

Uncovering Artifacts of Flow Measurement Tools

Ítalo Cunha

Thomson and UPMC Paris Universit  s

Fernando Silveira (Thomson and UPMC Paris Universit  s)

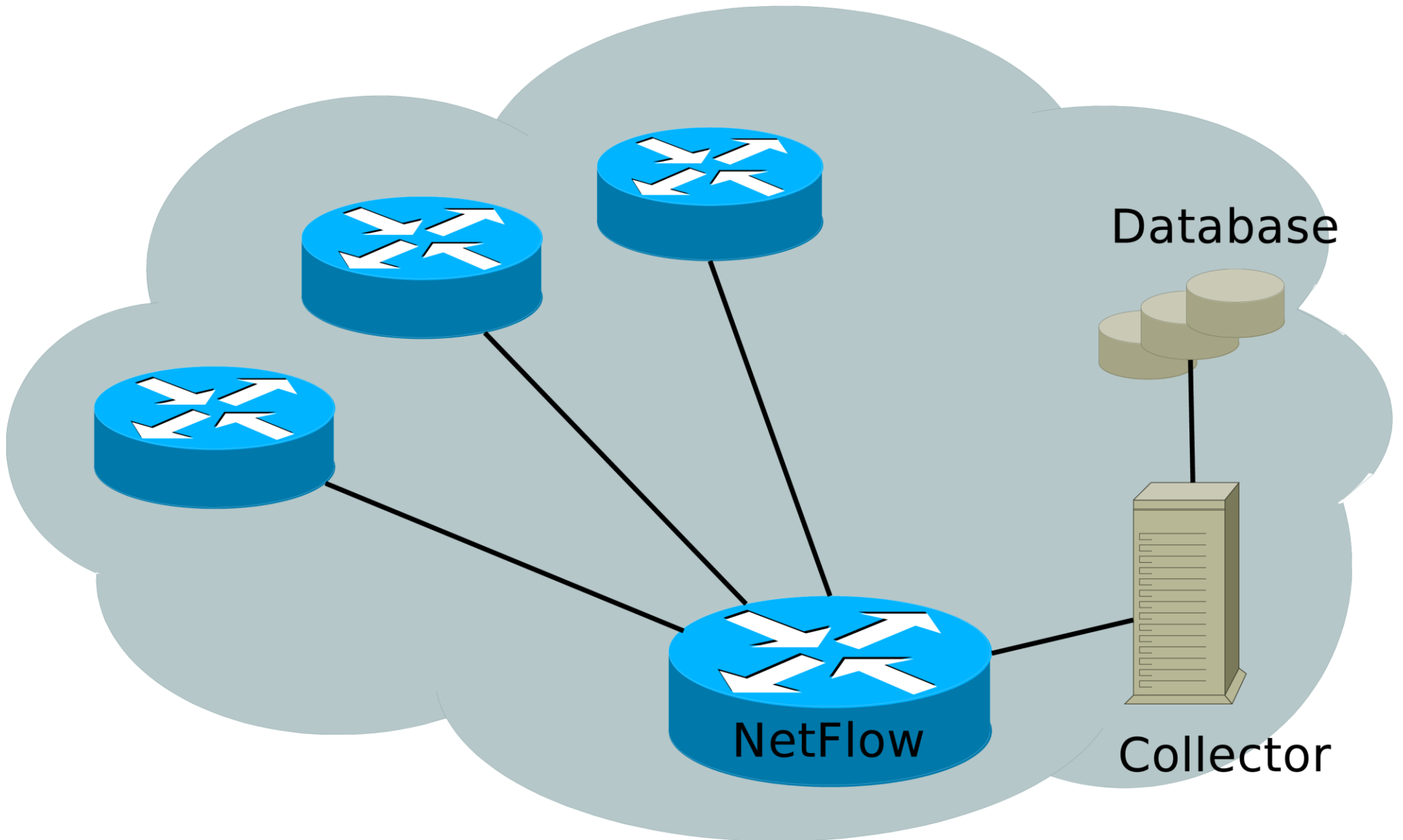
Ricardo Oliveira (UCLA)

Renata Teixeira (CNRS and UPMC Paris Universit  s)

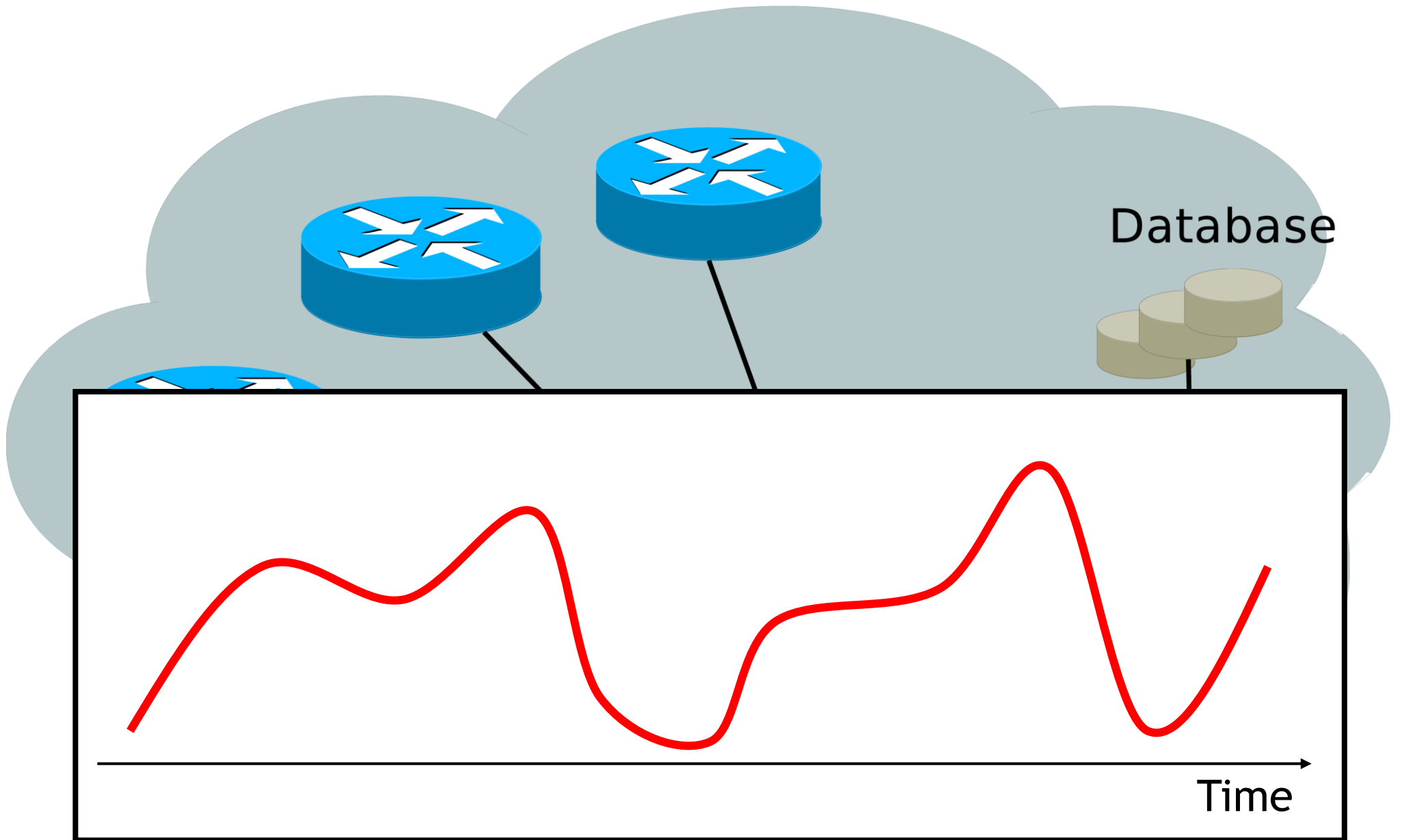
Christophe Diot (Thomson)

Passive and Active Measurement Conference, April 2009.

