Pretty Good BGP and the Internet Alert Registry

Josh Karlin[1] Stephanie Forrest[1] Jennifer Rexford[2]

[1]University of New Mexico

[2]Princeton University

June 5th 2006
NANOG 37

http://cs.unm.edu/~karlinjf/pgbgp/

Pretty Good BGP

Main Idea: Delay Suspicious Routes

- Lower the preference of suspicious routes (24hr)

Benefits

- Network has a chance to stop the attack before it spreads
- Accidental short-term routes do no harm
- No loss of reachability
- Adaptive
- Simple

The PGBGP Algorithm

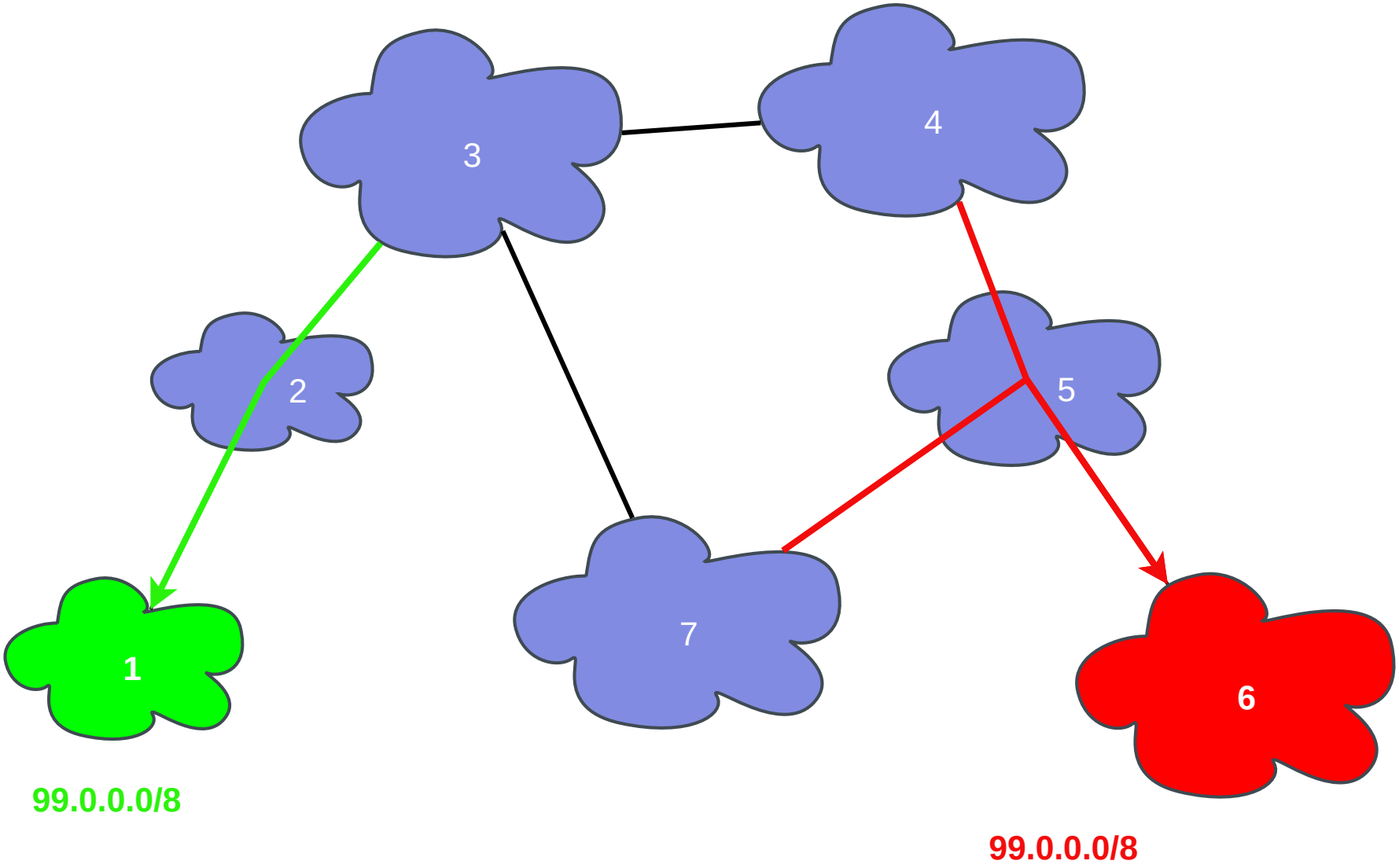
Detection

- Monitor BGP update messages
- Treat origin ASs for a prefix seen within the past few days as normal
- Treat new origin ASs as suspicious for 24 hours, then accept as normal (possible prefix hijack)
- Treat new sub-prefixes as suspicious for 24 hours, then accept as normal (possible sub-prefix hijack)

