Cybersecurity Institute
Université Grenoble Alpes

IARIA

A Public Key Infrastructure for Multi-embedded-agent Systems

Securware Keynote November 5th 2024

Presenter Annabelle.Mercier@lcis.grenoble-inp.fr

LCIS

INSTITUT FOURIER

on the basis of Arthur Baudet's PhD work (2020-2023)
Supervising team: O. Aktouf, A. Mercier, Ph. Elbaz-Vincent

Université Grenoble Alpes

financed by IDEX Université Grenoble Alpes

Ce travail a bénéficié d'une aide de l'Etat gérée par l'Agence Nationale de la Recherche au titre du programme « Investissements d'avenir » portant la référence ANR-15-IDEX-02.

Short bio

- Master's degree in computer science at University Nice Sophia Antipolis on contractualization of component-based software and nonfunctional properties.

- Ph.D. degree at School of Mines of St Étienne. Thesis in information retrieval domain with participations at international information retrieval campaigns (TREC, CLEF) to test proximity ranking approach on benchmarks.

- Associate Professor at the Univ. Grenoble Alpes and researcher at the LCIS lab since 2007. Several topics : services composition, detection of collective products (emergence) provided by autonomous and decentralized systems (multiagent) with a focus on testing and security, digital twins and CPS.

Annabelle Mercier

Université Grenoble Alpes – LCIS Lab

Outline

MEAS and Security: The general problem

The problem

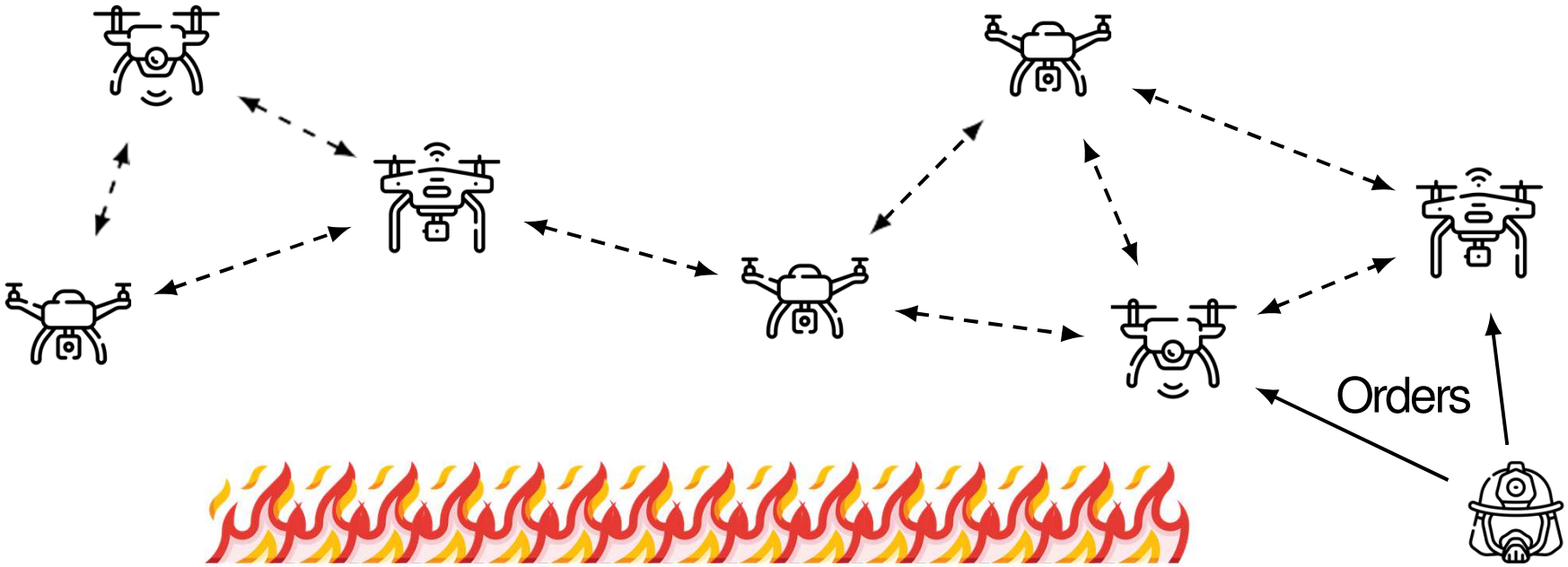
What's a Public Key Infrastructure?

MAKI: My Solution

Conclusion & Perspectives

From Networked Embedded Systems

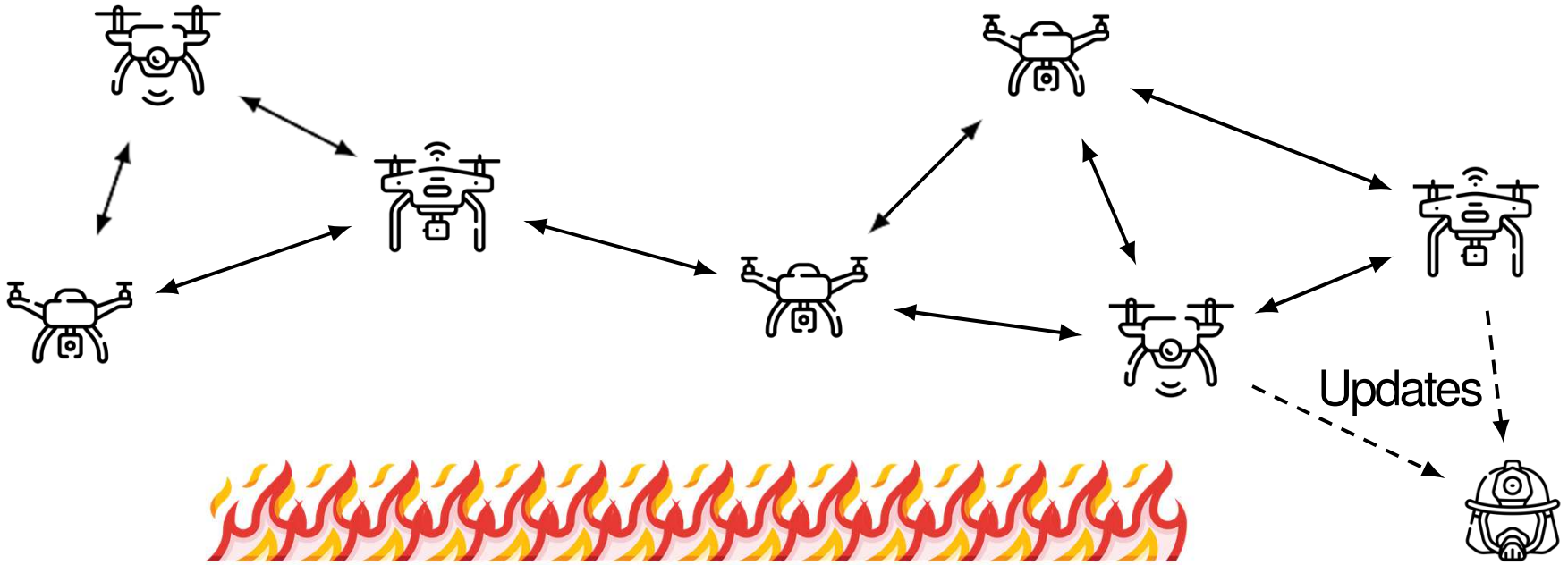
- Firefighters launch and give orders to drones
- Drones forward and follow orders



To Multi-Agent Systems of Embedded Agents

- Firefighters launch & replace drones
- Orders are set once

- Drones cooperate autonomously
- Firefighters are updated when necessary



Multi-Agent Systems of Embedded Agents (MEAS)
A Definition

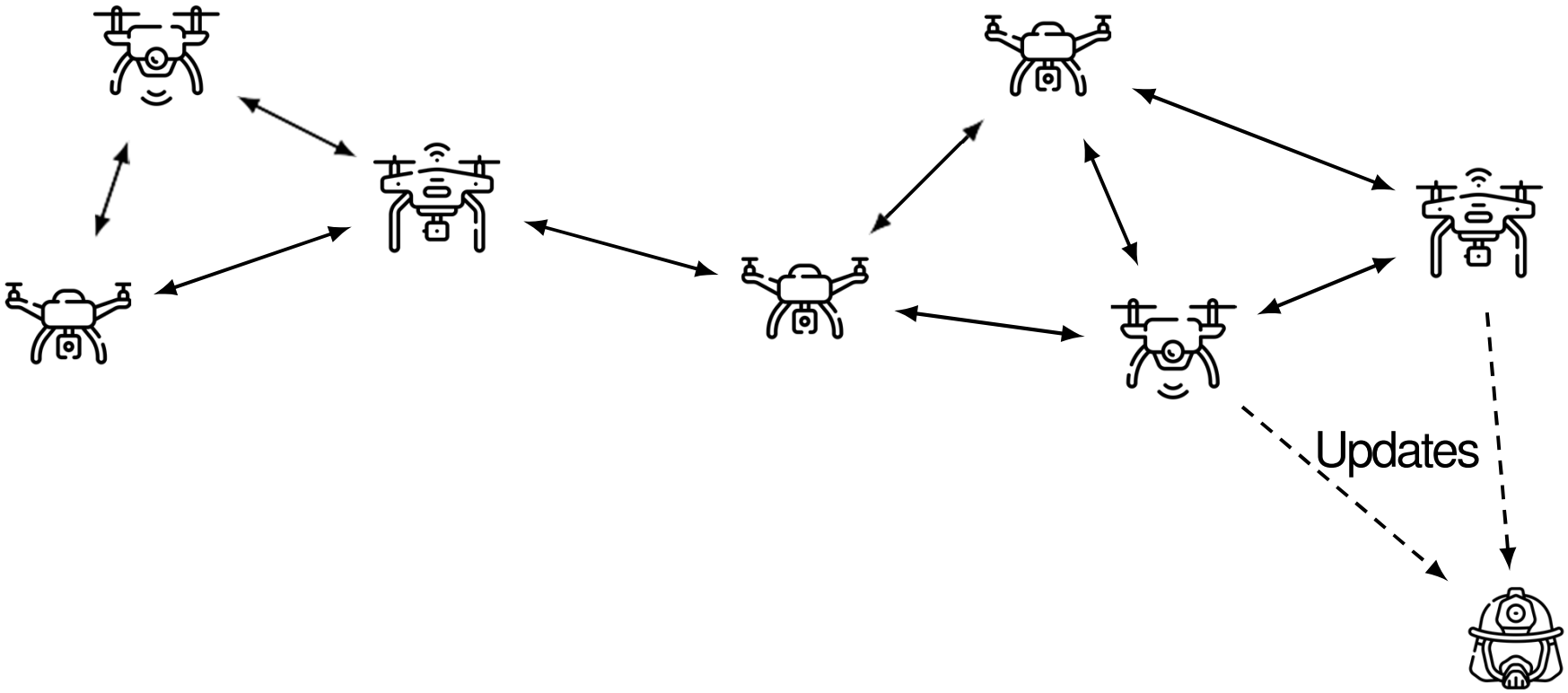
Embedded Agent

- Autonomous
- Resources & communication limitations
- Mobile

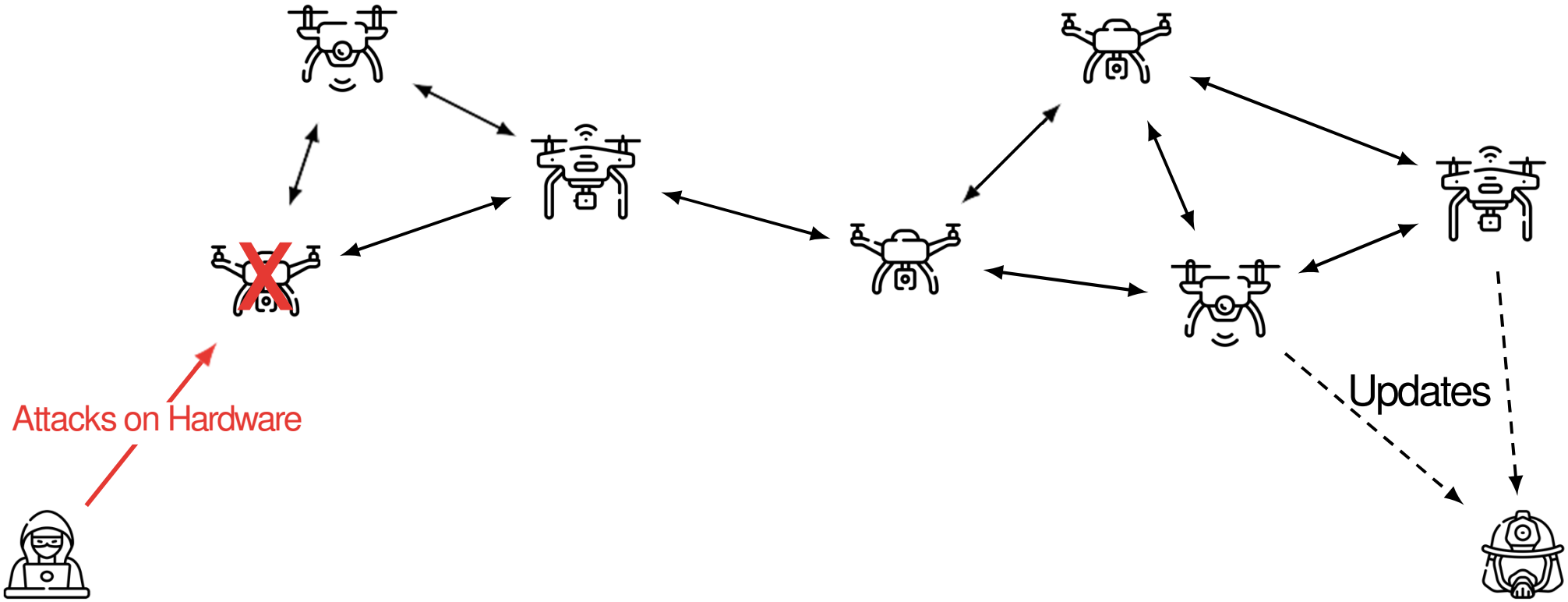
Multi-Agent System of Embedded Agents

- Global problem divided in smaller ones
- Cooperation between agents
- Decentralized
- Autonomous dynamic adaptation
- *Open*
- *Heterogeneous*

