Securing Multi-UAV Collaborative SLAM through ROS: A Machine Learning-based Anomaly Detection Approach

Muhammad Wicaksono, Muhammad Imad[ʁ], Soo Young Shin[*]

muhammadwicak97@kumoh.ac.kr, imadsafi08@kumoh.ac.kr[ʁ], wdragon@kumoh.ac.kr[*]

Department of IT Convergence engineering
Kumoh National Institute of Technology

Abstract

Multi-UAV systems have become increasingly prevalent in various applications, and ensuring their security is paramount. This paper proposes a novel approach to secure online anomaly detection within the Robot Operating System (ROS) framework, focusing on collaborative Simultaneous Localization and Mapping (SLAM). Despite structured paths, vulnerabilities in application layers can lead to unauthorized access and malicious attacks. To address this challenge, we present a robust anomaly detection ROS node that leverages machine learning and statistical techniques for real-time monitoring of data exchanges. By analyzing the dynamics of data flow and communication patterns among UAVs, our proposed system aims to detect anomalies indicative of potential security breaches. This research advances secure and reliable collaborative UAV systems with implications for various domains, including surveillance, search and rescue, and environmental monitoring.

Keywords : Multi-UAV Security, ROS Framework, Collaborative SLAM, Anomaly Detection.

I. Introduction

The use of multi-UAV to fly at controlled speeds and heights for specific tasks has attracted significant attention [1]. Given the complexity of the operational environment for multi-UAV, SLAM has been utilized in complex multi-agent applications. The operational multi-UAV performance of architectures relies on the ROS communication network architecture [2]. Several variants of ROS have been created, including ROS-1, which is commonly used in research and lacks network security features [3]. In response to security concerns, ROS2 was released, which introduced a DDS security standard. However, the DDS system still has many vulnerabilities that can protect compromised nodes. In [4], introduce an approach for real-time anomaly detection, which calculates the Hellinger distance between the probability distribution of observations collected within a sliding window and the expected emission probability distribution. To overcome this several challenges, our contributions are present the implementation of multi-UAV collaborative SLAM and discuss the security vulnerabilities in ROS-based multi-agent systems.

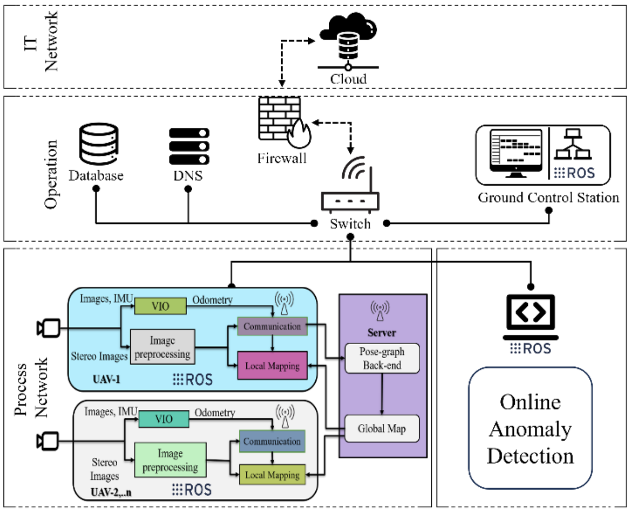

Fig. 1 Overview collaborative SLAM in multi-UAV.

II. Proposed System

The proposed system for securing Multi-UAV Collaborative SLAM through ROS employs a machine learning method, specifically Hidden Markov Models (HMMs) designed for anomaly detection in multi-UAV. At its core, the system establishes a model representing the expected (nominal) behavior of the

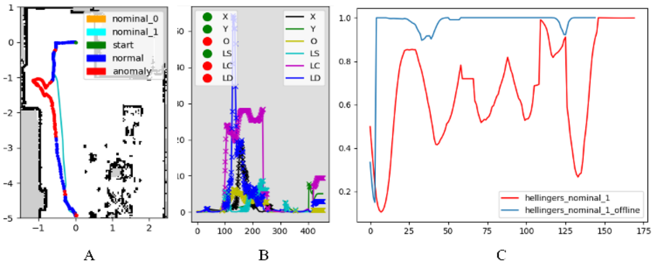

Fig. 2 Online anomaly detection, (A) simulation running in ICE LAB dataset [4], (B) current observation compared with the nominal distribution, (C) Hellinger measures dissimilarity between probability distributions.

UAVs engaged in collaborative SLAM tasks. This model, based on Hidden Markov Models, encapsulates the probabilistic transitions between different states of the UAVs during routine operation. As the UAVs perform collaborative SLAM activities, the system continuously monitors their behavior in real-time, capturing data on movement patterns, sensor readings, and communication interactions. Through a comparative analysis, the system evaluates the observed behavior against the expected behavior encoded in the Hidden Markov Model. This comparison is facilitated by computing the dissimilarity between the probability distributions of observed and nominal behaviors, using the Hellinger Distance statistical function. If the computed Hellinger Distance exceeds a predefined threshold, it signifies a significant deviation from the expected behavior, prompting the system to flag the UAV's behavior as anomalous, indicative of a potential security threat or malfunction. Furthermore, the system offers insights into the specific variable or aspect of UAV behavior responsible for the detected anomaly through Hellinger Distance decomposition, aiding in anomaly.

Ⅲ. Result Implementation

We used the publicly available dataset [4] and our own real-time experiment to determine the feasibility of the proposed method in real-world situations. The results of our experiments demonstrate that a constant detection threshold is sufficient for our anomaly detection system, and the bounded nature of our anomaly scores confers semantic meaning to such a threshold. The selection of an appropriate threshold depends on the specific application context. For instance.

IV. Conclusion and Future Work

This system provides a robust framework for detecting abnormal behaviors in collaborative SLAM scenarios, leveraging machine learning techniques and statistical analysis within the ROS environment. 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 ICAN(ICT Challenge and Advanced Network of HRD) program(IITP-2024-RS-2022-00156394) supervised by the IITP(Institute of Information & Communications Technology Planning & Evaluation) This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(2018R1A6A1A03024003)

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] D. Azzalini, A. Castellini dan M. Luperto, “HMMsforAnomalyDetection in Autonomous Robots,” dalam *Autonomous Agents and Multiagent Systems*, New Zealand, 2020.