



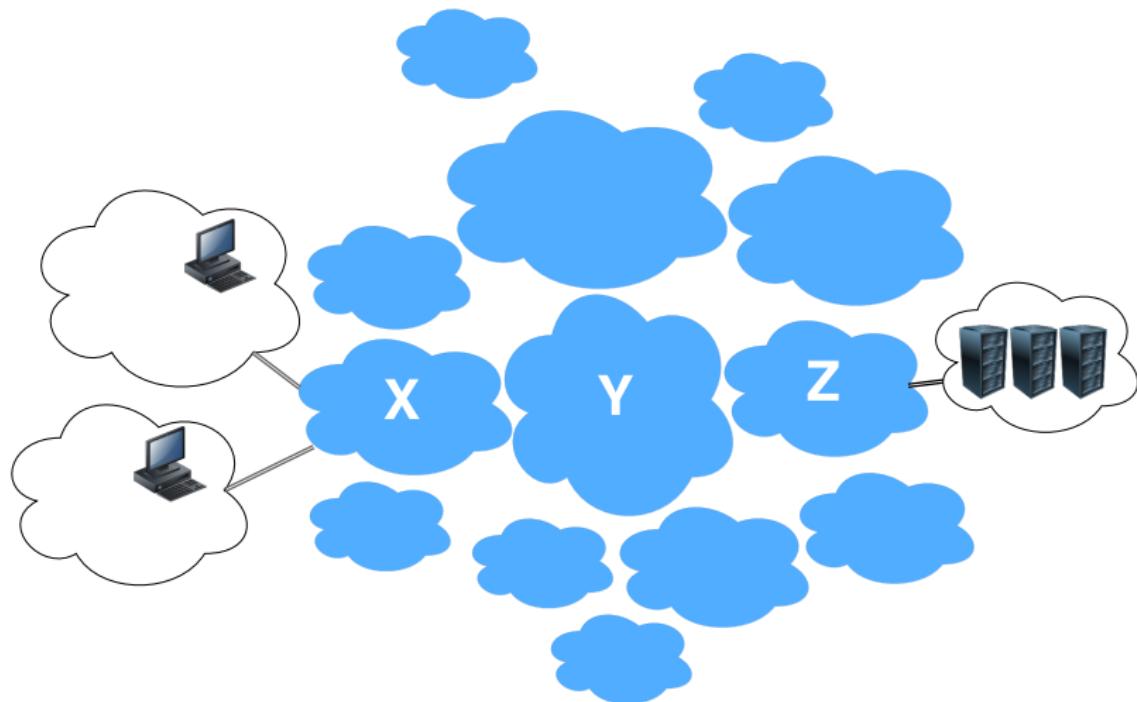
IHR: Monitoring Internet Health at Scale

