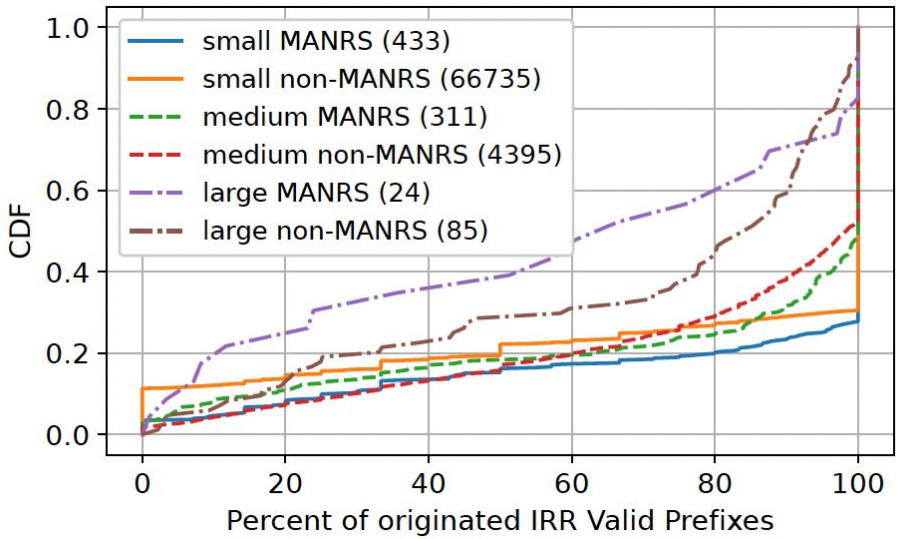
Conformance - IRR



Large ASes

- ***median MANRS AS*** *: 63.5%*
- ***median non-MANRS AS :*** *84%*

Conformance - IRR

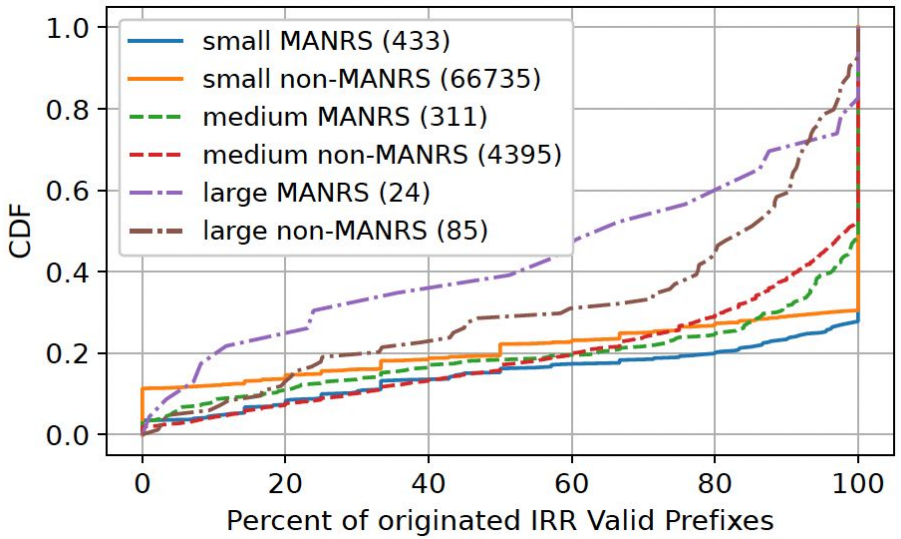


Large ASes

- ***median MANRS AS*** *: 63.5%*
- ***median non-MANRS AS :*** *84%*

Reason?

Conformance - IRR



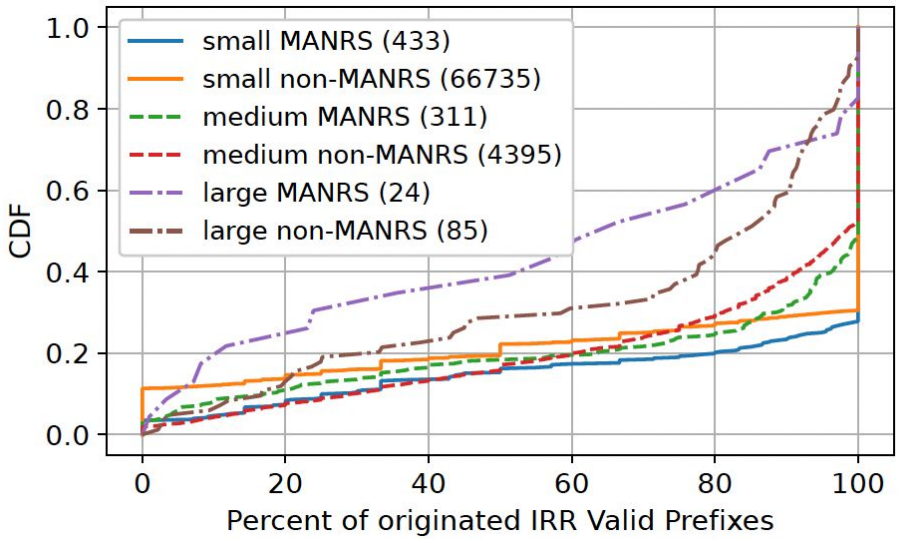
Large ASes

- ***median MANRS AS*** *: 63.5%*
- ***median non-MANRS AS :*** *84%*

Reason?

- *networks that adopt RPKI, do not update IRR records*

Conformance - IRR



Large ASes

- ***median MANRS AS*** *: 63.5%*
- ***median non-MANRS AS :*** *84%*

Reason?

- *networks that adopt RPKI, do not update IRR records*

Finding : Non-MANRS networks are more likely to register only in IRR !

MANRS Actions

Action 4 : Register intended BGP announcements in IRR or RPKI. Using RPKI is recommended.

