The Data-centric Web of Things: From Network Research to Standardized Networking

Prof. Dr. Thomas Schmidt

http://inet.haw-hamburg.de | t.schmidt@haw-hamburg.de

IoT: Connecting the Physical World to the Internet

Industrial Automation

IoT: Connecting the Physical World to the Internet

Industrial Automation

Connected Vehicles

IoT: Connecting the Physical World to the Internet

Industrial Automation

Connected Vehicles

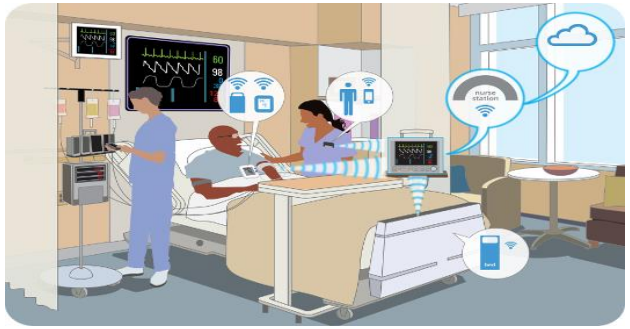
Smart Homes

IoT: Connecting the Physical World to the Internet

Industrial Automation

Connected Vehicles

Smart Homes



eHealth

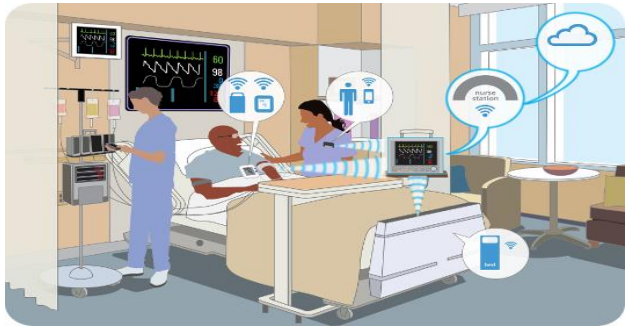
IoT: Connecting the Physical World to the Internet

Micro- & Nano Satellites

Industrial Automation

Connected Vehicles

Smart Homes



eHealth

Use Case: Gas Detection

- Harsh industrial environments
  - Dangerous events may occur
    - Gas exposure: toxic or combustible
    - Oxygen depletion
    - Gas leaks and flames
  - Areas are heavily regulated
    - Constrained access
    - Mandatory equipment
    - Mission protocols and logs

Resilience and timing are key requirements

Outline

- The Internet of Small Things with RIOT
- IoT Networking: Insights from Experimentation
- Security: Channel vs. Content Object
- Data-centric Web of Things with CoAP and OSCORE

The many faces of IoT

High-end IoT

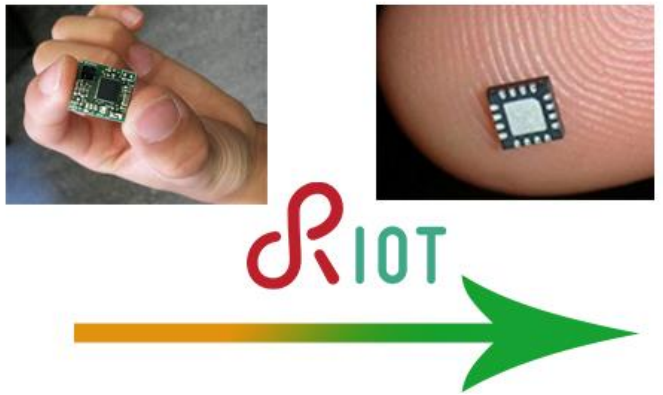
Processor: GHz, 32/64 Bit
Memory: M/Gbytes
Energy: Watt
Network access: 5G, WLAN

The many faces of IoT

High-end IoT

Processor: GHz, 32/64 Bit
Memory: M/Gbytes
Energy: Watt
Network access: 5G, WLAN

Low-end (or constrained) IoT



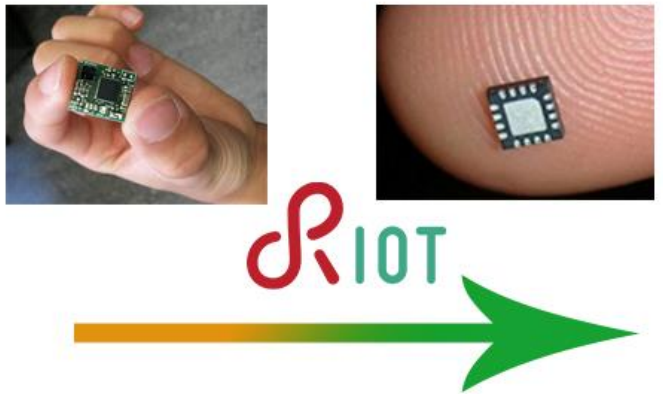
Processor: MHz, 8/16/32 Bit
Memory: kbytes
Energy: MWatt
Network access: 802.15.4, BLE, LoRA, NB-IoT

Microcontrollers are the challenging class of devices

High-end IoT

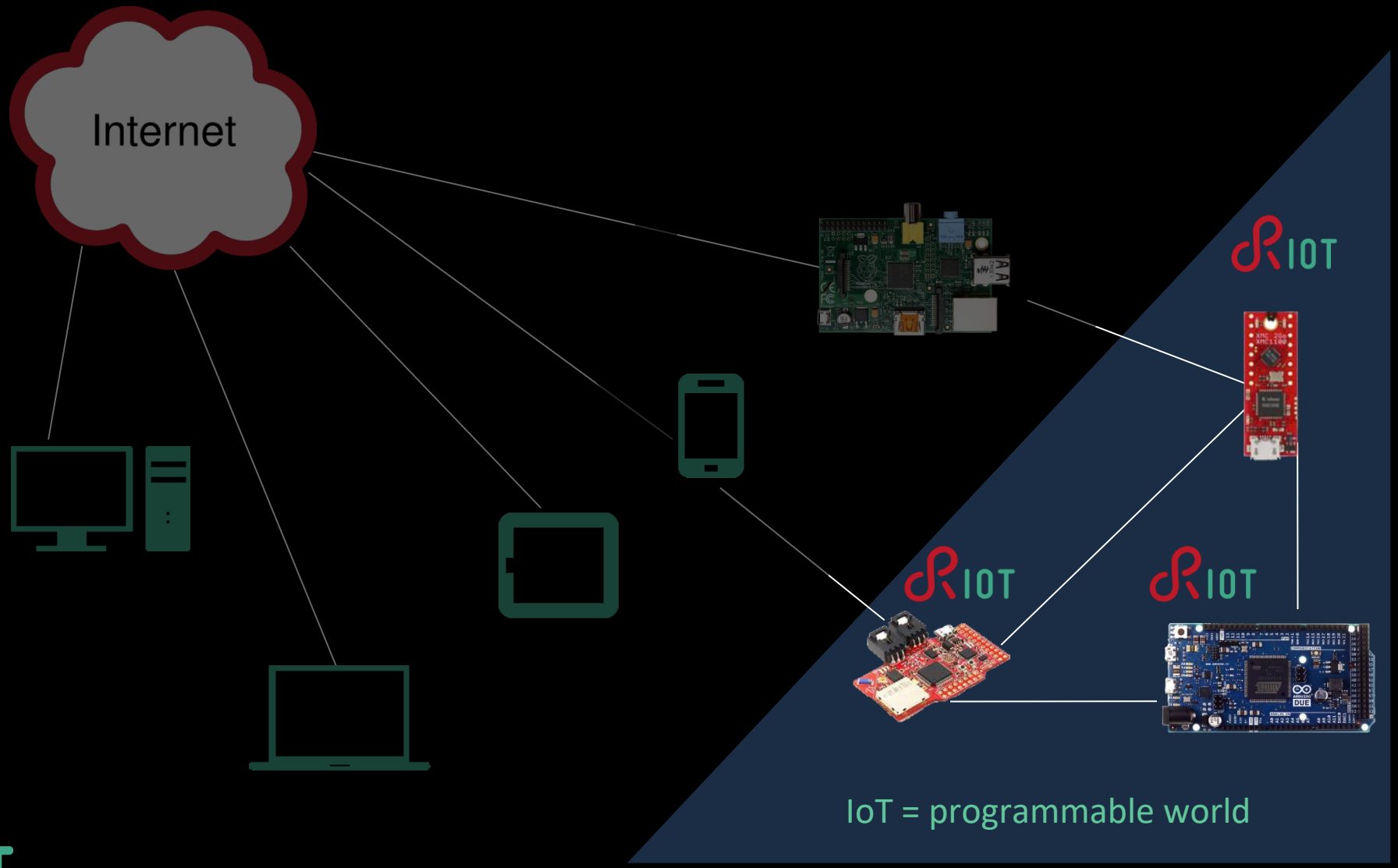
Processor: GHz, 32/64 Bit
Memory: M/Gbytes
Energy: Watt
Network access: 5G, WLAN

