Martine S. Lenders[2,6] (martine.lenders@tu-dresden.de), Christian Amsüss[7] (christian@amsuess.com), Cenk Gündogan[4] (cenk.gundogan@huawei.com), Marcin Nawrocki[2,5] (marcin.nawrocki@fu-berlin.de), Thomas C. Schmidt[3] (t.schmidt@haw-hamburg.de), Matthias Wählisch[1,6] (m.waehlisch@tu-dresden.de)

[1]Barkhausen Institut, Dresden, Germany | [2]Freie Universität Berlin, Germany | [3]HAW Hamburg, Germany | [4]Huawei Technologies, Munich, Germany | [5]NETSCOUT, Berkeley, CA, USA | [6]TU Dresden, Germany | [7]Unaffiliated, Vienna, Austria

Securing Name Resolution in the IoT: DNS over CoAP

Paris, CoNEXT'23, 2023-12-05

Outline

Motivation

CoAP: A Short Introduction

Design Guidance from IoT DNS Traffic

DNS over CoAP

Evaluation

Future Work: Concise DNS Message Representation

Conclusion

Outline

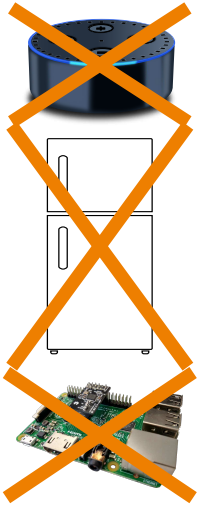
Motivation

Attack Scenario

Countermeasure

Encrypt name resolution triggered by IoT devices against eavesdropping

Challenge: Constrained IoT



Constrained nodes (RFC 7228):

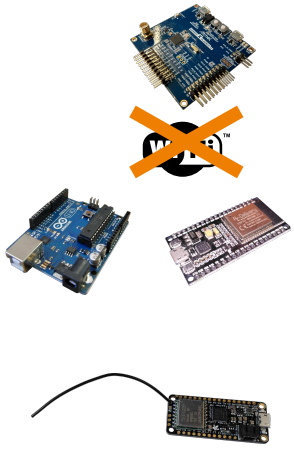
Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Challenge: Constrained IoT

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



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)

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

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)

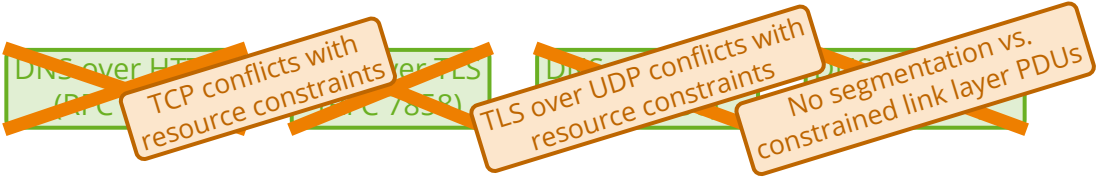
Possible Solutions

DNS over QUIC (RFC 9250)

DNS over DTLS (RFC 8094)

Possible Solutions

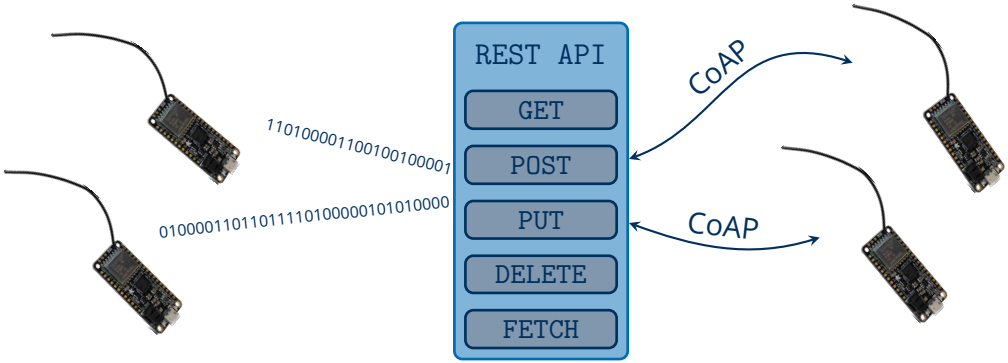
Possible Solutions



Possible Solutions

Outline

CoAP: The Constrained Application Protocol
“REST over UDP”



CoAP Security Modes

DTLS Datagram Transport Layer Security (≈ TLS over UDP)

