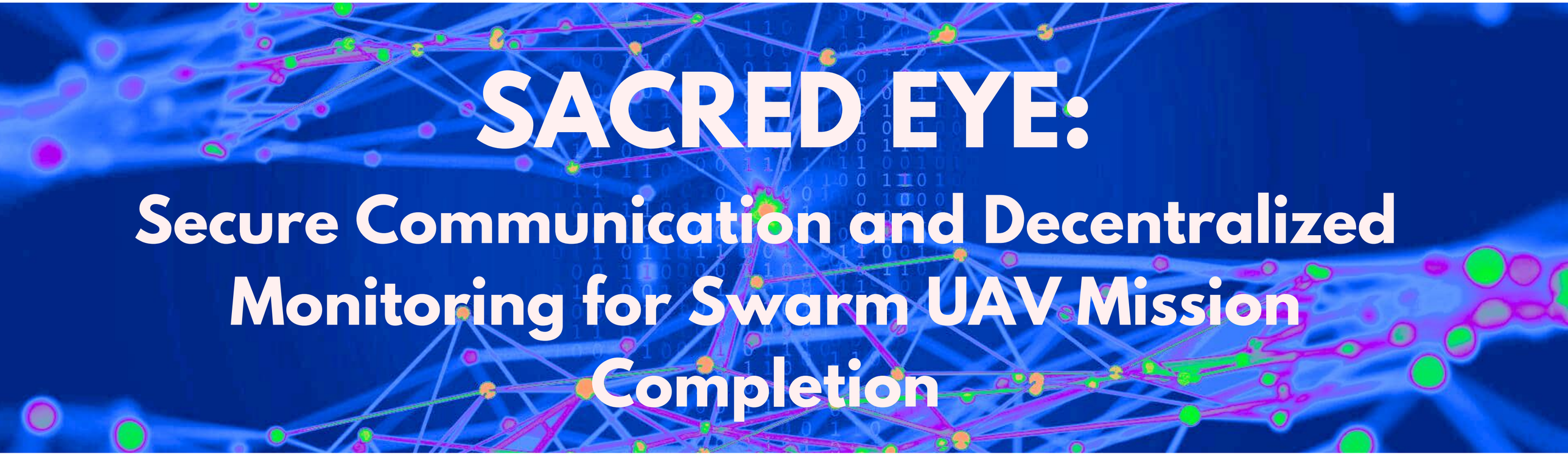


SACRED EYE:

Secure Communication and Decentralized Monitoring for Swarm UAV Mission Completion

Hugo Le Dirach
University of Toulouse
Toulouse, Occitanie, France

Amin Rezaei
California State University Long Beach
Long Beach, California, USA

Motivation

UAV Pros and Cons

+	−
Felxibility	**Felxibility**
Scalibility	**Scalibility**
Robustness	**Robustness**

Current Approches

- Rely on heavy cryptographic hardware such as PUFs
- swarms frequently operate in unpredictable environments where temperature, pressure, or humidity fluctuations can disrupt hardware-based authentication

Related Work Overview

Software-Based Approaches:

- Traditional methods (PKI, ECC, hash-based authentication, blockchain) provide strong security but demand high computational resources that exceed lightweight drone capabilities
- Emerging technologies like mobile edge computing and machine learning enable real-time threat detection but introduce significant energy consumption and latency issues

Hardware-Based Approaches:

- Physical security methods (TPMs, HSMs, PUFs) offer identity verification through unique device characteristics
- These solutions increase manufacturing costs, add physical weight to drones, and suffer from instability in harsh operational environments

Key Limitations of Existing Systems

- Centralized architectures create bottlenecks and single points of failure
- Resource constraints of lightweight UAVs incompatible with computationally intensive solutions
- Environmental vulnerabilities affect hardware reliability during missions

Our contribution

First Line of Defense

Standart symmetric encryption where we assume that the private ID is protected against unauthorized access, but the group key can be leaked.

Our contribution

First Line of Defense

Standart symmetric encryption where we assume that the private ID is protected against unauthorized access, but the group key can be leaked.

