CERIAS

The Center for Education and Research in Information Assurance and Security

Range-Based Multi-Robot Integrity Monitoring For Cyberattacks and Faults: An Anchor-Free Approach

Vishnu Vijay, Kartik A. Pant, Minhyun Cho, Yifan Guo, James M. Goppert, and Inseok Hwang

Motivation

- We consider a **multi-robot system (MRS)** subject to **spoofing attack** or **sensor fault** causing **localization error**.
- Such an occurrence could lead to **sub-optimal performance** of the MRS or **catastrophe** (see Fig 1).
- Many **existing literature** solve this problem by **using assumptions** that a **known subset of the MRS is not affected** by the attack or fault, which are limiting and difficult to ensure in practice.

Goal: Design a decentralized algorithm to detect, identify, and iteratively reconstruct localization error in MRS without anchors ("leaders" with unaffected position estimate)

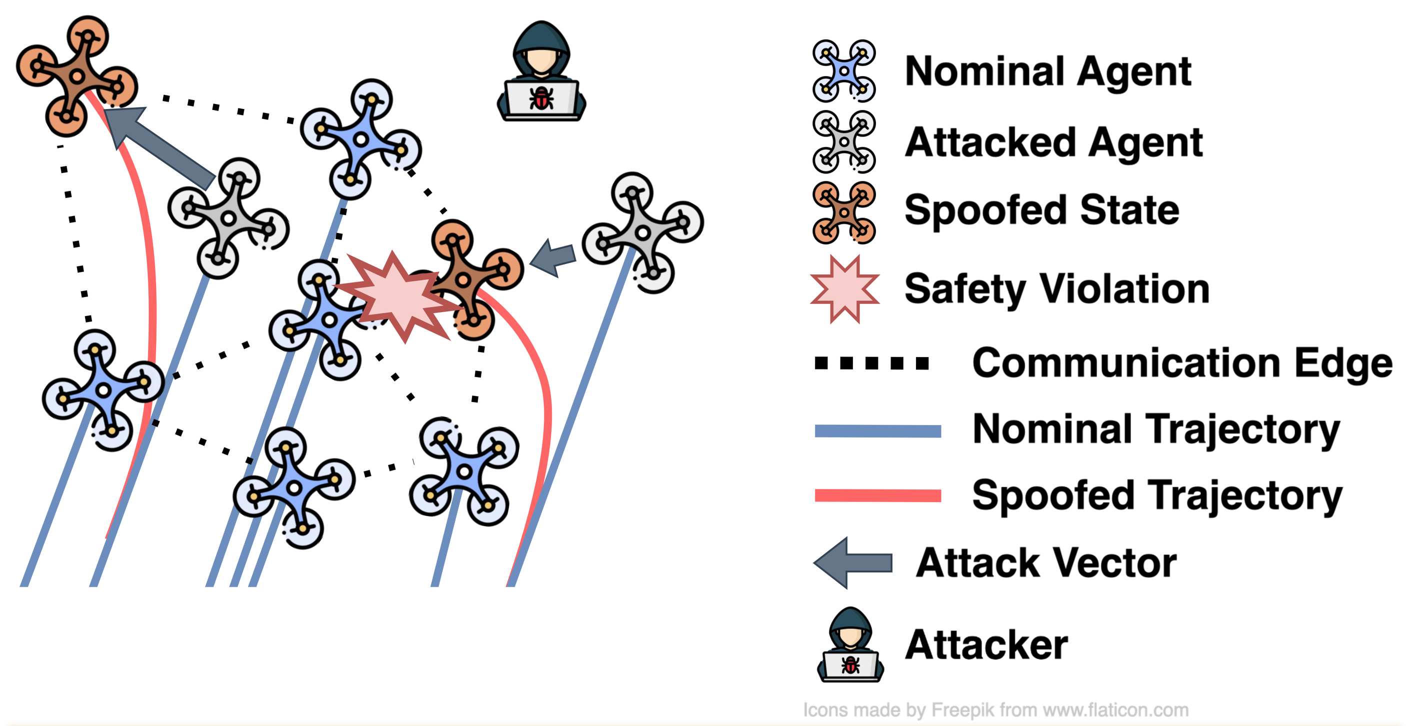

Fig 1: Illustration of spoofing attacks in MRS

Proposed Architecture

- Optimization problem is posed **leveraging a sparse-error assumption**, which is more realistic than known unaffected robots.
- The problem is relaxed using sequential convex optimization (SCP) and alternating direction of multiplier method (ADMM) to **enable real-time** and **decentralized error reconstruction**.
- While **each robot reconstructs its own local error vector**, a local **robot integrity measure** is computed and sent to a centralized integrity monitor. The integrity monitor **aggregates these robot integrities** into an **MRS integrity measure**. A threshold is used to **detect an error** and **identify the affected robot(s)**.

