Censored Planet

Ramakrishnan Sundara Raman
Reethika Ramesh
Steve Sprecher

Network Interference Detection

Network interference is any action by a network intermediary that violates the **confidentiality**, **integrity**, or **availability** of users' legitimate network traffic.

Background

At a global scale, measuring censorship is hard.

- Complex protocols
- Diverse DPIs and policies
- Routing and network traffic
- No ground truth

Measuring Censorship Globally

PROBLEM:

- How can we detect whether pairs of hosts around the world can talk to each other?

State of the art:

- RIPE Atlas, OONI probes
- Activists, VPNs, Research networks (PlanetLab)

Why does it matter?

- World Wide Web should be open to EVERYONE
- Confidentiality, integrity, and availability of users' legitimate network traffic should be a right
- Network interference takes away opportunities and degrades human dignity.
- Need a system to continuously measure censorship so that the information is available to everyone.

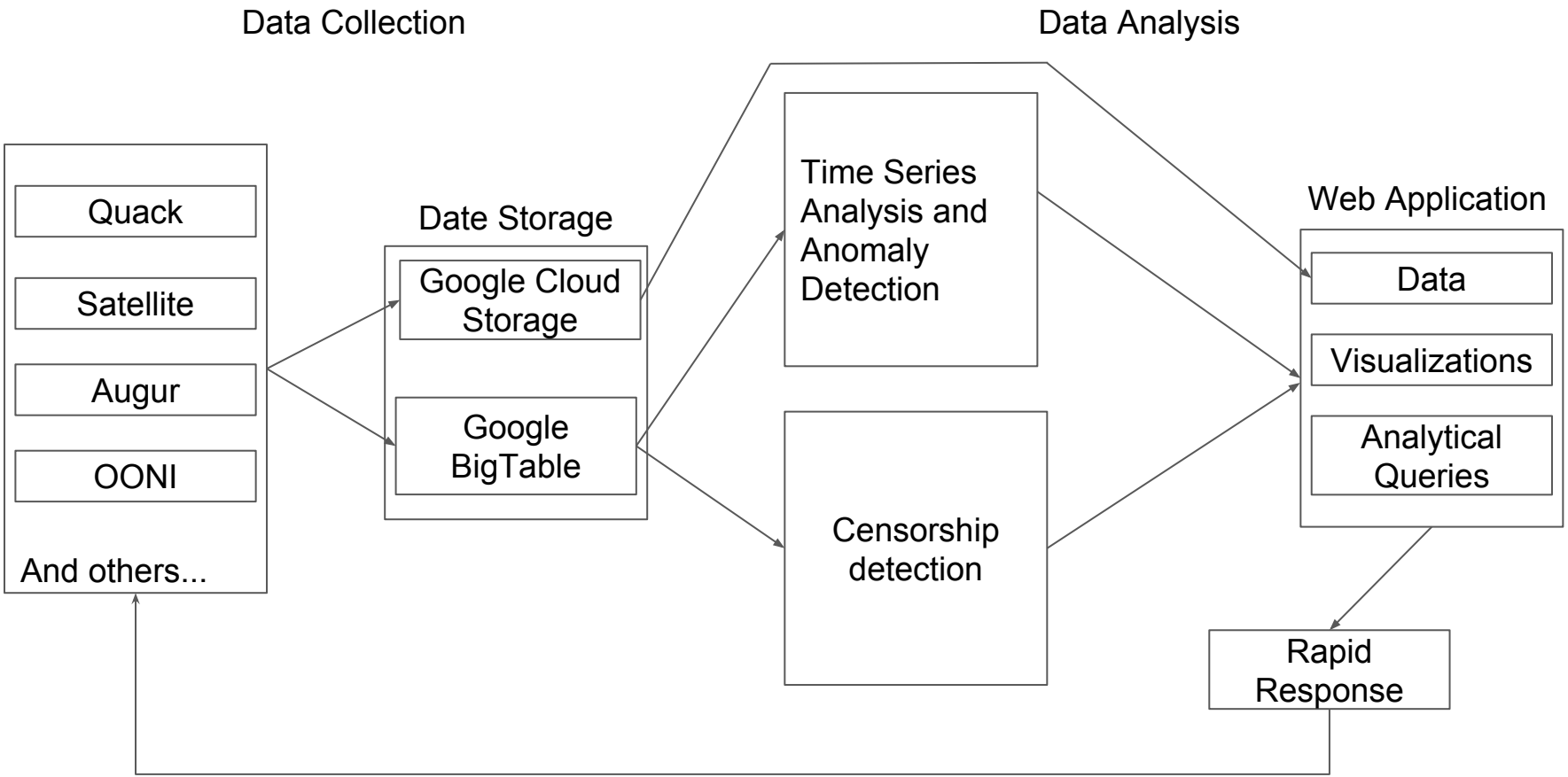
Related Work

- Not much….
  At least in aggregate & continuous measurement
- OONI and ICLab
- Censys

Remote Measurement Tools

DNS		Satellite (Iris) → Using Organizational Open Resolver
TCP/IP		Augur (Spooky Scan) → Using Global IPID routers
Application		Quack (Echo, Discard, etc) → Using services that echo

Censored Planet Design

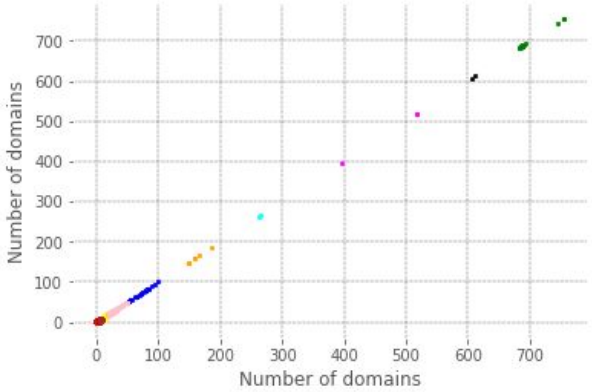


Progress - Data Collection

- Can use any measurement technique -> We are using OONI data too in addition to running our tools
- Finding reliable vantage points for measurement -> We are ranking vantage points based on performance in previous scans, and how often we can discover them.
- Augur cannot work with anycasting -> We Send spoofed packets to sites (from Michigan) with source IP set to machines we control around the world and observe if site contacts the machines. We will not consider any of the anycasted site for analysis.
- Ethically rate limiting our measurements -> We are sending only one request at a time to each vantage point.

Progress - Data Analysis

- Censorship Detection -> Use patterns in blocking to find similar techniques and policies -> A simple k-means clustering of blocking patterns yields promising initial results.



- Time series Analysis -> Compare between different algorithms for modelling and finding anomalies -> Current method is using exponential moving average and derivative and finds anomalies well.

Challenges

- How to model network topology? Routeviews?
- How to find censorship events of interest? Twitter?
- How to share data and knowledge? Tell us what you want to see from the data -> censoredplanet.org

Feedback

Censored Planet