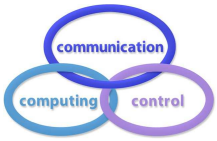
INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
Online ISSN 1841-9844, ISSN-L 1841-9836, Volume: 20, Issue: 3, Month: June, Year: 2025
Article Number: 7051, https://doi.org/10.15837/ijccc.2025.3.7051



CCC Publications

Adaptive Neural Networks for Mitigating GPS Spoofing Attacks in Unmanned Aerial Vehicles

A. Salgado, Y. Donoso

Alejandro Salgado
Department of Systems and Computer Engineering
Universidad de Los Andes, Colombia
Cra 1 N° 18A - 12, Bogotá, Colombia
a.salgadom@uniandes.edu.co

Yezid Donoso
Department of Systems and Computer Engineering
Universidad de Los Andes, Colombia
Cra 1 N° 18A - 12, Bogotá, Colombia
ydonoso@uniandes.edu.co

Abstract

Unmanned Aerial Vehicles (UAVs), or drones, have gained global attention over the past decades for their ability to perform diverse tasks without direct human intervention. With advances in artificial intelligence, UAV systems have not only improved, but also become more vulnerable to an increasing number of cyberattacks. This paper presents a study on detecting integrity failures in UAVs, focusing specifically on the GPS system. Theoretical background, methodology, and results are discussed, providing a comprehensive overview of adaptive neural networks developed to detect and mitigate the impact of these vulnerabilities in simulated scenarios.

Keywords: Unmanned Aerial Vehicle, GPS Integrity, Spoofing Attacks, Cybersecurity, Neural Networks, Anomaly Detection.

1 Introduction

Over the past decades, Unmanned Aerial Vehicles (UAVs), commonly known as drones, have captured global attention due to their ability to perform a variety of tasks without direct human assistance. These aerial devices can be remotely controlled or programmed to operate autonomously using microprocessors, sensors, and various communication technologies. The autonomy and flexibility of UAVs enable efficient task execution in less time and provide assistance in hazardous human operations [1].

The broad range of UAV applications is reflected in their classification into three main categories: military, commercial, and industrial. Each category addresses specific needs in different fields. This article focuses on military applications of UAVs, which provide navigation, secure communication, and reconnaissance capabilities in high-risk environments [1]. These applications highlight not only

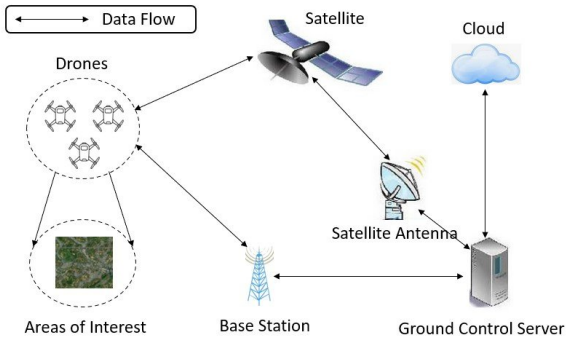


Figure 1: IoT Example Description [2]

the operational efficiency of UAVs but also their contribution to safety in situations where human intervention is limited. Consequently, the prevention and mitigation of cyberattacks become crucial.

In Colombia, the strategic importance of drones in military operations has been increasingly recognized by the government. The Colombian Aerospace Force has made a strategic decision to employ drones in support of high-risk operations. This commitment is evident in the establishment and development of the Basic School of Remotely Piloted Aircraft [3]. Such continuous growth underscores the critical role of drones in military operations.

Given the potential vulnerabilities of the GPS subsystem in UAVs and their implications for military applications, this article focuses on analyzing possible cybersecurity attacks targeting the integrity and data of UAVs. To address these concerns, this work incorporates a literature review and practical application through the simulation of integrity attacks and their mitigation. The goal of this work is to develop a neural network-based solution to detect and prevent attacks on the GPS system in simulated scenarios, serving as a blueprint for enhancing UAV security.

The remainder of this paper is structured as follows. Section 2 provides a comprehensive theoretical background, including an overview of UAV subsystems, cybersecurity challenges, and GPS-based navigation vulnerabilities. In Section 3, we outline the problem definition and the proposed approach, specifying the requirements and methodology. Section 4 details the development of our neural network-based detection system, including the mathematical model and implementation considerations. The experimental results and performance evaluation are presented in Section 5, demonstrating the effectiveness of our approach in detecting GPS spoofing attacks. Finally, Section 6 summarizes the key findings, discusses limitations, and suggests directions for future research.

2 Theoretical Framework

In this section, a literature review is conducted to provide context and justification for this work. This analysis aims to understand and address concepts related to unmanned aerial vehicles (UAVs), focusing particularly on their operation, potential threats, and the solutions suggested in the literature.

UAVs, or unmanned aerial vehicles, display a wide variety of sizes and specifications tailored to their specific applications. Key characteristics include payload capacity, which is the maximum weight a drone can carry, often critical in military applications where larger payloads are necessary for additional equipment. Flight mechanisms vary between rotary-wing drones, fixed-wing drones, and hybrids, depending on operational requirements. Range and altitude capabilities are crucial for remote operations and are particularly relevant when considering cyber threats. Speed and flight time are also essential as they determine a drone's ability to support sophisticated sensors and GPS systems for precise positioning and health monitoring during missions.

In military settings, the strategic importance of UAVs is highlighted by their ability to achieve high payloads, extend their operational range, and reach significant altitudes, capabilities essential for surveillance and tactical missions. These operational requirements necessitate the integration of advanced technologies that not only increase UAV efficiency in complex scenarios, but also improve their defenses against cyber threats.

2.1 Common UAV Subsystems

The architecture of UAVs is divided into several key subsystems that ensure their functionality, control, and ability to execute specific missions. The operational core of a UAV, the flight control system, is responsible for stabilization and includes sensors like gyroscopes and accelerometers to monitor movement, utilizing advanced flight computers and control algorithms for precise autonomous operations. The communication system manages data transmission between the UAV and ground control stations, using satellite technologies to support remote operations and secure communications against threats like espionage and spoofing.

In addition, UAVs rely on essential navigation and positioning systems, primarily GPS, supplemented by systems such as GNSS and visual navigation techniques to improve resilience and reduce GPS dependency. Payloads vary with mission and can include cameras, sensors, and other equipment, affecting UAV performance and requiring careful integration. Propulsion systems, customized to the design specifications, focus on enhancing energy efficiency with innovations in electric motors and battery technologies. Lastly, software and communication protocols, which include the operating system and flight controller firmware, are crucial for managing interactions and maintaining the integrity of the systems against cyber threats.

