Monitoring Internet Health at Scale

Romain Fontugne
IIJ Research Lab

November 12, 2018, AINTEC, Bangkok

Collaborations/Publications

Collaborators

- Anant Shah (Verizon)
- Emile Aben (RIPE NCC)
- Cristel Pelsser (Strasbourg University)
- Randy Bush (IIJ)

References

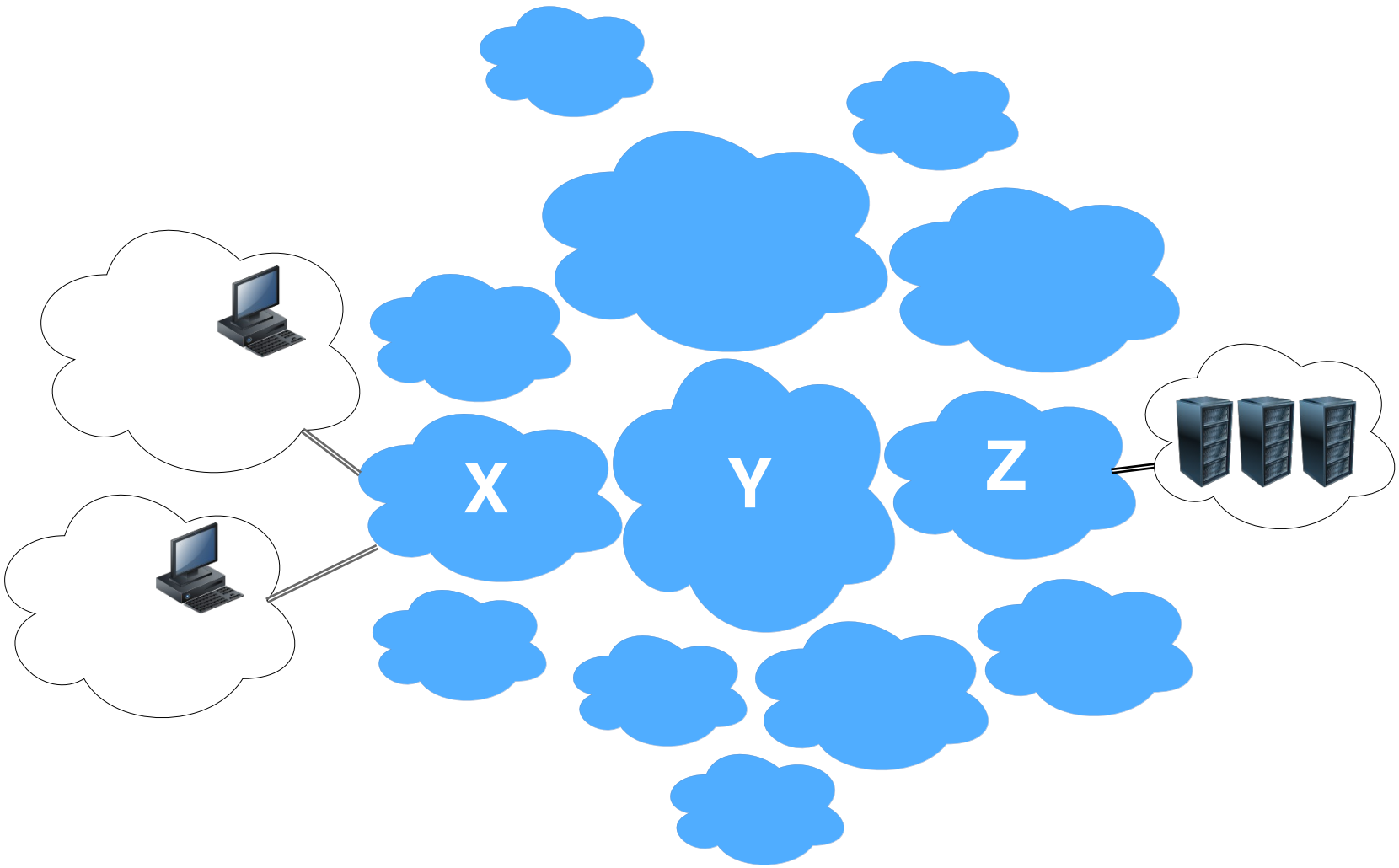
- A. Shah et al. "Disco: Fast, good, and cheap outage detection", TMA'17.
- R. Fontugne et al. "Pinpointing Delay and Forwarding Anomalies Using Large-Scale Traceroute Measurements", IMC'17.
- R. Fontugne et al. "The (thin) Bridges of AS Connectivity: Measuring Dependency using AS Hegemony", PAM'18.

Outline

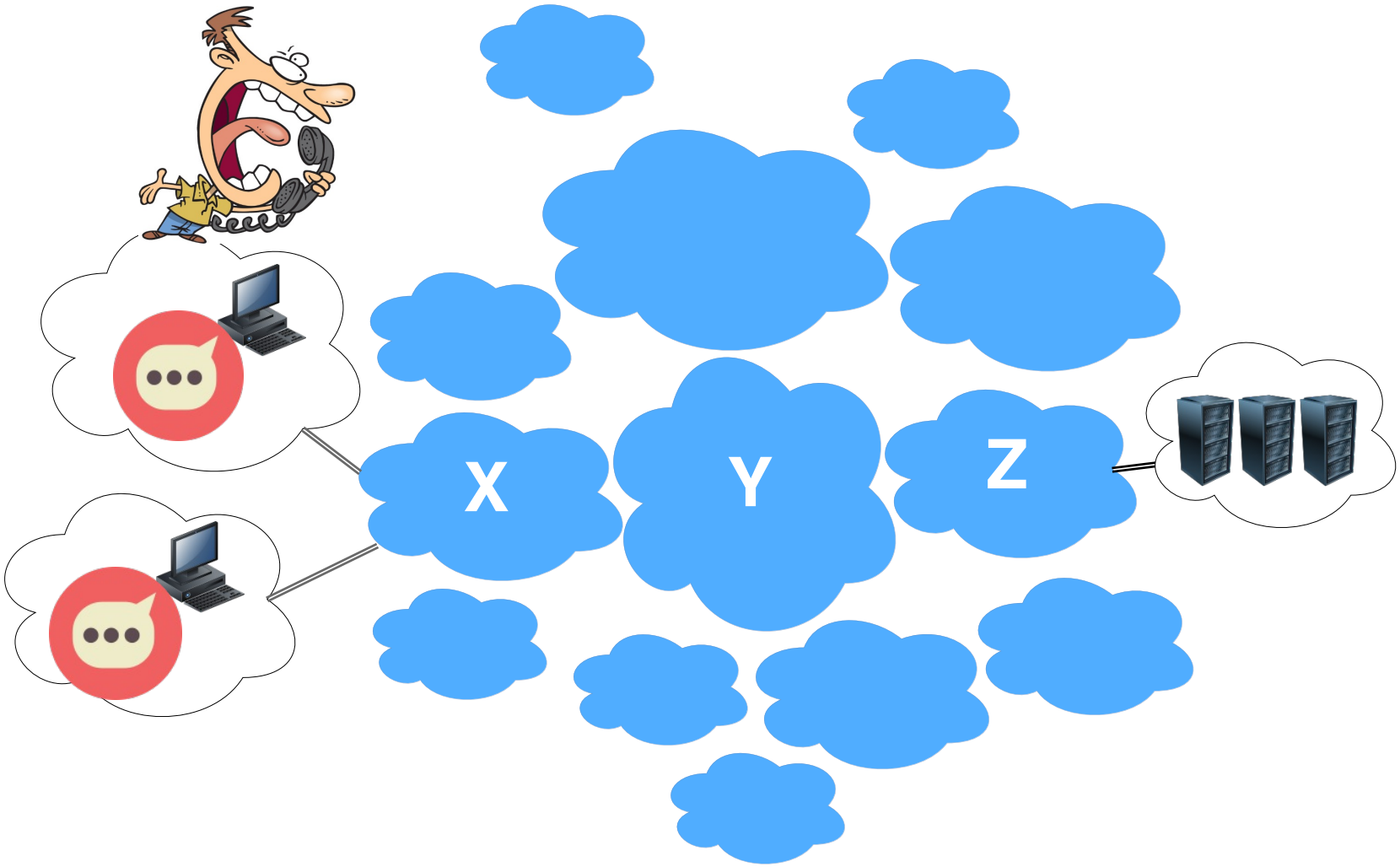
Monitoring Internet Health at Scale

- Why do we monitor networks conditions?
- What are the main difficulties?
- Overview of Internet Health Report (IHR)
  - Delay & forwarding anomaly detector
  - Outage detector
  - AS dependency

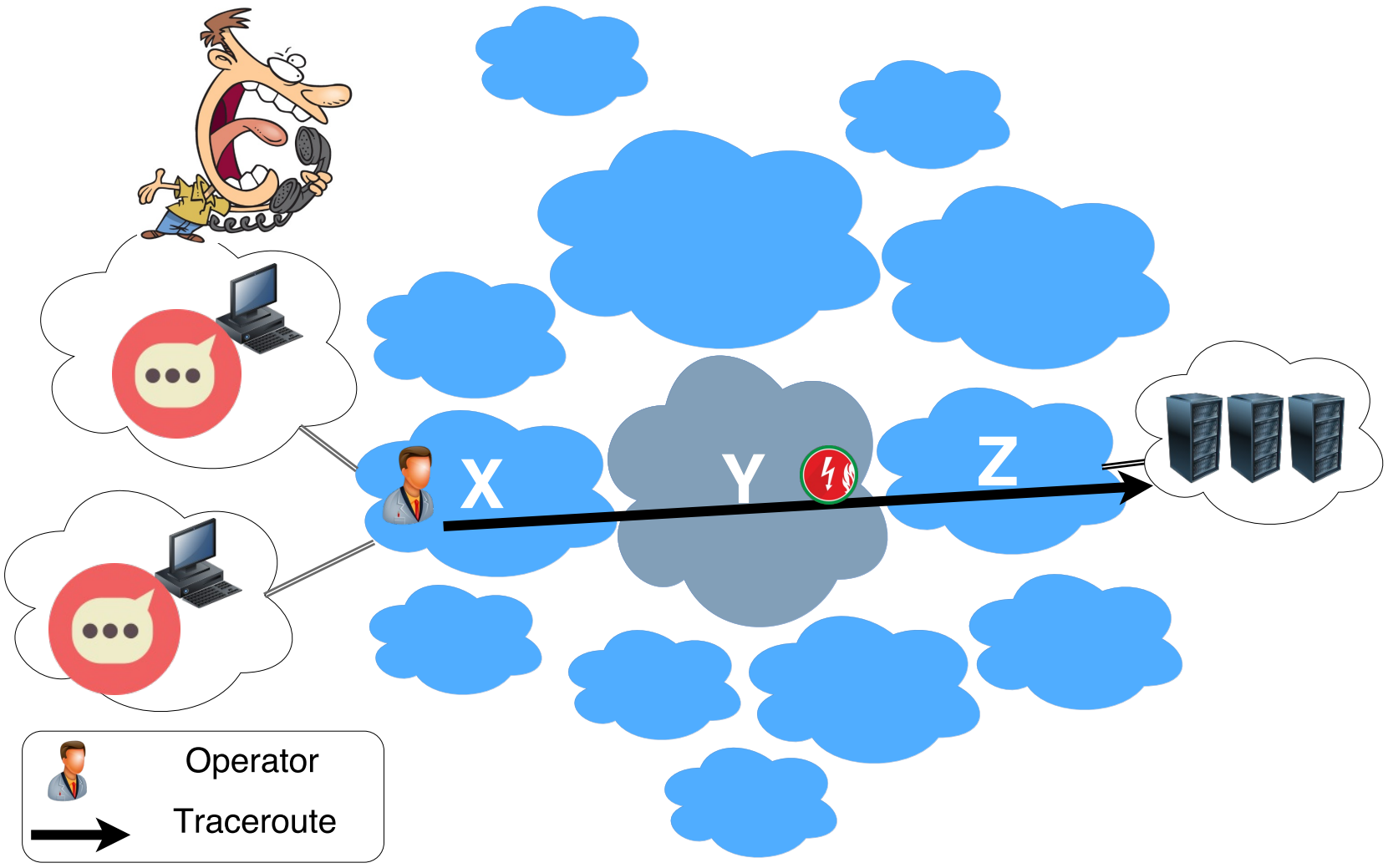
Internet: a network of networks



Internet: a network of networks



Internet: a network of networks



Internet's Health?

