Martine S. Lenders TU Dresden and FU Berlin, Germany
Christian Amsüss Unaffiliated, Vienna, Austria
Cenk Gündogan Huawei Technologies, Munich, Germany
Marcin Nawrocki FU Berlin, Germany, and NETSCOUT, Berkeley, CA, USA
Thomas C. Schmidt HAW Hamburg, Germany
Matthias Wählisch TU Dresden and Barkhausen Institut, Dresden, Germany

Securing Name Resolution in the IoT: DNS over CoAP

Paris, ACM CoNEXT'23, 2023-12-05

Contact: martine.lenders@tu-dresden.de

Outline

Motivation

A Brief Introduction into CoAP

Design Guidance from IoT DNS Traffic

DNS over CoAP

Evaluation

Further Improvements

Conclusion & Future Work

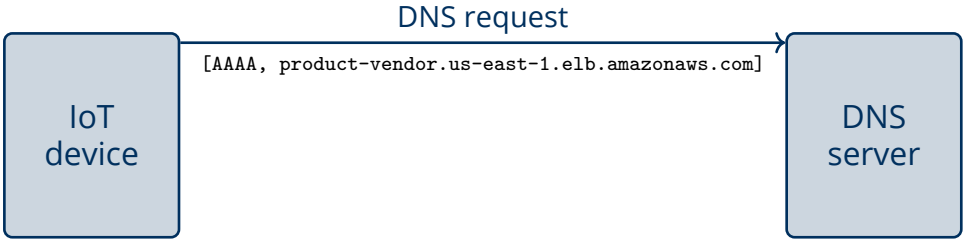
Outline

Motivation

Attack Scenario: Name resolution by IoT devices

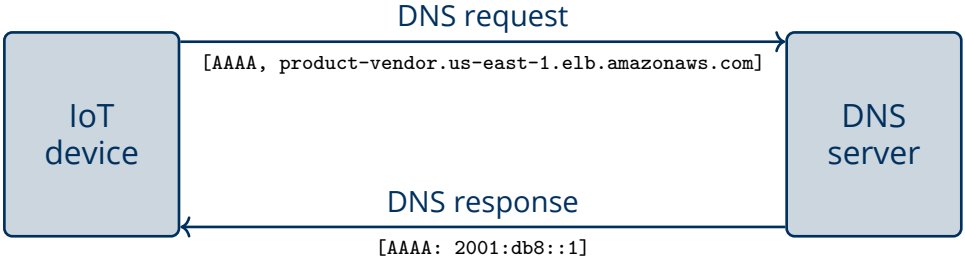
Motivation

Attack Scenario: Name resolution by IoT devices



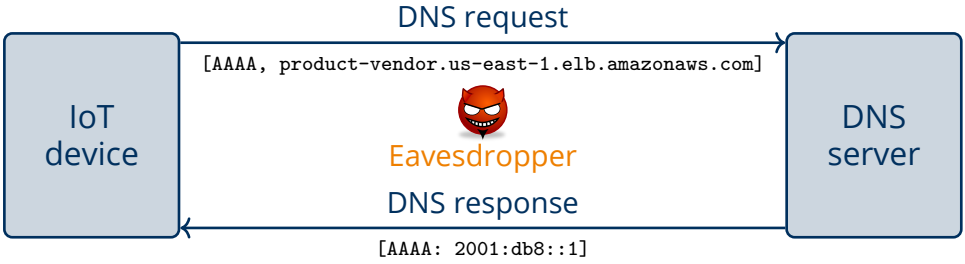
Motivation

Attack Scenario: Name resolution by IoT devices



Motivation

Attack Scenario: Name resolution by IoT devices

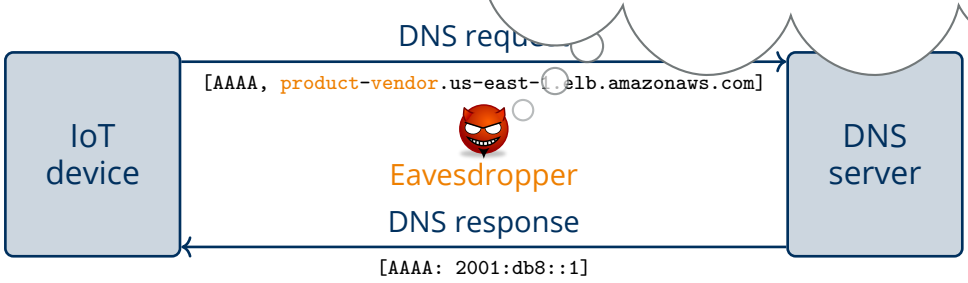


Motivation

Attack Scenario: Name resol

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=product+vendor

Name	Description
CVE-2019-XXXXX	Vendor Product are affected by a stack-based buffer overflow by an unauthenticated attacker which allows for **remote code execution.**
CVE-2023-YYYYY	Vendor Product ...

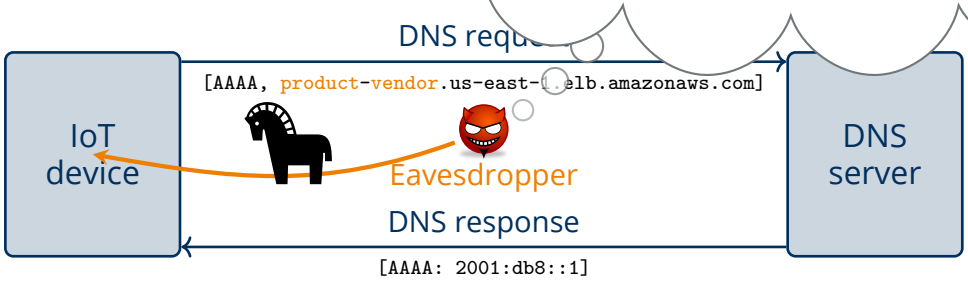


Motivation

Attack Scenario: Name resol

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=product+vendor

Name	Description
CVE-2019-XXXXX	Vendor Product are affected by a stack-based buffer overflow by an unauthenticated attacker which allows for **remote code execution.**
CVE-2023-YYYYY	Vendor Product ...

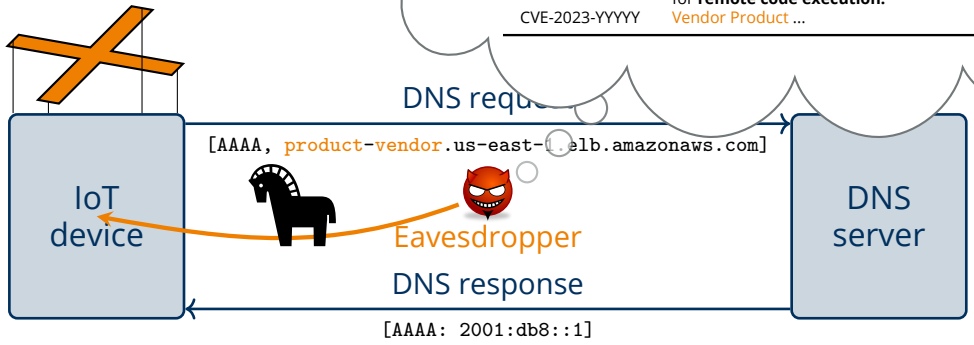


Motivation

Attack Scenario: Name resol

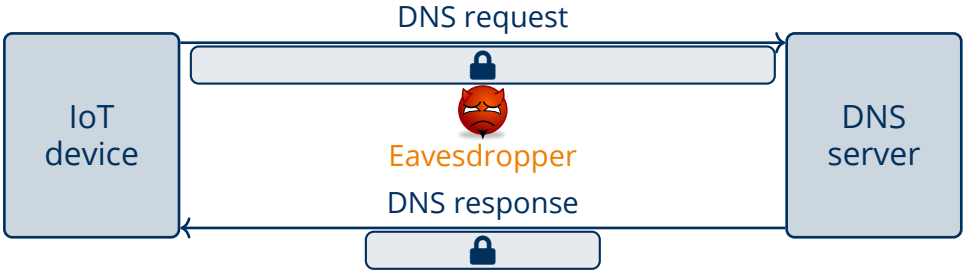
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=product+vendor

Name	Description
CVE-2019-XXXXX	Vendor Product are affected by a stack-based buffer overflow by an unauthenticated attacker which allows for **remote code execution.**
CVE-2023-YYYYY	Vendor Product ...



Motivation

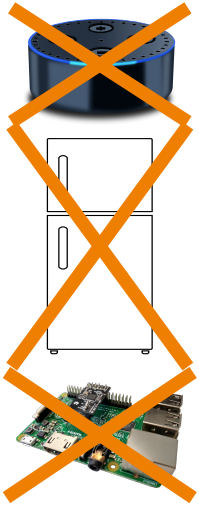
Attack Scenario: Name resolution by IoT devices



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

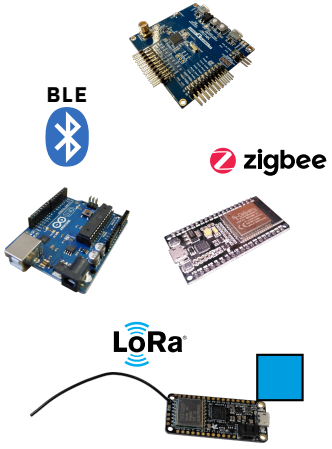
Constrained nodes (RFC 7228):

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)

Challenge: Constrained IoT



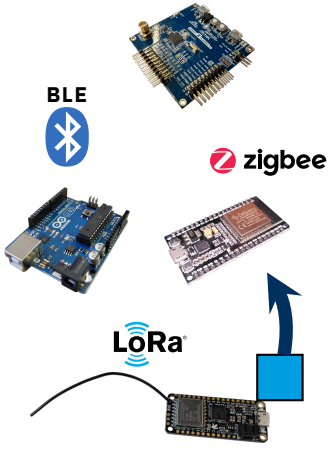
Constrained nodes (RFC 7228):

