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

Passive and Active Measurement Conference 2020

Cecilia Testart
MIT

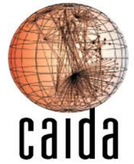
Philipp Richter
MIT

Alistair King
CAIDA, UC San Diego

Alberto Dainotti
CAIDA, UC San Diego

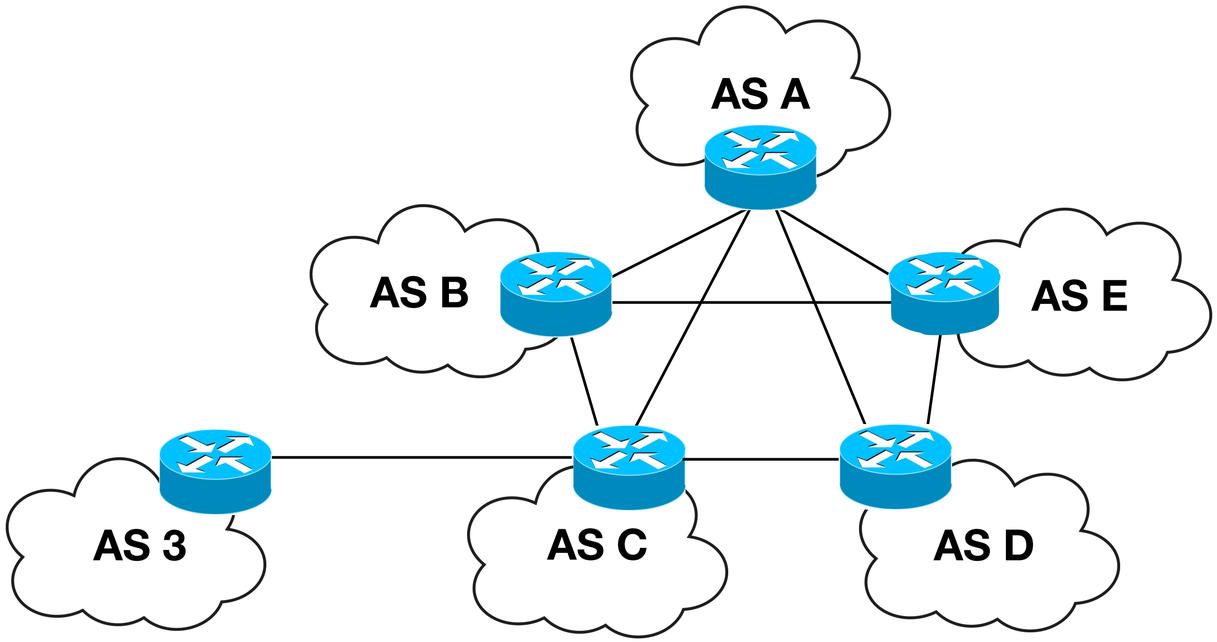
David Clark
MIT

Internet Policy Research Initiative
Massachusetts Institute of Technology

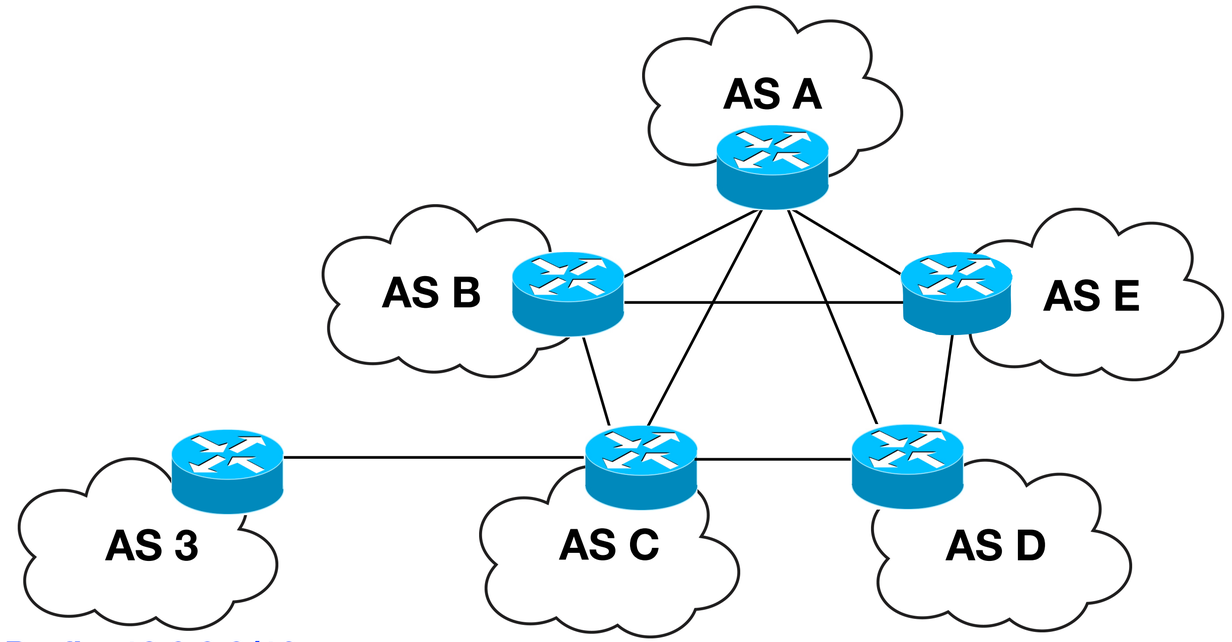


UC San Diego

The Border Gateway Protocol (BGP)

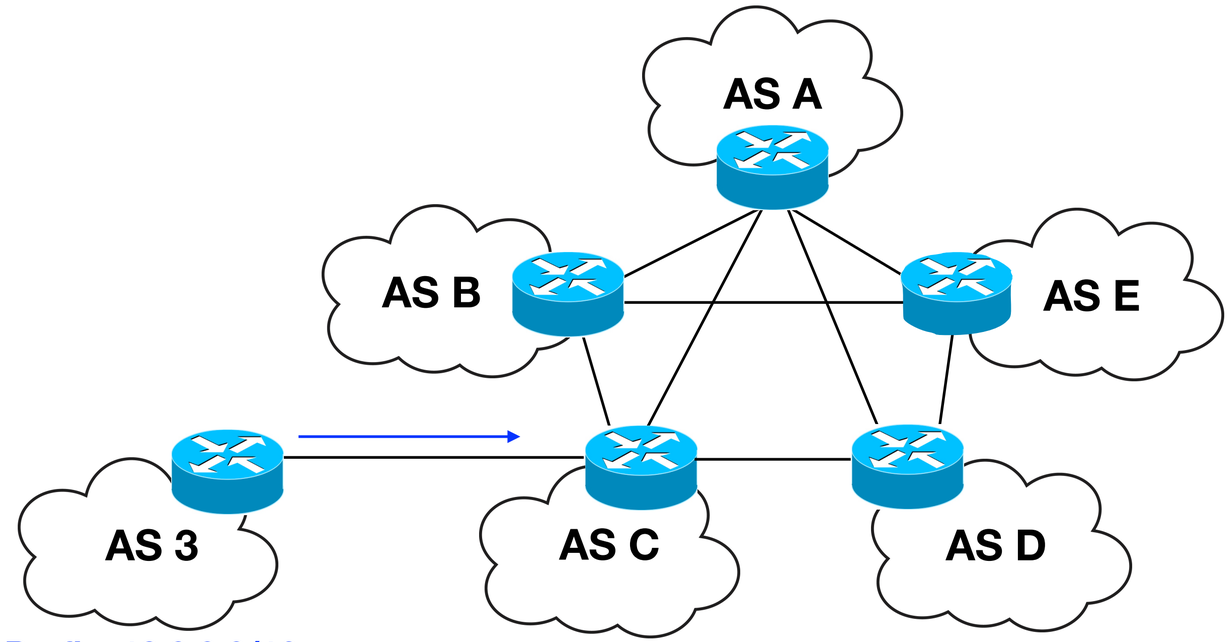


The Border Gateway Protocol (BGP)

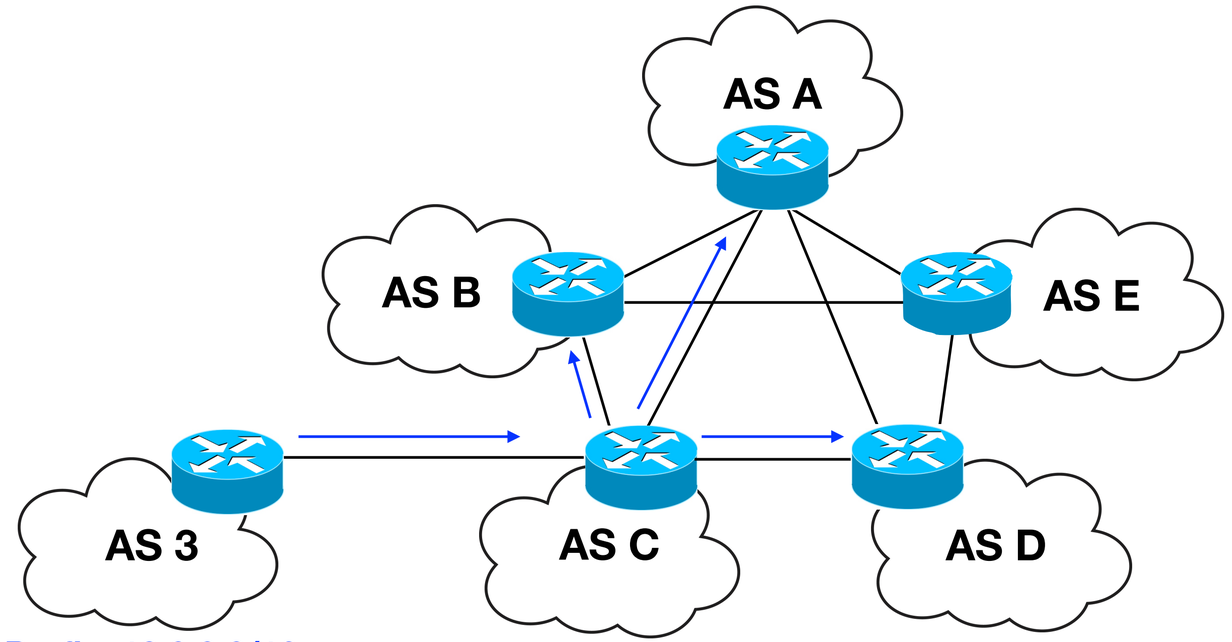


Prefix: 18.0.0.0/16
Origin: AS 3

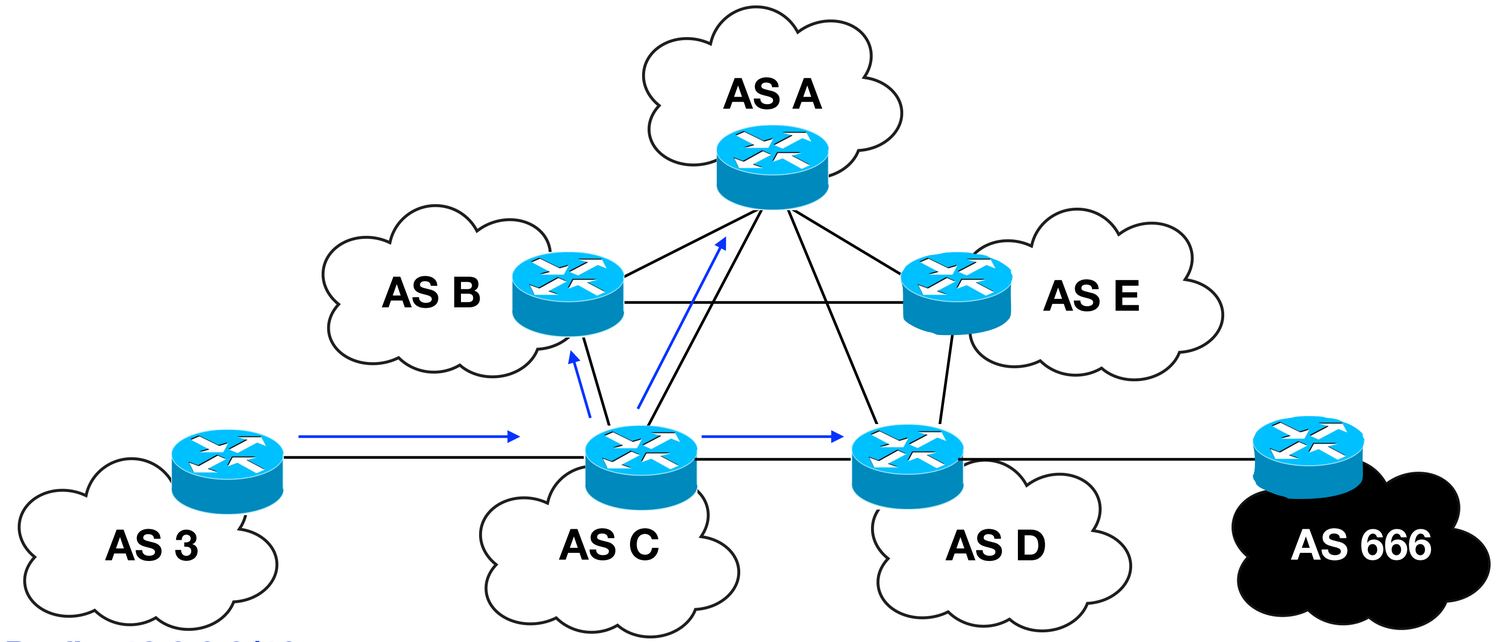
The Border Gateway Protocol (BGP)



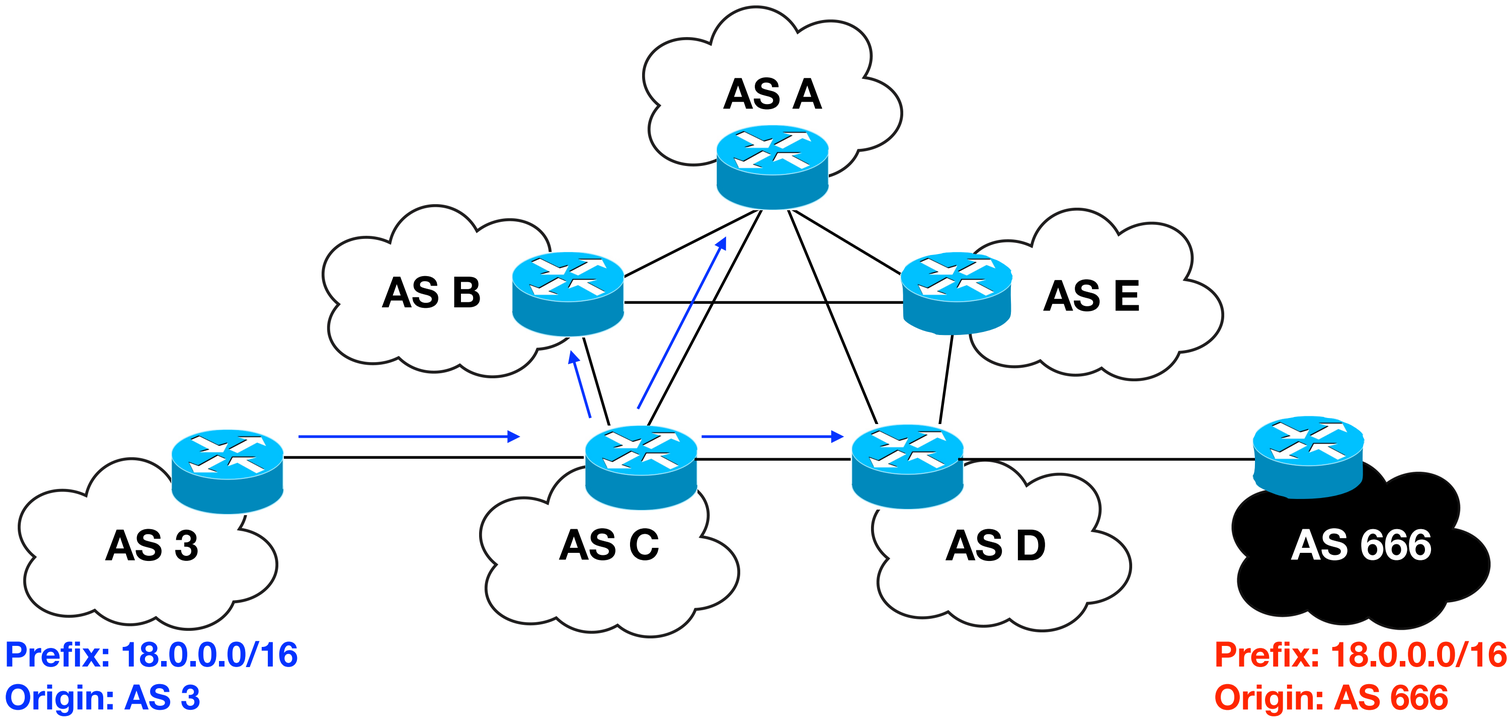
The Border Gateway Protocol (BGP)



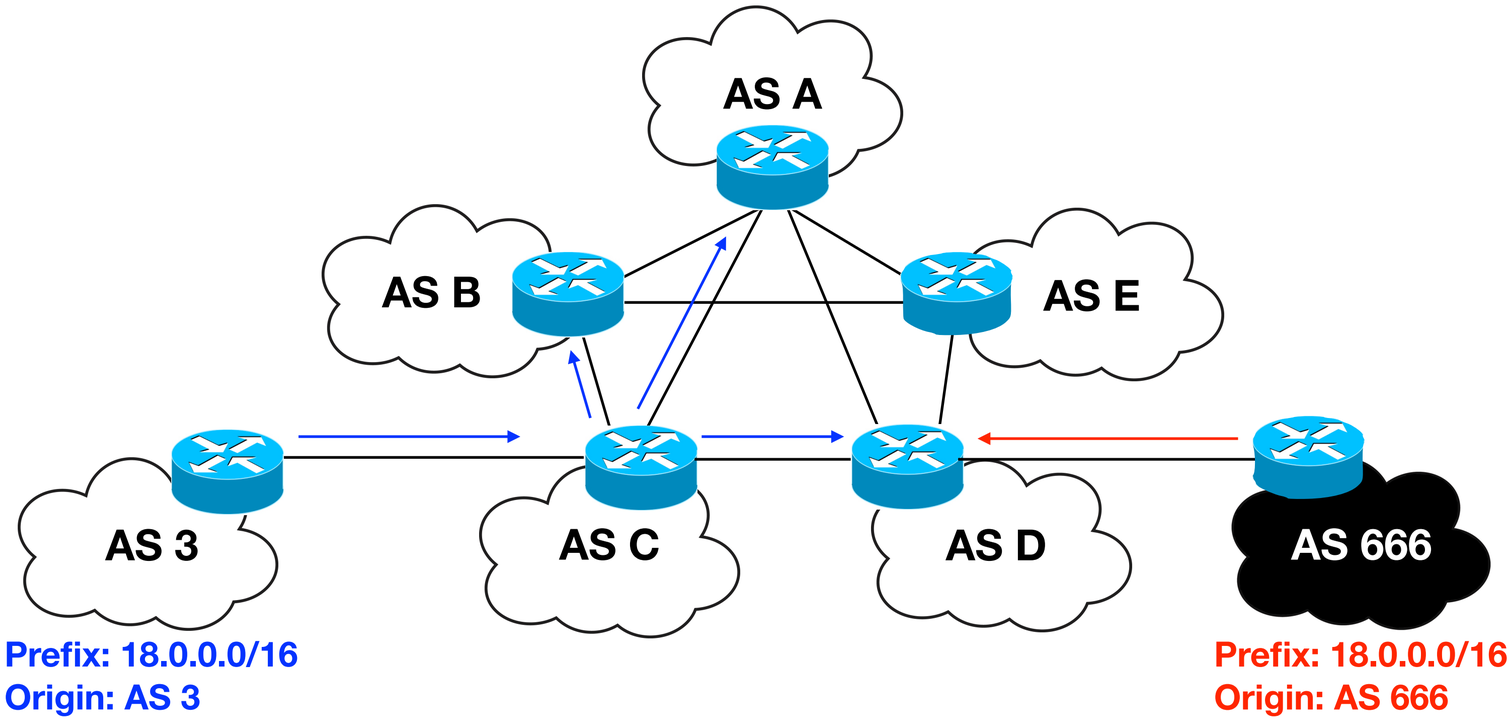
The Border Gateway Protocol (BGP)



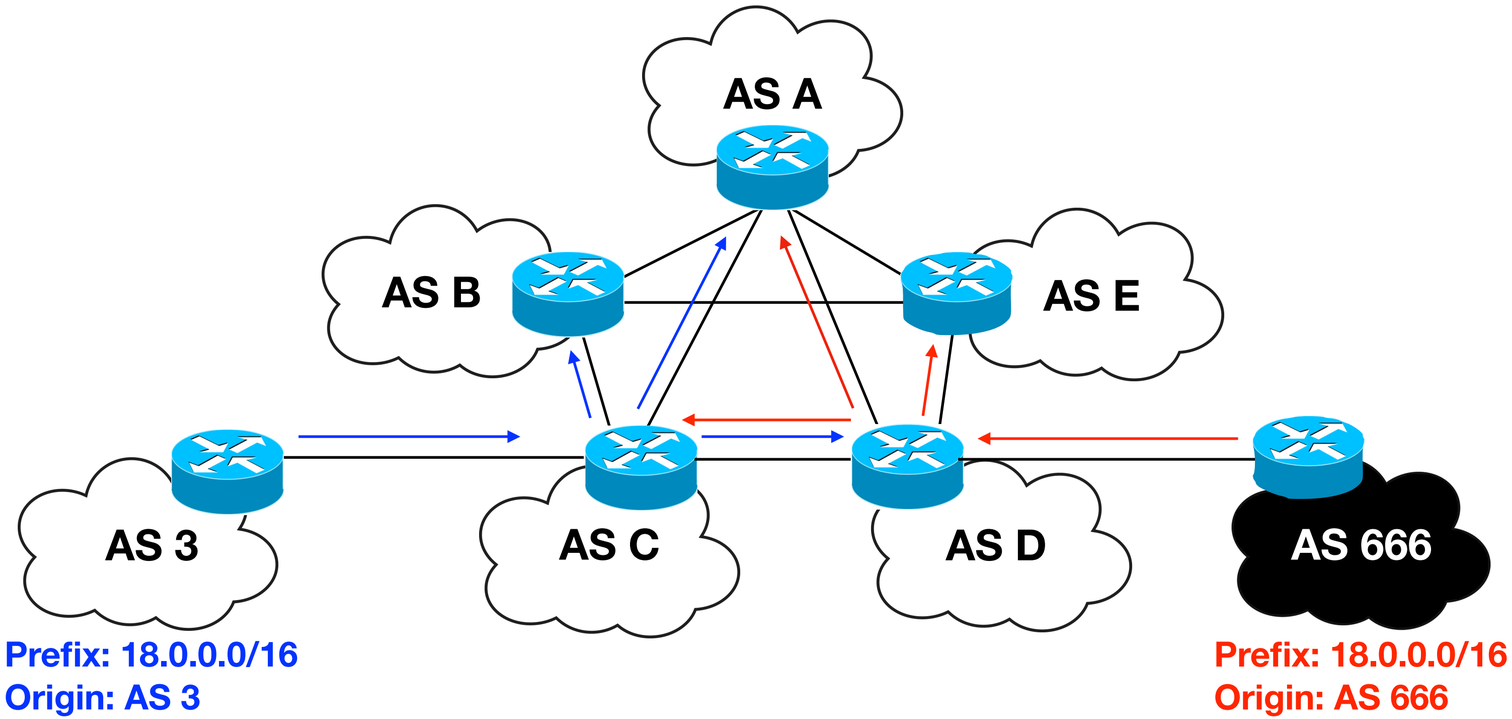
The Border Gateway Protocol (BGP)



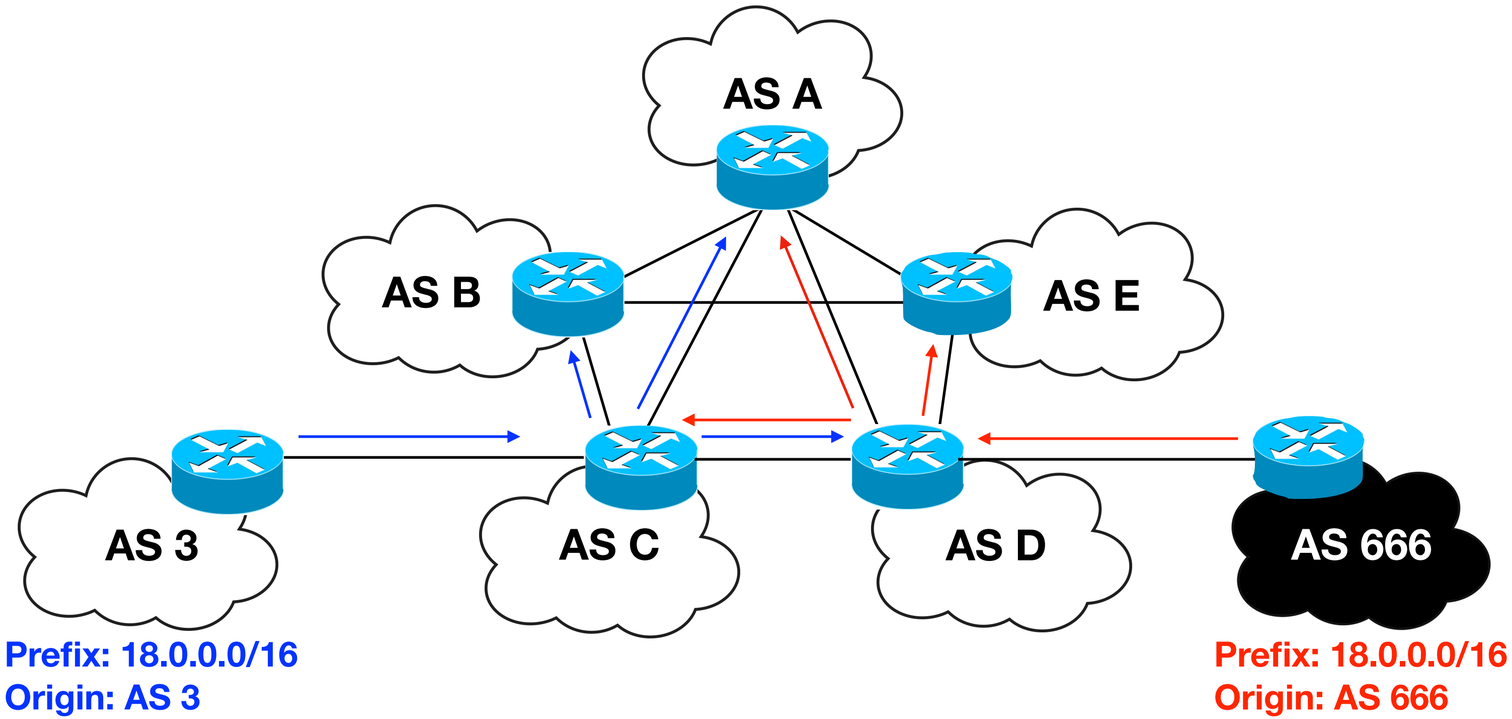
The Border Gateway Protocol (BGP)



The Border Gateway Protocol (BGP)



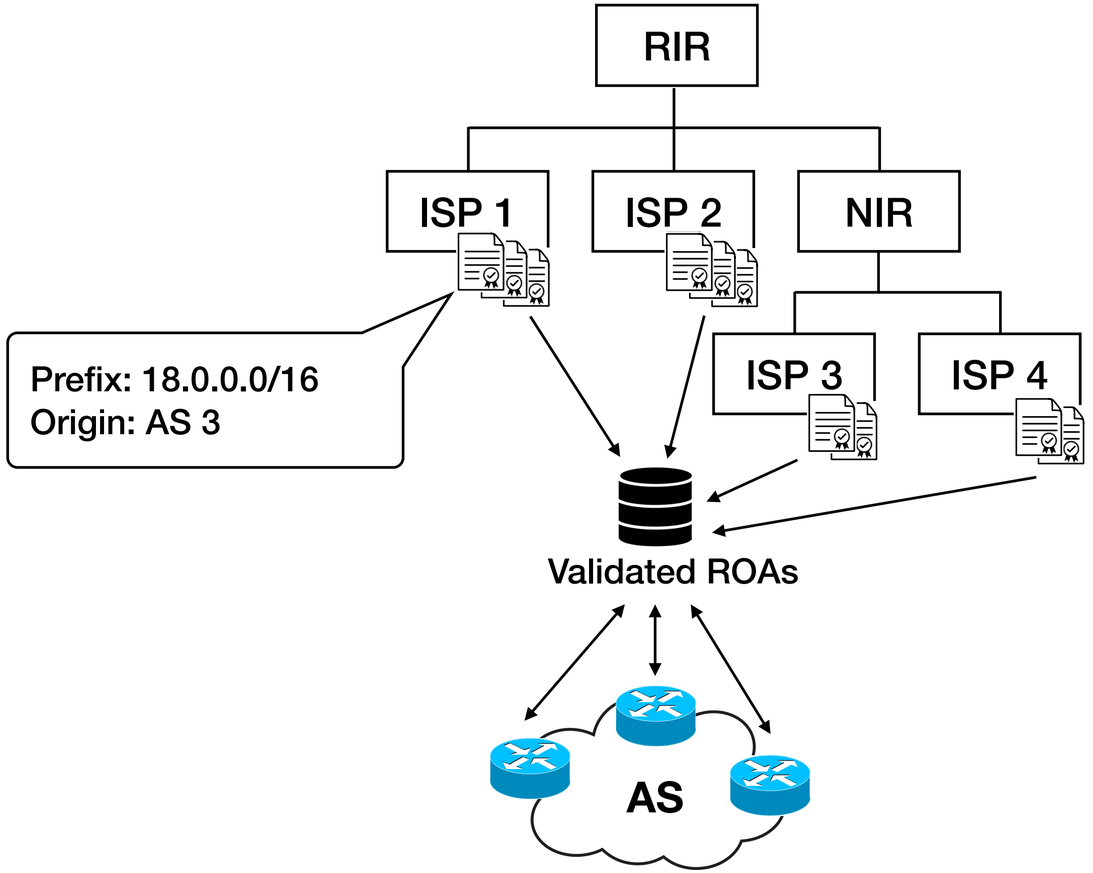
The Border Gateway Protocol (BGP)



- BGP lacks a mechanism for route validation.

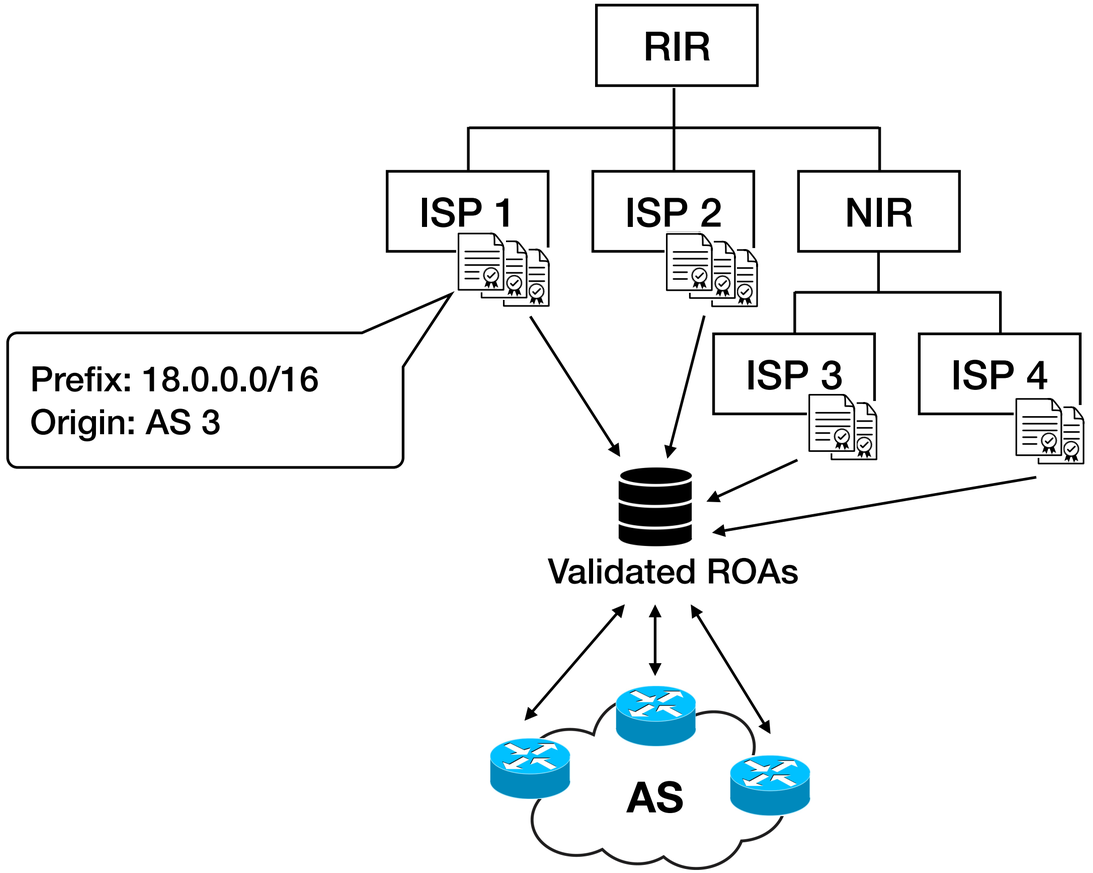
The Resource Public Key Infrastructure

- The RPKI is a framework to secure BGP using cryptographic records to validate prefix and origin in BGP announcements.
- Route Origin Authorizations (ROAs) map IP prefixes with valid AS origins.
- Networks can use the RPKI to validate announcements in BGP.



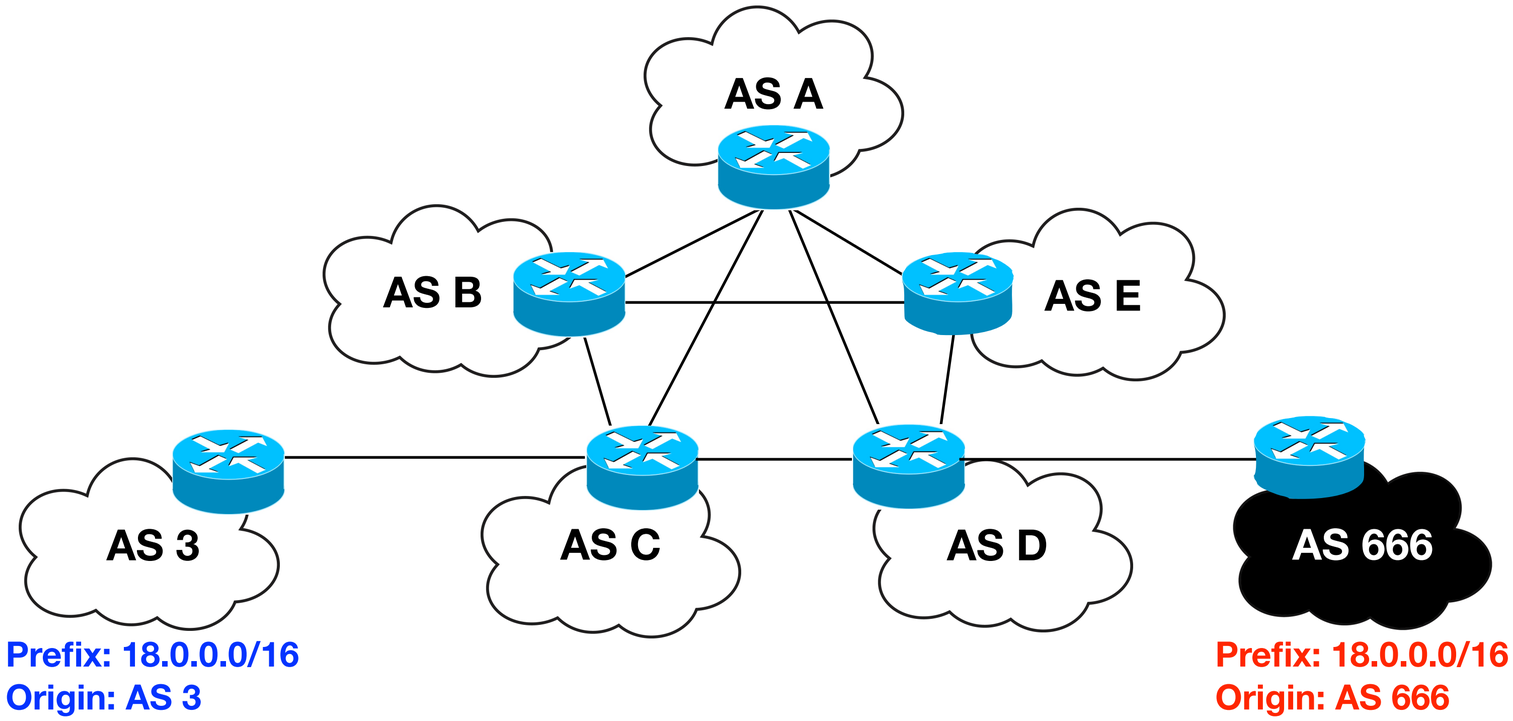
The Resource Public Key Infrastructure

- The RPKI is a framework to secure BGP using cryptographic records to validate prefix and origin in BGP announcements.
- Route Origin Authorizations (ROAs) map IP prefixes with valid AS origins.
- Networks can use the RPKI to validate announcements in BGP.

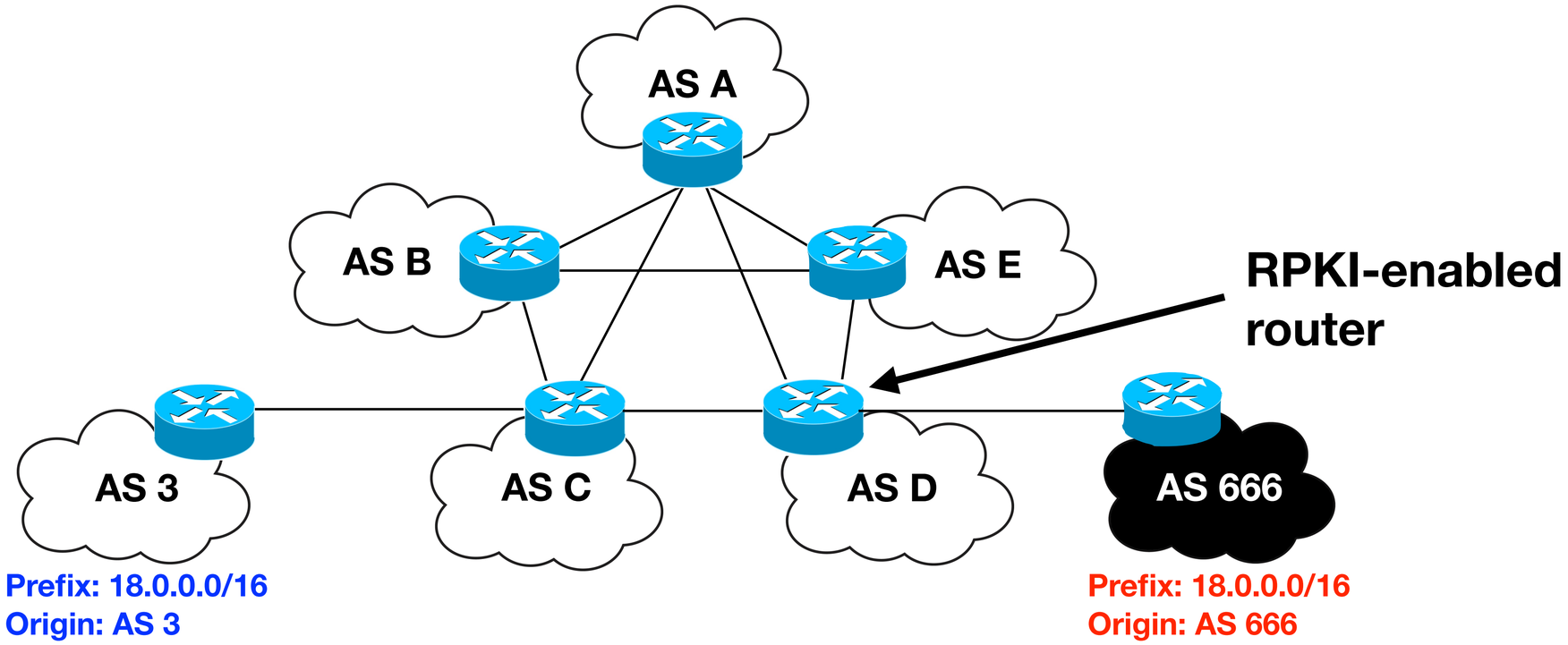


▶ About 20% of IP prefixes in BGP are covered by valid ROAs.

