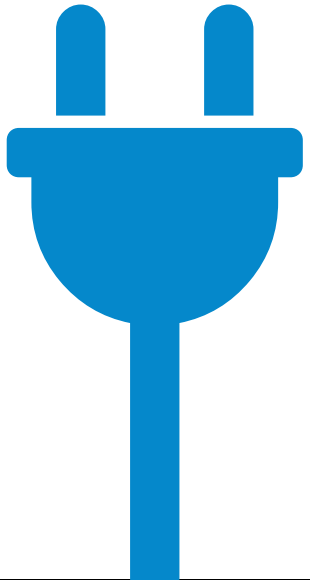
OONI

Investigating Internet Blackouts

From the edge of the network

Arturo Filastò
Leonid Evdokimov
Will Scott



4th April 2018

Table of Contents

State of the art

We divide the possible approaches to investigating internet blackouts into three broad categories:

- **Analyzing statistics** from existing datasets
- **Probing from "outside"**
- **Probing from the "edge"**

Each approach has pros and cons.

Analyzing statistics from existing datasets

We wrote a blog post on analysis of blackouts embedded within other measurement datasets.[1]

Useful datasets potentially including (or with holes due to) blackout data include:

- Google traffic reports
- MLab Measurements for a given country
- Geotagged tweets
- BGP announcement feeds

Pros

- If the dataset is already public, the use of it is easy

Cons

- This method isn't really conclusive, in the sense that there could very well be other reasons for a drop (or increase) in traffic from a given country
- Generally the resolution of the publicly available datasets is insufficient to identify small-scale blackouts

Active probing from "outside"

This involves doing network scans from a vantage point that is outside of the affected region. Example of this may involve doing ZMap-like scans of large network blocks or measuring "internet background radiation" as done by IODA.[2]

Pros

- You don't need to involve local participants/volunteers
- It's fairly easy to investigate a blackout in a new region

Cons

- It does not play well with Carrier grade NAT and IPv6, that are quite commonly used on mobile and modern networks (see: RIPE NCC Hostcount[3] for reasoning around "*After this analysis, it was obvious that the results of the Hostcount are not precise enough to be valuable*")
- Since the measurement is done from the outside it's not necessarily conclusive evidence. Some IP ranges may still be reachable (or announced), yet the users in the country cannot actually get access to the internet.

[1] https://ooni.torproject.org/post/examining-internet-blackouts
[2] https://www.caida.org/projects/ioda/
[3] https://labs.ripe.net/Members/markd/hostcount

Active probing from "the edge"

This involves the use of vantage points in countries under investigation, and running measurements directly.

Pros

- Measurements directly show conditions experienced at that network location.

Cons

- If the internet is blacked out, it's hard to efficiently get measurements "out".

Edge-based measurements are most likely to be able to positively identify blackouts, and provide deeper understanding of the mechanisms involved in blocking. By measuring the network from the "edge" we are able to truly capture what is the experience of a on-the-ground user and possibly come up with ways to minimise the impact of a blackout. However, unlike the other approaches, measurements captured within a blacked-out region are not immediately available to external researchers, and new strategies will need to be developed to exfiltrate them.

Because of the synergy with the existing OONI probe deployment and methodology and because of our existing focus into investigating the root technical mechanisms involved in blocking, we will focus on edge-based probing as the approach taken by OONI. To do this, we propose a methodology for integrating this probing as part of the OONI Probe mobile application.

Methodology

In the section we will outline what is our reasoning in terms of going about developing a methodology for investigating internet blackouts from the edge of the network. We will focus on techniques that can be implemented and deployed as part of a mobile application, but will also explore the possibility of having dedicated desktop/hardware deployments. Where relevant we will highlight which ones may require special permissions on the device or can only work on a particular mobile platform.

Outage detection

As a first step we need to have some form of heuristic that allows us to understand that a particular device is experiencing some form of network outage. This can be used as an indicator to then trigger more fine-grained and in-depth measurements.

Since this need to be done with a fairly high frequency, it's crucial that what we do to detect an outage consumes minimal amounts of network bandwidth and that we reserve the most bandwidth intensive measurements for the follow-up stage.

Each attempt to fetch some minimal document from HTTPS server is ~6KiB of data sent over the wire: DNS for A and AAAA, TLS handshake and teardown. That's ~17MiB a month if the test is done every ~15 minutes. The value of 15min comes from minimal inexact interval supported by Android's AlarmManager.[4]

Failures should trigger follow-up measurements to ensure that it's something that looks like a blackout and not just a temporary OONI service failure or blockage, last-mile failure (heavy wifi interference, or broken LAN switch, CPE failure), ISP subscription termination (e.g. quota depletion) or network glitch.

