Analyzing the Costs and Benefits of DNS, DoT, and DoH for the Modern Web

Austin Hounsel* Kevin Borgolte* Paul Schmitt*
Jordan Holland* Nick Feamster†
Princeton University* University of Chicago†

DNS Privacy Has Become a Significant Concern

- On-path network observers can spy on traditional DNS traffic (Do53)
- Two protocols have been proposed to encrypt DNS traffic
  - DNS-over-TLS (DoT)
  - DNS-over-HTTPS (DoH)

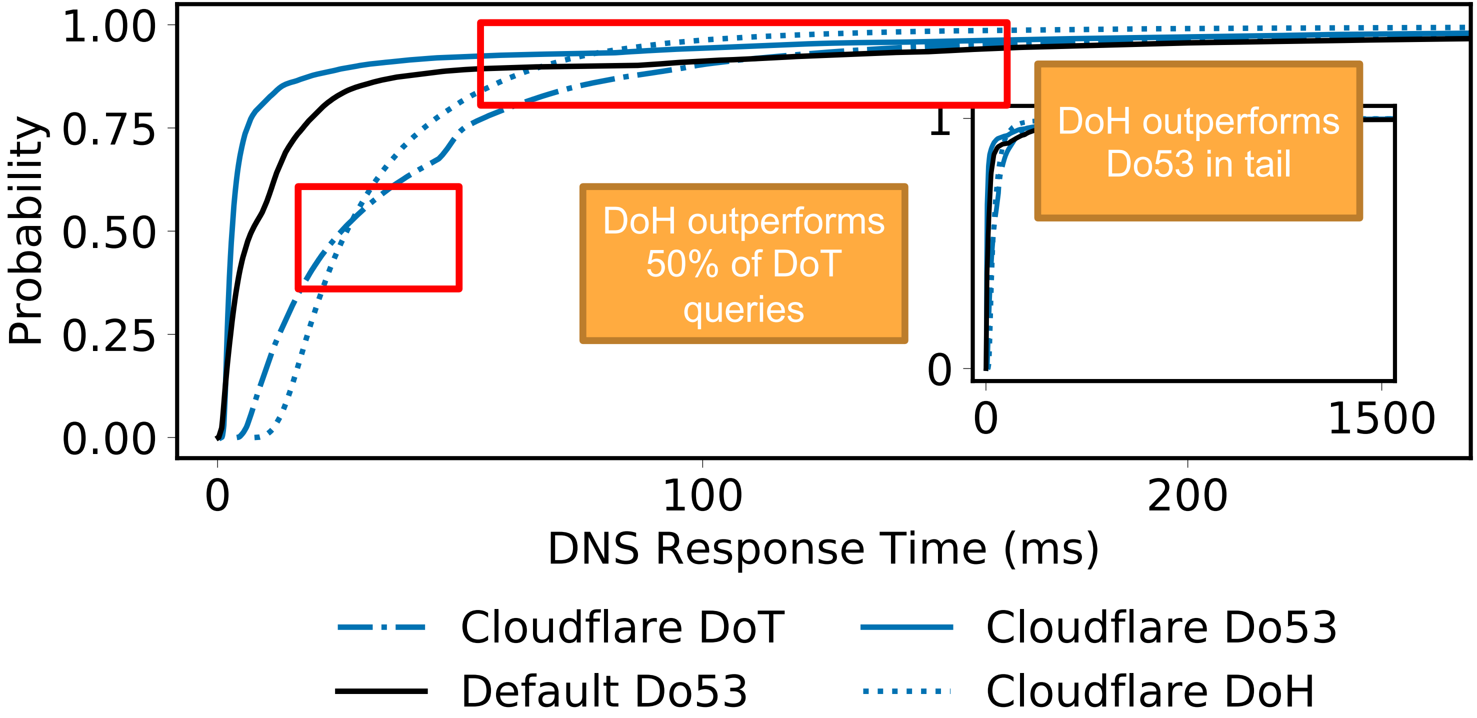
Contributions

- Extensive performance study of Do53, DoT, and DoH
  - Query response times
  - Page load times
  - Emulated network conditions
- Measurements from five global vantage points

