Leveraging the Science and Technology of Internet Mapping for Homeland Security

Young Hyun, Ken Keys, Amogh Dhamdhere, Bradley Huffaker, Josh Polterock, Marina Fomenkov, Dima Krioukov, and kc claffy

CAIDA/UCSD
DHS S&T
N66001-08-C-2029
March 2012

http://www.caida.org/
Addressing (Inter)national Security Needs

Objective: to improve DHS’ situational awareness and understanding of the structure, dynamics and vulnerabilities of the physical and logical topologies of the global Internet.

Solution: to develop and implement new measurement and data collection technologies and infrastructure.

- *Macroscopic insight into the global Internet infrastructure…*
Technical Approach

- Integrated 6 strategic measurement and analysis capabilities:
  1. New architecture for continuous topology measurements (Archipelago, or “Ark”)
  2. Topology analysis techniques, e.g. IP alias resolution
  3. Dual router- and AS-level graphs
  4. AS taxonomy and relationships
  5. Geolocation of IP resources
  6. Graph visualization

http://www.caida.org/funding/cybersecurity/
Benefits to DHS S&T

- Improve critical national capabilities:
  - situational awareness for homeland cyber security purposes
  - Internet measurement, analysis, and inference techniques
  - topology mapping: annotated AS+router graphs
  - geolocation technology assessment

- Address network science crisis:
  - flexibility in measurement methods
  - spend less time on non-research activities
  - rapid prototyping, high-level programming model

- Empirical basis for federal communications policy
Archipelago (Ark)

- Launched 12 Sept 2007 w/ 8 monitors
- 59 active IPv4 probers (March 2012)
  - 17 in US
- 28 active IPv6 probers
- Support for meta-data management
- Collaborators run vetted measurements on security-hardened platform
- Publish statistics and analysis of views from individual monitors

http://www.caida.org/projects/ark/
Ark Infrastructure

• **Archipelago** provides:
  • a powerful, globally distributed measurement infrastructure connected via the Internet to a central server at CAIDA
  • resource coordination using the Marinda tuple space
  • scalable system management
  • versatile and efficient measurement methods
  • flexible scheduling, data transfer, indexing, and archival

An environment for easy development and rapid prototyping of experiments.
Topology Data Architecture

existing workflow

AS relationships

BGP AS links

AS links

router topology

IPv4 topology

IPv6 topology

IPv4 DNS names

IPv6 DNS names

AS-router dual graph

AS graph with routers resolved inside ASes

work in progress

http://www.caida.org/
Archipelago Monitor Statistics

- Per-monitor analysis of IPv4 topology data

- Statistics aggregated across all monitors
  - AS path length distributions
  - Integrated RTTs

- Statistics from each monitor
  - Median RTT per country and US state (geographic map)
  - AS hop dispersion graphs (by AS hop and IP hop)
  - IP hop dispersion graphs
  - Distribution of path lengths (IP and AS)
  - RTT distribution (CCDF and quartiles vs hop distance)
  - RTT vs geographic distance
AS Dispersion by AS Hop

Monitor: Kantonsschule Zug (zrh2-ch)

http://www.caida.org/
AS Dispersion by IP Hop

Monitor: Kantonsschule Zug (zrh2-ch)

http://www.caida.org/
AS Dispersion by IP Hop: shows load balancing

Monitor: University of Washington (sea-us)

http://www.caida.org/
Median RTT to Destination Countries

- RTT plotted by country
  - Geolocate destinations with Netacuity (MaxMind Lite for public release)
  - Color each country by median RTT destinations

Monitor: University of Melbourne (mel-au)

http://www.caida.org/
Median RTT to Destination Countries

Monitor: Northeastern University (she-cn)

Monitor: AMS-IX Amsterdam, NL (ams2-nl)

http://www.caida.org/
Median RTT to Destination Countries

Sept 2010. Prior to new fiber down the west coast of Africa.


Monitor: CNRST Casablanca, Morocco (cmn-ma)

http://www.caida.org/
Chinese monitor (top): shows IP load balancing over many hops; Irish monitor (bottom): shows fewer IP hops to other ASes.
Ark Topology Measurement

- Ark continuously gathers the largest set of IPv4 and IPv6 topology data made available to academic researchers and government agencies.

