BGP Routing Security and Deployment Strategies

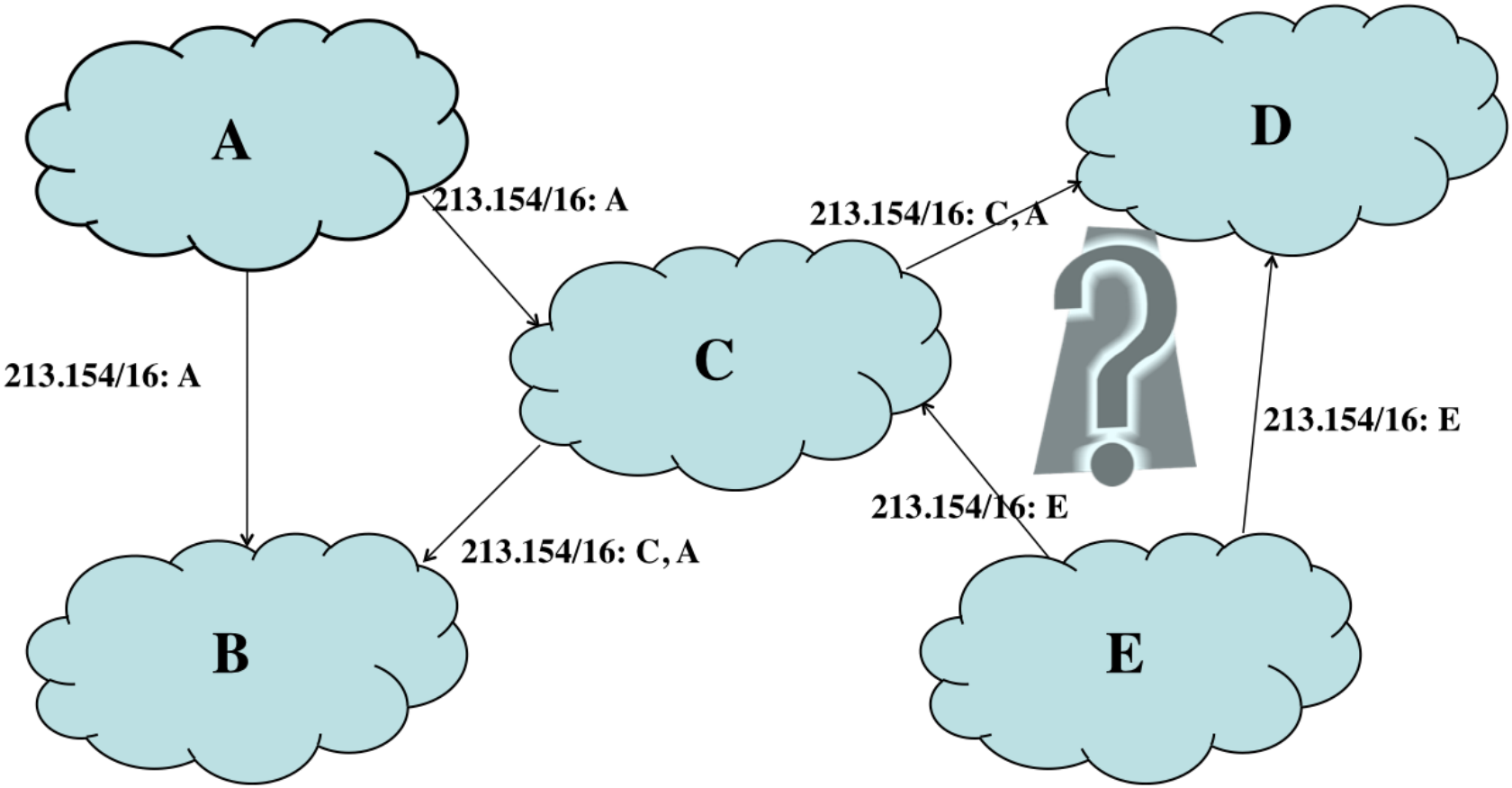
Bryan Eikema

Supervisors: Stavros Konstantaras & Benno Overeinder (NLnet Labs)