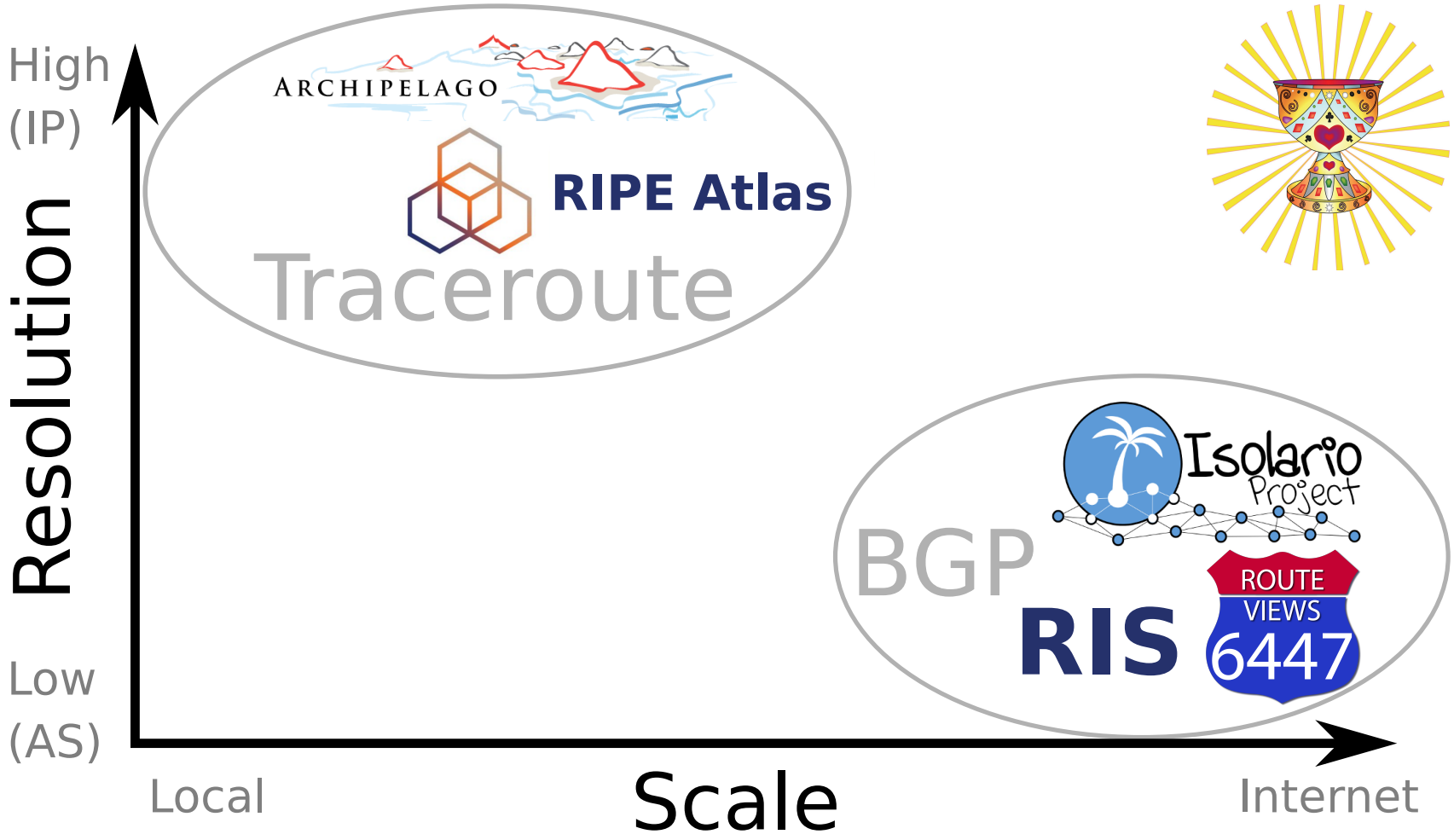
Goal: Monitor Internet's Health

- Automatically pinpoint connectivity issues

Main Challenges:

- Limited views on remote networks
- Slow process
- Internet is huge
  - Over 60k autonomous systems
- Constantly evolving

Problem Space / Data sources



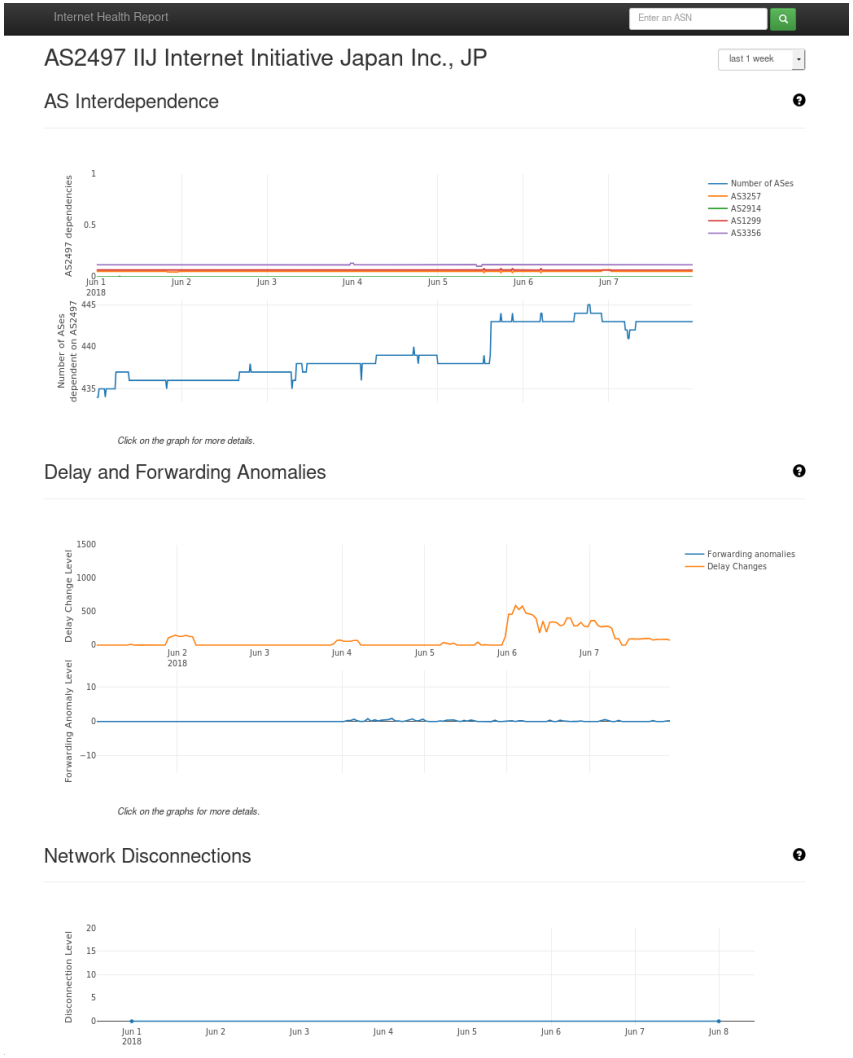
Internet Health Report: Current Status

Internet Health Report

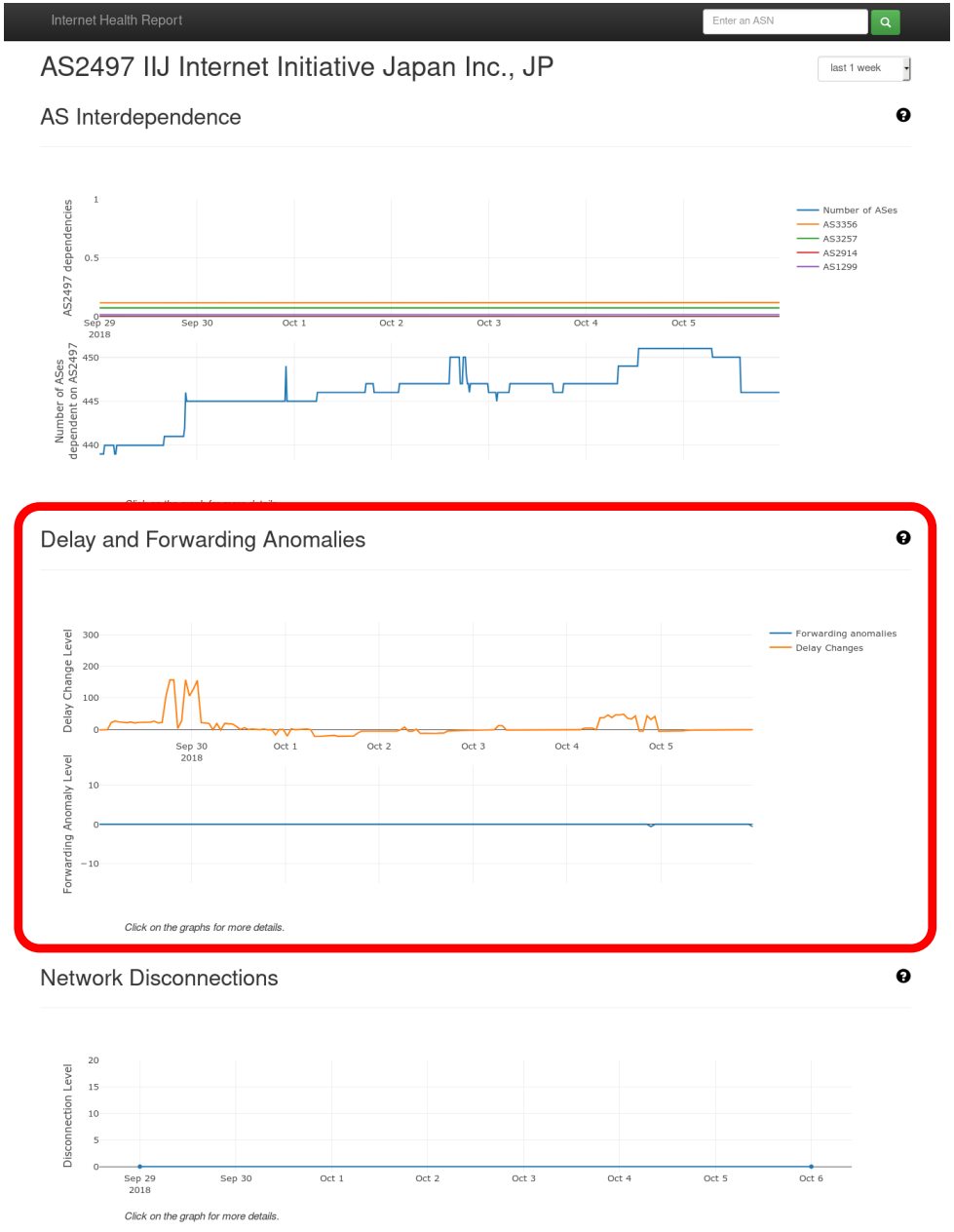
- `https://ihr.iijlab.net`
- Results publicly available
- Open source code

Three main components

- Delay/forwarding anomaly detection (traceroute)
- Outages detection (Atlas)
- AS dependencies monitoring (BGP)



Delay/Forwarding anomaly detection



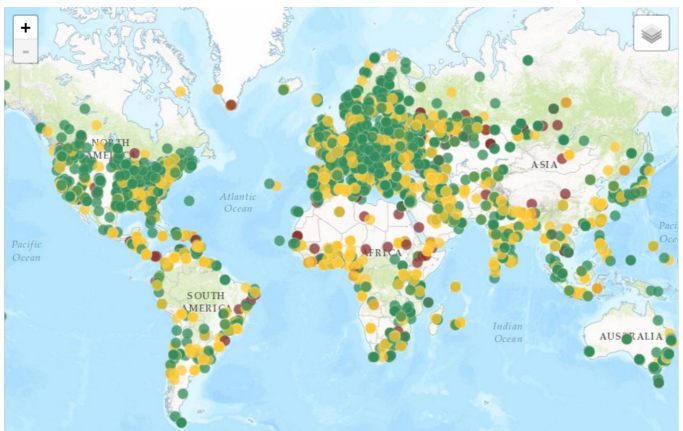
Goal and Dataset

Goal

- Monitor abnormal delays and routes in traceroutes

RIPE Atlas measurement platform

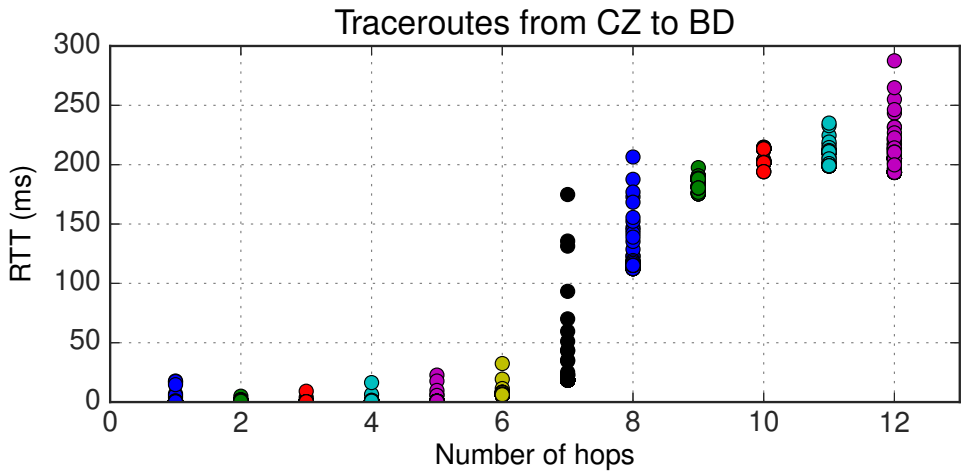
- About 10k devices world-wide
- Pings, traceroutes, DNS, NTP, HTTP, SSL measurements
- Long-lasting measurements

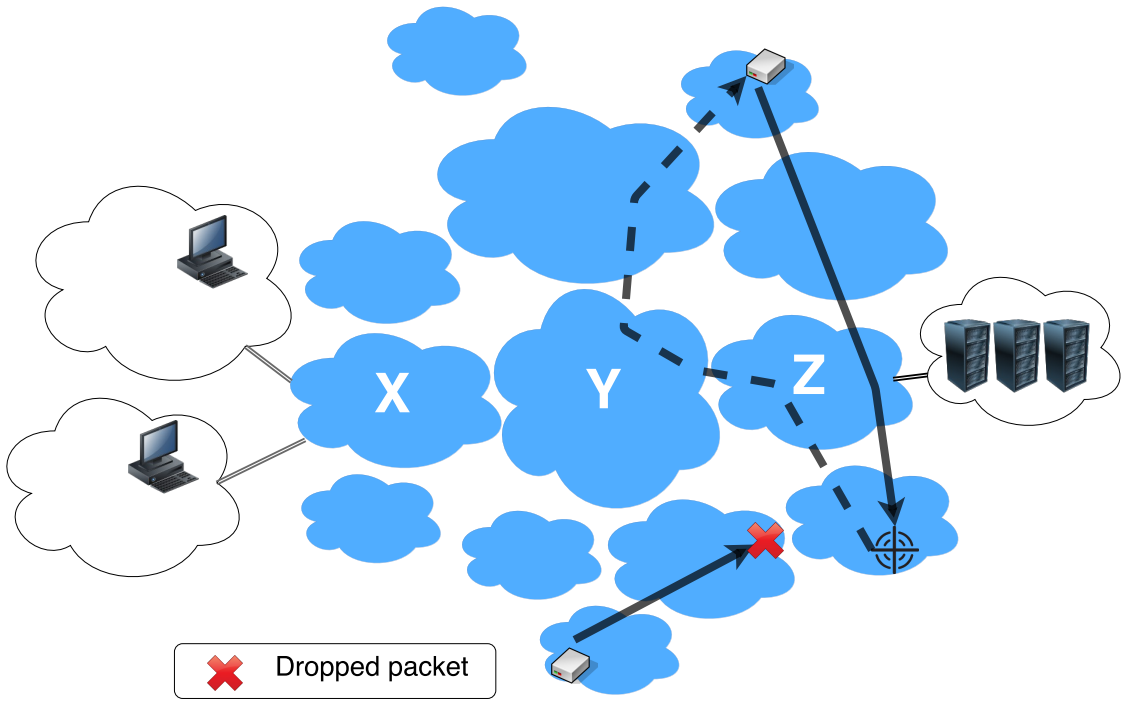


Monitor delays with traceroute?