<https://ihr.iijlab.net>

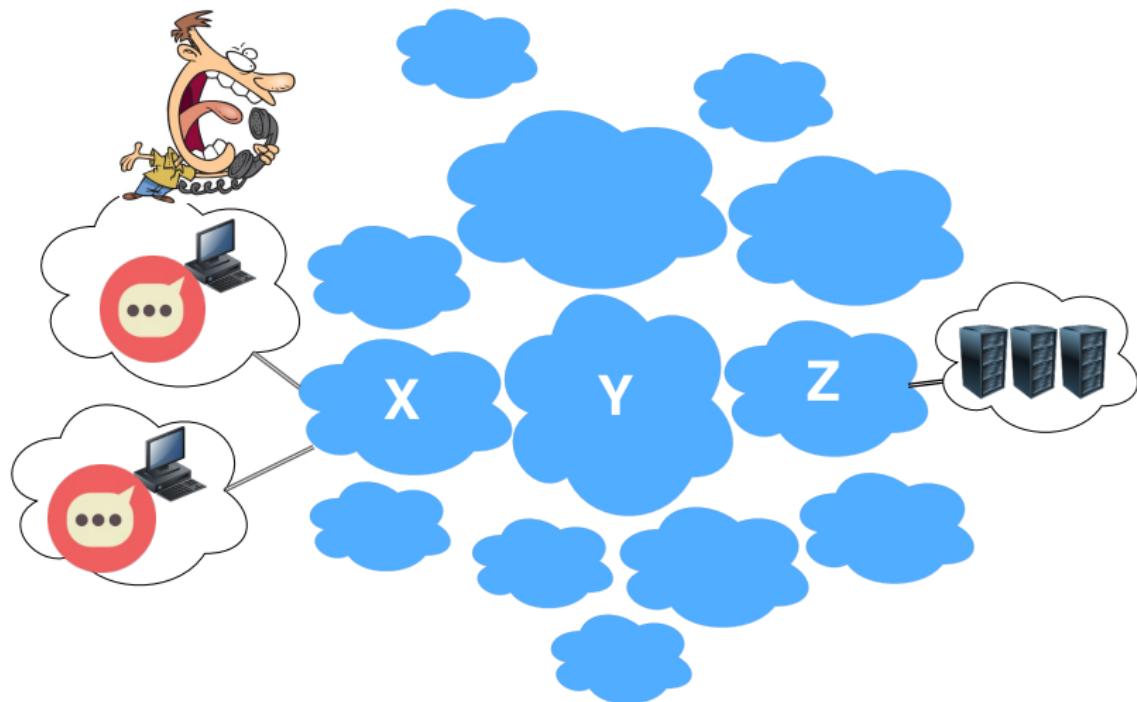
Romain Fontugne

IIJ Research Lab

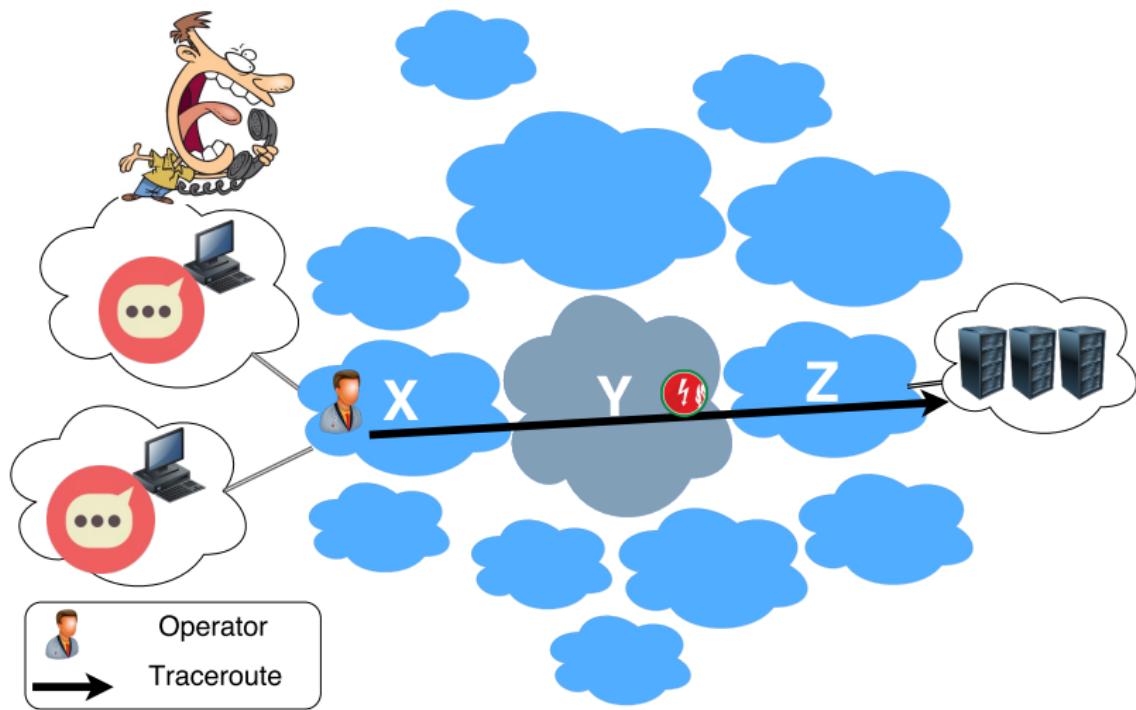
Internet: a network of networks



Internet: a network of networks



Internet: a network of networks



Internet Health Report?

