Hasso Plattner Institut

IT Systems Engineering | Universität Potsdam

Measuring BGP propagation using correlated spikes

Andrey Sapegin

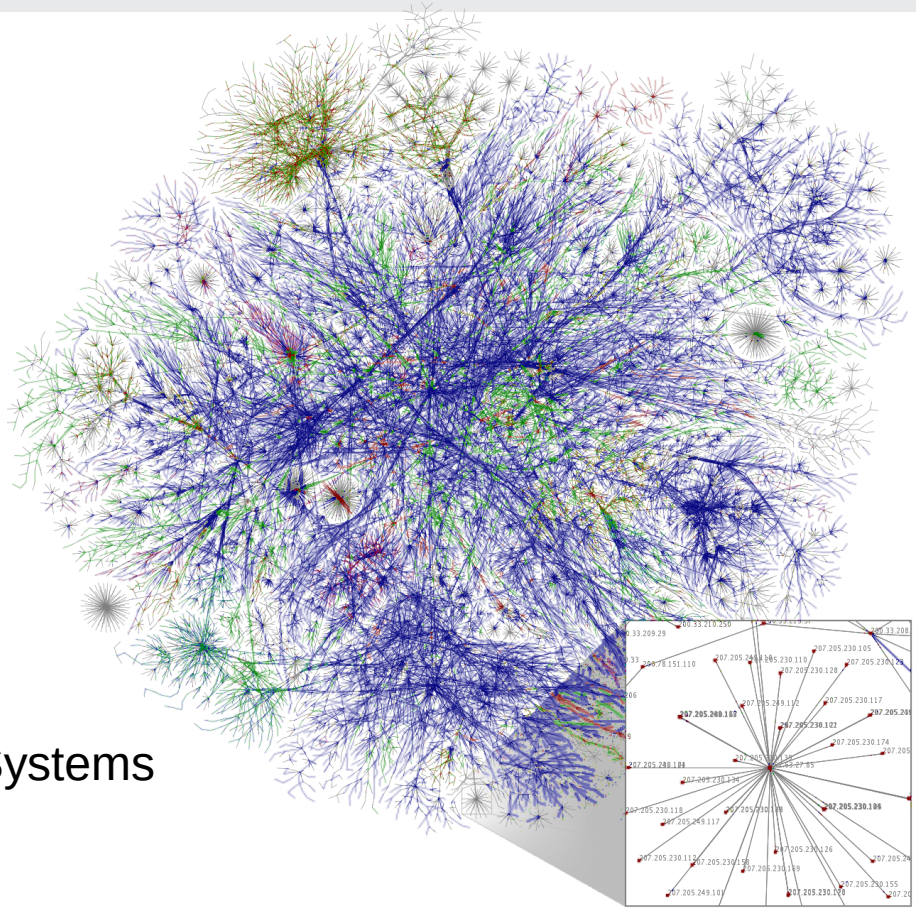
Chair "Internet Technologies and Systems"
Hasso Plattner Institute
University of Potsdam

BGP: Internet core routing protocol

> 500,000 networks

> 65,000 Autonomous Systems

~ 180,000 links between Autonomous Systems



[1]

How scalable is BGP?

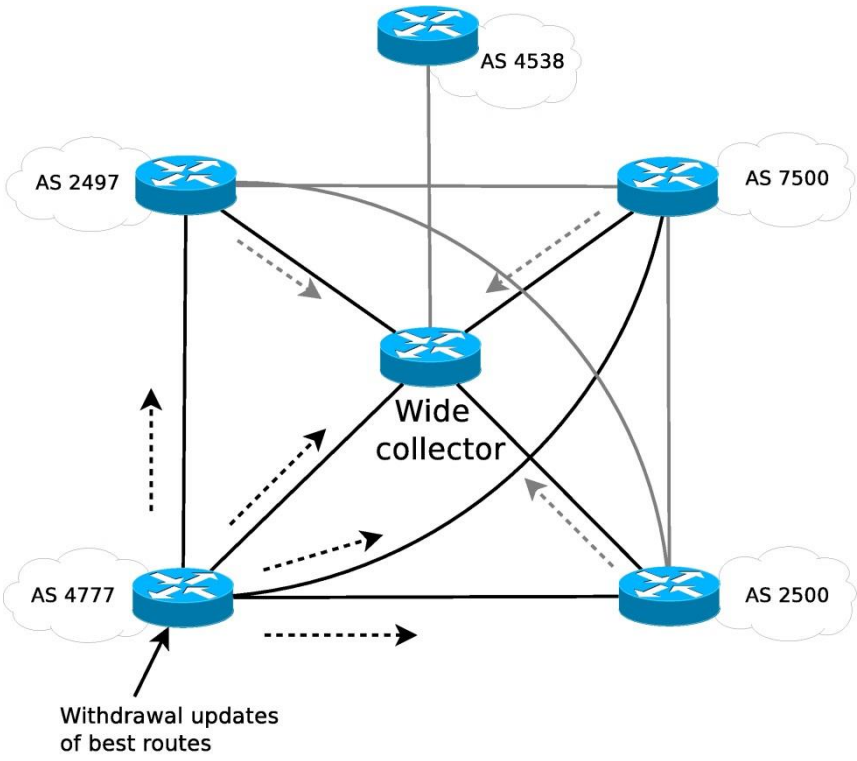
Internet grows:

- IPv6
- 4-byte AS numbers
- network virtualisation
- peering links between ISPs

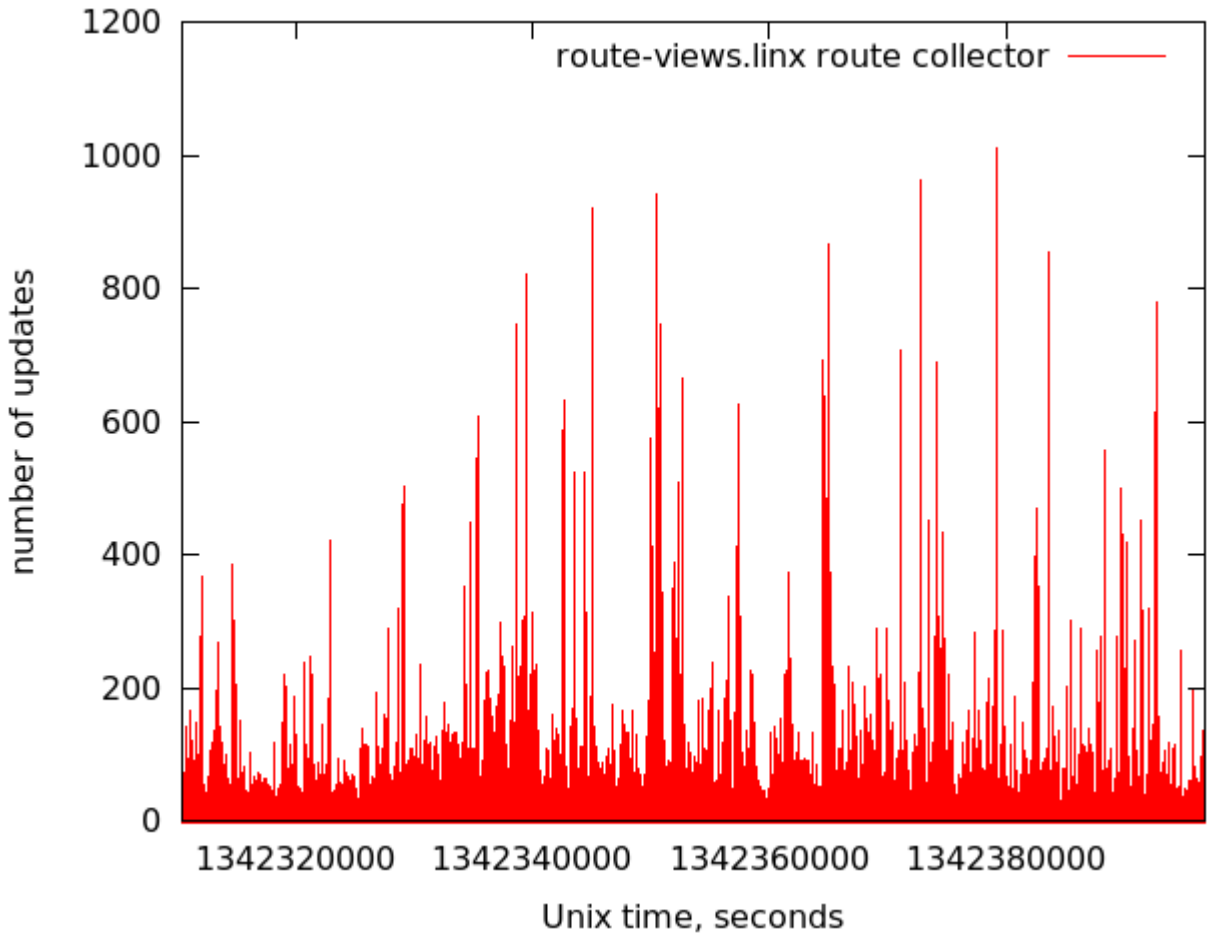
BGP works since early 90-es

How BGP works

- BGP Routers exchange update messages
- Routers send **only** changes of **best** routes to each other
- Updates contain Autonomous Systems Path to avoid loops, but does not contain information about **what and where** happened in the Internet topology

