Cyber DEfense Technology Experimental Research (DETER) Network
Evaluation Methods for Internet Security Technology (EMIST)

USC Information Sciences Institute • University of California, Berkeley • University of California, Davis • Penn State University
Purdue University • International Computer Science Institute • Stanford Research Institute (SRI) • Network Associates • SPARTA

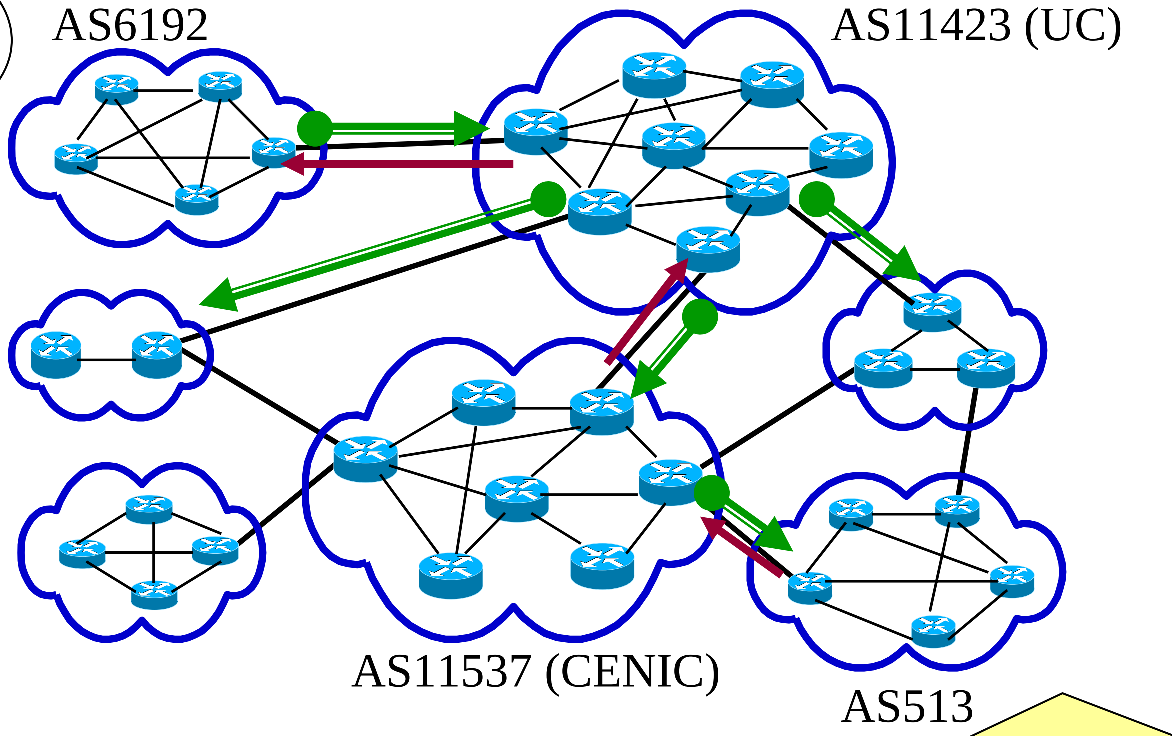
ELISHA: On Detection and Analysis of Anomalous Dynamics

S. Felix Wu
Computer Science Department
University of California, Davis

wu@cs.ucdavis.edu
http://www.cs.ucdavis.edu/~wu/

Autonomous Systems (ASes)

UCDavis:
169.237/16



an AS Path:
169.237/16 **513→11537→11423→ 6192**

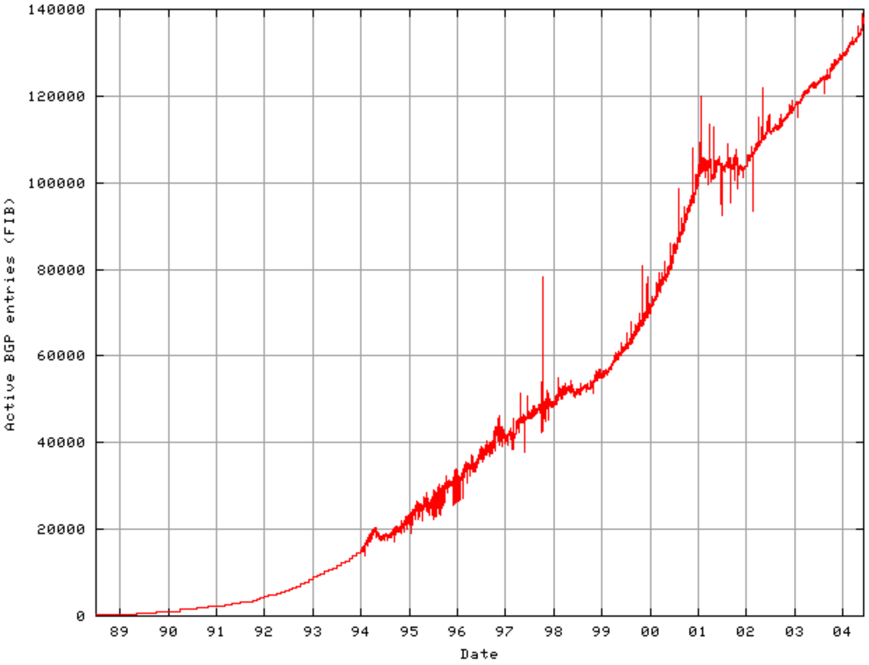
March 2002

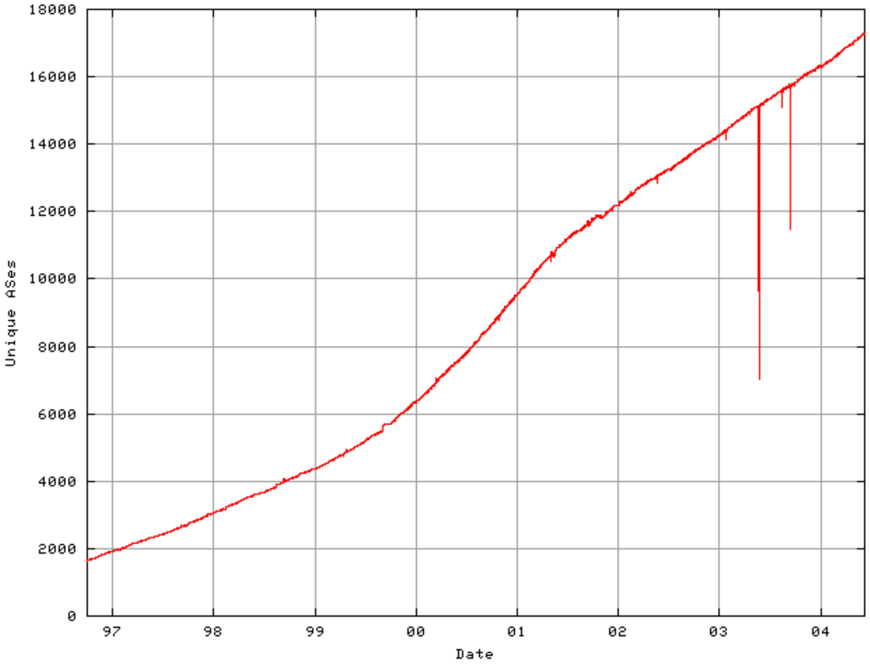
The “Internet“

as June 7, 2004

http://bgp.potaroo.net/cidr/

- 17273 Autonomous Systems
- 136515 IP Address Prefixes announced

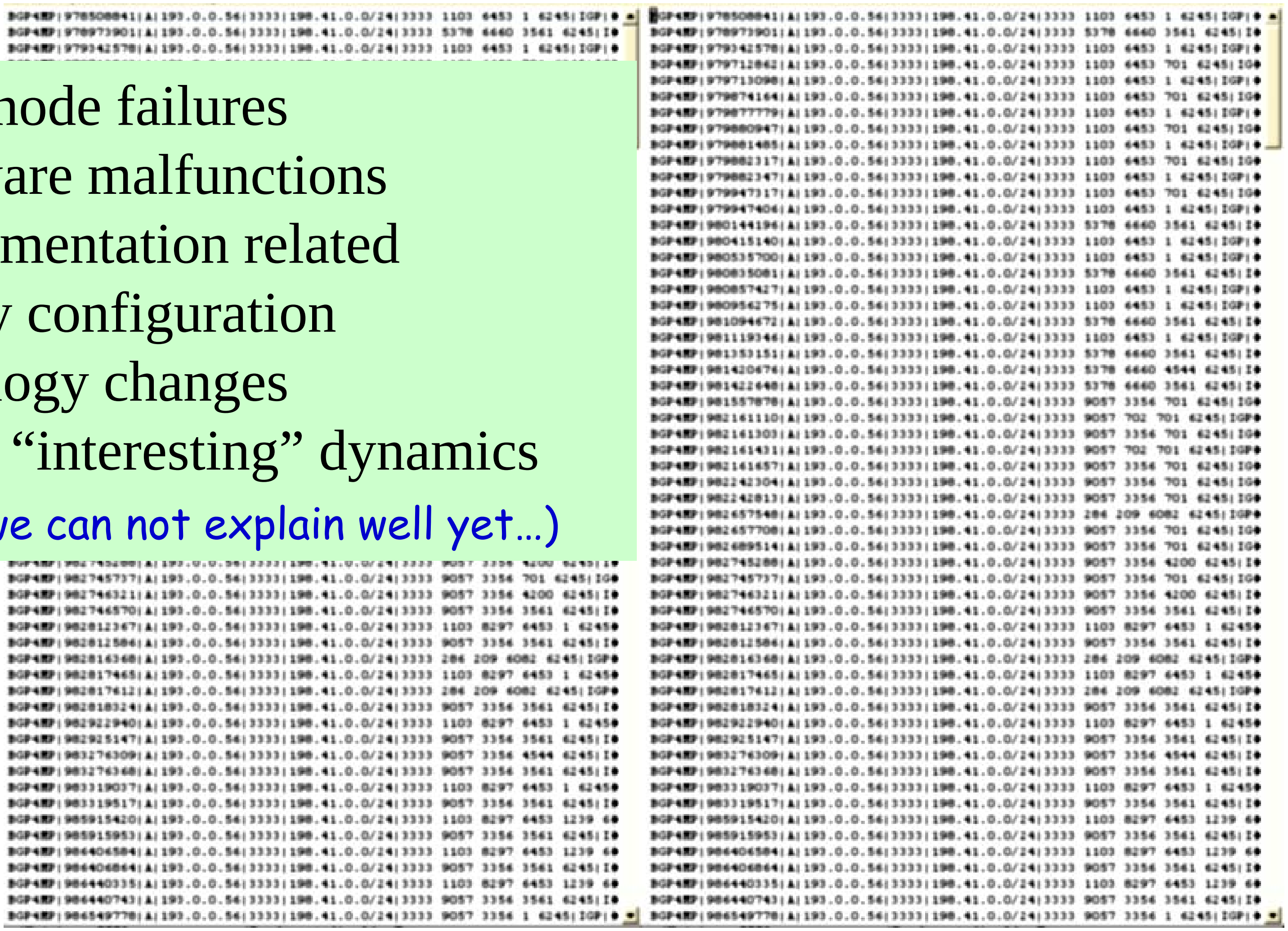




The Dynamics of “Internet”

- ➢Link/node failures
- ➢Software malfunctions
- ➢Implementation related
- ➢Policy configuration
- ➢Topology changes
- ➢Other “interesting” dynamics

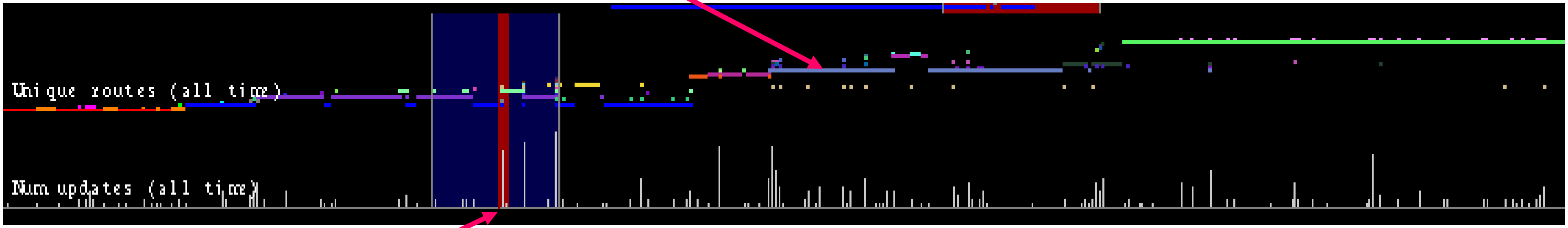
(that we can not explain well yet…)



```
BGP4MP|978508841|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|978973901|A|193.0.0.56|3333|198.41.0.0/24|3333 5378 6660 3561 6245|I●
BGP4MP|979342578|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|979712842|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 701 6245|IG●
BGP4MP|979713098|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|979874164|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 701 6245|IG●
BGP4MP|979877779|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|979880947|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 701 6245|IG●
BGP4MP|979881485|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|979882317|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 701 6245|IG●
BGP4MP|979882347|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|979947317|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 701 6245|IG●
BGP4MP|979947406|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|980144196|A|193.0.0.56|3333|198.41.0.0/24|3333 5378 6660 3561 6245|I●
BGP4MP|980415140|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|980535700|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|980835081|A|193.0.0.56|3333|198.41.0.0/24|3333 5378 6660 3561 6245|I●
BGP4MP|980857427|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|980954275|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|981094672|A|193.0.0.56|3333|198.41.0.0/24|3333 5378 6660 3561 6245|I●
BGP4MP|981119346|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|981353151|A|193.0.0.56|3333|198.41.0.0/24|3333 5378 6660 3561 6245|I●
BGP4MP|981420476|A|193.0.0.56|3333|198.41.0.0/24|3333 5378 6660 4544 6245|I●
BGP4MP|981422448|A|193.0.0.56|3333|198.41.0.0/24|3333 5378 6660 3561 6245|I●
BGP4MP|981557878|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982161110|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 702 701 6245|IGP●
BGP4MP|982161303|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982161431|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 702 701 6245|IGP●
BGP4MP|982161657|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982242304|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982242813|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982657548|A|193.0.0.56|3333|198.41.0.0/24|3333 286 209 6082 6245|IGP●
BGP4MP|982657708|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982689514|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982745288|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 4200 6245|I●
BGP4MP|982745737|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982746321|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 4200 6245|I●
BGP4MP|982746570|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|982812367|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1 6245●
BGP4MP|982812584|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|982816368|A|193.0.0.56|3333|198.41.0.0/24|3333 286 209 6082 6245|IGP●
BGP4MP|982817465|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1 6245●
BGP4MP|982817612|A|193.0.0.56|3333|198.41.0.0/24|3333 286 209 6082 6245|IGP●
BGP4MP|982818324|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|982922940|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1 6245●
BGP4MP|982925147|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|983276309|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 4544 6245|I●
BGP4MP|983276368|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|983319037|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1 6245●
BGP4MP|983319517|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|985915420|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1239 6●
BGP4MP|985915953|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|986406584|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1239 6●
BGP4MP|986406864|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|986440335|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1239 6●
BGP4MP|986440743|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|986549778|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 1 6245|IGP|●
```

