ONLINE DETECTION AND ANALYSIS OF INTER-DOMAIN ROUTING INSTABILITIES

By

Shivani Deshpande

An Abstract of a Thesis Submitted to the Graduate

Faculty of Rensselaer Polytechnic Institute

in Partial Fulfillment of the

Requirements for the Degree of

DOCTOR OF PHILOSOPHY

Major Subject: Electrical, Computer and Systems Engineering

The original of the complete thesis is on file
in the Rensselaer Polytechnic Institute Library

Examining Committee:

Prof. Biplab Sikdar, Thesis Adviser
Prof. Shivkumar Kalyanaraman, Member
Prof. Koushik Kar, Member
Prof. Bolek Szymanski, Member
Dr. Marina Thottan, Member

Rensselaer Polytechnic Institute
Troy, New York

February 2007
(For Graduation May 2007)

ABSTRACT

Border Gateway Protocol (BGP) is the default inter domain routing protocol. It has been designed to be scalable, so as to cope with the rapidly growing Internet. However, the policy based nature of BGP causes it to have poor isolation capabilities and any localized instability caused by a failure event may be propagated globally. As a result, the impact of different types of catastrophic events like worm attacks, power outages, accidental cable or link failures, etc. on connectivity in the Internet becomes much more severe and longer lasting. Thus, maintaining the stability of BGP is critical for preserving connectivity, thereby ensuring the delivery of data packets. Our approach to solving this problem is to detect the occurrence of BGP instabilities and to prevent their propagation. The detection algorithm proposed here, performs a statistical analysis of features extracted from BGP update message data to flag the onset of an instability. We perform sequential change detection on the feature time series using a Generalized Likelihood Ratio (GLR) based hypothesis test. In order to make the detection more robust, we also exploit the temporal correlation between changes detected across features and across peers. After the detection, we propose techniques to analyze the update message contents to identify the location of the root cause event. This information can then be used to design BGP policy rules that can help to prevent the instability propagation. Our system is designed to function online and can be deployed easily on any BGP router. We evaluate our system using real BGP data from periods of a number of failure events and SSFNet simulations. We show that it is efficient in detecting instabilities with minimum delay and very low false detection rates.