Martine S. Lenders, TU Dresden (martine.lenders@tu-dresden.de)
Thomas C. Schmidt, HAW Hamburg (t.schmidt@haw-hamburg.de)
Matthias Wählisch, TU Dresden & Barkhausen Institut Dresden (m.waehlisch@tu-dresden.de)

Secure Name Resolution in the IoT

DINR 2024 Virtual Workshop

Motivation

Attack Scenario

Countermeasure

Encrypt name resolution triggered by IoT devices against eavesdropping

Challenge: Constrained IoT

Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Challenge: Constrained IoT

BLE

zigbee

LoRa

Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained networks:

- Low throughput, high packet loss, asymmetric link characteristics
- High penalties on large packets (link layer fragmentation)

Characteristic	IEEE 802.15.4	BLE	LoRaWAN
Data rate [kBit/s]	124–162	125–2000	0.3–5
Frame size [bytes]	127	≥ 1280	59–250

Challenge: Constrained IoT

BLE

zigbee

LoRa

Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained

- Low thro… …nk characteris…
- High penalties on large packets (link la… …fragmentation)

0.000003% – 0.0009% of WiFi 6 data rate

Characteristic	IEEE 802.15.4	BLE	LoRaWAN
Data rate [kBit/s]	124–162	125–2000	0.3–5
Frame size [bytes]	127	≥ 1280	59–250

Possible Solutions for Encrypted DNS

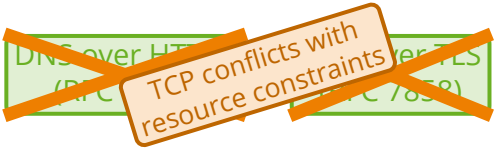
DNS over HTTPS (RFC 8484)

DNS over TLS (RFC 7858)

DNS over QUIC (RFC 9250)

DNS over DTLS (RFC 8094)

Possible Solutions for Encrypted DNS



DNS over QUIC (RFC 9250)

DNS over DTLS (RFC 8094)

Possible Solutions for Encrypted DNS

Possible Solutions for Encrypted DNS

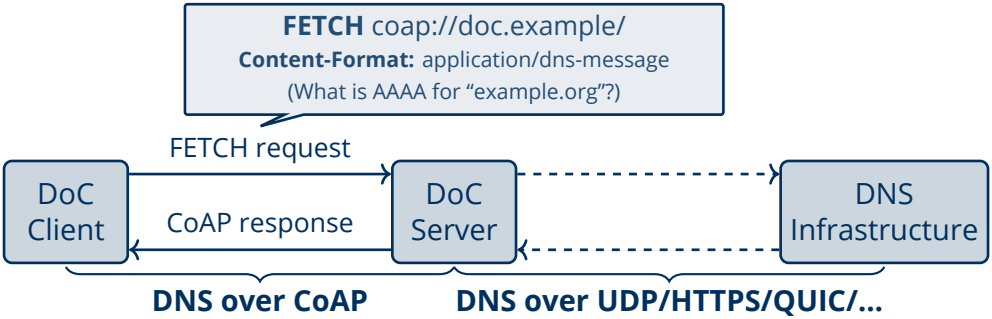
Possible Solutions for Encrypted DNS

Our proposal: DNS over CoAP

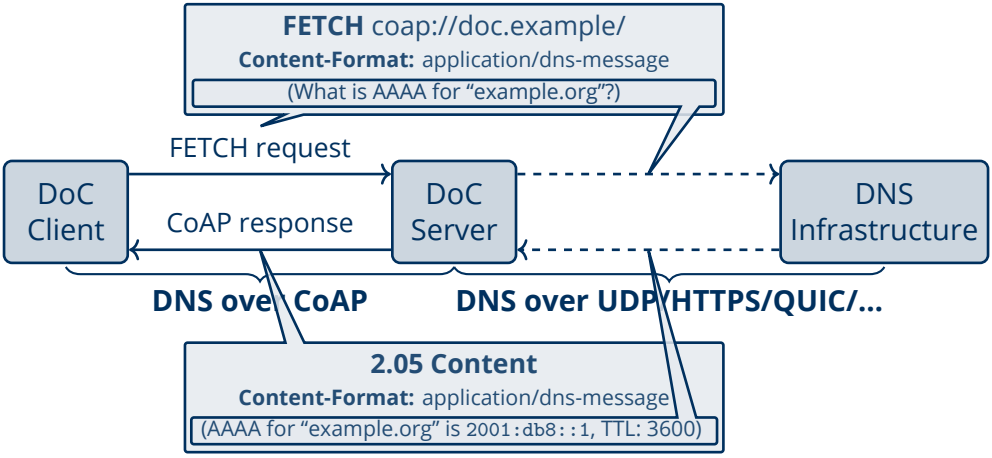
(https://datatracker.ietf.org/doc/draft-ietf-core-dns-over-coap/)

