UNIVERSITY OF CAMBRIDGE

Empirical Analysis of Route Leaks

Dongting Yu, Ross Anderson
Computer Laboratory
University of Cambridge
Feb 9, 2011

Confirmed route leaks

- Spans 11 months
- Confirmed route leaks at a large IXP
- Also observe these leaks from three other IXPs on other continents (RIPE RIS data)

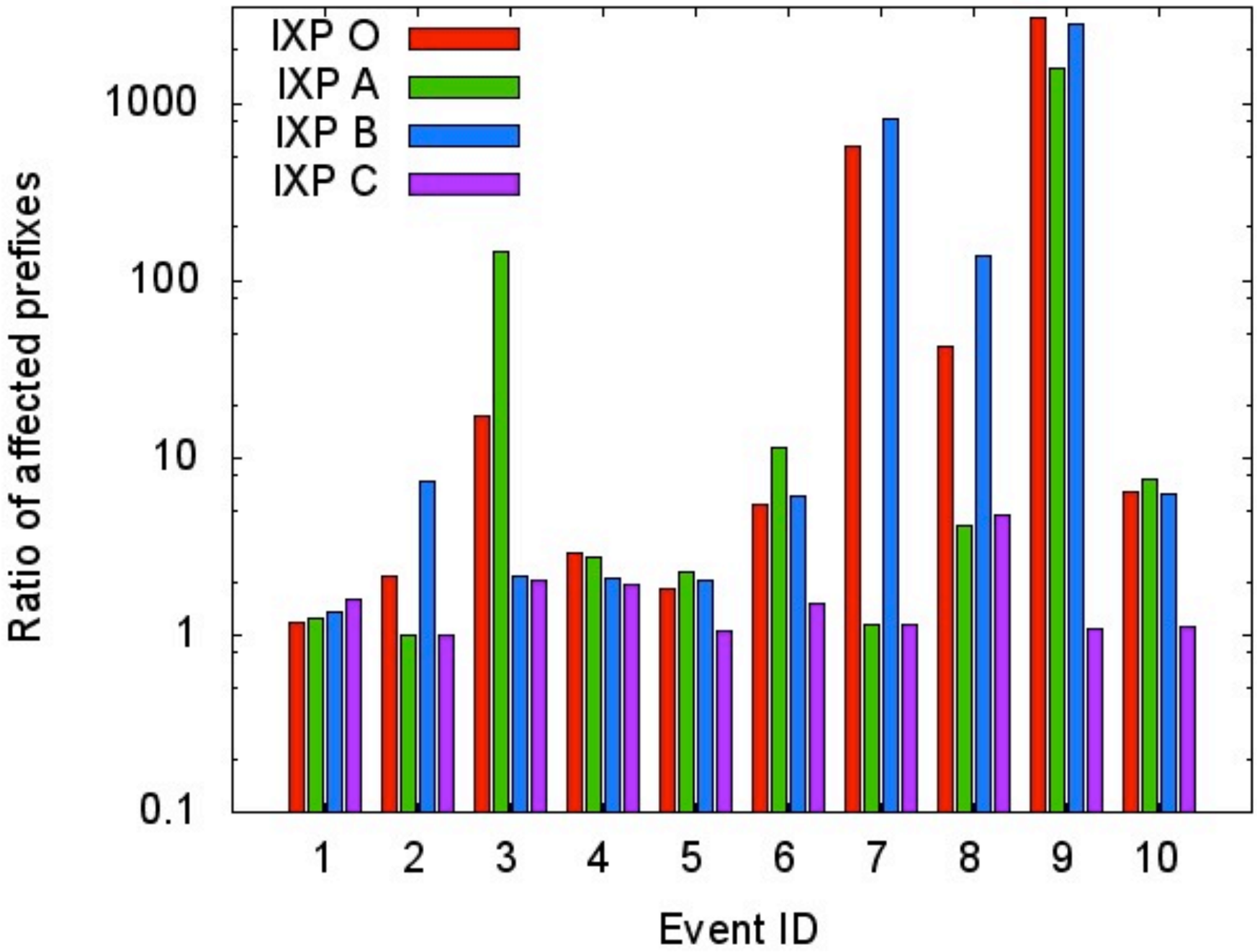
Findings

- 10 route leaks, about once a month
- These leaks generally follow same patterns
- We only have control-plane data, so cannot know about reachability

