Effects of RPKI Deployment on BGP Security

Alexandru Ștefănescu
alex.stefa@gmail.com

Benno Overeinder
NLnetLabs
benno@nlnetlabs.nl

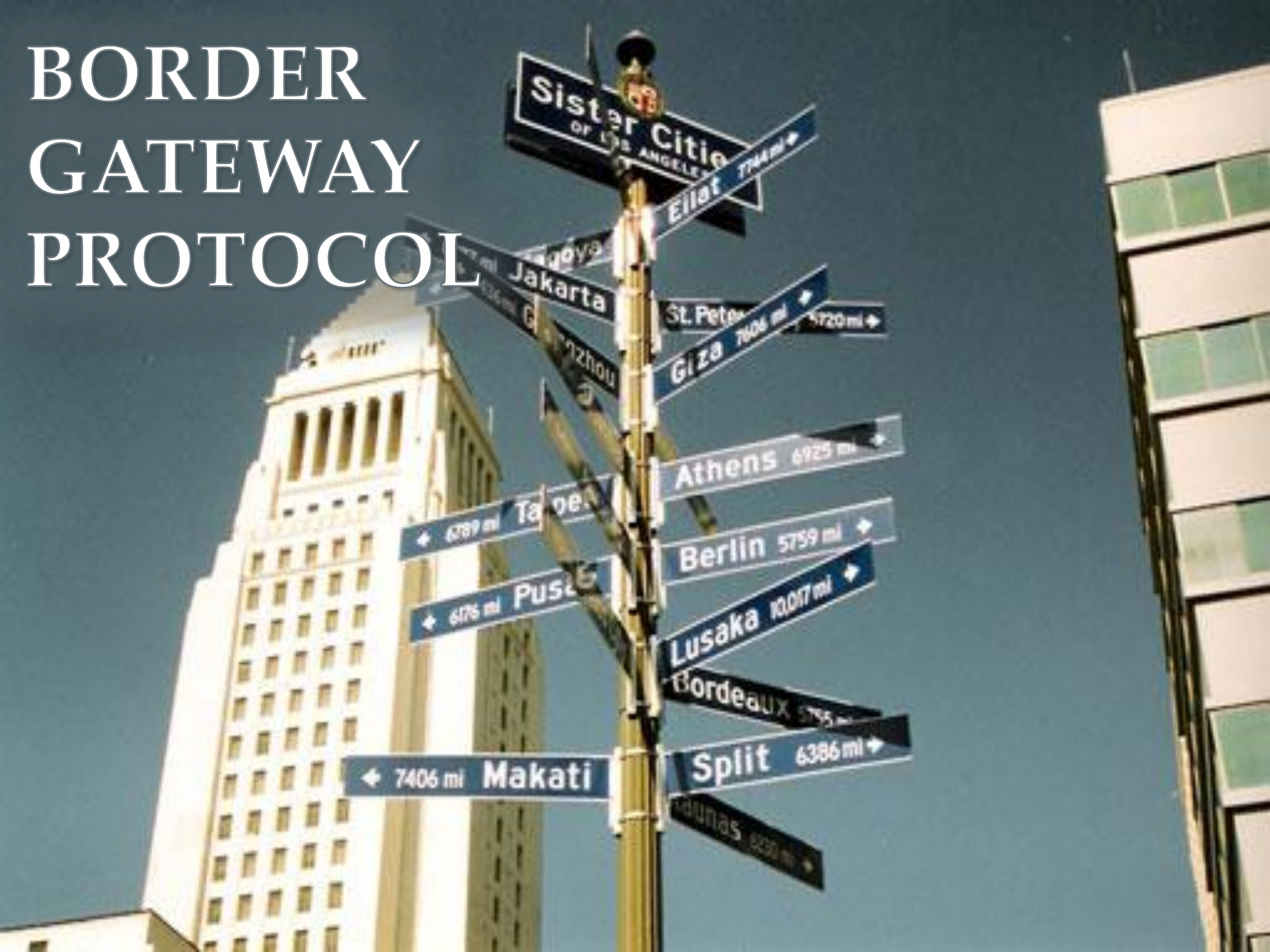
Guillaume Pierre
VU Amsterdam
gpierre@cs.vu.nl

