net.tagger: Crowdsourcing Local physical network infrastructure

CAIDA AIMS Workshop
UCSD, 16 April, 2019

Justin P. Rohrer
Robert Beverly
Riqui Schwamm
Dan Woodman
Marie Rogers

Naval Postgraduate School
net.tagger

• Background and Motivation
• Our Solution
• Preliminary Results
• Future Work
Topology Discovery

• Lots of work on *logical* topology discovery:
  • Active/passive measurements (traceroute, BGP, etc)
  • Finding IP, router, AS, or even organization-level graph

• Less work on *physical* topology in research space
  • Internet Atlas
  • Topology Zoo

  *net.tagger is a complementary project focusing on physical network infrastructure discovery*

• Focus on microscopic detail, vs existing macroscopic efforts
Why care about physical network?

- Identify logically independent, but physically dependent paths
- Improve critical infrastructure protection

Howard Street Tunnel
Fire

“Vandals cut N. Arizona fiber”

L3 California “Bad hole day”
How well do we know the physical network

• Existing work focuses on:
  • PUC databases
  • Published network maps

• No aggregated database
  • Infrastructure is global
  • PUC databases are local
  • Existing maps are frequently incorrect
How to map physical topologies?

• Latency-based geolocation from lots of vantage points?
  • Too inaccurate

• Buy maps from 3rd party companies?
  • Expensive, incomplete

• Have your grad students read the environmental impact statements at city hall?
  • Expensive, incomplete

• Or, just go look for it?

Make crowdsourced discovery easy
Available now on Android and IOS!
Crowdsourcing Model

• Develop list of street-level indicators of Internet infrastructure
• Develop app that allows users to tag location, type, provider, and metadata for indicators
• Compile results, analyze

Users answer the question “What is here?”
Later, researchers can ask “Where is X?”
Physical infrastructure markers everywhere

• Meta-data: provider name
Physical infrastructure markers everywhere

• Meta-data: keywords
### Dig Markings, warnings

<table>
<thead>
<tr>
<th>UTILITY</th>
<th>COLOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROPOSED EXCAVATION</td>
<td>WHITE</td>
</tr>
<tr>
<td>ELECTRIC POWER LINES, CABLES, CONDUIT AND LIGHTING CABLES</td>
<td>RED</td>
</tr>
<tr>
<td>POTABLE WATER</td>
<td>BLUE</td>
</tr>
<tr>
<td>STEAM, CONDENSATE, GAS OR OIL COMPRESSED AIR</td>
<td>YELLOW</td>
</tr>
<tr>
<td>TELECOMMUNICATIONS, ALARM OR SIGNAL LINES, CABLES OR CONDUIT</td>
<td>ORANGE</td>
</tr>
<tr>
<td>TEMPORARY SURVEY MARKINGS</td>
<td>PINK</td>
</tr>
<tr>
<td>SEWER AND STORM DRAINS</td>
<td>GREEN</td>
</tr>
<tr>
<td>CHILLED WATER, RECLAIMED WATER, IRRIGATION AND SLURRY LINES</td>
<td>PURPLE</td>
</tr>
<tr>
<td>OTHER</td>
<td>LIGHT BLUE</td>
</tr>
</tbody>
</table>
net.tagger app

- Crowdsource physical infrastructure discovery
- Users “tag” infrastructure using a free, easy-to-use mobile app
- Future: Win points for tagging, verifying
net.tagger app

• Aggregation and analysis on backend
• Postgres DB, based on Open StreetMaps schema
Quality of tags, mislabels

• Users may mislabel meta-data:
  • Wrong provider, wrong type

• Or even not infrastructure:
  • Mistake sewer for a telecom manhole
  • Mistake red dig markings for telecom
  • Mistake electrical vault for telecom

• Some tags are much more useful than others:

No provider, no type, unclear direction
Inferential Power

• Inferring likely points of infrastructure
  • “Connecting the dots”
  • Include physical constraints, e.g., transportation infrastructure, mountains, right-of-ways

• Data collected thus far suggests that there are lots of possible inferences

• Some case-studies:
Example: Inferring Path
Example: Inferring Path

Aggregation of tags + constraints can provide indication of likely fiber path
Example: Dig Warnings + Road

All 4 registered to same provider
Example: Duct + Features
Example: Access Points + Structure

- Dead-End Street
- “T15/20k”
- “Fiber Optic”

Cell Tower
Example: Shared Infrastructure

Markers suggest shared infrastructure

Large density of infrastructure
Example: St. Croix

- Minimal labeling
- No dig-marking program
- Most infrastructure above ground
Example: State of infrastructure

Southside Rd, St. Croix, USVI

Butler Bay, St. Croix, USVI
Preliminary deployments

- Available to anyone to beta-test
- In use as part of USVI disaster-recovery effort
- Actively bug-squashing and refining UI based on feedback from current users
- Significant maintenance to just keep pace with Android/IOS version and API changes
Open Questions:

• Capturing above-ground installations
• Integrating with OpenStreet Maps
• Correlation with pre-existing topology databases
  • Also helpful to seed tagging
• Incenting users
  • Bounties?
  • Leaderboards?
  • Point system?
• Sharing data
• Automated vision recognition
Security Impact

• “We don’t want attackers to know where is critical infrastructure /weak points!!”
  • This is security through obscurity argument (and, attackers already know)

• Politico, Jun 1, 2017:

In the throes of the 2016 campaign, the FBI found itself with an escalating problem: Russian diplomats, whose travel was supposed to be tracked by the State Department, were going missing.

The diplomats, widely assumed to be intelligence operatives, would eventually turn up in odd places, often in middle-of-nowhere USA. One was found on a beach, nowhere near where he was supposed to be. In one particularly bizarre case, relayed by a U.S. intelligence official, another turned up wandering around in the middle of the desert. Interestingly, both seemed to be lingering where underground fiber-optic cables tend to run.

According to another U.S. intelligence official, “They find these guys driving around in circles in Kansas. It’s a pretty aggressive effort.”
Summary

• net.tagger app for crowdsourced physical infrastructure discovery
• Complementary to existing techniques
• Initial analysis demonstrates possible powerful inferences
• Looking for your participation and feedback!

https://cmand.org/tagger/