Large Scale IPv6 Alias Resolution

Matthew Luckie

Overview

- IP-ID based alias resolution techniques
  - IP-ID used in reassembly to identify fragments that belong to same packet.
  - Commonly implemented as a counter in IPv4 (and v6)
  - ally
  - radargun / midar
- Problems applying TBT to large-scale alias resolution
  - ~9000 interfaces in set with incrementing IP-ID
- Current status

Overview – Ally

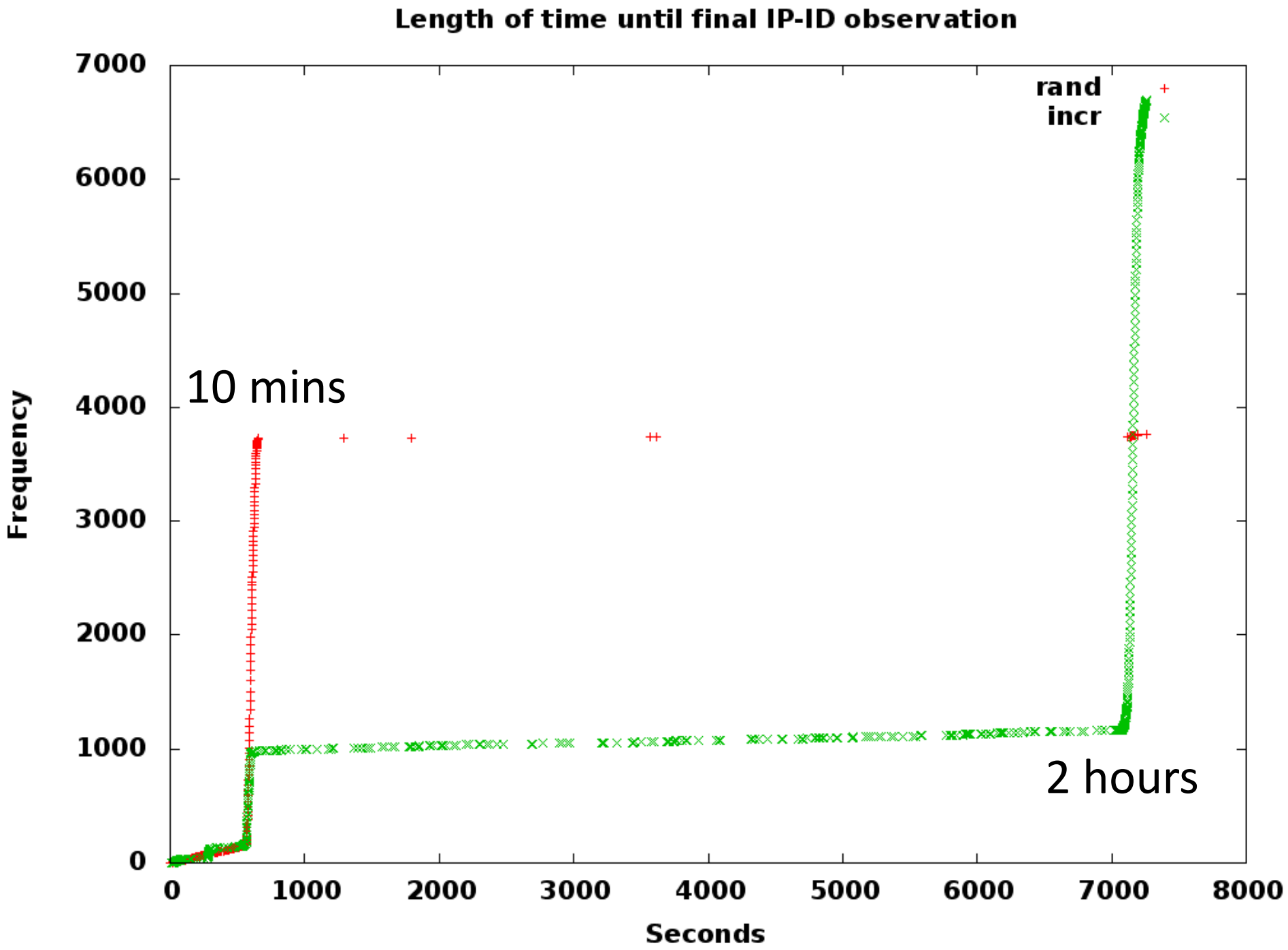
- Pairwise testing of candidate aliases.
  - Does not scale well, but useful to cross validate earlier measurements or confirm near-certain aliases
- Given interfaces X and Y
  - probe X, then Y, then X, then Y, then X
  - If an incrementing sequence of IP-ID values is returned, likely aliases.

