TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

Martine S. Lenders (martine.lenders@tu-dresden.de, miri64)

Evaluation of DNS over CoAP

Frankfurt a. M., RIOT Summit 2023, 2023-09-18

This Talk is Based on Our Paper

Accepted at CoNEXT'23, will be published in PACMNET:

> Martine S. Lenders, Christian Amsüss, Cenk Gündogan, Marcin Nawrocki, Thomas C. Schmidt, Matthias Wählisch. 2023. **Securing Name Resolution in the IoT: DNS over CoAP**, *Proceedings of the ACM on Networking (PACMNET)* 1, CoNEXT2, Article 6 (September 2023), 25 pages. `https://doi.org/10.1145/3609423`
>
> ArXiv pre-print: `https://arxiv.org/abs/2207.07486`

Outline

Motivation

Design Guidance from IoT DNS Traffic

DNS over CoAP

DoC RIOT Integration

Evaluation

Conclusion & Next Steps

Outline

Motivation

Design Guidance from IoT DNS Traffic

DNS over CoAP

DoC RIOT Integration

Evaluation

Conclusion & Next Steps

Motivation

Attack Scenario

Countermeasure: Encrypt name resolution triggered by IoT devices

Possible Solutions

DNS over HTTPS (RFC 8484)

DNS over TLS (RFC 7858)

Possible Solutions

DNS over HTTPS (RFC 8484)

DNS over TLS (RFC 7858)

DNS over QUIC (RFC 9250)

Possible Solutions

DNS over HTTPS (RFC 8484)

DNS over TLS (RFC 7858)

DNS over QUIC (RFC 9250)

DNS over DTLS (RFC 8094)

Possible Solutions

~~DNS over HTT~~
~~(RFC~~

TCP conflicts with
resource constraints

~~ver TLS~~
~~(RFC 7858)~~

DNS over QUIC
(RFC 9250)

DNS over DTLS
(RFC 8094)

Possible Solutions

~~DNS over HT…~~ ~~(R…C…)~~

~~…ver TLS~~ ~~(…FC 785…)~~

~~D…S~~

TCP conflicts with resource constraints

TLS over UDP conflicts with resource constraints

DNS over DTLS (RFC 8094)

Possible Solutions

Possible Solutions

Our proposal: DNS over CoAP

(https://datatracker.ietf.org/doc/draft-ietf-core-dns-over-coap/)

- **Encrypted communication** based on DTLS or OSCORE
- **Block-wise message transfer** to overcome Path MTU problem
- **Share system resources** with CoAP applications
  - Same socket and buffers can be used
  - Re-use of the CoAP retransmission mechanism

Outline

Data Corpus for IoT DNS Traffic Analysis

IoT data sets

YourThings[1] | IoTFinder[2] | MonIoTr[3]

- Collected throughout 2019
- DNS & mDNS (DNS-SD) traffic
- 90 consumer devices from 50 vendors
- 0.2 million queries
- 1.3 million responses
- 2336 unique queried names

IXP data set

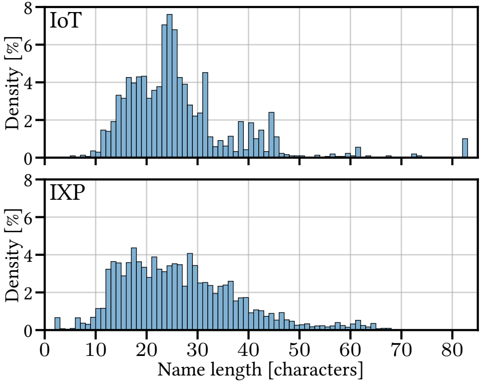
- Large Central European IXP
- Collected January 2022
- DNS only
- Sampling rate: 1/16000 pkts.
- 1.6 million queries
- 2.4 million responses
- Names anonymized to lengths

[1] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose. 2019. **SoK: Security Evaluation of Home-Based IoT Deployments**. In *IEEE S&P 2019*. 1362–1380.

