New Kid on the Block: Content Object Security for a Data-centric Web of Things

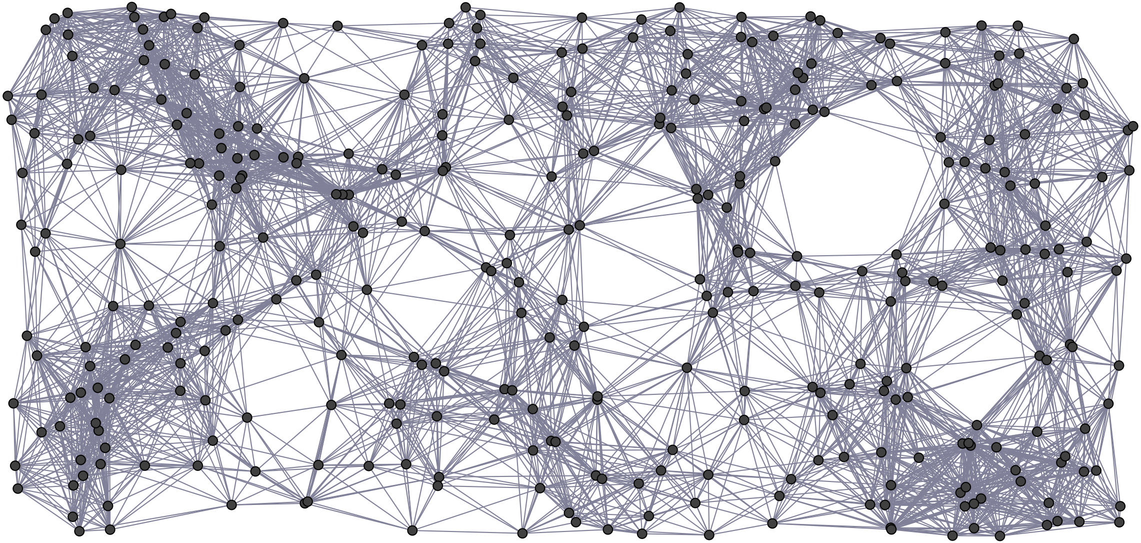
X-mas 2020

Cenk Gündoğan

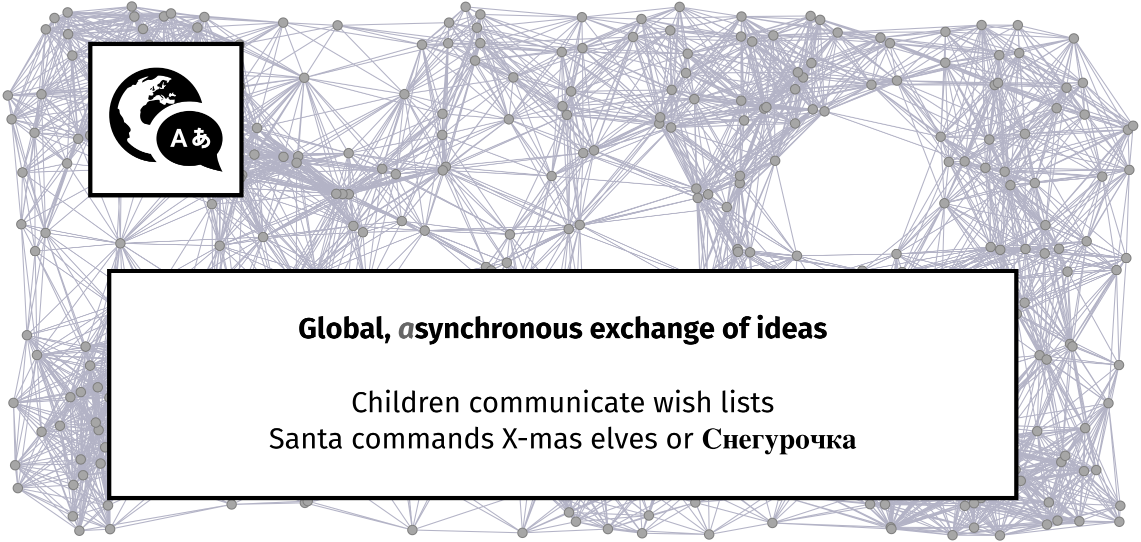
HAW Hamburg
cenk.guendogan@haw-hamburg.de