Second Line of Defense

We consider the case where the attacker would have had access to both the private ID and the group key and we use a synchronisation scheme to prevent intrusion during operations.

Our contribution

First Line of Defense

Standart symmetric encryption where we assume that the private ID is protected against unauthorized access, but the group key can be leaked.

Second Line of Defense

We consider the case where the attacker would have had access to both the private ID and the group key and we use a synchronisation scheme to prevent intrusion during operations.

Third Line of Defense

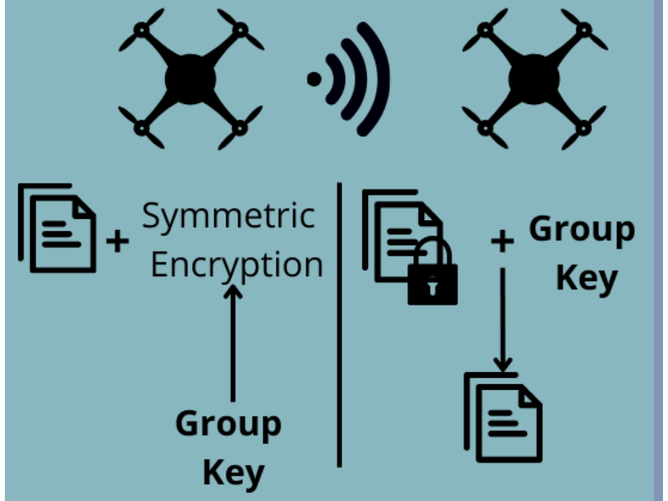
We consider an attacker who has access to the group key, private ID, and the circular variable. We then use a behavior monitoring method to ensure the proper completion of tasks