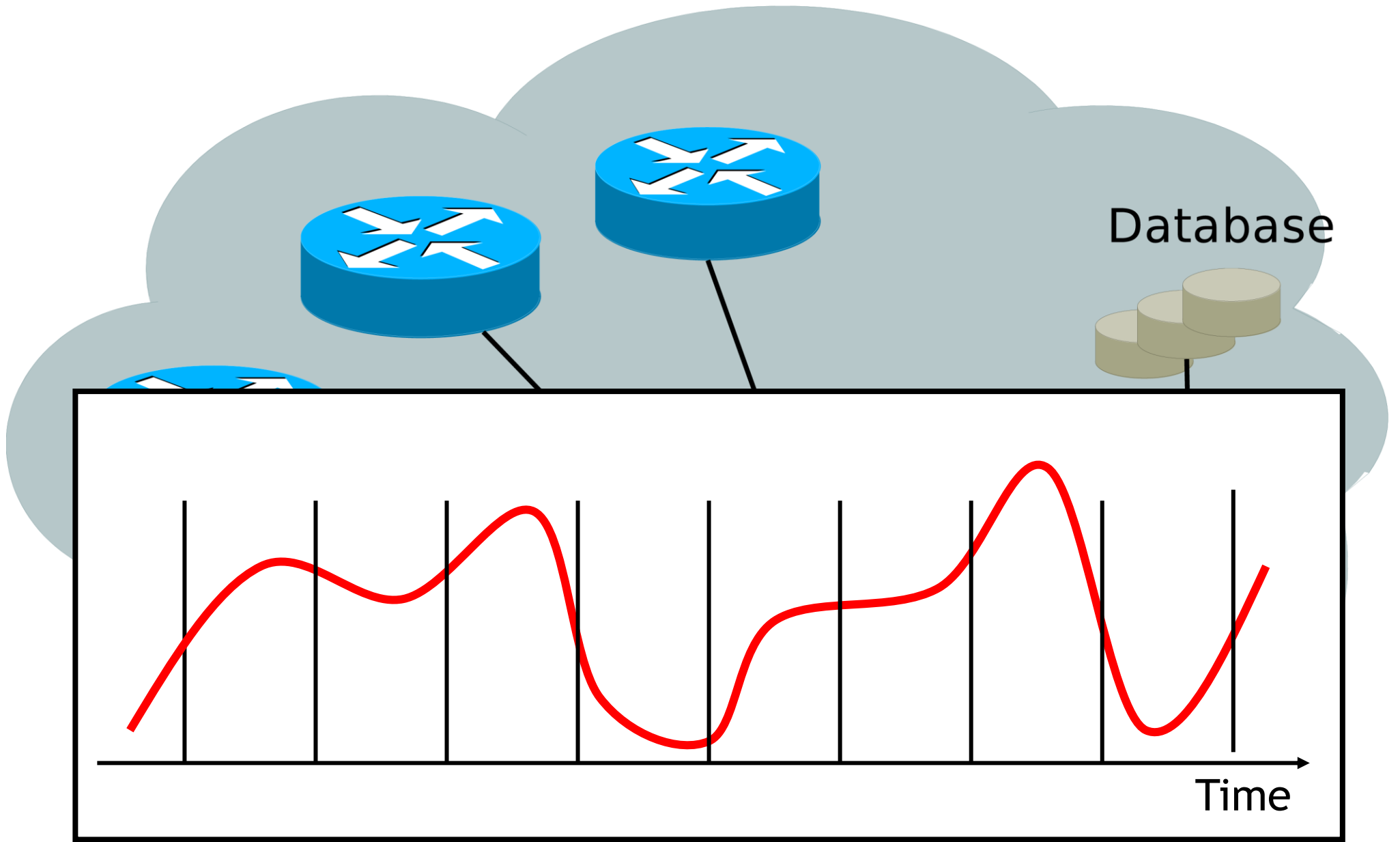
Flow Measurement Tools



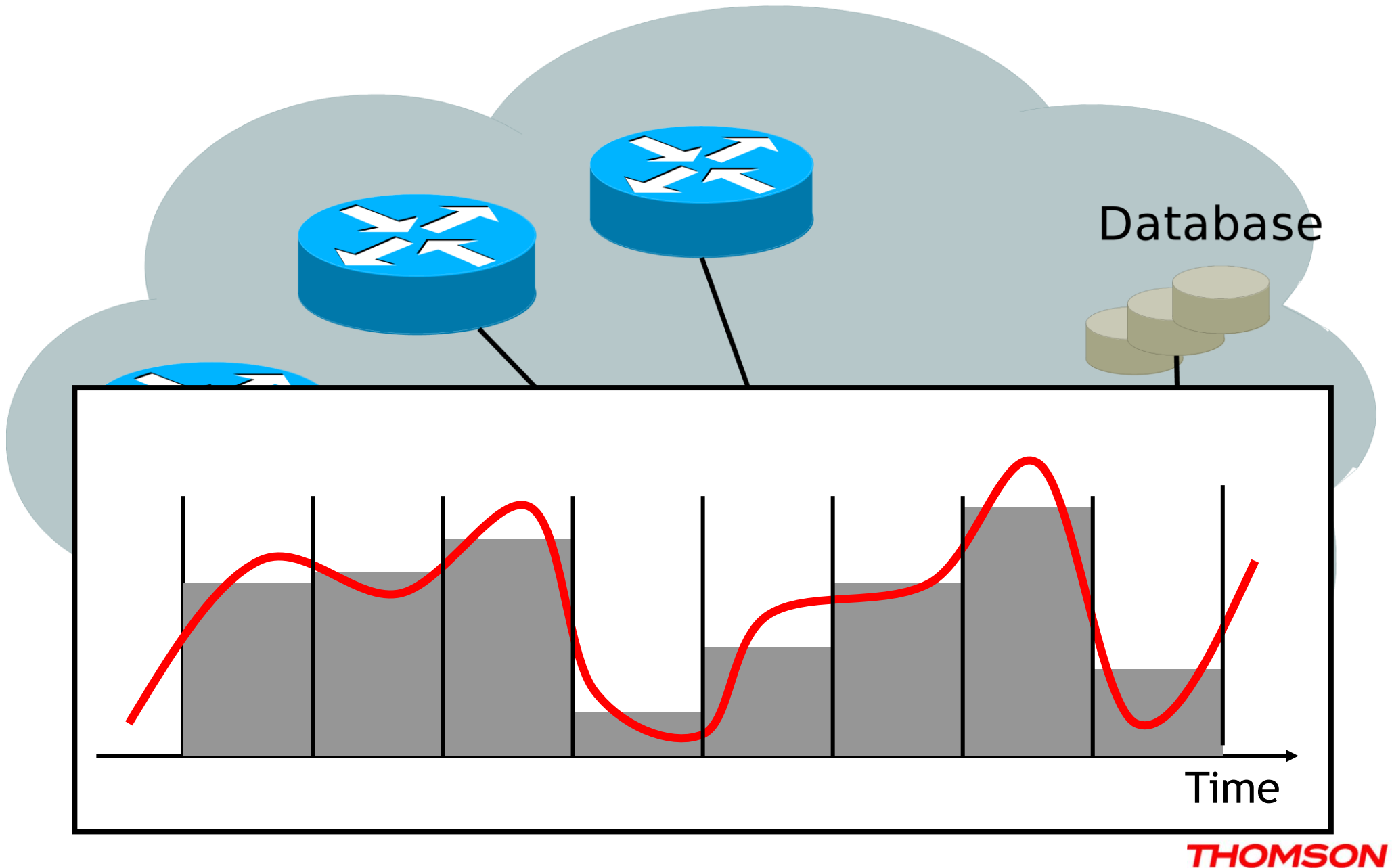
Flow Measurement Tools



Flow Measurement Tools



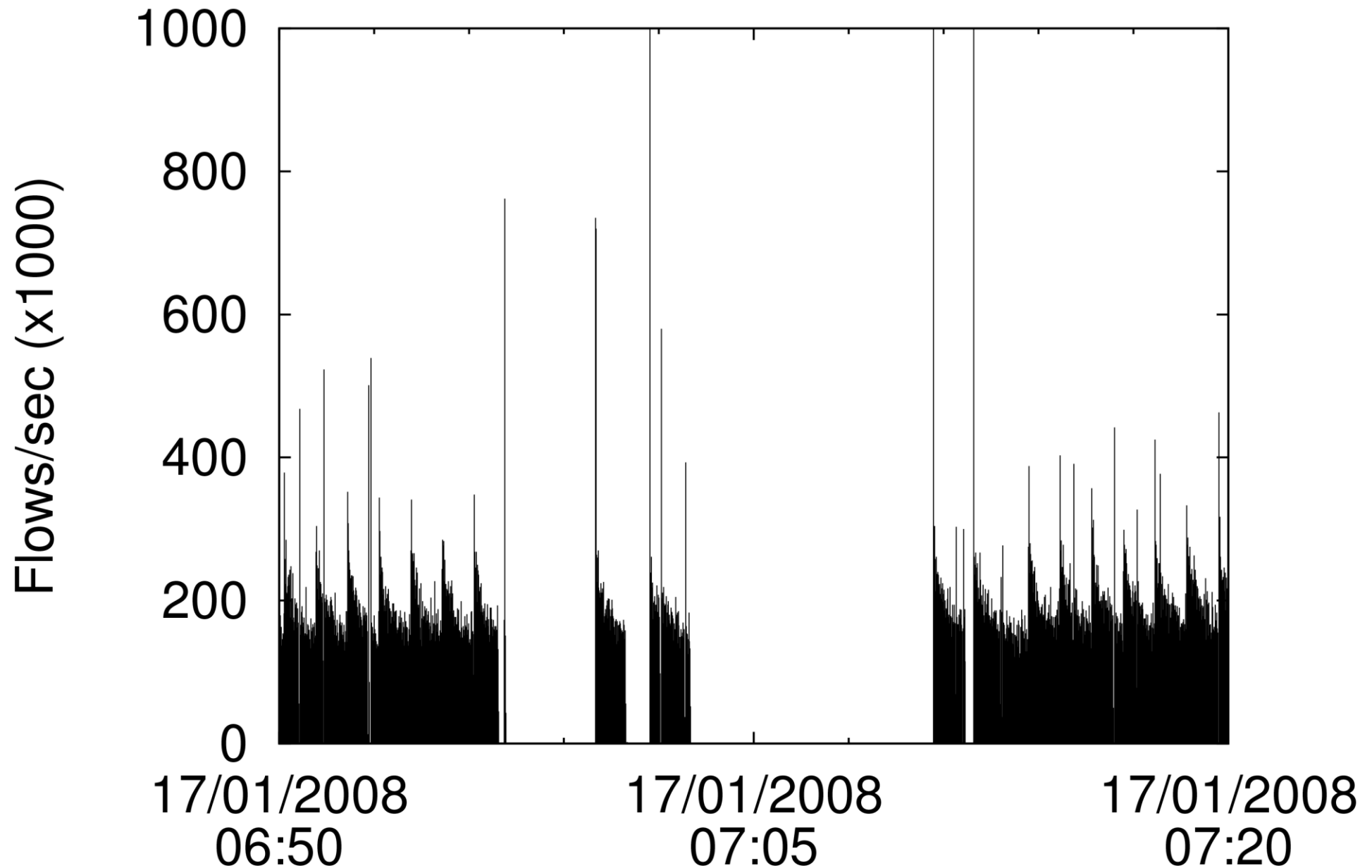
Flow Measurement Tools



Observation: Measurement Artifacts

- Small timescale analysis uncovered unexpected behavior
 - Periodic spikes in flow exports
