Measuring DNS over TLS from the Edge: Adoption, Reliability, and Response Times

Trinh Viet Doan, Irina Tsareva, Vaibhav Bajpai

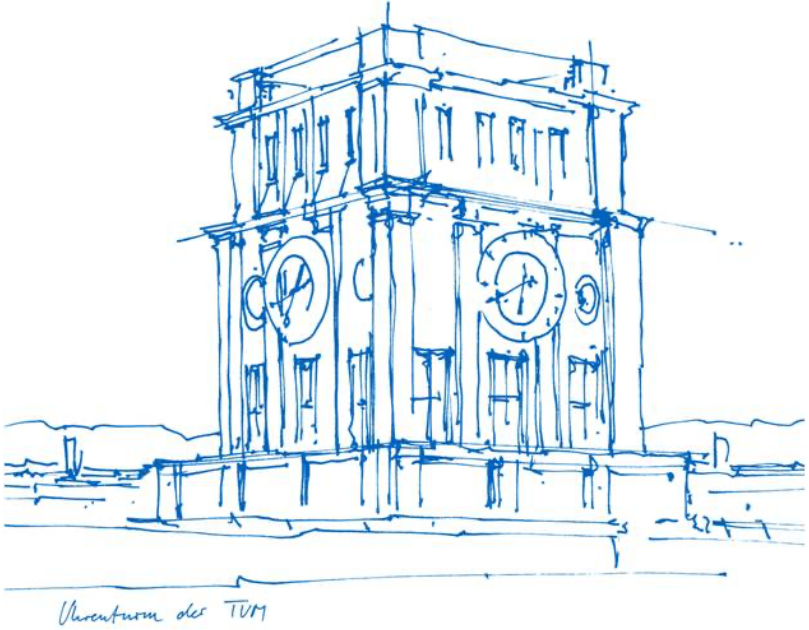
Technical University of Munich

Paper to appear in PAM 2021

IETF 110 | MAPRG | 2021-03-08

Measurement IDs & analysis scripts online:

https://github.com/tv-doan/pam-2021-ripe-atlas-dot



Findings

Adoption of DNS over TLS (DoT)

- Still quite low among resolvers (< 1%) but has been increasing

Reliability

- DoT failure rates inflated compared to DNS over UDP/53 (Do53)
- Likely due to middlebox interception

Response Times

- Higher by >100 ms when using DoT compared to Do53

DNS over TLS (DoT): Motivation

Standardized in May 2016 (RFC 7858)

TCP connection + TLS session on port `853` to secure DNS traffic

Previous DoT measurement studies on different aspects
(e.g., support, reachability, response times) from

- University network [1],
- Data centers [2],
- Proxy networks [3]

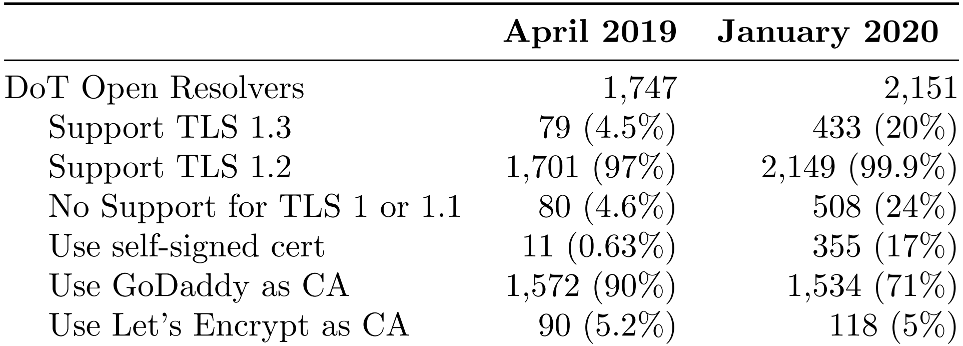
→ DoT measurements from home networks?