December 16, 2020

The Internet



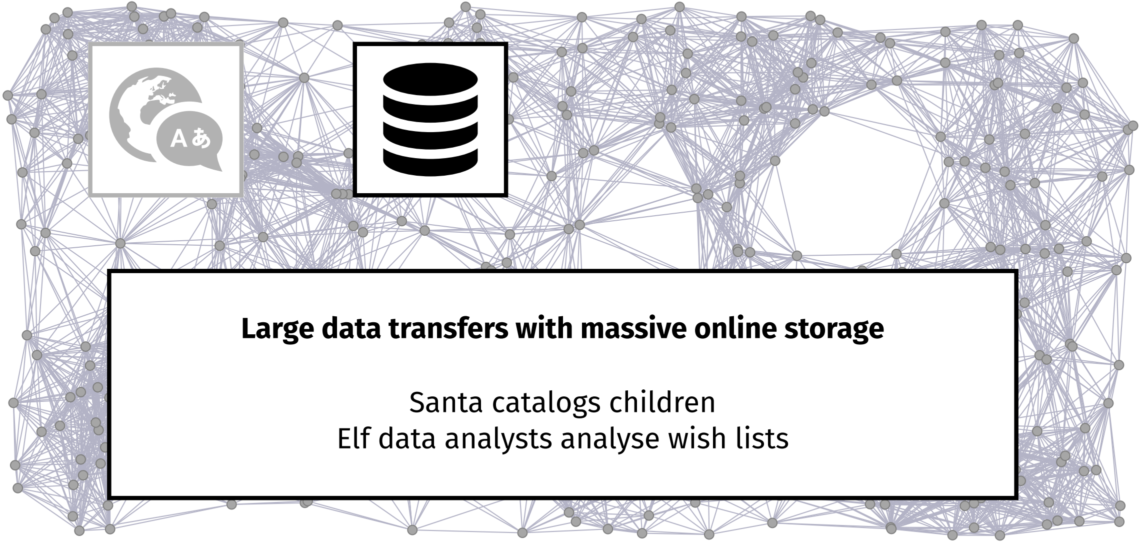
The Internet



Global, *a*synchronous exchange of ideas

Children communicate wish lists
Santa commands X-mas elves or **Снегурочка**

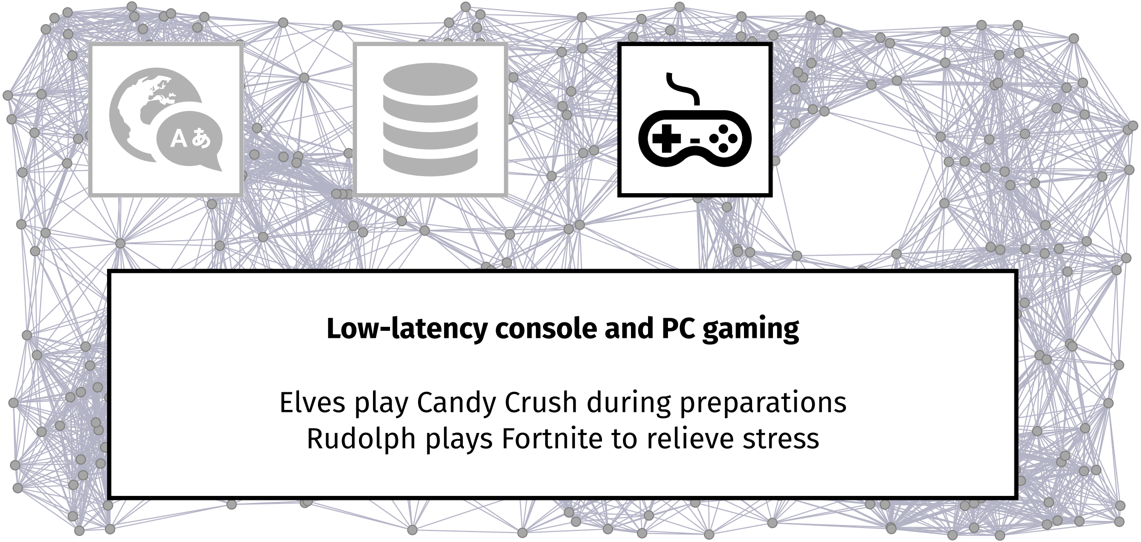
The Internet



Large data transfers with massive online storage

Santa catalogs children
Elf data analysts analyse wish lists

The Internet



Low-latency console and PC gaming

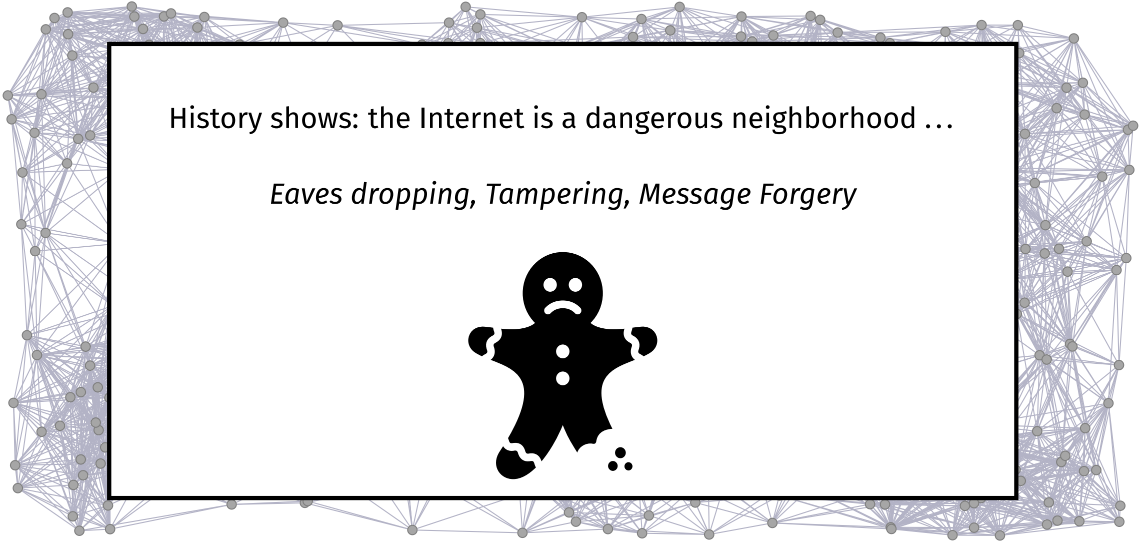
Elves play Candy Crush during preparations
Rudolph plays Fortnite to relieve stress

The Internet

B2B & B2C E-commerce

Santa orders toys from specialist retail stores
Parents browse Santa’s web shop

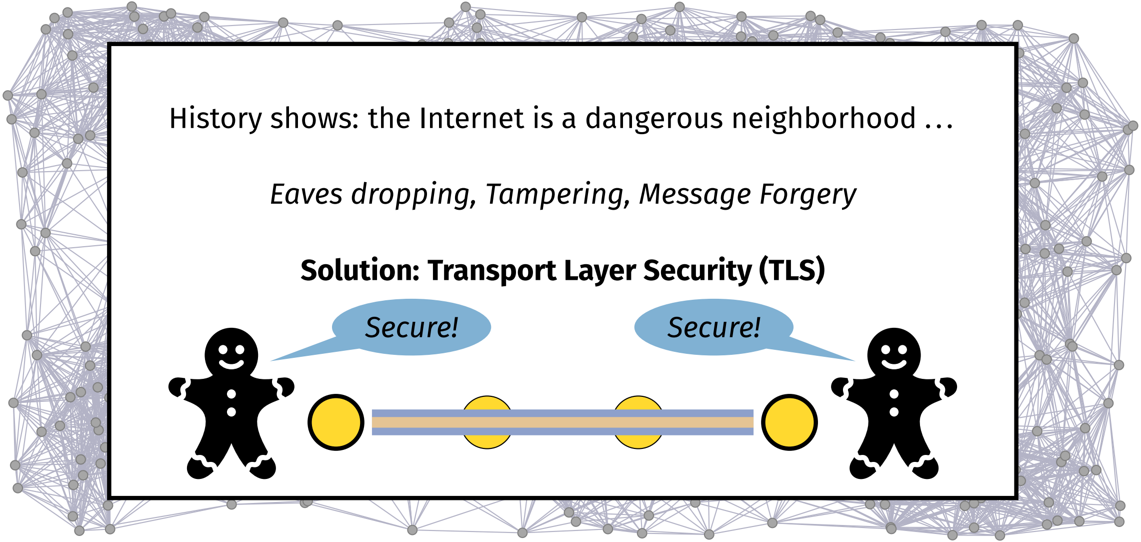
The Internet



History shows: the Internet is a dangerous neighborhood …

Eaves dropping, Tampering, Message Forgery

The Internet

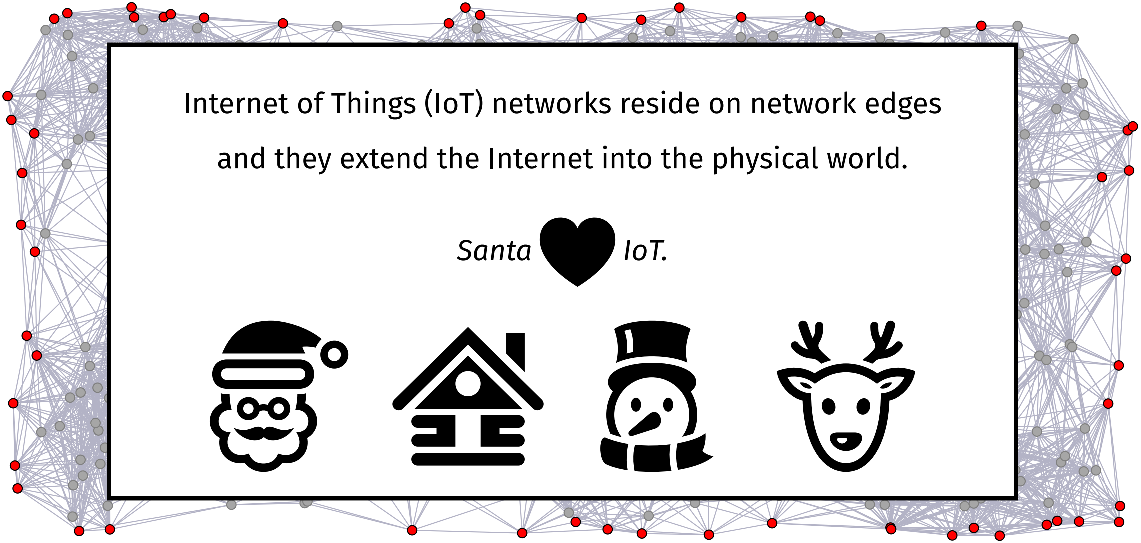


History shows: the Internet is a dangerous neighborhood ...

Eaves dropping, Tampering, Message Forgery

Solution: Transport Layer Security (TLS)

The Internet



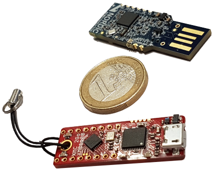
Internet of Things (IoT) networks reside on network edges

and they extend the Internet into the physical world.

