Enhanced Security and Coordination Framework for UAV Swarms Using Heterogeneous Communication Networks

Daniel Bonilla Licea(✉), Giuseppe Silano, and Martin Saska

Faculty of Electrical Engineering, Department of Cybernetics, Czech Technical University in Prague, 12135 Prague, Czech Republic
{bonildan,giuseppe.silano,martin.saska}@fel.cvut.cz

Abstract. Unmanned Aerial Vehicle (UAV) swarms offer remarkable capabilities across numerous fields, performing complex tasks with high efficiency and adaptability. However, safeguarding these swarms from cyber threats poses a significant challenge. This paper addresses "*Challenge 4: Enhanced Communication and Active Protection Framework*". We aim to solve key objectives by introducing a comprehensive framework aimed at bolstering the security and coordination of UAV swarms. Our framework incorporates communications-aware trajectory planning, the use of heterogeneous communication networks, advanced physical layer security measures, and Artificial Intelligence (AI)-driven strategies for detecting and mitigating attacks. By combining Optical Camera Communications (OCC) with conventional Radio Frequency (RF) systems and utilizing Reinforcement Learning (RL) and Federated Learning (FL), the proposed framework provides a robust, efficient, and secure operational environment for UAV swarms.

Keywords: UAV Swarms · Communication Framework · Cybersecurity · AI

1 Introduction

Unmanned Aerial Vehicle (UAV) swarms have the capability to operate autonomously and collaboratively, offering significant advantages over single-drone operations. These benefits include enhanced coverage, redundancy, and resilience [1]. To achieve effective coordination and communication within UAV swarms, various architectures have been proposed, with hierarchical architectures being the most widely adopted [2]. In a hierarchical structure, drones are organized in tiers, where higher-tier drones oversee and coordinate the actions of lower-tier drones. This arrangement simplifies command and control, reduces decision-making complexity at the individual drone level, and enhances scalability. The hierarchical approach is particularly favored for its efficiency in managing large swarms and its robustness in maintaining operational coherence [2].

However, hierarchical architectures also present challenges [3]. A major issue is the reliance on Radio Frequency (RF) communication systems for most UAV interactions.

D. B. Licea and G. Silano—Authors contributed equally to this work.

M. Andreoni and S. Thakkar (Eds.): GENZERO 2024,
Proceedings of 1st GENZERO Workshop, pp. 117–123, 2026.
https://doi.org/10.1007/978-981-95-1050-4_14

This makes these systems vulnerable to attacks such as RF jamming, which can disrupt communication or Global Navigation Satellite System (GNSS) signals, and GNSS spoofing, which can manipulate positional data. Additionally, UAV identity spoofing can lead to unauthorized control, while eavesdropping on communications can compromise sensitive information [4]. These vulnerabilities highlight the need for robust security measures to protect the integrity and reliability of UAV communication networks.

A traditional approach relying solely on cryptographic measures is insufficient to address the security challenges faced by UAV swarms and to maintain a secure and highly robust operation. To ensure swarm security, it is essential to employ Artificial Intelligence (AI)-based techniques for detecting such attacks and to integrate advanced cryptographic methods with physical layer security techniques. Additionally, heterogeneous communication networks that use both RF and optical communications provide are highly effective in increasing the security of UAV swarms. This approach leverages the large bandwidth provided by RF systems while benefiting from the immunity of optical systems to RF jamming and their significantly higher resistance to eavesdropping [5]. Moreover, communications-aware trajectory planning is a powerful tool for enhancing physical layer security in UAV communications [6]. This technique involves designing flight paths that minimize exposure to potential attacks and optimize the security of communication links.