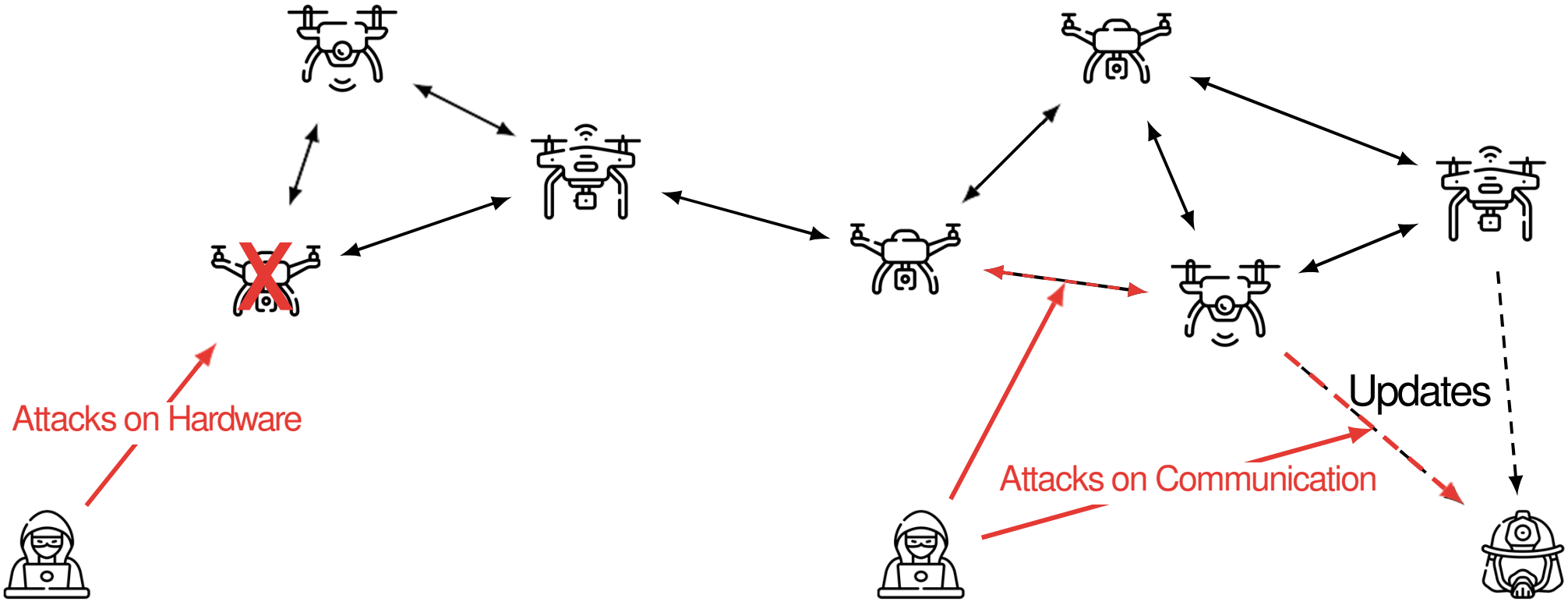
MEAS Are Vulnerable



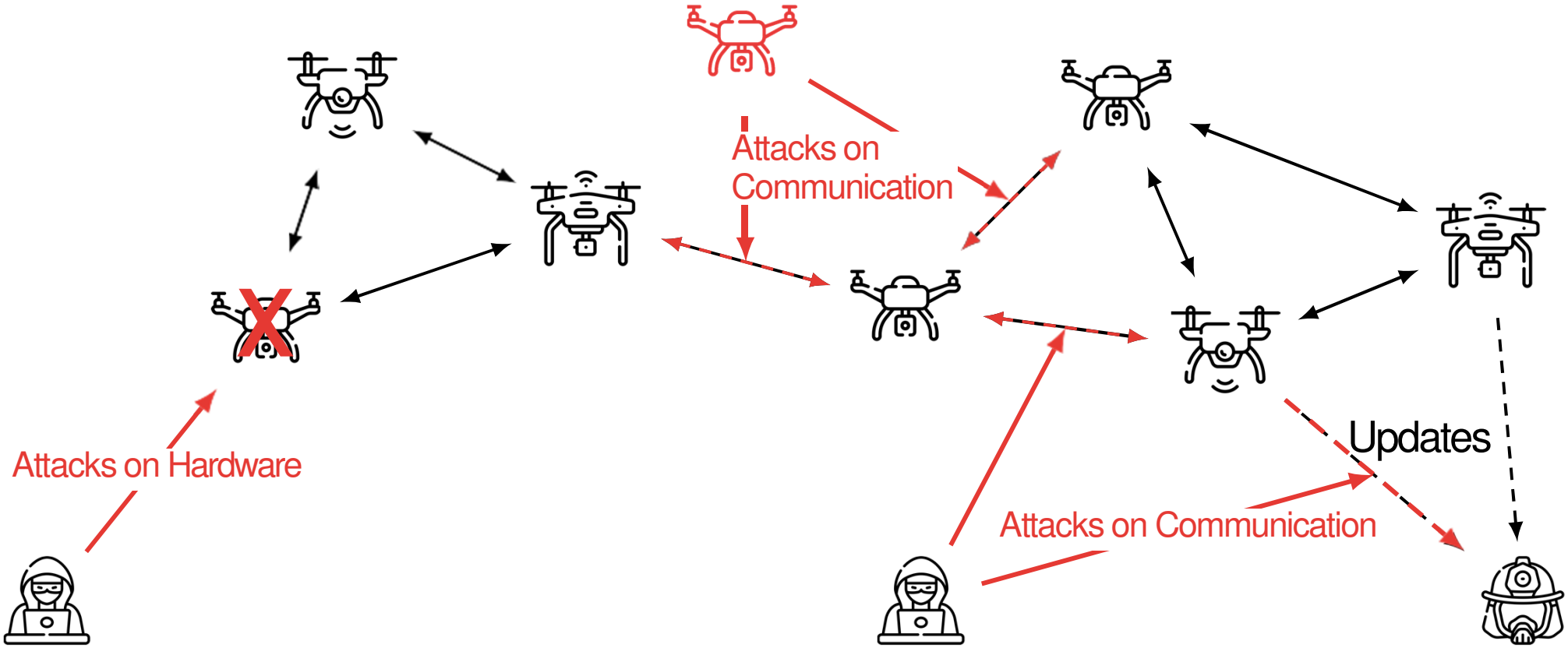
MEAS Are Vulnerable



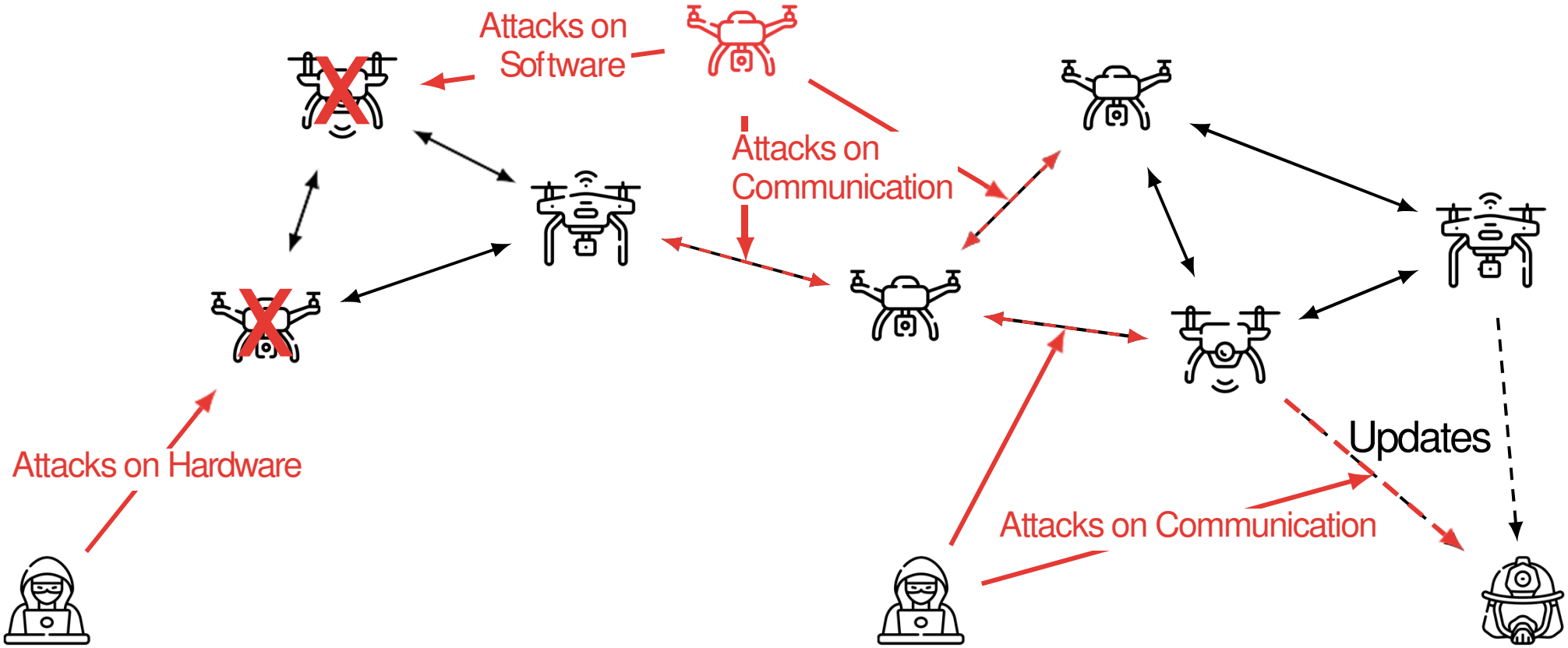
MEAS Are Vulnerable



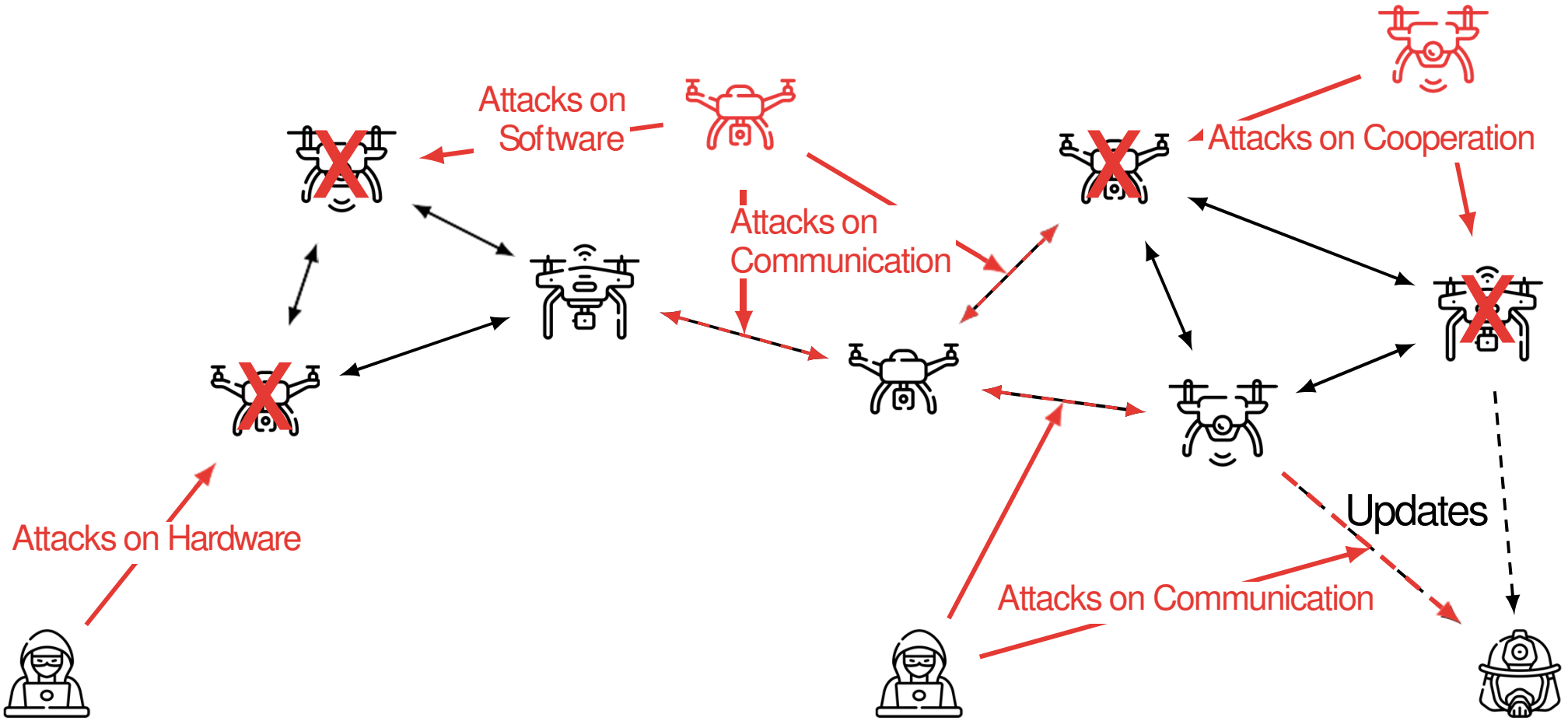
MEAS Are Vulnerable



MEAS Are Vulnerable



MEAS Are Vulnerable



So what do we do about it?

→ A Security Architecture

Security properties
(**nist_2020** [**nist_2020**])

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

How can we build it?

So what do we do about it?

→ A Security Architecture

Security properties
(**nist_2020** [**nist_2020**])

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

Explore the existing solutions

How can we build it?

Literature Review

Systematic Mapping Study

Quantitative systematic literature review: *what is done and how is it done?*