- From Sep 2007 through Feb 2012, we have collected more than 15.6 Billion traces (6.2 TB uncompressed, 1.9 TB compressed).
Topology Measurements over Time

http://www.caida.org/
Topology Datasets

1. **IPv4 Routed /24**: topology probes to each /24, continuously
2. **IPv4 Routed /24 DNS Names**: DNS annotations, also capture raw DNS query/response traffic
3. **IPv6 Topology**: topology probes to each routed IPv6 prefix
4. **Internet Topology Data Kit (ITDK)**: curated IPv4 data
5. **IPv4 Routed /24 AS Links**: AS adjacencies
6. **AS Relationships**: inferred AS business relationships
7. **AS Rank**: inferred AS ranking

http://www.caida.org/data/
IPv4 Routed /24 Topology

- ongoing large-scale topology measurements
- ICMP Paris traceroute to every routed /24 (9.7 million)
  - 57.9% of total IPv4 space (per Feb 2012 Route Views)
  - 7% increase since August 2010
  - probing rate = 100 probes per second
- running scamper probing tool
- dynamically assign measurements to teams of monitors
  - 3 teams active, 18-21 members/team
  - a cycle through every routed /24 takes 2-3 days
  - each /24 is probed once per cycle

http://www.caida.org/
**IPv6 Topology**

- ongoing large-scale topology measurements
- Ark monitors continuously probe BGP-announced prefixes /48 or shorter
  - 7,371 prefixes as of February 2012
- Each monitor probes a single random destination in each prefix using *scamper*

http://www.caida.org/
Internet Topology Data Kit Process

ITDK: Internet Topology Data Kit Process

The Cooperative Association for Internet Data Analysis

http://www.caida.org/
Internet Topology Data Kit (ITDK)

- Derived from two weeks of traceroute data probing IPv4 addresses
- Two router-level topologies
  1) Optimized for accuracy: MIDAR+iffinder
     highest confidence aliases with low false positives.
  2) Optimized for completeness: MIDAR+iffinder+kapar
     more alias coverage, more false positives (inflating routers)
- Data files: routers, links, router-to-AS mappings, geographic location of each router, DNS lookups of observed IP addresses.
Internet-scale Alias Resolution

- Goal: collapse observed interfaces into routers
- Earlier efforts at CAIDA: *iffinder, kapar* (APAR++)
- Most recent approach: *MIDAR* (inspired by RadarGun)
  - Two interfaces on same router respond in similar way
  - IP ID values in responses used as fingerprints to find aliases
    - IP ID is a 16-bit value in the IP header normally used for packet fragmentation and reassembly
    - Two interfaces on same router probed closely in time will return similar IP ID values: over time, similar time-series velocity.
- Architecture paper under peer review for TON 2012

http://www.caida.org/
Alias Resolution Misconceptions

// Unfortunately, faithfully mapping interface IP addresses to routers is a
difficult open problem known as the IP alias resolution problem [51, 28],
and despite continued research efforts (e.g., [48, 9]), it has remained a
source of significant errors. While the generic problem is illustrated in
Figure 2, its impact on inferring the (known) router-level topology of an
actual network (i.e., Abilene/Internet2) is highlighted in Figure 3 -- the
inability to solve the alias resolution problem renders in this case the
inferred topology irrelevant and produces statistics (e.g., node degree
distribution) that have little in common with their actual counterparts...In
view of these key limitations of traceroute, it should be obvious that
starting with the Pansiot and Grad data set, traceroute-based
measurements cannot be taken at face value and are of no or little use for
inferring the Internet's router-level topology. //

"Mathematics and the Internet: A Source of Enormous Confusion and
MIDAR Approach

- Monotonic ID-based Alias Resolution (MIDAR) is our extension of the RadarGun approach:
  - Monotonic Bounds Test: for two addresses to be aliases, their combined IP ID time series must be monotonic
  - Sliding window for scalable probing
  - 4 probing methods: TCP, UDP, ICMP, “indirect” (TTL expired)
  - Multiple monitors
MIDAR Elimination Stage

- Potential alias set found in Discovery stage
- Testing pair-wise not scalable, necessary, or always possible.
- Instead probe subsets [colors in graph], such that most addresses belong to only 1 subset
- Probe a subset in parallel
- Efficiently covers all pairs
- Reduces chance of rate limiting