Challenges:

- Noisy data
- Traffic asymmetry
- Packet loss





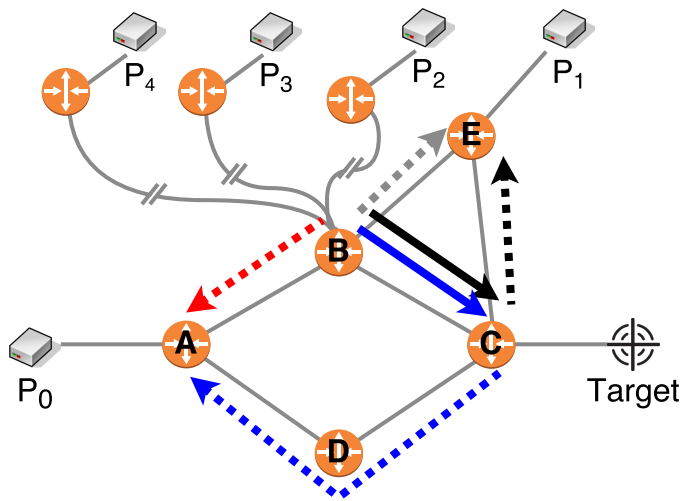
Approach (1)

Monitor in-network delays

- Combine traceroutes from multiple probes
- Compute the median RTT for common hops

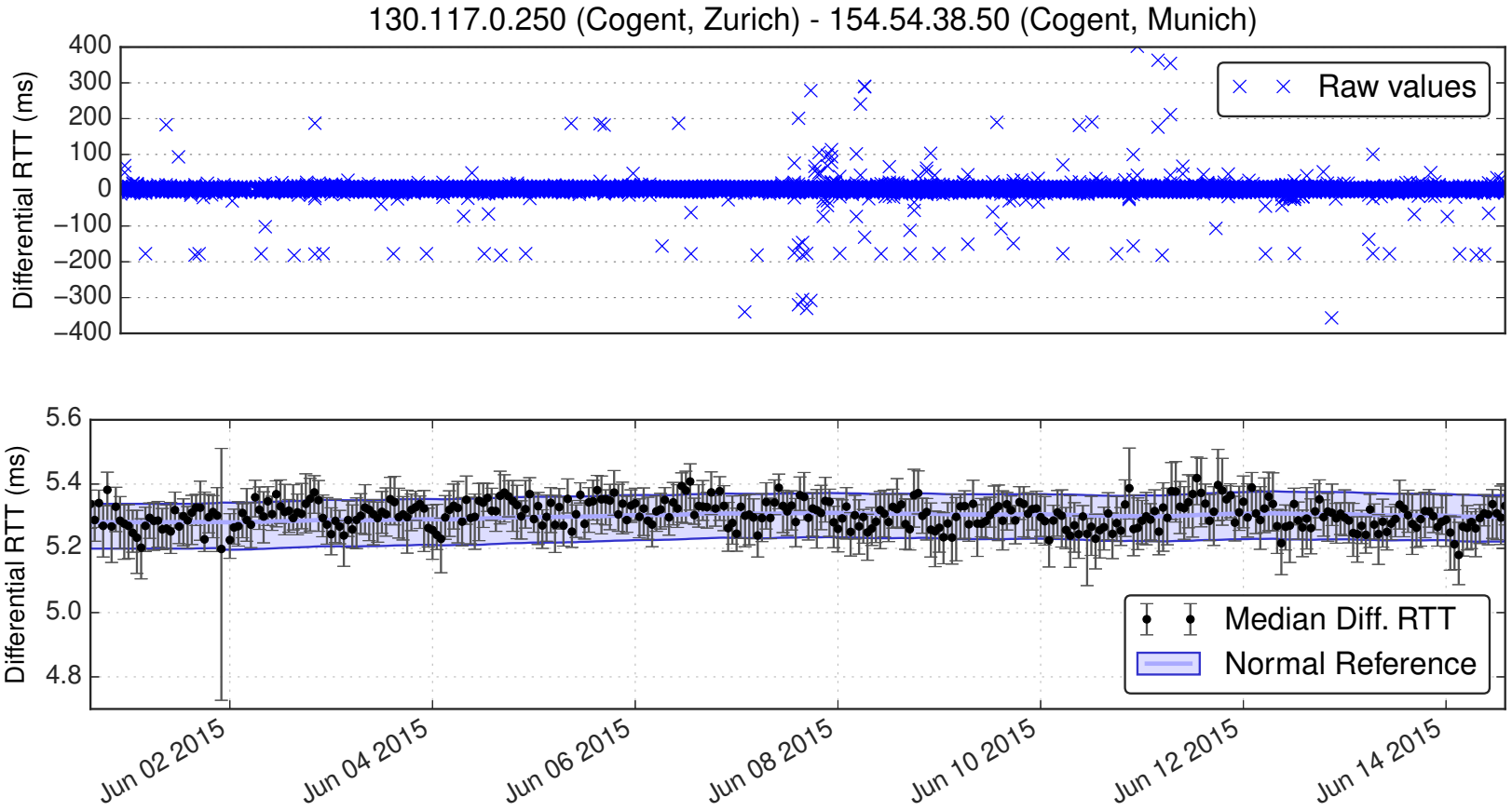
Benefits

- Robust to noise
- Mitigate traffic asymmetry problems



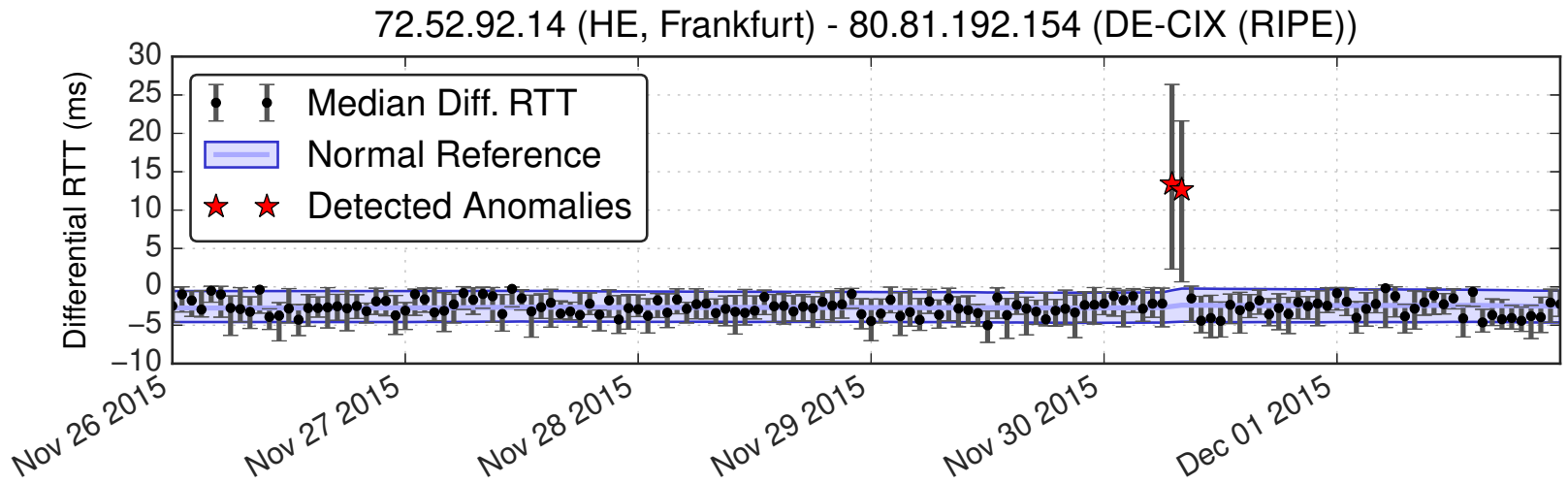
Median Diff. RTT: Example

Tier1 link, 2 weeks of data, 95 probes:



- **Stable** despite noisy RTTs
- Normally distributed
- Conf. interval: Wilson score
- Normal ref.: exp. smooth.

Detecting Delay Changes



Significant RTT changes:

Confidence interval not overlapping with the normal reference

Approach (2)

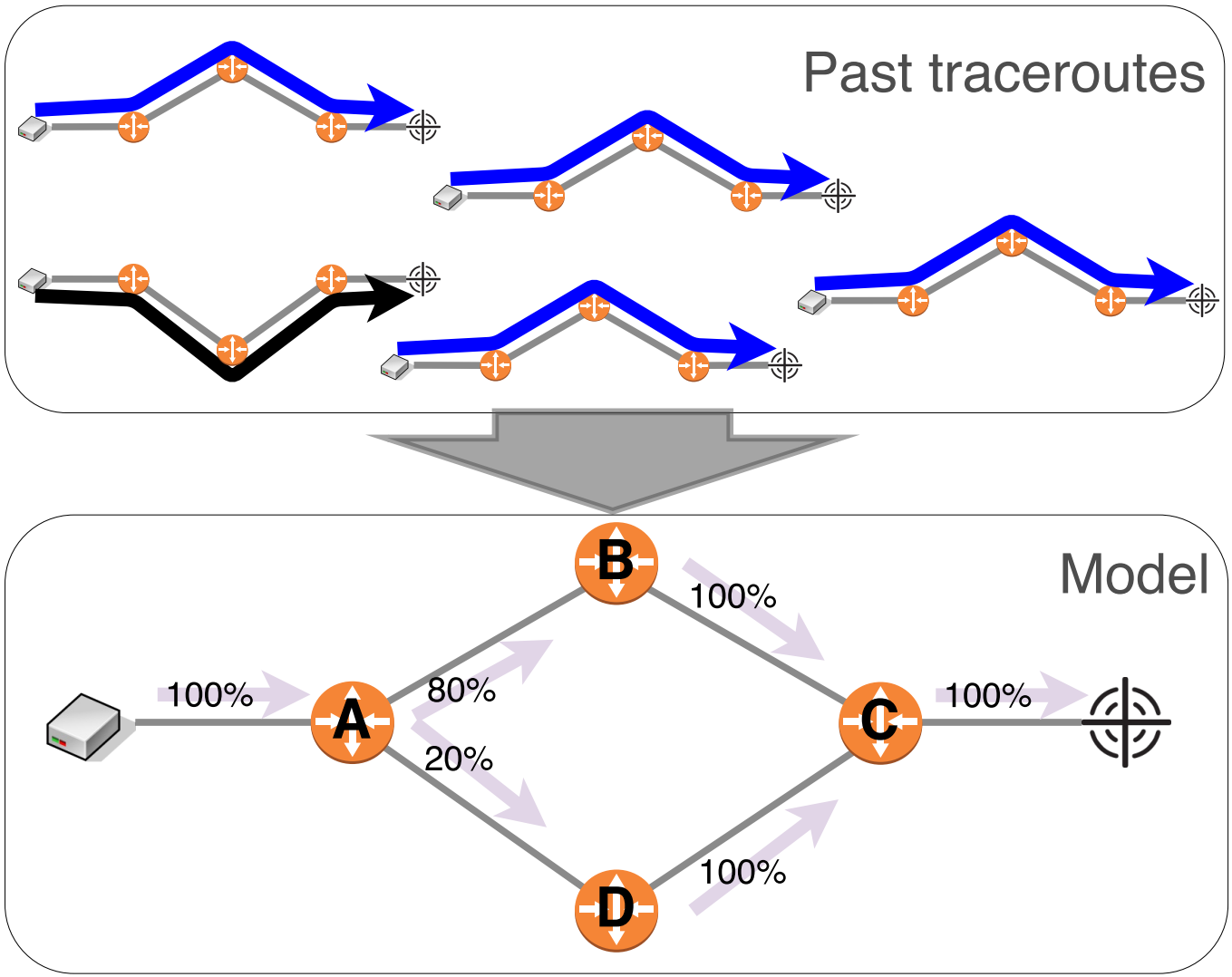
Monitor forwarding anomalies

- Sometimes we don't obtain expected data
  - Traffic is rerouted
  - Router is not responding
- Cannot obtain RTT values

$\rightarrow$ Need to model usual routes

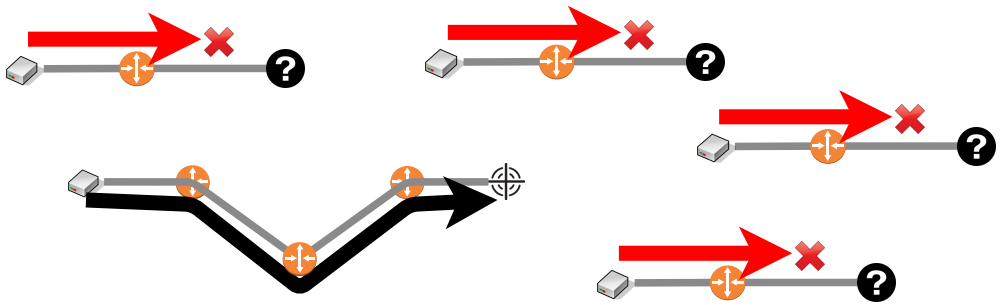
Packet forwarding model

Learn usual paths from past traceroutes:

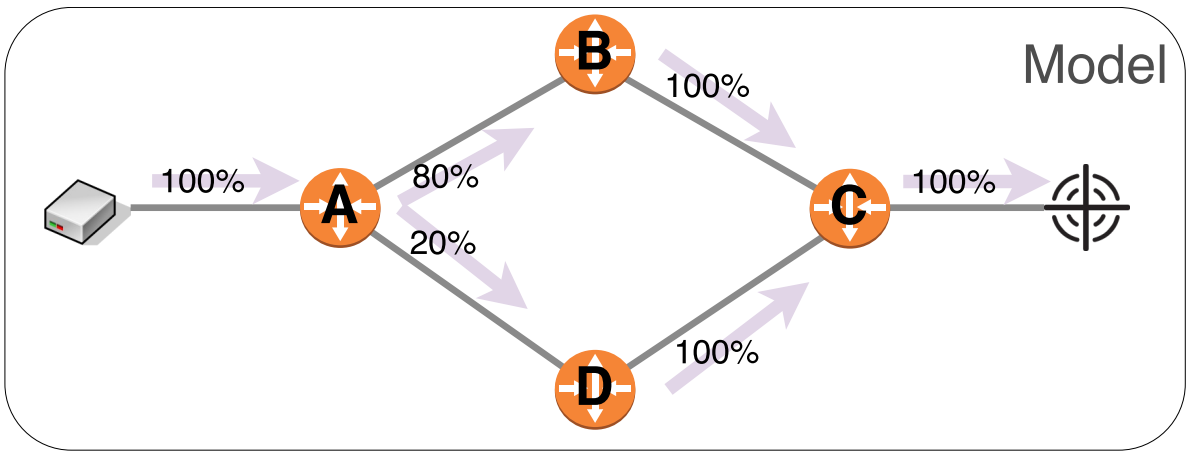


Identifying faulty links

In case of packet loss:



Query the model for the expected next hop



→ Link AB is dropping packets!