CoAP Security Modes

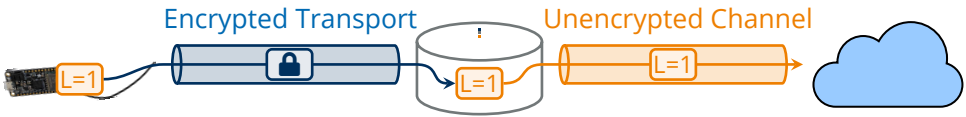
DTLS Datagram Transport Layer Security (≈ TLS over UDP)

CoAP Security Modes

DTLS Datagram Transport Layer Security (≈ TLS over UDP)

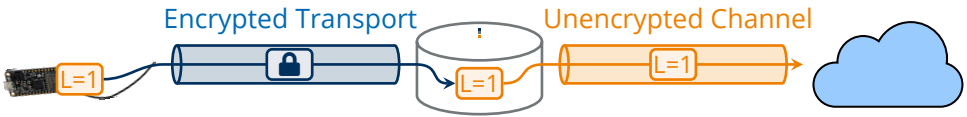
CoAP Security Modes

DTLS Datagram Transport Layer Security (≈ TLS over UDP)



CoAP Security Modes

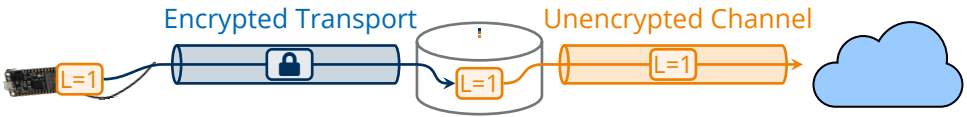
DTLS Datagram Transport Layer Security (≈ TLS over UDP)



OSCORE Object Security for Constrained RESTful Environment

CoAP Security Modes

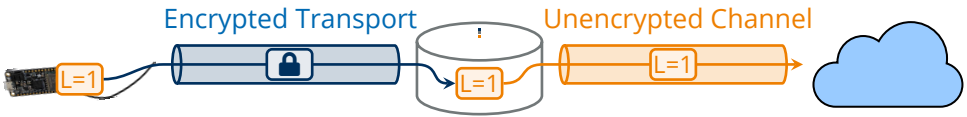
DTLS Datagram Transport Layer Security (≈ TLS over UDP)



OSCORE Object Security for Constrained RESTful Environment

CoAP Security Modes

DTLS Datagram Transport Layer Security (≈ TLS over UDP)



OSCORE Object Security for Constrained RESTful Environment

Outline

Motivation

CoAP: A Short Introduction

Design Guidance from IoT DNS Traffic

DNS over CoAP

Evaluation

Future Work: Concise DNS Message Representation

Conclusion

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

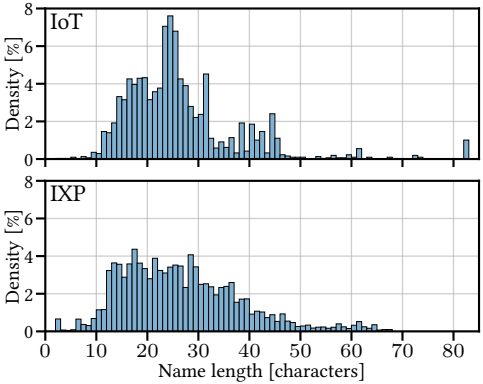
- Large Central European IXP
- Collected January 2022
- DNS only
- Sampling rate: 1/16000 pkts.
- 1.6 million queries
- 2.4 million responses
- Names anonymized to lengths

[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.

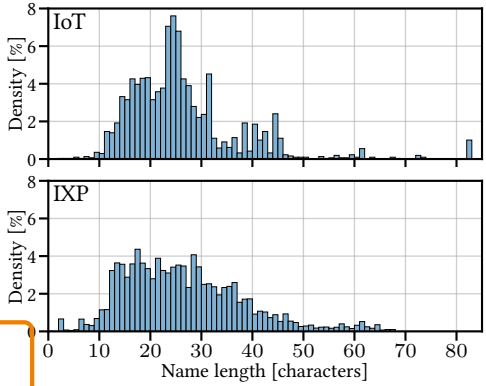
[3] J. Ren, D.J. Dubois, D. Choffnes, A.M. Mandalari, R. Kolcun, and H. Haddadi. 2019. **Information Exposure for Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach**. In *Proc. of the Internet Measurement Conference (IMC)*. ACM.

