LTS Efforts in Network Mapping

Dr. B. Ann Cox

Beverly.a.cox@ugov.gov

Laboratory for Telecommunications Sciences

College Park, MD

- The Laboratory for Telecommunications Sciences is a federal research lab located at the University of Maryland campus in College Park, MD. Our network-oriented research focuses on both wired and wireless, core and periphery.

- One of LTS's primary goals is to promote research collaboration between government, industry, and academia. To that end we have developed primary research partnerships with the University of Maryland Institute for Advanced Computer Studies and Telcordia Technologies.

LTS LABORATORY FOR TELECOMMUNICATIONS SCIENCES

LTS and Network Mapping

- Infrastructure Protection: Mapping our own networks to ensure only authorized users have access
- Attribution: In the event of an unauthorized user attempting to connect to our network, or in the case of a network attack, we want to know where it came from

What have we done?

- Network Mapping and Measurement Conference, 2008
- Support to Academic Researchers
- Contracted Research by Commercial Companies
- Not the sole supporter of any effort

NMMC 2008

- July 14-15, 2008 held at LTS building, College Park MD
  - » ~ 90 participants from government, industry, academia
  - » Speakers represented 7 different universities
  - » 15 different offices or agencies in the intelligence community
  - » 7 companies represented
  - » Attendees from three different countries
  - » Presentations by two large companies involved in network mapping

NMMC 2009

- June 8-9, 2009
- LTS building, College Park MD
  - »No Conference Fee
  - »Welcome Speakers from a wide range of network mapping topics
  - »Rotate to another site in 2010

IC Postdoctoral Fellowship Program

Competitive Selection Process

Topic Published as part of BAA in Dec 2008

PI proposals received Jan 2009

Now in the evaluation phase

Awards announced in June 2009

Emphasis of topic on passive network mapping of both the logical and physical network structure; no particular network specified so that the research may be applied to many kinds of networks

Cornell University: Octant

- Octant is an IP geolocation framework.
- Can incorporate both positive and negative information
- Initially designed to perform on-demand network measurements to locate a single ip address
- No information saved, all calculations done each time a request is made
- We support a passive approach (as much as possible)
- Enabled a collaboration with another university and a commercial company

University of Maryland, College Park

- Metro Area Geolocation: Existing techniques can geolocate an IP address to a metropolitan area (best available, about 25 km).

  Will the same techniques work within a metro area? If not, what might work?

- Pinpoint Technology: Time-based Localization, accurate to within a few feet.

University of Wisconsin, Madison

- Network Radar : Sending pairs of packets from a single source to two different destinations, measure the RTT and look at correlations.
- Packet tool under development to control number, timing, size, and type of packets used to generate data.

Questions?

Ann Cox

beverly.a.cox@ugov.gov