Secure and Authorized Client-to-Client Communication for LwM2M

Leandro Lanzieri [1], Peter Kietzmann [1], Thomas C. Schmidt [1], Matthias Wählisch [2]

RIOT Summit 2023

18th September 2023 – Frankfurt, Germany

leandro.lanzieri@haw-hamburg.de

HAW HAMBURG

Freie Universität Berlin

IoT Challenges

Vendor Incompatibility

Security Requirements

Device Constraints

Edge Collaboration

IoT Challenges

LwM2M

- Vendor Incompatibility
- Security Requirements
- Device Constraints
- Edge Collaboration

IoT Challenges

LwM2M

Our LwM2M Extensions

Vendor Incompatibility

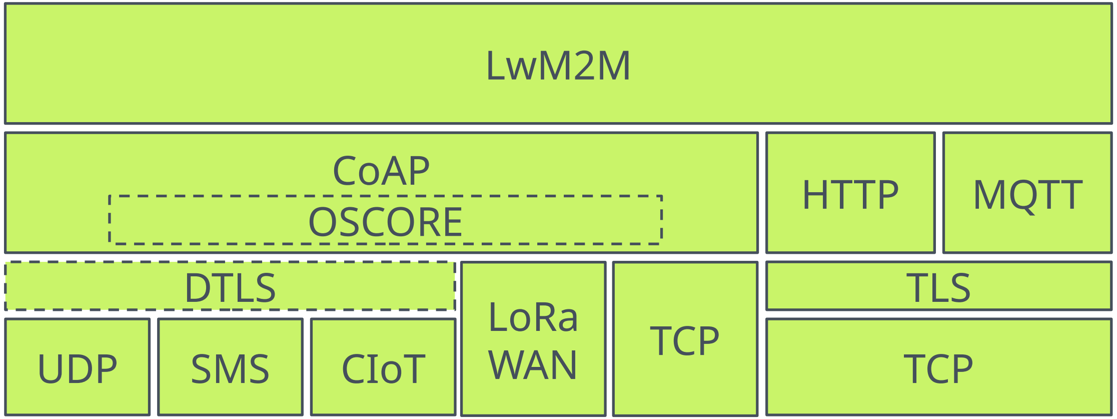
Security Requirements

Device Constraints

Edge Collaboration

LwM2M Overview

LwM2M Protocol Stack



LwM2M

CoAP

OSCORE

HTTP

MQTT

DTLS

LoRa WAN

TCP

TLS

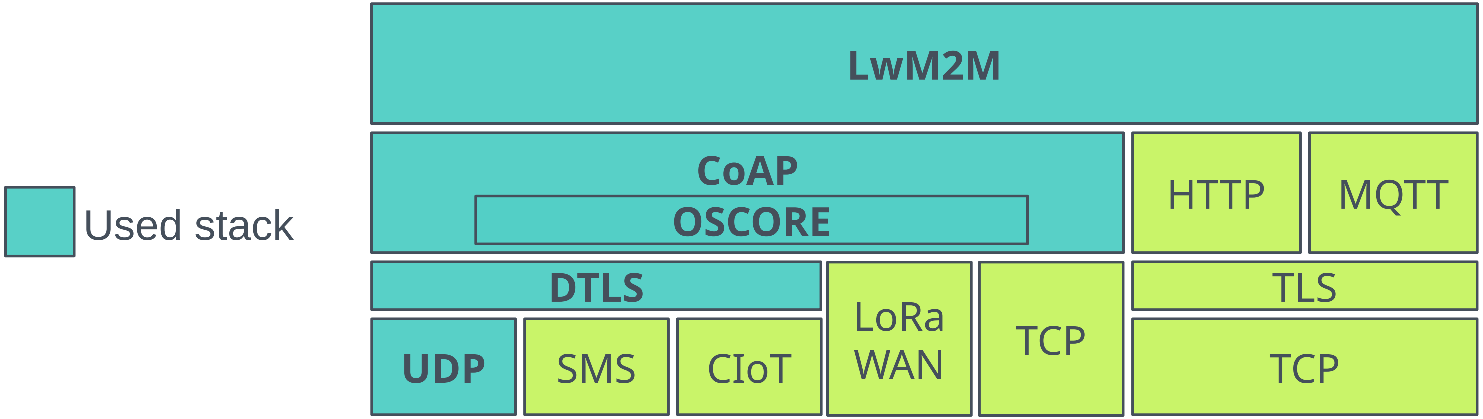
UDP

SMS

CIoT

TCP

LwM2M Protocol Stack



🟦 Used stack

LwM2M

CoAP

OSCORE

HTTP

MQTT

DTLS

LoRa WAN

TCP

TLS

UDP

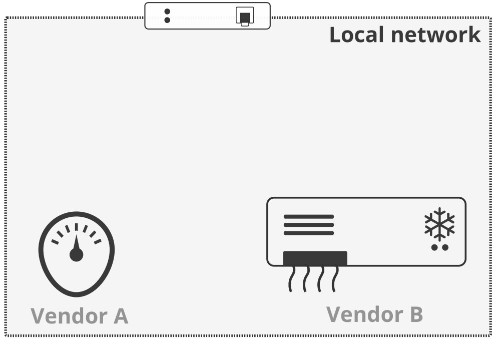
SMS

CIoT

TCP

LwM2M Background

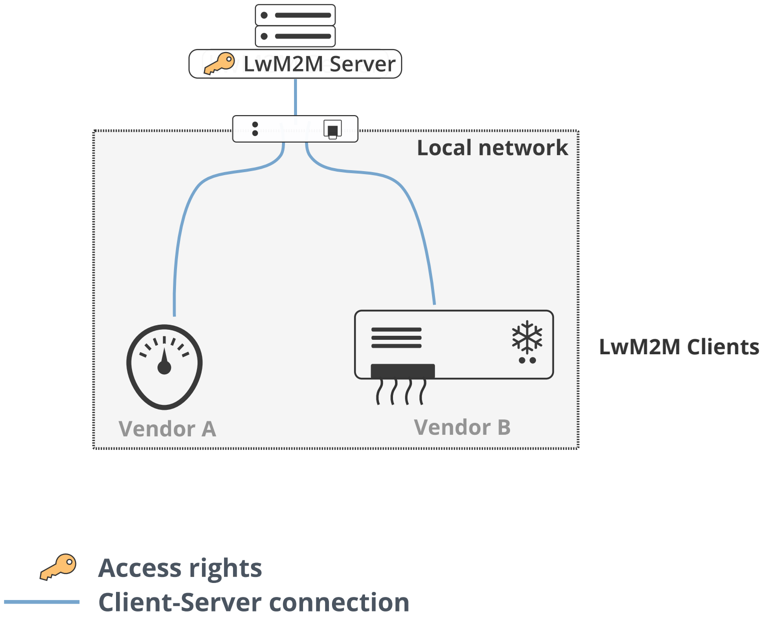
- **IoT Device management**
  - Semantic interoperability across vendors
  - Resource access control
  - Bootstrapping and software updates



LwM2M Background

- IoT Device management
  - Semantic interoperability across vendors
  - Resource access control
  - Bootstrapping and software updates

- **Two main entity types**
  - LwM2M Clients (IoT devices)
  - LwM2M Servers

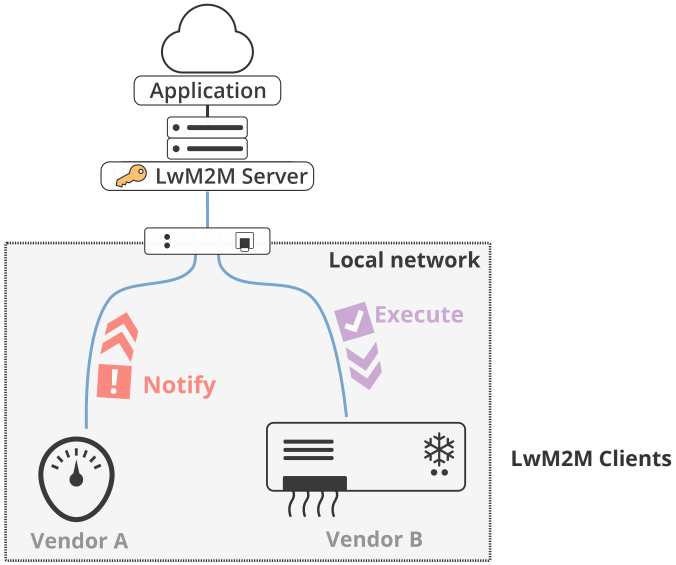


LwM2M Background

- **IoT Device management**
  - Semantic interoperability across vendors
  - Resource access control
  - Bootstrapping and software updates

- **Two main entity types**
  - LwM2M Clients (IoT devices)
  - LwM2M Servers

- **Only Servers perform operations on Clients**
  - Using established secure communication
  - Credentials and access rights are required
  - IoT applications interact with Clients only through Servers



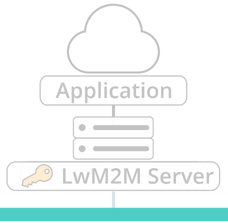
🔑 Access rights

— Client-Server connection

LwM2M Background

- **IoT Device management**
  - Semantic interoperability across vendors

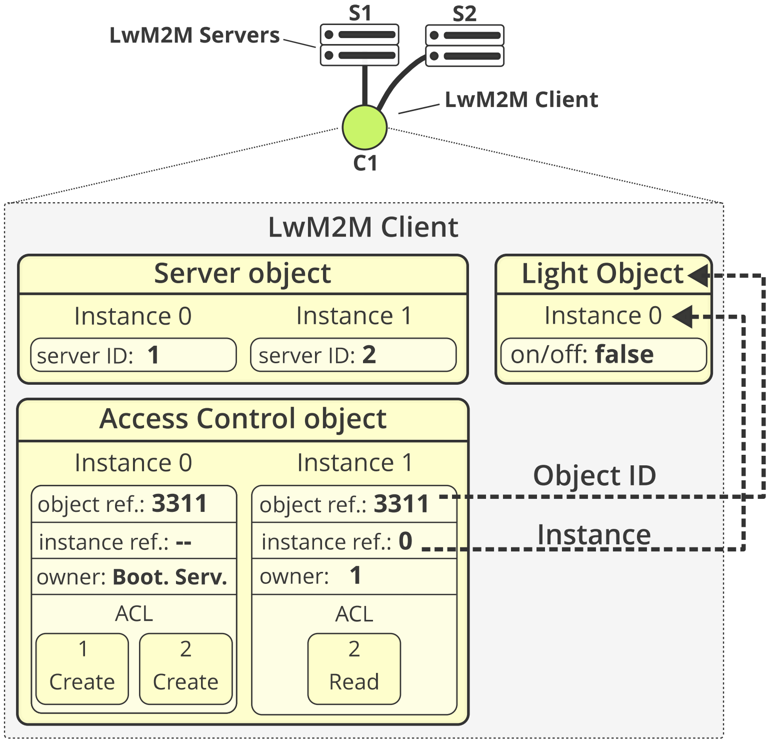
Server-Centric communication **prevents edge collaboration**.



- **Only Servers perform operations on Clients**
  - Using established secure communication
  - Credentials and access rights are required
  - IoT applications interact with Clients only through Servers

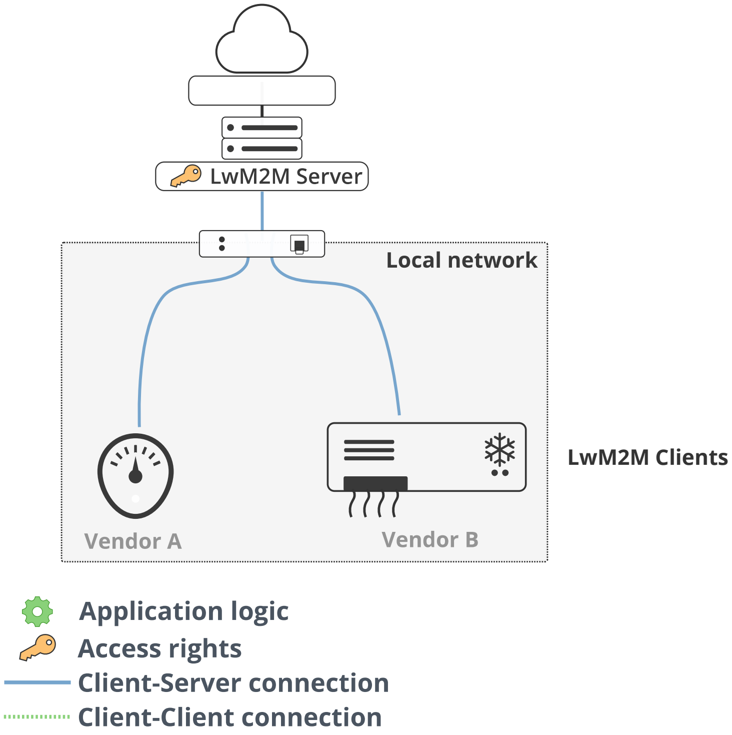
LwM2M Objects, Resources and Access Control

- **LwM2M Clients expose resources**
  - Resources are logically grouped into objects
- **Objects accept multiple operations**
  - Read, write, execute, create, etc.
- **Access control policies apply to objects**
  - Determine which operations a server may perform
  - Different servers may have different access