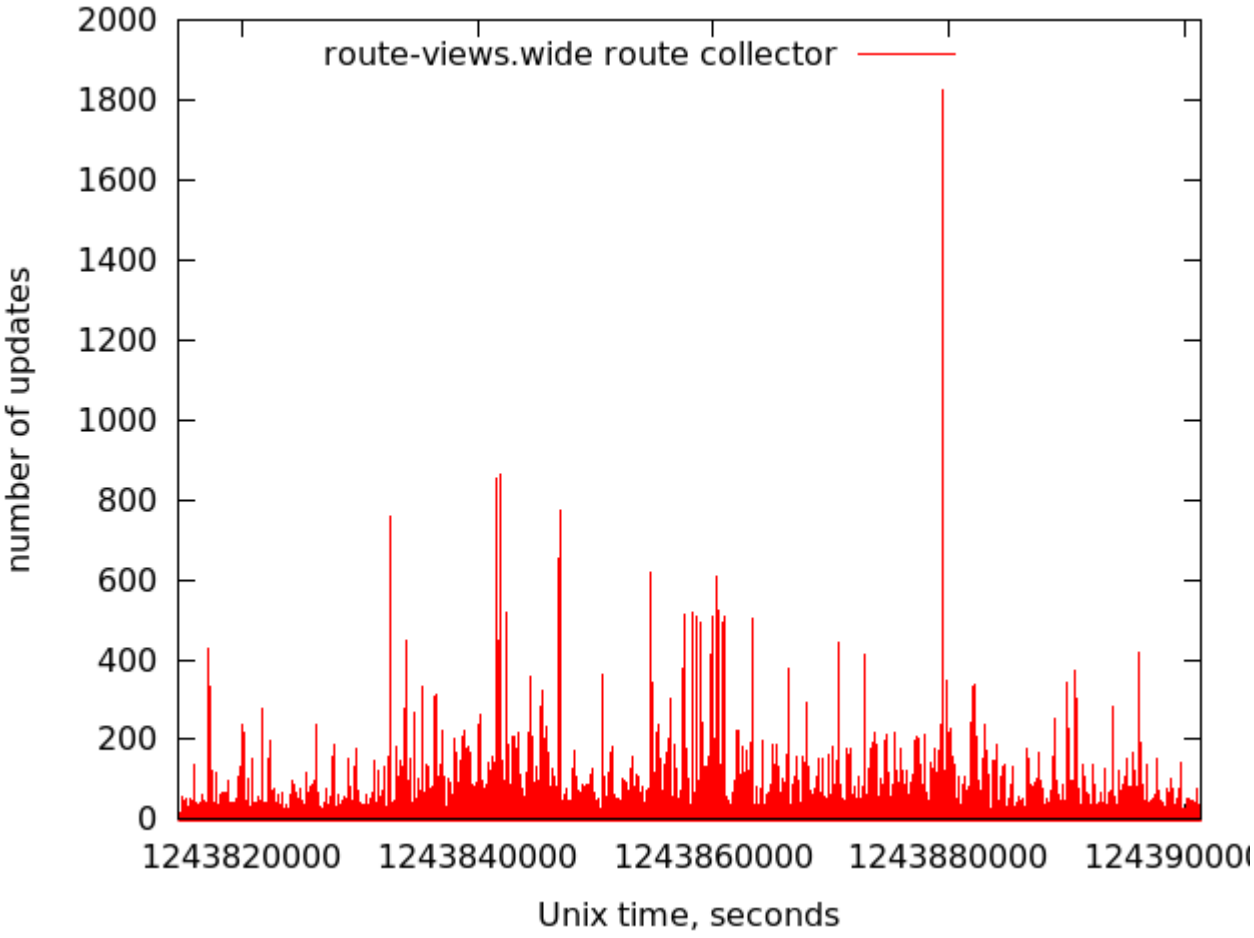


BGP spikes - main scalability issue 1/2



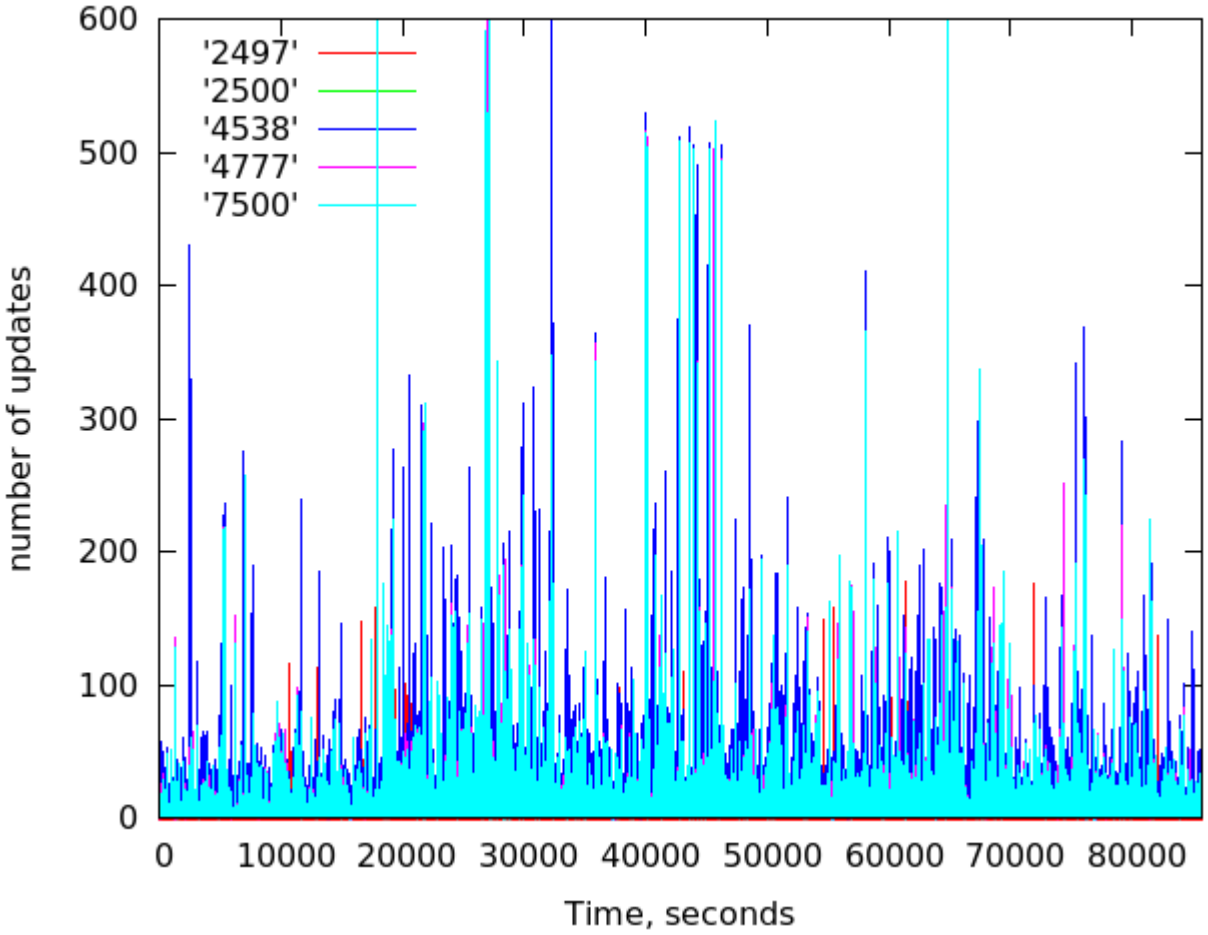
Updates at Linx route collector for 15.07.2012

