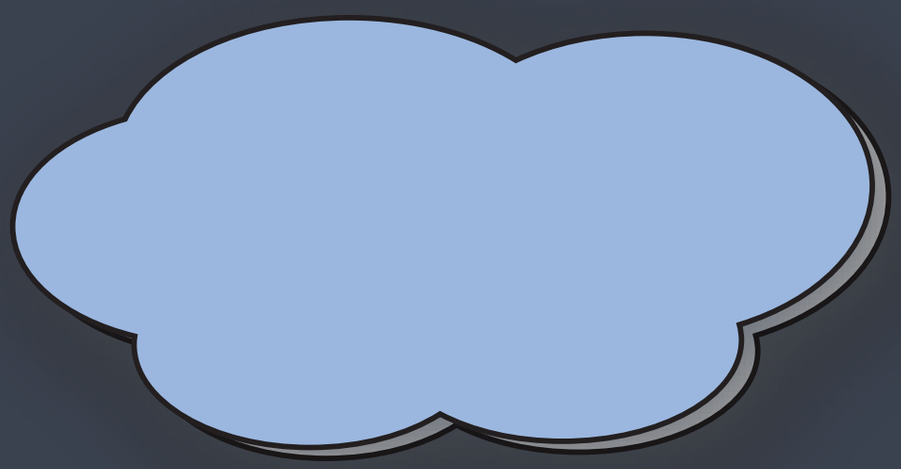
Improving the Security and Robustness of Internet Routing

Georgos Siganos: siganos@gmail.com

Michalis Faloutsos: michalis@cs.ucr.edu



138.23/16 5 13 100 40

- Origin AS Validation
- Path Validation

- S-BGP, SoBGP
- RPSEC
- Deployment Problems

What can we do today?

- IRR + RIR
- MyAS (RIPE)
- Our Approach

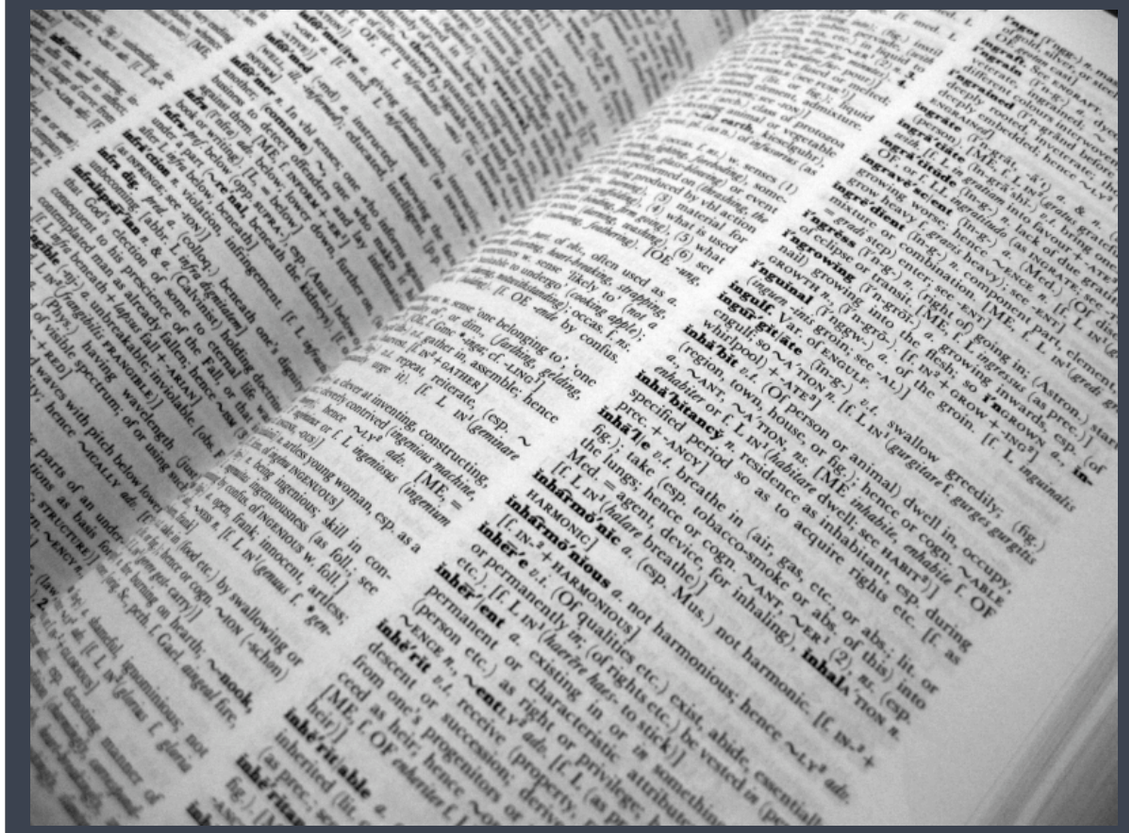
even for RIPE!!!

- Announced but NOT registered for RIPE prefixes 7866.
- 24% can not be Verified for RIPE.
- MyAS uses different data than RIR&IRR

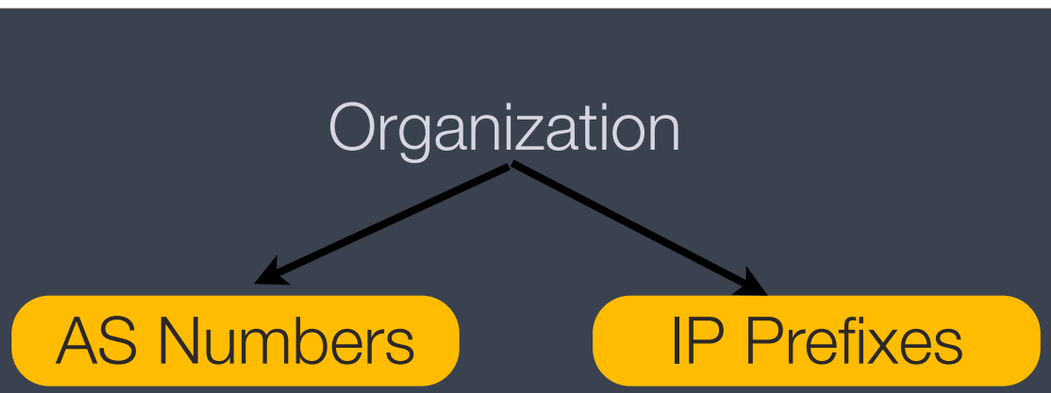
- Data & Methodology
- Validation Results
- ISP Reaction

Data & Methodology

- RIR-IRR
- How we do the validation



- ARIN
- RIPE
- APNIC
  - JPNIC, TWNIC, KRNIC, CCAIR
- LACNIC
  - BRNIC
- (AFRNIC)



Secure Validation

Route Records

Weak Validation

Technical personnel
DNS Server records
AUT-NUM policy
Email servers (tech)
No conflict

Heuristics

For the first two cases we check both the last asn and the second to last.