Attacks

1 Attacker spies on open communication

Protection schemes

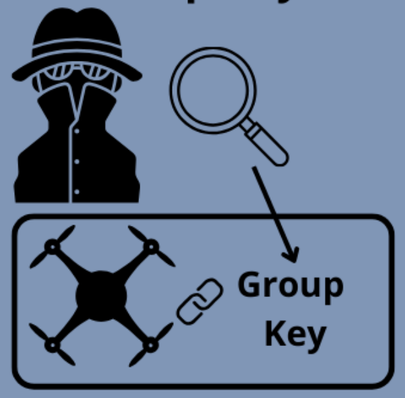
Symmetric Encryption with the Group Key



Attacks

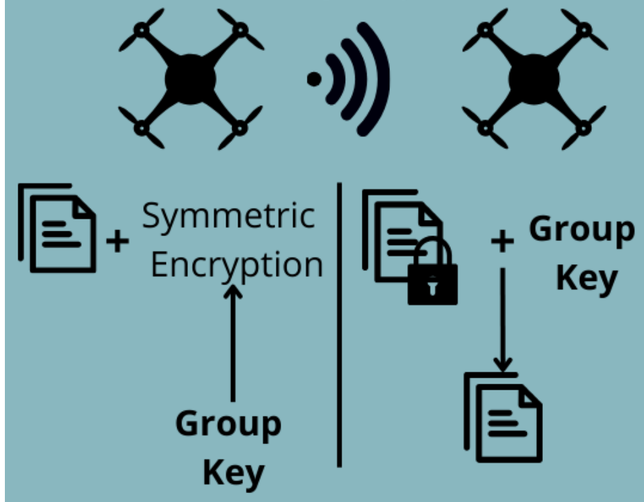
1 Attacker spies on open communication

2 Attacker get access to Group Key

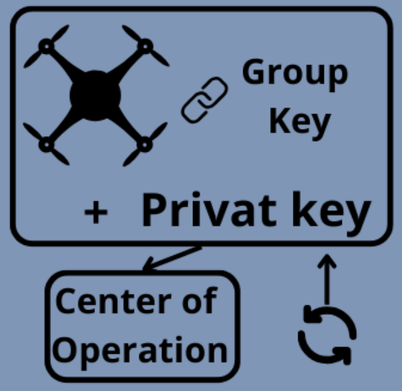


Protection schemes

Symmetric Encryption with the Group Key



Securing the Group Key

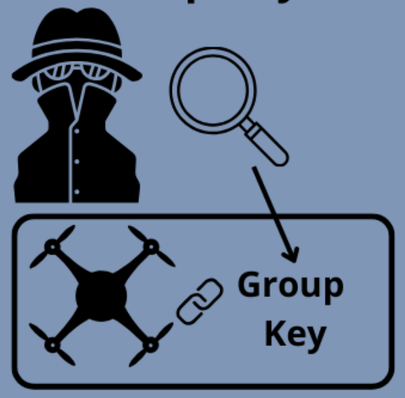


Use private key to update Group key

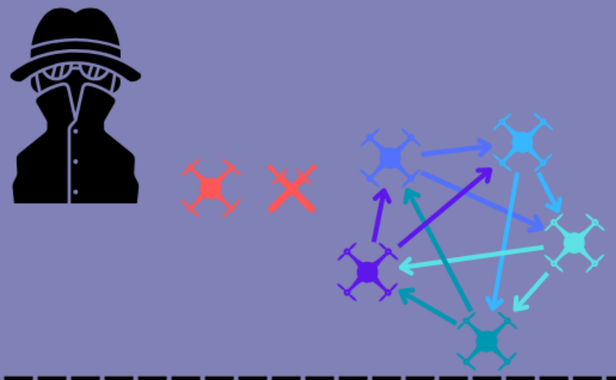
Attacks

1 Attacker spies on open communication

2 Attacker get access to Group Key

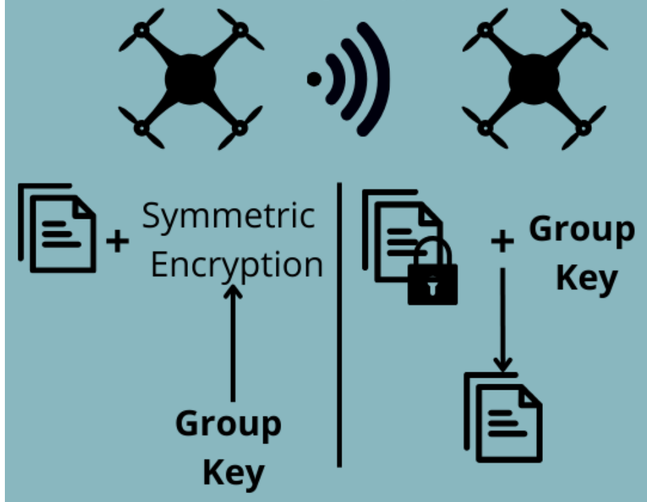


3 Attacker get access to both keys and tries to enter

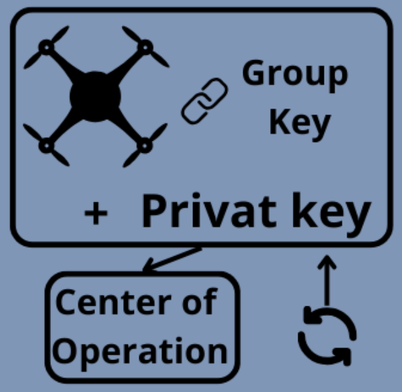


Protection schemes

Symmetric Encryption with the Group Key



Securing the Group Key