Case study: DDoS on DNS root servers

Two attacks:

- Nov. 30th 2015
- Dec. 1st 2015

Almost all server are anycast

- Congestion at the 531 sites?
- Found 129 instances altered by the attacks

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE

Networks

Internet's root servers take hit in DDoS attack

Who's testing the limits of the DNS system?

8 Dec 2015 at 23:10, Kieren McCarthy

The internet's root servers came under a c
effectively knocked three of the 13 critical p

The attack came just days before the Janet

According to a first analysis of the root serv
attack occurred on November 30, 2015 bet

Many, but not all, of the root servers receive
flood network connections and cause timec
messages for a single domain name; the s

Ultimately, the operators affected by the att
proper analysis is now underway to discove

Of perhaps most concern is the fact that ev
deal with such an attack, a number of the s

The root servers themselves make up the p
as a sort of global directory for all the other

Due to the internet's design, the servers the
you compare it to what companies like Goo
immediate problems for the wider internet,
thousands of other servers.

That said, any attack on the DNS' infrastruc
longer than a day, it would start causing sig

≤ 66% > 99% Data resolution: 10 minutes

Home Hacking Tech Cyber Attacks Vulnerabilities Malware Spying

The Hacker News™
Security in a serious way

Someone Just Tried to Take Down Internet's Backbone with 5 Million Queries/Sec

Wednesday, December 09, 2015 Swati Khandelwal

G+1 192 Like 5.9K Share 6538 Tweet 1049 Share 58 share 8417

The Internet's Backbone

DNS Root Servers Hit by a Massive Cyber Attack

Someone just DDoSed one of the most critical organs of the Internet anatomy – **The Internet's DNS Root Servers**.

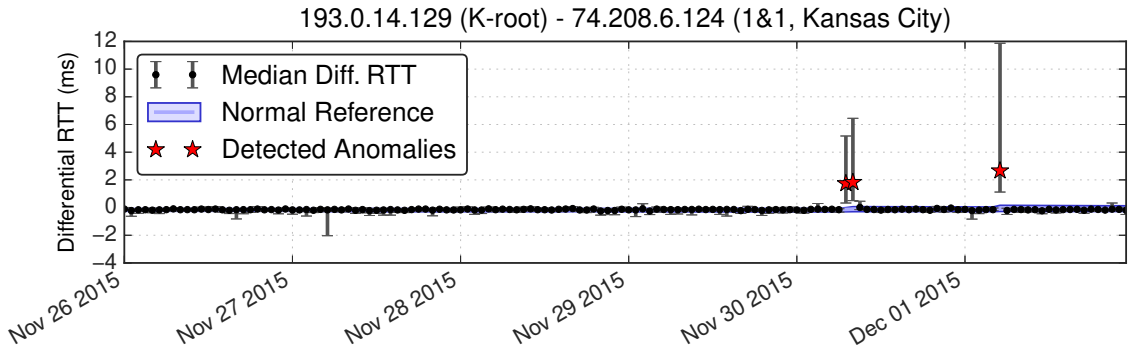
Early last week, a flood of as many as 5 Million queries per second hit many of the Internet's DNS (*Domain Name System*) Root Servers that act as the authoritative reference for mapping domain names to IP addresses and are a total of 13 in numbers.

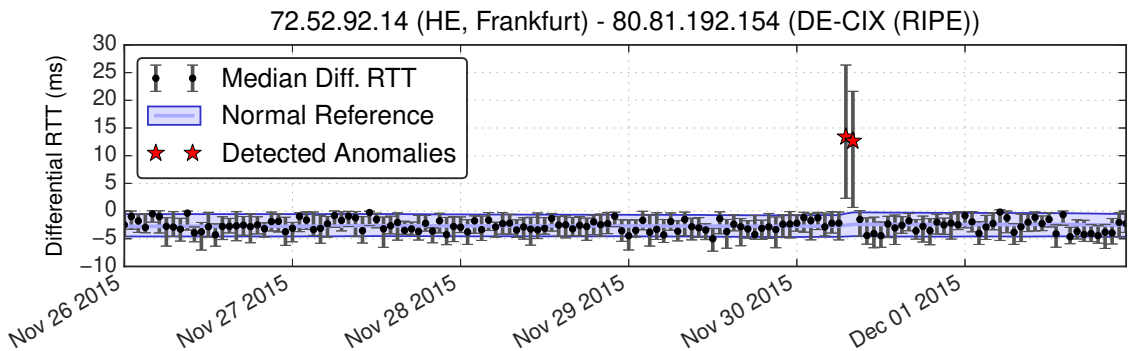
The attack, commonly known as **Distributed Denial of Service** (DDoS) attack, took place on two separate occasions.

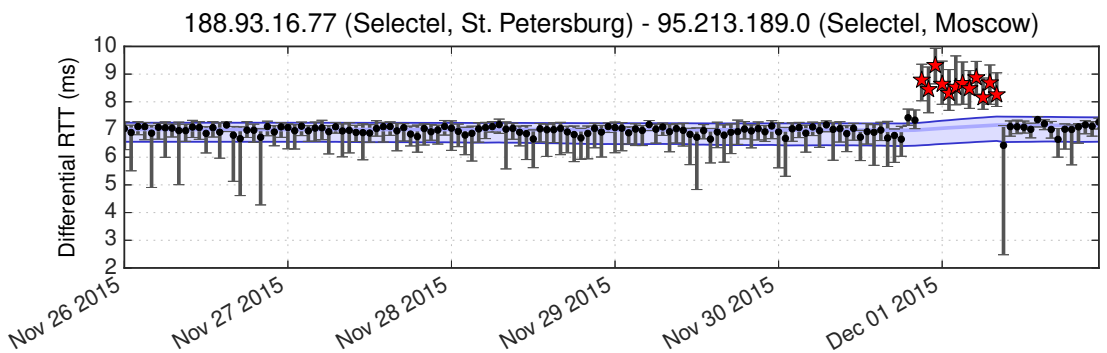
The first DDoS attack to the Internet's backbone root servers launched on *November 30* that lasted 160 minutes (*almost 3 hours*), and the second one started on *December 1* that lasted almost an hour.