 - Measurement gaps followed by spikes
- Artifacts prevalent in data from Abilene and GÉANT
 - Since 2004
 - Possible impact on previous work

Quick Look at Measurement Artifacts

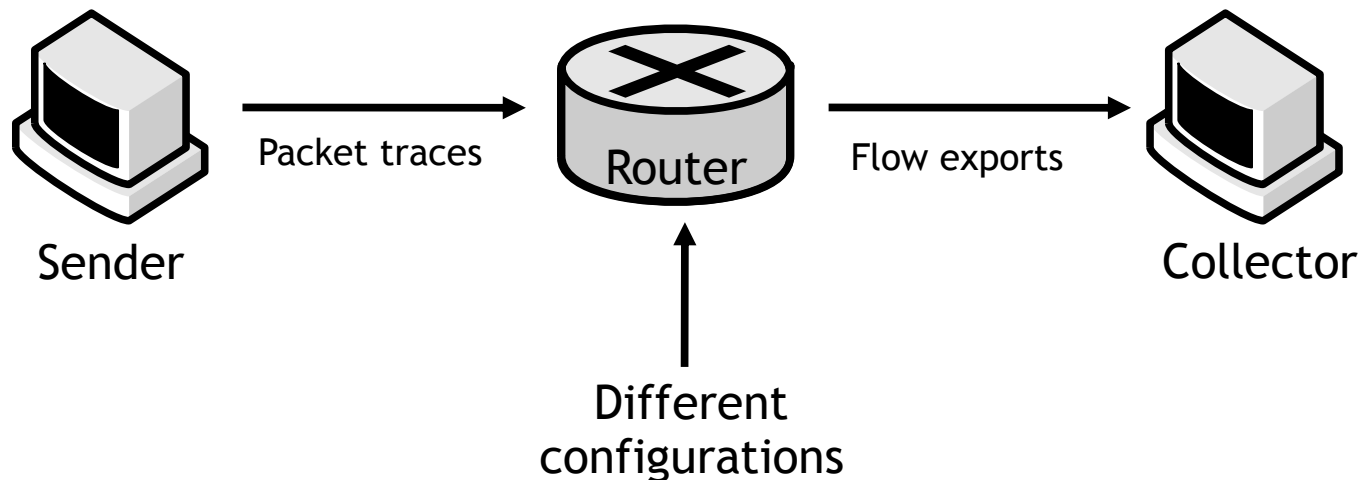


Outline

- Methodology
- Analysis of measurement artifacts
 - Periodic spikes in flow exports
 - Measurement gaps
- Potential impact on previous work