Santa ♥ *IoT.*

Common Internet of Things Deployment

- Constrained IoT devices, gateway, cloud services



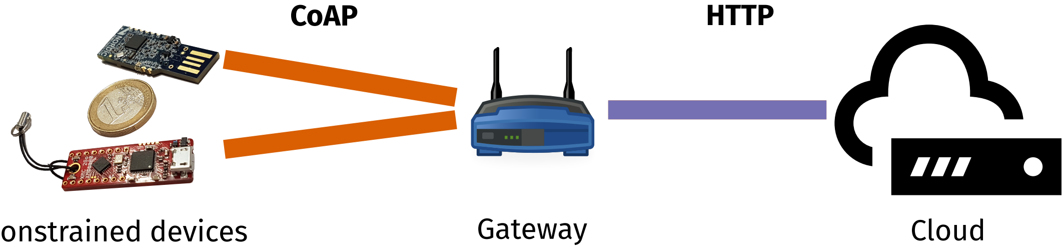
Constrained devices

Gateway

Cloud

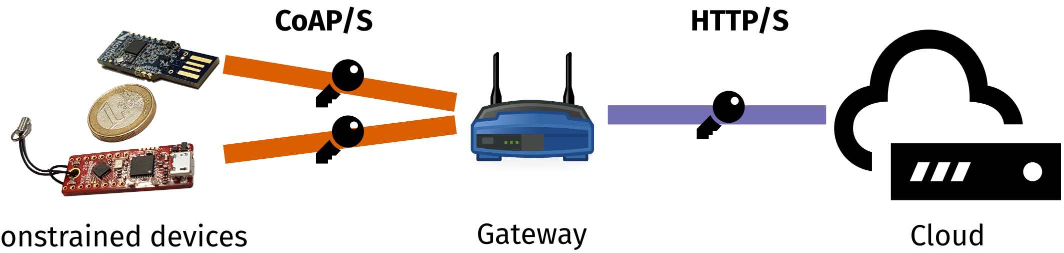
Common Internet of Things Deployment

- Constrained IoT devices, gateway, cloud services
- RESTful deployment using CoAP and HTTP (*Web of Things*)



Common Internet of Things Deployment

- Constrained IoT devices, gateway, cloud services
- RESTful deployment using CoAP and HTTP *(Web of Things)*
- Transport layer security (DTLS, TLS) between endpoints



The IoT is protected …

Thank You!
Any Questions?

The IoT is protected …

~~Thank You!~~

~~Any Questions?~~

…not so fast!

gotcha! ⟶

A Closer Look at Transport Layer Security for the IoT

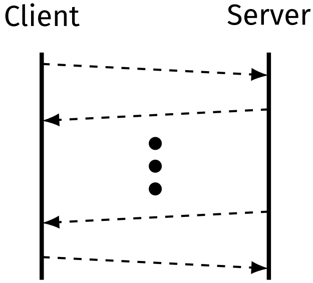
Datagram Transport Layer Security for CoAP

- Operates on top of UDP and is based on stream-oriented TLS
- Prevents eavesdropping, tampering, and message forgery
- Endpoint identification using 5-tuple (IP_{src}, $Port_{src}$, IP_{dst}, $Port_{dst}$, Protocol)

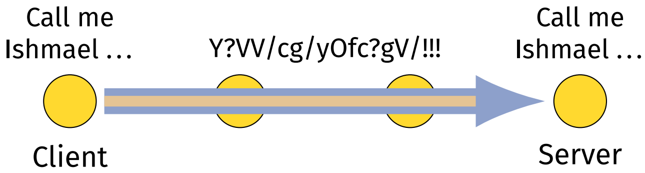
Datagram Transport Layer Security for CoAP

- Operates on top of UDP and is based on stream-oriented TLS
- Prevents eavesdropping, tampering, and message forgery
- Endpoint identification using 5-tuple (IP$_{src}$, Port$_{src}$, IP$_{dst}$, Port$_{dst}$, Protocol)

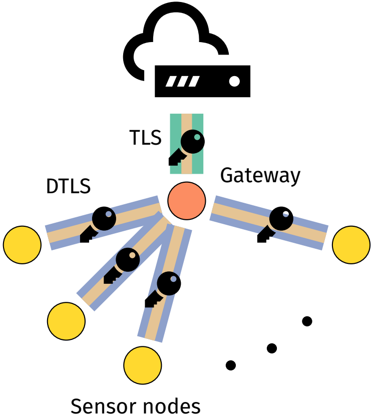
Handshake Layer

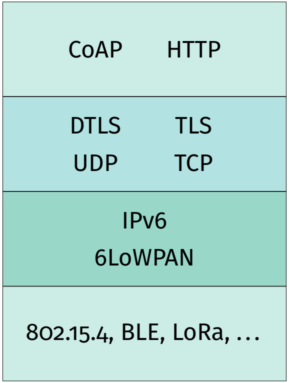


Record Layer



DTLS Challenges





CoAP HTTP

DTLS TLS

UDP TCP

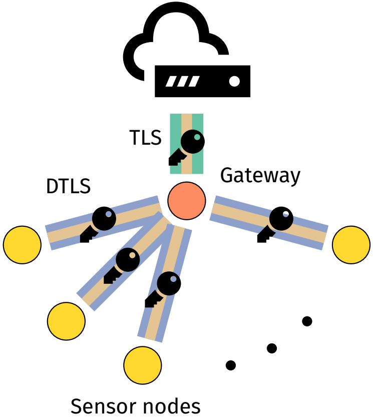
IPv6

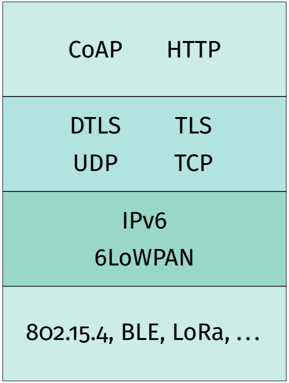
6LoWPAN

802.15.4, BLE, LoRa, . . .

DTLS Challenges

- Protocol conversion (CoAPS ⇒ HTTPS) harms end-to-end security





CoAP HTTP

DTLS TLS

UDP TCP

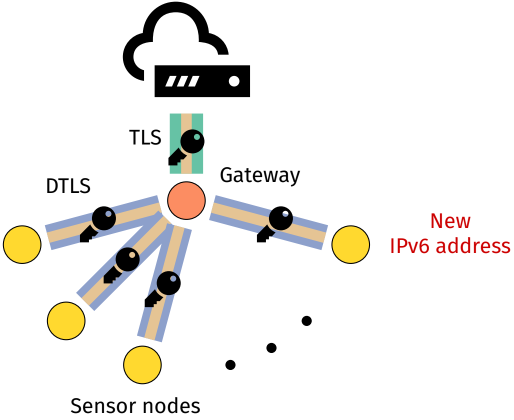
IPv6

6LoWPAN

802.15.4, BLE, LoRa, ...

DTLS Challenges

- Protocol conversion (CoAPS ⇒ HTTPS) harms end-to-end security
- Endpoint-based session management is costly on node mobility



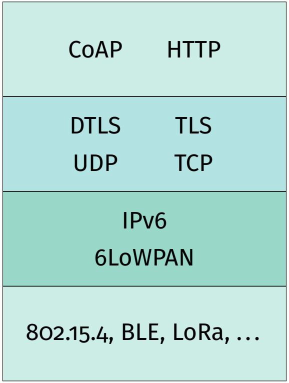
TLS

Gateway

DTLS

New
IPv6 address

Sensor nodes



CoAP HTTP

DTLS TLS

UDP TCP

IPv6

6LoWPAN

802.15.4, BLE, LoRa, . . .

Content Object Security for the IoT using CoAP

Content Object Security for CoAP

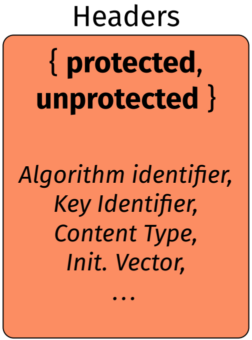
- OSCORE: Object Security for Constrained RESTful Environments
- Proposed standard (RFC8613) since July 2019
- Builds on COSE: CBOR Object Signing and Encryption (RFC8152)

Security

- Confidentiality (COSE)
- Integrity (COSE)
- Replay mitigations (OSCORE)