[2] R. Perdisci, T. Papastergiou, O. Alrawi, and M. Antonakakis. 2020. **IoTFinder: Efficient Large-Scale Identification of IoT Devices via Passive DNS Traffic Analysis**. In *IEEE EuroS&P 2020*. 474–489.

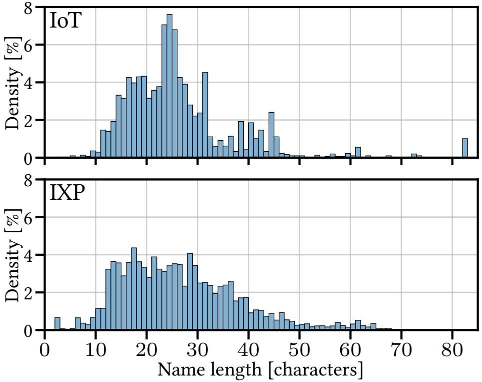
[3] J. Ren, D.J. Dubois, D. Choffnes, A.M. Mandalari, R. Kolcun, and H. Haddadi. 2019. **Information Exposure for Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach**. In *Proc. of the Internet Measurement Conference (IMC)*. ACM.

DNS IoT Traffic: Name Lengths



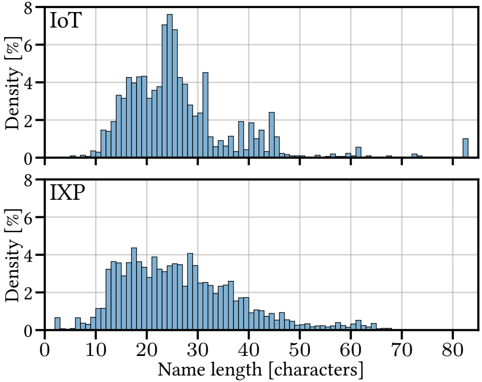
Data set	min	max	mode	μ	σ	Q_1	Q_2	Q_3
	Length of domain names [chars]							
YourThings	2	83	31	24.5	9.7	18	24	30
IoTFinder	7	82	24	26.8	10.5	20	24	30
MonIoTr	9	83	18	27.1	14.7	18	23	30
IoT total	2	83	24	25.9	1.3	19	24	30
IXP	0	68	17	26.1	1.7	17	25	33

DNS IoT Traffic: Name Lengths



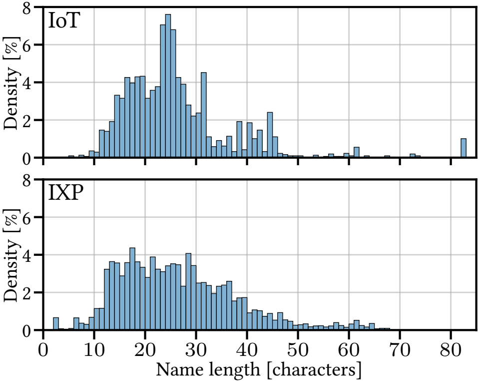
	Length of domain names [chars]							
Data set	min	max	mode	μ	σ	Q_1	Q_2	Q_3
YourThings	2	83	31	24.5	9.7	18	24	30
IoTFinder	7	82	24	26.8	10.5	20	24	30
MonIoTr	9	83	18	27.1	14.7	18	23	30
IoT total	2	83	24	25.9	1.3	19	24	30
IXP	0	68	17	26.1	1.7	17	25	33

