An Examination of Performance in Handling Multiple DNS Protocols Concurrently

Satoru Sunahara[1] and Saki Shiomi[2] Shigeki Hagihara[2]

[1] Hokkaido University, Kita 8 Nishi 5, Kita-ku, Sapporo, Hokkaido, Japan, suna@iic.hokudai.ac.jp,
[2] Chitose Institute of Science and Technology, 758-65 Bibi, Chitose, Hokkaido, Japan

Abstract. This study investigates the performance impact of concurrent queries on encrypted DNS protocols. We conducted experiments on a virtual machine, measuring query response times under several conditions. We compared single versus concurrent queries for individual protocols (Do53, DoT, DoH, DoH3, and DoQ), both with and without server certificate validation. We also isolated the time consumed by certificate validation and evaluated performance when low-overhead Do53 and high-overhead encrypted DNS queries were issued concurrently. Results showed that concurrent queries increased response times for all protocols, with the effect being most pronounced for encrypted protocols requiring certificate validation. This performance degradation was attributed to CPU resource contention during the computationally intensive validation process, as name resolution time remained stable. Interestingly, in mixed-protocol tests, Do53 performance degraded while encrypted protocol performance improved. We conclude that DNS query performance is highly dependent on computational resource allocation, a critical consideration for server configuration.

Keywords: DNS Performance, DNS over TLS, DNS over HTTPS, DNS over QUIC, DNS over HTTP/3, Privacy Enhancement

1 Background and Objectives

The Domain Name System (DNS) is a system that manages the correspondence between Internet Protocol (IP) addresses and domain names within IP networks, playing a vital role in enabling users to access the Internet. In recent years, encrypted DNS protocols such as DNS over TLS (DoT) [8], DNS over HTTPS (DoH) [5], and DNS over QUIC (DoQ) [9] have been proposed and are gradually being adopted, providing enhanced protection of user privacy through encryption. However, because encrypted DNS protocols require cryptographic computations, they generally exhibit degraded performance, for example, in terms of response time, when compared with traditional DNS. At present, if scalability is prioritized, traditional DNS remains the preferable choice, whereas if privacy protection is desired, one must accept the performance tradeoffs associated with encrypted DNS protocols [7][12][17].

J. Caro et al. (eds.), *Proceedings of the Workshop on Computation: Theory and Practice (WCTP 2025)*, Atlantis Highlights in Computer Sciences 24,
https://doi.org/10.2991/978-94-6239-638-8_30

The fundamental scaling strategy for DNS servers involves increasing the number of physical servers and distributing the load among them. To ensure that the traffic is not unevenly concentrated on specific servers, we may adopt a configuration in which a single DNS server supports multiple DNS protocols concurrently, in much the same way that a single web server can handle both Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) requests.

The performance of DNS protocols in single query scenarios has already been widely studied. For example, Sengupta et al. evaluated the performance of traditional DNS (hereafter referred to as Do53), DoH, and DoQ under single query conditions [16]. However, in practice, instead of deploying servers that support only a single protocol to mitigate load imbalance, a scaling policy may be adopted in which multiple servers are provisioned, each capable of supporting multiple DNS protocols. It remains unclear whether the performance characteristics observed in single query evaluations also hold under concurrent usage.

In particular, the method standardized in Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS (RFC 9539) [2] for ensuring privacy protection between full-service resolvers and authoritative DNS servers requires that Do53 and encrypted DNS protocols be requested concurrently. Under this standard, it remains unclear whether processing multiple DNS protocols concurrently can achieve performance comparable to that observed when each protocol is processed independently. In other words, when faster and slower processes are executed concurrently, there is a risk that the faster process may be adversely affected by the slower one, thereby failing to deliver its inherent performance. Accordingly, this study aims to clarify the performance impact that arises when queries using encrypted DNS protocols are executed concurrently.

2 Experimental Evaluation of Concurrent Encrypted DNS Query Performance and Protocol Interaction

This section introduces the experimental environment and elaborates on experiments concerning the performance of concurrent queries for encrypted DNS and the interaction between Do53 and encrypted DNS protocols. Section 2.1 describes the experimental environment constructed for evaluating the performance of concurrent queries for encrypted DNS. Section 2.2 details the methodology and results of performance measurements for individual protocols. Section 2.3 formulates hypotheses regarding the causes of performance degradation based on the experimental results from Section 2.2 and outlines experiments to validate these hypotheses. Section 2.4 presents a discussion confirming the validity of the hypotheses put forth in Section 2.3. Section 2.5 describes the methodology and results for measuring the performance of concurrent queries involving different protocols. Section 2.6 discusses the interaction between concurrent queries of different protocols.

