Detecting network outages using different sources of data

TMA Experts Summit, Paris, France

Cristel Pelsser
University of Strasbourg / ICube
June, 2019
Some perspective on:

- From unsolicited traffic
  *Detecting Outages using Internet Background Radiation.* Andrés Guillot (U. Strasbourg), Romain Fontugne (IIJ), Philipp Winter (CAIDA), Pascal Mérindol (U. Strasbourg), Alistair King (CAIDA), Alberto Dainotti (CAIDA), Cristel Pelsser (U. Strasbourg). TMA 2019.

- From highly distributed permanent TCP connections

- From large-scale traceroute measurements
  *Pinpointing Anomalies in Large-Scale Traceroute Measurements.* Romain Fontugne (IIJ), Emile Aben (RIPE NCC), Cristel Pelsser (University of Strasbourg), Randy Bush (IIJ, Arrcus). IMC 2017.
Understanding Internet health? (Motivation)

- To speedup failure identification and thus recovery
- To identify weak areas and thus guide network design
Manual observations and operations

- Traceroute / Ping / Operators’ group mailing lists
- Time consuming
- Slow process
- Small visibility

→ Our goal: Automatically pinpoint network disruptions (i.e. congestion and network disconnections)
A single viewpoint is not enough

Our goal: mine results from deployed platforms

Cooperative and distributed approach

Using existing data, no added burden to the network
Outage detection from unsolicited traffic
Dataset: Internet Background Radiation

Internet

P1 is advertised to the Internet

P1
Dataset: Internet Background Radiation

Internet

Scans, responses to spoofed traffic

P1 is advertised to the Internet

P1
Spoofed traffic

Internet

P1

Sends traffic with source in P1

Scans, responses to spoofed traffic

P1 is advertised to the Internet

Dataset: Internet Background Radiation
Spoofed traffic

- P1 is advertised to the Internet.
- Scans, responses to spoofed traffic.
- Sends traffic with source in P1.
- Responds to spoofed traffic.
- P1 is advertised to the Internet.
Dataset: IP count time-series (per country or AS)

Use cases: Attacks, Censorship, Local outages detection

Figure 1: Egyptian revolution

⇒ More than 60,000 time series in the CAIDA telescope data.

We use drops in the time series are indicators of an outage.
Current methodology used by IODA

Detecting outages using **fixed thresholds**
Our goal

Detecting outages using **dynamic thresholds**
Outage detection process

![Graph showing time series data with labeled training, validation, and test periods.](image-url)
Outage detection process

Prediction and confidence interval
When the real data is outside the prediction interval, we raise an alarm.

We want a prediction model that is robust to the seasonality and noise in the data → We use the SARIMA model\(^1\).

\(^1\)More details on the methodology on wednesday.
Characteristics

- 130 known outages
- Multiple spatial scales
  - Countries
  - Regions
  - Autonomous Systems
- Multiple durations (from an hour to a week)
- Multiple causes (intentional or non intentional)
Evaluating our solution

Objectives

• Identifying the minimal number of IP addresses
• Identifying a good threshold

Threshold

• TPR of 90% and FPR of 2%

Figure 2: ROC curve
Comparing our proposal (Chocolatine) to CAIDA’s tools

- More events detected than the simplistic thresholding technique (DN)
- Higher overlap with other detection techniques
- Not a complete overlap
  → difference in dataset coverage
  → different sensitivities to outages
Outage detection from highly distributed permanent TCP connections
Proposed Approach

Disco:

- Monitor long-running TCP connections and synchronous disconnections from related network/area
- We apply Disco on RIPE Atlas data, where probes are widely distributed at the edge and behind NATs/CGNs providing visibility Trinocular may not have

→ Outage = synchronous disconnections from the same topological/geographical area
Assumptions / Design Choices

Rely on TCP disconnects

- Hence the granularity of detection is dependent on TCP timeouts

Bursts of disconnections are indicators of interesting outage

- While there might be non-bursty outages that are interesting, Disco is designed to detect large synchronous disconnections
Proposed System: Disco & Atlas

RIPE Atlas platform

- 10k probes worldwide
- Persistent connections with RIPE controllers
- Continuous traceroute measurements (see outages from inside)

→ Dataset: Stream of probe connection/disconnections (from 2011 to 2016)
1. Split disconnection stream in sub-streams (AS, country, geo-proximate 50km radius)

2. Burst modeling and outage detection

3. Aggregation and outage reporting
Why Burst Modeling?

Goal: How to find synchronous disconnections?

- Time series conceal temporal characteristics
- Burst model estimates disconnections arrival rate at any time

Implementation: Kleinberg burst model\(^2\)

Monkey causes blackout in Kenya at 8:30 UTC June 7th 2016

Same day RIPE rebooted controllers
Results

Outage detection:

- Atlas probes disconnections from 2011 to 2016
- Disco found 443 significant outages

Outage characterization and validation:

- Traceroute results from probes (buffered if no connectivity)
- Outage detection results from Trinocular
Comparison to traceroutes:

- Probes in detected outages can reach traceroutes destination?
  → Velocity ratio: proportion of completed traceroutes in given time

→ Velocity ratio ≤ 0.5 for 95% of detected outages
Comparison to Trinocular (2015):

- Disco found 53 outages in 2015
- Corresponding to 851 /24s (only 43% is responsive to ICMP)

Results for /24s reported by Disco and pinged by Trinocular:

- 33/53 are also found by Trinocular
- 9/53 are missed by Trinocular (avg time of outages < 1hr)
- Other outages are partially detected by Trinocular

23 outages found by Trinocular are missed by Disco

- Disconnections are not very bursty in these cases

→ Disco’s precision: 95%, recall: 67%
Outage detection from large-scale traceroute measurements
Dataset: RIPE Atlas traceroutes

Two repetitive large-scale measurements

- **Builtin**: traceroute every 30 minutes to all DNS root servers ($\approx 500$ server instances)
- **Anchoring**: traceroute every 15 minutes to 189 collaborative servers

Analyzed dataset

- May to December 2015
- 2.8 billion IPv4 traceroutes
- 1.2 billion IPv6 traceroutes
Monitor delays with traceroute?

