A Novel Graph Spectra Approach to Anomaly Detection in Border Gateway Protocol

Leigh Metcalf[1], Will Casey[2], Timur Snoke[3], Heeralal Janwa[4], Shirshendu Chatterjee[5], and Ernest Battifarano[6]

[1] Carnegie Mellon University, Pittsburgh PA 15213, USA
lmetcalf@andrew.cmu.edu
[2] US Naval Academy Annapolis, MD, USA
wcasey@usna.edu
[3] Carnegie Mellon University, Pittsburgh PA 15213, USA
emailtsnoke@andrew.cmu.edu
[4] University of Puerto Rico San Juan, USA
heeralal.janwa@upr.edu
[5] City University of New York, Graduate Center and City College New York, NY, USA
shirchat1@gmail.com
[6] Retired at New York, NY, US
ernest.battifarano@gmail.com

Abstract. We carry out an effective clustering of distributed time series graphs. The work uses singular value decomposition (SVD) of spectral gaps of graphs derived from BGP data found at the RouteViews Project at the University of Oregon. We detect extremal events and examine anomalous events that cause disruptions in Internet routing. We use spectral gaps to examine how redundant and sparse the graph is. We base the anomaly detection method in BGP networks on the fact that a drop in the value would signify a lack of this redundancy, which in the distributed redundant Internet would be an anomalous event.

Keywords: BGP, graph, spectral-gap, expanders, time series, time series clustering, spectral clustering, SVD, power-law