UNIVERSITÀ DEGLI STUDI ROMA TRE
Dipartimento di Informatica e Automazione

Measuring and Visualizing Inter-domain Routing Dynamics with BGPATH

Luca Cittadini
Tiziana Refice
Alessio Campisano
Giuseppe Di Battista
Claudio Sasso

IEEE Symposium on Computers and Communications (ISCC 2008)
Jul 8th, 2008

Outline

- Motivations
- Goals
- Basic ideas
- Analyze a route change using BGPath
- Stream-based computation
- Conclusions and future work

Motivations

- Policy routing
  - Flexibility
  - Fault prone, difficult to debug, …
- Monitoring and data collection
  - Distributed and publicly available monitors
  - Historical repositories (*RIS, RV*)
  - Huge amount of data
- Semi-automatic analysis tools
  - Internet-wide (*LinkRank*, [NOMS'04])
  - ISP-oriented (*BGPlay*, [GD'03], *Cyclops* [SIGCOMM'06])

Goals

- Provide the user with valuable information about inter-domain routing dynamics, in order to help detection and analysis of network events
  - Define metrics to describe inter-domain routing behavior
  - Compute metric on huge amount of input BGP data, fulfilling near real time constrains
  - Visualize computed values to easily detect inter-domain routing events
- Bridge the gap between Internet-wide and ISP-oriented approaches

Basic ideas

In theory… [NOMS'08]

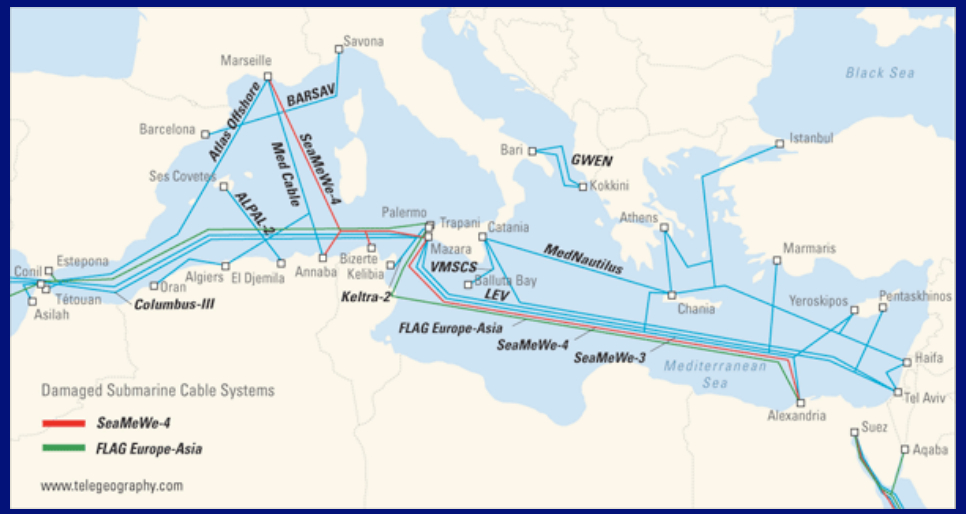
- Collect data from many monitors
- Evaluate data source reliability, in order to filter out data collection 'noise'
- Model inter-domain routing dynamics in terms of 'usage' of inter-domain links over time for *all the routed prefixes*
- Analyze inter-domain routing of *user-defined prefix*, in order to identify network events affecting it

Basic ideas
… in practice [ISCC'08]

- *Efficient* algorithms and implementations to compute data source reliability and link usage
  - Huge amount of data (BGP updates)
    - **~2** GB/day, **~50M** updates/day
    - **~100K** inter-domain links, **~250K** prefixes, **~800** monitors
  - Need for nearly real-time information, to detect and analyze inter-domain routing outages
- *Effective* visualization of inter-domain information (raw and computed)
  - Multidimensional data (time, topology, monitors, prefixes)

Analyze a route change using BGPath

- *Use case:*
  - Fiber cuts in the Mediterranean Sea
  - Outage period: 01/23-02/14, 2008

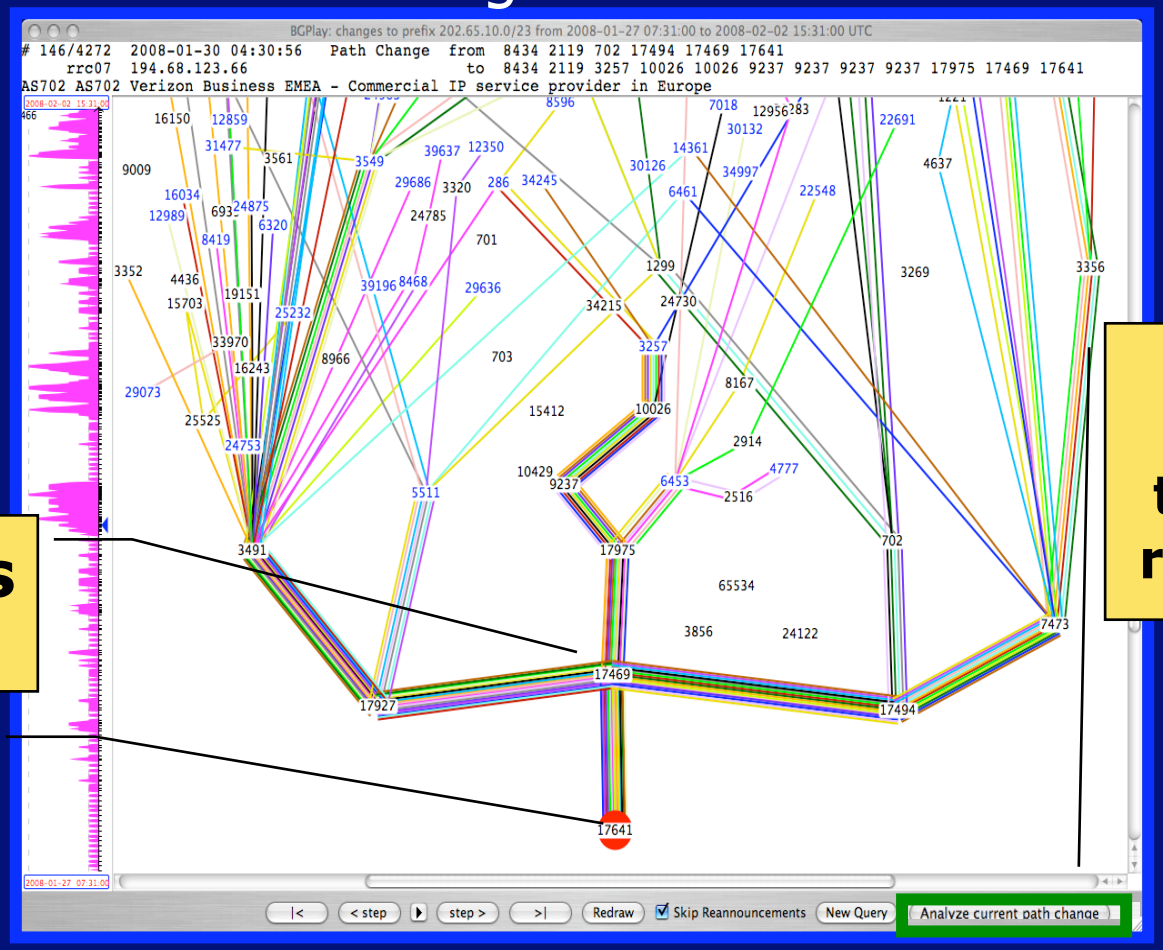


Let's focus on

- SEA-ME-WE-4 cable cut
- as observed by **AS17641** (Infotech, BD), which originates **202.65.10.0/23**