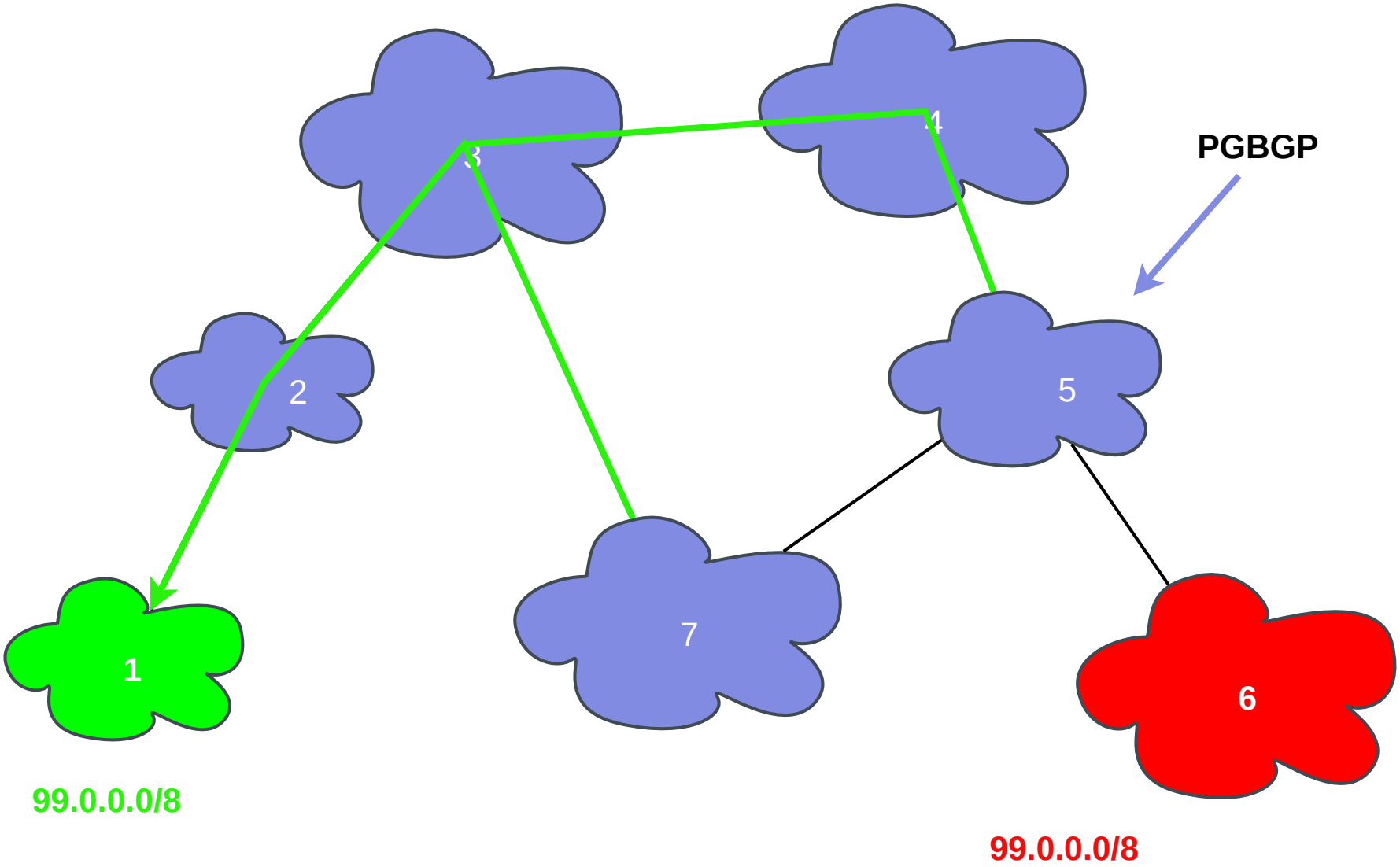
Response

- Suspicious origin AS routes are temporarily given low local preference
- Suspicious sub-prefixes are temporarily ignored (not forwarded to)

