Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 25, MARCH 2026

DOI: **10.37943/25GEVU5826**

Gulzhamal Tursunbayeva
PhD student, Department of Information Security
g.tursunbaeva@enu.kz, orcid.org/0000-0002-2044-8027
L.N. Gumilyov Eurasian National University, Kazakhstan
Gani Sergazin
PhD, Associate Professor, Department of Automation and Control
g.balbayev@gmail.com, orcid.org/0000-0003-2762-473X
ALT University named after M. Tynyshpayev, Kazakhstan
Dina Satybaldina
Candidate of Physical and Mathematical Sciences, Professor,
Head of Research Institute of Information Security and Cryptology
satybaldina_dzh@enu.kz, orcid.org/0000-0003-0291-4685
L.N. Gumilyov Eurasian National University, Kazakhstan
Nawras Al Bukhari
Master student, Department of Computer Engineering
nawrasalbukhari@gmail.com, orcid.org/0009-0008-3682-2029
Almaty Technological University, Kazakhstan
Arman Uzbekbayev
PhD Student, Department of Aerospace and Electronic Engineering
niipntkz@gmail.com, orcid.org/0009-0003-6728-0748
Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, Kazakhstan
Abu-Alim Ayazbay,
PhD, Senior Lecturer, Department of Aerospace and Electronic Engineering
work_abu@hotmail.com, orcid.org/0000-0002-5941-3462
Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, Kazakhstan

DEVELOPMENT AND VERIFICATION OF CYBER SECURITY ARCHITECTURE FOR UNMANNED AERIAL VEHICLE TELEMETRY BASED ON SIMULATION MODELLING

Abstract: The rapid development and widespread adoption of unmanned technologies have led to significant advancements across various fields of human activity. At the same time, the risks associated with the unauthorized use of unmanned aerial systems have increased. This has led to the emergence of a distinct area of research focused on countermeasures and the protection of various components and platforms within unmanned aerial systems. Despite the existence of current methods for detecting attacks and anomalies, their effectiveness is significantly reduced under complex operational scenarios, including dynamically changing environments, interference, small target sizes, and low radar visibility. To address this issue, this study presents the main findings of a comprehensive analysis of contemporary cyber threats and vulnerabilities arising in unmanned aerial vehicle (UAV) systems. Based on this analysis, an up-to-date classification of existing types of attacks on the basic architecture of UAVs has been compiled. This enabled an examination of the main protection methods for ensuring the security of UAV systems and components, as well as the classification of methods for detecting cyberattacks on their systems. Based on the data obtained, a multi-level protection architecture was developed, comprising three main levels: a secure communication channel, a secure flight controller, and a secure ground control station.

The software environment developed for simulating telemetry streams in Python 3.12 enabled the generation of packets in Micro Air Vehicle Link (MAVLink)/ User Datagram Protocol (UDP)/ Transmission Control Protocol (TCP) format, as well as the simulation of attacks and the detection of network anomalies in the UAV telemetry system. The results obtained include the processing of 97 MAVLink packets, where the proportion of anomaly injections was 10%, totalling 118 units. The average MAVLink packet delay was 0.037 seconds, which indicates stable operation of the telemetry channel. Experimental verification comprising 100

Received: 04.02.2026 Accepted: 25.02.2026 Published: 30.03.2026

DOI: 10.37943/25GEVU5826

cycles demonstrated the ability to detect data packet structure violations, false identifiers, coordinate substitution, and delay anomalies.

Keywords: unmanned aerial vehicles; telemetry channel; Unmanned Aerial Vehicle cyber defence; anomaly detection; Micro Air Vehicle Link; statistical analysis of telemetry; communication channel protection; cyber resilience; telemetry modelling; multi-layered defence architecture.

Introduction

Today, the widespread use of unmanned aerial vehicles (UAVs) for commercial, civil, and military purposes has significantly increased the need for the security of their systems, mechanisms, and components [1]. Given that they are increasingly used to perform a wide variety of tasks, ranging from infrastructure inspection, aerial photography, environmental monitoring, and remote sensing to the delivery of parcels to hard-to-reach locations, they are extremely vulnerable to cyber-attacks. These threats can disrupt the execution of various missions and compromise data integrity, including causing physical damage to UAVs [2]. As the scale and complexity of tasks and missions across various sectors expand, the growing reliance on digital platforms and systems exposes them to a wide range of cybersecurity threats.

The operational integrity of a UAV platform depends directly on the security of its core subsystems, such as telemetry links, command and control channels, Global Navigation Satellite System (GNSS), and Global Positioning System (GPS) based navigation, remote identification mechanisms, and cloud-based monitoring and data storage services [3]. A basic block diagram of the UAV's core architecture, showing its main components, is presented in Figure 1.

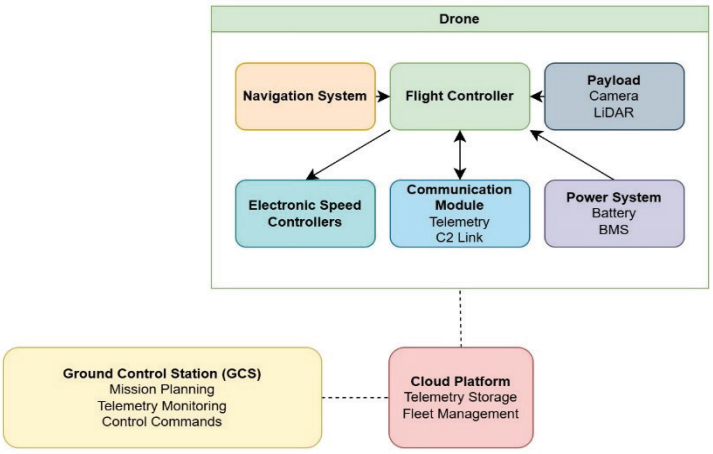


Figure 1. Basic UAV architecture

The block diagram of basic UAV architecture consists of three main components:

1. The UAV's onboard segment ensures the UAV's autonomous operation in the airspace. In this block, automatic control algorithms are implemented directly within the Flight Controller subsystem, whilst the Navigation System subsystem is used to determine the UAV's position, speed, and altitude. The transmission of telemetry data and the reception of control commands via a specified channel are handled by the Communication Module subsystem. To carry out various missions, the UAV may be equipped with a Payload. Power is supplied to all on-board UAV components, and their stable operation is maintained in real time via the Power System subsystem.

2. The UAV ground control system enables mission planning, monitoring, and control of telemetry parameters, including command-and-control of the UAV.

3. The UAV cloud platform is designed for data processing and storage.

Communication between the UAV and the ground station is carried out via a radio channel or a cellular network using data transmission protocols. Data exchange between the UAV ground control system and the cloud platform takes place via the Internet.

A failure in the functionality of any of these components may lead to a loss of stability in UAV flight control in the airspace, a reduction in the accuracy of navigation decisions, and a complete loss of

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 25, MARCH 2026

communication with the ground station, which ultimately increases the likelihood of emergencies and creates a risk of mission failure.