BGP spikes - main scalability issue 1/2



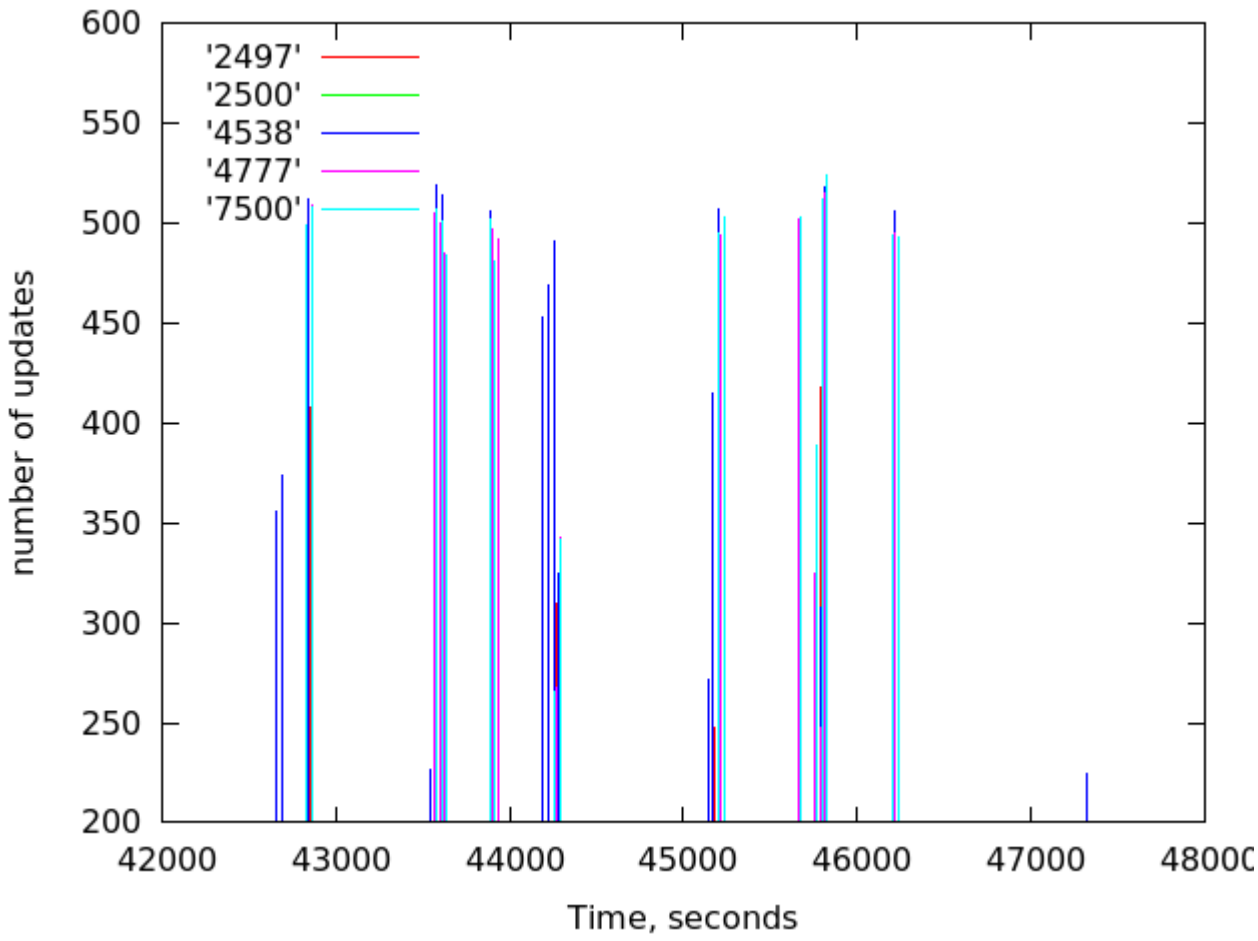
Updates at Wide route collector for 01.06.2009

