Analysing the Energy consumption of a DNS resolver

Nicolas Renout*, Gatien Roujanski*, Sandoche Balakrichenan† Jehan Procaccia*, Michel Marot*, Benoit Ampeau†
*SAMOVAR, Télécom SudParis, Institut Polytechnique de Paris, 91120 Palaiseau, France
†Association française Pour le Nommage Internet en Coopération (Afnic), 7 avenue du 8 mai 1945,
78280 Guyancourt, France

***Abstract*—Domain Name System (DNS) resolution, a fundamental component of Internet communication, plays a crucial role in how data centers function and deliver services to end-users. This article addresses a significant research gap in energy-efficient data center management by focusing on measuring and analysing DNS resolver energy consumption. We introduce a mathematical model to estimate the number of transmitted packets, conduct controlled experiments, and examine the energy impact of security mechanisms such as TLS handshakes and encryption/decryption processes. As part of this ongoing work, we aim to refine the model based on experimental results and leverage it to support the evaluation and optimization of DNS operations in data center environments.**

I. Introduction

In 2022, data centers consumed 460 TWh (2% of global demand) [1] of electricity, and their consumption is expected to surpass 1,000 TWh by 2026. Nearly 50% [2] of this energy is used by IT infrastructure (servers, networks, storage), emphasizing the need for energy-efficient solutions.

Domain Name System (DNS) plays a vital role in data center operations, facilitating load balancing, routing, and CDN traffic management. Originally designed as a lightweight, stateless protocol using UDP, DNS was energy-efficient with a minimal carbon footprint. However, as privacy and security concerns have grown, DNS has evolved beyond its original design, integrating encryption and reliability through protocols like DNS over TLS (DoT) [3], and HTTPS (DoH) [4] to enhance privacy, security, and resilience. With around 24% of DNS traffic now encrypted [5], its environmental impact can no longer be considered negligible. This shift highlights the need to reassess and measure the energy consumption of DNS traffic, a topic previously unexplored in research.

This ongoing work explores a key research gap by developing a preliminary methodology to measure DNS resolver energy consumption. It incorporates traffic modelling, network measurements, and an initial analysis of the energy implications of security protocols like TLS in the DNS.

II. Related Work

While existing energy measurement studies focus on web services [6], cloud computing [7] [8], and general network traffic energy efficiency [9], DNS remains overlooked despite its essential role in internet operations.

978-3-903176-74-4

However, there are reports [10] [11] which emphasize the necessity of conducting energy measurements on DNS. Focusing on DNS, the study [12] conducted at the National Institute of Standards and Technology (NIST) proposes an analytical model validated by simulation to optimise revenue loss in terms of delay and energy cost. [13] evaluates the performance of DNS software from an energy efficiency perspective.

As highlighted in the Internet Society blog [14], different stakeholders present legitimate arguments for and against the pervasive encryption of DNS traffic. In distributed systems like DNS, where approximately 24% of traffic is currently encrypted, a figure that continues to rise, the impact of encryption on power usage is becoming increasingly relevant. Research indicates that implementing security protocols such as TLS, fundamental to encrypted DNS resolution, can significantly increase energy consumption [15] [16]. Studies estimate that the energy overhead associated with TLS can reach approximately 35%, though this value varies across different research findings.

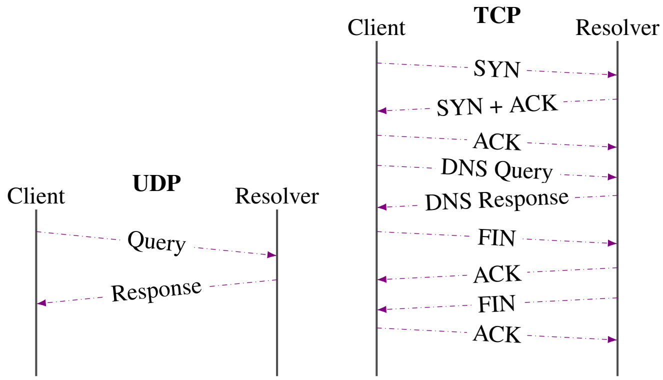
III. Mathematical model for the DNS traffic

Research conducted by USC/ISI and APNIC Labs [17] demonstrates that a single DNS query and its corresponding response can be highly verbose, potentially generating hundreds of packets due to retries, additional lookups, or protocol overhead. Mathematical modelling will help us understand complex DNS traffic behaviour. As this work is still in its early stages, we plan to begin with a simplified model to estimate the number of DNS packets exchanged with and without caching.