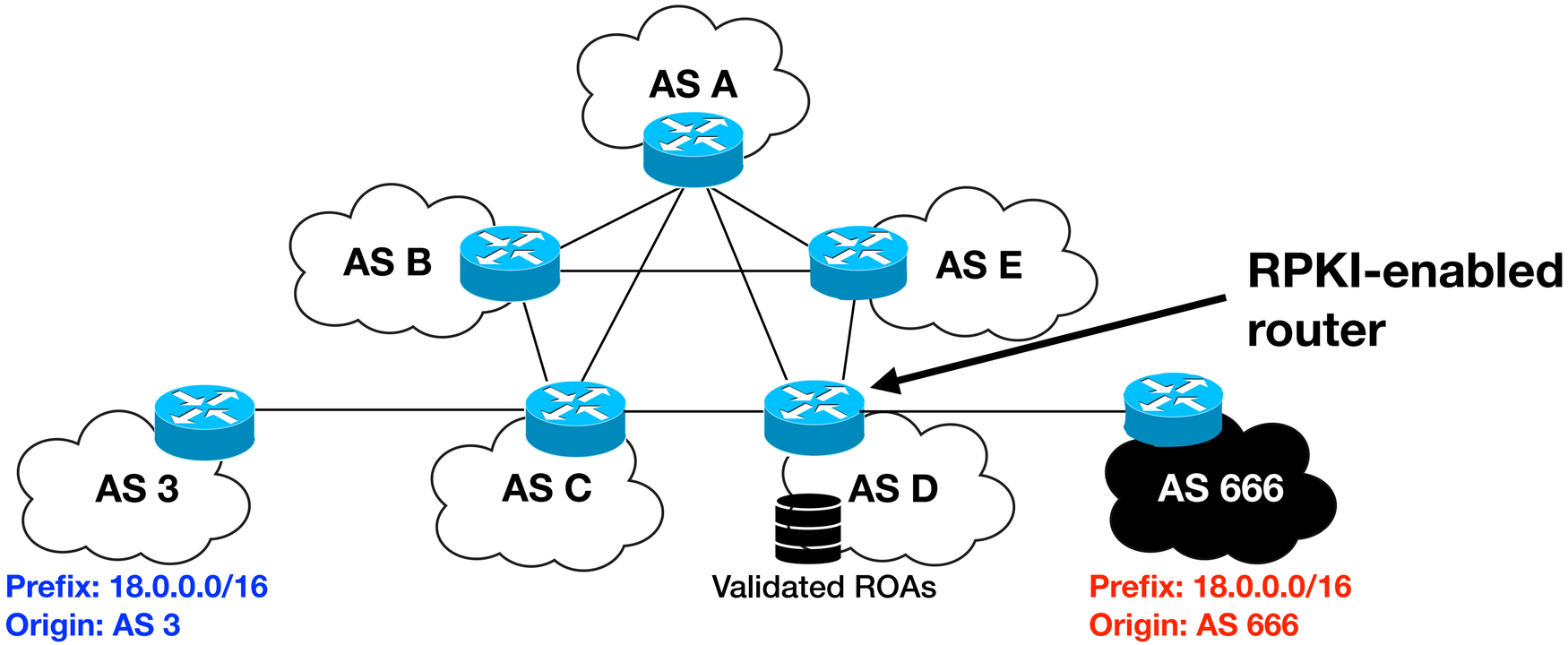
RPKI enforcement in BGP



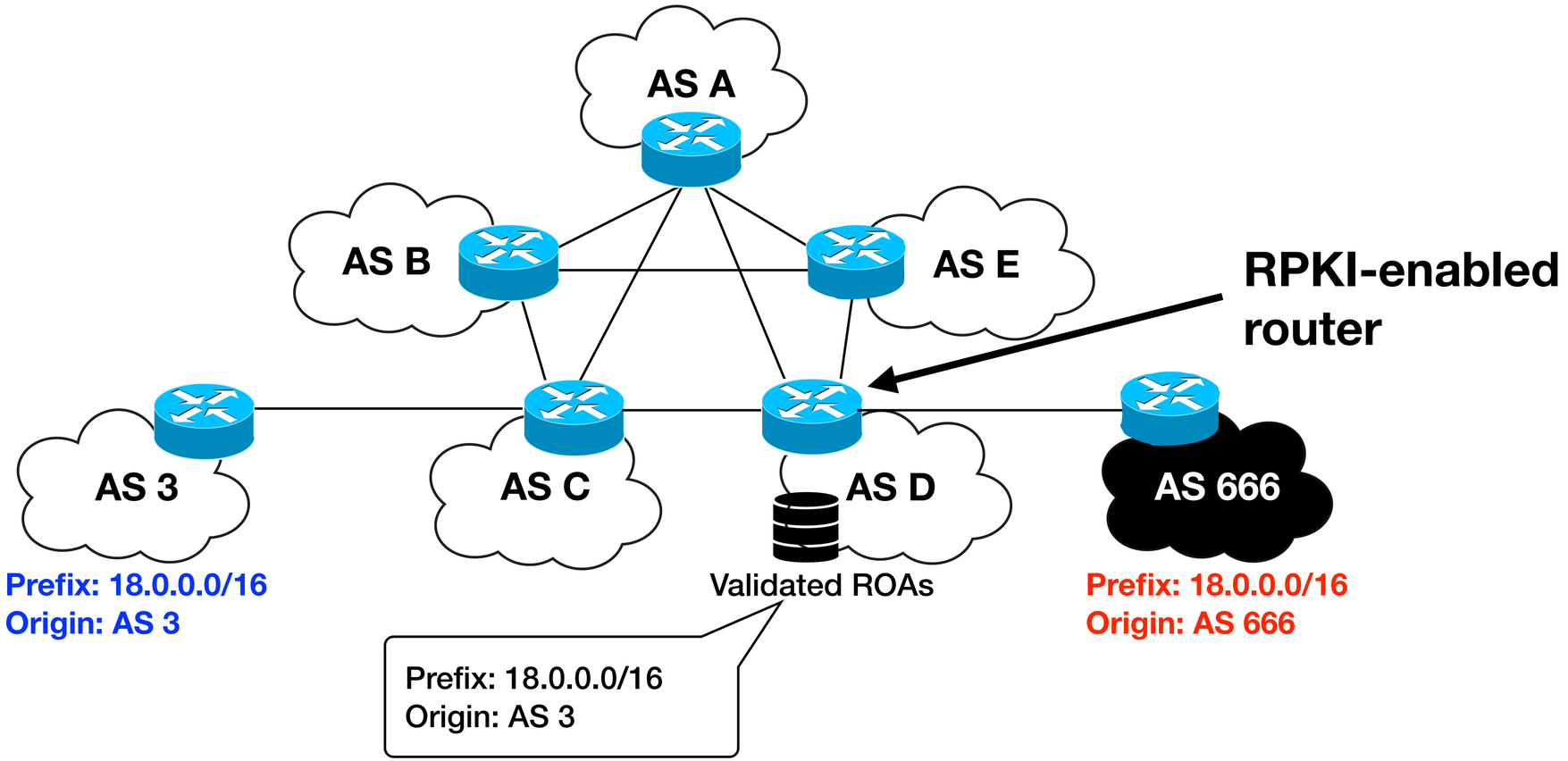
RPKI enforcement in BGP



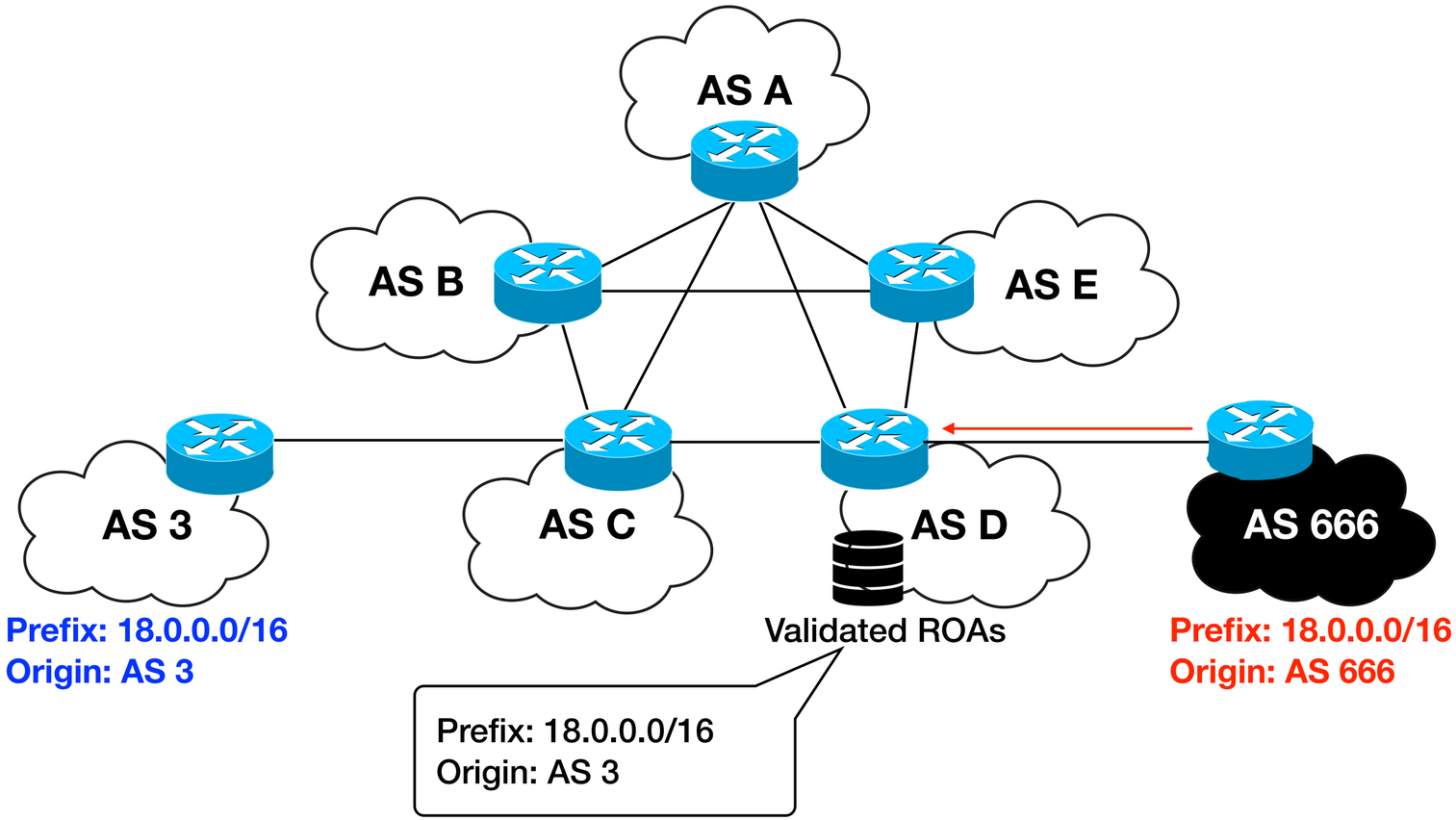
RPKI enforcement in BGP



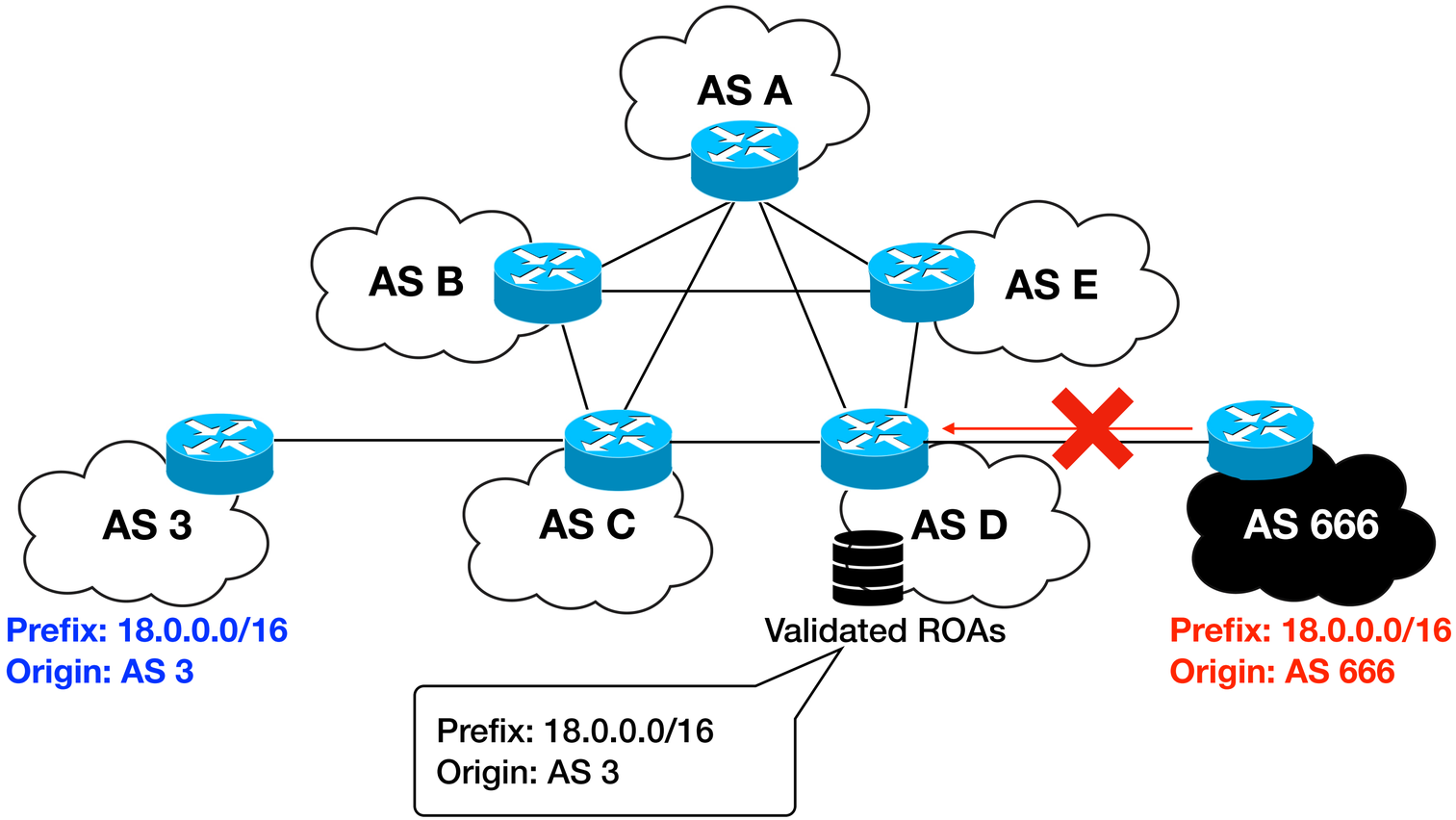
RPKI enforcement in BGP



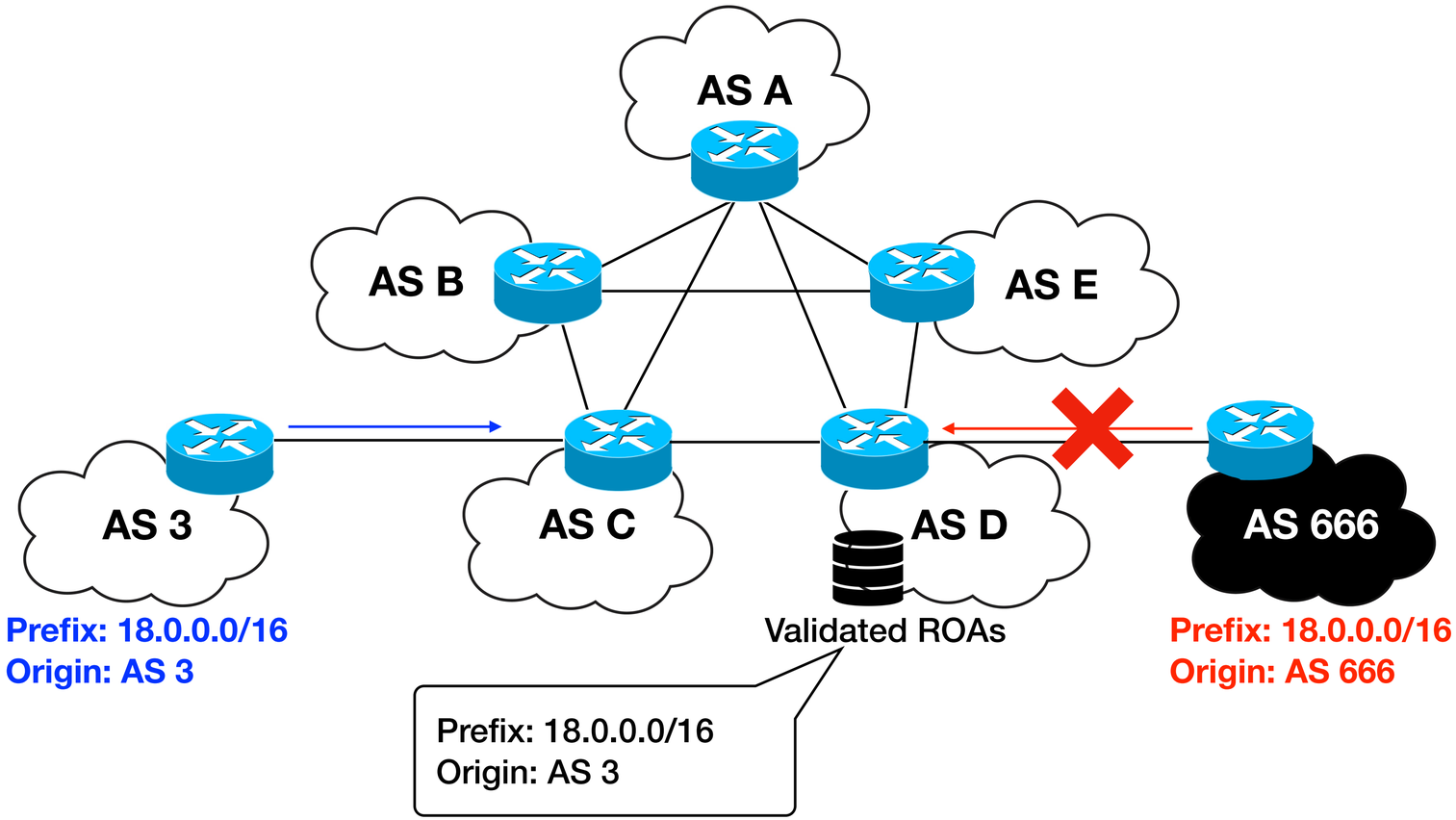
RPKI enforcement in BGP



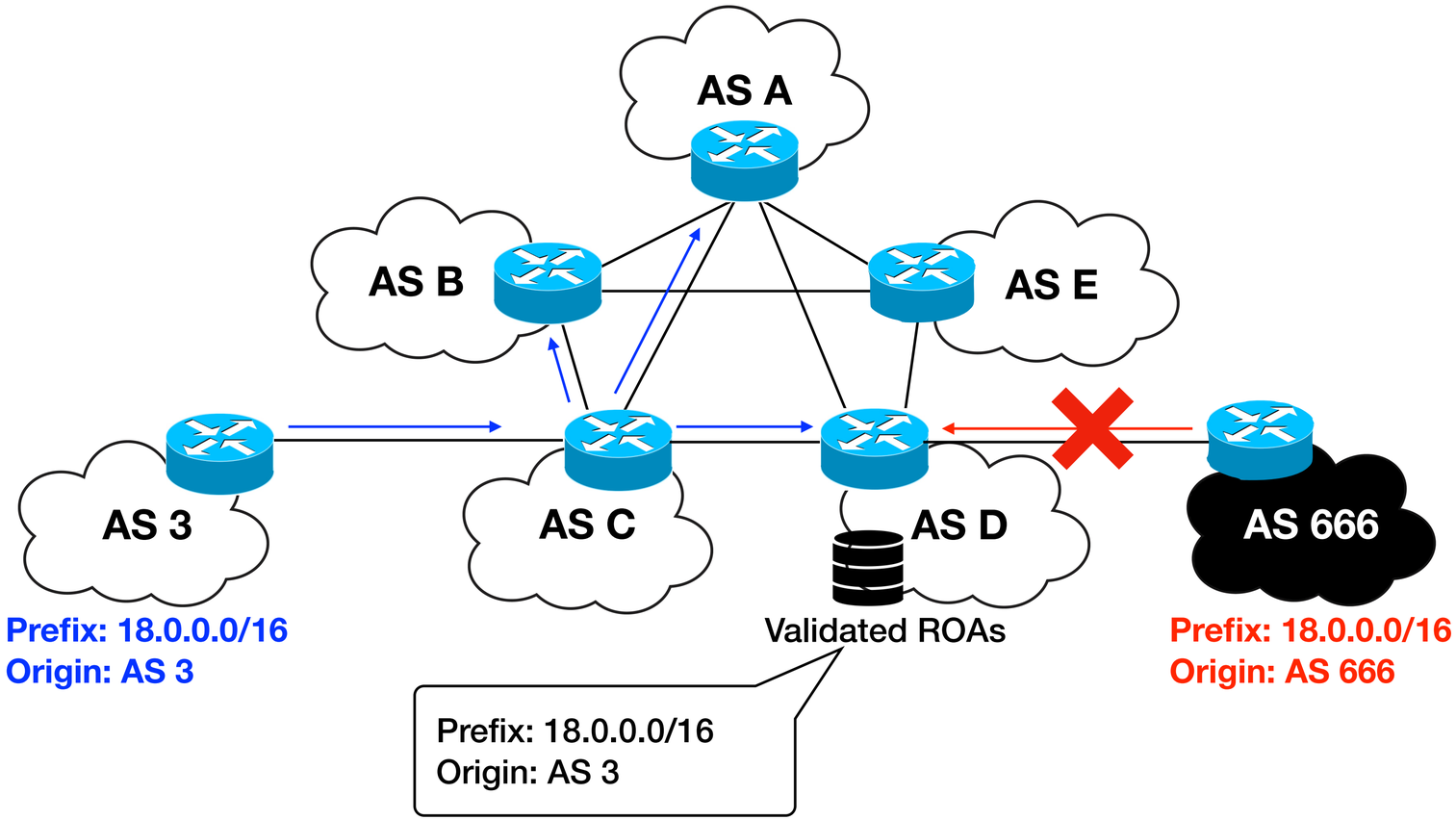
RPKI enforcement in BGP



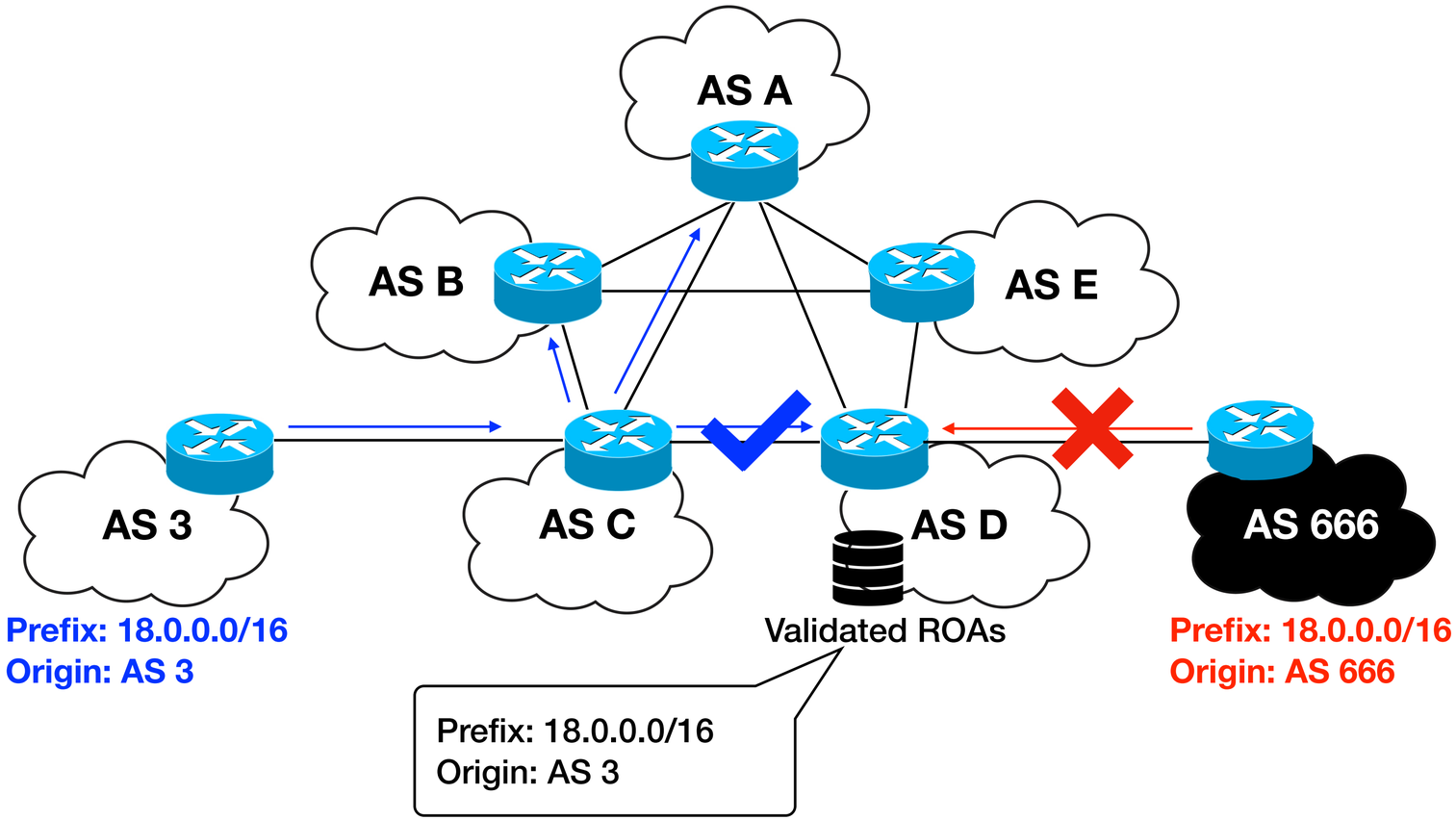
RPKI enforcement in BGP



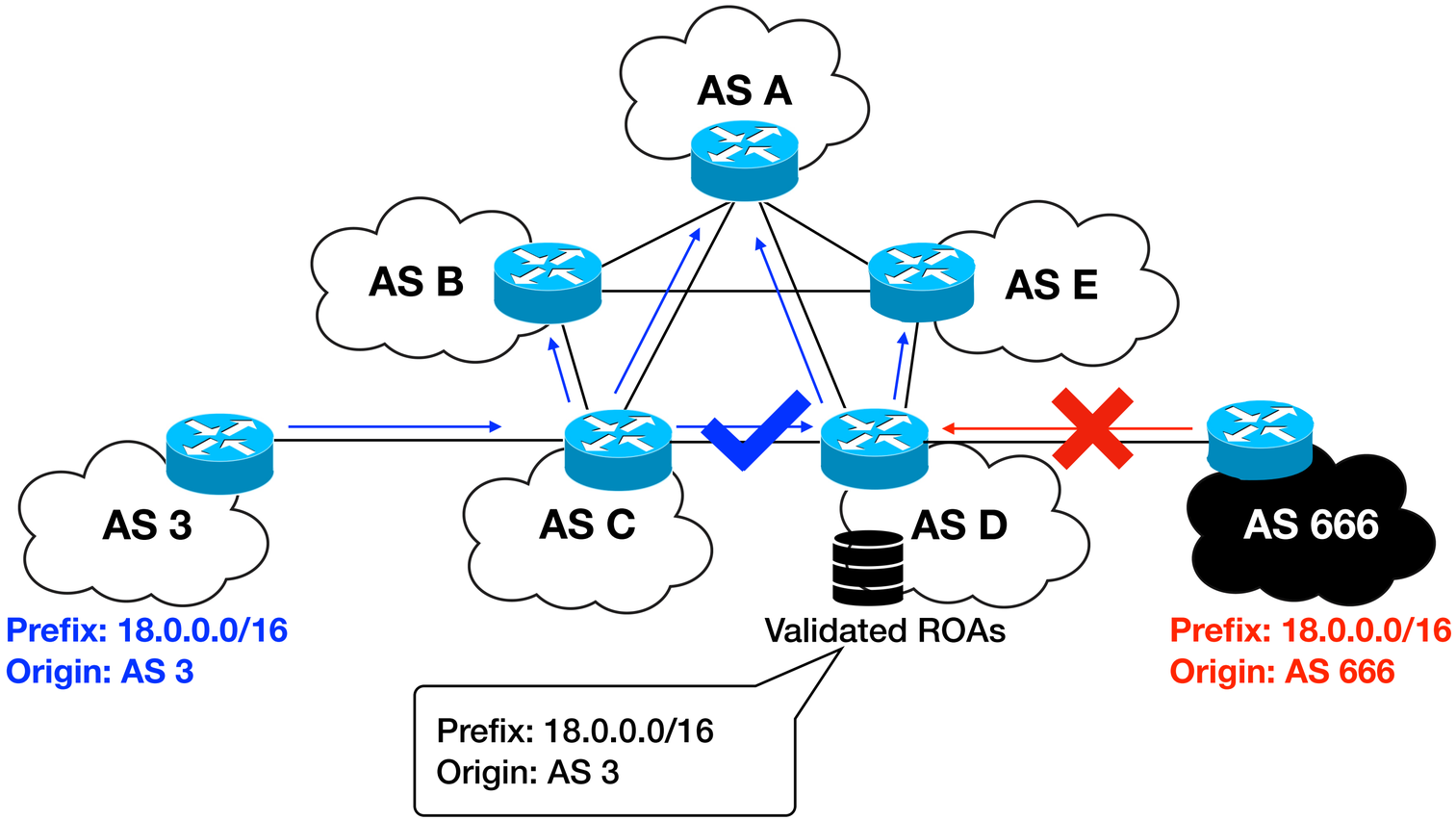
RPKI enforcement in BGP



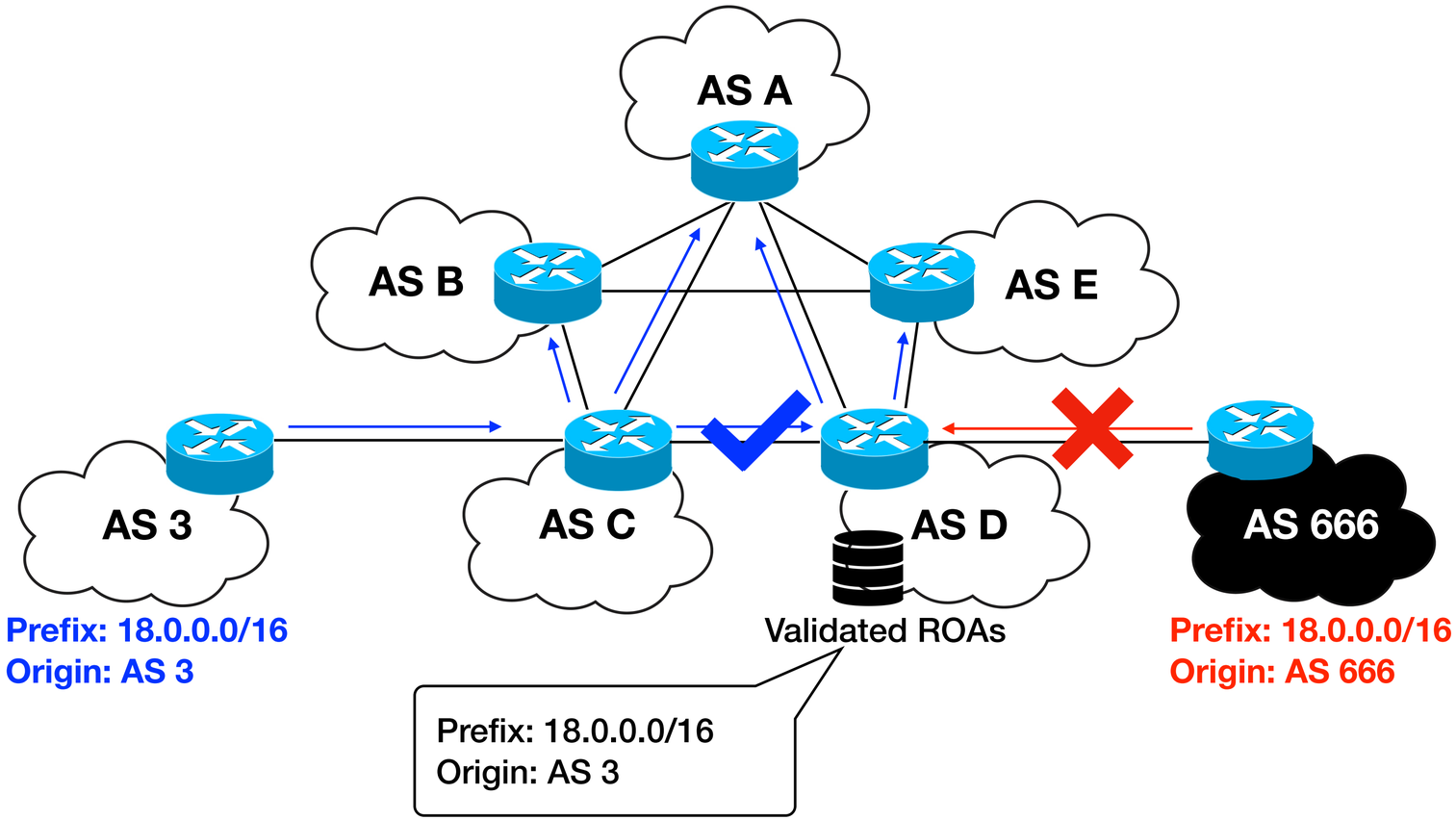
RPKI enforcement in BGP



RPKI enforcement in BGP



RPKI enforcement in BGP



- Only anecdotal evidence of RPKI enforcement.

Research goal

To what degree does registration in the RPKI protect a network from illicit announcements of their prefixes?

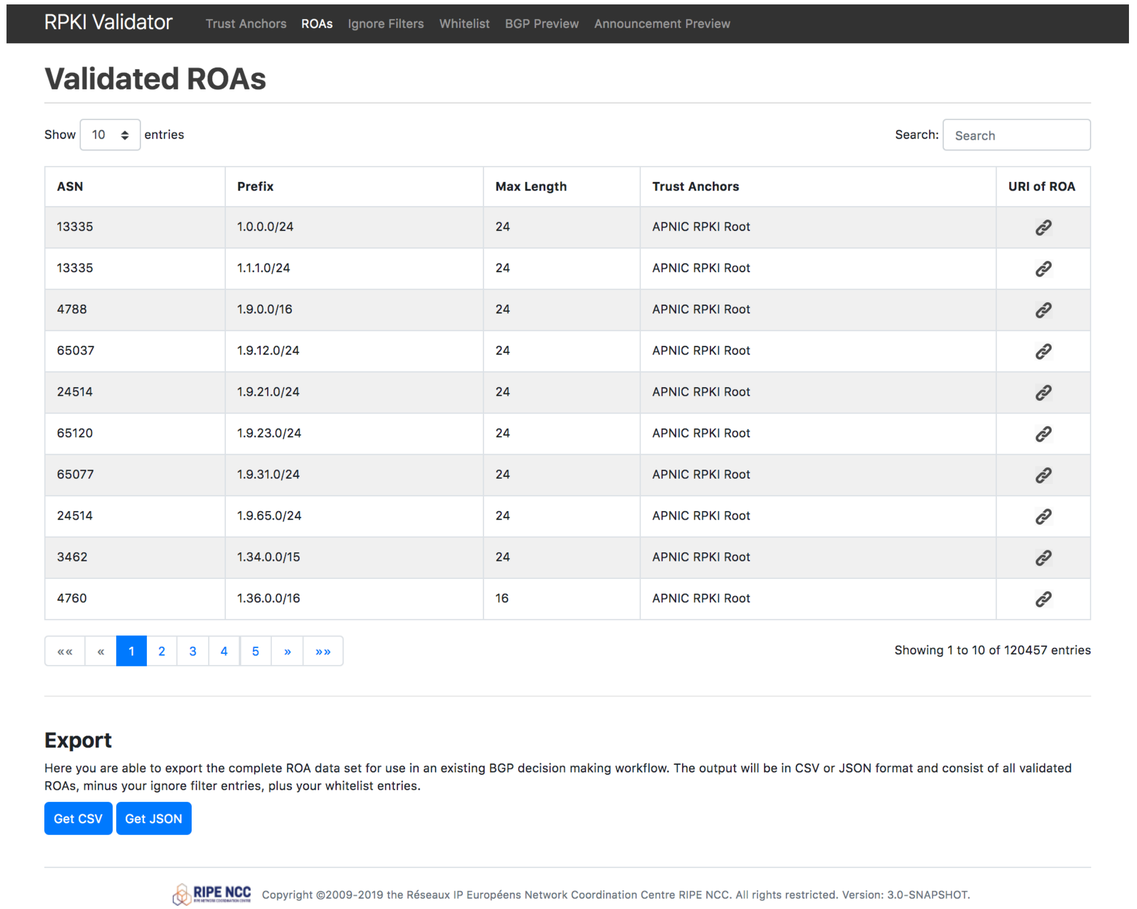
(i) Measure RPKI enforcement over time

(ii) Study the visibility of prefix origin pairs depending on their RPKI status

(iii) Analyze visibility of prefixes in the case of conflicts

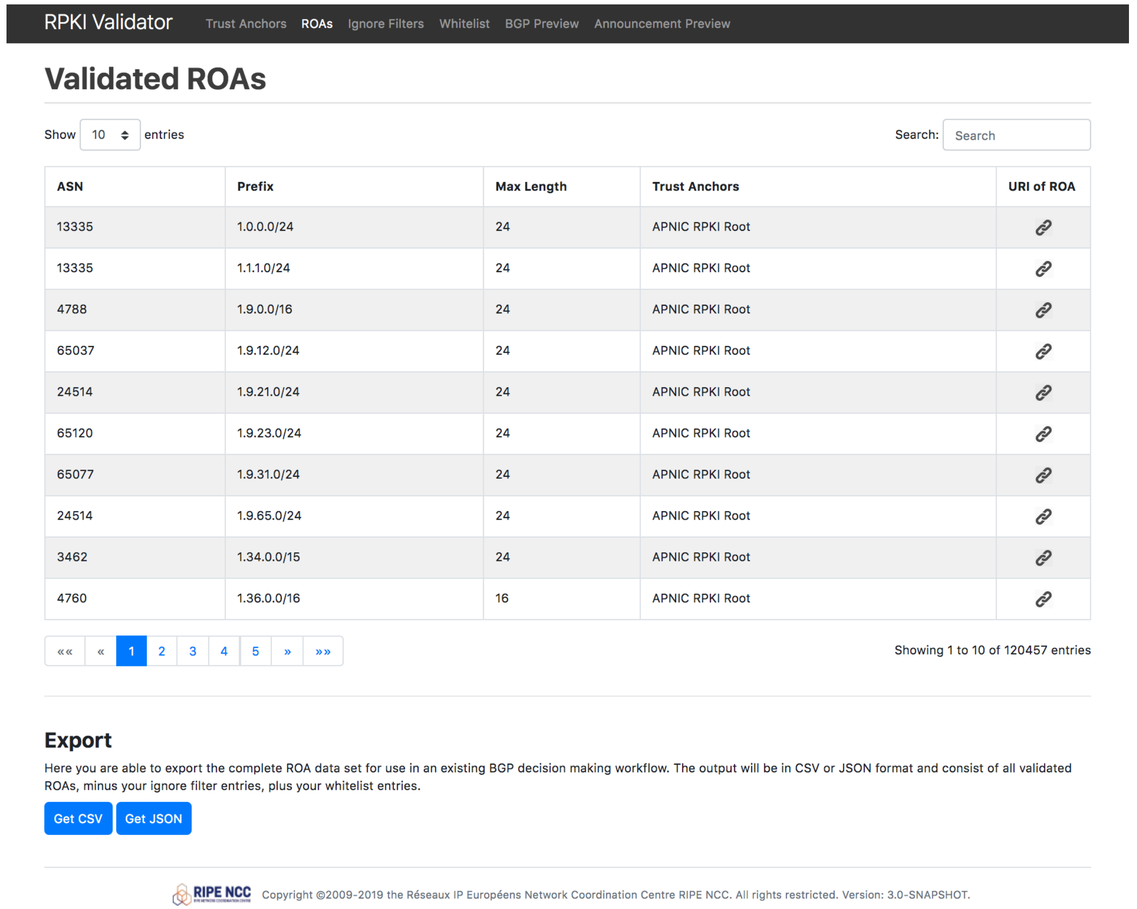
RPKI and BGP dataset

- **RPKI data:**
  - Daily list of validated ROAs from RIPE NCC RPKI validator (Sep. 2019).
  - Historical lists of validated ROAS made available by Chung et al (Apr. 2017 - Sep. 2019).



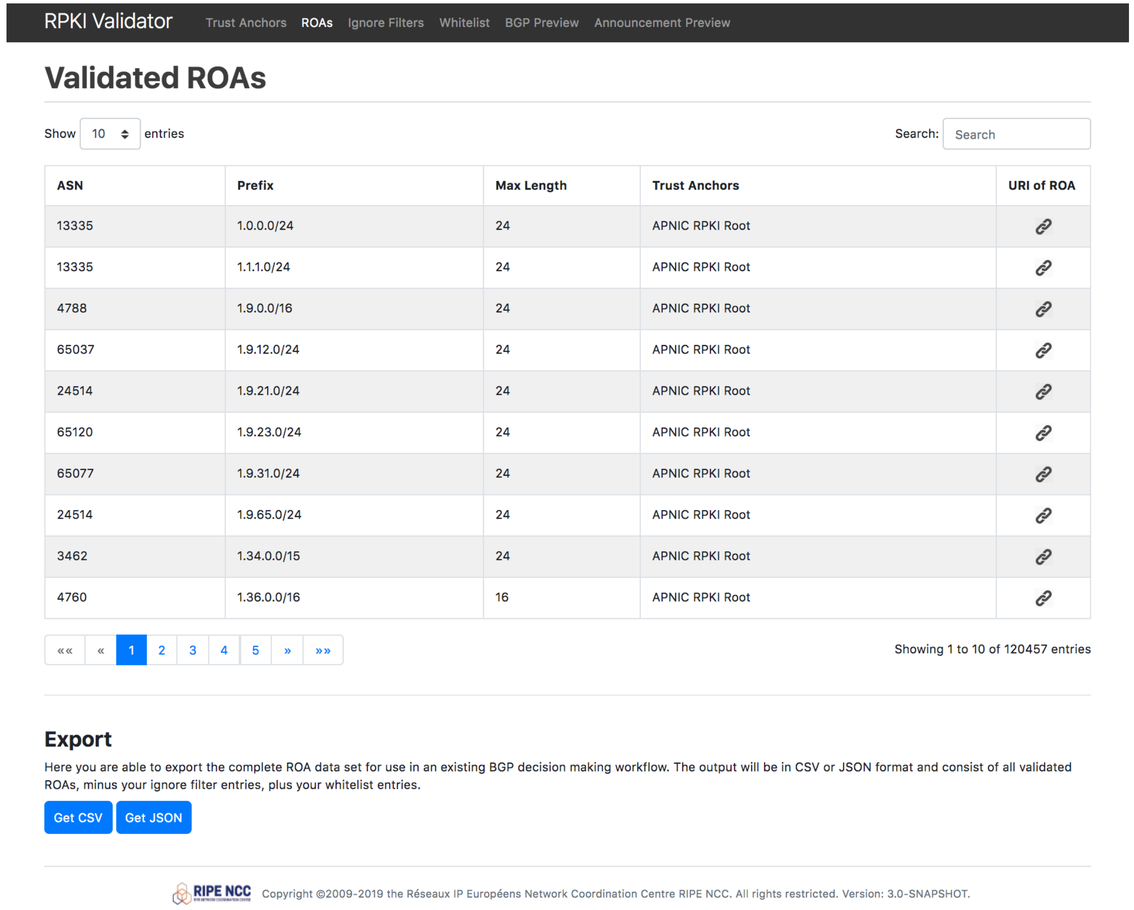
RPKI and BGP dataset

- **RPKI data:**
  - Daily list of validated ROAs from RIPE NCC RPKI validator (Sep. 2019).
  - Historical lists of validated ROAS made available by Chung et al (Apr. 2017 - Sep. 2019).
- **Longitudinal BGP dataset:**
  - RIB dumps from all RIPE RIS and RouteViews collectors on the first day of the month (Apr. 2017 - Jan. 2020).

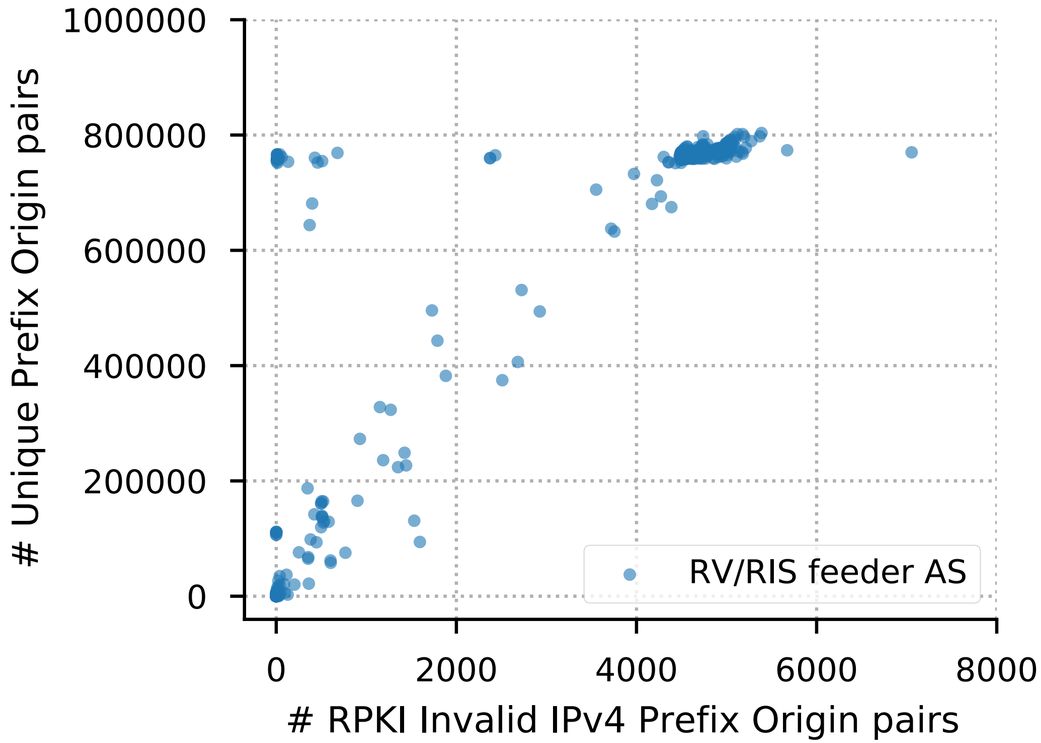


RPKI and BGP dataset

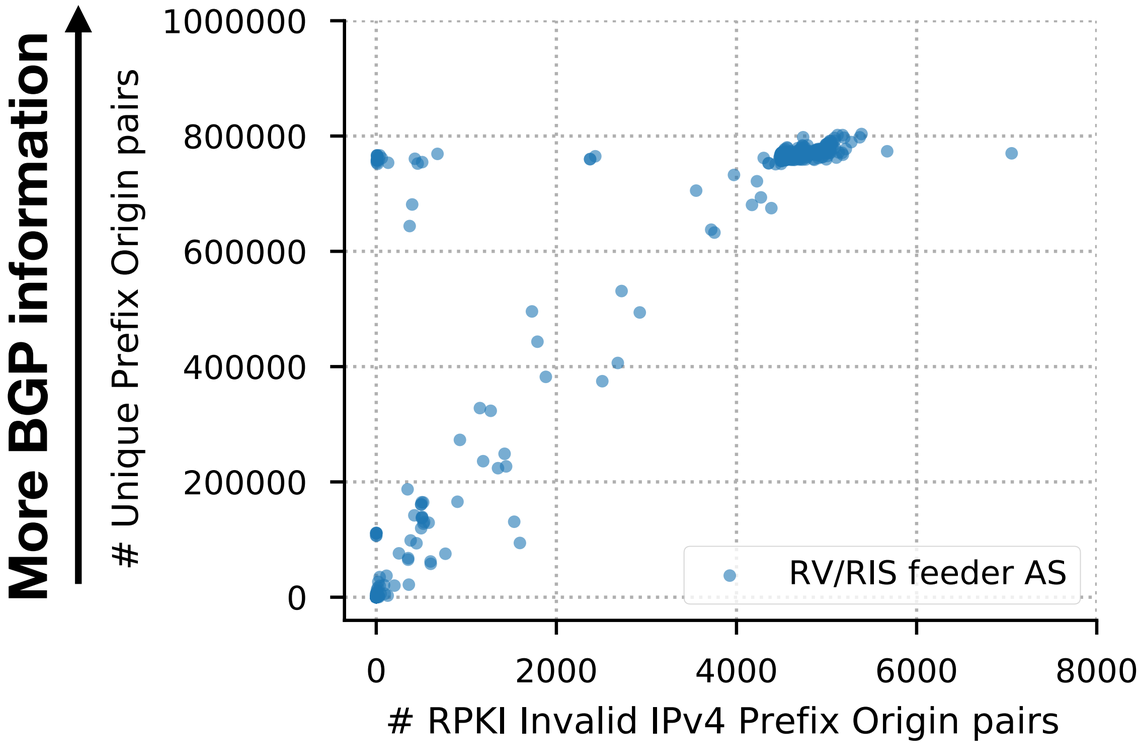
- **RPKI data:**
  - Daily list of validated ROAs from RIPE NCC RPKI validator (Sep. 2019).
  - Historical lists of validated ROAS made available by Chung et al (Apr. 2017 - Sep. 2019).
- **Longitudinal BGP dataset:**
  - RIB dumps from all RIPE RIS and RouteViews collectors on the first day of the month (Apr. 2017 - Jan. 2020).
- **Fine-Grained BGP dataset:**
  - All BGP updates from RIPE RIS and RouteViews collector peers to compute (prefix, origin AS, visibility, timestamp) every 5 min (Sep.2019).