DNS IoT Traffic: Name Lengths



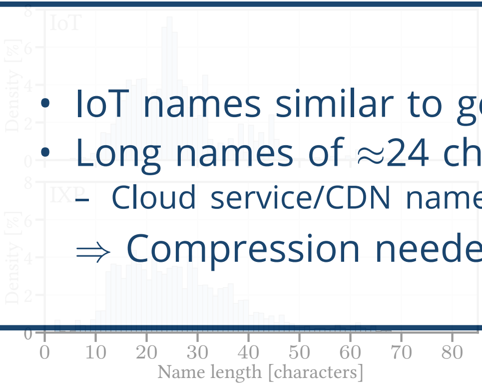
Data set	min	max	mode	μ	σ	Q_1	Q_2	Q_3
	Length of domain names [chars]							
YourThings	2	83	31	24.5	9.7	18	24	30
IoTFinder	7	82	24	26.8	10.5	20	24	30
MonIoTr	9	83	18	27.1	14.7	18	23	30
IoT total	2	83	24	25.9	1.3	19	24	30
				≈	≈	≈	≈	≈
IXP	0	68	17	26.1	1.7	17	25	33

DNS IoT Traffic: Name Lengths



	Length of domain names [chars]							
Data set	min	max	mode	μ	σ	Q_1	Q_2	Q_3
YourThings	2	83	31	24.5	9.7	18	24	30
IoTFinder	7	82	24	26.8	10.5	20	24	30
MonIoTr	9	83	18	27.1	14.7	18	23	30
IoT total	2	83	24	25.9	1.3	19	24	30
IXP	0	68	17	26.1	1.7	17	25	33

DNS IoT Traffic: Name Lengths



- IoT names similar to general Internet names
- Long names of $\approx$24 characters typical
  - Cloud service/CDN names (e.g. `e123.abcd.akamaiedge.net`)

$\Rightarrow$ Compression needed for DoC (via Content-Format)

DNS IoT Traffic: Record Type

Queried	IoT Devices		
Record Type	w/ mDNS	w/o mDNS	IXP
`A`	53.6%	75.8%	64.5%
`AAAA`	16.4%	23.5%	17.6%
`ANY`	8.2%	—	1.7%
`HTTPS`	—	—	9.1%
`NS`	—	—	0.7%
`PTR`	19.6%	0.3%	1.8%
`SRV`	1.0%	—	0.4%
`TXT`	1.2%	0.1%	0.7%
Other	< 0.1%	0.3%	3.5%

DNS IoT Traffic: Record Type

Queried	IoT Devices		
Record Type	w/ mDNS	w/o mDNS	IXP
A	53.6%	75.8%	64.5%
AAAA	16.4%	23.5%	17.6%
ANY	8.2%	—	1.7%
HTTPS	—	—	9.1%
NS	—	—	0.7%
PTR	19.6%	0.3%	1.8%
SRV	1.0%	—	0.4%
TXT	1.2%	0.1%	0.7%
Other	< 0.1%	0.3%	3.5%

Mainly address resolution

DNS IoT Traffic: Record Type

Queried Record Type	IoT Devices w/ mDNS	IoT Devices w/o mDNS	IXP
A	53.6%	75.8%	64.5%
AAAA	16.4%	23.5%	17.6%
ANY	8.2%	—	1.7%
HTTPS	—	—	9.1%
NS	—	—	0.7%
PTR	19.6%	0.3%	1.8%
SRV	1.0%	—	0.4%
TXT	1.2%	0.1%	0.7%
Other	< 0.1%	0.3%	3.5%

Mainly address resolution

Also service discovery & information

DNS IoT Traffic: Record Type

Mainly address resolution

Also service discovery & information

- Name resolution should be favored by DoC
- Group OSCORE may offer solution for encrypted DNS-SD
- Unsolicited `NS` records increase response size
  $\Rightarrow$ Should be avoided with DoC

Outline

DNS over CoAP (DoC)

- Just map the DoH methods **GET** and **POST**?

DNS over CoAP (DoC)

- Just map the DoH methods **GET** and **POST**?

