IMC 2017
Internet Measurement Conference
London UK

Foundation for Research and Technology – Hellas
FORTH INSTITUTE OF COMPUTER SCIENCE

INSPIRE Group

University of Crete, Department of Computer Science

IIJ Research Lab Japan
IIJ Internet Initiative Japan

Alexandros Milolidakis, Romain Fontugne, George Nomikos, Vasileios Kotronis, Lefteris Manassakis, Xenofontas Dimitropoulos

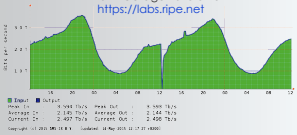
DETECTING ANOMALIES AT COLOCATION FACILITIES USING RIPE ATLAS

1. MOTIVATION

- Terabits of traffic are exchanged on an hourly basis through Internet eXchange Points, located at colocation facilities
- In the case of power failure or malfunction at colocation routers, major traffic outages can take place
- Most outages remain unreported

This work focuses on data plane measurements to shed more light on affected facilities.

AMS-IX Outage 2015-5-13
https://labs.ripe.net



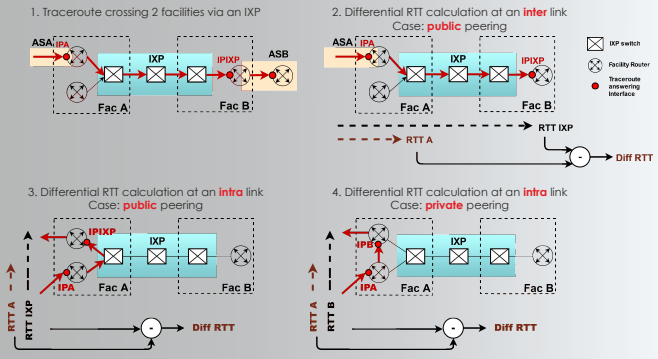
2. METHODOLOGY

1. Find IXP-facing routers within the traceroute data

Datasets used:
- RIPE Atlas 2015 IPv4 traceroute measurements [1]
- PeeringDB [2]
- CAIDA's IP-to-Alias resolution [3]

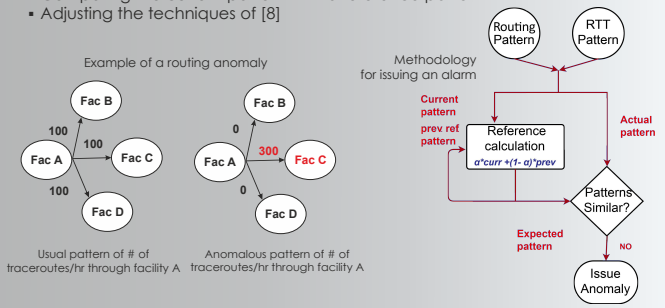
2. Detect the router facilities

Datasets used: Routeviews prefix-to-AS mapping [4]
Methodology used: Facility detection algorithm [5]



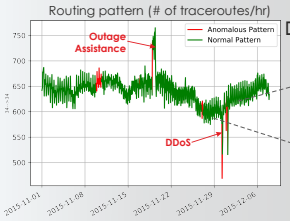
Assumptions
- Routers reply to traceroutes from their inbound interface
- The IXP-IP and the next hop-IP belong to the same AS
- PeeringDB [2] offers sufficient facility/IXP-level information for the ASes included in the traceroutes

3. Detect routing and RTT anomalies at inter and intra facility links by:
- Comparing the current pattern with a reference pattern
- Adjusting the techniques of [8]



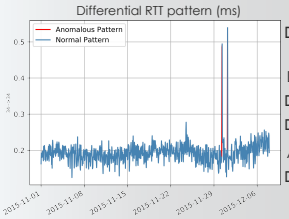
3. RESULTS

1. Intra-facility link outage:
Telehouse London (Docklands North)



Detected: Telehouse London assisting in the mitigation of Sovereign House Outage[6]

Sovereign - Telehouse Distance = 1.46Km

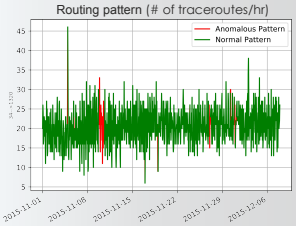


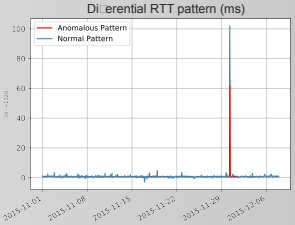
Detected: Telehouse London affected by Nov 30 DDoS attack [7]

Dates/times reported by **DNS Root servers:**
- Nov 30, 2015 at 06:50 UTC
- Dec 1, 2015 at 05:10 UTC

Additionally reported by **our system:**
- Nov 30, 2015 at 23: 00 UTC

2. Inter-facility link outage during the DDoS period:
Telehouse London → Equinix Amsterdam (AM3)
Observed only by delay change





4. FUTURE WORK

Facility detection improvements:
- Merge with additional IXP/facility databases to improve accuracy and coverage
- Use additional traceroute datasets (e.g., CAIDA's Ark)

Further Improvements on alarm detection:
- Locate the source of the alarm:
  1. Facility router
  2. Colocated IXP
  3. Facility

Migration to RIPE Atlas live streaming for real-time monitoring

REFERENCES
[1] RIPE Atlas, https://atlas.ripe.net
[2] PeeringDB, www.peeringdb.com
[3] CAIDA UCSD Internet Topology Data Kit - <2015-08>, http://www.caida.org/data/internet-topology-data-kit
[4] CAIDA UCSD Routeviews IPv4 Prefix-to-AS mappings Datasets (pfx2as) - <2015>, https://www.caida.org/data/routing/routeviews-prefix2as.xml
[5] Giotsas et al. "Mapping peering interconnections to a facility", Proc. of CoNEXT, ACM, 2015
[6] Sovereign House outage https://www.theregister.co.uk/2015/11/18/telecity_outage_fix_failed/
[7] November 30, 2015 DDoS attack report http://www.root-servers.org/news/events-of-20151130.txt
[8] Fontugne et al. "Pinpointing Delay and Forwarding Anomalies Using Large-Scale Traceroute Measurements", Proc. of IMC, ACM, 2017

RESEARCH TEAM
Alexandros Milolidakis[1,2], Romain Fontugne[3], George Nomikos[1], Vasileios Kotronis[1], Lefteris Manassakis[1], Xenofontas Dimitropoulos[1,2]
alexmil@ics.forth.gr, romain@iij.ad.jp, gnomikos@ics.forth.gr, vkotronis@ics.forth.gr, leftman@ics.forth.gr, fontas@ics.forth.gr
[1]FORTH, Greece [2]University of Crete, Greece [3]IIJ Research Lab, Japan
www.inspire.edu.gr