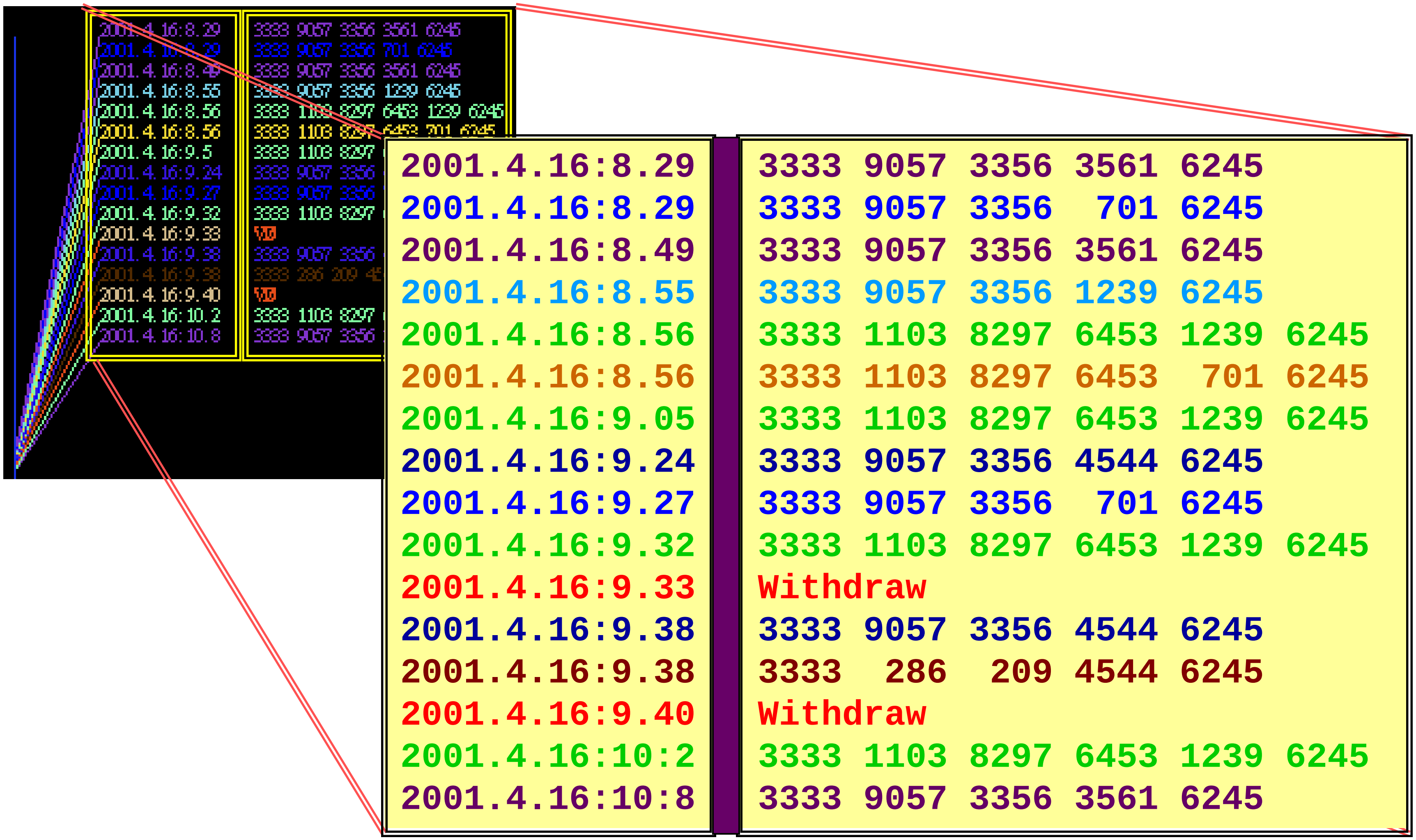
Routing Dynamics in 2001

a color dot = an AS Path being used

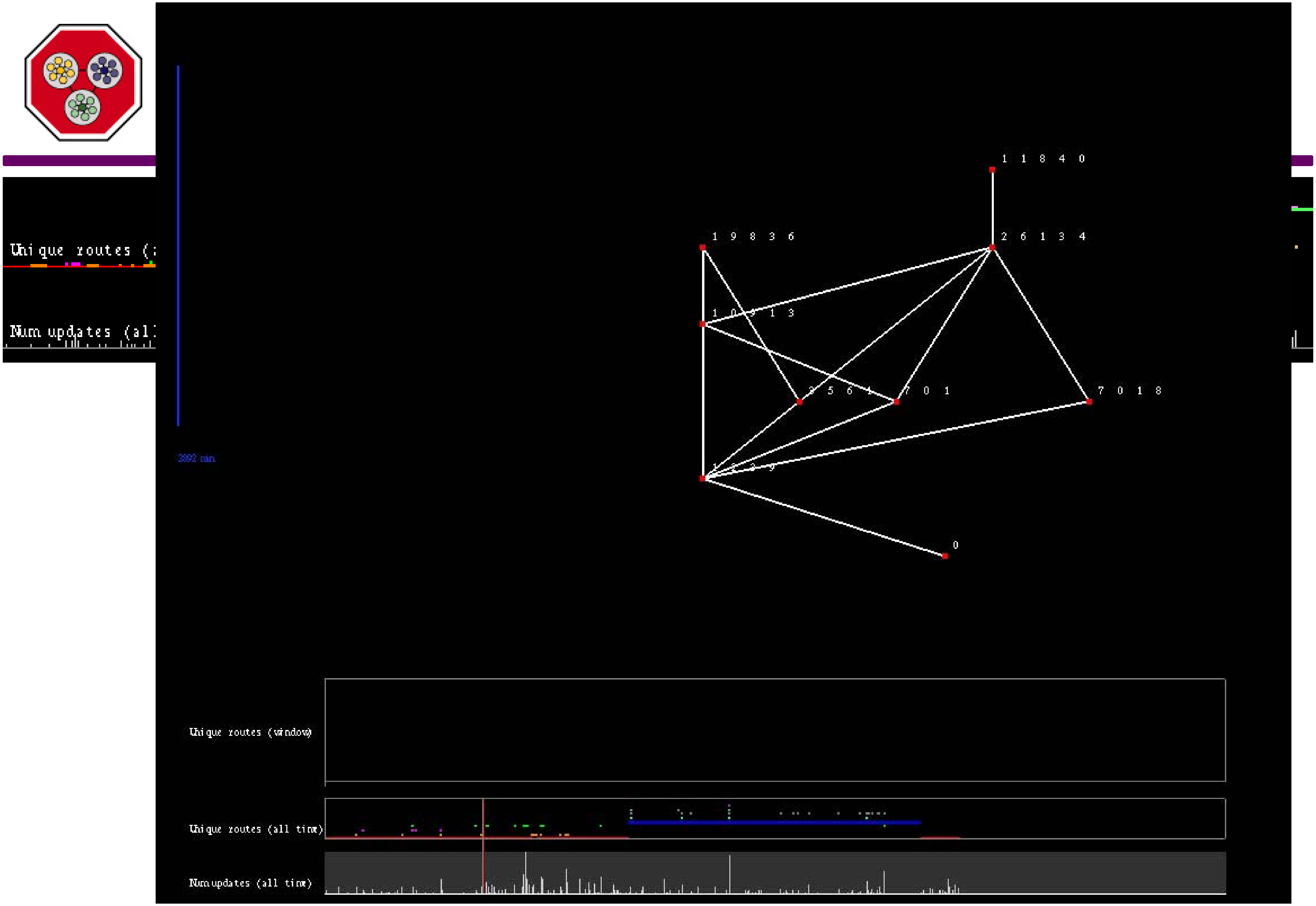


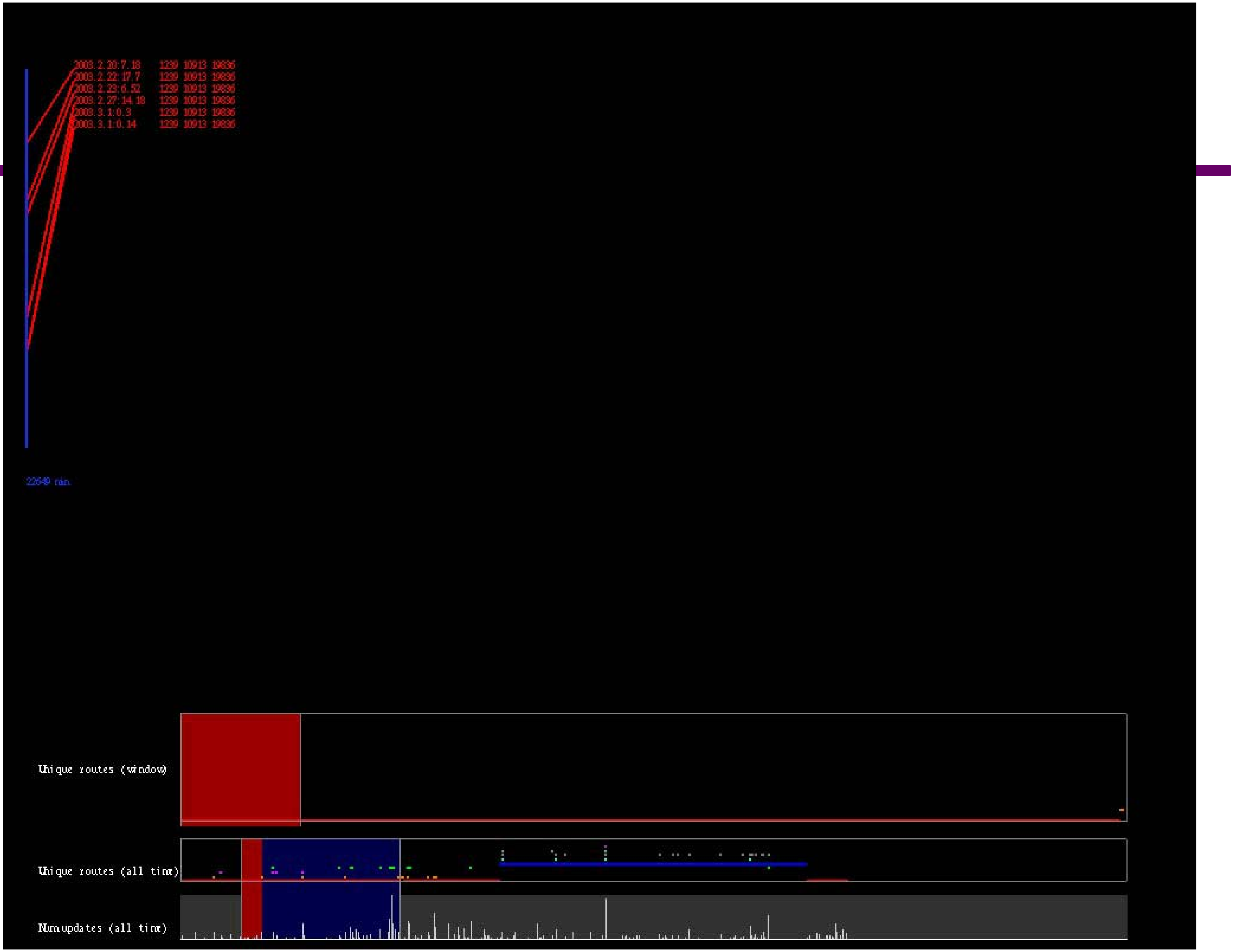
# of BGP updates over a fixed period of time (e.g., 2 hours)

DNS Root-A Server



```
2001.4.16:8.29   3333 9057 3356 3561 6245
2001.4.16:8.29   3333 9057 3356  701 6245
2001.4.16:8.49   3333 9057 3356 3561 6245
2001.4.16:8.55   3333 9057 3356 1239 6245
2001.4.16:8.56   3333 1103 8297 6453 1239 6245
2001.4.16:8.56   3333 1103 8297 6453  701 6245
2001.4.16:9.05   3333 1103 8297 6453 1239 6245
2001.4.16:9.24   3333 9057 3356 4544 6245
2001.4.16:9.27   3333 9057 3356  701 6245
2001.4.16:9.32   3333 1103 8297 6453 1239 6245
2001.4.16:9.33   Withdraw
2001.4.16:9.38   3333 9057 3356 4544 6245
2001.4.16:9.38   3333  286  209 4544 6245
2001.4.16:9.40   Withdraw
2001.4.16:10:2   3333 1103 8297 6453 1239 6245
2001.4.16:10:8   3333 9057 3356 3561 6245
```


Unique routes (:
Num updates (al
2892 min.
11840
26134
19836
10913
3561
701
7018
1239
0
Unique routes (window)
Unique routes (all time)
Num updates (all time)



```
2003.2.20:7.18     1239 10913 19836
2003.2.22:17.7     1239 10913 19836
2003.2.23:6.52     1239 10913 19836
2003.2.27:14.18    1239 10913 19836
2003.3.1:0.3       1239 10913 19836
2003.3.1:0.14      1239 10913 19836
```

Examining BGP anomalies is an expensive process even with the right tools!

- Given an ocean of BGP updates events:
  - Can we identify, maybe in a probabilistic sense, **a much smaller subset** (or **the most important subset**) of these events for the network operators to investigate?

Signature and Statistics

Signature-based detection

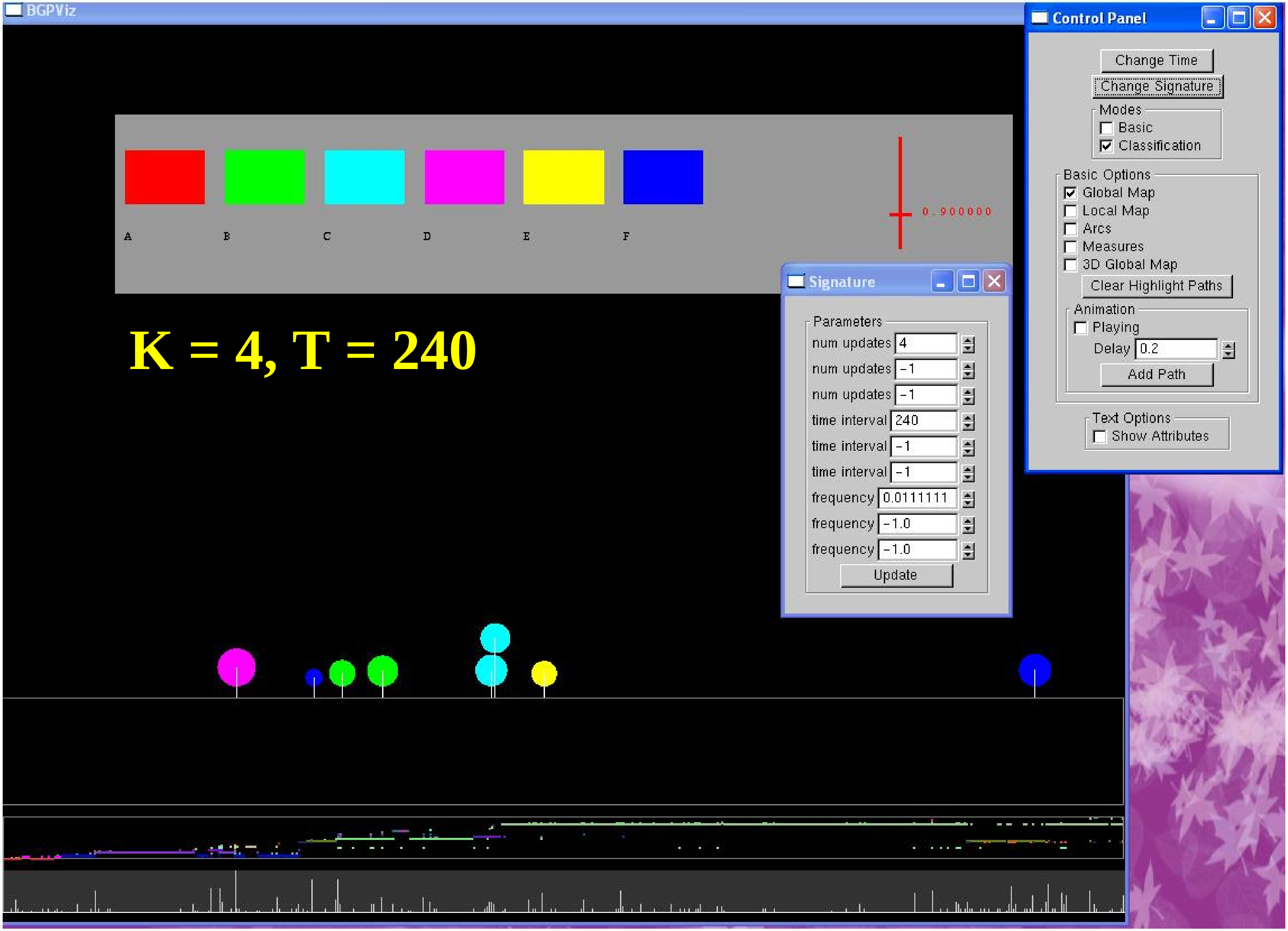
- Pre-define the signatures of anomalies
- Pattern matching

Convert “*our limited/partial understanding/modeling*” about BGP into detection heuristics (i.e., 6 signatures)

Statistics-based detection

- Build statistics profile for expected behaviors
- Compare testing behaviors with expected behaviors
- Significant deviation

Based on *our experience*, select a set of “features” (5 features in this paper) that will likely to distinguish expected from unexpected BGP behavior.



K = 4, T = 240

Signature

Parameters

num updates 4
num updates -1
num updates -1
time interval 240
time interval -1
time interval -1
frequency 0.0111111
frequency -1.0
frequency -1.0

Update

Control Panel

Change Time
Change Signature

Modes
□ Basic
☑ Classification

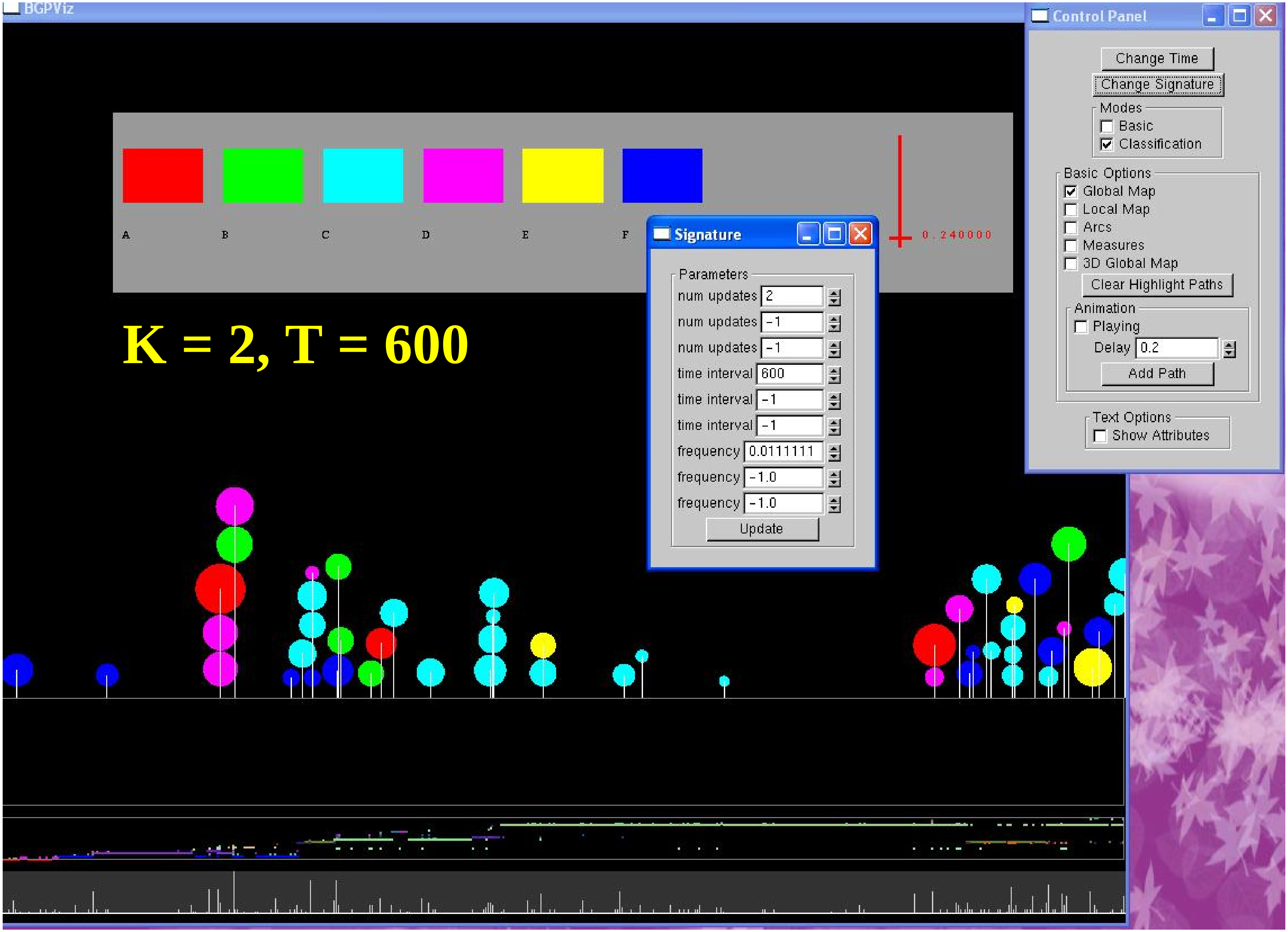
Basic Options
☑ Global Map
□ Local Map
□ Arcs
□ Measures
□ 3D Global Map