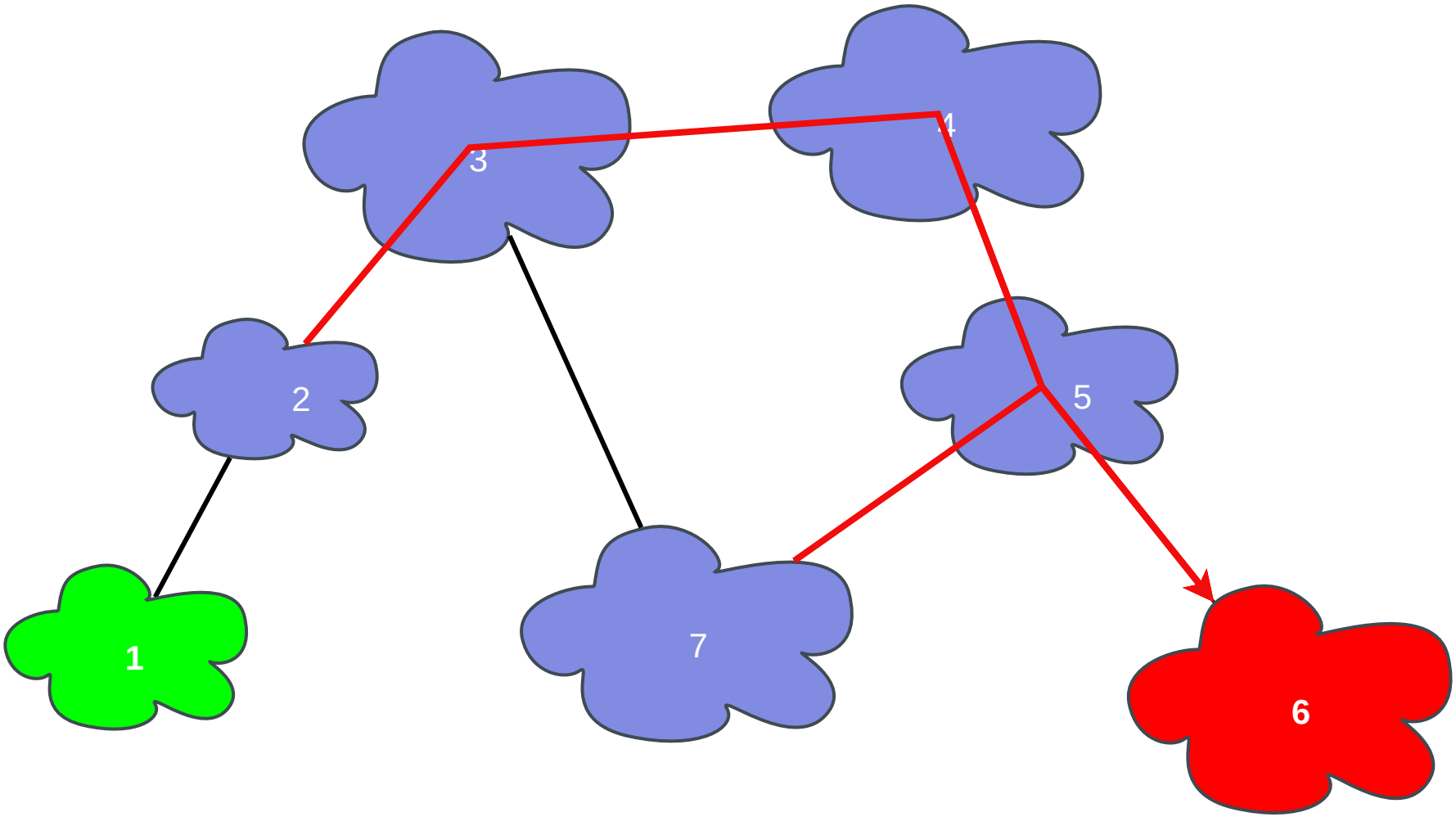
Example Prefix Hijack (without PGBGP)



