



**HAL**  
open science

## 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-04630627v1>**

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.



Distributed under a Creative Commons Attribution 4.0 International License

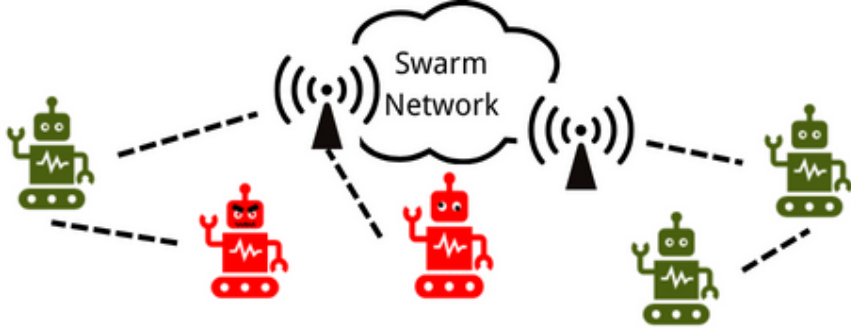
# Standards-based Remote Attestation for Internet-of-Things Swarms

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.

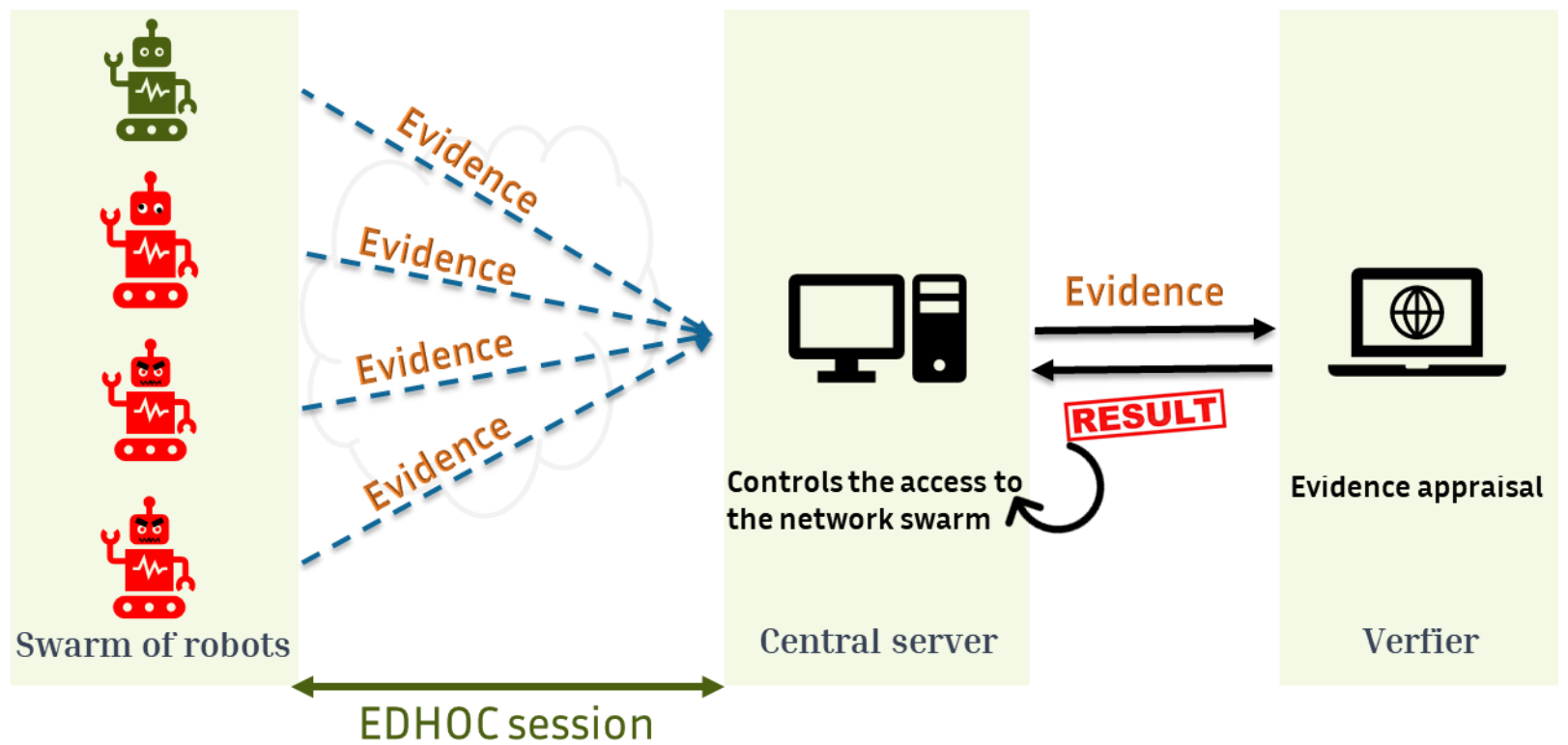


## Background: Remote attestation

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.