Overview – Radargun / MIDAR

- Probe all interfaces in parallel and compute aliases offline.
- Radargun
  - aliases have similar velocities and IP-ID distance is within a fudge factor
- MIDAR
  - (a lot of algorithm to scale to millions of interfaces)
  - aliases return monotonically incrementing IP-ID values from non-overlapping probes

Issues applying Radargun / MIDAR with IPv6

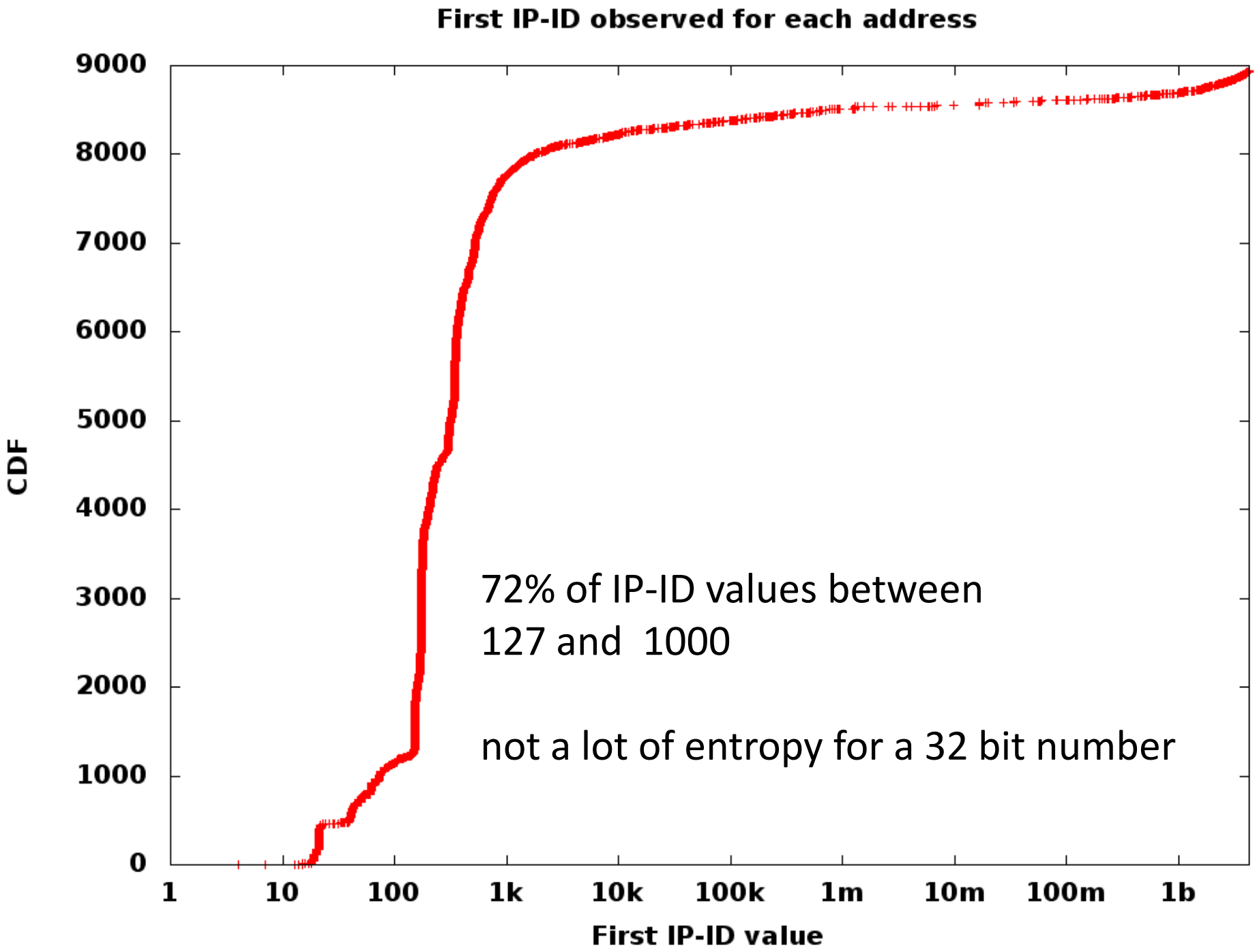
- Need to periodically send router PTBs so it will send fragments with IP-ID
- Need to solicit large responses so the router will fragment
  - IPv6 min MTU: 1280 bytes.
  - IPv4 probes are typically < 40 bytes
    - i.e. 30x smaller
  - Can solicit atomic fragments. TODO item.

