Cybersecurity Threats and Defense Mechanisms in Communication link of Unmanned Aerial Vehicles

Kamil Aghayev[1], Farhad Yusifov[2]
[1]Azerbaijan State Oil and Industry University, Baku, Azerbaijan
[2]Institute of Information Technology, Baku, Azerbaijan
[1]*kamil03agayev@gmail.com*, [2]*farhadyusifov@gmail.com*

***Abstract*— In the 21st century, the rapid development of Unmanned Aerial Vehicles (UAVs) has changed them into critical components for infrastructure, logistics, and national security. However, secure communication standards have lagged behind, leaving the aircraft-Ground Control System link vulnerable to cyber-physical attacks. This thesis focuses on the necessity of implementing complex defense mechanisms to provide robust protection against RF Jamming, GNSS spoofing, and Man-in-the-Middle attacks. At the communication link layer, this research dissects the MAVLink protocol to expose the structural vulnerabilities. These results highlight a structural trade-off: highly secure communication can be reached using integration of fundamental cryptographic safeguards.**

Keywords*— *MAVLink, UAV, GPS Spoofing, MitM attack, RF Jamming.

I. INTRODUCTİON

Unlike traditional networks, which are protected by physical perimeters, UAV communication works entirely on the open radio frequency range, which creates an enormous attack surface. By exploiting the physics of the signal, an attacker can manipulate transmitted signals and take control of the UAV. These threats demonstrate the urgent need for developing robust defense methods to ensure the security and integrity. By securing a communication link, it's also important to keep a minimal timeout for encrypting and decrypting transmitted packets, which directly affects the latency between the UAV and the Ground Control System. With them, the communication protocol must also be implementable in mass production. In addition to minimizing latency, the mitigation defense mechanisms should be adaptable to various UAV models and protocols. Research by Butun et al. [1] found that approximately 95% of active commercial UAV deployments use the MAVLink protocol without strict requirement signing enabled. These counts are the best surface for unauthorized command injection using basic, low-cost Software-Defined Radios (SDRs) by a malicious attacker. As proposed by Humphreys [2], over 82% of commercial-level GNSS modules are unable to detect spoofed satellite signals.

During that period, the UAV accepts misleading coordinates and time. Based on the findings of Nesterova et al [3], a narrowband jamming from a 1Watt source can terminate 100% communication link in a 500-meter range at 2.4Ghz using a $50 jammer. These statistics show a critical threshold cost for the effective disruption of the communication of the majority of drones.

II. UAV-GCS ARCHİTECTURE AND MAVLİNK PROTOCOL

The operational reliability of an Unmanned Aerial Vehicle is entirely dependent on the stability of its communication link with the Ground Control System. This architecture is composed of two data streams: the Uplink and the Downlink. Uplink data stream provides transmitting data for controlling UAV position and features and downloading a data stream used for transmitting telemetry data, such as coordinates, speed, altitude, etc., of the UAV. Depending on the UAV, there can be video downloading for stress-free real-time video translation. UAV-GSC architecture consists of 3 components as depicted in Fig 1 [4]. Unmanned Aerial Vehicles are aircraft that operate without an onboard human pilot and are controlled remotely by a ground control system. It consists of a flight controller (ArduPilot, STM32f405, or PX4), a GPS module (GPS, GLONASS, Galileo), Sensors (Accelerometer, Gyroscope, Barometer, etc.), an RF receiver, a video transmitter, and telemetry devices.

The ground control system controls the UAV and exchanges data with it in real time. GCS combines Telemetry and video receiver modules, and an RF transmitter. Software for GCS can be used, such as Mission Planner and QGroundControl. An RF datalink operating at 433/900 MHz is used to transmit telemetry data between the GCS and the UAV. The maximum distance in this frequency is maximum (up to 5-50km), but the latency is high (approximately 20-200ms). The operator uses the 2.4 GHz RC to control the UAV from the GCS. It operates over a medium distance (0.5-15km deepened by the transmitter power), and latency is minimal (5-20ms). Video Downlink 5.8GHz - is a critical component of the UAV communication system, used for transmitting visual data from the camera on the UAV to the GCS in real-time. The maximum distance is about (0.5-5km). Video downlink is fundamentally divided into analog and digital transmission systems.

Each version has its own advantages and disadvantages in terms of latency, distance, and video quality. Data packets in

DOI: 10.25045/forensic.gov.2026.63

the MAVLink protocol consist of bytes, each with its own purpose as shown in Table 1 [5, 6].