(**petersen_guidelines_2015**, **biolchini_systematic_2005**, **kitchenham_guidelines_2007** [**petersen_guidelines_2015**, **biolchini_systematic_2005**, **kitchenham_guidelines_2007**])

Research questions

RQ1 What are the main **security properties** studied in multi-embedded-agent systems?

RQ2 What are the specific **technical solutions** for securing multi-embedded-agent systems?

RQ3 Which **parts of a global security architecture** for multi-embedded-agent systems are studied?

---

baudet_systematic_2021.

Literature Review: Conclusion

RQ. 1 **Trust** and **Cryptography**

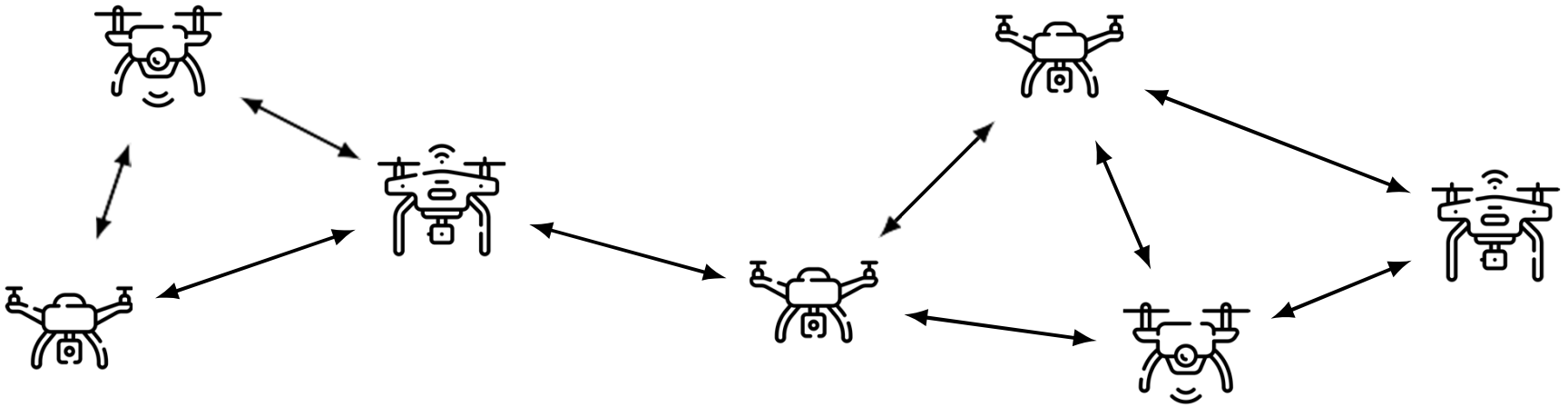
RQ. 2 **Availability** and **Secure Communications**

RQ. 3 *Most of works rely on* ***Cryptography***

$\Longrightarrow$ **No key management systems!!**

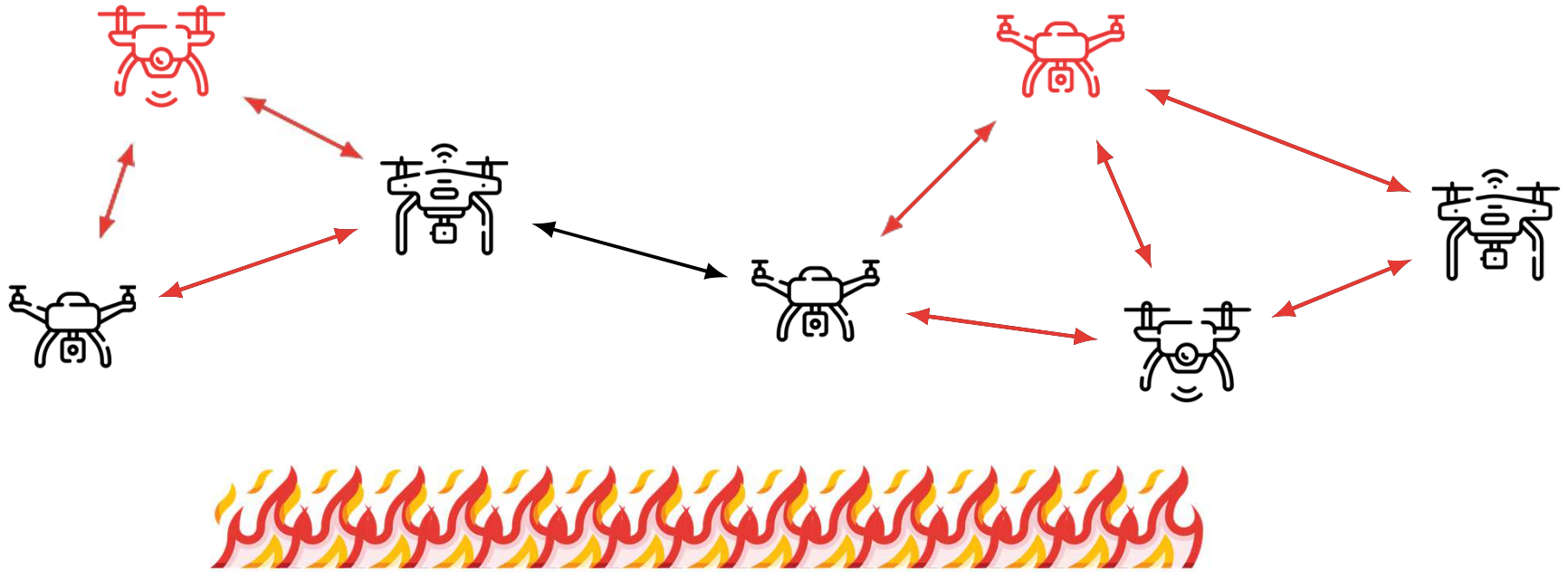
How to enable cryptography for autonomous and decentralized embedded systems?

