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

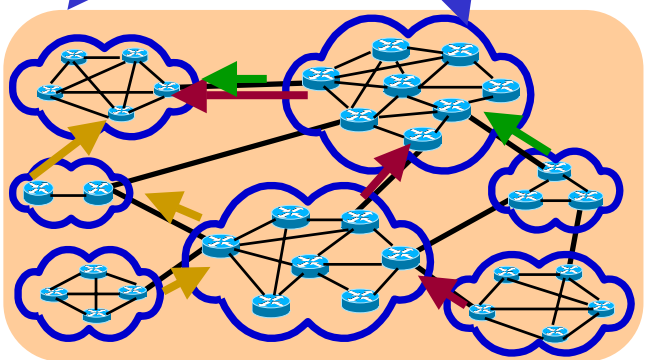
- Semi-Realistic BGP experimental Testbed
  - Recreate Routing Dynamics
  - Artificial attacks
  - Analysis, Characterization and Profiling
  - Visualization

Testbed Architecture

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

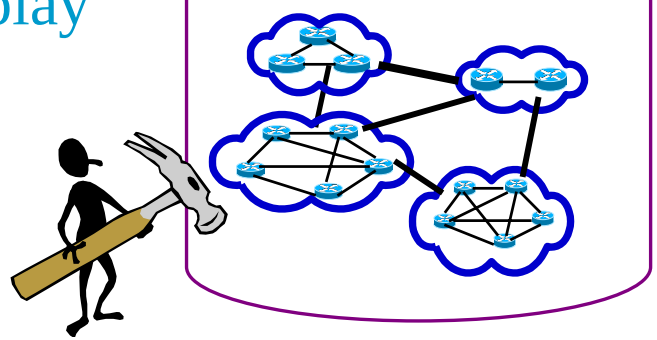
Routeview

...



BGP replay

Testbed

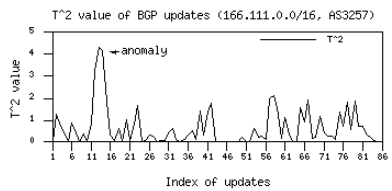


Attack
Experiments

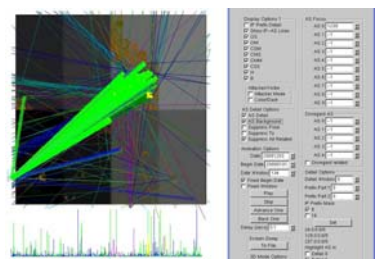
DeterLab

93 nodes (zebra routers)

5 commercial routers (Cisco 12000, 2600, IBM 2210)

