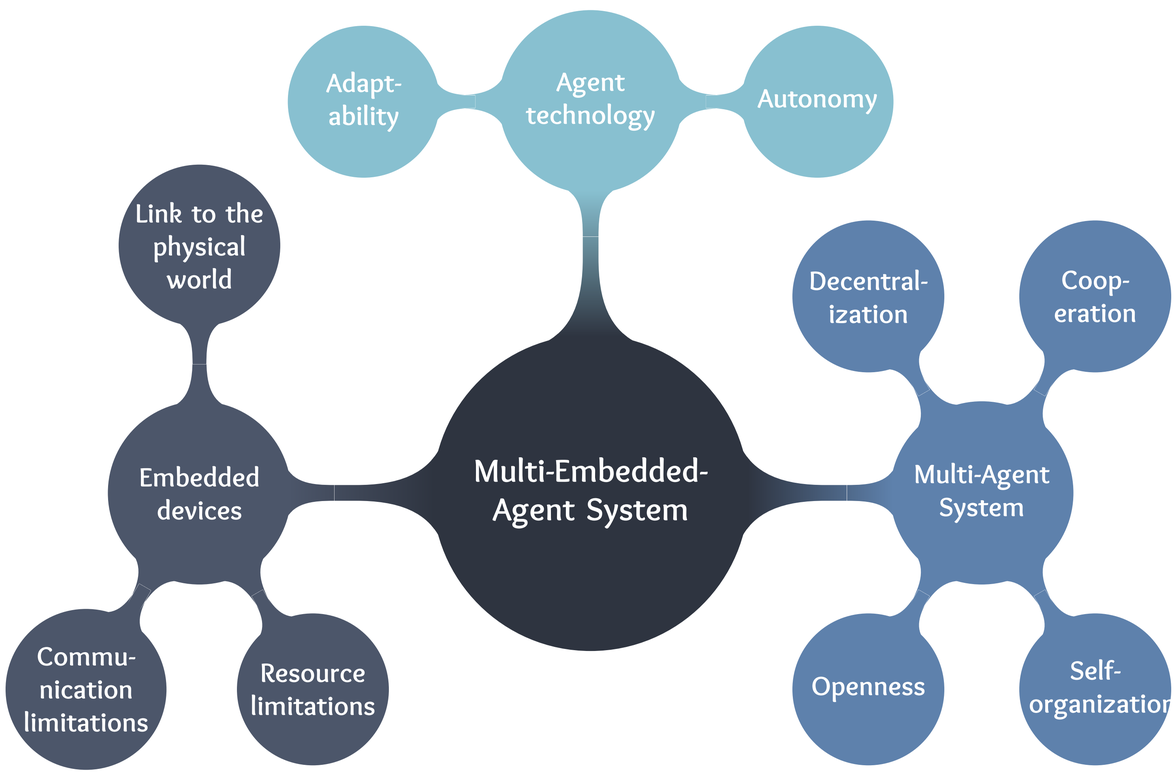
Decentralized key management for Multi-Embedded-Agent Systems

Arthur Baudet, Oum-El-Kheir Aktouf, Philippe Elbaz-Vincent, Annabelle Mercier

LCIS — INSTITUT FOURIER

Context: Increase of autonomy in distributed systems to cope with the complexity of nowadays applications
Objective: Provide confidentiality, authenticity and integrity to these decentralized systems by deploying a specially designed public key infrastructure

Multi-Embedded-Agent System Properties



MEAS can be used in

- Wireless Sensor Networks
- Autonomous Vehicle Networks
- Mobile Ad Hoc Networks
- Any distributed systems of embedded devices

Threat model and constraints

- Attackers can tamper with and forge messages
- Attackers have similar resources as agents (mote-class)
- Attackers can generate as many identities as they want (Sybil attacks)
- Physical interception (e.g., selective jamming) is impossible or at least possible to detect
- No preexisting knowledge of the system
- No preexisting trust in the agents (Byzantine model)

Multi-Agent Key Infrastructure (MAKI)

Lightweight Public Key Infrastructure (PKI)

- Certificate Authorities (CAs) are self-signed
- Small, short-lived certificate
- Coordination through Registration Authorities (RAs)
- Explanatory Certificate Revocation List (CRL)
- CAs certificates are not stored beforehand
- Each identity is a pair of `(name, public key)`