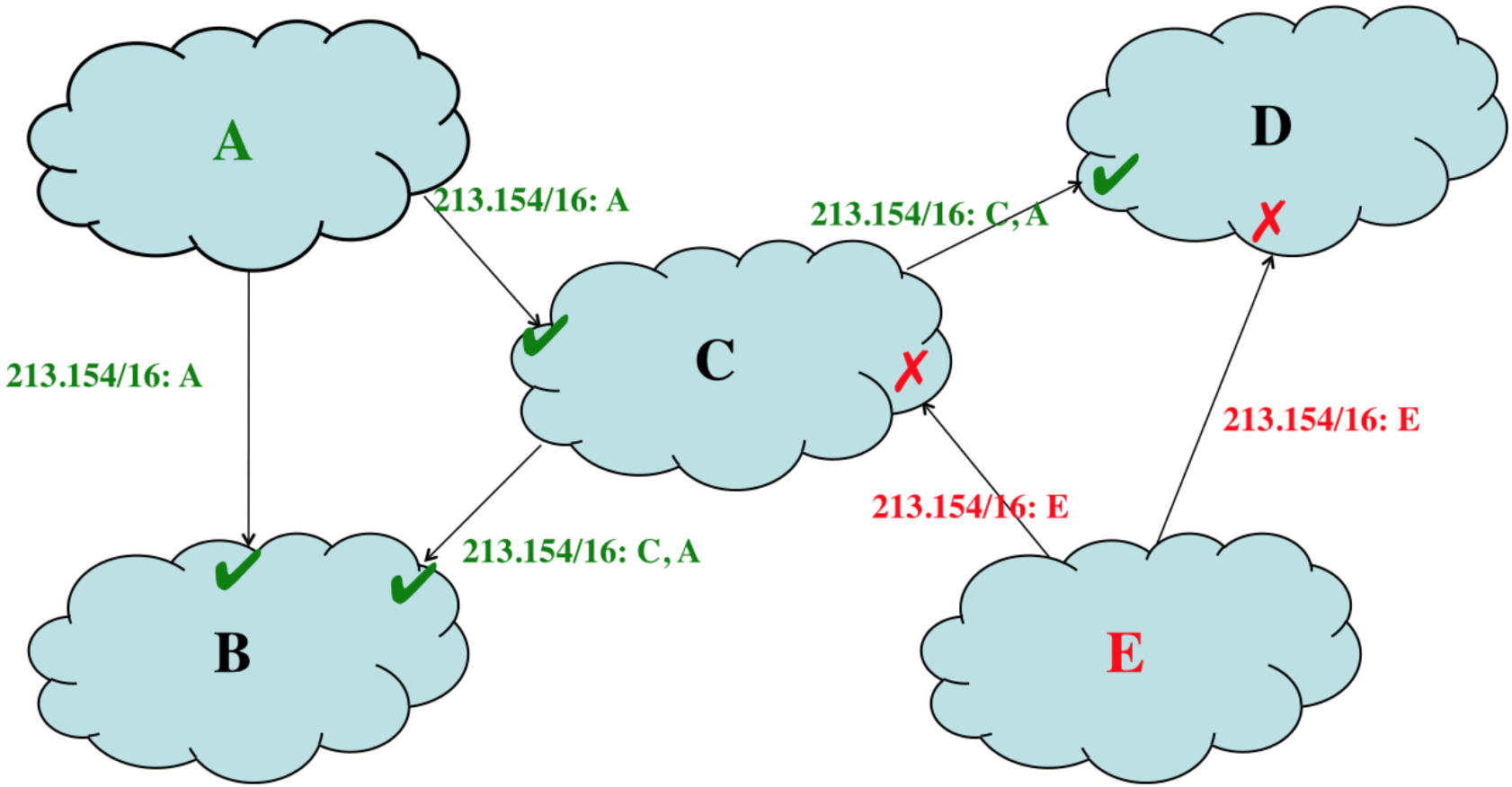
BGP Incidents

- April 1997: The "AS 7007 incident”
- May 2003: Northrop Grumman hit by spammers
- May 2004: Malaysian ISP blocks Yahoo Santa Clara data center
- December 2004: TTNet in Turkey hijacks the Internet (Christmas Turkey hijack)
- January 2006: Con-Edison hijacks a chunk of the Internet
- February 2008: Pakistan’s attempt to block YouTube access within their country takes down YouTube globally
- August 2008: Kapela & Pilosov showed effective man-in-the-middle attack
- April 2010: “China Hijacks 15% of the Internet”

Border Gateway Protocol (BGP)



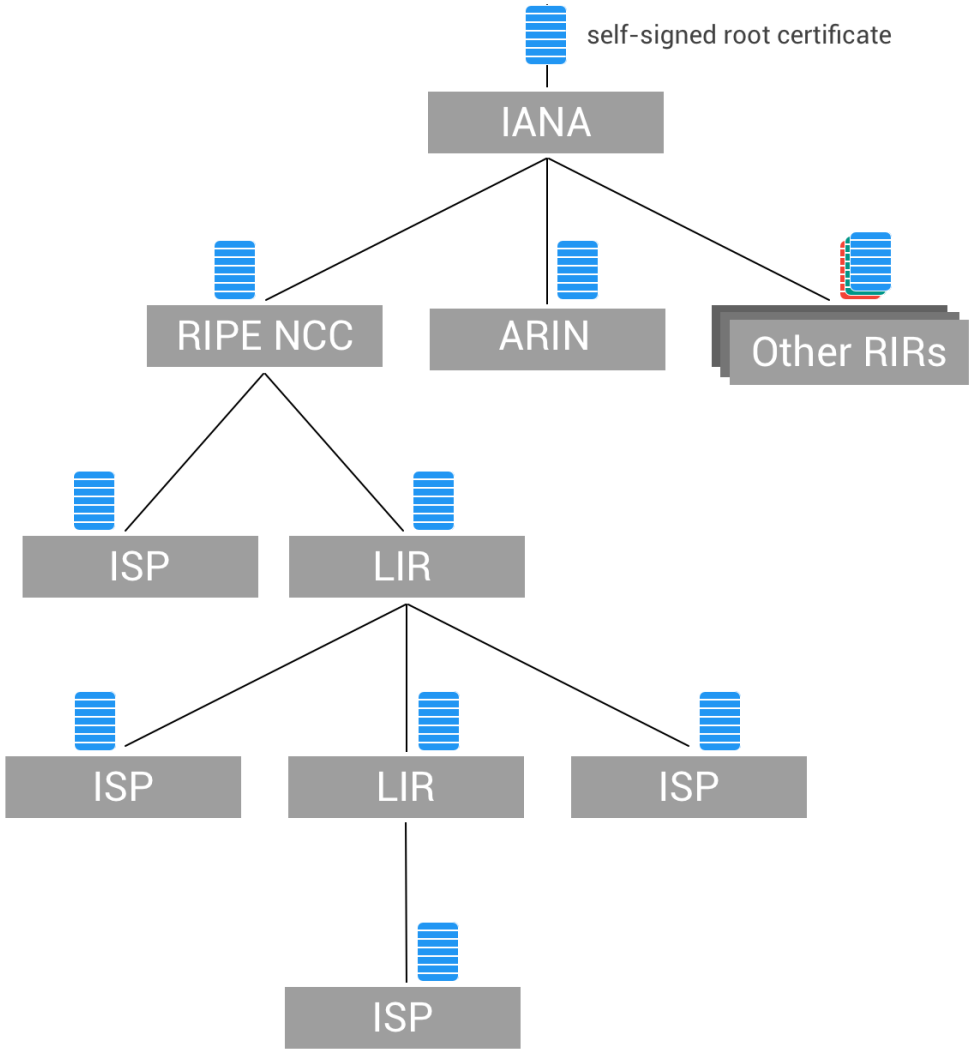
Problems with BGP



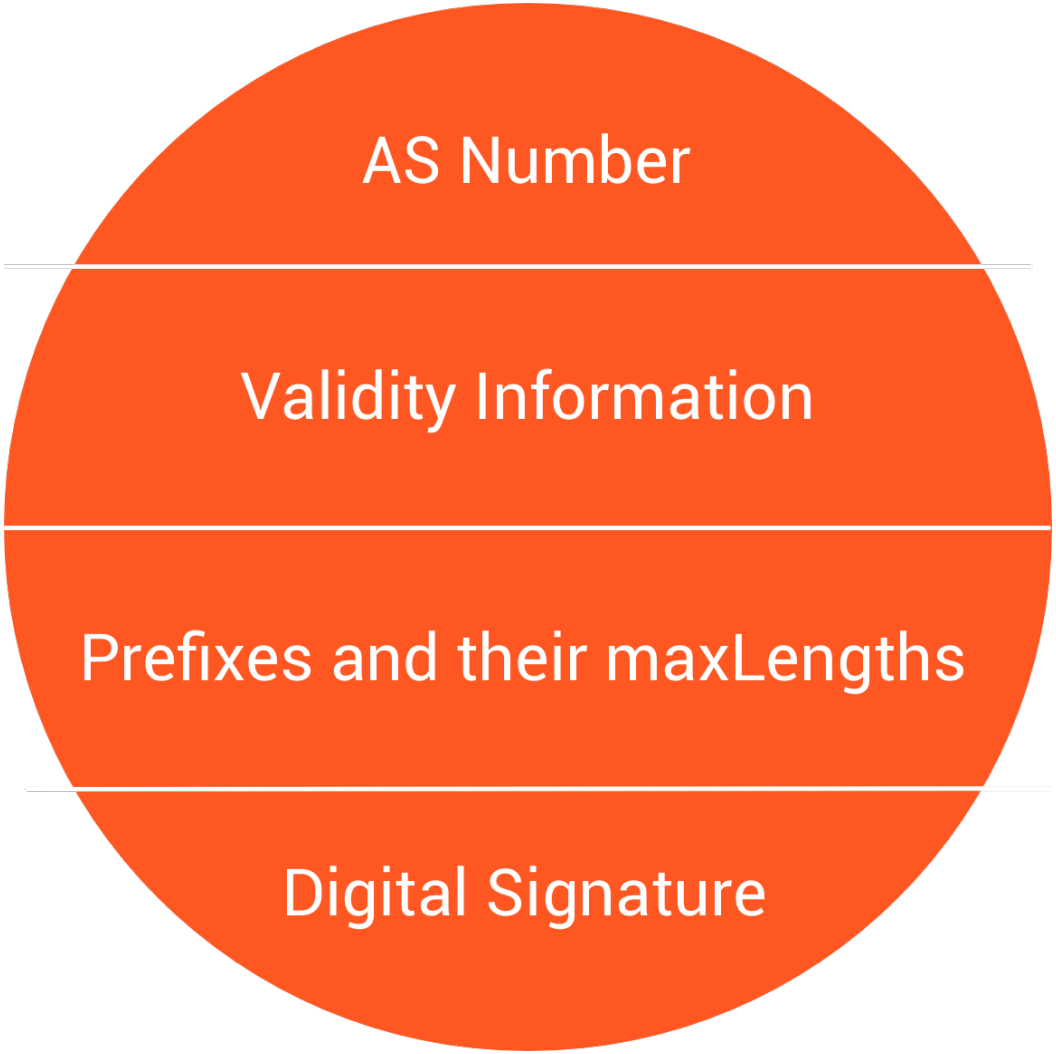
Resource Public Key Infrastructure (RPKI)