Attack Model specification



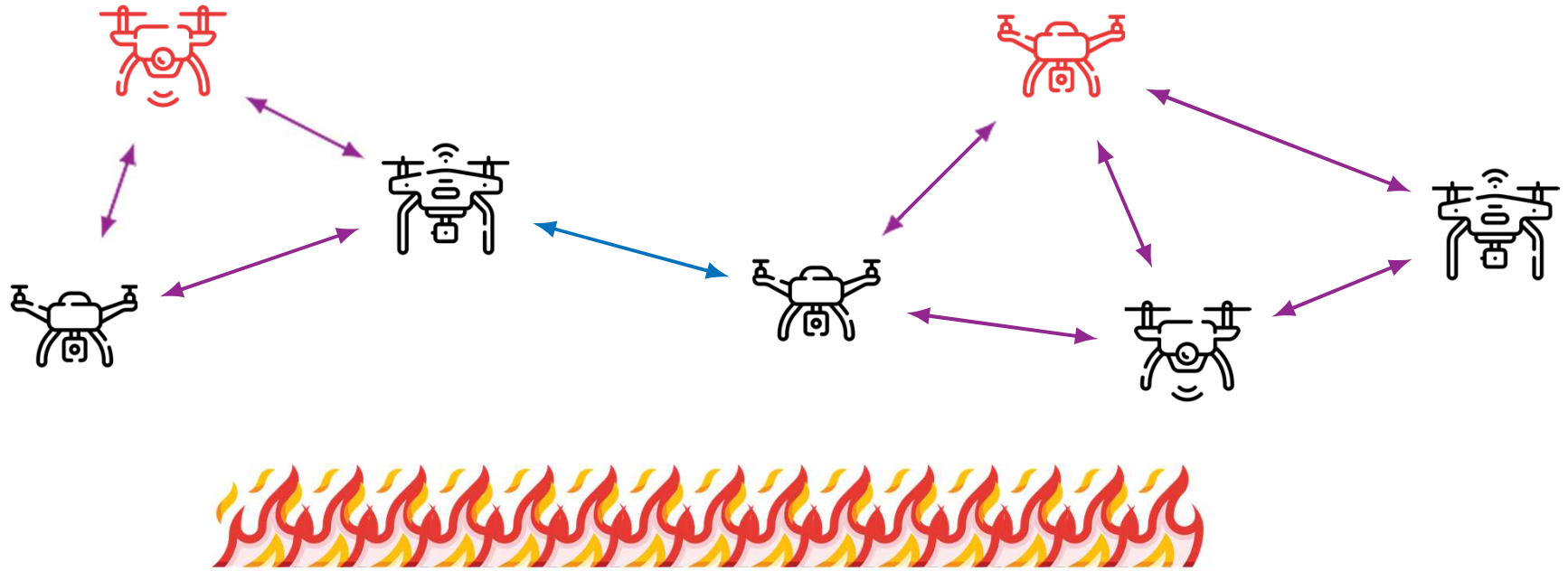
Attack Model

- Insider attackers
- Complete control over communication
- Unknown behavior



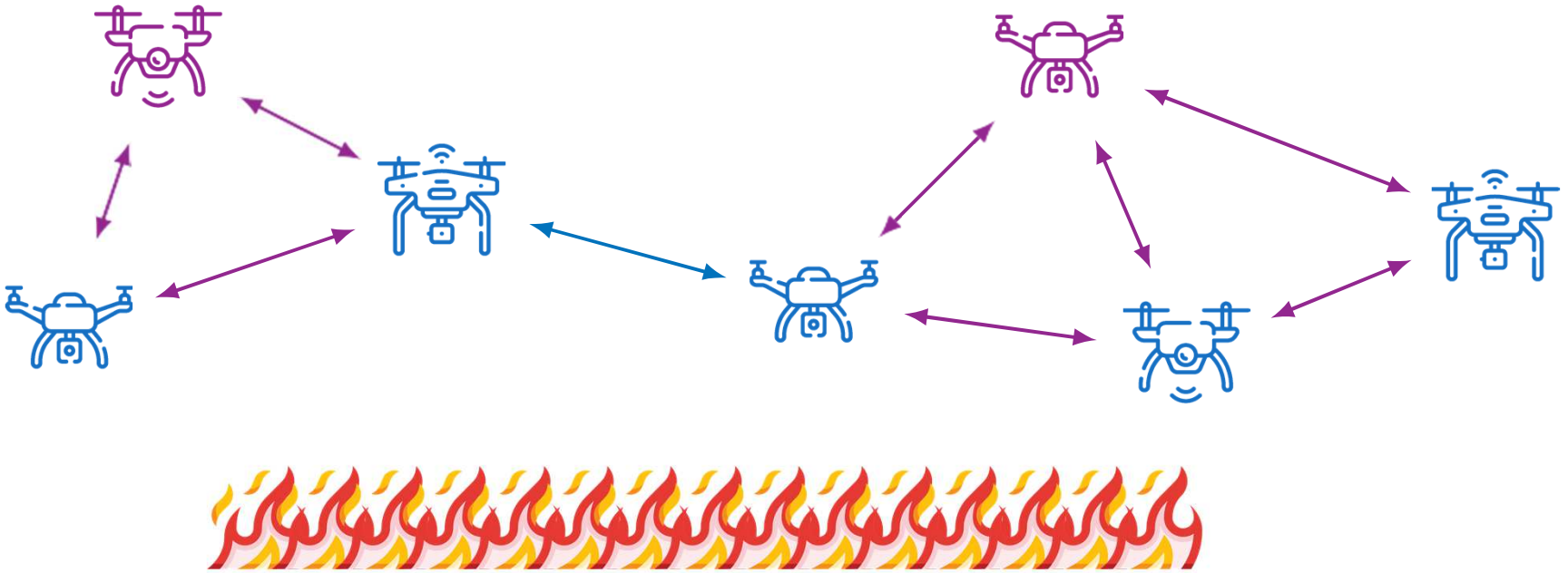
Security Concerns

- Communications Integrity
- Communications Authenticity



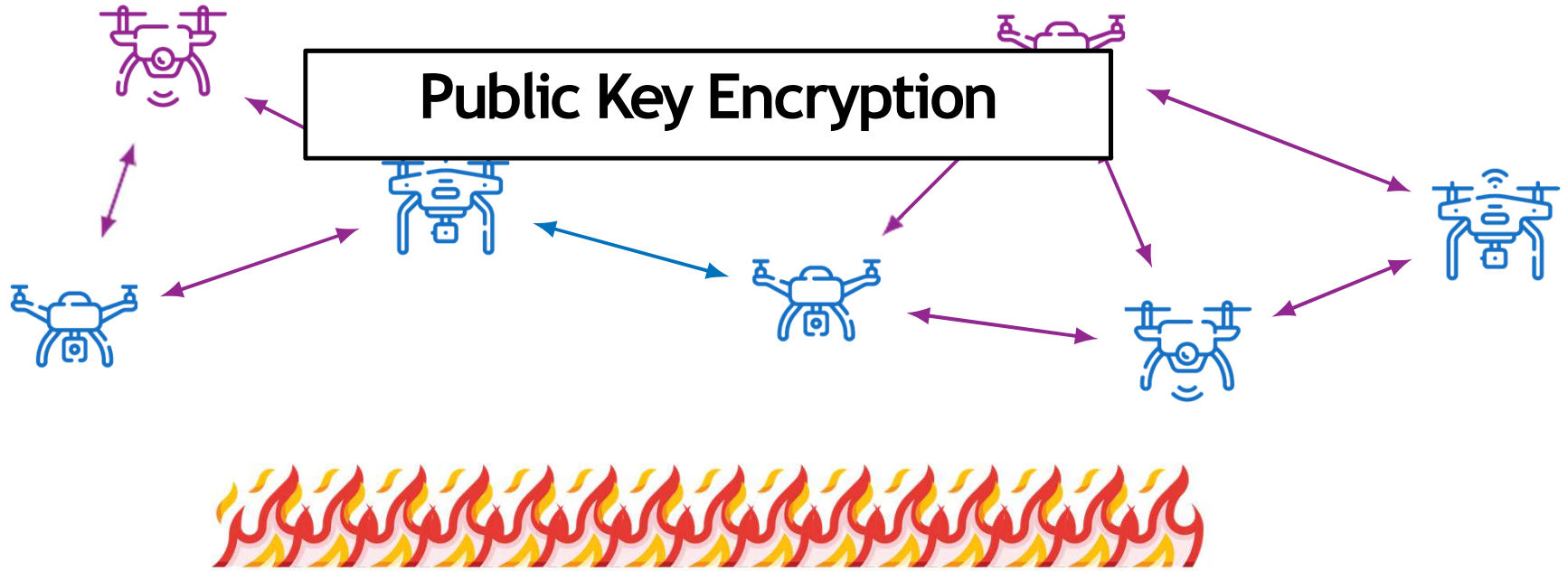
Security Concerns

- Communications Integrity
- Communications Authenticity
- Accountability



Security Concerns

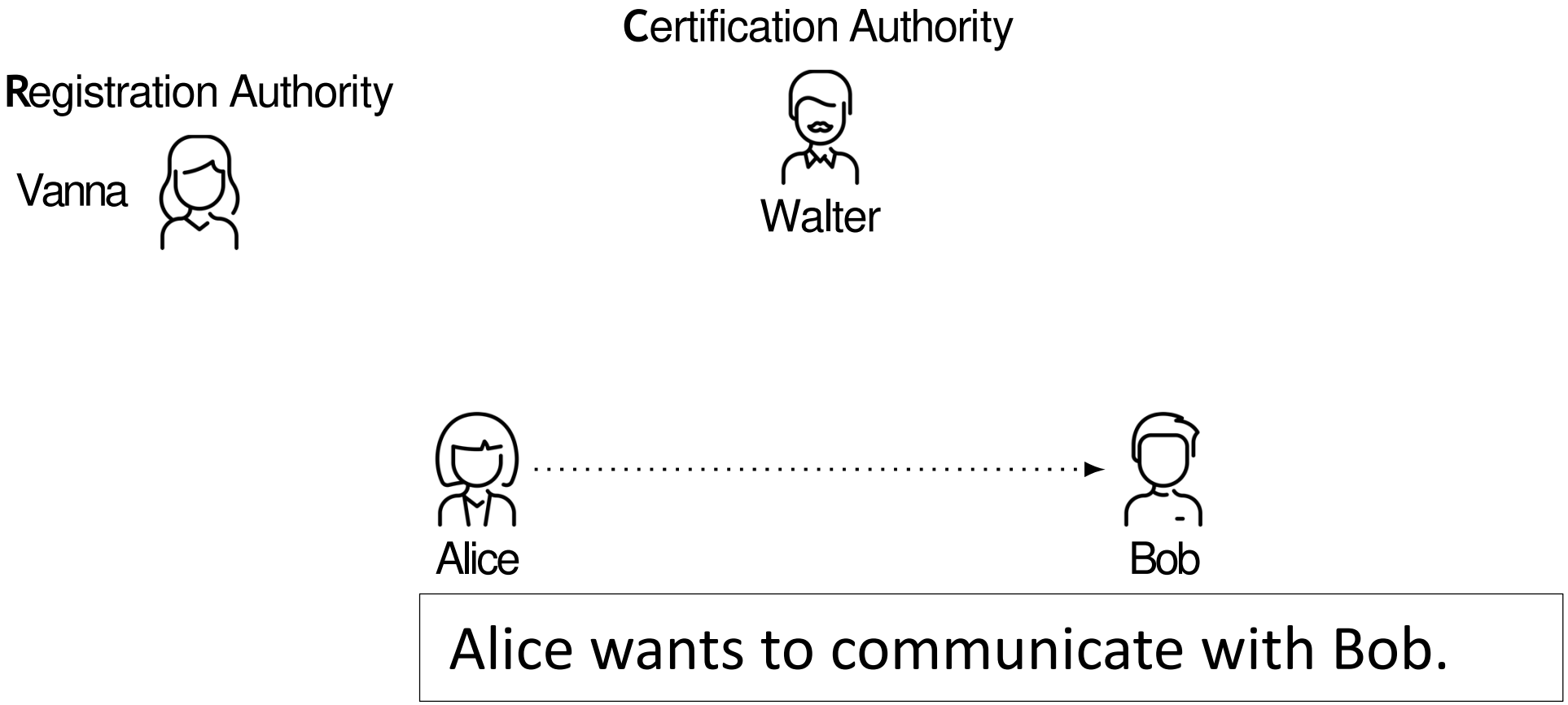
- Communications Integrity
- Communications Authenticity
- Accountability



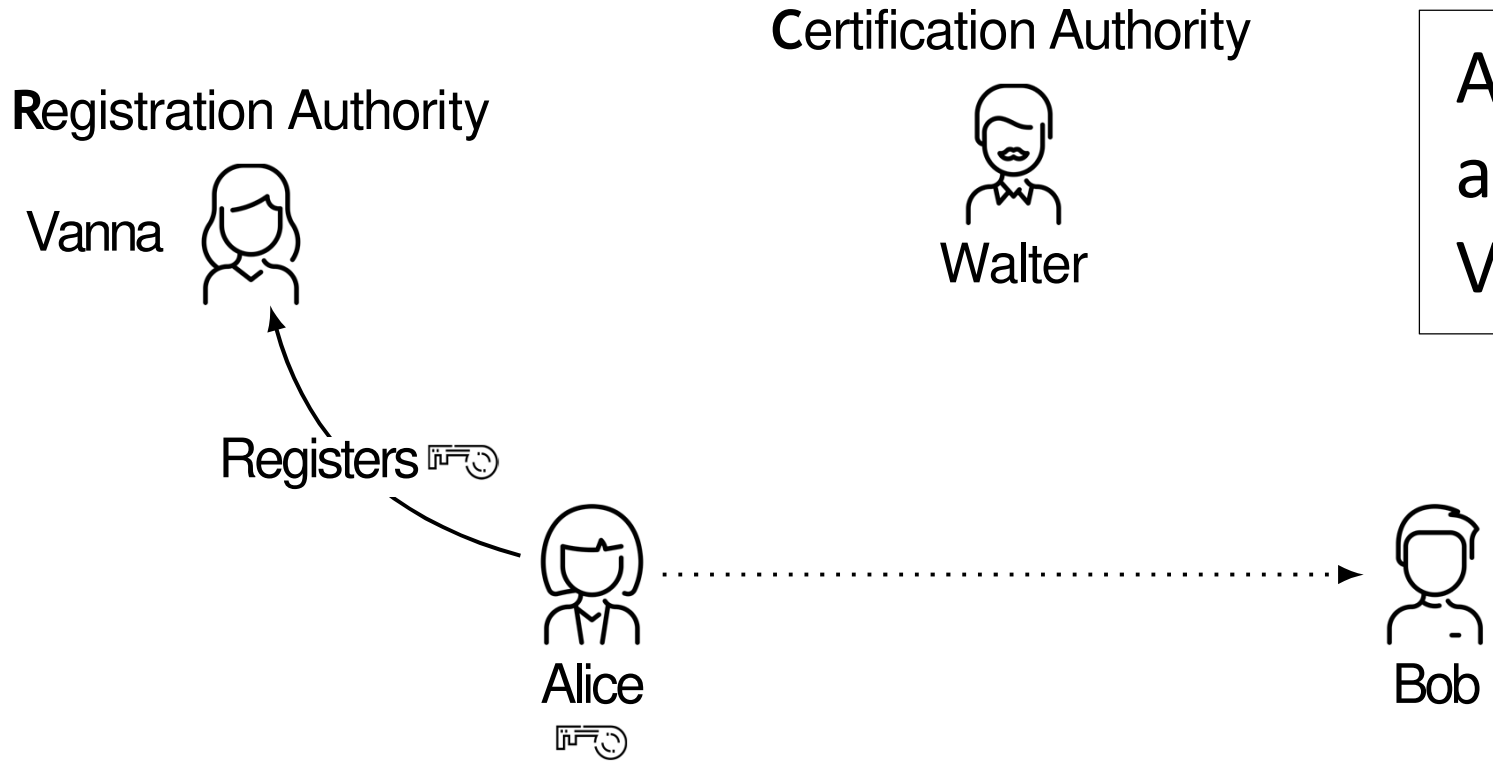
Public Key Infrastructure
Definition

“The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.” **nist_2020** [**nist_2020**].