Low-end (or constrained) IoT



Processor: MHz, 8/16/32 Bit
Memory: kbytes
Energy: mWatt
Network access: 802.15.4, BLE, LoRA, NB-IoT

RIOT: The Friendly OS for the IoT



IOT

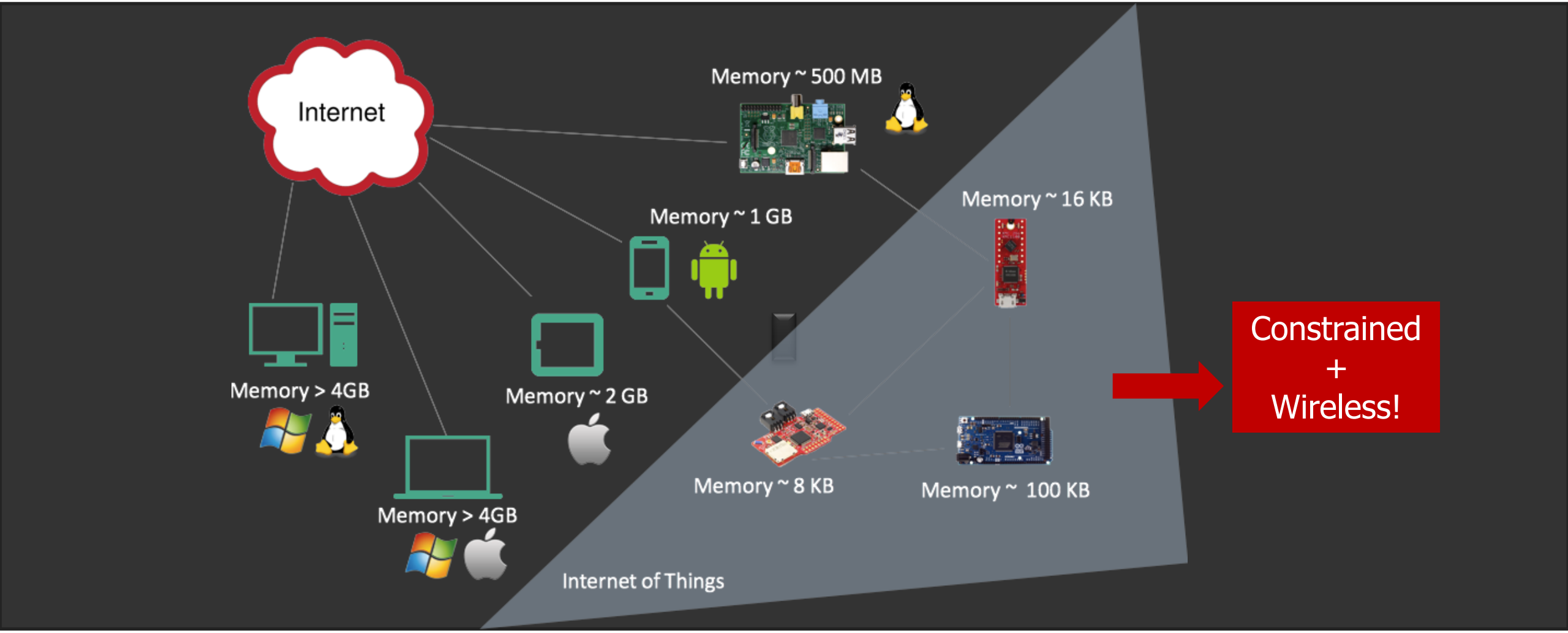
If your IoT device cannot run Linux, then run