Input: a route change

- BGPath integrates with BGPlay, in order to graphically select a BGP route change

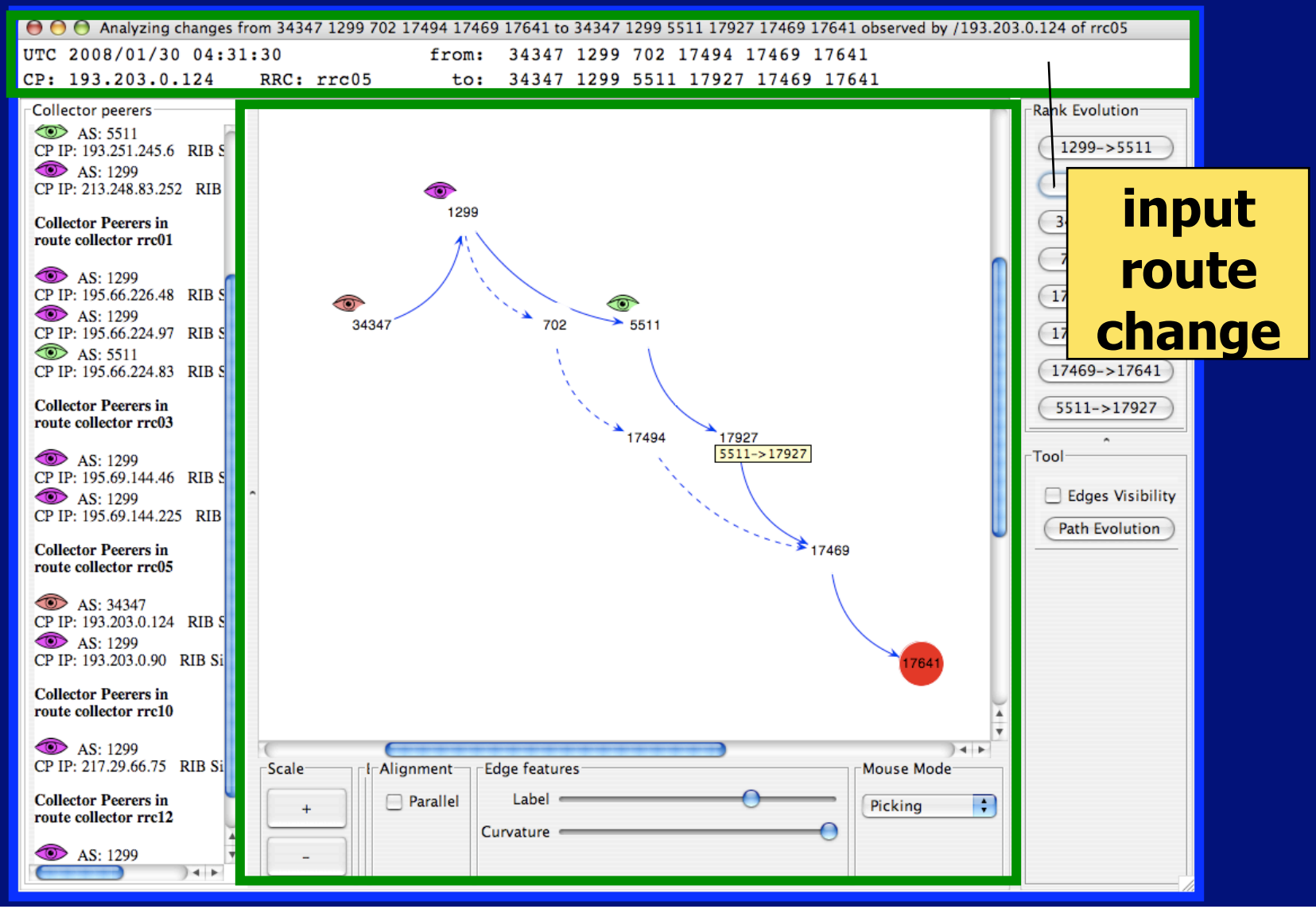


Infotech's upstream

Infotech

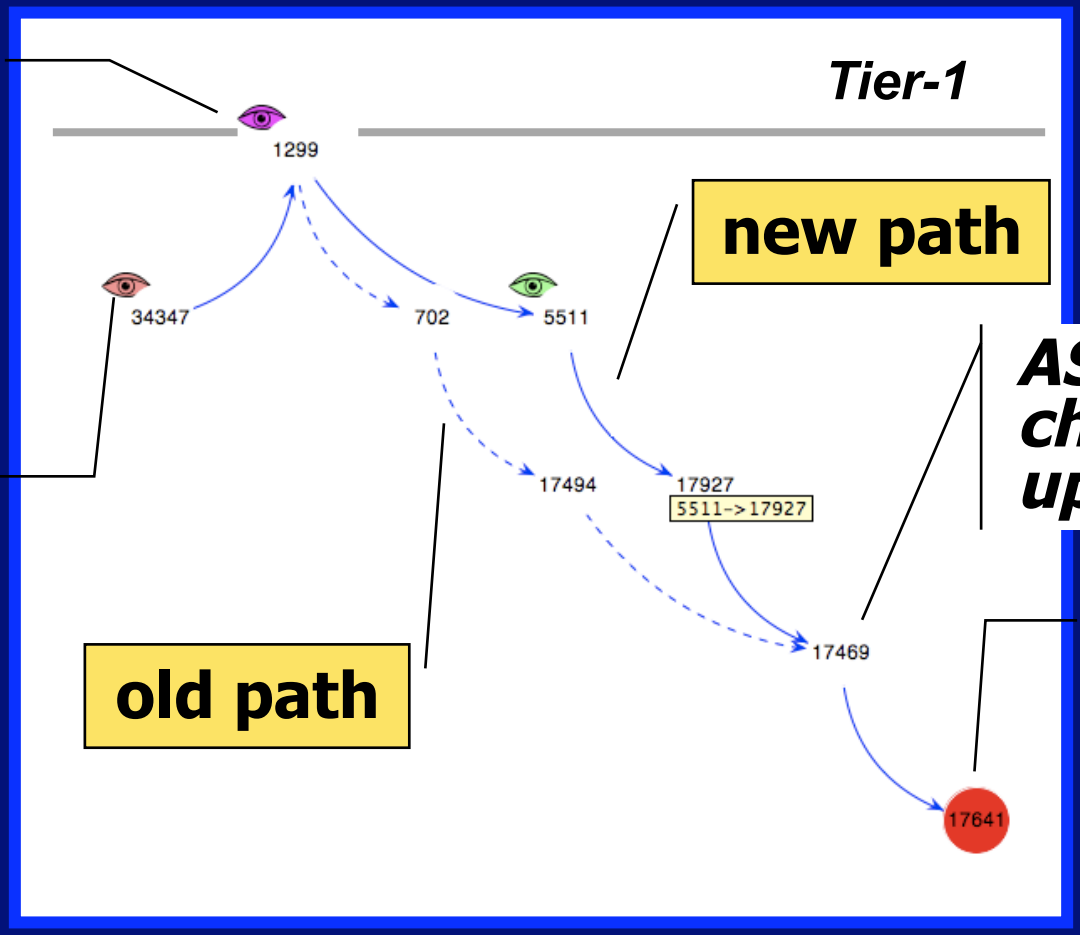
Launch BGPath on the selected route change