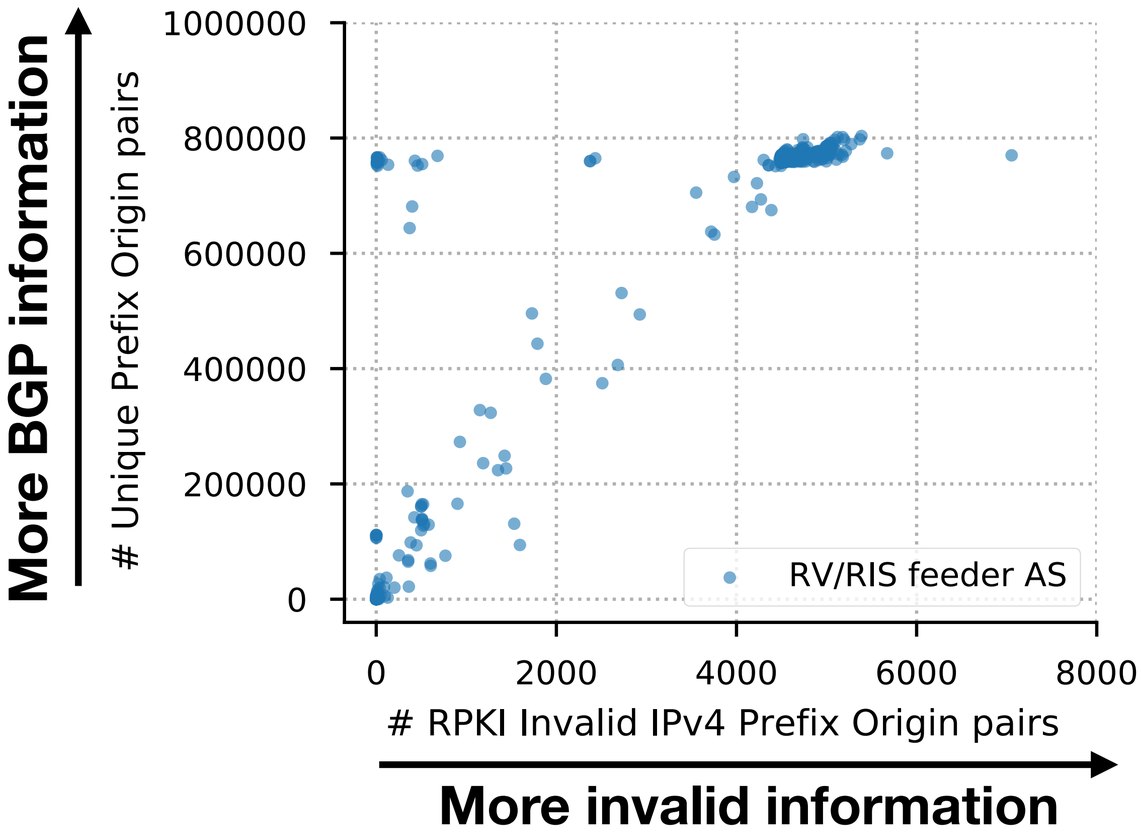
Detecting RPKI filtering



Detecting RPKI filtering

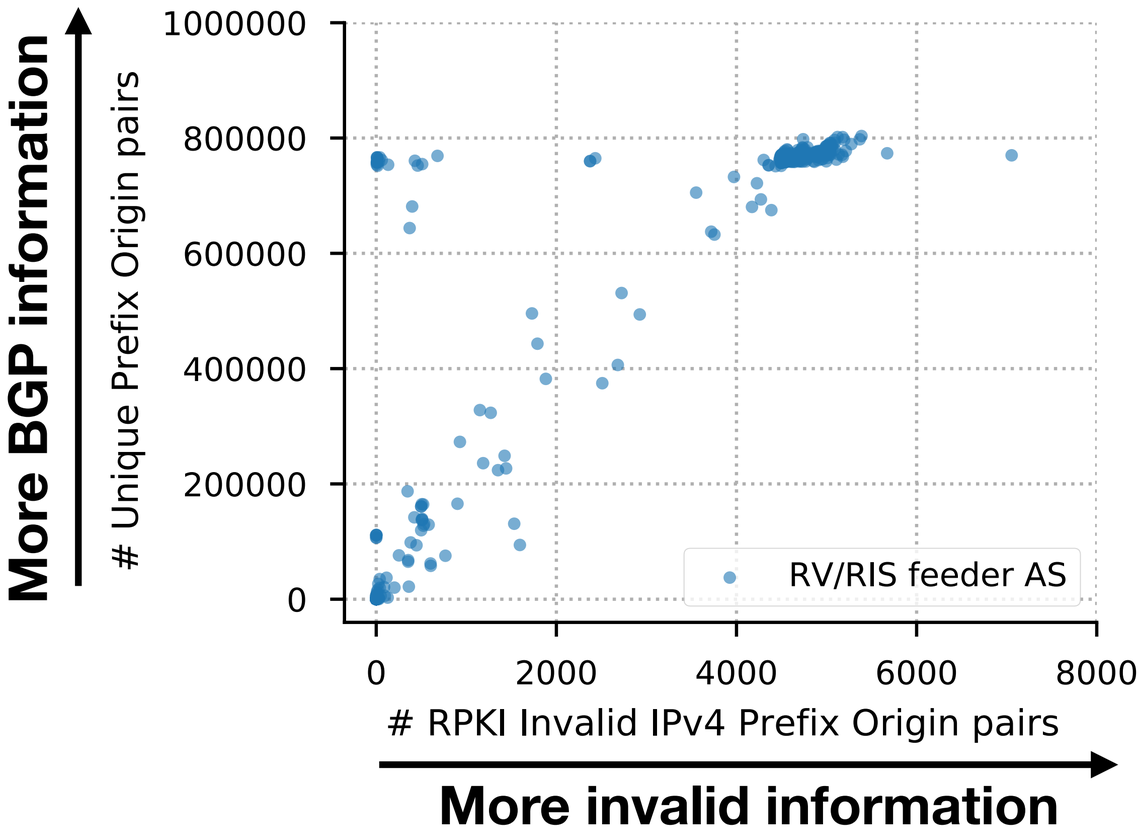


Detecting RPKI filtering



Detecting RPKI filtering

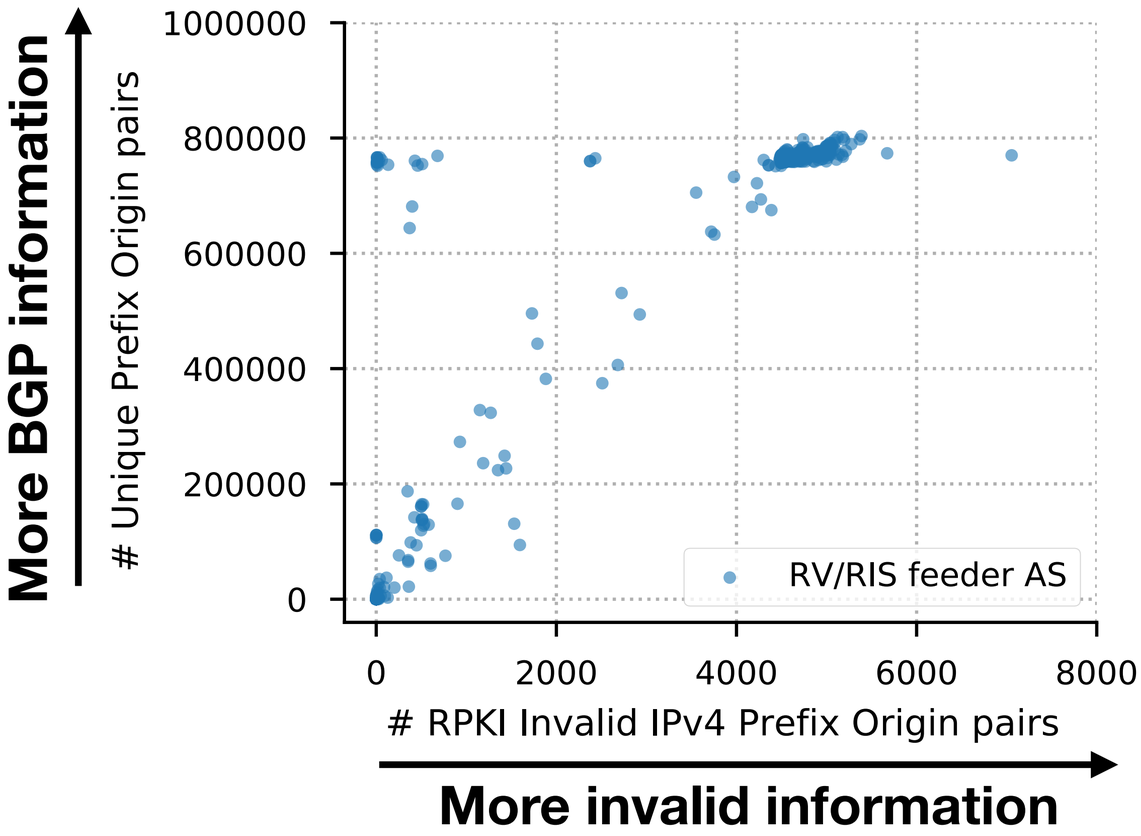
Two steps to detect filtering:



Detecting RPKI filtering

Two steps to detect filtering:

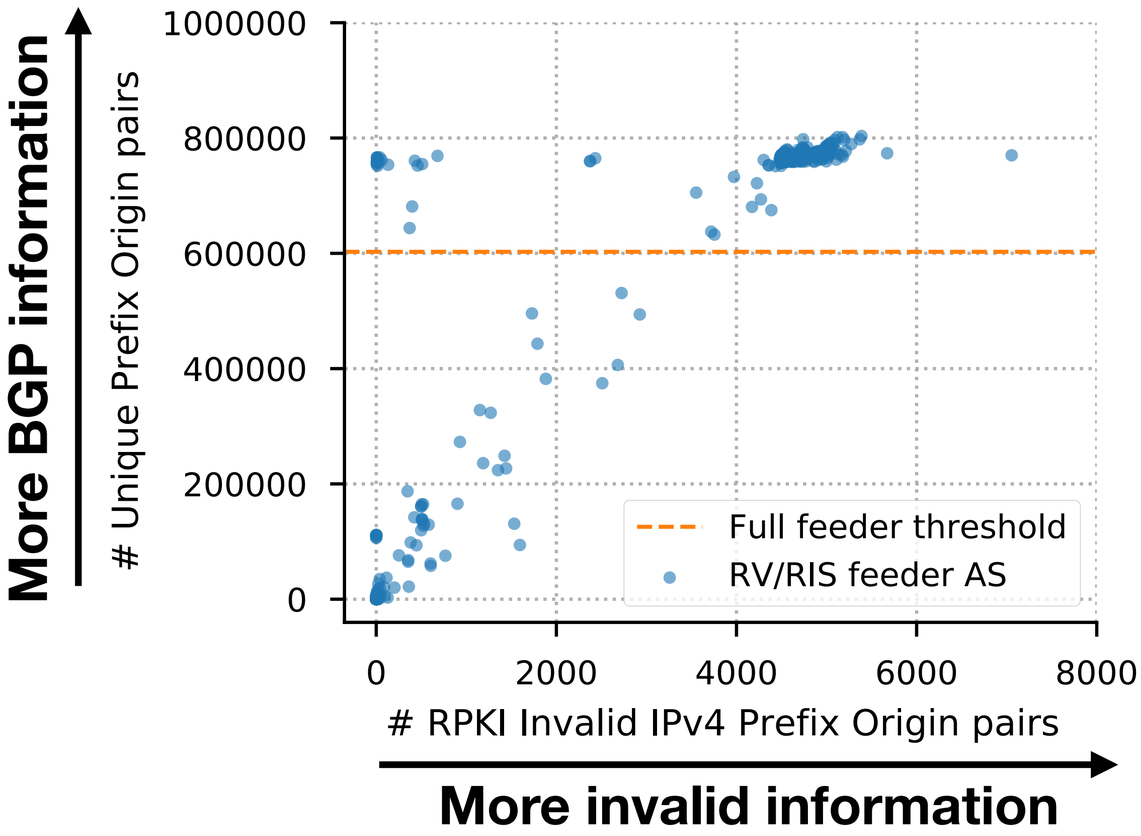
(1) Select full-feeder ASes: ASes that share their full routing table with BGP collectors



Detecting RPKI filtering

Two steps to detect filtering:

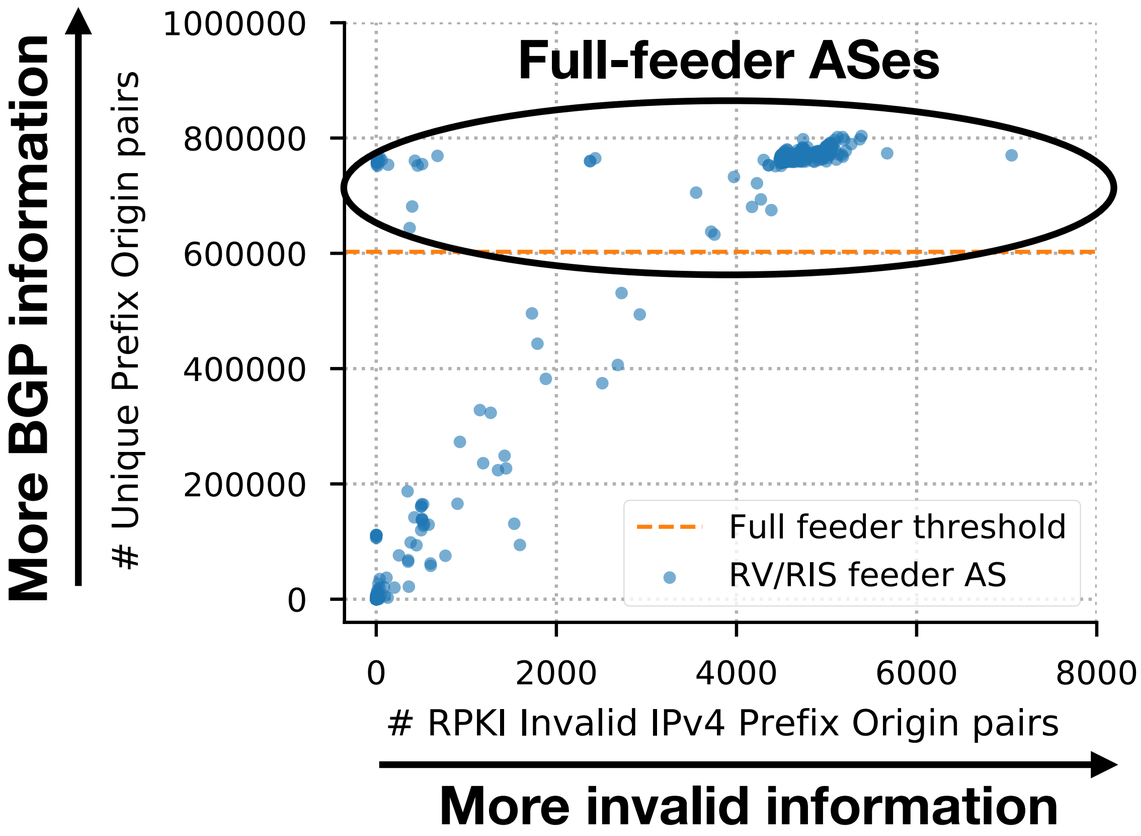
(1) Select full-feeder ASes: ASes that share their full routing table with BGP collectors



Detecting RPKI filtering

Two steps to detect filtering:

(1) Select full-feeder ASes: ASes that share their full routing table with BGP collectors

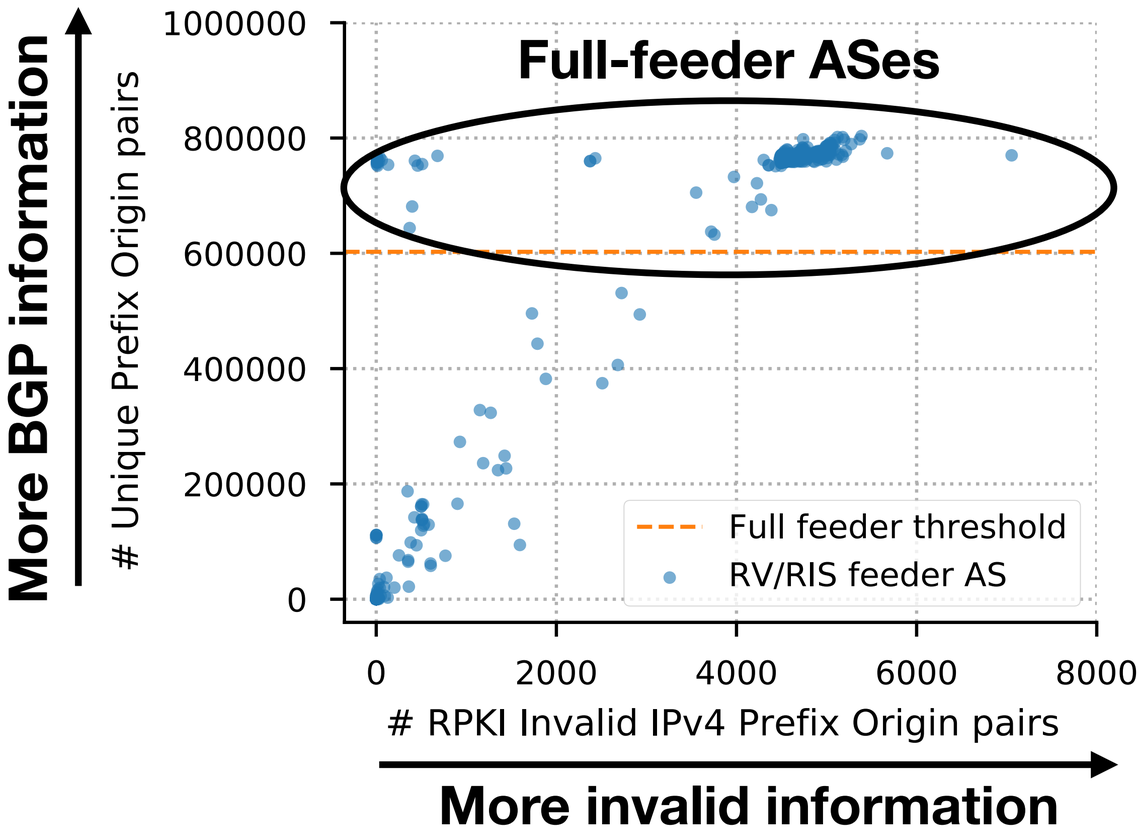


Detecting RPKI filtering

Two steps to detect filtering:

(1) Select full-feeder ASes: ASes that share their full routing table with BGP collectors

(2) Select ASes forwarding low counts of RPKI-invalid announcements.

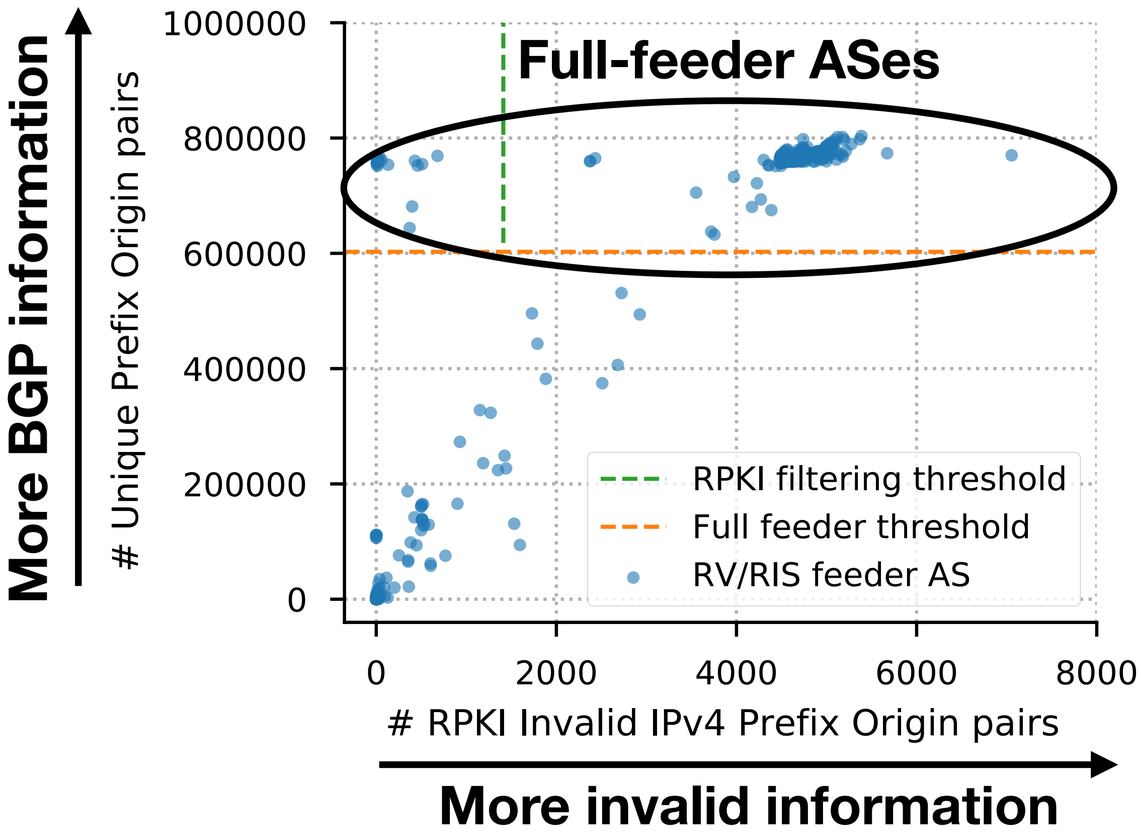


Detecting RPKI filtering

Two steps to detect filtering:

(1) Select full-feeder ASes: ASes that share their full routing table with BGP collectors

(2) Select ASes forwarding low counts of RPKI-invalid announcements.

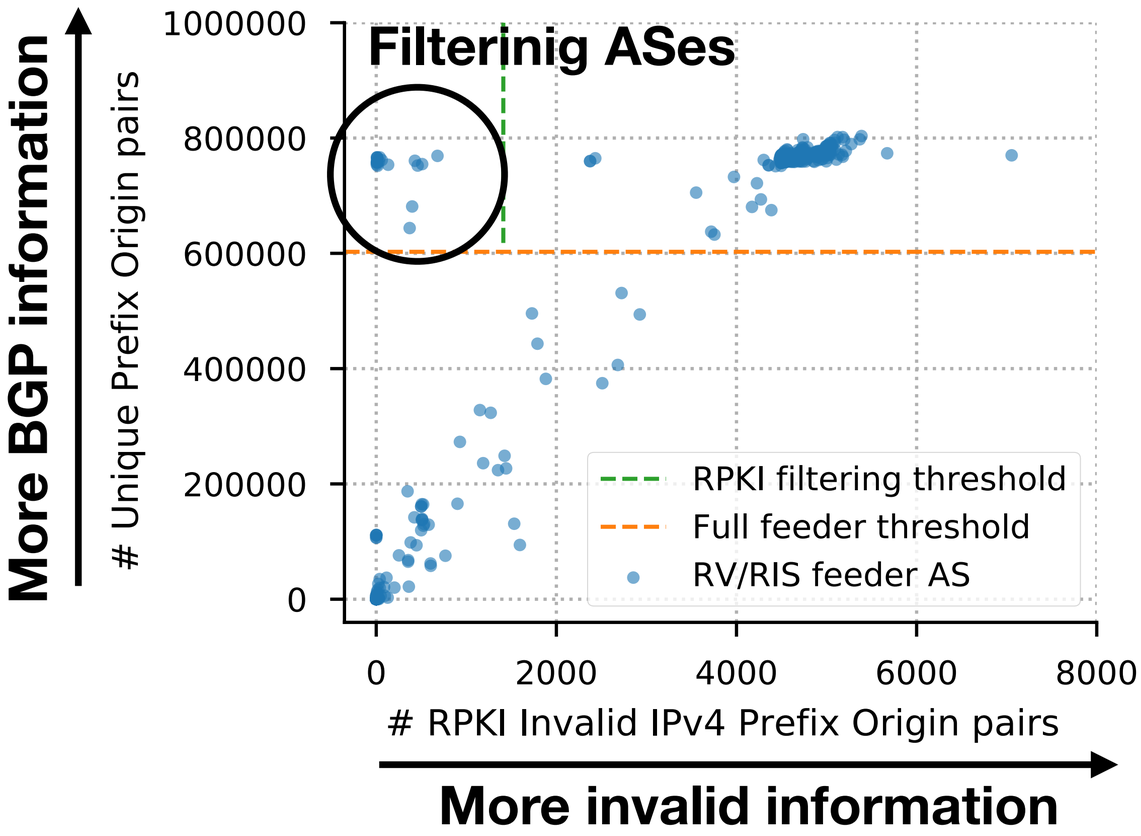


Detecting RPKI filtering

Two steps to detect filtering:

(1) Select full-feeder ASes: ASes that share their full routing table with BGP collectors

(2) Select ASes forwarding low counts of RPKI-invalid announcements.

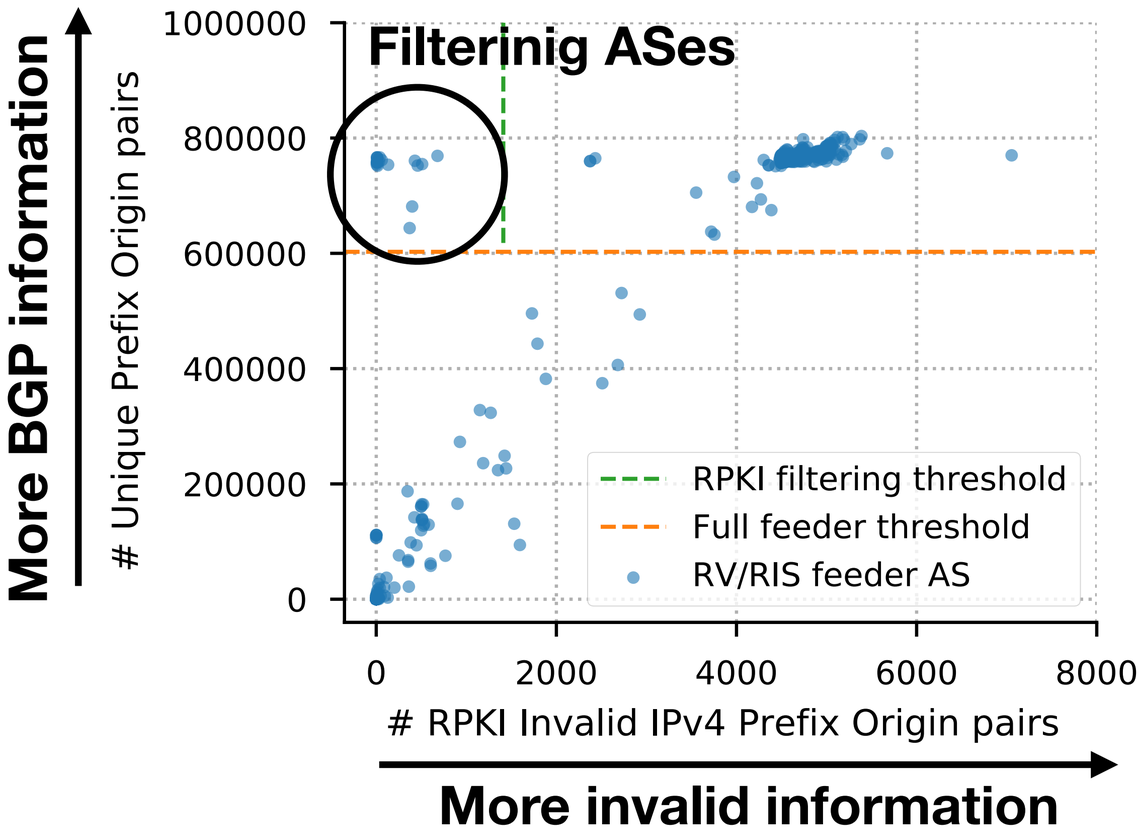


Detecting RPKI filtering

Two steps to detect filtering:

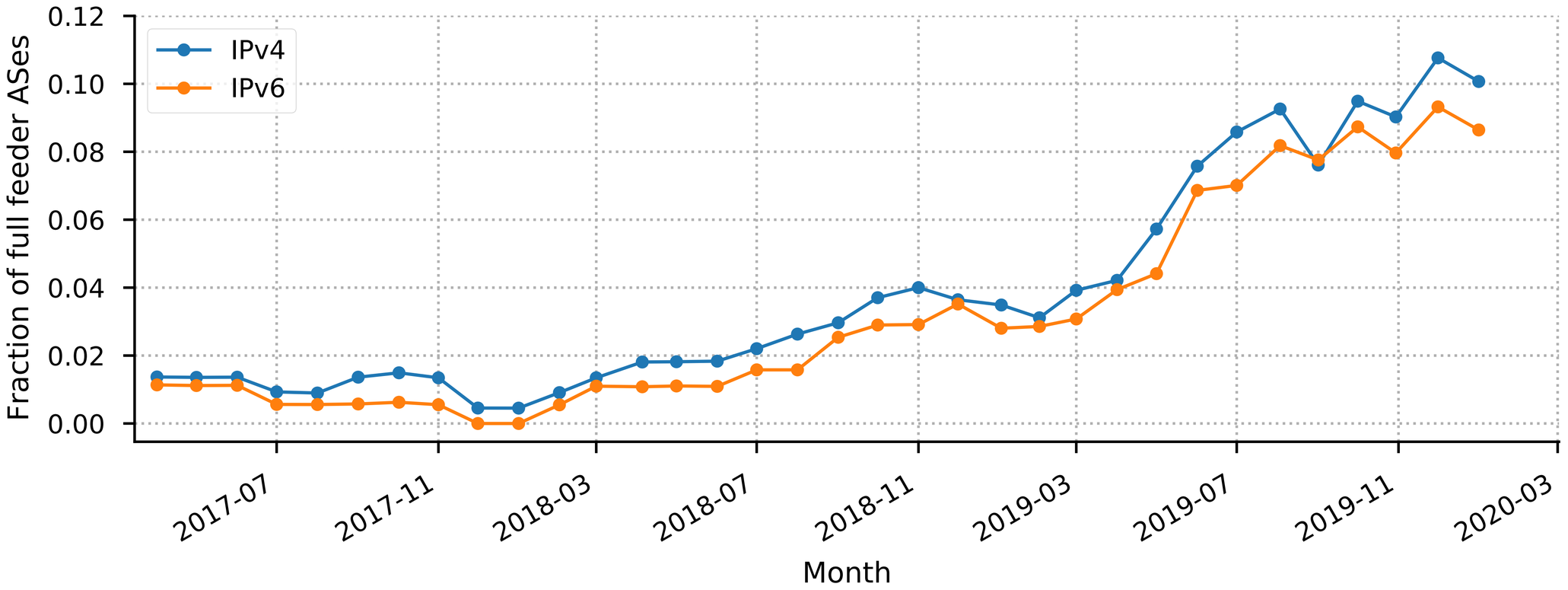
(1) Select full-feeder ASes: ASes that share their full routing table with BGP collectors

(2) Select ASes forwarding low counts of RPKI-invalid announcements.

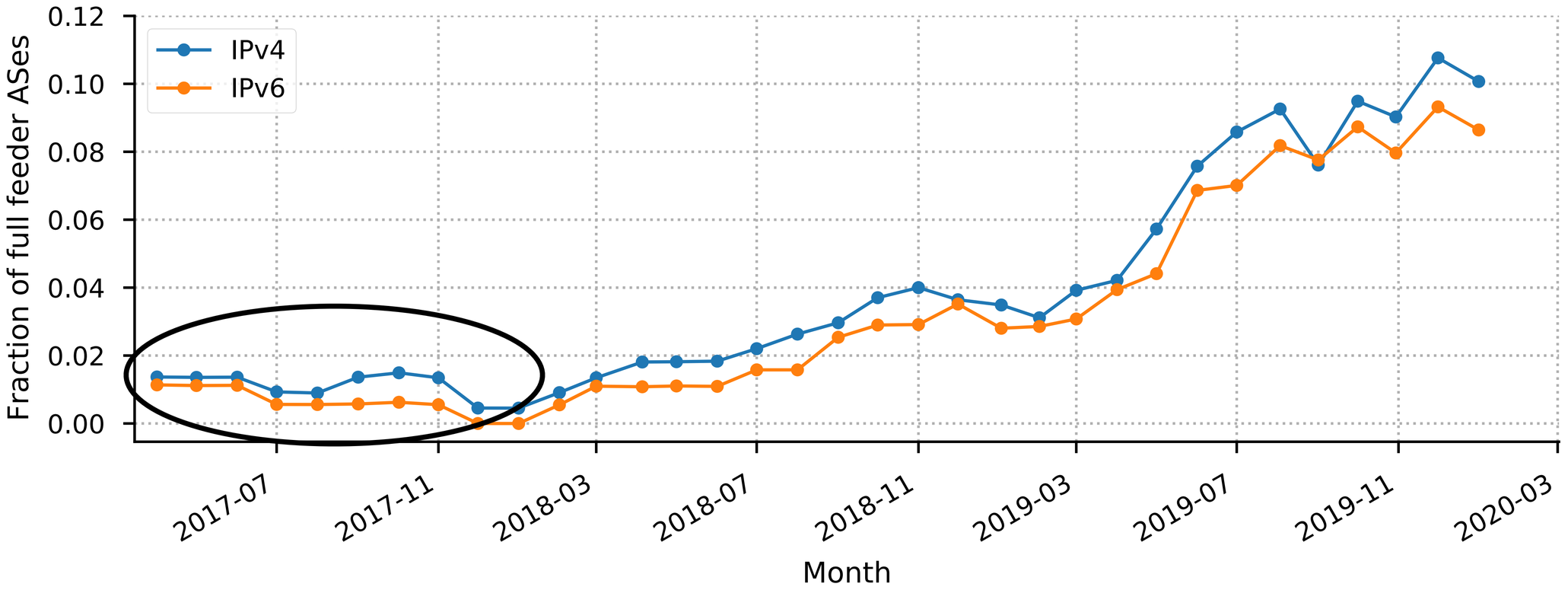


- We can detect RPKI filtering with high certainty for full feeder ASes.

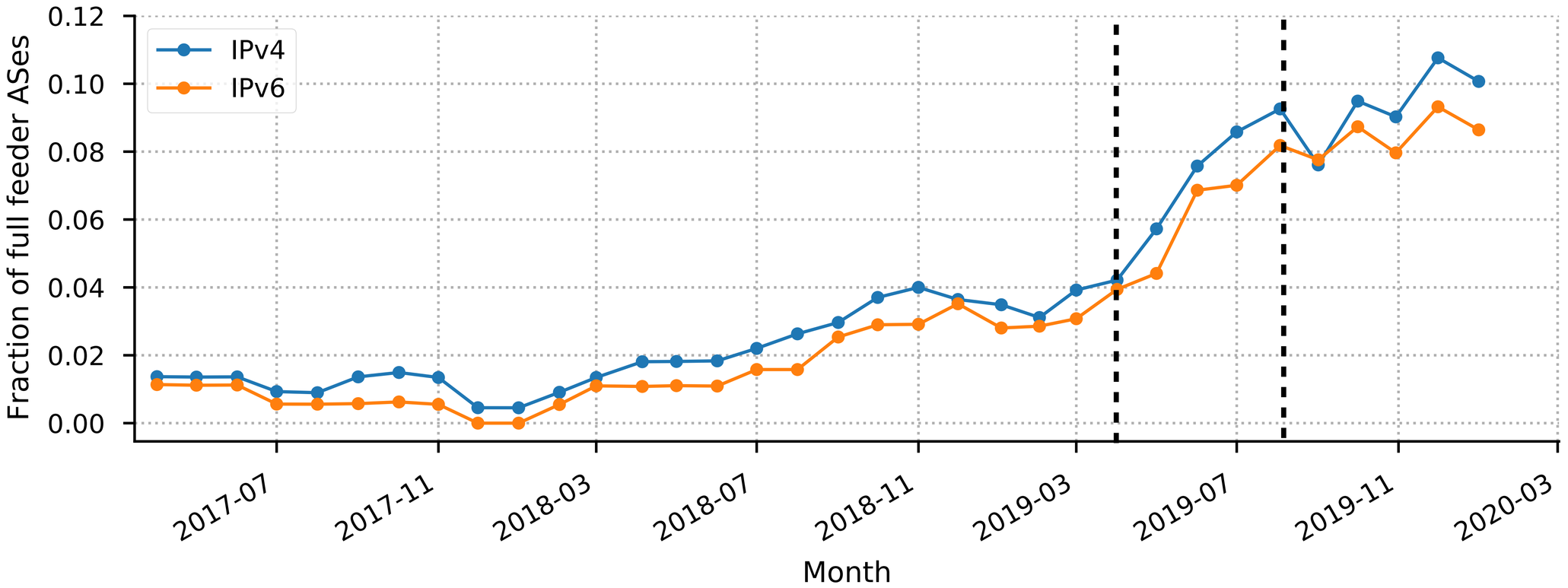
RPKI enforcement is starting to gain traction



RPKI enforcement is starting to gain traction

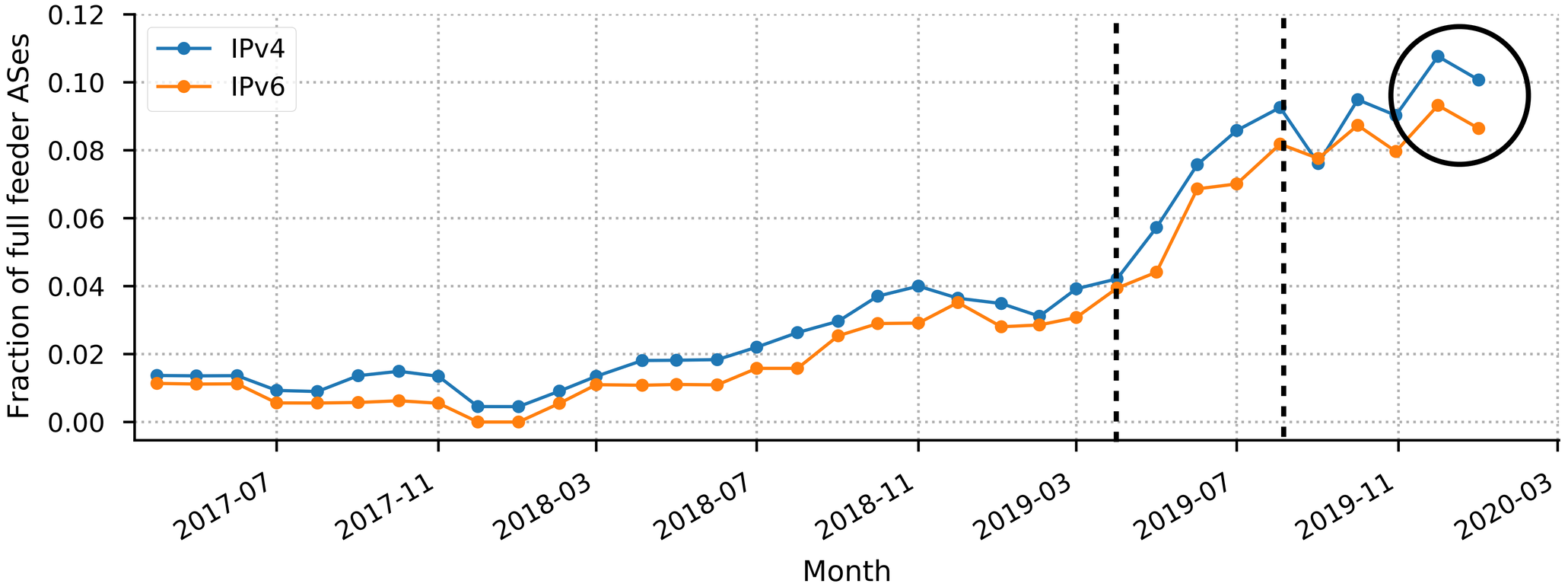


RPKI enforcement is starting to gain traction



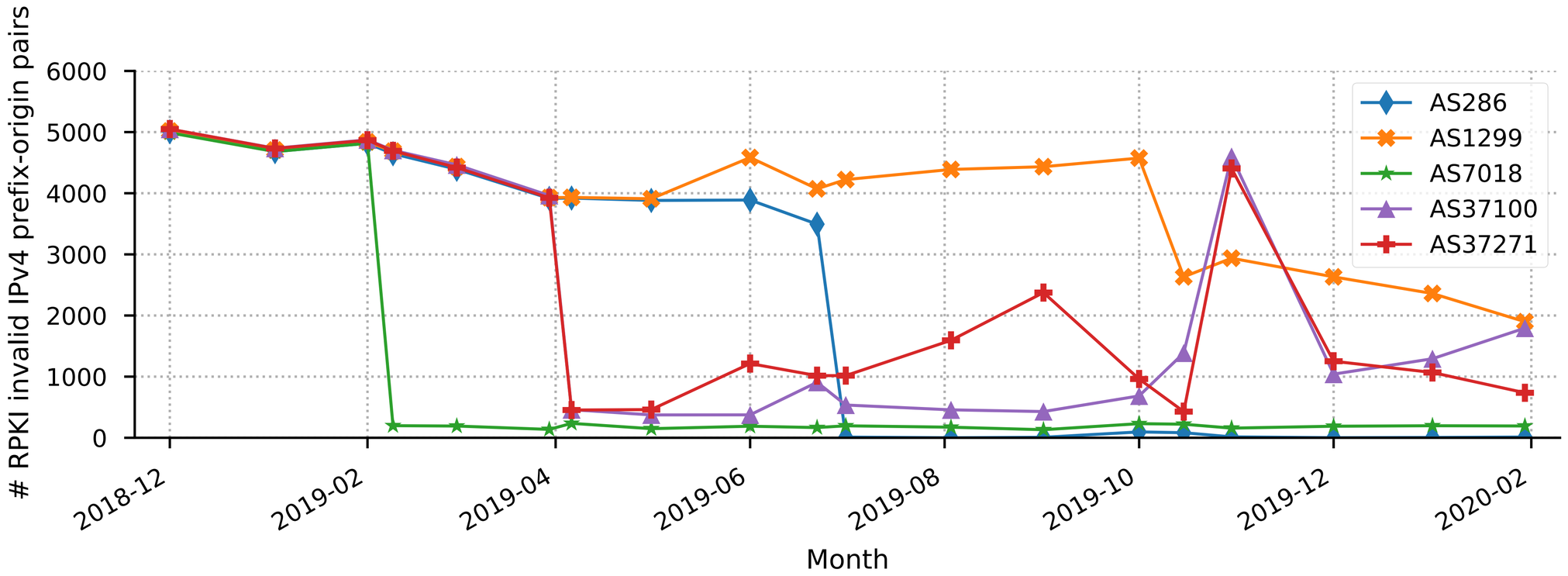
- Major increase between April and August 2019.

RPKI enforcement is starting to gain traction

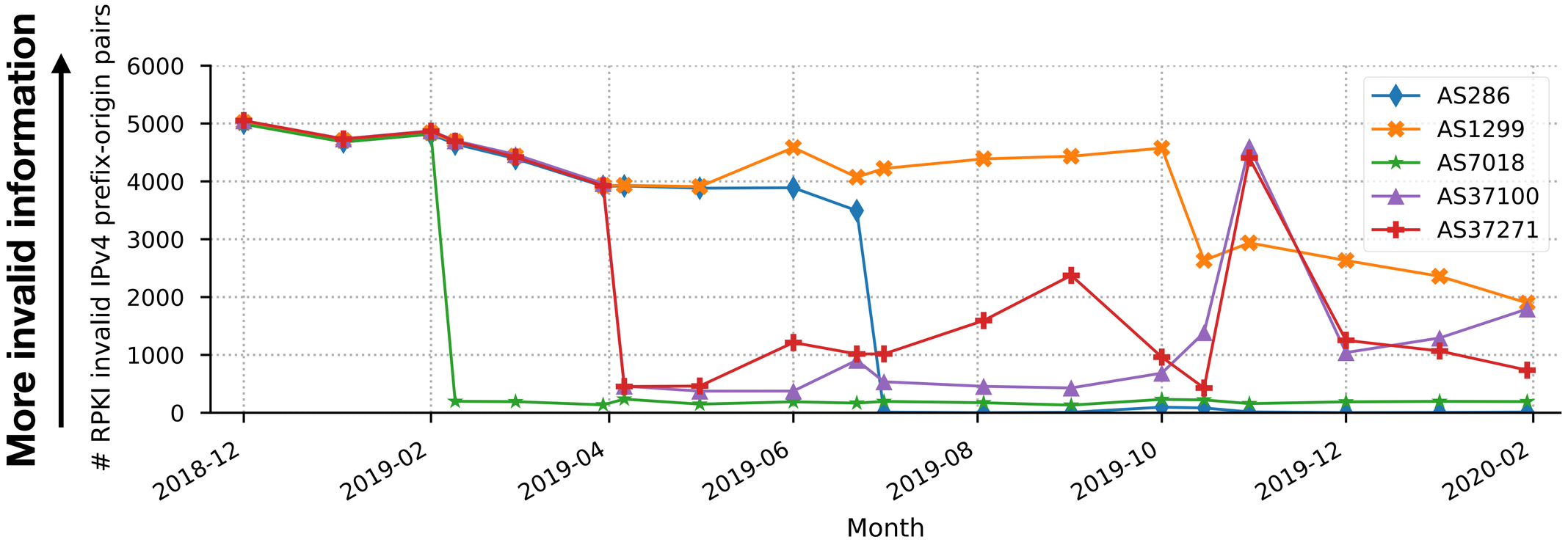


- Major increase between April and August 2019.
- 10% of considered ASes are enforcing RPKI in February 2020.