DNS IoT Traffic: Name Lengths



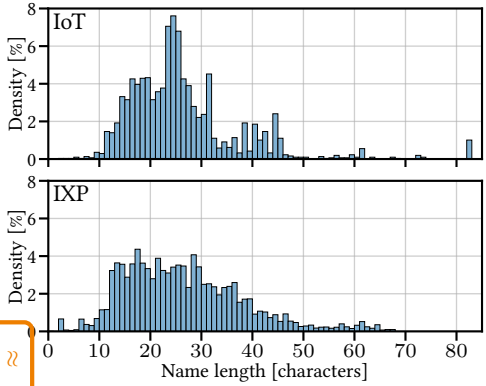
	Length of domain names [chars]							
Data set	min	max	mode	μ	σ	Q_1	Q_2	Q_3
YourThings	2	83	31	24.5	9.7	18	24	30
IoTFinder	7	82	24	26.8	10.5	20	24	30
MonIoTr	9	83	18	27.1	14.7	18	23	30
IoT total	2	83	24	25.9	1.3	19	24	30
IXP	0	68	17	26.1	1.7	17	25	33

DNS IoT Traffic: Name Lengths



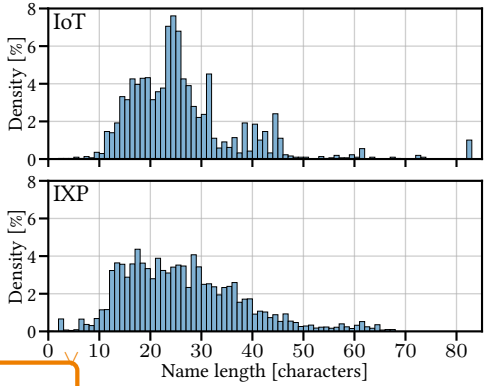
	Length of domain names [chars]							
Data set	min	max	mode	μ	σ	Q_1	Q_2	Q_3
YourThings	2	83	31	24.5	9.7	18	24	30
IoTFinder	7	82	24	26.8	10.5	20	24	30
MonIoTr	9	83	18	27.1	14.7	18	23	30
IoT total	2	83	24	25.9	1.3	19	24	30
IXP	0	68	17	26.1	1.7	17	25	33

DNS IoT Traffic: Name Lengths



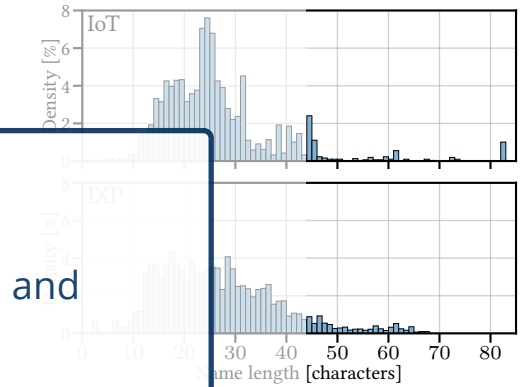
	Length of domain names [chars]							
Data set	min	max	mode	μ	σ	Q_1	Q_2	Q_3
YourThings	2	83	31	24.5	9.7	18	24	30
IoTFinder	7	82	24	26.8	10.5	20	24	30
MonIoTr	9	83	18	27.1	14.7	18	23	30
IoT total	2	83	24	25.9	1.3	19	24	30
IXP	0	68	17	26.1	1.7	17	25	33

DNS IoT Traffic: Name Lengths



	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



	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: 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		IXP
		w/o mDNS	
A	75.8%	75.8%	64.5%
AAAA	23.5%	23.5%	17.6%
ANY	—	—	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		IXP
		w/o mDNS	
A	75.8%	75.8%	64.5%
AAAA	23.5%	23.5%	17.6%
ANY	—	—	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/o mDNS	IXP
A	75.8%	64.5%
AAAA	23.5%	17.6%
HTTPS	—	1.7%
NS	—	9.1%
PTR	—	0.7%
SRV	19.6%	0.3%
TXT	1.0%	—
Other	1.2%	0.1%
	< 0.1%	0.3%

Mainly address resolution

should be favored by DoC

nay offer solution for
D

ords increase response size
ded with DoC

Outline

Motivation

CoAP: A Short Introduction

Design Guidance from IoT DNS Traffic

DNS over CoAP

Evaluation

Future Work: Concise DNS Message Representation

Conclusion

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)