Problem	**Description**
Unauthorized Access and Manipulation	UAVs face significant cyberattack risks, where hackers seek unauthorized access to manipulate flight controls or compromise onboard sensors' integrity.
Limited Computational Resources	UAVs' design prioritizes hardware lightness and energy efficiency, restricting the implementation of stronger security measures.
Wireless Communication Vulnerabilities	UAVs' dependence on wireless protocols makes them susceptible to interception, electronic eavesdropping, and jamming attacks.
Physical Vulnerability	Risk of physical manipulation or theft, leading to unauthorized access to sensitive data or malicious use of the vehicle.
Evolving Threats and Techniques	The dynamic nature of cyber threats necessitates evolving and adapting security strategies.

Table 1: Problems in UAV Cybersecurity [2, 4]

Cyberattacks aim to affect one of the subsystems, altering the mission and leading to the complete system's compromise. The most prone subsystems to attacks are Flight Control Systems, Communication Systems, and Navigation and Positioning Systems [5].

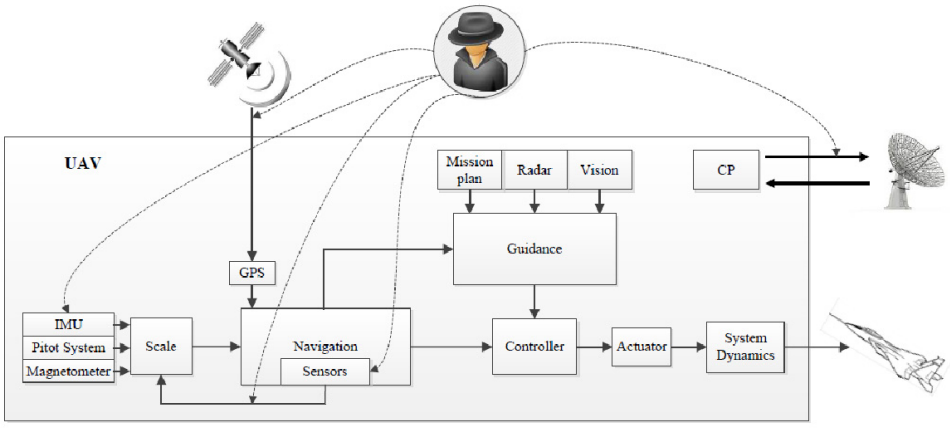


Figure 2: Common Vulnerable Subsystems to Cyber Attacks [5]

Multiple attacks target UAVs, the most common being data integrity compromises, information hijacking, privilege escalation, and forced landing. STRIDE analysis aids in threat modeling by

examining Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges. In this analysis, hijacking emerges as the predominant threat against UAVs [4].

Attack	**Description**	**Affected Subsystems**
Password Cracking	Exploits authentication vulnerabilities using brute force or password exploitation techniques.	Flight Control, Software, and Communication Protocols
Identity Spoofing in SDK	Manipulates user authentication information to mimic legitimate user actions.	Flight Control, Software, and Communication Protocols
GPS Spoofing	Generates false GPS signals to mislead the UAV's flight controller.	Navigation and Positioning, Flight Control
Open WiFi and Deauthentication	Gains unauthorized control through open WiFi networks or by sending continuous deauthentication packets.	Communication, Software, and Communication Protocols
System File Manipulation	Gains direct system access via Telnet to alter the UAV's system files.	Flight Control, Software, and Communication Protocols
Man-in-the-Middle (MitM) Attacks	Intercepts and can alter the information transmitted between the UAV and the control station.	Communications, Flight Control
Communication System Overload	Disrupts service using DoS tools to overload the UAV's communication systems.	Communications
Navigation System Compromise	Employs techniques such as buffer overflow and ARP cache poisoning to attack the navigation system.	Navigation and Positioning

Table 2: Common Cyber Attacks on UAVs [4]

2.2 GPS System in UAVs

The Global Positioning System (GPS) provides precise location and time data to UAVs through signals transmitted by satellites. The GPS system includes a receiver that captures these signals, allowing it to calculate its three-dimensional position based on the signal reception time [6]. The input of a GPS system consists of signals received from multiple GPS satellites. By receiving signals from at least four satellites, geometric calculations can determine the satellite's position with an uncertainty range of 5 to 10 meters. Ground monitoring stations correct any transmission errors during data transfer from the satellites. The position (x, y, z) of a GPS receiver can be calculated by solving the following equations for each satellite:

$$\rho_i = \sqrt{(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2} + c \cdot \Delta t \tag{1}$$

Where:

- ρ_i represents the pseudorange, or the approximate distance from the satellite i to the GPS receiver.
- (x_i, y_i, z_i) are the coordinates of satellite i.
- (x, y, z) are the coordinates of the GPS receiver (to be determined).
- c is the speed of light.
- Δt is the reciever clock bias relative to the GPS time.

Combining GPS signals with an inertial navigation system (INS) enables UAVs to maintain precise navigation even when GPS signals are weak or temporarily unavailable, using the Inertial Measurement Unit (IMU) to estimate position, speed and orientation during flight [8].

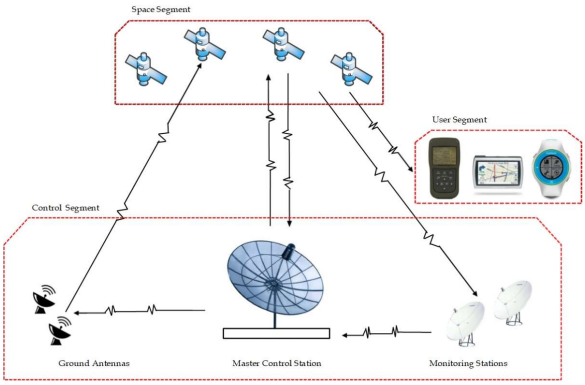


Figure 3: Graphic representation of GPS signals [7]

2.3 Cybersecurity Issues in UAV Systems

Before delving into common cyberattacks, it is essential to understand the general challenges cybersecurity engineers face with UAVs.