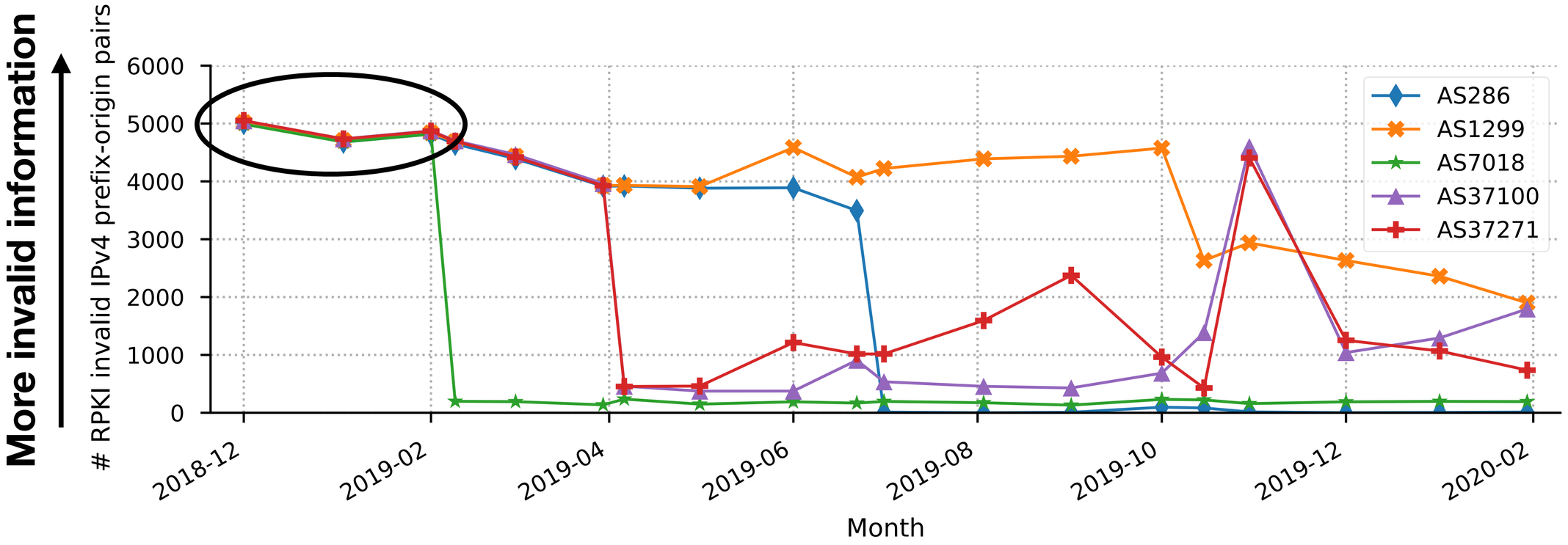
Cross-validation with public announcements of RPKI filtering



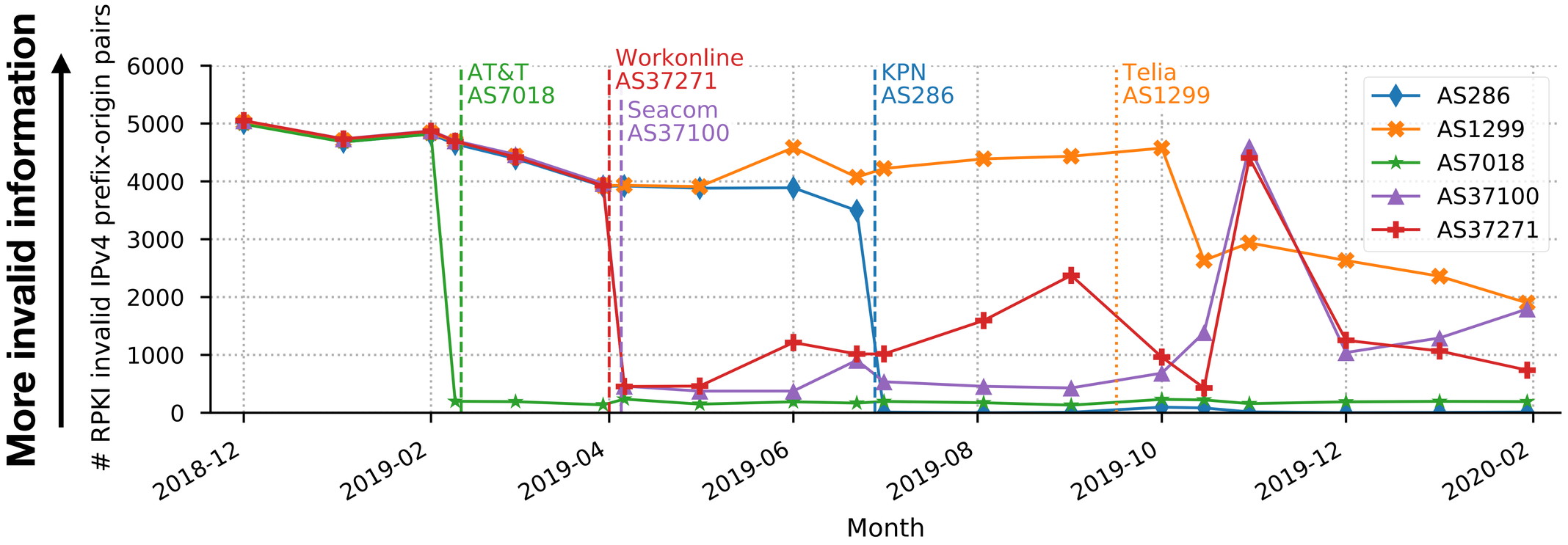
Cross-validation with public announcements of RPKI filtering



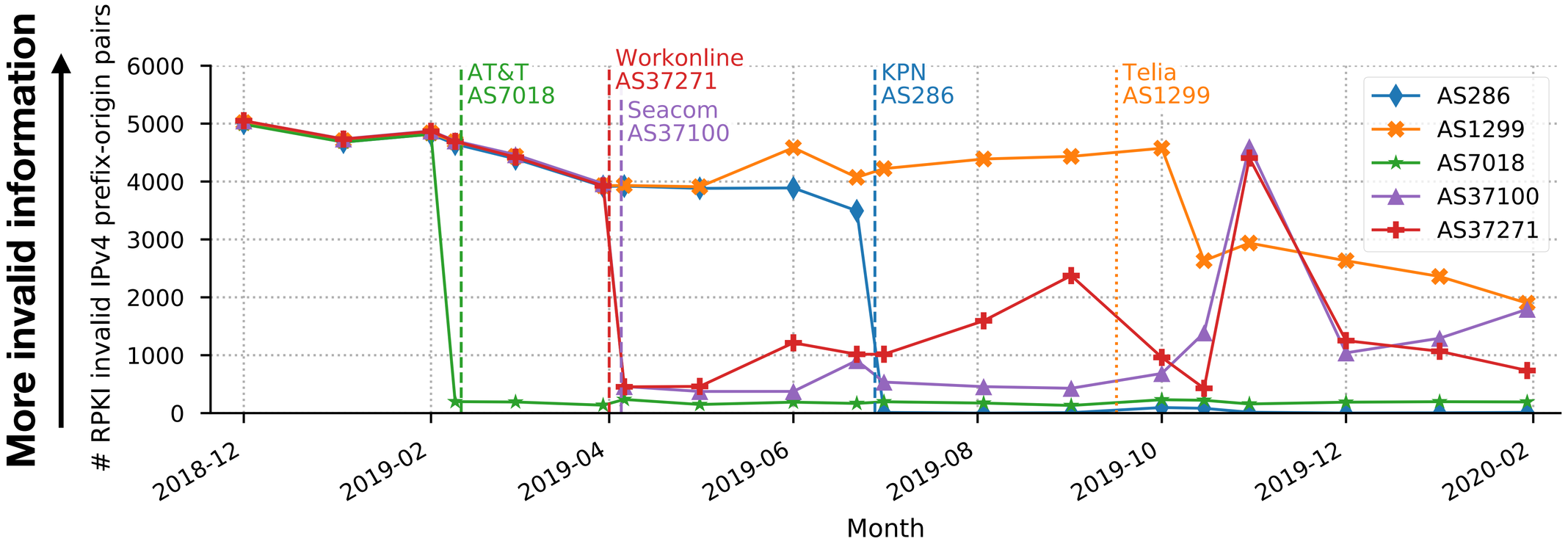
Cross-validation with public announcements of RPKI filtering



Cross-validation with public announcements of RPKI filtering

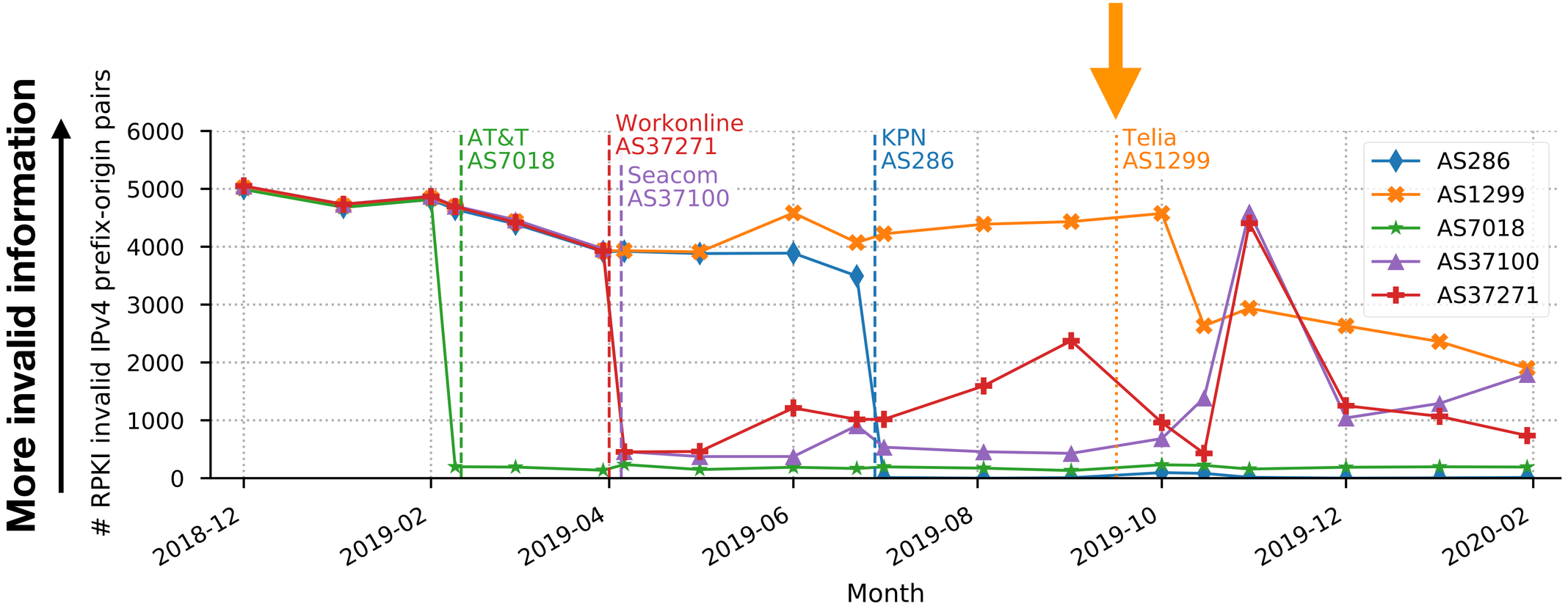


Cross-validation with public announcements of RPKI filtering



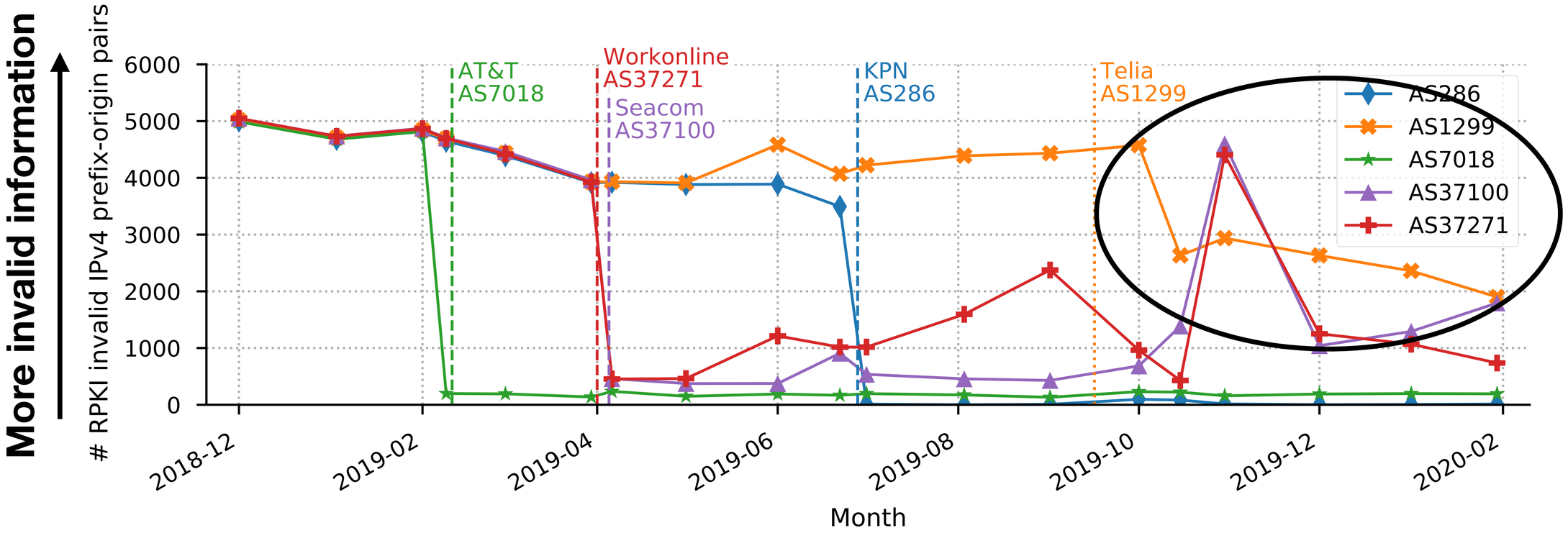
- We detect when ASes start enforcing RPKI filtering.

Cross-validation with public announcements of RPKI filtering



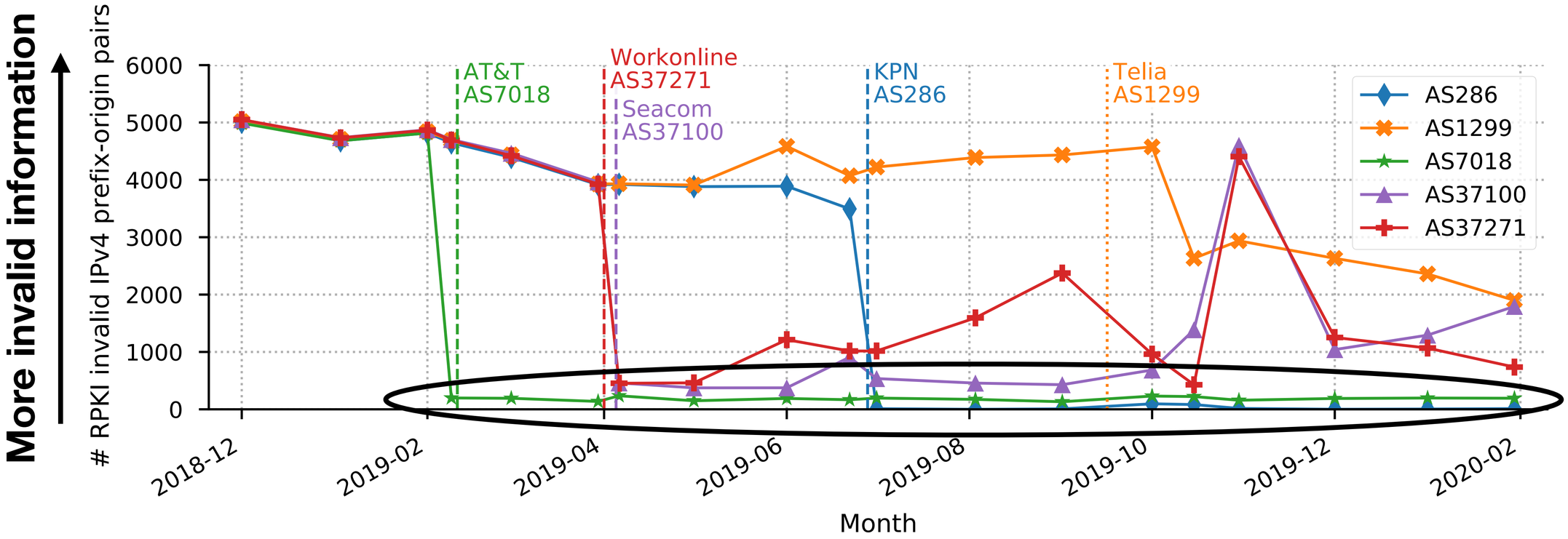
- We detect when ASes start enforcing RPKI filtering.

Cross-validation with public announcements of RPKI filtering



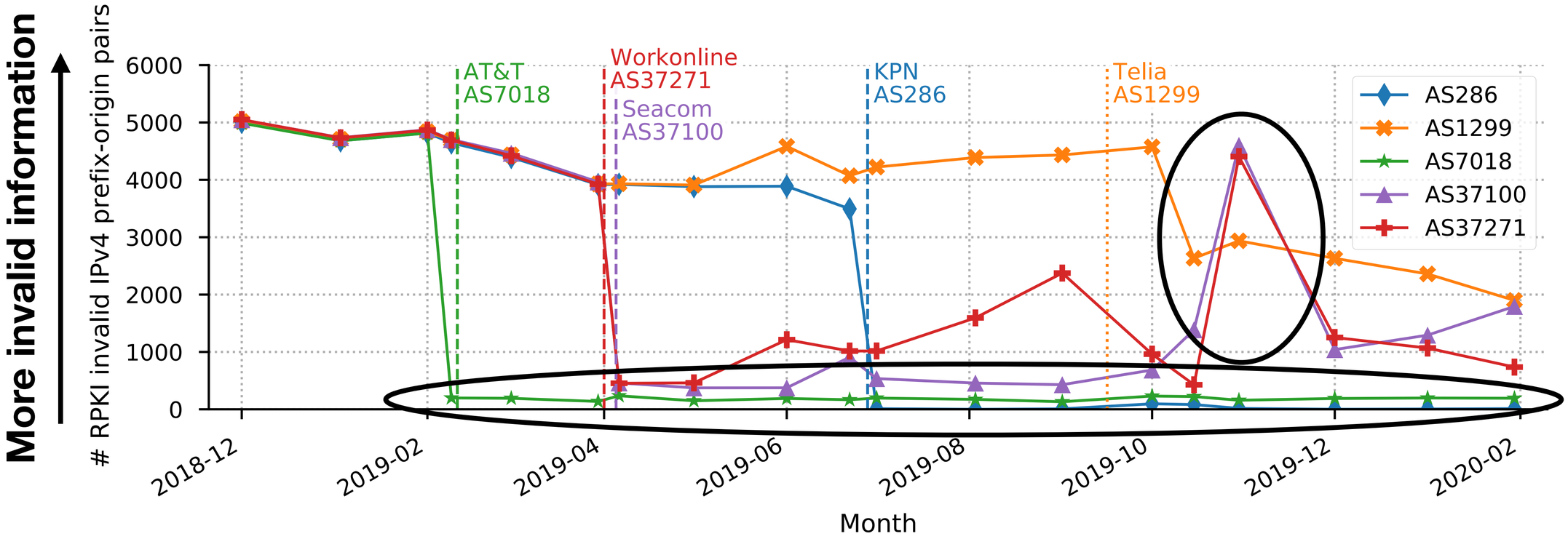
- We detect when ASes start enforcing RPKI filtering.

Cross-validation with public announcements of RPKI filtering



- We detect when ASes start enforcing RPKI filtering.

Cross-validation with public announcements of RPKI filtering



- We detect when ASes start enforcing RPKI filtering.
- No ASes filters all RPKI-invalid announcements.

Reasons for partial filtering

- **Selective RPKI Trust Anchor (TA) filtering:** some networks do not consider ROAs from the ARIN TA, resulting in more invalid prefix-origins propagated by them.

- **Selective filtering depending on AS relationships:** several network operators announced to implement filtering only for routes received from peers, but not customer networks.

- **Operational deployment issues**: some network operators reported compatibility issues with RPKI validator implementations and router software, prompting them to deploy RPKI-filtering in a subset of their border routers.

Fine-grained BGP & RPKI dataset

Prefix-origin timelines	Count	%
IPv4 total	883,400	100%
RPKI covered	147,870	17%
RPKI-valid	139,537	16%
RPKI-invalid	8,333	1%
IPv6 total	91,313	100%
RPKI covered	17,656	21%
RPKI-valid	362	19%
RPKI-invalid	1155	2%

Fine-grained BGP & RPKI dataset

Prefix-origin timelines	Count	%
IPv4 total	883,400	100%
RPKI covered	147,870	17%
RPKI-valid	139,537	16%
RPKI-invalid	8,333	1%
IPv6 total	91,313	100%
RPKI covered	17,656	21%
RPKI-valid	362	19%
RPKI-invalid	1155	2%

Covered IPv4

Covered IPv6

Fine-grained BGP & RPKI dataset

Prefix-origin timelines	Count	%
IPv4 total	883,400	100%
RPKI covered	147,870	17%
RPKI-valid	139,537	16%
RPKI-invalid	8,333	1%
IPv6 total	91,313	100%
RPKI covered	17,656	21%
RPKI-valid	362	19%
RPKI-invalid	1155	2%

Invalids IPv4

Invalids IPv6

Fine-grained BGP & RPKI dataset

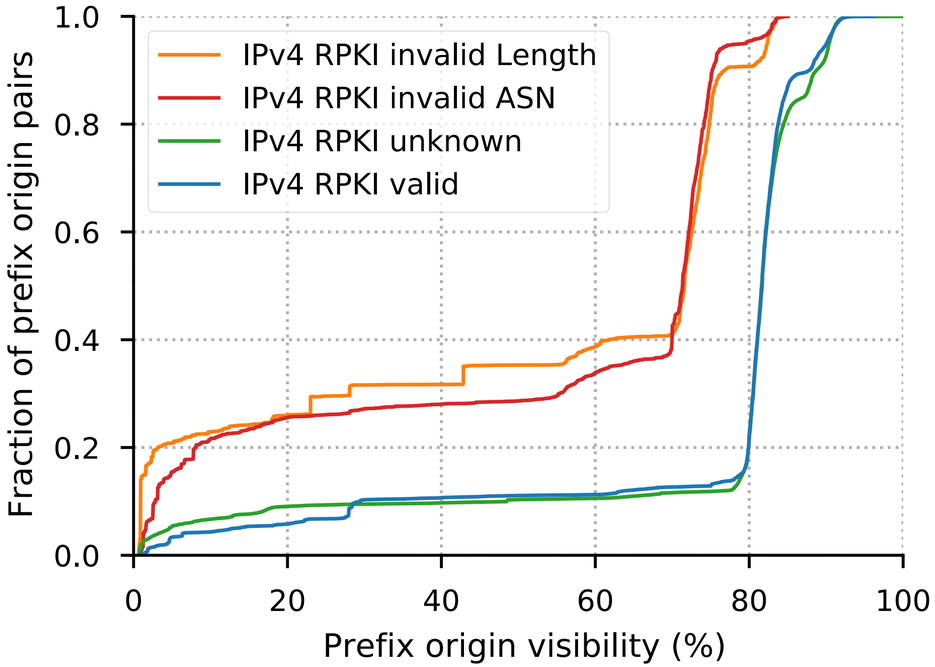
Prefix-origin timelines	Count	%
IPv4 total	883,400	100%
RPKI covered	147,870	17%
RPKI-valid	139,537	16%
RPKI-invalid	8,333	1%
IPv6 total	91,313	100%
RPKI covered	17,656	21%
RPKI-valid	362	19%
RPKI-invalid	1155	2%

Invalids IPv4

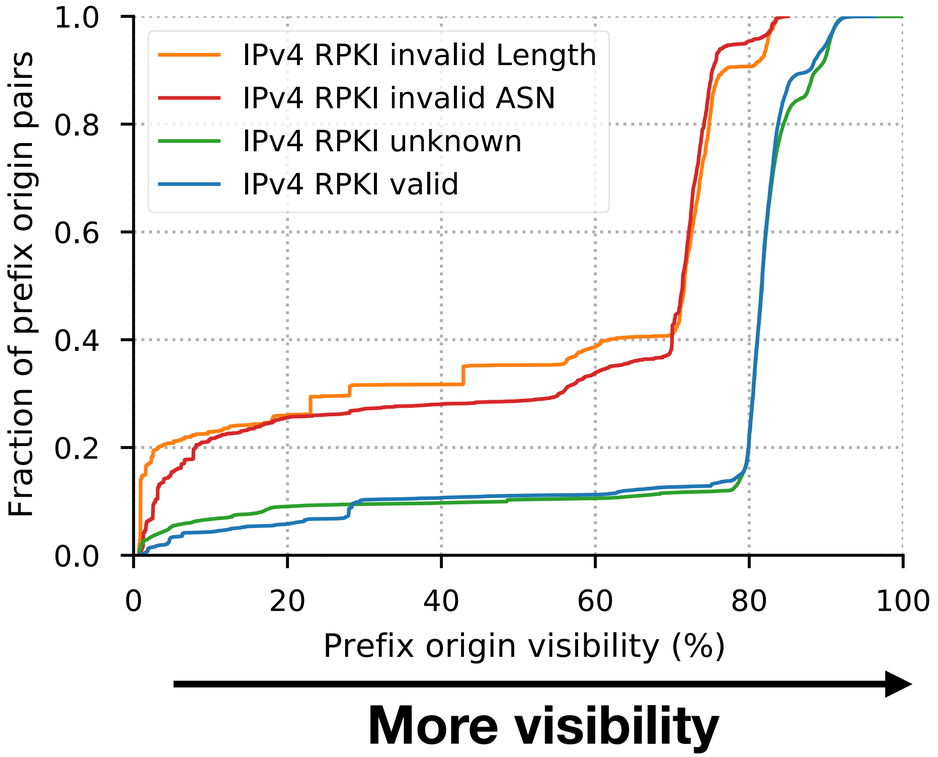
Invalids IPv6

- IPv4 and IPv6 results follow similar trends

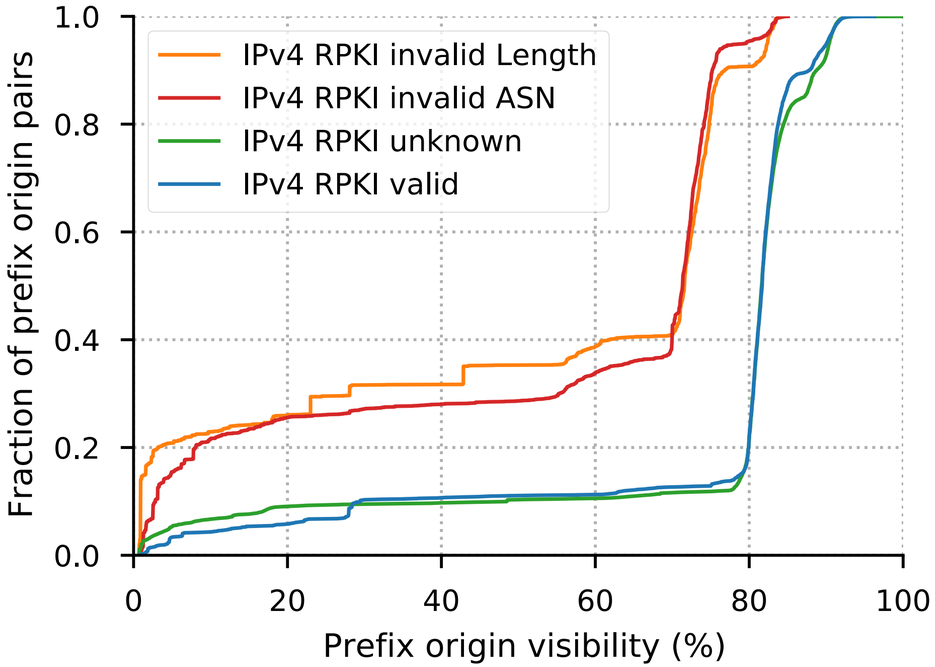
Prefix-origin pairs visibility by RPKI status



Prefix-origin pairs visibility by RPKI status

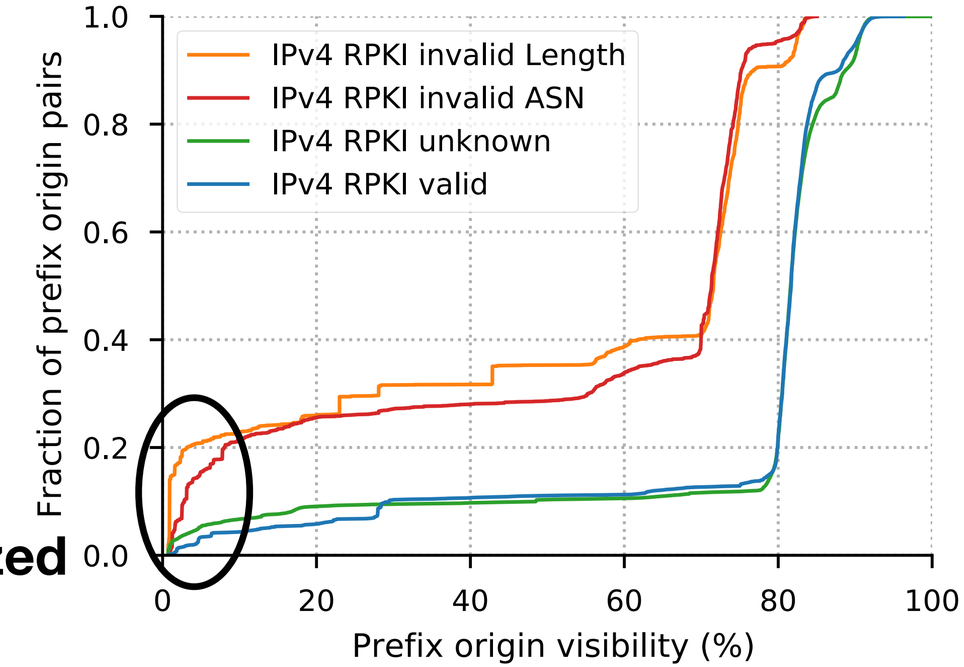


Prefix-origin pairs visibility by RPKI status



- **RPKI-invalid** prefixes **are less visible** than RPKI-valid or -unknown:

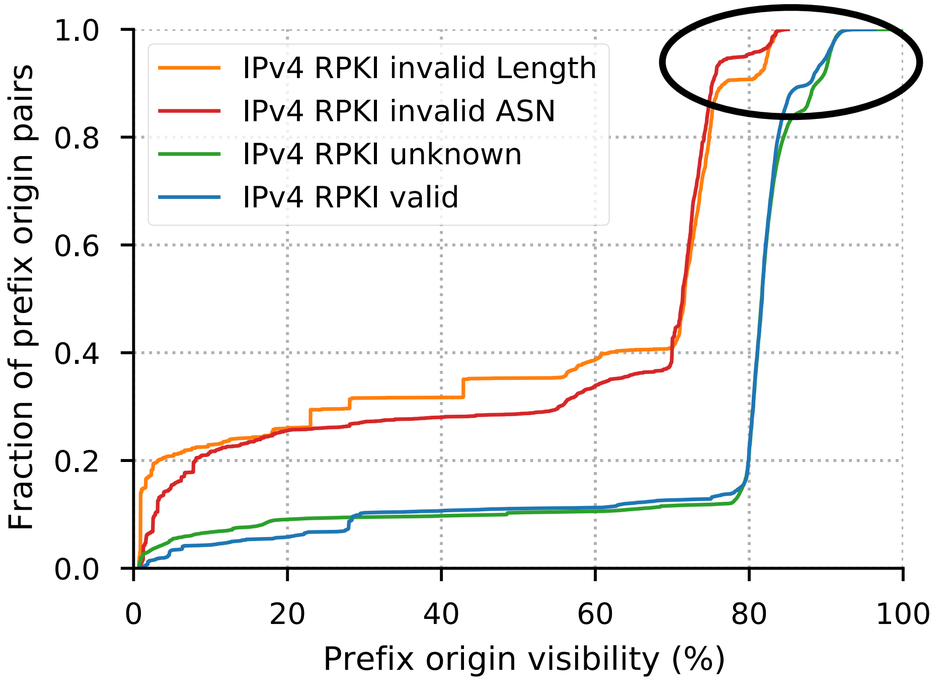
Prefix-origin pairs visibility by RPKI status



Very localized prefixes

- **RPKI-invalid** prefixes **are less visible** than RPKI-valid or -unknown:
  - large share (20%) of **very localized** RPKI-invalid prefixes

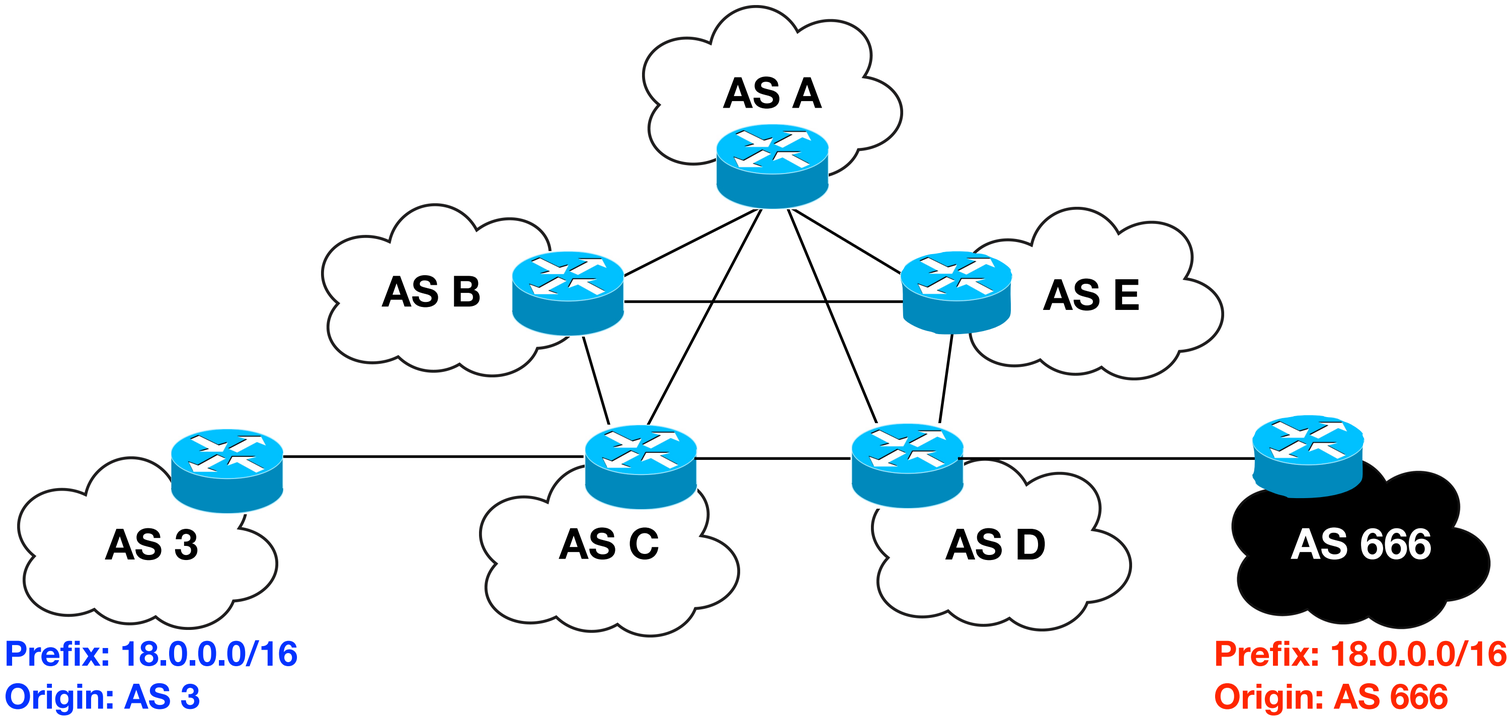
Prefix-origin pairs visibility by RPKI status



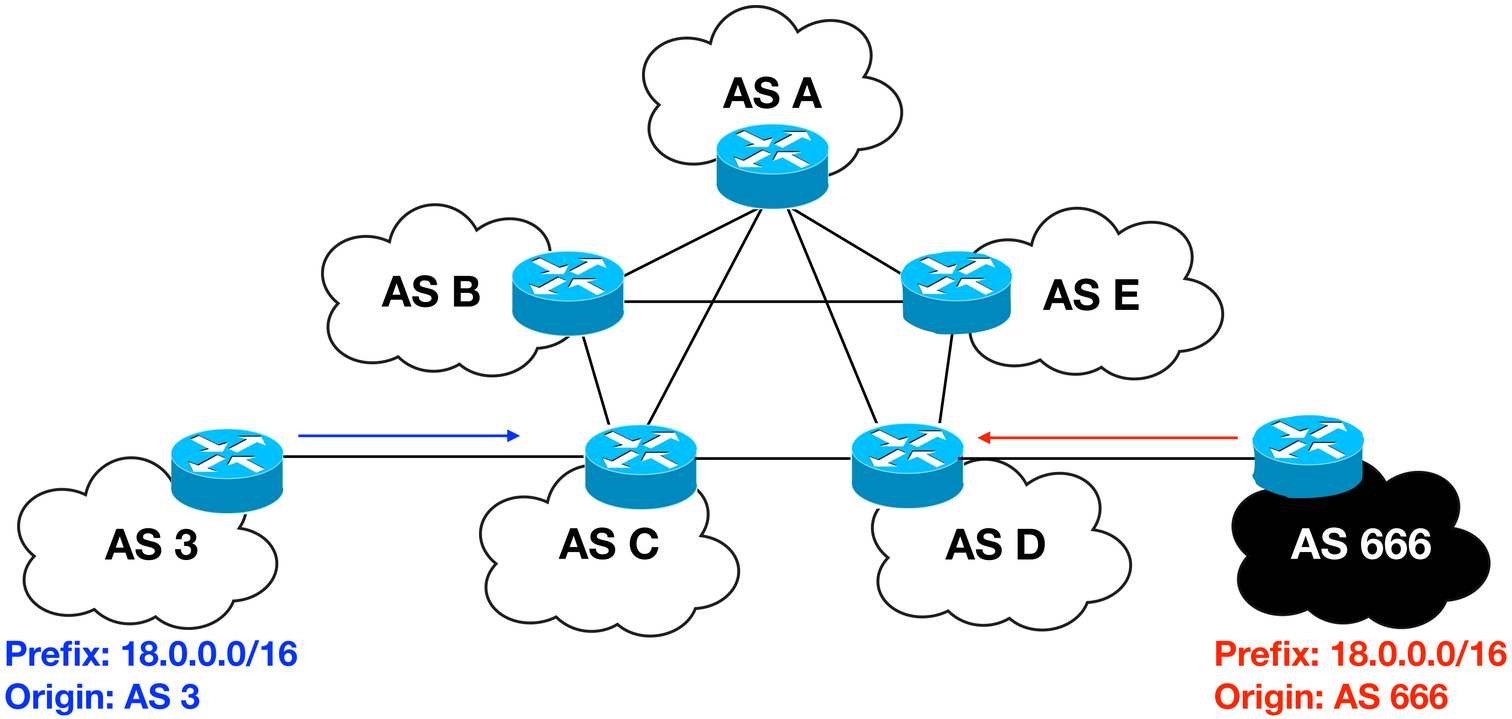
High visibility prefixes

- **RPKI-invalid** prefixes **are less visible** than RPKI-valid or -unknown:
  - large share (20%) of **very localized** RPKI-invalid prefixes
  - RPKI-invalid prefixes **never** reach the **higher levels of visibility**

