ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Peeling Away Timing Error in NetFlow Data

Brian Trammell, Bernhard Tellenbach,
Dominik Schatzmann, and Martin Burkhart

PAM 2011, Atlanta, Georgia, USA, 22 March 2011

Common Sense in Flow Data Analysis

- "Everyone knows you don't use NetFlow for timing."
  - Export and cache delays – unfit for "real-time".
  - Poor synchronization among routers – correlation is hard.
- "We measure the world in *n*-second bins."
  - Works for billing!
- But: the protocol advertises milliseconds
  - Good for initiator biflow matching [RFC 5103]…
  - …or approximate passive RTT…
- …So let's try it anyway.

Overview

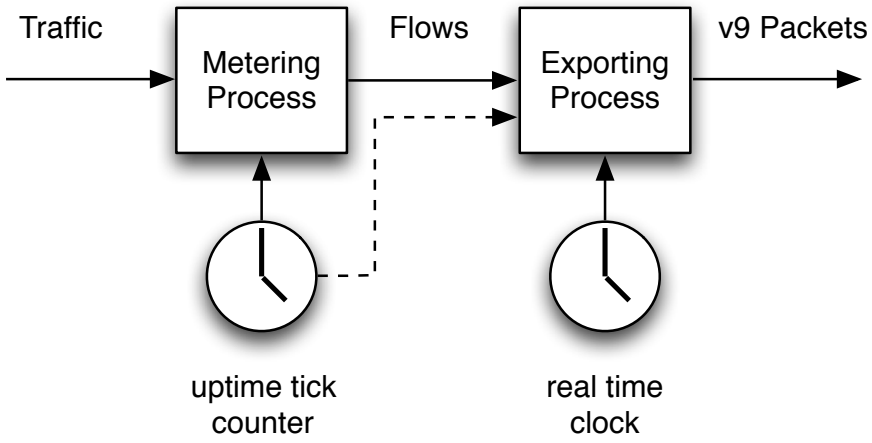
- Timing in NetFlow v9
  - How it works
  - How it breaks
- Basetime distribution and correction
- Validation
- Conclusions

Acknowledgments

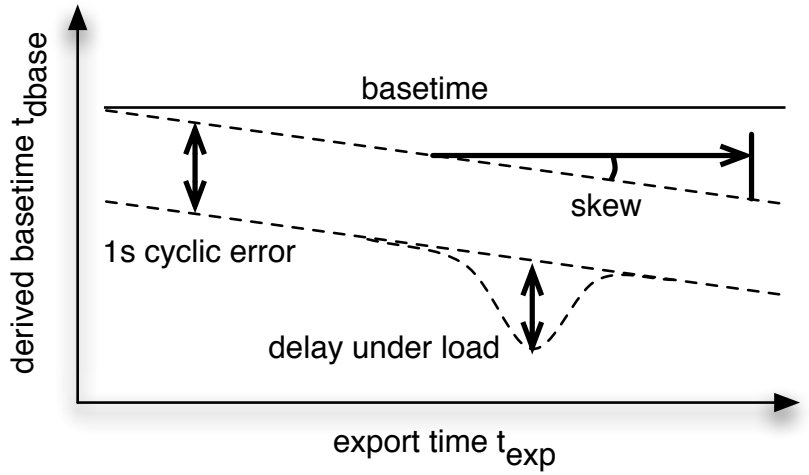
Thanks to the DEMONS project [http://fp7-demons.eu] for its support of this work, and to SWITCH for access to the dataset used in this study.

How does NetFlow timing work?

- Metering process generates flows, notes timestamps as *ticks* (timer interrupts since start)
- Export process ties ticks to real time with an *export timestamp* in epoch time

