ISSN 2075-1087, Gyroscopy and Navigation, 2025, Vol. 16, No.1, pp. 40-55.
Russian Text © The Author(s), 2025, published in Giroskopiya i Navigatsiya, 2025, No.1, pp. 64–90.

Fault Tolerant and Cyber Resilient Formation Control of Multiple UAVs

Hasan Shouib[a], Majd Saied[a,b*], Clovis Francis[c], Hassan Shraim[a] and Ziad Noun[b]

[a]*Scientific Research center in Engineering, Faculty of engineering, Lebanese University, Hadath, Lebanon*
[b]*Lebanese International University, Faculty of Engineering, Bekaa, Lebanon*
[c]*Arts et Métiers PariTech, Campus de Châlons en Champagne, France*
**e-mail: majd.elsaied@ul.edu.lb*
Received: September 14, 2024; revised January 14, 2025; accepted April 1, 2025

Abstract: In recent times, there has been a notable increase in the use of Unmanned Aerial Vehicles (UAVs) worldwide, driven by a growing demand for their versatile applications across various domains. However, alongside their beneficial applications, there has been a concerning emergence of malicious UAVs use by cyber criminals. These unauthorized activities pose significant risks, with the potential for destructive consequences. Consequently, there is a pressing need for the development and implementation of detection, protection, and prevention measures to mitigate these threats effectively.
The primary objective of this paper is to explore the evolving risks associated with cyber-attacks in formation flights of UAVs, along with the corresponding countermeasures aimed at tolerating such threats. The work proposes a hybrid fault diagnosis scheme and fault-tolerant cooperative controllers for multiple UAVs under faults and cyber attacks. The proposed hybrid fault diagnosis scheme combines rule-based and model-based approaches. Three realistic attack scenarios are simulated including the Man-in-the-Middle attack and the GPS spoofing. The results show that the proposed scheme is able to ensure the safe operation of UAVs in the fleet by effectively diagnosing faults and enabling proactive measures to mitigate potential risks.

Keywords: unmanned aerial vehicles, formation control, cybersecurity, fault tolerance.

1. INTRODUCTION

In our ever more digital world, cybersecurity has become crucial, covering a wide range of technologies and applications. Among these, unmanned aerial vehicles (UAVs) have as an innovative technological tool finding wide-ranging uses in delivery services, inspection and surveillance. As UAVs progress towards greater autonomy, ensuring their cybersecurity becomes paramount. Cyberthreats pose significant risks to the safety, functionality and integrity of these UAVs [1]. The need to tackle the challenges related to coordinating and controlling individual or fleets of these UAVs under cyberthreats becomes increasingly imperative [2].

The operation of unmanned aerial vehicles depends on advanced software, wireless communication networks, and data exchange protocols, rendering them vulnerable to cyberthreats. A significant worry in UAV cybersecurity is its susceptibility to hijacking [3]. This attack involves gaining unauthorized control over the UAV's command and control system. Attackers may exploit vulnerabilities in the communication protocols or compromise the authentication mechanisms to take control of the UAV. Once hijacked, the attacker can manipulate the UAV's movements, actions, and payload, potentially posing a threat to public safety, privacy, or sensitive areas. Another challenge lies in file/media access where the attack goal focuses on unauthorized access to the files and media stored within the UAV's systems [4]. UAVs often capture and store data such as images, videos, or sensor readings. Attackers may attempt to gain access to these files for various purposes, such as extracting sensitive information, compromising privacy, or obtaining valuable intellectual property. Unauthorized file/media access can lead to data breaches, privacy violations, or misuse of captured information. Crash/land is another type of attack that can be particularly dangerous if the UAV is in a sensitive location or performing critical tasks [5]. By compromising the UAV's control system, attackers may force the UAV to crash into obstacles, buildings, or other objects, causing property damage or injury. Alternatively, they may attempt to remotely land the UAV in an unauthorized location, which

can lead to the loss of the UAV or to compromise its sensitive payloads. Furthermore, eavesdropping attack is another concern to consider [6]. It involves intercepting and listening to the wireless communications between the drone and the ground control station. Attackers may exploit vulnerabilities in the communication protocols or use specialized equipment to capture and analyze the transmitted data.

These threats require the development of robust and effective diagnosis systems that can detect, mitigate, and recover from cyberattacks and faults in real-time. Such systems are crucial for ensuring the reliability, stability, and continued functionality of the fleet, as well as mitigating potential risks to the surrounding environment and human operators.

In this paper, we delve into the vulnerabilities arising from message modification in the communication channel between the ground station and UAVs. We explore the detrimental effects that such attacks can have on the overall functioning of UAV fleets operating in close coordination. Additionally, we consider the impact of sensor faults and actuator faults on the reliability and performance of these systems.

This paper presents a small overview of the cyberthreats faced by UAVs and proposes a hybrid fault-tolerant control (FTC) for a formation of multiple unmanned aerial vehicles in the presence of physical faults actuators and sensors faults and cyberattacks. The Artificial Bee Colony (ABC) algorithm is used for the formation control.

The main contributions of this paper are summarized as:

- Simulation and analysis of three attack scenarios against a hexarotor in a fleet, including deceptive and multiplicative/additive Man-in-the-Middle (MITM) attacks and a GPS spoofing attack. The literature review reveals that cyber attacks against UAVs, particularly spoofing and man-in-the-middle attacks, are prevalent and can have severe consequences. The analysis involves investigating the vulnerabilities and potential risks associated with these attacks.
- Development and simulation of a hybrid fault-tolerant and cyber-resilient formation control for multiple unmanned aerial vehicles using a combination of rule-based and model-based approaches. By leveraging analytical models and predefined features associated with the signatures of known attack patterns, the detection system can efficiently identify and respond to cyber-attacks. This novel control system ensures coordinated movements and enhances fault tolerance capabilities within the UAV fleet.

The remaining of this paper is organized as follows. Section II reviews cyber attack types, vulnerabilities, and existing countermeasures. Section III analyzes physical faults and cyberattacks in a formation control system. It focuses on three attack scenarios targeting a single UAV within a fleet. The proposed hybrid FTC scheme is described in Section IV alongside with the formulations of the rule-based and model-based units. Section V discusses the simulation results. Finally, the conclusions are drawn in Section VI.

2. CYBER ATTACKS ON UNMANNED AERIAL VEHICLES AND CYBER COUNTERMEASURES

This section provides an overview of the common cyber attacks encountered by UAVs and the adopted countermeasures proposed in the literature. Understanding these attacks is essential for developing effective countermeasures and ensuring the safe and reliable operation of UAV systems.

2.1. Cyber Attacks on UAV Systems

The cyberattacks that can occur on UAV systems include GPS spoofing [7], GPS Jamming [8], Man In The Middle [9], WiFi Deauthentification [10], Denial of Service [11] and Deception Attack [12].

GPS spoofing emerges as the prevailing and most extensively studied cyber-attack on small unmanned aerial systems. It stands out as the most common and well-known mean of attack, with two documented incidents found in [13–14]. GPS spoofing against a UAV is a technique in which the GPS receiver on the UAV is tricked into receiving false GPS signals, causing the vehicle to deviate from its intended course or location. This can be achieved by broadcasting fake GPS signals that appear to be coming from a legitimate GPS satellite but with altered information about the location, time, or identity of the satellite. As a result, the UAV may be misled into thinking it is at a different location than it actually is, or following a different flight path than intended. This can lead to potentially dangerous situations such as collisions, crashes or unauthorized access to sensitive areas. After a UAV is compromised and hijacked, then the very

same UAV can act as a mobile stealth spoofer against other targets [8]. To mitigate the risk of GPS spoofing, UAVs can be equipped with anti-spoofing technologies such as multi-sensor navigation systems, signal authentication, or frequency diversity.

The man-in-the-middle attack is a type of cyber attack where an attacker intercepts the communication between the UAV and its ground control station (GCS) and inserts himself as a middleman [9]. The attacker can then manipulate the communication between the UAV and the GCS, either by modifying data, injecting false data or commands, or blocking legitimate data or commands. The attackers can even enter their false data within the same structure of correct data [15].

The deception attacks can be categorized into two types: node attacks and communication path attacks [12]. In a node attack, malicious data manipulates the control input of a UAV, affecting its behavior. Communication path attacks involve injecting deceptive data into the information broadcasted from a compromised UAV node. These attacks pose risks to UAV systems, compromising control, navigation, and communication, and require detection and mitigation for secure and reliable operation.

2.2. Cyber Countermeasures

Various countermeasures have been proposed in the literature to mitigate the risks posed by cyber-attacks on UAV systems. These countermeasures aim to enhance the security and resilience of UAV systems against different attack vectors.

