Bond Internet Systems

Impact of DNS over TCP a resolver point of view

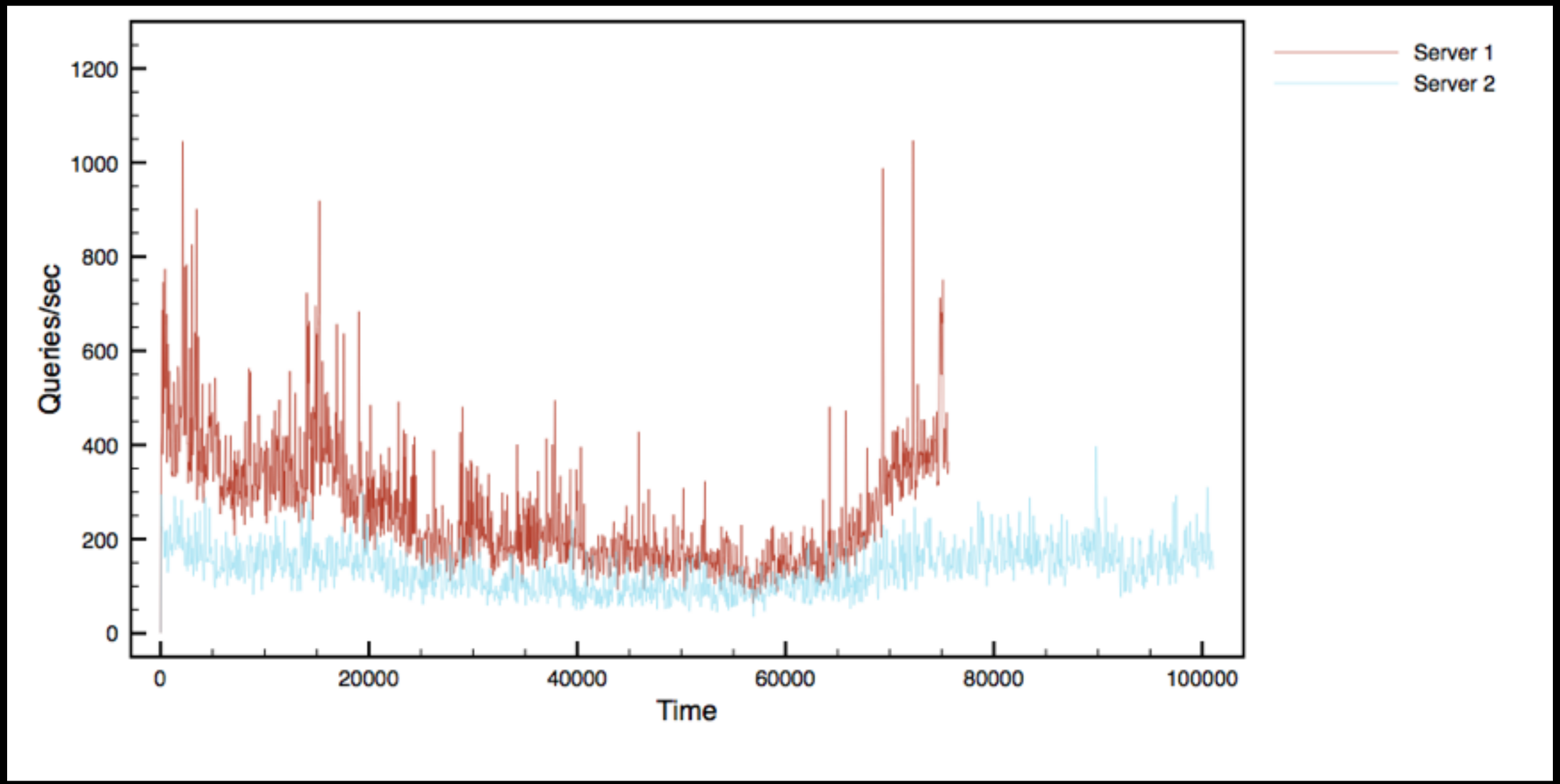
João Damas
Mónica Cortés

Objective

Look at traffic between DNS recursive resolvers and the authoritative servers they query and…