RIOT

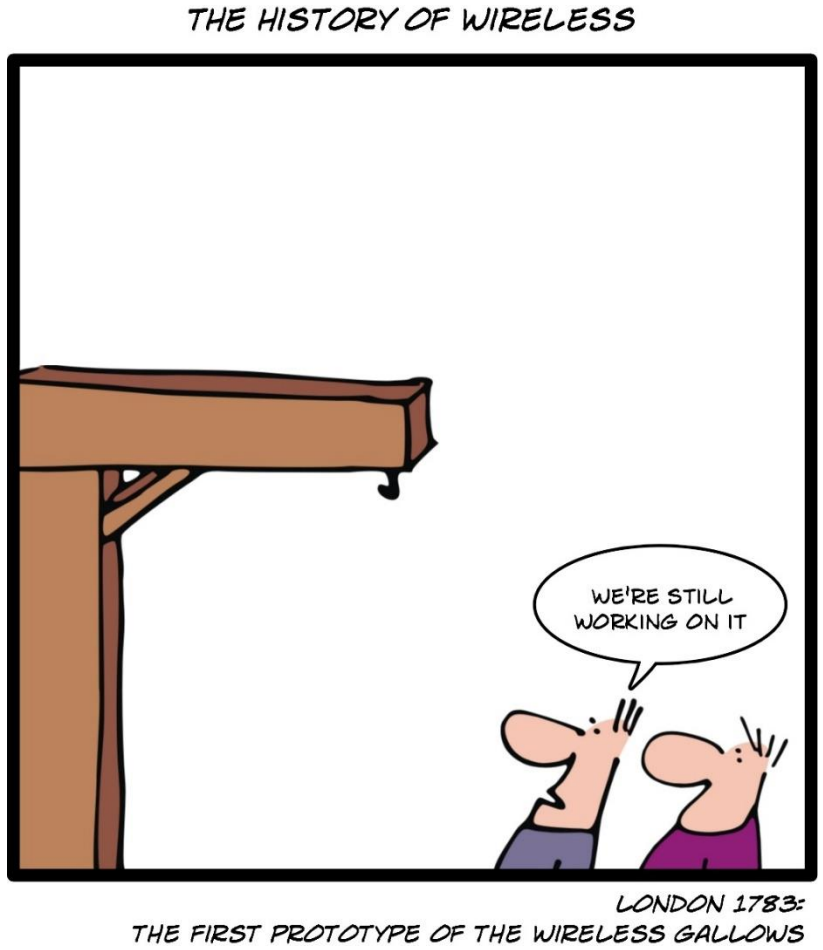
RIOT: Facts sheet

- Microkernel architecture (for robustness)
  - The kernel itself uses ~1.5K RAM @ 32-bit
- Efficient hardware abstraction (for portability)
- Tickless scheduler (for energy efficiency)
- Deterministic O(1) scheduling (for real-time)
- Low latency interrupt handling (for reactivity)
- Modular structure (for adaptivity)
- Preemptive multi-threading & powerful IPC
- Appealing API, support for ≈ 250 boards

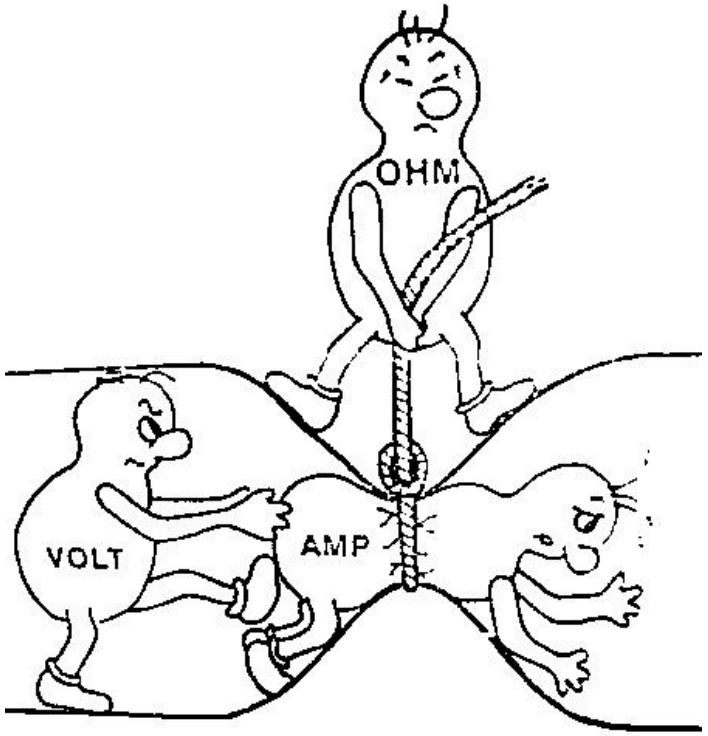
The Constrained Internet of Things (IoT)



Low Power Lossy Wireless



Key problem: Energy



HAW HAMBURG

Large-scale Testbed Experimentation

IOT NETWORKING

HAW HAMBURG

How can we build reliable and robust networking on top of these low-power lossy wireless links?

WSN History: Directed diffusion (Intanagonwiwat et al. `03)

Make Wireless Sensor Networks robust by

1. Request/Response data access with reverse path forwarding
2. Hop-wise data transfer
3. In-network caching

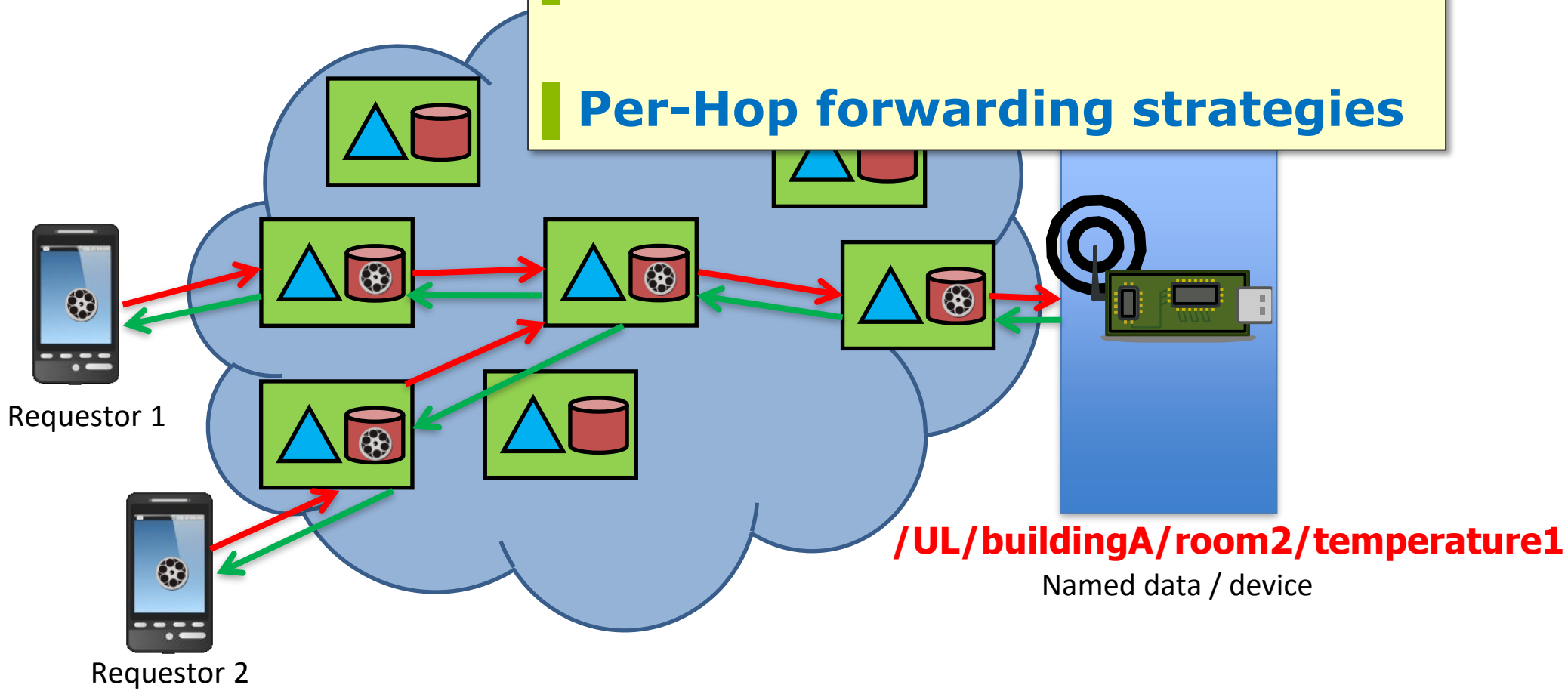
Networking Named Content (Jacobson `09)