- Resource Certificates (X.509)
- Validate holdership of internet number resources
- Mirrors the existing resource allocation infrastructure

Resource Public Key Infrastructure (RPKI)



Route Origination Authorization (ROA)



Securing BGP using the RPKI

- Origin Validation
  - UNKNOWN, VALID or INVALID
- Policies

Research Questions

- What is the impact on routing security for different origin validation deployment strategies?
- What is the impact on routing security for different origin validation security policies?
- What is the current status of routing security given the current publication and potential usage of RPKI data?

Approach

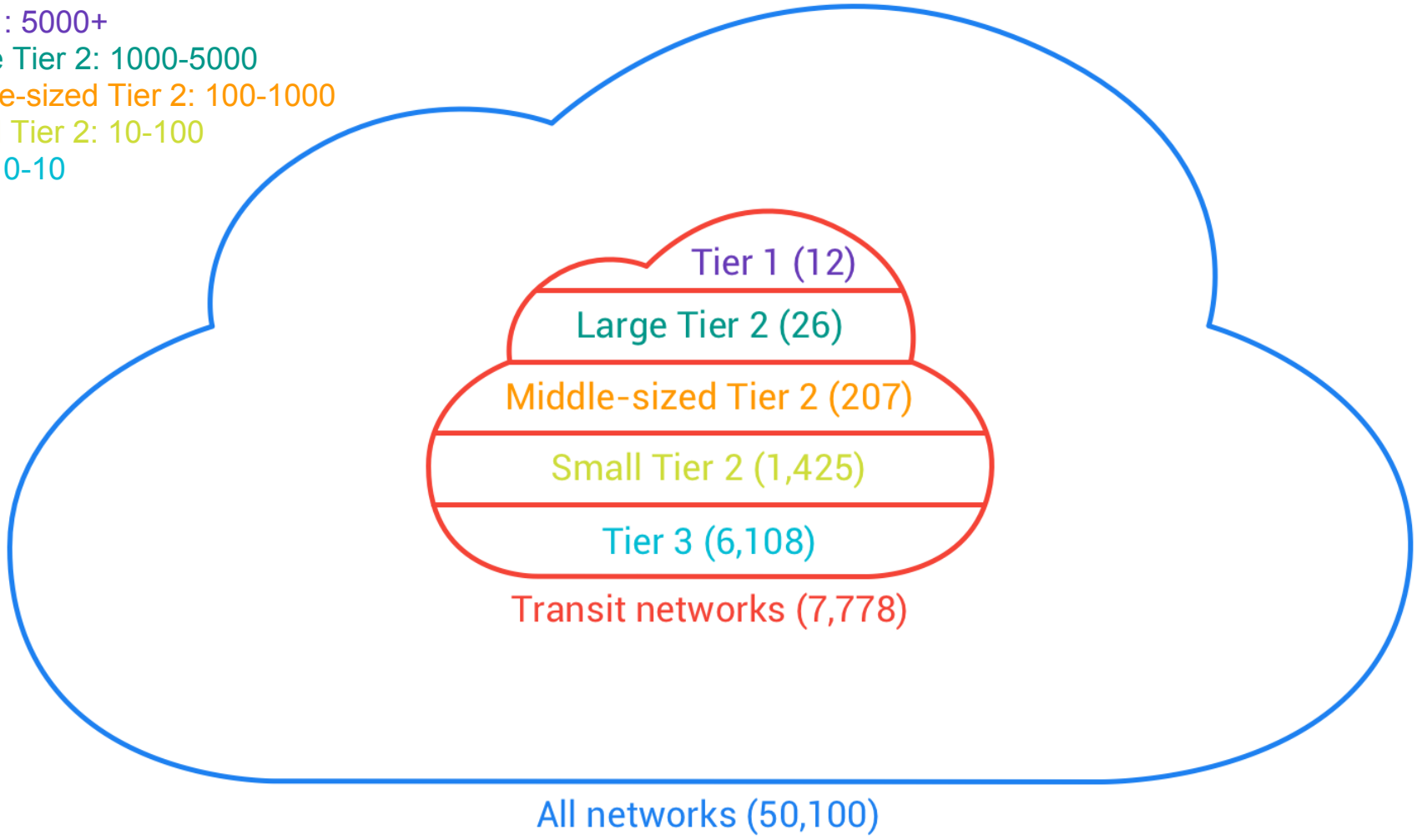
- Simulate using BGPsim
- CAIDA network data
- Define security policies & deployment strategies
- Experiments to measure security & performance