Can AS3333 be the origin of 193.0.0.0/21?

```
aut-num:     AS3333
as-name:     RIPE-NCC-AS
descr:       RIPE Network Coord. Centre
remarks:
remarks:     +--------------------------+
remarks:     | AMS-IX Nikhef            |
remarks:     +--------------------------+
remarks:
remarks:
import:    ...
export:    ...
admin-c:     AMR68-RIPE
admin-c:     RDK-RIPE
tech-c:      OPS4-RIPE
mnt-by:      RIPE-NCC-MNT
source:      RIPE
```

```
inetnum:        193.0.0.0 - 193.0.7.255
netname:        RIPE-NCC
descr:          RIPE Network Coord. Centre
descr:          Amsterdam, Netherlands
remarks:        Used for RIPE NCC infr.
country:        NL
admin-c:        AMR68-RIPE
admin-c:        RDK-RIPE
tech-c:         OPS4-RIPE
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-MNT
mnt-lower:      RIPE-NCC-MNT
source:         RIPE
```

```
route:          193.0.0.0/21
descr:          RIPE-NCC
origin:         AS3333
mnt-by:         RIPE-NCC-MNT
changed:        ripe-dbm@ripe.net 19980225
changed:        joao@ripe.net 19980720
changed:        joao@ripe.net 20000908
source:         RIPE
```

Can AS10745 be the origin of 192.149.252.0/24?

```
ASHandle:           AS10745
OrgID:              ARIN
ASName:             ARIN
ASNumber:           10745
RegDate:            1997-11-14
Updated:            2003-04-30
TechHandle:         ARIN-HOSTMASTER
Source:             ARIN
```

```
NetHandle:      NET-192-149-252-0-1
OrgID:          ARIN
Parent:         NET-192-0-0-0-0
NetName:        ARIN-NET
NetRange:       192.149.252.0 -
192.149.252.255
NetType:        assignment
RegDate:        1997-11-05
Updated:        2004-05-03
NameServer:     NS1.ARIN.NET
NameServer:     NS2.ARIN.NET
TechHandle:     ARIN-HOSTMASTER
Source:         ARIN
```

```
route:      192.149.252.0/24
descr:      ARIN
            4506 Daly Drive, Suite 200
            Chantilly, VA 20151, US
origin:     AS10745
notify:     rtreg@arin.net
mnt-by:     MNT-ARIN
changed:    lwang@arin.net 19990225
source:     ARIN
```

Can AS7195 be the origin of 200.24.75/24?

```
aut-num: 7195
owner:   Telecorp Colombia S.A.
city:    Bogota
country: CO
owner-c: FEH2
```

```
inetnum:     200.24.75/24
status:      reassigned
owner:       El portal de Internet S.A.
city:        Bogota
country:     CO
owner-c:     FEH2
tech-c:      FEH2
inetrev:     200.24.75/24
nserver:     NS.GLOBALONE.NET.CO
nserver:     NS2.GIP.NET
nserver:     NS3.GIP.NET
inetnum-up:  200.24.64/19
```

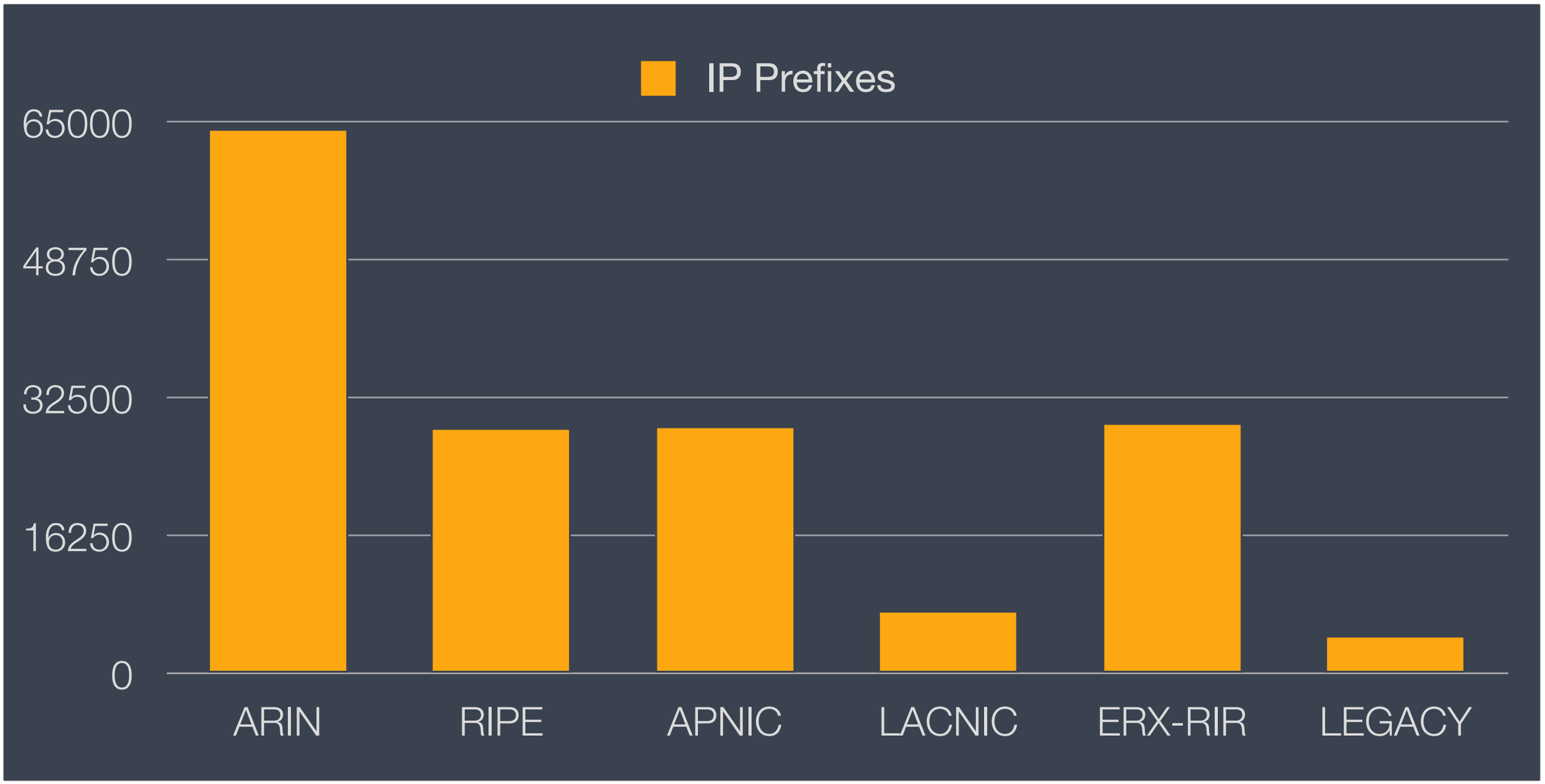
Evaluation of Approach

- Dec. 28 2004- Jan. 09 2005
- Origin AS Validation
- Reactive Approach

	RRC03	RV2	RRC06
Unique (Prefix,Origin AS)	164,152	177,507	158,498
Number of Flags	6,008	6,109	6,039
Percentage of Flags	3.5%	3.4%	3.8%

