

Lightweight Authorization using EDHOC

<https://datatracker.ietf.org/doc/draft-ietf-lake-authz> ([diff](#))

Geovane Fedrecheski, Inria

Contents

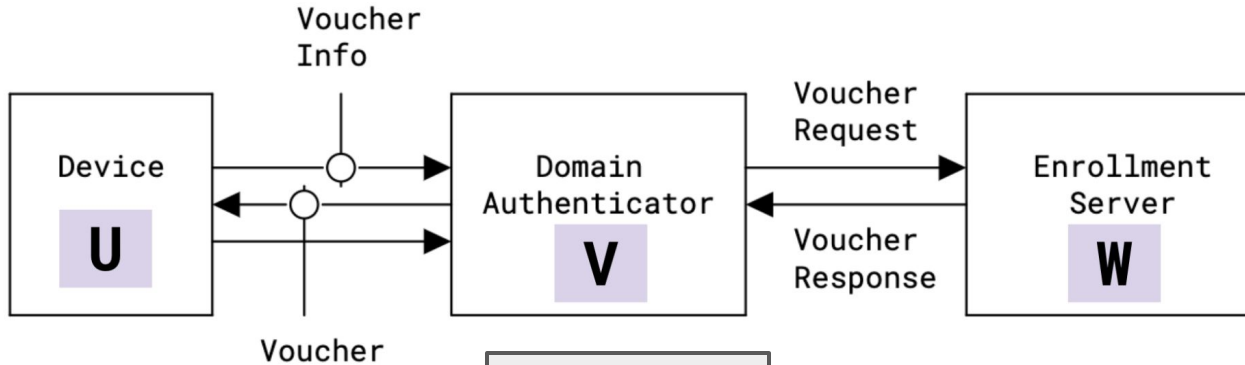
- draft updates
 - we gave it a **name**
 - **new section**: optimization strategies
 - broadcast & advertisement
 - **new appendix**: use with EDHOC reverse flow
 - **new appendix**: example advertisement strategies
 - **next steps**
- performance evaluation

draft updates

Recap: Lightweight Authorization using EDHOC

Also referred to as:

- **authz**
- **zero-touch** network join

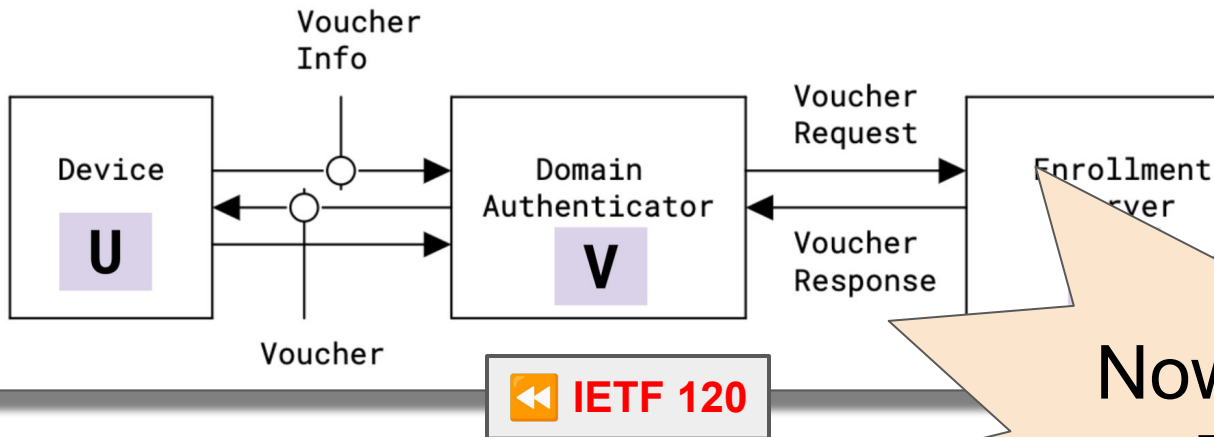


◀ IETF 120

Recap: Lightweight Authorization using EDHOC

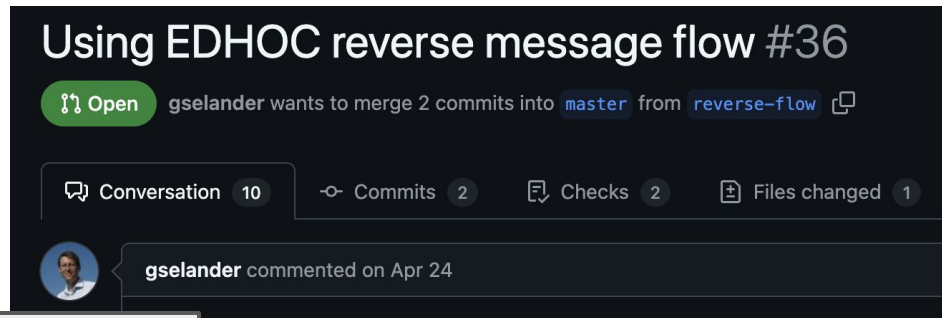
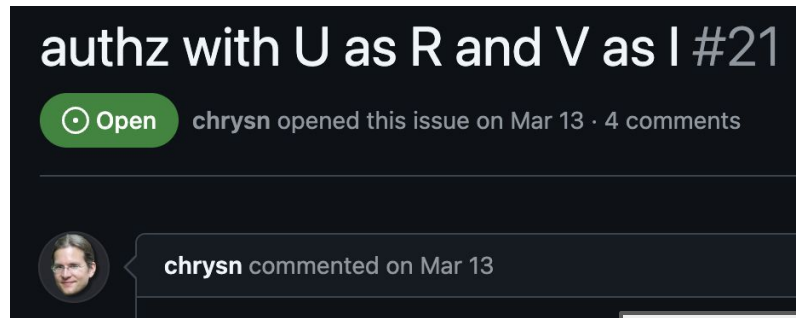
Also referred to as:

- **authz**
- **zero-touch network join**



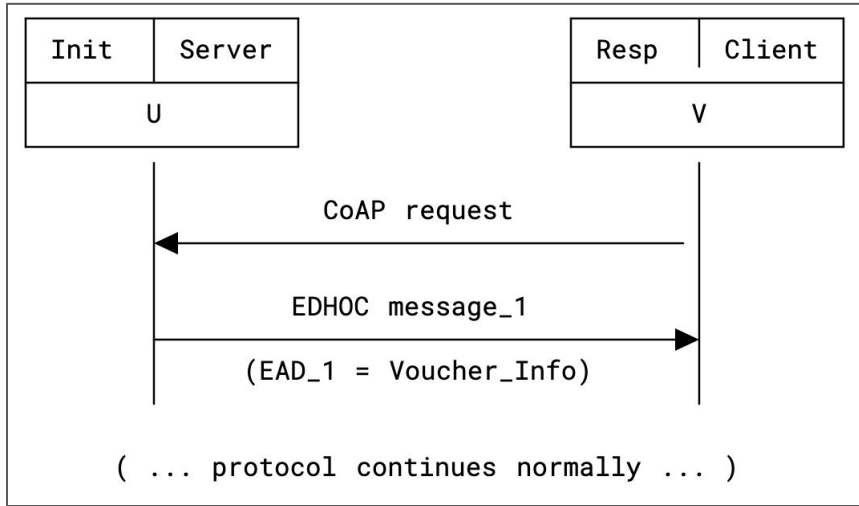
Now called
ELA!