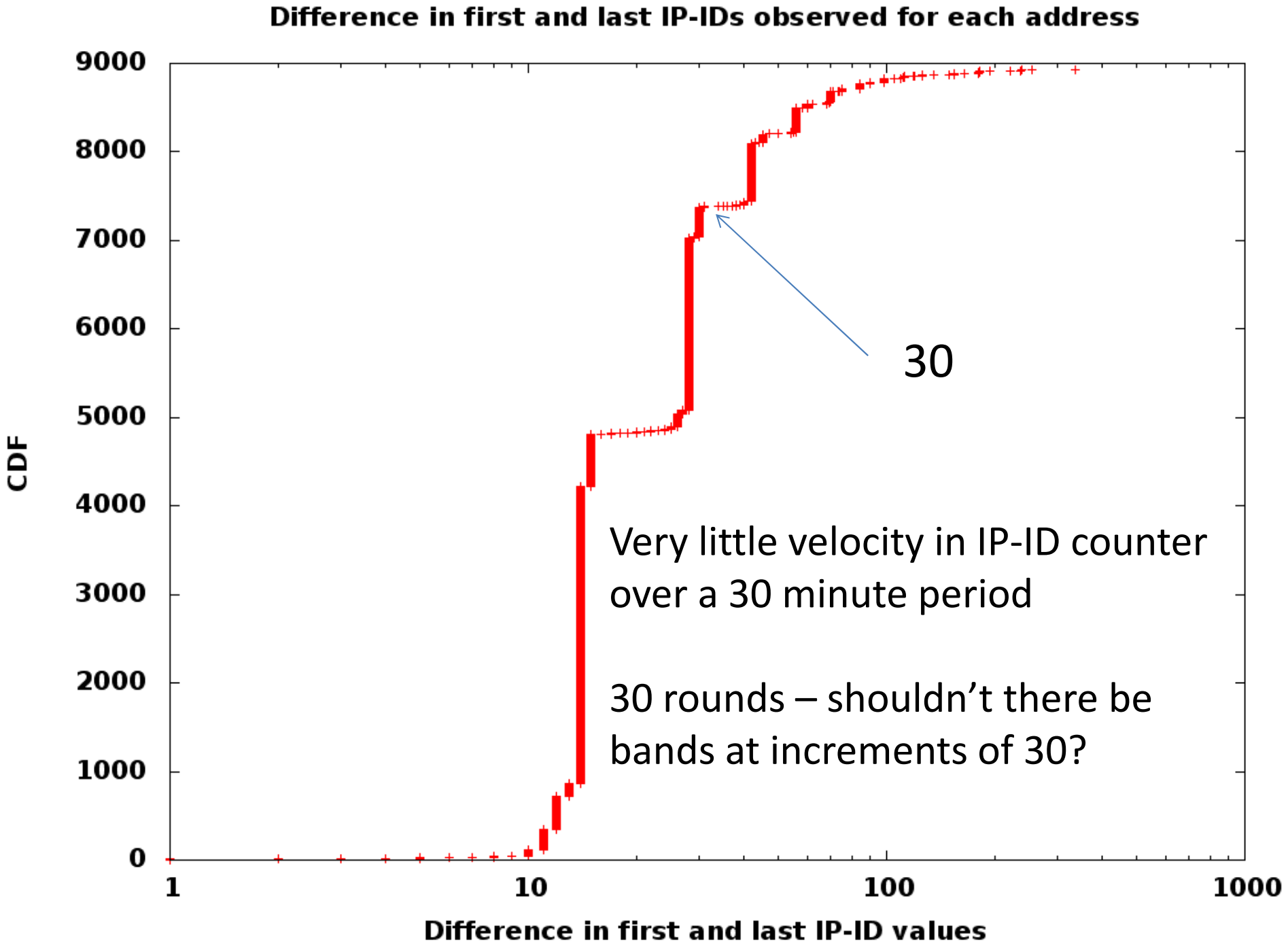

Length of time until final IP-ID observation
rand
incr
10 mins
2 hours
Frequency
Seconds
0
1000
2000
3000
4000
5000
6000
7000
8000