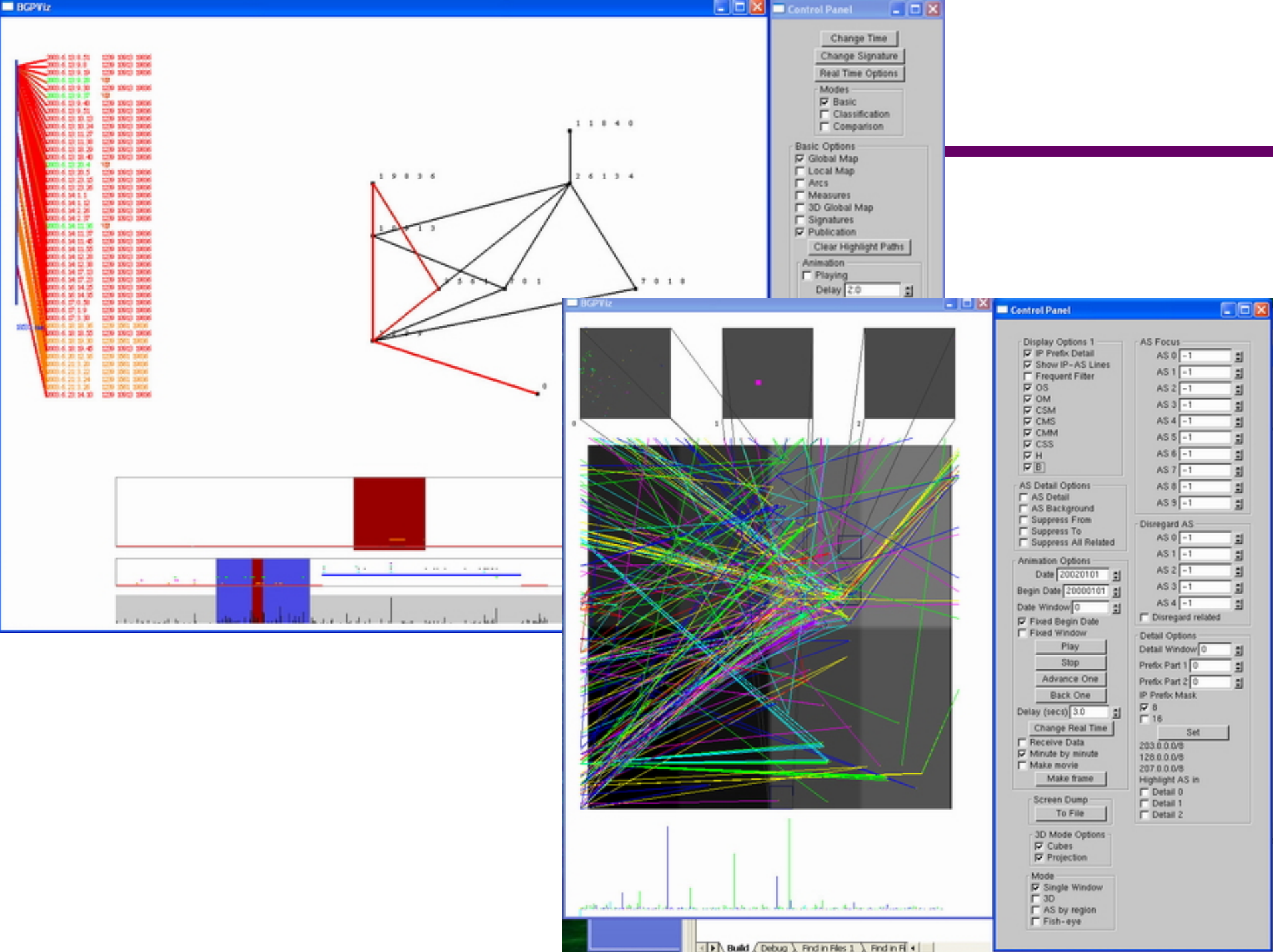


Anomaly Detection

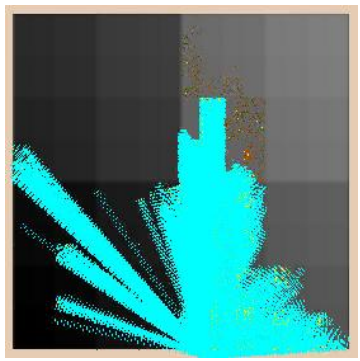


Visualization

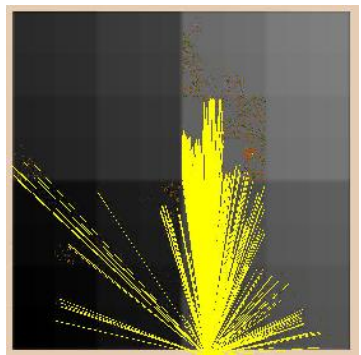
“Get the real BGP data”


BGPViz
Control Panel
Change Time
Change Signature
Real Time Options
Modes
Basic
Classification
Comparison
Basic Options
Global Map
Local Map
Arcs
Measures
3D Global Map
Signatures
Publication
Clear Highlight Paths
Animation
Playing
Delay
2.0
BGPViz
Control Panel
Display Options 1
IP Prefix Detail
Show IP-AS Lines
Frequent Filter
OS
OM
CSM
CMS
CMM
CSS
H
B
AS Detail Options
AS Detail
AS Background
Suppress From
Suppress To
Suppress All Related
Animation Options
Date
20020101
Begin Date
20000101
Date Window
0
Fixed Begin Date
Fixed Window
Play
Stop
Advance One
Back One
Delay (secs)
3.0
Change Real Time
Receive Data
Minute by minute
Make movie
Make frame
Screen Dump
To File
3D Mode Options
Cubes
Projection
Mode
Single Window
3D
AS by region
Fish-eye
AS Focus
AS 0
AS 1
AS 2
AS 3
AS 4
AS 5
AS 6
AS 7
AS 8
AS 9
Disregard AS
Disregard related
Detail Options
Detail Window
Prefix Part 1
Prefix Part 2
IP Prefix Mask
8
16
Set
203.0.0.0/8
128.0.0.0/8
207.0.0.0/8
Highlight AS in
Detail 0
Detail 1
Detail 2
Build
Debug
Find in Files 1