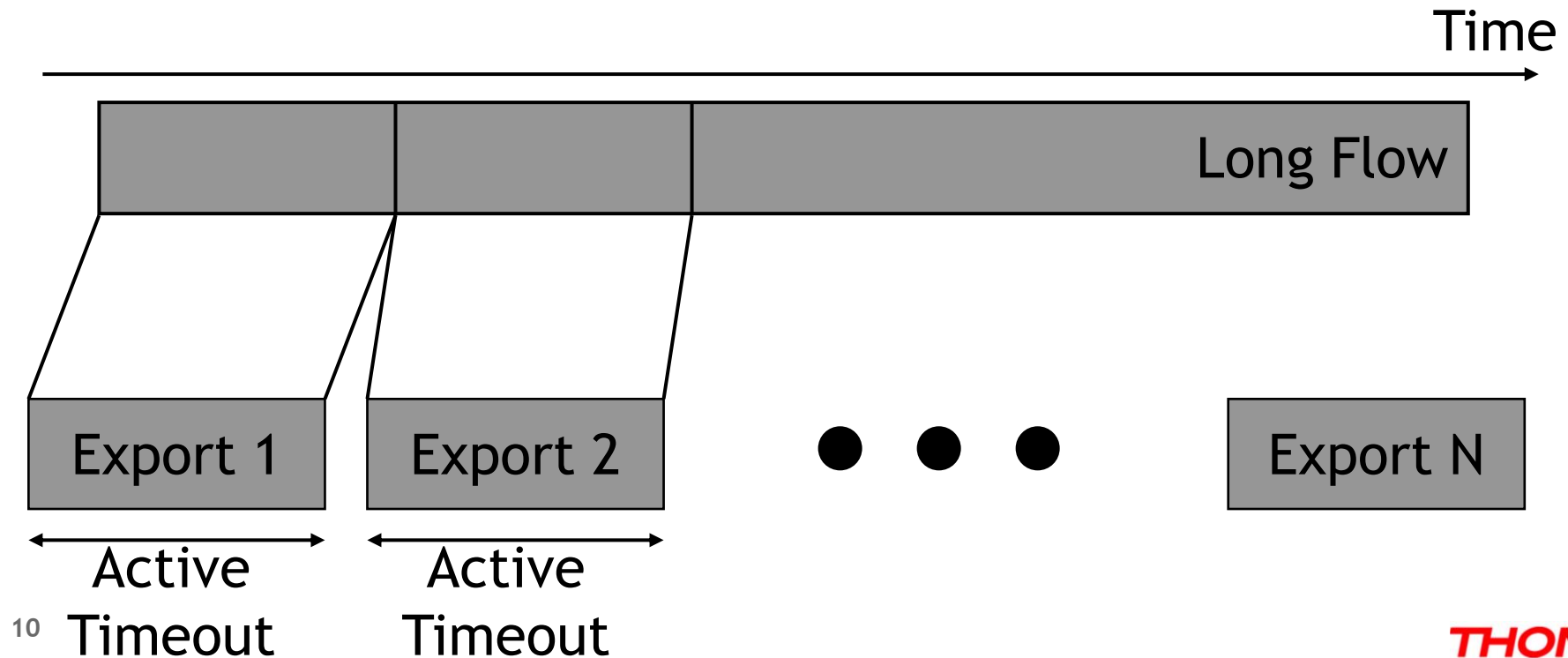
Methodology

- **Replay synthetic and real packet traces**
 - Controlled environment
- **Vary router configuration**
 - Active and inactive timeouts
 - Sampling rate



Methodology

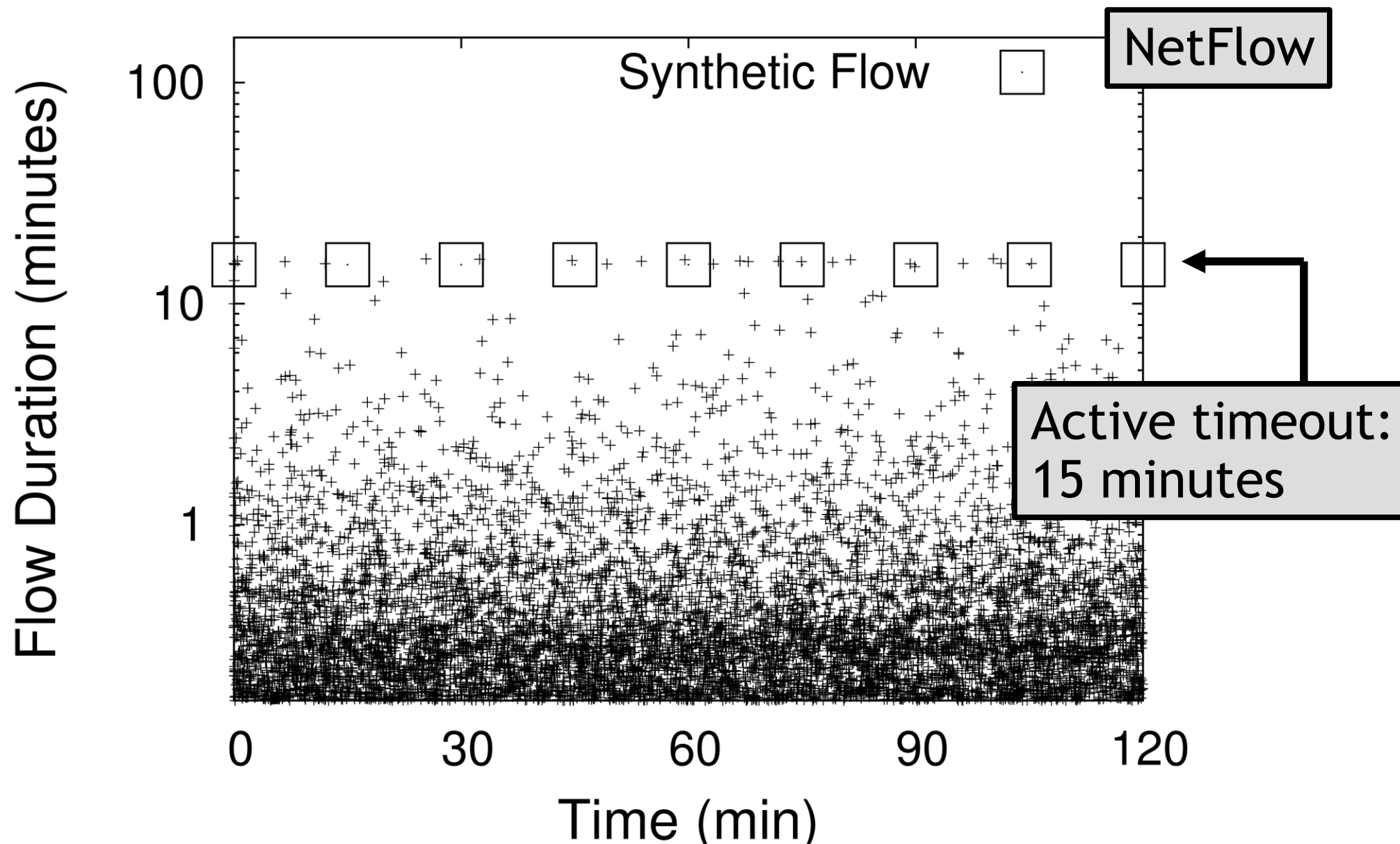
- Replay synthetic and real packet traces
 - Controlled environment
- Vary router configuration
 - Active and inactive timeouts
 - Sampling rate



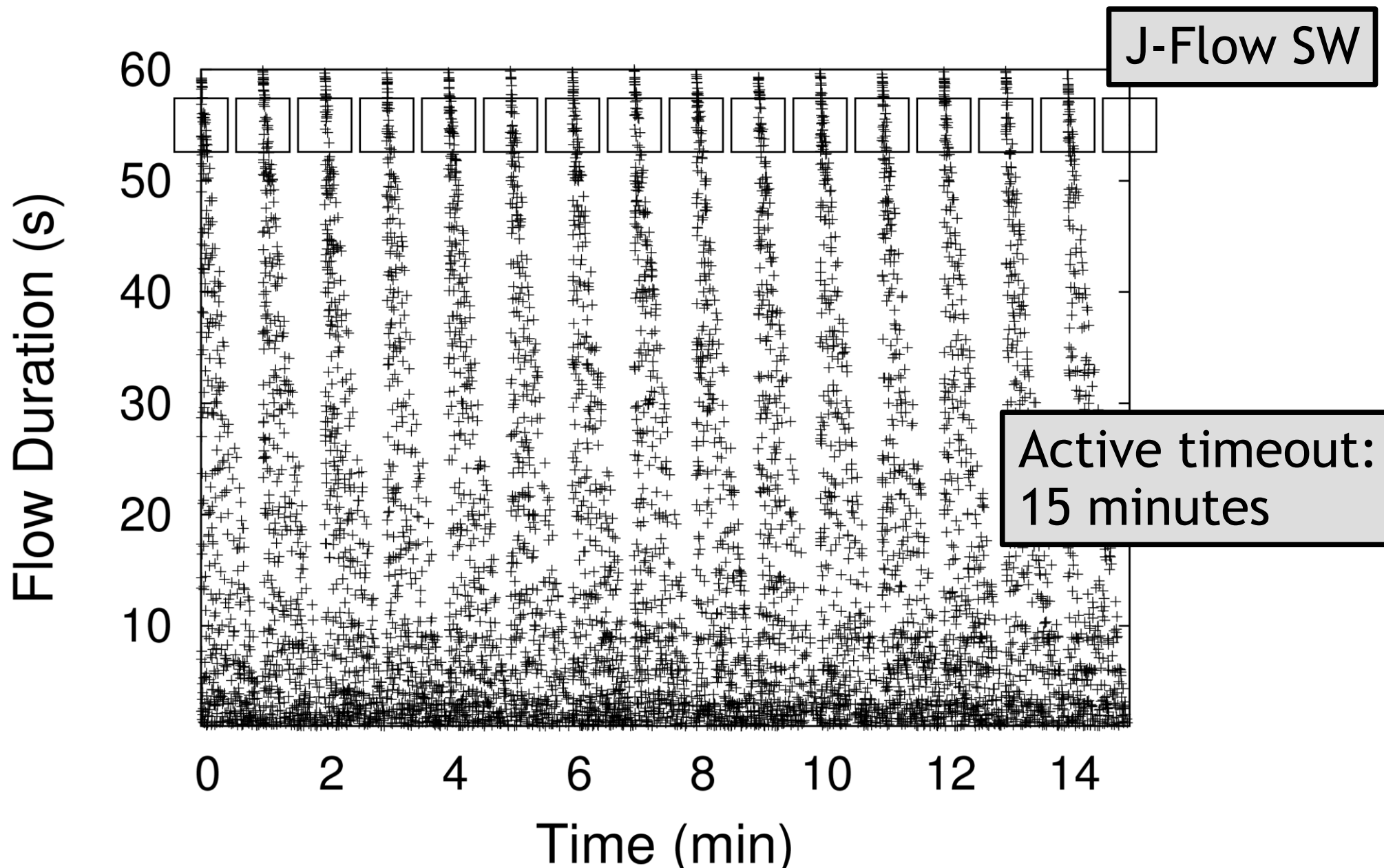
Test Different Implementations

- Cisco NetFlow (software)
- Juniper J-Flow in software
 - Shares CPU with control-plane processes
- Juniper J-Flow in hardware
 - Uses a dedicated measurement card