- **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

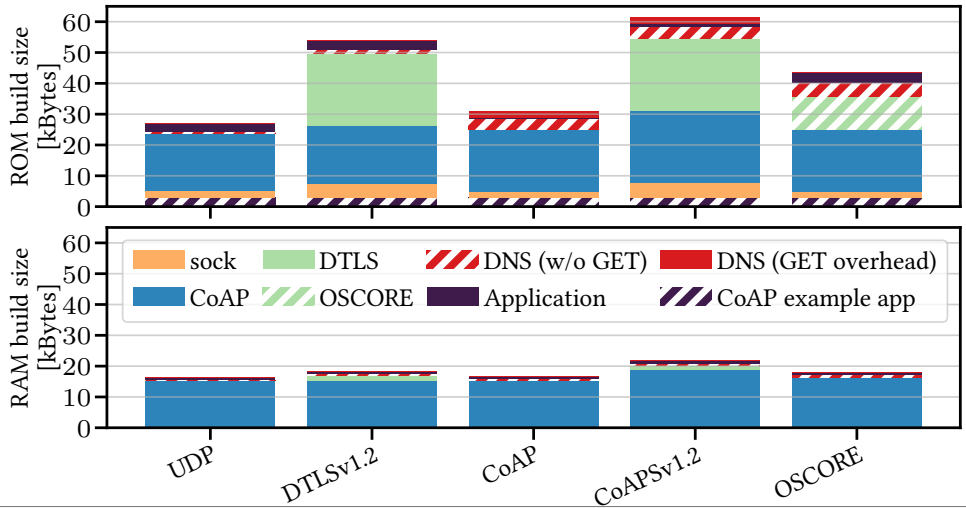
DNS over CoAP (DoC): Example Query



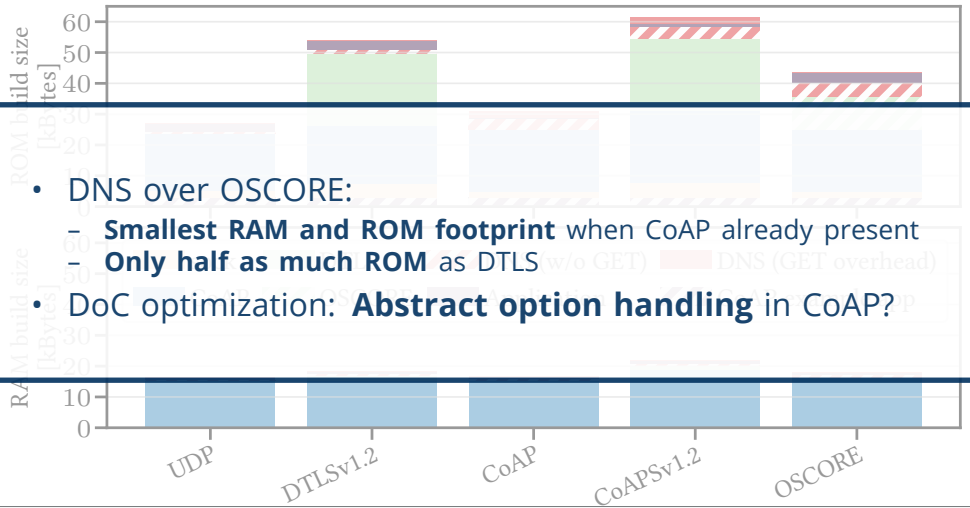
DNS over CoAP (DoC): Example Query



Evaluation: Memory Consumption



Evaluation: Memory Consumption

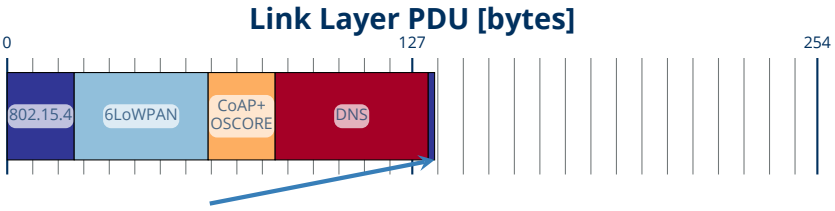


- DNS over OSCORE:
  - **Smallest RAM and ROM footprint** when CoAP already present
  - **Only half as much ROM** as DTLS
- DoC optimization: **Abstract option handling** in CoAP?

A Concise DNS Message Representation

Constrained Networks, e.g., IEEE 802.15.4 with PDU of 127 bytes

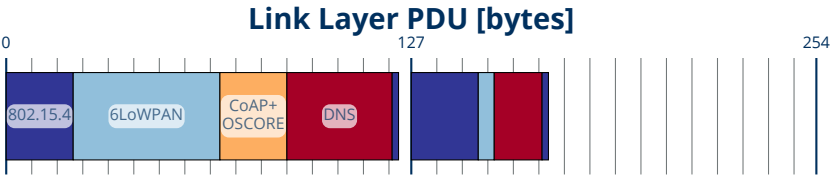
Name Length	Message Type
2 chars	AAAA Response



A Concise DNS Message Representation

Constrained Networks, e.g., IEEE 802.15.4 with PDU of 127 bytes

Name Length	Message Type
2 chars	AAAA Response



⇒ Fragmentation

A Concise DNS Message Representation

Constrained Networks, e.g., IEEE 802.15.4 with PDU of 127 bytes

Name Length	Message Type
2 chars	AAAA Response

⇒ Fragmentation

A Concise DNS Message Representation

Constrained Networks, e.g., IEEE 802.15.4 with PDU of 127 bytes

Concise DNS messages are needed

`application/dns+cbor`

Media Type and Content-Format

(*i.e.*, usable with both DoC and DoH)

`https://datatracker.ietf.org/doc/draft-lenders-dns-cbor/`

Conclusion & Future Work

Secure & privacy-friendly DNS is ready for the constrained IoT:

- DNS over CoAP provides encrypted, cachable, and segmentable DNS
- En par in resolution time with existing UDP-based transfer protocols
- OSCORE outperforms DTLS and CoAPS both in packet and memory size

Future Work:

- Specify and evaluate concise DNS message format (`draft-lenders-dns-cbor`)
- Wishlist for data sets
  - DNS traffic traces including AAAA, SOA, and SVCB/HTTPS records
  - DNS zone files including AAAA, CNAME, NS, PTR, SOA, and SVCB/HTTPS records

Anybody open for collaboration?