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



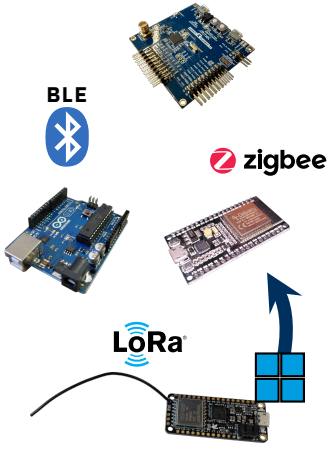
Constrained nodes (RFC 7228):

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



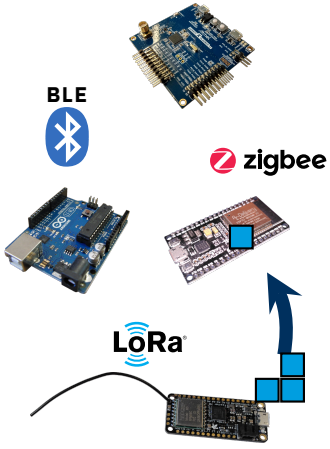
Constrained nodes (RFC 7228):

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



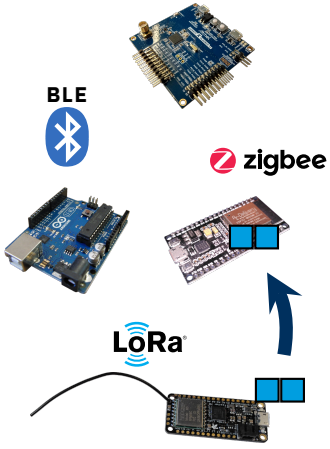
Constrained nodes (RFC 7228):

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



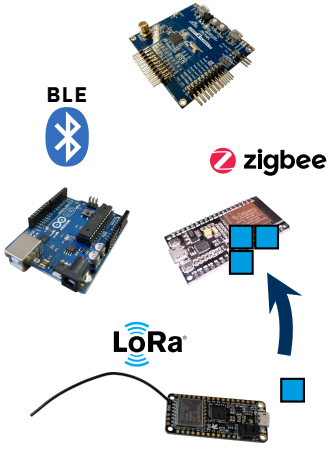
Constrained nodes (RFC 7228):

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



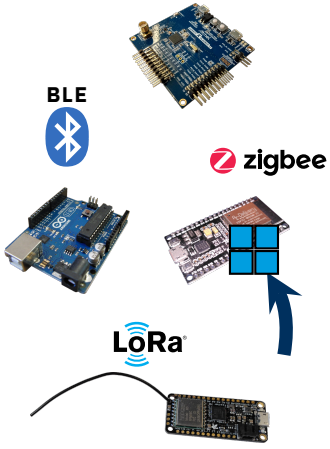
Constrained nodes (RFC 7228):

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



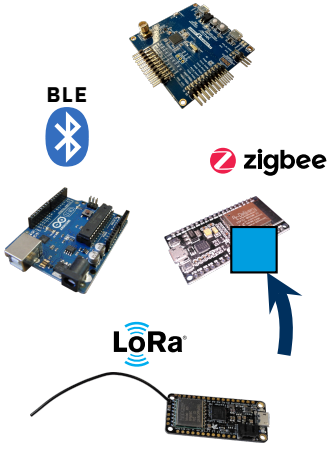
Constrained nodes (RFC 7228):

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



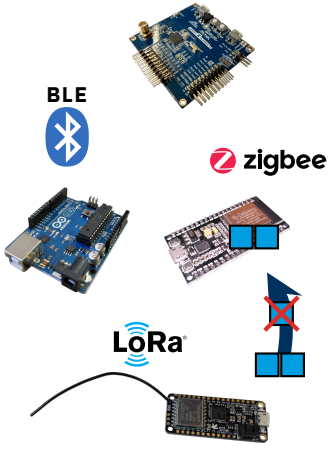
Constrained nodes (RFC 7228):

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



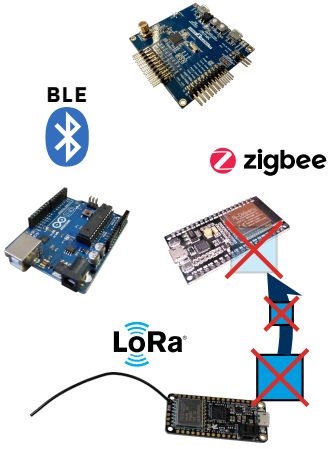
Constrained nodes (RFC 7228):

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



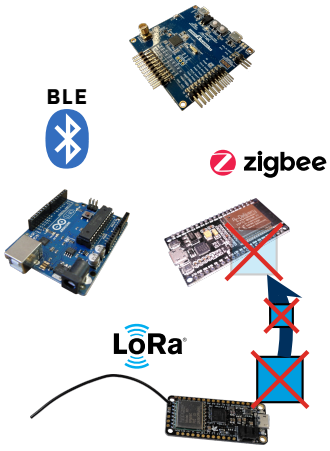
Constrained nodes (RFC 7228):

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



Constrained nodes (RFC 7228):

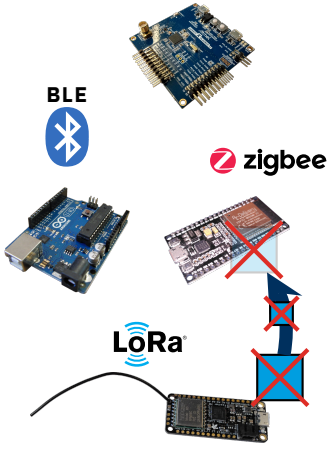
Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

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



Constrained nodes (RFC 7228):

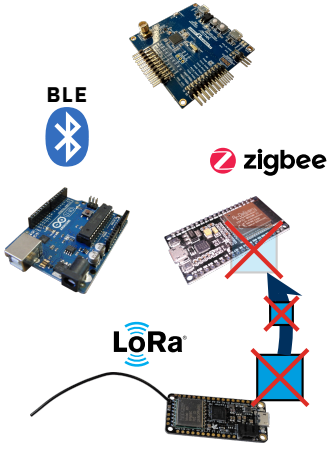
Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

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



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 characteristics
- High penalties on large packets (link la… …fragmentation)

0.000003% – 0.0009%
slower than WiFi 6

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)

Possible Solutions for Encrypted DNS

DNS over HTTPS (RFC 8484)

DNS over TLS (RFC 7858)

DNS over QUIC (RFC 9250)

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)

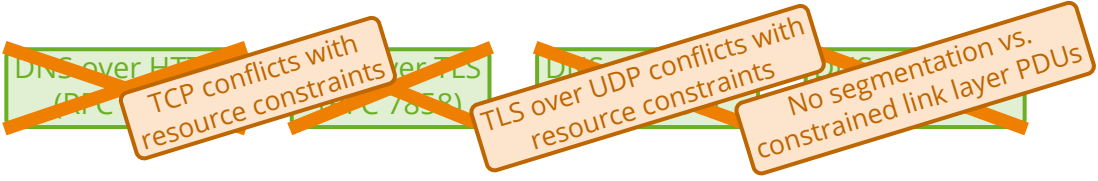
Possible Solutions for Encrypted DNS

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** provides message segmentation
- **En-route caching** mitigates high link layer packet loss
- **Share system resources** with CoAP applications
  - Same socket and buffers can be used
  - Re-use of the CoAP retransmission mechanism

Outline

Motivation

A Brief Introduction into CoAP

Design Guidance from IoT DNS Traffic

DNS over CoAP

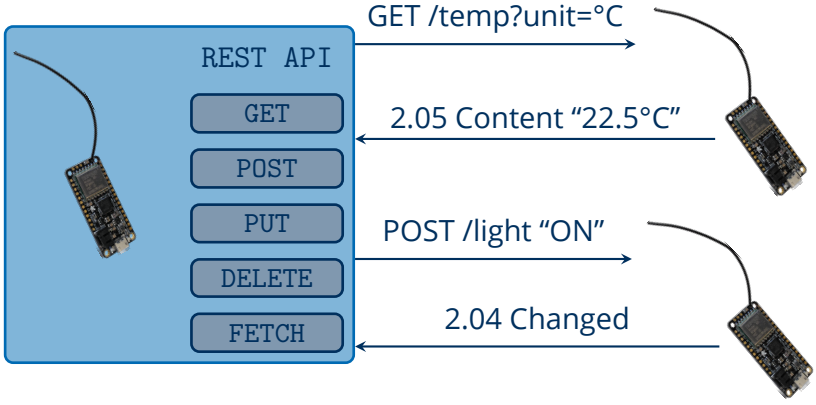
Evaluation

Further Improvements

Conclusion & Future Work

CoAP: The Constrained Application Protocol

“REST over UDP” ∼ The HTTP for IoT



CoAP Security Modes

DTLS Datagram Transport Layer Security (≈ TLS over UDP)

CoAP Security Modes

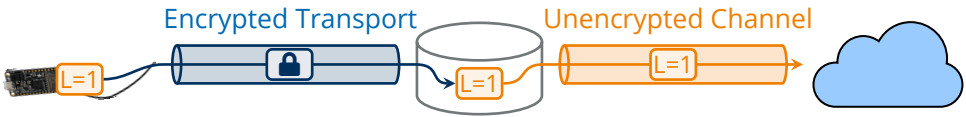
DTLS Datagram Transport Layer Security (≈ TLS over UDP)

CoAP Security Modes

DTLS Datagram Transport Layer Security (≈ TLS over UDP)

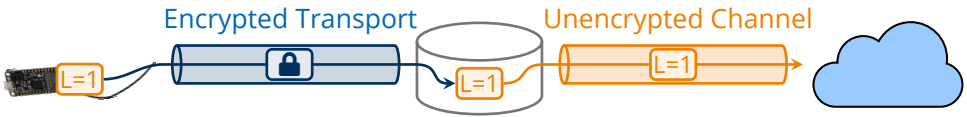
CoAP Security Modes

DTLS Datagram Transport Layer Security (≈ TLS over UDP)