Action 4 Conformance

CDN - need 100% coverage

- *17/20 CDNs were conformant (1 participant CDN does not announce any prefixes!)*
- *Other CDNs have > 98% coverage*
- *Complicated business relations, hence difficult to get 100% coverage*

Action 4 Conformance

CDN - need 100% coverage

- *17/20 CDNs were conformant (1 participant CDN does not announce any prefixes!)*
- *Other CDNs have > 98% coverage*
- *Complicated business relations, hence difficult to get 100% coverage*

ISPs - need more than 90% coverage

- *5.1% ASes do not conform*
- *These ASes belong to 15 ISPs*
- *Stub ASes of large networks generating less than 3 prefixes*

Case Study

- *Three con-conformant CDNs*
- *Three largest non-conformant ISPs*

	RPKI Invalid (NotFound)	Sibling/C-P	Unrelated	IRR Invalid & RPKI NotFound	Sibling/C-P	Unrelated
CDN1	3	3 (100%)	0	48	38 (79.2%)	10 (20.8%)
CDN2	(1)	0	1 (100%)	0	0	0
CDN3	0	0	0	5	5 (100%)	0
ISP1	1	0	1 (100%)	302	154 (51.0%)	148 (49.0%)
ISP2	8	6 (75.0%)	2 (25.0%)	272	152 (55.9%)	120 (44.1%)
ISP3	1	1 (100%)	0	486	359 (73.9%)	127 (26.1%)

Case Study

- *Most prefix-origins that were not conformant were IRR invalid instead of RPKI Invalid.*
- *RPKI Invalid prefix-origins suffer more visibility reduction in the global routing table*

	RPKI Invalid (NotFound)	Sibling/C-P	Unrelated	IRR Invalid & RPKI NotFound	Sibling/C-P	Unrelated
CDN1	3	3 (100%)	0	48	38 (79.2%)	10 (20.8%)
CDN2	(1)	0	1 (100%)	0	0	0
CDN3	0	0	0	5	5 (100%)	0
ISP1	1	0	1 (100%)	302	154 (51.0%)	148 (49.0%)
ISP2	8	6 (75.0%)	2 (25.0%)	272	152 (55.9%)	120 (44.1%)
ISP3	1	1 (100%)	0	486	359 (73.9%)	127 (26.1%)

Case Study

- *Most prefix-origins that were not conformant were IRR invalid instead of RPKI Invalid.*
- *RPKI Invalid prefix-origins suffer more visibility reduction in the global routing table*
- *Sibling/C-P : using AS2Org Datasets*
  - *Sibling : Two ASes owned by the same organization*
  - *C-P : Customer-Provider relations*

	RPKI Invalid (NotFound)	Sibling/C-P	Unrelated	IRR Invalid & RPKI NotFound	Sibling/C-P	Unrelated
CDN1	3	3 (100%)	0	48	38 (79.2%)	10 (20.8%)
CDN2	(1)	0	1 (100%)	0	0	0
CDN3	0	0	0	5	5 (100%)	0
ISP1	1	0	1 (100%)	302	154 (51.0%)	148 (49.0%)
ISP2	8	6 (75.0%)	2 (25.0%)	272	152 (55.9%)	120 (44.1%)
ISP3	1	1 (100%)	0	486	359 (73.9%)	127 (26.1%)

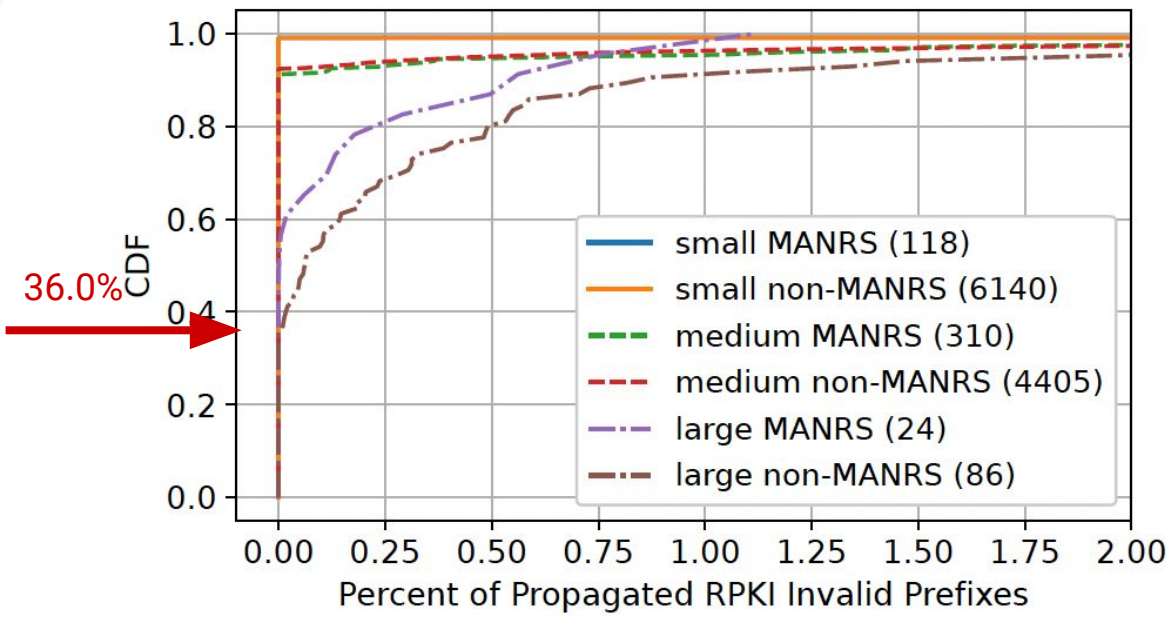
Case Study

- *Most prefix-origins that were not conformant were IRR invalid instead of RPKI Invalid.*
- *RPKI Invalid prefix-origins suffer more visibility reduction in the global routing table*
- *Sibling/C-P : using AS2Org Datasets*
  - *Sibling : Two ASes owned by the same organization*
  - *C-P : Customer-Provider relations*

	RPKI Invalid (NotFound)	Sibling/C-P	Unrelated	IRR Invalid & RPKI NotFound	Sibling/C-P	Unrelated
CDN1	3	3 (100%)	0	48	38 (79.2%)	10 (20.8%)
CDN2	(1)	0	1 (100%)	0	0	0
CDN3	0	0	0	5	5 (100%)	0
ISP1	1	0	1 (100%)	302	154 (51.0%)	148 (49.0%)
ISP2	8	6 (75.0%)	2 (25.0%)	272	152 (55.9%)	120 (44.1%)
ISP3	1	1 (100%)	0	486	359 (73.9%)	127 (26.1%)

Possible misconfigurations?

