BGP SECURITY
PAST, PRESENT & PIPA

Akmal Khan

08-27-2009

mmLab
Multimedia and Mobile communications Laboratory

Outline

- **Introduction**
- **Related Work**
- **Proposed Solution**
- **Experimental Results**
- **Conclusion**

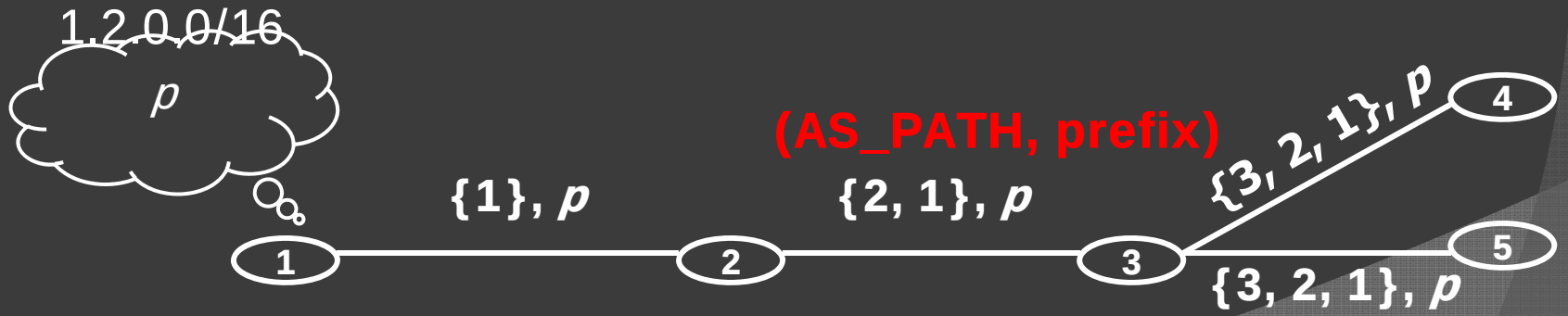
Multimedia and Mobile communications Laboratory

Internet Abstractions

- Collection of Hosts, Routers,Point of Presence(PoP's) or
- Autonomous System(AS)
  - An AS is a connected group of one or more IP prefixes run by one or more network operators which has a SINGLE and CLEARLY DEFINED routing policy(RFC 1930)

Border Gateway Protocol (BGP)

- Inter-domain routing protocol(Inter AS)
  - Critical Communications and Business Infrastructure!
- Vulnerable to different threats
  - Configuration/Human Errors
    - "Patches" applied as threats are exploded
    - E2E solutions require collaboration