VU Amsterdam – 12 July 2011

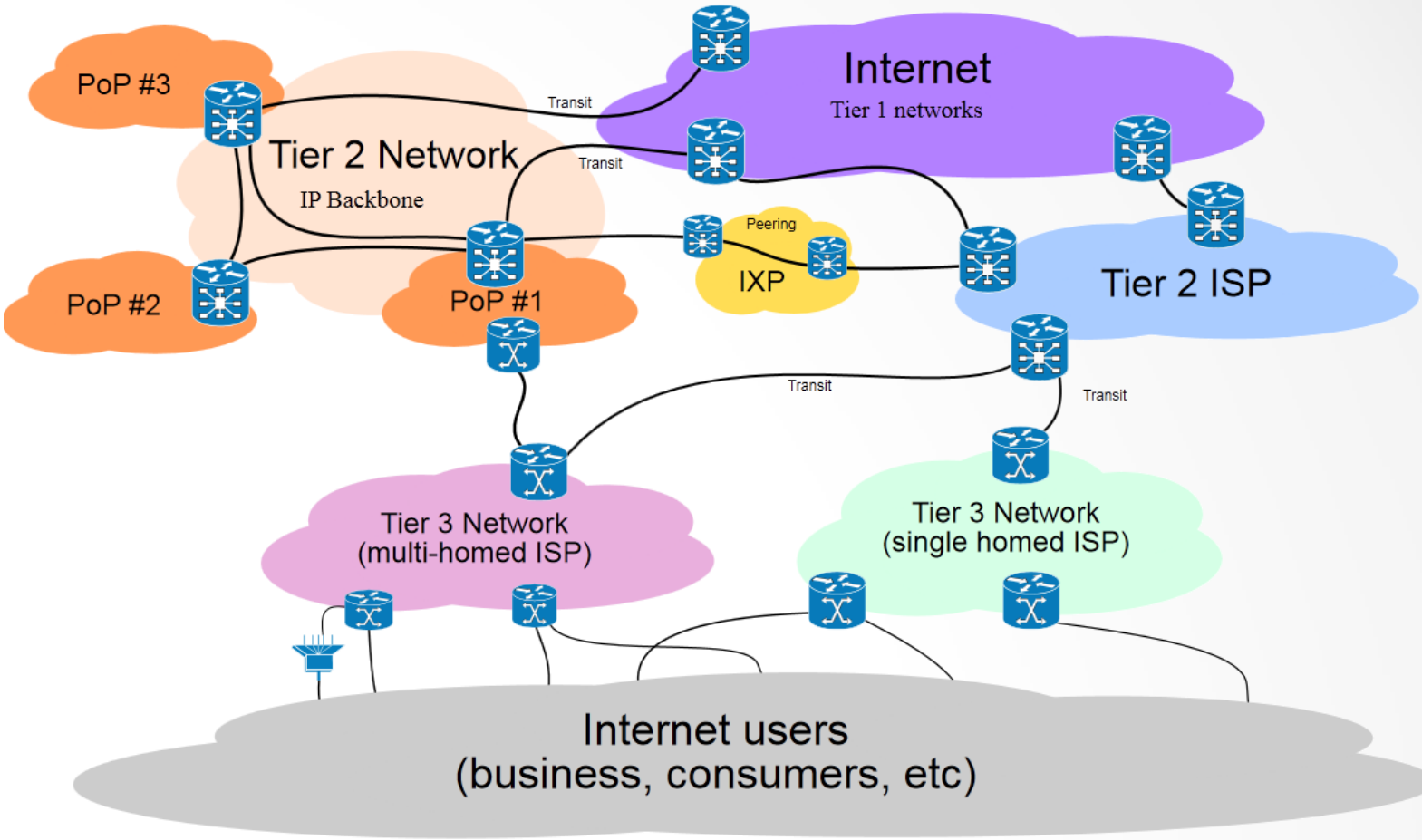
Outline

- BGP Routing
- Securing BGP
- BGP Modeling & Simulation
- Simulation Results

BORDER GATEWAY PROTOCOL



AS Level Internet



From http://en.wikipedia.org/wiki/File:Internet_Connectivity_Distribution_%26_Core.svg

Border Gateway Protocol (BGP)

- Responsible for Internet connectivity
- Concepts
  - Autonomous System (AS)
  - Prefix routing
- Routing decisions based on
  - Path length
  - Network policies
  - ***Business relations*** (customer, provider, peer, sibling)
- Scaling at massive rate
  - AS count: **~37k**
  - Prefix count: **~360k** (IPv4) & ~7k (IPv6)

Problems with BGP

- BGP pathological behaviors
  - Large number of types of attack have been described
  - Very few mitigation actions taken
- Increased impact of attacks on today's Internet as an essential and ubiquitous service
  - Pakistan Telecom hijacking of YouTube in Feb 2008
  - 15% of global Internet traffic redirected through China Telecom for 18min in April 2010 (acknowledged months later)

Securing BGP

- Main cause of malfunction: *misconfiguration*
- Several security additions proposed: **S-BGP**, psBGP, soBGP, IRV, etc
- Most important based on RPKI deployment
- *BGP cannot be secured overnight!*
- ASes as commercial entities must also realize it's in their own interest

Project Goals

- Study the effect of BGP deployment scenarios
- Find out order to start securing ASes for maximum benefit
- Better protocol understanding: relation between no. of secured ASs and validated routes
  - Impact of securing just biggest ASs (e.g. Tier 1)
  - How important is securing CDNs?

BGP Security Mechanisms

- Secure Origin Authentication **(SOA)**
  - Routes in BGP updates contain signature of origin AS
  - Each AS validates signature by looking in a distributed cache
  - Will there be downtimes?
- Path Validation **(PV)**
  - When forwarding route advertisements to neighbors, ASes sign route with chain hash function

BGP Modeling & Simulation (1)

- You can't simulate the Internet!
- **Abstract** protocol and network:
  - no physical network modeling, 1 AS = 1 node (ignore IBGP)
  - standard BGP features: explicit prefix tables, announce and withdraw messages, route propagation according to policies, etc.
- Security model:
  - tag BGP messages as being *validated* or not
  - security policies assigned to ASes individually

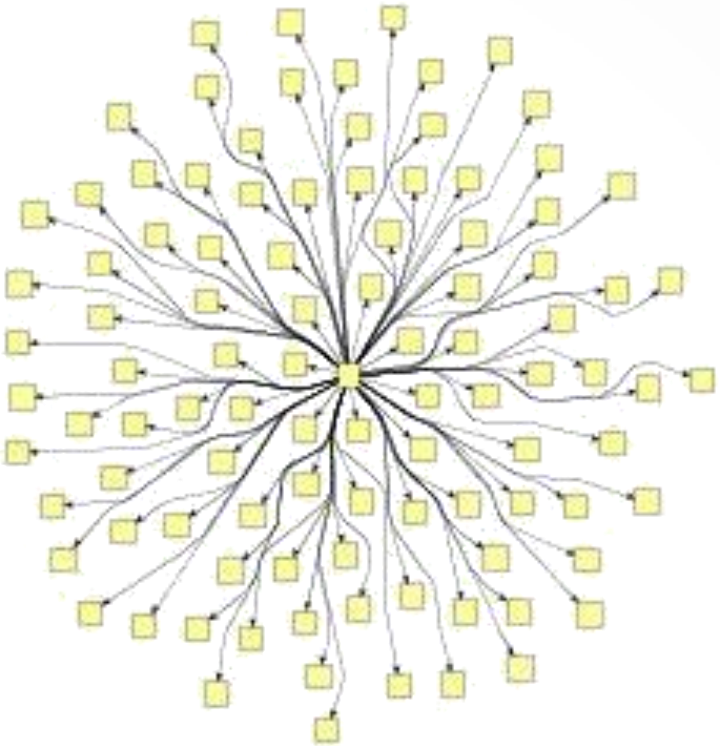
BGP Modeling & Simulation (2)

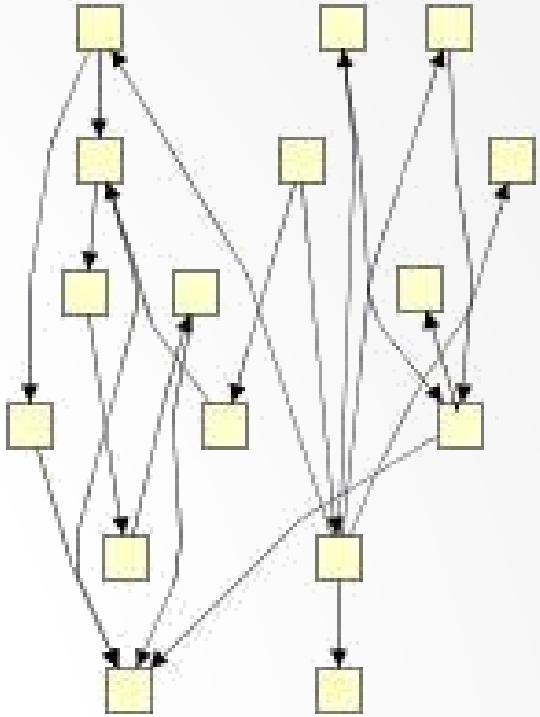
- Allow for easy implementation of security solutions
  - We can emulate practically any proposed security additions
- Do not perform crypto computations, but emulate
- Abstract what you can, but run everything in (scaled) real-time
- Gather as much real-world data/scenarios and run the simulation upon them