CoAP Security Modes

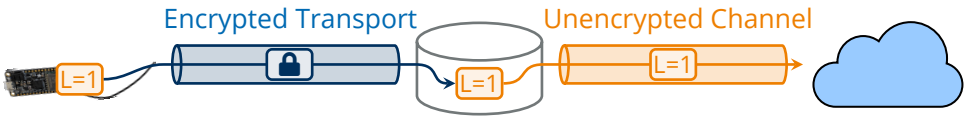
DTLS Datagram Transport Layer Security (≈ TLS over UDP)



OSCORE Object Security for Constrained RESTful Environment

CoAP Security Modes

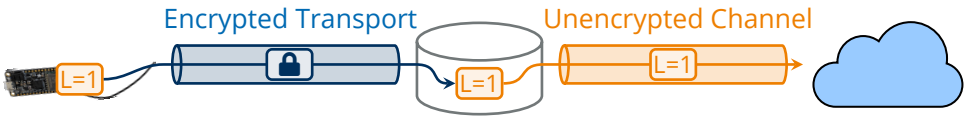
DTLS Datagram Transport Layer Security (≈ TLS over UDP)



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

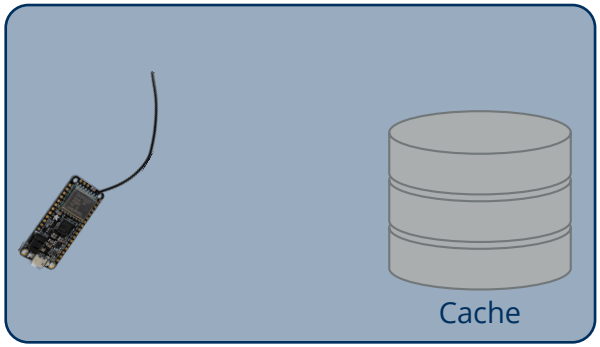
CoAP Caching

Client

Cache

Server

CoAP Caching

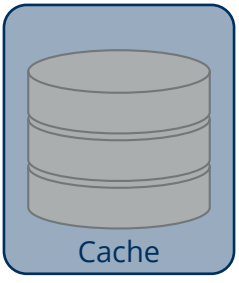


On client node

Server

CoAP Caching

Client

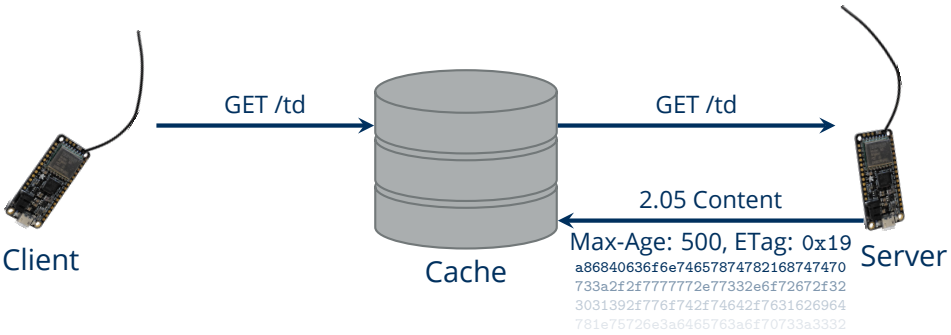


On proxy node

Server

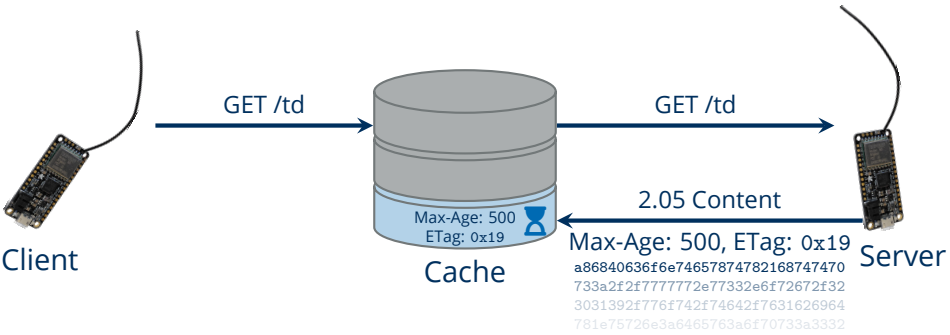
CoAP Caching

Caching provides **decoupling from packet loss**



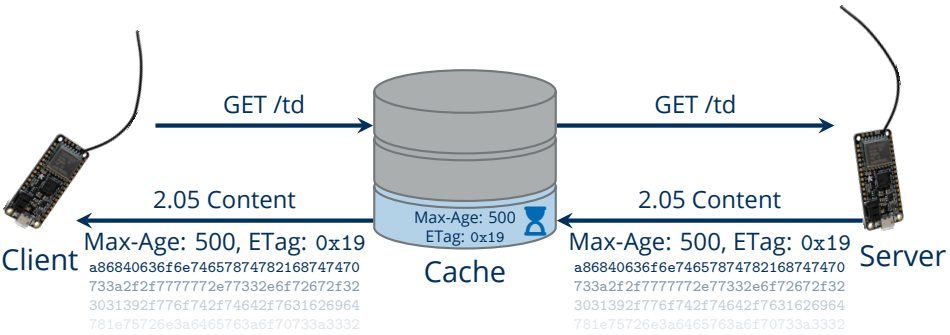
CoAP Caching

Caching provides **decoupling from packet loss**



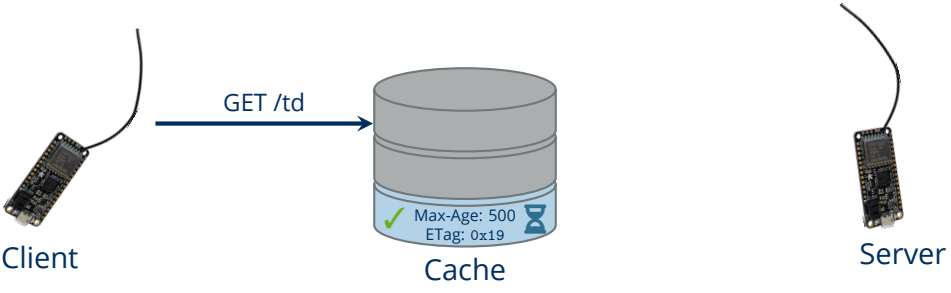
CoAP Caching

Caching provides **decoupling from packet loss**



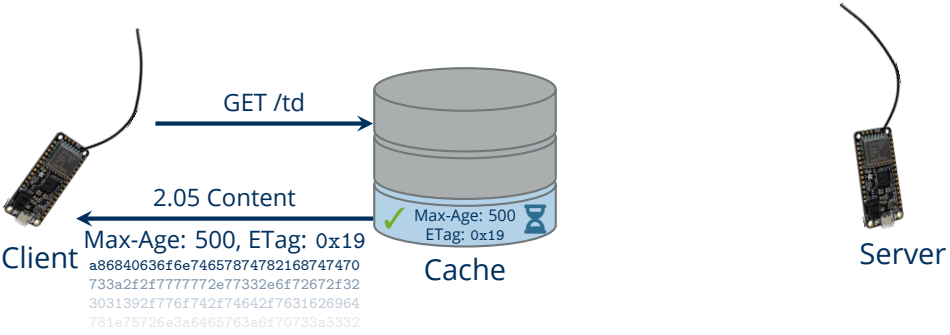
CoAP Caching

Caching provides **decoupling from packet loss**



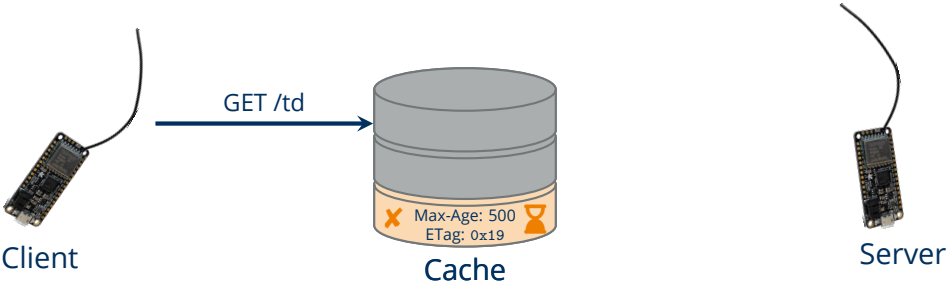
CoAP Caching

Caching provides **decoupling from packet loss**



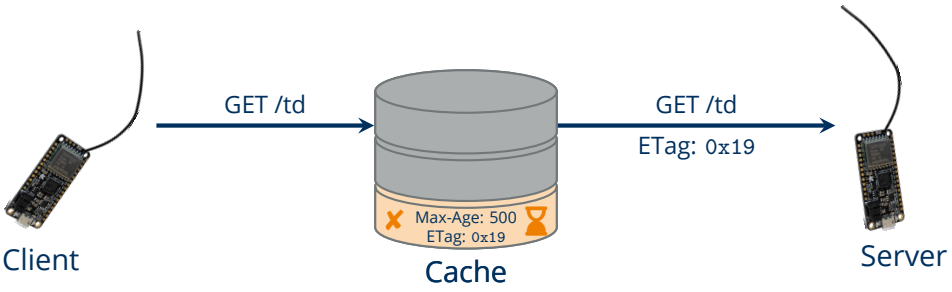
CoAP Caching

What if cache entry goes stale?



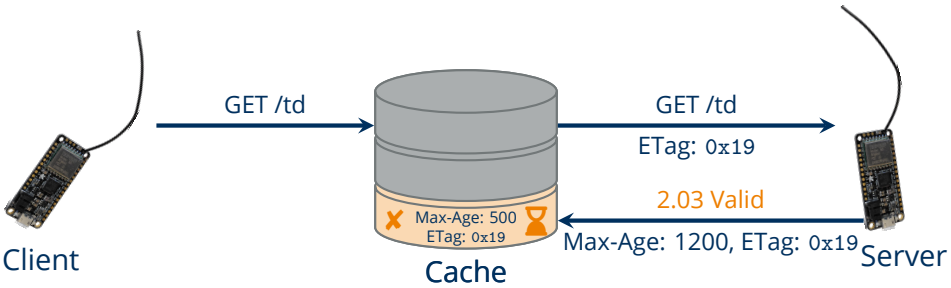
CoAP Caching

What if cache entry goes stale?