Traceroute to “www.target.com”

```
$ traceroute www.target.com
traceroute to target, 30 hops max, 60 byte packets
1  A   0.775 ms  0.779 ms  0.874 ms
2  B   0.351 ms  0.365 ms  0.364 ms
3  C   2.833 ms  3.201 ms  3.546 ms
4  Target 3.447 ms  3.863 ms  3.872 ms
```
Monitor delays with traceroute?

Challenges:
- Noisy data
Monitor delays with traceroute?

Challenges:
- Noisy data
- Traffic asymmetry
What is the RTT between B and C?

```
~$ traceroute www.target.com
traceroute to target, 30 hops max, 60 byte packets
 1 A  0.775 ms  0.779 ms  0.874 ms
 2 B  0.351 ms  0.365 ms  0.364 ms
 3 C  2.833 ms  3.201 ms  3.546 ms
 4 Target  3.447 ms  3.863 ms  3.872 ms
```

\[ \text{RTT}_C - \text{RTT}_B = \text{RTT}_{CB}? \]
What is the RTT between B and C?

- No!
- Traffic is asymmetric
- $RTT_B$ and $RTT_C$ take different return paths!
What is the RTT between B and C?

- No!
- Traffic is asymmetric
- \( RTT_B \) and \( RTT_C \) take different return paths!
- Differential RTT: \( \Delta_{CB} = RTT_C - RTT_B = d_{BC} + e_p \)
Problem with differential RTT

Monitoring $\Delta_{CB}$ over time:

$\rightarrow$ Delay change on BC? CD? DA? BA???
Proposed Approach: Use probes with different return paths

Differential RTT: \( \Delta_{CB} = x_0 \)
Proposed Approach: Use probes with different return paths

Differential RTT: $\Delta_{CB} = \{x_0, x_1\}$
Proposed Approach: Use probes with different return paths

Differential RTT: $\Delta_{CB} = \{x_0, x_1, x_2, x_3, x_4\}$
Proposed Approach: Use probes with different return paths

Differential RTT: \( \Delta_{CB} = \{x_0, x_1, x_2, x_3, x_4\} \)

Median \( \Delta_{CB} \):
- Stable if a few return paths delay change
- Fluctuate if delay on BC changes
Median Diff. RTT: Tier1 link, 2 weeks of data, 95 probes

- **Stable** despite noisy RTTs (not true for average)
- Normally distributed

![Graph showing differential RTTs and median values over time](image-url)
Detecting congestion

Significant RTT changes:
Confidence interval not overlapping with the normal reference
Results

**Analyzed dataset**

- Atlas *builtin/anchoring* measurements
- From May to Dec. 2015
- 2.8 billion IPv4 traceroutes
- 1.2 billion IPv6 traceroutes
- Observed 262k IPv4 and 42k IPv6 links (core links)

We found a lot of congested links!
Let’s look at one example
Australia's internet hit hard by massive Malaysian route leak

Telekom Malaysia apologises for BGP bungle.

Earlier today a massive route leak initiated by Telekom Malaysia (AS4788) caused significant network problems for the global routing system. Primarily affected was Level3 (AS3549 - formerly known as Global Crossing) and their customers. Below are some of the details as we know them now.

Starting at 08:43 UTC today June 12th, AS4788 Telekom Malaysia started to announce 179,000 of prefixes to Level3 (AS3549, the Global crossing AS), whom in turn accepted...
Study case: Telekom Malaysia BGP leak
Study case: Telekom Malaysia BGP leak
Study case: Telekom Malaysia BGP leak
Study case: Telekom Malaysia BGP leak

Not only with Google... but about 170k prefixes!
Rerouted traffic has congested Level3 (120 reported links)

- Example: 229ms increase between two routers in London!
Reported links in London:

- Delay increase
- Delay & packet loss

→ Traffic staying within UK/Europe may also be altered
But why did we look at that?

Per-AS alarm for delay

Figure 8: Delay change magnitude for all monitored IP addresses in two Level(3) ASs.
We proposed 3 different techniques to detect outages for 3 different sources of data

- Each source of data has its own coverage
  - Core links (congestion and failures)
  - Prefix, country, region, AS disconnections
We proposed 3 different techniques to detect outages for 3 different sources of data

- Each source of data has its own coverage
  - Core links (congestion and failures)
  - Prefix, country, region, AS disconnections
- Each source of data has its own noise, properties
  - Identifying the suitable model is a challenge
Conclusions and perspectives (2)

There is no substantial, state of the art ground truth to validate the results. We resort to

- the comparison of different techniques with different coverages
- evaluations on the basis of partial ground truth
- characterizations of the detected outages based on the detection algorithm used
http://ihr.iijlab.net