Developing suitable, optimal solutions to ensure UAV safety is complicated by a number of factors [4]. The most common of these is the extremely limited computing power available on board the UAV [5]. This restricts the scope for implementing software and its components to ensure the security and integrity of transmitted data. Furthermore, ground control stations for UAVs are often simple remote-control devices that have limitations when it comes to installing additional software-based safety functions [6]. Problems associated with restrictions on the size and weight of UAVs render many hardware-based security solutions impractical. In particular, many security mechanisms developed for traditional computer systems and data transmission networks cannot be directly applied to UAVs [7]. Another major factor contributing to security breaches may be the physical seizure of UAVs, due to their increased visibility in the airspace [8]. These factors provide attackers with more opportunities to interact with UAVs to cause interference, spoof signals, and intercept data, disrupting command and control communications, potentially leading to flight suspension or unpredictable changes in the UAV's flight path.

In this field, a great deal of research has focused on classifying UAV vulnerabilities and types of attacks [9], including the development of defence methods [10]. However, existing approaches differ in their perspectives, depending on the architecture of the UAV system. Most of them demonstrate the main attack vectors targeting the flight controller, the ground control station, and the data transmission channel, including GPS spoofing, signal jamming, Denial of Service (DoS) attacks, video stream spoofing, and the injection of malicious code. Numerous studies over the past decades have focused on identifying potential vulnerabilities and classifying types of attacks based on weaknesses in UAV system architecture [11]. Generally, UAV cyber threats have been classified according to the targeted system components (flight controller, ground control station, and data transmission channel) and the attacker's capabilities (data disclosure, gaining knowledge of the system, and disrupting operations) [12]. Many vulnerabilities to attacks by malicious actors are largely related to wireless communication protocols, on-board sensors, and automated control loops [13].

Many studies have examined modern types of attacks on UAVs, with the most common types identified as GPS signal spoofing, command injection, data link jamming, or denial-of-service (DoS) attacks [14]. Consequently, failure to detect and prevent attacks on UAV components in a timely manner can lead to mission failure, breaches of confidentiality, or even physical harm. In the research of A. Zuev, O. Gryb, S. Shvets, and V. Makarov, they note a significant increase in risk in cases where UAVs operate autonomously or interact with ground-based or cloud-based control systems [15]. In the research of P. Wang et al. argue that attacks involving the jamming or spoofing of GPS signals are carried out to disable the UAV's navigation system [16]. At present, GPS signals in UAV systems are often unencrypted, which significantly simplifies the execution of such attacks; consequently, signal spoofing with false, random coordinates can cause the UAV to become disoriented and crash. In many cases, disruption to position broadcasting (analogous to ADS-B) occurs due to jamming of Ground Control Station (GCS) control signals [17]. A communication failure triggers fail-safe modes, causing the UAV to fly erratically and potentially leading to a collision, resulting in a catastrophic outcome. Signal spoofing in the telemetry and video surveillance system can mislead the operator controlling the UAV remotely [18]. There are also attacks involving the manipulation of captured video. In this case, intercepting system data to replace real video with falsified footage allows the attacker to take control. According to the research by S. Gupta et al., this attack method can be combined with GPS coordinate spoofing [19]. The injection of falsified data from the UAV's sensors is carried out via external interference or internal access to destabilize the flight mode [20]. Malicious hardware and software (Trojans, backdoors, command injections, etc.) can be introduced to steal confidential data or to deliberately disable the protection system in order to cause a failure in the UAV control system. In the research of Z. Yu and Q. Wang, authors noted the importance of timely prevention of unauthorized disclosure of UAV system communications [21]. This type of attack is carried out with the aim of unauthorized access to and leakage of personal data, and may lead to the compromise of dispatch software, the generation of incorrect tasks, routing failures, and operational disruptions. In many studies, including those by A. P. Zhao et al. [20] and Z. Yu and Q. Wang [21], a 'Denial of Service' (DoS) attack is considered one of the most common types of attacks on UAVs. In most cases, an unplanned sudden overload of the UAV's computing resources or network channels leads to a halt in operations, a reduction in performance, or the system entering an unintended operational state.

DOI: 10.37943/25GEVU5826

A general analysis of existing research in this area suggests that cyberattacks on UAVs can affect all components and subsystems of the UAV's basic architecture and are classified as shown in Figure 2.

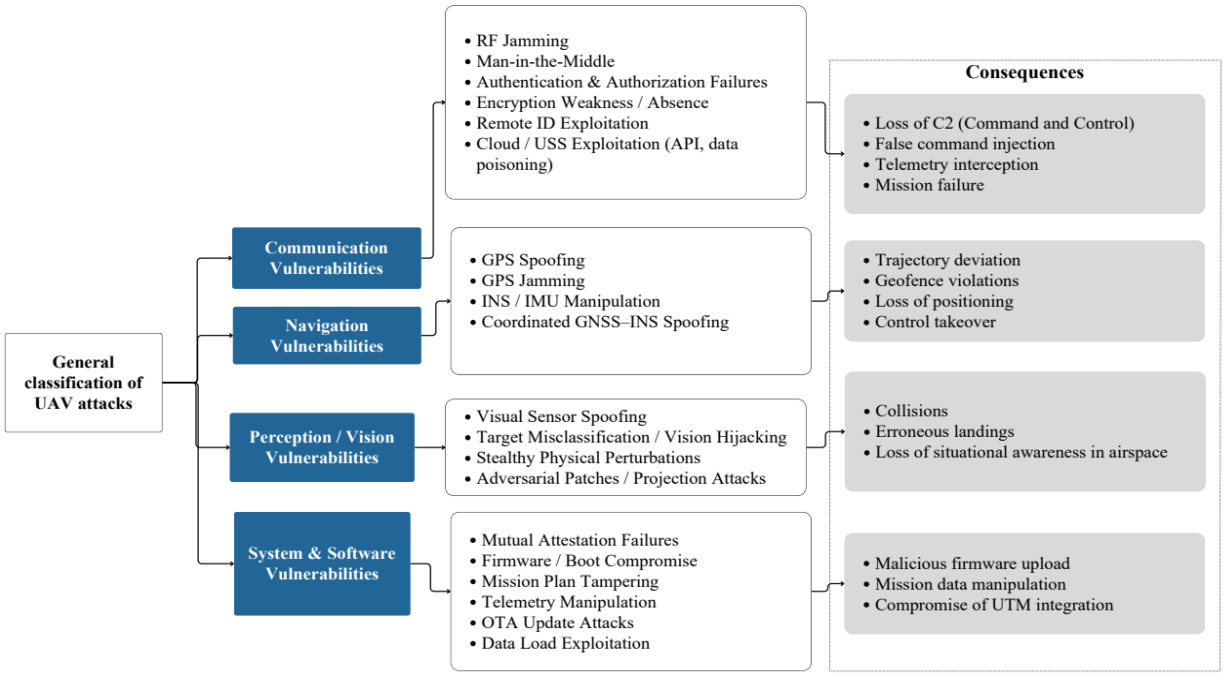


Figure 2. Main classification of existing types of attacks on the basic UAV architecture

By their very nature, UAVs are more vulnerable to attacks than manned aircraft. This is due to the absence of human intervention, including a heavy reliance on wireless communications and the presence of unprotected hardware architecture. Currently, the most common attacks target four areas: UAV sensors, communications, software, and cybersecurity. Cyberattacks on UAVs target communication channels, the navigation subsystem, the flight controller, the payload, the power system, and the ground-to-cloud infrastructure, creating a multi-layered attack surface, which highlights the need to develop appropriate solutions to ensure UAV security.

The aim of the study is to develop a conceptual model of a system for protecting UAVs against cyberattacks at the level of the communication channel, the on-board computing platform, and the ground control station, and to devise a method for detecting anomalies in the UAV's telemetry channel based on simulation modelling.