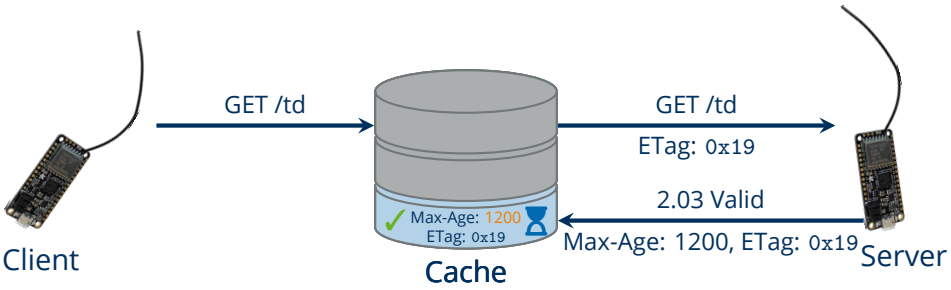
CoAP Caching

Cache validation **reduces data overhead**



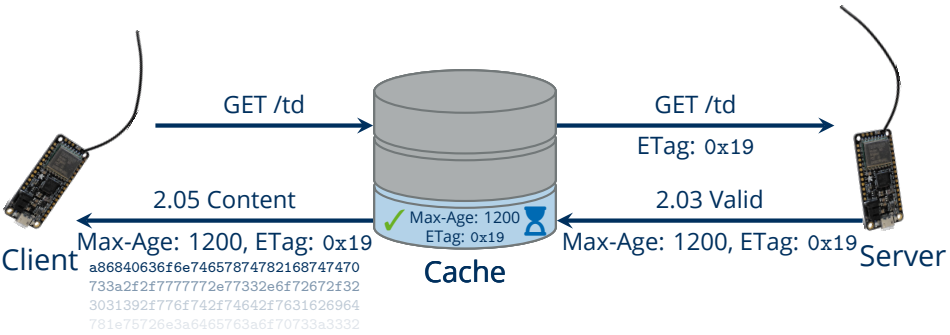
CoAP Caching

Cache validation **reduces data overhead**



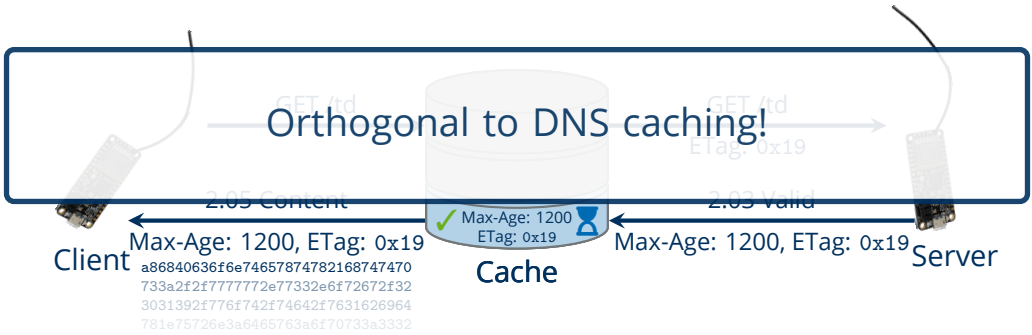
CoAP Caching

Cache validation **reduces data overhead**



CoAP Caching

Cache validation **reduces data overhead**



Outline

Motivation

A Brief Introduction into CoAP

Design Guidance from IoT DNS Traffic

DNS over CoAP

Evaluation

Further Improvements

Conclusion & Future Work

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

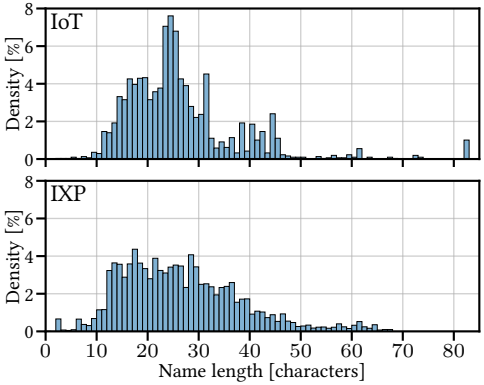
- Large Central European IXP
- Collected January 2022
- DNS only
- Sampling rate: 1/16000 pkts.
- 1.6 million queries
- 2.4 million responses
- Names anonymized to lengths

[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.

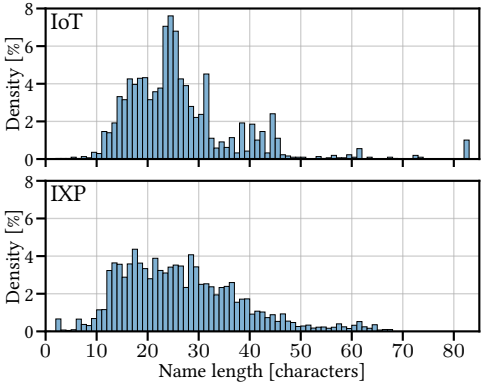
[3] J. Ren, D.J. Dubois, D. Choffnes, A.M. Mandalari, R. Kolcun, and H. Haddadi. 2019. **Information Exposure for Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach**. In *Proc. of the Internet Measurement Conference (IMC)*. ACM.

DNS IoT Traffic: Name Lengths



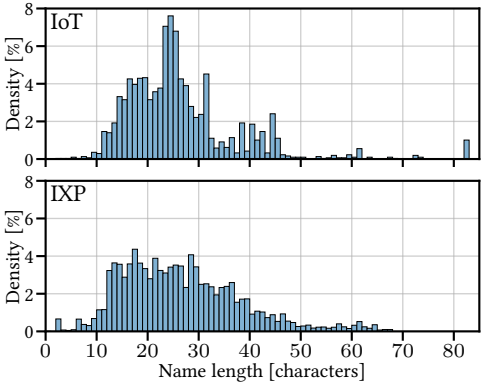
	Length of domain names [chars]				
Data set	Min	Max	Mean	Std. Dev.	Median
YourThings	2	83	24.5	9.7	24
IoTFinder	7	82	26.8	10.5	24
MonIoTr	9	83	27.1	14.7	23
IoT total	2	83	25.9	1.3	24
IXP	0	68	26.1	1.7	25

DNS IoT Traffic: Name Lengths



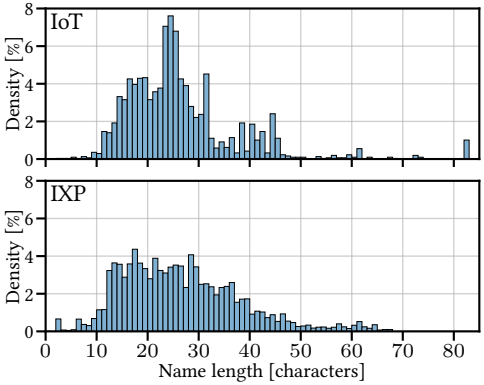
	Length of domain names [chars]				
Data set	Min	Max	Mean	Std. Dev.	Median
YourThings	2	83	24.5	9.7	24
IoTFinder	7	82	26.8	10.5	24
MonIoTr	9	83	27.1	14.7	23
IoT total	2	83	25.9	1.3	24
IXP	0	68	26.1	1.7	25

DNS IoT Traffic: Name Lengths



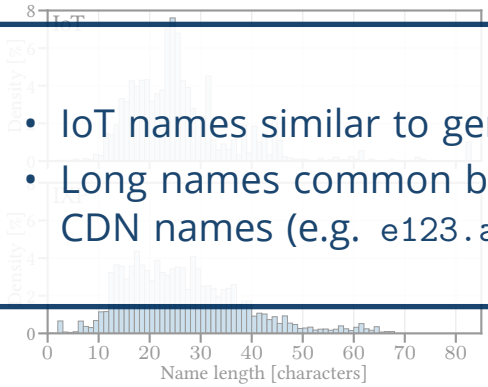
	Length of domain names [chars]				
Data set	Min	Max	Mean	Std. Dev.	Median
YourThings	2	83	24.5	9.7	24
IoTFinder	7	82	26.8	10.5	24
MonIoTr	9	83	27.1	14.7	23
IoT total	2	83	25.9	1.3	24
IXP	0	68	26.1	1.7	25

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

Queried Record Type	IoT Devices w/ mDNS	IoT Devices w/o mDNS	IXP
AAAA	16.4%	23.5%	17.6%
A	8.2%	—	1.7%
PTR	—	—	9.1%
NS	—	—	0.7%
SRV	1.5%	—	1.8%
HTTPS	—	—	0.4%
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
  $\Rightarrow$ Should be avoided with DoC

Also service discovery & information

Outline

Motivation

A Brief Introduction into CoAP

Design Guidance from IoT DNS Traffic

DNS over CoAP

Evaluation

Further Improvements

Conclusion & Future Work

DNS over CoAP (DoC)

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

DNS over CoAP (DoC)

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

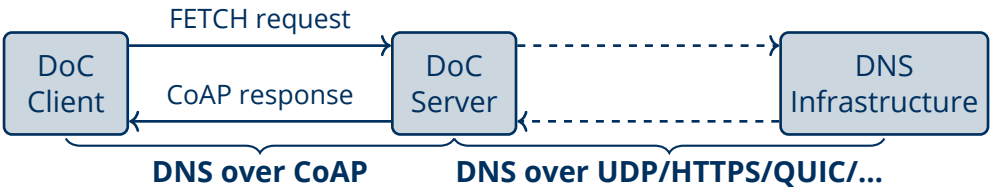
	HTTP	
	GET	POST
Responses cacheable	✓	✗
Application data carried in body	✗	✓
Block-wise transferable query	✗	✓

DNS over CoAP (DoC)