Simulate the effect on the recursive server of using TCP for all DNS traffic

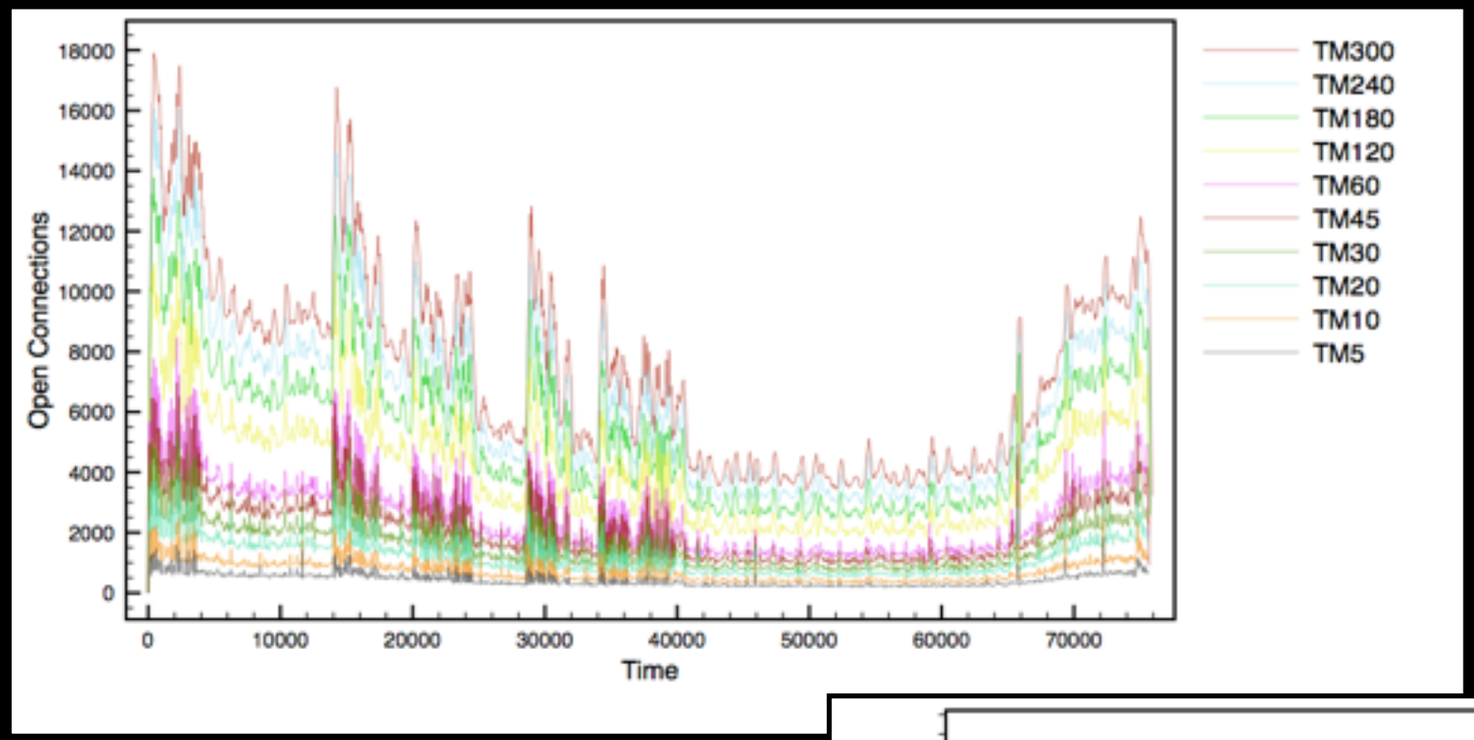
- The data
- The cost
- The benefit
- The need