NDN leads Information Centric Networking

- Accessing Data by Name
  - no addresses involved
- Hop-wise Data Replication
- Content Object Security
- Adaptive Forwarding
- In-network Caching
- Asynchronous Multi-Fanout

Information Centric Networking (ICN)

- Accessing Named Data Objects
- Data-centric security approach
- Ubiquituous Caching
- Per-Hop forwarding strategies



Our Approach: Experimentally Driven Research

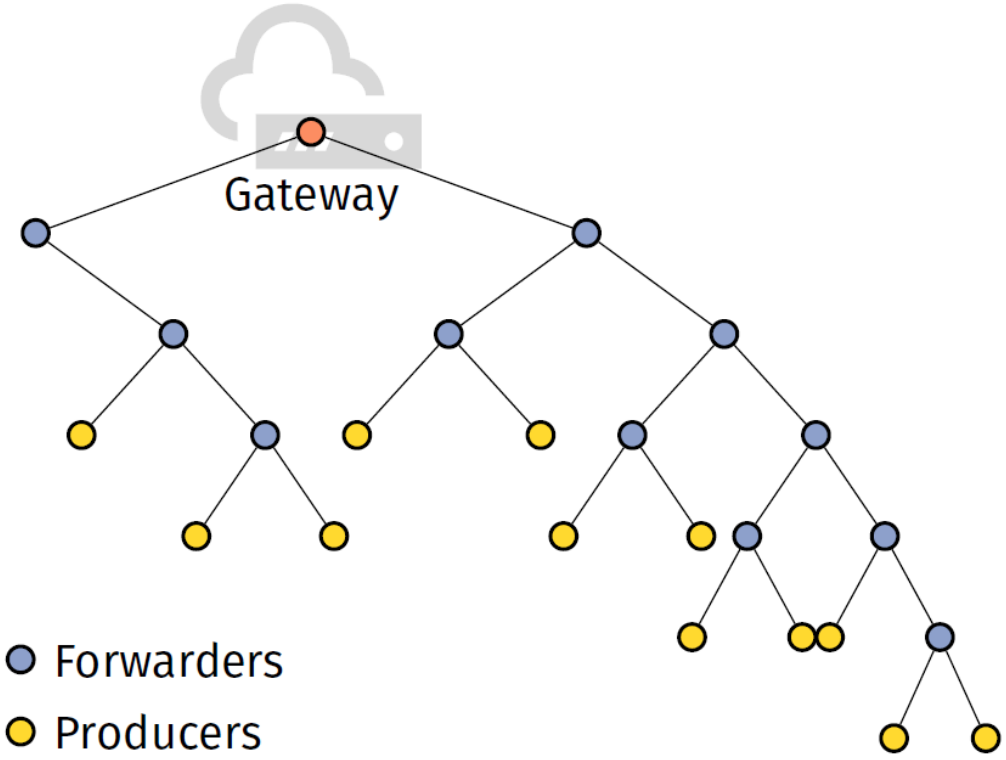
Multihop IoT networks:

FIT IoT Testbed (Inria)

Topology: Trees of 20 to 200 forwarders and producers

Hardware: M3 node, 802.15.4/BLE/LoRa

Software: RIOT



RIOT Network Stacks

CoAP with Proxy

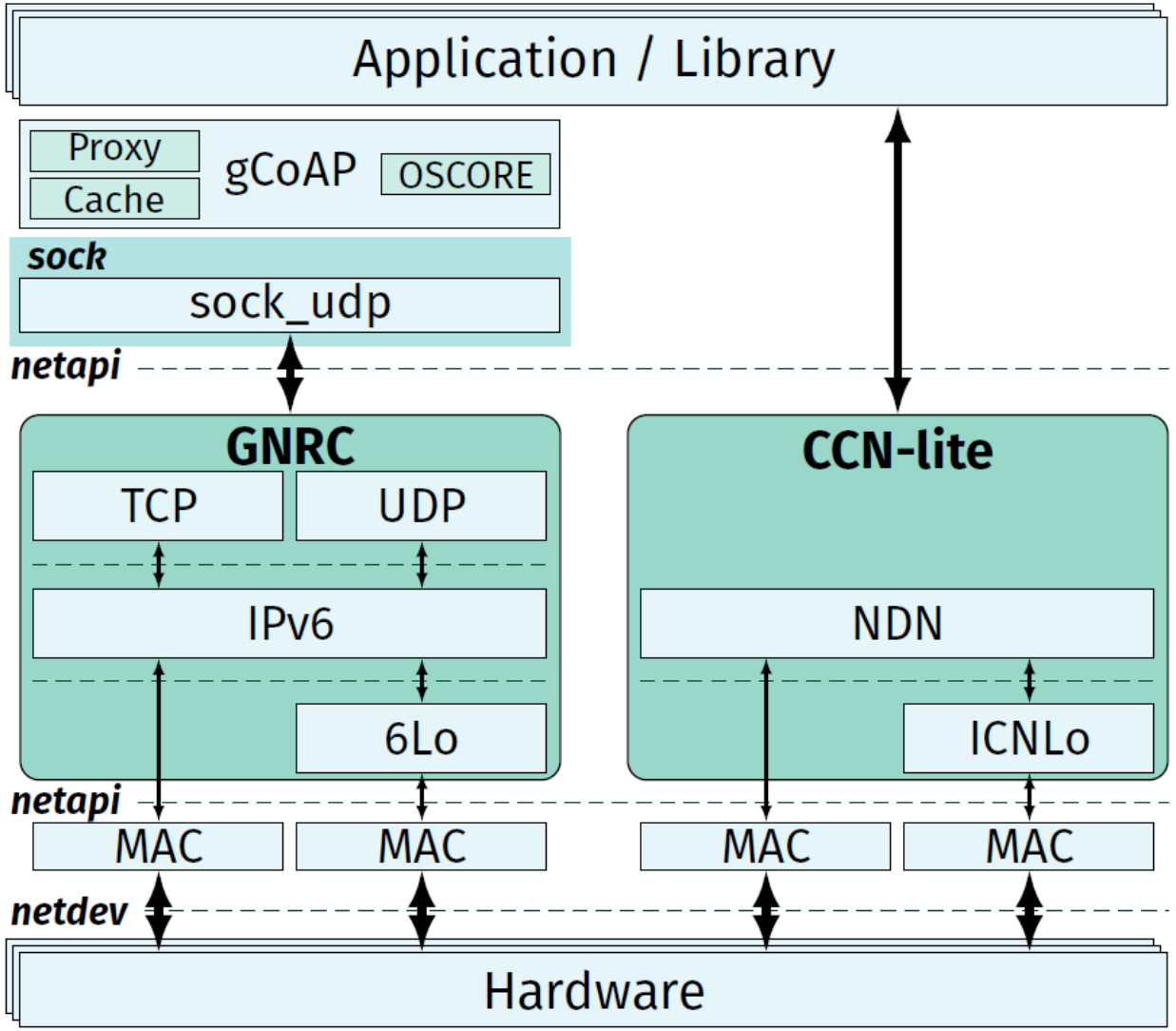
- Stateful proxying and caching in gCoAP