Clear Highlight Paths

Animation
□ Playing
Delay 0.2

Add Path

Text Options
□ Show Attributes



K = 2, T = 600

Signature

Parameters

num updates 2

num updates -1

num updates -1

time interval 600

time interval -1

time interval -1

frequency 0.0111111

frequency -1.0

frequency -1.0

Update

Control Panel

Change Time

Change Signature

Modes

□ Basic

☑ Classification

Basic Options

☑ Global Map

□ Local Map

□ Arcs

□ Measures

□ 3D Global Map

Clear Highlight Paths

Animation

□ Playing

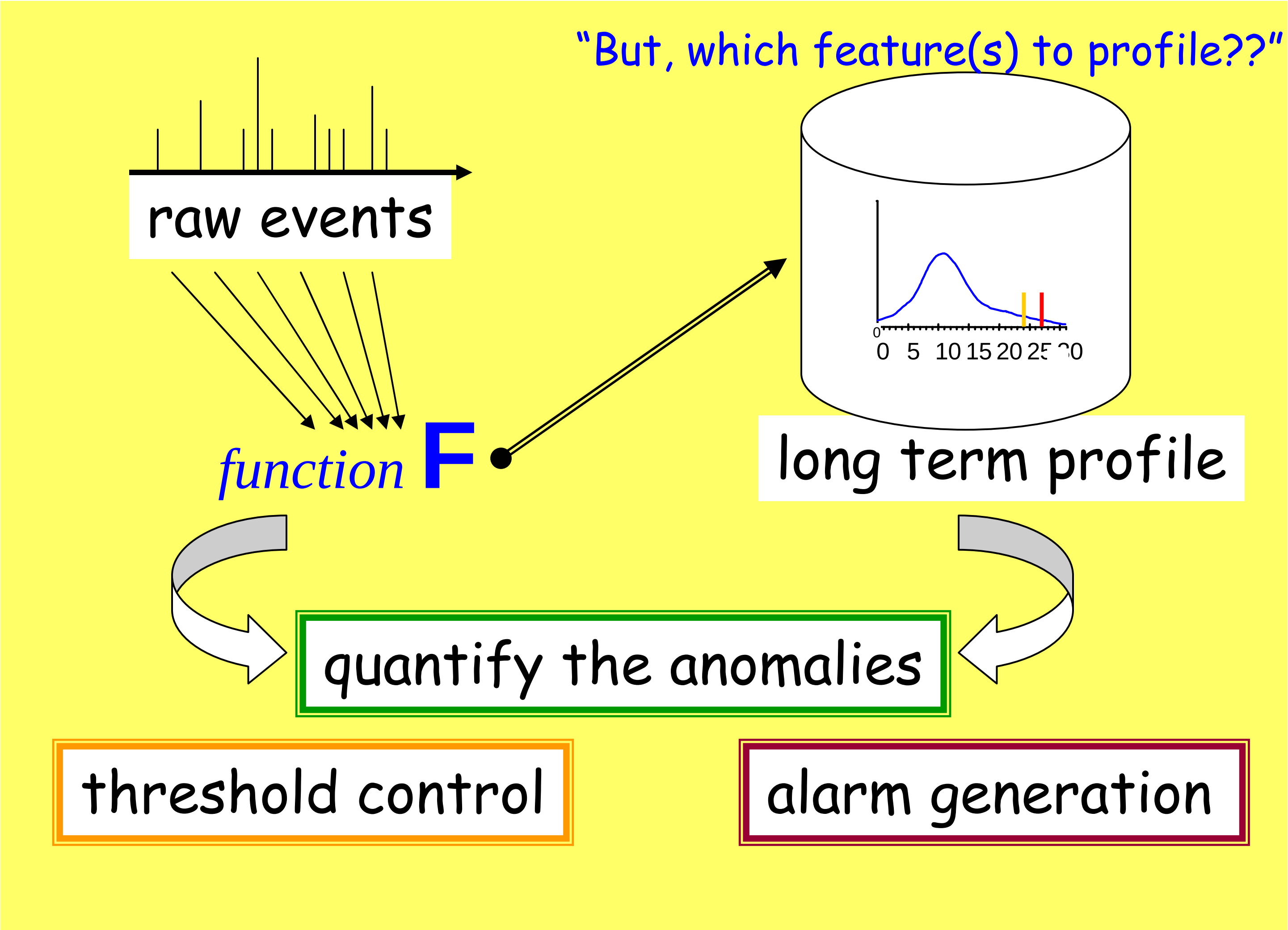
Delay 0.2

Add Path

Text Options

□ Show Attributes

Anomalies in Statistics



"But, which feature(s) to profile??"

raw events

function **F**

long term profile

quantify the anomalies

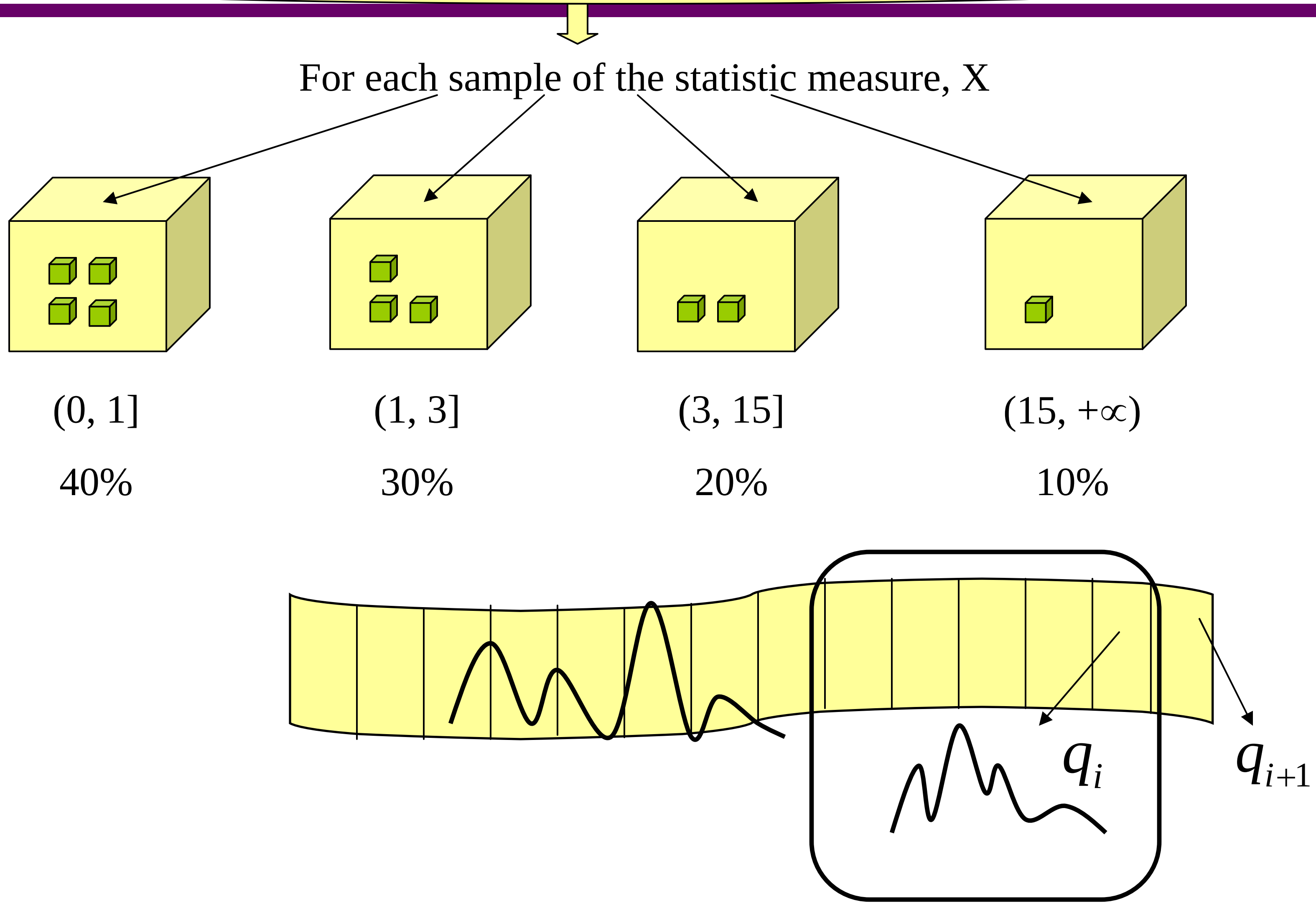
threshold control

alarm generation

5 Features/Measures

- Intensity Measures
  - BGP Update Message Arrival Frequency
  - Number of AS paths
- Categorical Measures
  - BGP Updates Types
  - AS path Occurrence Frequency
- Counting Measure
  - AS path Difference

BGP Update Messages



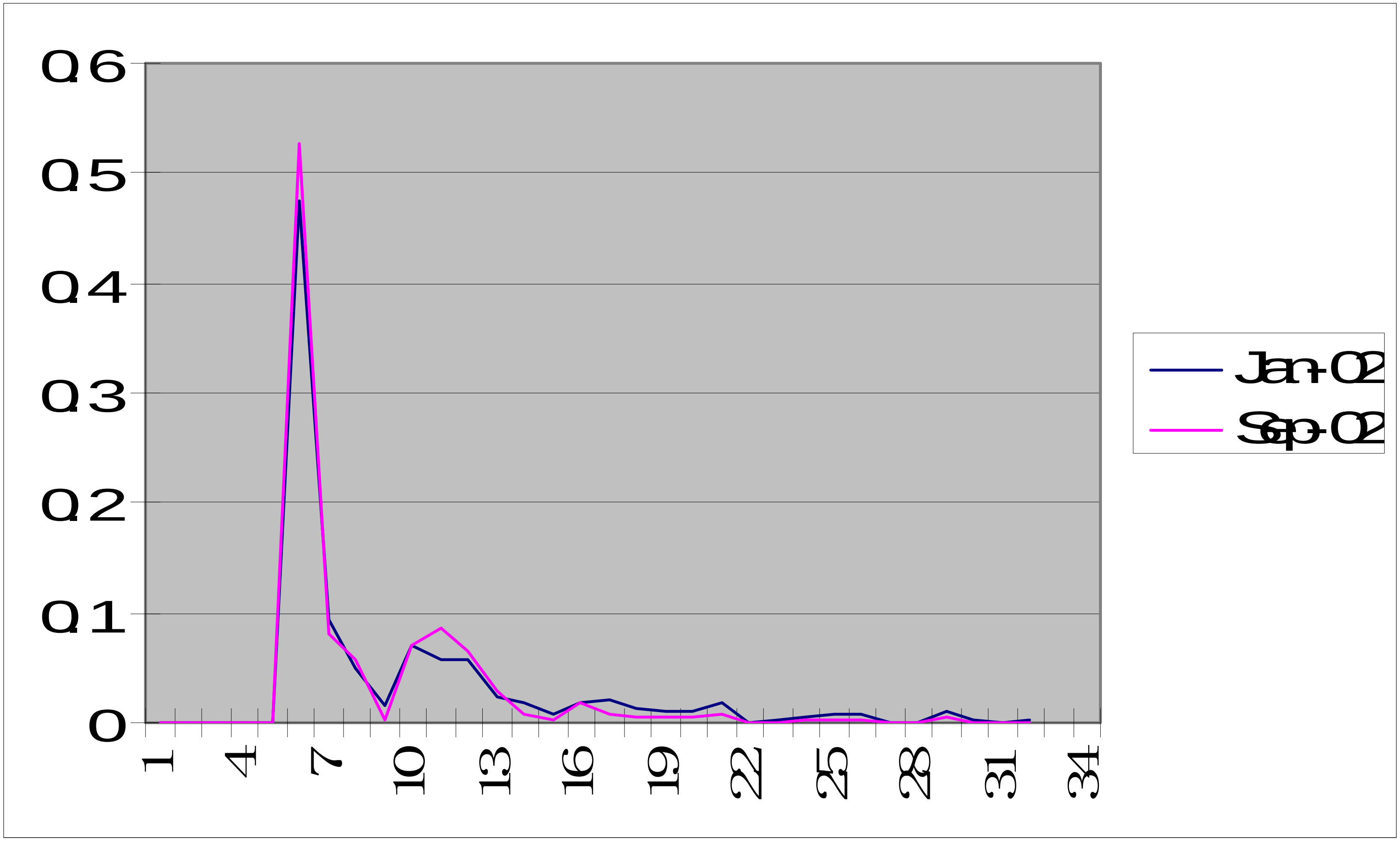
For each sample of the statistic measure, X

(0, 1]	(1, 3]	(3, 15]	(15, +∝)
40%	30%	20%	10%

AS path Occurrence Frequency (M4)

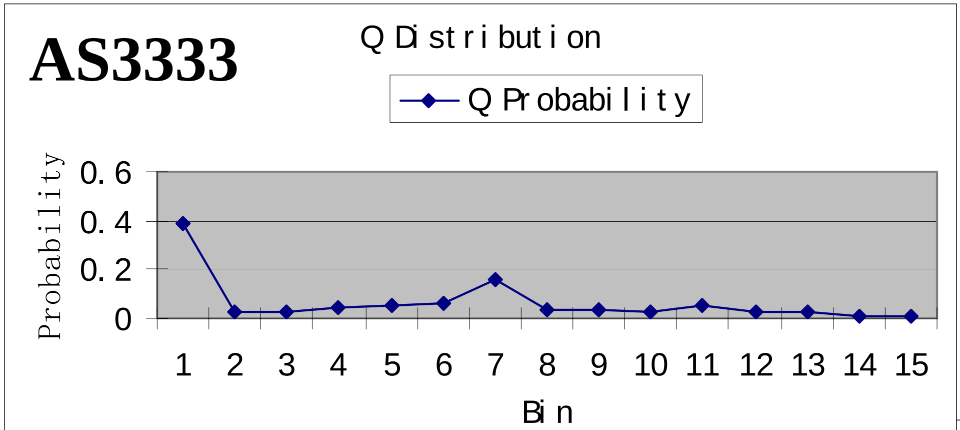
ID	AS PATH	Probability
1	3333 6461 15169	0.435875
2	3333 5378 6461 15169	6.54531e-05
3	3333 9057 6461 15169	0.272716
4	3333 286 1901 6461	0.000425322
5	3333 1103 9057 6461 15169	0.00030315
6	3333 1103 9057 3356 6461 15169	0.000313596
7	3333 286 6461 15169	0.024425
8	3333 1103 3549 6461 15169	0.0519801
…	…	…

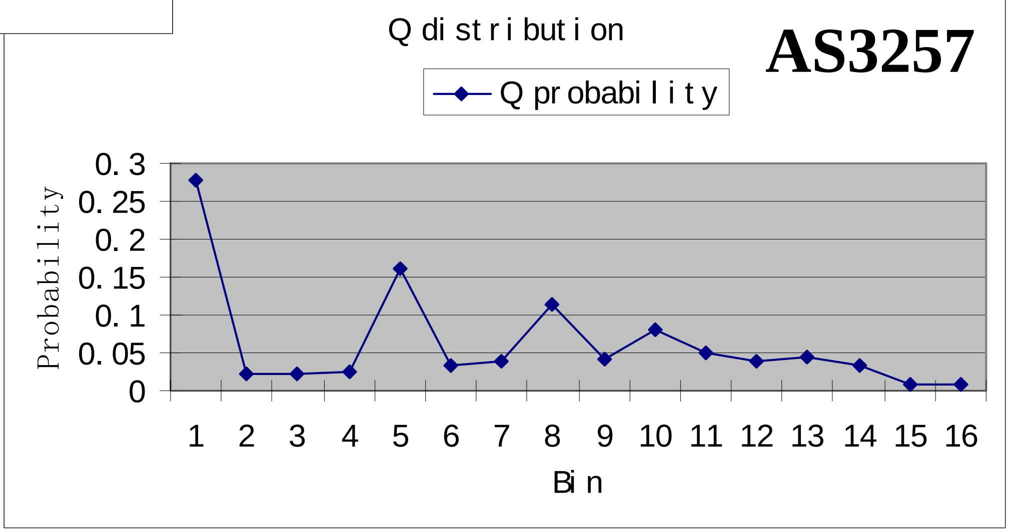
Q Distributions



AS3257 versus AS3333

(Q distri. on M1 in 2002 for 166.111/16)



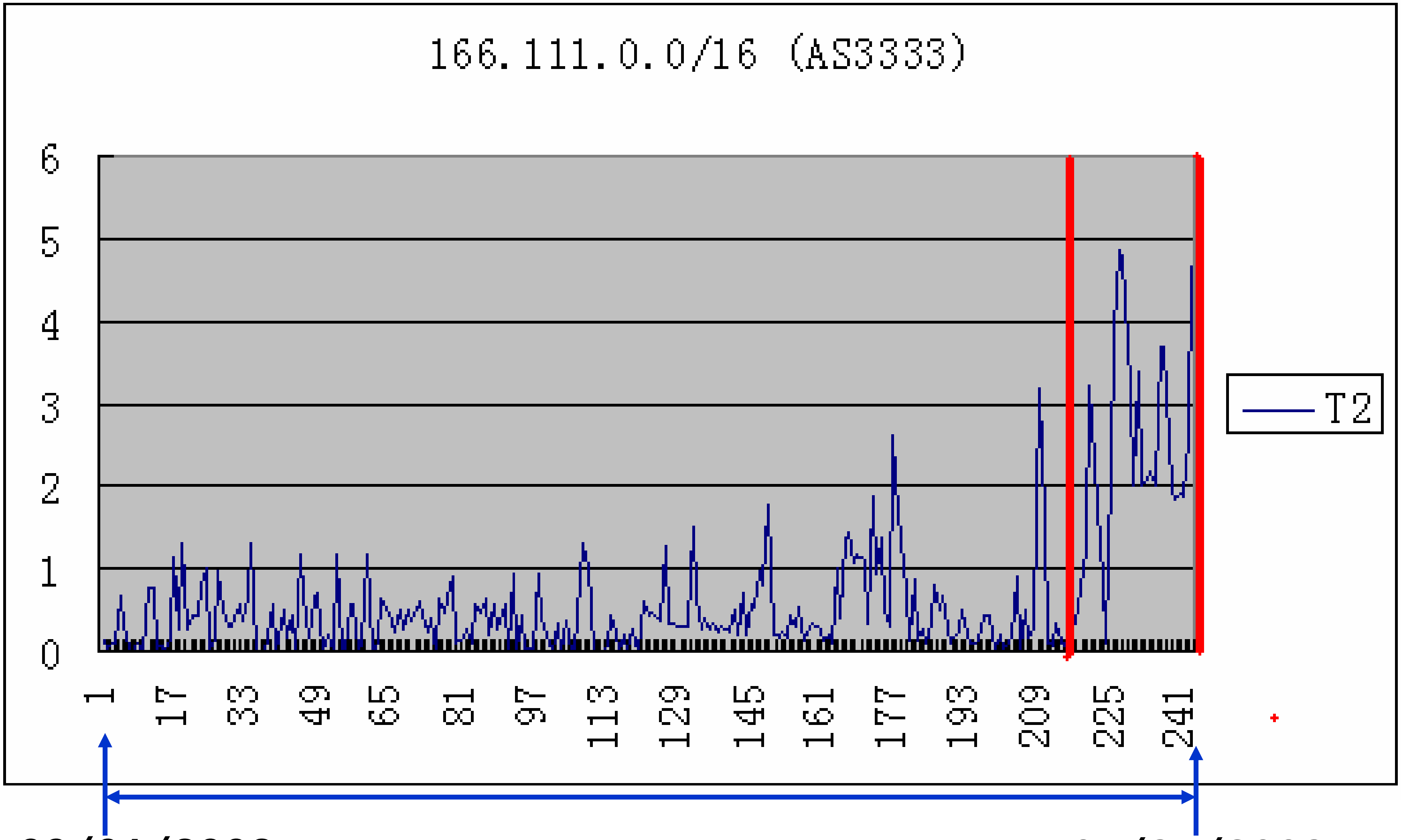


SQL Worm Attacks
(January 25, 2003)

