Cybersecurity Institute

Reshaping technologies and social sciences

Decentralized Public Key Infrastructure for Autonomous Embedded Systems

Arthur Baudet, **Oum-El-Kheir Aktouf,**
Annabelle Mercier, Philippe Elbaz-Vincent
arthur.baudet@lcis.grenoble-inp.fr

C&ESAR — 2022-11-16

financed by
IDEX 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).
Reproduction prohibited without written permission of the authors.

Ongoing work

Agent

- Physical or software entity
- Autonomous (proactive or/and reactive)

Embedded agent

- Resources limitations
- Communication limitation
- Mobility

Multi-Agent Key Infrastructure

- >2 agents
- Decentralized
- Global problem divided in smaller problems
- Cooperation between agents
- Open
- Dynamic
- Heterogeneous

Russell et al., Wooldridge et al. [1, 2]

Wildfire Monitoring

Drones monitoring a wildfire

Wildfire Monitoring

Drones monitoring a wildfire and intruders

Availability
Communication Integrity

What is done
to secure MEAS?

State of the Art

What is done
to secure MEAS?

→ Availability
Communication Integrity

→ Trust Management System
Cryptography

State of the Art

What is done
to secure MEAS?

Availability
Communication Integrity

Trust Management System
Cryptography

State of the Art

What is done
to secure MEAS?

Availability
Communication Integrity

Trust Management System
Cryptography

Pre-loaded certificate & key
Third-party

State of the Art

What is done
to secure MEAS?

Availability
Communication Integrity

Trust Management System
Cryptography

Pre-loaded certificate & key
Third-party

Conflict with
Autonomy & Heterogeneity

Cybersecurity Institute

Attacker Model

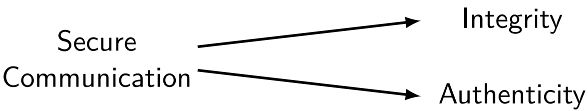
“Insider attack”: Similar resources as nodes

Control over communication medium: Tampering, replay, etc.

Attacker Model

"Insider attack": Similar resources as nodes

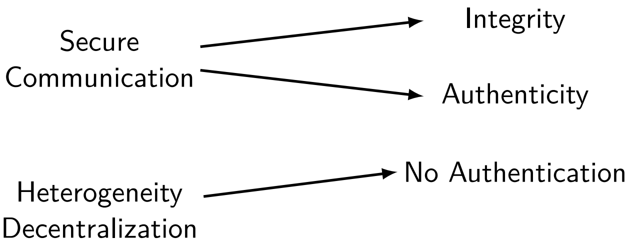
Control over communication medium: Tampering, replay, etc.



Attacker Model

"Insider attack": Similar resources as nodes

Control over communication medium: Tampering, replay, etc.



Objective

Attacker Model

"Insider attack": Similar resources as nodes

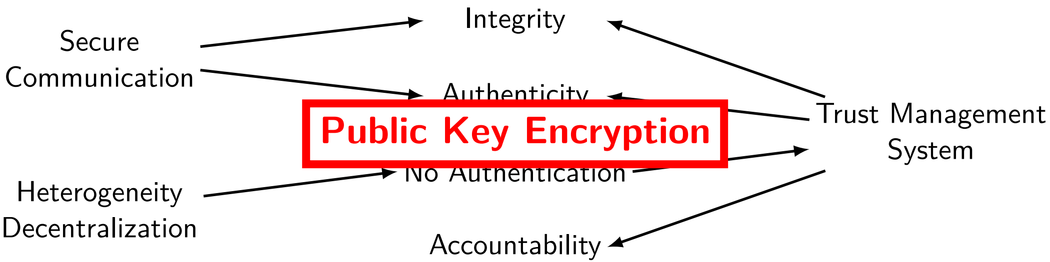
Control over communication medium: Tampering, replay, etc.

Cybersecurity Institute

Attacker Model

"Insider attack": Similar resources as nodes

Control over communication medium: Tampering, replay, etc.



Multi-Agent Key Infrastructure (MAKI)
Public Key Infrastructure for Multi-Agent System

Multi-Agent Key Infrastructure (MAKI)
Public Key Infrastructure for Multi-Agent System

Main Rule

Messages must be signed with a key linked to a valid certificate.