Methodology

Part I – Adoption

- Scanning IPv4 address space for open DNS resolvers (UDP/53)
- Checking DoT support (0.15%) for the 1.2M found IP endpoints in April 2019 [1]

→ Repeated from university network in January 2020 (0.18%)



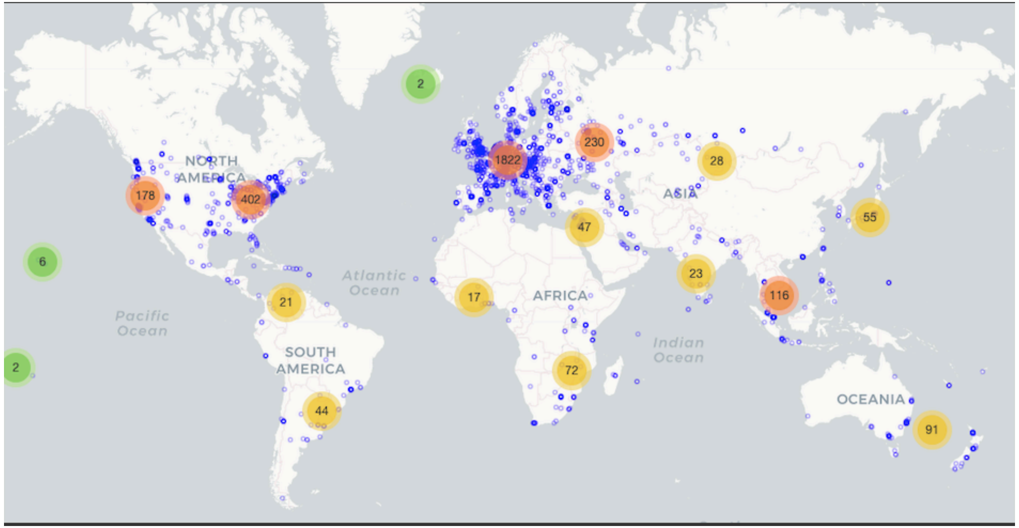
	April 2019	January 2020	
DoT Open Resolvers	1,747	2,151	+ 23.1%
Support TLS 1.3	79 (4.5%)	433 (20%)	+ 448%
Support TLS 1.2	1,701 (97%)	2,149 (99.9%)	+ 26.3%
No Support for TLS 1 or 1.1	80 (4.6%)	508 (24%)	+ 535%
Use self-signed cert	11 (0.63%)	355 (17%)	
Use GoDaddy as CA	1,572 (90%)	1,534 (71%)	
Use Let's Encrypt as CA	90 (5.2%)	118 (5%)	

→ Increasing support for DoT and newer TLS versions

Methodology

Part II – Reliability and Response Times

- RIPE Atlas
  - DoT measurements available since 2018
  - DNS requests from 3.2k home probes (IPv4-capable + V3)



Methodology

Part II – Reliability and Response Times

- RIPE Atlas
  - DoT measurements available since 2018
  - DNS requests from 3.2k home probes (IPv4-capable + V3)

- DNS requests
  - Once a day over one week in July 2019
  - Both DoT + DNS over UDP/53 (Do53)
  - A records over IPv4 for 200 domains
  - 15 public resolvers (5 with DoT support) + local probe resolvers

→ **Around 90M DNS requests/responses in total**

		DoT?
1)	CleanBrowsing	✓
2)	Cloudflare 1.1.1.1	✓
3)	Comodo Secure DNS	-
4)	CZ.NIC ODVR	-
5)	Oracle + Dyn	-
6)	DNS.WATCH	-
7)	Google Public DNS	✓
8)	Neustar UltraRecursive	-
9)	OpenDNS	-
10)	OpenNIC	-
11)	Quad9	✓
12)	SafeDNS	-
13)	UncensoredDNS	✓
14)	VeriSign Public DNS	-
15)	Yandex.DNS	-
16)	*Local resolvers*	?

DoT responses for 13 probes (0.4%)