In this paper, we address "*Challenge 4: Enhanced Communication and Active Protection Framework*". We aim to solve the key objectives of deploying advanced encryption and authentication techniques to safeguard drone communications, utilizing AI to optimize communication strategies and enhance resilience against environmental and malicious disruptions, implementing anomaly detection algorithms to quickly identify and counteract communication threats in real time, and establishing proactive defenses to maintain the integrity and reliability of communications under adversarial conditions with the proposed framework. The proposed approach includes the following key components:

- *Communications-Aware Trajectory Planning:* We build upon our previously developed framework for communications-aware trajectory planning [7,8] and adapt it to the multi-agent scenario. The framework is designed to increase communication reliability using directional antennas that are less vulnerable to jamming;
- *Heterogeneous Communication Networks:* We employ heterogeneous communication networks that we developed, incorporating both RF communication systems and Optical Camera Communications (OCC) systems for UAVs [2].
- *Physical Layer Security Techniques*: We exploit advanced physical layer security techniques enhance the robustness of UAV-to-UAV communication links, increasing their resistance to potential threats [9,10].
- *AI for Attack Detection and Adaptive Response:* We utilize AI to improve the detection of attacks and rely on Reinforcement Learning (RL) to adapt the swarm's behavior to ever-changing and unforeseen situations.

2 Communication and Coordination Framework

In this section, we present our comprehensive communication and coordination framework for hierarchical UAV swarms. This framework operates using a fog-edge formation mechanism, integrating fog and edge computing concepts [11] to enhance the processing capabilities and communication efficiency within UAV swarms. This approach enables real-time data processing and low-latency communication. The framework is divided into four key components: *Advanced Encryption and Authentication*, *AI-Optimized Communication Strategies*, *Real-Time Anomaly Detection*, and *Proactive Defense Mechanisms*. The proposed framework is developed using ROS2 and tested in the Gazebo simulator. Figure 1 outlines the proposed communication and coordination framework.

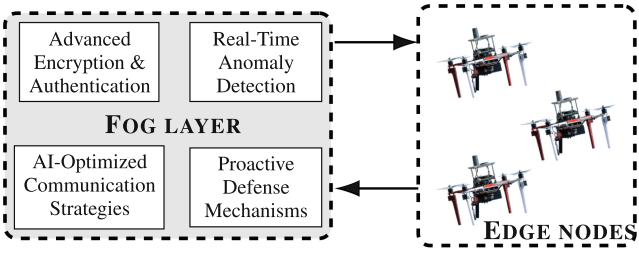


Fig. 1. Proposed communication and coordination framework. Arrows represent the data exchanged among drones.

2.1 Advanced Encryption and Authentication

One of the characteristics of OCC is its immunity to RF jamming, allowing many-to-many communications through the principle of spatial separability [6]. Additionally, eavesdropping on OCC is challenging without being in close proximity and equipped with the correct hardware. Heterogeneous communication networks that combine RF and optical communications offer the advantages of both systems. In this context, we propose a new authentication system for UAVs based on heterogeneous communications networks composed of OCC systems (e.g., UVDAR [2], designed by our team) and RF communications systems.

This authentication technique operates as follows: Each UAV is equipped with an OCC system composed of a camera and various LEDs that can emit arbitrary optical signals. Additionally, they are equipped with RF communications systems. Initially, UAV-zero (initially authenticated by the user) emits a command through its RF communication system for the other UAVs to initiate their authentication. The responding UAVs reply through their RF systems with a message that includes their ID and physical coordinates while simultaneously emitting valid optical signals through their LEDs. When UAV-zero receives the RF message, it uses its camera to verify the coordinates indicated by the other UAVs and retrieves the emitted optical signals.

If the initial message was emitted by a malicious entity that is not a UAV, UAV-zero would not detect any optical signals at the specified coordinates. If the malicious

agent is a UAV equipped with the same OCC system, it would need to know the valid optical signals beforehand to be authenticated by UAV-zero. This requirement makes the authentication technique very difficult to deceive in practice.

2.2 AI-Optimized Communication Strategies

In this section, we introduce AI-optimized communication strategies that enhance the robustness and efficiency of UAV swarm operations using RL. RL is a type of machine learning where an agent learns to make decisions by performing actions in an environment to maximize cumulative rewards. For UAV swarms, RL agents are embedded within each UAV to optimize communication protocols in real-time.

