# Trajectory-Aware Framework for Multi-UAV Collaborative SLAM Under ROS Network Vulnerabilities

Muhammad Wicaksono, Muhammad Imad*, Man Hee Lee*, Soo Young Shin*
{muhammadwicak97, imadsafi08*, fordmore*, wdragon*} @kumoh.ac.kr

Department of IT Convergence ngineering
Kumoh National Institute of Technology

## Abstract

This paper presents a machine learning-enhanced planning framework for resilient multi-UAV collaboration within ROS-based systems. The proposed system integrates learning models to improve adaptive decision-making during autonomous navigation and collaborative SLAM in dynamic and cluttered environments. Machine learning is also employed to identify irregular behaviors and enhance path planning robustness. The system's performance is evaluated using benchmarking datasets and real-world UAV missions, with a focus on path planner reliability and system-level resilience. By embedding intelligence into both planning and monitoring components, the framework improves coordination, adaptability, and safety in multi-UAV reconnaissance operations under challenging conditions.

Keywords : UAV, Frontier Exploration, Depth Camera, Glass Detection

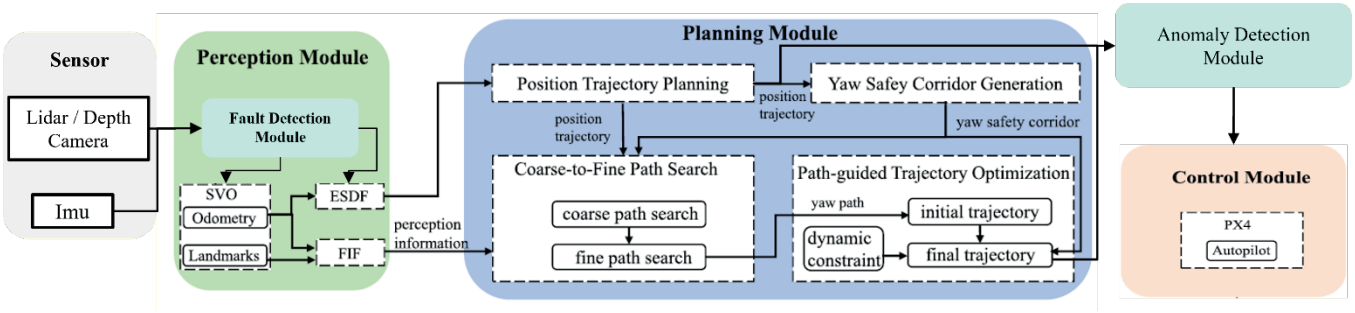


Fig. 1 Overview planner architecture.

## I. Introduction

The deployment of multi-Unmanned Aerial Vehicles (multi-UAV) flying at controlled speeds and altitudes for specialized tasks has garnered considerable attention in recent research [1]. Due to the inherent complexity associated with multi-agent operational environments, Simultaneous Localization and Mapping (SLAM) techniques have emerged as crucial components in enhancing the autonomy and collaboration of UAV swarms. The effective performance of these multi-UAV systems significantly depends on their underlying communication frameworks, commonly facilitated by Robot Operating System (ROS)-based networks [2].

Several ROS variants have been developed to address specific application needs. ROS-1, widely utilized in academic and research settings, is noted for its lack of robust network security features [3]. Aiming to address these vulnerabilities, ROS2 was introduced, incorporating the Data Distribution Service (DDS) security standard.

Addressing these security concerns, our study focuses on early anomaly detection by monitoring deviations between planned trajectories and actual UAV behaviors. Specifically, we implement a collaborative multi-UAV SLAM framework and conduct a systematic analysis to identify and mitigate security vulnerabilities in ROS-based multi-agent systems.

