DNS in Constrained Network Scenarios

DNS over CoAP & CBOR of DNS Messages

draft-ietf-core-dns-over-coap*

draft-lenders-dns-cbor†

---

*†**Martine S. Lenders**, *Christian Amsüss, †Carsten Bormann, *Cenk Gündoğan,
*†Thomas C. Schmidt, *†Matthias Wählisch

IETF 118, dnsop WG, Session II, 2023-11-10

Outline

Motivation

DNS over CoAP

CBOR Representation

Status

- draft-ietf-core-dns-over-coap
- draft-lenders-dns-cbor

Conclusion

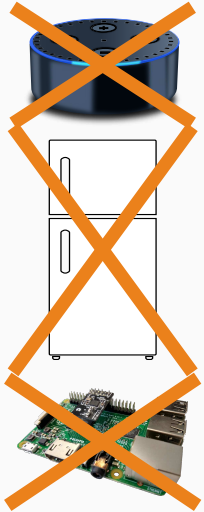
Motivation

Attack Scenario

Countermeasure

Encrypt name resolution triggered by IoT devices against eavesdropping

Challenge: Constrained IoT



Constrained nodes (RFC 7228):

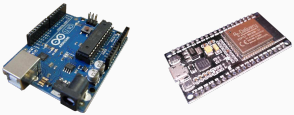
Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

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

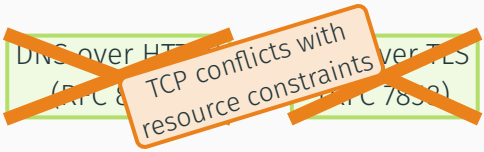
DNS over HTTPS (RFC 8484)

DNS over TLS (RFC 7858)

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

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** provides message segmentation
- **Share system resources** with CoAP applications on constrained devices
  - Same socket and buffers can be used
  - Re-use of the CoAP retransmission mechanism

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)

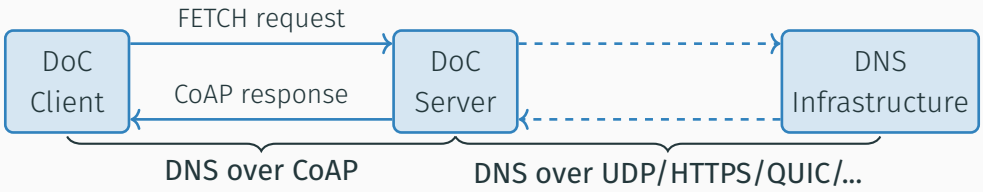
- Just map the DoH methods **GET** and **POST**?
- **FETCH** method in CoAP: best of both worlds (RFC 8132)

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

DNS over CoAP (DoC)

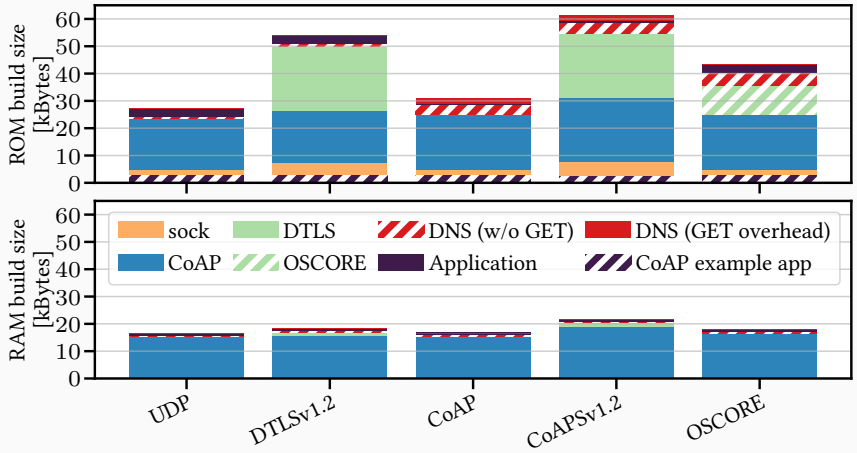
- Just map the DoH methods **GET** and **POST**?
- **FETCH** method in CoAP: best of both worlds (RFC 8132)

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



Evaluation: Memory Consumption

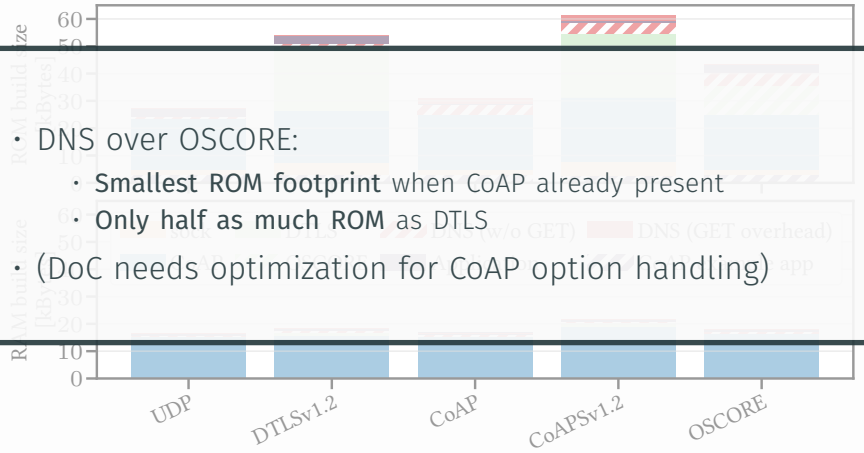
DNS Clients (+ CoAP application) for RIOT on Cortex-M3 microcontroller[1]