In [16] the authors proposed a cyber detection system for UAV networks to prevent dangerous and potentially lethal attacks. The system is based on Intrusion Detection Systems (IDS) and aims to protect data integrity and network availability. It employs specific detection policies to promptly identify and detect cyber attacks. The system utilizes an intrusion detection technique to identify malicious UAVs and incorporates a threat estimation model based on a Belief approach to reduce false positive and negative rates.

The key mechanisms of IDSs can be classified into four categories:

- Specification based [17]: In this approach, a UAV-IDS incorporates rules that are specified based on the expected behaviors of UAVs. These rules are applied to monitor the successful executions of the UAV system. By checking if the observed behavior aligns with the specified rules, deviations can be detected and flagged as potential intrusions.
- Signature based [18]: This method aims to detect known attacks by using predefined known signatures. The IDS compares the observed activities with the signatures in its database. When anomaly activities are detected, a detection operation is triggered to identify a matched signature, indicating the presence of an intrusion.
- Anomaly based [19]: Anomaly behavior detection focuses on identifying failures or illegal activities observed in a system. This method can detect both known and unknown attacks by using learning or filtering mechanisms. By establishing a baseline of normal behavior, any deviations from this baseline are considered anomalies and may indicate the presence of an intrusion.
- Hybrid based [20]: The hybrid approach integrates two or more detection methods, such as specification and anomaly-based techniques. By combining multiple detection methods, a hybrid IDS can provide a stronger detection policy that is capable of detecting both known and unknown attacks. This approach leverages the strengths of different detection mechanisms to enhance overall system security.

Several researchers considered the more challenging case of Intrusion Detection Systems for multiple UAVs. The detection process for such attacks is conducted at the base station level, where UAVs periodically transmit collected data for analysis. It is expected that all UAVs in the same area should report the same phenomena [21]. Therefore, the detection strategy relies on this observation to identify infected UAVs. A Mahalanobis distance was employed to recognize malicious UAVs that transmit erroneous data to the base station in [16]. The most widely recognized threat to network availability is DoS attacks. In the case of wormhole attacks, the authors in [16] proposed a strategy to detect the malicious UAV. The detection that takes place at the base station level is based on the calculation of the Message Dropping Rate (MDR) from the packets received from UAVs. The base station identifies a UAV node with a higher MDR compared to its neighboring UAVs as a potential perpetrator of a wormhole attack. Moreover, the computation of threat level in this research uses the Belief approach, which is particularly suitable for accu-

rately determining the behavioral patterns of monitored UAVs, and distinguishing between normal and malicious nodes [22].

In another proposed approach [23], the IDS design uses simple specification-based behavior rules for each UAV. These rules are designed to detect insider attackers who exploit vulnerabilities in embedded sensors or actuators. The authors provide specific behavior rules used to detect a malicious UAV, such as identifying unauthorized deployment of landing gear when the UAV is outside its designated air base. This behavior indicator effectively detects attackers attempting to take control of the UAV by manipulating its landing gear module.

A review on the cyber security analysis of UAV systems including the attacks, limitations, and recommendations is provided in [24].

3. PHYSICAL FAULTS AND CYBER ATTACKS IN A FORMATION CONTROL SYSTEM

In this paper, we focus on three scenarios of cyber attacks targeting a single UAV among a fleet of six UAVs. The aim is to address the challenges posed by these faults and attacks through the development of intelligent detection methods and the integration of formation fault-tolerant and cyber-resilient controllers for UAVs.

Two types of attacks are adopted in this paper. The first one involves modifying the transmitted position of the UAV, while the second type focuses on GPS spoofing against a specific UAV within a fleet. Each type includes multiple attack forms. To simulate them, we use MITM attacks to compromise the communication channels. By gaining control over the communication channels, we can manipulate the UAV's position or spoof GPS signals to deceive the targeted UAV [25].

To implement the proposed attacks, we rely on several basic assumptions outlined below:

- A1: An attacker has basic abilities of calculation, information storage, and communication.
- A2: The attacker can intercept the communication channel between the UAVs and the ground station. It can modify or replace the control information and transmit the elaborate control information to the ground station.
- A3: Before attacks, the UAVs keep the desired formation shape and move toward predefined destinations.

To induce physical effects on the UAV formation, these attacks concentrate on manipulating the positions and velocities of UAVs. The position attacks can cause UAVs to deviate from desired positions. In general, the position attacks can hijack vehicle swarm to a predefined region. However, whenever using a formation algorithm based on metaheuristic optimization, the attacker cannot hijack the UAV to another target point because the optimization algorithm drives the UAVs around a fixed point (defined by the operator) where it is not transmitted within the communicated data between UAVs and the ground station. Then it only could cause the entire formation to break down and possibly lead to a collision or other safety hazards.

3.1. Attack Scenario 1: GPS Spoofing attack against one UAV

We consider a scenario where a GPS spoofing attack is generated against one UAV within the fleet, which involves sending fake GPS signals to the targeted UAV, causing it to believe that it is in a different location than it actually is. This can lead the attacked UAV to send incorrect position information to the ground station, which can cause the entire fleet to become misaligned disrupting the formation's overall shape and trajectory. This can also increase the risk of collision between the UAVs. However, in a perfect scenario, where the GPS spoofing attack is highly precise and only affects the targeted UAV, the minimum circle diameter the UAVs formed on would need to be large enough to ensure that the signals from the legitimate GPS satellites are not reaching the nearby UAVs.

To mitigate the effects of the GPS spoofing attack, an integrated countermeasure system is employed:

- State Observer Integration: A non-linear state observer is used to estimate the UAV's position $\hat{P} = [\hat{x}, \hat{y}]$ based on its kinematic model.
- Data Comparison: Let $P_{GPS} = [x_{GPS}, y_{GPS}]$ denote the position provided by the GPS sensor, and $P_{ACC} = [x_{ACC}, y_{ACC}]$ the position calculated from the accelerometer. The system compares P_{GPS}, P_{ACC} and the estimated position $\hat{P}$ using the following criteria:

$$|x_{GPS} - x_{ACC}| > \delta_x \text{ and } |y_{GPS} - y_{ACC}| > \delta_y \quad (1)$$
$$|x_{ACC} - \hat{x}| \le \epsilon_x \text{ and } |y_{ACC} - \hat{y}| \le \epsilon_y,$$

where δ_x, δ_y, ϵ_x and ϵ_y are thresholds.

- Priority Assignment: If the above conditions are satisfied, the accelerometer-based data P_{ACC} is prioritized over the GPS-based data P_{GPS}.

By employing this method, the system swiftly identifies and counteracts GPS spoofing attacks, preventing significant fleet misalignment or collisions. This approach ensures enhanced reliability and operational safety for the UAV fleet.

3.2. Attack Scenario 2: Deception Attack (MITM)

When a deception attack occurs on the communication path, the malicious data will be injected into the information broadcasted from the affected UAV node [12]. We suppose that the attacker can intercept and modify the communication link between the UAV and the ground station. This can be achieved by using a man-in-the-middle attack to intercept and modify the data packets. The attacker modifies the position information of the UAV, $P_{UAV} = [x, y]$ and sends incorrect location data to the ground station, $P_{UAV}^{attacked} = P_{UAV} + [\Delta x, \Delta y]$ with Δx and Δy being the injected malicious offsets, causing it to calculate the desired positions in the formation based on wrong information. The other UAVs then receive incorrect position information, they will adjust their own positions based on this data. This could lead to an increased risk of collision between the UAVs, which can be dangerous and cause damage or injury.

To mitigate the effects of a deception attack, the following countermeasure is implemented:

- State Observer Integration: A non-linear state observer estimates the actual position of the UAV, denoted as $\hat{P} = [\hat{x}, \hat{y}]$, based on the UAV's kinematic model.
- Residual-Based Detection: The system evaluates the residuals between the estimated position $\hat{P}$ and the transmitted position $P_{UAV}^{attacked}$ stored in the neighbor matrices of other UAVs. An attack is flagged if:

$$\begin{aligned} |\hat{x} - x_{neighbor}| > \delta_x \\ |\hat{y} - y_{neighbor}| > \delta_y \end{aligned}, \quad (2)$$

where δ_x and δ_y are the detection thresholds.

- Observer-Based Data Substitution: Upon detecting an attack, the estimated position $\hat{P}$ replaces the transmitted data $P_{UAV}^{attacked}$ in the ABC algorithm for fleet position updates.