	HTTP	
	GET	POST
Cacheable	✓	✗
Application data carried in body	✗	✓
Block-wise transferable query	✗	✓

DNS over CoAP (DoC)

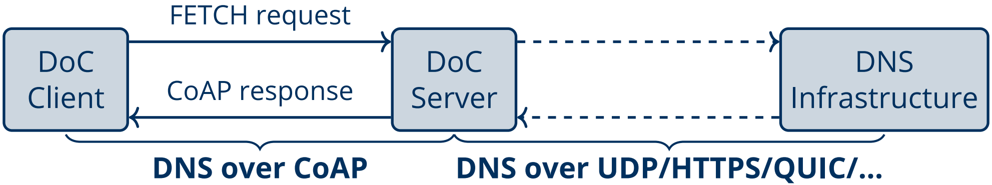
- Just map the DoH methods **GET** and **POST**?
- **FETCH** method in CoAP: best of both worlds (RFC 8132)

	HTTP GET	HTTP POST	CoAP FETCH
Cacheable	✓	✗	✓
Application data carried in body	✗	✓	✓
Block-wise transferable query	✗	✓	✓

DNS over CoAP (DoC)

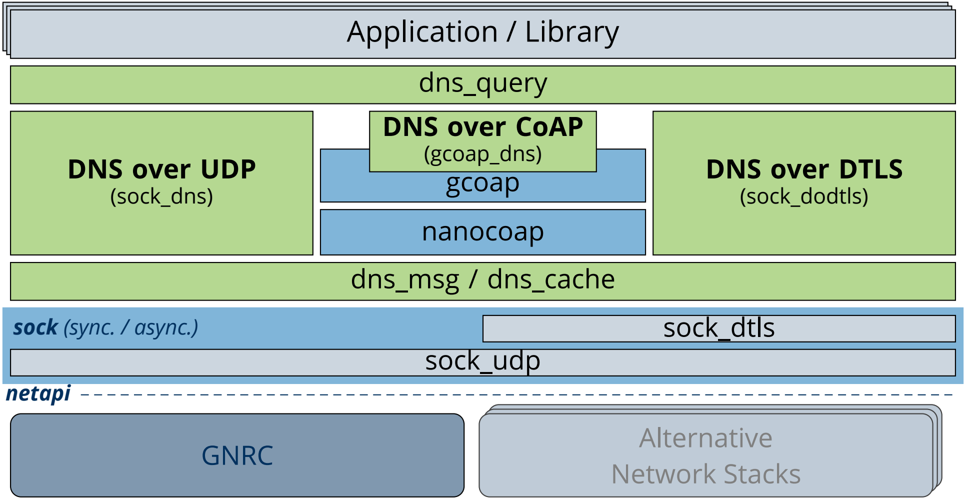
- Just map the DoH methods **GET** and **POST**?
- **FETCH** method in CoAP: best of both worlds (RFC 8132)

	CoAP		
	HTTP		
	GET	POST	FETCH
Cacheable	✓	✗	✓
Application data carried in body	✗	✓	✓
Block-wise transferable query	✗	✓	✓