LwM2M Client-to-Client (C2C) Communication

Extended LwM2M Deployment



LwM2M Server

Local network

LwM2M Clients

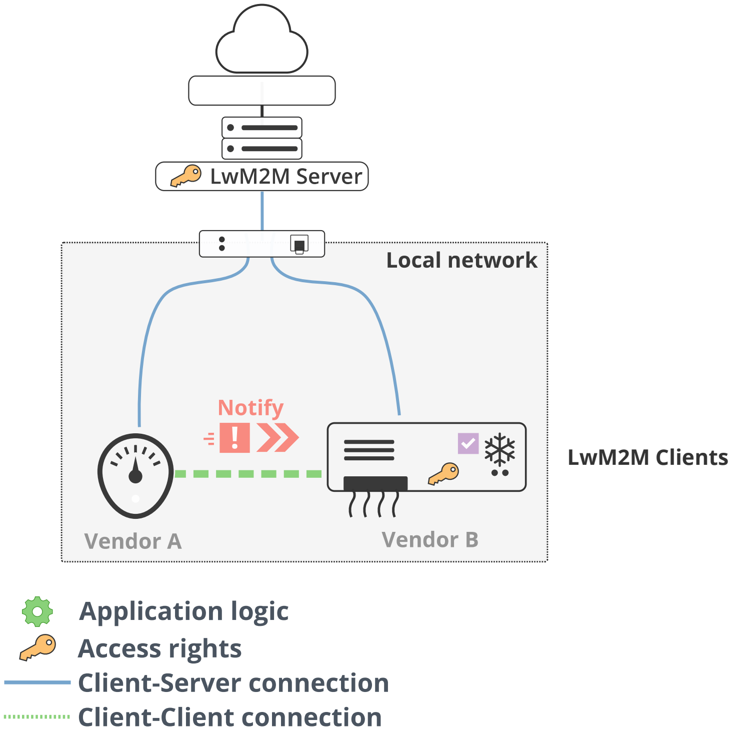
Vendor A

Vendor B

- ⚙ Application logic
- 🔑 Access rights
- — Client-Server connection
- ⋯ Client-Client connection

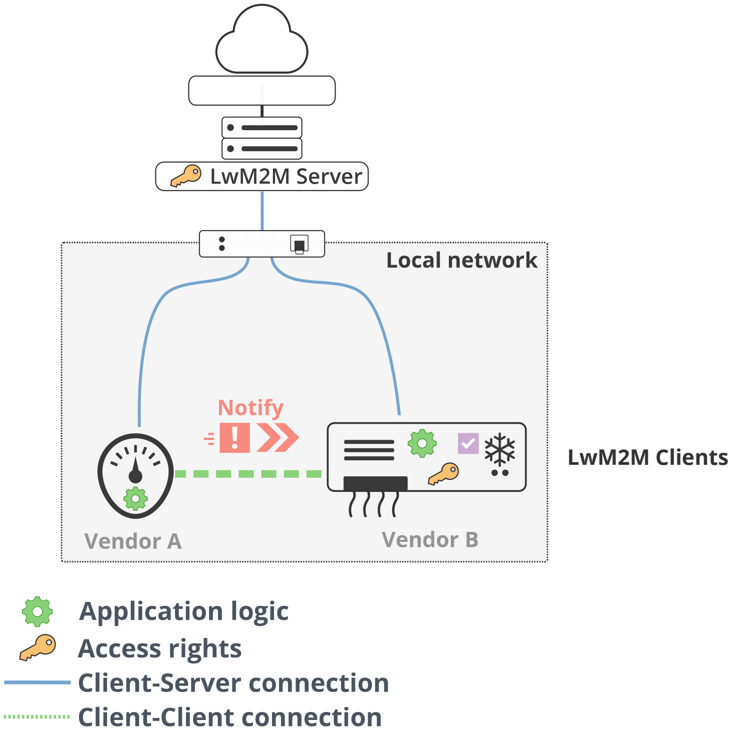
Extended LwM2M Deployment

- Clients operate on other Clients resources



Extended LwM2M Deployment

- Clients operate on other Clients resources
- **Application logic is distributed on the edge**
  - Reduces latency
  - Increases bandwidth
  - Local communication



LwM2M Server

Local network

Notify

LwM2M Clients

Vendor A

Vendor B

Application logic

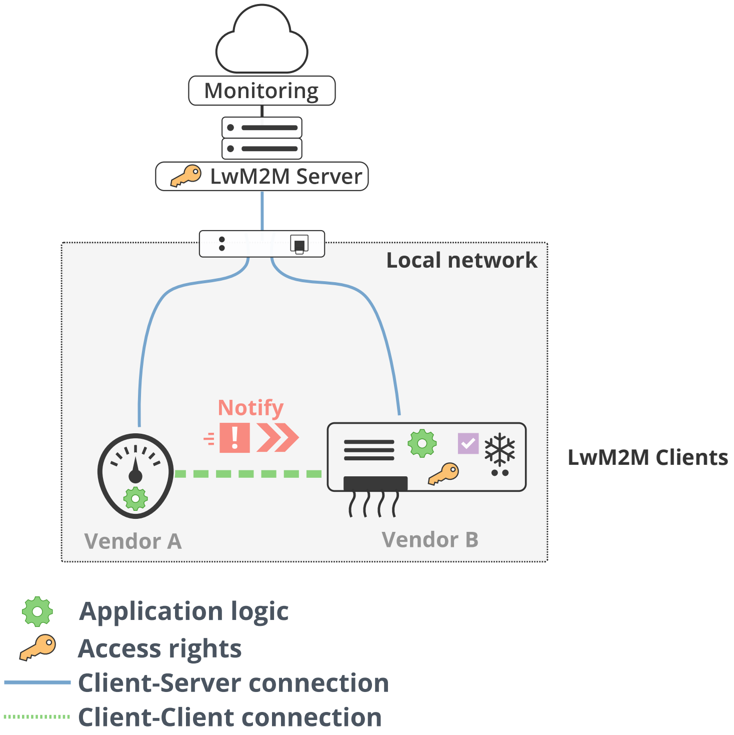
Access rights

Client-Server connection

Client-Client connection

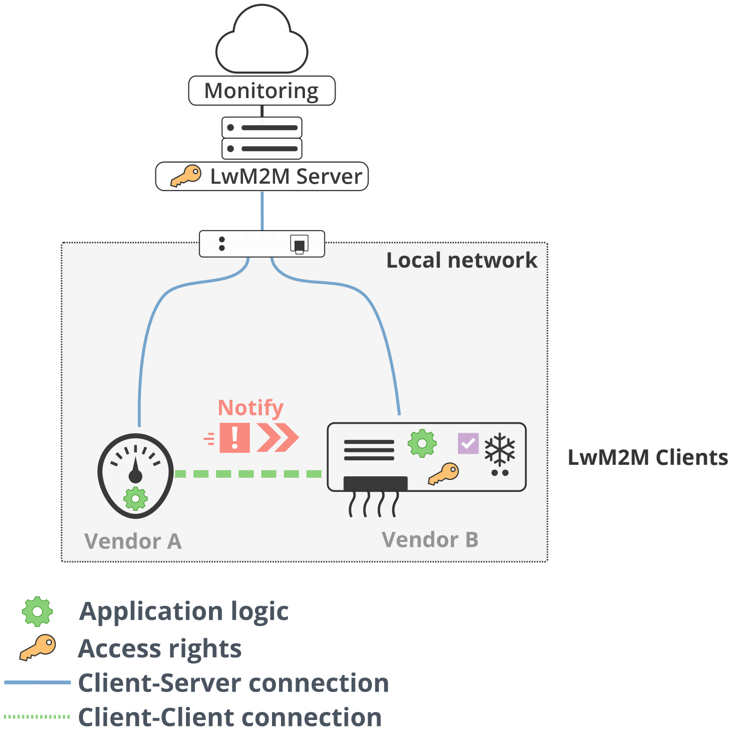
Extended LwM2M Deployment

- Clients operate on other Clients resources
- Application logic is distributed on the edge
  - Reduces latency
  - Increases bandwidth
  - Local communication
- Servers monitor and manage Clients



Extended LwM2M Deployment

- Clients operate on other Clients resources
- Application logic is distributed on the edge
  - Reduces latency
  - Increases bandwidth
  - Local communication
- Servers monitor and manage Clients
- New LwM2M objects
  - **Client** object: communication information
  - **Client Security** object: credentials for secure channel
  - **Client Access Control** object: remote clients access rights
- Extended interfaces
  - Allow client operation
  - Handle client access rights

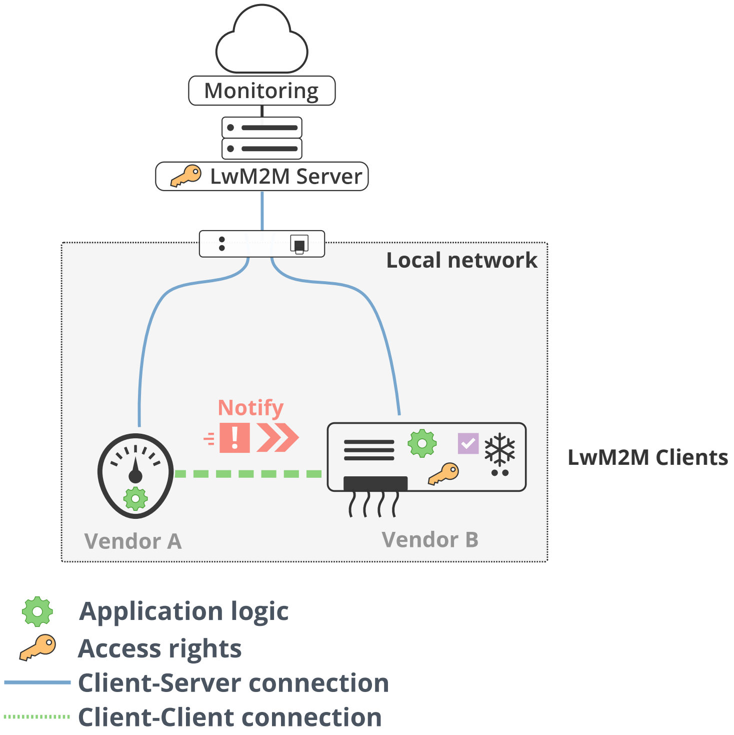


Extended LwM2M Deployment

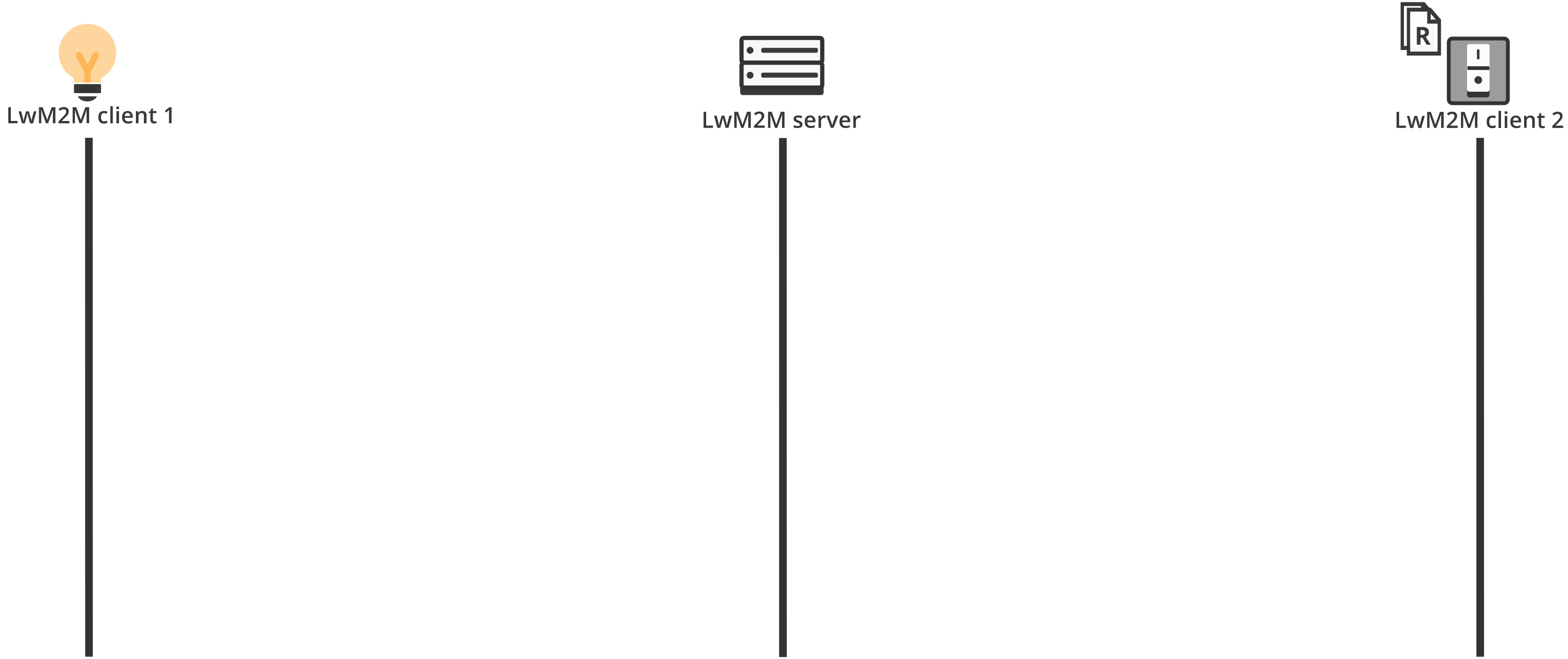
- Clients operate on other Clients resources
- Application logic is distributed on the edge
  - Reduces latency
  - Increases bandwidth
  - Local communication
- Servers monitor and manage Clients

- **New LwM2M objects**
  - **Client** object**:** communication information
  - **Client Security** object**:** credentials for secure channel
  - **Client Access Control** object**:** remote clients access rights
- **Extended interfaces**
  - Allow client operation
  - Handle client access rights