BGPath - overview

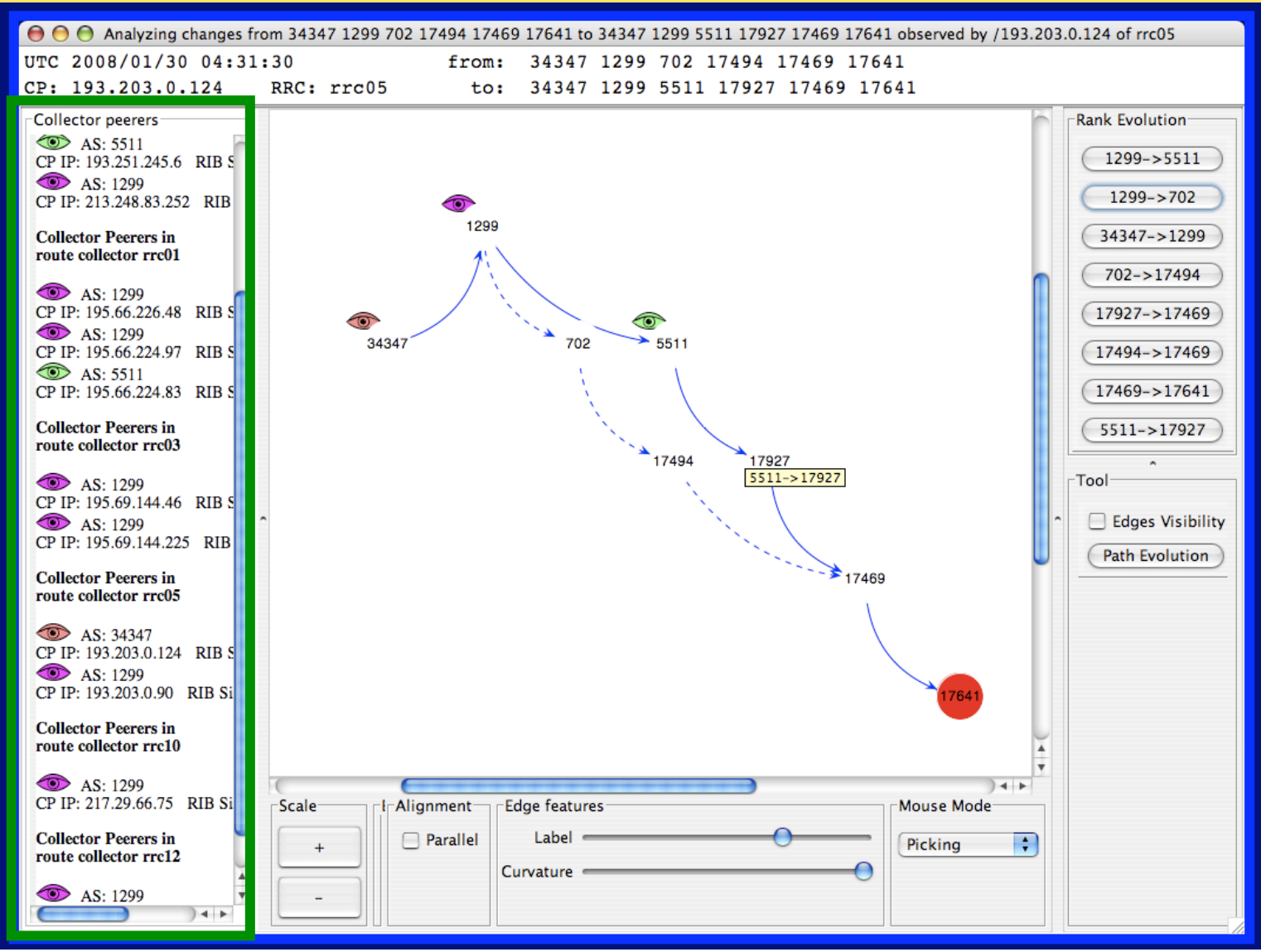


Customer-provider hierarchy

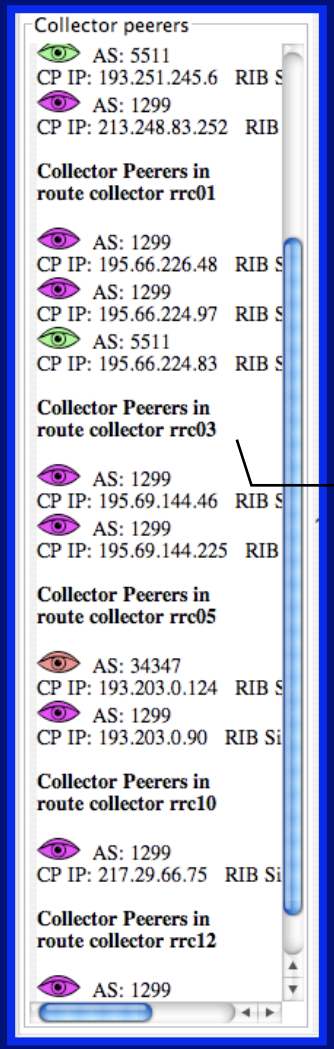
- Place the route change in the Internet hierarchy, in order to assess the impact of the change on the network