Reliability

Based on *failure rates*

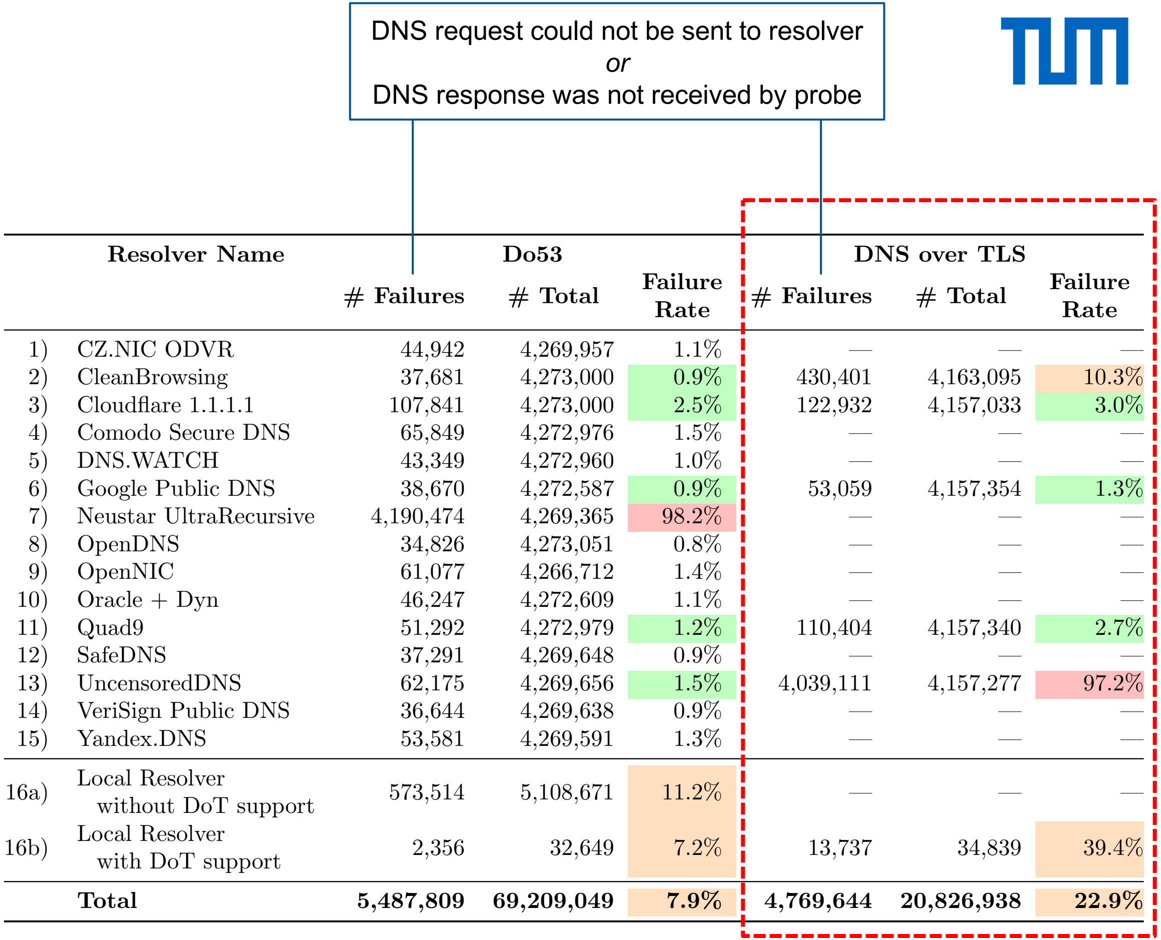
Most common errors:

- Timeouts
- Socket errors
- `connect()` errors
- TCP/TLS errors (DoT exclusive)

Comparing Do53 and DoT

→ **Inflated failure rates for DoT** by 0.4–32.2 percentage points

→ Blackholing of DoT packets due to middlebox ossification (TCP/`853`)?



DNS request could not be sent to resolver
or
DNS response was not received by probe

	Resolver Name	Do53			DNS over TLS		
		# Failures	# Total	Failure Rate	# Failures	# Total	Failure Rate
1)	CZ.NIC ODVR	44,942	4,269,957	1.1%	—	—	—
2)	CleanBrowsing	37,681	4,273,000	0.9%	430,401	4,163,095	10.3%
3)	Cloudflare 1.1.1.1	107,841	4,273,000	2.5%	122,932	4,157,033	3.0%
4)	Comodo Secure DNS	65,849	4,272,976	1.5%	—	—	—
5)	DNS.WATCH	43,349	4,272,960	1.0%	—	—	—
6)	Google Public DNS	38,670	4,272,587	0.9%	53,059	4,157,354	1.3%
7)	Neustar UltraRecursive	4,190,474	4,269,365	98.2%	—	—	—
8)	OpenDNS	34,826	4,273,051	0.8%	—	—	—
9)	OpenNIC	61,077	4,266,712	1.4%	—	—	—
10)	Oracle + Dyn	46,247	4,272,609	1.1%	—	—	—
11)	Quad9	51,292	4,272,979	1.2%	110,404	4,157,340	2.7%
12)	SafeDNS	37,291	4,269,648	0.9%	—	—	—
13)	UncensoredDNS	62,175	4,269,656	1.5%	4,039,111	4,157,277	97.2%
14)	VeriSign Public DNS	36,644	4,269,638	0.9%	—	—	—
15)	Yandex.DNS	53,581	4,269,591	1.3%	—	—	—
16a)	Local Resolver without DoT support	573,514	5,108,671	11.2%	—	—	—
16b)	Local Resolver with DoT support	2,356	32,649	7.2%	13,737	34,839	39.4%
	Total	**5,487,809**	**69,209,049**	**7.9%**	**4,769,644**	**20,826,938**	**22.9%**

