

A Data-centric CoAP Transport

T2TRG Interim

Cenk Gündoğan¹

¹HAW Hamburg

October 26, 2021

cenk.guendogan@haw-hamburg.de

Information-Centric Networking (ICN)

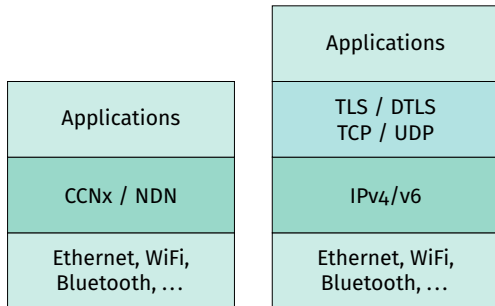
- ▶ Alternative networking paradigm
- ▶ Specialization on content delivery
- ▶ Loose coupling of data and host endpoints

Prominent architectures

- ▶ Named-Data Networking (NDN)
- ▶ Content-Centric Networking (CCNx)

Protocol features

- ▶ Name-based, stateful forwarding
- ▶ In-network content caching
- ▶ Content object security



Technical Aspects of CCNx / NDN

Communication Model

- ▶ Request-response paradigm
- ▶ Layer 3 primitives: Interest & Data

Interest /T2TRG/interim/sensor



Technical Aspects of CCNx / NDN

Communication Model

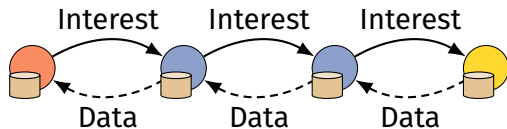
- ▶ Request-response paradigm
- ▶ Layer 3 primitives: Interest & Data

Interest / T2TRG / interim / sensor



Forwarding & Flow Balance

- ▶ Request state on each hop
- ▶ Hop-wise caching & retransmissions



Technical Aspects of CCNx / NDN

Communication Model

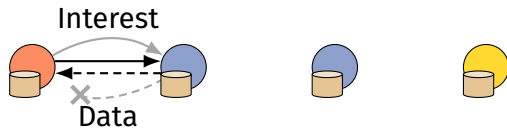
- ▶ Request-response paradigm
- ▶ Layer 3 primitives: Interest & Data

Interest / T2TRG / interim / sensor



Forwarding & Flow Balance

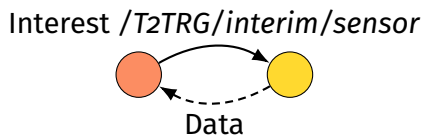
- ▶ Request state on each hop
- ▶ Hop-wise caching & retransmissions



Technical Aspects of CCNx / NDN

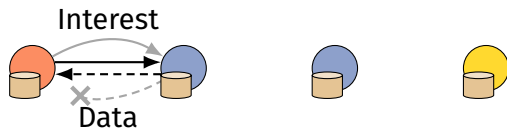
Communication Model

- ▶ Request-response paradigm
- ▶ Layer 3 primitives: Interest & Data



Forwarding & Flow Balance

- ▶ Request state on each hop
- ▶ Hop-wise caching & retransmissions



Content Object Security

- ▶ Individually verifiable data packets using HMAC or digital signatures
- ▶ End-to-end protection beyond untrusted gateways

Outline

Constructing a Data-centric Web of Things

Enabling a Reliable Multiparty Content Retrieval

Use Case: Firmware Updates

Constructing a Data-centric Web of Things

Benefits of Information-centric Properties for the IoT

Research indicates: promising candidate for IoT deployments

**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, reduces session management complexity and allows multi-party communication