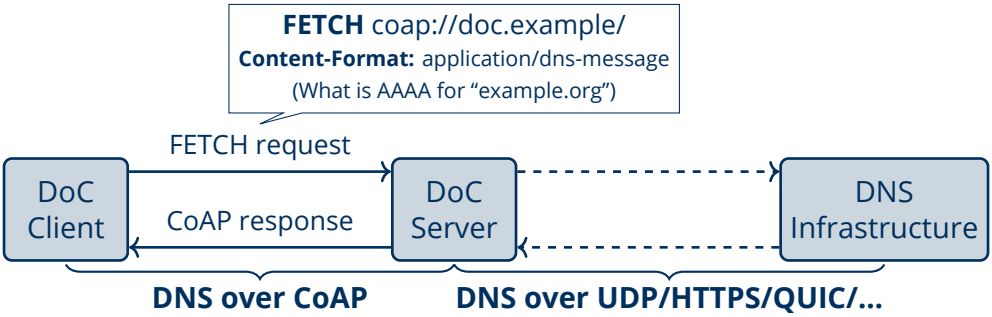
- Just map the DoH methods **GET** and **POST**?
- **FETCH** method in CoAP: best of both worlds (RFC 8132)

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

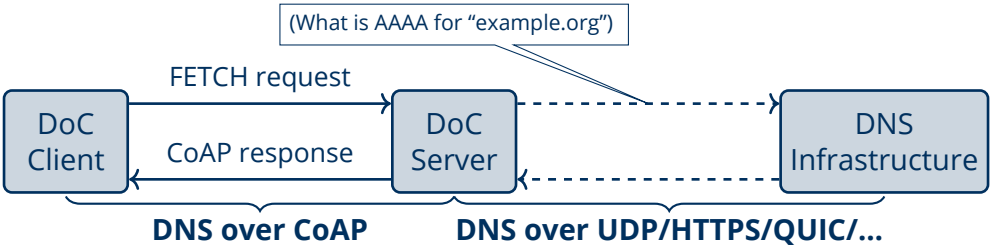
DNS over CoAP (DoC): Example Query



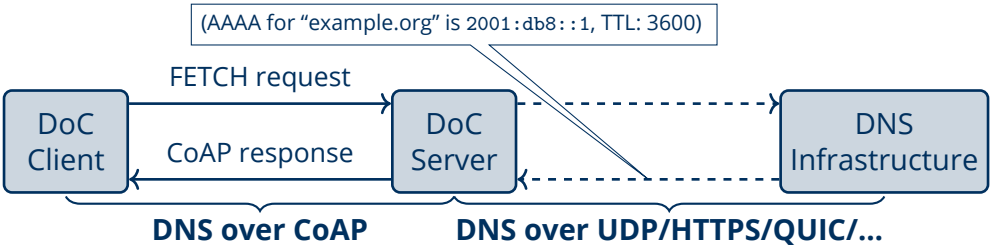
DNS over CoAP (DoC): Example Query



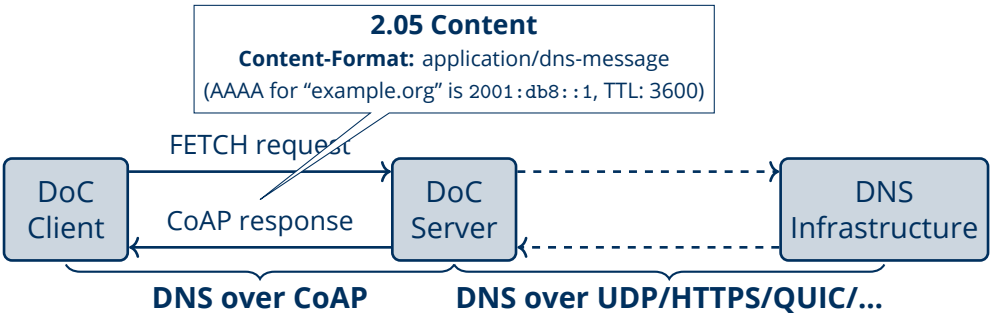
DNS over CoAP (DoC): Example Query



DNS over CoAP (DoC): Example Query



DNS over CoAP (DoC): Example Query



Outline

Motivation

A Brief Introduction into CoAP

Design Guidance from IoT DNS Traffic

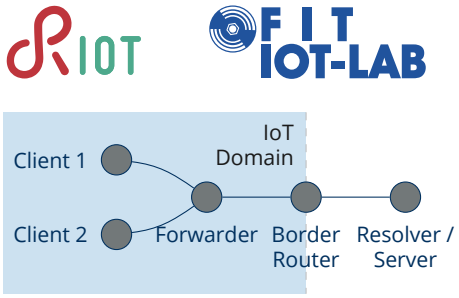
DNS over CoAP

Evaluation

Further Improvements

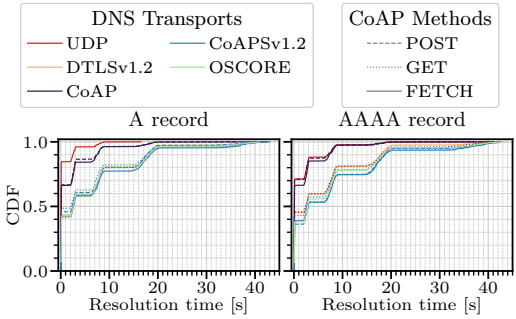
Conclusion & Future Work

Evaluation Setup: DNS Transfer Protocol Comparison

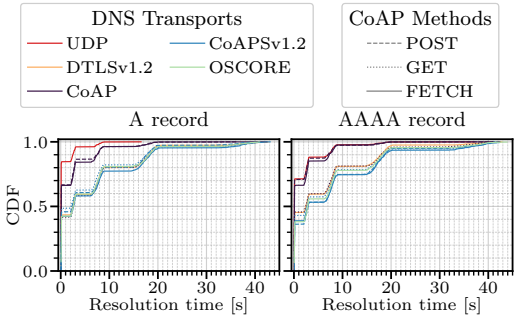


- Client 1 and 2 query records for names of length 24 chars (median of IoT data) via
  - UDP
  - DTLSv1.2
  - CoAP (unencrypted)
  - CoAPSv1.2 (CoAP over DTLSv1.2)
  - OSCORE
- 50 A and AAAA records each (most in IoT data)
- Poisson distribution: $\lambda = 5$ queries / sec
- 10 runs on IoT-nodes (incl. border router): Cortex-M3 with IEEE 802.15.4 radio

Experiment: Resolution Time

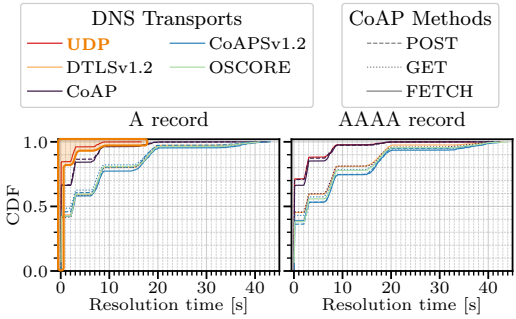


Experiment: Resolution Time



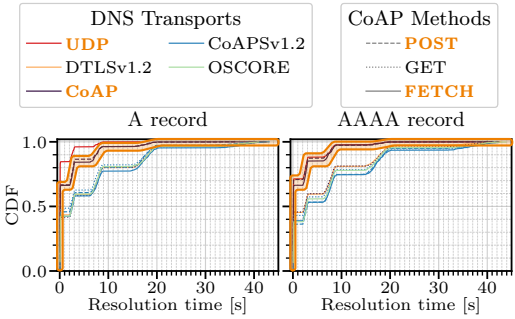
Clear performance groups visible

Experiment: Resolution Time



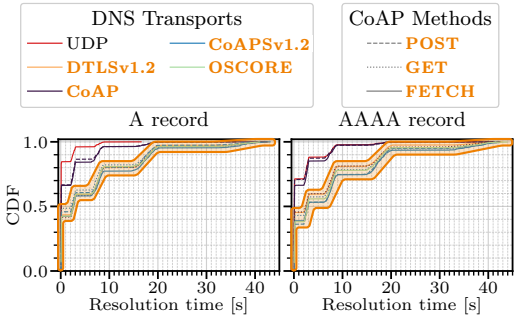
Group 1

Experiment: Resolution Time



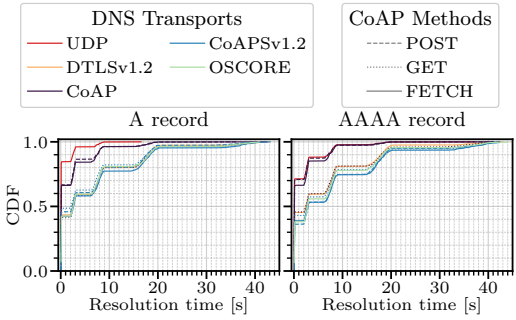
Group 2

Experiment: Resolution Time



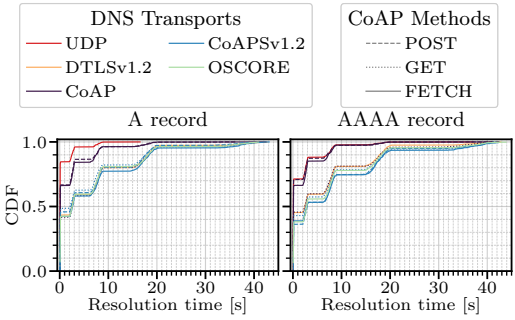
Group 3

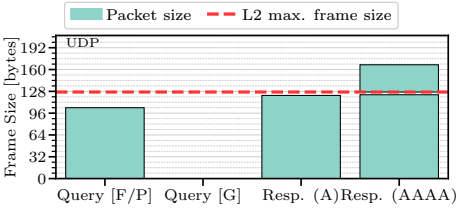
Experiment: Resolution Time



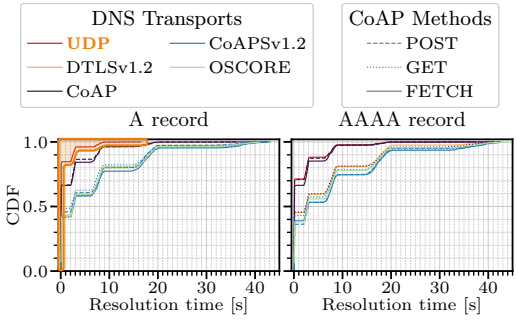
Where do performance groups come from?