Security Policies

- Hesitant
- Prefer
- Secure
- Strict

Deployment Strategies

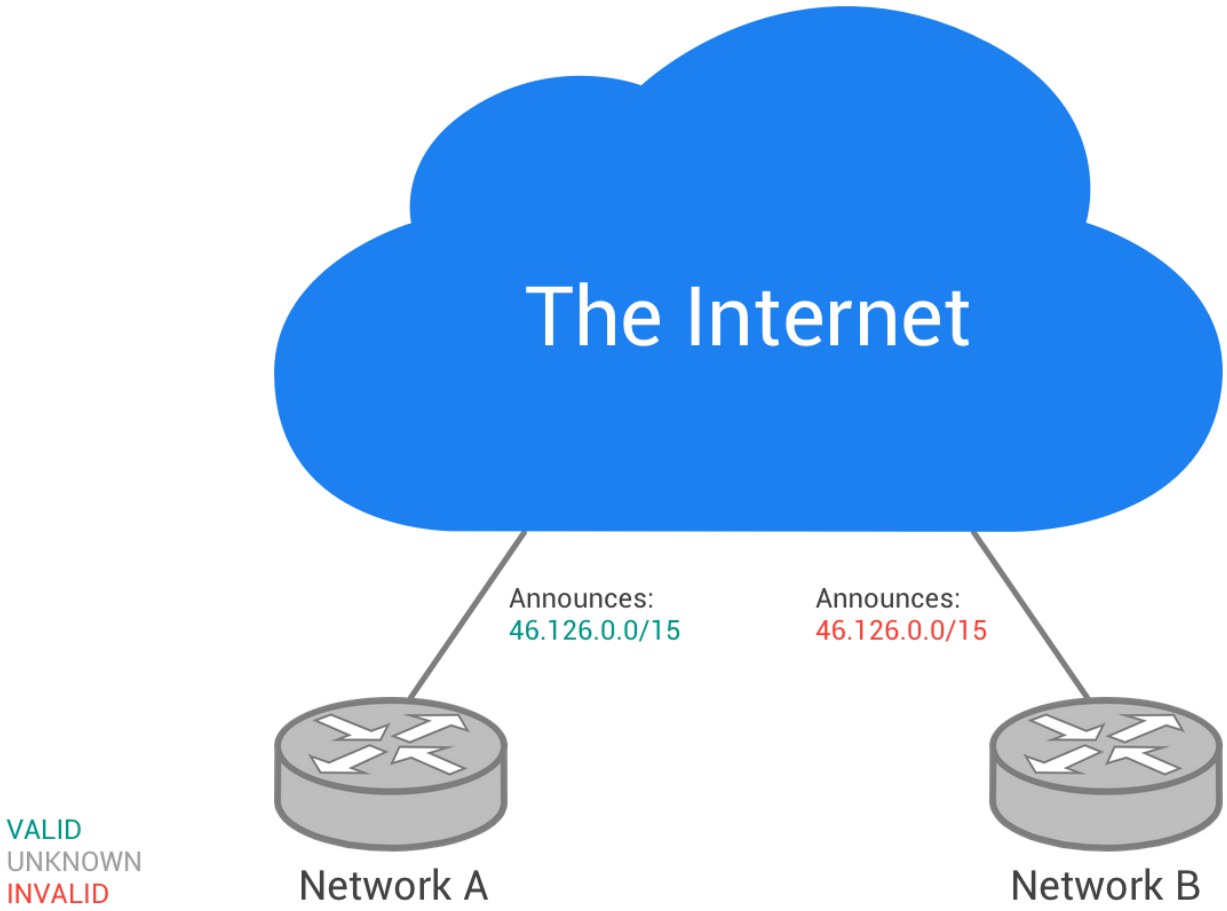
Customer Cone Sizes:
Tier 1: 5000+
Large Tier 2: 1000-5000
Middle-sized Tier 2: 100-1000
Small Tier 2: 10-100
Tier : 0-10



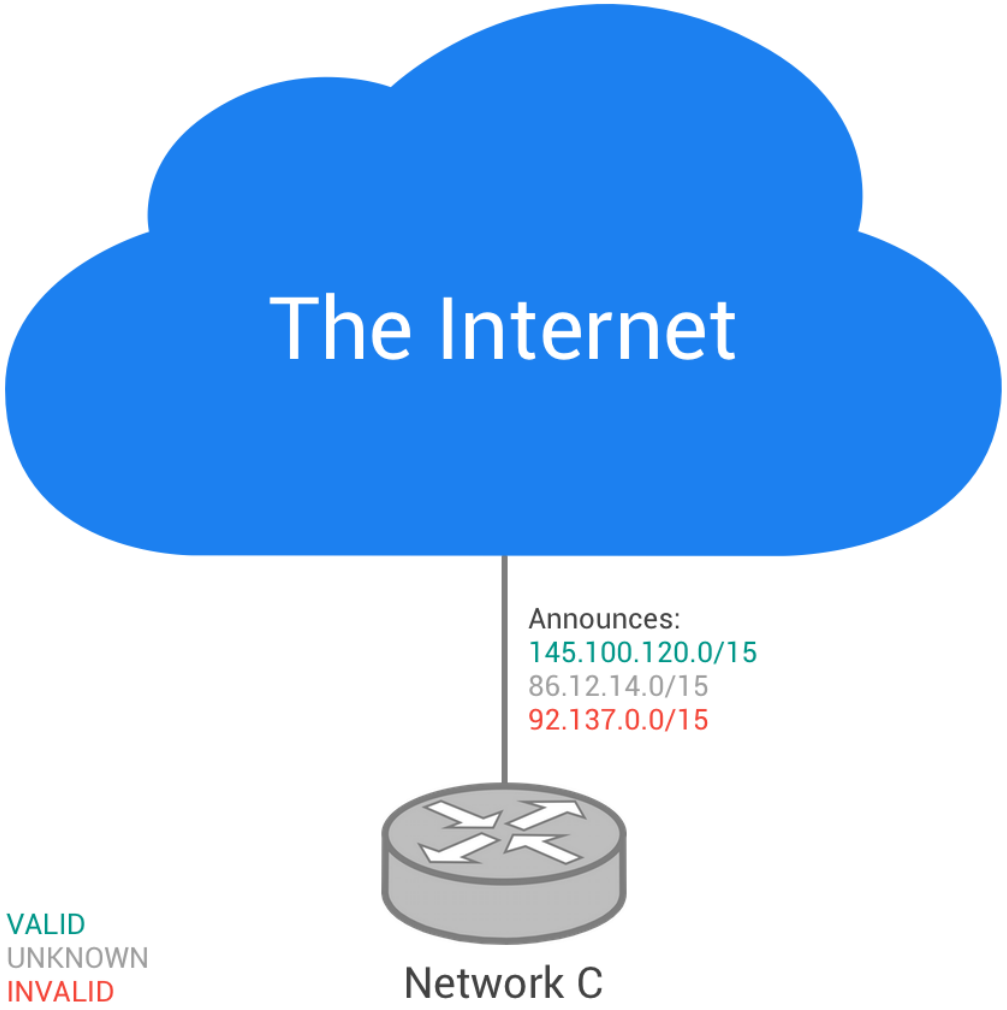
Current Status of Routing Security

- Current publication of ROAs
- What if those ASes do origin validation?