Our Simulator

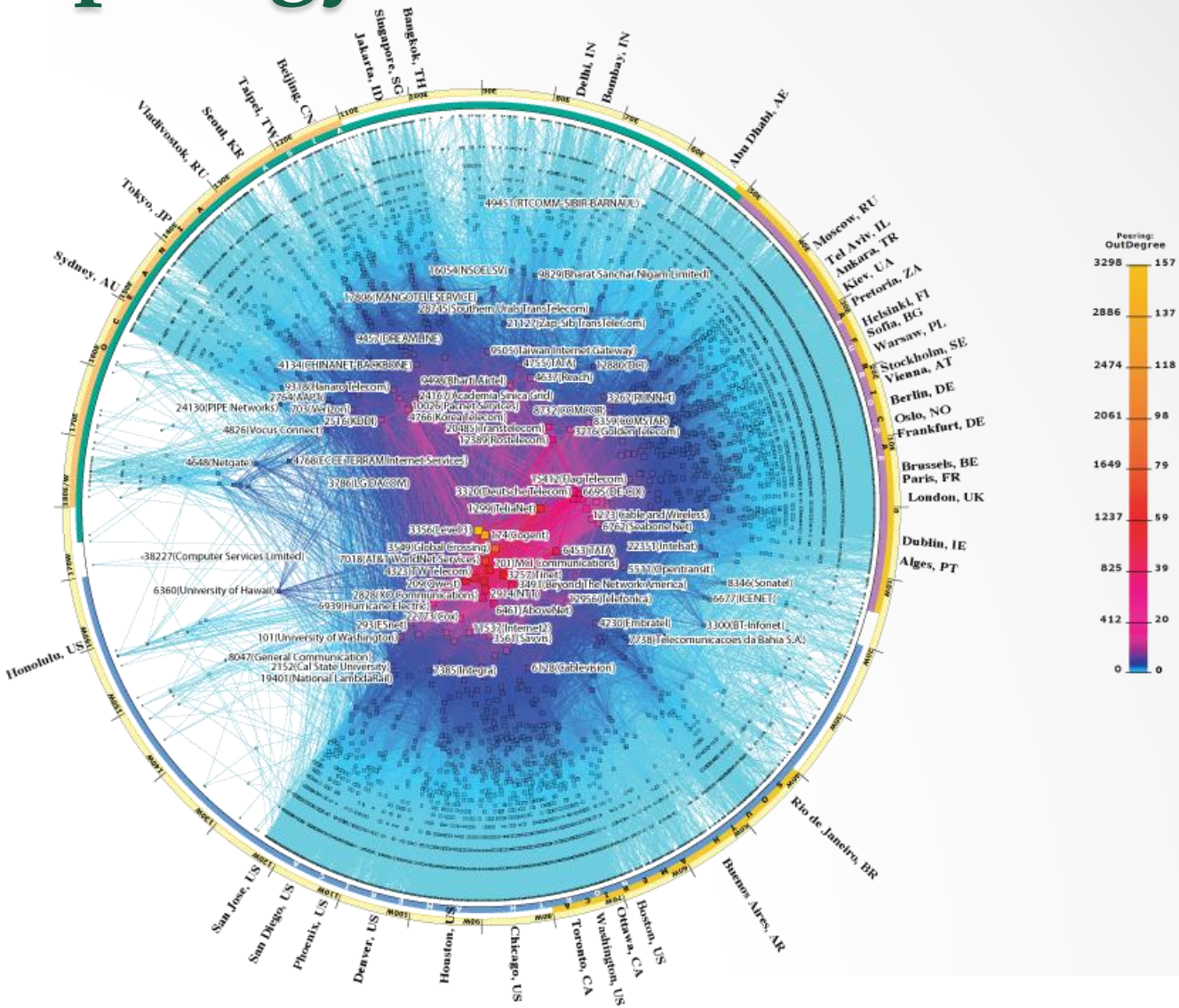
- Enhanced version of simulator by M. Wojciechowski (2009)
- Java simulator running on DAS-4 homogeneous cluster; low latency network
- Each AS is a separate thread (>1000 threads per node)
- Allows easy tweaking of BGP behavior and security policies
- Uses network annotated adjacencies from CAIDA for 2010

BGP Topology





BGP Topology



Simulation Process

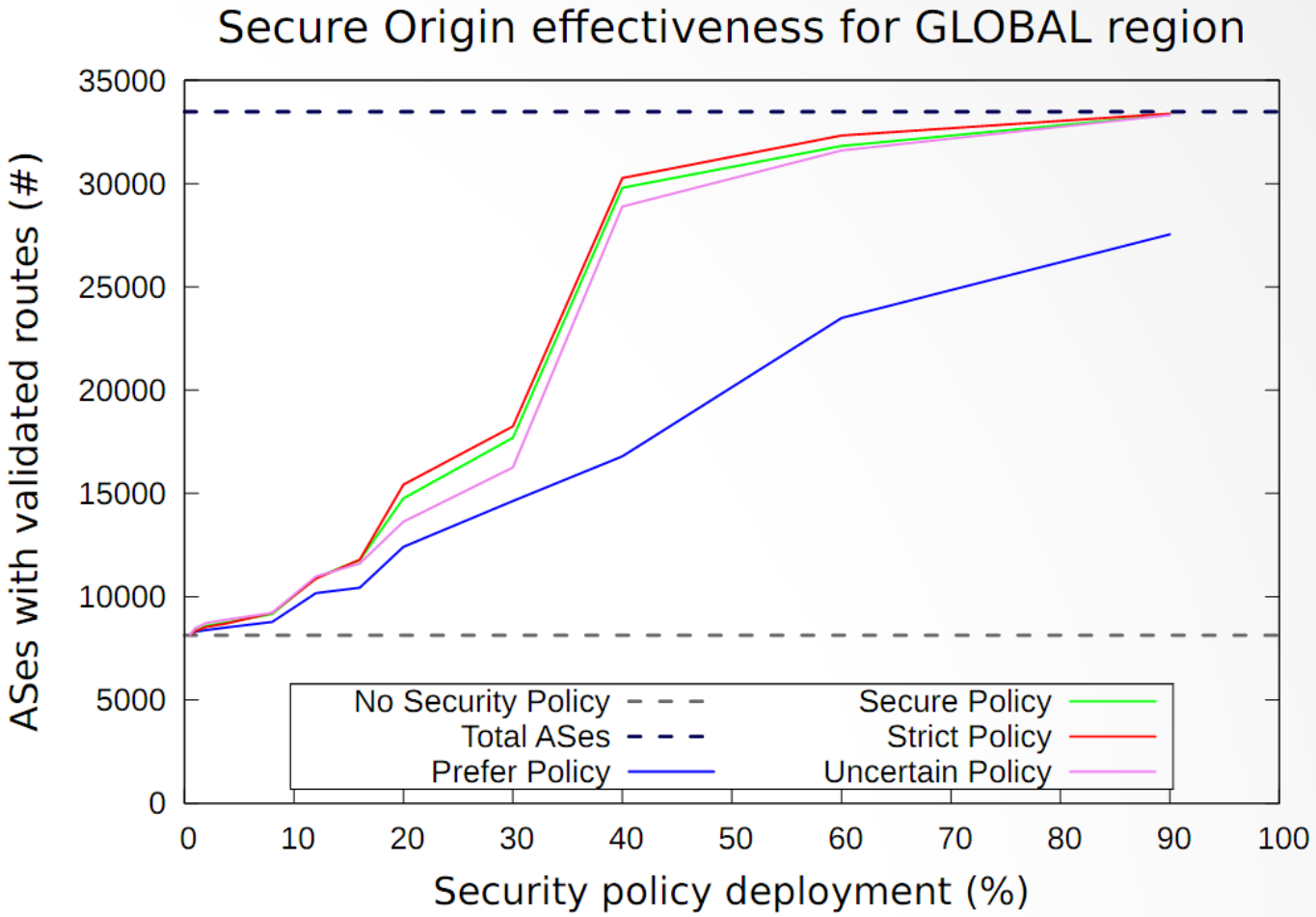
- Running scenarios:
  1. Assign security policies in various percentages
  2. **Announce the same prefix from two ASes**
     (one secured AS and one rogue AS)
  3. Wait for prefix to propagate
  4. Count routes to **secured** AS