- **Unauthorized Access and Manipulation**: Implement robust encryption algorithms and authentication methods to secure communications between UAVs, satellites, and ground stations [9].
- **Limited Computational Resources**: Ensure that UAV systems meet high-security standards to mitigate public safety risks.
- **Wireless Communication Vulnerabilities**: Strengthen communication security with adaptive modulation, frequency hopping, and advanced signal processing techniques [10].
- **Physical Vulnerability**: Integrate self-diagnostic mechanisms, apply redundancy strategies, and develop adaptive response capabilities.
- **Evolving Threats and Techniques**: Conduct training programs and awareness campaigns for UAV operators to improve operational safety and prevent incidents.

2.4 Integrity Attacks on UAVs

Integrity attacks aim to alter, manipulate, or destroy data or system processes, jeopardizing the reliability and accuracy of UAVs. These attacks vary in methods and complexity, ranging from injecting false data to exploiting software vulnerabilities to modify UAV behavior.

2.4.1 Spoofing GPS

GPS spoofing involves emitting false GPS signals to deceive the receiver into believing it is located elsewhere. This exploits the unencrypted nature of civilian GPS signals, making them vulnerable to spoofing attacks. Such attacks can range from low-cost portable transmitters to sophisticated devices such as the LabSat 3 GPS Simulator. Given that weak legitimate GPS signals from distant satellites can easily be overpowered by nearby false signals, this vulnerability is significant [11]. Notably, in 2011, Iranian forces reportedly took control of an RQ-170 Sentinel, probably through GPS spoofing, underscoring the vulnerability of GPS sensors [12, 13]. Potential solutions include cryptographic authentication of GPS signals, anomaly detection systems using machine learning, and failure to use alternative navigation methods [14, 15].

2.4.2 Interference GPS (DoS)

GPS interference, or jamming, involves transmitting signals at the same frequency as GPS to block legitimate signals, effectively disrupting GPS functionality. This form of attack is simple and is often

used in illegal activities to evade detection or disrupt operations. Recent conflicts, such as the war in Ukraine, have demonstrated the use of GPS jamming to alter aerial navigation, highlighting the need for robust systems [16, 17, 18]. Mitigation strategies include employing detection and filtering technologies to identify and discard jamming signals, and the integration of alternative navigation systems such as GLONASS or inertial navigation systems (INS) for redundancy [19, 20, 21, 22].

2.4.3 Man-in-the-Middle (MitM) Attacks

MitM attacks intercept and potentially alter communications between UAVs and control stations, threatening data integrity and confidentiality. These attacks exploit vulnerabilities in communication protocols, insufficient encryption, or insecure networks. For instance, in 2016, drone communications were compromised due to weak encryption, allowing attackers to take control with inexpensive hardware [23, 24, 25]. Countermeasures include implementing end-to-end encryption, mutual authentication using digital certificates or preshared keys, and employing Virtual Private Networks (VPNs) for enhanced security. Intrusion detection systems can also monitor and block suspicious traffic patterns in real time, mitigating potential damage [26, 27, 28].

2.4.4 Software and Firmware Compromise

Software and firmware compromises involve infecting UAV systems with malicious code, altering their operation, or causing loss of control. Vulnerabilities may stem from unpatched exploits or malicious code injections during updates. For example, during the Ukraine-Russia conflict, Ukrainian forces reportedly compromised the Russian drone firmware, leading to operational failures [29, 30]. To address these issues, secure development practices are essential, including thorough code reviews, penetration testing, and secure update processes with authentication and integrity checks. Encrypting update communications and using digital signatures for software authentication are also vital [31].

2.5 Application of Neural Networks in UAVs

Adaptive neural networks, which adjust their structure during learning, are invaluable in dynamic environments where data may evolve over time. In UAVs, these networks enhance navigation and security by optimizing flight routes and analyzing sensor data. One innovative application is the detection of falsified GPS signals, crucial for maintaining security and integrity in UAV operations [32]. For this study, adaptive neural networks are deployed to detect falsified GPS signals in real time, allowing the system to recognize normal signal patterns and identify anomalies indicative of external interference, thus enhancing UAV security, autonomy, and reliability in critical operations.

3 Design and Specifications

3.1 Problem Definition

Continuous advancements in communication systems have significantly improved the operation of Unmanned Aerial Vehicles (UAVs). However, these developments also introduce new security challenges that engineers and system designers must tackle. Integrity attacks, especially spoofing attacks, are particularly concerning due to their increasing frequency in recent years. The associated risks are substantial, including the potential loss or hijacking of the vehicle. The GPS system, becomes a prime target for criminal activities due to its vulnerability. GPS signals, weak and error-prone from their long journey from satellites over a thousand kilometers away, are highly susceptible to both intentional and unintentional interference. The unencrypted nature of GPS signals and the availability of signal manipulation tools exacerbate their vulnerability. Spoofing attacks pose significant risks not only to UAV systems but also to other critical infrastructures like power and telecommunications networks, which depend on GPS for synchronization and operations.

In this context, the central issue addressed by this study is the integrity of GPS positioning measurements—longitude, latitude, and altitude—in UAV systems. While various mitigation schemes exist, many are either not completely secure, are unstable, or involve high costs. Consequently, this

study aims to develop a cost-effective solution that enhances the security of GPS systems in UAVs against spoofing attacks through adaptive neural network techniques to detect anomalies in real-time.

3.2 Specifications and Development Methodology

The development of this system centers on stringent functional and non-functional requirements essential for effective operation. Functionally, the system optimizes processing resources to ensure efficient operations without excessive computational demands and must detect various types of spoofing attacks within 30 seconds of spotting suspicious GPS signal variations. Although complete detection of all attack types might not be feasible due to their complexity, the system aims to implement the detection model and algorithm purely in software, negating the need for additional hardware. From a non-functional perspective, the system is designed to achieve a reliability rate where at least 90% of spoofing attacks are accurately identified, ensuring efficiency in detection time.

The development methodology of the solution involves a structured approach beginning with mathematical modeling of adaptive neural networks to form the detection logic, followed by coding and simulation in MATLAB. This environment is utilized for its robust simulation and data analysis tools, facilitating the development and testing of detection algorithms. Simulated tests in MATLAB assess the system's performance under various spoofing scenarios affecting latitude, longitude, and altitude measurements. Each model is rigorously compared with existing solutions to evaluate its strengths and weaknesses, thus refining its effectiveness. Additionally, while the proposal remains a simulation, considerations are made regarding the adaptability of the methodologies and software for real-world UAV applications, including adjustments needed for integrating the software into UAV operating systems and handling GPS measurements appropriately.