Benefits of Information-centric Properties for the IoT

Research indicates: promising candidate for IoT deployments

Stateful
Forwarding

Caching

Content
Object Security

CoAP Proxy

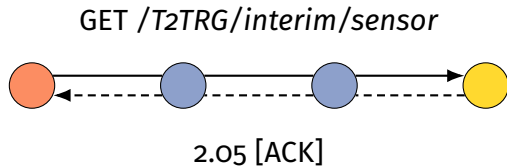
OSCORE

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

Constructing a Data-centric CoAP Deployment

Standard deployment

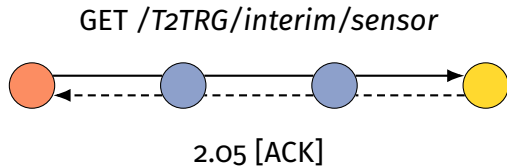
CoAP client / server + IPv6 forwarders
End-to-end retransmissions



Constructing a Data-centric CoAP Deployment

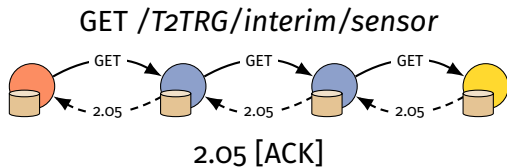
Standard deployment

CoAP client / server + IPv6 forwarders
End-to-end retransmissions



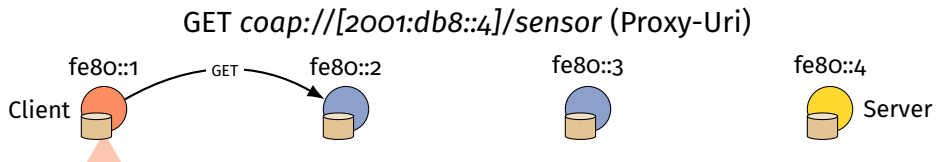
Data-centric deployment

*CoAP client / server + **CoAP proxies***
Hop-by-hop request state
Hop-wise caching & retransmissions
Forwarding decision on names

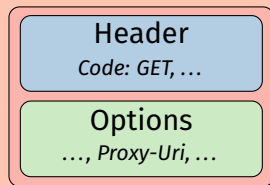


[ACM ICN'20] Toward a RESTful Information-Centric Web of Things [...]

Forwarding Details



- ▶ Forward request to next proxy (fe80::2)
- ▶ Point request state to localhost



Proxy-level
Forwarding Information Base

Destination	Next-hop
2001:db8::4/sensor	fe80::2

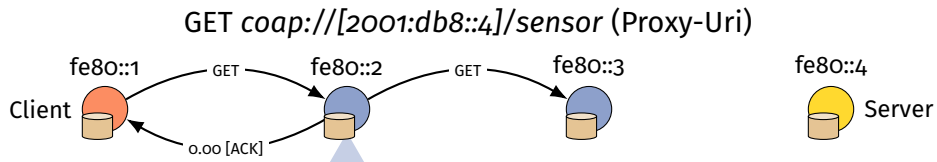
Request Table

Cache Key	Source
Key _i	::1/128

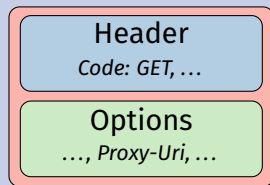
Cache

Cache Key	Response
—	—

Forwarding Details



- ▶ Acknowledge with empty response
- ▶ Forward request to next proxy (fe80::3)
- ▶ Point request state to previous proxy (fe80::1)



Proxy-level
Forwarding Information Base

Destination	Next-hop
2001:db8::4 /sensor	fe80::3

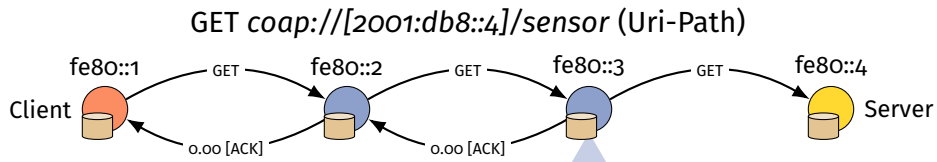
Request Table

Cache Key	Source
Key _i	fe80::1

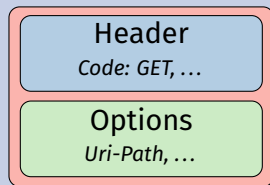
Cache

Cache Key	Response
—	—

Forwarding Details



- ▶ Acknowledge with empty response
- ▶ Forward request to global address (2001:db8::4)
- ▶ Point request state to previous proxy (fe80::2)