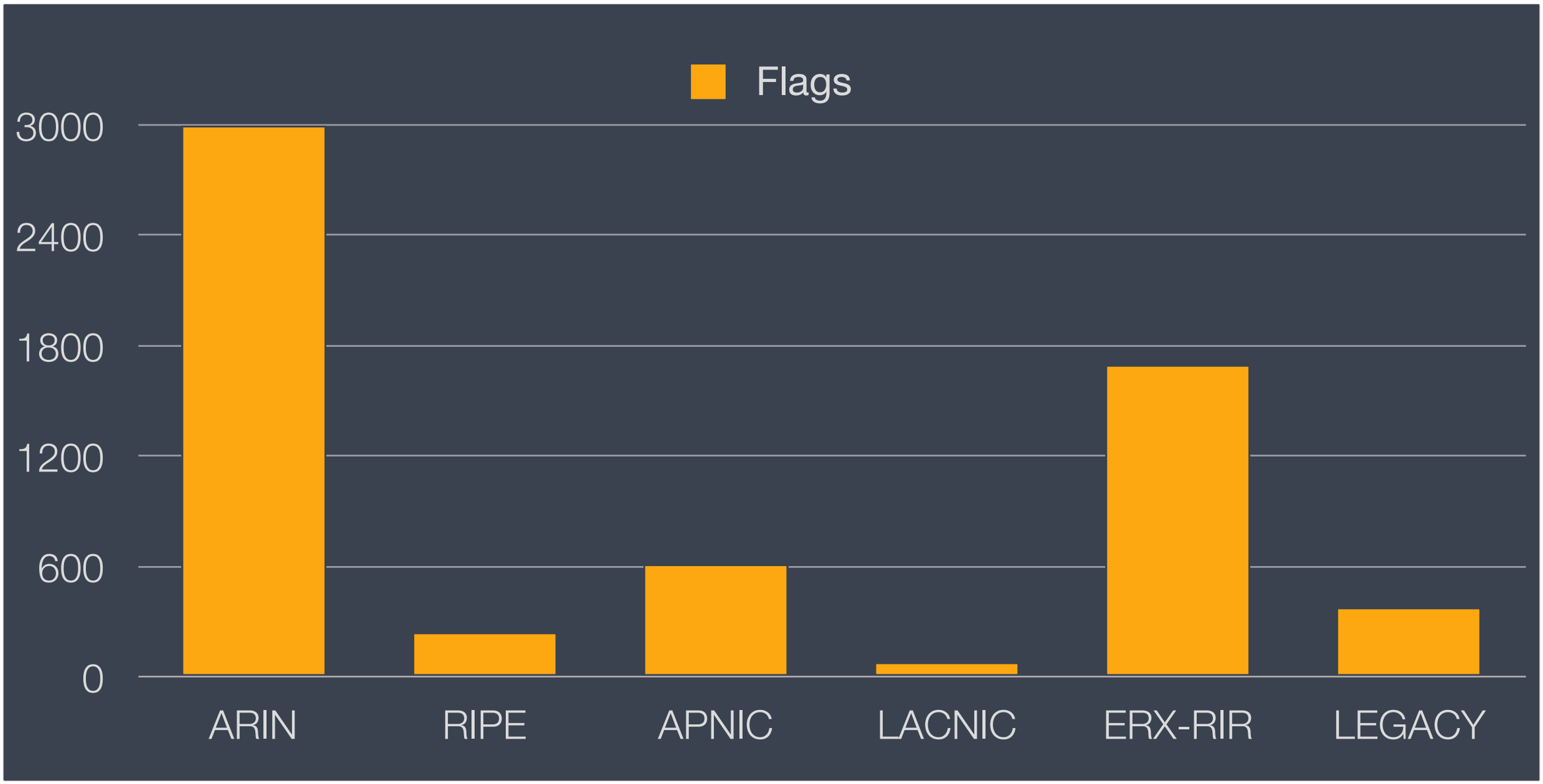
Origin AS Flags

Aggregate Numbers



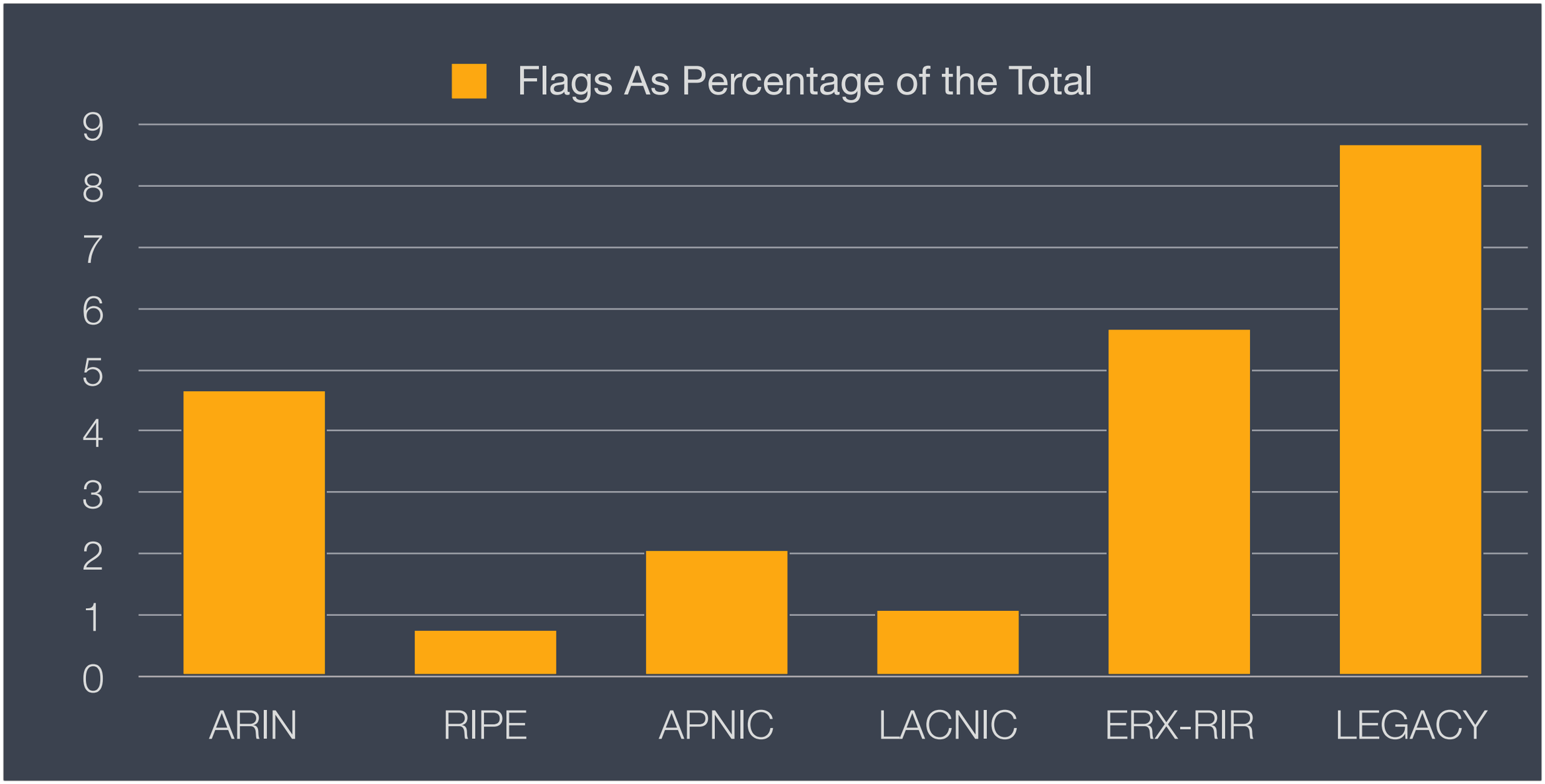
IP Prefixes per RIR

As seen by RRC03