Our Research on DNS over CoAP

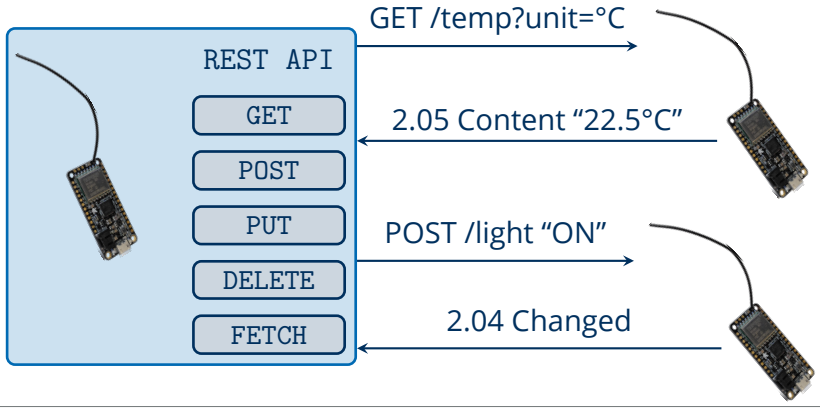
Martine S. Lenders, Christian Amsüss, Cenk Gündogan, Marcin Nawrocki, Thomas C. Schmidt, Matthias Wählisch. 2023. **Securing Name Resolution in the IoT: DNS over CoAP**, *Proceedings of the ACM on Networking (PACMNET)* 1, CoNEXT2, Article 6 (September 2023), 25 pages. https://doi.org/10.1145/3609423

arXiv pre-print: https://arxiv.org/abs/2207.07486
Specification: https://datatracker.ietf.org/doc/draft-ietf-core-dns-over-coap