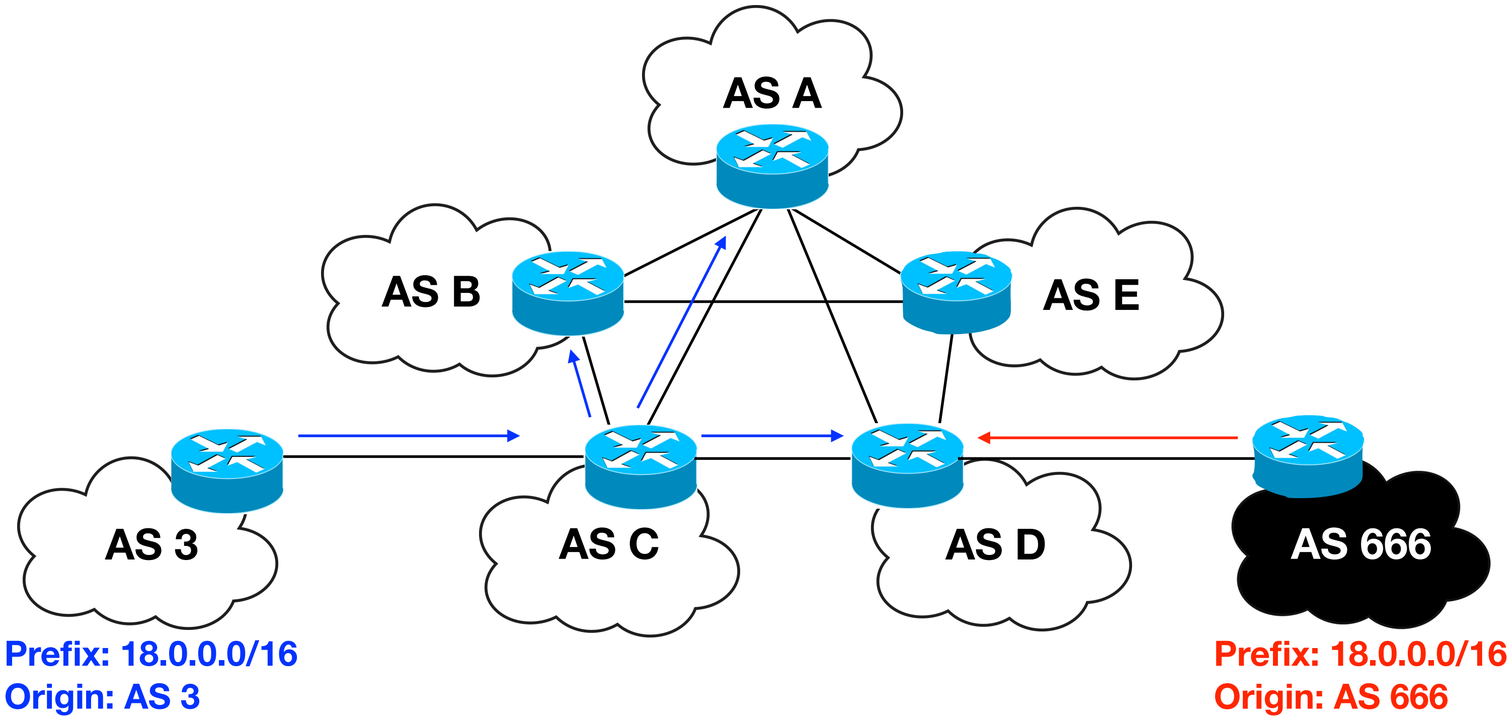
Multiple Origin AS (MOAS) conflicts



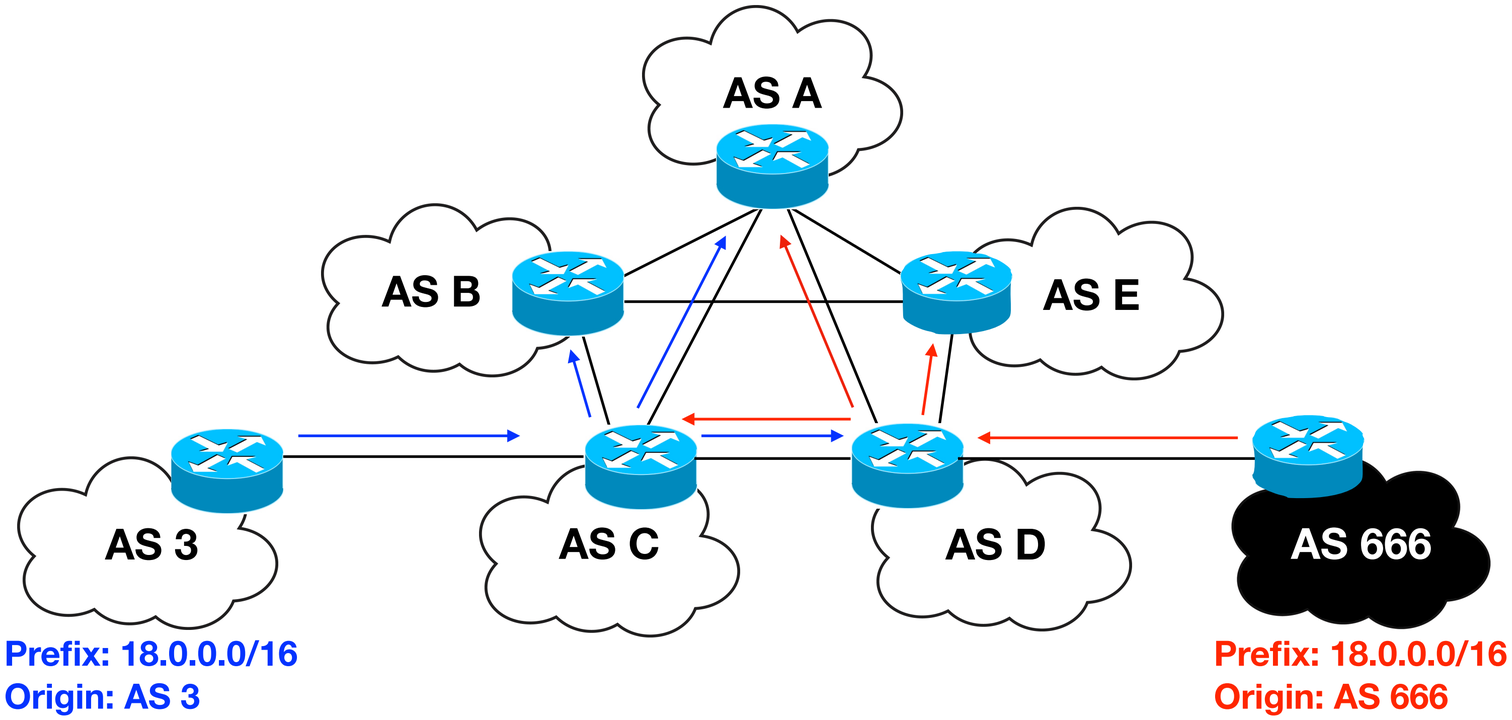
Multiple Origin AS (MOAS) conflicts



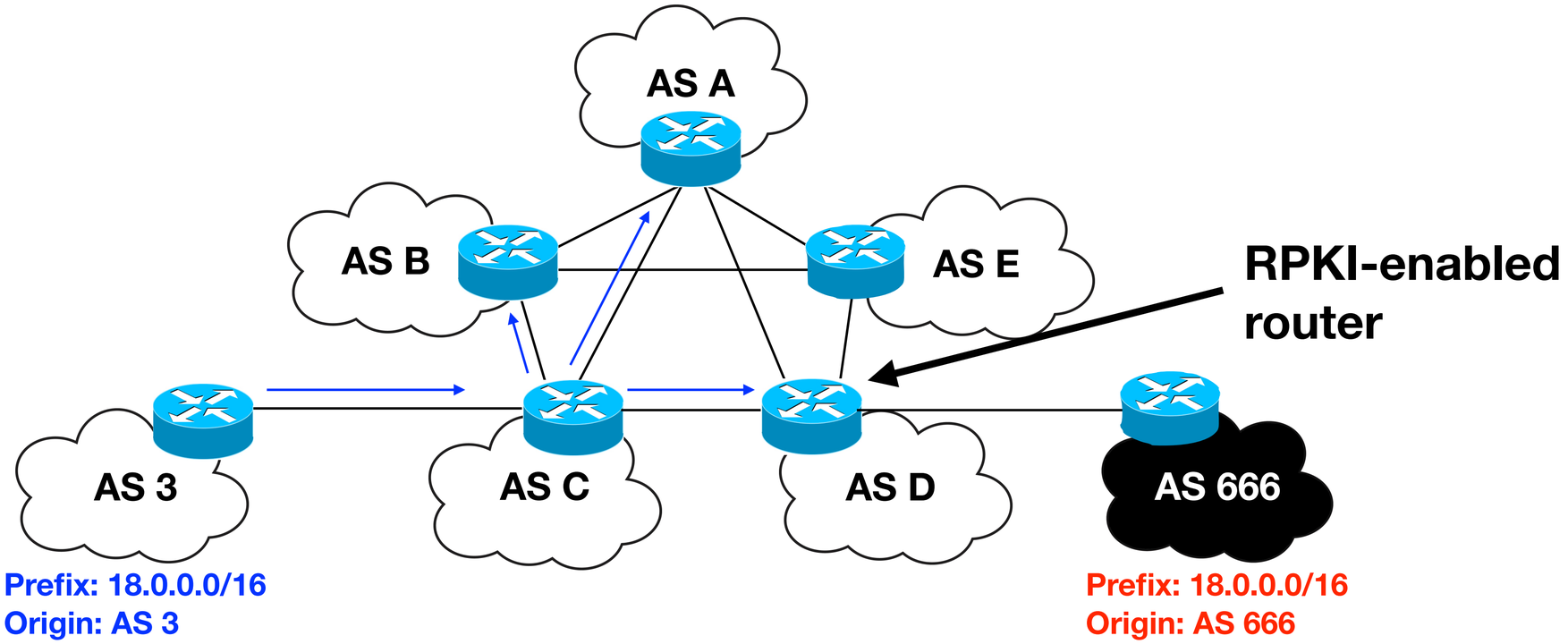
Multiple Origin AS (MOAS) conflicts



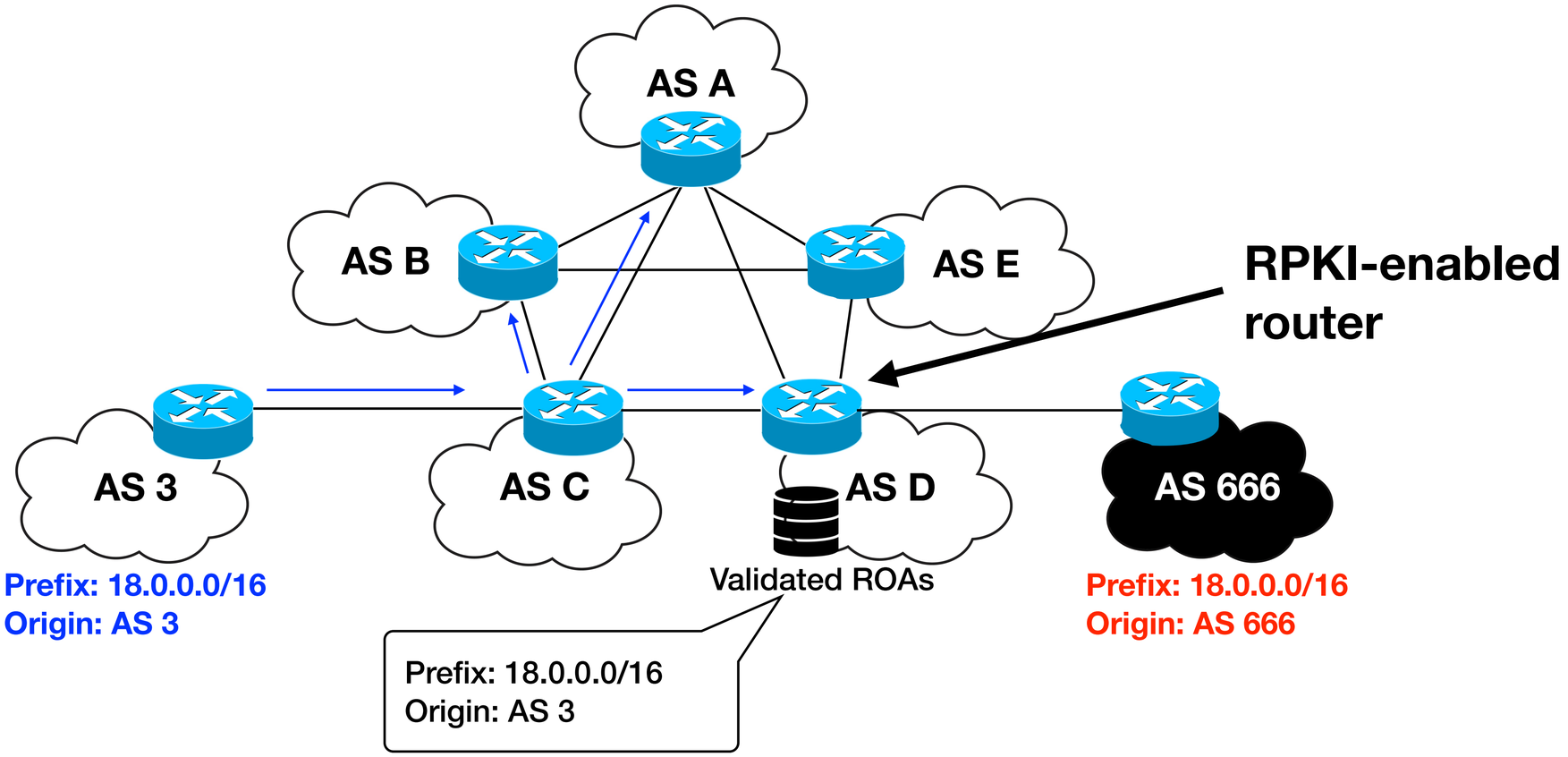
Multiple Origin AS (MOAS) conflicts



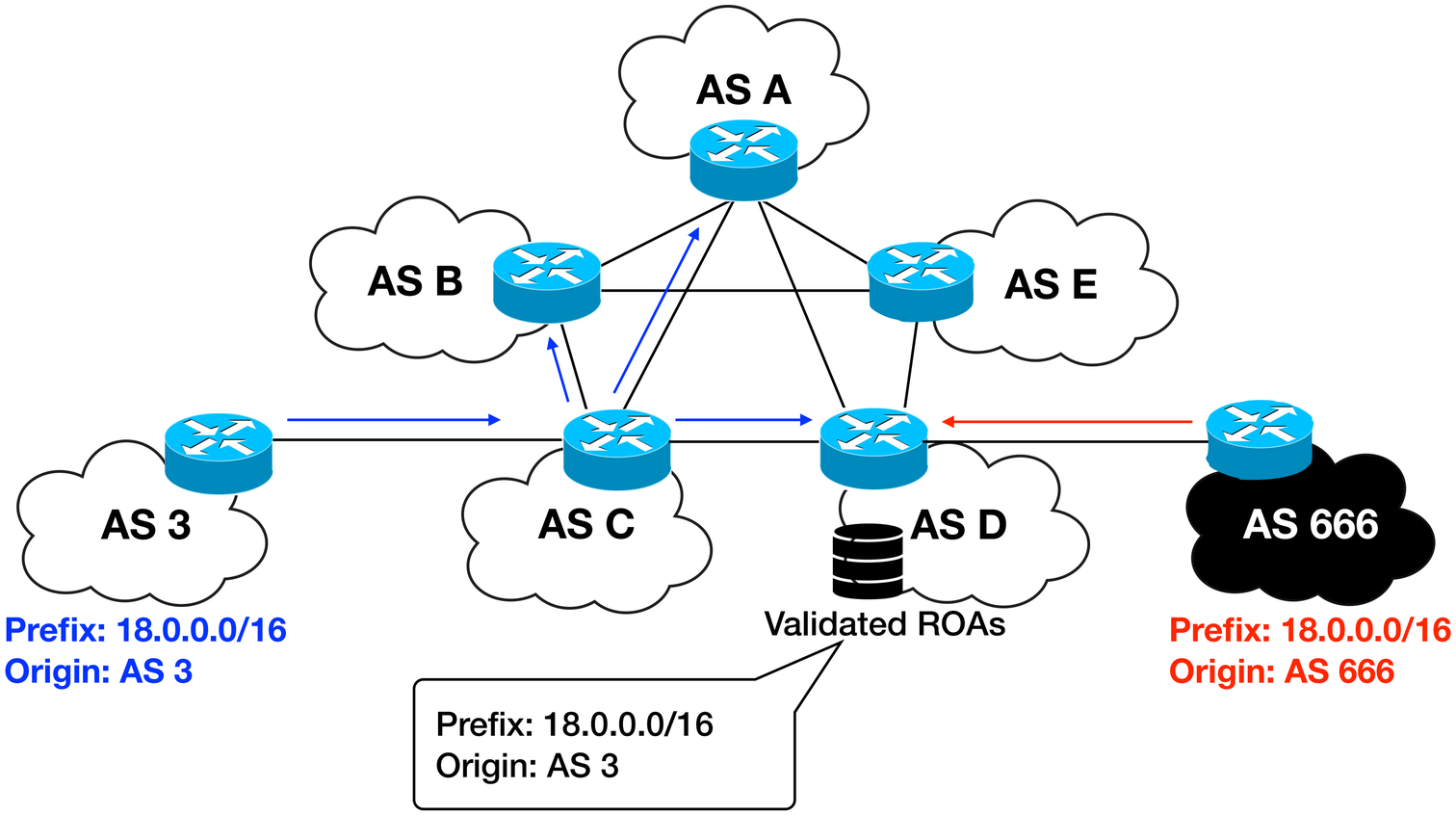
Multiple Origin AS (MOAS) conflicts



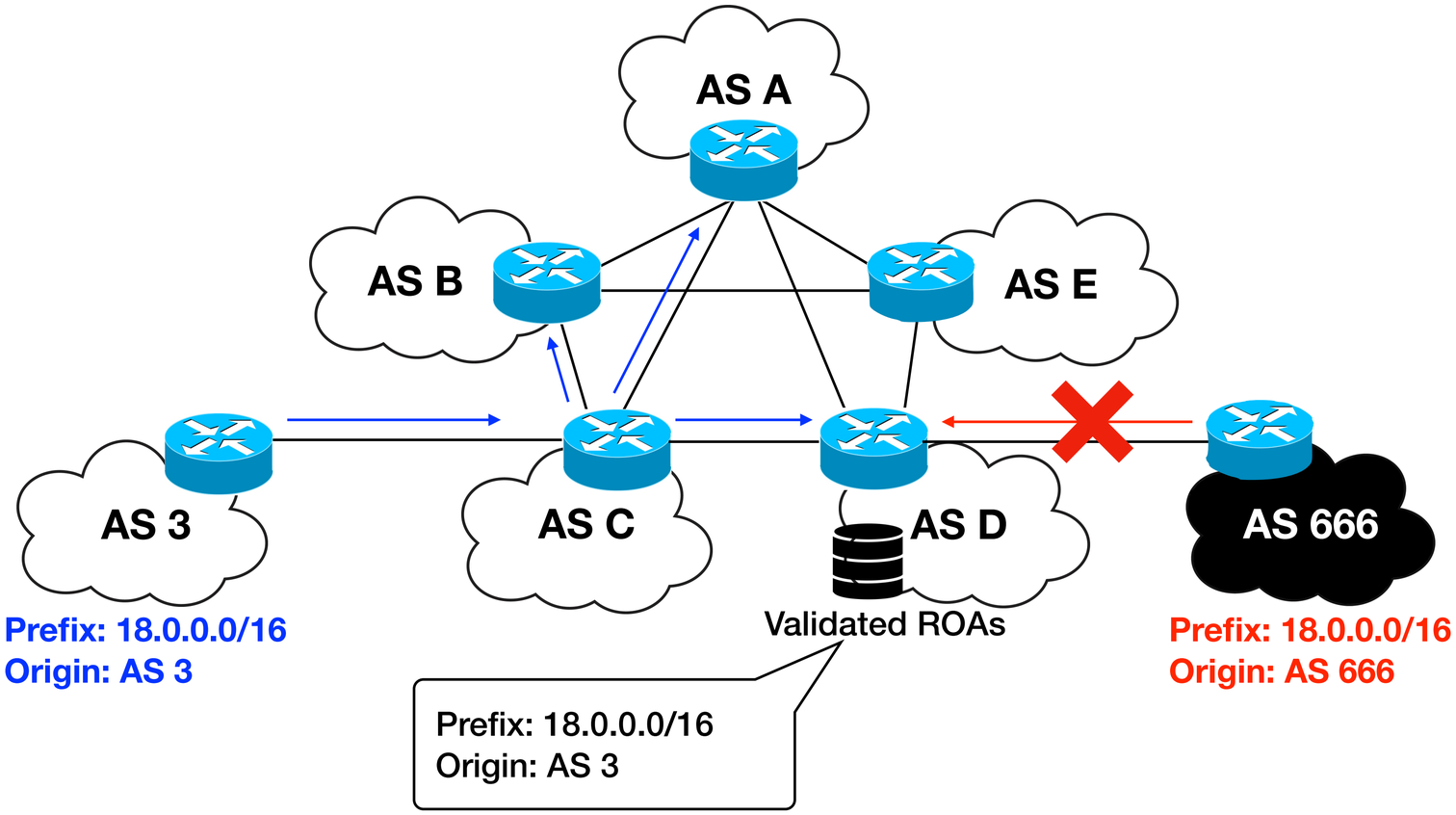
Multiple Origin AS (MOAS) conflicts



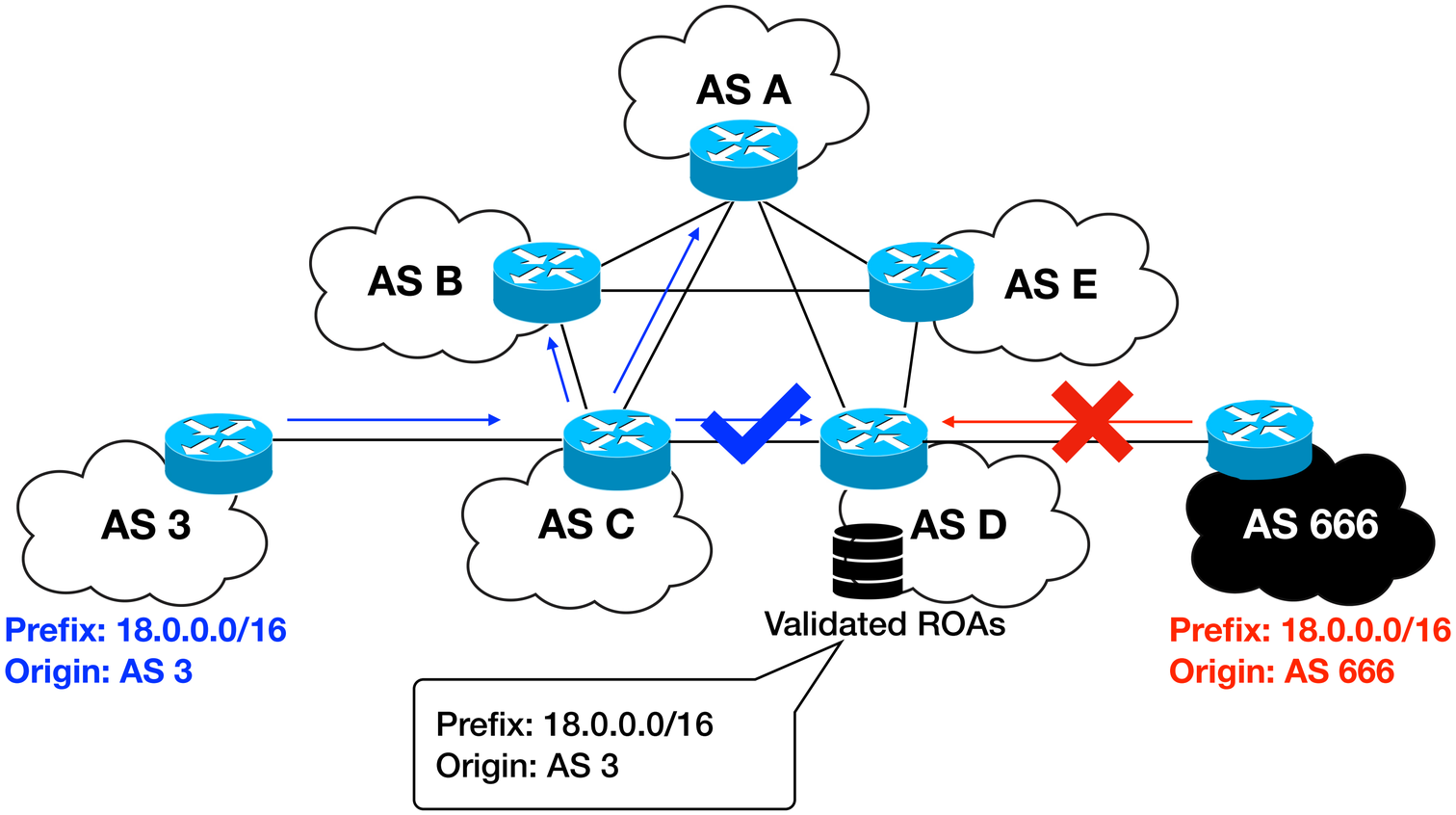
Multiple Origin AS (MOAS) conflicts



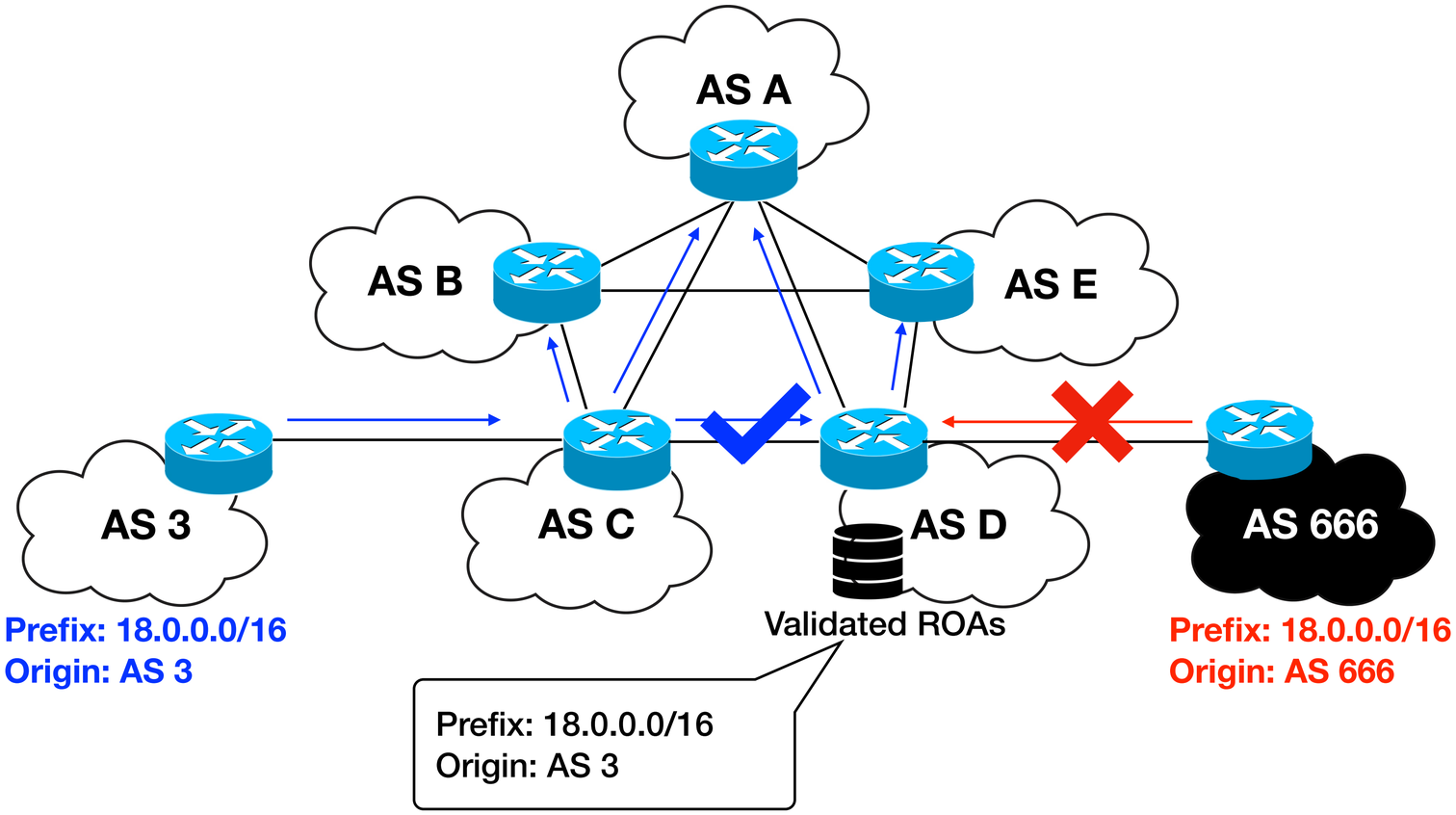
Multiple Origin AS (MOAS) conflicts



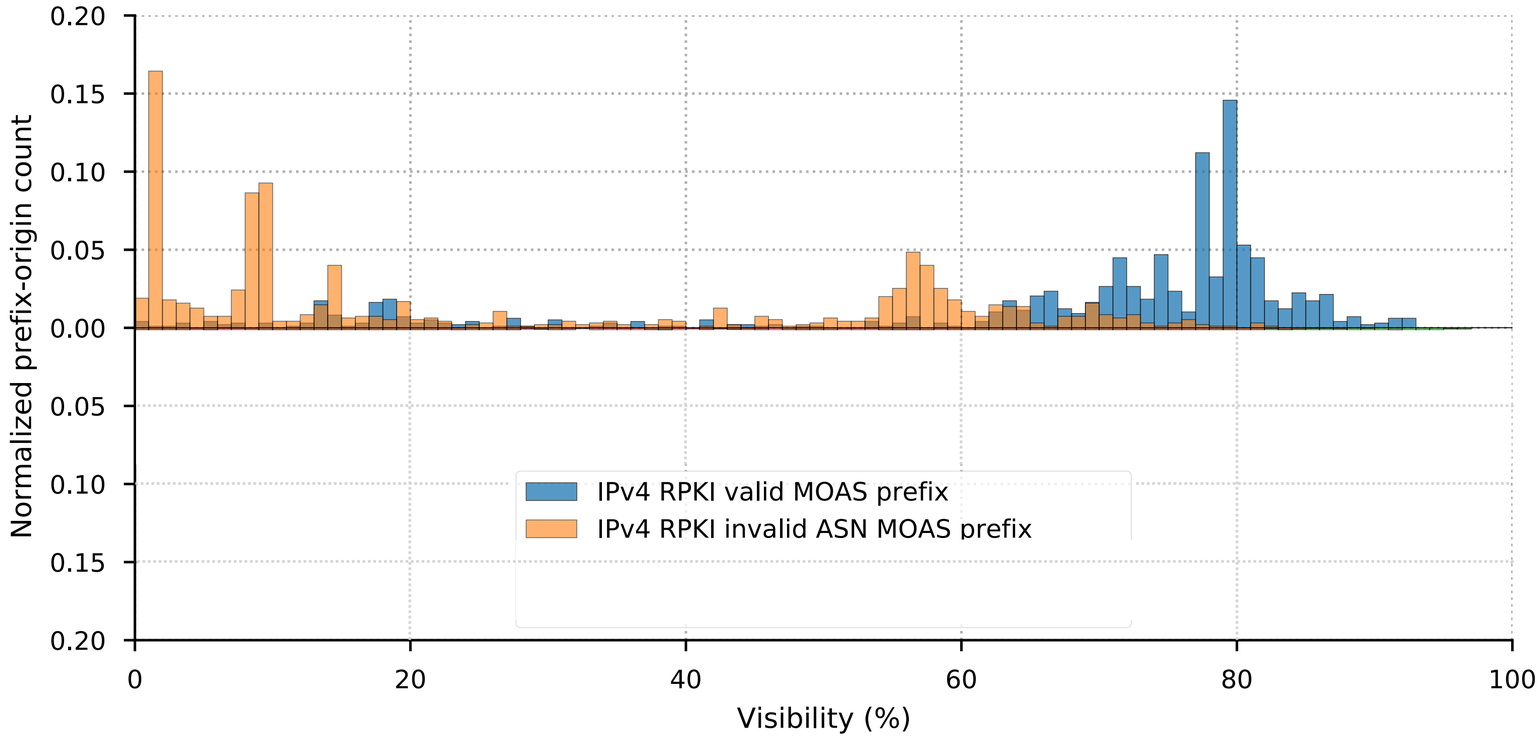
Multiple Origin AS (MOAS) conflicts



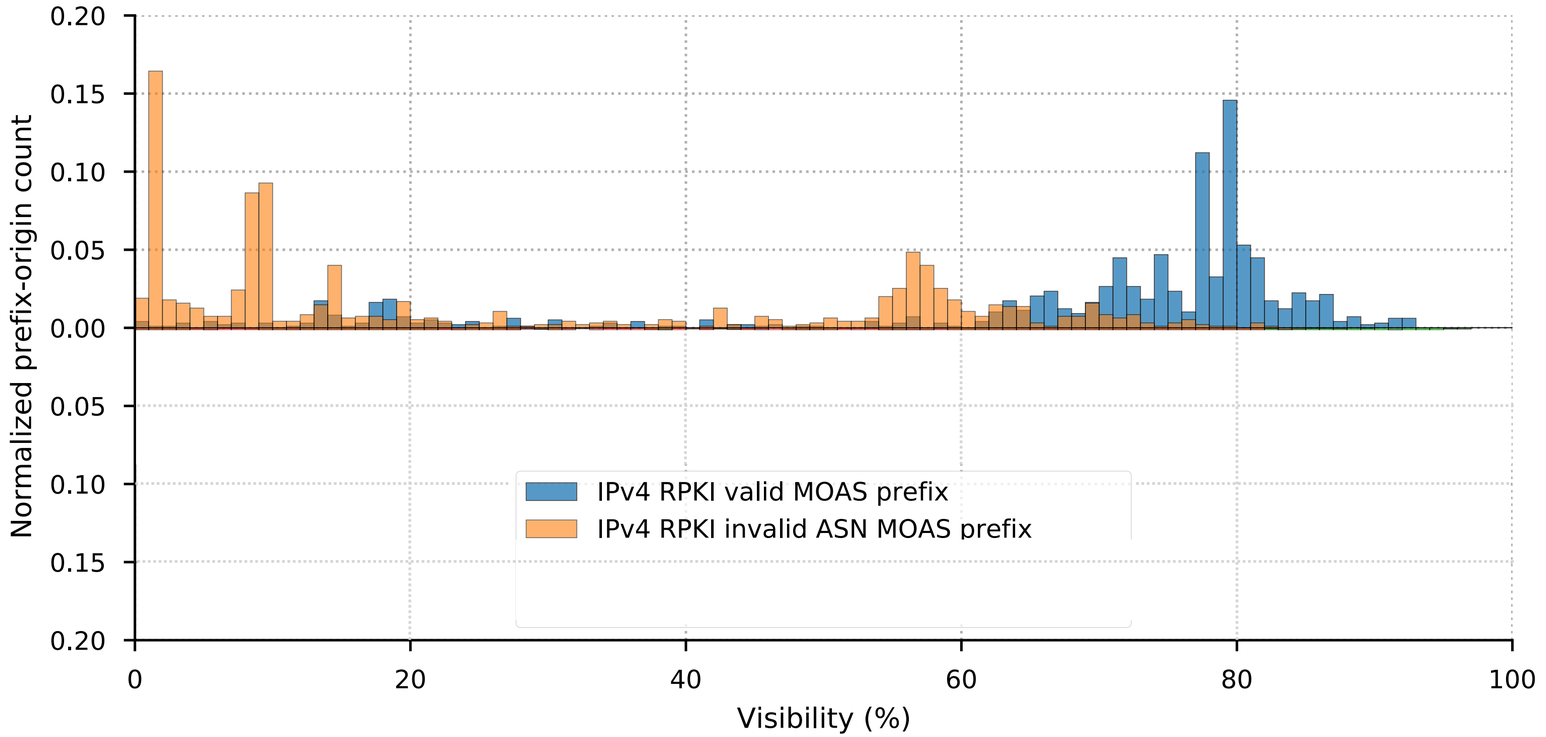
Multiple Origin AS (MOAS) conflicts



Prefix-origin visibility in the case of MOAS conflicts

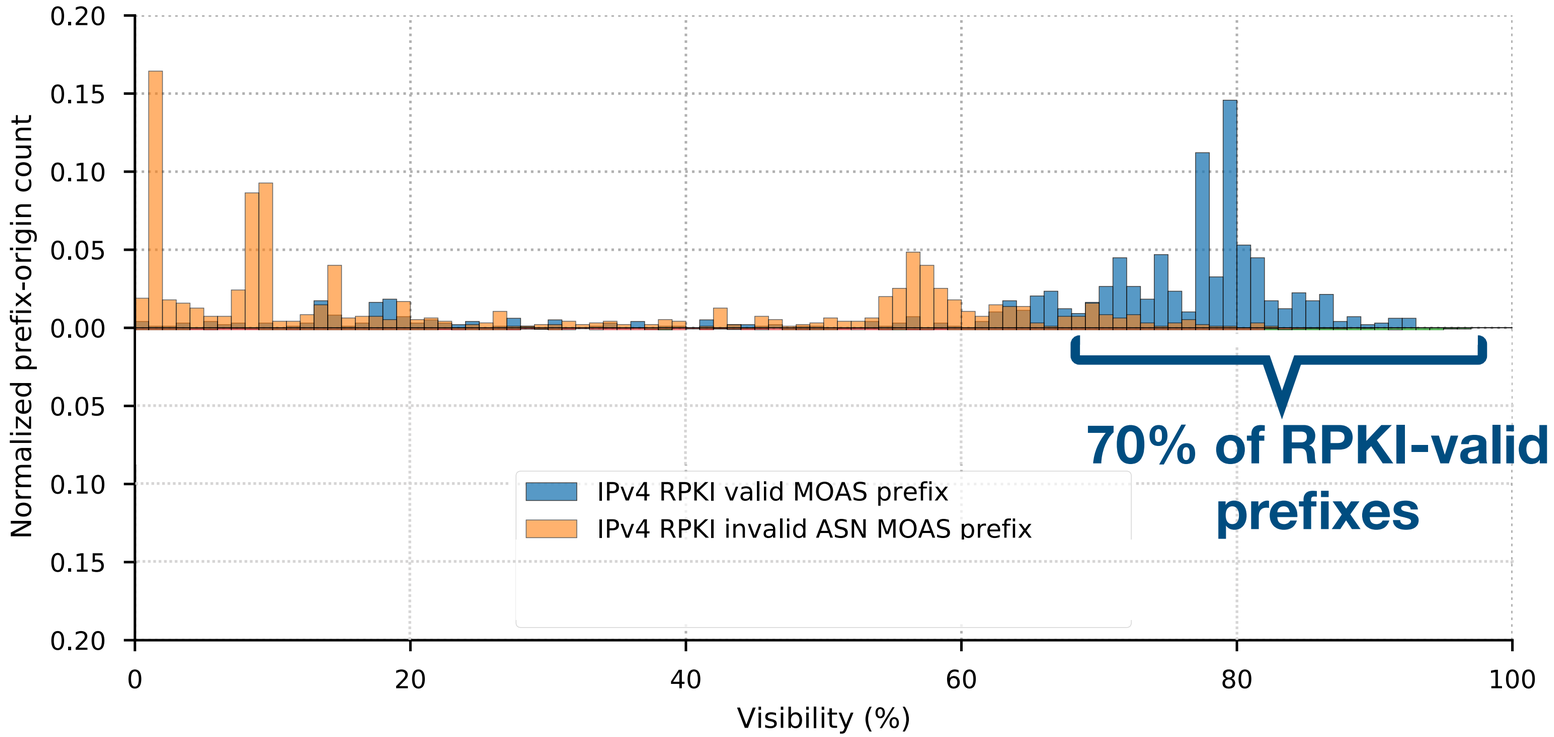


Prefix-origin visibility in the case of MOAS conflicts



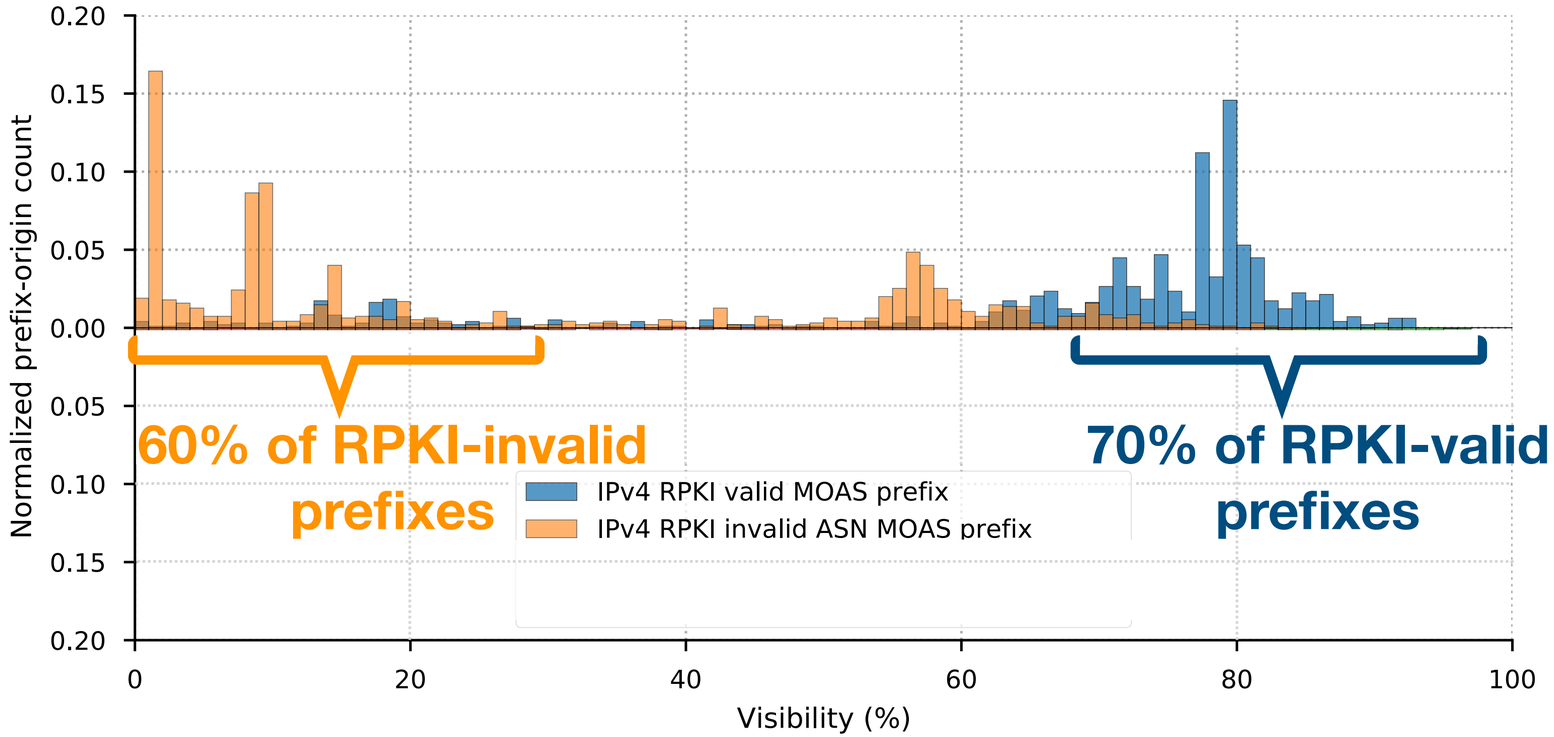
- RPKI-valid prefixes **dominate visibility** in MOAS conflicts.

Prefix-origin visibility in the case of MOAS conflicts



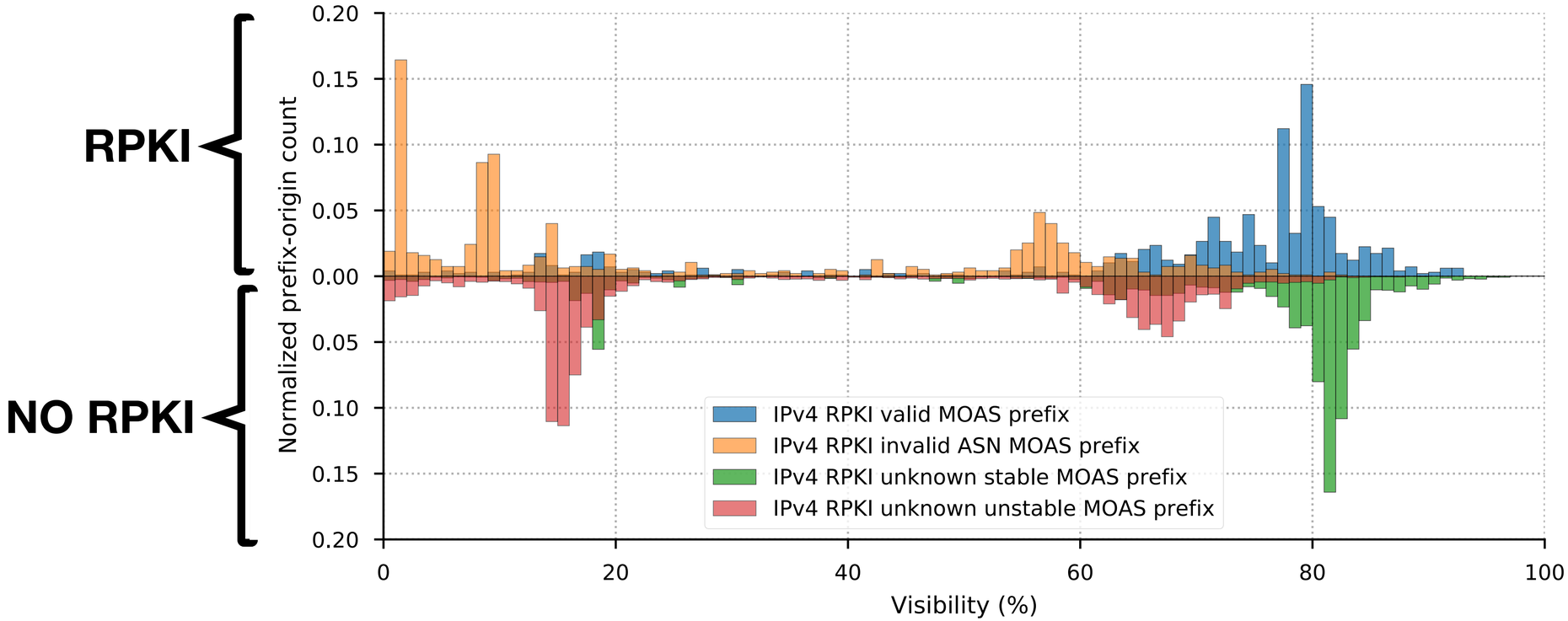
- RPKI-valid prefixes **dominate visibility** in MOAS conflicts.

Prefix-origin visibility in the case of MOAS conflicts



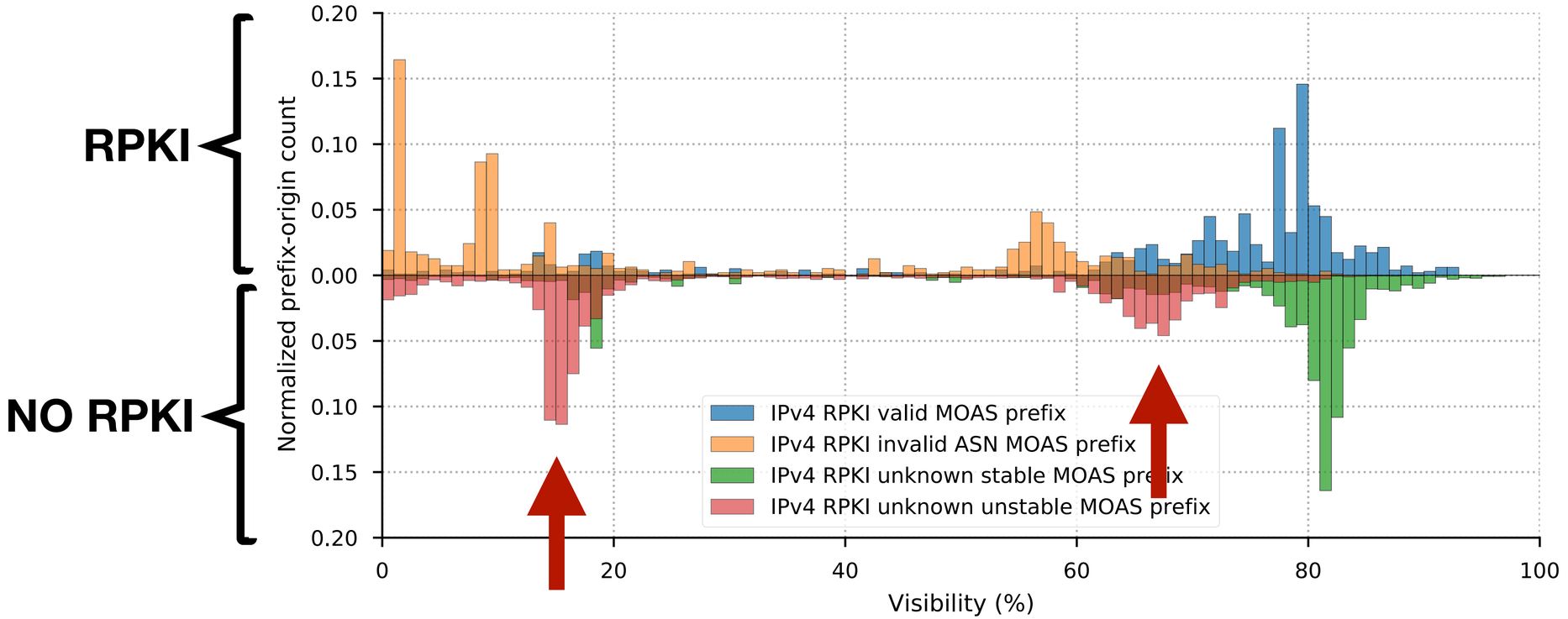
- RPKI-valid prefixes **dominate visibility** in MOAS conflicts.