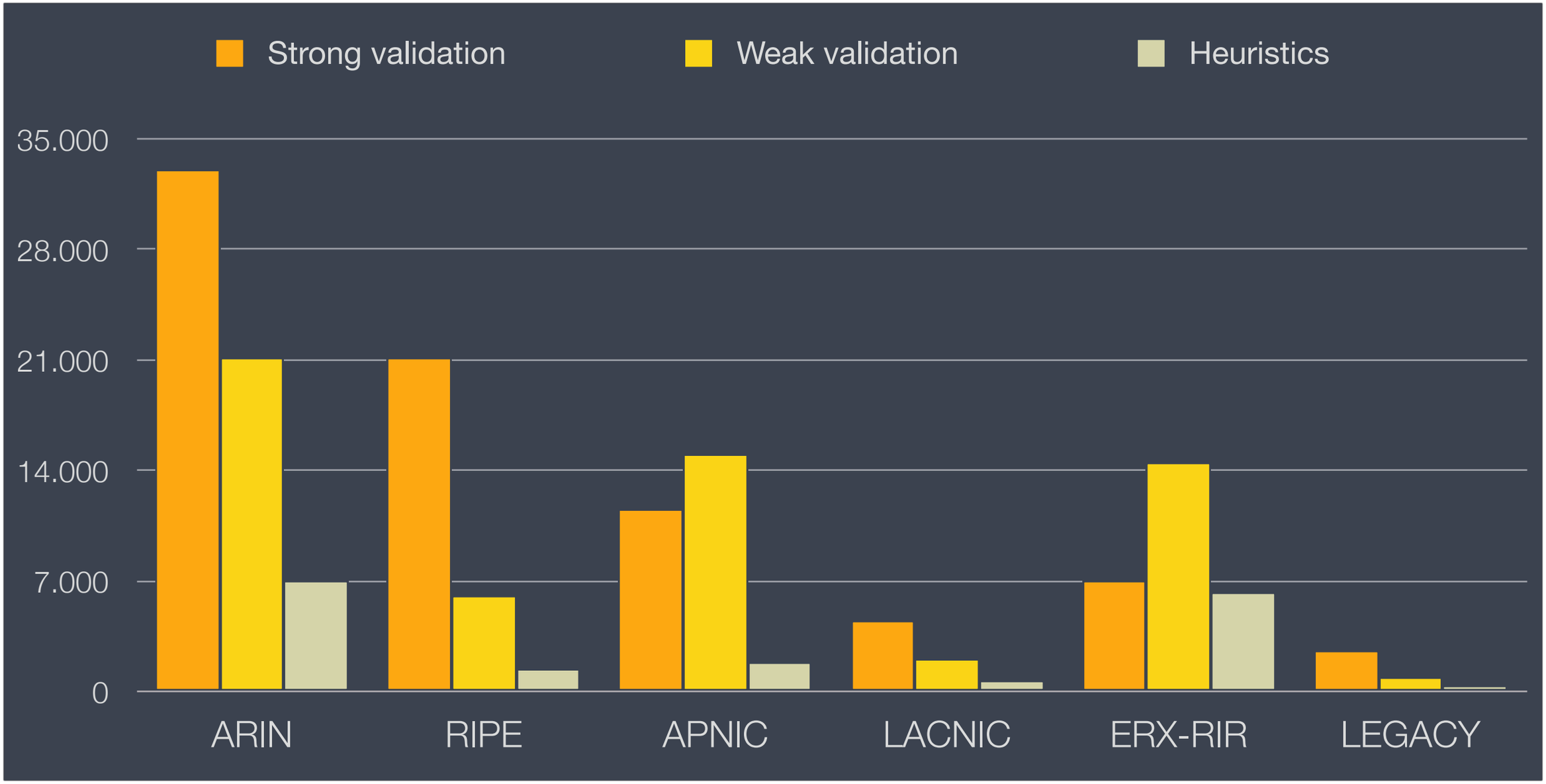
Flags per RIR

As seen by RRC03



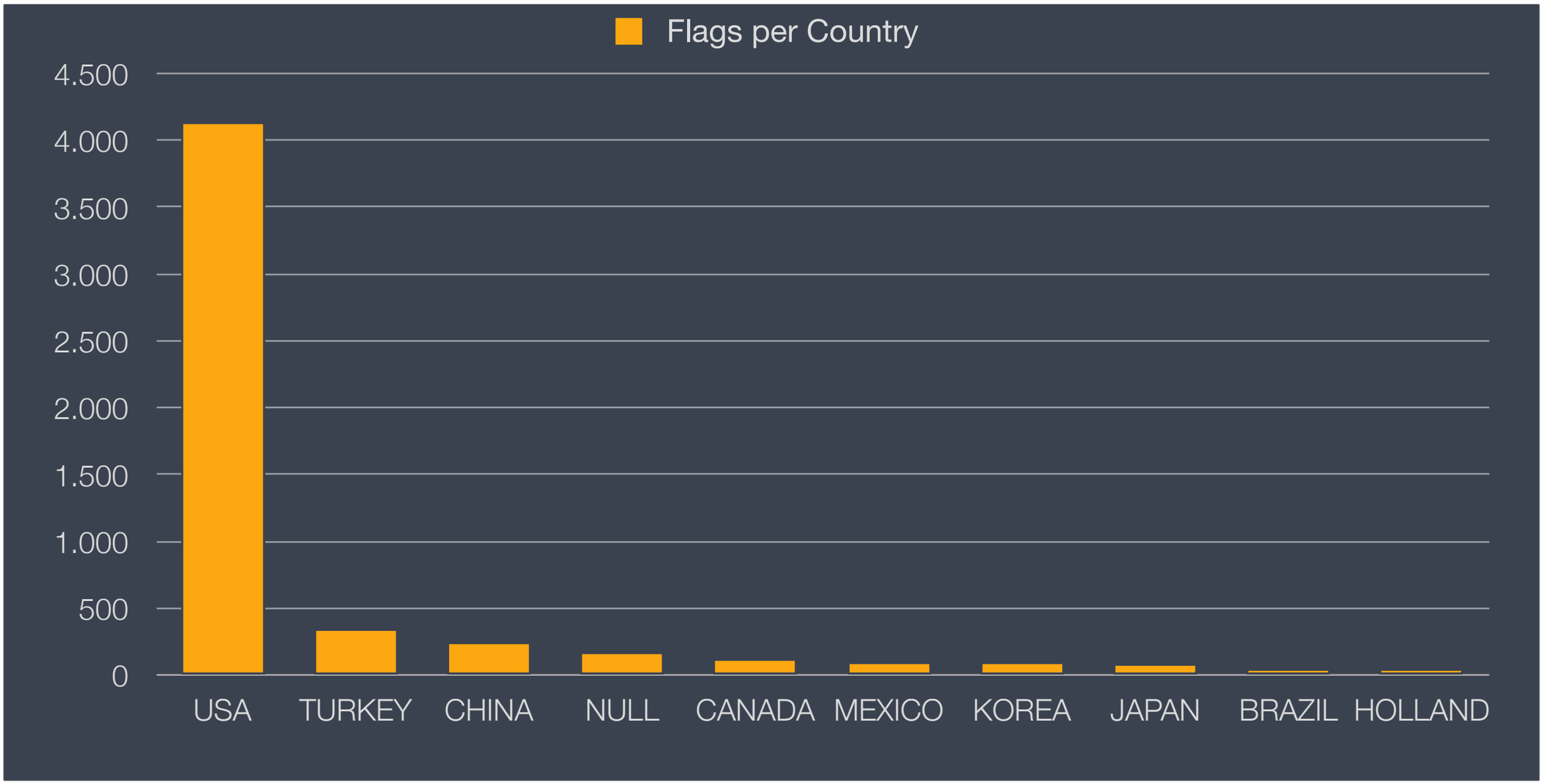
Percentage of flags per RIR

As seen by RRC03