3.3. Attack Scenario 3: Multiplicative/Additive (MITM)

This attack scenario focuses on analyzing and mitigating hybrid attacks that target the desired trajectory of the UAV. These attacks include both multiplicative attacks, denoted as $Ø P_{desired}$, and additive attacks, denoted as X_a [26].

$$P_{manipulated} = Ø P_{desired} + X_a. \quad (3)$$

where:

$$\begin{cases} Ø = 1 \ \& \ X_a \neq 0 \text{ for additive attacks} \\ Ø \neq 1 \ \& \ X_a = 0 \text{ for multiplicative attacks} \end{cases}.$$

The inclusion of multiplicative attacks is motivated by the fact that attackers can potentially infiltrate the computing platform and generate such signals. Additive attacks, on the other hand, encompass various types such as unknown bias attacks and harmonic attacks with unknown phase and amplitude. The transmitting and computing platform is vulnerable to compromise by attackers, leading to severe manipulation of the desired trajectory data.

The following countermeasure system is employed to detect trajectory manipulation attacks, such as additive or multiplicative modifications to the desired trajectory $P_{desired} = [x_{desired}, y_{desired}]$, transmitted from the ground station to the UAV. The estimated trajectory using the observer state estimator is denoted as $\hat{P} = [\hat{x}, \hat{y}]$. An attack is detected if the discrepancy between the transmitted trajectory and the estimated trajectory exceeds a predefined threshold:

$$\begin{aligned} |\hat{x} - x_{desired}| > \delta_x \\ |\hat{y} - y_{desired}| > \delta_y \end{aligned}. \quad (4)$$

This criterion enables the identification of deviations caused by additive or multiplicative attacks on the transmitted trajectory data. To mitigate the effects of detected attacks, the following countermeasures are executed:

- Packet Transmission: Two packets of information are generated at the ground station: 1) $P_{nearest,true}$: True desired trajectory intended for the nearest UAV *i* in proximity to the at-

tacked UAV. 2) P_{true} : True desired trajectory for the attacked UAV.

- Packet Content: For the nearest UAV *i*, the transmitted packet ensures it receives the correct trajectory unaffected by the manipulation: $P_{nearest,true} = P_{i,desired}$. For the attacked UAV, the packet overrides the manipulated trajectory and restores the true desired trajectory: $P_{true} = P_{desired}$.
- System Security and Fleet Coordination: By transmitting corrected trajectory information to the affected UAVs, the system preserves the integrity of fleet coordination. This approach ensures that UAVs follow their intended paths, avoiding misalignment or collision risks.

4. HYBRID FAULT DIAGNOSIS SCHEME

In this paper, a hybrid diagnosis system is proposed and relies on rule-based and model-based approaches. The rule-based approach leverages predefined rules and expert knowledge to detect and diagnose faults and attacks, while the model-based approach utilizes system models and algorithms to analyze system behavior and identify deviations from expected norms [27]. The integration of both rule-based and model-based approaches enables a comprehensive and effective diagnosis system for UAVs. Rapid detection and diagnosis of faults and attacks provide the necessary information to the fault-tolerant and cyber-resilient controllers, allowing them to take appropriate actions to mitigate the effects of these events in real time.

4.1. State Observer Design

In the context of generating residuals for fault and attack detection, it is crucial to design an effective state observer that can accurately reconstruct or estimate the state or output vector of the system. These residuals serve as indicators of faults or attacks within the system. Deviations between the estimated and actual outputs beyond a certain threshold can be indicative of anomalies, and further analysis will be performed to identify and diagnose the underlying issues. The UAV system model can be expressed in state space representation as follows:

$$\dot{X} = AX + Bu + H\left(X\right). \tag{5}$$

With $X = \left[x\, y\, z\, \dot{x}\, \dot{y}\, \dot{z}\, \phi\ \theta\ \psi\ \dot{\phi}\dot{\theta}\ \dot{\psi} \right]^T$ being the state vector including the positions *x*, *y*, *z* and angular roll ϕ pitch θ and yaw ψ orientations with their derivatives and $u = \left[U\, \tau_\phi\ \tau_\theta\ \tau_\psi \right]^T$ is the input vector consisting of the total thrust *U* and the three roll, pitch and yaw torques respectively.

$$A = \begin{bmatrix} \mathbf{0}_{3\times3} & \boldsymbol{I}_{3\times3} & \mathbf{0}_{3\times3} & \mathbf{0}_{3\times3} \\ \mathbf{0}_{3\times3} & \mathbf{0}_{3\times3} & \mathbf{0}_{3\times3} & \boldsymbol{I}_{3\times3} \\ \mathbf{0}_{3\times3} & \mathbf{0}_{3\times3} & \mathbf{0}_{3\times3} & \mathbf{0}_{3\times3} \\ \mathbf{0}_{3\times3} & \mathbf{0}_{3\times3} & \mathbf{0}_{3\times3} & \mathbf{0}_{3\times3} \end{bmatrix} \text{ and}$$

$$B = \begin{bmatrix} & \mathbf{0}_{3\times4} & \\ \frac{1}{m} & 0 & 0 & 0 \\ \frac{1}{m} & 0 & 0 & 0 \\ \frac{1}{m} & 0 & 0 & 0 \\ & \mathbf{0}_{3\times4} & \\ 0 & \frac{1}{J_x} & 0 & 0 \\ 0 & 0 & \frac{1}{J_y} & 0 \\ 0 & 0 & 0 & \frac{1}{J_z} \end{bmatrix}$$

are the state and input matrices of the linearized UAV model with $\mathbf{0}_{3\times3}$ and $\boldsymbol{I}_{3\times3}$ being the 3×3 identity and zero matrices. I_x, I_y and I_z are the hexarotor moments of inertia around the *x*, *y* and *z* axes, *m* is the mass and *g* is the acceleration due to gravity.

$$H = \left[\mathbf{0}_{5\times1} \quad 0 \quad -g \quad 0_{3\times1} \quad \frac{J_y - J_z}{J_x}\dot{\theta}\dot{\psi} \quad \frac{J_z - J_x}{J_y}\dot{\phi}\dot{\psi} \quad \frac{J_x - J_y}{J_z}\dot{\phi}\dot{\theta} \right]^T.$$

is the vector describing the nonlinearities of the model [28]. *X* is the state vector consisting of the position, attitude and altitude variables, and *u* the input vector consisting of the input thrust and the three input torques.

The observer model is given by:

$$\begin{aligned} \hat{\dot{X}} &= A\hat{X} + Bu + H\left(X\right) + K\left(Y - C\hat{X}\right) \\ \hat{Y} &= C\hat{X} \end{aligned}. \tag{6}$$

Two consecutive observers, one for the attitude and one for the position and altitude, are designed with state and input vectors X_1, Y_1, X_2, Y_2 defined as below:

$$X_1 = \left[\phi\ \theta\ \psi\ \dot{\phi}\ \dot{\theta}\ \dot{\psi}\right]^T, X_2 = \left[x\ y\ z\ \dot{x}\ \dot{y}\ \dot{z}\right]^T$$
$$Y_1 = \left[\phi\ \theta\ \psi\right]^T, Y_2 = \left[x\ y\ z\right]^T \quad (7)$$

Note that the diagnosis process developed involves two distinct parts: the first part is executed within each individual UAV and the second one is executed at the ground station. Note that the state observers presented in this section are running on each individual UAV and at the ground station enhancing the diagnosis at both parts of the fleet system.

4.2. Diagnosis unit within each individual UAV

The fault diagnosis scheme proposed in this section is based on a fuzzy logic unit to assess the degree of faults and the capability of each UAV to perform its task within the team. Its primary objective is to enable the detection of sensor and actuator faults within a system and subsequently compensate for any loss or degradation caused by these faults, whenever feasible. It aims to identify deviations from expected sensor readings and actuator responses. Once a fault is detected, the algorithm endeavors to mitigate its impact by implementing appropriate compensation strategies taking into consideration the following assumptions [29]:

- Assumption 1: Each vehicle in the fleet is equipped with its own fault detection and tolerance scheme to detect faults and to determine its ability to complete the mission.
- Assumption 2: Each vehicle sends a package of information, including their states, positions, velocities, and fault degrees, to the ground station.
- Assumption 3: Each vehicle in the fleet possesses its own fuzzy logic controller to determine the degree of the fault and send it to the ground station to decide whether to continue the mission or abort it.

4.2.1. Case of a Sensor Fault Detection

In this part we consider the case of faults on the accelerometer sensor. The hexarotor UAV heavily relies on accelerometer readings to extract angular acceleration, which is then used to calculate the roll (ϕ) and pitch (θ) angles as below:

$$\phi = \arctan\frac{a_y}{a_z}, \quad (8)$$

$$\theta = \arctan\left(-\frac{a_x}{\sqrt{a_y^2 + a_z^2}}\right), \quad (9)$$

Where a_x and a_y represent the accelerometer readings along the x and y axes respectively.