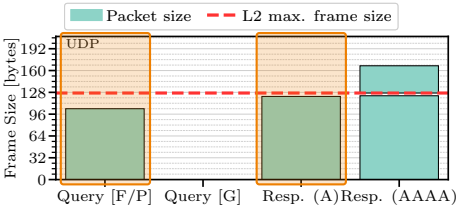
Experiment: Resolution Time & Packet Sizes





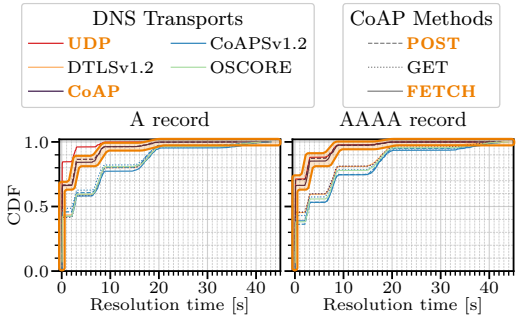
Experiment: Resolution Time & Packet Sizes

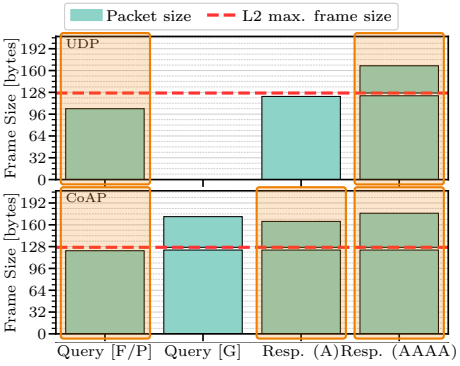




Group 1
No message fragmentation

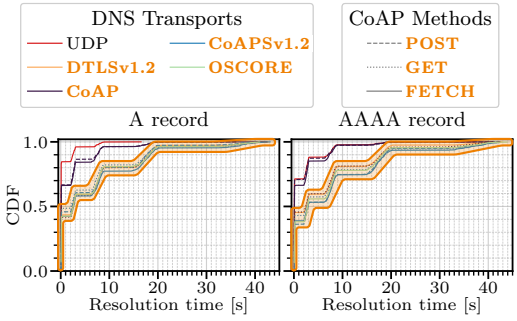
Experiment: Resolution Time & Packet Sizes

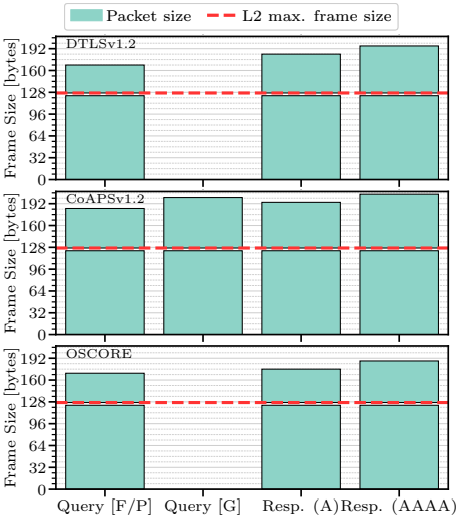




Group 2
Query unfragmented
Response fragmented

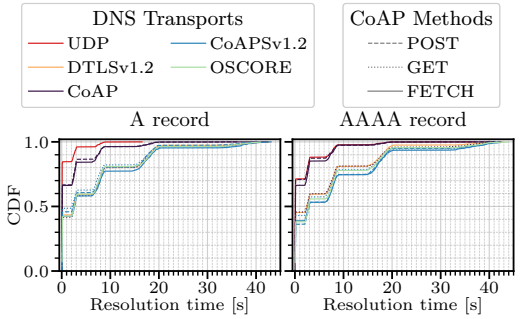
Experiment: Resolution Time & Packet Sizes

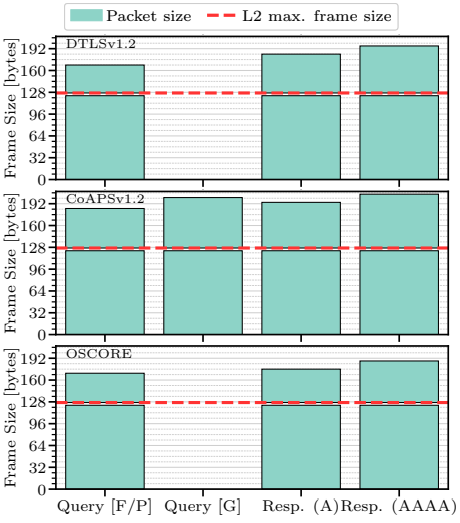




Group 3
Both messages fragmented

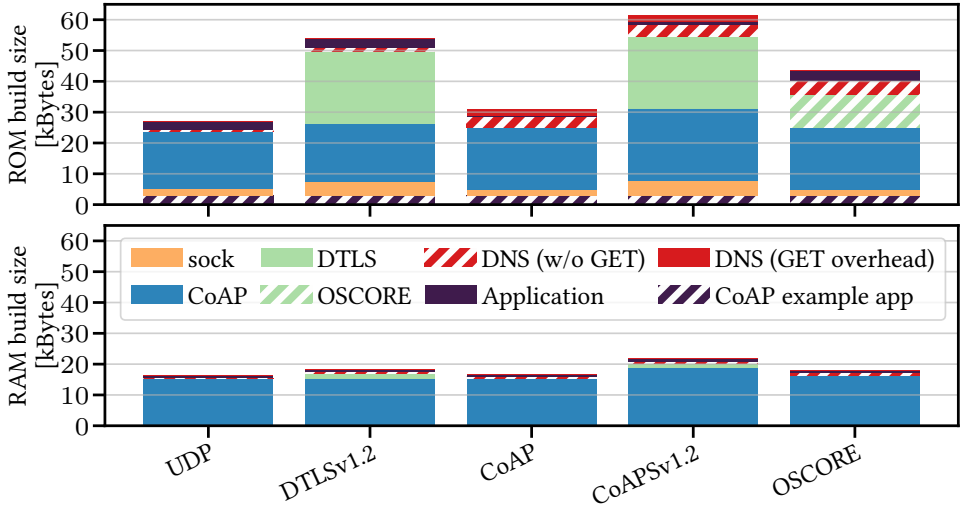
Experiment: Resolution Time & Packet Sizes



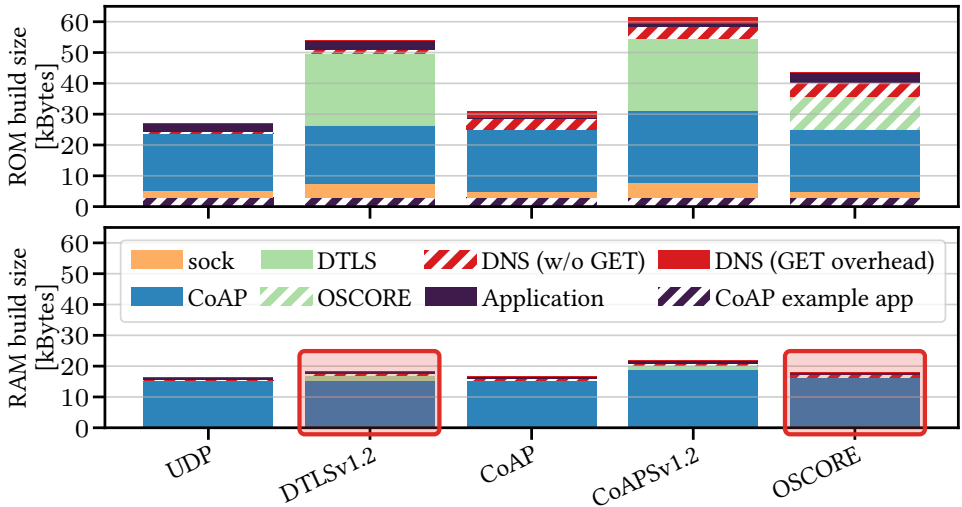


⇒ **Fragmentation has larger impact on performance** compared to transfer protocol or CoAP method