Proxy-level
Forwarding Information Base

Destination	Next-hop
—	—

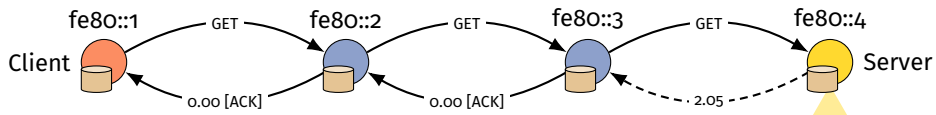
Request Table

Cache Key	Source
Key _i	fe80::2

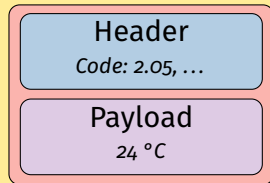
Cache

Cache Key	Response
—	—

Forwarding Details



► Reply with sensor data



Proxy-level
Forwarding Information Base

Destination	Next-hop
—	—

Request Table

Cache Key	Source
—	—

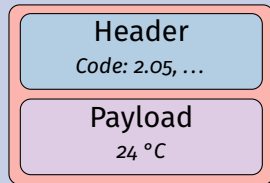
Cache

Cache Key	Response
—	—

Forwarding Details



- Forward response to fe80::2
- Consume request state



Proxy-level
Forwarding Information Base

Destination	Next-hop
—	—

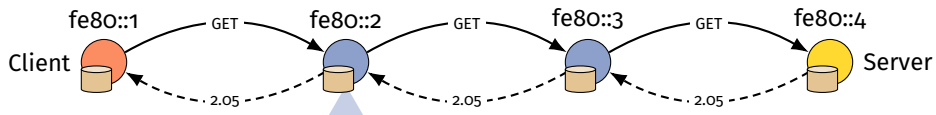
Request Table

Cache Key	Source
Key _i	fe80::2

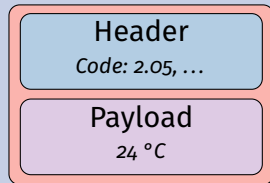
Cache

Cache Key	Response
Key _i	Resp _i

Forwarding Details



- ▶ Forward response to fe80::1
- ▶ Consume request state



Proxy-level
Forwarding Information Base

Destination	Next-hop
2001:db8::4/sensor	fe80::3

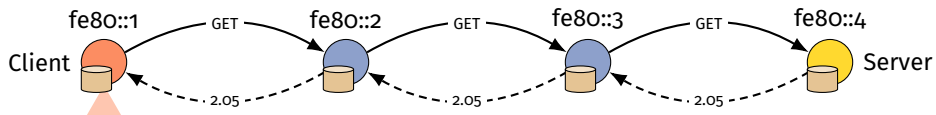
Request Table

Cache Key	Source
Key _i	fe80::1

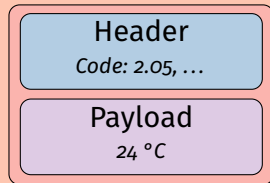
Cache

Cache Key	Response