Unexpected Finding

- **Despite higher response times, page load times with encrypted DNS transports can be faster than Do53**

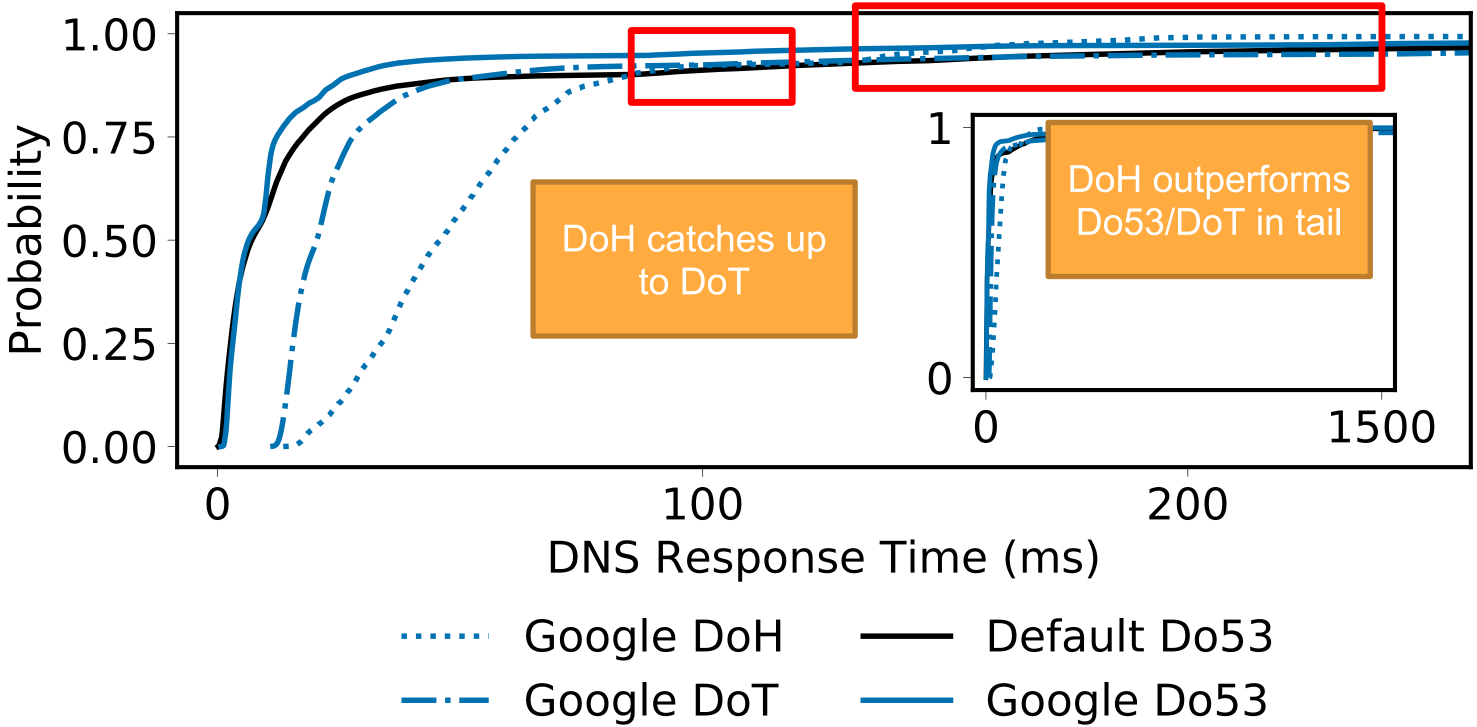
DNS Responses from Cloudflare at Frankfurt



