BGP HIJACKING

OS3: Bram ter Borch & Jeroen Schutrup

National Cyber Security Center

BORDER GATEWAY PROTOCOL (BGP)

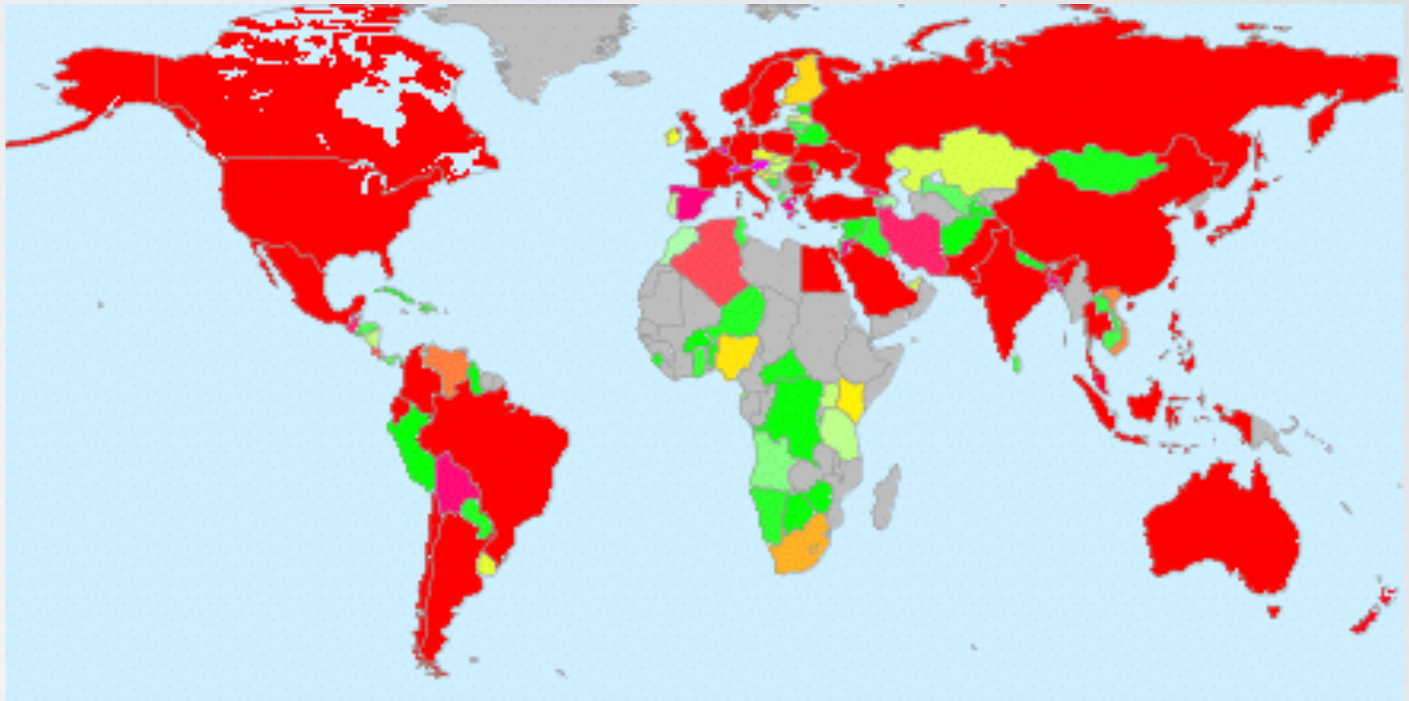
- Internets main routing protocol
- RFC 4271 - original from 1989
- Connects Autonomous Systems (AS)
- BGP hijack

WHAT IS A BGP HIJACK

- Prefix hijack

- Subnet hijack

- AS and prefix hijack



1) http://www.bgpmon.net/chinese-isp-hijacked-10-of-the-internet/

- AS and subnet hijack

- Supernet hijack (introduced in our paper)

EXISTING SOLUTIONS

Web based

- BGPMON
- DYN.com

Tooling

- PHAS
- iSPY
- BGPmon.py

Theoretical

- Hu et al. (fingerprinting and traceroute)
- Zheng et al. (traceroute to monitored networks from reference point)

LIMITATIONS & CHALLENGES

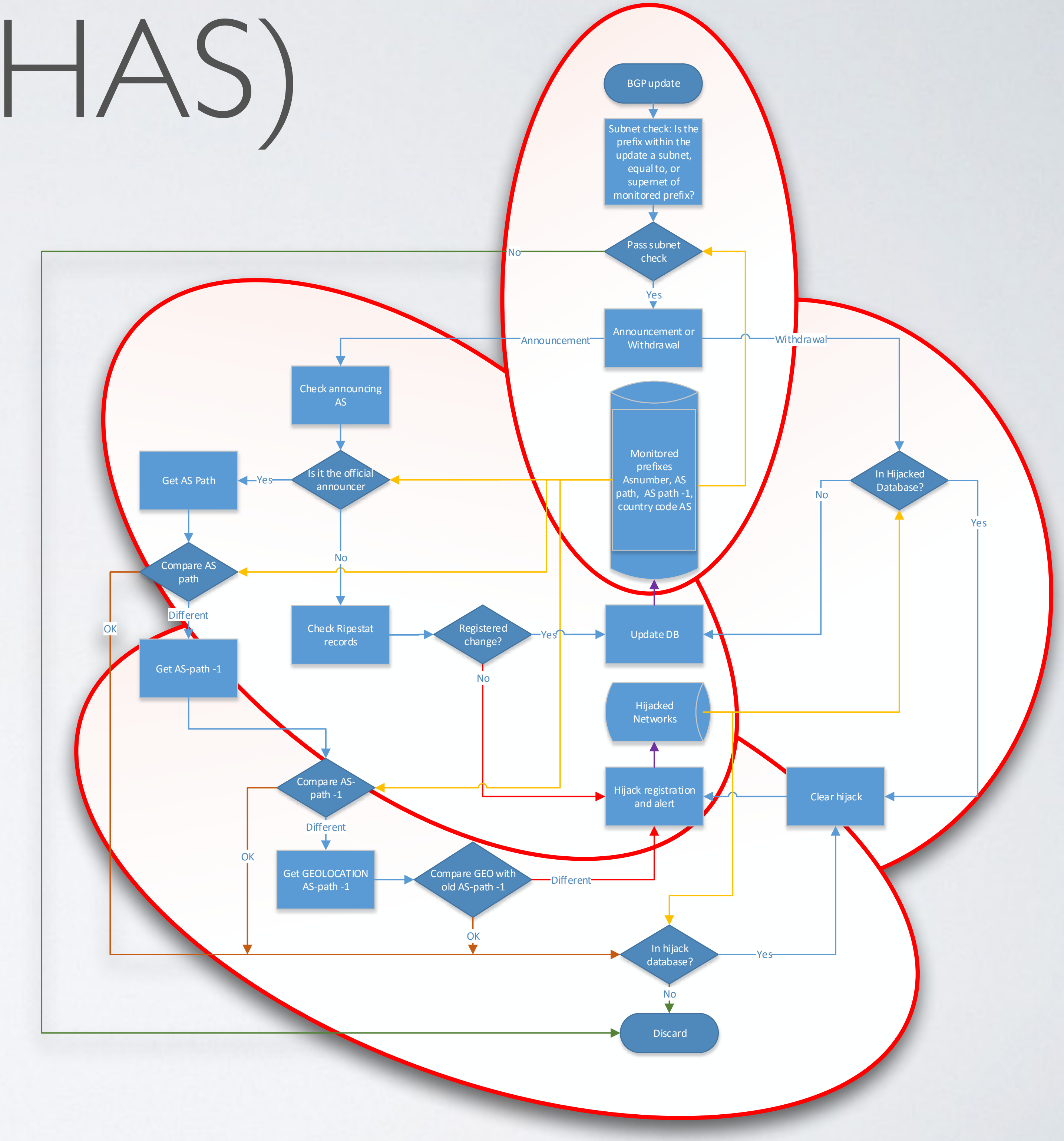
- Limited to online prefixes
- Noise generation
- Lacking Multiple Origin AS (MOAS) Support
- Information disclosure