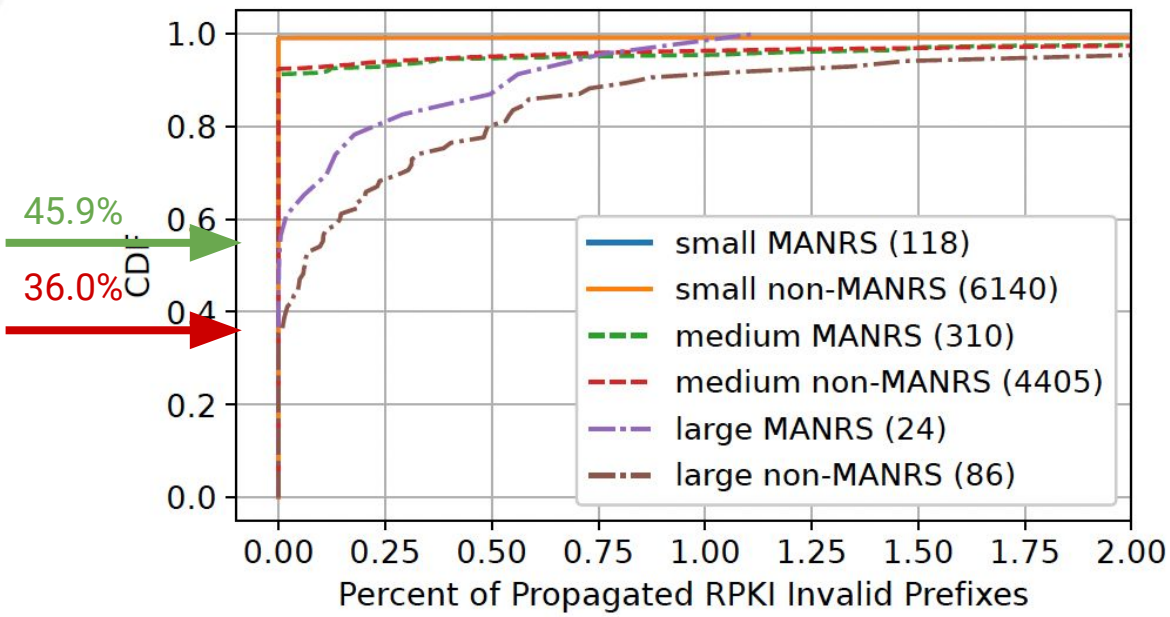
Route Filtering - RPKI



Large ASes

- ***non-MANRS :*** 31/86 (36.0%) ASes propagate no invalid prefixes

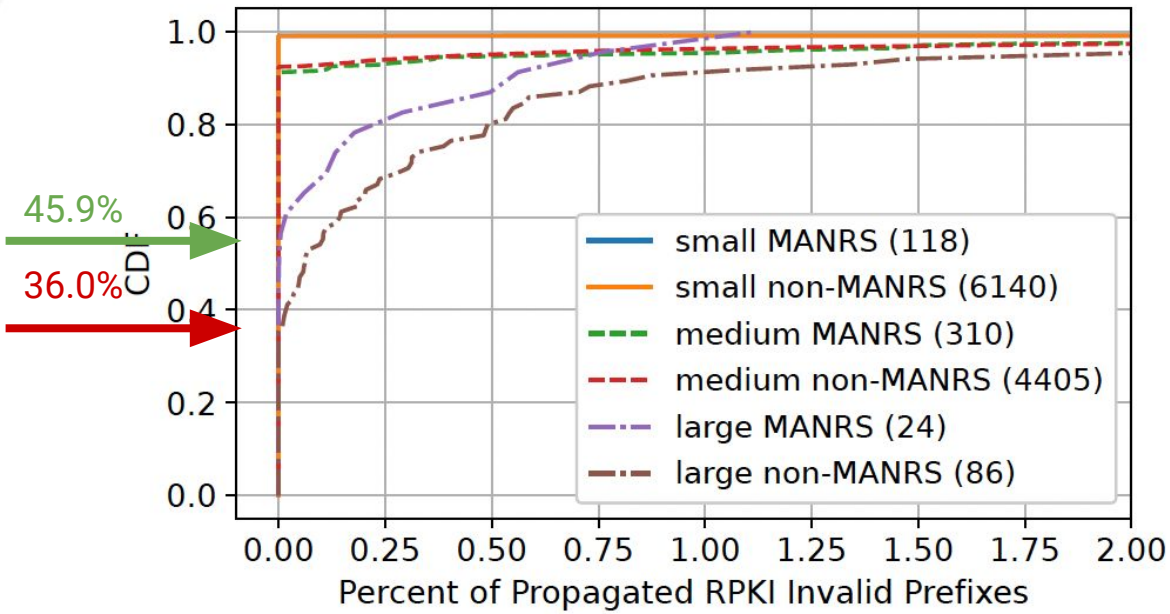
Route Filtering - RPKI



Large ASes

- ***non-MANRS :*** 31/86 (36.0%) ASes propagate no invalid prefixes
- ***MANRS :*** 11/24 (45.9%) ASes propagate no invalid prefixes