Methods and Materials

In recent years, the increasing use of UAVs has significantly heightened concerns regarding their cyber resilience. The lack of robust protection makes them more vulnerable to the exploitation of software vulnerabilities, the introduction of malware, and unauthorized modifications to the software. The development of a robust protection system and the security of its components is becoming essential to ensure its functionality when carrying out various missions [22].

To date, researchers from around the world have developed and analyzed numerous approaches and methods aimed at countering attacks on UAVs. In this regard, the research by E. Pekarčík et al. analysed various types of security threats to UAVs [23]. Demonstrating a comprehensive analysis of existing attacks by researchers, a cyber-threat model was proposed, and methods for enhancing the security of UAV components were discussed. Similar studies have also focused on the development of improved methods for communication channel encryption, protection against 'denial-of-service' (DoS) attacks, and intrusion detection systems. Some of these studies yielded interesting conclusions. Some authors argue that the timely detection of passive interception and the implementation of robust encryption protocols and secure communication channels can contribute to a significant improvement in UAV security. In their research, H. Jalil Hadi et al. focused primarily on developing an effective condition assessment method based on data obtained from intelligent sensor systems to detect attacks on UAV communication data [24]. This made it

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 25, MARCH 2026

possible to prevent the interception of confidential information transmitted via navigation commands and telemetry systems. Furthermore, to protect critical information regarding the architecture and operation of UAV networks and to ensure the safe and reliable integration of UAVs into airspace, many regulatory bodies in various countries have developed cybersecurity guidelines. After analyzing established UAV cybersecurity standards, R. S. Tucker et al. [25] concluded that the Federal Aviation Administration (FAA) regulations are designed to protect UAV communication channels from eavesdropping, jamming, and unauthorized access [26]. In this regard, a similar regulation by the European Union Aviation Safety Agency (EASA) outlines cybersecurity and data protection measures for UAV operations [27]. To protect unmanned aerial vehicle (UAV) networks from cyber threats, cryptographic methods ensuring the confidentiality, integrity, and authenticity of transmitted data, including blockchain-based identity management, are employed. In addition to the regulations, the importance of ensuring that security measures comply with the ISO/IEC 27001 cybersecurity standards is noted [28]. An analysis of existing best industry practices reveals that robust UAV cybersecurity systems are established using various methods, which are classified as shown in Table 1.

Table 1. Classification of methods for detecting cyber-attacks in UAVs

No.	Detection method	Principle of operation	Examples of application	Advantages	Limitations
1	Signature-Based	Comparison of traffic or behaviour with known attack patterns	Intrusion Detection System (IDS) according to the rules, verification of MAVLink commands	High accuracy for known attacks, low computational load	Does not detect new (zero-day) attacks
2	Anomaly-Based	Detection of deviations from the normal operating profile	Telemetry analysis, latency monitoring, packet frequency	Enables the detection of unknown attacks	False alarms are possible.
3	ML-Based	Classification of behavior based on trained models	Detection of GPS spoofing, DoS, telemetry injections	High adaptability, detection of complex attacks	Requires training data and computational resources
4	Cryptographic verification	Verification of data integrity and authenticity	Digital signatures, HMAC, secure boot	High protection of integrity and authenticity	Does not identify behavioral abnormalities
5	Behavioral Detection	Comparison of actual behavior with a physical flight model	GNSS and Inertial Measurement Unit (IMU) cross-checking, trajectory control	Effective for navigation attacks	Requires an accurate motion model

A comprehensive study of existing cyber-attacks on UAVs and the effectiveness of existing methods has led to the development of a multi-level cyber defense system for UAVs, which is shown in Figure 3.

DOI: 10.37943/25GEVU5826

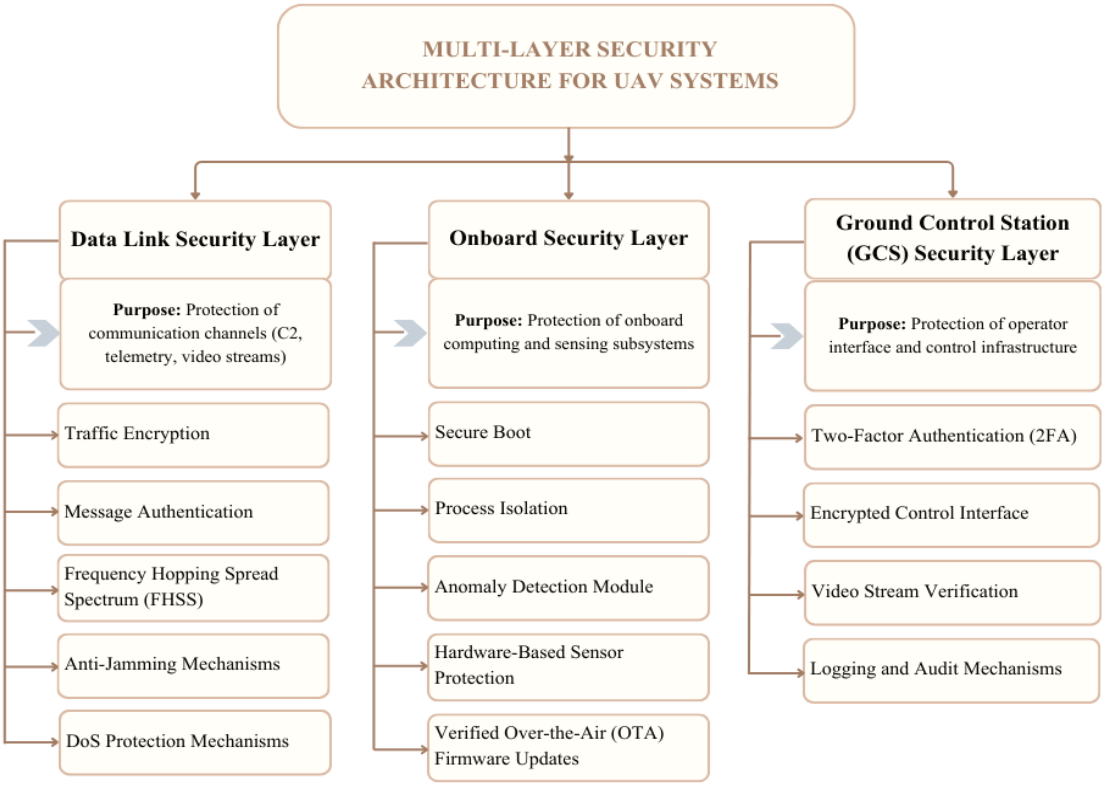
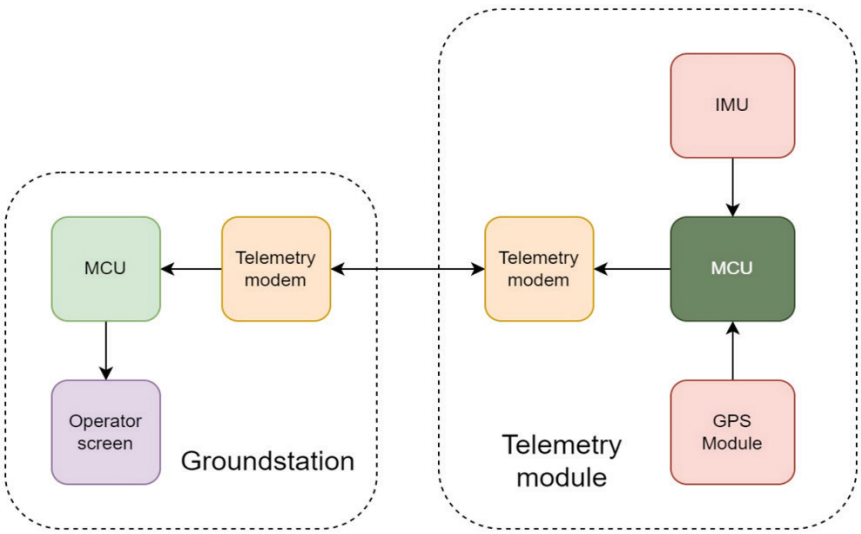


Figure 3. Conceptual architecture of the UAV cyber defence system

In the conceptual architecture for the UAV cyber defence system that has been developed, security is ensured simultaneously at the level of the communication channel, the on-board computing platform, and the ground control station. Unlike existing solutions, the approach presented here integrates the protection of navigation, telemetry streams, the sensor suite, actuator modules, and the operator interface into a single continuous chain.