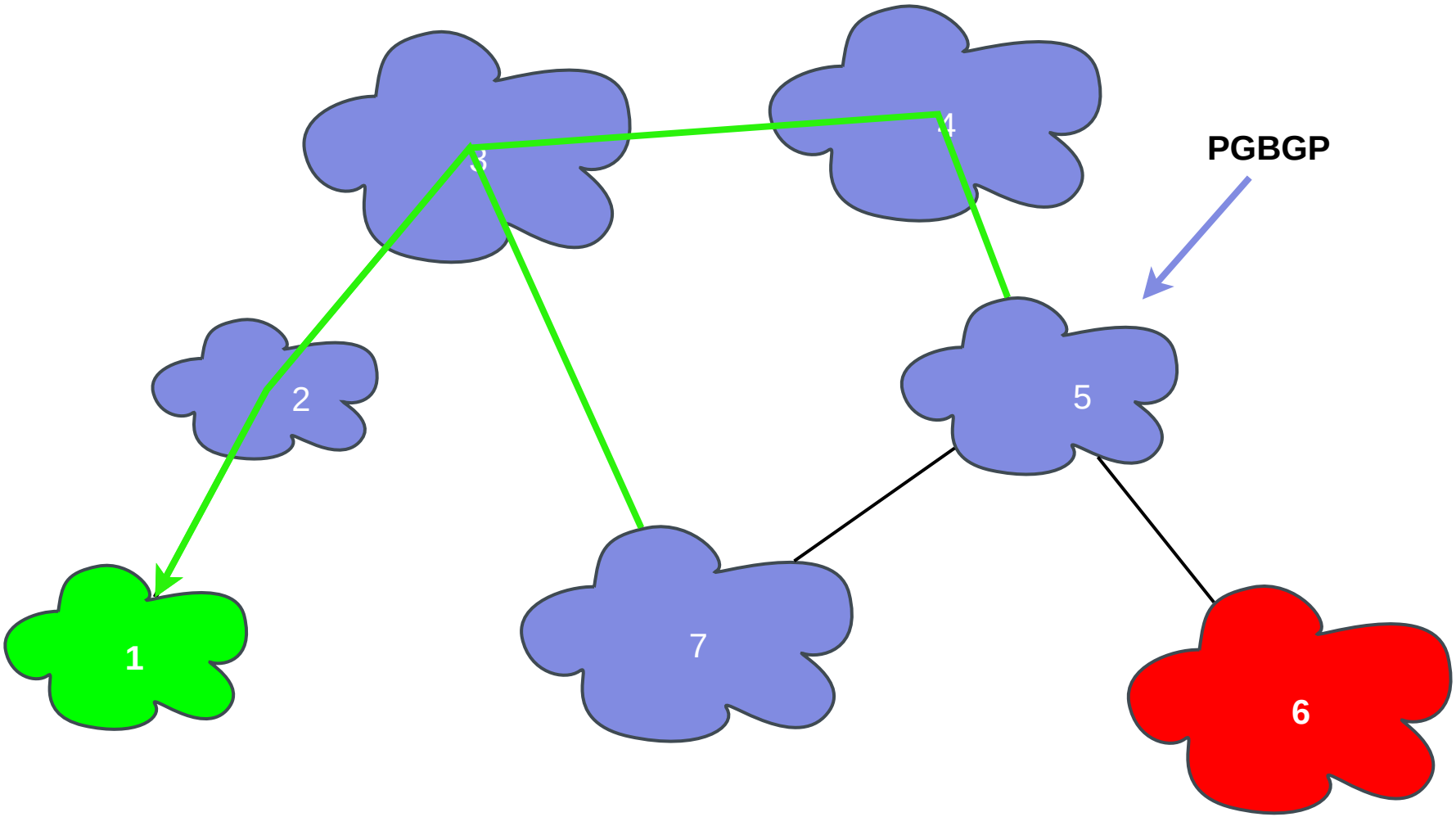
Example Prefix Hijack (with PGBGP)



