The RPKI and Route Origin Validation:

Advances in Deployment and Measurement

PhD Qualifier Examination – Presentation

John Kristoff

jkrist3@uic.edu

COMPUTER SCIENCE
COLLEGE OF ENGINEERING

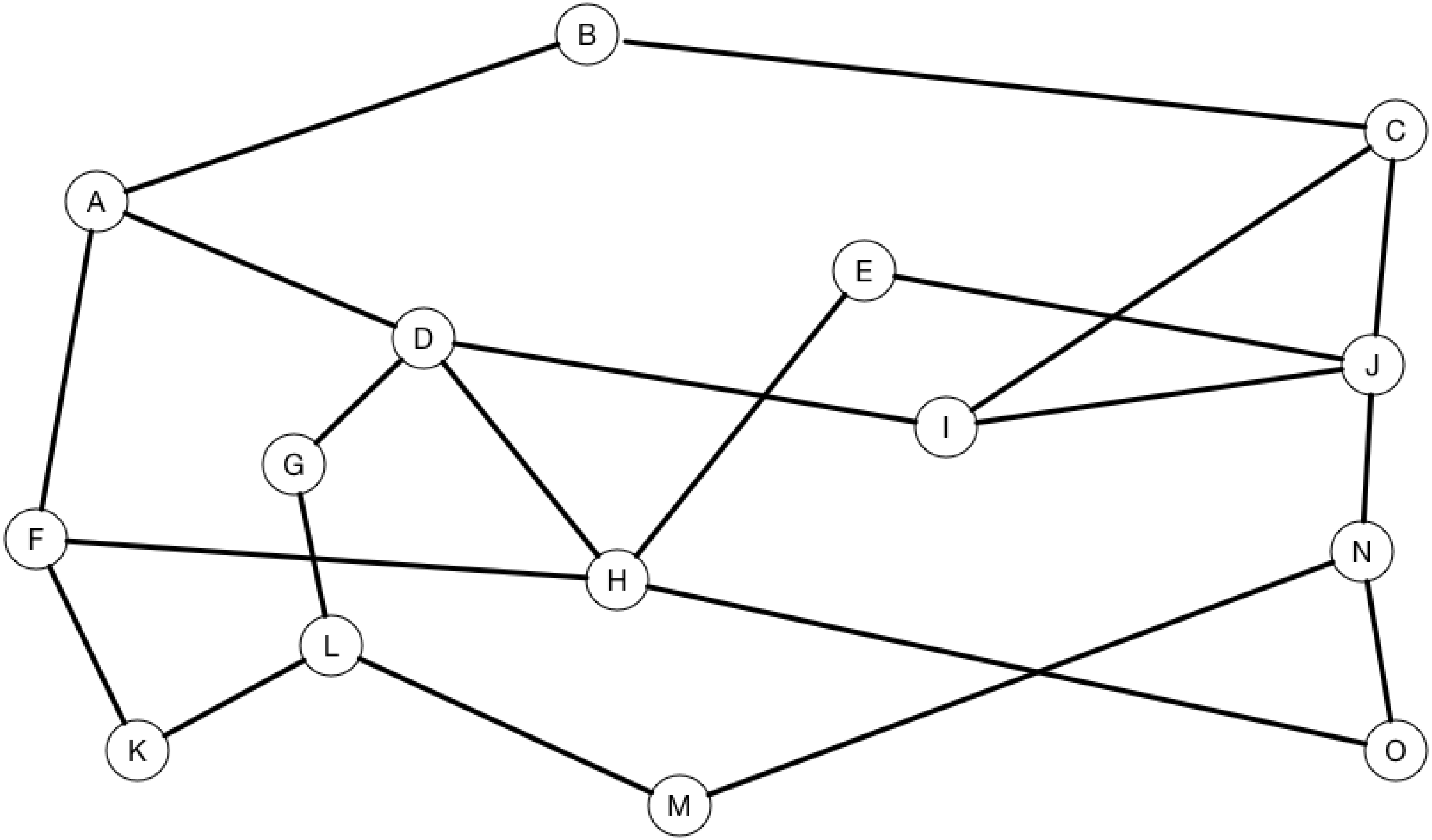
UIC

Outline

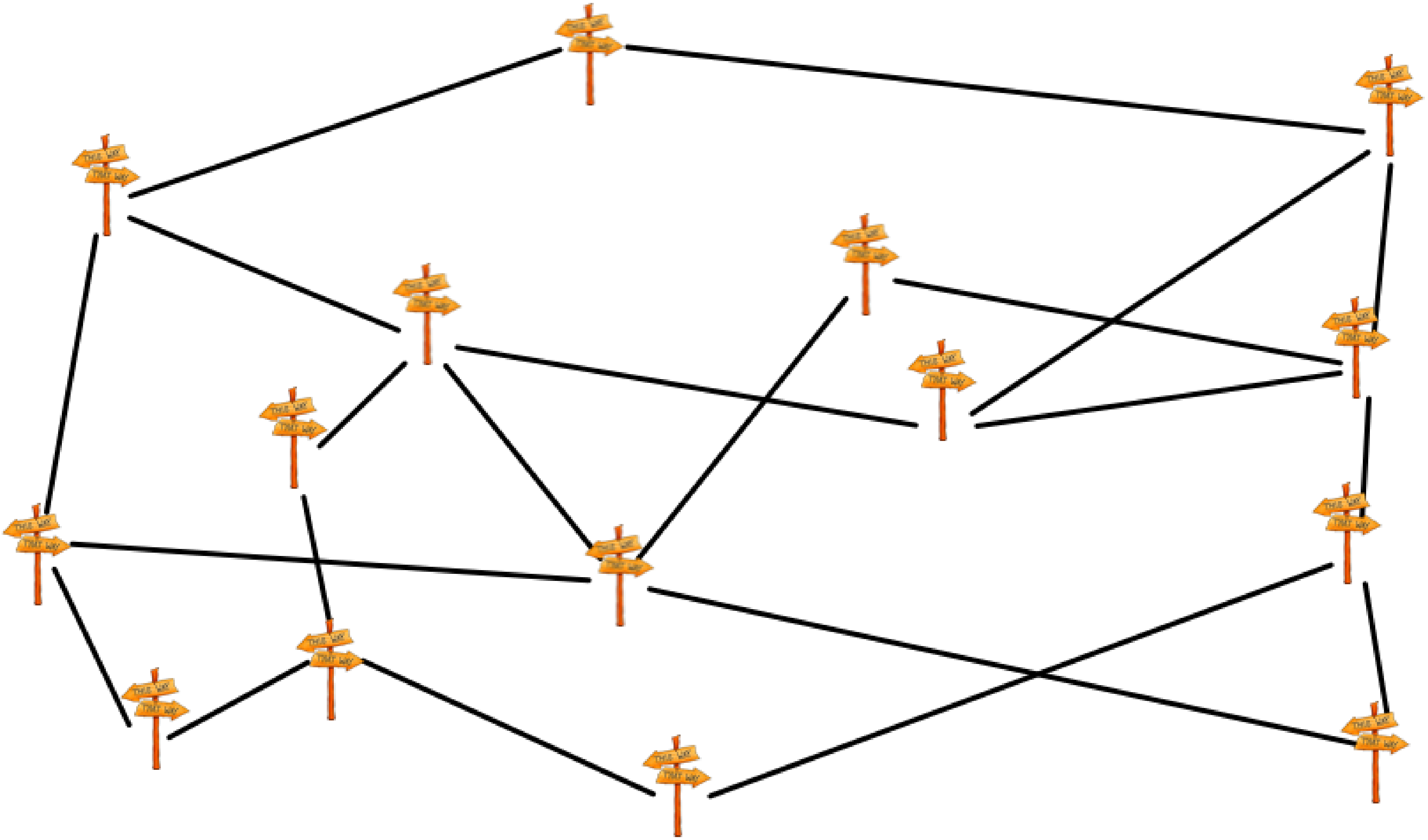
- Introduction
- Background
- Uncontrolled Passive ROV Measurement
- Controlled Active ROV Measurement
- Data Plane Experiments
- Deployment Challenges
- Future Work
- Conclusion

Internet Routing

***adapted from Tannebaum, Computer Networks, Fig. 5-5(a)**



Destination-directed



Most Specific Wins

- How much does this computer cost?
  - It is not free
  - Somewhere between $1500 and $2000
  - With tax, $1768.59
- Who can get me to 192.0.2.1?
  - If you don’t hear from anyone, I’ll take you
  - That is not far from where I’m going, jump in
  - Hey, that is me! This way...