For a detailed analysis of the effectiveness of the proposed multi-level architecture, it is advisable to examine its functional components separately. Among these, the telemetry communication channel is of particular importance, as it is this channel that ensures the continuous exchange of control commands and flight parameters between the on-board system and the ground control station.

The telemetry channel, which transmits control commands and flight parameters, is a critical component of a UAV that is vulnerable to injection attacks, identity spoofing, and packet integrity breaches. The structure of the UAV telemetry system is shown in Figure 4.



Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 25, MARCH 2026

Figure 4. Structure of the UAV telemetry system

The diagram illustrates the structural organization of telemetry communication between the ground control station and the UAV's on-board telemetry module. The ground control station comprises a microcontroller unit (MCU), an operator interface, and a telemetry modem, which facilitates two-way data exchange. Control commands from the operator are transmitted via the MCU to the radio modem and then over a wireless communication channel. The on-board telemetry module contains its own MCU, connected to navigation and inertial sensors (GPS module, IMU). The telemetry modem receives control commands and transmits flight parameters (coordinates, orientation, speed, system status) back to the ground station. An analysis of the literature has identified the most common telemetry communication protocols used by UAVs as MAVLink, User Datagram Protocol (UDP), and Transmission Control Protocol (TCP) [29].

The Micro Air Vehicle Link (MAVLink) protocol is used in UAV systems to provide radio communication within a limited range at an average data rate in line-of-sight mode [30]. A distinctive feature of MAVLink is its low redundancy and small packet size, which makes it effective for radio channels with limited bandwidth. However, in its basic version, the protocol does not provide built-in encryption, which creates risks of message interception and injection [31]. The TCP and UDP transport protocols are used for the transmission of real-time telemetry data [32]. They are widely used in both wired and wireless networks. The use of TCP ensures reliability, guarantees delivery of data in a specific order, and provides congestion control. However, the acknowledgement mechanism increases latency, which limits its use in time-critical control channels. UDP places less emphasis on reliability parameters than TCP in order to focus on the real-time delivery of data packets. This makes UDP preferable for telemetry and video streams, but at the same time increases vulnerability to spoofing attacks and packet injection [33].

At this stage of the research, a detailed analysis of the message structure, including serial number fields, checksum verification logic, and formal definitions of data fields, enabled the identification of three main types of vulnerabilities:

- lack of or weak encryption, packet substitution;
- vulnerabilities caused by the use of predictable identifiers;
- inconsistencies in checksum verification.

These results formed the empirical basis for presenting threat models within the telemetry module. For a more detailed analysis, a structural and functional diagram of the software-based UAV telemetry exchange system is presented in Figure 5.

DOI: 10.37943/25GEVU5826

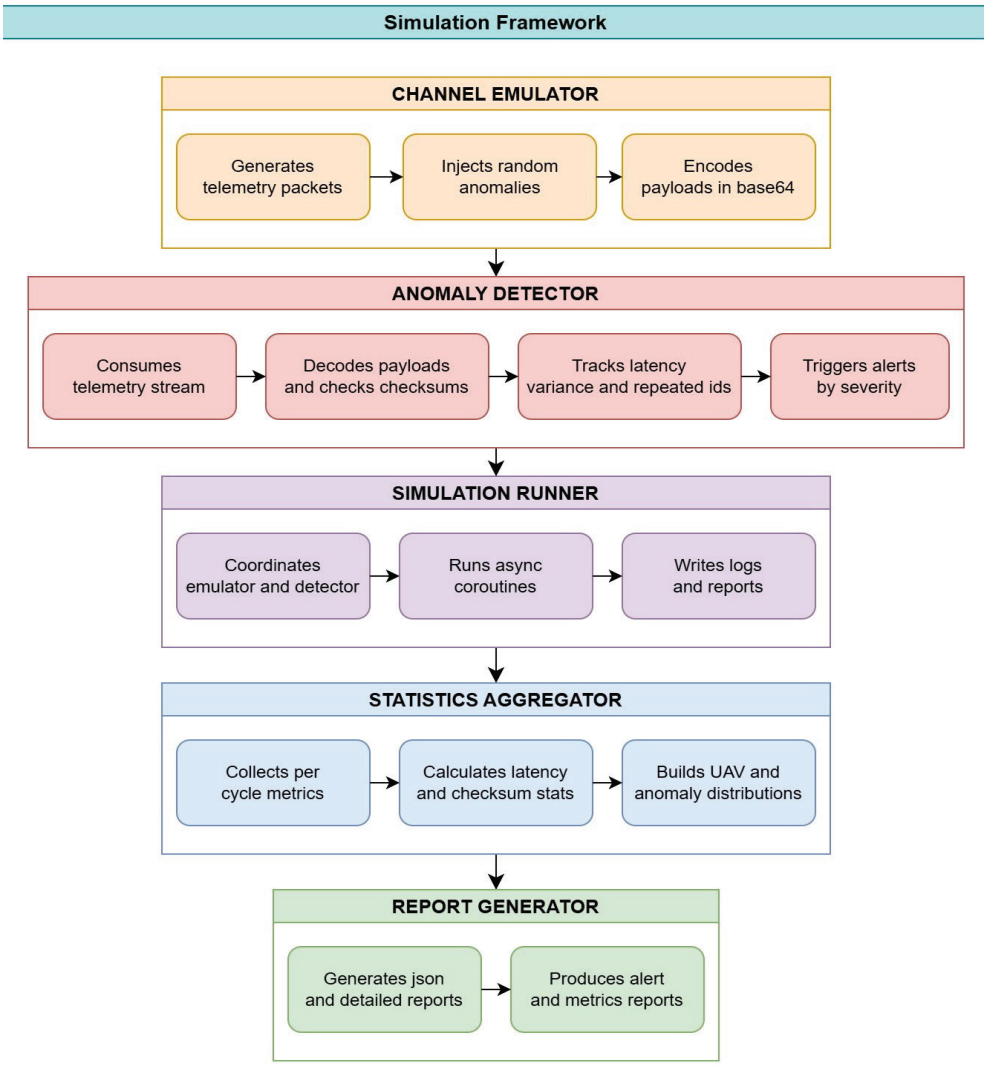


Figure 5. Functional architecture of the UAV telemetry channel emulation and anomaly detection system

The Channel Emulator is used to generate telemetry packets, inject random anomalies, and coordinate the payload in Binary-to-text encoding (Base64) format. It is used to simulate real-world data transmission conditions. The Anomaly Detector module is used to decode the payload and verify checksums. It analyses repeating identifiers and delay variations and, depending on the severity level of events, triggers notifications. The Statistics Aggregator module collects metrics by processing cycles, calculates delay statistics and checksums, and generates anomaly distributions. Coordination between the existing modules is carried out via an event loop. The Report Generator generates JavaScript Object Notation (JSON) reports, event logs, and summary system metrics.