Correlated spikes 1/2



Updates at Wide route collector plotted by monitor

Correlated spikes 2/2

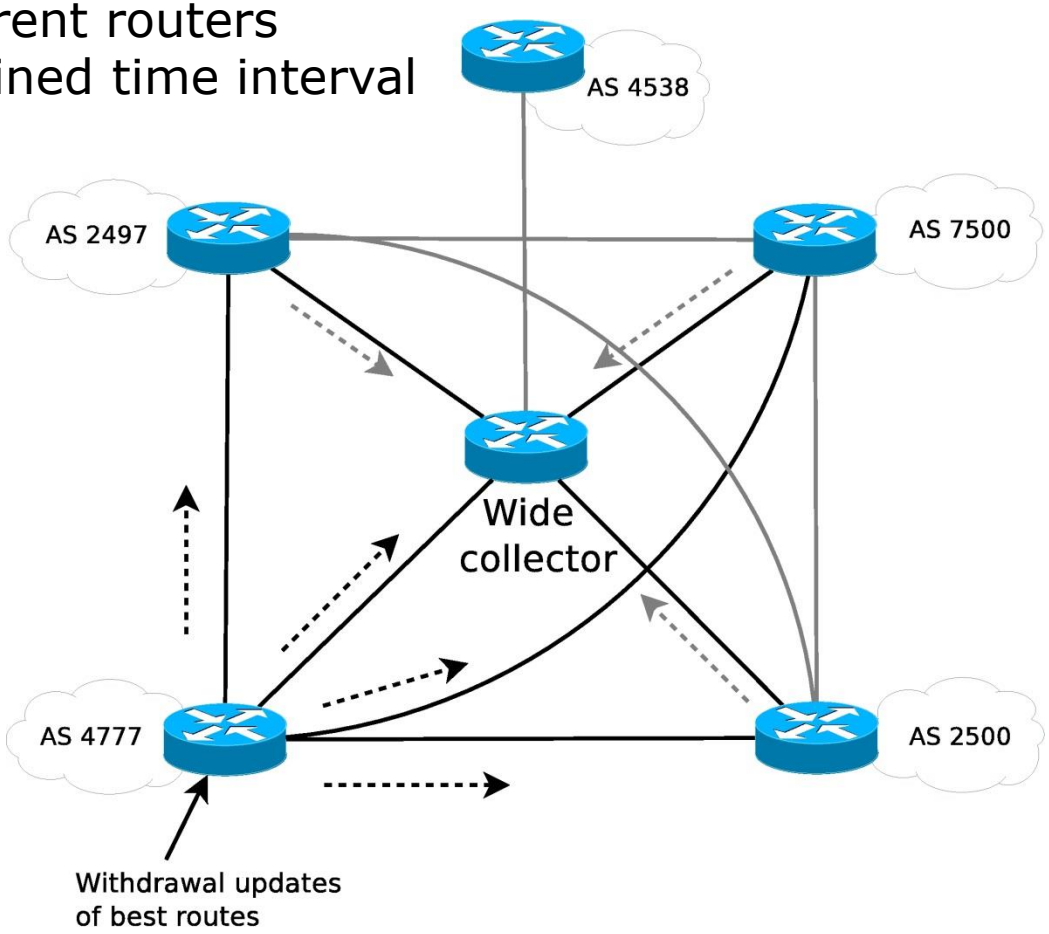


Updates at Wide route collector plotted by monitor, zoomed

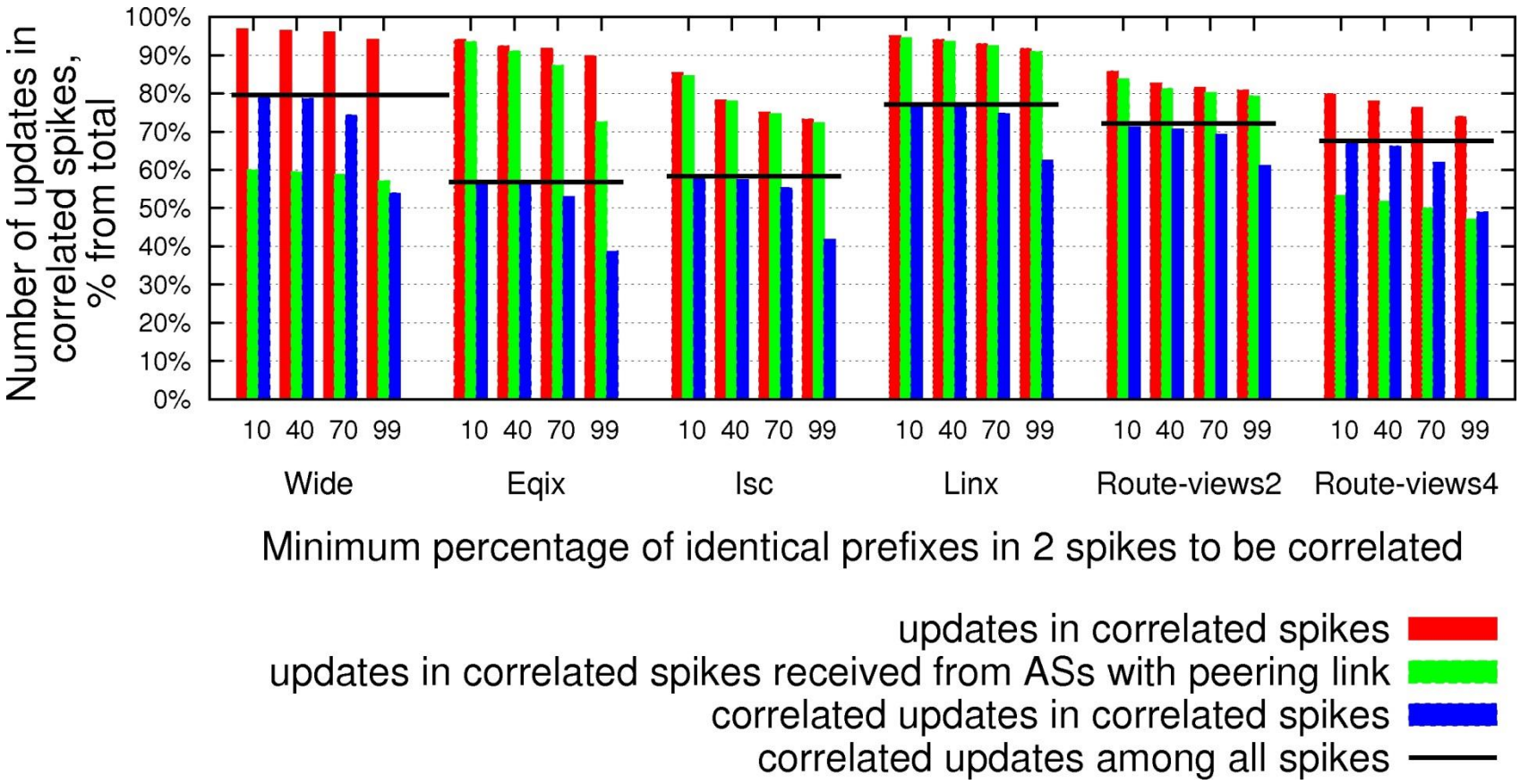
Correlation and propagation: artificial example

Correlated spikes:

- contain fraction of updates/withdrawals for same prefixes
- are received from different routers
- are received within defined time interval