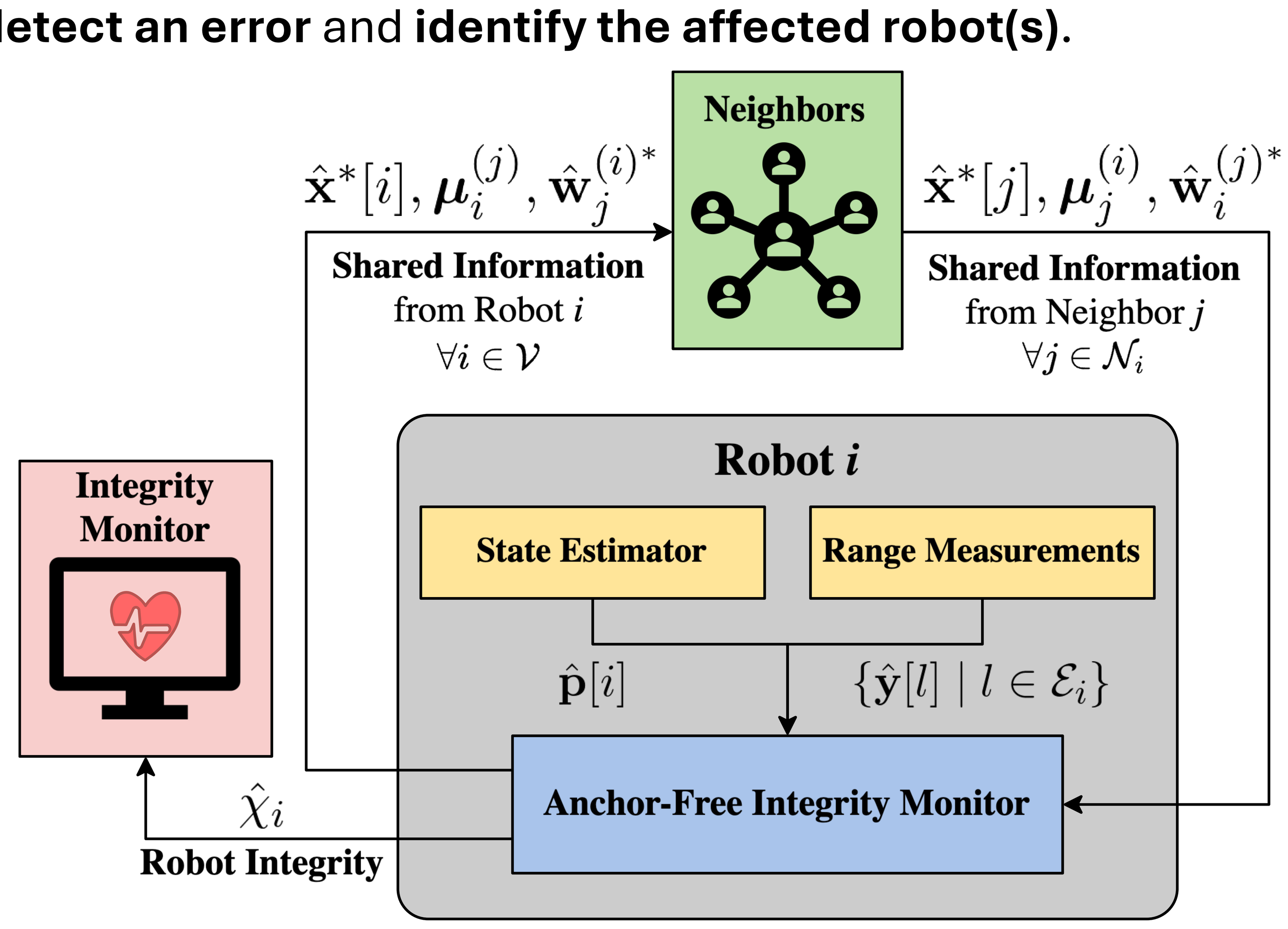

Fig 2: Overall system architecture

Simulation Results

The **algorithm is tested on the example MRS** in Fig 3, which shows the **estimated** and **true robot states** alongside the **true error vectors**