Backup Slides

CoAP: The Constrained Application Protocol

“REST over UDP” ∼ The HTTP for IoT



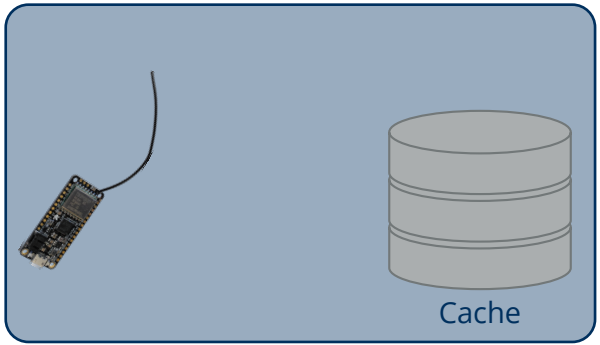
CoAP Caching

Client

Cache

Server

CoAP Caching

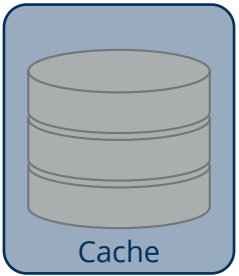


On client node

Server

CoAP Caching

Client

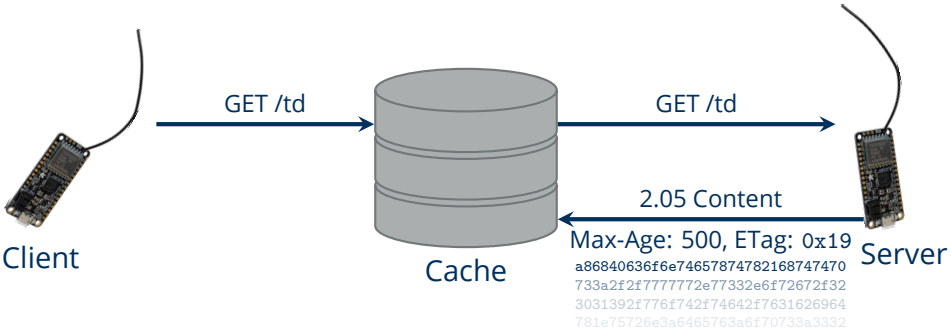


On proxy node

Server

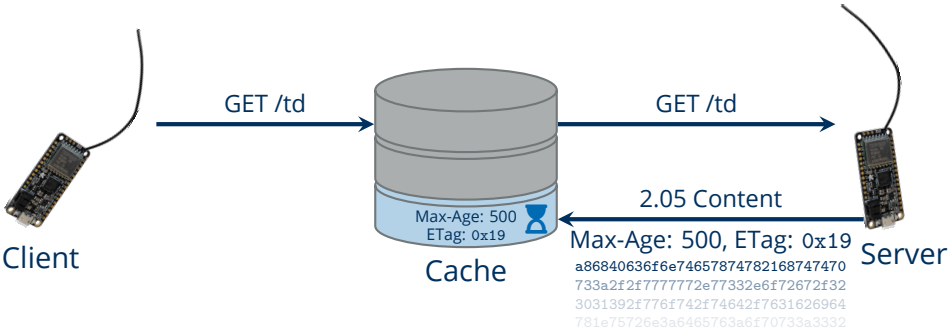
CoAP Caching

Caching provides **decoupling from packet loss**



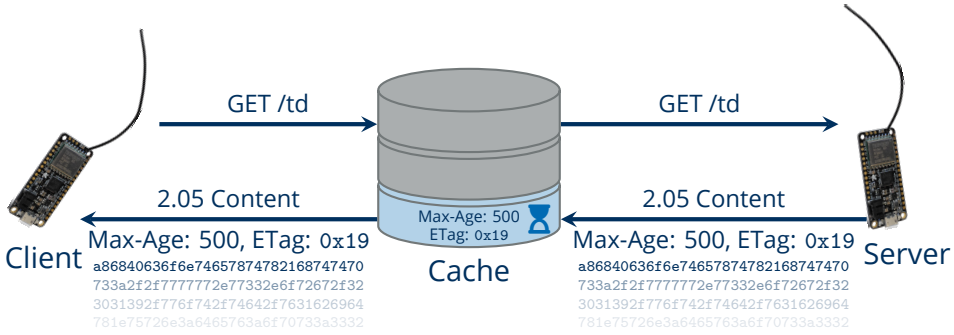
CoAP Caching

Caching provides **decoupling from packet loss**



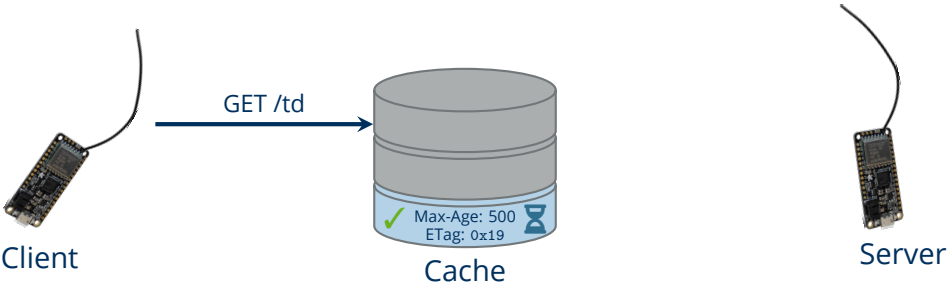
CoAP Caching

Caching provides **decoupling from packet loss**



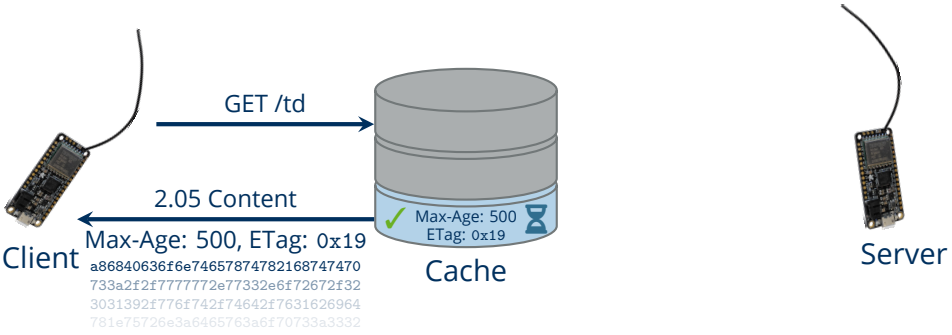
CoAP Caching

Caching provides **decoupling from packet loss**



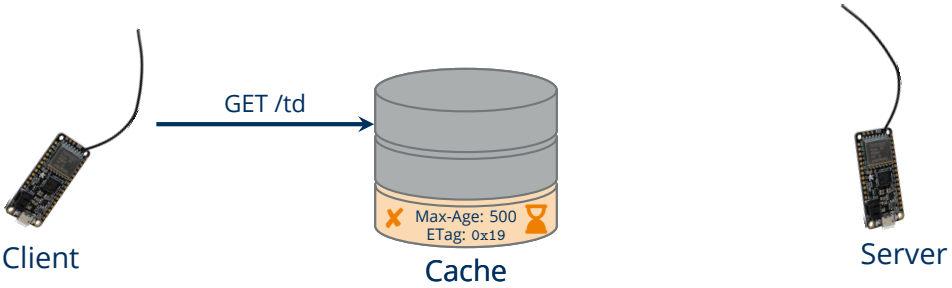
CoAP Caching

Caching provides **decoupling from packet loss**



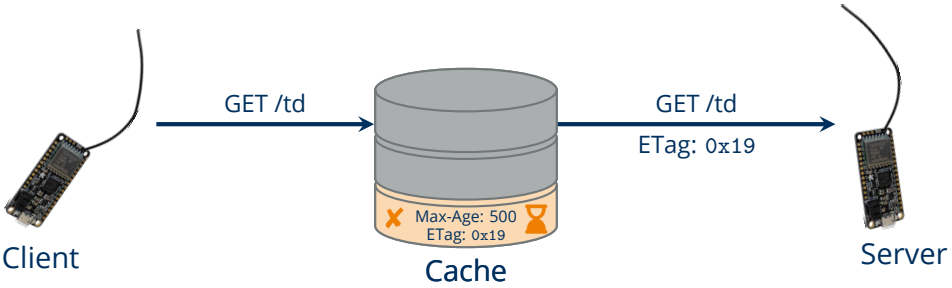
CoAP Caching

What if cache entry goes stale?



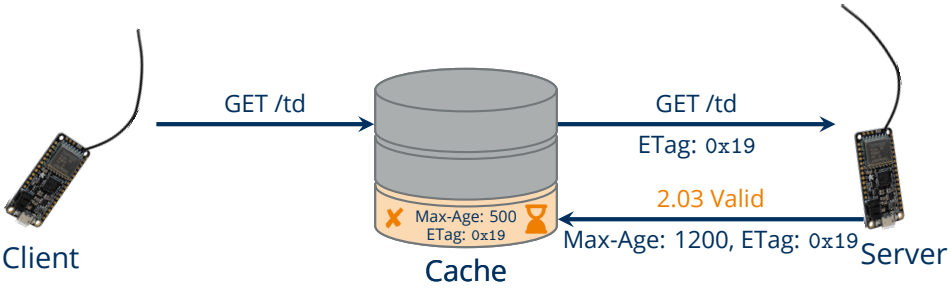
CoAP Caching

What if cache entry goes stale?