Hypotheses

1. Standard cryptography is secured
2. Basic routing exists
3. An adequate Trust Management System (TMS) is running

Identity $\longleftrightarrow$ Public Key

Cybersecurity Institute

Identity ⟷ Public Key

Role: None

- Default
- Require a CA to get a certificate
- Share its certificate

Role: Certification Authority (CA)

- Deliver, store and revoke certificates
- Self-signed or cross-certified
- Share its certificate

Identity $\longleftrightarrow$ Public Key

Role: None

- Default
- Require a CA to get a certificate
- Share its certificate

Role: Certification Authority (CA)

- Deliver, store and revoke certificates
- Self-signed or cross-certified
- Share its certificate

Revocation

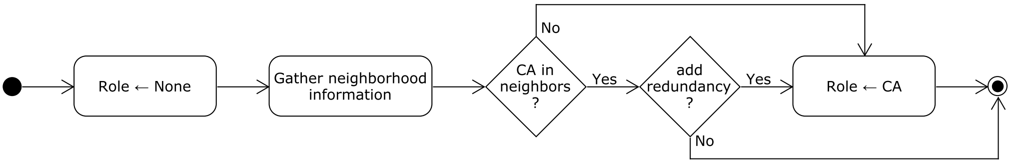
- Certificate Revocation List
- Short-lived certificate

Global Rules

- At least one CA is required
- > 1 CA is advisable to prevent single-point-of-failure situations
- Agents choose their roles
- Any agent can become a CA

Global Rules

- At least one CA is required
- >1 CA is advisable to prevent single-point-of-failure situations
- Agents choose their roles
- Any agent can become a CA



Role self-assignment flowchart

Cybersecurity Institute

3 Thresholds

- Low
- Moderate
- High

Cybersecurity Institute

3 Thresholds

- Low
- Moderate
- High

Interaction Rules

Certificate Authority	
Delivering a certificate	Moderate or None
Revoking a certificate	Moderate
Requesting a cross-certification	High
Accepting a cross-certification request	High
None	
Requesting a certificate	Moderate or None

Interaction Rules

Certificate Authority	
Delivering a certificate	Moderate or None
Revoking a certificate	Moderate
Requesting a cross-certification	High
Accepting a cross-certification request	High
None	
Requesting a certificate	Moderate or None