RESEARCH QUESTION

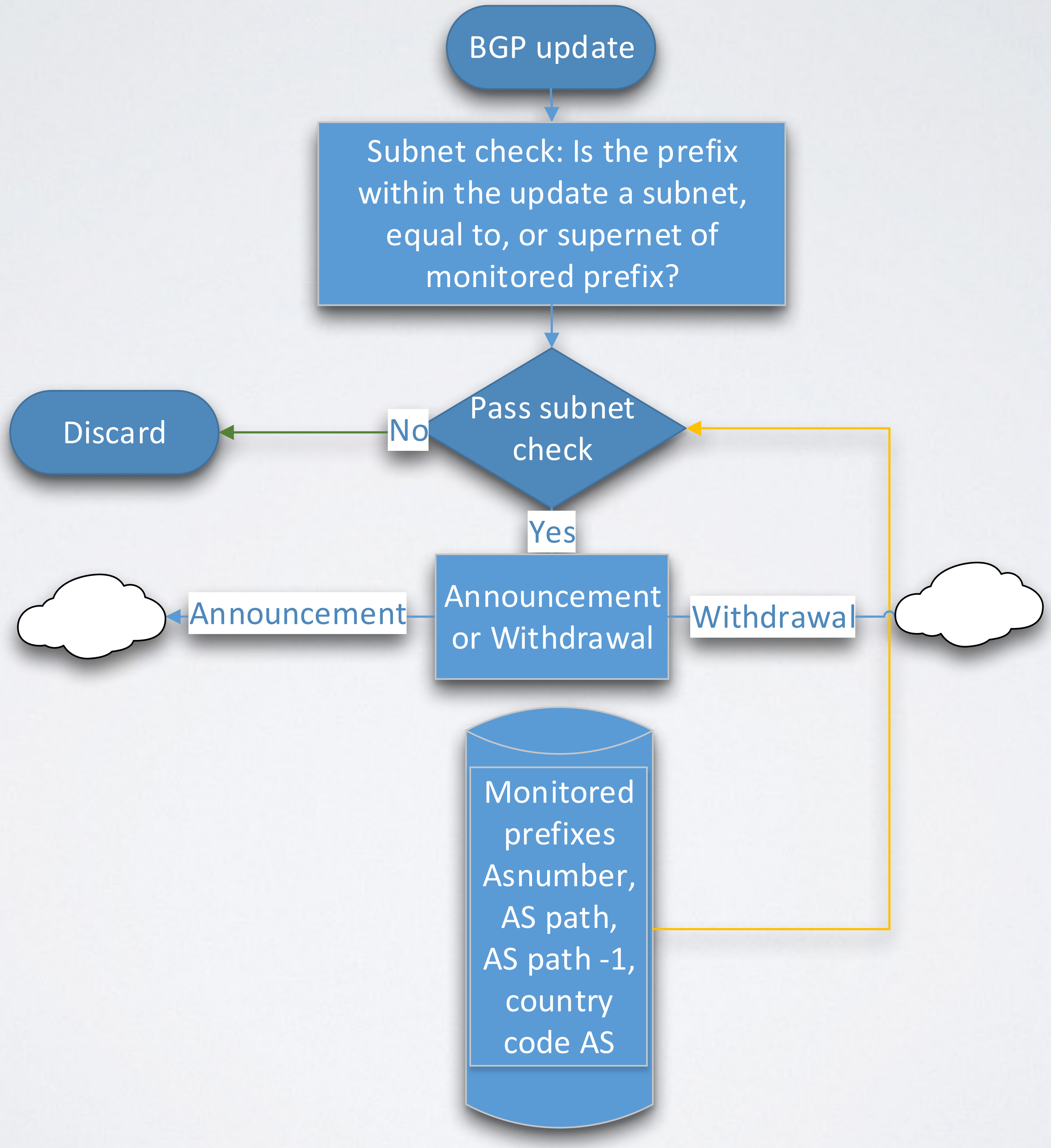
How to create an early detection system for BGP hijacks for a fixed number of IP ranges and AS numbers using public resources?

PROPOSED MODEL (BHAS)

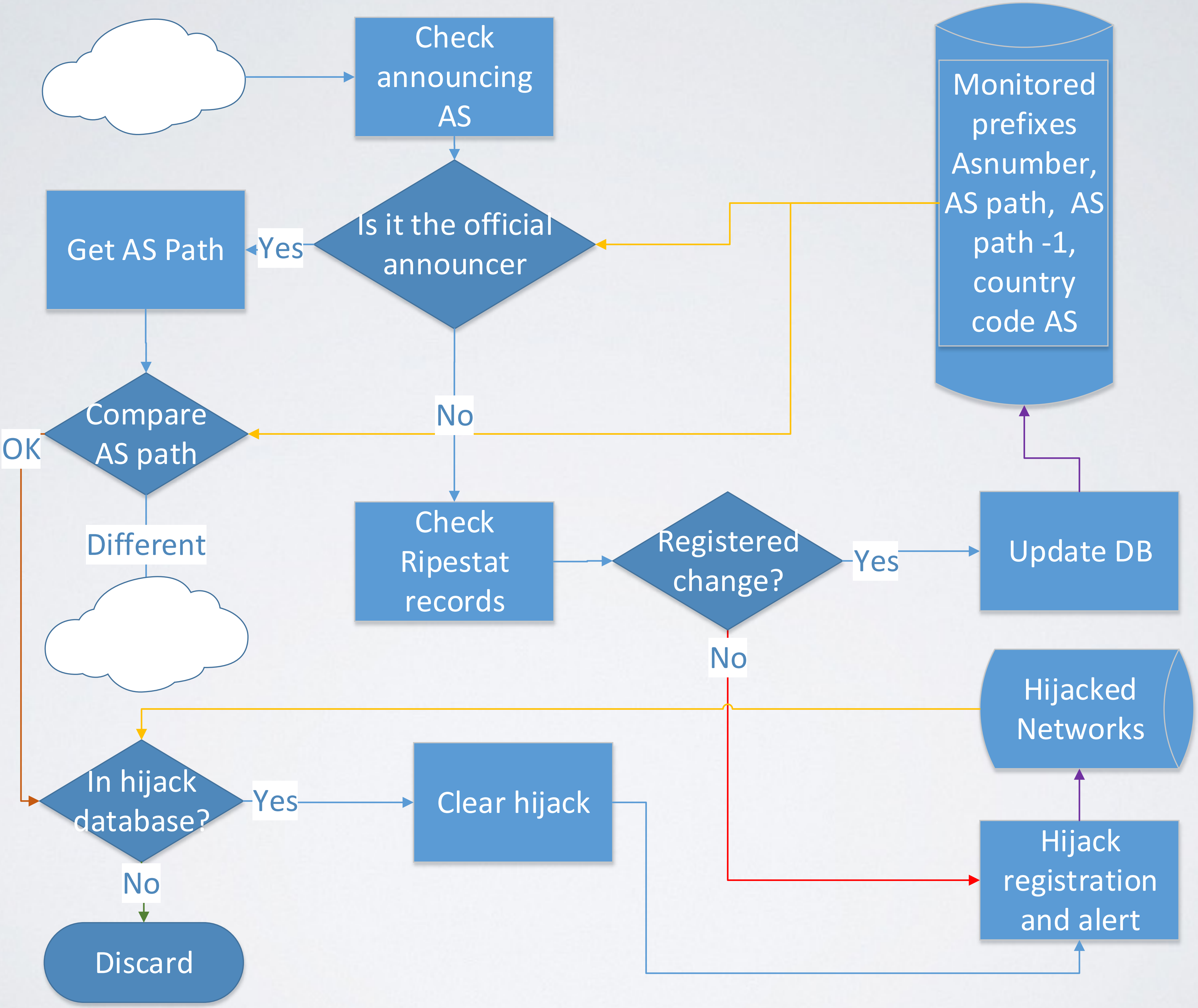
- Requires full BGP feed
- Supports IPv4 and IPv6
- Support MOAS
- Support Multi-homing



