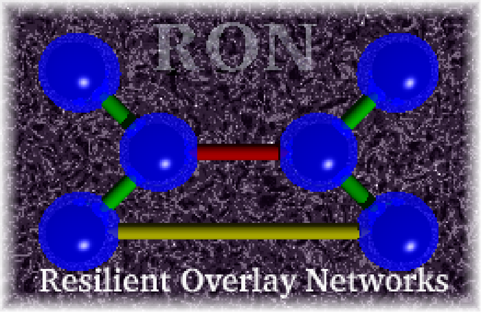

Resilient Overlay Networks

Today's Internet backbone is effectively non-transitive. You may be able to visit MIT, and MIT may be able to visit a site in which you're interested, but that's no guarantee that you can visit that site.

Relaxing that a bit farther, there is considerable evidence that for technical and political reasons, routing on the internet frequently ignores paths which may be better able to carry traffic. From a security perspective, an attacker's job is made easier because restricted routing creates more single points of failure which an end-user is unable to simply "route around."

The resilient overlay networks project is designing a framework which can be used by either applications or network routers to take advantage of these traffic shunts to improve performance. RON nodes will self-configure an overlay network to transmit packets over the underlying Internet infrastructure which will automatically select paths to avoid network problems. Because of their relatively small size (under 50 nodes), RONs will be able to take advantage of more aggressive path selection and detection methods than conventional internet routers. Because RONs are administered in a single domain, they can incorporate additional security features (like a secure VPN), and they can base their path selection upon their own requirements, not a global approximation such as shortest path.

Components of the project:

- End-to-end low-impact active performance measurement
- Routing and topology maintenance (courtesy of INS)
- Integration of performance data in an easily accessible performance database.
- Libraries for easy application use of overlay networks.
- RON router nodes, using Click to provide transparent encapsulation of packets into the overlay network.

Project Members

Faculty

[Hari Balakrishnan] [M. Frans Kaashoek] [Robert Morris]

Graduate Students

[David Andersen] [Kyle Jamieson]

Papers and Presentations

- Slides from a presentation comparing existing link probing mechanisms.
- RON Overview presentation, in [HTML] [Postscript] [Powerpoint] formats.

Related Work

Comments about how specific other pieces of work relate to RONS can be found in related work details.

- The CAIDA Network Measurement Tools Taxonomy, a list of many network probing utilities.
- The X-Bone Project is working to make overlay networks easy to create, primarily with an eye towards creating IP overlay networks for rapid deployment of new protocols like IPv6 (see the 6bone home page) and multicast (over the

"I'm happy to announce the release of v2.0b1 of the SPAND toolkit. SPAND (Shared Passive Network Performance Discovery) is a system that allows applications to measure the application-level network performance to distant network sites, share that information with other clients, and use the information to make intellegent application-level decisions."

A USITS paper by Srini and Mark describes SPAND [ps] [local ps]
Mark Stemm's thesis is available: [html] [ps] [local ps] , and it discusses SPAND in detail.

- The IDMaps Project at the University of Michigan. (The Internet Distance Maps project). Working towards a "server" which can provide pairwise internet distance information.
- The Internet Protocol Performance Metrics page, containing the IETF IPPM project resources.
- The Detour Project at the University of Washington. They developed "sting", which uses TCP to determine forward and reverse path packet loss rates.
- Yallcast is an open-source project to develop software allowing hosts to form a content distribution topology. Their architecture paper is available in [html] [ps] [local ps] formats. They want to position themselves above TCP/IP but below the application. They create a tunnelled shared tree topology and a tunnelled mesh
- Commercial products

  There are several commercial products which use some of the techniques we're exploring. VisualRoute measures per-hop loss and delays. VitalSigns' NetMedic product uses bprobes and application-specific metrics to report network performance.

- A Nanog presentation from UUNET describing their denial of service tracking overlay network.
- Stuff stolen from ISI's xbone refs page that I still need to categorize:
  - MorphNet (Argonne National Lab - ANL)
  - Supranet (CRATOS)
  - Virtual Network Service - VNS (CMU)

David G. Andersen
Last modified: Mon Mar 13 18:26:02 EST 2000