Key Performance Indicators (KPI) were used to quantitatively assess the accuracy of attack detection and the robustness of the developed system. The following indicators were used in this study:

1. In the presented functional architecture of the system for emulating and detecting anomalies in the UAV telemetry channel, the checksum verification mechanism for MAVLink packets can be expressed as follows:

$$CRC_{valid} = \sum_{i=1}^{n} b_i \ mod\ 256, \quad (1)$$

where CRC_{valid} – valid is the expected checksum value that is determined by calculation from the contents of the MAVLink packet;

the value of the i-th byte in the telemetry packet payload;

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 25, MARCH 2026

n – is the total number of bytes in the payload of the MAVLink packet;

mod 256 - module operation to ensure that the checksum corresponds to one byte (0-255) that corresponds to the structure of the MAVLink packet.

This value serves as the reference checksum and is used in the simulation to quantify errors in the communication channel. The absence of data transmission errors is confirmed by the fact that the calculated checksum matches the one received in the MAVLink packet.

2. To quantify the frequency of errors in the checksum, the error rate is determined as follows:

$$R_{CS} = \frac{N_{mismatch}}{N_{total}} \cdot 100\%, \quad (2)$$

where $N_{mismatch}$ - the number of packets for which the calculated checksum did not match the received checksum.

N_{total} – total number of telemetry packets processed in the simulation window.

The resulting R_{CS} coefficient reflects the proportion of telemetry packets in which a checksum discrepancy is detected. Under normal operating conditions, the value of this indicator tends towards zero; if it increases, it becomes necessary to activate mechanisms to detect interference with the telemetry stream.

3. Under normal operating conditions, the typical delivery time of a packet from the on-board module to the ground station is characterized by the average delay. This is used to assess the impact of detection algorithms on the characteristics of the telemetry channel. The mathematical model of channel delays in this case is defined as follows:

$$\mu = \frac{1}{N}\sum_{i=1}^{N} d_i \ , \quad (3)$$

where d_i – transmission delay of the *i* telemetry packet;

N – total number of packets processed.

This indicator allows the impact of network conditions and data processing algorithms on the stability of data exchange between the on-board module and the ground station to be assessed.

4. The telemetry exchange instability indicator is characterized by the delay variance, which is determined as follows:

$$\sigma^2 = \frac{1}{N}\sum_{i=1}^{N}(d_i - \mu)^2 \ . \quad (4)$$

This parameter allows the stability of the communication channel to be assessed. Low values indicate that the system operates reliably even in the face of attacks.

5. The statistical criterion for deviations in packet transmission from normal operation is assessed using the packet delay anomaly criterion and is determined as follows:

$$|d_i - \mu| > k\sigma \ , \quad (5)$$

where k - is the sensitivity threshold, usually values 2 (confidence interval ~ 95%) or 3 (confidence interval ~ 99.73%) are taken, and depends on the sensitivity of the detector and the probability of false alarms;

This metric enables the identification of temporal anomalies where classification falls within the acceptable statistical range.

6. The effectiveness of the detection algorithm is characterized by a model for estimating the probability of detecting attacks:

$$P_D = \frac{N_{detected}}{N_{injected}} \ , \quad (6)$$

where $N_{detected}$ – number of artificially introduced anomalies;

DOI: 10.37943/25GEVU5826

$N_{injected}$ - number of correctly detected anomalies.

The probability of correctly detecting an attack is estimated in the range from 0 to 1. It is characterised by the system's ability to correctly detect intrusions. Values close to 1 indicate that the system is highly sensitive to attacks.

$$0 \leq P_D \leq 1 \, . \tag{7}$$

8. The false positive rate reflects the system's ability to avoid incorrectly classifying normal packets as anomalous.

$$P_{FA} = \frac{N_{false}}{N_{normal}} \tag{8}$$

N_{normal} – number of packets in normal mode

N_{false} – the number of misclassified packets

This metric assesses the likelihood that the system will report an anomaly when none exists. If the P_{FA}value is excessively high, this may lead to unnecessary security responses and a loss of confidence in the system.

9. The checksum error rate characterizes the proportion of packets in which a data integrity violation has been detected, and is calculated as follows:

$$\mathrm{C}_{error} = \frac{N_{error}}{N_{total}} \tag{9}$$

N_{error} - the number of packets with a checksum error;

N_{total} - the total number of packets processed.

This metric enables a quantitative assessment of the intensity of attacks aimed at compromising the integrity of telemetry data.

The detector's threshold values were selected empirically based on a series of preliminary experiments and an analysis of the distribution of delays and checksum errors during normal system operation. Thresholds for delay, checksum errors, and repeated identifiers can be set using the parameters latency_threshold, checksum_threshold, and repeat_id_threshold. The configuration parameters of the anomaly detector are presented in Table 2.

Table 2. Anomaly detector configuration parameters

№	Parameter	Symbol	Value
1	Maximum permissible packet delay	latency_threshold	0.03÷0.1 c
2	Checksum error threshold	checksum_threshold	0.05÷0.15
3	Identifier repetition threshold	repeat_id_threshold	2÷5
4	Delay anomaly detection coefficient	k	3

They allow for more detailed configuration of anomaly detection sensitivity.

10. If the thresholds exceed the set limit, the event is logged in the system under the following severity categories: medium, high, and critical. In this case, the threat severity assessment in the multi-level model system will be as follows:

$$S_i = \begin{cases} critical & if\ R_{CS} > \theta_{CS}^{high}\ AND\ f_j > \theta_{id} \\ high & if\ R_{CS} > \theta_{CS}^{high}\ OR\ |d_i - \mu| > 3\sigma_d \\ medium & if\ payload_{malformed} = true\ OR |d_i - \mu| > 2\sigma_d \end{cases}, \tag{10}$$

where S_i – severity classification assigned to the i -th detected anomaly;

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 25, MARCH 2026

θ_{CS}^{high} – upper checksum mismatch threshold parameter (checksum_threshold);

f_j – frequency of UAV identifier repetition in the current processing window is determined by the ratio of the number of n_j identifier occurrences to the total number of N packets:

$$f_j = \frac{n_j}{N} \tag{11}$$

θ_{id} – ID recurrence threshold parameter (repeat_id_threshold);

$payload_{malformed}$ – Boolean indicator equal to the moment when the payload of the packet decoded in the Base64.

To verify the proposed architectural model, a practical implementation was carried out in the Python 3.12 environment, within which a software simulation platform for the UAV telemetry channel was developed.

The implementation is based on the joint operation of telemetry packet generation modules, an anomaly injection mechanism—including a fault detection subsystem-and blocks for statistical processing of results. Simulation modelling of the telemetry channel involves several stages: development of the simulation software platform; generation of telemetry data; introduction of anomalies (attack injections); data processing and KPI calculation.