Key _i	Resp _i

Forwarding Details



- Receive response at application
- Consume request state



Proxy-level
Forwarding Information Base

Destination	Next-hop
2001:db8::4/sensor	fe80::2

Request Table

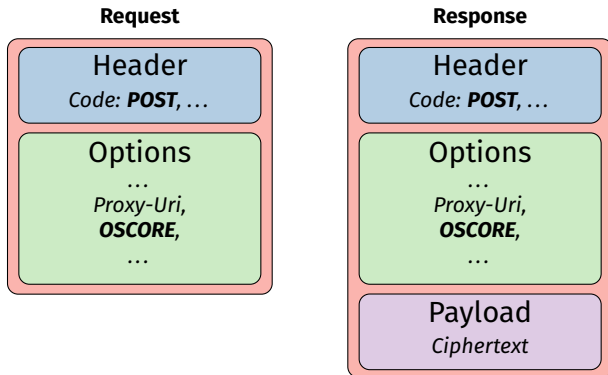
Cache Key	Source
Key _i	::1/128

Cache

Cache Key	Response
Key _i	Resp _i

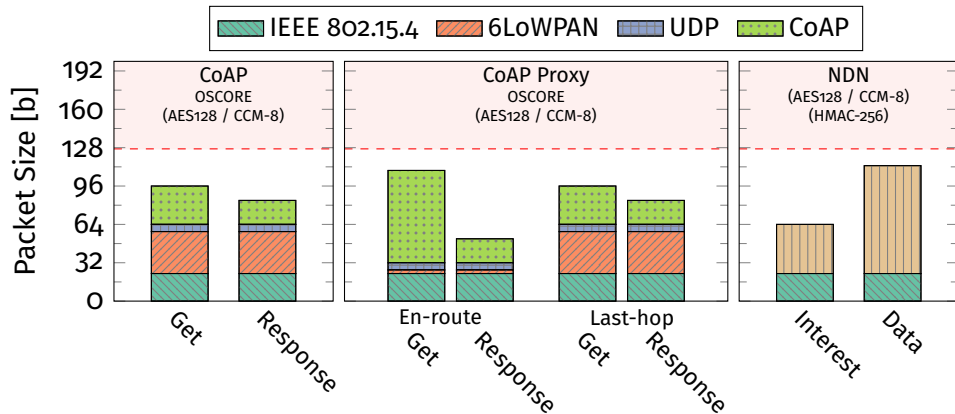
OSCORE: Content Object Security

- ▶ Provides confidentiality, integrity, and replay mitigations
- ▶ Wraps CoAP in CoAP with method: POST
- ▶ Proxy-Uri remains outside OSCORE (host part only? with path?)
- ▶ Trade-off: fine-grained forwarding control vs. privacy



Packet Structure Dissection

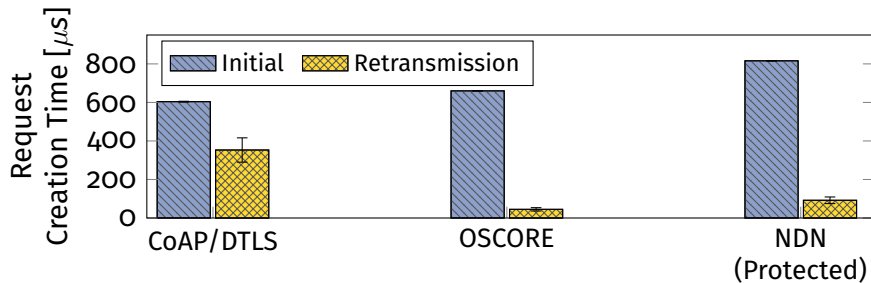
- ▶ Maximum frame size for IEEE 802.15.4 is 127 bytes



Stateful proxying reduces en-route message size (link-local addr. compression)

Request Creation Time

- ▶ Message retransmissions are frequent in low-power regimes
- ▶ **CoAP**: Application layer retransmissions
- ▶ **NDN**: Network layer retransmissions



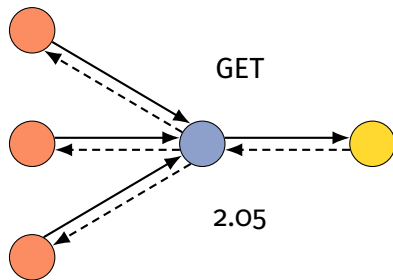
Content object security reduces strain on retransmissions