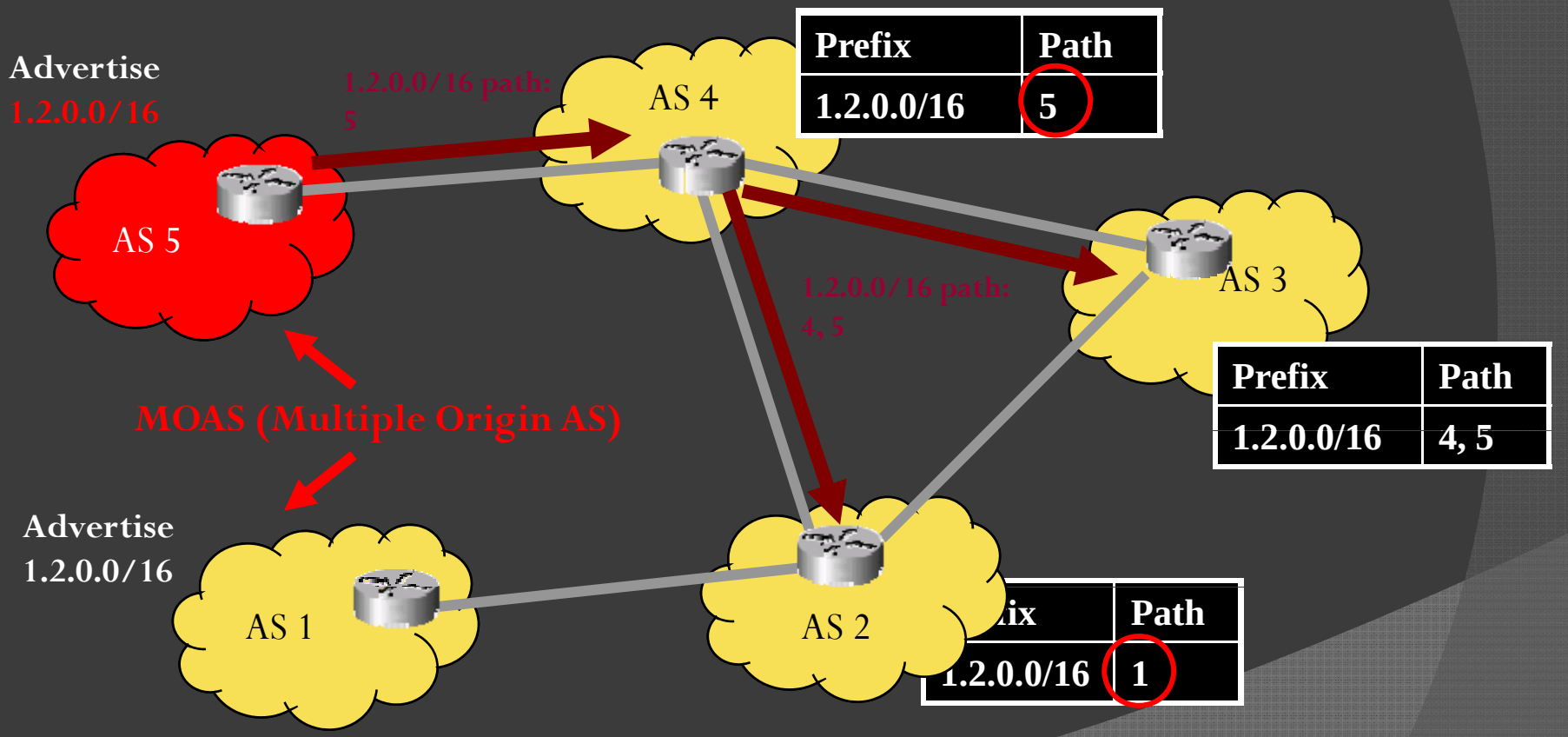


Prefix Hijacking 101

- Announce someone else's prefix
- Announce a more specific of a someone else's prefix
- Synopsis: You are trying to “steal” someone else’s traffic by getting it routed to you.
- Capture, sniff, redirect, manipulate traffic as you wish.

mmlab
Multimedia and Mobile communications Laboratory

Prefix Hijacking…simple case



Types of Prefix hijacking(PH)

[Type1]Prefix hijacking /Duplicate PH

- AS1 owns 1.2.0.0/16 but advertised by AS2

[Type2]Sub prefix hijacking

- AS2 advertises 1.2.3.0/24

[Type3]AS Path Spoofing

- AS5 announce [5 1] without having peering with AS1

[Type4]Independent PH

- AS2 use Bogons (unused address space)

[Type5]Man in the middle (MITM) Attacks

mmlab
Multimedia and Mobile communications Laboratory

BGP Prefix hijacking Incidents

- Did AS13214 really hijack the Internet?
  - http://bgpmon.net/blog/?p=80
- Cyclops detects global routing leak by AS13214
- Don't be afraid of AS3130..April 2009
  - http://cyclops.cs.ucla.edu/
- WorldofWarcraft.com and WoWarmory.com sub-prefix hijacked (July 2008)
- YouTube's prefix hijacked by Pakistan Telecom February 2008

mmLab
Multimedia and Mobile communications Laboratory

Outline

- **Introduction**
- **Related Work**
- **Proposed Solution**
- **Experimental Results**
- **Conclusion**

Multimedia and Mobile communications Laboratory

Major Research Groups

- University of California Los Angeles(Lixia Zhang)
  - Internet Research Lab(irl)
- CAIDA
- Colorodo State University (Dan Massey)
  - Network Security Research Group
- University of Princeton(Jennifer Rexford)
  - Incrementally Deployable Secure Interdomain Routing
- University of Michigan(Z.Morley Mao)
  - RobustNet Group

Major Research Groups

- National Institute of Standards and Technology(Advanced Network Technologies Division)
  - Trustworthy Networking
  - BGP Security and Routing Robustness
  - http://w3.antd.nist.gov/
- University of Swinburne (Geoff Huston)
  - CAIA
- UCL,Loouvain-la-Neuve,Belgium(Olivier Bonaventure)
  - INL:IP Networking Lab

mmLab
Multimedia and Mobile communications Laboratory

BGP Solutions Categories

- Prevention
  - S-BGP,SO-BGP,SPV
- Mitigation
  - Wang et.al,PG-BGP,Zhang et al.Anycast Routing
- Detect & Alert
  - myASN,IAR,Phas->Cyclops,BGPmon.net
- Detect & Recover
  - Probabilistic IP Prefix Hijacking(PIPA)

Table 1 : Prefix Hijacking Solutions

	Detection System	Alarm Type	Prefix/ Duplicate PH	Subprefix PH	Super/ Independent PH	Path Spoofing	MITM
PHAS [mohit et al]	H	Origin, Last Hop, Sub Allocation	Y	Y	N	limited	N
PG-BGP [J.Karlin et al]	H	Prefix, Sub Prefix	Y	Y	N	Y	limited
K.Sriram et al. [	H+R	N	Y	Y	N	Y	N
Nemecis	R	N	Y	Y	N	N	N
Hu et al.	H	N	Y	Y	N	Y	N

Table 1 : Taxonomy of Prefix Hijacking Solutions (PH: Prefix Hijacking, Y: yes, N: No, H: History, R: Registry, Un: Unreachability, MITM: Man In The Middle)