Goal: Monitor Internet's Health

- Automatically pinpoint connectivity issues

Main Challenges:

- Internet is huge
 - Over 60k autonomous systems
 - Billions of connected devices
- Constantly evolving
- Limited views on remote networks



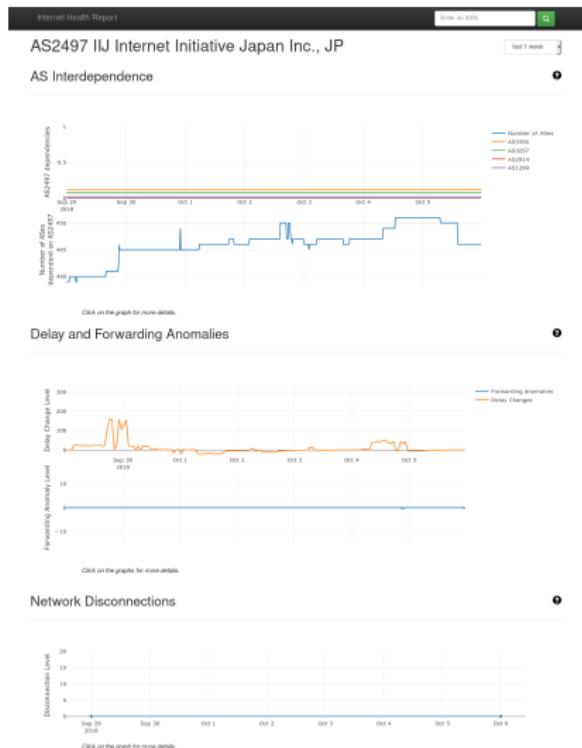
Internet Health Report: Current Status

Three main components

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

Internet Health Report

- Results publicly available:
<https://ihr.iijlab.net>
- Open source code:
<https://github.com/InternetHealthReport>



Delay/Forwarding anomaly detection



AS2497 IIJ Internet Initiative Japan Inc., JP

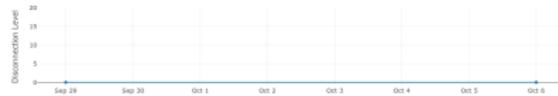
AS Interdependence



Delay and Forwarding Anomalies



Network Disconnections



Click on the graph for more details.

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



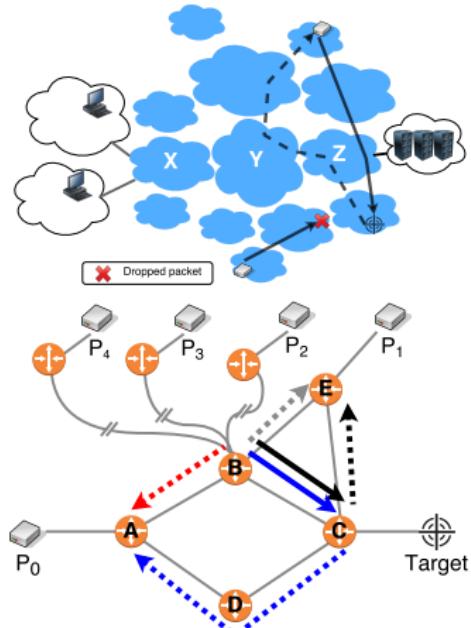
Delay/Forwarding anomalies

Challenges:

- Noisy data
 - Traffic asymmetry
 - Packet loss

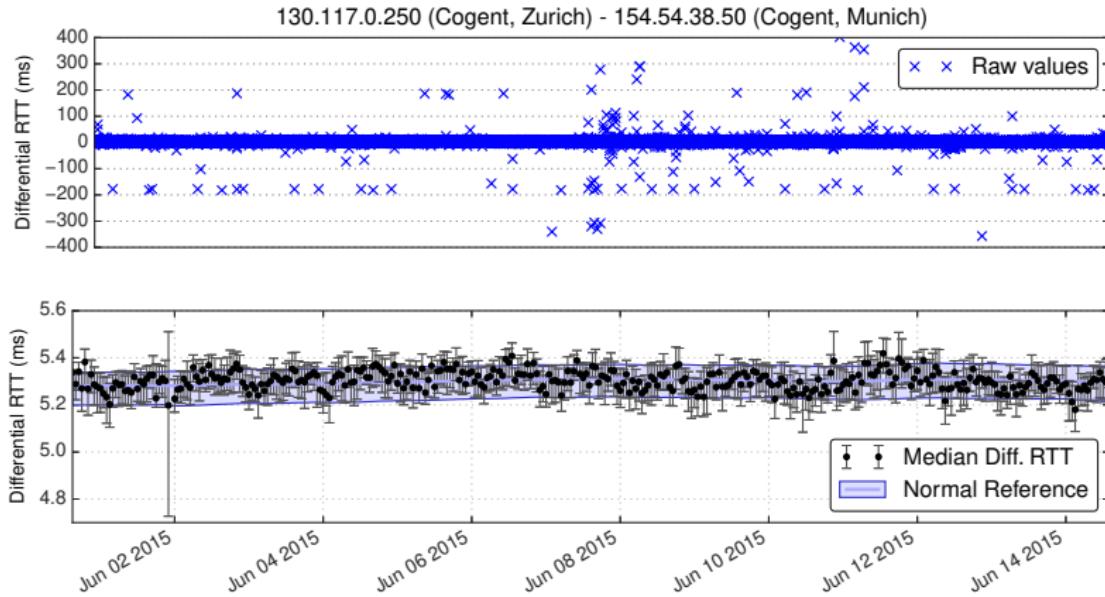
Approach

- Monitor link delays from numerous vantage points
 - Robust statistics: median variant of Central Limit Theorem
 - Model packet forwarding
 - Report anomalies



Median Diff. RTT: Example

Tier1 link, 2 weeks of data, 95 probes:

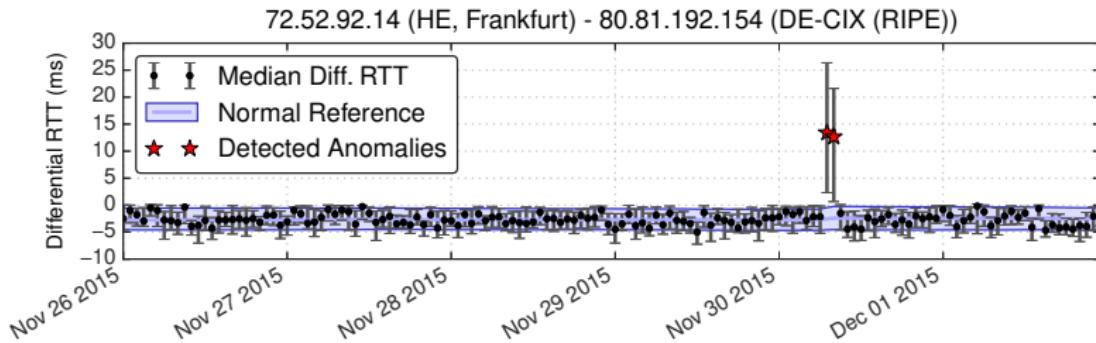


- **Stable** despite noisy RTTs
- Normally distributed
- Conf. interval: Wilson score
- Normal ref.: exp. smooth.