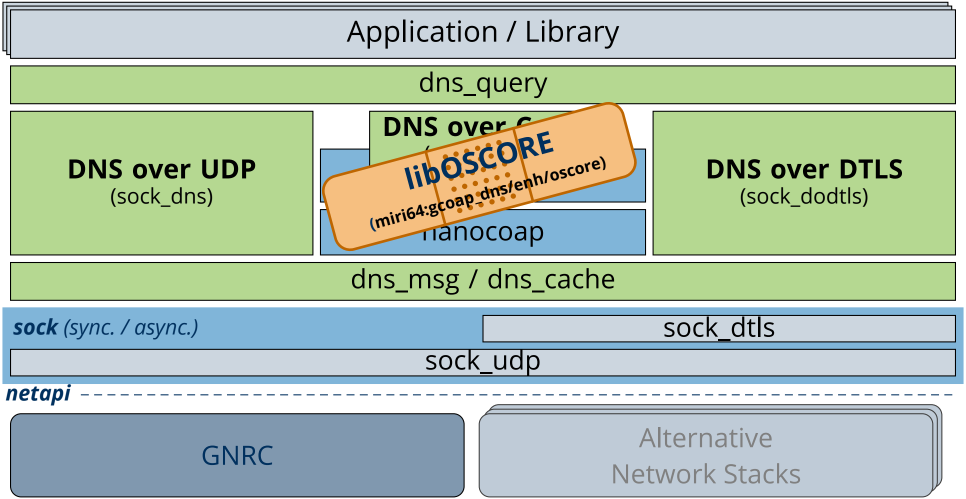


Outline

DoC RIOT Integration



DoC RIOT Integration



Outline

Motivation

Design Guidance from IoT DNS Traffic

DNS over CoAP

DoC RIOT Integration

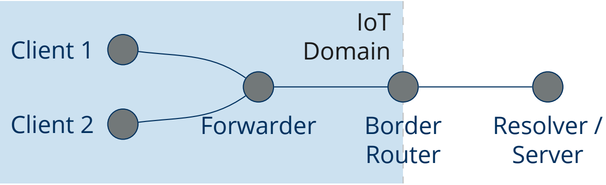
Evaluation

Conclusion & Next Steps

Evaluation Setup: DNS Transport Comparison

Name properties: Based on empirically measured data from IoT devices

Testbed experiments:

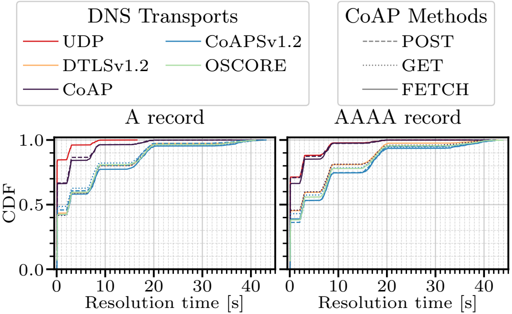


RIOT

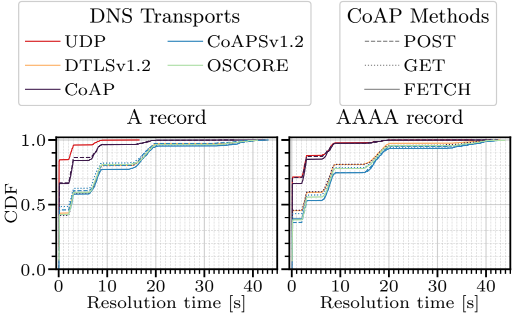
FIT IOT-LAB

- Clients query 50 A or AAAA records for names of length 24 chars via DNS over UDP / DTLSv1.2 / CoAP (unencrypted) / CoAPSv1.2 / OSCORE
- Poisson distribution: $\lambda = 5$ queries / sec (ignoring `NSTART=1` requirements)
- 10 runs on IoT-nodes (incl. BR): Cortex-M3 with IEEE 802.15.4 radio