3 Thresholds

- Low
- Moderate
- High

Delevering certificate: $\nearrow$ trust

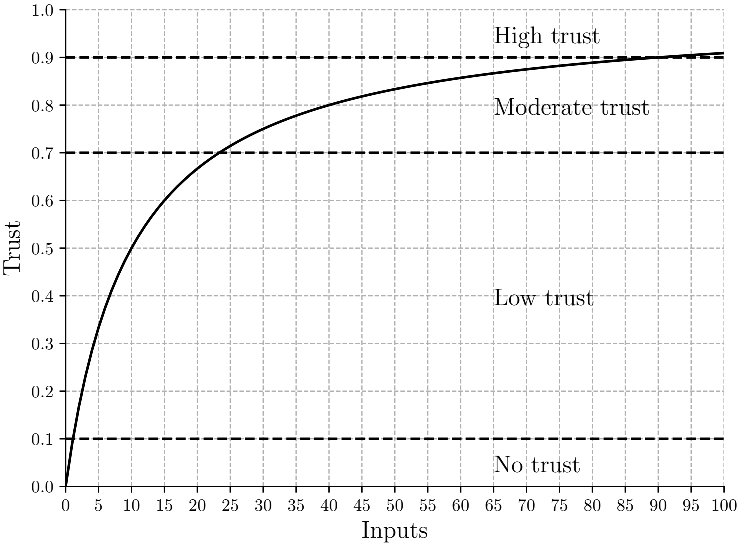
Being cross-certified: $\nearrow$ trust

Ignoring requests: $\searrow$ trust

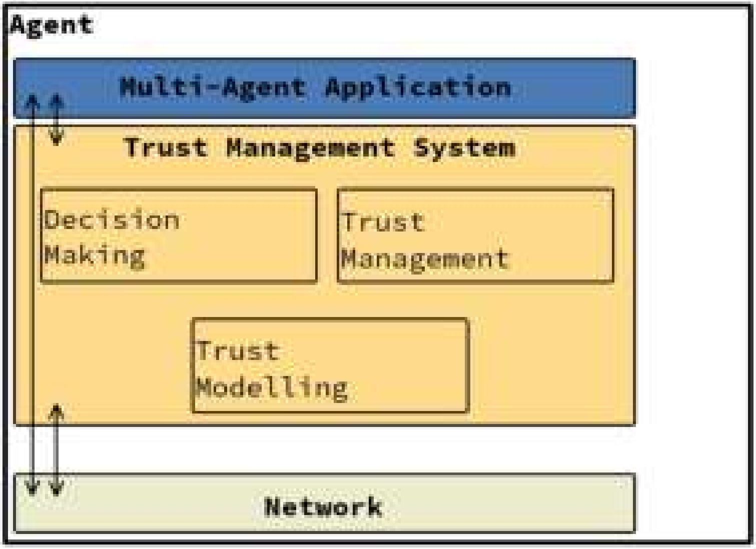
Trust Modelling

$$f : \mathbb{N} \to \mathbb{N}_+$$
$$x \mapsto \frac{x}{x+10}$$

- Slow increase
- Fast decrease

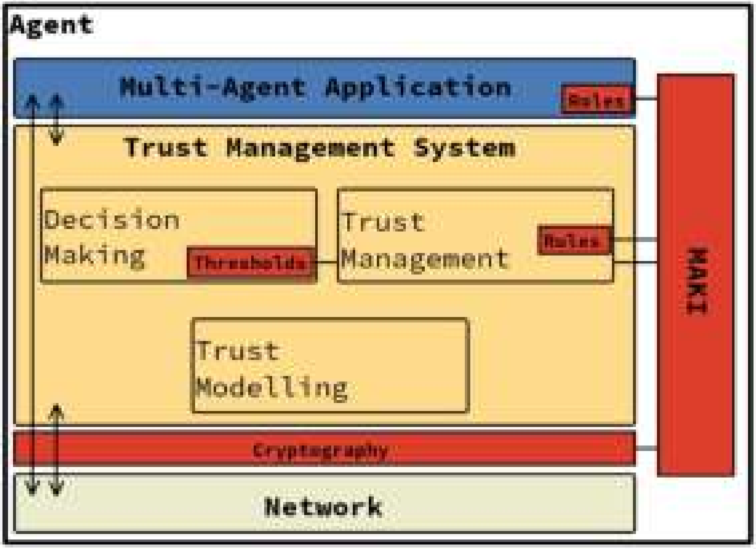


Cybersecurity Institute



Agent architecture without MAKI

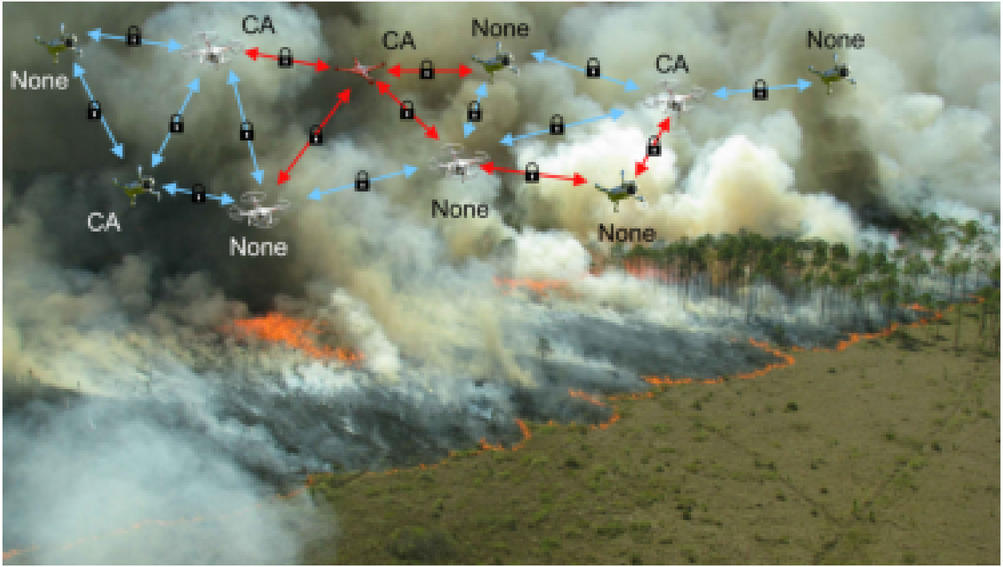
Cybersecurity Institute



Agent architecture with MAKI

Wildfire Monitoring

Cybersecurity Institute



Drones monitoring a wildfire executing MAKI

Cybersecurity Institute

Q1: Does the TMS really benefits from MAKI?

Q2: Does the self-organization leads to the correct organization?

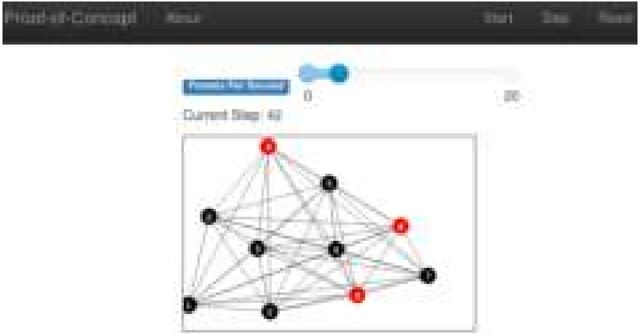
Q1: Does the TMS really benefits from MAKI?

