Remote Attacks on UAV based MAVlink Protocol & disruption of their operation

Based on [Micro Air Vehicle Link (MAVlink) in a Nutshell: A Survey](https://www.readcube.com/articles/10.1109%2Faccess.2019.2924410)

**[Abstract]** Until about a decade ago, UAV's were the domain of military and security officials alongside event photographers. However, recently they become a fertile ground for annoying elements who photograph other people's balconies without permission, and terrorist elements which use them to send explosives in the air.

Either way, the use of drones is expanding more and more, and there is a growing need to take over drones while they are in the air, immediately, usually for security reasons. We'll focus UAV's based on The Micro Air Vehicle Communication Protocol (MAVLink Protocol) which used for bidirectional communications between the drone and the base station, and according to open sources information, it will soon become a worldwide standard protocol. Our goal is to examine and search for vulnerabilities in favor of possible attacks and also ways of defense and countermeasures from them.

**[Introduction]** MAVLink is a communication protocol for UAV systems, which specifies a comprehensive set of messages exchanged between unmanned systems and ground stations (GCS). The protocol is used in major autopilot systems, mainly ArduPilot and PX4. MAVLink is designed as a Marshaling library (translating a data structure or object state into a format that can be stored), which means that it serializes messages of the states of the system and the commands that it has to execute into a specific binary format.

The binary serialization nature of the MAVLink protocol makes it lightweight as it has minimal overhead as compared to other serialization techniques such as XML or JSON.