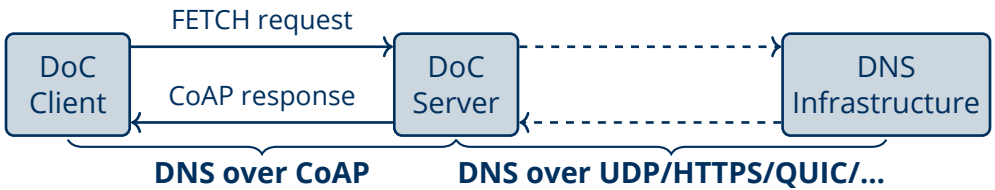
- Just map the DoH methods **GET** and **POST**?
- **FETCH** method in CoAP: best of both worlds (RFC 8132)

	CoAP		
	HTTP		
	GET	POST	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

Motivation

CoAP: A Short Introduction

Design Guidance from IoT DNS Traffic

DNS over CoAP

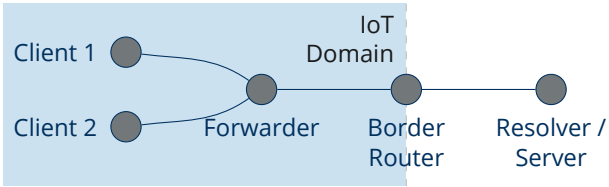
Evaluation

Future Work: Concise DNS Message Representation

Conclusion

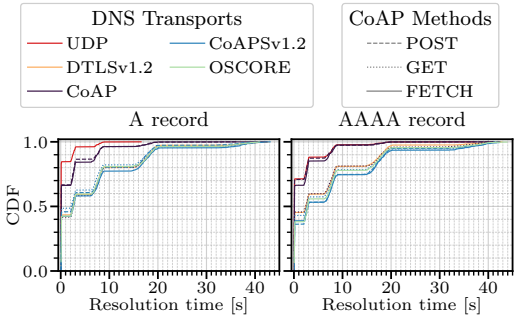
Evaluation Setup: DNS Transport Comparison

Name properties: Based on empirically measured data from IoT devices
Testbed experiments:

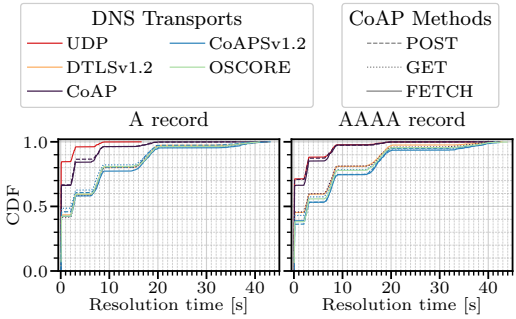


- Clients query 50 A or AAAA records for names of length 24 chars
  via DNS over UDP / DTLSv1.2 / CoAP (unencrypted) / CoAPSv1.2 / OSCORE
- Poisson distribution: $\lambda = 5$ queries / sec (ignoring `NSTART=1` requirements)
- 10 runs on IoT-nodes (incl. BR): Cortex-M3 with IEEE 802.15.4 radio