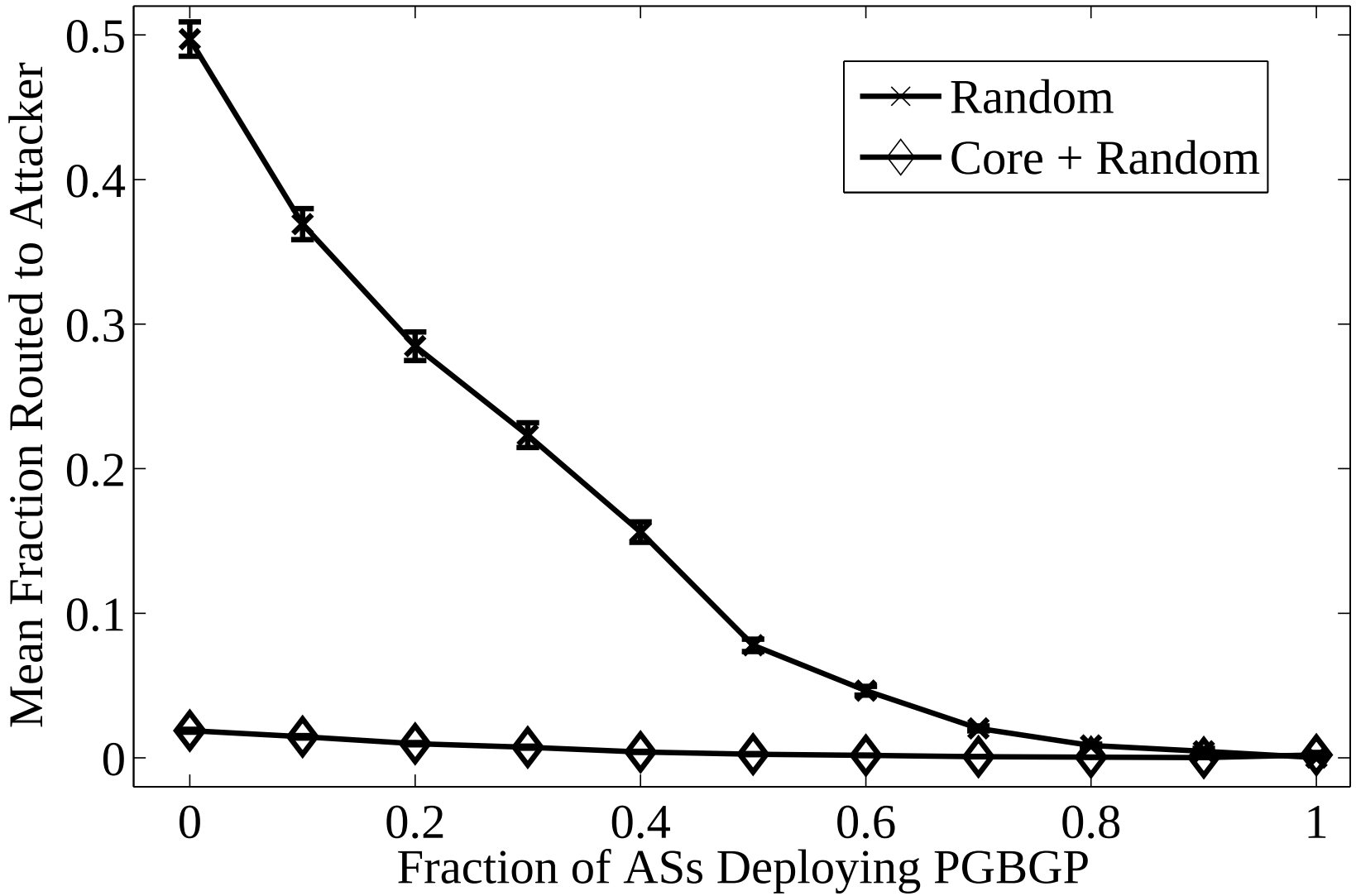
Example Sub-Prefix Hijack (without PGBGP)



