Sniffing and Spoofing of UAV C2 messages

Babak Badnava

Presented as a final project for EECS 866

December 2022

Overview

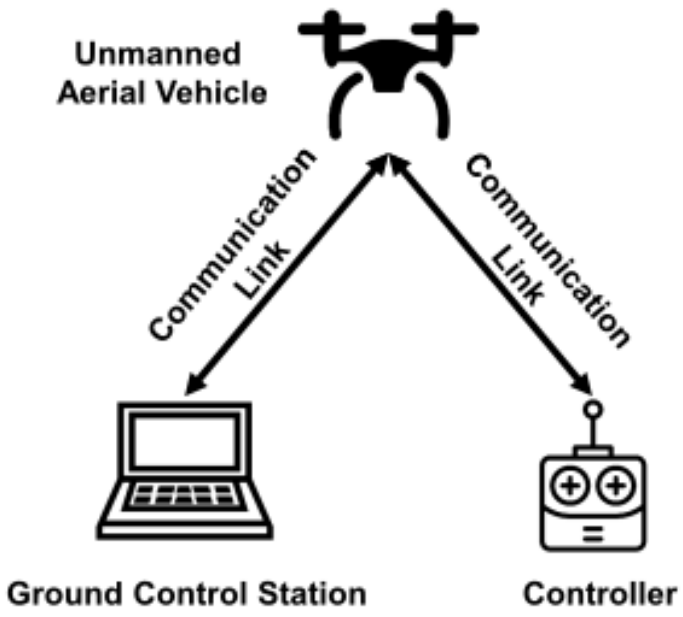
- Introduction
- Communication models for UAVs
- Potential threats to UAV systems
- Attack model and implementation
- Mitigations

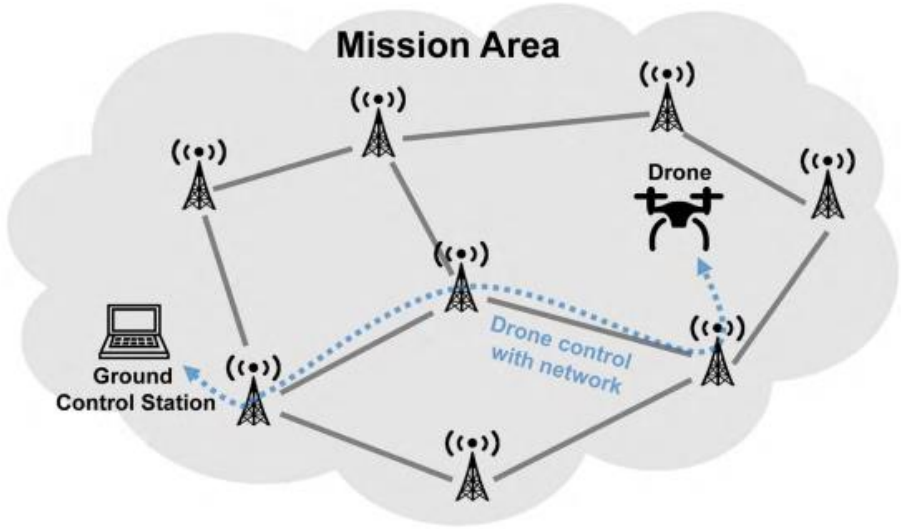
Unmanned Aerial Vehicles (UAVs)

- Use cases:
  - Mapping and surveying
  - Aerial photography and videography
  - Search and rescue
  - Military
  - Entertainment
  - …
- Secure communication is critical

Communication models for UAVs

- Direct command and control (C2) link
  - Bluetooth
  - WiFi
  - LoRa
- C2 link over the network
  - Cellular
  - Satellite



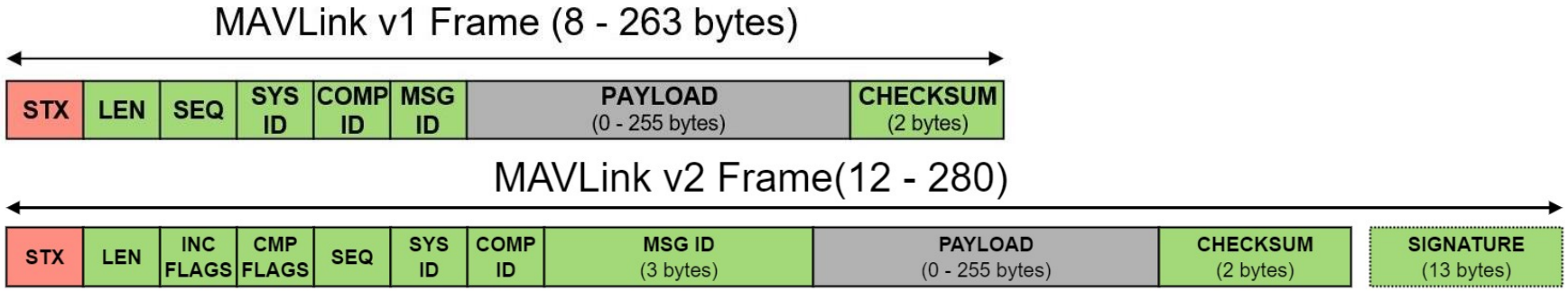


Images taken from [1]