Route Filtering - RPKI

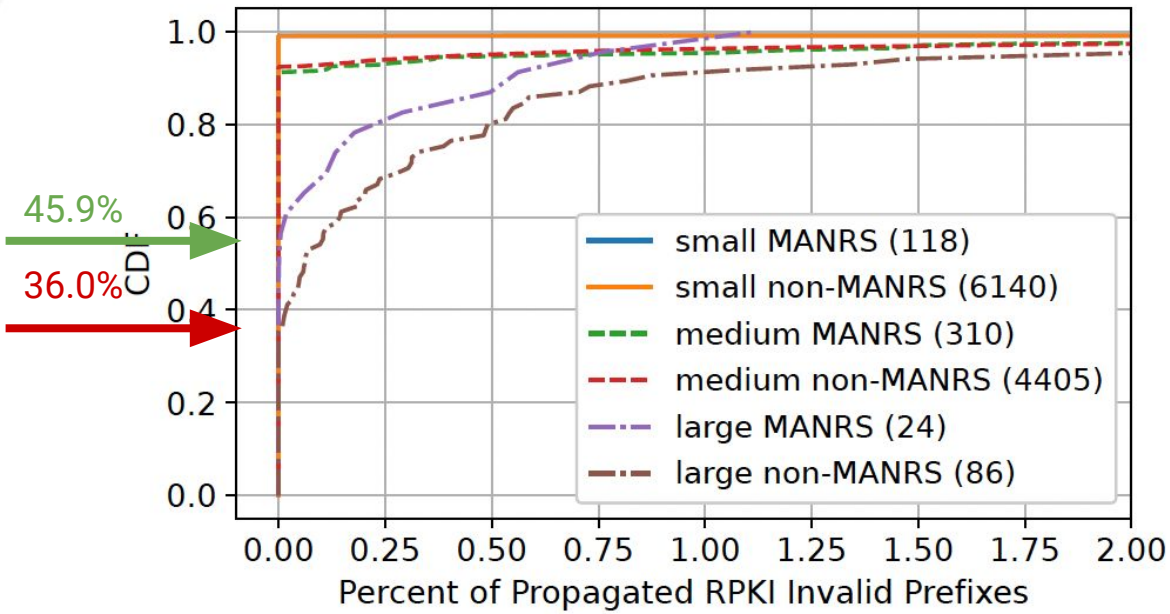


Large ASes

- ***non-MANRS :*** 31/86 (36.0%) ASes propagate no invalid prefixes
- ***MANRS :*** 11/24 (45.9%) ASes propagate no invalid prefixes

Small networks are mostly edge ASes and have almost no customers. They propagate few prefixes in general.

Route Filtering - RPKI



Large ASes

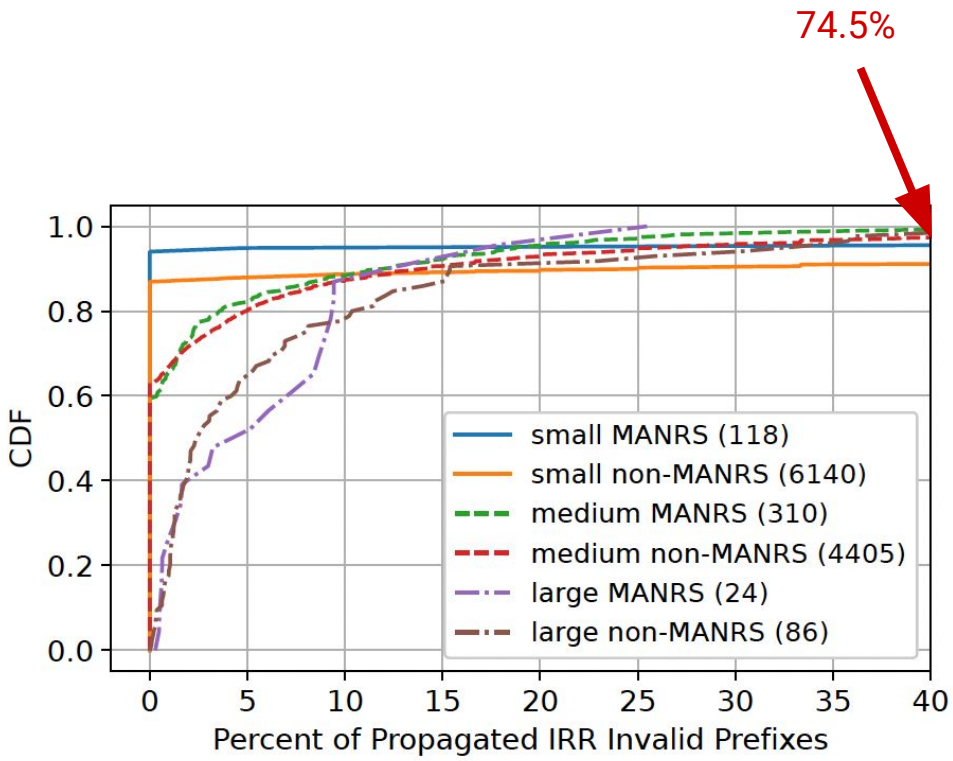
- ***non-MANRS :*** 31/86 (36.0%) ASes propagate no invalid prefixes
- ***MANRS :*** 11/24 (45.9%) ASes propagate no invalid prefixes

Small networks are mostly edge ASes and have almost no customers. They propagate few prefixes in general.

Finding : *Large MANRS ASes were less likely to propagate RPKI invalid announcements compared to non-MANRS ASes*