[1]M.S. Lenders, C. Amsüss, C. Gündogan, M. Nawrocki, T.C. Schmidt, M. Wählisch. 2023. **Securing Name Resolution in the IoT: DNS over CoAP**, in *PACMNET* 1, CoNEXT2, Article 6 (September 2023), 25 pages. https://doi.org/10.1145/3609423

Evaluation: Memory Consumption

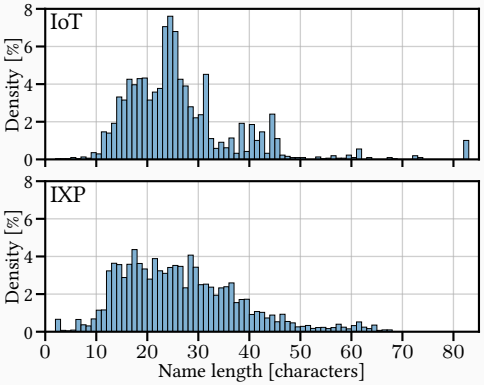
DNS Clients (+ CoAP application) for RIOT on Cortex-M3 microcontroller[1]



- DNS over OSCORE:
  - **Smallest ROM footprint** when CoAP already present
  - **Only half as much ROM** as DTLS
- (DoC needs optimization for CoAP option handling)

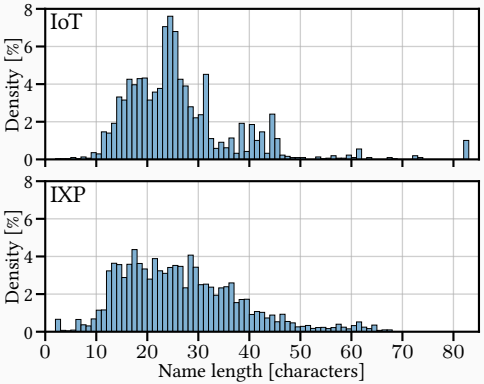
[1]M.S. Lenders, C. Amsüss, C. Gündogan, M. Nawrocki, T.C. Schmidt, M. Wählisch. 2023. **Securing Name Resolution in the IoT: DNS over CoAP**, in *PACMNET* 1, CoNEXT2, Article 6 (September 2023), 25 pages. https://doi.org/10.1145/3609423

DNS IoT Traffic: Name Lengths Based on Empirical Data



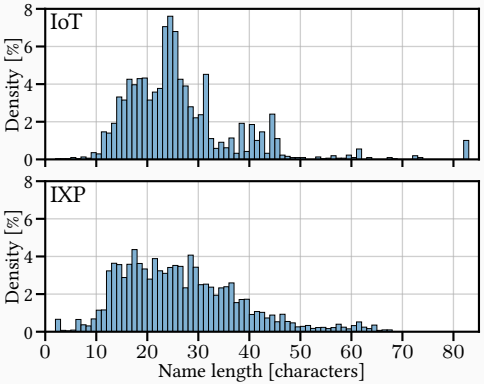
	Length of domain names [chars]							
Data set	min	max	mode	μ	σ	Q_1	Q_2	Q_3
YourThings	2	83	31	24.5	9.7	18	24	30
IoTFinder	7	82	24	26.8	10.5	20	24	30
MonIoTr	9	83	18	27.1	14.7	18	23	30
IoT total	2	83	24	25.9	1.3	19	24	30
IXP	0	68	17	26.1	1.7	17	25	33

DNS IoT Traffic: Name Lengths Based on Empirical Data



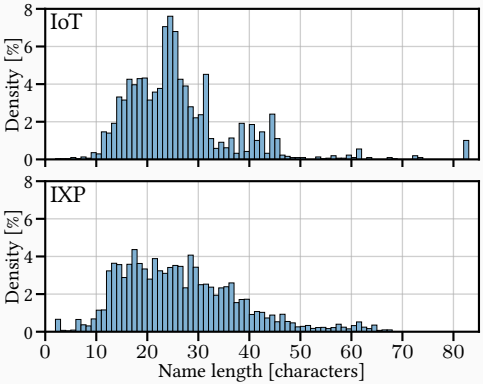
	Length of domain names [chars]							
Data set	min	max	mode	μ	σ	Q_1	Q_2	Q_3
YourThings	2	83	31	24.5	9.7	18	24	30
IoTFinder	7	82	24	26.8	10.5	20	24	30
MonIoTr	9	83	18	27.1	14.7	18	23	30
IoT total	2	83	24	25.9	1.3	19	24	30
IXP	0	68	17	26.1	1.7	17	25	33