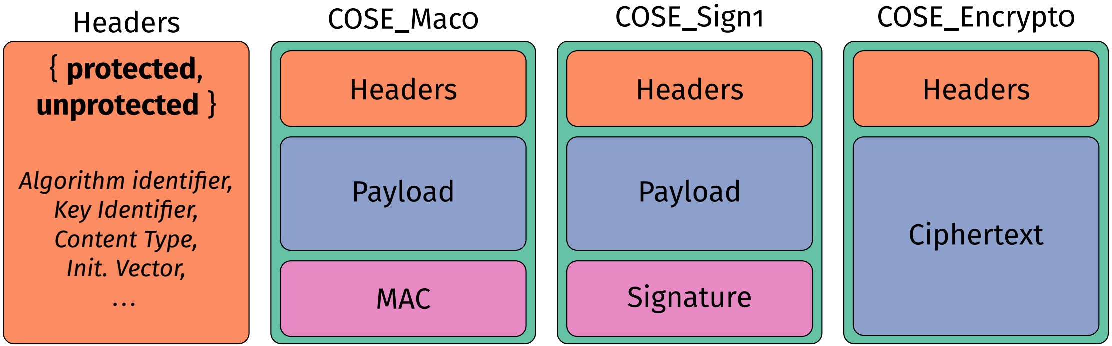
COSE: CBOR Object Signing and Encryption

- **Data Organization** and **Cryptographic Operations** (MAC, Sign, Encrypt)
- CBOR: Concise Binary Object Representation
- COSE builds and improves on JOSE (JSON Object Signing and Encryption)



COSE: CBOR Object Signing and Encryption

- **Data Organization** and **Cryptographic Operations** (MAC, Sign, Encrypt)
- CBOR: Concise Binary Object Representation
- COSE builds and improves on JOSE (JSON Object Signing and Encryption)



Headers

{ **protected**, **unprotected** }

Algorithm identifier,
Key Identifier,
Content Type,
Init. Vector,
...

COSE_Mac0

Headers

Payload

MAC

COSE_Sign1

Headers

Payload

Signature

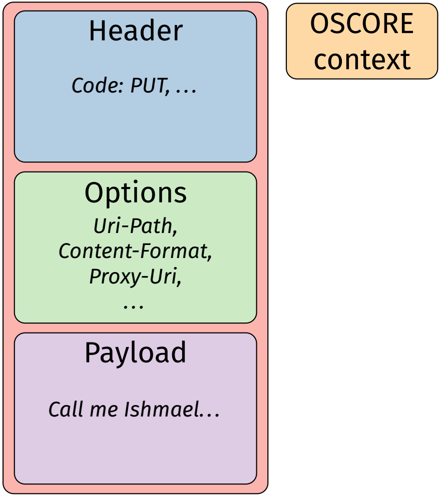
COSE_Encrypt0

Headers

Ciphertext

OSCORE Integration into CoAP

Unprotected CoAP



Header

Code: PUT, …

Options

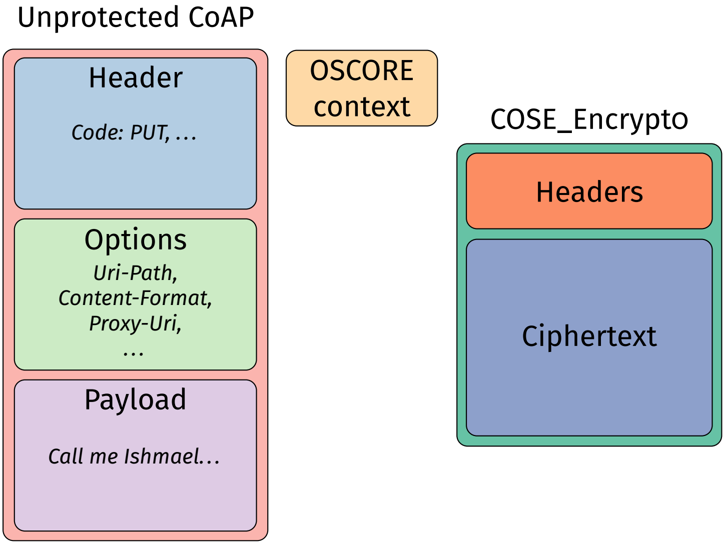
Uri-Path,
Content-Format,
Proxy-Uri,
…

Payload

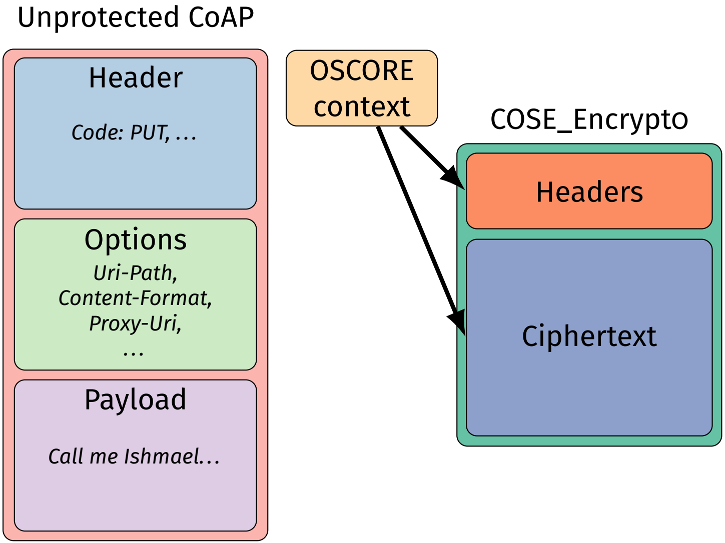
Call me Ishmael…

OSCORE context

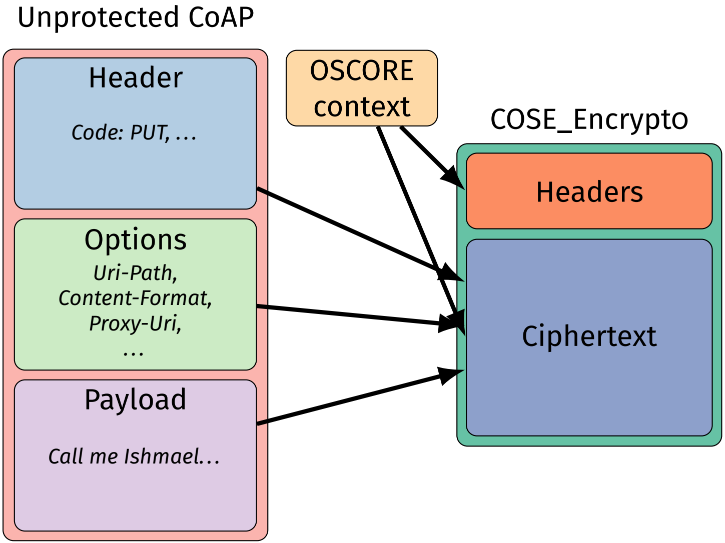
OSCORE Integration into CoAP



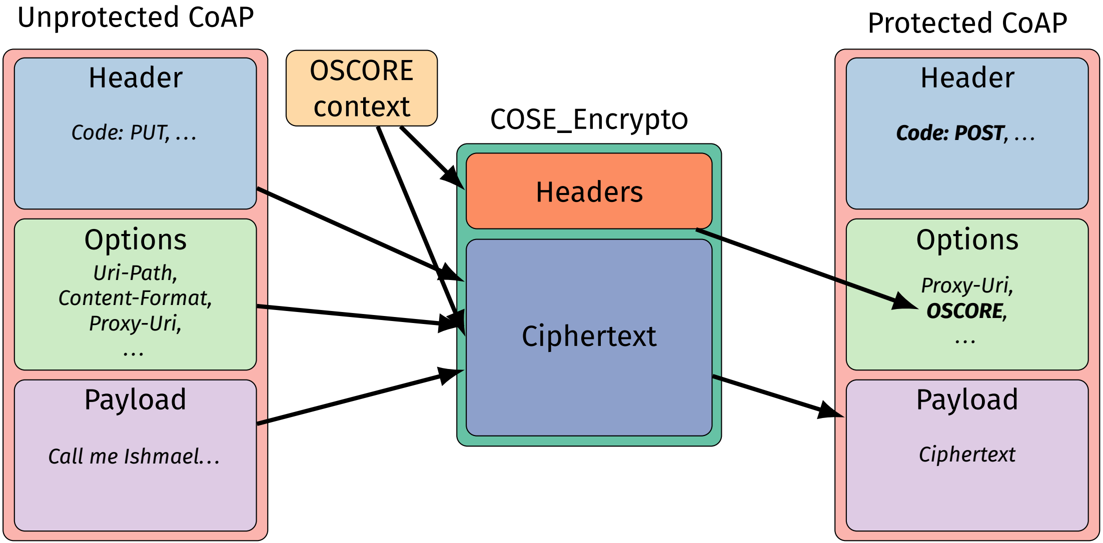
OSCORE Integration into CoAP



OSCORE Integration into CoAP



OSCORE Integration into CoAP



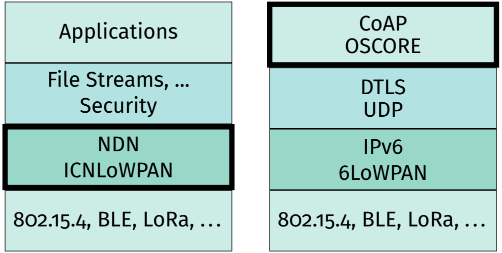
Content Object Security for the IoT using Named-Data Networking