+ new appendix: use with **EDHOC reverse flow**



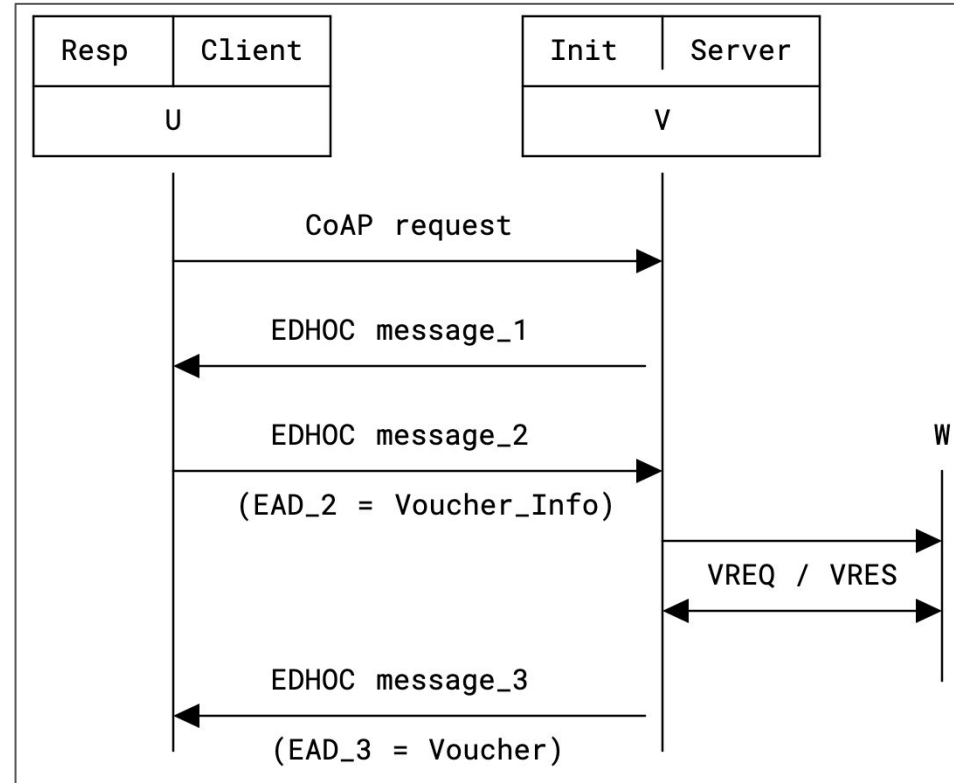
◀ earlier this year

+ new appendix: use with **EDHOC** reverse flow



1. U is Init/Server
2. U is Resp/Client

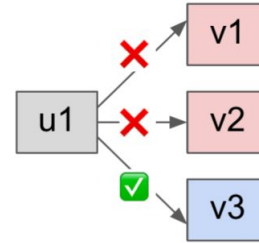
Different identity protection / trigger side
Choice depends on application



+ new section: **optimization strategies**

Problem at -00 version:

- blind attempts may lead to **several retries**



Consume
time ⌚ and
energy 🔋

⏪ IETF 120

+ new section: **optimization strategies**

1. U broadcasts message_1

- **minimal changes** to the protocol
- first successful message_2 is accepted
- error messages suppressed at V
 - Discussed during Hackathon

2. V advertises support for ELA

- V sends a **V_INFO** struct
 - contains e.g. V's domain name
- **too many ways to implement**
 - EDHOC forward/reverse
 - initiated by device/network
 - CoAP client/server

+ new appendix: **example advertisement strategies**

- **too many ways to implement**
 - EDHOC forward/reverse
 - initiated by device/network
 - CoAP client/server