4 Solution Development

In this study, we simulate spoofing attacks using a GPS signal generator to alter latitude, longitude, and altitude measurements. Initially, these attacks start with the transmission of false signals that mimic legitimate GPS signals, albeit with such low power that they blend with the background noise. The power of these false signals gradually increases until they overshadow the real signals. To evaluate the effectiveness of our adaptive neural network in detecting these attacks, we create scenarios that mimic real-world conditions post-reception of GPS signals. This simulation involves both genuine and spoofed GPS signals, where alterations may occur in any of the three dimensions.

Our simulations assume that GPS signals are processed values of latitude, longitude, and altitude, bypassing the initial signal calculations from multiple satellites. This focus on the integrity of post-processed GPS data aligns our scenarios closely with real-life situations, where the primary concern is verifying the authenticity of GPS information after it has been computed. By parameterizing each attack scenario—varying the attack's duration, the magnitude of signal alteration, and the affected GPS parameters—we effectively test the resilience of our model across different complexities. This methodology ensures that our findings are applicable in practical settings, providing robust insights into the system's capability to detect and mitigate GPS spoofing attacks.

4.1 Mathematical Model of the Adaptive Neural Network for GPS

To begin modeling, it is crucial to understand the mathematical behavior of the GPS signals received by the UAV during an integrity attack. We consider a nonlinear system simplified for latitude, longitude, and altitude, characterized by the following equations:

$$\dot{x}(t) = f(x(t)) + g(x(t))u(t) + D(x,t) \tag{2}$$

$$y(t) = h(x(t)) + f_s(x,u) \tag{3}$$

Where:

- $u(t) \in \mathbb{R}^m$ represents the input vector, corresponding to the authentic GPS signals for latitude, longitude, and altitude.

- $y(t) \in \mathbb{R}^n$ is the output vector, including measurements perturbed by spoofing in the three dimensions.
- $x(t) \in \mathbb{R}^n$ is the state vector, describing the evolution of the GPS system under normal and attack conditions.
- $f : \mathbb{R}^n \to \mathbb{R}^n$ is the state function modeling the natural dynamics of the GPS system.
- $g : \mathbb{R}^n \to \mathbb{R}^{n\times m}$ is the input function, modeling how authentic GPS signals impact the system.
- $D : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n$ represents the system's uncertainties and perturbations not related to spoofing.
- $h : \mathbb{R}^n \to \mathbb{R}^n$ is the output function linking the system state to the GPS measurements.
- $f_s(x, u)$ is the spoofing function, injecting fault data into the system and altering GPS signals.

The spoofing attack model, $f_s(x, u)$, is defined as:

$$f_s(x,t) = \begin{cases} 0 & \text{if no attack is present} \\ z & \text{if an attack is occurring} \end{cases} \tag{4}$$

Here, z represents the input signal induced by the attacker, simulating the false sum over the real GPS measurements that incrementally increases throughout the duration of the attack. This model captures the dynamics and impact of spoofing attacks on the GPS system, enabling us to develop and test detection strategies effectively.

4.2 Mathematical Definition of the GPS Neural Network

Initially, we define a nonlinear observer that estimates the system state, denoted as $\hat{x}(t)$, which represents the estimated GPS position. The estimation is based on the measured outputs and a system model, described by the equation:

$$\dot{\hat{x}}(t) = f(\hat{x}(t)) + g(\hat{x}(t))u(t) + L(y(t) - h(\hat{x}(t))) \tag{5}$$

where L is the observer gain, designed to ensure the convergence of the system state estimation error $(\hat{x}(t) - x(t))$.

Subsequently, a neural network is employed to directly estimate $\hat{x}(t)$ from the inputs and outputs. The neural network is defined as follows:

$$\hat{x}(t) = W_2\sigma(W_1 y(t) + b_1) + b_2 \tag{6}$$

where:

- W_1, W_2, b_1, b_2 represent the weights and biases of the network.
- σ is the activation function, defined here as $\sigma(x) = \frac{1-e^{-x}}{1+e^{-x}}$.

To refine the estimation process, an approach based on the Extended Kalman Filter (EKF) is employed to adjust the weights and biases of the neural network based on the estimation error and system dynamics. The EKF equations are as follows:

$$\hat{x}^-(t) = \hat{x}(t-1) + \Delta t \cdot f(\hat{x}(t-1), u(t-1)) \tag{7}$$

$$P^-(t) = F(t-1)P(t-1)F^T(t-1) + Q \tag{8}$$

$$K(t) = P^-(t)H^T[H(t)P^-(t)H^T + R]^{-1} \tag{9}$$

$$\hat{x}(t) = \hat{x}^-(t) + K(t)(y(t) - h(\hat{x}^-(t))) \tag{10}$$

$$P(t) = (I - K(t)H(t))P^{-}(t) \tag{11}$$

In these equations:

- $\hat{x}(t)$ is the estimated state of the system at time t. The EKF attempts to approximate this state as accurately as possible despite nonlinearities and noise.
- $\hat{x}^{-}(t)$ is the a priori state prediction, i.e., the state estimation before the correction made upon receiving a new measurement.
- Δt is the time step between estimates.
- $f(\cdot)$ is the function that models the system dynamics. It is a nonlinear function describing how the system state evolves over time.
- $u(t-1)$ is the control input or action applied to the system at time $t-1$.
- F and H are the Jacobian matrices of the functions f and h with respect to the state. They provide a local linearization of the system dynamics function around the most recent estimated state.
- Q and R represent the covariances of the process noise and measurement noise, respectively. They provide the inherent uncertainty in the system dynamics, such as external disturbances or inaccurate modeling.
- $P(t)$ is the estimation error covariance.
- $K(t)$ is the Kalman gain. It determines how to adjust the a priori state estimation based on the new measurement to obtain the a posteriori estimation.
- L is the observer gain matrix.

4.3 Neural Network Architecture

The architecture of the neural network in this work is a design-from-scratch implementation, where the weight parameters are initially set to random values. This foundational design allows the system to begin learning without any prior biases, adapting its parameters purely based on the data it processes. As the system operates, it continually compares the expected signal—generated based on the model's current understanding of normal GPS behavior—with the actual received signal. This comparison is central to the system's ability to detect anomalies, as it enables the identification of deviations from expected GPS signal patterns, which may indicate spoofing attacks. The parameters of the neural network, as well as those of the integrated Kalman filter, are dynamically adjusted based on these comparisons, refining the model's accuracy over time through continuous feedback and learning.

4.3.1 Initial State Estimation

The process starts with the Observer calculating an initial estimation of the system's state. This state is based on the input data, which includes the raw signal over time of the GPS simulated position.

