

Spatio-temporal Analysis of Internet Routing: Discovery of Global Routing Instabilities Due to Worm Attacks and Other Events

James H. Cowie
Andy T. Ogielski (Renesys Corporation)
ato.renesys.com

Abstract

Analysis of BGP routing message traffic from many Internet locations provides an accurate spatio-temporal picture of the dynamic state of the global connectivity. BGP (Border Gateway Protocol) is the Internet standard providing a global routing infrastructure.

When a BGP router's best route to a given network address has changed (for better or worse), it sends out route update messages to each neighboring peer router. Therefore, by establishing BGP peering connections with a large number of important BGP routers worldwide, analysis of collected message streams can provide a great deal of information about instantaneous connectivity of the entire Internet, about routing dynamics over a wide range of time scales, and about connectivity failures and "routing storms".

We will present our recent results obtained from real-time multiresolution analysis of live, time-stamped streams of BGP routing messages collected from about 200 routers worldwide, from the multiple monitoring locations of RIPE RIS, RouteViews, and Renesys data collection centers.

We will discuss techniques used to discover the emergence of high-rate, long-lived global routing instabilities, which cause significant, widespread degradation in the end-to-end utility of the global Internet, and we will analyze some of their mechanisms. Case studies of our discovery of unexpectedly large routing instabilities triggered by the spread of Internet worms (Code Red II and Nimda) will illustrate the presentation.

This work leads to new research areas in multiresolution analysis on graphs, statistics of path spaces, and related fields.