CoAP with OSCORE

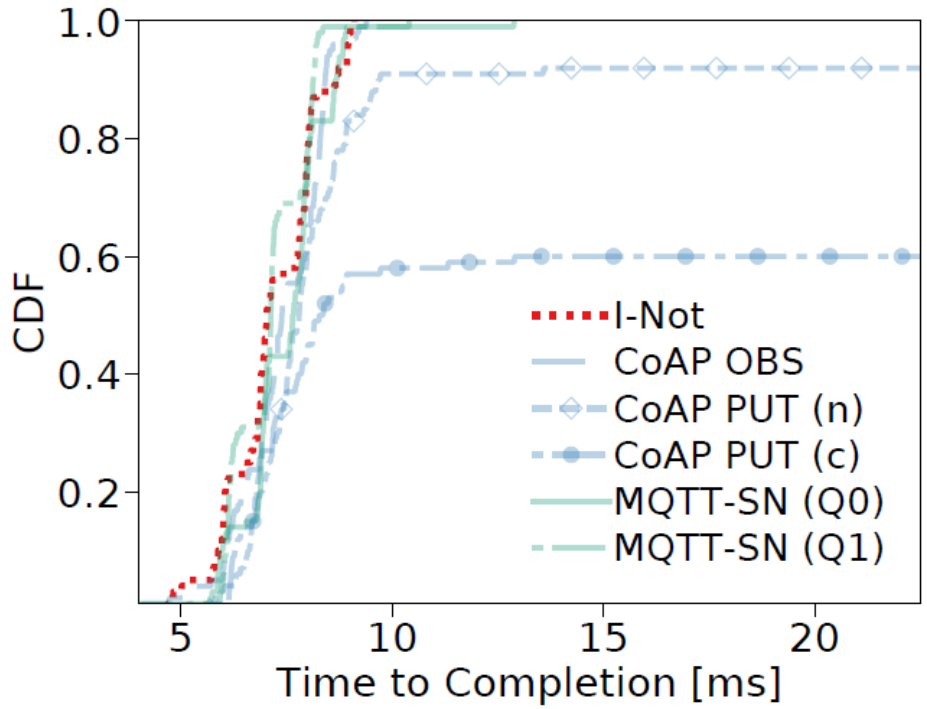
- gCoAP integrates libOSCORE package

NDN with CCN-lite

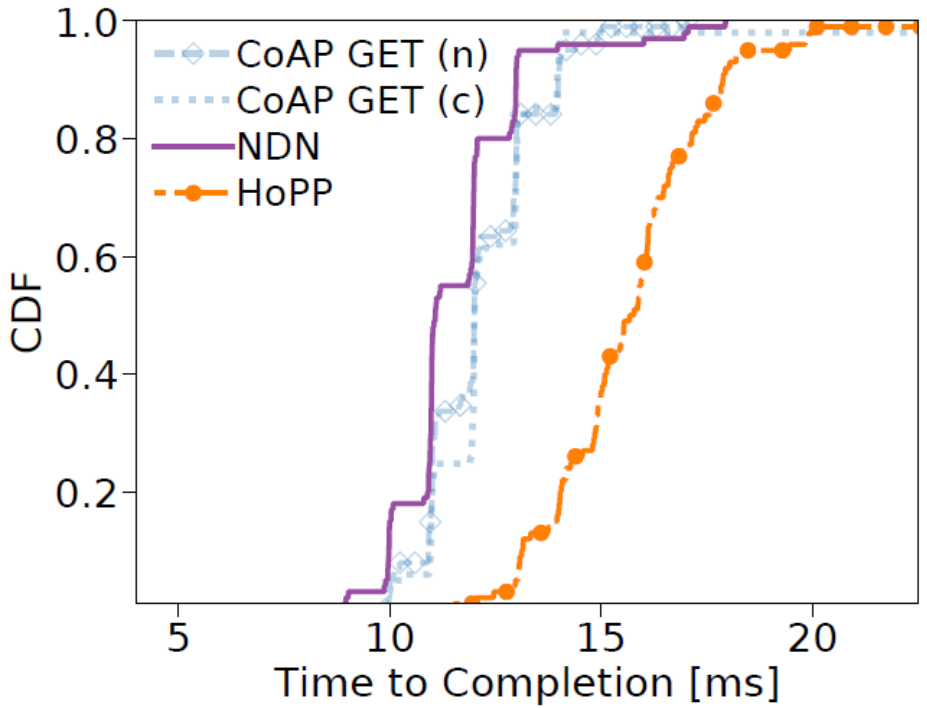
- CCN-lite integrates into RIOT networking



