

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

Yuxuan Song, Mališa Vučinić, Thomas Watteyne

▶ To cite this version:

Yuxuan Song, Mališa Vučinić, Thomas Watteyne. Scientific poster: Standards-based Remote Attestation for Internet-of-Things Swarms. IEEE International Conference on Robotics and Automation (ICRA), Breaking Swarm Stereotypes workshop, May 2024, Yokohama, Japan. hal-04630627

HAL Id: hal-04630627 https://inria.hal.science/hal-04630627

Submitted on 1 Jul 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers. L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



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

OpenSwarm

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.

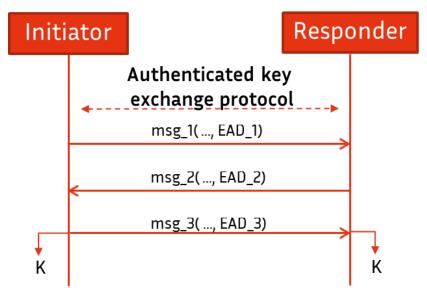


Background: Remote attsetation

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.

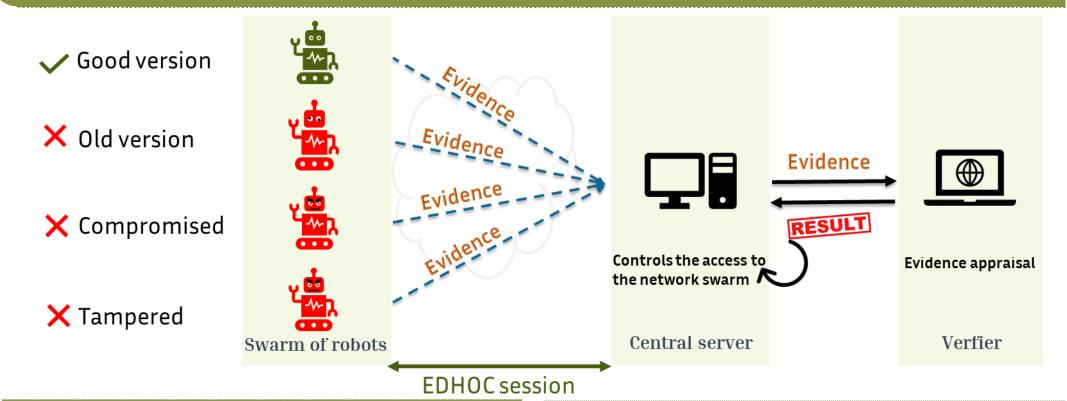
Background: EDHOC protocol

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



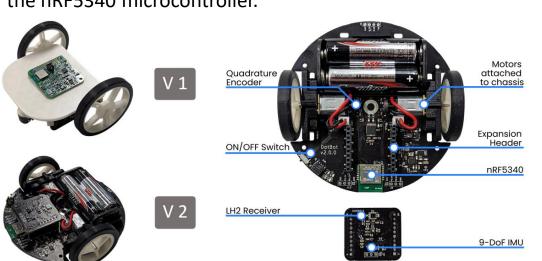
Attestation evidence is carried in EDHOC's External Authorization Data (EAD) fields.

Remote attestation over EDHOC for robot swarm



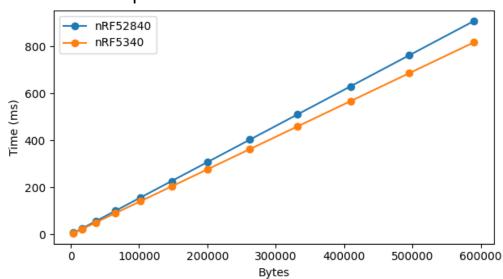
Evaluation

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

[1] H. Birkholz, D. Thaler, M. Richardson, N. Smith, and W. Pan, Remote ATtestation procedureS (RATS) Architecture, Internet Engineering Task Force (IETF) Std.

[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.