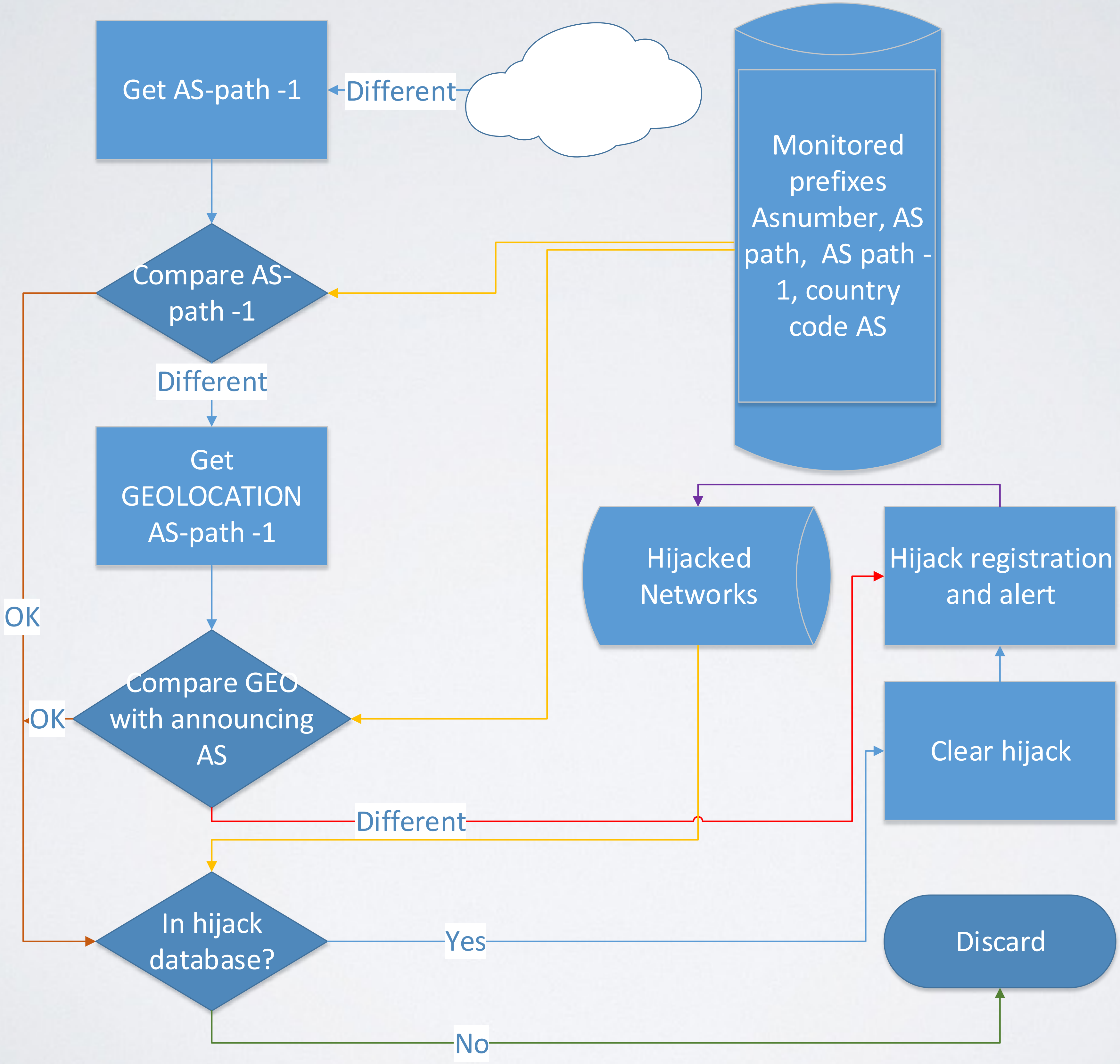
INITIALIZATION


BGP update
Subnet check: Is the prefix within the update a subnet, equal to, or supernet of monitored prefix?
Pass subnet check
No
Discard
Yes
Announcement or Withdrawal
Announcement
Withdrawal
Monitored prefixes Asnumber, AS path, AS path -1, country code AS