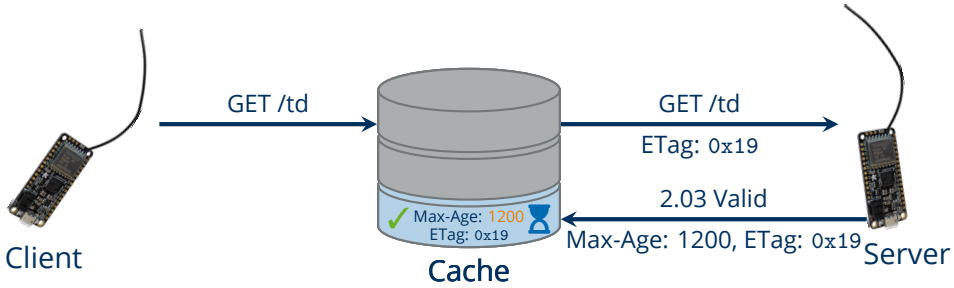
CoAP Caching

Cache validation **reduces data overhead**



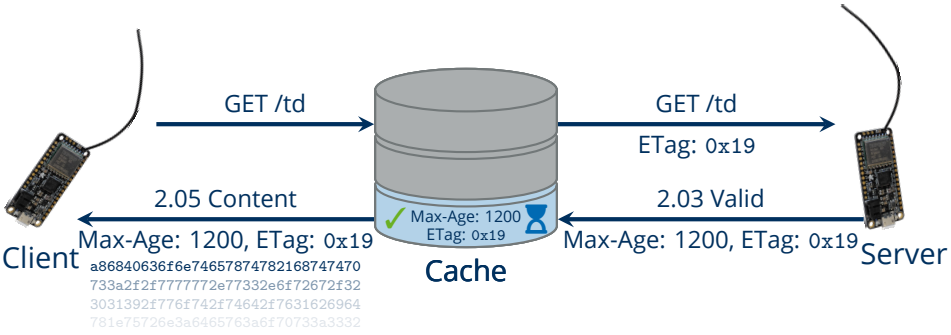
CoAP Caching

Cache validation **reduces data overhead**



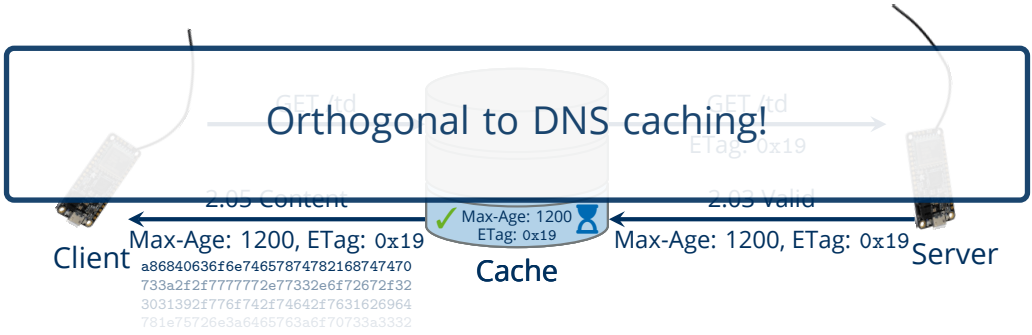
CoAP Caching

Cache validation **reduces data overhead**



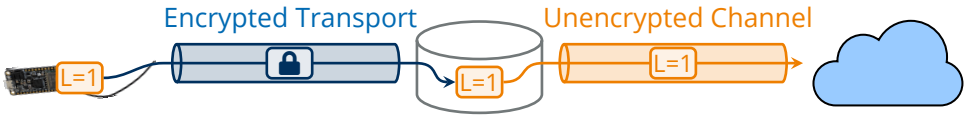
CoAP Caching

Cache validation **reduces data overhead**



CoAP Security Modes

DTLS Datagram Transport Layer Security (≈ TLS over UDP)



OSCORE Object Security for Constrained RESTful Environment

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

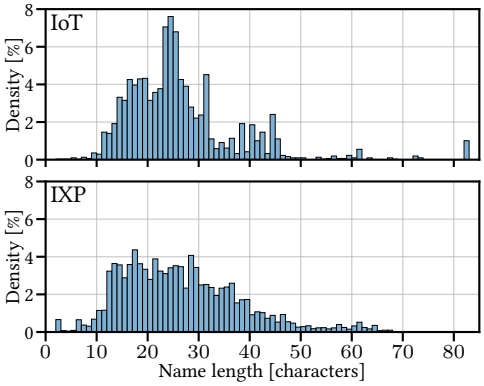
- Large Central European IXP
- Collected January 2022
- DNS only
- Sampling rate: 1/16000 pkts.
- 1.6 million queries
- 2.4 million responses
- Names anonymized to lengths

[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.