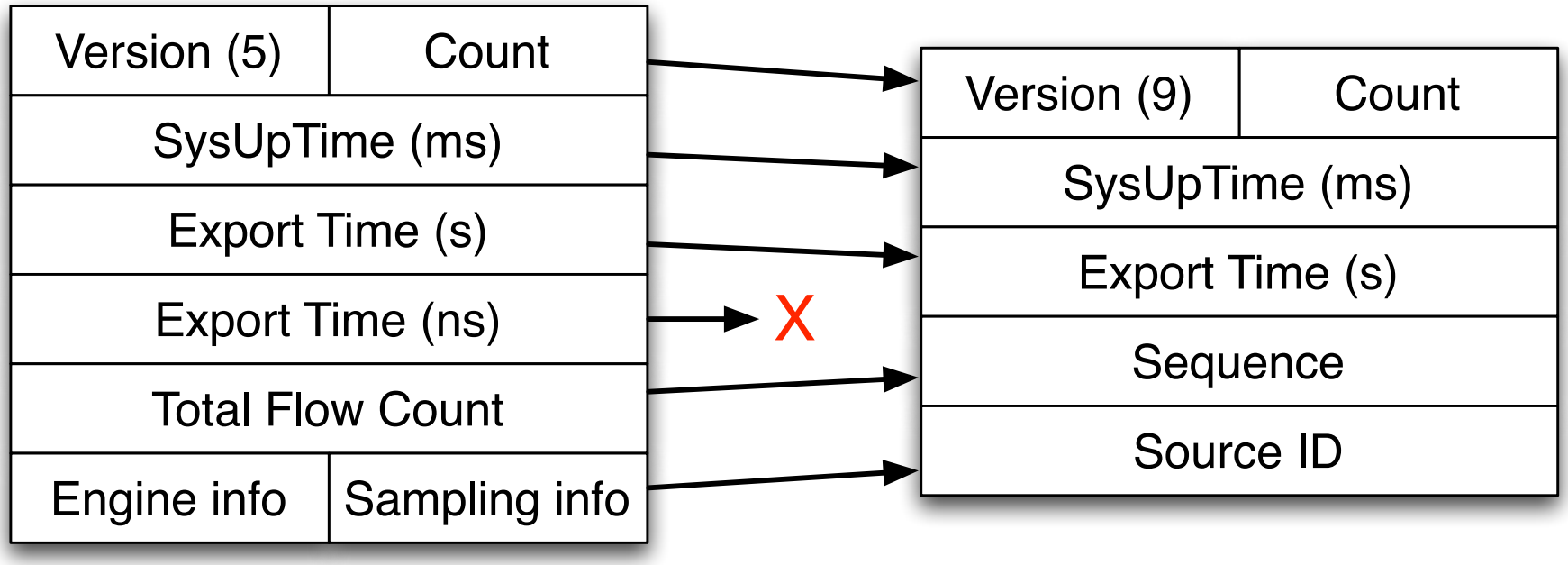


How does NetFlow timing break?



- Flow timestamps in ticks converted to real time by adding a *basetime* (i.e. real time of tick 0)
- Export clock and tick counter not in sync, leading to skew
- Export can be delayed
- Basetime export is *flawed by design*