Contribution 1

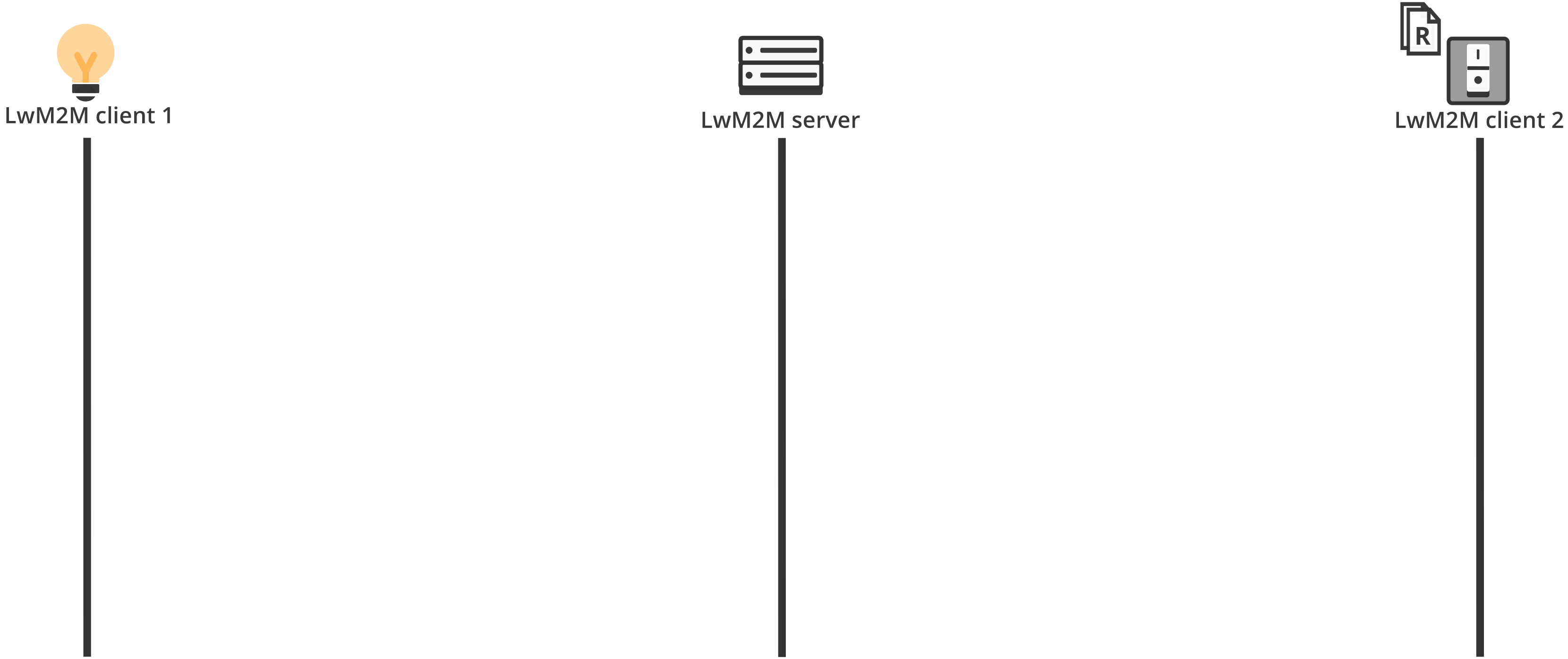


Third Party Authorization of LwM2M Clients

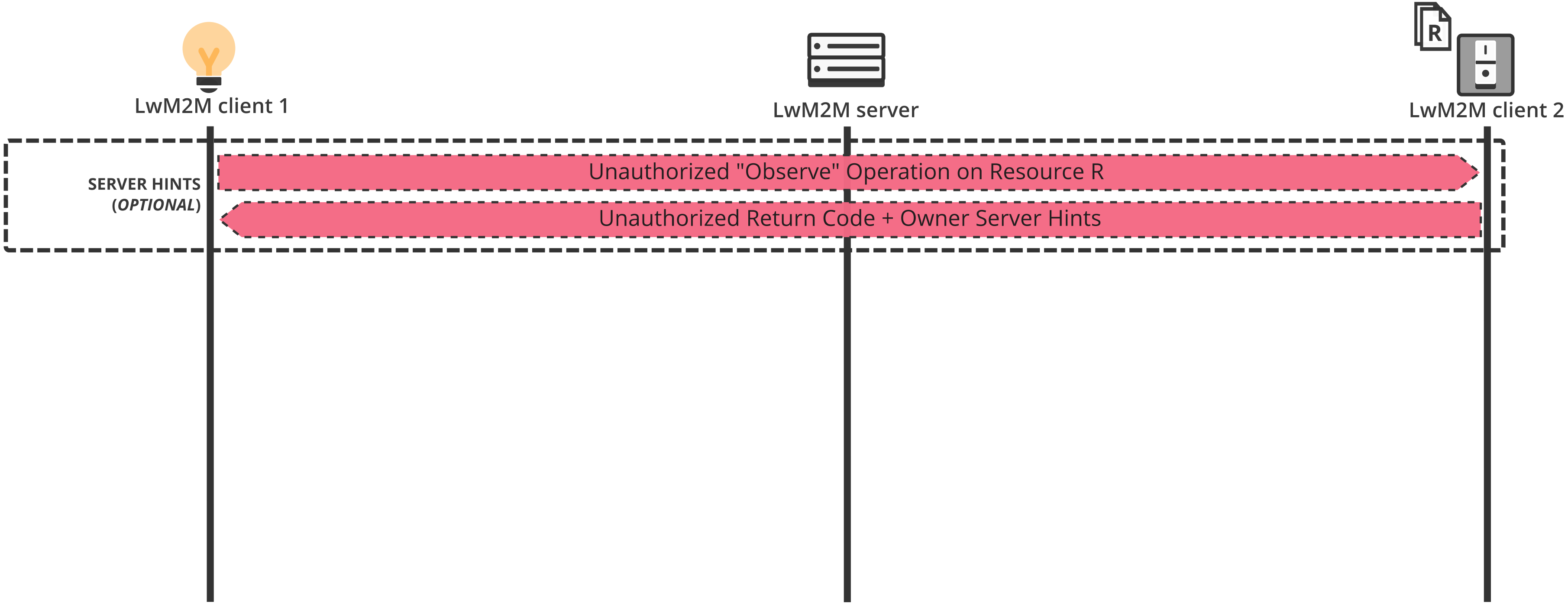


Third Party Authorization of LwM2M Clients

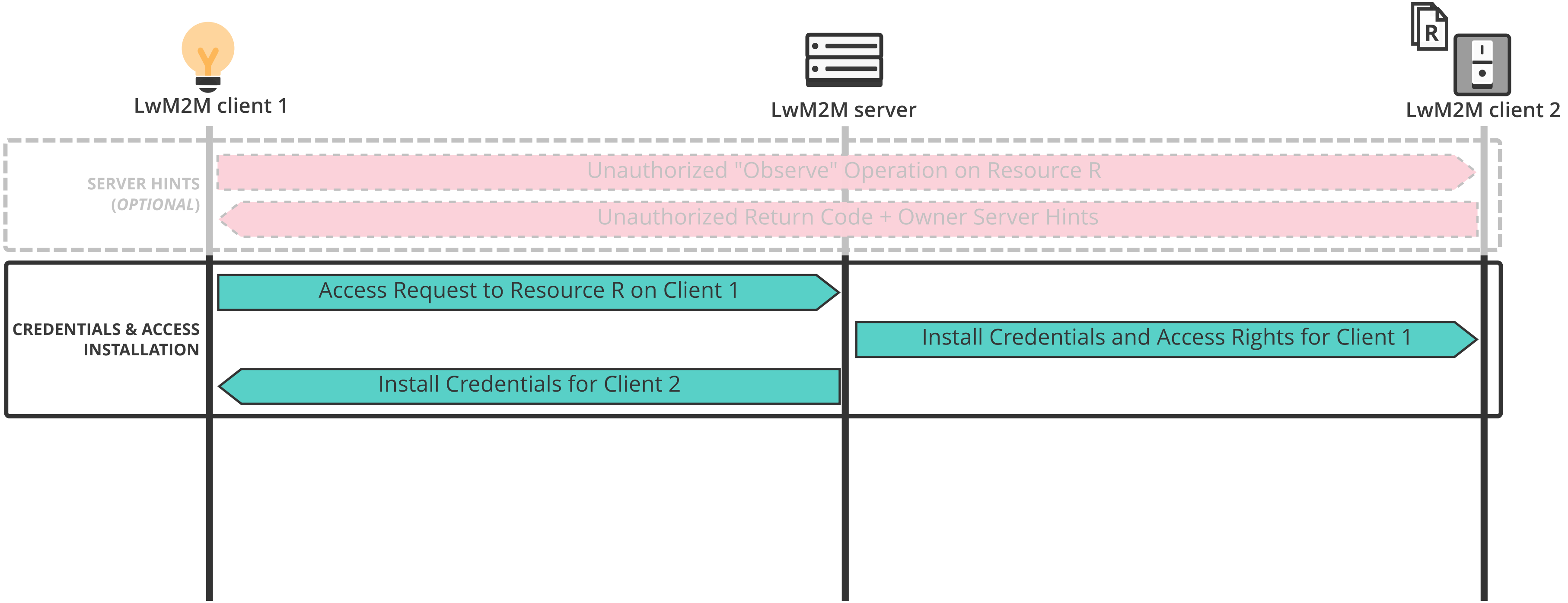
Contribution 2



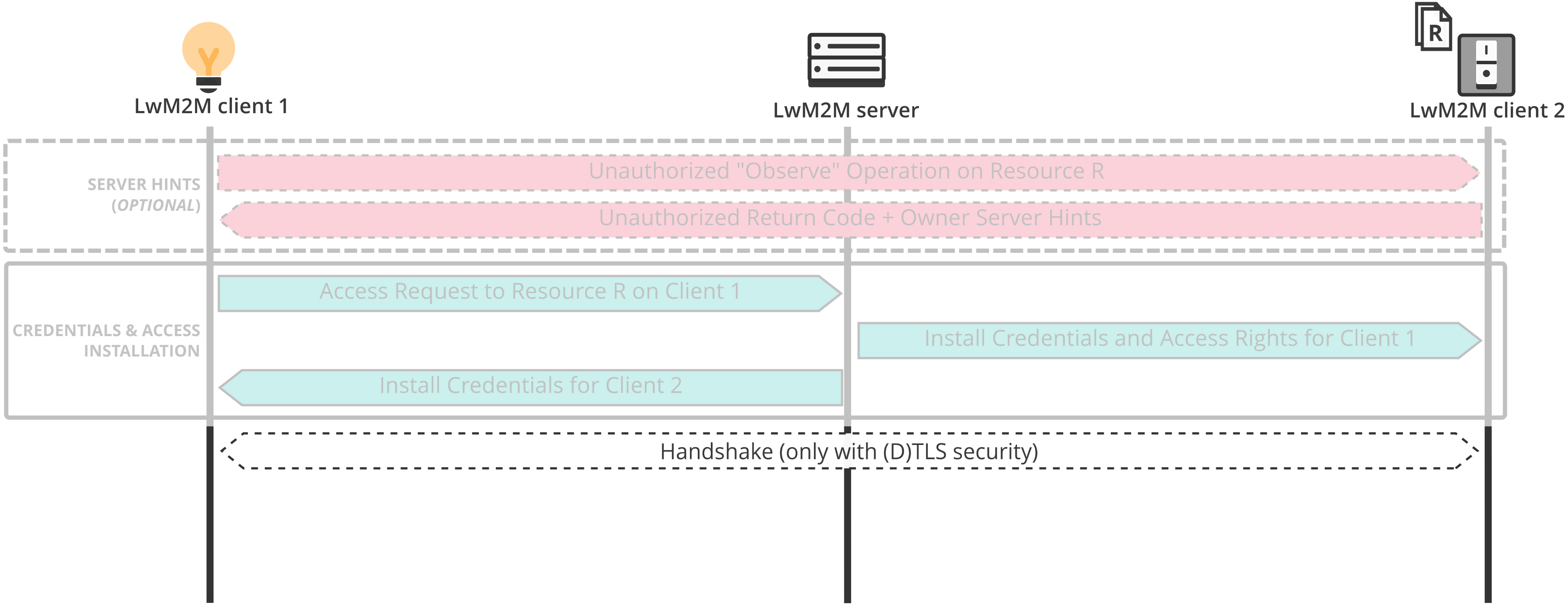
Third Party Authorization of LwM2M Clients


R
LwM2M client 1
LwM2M server
LwM2M client 2
SERVER HINTS
(*OPTIONAL*)
Unauthorized "Observe" Operation on Resource R
Unauthorized Return Code + Owner Server Hints

Third Party Authorization of LwM2M Clients

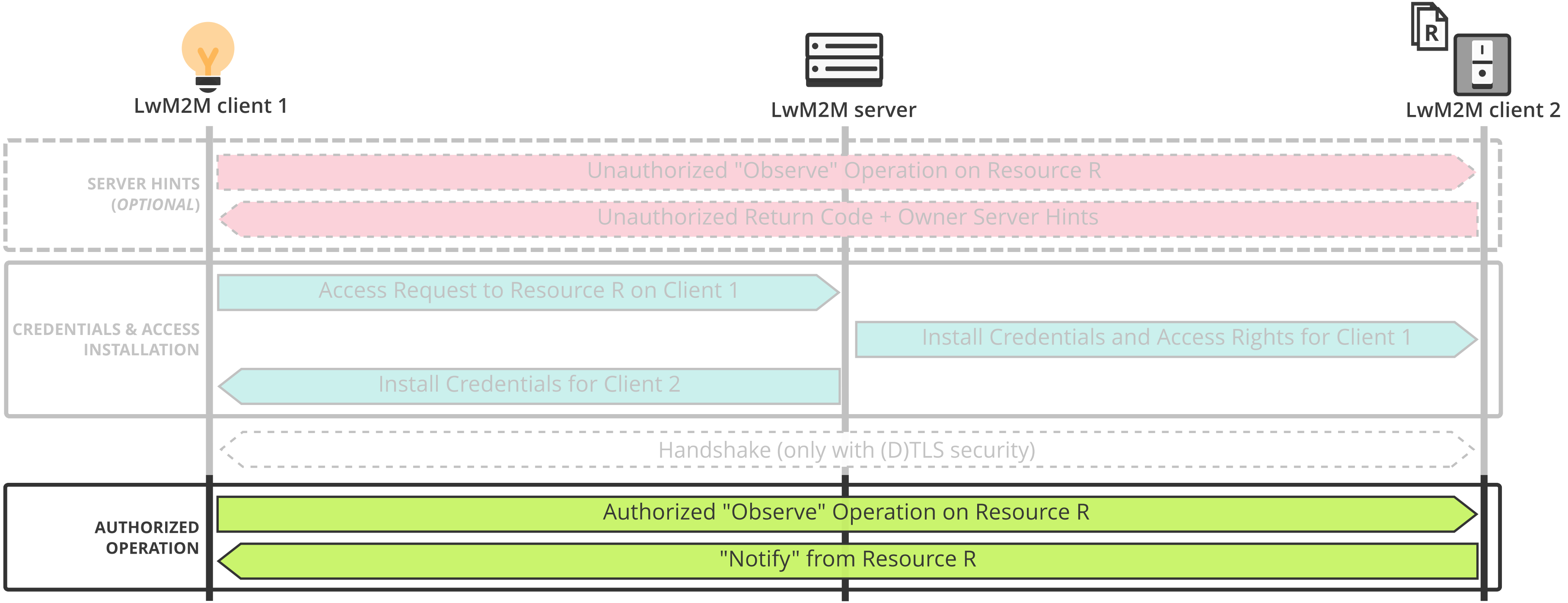

R
LwM2M client 1
LwM2M server
LwM2M client 2
SERVER HINTS
(OPTIONAL)
Unauthorized "Observe" Operation on Resource R
Unauthorized Return Code + Owner Server Hints
CREDENTIALS & ACCESS
INSTALLATION
Access Request to Resource R on Client 1
Install Credentials and Access Rights for Client 1
Install Credentials for Client 2