Enabling a Reliable Multiparty Content Retrieval

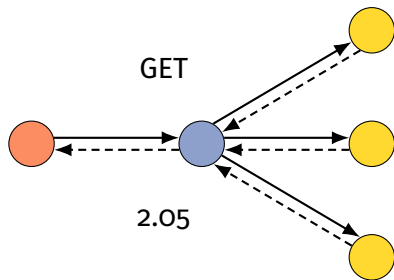
Multi-party Communication

- ▶ CCNx / NDN has integral support for multi-party communication
- ▶ Data-centric CoAP deployments inherit the same feature set

**Request aggregation &
Response fan-out**



**Request fan-out &
Response deduplication**



Problems with Naïve OSCORE Integration

Stateful Forwarding

- ▶ Strong message binding of OSCORE confines request aggregation to request-response pairs
- ⇒ single-party, single-request

Caching

- ▶ Cryptographic protection of OSCORE naturally prevents data access for other peers
- ⇒ single-party, single-request

[IEEE LCN'21] RESTful Multiparty Access to a Data-Centric WoT [...]

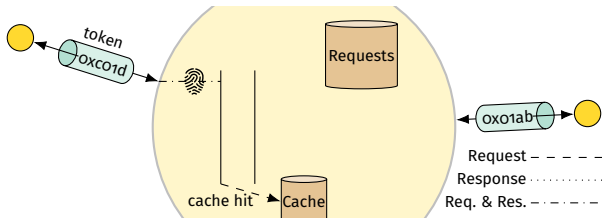
Extending the Data-centric WoT

Multiparty cache utilization

- ▶ Members assume role of a virtual client (draft-amsuess-core-cacheable-oscore)
- ▶ Iterated requests from a virtual client to same resource are identical

Multiparty forwarding

- ▶ Requests aggregate per cache key
- ▶ Responses fan out to all matching requests



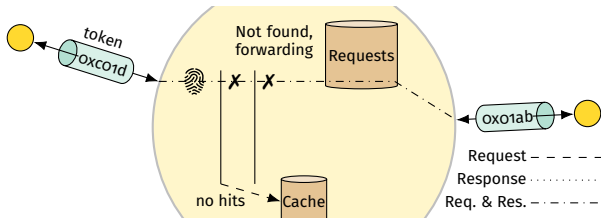
Extending the Data-centric WoT

Multiparty cache utilization

- ▶ Members assume role of a virtual client (draft-amsuess-core-cacheable-oscore)
- ▶ Iterated requests from a virtual client to same resource are identical

Multiparty forwarding

- ▶ Requests aggregate per cache key
- ▶ Responses fan out to all matching requests



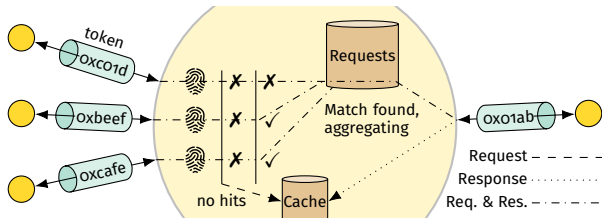
Extending the Data-centric WoT

Multiparty cache utilization

- ▶ Members assume role of a virtual client (draft-amsuess-core-cacheable-oscore)
- ▶ Iterated requests from a virtual client to same resource are identical

Multiparty forwarding

- ▶ Requests aggregate per cache key
- ▶ Responses fan out to all matching requests