Single Hop: Push versus Pull



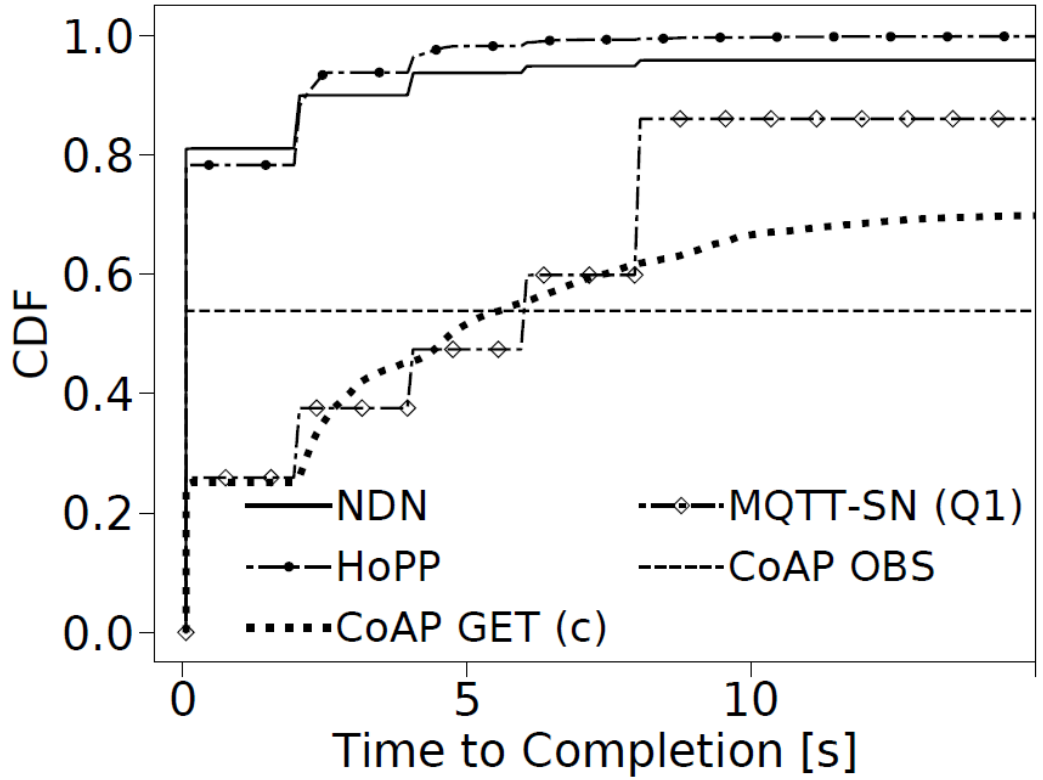
Push protocols



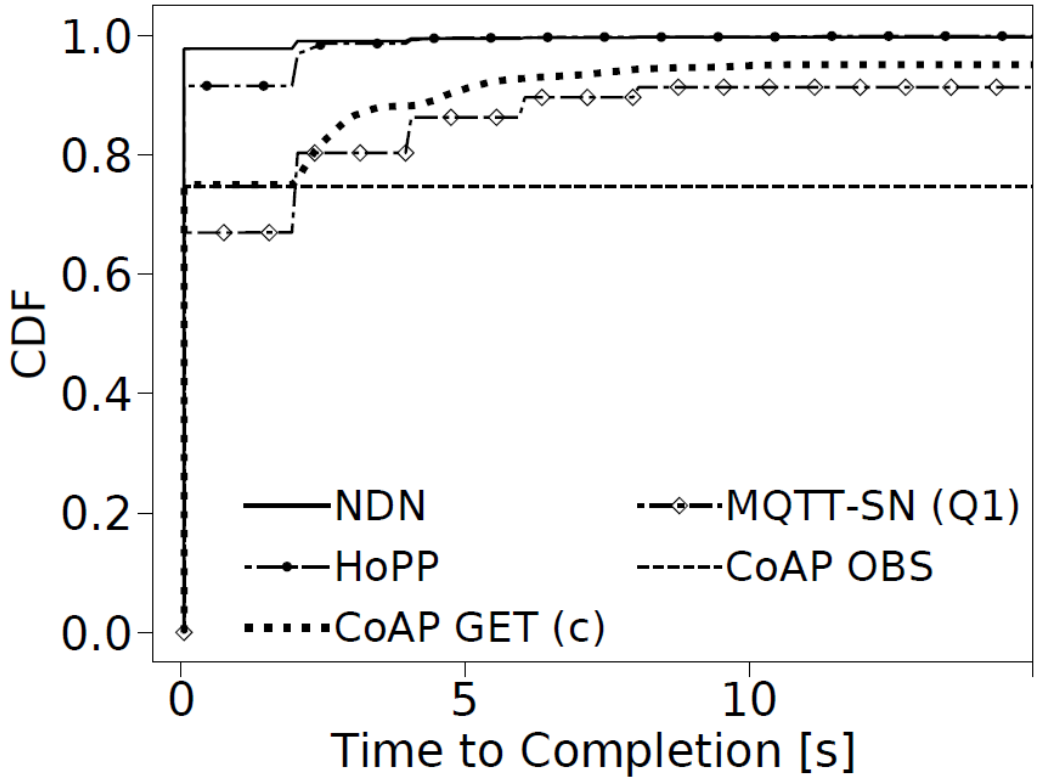
Pull protocols

Publishing Interval: 50 ms

The Multihop Case

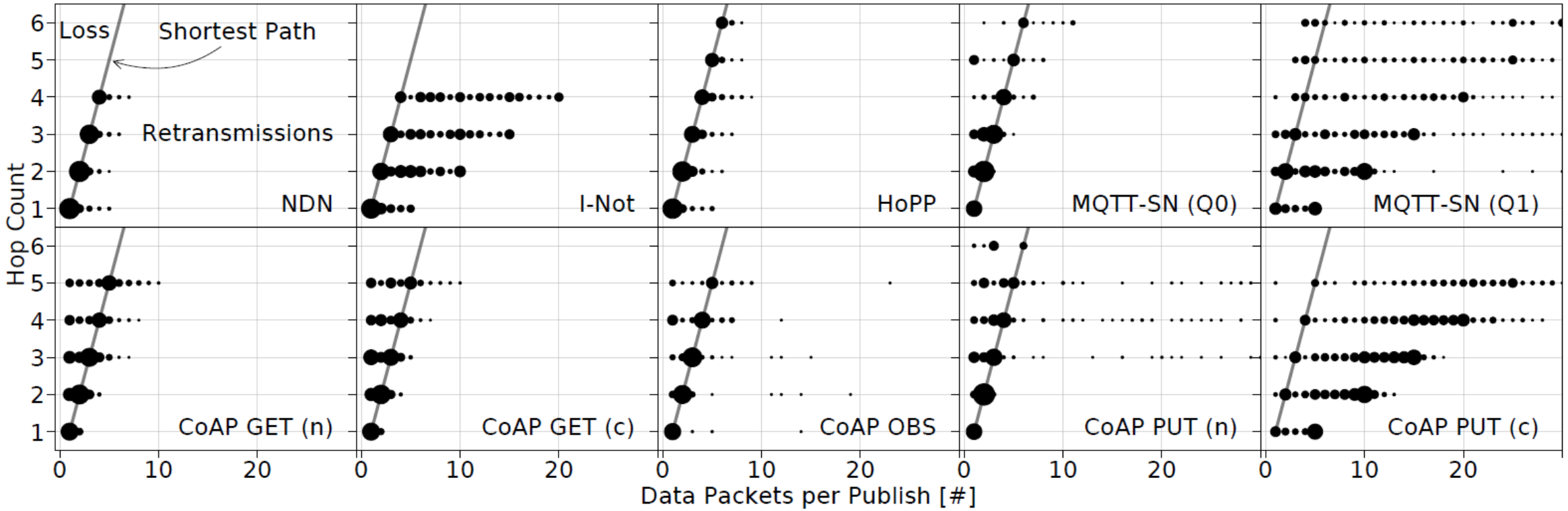


(a) 5 s publishing interval

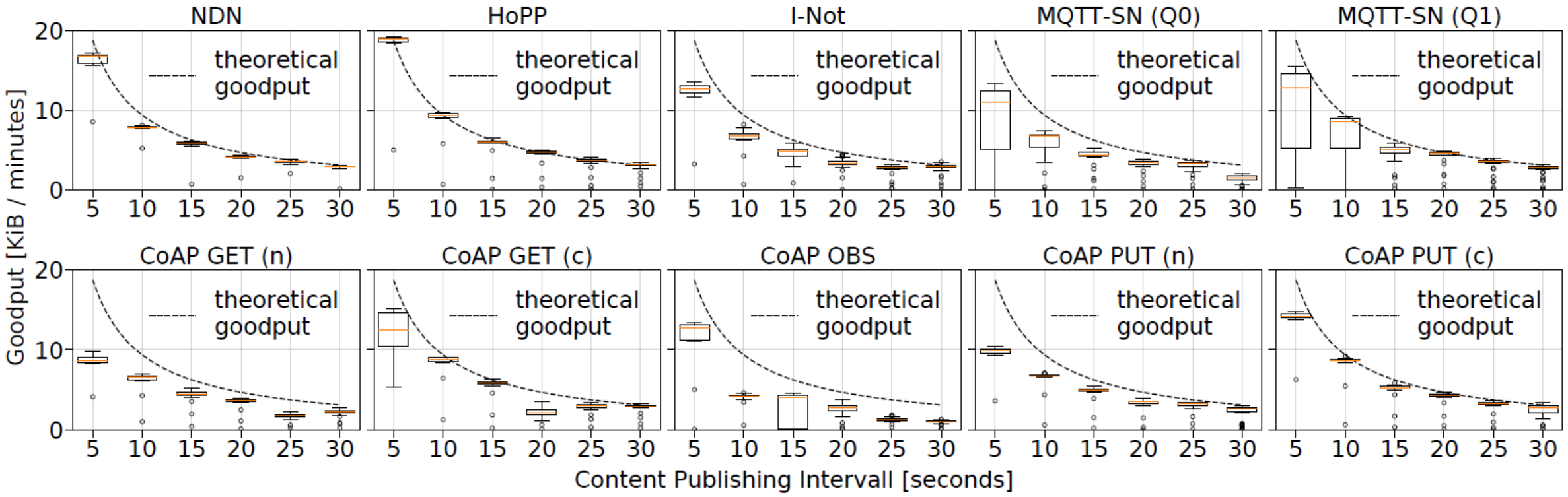


(b) 30 s publishing interval

Behind the Scene: Link Stress



Effectiveness: Networking Goodput

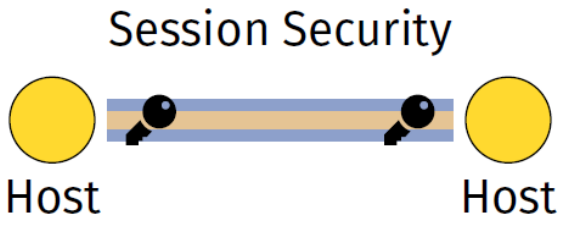


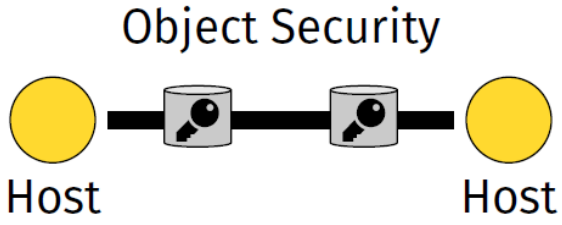
How to Secure Content in Networks?

SECURITY

Two Approaches to Securing Content in the Net

- Session security: securing channels
  - Requires session establishment
  - Well known approach from (D)TLS
- Content object security: securing content
  - Enables content replication and caching
  - New approach with NDN and OSCORE





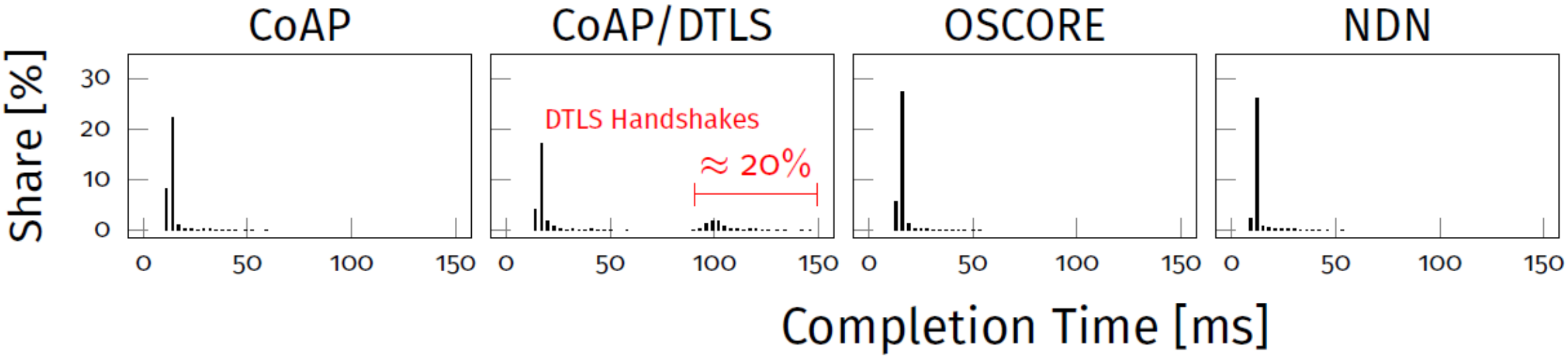
Comparison of Security Properties

	CoAP		NDN
	DTLS	OSCORE	Protected
Request Message			
Integrity	✓	✓	(✓)
Authenticity	✓	✓	(✓)
Confidentiality	✓	✓	✘*
Response Message			
Integrity	✓	✓	✓
Authenticity	✓	✓	✓
Confidentiality	✓	✓	✘*

* provided on application layer

Performance Impact

- Security data increases packet sizes
- DTLS session establishment is susceptible to late retries
- OSCORE and NDN remain lean



HAW HAMBURG

Back to standards

DATA-CENTRIC WOT

HAW HAMBURG

NDN is incompatible with the Internet: Can we build an ICN-style Internet only with restful standard protocols?