Different prefixes manifests different behaviors

Prefixes		Observation point		
		AS3333	AS2914	AS7018
Popular prefixes	Yahoo	Normal	Normal	Normal
	Real-networks	Normal	Normal	Normal
Root_A 198.41.0.0/24		Normal	Normal	Normal
DoD prefix 199.226.96.0/20		Warning	Warning	Warning
Korean’s prefix 203.250.84.0/24		Warning	Warning	Warning
China’s prefix 166.111.0.0/16		Warning	Warning	Warning

T^2 Value of Tsinghua University



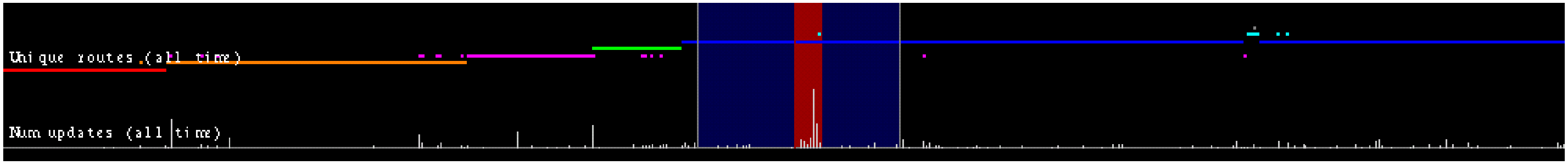
09/01/2002

01/31/2003

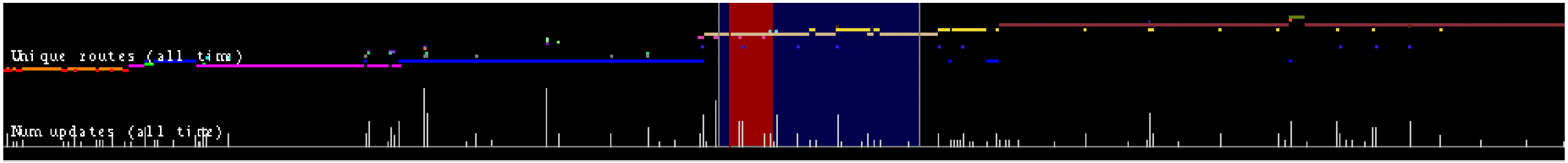
AS2914 versus AS3333

(two different peer ASes)

AS2914 in 2001



AS3333 in 2001



Comparison of 3 Prefixes

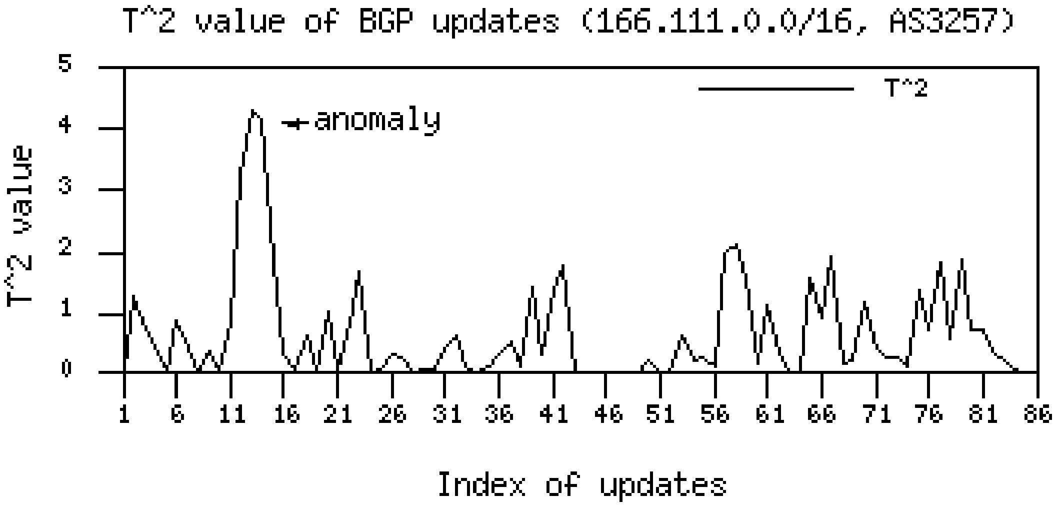
Prefixes\Measure	S1	S2	S3	S4	S5	T^2
166.111.0.0/16	1.032996	2.809773	2.610673	1.220799	2.659919	4.868608
203.250.84.0/24	1.607696	1.967813	2.554678	0.212015	2.046884	3.235723
199.226.96.0/20	2.497571	1.907853	2.366445	0.773497	2.313003	4.285221

- Large S3 comes from withdrawal messages
- Large S2 indicates arrival of new AS path
- Large S5 is because the new path is significantly different with the primary path

The BGP Path to Beijing

(Networking'2004)

01/10/2003 500 seconds


T^2 value of BGP updates (166.111.0.0/16, AS3257)

The primary path: 3257 1239 9405 4538 (via SPRINT)

A new path: 3257 3356 12013 3681 20080 11537 9405 4538

last for approximately 500sec

AS3356:	L3 Network
AS12013 :	Florida Atlantic University
AS3681:	Florida International University
AS20080:	Florida International University
AS11537:	Abilene Network(Abilene)
AS9405:	TPS-CN-AS (Tsinghua University, Beijing)
AS4538:	China Education and Research Network Center

Response from AS11537

From: Brent Sweeny sweeny@indiana.edu:

...

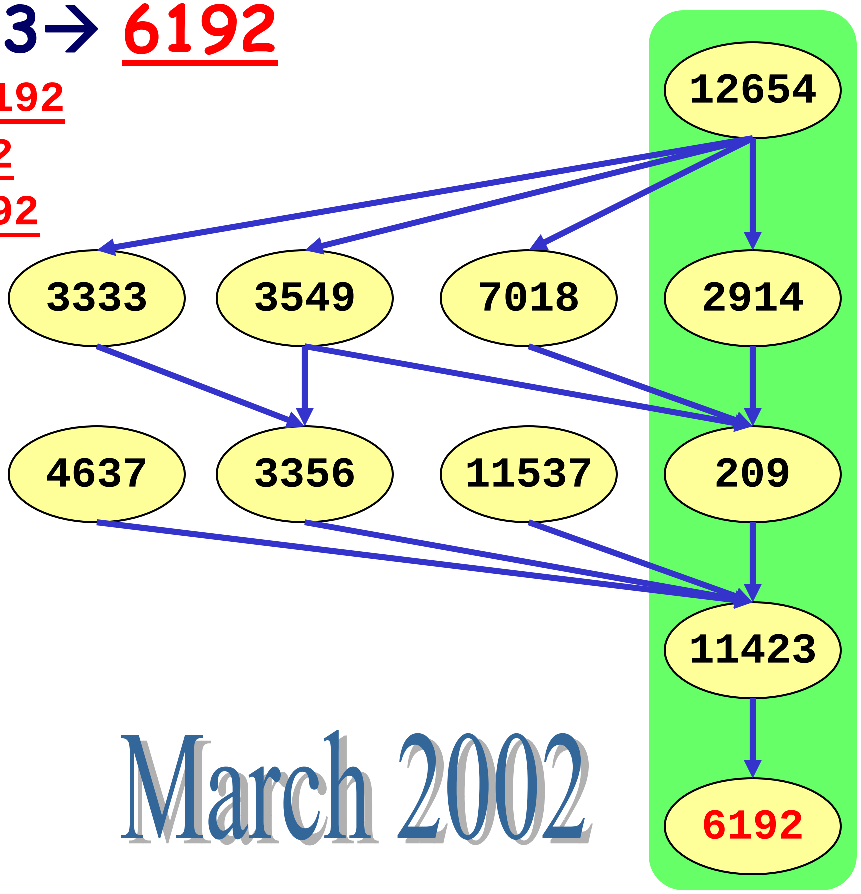
now to what the logs show me, after examining them for the whole day of Jan 10 2003: **the biggest change that day, taking place at about 10amEST on all of our routers, was a change made to finally disable OSPF** (ISIS had been turned up some time earlier and was preferred; this last step was to remove OSPF entirely). even though OSPF wasn't preferred, the change to the rib could conceivably have caused shimmies through the routers' routing processes and forwarding tables as they rearranged themselves for a short time--I don't think we were aware of anything like what you've seen at the time, but it could have happened and we might not have noticed. other things going on during the day were: - what appears to be some more futzing with OSPF 1032-1034EST - some interface debugging work 1400-1558EST - removing some BGP neighbors 1214-1215EST and 1558-1600EST

BGP Anomalies

- Detection and Analysis of Anomalies
- Elisha, a tool:
  - integration of visualization, signatures, and statistics
  - interactive investigation
  - explanation-based analysis/learning

Origin AS in an AS Path

- UCDavis (AS-6192) owns 169.237/16 and AS-6192 is the origin AS
- AS Path: **513→11537→11423→ 6192**
  - 12654 13129 6461 3356 11423 6192
  - 12654 9177 3320 209 11423 6192
  - 12654 4608 1221 4637 11423 6192
  - 12654 777 2497 209 11423 6192
  - 12654 3549 3356 11423 6192
  - 12654 3257 3356 11423 6192
  - 12654 1103 11537 11423 6192
  - 12654 3333 3356 11423 6192
  - 12654 7018 209 11423 6192
  - 12654 2914 209 11423 6192
  - 12654 3549 209 11423 6192



March 2002

169.237/16

November 2004

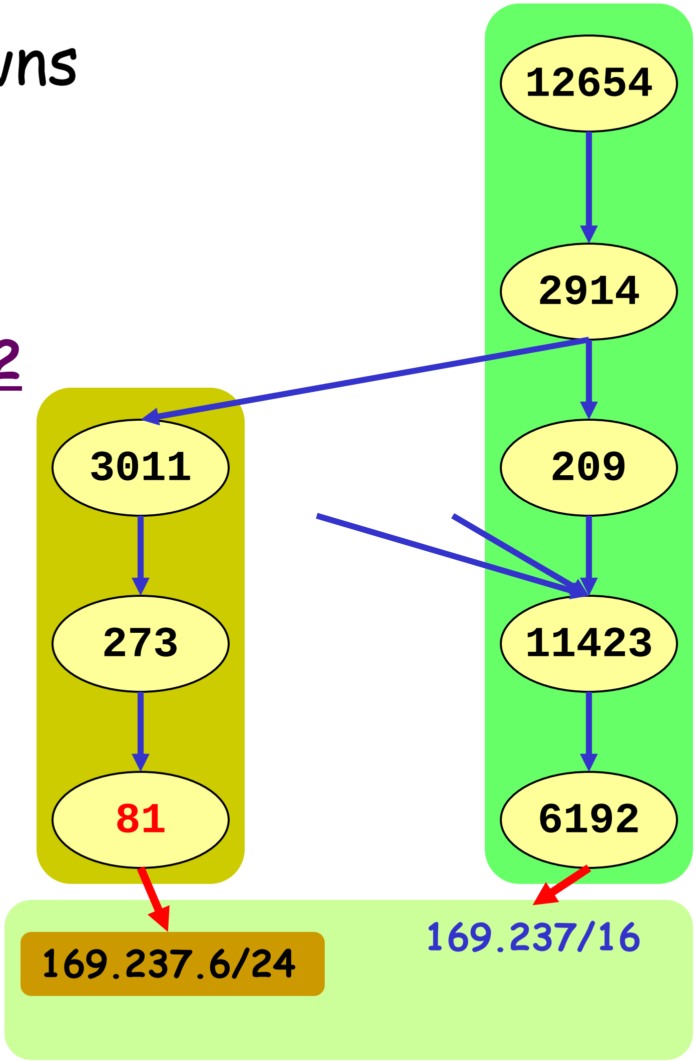
```
               2152 6192                       1668 3356 2152 6192
       286 174 2152 6192                       3257 3356 2152 6192
      2914 174 2152 6192     21202 30912 29518 3549 3356 2152 6192
 3130 2914 174 2152 6192                       3561 3356 2152 6192
      3292 174 2152 6192                       5511 3356 2152 6192
      3549 174 2152 6192                       6453 3356 2152 6192
 2493 3602 174 2152 6192                       7018 3356 2152 6192
      5462 174 2152 6192                            3557 2152 6192
      5503 174 2152 6192                       1221 4637 2152 6192
      5511 174 2152 6192                            6539 2152 6192
      6667 174 2152 6192                            6939 2152 6192
      6762 174 2152 6192                       3257 6939 2152 6192
      6895 174 2152 6192            16150 8434 3257 6939 2152 6192
     15444 174 2152 6192                       5390 6939 2152 6192
           293 2153 6192                       8121 6939 2152 6192
          2497 2152 6192                       8426 6939 2152 6192
     4777 2497 2152 6192                      12956 6939 2152 6192
     7500 2497 2152 6192                      13237 6939 2152 6192
          3303 2152 6192                      15444 6939 2152 6192
          3356 2152 6192                           11608 2152 6192
 2905 701 3356 2152 6192                10876 4600 11537 2153 6192
     1239 3356 2152 6192                      7660 11537 2153 6192
3130 1239 3356 2152 6192
```

AS2152 CSU-53 California State University

AS2153 CSU-53 California State University

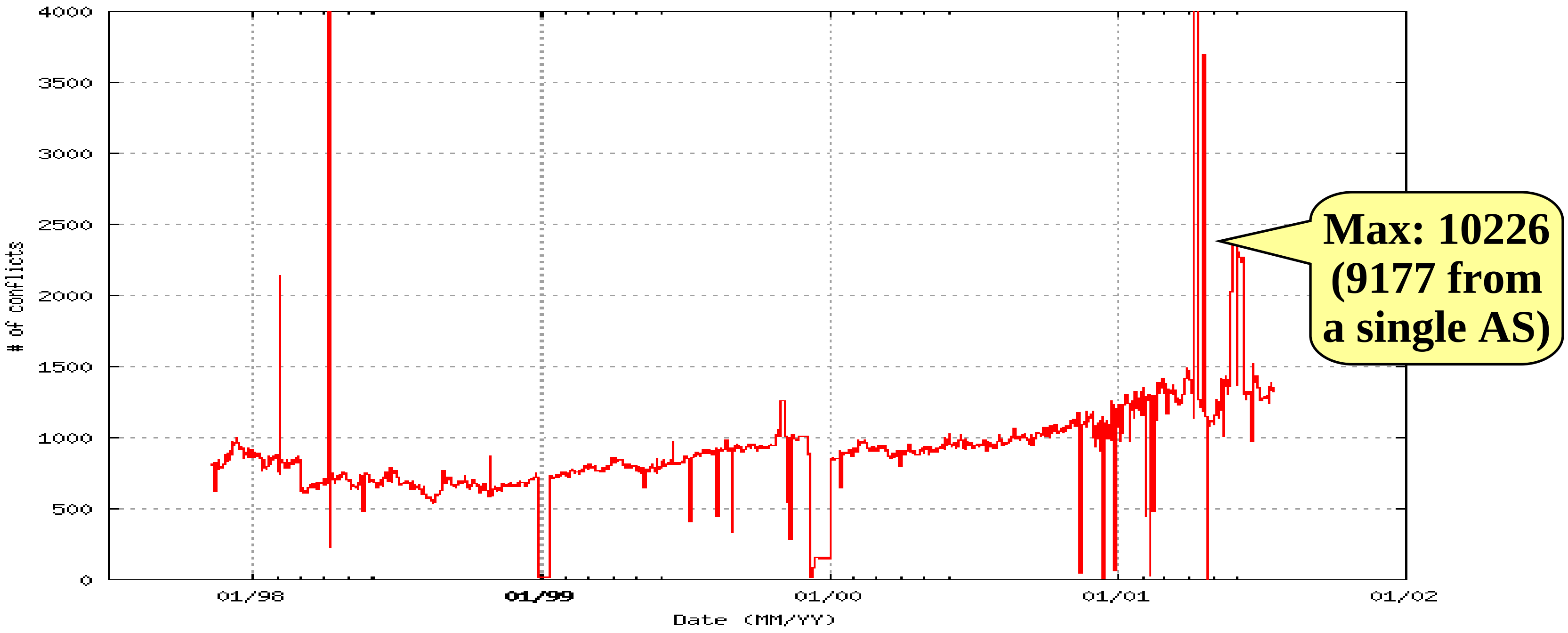
Origin AS Changes (OASC)

- Ownership: UCDavis (AS-6192) owns 169.237/16 and AS-6192 is the origin AS
- **Current**
  - AS Path: **2914→209→11423→ 6192**
  - for prefix: 169.237/16
- **New**
  - AS Path: **2914→3011→273→ 81**
  - even worse: 169.237.6/24
- Which route path to use?
- Normal or Abnormal??