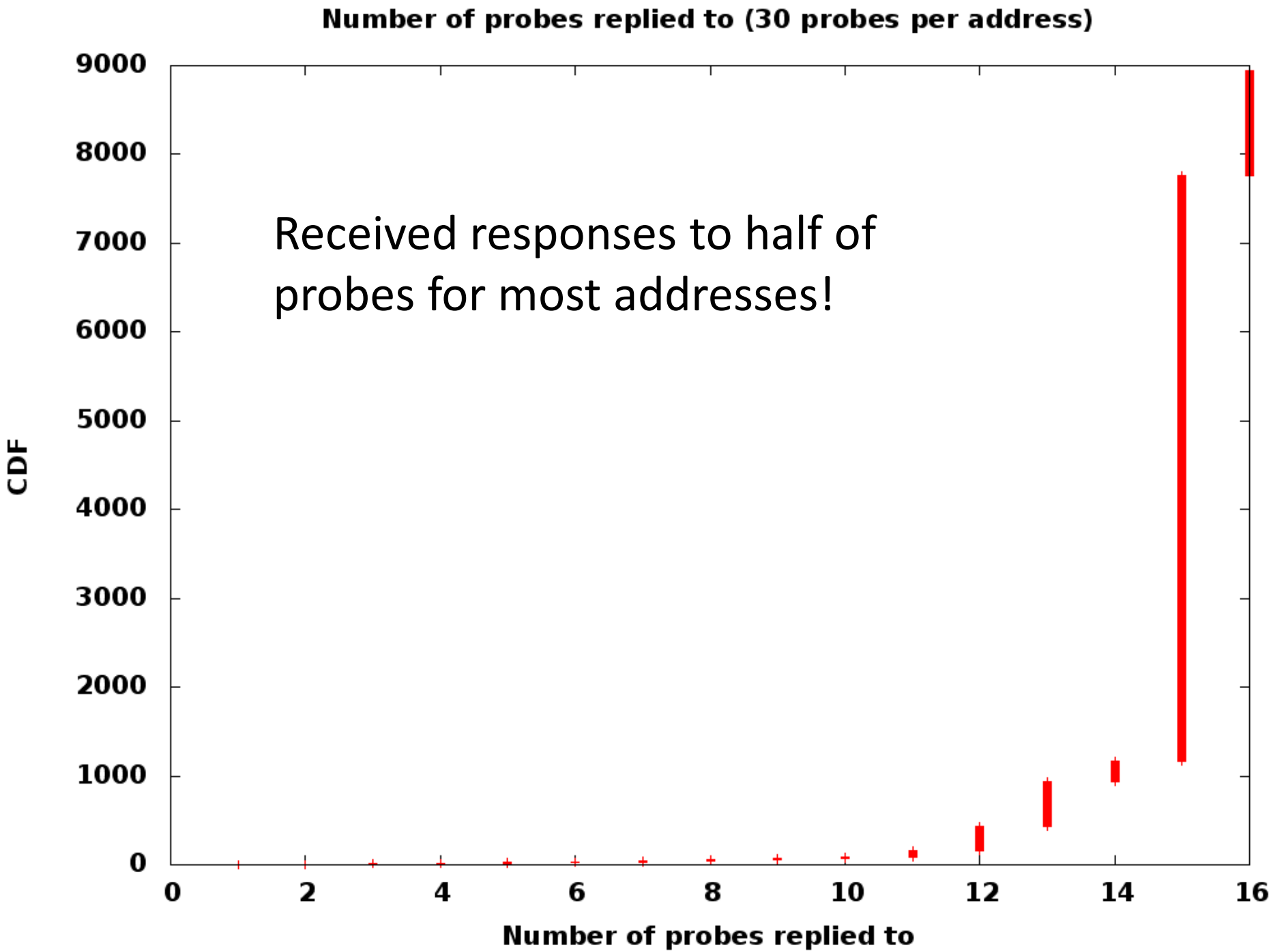
First attempt at radargun prober

- Send PTBs whenever a packet is received without a fragmentation header
  - Do not re-probe address
  - Original probe considered ‘lost’

- 30 one-min rounds
- 1300 byte ICMP echo request packets
- i.e. 300 x 1300 byte pps (390,000 bps)
  - Much higher data rate than if we sent small probes


First IP-ID observed for each address
CDF
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
1
10
100
1k
10k
100k
1m
10m
100m
1b
First IP-ID value
72% of IP-ID values between
127 and 1000
not a lot of entropy for a 32 bit number


Difference in first and last IP-IDs observed for each address
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
CDF
1
10
100
1000
Difference in first and last IP-ID values
30
Very little velocity in IP-ID counter over a 30 minute period
30 rounds – shouldn't there be bands at increments of 30?


Number of probes replied to (30 probes per address)
Received responses to half of probes for most addresses!
CDF
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
0
2
4
6
8
10
12
14
16
Number of probes replied to

Second attempt

- Lack of entropy in IP-ID further motivates sequence of non-overlapping probes / responses.
- 10 one-min rounds
  - each round with probe order shuffled

Results

- 2492 pairs with incrementing, non-overlapping IP-ID values