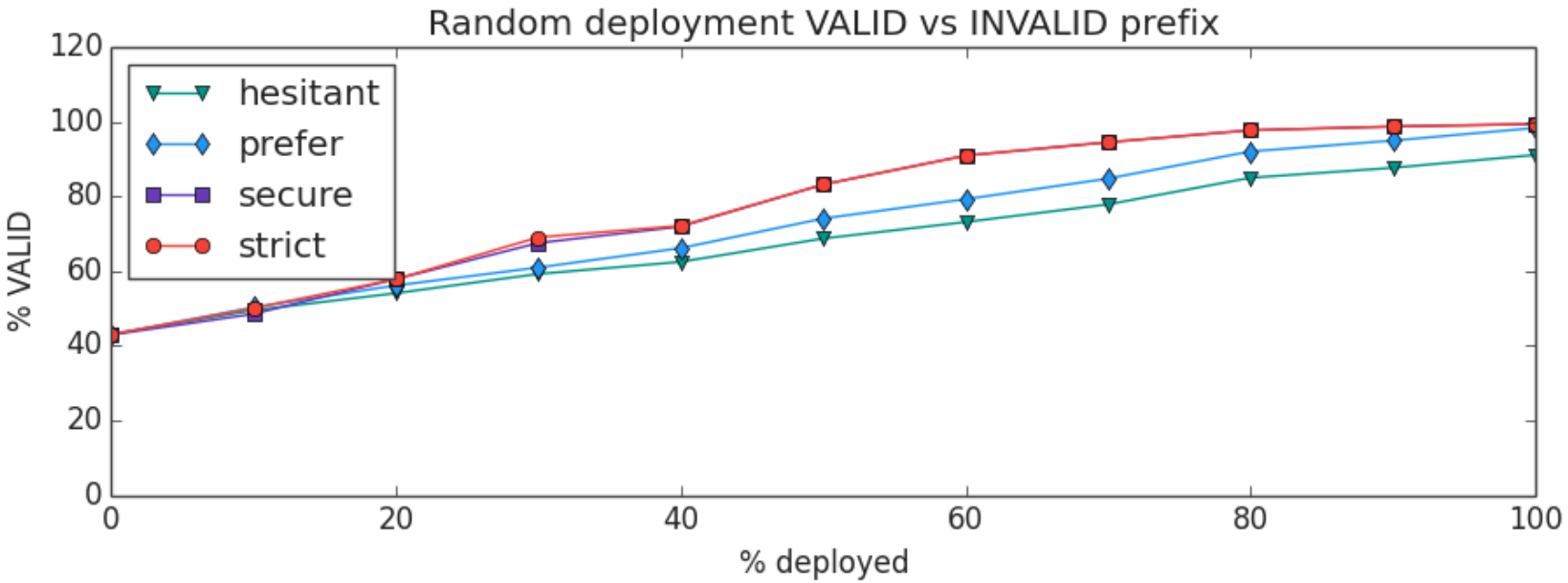
Security Experiment



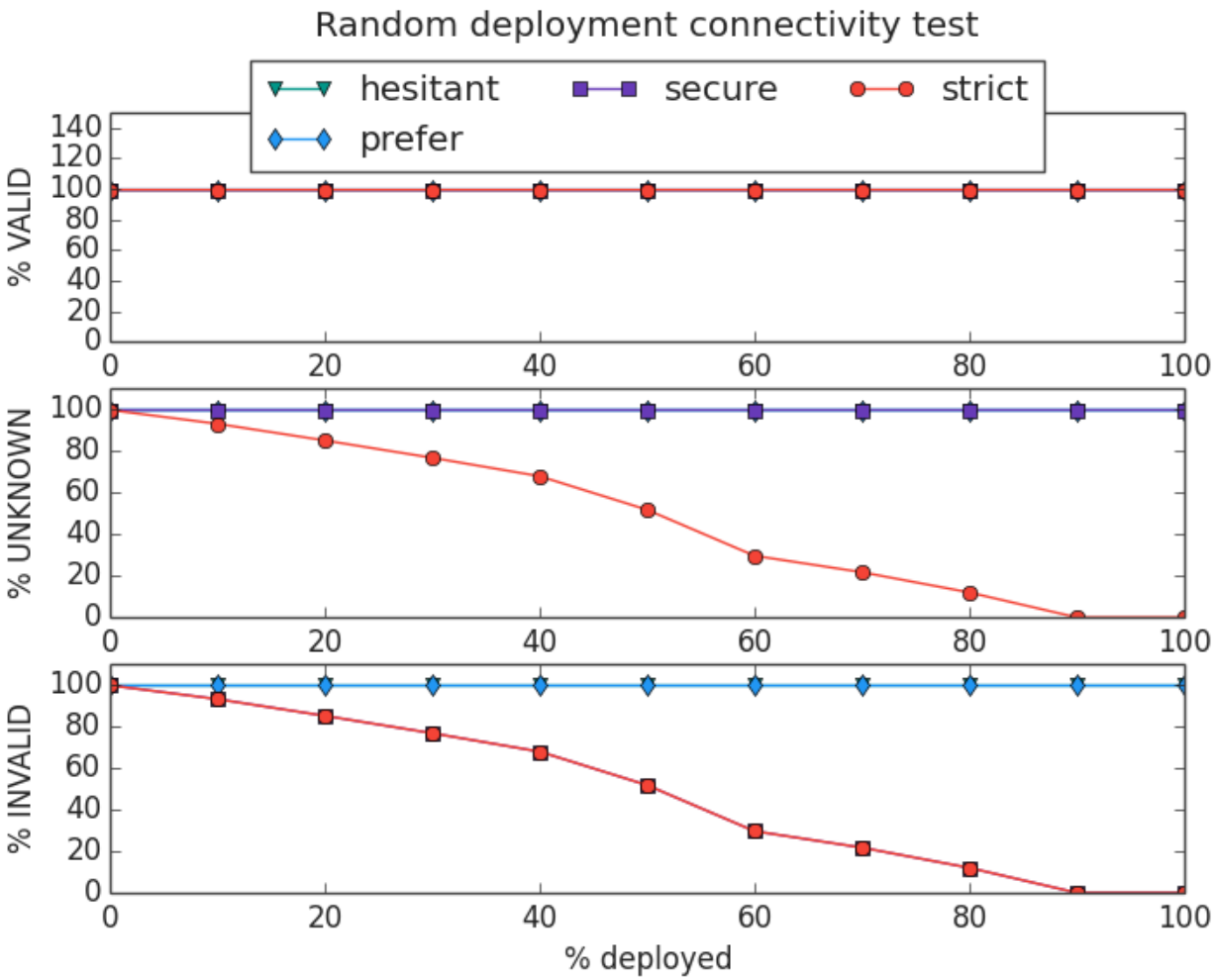
Performance Experiment



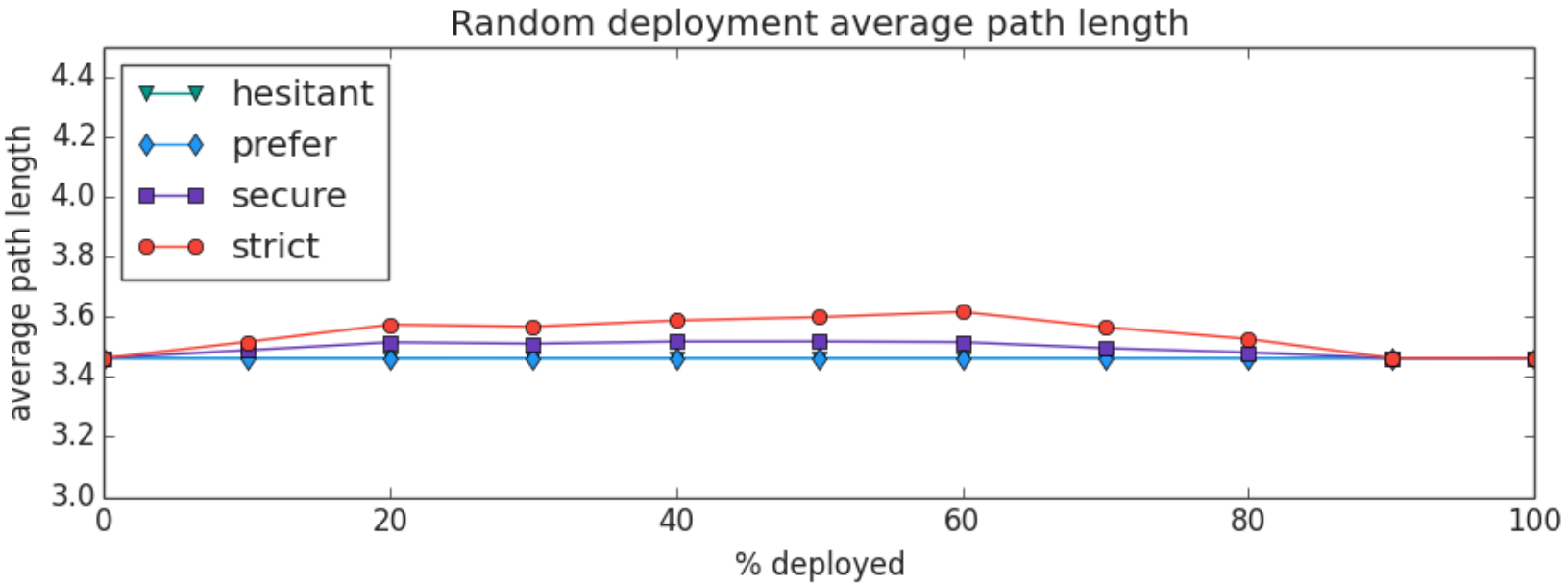
Random Deployment: Security



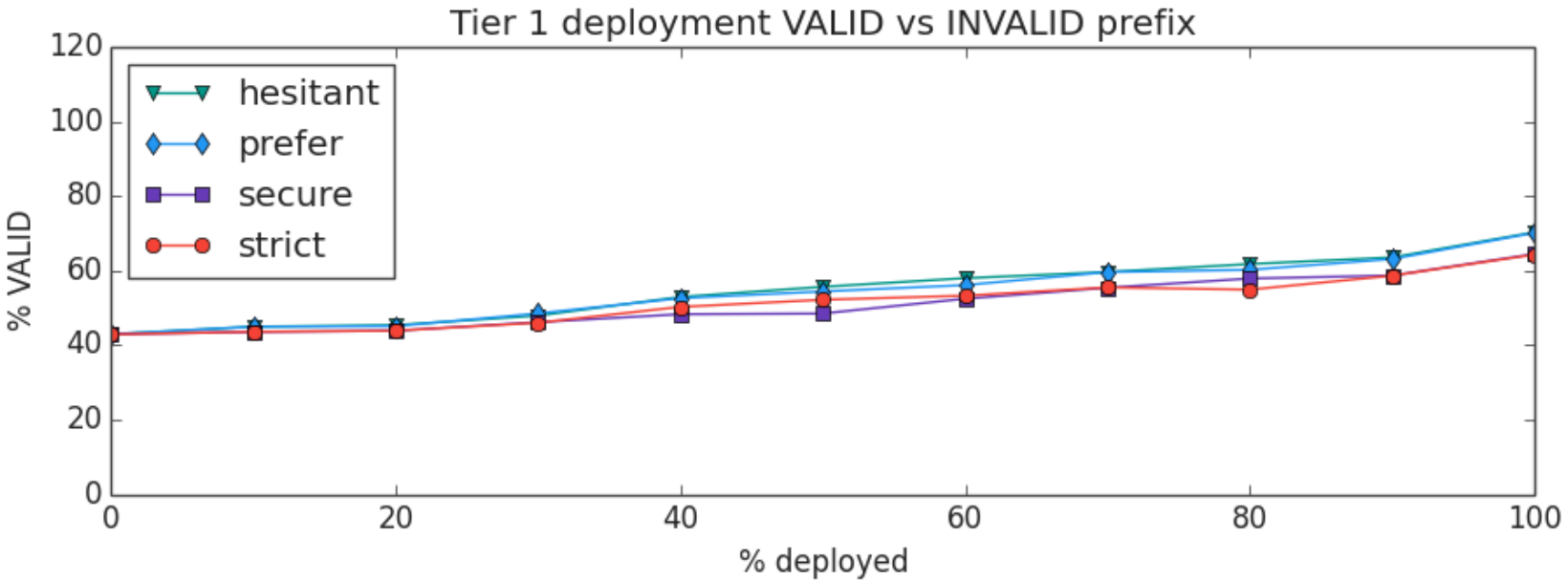
Random Deployment: Connectivity