Infamous Route Hijackings

- “AS 7007 Incident”
- Pakistan Telecom censorship and YouTube
- Crypto-currency theft

Outline

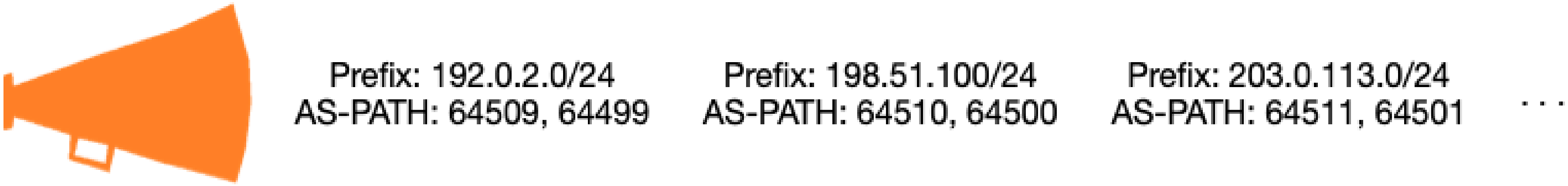
- Introduction
- Background
- Uncontrolled Passive ROV Measurement
- Controlled Active ROV Measurement
- Data Plane Experiments
- Deployment Challenges
- Future Work
- Conclusion

Background

- Route Filters and Max Limits
- Internet Routing Registry
- S-BGP and soBGP

- The RPKI
- ROAs
- ROV

Route filters and Max Limits



Prefix: 192.0.2.0/24
AS-PATH: 64509, 64499

Prefix: 198.51.100/24
AS-PATH: 64510, 64500

Prefix: 203.0.113.0/24
AS-PATH: 64511, 64501

. . .

```
prefix-limit {
    maximum 10000;
}
...
policy-statement sanitize-bgp {
    term rfc1918 {
        from {
            prefix-list-filter rfc1918 orlonger;
        }
        then reject;
    }
```

Internet Routing Registry (IRR)

- Routing policy database(s)
- Intended to help automation and troubleshooting
- Of varying completeness and quality

```
route:          140.192.0.0/16
descr:          DePaul University
descr:          1 E Jackson
descr:          Chicago, IL 60604
origin:         AS20130
member-of:      RS-DEPAUL
```

S-BGP and soBGP

- Modifications or extensions to BGP
- Addition of PKI to authenticate routing data
- Neither system deployed
- Both influenced what was to come

The Resource Public Key Infrastructure (RPKI)

- Specifications published in 2012
- Distributed, hierarchical PKI for routing objects
- Regional Internet Registries (RIRs) as anchors
- Actively being deployed

Route Origin Authorization (ROA)

```
ROA Name: DEPAUL AS20130
Origin AS: 20130
Validity Period: 02-12-2019 to 02-12-2029
Resources:
    2604:95C0::/32
    2620:0:2250::/48
    75.102.192.0/18
    216.220.176.0/20
```

```
-----BEGIN SIGNATURE-----
CphdY76ofLDDsBzKseuivh9fp8j8f95xZSQrs75MF+GU0nP5OKKtnJ6UvFLZH6L8YEWcxiGGuwTzg
K0Puea+slXnXU+UgalmitqJOHwXbobAm7DCWou2wT2fIWqZHTUpX99/jFlSn34ozp2NFWJCT8ba4W
lNgnIsevnaeoe2KzEUbaawYCOskLU9B7aAPFhBHbuGGhQYpx08n3zLYj1RMIOyOyl8NuSi3cfI0Kb
RZjhtIF3Pe9LebuqrwiBhRaFxzvFLM4g6zDff62/7Hnmt6PFio0Rn1UWPq2plDymT5peluCdDiL3M
/DsGrEgqRfwQKqll6HuRKaZVoHa0cNWPdw==
-----END SIGNATURE-----
```