BGP MOAS/OASC Events

(IMW’2001, Explanation ➔ DSOM’2003)



Max: 10226 (9177 from a single AS)

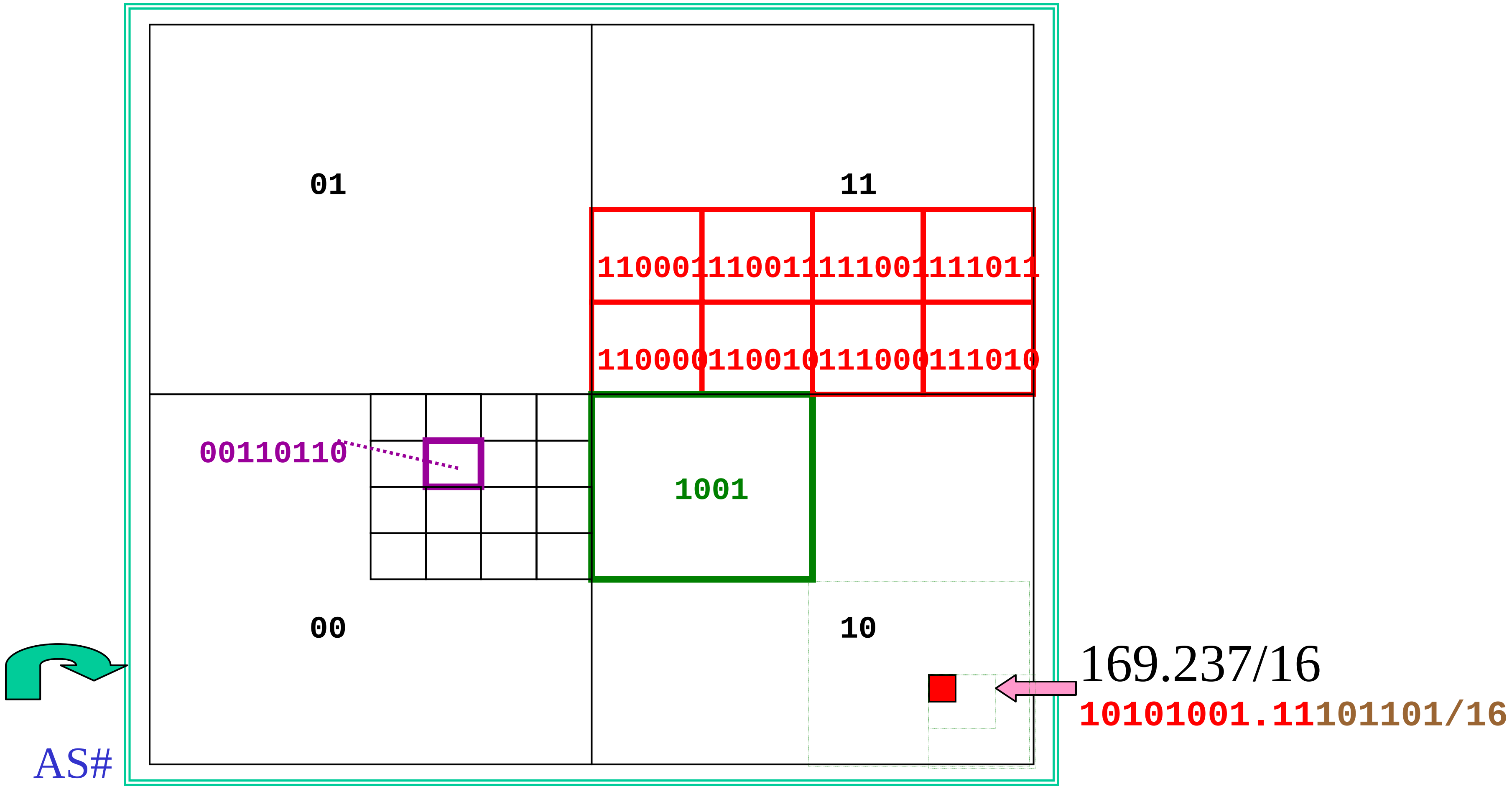
year	Median number	increase rate	#BGP table entries	increase rate
1998	683		52000	
1999	810.5	18.7%	60000	15.40%
2000	951	17.3%	80000	33.30%
2001	1294	34.8%	109000	36%

Real-Time OASC Detection

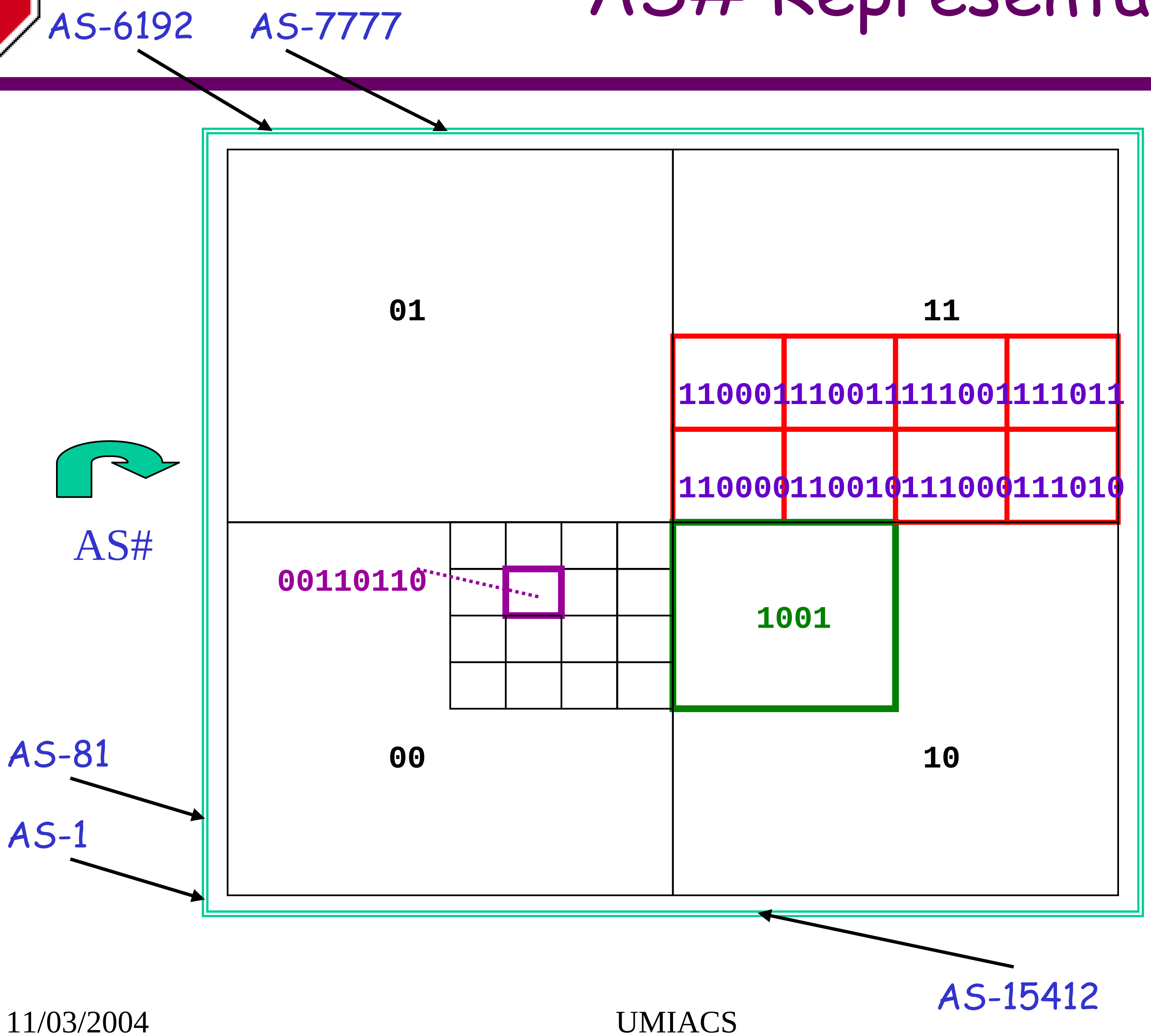
- Low level events: BGP Route Updates
- High level events: OASC
  - 1000+ per day and max 10226 per day
  - per 3-minutes window in real-time demo

- IP address blocks
- Origin AS in BGP Update Messages
- Different Types of OASC Events

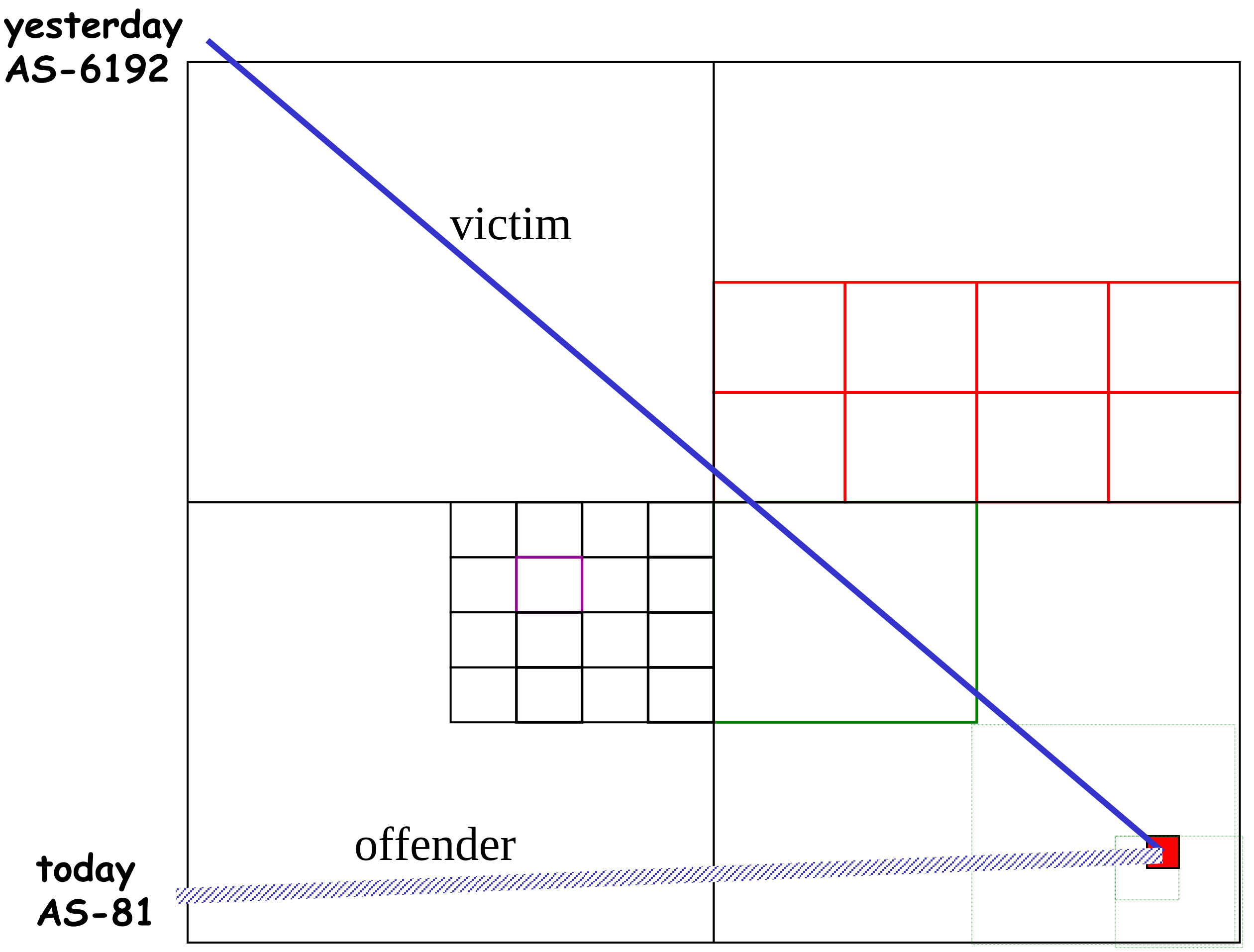
Qua-Tree Representation of IP Address Prefixes



AS# Representation



AS81 punched a “hole” on 169.237/16

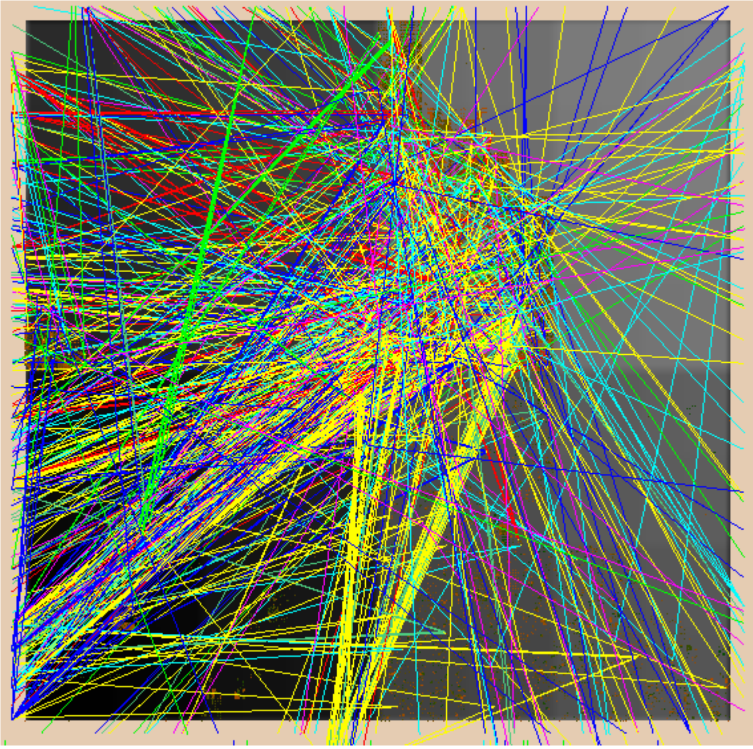


yesterday
169.237/16

today
169.237/16
169.237.6/24

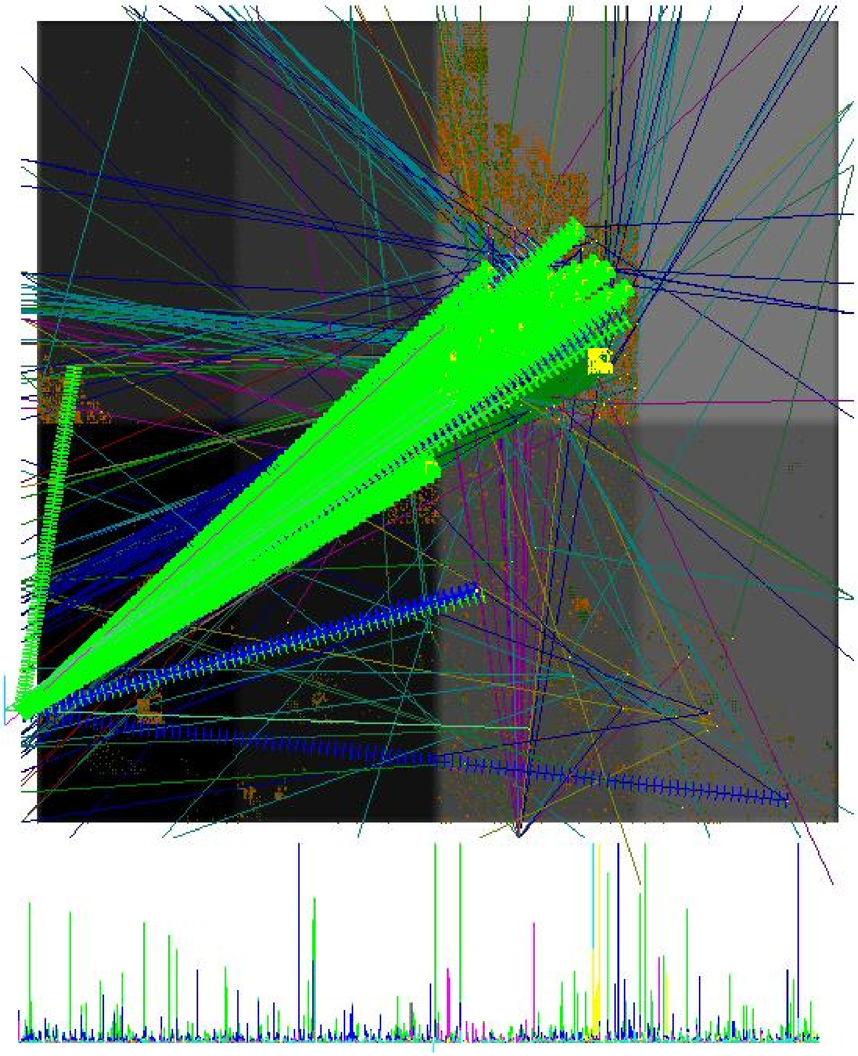
OASC Event Types

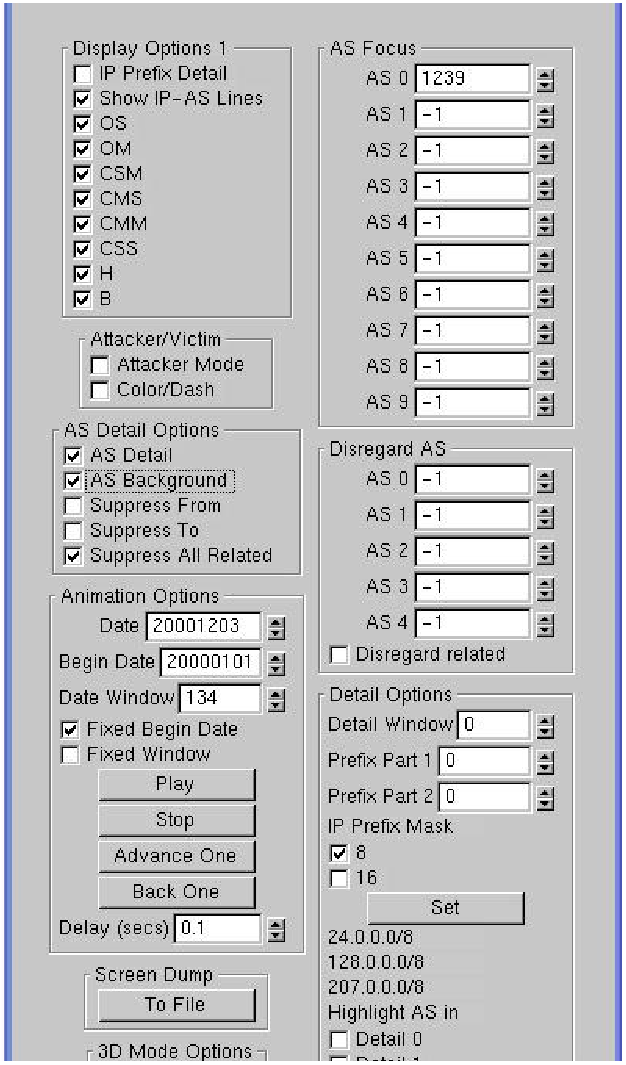
- Using different colors to represent types of OASC events
- C type: CSS, CSM, CMS, CMM
- H type: H
- B type: B
- O type: OS, OM



SPRINT (AS-1239)

(on December 3, 2000, 3000+ B events)





Display Options 1

- ☐ IP Prefix Detail
- ☑ Show IP-AS Lines
- ☑ OS
- ☑ OM
- ☑ CSM
- ☑ CMS
- ☑ CMM
- ☑ CSS
- ☑ H
- ☑ B

Attacker/Victim

- ☐ Attacker Mode
- ☐ Color/Dash

AS Detail Options

- ☑ AS Detail
- ☑ AS Background
- ☐ Suppress From
- ☐ Suppress To
- ☑ Suppress All Related

Animation Options

- Date 20001203
- Begin Date 20000101
- Date Window 134
- ☑ Fixed Begin Date
- ☐ Fixed Window