- Factors:
  - What if topology changes?
  - What is the impact of different types of security policies?
  - What is the impact of different security policy distributions?
  - How does it differ when prefix announced by stubs vs. large ASs?

Security Policies

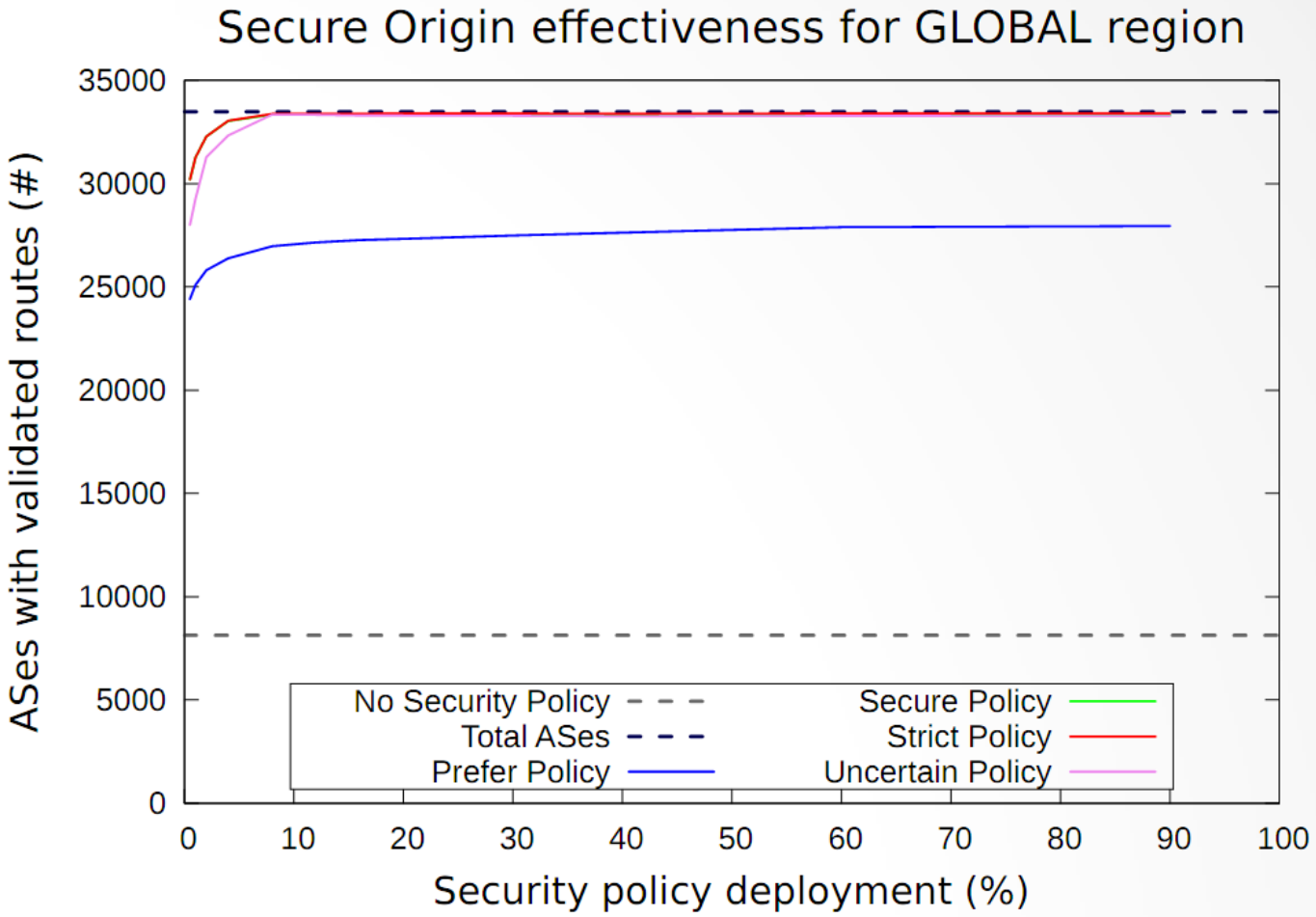
- **Ignore**
  - Standard BGP
- **Prefer**
  - Choose validated route between routes of same length
  - Most realistic
- **Secure**
  - Always prefer validated routes over unknown
- **Strict**
  - Accept *only* validated routes
- **Uncertain**
  - Same as Secure, but introducing introducing route validation *unavailability* in 10% of cases