BGPath - overview



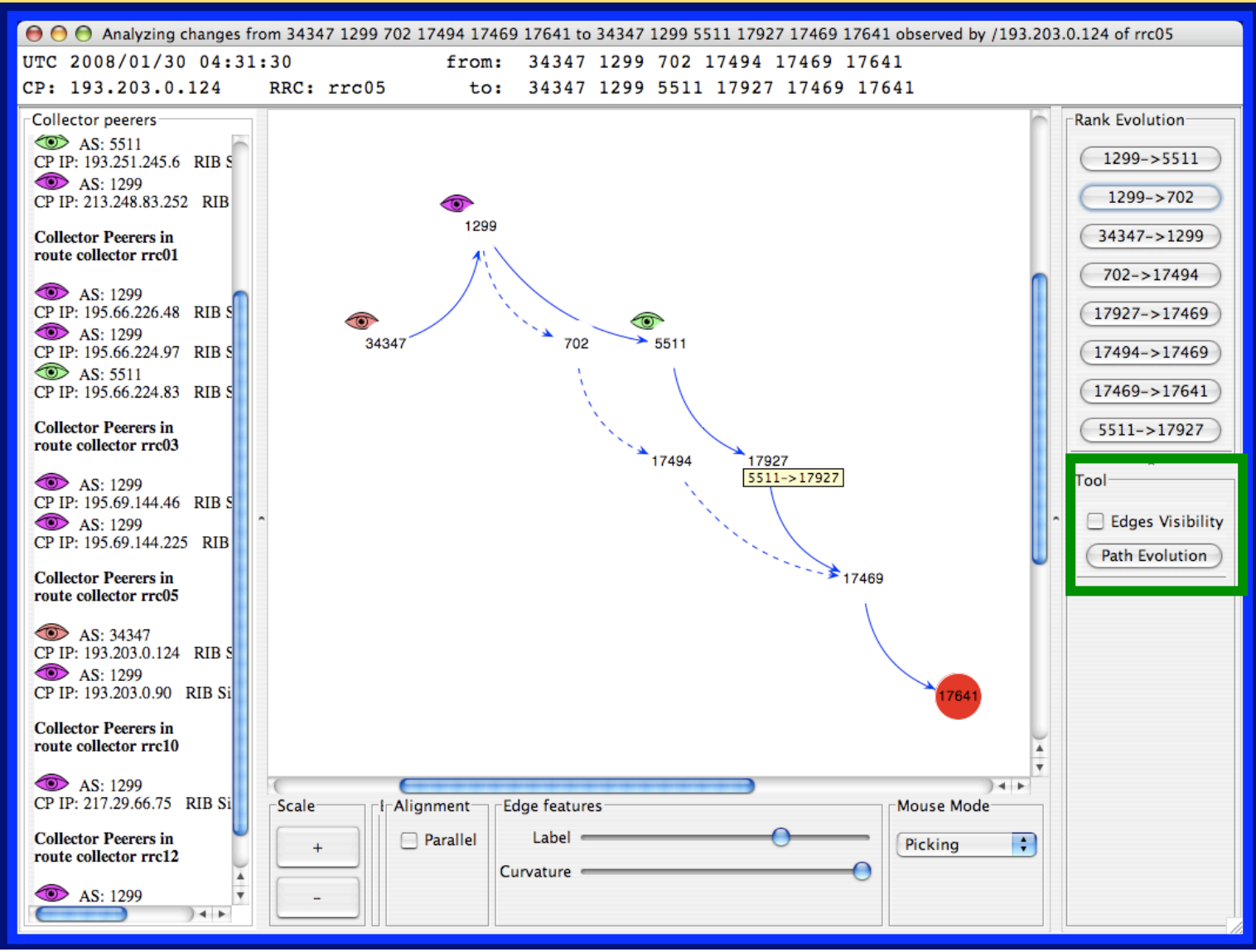
Monitor resets



- Infer resets of connections between any monitor and the collection system, in order to identify unreliable data sources