BGP correlation in numbers

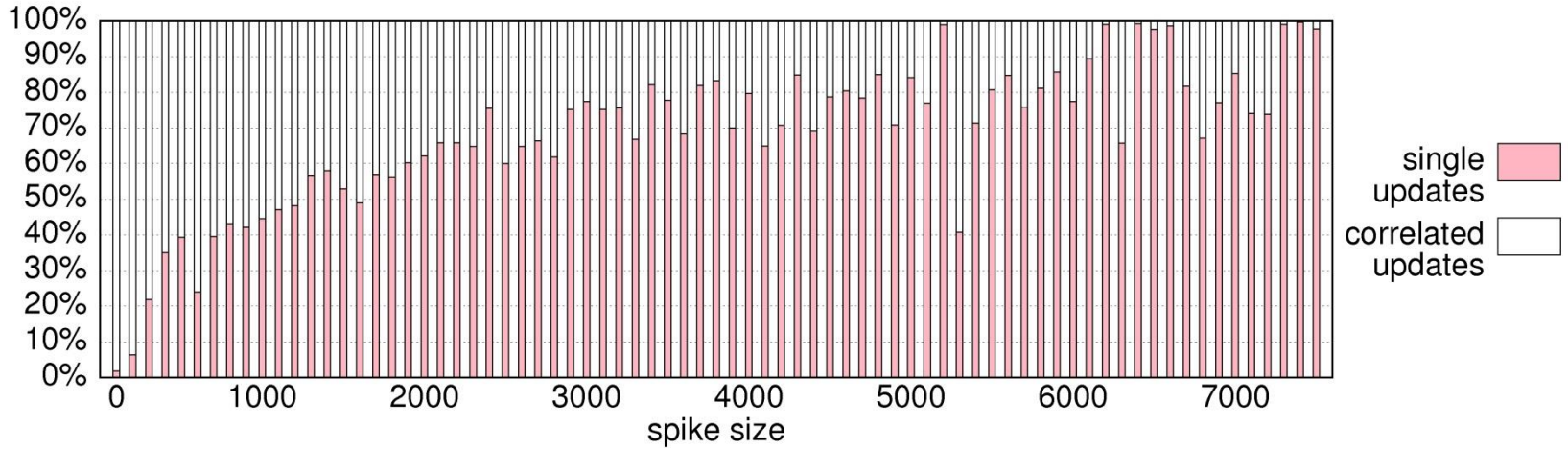


Note: Number of correlated spikes/updates depends on number of connections between monitors

What tells us correlation in BGP updates?

- Correlation reflects propagation of routing events
- Major part of BGP updates is correlated
- Correlated updates could be used as an additional information source for BGP analysis.
- Using correlation, it is possible to estimate locality of routing events

Classification of BGP updates



Classification of BGP updates on a per-bin basis, time interval 120 s.

- Correlated updates form 80% of total
- Major part of big spikes is single and does not propagate globally through the Internet
- Update churn seen in small spikes (0-200 updates per second) reflects normal propagation of BGP updates

How global do routing events propagate?

Methodology.

For each correlated spike:

1. Find group of spikes correlated with given within the time interval
2. Exclude spikes from Autonomous Systems with small total number of received updates

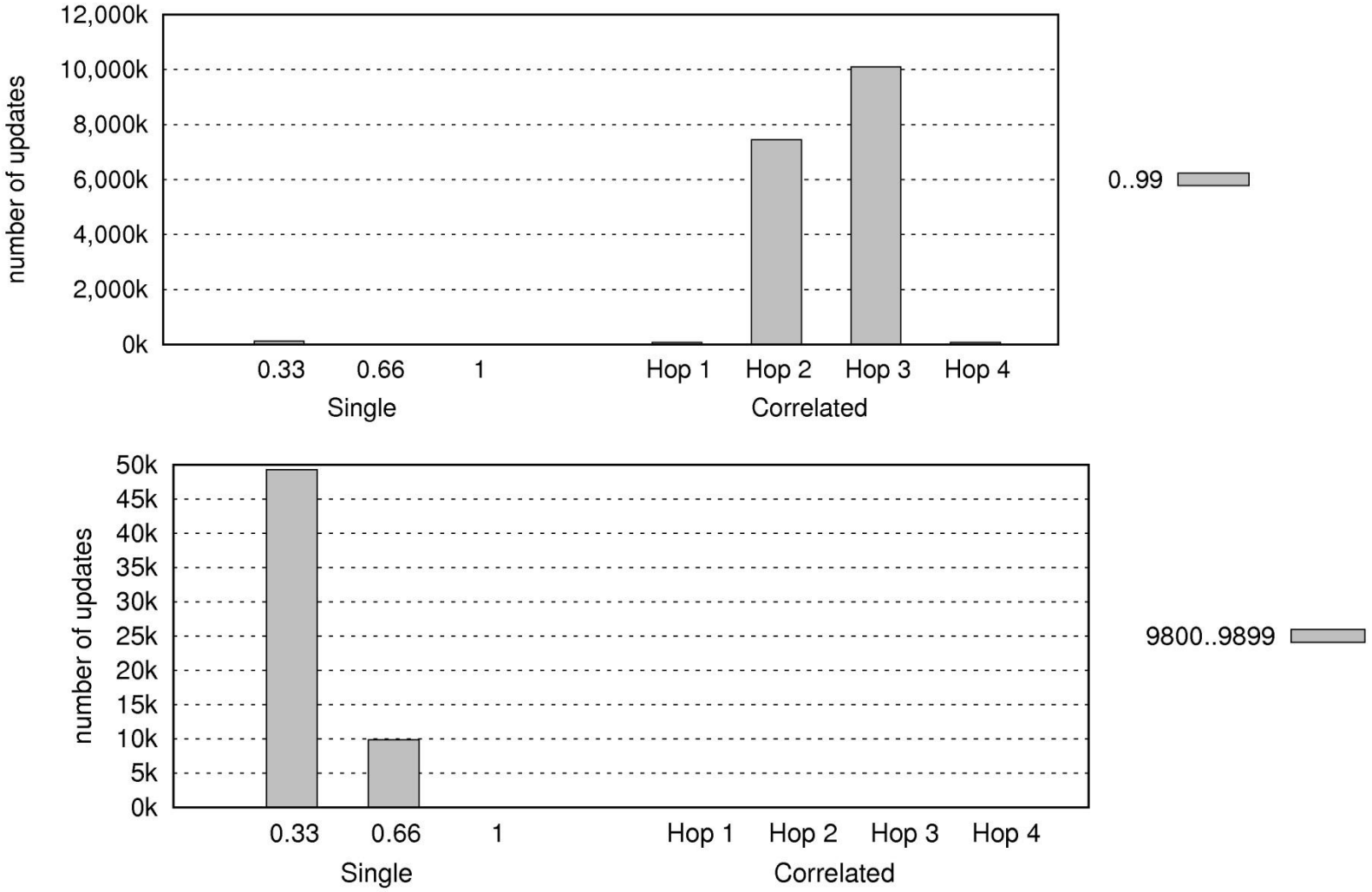
$$Update\_Sum_{<as,r>}(x) > threshold_{pairs} \times Update\_Sum(x)$$