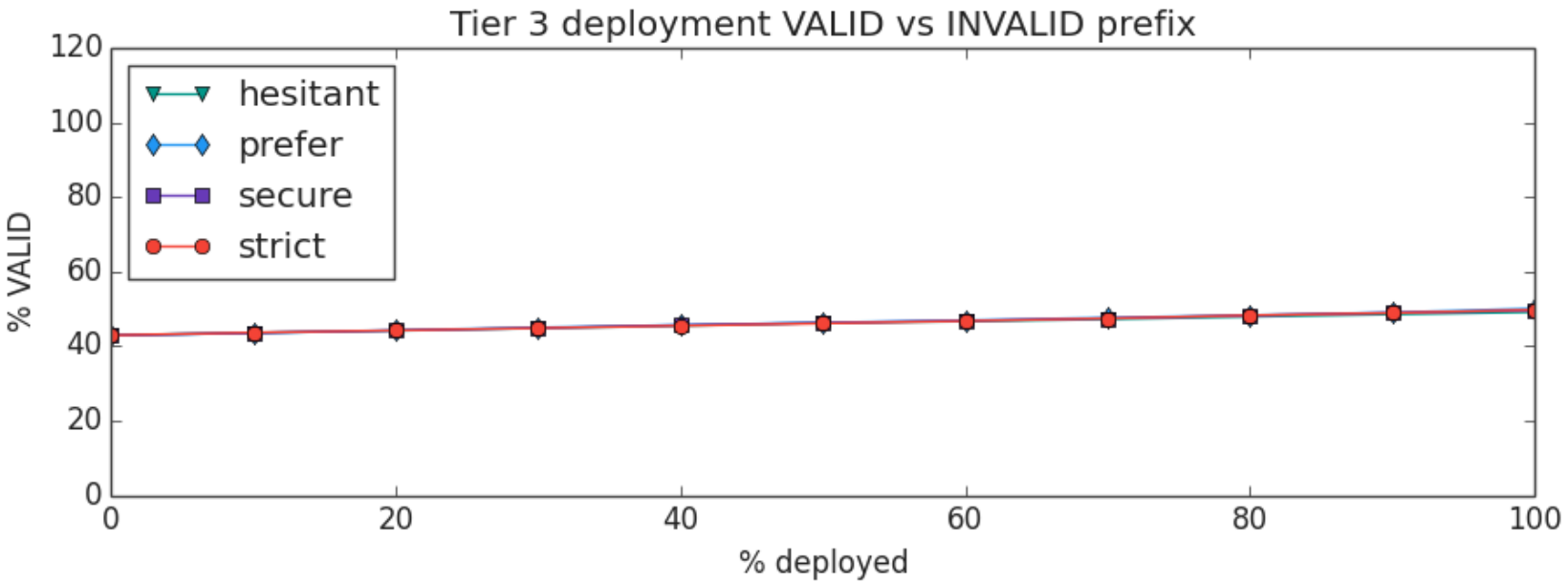
Random Deployment: Path Length



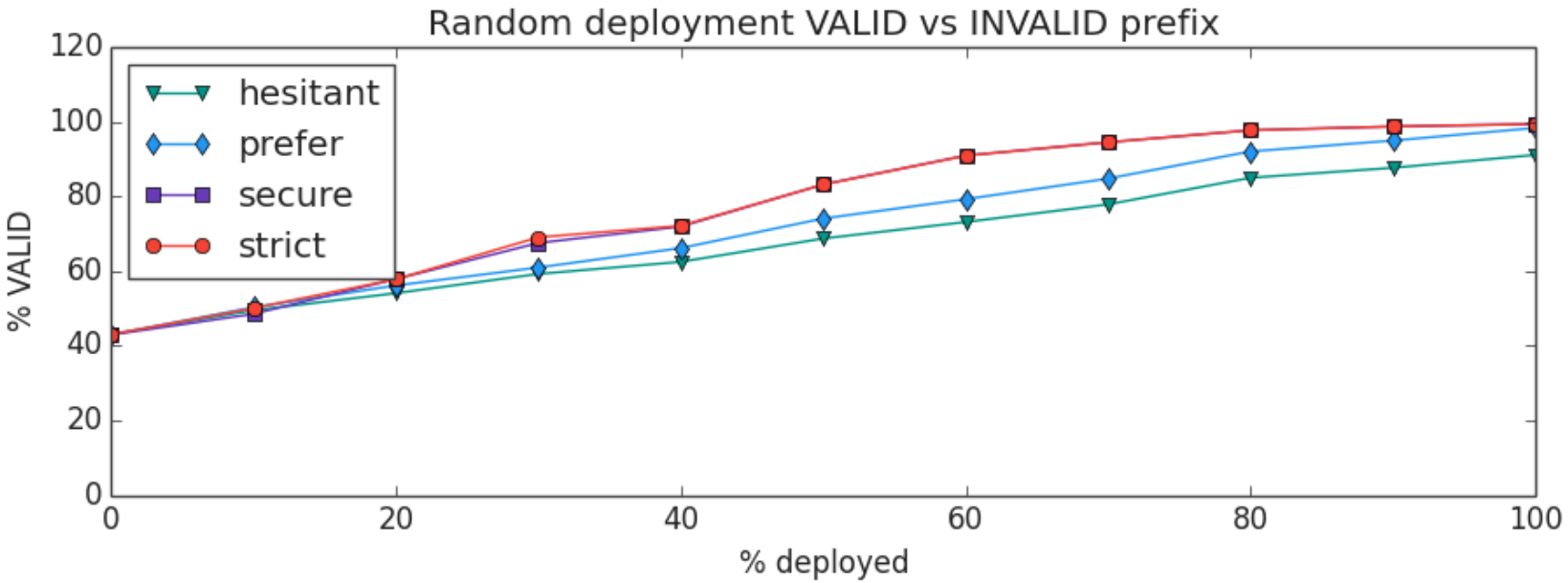
Tier 1 Deployment: Security



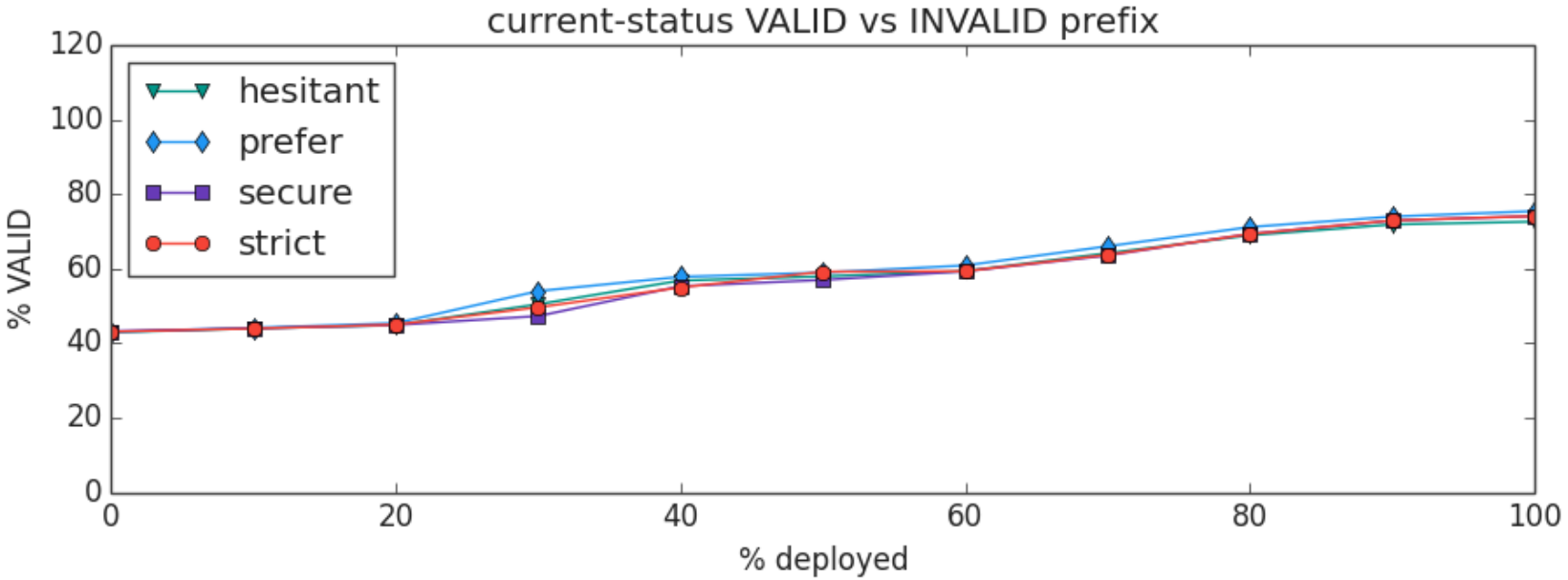
Tier 3 Deployment: Security



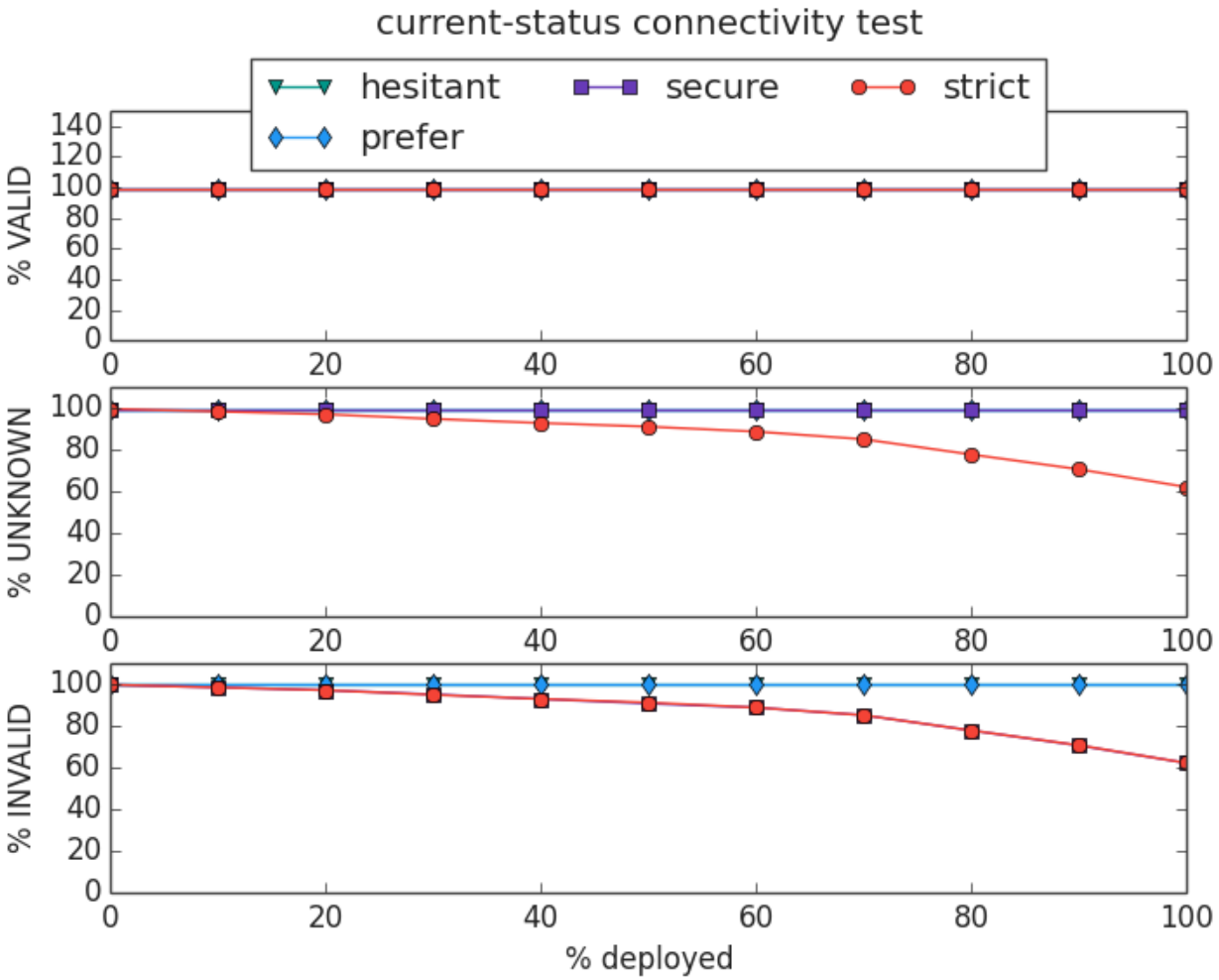
Random Deployment: Security