Therefore, any erroneous readings or faults in the accelerometer can significantly impact these angles, subsequently affecting the behavior of the drone. Such deviations can potentially lead to disastrous outcomes. Thus, it is crucial to ensure the accuracy and reliability of the accelerometer measurements to maintain the stability and safe operation of the hexarotor UAV. To overcome these faults and mitigate their impact on the hexarotor UAV's stability, the designed observer mentioned earlier is utilized. This observer estimates the roll $\hat{\phi}$ and pitch $\hat{\theta}$ angles based on available sensor data (the accelerometer readings). By comparing the estimated angles with the actual ones obtained from the accelerometer, any discrepancies can be detected:

$$\Delta\phi = \phi - \hat{\phi}$$
$$\Delta\theta = \theta - \hat{\theta} \quad (10)$$

If the discrepancies $\Delta\phi$ and $\Delta\theta$ exceed predefined thresholds, this indicates a potential fault in the accelerometer readings. In such cases, the observer's estimated angles $\hat{\phi}$ and $\hat{\theta}$ are used within the control system as a reliable substitute for the faulty sensor data. This approach ensures that the hexarotor UAV can continue to operate safely and maintain stability even in the presence of sensor faults.

4.2.2. Case of a Motor Fault Detection

To isolate a faulty motor in a hexarotor UAV, a monitoring approach based on observing the behavior of each angle (ϕ, θ, and ψ) is employed. This approach leverages the fact that a motor failure will result in a distinct and significant deviation in the drone's reaction compared to the other five functioning motors. By continuously monitoring the angles ϕ, θ, and ψ, deviations or abnormal behavior in these angles can be detected. A motor failure will cause an imbalance in the forces generated by the rotors, leading to an altered response in the UAV's orientation. Since each motor contributes to the

overall balance and stability of the UAV, a malfunctioning motor will cause a noticeable difference in the angles as depicted in [30].

4.2.3. Fault-Tolerant Control and System Recovery

To achieve system recovery we conducted, in a previous work, a controllability analysis [31] in a hexarotor UAV when one or more actuators fail. The analysis focuses on two hexarotor configurations: PPNNPN and PNPNPN, representing the direction of rotation of each motor (P for Positive, N for Negative). The controllability study reveals that the hexarotor UAV with a PNPNPN configuration is not controllable in the event of single or multiple actuator failures. Therefore, this configuration is unsuitable for fault-tolerant control studies. On the other hand, the PPNNPN configuration remains controllable only in the case of seven expected actuator failure scenarios. However, if the number of faulty motors exceeds two, the system becomes uncontrollable.

The objective of a reconfigurable control system in the event of a motor failure in a multirotor is to redistribute the control effort among the remaining functioning motors to maintain stability and satisfactory performance. In [31], we used an offline Nonlinear Constrained Optimization approach to set a predefined laws to drive the healthy motors based on the detected faulty situation. To facilitate the reconfiguration process and to ensure ease of implementation and testing, a lookup table with mixer gains is pre-calculated, taking into account the anticipated failure scenarios.

The decision to reconfigure the fleet is taken at the ground station based on two main constraints, the degree of damage of the unhealthy vehicle $\gamma \in [0,1]$ and the vehicle's ability to perform its task $\delta \in [0,1]$. The output of the fuzzy logic controller determines whether the unhealthy UAV should leave the fleet, triggering the remaining team members to reconfigure into a new formation, or if the unhealthy UAV should continue in the formation phase to complete its mission. The UAV transmits these two signals to the ground station, defining their state of health to take action. The fuzzy logic controller scheme is employed by each UAV as follows:

1) Degree of damage of the unhealthy vehicle γ
a) H for Healthy: $\gamma \le 20\%$
b) LD for Low Damage: $21\% \le \gamma \le 40\%$
– Stands for sensors faults
c) MD for Medium Damage: $41\% \le \gamma \le 60\%$
– Stands for 1 motor failure
d) SD for Severe Damage: $61\% \le \gamma \le 80\%$
– Stands for 2 motors failures
e) CD for Complete Damage: $81\% \le \gamma \le 100\%$
– Stands for uncontrollable damage (such as battery power loss, more than two motor failures…).
2) The vehicle's ability to perform its task δ
a) Sensor fault stands for $\delta = 1$
b) For 1 motor failure:
– For controllable motors cases: $\delta = 1$ else $\delta = 0$
c) For 2 motors failures:
– For controllable motors cases: $\delta = 1$ else $\delta = 0$.

Note: If $\delta = 1$ then the UAV is able to resume its mission.

4.3. Diagnosis unit at the ground station

At the ground station, an architecture is developed to detect and make decisions regarding the type of attack present and appropriate actions to be taken. τ is the signal used within the cost function such that:

$$\begin{cases} \tau = 0, \text{ Reconfigure} \\ \tau = 1, \text{ Complete mission} \end{cases}. \quad (11)$$

The two algorithms implemented at this level are detailed in Fig. 1 and Fig. 2.

It is noted that:

- The decision taken in attack scenarios 1 and 2 is to set the used position (X_i, Y_i) in the calculations of the fleet planning algorithm as the estimated values instead of the wrong delivered ones from the affected UAV.
- GPS spoofing alarm is a signal sent by the UAV revealing that there is a significant difference between the position calculated by the accelerometer and that given by the GPS sensor, such that the accelerometer measurements are compatible with the estimated position by the observer to make sure that the GPS sensor is faulty.
- P_{id} is the position desired induced by the fleet planning algorithm at the ground state and P_{ie} is the estimated position.
- A navigation packet will be forwarded to the malicious UAV which will notice that it is under attack from the AS3 signal sent within the packet, then the UAV will take the packet's desired positions instead of the malicious ones.

Algorithm .1: Attacks 1 & 2 Detection and Compensation

begin
  if $|Xi_{estimated} - Xi_{deliverd}| > \sigma$ || $|Yi_{estimated} - Yi_{delivered}| > \sigma$ & $AS3 = 0$ **then**
    /* Abnormal deviation is observed*/;
    if γ_i *is* H **then**
      /* UAV I is healthy, no faults exist*/;
      if *GPS spoofing alarm = 1* **then**
        /* Attack scenario 1 is detected */;
        /*Set the estimated position to be used in fleet planning algorithm calculations */;
        AS1=1;
        Set $Xi = Xi_{estimated}$ & $Yi = Yi_{estimated}$
      else
        /* Attack scenario 2 is detected */;
        AS2=1;
        Set $Xi = Xi_{estimated}$ & $Yi = Yi_{estimated}$
    else
      if $\delta_i = 1$ **then**
        /*UAV I is able to continue it's mission */;
        Set $\tau = 1$
      else
        /*Reconfigure */;
        Set $\tau = 0$
  else
    /*No risks in terms of attacks 1 & 2 */;

Fig. 1. Algorithm 1: Attacks 1 & 2 Detection and Compensation

Algorithm .2: Attack 3 Detection and Compensation

begin
  if $|Pi_d - Pi_e| > \rho$ **then**
    /* The UAV deviates from it's desired trajectory */;
    if γ_i *is* H **then**
      /* UAV I is healthy, no faults exist*/;
      if $AS1 = 0$ & $AS2 = 0$ **then**
        /* Attack scenario 3 is detected */;
        Set AS3=1;
        /* Send packet NP to the nearest UAV that consists of: */

$$\begin{cases} Xi_{desired} \\ Yi_{desired} \\ AS3 \end{cases}$$

      else
        /*Attack scenario 1 or 2 has been detected */;
    else
      if $\delta_i = 1$ **then**
        /*UAV I is able to continue it's mission */;
        Set $\tau = 1$
      else
        /*Reconfigure */;
        Set $\tau = 0$
  else
  /*No risk in terms of attack 3 */;

Fig. 2. Algorithm 2: Attack 3 Detection and Compensation.

5. SIMULATION AND RESULTS

In this work, we use the Artificial Bee Colony Algorithm for the formation control. A leaderless strategy is adopted and the formation control problem is formulated as an optimization task, which implies driving and positioning six hexarotor UAVs on a circle around a defined target point.