A. *Estimating the number of packets - UDP*

A DNS query and its corresponding response will use the same transport protocol, UDP or TCP. To count the number of packets *(N)* transmitted over a network for a DNS query/response, we derived a mathematical formula as explained below:

In the figure *(1a)*, the assumption is that the transport protocol used is UDP. To consider packet loss and the need to resend the packets, we define the retry coefficient as:$\alpha \geq 0$. To simplify the calculation, we set: $\epsilon = 1 + \alpha$, in the case of loss and $\epsilon = 1$, if there is no loss, since the retransmission coefficient $\alpha = 0$.



(a) UDP query modeling. (b) TCP query modeling.

Fig. 1: UDP & TCP query model.

To determine the number of packets transmitted and received over a network link using UDP (transport layer) and IP (network layer), we take into account that each IP-level exchange involves two packets, one for the request and one for the response, excluding any retransmissions that may occur due to packet loss. Therefore, the total number of packets (N) transmitted over UDP can be expressed as:

$$N = 2\epsilon(WithCache)$$

If there is no cache, the DNS query has to pass through the DNS root, the Top Level Domain (TLD) and the Second Level Domain (SLD) to get a response. Hence, for resolving a domain name without cache: $N = 8\epsilon$ *(Without Cache)* $[N = 2\epsilon + 3 * 2\epsilon]$

Estimating the number of packets - TCP

The number of packets exchanged on the network for a DNS query over TCP (*figure 1b*) can be estimated using the following formula:

$$N = (3 + 4 + 2 + 2)\varepsilon = 11\varepsilon \textit{(With Cache)}$$

where:

- $\varepsilon = 1 + \alpha$ is the *retransmission coefficient*, with $\alpha \geq 0$ representing potential network perturbations or packet loss. When $\alpha = 0$, we assume ideal conditions ($\varepsilon = 1$).
- The constant 3 corresponds to the TCP 3-way handshake: `SYN`, `SYN+ACK`, and `ACK`.
- The constant 4 accounts for the TCP connection termination: `FIN`, `ACK`, `FIN`, and `ACK`.
- The factors of 2 indicate that TCP acknowledgments are not piggybacked and require separate packets.

TABLE I: Estimated packet count for DNS resolution under certain assumptions

	DNS UDP	DNS TCP	DoT		DoH	
With Cache	2	11	21	4*	25	4*
Without Cache	8	17	27	10*	31	10*
DNSSEC†	18	27	37	20*	41	20*

We extended the mathematical model to account for encrypted DNS traffic, such as DoT and DoH, both with and without caching. The corresponding values for various DNS scenarios are presented in the **Table I**. Values marked with an asterisk (*) indicate TCP connection reuse, which reduces handshake overhead for multiple queries.

IV. Methodology and Experimental Setup

We use the model to estimate packet behaviour and must validate it against real-world measurements to refine our assumptions. DNS energy consumption should be measured at four key points: the authoritative server (root, TLD, SLD), the resolver, the client device, and the network. This article **focuses specifically on energy consumption at the resolver level**.

The measurement setup has three machines: a resolver, a DNS client, and a third machine (*Port mirroring is enabled on the switch to observe traffic traversing the resolver*) that stores the measurement logs. These machines are dedicated to our experiment and do not run any other service.