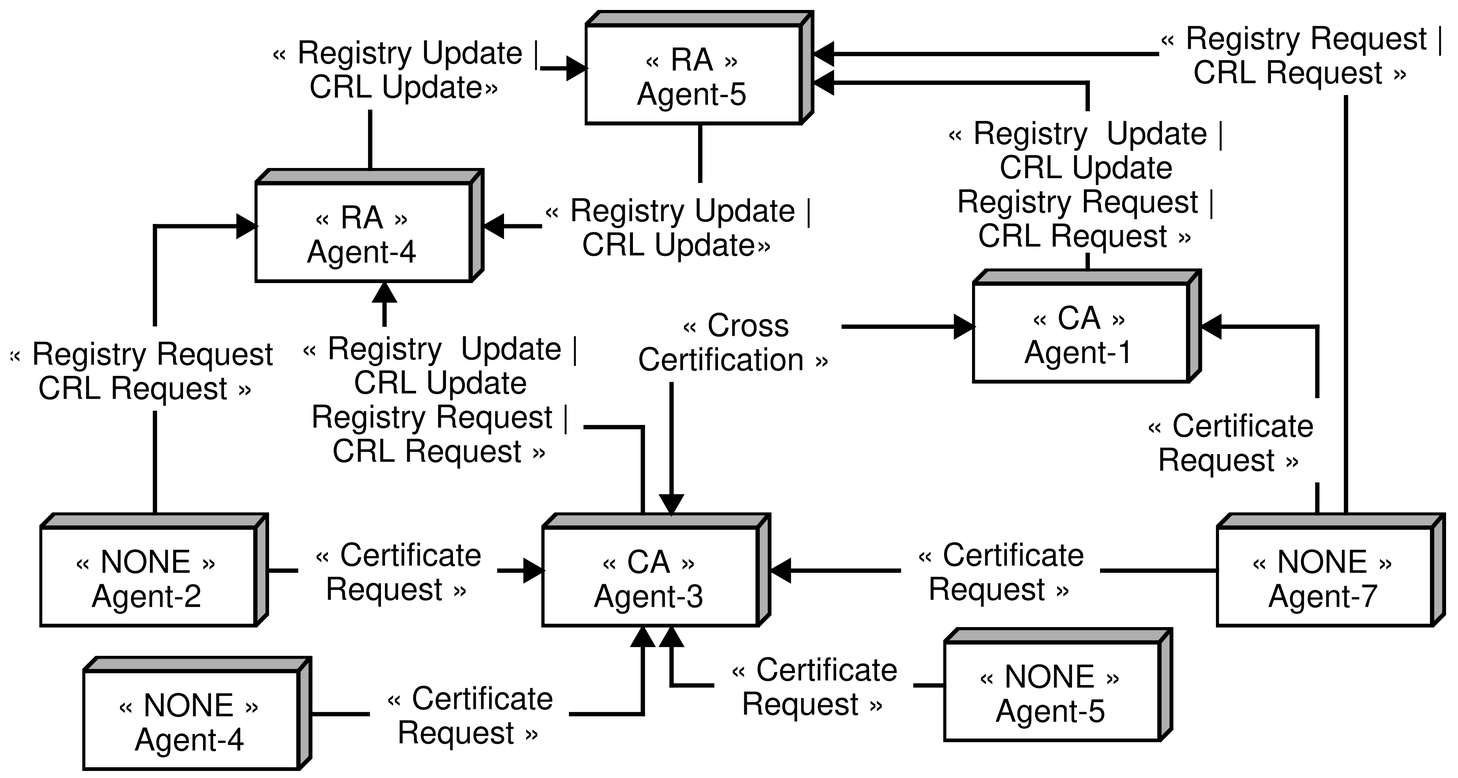
Trust Management System

- To choose the right CA/RAs
- To detect intruders
- To trigger the intruders revocation

Adaptation algorithms

- 3 roles: CA, RA, None (default)
- CAs/RAs elections or self-appointments

Example of interactions in MAKI



Contributions

- Authenticity and integrity check for communications using signatures
- Accountability for each communication using signatures
- Confidentiality when necessary using symmetric encryption
- Exclusion using CRL and not renewing expired certificates

Certificate Authority responsibilities

- Deliver certificates
- Update RA
- Revoke certificates of untrusted identities

Registration Authority responsibilities

- Store valid certificates
- Store the CRL
- Coordinate to maintain information up to date
- Share information when requested

Challenges and future work

Maintaining a shared database is not trivial and not secure when there is no initial trust between the maintainers. We are working on a blockchain-based solution to replace the RAs by a blockchain adapted to our needs and constraints.

The total autonomy of the agents requires the designers to define various rules to dissociate malicious from benevolent agents, especially for CAs and RAs.

The trust model should be fine tuned to reduce the benefits of maintaining multiple identities at once.

System startup is critical as it may lead to malicious agent gaining weight in the system very early. A solution would be to start the system in a controlled environment before opening it so that benevolent CAs and RAs could gain trust of the first agents; reducing the risk of having only malicious authorities.

Contact: `arthur.baudet@lcis.grenoble-inp.fr`

Cybersecurity Institute
Université Grenoble Alpes

This work is supported by the French National Research Agency in the framework of the "Investissements d'avenir" program (ANR-15-IDEX-02)