SPEEDTRAP: INTERNET-SCALE IPV6 ALIAS RESOLUTION

Matthew Luckie, Robert Beverly*,
William Brinkmeyer*, k claffy
mjl@caida.org

CAIDA - University of California, San Diego
*Naval Postgraduate School

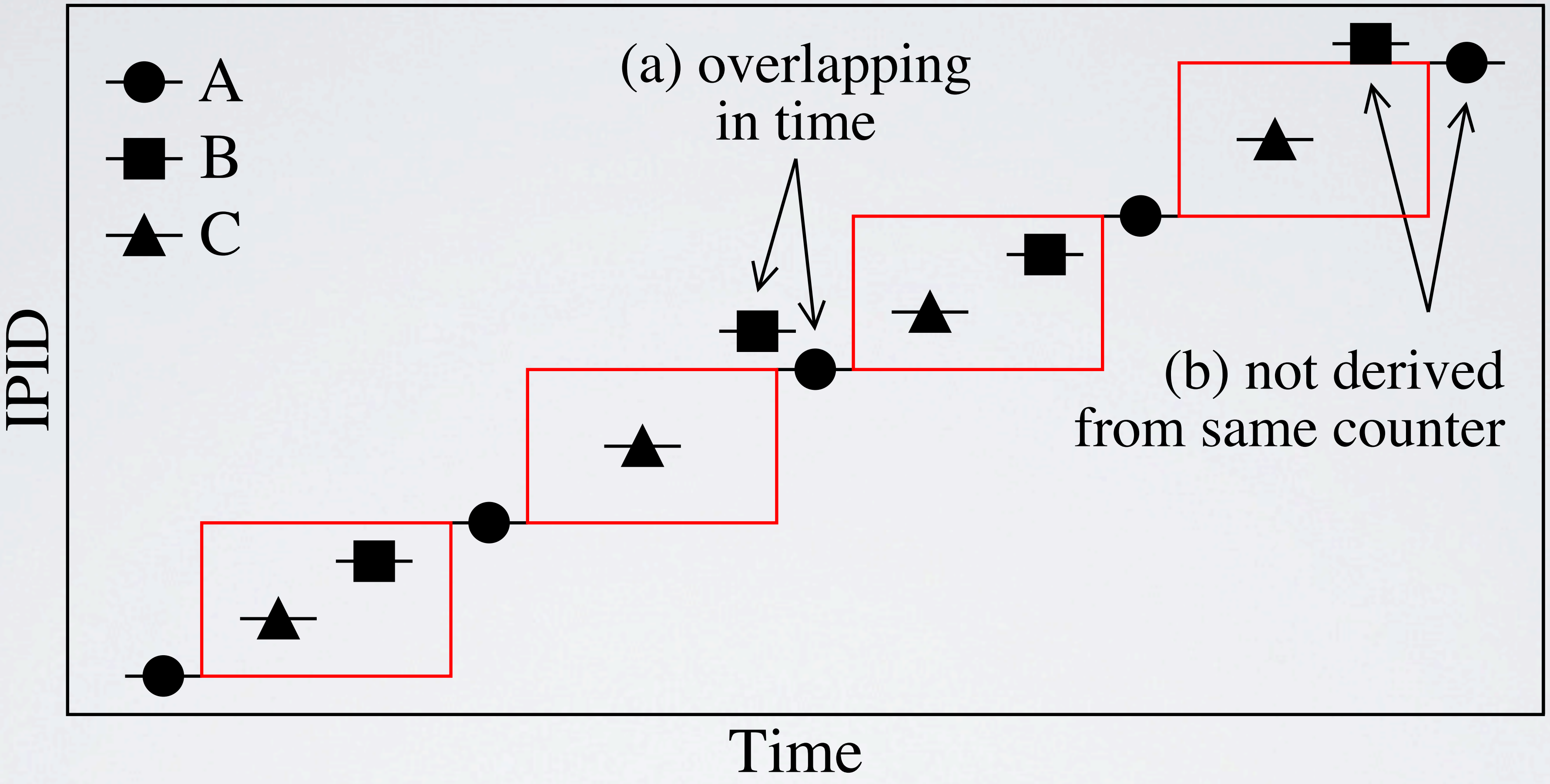
ACM SIGCOMM Internet Measurement Conference: Barcelona, Spain, Oct 2013