2.1 Experimental Environment

This section describes the methodology for constructing an experimental environment designed to evaluate multiple distinct DNS query types. When evaluating the performance of DNS queries across different protocols, specifically DoT, DoH, DoQ, and DNS over HTTP/3(DoH3), it is crucial to unify the programming language used for their implementation. This measure ensures that observed performance discrepancies are not attributable to variations in the underlying language's efficiency. We selected natesales/q [13], which is uniformly implemented in the Go language, as the DNS client. In addition, dnsdist, primarily implemented in C++, was chosen as the DNS load balancer [14]. The configuration of the experimental environment is illustrated in Figure 1. We constructed the experimental environment within a virtualized setup on a single server in order to eliminate external factors that could degrade communication performance, such as network latency and security appliances. The physical server was equipped with 4 CPU cores, 16 GB of memory, and a Solid State Drive (SSD) for storage. Both the host OS and guest OS were Ubuntu 24.04. For the virtual machine used in the performance evaluation, 2 CPU cores and 8 GB of memory were allocated. The DNS server software used in this study was Bind9 [10].

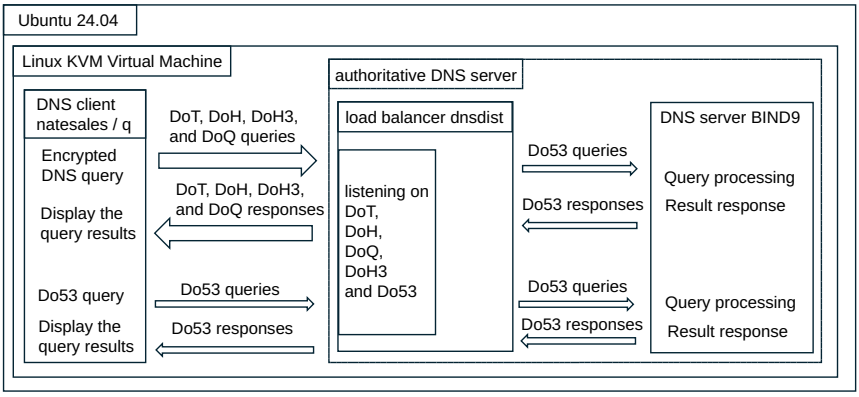

Fig. 1. Experimental environment configuration

2.2 Performance evaluation of concurrent encrypted DNS queries

As a baseline, we first measured the performance of single-protocol queries under both sequential and concurrent conditions. Specifically, we evaluated Do53, a lightweight protocol, and the encrypted protocols DoH, DoH3, DoT, and DoQ.

For each protocol, query latency was measured from initiation to completion using two methods: (i) sequential queries issued with intervals and (ii) concurrent queries issued without intervals. In the sequential case, an interval of 2000 ms was introduced between queries to prevent concurrent processing, and a total of 100 queries were executed. In the concurrent case, 100 queries were executed without any intervals. For the encrypted DNS protocols, measurements were conducted under two conditions: with and without server certificate validation.

The experimental results are summarized in Table 1. In Table 1, the condition with certificate validation indicates that server certificate validation was performed during queries, whereas without certificate validation indicates that it was not performed. The column Protocol refers to the DNS protocols evaluated, while Average, Standard Deviation, and Median respectively denote the average, standard deviation, and median query response times across 100 queries. All values were rounded to three decimal places. Furthermore, Table 2 presents the ratio of query times between sequential and concurrent executions.

As shown in Table 1, query response times increased when queries were issued concurrently without intervals, compared to sequential queries with intervals. This increase was observed for all protocols tested, both with and without server certificate validation. In addition, as shown in Table 2, for encrypted protocols without certificate validation, the ratio of query times between concurrent and sequential executions averaged 15.961, with a maximum of 25.510 for Do53. In contrast, when certificate validation was enabled, the ratio increased further, averaging 38.825 and reaching a maximum of 42.483 for DoQ. These results demonstrate that performing server certificate validation leads to larger increases in query time ratios compared to cases without validation.