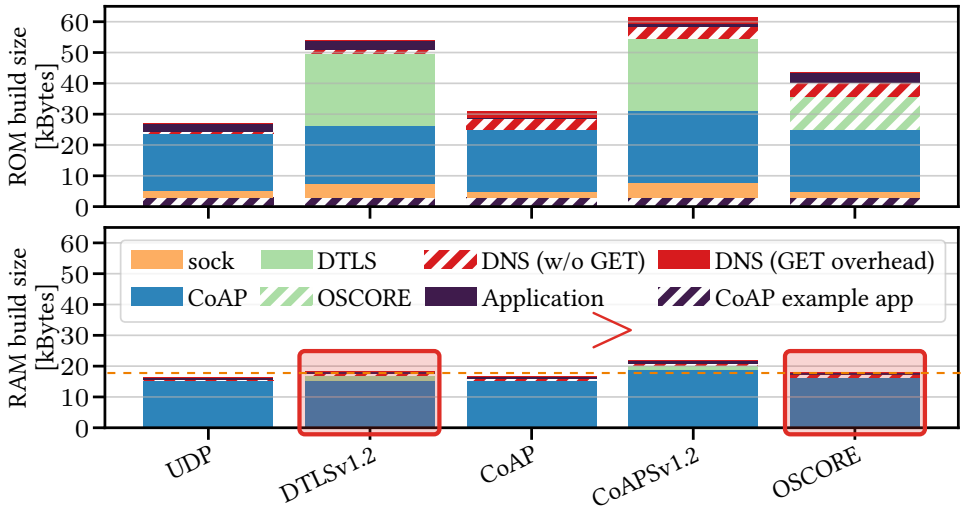
Memory Consumption



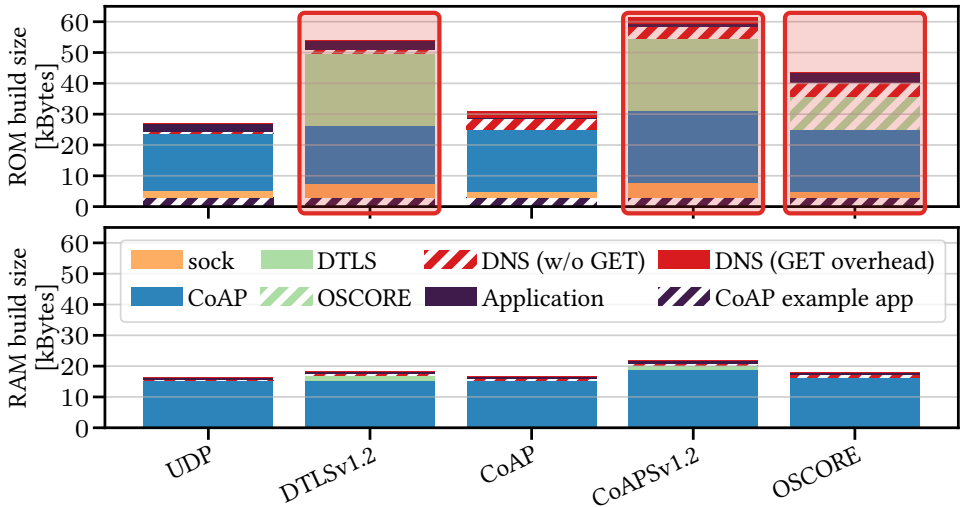
Memory Consumption



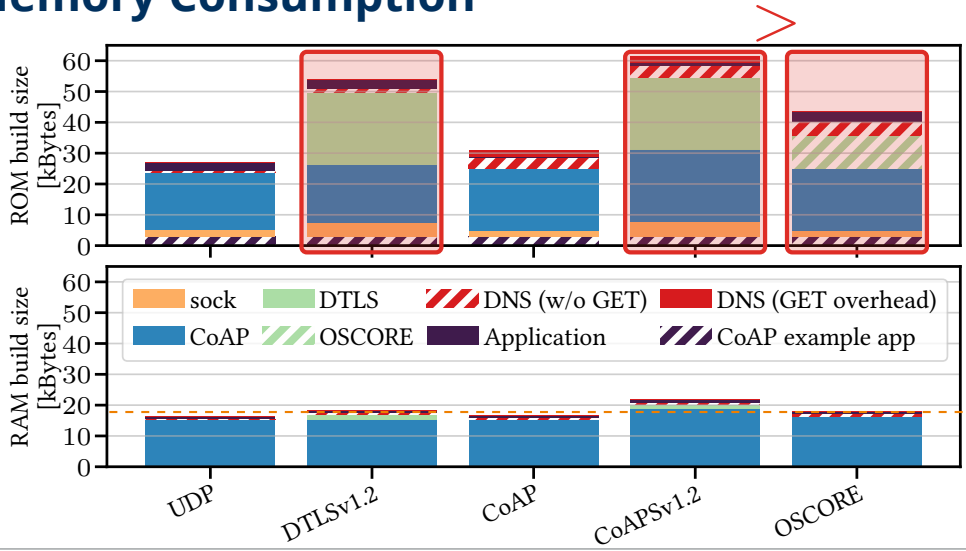
Memory Consumption



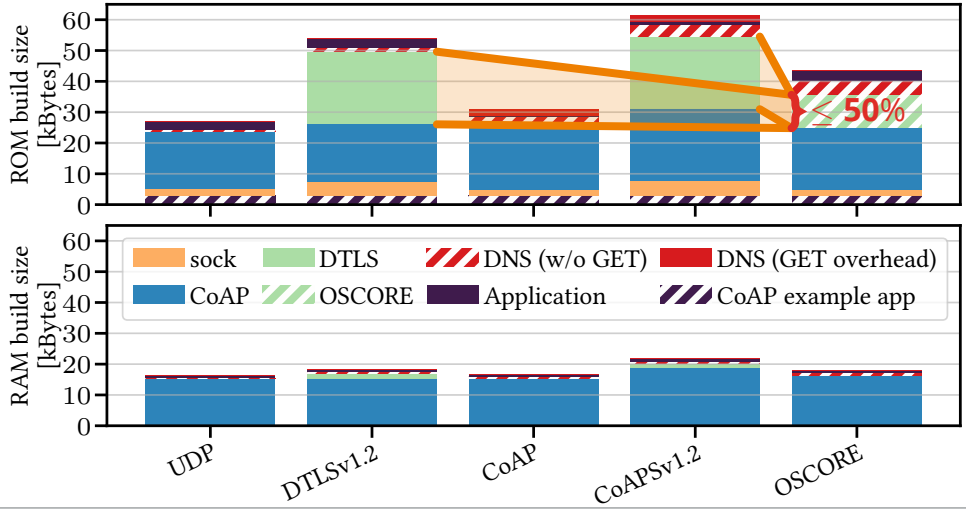
Memory Consumption



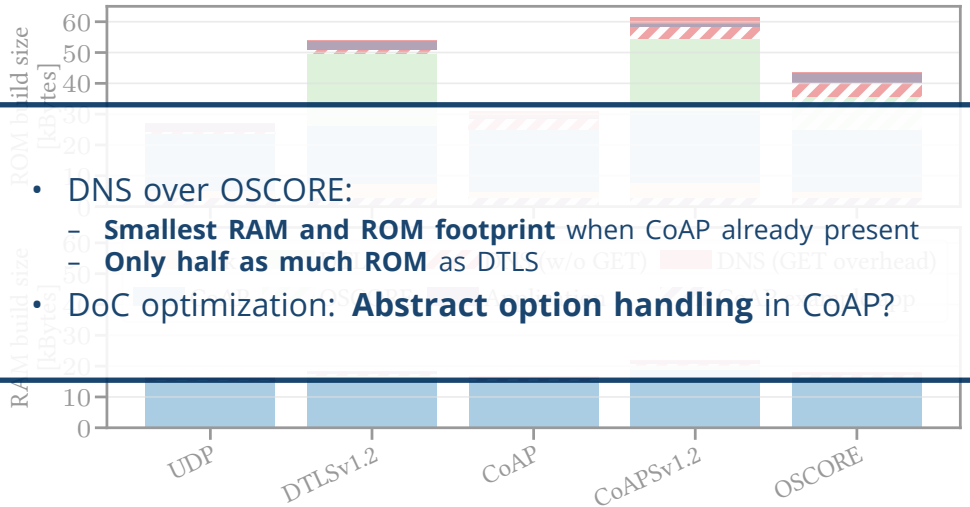
Memory Consumption



Memory Consumption



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?

Outline

Motivation

A Brief Introduction into CoAP

Design Guidance from IoT DNS Traffic

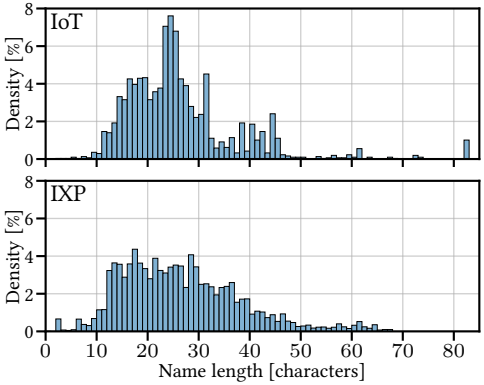
DNS over CoAP

Evaluation

Further Improvements

Conclusion & Future Work

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

Further Improvements

Concise DNS Message Representation

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

Name Length

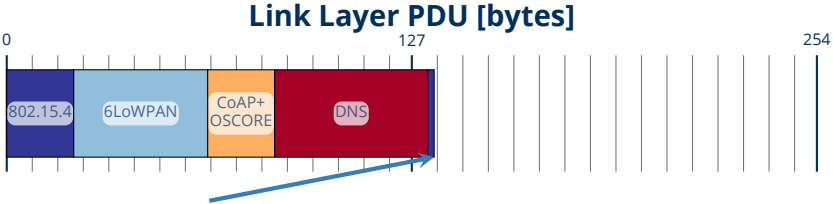
2 chars (minimum)

Further Improvements

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

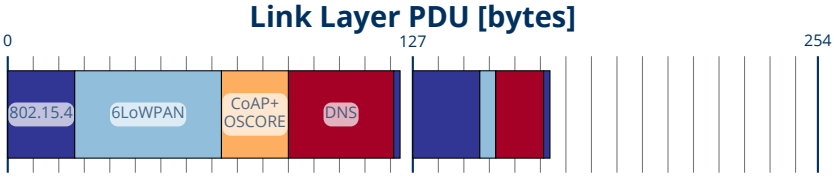


Further Improvements

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



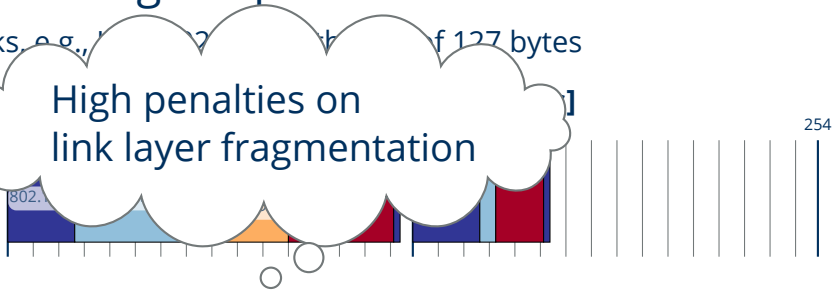
⇒ Fragmentation

Further Improvements

Concise DNS Message Representation

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

Name Length	Messa[illegible] Type	]
2 chars	AAAA Response	



⇒ Fragmentation

Further Improvements

C

Co

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/`

Objectives:

- Concise encoding of DNS messages using existing implementation (CBOR)
- Omits (redundant) DNS fields in DNS queries and responses
- Provides (optional) address and name compression using CBOR-packed

