Ensuring a Secure Communication between a GCS and a UAV via the MAVlink protocol

Pavlo Mykytyn[1,2], Ievgen Kabin[1], Zoya Dyka[1]
and Peter Langendörfer[1,2]

{mykytyn, kabin, dyka, langendoerfer}@ihp-microelectronics.com

[1]IHP - Leibniz-Institut für innovative Mikroelektronik
Frankfurt (Oder), Germany

[2]BTU Cottbus-Senftenberg
Cottbus, Germany

33rd Crypto Day, 17th of September 2021

In the last years, the use of Unmanned Aerial Vehicles (UAVs) also known as drones for private and commercial purposes went up significantly. Modern UAVs are very adaptable, require low maintenance and have low operational costs. However, autonomous UAVs are still an emerging and developing technology. Any UAV, including a group of autonomous UAVs, has to be connected via a radio (telemetry) link to the Ground Control Station (GCS) to be guided remotely by an operator or by a preprogrammed mission path.

In order to establish a connection between UAVs and GCS, a standardized communication protocol called MAVlink (Micro Air Vehicle Link) [1] is widely used. It is an open source lightweight communication protocol designed for fast and simple communication between the GCS and an autonomously operated vehicle. When the protocol was designed and first released in 2009 as MAVlink v1.0, it did not include any security features, meaning that the messages were sent over the air as plaintext. Considering that the protocol has become an unofficial standard for the communication between a GCS and a UAV and is supported by the popular autopilot systems like PX4 [2] and Ardupilot [3], in 2017 MAVlink v2.0 was released, which included a message signing feature to provide data authenticity and integrity. However, the message confidentiality is not provided, i.e. the sensitive information such as mission plans or GPS coordinates of UAVs can be intercepted by an attacker, putting the whole mission and safety of the UAV at risk.

To avoid such risks and ensure data confidentiality we propose to integrate a fast and lightweight encryption algorithm based on Vernam XOR Cipher [4]. The proposed encryption method, combined with the MAVlink v2.0 message signing feature, provide data confidentiality, authenticity and integrity. The proposed encryption can be achieved by a slight modification of the communication protocol and will result in low computational overhead.

References

[1] MAVlink. - micro air vehicle link. `https://mavlink.io/en/`. [Online; accessed 18-August-2021].

[2] PX4. - open source autopilot system. `https://px4.io/`. [Online; accessed 18-August-2021].

[3] Ardupilot. - autopilot system. `https://ardupilot.org/ardupilot/index.html`. [Online; accessed 18-August-2021].

[4] Gilbert S Vernam. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the AIEE*, 45(2):109–115, 1926.