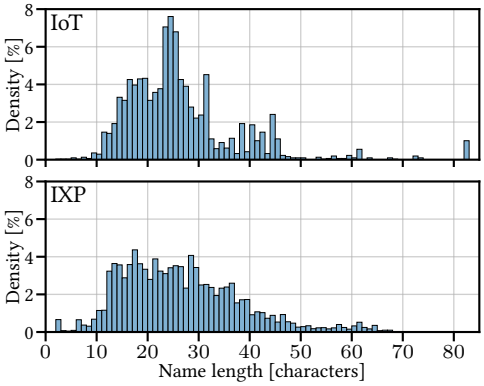
[3] J. Ren, D.J. Dubois, D. Choffnes, A.M. Mandalari, R. Kolcun, and H. Haddadi. 2019. **Information Exposure for Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach**. In *Proc. of the Internet Measurement Conference (IMC)*. ACM.

DNS IoT Traffic: Name Lengths



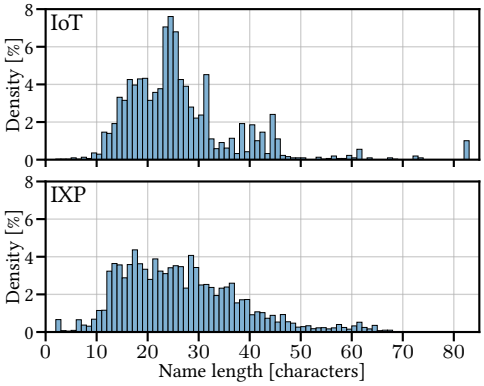
	Length of domain names [chars]				
Data set	Min	Max	Mean	Std. Dev.	Median
YourThings	2	83	24.5	9.7	24
IoTFinder	7	82	26.8	10.5	24
MonIoTr	9	83	27.1	14.7	23
IoT total	2	83	25.9	1.3	24
IXP	0	68	26.1	1.7	25

DNS IoT Traffic: Name Lengths



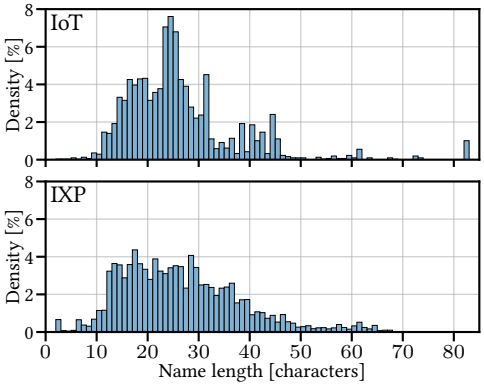
	Length of domain names [chars]				
Data set	Min	Max	Mean	Std. Dev.	Median
YourThings	2	83	24.5	9.7	24
IoTFinder	7	82	26.8	10.5	24
MonIoTr	9	83	27.1	14.7	23
IoT total	2	83	25.9	1.3	24
IXP	0	68	26.1	1.7	25

DNS IoT Traffic: Name Lengths



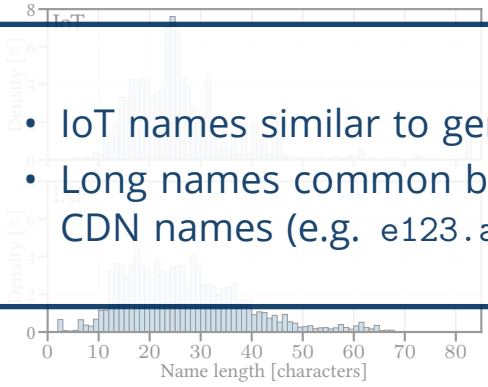
	Length of domain names [chars]				
Data set	Min	Max	Mean	Std. Dev.	Median
YourThings	2	83	24.5	9.7	24
IoTFinder	7	82	26.8	10.5	24
MonIoTr	9	83	27.1	14.7	23
IoT total	2	83	25.9	1.3	24
IXP	0	68	26.1	1.7	25

DNS IoT Traffic: Name Lengths



	Length of domain names [chars]				
Data set	Min	Max	Mean	Std. Dev.	Median
YourThings	2	83	24.5	9.7	24
IoTFinder	7	82	26.8	10.5	24
MonIoTr	9	83	27.1	14.7	23
IoT total	2	83	25.9	1.3	24
IXP	0	68	26.1	1.7	25

DNS IoT Traffic: Name Lengths



- IoT names similar to general Internet names
- Long names common because of cloud services and CDN names (e.g. `e123.abcd.akamaiedge.net`)

DNS IoT Traffic: Queried 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%

DNS IoT Traffic: Queried 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

DNS IoT Traffic: Queried 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: Queried Record Type

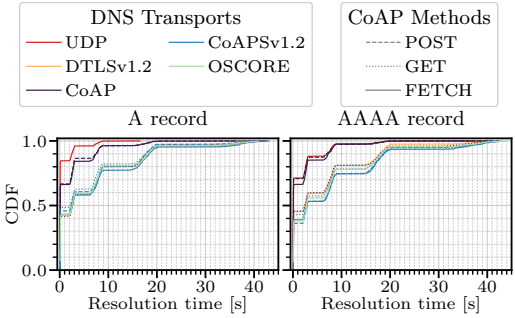
Mainly address resolution

Also service discovery & information

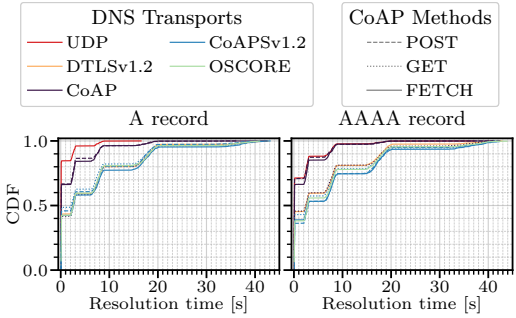
Queried Record Type	IoT Devices w/ mDNS	IoT Devices w/o mDNS	TXP
AAAA	16.4%	23.5%	17.6%
NS	—	—	9.1%
TXT	1.2%	0.1%	0.7%
Other	< 0.1%	0.3%	3.5%