4.3.2 Process Initial Estimations and Inferences

The Neural Network receives the initial state estimation from the Observer. It processes this information to make inferences about the current state, utilizing its layers of neurons which adapt their weights as more data is processed. Currently the estimation is being done through the velocity values, which would imitate the information that is collected by the IMU.

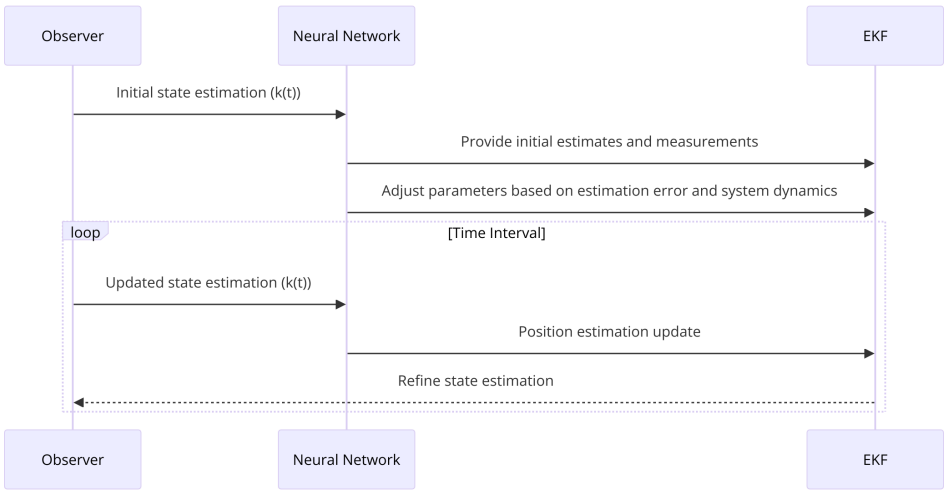


Figure 4: Neural Network Architecture Diagram

4.3.3 Adjust Parameters Based on Error and Dynamics

The EKF takes the inferences from the Neural Network and adjusts its parameters to minimize estimation errors. This is done by comparing the expected signals with the real received signals, identifying discrepancies that may indicate errors or spoofing attacks.

4.3.4 Refine State Estimation:

Following the adjustments, the EKF outputs a refined state estimation, improving the accuracy of the real signal, applying changes when it is detected as spoofing attacks.

4.3.5 Feedback Loop and Time Iteration

The updated state estimation is then looped back to the Observer. This marks the beginning of a new iteration where the Observer uses this updated estimation as the new initial state for the next cycle. This feedback loop allows the system to continuously adapt and refine its predictions based on new data and previous experiences.

4.3.6 Continuous Iteration

The cycle repeats at each time interval, allowing for ongoing adjustments and refinements. This iterative process is crucial for the system's ability to dynamically respond to changes and potential threats detected in the GPS signals.

4.4 Implementation in MATLAB

The position estimation system was implemented in MATLAB by following the next initialization for each iteration of simulated scenarios:

4.4.1 Neural Network

The neural network architecture includes 3 inputs (latitude, longitude, altitude), 3 outputs, and a hidden layer with 10 neurons. Weights and biases were initialized randomly as follows:

- *Inputs:* 3 (latitude, longitude, altitude)
- *Outputs:* 3 (position estimates)
- *Hidden Layer:* 10 neurons

- *Weights:* Initialized with random values using a normal distribution
- *Activation Function:* Hyperbolic tangent (tanh)

4.4.2 Extended Kalman Filter (EKF)

The EKF was implemented to refine the neural network's position estimates by adjusting parameters based on estimation errors. The key parameters were set as:

- *Initial Estimation Error Covariance (P):* Identity matrix
- *Process Noise Covariance (Q):* $0.01 \times I$
- *Measurement Noise Covariance (R):* $0.1 \times I$

This approach allows continuous improvement of position estimates by combining direct GPS measurements with the UAV's internal dynamics.

5 Results

To ensure that the GPS state estimation system effectively functions under various conditions and can detect and mitigate spoofing attacks, several validation tests were implemented. These tests are designed to evaluate both the accuracy of the state estimation and the network's ability to identify and respond to real-time spoofing attacks. The methods used are detailed below:

5.1 Simulation of Flight Patterns and Spoofing Attacks

Simulated UAV flight trajectories were generated in MATLAB, incorporating variations in latitude, longitude, and altitude under both normal conditions and spoofing attacks. To replicate real-world conditions, noise was added to the simulated signals to mimic typical GPS measurement errors, while specific spoofing patterns were introduced at various times to evaluate the system's detection capabilities. The system's state estimation accuracy was validated by comparing the real state estimations with those provided by the neural network and EKF, using mean squared error (MSE) as a metric for each state component (latitude, longitude, and altitude). The system's ability to detect spoofing was assessed by marking significant deviations between expected and actual measurements, with performance quantified through true positive and false positive rates.

To ensure consistent results, each flight and attack scenario was simulated multiple times, covering different noise configurations and spoofing types, which highlighted the influence of random initial neural network weights on result variability. Statistical analyses were conducted to evaluate the variance and reliability of the system's estimates and detections. The neural network parameters, including the number of layers, neurons per layer, and activation function, were optimized based on the outcomes of these tests with the values used mentioned in the last section. Overall, nine scenarios with varying latitude, longitude, and altitude were evaluated, with two scenarios detailed in the document to comprehensively illustrate the testing process and results.

5.2 Scenario: Latitude Attack Simulation

This scenario simulates a flight pattern that includes constant northward and southward movements, with lateral and altitude variations designed to test spoofing detection capability. During one-third of the time, a spoofing attack on latitude is introduced, gradually altering its trajectory.

An attack was simulated that artificially increased the variation of latitude during a specific segment of the signal. The analysis reveals that the longitude and altitude signals remained stable and showed minimal variations, indicating that the attack focused exclusively on latitude. The estimation provided by the model, which combines the neural network and the extended Kalman filter (NN+EKF), adequately adjusts during the attack, maintaining fidelity with the real trajectory in dimensions not affected by the spoofing.

