Enhancing UAV Data Security Using Lightweight Cryptography Module

Szymon Baliński, Paweł Śniatała, Maciej Sobieraj
Poznan University of Technology
Poznan, Poland
szymon.balinski@put.poznan.pl

Junfei Xie
San Diego State University
San Diego, USA
jxie4@sdsu.edu

I. Introduction

UAVs are becoming widely available and are used in many fields, ranging from military and commercial applications to hobbyist use. At the same time, depending on the application, an appropriate level of data security is required. In military applications, we use advanced encrypted communication channels with the highest level of security, such as Advanced Encryption Standard (AES) and military protocols. Commercial drones require varying levels of security depending on their specific applications. The article presents an implementation of the lightweight cryptography module dedicated to secure Unmanned Aerial Vehicle (UAV) or IoT data transmission and/or storage. The ASCON algorithm was implemented on the ESP32 microcontroller platform. The system is built on the ESP32 module integrated with the camera and is ready for installation on the UAV platform.

II. Selection of Hardware Platform and Encryption Algorithm

A. ESP32 module

Given the analysis of the literature and the need for computing power and energy savings through a particular microcontroller, the authors chose to use ESP32-S3 microcontroller as hardware platforms used to encrypt data transmission in UAVs. The built-inWi-Fi and Bluetooth modules with efficient energy consumption make this microcontroller ideal for application on UAV platforms or more general IoT projects.

III. Encryption Module Implementation

Given the design constraints of the encryption device installed on the drone, implementing an encryption algorithm from the Lightweight Cryptography class is the obvious choice. When choosing a specific algorithm, there are many criteria to consider. Key criteria include: security, performance, resource consumption, implementation complexity, resistance to side-channel attacks, licensing and intellectual property, compliance with standards, scalability and flexibility, implementation experience. Taking these criteria into account, the ASCON algorithm was chosen. In 2023, the National Institute of Standards and Technology (NIST) announced the selection of the ASCON family of algorithms to provide efficient cryptographic solutions for resource-constrained devices. As mentioned above, the developed module is designed for use on small UAV platforms. As shown in Fig. 1, it can be used in various contexts. It can be applied to encrypt data transmitted between drones, for example, in an airborne network configuration, as well as for secure encrypted data transmission from the drone to the ground, where the data are stored in a secure format. Finally, an authorized operator may decrypt and read the data.

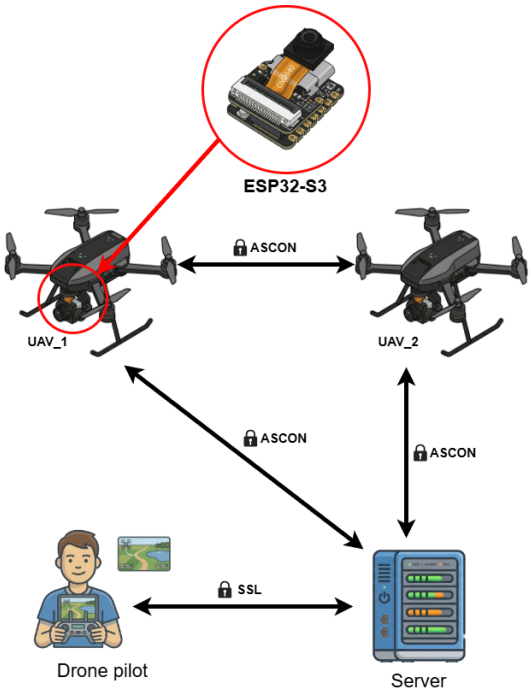

Fig. 1. Example application of the elaborated module.

The firmware running on the XIAO ESP32-S3 Sense platform is responsible for image capture, payload encryption, and continuous transmission to the receiving server over a TCP connection maintained within the local Wi-Fi network. Upon initialization, the module establishes a Wi-Fi connection in station mode and opens a persistent TCP socket to the designated server address.

Acknowledgements

This work was supported by Grant NAWA/NSF: Impress-U, ID BPN/NSF/2023/1/00005 and NSF CAREER-2048266, “Towards Networked Airborne Computing in Uncertain Airspace: A Control and Networking Facilitated Distributed Computing Framework”.