## Ⅱ. Proposed System

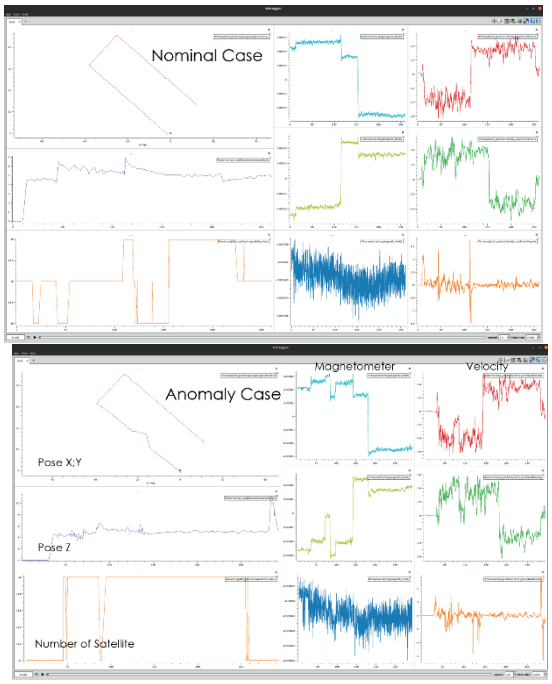


Fig. 2 Result Anomaly and Nomina Case in UAV Collaborative

The overall proposed system investigates the concept of collaborative multi-UAV SLAM, as illustrated in Fig. 1. The designed framework aims to facilitate early warning anomaly by allocating specific system components to a centralized server. UAV agents interact with the server to offload computationally intensive tasks and retrieve processed data. Both the UAV agents and the centralized server utilize a communication module based on the ROS infrastructure, enabling message passing over wireless networks. Previous work, such as the penetration testing presented in [3], demonstrates the susceptibility of ROS to malicious data manipulation using tools like RosPenTo. Consequently, in the context of multi-UAV systems, these vulnerabilities can lead to severe disruptions and compromise mission-critical operations. Therefore, the proposed framework integrates early anomaly detection mechanisms to continuously monitor deviations between planned UAV trajectories and actual behaviors, enhancing the robustness and security of collaborative multi-UAV SLAM systems.

The experimental results clearly demonstrate two distinct scenarios for the multi-UAV SLAM system, namely the **nominal case** and the **anomaly case**, as shown in Fig. 2. In the nominal case, the UAV trajectory follows the predefined path accurately, exhibiting stable positional data, consistent velocity profiles, stable magnetometer readings, and a consistent number of satellite connections, indicating normal system operation. Conversely, the anomaly case illustrates noticeable deviations from the planned trajectory, reflected prominently in positional data (particularly in the Z-axis).

## Ⅳ. Conclusion and Future Work

This study was proposed a data security assessment of the robot operating system in the multi-UAV cooperative reconnaissance missions. In this paper was implementing a centralized collaborative SLAM framework for robotic agents. This proposed system was aim to stipulate the inclusion of data security of ROS in the multi-UAV cooperation. In the future the Quantum-Resistant Authentication Protocols will investigate and design authentication protocols resilient to quantum attacks, ensuring the confidentiality and integrity of communication channels within multi-UAV systems.

## ACKNOWLEDGMENT

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2025-RS-2024-00437190) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation, 50%) This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ICAN(ICT Challenge and Advanced Network of HRD) program(IITP-2025-RS-2022-00156394) supervised by the IITP(Institute of Information & Communications Technology Planning & Evaluation, 50%)

## References

[1] B. Michael , N. Janosch , G. Pascal , S. Thomas , R. Joern , O. Sammy , W. A. Markus dan S. Roland , “The EuRoC MAV Datasets,” dalam *The International Journal of Robotics Research*, 2016.

[2] C. Mitch, R. Prakash dan F. Saleh, “UAV swarm communication and control architectures: a review,” *Journal of Unmanned Vehicle Systems,* pp. 93-106, 2019.

[3] D. Bernhard, B. Benjamin, T. Sebastian , K. Severin, R. Stefan dan S. Peter, “Security for the Robot Operating System,” *Robotics and Autonomous Systems,* vol. 98, pp. 192-203, 2017.

[4] Z. Quanyan, R. Stefan, D. Bernhard dan M. V. V´ıctor , “An Introduction to Robot System,” arXiv, 10 September 2021. [Online]. Available: https://arxiv.org/pdf/2103.05789.pdf. [Diakses 05 01 2024].