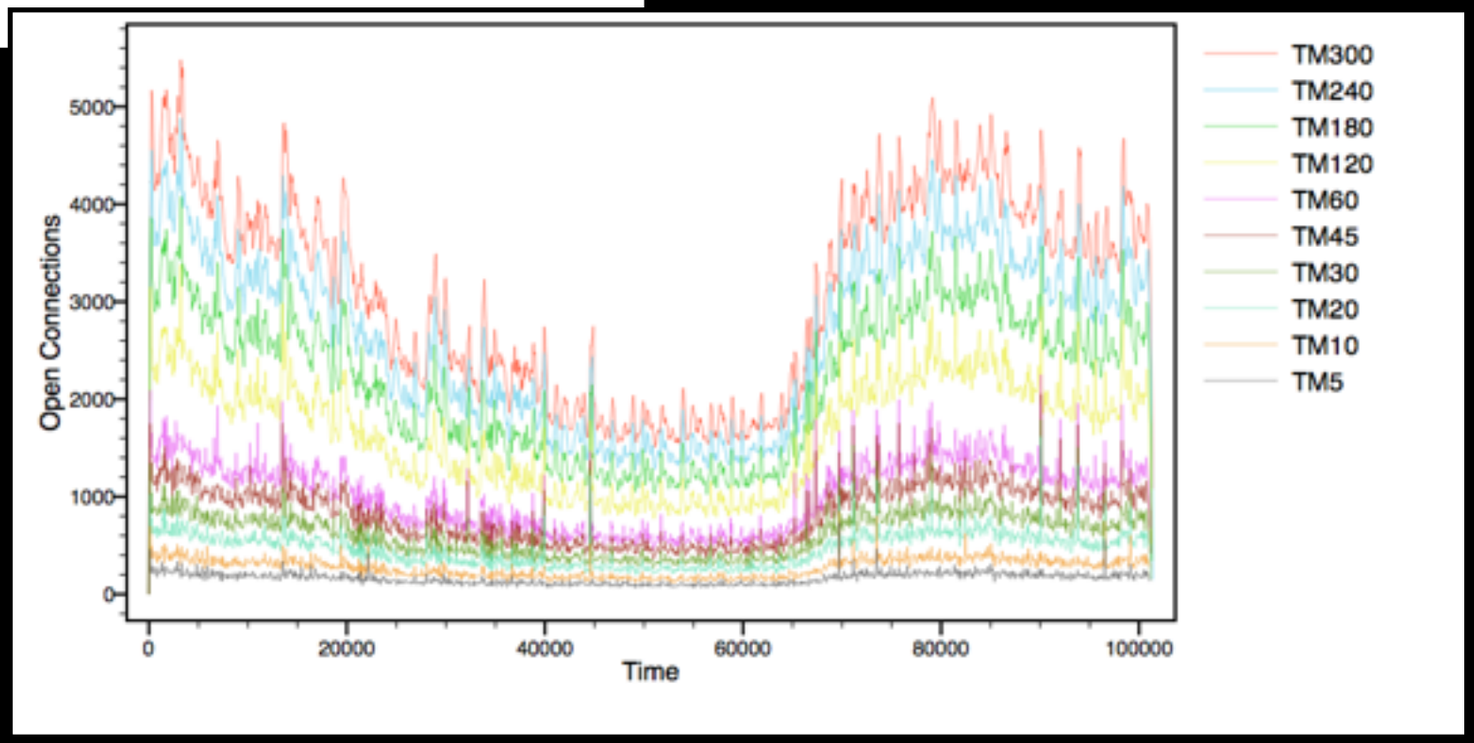

Server 1
Server 2
Queries/sec
1200
1000
800
600
400
200
0
0
20000
40000
60000
80000
100000
Time

Data (qps)

The cost

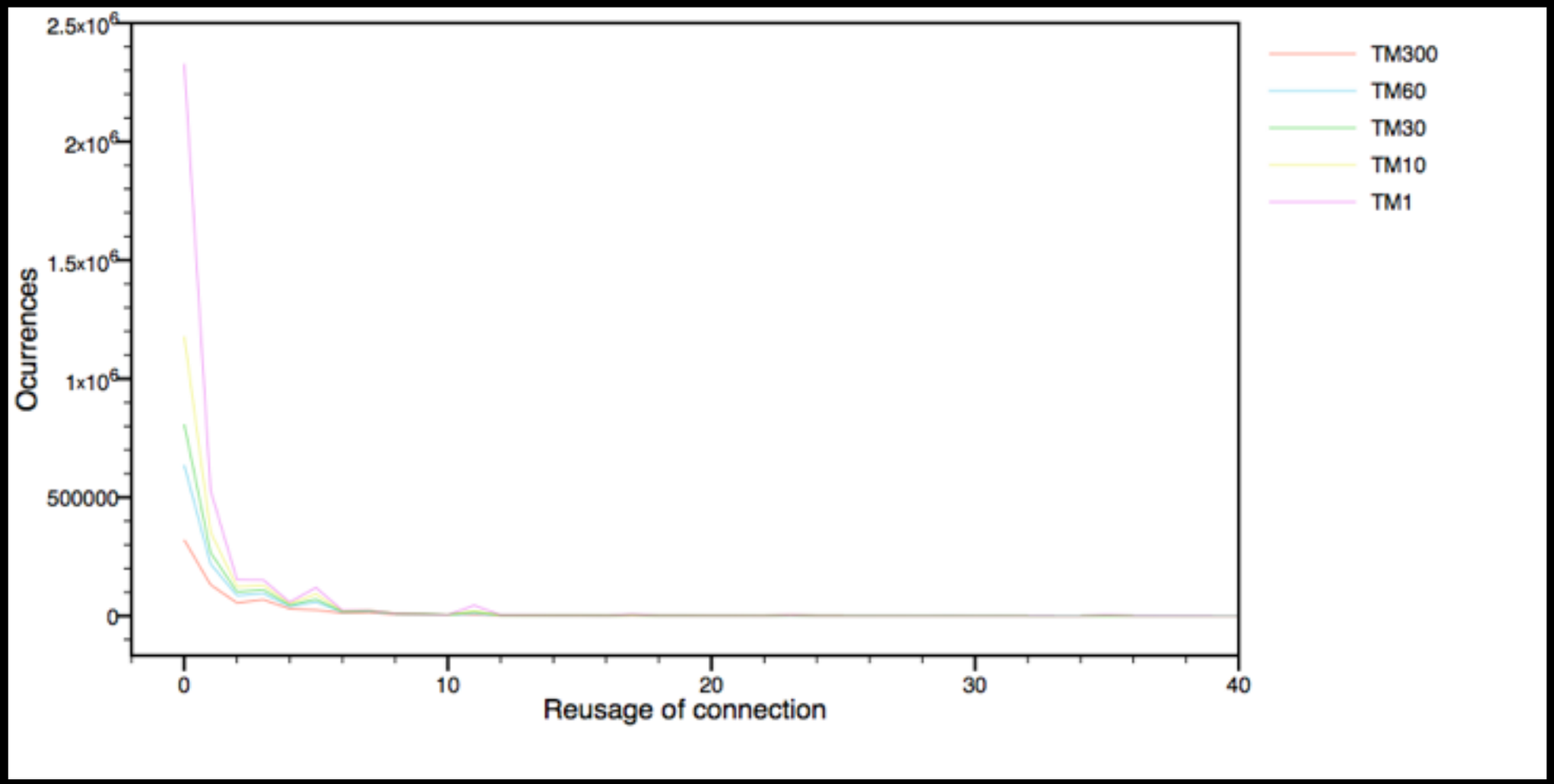
- Main impact of using TCP for everything is the state that is kept on the server, which is proportional to the number of established connections at a given time