MOTIVATION

- How is the router-level structure of the IPv6 Internet evolving as IPv6 is deployed?
- Answering this question requires traceroute and alias resolution
- So far, no Internet-scale alias resolution technique for IPv6 exists
- *Speedtrap* is a step in this direction
  - we use IP-ID to fingerprint IPv6 routers
  - try to send the minimum number of packets given lack of counter velocity
- Related work in IPv4 (Mercator, DisCarte, RadarGun, MIDAR) does not apply
  - Common source address IPv4 hack is ruled out by IPv6 RFCs
  - All IPv6 IDs have similar offset and velocity given lack of counter movement

MONOTONIC BOUNDS TEST

(MBT, from MIDAR [ToN 2013])



- MBT suggests A and C share an IP-ID counter
- A and B do not share a counter

OBTAINING IPV6 IP-IDS

- The IPv6 header does not include an ID field
- We exploit IPv6 fragmentation behaviour (packets are fragmented only at the source) using the ID field in the IPv6 fragmentation header
- **Too-Big-Trick**:
  - Send 1300B ICMP echo request.
  - If echo reply > 1280B, send Packet Too Big (PTB)
  - Host should respond to further echo requests with fragmented echo replies with IP-ID until Path-MTU cache entry expires (typically >= 2hrs)

DATA

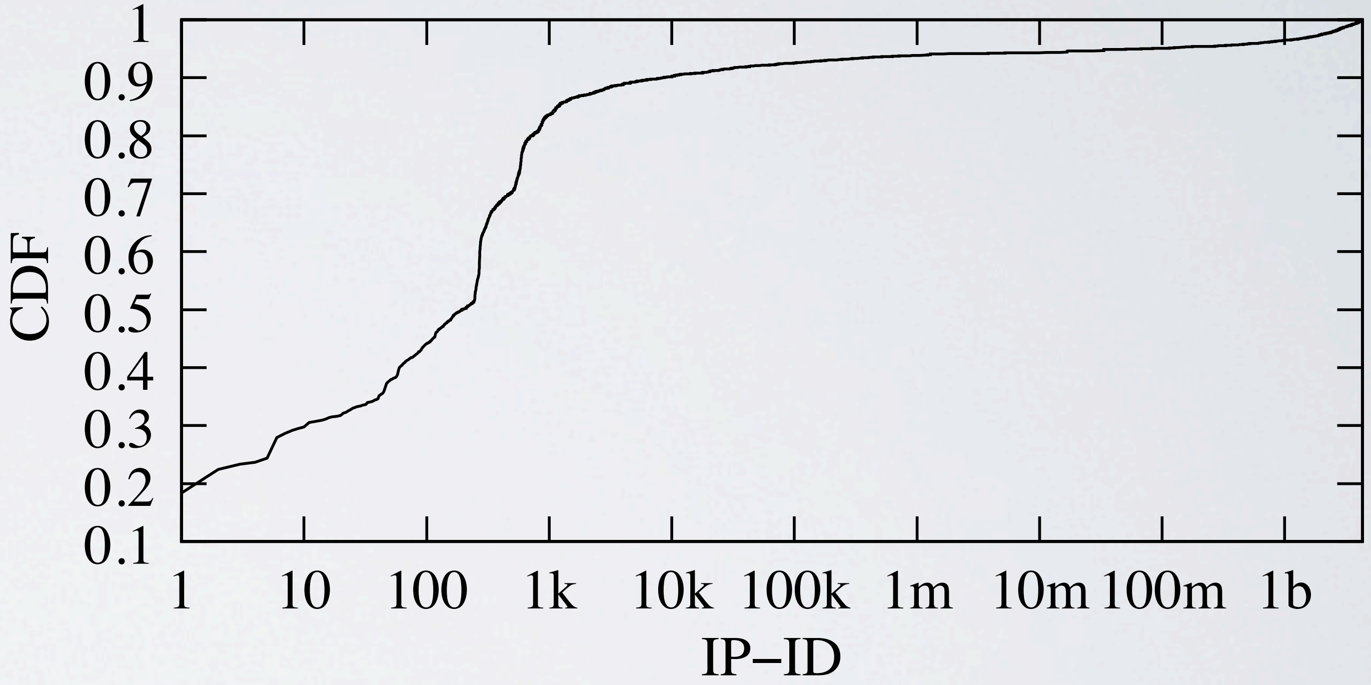
(input)