Q2: Does the self-organization leads to the correct organization?

Simulation

Yet Another Multi-Agent Systems Simulator (YAMASS)

- In-house simulator
- Ongoing work
- Based on Mesa [3]
- Allows easy reproducibility
- Enforces agents positioning

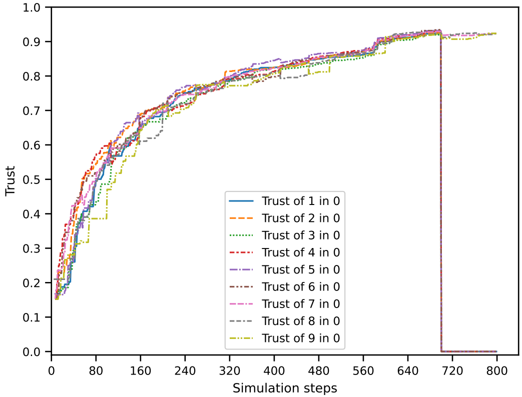


Simulation of a MEAS executing MAKI in YAMASS
Red: CA, Black: None

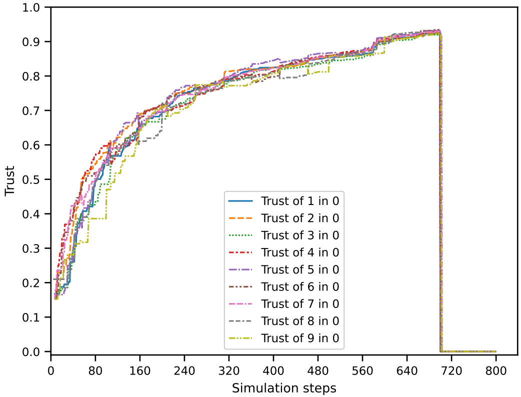
- 10 agents
  - ↦ 4 possible CAs: $\mathcal{A}_6, \mathcal{A}_7, \mathcal{A}_8, \mathcal{A}_9$
    - ↦ 3 CAs: $\mathcal{A}_6, \mathcal{A}_8, \mathcal{A}_9$
- All in communication range
- Application is emulated

Scenario I — None agent intrusion

None agent ($\mathcal{A}_0$) is malicious



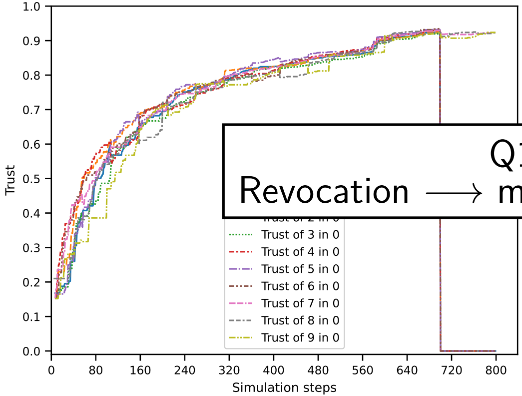
Trust variation without revocation



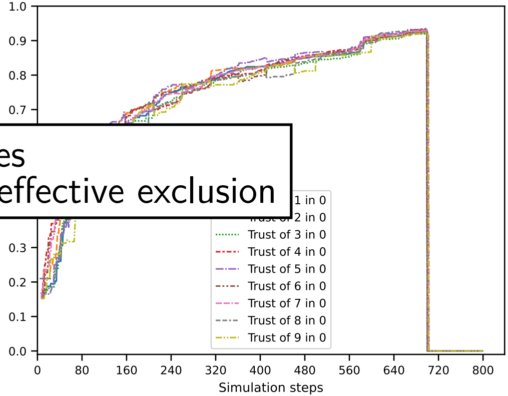
Trust variation with revocation

Cybersecurity Institute

None agent ($\mathcal{A}_0$) is malicious



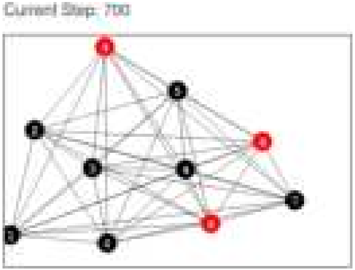
Trust variation without revocation



Trust variation with revocation

Q1: Yes
Revocation $\longrightarrow$ more effective exclusion

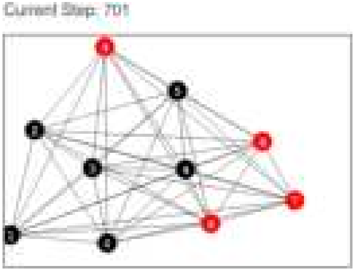
All the CAs ($\mathcal{A}_6$, $\mathcal{A}_8$, $\mathcal{A}_9$) are malicious