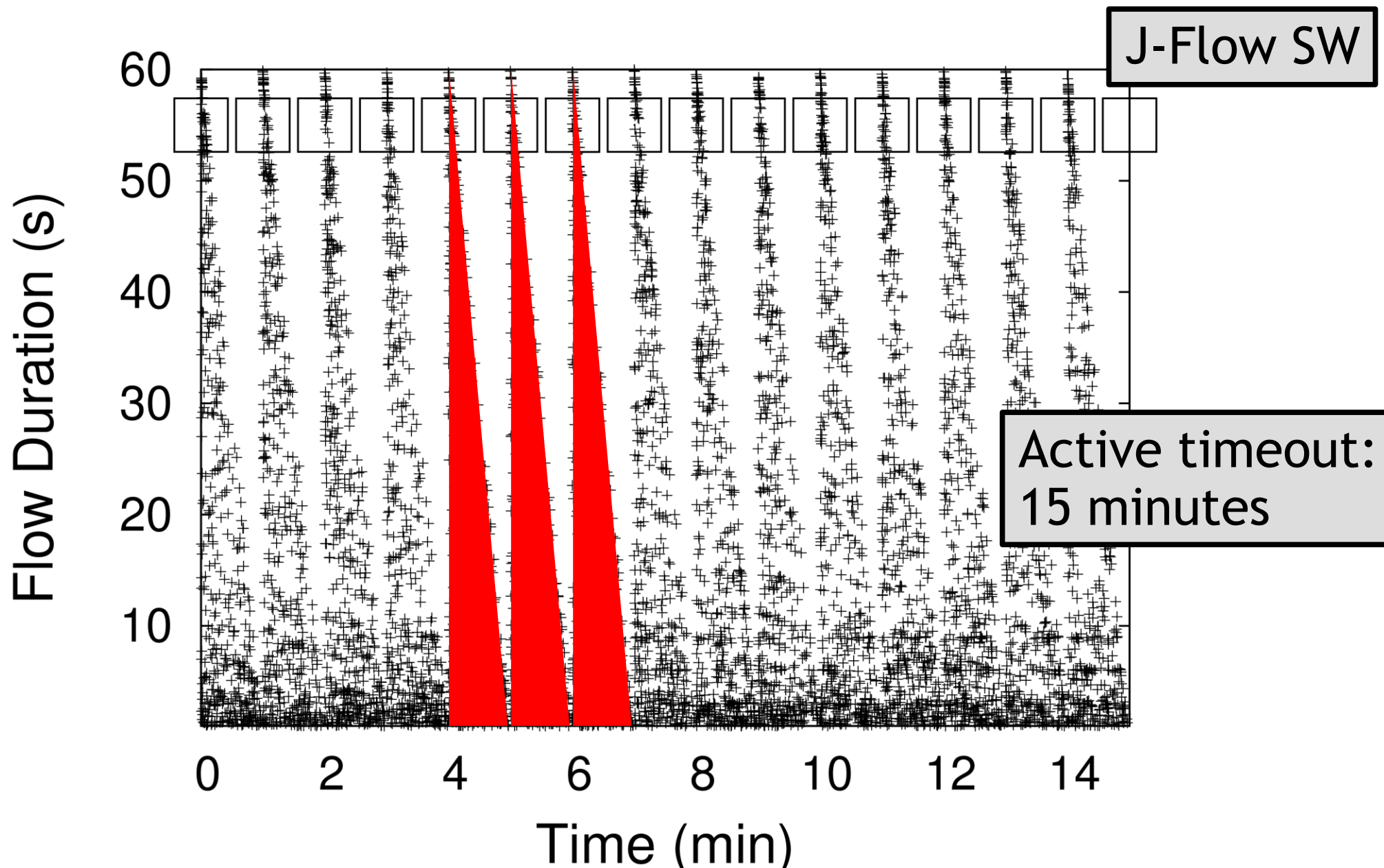
Expected Behavior for Flow Exports



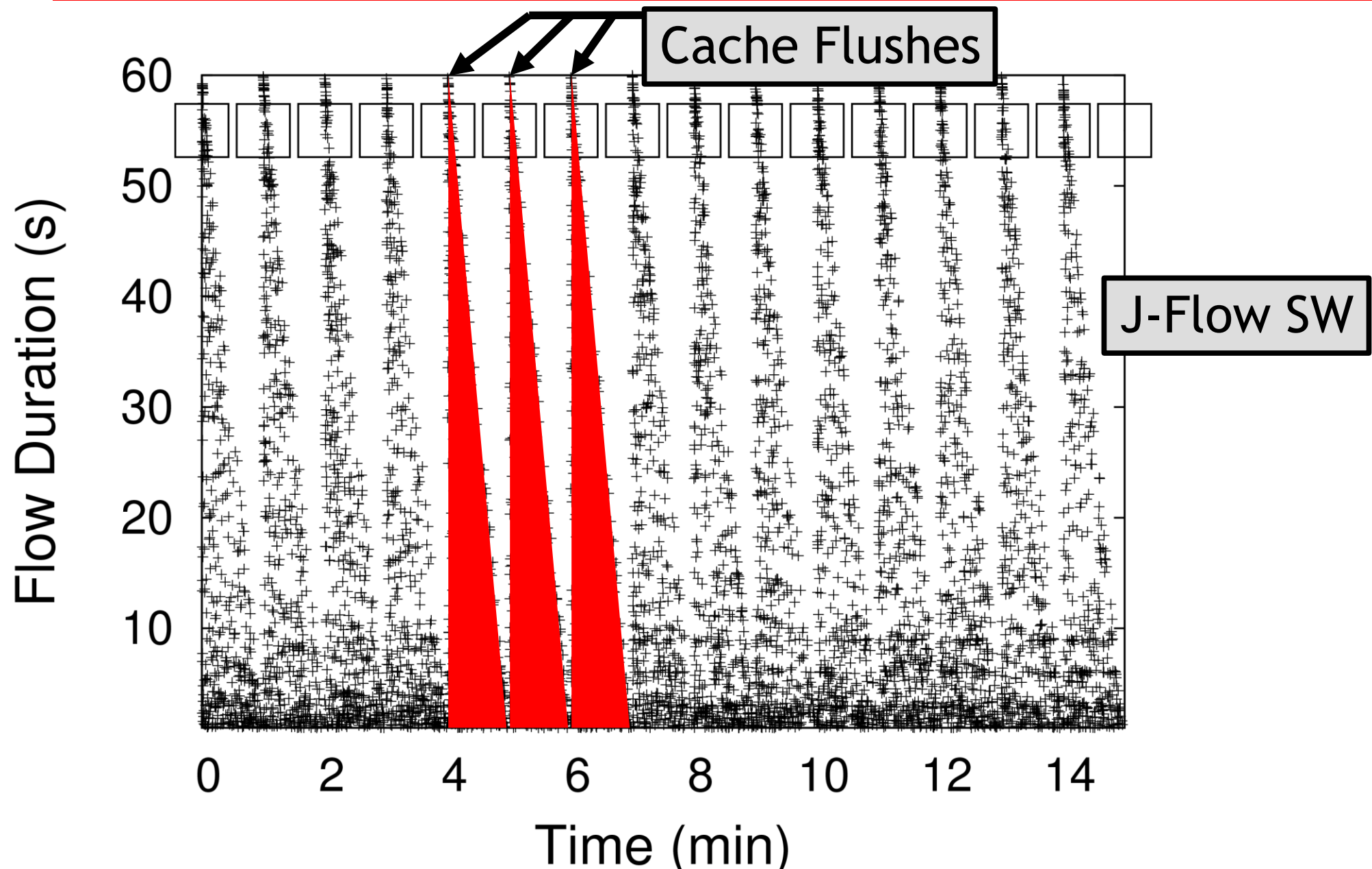
Periodicity in Flow Exports



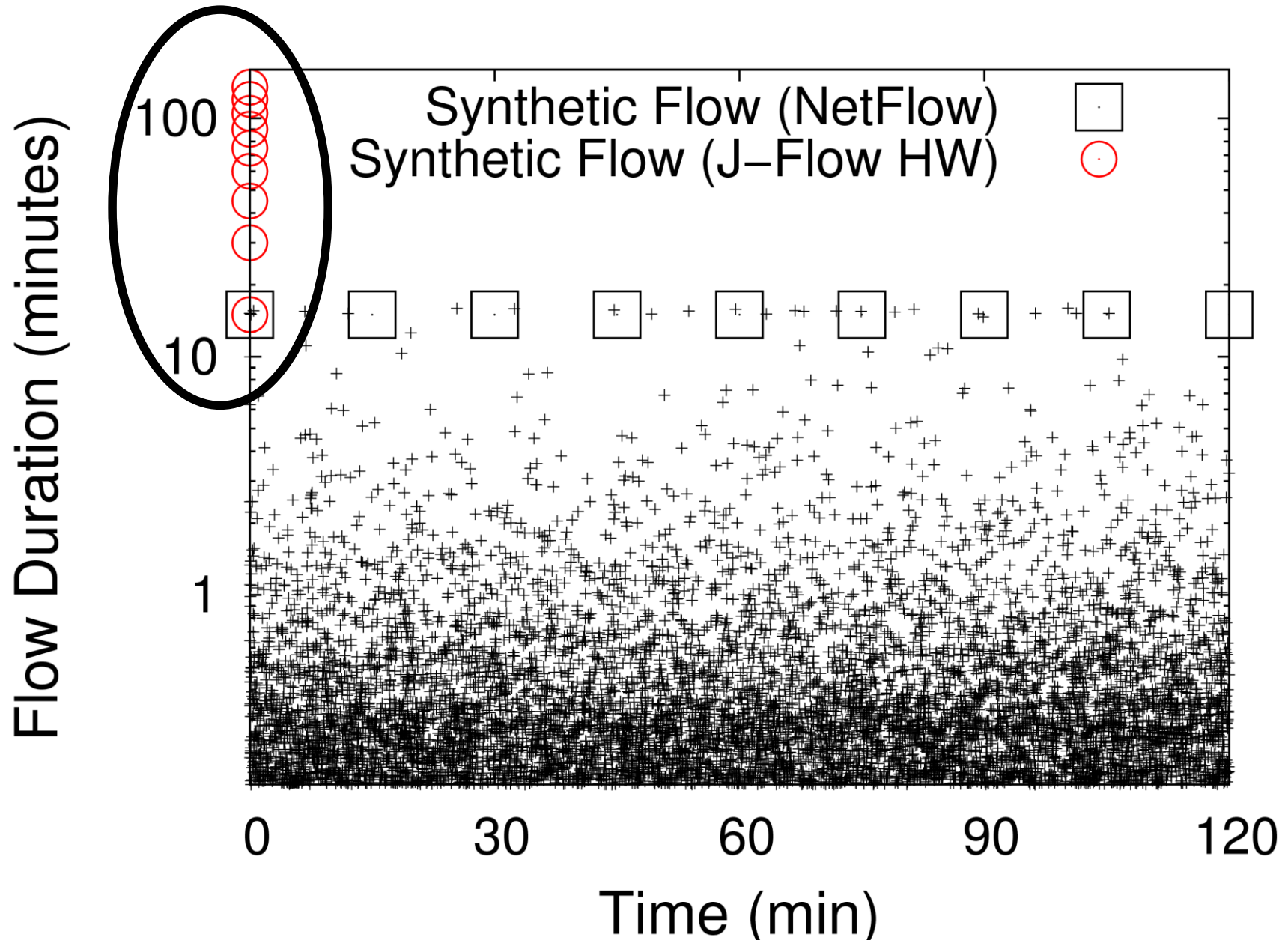
Periodicity in Flow Exports