Experiment: Resolution Time

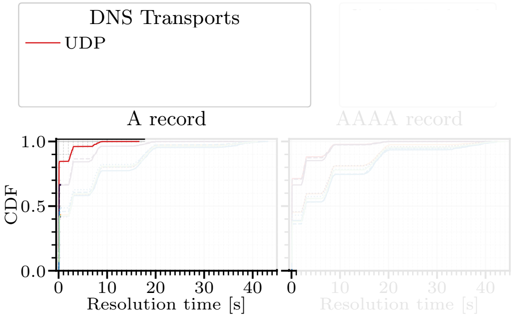


Experiment: Resolution Time



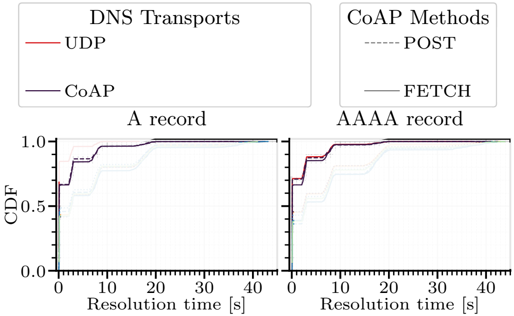
Clear performance groupings visible

Experiment: Resolution Time



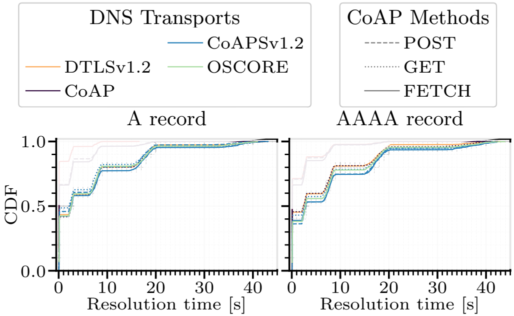
Group 1

Experiment: Resolution Time



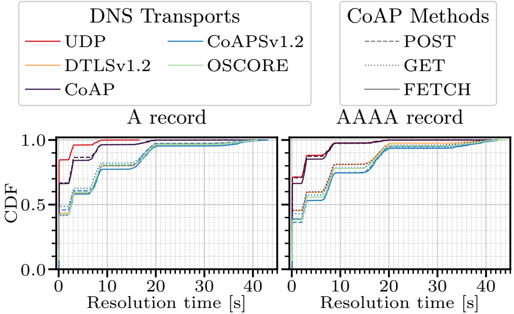
Group 2

Experiment: Resolution Time



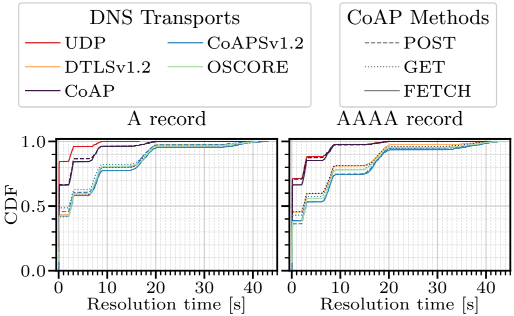
Group 3

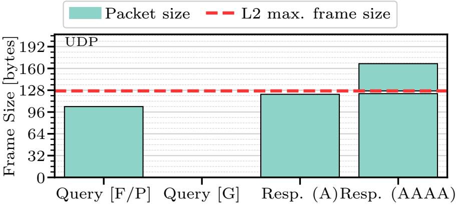
Experiment: Resolution Time



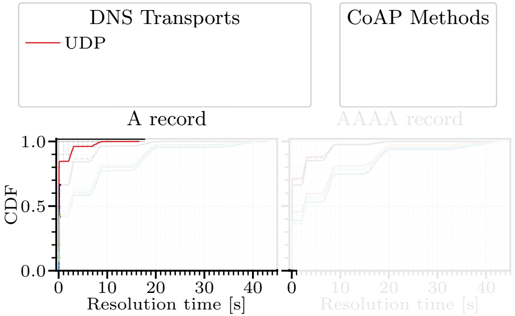
Where do performance groups come from?

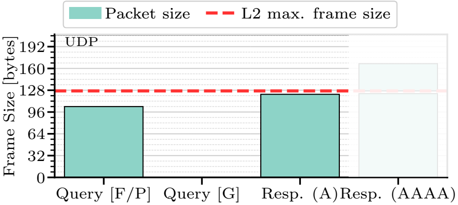
Experiment: Resolution Time & Packet Sizes





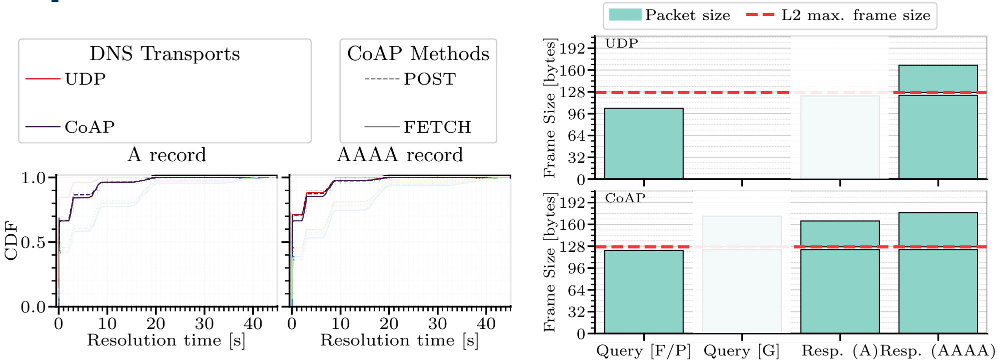
Experiment: Resolution Time & Packet Sizes