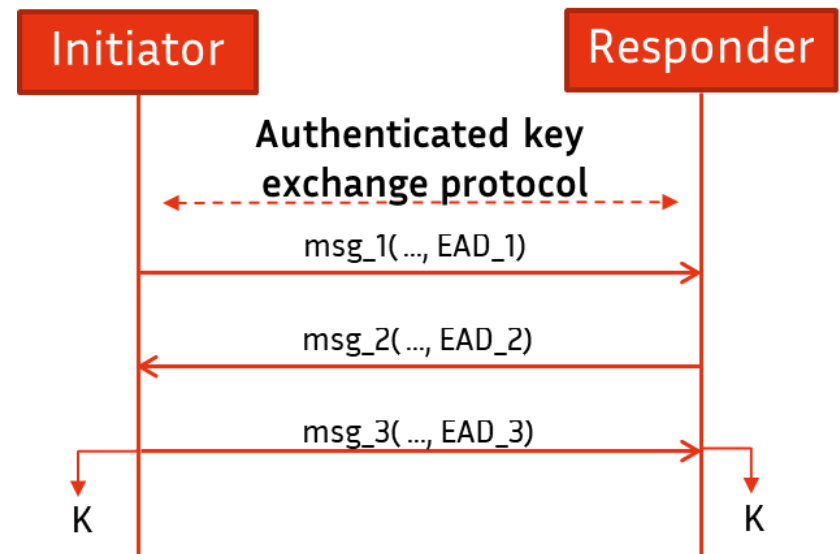
## Remote attestation over EDHOC for robot swarm

- ✓ Good version
- ✗ Old version
- ✗ Compromised
- ✗ Tampered



## Background: EDHOC protocol

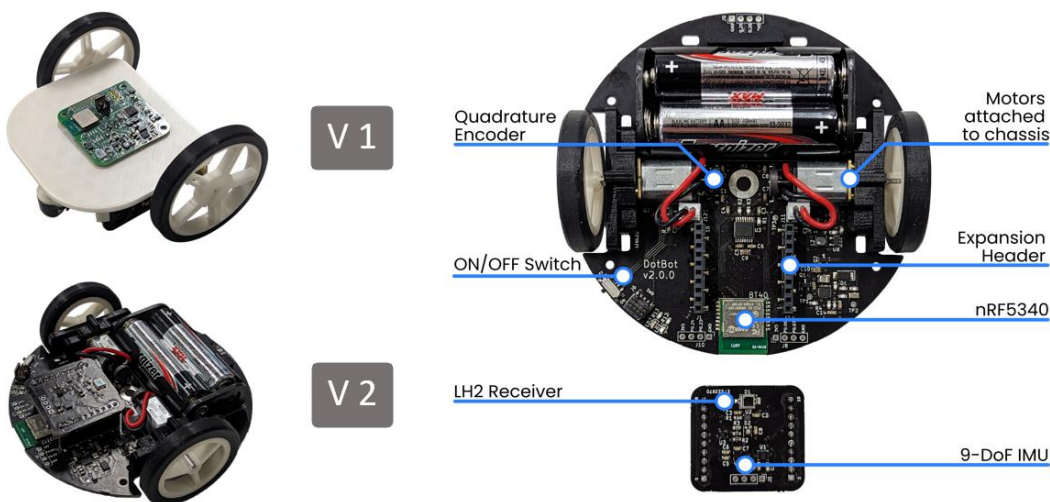
Ephemeral Diffie-Hellman over COSE (EDHOC) protocol [2] is a highly compact and efficient protocol that enables **authenticated key exchange** in **constrained** scenarios.



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

## 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.