Detecting Delay Changes

Significant RTT changes:

Confidence interval not overlapping with the normal reference



Other Examples:

- Delay increase on JP/AU sea cable
- Delay increase during memcached DDoS attacks
- Packets wandering in Cogent

Outage Detection



Outage detection

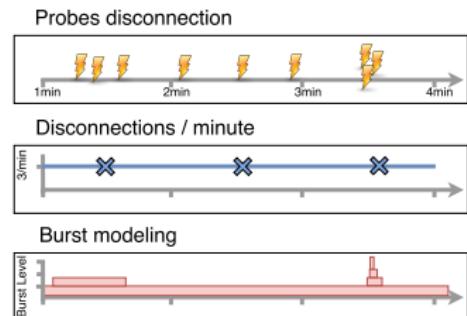
Goal

- Find important disconnections/shutdown on the Internet



Disco

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

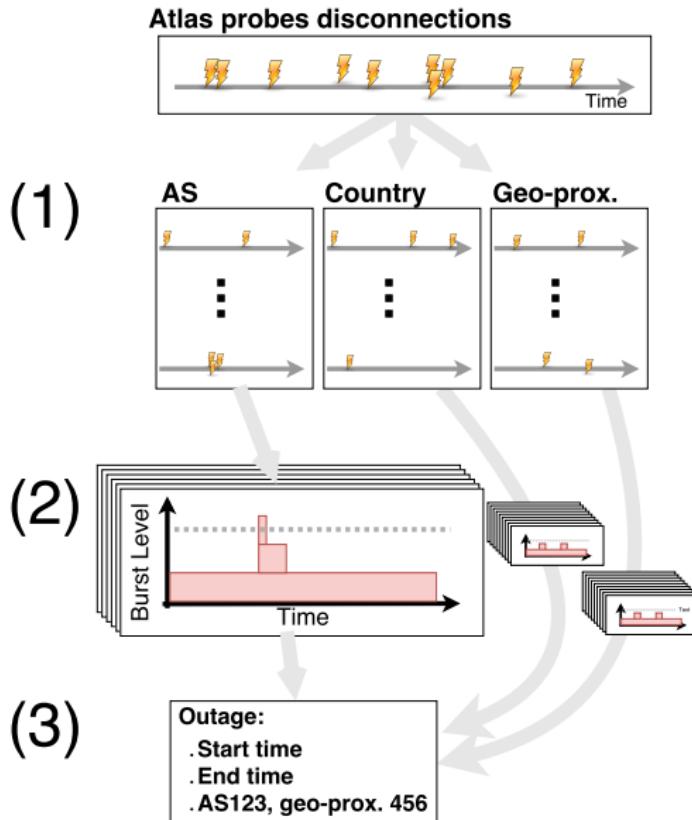


Disco Overview

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

2. Burst modeling and outage detection

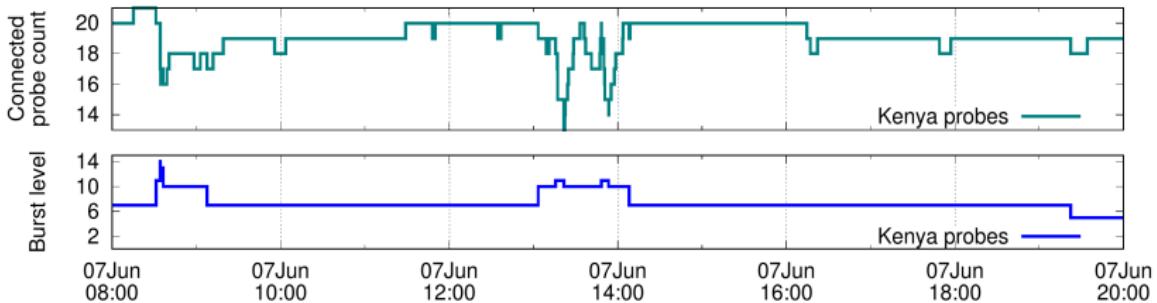
3. Aggregation and outage reporting



Burst modeling: Example



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



AS dependency

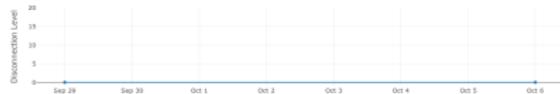


Delay and Forwarding Anomalies



Click on the graphs for more details

Network Disconnections



[Click on the graph for more details](#)

