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

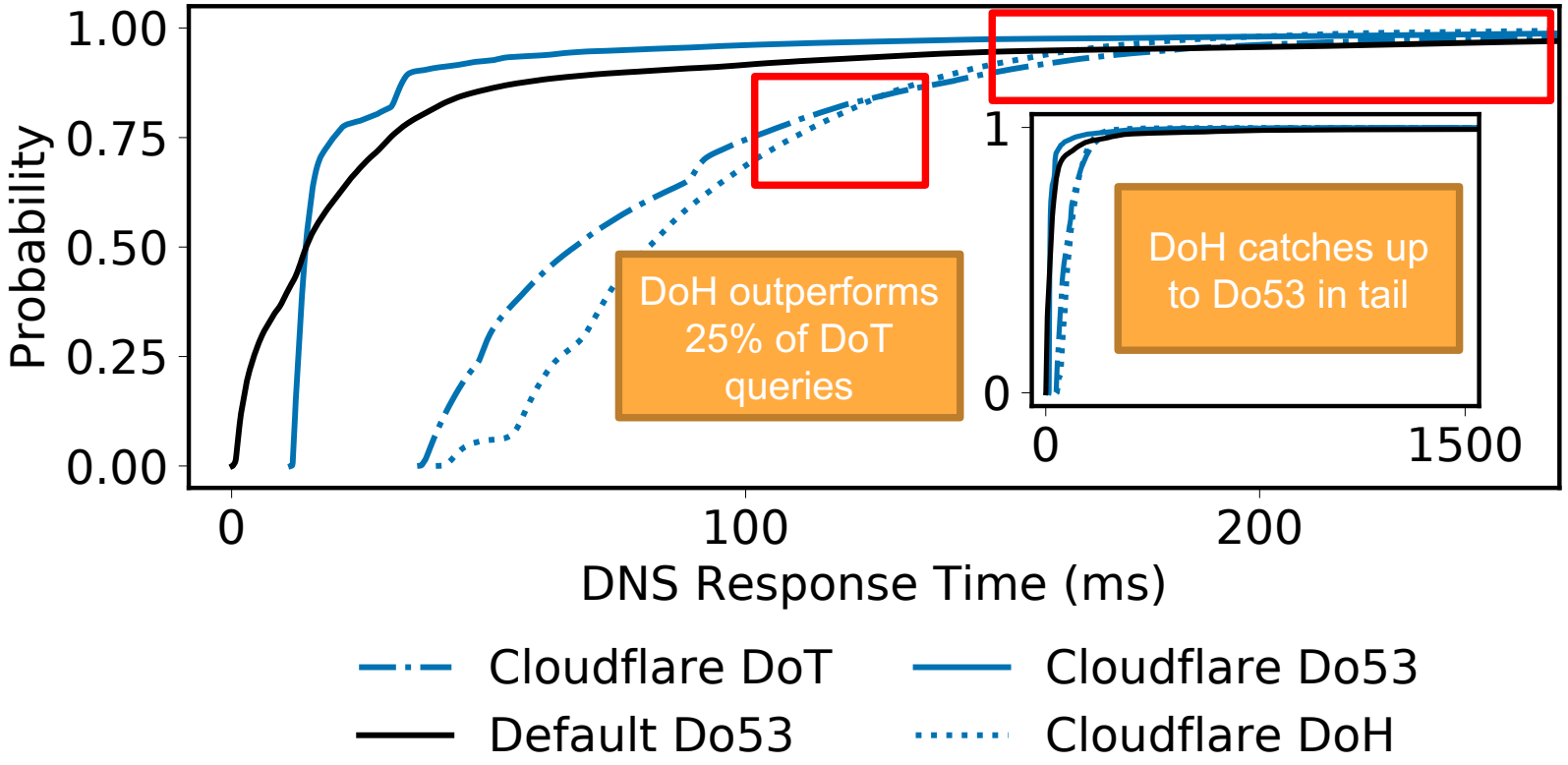
Contributions

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

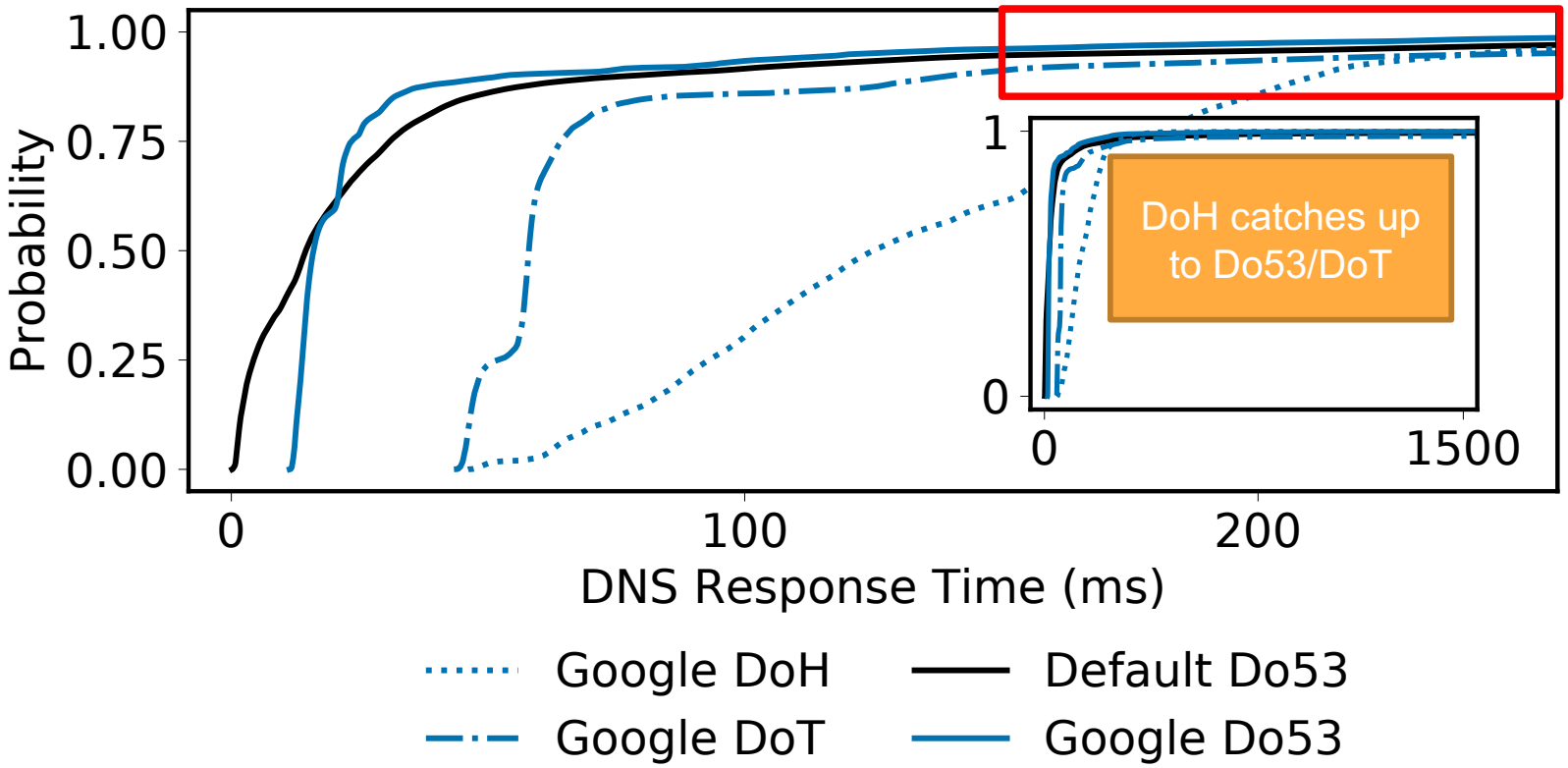
Unexpected Finding

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

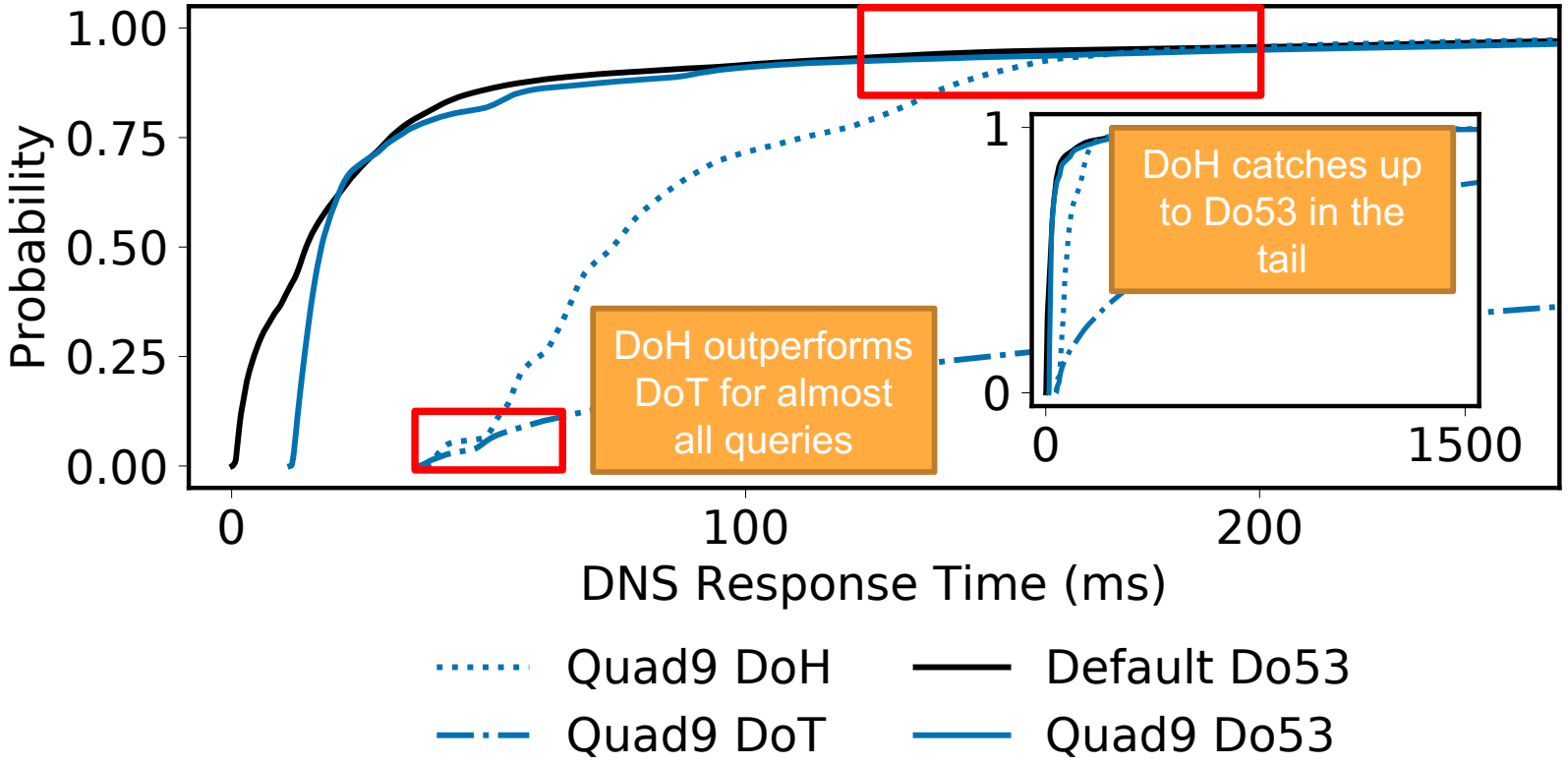
DNS Responses from Cloudflare at Ohio



DNS Responses from Google at Ohio



DNS Responses from Quad9 at Ohio



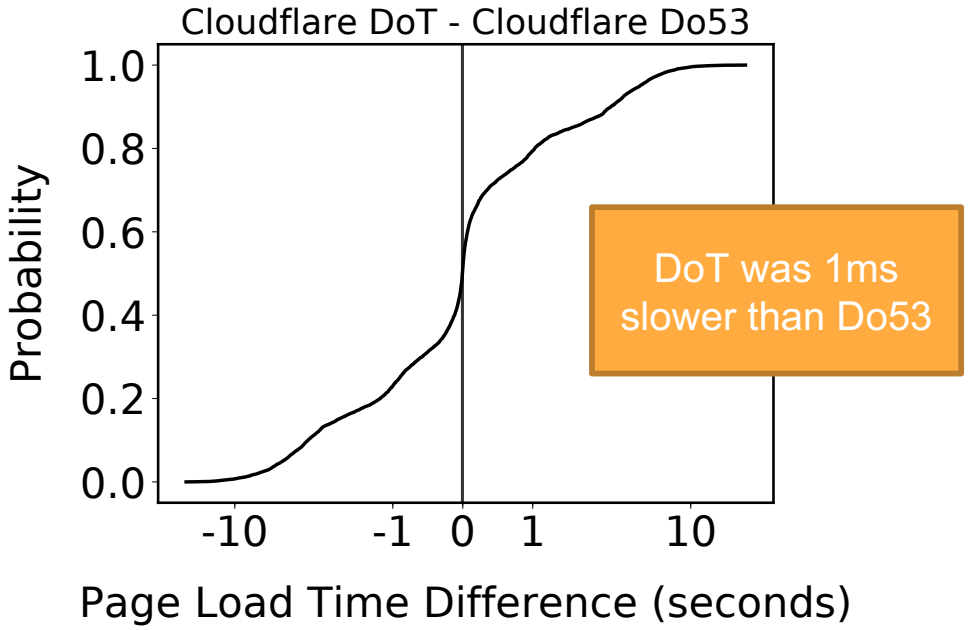
Takeaway: DoH Can Outperform Do53

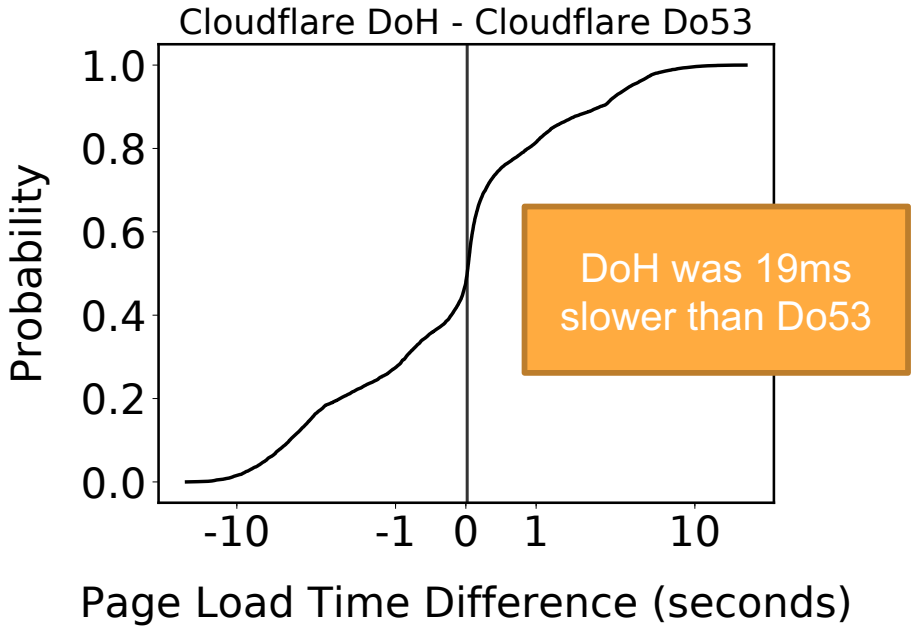
- DoH has a higher mean but lower variance
- Several possible explanations
  - HTTP caching at the edge
  - Wire format caching

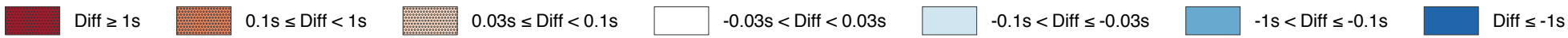
Emulated Cellular Conditions

- We emulated 4G, lossy 4G, and 3G network conditions
  - DoH and DoT are starting to be offered on phones
  - Performance may be significantly different

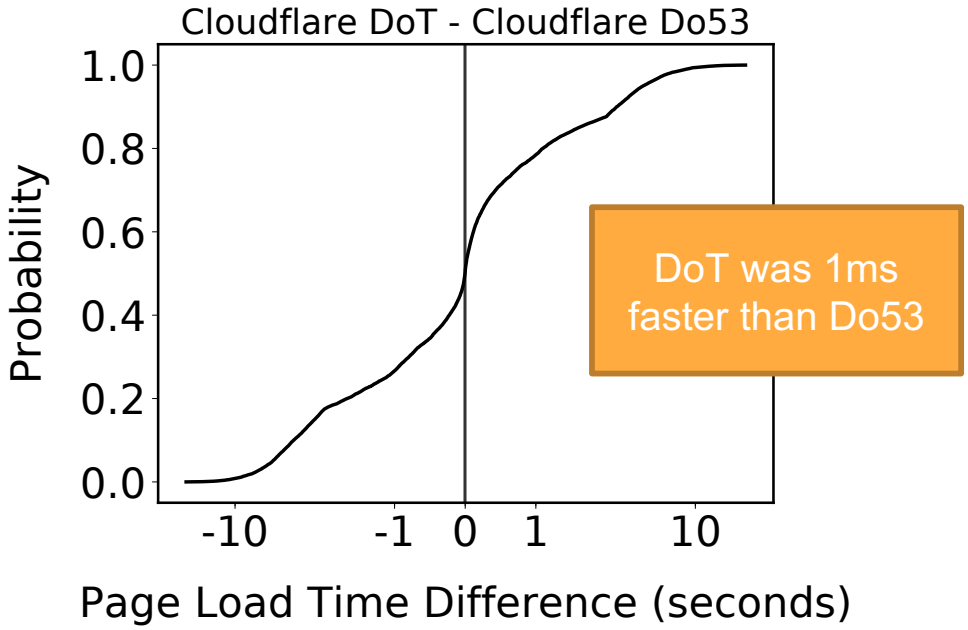
Page Loads with Cloudflare at Ohio

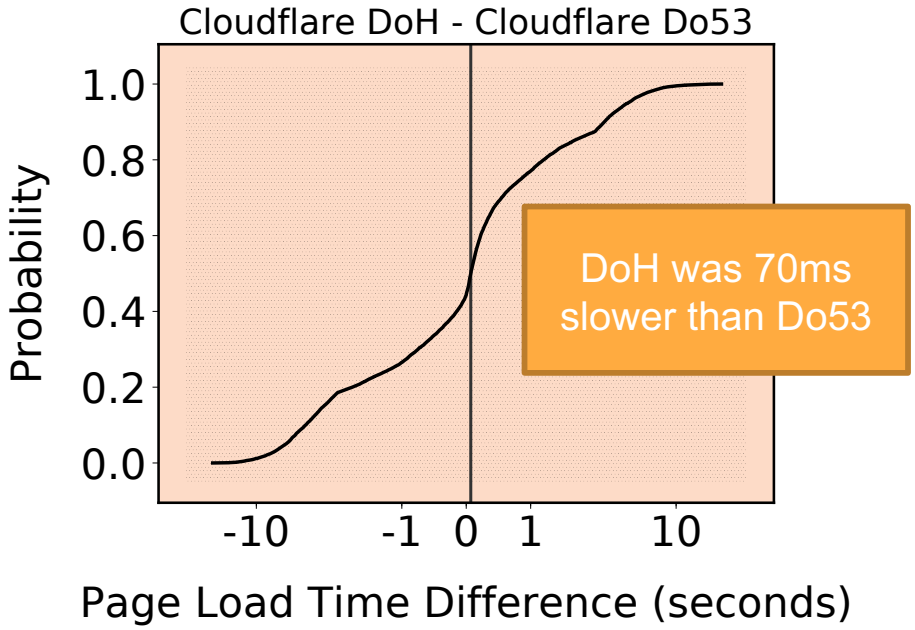


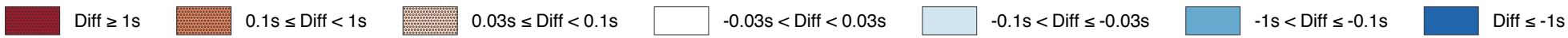




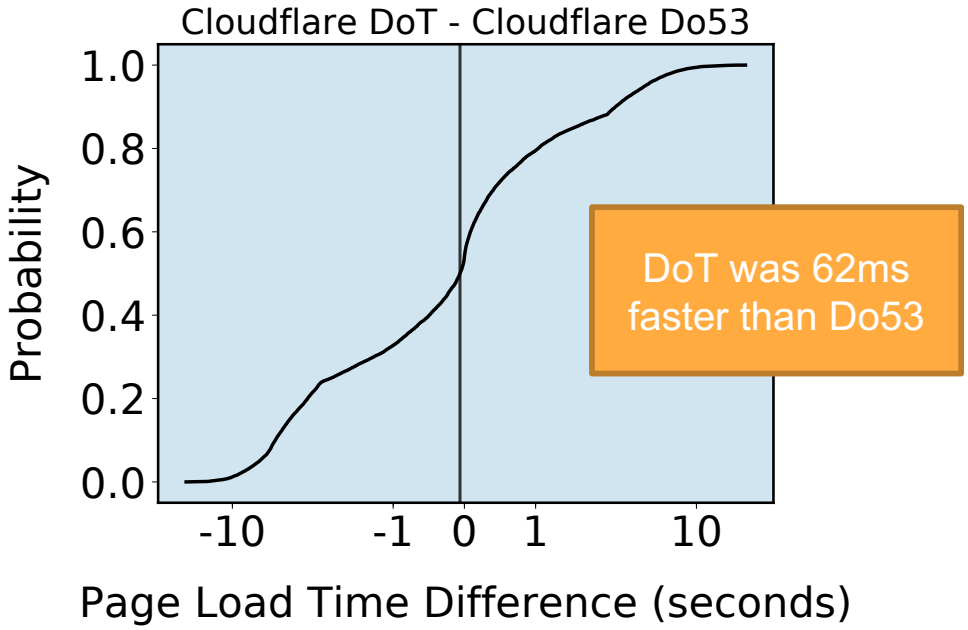
Page Loads with Cloudflare at Ohio (4G)

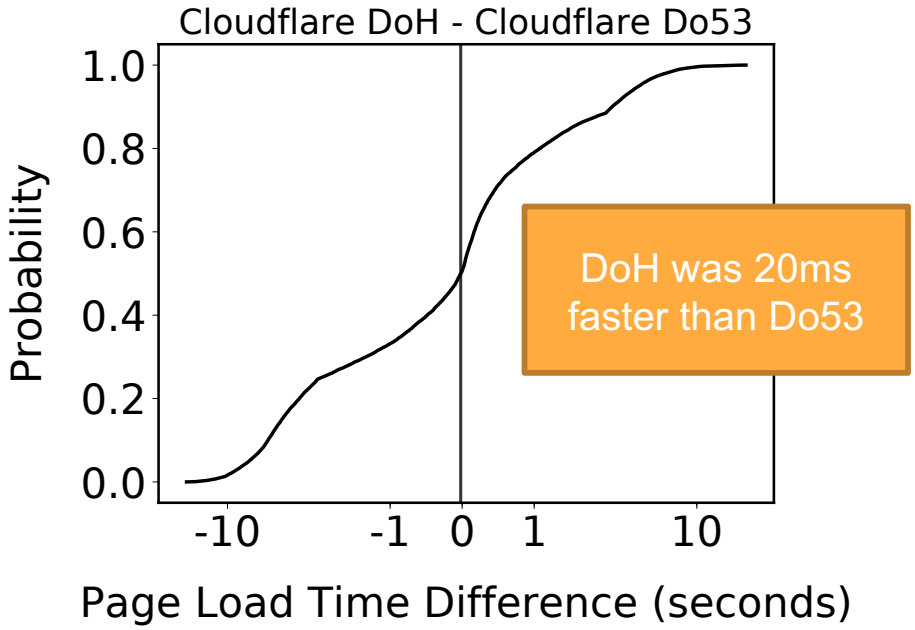


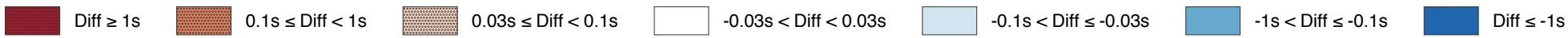




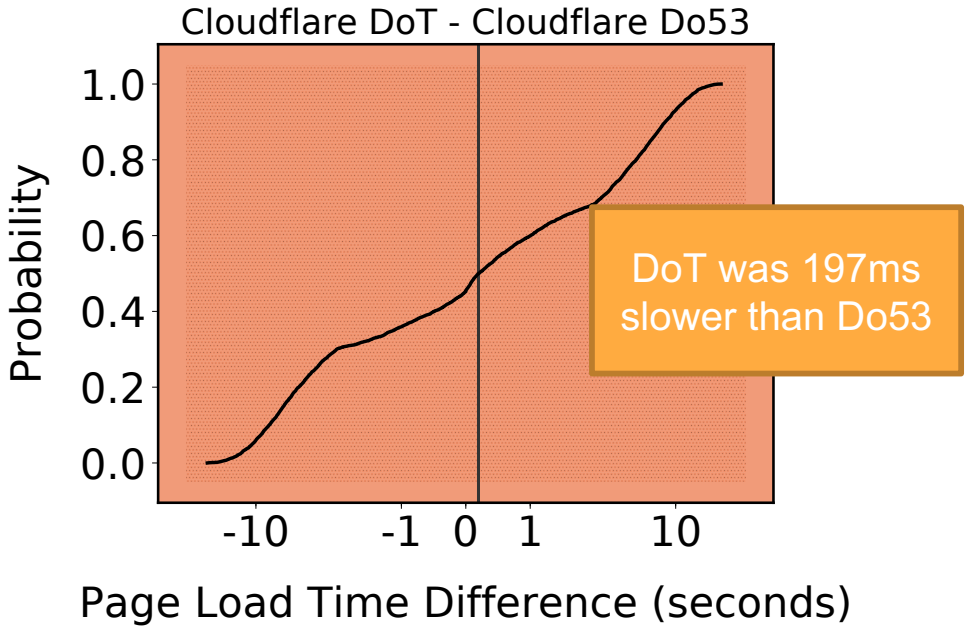
Page Loads with Cloudflare at Ohio (Lossy 4G)

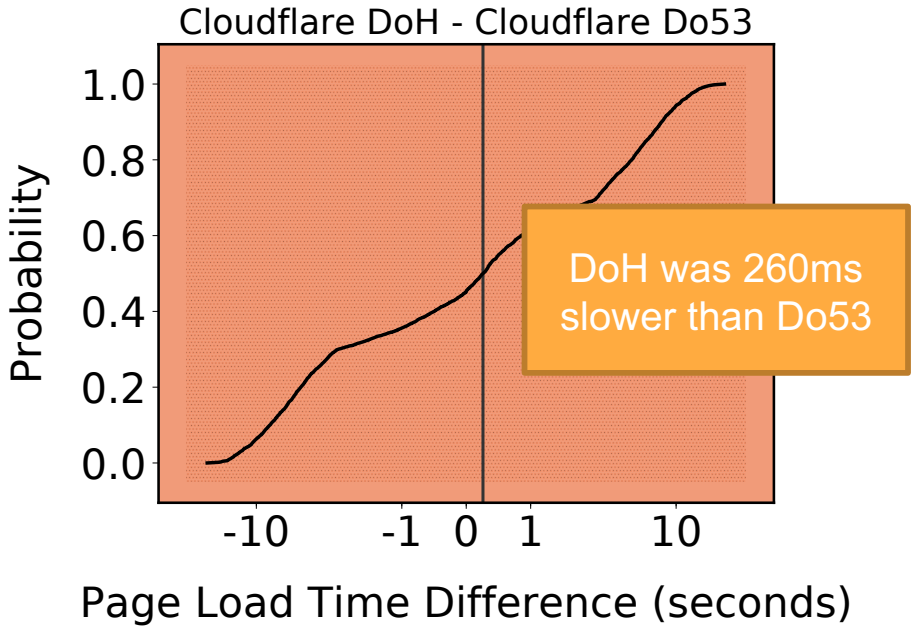


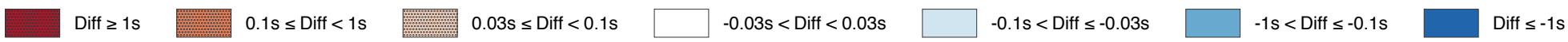




Page Loads with Cloudflare at Ohio (3G)







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

- Extensive performance study of Do53, DoT, and DoH
  - Query response times
  - Page load times
  - Emulated network conditions
- Future work: performance analyses over diverse networks