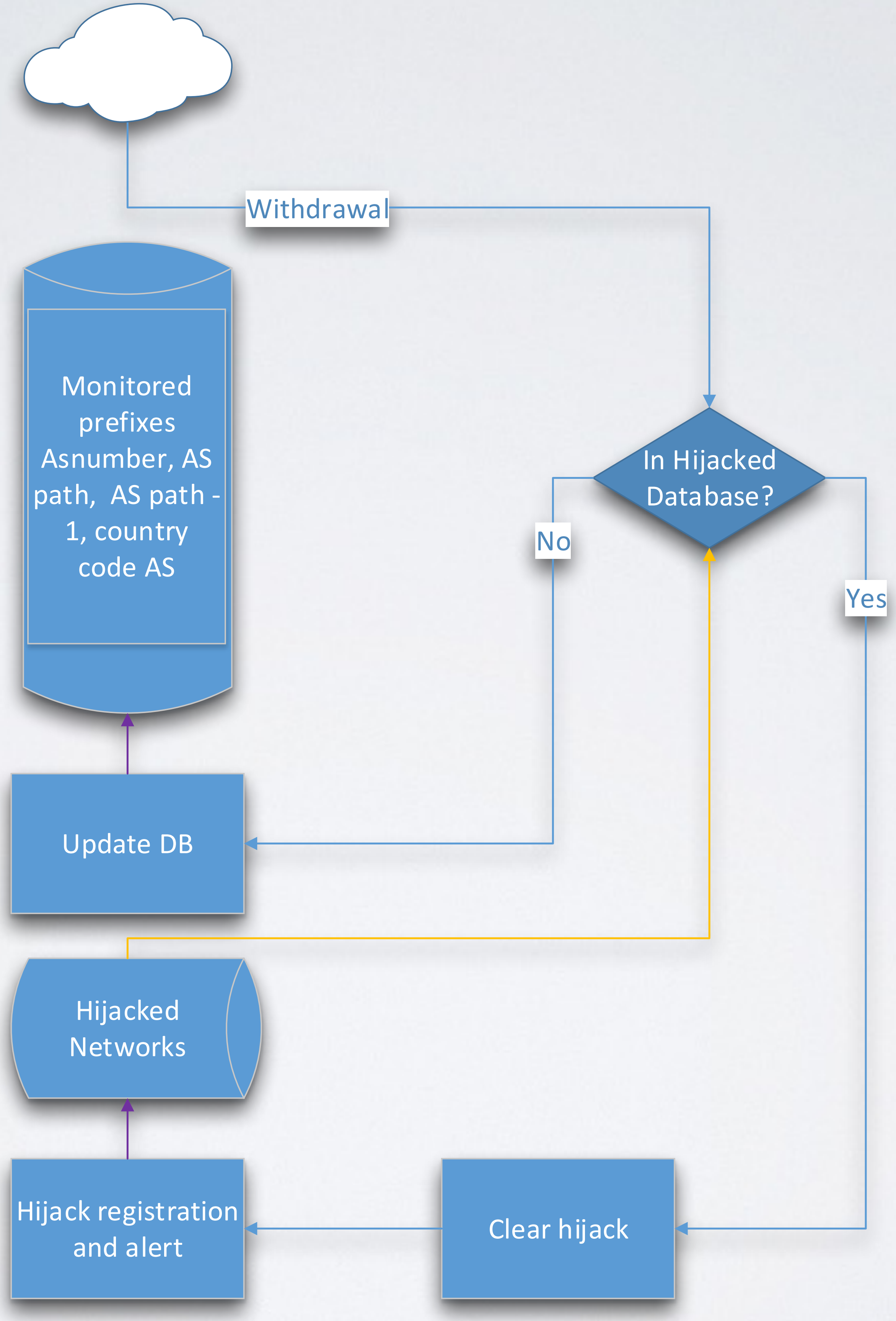
SUBNET, PREFIX AND SUPERNET DETECTION



AS HIJACK DETECTION


Get AS-path -1
Different
Monitored prefixes Asnumber, AS path, AS path -1, country code AS
Compare AS-path -1
Different
Get GEOLOCATION AS-path -1
OK
Hijacked Networks
Hijack registration and alert
Compare GEO with announcing AS
OK
Clear hijack
Different
In hijack database?
Yes
Discard
No

WITHDRAWAL

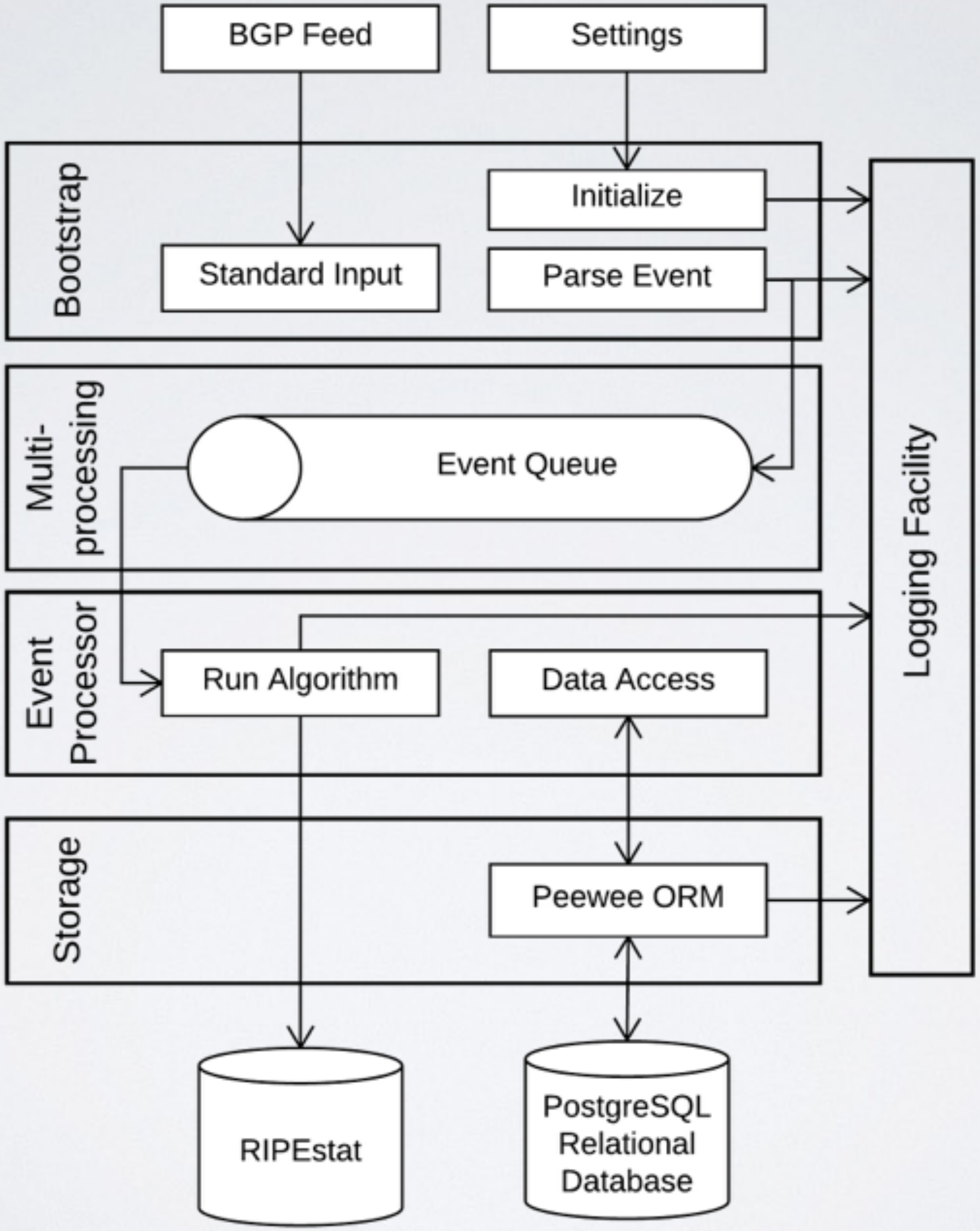

Withdrawal
Monitored prefixes Asnumber, AS path, AS path - 1, country code AS
In Hijacked Database?
No
Yes
Update DB
Hijacked Networks
Hijack registration and alert
Clear hijack

PROOF OF CONCEPT

Build within 2 days
ExaBGP
Python application
Multithreaded
Postgres database
Peewee ORM