Cyclops..AS-Centric Visualization tool

- Data sources
  - BGP routing tables + updates: Route Views, RIPE, Abilene, CERNET BGP View
  - Route Servers: Packet Clearing House, UCR, traceroute.org, Route Server Wiki
  - Looking Glasses: traceroute.org, NANOG, Looking Glass Wiki
- Others
  - Mapnet,Otter,HERMES,VAST,FixedOrbit

http://cyclops.cs.ucla.edu/

Some More tools

- PCH-Prefix Sanity Checker
- RIPE-MyASN Service
- BGPPlay
- BGPmon.net

Multimedia and Mobile communications Laboratory

Tools to use & get inspiration

Linux Distribution(Ubuntu),Java,C/C++,Perl,Python, mySQL,…

- Quagga 0.99.14
- IRRd - Internet Routing Registry 2.3.9
- Irrtoolset 4.8.5
- IrrPowerTools
- StraighRV
- MRT dump file manipulation toolkit(MDFMT) version 0.2
  - BGP4MP
  - TableDump V2
- Prefixanalyzer
- Pybgpdump
- Dpkt 1.6
- LinkRank Beta 02

- ....

mmLab
Multimedia and Mobile communications Laboratory

Outline

- **Introduction**
- **Related Work**
- **Proposed Solution**
- **Partial Experimental Results**
- **Conclusion**

Multimedia and Mobile communications Laboratory

PIPA Data Sources

- RIR/Internet Route Registry(IRR)
  - Registration information/Policy Information
    - RADb,RIPE,ARIN,APNIC
- BGP Data Collectors
  - RouteViews(240), RIPE-RIS(>600)
    - No. of BGP collector deployed around the world
- New Data Source [unreachability information]
  - Hubble Project/iPlane[Ethan K.et al]

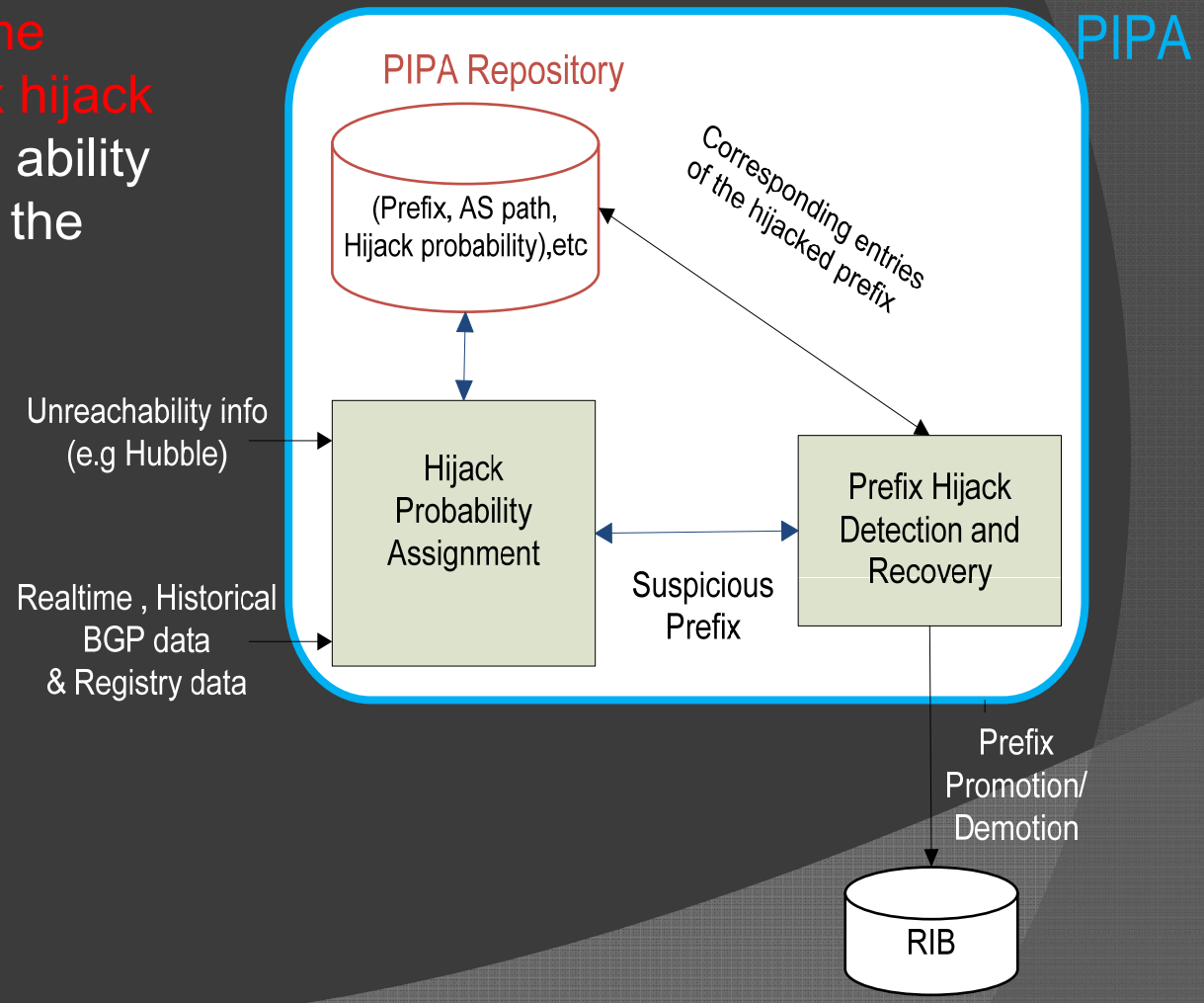
How is Unreachability helpful?