Header evolution, v5 to v9



Cyclic basetime error

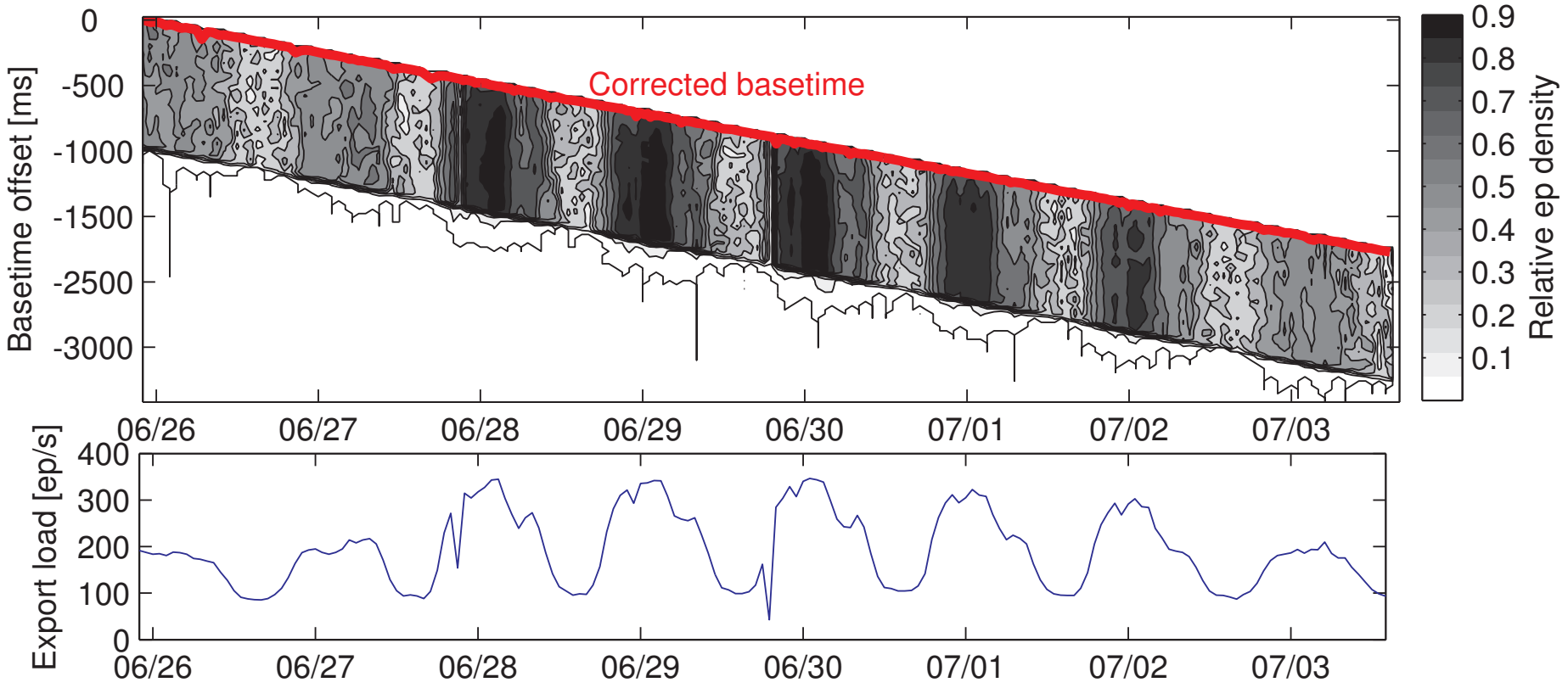
- Basetime can be independently derived from each export packet.
- NetFlow v9 header truncates nanoseconds portion of export time, present in v5.
- → Up to one second of error, repeating