SOA: Global Deployment – Random Strategy



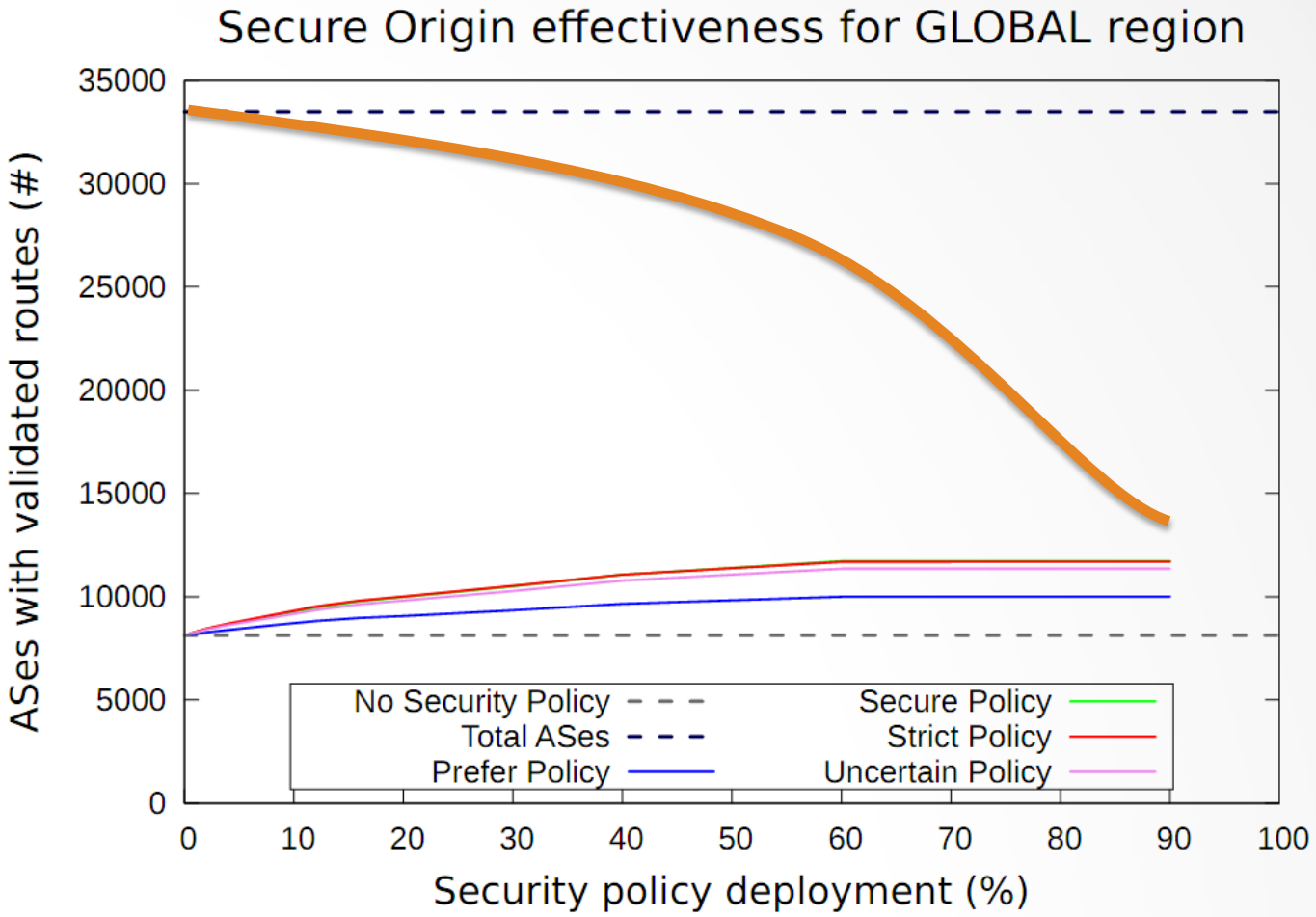
AS3265 / **XS4ALL** / #2127 VS. AS30890 / **Evolva Intercom SRL** / #168

SOA: Global Deployment – Top-down Strategy



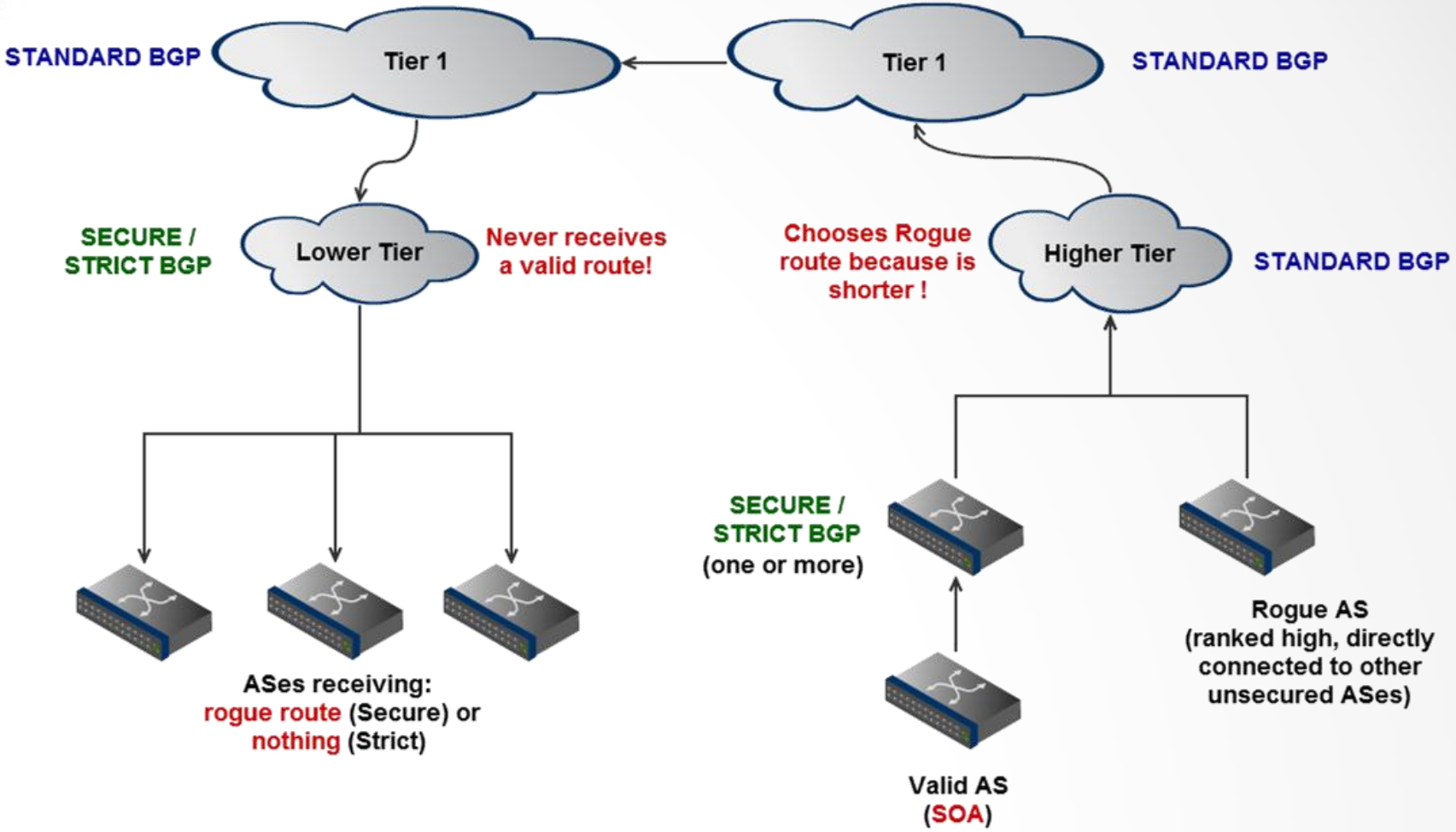
AS3265 / **XS4ALL** / #2127 VS. AS30890 / **Evolva Intercom SRL** / #168