- Internet Goals : Global Reachability
- Prefix hijacking can affect some of the Ases.
  - E.g. AS5 hijacked the Prefix of AS1 and black hole all the traffic
  - Applications in some AS will observe Unreachability
- There are projects like Hubble/iPlane which provides information about the blackholes & unreachabilities duration
  - Help detecting prefix hijacking
  - Pinpointing the location of hijacker

Probabilistic IP Prefix Authentication (PIPA)

Continuously update the Probability of prefix hijack based on its reach ability information around the world

Possible promotion /demotion of historically best BGP Path of certain prefix



Multimedia and Mobile communications Laboratory

Hijack Probability Assignment

- Every Prefix can be assigned a Hijack Probability based on it's conformance with
  - Historical Standings
  - Registry Standings
  - Real time Unreachability statistics
- Non conformance with History/Registry can raise early Alarms and Recovery process can be started.
  - Probability score can be continuously updated based on real time statistics i.e. BGP updates, etc.

mmLab
Multimedia and Mobile communications Laboratory

Prefix Hijack Detection Challenge

- How to differentiate between different unreachability
  - Unreachability due to equipment failures , line cuts, etc.
- MITM: When there are no un-reachabilities
- How to detect MOAS conflicts
  - Registry data if accurately updated
  - Maintaining knows AS home Set
    - IP Prefix: 1.2.0.0/16
    - Owner AS: AS1
    - IP Prefix Homes : AS1,…