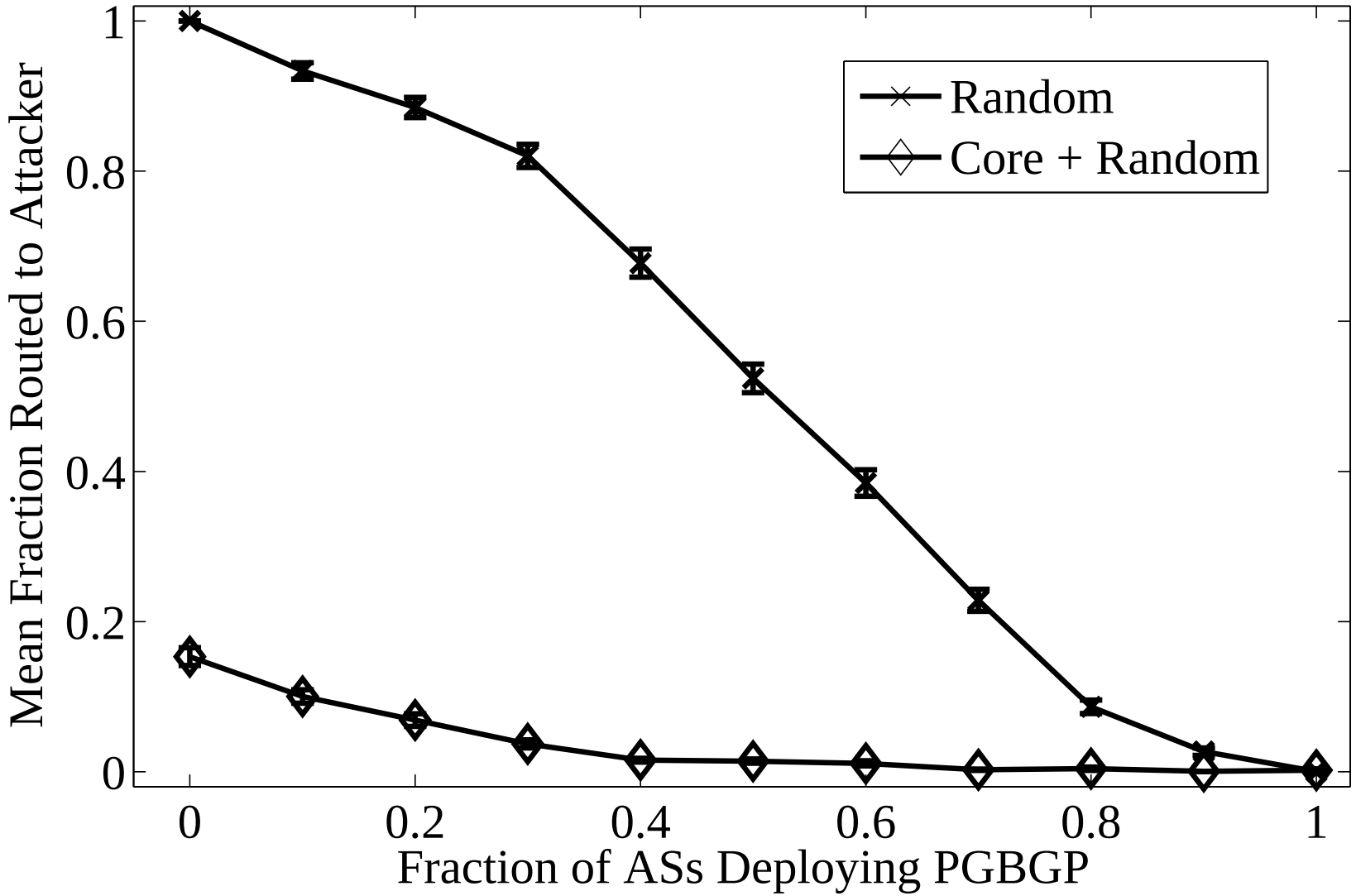
Example Sub-Prefix Hijack (with PGBGP)



Prefix Hijack Suppression



Sub-Prefix Hijack Suppression



Hijacks in the Wild

- 1997: AS 7007 sub-prefix hijacked most of the Internet for over 2 hours
- December 2005: Estimated 26-95 successful prefix hijacks (Boothe et al)
- January 2006: Panix's /16 stolen by Con Edison (as well as others) (Underwood)
- February 26 2006: Sprint and Verio briefly announced TTNET as the origin AS for 4/8, 8/8, and 12/8

Almost 10 years of hijacks and no viable solution has been deployed

The Internet Alert Registry

The IAR verifies hijack attempts

- A (near) real-time database of suspicious routes
- Email alerts are sent to those who opt-in for the ASs they choose to receive alerts for
  - Operators receive alerts only when their AS has caused the hijack, or is the victim of the hijack
- Tier-1 ASs receive one hijack alert per day on average
- We have a working prototype

What About Other Solutions?

Solutions with Guarantees (and lots of overhead)

- sBGP
- soBGP
- psBGP

Anomaly Detectors

- Whisper
- MOAS lists
- Geographic based

Good Practice

- Proper route filters

Conclusion

Why Pretty Good BGP?

- Maintains Autonomy
- Incrementally Deployable
  - No flag day
  - No change to the BGP protocol!
  - Effective with a small deployment
  - Only requires a software upgrade or change in configuration generation
- Minimum Operator Intervention

http://cs.unm.edu/~karlinjf/pgbgp/