$$t_{base} = t_{export} + t_{uptime}$$

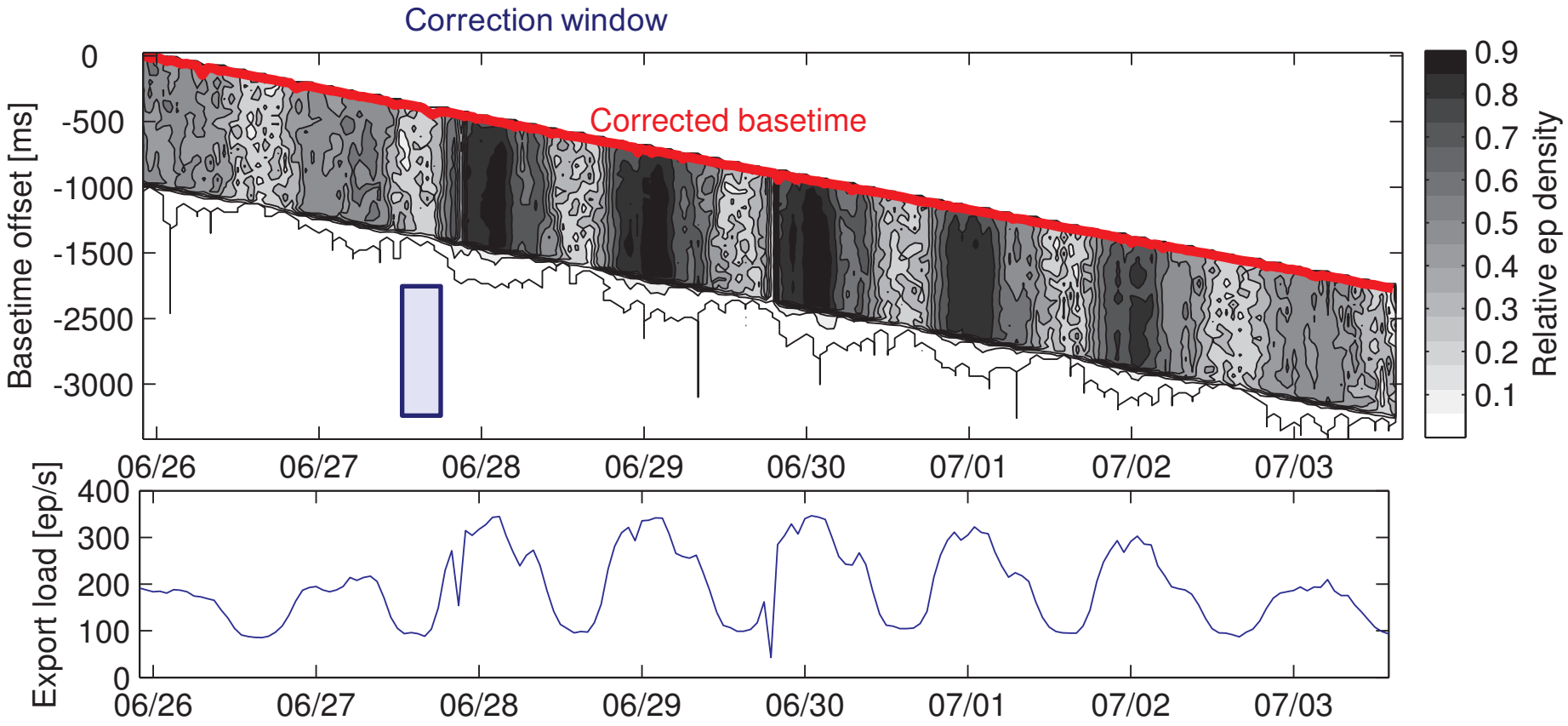
$$t_{base} = \lfloor t_{export} \rfloor + t_{uptime}$$