Our RL framework includes the *state*, which represents the current conditions of the UAV swarm, including positions, signal strengths, and link statuses. The *action* space involves adjusting transmission power, selecting communication channels, and switching between RF and optical communication modes. The *reward* function balances communication reliability, latency, and energy consumption. Positive rewards are given for maintaining high-quality links, while negative rewards result from link failures or excessive energy use.

Each UAV, equipped with an RL agent, learns optimal communication strategies through interactions with the environment. Using algorithms like Deep Q-Networks, the agents continuously update their policies based on received rewards. This process ensures that the UAVs adapt to changing conditions and dynamic network topologies, enhancing the overall performance and resilience of the swarm.

AI-optimized communication strategies offer significant advantages. They allow UAVs to adapt to unforeseen challenges, such as interference or signal blockages, ensuring effective communication in various conditions. The decentralized nature of RL makes this approach scalable for large swarms. Additionally, continuous learning and adaptation improve the resilience of the swarm against communication disruptions, including RF jamming and signal interference. By dynamically adjusting protocols based on real-time conditions, these strategies enhance the reliability, efficiency, and security of UAV operations.

2.3 Real-Time Anomaly Detection

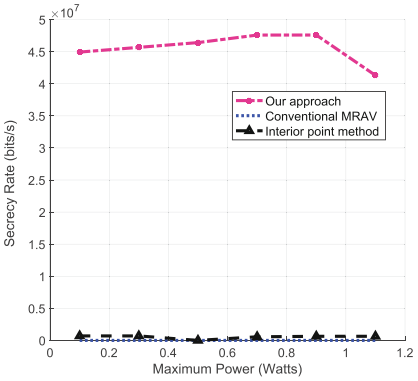
Detection of anomalies is crucial for identifying attacks and implementing appropriate countermeasures. Our approach leverages AI to detect abnormal behaviors and inconsistencies between different sensors that may indicate an attack. For instance, if an RF receiver detects an increase in received power along with an increase in the bit error rate, it can suspect a jamming attack. This information is then shared among all the UAVs via the optical network, which remains unaffected by RF jamming.

Once this data is distributed, a Federated Learning (FL) algorithm [12] processes the collective information from all UAVs to confirm the attack. FL enables UAVs to collaboratively learn a shared model while keeping their data decentralized, enhancing privacy and security. The algorithm can also attempt to estimate the location or direction of the attacker based on the shared data. This distributed AI approach not only detects

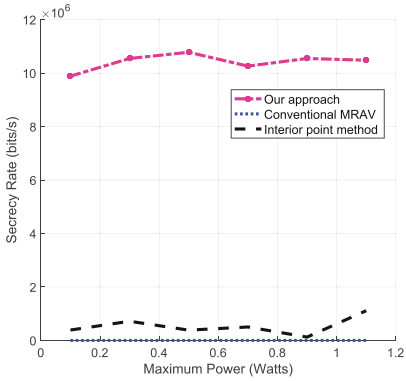
jamming attacks but is also effective against more sophisticated threats such as proactive eavesdropping or deauthentication attacks, which rely on jamming.

2.4 Proactive Defense Mechanisms

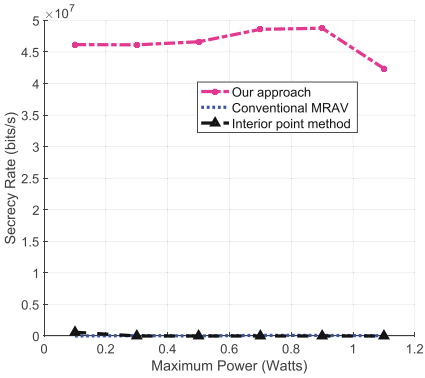
The first line of defense is to hide communications from malicious agents. One way to achieve this is through the use of covert communications, where legitimate transmitters emit artificial noise when they do not have data to transmit. The idea behind this strategy is to confuse malicious nodes, making it difficult for them to determine when actual data exchanges are occurring among the UAVs.