DoH outperforms 50% of DoT queries

DoH outperforms Do53 in tail

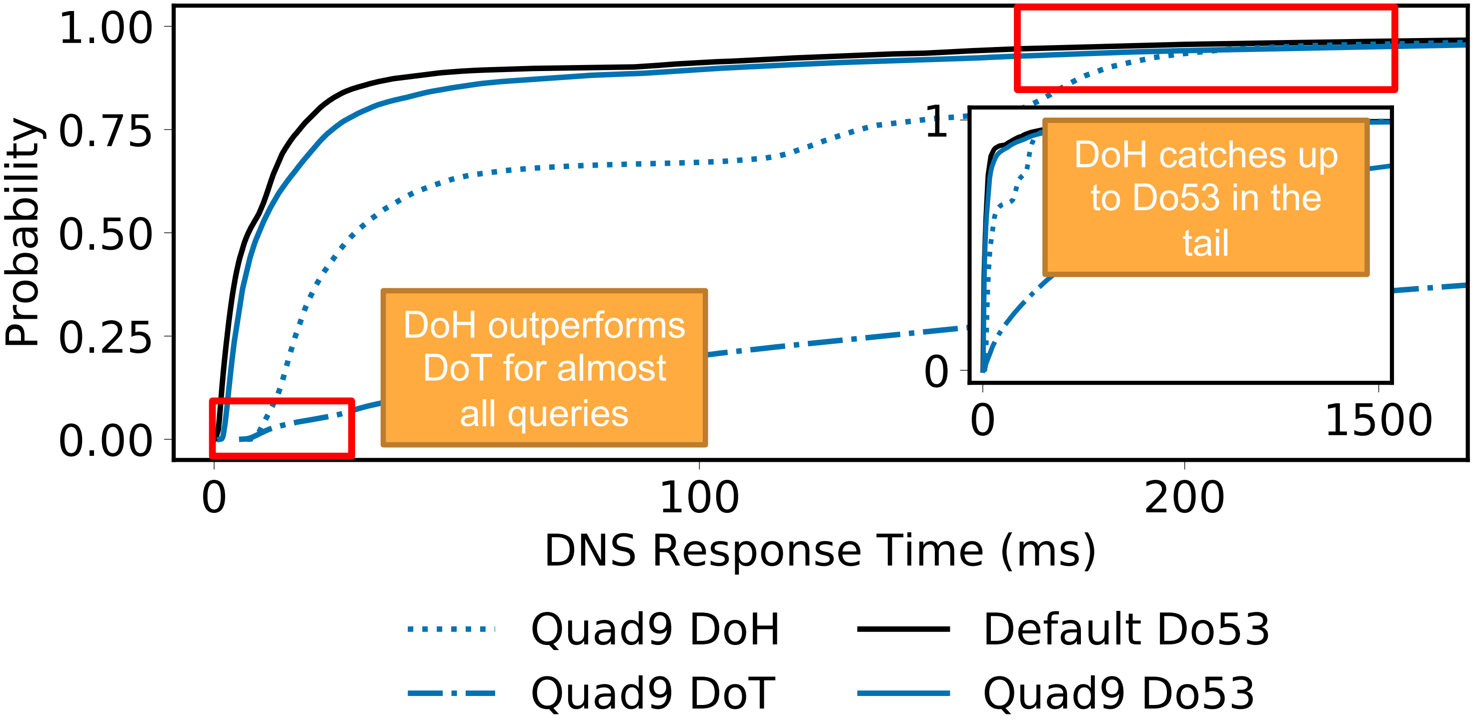
DNS Responses from Google at Frankfurt



DoH catches up to DoT

DoH outperforms Do53/DoT in tail

DNS Responses from Quad9 at Frankfurt



DoH outperforms DoT for almost all queries

DoH catches up to Do53 in the tail

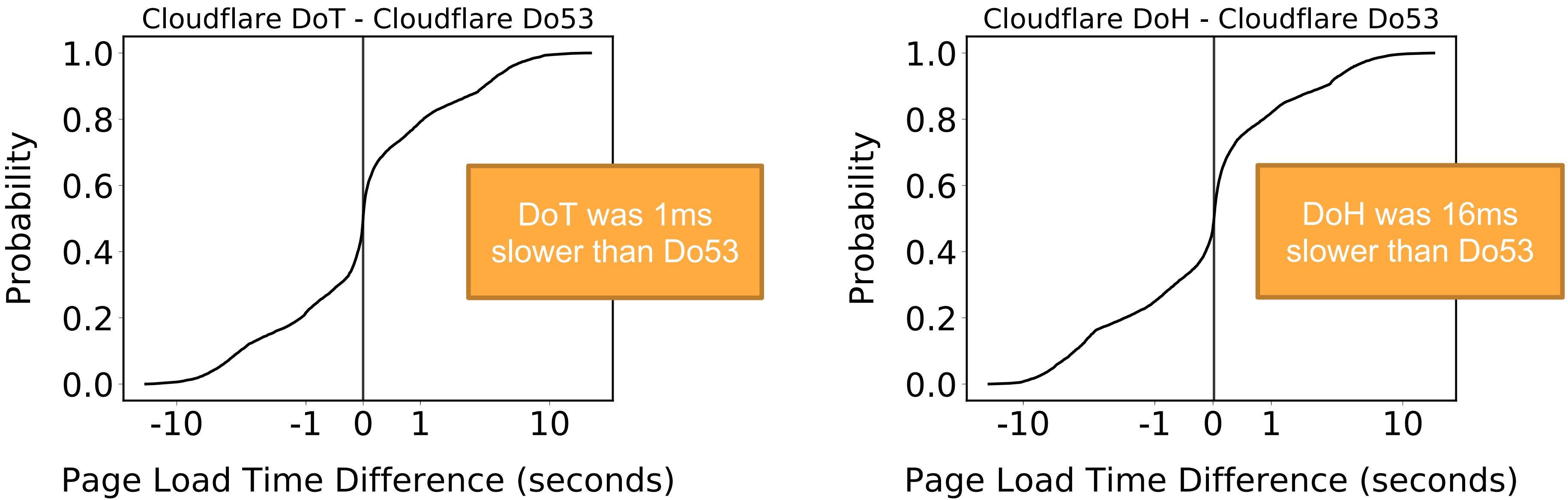
Takeaway: DoH Can Outperform Do53

- DoH outperforms Do53 in the tail of response times
  - Higher mean but lower variance
- HTTP caching of the wire format may help

Emulated Cellular Conditions

- We performed measurements with emulated cellular conditions
  - DoH and DoT are starting to be offered on phones
  - Performance may be significantly different