Third Party Authorization of LwM2M Clients



LwM2M client 1
LwM2M server
R
LwM2M client 2
SERVER HINTS
(*OPTIONAL*)
Unauthorized "Observe" Operation on Resource R
Unauthorized Return Code + Owner Server Hints
CREDENTIALS & ACCESS
INSTALLATION
Access Request to Resource R on Client 1
Install Credentials and Access Rights for Client 1
Install Credentials for Client 2
Handshake (only with (D)TLS security)

Third Party Authorization of LwM2M Clients



LwM2M client 1

LwM2M server

LwM2M client 2

SERVER HINTS (*OPTIONAL*)

Unauthorized "Observe" Operation on Resource R

Unauthorized Return Code + Owner Server Hints

CREDENTIALS & ACCESS INSTALLATION

Access Request to Resource R on Client 1

Install Credentials and Access Rights for Client 1

Install Credentials for Client 2

Handshake (only with (D)TLS security)

AUTHORIZED OPERATION

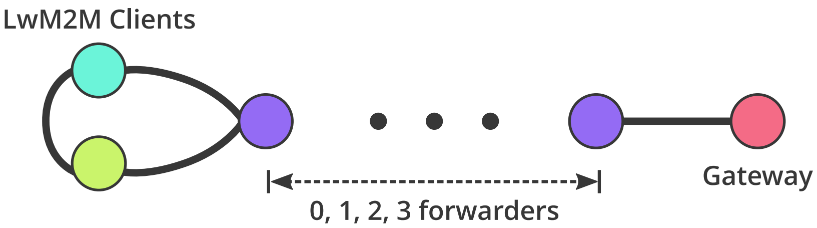
Authorized "Observe" Operation on Resource R

"Notify" from Resource R

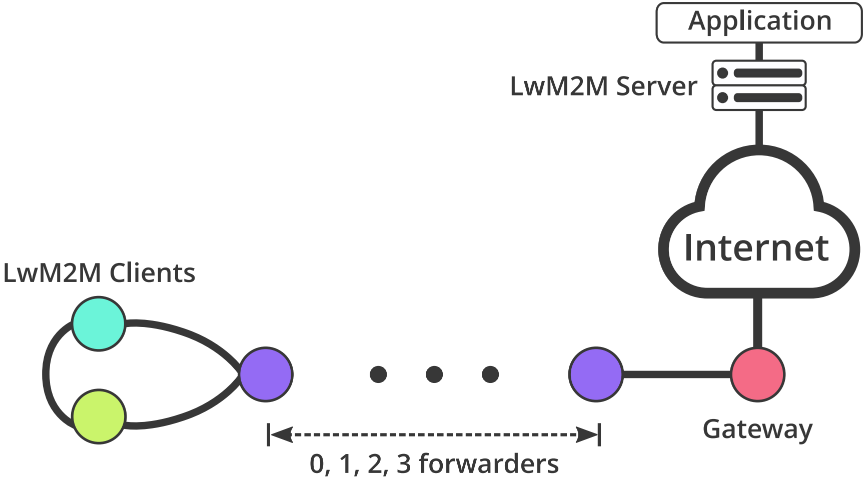
Experimental Evaluation

Experimental Setup

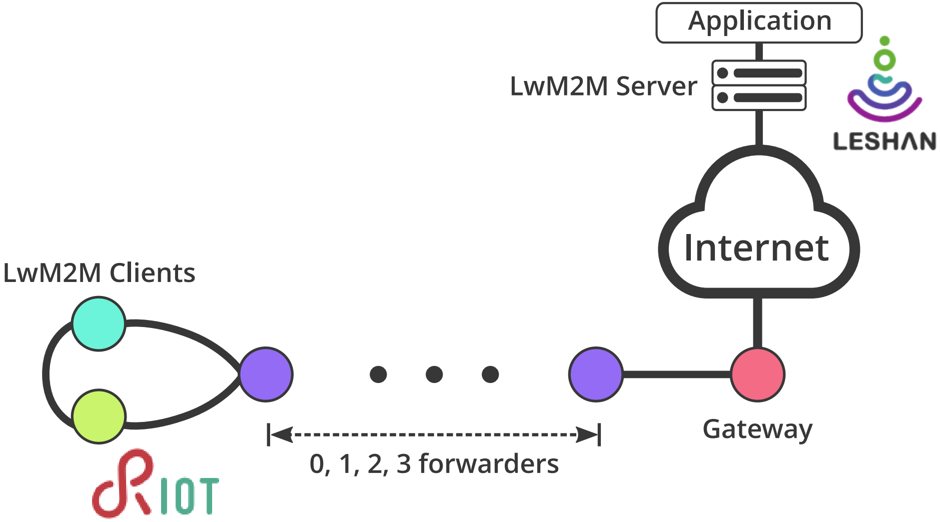
Experimental Setup



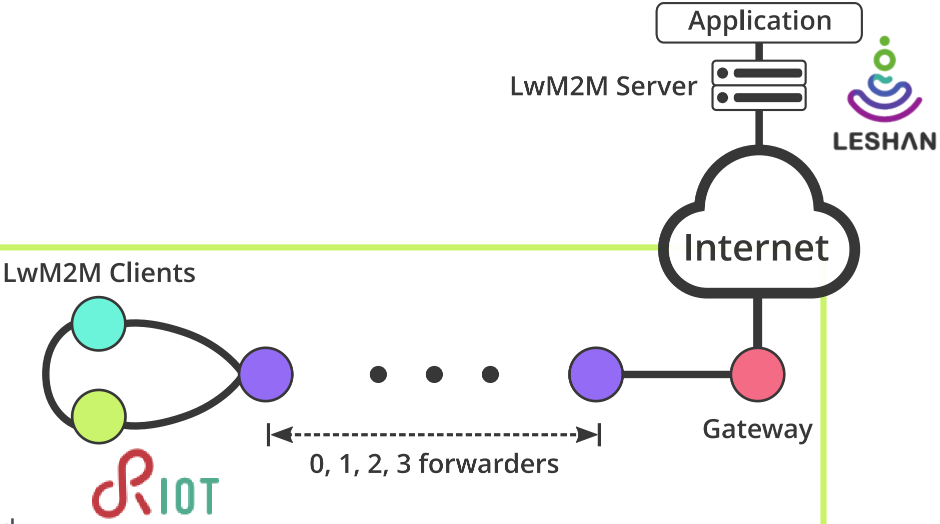
Experimental Setup



Experimental Setup



Experimental Setup



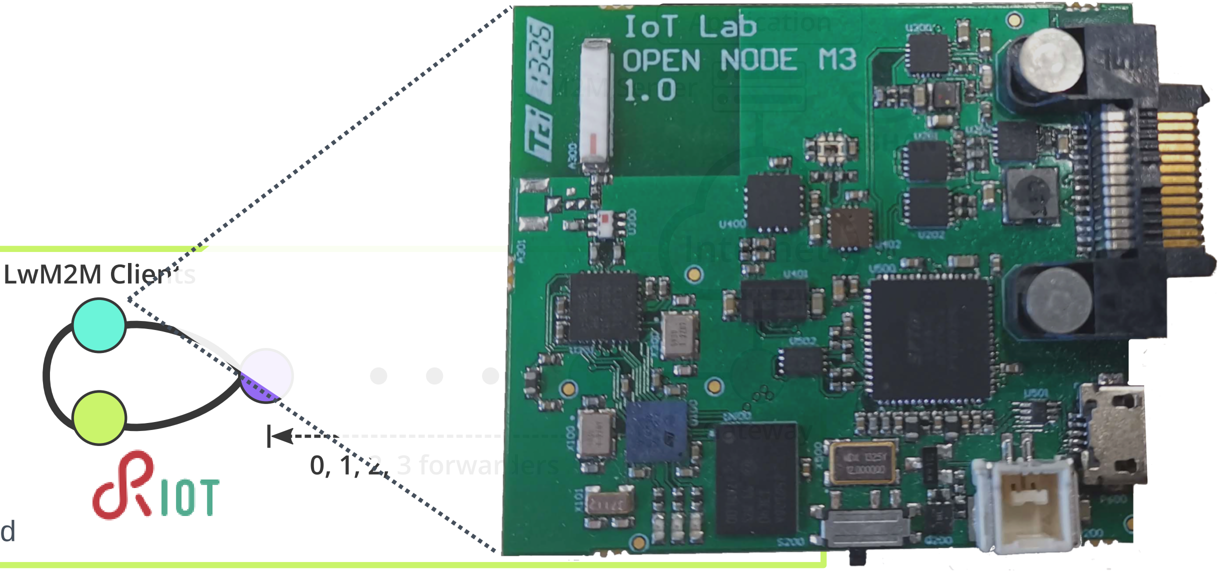
FIT IOT-LAB

- Inria Grenoble site
- 350 nodes evenly spread

Experimental Setup

FIT IOT-LAB

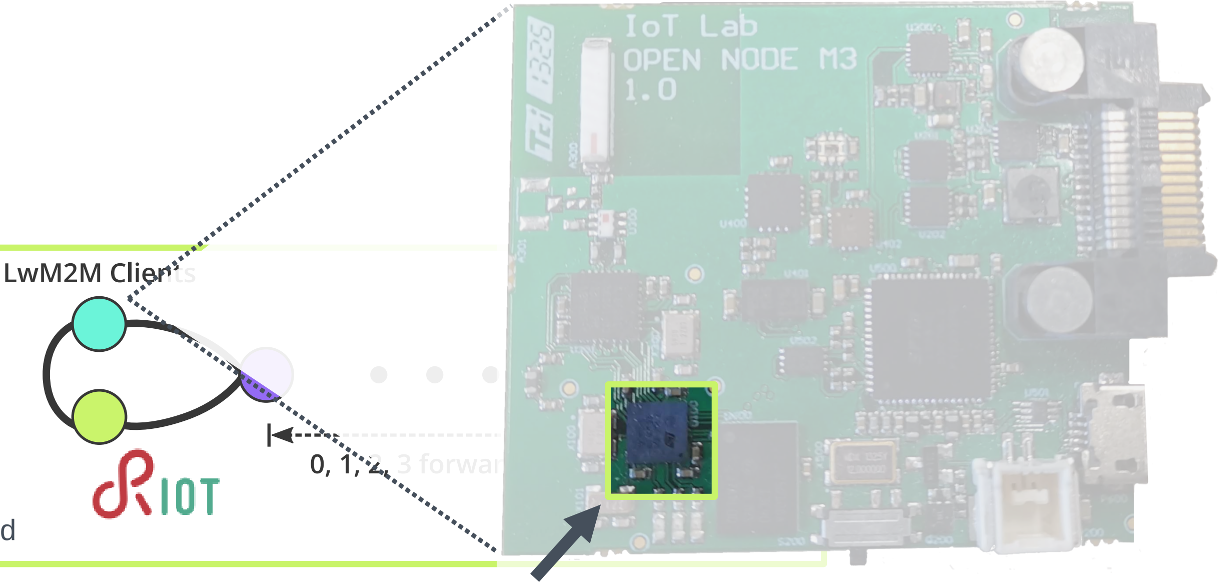
- Inria Grenoble site
- 350 nodes evenly spread