Public Key Infrastructure
Certificate Delivery

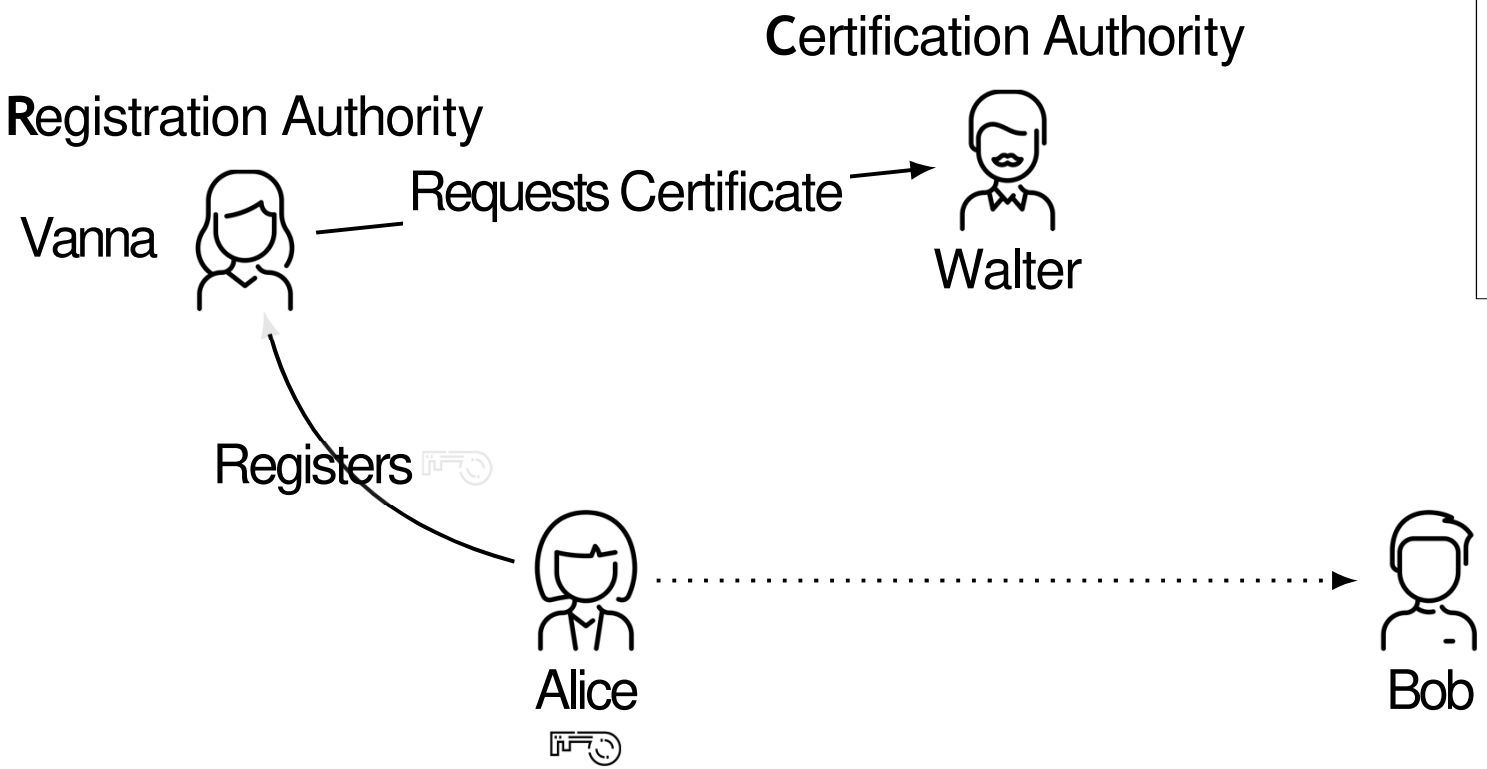


Public Key Infrastructure
Certificate Delivery



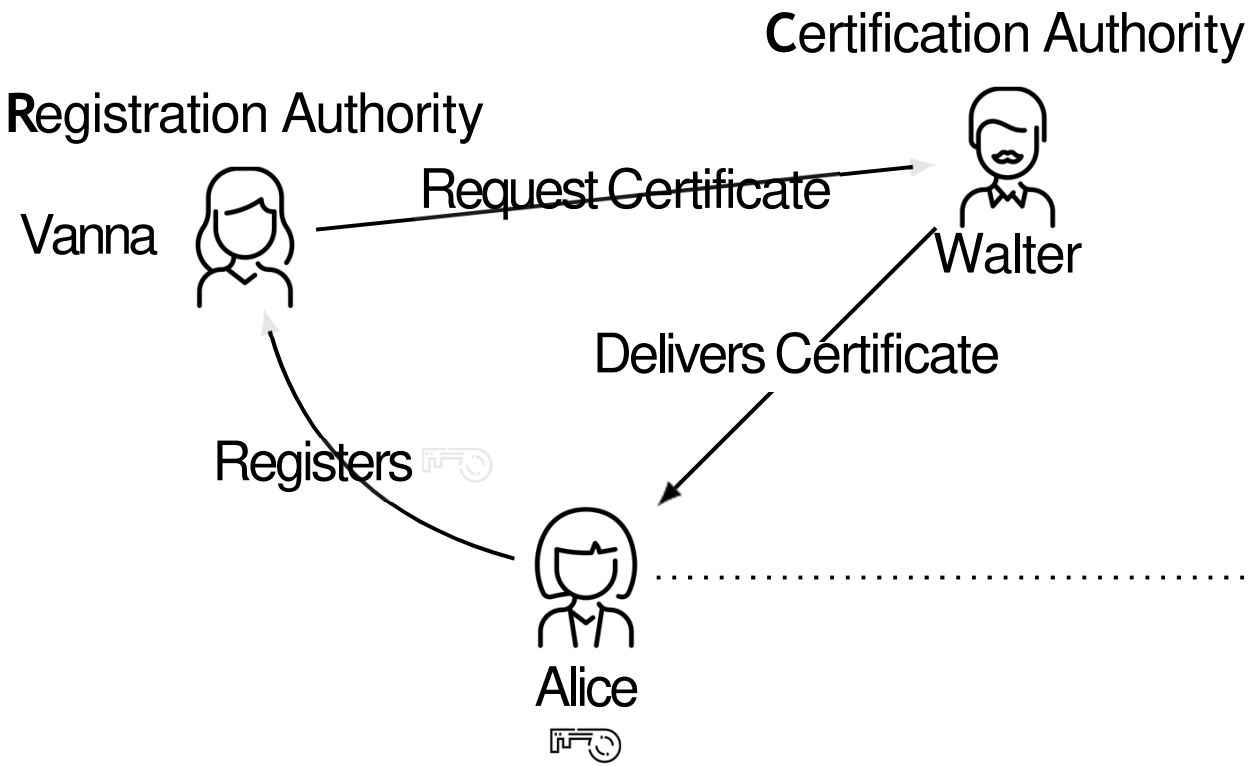
Alice registers with an authority Vanna.

Public Key Infrastructure
Certificate Delivery



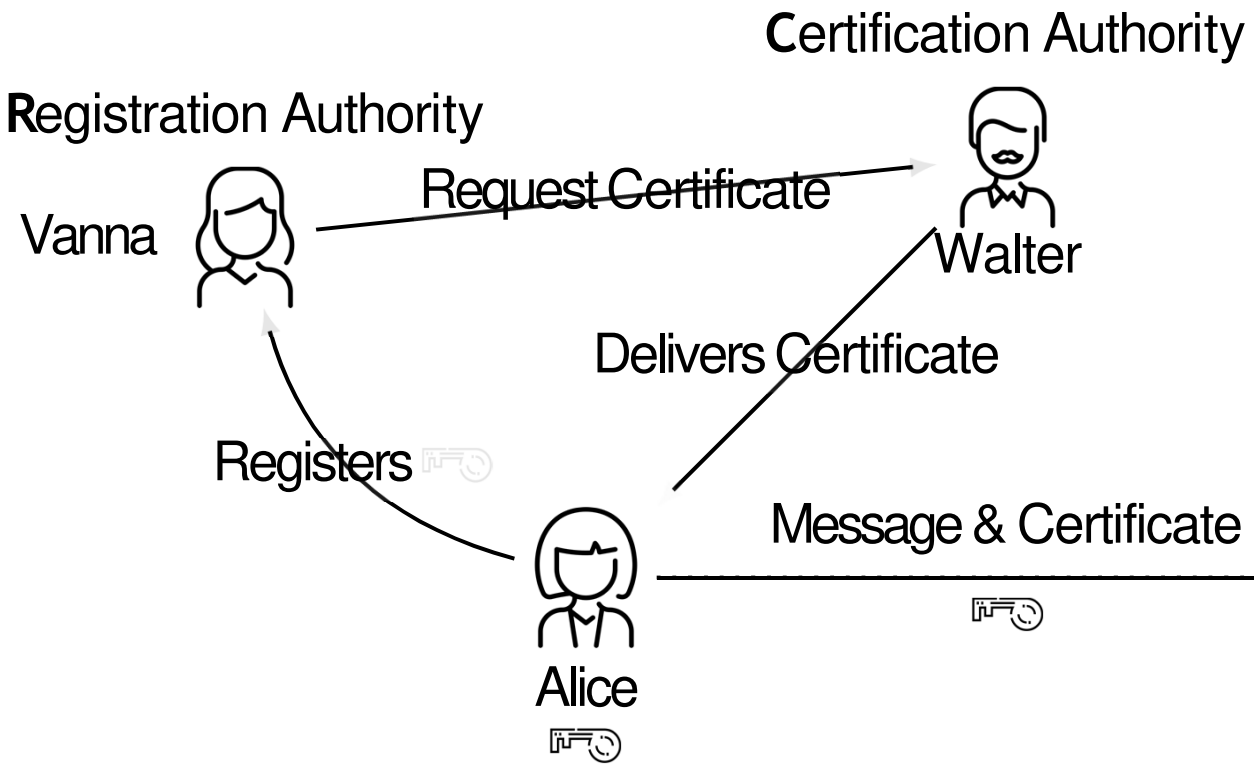
Vanna makes a certificat request to Walter

Public Key Infrastructure
Certificate Delivery



Walter then performs authentication and generates a certificate request for Alice.
This certificate acts like an ID card for Alice, confirming that the key indeed belongs to her.

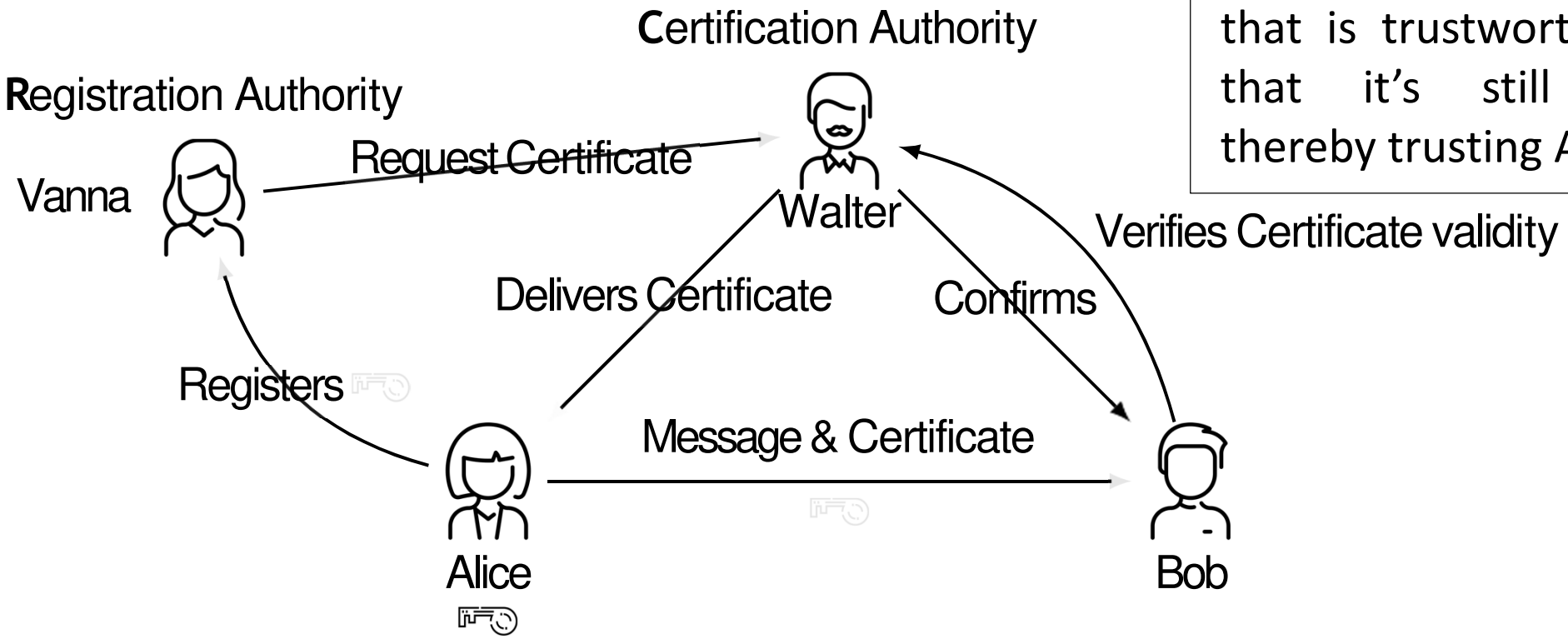
Public Key Infrastructure
Certificate Delivery