Results

Telemetry processing is viewed as a continuous process involving the gradual accumulation of statistical data, which enables even subtle signs of attempted attacks to be detected. The requirements and technical specifications for security and cyber defence are based on the software capabilities that must be incorporated into the UAV system to detect the main forms of interference or damage. In particular, the system must be capable of identifying missing segments, erroneously generated payloads, and spoofed UAV identifiers. The nature of attacks carried out via the telemetry channel compromises the integrity, authenticity, or continuity of the UAV's functionality, which is critically dangerous.

The developed system architecture provides for the implementation of a modular software platform designed to simulate a realistic telemetry environment for UAVs. The defence structure is based on three functional levels: prevention, detection, and response. Each module differed conceptually from the others but was designed to interact within a common simulation environment. In this reporting cycle, the focus was on the detection level, and it was planned to integrate the prevention and response levels more deeply in subsequent phases.

The prevention layer will provide cryptographic protection and secure transmission protocols; however, it is more complex in terms of key management, and its implementation will be considered once the development of anomaly detection mechanisms has been completed. The response layer enables warnings to be issued and system responses to be triggered based on the confirmation of telemetric anomalies. At this stage, this module has been developed in a basic form with elementary functions. This process will be implemented depending on the test results and the ability to detect attacks in more complex scenarios. The workflow is visualised and presented in Figure 6.

DOI: 10.37943/25GEVU5826

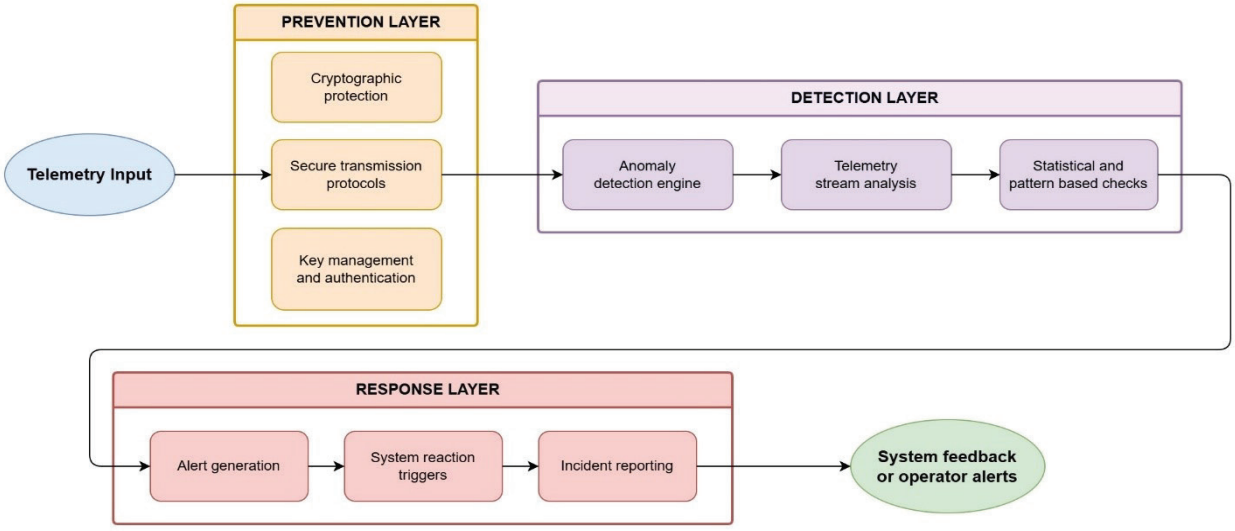


Figure 6. Multi-layered cyber defence architecture for a UAV telemetry channel

The multi-layered cyber defence architecture of the UAV telemetry channel ensures a continuous chain of protection for UAV telemetry exchanges.

The simulation platform in the Python 3.12 software environment consists of three main modules: ChannelEmulator, AnomalyDetector, and SimulationRunner. These modules were developed in iterations, each of which underwent independent unit testing and verification to ensure internal consistency of results and traceability.

The channel emulator is the source of telemetry data. It generates synthetic packets with realistic UAV identifiers, timestamps, and other flight parameters, such as altitude, speed, heading, and battery charge level. The encrypted communication channel and payloads are encoded using Base64. The system also features controlled anomaly injection: randomly introduced errors include packet loss, corrupted payloads, and fake UAV identifiers. This allows the system's performance to be observed under repeatable, semi-random conditions.

Another key component, AnomalyDetector, provides core analysis functionality. It processes a real-time telemetry stream, decodes each payload, and verifies the embedded checksums. It also calculates and tracks statistical metrics, such as latency variance and repeated UAV identifiers, to identify unusual patterns.

Thresholds for latency, checksum errors, and repeated IDs can be set using the parameters: latency_threshold, checksum_threshold, repeat_id_threshold. These allow for fine-tuning of detection sensitivity. If these thresholds are exceeded, the system logs the event with an assigned severity level: medium, high, or critical.

SimulationRunner links both components together, managing the execution process. It ensures that ChannelEmulator and AnomalyDetector run concurrently using Python's asyncio coroutines, emulating a real-time communication channel. The interrelationship of the modules and components presented is shown in Figure 5.

Deterministic random seeds are used to ensure repeatable results a very important feature for verification and regression testing. After each simulation run, *SimulationRunner* produces two kinds of output: a timestamped *.log file* recording all detected anomalies, and a structured. json *report* summarizing key metrics from the execution, nevertheless, as a conclusion of the written modules and components, the following diagram explains the relationship between components that have been coded.

Discussion

To check the functionality of the proposed telemetry channel model, a series of experiments was carried out, where the main results of the UAV telemetry channel simulation are presented in Table 3

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 25, MARCH 2026

Table 3. Main results of the UAV telemetry channel simulation platform

№	Indicator	Value	Interpretation
1	Number of simulation cycles	100	Representative model run
2	Proportion of injection anomalies	10%	Controlled load on the detection system
3	Packages processed	97	Minor losses caused by simulated failures
4	Checksum mismatches detected	6	Data integrity violations detected
5	Total number of recorded anomalies	118	The system demonstrates high sensitivity.
6	Average packet delay	0.037 сек	Stable channel performance under load
7	Delay dispersion	1.45×10^{-4}	Low transmission variability
8	Output formats	.log, .json	Double verification and traceability
9	Repeatability of the experiment	Deterministic random seeds	Ensuring reproducibility of results
10	Probability of false positives	0.03÷0.08	Probability of false positives from the delay threshold
11	Implementation environment	Python 3.12	Asynchronous telemetry processing

Most of the events in the obtained simulation results were classified as significant, and the distribution by criticality level was 100 high, 14 medium, and 4 critical. In terms of processed data, most anomalies were caused by high checksum failure rates, unusually frequent repetitions of UAV identifiers, or identification of fake UAV tags such as UAV_612, UAV_162, and UAV_678. All anomalies detected were recorded in a file named anomalies _ 20251112 _ 163329.log. The event log of this .log file is shown in Figure 7:

Figure 7. Log view

These entries provide trace evidence of the functionalities of real-time detection in the system and, when generated, can be cross-checked with generated JSON summaries. The matching .json report contains total packets processed, latency statistics, and severity breakdowns along with execution timestamps that give a quantitative view of each simulation run.

The logging framework developed during this phase proved very useful in troubleshooting and validation. In fact, unexpected behaviors, such as delayed alerts or anomaly entry misses, were much easier to diagnose by comparing outputs in both *.log* and *.json* formats. Maintaining this dual-output system ensures that each anomaly is both chronologically documented and analytically summarized, as shown in Figure 8.

