DOI 10.5162/iCCC2024/P15

Mobilität

Towards Secure and Reliable Heterogeneous Real-time Telemetry Communication in Autonomous UAV Swarms

Pavlo Mykytyn[1, 2], Marcin Brzozowski[1], Zoya Dyka[1, 2], Peter Langendörfer[1, 2]
[1] IHP - Leibniz-Institut für innovative Mikroelektronik, Frankfurt (Oder), Germany
[2] BTU Cottbus-Senftenberg Cottbus, Germany
pavlo.mykytyn @b-tu.de

In the advent of cutting-edge autonomous systems, Unmanned Aerial Vehicles (UAVs) are becoming an essential part of the solutions for a multitude of complex problems, ranging from efficient management of large agricultural fields, search and rescue missions in areas with challenging terrain, rapid delivery of critical medicine or goods, to disaster response missions in order to alleviate the consequences of natural catastrophes. Increased research interest and extensive development in this field have propelled the evolution of autonomous and semi-autonomous UAV swarms to tackle those tasks and missions even more effectively and efficiently. One of the cornerstones of a safe UAV swarm mission is the secure and reliable real-time telemetry communication within the UAV swarm, and to the Base Station (BS). Real-time telemetry communication is an essential channel for command, control, and data transfer, it shapes the core of the mission control framework as well as data acquisition and distribution architecture. In this paper we portray our research and development path to a secure and reliable all-to-all UAV swarm communication, including the exploration and examination of different peer-to-peer telemetry radios such as 433 MHz SiK radio from Holybro or RFD868x-EU radio from RFDesign. We examine the drawbacks and security vulnerabilities of a homogenous peer-to-peer telemetry communication approach, describe lessons learned and discuss the transition to a heterogeneous model that combines multiple communication technologies such as Sub-GHz, 2.4 GHz Wi-Fi, and 5G/LTE. We also investigate and describe the security loopholes of the MAVlink communication protocol, and present a dedicated multi-hop, all-to-all heterogeneous approach to ensure the integrity and confidentiality of real-time telemetry data. We argue that diversity in the communication stack enhances redundancy and ensures persistence of network connectivity, even under the most challenging conditions. The fusion of different communication technologies leverages their unique characteristics, thereby mitigating single points of failure and enhancing the resilience of the network against cyber – attacks and interferences. Our lessons learned reflect the need of a balanced approach with strong security measures and agile real-time communication, underlining the importance of lightweight yet effective security frameworks. Finally, we present our key exchange and data encryption mechanism, specifically tailored to meet the needs of the multi-hop all-to-all UAV swarm communication nature, provide data integrity and confidentiality, and ensure the real-time communication is not impaired by delays and additional overhead posed by the security mechanisms. The key exchange and data encryption process that takes place at the beginning of each flight session is schematically represented by the Figure 1 below.

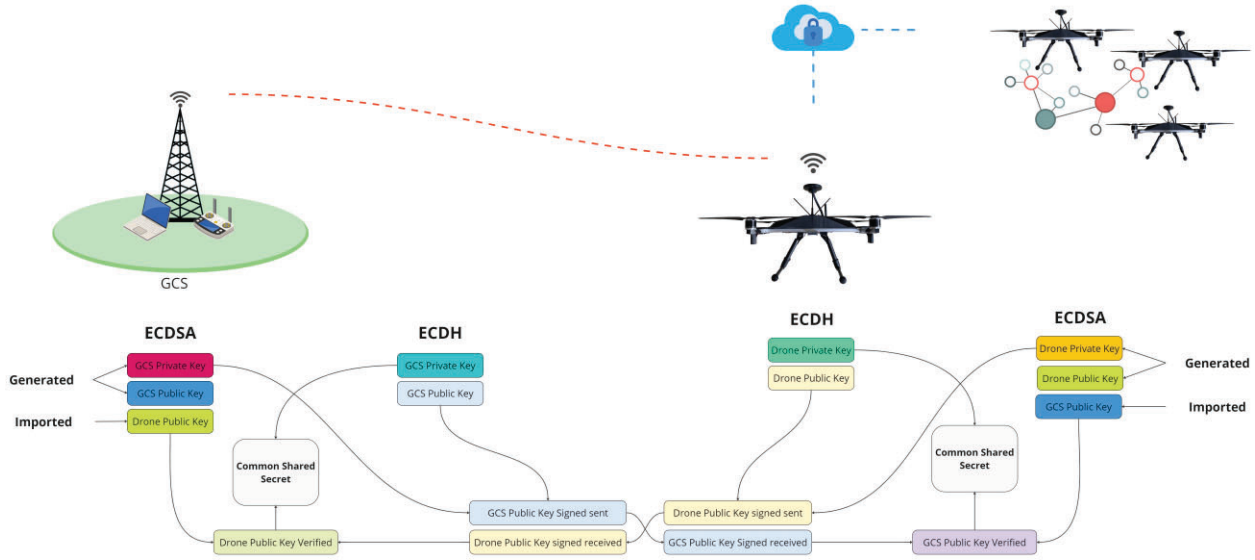

Figure 1: Initialization and encryption key exchange process for a secure communication session