mmLab
Multimedia and Mobile communications Laboratory

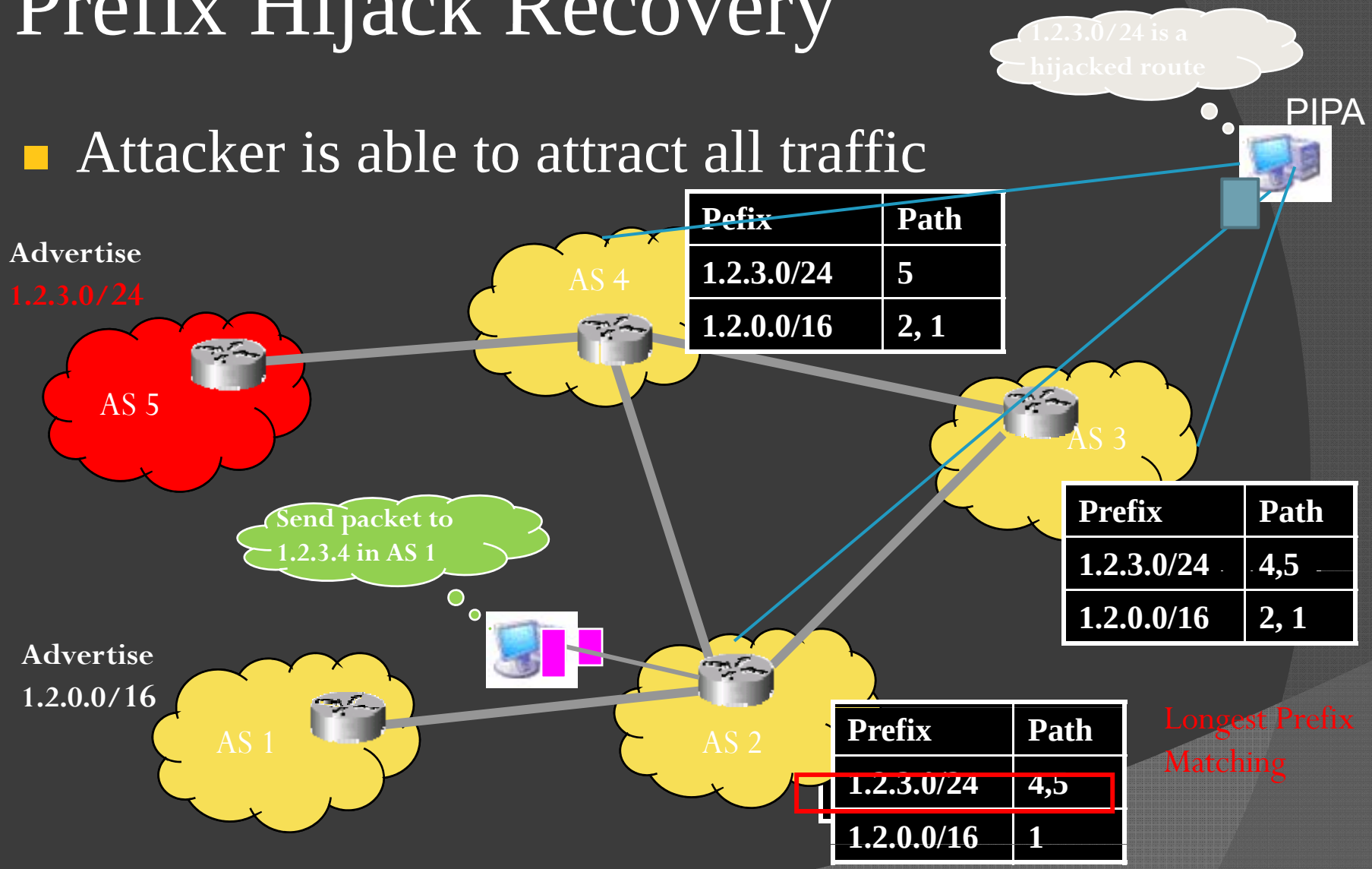
Prefix Hijack Recovery

- Network operator announces more specific prefix to recover from Prefix hijack situation
  - Longest Prefix Matching Wins
  - But what if that is the one already hijacked.
    - Contact the malicious/misconfigured party or its provider
- PIPA based on its results can suggest to particular AS to use Previous used route which it was using before the introduction of new malicious or erroneous prefix

mmLab
Multimedia and Mobile communications Laboratory

Prefix Hijack Recovery

- Attacker is able to attract all traffic



Pefix	Path
1.2.3.0/24	5
1.2.0.0/16	2, 1

Prefix	Path
1.2.3.0/24	4,5
1.2.0.0/16	2, 1

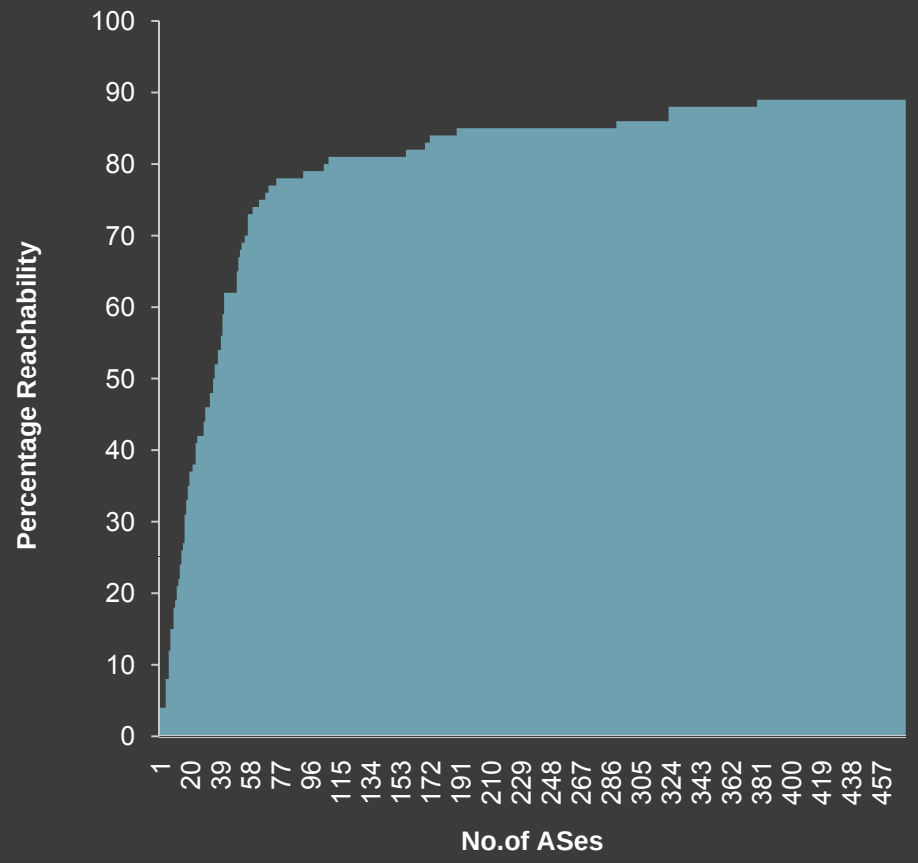
Prefix	Path
1.2.3.0/24	4,5
1.2.0.0/16	1

Outline

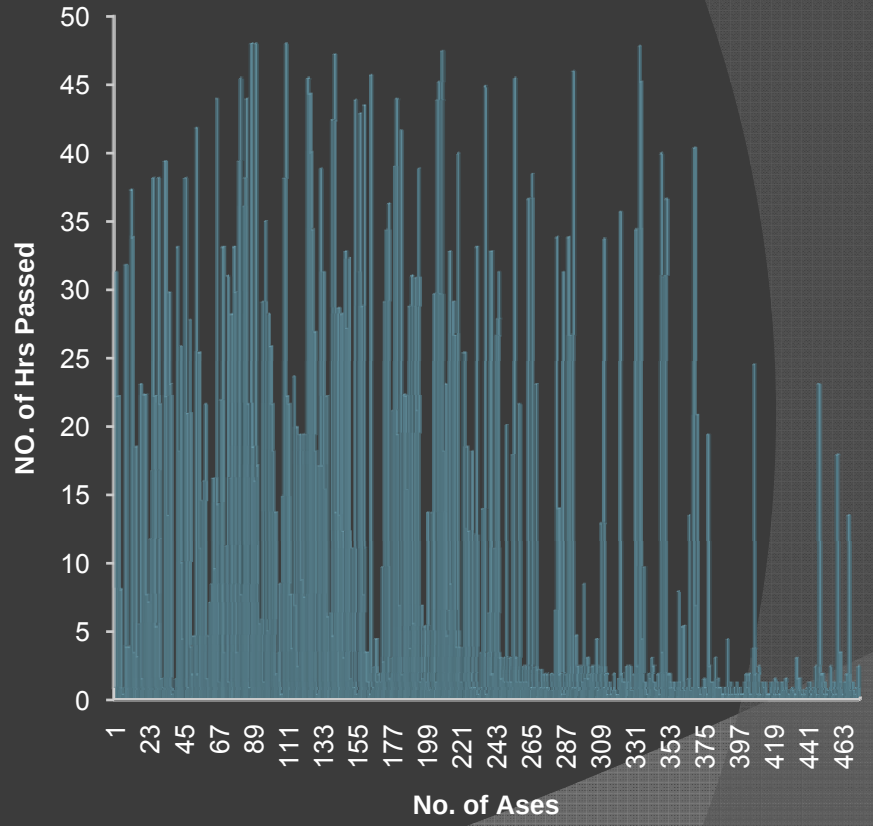
- **Introduction**
- **Related Work**
- **Proposed Solution**
- **Experimental Results**
- **Conclusion**