Massive Attacks Knocked Many of the 13 Root Servers Offline

Observed delay changes

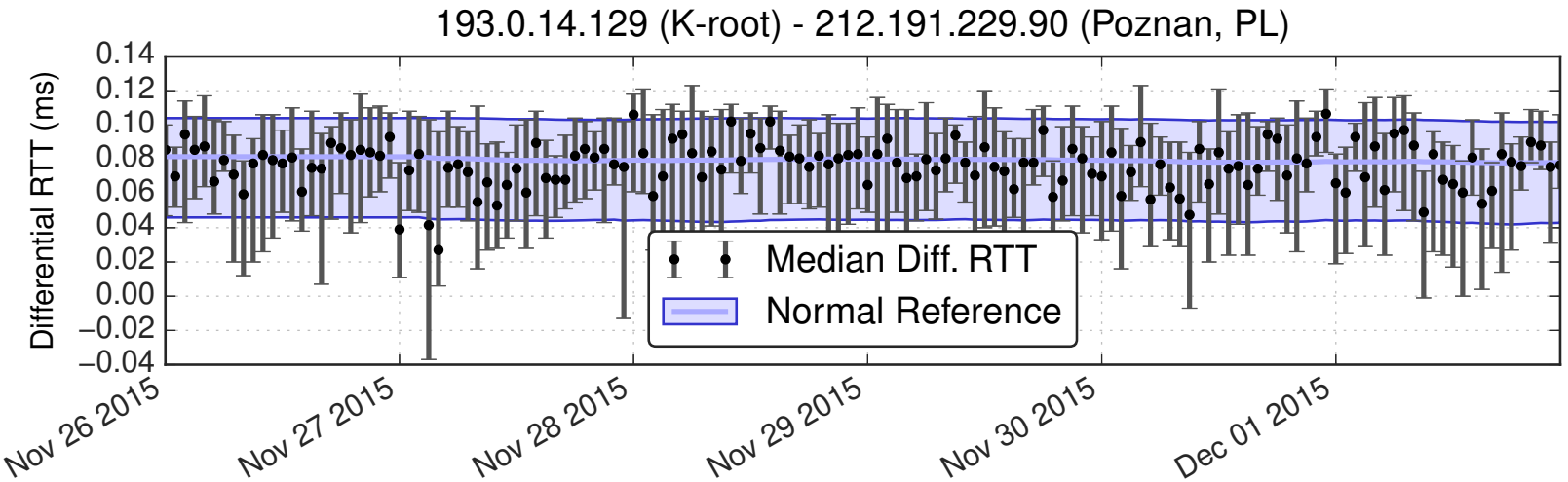






- Certain servers are affected only by one attack
- Continuous attack in Russia

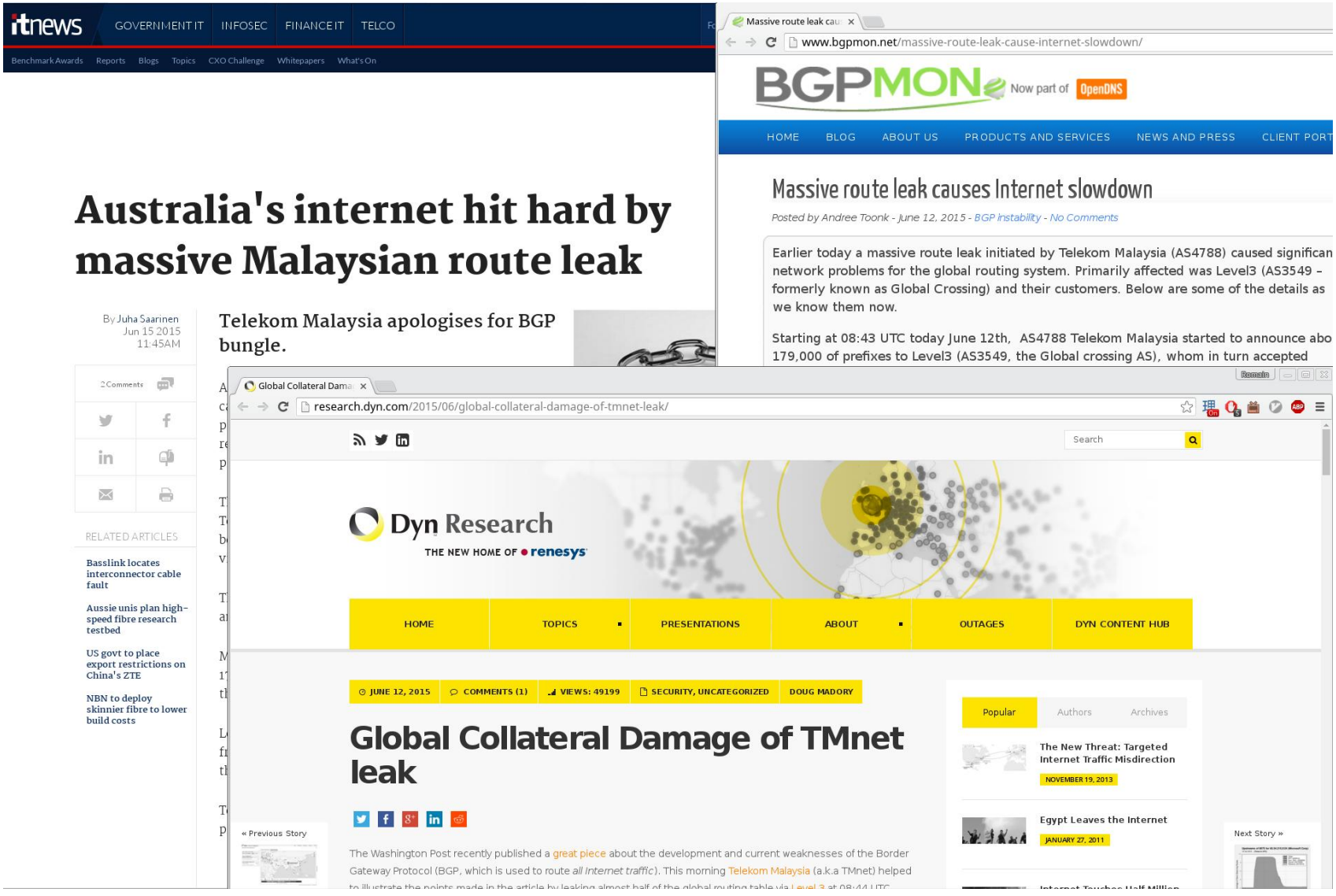
Unaffected root servers



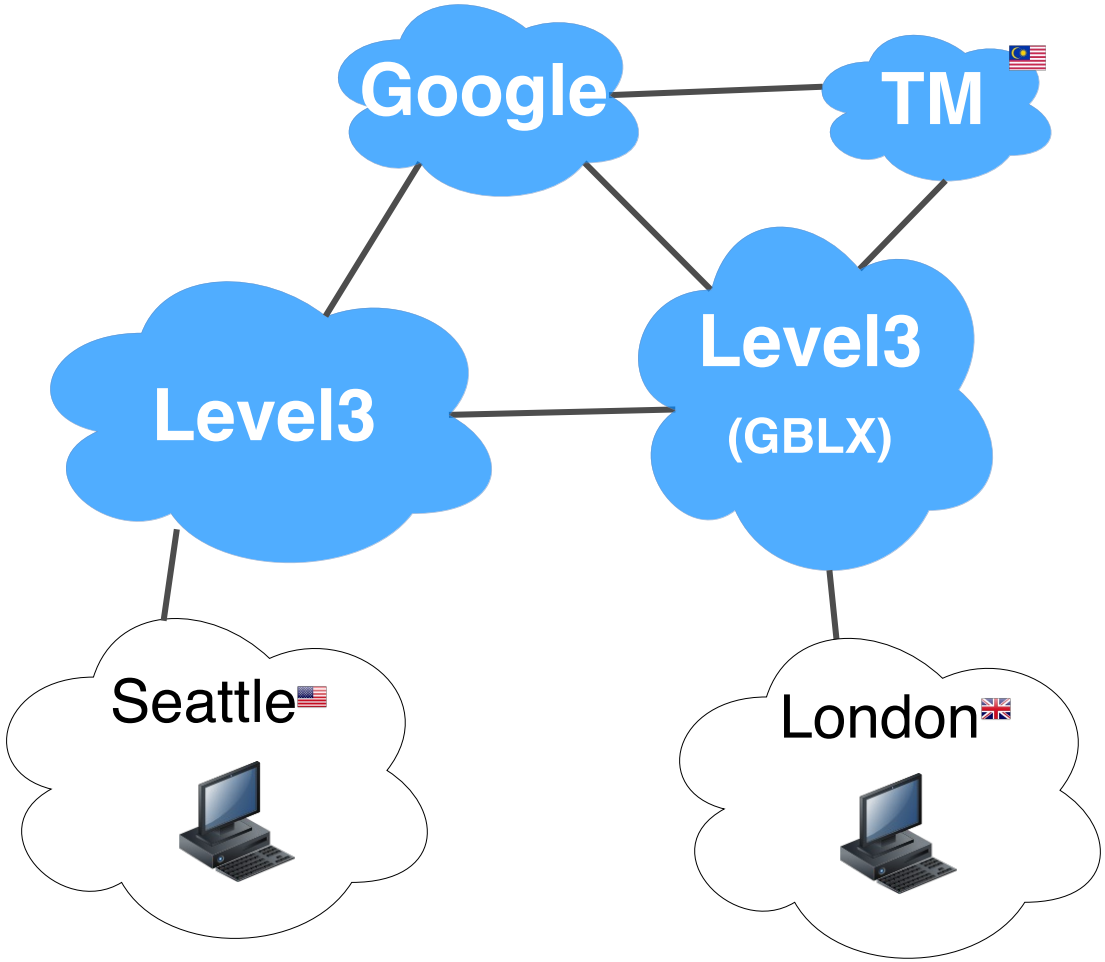
Very stable delay during the attacks

- Thanks to anycast!
- Far from the attackers

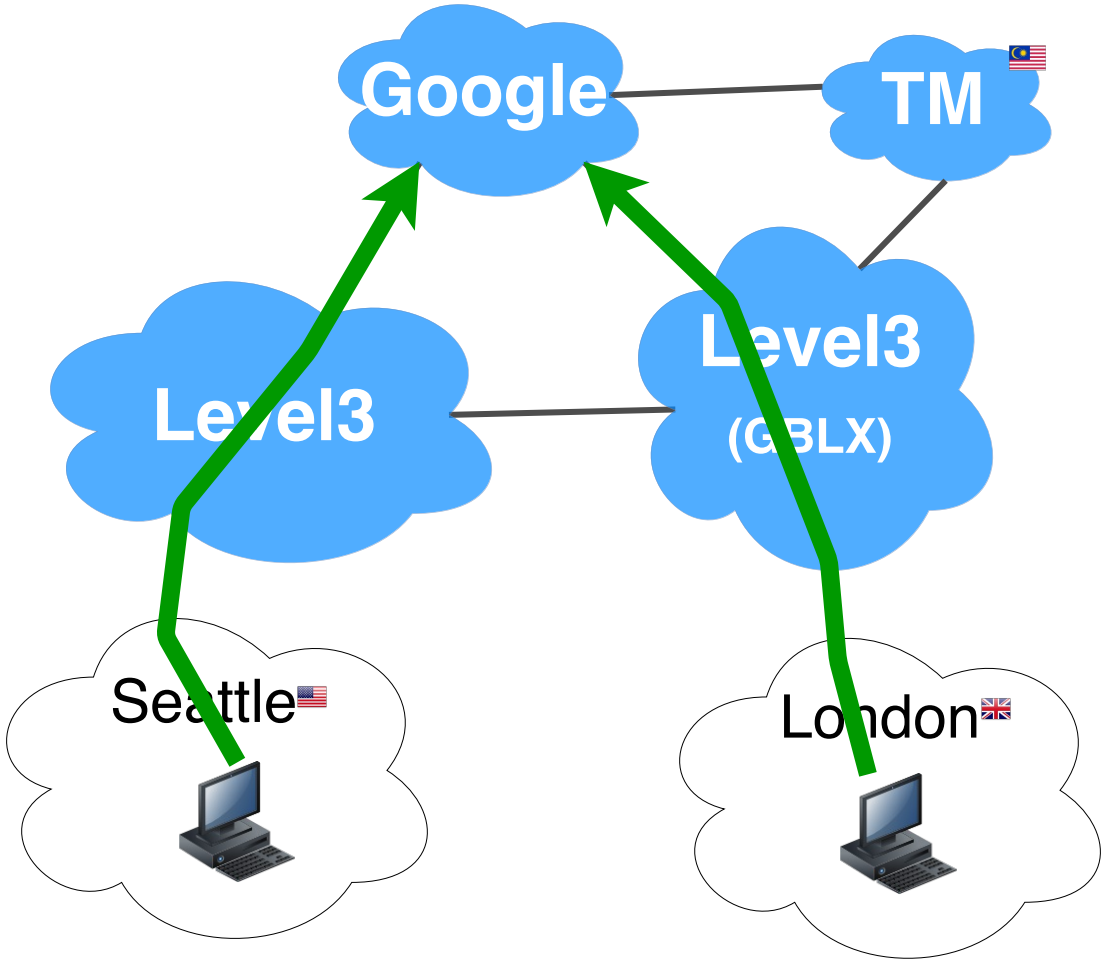
Study case: Telekom Malaysia BGP leak



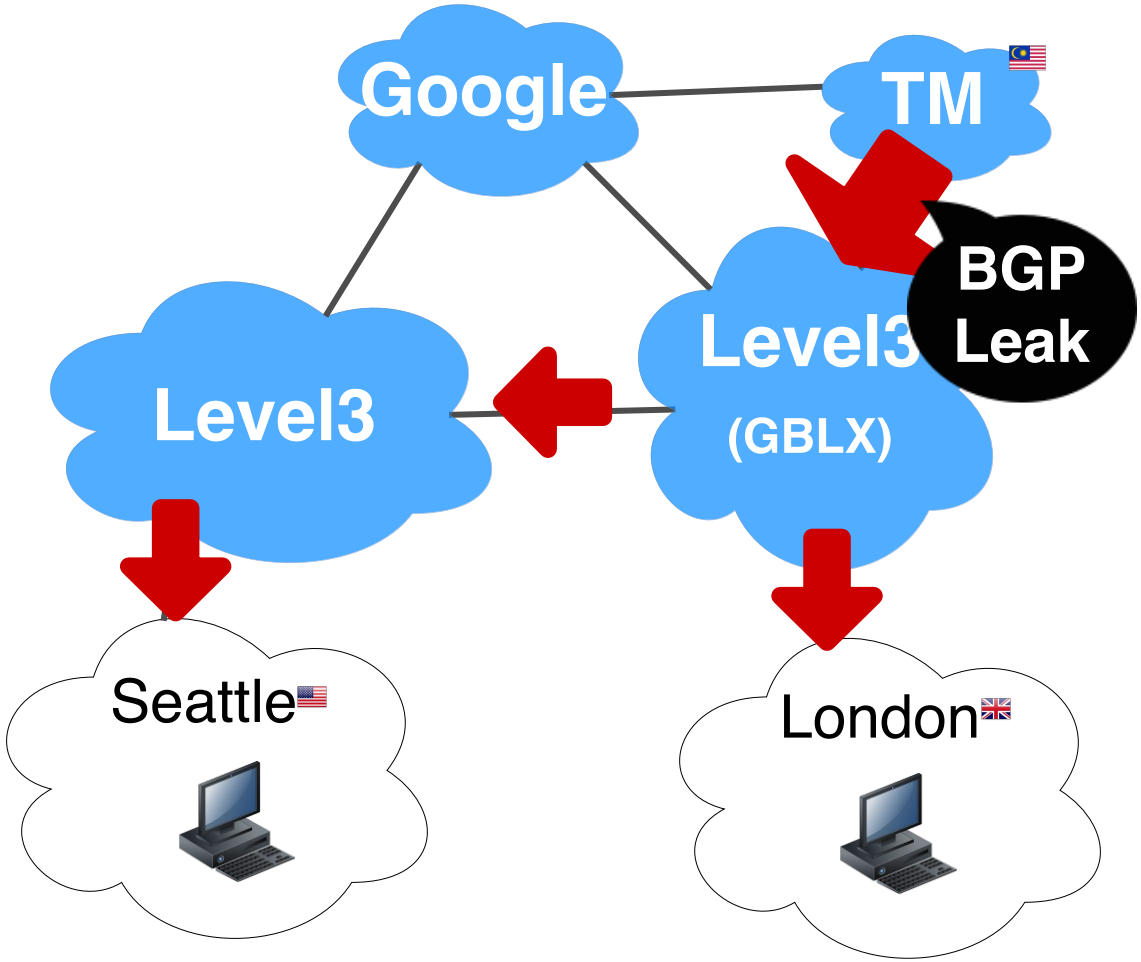
Study case: Telekom Malaysia BGP leak



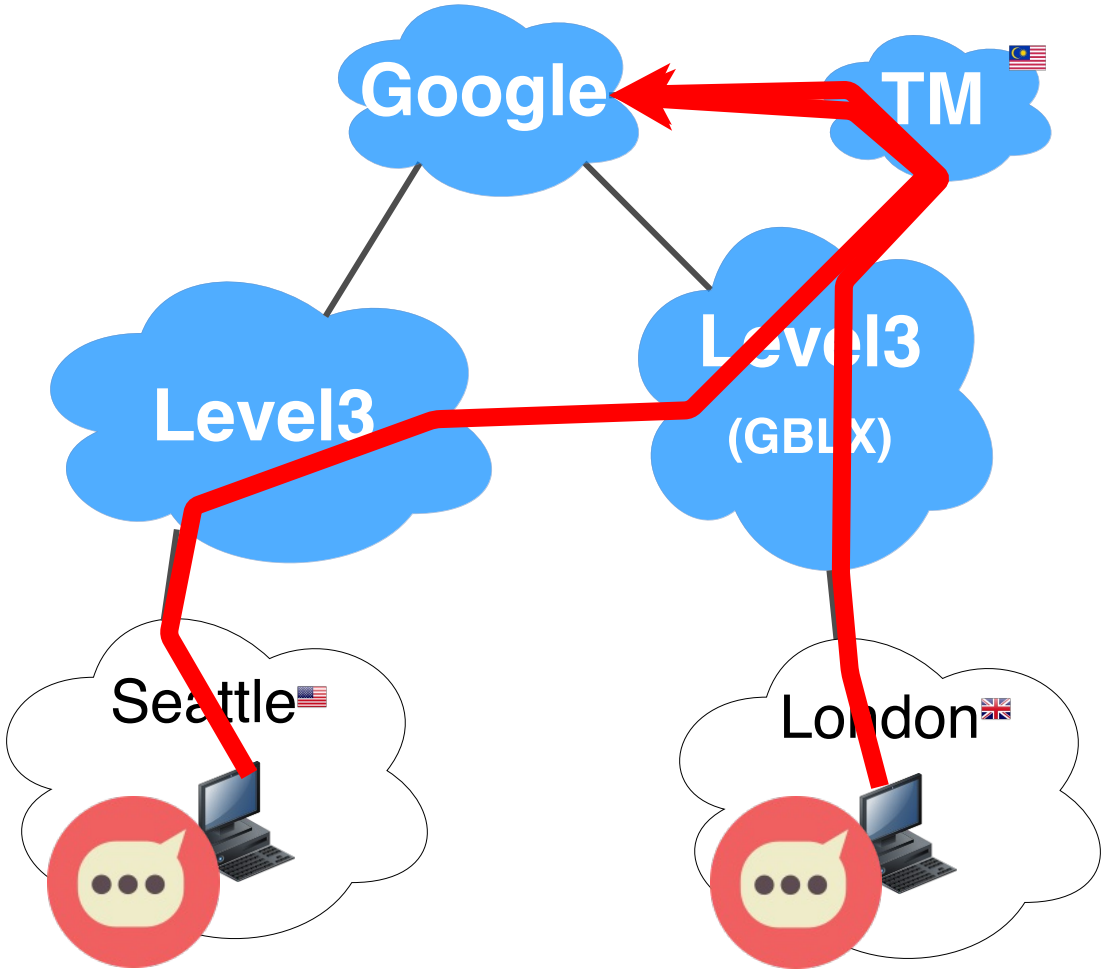
Study case: Telekom Malaysia BGP leak



Study case: Telekom Malaysia BGP leak



Study case: Telekom Malaysia BGP leak

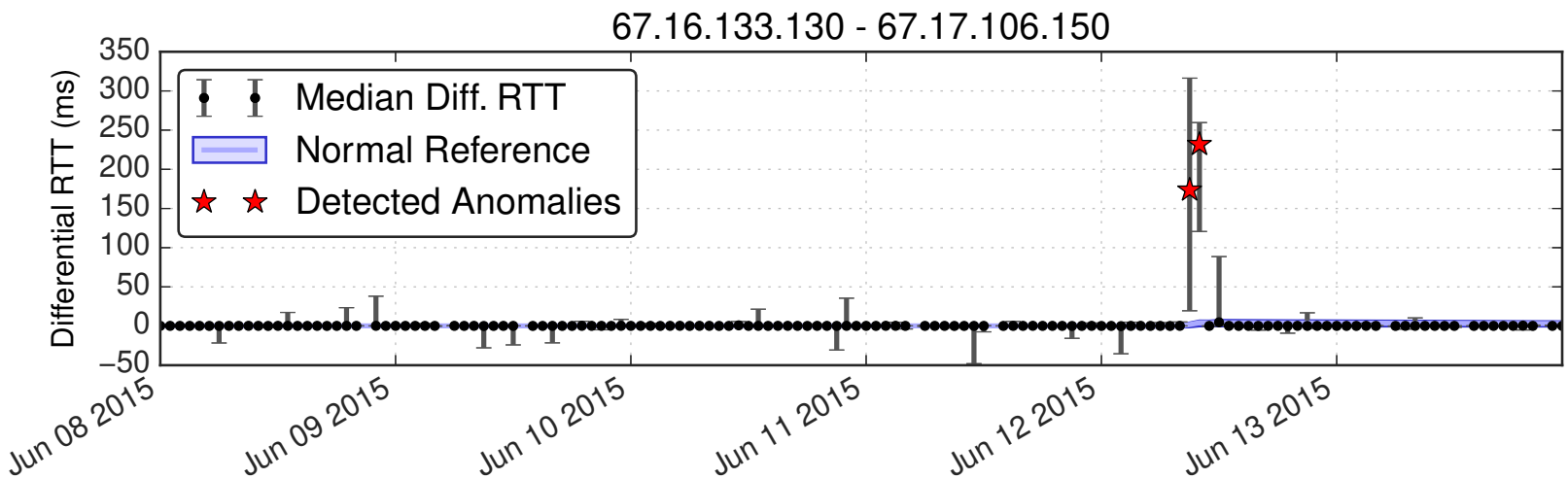


Not only with Google... but about **170k prefixes!**

Congestion in Level3

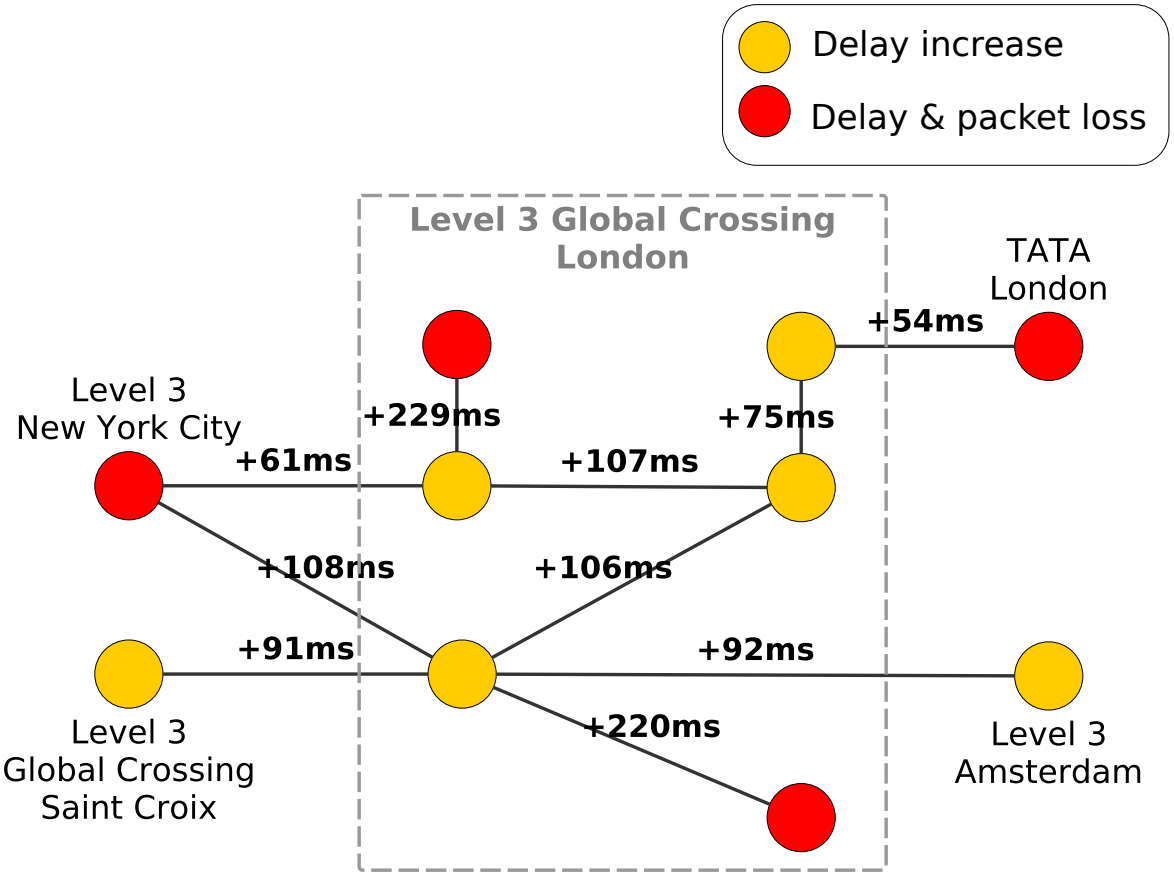
Rerouted traffic has congested Level3 (120 reported links)