DNS IoT Traffic: Name Lengths Based on Empirical Data



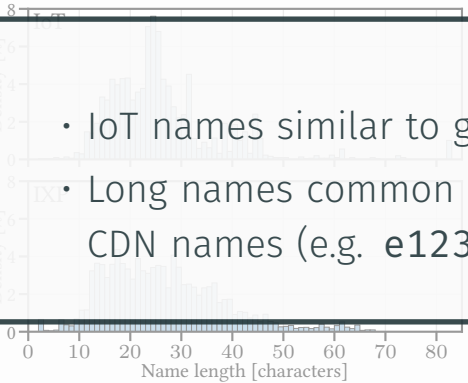
	Length of domain names [chars]							
Data set	min	max	mode	μ	σ	Q_1	Q_2	Q_3
YourThings	2	83	31	24.5	9.7	18	24	30
IoTFinder	7	82	24	26.8	10.5	20	24	30
MonIoTr	9	83	18	27.1	14.7	18	23	30
IoT total	2	83	24	25.9	1.3	19	24	30
IXP	0	68	17	26.1	1.7	17	25	33

DNS IoT Traffic: Name Lengths Based on Empirical Data



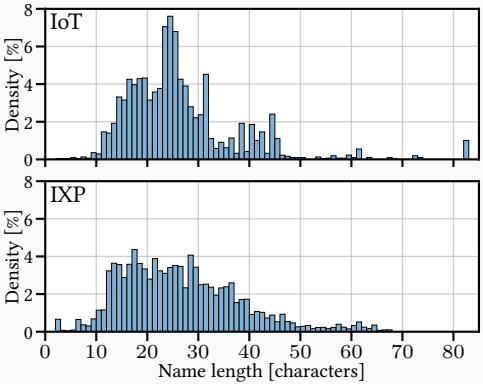
	Length of domain names [chars]							
Data set	min	max	mode	μ	σ	Q_1	Q_2	Q_3
YourThings	2	83	31	24.5	9.7	18	24	30
IoTFinder	7	82	24	26.8	10.5	20	24	30
MonIoTr	9	83	18	27.1	14.7	18	23	30
IoT total	2	83	24	25.9	1.3	19	24	30
IXP	0	68	17	26.1	1.7	17	25	33

DNS IoT Traffic: Name Lengths Based on Empirical Data



- 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: Name Lengths Based on Empirical Data



	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

Packet Size for Empirical Name Lengths

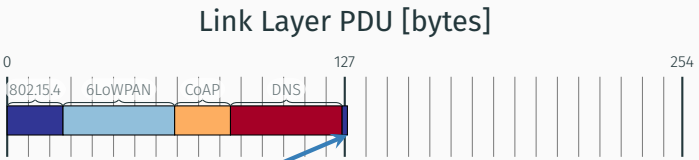
Constrained Networks, e.g., IEEE 802.15.4 with PDU of 127 bytes

Name Length	
2 chars	(minimum)

Packet Size for Empirical Name Lengths

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

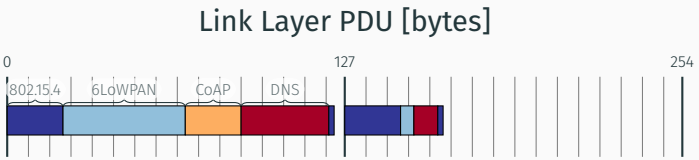
Name Length	Message Type
2 chars	AAAA Response



Packet Size for Empirical Name Lengths

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

Name Length	Message Type
2 chars	AAAA Response



⇒ Fragmentation

Packet Size for Empirical Name Lengths

Constrained Networks, e.g., IEEE 15 DU 27 bytes

Name Length	Messa Type
2 chars	AAAA Response

⇒ Fragmentation

Packet Size for Empirical Name Lengths

C

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/`

draft-ietf-core-dns-over-coap

- First presented in CoRE WG at IETF 113
- CoRE WG work mostly done, waiting for more implementations
- Still ongoing discussion: Bootstrapping DoC in SVCB records
  - ALPN ID for CoAP over DTLS missing
  - SVCB with OSCORE/EDHOC completely unspecified
  - However: SVCB of large interest to CoRE WG in general
    (e.g. to reduce growing number of coap+...:// URI schemata)
  - Plan: publish problem statement document that will be referenced by DoC draft

draft-lenders-dns-cbor

- First presented in CBOR WG at IETF 115
- Ongoing discussions & TBD:
  - Which CBOR-packed method should be used for name compression?
  - Allow for >1 question in messages?

Conclusion

- DNS over CoAP is needed!
  - DNS over UDP conflicts with privacy requirements
  - DNS over HTTPS/TLS/QUIC/DTLS conflicts with resource constraints
- En par in performance with existing (UDP-based) transfer protocols
  - Advantage in packet size and memory consumption over other encrypted transfer protocols
- CBOR-based message format to avoid expensive fragmentation
- Reference implementations in Python and for the embedded OS RIOT

Backup slides

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.