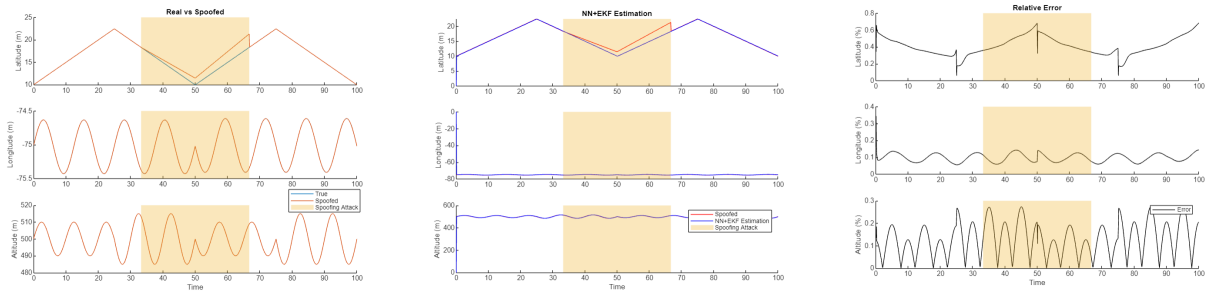


Figure 5: Comparative Analysis of Latitude Attacks. On the left: Real vs Spoofed, Center: Model Estimation vs Spoofed, On the right: Relative Error

The evaluation of the altitude estimation shows that the model correctly predicts and maintains the signal without deviations induced by the attack, thus confirming the robustness and proper functioning of the detection system. Regarding relative error measurements, it is observed that despite constant sinusoidal variations in longitude and altitude signals, the error remains below 0.2%, a value considered insignificant for this type of application.

However, the error in latitude, which was directly affected by the attack, varies between 1% and 4% throughout the simulation. The highest error values are observed especially during the abrupt changes induced and at the moment of the attack. This indicates that the model was not only successful in detecting the attack at the instant it occurred, but it also managed it within an acceptably low error margin, highlighting its effectiveness in mitigating spoofing under controlled test conditions. It is also noticeable that there is consistent shifment in the error value even when no spoofing attack is presented, this is due to the design from scratch architecture of the neural network.

5.3 Scenario: Longitude and Altitude Attack Simulation

This scenario simulates a flight with linear variations in longitude and altitude. The flight gradually ascends until the halfway point of the simulated time and then descends at the same rate. A spoofing attack is introduced in the second and third quarters of the simulation period, altering both longitude and altitude.

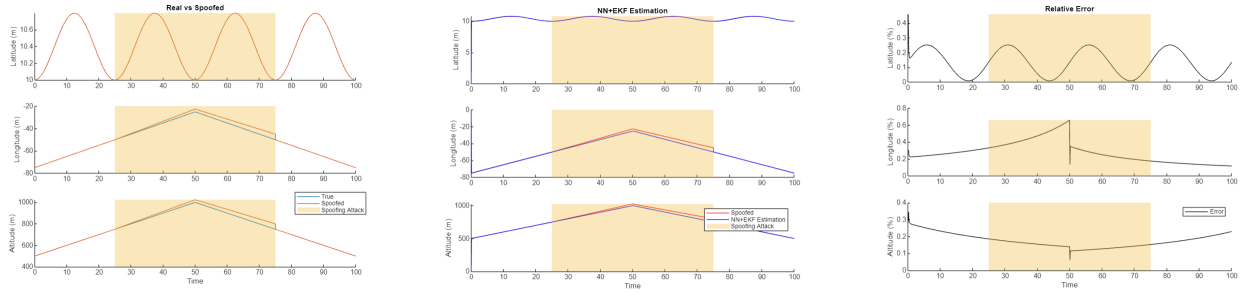


Figure 6: Comparative Analysis of Longitude and Latitude Attacks. On the left: Real vs Spoofed, Center: Model Estimation vs Spoofed, On the right: Relative Error

This test scenario focused on spoofing attacks that simultaneously affected longitude and altitude measurements, generating significant deviations from true values. Visualization of the real versus spoofed data shows a substantial alteration in the estimated trajectory, especially in altitude during the second half of the simulated time period, with increases reaching up to 100 meters above the true value.

The model integration demonstrated an ability to accurately estimate true values despite the interferences. During the attack, the NN+EKF managed to minimize discrepancies, maintaining estimations within a relatively low error margin: altitude error remained below 0.3% except during

the attack, where it briefly increased. Regarding longitude, the error rose to approximately 0.5%, coinciding with the attack phases.

5.4 Results Analysis

The state estimation system for GPS using a combination of neural network and Extended Kalman Filter (EKF) has proven effective under various simulated conditions, including no-attack environments and specific spoofing attacks. The tests have highlighted the model's ability to accurately follow the real trajectory under normal conditions and adapt quickly to induced manipulations in GPS data.

- **Robustness under Attack:** The model has shown a remarkable ability to detect and adjust estimates in response to spoofing attacks. Although the measurement error increases during attacks, particularly in the specific dimension affected, the system manages to return to a near-real trajectory once the attack ceases.
- **Stability in Normal Conditions:** In no-attack scenarios, the model has maintained a very low relative error, demonstrating its ability to perform precise and reliable tracking under standard operating conditions.
- **Response to Dynamic Variations:** There is a trend of increasing error at points where signals experience abrupt changes, even in the absence of spoofing. This suggests that the model, although efficient, could improve its response capability to rapid and dynamic variations in input data.

5.5 Key Observations and Trends

- **Sensitivity to Abrupt Changes:** The current model could be improved by increasing its sensitivity to abrupt signal changes without significantly increasing the error. Including adaptive layers or deep learning techniques that allow greater flexibility and adaptability could be explored. This sensitivity is due to the use of a design from scratch architecture.
- **Reduction of False Positives:** While the model is competent in correctly identifying an attack during spoofing events, there is room for improvement in minimizing false positives, i.e., situations where the model might incorrectly interpret a legitimate fluctuation as an attack.
- **Parameter Optimization:** Continuing to optimize the neural network parameters, including exploring different network architectures, could potentially improve the model's accuracy and efficiency. This includes adjusting the number of layers, neurons per layer, and activation functions based on iterative testing and feedback on system performance.

5.6 Summary of Results

The results so far are promising and demonstrate the model's viability for real-world applications, especially in scenarios where security and accuracy are paramount. However, like any AI and machine learning-based system, the refinement process is ongoing and requires adjustments based on testing and continuous evaluation of performance under varied conditions. Implementing improvements based on detailed observations will help progress towards a more robust and reliable system for accurate navigation and tracking in multiple scenarios. This paper should be taken as a guide rather than a final solution for this model. The results are presented in table 3.

6 Conclusions

6.1 Work Summary

This work has focused on detecting and preventing spoofing attacks on the GPS system of Unmanned Aerial Vehicles (UAVs) using adaptive neural networks and Extended Kalman Filters (EKF).