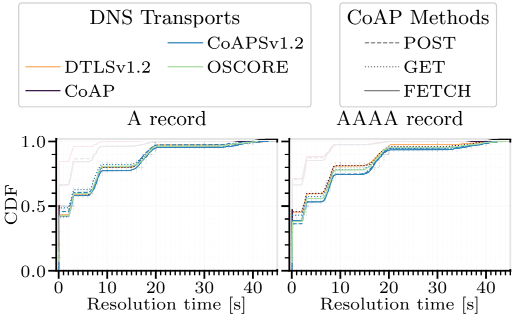
Group 1
No message fragmentation

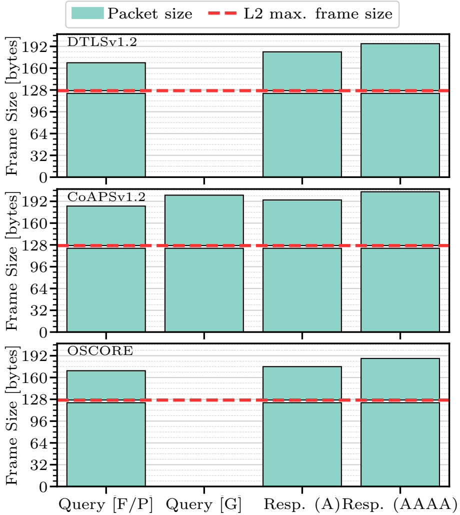
Experiment: Resolution Time & Packet Sizes



Group 2
Query unfragmented
Response fragmented

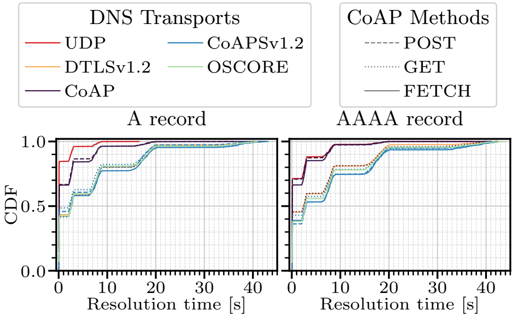
Experiment: Resolution Time & Packet Sizes

