Scientific poster: Standards-based Remote Attestation for Internet-of-Things Swarms

Yuxuan Song, Mališa Vučinić, Thomas Watteyne

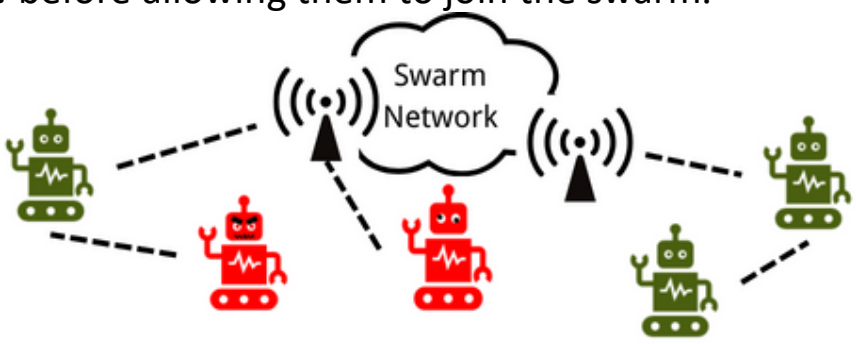
Standards-based Remote Attestation for Internet-of-Things Swarms

Yuxuan Song, Mališa Vučinić, Thomas Watteyne
Inria Paris, France
first.last@inria.fr

How to ensure that ***ONLY*** robots with ***verified and trustworthy*** software and hardware configurations are allowed to join the swarm ?

Assumption

Individuals in the swarm are attested through a ***central node*** before allowing them to join the swarm.

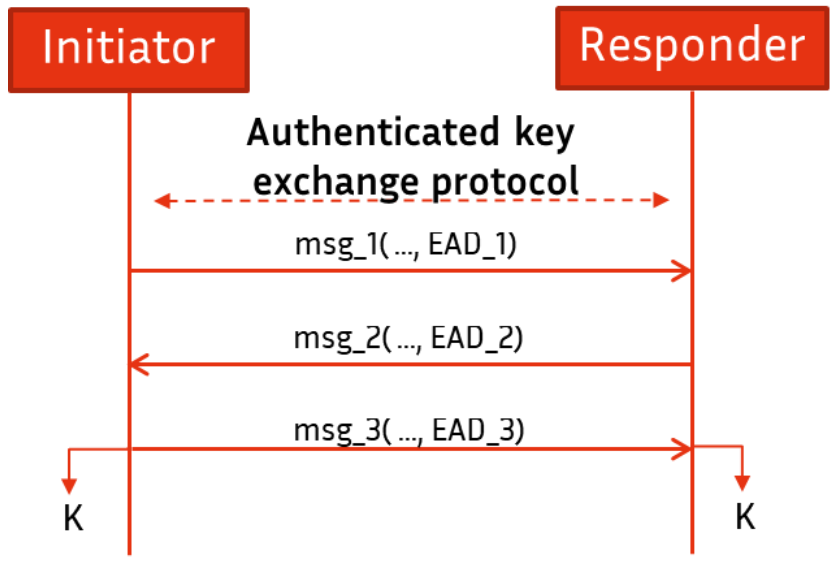


Background: Remote attsetation

Remote attestation [1] is a ***security process*** that can help the swarm central server establish a level of trust in the robot before allowing the robot to join the swarm.