[4] https://developer.android.com/reference/android/app/AlarmManager.html

Follow up measurements

By follow up measurements we mean what network measurements should be run on the device that can lead to useful telemetry to understand if an internet blackout has occurred and characterize its nature.

OONI Probes have different abilities to inspect the network environment.
Below are the classes of follow-up measurements depending on the class of probe:

- Probe with IP connectivity (both mobile and desktop)
- Probe connected to the GSM network (mobile probe connected to the GSM network or desktop probe with GSM modem)

Probes with IP connectivity

They can do the following measurements (ordered by implementation complexity):

1. Send DNS query for `.` (root domain) to local nameserver and root nameservers
2. UDP traceroute with `.` query
3. UDP traceroute with NTP query to some set of "stable" NTP servers
4. Traceroute to some address in some set of unroutable prefixes
5. HTTP traceroute to `http://example.net/` and Google/Apple/Mozilla captive portal endpoints
6. HTTP and ICMP-PING check for `http://${default_gateway}/`
7. Repeat (6) for next hops that are common to all traceroutes
8. PMTU discovery to example.net and captive portal endpoints
9. TCPMSS discovery to test-helper endpoint
10. Tests to various network services within same AS (open resolvers, webservers... censys & shodan)

Both (2) and (3) are useful as DNS may be intercepted for network censorship purposes, but that's usually not the case for NTP. Comparison of (4) to (3) and (2) will reveal the nearest router that is able to discard unroutable prefix, thus, likely holding full-view. If (2), (3) and (4) all are the same that means that the cause of the outage is ***UNLIKELY*** a cable cut and/or temporary routing glitch.

(5) MAY be useful to distinguish "internet blackout" from ISP subscription termination (e.g. quota depletion): some ISPs redirect HTTP queries to some sort of captive portal reminding the user to top up the account.

(6), (7) and (8) try to draw a line between "user's LAN" and "ISP network" and may be used to ensure that the LAN is well-functioning. Errors have little meaning for these tests (unless prior knowledge about that specific network is accumulated by OONI Probe, it's unclear if we want to accumulate that knowledge like MAC addresses of the router even locally), but successes indicate that CPE and LAN are probably okay. (8) will highlight the hop having some sort of tunnel.

There may be other UDP-based network services that are useful for traceroutes purposes (e.g. SNMP), but they're not so widespread. There are other well-known public network protocols besides HTTP-based captive portals detectors and public DNS resolvers, e.g. it's possible to check if A-GPS MSA endpoints are reachable.[5] The reason to check various protocols is to ensure that the "blackout" is not protocol-specific.

[5] http://iatip.blogspot.com/2013/03/be-careful-with-assisted-gps.html

Probe connected to the GSM network

The case means that IP connectivity can't be established. Unfortunately there is little that can be done in this case (and this is, probably, the most interesting case): OONI considers that requiring root capabilities for mobile OONI Probe application is not something that is currently possible. That's why OONI can't gather additional GSM statistics like IMSI catcher and jamming detector applications do via GSM modem diagnostics port.

The methodology is to analyze data en masse: lack of OONI Probe orchestration requests may suggest that some probes are gone because of a blackout, but blackouts do not happen daily, so it's crucial to understand a reason for gone probe.

The probe may memoize various geo-specific data (GPS data, GSM net name, Cell ID, WiFi MAC addresses) and network-state data (including state of Data and Airplane-mode toggles) and upload these measurements afterwards. Possibly, converting geo data to single privacy-preserving data point when the network is back.

Also, the probe may include a sequence number to orchestration queries and restrain of sending the queries when it detects "user-initiated network blackout" (airplane mode). That sequence number may also help to distinguish genuine network problems from "end-user's problems".

Sending back the measurements

Due to the nature of internet blackouts, once we have gathered enough evidence that something is happening on the network, A major challenge will be efficiently relaying that information to external researchers for analysis.

The basic approach OONI expects to follow is to have probes collect all the data described in the probes section above and send it back to our central servers once the blackout is over and internet connectivity is restored. However if we are interested in gaining more real-time information while the blackout is happening, we are also evaluating other possible strategies that may work even while there is an ongoing blackout.

