Detection and Analysis of Large-scale Internet Infrastructure Outages

http://www.caida.org/projects/ioda

SUMMARY

Public and private sector stakeholders around the world seek ways to ensure that the Internet provides the level of reliability and resilience we have long taken for granted from the telephony network. Unfortunately, in spite of the societal and economic impact of Internet connectivity disruptions, we lack near-realtime, scalable and validated methodologies and tools to identify and understand large-scale Internet outages.

Based on experimental work in which we combined measurements at the control plane, active probing and passive traffic analysis [1,2], CAIDA developed an **operational prototype system that monitors the Internet, in near-realtime,** with the goal of **identifying macroscopic Internet outages** affecting the edge of the network, i.e., significantly impacting an AS or a large fraction of a country.

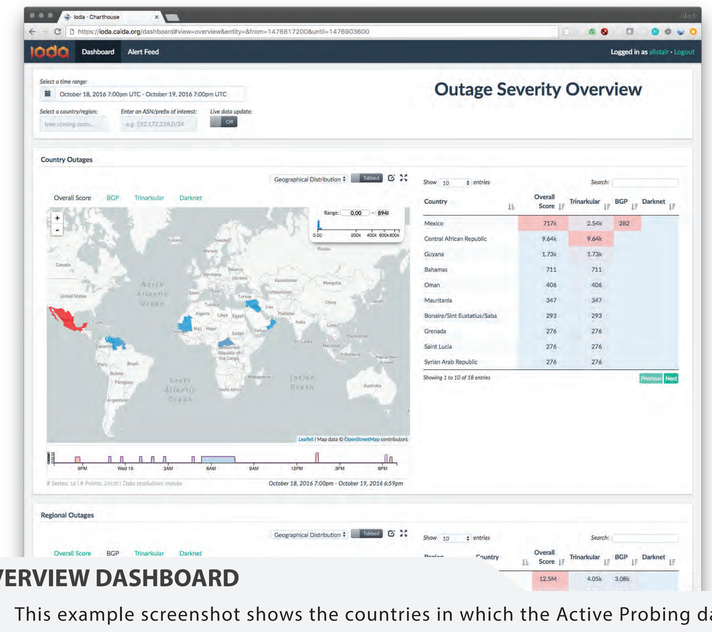
The **IODA** system processes and analyzes measurements from:

- **Global Internet routing (BGP):** we use data from ~500 monitors of the RouteViews and RIPE RIS projects to establish which network blocks are reachable based on the Internet control plane.
- **Internet Background Radiation (IBR):** we process unsolicited traffic reaching the UCSD Network Telescope monitoring a substantial portion of unutilized /8 address space.
- **Active probing:** we continuously probe a large fraction of the IPv4 address space from CAIDA Ark nodes distributed worldwide and use a methodology developed by University of Southern California [3] to infer when a /24 block is affected by a network outage.

Our outage inference system combines information from these three data sources, establishes the relevance of an event and generates **alerts**. The outage events and the corresponding signals obtained through automated analysis are displayed on **dashboards** and interactive graphs that allow the user to further inspect the data.