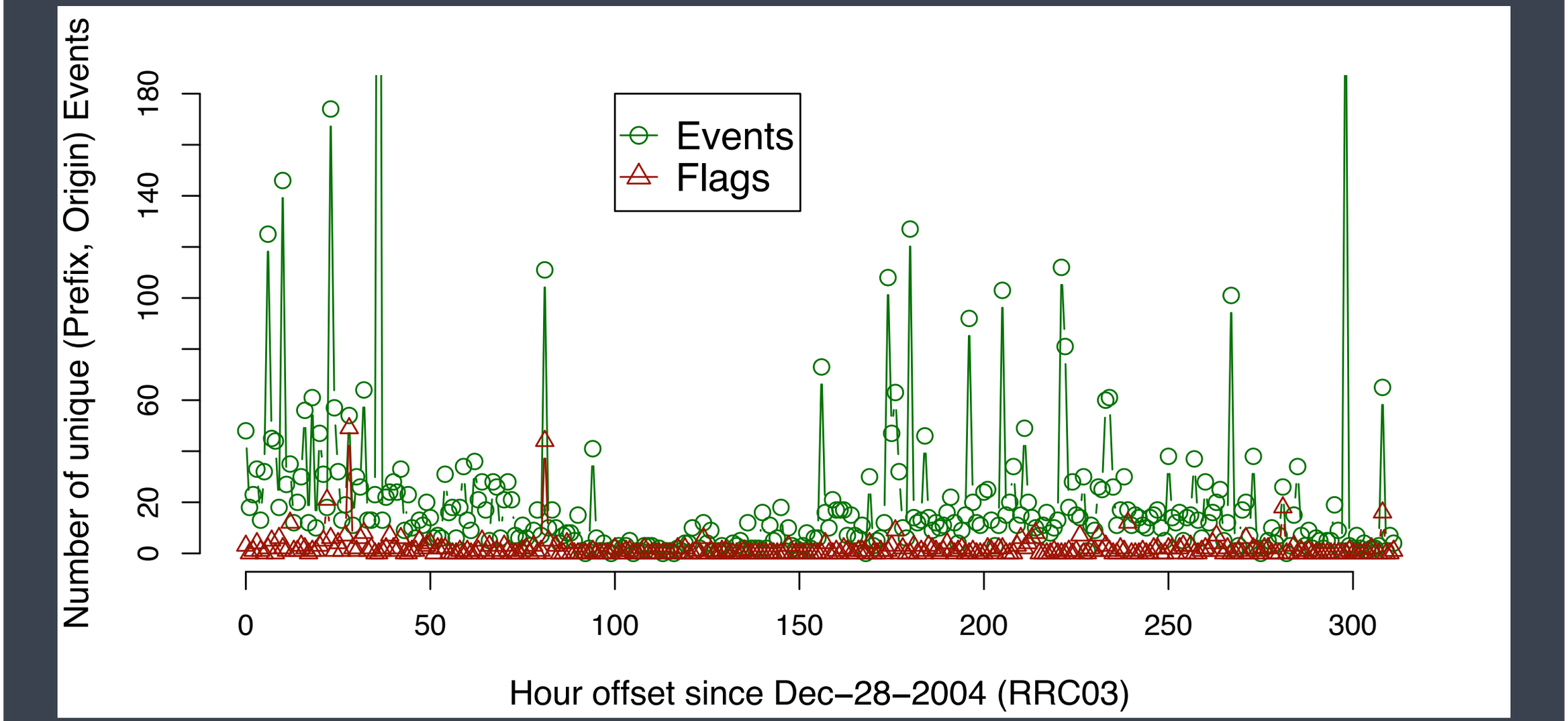
Validation Details

AS seen by RRC03

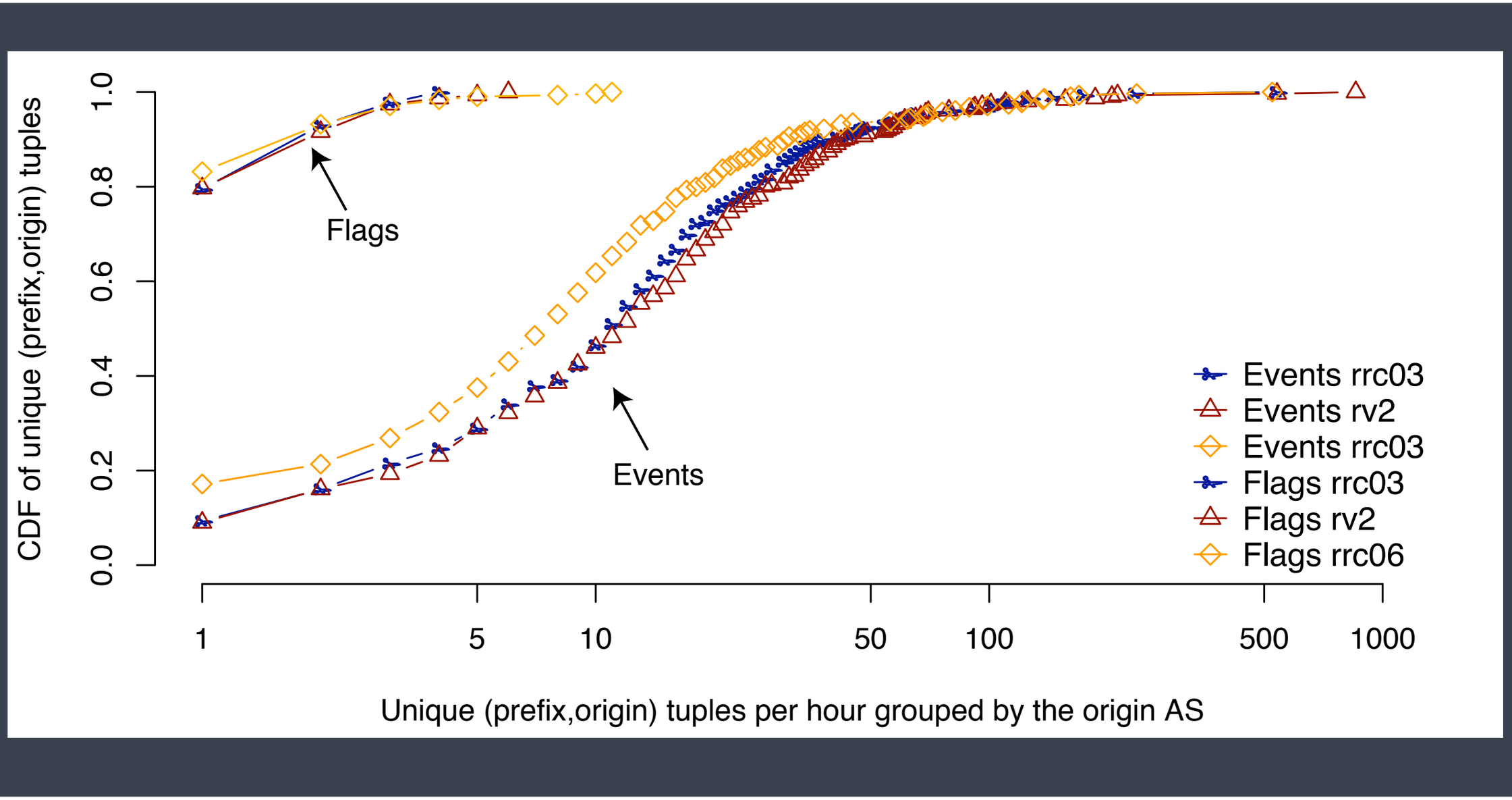


Origin AS Flags