$$E_{cyclic} = \lfloor t_{export} \rfloor - t_{export}$$

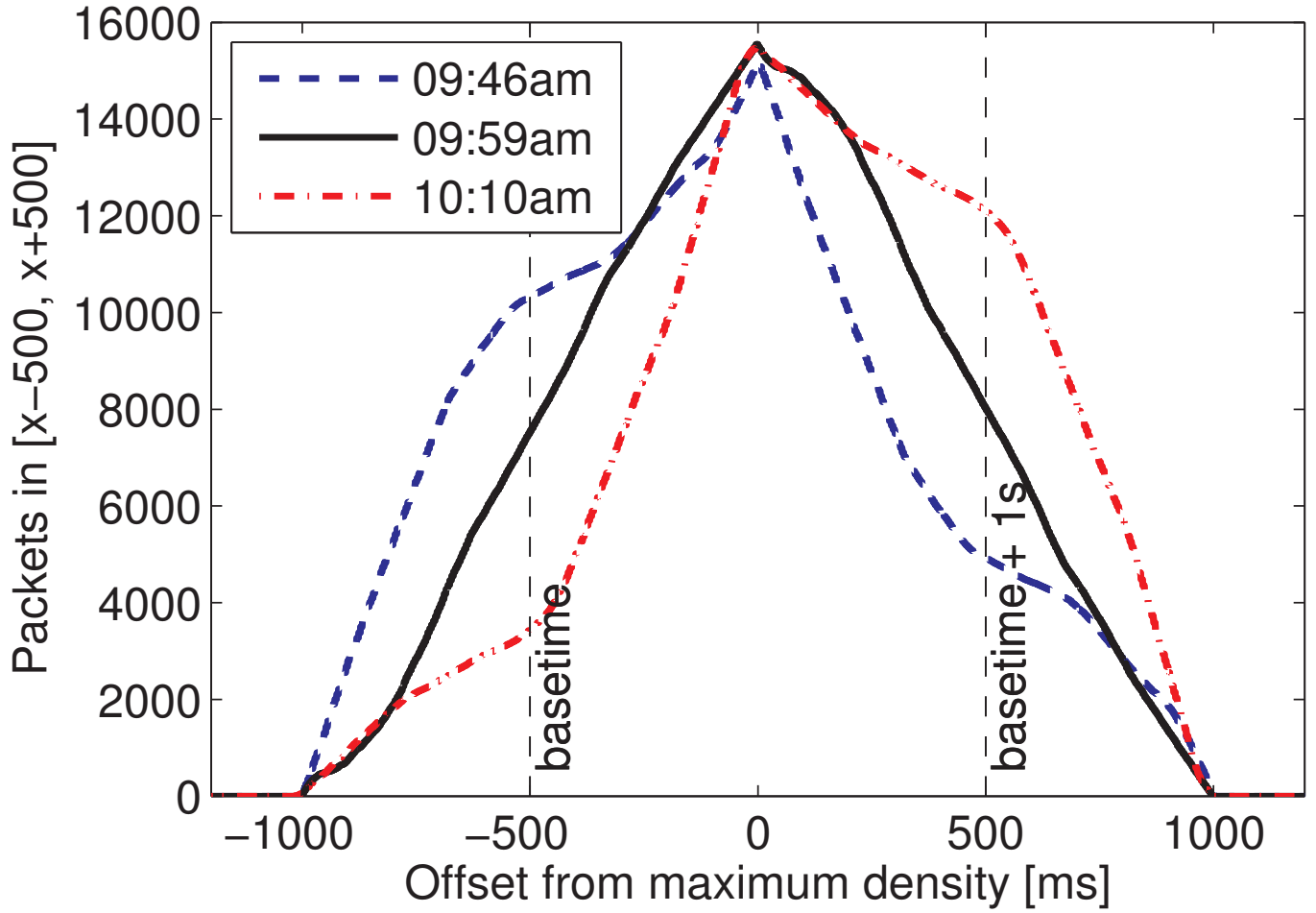
Basetime distribution



Basetime correction

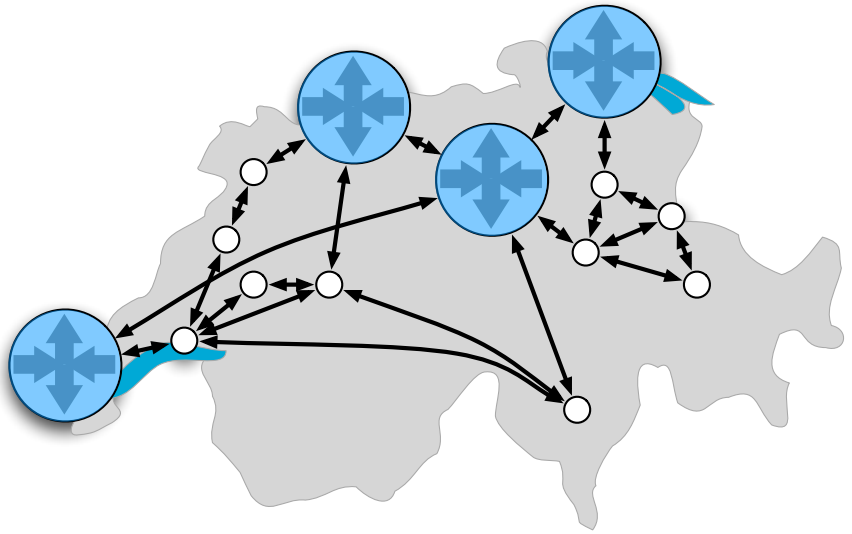


Basetime correction



SWITCH flow data repository

- Swiss Research and Education Network
- ~2¼M addresses (IPv4)
- Unsampled v9 from 6 border routers at 4 POPs
  - Cisco 6500, 7600
- Stored as raw v9 packet stream, .bz2