Experiment: Resolution Time

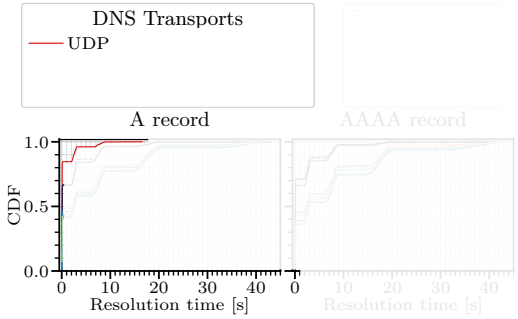


Experiment: Resolution Time



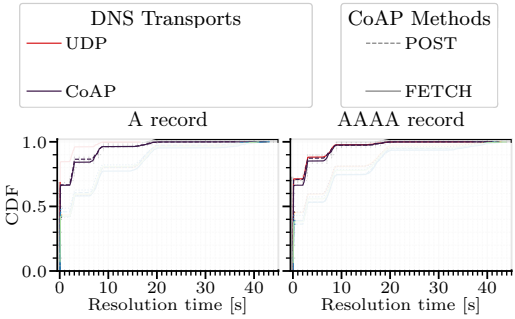
Clear performance groupings visible

Experiment: Resolution Time



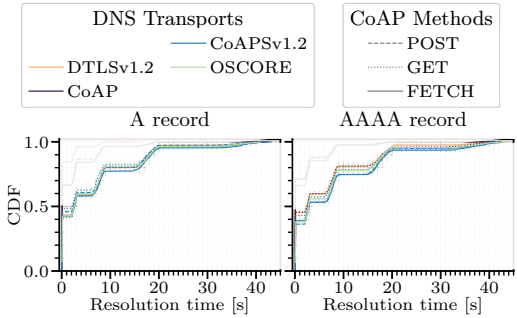
Group 1

Experiment: Resolution Time



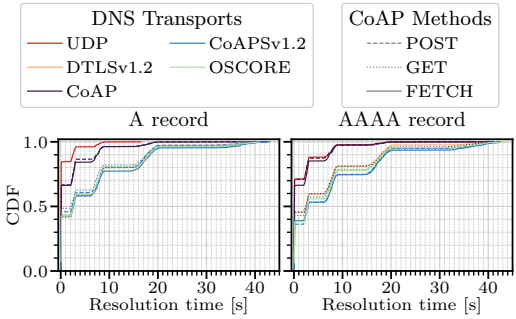
Group 2

Experiment: Resolution Time



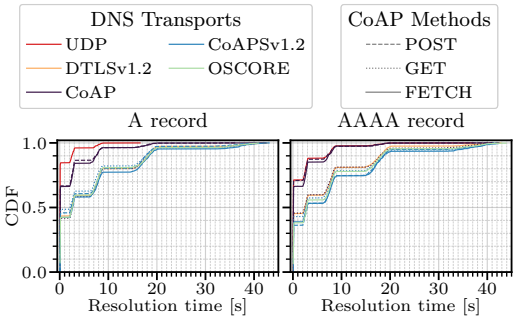
Group 3

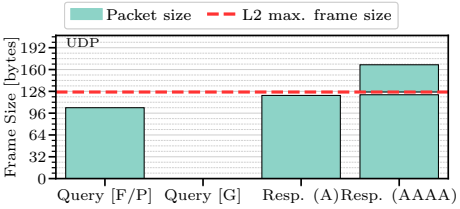
Experiment: Resolution Time



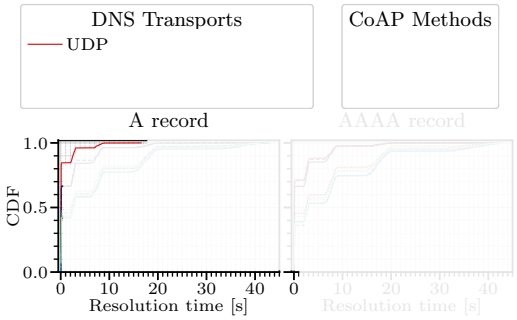
Where do performance groups come from?

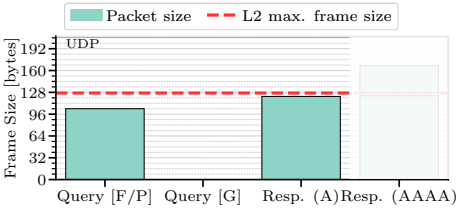
Experiment: Resolution Time & Packet Sizes





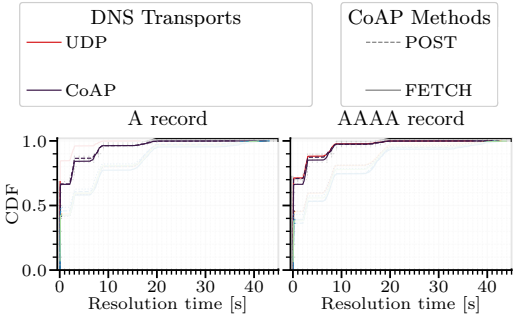
Experiment: Resolution Time & Packet Sizes

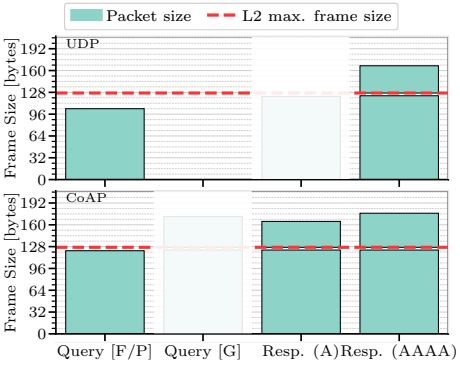




Group 1
No message fragmentation

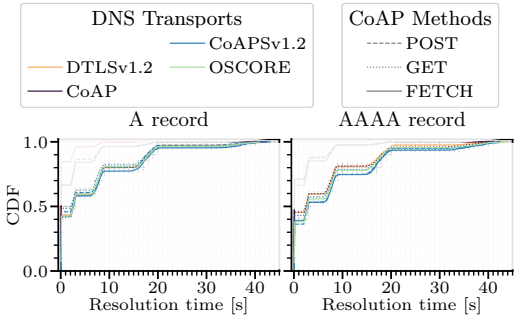
Experiment: Resolution Time & Packet Sizes