SOA: Global Deployment – Medium Strategy

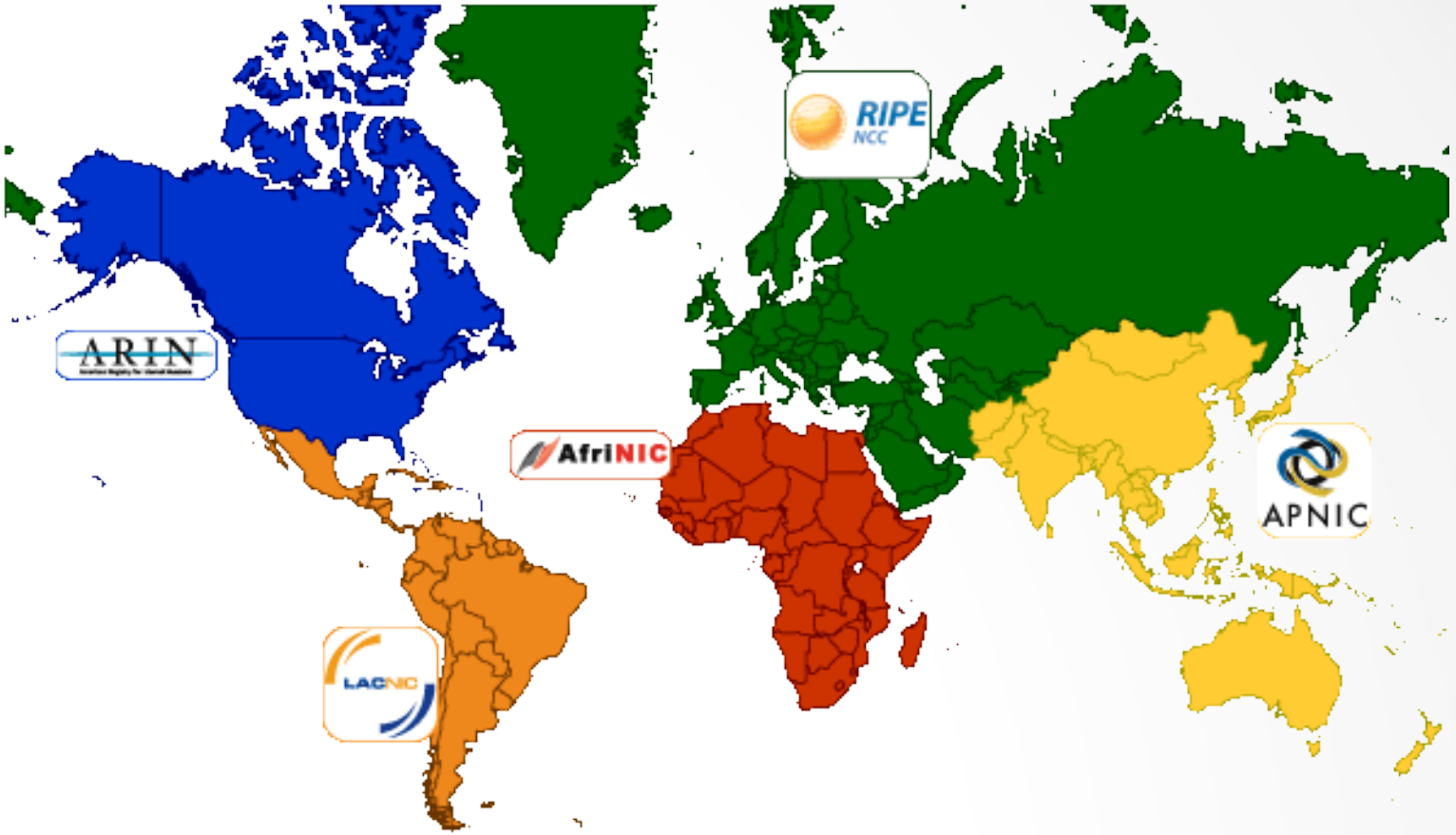


AS3265 / **XS4ALL** / #2127 VS. AS30890 / **Evolva Intercom SRL** / #168

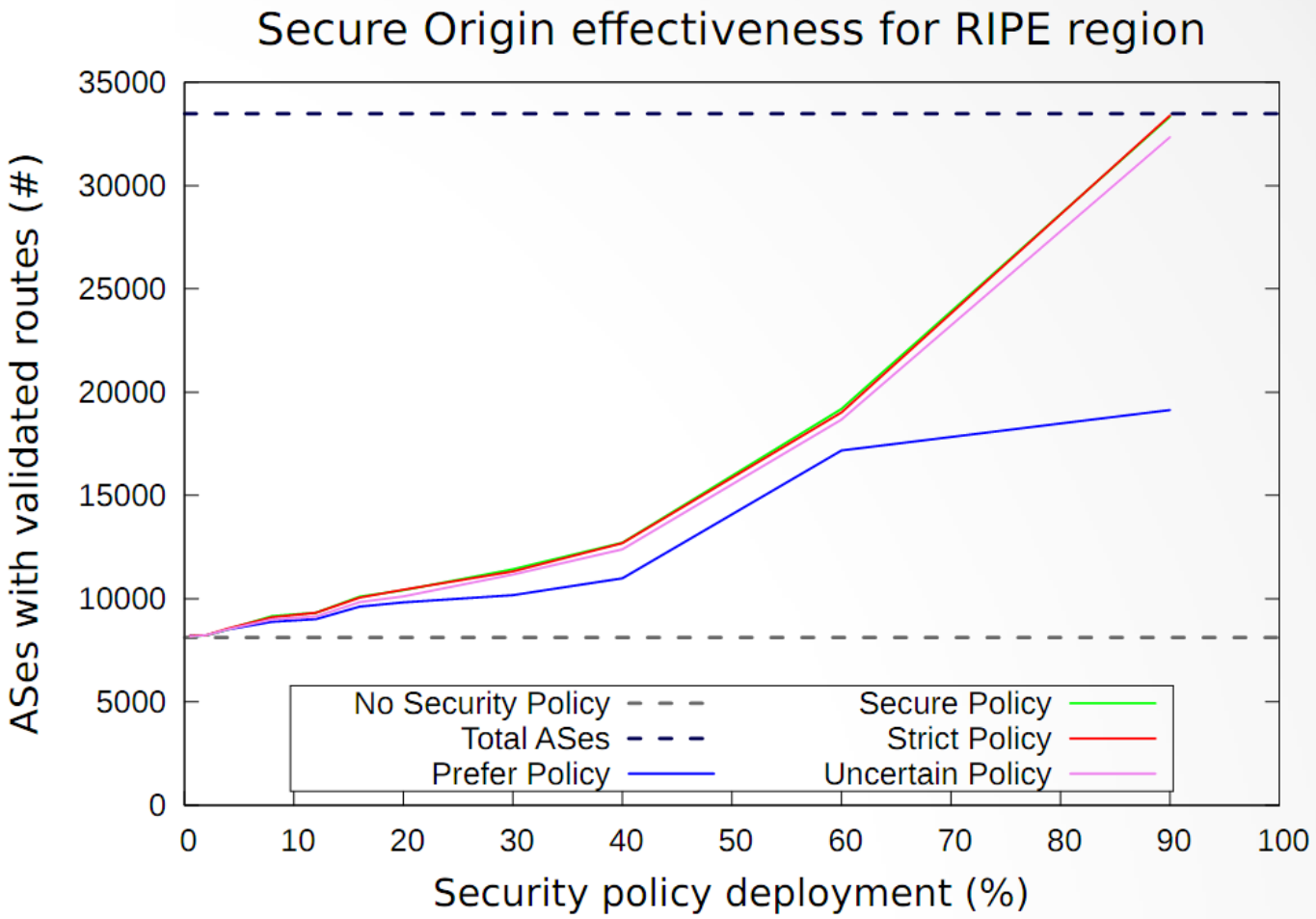
Inducing un-connectivity



Internet RIRs



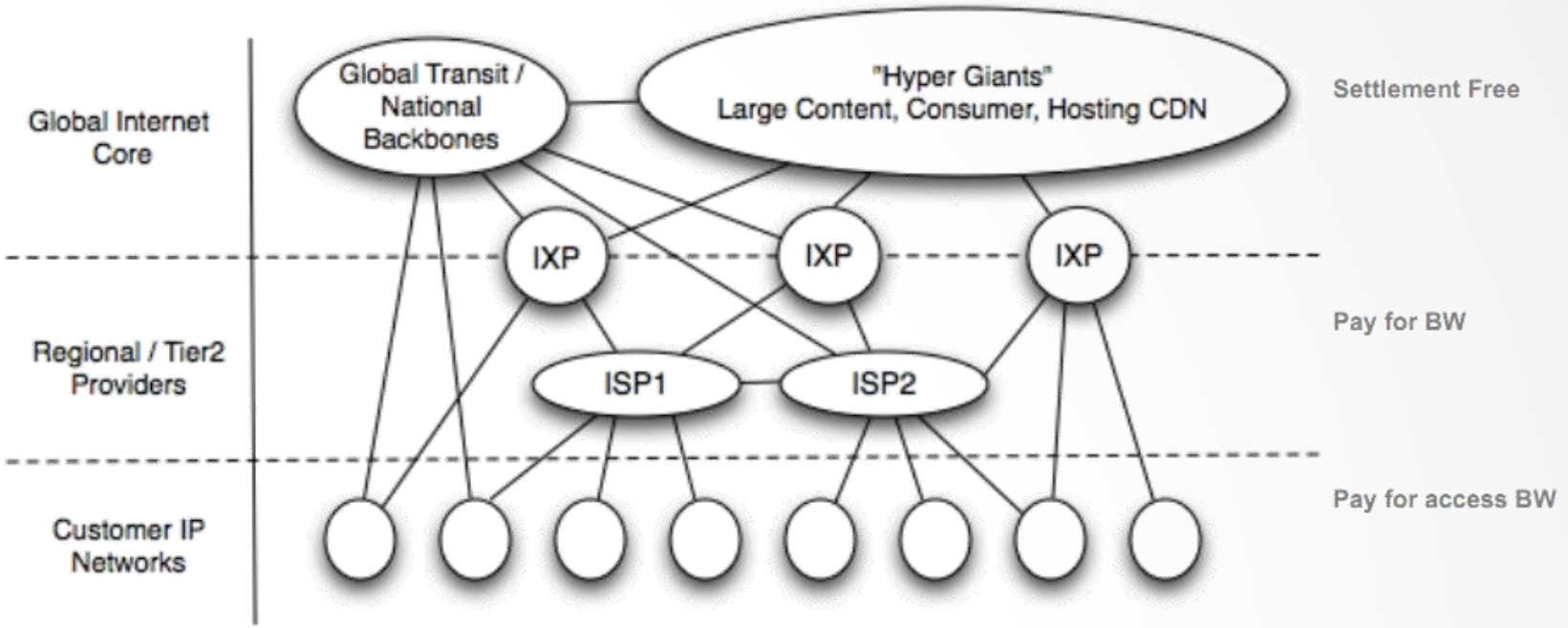
SOA: RIPE Deployment – Random Strategy



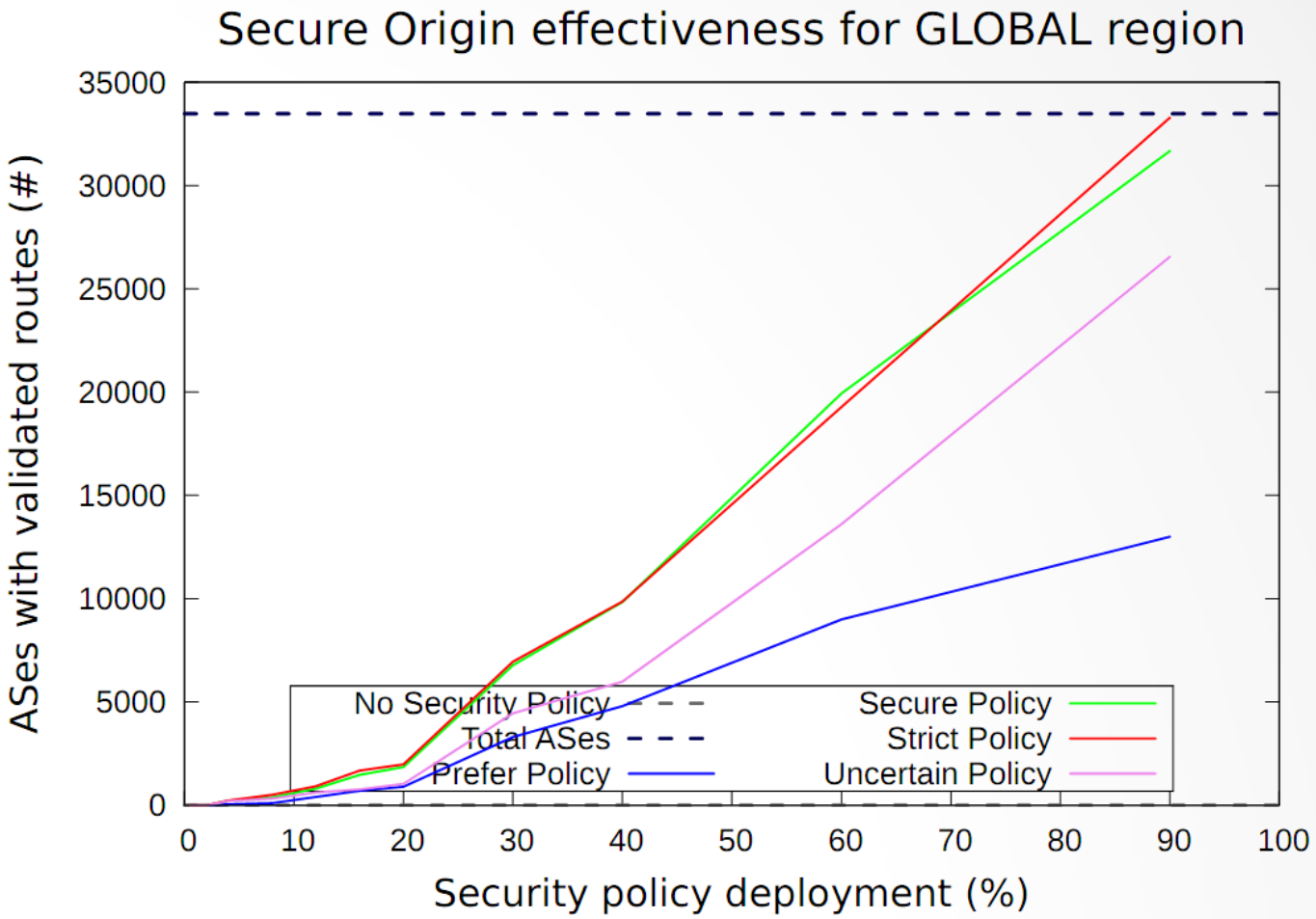