Multimedia and Mobile communications Laboratory

Ases Reachability



No.of Hrs Passed



mmLab
Multimedia and Mobile communications Laboratory

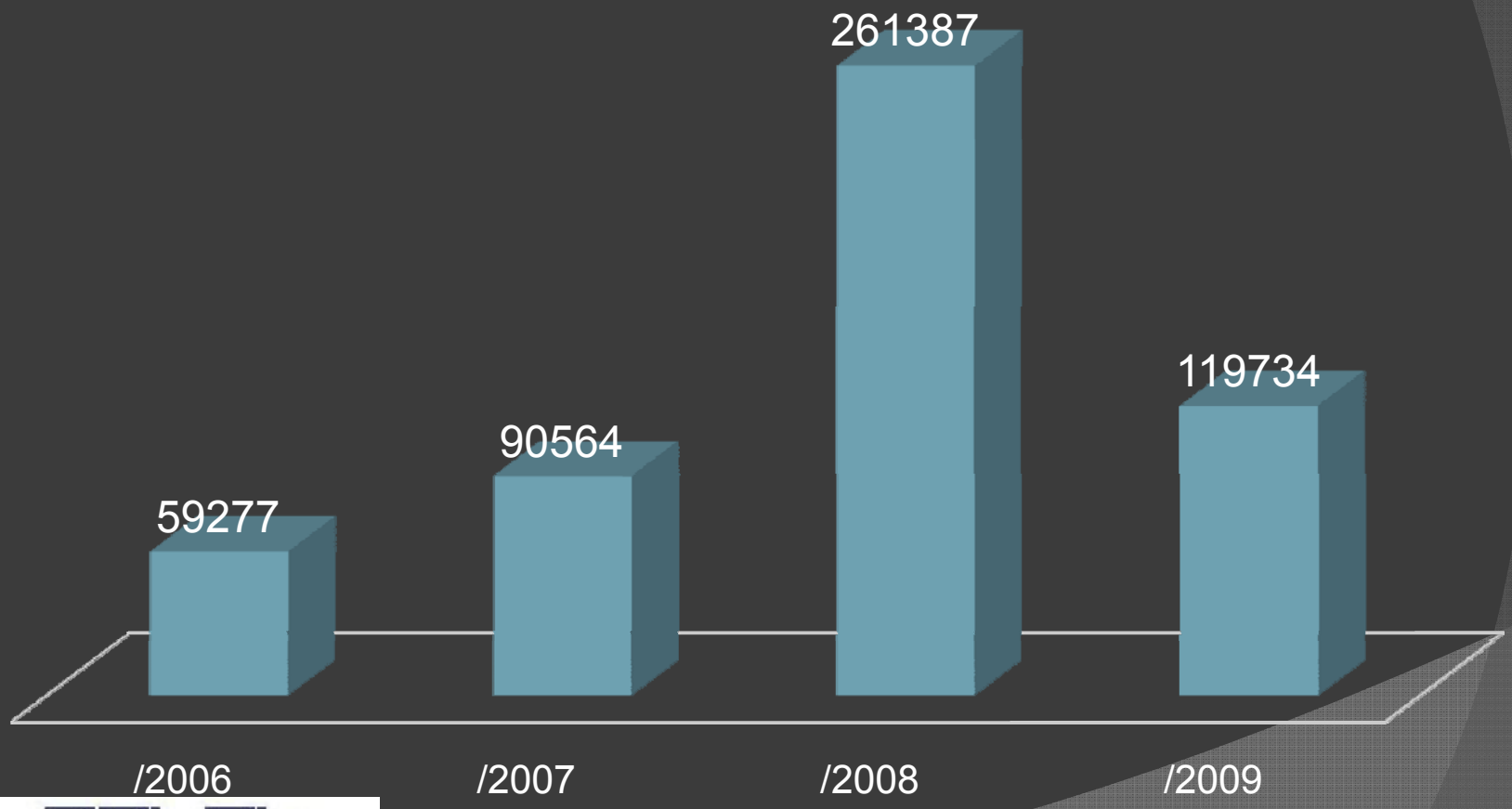
Experimental Methodology

- Initial experimental Results
  - Comparison of False Alarms with PGBGP
  - Data collected
  - PGBGP suspicious Announcements(5/2006-3/2009)
    - Provided by Josh Karlin
    - Public RIR/IRR data
    - Hubble unreachability statistics
  - Run checks to see whether routes are suspicious as announced by PGBGP IAR.