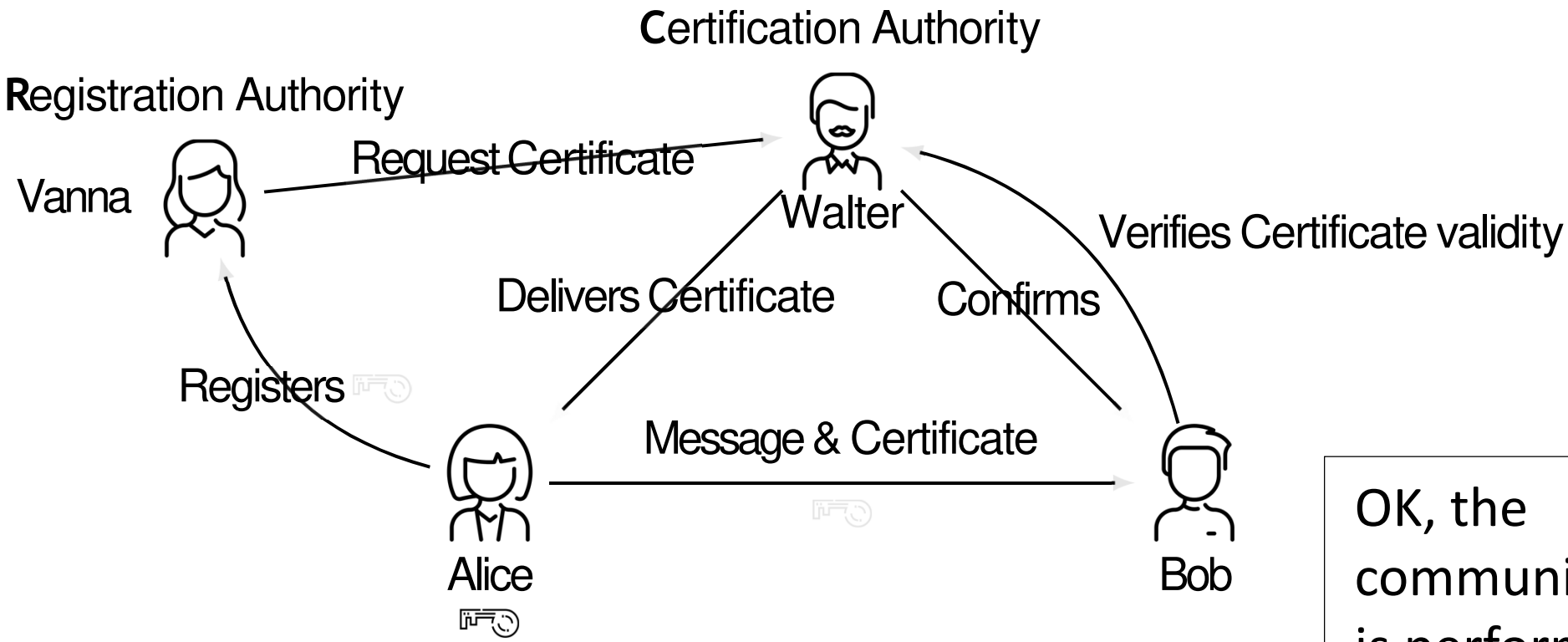
After Alice generates her key, she requests an ID that verifies it as hers. The authority then issues this certificate to Alice, which essentially becomes her identity. When Alice sends a message, she includes the certificate, which Bob can then request to validate.

Public Key Infrastructure
Certificate Delivery

At this point, Bob can verify to the entity that issued the certificate that is trustworthy and that it's still valid, thereby trusting Alice.



Public Key Infrastructure
Certificate Delivery



OK, the communication is performed.

Public Key Infrastructure
Certificate Revocation

Certification Authority

Walter

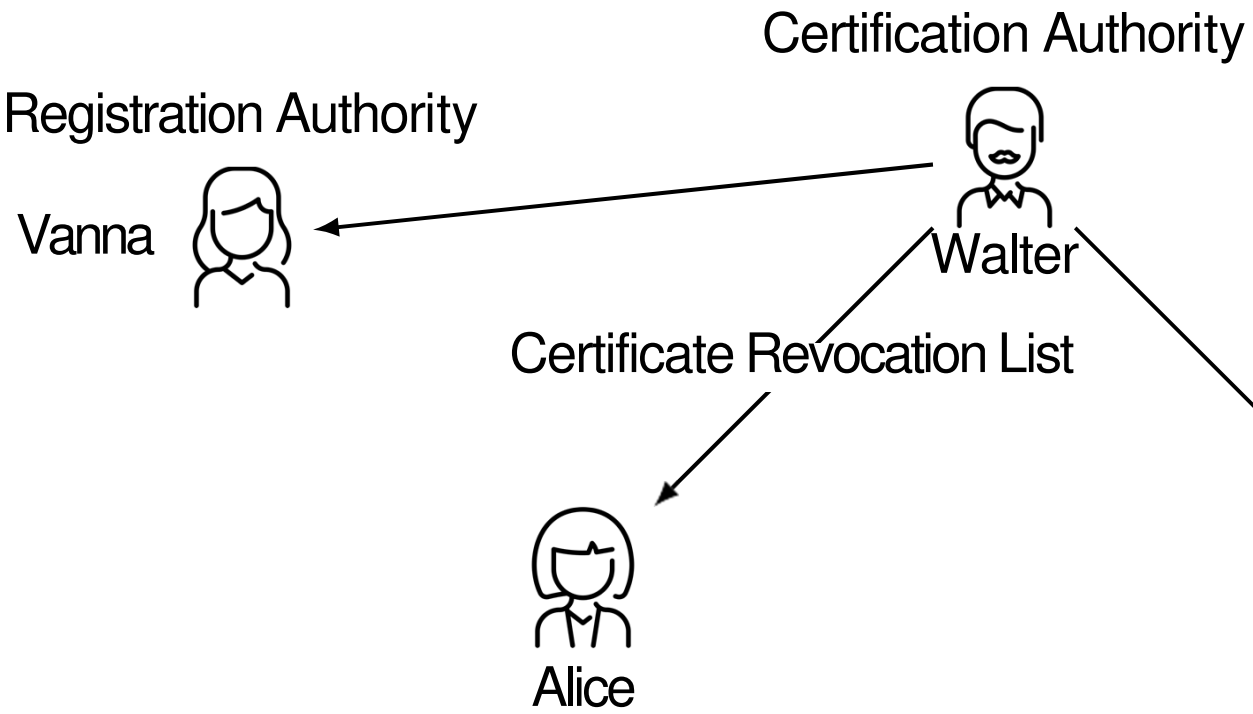
Registration Authority

Vanna 

Alice

Bob

Public Key Infrastructure
Certificate Revocation



Since the certificate itself is digital, the authority cannot physically retrieve it from Alice. Instead, it maintains a list of revoked certificates and simply adds any revoked ones to that list.

Public Key Infrastructure for Autonomous Decentralized Systems

	Low computation cost	Low memory cost	Autonomy
PKI X.509 (Telecommunication Standardization Sector of ITU [6])	✓	✓	✗
Custom PKI (Avramidis et al., Blanch-Torné et al., Dumas et al. [7–9])	✓	✓	✗
Alternative PKI (Okamoto et al., Cui et al. [10, 11])	✓	✓	✗
Blockchain based PKI (Singla et al., Yakubov et al., Qin et al. [12–14])	✗	✗	✓

Multi-Agent Key Infrastructure (MAKI)

{ Public Key Infrastructure for Multi-Agent System }

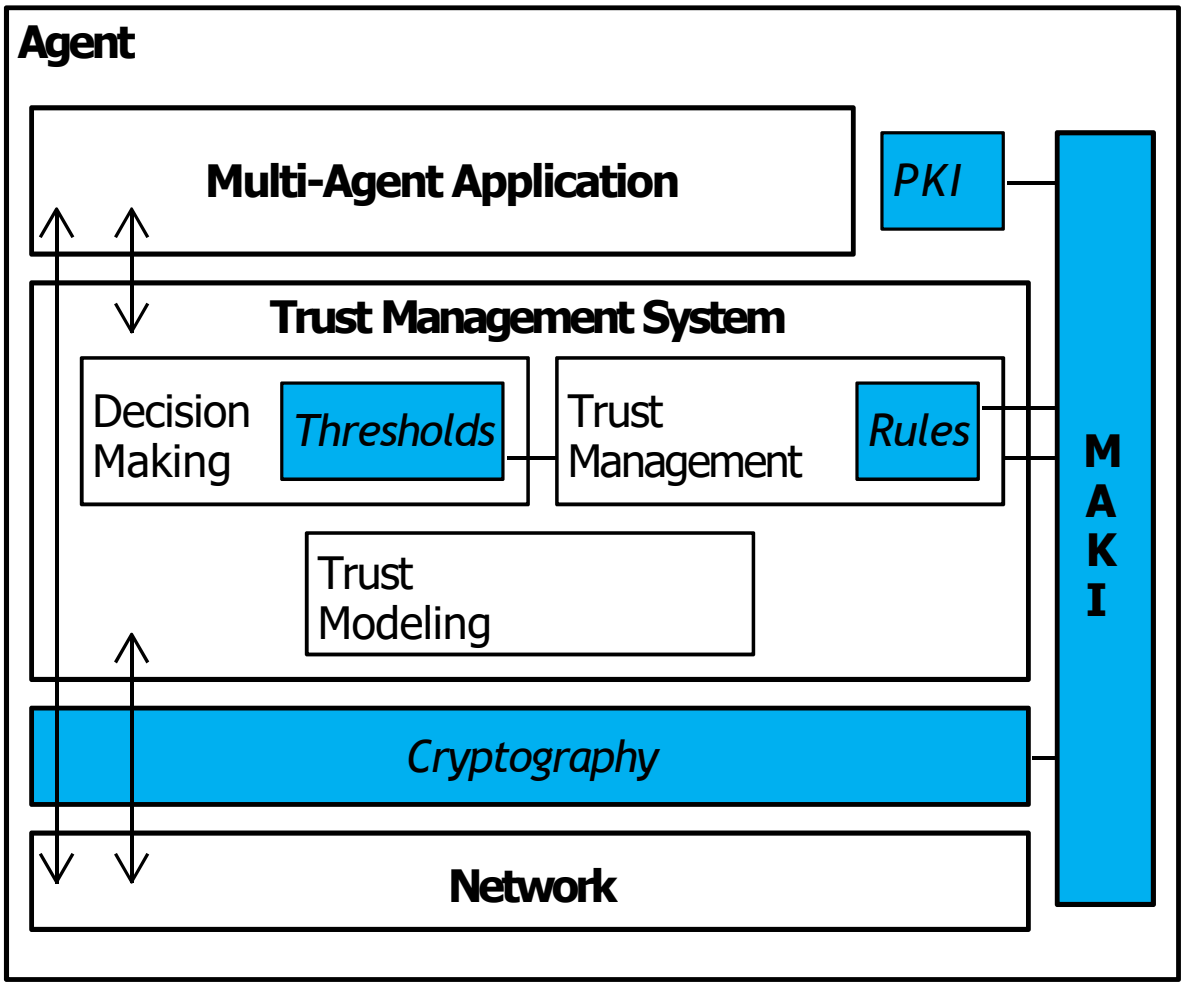
Hypotheses

Standard cryptography is secured
Basic routing exists
An adequate Trust Management System is running

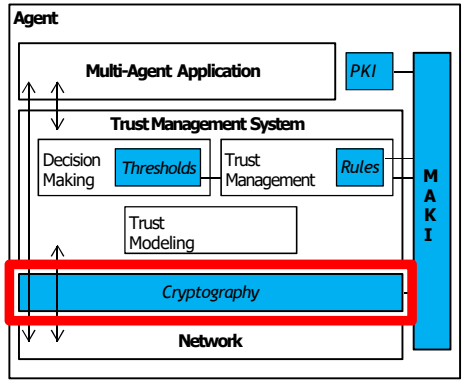
Main Rules

Messages must be signed
One key for one identity
Key must be linked to a valid certificate

Agent Architecture



Cryptography



We only need signature

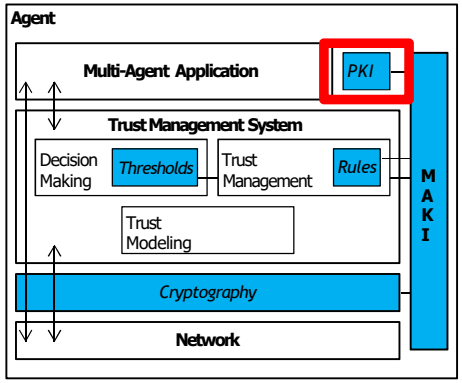
Unsigned or invalidly signed messages should be ignored