NDN: Named-Data Networking

- Proposed Future Internet architecture since 2006 (CCN)
- Follows Information-Centric Networking (ICN) paradigm
- Replaces IP on the network layer

Key Aspects

- Pull-driven content retrieval
- No endpoint addressing
- Routable content names
- Hop-wise network caches
- Inherent multicast support
- Content object security



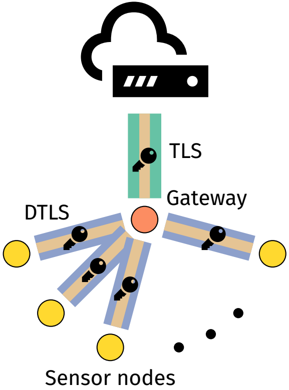
Applications	CoAP OSCORE
File Streams, ... Security	DTLS UDP
NDN ICNLoWPAN	IPv6 6LoWPAN
802.15.4, BLE, LoRa, ...	802.15.4, BLE, LoRa, ...

Research indicates: NDN promotes resilience in constrained IoT deployments.

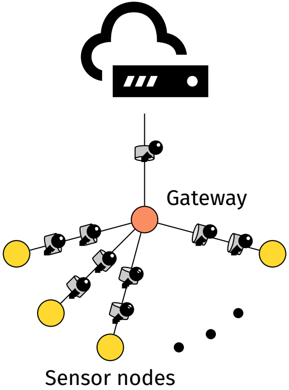
Protocol Performance Evaluation

Protocol Ensemble

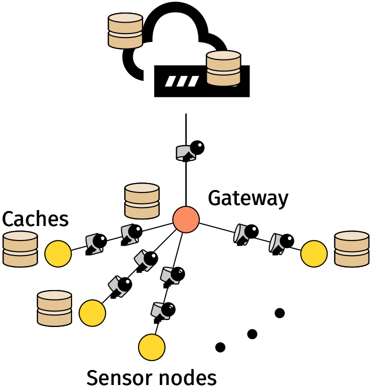
CoAP over DTLS



CoAP with OSCORE

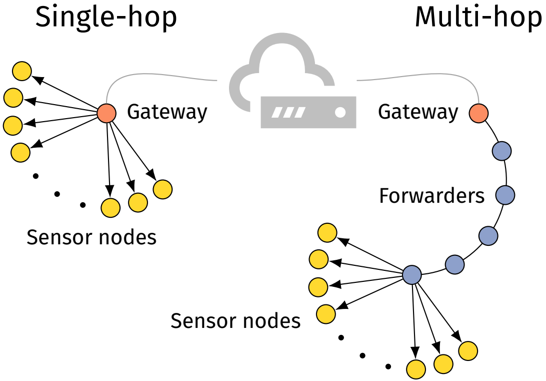


NDN



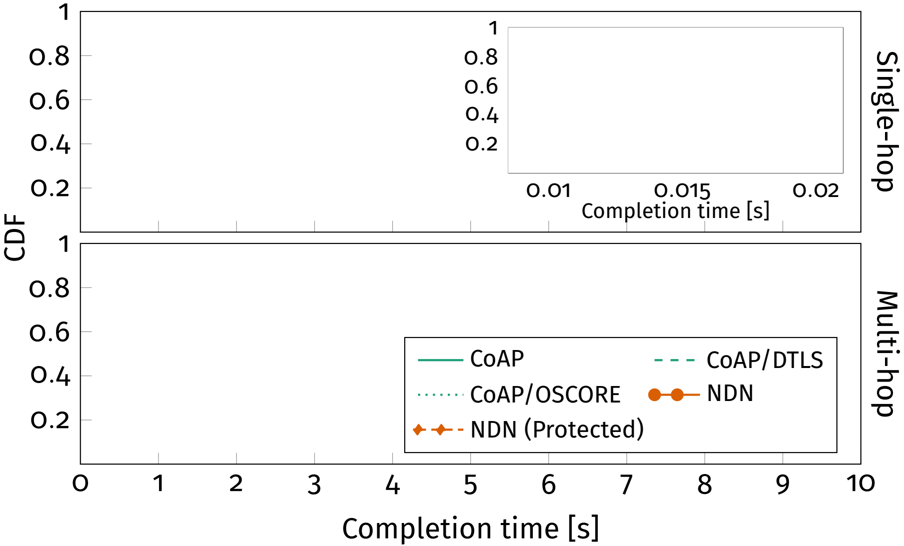
Testbed Setup

Hardware	M3 node in IoT Lab testbed, IEEE 802.15.4
Software	RIOT with tinyDTLS, libOSCORE, CCN-lite
Topology	Single- & Multi-hop
Scenario	Gateway requests 2-byte temperature every ≈ 2 s

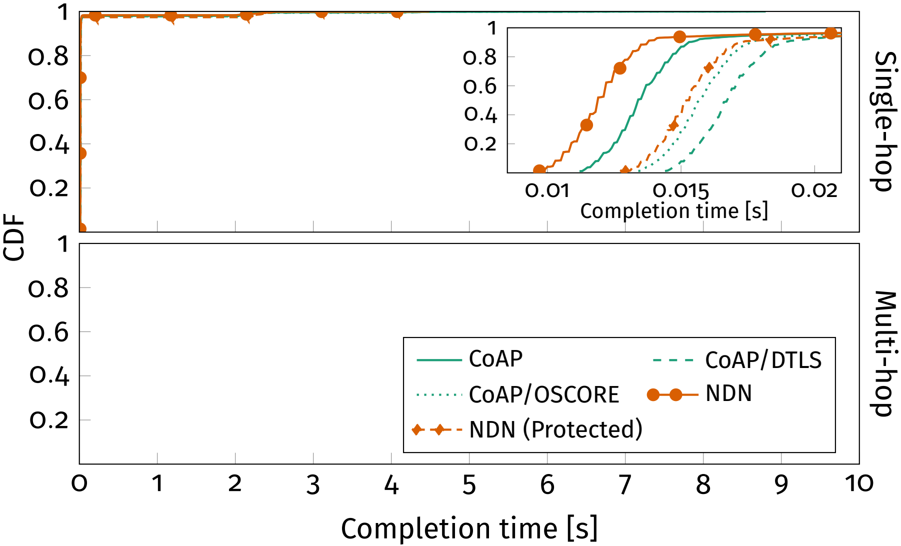


[Networking'20] IoT Content Object Security with OSCORE and NDN: A First Experimental Comparison