Use private key to update Group key

Circulare variable

= *...ezrb4se6r5t4beb6t4e5rstr...*

Message t = n : "rb4s" +

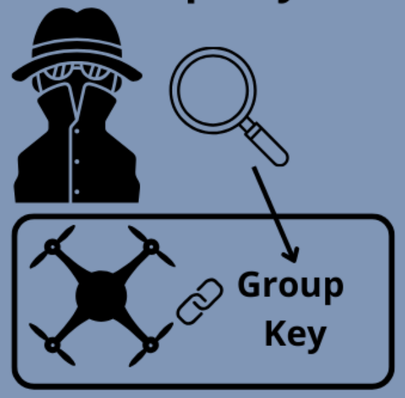
Message t = n+1 : "e6r5" +

Drones use a common secret to comunicate with one-time-use iteration

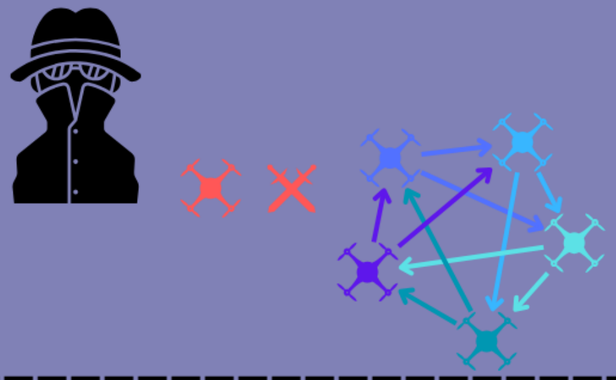
Attacks

1 Attacker spies on open communication

2 Attacker get access to Group Key



3 Attacker get access to both keys and tries to enter

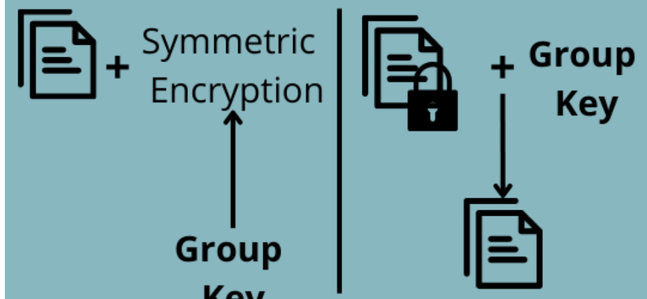


4 Attacker get access to both keys

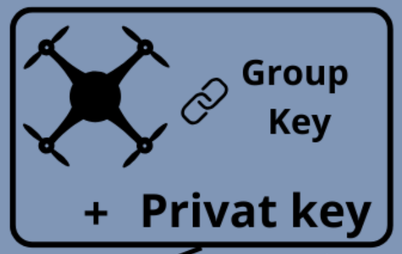
Group Key + Privat key

Protection schemes

Symmetric Encryption with the Group Key

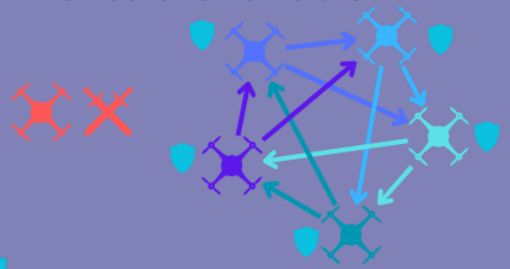


Securing the Group Key



Use private key to update Group key

Circulare variable



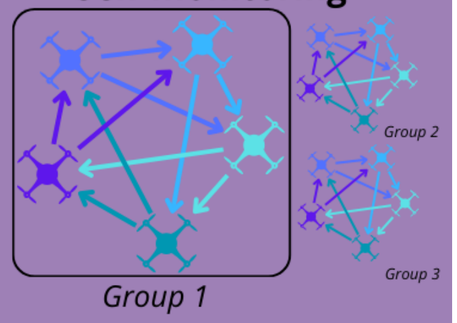
= ...ezrb4se6r5t4beb6t4e5rstr...