Scenario	Max Relative Error	Notes
Latitude Attack	4%	Highest error during attack peaks
Longitude Attack	0.5%	Notable variations during attack
Altitude Attack	1.5%	Significant deviations during attack
Latitude and Longitude Attack	7% (Latitude)	High error during simultaneous attacks
	0.4% (Longitude)	
Latitude and Altitude Attack	2% (Latitude)	Manageable error increase during attack
	1.5% (Altitude)	
Longitude and Altitude Attack	0.5% (Longitude)	Effective adjustment post-attack
	0.3% (Altitude)	Slight increase during attack
Latitude, Longitude, and Altitude Attack	6% (Latitude)	High error in complex scenarios
	1% (Longitude)	
	0.2% (Altitude)	
No Attack	$< 0.05\%$	Low error in normal conditions

Table 3: Summary of Results

Initially, a study was conducted on various cybersecurity attacks that can affect UAVs, narrowing the scope of the paper to specifically focus on integrity attacks on GPS systems. This phase was essential to understand the current issues and evaluate the solutions implemented to date.

The model development included several stages, from data collection to simulation implementation in MATLAB. Multiple flight scenarios and spoofing attacks were designed and simulated to validate the effectiveness of the model. These scenarios included variations in operational conditions, such as different levels of noise and types of attacks. The results demonstrated that the proposed system can detect and mitigate spoofing attacks with a high degree of accuracy, maintaining the integrity of GPS measurements under various operational conditions. The implementation of the extended Kalman filter, in combination with the adaptive neural network, allowed for real-time position estimation adjustments, ensuring greater robustness and accuracy in anomaly detection.

6.2 Performance and Limitations

The model's performance was evaluated in terms of the accuracy of position estimation and the ability to detect spoof attacks. The results indicated that the model could detect deviations induced by spoofing attacks and adjust position estimates to maintain the integrity of GPS signals. Additionally, a comprehensive review of the cybersecurity literature was conducted, identifying the characteristics of the attacks, their functionality, and the solutions developed to date.

The main strengths of the model include its ability to dynamically adapt to different noise conditions and types of attacks, and its accuracy in detecting subtle deviations in GPS signals. However, some limitations were identified, such as variation in accuracy during peaks of abrupt change and the need for constant adjustments in neural network parameters to optimize performance. Moreover, the model showed sensitivity to weight initialization, which could affect its performance in diverse operational scenarios. It is important to note that this work should be used as a guide, as it requires several adjustments to the code and the proposed solution to work correspondingly with the UAV used.

6.3 Problems Encountered and Possible Solutions

During the work's development, several problems were identified, including the neural network's sensitivity to weight initialization and the variability in GPS signals due to environmental factors.

These problems were addressed by implementing an extended Kalman filter, which improves the model's robustness and its ability to adapt to changes in operational conditions.

Another proposed solution was the dynamic adjustment of neural network parameters, which allowed for real-time performance optimization. A function with position estimation using a speed estimate, simulating an IMU, was implemented to reduce the impact of variability in GPS signals and improve the model's stability. However, it was found that this necessity limits the model's operation to scenarios where a real IMU is not available or an attack is generated on said system. Additionally, there was not enough time or resources to implement and test the system in a real UAV.

6.4 Validation of Results

Quantitatively, the accuracy of position estimates was evaluated by calculating the Mean Squared Error (MSE), which measures the average squared difference between the positions estimated by the system and the actual positions. A low MSE value indicates high accuracy in position estimation, which is essential for maintaining UAV operations' integrity in the presence of spoofing attacks. The results consistently showed low MSE values, confirming the system's accuracy under various operational conditions.

7 Future Work

This study has laid a robust foundation for advancing cybersecurity in UAV systems, identifying several paths for future research and development. As cybersecurity is a rapidly evolving field, continuous updates on new challenges and solutions are imperative. Keeping abreast of the latest trends through ongoing engagement with current publications, specialized conferences, and collaborations with experts in the field is crucial to stay ahead of sophisticated cyber threats like spoofing attacks.

Transitioning from simulated environments to real-world applications is a critical next step. This involves replacing simulated IMU inputs with real Inertial Measurement Units in the neural network simulations to better mimic UAV operational conditions and adjusting the model to accommodate different types of IMUs and GPS systems. Implementing the refined system in actual UAVs will allow for comprehensive testing under varied environmental conditions and attack scenarios, providing valuable empirical data to train and enhance the neural network model. This hands-on testing is essential not only for assessing the system's effectiveness in real operational contexts but also for gauging its resilience against a broader spectrum of cyber threats.

Finally, the iterative refinement of the system based on real-world testing outcomes will facilitate continuous model improvement. This includes tweaking the neural network parameters for better accuracy and adaptability, incorporating advanced learning algorithms for improved anomaly detection, and exploring new signal processing techniques. Such enhancements will ensure the system remains robust and effective against evolving cybersecurity threats, thereby bolstering the security posture of UAV operations.

8 Footnotes

Funding

This research received no external funding.

Author Contributions

A. Salgado carried out the literature review, designed the solution, analyzed the results, and wrote the manuscript. Y. Donoso defined the problem, supervised the work, and contributed to the manuscript writing.

Conflict of Interest

The authors declare no conflict of interest.

Supporting Information

The detailed implementation of this paper, including all simulated scenarios and results, can be found in the thesis of A. Salgado (2024), titled "Detección de fallos de integridad en sistemas de posicionamiento (GPS) de vehículos aéreos no tripulados (UAVs)," available at Universidad de los Andes. The source code for this work is available upon request. Full text available at: https://hdl.handle.net/1992/75192.

References

[1] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned aerial vehicles (uavs): practical aspects, applications, open challenges, security issues, and future trends," *Intelligent Service Robotics*, vol. 16, no. 1, pp. 109–137, 2023.

[2] Y. Wencheng, W. Song, Y. Xuefei, W. Xu, and H. Jiankun, "A review on security issues and solutions of the internet of drones," *IEEE Open Journal of the Computer Society*, vol. 3, pp. 96–110, 2022.

[3] F. A. Colombiana. (2022, October 4) Fuerza aeroespacial colombiana asi se va a las estrellas. Último acceso: 10 Febrero 2024. [Online]. Available: https://www.fac.mil.co/es

[4] S. Wasswa, M. S. Mojtaba, and S. Fawad, "Cybersecurity in unmanned aerial vehicles: a review," *SCIENDO - INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS*, vol. 16, no. 1, 2023.