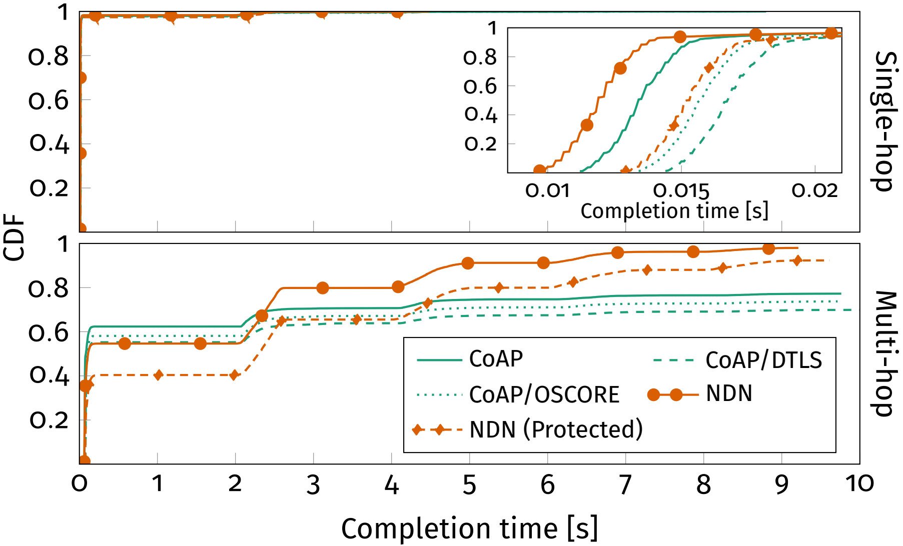
Time to Content Arrival



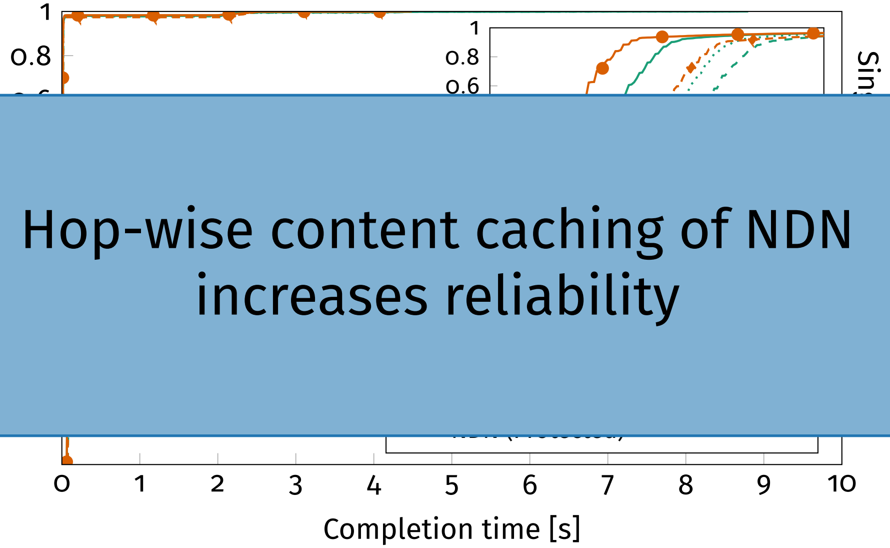
Time to Content Arrival



Time to Content Arrival



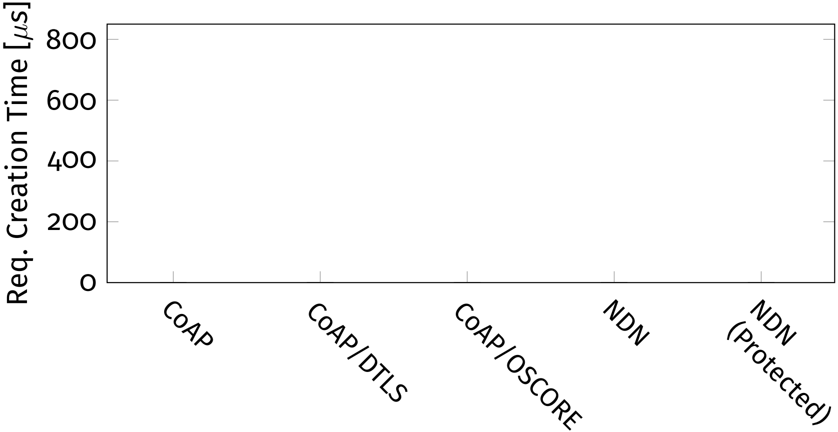
Time to Content Arrival



Hop-wise content caching of NDN increases reliability

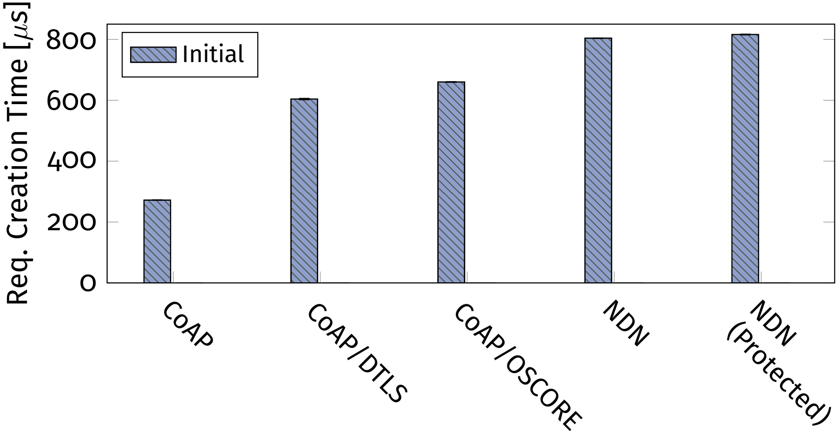
Request Creation Time

- Message retransmissions are frequent in low-power regimes
- **CoAP:** End-to-end application layer retransmissions
- **NDN:** Hop-by-hop network layer retransmissions



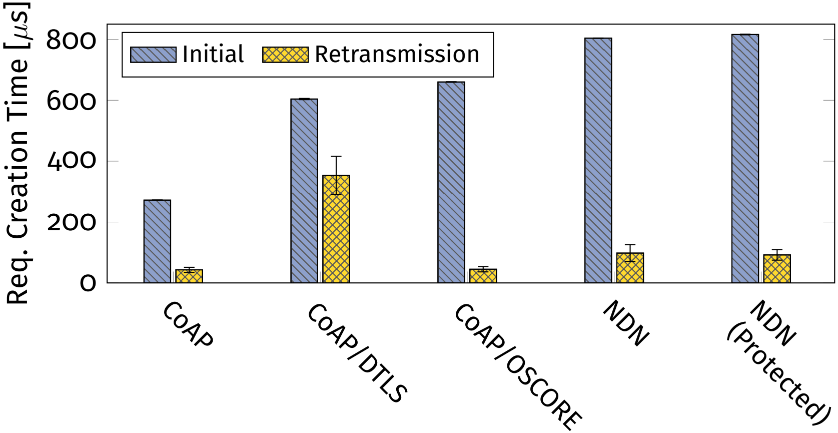
Request Creation Time

- Message retransmissions are frequent in low-power regimes
- **CoAP:** End-to-end application layer retransmissions
- **NDN:** Hop-by-hop network layer retransmissions



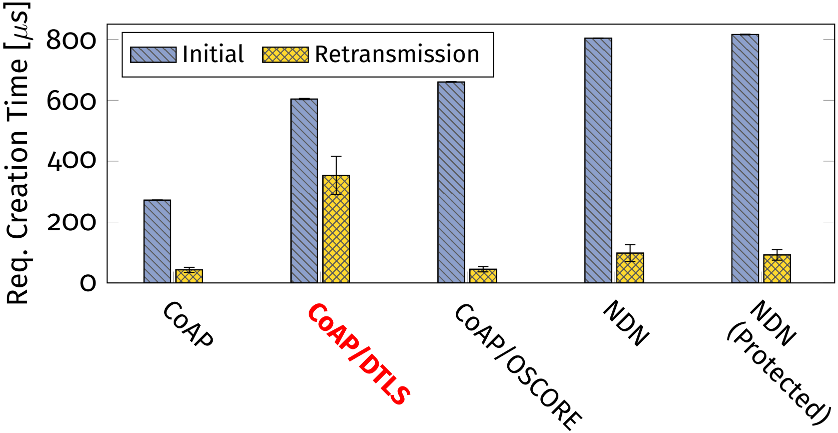
Request Creation Time

- Message retransmissions are frequent in low-power regimes
- **CoAP:** End-to-end application layer retransmissions
- **NDN:** Hop-by-hop network layer retransmissions



Request Creation Time

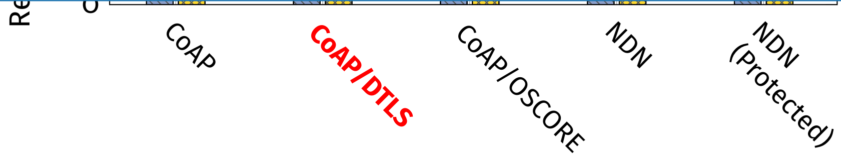
- Message retransmissions are frequent in low-power regimes
- **CoAP:** End-to-end application layer retransmissions
- **NDN:** Hop-by-hop network layer retransmissions



Request Creation Time

- Message retransmissions are frequent in low-power regimes
- **CoAP:** End-to-end application layer retransmissions

DTLS record layer generates higher load on retransmissions



Evaluation Takeaways

- OSCORE brings a lean object security to the constrained IoT
- CoAP/DTLS shows overhead on endpoint changes and retransmissions
- NDN has a higher reliability due to hop-wise caching

Evaluation Takeaways

- OSCORE brings a lean object security to the constrained IoT
- CoAP/DTLS shows overhead on endpoint changes and retransmissions
- **NDN has a higher reliability due to hop-wise caching**

Benefits of Information-centric Properties for the IoT

Stateful Forwarding

Caching

Content Object Security

- **Stateful forwarding** and **caching** shorten request paths and reduce link traversals on retransmissions
- **Content object security** enables end-to-end security and reduces session management complexity

Constructing an Information-centric Web of Things

[ICN'20] Toward a RESTful Information-Centric Web of Things [. . .]