Message t = n : "rb4s" +

Message t = n+1 : "e6r5" +

Drones use a common secret to comunicate with one-time-use iteration

Self-monitoring



Drones are grouped and monitor each other but don't know who's monitoring them

Second Line of Defense

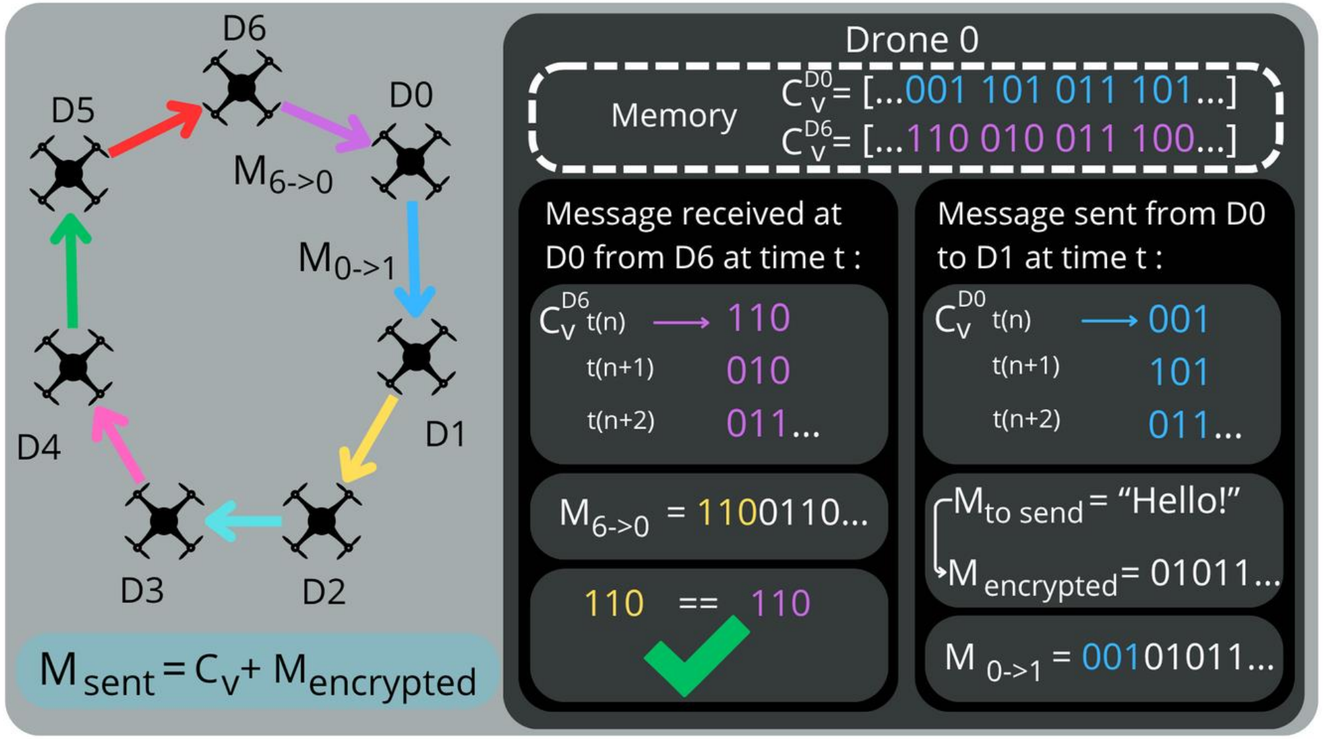


Fig 1: One-path configuration

1. **The Threat**: Protects against attackers who compromise both private ID and group key—scenarios where traditional authentication fails completely.
2. **The Mechanism**: Each message contains a time-indexed fragment from a pre-generated sequence stored onboard; only UAVs with synchronized circular variables for the current time step can validate messages.
3. **The Defense**: Decentralized monitoring where drones don't know who's watching them; single-use fragments follow a circular pattern making replay attacks impossible since wrong fragments instantly expose attackers using only lightweight string operations.