Examples of bridges

http://www.caida.org/
# MIDAR Results

<table>
<thead>
<tr>
<th></th>
<th>2010-01</th>
<th>2010-04</th>
<th>2010-07</th>
<th>2011-04</th>
<th>2011-10</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input address</strong></td>
<td>1.12 M</td>
<td>1.50 M</td>
<td>1.90 M</td>
<td>2.32 M</td>
<td>2.19 M</td>
</tr>
<tr>
<td><strong>Monotonic address</strong></td>
<td>0.99 M</td>
<td>1.20 M</td>
<td>1.44 M</td>
<td>1.87 M</td>
<td>1.83 M</td>
</tr>
<tr>
<td><strong>Possible pairs</strong></td>
<td>486 G</td>
<td>724 G</td>
<td>1038 G</td>
<td>1754 G</td>
<td>1676 G</td>
</tr>
<tr>
<td><strong>Shared pairs after</strong></td>
<td>1.63 M</td>
<td>4.00 M</td>
<td>5.49 M</td>
<td>6.83 M</td>
<td>7.00 M</td>
</tr>
<tr>
<td><strong>Discovery stage</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Final Results</strong></td>
<td>0.433 M</td>
<td>1.36 M</td>
<td>1.67 M</td>
<td>2.49 M</td>
<td>2.68 M</td>
</tr>
<tr>
<td>• Shared pairs</td>
<td>69 k</td>
<td>108 k</td>
<td>121 k</td>
<td>125 k</td>
<td>118 k</td>
</tr>
<tr>
<td>• Routers</td>
<td>189 k</td>
<td>383 k</td>
<td>426 k</td>
<td>413 k</td>
<td>403 k</td>
</tr>
<tr>
<td>• Addresses on routers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- We have continually improved MIDAR over time:
  - increasing input size of the graph; and
  - improving accuracy and effectiveness of methods.

http://www.caida.org/
AS Rank

- based on inferred economics of AS business relationships
- uses data from global routing tables
- orders by “customer cone”: number of IP prefixes advertised by each AS, by its customer ASes, by their customer ASes, and so on

http://as-rank.caida.org/
AS Rank: screen shot

http://www.caida.org/
AS Rank (cont)

- Tabular views of inferred ISP info, rank, degree, customer cone size, customers, peers, and providers.
AS Rank Validation

- Interface to provide corrections to relationships

<table>
<thead>
<tr>
<th>rank</th>
<th>neighbor AS</th>
<th>neighbor name</th>
<th>type</th>
<th>correction</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>3549</td>
<td>Global Crossing Ltd.</td>
<td>↔ peer</td>
<td>provider</td>
</tr>
<tr>
<td>4</td>
<td>6461</td>
<td>Metromedia Fiber Net</td>
<td>↑ provider</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>3257</td>
<td>Tinet SpA</td>
<td>↑ provider</td>
<td>peer</td>
</tr>
<tr>
<td>6</td>
<td>1239</td>
<td>Sprint</td>
<td>↔ peer</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>2914</td>
<td>NTT America, Inc.</td>
<td>↔ peer</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>174</td>
<td>Cogent/PSI</td>
<td>↔ peer</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>7018</td>
<td>AT&amp;T Services, Inc.</td>
<td>↔ peer</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>3320</td>
<td>Deutsche Telekom AG</td>
<td>↔ peer</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>6453</td>
<td>TATA Communications</td>
<td>↔ peer</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>701</td>
<td>MCI Communications S</td>
<td>↔ peer</td>
<td></td>
</tr>
</tbody>
</table>

Disclaimer: We show these corrections as examples of the interface not as actual corrections received by TeliaNet Global Network.
Geolocation Tools Comparison

- Service evaluation criteria
  - What geographic granularity does it provide?
    - Continent, country, state/prefecture, city, zip code
  - What Internet identifier granularity does it support?
    - IP address, network prefix, Autonomous System (AS)
  - Does accuracy vary by region or type of network?

- We evaluated: Digital Envoy's Netacuity, MaxMind (Free and commercial), IP2Location, Ipligence, and HostIP.info. Quova and Akamai remain unwilling to participate.