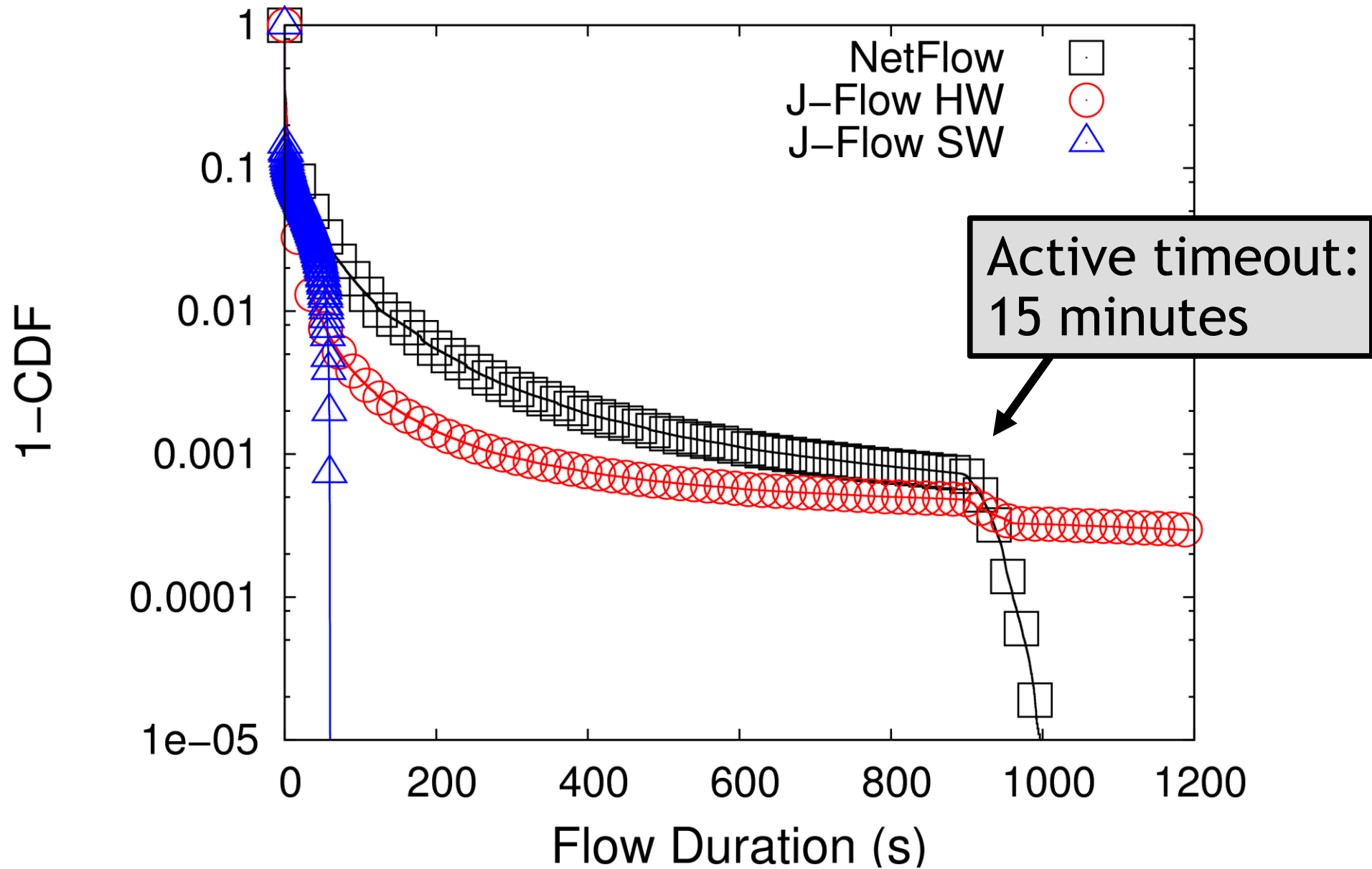
Periodic Exports Due to Cache Flush



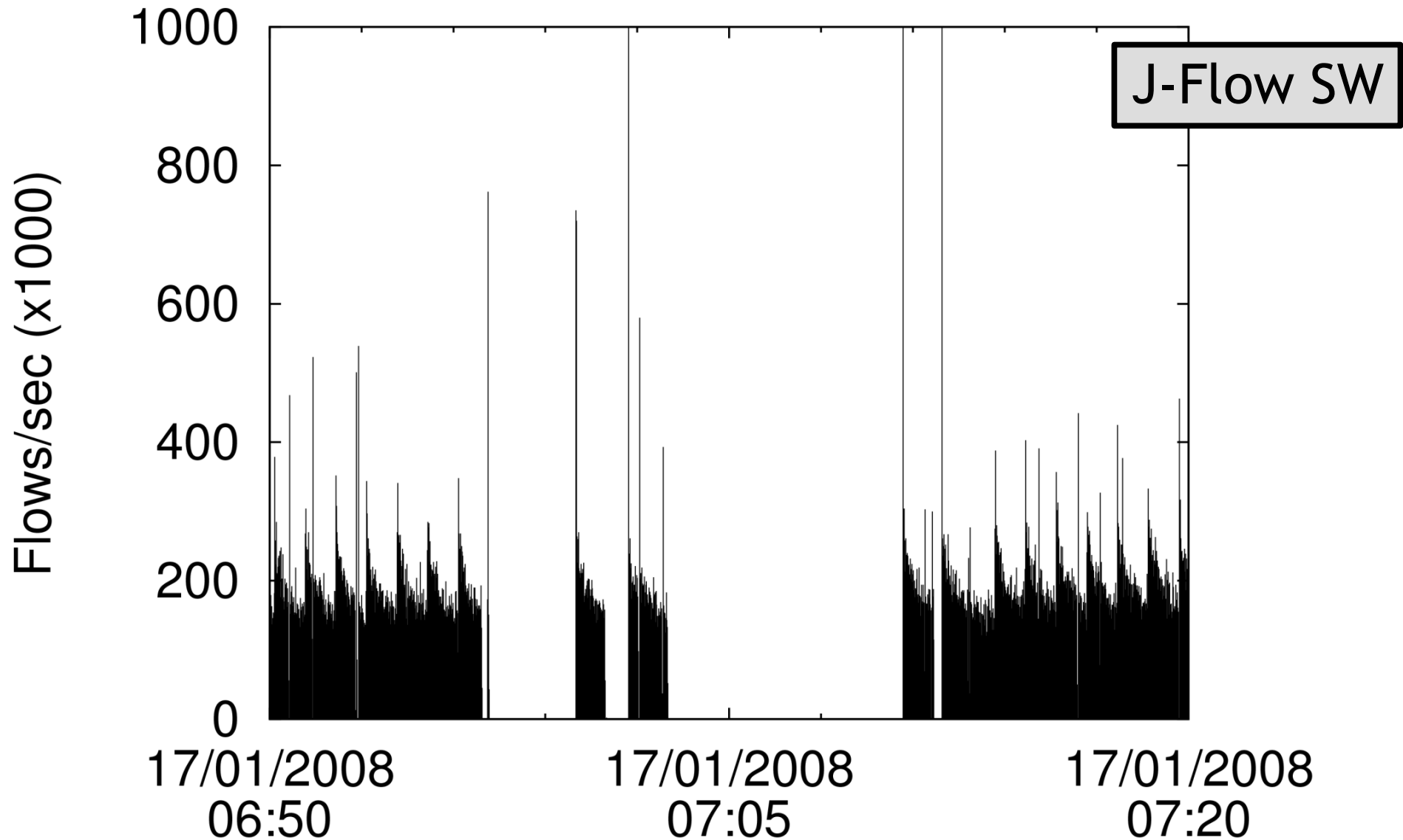
Cache Flush with J-Flow Hardware



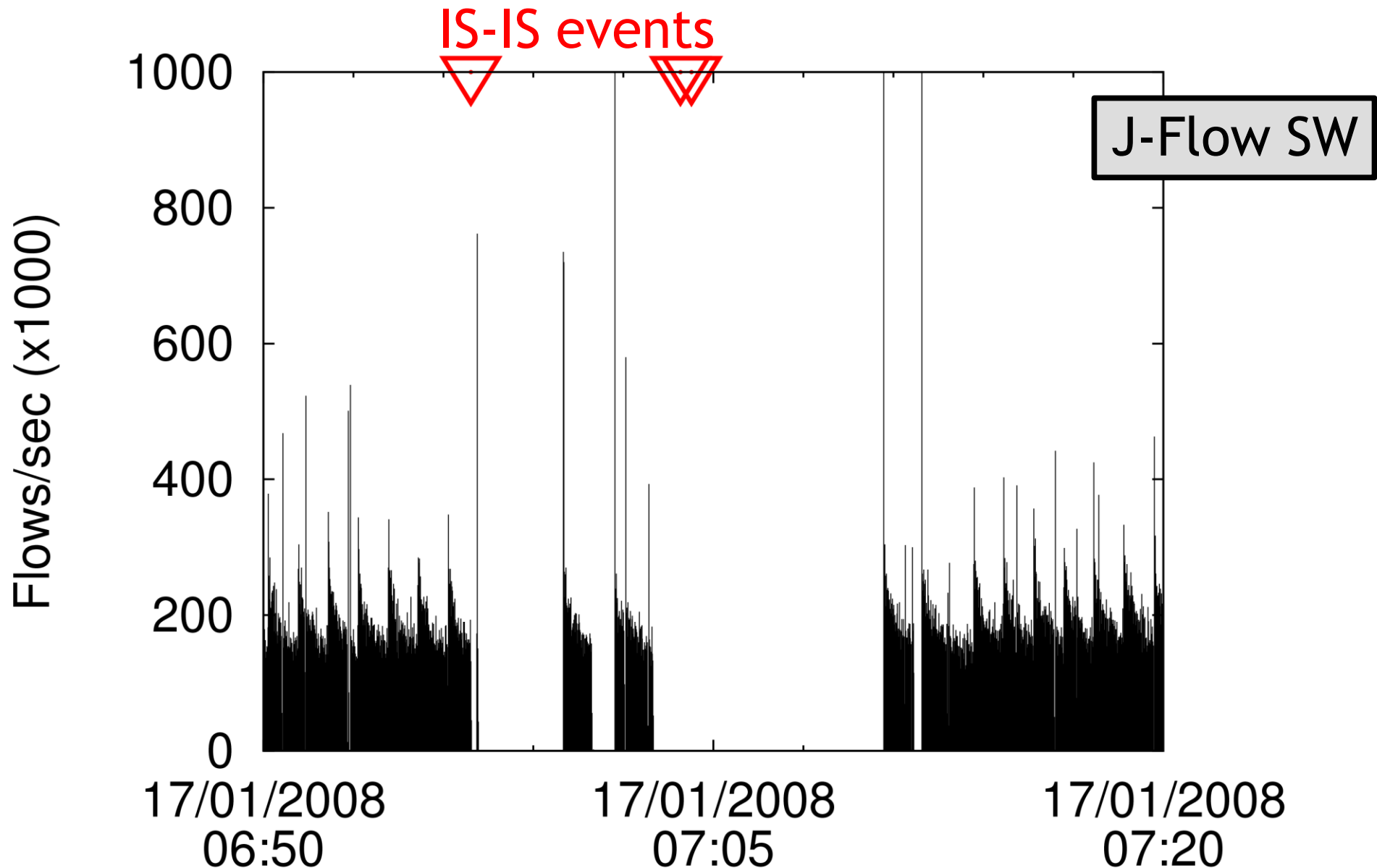
Impact of Cache Flashes