Communication protocol

Image taken from [3]

- MAVLink
  - A message-based UAV communication protocol
  - One of the most widely used protocols for drone control.
    - Ardupilot and PX4
- Vulnerabilities
  - No message encryption is incorporated to improve efficiency
  - Transparent message frames and message



Images taken from https://mavlink.io/en/guide/serialization.html

Potential threats to UAV systems

- Denial of service
- Eavesdropping
- Packet injection/Hijacking
- Jamming
- ICMP Flooding

Security objective	System objective	Attack method
Confidentiality	GCS	Virus
		Malware
		Keyloggers
		Trojans
	UAV	Hijacking
	Communication Link	Eavesdropping
		Man-in-the-middle
Integrity	Communication Link	Packet injection
		Replay attack
		Man-in-the-middle
		Message deletion
Availability	GCS	Denial of service
	UAV	Fuzzing
	Communication Link	Jamming
		Flooding
		Buffer overflow

Image taken from [1]

Attack model

- A man in the middle
  - By attacking GCS and/or drone can harm the drone
- Sniff packets that is being sent to either GCS or the drone

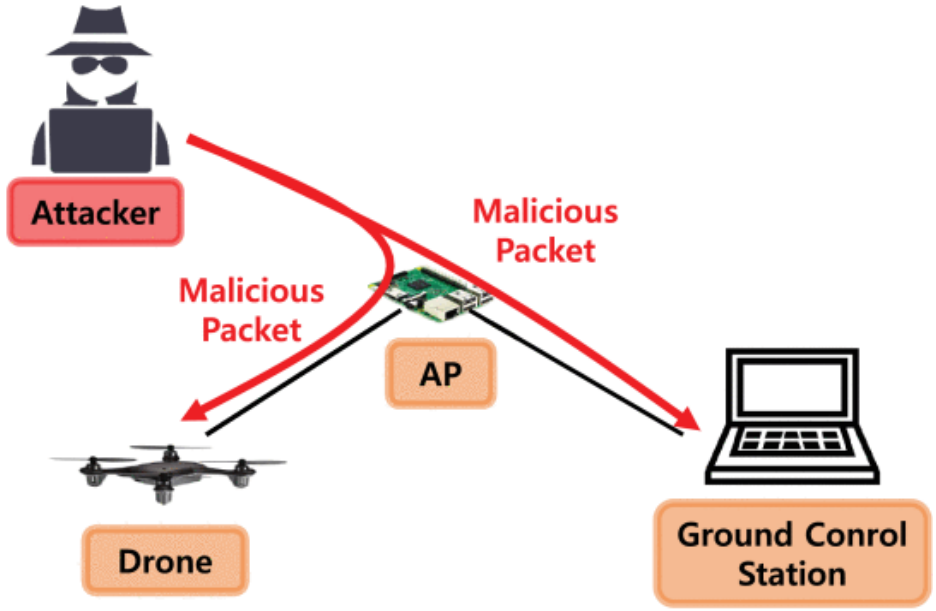


Image taken from [1]

Attack implementation

- GCS: a mission planner or a python code to control the UAV
- Drone: simulated using Ardupilot simulation in the loop (SITL)
- Wireshark or python code to sniff the packets sent to/from drone

Parsing MAVLink messages in Wireshark

- Need to generate MAVLink Lua plugin for Wireshark
  - Specify MAVLink protocol version
  - Mavlink message description file
- Load the plugin in the Wireshark and capture the ongoing traffic