State of the system
before the detection
Red: CA, Black: None

Cybersecurity Institute

All the CAs ($\mathcal{A}_6$, $\mathcal{A}_8$, $\mathcal{A}_9$) are malicious

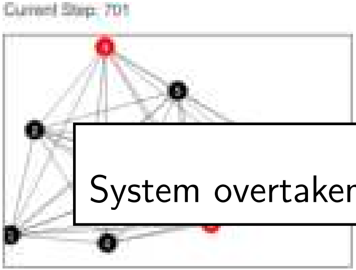


State of the system
after the detection
Red: CA, Black: None

```
step:701
agent:7:<>:CertAdvert(Certificate(issuer: 7,
subject: 7, ...))
agent:0:=>:CertReq(src: 0, dest: 7)
agent:1:=>:CertReq(src: 1, dest: 7)
agent:3:=>:CertReq(src: 3, dest: 7)
agent:2:=>:CertReq(src: 2, dest: 7)
agent:4:=>:CertReq(src: 4, dest: 7)
agent:5:=>:CertReq(src: 5, dest: 7)
```

Simplified excerpt of the execution trace

All the CAs ($\mathcal{A}_6$, $\mathcal{A}_8$, $\mathcal{A}_9$) are malicious



State of the system
after the detection
Red: CA, Black: None

```
step:701
agent:7:<>:CertAdvert(Certificate(issuer: 7,
subject: 7, ...))
agent:2:=>:CertReq(src: 2, dest: 7)
agent:4:=>:CertReq(src: 4, dest: 7)
agent:5:=>:CertReq(src: 5, dest: 7)
```

Simplified excerpt of the execution trace

Q2: Yes
System overtaken $\longrightarrow$ Self-organization: $\mathcal{A}_7$ becomes a CA

Takeaway

- No standard for key management in decentralized autonomous systems
- ✓ MAKI: Multi-Agent Key Infrastructure is PKI for decentralized autonomous systems
- → Stronger hypotheses can be taken

- × Slow start
- × Few strong assurances

Future work

→ Self-Organization validation: Model checking

→ Proof-of-Concept: State of the art trust model

→ Sharing certificates: Blockchain-based solution

Thank you for your attention

Questions?

[1] Stuart J Russell and Peter Norvig. *Artificial intelligence: a modern approach*. 1995. ISBN: 0-13-360124-2.

[2] Michael Wooldridge and Nicholas R Jennings. "Intelligent agents: Theory and practice". In: *The knowledge engineering review* 10.2 (1995), pp. 115–152. DOI: 10.1017/S0269888900008122.

[3] Jackie Kazil, David Masad, and Andrew Crooks. "Utilizing Python for Agent-Based Modeling: The Mesa Framework". In: *Social, Cultural, and Behavioral Modeling*. Vol. 12268. 2020, pp. 308–317. DOI: 10.1007/978-3-030-61255-9_30.

[4] National Institute of Standards and Technology. *Security and Privacy Controls for Information Systems and Organizations*. Tech. rep. NIST Special Publication 800-53, Revision 5. Washington, D.C.: U.S. Department of Commerce, 2020. DOI: 10.6028/NIST.SP.800-53r5.

[5] Jason Chia, Swee-Huay Heng, Ji-Jian Chin, Syh-Yuan Tan, and Wei-Chuen Yau. "An Implementation Suite for a Hybrid Public Key Infrastructure". In: *Symmetry* 13 (Aug. 2021), p. 1535. DOI: 10.3390/sym13081535.

[6] Arthur Baudet, Oum-El-Kheir Aktouf, Annabelle Mercier, and Philippe Elbaz-Vincent. "Systematic Mapping Study of Security in Multi-Embedded-Agent Systems". In: *IEEE Access* 9 (2021), pp. 154902–154913. DOI: 10.1109/ACCESS.2021.3128287.

[7] The under construction, forest wildfire, drones and padlocks figures are under the Pixabay License (Free for commercial use, No attribution required, https://pixabay.com/service/terms/#license, last visited the 2022-11-07). Thank you users Josethestoryteller, maja7777, dayamay, PublicDomainImages, and Clker-Free-Vector-Images for sharing them.