Cyber Security Research and Development

TTA 5 – Internet Tomography and Topography

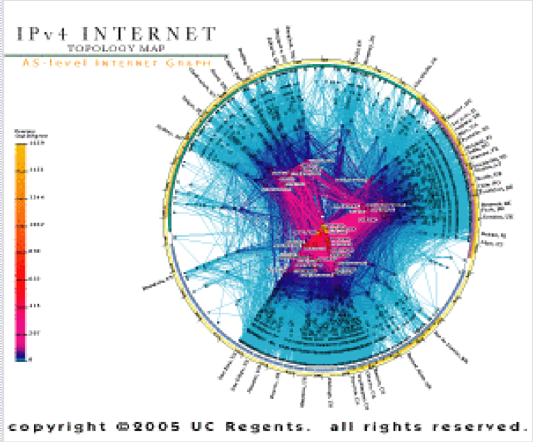
May 2007

Rick Lichtenfels
National Communications System

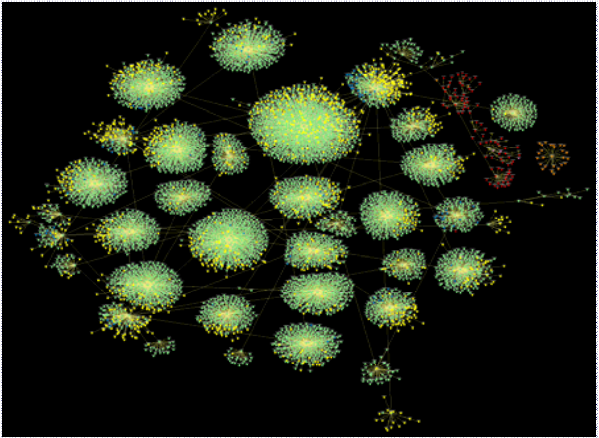
Homeland
Security

Overview of Internet tomography and topography analysis

Network tomography analysis consists of inferring unobserved characteristics of the Internet based on what can be measured and observed without requiring the full cooperation of the network



[1]



Network topography analysis utilizes active discovery and targeted data collection to provide a detailed representation of a specific network

[1] *Image Source: CAIDA*

The NCS has leveraged network tomography and topography analysis to achieve several objectives

Router-level network mapping

- Identification of critical assets, facilities, and links supporting end users or systems of high interest
- Discovery of upstream providers and routers through BGP data analysis and proprietary tools
- Geolocation of backbone and access routers through traceroute analysis

Autonomous System (AS)-level network mapping

- Identification of Internet Service Provider (ISP) interconnectivity
- Discovery of regional Internet architecture and deployed infrastructure

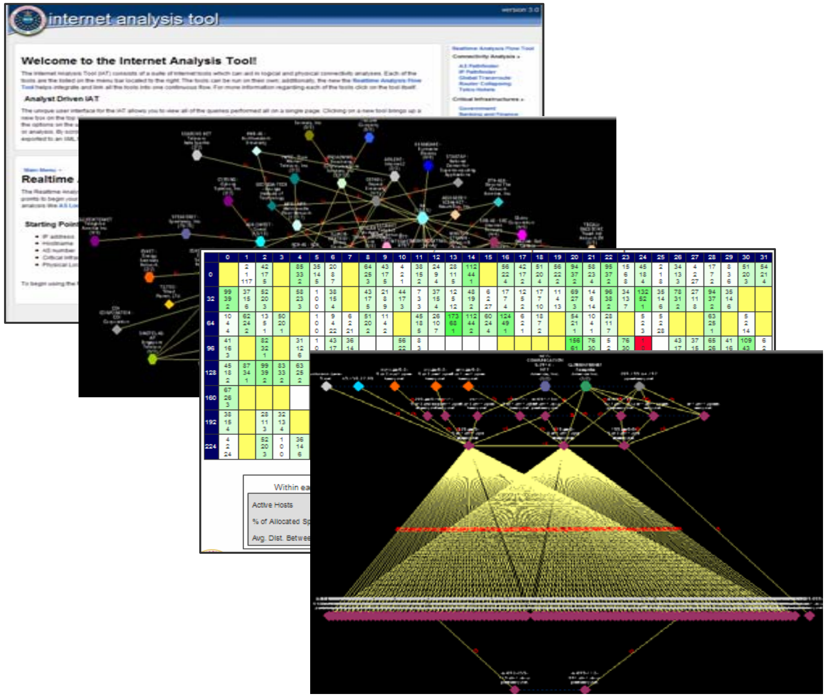
Network transformation

- Trending Internet routing changes over time as a result of physical or logical events through BGP and traceroute data analysis
- Predicted restoration of backbone and access network service after catastrophic events

Homeland Security

Various tools and data sets may be utilized to conduct tomography and topography analysis

- The NCS-developed Internet Analysis Tool (IAT) incorporates Regional Internet Registry data as well as multiple BGP feeds and globally distributed traceroute measurement tools
- CAIDA’s Skitter project provides visualizations and metrics describing global network connectivity
- Targeted traceroutes and data mining yield regional backbone service providers and access networks within specific geographic regions
- Proprietary tools are used to audit IP address space utilization and identify routing anomalies within a private network through network scans and nodal analysis
- Targeted traceroutes and open source research provide carrier-specific connectivity data



The NCS currently faces several challenges in improving its tomographic analysis capabilities

In conducting network tomography and topography analyses, disparate tools and datasets presenting different and complementary views typically need to be reconciled with each other

- **Tool and data integration** – Currently, tools and data acquired from different sources must be integrated manually by analysts, resulting in increased analysis response times.
  - It is difficult to associate real-time BGP feed data with larger (and more static) RIR data sets
  - Physical or geographic data is often required to provide actionable direction; without carrier cooperation, logical assets can be difficult to physically locate with a high degree of certainty

Additionally, certain tools or data sets needed for analysis may not currently exist, and may require the NCS to develop tools and methodologies to create them

- **Bulk data processing** – Analysis of large data sets, such as the regional Internet registries or IP aliasing on large sets, may be computationally intensive. Additional analysis would help to identify methodologies and tools which could be used to conduct analyses more quickly

The NCS has identified several immediate areas for improvement in tomographic and topographic analysis

Several tomography and topography analysis focus areas warrant further research and development, including—

- Extracting peering relationships from AS paths within BGP tables and from IP-IP links within massive numbers of traceroutes;
- Developing the capability to quickly and accurately map IP addresses, hosts, routers, etc. to physical locations;
- Increasing the accuracy of currently available tools or methodologies for matching IP addresses to router interfaces; and
- Efficiently building logically connected maps (e.g., router-level or AS-level) of Internet devices through traceroute and BGP data;

Homeland Security