Communication Model & Flow Control

- CoAP GET method provides request-response paradigm
- Acknowledgments for requests and optionally for responses

Stateful Forwarding & Caching

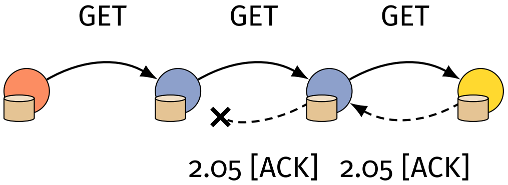
- CoAP proxies [RFC7252] forward requests and return responses
- Proxies perform response caching

Content Object Security

- OSCORE [RFC8613] provides Authenticated Encryption with Associated Data
- End-to-end security across gateways

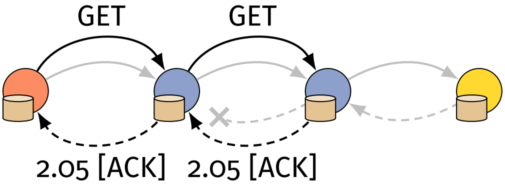
Deploying an Information-centric Web of Things

- Proxy on each forwarding node
- Hop-wise retransmissions & caching
- OSCORE protected messages



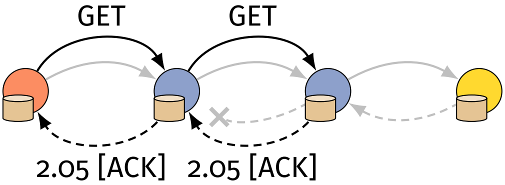
Deploying an Information-centric Web of Things

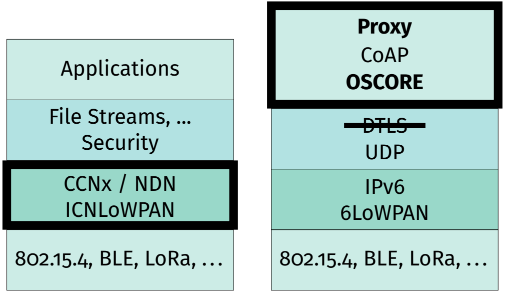
- Proxy on each forwarding node
- Hop-wise retransmissions & caching
- OSCORE protected messages



Deploying an Information-centric Web of Things

- Proxy on each forwarding node
- Hop-wise retransmissions & caching
- OSCORE protected messages





Applications

File Streams, ...
Security

CCNx / NDN
ICNLoWPAN

802.15.4, BLE, LoRa, . . .

Proxy
CoAP
OSCORE

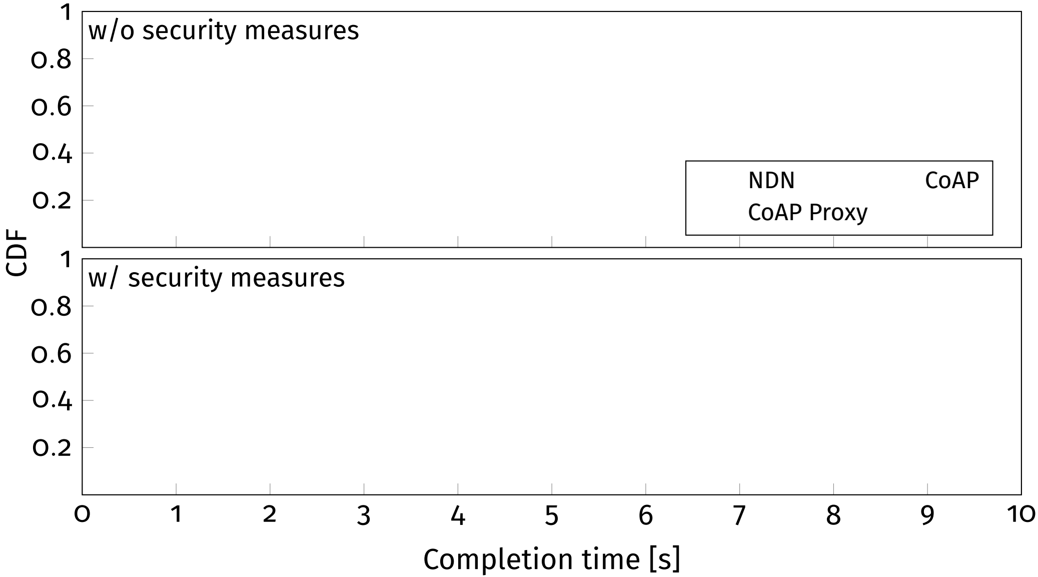
~~DTLS~~
UDP

IPv6
6LoWPAN

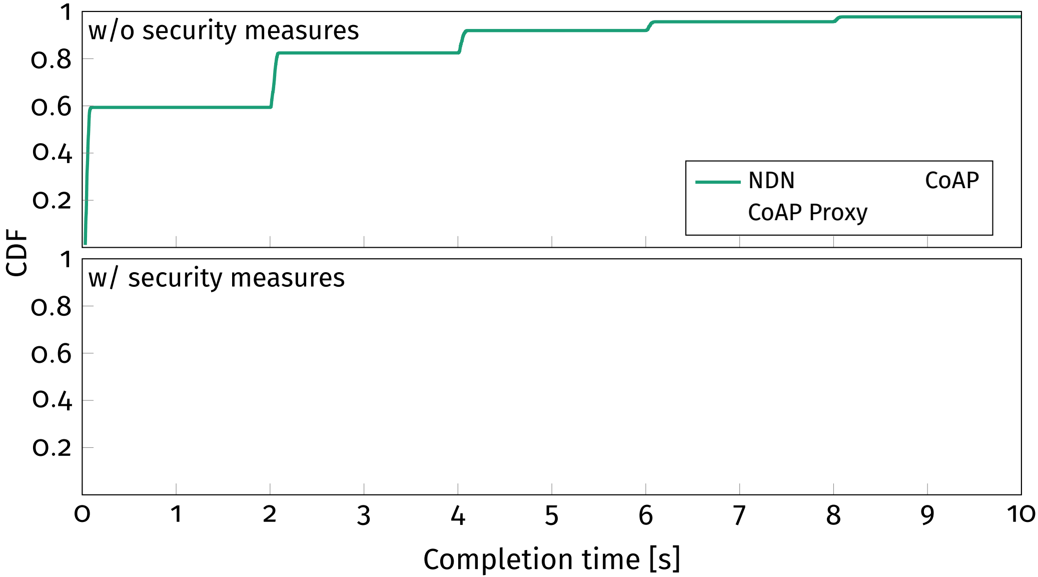
802.15.4, BLE, LoRa, . . .