DOI: 10.37943/25GEVU5826

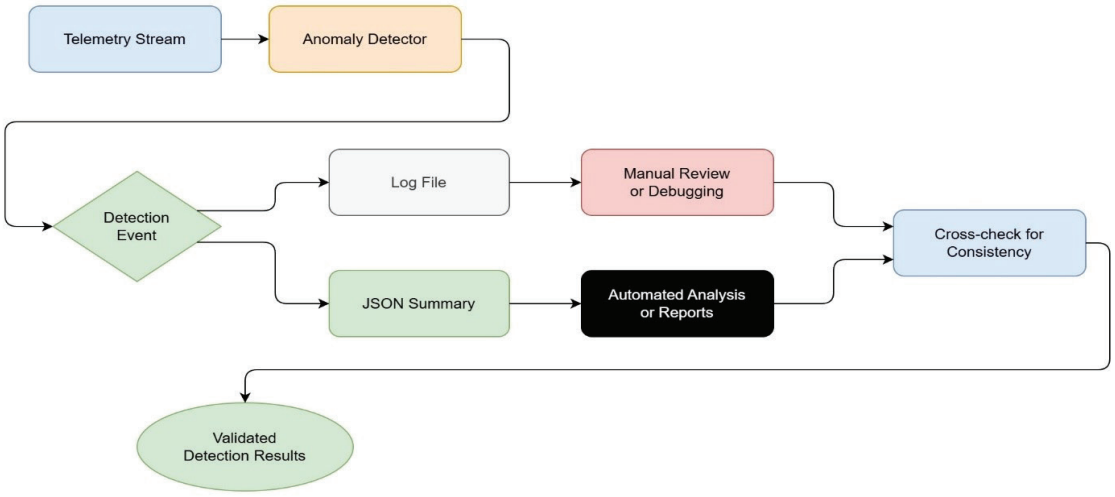


Figure 8. Double exit mechanism

The findings supported the initial hypothesis that statistical telemetry analysis, if continuously applied and supported by modular modeling tools, could provide a practical framework for early anomaly detection even in the absence of machine learning (ML) algorithms. This contribution is an important step towards creating a full-fledged cyber defense system for UAV platforms.

Conclusion

The use of signature methods provides high detection accuracy when detecting known attacks on UAVs. However, despite the presence of a low computational load during implementation, it is not able to effectively identify new types of attacks with a sudden change in their characteristics. Also, machine learning-based methods are highly adaptive and are capable of detecting complex attack patterns, including GPS spoofing and DoS. In most cases, they are applicable in complex attack scenarios where training data sets and significant computing resources are required. This makes it not applicable in conditions of limited computing power of on-board UAV systems. Unlike these approaches, the proposed method is based on deterministic analysis of telemetric parameters (checksums, delays, and packet identifiers) and does not require prior training. This provides low computational complexity and real-time applicability on resource-constrained platforms.

The results of the simulation demonstrate the effectiveness of the proposed method for detecting anomalies in a telemetric communication channel in the presence of navigation and telemetric distortions formed in the controlled environment. Verification of the system was carried out in a sequential order of observation of the system operating in continuous data transmission mode, where an analysis of the trajectory of anomalies, their development, and the moment of the system transition from a stable state to a pre-emergency or emergency one was carried out.

The practical implementation of the architecture in the form of a software simulation platform in the Python 3.12 environment provided reproducible telemetry exchange modeling and controlled injection of anomalies. The results of a series of experiments confirmed the effectiveness of the statistical method for detecting anomalies based on the analysis of delays, repeatability of identifiers, and checksum errors. The system has demonstrated resistance to simulated effects while maintaining stable time characteristics of data transmission. The results support the hypothesis that deterministic statistical analysis of telemetry flows can provide detection of anomalies at early stages without involving resource-intensive machine learning algorithms, which is especially important for systems with limited computing resources.

At the same time, the proposed approach is inferior in its ability to identify complex multidimensional and hidden attacks and requires preliminary adjustment of threshold parameters, which can affect the level of false positives. Prospects for further research are associated with in-depth integration of the cryptographic level of protection, expansion of attack scenarios, as well as testing the proposed approach in hardware-real conditions of UAV operation.

Acknowledgment

This research was funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant №AP26101065)

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 25, MARCH 2026

References

[1] Islam, M. S., Mahmoud, A. S., & Sheltami, T. R. (2025). AI-Enhanced Intrusion Detection for UAV Systems: A Taxonomy and Comparative Review. Drones, 9(10), 682. https://doi.org/10.3390/drones9100682

[2] Alsumayt, A., Nagy, N., Alsharyofi, S., Alahmadi, R., Al-Rabie, R., Alesse, R., Alibrahim, N., Alahmadi, A., Alghamedy, F. H., & Alfawaer, Z. (2026). Cutting-Edge DoS Attack Detection in Drone Networks: Leveraging Machine Learning for Robust Security. Sci, 8(1), 20. https://doi.org/10.3390/sci8010020

[3] Tlili, F., Ayed, S., & Fourati, L. C. (2024). Exhaustive distributed intrusion detection system for UAVs attacks detection and security enforcement (E-DIDS). Computers & Security, 142, 103878. https://doi.org/10.1016/j.cose.2024.103878

[4] Alshamrani, A., & Alghamdi, A. M. (2026). Zero-shot attack detection in UAV networks using foundation models. Alexandria Engineering Journal, 136, 105–124. https://doi.org/10.1016/j.aej.2025.12.065

[5] Mohammed, U. M., Omolara, A. E., Abiodun, O. I., Rasheed, J., Osman, O., Lar, P. M., Adeyinka, P. O., & Olugbenga, A. G. (2025). Cyber threat in drone systems: Bridging real-time security, legal admissibility, and digital forensic solution readiness. Frontiers in Communication and Networks, 6, 1661928. https://doi.org/10.3389/frcmn.2025.1661928

[6] Burbank, J., Caleb, T., Andam, E., & Kaabouch, N. (2026). Detection and Mitigation of Cyber Attacks on UAV Networks. Electronics, 15(2), 317. https://doi.org/10.3390/electronics15020317

[7] Sharifi, I., Ghazanfari, M., Taye, A., Wei, P., Ahmed, M. H., Kim, H. T., Ghasemi, M., Gupta, V., Dahle, N., Canady, R., Diaz Gonzalez, A., Coursey, A., Bjorkman, B., Lemieux-Mack, C., Ward, B. C., Koutsoukos, X., Biswas, G., Herencia-Zapana, H., Hasan, S., Amundson, I., Fotiadis, F., Topcu, U., Lu, J., Chen, Q. A., Aryal, N., Ibrahim, A., Ras, A. K., & Shirkhodaie, A. (2026). A survey of security challenges and solutions for UAS traffic management (UTM) and small unmanned aerial systems (sUAS). https://doi.org/10.48550/arXiv.2601.08229

[8] Yoo, J. D., Kim, G. M., Song, M. G., & Kim, H. K. (2025). MeNU: Memorizing normality for UAV anomaly detection with a few sensor values. Computers & Security, 150, 104248. https://doi.org/10.1016/j.cose.2024.104248

[9] H. Tang and Y. Chen, "Composite Observer-Based Resilient MPC for Heterogeneous UAV-UGV Systems Under Hybrid Cyberattacks," in IEEE Transactions on Aerospace and Electronic Systems, vol. 61, no. 4, pp. 8277-8290, Aug. 2025, https://doi.org/10.1109/TAES.2025.3542737