Georgia Tech

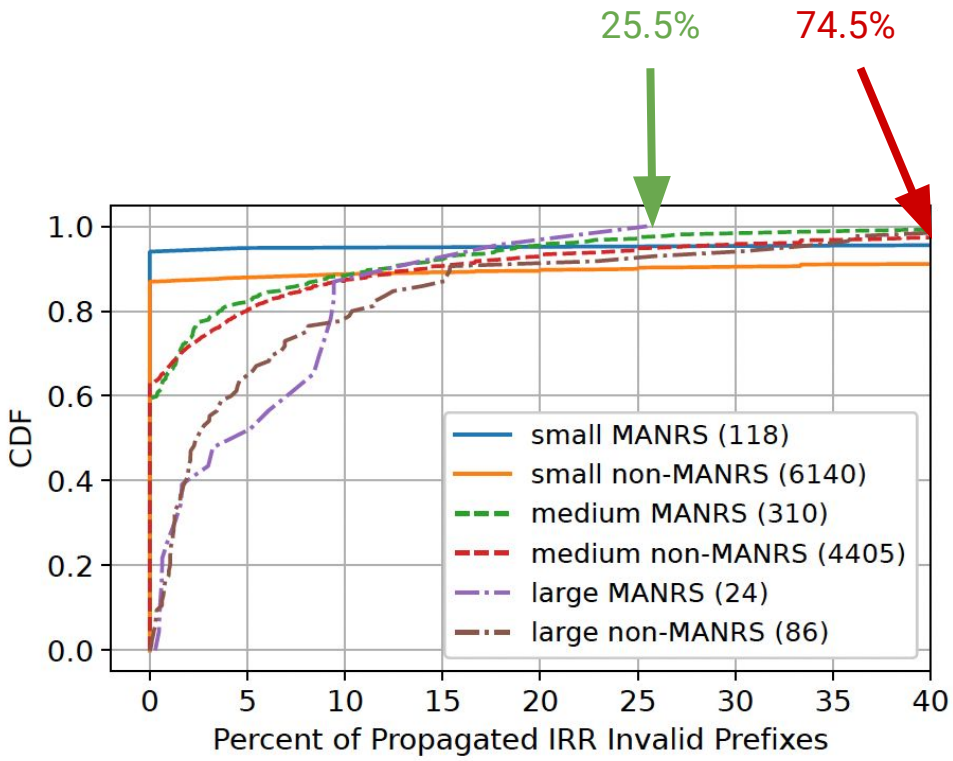
Route Filtering - IRR



Large ASes

- ***non-MANRS :*** Propagate 74.5% IRR Invalid announcements

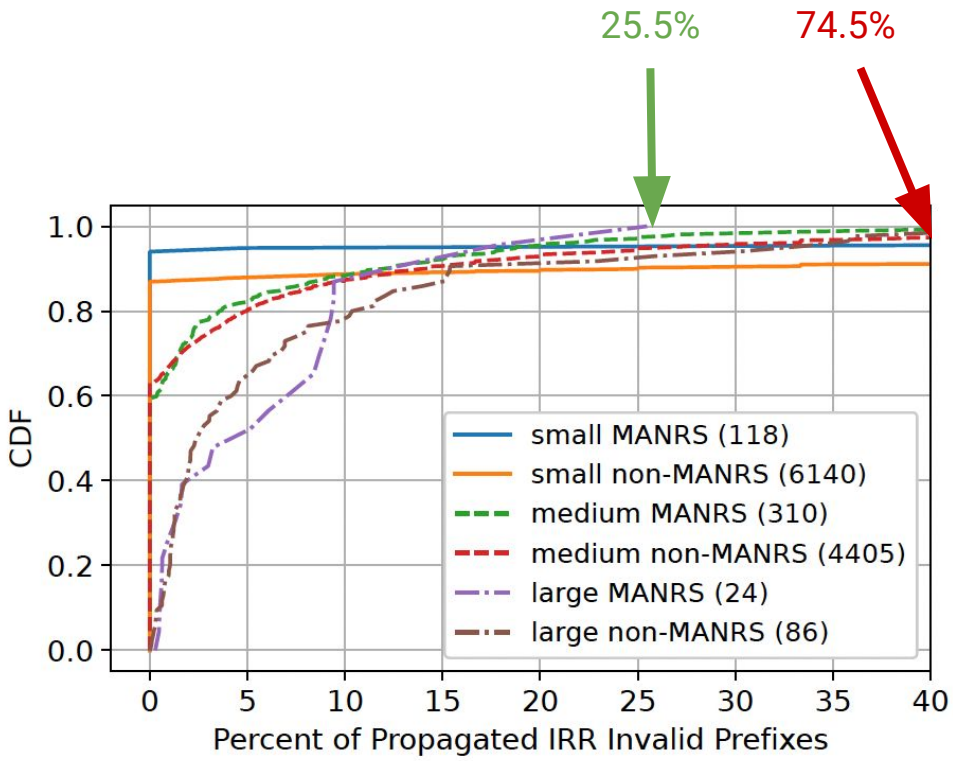
Route Filtering - IRR



Large ASes

- ***non-MANRS :*** Propagate 74.5% IRR Invalid announcements
- ***MANRS :*** Propagate 25.5% IRR invalid announcements

Route Filtering - IRR



Large ASes

- ***non-MANRS :*** Propagate 74.5% IRR Invalid announcements
- ***MANRS :*** Propagate 25.5% IRR invalid announcements

Finding : *Small MANRS ASes were less likely to propagate IRR invalid announcements compared to non-MANRS ASes*

Georgia Tech

More findings

- 83% of MANRS ASes were fully conformant to MANRS Action 1
- MANRS ASes were more likely to be Action 1 conformant

More findings

- 83% of MANRS ASes were fully conformant to MANRS Action 1
- MANRS ASes were more likely to be Action 1 conformant

Action 1 :
Prevent propagation of incorrect routing information

More findings

- 83% of MANRS ASes were fully conformant to MANRS Action 1
- MANRS ASes were more likely to be Action 1 conformant
- RPKI Invalid BGP prefixes were more likely to propagate through non-MANRS networks

Action 1 :
Prevent propagation of incorrect routing information

More findings

- 83% of MANRS ASes were fully conformant to MANRS Action 1
- MANRS ASes were more likely to be Action 1 conformant
- **RPKI Invalid BGP prefixes were more likely to propagate through non-MANRS networks**

Action 1 :
Prevent propagation of incorrect routing information

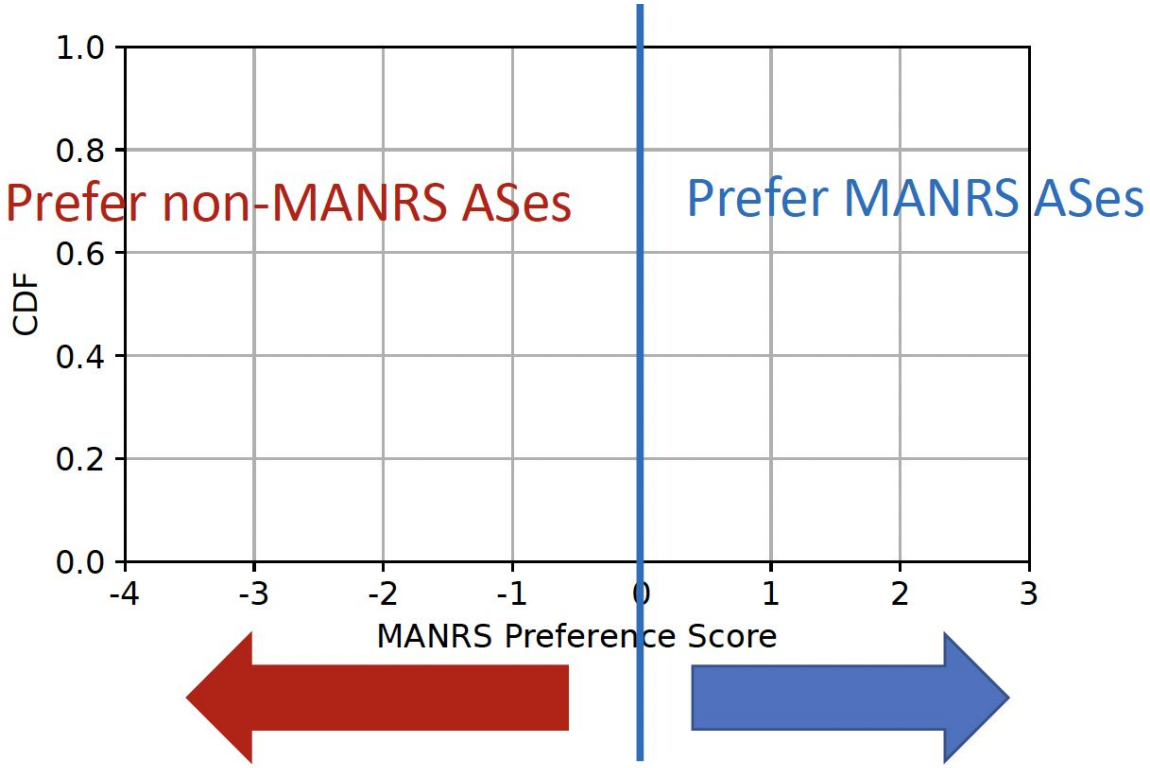
MANRS Preference Score

Hegemony Metric: the fraction of AS paths that transit a given AS to reach a specified set of address space