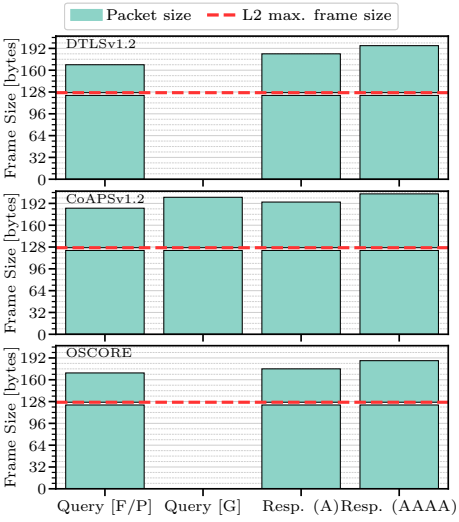




Group 2
Query unfragmented
Response fragmented

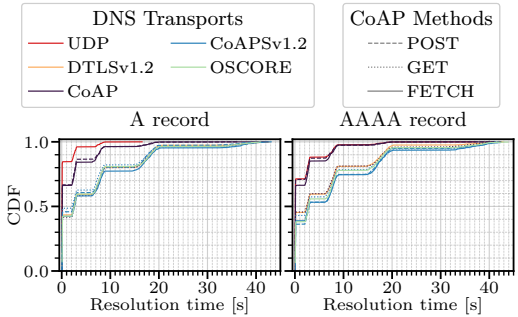
Experiment: Resolution Time & Packet Sizes

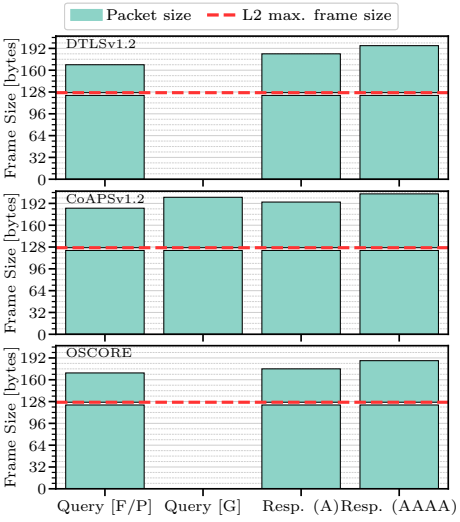




Group 3
Both messages fragmented

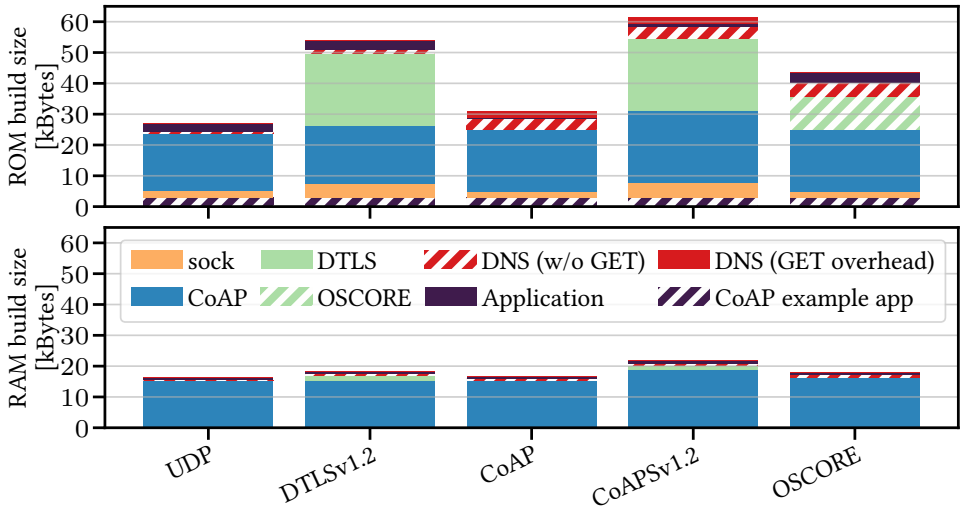
Experiment: Resolution Time & Packet Sizes