Second Line of Defense

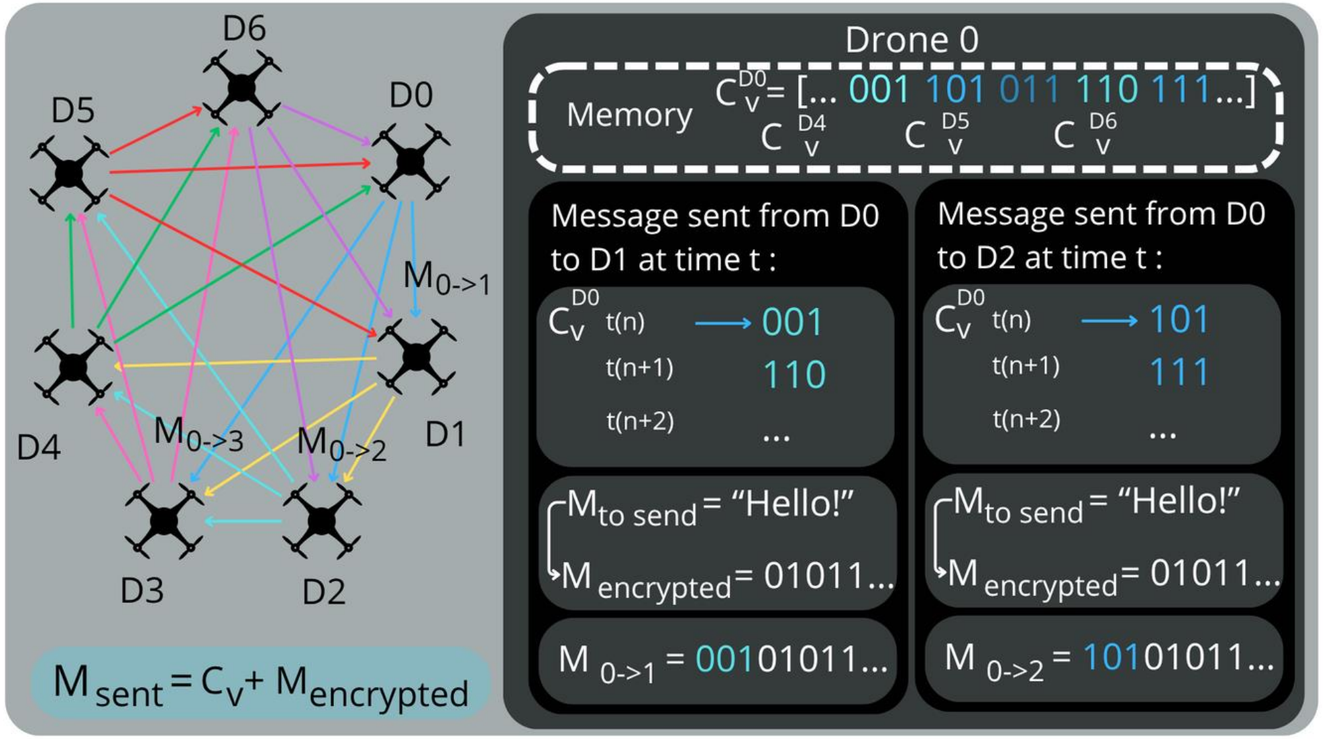


Fig 2 : Three-path configuration

Here we have a three path configuration where three single-use fragment are needed, giving a more robust cycle.