Experimental Setup

FIT IOT-LAB

- Inria Grenoble site
- 350 nodes evenly spread



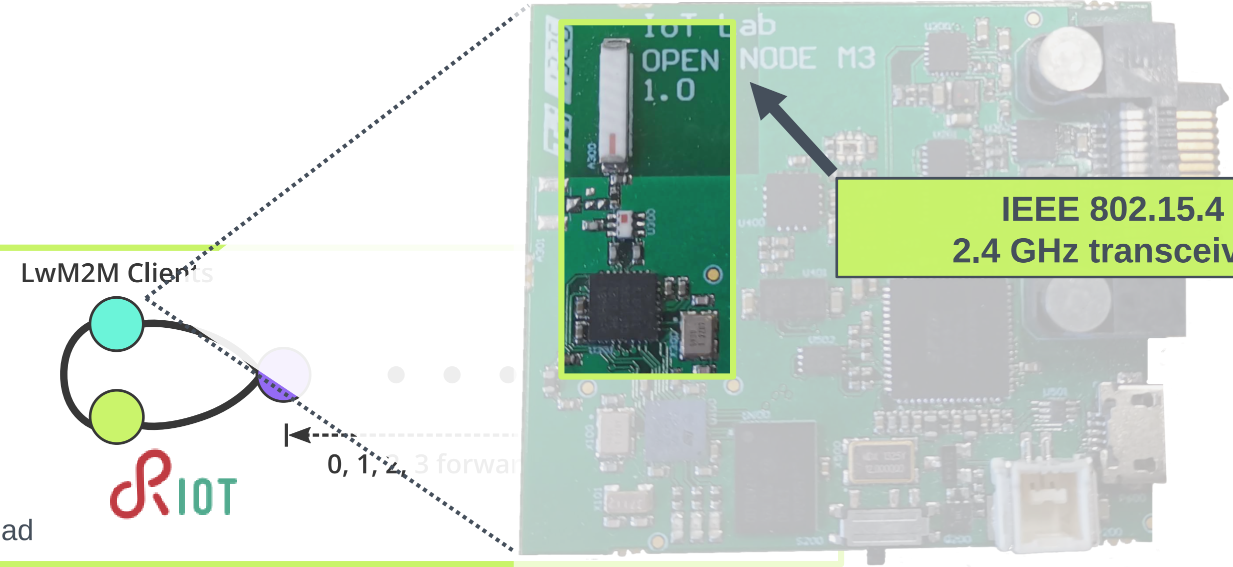
RIOT

ARM Cortex-M3 @ 72 MHz
64 KiB RAM + 512 KiB ROM

Experimental Setup

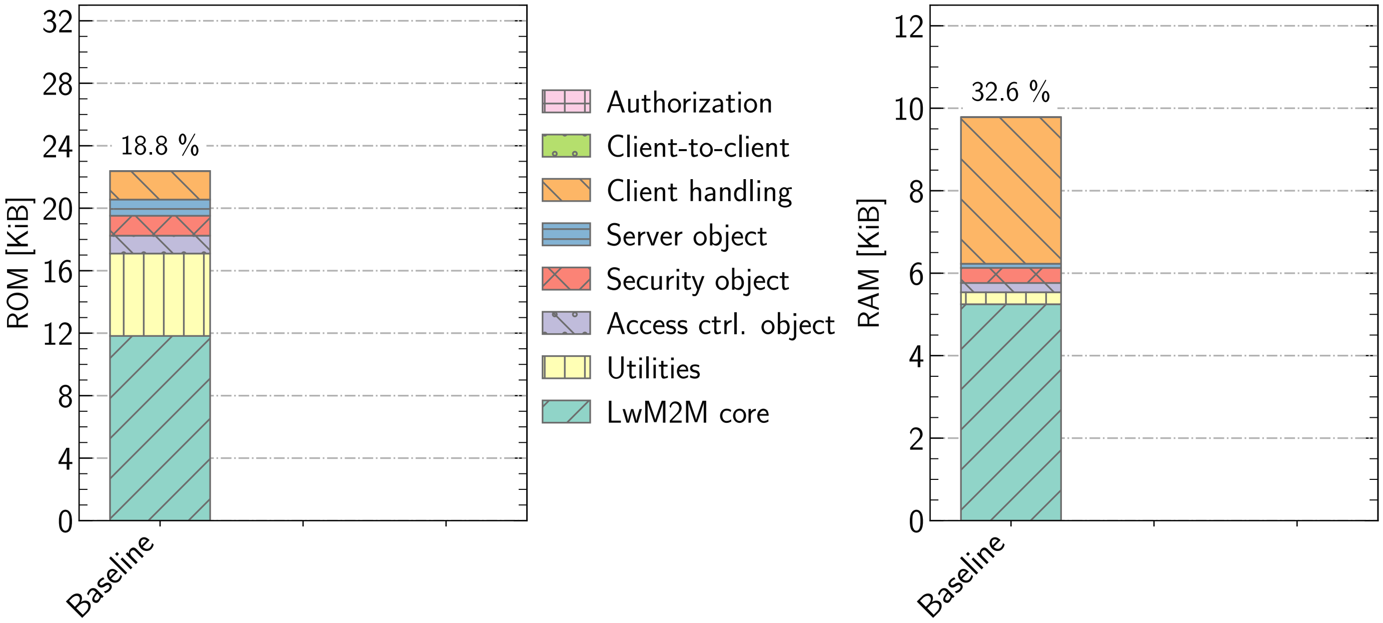
FIT IOT-LAB

- Inria Grenoble site
- 350 nodes evenly spread

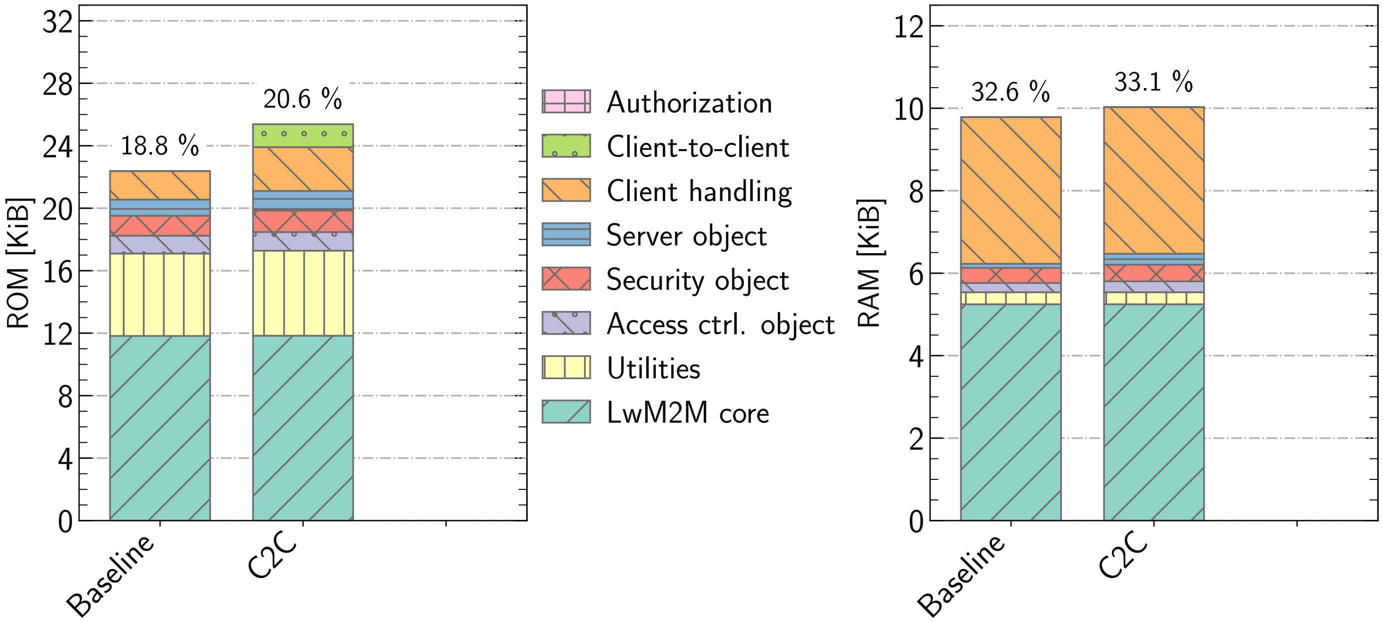


IEEE 802.15.4
2.4 GHz transceiver

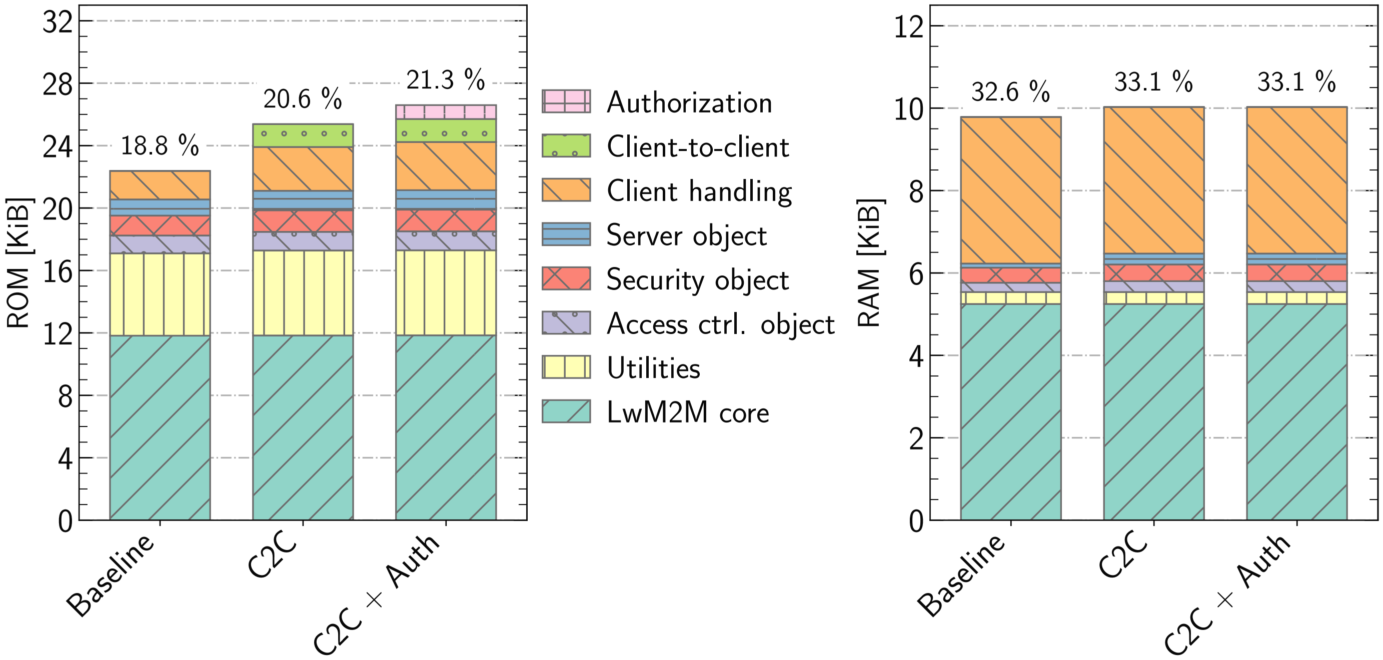
Firmware Size



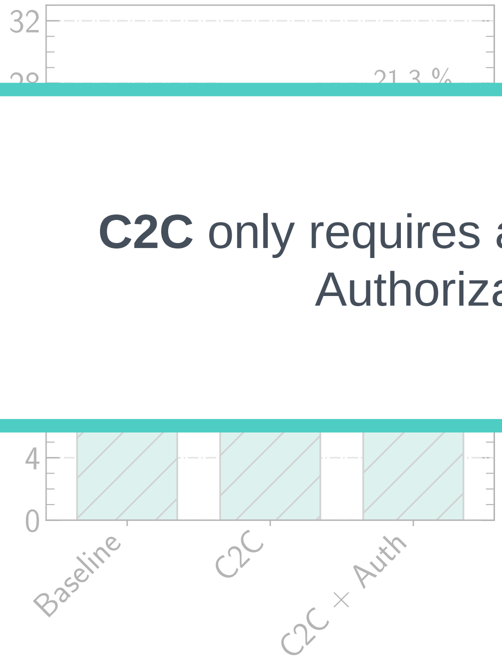
Firmware Size

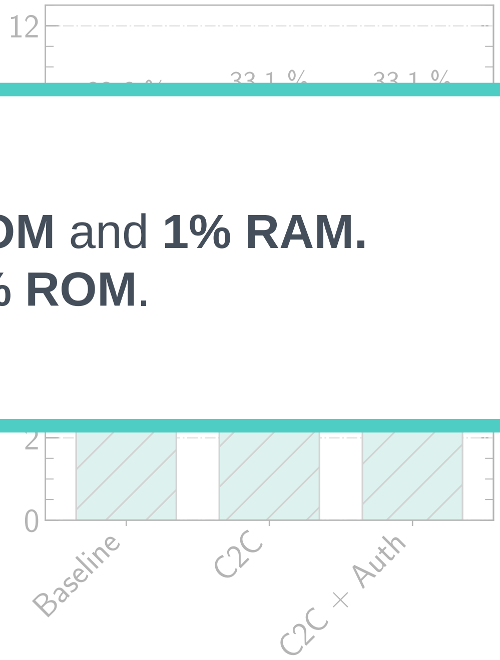


Firmware Size



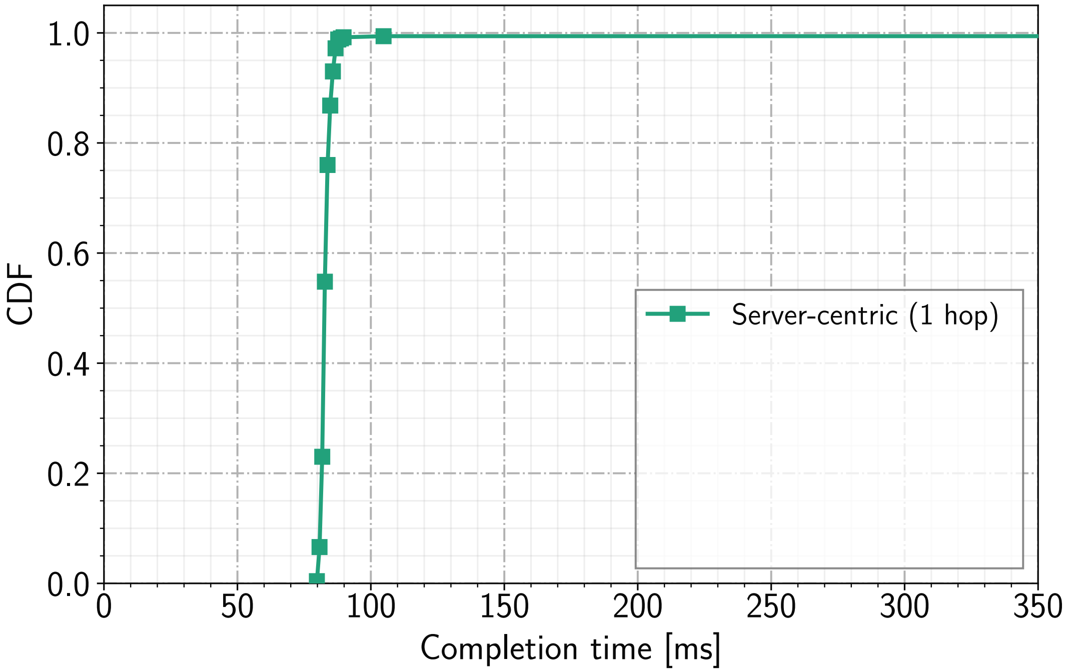