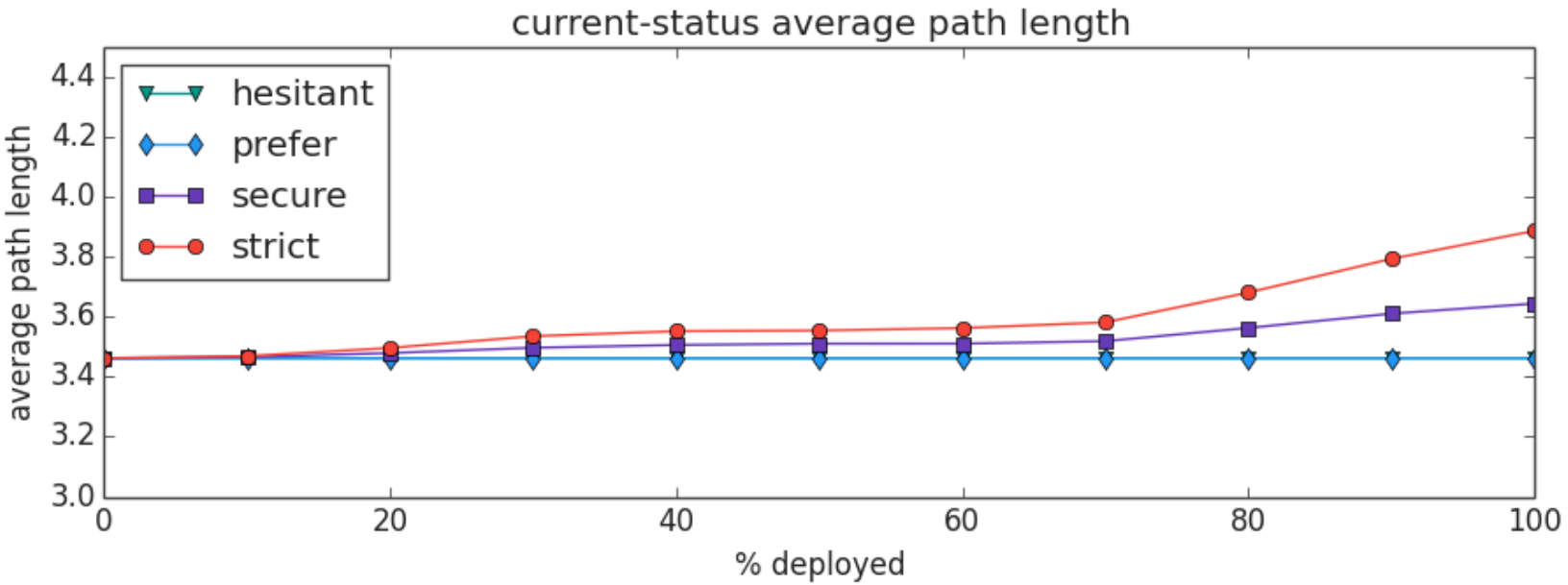
Current Status of Routing Security



Current Status of Routing Security



Current Status of Routing Security



Conclusions

- Structural deployment performs better than random deployment.
- Deploying origin validation to small groups of large ASes give better results than deploying to large groups of small ASes.
- Secure and strict policies can have a positive effect on security, but have a large negative impact on performance.
- Deploying origin validation to ROA-publishing ASes can have a large positive impact on routing security.

Questions?