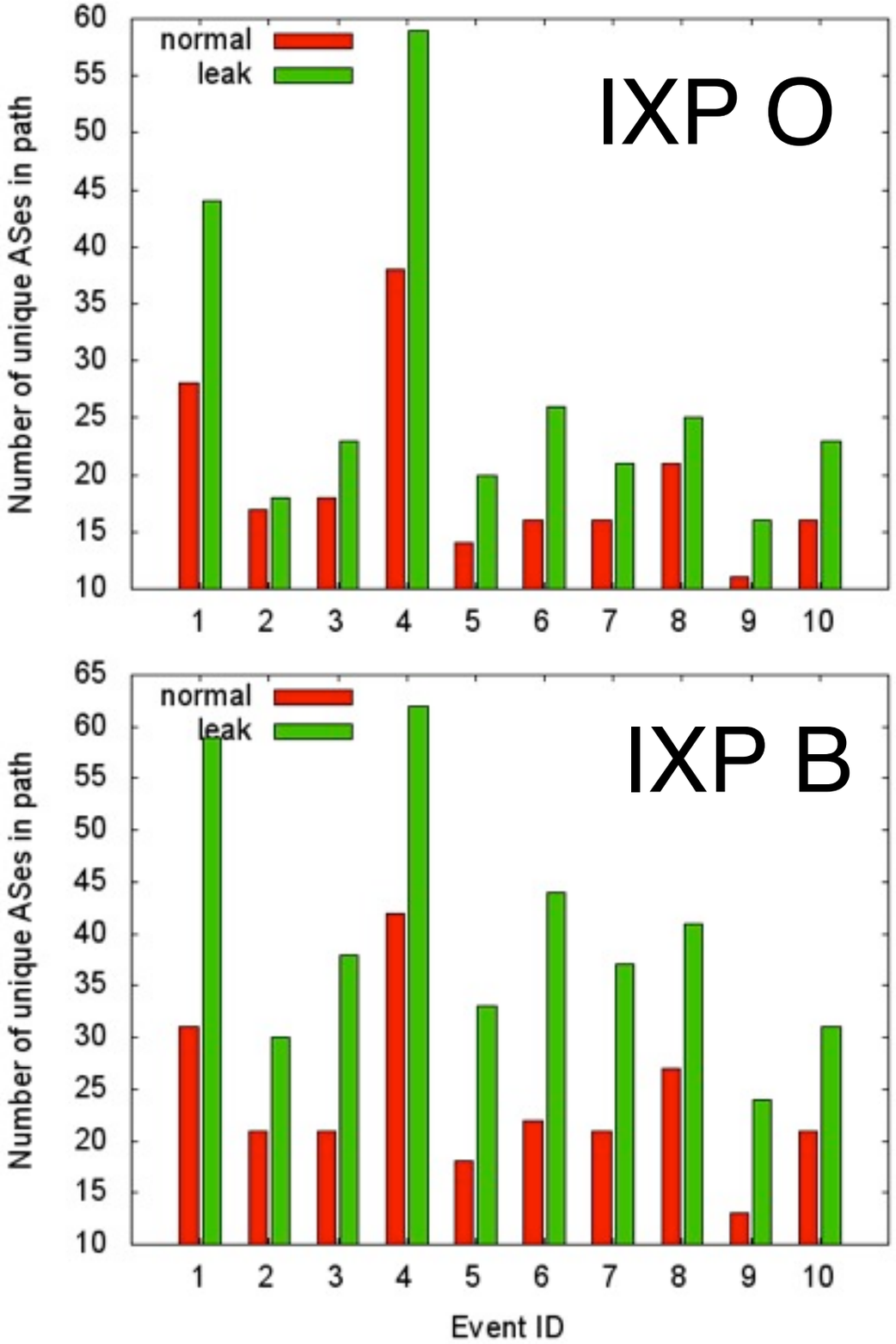
Findings

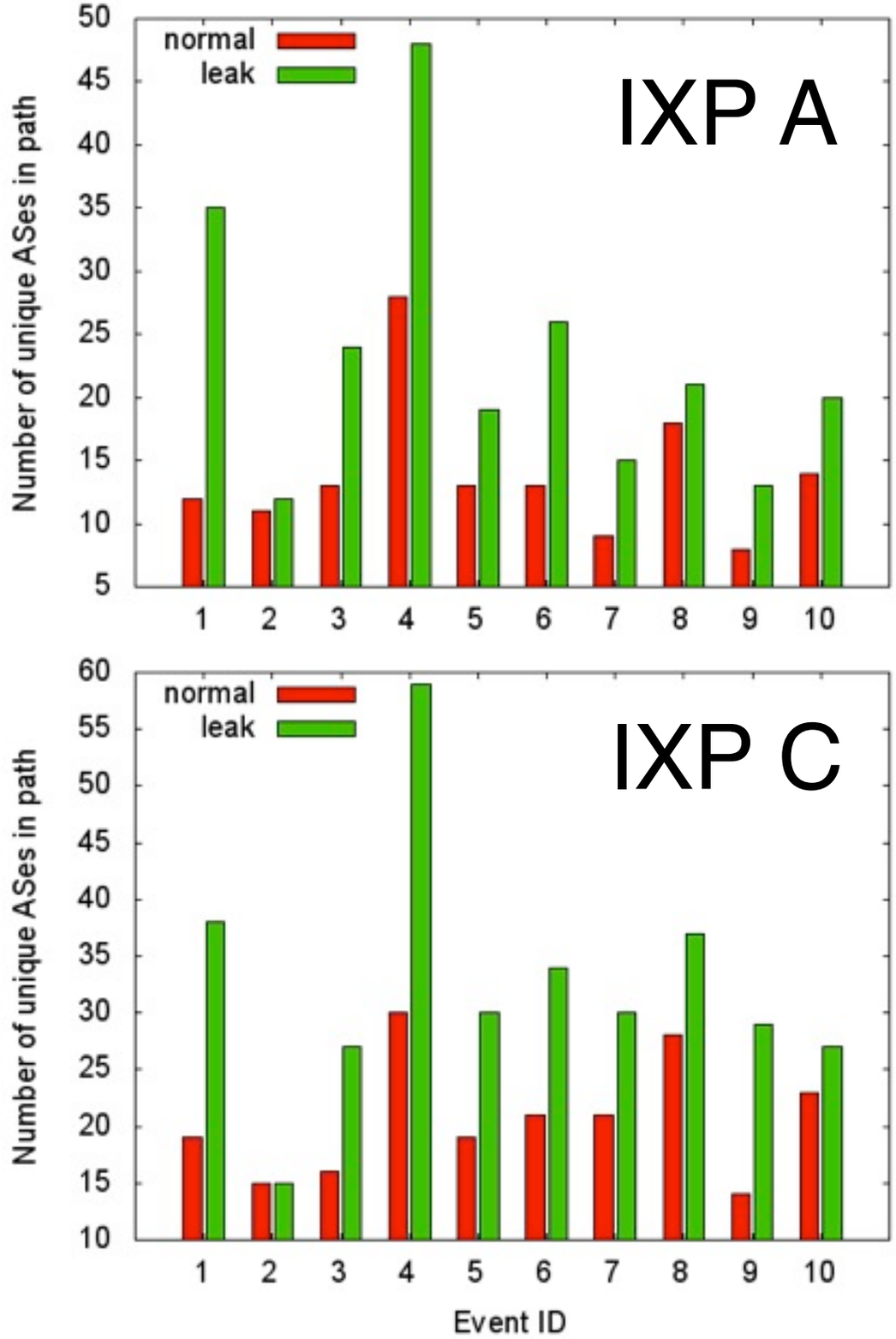
- Leaked prefixes are not originated by the leaker!
- We analyse by looking at affected prefixes and ASes
- IXP O is the originating IXP, the other three are A, B, and C.

