

An Empirical Study of the Cost of DNS-over-HTTPS


Timm Böttger, Felix Cuadrado, Gianni Antichi, Eder Leão Fernandes,

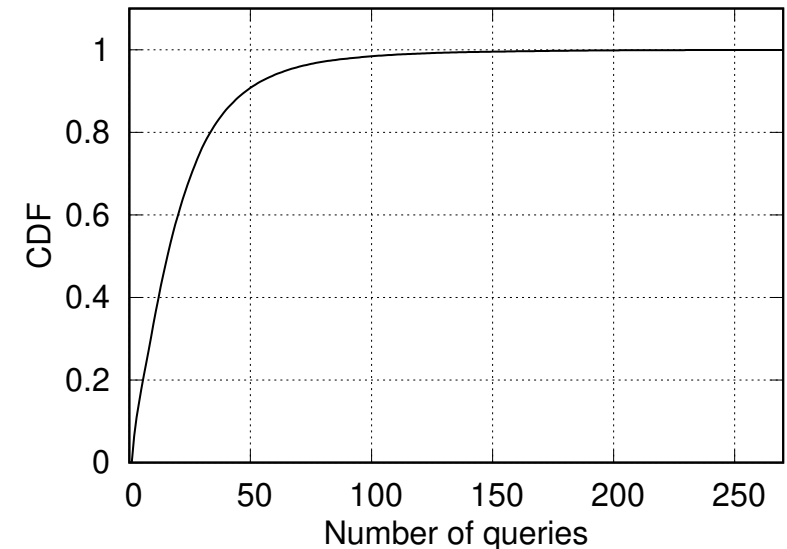
Gareth Tyson, Ignacio Castro and Steve Uhlig

timm.boettger@qmul.ac.uk



You cannot go without DNS

- Vital component for essentially all networked applications
- Especially in web context
 - Not only to access main (web-) application
 - But significant amount of embedded third-party resources
-  Critical infrastructure in today's Internet. But it is 'safe' enough?



DNS-over-HTTPs (DoH)

- Standardized as RFC 8484
- Significant support from industry, e.g.,
 - Google
 - Cloudflare
 - Mozilla
- Firefox DoH 'trial' with Cloudflare

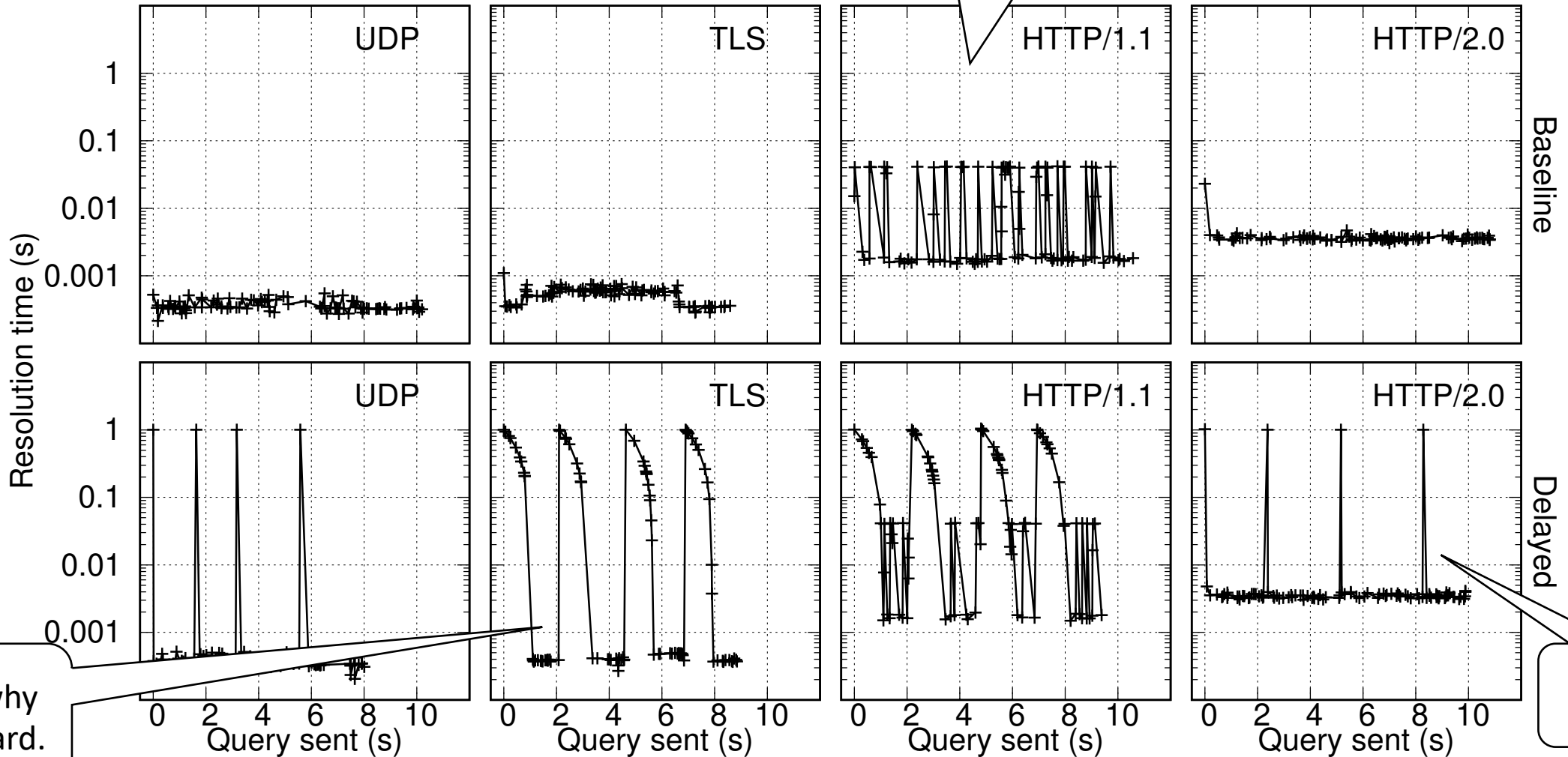


Transports for secure DNS

- Assess impact of different transport protocols on resolution time
- UDP, TLS, HTTP/1.1 with pipelining, HTTP/2.0
- Use threaded approach on client
 - Resolver can reply as fast as it can
- Send 100 requests to resolver (Poisson, 10 arrivals per second)
- Delay one in 25 queries by 1 sec on the DNS resolver

Transports for secure DNS

Major browser do not support HTTP/1.1 with pipelining



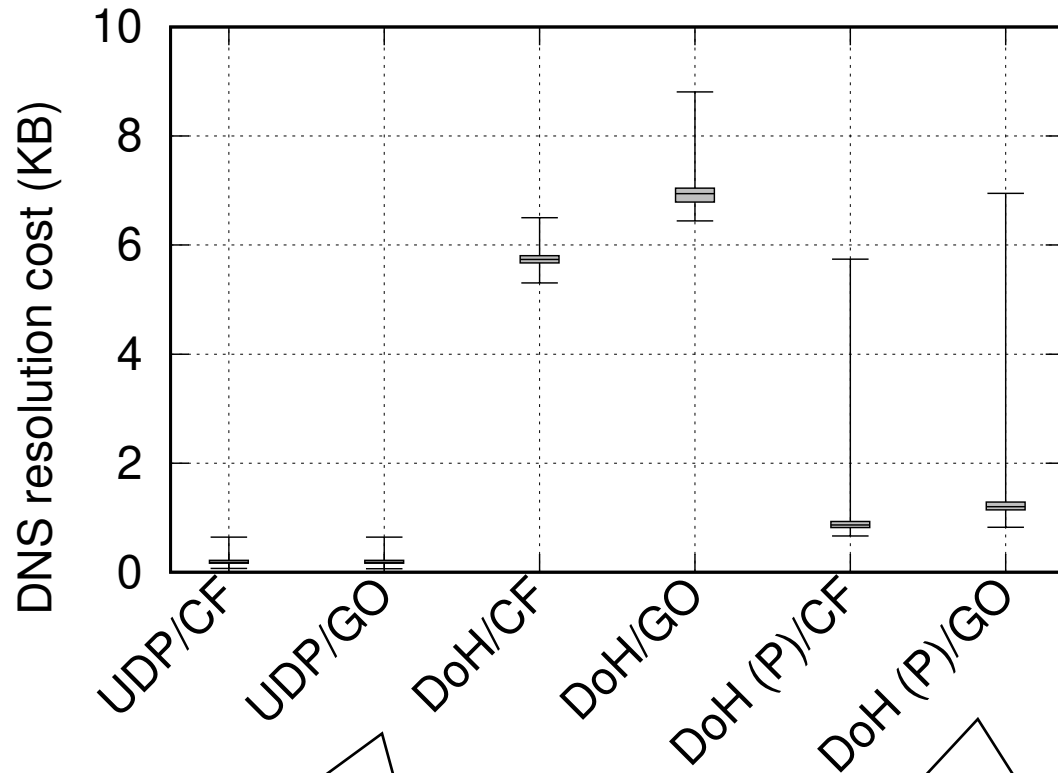
This is why DoT is hard.

Use HTTP/2.0

Cost of DoH

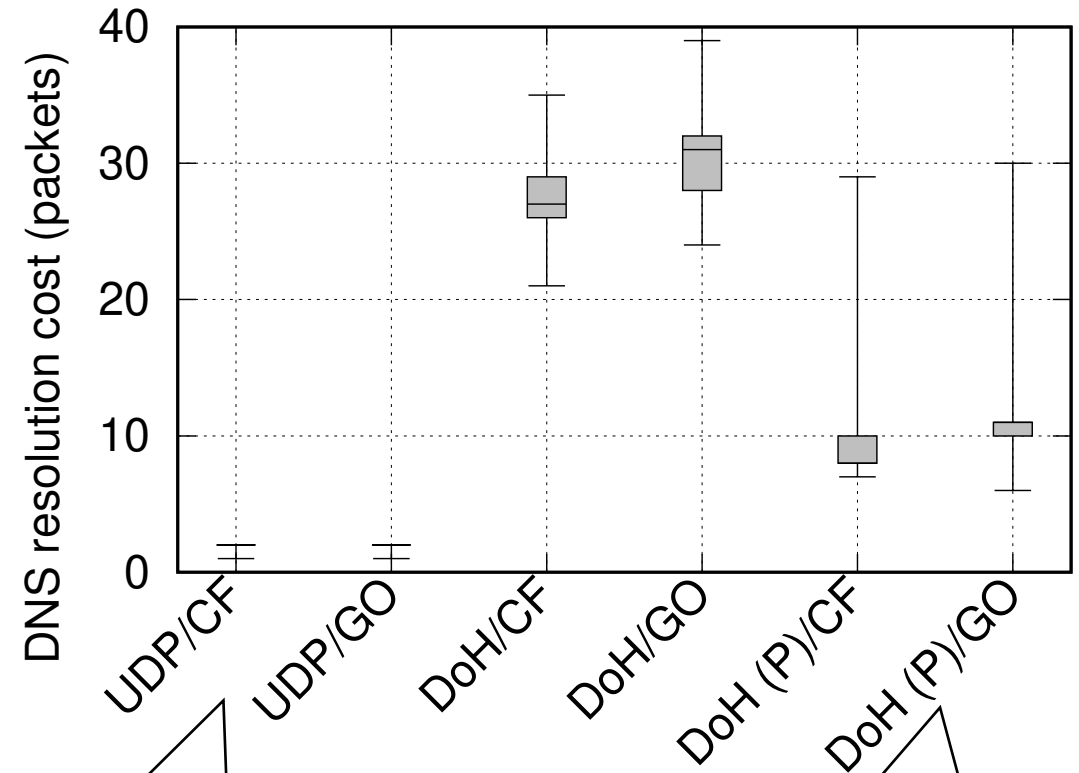
- Instances isolated via Docker containers
- Firefox webbrowser with DoH support
- Use a realistic (?) set of domain names
 - Fetch Alexa Top 100k
 - 2,178,235 DNS queries
 - 281,414 unique domain names

The cost of DoH



DoH consumes more bytes (up to 30x)

Batching of requests necessary (4x overhead)



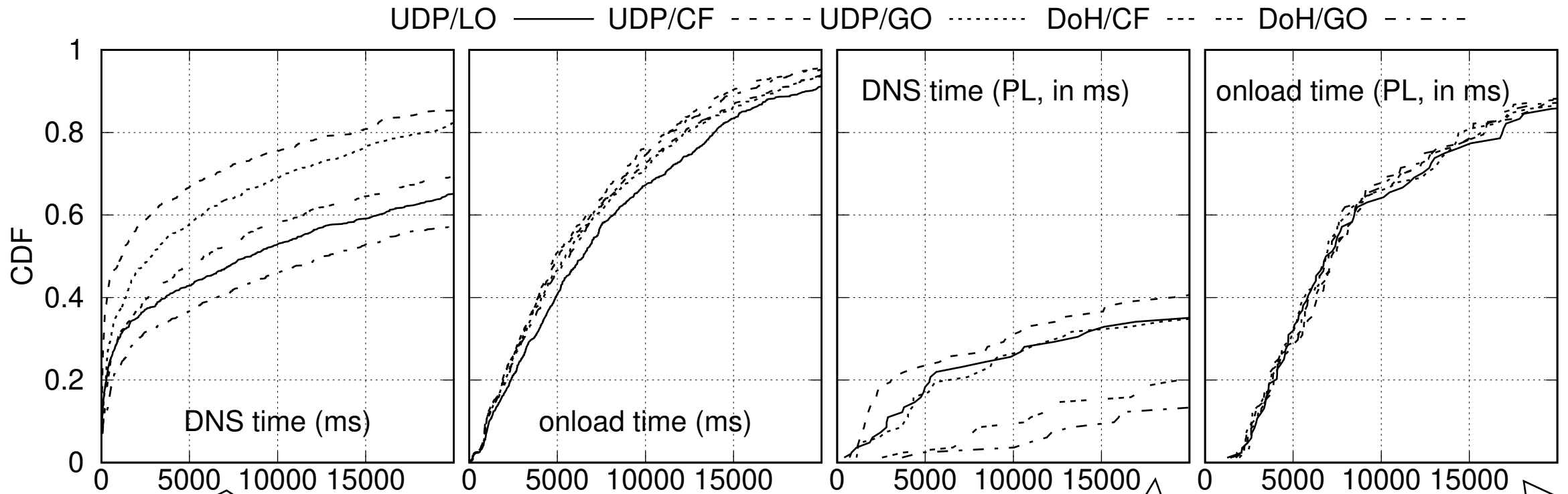
UDP DNS two packet exchange

Up to 15x packet overhead

Performance impact of DoH

- Resolve top 1,000 Alexa pages, 3x each
- Measure DNS time (sequentially) and onload event
- Firefox webbrowser with DoH support
- sitespeed.io framework for instrumentation
 - They make Browsertime (wrapping scripts + Selenium + browser instrumentation)
- Experiments mostly from local vantage point
- Tried to use PlanetLab, but many nodes unavailable or outdated

Performance impact of DoH



UDP faster than DoH

Slow local
resolver

Similar
loadtimes, again
local is slower

Very limited
coverage

Same trend in results
(except for local
resolver)

Summary

- DoH is out there and strongly supported
- With HTTP/2.0 first usable standard (head of line blocking)
- DoH comes with higher overhead compared to plain UDP
- Can come without apparent performance penalties
 - But further research needed here.