Performing BGP Experiments on a Semi-Realistic Internet Environment

Ke Zhang, Soon-Tee Teoh, Shih-Ming Tseng, Chen-Nee Chuah, Kwan-Liu Ma, S. Felix Wu
University of California, Davis
Focus ➔ Evaluation

- BGP Security Evaluation
- BGP Routing Dynamics

- Semi-Realistic BGP experimental Testbed
  - Recreate Routing Dynamics
  - Artificial attacks
  - Analysis, Characterization and Profiling
  - Visualization
Testbed Architecture

1 peer (SPRINT)
Full Routing Table (9MB compressed)
BGP Updates (2 hours -- 168KB)

DeterLab
93 nodes (zebra routers)
5 commercial routers (Cisco 12000, 2600, IBM 2210)

"Get the real BGP data"
What was AS-15412 doing in April 2001?
Anomaly Detection and Interactive Visualization

raw events

function \( F \)

Statistical profile

quantify the anomalies

High threshold

Low threshold

threshold = 0.9  \( k = 3  \)  \( T = 360 \)  \( \alpha = 0.01 \)

threshold = 0.42  \( k = 3 \)  \( T = 300 \)  \( \alpha = 0.01, 0.03 \)

K = 3

K = 5
Two Experiments

- **Origin AS Changes**
  - IP address prefixes/traffic stealing

- **Differential Damping penalty**
  - Remotely deny routing services
Different RFD implementation

SSFNet  Zebra Router  Cisco Router