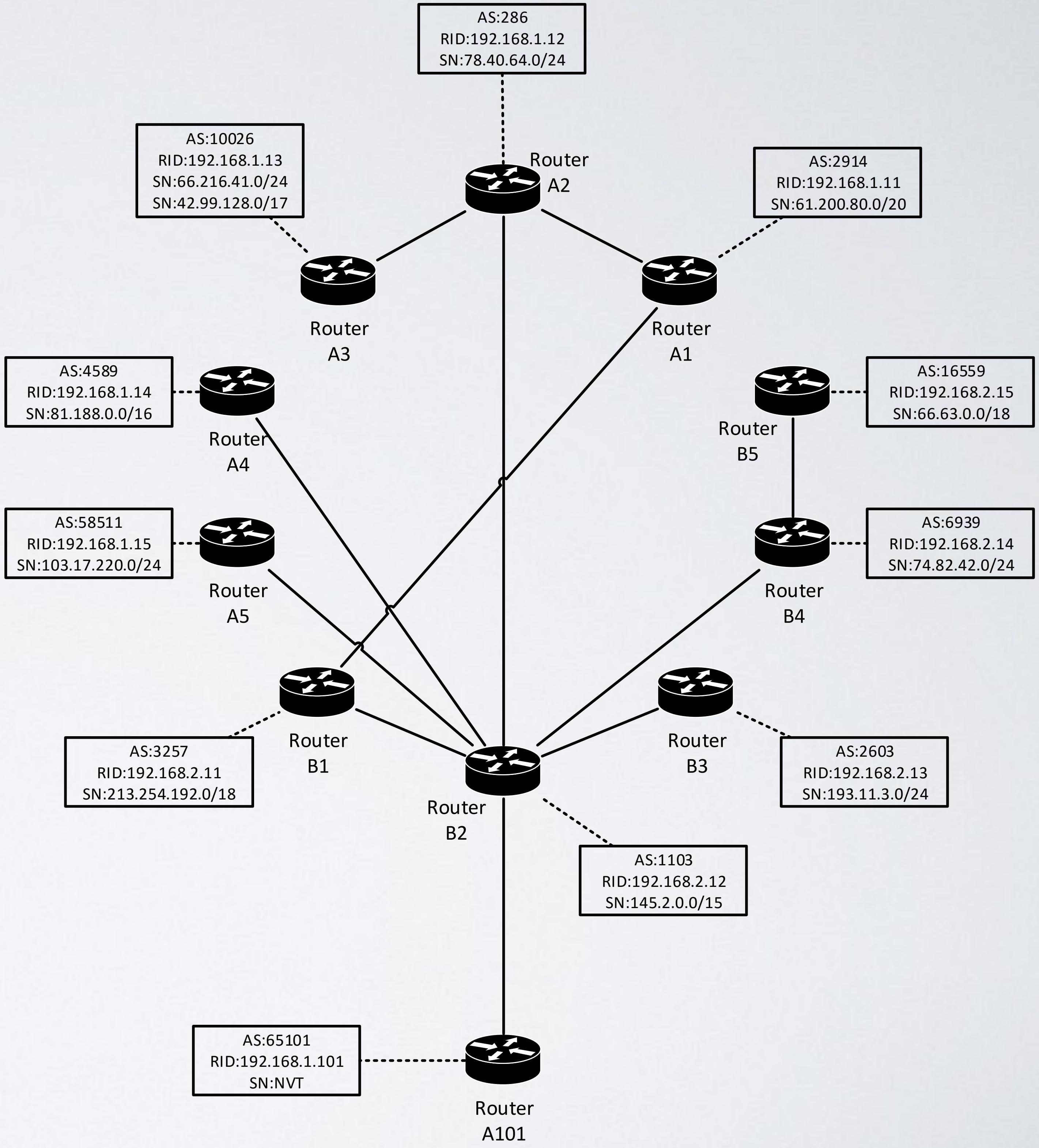
1) https://prince2pm.files.wordpress.com/

ARCHITECTURE



TEST CASES

- All five types of hijacks
- Virtualized environment
- IRR records



AS:286
RID:192.168.1.12
SN:78.40.64.0/24

Router A2

AS:10026
RID:192.168.1.13
SN:66.216.41.0/24
SN:42.99.128.0/17

Router A3

AS:2914
RID:192.168.1.11
SN:61.200.80.0/20

Router A1

AS:4589
RID:192.168.1.14
SN:81.188.0.0/16

Router A4

AS:16559
RID:192.168.2.15
SN:66.63.0.0/18

Router B5

AS:58511
RID:192.168.1.15
SN:103.17.220.0/24

Router A5

AS:6939
RID:192.168.2.14
SN:74.82.42.0/24

Router B4

AS:3257
RID:192.168.2.11
SN:213.254.192.0/18

Router B1

Router B2

Router B3

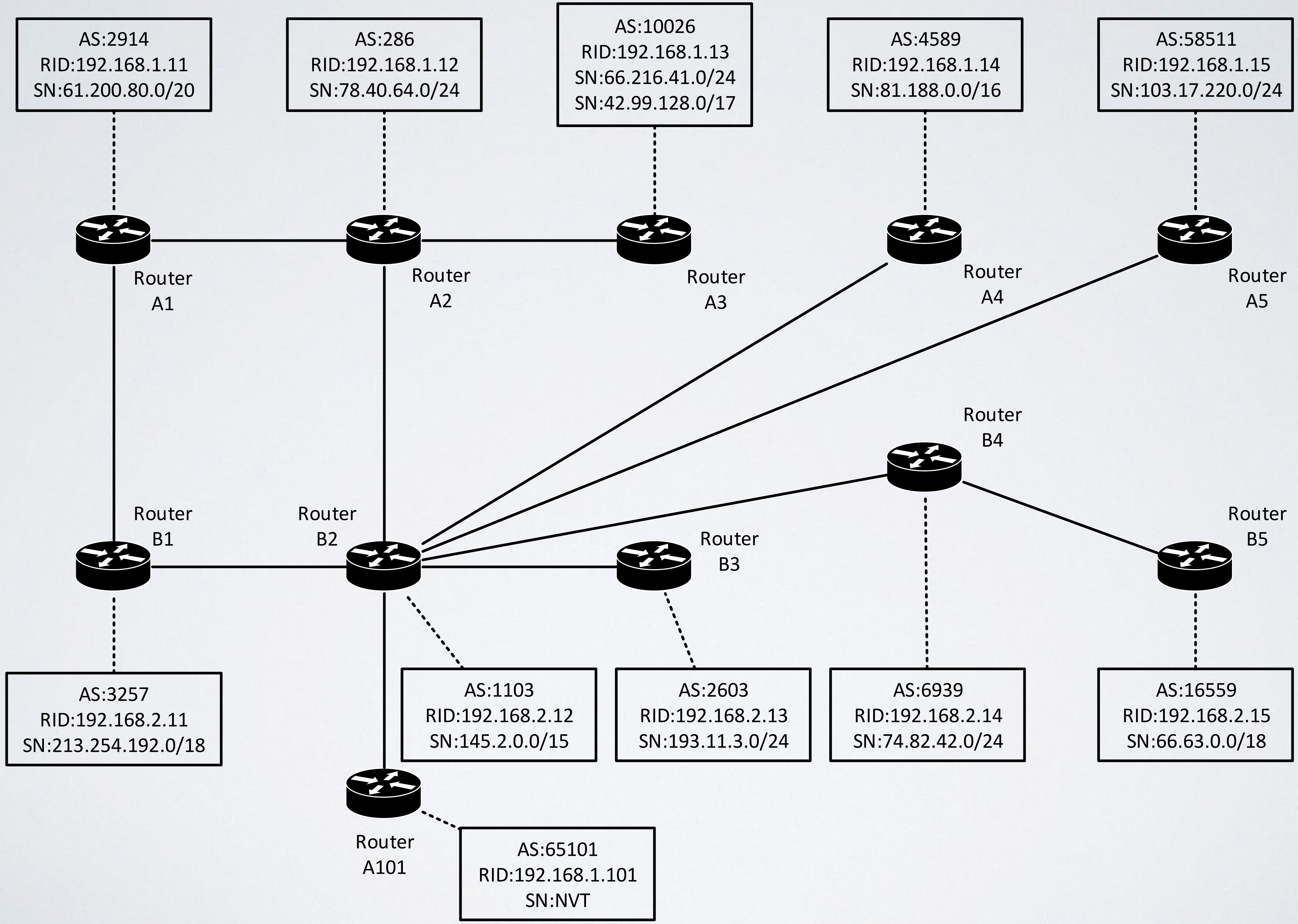
AS:2603
RID:192.168.2.13
SN:193.11.3.0/24