- Results generally agreed on IP-address-to-country mappings
  - MaxMind Lite and GeoIP had the highest level of agreement (99.1%)
  - IPligence had the lowest level (94.3%)
  - Finer granularity harder to evaluate
  - Netacuity and MaxMind GeoIP performed “best” in our testing
Integrated Visualization of Topological Connectivity

- AS-level graph

http://www.caida.org/
Integrated Visualization of Topological Connectivity

- Router-level graph (prototype)
Internet Topology Data Comparison

• Topology maps needed to analyze or model Internet structure
  • many studies use single, inconsistent, incomplete, or undocumented sources which can undermine integrity of analysis results
  • objective: enabling informed selection of topology datasets

• Approach: systematic comparison of best available data sources
  • characterizing the Internet topology at three granularities: IP address (interface), router, Autonomous System (AS)
  • most comprehensive study: sources, metrics, methods, results

URL: http://www.caida.org/research/topology/topo_comparison/

http://www.caida.org/
Published Experiments Using Ark

1) “Traceroute Probe Method and Forward IP Path Inference”, IMC'08.
2) “Understanding the efficacy of deployed internet source address validation filtering”, IMC'09.

http://www.caida.org/
## Published Experiments Using Ark

<table>
<thead>
<tr>
<th></th>
<th>Title</th>
<th>Details</th>
</tr>
</thead>
</table>

- **Another 107 articles in Google scholar cite or use data from Ark as of 02 sept 2011.**

http://www.caida.org/
Scheduled, Planned Activities

- Deploy 1-2 monitors/month to measure IPv4 and IPv6 topology
- Continue to release and refine ITDK
- Publish alias resolution study and release three versions of code
- Annotated router-level graph visualization and database support
- Topology on demand measurements
- AIMS 2012 Workshop report -> CCR
- Explore coupling of data plane and (DHS-funded BGPmon) control plane data
- AS Rank documentation, validation and improved algorithms and interface
- Develop a web-based interface to topo-on-demand service

http://www.caida.org/
### BAA Number: Cyber Security BAA 07-09
### Title: Science and Technology of Internet Topology Mapping

#### Walrus visualizations of round-trip time measurements made by CAIDA’s macroscopic Internet topology monitor located in Herndon, VA, USA.

#### Internet Topology Mapping:
1. Operational infrastructure to support continuous Internet topology mapping.
2. Periodic active probing of 100% of BGP prefixes announced in publicly available routing tables.
3. ISP relationship inference with accuracy up to 98%.
4. Topologies at the router and AS granularity annotated with AS relationships, AS types, geolocations, latencies, etc.
5. Empirically grounded quantified understanding of robustness, reliability, scalability and other characteristics of the Internet topology as critical infrastructure.
6. Improved annotated topology maps will enhance modeling and monitoring capabilities to help identify threats and predict cascading impacts of damage scenarios.
7. Visualization capabilities will provide powerful interface for use by DHS and other national security personnel.

#### Technical Approach:
1. Expand current deployment of new distributed platform for continuous measurement of Internet topology, performance, state, and other characteristics.
2. Use and improve IP alias resolution techniques to identify common routers to which IP interfaces belong.
3. Further test and improve performance of software to convert IP technology data into router-level and AS-level graphs.
4. Utilize CAIDA’s AS relationship and AS taxonomy inference techniques and data infrastructure to annotate AS graphs with AS types and relationships.
5. Apply and evaluate publicly available geolocation tools for use in annotating topologies with geographic data.
6. Use CAIDA’s or other visualization capabilities to depict structure and vulnerability-related characteristics of observed annotated Internet topologies.

#### Schedule, Deliverables, Contact Info:
1. Current: new active measurement architecture: design complete; prototype implementation being tested.
2. Year 1:
   a. establish on-going IPv4 topology measurements using the new infrastructure;
   b. release software for calculation and exhaustive analysis of topology characteristics.
3. Year 2:
   a. weekly updates of router topology with IP aliases resolved using best available techniques;
   b. weekly updates of AS/router graphs annotated with inferred AS relationships and types.
4. Year 3:
   a. topology annotated with latencies and geolocations;
   b. annotated AS/router topology visualizations.
5. POC: Jennifer Ford, UCSD Contracts&Grants, 9500 Gilman Dr. MC 0934, La Jolla, CA 92093-0934  Fax: (858) 534-0280