Tracing RPKI Invalid Propagation using IYP & Scamper

DEEPAK GOUDA | GEORGIA TECH
ROMAIN FONTUGNE | IIJ

2025-02-11

PROPAGATION OF RPKI INVALIDS

- 1.05% of routed IPv4 prefixes are RPKI Invalid [1]
- 22.3% of Autonomous Systems are fully protected from invalid announcements [2]

[1] https://rpki-monitor.antd.nist.gov

[2] https://rovista.netsecurelab.org/analytics

PROPAGATION OF RPKI INVALIDS

- 1.05% of routed IPv4 prefixes are RPKI Invalid [1]
- 22.3% of Autonomous Systems are fully protected from invalid announcements [2]
- **Route Origin Validation** - reject RPKI invalid announcements

[1] https://rpki-monitor.antd.nist.gov

[2] https://rovista.netsecurelab.org/analytics

PROPAGATION OF RPKI INVALIDS

- 1.05% of routed IPv4 prefixes are RPKI Invalid [1]
- 22.3% of Autonomous Systems are fully protected from invalid announcements [2]
- **Route Origin Validation** - reject RPKI invalid announcements

(actual routing decisions differ)

[1] https://rpki-monitor.antd.nist.gov

[2] https://rovista.netsecurelab.org/analytics

PROPAGATION OF RPKI INVALIDS

- 1.05% of routed IPv4 prefixes are RPKI Invalid [1]
- 22.3% of Autonomous Systems are fully protected from invalid announcements [2]
- **Route Origin Validation** - reject RPKI invalid announcements

  (actual routing decisions differ)
- RPKI invalid prefixes have lower visibility [3]

[1] https://rpki-monitor.antd.nist.gov

[2] https://rovista.netsecurelab.org/analytics

[3] To Filter or not to Filter: Measuring the Benefits of Registering in the RPKI Today

PROPAGATION OF RPKI INVALIDS

- 1.05% of routed IPv4 prefixes are RPKI Invalid [1]
- 22.3% of Autonomous Systems are fully protected from invalid announcements [2]
- **Route Origin Validation** - reject RPKI invalid announcements
  (actual routing decisions differ)
- RPKI invalid prefixes have lower visibility [3]

Q1: Verify if RPKI Invalid prefixes have more hops, higher RTT

Q2: Do ASes in RoVista dataset drop all invalids?

[1] https://rpki-monitor.antd.nist.gov

[2] https://rovista.netsecurelab.org/analytics

[3] To Filter or not to Filter: Measuring the Benefits of Registering in the RPKI Today

METHODOLOGY

1. Find RPKI Invalid prefixes on BGP **- Internet Yellow Pages**
2. Find active hosts in the prefix **- Internet Yellow Pages**
3. Perform traceroutes from multiple vantage points
    a. Intermediate IPs
    b. RTT **- Scamper**
    c. Hops

Control : Perform RTT measurement for RPKI valid prefixes originated from same AS

RESULTS

- Percentage of Traceroutes reaching the destination
    - RPKI Invalid - **25.7%**
    - RPKI Valid - **50.2%**
- **70.6%** RPKI invalids have higher number of intermediate hops
- **72.5%** RPKI invalids have higher RTT