AS:1103
RID:192.168.2.12
SN:145.2.0.0/15

AS:65101
RID:192.168.1.101
SN:NVT

Router A101

TEST ENVIRONMENT



AS:2914
RID:192.168.1.11
SN:61.200.80.0/20

AS:286
RID:192.168.1.12
SN:78.40.64.0/24

AS:10026
RID:192.168.1.13
SN:66.216.41.0/24
SN:42.99.128.0/17

AS:4589
RID:192.168.1.14
SN:81.188.0.0/16

AS:58511
RID:192.168.1.15
SN:103.17.220.0/24

AS:3257
RID:192.168.2.11
SN:213.254.192.0/18

AS:1103
RID:192.168.2.12
SN:145.2.0.0/15

AS:2603
RID:192.168.2.13
SN:193.11.3.0/24

AS:6939
RID:192.168.2.14
SN:74.82.42.0/24

AS:16559
RID:192.168.2.15
SN:66.63.0.0/18

AS:65101
RID:192.168.1.101
SN:NVT

RESULTS - ANALYSIS - CONCLUSION

RESULTS TEST ENVIRONMENT

- All types of BGP hijacks are reported
- Prevents data disclosure to third parties

IRR RECORDS

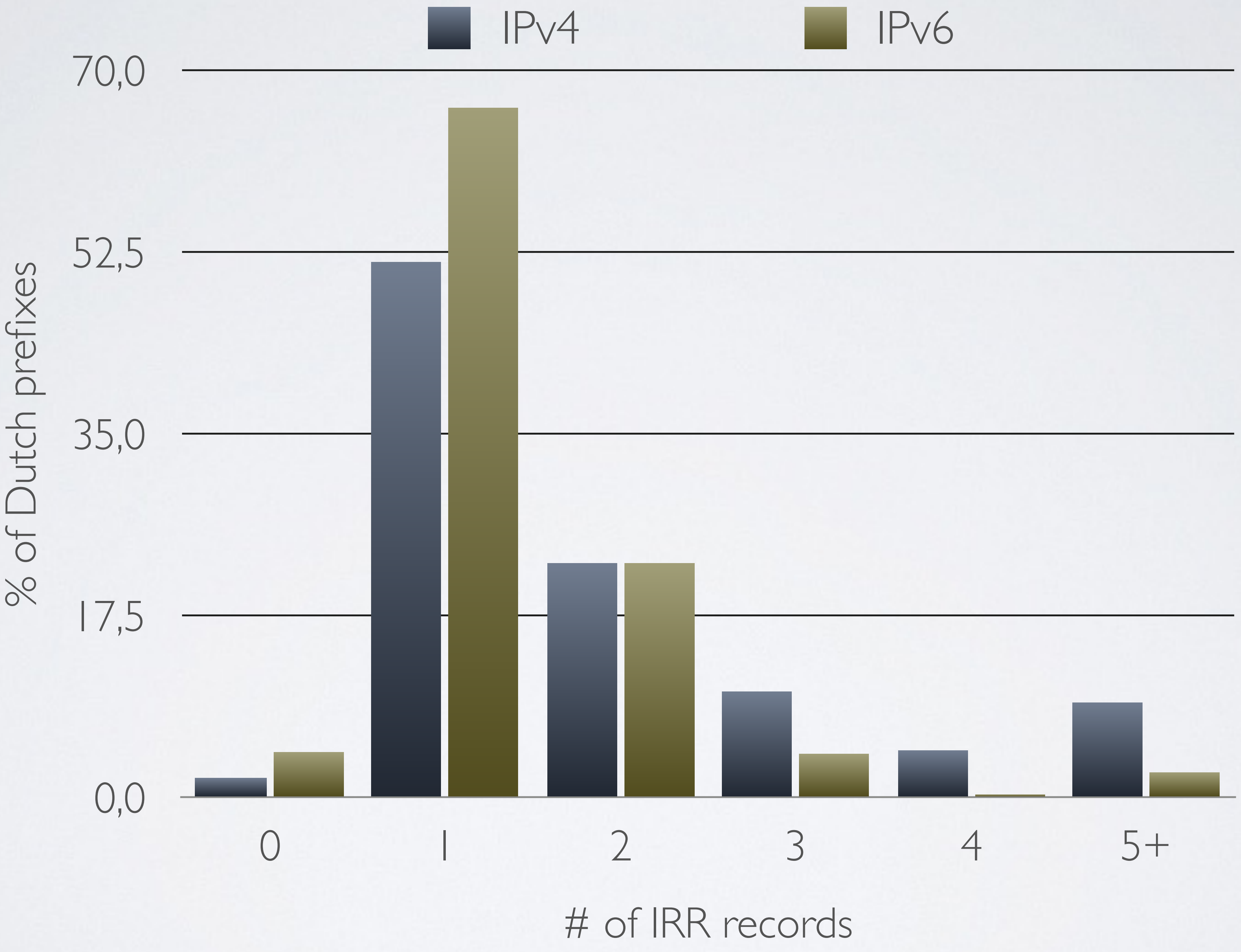
“As it turns out 46% of all the prefixes in the routing table today have a valid route object.”

BGPmon.net (2009)

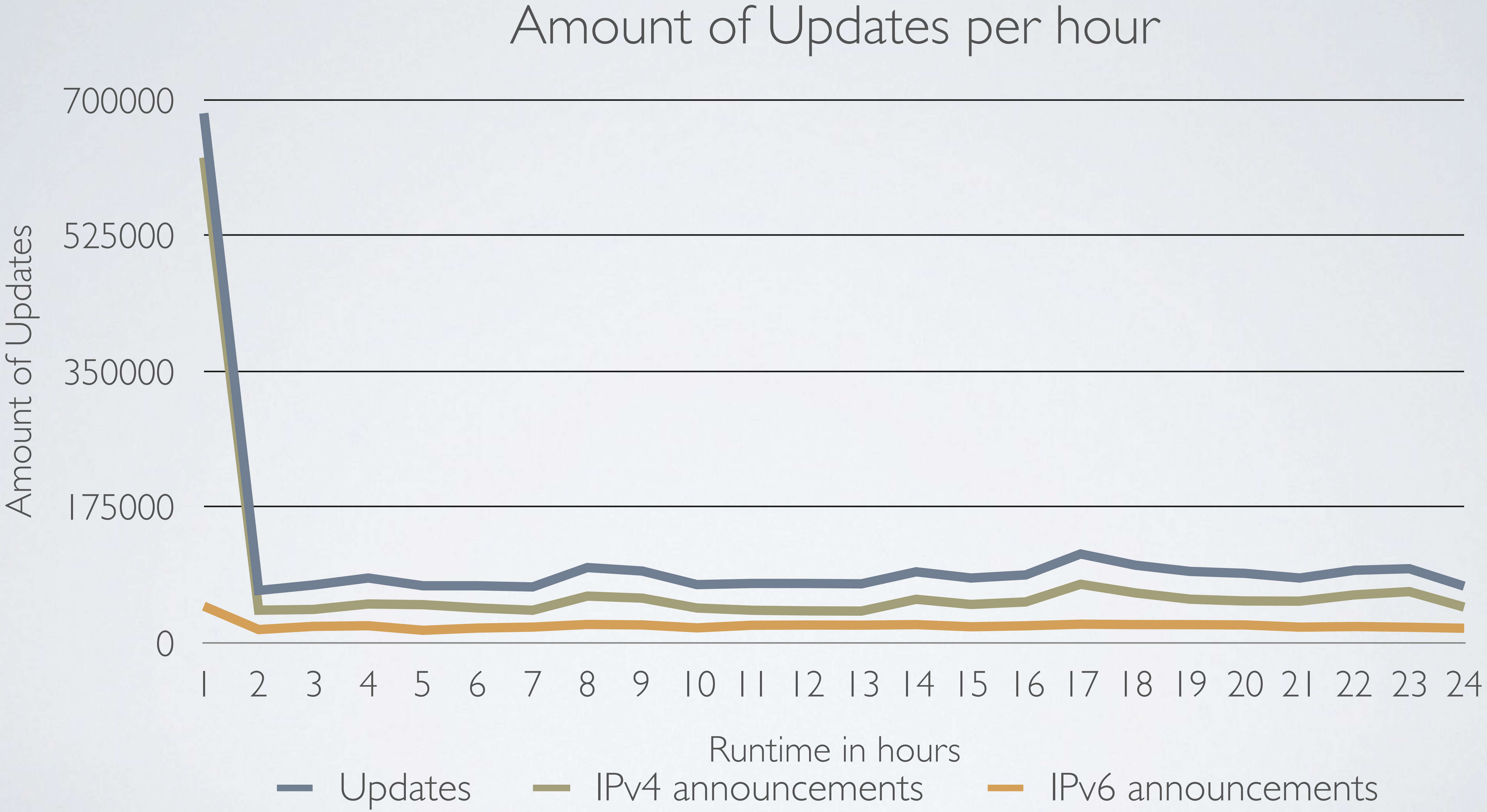
“Russia is way ahead of the others with 88.4% coverage”