Firmware Size



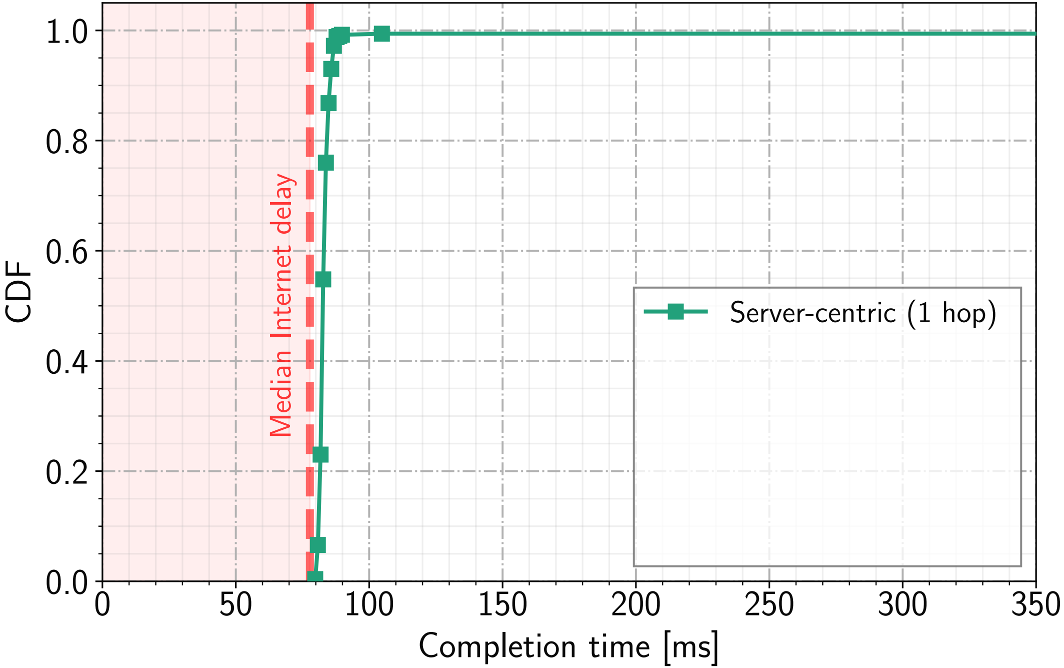


C2C only requires additional **3% ROM** and **1% RAM.**
Authorization an extra **5% ROM**.

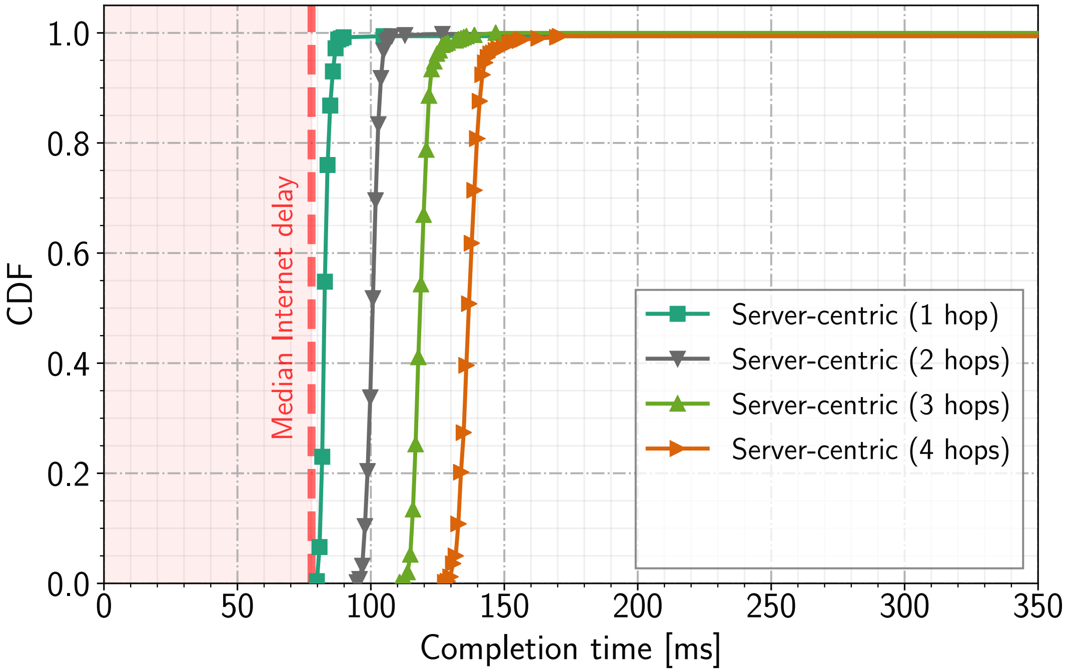
Notification Arrival Time



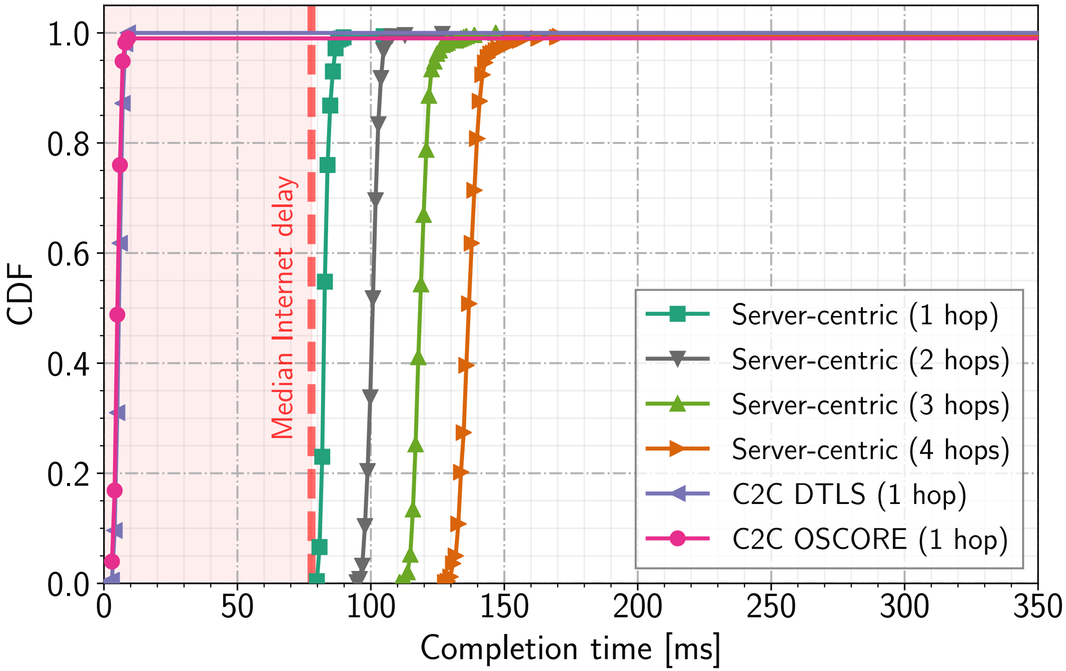
Notification Arrival Time



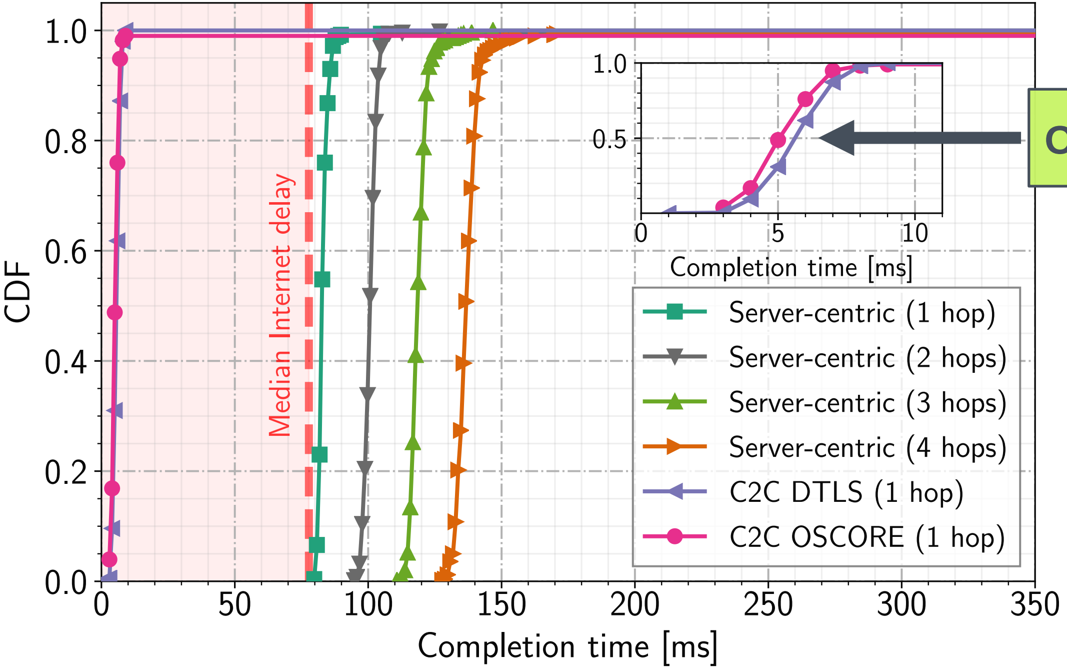
Notification Arrival Time



Notification Arrival Time

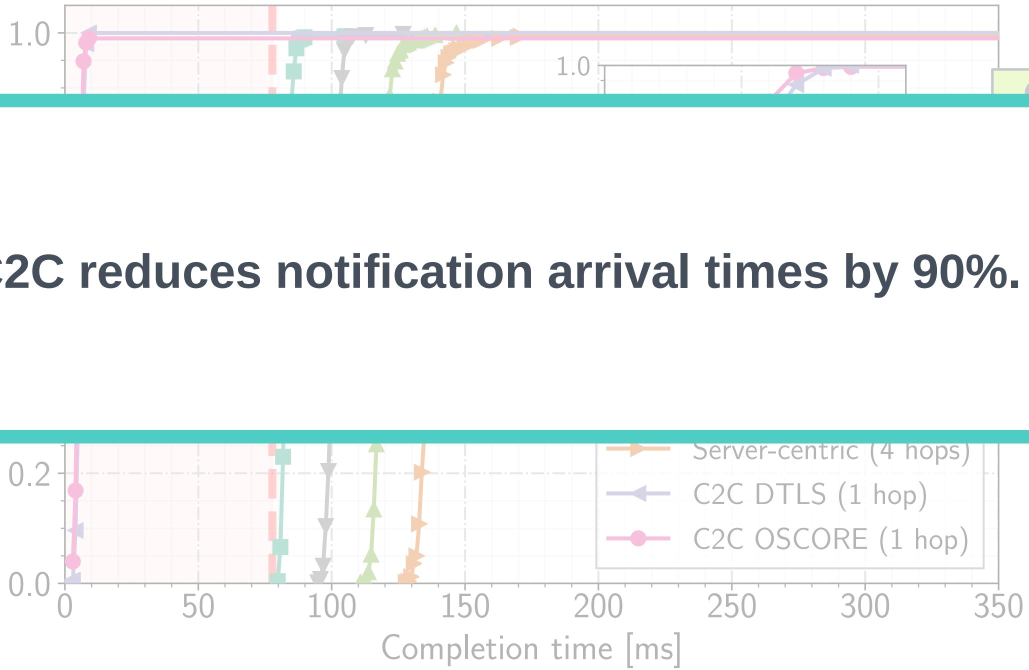


Notification Arrival Time



OSCORE is faster

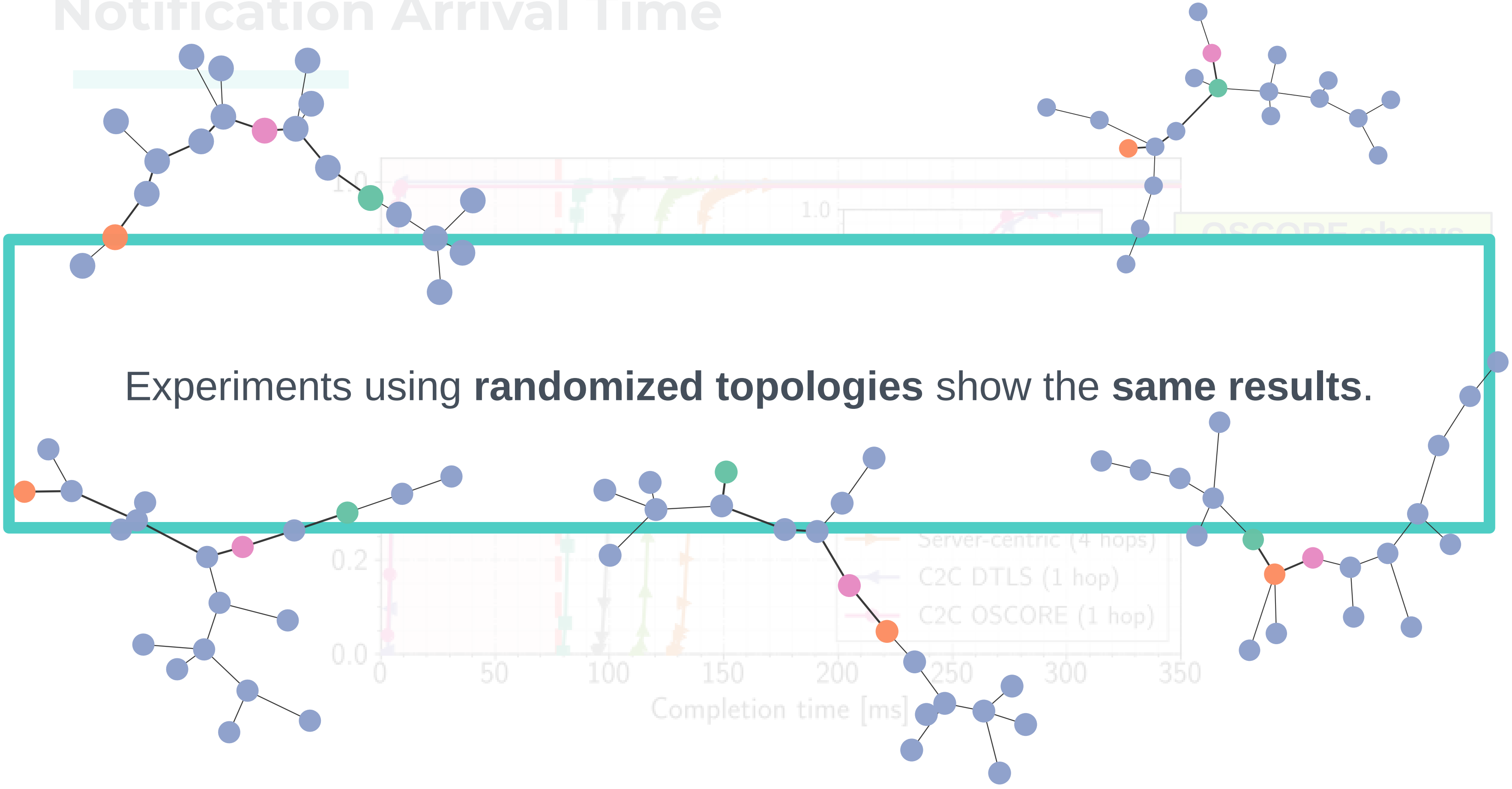
Notification Arrival Time



OSCORE shows

C2C reduces notification arrival times by 90%.