$$threshold_{pairs} = 1/2 * 1/Monitor\_pairs_x$$

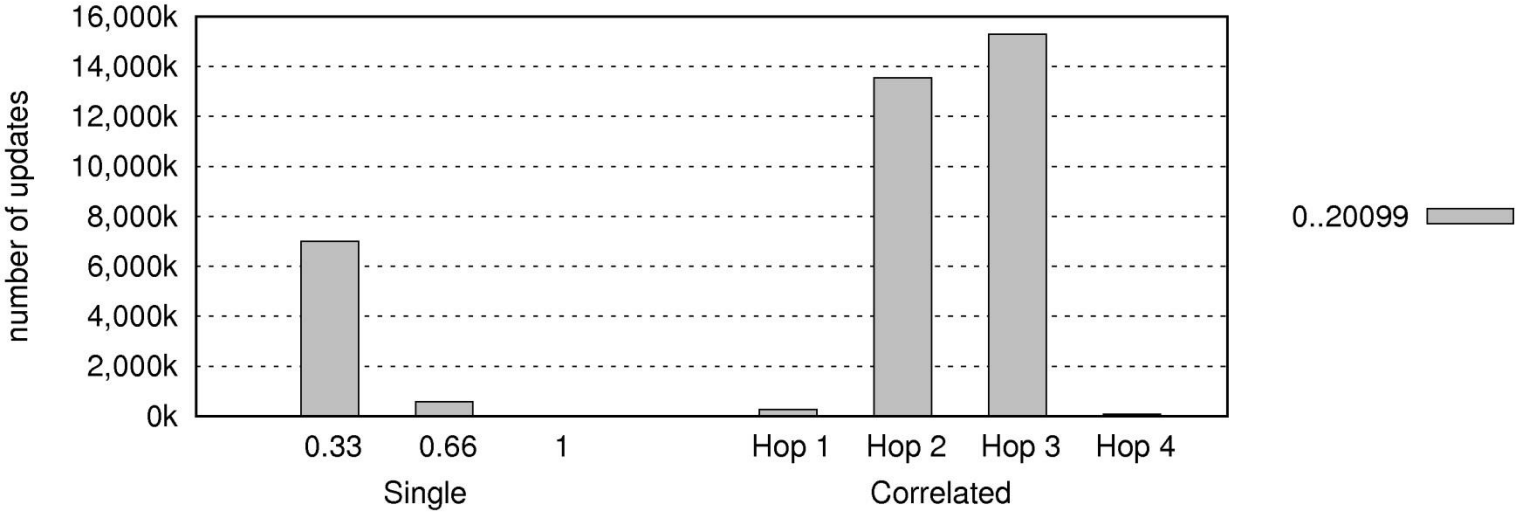
$$Max\_Spike_{\langle as,r \rangle}(x) > 0.33 \times Max\_SameAS\_updates(x)$$

3. Using Internet topology (map file), determine maximum distance between 2 Autonomous Systems in the group of spikes correlated with the given one

Propagation in hops 1/2



Propagation in hops 2/2



- Most routing events propagate 2 or 3 hops away (usual BGP path lasts from 3 to 5 hops)
- For many spikes, classified as single, our visibility is limited

Conclusion

- Correlated spikes reveal propagation of a set of routing events
  - could be used to estimate locality of routing events
- Most of BGP updates come in small spikes
- Update churn is “normal” and reflects BGP event propagation process
- Big spikes are usually local and do not affect major part of Internet
- Correlated spikes are valuable source of information, if combined with topology data and inter-arrival times

Thank You!

For more details please read “Andrey Sapegin and Steve Uhlig. "On the extent of correlation in BGP updates in the Internet and what it tells us about locality of BGP routing events." Elsevier Computer Communications Journal (2013), DOI.”

[1] Created by Matt Britt using data from the OPTE project.