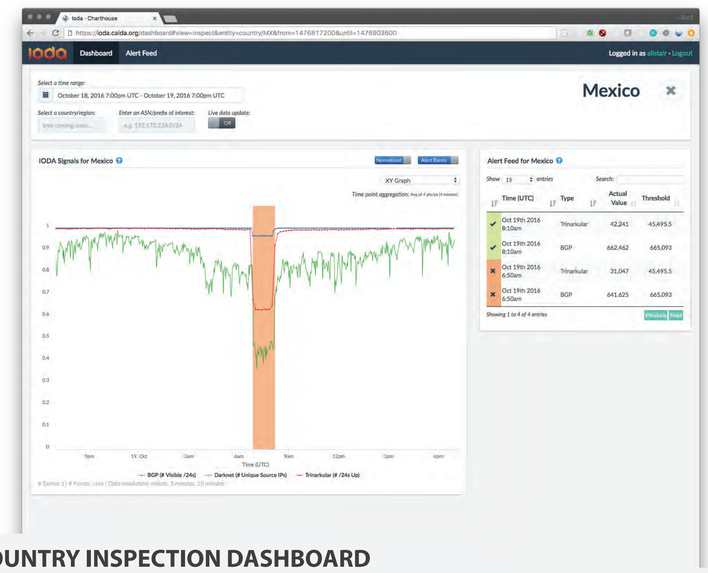
[1]A. Dainotti et al. "Analysis of Country-wide Internet Outages Caused by Censorship", ACM SIGCOMM IMC 2011
[2]A. Dainotti et al. ""Extracting bene t from harm: using malware pollution to analyze the impact of political and geophysical events on the Internet", ACM SIGCOMM CCR, Jan 2012
[3]L. Quan et al. "Trinocular: Understanding Internet Reliability Through Adaptive Probing", ACM SIGCOMM 2013.

INTERACTIVE VISUAL INTERFACE



OVERVIEW DASHBOARD

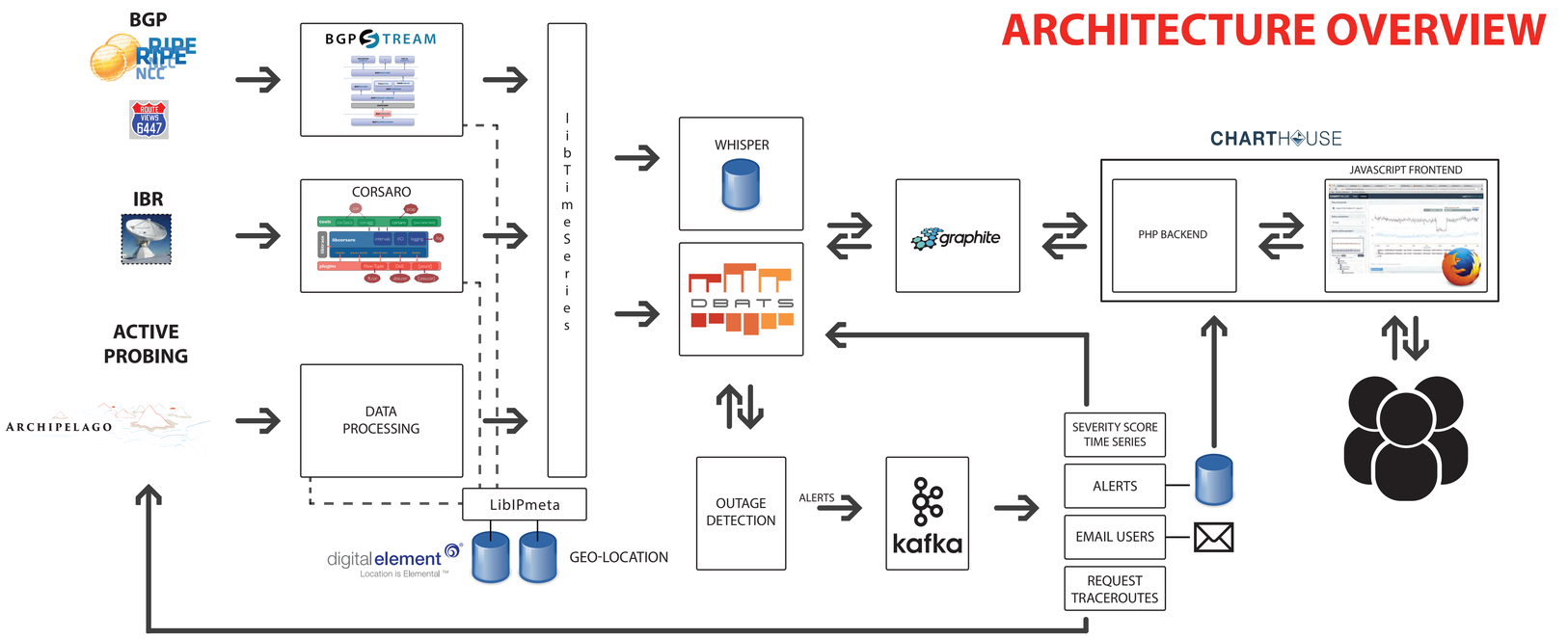
This example screenshot shows the countries in which the Active Probing data indicated an outage. The table on the right shows a list of countries with inferred outages, ranked by "Overall Score", computed as a combination of the outage severity scores of the three primary data sources.