Grouped by the country of registration of the AS

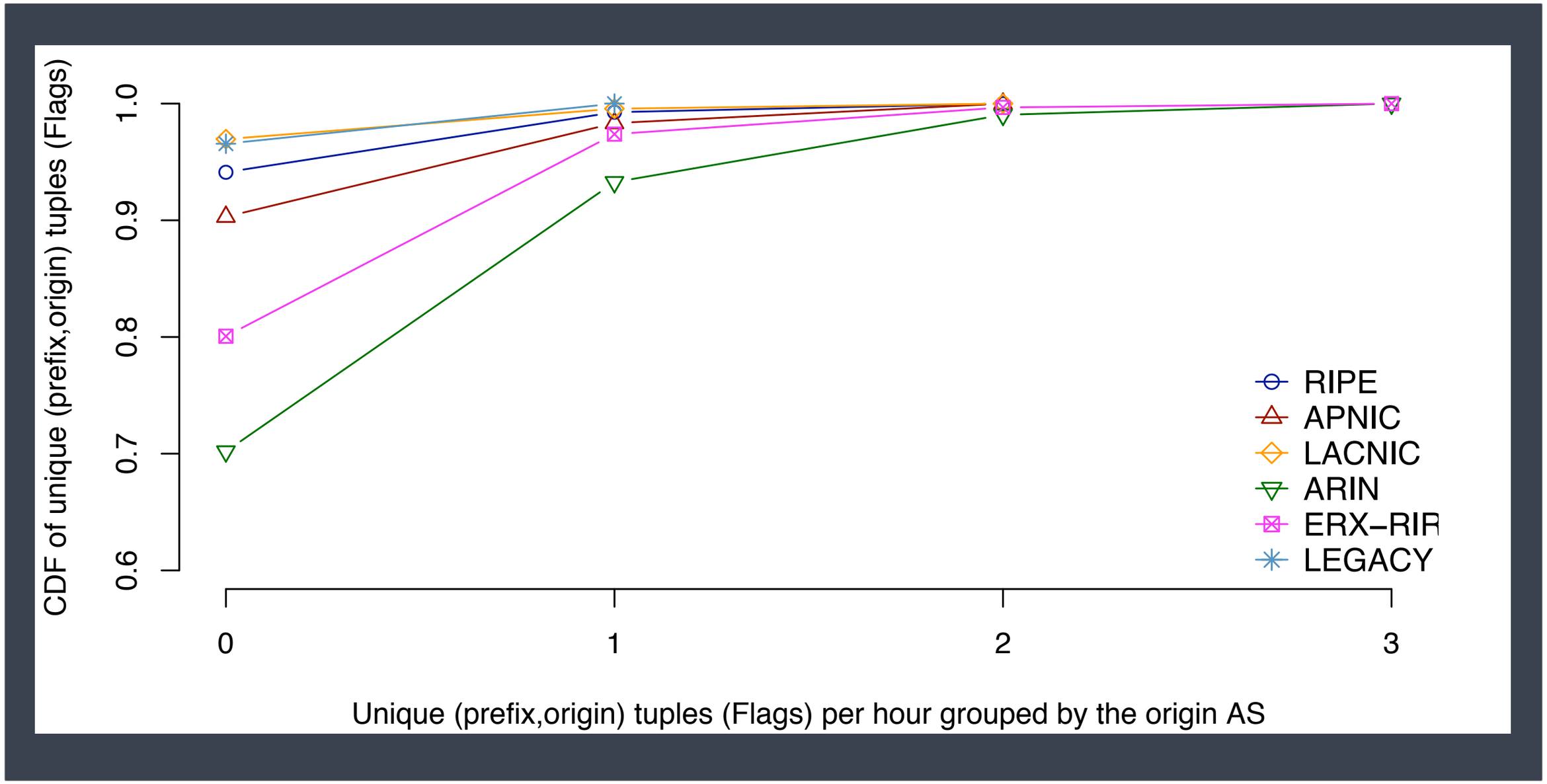


Evolution of Origin AS



Events & Flags

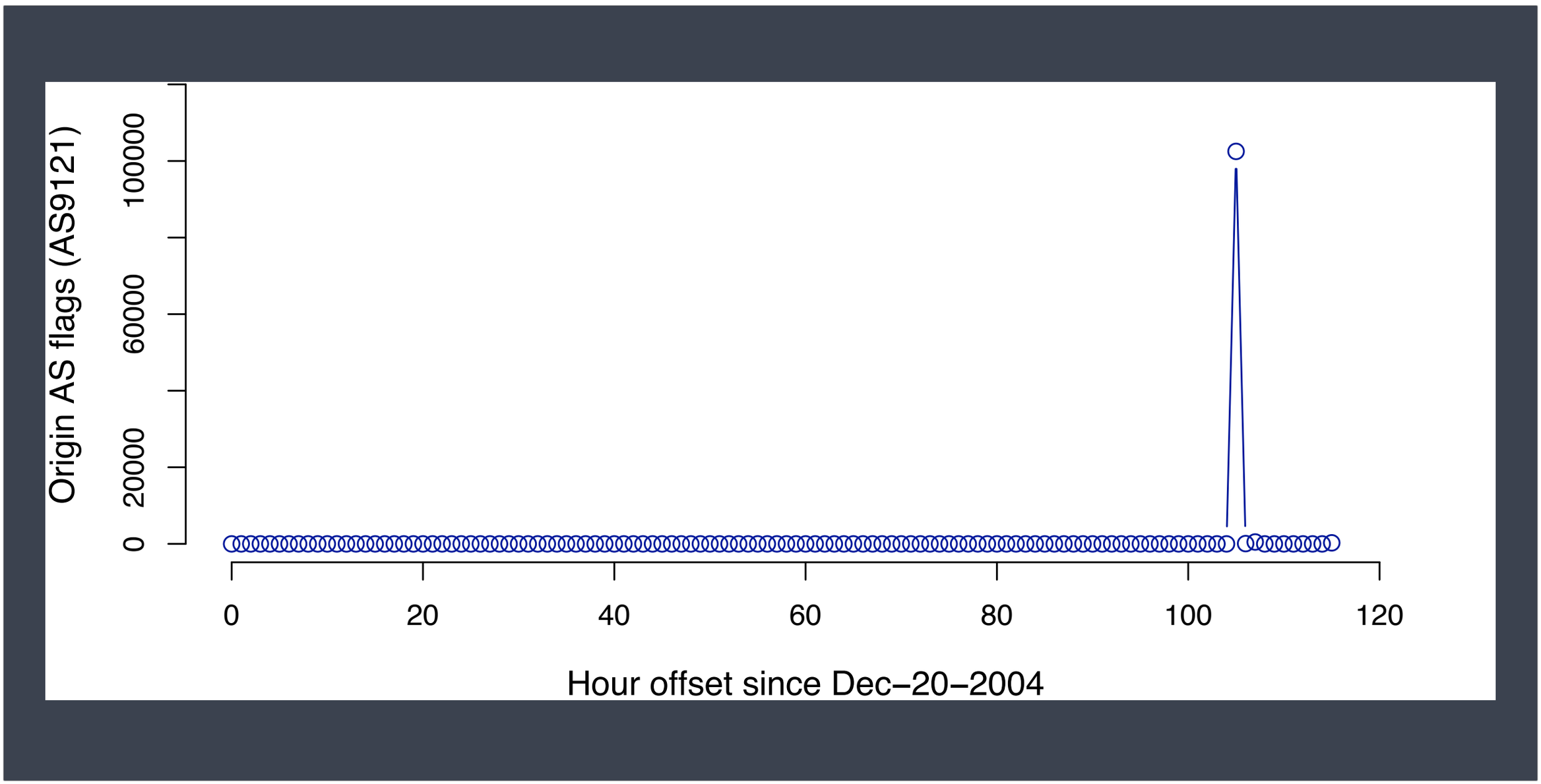