- All IPv6 interfaces observed by CAIDA's Archipelago (Ark) infrastructure for March 2013.
  - 27 VPs probed random address in each routed prefix, once per day
  - 52,986 interfaces in 2000::/3 unicast prefix observed

CHALLENGES

(and limitations)

- **32.1%** of interfaces send fragmented responses with incrementing IP-ID values.
  - 17.9% send random IP-IDs
  - 30.2% do not respond to ping
  - 19.8% appear to ignore PTB



- **Little velocity**: fragment counters start at one, increment only when a fragmented packet is sent. Routers rarely send fragmented packets
- **Large packets required**: 1300B **46x** larger than equivalent packets in IPv4

SPEEDTRAP ALGORITHM

(induce IP-ID velocity to catch aliases)

- In absence of entropy, large packet requirement, try to infer aliases using minimum number of necessary probes.

- We use 20 PPS, but no reason not to use larger PPS

1. Determine IP-ID behaviour of interfaces

2. Solicit **sequence of non-overlapping fragments** from all interface-pairs (for **MBT**)

3. Distill candidate routers, **force distinct shared counters to diverge**

4. Pair-wise testing of candidate routers to confirm

SPEEDTRAP ALGORITHM

(step 2: solicit non-overlapping sequence)

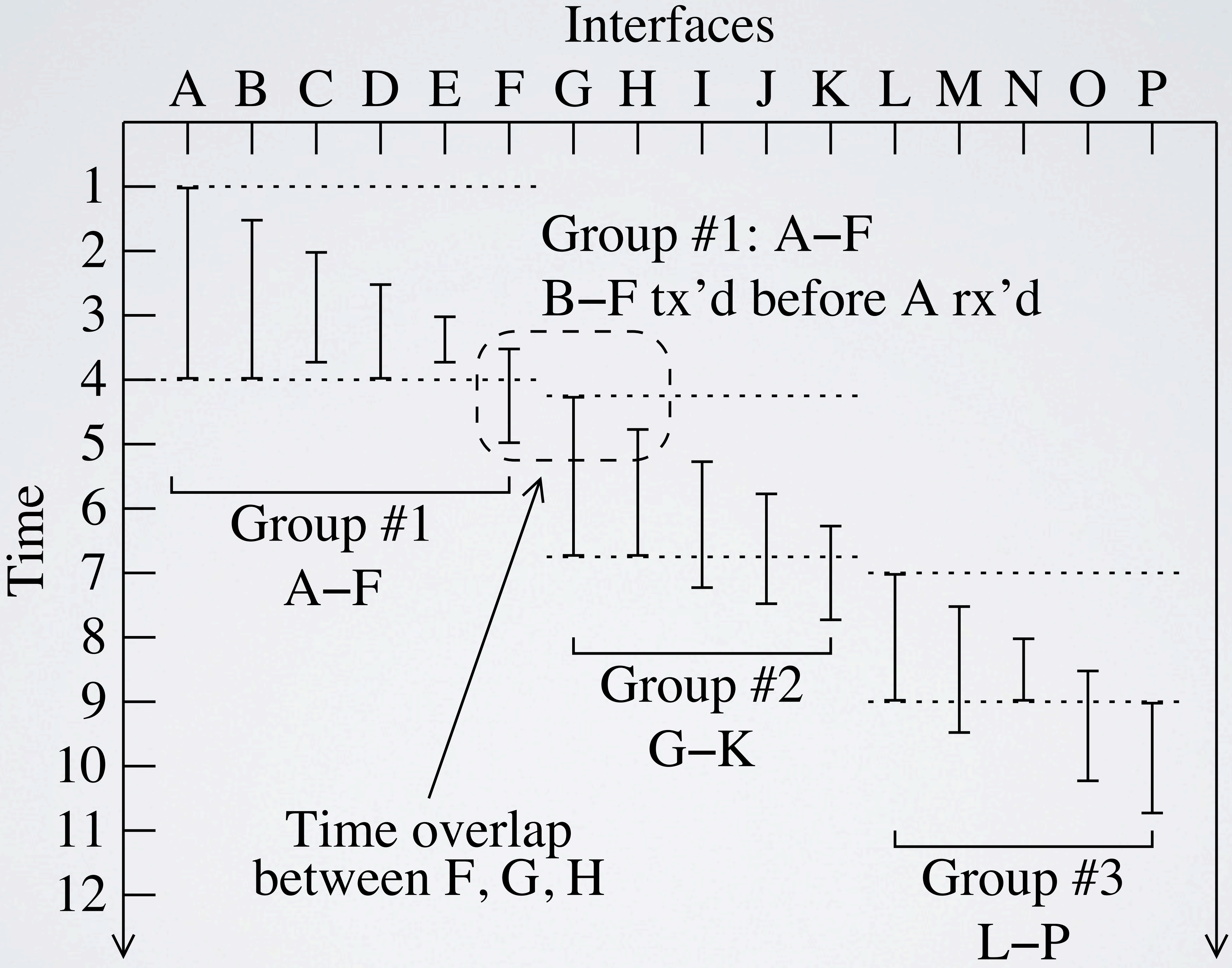
- Break step 2 into three rounds. Each round solicits a single fragmented response from each interface.