Page Loads with Cloudflare at Frankfurt



Cloudflare DoT - Cloudflare Do53

Cloudflare DoH - Cloudflare Do53

DoT was 1ms slower than Do53

DoH was 16ms slower than Do53

🟥 Diff ≥ 1s

▨ 0.1s ≤ Diff < 1s

▨ 0.03s ≤ Diff < 0.1s

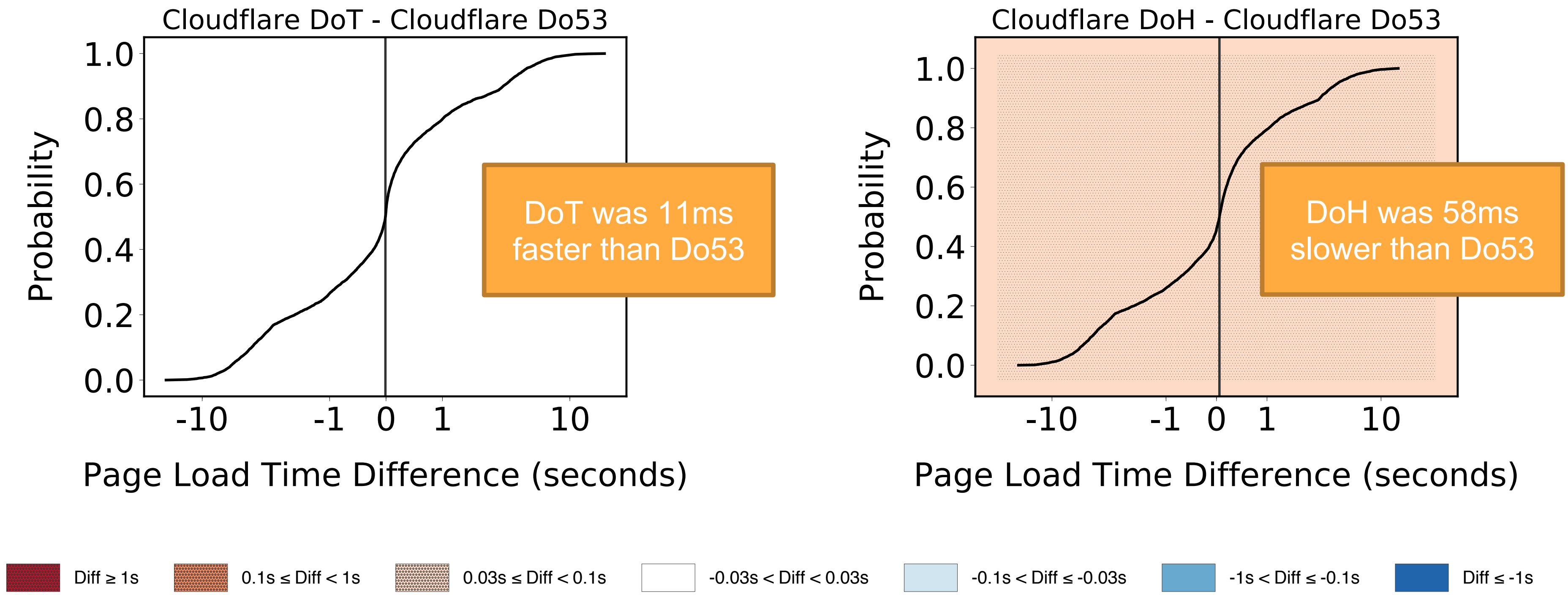
□ -0.03s < Diff < 0.03s

🟦 -0.1s < Diff ≤ -0.03s

🟦 -1s < Diff ≤ -0.1s

🟦 Diff ≤ -1s

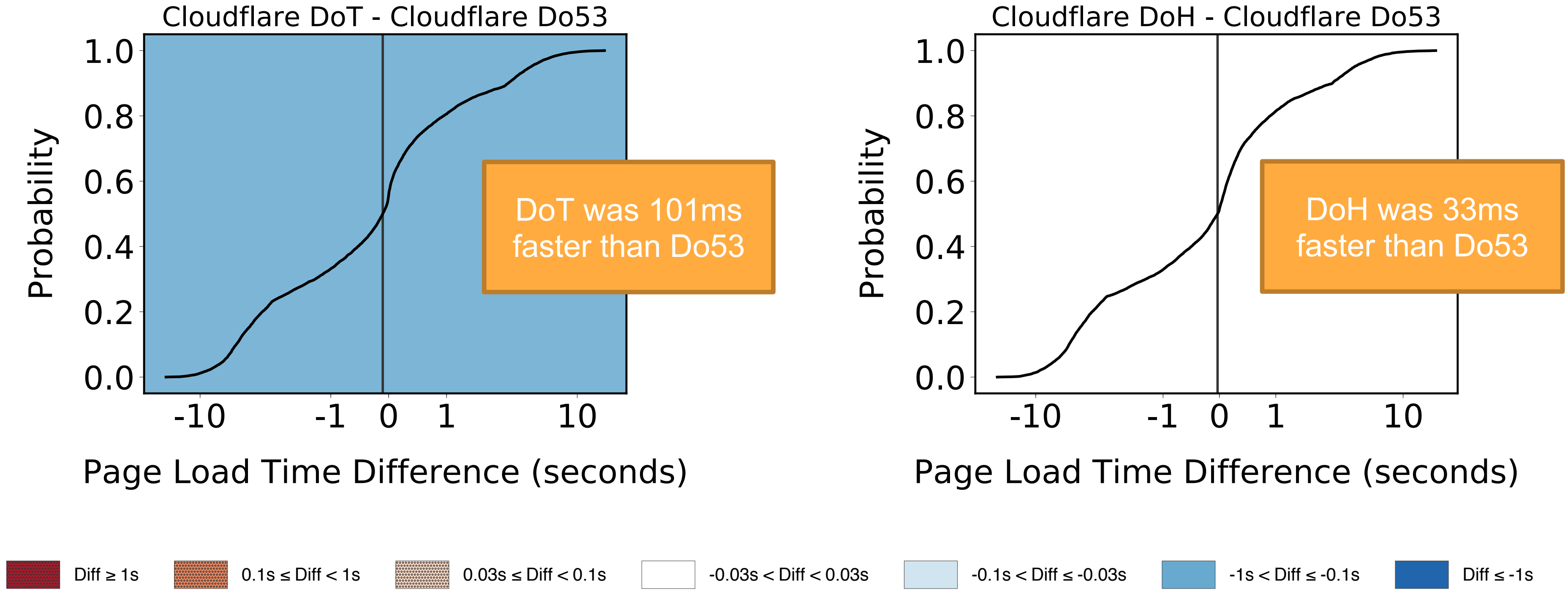
Page Loads with Cloudflare at Frankfurt (4G)



DoT was 11ms faster than Do53

DoH was 58ms slower than Do53

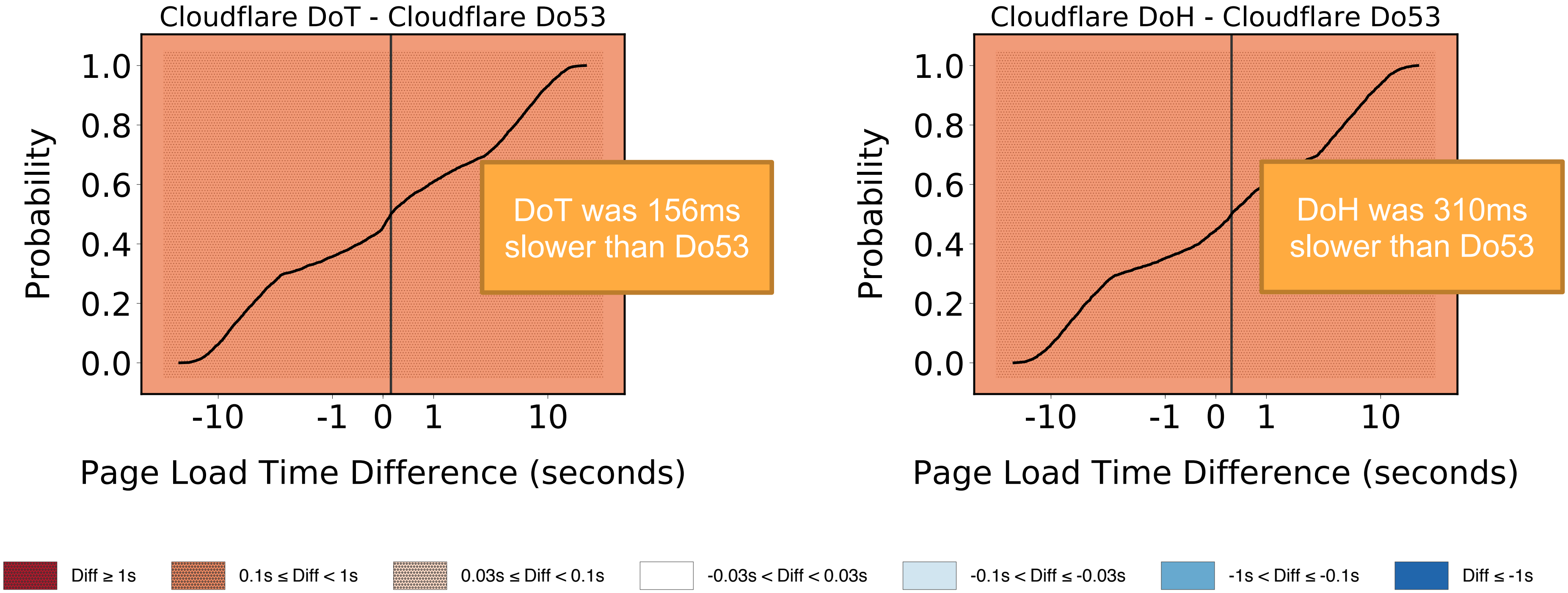
Page Loads with Cloudflare at Frankfurt (Lossy 4G)



DoT was 101ms faster than Do53

DoH was 33ms faster than Do53

Page Loads with Cloudflare at Frankfurt (3G)



DoT was 156ms slower than Do53

DoH was 310ms slower than Do53

Takeaway: TCP Helps Page Load Times

- TCP packets can be retransmitted after 2x RTT
- Timeout of Do53 is set to 5 seconds by default in Linux

Summary

- Measured Do53, DoT, and DoH performance from five vantage points
- Future work: performance analyses over diverse networks
  - Residential ISPs