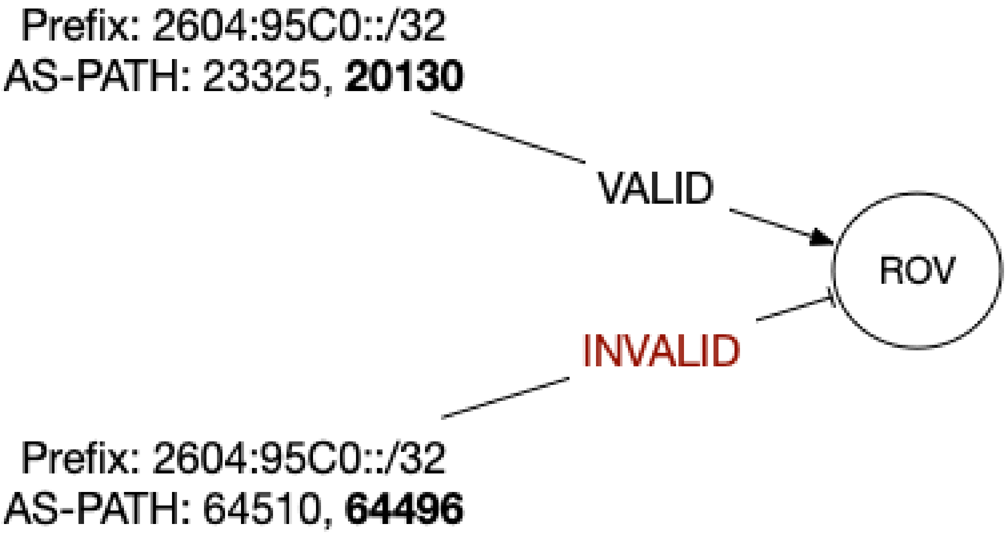
Route Origin Validation (ROV)

ROA Name: DEPAUL AS20130

Origin AS: 20130

Validity Period: 02-12-2019 to 02-12-2029

Resources: 2604:95C0::/32, ...



RPKI + ROAs → ROV

- RPKI = **repository**
- ROAs = **signed objects**
- ROV = secure routing?

- NOTE:
  - ROV only validates “origin” and “prefix”
  - AS-PATHS not protected by ROV
  - ROV is most effective at mitigating accidents

Secure Routing Summary

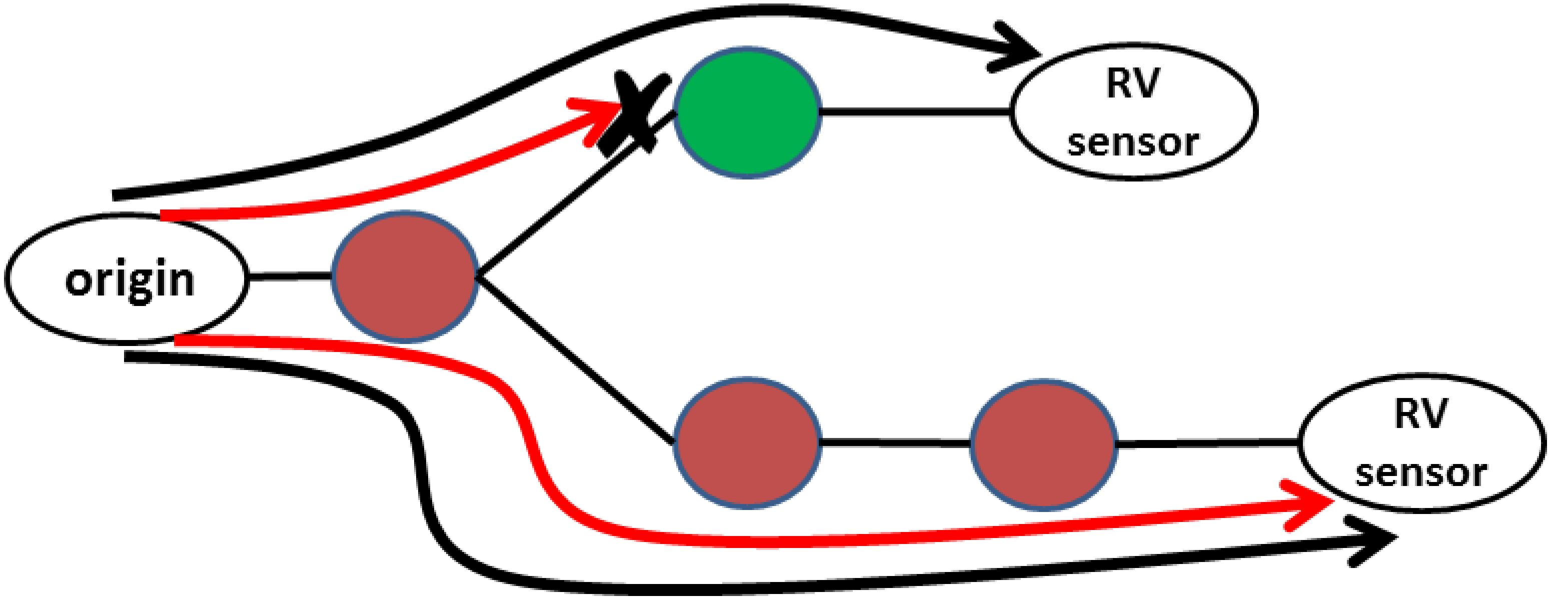
	Utility	Consistency	Ease of Use	Cost
Route Filters	Medium	Low	Medium	Low
Max Limits	Low	Low	High	Low
IRRs	Medium	Low-Medium	Low	Medium
S-BGP / soBGP	High	High	N/A	High
RPKI/ROAs/ROV	**Medium**	**High**	**Medium**	**Medium**