1. Solicit response from all incrementing interfaces, in parallel
2. Probe interfaces which had overlapping samples in step one separately. Probe groups in parallel.
3. Solicit response from all incrementing interfaces, in parallel

- Product is sequence of non-overlapping responses for MBT

SPEEDTRAP ALGORITHM

(step 2: solicit non-overlapping sequence, round 2)

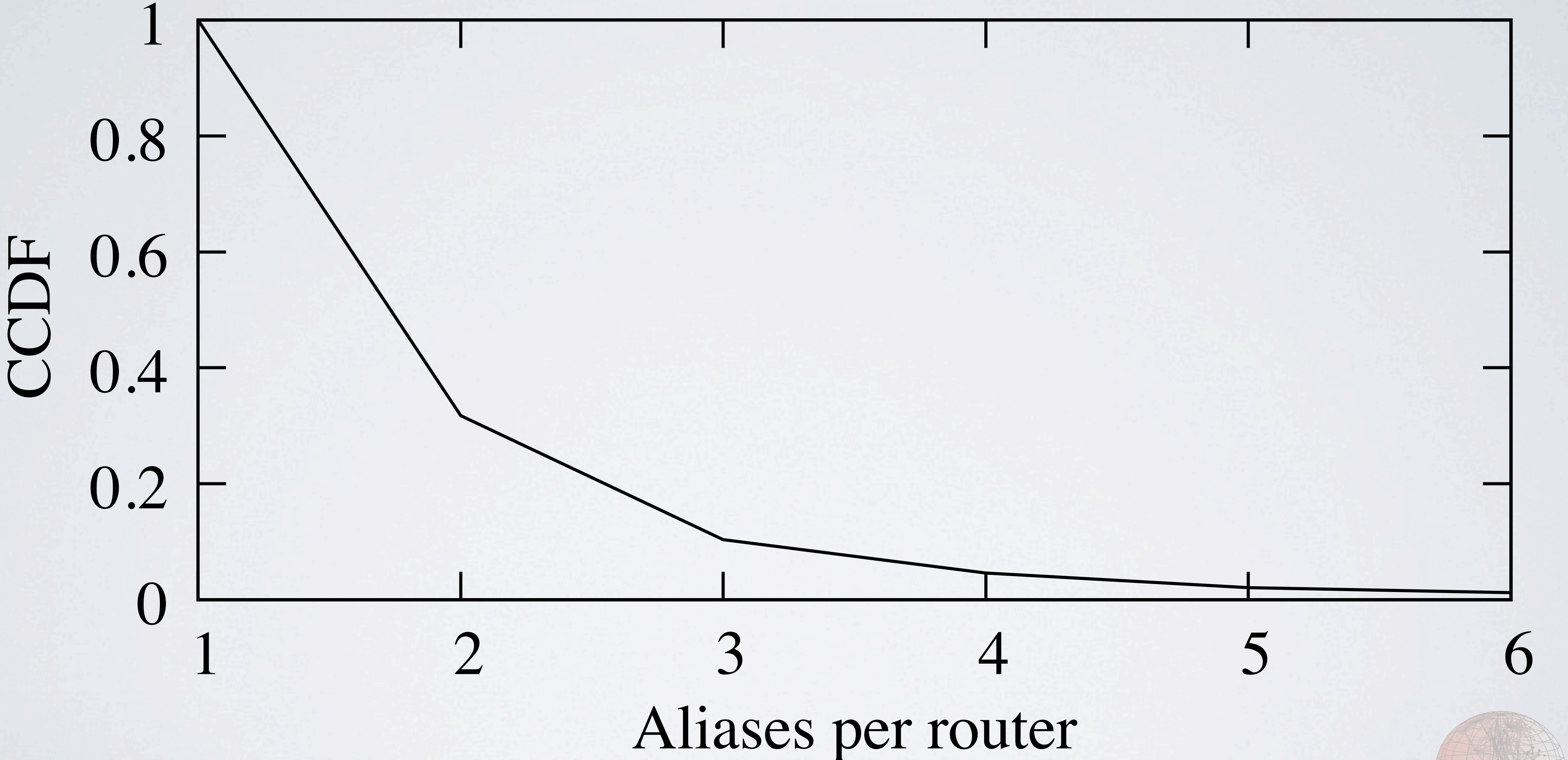


PACKETS AND TIME

(for 52,986 addresses at 20pps)

Step		Packets	Time
1	IPID behaviour	317,814	5:35:44
2	Non-overlapping sequence	80,017	1:15:31
3	Distill candidate routers	34,659	1:15:43
4	Pair-wise testing	63,765	1:01:12
Total:		496,255	9:08:10

ALIASES PER ROUTER



VALIDATION

(2% of inferred routers validated)