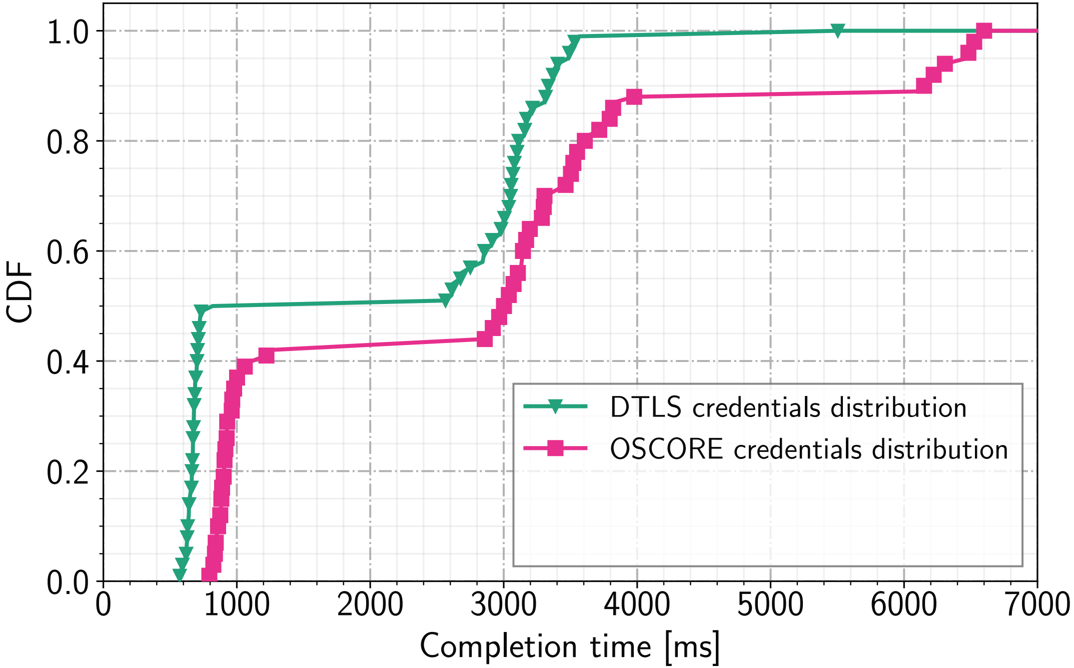
Notification Arrival Time



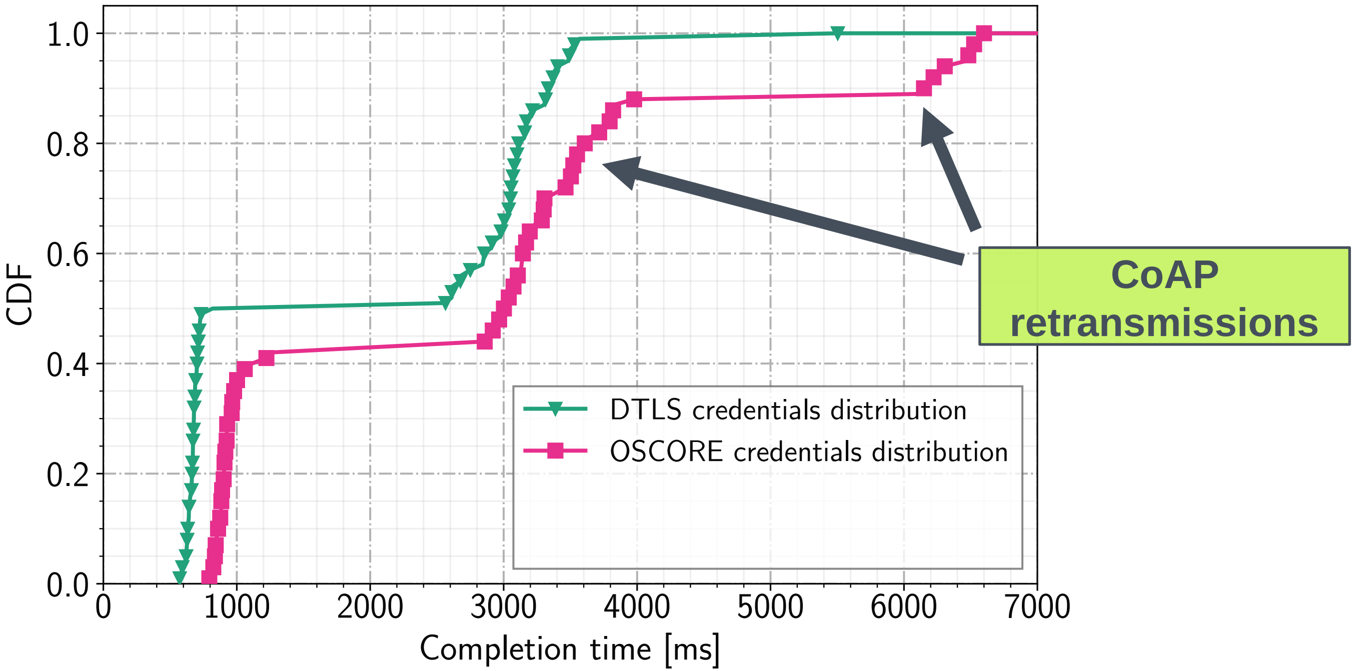
OSCORE shows

Experiments using **randomized topologies** show the **same results**.

Authorization Request & First C2C Operation

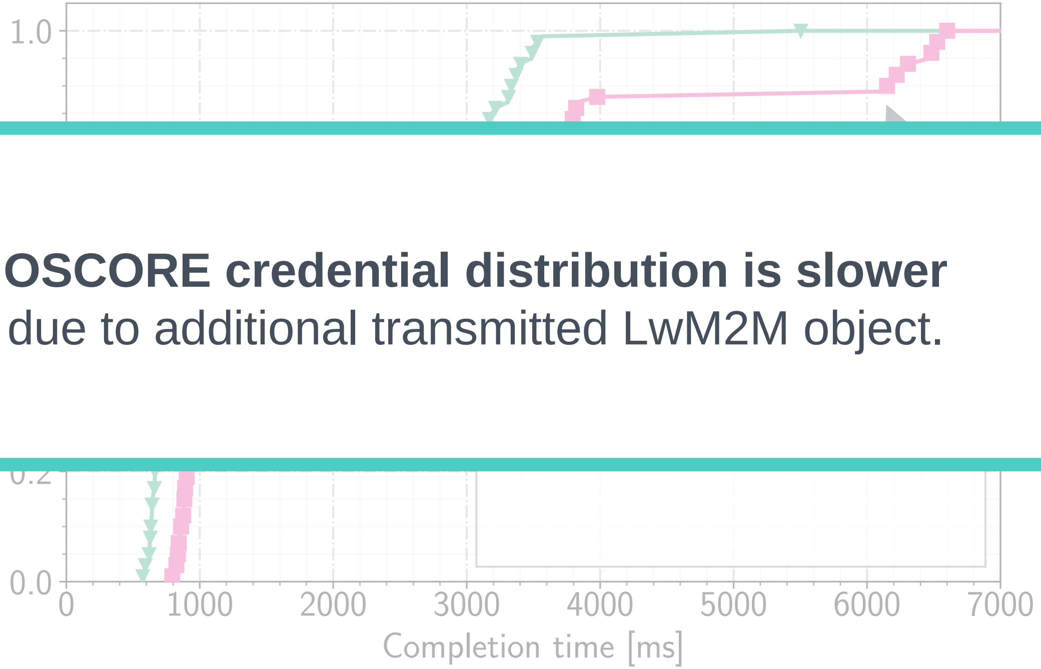


Authorization Request & First C2C Operation



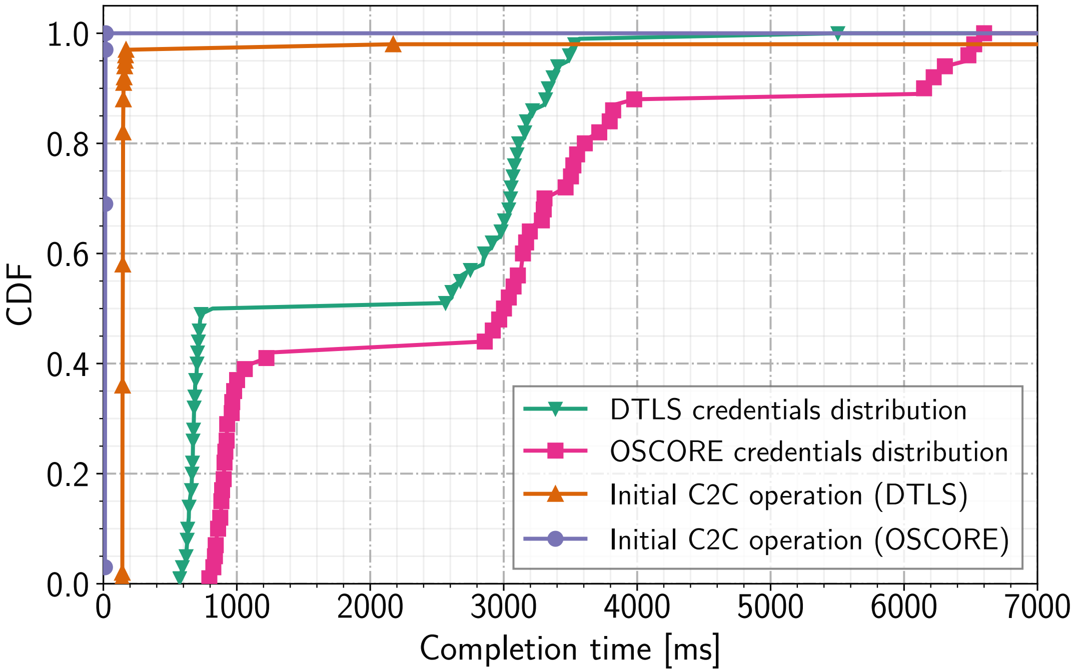
CoAP retransmissions

Authorization Request & First C2C Operation

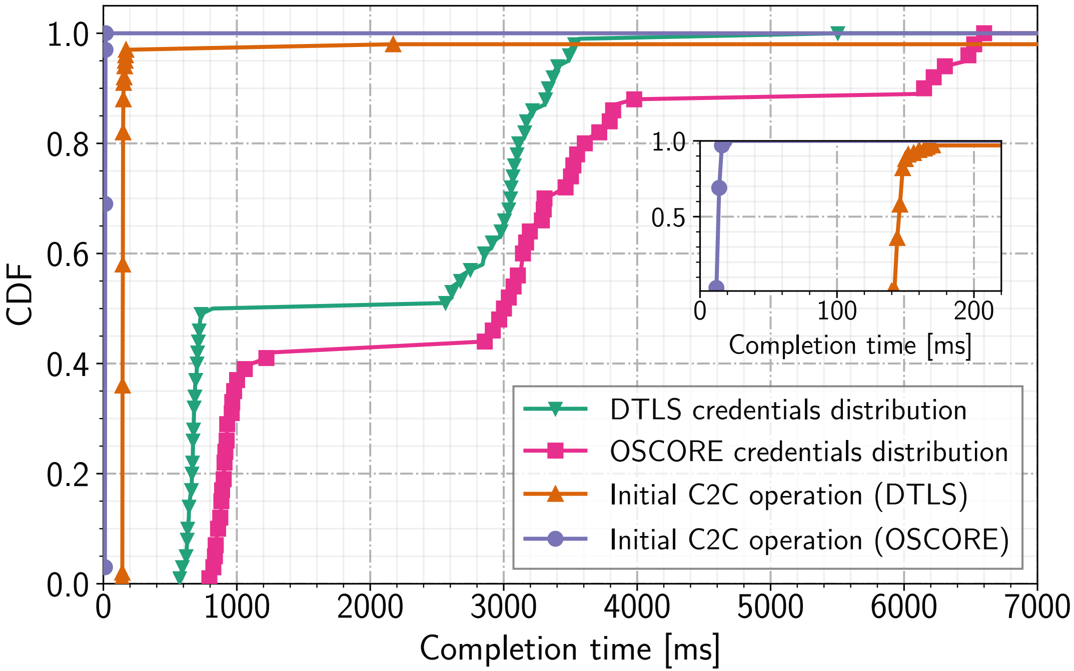


OSCORE credential distribution is slower
due to additional transmitted LwM2M object.