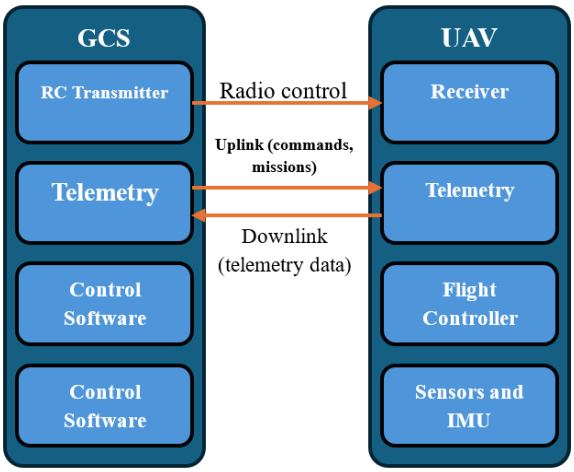

Figure 1. UAV-GCS architecture elements

TABLEL I. MAVLINK PACKET CONTAINING BYTES DESCRIPTION

Byte	Acronym	Description
0	**STX**	Indicates the start of a packet. For MAVLink 1, it's 0xFE; for MAVLink 2, it's 0xFD.
1	**LEN**	Length of data
2	**INC**	It's a flag used to check whether a packet is signed.
3	**CMP**	Optional packet features that a receiver could ignore if not recognized, ensuring that a new protocol version does not break communication with older protocols
4	**SEQ**	For the following sequence of packets used to detect lost packets.
5	**SYS**	Determines the unique ID of the device, such as UAV1, UAV2, etc.
6	**COMP**	ID of an internal component, such as a camera or sensor.
7-9	**MSG**	Message ID. It determines the type of message, such as Altitude or Longitude.
10+	**DATA**	Payload (send packets)
+2	**CRC**	For verifying damaged packets during transmission
+13	**SIG**	An optional security feature for verifying message authenticity.

Weaknesses of the MAVLink protocol:

- While sending, do not use encryption; send as plain text.
- CRC byte checks only payload length, not security.
- There is no checking of the authentication of the pocket sender (optional signing in MAVLink 2, which is not commonly used)
- Vulnerable to replay attacks and to unauthorized packet injection.

III. CYBERSECURİTY THREATS İN UAV GROUND CONTROL SYSTEMS

During navigation, UAVs use GPS signals broadcast by satellites. Using precise distance calculations between each satellite, it detects the exact coordinates on Earth. Furthermore, the GNSS signals are not encrypted and are not authenticated by the receiver. Consider a scenario where the attacker injects fake, generated GPS signals, and the UAV receives them as normal GNSS signals. As a result, the UAV gets confused by real and injected GNSS signals, as shown in Picture 1. To mitigate GPS spoofing, GNSS data can be fused with IMU and other onboard sensor measurements. For instance, a rapid change in coordinate position that is not corroborated by corresponding motion measurements from the IMU may indicate potential GPS spoofing. The other way of preventing GPS spoofing is by monitoring fast-changing GNSS signal levels in a short time. RF Jamming is a technique used to attenuate or intercept RF signals between the UAV and GCS. The primary purpose of this is to inject signals into the communication link. Key classifications of RF Jamming:

- as Wideband noise injection - refers to the injection of randomly selected bits into communication links. In the basic variants, it could be done using random injection of analog signals

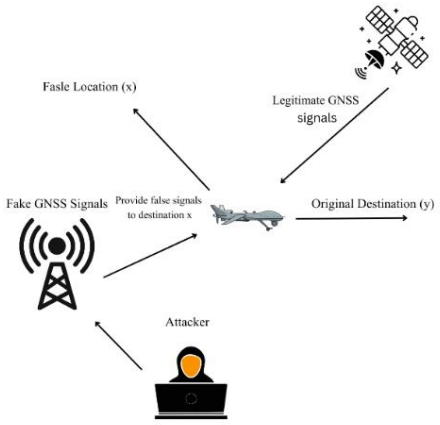

Figure 2. GPS Spoofing scheme

- Frequency Oscillation - is characterized by injections across various frequencies, which appear to be noisily affecting all bands.
- Narrowband spot signaling - denotes a technique where the attacker injects noise signals in a narrow range of frequencies, which is used for communication with the UAV
- Dynamic Frequency-based tracking is a jamming method where the attacker analyzes the victim's signals and immediately switches to the same frequency and injects malicious or noise signals into the communication link.
- Protocol-aware Injection is an advanced jamming type where the attacker understands the communication protocol logic and injects packets that are received from the UAV as a valid message [7].

In the preceding chapters, we examined RF Jamming and GPS Spoofing, which pose significant threats to the operational availability of UAVs. However, an equally hazardous attack

method is the MitM attack (Man-in-the-Middle). In this attack, the attacker sits between the GCS and the UAV. Unlike brute-force jamming, MitM attacks target the communication layer, manipulate communication channels, and either understand the communication protocol, gain unauthorized control, or modify telemetry. MitM attacks are divided into passive and active methodologies. In a passive MitM attack, the adversary monitors the communication link and intercepts transmitted packets without modifying them primarily to understand the parsing logic. Unlike the previous method, an active attack poses a critical threat to communication between the GCS and the UAV. In this methodology, the adversary moves beyond passive listening, modifying packets before they reach their destination and injecting its own packets.