How to Best Access Content in the WoT?

Problems with End-to-End data delivery

- Constrained devices shielded by gateways
- Transcoding gateways break E2E security
- Multi-hop forwarding in lossy regimes
- Changing paths by link flux and mobility

Alternative transport concepts

- Information-centric data replication
- WoT relies on REST access by CoAP

Lessons Learned from Information Centric Networking

Performance Boosts from 10 Years of Research

Adaptive Forwarding

In-network Caching

Content Object Security

Adaptive 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

Lessons Learned from Information Centric Networking

Performance Boosts from 10 Years of Research

Adaptive Forwarding	In-network Caching	Content Object Security
	CoAP Proxy	OSCORE

Adaptive 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

Smart & Resilient Network Layer

- Hop-wise Data Replication
- Content Object Security
- Adaptive Forwarding
- In-network Caching
- Asynchronous Multi-Fanout
- RESTful Access with CoAP

Smart & Resilient Network Layer

Data-Centric Web of Things

- Hop-wise Data Replication
- Content Object Security
- Adaptive Forwarding
- In-network Caching
- Asynchronous Multi-Fanout
- RESTful Access with CoAP

Forwarding OSCORE Content Objects w/ Proxies

Cacheability

- Strong response binding prevents cache hits for subsequent requests
- Use retransmission caches to recover messages of same transaction