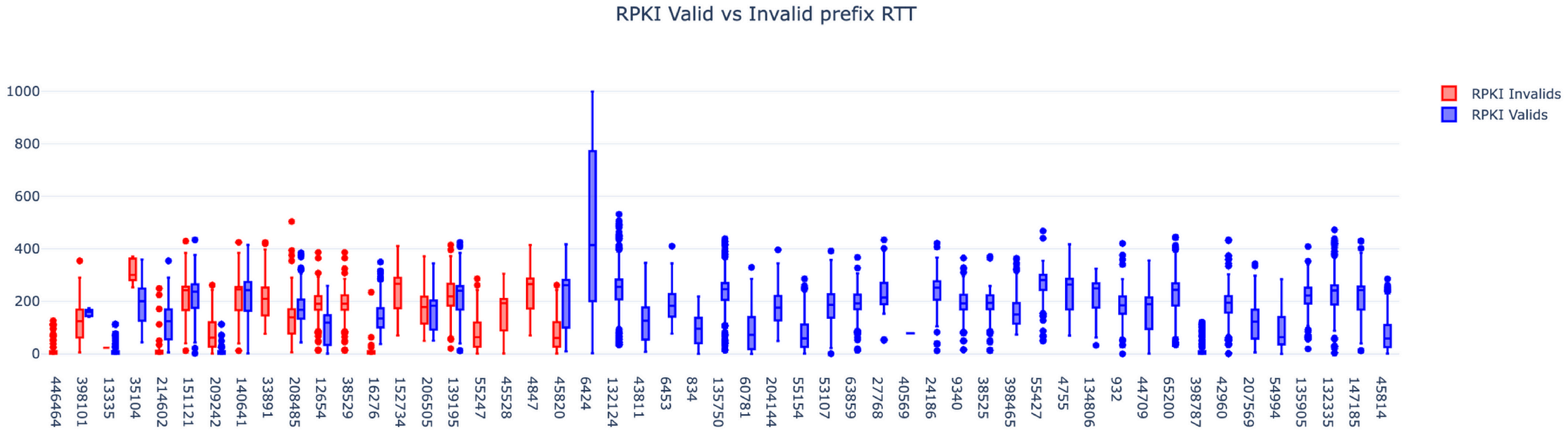
RESULTS

- Percentage of Traceroutes reaching the destination
  - RPKI Invalid - **25.7%**
  - RPKI Valid - **50.2%**
- **70.6%** RPKI invalids have higher number of intermediate hops
- **72.5%** RPKI invalids have higher RTT

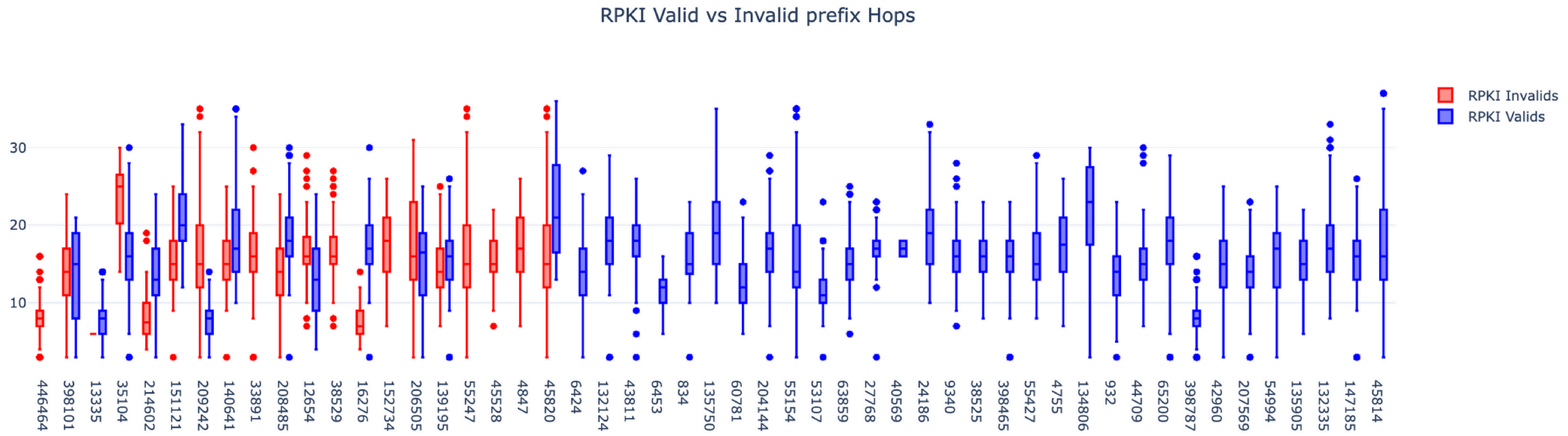
Cloudflare

- RPKI Invalid
  - Completion Rate - **0.67%**
  - Mean RTT - **27.5 ms**
- RPKI Valid
  - Completion Rate - **99.26%**
  - Mean RTT - **8 ms**