research.dyn.com (2009)

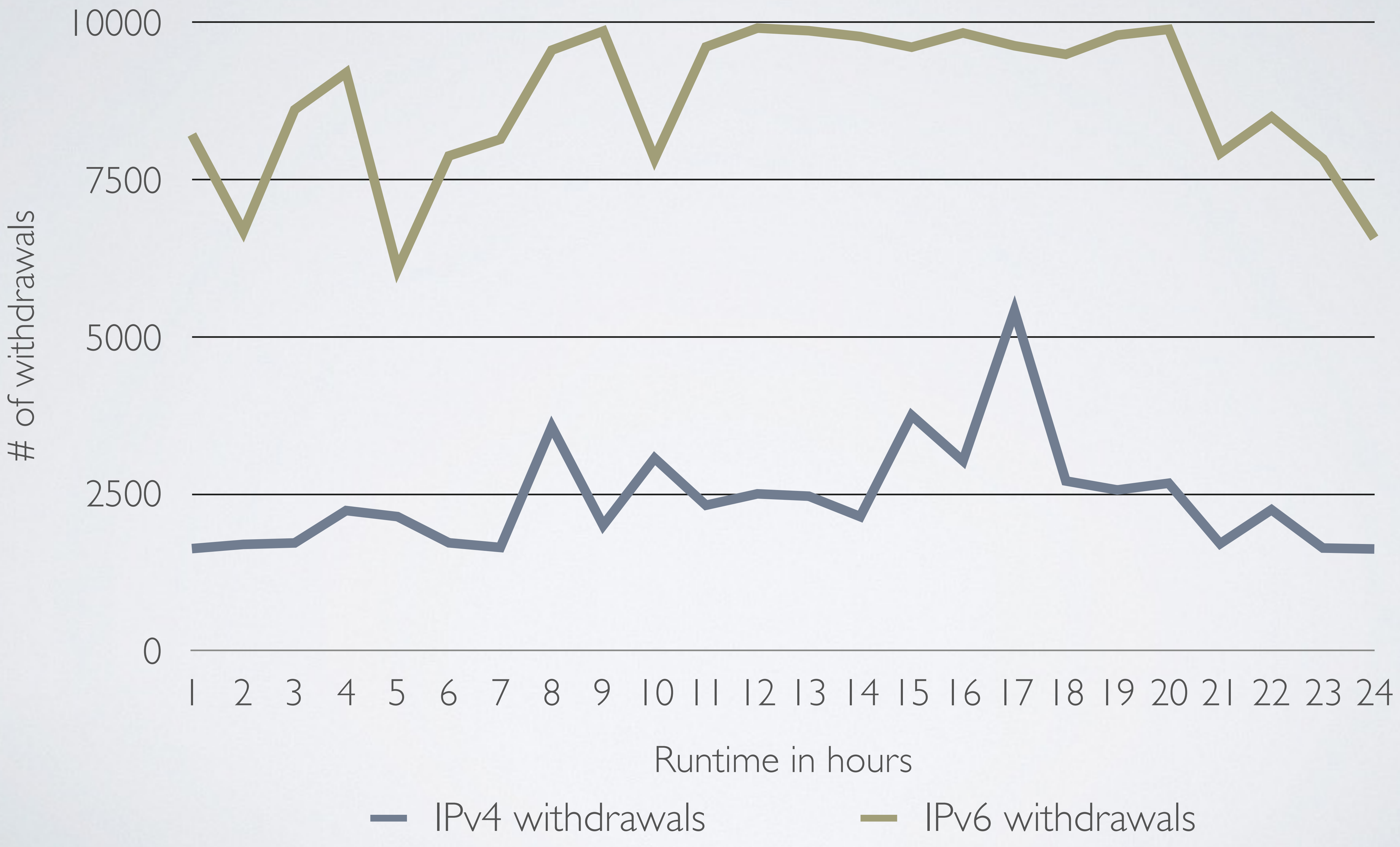
RESULTS - IRR RECORDS



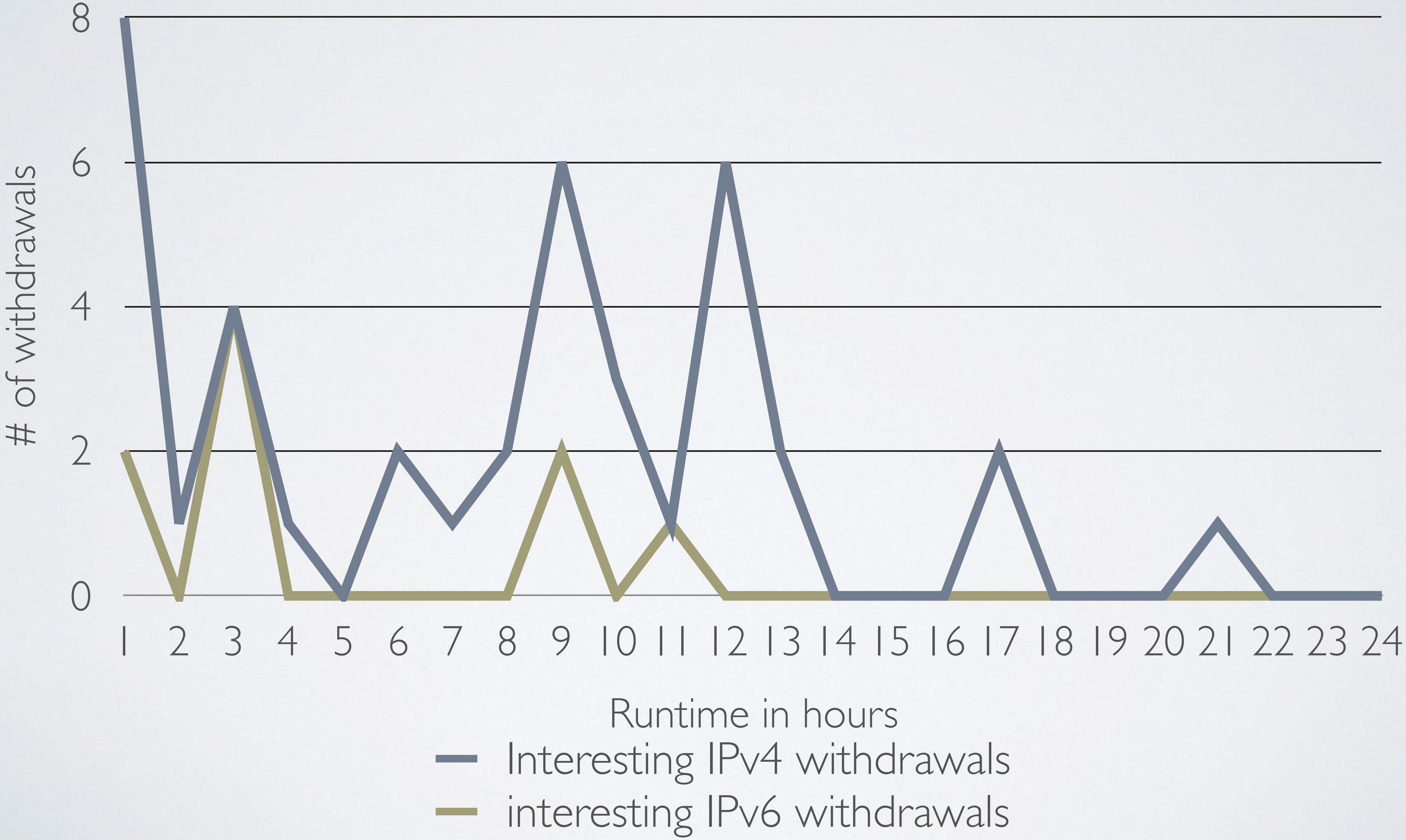
RESULTS - UPDATES



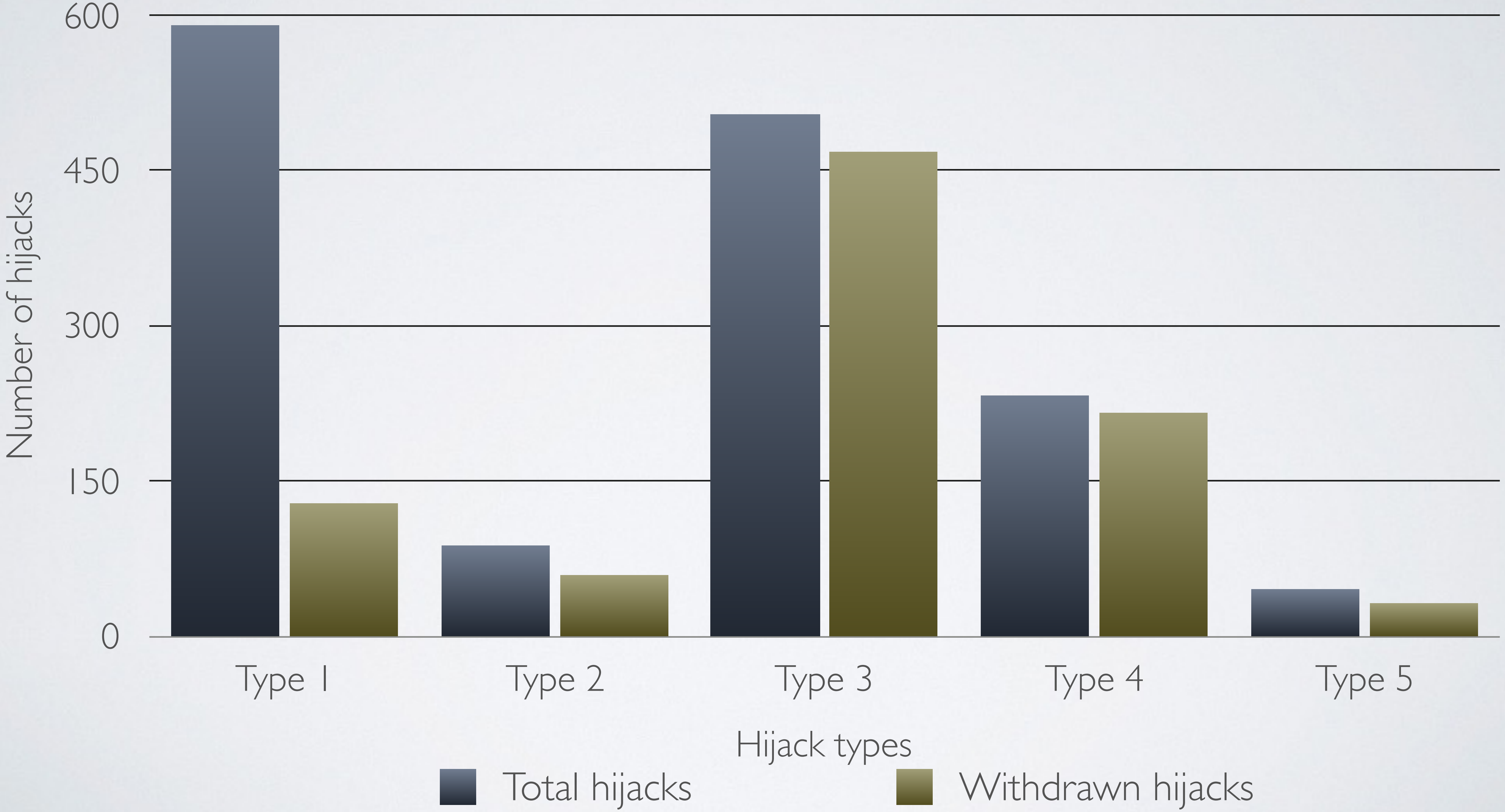
RESULTS - WITHDRAWALS



RESULTS - INTERESTING WITHDRAWALS



RESULTS - HIJACKS



ANALYSIS

Dutch IRR registration coverage better than expected
Algorithm works
Architecture scales
More IPv6 withdrawals
9 hijacks every hour

LIMITATIONS

Model limitations

- Number of BGP feeds
- IRR registration
- Upstream AS geolocation

Future work

- Connect to live BGP feed for further analysis
- Correlate to real BGP hijacks
- Compare to other solutions

CONCLUSIONS

- The proposed model is tested successfully

CONCLUSIONS

- The proposed model is tested successfully
- IPv4 IRR registration coverage is 98% for Dutch ASes
- IPv6 IRR registration coverage is 96% for Dutch ASes

CONCLUSIONS

- The proposed model is tested successfully

- IPv4 IRR registration coverage is 98% for Dutch ASes

- IPv6 IRR registration coverage is 96% for Dutch ASes

- Lower number of MOAS networks for IPv6

CONCLUSIONS

- The proposed model is tested successfully
- IPv4 IRR registration coverage is 98% for Dutch ASes
- IPv6 IRR registration coverage is 96% for Dutch ASes
- Lower number of MOAS networks for IPv6
- Reported hijacks: 1460 out of 10.5 million updates

QUESTIONS