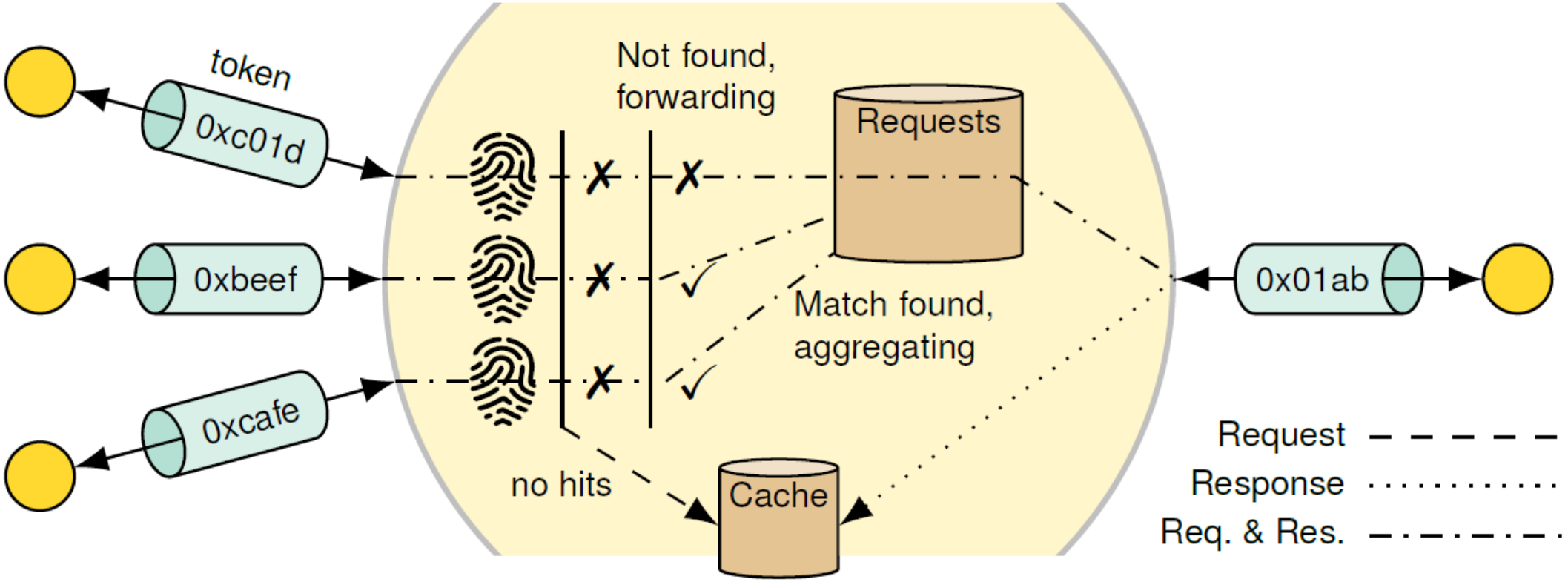
Proxy on each forwarding node

- OSCORE Objects cached
- Hop-wise message timeout
- Retransmissions on each forwarder

Decoupling of data from location

- Link-local IP addressing
- Forwarding via resource name

Forwarding and Caching with CoAP Proxy



Group Capabilities in OSCORE

Protocol	Caching	Request Aggregation	Response Fan-out
OSCORE	—	—	—
OSCORE Proxy	single party	only retransmissions	—
Deterministic OSCORE Proxy	multiple parties	multiple parties	✓
NDN	multiple parties	multiple parties	✓

Constructing a Data-Centric Web of Things

Communication Model & Flow Control

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

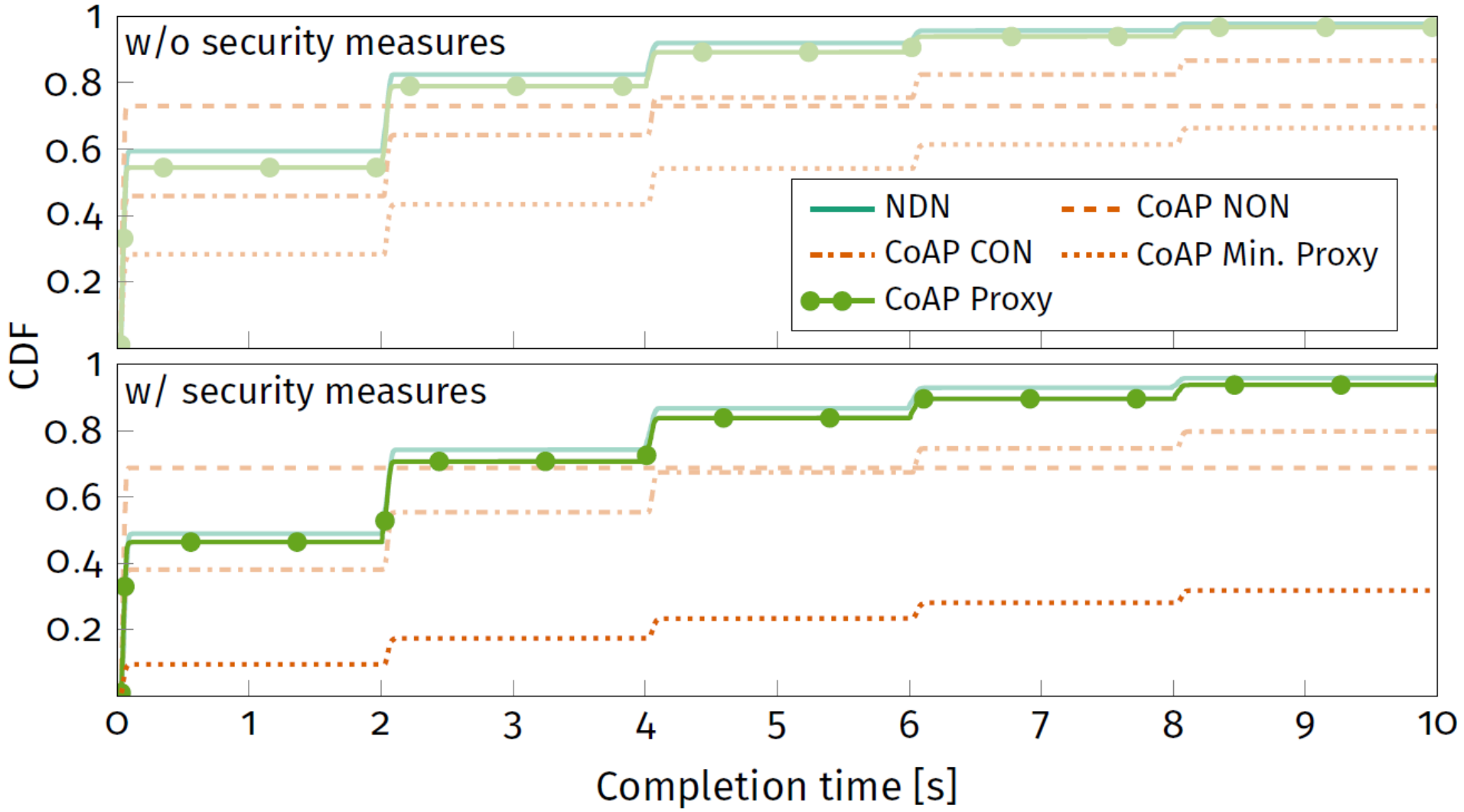
Adaptive Forwarding & Caching

- CoAP proxies forward requests and build reverse path
- Proxies cache incoming responses

Content Object Security

- OSCORE provides authenticated encryption
- End-to-end security persists across gateways

Time to Content Arrival



Takeways

Almost 20 years of research favor ICN principles for the IoT

1. Named access to data
2. Hop-by-hop data transfer
3. Content object security
4. In-network caching

We are now arriving at standard Internet protocols to support this

- CoAP w/ Proxy
- (Group-) OSCORE

Let’s start to build a Data-centric Web of Things!

Thanks & Questions ?