RTT


RPKI Valid vs Invalid prefix RTT
RPKI Invalids
RPKI Valids
1000
800
600
400
200
0
446464
398101
13335
35104
214602
151121
209242
140641
33891
208485
12654
38529
16276
152734
206505
139195
55247
45528
4847
45820
6424
132124
43811
6453
834
135750
60781
204144
55154
53107
63859
27768
40569
24186
9340
38525
398465
55427
4755
134806
932
44709
65200
398787
42960
207569
54994
135905
132335
147185
45814

HOPS


RPKI Valid vs Invalid prefix Hops
RPKI Invalids
RPKI Valids
30
20
10
446464
398101
13335
35104
214602
151121
209242
140641
33891
208485
12654
38529
16276
152734
206505
139195
55247
45528
4847
45820
6424
132124
43811
6453
834
135750
60781
204144
55154
53107
63859
27768
40569
24186
9340
38525
398465
55427
4755
134806
932
44709
65200
398787
42960
207569
54994
135905
132335
147185
45814

TESTING ROVISTA

- We remove RPKI invalids with an RPKI Valid/NotFound covering prefix
- If we are able to traceroute RPKI Invalids, **no intermediate ASes are dropping invalids**
- Methodology
  - Map IP to prefix and prefix to ASN **- Internet Yellow Pages**
  - Check if intermediate ASes perform ROV **- Internet Yellow Pages**

OBSERVATION

- Traceroute to 103.21.244.12 from UCSD goes through CENIC and Cloudflare

OBSERVATION

- Traceroute to 103.21.244.12 from UCSD goes through CENIC and Cloudflare
- **Cloudflare**
  - RoVista : ROV Filtering Ratio - upto 100%
  - They own the prefix, they originate it!
  - So, testing? isbgpsafeyet?

OBSERVATION

- Traceroute to 103.21.244.12 from UCSD goes through CENIC and Cloudflare
- **Cloudflare**
  - RoVista : ROV Filtering Ratio - upto 100%
  - They own the prefix, they originate it!
  - So, testing? isbgpsafeyet?
- **CENIC**
  - RoVista : ROV Filtering Ratio - 66%
  - Our observation : Not dropping invalids

OBSERVATION

- Traceroute to 103.21.244.12 from UCSD goes through CENIC and Cloudflare
- **Cloudflare**
  - RoVista : ROV Filtering Ratio - upto 100%
  - They own the prefix, they originate it!
  - So, testing? isbgpsafeyet?
- **CENIC**
  - RoVista : ROV Filtering Ratio - 66%
  - Our observation : Not dropping invalids

We can use Scamper to test ROV policies of ASes!

Questions?

Backup Slides

OBSERVATION

- Traceroute to 103.21.244.12 goes through CENIC and Cloudflare
- **Cloudflare**
  - RoVista ✅
  - They own the prefix
  - So, testing? isbgpsafeyet?
- **CENIC**
  - RoVista ✅
  - Not dropping invalids from Cloudflare

We can use Scamper to test ROV policies of ASes!