- Example: 229ms increase between two routers in London!



Congestion in Level3

Reported links in London:



→ Traffic staying within UK/Europe may also be altered

More Examples

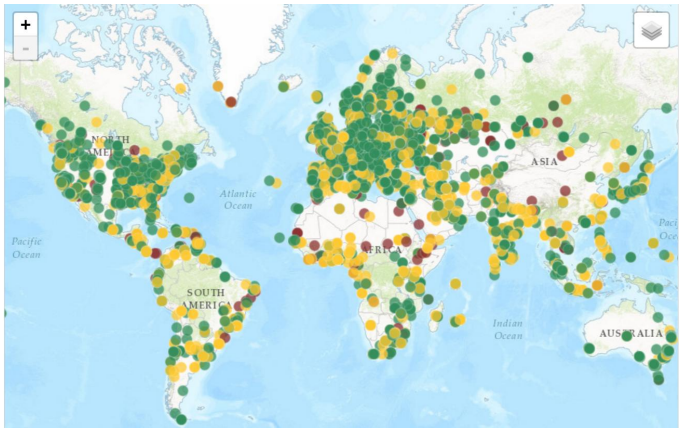
Examples from IHR website:

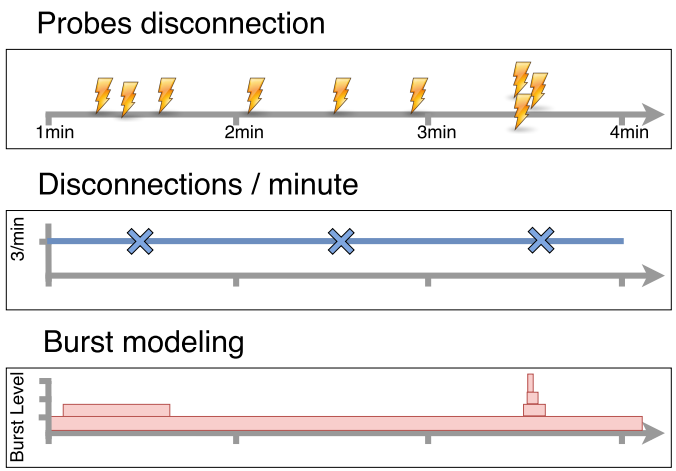
- Delay increase on JP/AU sea cable
- Akamai/prolexic delay increase during memcached DDoS attacks

Outage Detection

Outage detection

- Monitor Atlas probes disconnections
- Identify burst of disconnections
- Report the corresponding network or geo area



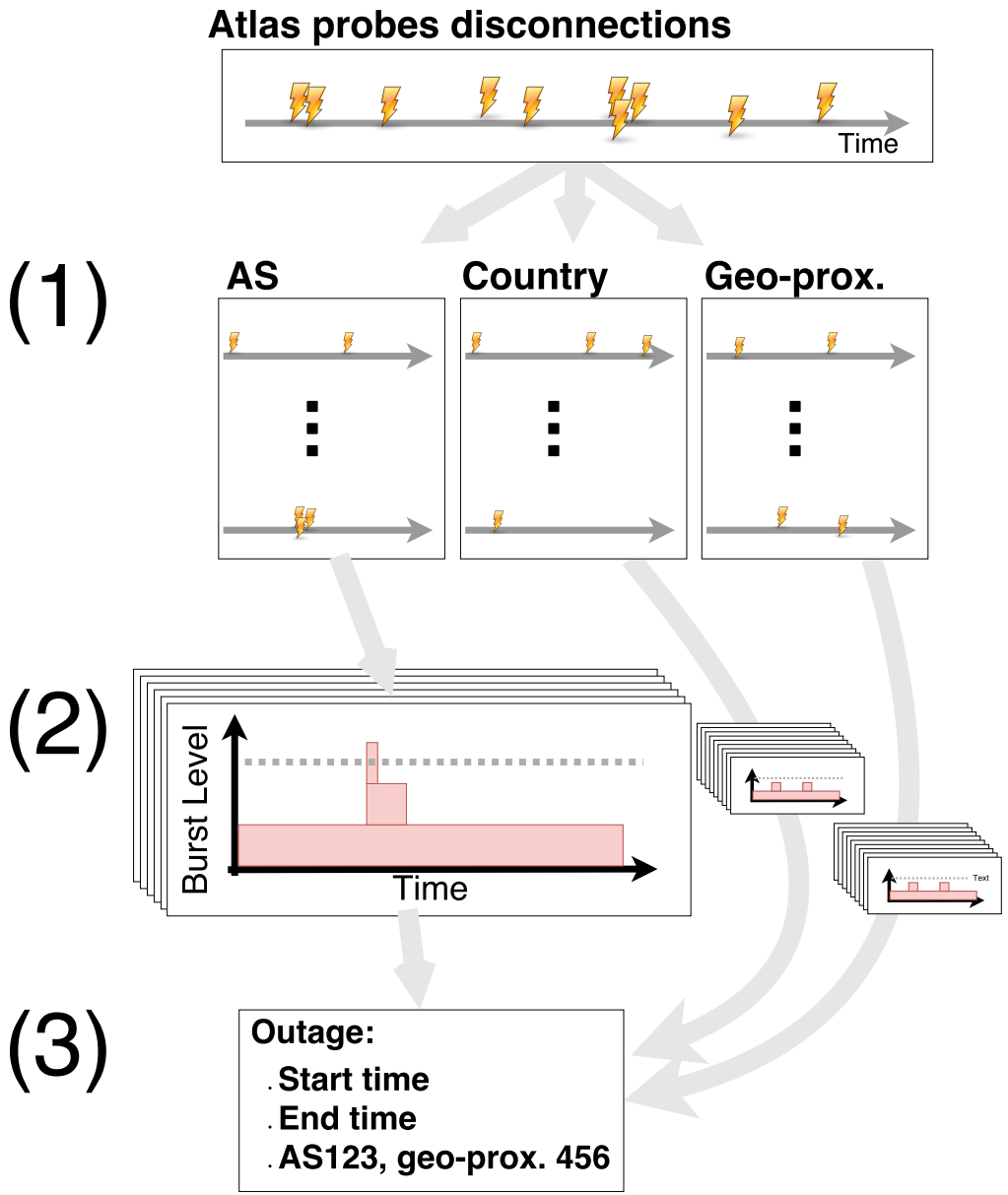


Disco Overview

1. Split disconnections in sub-streams (AS, country, geo-proximate 50km radius)

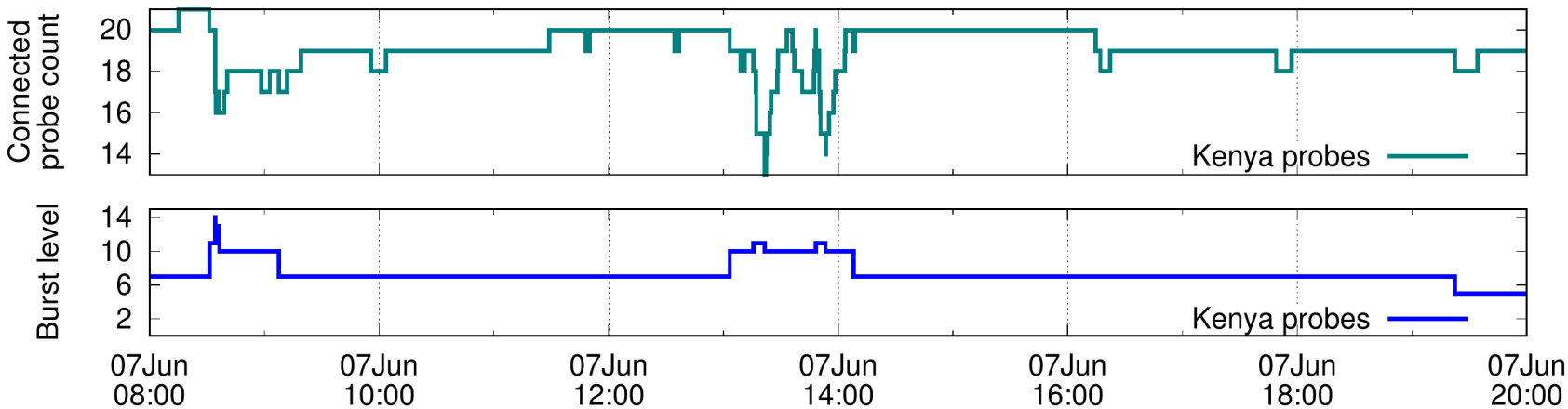
2. Burst modeling and outage detection

3. Aggregation and outage reporting



Burst modeling: Example

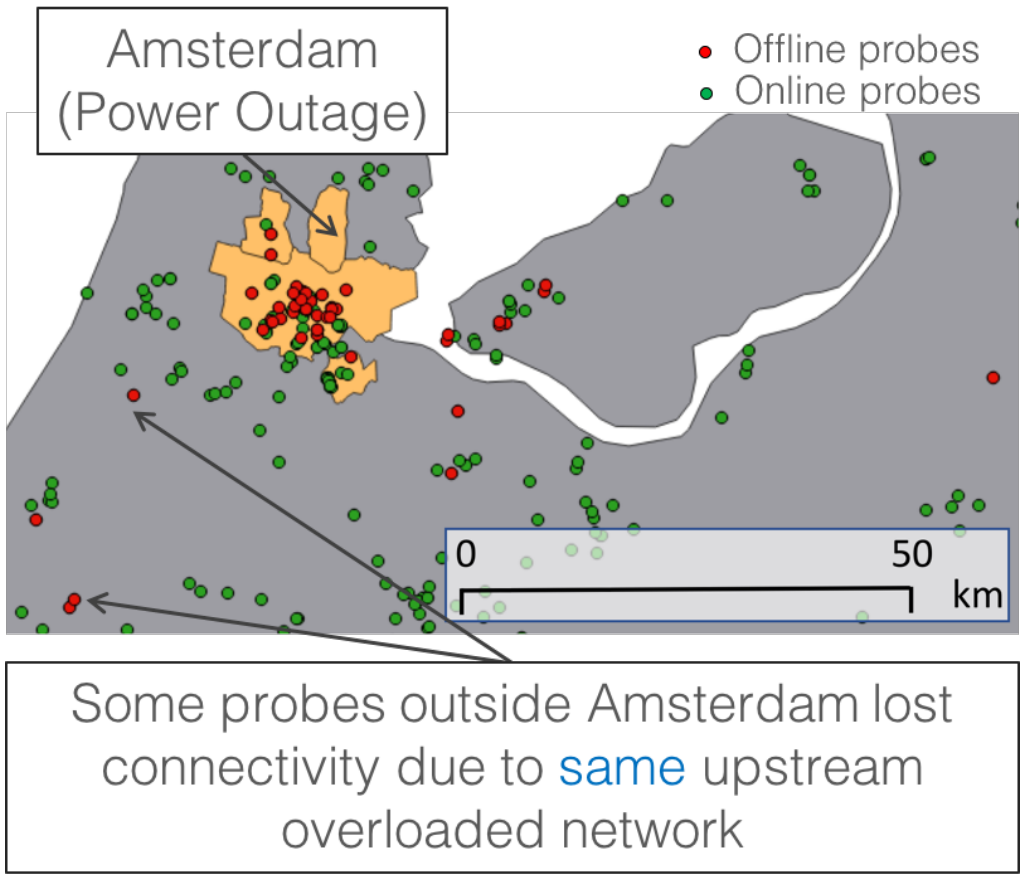
- Monkey causes blackout in Kenya at 8:30 UTC June, 7th 2016
- Same day RIPE rebooted controllers