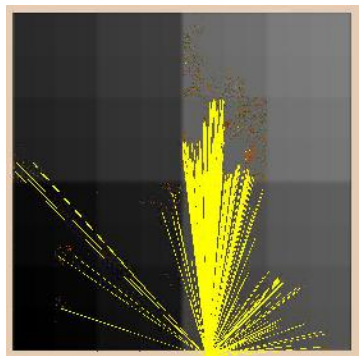
Interactive Visual Correlation



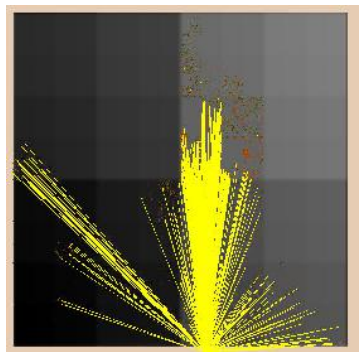
Apr 6



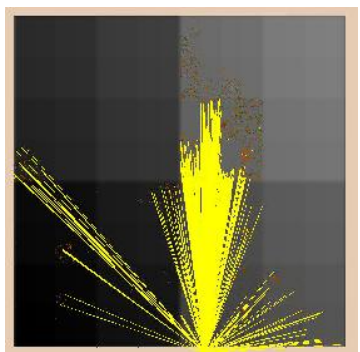
Apr 7



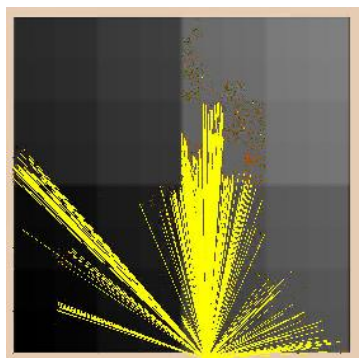
Apr 8



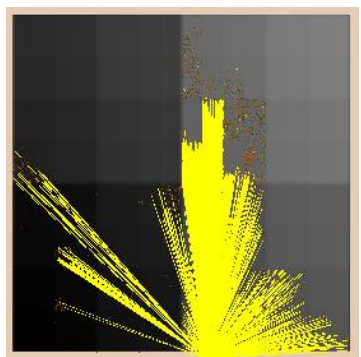
Apr 9



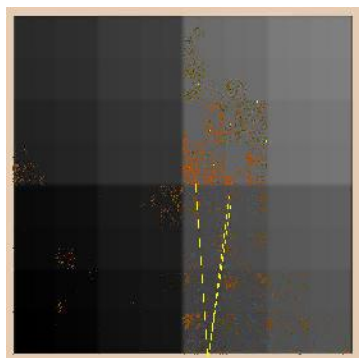
Apr 10



Apr 11



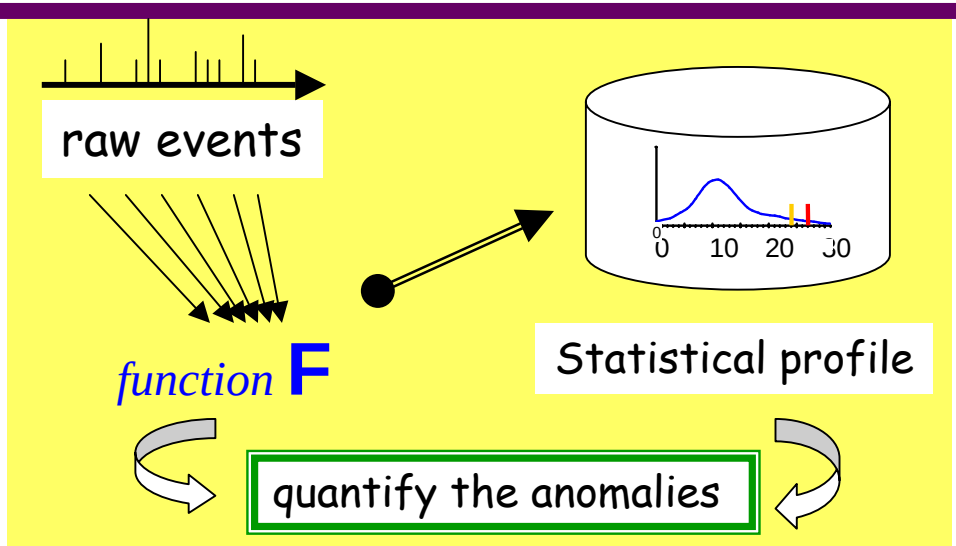
Apr 12



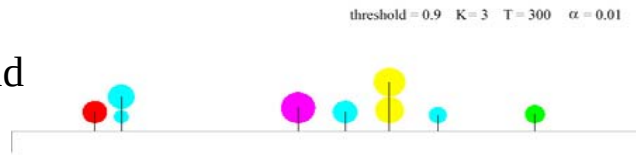
Apr 13

What was AS-15412 doing in April 2001?