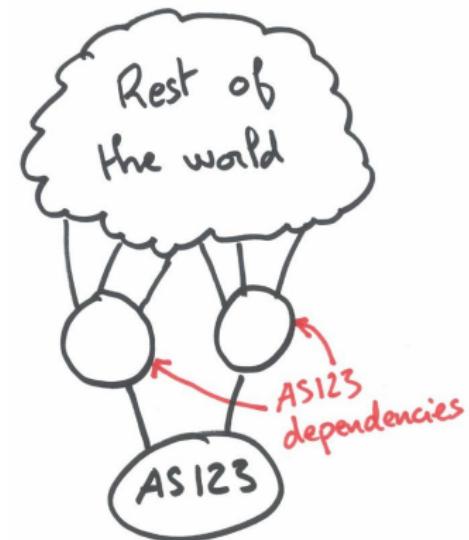
AS dependency

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

Example:

- NAIST



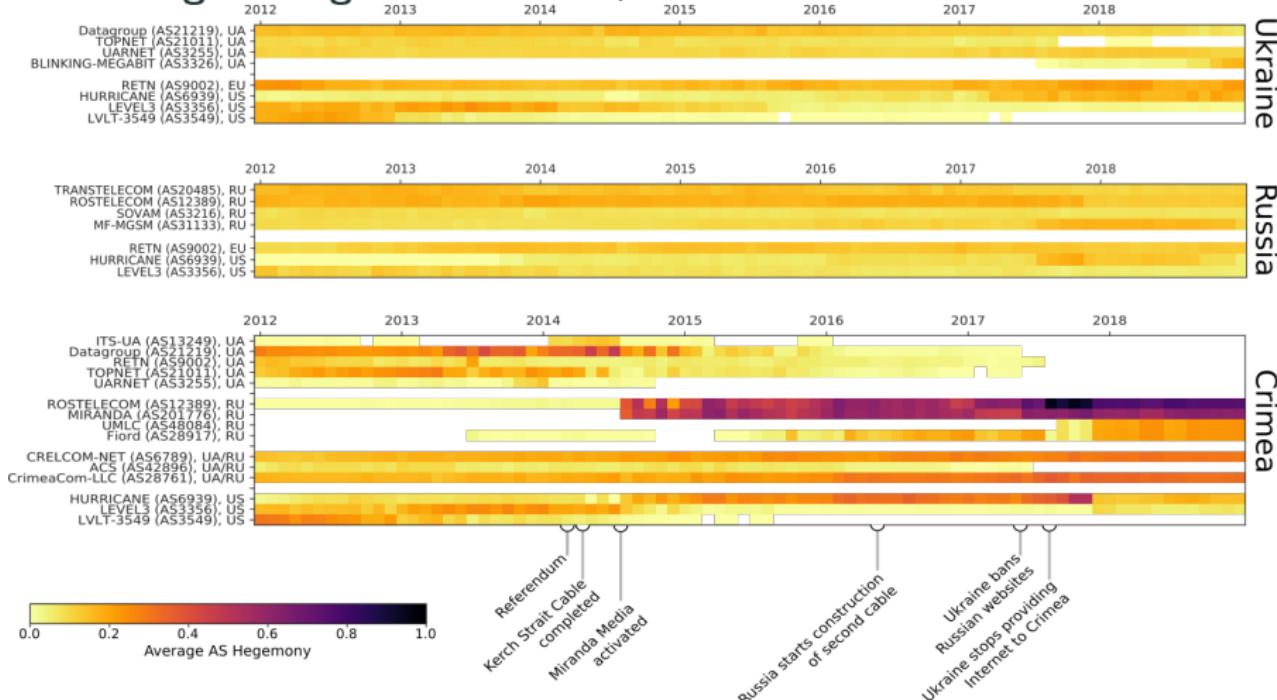
Online Results: Recent Examples

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

Study case: Internet in Crimea