2.3 Discussion and Hypotheses on the Performance of Concurrent Encrypted DNS Queries

From the results described in Section 2.2, it was observed that concurrent queries using encrypted DNS protocols significantly increased query times. Furthermore, query times were found to be larger when server certificate validation was performed than when it was not. Since certificate validation involves public-key cryptographic operations, which are computationally expensive, we formulated the following hypothesis:

Hypothesis: Concurrent queries induce contention for computational resources such as CPU within the server. As a result, fewer resources are available per query compared to sequential execution, thereby increasing query times.

To test this hypothesis, we modified the q command to measure the time required for certificate validation as well as the time required for name resolution. Following this modification, we conducted the following experiments. For Do53, DoH, DoH3, DoT, and DoQ, we measured three metrics under two conditions sequential queries with intervals and concurrent queries without intervals: (i) the total query time, defined as the time from query initiation to completion, (ii) the certificate validation time, defined as the time from query initiation to the completion of the handshake including server certificate validation, and (iii)

Table 1. Performance Measurement Results of Single and Concurrent Queries Across Protocols

Condition	Protocol	Average (ms)	Standard Deviation (ms)	Median (ms)
Certificate Validation: Enabled Single Query	DoH	18.742	4.957	17.636
	DoH3	19.401	3.780	18.531
	DoT	18.324	4.598	17.417
	DoQ	19.159	4.169	18.304
Certificate Validation: Enabled Concurrent Queries	DoH	634.020	195.772	629.429
	DoH3	812.936	245.545	783.318
	DoT	679.505	190.535	667.800
	DoQ	813.946	246.983	822.967
Certificate Validation: Disabled Single Query	Do53	0.639	0.175	0.616
	DoH	3.397	1.343	3.108
	DoH3	3.989	0.900	3.821
	DoT	3.025	0.858	2.872
	DoQ	3.668	0.954	3.541
Certificate Validation: Disabled Concurrent Queries	Do53	16.301	12.087	13.759
	DoH	36.612	19.119	35.556
	DoH3	59.717	33.376	59.341
	DoT	39.477	27.855	35.606
	DoQ	56.840	38.038	53.236

the name resolution time, defined as the time from the completion of the handshake to query completion. For encrypted DNS protocols, measurements were conducted under both conditions—with and without server certificate validation. As in Section 2.2, the sequential method introduced a 2000 ms interval between queries to prevent overlapping processing, with 100 queries issued in total, whereas in the concurrent method, 100 queries were issued without intervals.

The experimental results are summarized in Table 4. In this table, the encryption time refers to the duration from query initiation to handshake completion, while the name resolution time refers to the duration from handshake completion to query completion. The increase in query time for concurrent execution, compared to sequential execution, was observed primarily in the handshake phase (from query initiation to handshake completion). By contrast, the duration from handshake completion to query completion showed almost no variation, regardless of the DNS protocol or query interval. These findings indicate that the increase in query time is attributable to the additional computational load imposed by cryptographic operations during certificate validation.

2.4 Discussion on the Impact of Interactions in Queries

From Table 3, it can be observed that when comparing sequential and concurrent queries, there is little difference in the time required for name resolution, whereas a substantial difference is seen in the time required for certificate vali-

Table 2. Ratio of Concurrent Query Time to Single Query Time

Condition	Protocol	Query Time Ratio
Certificate Validation: Enabled Ratio of Concurrent Query Time to Single Query Time	DoH	33.829
	DoH3	41.902
	DoT	37.083
	DoQ	42.483
	Average	38.825
Certificate Validation: Disabled Ratio of Concurrent Query Time to Single Query Time	Do53	25.510
	DoH	10.777
	DoH3	14.970
	DoT	13.049
	DoQ	15.496
	Average	15.961

dation. Considering that server certificate validation requires significant computational resources, this result supports our hypothesis that concurrent queries cause contention for computational resources such as CPU, thereby reducing the resources available per query compared to sequential execution and increasing the time required for certificate validation.

Whether to perform certificate validation and whether to employ encrypted DNS protocols should ultimately depend on the performance and privacy requirements of users and server administrators. If the goal is to maximize query performance without considering privacy protection, queries using Do53 should be adopted, as they can be completed within 0.05 seconds even under concurrent load on the server. Conversely, prioritizing privacy protection by employing certificate validation and encrypted DNS protocols introduces a performance penalty, as query times increase when the server is under load. However, our experimental results indicate that even under concurrent load, queries are completed in less than one second on average. Therefore, if such performance degradation is acceptable, the use of certificate validation and encrypted DNS protocols is a valid and effective choice for enhancing privacy protection.

RFC 9539 outlines the internationally recommended standards for DNS protocols as established by the Internet Engineering Task Force (IETF). It states that adverse effects, such as excessive consumption of computational resources (e.g., CPU and memory), should be minimized. Moreover, while server certificate validation enables more secure communication, it should remain optional for users and server administrators, and connections should be accepted regardless of whether certificate validation is performed. Since the degree of performance degradation under load varies depending on whether certificate validation is conducted, an alternative option is to use encrypted DNS protocols without certificate validation.

In this section, we evaluated the performance of DNS protocols when used individually, comparing Do53 with encrypted DNS protocols. However, because encrypted DNS protocols are not fully compatible with Do53, it is difficult to

Table 3. Measurement Results of Time Required for Certificate Validation and Name Resolution

Condition	Protocol	Time Required for Certificate Validation(ms)	Time Required for Name Resolution(ms)
Certificate Validation: Enabled Single Query	DoH	18.702	0.034
	DoH3	19.332	0.057
	DoT	18.292	0.027
	DoQ	19.085	0.061
Certificate Validation: Enabled Concurrent Queries	DoH	633.949	0.059
	DoH3	812.798	0.129
	DoT	679.457	0.041
	DoQ	813.865	0.069
Certificate Validation: Disabled Single Query	Do53	0.587	0.041
	DoH	3.330	0.055
	DoH3	3.905	0.069
	DoT	2.927	0.077
	DoQ	3.592	0.061
Certificate Validation: Disabled Concurrent Queries	Do53	21.269	0.030
	DoH	36.567	0.040
	DoH3	59.648	0.025
	DoT	39.434	0.039
	DoQ	56.787	0.048

achieve a unified deployment of DNS protocols. In practice, therefore, both Do53 and encrypted DNS protocols are expected to be used concurrently. Furthermore, RFC 9539 specifies that queries should ideally be issued unilaterally and concurrently using both Do53 and encrypted DNS protocols. It remains unclear, however, whether the concurrent use of DNS protocols with differing computational requirements affects query performance.

Accordingly, the next section presents an evaluation of the performance impact when queries are executed concurrently across DNS protocols with different computational complexities.

2.5 Performance Measurement of concurrent Queries to Do53 and Encrypted DNS Protocols

To examine whether concurrent queries using DNS protocols with different computational complexities affect performance, we conducted a series of measurements. In these experiments, Do53, which is a lightweight protocol, was combined with one of the encrypted protocols, namely DoH, DoH3, DoT, or DoQ. Query completion times from initiation to termination were measured when queries were issued concurrently without intervals. For the encrypted DNS protocols, measurements were performed under two conditions: with server certificate validation and without server certificate validation. As in Section 2.2, 100 queries were executed consecutively without intervals.

Table 4 shows the query times of Do53 when executed concurrently with encrypted DNS protocols, while Table 5 shows the query times of the encrypted DNS protocols when executed concurrently with Do53. In Tables 4 and 5, Protocol refers to the DNS protocol for which the query time was measured, and Concurrent Protocol refers to the DNS protocol executed concurrently with it. The entries without certificate validation (reference) and with certificate validation (reference) correspond to the average query times for each DNS protocol when executed individually, as reported in Table 1. Furthermore, Table 6 presents the ratio of query times for concurrent execution relative to single-protocol execution.

The experimental results show that when Do53 was executed concurrently with DoH, DoH3, DoT, or DoQ, its query time increased compared to its execution in isolation, as indicated in Table 6. In contrast, the encrypted DNS protocols exhibited reduced query times when executed concurrently with Do53, as shown in Table 5. This trend was observed both with and without server certificate validation. As reported in Table 6, without certificate validation, the ratio of concurrent to single-protocol query times averaged 1.200 for Do53 and 0.544 for the encrypted DNS protocols. With certificate validation, the ratios averaged 2.097 for Do53 and 0.440 for the encrypted DNS protocols. These results indicate that when Do53 and encrypted DNS protocols were executed concurrently, the performance of Do53 decreased while the performance of the encrypted DNS protocols improved. Moreover, the magnitude of both performance degradation and improvement became more pronounced when server certificate validation was enabled.

Table 4. Query Time of Do53 When Queried Concurrently with Encrypted DNS

Certificate Validation	Protocol	Concurrently Queried Protocols	Average (ms)	Standard Deviation (ms)	Median (ms)
Enabled	Do53	DoH	33.682	19.019	34.586
		DoH3	35.477	21.507	34.152
		DoT	32.789	18.523	33.586
		DoQ	34.773	20.943	35.034
Disabled	Do53	DoH	18.370	11.698	17.819
		DoH3	20.440	11.237	19.514
		DoT	18.178	12.167	16.189
		DoQ	21.245	12.587	20.713
(Reproduced from Table 1) -	Do53	-	16.301	12.087	13.759

2.6 Discussion on the Performance Measurement of Concurrent Queries to Do53 and Encrypted DNS Protocols

From the results described in Section 2.5, it was found that when Do53 and encrypted DNS protocols were queried concurrently, the performance of the en-

Table 5. Query Time of Encrypted DNS When Queried Concurrently with Do53

Certificate Validation	Protocol	Concurrently Queried Protocols	Average (ms)	Standard Deviation (ms)	Median (ms)
Enabled	DoH	Do53	310.891	97.928	308.376
	DoH3		356.846	126.207	349.958
	DoT		293.467	93.860	286.910
	DoQ		324.111	112.467	313.857
Disabled	DoH	Do53	23.202	12.327	22.634
	DoH3		28.797	12.857	28.468
	DoT		22.832	11.967	21.439
	DoQ		27.462	12.873	27.537
(Reproduced from Table 1) Enabled	DoH	-	634.020	195.772	629.429
	DoH3		812.936	245.545	783.318
	DoT		679.505	190.535	667.800
	DoQ		813.946	246.983	822.967
(Reproduced from Table 1) Disabled	DoH	-	36.612	19.119	35.556
	DoH3		59.717	33.376	59.341
	DoT		39.477	27.855	35.606
	DoQ		56.840	38.038	53.236

crypted DNS protocols, which impose a heavier computational load, improved compared to when they were executed individually. This improvement occurred because the coexistence of Do53 queries reduced the number of encrypted DNS queries processed concurrently by the server, thereby leaving more computational resources available per query.

When server certificate validation was enabled, Figures 2 and 3 illustrate the start and end times of DoH queries. Figure 2 shows the timing of DoH queries when executed alone under concurrent conditions, whereas Figure 3 shows the timing when DoH queries were executed concurrently with Do53. The query timeline is expressed relative to the time at which the server received the first query, designated as time zero.

As shown in Figure 2, the execution intervals of individual DoH queries overlap significantly when DoH is executed alone. In contrast, Figure 3 indicates that DoH and Do53 queries are processed alternately, resulting in less overlap in their execution intervals. Consequently, resource contention is reduced, and the execution duration of DoH queries becomes shorter when executed concurrently with Do53 compared to when executed in isolation. In addition, while delays in the initiation of some queries were observed in the case of DoH alone, such delays largely disappeared when DoH was executed concurrently with Do53. These observations suggest that encrypted DNS protocols with heavy computational demands can achieve improved performance, such as reduced query times and fewer delays, when executed concurrently with lightweight protocols like Do53, due to the reduction of concurrent load and mitigation of resource contention.

On the other hand, the performance of Do53, the lightweight protocol, was degraded when executed concurrently with encrypted DNS protocols. This degra-

Table 6. Ratio of Query Time for Multiple Protocols to that for a Single Protocol

Condition	Protocol	Concurrently Queried Protocols	Query Time Ratio
Certificate Validation: Enabled/Concurrent Queries Ratio of Query Time for Multiple Protocols to that for a Single Protocol	Do53	DoH	2.066
		DoH3	2.176
		DoT	2.011
		DoQ	2.133
		Average	2.097
Certificate Validation: Disabled/Concurrent Queries Ratio of Query Time for Multiple Protocols to that for a Single Protocol	Do53	DoH	1.127
		DoH3	1.254
		DoT	1.115
		DoQ	1.303
		Average	1.200
Certificate Validation: Enabled/Concurrent Queries Ratio of Query Time for Multiple Protocols to that for a Single Protocol	DoH	Do53	0.490
	DoH3		0.439
	DoT		0.432
	DoQ		0.398
		Average	0.440
Certificate Validation: Disabled/Concurrent Queries Ratio of Query Time for Multiple Protocols to that for a Single Protocol	DoH	Do53	0.634
	DoH3		0.482
	DoT		0.578
	DoQ		0.483
		Average	0.544

dation was caused by competition for computational resources, as the resource-intensive encrypted DNS protocols consumed a disproportionate share of CPU and other resources, leaving fewer resources available for Do53 queries.

At present, Do53 is the most widely used DNS protocol. Thus, when servers are configured to handle both encrypted DNS and Do53 queries concurrently, there are advantages, such as the ability to manage zone information within a single server. However, there is also the potential drawback that the performance of Do53, which is inherently lightweight, may degrade due to the influence of encrypted DNS queries, thereby impacting end users. Possible approaches to mitigate the degradation of Do53 performance include the following:

- Dividing servers so that each server is dedicated to handling a single type of DNS protocol, thereby avoiding competition for computational resources such as CPU.
- Implementing scheduling mechanisms within a single server that prioritize queries based on their computational demands.
- Offloading cryptographic operations, which require significant computational resources, to dedicated hardware or auxiliary systems.
- Applying rate-limiting to computationally expensive queries, such as those from encrypted DNS protocols, in order to alleviate server load.

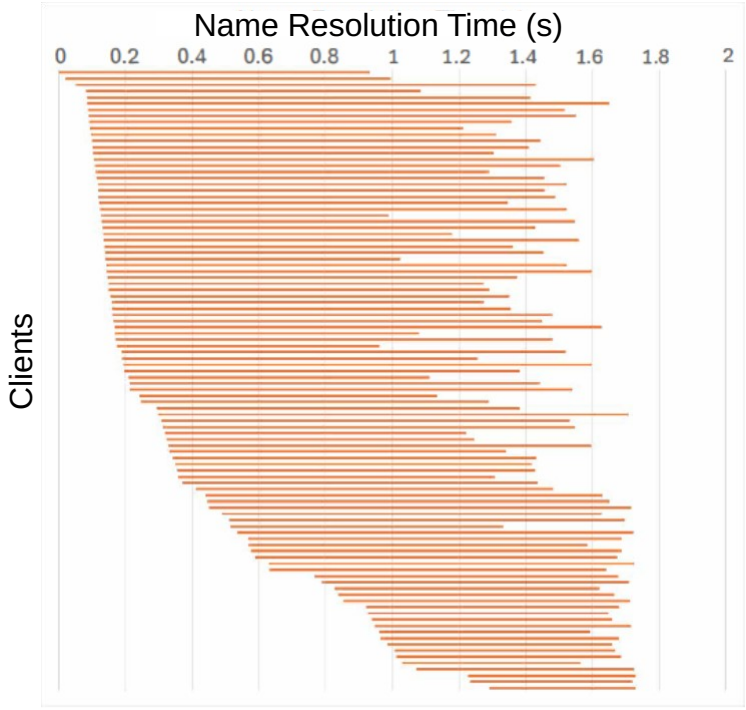

Fig. 2. Name Resolution Time from Start to Completion of a Single DoH Query

3 Related Work

A considerable number of studies have examined the performance of individual DNS protocols.

Wu et al. reported that certain implementations of DoQ fail to satisfy the requirements of the relevant RFCs (specifically those pertaining to QUIC [11]), thereby posing a risk of amplification attacks [19]. Given that DoQ relies on the QUIC protocol, stringent limitations on the amount of data sent in response to a client's request are essential for both maintaining performance and preventing such attacks.

Sunahara et al. proposed a method for detecting encrypted protocols that is both safer and faster than the conventional approach outlined in RFC 9461 [15], which relies on plaintext communication using SVCB records. Their approach involves embedding the cryptographic protocols supported by the child authori-

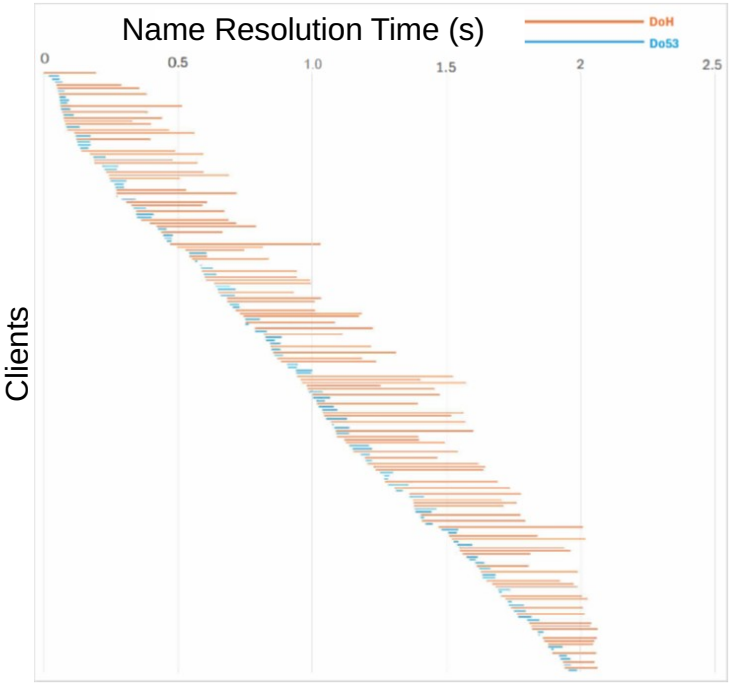

Fig. 3. Name Resolution Time from Start to Completion of Concurrent Queries to Do53 and DoH

tative DNS server directly into the NS records of the parent authoritative server [18].

Hanna et al. demonstrated that integrating DNS Security Extensions (DNSSEC) [4] and DoT into a 5G edge DNS resolver yielded superior performance compared to public DNS servers, such as OpenDNS [3].

Hounsel et al. [6] investigated the impact of traditional Do53, DoT, and DoH on query response time and web page load time. Their findings revealed that although the response times of DoH and DoT are generally longer than that of Do53, both protocols achieved better performance than Do53 in terms of page load time. However, when throughput decreased and substantial packet loss and latency occurred, Do53 provided the fastest web page loading. They further demonstrated that Do53 and DoT achieved a higher success rate in web page loading compared to DoH.

In the present study, query response time was employed as the principal performance metric for DNS protocols. Nevertheless, research on DNS performance continues to extend beyond response time. For example, Dikshit et al. [1] investigated the resilience of Do53 servers against Denial of Service (DoS) attacks. With the recent introduction of IPv6 and DNSSEC, DNS messages tend to increase in size. When fallback to Transmission Control Protocol (TCP) is exploited, message fragmentation becomes more likely, raising concerns regarding the resilience of DNS servers to DoS attacks.

4 Conclusion

In this paper, we conducted a performance evaluation of concurrent queries using encrypted DNS protocols, with the objective of gaining insights into the performance implications that arise when such queries are executed concurrently. Specifically, we measured the performance of single-protocol queries versus concurrent queries, the performance impact of server certificate validation, and the performance of concurrent queries across heterogeneous protocols. The results revealed the following:

- For single DNS protocol queries, issuing multiple queries concurrently without intervals increases query latency.
- When server certificate validation is performed, query times become significantly longer compared to cases without validation. This increase is attributable to competition for computational resources, such as CPU cycles, which prolongs query processing time.
- In concurrent queries involving DNS protocols of differing computational complexity, lightweight protocols such as Do53 exhibit degraded performance due to the influence of heavier protocols, whereas resource-intensive protocols such as DoH and DoH3 benefit from the presence of lighter protocols and demonstrate improved performance.

Through these findings, we clarified the performance impacts of concurrent queries involving Do53 and encrypted DNS protocols. This enables both end users and server administrators to make more informed choices regarding DNS protocols, selecting those that balance performance and privacy protection requirements most effectively.

This study was conducted within a virtualized environment designed to provide idealized experimental conditions. However, in operational settings, additional factors such as network latency must be considered, and it remains unclear whether performance results equivalent to those observed in the virtual environment can be achieved in practice. Therefore, further research is required to evaluate query performance in physical environments.