Grouped by the origin AS



Flags per RIR

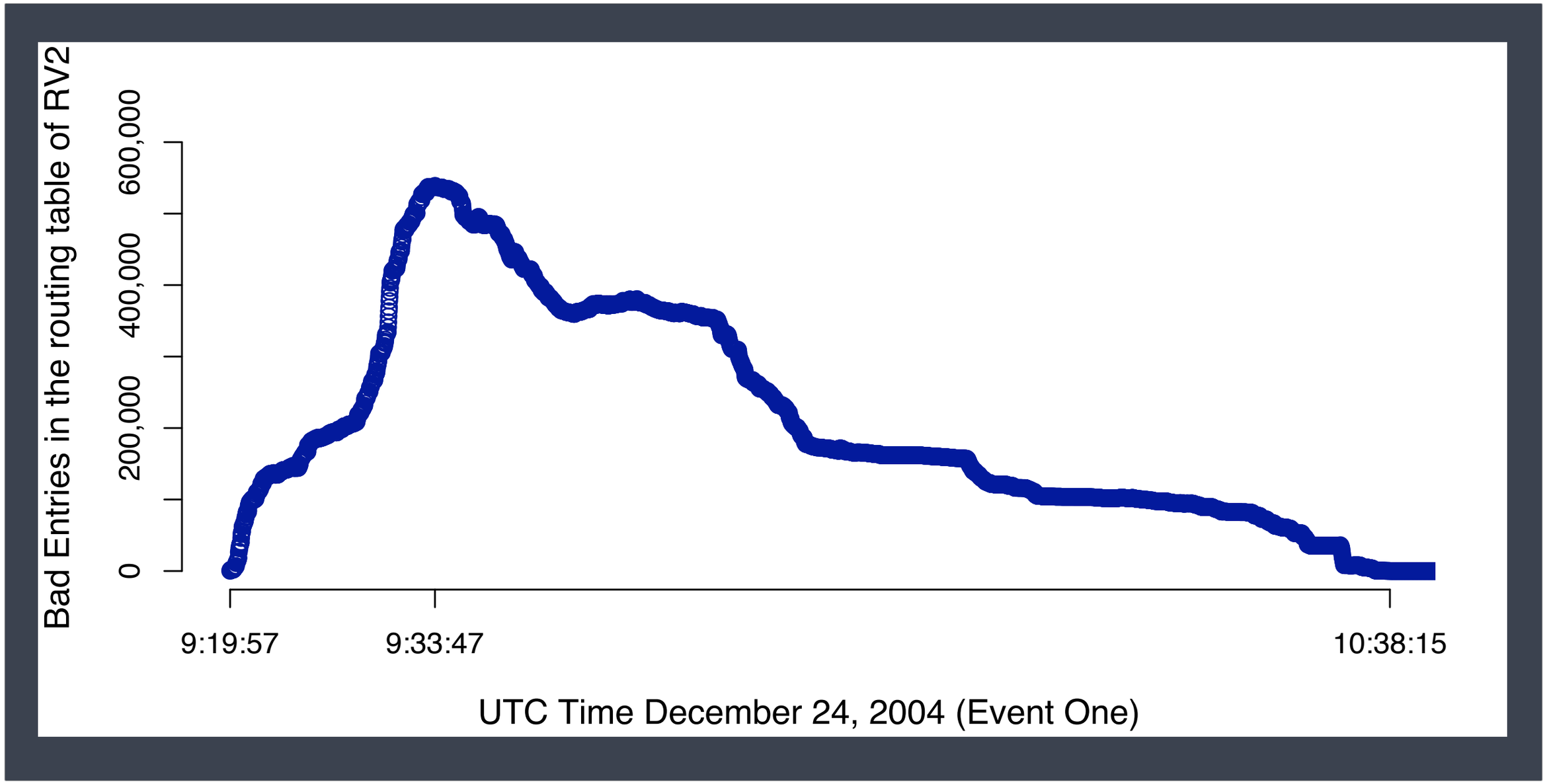
The profile of a routing leak

- AS9121 Event
- How fast ISPs reacted?