- A/AAAA resolution is prevalent also in the IoT
- Group OSCORE may offer solution for encrypted DNS-SD
- Unsolicited `NS` records increase response sizes
  ⇒ Should be avoided with DoC

Experiment: Resolution Time

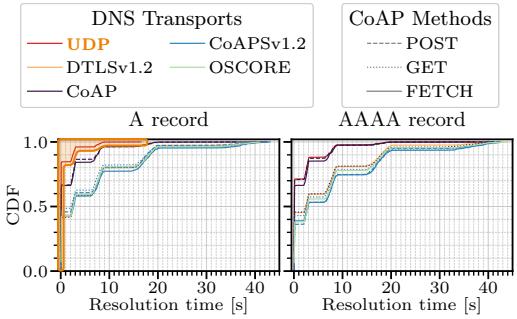


Experiment: Resolution Time



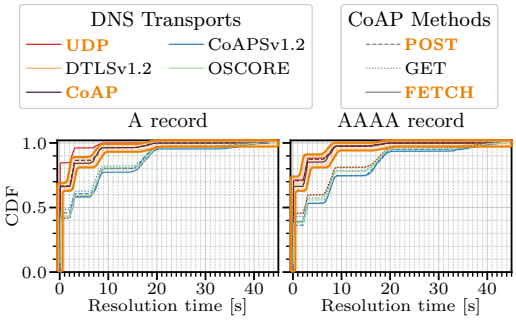
Clear performance groups visible

Experiment: Resolution Time



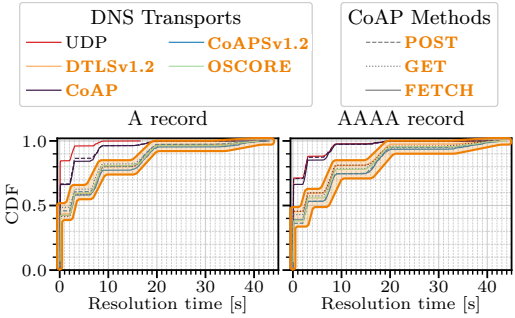
Group 1

Experiment: Resolution Time



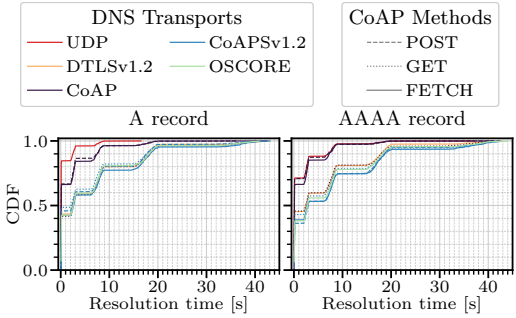
Group 2

Experiment: Resolution Time



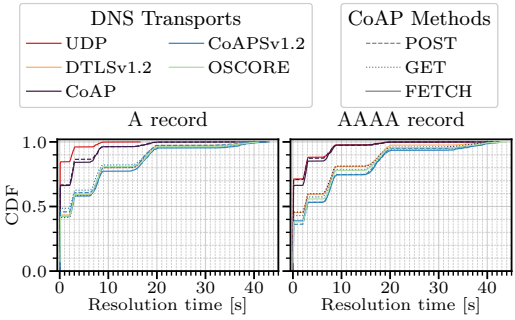
Group 3

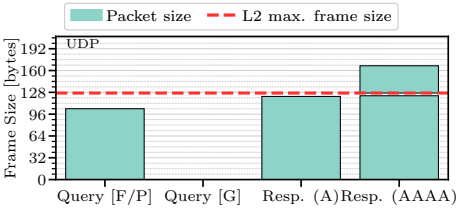
Experiment: Resolution Time



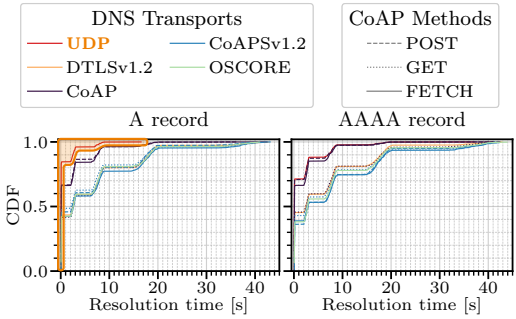
Where do performance groups come from?

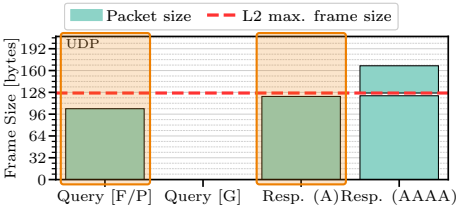
Experiment: Resolution Time & Packet Sizes





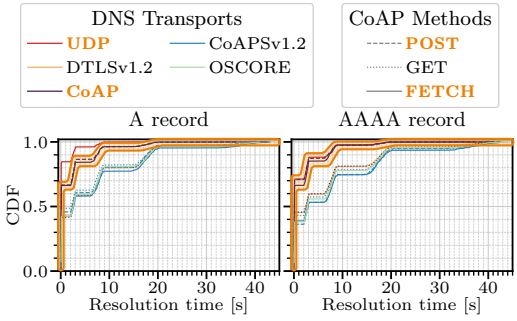
Experiment: Resolution Time & Packet Sizes