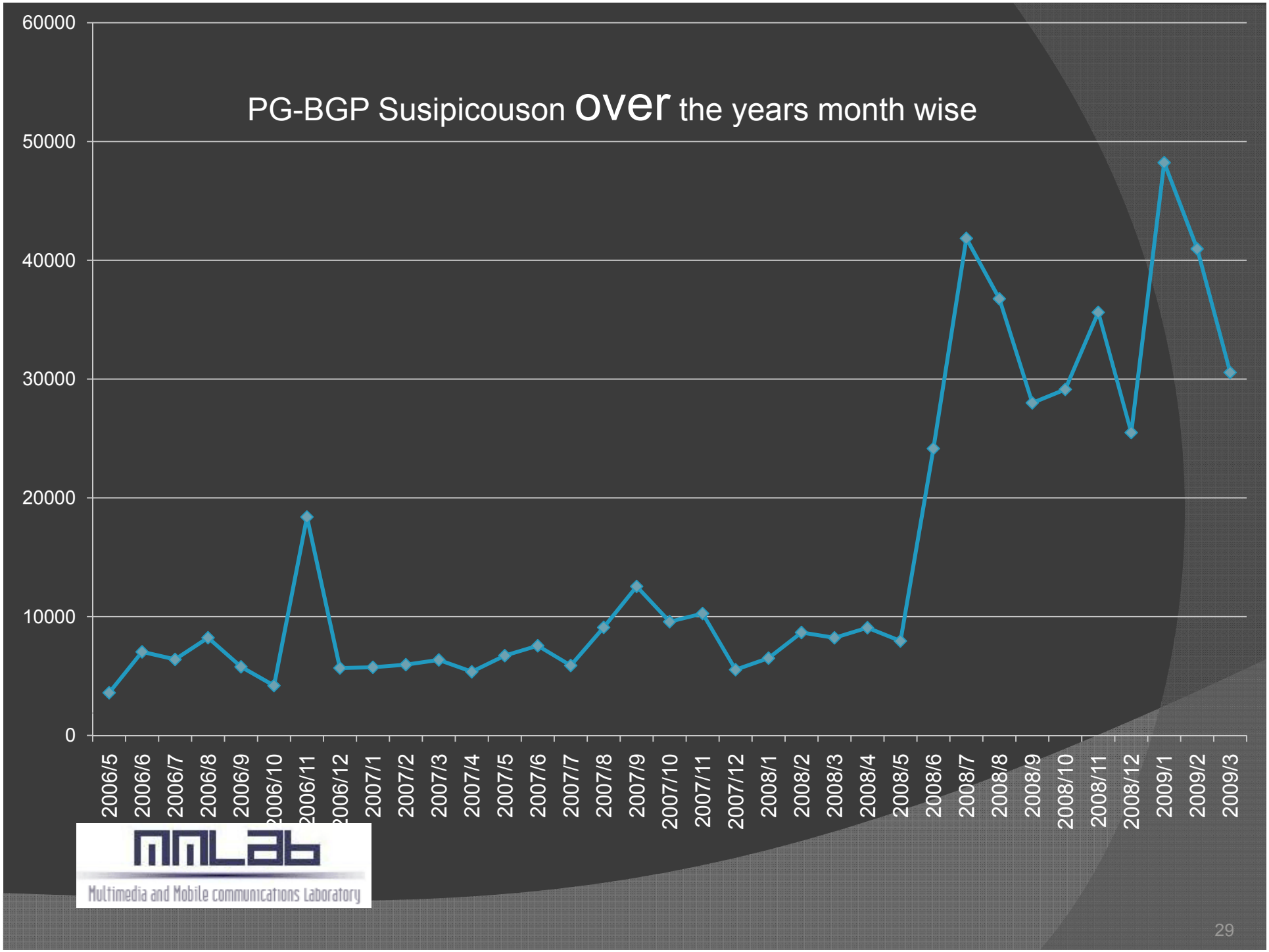
    Result: Too much suspicion is not good