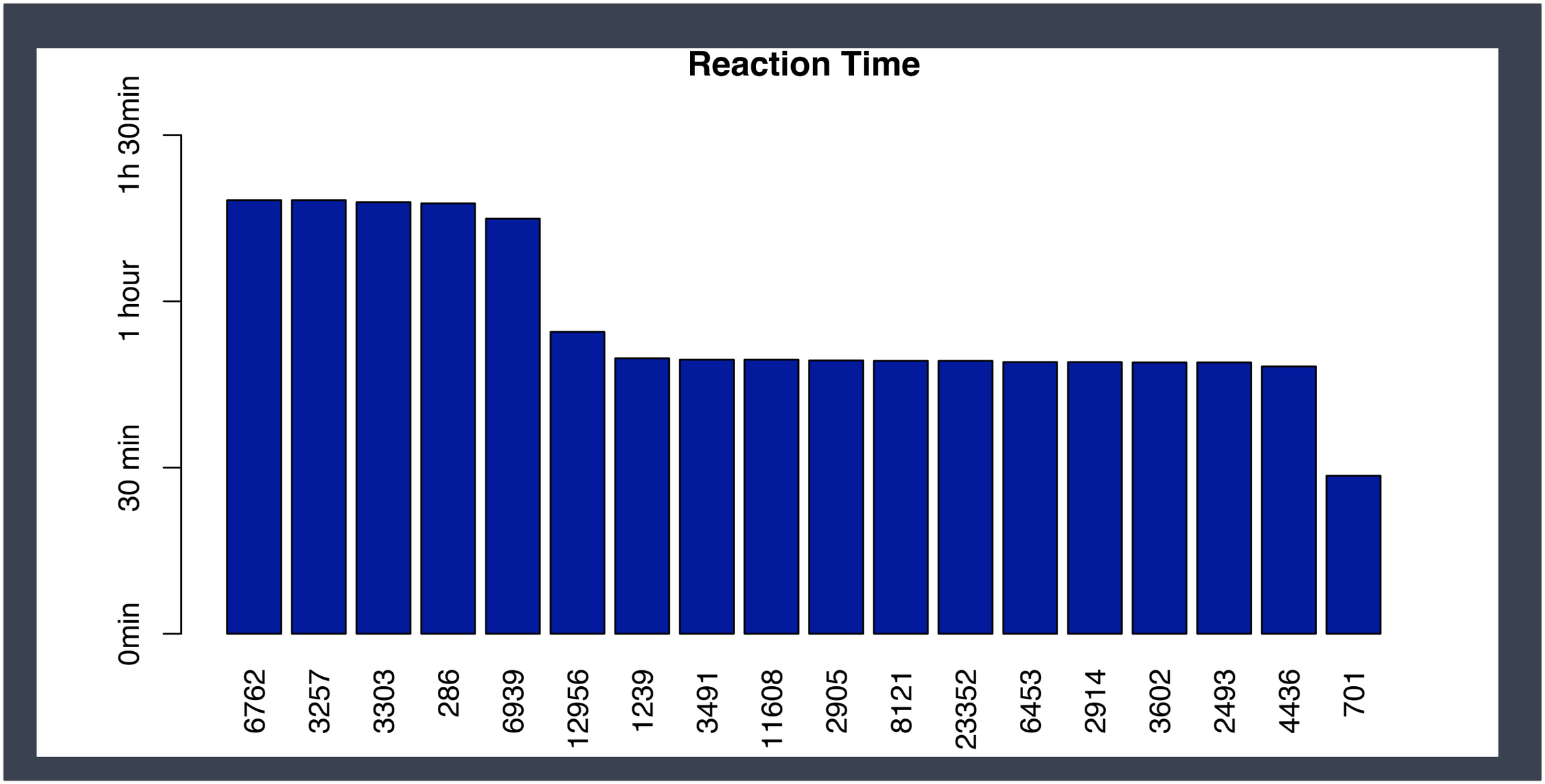
Flags by AS9121

As seen by RV2



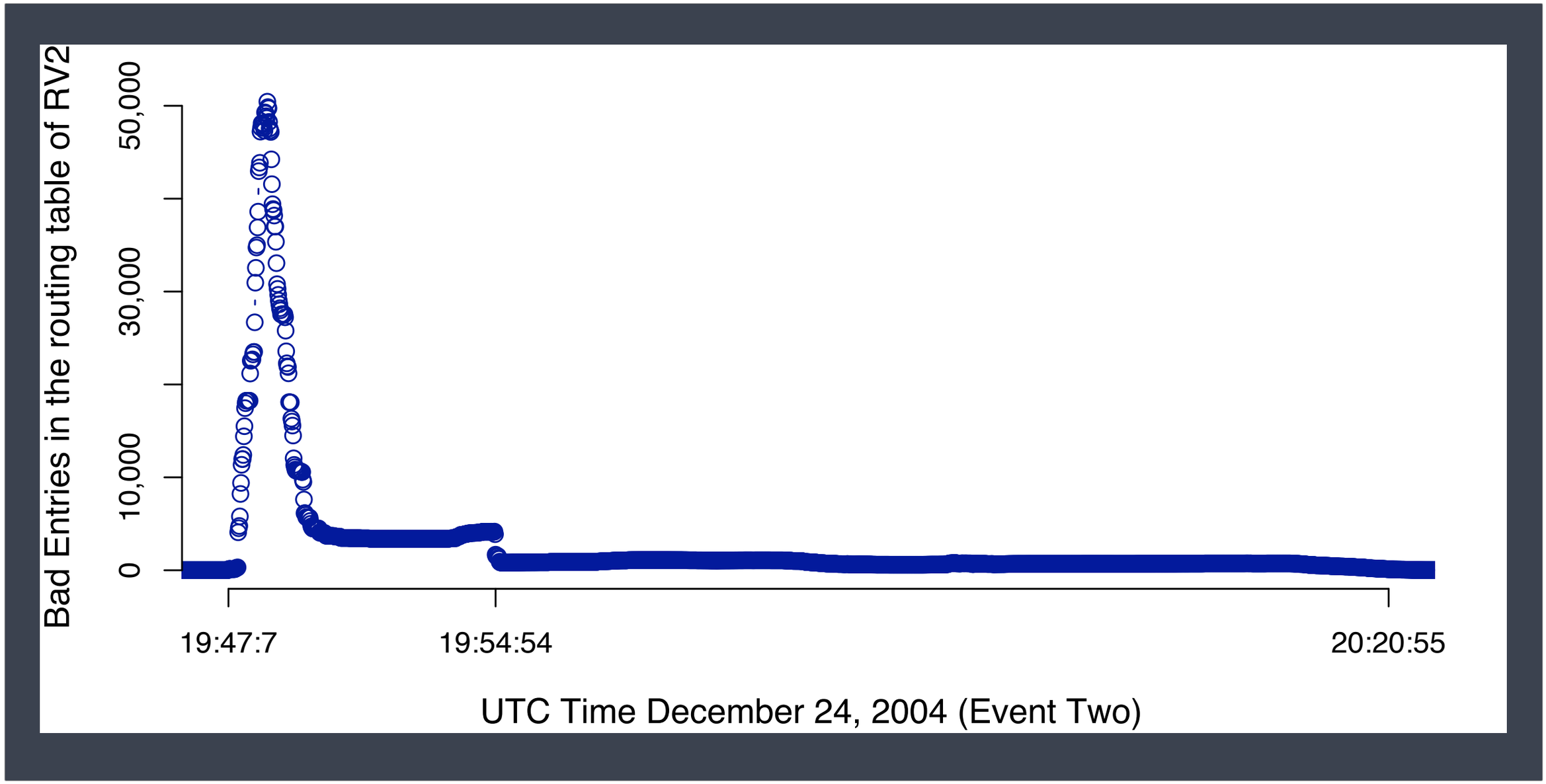
AS9121 Event One

AS seen by RV2



ISP reaction time

Event One



AS9121 Event Two

AS seen by RV2

Conclusions

- We can validate ~97% of the prefixes
- A reactive approach would generate 0-3 flags per hour.
- Can we resolve routing errors within minutes?