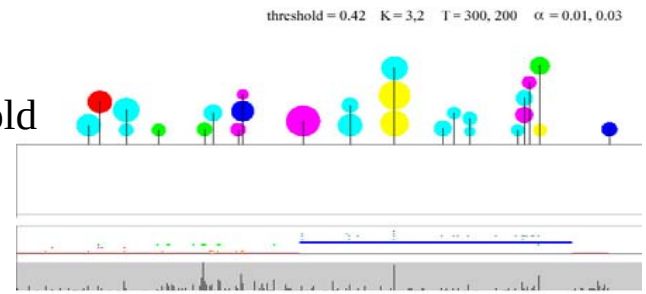
Anomaly Detection and Interactive Visualization

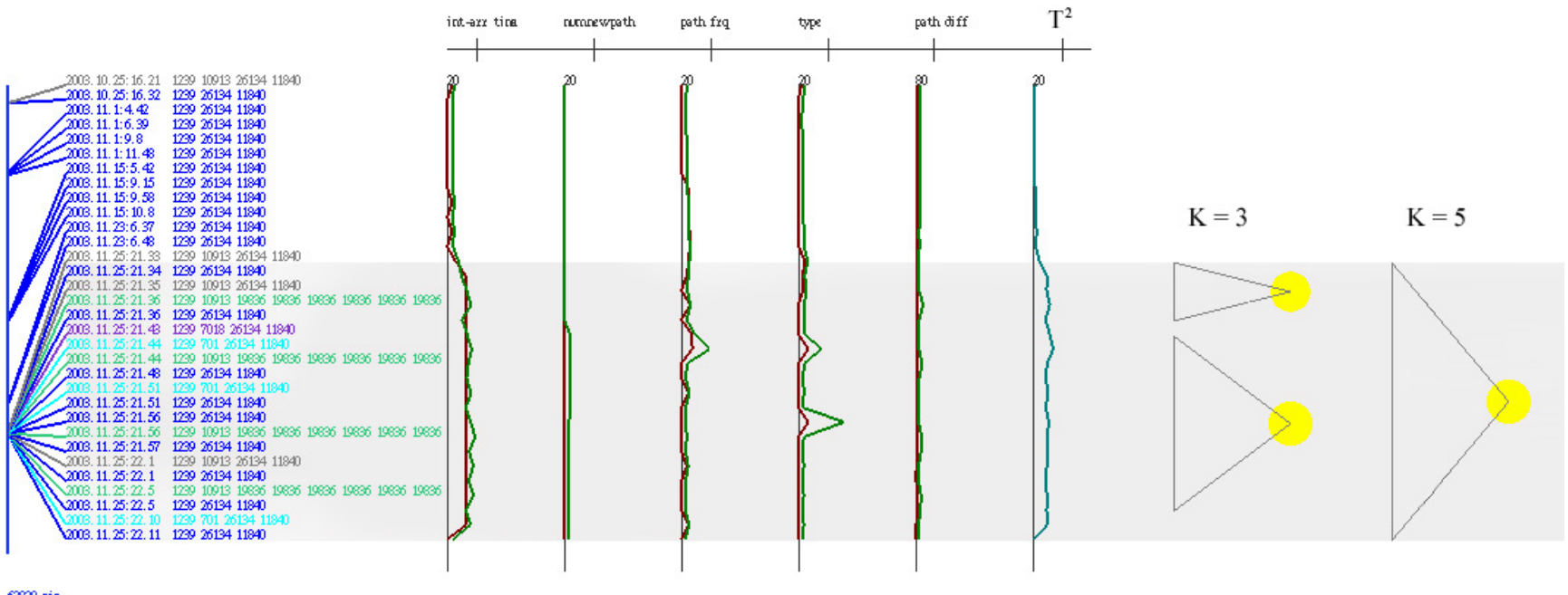


High threshold



Low threshold





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