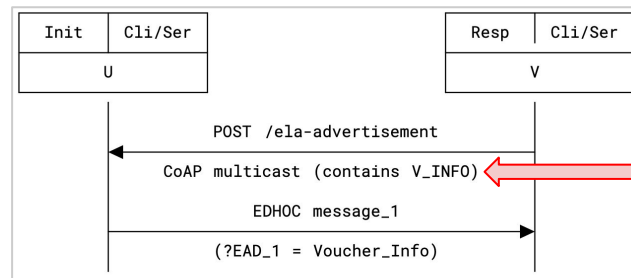
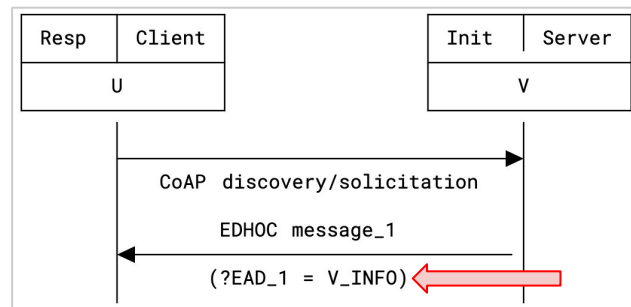
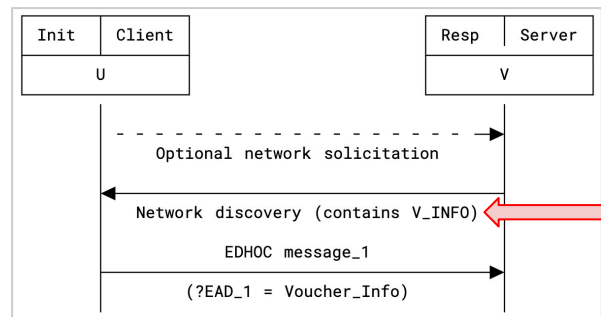
- many, many discussions
- in the end, it's network/application specific
- ELA is transport-agnostic, like EAP
- profiles will be needed

in this draft: just show a few representative *examples*

+ new appendix: **example advertisement strategies**

Evolve into
"mini-profiles"?

- 1 **V_INFO in network beacons**
 - works for BLE, IEEE 802.15.4
- 2 **V_INFO in EAD_1**
 - EDHOC reverse flow,
any link layer
- 3 **V_INFO in a CoAP Multicast Packet**
 - U as initiator, any link layer



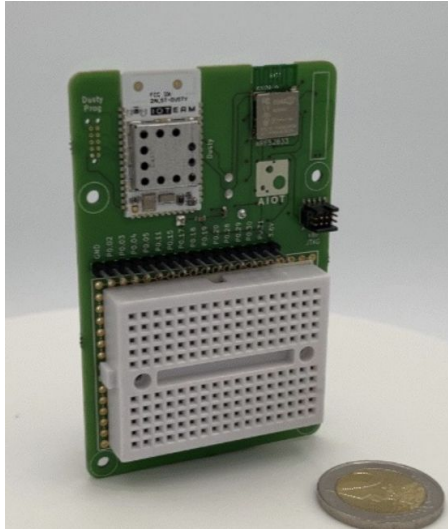
next steps (*super fresh discussion*)

- homogenize protocol elements for EDHOC reverse flow
 - e.g. VREQ includes message_1_or_2
- have the **core** specification solve **just** lightweight authorization
 - interoperable
- separate section for enrollment use cases
 - discuss broadcast of message_1, advertisements, etc.