- Forwards on service names
- Reflects ICN properties on app layer
- Bonus: link-local IPv6 addresses benefit 6LoWPAN compression

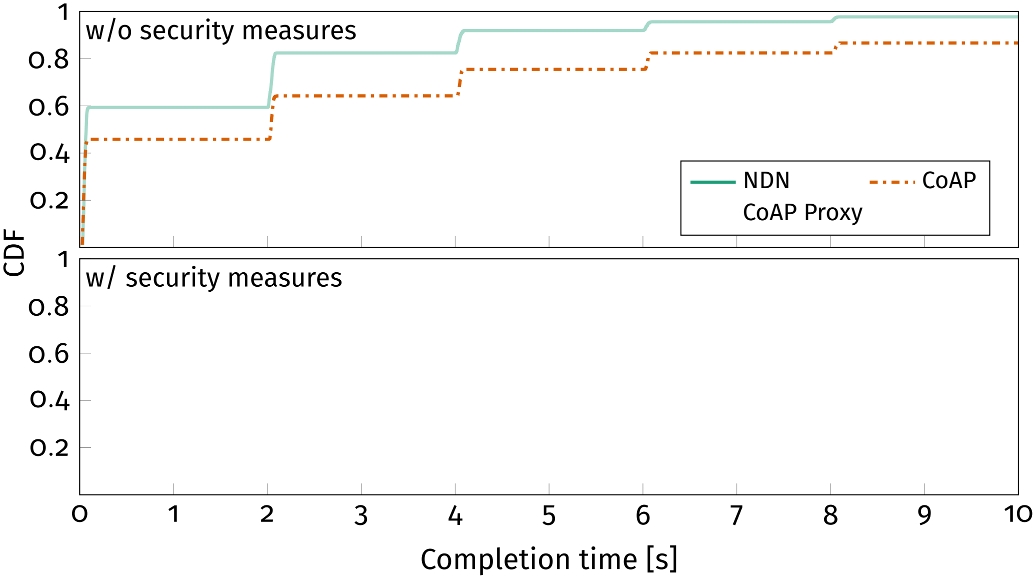
Time to Content Arrival



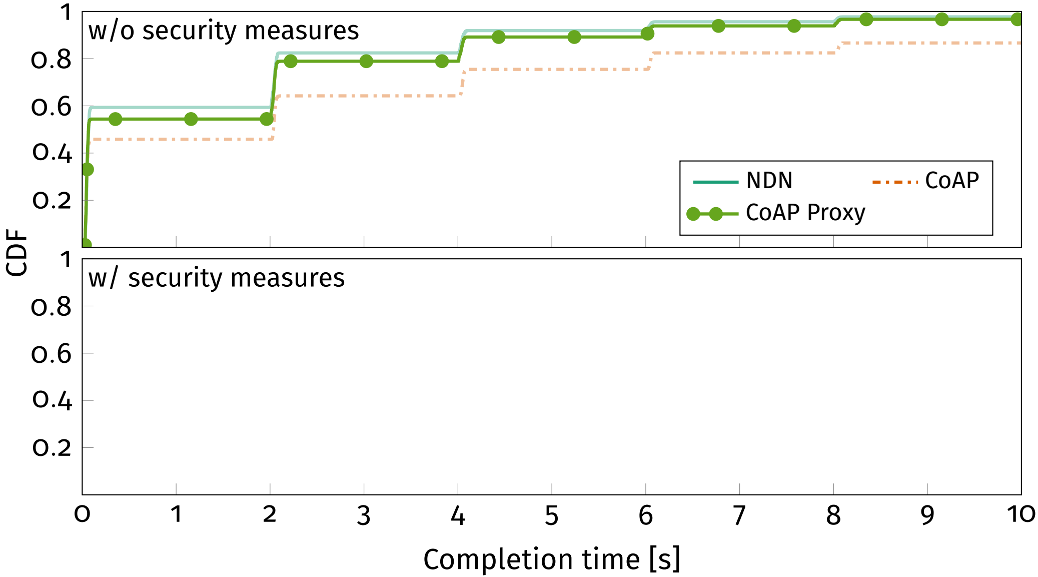
Time to Content Arrival



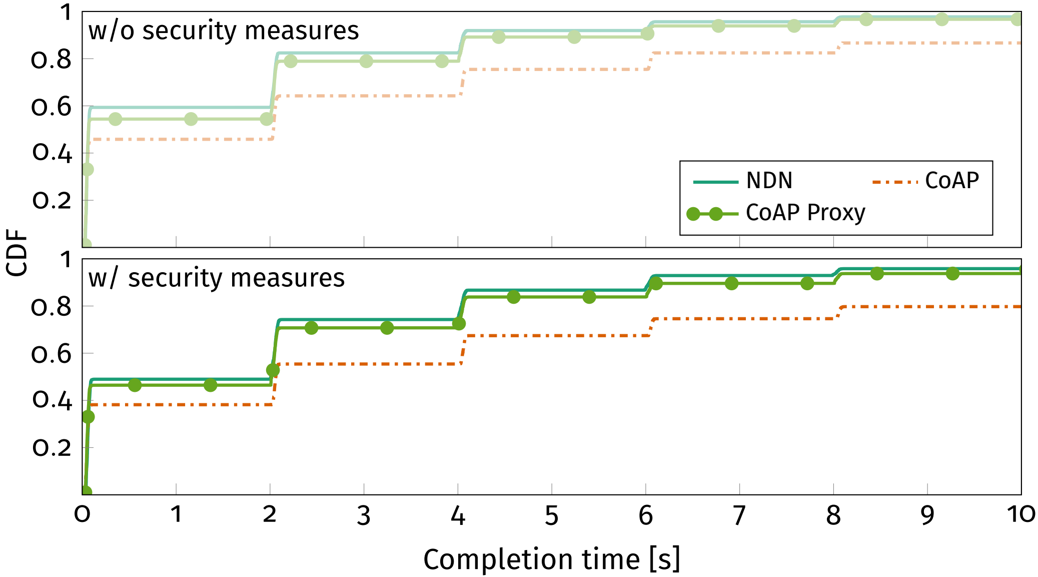
Time to Content Arrival



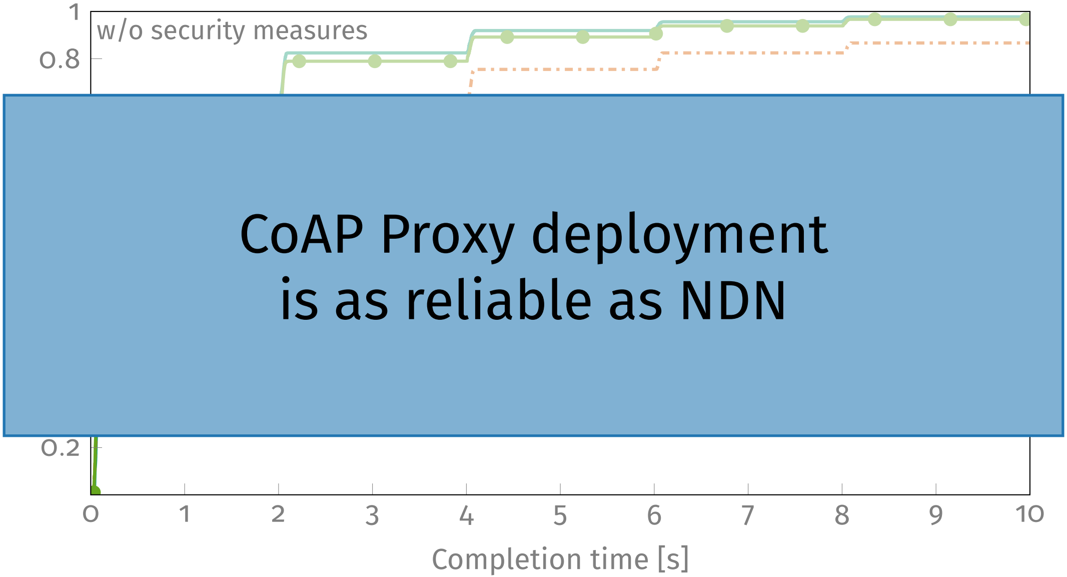
Time to Content Arrival



Time to Content Arrival



Time to Content Arrival



CoAP Proxy deployment
is as reliable as NDN

Conclusion & Outlook

Takeaways

- Information-centric WoT can be built with CoAP standard features
- Stateful forwarding and hop-wise caching improves reliability for CoAP
- Deployment chance for NDN features in existing IoT infrastructure

Next Step

- Investigate multicast properties of an information-centric Web of Things

Thank You!
Any Questions?