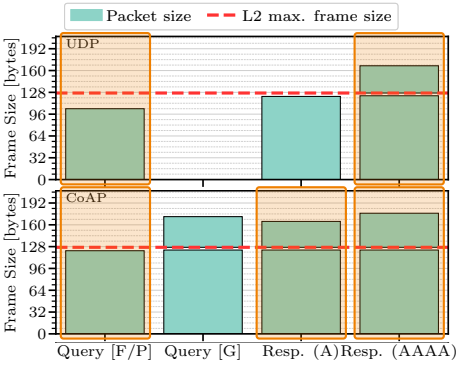




Group 1
No message fragmentation

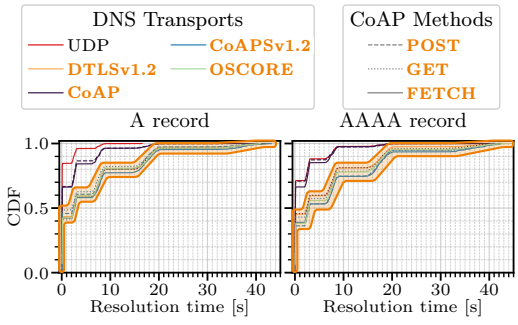
Experiment: Resolution Time & Packet Sizes

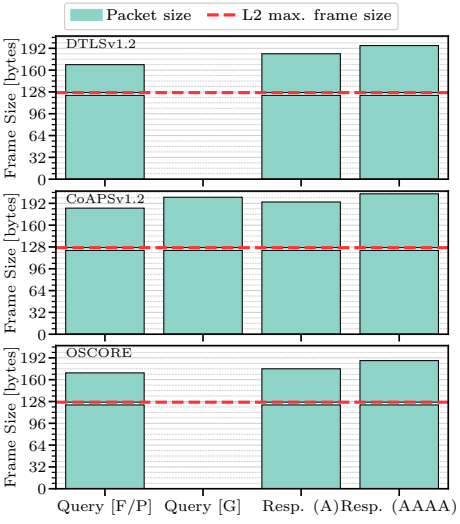




Group 2
Query unfragmented
Response fragmented

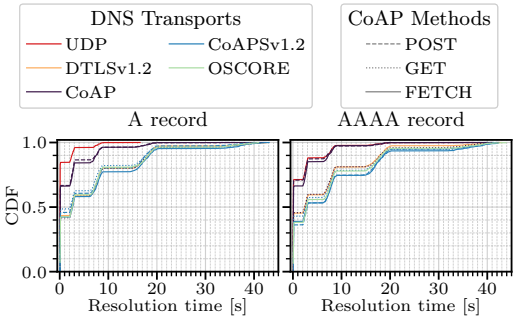
Experiment: Resolution Time & Packet Sizes

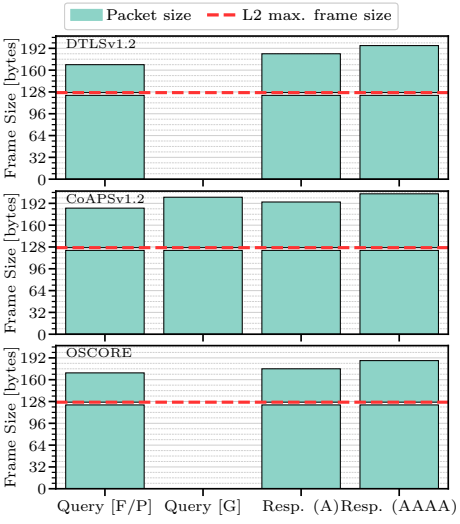




Group 3
Both messages fragmented

Experiment: Resolution Time & Packet Sizes

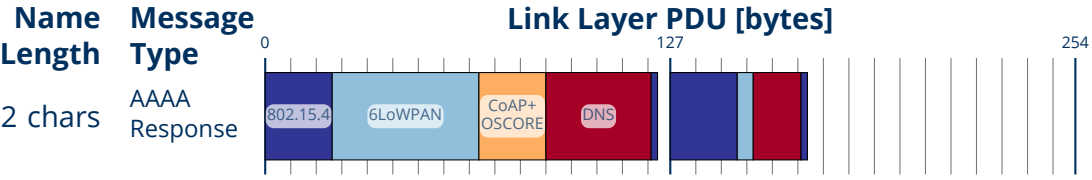




⇒ **Fragmentation has larger impact on performance** compared to transfer protocol or CoAP method

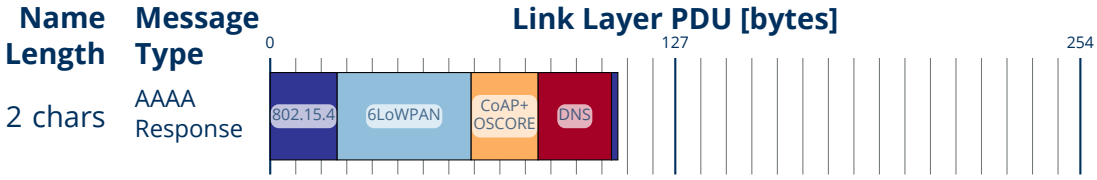
A Concise DNS Message Representation

Constrained Networks, e.g., IEEE 802.15.4 with PDU of 127 bytes



A Concise DNS Message Representation

Constrained Networks, e.g., IEEE 802.15.4 with PDU of 127 bytes



Our Research on DNS over CoAP

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