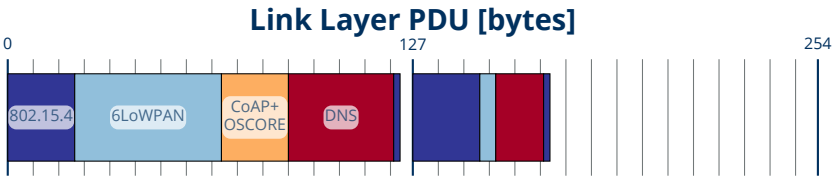
Further Improvements

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




```
11 ac 80 00 00 01 00 01 00 00 00 00 02 67 77 00
00 1c 00 01 c0 0c 00 1c 00 01 00 00 0e 10 00 10
20 01 0d b8 00 00 00 00 00 00 00 00 00 00 00 01
```

Classic DNS

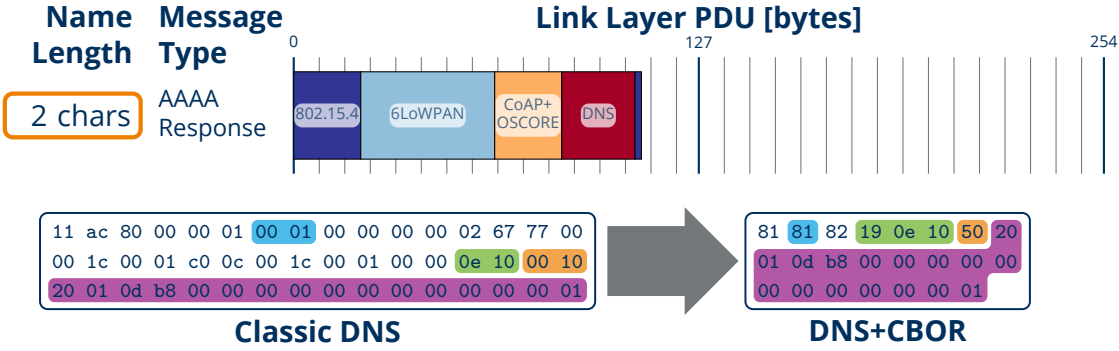
```
81 81 82 19 0e 10 50 20
01 0d b8 00 00 00 00 00
00 00 00 00 00 00 01
```

DNS+CBOR

Further Improvements

Concise DNS Message Representation

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



Outline

Motivation

A Brief Introduction into CoAP

Design Guidance from IoT DNS Traffic

DNS over CoAP

Evaluation

Further Improvements

Conclusion & Future Work

Conclusion & Future Work

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

- DoC with FETCH 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`)
- Potential mDNS protection with Group OSCORE?

Reproducible Research: Our Artifacts

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

Standardization in IETF:

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

Backup slides

Outline

IoT DNS Traffic

Comparison with QUIC

Evaluation: Caching Approaches

Name Length: More Statistical Properties

	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

Outline

IoT DNS Traffic

Comparison with QUIC

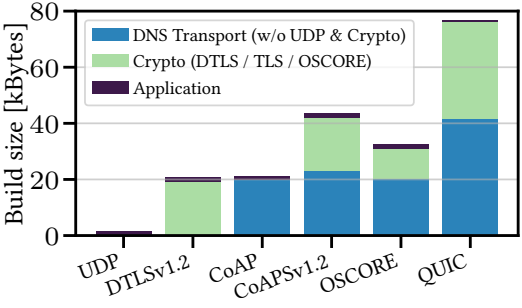
Evaluation: Caching Approaches

Comparison with QUIC: Method

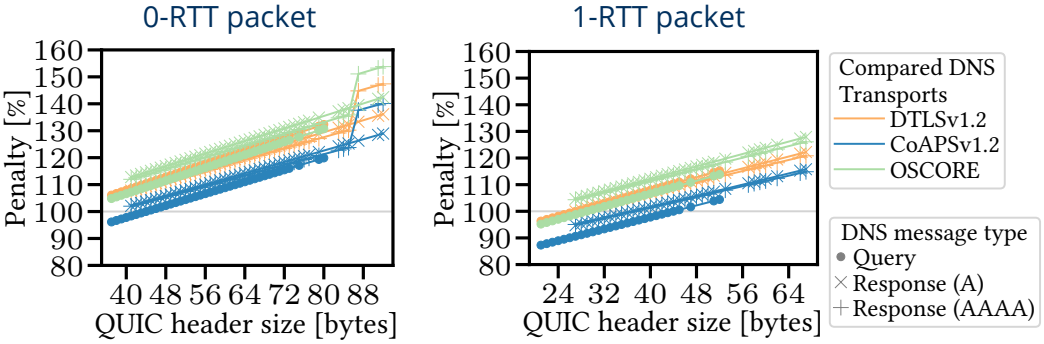
- Point of Reference: Quant[1]
- Memory Size: Quant & our requester application build for ESP32
- Packet Size: Numerical evaluation based on RFC9000

[1] Lars 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).

Comparison with QUIC: Code Sizes



Comparison with QUIC: Additional Link Layer Data



Outline

IoT DNS Traffic

Comparison with QUIC

Evaluation: Caching Approaches

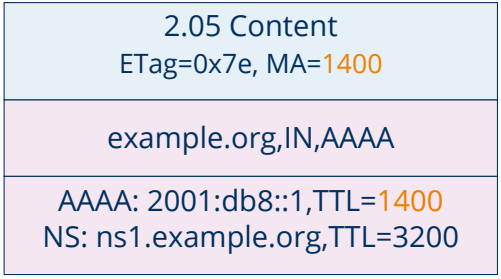
Caching Approaches

DoH-like

example.org,IN,AAAA
AAAA: 2001:db8::1,TTL=1800 NS: ns1.example.org,TTL=3600

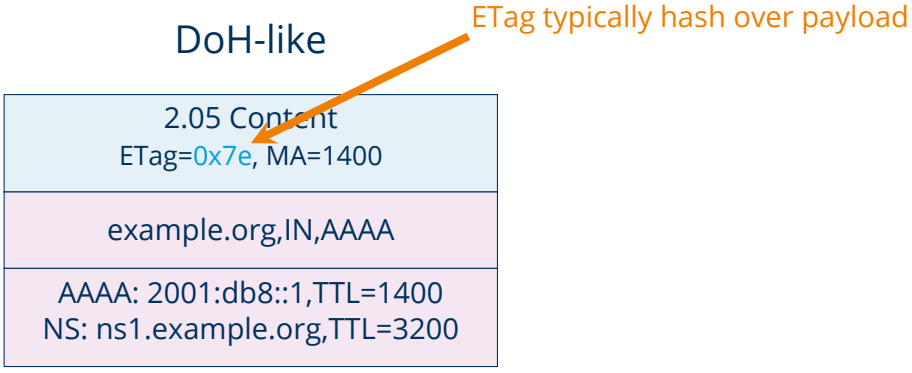
Caching Approaches

DoH-like



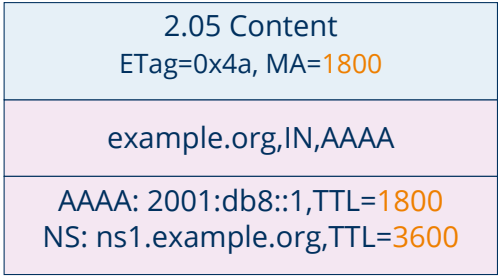
Caching Approaches

DoH-like



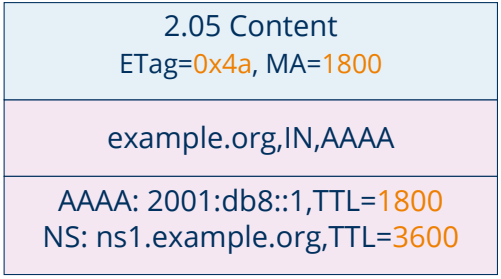
Caching Approaches

DoH-like



Caching Approaches

DoH-like



Caching Approaches

DoH-like

2.05 Content ETag=0x4a, MA=1800
example.org,IN,AAAA
AAAA: 2001:db8::1,TTL=1800 NS: ns1.example.org,TTL=3600

⇒ Cache validation fails on TTL changes

Caching Approaches

DoH-like

2.05 Content ETag=0x4a, MA=1800
example.org,IN,AAAA
AAAA: 2001:db8::1,TTL=1800 NS: ns1.example.org,TTL=3600

EOL-TTLs

example.org,IN,AAAA
AAAA: 2001:db8::1,TTL=1400 NS: ns1.example.org,TTL=3200

⇒ Cache validation fails on TTL changes

Caching Approaches

DoH-like

2.05 Content ETag=0x4a, MA=1800
example.org,IN,AAAA
AAAA: 2001:db8::1,TTL=1800 NS: ns1.example.org,TTL=3600

EOL-TTLs

2.05 Content ETag=0x95, MA=1400
example.org,IN,AAAA
AAAA: 2001:db8::1,TTL=0 NS: ns1.example.org,TTL=0

⇒ Cache validation fails on TTL changes

Caching Approaches

DoH-like

2.05 Content ETag=0x4a, MA=1800
example.org,IN,AAAA
AAAA: 2001:db8::1,TTL=1800 NS: ns1.example.org,TTL=3600

EOL-TTLs

2.05 Content ETag=0x95, MA=1800
example.org,IN,AAAA
AAAA: 2001:db8::1,TTL=0 NS: ns1.example.org,TTL=0

⇒ Cache validation fails on TTL changes

Caching Approaches

DoH-like

2.05 Content ETag=0x4a, MA=1800
example.org,IN,AAAA
AAAA: 2001:db8::1,TTL=1800 NS: ns1.example.org,TTL=3600

⇒ Cache validation fails on TTL changes

EOL-TTLs

2.05 Content ETag=0x95, MA=1800
example.org,IN,AAAA
AAAA: 2001:db8::1,TTL=0 NS: ns1.example.org,TTL=0

⇒ Decoupling of cache validation from TTL changes

Evaluation: Caching Approaches