Project Preview

**Why does MAVLink need to be encrypted?**

**Is there any precedence for MAVLink encryption?**

* Yes, a paper published in 2019 tackled this same issue. It can be found [here](https://doi.org/10.48550/arXiv.1905.00265).

MAVLink Basics - What is it?

**MAVLink is a Serial Protocol**

* Serial communication is the process of sending data one bit at a time in a series of bits.

**MAVLink Uses A Hybrid Pattern**

* MAVLink is structured both as a publish-subscribe and point-to-point interface. Publish-subscribe means that one end (typically the base) acts as a publisher that sends predictable patterns of information to a subscriber (typically the remote device). Point-to-point just means that communication is happening between two points (devices).

MAVLink Protocol Deep-Dive

**Message Structure (MAVLink 2)**

Messages sent over MAVLink follow a specific pattern outlined [here](https://mavlink.io/en/guide/serialization.html).

In specific, the protocol's packets follow the pattern below, in order.

* Packet Start Marker: A marker that identifies the start of a new packet.
* Packet Length
* Incompatibility Flags
* Compatibility Flags
* Packet Sequence Number: Detects packet loss with incrementing sequence numbers.
* System ID (Sender): ID of the vehicle sending the packet. 0 is reserved for the source address.
* Component ID (Sender): ID of the component (camera, gps, etc.).
* Message ID
* Payload
* Checksum
* Signature: Optional signature to verify that the packet hasn't been tampered with.

Potential Attacks

**Eavesdropping**

* If the MAVLink protocol is to be used to transmit sensitive data, it will be important to encrypt the payload to avoid eavesdropping attacks. An encrypted payload means that only a ground station with the encryption key can decode the payload.

**Man In The Middle (MITM)**

* A bad actor may intercept a MAVLink message, change its contents, and send it on to its location. Typical MAVLink messages are vulnerable to this attack. The signing method explained in “Potential Solutions” below.

**Replay**

* A replay attack occurs when a bad actor records a signal sent from one party to another and replays it at a later time. This could be used to move or crash the drone, or replay past messages from the drone to the ground station.

Potential Solutions

**MAVLink2 Signing**

* MAVLink2 has built-in encryption which is used to verify that the message being received came from the right ground station. It doesn't encrypt any of the message data, but simply tells the drone whether or not it should act on the data. More information can be found [here](https://ardupilot.org/planner/docs/common-MAVLink2-signing.html).

**Whole Message Encryption**

* If the entire message is encrypted, it would prevent bad actors from any of the previous attacks. This will, however, have considerable overhead.