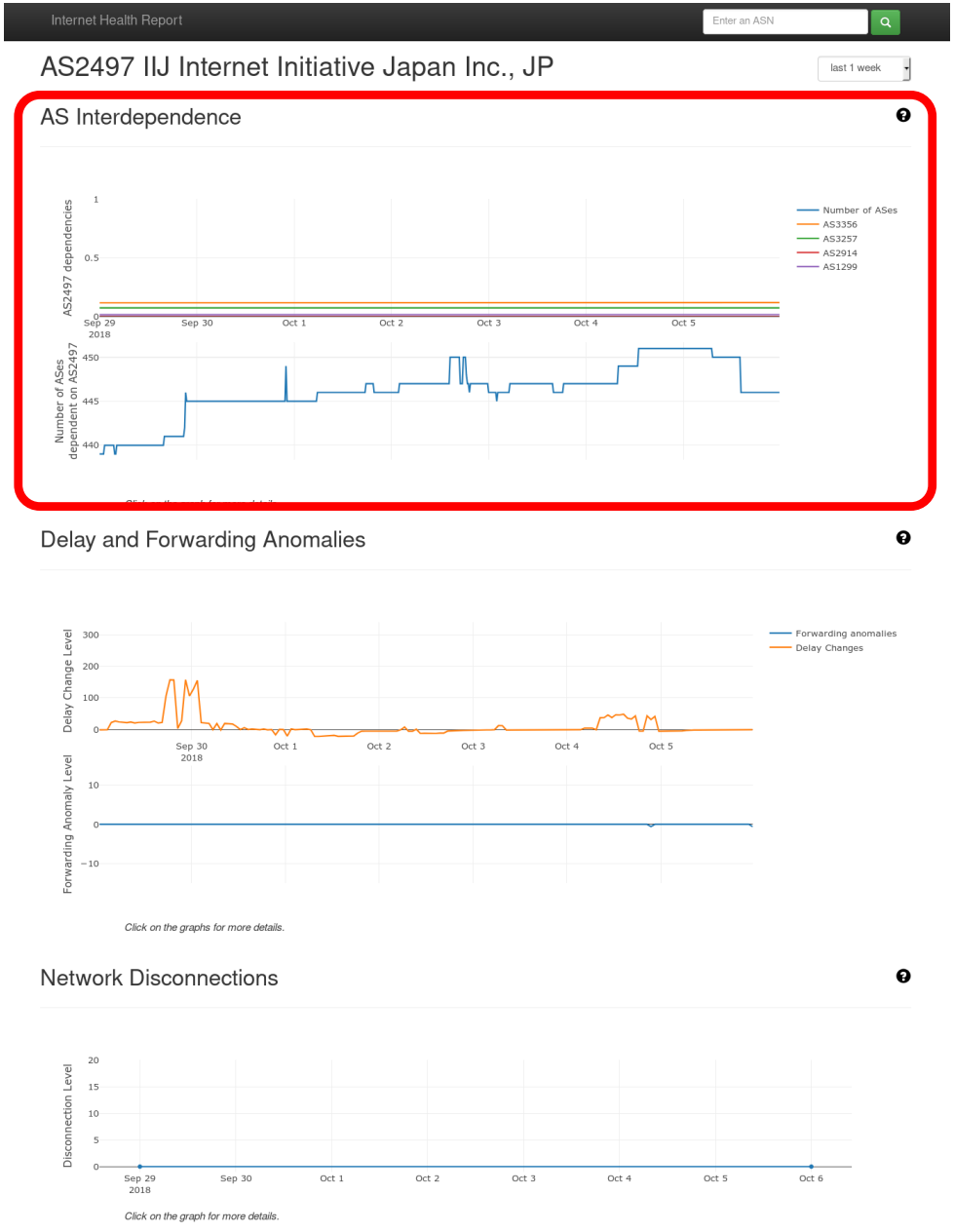
Example of geo-proximate outage

Amsterdam outage (2017)

- Disco's detection correlated with network problems between two network elements of a large provider



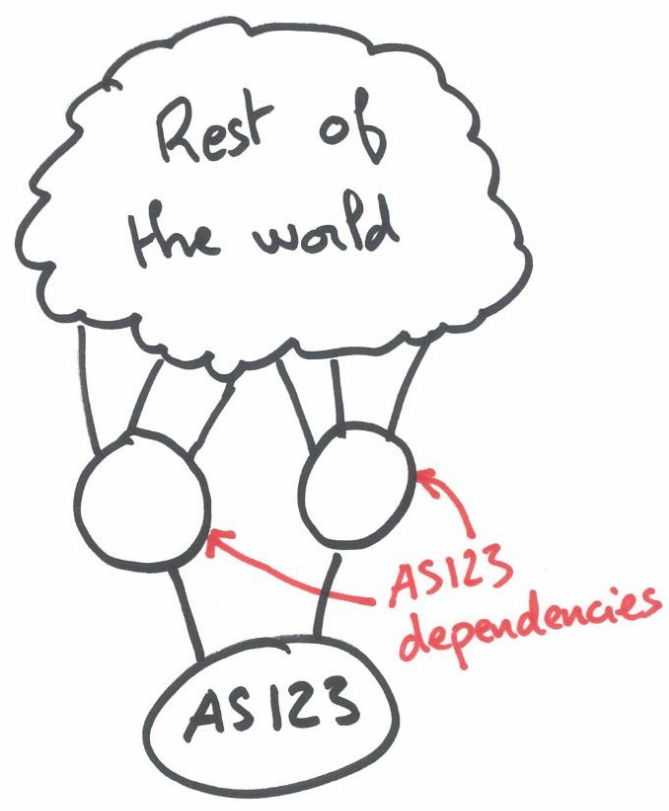
AS dependency



AS dependency

Monitoring AS Dependency

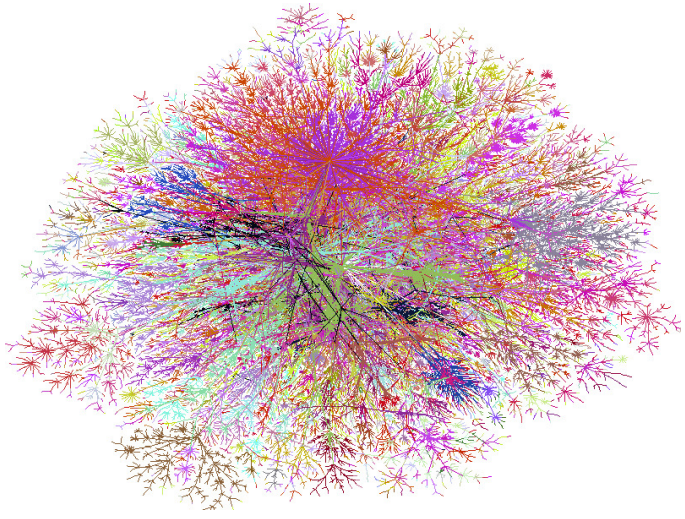
- A network's connectivity depends on other networks
- Dependency changes may reveal routing anomalies
- Help operators to plan and assess infrastructure deployments

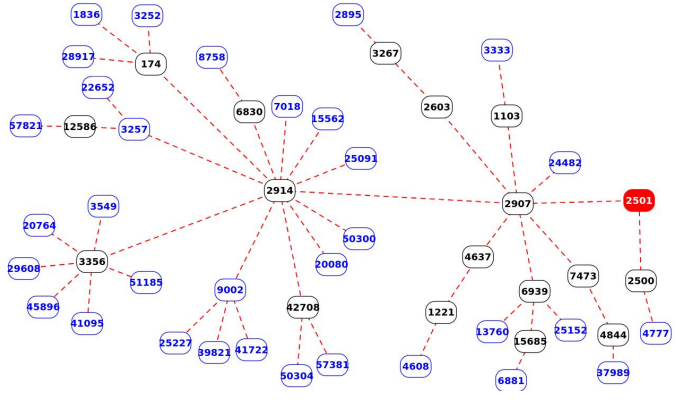


Approach

Measuring AS centrality:

- Dataset: BGP data
- Make AS graphs
- Two types of graph
  - Global graph: the whole Internet
  - Local graph: paths towards a single AS
- Measure nodes *centrality*:
  - Common transit networks
  - *AS Dependencies*

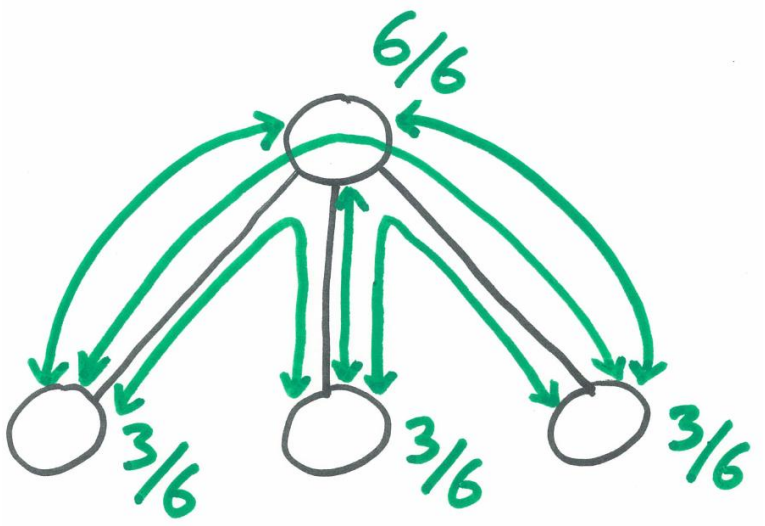




In Theory...

Betweenness Centrality (BC)

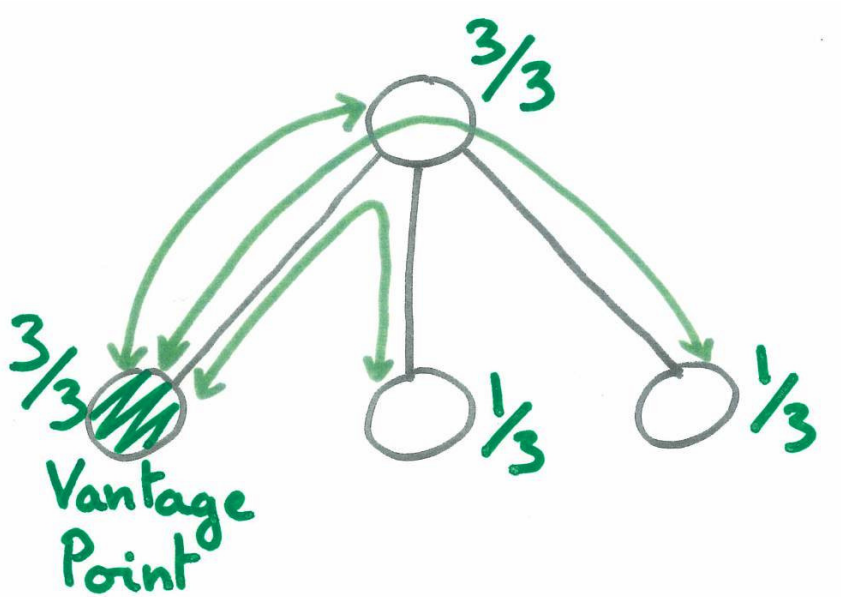
- Common centrality metric in graph theory
- Measure the fraction of paths going through an AS



...in Practice

BC and path sampling

- We don't know all AS paths on the Internet
- RIS and RV give about 300+ vantage points out of 58k ASes
- BGP collections $\neq$ random sampling