Third Line of Defense

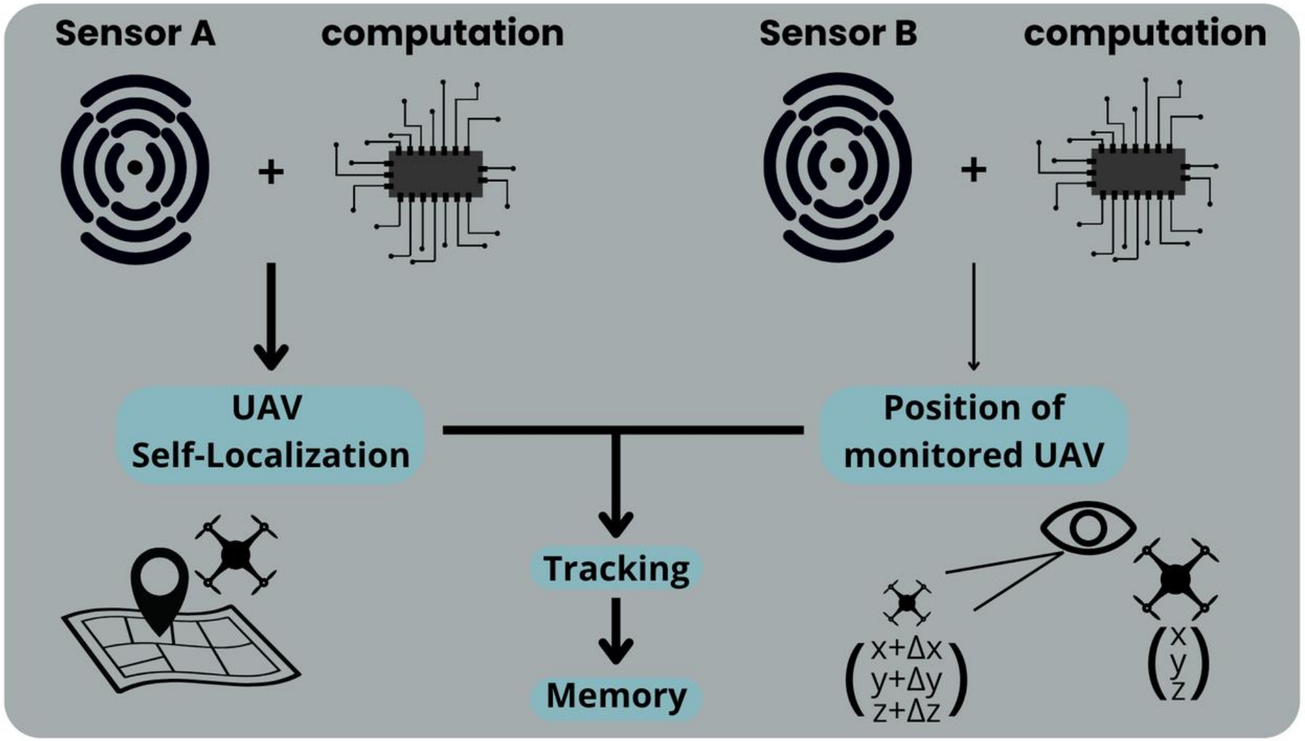
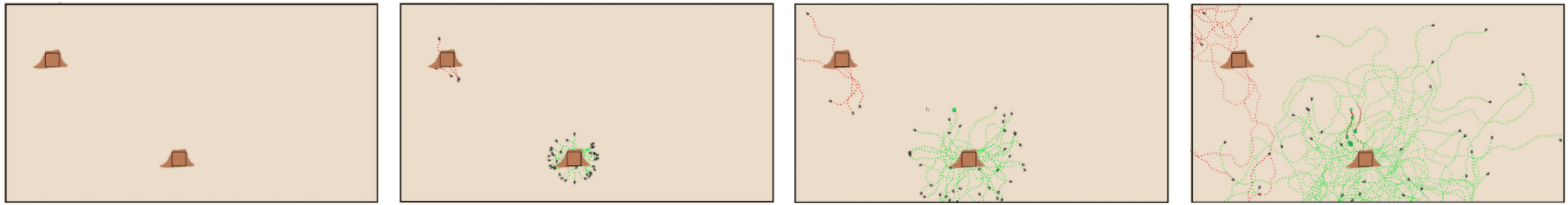


Fig 3 : Behavior monitoring based on localization

1. **Ultimate Breach Scenario**: Addresses complete credential compromise—attacker possesses private ID, group key, AND circular variable, rendering all authentication useless.
2. **Decentralized Monitoring**: UAVs observe each other via Bluetooth signals and Mobile-to-Mobile Localization (Time-of-Arrival/Angle-of-Arrival), comparing expected mission trajectories against real-time observed movements.
3. **Anomaly Detection & Resilience**: Deviation beyond threshold flags rogue units; distributed monitoring prevents single-point manipulation—even delayed attacks are caught by neighboring drones, ensuring mission integrity survives total credential theft.

Experiments

Using ant behavior simulation to test our proposed framework, particulary the behavior analysis



(a) Initialization of the anthills with random position

(b) Ants leaving their hill with the behavior *Random Walk*; green pheromones are allies ants and red pheromones are for the rogue ants

(c) Food appears in the simulation, and ants can capture it and change behavior to *Go Back Home*

