Data Security Assessment of the Robot Operating System in the Multi-UAV Cooperative Reconnaissance Missions

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

This paper presents a comprehensive data security assessment of a robot operating system (ROS) utilized in an autonomous multi-unmanned aerial vehicle (UAV) cooperative reconnaissance mission. The primary objectives of this study are to implement collaborative Simultaneous Localization and Mapping (SLAM) for multi-UAV cooperation and to establish the inclusion of data security within the ROS for reconnaissance missions. This study employed an extensive analysis of benchmarking datasets and real-time flight demonstrations to identify vulnerabilities in ROS-based data sharing. Finally, this article proposes a quantum secure data solution to safeguard against cyber-attacks targeting ROS communication block.

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

I. Introduction

The use of multi-UAV to fly at c [1]ontrolled 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], the integration of post-quantum secure encryption schemes with robotic operating ROS was report due to ensuring the network communications layer stay secure even attack by quantum computing advances. 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.

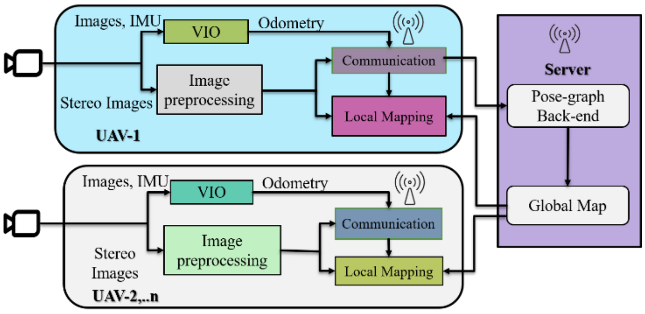

Fig. 1 Overview collaborative SLAM architecture.

Ⅱ. Proposed System

The overall proposed system start from investigates the concept of multi-UAV collaborative SLAM. In fig. 1, the proposed framework aim to effectively transmit computational intent in real-time by allocating certain system components to a centralized server. The UAV can use the server to offload and download information. Both the server and agents run a communication module that utillized the ROS communication infrastructure for message passing over a wireless network. However, ROS communication also renders the system susceptible to the rapid infiltration of malicious components. In [3], the penetration testing of ROS is

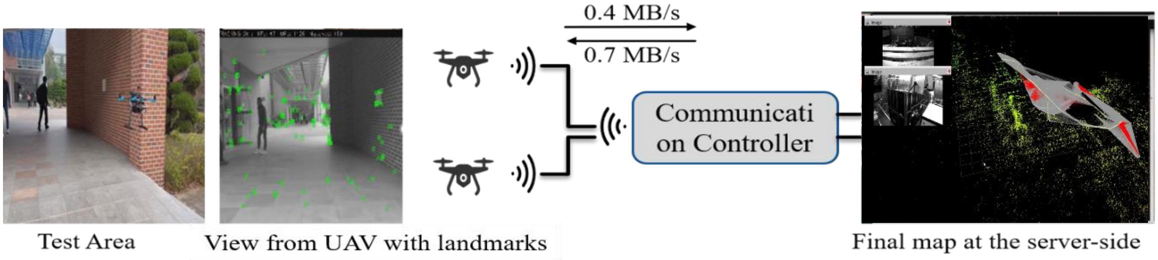
0.4 MB/s
0.7 MB/s
Communicati on Controller
Test Area
View from UAV with landmarks
Final map at the server-side

Fig. 2 Flowchart Object Detection

deployed, with the developed RosPenTo to show manipulated data. This application allows the publisher or subscriber to isolate conditions that also inject false data. The comparison in default ROS configuration, the execution of actions by an attacker is not impeded. When security measures are implemented at the application level, it is observed that the attacker may still subscribe or publish. In the given scenario, the potential consequences are far-reaching and serious. The quantum threat amplifies the urgency of securing these systems against unauthorized access or manipulation. This is paramount to safeguarding the integrity, reliability, and safety of multi-UAV operations. Therefore, the implementation of such measures is crucial to ensure the secure and reliable operation of multi-UAV systems.

Ⅲ. Result Implementation

We used the publicly available EuRoC dataset [1] and our own real-time experiment to determine the feasibility of the proposed method in real-world situations. Initially, a server map is created for each agent. The authors then detected an overlap between the server maps of agents 1 and 2, leading to the formation of a new server map that operated at the distances of both agents, as depicted in the accompanying figure. Finally, all UAVs are localized on the same map, allowing them to continue their onboard estimations and collaborations, as shown in the fig.₩ref{fig3.

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. An in-depth analysis has been made on datasets and practicality of the proposed frameworks is demonstrated with real time flights. 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-2023-RS-2023-00259061) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

“This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the Grand Information Technology Research Center support program (IITP-2022-2020-0-01612) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation)”

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].