The Artificial Bee Colony algorithm [30] is inspired by the intelligent foraging behavior of honey bee swarms. It aims to solve nonlinear searching problems by simulating the behavior of a honey bee swarm in search of food sources. The algorithm consists of three groups of bees: employed bees, onlookers, and scouts. Each food source is associated with an employed bee, and the number of employed bees is equivalent to the number of food sources. Employed bees visit their food sources and communicate their findings through dance in the hive. Onlookers observe these dances and choose their food sources accordingly. If an employed bee's food source is abandoned, it becomes a scout and searches for a new food source. In the ABC algorithm, the position of a food source represents a possible solution to an optimization problem, and the nectar amount of a food source corresponds to the fitness of the associated solution. The number of employed bees and onlooker bees in the colony is equal to the number of solutions in the population.

In the following, we consider that a formation of six hexarotor UAVs is controlled by the ABC algorithm and we analyze the effects of the different attacks on the formation.

The multi-hexarotor system can be modeled as an undirected graph $G=(V,\mathcal{E})$, where the nodes $V=\{1,2,\dots N\}$ represent individual hexarotor UAVs, and the edges $\mathcal{E}$ represent the connections between pairs of agents [32]. Two nodes are considered adjacent if they are connected by an edge.

$$\Lambda_i(t)=\rho\left(|P_d-\left[\xi_i(t)+h\right]|-d_{ip}^d\right)+\sum_{\substack{j=1,\\ j\neq i}}^{N}k_j(t)\delta_{ij}(t)\left(\left|\xi_i(t)-\left[\xi_i(t)+h\right]\right|-d_{ij}^d\right) \quad (12)$$

with d_{ip}^d being the required distance between the vehicle and the rendezvous destination P_d. d_{ij}^d is the required distance between the vehicle i and its neighbor j, and $\xi_i(t)$ is the position vector of the UAV i. ρ is a constant greater than 1. This choice is verified by the need to orient each UAV_i position with the direction of P_d. $\delta_{ij}(t)$ is defined as:

$$\delta_{ij}(t)=1+e^{\frac{c-a_{ij}(t)}{\sigma}} \quad (13)$$

The value of $\delta_{ij}(t)$ depends on the difference between the distance between two UAVs, i and j, and the safety distance, c ($c>0$). It approaches 1 as the distance between the UAVs becomes equal to c. The parameter σ is a constant within the range $[0,1]$.

The main purpose resides in obtaining the best vector h for each UAV i that minimizes the cost function $\Lambda_i(t)$ and the desired trajectory P_{iref} for each UAV i at each time t_d will be:

$$P_{iref}(t+t_d)=P_{iref}(t)+h$$

The term $k_j(t)=\{0,1\}$ in the cost function describes the state of health of the UAV j.

The hexarotor considered in this work is shown in Fig. 3.

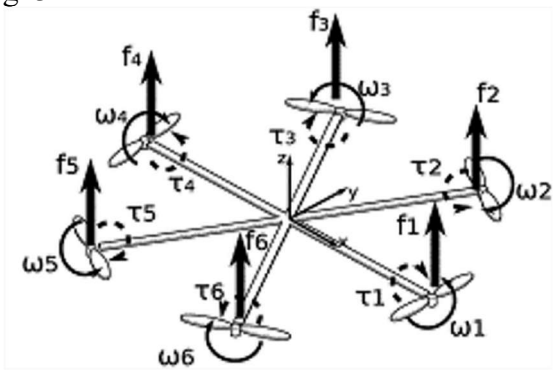


Fig. 3. The hexarotor UAV.

Its parameters are summarized as follows: m = 1.6 Kg, $J_x=J_y=0.0255$ Kg·m^2, $J_z=0.0388$ Kg·m^2 and arm length $L=0.23\ m$. The six hexarotors in the formation are tasked to form a circle of radius $r=6m$ centered at the point $P_d(15,10)$.

An adjacency matrix is defined as an $N\times N$ matrix, where the elements a_{ij} are 1 if a connection exists between two nodes i and j and 0 otherwise. The multi-hexarotor formation problem is formulated below where the cost function for each agent i is defined by the following expression:

5.1. Attack Scenario 1

The attack scenario 1 (GPS spoofing) targets a specific UAV within a fleet. The objective of this attack is to either remove the targeted UAV from the formation or cause collisions between drones. In the simulated example, we assume that the attacker's goal is to isolate hexarotor 1 from the fleet. To achieve this objective, the attacker manipulates the GPS sensor data of the targeted UAV. Specifically, the attacker alters the location information provided by the GPS sensor by shifting the x position by 4 meters and the y position by 5 meters, leading to a spoofed position as follows:

$$P_{spoofed}=\begin{bmatrix}x_1+4\\ y_1+5\end{bmatrix} \quad (14)$$

where $P_{spoofed}$ represents the position perceived by other UAVs and the ground station, and (x_1,y_1) is the true position of hexarotor 1. In this attack scenario, each hexarotor in the fleet perceives the position of hexarotor 1 as the spoofed GPS coordinates. For instance, hexarotor i will interpret hexarotor 1's position as:

$$neighbor_i(1,1:2)=P_{spoofed}=\begin{bmatrix}x_1+4\\ y_1+5\end{bmatrix} \quad (15)$$

where $i\in[2,3,4,5,6]$ and $neighbor_i$ represents the matrix that stores information about hexarotor i's five neighbors. Each row in $neighbor_i$ corresponds to a specific neighboring UAV, and each column stores relevant position and distance data for that neighbor. In $neighbor_i(1,1:2)$, the first index, 1, refers to the first row, which stores the position of hexarotor 1, and the indices 1:2 refer to the first two columns, which hold the x and y coordinates, re-

spectively. This deliberate manipulation of the GPS data misleads the UAV's navigation system. The UAV is tricked then into believing that its actual position is different from its intended position.

Figures 4a and 4b illustrate this situation, where the x and y positions of the UAV are simulated to be the manipulated (tricked) position after $t = 250\ s$, where the attack is initiated.

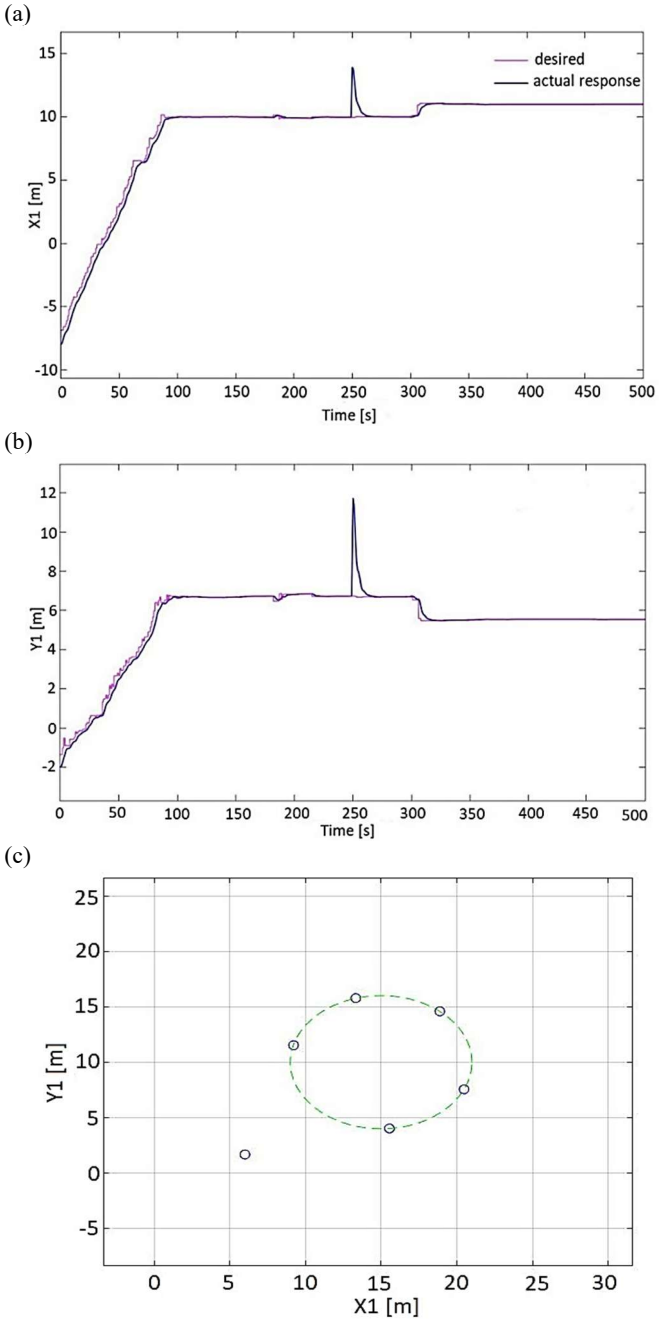


Fig. 4. UAV 1 position under attack scenario 1 (a) UAV 1 x-position under attack scenario 1, (b) UAV 1 y-position under attack scenario 1, (c) UAV1 deviated position in the fleet under attack scenario 1.