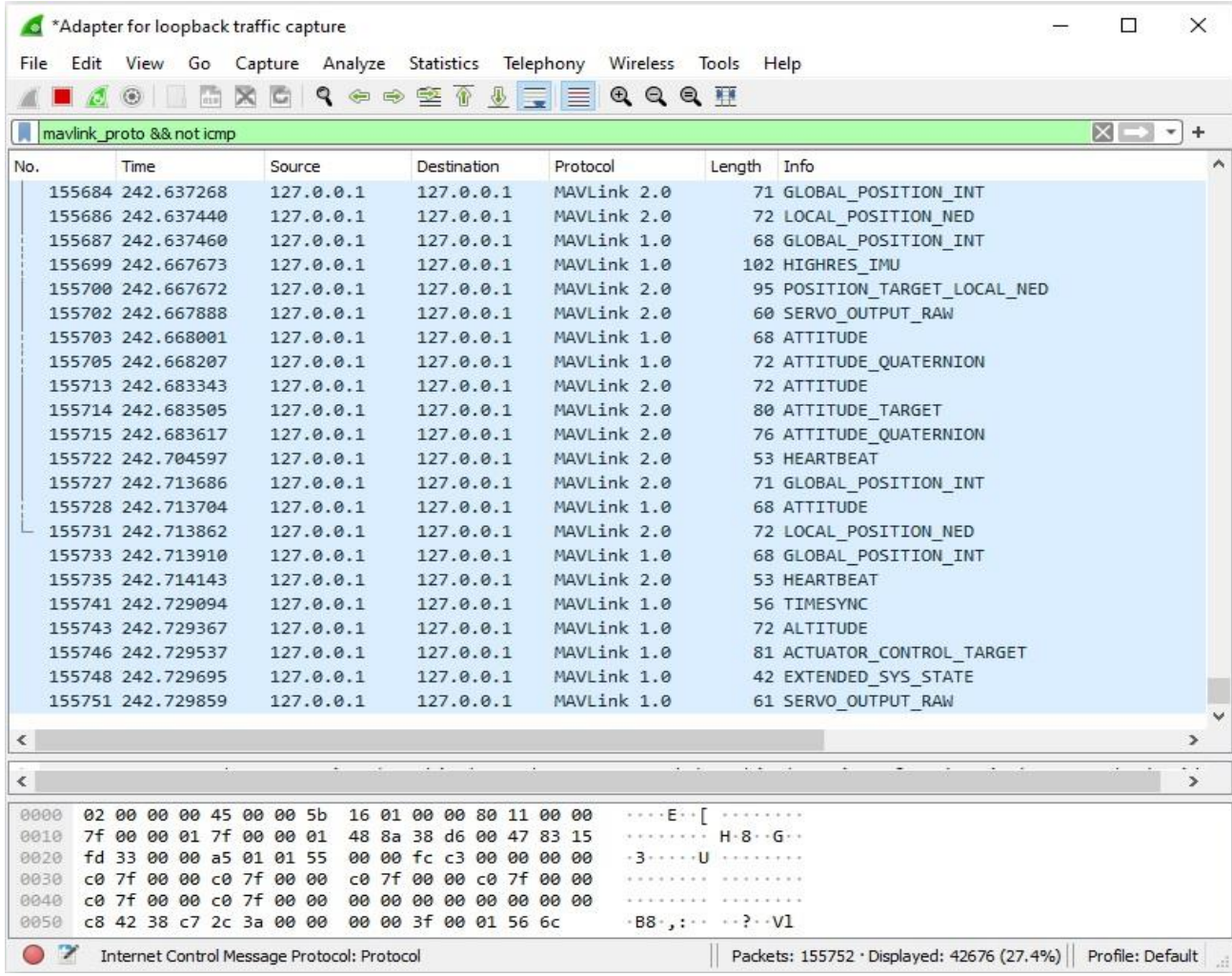


Image taken from: https://mavlink.io/en/guide/wireshark.html

Securing MAVLink Protocol

- Confidentiality of the exchanged messages between UAVs and GCSs can be guaranteed by encryption [3]
  - Advanced Encryption Standard in Counter Mode (AES-CTR)
  - Advanced Encryption Standard in Cipher Block Chaining Mode (AES-CBC)
  - RC4
  - CHaCha20
- Encryption process
  - MAVLink Identifier ID cannot be encrypted
  - Encrypt the message payload
- Other than RC4, the rest would not introduce a huge CPU, memory, and time overload compared to unencrypted MAVLink messages

Securing MAVLink Protocol

- But can we really guarantee confidentiality by encrypting only the payload data?
  - MAVLink has a finite set of messages, some of them have no arguments or payload data
  - Could dictionary attack be possible in this case?

Refrences

- [1] Y. -M. Kwon, J. Yu, B. -M. Cho, Y. Eun and K. -J. Park, "Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles," in IEEE Access, vol. 6, pp. 43203-43212, 2018, doi: 10.1109/ACCESS.2018.2863237.
- [2] H. Xu et al., "Experimental Analysis of MAVLink Protocol Vulnerability on UAVs Security Experiment Platform," 2021 3rd International Conference on Industrial Artificial Intelligence (IAI), 2021, pp. 1-6, doi: 10.1109/IAI53119.2021.9619330.
- [3] A. Allouch, O. Cheikhrouhou, A. Koubâa, M. Khalgui and T. Abbes, "MAVSec: Securing the MAVLink Protocol for Ardupilot/PX4 Unmanned Aerial Systems," 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), 2019, pp. 621-628, doi: 10.1109/IWCMC.2019.8766667.