Prefix-origin visibility in the case of MOAS conflicts



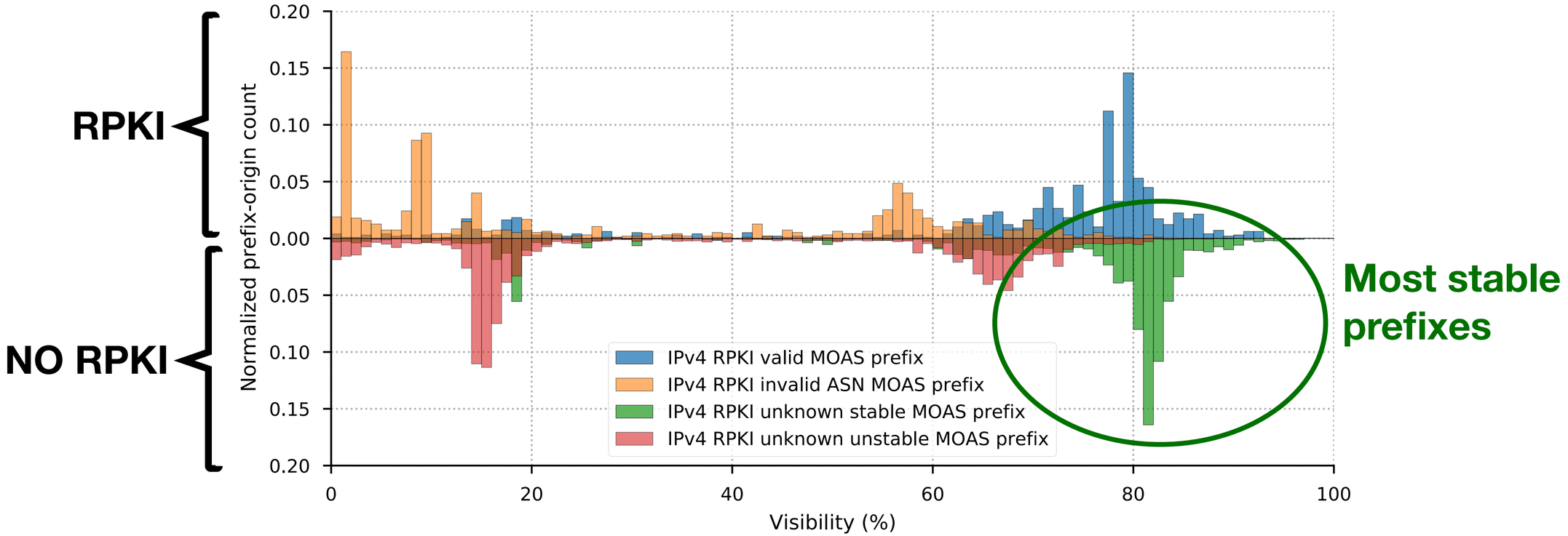
- RPKI-valid prefixes **dominate visibility** in MOAS conflicts.

Prefix-origin visibility in the case of MOAS conflicts



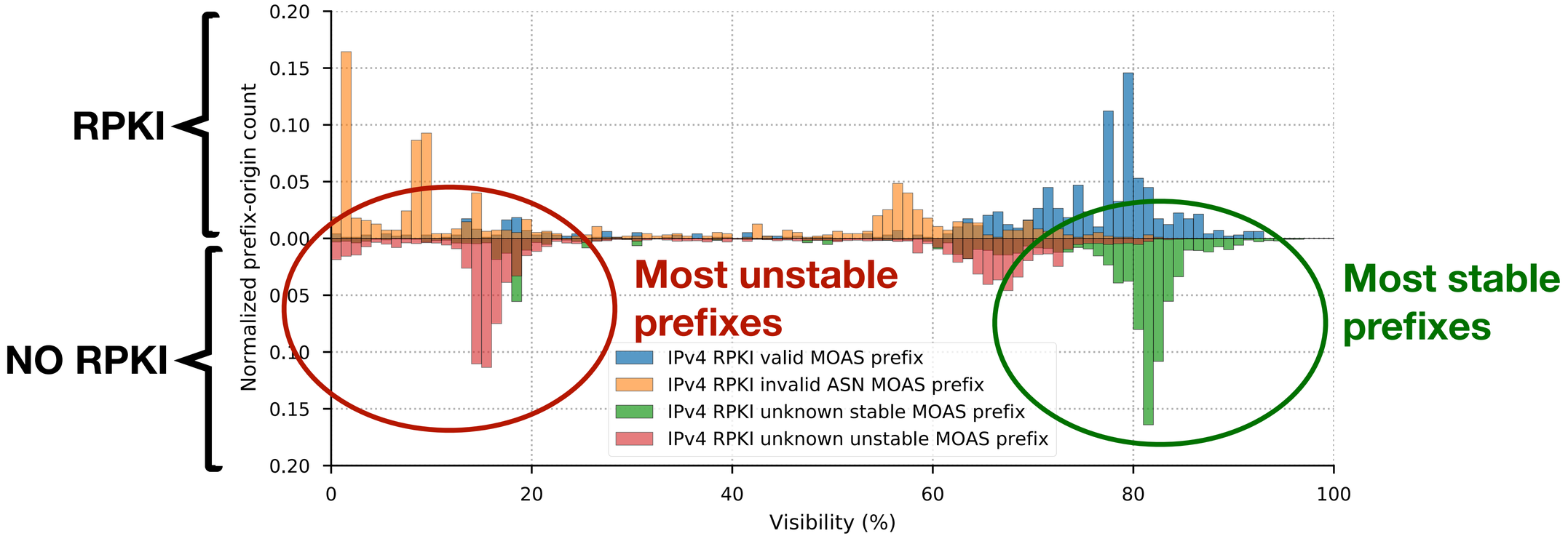
- RPKI-valid prefixes **dominate visibility** in MOAS conflicts.

Prefix-origin visibility in the case of MOAS conflicts



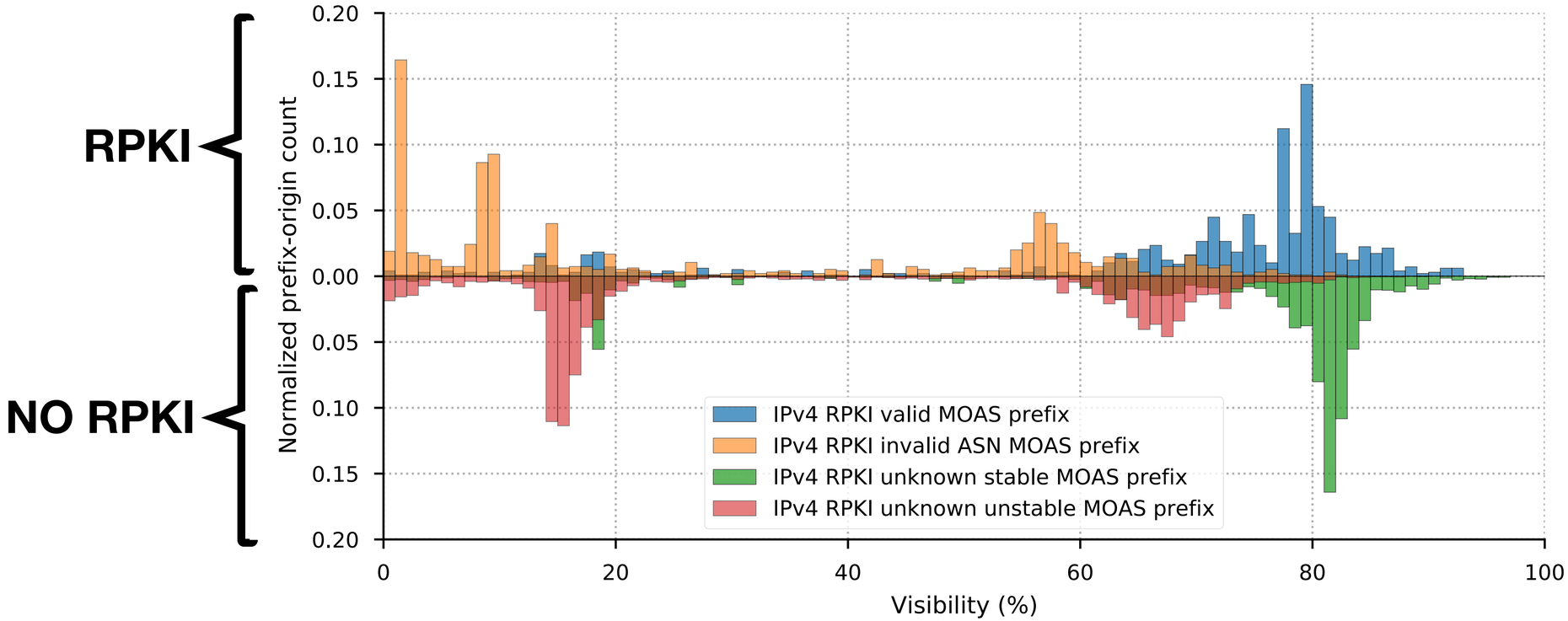
- RPKI-valid prefixes **dominate visibility** in MOAS conflicts.

Prefix-origin visibility in the case of MOAS conflicts



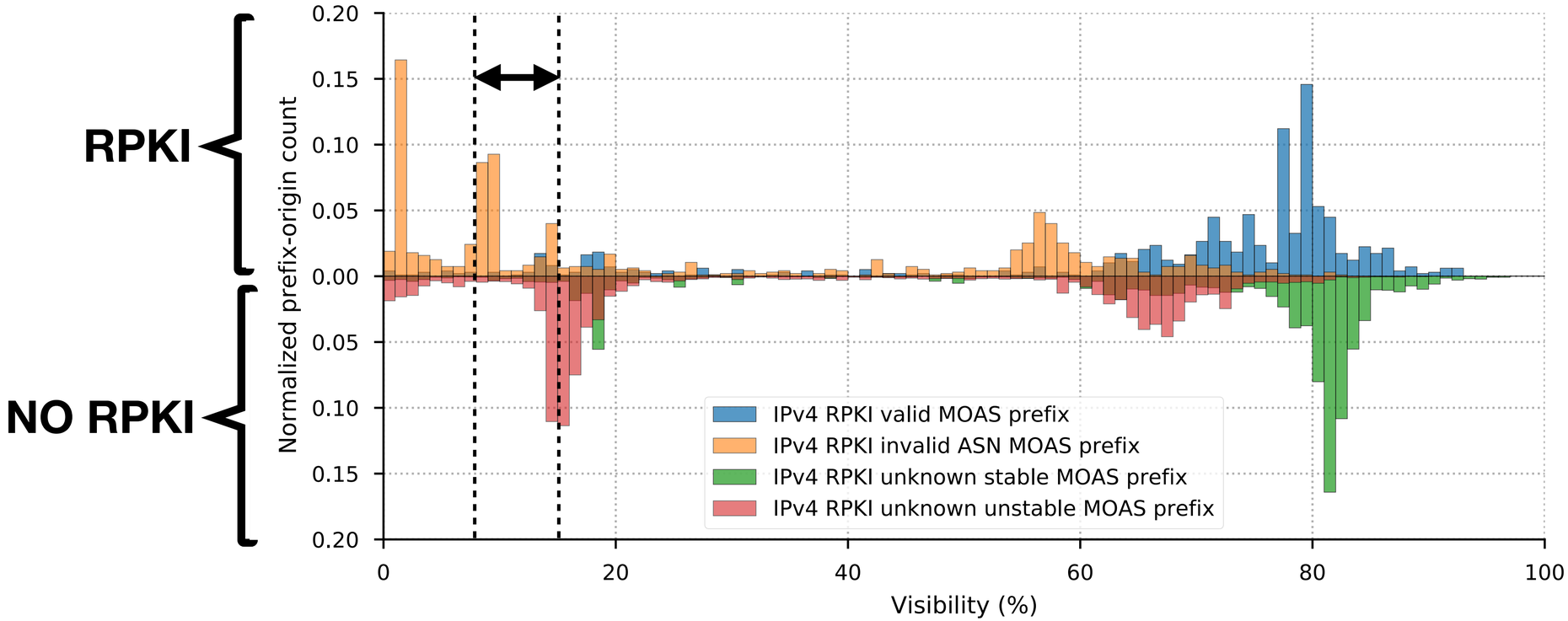
- RPKI-valid prefixes **dominate visibility** in MOAS conflicts.

Prefix-origin visibility in the case of MOAS conflicts



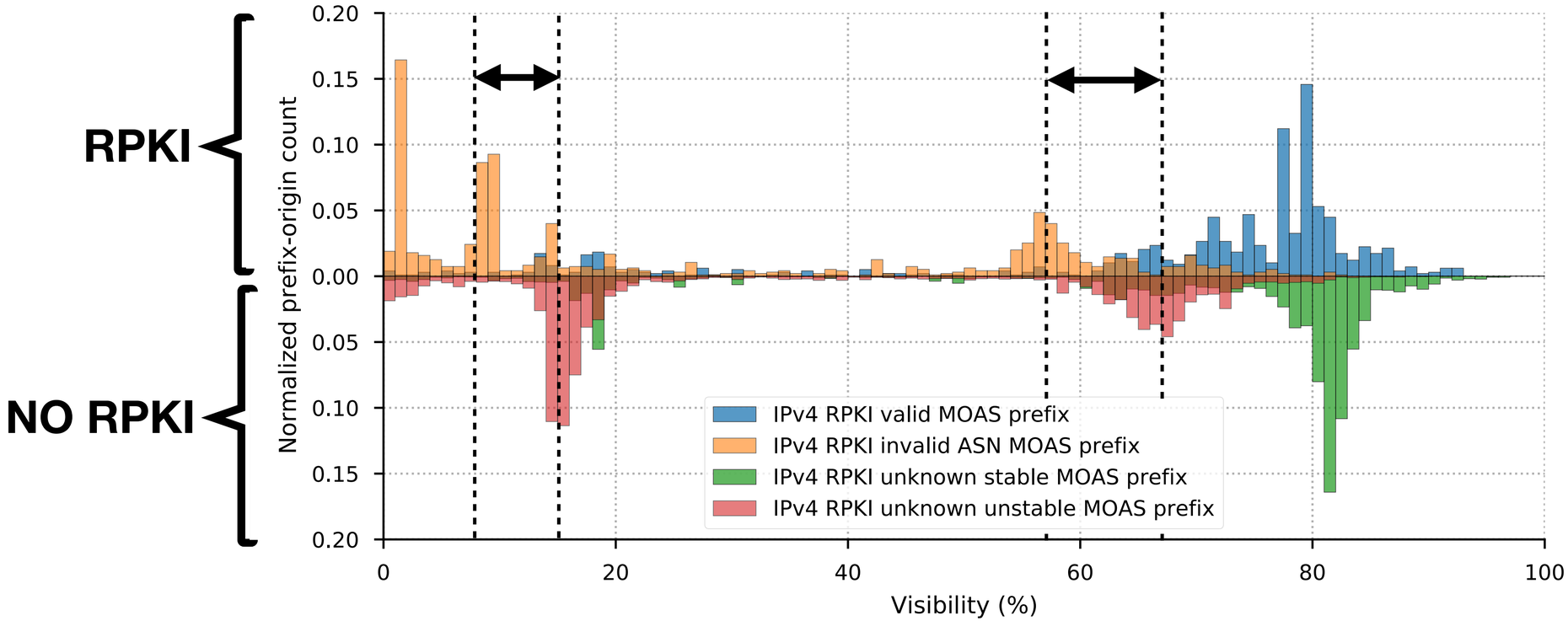
- RPKI-valid prefixes **dominate visibility** in MOAS conflicts.

Prefix-origin visibility in the case of MOAS conflicts



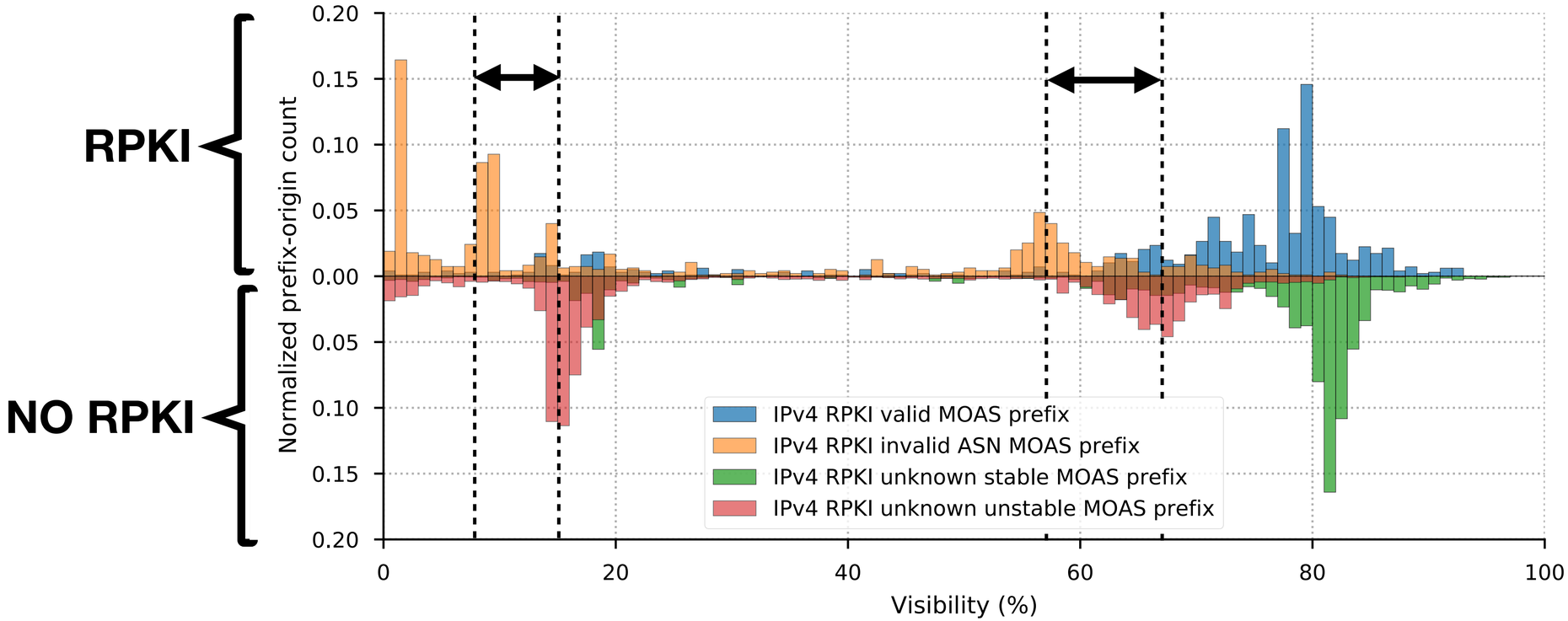
- RPKI-valid prefixes **dominate visibility** in MOAS conflicts.

Prefix-origin visibility in the case of MOAS conflicts



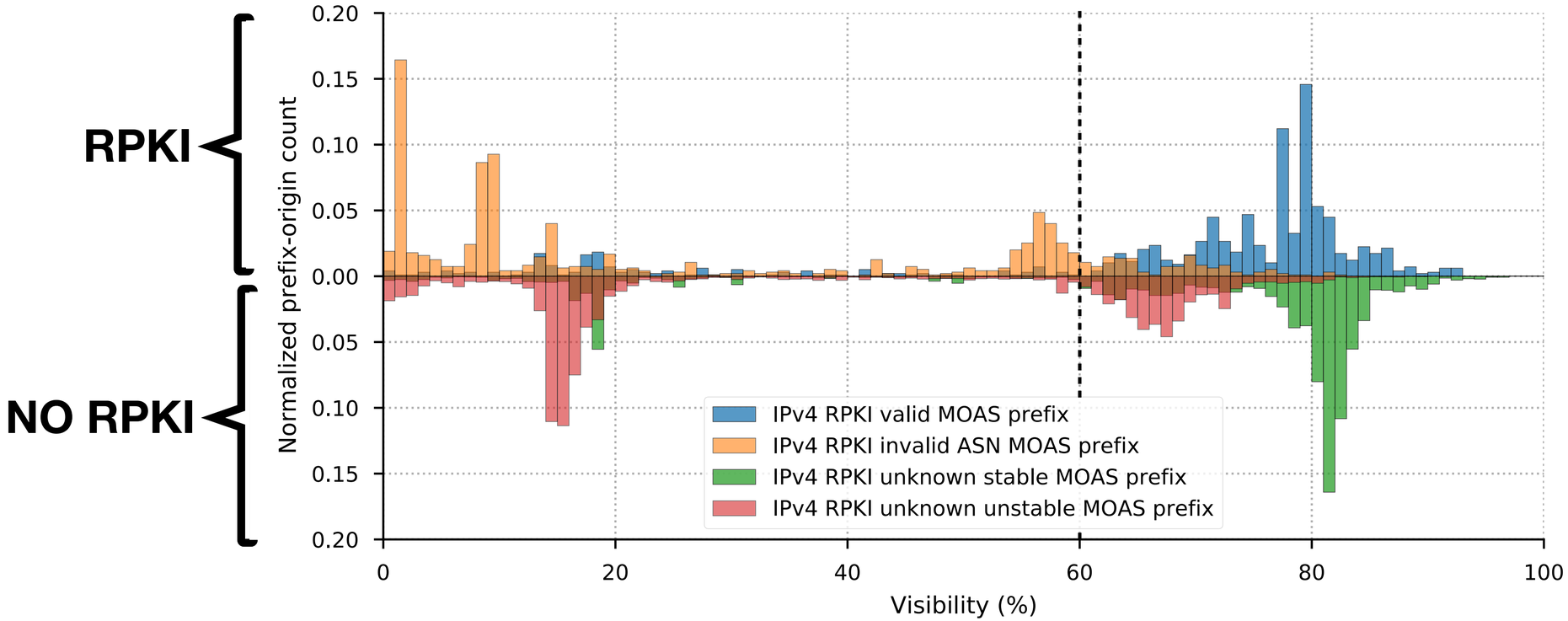
- RPKI-valid prefixes **dominate visibility** in MOAS conflicts.

Prefix-origin visibility in the case of MOAS conflicts



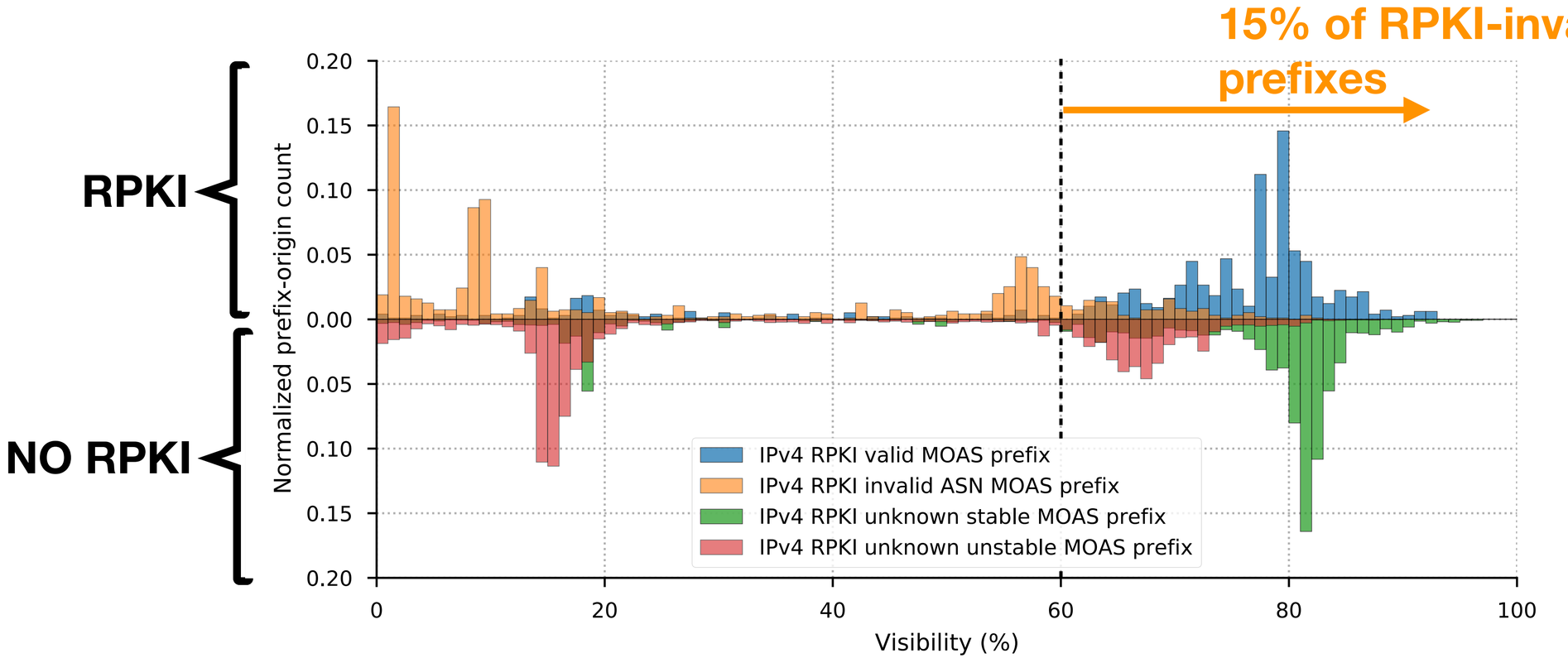
- RPKI-valid prefixes **dominate visibility** in MOAS conflicts.
- RPKI helps **protect legitimate prefix** from illicit announcements.

Prefix-origin visibility in the case of MOAS conflicts



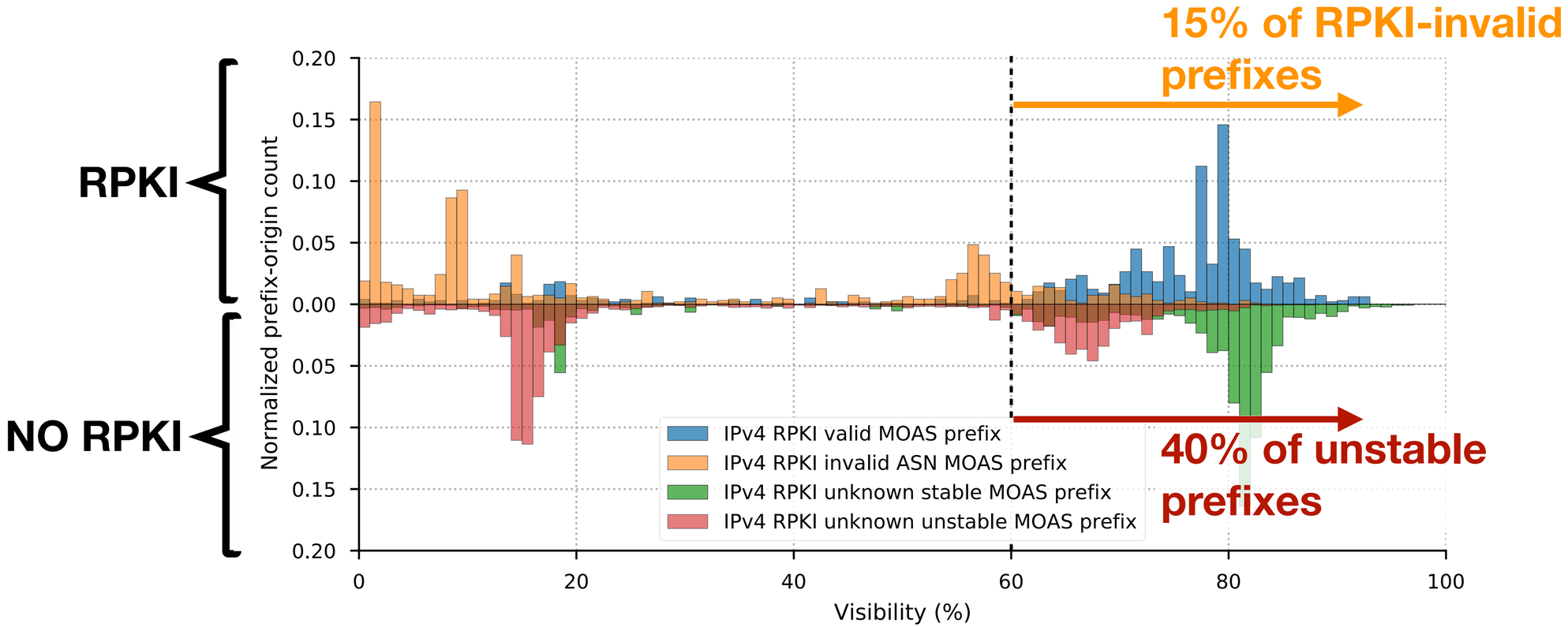
- RPKI-valid prefixes **dominate visibility** in MOAS conflicts.
- RPKI helps **protect legitimate prefix** from illicit announcements.

Prefix-origin visibility in the case of MOAS conflicts



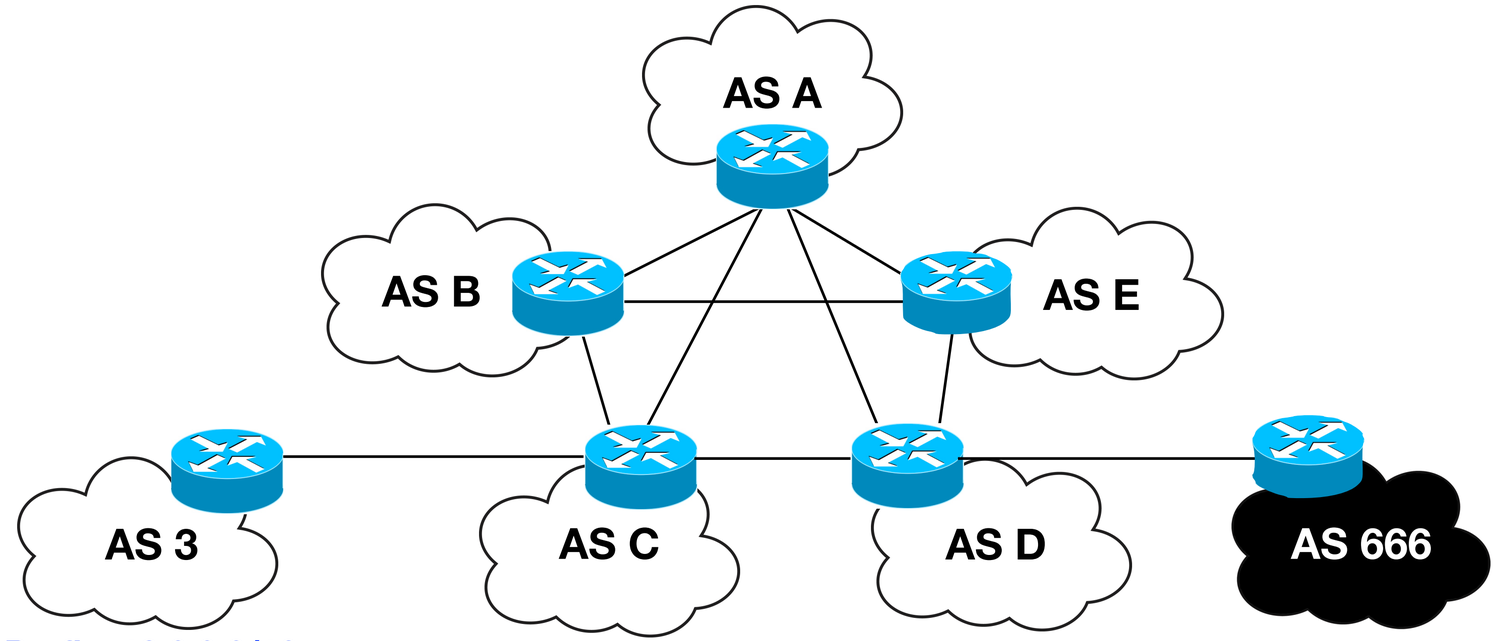
- RPKI-valid prefixes **dominate visibility** in MOAS conflicts.
- RPKI helps **protect legitimate prefix** from illicit announcements.

Prefix-origin visibility in the case of MOAS conflicts

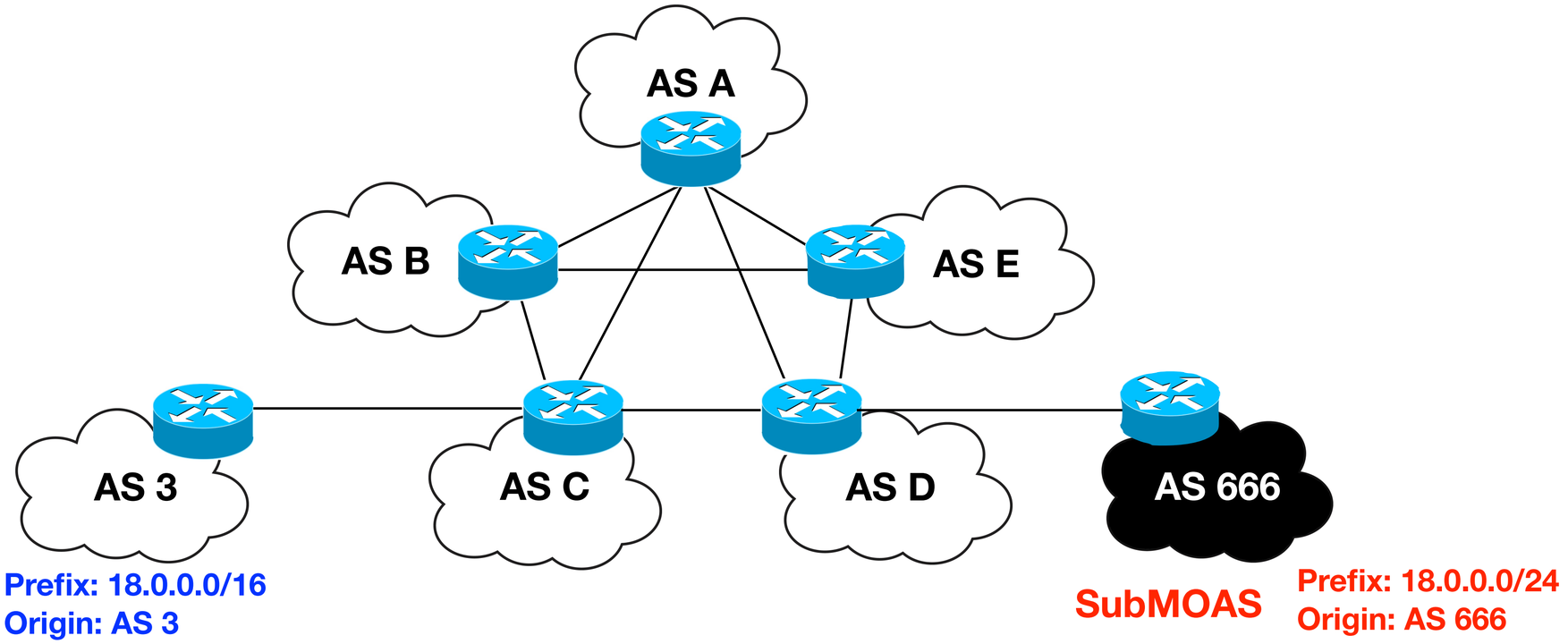


- RPKI-valid prefixes **dominate visibility** in MOAS conflicts.
- RPKI helps **protect legitimate prefix** from illicit announcements.