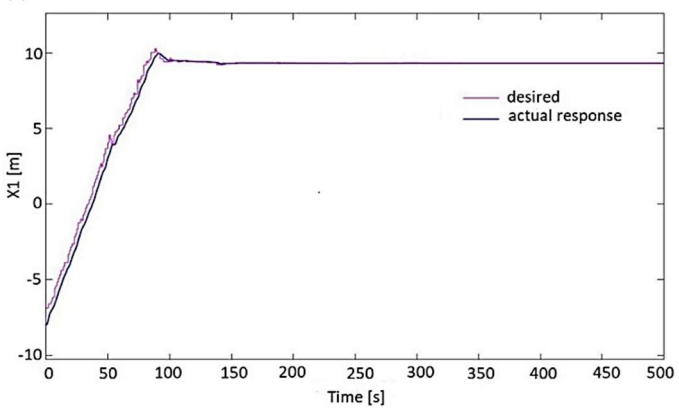
As a result, the controller receives incorrect information about the UAV's location and initiates corrective measures to return it to the desired position. However, the UAV actually deviates from its intended position by $4m$ on the x-axis and $5m$ on the y-axis and leaves the fleet as shown in Fig. 4c. The second deviation from the desired position at $t = 300\ s$ is caused by incorrect calculations made at the ground station, resulting from the reception and utilization of the manipulated position data sent by the attacked drone.

When the diagnosis system is activated, it quickly detects any discrepancies in the GPS sensor data of the UAV. Within a remarkably short timeframe of $0.001\ s$, the GPS spoofing alarm is triggered if the system identifies incorrect GPS readings (placed inside the UAV). To determine the faulty sensor, the system GPS data with the position calculated by the accelerometer and the estimated data as stated before. The discrepancies are checked as follows: if the differences between the GPS data and the accelerometer data for the x_1 and y_1 coordinates, denoted by x_{1GPS}, x_{1ACC}, y_{1GPS} and y_{1ACC}, exceed a threshold of 0.5 meters and the differences between the accelerometer data and the estimated positions, $\hat{x}_1$ and $\hat{y}_1$, are less than 0.2 meters, a GPS spoofing alarm for the x_1 and y_1 coordinates is triggered:

$$|x_{1GPS} - x_{1ACC}| > 0.5\ \&|y_{1GPS} - y_{1ACC}| > 0.5\ \&$$
$$\&|x_{1ACC} - \hat{x}_1| < 0.2\ \&\ |y_{1ACC} - \hat{y}_1| < 0.2$$

The estimated position is obtained using the nonlinear observer described previously, with a diagonal gain matrix with diagonal elements set to a value of 15.

In this case the system prioritizes the accelerometer readings over the GPS readings. Figures 5a and 5b demonstrate the effectiveness of the detection mechanisms and timeframes in swiftly and accurately identifying and responding to GPS spoofing attacks. Potential disasters and negative effects resulting from such attacks are avoided.



(b)

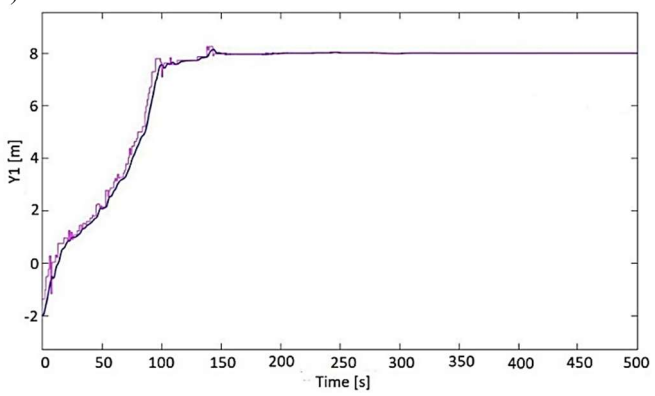


Fig. 5. UAV 1 position after compensation. (a) UAV 1 *x*-position under AS1 with compensation, (b) UAV 1 *y*-position under AS1 with compensation.

5.2. Attack Scenario 2

In this scenario, an attacker maliciously injects false position data at $t = 250\,s$ into the transmitted information of the hexarotor number 2 to the ground station. The attacker alters the x and y coordinates of the neighboring hexarotors by adding a factor of 50 to their positions:

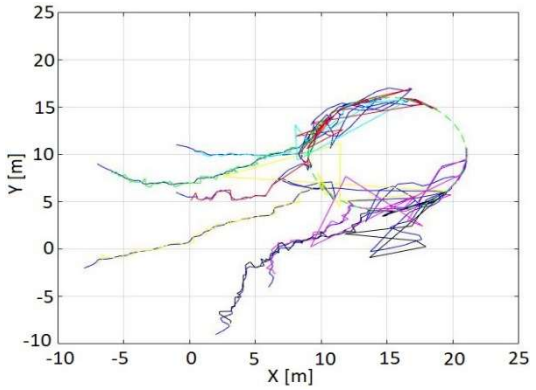
$$neighbor_i\left(2,1:2\right)) = neighbor_i\left(2,1:2\right)) + 50 \quad (16)$$

with $i \in \left[1,3,4,5,6\right]$. As a result, the ground-based ABC algorithm calculates incorrect desired positions for the entire formation based on this erroneous information. Subsequently, the other drones in the formation receive and adjust their positions according to the flawed data, leading to collisions between the UAVs as illustrated in Figures 6a, 6b and 6c. These collisions pose significant risks, potentially causing damage and injury. This fault is detected by checking the residuals between the estimated position of the hexarotor 2 from the nonlinear observer and the position of this hexarotor as stored in the $neighbor_i$ vectors of the other UAVs:

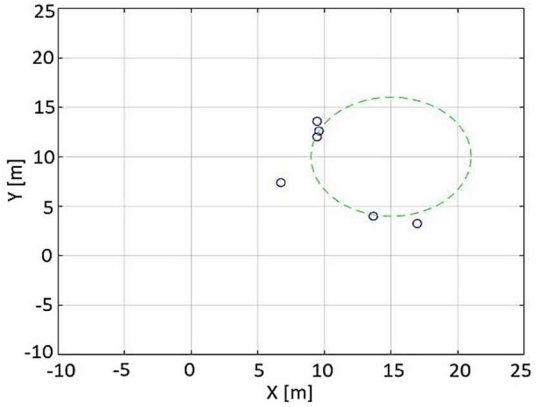
$$|\hat{x}_2 - neighbor_i\left(2,1\right)| > 10\ \&$$
$$\&\,|\hat{y}_2 - neighbor_i\left(2,2\right)| > 10.$$

By implementing the proposed countermeasure for attack scenario 2 consisting of using the estimated positions of the second hexarotor in the ABC algorithm, the safety of the UAV fleet during flight can be ensured. In this scenario, the attack is detected after $1s$ at $t = 251\ s$, effectively mitigating its impact. As depicted in Fig. 6.c, the actual effect on the UAVs occurs approximately $50s$ after the attack's initiation. The delay in the fleet's response to the attack is primarily attributed to the calculation time required by the ABC algorithm at the ground station. Nonetheless, the effectiveness of the countermeasure lies in the ability to detect the attack and prevent its consequences from manifesting within the fleet during the flight.

(a)



(b)



(c)

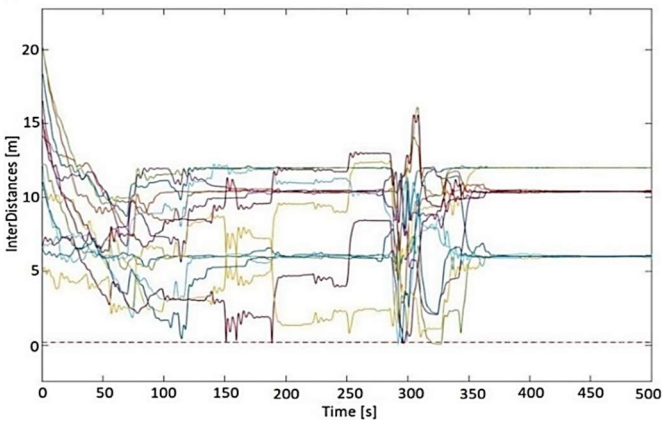


Fig.6. Formation behavior under attack scenario 2. (a) Formation under attack scenario 2 (b) Formation under attack scenario 2 at time $t = 300$ s (c) Interdistances between drones.

