Anycast Enumeration and Geolocation

Geolocation techniques fail with anycast IPs!

- Where is Google's 8.8.8.8?
  - **Mountain View** (IP2Location).
  - **New York, New York** (Geobytes).
  - **United States** (Maxmind).

- Our methodology
  - Determines if a service uses IP anycast.
  - Enumerates replicas sharing the same IP address.
  - Geolocates those replicas.

Methodology Workflow

Measure
Latency
Planetlab, Ripe

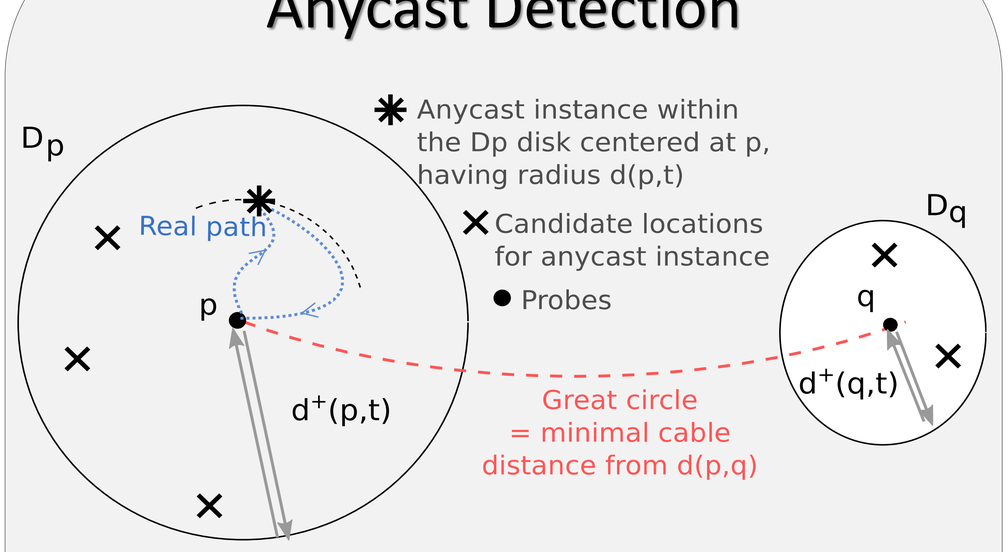
Detect
Speed of light violations

Enumerate
Solve MIS
5-approximation (Greedy)