(d) Food is brought back to the anthill

Fig 4 : The developed simulator for ant-based swarm UAV communication

Experiments

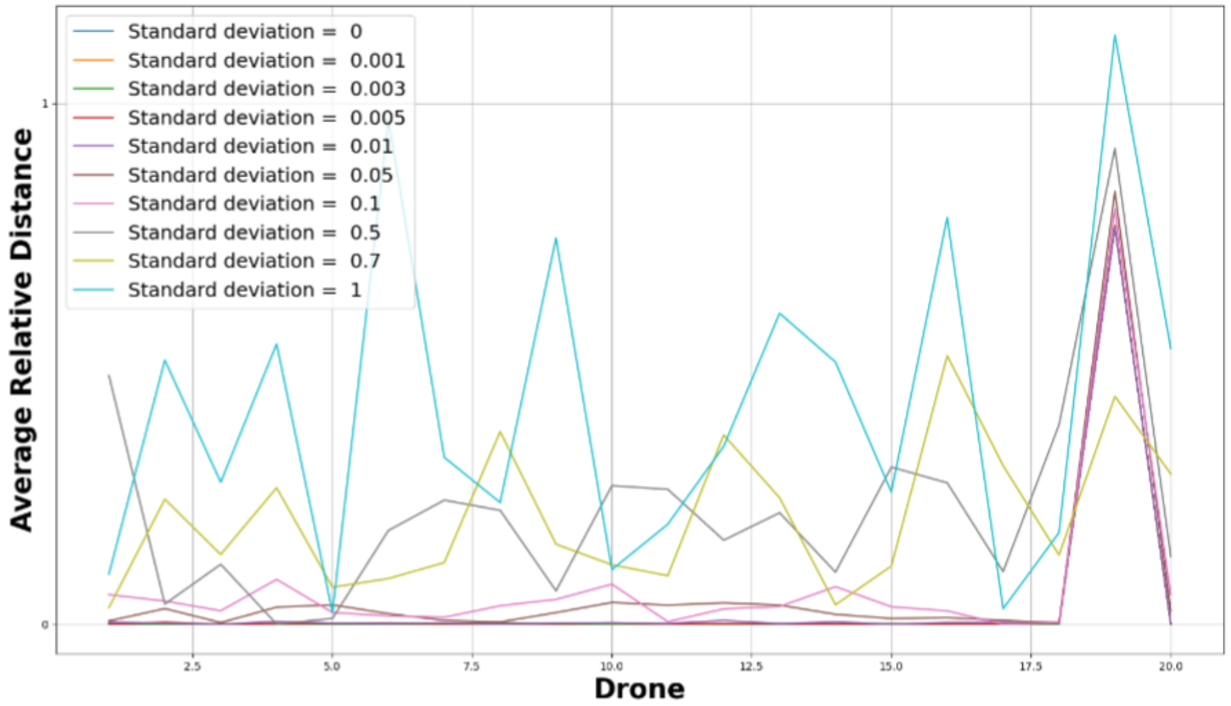


Fig 5 : ARD from the expected behavior per UAV and per standard deviation for a 1000-cycle simulation

1. **Platform & Model**: Python/Pygame simulation mimicking ant colony foraging behavior—coordination, communication, and task completion mirror UAV swarm operations with food retrieval representing mission objectives.
2. **Attack Scenarios**: Allied ants vs. rogue ants test all three security layers (private IDs, group keys, circular variables) under infiltration and misbehavior conditions.
3. **Validation Results**: Visualizes real-time exclusion of compromised agents through failed circular variable checks and trajectory deviation flags—enabling rapid assessment of swarm coordination, communication timing, and security mechanism performance impact.

Key Findings: Layered Defense Superiority

1. **Multi-Layer Protection**: Periodic group key updates minimize long-term exposure; circular variables provide lightweight defense against mid-mission infiltration (a gap in existing models); behavioral monitoring catches fully-credentialed malicious/hijacked UAVs
2. **Decentralized Resilience**: System eliminates single points of control by distributing security across identification, encryption, synchronization, and behavior verification—transforming individual vulnerabilities into collective strength
3. **Operational Impact**: Enables reliable swarm UAV operations in unpredictable and adversarial environments where traditional centralized security models would fail under coordinated attacks or credential compromise

Questions ?

Hugo Le Dirach
University of Toulouse
Toulouse, Occitanie, France

Amin Rezaei
California State University Long Beach
Long Beach, California, USA