Affected prefixes

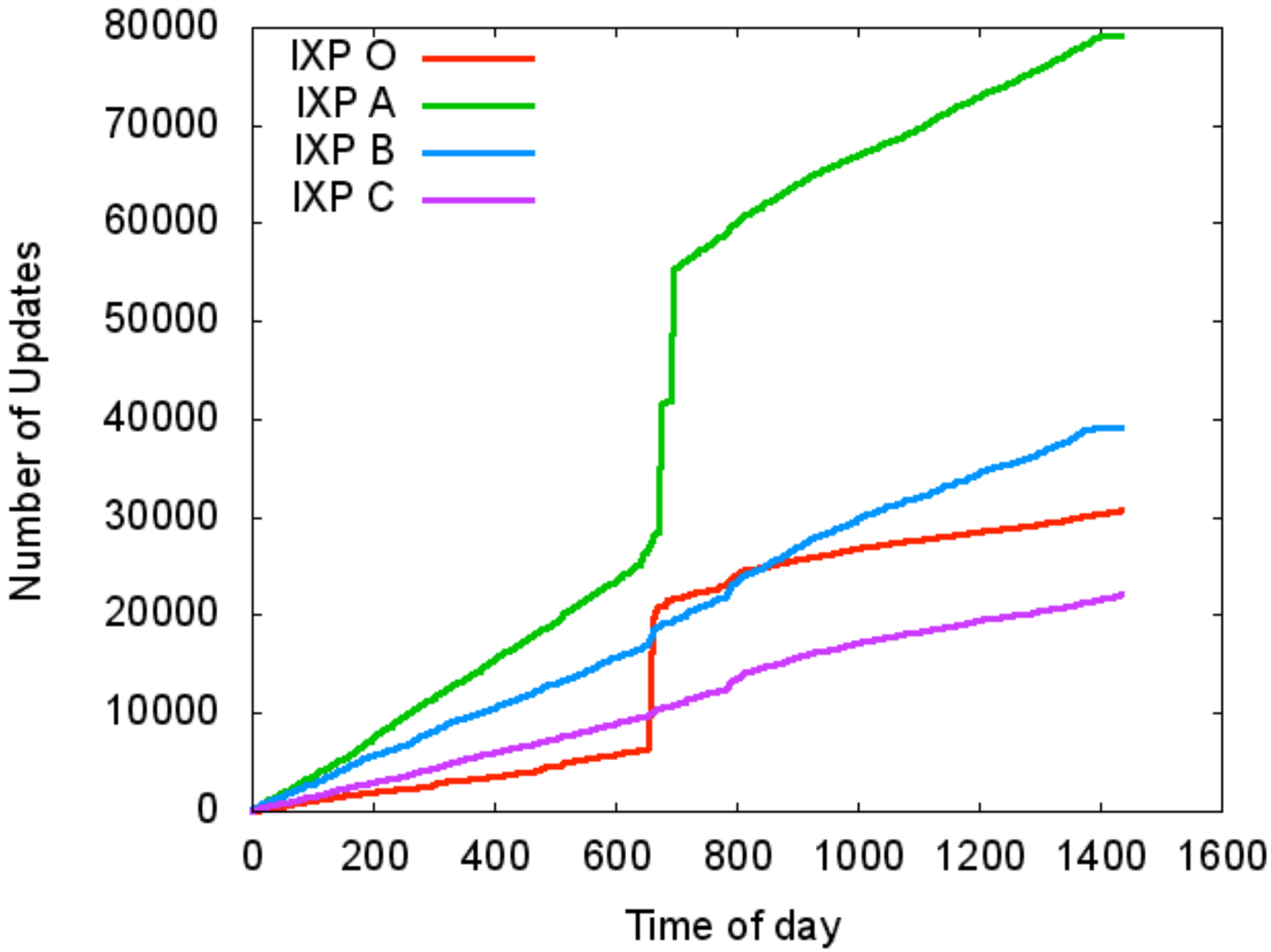


Affected ASes





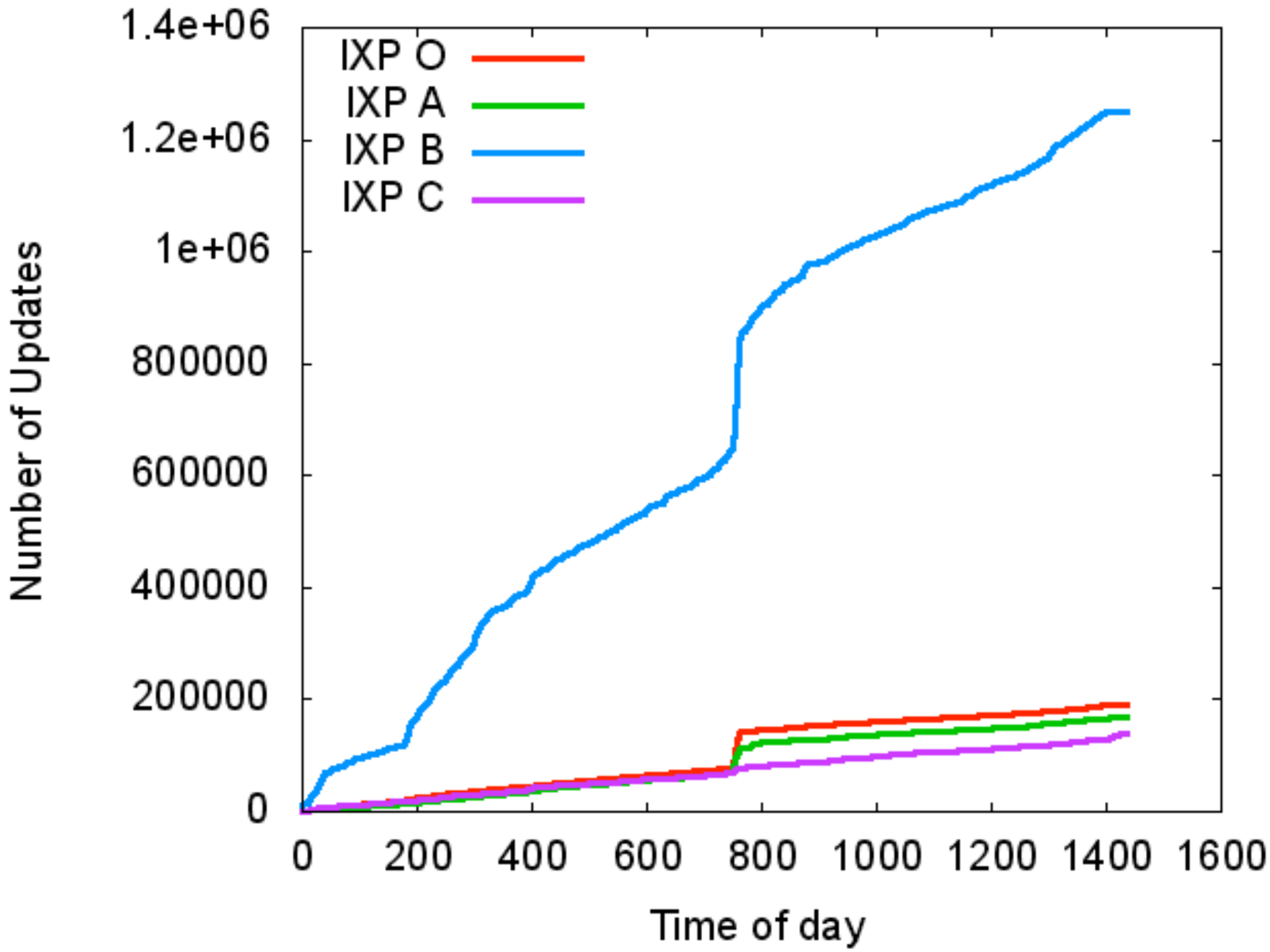
Update frequency of affected prefixes



Max 5-min interval: 13,283 updates