[5] A. Abbaspour, K. K. Yen, and A. Sargolzaei, "Detection of fault data injection attack on uav using adaptive," *Procedia Computer Science*, vol. 95, pp. 193–200, 2016.

[6] P. Misra and P. Enge, *Global Positioning System.* Lincoln, Mass.: Ganga-Jamuna Press, 2006.

[7] J. Nemus. (2014, March 7) Errores mediciones gps. Último acceso: 10 Marzo 2024. [Online]. Available: http://fjalejandre.blogspot.com/2014/03/erroresmedicionesGPS.html

[8] R. Rifandi, S. F. Assagaf, and Y. D. Windy, "An insight about gps," *Utrecht University*, 2013.

[9] B. D. Deebak and F. Al-Turjman, "A smart lightweight privacy preservation scheme for iot-based uav communication systems," *Comput Commun*, vol. 162, pp. 102–117, 2020.

[10] K. Wen, S. Wang, Y. Wu, J. Wang, L. Han, and Q. Xie, "A secure authentication protocol supporting efficient handover," *E mathematics*, vol. 12, p. 716, 2024.

[11] F. Jahan, W. Sun, and A. Y. Javaid, "Analysis of global positioning system-based attacks and a novel global positioning system spoofing detection/mitigation algorithm for unmanned aerial vehicle simulation," *SIMULATION: Transactions of The Society for Modeling and Simulation International*, pp. 1–15, 2017.

[12] C. W. Staff. (2011) Obama says u.s. has asked iran to return drone aircraft. [Online]. Available: https://www.cnn.com/2011/12/12/world/meast/iran-us-drone

[13] K. Hartmann and C. Steup, "The vulnerability of uavs to cyber attacks - an approach to the risk assessment," in *2013 5th International Conference on Cyber Conflict*, 2013.

[14] S. Zhang, Y. Liu, Z. Han, and Z. Yang, "A lightweight authentication protocol for uavs based on ecc scheme," *drones MDPI*, 2023.

[15] X. Wei, C. Sun, M. Lyu, Q. Song, and Y. Li, "Constdet: Control semantics-based detection for gps spoofing attacks on uavs," *remote sensing MDPI*, vol. 14, no. 21, pp. 55–87, 2022.

[16] K. T. Seferoglu and A. S. Turk, "Review of spoofing and jamming attack on the global navigation systems band and countermeasure," in *9th International Conference on Recent Advances in Space Technologies (RAST)*, 2019.

[17] D. Goward. (2024, January 31) As baltics see spike in gps jamming, nato must respond. [Online]. Available: https://www.breakingdefense.com/2024/01/as-baltics-see-spike-in-gps-jamming-nato-must-respond

[18] E. Howell. (2022, April 14) How russia's gps satellite signal jamming works, and what we can do about it. [Online]. Available: https://www.space.com/gps-signal-jamming-explainer-russia-ukraine-invasion

[19] S.-J. Lee, Y.-R. Lee, S.-E. Jeon, and I.-G. Lee, "Machine learning-based jamming attack classification and effective defense technique," *Computers & Security*, vol. 128, pp. 103–169, 2023.

[20] S. Z. Khan, M. Mohsin, and W. Iqbal, "On gps spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions," *PeerJ Comput Sci*, vol. 7, 2021.

[21] A. Kumar and G. Petropolous, "Application of gps and gnss technology in geosciences," *GPS and GNSS Technology in Geosciences*, 2021.

[22] M. Ahmad, S. Ahmed, and S. Shahid, "Impact and detection of gps jammers and countermeasures against jamming," *International Journal of Scientific and Engineering Research*, vol. 9, no. 12, 2018.

[23] T. K. Mohd and E. M. Tesfa, "Exploring technical capabilities of unmanned aerial vehicles," in *IEEE Annual Computing and Communication Workshop and Conference (CCWC)*, 2023.

[24] S. Khandelwal. (2016, April 1) Hacker hijacks a police drone from 2 km away with $40 kit. [Online]. Available: https://thehackernews.com/2016/04/hacking-drone.html

[25] H. J. Hadi, Y. Cao, K. U. Nisa, A. M. Jamil, and Q. Ni, "A comprehensive survey on security, privacy issues and emerging defence technologies for uavs," *Journal of Network and Computer Applications*, vol. 213, 2023.

[26] R. Aissaoui, J.-C. Deneuville, C. Guerber, and A. Pirovano, "A survey on cryptographic methods to secure communications for uav traffic management," *Vehicular Communications*, vol. 44, 2023.

[27] C. Rametta, F. Beritelli, R. Avanzato, and M. Russo, "A smart vpn bonding technique for drone communication applications," in *15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2019.

[28] E. Ntizikira, W. Lei, F. Alblehai, K. Saleem, and M. A. Lodhi, "Secure and privacy-preserving intrusion detection and prevention in the internet of unmanned aerial vehicles," *Security in IoT Environments*, vol. 23, no. 19, 2023.

[29] M. Taylor, J. Boubin, H. Chen, and C. Stewart, "A study on software bugs in unmanned aircraft systems," in *International Conference on Unmanned Aircraft Systems*, Athens, Greece, 2021.

[30] U. Pravda. (2024, February 8) Cyber-attack by ukrainian defence intelligence: large-scale failure of russian drone control program occurs. [Online]. Available: https://www.pravda.com.ua/eng/news/2024/02/8/7440974/

[31] J. W. Seo, A. Islam, M. Masuduzzaman, and S. Y. Shin, "Blockchain-based secure firmware update using an uav," in *ICTC 2022*, vol. 12, 2023.

[32] A. I. Khan and Y. Al-Mulla, "Unmanned aerial vehicle in the machine learning environment," in *The 10th International Conference on Emerging ubiquitous Systems and Pervasive Networks*, 2019.

Copyright ©2025 by the authors. Licensee Agora University, Oradea, Romania.
This is an open access article distributed under the terms and conditions of the Creative Commons Attribution-NonCommercial 4.0 International License.
Journal's webpage: http://univagora.ro/jour/index.php/ijccc/

This journal is a member of, and subscribes to the principles of,
the Committee on Publication Ethics (COPE).
https://publicationethics.org/members/international-journal-computers-communications-and-control

Cite this paper as:

Salgado, A.; Donoso, Y. (2025). Detection of Integrity Failures in GPS Systems of Unmanned Aerial Vehicles (UAVs), *International Journal of Computers Communications & Control*, 20(3), 7051, 2025.

https://doi.org/10.15837/ijccc.2025.3.7051