5.3. Attack Scenario 3

In this simulated attack scenario, the attacker intercepts and manipulates the desired trajectory, $P_{2desired} = \left(x_{2desired}, y_{2desired}\right)$, transmitted from the ground station to the hexarotor 2. Specifically, a multiplicative attack is simulated, where the desired position generated by the ABC algorithm is multiplied by a factor of 1.5 at time $t = 250\ s$.

The impact of this manipulation on the x and y positions of hexarotor 2 is illustrated in Fig. 7a. By altering the desired trajectory, the attacker can potentially disrupt the UAV's intended path and navigation.

(a)

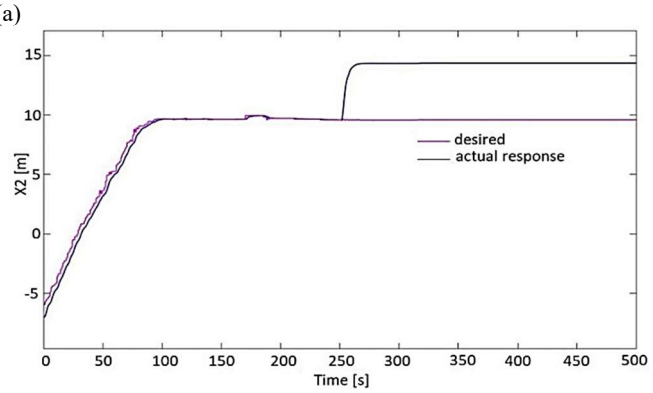


Fig. 7a. UAV2 position under attack scenario 3: a) x-position of UAV2 under attack scenario 3.

(b)

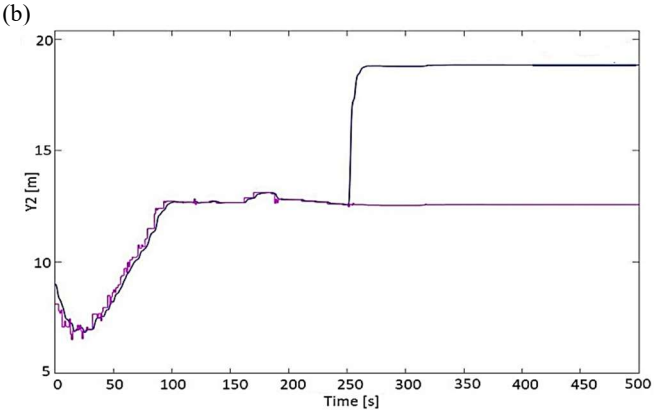


Fig. 7b. UAV2 position under attack scenario 3: y-position of UAV2 under attack scenario 3.

By activating the hybrid diagnosis system, the attack in the simulated scenario is detected at $t = 251.6\ s$. Upon detection, the system promptly responds by tolerating the attack. The response involves sending the true positions to the UAV as discussed previously, effectively mitigating the impact of the multiplicative manipulation of the desired trajectory in Fig. 8.

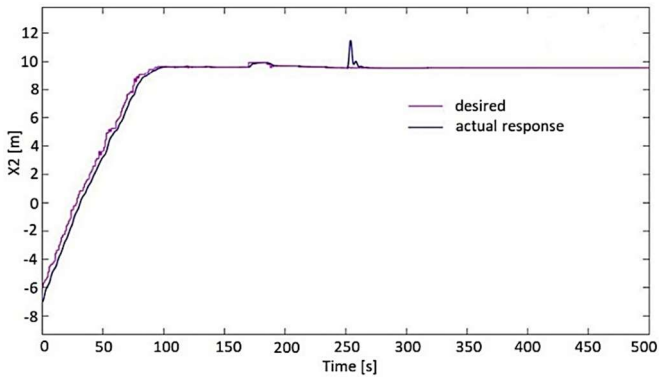


Fig. 8. X-position of UAV2 after compensation under attack scenario 3.

5.4. Actuator and Sensor Faults

5.4.1. Sensor Faults

In this example, a fault is injected in the measurement of the accelerometer's $\ddot{\phi}$, with a bias of 0.1. As a result, the UAV attempts to bring the accelerometer reading back to zero in order to maintain stability along the y-axis position. However, in reality, the angle ϕ deviates from zero, potentially leading to disastrous consequences such as drone falling, collisions, and damage.

At $t = 300\ s$ the bias is injected into the measurement of $\ddot{\phi}$. Figure 9 represents the estimated value of ϕ, which deviates from zero at $t = 300\ s$, and the measured value, which returns to zero due to the influence of the controller. The fault is detected in around 1.5 s and gamma is set to be 0.3.

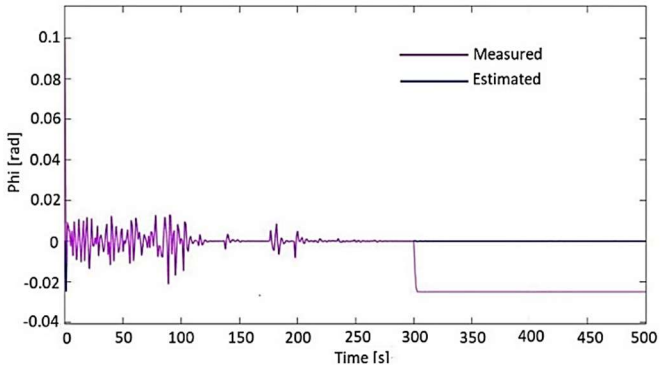


Fig. 9. ϕ estimated vs ϕ measured under accelerometer sensor fault.

To tolerate this fault and maintain stability, the estimated value of ϕ, which represents the actual value, is utilized instead of relying on the erroneous measurement from the accelerometer. By using the estimated value, the UAV can accurately compensate for the bias and ensure the stability of the system. This approach helps prevent potential disasters resulting from the deviation of the accelerometer measurements and maintains the safety and integrity of the drone's operation.

5.4.2. Motors Failures

In this simulated scenario, a full failure of motor 2 in UAV 1 occurs at $t = 250\ s$, followed by a full failure of motor 6 at $t = 300\ s$. Both consecutive motor failures are detected swiftly, with the motor 2 fault being detected in 0.2 s in Fig. 10a and the motor 6 fault being detected in 0.6 s in Figure 10b. The motor failure isolation method relies on analyzing the hexarotor's behavior following each motor failure, as each

motor failure produces a unique signature in the angle deviations as shown in Table 1.

Table 1.
Detection of faulty motor based on UAV behavior

	M_1	M_2	M_3	M_4	M_5	M_6
$\dot{\phi}$	+	–	–	–	+	+
$\dot{\theta}$	–	–	+	+	+	+
$\dot{\psi}$	+	–	–	+	-	+

The system sends then a signal, γ, which represents the degree of damage. Between times 250 s and 300 s, when only one motor is faulty, γ is changed to 0.5. After $t = 300\ s$, when two motors are faulty, γ is changed to 0.7. However, the signal delta remains at 1, indicating that the faults can be compensated and the UAV has the capability to continue its mission despite the motor failures. The faults are tolerated by applying the multiplexing method detailed in [31], as evidenced by the x position of the UAV shown in Fig. 11.

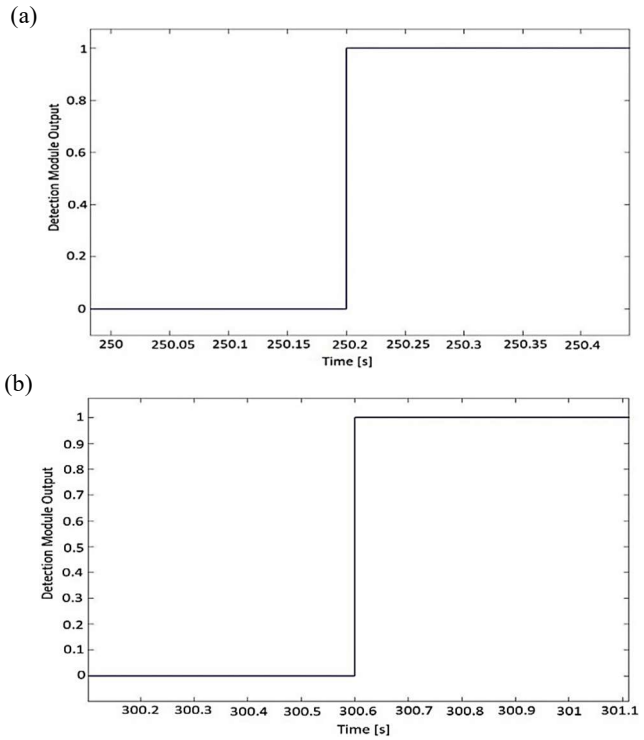


Fig. 10. Output of the detection module under motors 2 and 6 failures. (a) Detection time of motor 2 failure (b) Detection time of motor 6 failure.