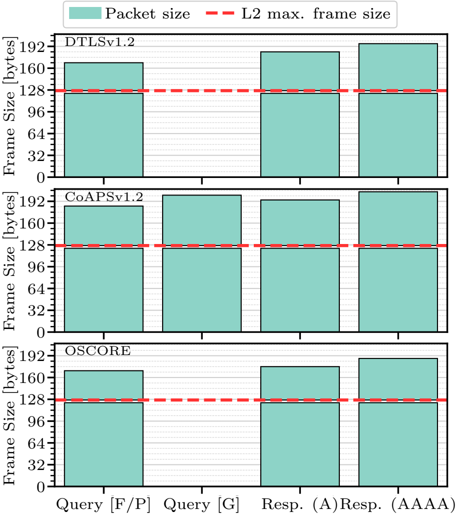




Group 3
Both messages fragmented

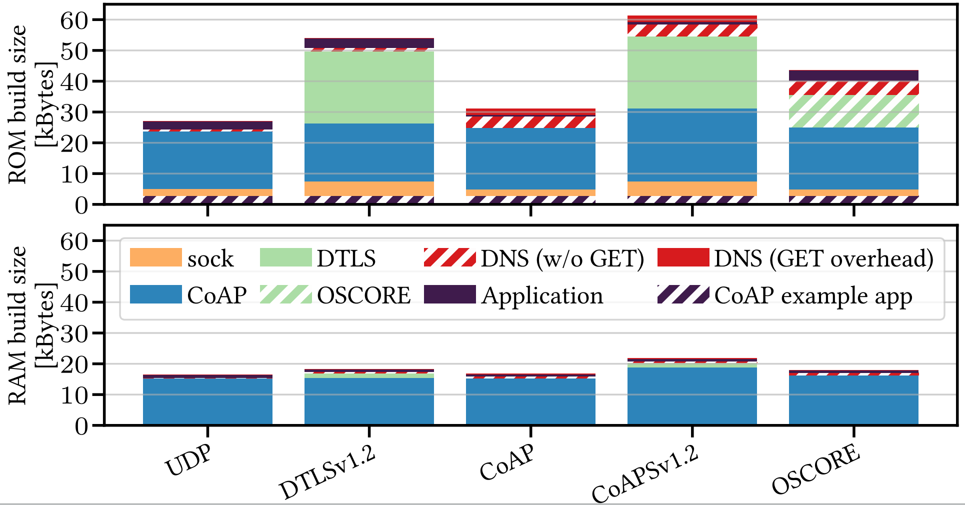
Experiment: Resolution Time & Packet Sizes



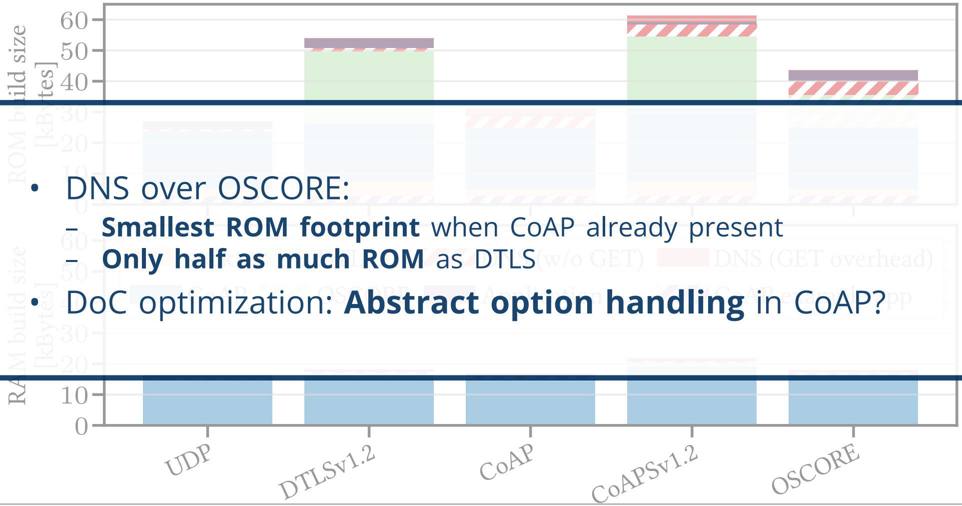


⇒ Fragmentation has larger impact on performance compared to transport or CoAP method

Memory Consumption



Memory Consumption



- DNS over OSCORE:
  - **Smallest ROM footprint** when CoAP already present
  - **Only half as much ROM** as DTLS
- DoC optimization: **Abstract option handling** in CoAP?

Outline

Motivation

Design Guidance from IoT DNS Traffic

DNS over CoAP

DoC RIOT Integration

Evaluation

Conclusion & Next Steps

Conclusion & Next Steps

- DoC with FETCH provides encrypted DNS for constrained IoT
  - Segmentable with block-wise transfer
  - En-route caching at CoAP proxies
- OSCORE outperforms CoAPS both in packet and build size
- Next:
  - Concise and compressed DNS message format (`draft-lenders-dns-cbor`)
  - mDNS protection with Group OSCORE?

Reproducible Research: Our Artifacts

- https://zenodo.org/record/8193681
- https://github.com/anr-bmbf-pivot/Artifacts-CoNEXT23-DoC