Delay (secs) 0.1

Screen Dump

3D Mode Options

AS Focus

- AS 0 1239
- AS 1 -1
- AS 2 -1
- AS 3 -1
- AS 4 -1
- AS 5 -1
- AS 6 -1
- AS 7 -1
- AS 8 -1
- AS 9 -1

Disregard AS

- AS 0 -1
- AS 1 -1
- AS 2 -1
- AS 3 -1
- AS 4 -1
- ☐ Disregard related

Detail Options

- Detail Window 0
- Prefix Part 1 0
- Prefix Part 2 0

IP Prefix Mask

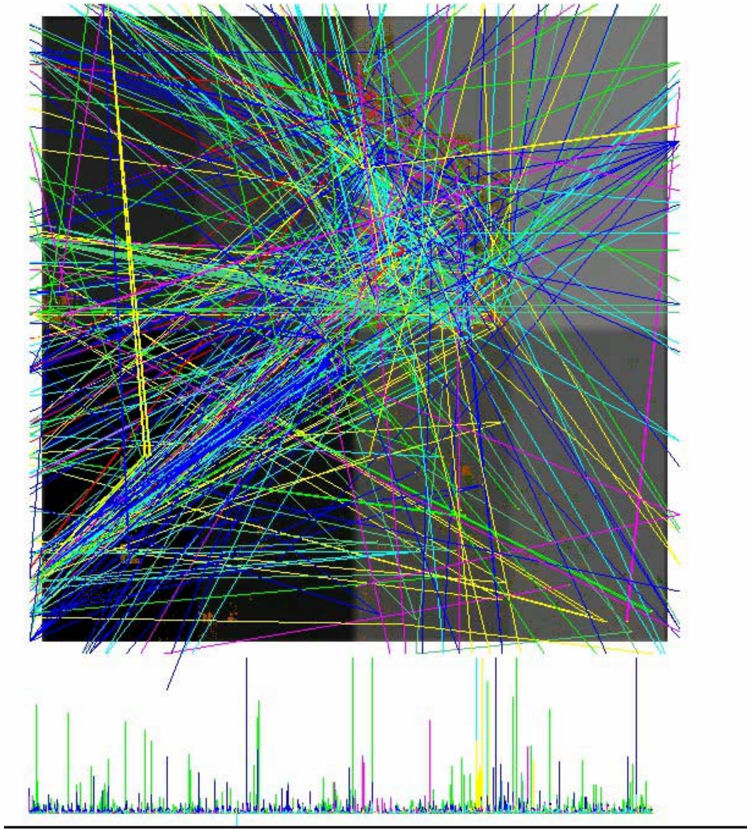
- ☑ 8
- ☐ 16

24.0.0.0/8
128.0.0.0/8
207.0.0.0/8

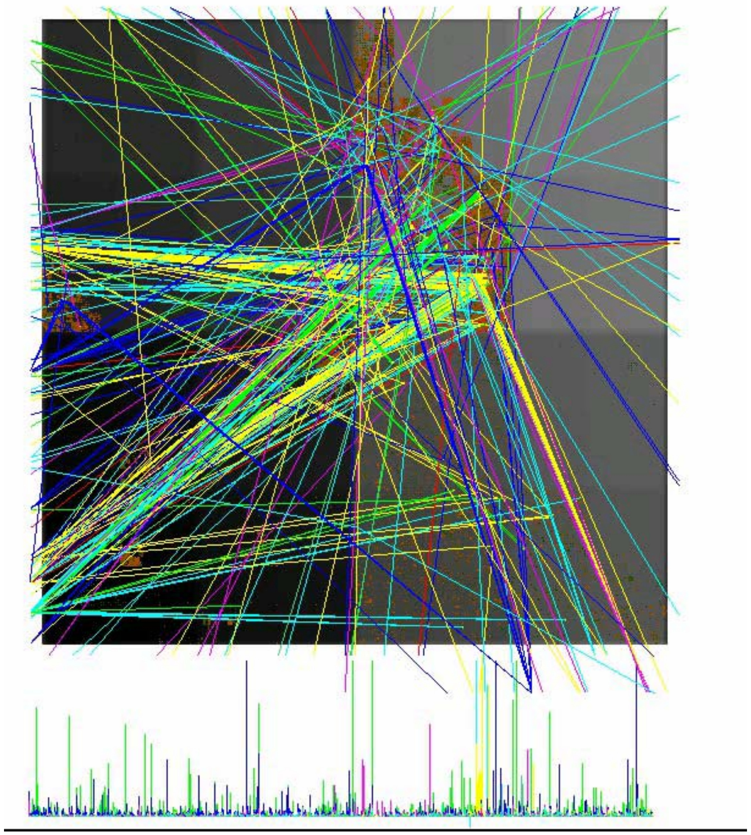
Highlight AS in

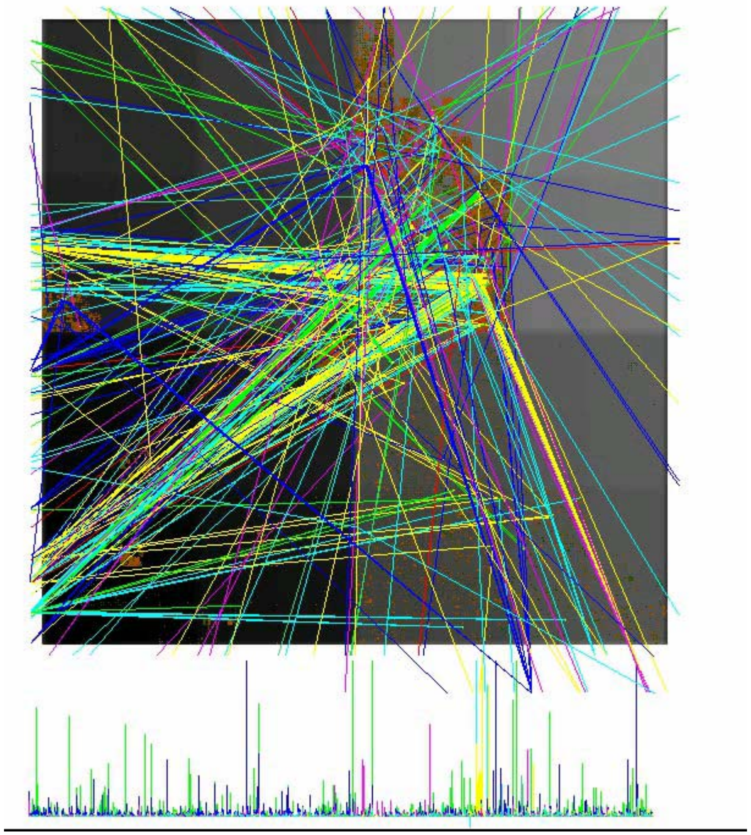
- ☐ Detail 0

“Normal“

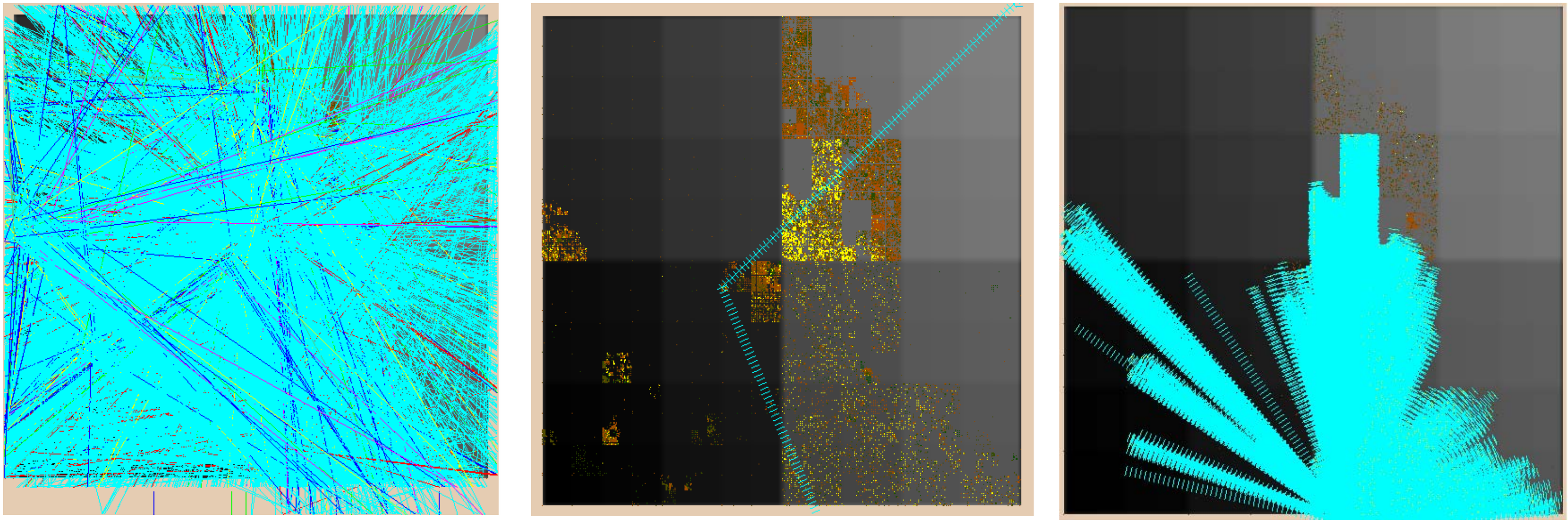


AS15412 in April, 2001



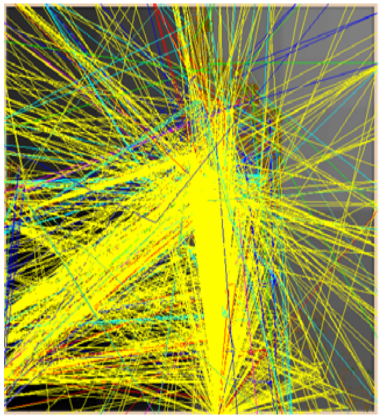


April 6, 2001

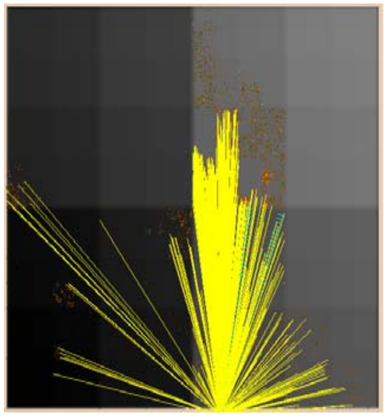


AS15412 caused 40K+ MOAS/OASC events within 2 weeks…

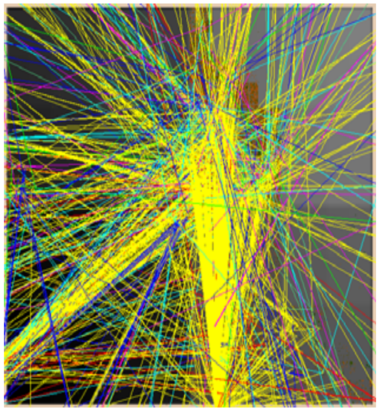
April 7-10, 2001



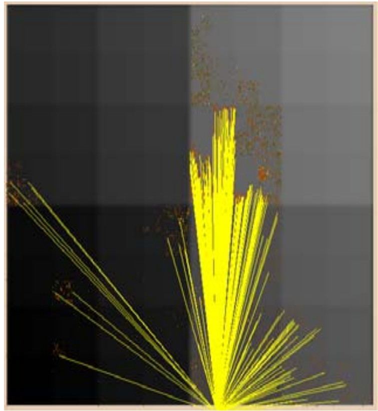
04/07/2001 all



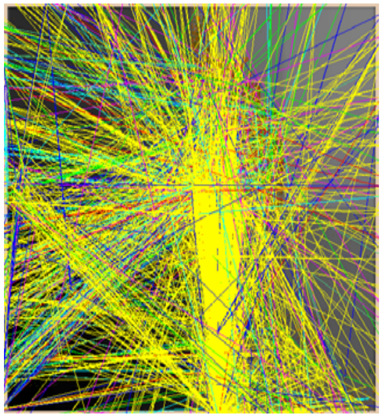
04/07/2001 15412



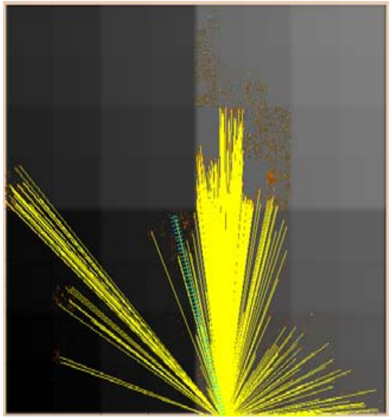
04/08/2001 all



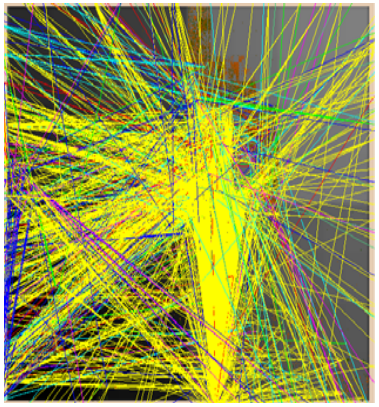
04/08/2001 15412



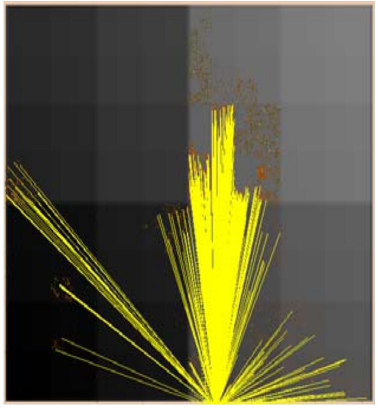
04/09/2001 all



04/09/2001 15412

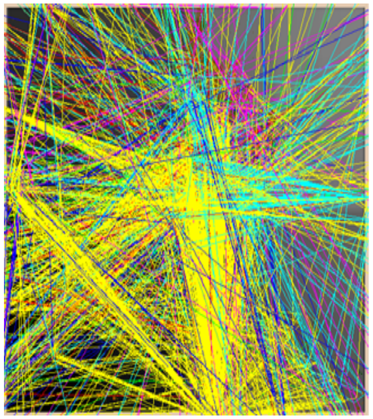


04/10/2001 all

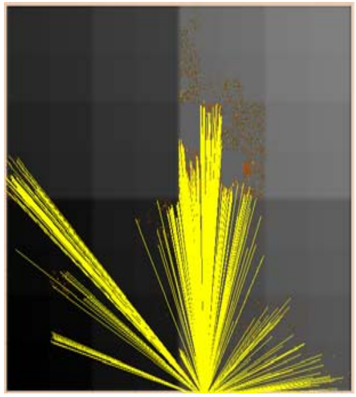


04/10/2001 15412

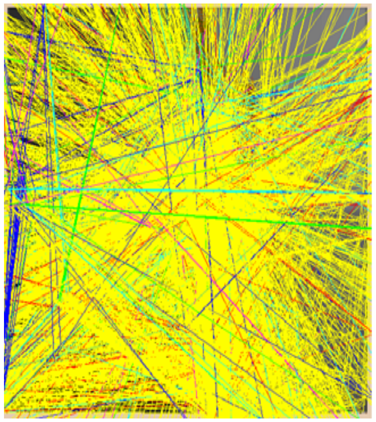
April 11-14, 2001



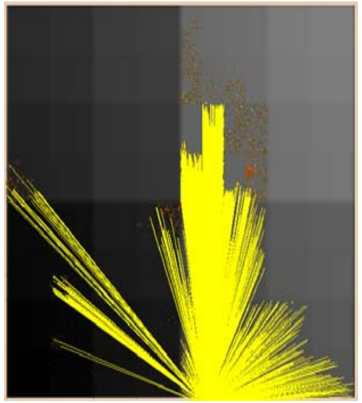
04/11/2001 all



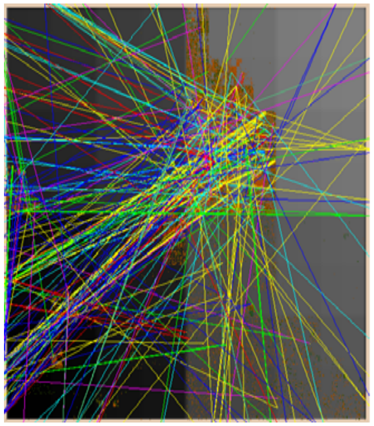
04/11/2001 15412



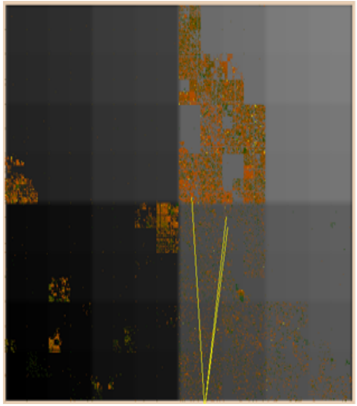
04/12/2001 all



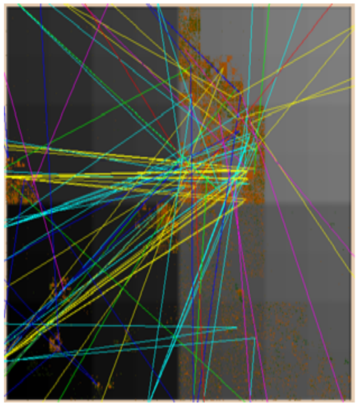
04/12/2001 15412



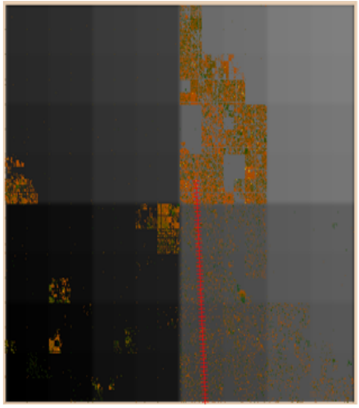
04/13/2001 all



04/13/2001 15412

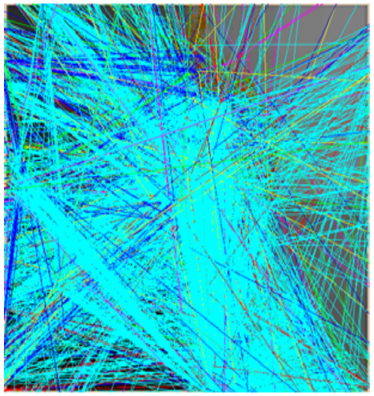


04/14/2001 all

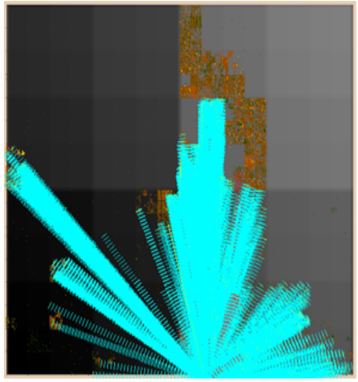


04/14/2001 15412

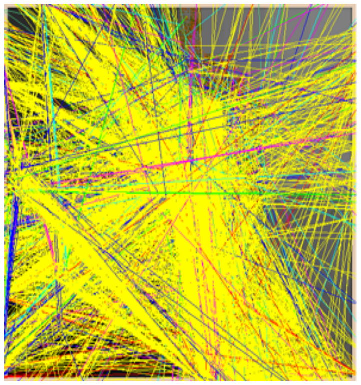
April 18-19, 2001 – Again??