- First, we show how **varying the ADMM penalty parameter** ρ can **mitigate the effect of noise** on the error vector reconstruction.
- Next, we show how the **proposed cold start method is more robust against time-varying network topology** compared to the typical warm start method of ADMM.

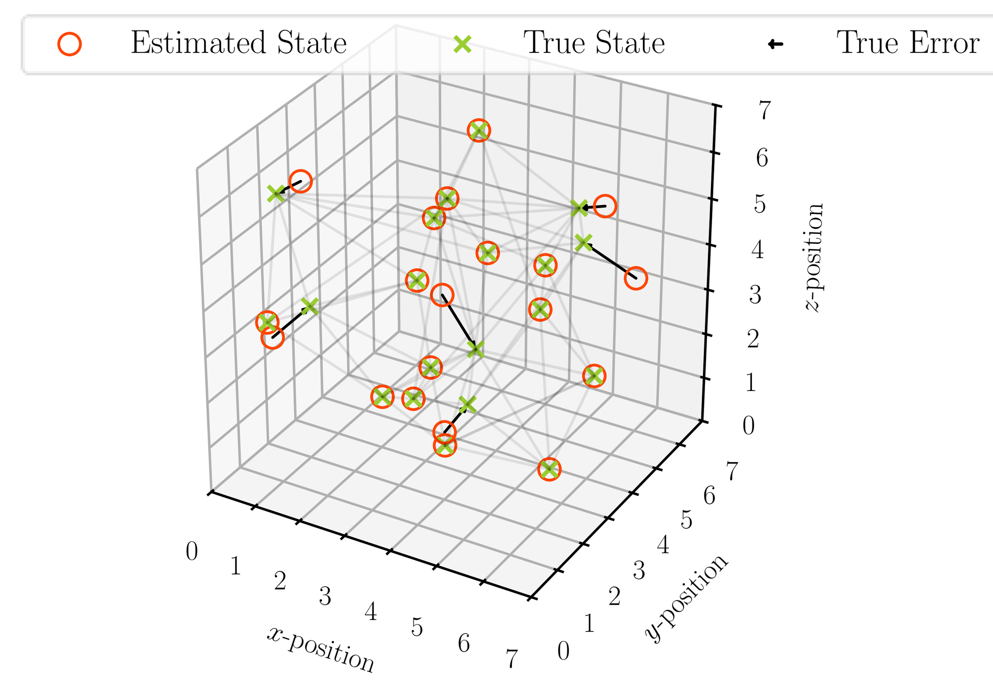

Fig 3: Example MRS configuration

Effect of Noise on Error Reconstruction

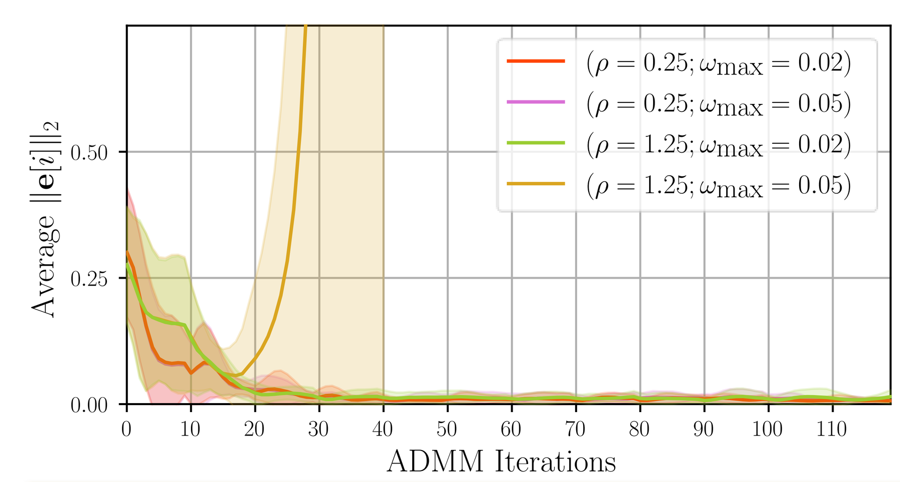

Fig 4a: Comparing trials with varying ρ and ω_{max} values

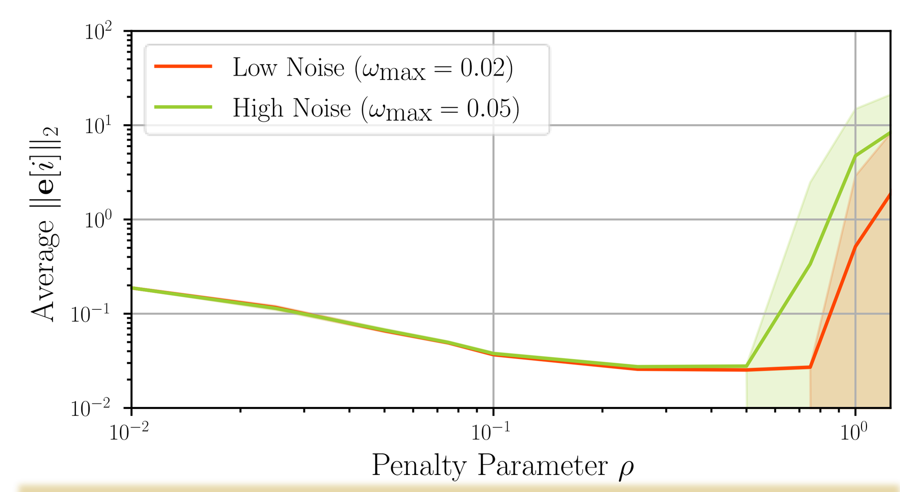

Fig 4b: Monte Carlo simulations with varying ρ and ω_{max} values