AS hegemony

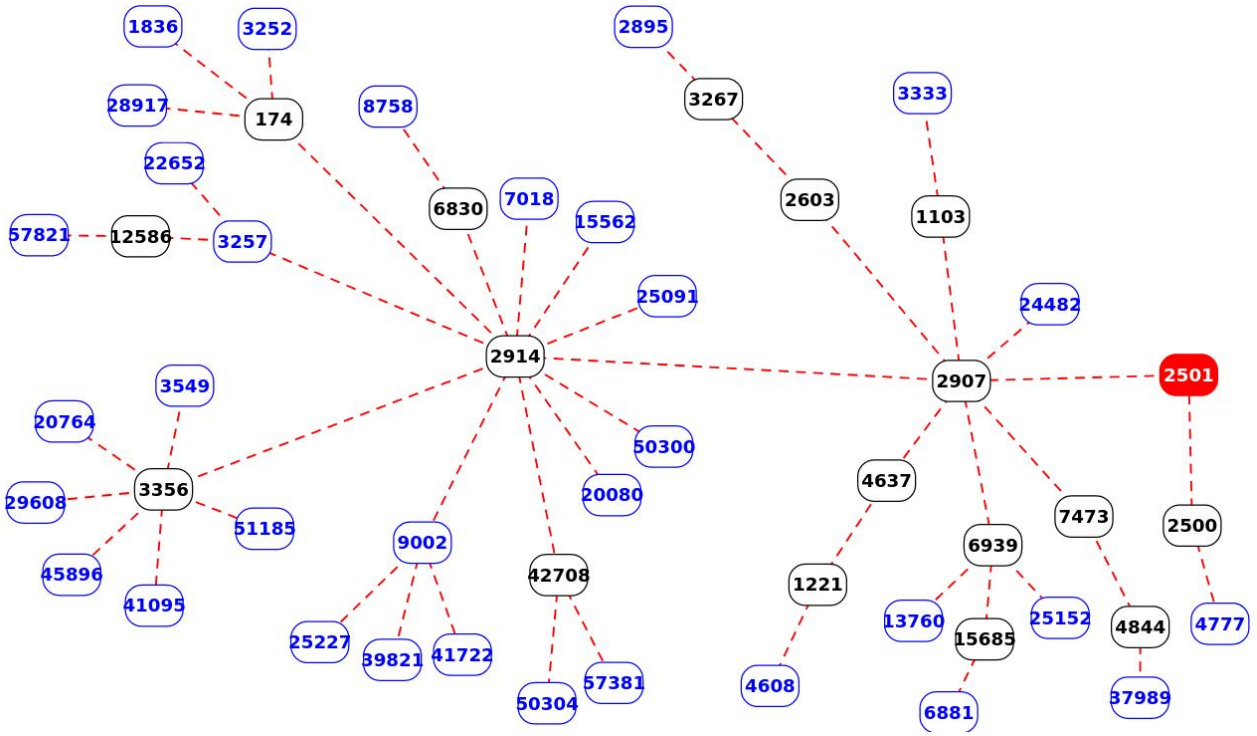
$$\mathcal{H}(v,\alpha) = \frac{1}{n - (2\lfloor \alpha n \rfloor)} \sum_{j=\lfloor \alpha n \rfloor + 1}^{n - \lfloor \alpha n \rfloor} BC_{(j)}(v) h$$

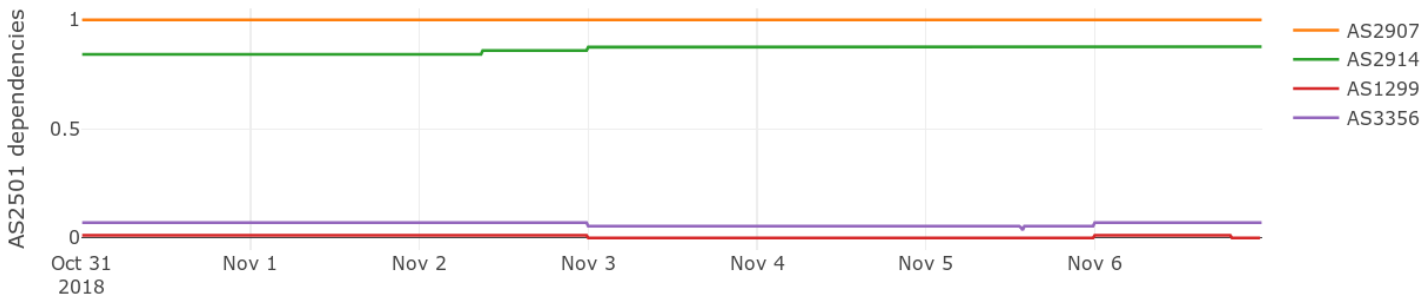
Benefits:

- Same meaning as Betweenness Centrality
- Vantage point consensus
- Robust to sampling
- Adapted to BGP

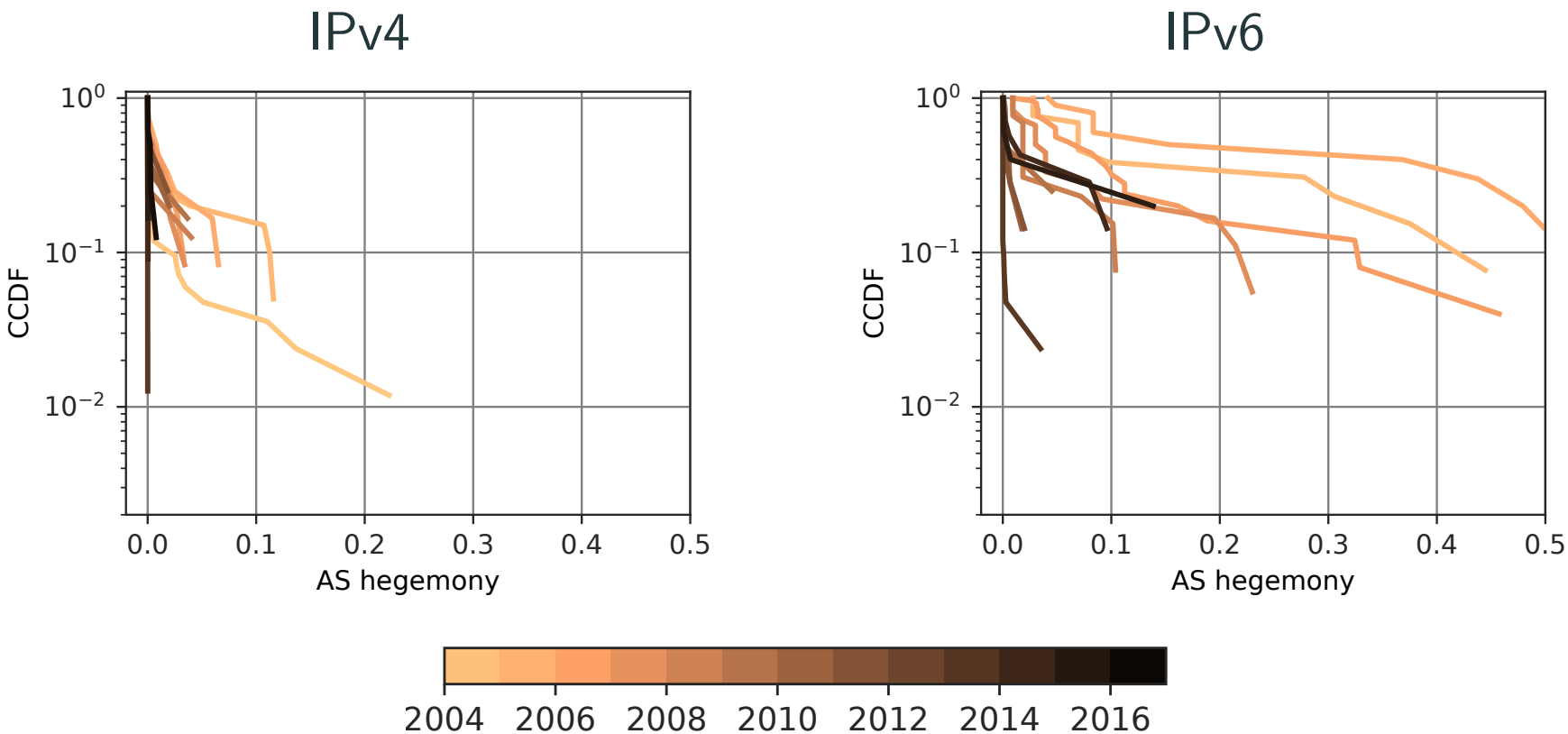
Example AS hegemony

AS hegemony ≈ Betweenness centrality





Local Graph: Google

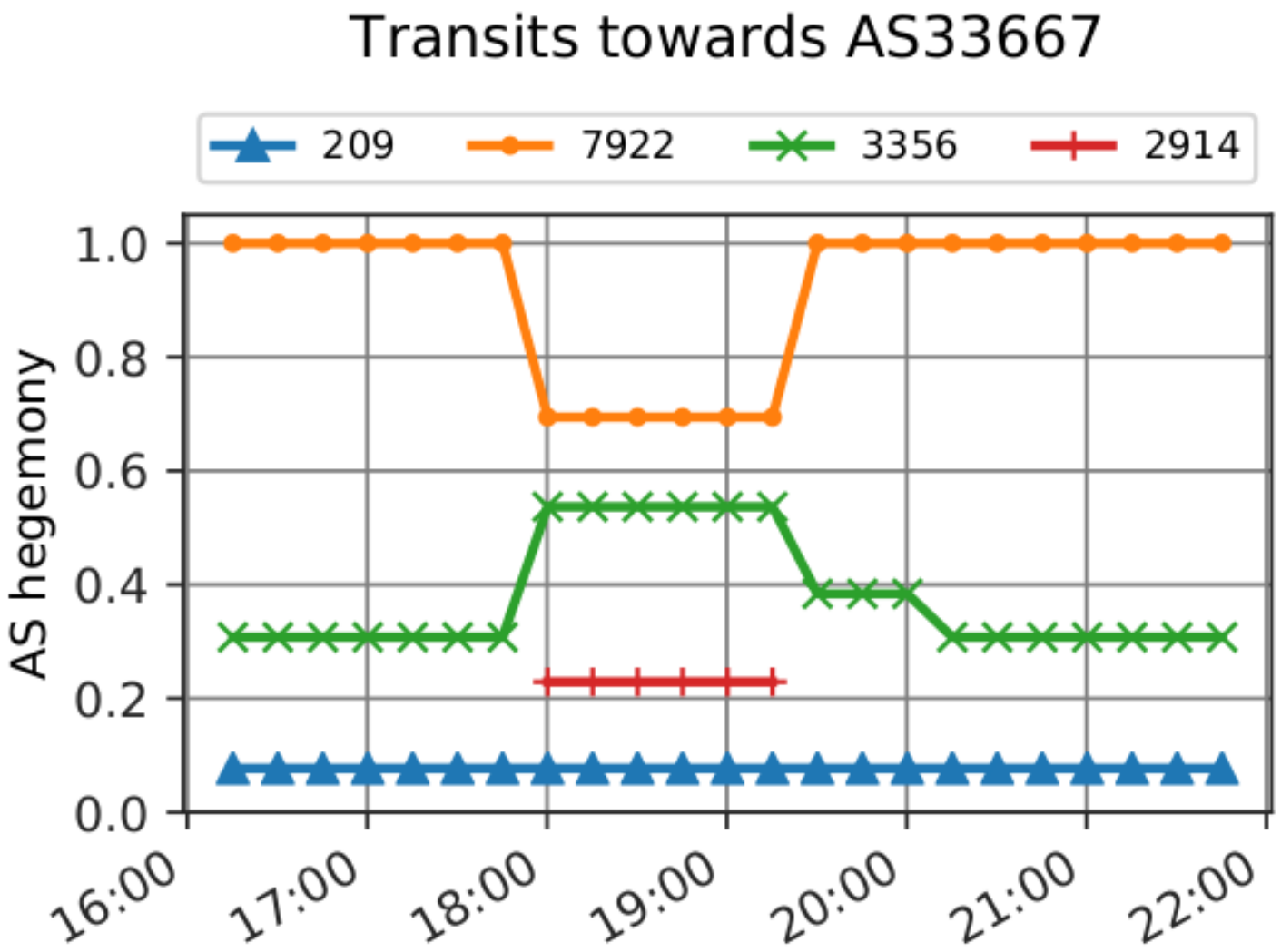


→ IPv4: Recently measured no dependency

→ IPv6: Noticeable dependence to Hurricane Electric

Example of AS hegemony change

BGP leak Level3/Comcast (2017/11/07)



Online Results: Examples in 2018

Internet Health Report: `https://ihr.iijlab.net`

- DoS attack
  - Attack against Github on Feb. 28th
  - Attacks during Russian elections Mar. 18th
- Outage
  - Power outage in northern Brazil, Mar. 21st
  - DECIX outage, Apr. 4th
  - The fall of Bitcanal (*the Hijack factory*), July
- BGP leak
  - Leak from CloudFlare, Jul. 1st
- Censorship
  - Country-level bottlenecks: Iran, China, Pakistan, ...
  - CrimeaCom in 2013 vs. CrimeaCom in 2018
  - Exams in Iraq, June
  - Protests in Iraq, Jul. 14-15th

Summary

Internet Health Report

- Monitor connectivity issues
- Delay, disconnection and routing anomalies
- `https://ihr.iijlab.net`

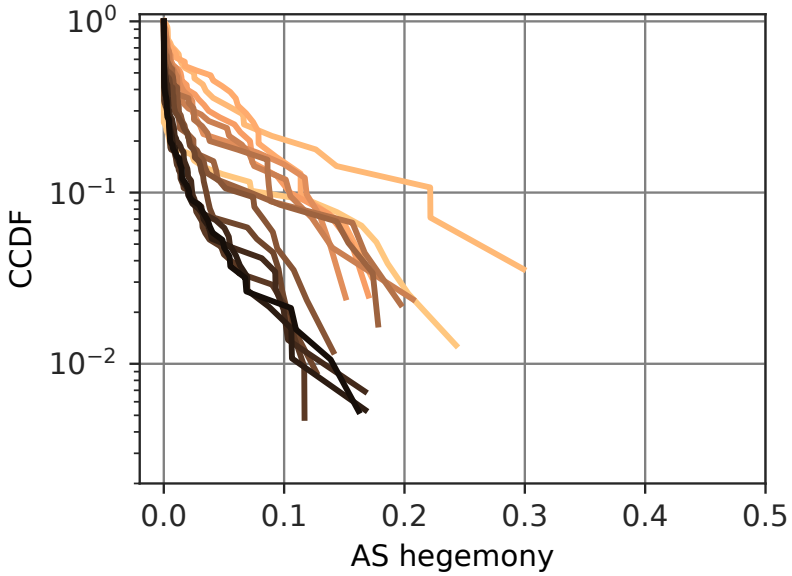
References

- A. Shah et al. "Disco: Fast, good, and cheap outage detection", TMA'17.
- R. Fontugne et al. "Pinpointing Delay and Forwarding Anomalies Using Large-Scale Traceroute Measurements", IMC'17.
- R. Fontugne et al. "The (thin) Bridges of AS Connectivity: Measuring Dependency using AS Hegemony", PAM'18.

Backup

Akamai

IPV4 local graph:



IPv6 local graph: