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
{ahounsel,borgolte,pschmitt,jordanah,feamster}@cs.princeton.edu

Abstract

We measure the effect of DoH and DoT on name resolution performance and content delivery. We find that although DoH and DoT response times can be higher than for conventional DNS (Do53), *DoT performs better than DoH and Do53 in terms of page load times.* However, when network conditions degrade, webpages load quickest with Do53, and up to one second faster compared to DoH. Furthermore, in a substantial amount of cases, a webpage may not load at all with DoH, while it loads successfully with DoT and Do53. Our in-depth analysis reveals various opportunities to readily improve DNS performance, for example through *opportunistic partial responses* and *wire format caching*.

1 Introduction

The Domain Name System (DNS) underpins nearly all Internet communication; DNS lookups map human-readable domain names to corresponding IP addresses of Internet endpoints. Because nearly every Internet communication is preceded by a DNS lookup—and because some applications, including the Web, may require tens to hundreds of DNS lookups for a single transaction such as a page load—the performance of DNS is a paramount concern. Many historical DNS design decisions and implementations (e.g., caching, running DNS over UDP instead of TCP) have thus focused on minimizing the latency of each DNS lookup.

In the past several years, however, DNS privacy has become an significant concern and design consideration [1]. Past research has shown that DNS lookups can reveal various aspects of user activity including the web sites and web pages that a user is visiting, and even the devices that a user may have in their home (and how they are using them) [2, 7]. As a result, various efforts have developed to send DNS queries over different transport protocols—including encrypted transport. Two prominent examples are DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH) [3, 4]. In both cases, a client sends DNS queries to the resolver over an encrypted transport, which in turn relies on the Transmission Control Protocol (TCP).

Encrypted transports introduce new performance costs, including the overhead associated with TCP and TLS connection establishment, as well as additional application-layer overhead. The extent of these performance costs is not yet well-understood. An early preliminary study from Mozilla found that DoH lookups are only marginally slower than conventional, unencrypted DNS over port 53 (Do53). However, Mozilla only measured resolution timings, which does not reflect the holistic end-user experience [6].

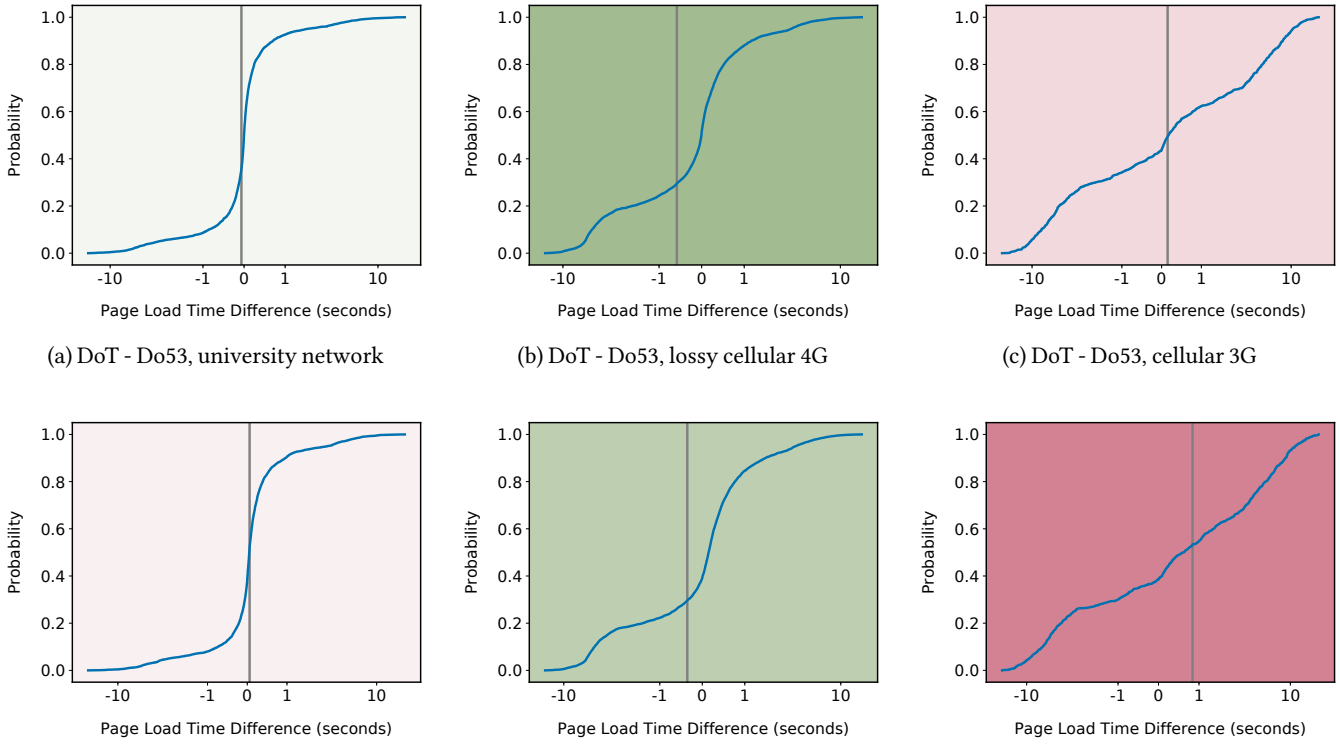
This work seeks to measure how encrypted transports for DNS affect end-user experience in web browsers. We find that DNS queries are typically slower with encrypted transports. Much to our surprise, however, we discovered that using DoT results in *faster* page load times compared to using Do53 and DoH. When exploring the underlying reasons for this behavior, we discovered that encrypted transports have previously ignored quirks that significantly affect application performance. For example, although DoT utilizes a reliable, encrypted transport layer, the initial overhead of TCP and TLS connection establishment for DoT can be amortized over ≈23 DNS queries, which is a relatively small number of queries for modern applications.

This paper makes the following contributions:

- *We provide the first extensive performance study of Do53, DoT, and DoH.* We measure DNS lookup and page load times across Do53, DoT, and DoH. We evaluate these DNS transports and implementations of them using popular open recursive resolvers operated by Cloudflare, Quad9, and Google, as well as a conventional DNS resolver operated by a university network.
- *We show that encrypted DNS transports can lead to improved user experience compared to unencrypted DNS.* We find that DNS lookup times for DoH and DoT are generally slower than Do53. However, page load times are often *fastest* when using DoT. We offer several possible explanations, such as differences in UDP application timeouts and TCP retransmission times.
- *We give generally applicable insights to optimize DNS performance.* We identify underlying reasons for why DoT outperforms Do53 in page load times. Based on these insights, we then propose several optimizations to improve DNS lookup times, such as wire-format caching and support for partial responses.

ANRW '19, July 22, 2019, Montreal, QC, Canada

ACM ISBN 978-1-4503-6848-3/19/07…$15.00
341129



(a) DoT - Do53, university network

(b) DoT - Do53, lossy cellular 4G

(c) DoT - Do53, cellular 3G

(d) DoH - Do53, university network

(e) DoH - Do53, lossy cellular 4G

(f) DoH - Do53, cellular 3G

Figure 1: Comparison of page load times using Cloudflare's resolver from three networks.

2 Effect of Network Conditions

To understand the relationship between network conditions and DNS protocols, we measure page load times while using Cloudflare's recursor. We single out Cloudflare because their recursors performed best in comparison to all others in terms of page load times. Figure 1 compares page load times across a university network, a lossy cellular 4G network, and a cellular 3G network. Each plot shows a CDF for the difference in page load times between two protocols on a given network.

Page loads that use Cloudflare Do53, DoT, and DoH on a university network perform similarly well, with DoT performing slightly better than Do53 (1a), and DoH performing slightly worse than Do53 (1d). However, on the lossy 4G network, DoT performs significantly better than Do53 (1b), and DoH performs better than Do53 (1e).

It may seem counter-intuitive that page loads using DoT and DoH perform better than Do53 on the lossy 4G network. However, we hypothesize that the differences between how TCP and UDP handle timeouts offer a possible explanation. For example, the default timeout for Do53 requests in Linux is set to 5 seconds by `resolvconf` [5]. For DoT and DoH on the other hand, DNS packets may be retransmitted within 2x the round-trip-time latency to a recursive resolver because of TCP. If the round-trip time to a recursive resolver is on the order of hundreds of milliseconds, then DoT and DoH will more quickly re-transmit dropped packets than Do53.

However, as throughput decreases and loss increases on a 3G network, DoT and DoH are no longer able to outperform Do53 in page loads. We believe this can be attributed to their higher overhead compared to Do53, which contributes to link saturation for most websites. Correspondingly, DoH has a higher overhead than DoT, which leads to significantly slower page loads (Figure 1c and Figure 1f).

3 Conclusion

In this work, we investigated DNS timings and page load times using different DNS transport protocols in multiple network conditions. We find that although privacy-focused DNS protocols result in higher resolution times for individual queries, page load times improve due to inherent benefits of the underlying transport protocols.

Our findings also indicate that a user's recursor choice can have a significant impact on the number of pages that load successfully, and reduce the time they need to load. Therefore, users should choose their DNS protocol based on network conditions and their recursor based on intuitive metrics like successful page loads and page load time, instead of pure DNS response time, as the specific recursor choice can lead to direct quality of life improvements.

References

[1] Stephane Bortzmeyer. *DNS Privacy Considerations*. Tech. rep. 7626. (Informational). RFC Editor, Aug. 2015. URL: http://www.ietf.org/rfc/rfc7626.txt.

[2] Wes Hardaker. "Analyzing and Mitigating Privacy with the DNS Root Service". In: *Proceedings of the 2018 DNS Privacy Workshop*. Ed. by Sara Dickinson, Allison Mankin, and Melinda Shore. San Diego, CA, USA: Internet Society (ISOC), Feb. 18, 2018. URL: https://www.isi.edu/%5C%7ehardaker/papers/2018-02-ndss-analyzing-root-privacy.pdf (visited on 05/13/2019).

[3] Paul Hoffman and Patrick McManus. *DNS Queries over HTTPS (DoH)*. Tech. rep. 8484. (Proposed Standard). RFC Editor, Oct. 2018. URL: http://www.ietf.org/rfc/rfc8484.txt.

[4] Zi Hu, Liang Zhu, John Heidemann, Allison Mankin, Duane Wessel, and Paul Hoffman. *Specification for DNS over Transport Layer Security (TLS)*. Tech. rep. 7858. (Proposed Standard). RFC Editor, May 2016. URL: http://www.ietf.org/rfc/rfc7858.txt.

[5] Michael Kerrisk. *resolv.conf - Linux Manual Page*. URL: http://man7.org/linux/man-pages/man5/resolv.conf.5.html (visited on 05/30/2019).

[6] Patrick McManus. *Firefox Nightly Secure DNS Experimental Results*. Aug. 28, 2018. URL: https://blog.nightly.mozilla.org/2018/08/28/firefox-nightly-secure-dns-experimental-results/ (visited on 05/11/2019).

[7] Liang Zhu, Zi Hu, John Heidemann, Duane Wessels, Allison Mankin, and Nikita Somaiya. "Connection-oriented DNS to Improve Privacy and Security". In: *Proceedings of the 36th IEEE Symposium on Security & Privacy (S&P)*. Ed. by Vitaly Shmatikov and Lujo Bauer. San Jose, CA, USA: Institute of Electrical and Electronics Engineers (IEEE), May 2015. ISBN: 978-1-4673-6949-7. DOI: 10.1109/sp.2015.18.