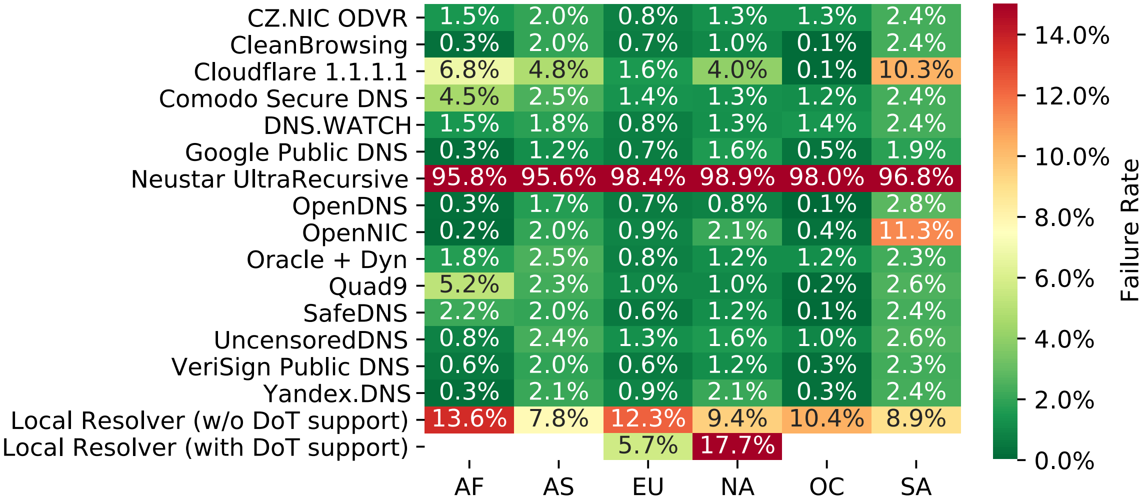
Reliability

Regional split by continent location of probe (ground truth)

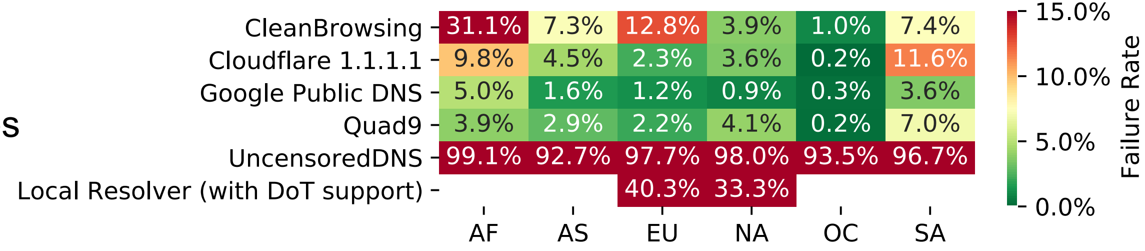
Varying DoT failure rates regarding continents and resolvers; from ≤1% to >10% for most cells