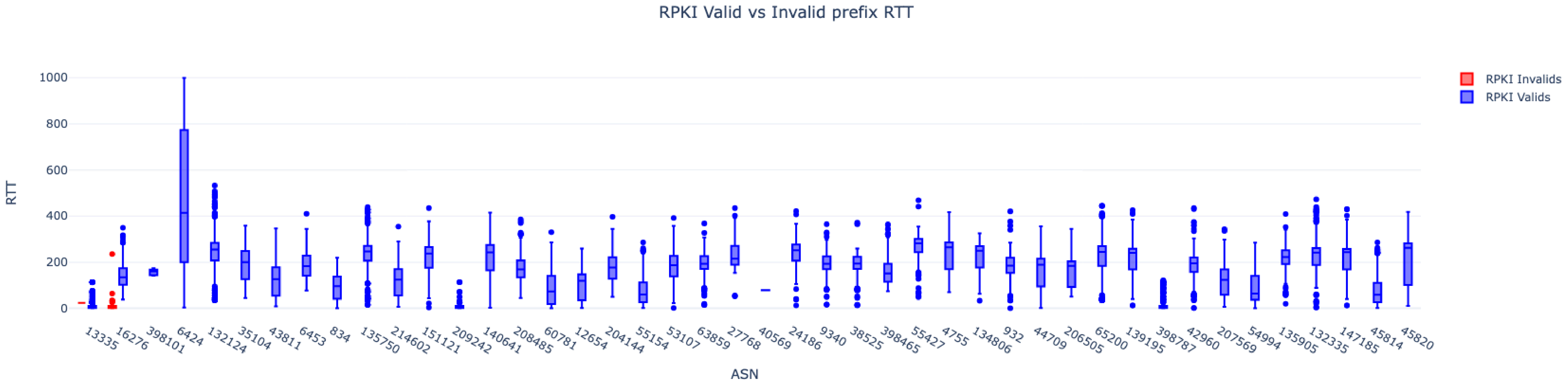
RESULTS

- Completion rate
  - RPKI Invalid - **0.9%**
  - RPKI Valid - **58.2%**
- **95.5%** RPKI invalids have higher number of intermediate hops
- **97.8%** RPKI invalids have higher RTT

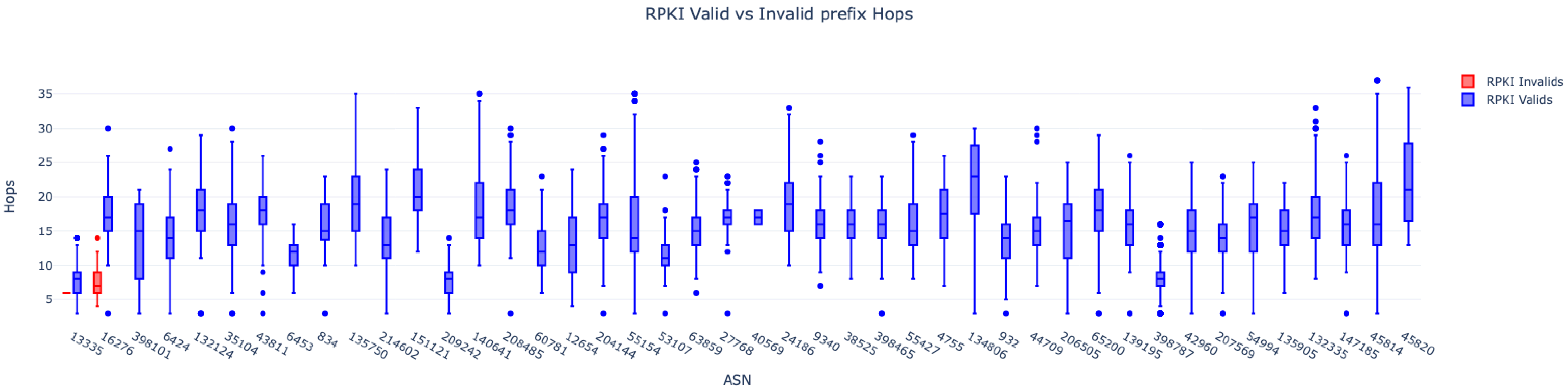
Cloudflare

- RPKI Invalid
  - Completion Rate - **0.8%**
  - Mean RTT - **24 ms**
- RPKI Valid
  - Completion Rate - **98.1%**
  - Mean RTT - **8 ms**

RTT


RPKI Valid vs Invalid prefix RTT
RTT
1000
800
600
400
200
0
ASN
13335
16276
398101
6424
132124
35104
43811
6453
834
135750
214602
151121
209242
140641
208485
60781
12654
204144
55154
53107
63859
27768
40569
24186
9340
38525
398465
55427
4755
134806
932
44709
206505
65200
139195
398787
42960
207569
54994
135905
132335
147185
45814
45820
🟥 RPKI Invalids
🟦 RPKI Valids

HOPS


RPKI Valid vs Invalid prefix Hops
Hops
35
30
25
20
15
10
5
ASN
13335
16276
398101
6424
132124
35104
43811
6453
834
135750
214602
151121
209242
140641
208485
60781
12654
204144
55154
53107
63859
27768
40569
24186
9340
38525
398465
55427
4755
134806
932
44709
206505
65200
139195
398787
42960
207569
54994
135905
132335
147185
45814
45820
RPKI Invalids
RPKI Valids