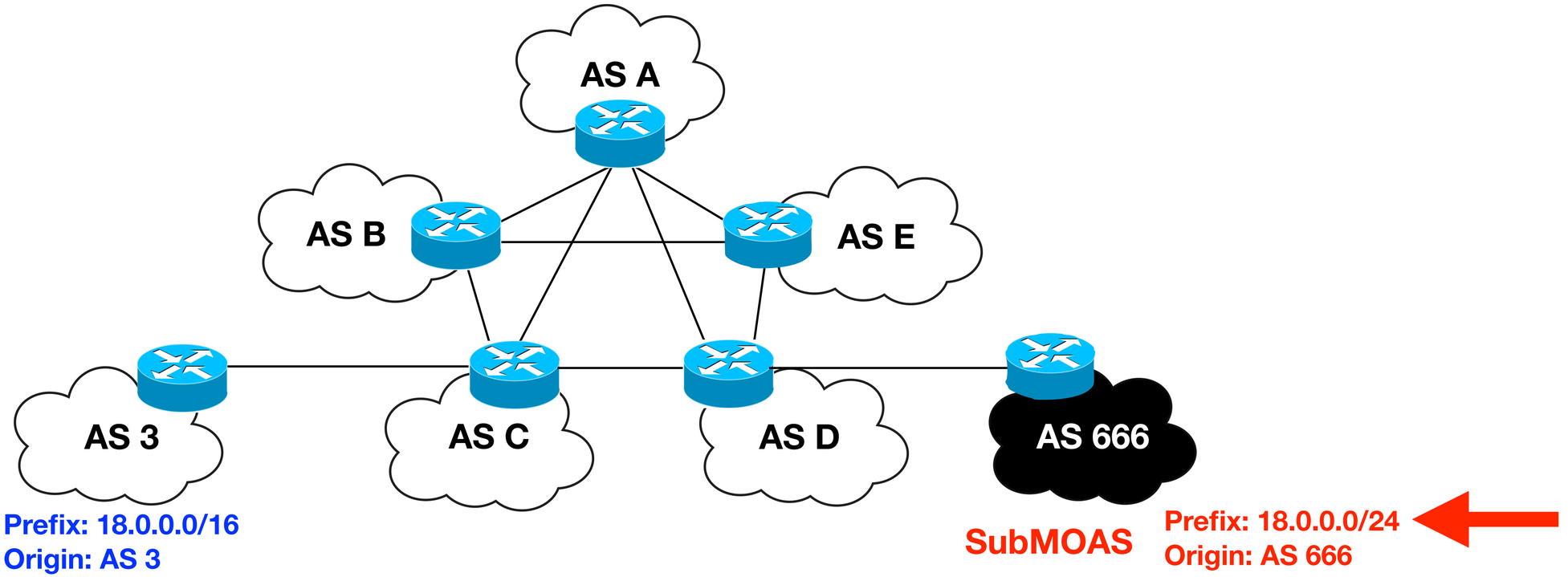
SubMOAS and subprefix conflicts



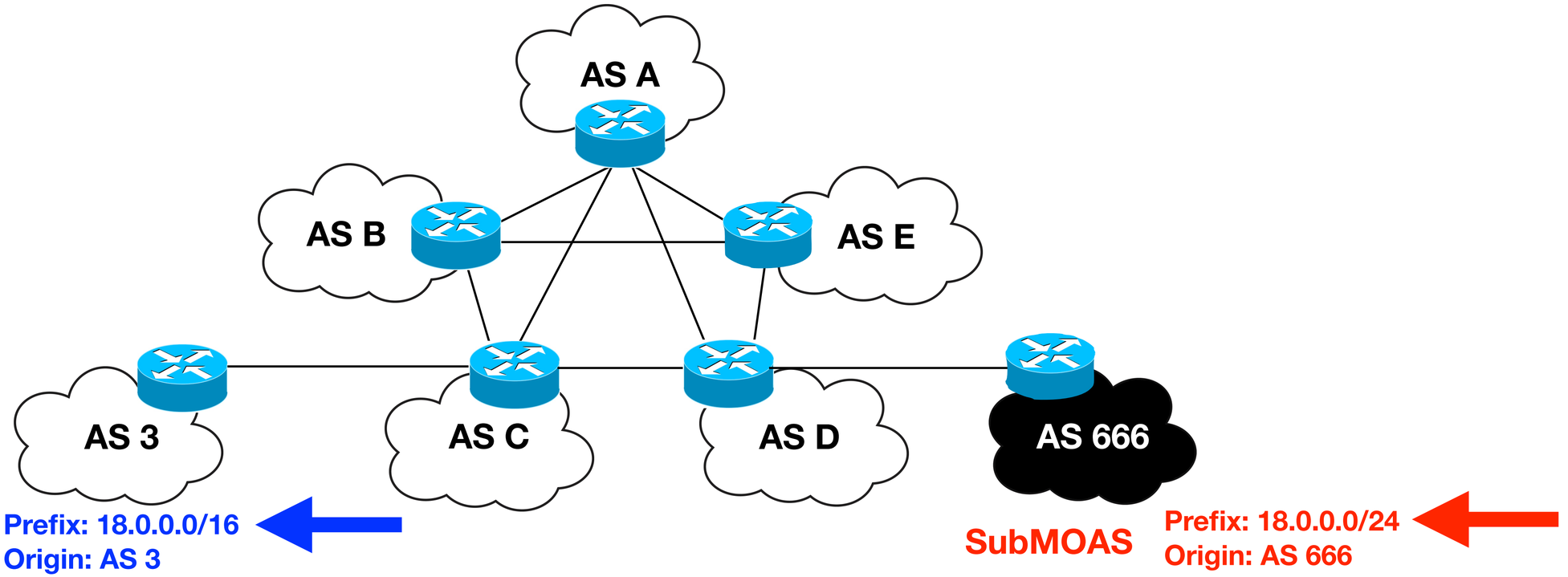
SubMOAS and subprefix conflicts



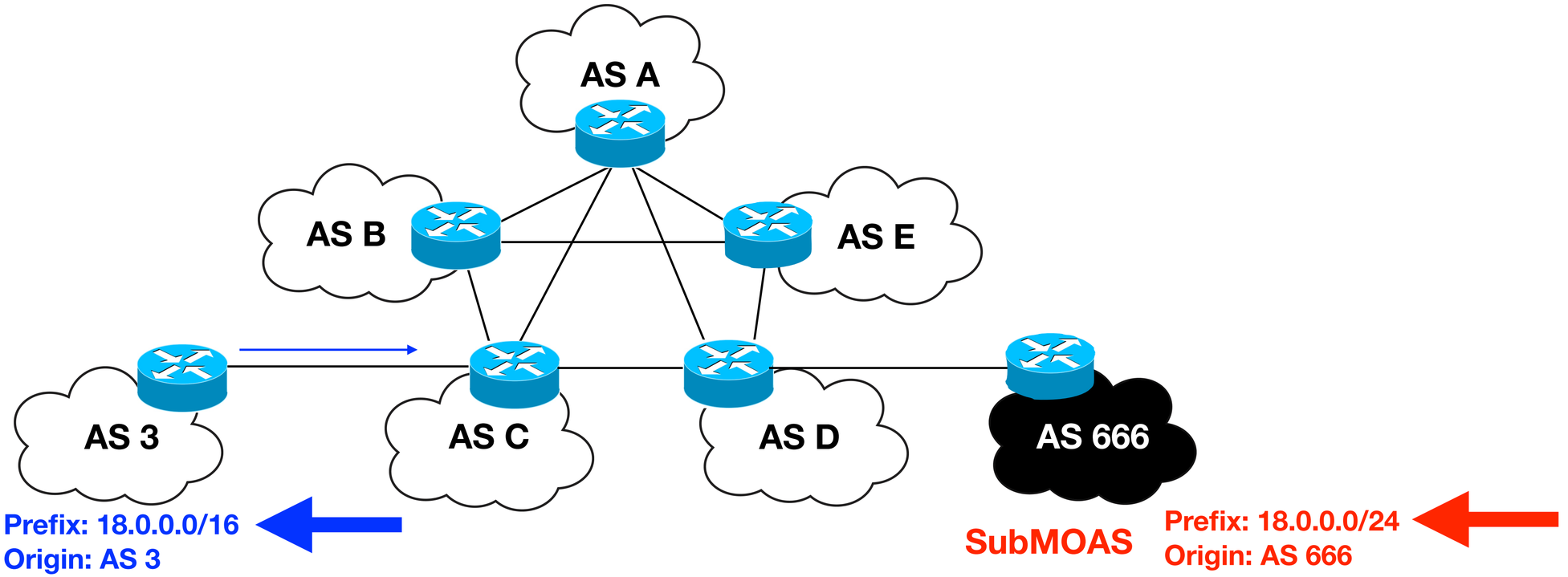
SubMOAS and subprefix conflicts



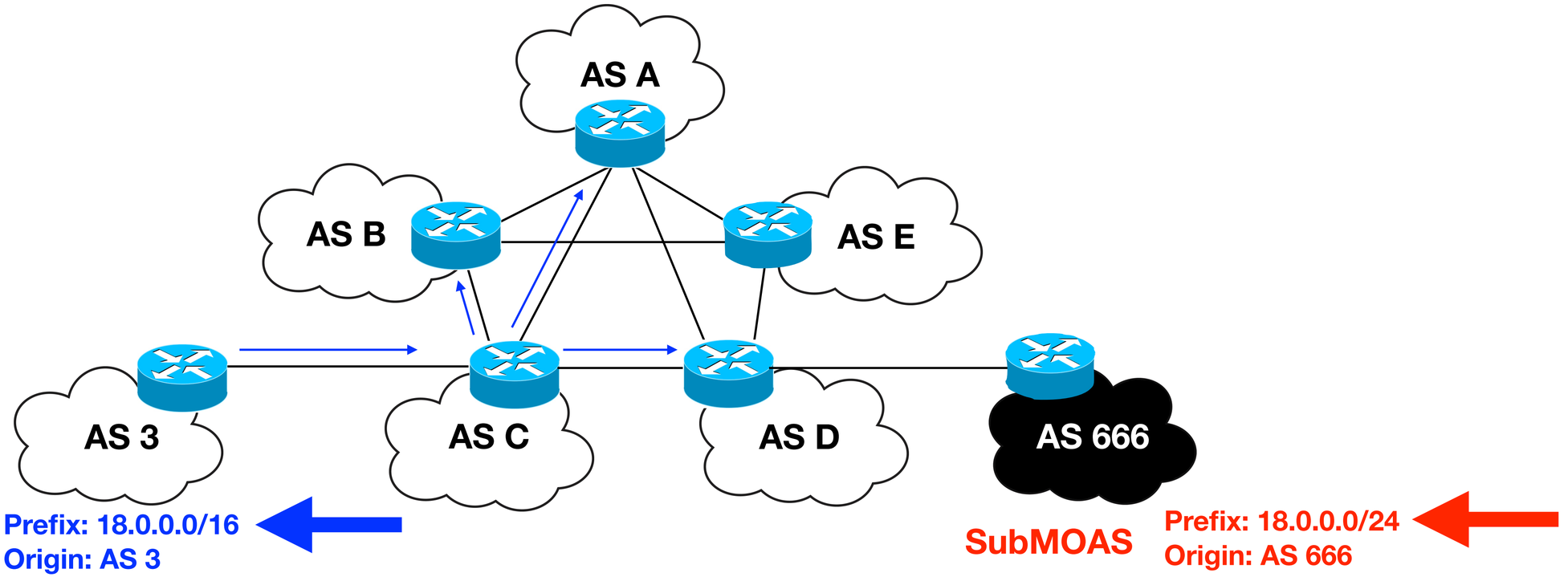
SubMOAS and subprefix conflicts



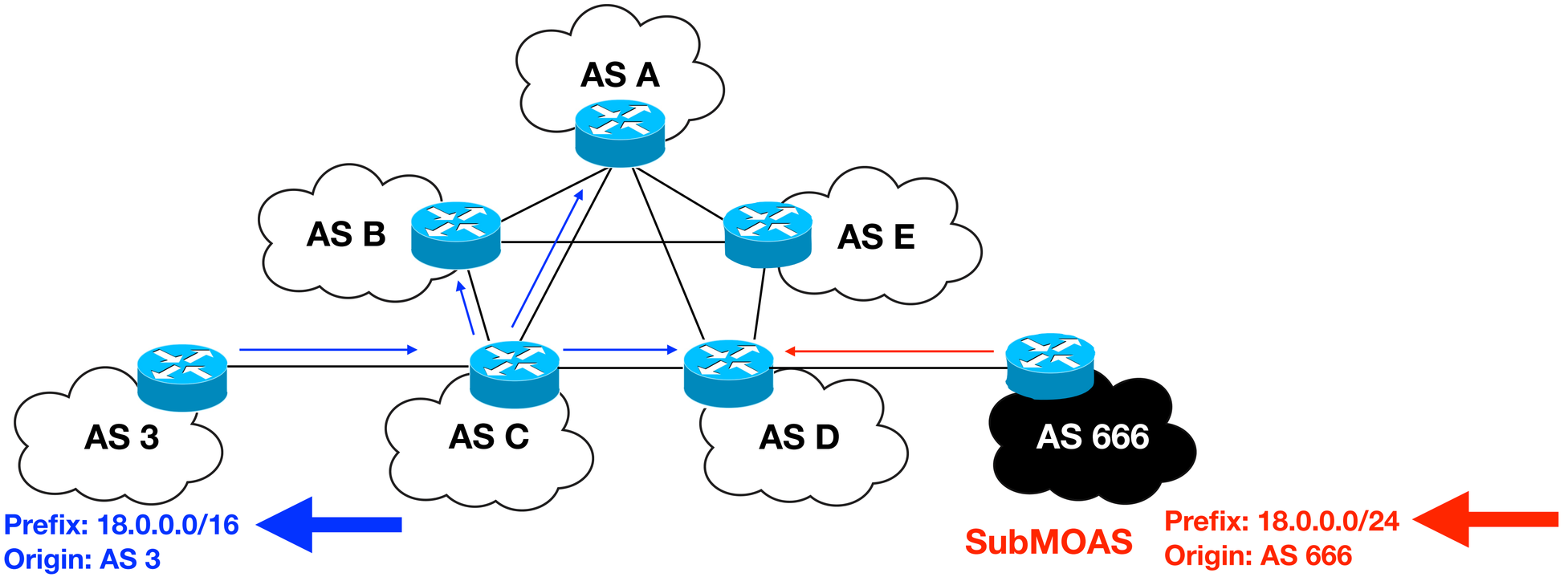
SubMOAS and subprefix conflicts



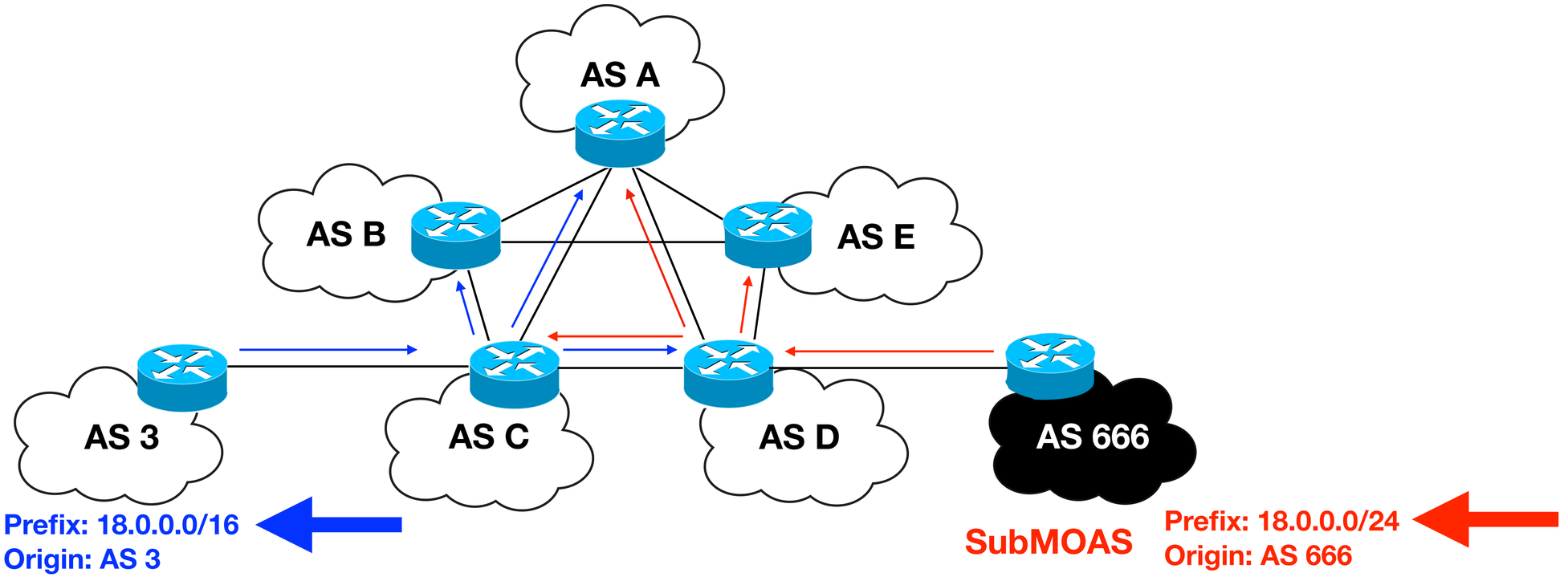
SubMOAS and subprefix conflicts



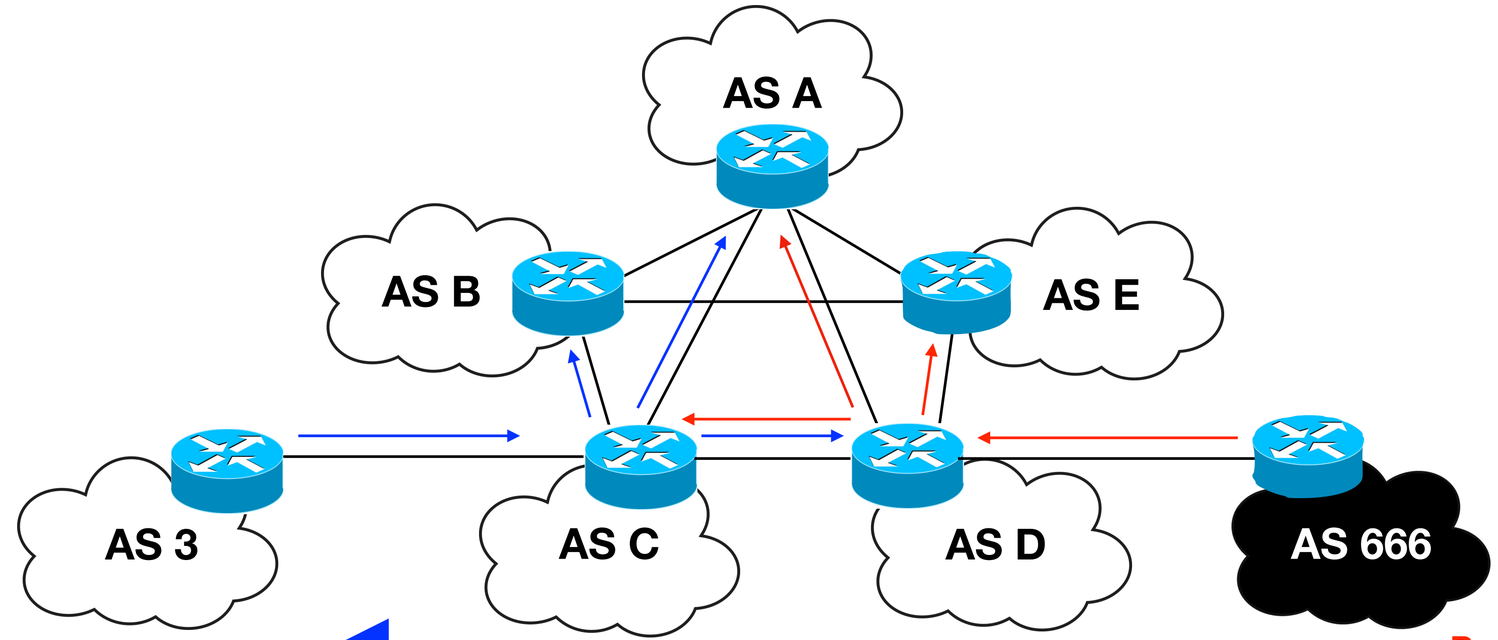
SubMOAS and subprefix conflicts



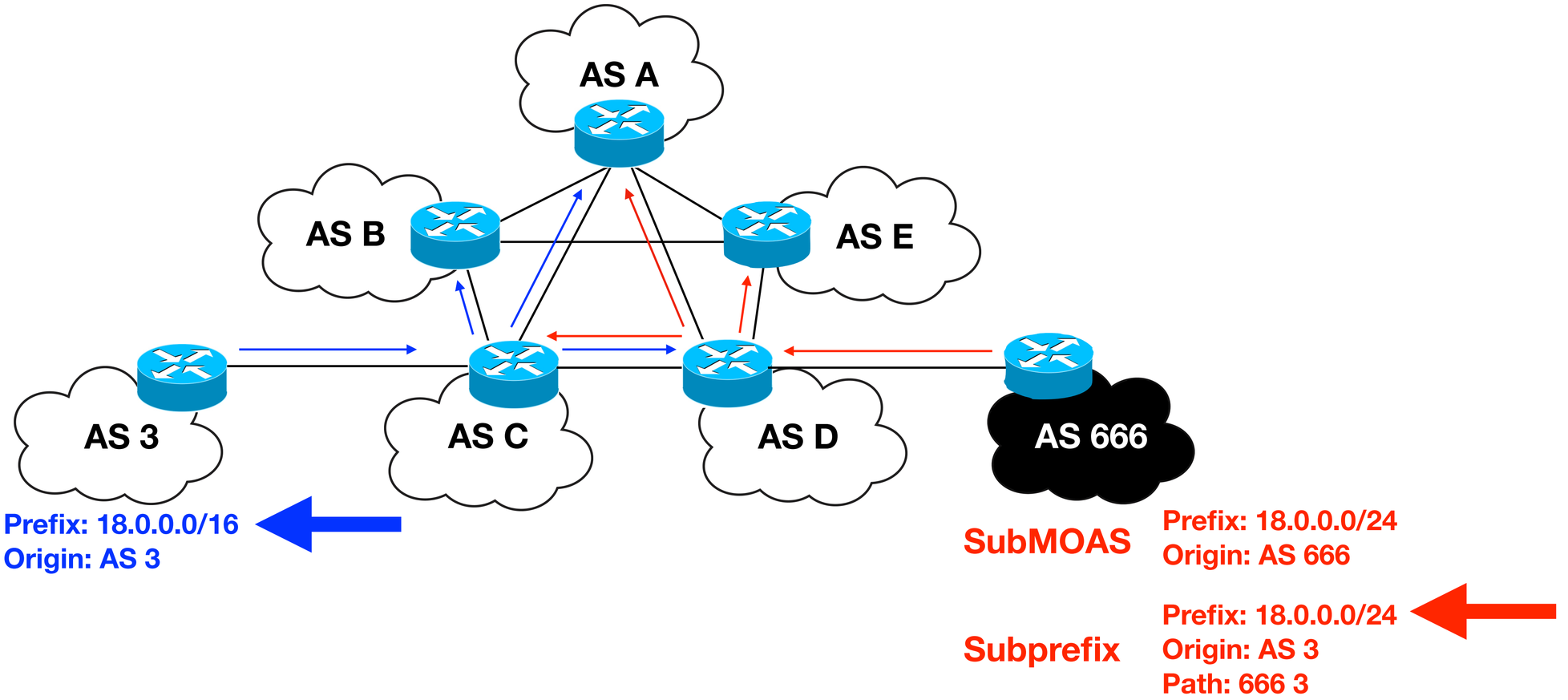
SubMOAS and subprefix conflicts



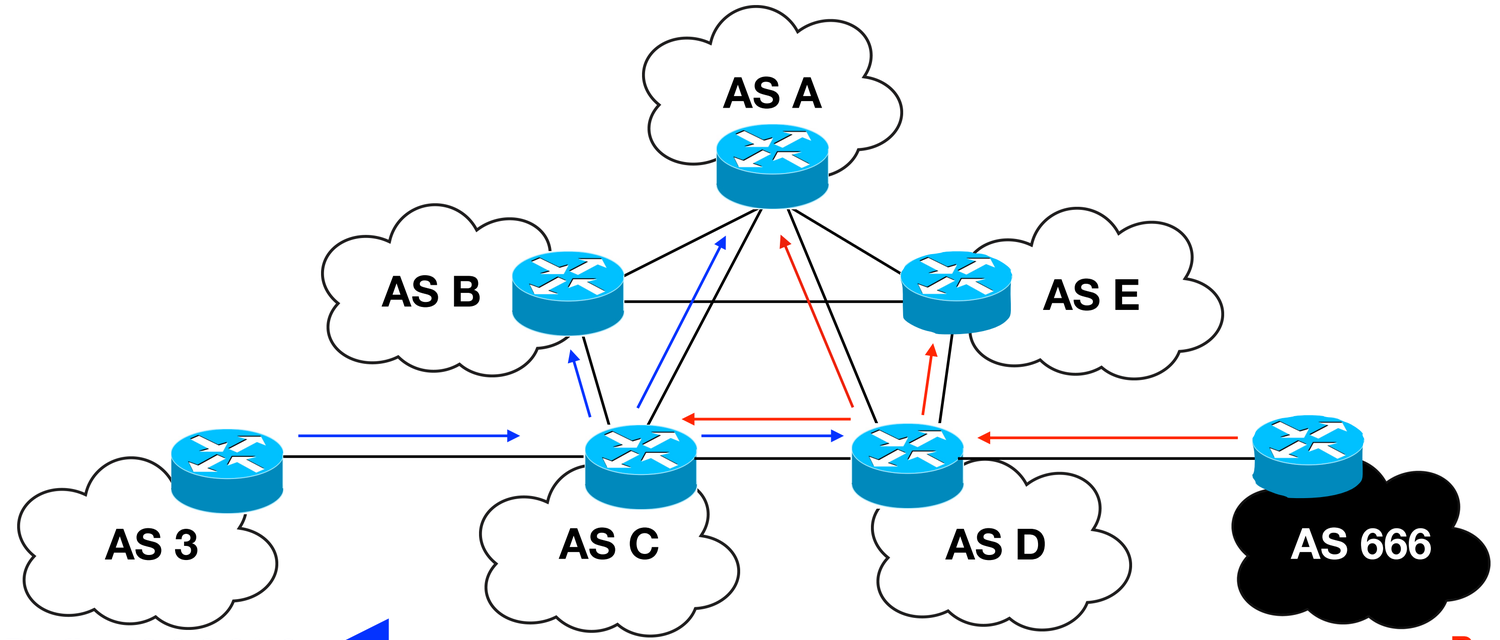
SubMOAS and subprefix conflicts



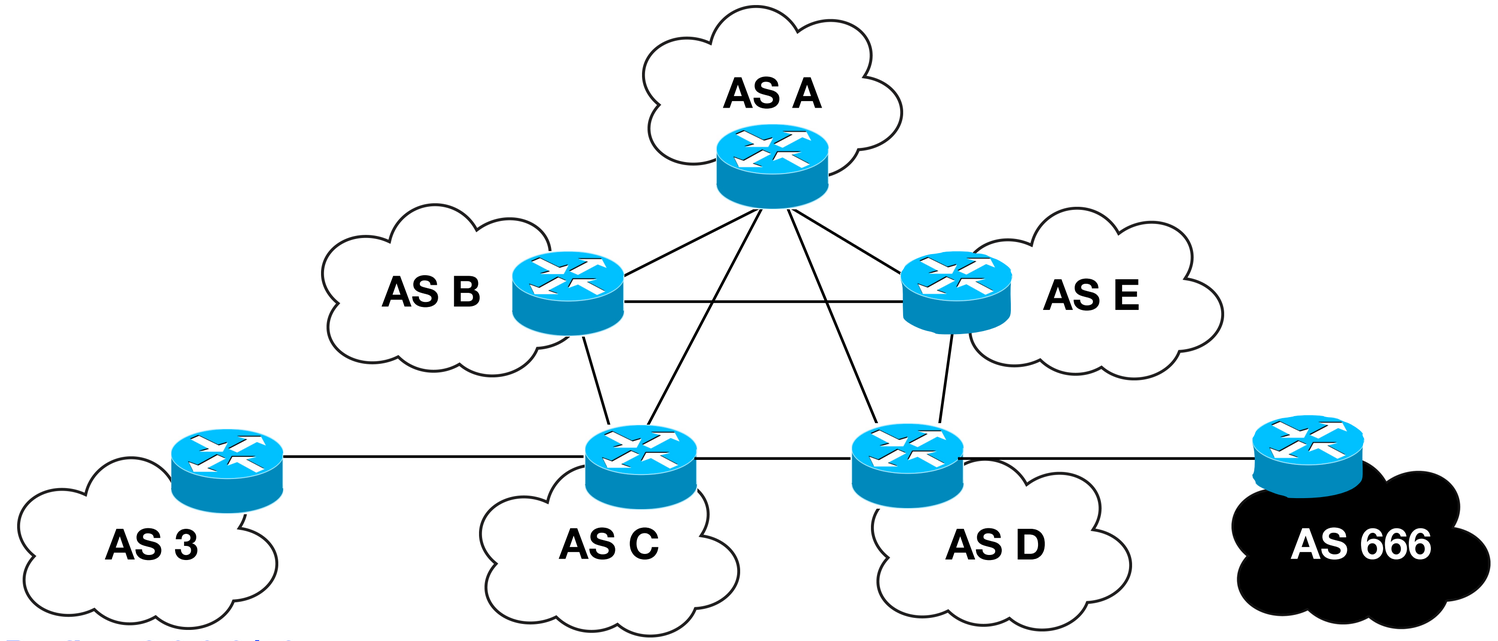
SubMOAS and subprefix conflicts



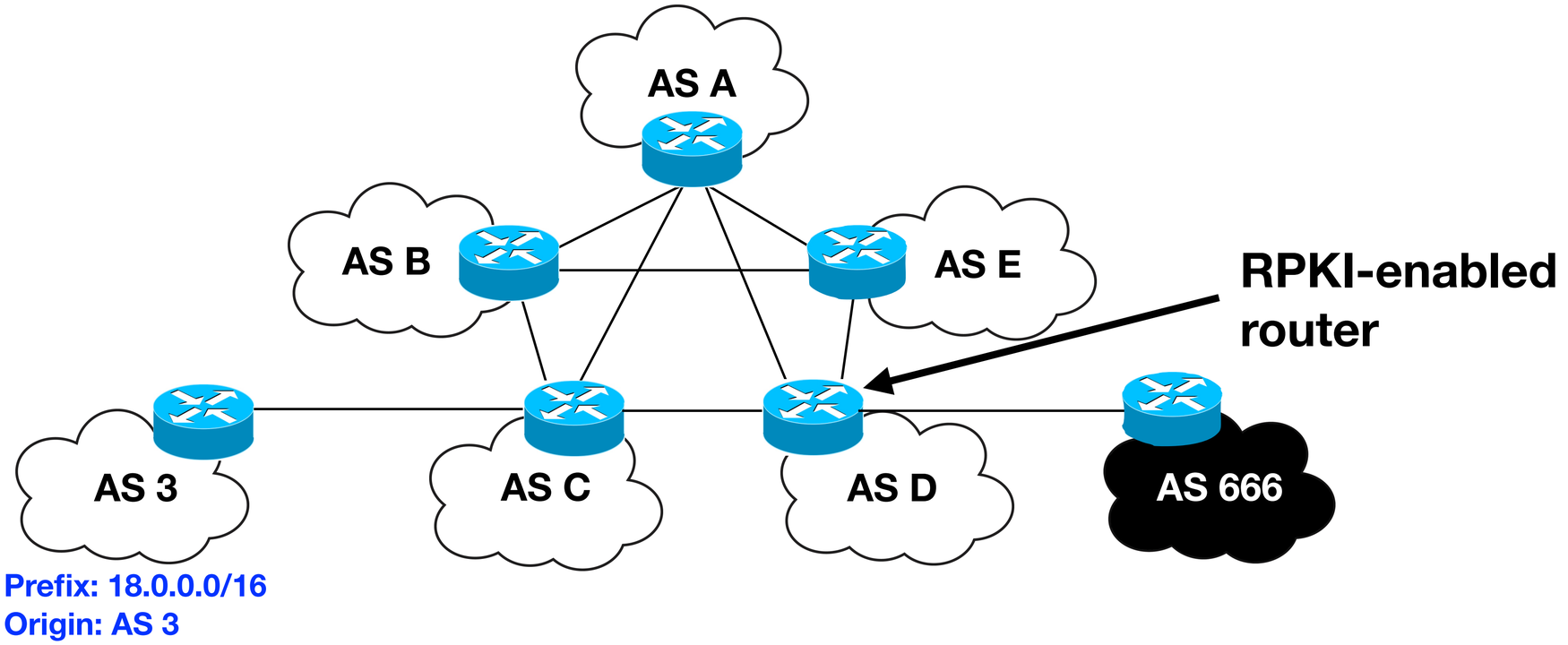
SubMOAS and subprefix conflicts



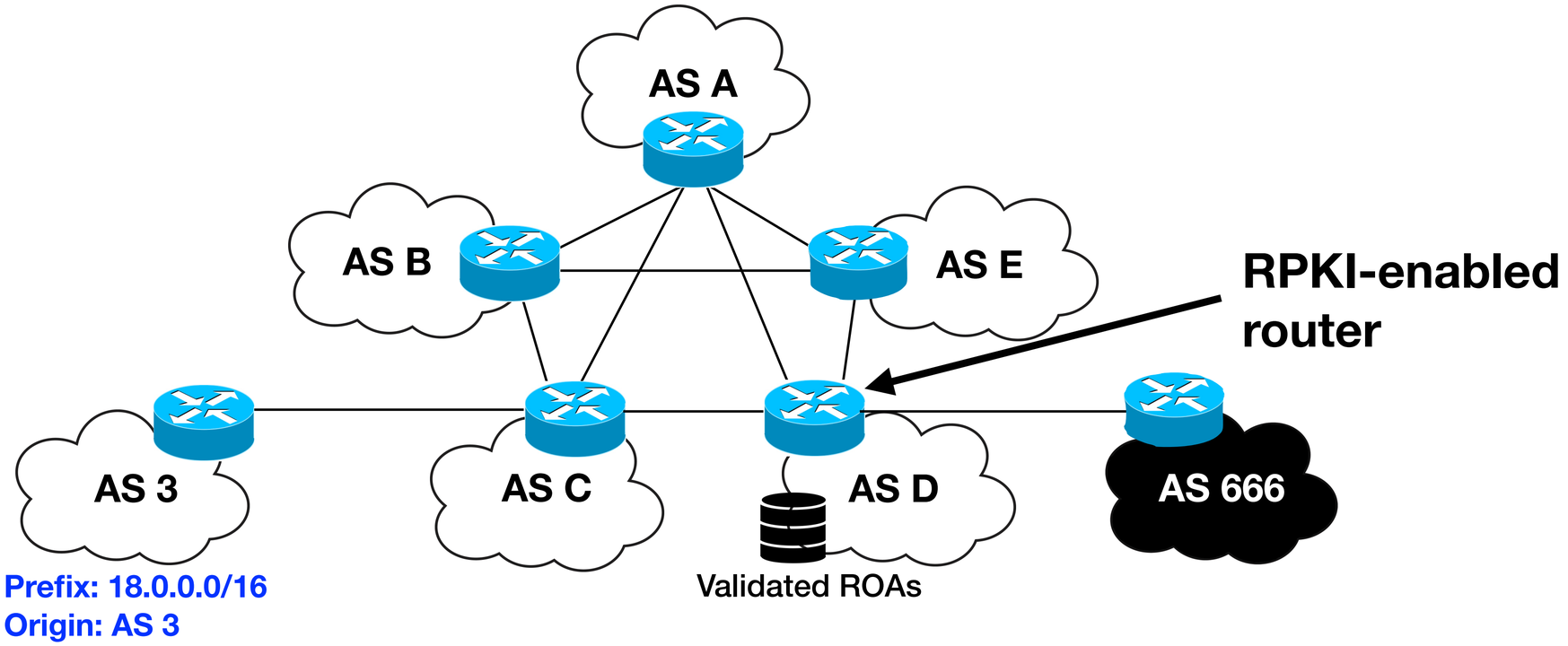
SubMOAS and subprefix conflicts with RPKI



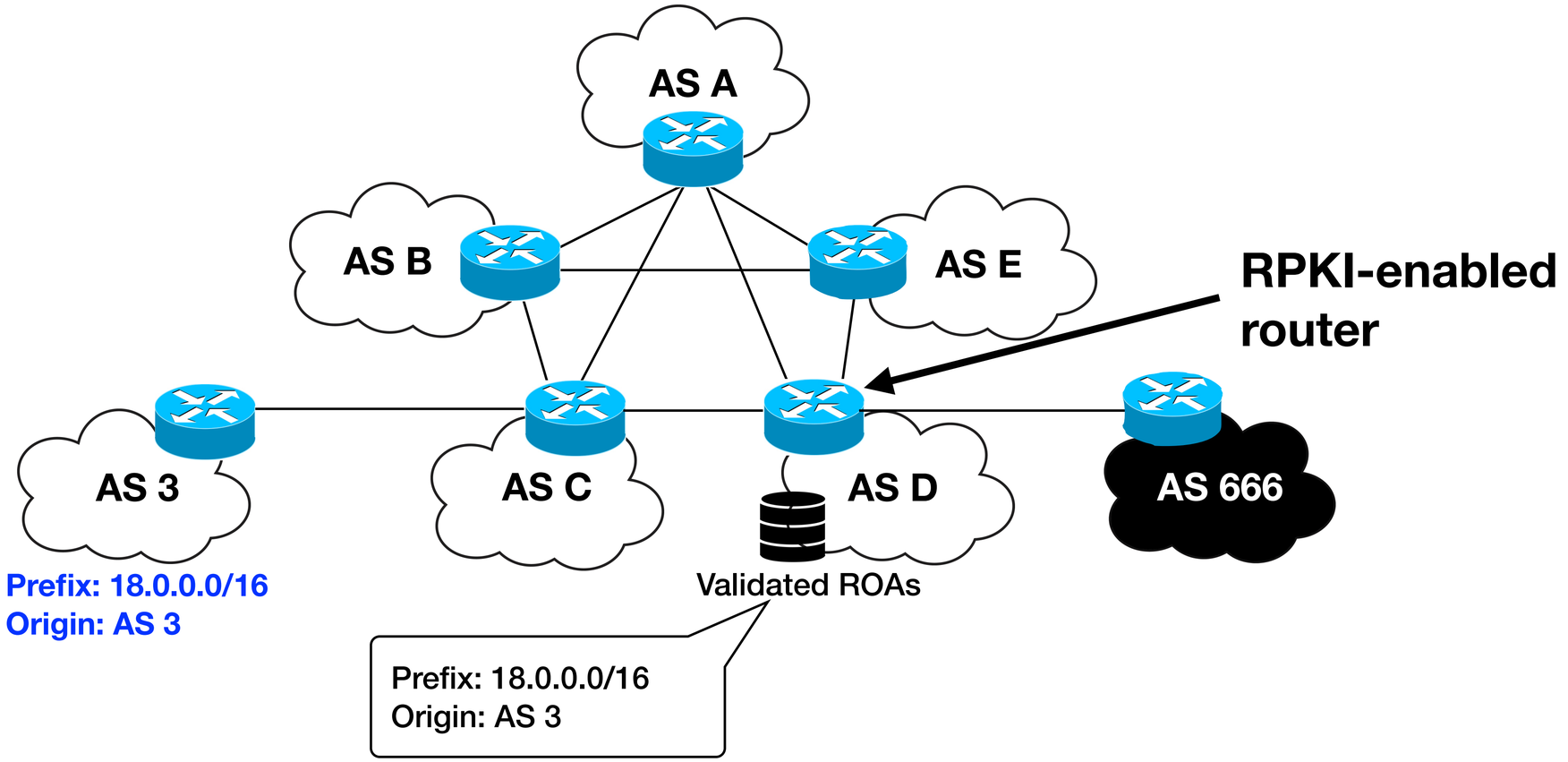
SubMOAS and subprefix conflicts with RPKI



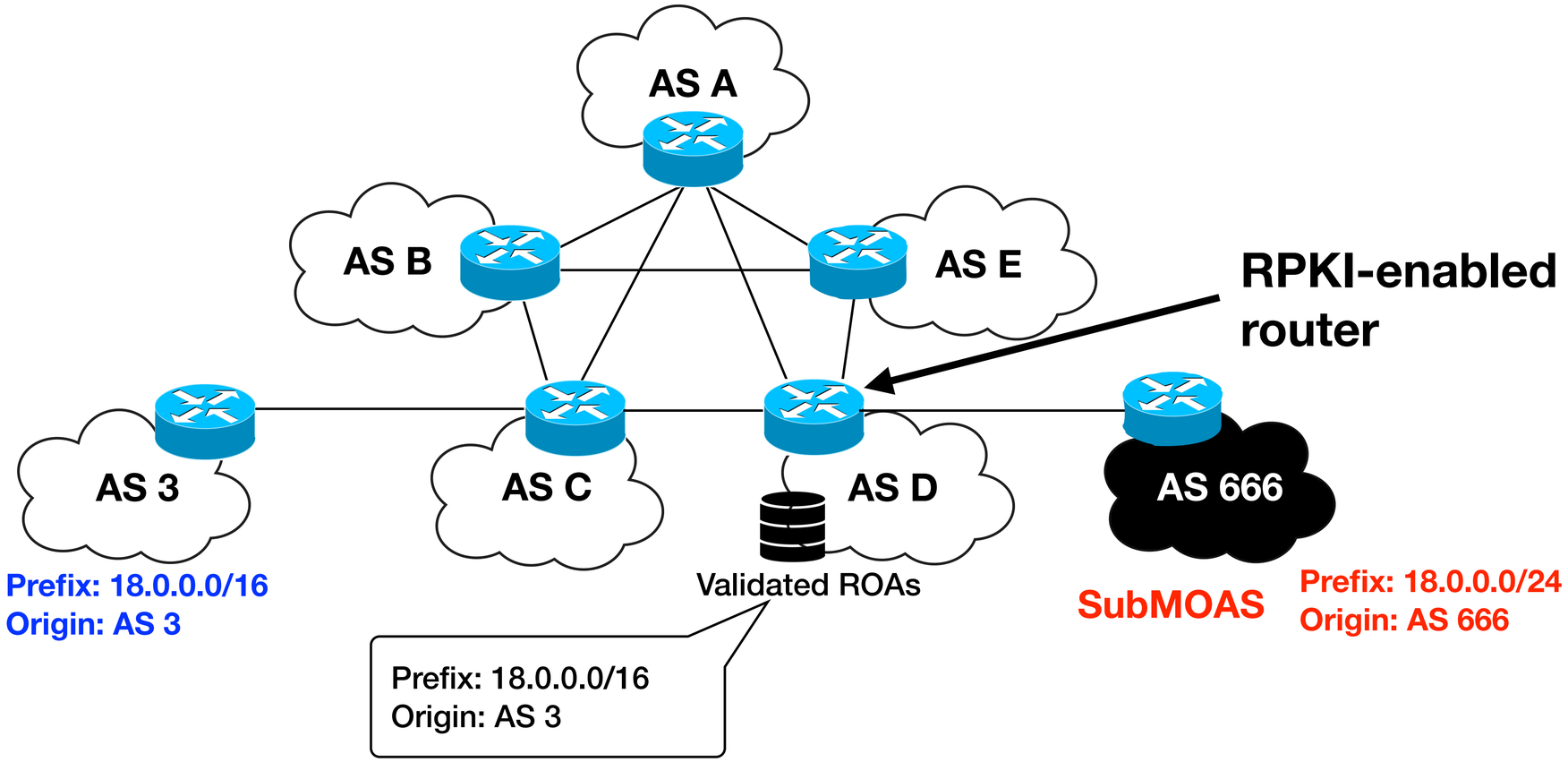
SubMOAS and subprefix conflicts with RPKI



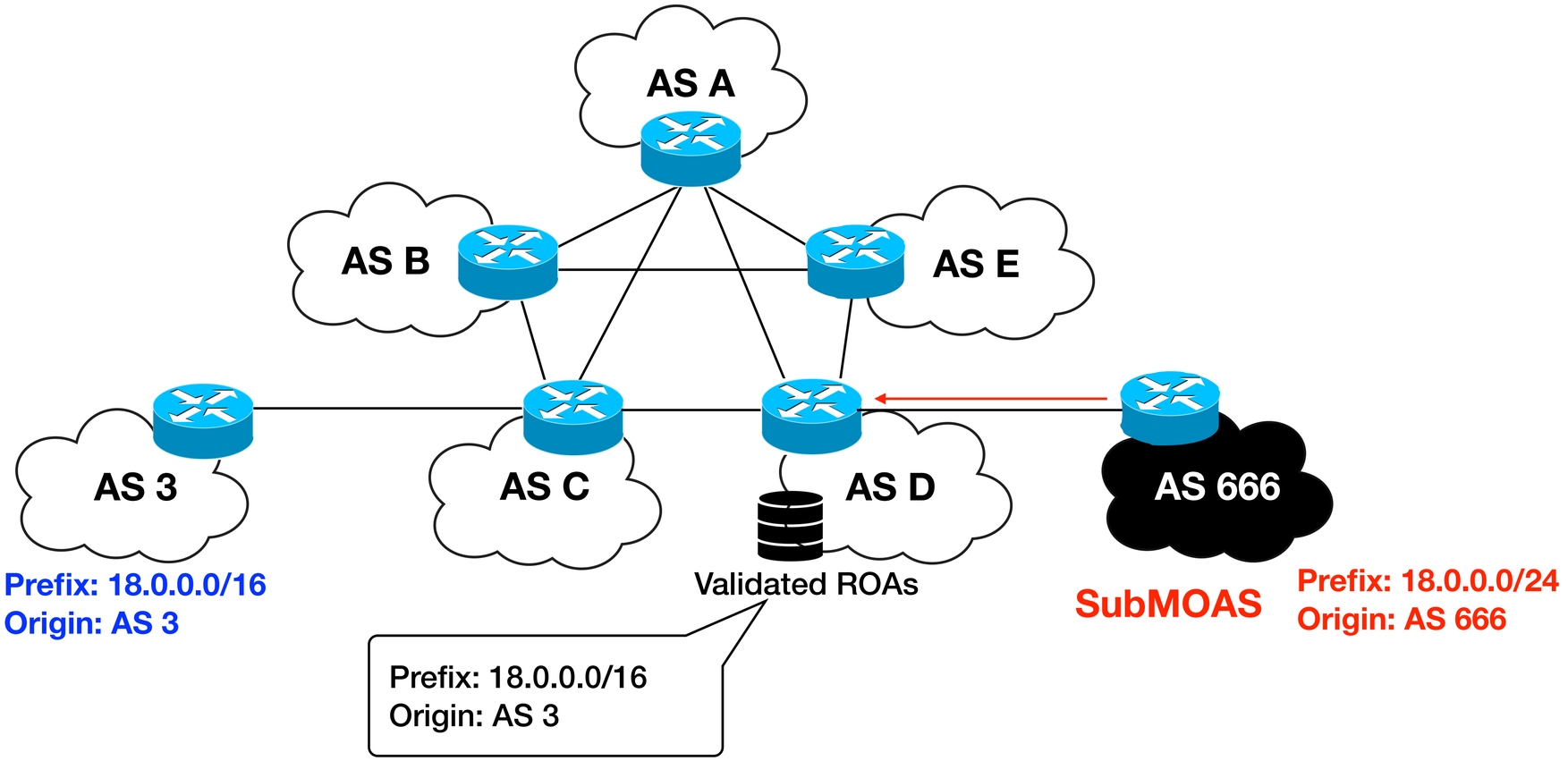
SubMOAS and subprefix conflicts with RPKI



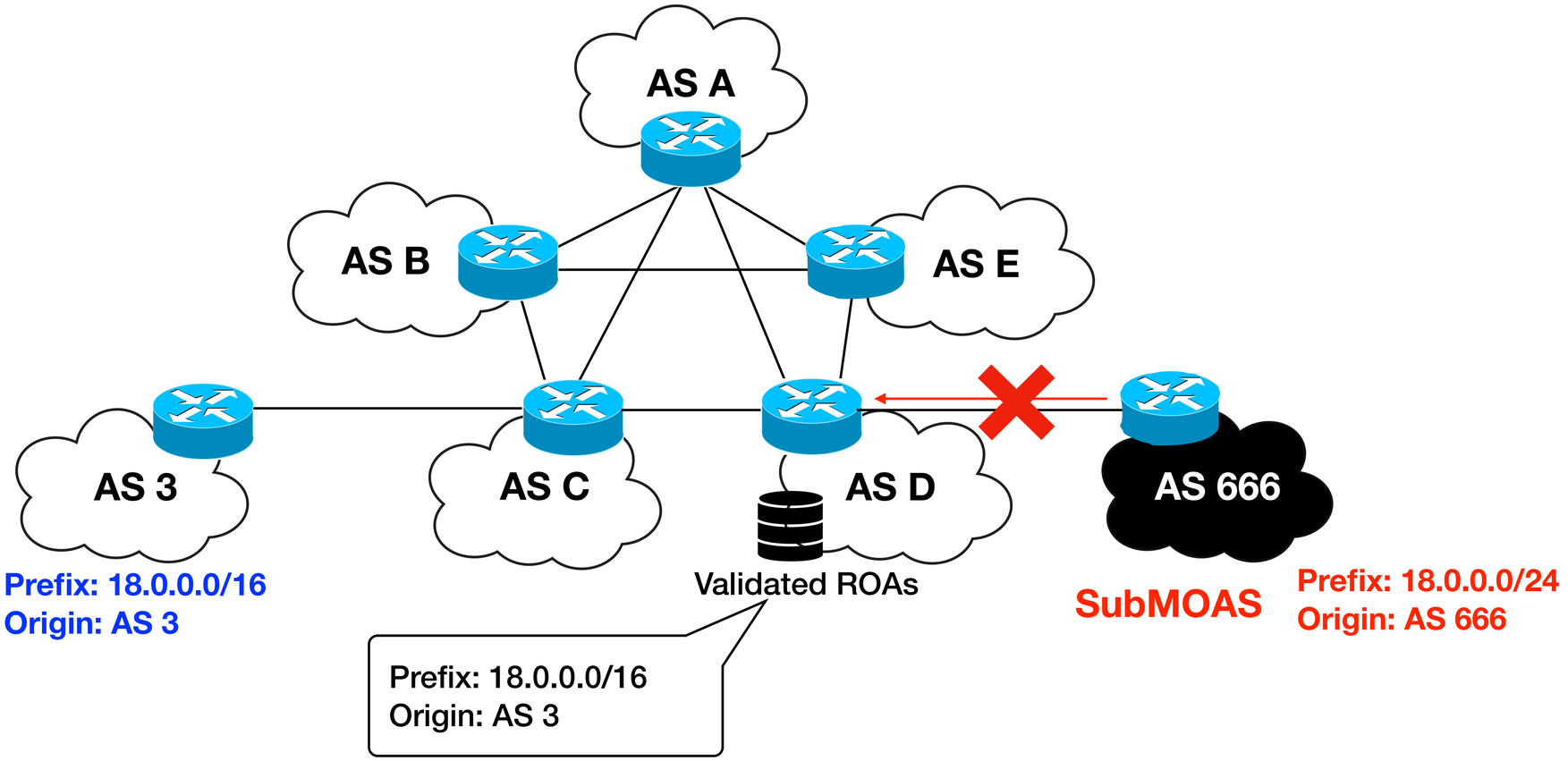
SubMOAS and subprefix conflicts with RPKI



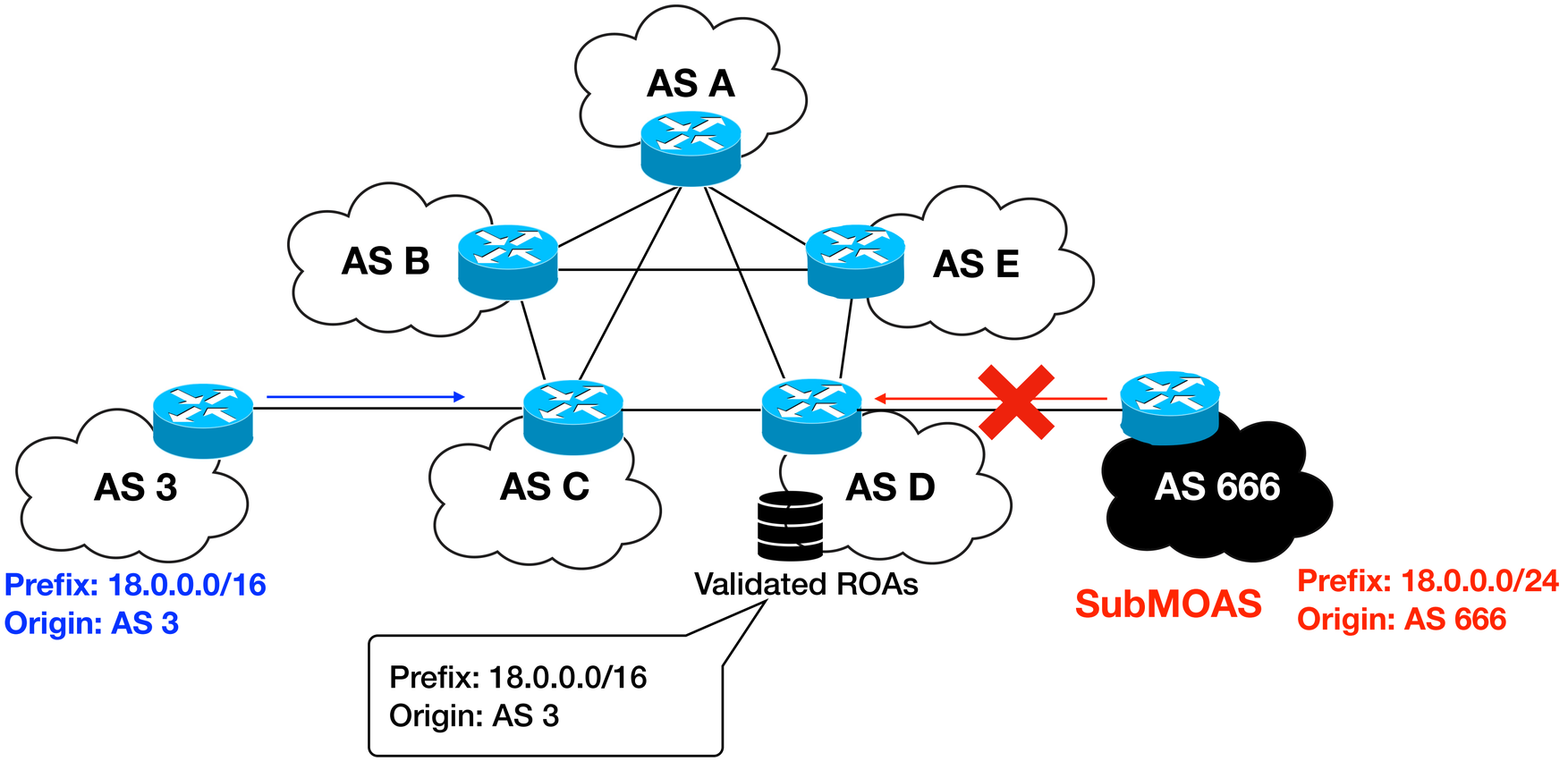
SubMOAS and subprefix conflicts with RPKI