Evaluation of ELA

Evaluation: two hardware platforms / network types

ELA vs EAP-EDHOC



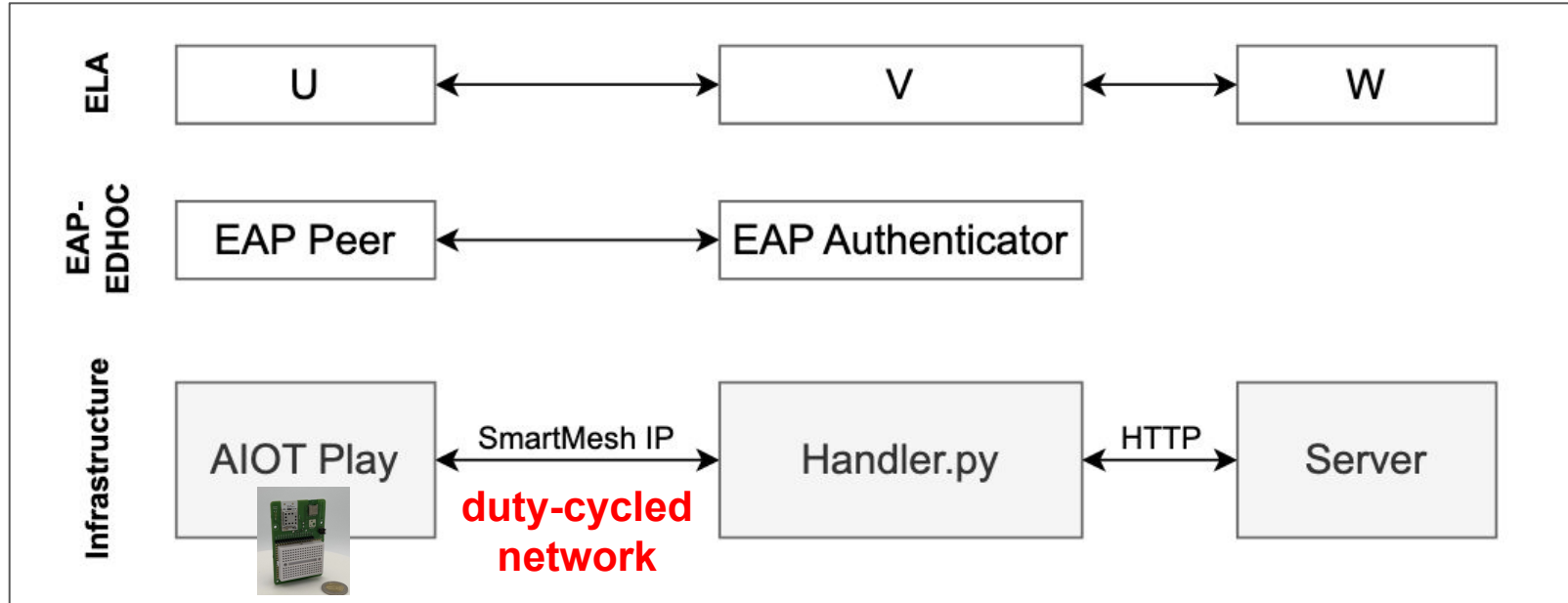
AIOT Play (nRF52833)
SmartMesh IP

ELA on DotBots

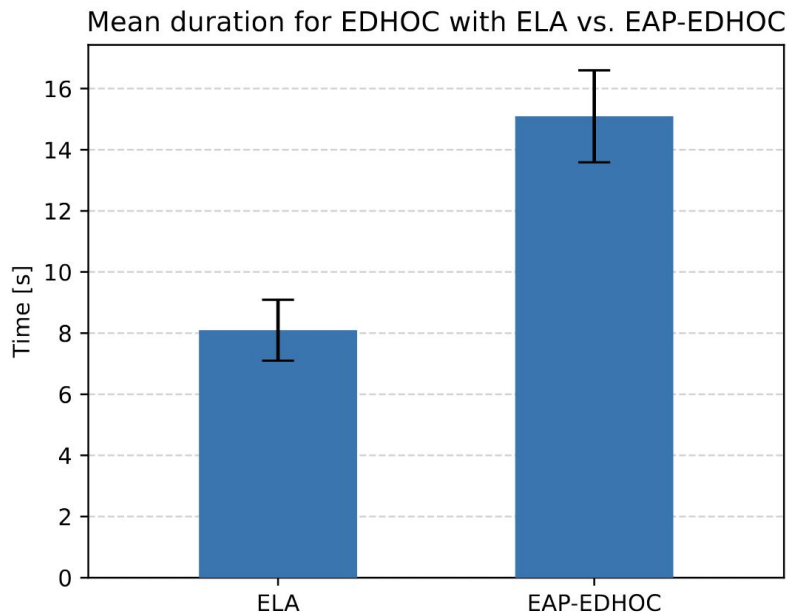