Event #3

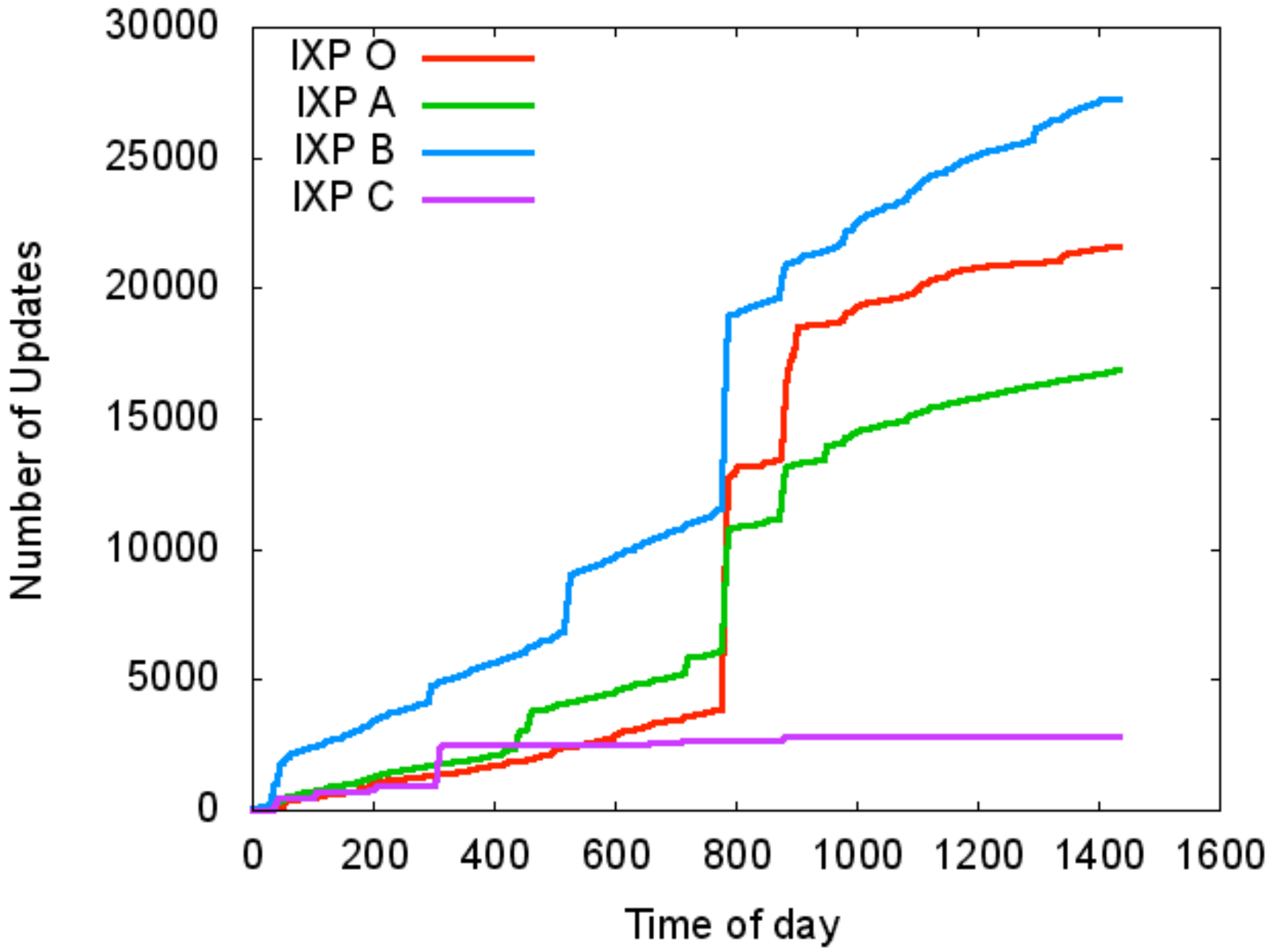
Update frequency of affected prefixes



Max 5-min interval: 142,827 updates

Event #4

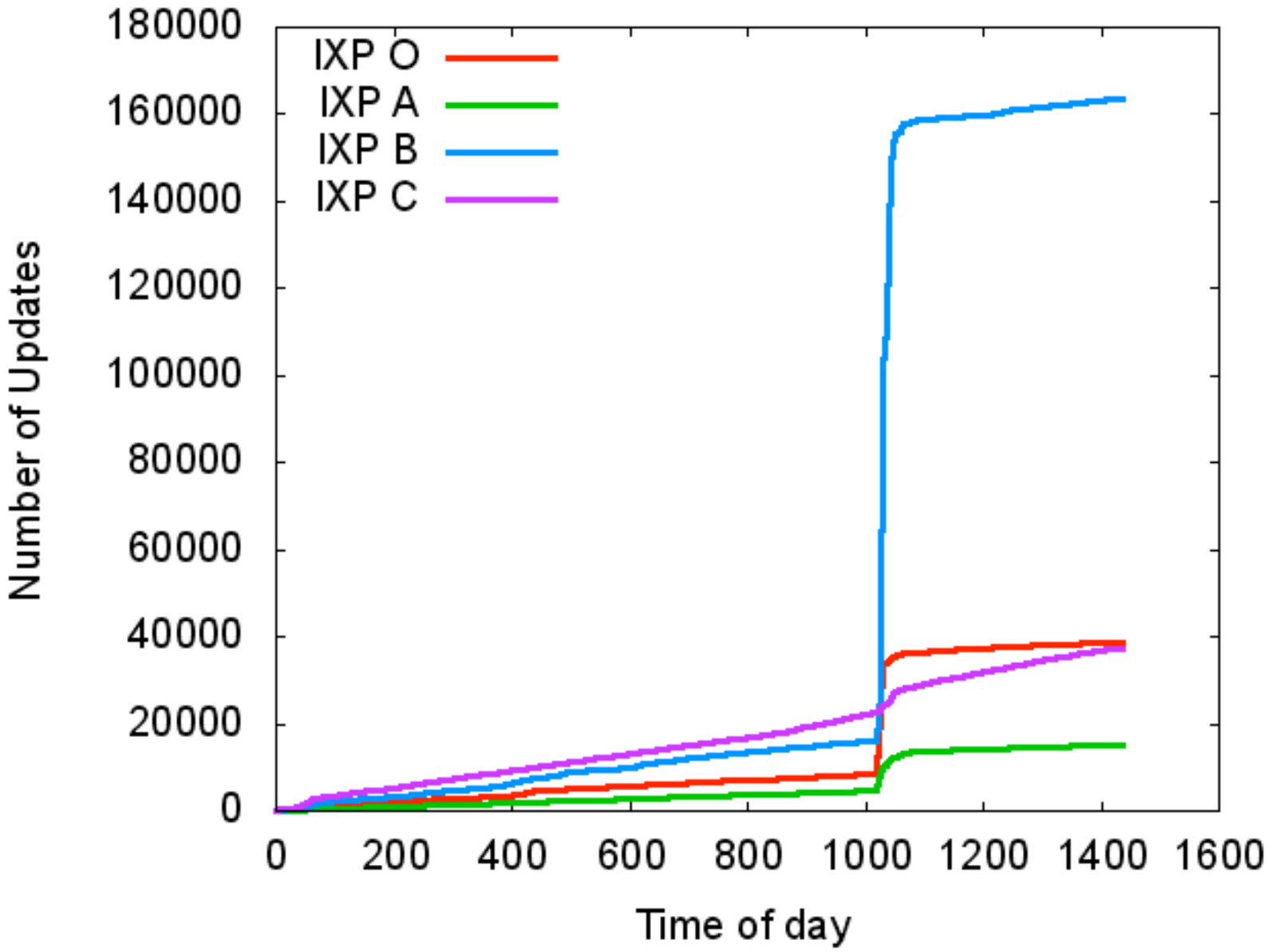