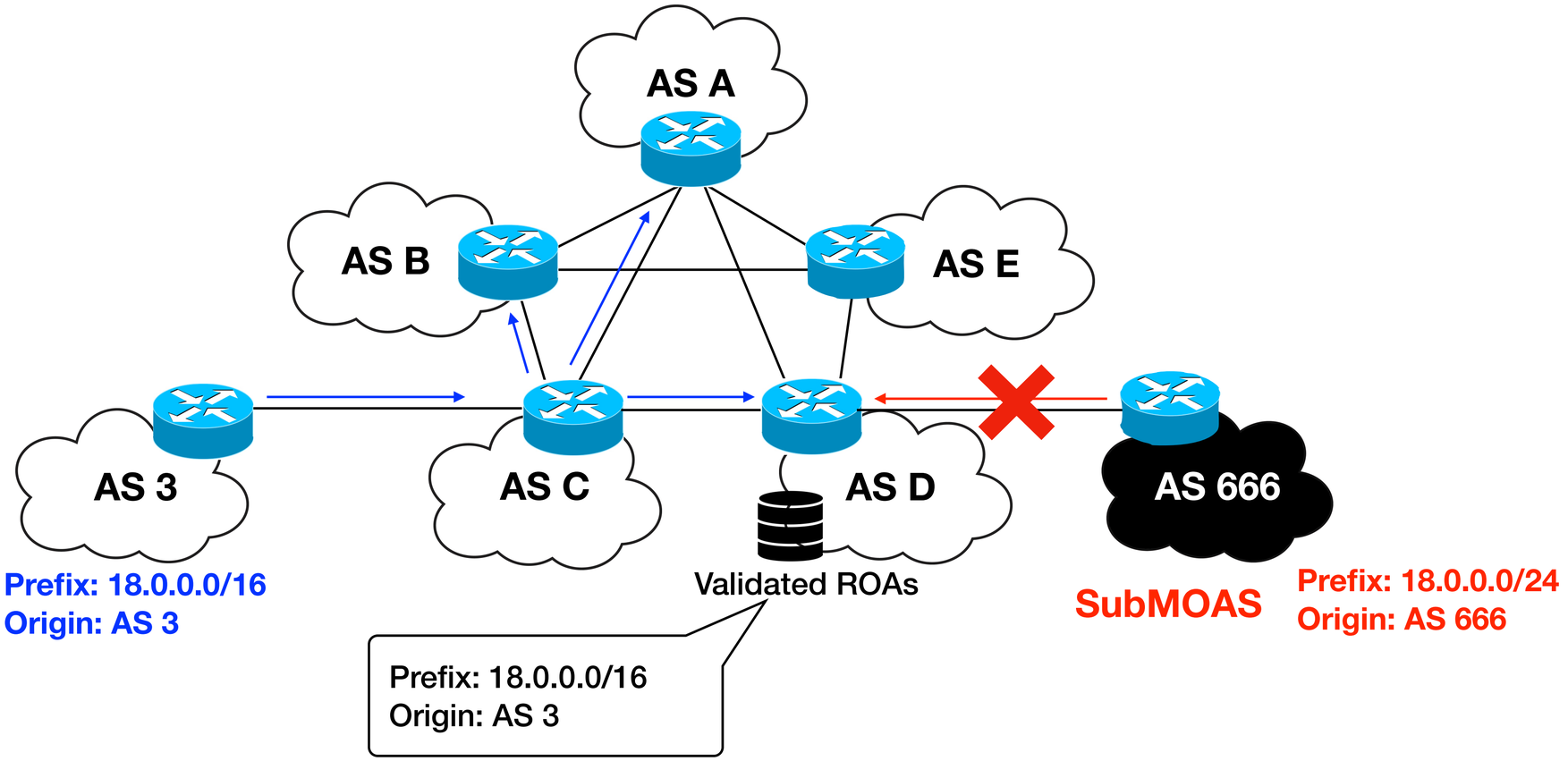
SubMOAS and subprefix conflicts with RPKI



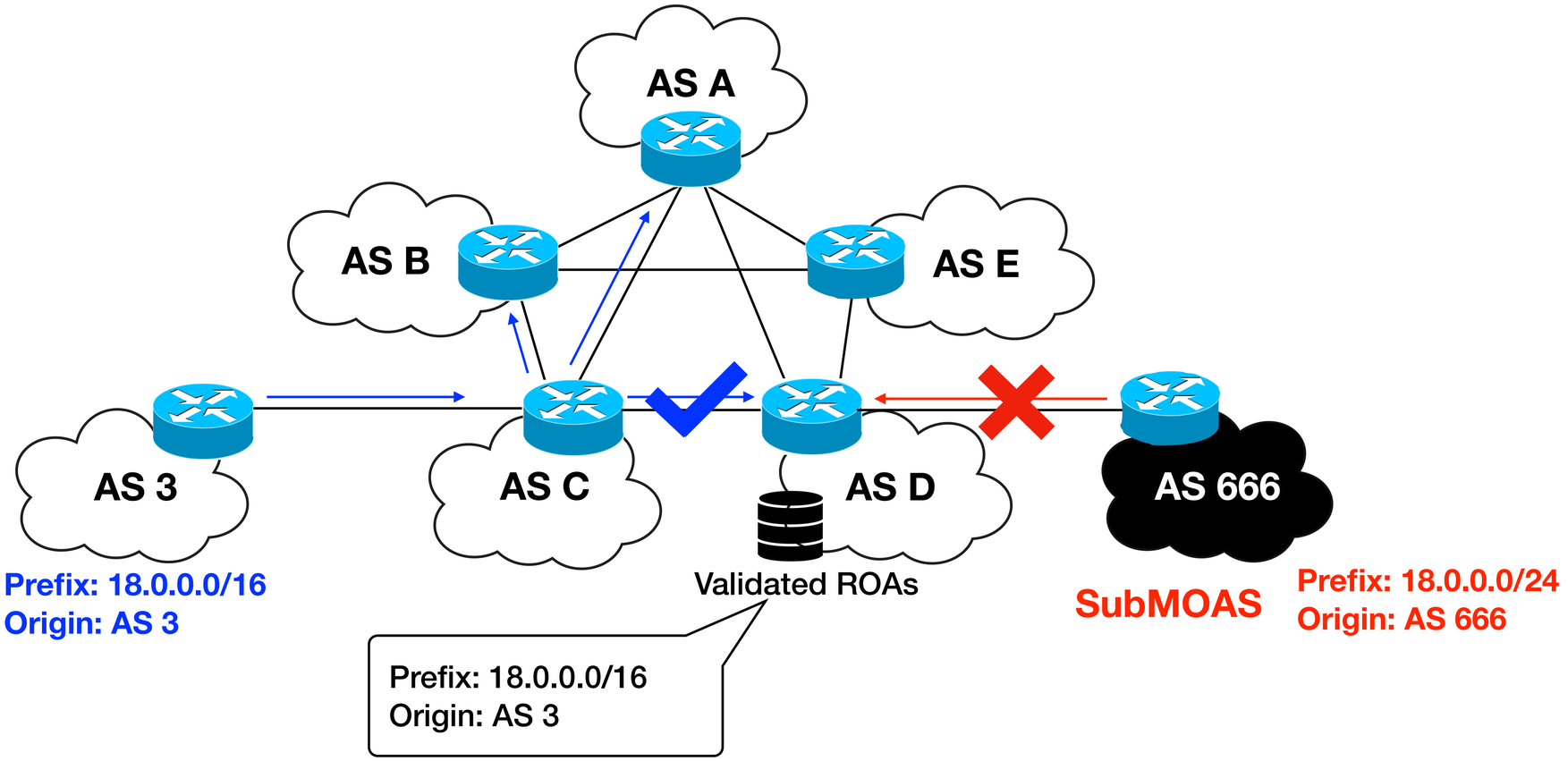
SubMOAS and subprefix conflicts with RPKI



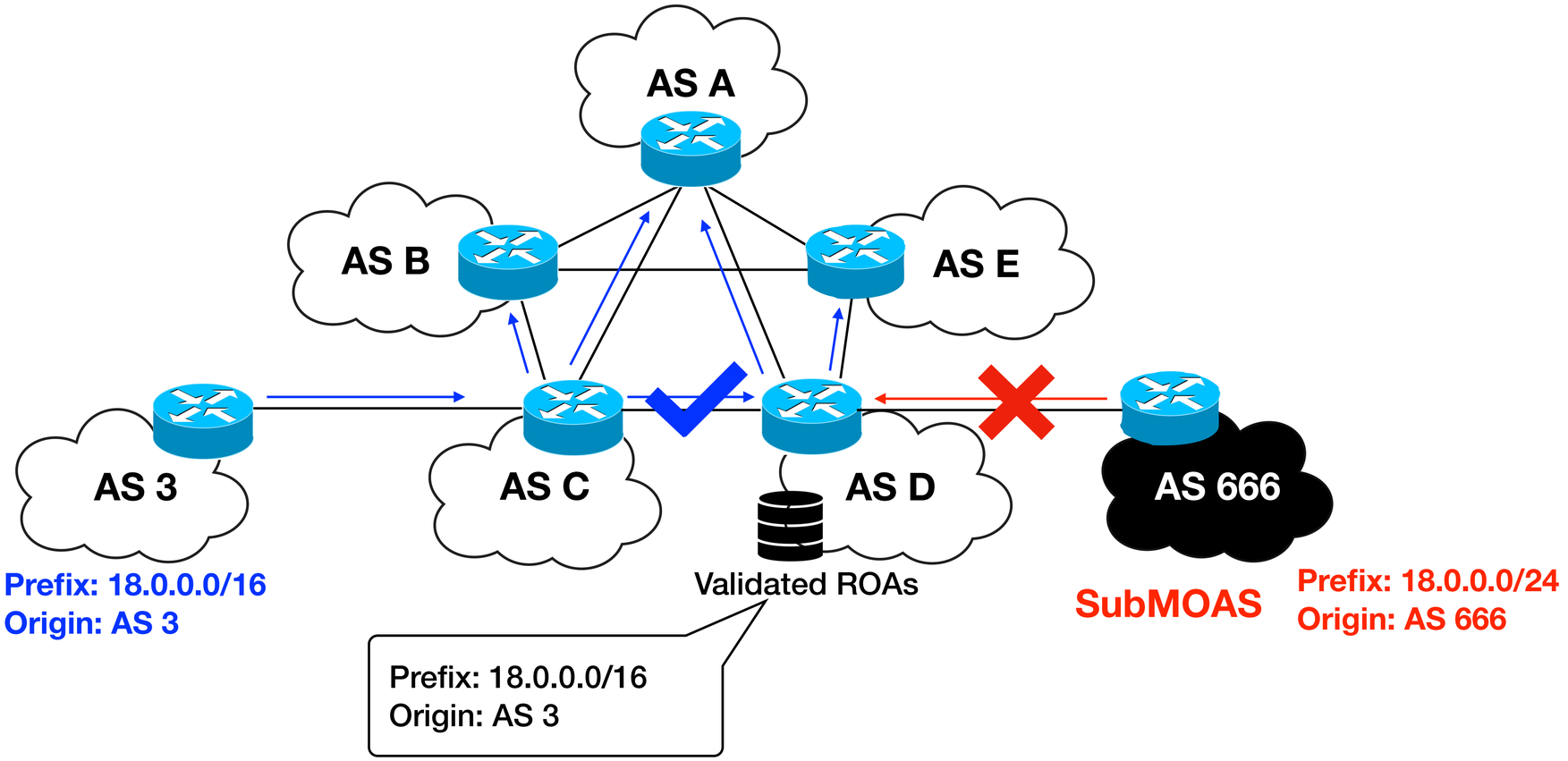
SubMOAS and subprefix conflicts with RPKI



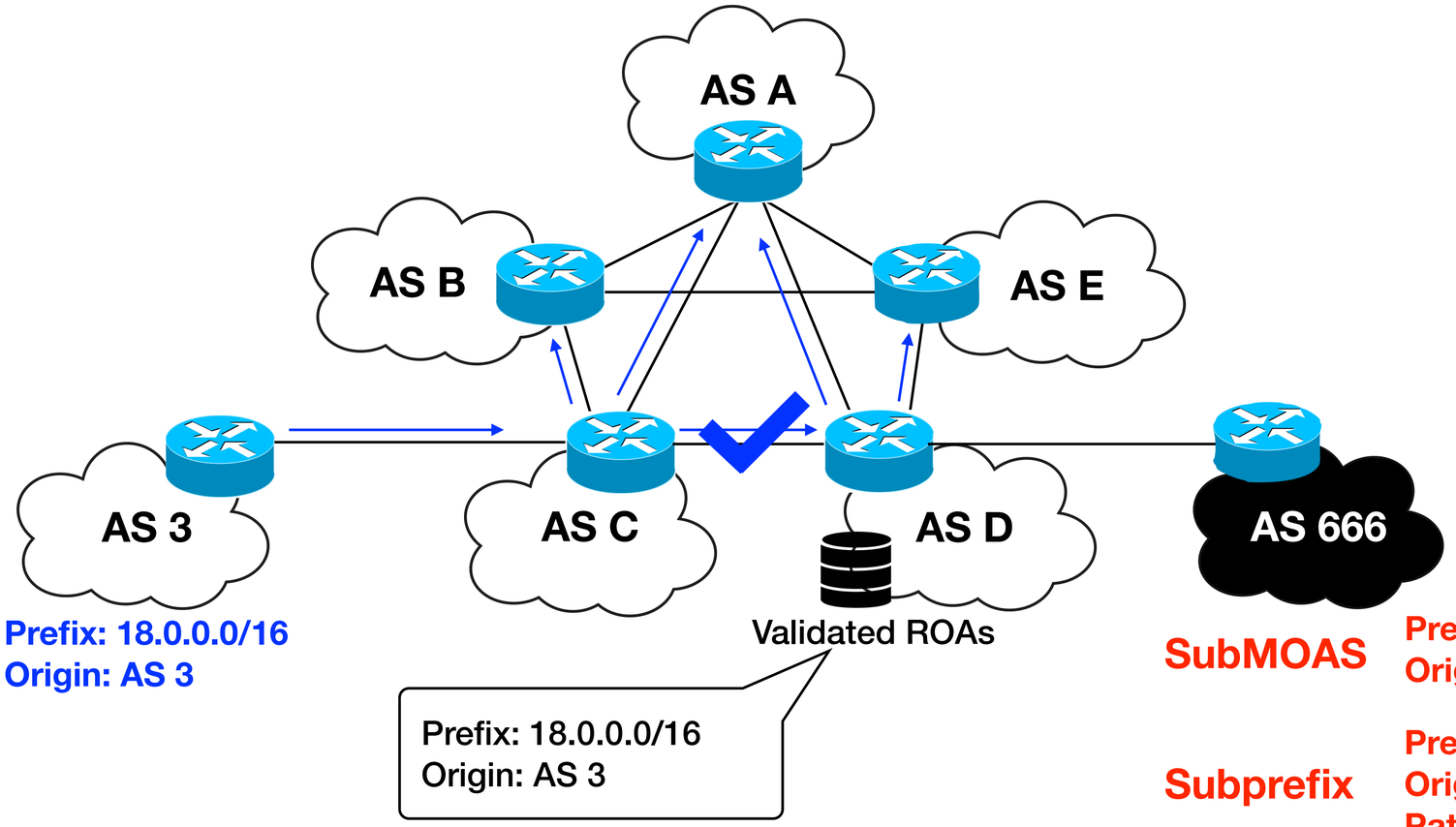
SubMOAS and subprefix conflicts with RPKI



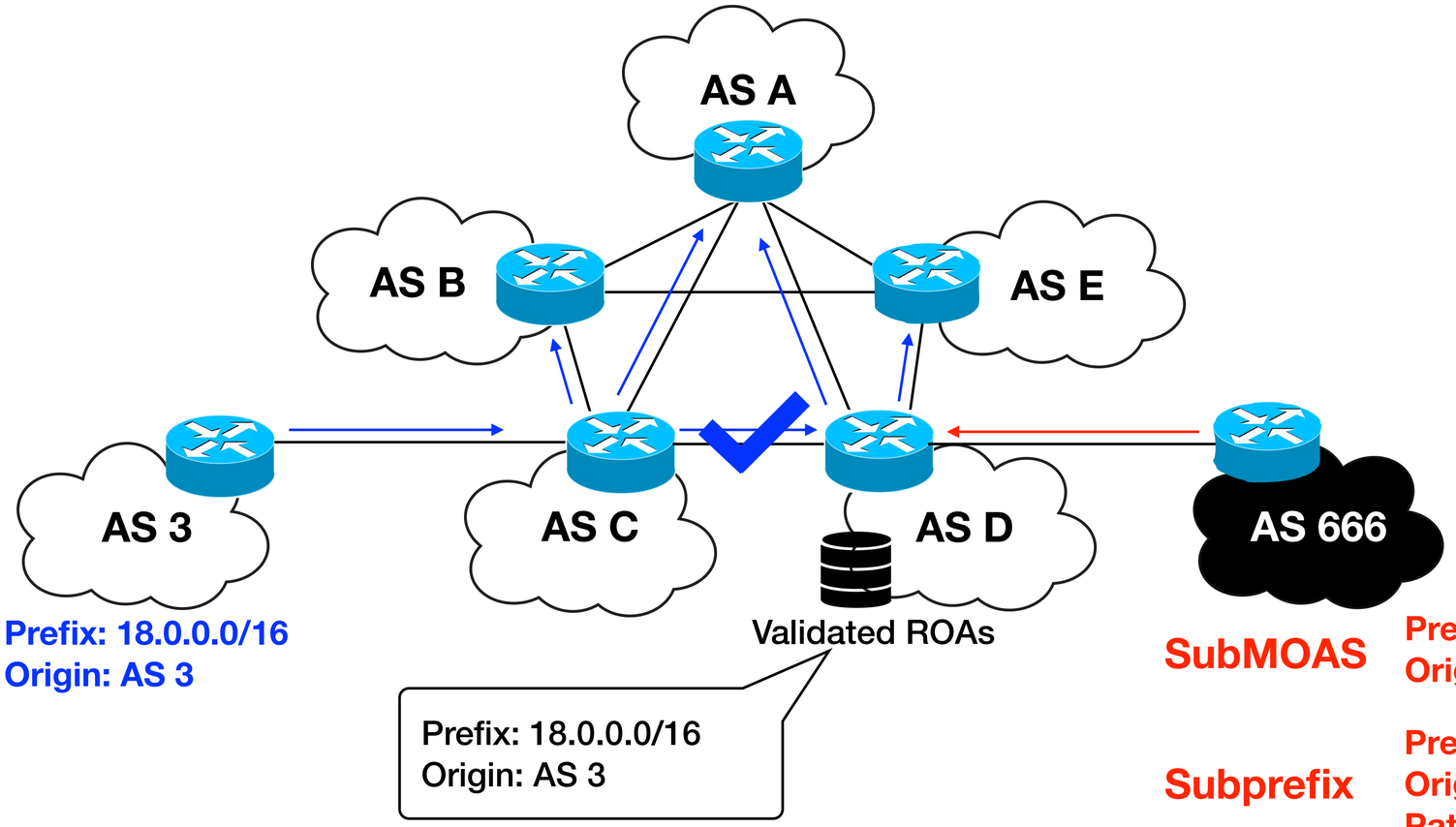
SubMOAS and subprefix conflicts with RPKI



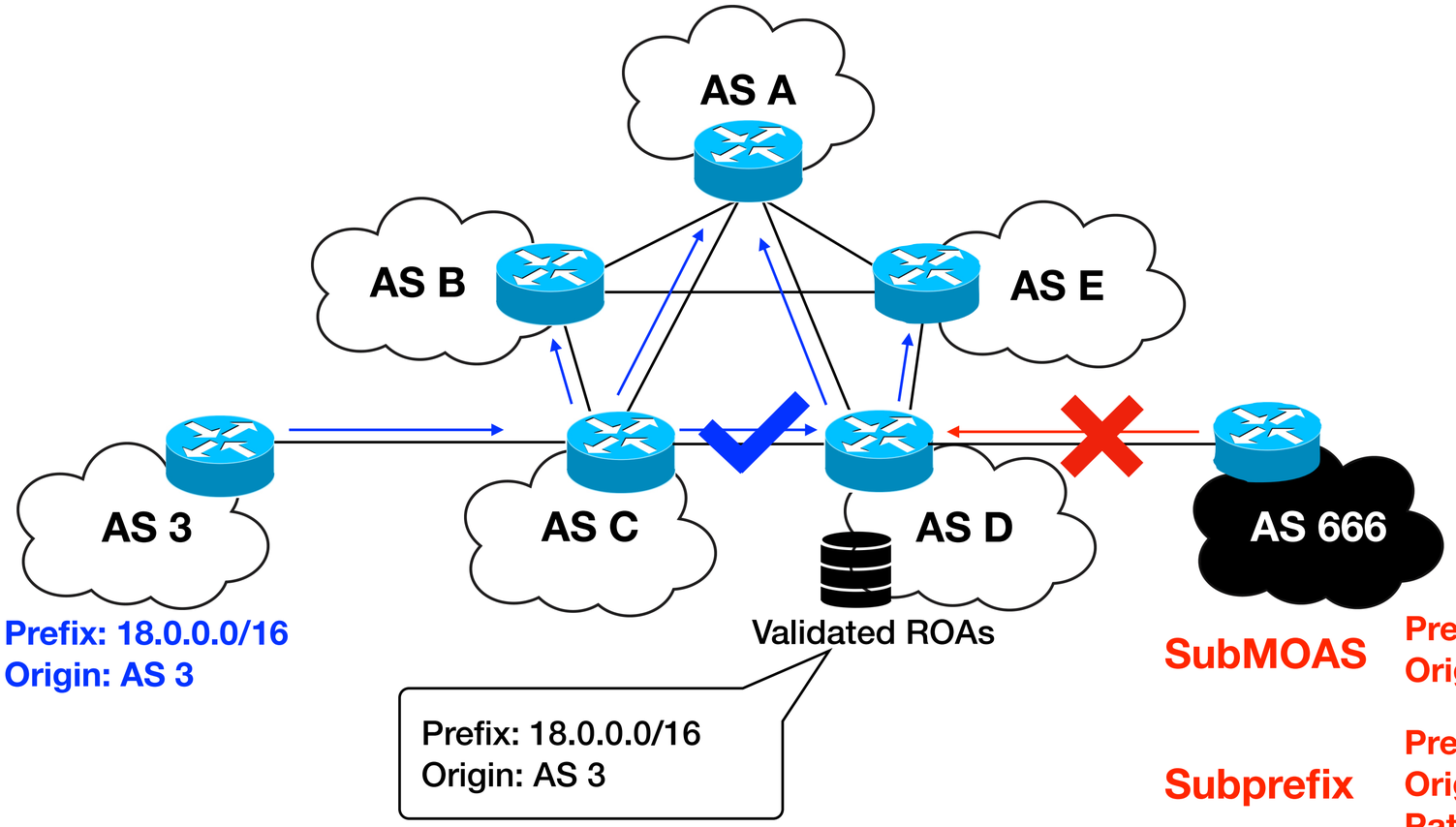
SubMOAS and subprefix conflicts with RPKI



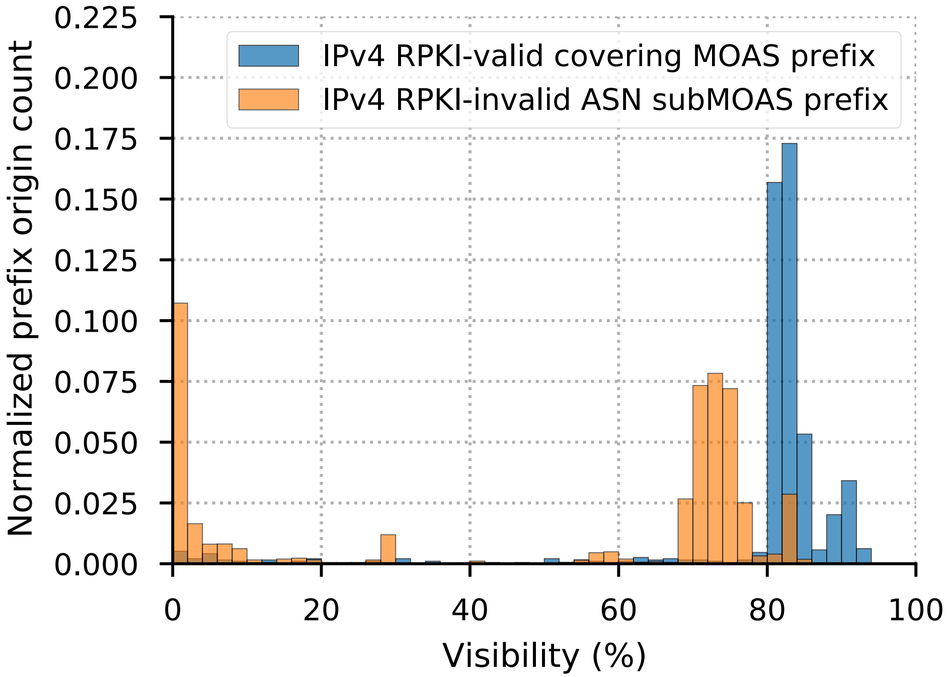
SubMOAS and subprefix conflicts with RPKI

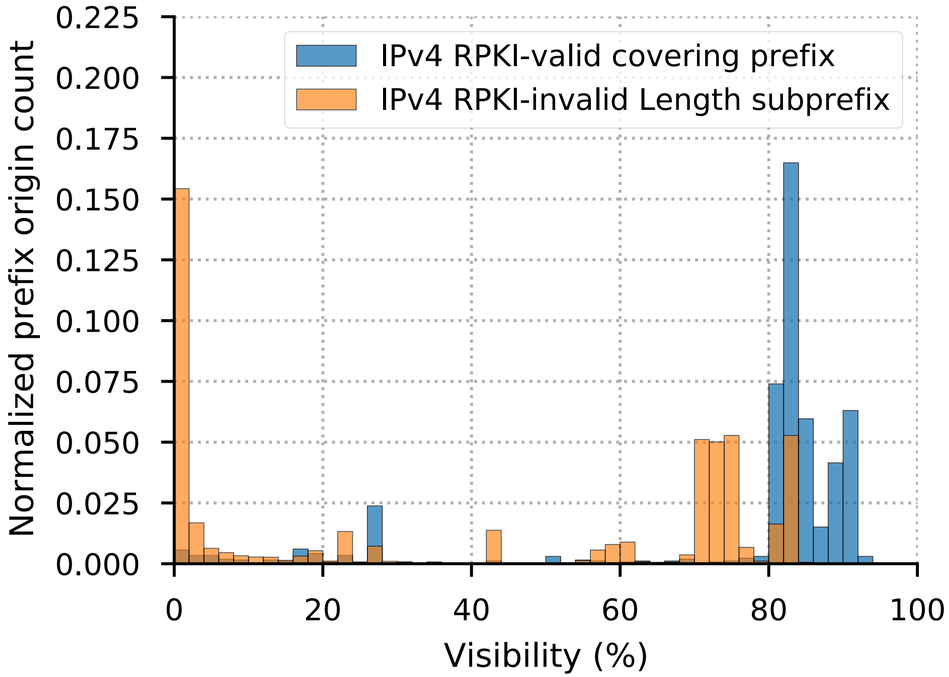


SubMOAS and subprefix conflicts with RPKI

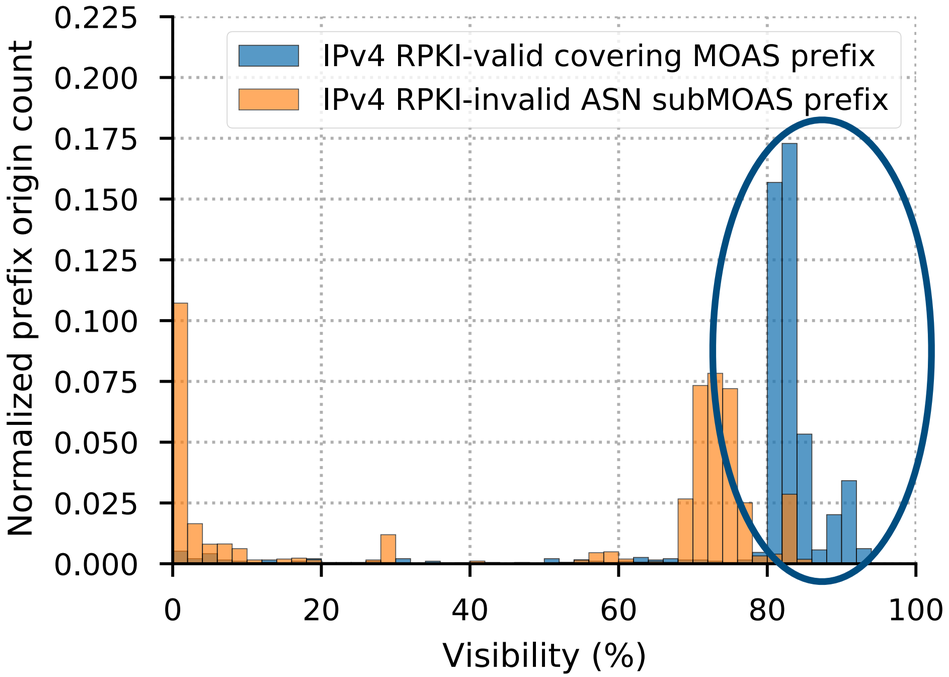


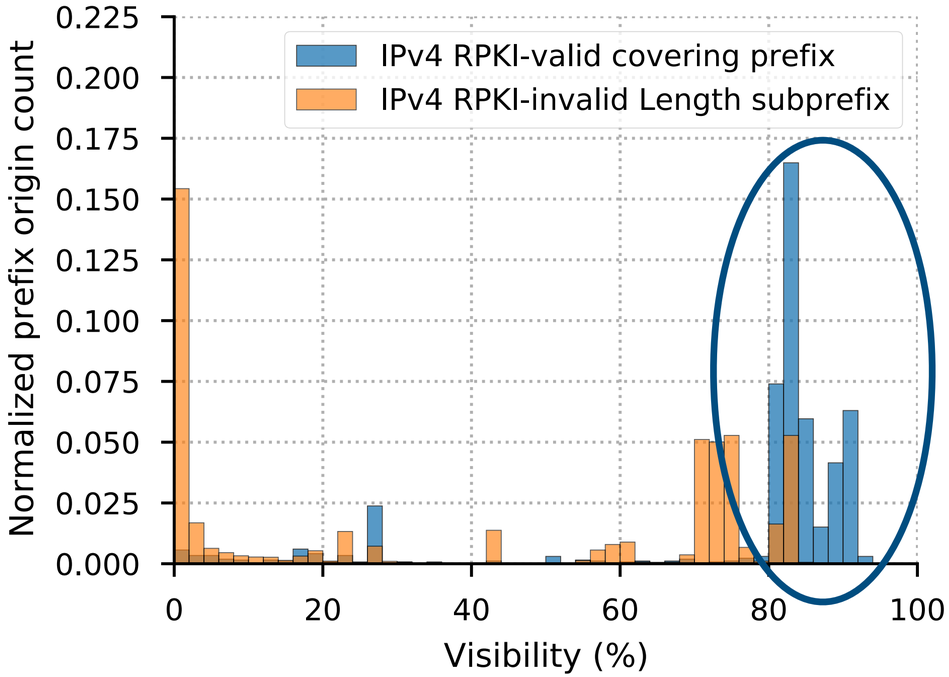
Visibility of subprefixes covered by RPKI



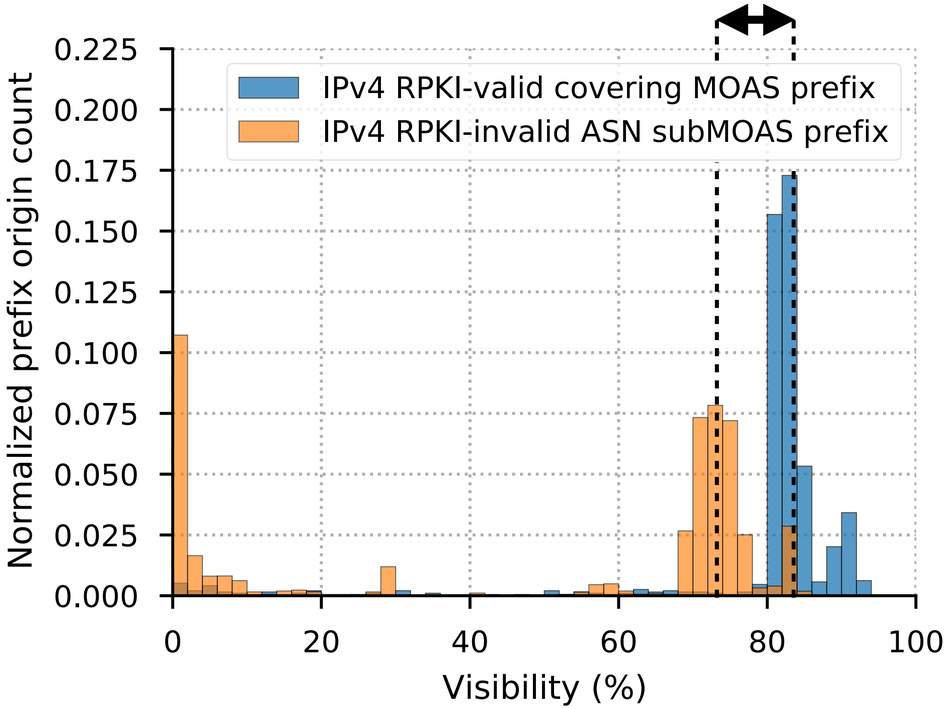


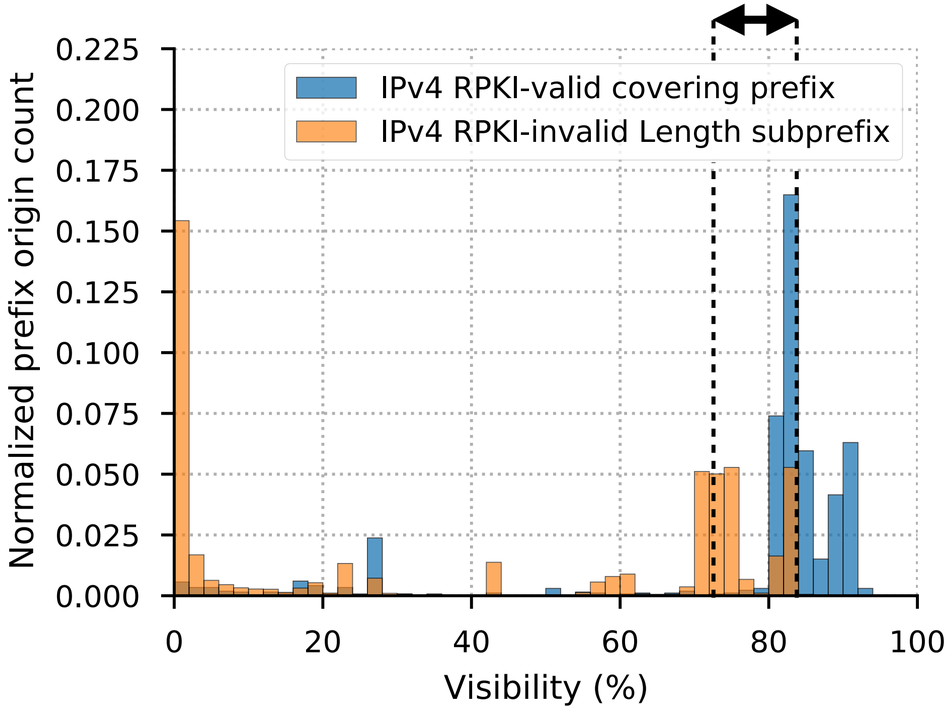
Visibility of subprefixes covered by RPKI



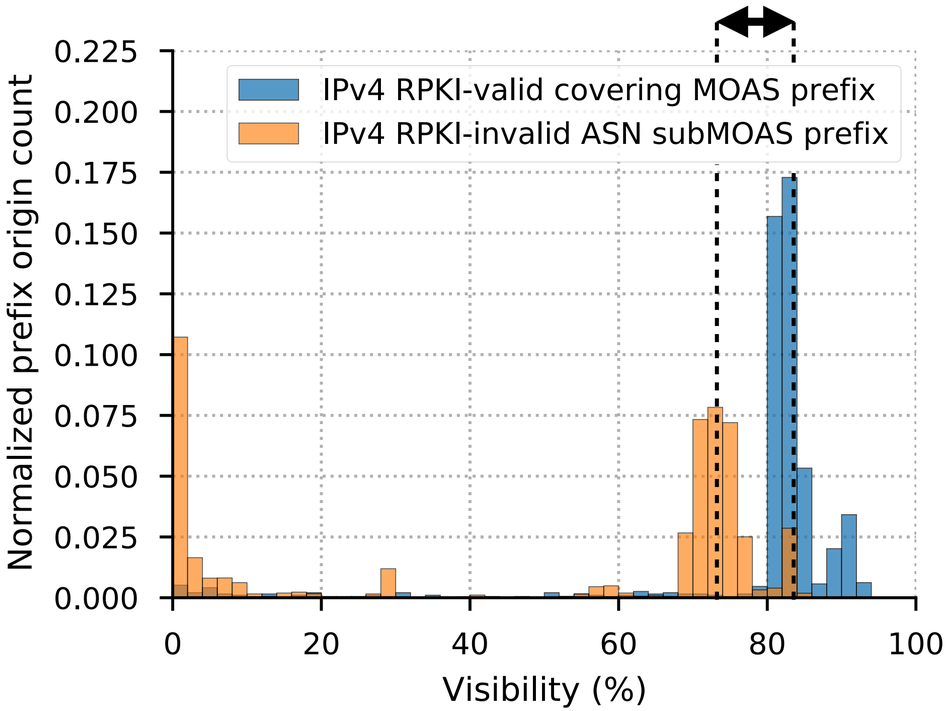


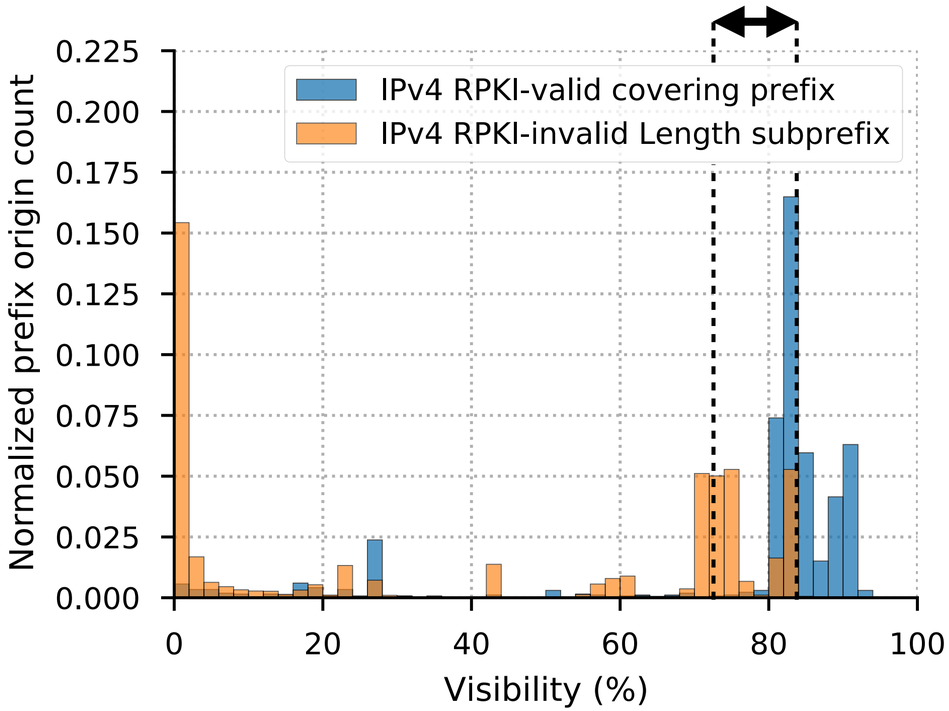
Visibility of subprefixes covered by RPKI





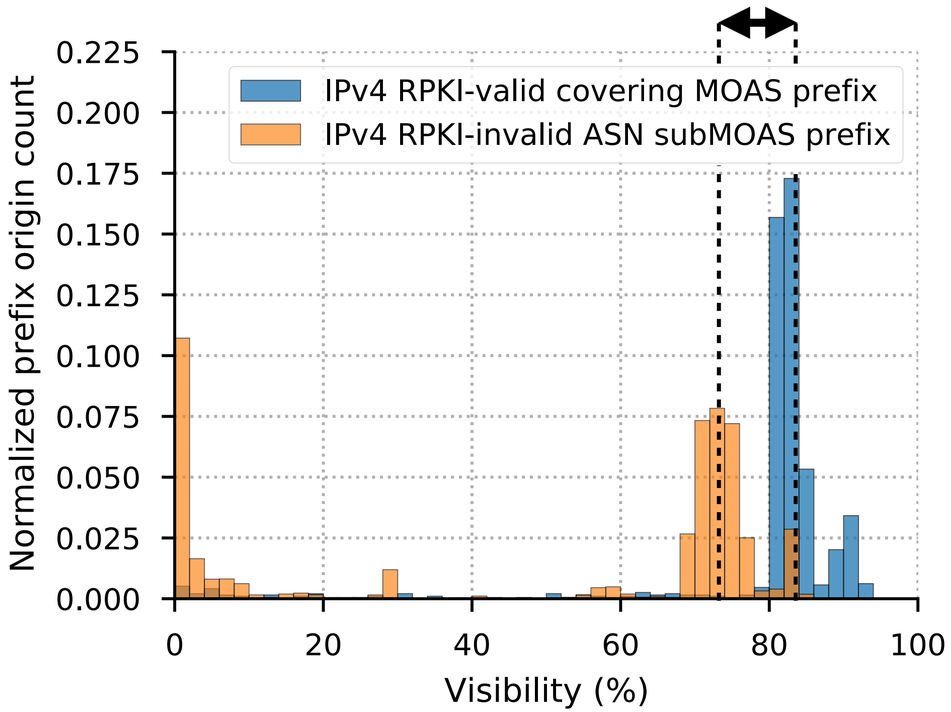
Visibility of subprefixes covered by RPKI

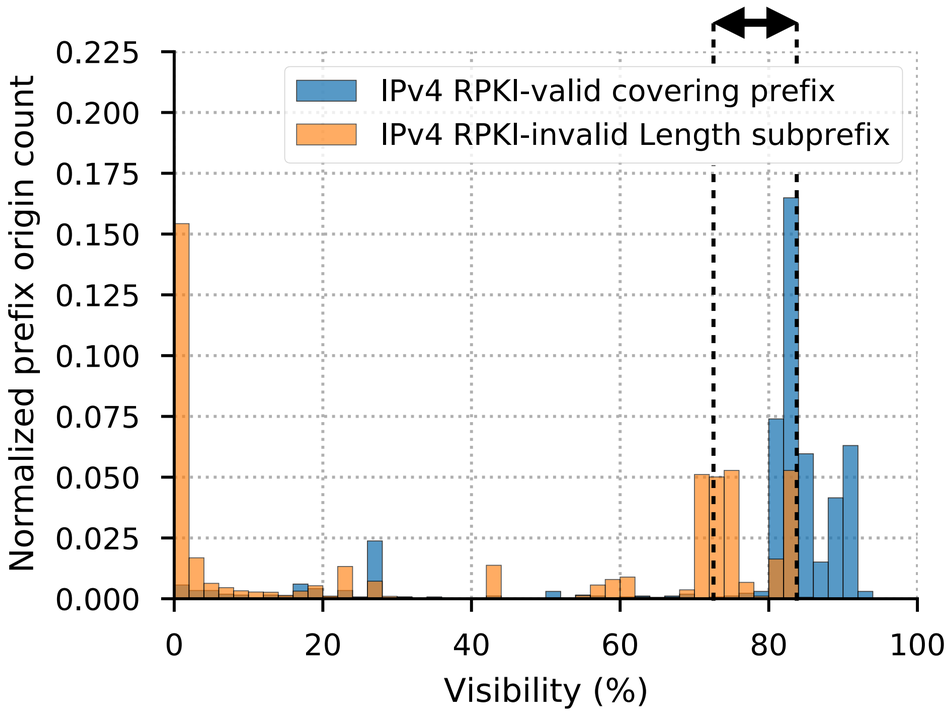




- RPKI-invalid sub prefixes announcements have 10-15% less visibility.

Visibility of subprefixes covered by RPKI





- RPKI-invalid sub prefixes announcements have 10-15% less visibility.
- **RPKI reduces reachability of subMOAS and subprefix path hijacks.**

Key takeaways

- Longitudinal analysis of **RPKI enforcement** shows **growing** number of ISPs begin to filter RPKI-invalid announcements.
- Passive method allows for **continuous monitoring** of RPKI enforcement.
- **First** study to measure the **benefit** of registering prefixes in the **RPKI**.
- RPKI enforcement starts to **bring real value to networks:**
  - limits the propagation of illicit announcements,
  - reduces visibility of challenging announcements in case of conflicts.

Key takeaways

- Longitudinal analysis of **RPKI enforcement** shows **growing** number of ISPs begin to filter RPKI-invalid announcements.
- Passive method allows for **continuous monitoring** of RPKI enforcement.
- **First** study to measure the **benefit** of registering prefixes in the **RPKI**.
- RPKI enforcement starts to **bring real value to networks:**
  - limits the propagation of illicit announcements,
  - reduces visibility of challenging announcements in case of conflicts.