Outline

- Introduction
- Background
- Uncontrolled Passive ROV Measurement
- Controlled Active ROV Measurement
- Data Plane Experiments
- Deployment Challenges
- Future Work
- Conclusion

Uncontrolled Passive ROV

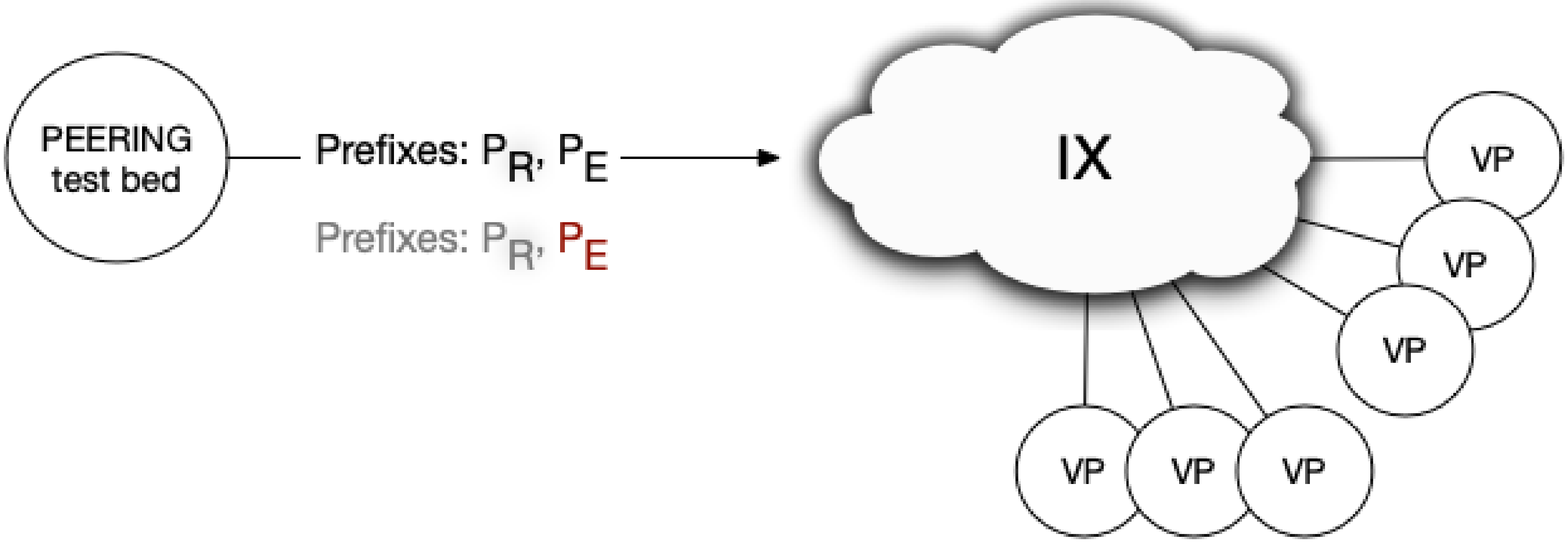
image credit: Gilad, et. Al, “Are We There Yet? On RPKI’s Deployment and Security”