nRF5340, raw BLE

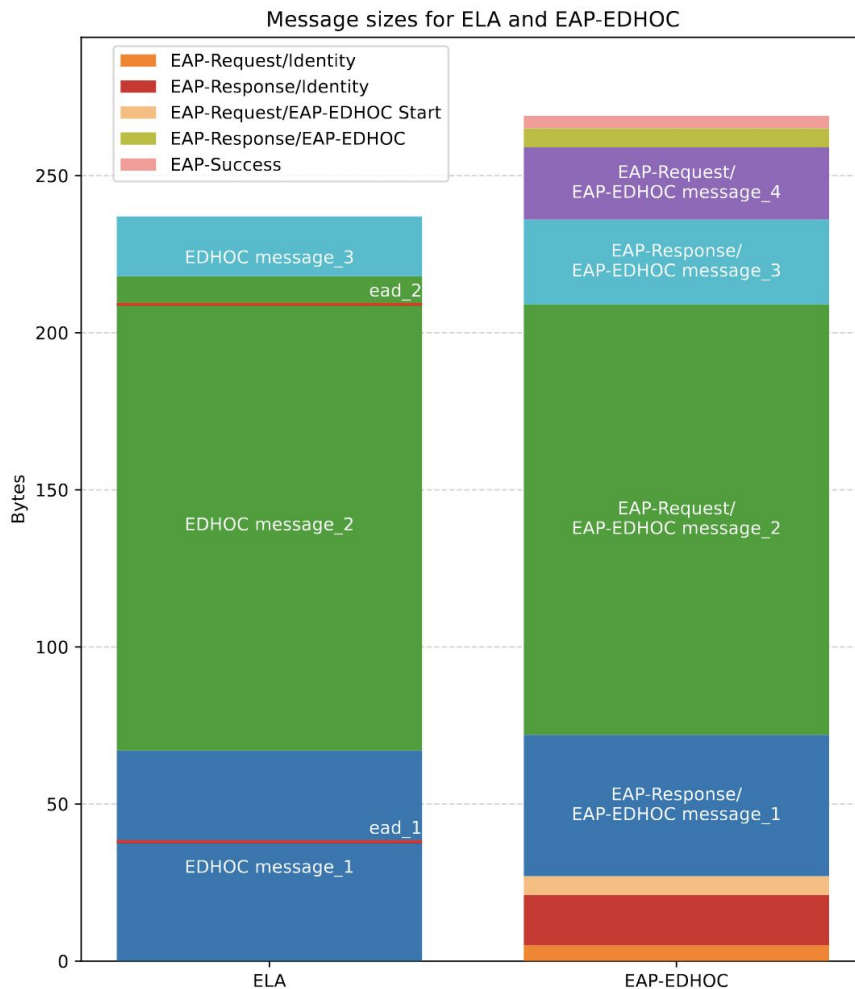
ELA vs. EAP-EDHOC



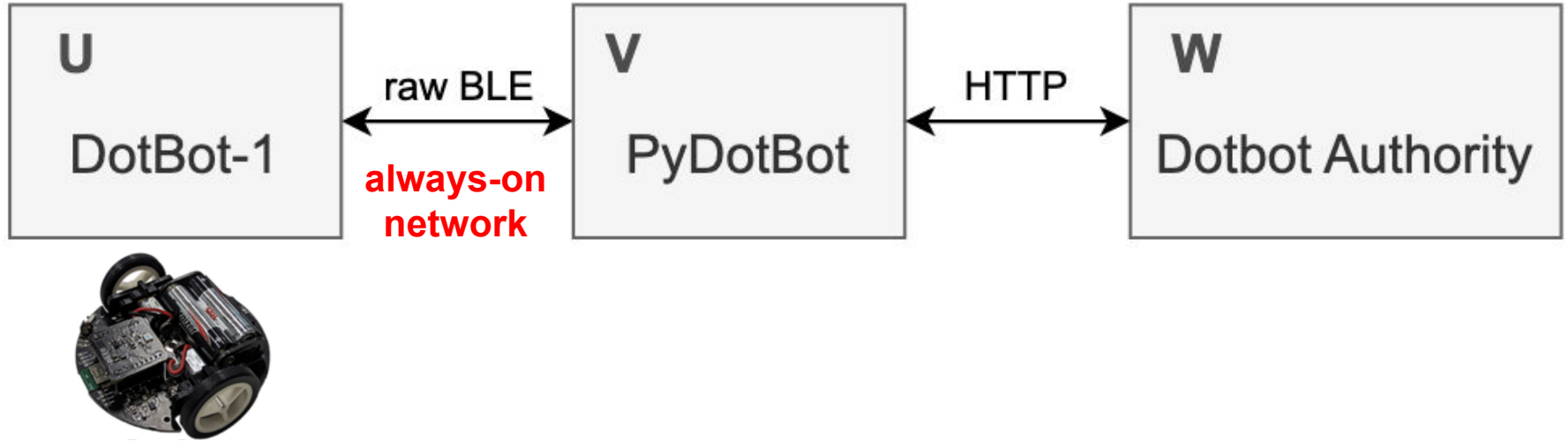
ELA vs. EAP-EDHOC



- Packet sizes: ~10% diff
- Handshake time: ~50% diff
