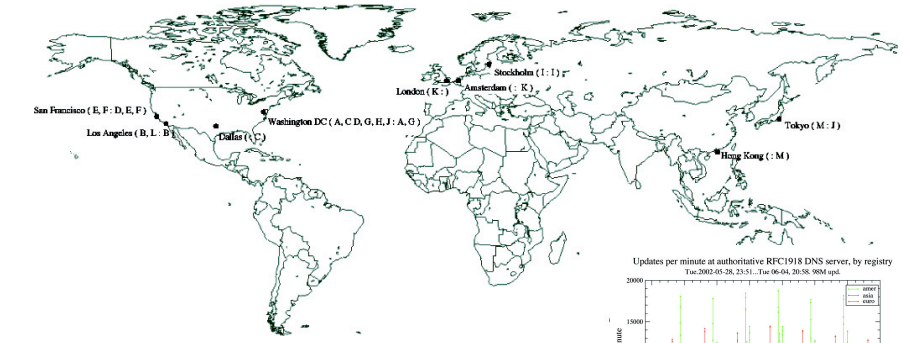
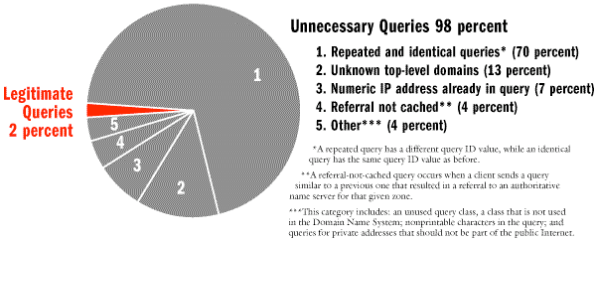
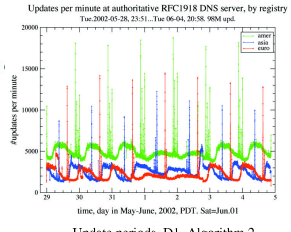
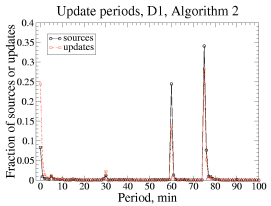
Macroscopic Internet Data Collection and Analysis









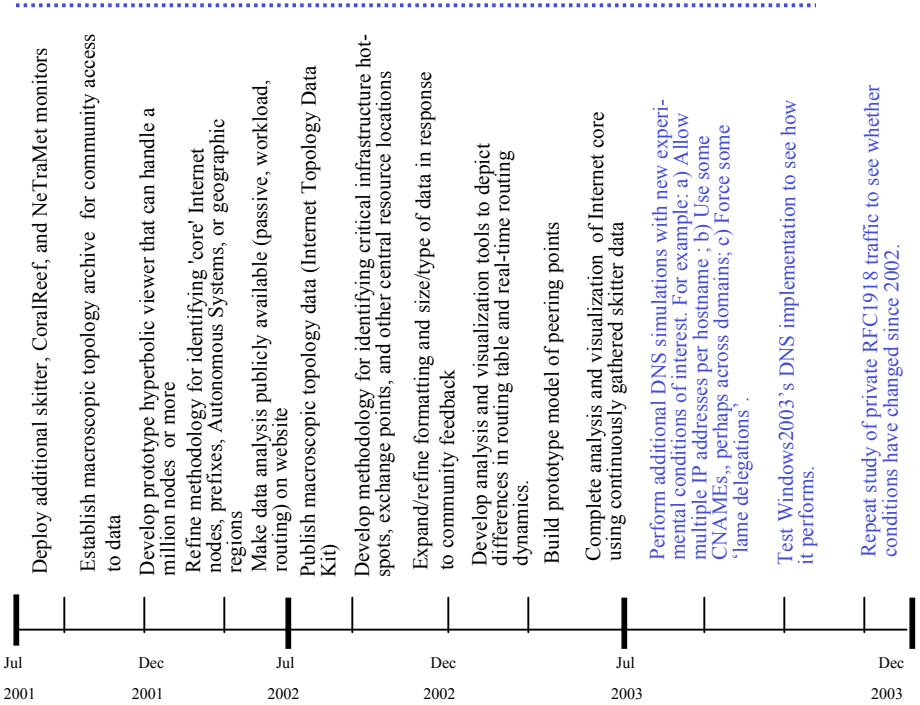
Analysis of DNS root name server queries reveals large amounts of unnecessary and illegitimate traffic.

Impact

- Discovered that only a small portion of queries to a DNS root nameserver were legitimate. Categorized the unnecessary traffic and discovered that much of it is the result of simple misconfigurations of firewalls and poorly chosen defaults for vendor-specific DNS implementations.
- Matched periodicity of undesirable, spurious private (RFC1918) DNS updates to documented behavior of Windows2000 and WindowsXP DNS.
- Analyzed DNS root and gTLD performance during the October 2002 DNS DoS attack.
- Provided real data for the NMS Integrated Demo: Supplied packet level traces to ISI for use in their RAMP tool. Also provided flow summary data to GeorgiaTech to model background traffic not modeled by RAMP.
- Customized CoralReef passive monitoring tools to provide network performance data for potential use by DoD in the ForceNET Limited Objective Experiment (LOE).

New Ideas

- Devised a methodology for simulating the Domain Name System in order to test different caching DNS nameserver implementations.
- Used binary auto-correlation algorithm to discover periodic behavior within undesirable private RFC1918 DNS updates to the root nameservers.
- Refined Internet routing geopolitical analysis and visualization, especially for exchange (IX) and peering points.
- Enhanced automated analysis of DNS root, gTLD, and ccTLD nameserver performance using NeTraMet passive monitors.



caida

Cooperative Association for Internet Data Analysis / UCSD - Dr. K Claffy, PI