Update frequency of affected prefixes



Max 5-min interval: 4,537 updates

Event #5

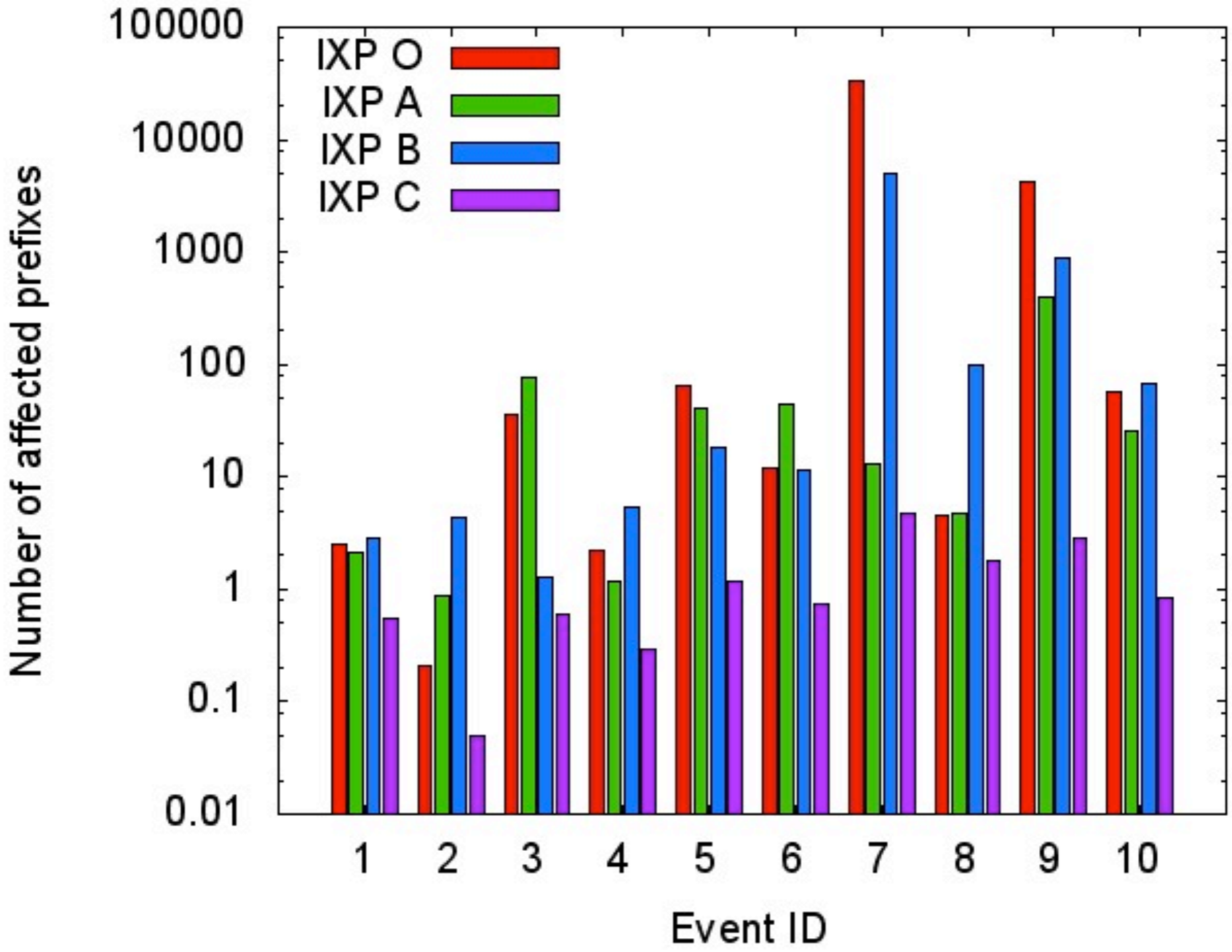
Update frequency of affected prefixes



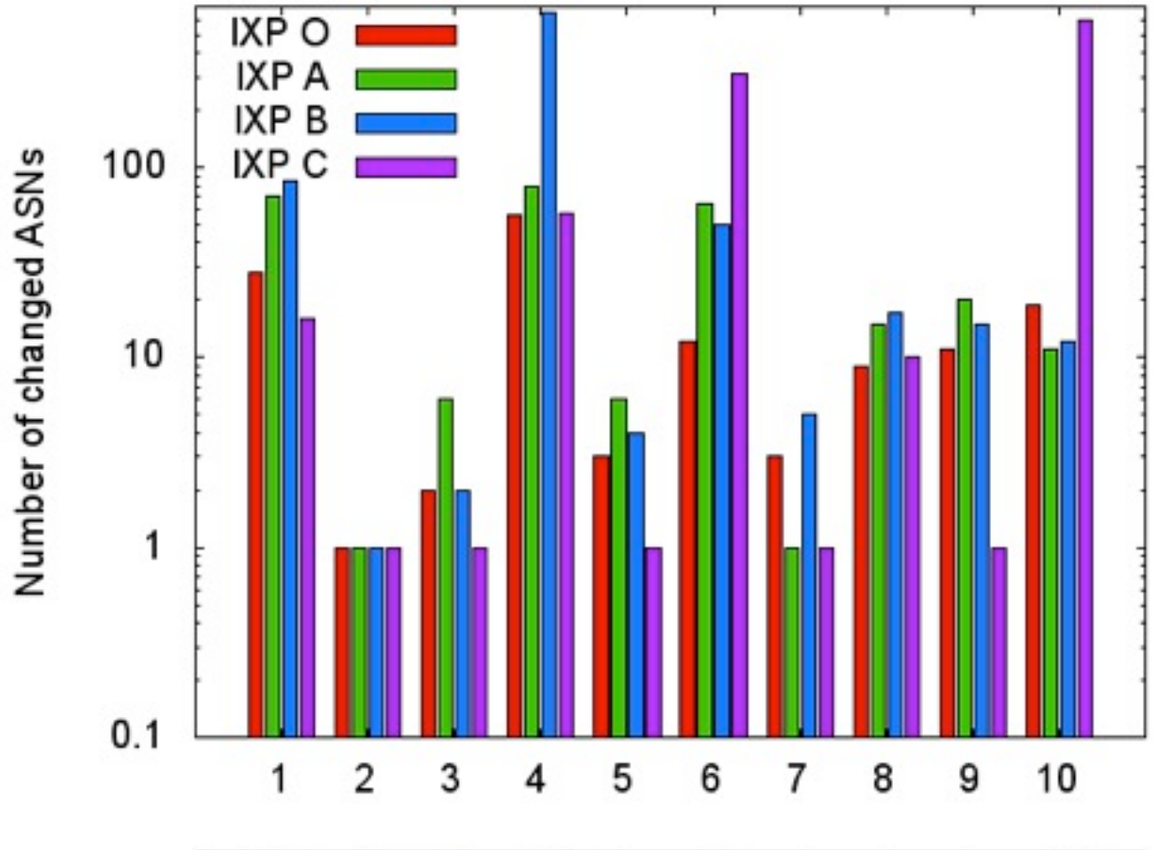