Higher failure rates in AF and SA

DoT failure rates for local resolvers much higher than for most public ones

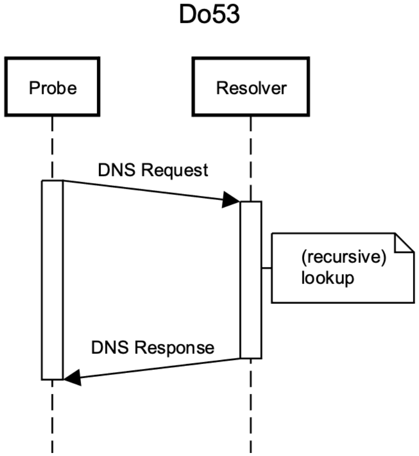


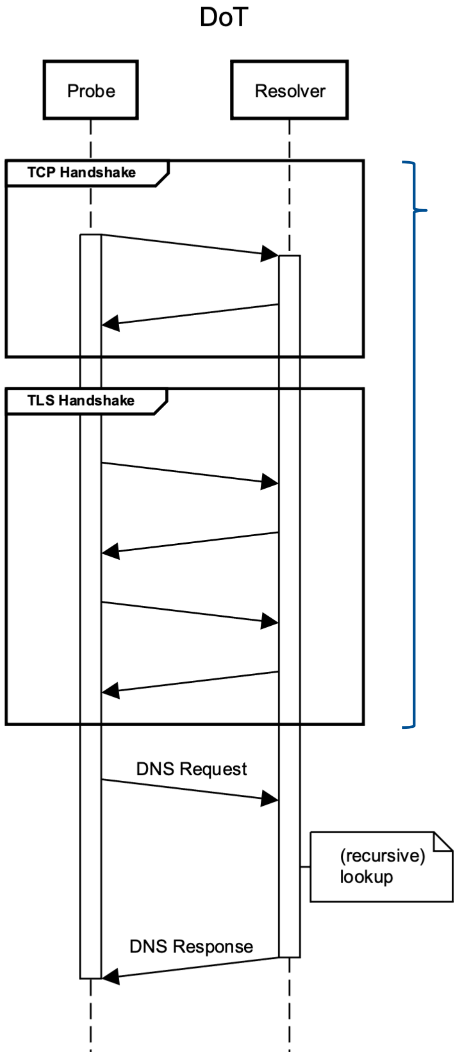
	AF	AS	EU	NA	OC	SA
CZ.NIC ODVR	1.5%	2.0%	0.8%	1.3%	1.3%	2.4%
CleanBrowsing	0.3%	2.0%	0.7%	1.0%	0.1%	2.4%
Cloudflare 1.1.1.1	6.8%	4.8%	1.6%	4.0%	0.1%	10.3%
Comodo Secure DNS	4.5%	2.5%	1.4%	1.3%	1.2%	2.4%
DNS.WATCH	1.5%	1.8%	0.8%	1.3%	1.4%	2.4%
Google Public DNS	0.3%	1.2%	0.7%	1.6%	0.5%	1.9%
Neustar UltraRecursive	95.8%	95.6%	98.4%	98.9%	98.0%	96.8%
OpenDNS	0.3%	1.7%	0.7%	0.8%	0.1%	2.8%
OpenNIC	0.2%	2.0%	0.9%	2.1%	0.4%	11.3%
Oracle + Dyn	1.8%	2.5%	0.8%	1.2%	1.2%	2.3%
Quad9	5.2%	2.3%	1.0%	1.0%	0.2%	2.6%
SafeDNS	2.2%	2.0%	0.6%	1.2%	0.1%	2.4%
UncensoredDNS	0.8%	2.4%	1.3%	1.6%	1.0%	2.6%
VeriSign Public DNS	0.6%	2.0%	0.6%	1.2%	0.3%	2.3%
Yandex.DNS	0.3%	2.1%	0.9%	2.1%	0.3%	2.4%
Local Resolver (w/o DoT support)	13.6%	7.8%	12.3%	9.4%	10.4%	8.9%
Local Resolver (with DoT support)			5.7%	17.7%		



	AF	AS	EU	NA	OC	SA
CleanBrowsing	31.1%	7.3%	12.8%	3.9%	1.0%	7.4%
Cloudflare 1.1.1.1	9.8%	4.5%	2.3%	3.6%	0.2%	11.6%
Google Public DNS	5.0%	1.6%	1.2%	0.9%	0.3%	3.6%
Quad9	3.9%	2.9%	2.2%	4.1%	0.2%	7.0%
UncensoredDNS	99.1%	92.7%	97.7%	98.0%	93.5%	96.7%
Local Resolver (with DoT support)			40.3%	33.3%		

Response Times





Connection and session typically reused for subsequent domain lookups with DoT to minimize overhead

DoT with RIPE Atlas:
Separate connections and sessions for each DoT measurement (i.e., not kept alive in between)

→ **DoT response times measured by probes include full handshakes**

→ Resembling rough upper bounds for DoT lookups

Response Times

5^{th} percentiles of *(probe, resolver)* tuples
to approximate response times of cached records