Change of regime in Crimea, 2014



Summary

Internet Health Report

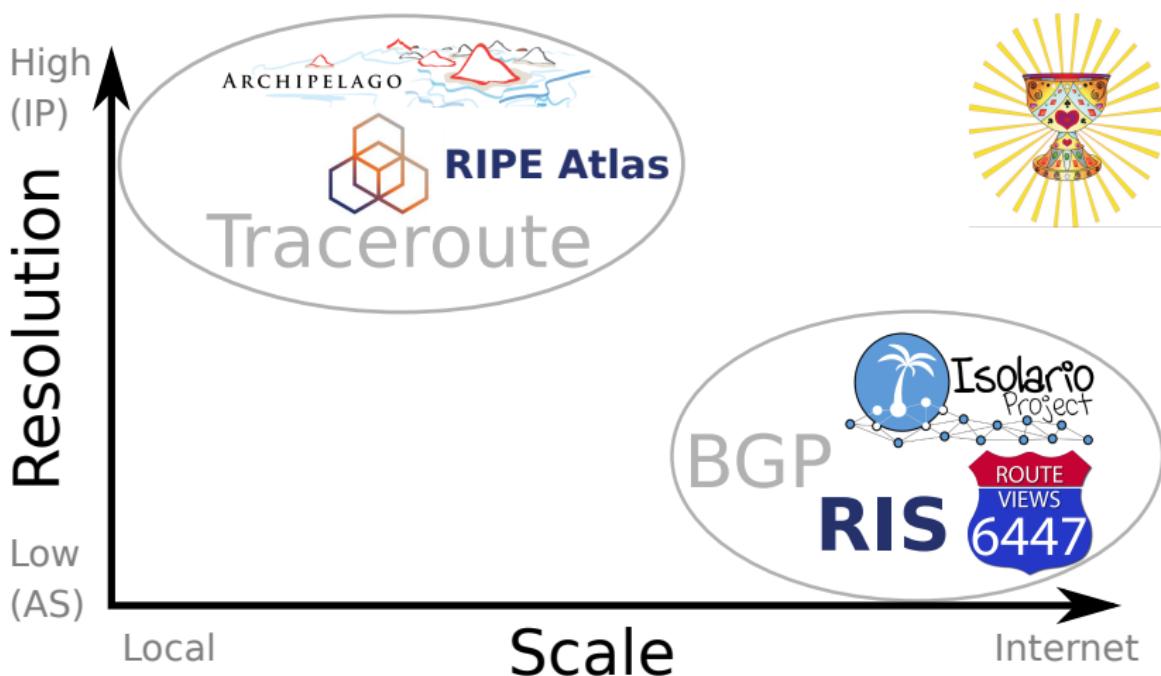
- Monitor connectivity issues
- Delay, disconnection and routing anomalies
- <https://ihr.iijlab.net>
- romain@iij.ad.jp

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.