According to anecdotal reporting, it may be the case that during some blackouts, only the Internet is affected, but phone SMS and voice communication remain active.
If that is the case a possible strategy could be to relay information via:

- A SMS message with some amount of information encoded in the message body
- Interaction with a USSD[6] service is a potential alternative.
- Placing a voice call to a local VoIP extension and transmitting the data as audio or DTMF, similarly to how an analog modem or IVR would work

If these methods were to fail, we could also consider encouraging users to travel to unaffected regions (or find someone with BGAN[7] connection) and then transmit the data over the internet.

While transmitting OONI data over hamradio[8] (amateur radio) may be considered an interesting exercise, it's probably imperfect idea as hamradio operators are subject to licensing in most countries, intentional internet blackouts are usually triggered during politically sensitive events and it's unclear if transmitting alike data violates licensing terms or not. On the other hand, finding a local hamradio operator may be an easier task for OONI Probe user than finding someone with BGAN connectivity.

[6] https://en.wikipedia.org/wiki/Unstructured_Supplementary_Service_Data
[7] https://en.wikipedia.org/wiki/Broadband_Global_Area_Network
[8] https://en.wikipedia.org/wiki/Amateur_radio

For even more extreme circumstance, we could also ask users to travel to a specific, close, geopoint with a 1m x 1m space blanket at a given time and look at satellite images to spot the presence or these white/golden squares.

In any case we would like the OONI Probe to notify the user that we suspect an internet outage is ongoing and allow them to enrich the measurement data with user supplied information such as:

- Where they informed that a internet blackout was going to happen?
- Are they aware of an ongoing power outage?
- Are they able to confirm the outage through some other means?
- Is their landline phone working?
- Metadata pertaining to the ISP they are on

This will also be an opportunity to confirm some data that we can derive automatically, for example the ISP and their location.

Probe location

In order to properly qualify internet blackouts, it's important that we have granular location information. Since OONI is committed to protecting users privacy to the extent that it's possible, we plan on developing a strategy to send back location information that is granular enough to be useful, yet not pose a privacy risk for the users.

Currently OONI probe includes only ASN and Country information by default. Moreover the user can also include their IP address on an opt-in basis. To investigate internet blackouts, which often times are localised to only a region or even city, we need more precise location information.

Our idea is to build some geographical contours (using OpenStreetMap as a basis) or level3 or level4 regions. The probe will then ask the phone for the GPS coordinate, but we will send back to OONI only the contour that they are located inside of. This way users will still just send back location information that is accurate to the city level (in the most granular case) and not compromise their safety.

Implementation plan

In this section we will outline how we plan to validate which techniques are most useful and can actually be implemented as part of our OONI Probe mobile app.

1. Implement the tests described in the methodology section as "Proof of concept" quality code
2. Develop a test bed that includes the PoC quality tests
3. Get at least one vantage point in a country that is affected by regular internet blackouts and have somebody run these experiments
4. Evaluate the results from (3) and understand which techniques work and which ones don't work and implement a subset of them as part of OONI Probe mobile

Hardware based test bed

Through a hardware based test bed that we will ask on the grounds partners to host, we will gather high quality network measurements. The reason to choose a hardware based approach for this initial prototype is that it allows us to iterate faster on results and try out more ideas that may not be technically feasible in a mobile app environment.

The feature set we are going to consider for an MVP are the following:

- Remote access via ssh
- Redundant network connections (via 3G modems and ideally also LAN)
- DNS query and traceroute based tests from the vantage point of the probe (points (1) ... (8) listed in the “Probes with IP connectivity” section) and store the experiment results locally.

Experimental mobile app release

In the initial phase, as soon as the hardware test bed is deployed, we will also ship as part of the mobile app an opt-in experimental feature to carry out internet blackouts testing.
We will be reaching out to partners in affected regions to enabled this advanced setting and try out the experiments.

Based on what we learn with the hardware test bed we will iterate on the experimental feature. The reason to include it as an opt-in advanced setting is that, due to the experimental nature of these tests, they could lead to making the rest of the app less stable and therefore we will only be trying it out with a subset of all our users.

Features that will be needed in order to make this work on mobile are:

- Approximation of the GPS coordinates of the probe
- Implementation of the tests researched in the Hardware based test bed as part of Measurement Kit
- Some backend logic to orchestrate the probes

Stable mobile app release

When this is ready we will be shipping the methodology, and enabled by default, in all OONI Probe instances.