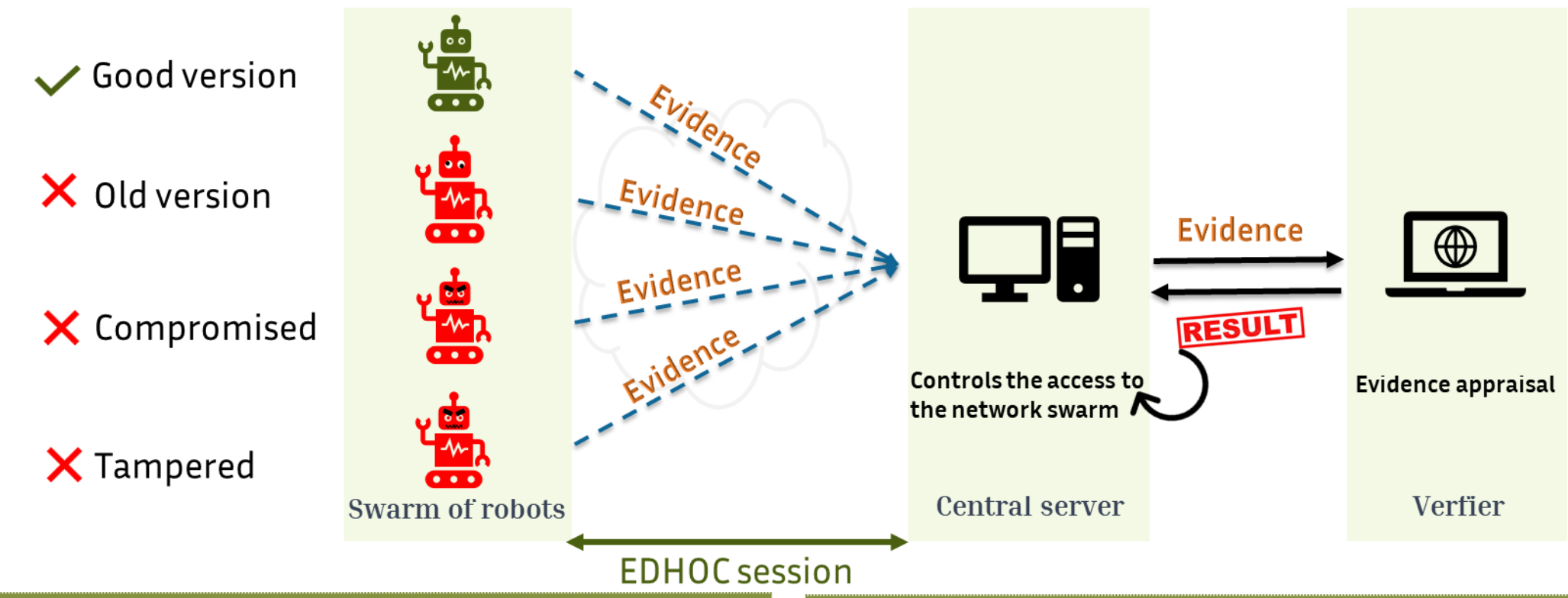
Background: EDHOC protocol

Ephemeral Diffie-Hellman over COSE (EDHOC) protocol [2] is a highly compact and efficient protocol that enables ***authenticated key exchange*** in ***constrained*** scenarios.



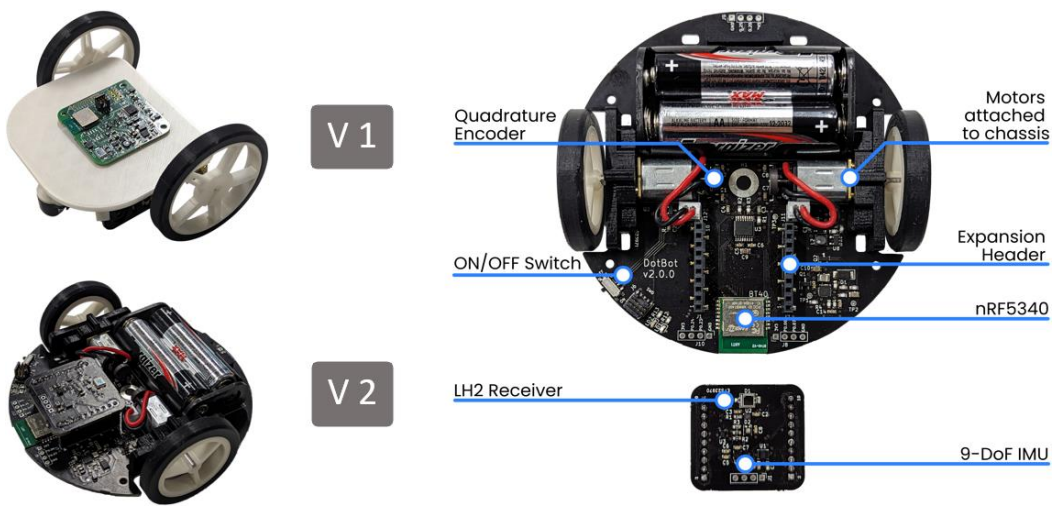
Attestation evidence is carried in EDHOC's External Authorization Data (EAD) fields.

Remote attestation over EDHOC for robot swarm



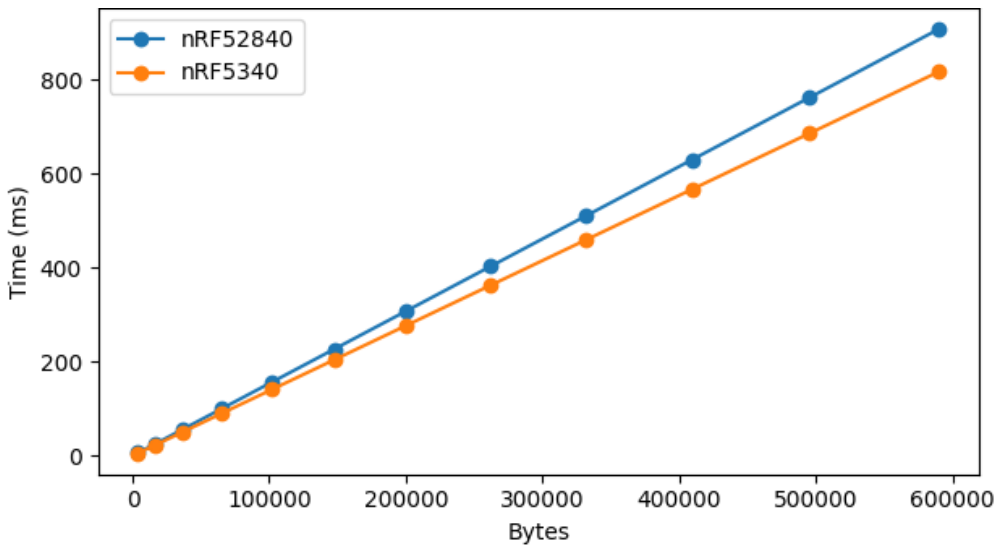
Evaluation

The micro-robots run on the nRF52840 microcontroller and the nRF5340 microcontroller.



Result

The feasibility of hashing the entire evidence on the constrained platforms.



ICRA2024 YOKOHAMA | JAPAN

[1] H. Birkholz, D. Thaler, M. Richardson, N. Smith, and W. Pan, Remote ATtestation procedureS (RATS) Architecture, Internet Engineering Task Force (IETF) Std. RFC9334, 2023.
[2] G. Selander, J. Preuß Mattsson, and F. Palombini, Ephemeral DiffieHellman Over COSE (EDHOC), Internet Engineering Task Force (IETF) Std. RFC9528, 2024.

** This document is issued within the frame and for the purpose of the OpenSwarm project. This project has received funding from the European Union's Horizon Europe Framework Program under Grant Agreement No. 101093046. Views and opinions expressed are however those of the author(s) only and the European Commission is not responsible for any use that may be made of the information it contains.*