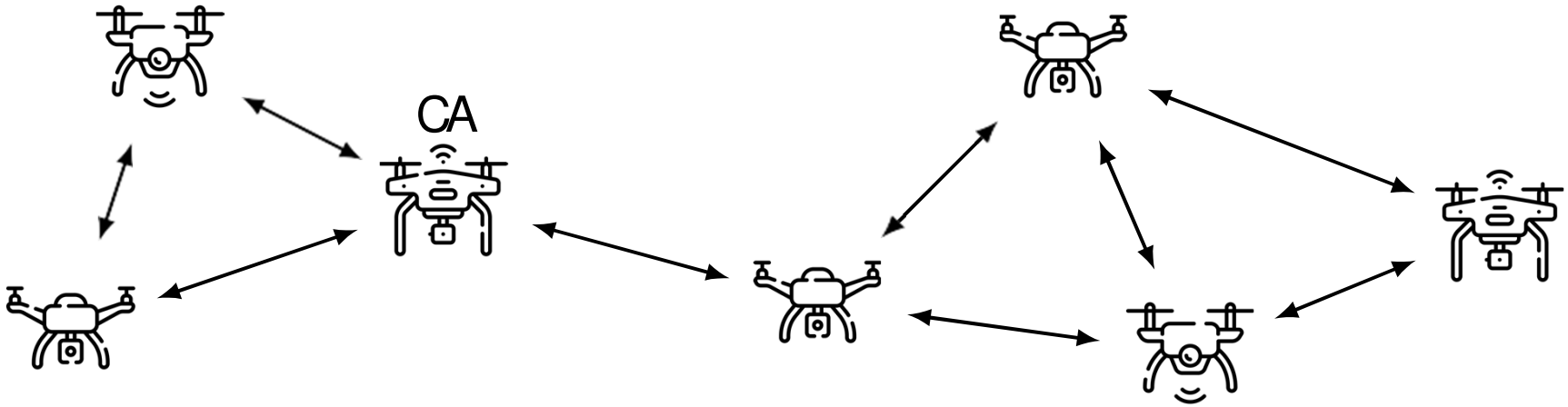
Following NIST's recommendations (**mckay_report_2017** [**mckay_report_2017**])

- Elliptic-Curve Cryptography
- Elliptic Curve Digital Signature Algorithm
- 256-bits key
- NIST P-256 (SECP256R1) Curve

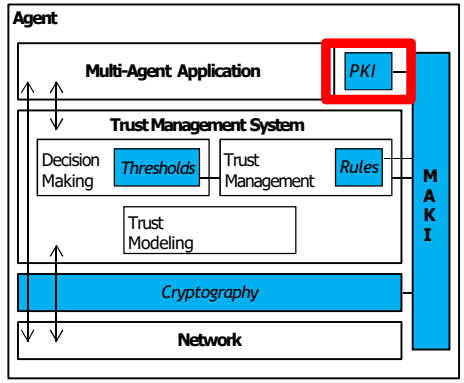
PKI: Certificate Management

- CAs deliver certificates

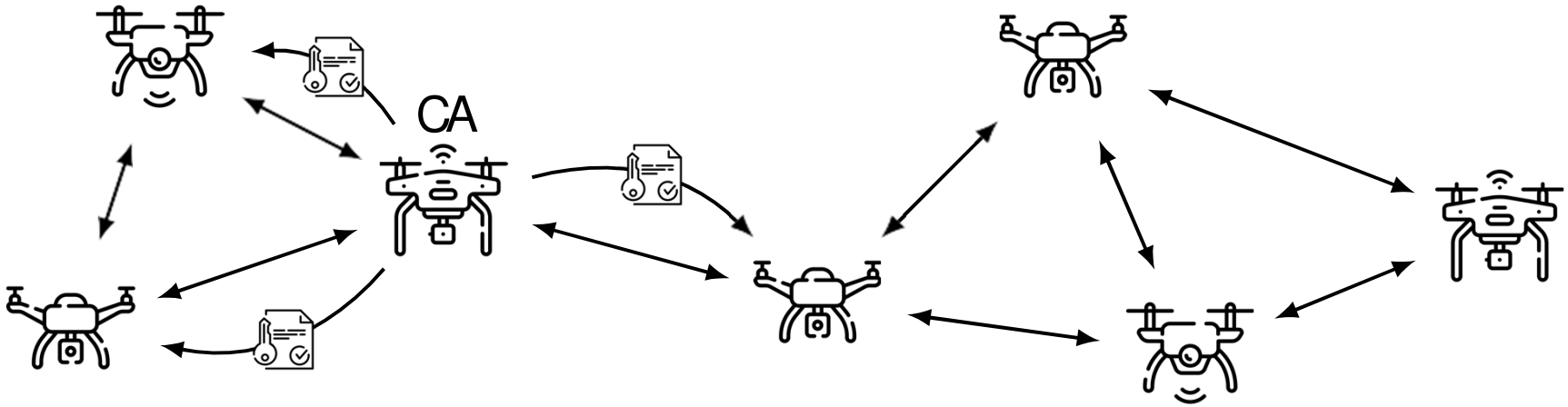




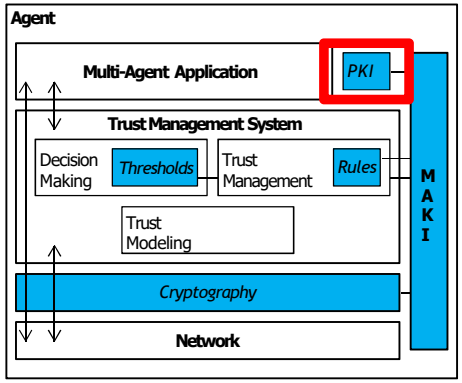
PKI: Certificate Management



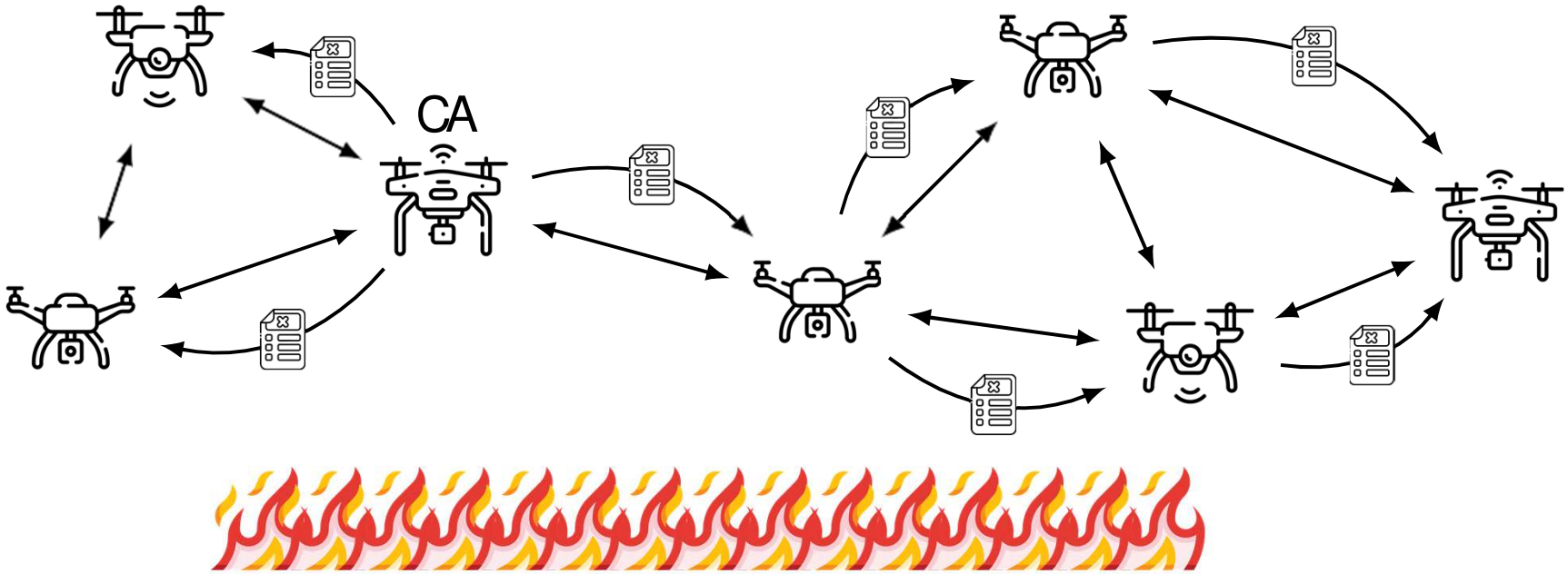
- CAs deliver certificates



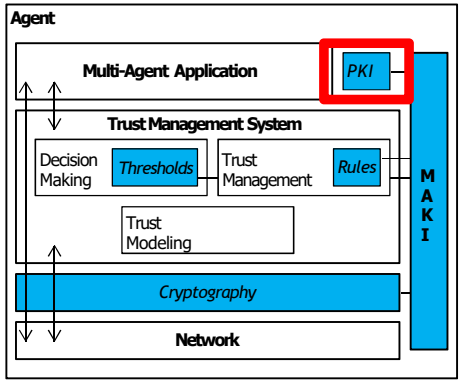
PKI: Certificate Management



- CAs deliver certificates
- CAs revoke certificates
- Revocation using Certificate Revocation List (CRL) & short-lived certificates



PKI: Organization



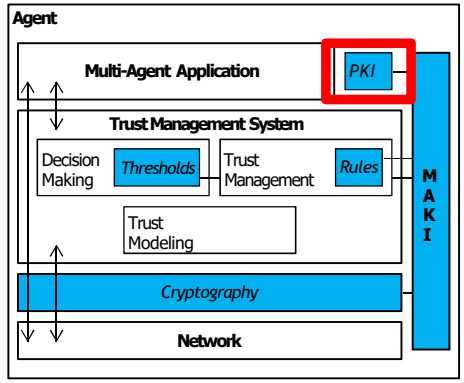
Certification Authority - CA

- Delivers and stores certificates
- Revokes certificates
- Shares its certificate

None

- Default Role
- Needs a CA to get a certificate
- Shares its certificate

PKI: Self-Organization

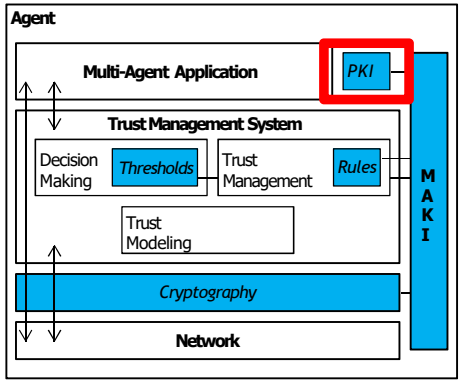


Coalition-based Multi-Agent System
(picard:emse-00675577 [picard:emse-00675577])

- Agents make choices for themselves
- Agents are aware of parts of the organization

→ Agents adapt the organization to the changes (self- and re-organization) w.r.t. their knowledge

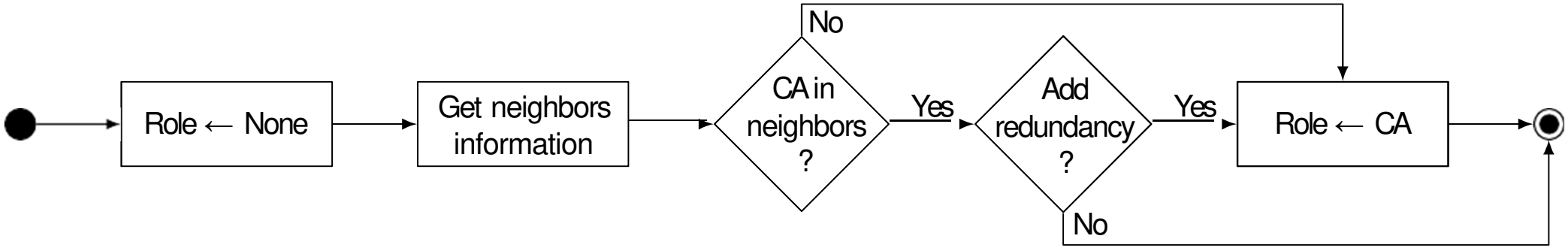
PKI: Self-Organization



Rules

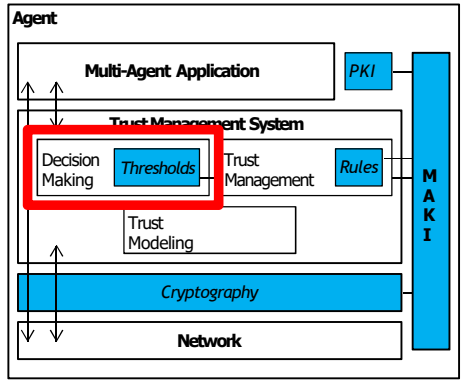
- Agents choose their roles
- Any agent can become a CA

- At least one CA is required
- > 1 CA is advisable to prevent single-point-of-failure



Role self-assignment flowchart

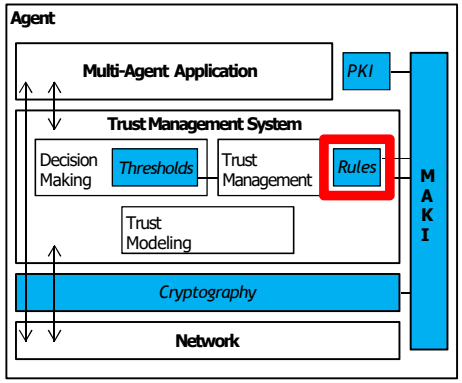
TMS: Decision Making



Thresholds: ▪ Low ▪ Moderate ▪ High

	Decision	Required Trust
Certification Authority	Delivering a certificate to a None	Moderate or None
	Revoking a certificate	Moderate
	Requesting a certificate	High
	Delivering a certificate to a CA	High
None	Requesting a certificate	Moderate or None