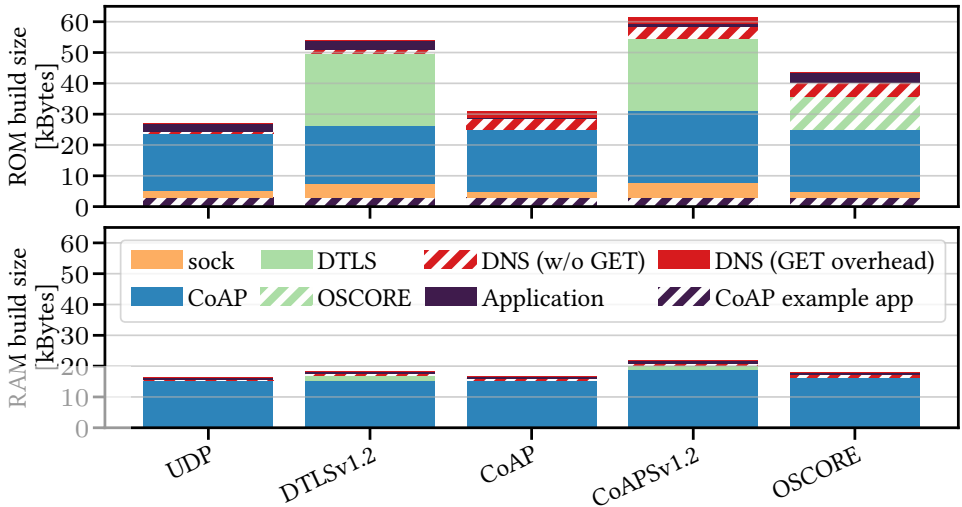


⇒ **Fragmentation has larger impact on performance** compared to transfer protocol or CoAP method

Memory Consumption



Memory Consumption



Outline

Motivation

CoAP: A Short Introduction

Design Guidance from IoT DNS Traffic

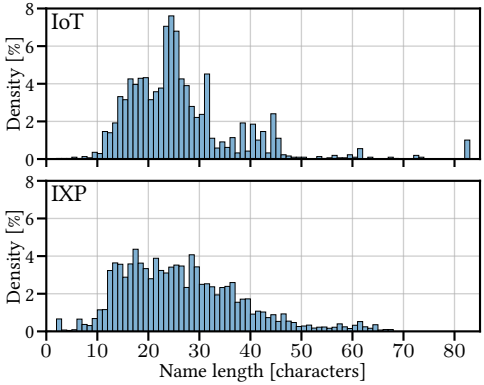
DNS over CoAP

Evaluation

Future Work: Concise DNS Message Representation

Conclusion

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

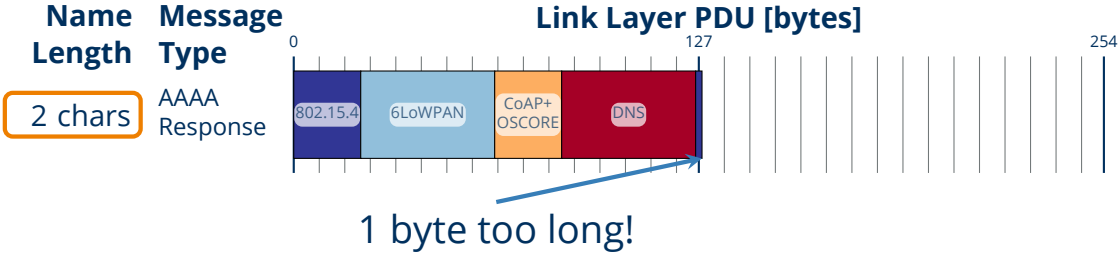
Future Work: Concise DNS Message Representation

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

Name Length	
2 chars	(minimum)

Future Work: Concise DNS Message Representation

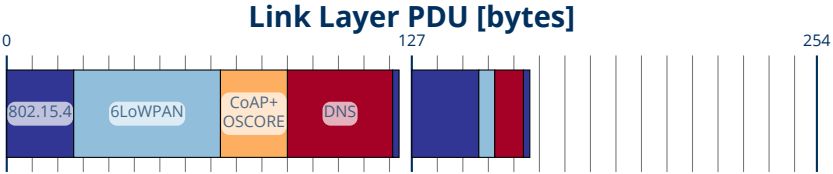
Constrained Networks, e.g., IEEE 802.15.4 with PDU of 127 bytes