mmLab
Multimedia and Mobile communications Laboratory

PG-BGP Alerts 5/2006-3/2009



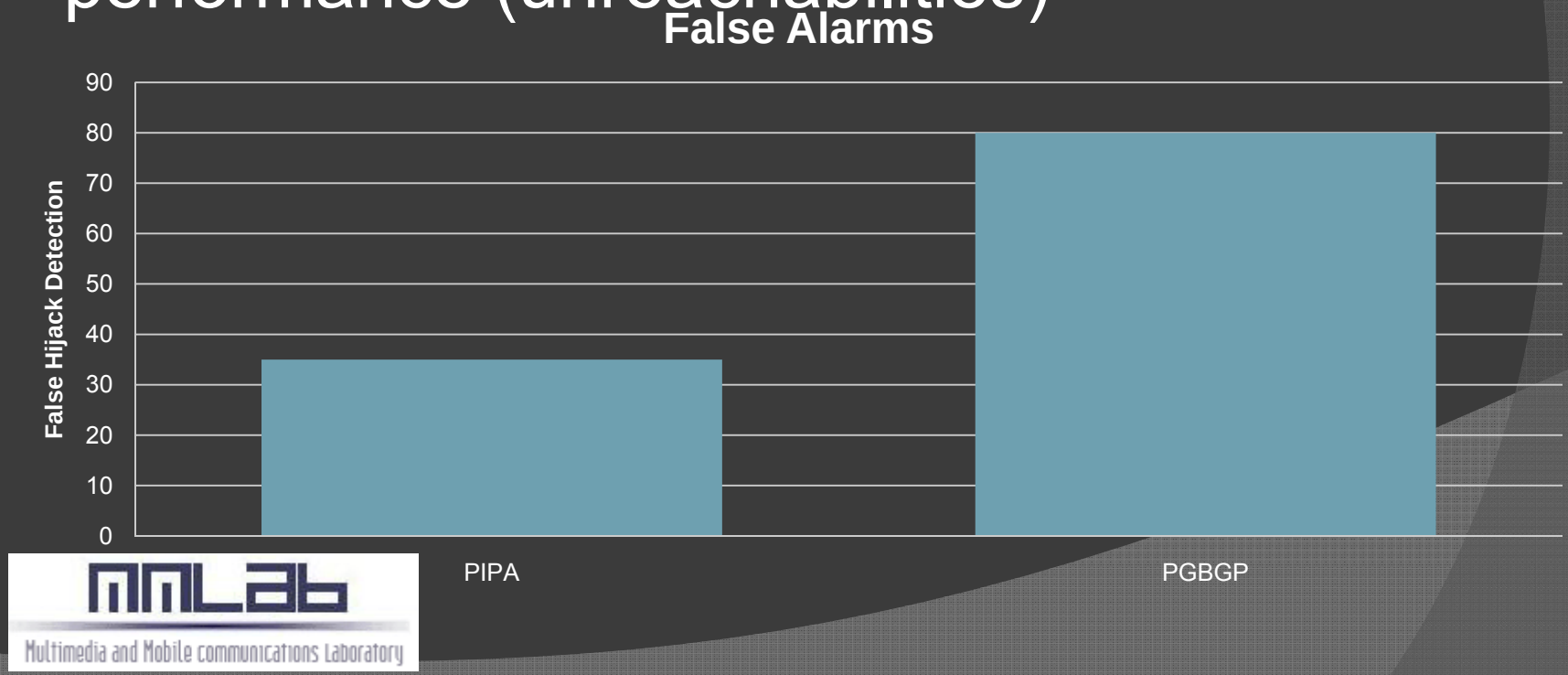
Multimedia and Mobile communications Laboratory



mmLab
Multimedia and Mobile communications Laboratory

Comparison with PGBGP

- PGBGP-marks new routes suspicious if they do not conform to the History BGP[24 hrs]
- PIPA—Let them work but observer their performance (unreachabilities)



Multimedia and Mobile communications Laboratory

Conclusion & Future Work

- Extensive Review of existing solutions
- Inclusion of New data source for PH detection
  - “unreachability” data collected in real time.
- Can Internet Self recover from PH?
  - Proposed PH recovery mechanism
  - Where can we find self healing property of Internet?
- We are working on the full level implementation and experimental results of

Multimedia and Mobile communications Laboratory

Conclusion & Future Work

- Extensive Review of existing solutions
- Inclusion of New data source for PH detection
  - "unreachability" data collected in real time.
- Can Internet Self recover from PH?
  - Proposed PH recovery mechanism
  - Where can we find self healing property of Internet?
- We are working on the full level implementation and experimental results of

Multimedia and Mobile communications Laboratory

Some ? To myself

- What about the current state of implementation of PKI for DNSSEC/Who IS.
  - How can we include/adopt that?
- How to deploy PIPA?
- How PIPA detects MITM?
- ??

References

- [Ethan K. et al]Studying Black holes in the Internet with Hubble http://hubble.cs.washington.edu
- [M. Lad et.al] PHAS: A Prefix Hijack Alert System,|| in USENIX Security Symposium 2006.
- [Hu et al.] Accurate Real-time Identification of IP Prefix Hijacking,*I EEE Security and Privacy, Oakland, 2007*
- [J. Karlin, et al.] Pretty Good BGP: Improving BGP by Cautiously Adopting Routes,IEEE ICNP 2006, Santa Barbara, CA, USA, Nov. 2006
  - Internet Alert Registry[http://iar.cs.unm.edu]
- [G. Siganos et al.],A Blueprint for Improving the Robustness of Internet Routing,Security '06, 2006.

mmLab
Multimedia and Mobile communications Laboratory

Thank You

Questions

raoakhan@mmlab.snu.ac.kr

mmlab
Multimedia and Mobile communications Laboratory