All the monitors with routes towards 202.65.10.0/23

BGPath - overview

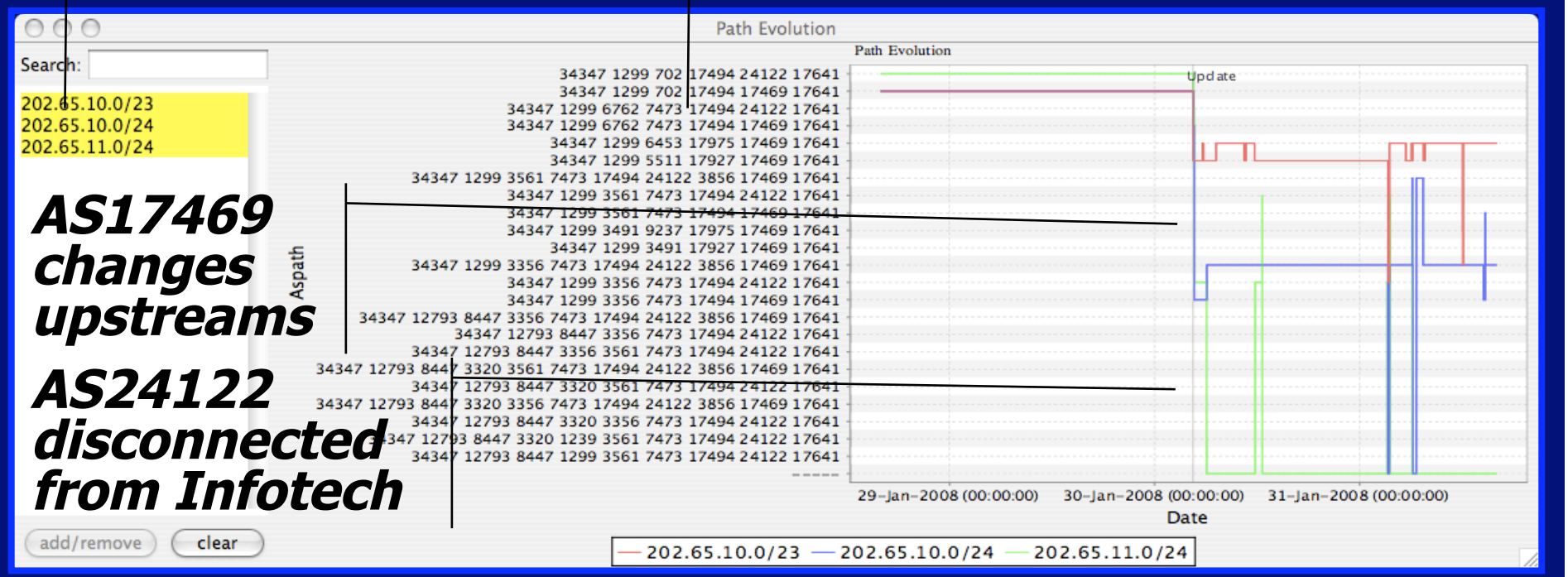


AS-path evolution

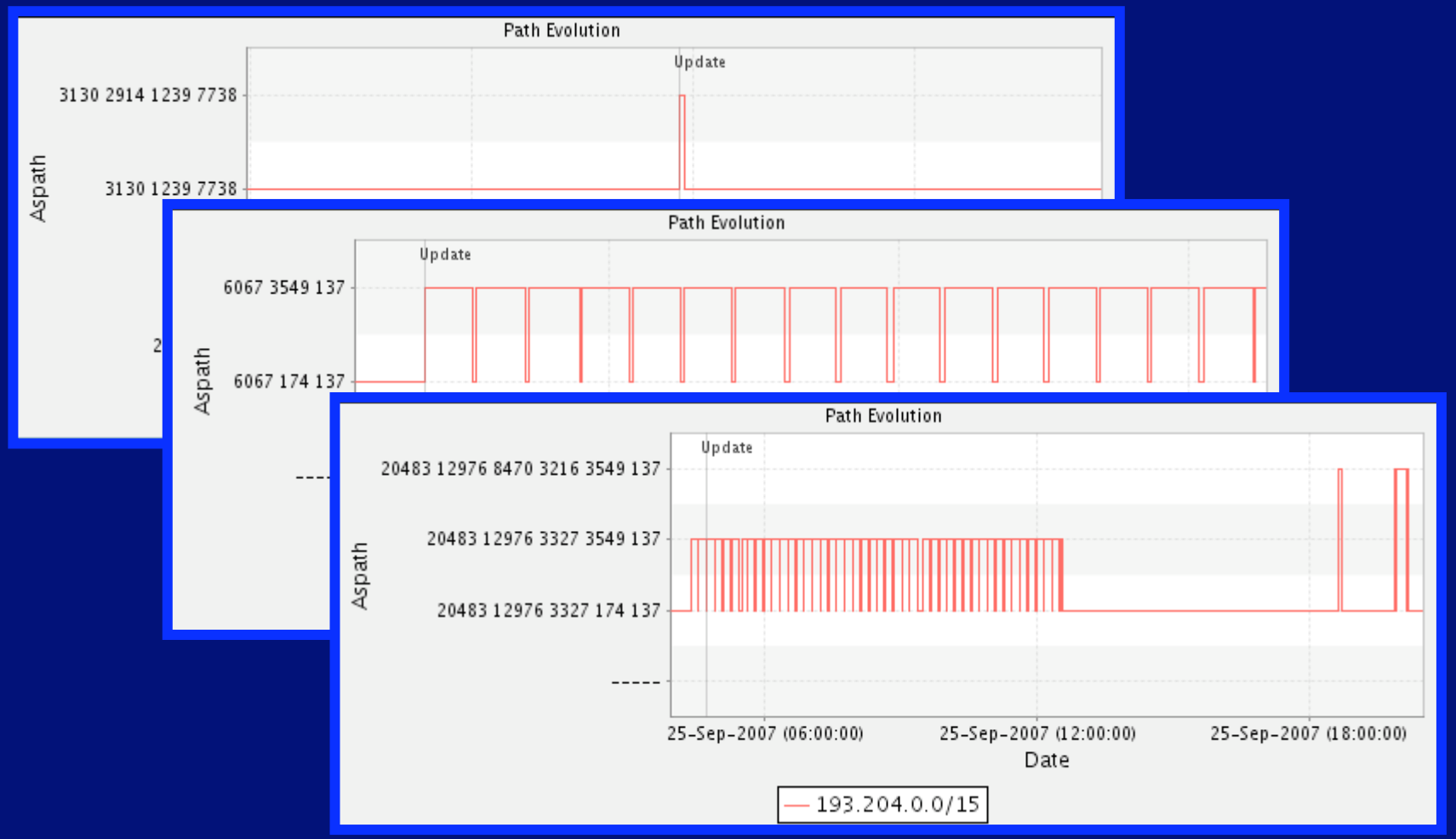
- Plot the AS paths of prefixes over time, in order to help identify patterns in routing dynamics