- Probed with ally, 5 probes, 1 sec intervals:
  - 14 not aliases: 0.6% of pairs
    - Rejected with very close IP-IDs, often the same value
  - 173 packet loss (no classification): 7% of pairs
    - Another attempt would enable these to be classified.
  - 2305 aliases: 92.5% confirmed
    - 910 routers, 90% of them with two observed aliases

Reducing packet loss / data rate

- Probe with larger windows?
  - Relies on remote system caching PTB
  - Tried a window of 3 minutes but had half as many candidate aliases. i.e. performed worse.
    - Need to spend time in data figuring out why
- We have ideas for smarter probing given extremely low IP-ID velocity
  - Need to implement and evaluate them.

Applications to IPv4

- http://datatracker.ietf.org/doc/draft-ietf-intarea-ipv4-id-update/
  - Would set IP-ID value only when the packet is fragmented

- Do IPv4 routers that set a constant IP-ID value set a non-constant IP-ID if they have to fragment the response?

Summary

- Not trivial to re-apply IPv4-based IP-ID alias resolution techniques.
  - Data rate required in IPv6 much larger
  - Need to solicit fragments
- Need to try alternative methods: UDP and TCP
  - UDP will require router to accept an ICMP error (PTB) for another ICMP error (port unreach)
  - Both rely on atomic fragments because responses <= 1280 bytes.