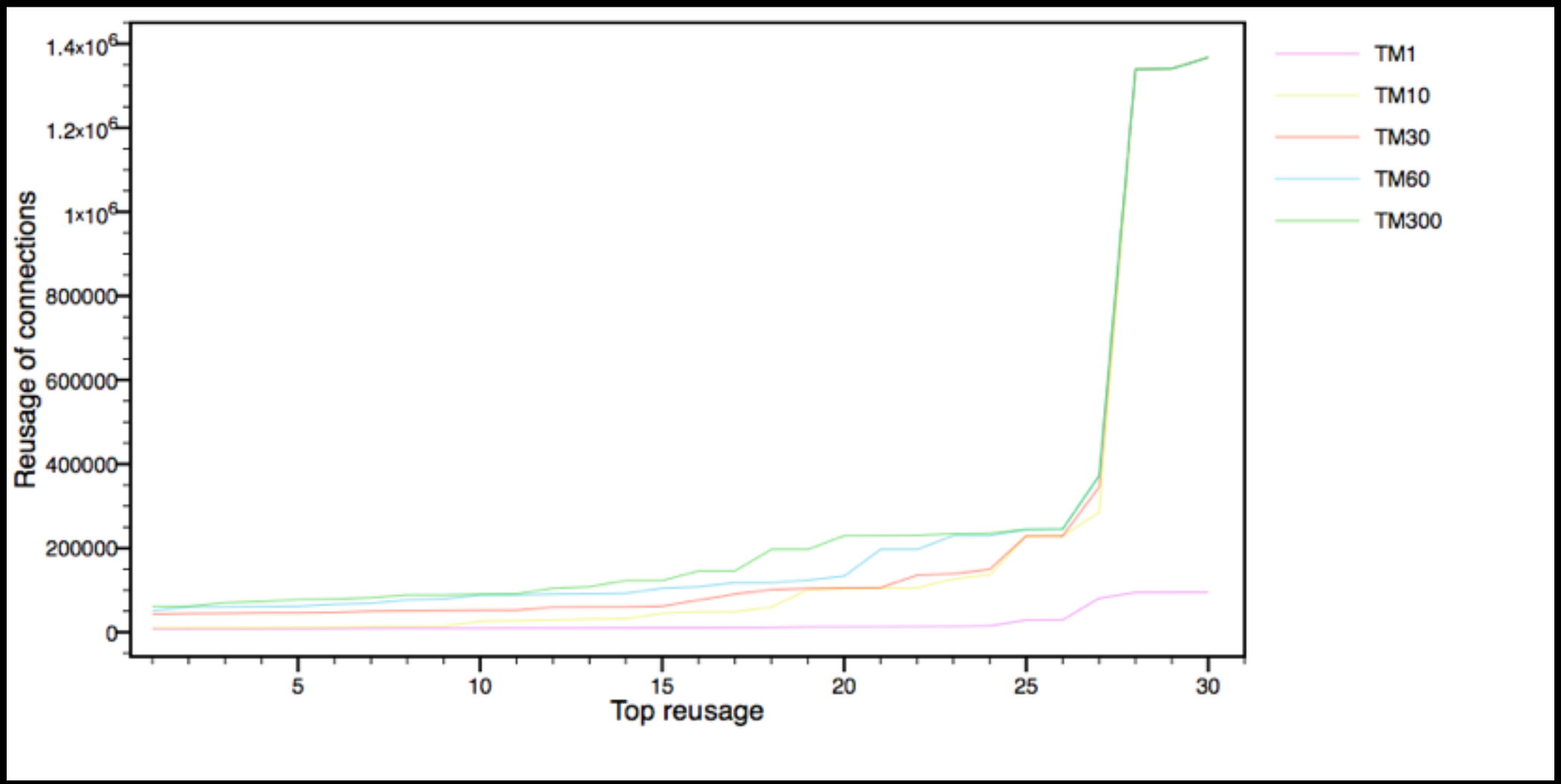


connections

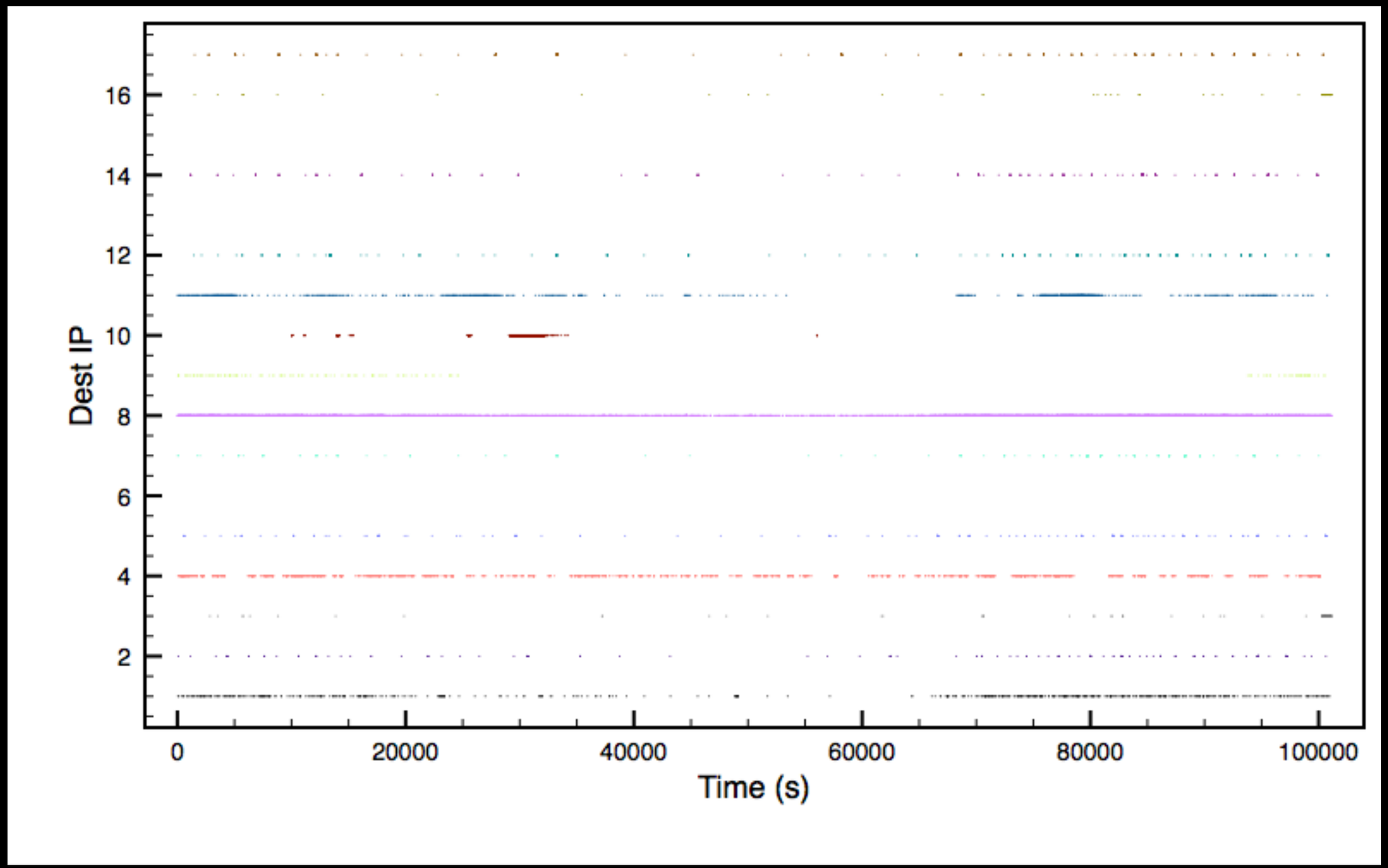
The benefit



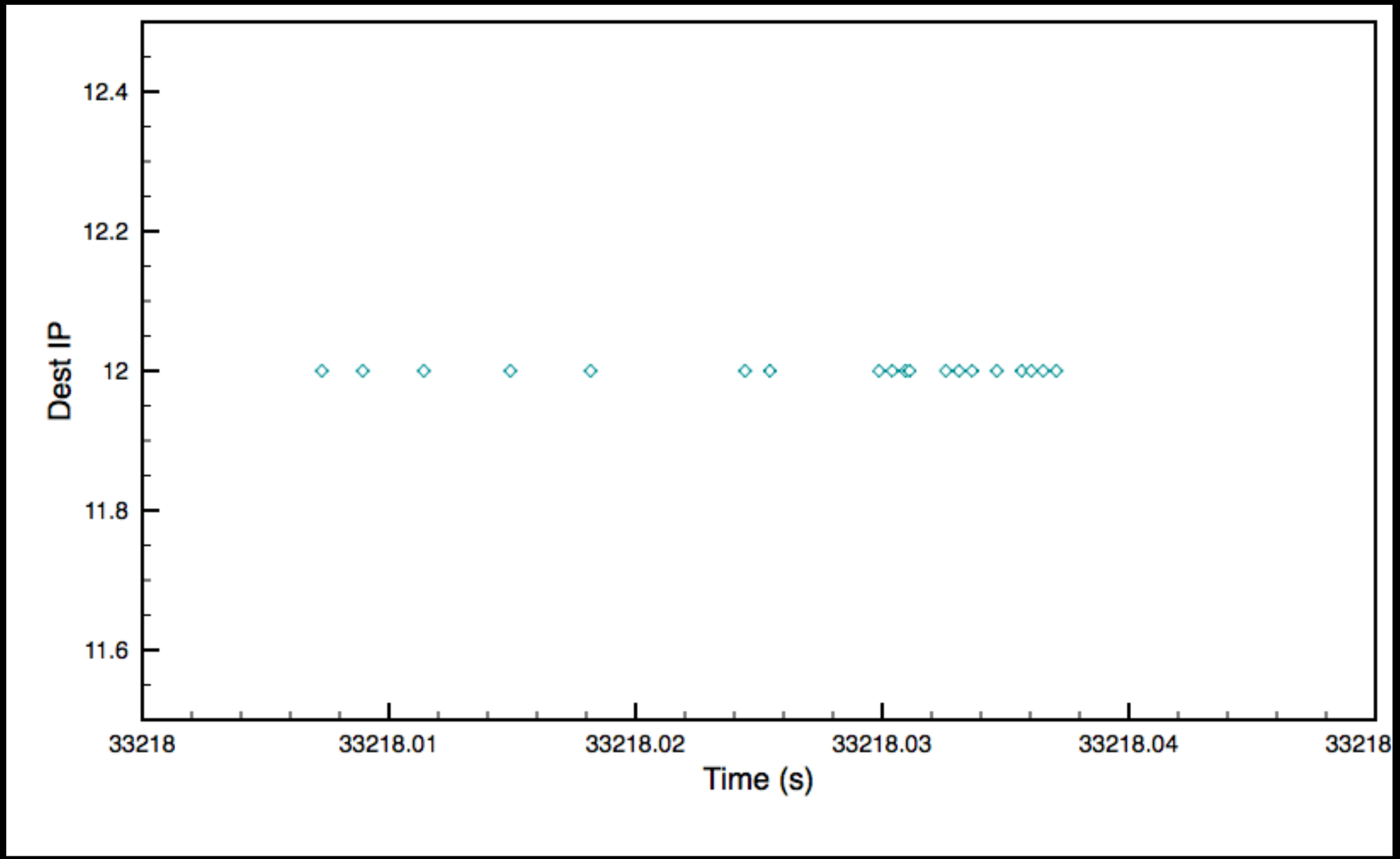
connection reuse



connection reuse



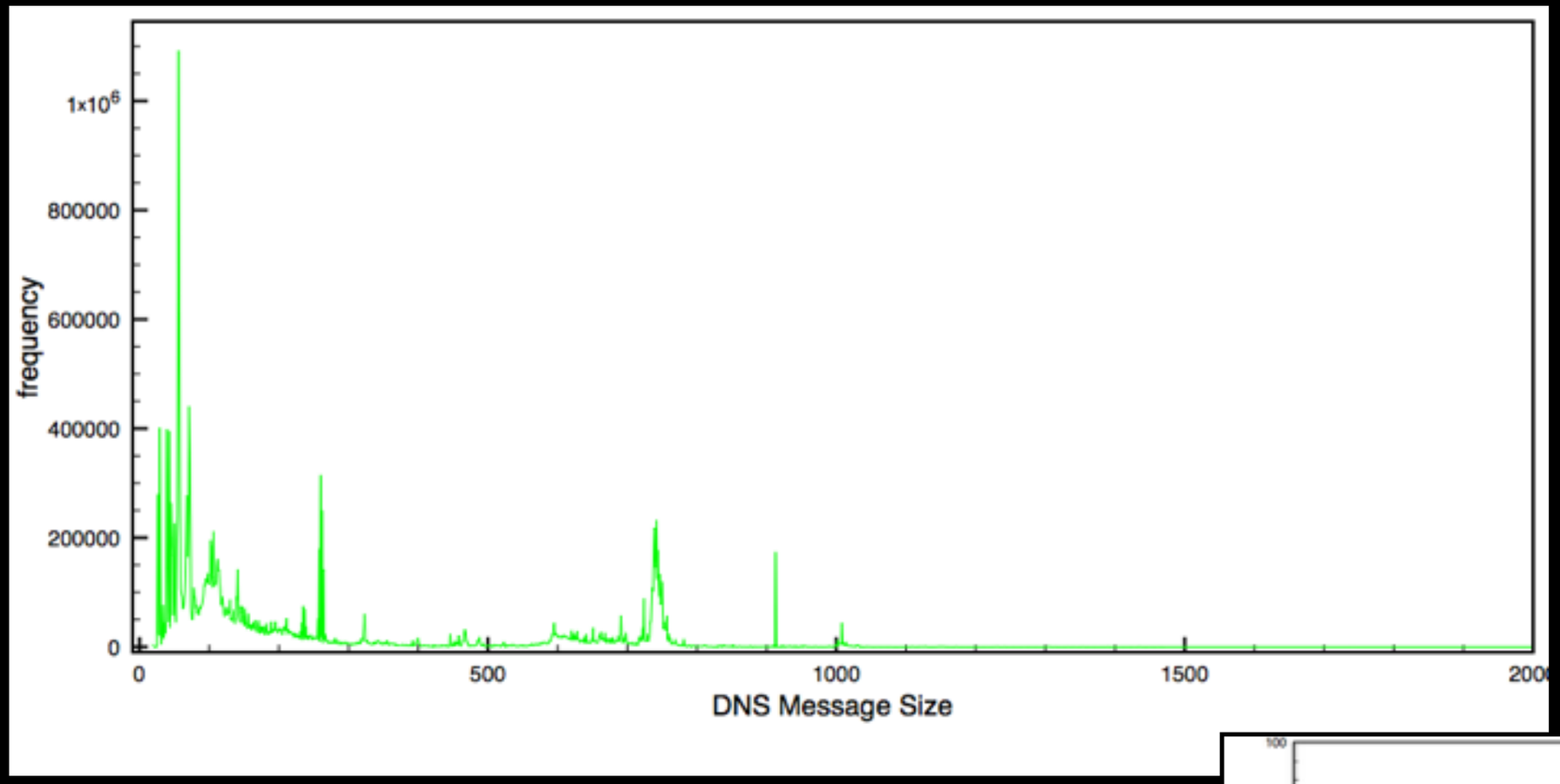
query timeline