We employ three complementary tools that capture both system-wide and process-specific metrics to measure power consumption. Yocto-Watt [18] is a high-precision hardware wattmeter installed between the resolver's power plug and the electrical outlet, offering accurate total power measurements with a precision of 0.02 W. Scaphandre [19] is used to isolate energy consumption at the process level, allowing us to track the power usage of services like Bind9 specifically. Ecofloc [20] is a software-based tool that monitors resource usage such as CPU, RAM, and other system components on a per-process basis.

Since individual DNS requests are lightweight, their energy impact is difficult to isolate in measurements. To address this, we vary the query rate and analyze power consumption as a function of it. Therefore, all results are presented relative to the query rate.

We compare power consumption across DNS (UDP), DoT (TLS), and DoH (HTTPS). For DoH, we use DNSdist, and for DoT, we employ Stunnel as a proxy since Bind9 lacks native DoT, DoH support.

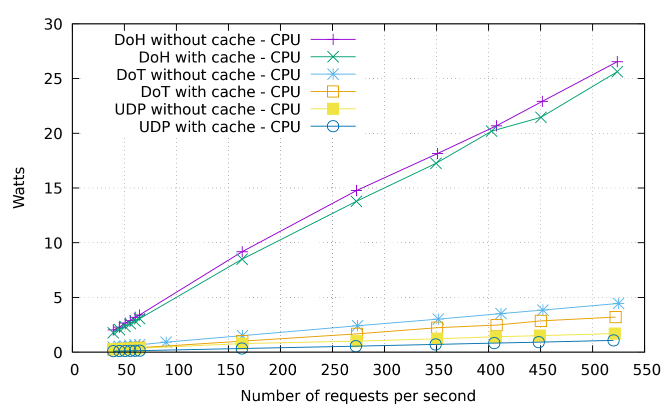


Fig. 2: DNS consumption of CPU

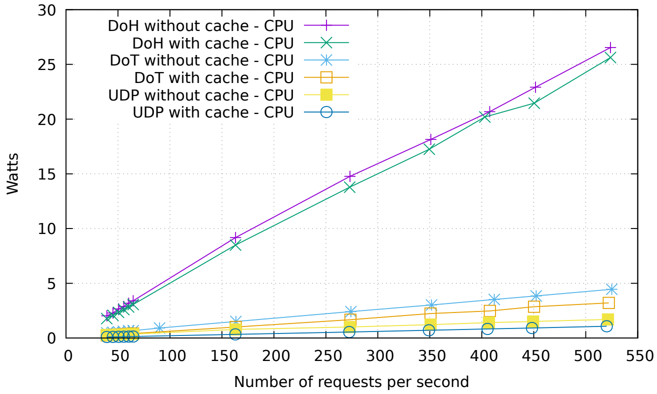


Fig. 3: DNS consumption of RAM

We aim to measure the resolver's power consumption for various request rates (n) ranging from 50 to 600 queries per second (specifically 50, 100, 200, 400, and 500 qps). Each measurement is performed with and without the cache category.

Without Cache: Using a database of the most searched domain names (Alexa Rank by category, 2020, containing 360,000 entries), the ***DNS Client machine*** begins at a random point and sequentially queries domain names, adhering to the specified rate. For each rate, three iterations are executed. We introduce a pause between each iteration to allow the resolver to return to an idle or "no-load" state. To simplify the process, we measure only the resolver's total power consumption per rate over 30 minutes. The aim is to detect any noticeable increase in power consumption rather than obtain fine-grained per-request measurements.

With Cache: This measurement mirrors the no-cache scenario, with the sole difference being that all queries consistently target the same domain: *'afnic.fr'*. This setup is designed to evaluate the impact of DNS caching on energy consumption.

Figure 2 & 3 presents CPU and RAM power consumption as a function of DNS query rate for three protocols: DNS over UDP, DoT, and DoH. As expected, CPU usage is highest for DoH, consuming approximately six times more power than DoT, which consumes approximately three times more than traditional DNS over UDP. This highlights a disparity that is not fully explained by the analytical model introduced in **section III**. For example, while the model estimates a packet ratio of approximately 4:1 between DoH and UDP ($31/8 \approx 4$ packets), this does not account for the observed sixteen-fold increase in CPU consumption. The CPU remains the primary contributor to energy usage among all system components, whereas RAM consumption is negligible. Notably, DNS caching has only a marginal effect on power consumption, with a difference of roughly 1 watt between cached and noncached scenarios.

Figure 4 shows the total power consumption of the server, measured by the wattmeter (Yocto-Watt), as a function of the DNS query rate per second. This measurement accounts for the entire machine, including all hardware components (such as RAM, CPU, Network card etc.). A key observation is the presence of a baseline consumption of approximately 20 Watts, regardless of the protocol used. This idle power reflects the minimum energy required to keep the system running, i.e., covering components such as the graphics card, basic OS operations, and background processes. These results are consistent with the CPU and RAM measurements obtained via Ecofloc. For DoH, the CPU and RAM consumption sum, when added to this baseline, closely matches the total consumption observed with Yocto-Watt. A similar coherence is seen with UDP. However, in the case of DoT, the correlation is less clear, indicating that further investigation is needed to fully account for the observed power profile.

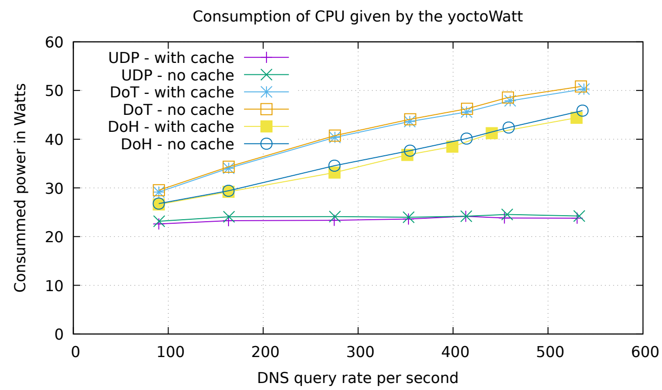


Fig. 4: Comparison of the DNS consumption given by the yoctoWatt in function of the received query rate, for UDP, DoH and DoT, with and without ca che

V. Conclusion & Future evolution

While DNS represents only a small fraction of overall Internet traffic, its global energy impact is far from negligible. This ongoing work introduces a methodology to analyse DNS power consumption at the resolver level, combining a mathematical model with experimental measurements across different DNS protocols, including UDP, DoT, and DoH. Our initial findings confirm that security-enhanced protocols significantly increase energy usage. The model aligns well with measurement results in certain scenarios; however, discrepancies were observed, for example, with DoT, likely due to implementation-specific factors.

To improve accuracy, we plan to refine the model by incorporating packet sizes. This enhancement is especially relevant for encrypted protocols like DoT and DoH, where the TLS 1.3 handshake requires the server to transmit its certificate chain. These chains typically consist of X.509 certificates, whose sizes vary based on the cryptographic algorithm, averaging around 1500 bytes for RSA and approximately 800 bytes for ECDSA. The current model provides a simplified view of the number of packets and does not yet account for the packet size, which we aim to integrate in future iterations.

REFERENCES

[1] International Energy Agency. Electricity 2024, Analysis and forecast to 2026. [Online]. Available: https://iea.blob.core.windows.net/assets/18f3ed24-4b26-4c83-a3d2-8a1be51c8cc8/Electricity2024-Analysisandforecastto2026.pdf

[2] D. Al Kez, A. Foley, F. Ahmed, M. O'Malley, and S. Muyeen, "Potential of data centers for fast frequency response services in synchronously isolated power systems," *Renewable and Sustainable Energy Reviews*, vol. 151, no. 111547, p. 111547, Nov. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S136403212100825X#bib21

[3] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, and P. E. Hoffman, "Specification for DNS over Transport Layer Security (TLS)," RFC 7858, May 2016. [Online]. Available: https://www.rfc-editor.org/info/rfc7858

[4] P. E. Hoffman and P. McManus, "DNS Queries over HTTPS (DoH)," RFC 8484, Oct. 2018. [Online]. Available: https://www.rfc-editor.org/info/rfc8484

[5] ASia Pacific Network Information Center. Encrypted DNS Use by Country - Asia Pacific Network Information Center Stats. [Online]. Available: https://stats.labs.apnic.net/edns

[6] Sustainable Web Design. Estimating Digital Emissions What is the Sustainable Web Design Model? [Online]. Available: https://sustainablewebdesign.org/estimating-digital-emissions/

[7] M. Lin, A. Wierman, L. Andrew, and E. Thereska, "Dynamic right-sizing for power-proportional data centers," *IEEE/ACM Transactions on Networking*, vol. 21, pp. 1098–1106, 04 2011.

[8] M. Lasemi, S. Alizadeh, M. Assili, Z. Yang, P. Baboli, A. Arabkoohsar, A. Raeiszadeh, M. Brand, and S. Lehnhoff, "Energy cost optimization of globally distributed internet data centers by copula-based multidimensional correlation modeling," *Energy Reports*, vol. 9, pp. 631–644, Dec. 2023.

[9] S. El-Zahr, P. Gunning, and N. Zilberman, "Exploring the benefits of carbon-aware routing," *PACMNET*, vol. 1, no. CoNEXT3, pp. 20:1–20:24, 2023. [Online]. Available: https://doi.org/10.1145/3629165

[10] Domain Lions. The Environmental Impact of Domain Name Servers: Sustainable Solutions. [Online]. Available: https://domainlions.com/blog/the-environmental-impact-of-domain-name-servers-sustainable-solutions

[11] E. Casalicchio, M. Caselli, A. Coletta, and I. N. Fovino, "DNS as critical infrastructure, the energy system case study," *Int. J. Crit. Infrastructures*, vol. 9, no. 1/2, pp. 111–129, 2013. [Online]. Available: https://doi.org/10.1504/IJCIS.2013.051605

[12] Z. Wang and S. Rose, "Energy-aware DNS server allocating," *Sustain. Comput. Informatics Syst.*, vol. 19, pp. 253–261, 2018. [Online]. Available: https://doi.org/10.1016/j.suscom.2018.07.002

[13] A. Hankel, R. van den Hoed, E. Hoekstra, and R. van Rijswijk, "Measuring software energy efficiency: Presenting a methodology and case study on dns resolvers," in *2016 18th Mediterranean Electrotechnical Conference (MELECON)*, 2016, pp. 1–6.

[14] Internet Society. Encrypted DNS Factsheet What is DNS, and Why is it Critical? [Online]. Available: https://www.internetsociety.org/resources/doc/2023/fact-sheet-encrypted-dns/

[15] Akshay Narayan and Michael Chen and Vern Paxson. Measuring The Energy Impact of Security Protocols. [Online]. Available: https://akshayn.xyz/res/energy-impact-of-security-protocols-cs261.pdf

[16] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "Analyzing the energy consumption of security protocols," in *Proceedings of the 2003 International Symposium on Low Power Electronics and Design, 2003, Seoul, Korea, August 25-27, 2003*, I. Verbauwhede and H. Roh, Eds. ACM, 2003, pp. 30–35. [Online]. Available: https://doi.org/10.1145/871506.871518

[17] Wes Hardraker, Geoff Houston, João Damas. DNS Deep Dive. [Online]. Available: https://labs.apnic.net/presentations/store/2020-07-23-108-tdd-sessb-dns-deep-dive.pdf

[18] Yoctopuce, "Yocto-watt," https://www.yoctopuce.com/FR/products/capteurs-electriques-usb/yocto-watt, last access march 2025.

[19] Scaphandre, "Scaphandre," https://hubblo-org.github.io/scaphandre-documentation/, last access April 2025.

[20] H. H. A. Valera, "Ecofloc: Energy measuring system tool for linux," https://github.com/hhumbertoAv/ecofloc, 2022.