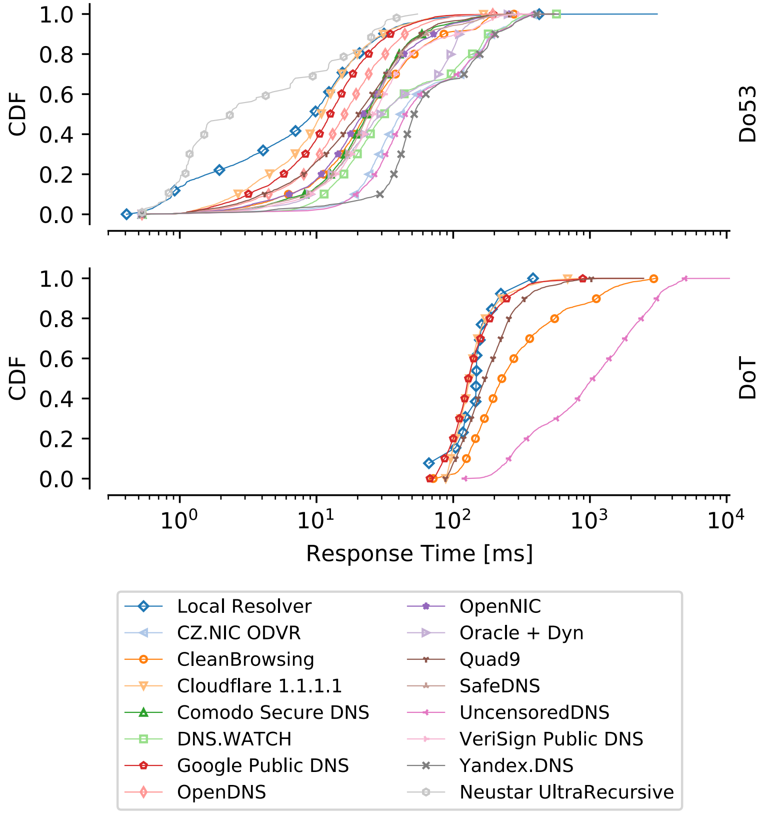
Do53: medians around 10–30 ms for most resolvers

DoT: medians roughly 130–150 ms for faster resolvers

Comparing Do53 and DoT

→ **DoT response times inflated by more than 100 ms compared with Do53**

→ DoT response times for local resolvers (median 147 ms) comparable to faster public resolvers



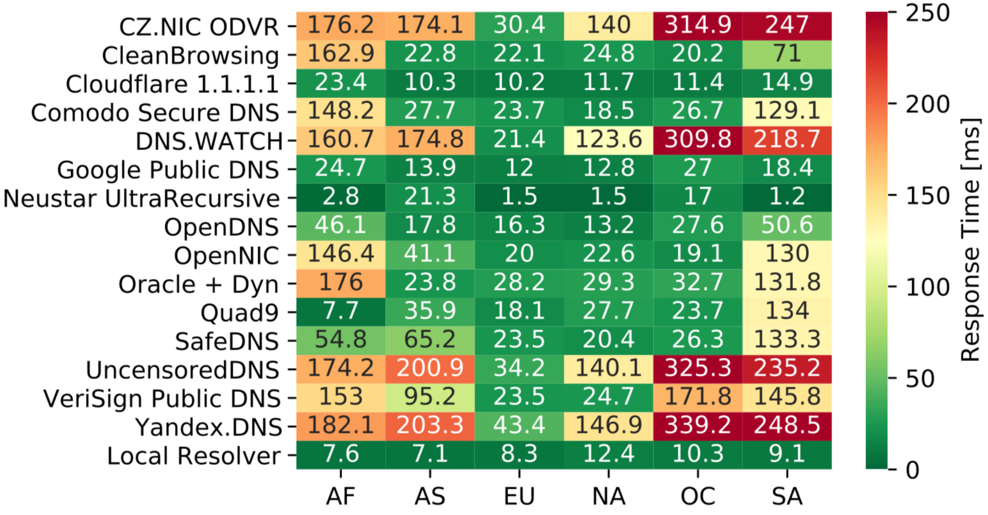
Response Times

Regional split by continent location of probe (ground truth)