IV. Cyber-Physical Defense Mechanisms For UAV Ground Control Systems

One of the most effective defense methods against GPS spoofing is synchronizing GNSS data with internal sensors such as a gyroscope, accelerometer, magnetometer, and barometer. By using these measurements, the UAV can detect GPS spoofing. If GNSS coordinates jump rapidly and do not align with measurement values, it could indicate a potential spoofing threat. Direction-of-Arrival is the process of calculating the specific angles (azimuth and elevation) of satellites. In other words, it detects where the signals are coming from; for this purpose, it uses multi-antenna filtering. When a signal hits multiple elements of an antenna, it reaches them at different times, and when the antenna receives these signals, it calculates the phase differences and can determine their angles. When an adversary injects its spoofed signals, it comes from one source, and the system detects the fault. Encrypted GNSS signals exhibit one of the strongest defenses against GPS spoofing. Here, cryptographic methods are used for the encryption of GNSS data to ensure the origin of these signals. Most known systems, such as GPS L1 C/A, GLONASS L1OF, and BeiDou B1I, are not encrypted and are all open and unauthenticated. But military Encrypted signals, such as GPS P(Y)-code, GLONASS L1SA, are secure encrypted, and to ensure they come from the originating satellite, they use a secret key, which means if an attacker doesn't know the secret key, he cannot generate spoofing signals in the correct structure [8]. Spread Spectrum Communication is a method where the UAV and GCS rapidly switch to randomly selected frequencies shared between them. It makes communication harder to jam by altering the data channel. Multi-channel redundancy. In this technique, the receiver and transmitter communicate on multiple independent frequencies, such as 900 MHz and 2.4 GHz. As a result, even if one channel is jammed, communication still does not terminate. This method requires more complex jamming equipment to terminate all channels at once - jammer detection and Autonomous failsafe behavior. UAVs can detect jamming by monitoring the communication link and increasing the power of signals caught by the antenna. When RF Jamming is detected, the UAV enters Return-to-Home, autonomous navigation, or switches to a backup communication link such as LTE/5G, LoRa. End-to-End Encryption (E2EE) and Mutual Authentication are the most robust methods against MitM attacks. Traditional communication links are often encrypted, whereas the application layer is not. E2EE ensures that data is encrypted by secret keys for secure communication between the UAV and the GCS. Mutual Authentication is a "zero-trust" method where nodes for verifying each other use digital certificates before establishing a link.

Conclusion

Across all referenced works, a common theme emerges: availability and performance were historically prioritized over security in UAV communication protocol design. So, attackers could exploit these vulnerabilities for their malicious purposes. In summary, this research confirms that there is a demand for rapidly developing cybersecurity mechanisms; UAV communication security still faces cyber-physical threats over communication links, such as RF Jamming, GNSS spoofing, and man-in-the-middle attacks, which can be done using low-cost (Software-Defined-Radio) SDRs [8, 9]. Given these vulnerabilities, there is a clear need for security design principles and multi-layer security methods. In addition, standardization of communication protocols should accept minimum security requirements, due to UAVs being implemented in commercial and high-risk applications.

References

[1] I. Butun et al., "Security Analysis of MAVLink Protocol for Unmanned Aerial Vehicles," IEEE Access, 2022.

[2] T. E. Humphreys, "The Vulnerability of Unmanned Aerial Vehicles to GPS Spoofing," The University of Texas at Austin, 2021.

[3] N. Nesterova et al., "Experimental Evaluation of RF Jamming Impact on UAV Communication Links," Sensors, MDPI, 2021.

[4] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," ACM Trans. Cyber-Phys. Syst., vol. 1, no. 2, pp. 1–25, Nov. 2016, doi: 10.1145/3001836.

[5] M. A. Hamza, M. Mohsin, M. Khalil, and S. M. K. A. Kazmi, "MAVLink protocol: A survey of security threats and countermeasures," Proc. 4th Int. Conf. Digital Futures and Transformative Technologies (ICoDT2), Oct. 2024, doi: 10.1109/ICoDT262145.2024.10740195.

[6] M. Ficco, R. Palmiero, M. Rak, and D. Granata, "MAVLink protocol for unmanned aerial vehicle: Vulnerabilities analysis," in Proc. 2022 IEEE DASC/PiCom/CBDCom/CyberSciTech, Falerna, Italy, Sep. 2022, doi: 10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927895

[7] Y. Zidane, J. S. Silva, and G. Tavares, "Jamming and spoofing techniques for drone neutralization: An experimental study," Drones, vol. 8, no. 12, Art. no. 743, Dec. 2024, doi: 10.3390/drones8120743.

[8] K. Pärlin, M. M. Alam, and Y. Le Moullec, "Jamming of UAV remote control systems using software-defined radio," in Proc. 2018 Int. Conf. Military Communications and Information Systems (ICMCIS), Warsaw, Poland, May 2018, doi: 10.1109/ICMCIS.2018.8398711.

[9] B. Branco, J. S. S. Silva, and M. Correia, "Cyber-attacks on commercial drones: A review," IEEE Access, 2025, Doi: 10.1109/ACCESS.2025.3527698.