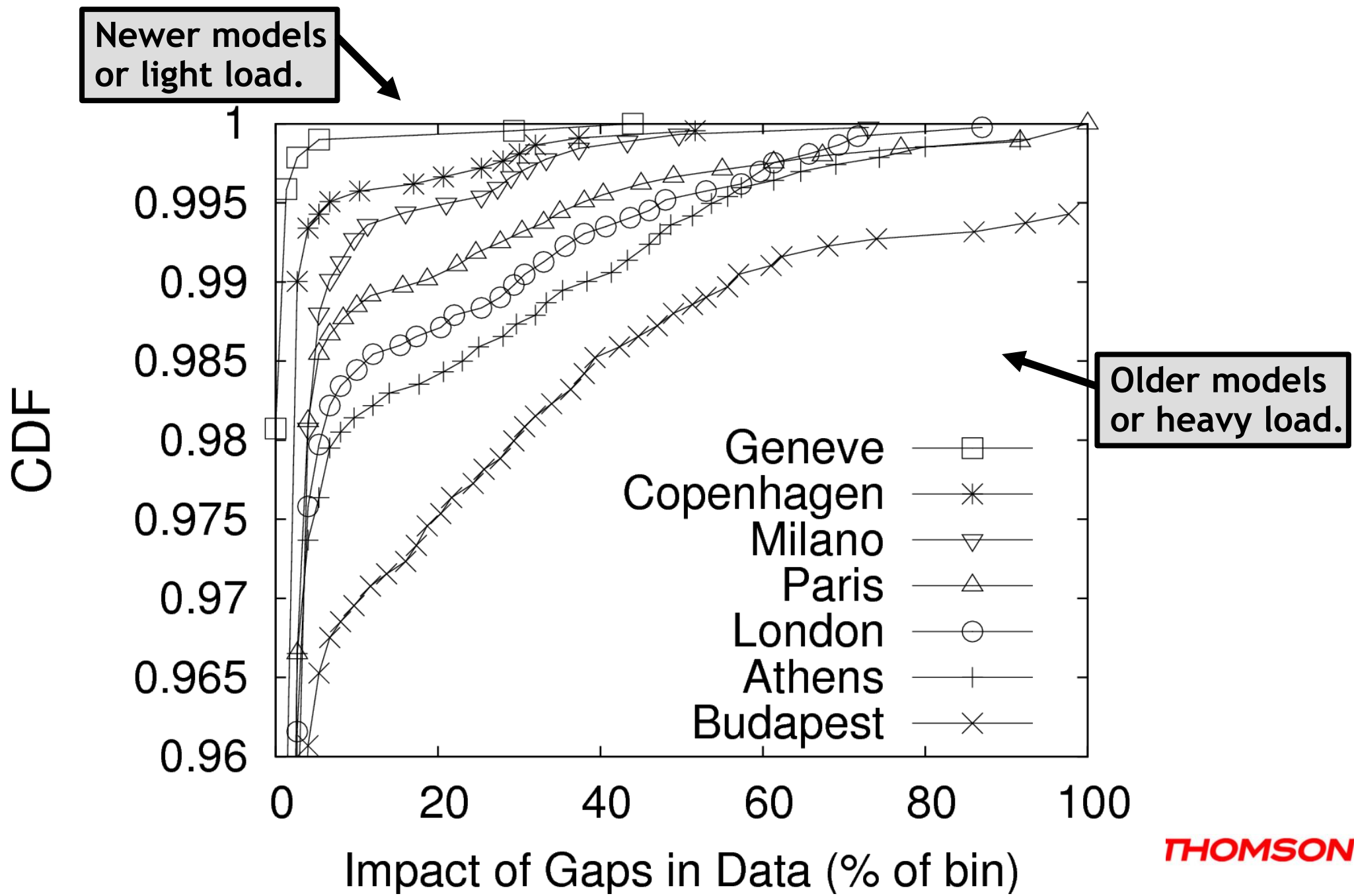
Measurement Gaps



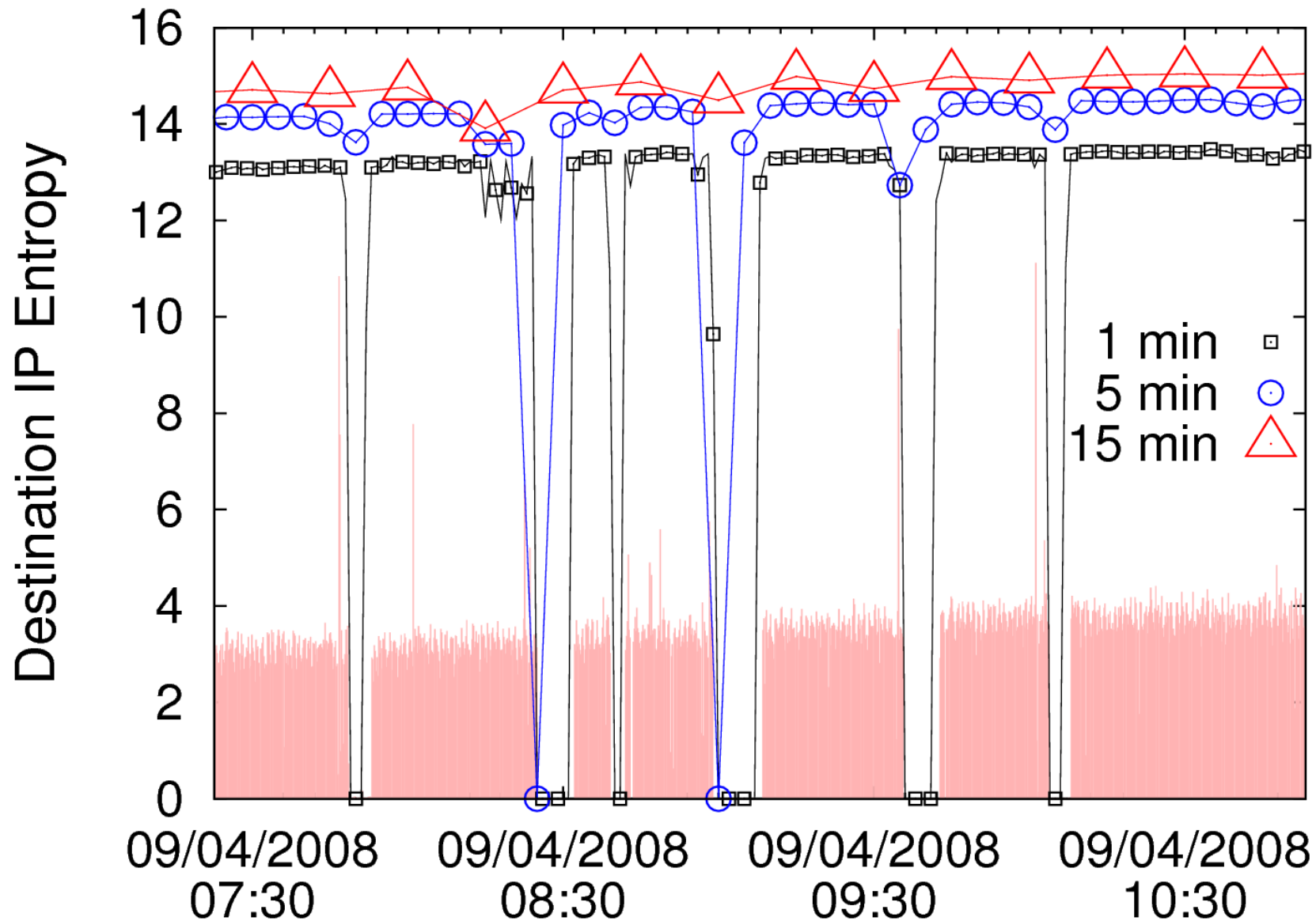
Measurement Gaps: Caused by Routing Events



Quantifying the Impact of Gaps



Impact of Gaps on Entropy



Takeaways

- Gaps solved by patch in JunOS Mid-2008
 - Historical data is still affected (and used for research)
- No plans to fix periodic cache flushes
- Other artifacts can be hidden

Double-check and don't trust the data blindly.

Questions?

Thank you!