AS3265 / **XS4ALL** / #2127 VS. AS30890 / **Evolva Intercom SRL** / #168

Securing CDNs

- The New Internet – "Hyper Giants" CDNs
  Craig Labovitz (Arbor Networks)

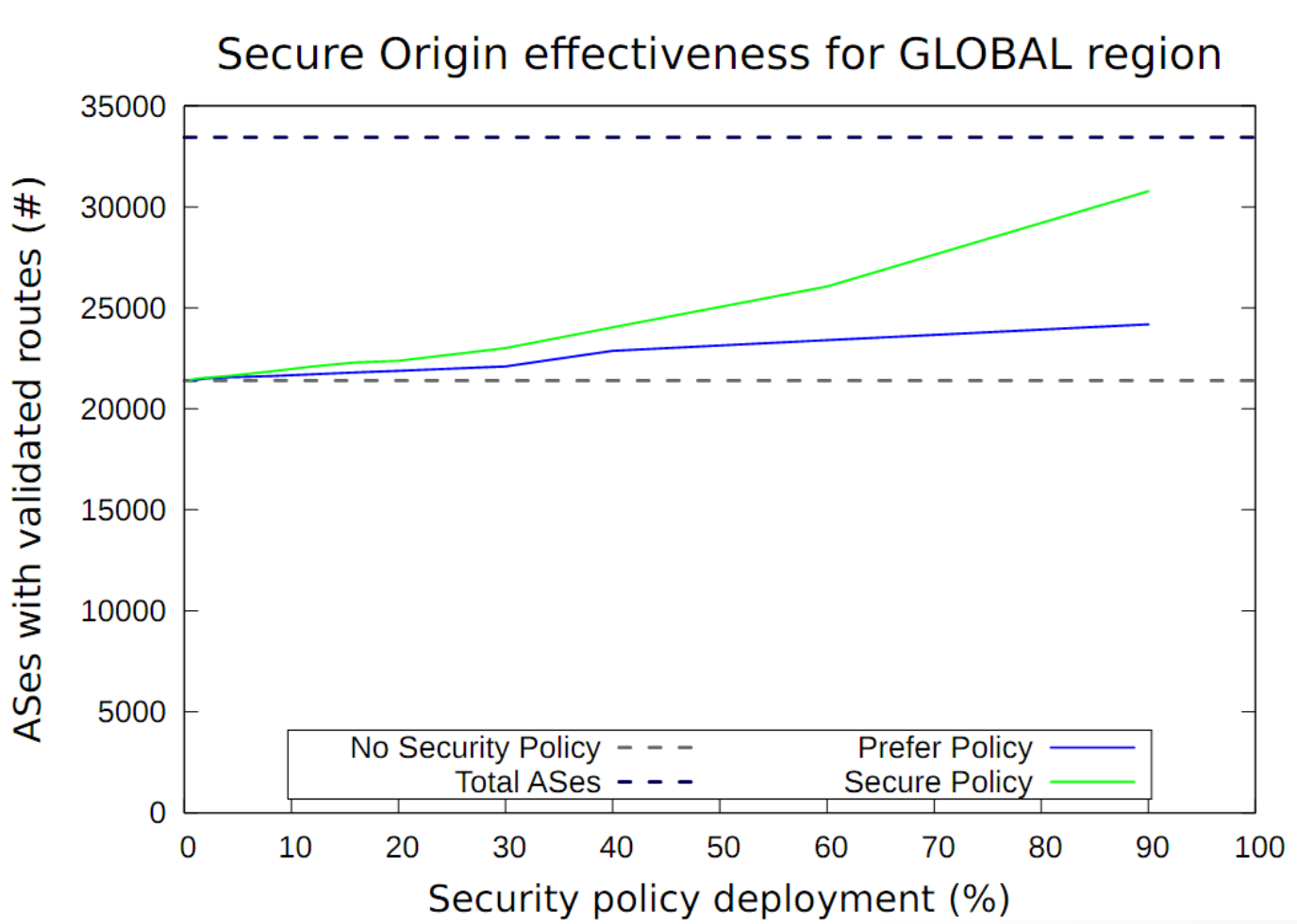


SOA: Global Deployment – Random Strategy



AS15169/ **Google Inc.** / #119 VS. AS45773 / **PERN AS Islamabad** / #10436

PV: Global Deployment – Top-down Strategy



AS1357/ **Vodafone Espana** / #4156 VS. AS35725 / **Cosmote RO** / #4118

Conclusions

- A bit better understanding of BGP
- More detailed simulations of security deployment
- Guide for favorable turnover for investments in BGP security
- Results show trends instead of specific AS behavior due to many levels of abstractions
- Future study: Include time dynamic experiments in study (convergence time of validated vs. rogue prefix announcements)