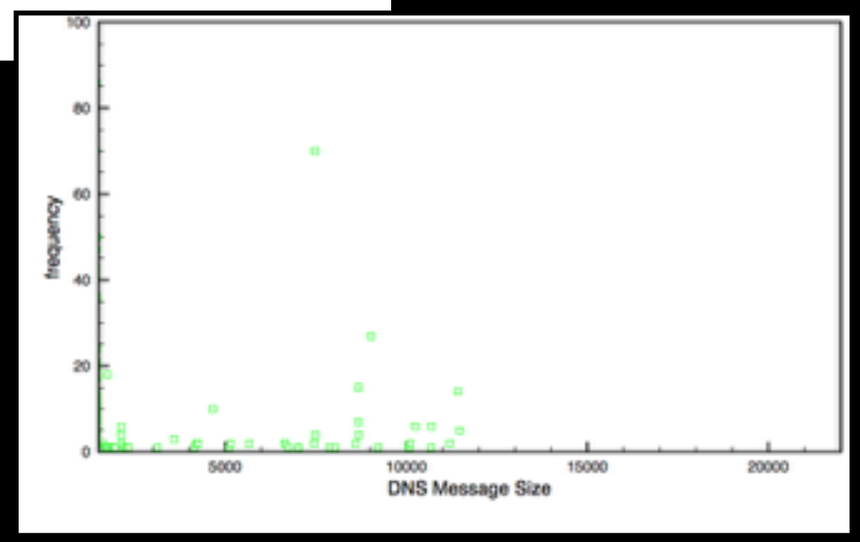


query timeline zoom

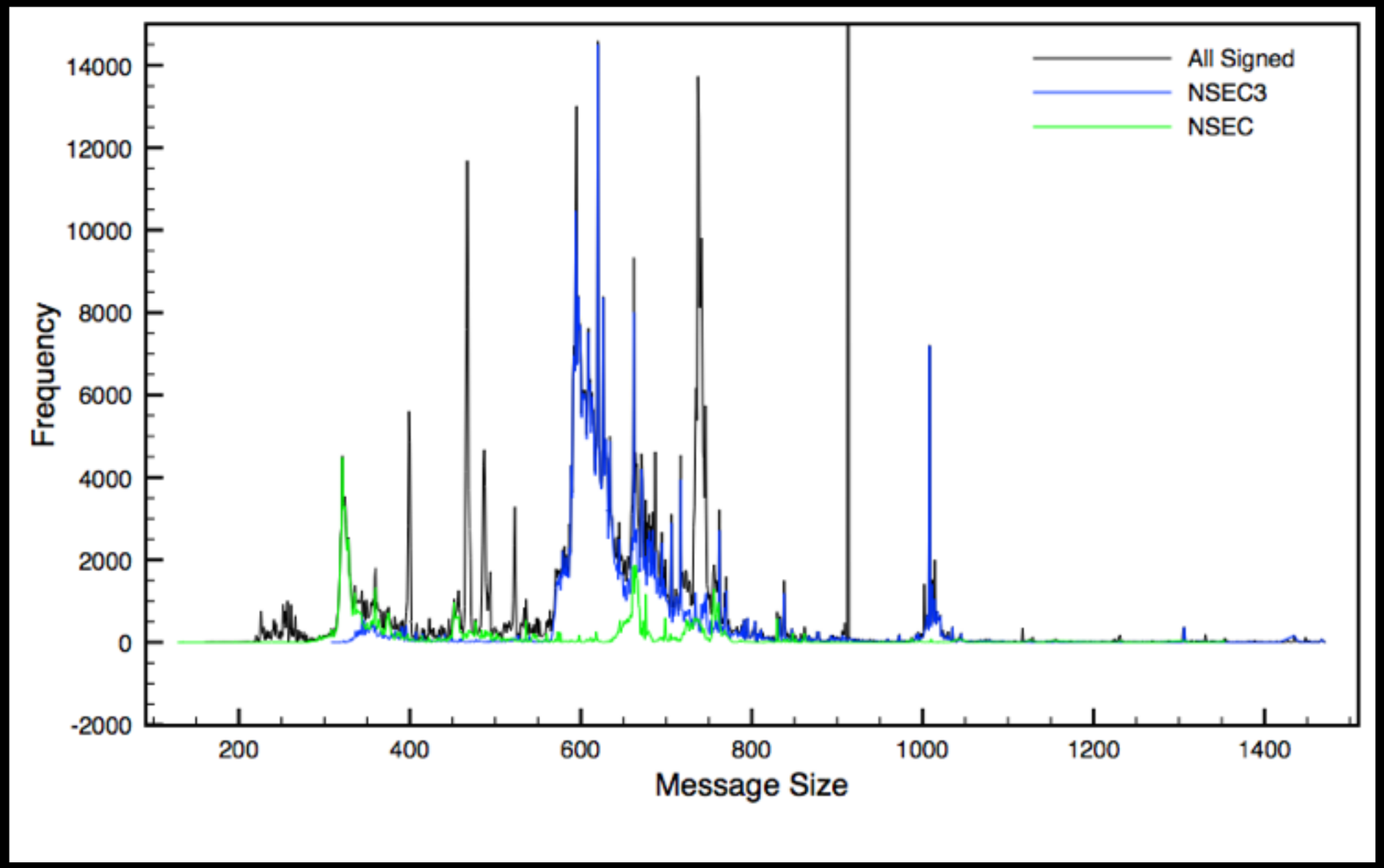
The *need*

- Helps with spoof prevention
  - reflection attacks
- Do we need it to cope with larger messages?
  - DNSSEC, in particular NSEC3
  - Long NS lists, other





Size distribution - all



Size distribution - DNSSEC

Observations

- Message size doesn’t seem to be a big problem at this time
- Management of TCP timeout is critical
- Some servers would reuse connections quite effectively
  - queries come in bursts.
    - tuning and signalling needed

Next steps

- Analyse impact on the recursive->stub
  - Coming up

Thanks

Our thanks to:

Comcast (grant)

Questions?

joao@bondis.org
monica@bondis.org