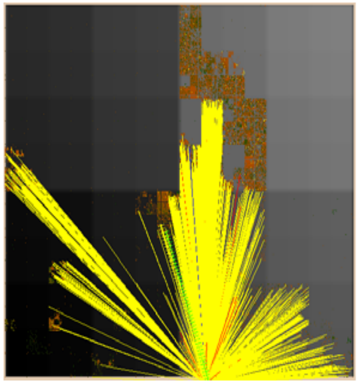
04/18/2001 all



04/18/2001 15412

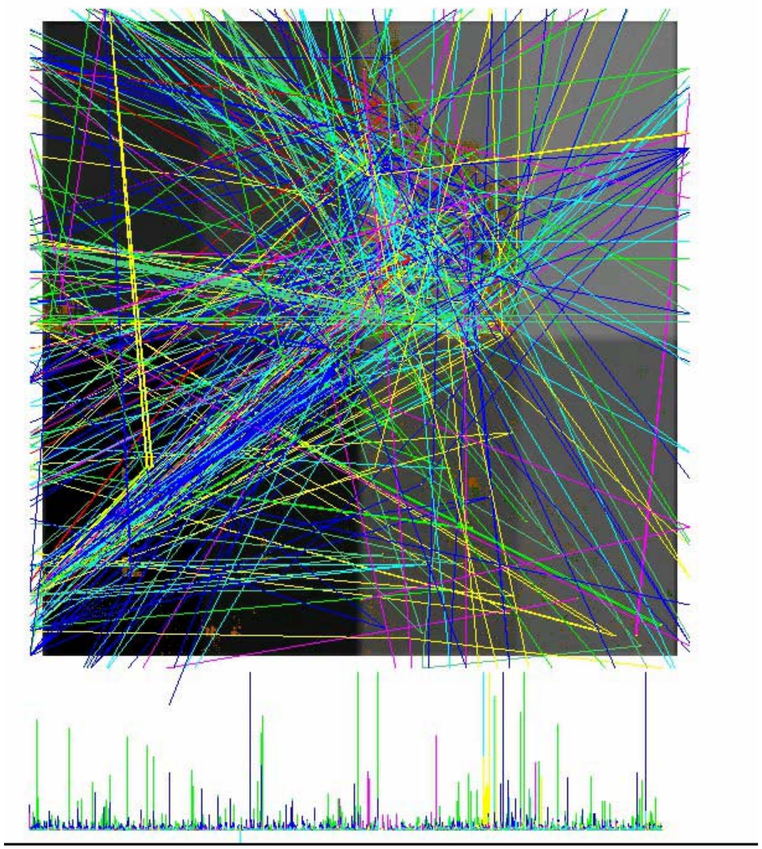


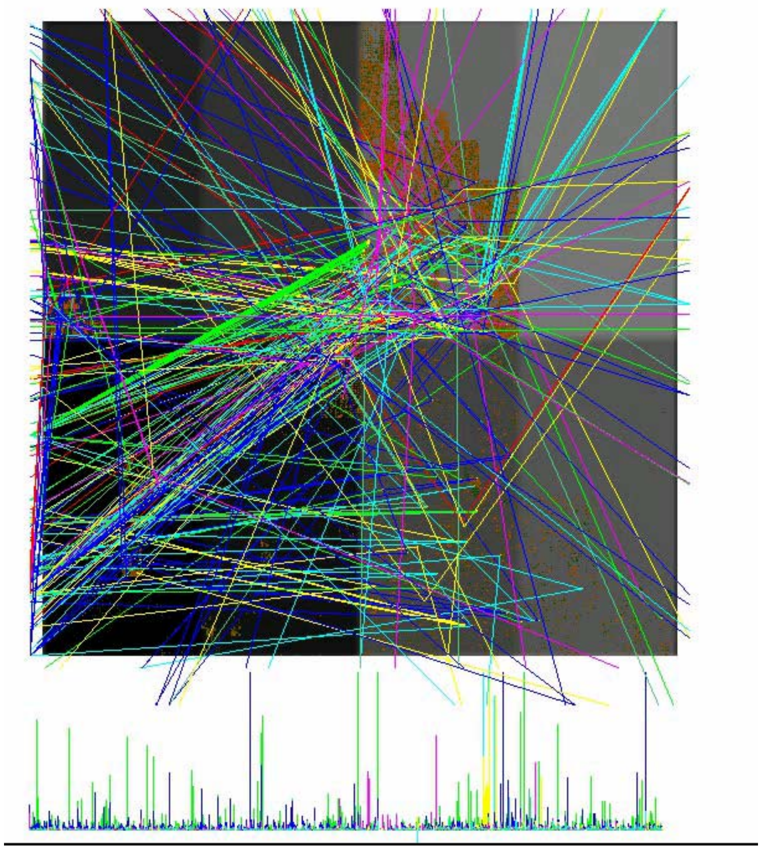
04/19/2001 all



04/19/2001 15412

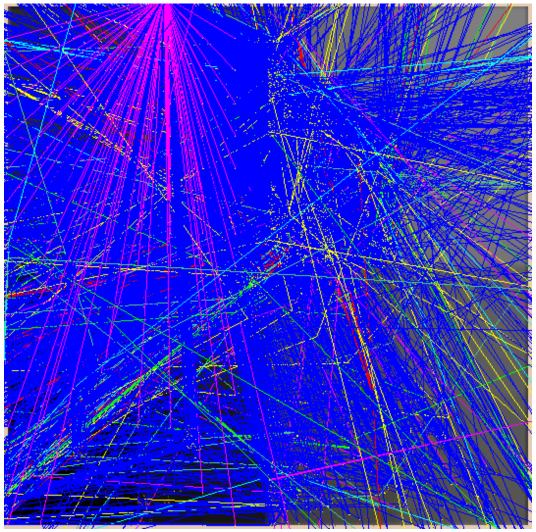
AS7777 in 08/14/2000 the Pink in 02/19/2001

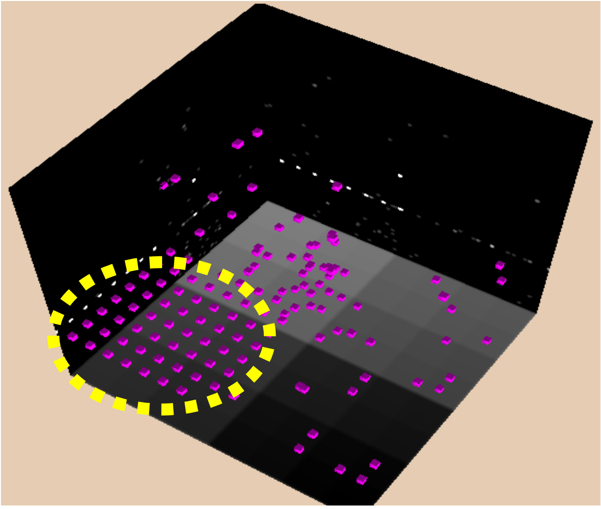


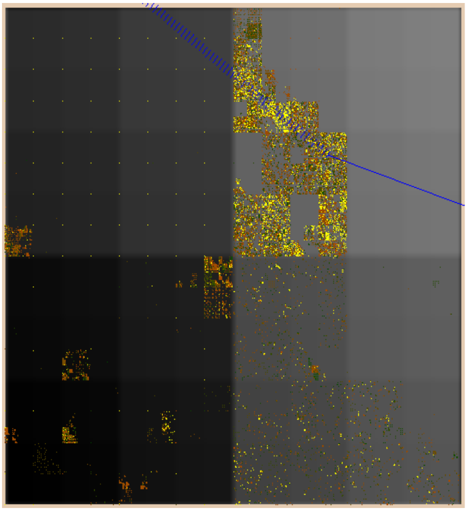


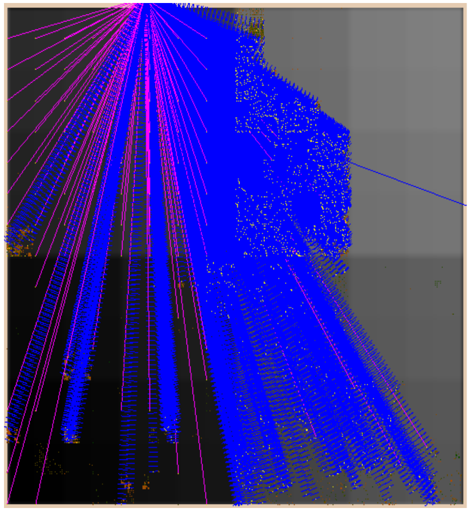
August 14, 2000

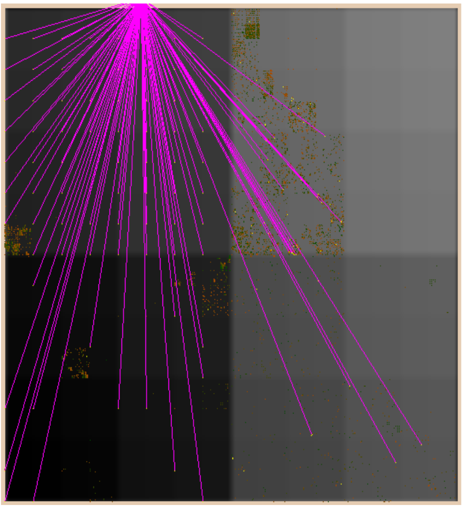
AS-7777 punched hundreds of holes.











EBL-based Analysis

- Which types of “screens” are more interesting and why?
- Why was AS15412 picked for further special examination?
- Under this context, why were we only focusing on April 6-12 and April 18-19?
  - Or, why is April 16 irrelevant?
- Why are April 12 and 18 similar?
- What is the difference between these two instances in April of 2001?

Example #1: AS7332 & AS3669

- Can you investigate the relationship between AS-7332 and AS3669? (BTW, who are they?) And, they have a lot of interesting OASC interactions in 2000.

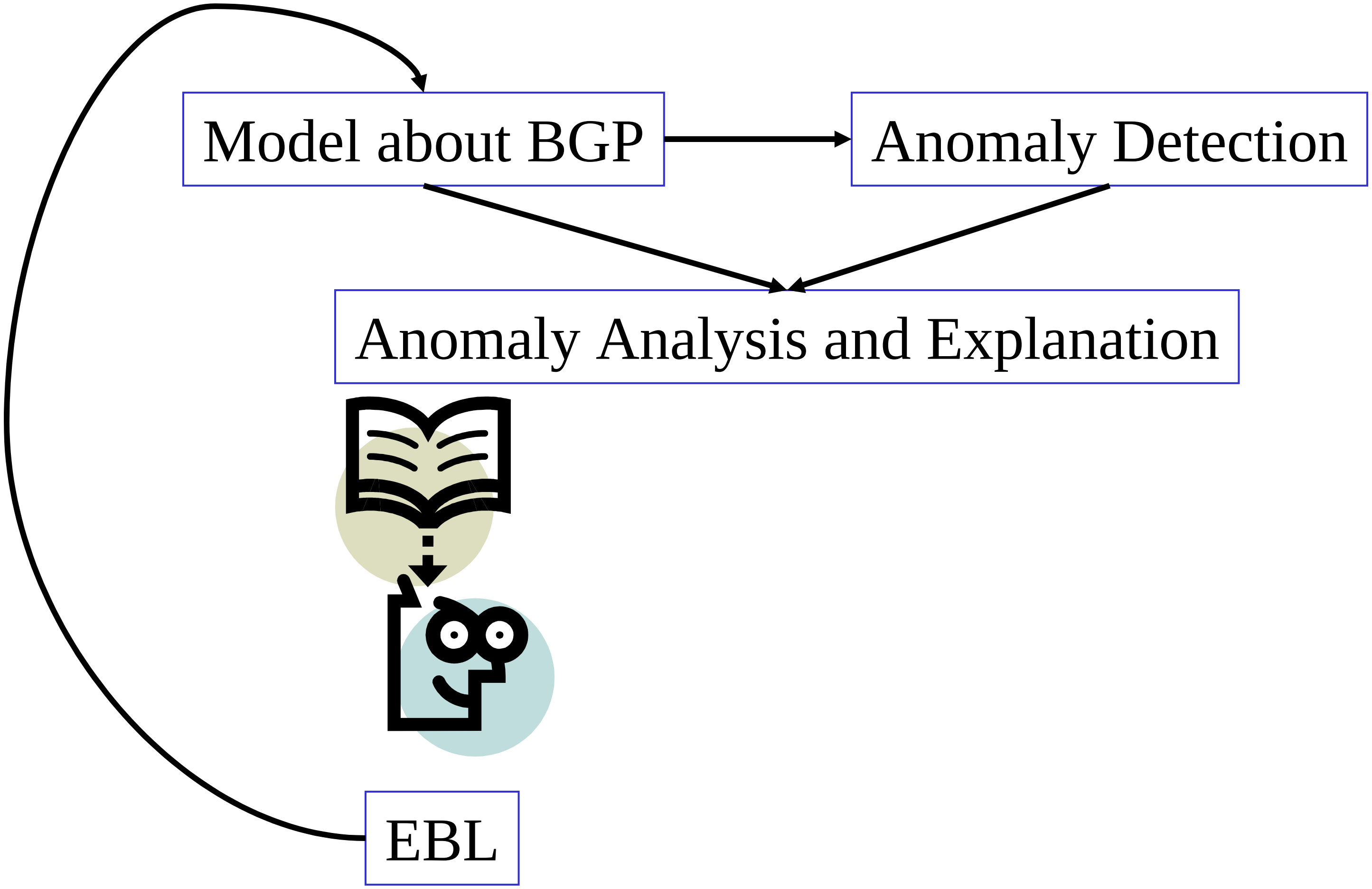
- Both AS3669 and AS7332 belongs to iquest.net.

Example #2: AS-3356

- 403 CSMs 06/18/2003
- 370 CMSs 07/01/2003

- 106 CMSs 10/18/2003
- 105 CSMs 10/19/2003
- 2 CSMs 10/20/2003
- 104 CMSs 10/22/2003

Learning via Anomaly Explanation



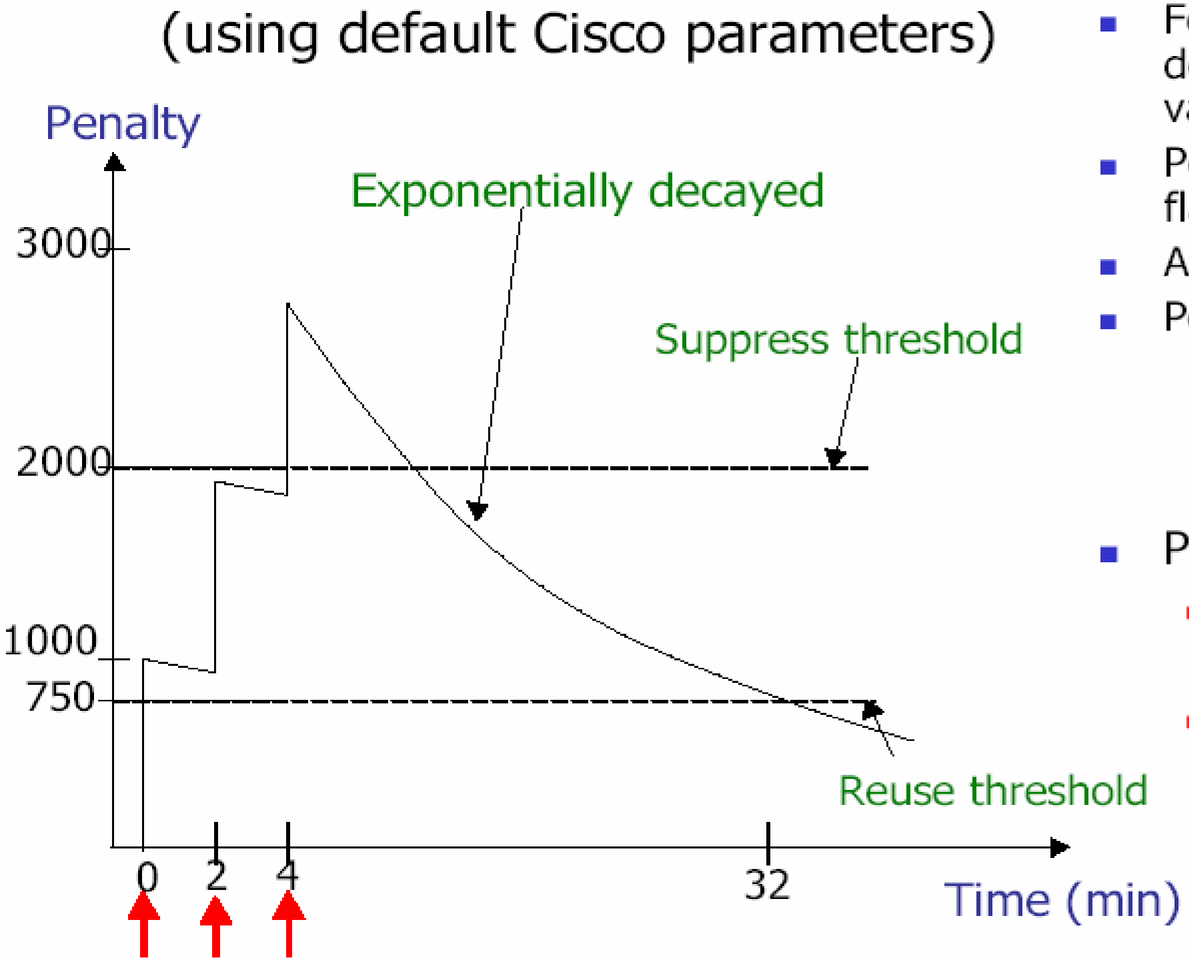
Model about BGP

Anomaly Detection

Anomaly Analysis and Explanation

EBL

Route Flap Damping (RFC 2439)

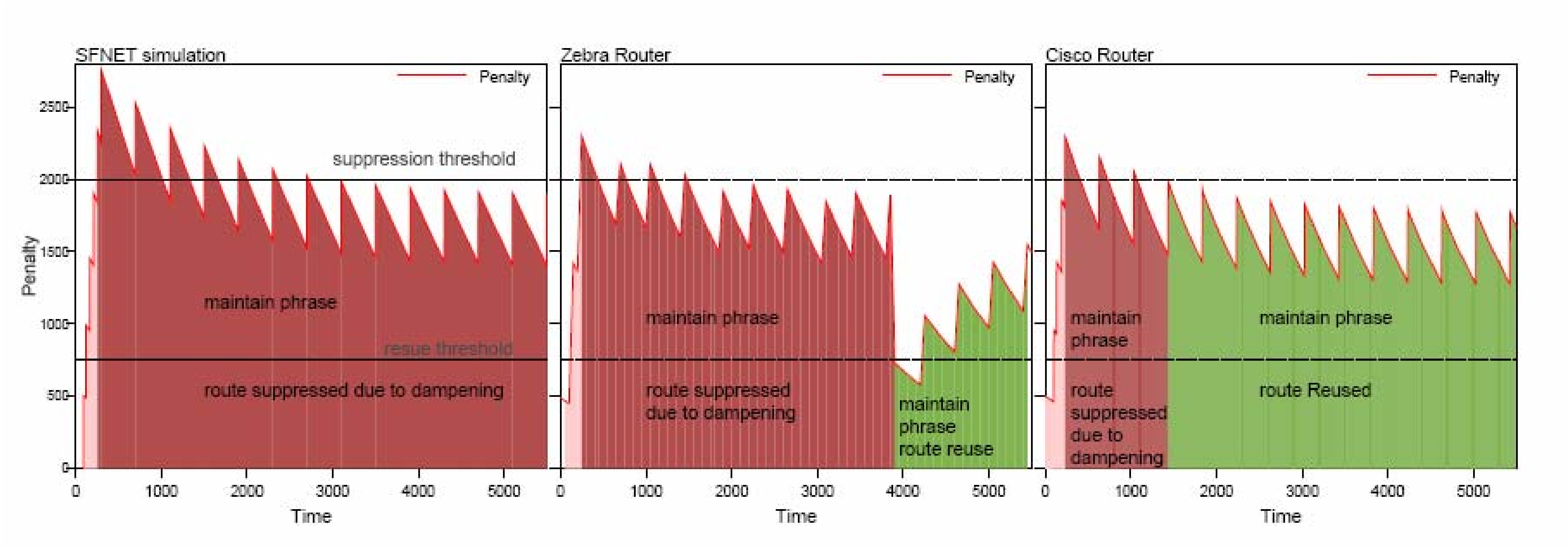


- For each peer, per destination, keep a penalty value
- Penalty increases for each flap
- A flap is a route change
- Penalty decays exponentially

$$P(t') = P(t)e^{-\lambda(t'-t)}$$

- Parameters:
  - Fixed:
    Penalty increment
  - Configurable:
    half-life, suppress-, reuse-threshold, max suppressed time