(a) Without jittering and uncertainty.



(b) With jittering.



(c) With uncertainty about the eavesdropper's position.

Fig. 2. The secrecy rate plotted against the maximum power for both the proposed approach and the two benchmarks without any jittering on the UAVs orientation and with perfect knowledge of the eavesdroppers position.

Another line of defense involves ensuring that legitimate transmitters focus their emitted power in the direction of legitimate receivers while minimizing power emission towards potential malicious receivers [10]. Similarly, this strategy aims to ensure that

legitimate receivers experience high channel gain from legitimate transmitters and low channel gain from malicious transmitters [9].

This can be achieved through various methods. One solution is the use of multi-antenna arrays and beamforming techniques. Another approach involves using omni-directional UAVs and optimizing their orientation, as demonstrated in [9,10], and depicted in Fig. 2. A third solution is to use under-actuated UAVs equipped with motorized antennas whose orientation can be controlled.

3 Conclusions

In this paper, we introduced a comprehensive communication and coordination framework to improve the security and operational efficiency of hierarchical UAV swarms. Our framework addresses key vulnerabilities in UAV communication systems, enhancing resilience against cyber threats such as jamming, spoofing, and eavesdropping. AI-driven methods for real-time anomaly detection and adaptive response ensure secure and efficient operations in dynamic and hostile environments. Future work will refine the AI models for more precise anomaly detection and explore integrating additional communication technologies to further enhance the system's robustness and scalability. Additionally, significant efforts will be dedicated to transitioning from simulation to real-world implementation, including conducting field experiments to validate the framework's effectiveness in practical scenarios and ensuring it performs reliably under real-world conditions.

Acknowledgment. This work was partially funded by EU under ROBOPROX (reg. no. CZ.02.01.01/00/22 008/0004590), by the Czech Science Foundation (GAČR) project no. 23-07517S, and by the CTU grant no. SGS23/177/OHK3/3T/13.

References

1. Chung, S.-J., et al.: A survey on aerial swarm robotics. IEEE Trans. Rob. **34**(4), 837–855 (2018)
2. Horyna, J., et al.: Decentralized swarms of unmanned aerial vehicles for search and rescue operations without explicit communication. Auton. Robot. **47**, 77–93 (2023)
3. Adil, M., et al.: A systematic survey: security threats to UAV-aided IoT applications, taxonomy, current challenges and requirements with future research directions. IEEE Trans. Intell. Transp. Syst. **24**(2), 1437–1455 (2023)
4. Kumari, N., et al.: Towards reliable identification and tracking of drones within a swarm. J. Intell. Robot. Syst. **110**(84), 1–31 (2024)
5. Chowdhury, M.Z., et al.: A comparative survey of optical wireless technologies: architectures and applications. IEEE Access **6**, 9819–9840 (2018)
6. Pandey, G.K., et al.: Security threats and mitigation techniques in UAV communications: a comprehensive survey. IEEE Access **10**, 112858–112897 (2022)
7. Bonilla Licea, D., et al.: When robotics meets wireless communications: an introductory tutorial. Proc. IEEE **112**(2), 140–177 (2024)
8. Bonilla Licea, D., et al.: Communications-aware robotics: challenges and opportunities. In: International Conference on Unmanned Aircraft Systems, pp. 366–371 (2023)

9. Bonilla Licea, D., et al.: Omnidirectional multi-rotor aerial vehicle pose optimization: a novel approach to physical layer security. In: IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 9021–9025 (2024)
10. Bonilla Licea, D., et al.: Harnessing the potential of omnidirectional multi-rotor aerial vehicles in cooperative jamming against eavesdropping. In: IEEE Conference on Global Communications (2024, to Appear)
11. Pujol, V.C., et al.: Fog robotics-understanding the research challenges. IEEE Internet Comput. **25**(5), 10–17 (2021)
12. Li, L., et al.: A survey on federated learning. In: IEEE 16th International Conference on Control & Automation, pp. 791–796 (2020)