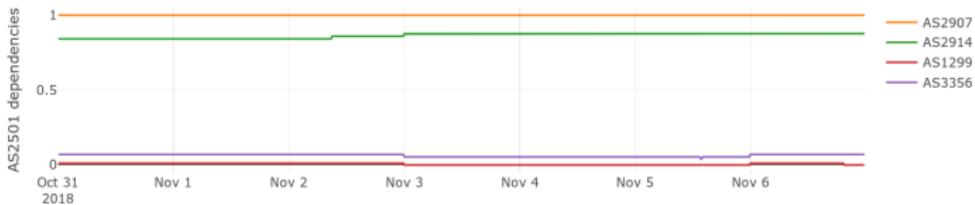
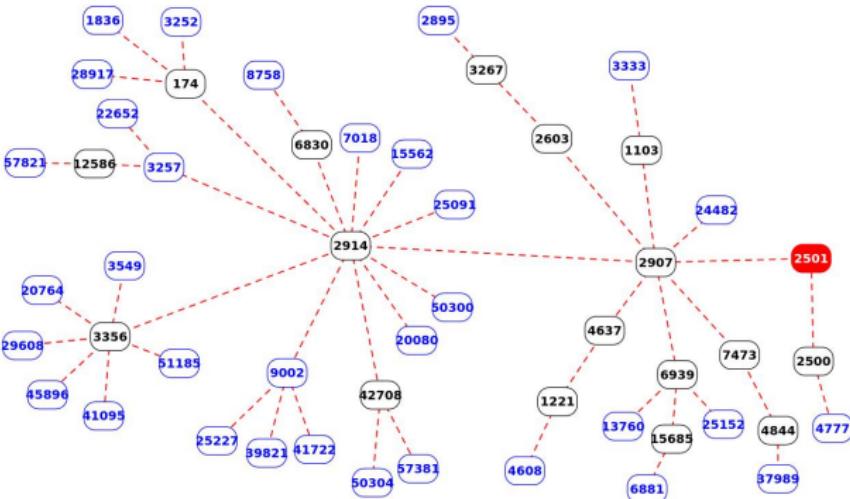
Backup

Problem Space / Data sources

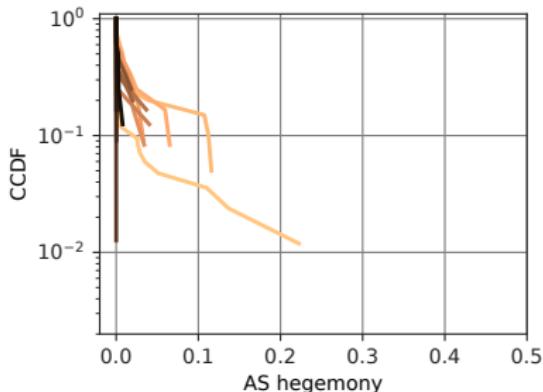


Example AS hegemony

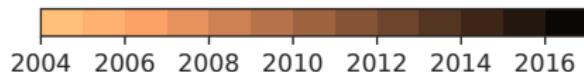
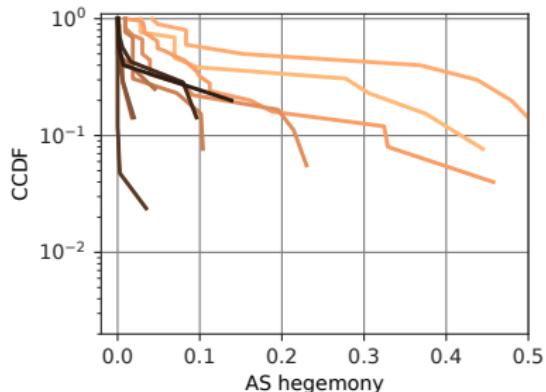
AS hegemony \approx Betweenness centrality



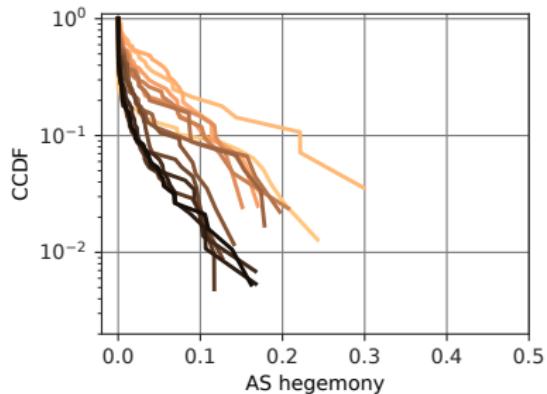
IPv4 local graph:



IPv6 local graph:



IPv4 local graph:



IPv6 local graph:

