SANOG 41

innog7
Indian Network Operators Group

April 2024

Performance Analysis of DoT, DoH, and DoQ across Internet-Connected Resolvers

By,
Moulya D M
Teesta Koch
Dr. Saumya Hegde
Department of Computer Science and Engineering,
NITK, Surathkal

Agenda

1. Domain name system (DNS)
2. Encrypted DNS protocols
3. Performance analysis of the encrypted DNS protocols
4. Experimental setup 1
5. Experimental setup 2
6. Results and key takeaways - Setup 1
7. Results and key takeaways - Setup 2
8. Downside of privacy
9. Future scope

Domain Name System (DNS)

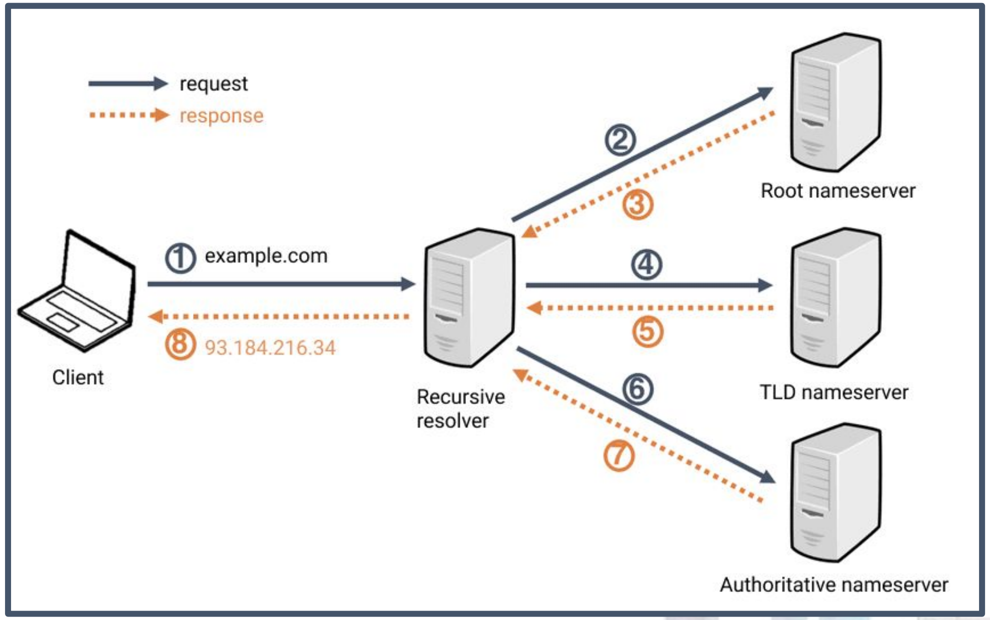


Fig: DNS Resolution [1]

DNS translates human readable domain names (for example, www.amazon.com) to machine readable IP addresses (for example, 192.168.0.1).

What are the drawbacks of traditional DNS?

- **Interception of messages**: DNS queries are sent in plain text, making them vulnerable to eavesdropping.
- **Redirection to fake websites**: Malicious actors can intercept DNS requests and redirect them to fake websites designed to steal your data or infect your device with malware.
- **Privacy invasion**: ISPs and other entities can see your browsing history based on your unencrypted DNS queries.

Encrypted DNS Protocols

DNS over TLS (DoT)

- Encrypts DNS queries using the secure Transport Layer Security (TLS) protocol on a dedicated port (TCP port 853).
- In TLS, the server authenticates itself to the client using a certificate. This ensures that no other party can impersonate the server.

DNS over HTTPS (DoH)

- Encrypts and embeds DNS queries in an HTTPS messages on a dedicated port (TCP port 443).
- DNS queries and responses are camouflaged along with normal HTTPS traffic, since it all comes and goes from the same port.

DNS over Quic (DoQ)

- Encrypts DNS queries using the QUIC protocol over the dedicated ports
- QUIC takes TCP, TLS and the stream capability of HTTP/2 and merge them into a natively encrypted protocol implemented on top of UDP.

Performance analysis of the encrypted DNS protocols

- What is the need for performance analysis ?
  - To identify the bottlenecks in encrypted DNS protocols and propose further optimizations.
  - To select the most suitable protocol for our network environment.
- What are the Metrics measured ? Handshake time, Response time and Total time taken to resolve a query.

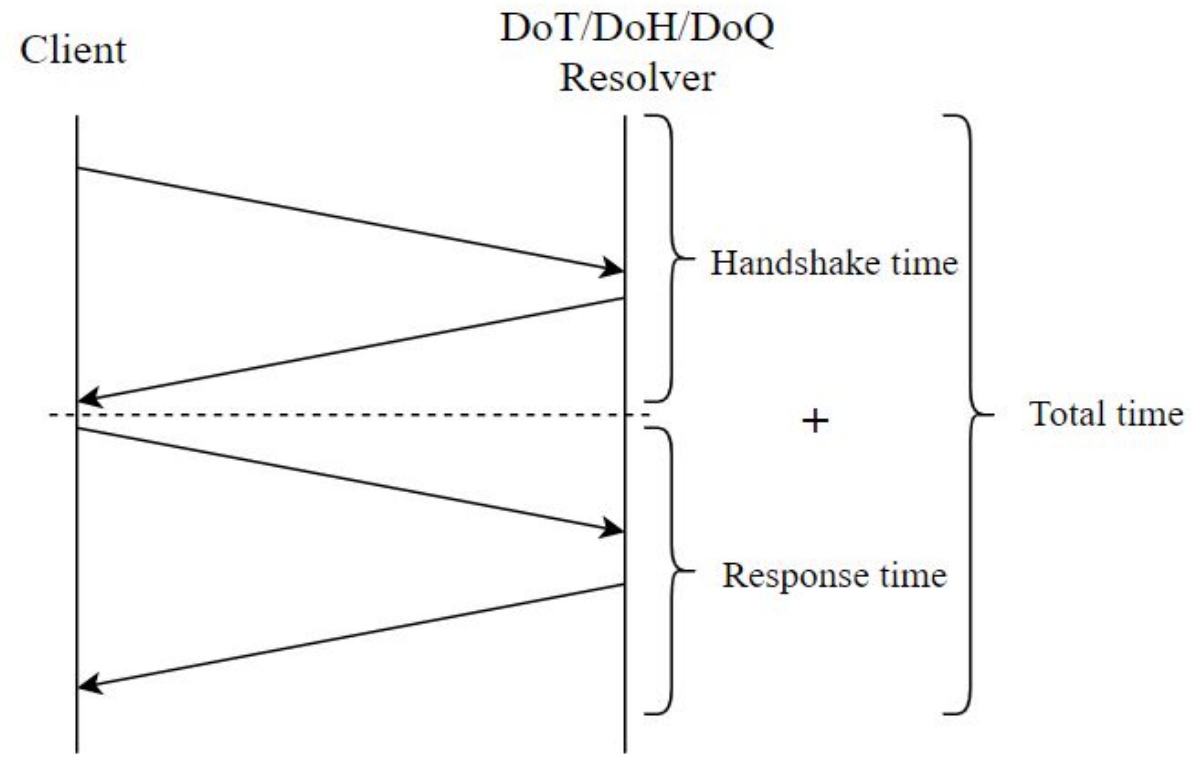


Fig: Metrics considered in the analysis

Performance analysis of the encrypted DNS protocols

- Why did we choose these metrics ?
  - **Handshake time** measures the time required to establish a connection between the client and server.
  - Handshake time introduces additional overhead in the communication process.
  - **Response time** measures how quickly a DNS query sent by a client gets the appropriate response.
  - **Total time** measures the time taken for the entire time taken for the entire DNS transaction.
  - Response time and total time are crucial in DNS resolution as they directly impact user experience.

Performance analysis of the encrypted DNS protocols

- To understand the performance of encrypted DNS protocols, two experiments were carried out
  - Local experiment:
    - Local DNS resolver and authoritative DNS server that supports DoT, DoH and DoQ was setup using CoreDNS.
    - Tool q was used in the client side to send queries and total time was used as metrics.
    - Results from local setup showed that DoQ performs better then DoT and DoH.
  - Second experiment (presented here) involved conducting performance analysis over internet connected resolver.

Experimental Setup 1: Measurements from all the resolvers supporting the three protocols over the internet.

- **Discovery phase: Identification of the DoT/DoH/DoQ resolvers**
    - ZMAP [3] was used to scan the entire IPv4 address space to check if the standardized ports are open from a single vantage point.
    - Identification of DoT and DoH resolvers:
        - ZMap's built-in DNS probing packet was used to discover all the DoT/DoH resolvers in the world.
        - IP addresses are checked to see if they are running the particular protocol in their standardized ports by querying for an A record of www.google.com for DoT and DoH.

- Identification of DoQ resolvers:
  - To identify QUIC, a tailored packet containing the Initial QUIC handshake frame and an invalid version number of 0 is sent to the standard ports of QUIC.
  - If the server is enabled with QUIC it sends back the version negotiation packet back.
  - QUIC target list is verified again by Application-Layer Protocol Negotiation (ALPN) identifiers which results in a list of DoQ-capable using verify-DoQ [12].
- 348 resolvers supporting all the three encrypted connections were discovered.

- **Metric collection phase: Handshake time, response time and total time**
  - Regions of identified resolvers were found out using the https://ip-api.com/json/ API.
  - To collect information about Handshake time, response time and total time, DNSPerf [5] tool was used.
  - DNSPerf queries all the target server for an A record for the domain name www.test.com and returns the results in the form of a database.
  - Python scripts were used to visualize the data.

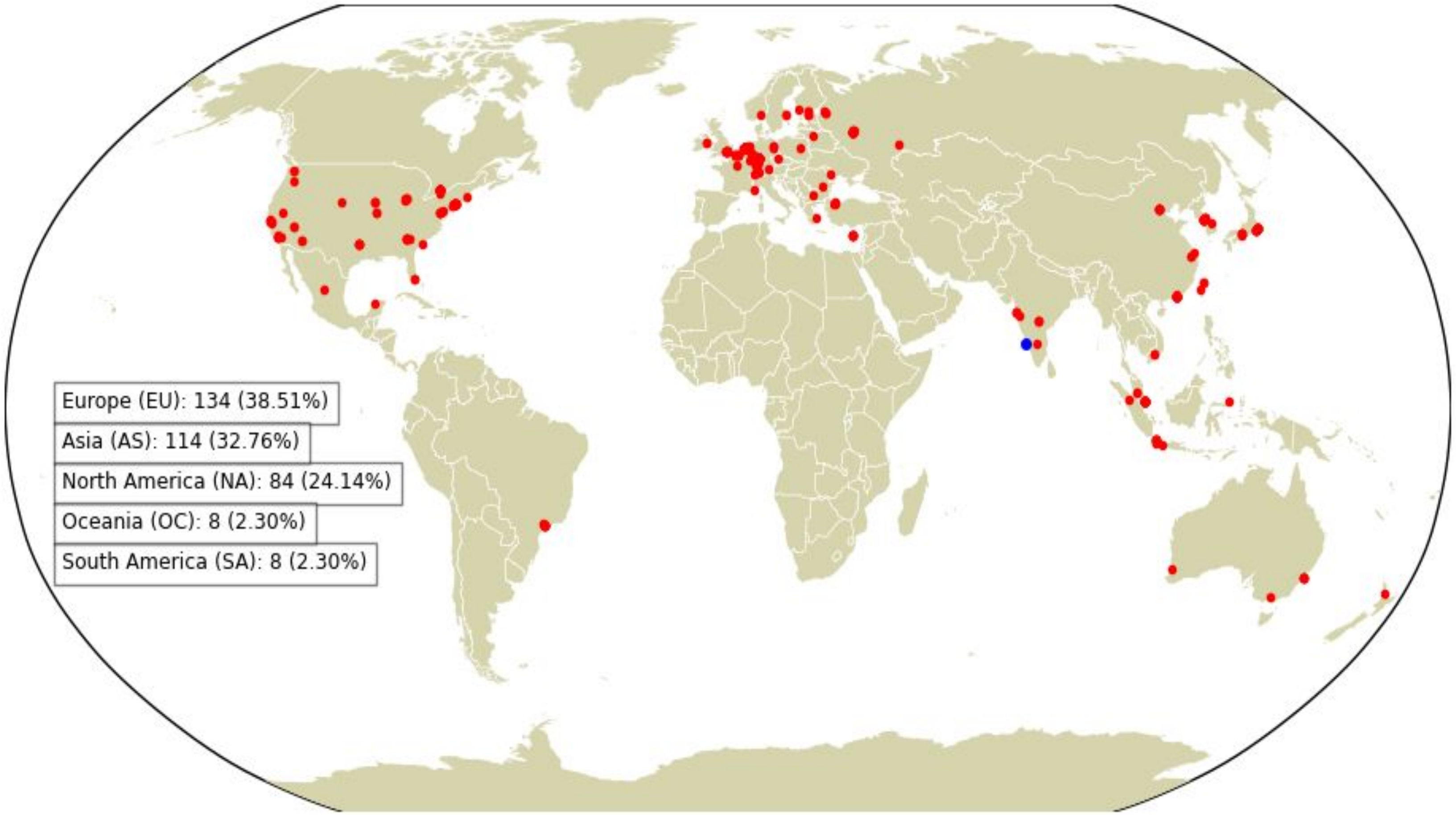


Fig: Distribution of DNS resolvers that support encrypted DNS protocol across the world as of April-12-2023

Experimental Setup 2: Extensive Measurement from the known resolvers

- **Discovery phase:**
  - Resolvers considered: Adguard, Privacy first and NextDNS.
- **Information gathering phase:**
  - Tools used: q [7] and godnsbench [6].
  - Resolvers were hit by different loads of DNS queries and total time taken to resolve the queries were recorded.
    - 500 random queries for A record were sent using q.
    - 1000 random queries for A record were sent using godnsbench in 10 parallel connection.
  - It was repeated for 5 times and average total time was considered.

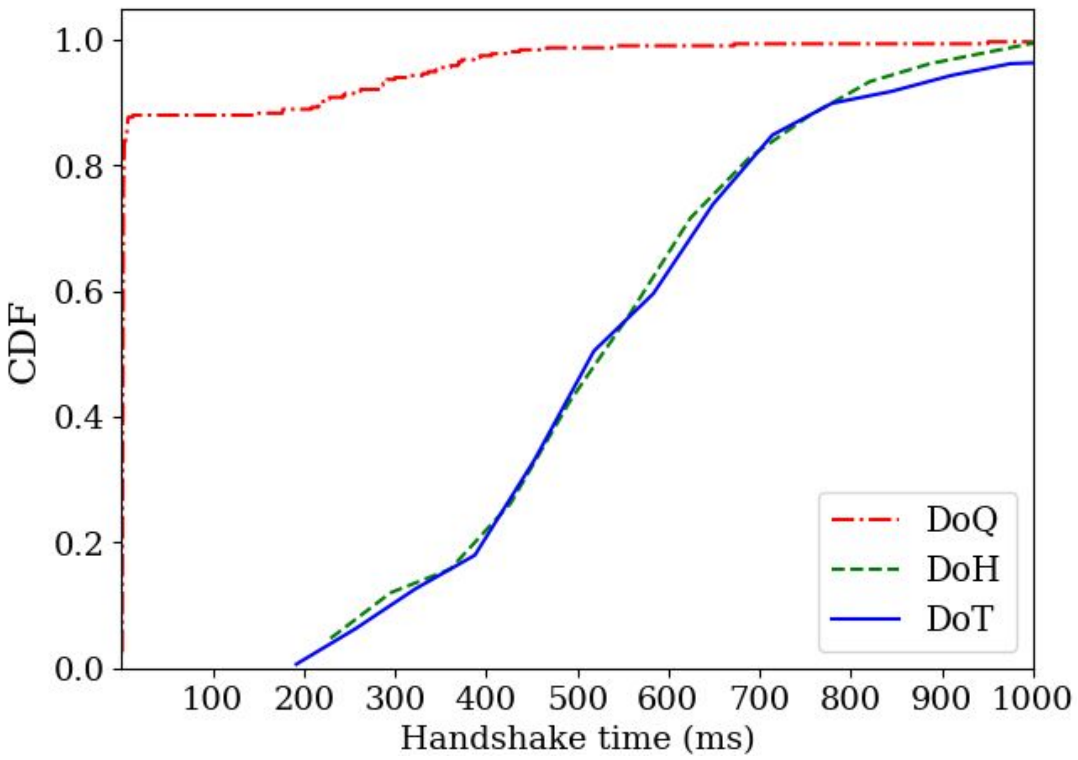
Note: No cached responses were considered in both the experiments.

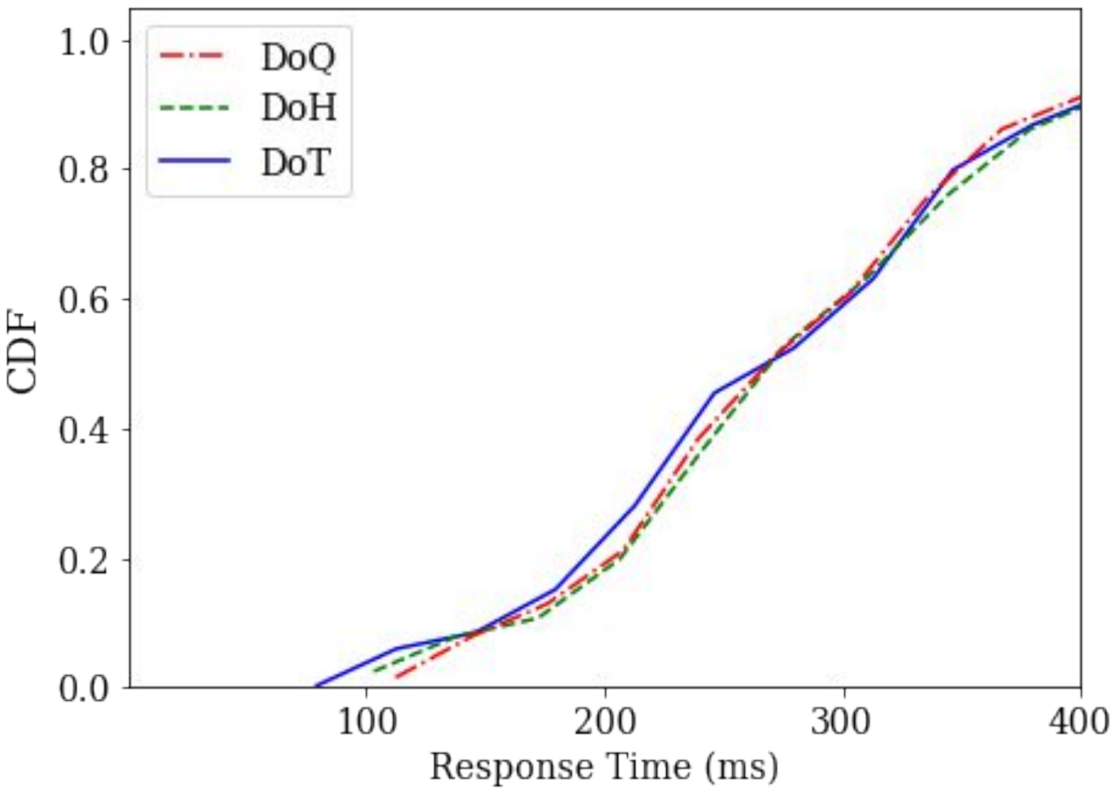
Table 1: Summary of tools used

Tools	Why was it used?
ZMAP	To scan the entire IPv4 address space for all the three protocols.
DNSPerf	Record the Handshake time and Total time by sending queries.
godnsbench	To send the desired load of queries to different resolvers parallely.
q	To send the desired load of queries to different resolvers sequentially.

Results and key takeaways - Setup 1

- Results are plotted using CDF (Cumulative Distribution Function) graph.
- Y axis represent CDF and X axis represents time (ms).

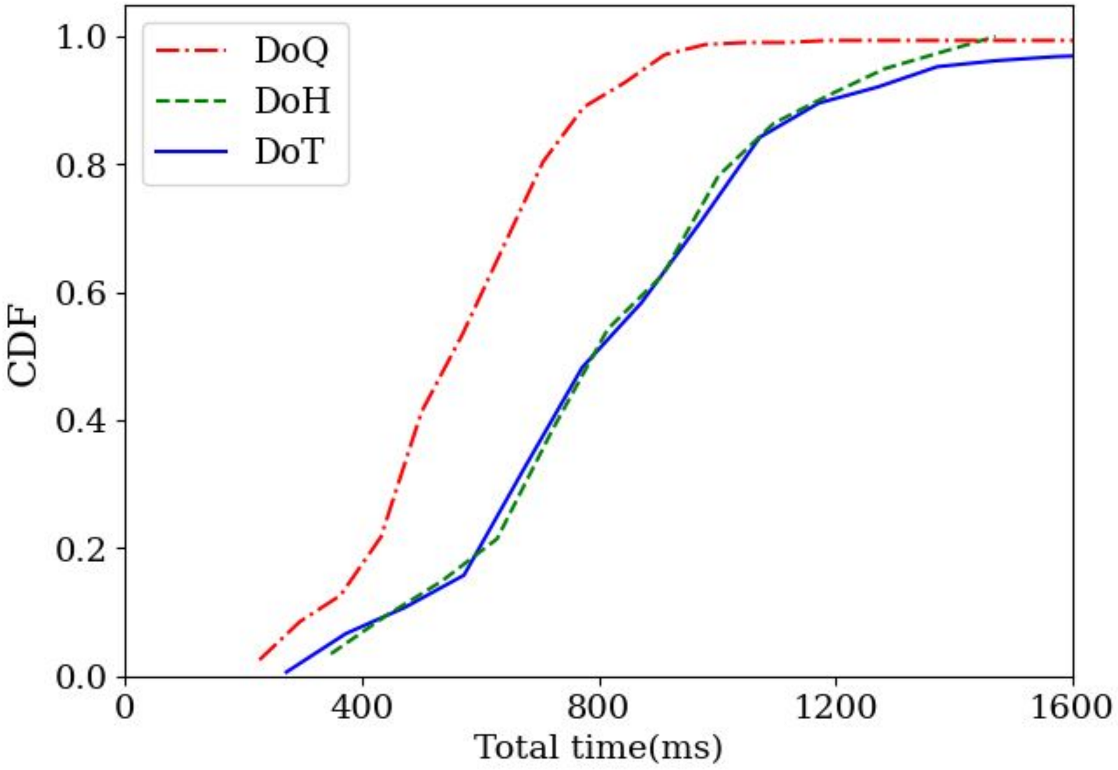




- DoT and DoH have similar handshake time.
- More than 80% of DoQ handshake are negligible value, which shows.0-RTT support from DoQ resolvers.

- Similar response time is observed in all three protocols.
- DoQ response times are slightly faster than DoT and DoH.

Results and key takeaways - Setup 1



- DoQ has the lowest total resolution times.
- Lesser Handshake time contributes in faster query resolution.

Results and takeaways - Setup 2

- Results are plotted using Bar chart.
- Y axis represents Total time (ms) and X axis represents DNS providers

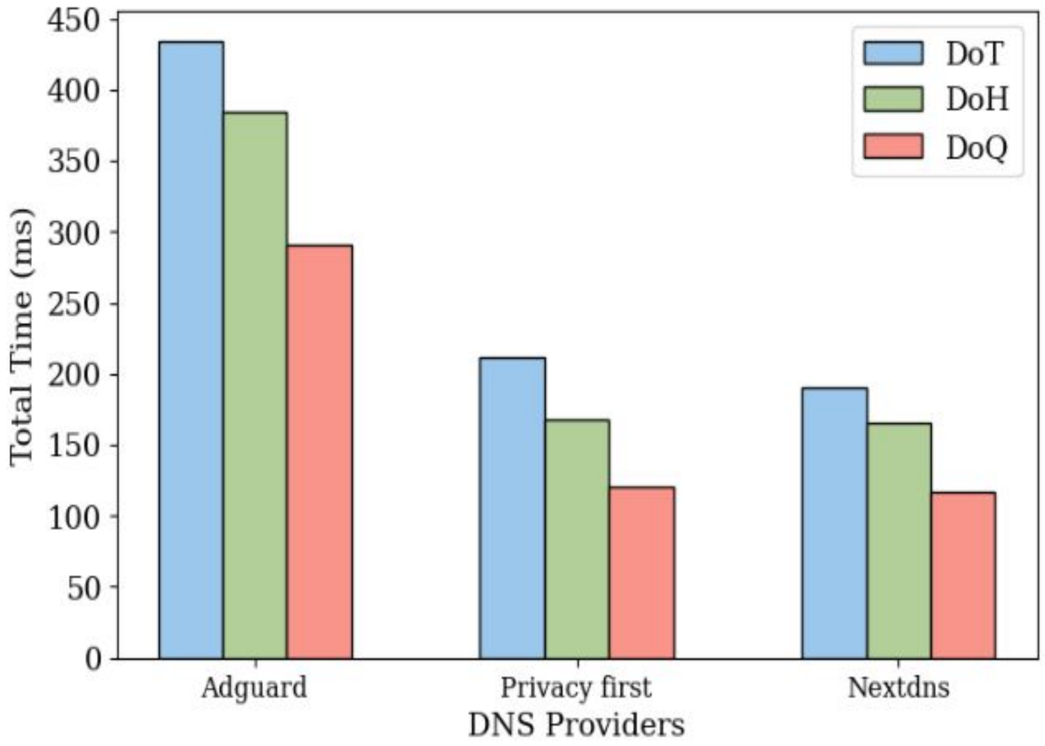


Fig: Total time using q tool

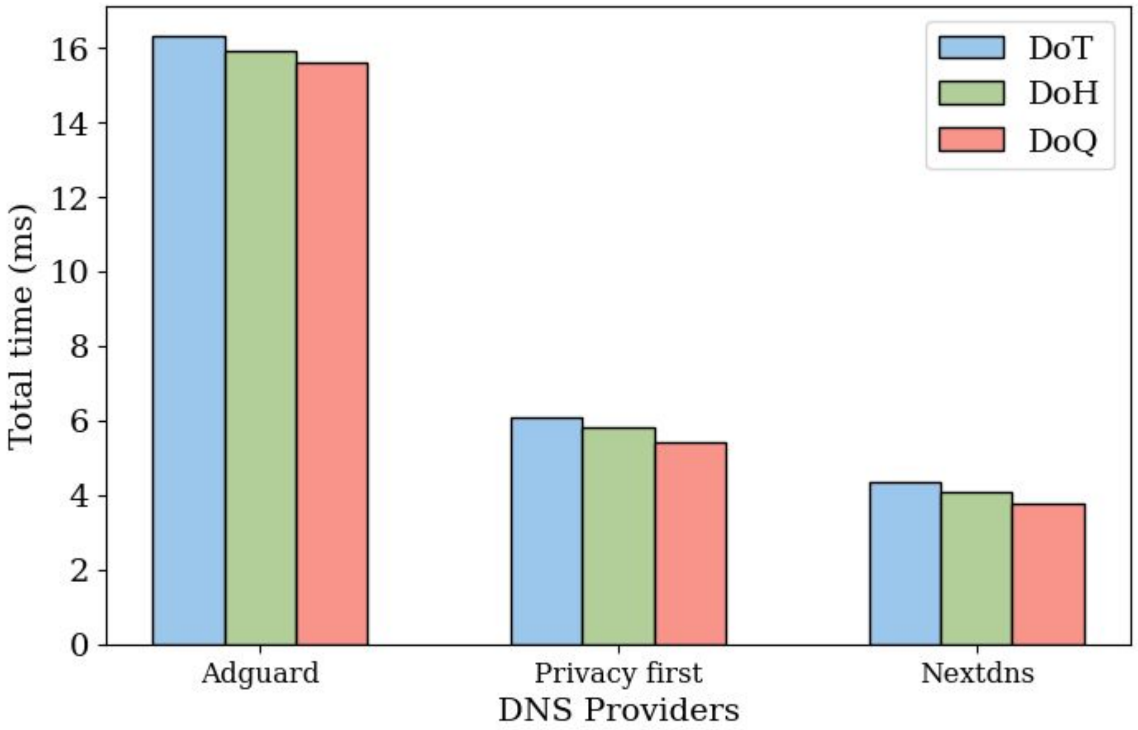


Fig: Total time using godnsbench tool

- DoQ resolves the query is lesser time compared to DoT and DoH.
- Nextdns resolver resolves the query faster than Adguard and Privacy First DNS.

Increase in the adoption of DNS resolvers configured with encrypted connection

Table 2: Number of DoT, DoH and DoQ resolvers discovered as of April-12-2023

Number of DoT resolvers	Number of DoH resolvers	Number of DoQ resolvers
1,796	1,796	1,726

- ≈2.86% increase in DoT resolver from the previous study [5]
- ≈92.91% increase in DoH resolver from the previous study [13]
- ≈41.82% increase in DoQ resolver from the previous study [14]

Can Privacy of Encrypted Protocols be misused?

- Traditional firewalls primarily focus on inspecting data packets at lower levels of the network model.
- This means they analyze elements like IP addresses and port numbers, making them ineffective in directly checking the content of encrypted protocols.
- With encrypted protocols like **DoT, DoH, and DoQ**, the content is hidden, making it difficult to identify malicious requests.

Recent attacks on Encrypted protocols

- New Godlua Backdoor malware Found Abusing DNS Over HTTPS (DoH) Protocol [9].
- ChamelDoH linux Backdoor Utilizing DNS-over-HTTPS Tunneling for Covert CnC [10].

Next step

- DoQ offers good query resolution time and significant security benefits by protecting user privacy.
- However, their encryption also presents challenges for traditional firewalls that rely on inspecting content for threat detection.
- Future Work involves simulating an attacker environment like Godlua for **DNS-over-QUIC (DoQ)** and using machine learning (ML) to differentiate between legitimate and malicious traffic.

References

1. https://www.researchgate.net/figure/Domain-resolution-process-with-a-recursive-resolver_fig1_330006223
2. https://developers.cloudflare.com/1.1.1.1/encryption/dns-over-https/
3. https://zmap.io/zmap,
4. https://github.com/DNS-OARC/dnsperf
5. https://github.com/mgranderath/dnsperf
6. https://github.com/ameshkov/godnsbench
7. https://github.com/natesales/q
8. https://blog.apnic.net/2021/09/13/the-prevalence-of-dns-over-https/
9. https://datatracker.ietf.org/meeting/113/materials/slides-113-maprg-one-to-rule-them-all-a-first-look-at-dns-over-quic

MUMBAI
- INDIA -

References

10.https://thehackernews.com/2023/06/chameldoh-new-linux-backdoor-utilizing.html

11.https://www.bleepingcomputer.com/news/security/new-godlua-malware-evades-traffic-monitoring-via-dns-over-https/

12. https://github.com/mgranderath/verify-doq

13. https://blog.apnic.net/2022/03/29/a-first-look-at-dns-over-quic/

14. https://blog.apnic.net/2021/09/13/the-prevalence-of-dns-over-https/

15. https://casey.byu.edu/papers/2019_conext_dns_privacy.pdf

Thank you !!