Effect of Cold Start on Error Reconstruction

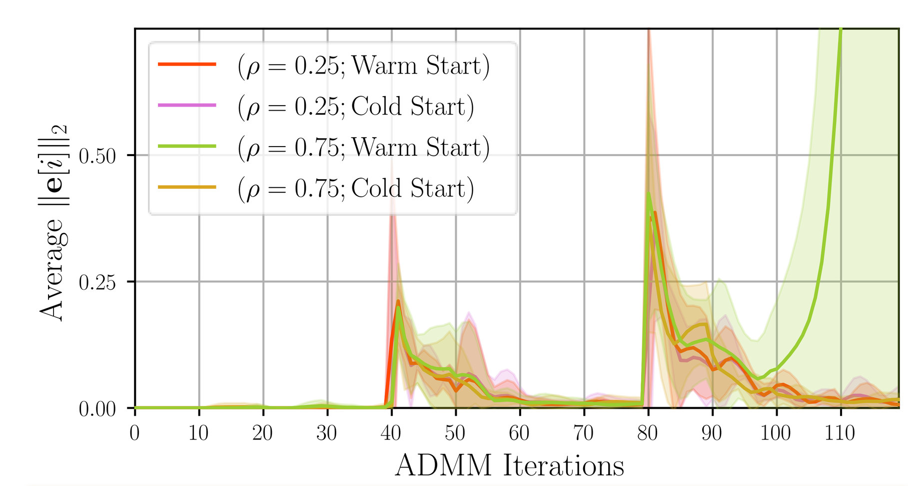

Fig 5a: Comparing trials at varying ρ with warm vs. cold start

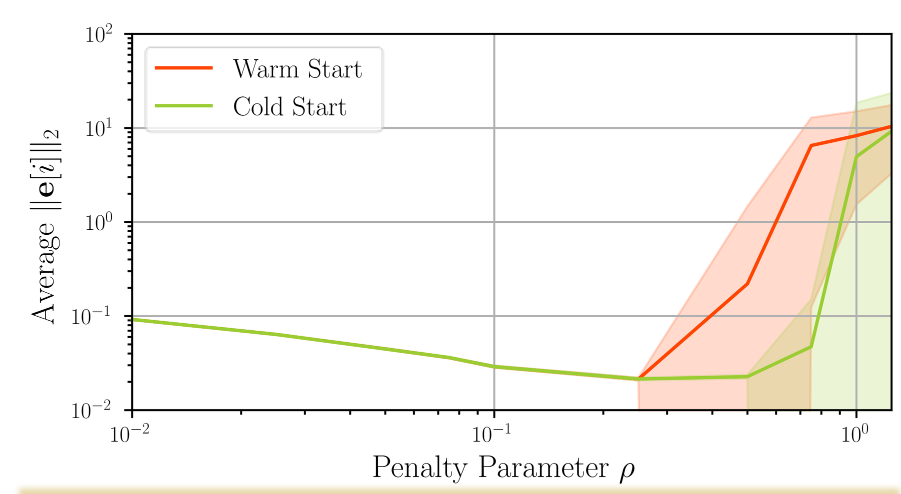

Fig 5b: Monte Carlo simulations at varying ρ with warm vs. cold start

Mixed-Reality Experiment Results

The **MIXED-SENSE** [2] framework enables **high-fidelity experiments** by **emulating GNSS sensor** measurements. **Real Crazyflie UAVs** and virtual **PX4-SiTL instances** are used in a ROS2-Gazebo environment.

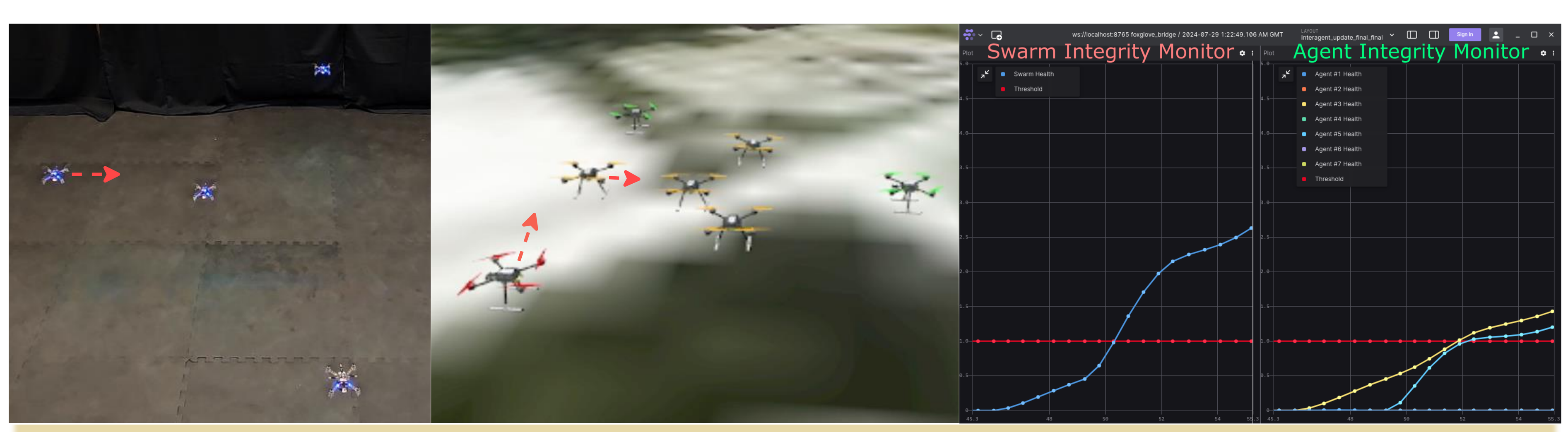

Fig 6: Mixed reality experiments. *Left*: Real Crazyflie UAVs in motion-capture environment. *Center*: Real + Virtual UAVs in Gazebo. *Right*: Integrity monitors for MRS and individual robots.

PURDUE UNIVERSITY

[1] Vijay, V., Pant, K. A., Cho, M., Guo, Y., Goppert, J. M., & Hwang, I. (2024)."Range-based Multi-Robot Integrity Monitoring Against Cyberattacks and Faults: An Anchor-Free Approach." IEEE Robotics and Automation Letters, 2025.
[2] Pant, K. A., Lin, L. Y., Kim, J., Sribunma, W., Goppert, J. M., & Hwang, I. (2024). "MIXED-SENSE: A Mixed Reality Sensor Emulation Framework for Test and Evaluation of UAVs Against False Data Injection Attacks." IROS, 2024.

CERIAS