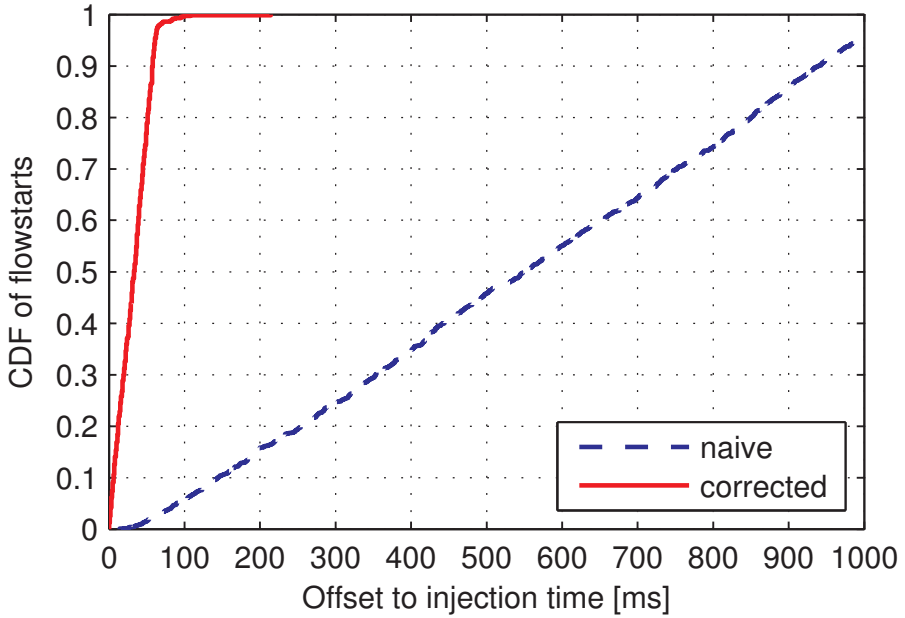
SWITCH
Serving Swiss Universities

Validation

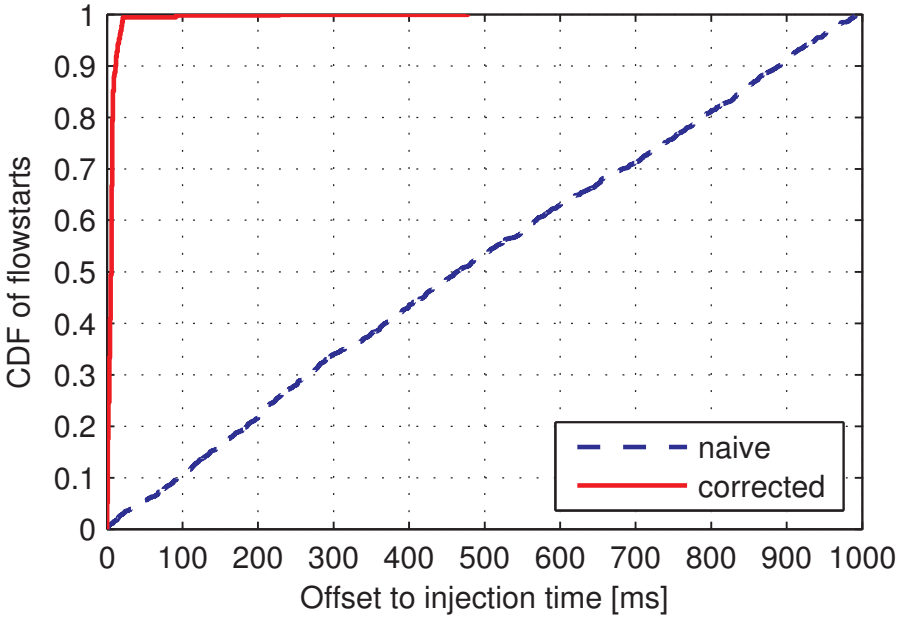
- Injection of known single-packet flows to known hosts via known routes over the SWITCH network
- Comparison of known timing to flow timestamps using uncorrected and corrected basetimes
- Comparison to non-Cisco implementation on an experimental local network

Validation

Cisco (SWITCH)



softflowd



Conclusions

- NetFlow v9…
  - …advertises 1ms accuracy, delivers 1s accuracy
  - …correctable to ~1ms accuracy in general case
  - …***but*** only correctable to ~64ms accuracy on Cisco
    - Insufficient for RFC 5103 biflows, insufficient for passive RTT.
  - ∴ for precision timing, consider dedicated flow meters.
- Keeping raw data essential for research
  - This study used metadata that would be lost with conversion to another format.
  - Implementation details matter in network measurement.

Questions?

- trammell@tik.ee.ethz.ch