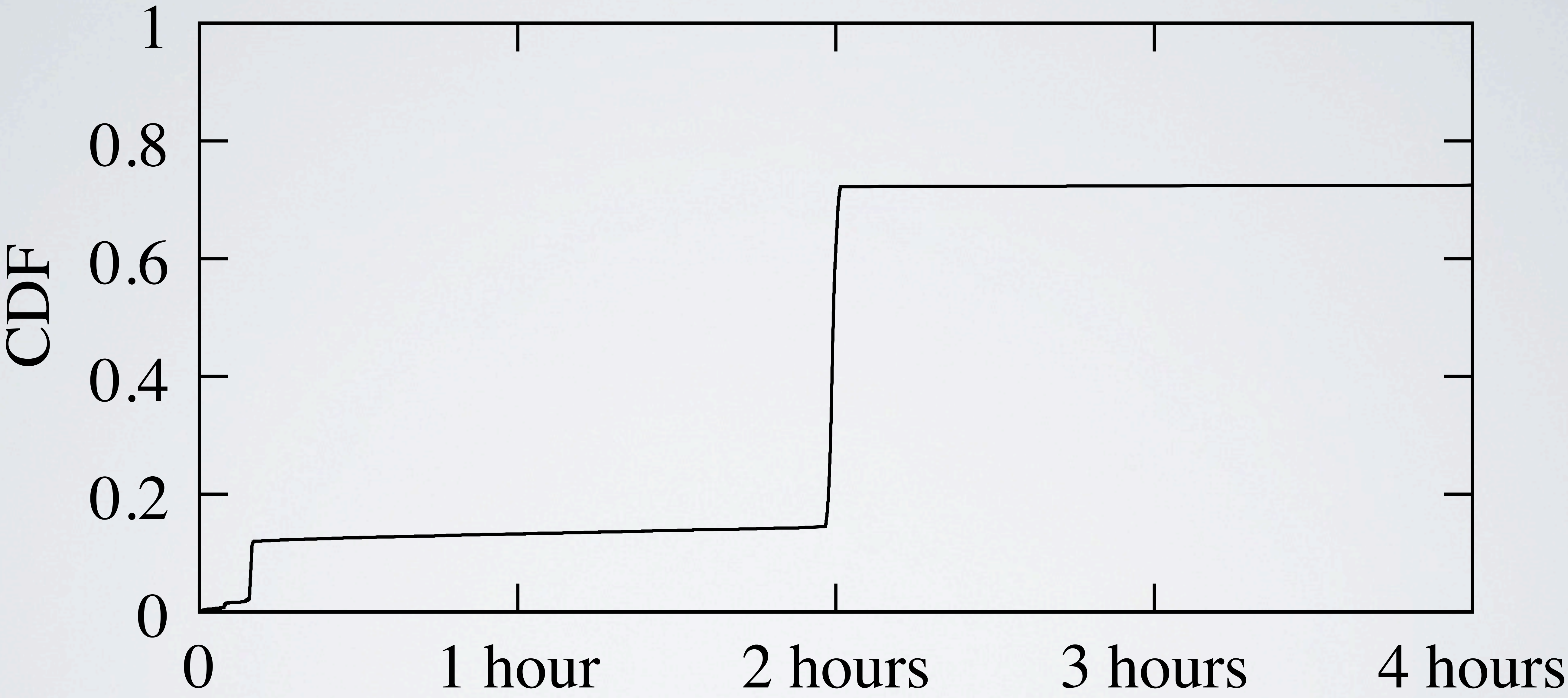
Validation name	STP-1	STP-2	AP	Tier1
Data source	RANCID	DNS	DNS	DNS
Routers				
Incrementing IPID	43	40	86	50
Random IPID		43	85	98
No Fragments		11	84	77
No Echo Replies			8	11
Mixed			4	3
Total Routers	70	94	267	239
Interfaces	151/750	85/279	138/1008	79/625
Correct	**150/151**	**85/85**	**137/138**	**79/79**

SUMMARY

- We developed and validated an Internet-scale IPv6 alias resolution technique
- **Code freely available**
  - http://www.caida.org/tools/measurement/scamper/
  - man sc_speedtrap
- Also in paper:
  - tomography of where PTBs might be filtered, allowing more aliases to be resolved
  - evaluation of scalability

