Timeouts: Beware Surprisingly High Delay

By Ramakrishna Padmanabhan, Patrick Owen, Aaron Schulman, Neil Spring

David Labode

Outline

1. Introduction
2. Importance of Probe Timeouts
3. Datasets Overview
4. The Recommended Timeout Value
5. Do long Ping Times really exist?
6. Why do Pings take so long?
7. Conclusion

1. Introduction

- Paper addresses researchers who work with active probing of hosts on the internet
- Hypothesis: timeouts generally used in research are too short (~ 3 seconds)
- Goal: find a reasonable timeout value to use in this field of study

2. Importance of Probe Timeouts

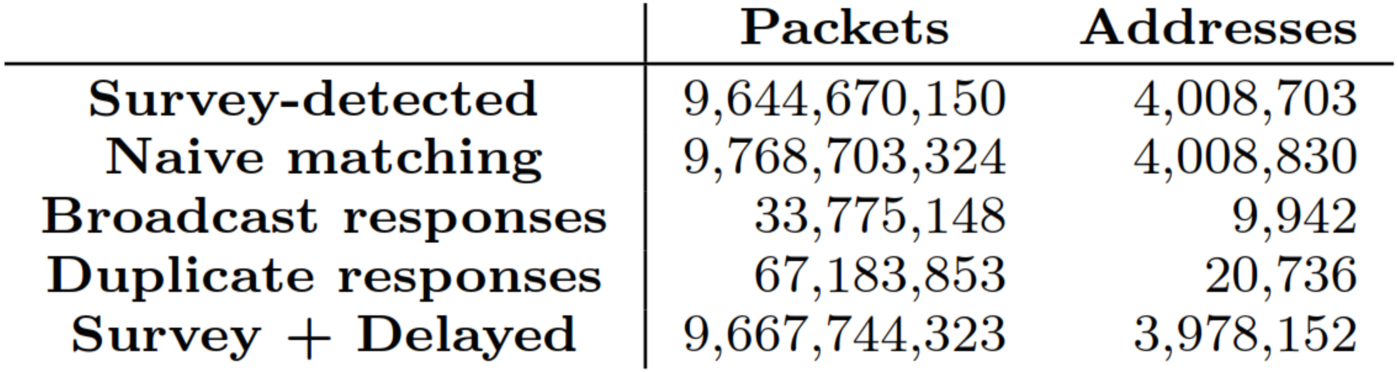
- Paper argues: active probing timeout values need to be selected carefully → influence data measurably
- Too short timeouts:
  - Packets delayed due to congestions? → Host declared offline falsely
- Too long timeouts:
  - More states need to be maintained on the researchers side
  - Hardware limitations might weigh in

3. Datasets Overview

- ISI survey data set
  - Internet wide survey, 24.000 /24 blocks (1% of globally allocated IPs)
  - Each survey: probe all 256 addresses once each 11min for 2 weeks
  - 103 surveys completed between 04/2006 and 02/2015
- Data format
  - Matched responses: answer came in under 3 seconds
  - Unmatched responses: answer took longer than 3 seconds
    - Delayed
    - Broadcast responses (response from different IP than request)
    - DoS responses (cases where hosts answered with >4 packets)

4. The Recommended Timeout Value

- Combined dataset
  - Originally matched + later matched packets
  - Broadcast/Duplicate addresses are filtered out



	Packets	Addresses
Survey-detected	9,644,670,150	4,008,703
Naive matching	9,768,703,324	4,008,830
Broadcast responses	33,775,148	9,942
Duplicate responses	67,183,853	20,736
Survey + Delayed	9,667,744,323	3,978,152

- Data collected from newly forged dataset
  - To detect 95% of pings from 95% of addresses → ~5 second timeout
  - Delay of 1% of pings from 1% of addresses > 145 seconds

4. The Recommended Timeout Value

- Answer to research question:
  - **60 second timeouts** or no timeout value at all if possible
    - covers 98% of echo replies from 98% of addresses
    - ≈ 96% of all responses
  - Compromise between wait time and detection rate

5. Do long Ping Times really exist?

- Are extreme ping times (> 100 sec) real? Or a byproduct of:
  - ISI probing scheme?
  - Errors in data sets?
  - Discrimination of ICMP in relation to TCP/UDP?

➔ Own study on long ping times using own TCP/UDP test and ZMap & Scamper

5. Do long Ping Times really exist?

- TCP/UDP testing
  - Send ICMP/TCP/UDP probes 20 minutes apart

  → No discrimination
- Scamper study
  - Pick high-latency addresses from ISI dataset (2000 IPs)
  - Ping each address 1000 times
  - Results:
    - Most latencies < 10 seconds
    - But 0.17% of responses took > 100 seconds

    → Latency prone addresses change, but…

    … existence of extremely high delays verified!

5. Do long Ping Times really exist?

- ZMap data
  - Request & response-data from 04/2015 to 07/2015
  - Results:
    - 5% of responses took > 1 second
    - 0,1% of responses took > 75 seconds
    - Again: existence of extremely high latencies verified!
- Additional Findings
  - Timeout required to catch 90% of responses:
    - 2007: ~2 seconds
    - 2011: ~5 seconds

    → Latencies increased over the years

6. Why do Pings take so long?

- Use Maxmind to find geographic location and Autonomous System of high-latency hosts
    - Are Satellite links the cause of ultra high delays?
        - Satellites have a theoretical minimum latency of 500ms
        - The highest ping measured was 517 seconds high
        - But 99% of satellite pings are < 3 seconds

→ Satellites are not the cause of extremely high latency

6. Why do Pings take so long?

- Also found with Maxmind
    - Most high latency hosts are in cellular Autonomous Systems

- 2 Categories
    - Latencies > 1 second → “Turtle”
    - Latencies > 100 seconds → “Slow Turtle”

- South America & Asia account for 75% of all Turtles
- 1/4 of all South American and 1/3 African hosts is also a Turtle

6. Why do Pings take so long?

- What is the source of Turtles in cellular ASes?
  - First ping behavior:

extraordinary temporary, initial latency due to MAC-layer time slot negotiation or device wake-up

- What is the source of slow turtles?
  - No real source, only 2 main patterns:
    - latencies steadily decay
    - latencies continuously high and loss in between

7. Conclusion

- Latencies are higher than expected…
- …and have been increasing over the years
- Latencies are NOT part of measurement choices (ICMP)
- NOT due to vantage points
- NOT due to probing schemes
- NOT caused by satellite per se
- Often caused by initial communication over cellular ASes

7. Conclusion

- Key takeaways:
  - Listen long echo responses! Host might just be slow, not offline
  - Design probing with 60 second timeout or no timeout at all

Discussion