[10] R. Romagnoli, B. H. Krogh, D. de Niz, A. D. Hristozov and B. Sinopoli, "Software Rejuvenation for Safe Operation of Cyber–Physical Systems in the Presence of Run-Time Cyberattacks," in IEEE Transactions on Control Systems Technology, vol. 31, no. 4, pp. 1565-1580, July 2023, https://doi.org/10.1109/TCST.2023.3236470

[11] S. Qiu and H. Liu, "A new zonotope-based attack detection method for UAV," 2022 41st Chinese Control Conference (CCC), Hefei, China, 2022, pp. 4276-4280, https://doi.org/10.23919/CCC55666.2022.9902124

[12] B. M. Horowitz, "Cyberattack-Resilient Cyberphysical Systems," in IEEE Security & Privacy, vol. 18, no. 1, pp. 55-60, Jan.-Feb. 2020, https://doi.org/10.1109/MSEC.2019.2947123

[13] H. Yang, Z. Yu and Y. Zhang, "Observer-Based Adaptive Resilient Fault-Tolerant Cooperative Control for Multiple Fixed-Wing UAVs Subject to Cyberattacks and Actuator Faults," in IEEE Internet of Things Journal, vol. 13, no. 3, pp. 5179-5192, https://doi.org/10.1109/JIOT.2025.3642912

[14] M. Tahavori, "A System-Theoretic Measure for Quantification of Vulnerabilities to Cyber Attacks with Application to Unmanned Aerial Vehicles," 2020 7th International Conference on Control, Decision and Information Technologies (CoDIT), Prague, Czech Republic, 2020, pp. 492-495, https://doi.org/10.1109/CoDIT49905.2020.9263905

[15] A. Zuev, O. Gryb, S. Shvets and V. Makarov, "Evaluating and Ensuring the Cybersecurity of Power Line Remote Monitoring Systems," 2018 IEEE 3rd International Conference on Intelligent Energy and Power Systems (IEPS), Kharkiv, Ukraine, 2018, pp. 271-274, https://doi.org/10.1109/IEPS.2018.8559572.

[16] P. Wang et al., "QUADFormer: Learning-Based Detection of Cyber Attacks in Quadrotor UAVs," in IEEE Transactions on Control Systems Technology, vol. 34, no. 1, pp. 59-73, Jan. 2026, https://doi.org/10.1109/TCST.2025.3598255

[17] H. Rezaee, E. Salvato, G. Fenu and T. Parisini, "Resilient Coverage by Teams of Quadrotor UAVs: Theory and Experiments," in IEEE Transactions on Control Systems Technology, vol. 32, no. 6, pp. 2009-2022, Nov. 2024, https://doi.org/10.1109/TCST.2024.3389350

[18] R. S. Tucker, M. Nadeem and S. Pervez, "Real-Time Detection and Mitigation of GPS Spoofing in UAV Systems," 2025 12th International Conference on Information Technology (ICIT), Amman, Jordan, 2025, pp. 154-160, https://doi.org/10.1109/ICIT64950.2025.11049153

[19] S. Gupta et al., "GPS Spoof and Detect in Ardupilot Simulating UAVs," 2023 OITS International Conference on Information Technology (OCIT), Raipur, India, 2023, pp. 817-822, https://doi.org/10.1109/OCIT59427.2023.10430778

[20] A. P. Zhao et al., "Uncrewed Aerial Vehicle-Based Cyberattacks on Microgrids," in IEEE Transactions on Industry Applications, vol. 62, no. 2, pp. 3212-3225, March-April 2026, https://doi.org/10.1109/TIA.2025.3618810

[21] Z. Yu and Q. Wang, "Analysis of future demand for a general-purpose UAV Attitude and Heading Reference system," 2024 36th Chinese Control and Decision Conference (CCDC), Xi'an, China, 2024, pp. 94-99, https://doi.org/10.1109/CCDC62350.2024.10587514

[22] H. J. Hadi, Y. Cao, M. K. Khan, N. Ahmad, Y. Hu, and C. Fu, "UAV-NIDD: A Dynamic Dataset for Cybersecurity and Intrusion Detection in UAV Networks," in IEEE Transactions on Network Science and Engineering, vol. 12, no. 4, pp. 2739-2757, July-Aug. 2025, https://doi.org/10.1109/TNSE.2025.3553442

[23] Pekarčík, E. Chovancová, M. Havrilla and M. Hasin, "Security analysis of attacks on UAV," 2023 IEEE 21st World Symposium on Applied Machine Intelligence and Informatics (SAMI), Herl'any, Slovakia, 2023, pp. 57-62, https://doi.org/10.1109/SAMI58000.2023.10044500

[24] H. Jalil Hadi, Y. Cao, S. Li, Y. Hu, J. Wang and S. Wang, "Real-Time Collaborative Intrusion Detection System in UAV Networks Using Deep Learning," in IEEE Internet of Things Journal, vol. 11, no. 20, pp. 33371-33391, 15 Oct.15, 2024, https://doi.org/10.1109/JIOT.2024.3426511

[25] R. S. Tucker, M. Nadeem and S. Pervez, "Real-Time Detection and Mitigation of GPS Spoofing in UAV Systems," 2025 12th International Conference on Information Technology (ICIT), Amman, Jordan, 2025, pp. 154-160, https://doi.org/10.1109/ICIT64950.2025.11049153

[26] Federal Aviation Administration. (2023, December 19). National Airspace System (NAS) cybersecurity incident detection, reporting, and response policy (Order JO 1370.128). Federal Aviation Administration, https://www.faa.gov

[27] European Union Aviation Safety Agency. (2023). Regulations (EU) 2023/203 - Information security (Part-IS). https://www.easa.europa.eu/en

[28] International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. ISO. https://www.iso.org/standard/27001

[29] A. Yu, I. Kolotylo, H. A. Hashim and A. E. E. Eltoukhy, "Electronic Warfare Cyberattacks, Countermeasures, and Modern Defensive Strategies of UAV Avionics: A Survey," in IEEE Access, vol. 13, pp. 68660-68681, 2025, https://doi.org/10.1109/ACCESS.2025.3561068.

[30] U. V. Dad, D. T. Gandhi, D. B. Panchal, S. M. Agarwal and K. K. Sood, "MAVLink Protocol Customization for UAV Telemetry and Control Over a Low Data Rate SATCOM Link," 2024 IEEE 21st India Council International Conference (INDICON), Kharagpur, India, 2024, pp. 1-5, https://doi.org/10.1109/INDICON63790.2024.10958424.

[31] H. Xu et al., "Experimental Analysis of MAVLink Protocol Vulnerability on UAVs Security Experiment Platform," 2021 3rd International Conference on Industrial Artificial Intelligence (IAI), Shenyang, China, 2021, pp. 1-6, https://doi.org/10.1109/IAI53119.2021.9619330

[32] V. S, R. R, S. Selvan, S. S. S, S. K and S. R, "A Survey on Modern Innovative Secured Transport Layer Protocols on Recent Advances," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2023, pp. 1088-1093, https://doi.org/10.1109/ICCMC56507.2023.10084044

[33] S. N, A. K. V and S. Krishnakumar, "Detection of ARP Spoofing Attacks in Software Defined Networks," 2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS), Coimbatore, India, 2023, pp. 422-426, https://doi.org/10.1109/ICISCoIS56541.2023.10100567