 - *duty-cycled network*

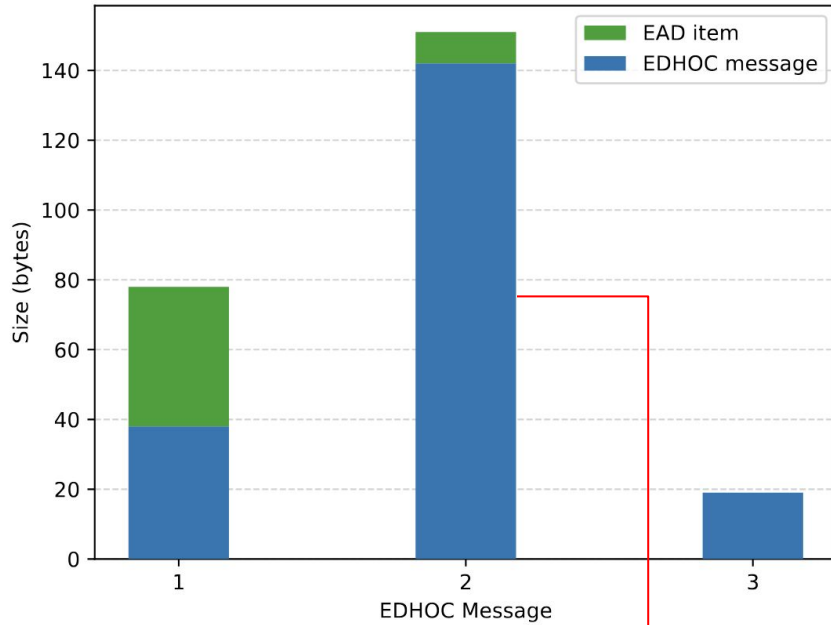


ELA on DotBots

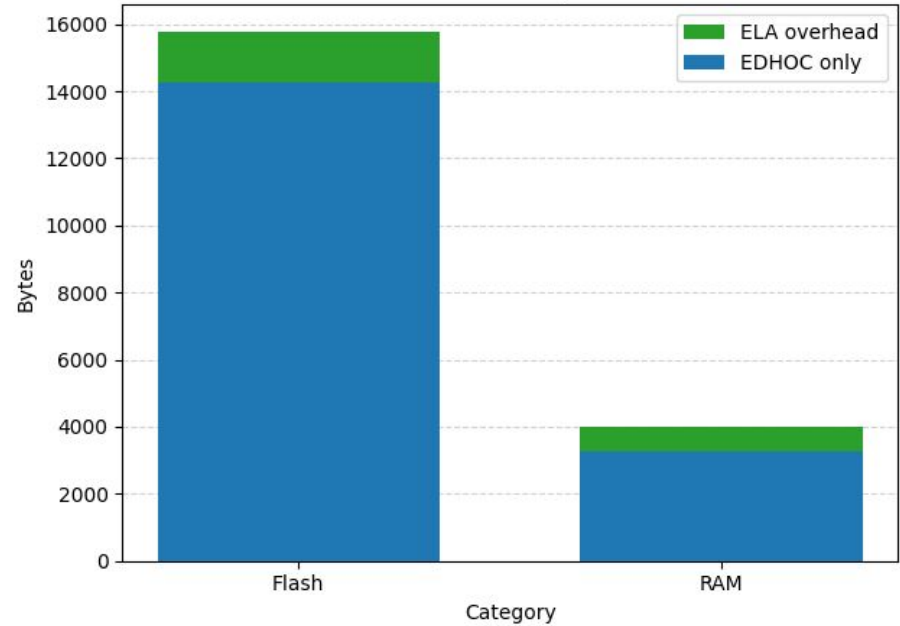


Message sizes and memory usage

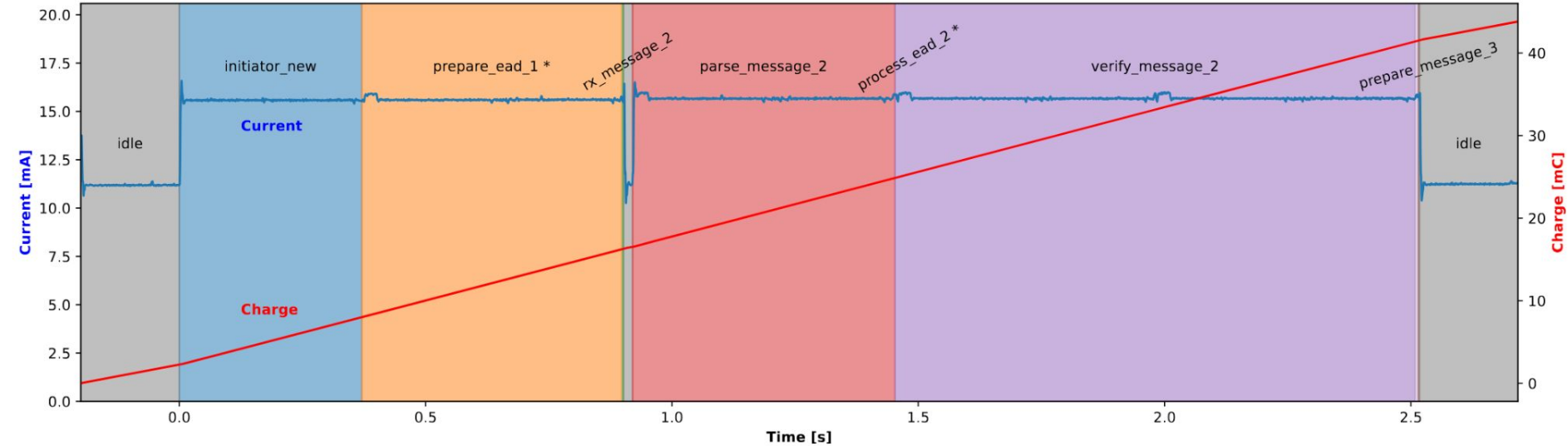
Message sizes for EDHOC with ELA



Flash and RAM Usage with ELA



Energy consumption during handshake



crypto done in software

thanks!
thoughts?

<https://datatracker.ietf.org/doc/draft-ietf-lake-authz>

geovane.fedrecheski@inria.fr