Future Work: 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

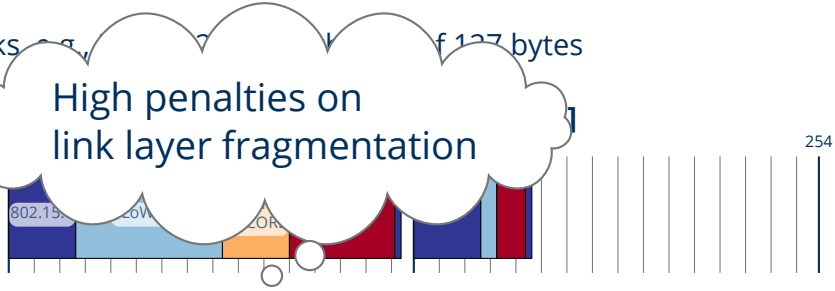


⇒ Fragmentation

Future Work: Concise DNS Message Representation

Constrained Networks, e.g., [illegible] of 127 bytes

Name Length	Message Type
2 chars	AAAA Response



⇒ Fragmentation

Future Work: Concise DNS Message Representation

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/`

Outline

Motivation

CoAP: A Short Introduction

Design Guidance from IoT DNS Traffic

DNS over CoAP

Evaluation

Future Work: Concise DNS Message Representation

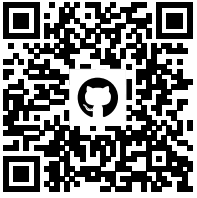
Conclusion

Conclusion & Next Steps

- DoC with FETCH provides encrypted DNS for constrained IoT
  - Segmentable with block-wise transfer
  - En-route caching at CoAP proxies
- En par in resolution time with existing UDP-based transfer protocols
- OSCORE outperforms DTLS and CoAPS both in packet and build size
- Next:
  - Concise 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



Backup slides

Outline

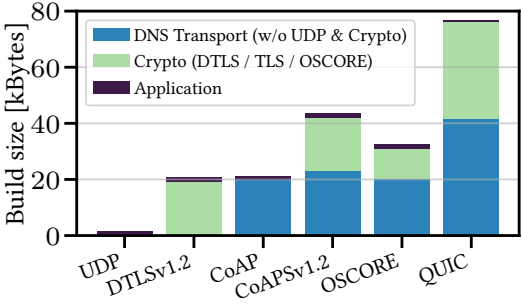
Comparison with QUIC

Evaluation: Caching Approaches

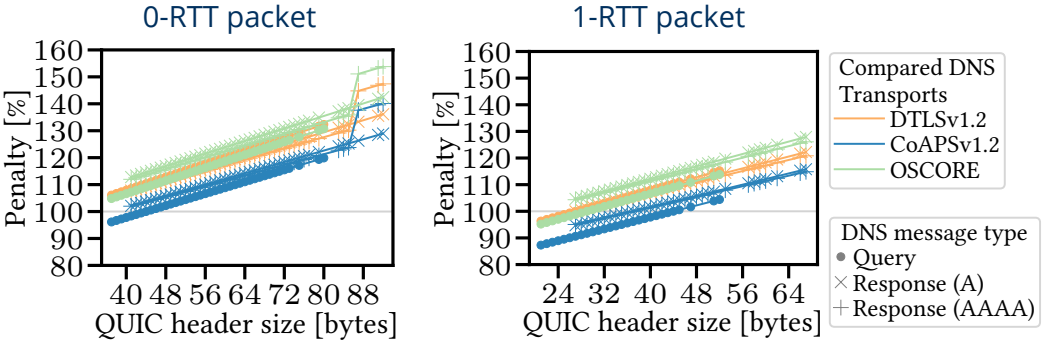
Comparison with QUIC: Method

- Point of Reference: QuantLars Eggert. 2020. Towards Securing the Internet of Things with QUIC. In *Proc. of 3rd NDSS Workshop on Decentralized IoT Systems and Security (DISS)* (San Diego, CA, USA). Internet Society (ISOC).
- Memory Size: Quant & our requester application build for ESP32
- Packet Size: Numerical evaluation based on RFC9000

Comparison with QUIC: Code Sizes



Comparison with QUIC: Additional Link Layer Data



Outline

Comparison with QUIC

Evaluation: Caching Approaches

Evaluation: Caching Approaches