Different Behaviors



SSFNet **Zebra** **Cisco**

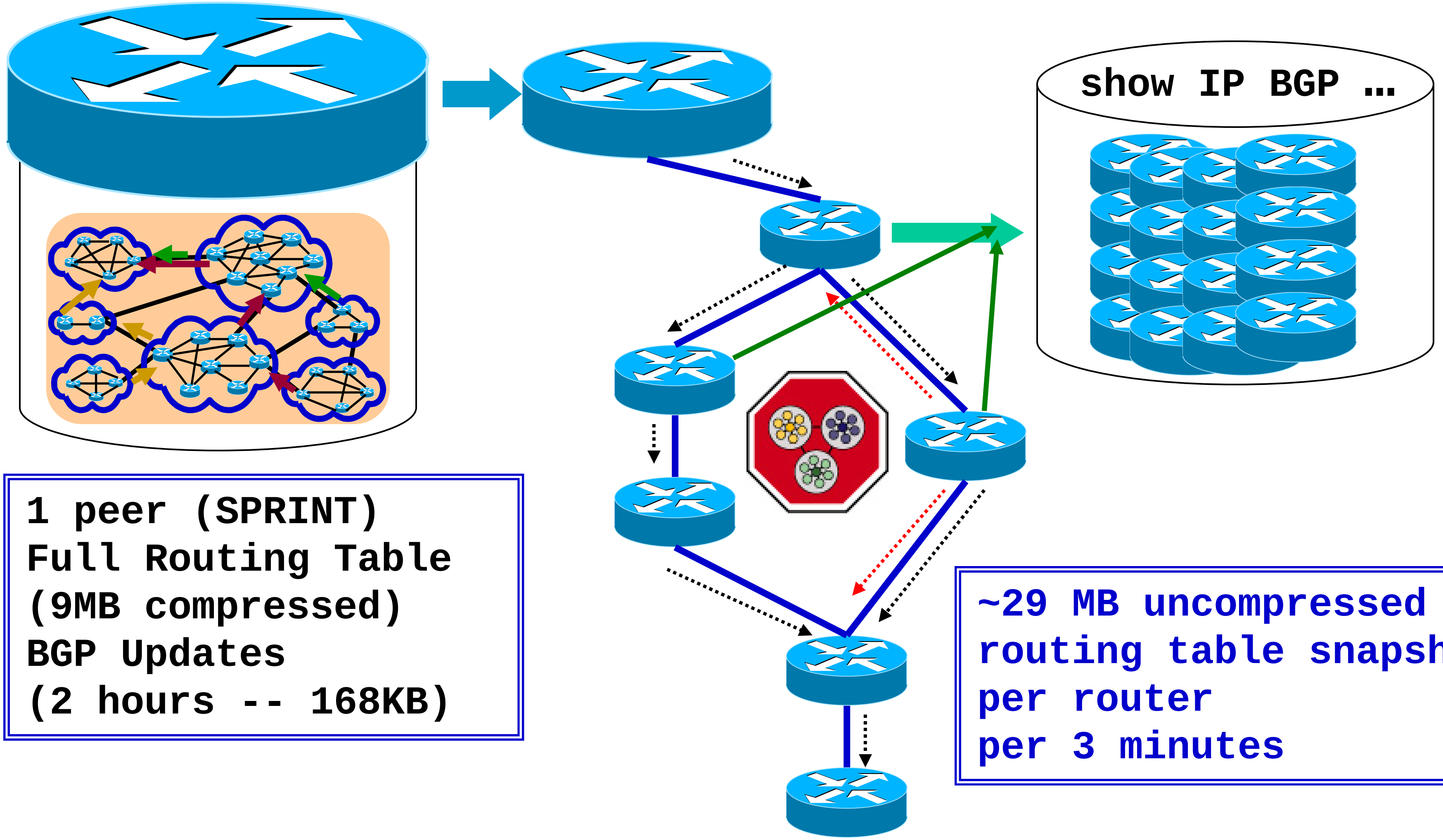
Remarks

Elisha OASC Program/Data(00~04)/Documents:
http://wwwcsif.cs.ucdavis.edu/~tsengs/OASC-Ver-2004-11-02.zip

Just like many other large-scale complex dynamic systems, BGP Anomaly Analysis is indeed very challenging:

Data/Knowledge Information Modeling & Correlation
Visual and Interactive Interface
Data Mining Techniques
Experiments and Simulation

Collecting the Results



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

~29 MB uncompressed
routing table snapshot
per router
per 3 minutes

Real-Time OASC Attack Movie

(per 3-minutes check)

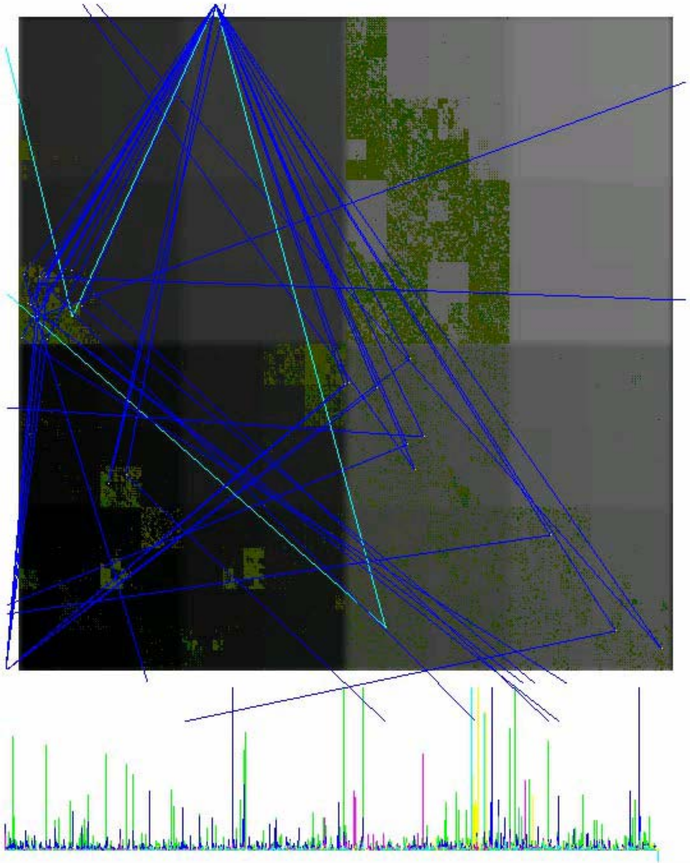
1.5 messages per second

1000 attack messages on

1000 randomly selected prefixes

(1000/136515, ~1%)

```
12.1 .96.2 24 129.30.18.0/24
129. 2.12 24 145.8.160.0/25
146. 180. 5 151.198.60.0/25
152. 44.0. 5 165.254.18.0/25
165. 65.0/ 24 170.76.14.0/25
192. .0/24 192.139.235.0/24
192. 60.1 5 192.197.51.0/25
192. 8.87. 4 192.251.75.0/24
192. /24 25 192.67.53.0/25
192. 92.7 24 192.88.78.0/24
192. /24 193.178.164.0/24
193. 19 5 193.231.4.0/24
193. /24 1 194.102.107.0/25
194. 15.21 4 194.29.205.0/24
194. 95.14 195.232.191.0/25
195. .0/25 5 196.41.205.0/25
196. .184 4 198.175.70.0/25
198.180.150.0/25 198.181.248.0/24 198.182.170.0/24 198.184.0.0/24 198.184.209.0/24 198.186.38.0/25 198.187.236.0/24 198.190.59. 4 198.206.54.0/24
198.212.147.0/25 198.215.2.0/25 198.22.152.0/24 198.22.19.0/25 198.228.90.0/25 198.233.27.0/25 198.234.226.0/24 198.235.29.0/2 25 198.26.28.0/24
198.36.193.0/25 198.4.6.0/24 198.49.44.0/24 198.5.5.0/24 198.50.88.0/25 198.51.254.0/24 198.55.73.0/25 198.59.49.0/25 198.68 25 198.99.67.0/25
199.1.213.0/24 199.10.62.0/25 199.104.108.0/25 199.104.81.0/25 199.107.166.0/24 199.111.17.0/25 199.112.49.0/25 199.121.125.0/2 199.175.157.0/24
199.179.81.0/25 199.185.118.0/24 199.191.34.0/25 199.201.245.0/25 199.212.62.0/24 199.221.80.0/24 199.224.6.0/25 199.229.23.0/25 199.248.177.0/25
199.249.200.0/25 199.249.207.0/24 199.252.34.0/25 199.26.35.0/24 199.29.224.0/25 199.40.205.0/24 199.51.112.0/24 199.51.127 4 199.79.138.0/25
199.80.74.0/24 199.85.5.0/25 199.88.249.0/25 200.10.182.0/24 200.105.54.0/24 200.108.14.0/25 200.12.101.0/25 200.14.11.0/25 2 5 200.23.103.0/25
200.24.5.0/24 200.25.74.0/24 200.27.212.0/25 200.27.22.0/25 200.29.138.0/24 200.30.138.0/25 200.30.195.0/24 200.30.238.0/24 200. 24 200.37.30.0/25
200.39.141.0/25 200.39.159.0/24 200.41.10.0/24 200.41.119.0/25 200.47.46.0/24 200.51.186.0/24 200.53.214.0/25 200.55.197.0/25 200 5 200.69.199.0/25
200.69.30.0/25 200.73.87.0/25 200.75.12.0/24 200.75.72.0/24 200.76.155.0/24 200.76.170.0/25 200.76.186.0/24 200.77.144.0/25 200.8 202.124.171.0/24
202.127.3.0/25 202.128.175.0/25 202.131.129.0/25 202.133.81.0/25 202.134.128.0/25 202.134.138.0/24 202.134.160.0/24 202.14.234 4 202.153.44.0/25
202.154.162.0/24 202.155.56.0/25 202.162.38.0/24 202.165.140.0/25 202.165.70.0/25 202.171.105.0/25 202.177.205.0/25 202.179.133 5 202.27.140.0/24
202.3.227.0/25 202.3.77.0/25 202.40.179.0/25 202.41.70.0/24 202.44.37.0/25 202.51.235.0/24 202.55.143.0/24 202.57.222.0/24 202 24 202.87.87.0/25
202.88.142.0/25 202.9.229.0/25 202.94.92.0/25 203.1.248.0/24 203.10.216.0/24 203.118.186.0/25 203.12.64.0/25 203.12.69.0/25 5 203.135.36.0/24
203.14.36.0/24 203.14.91.0/25 203.157.14.0/24 203.157.81.0/25 203.176.1.0/24 203.187.199.0/25 203.193.129.0/25 203.196.227.0 203.232.108.0/25
203.233.85.0/25 203.234.105.0/24 203.234.41.0/25 203.234.65.0/25 203.234.81.0/25 203.24.95.0/25 203.249.147.0/24 203.252.210 5 203.34.141.0/25
203.5.121.0/25 203.55.179.0/25 203.55.44.0/24 203.56.107.0/24 203.6.244.0/24 203.77.205.0/24 203.8.94.0/25 203.82.44.0/25 203.83. 24 203.98.85.0/25
204.116.21.0/25 204.119.0.0/25 204.126.166.0/25 204.126.240.0/25 204.130.139.0/24 204.141.229.0/25 204.142.70.0/25 204.146.60.0 204.209.158.0/24
204.209.164.0/24 204.213.141.0/24 204.213.147.0/24 204.213.159.0/24 204.213.27.0/24 204.214.98.0/24 204.222.167.0/25 204.225.11 5 204.27.238.0/25
204.34.12.0/25 204.44.12.0/25 204.44.17.0/24 204.48.118.0/25 204.52.210.0/24 204.59.80.0/24 204.75.199.0/24 204.86.207.0/2 205.144.65.0/24
205.145.61.0/25 205.152.245.0/25 205.156.31.0/25 205.159.16.0/24 205.159.239.0/25 205.160.215.0/25 205.162.207.0/25 205 205.211.129.0/25
205.214.213.0/25 205.218.252.0/24 205.219.177.0/24 205.235.115.0/25 205.236.65.0/24 205.240.67.0/24 205.66.120.0/24 205.70.9.0/ 206.165.240.0/24
206.167.63.0/24 206.168.220.0/24 206.18.60.0/24 206.182.132.0/25 206.183.134.0/24 206.183.158.0/25 206.217.178.0/25 206.218.17 4 206.96.227.0/25
207.102.227.0/25 207.106.84.0/25 207.112.157.0/25 207.117.36.0/24 207.139.37.0/25 207.156.200.0/24 207.162.225.0/25 207. 207.206.195.0/25
207.215.205.0/25 207.218.177.0/25 207.226.243.0/25 207.228.151.0/24 207.231.72.0/24 207.248.200.0/25 207.248.59.0/24 207.25.12 4 207.86.249.0/25
208.10.217.0/25 208.10.25.0/24 208.146.159.0/25 208.15.138.0/25 208.155.27.0/25 208.16.20.0/24 208.16.74.0/24 208.186.200. 5 208.47.112.0/24
208.47.225.0/24 208.49.164.0/24 208.52.86.0/24 208.54.201.0/25 208.57.14.0/24 208.57.172.0/24 208.57.240.0/25 208.57.51.0/ 209.149.181.0/24
209.149.199.0/24 209.149.239.0/25 209.149.247.0/24 209.150.78.0/25 209.159.232.0/24 209.162.226.0/24 209.162.250.0/24 20 209.185.175.0/24
209.186.217.0/25 209.213.214.0/24 209.214.38.0/24 209.215.168.0/24 209.215.198.0/24 209.215.248.0/25 209.215.71.0/25 209 209.251.243.0/25
209.41.207.0/24 209.41.226.0/25 209.5.126.0/25 209.71.7.0/24 209.74.227.0/24 209.83.173.0/25 210.105.69.0/24 210.114.108.0/2 5 210.184.96.0/24
210.210.5.0/24 210.214.7.0/24 210.51.232.0/24 210.53.39.0/25 210.56.23.0/25 210.9.134.0/25 210.96.160.0/25 211.100.27.0/25 211.220.214.0/25
211.229.145.0/24 211.232.254.0/24 211.36.224.0/25 211.4.243.0/24 211.50.56.0/25 212.100.220.0/24 212.106.83.0/25 212.116.152 5 212.98.148.0/25
213.130.12.0/25 213.133.223.0/25 213.143.57.0/25 213.152.93.0/24 213.166.13.0/25 213.190.81.0/24 213.207.147.0/25 213.228.24 25 214.3.169.0/24
214.3.74.0/24 214.3.83.0/25 214.4.138.0/24 216.107.104.0/24 216.109.106.0/24 216.109.15.0/25 216.110.115.0/25 216.115.168.0/24 5 216.138.89.0/24
216.145.89.0/25 216.147.155.0/24 216.148.248.0/24 216.150.89.0/25 216.158.86.0/25 216.176.39.0/24 216.200.108.0/25 216.206.132.0 216.252.182.0/24
216.47.254.0/24 216.47.255.0/25 216.54.187.0/25 216.60.234.0/24 216.69.3.0/24 216.72.125.0/24 216.76.181.0/25 216.76.96.0 5 217.169.43.0/24
217.171.103.0/25 217.20.163.0/24 217.21.50.0/24 217.22.115.0/24 217.26.168.0/25 217.27.48.0/25 217.65.66.0/25 217.79.75.0/2 4 24.106.136.0/25
24.117.180.0/25 24.117.82.0/24 24.119.252.0/25 24.119.94.0/24 24.154.217.0/24 24.154.32.0/24 24.154.76.0/25 24.204.37.0/24 2 0/25 40.0.40.0/24
61.11.236.0/24 61.183.1.0/24 61.250.88.0/24 61.252.65.0/24 61.81.105.0/24 61.95.224.0/24 61.95.244.0/25 62.100.130.0/25 62.22 4 63.108.136.0/24
63.110.36.0/25 63.118.247.0/24 63.121.135.0/24 63.122.89.0/25 63.144.255.0/24 63.160.157.0/24 63.164.114.0/24 63.165.42.0/24 63.170.119.0/24 63.170.145.0/25 63.170.161.0/25 63.171.232.0/25 63.173.163.0/25 63.192.141.0/24 63.215.129.0/25 63.223.1.0/25
63.223.3.0/24 63.72.61.0/25 63.84.187.0/24 63.84.48.0/24 63.85.236.0/24 63.95.22.0/24 63.97.179.0/24 64.110.74.0/25 64.117.145.0/25 64.132.202.0/24 64.134.184.0/25 64.134.3.0/24 64.139.86.0/25 64.154.26.0/24 64.163.11.0/24 64.174.7.0/24 64.178.221.0/25
64.200.238.0/24 64.201.181.0/25 64.208.51.0/25 64.232.80.0/25 64.241.64.0/25 64.251.28.0/25 64.251.3.0/24 64.46.68.0/24 64.49.46.0/25 64.6.1.0/25 64.63.245.0/25 64.68.5.0/25 64.76.151.0/25 64.76.88.0/24 64.86.249.0/24 64.90.27.0/25 64.94.188.0/25
64.95.215.0/25 64.95.225.0/25 64.95.234.0/25 64.95.31.0/25 65.112.189.0/24 65.124.123.0/25 65.124.23.0/25 65.147.147.0/25 65.161.45.0/24 65.162.23.0/25 65.167.225.0/25 65.169.157.0/25 65.170.79.0/24 65.171.50.0/25 65.174.225.0/24 65.194.98.0/25
65.196.8.0/25 65.197.36.0/25 65.197.39.0/24 65.199.174.0/24 65.204.179.0/25 65.205.191.0/24 65.207.50.0/24 65.208.230.0/25 65.218.237.0/24 65.222.125.0/25 65.223.249.0/25 65.23.112.0/24 65.240.61.0/24 65.241.71.0/25 65.247.181.0/24 65.43.51.0/24
65.74.193.0/24 65.77.29.0/25 65.90.55.0/25 66.102.111.0/24 66.112.62.0/25 66.126.188.0/24 66.13.126.0/25 66.13.218.0/24 66.13.73.0/24 66.133.10.0/24 66.133.17.0/24 66.134.62.0/25 66.135.251.0/24 66.15.191.0/25 66.15.95.0/25 66.150.190.0/24
```



Acknowledgements

- DARPA FNIISC (UCLA, USC-ISI, NCSU, UCDavis)
  - Lixia Zhang, Allison Mankin, Dan Massey and others
- NSF/DHS DETER/EMIST
  - Chen-Nee Chuah, Ke Zhang, Shih-Ming Tseng, Soon-Tee Teoh (UC Davis), Sandra Murphy (SPARTA), Sonia Fahmy (Purdue), Patrick McDaniel (Penn. State Univ.)
- NIST BGP-SSFNet
- Many others….