COUNTRY INSPECTION DASHBOARD

This example screenshot shows an inferred outage that affected Mexico on October 18, 2016. The graph on the left shows the raw signal from all three of the primary IODA data sources (BGP - blue line, IBR - green line, and Active Probing - red line), overlaid with an orange band indicating duration of the inferred outage. The table on the right shows the raw alert data generated by the Automated Outage Detection component of IODA.

ARCHITECTURE OVERVIEW



PROJECT OUTCOMES

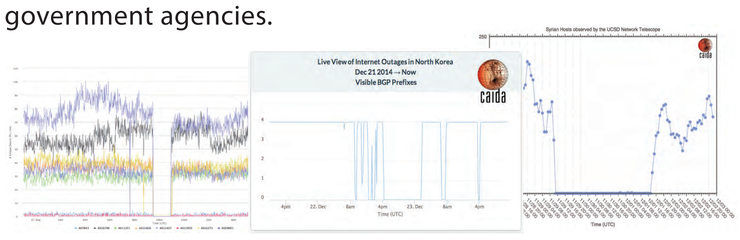
INTERESTED PARTIES AND COLLABORATORS

This project spurred several collaborations:
- With other **academic** researchers to experiment with integration of new detection methodologies, and improve our own.
- With **Industry**: Comcast is using IODA to support their own research on Internet reliability and performance; we are collaborating with Cisco Systems to support Cisco's OpenBMP in BGPStream. Both organizations funded part of our work.
- With **Government agencies**: the U.S. Federal Communications Commission is interested in technology transfer of our research results and infrastructure capabilities. The DHS S&T supports operation of the UCSD Network Telescope and generation of datasets on Internet outages with applicability to cybersecurity.

OUTREACH

We reported and **documented several relevant episodes** of connectivity disruption, including outages affecting large U.S. residential broadband ISPs, as well as entire countries almost entirely disconnected from the Internet (e.g., North Korea, Sudan, Syria).

- We published **10 research papers**, and gave more than **20 presentations** in prestigious international venues with participation of industrial and academic communities (**IETF, NANOG, RIPE, ACM IMC,** etc.) as well as in meetings with government agencies.



SOFTWARE TECHNOLOGIES

The IODA system is designed as **"Software as a Service",** being based on a complex distributed infrastructure and on large and diverse live data streams as input. The prototype system is running as an experimental service 24/7 and interactive dashboards are accessible at ***ioda.caida.org***

We released the software components we developed in this project with an **open source license**. Several of the project's software components offer general applicablity to research and applicative fields of networking. For example, BGPStream, one of the flagship software platforms developed for IODA, delivers a framework that has filled a large gap in the availability of efficient tools and programmer interfaces for the analysis and monitoring of Internet global routing.

CHARTHOUSE
CORSARO
LibTimeSeries

TEAM

Alberto Dainotti (PI) | Kc Claffy (CoPI) | Vasco Asturiano | Karyn Benson | Bradley Huffaker | Ken Keys | Alistair King | Ryan Koga | Alex Ma | Chiara Orsini

Funding sources:
NSF CNS-1228994
DHS S&T C.A. FA8750-12-2-0326

SDSC SAN DIEGO SUPERCOMPUTER CENTER
UC San Diego
caida