prefixes originated by Infotech

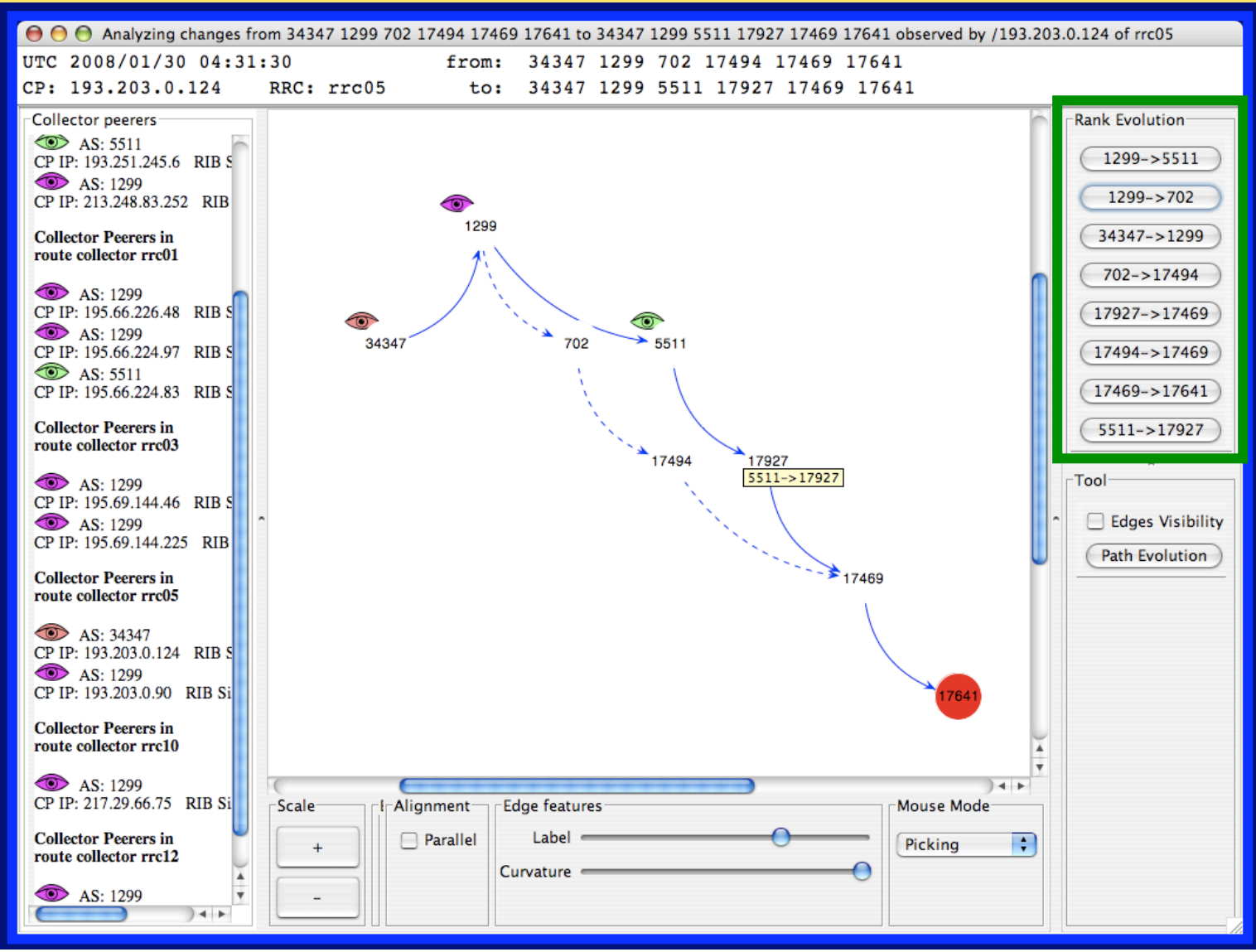
AS-paths from Infotech to CNH



AS-path evolution in the wild

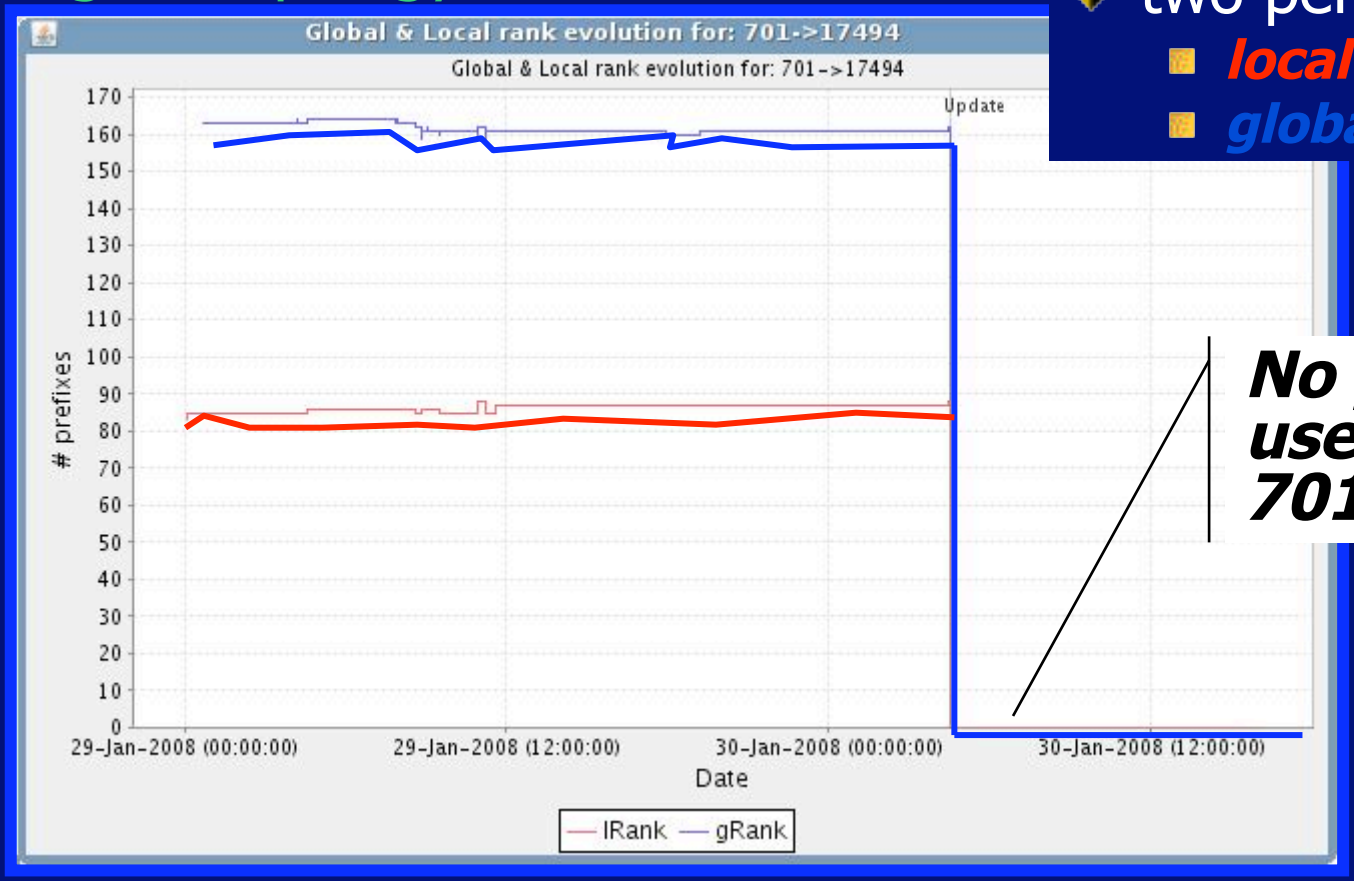


BGPath - overview



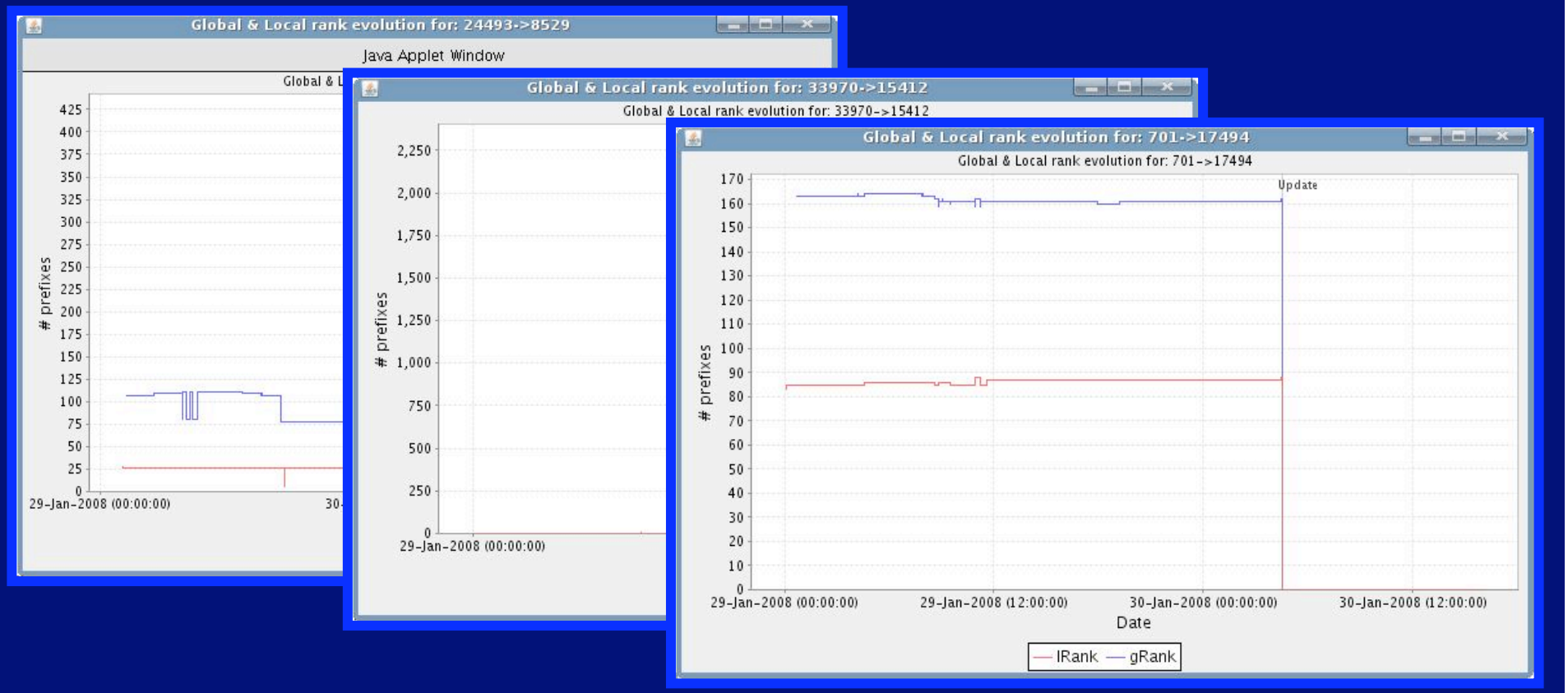
‘Usage’ of inter-domain links

- Measure the # prefixes through inter-domain links, in order to pinpoint macro events affecting physical and/or logical topology
  - two perspectives:
    - ***local*** : one monitor
    - ***global*** : all monitors