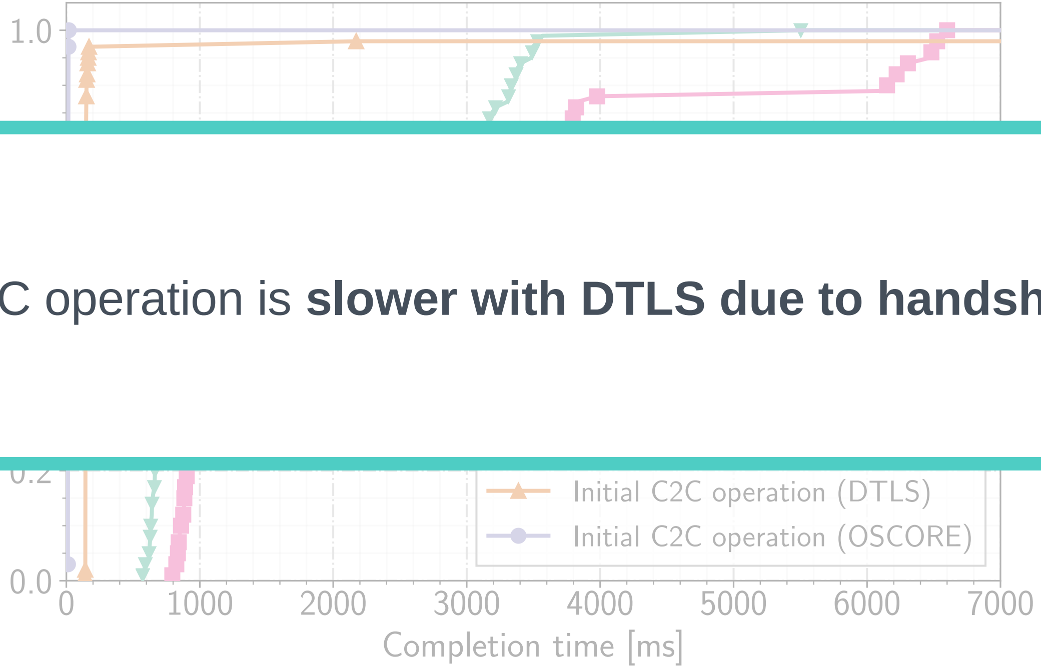
Authorization Request & First C2C Operation



Authorization Request & First C2C Operation

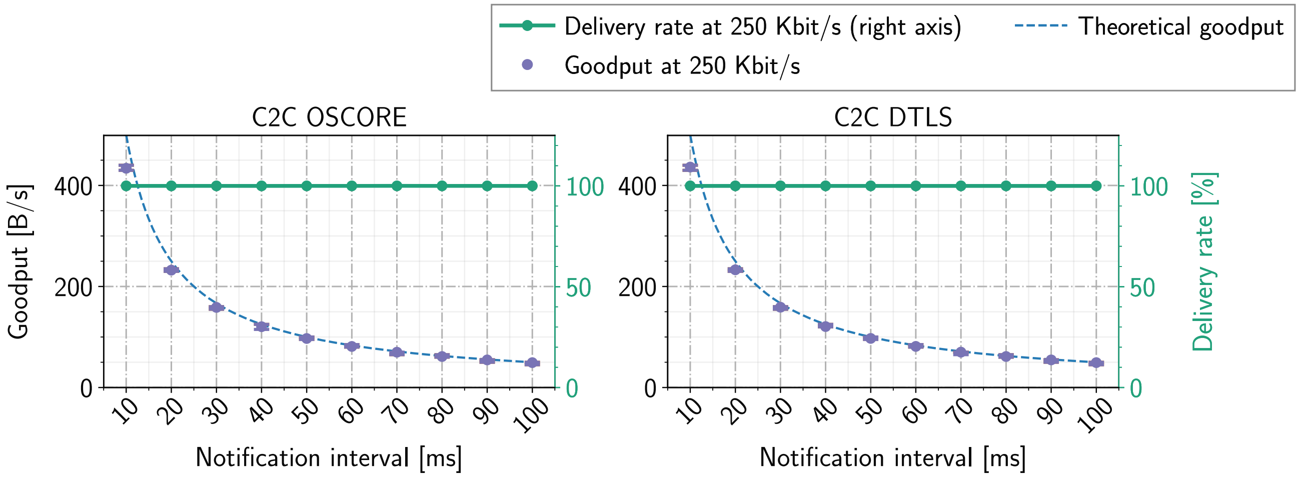


Authorization Request & First C2C Operation

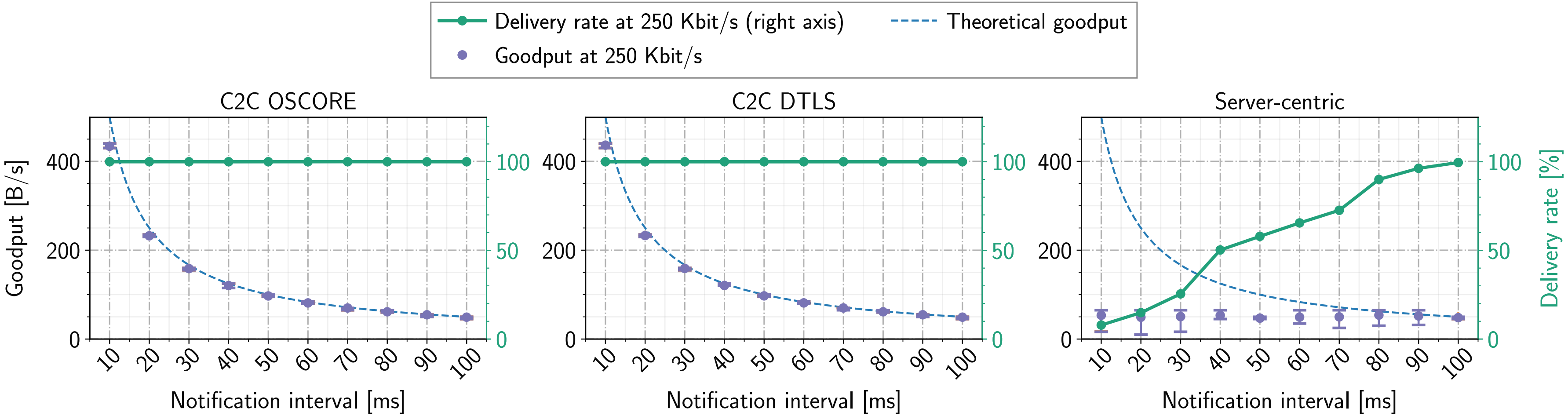


Initial C2C operation is **slower with DTLS due to handshake.**

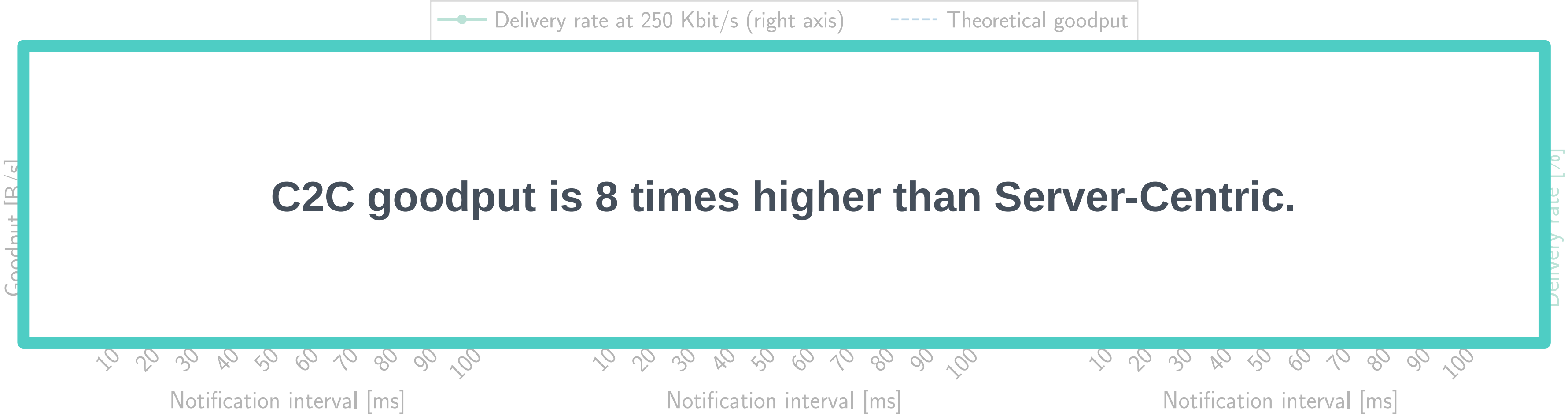
Maximum Goodput with One Hop



Maximum Goodput with One Hop

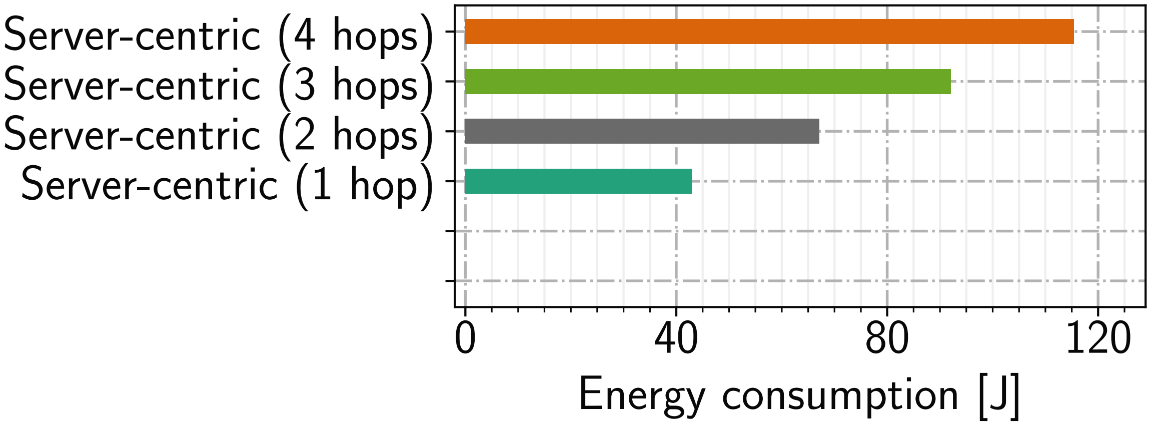


Maximum Goodput with One Hop

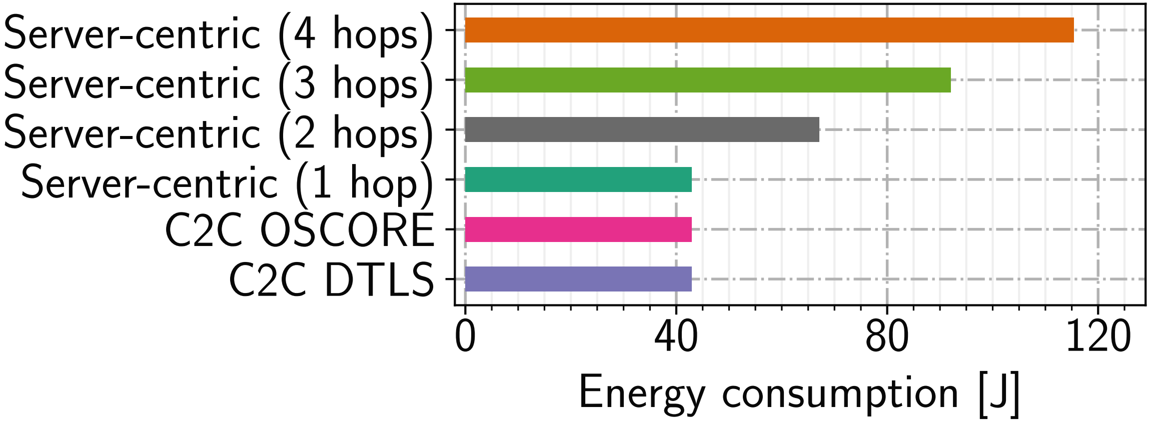


C2C goodput is 8 times higher than Server-Centric.

Energy Consumption



Energy Consumption



Energy Consumption

C2C adds **no energy overhead.**
Using less hops reduces energy requirement.

Conclusion & Outlook

- **We contributed**
  - A **third party authorization mechanism** for LwM2M Clients
  - New LwM2M objects and extended interfaces for **C2C communication**
  - An empirical **performance analysis** on real hardware
  - Public and **open source implementation** of the extensions

Conclusion & Outlook

- **We contributed**
  - A **third party authorization mechanism** for LwM2M Clients
  - New LwM2M objects and extended interfaces for **C2C communication**
  - An empirical **performance analysis** on real hardware
  - Public and **open source implementation** of the extensions

- **Our results show that**
  - C2C reduces data arrival times **by up to 90%**
  - C2C yields a more reliable and **8 times higher goodput**
  - Our extensions produce a relatively **small memory footprint**

Conclusion & Outlook

- **We contributed**
  - A **third party authorization mechanism** for LwM2M Clients
  - New LwM2M objects and extended interfaces for **C2C communication**
  - An empirical **performance analysis** on real hardware
  - Public and **open source implementation** of the extensions

- **Our results show that**
  - C2C reduces data arrival times **by up to 90%**
  - C2C yields a more reliable and **8 times higher goodput**
  - Our extensions produce a relatively **small memory footprint**

- **In future work we will**
  - Analyse the applicability of ACE-OAuth framework to LwM2M
  - Explore the integration with Group OSCORE for multiple observations

Thank You!

Our code can be found online

`https://github.com/inetrg/ipsn-2022-lwm2mc2c`