$$PS_k^{MANRS} = \sum_{i=1}^{m} AS_i^{MANRS} - \sum_{j=1}^{n} AS_j^{XMANRS}$$

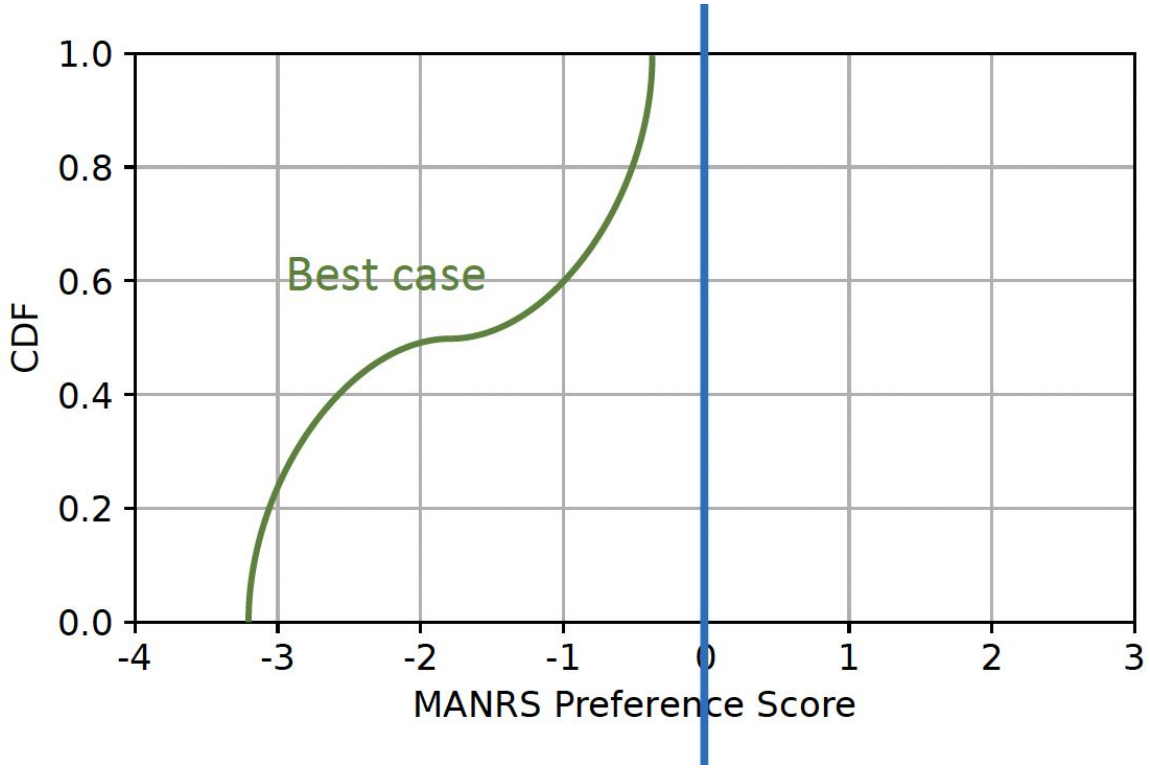
- PS_k^{MANRS} : MANRS preference score
- AS_i^{MANRS} : Hegemony score of ith MANRS AS
- AS_i^{XMANRS}: Hegemony score of ith non-MANRS AS

MANRS Preference Score



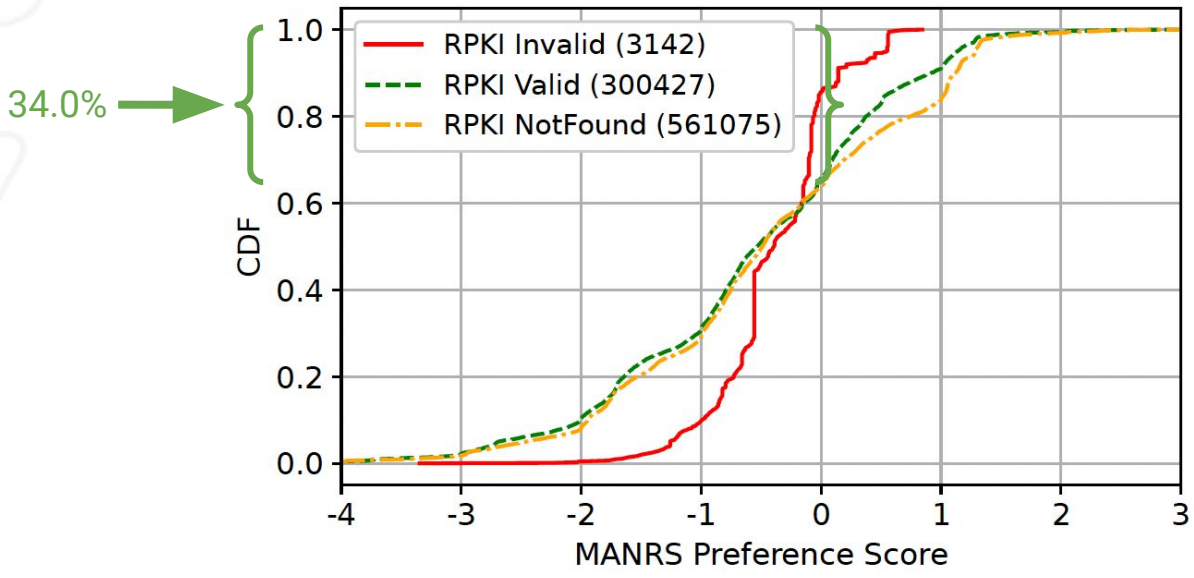
Source : https://www.caida.org/catalog/media/2022_mind_your_manrs_imc/mind_your_manrs_imc.pdf