Geolocate
Classification
Maximum likelihood

Iterate
Feedback

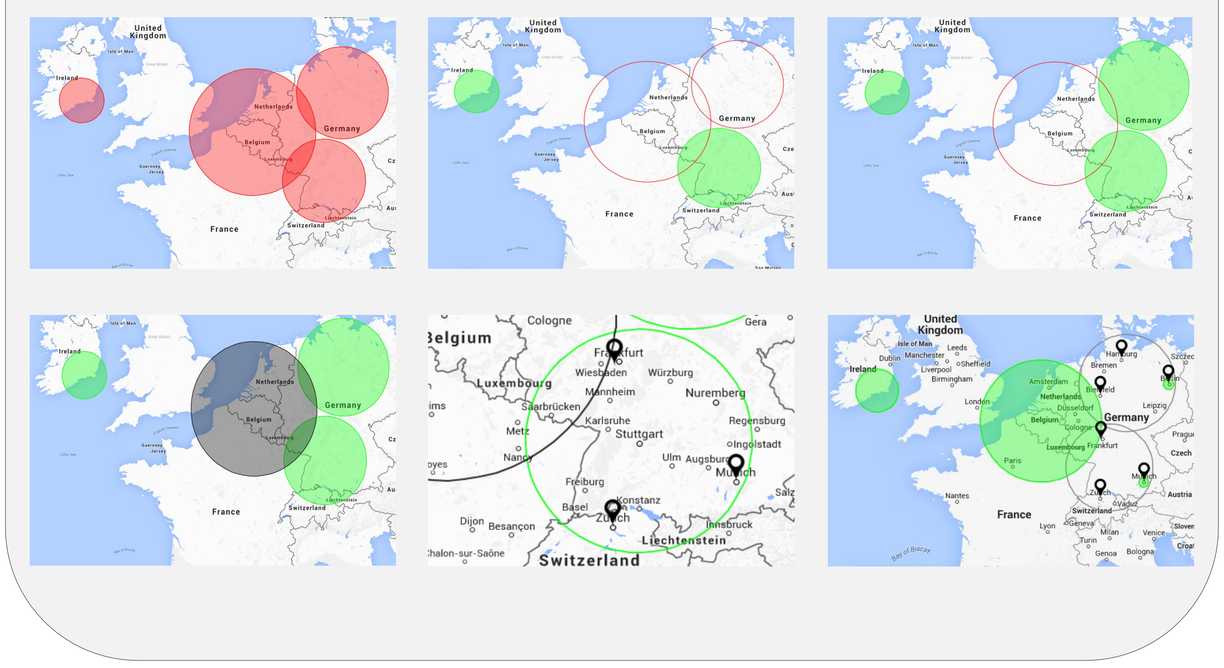
Anycast Detection



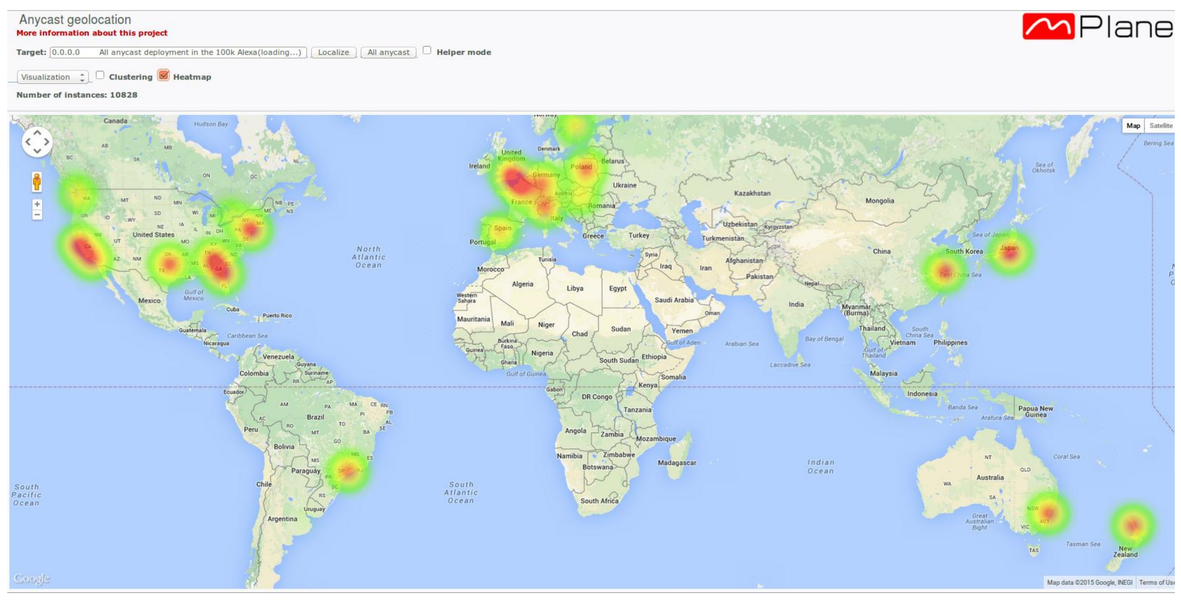
Speed of light violation:

$$d(p,q) > d(p,t) + d(q,t)$$

Anycast Enumeration and geolocation



Web demo of anycast census IPs [1]



Validation results at a glance

- Flexible: Protocol agnostic unlike DNS-based state of the art.
- Lightweight: 1000x fewer vantage points than state of the art.
- Validation (over DNS for comparison):
  - Over 50% recall.
  - Correct geolocation in 80% of cases.
  - 361km mean error for remaining case.

SCAN ME

Cicalese Danilo
Joumblatt Diana
Rossi Dario

Buob Marc-Olivier
Auge Jordan
Friedman Timur

[1] http://goo.gl/Ff8gdQ