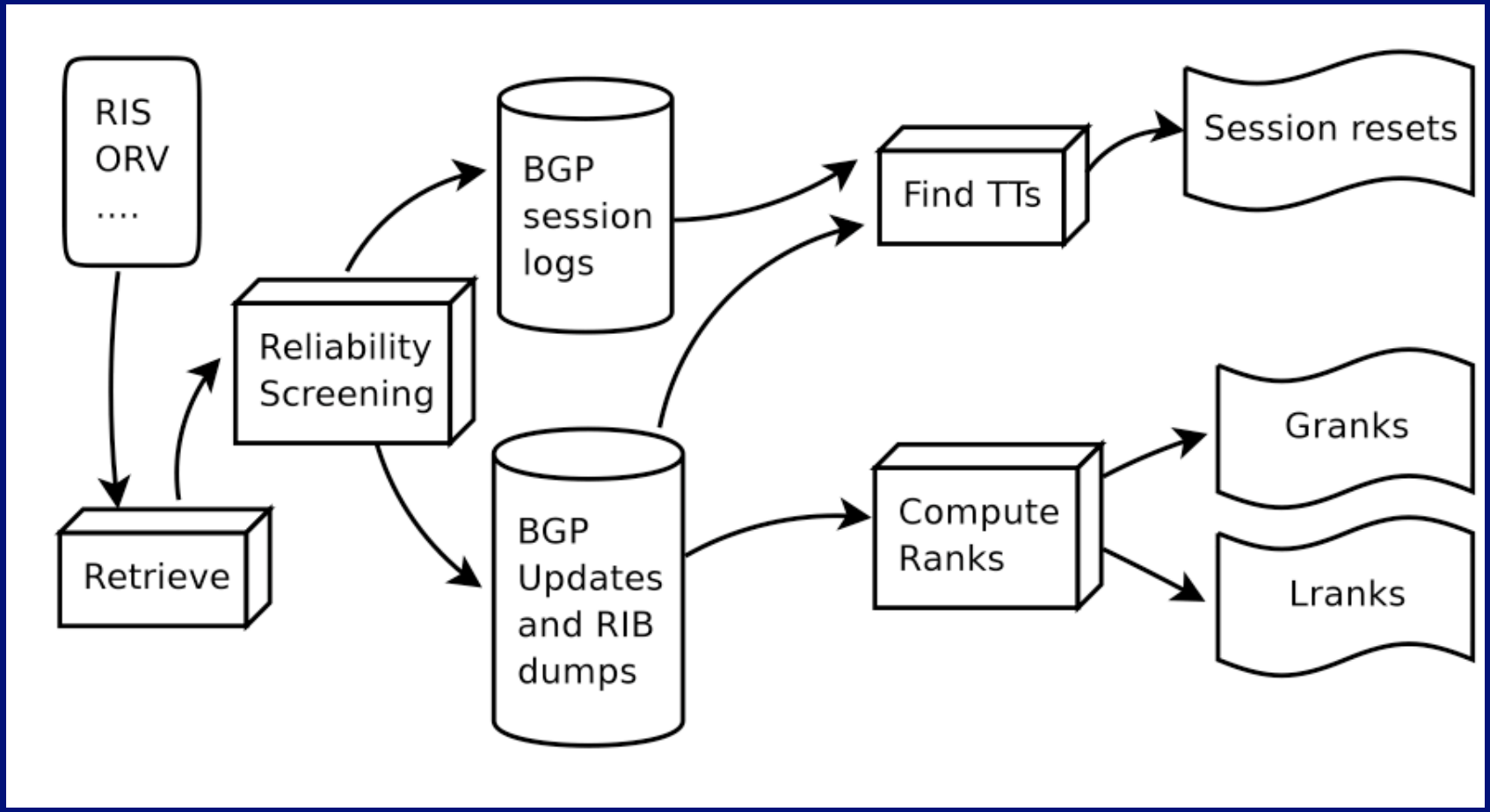


No prefixes use AS-link 701-17494

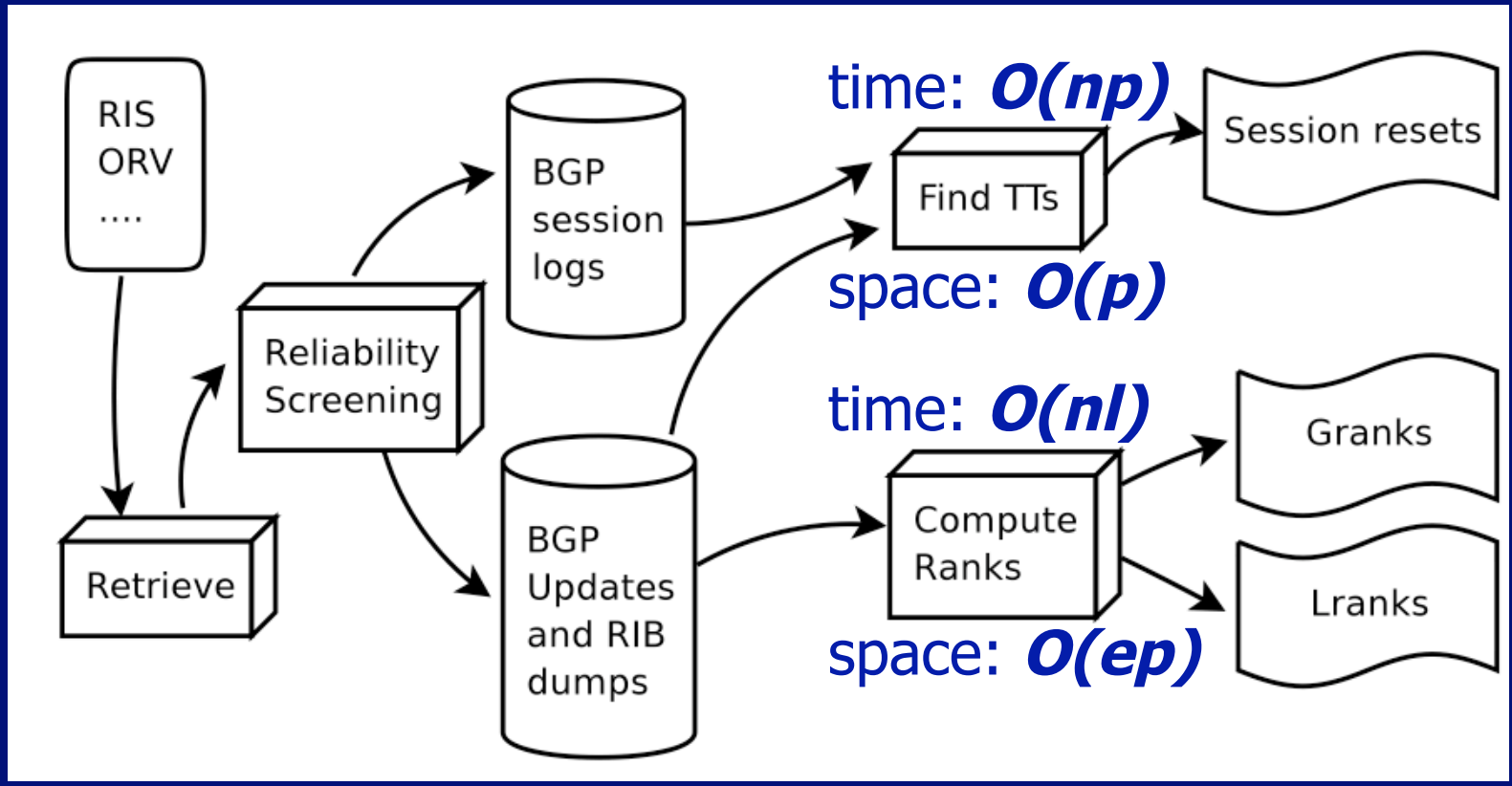
‘Usage’ of inter-domain links in the wild



Stream-based approach

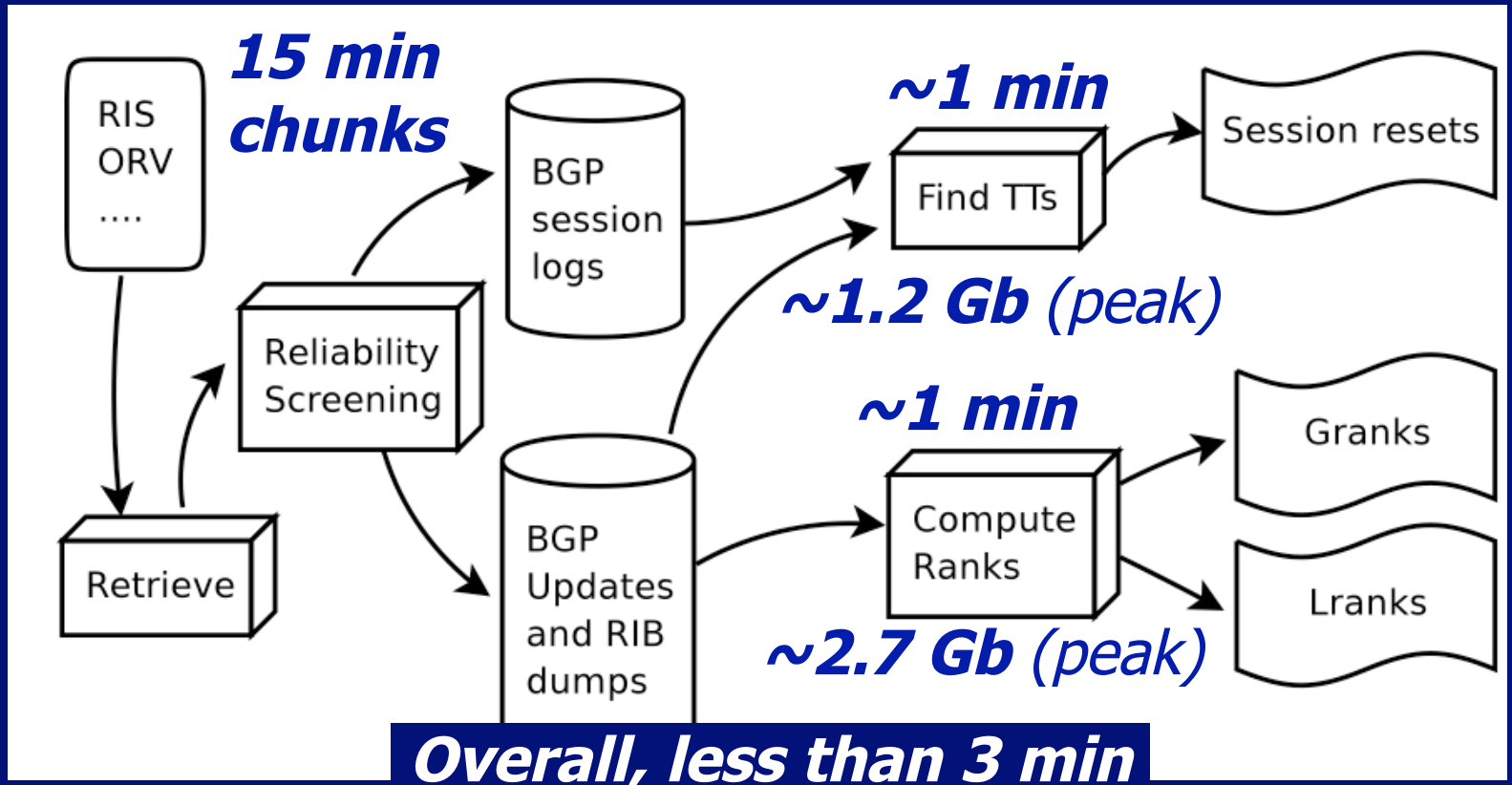


Time and space complexity



n: # route changes (~50M/d)
p: # all known prefixes (250k)
l: max AS-path length (~7)
e: # edges (~100k)

Time and space performance



Nearly real-time computation

Conclusions

- **BGPath**, publicly available system with
  - Global and ISP view of routing dynamics
  - *Efficient* computation of data source reliability and inter-domain link usage
  - *Effective* graphical visualization of fine grained and aggregated information about user-specified route changes
- Already extensively used to analyze
  - Mediterranean fiber cuts (Jan 2008)
  - Hijacking of the YouTube prefix by Pakistan Telekom (Feb 24th 2008)

Future work

- Extend BGPath's user interface with additional routing information
- Define new metrics, in order to better model inter-domain routing dynamics
- Deploy pattern recognition modules, in order to automatically pinpoint network events and their root causes
- Further BGP forensic analyses