MANRS Preference Score



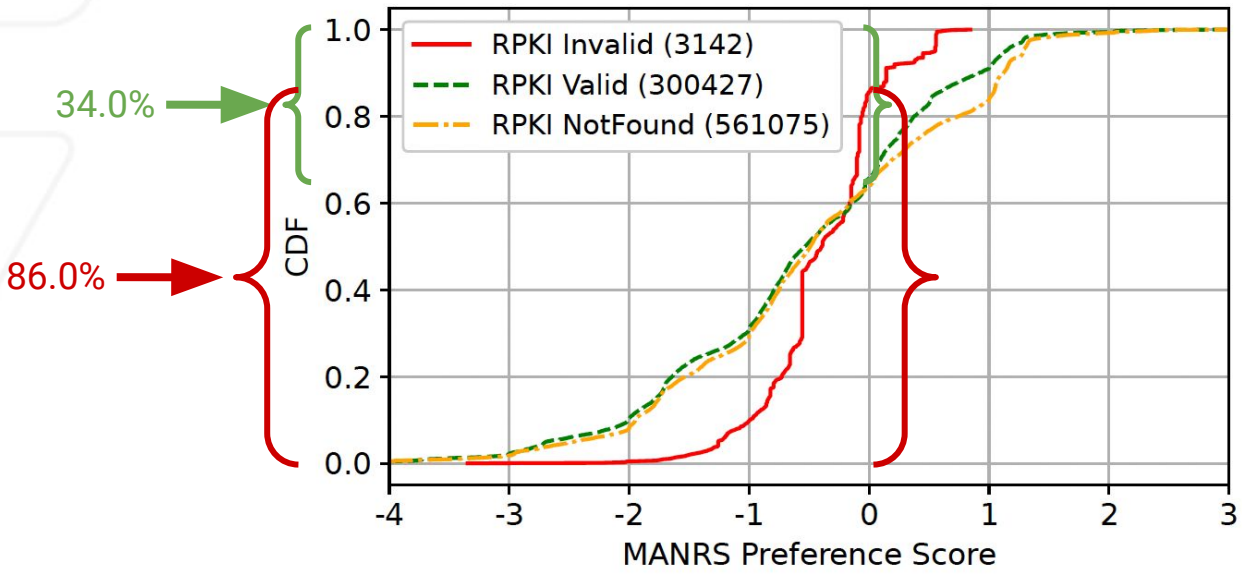
Source : https://www.caida.org/catalog/media/2022_mind_your_manrs_imc/mind_your_manrs_imc.pdf

RPKI Filtering Effectiveness



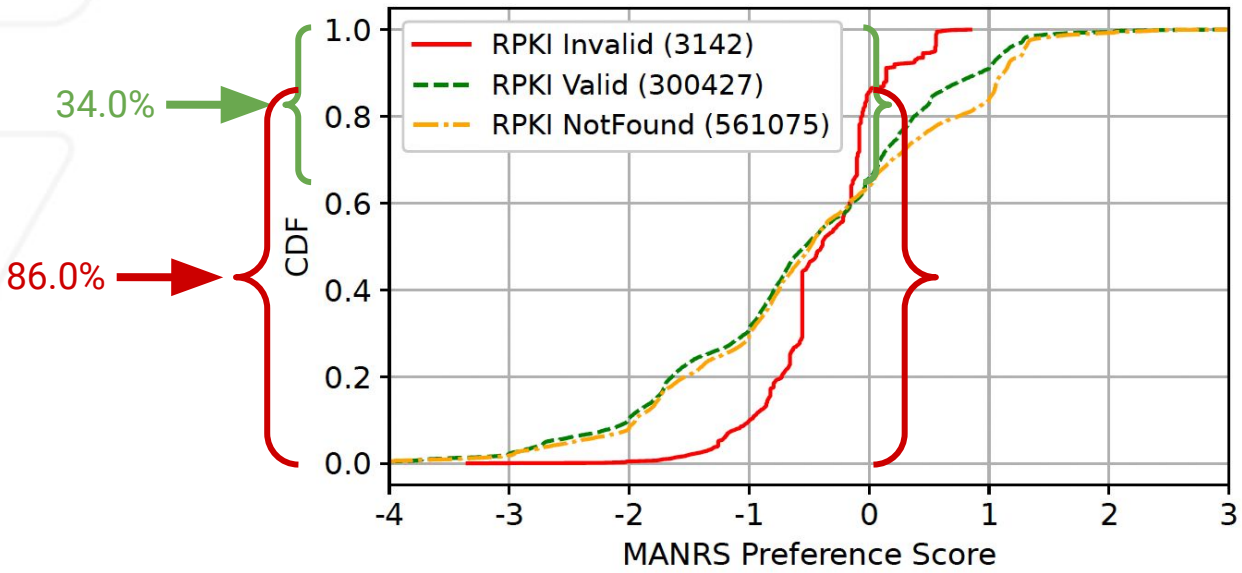
- ***Valid prefixes :*** 34% preferred to transit via MANRS ASes

RPKI Filtering Effectiveness



- ***Valid prefixes :*** 34% preferred to transit via MANRS ASes
- ***Invalid prefixes :*** 14% preferred to transit via MANRS ASes

RPKI Filtering Effectiveness



- ***Valid prefixes :*** 34% preferred to transit via MANRS ASes
- ***Invalid prefixes :*** 14% preferred to transit via MANRS ASes

Finding : *RPKI Invalid announcements were more likely to propagate through non-MANRS networks*