Max 5-min interval: 74,782 updates

Event #8

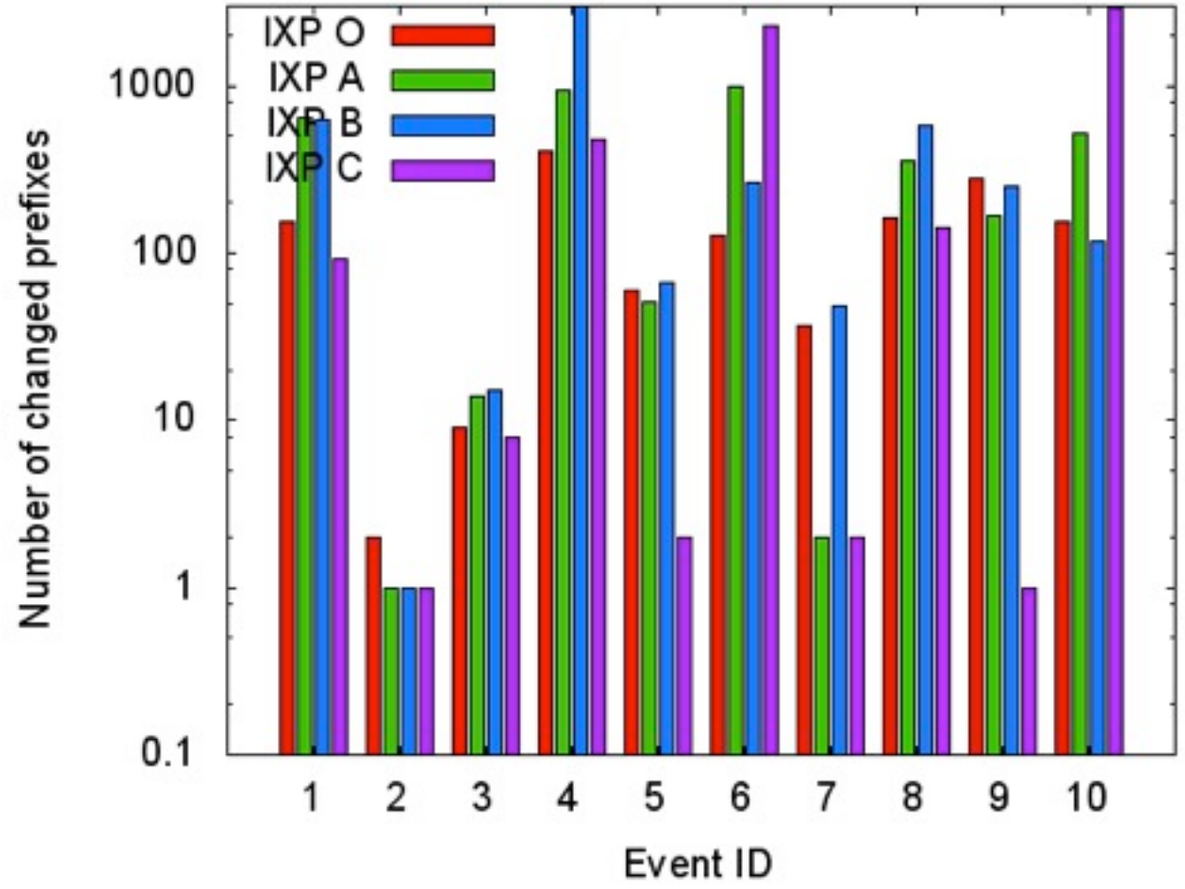
Peak 5-minute interval update frequencies



Number of ASNs that had their originated prefix changed



Number of prefixes that had their originating ASN changed



Discussion

- Transit (non)diversity
- Router performance during spikes

Thank you!

dongting.yu@cl.cam.ac.uk