TMS: Trust Management



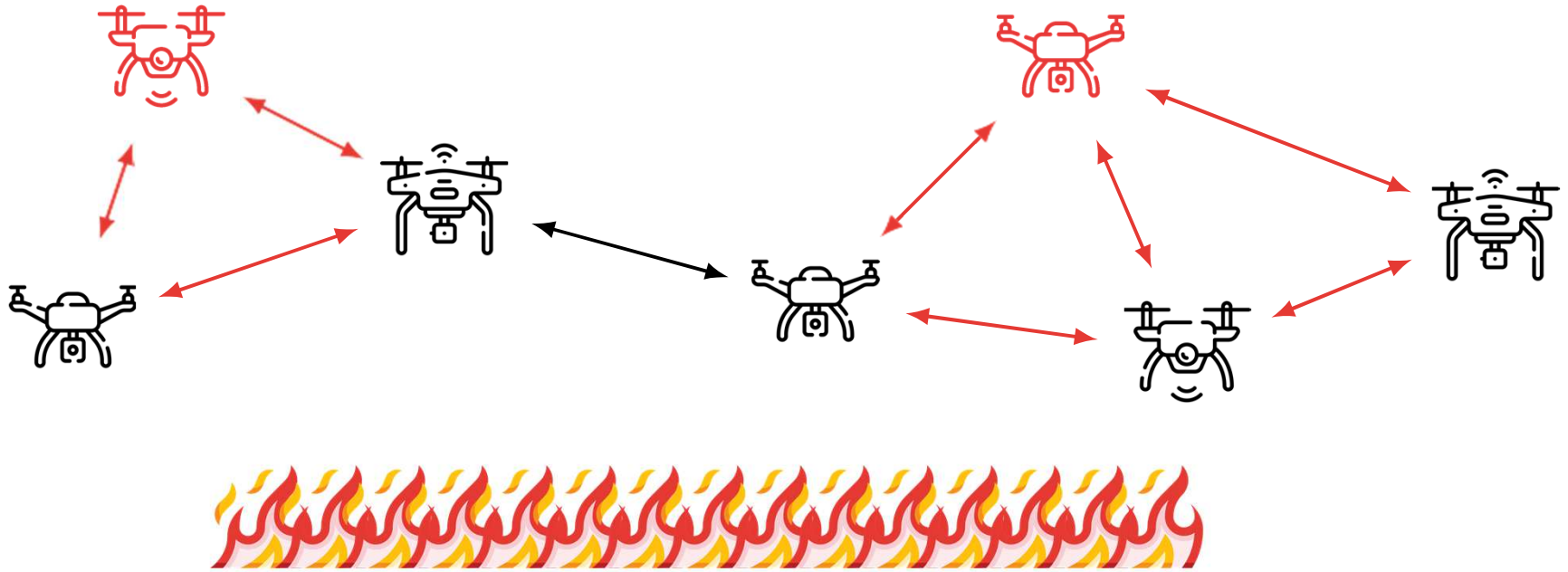
Delivering certificate increases trust

Ignoring requests decreases trust

Inter-CA certification increases trust

Wildfire Monitoring

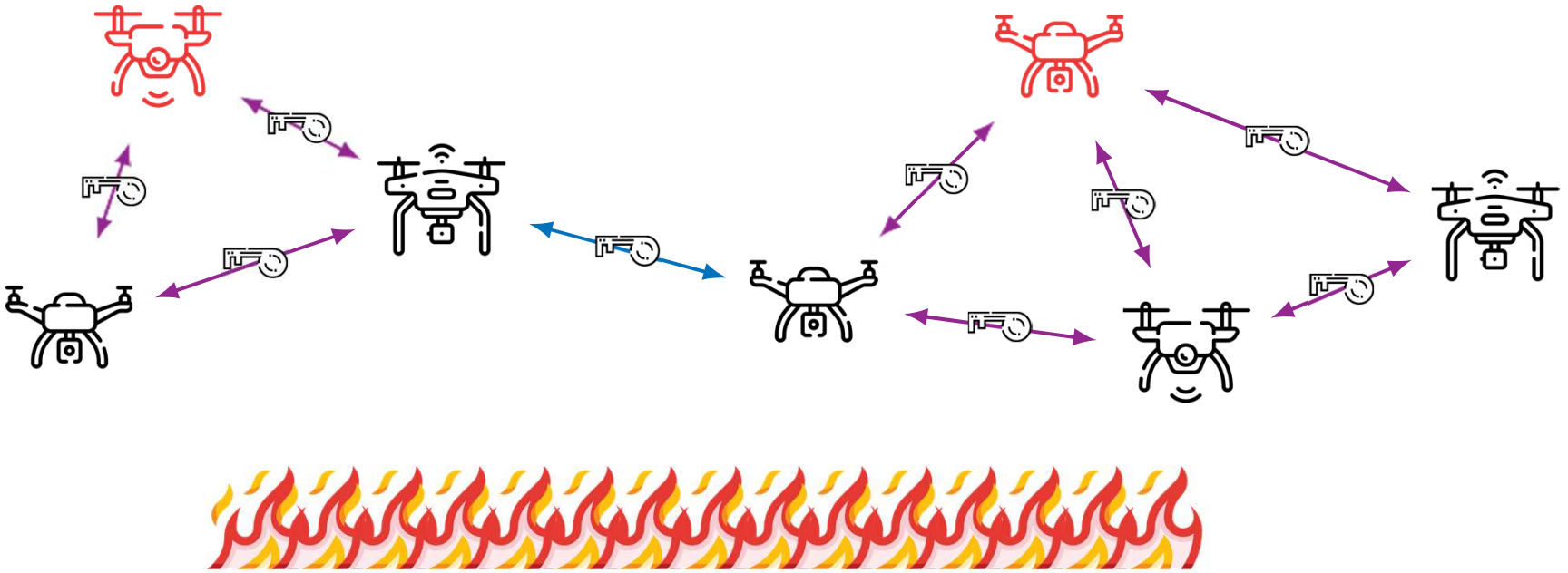
This system enables secure communications through digital signatures,



Wildfire Monitoring

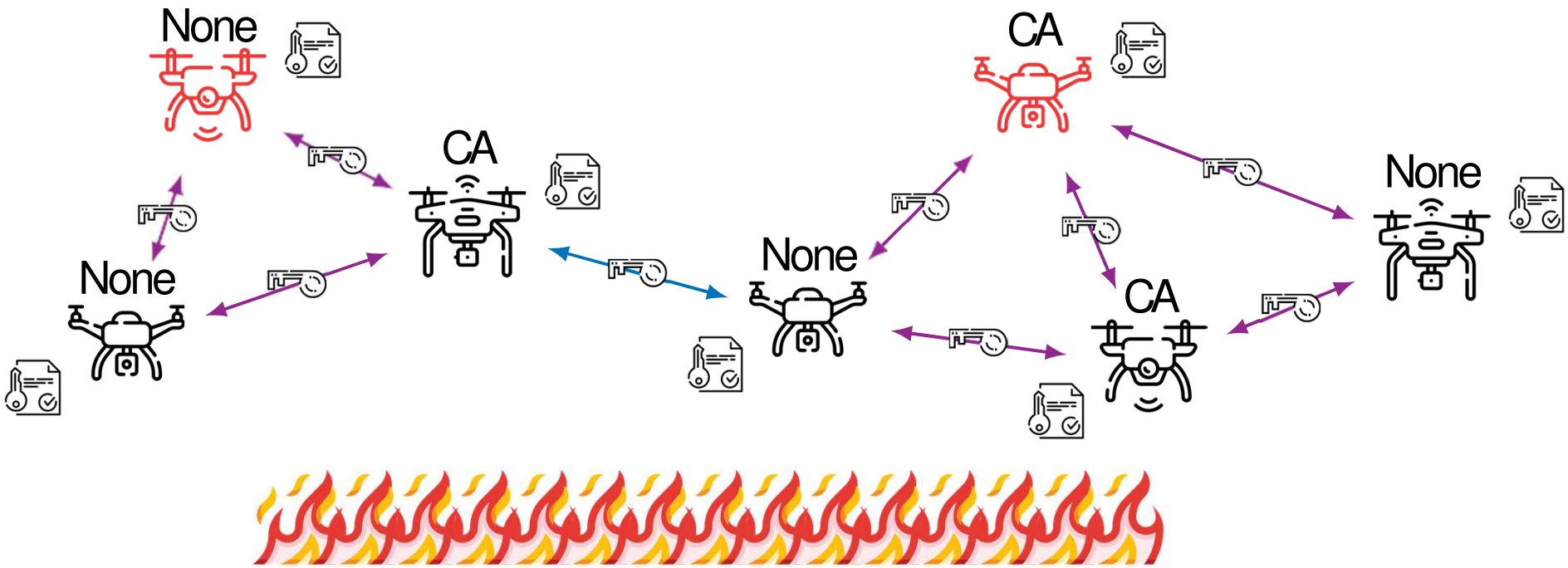
- Integrity and Authenticity using signatures

  as well as certificate-based revocation mechanisms.



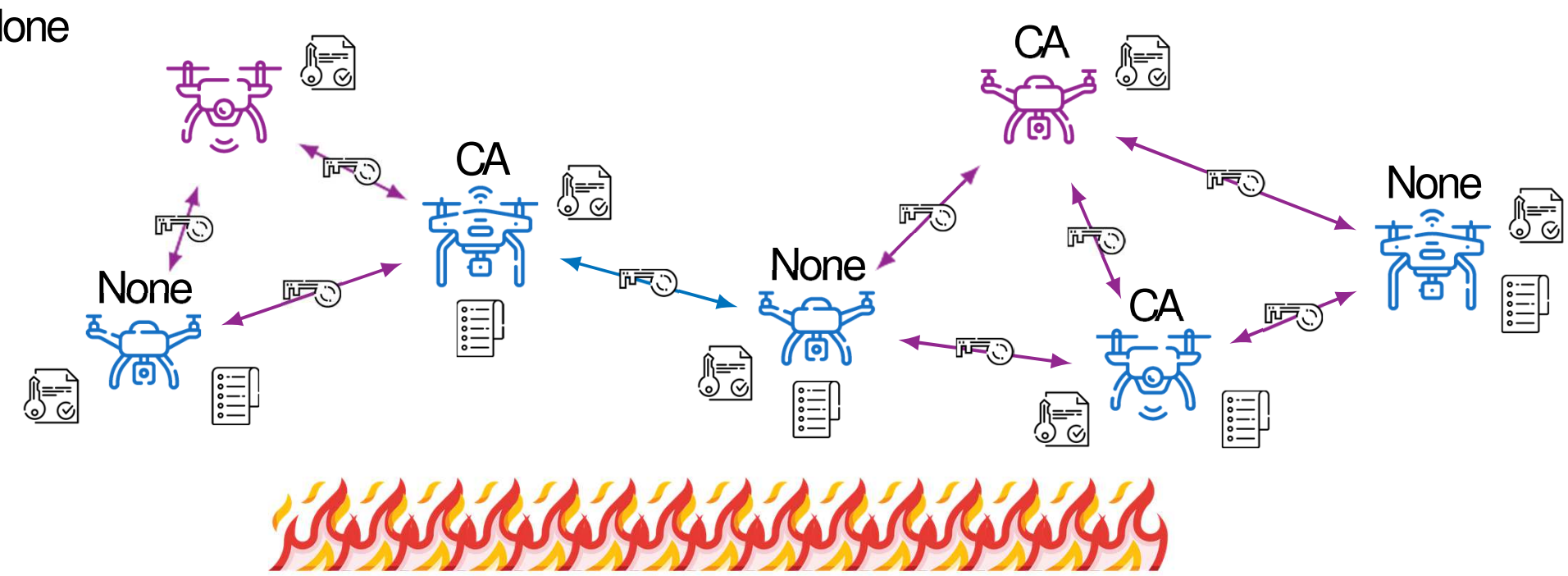
Wildfire Monitoring

- Integrity and Authenticity using signatures
- Access control using certificates



Wildfire Monitoring

- Integrity and Authenticity using signatures
- Accountability using Signature
- Access control using certificates



Conclusion

Multi-Agent Systems of Embedded Agents are vulnerable

So Security Architecture

But Impossible to deploy cryptography

So Multi-Agent Key Infrastructure

And It works!

What now?

- Enhance information sharing *(work in progress)*
- Allow agents to adapt their security level *(UGA/IRGA project)*
- Explore threshold cryptography, attribute-based cryptography

Thank you for you attention

For more information

https://www.youtube.com/watch?v=EnEpnUUoMDE

https://theses.hal.science/tel-04672641