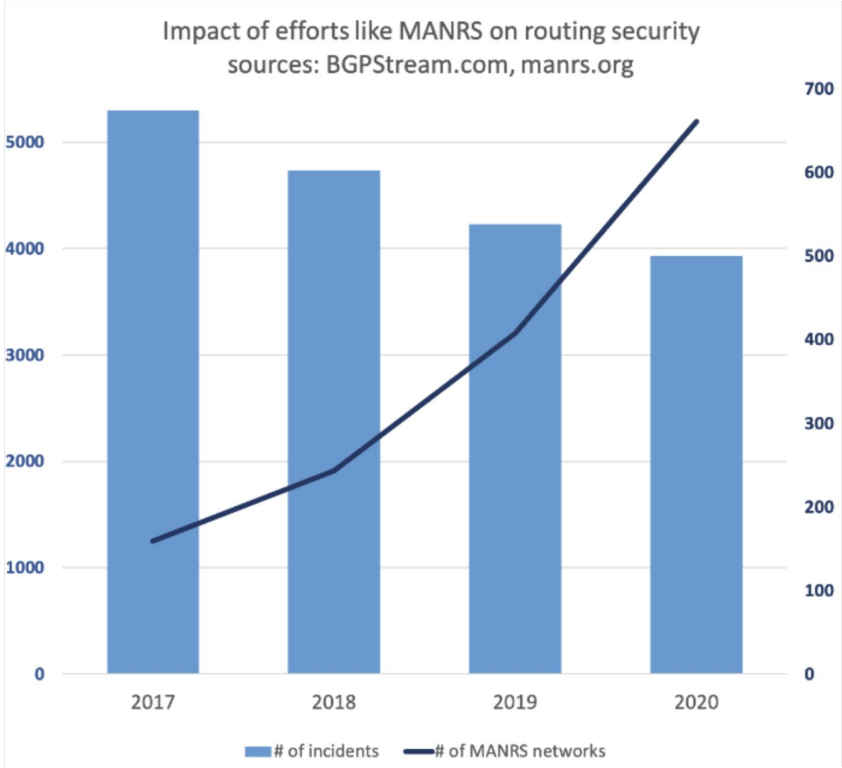
Georgia Tech

Future Work

- Study the impact of MANRS by comparing the number of routing incidents before and after the launch of MANRS
- Extending this study to actions that are not related to routing and to other MANRS programs such as the IXP program

Conclusion

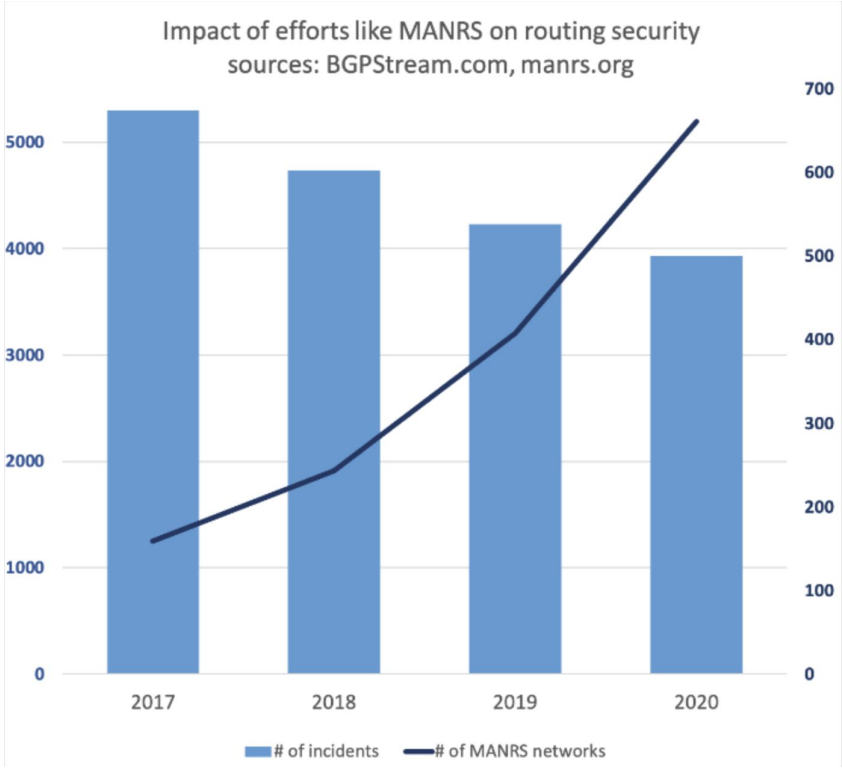
- MANRS participation



https://www.manrs.org/resources/community-report-2020/

Conclusion

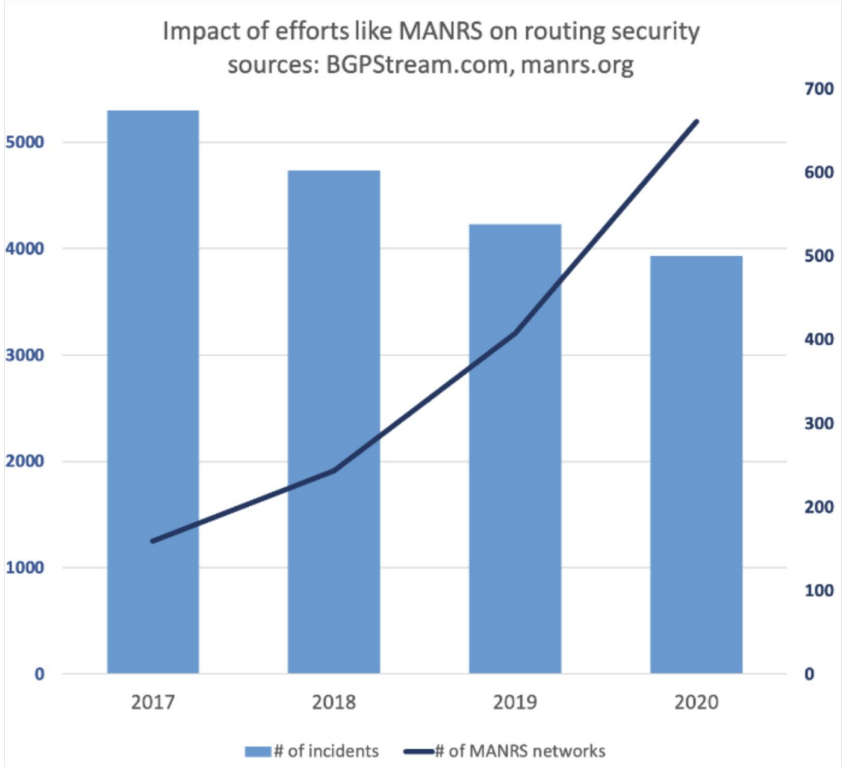
- MANRS participation
- MANRS members are more likely to register and maintain routing objects in comparison to non-MANRS members



https://www.manrs.org/resources/community-report-2020/

Conclusion

- MANRS participation
- MANRS members are more likely to register and maintain routing objects in comparison to non-MANRS members
- Invalid prefixes are preferentially routed through non-MANRS networks



https://www.manrs.org/resources/community-report-2020/

Thank You!