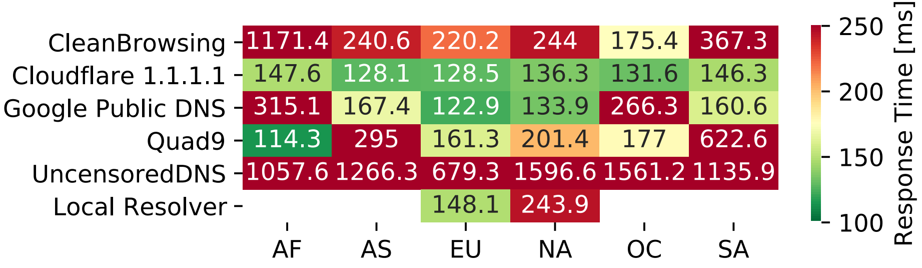
Highly varying response times for DoT regarding continents and resolvers

Higher response times in AF and SA

DoT response times for local resolvers roughly comparable to faster cases of public resolvers for EU probes (slower cases for NA probes)



	AF	AS	EU	NA	OC	SA
CZ.NIC ODVR	176.2	174.1	30.4	140	314.9	247
CleanBrowsing	162.9	22.8	22.1	24.8	20.2	71
Cloudflare 1.1.1.1	23.4	10.3	10.2	11.7	11.4	14.9
Comodo Secure DNS	148.2	27.7	23.7	18.5	26.7	129.1
DNS.WATCH	160.7	174.8	21.4	123.6	309.8	218.7
Google Public DNS	24.7	13.9	12	12.8	27	18.4
Neustar UltraRecursive	2.8	21.3	1.5	1.5	17	1.2
OpenDNS	46.1	17.8	16.3	13.2	27.6	50.6
OpenNIC	146.4	41.1	20	22.6	19.1	130
Oracle + Dyn	176	23.8	28.2	29.3	32.7	131.8
Quad9	7.7	35.9	18.1	27.7	23.7	134
SafeDNS	54.8	65.2	23.5	20.4	26.3	133.3
UncensoredDNS	174.2	200.9	34.2	140.1	325.3	235.2
VeriSign Public DNS	153	95.2	23.5	24.7	171.8	145.8
Yandex.DNS	182.1	203.3	43.4	146.9	339.2	248.5
Local Resolver	7.6	7.1	8.3	12.4	10.3	9.1



	AF	AS	EU	NA	OC	SA
CleanBrowsing	1171.4	240.6	220.2	244	175.4	367.3
Cloudflare 1.1.1.1	147.6	128.1	128.5	136.3	131.6	146.3
Google Public DNS	315.1	167.4	122.9	133.9	266.3	160.6
Quad9	114.3	295	161.3	201.4	177	622.6
UncensoredDNS	1057.6	1266.3	679.3	1596.6	1561.2	1135.9
Local Resolver			148.1	243.9		

Conclusion

DoT Adoption

- Still low among open IPv4 resolvers (0.18%), however, has increased by 23.1% within nine months
- RIPE Atlas: Low adoption among local probe resolvers (0.4%)

Reliability

- DoT failure rates inflated by 0.4–32.2 percentage points compared to Do53
- Likely due to issues along the path (middlebox ossification)

Response Times

- Higher by >100 ms for initial connection/session and lookup when using DoT
- Comparable for local resolvers and public resolvers

Measurement IDs & analysis scripts online:

https://github.com/tv-doan/pam-2021-ripe-atlas-dot

Trinh Viet Doan
doan@in.tum.de

Irina Tsareva
irina.tsareva@tum.de

Vaibhav Bajpai
bajpaiv@in.tum.de

References

[1] Deccio, C.T., Davis, J.: DNS Privacy in Practice and Preparation. In: Conference on Emerging Networking Experiments And Technologies. pp. 138–143 (2019), https://doi.org/10.1145/3359989.3365435

[2] Hounsel, A., Borgolte, K., Schmitt, P., Holland, J., Feamster, N.: Comparing the Effects of DNS, DoT, and DoH on Web Performance. In: The Web Conference. pp. 562–572. ACM / IW3C2 (2020), https://doi.org/10.1145/3366423.3380139

[3] Lu, C., Liu, B., Li, Z., Hao, S., Duan, H., Zhang, M., Leng, C., Liu, Y., Zhang, Z., Wu, J.: An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come? In: Internet Measurement Conference. pp. 22–35. ACM (2019), https://doi.org/10.1145/3355369.3355580