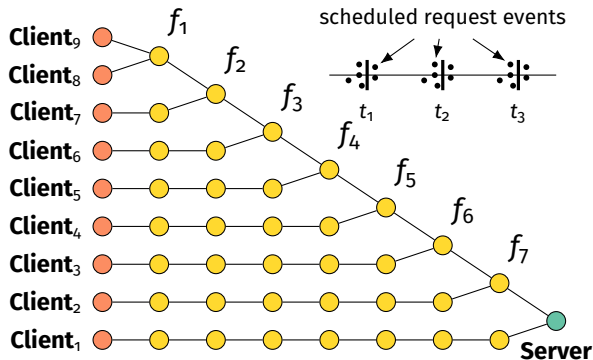
Testbed Setup

Hardware M3 node in IoT Lab testbed,
IEEE 802.15.4

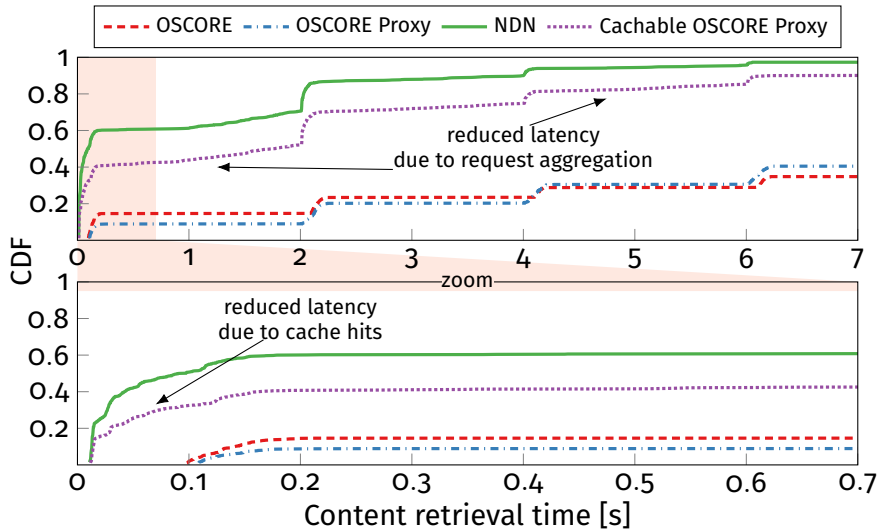
Software 

Topology 9 clients, 35 forwarders,
1 server

Scenario Clients request latest
instruction every ≈ 1 s



Time to Content Arrival (Client₉)



Request aggregation and caching improve network performance

Use Case: Firmware Update

Data-centric Firmware Propagation

Motivation

- ▶ General purpose devices require software updates
- ▶ Increasing security demands require similar practices for IoT

A secure and reliable firmware propagation in low-power regimes is mandatory

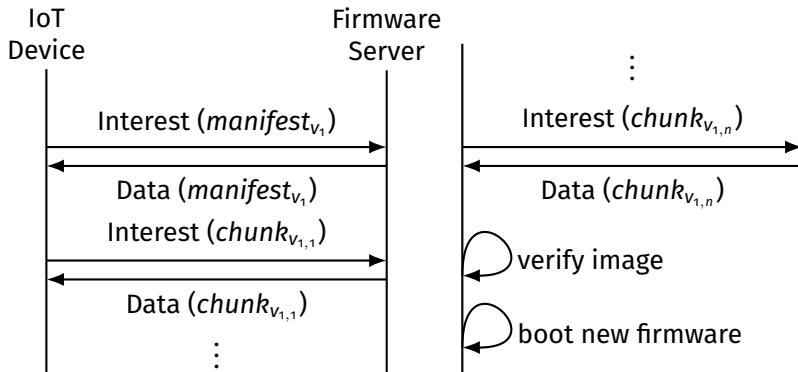
Challenges

- ▶ Updates are resource-consuming and show as peak loads in the Internet
- ▶ IoT firmware images are 1–2 orders of magnitude larger than sensor values

Update propagations can lead to DDoS and break security

Firmware Retrieval

- ▶ NDN interchangeable with data-centric CoAP block-wise transfer



[ACM ICN'21] Reliable Firmware Updates for the information-centric IoT [...]