References

1. Dikshit, P., Kosek, M., Faulhaber, N., Sengupta, J., Bajpai, V.: Evaluating dns resiliency and responsiveness with truncation, fragmentation & dotcp fallback. IEEE Transactions on Network and Service Management pp. 1–1 (Feb 2024)
2. Gillmor, D.K., Salazar, J., Hoffman, P.E.: Unilateral opportunistic deployment of encrypted recursive-to-authoritative DNS. IETF RFC9539 (Mar 2024)
3. Hanna, Y., Pineda, D., Akkaya, K., Aydeger, A., Harrilal-Parchment, R., Albalawi, H.: Performance evaluation of secure and privacy-preserving dns at the 5g edge. In: 2023 IEEE 20th Int. Conf. on Mobile Ad Hoc and Smart Systems (MASS). pp. 89–97 (Sep 2023), DOI:10.1109/MASS58611.2023.00019
4. Hoffman, P.E.: DNS Security Extensions (DNSSEC). IETF RFC 9364 (Feb 2023)
5. Hoffman, P.E., McManus, P.: DNS queries over HTTPS (DoH). IETF RFC8484 (Oct 2018)
6. Hounsel, A., Borgolte, K., Schmitt, P., Holland, J., Feamster, N.: Comparing the effects of dns, dot, and doh on web performance. In: Proc. of The Web Conf. 2020. p. 562–572. WWW '20, Association for Computing Machinery, New York, NY, USA (Apr 2020), DOI:10.1145/3366423.3380139
7. Hu, G., Fukuda, K.: Privacy leakage of dns over quic: Analysis and countermeasure. In: 2024 Int. Conf. on Artificial Intelligence in Information and Communication (ICAIIC). pp. 518–523 (2024), DOI:10.1109/ICAIIC60209.2024.10463369
8. Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., Hoffman, P.E.: Specification for DNS over transport layer security (TLS). IETF RFC7858 (May 2016)
9. Huitema, C., Dickinson, S., Mankin, A.: DNS over dedicated QUIC connections. IETF RFC9250 (May 2022)
10. Internet Systems Consortium, Inc.: ISC Bind9, https://www.isc.org/bind/, https://www.isc.org/bind/, accessed on 21 Feb. 2025
11. Iyengar, J., Thomson, M.: QUIC: A UDP-based multiplexed and secure transport. IETF RFC9000 (May 2021)
12. Kosek, M., Schumann, L., Marx, R., Doan, T.V., Bajpai, V.: Dns privacy with speed? evaluating dns over quic and its impact on web performance. In: Proc. of the 22nd ACM Internet Measurement Conf. p. 44–50. IMC '22, Association for Computing Machinery, New York, NY, USA (2022), DOI:10.1145/3517745.3561445
13. natesales: natesales/q, https://github.com/natesales/q, accessed on 21 Feb. 2025
14. PowerDNS: dnsdist, https://www.dnsdist.org/index.html, accessed on 21 Feb. 2025
15. Schwartz, B.M.: Service binding mapping for DNS servers. IETF RFC9461 (Nov 2023)
16. Sengupta, J., Kosek, M., Fries, J., Ferlin-Reiter, S., Bajpai, V.: On cross-layer interactions of quic, encrypted dns and http/3: Design, evaluation, and dataset. IEEE Trans. on Netw. and Service Manag. 21(3), 2992–3007 (Apr 2024)
17. Sunahara, S., Jin, Y., Iida, K., Takai, Y.: A framework for institutional privacy considered full DNS over HTTPS architecture. IEEE Access (advance publication) pp. 1–14 (Feb 2025)
18. Sunahara, S., Jin, Y., Iida, K., Yamai, N., Takai, Y.: A privacy-preserving full dns over https architecture via compatible ns record based information sharing. IEICE Transactions on Communications pp. 1–15 (Sep 2025), DOI:10.23919/transcom.2025CEP0007
19. Wu, Y., Li, C., Dong, W., Dong, C., Yang, J., Zhang, H.: Post-standardization analysis of doq: Deployment, certificates ecosystem and implementation. In: NOMS 2025-2025 IEEE Network Operations and Management Symposium. pp. 1–9 (2025), DOI:10.1109/NOMS57970.2025.11073572