Evaluation: Uncontrolled Passive

- Local AS BGP policies not considered
- An AS originating both invalid/valid should be rare
- Results could not be reproduced

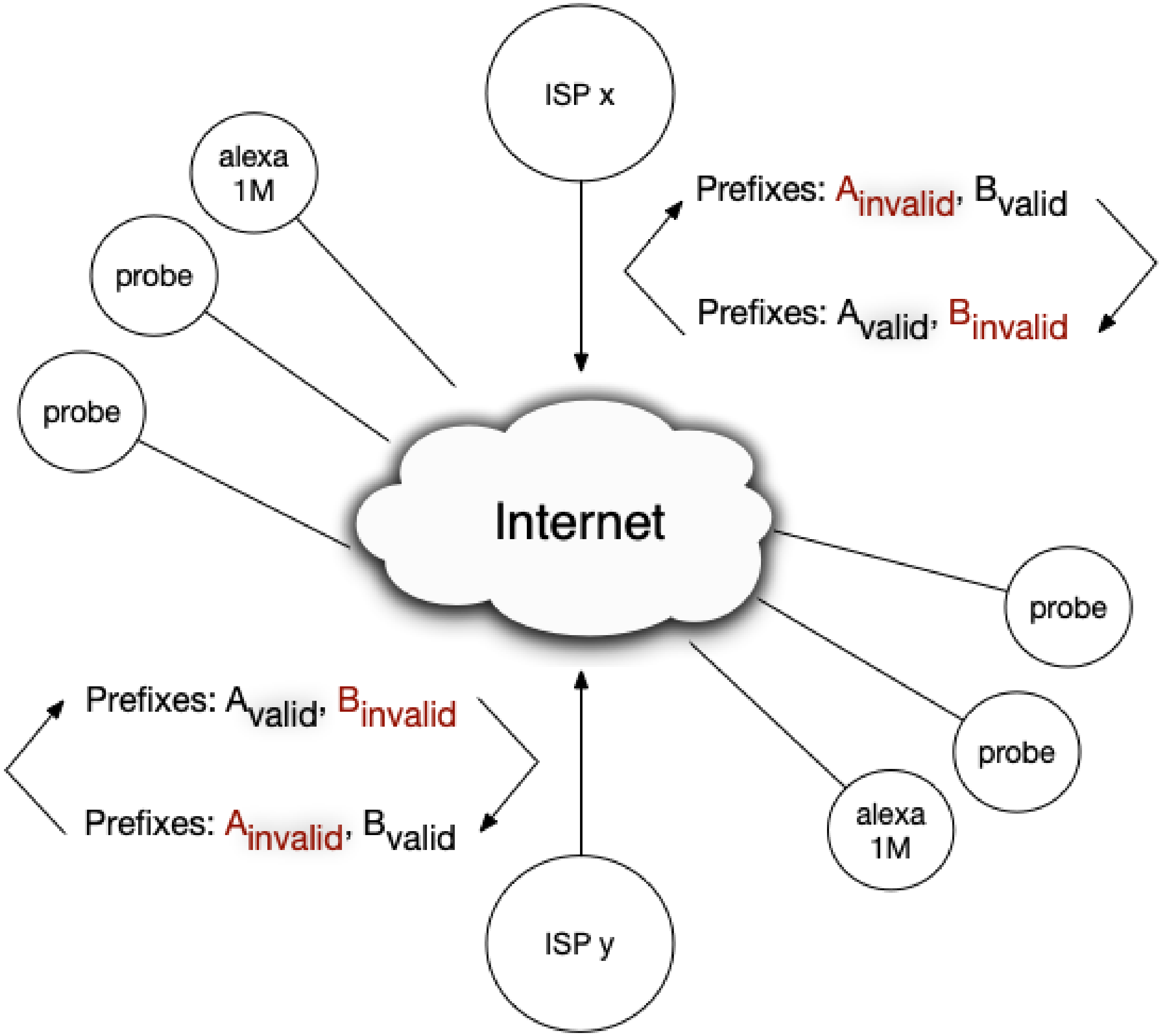
Controlled Active ROV



Evaluation

- Significantly improves ROV detection reliability
- Coverage limited to test bed connectivity
- Passive uncontrolled approach over counts ROV

Data Plane Experiments


ISP x
alexa 1M
probe
probe
Prefixes: $A_{invalid}$, B_{valid}
Prefixes: A_{valid}, $B_{invalid}$
Internet
probe
probe
alexa 1M
Prefixes: A_{valid}, $B_{invalid}$
Prefixes: $A_{invalid}$, B_{valid}
ISP y

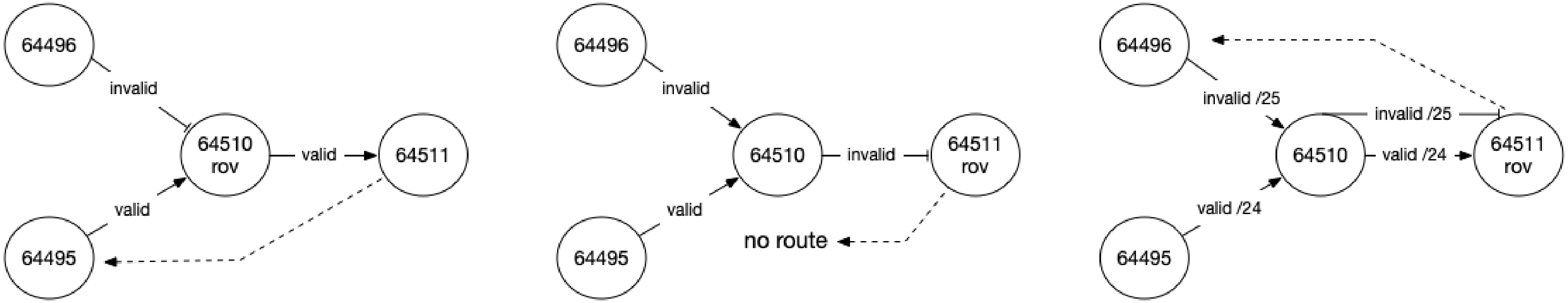
Evaluation

- Local AS policy can mask ROV enforcement
- Traceroute-driven results are unpredictable
- Alexa 1M sites may be distributed (e.g. CDN)

Deployment Challenges

- Limited incentives for early adopters
- Hesitation due to high number of invalid routes
- Sub-allocations may invalidate routes
- Utility limited to preventing “accidents”
- Unexpected partitioning or traffic forwarding*
- Loose versus strict ROAs
- Political, social, and economic limitations

Partial ROV Adoption Scenarios



(a) Benefit

(b) Disconnection

(c) Hijack

Future Work

- New optional, non-transitive validity attribute
- BMP extension for validity state

Conclusion

- The RPKI, ROAs, and ROV active area of work
- Local, hidden BGP policies pose challenges
- Active, controlled experiments with neighbor networks produce the most reliable results

Primary Comparative Sources

- Gilad, Y, Cohen A, Herzberg A, Schapira M, Shulman H. **Are We There Yet? On RPKI's Deployment and Security**. Network and Distributed Security Symposium (NDSS) 2017.
- Reuter A, Bush R, Cunha I, Katz-Bassett E, Schmidt T, Wählisch M. **Towards a Rigorous Methodology for Measuring Adoption of RPKI Route Validation and Filtering**. ACM SIGCOMM Computer Communication Review 48, no. 1, pp. 19-27, 2018.
- Hlavacek T, Herzberg A, Shulman H, Waidner M. **Practical Experience: Methodologies for Measuring Route Origin Validation**. 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2018.

Thank You!

Paper, slide deck, and references archived at:

https://github.com/jtkristoff/wcp