Retrieval Strategies

Concurrent Retrievals

- ▶ Nodes retrieve missing chunks and also forward to downstream nodes
- ▶ Multiple nodes on a path perform update concurrently

Cascading Retrievals

- ▶ Nodes block downstream chunk requests while local retrieval is running
- ▶ Single node on a path performs update at a time

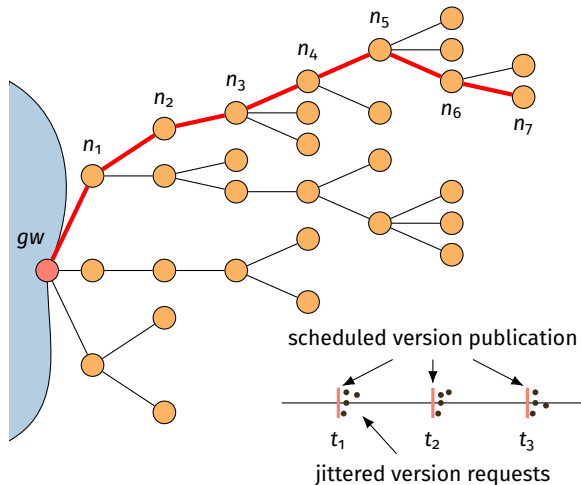
Experiment Setup

Hardware M3 node in IoT Lab testbed,
IEEE 802.15.4

Software 

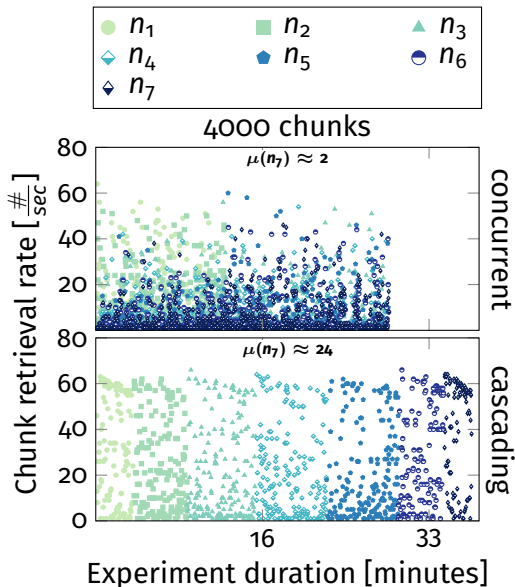
Topology 30 devices, 1 gateway

Scenario Devices request new
firmware version



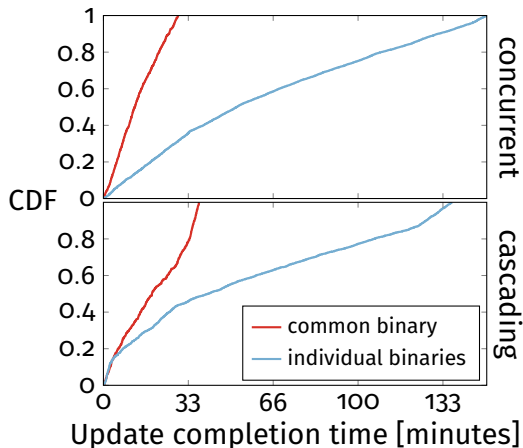
Goodput Analysis

- ▶ All devices download 128KiB common firmware image
- ▶ Concurrent retrievals saturate network resources
- ▶ Cascading retrievals shorten nodal update time



Update Completion Time

- ▶ All devices download 128KiB firmware image
- ▶ Common binary benefits from hop-wise cache hits
- ▶ Individual binaries degrade overall network performance



Conclusion & Outlook

Takeaways

- ▶ Hop-wise content replication fosters efficient, reliable disseminations
- ▶ Stateful forwarding & object security enable secure multi-party comm.
- ▶ Data-centric CoAP brings new perspectives for IoT deployments

Future Work

- ▶ Inspect dynamic proxy discovery
- ▶ Explore alternative identifiers in Proxy-Uri