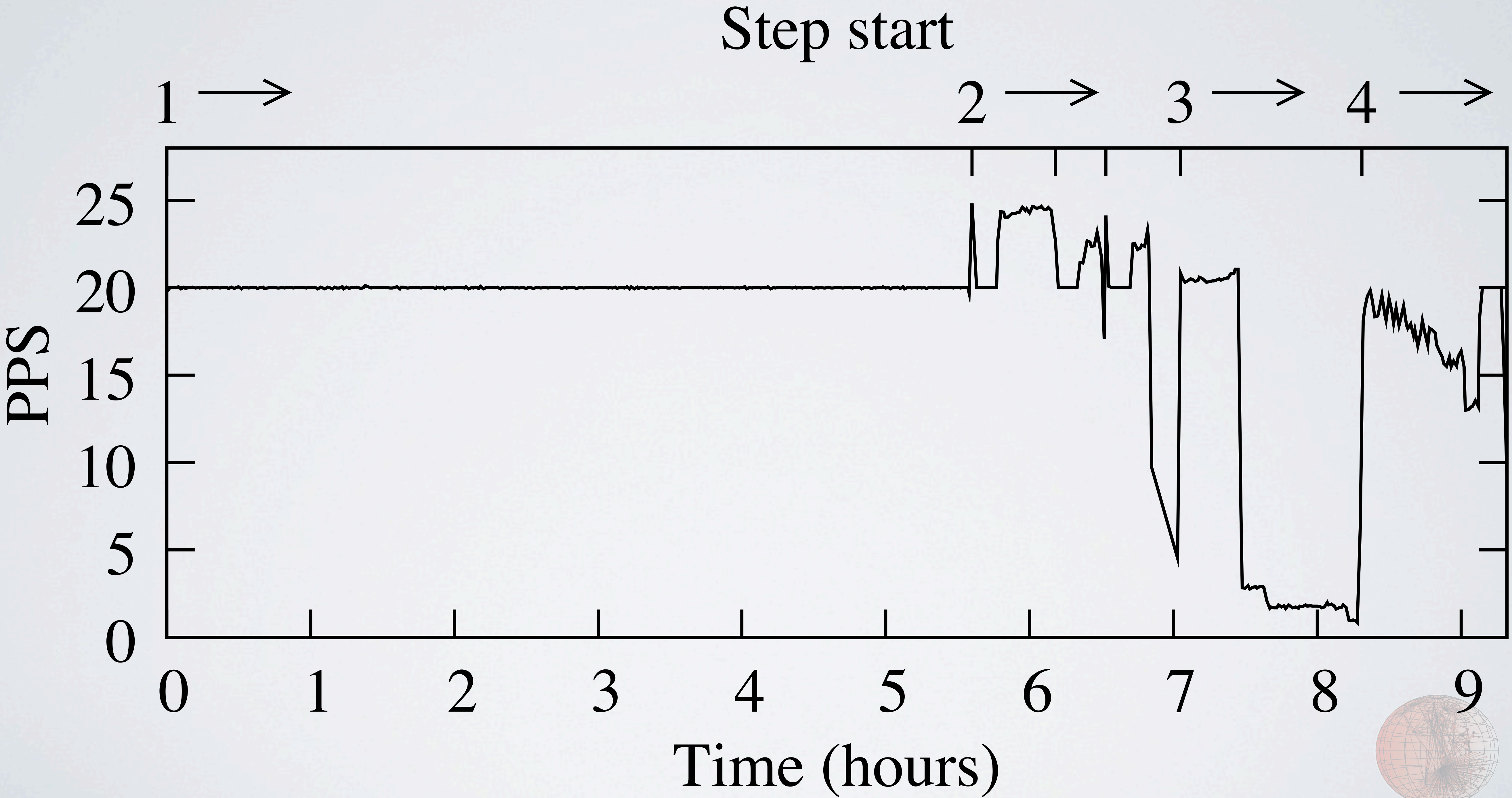
PMTU CACHE

(how long will routers fragment packets?)



PPS RATE

(are we limited by PPS rate or algorithm?)



RELATED WORK

(IPv4 fingerprinting techniques, $O(N^2)$)

- N. Spring, R. Mahajan, D. Wetherall, *"Measuring ISP topologies with Rocketfuel"*, ACM SIGCOMM 2002

Ally:
Infer IP-ID values for two addresses derive from single shared counter

- J. Sherry, E. Katz-Bassett, M. Pimenova, H.V. Madhyastha, T. Anderson, A. Krishnamurthy, *"Resolving IP aliases with pre-specified timestamps"*, ACM SIGCOMM IMC 2010.

Pre-specified IP Timestamp Option

RELATED WORK

(Scalable IPv4 fingerprinting techniques)

- R. Govindan, H. Tangmunarunkit, *"Heuristics for Internet map discovery"*, IEEE INFOCOM, 2000

Mercator:
Common Source Address
in ICMP Port Unreachables

- R. Sherwood, A. Bender, N. Spring, *"DisCarte: a disjunctive Internet cartographer"*, ACM SIGCOMM 2008

DisCarte:
Analytical + Record Route

- A. Bender, R. Sherwood, N. Spring, *"Fixing Ally's growing pains with velocity modeling"*, ACM SIGCOMM IMC 2008

RadarGun:
Probe addresses in M rounds.
Two addresses are aliases if
they produce a linear
timeseries and the
timeseries are within a
threshold

- K. Keys, Y. Hyun, M. Luckie, k claffy, *"Internet-scale IPv4 alias resolution with MIDAR"*, IEEE/ACM Transactions on Networking 2013

MIDAR:
Probe N addresses in a
sliding window according
to IP-ID velocity.
Two addresses are aliases
if they pass Monotonic
Bounds Test (MBT)