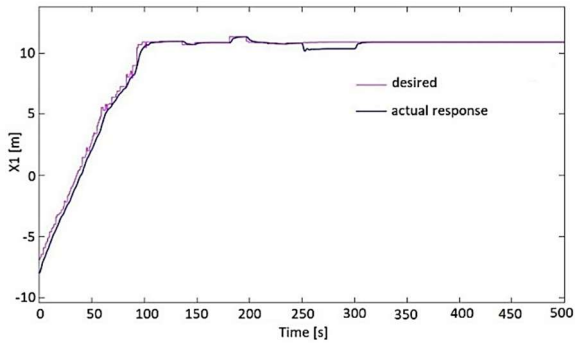


Fig. 11. X-position of UAV1 under two motors failures.

5.4.3. Reconfiguration when $\delta = 0$

In this example, the presence of a faulty UAV, specifically UAV4, is considered. After 50 s of flight, the fault diagnosis mechanism identifies UAV4 as faulty, causing it to send a signal $\delta = 0$ indicating the presence of 1 or 2 faulty motors that cannot be compensated. UAV4 becomes motionless, either landing safely or with some damage, depending on the extent of the damage caused by the fault. Consequently, the term $k_4(t)$ of the cost function of the other UAVs is set to 0. Despite the fault, the remaining five faultless UAVs successfully continue their mission with the assistance of the reconfiguration module's modifications to the optimization module. They form a circle topology around the target point without any collisions. Figure 12 illustrates the ability of the five faultless UAV to maintain formation and reach the target point.

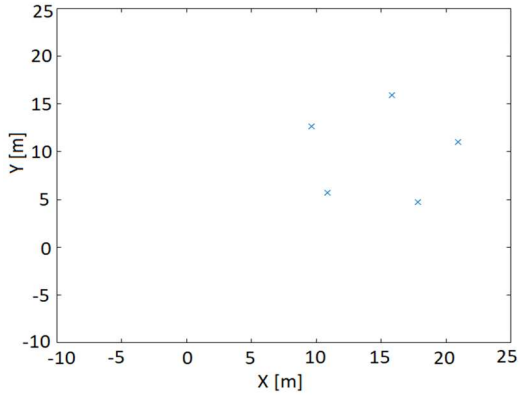


Fig. 12. Final positions computed by ABC algorithm in faulty agent case.

6. CONCLUSION AND FUTURE WORK

This paper provides a comprehensive exploration of vulnerabilities and countermeasures related to cyber attacks on unmanned aerial vehicles (UAVs). It addresses the challenges of three attack scenarios against a hexarotor in a fleet, including Man-in-the-Middle (MITM) attacks and a GPS spoofing attack, and proposes solutions, including individual diagnosis systems within each UAV and a detection process at the ground station, aiming to enhance overall resilience and fault-tolerant capabilities of UAV fleets. Extensive simulations validate the effectiveness of the control method in mitigating adversarial attacks and system faults. The research offers valuable insights into cybersecurity and control strategies, contributing to the field for safer UAV operations in the face of evolving cyber threats. Future work should focus on extending the proposed approach to handle more complex attack

scenarios such as jamming, hijacking, or spoofing multiple UAVs simultaneously, exploring advanced diagnosis and compensation techniques using machine learning or artificial intelligence. These future directions aim to contribute to the advancement of UAV cybersecurity, fostering the development of robust and resilient control systems.

CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

1. B. Ly and R. Ly, Cybersecurity in unmanned aerial vehicles, *Journal of Cyber Security Technology*, 5 (2), 120–137 (2021). https://doi.org/10.1080/23742917. 2020.1846307
2. J. Guerrero and R. Lozano, *UAV fight formation control: Flight Formation Control Strategies for Mini UAVs*, John Wiley & Sons, Ltd, 135–163 (2012). https://doi.org/10.1002/9781118387191.ch7
3. Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu and W. Yi, An Efficient UAV Hijacking Detection Method Using Onboard Inertial Measurement Unit, *ACM Trans. Embed. Comput. Syst.*, 17 (6), 1–19 (2018). https://doi.org/10.1145/3289390
4. S.R. Sindiramutty et al., Data Security and Privacy Concerns in Drone Operations. *Cybersecurity Issues and Challenges in the Drone Industry,* IGI Global, 236–290 (2024). https://doi.org/10.4018/979-8-3693-0774-8.ch010
5. V. Chamola, P. Kotesh, A. Agarwal, Naren, N. Gupta and M. Guizani, A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques, *Ad Hoc Networks*, 111, 102324 (2021). https://doi.org/10.1016/j.adhoc.2020.102324
6. T. M. Hoang, N. M. Nguyen and T. Q. Duong, Detection of Eavesdropping Attack in UAV-Aided Wireless Systems: Unsupervised Learning With One-Class SVM and K-Means Clustering, *IEEE Wireless Communications Letters*, 9(2), 139–142 (2020). https://doi.org/10.1109/LWC.2019.2945022
7. C. G. Leela Krishna and Robin R. Murphy, A review on cybersecurity vulnerabilities for unmanned aerial vehicles, *IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)* (China, 2017). https://doi.org/10.1109/SSRR.2017.8088163
8. S. M. Giray, Anatomy of Unmanned Aerial Vehicle Hijacking With Signal Spoofing, *International Conference on Recent Advances in Space Technologies (RAST)*, Istanbul, Turkey, 2013. https://doi.org/10.1109/RAST.2013.6581320
9. S. Dahiya, and M. Garg Unmanned Aerial Vehicles: Vulnerability to Cyber Attacks, *International Conference on Unmanned Aerial System in Geomatics,* (India, 2019), pp. 201–211. https://doi.org/10.1007/978-3-030-37393-1_18
10. G. Alsuhli, A. Fahim, and Y. Gadallah, A survey on the role of UAVs in the communication process: A technological perspective, *Computer Communications*, 194, 86–123 (2022). https://doi.org/10.1016/j.comcom.2022.07.021
11. O. Westerlund, and R. Asif, Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things, *International Conference on Unmanned Vehicle Systems-Oman (UVS)*, (Muscat, Oman, 2019), pp. 1–10. https://doi.org/10.1109/UVS.2019.8658279
12. B. Han, J. Jiang, T. Cao, and J. Liu, Adaptive Observer-based Security Formation Control for Multiple Unmanned Aerial Vehicles under Cyber-Attacks, *China Automation Congress (CAC)*, (Beijing, China, 2021). https://doi.org/10.1109/CAC53003.2021.9728634
13. T. Humphreys, *Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing*, University of Texas at Austin, 2012.
14. S.-H. Seo, B.-H. Lee, S.-H. Im, and G.-I. Jee, Effect of spoofing on unmanned aerial vehicle using counterfeited gps signal, *Journal of Positioning, Navigation, and Timing*, 4(2), 57–65 (2015). https://doi.org/10.11003/JPNT.2015.4.2.057
15. A. Abbaspour, K. Yen, S. Noei, and A. Sargolzaei, Detection of Fault Data Injection Attack on UAV Using Adaptive Neural Network, *Procedia Computer Science*, 95, 193–200 (2016). https://doi.org/10.1016/j.procs.2016.09.312
16. H. Sedjelmaci, S. Mohammed Senouci, and M. Messous, How to Detect Cyber-Attacks in Unmanned Aerial Vehicles Network?, *IEEE Global Communications Conference (GLOBECOM)*, (Washington, DC, USA, 2016). https: //doi.org/10.1109/GLOCOM.2016.7841878
17. C. Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, A specification-based intrusion detection system for AODV, *ACM workshop on Security of ad hoc and sensor networks*, (Fairfax, Virginia, 2003), pp. 125–134. https: //doi.org/10.1145/986858.986876
18. V. Vaidya, *Dynamic signature inspection-based network intrusion detection*, US Patent 6,279, 2001.
19. A. Patcha and J.-M. Park, An overview of anomaly detection techniques: Existing solutions and latest technological trends, *Computer networks*, 51(12), 3448–3470 (2007). https://doi.org/10.1016/j.comnet.2007.02.001
20. M. A. Aydın, A. H. Zaim, and K. G. Ceylan, A hybrid intrusion detection system design for computer network security, *Computers & Electrical Engineering*, 35(3) (2009), pp. 517–526. https://doi.org/10.1016/j.compeleceng.2008.12.005
21. R. Mitchell and I. R. Chen, Specification-based intrusion detection for unmanned aircraft systems, *First ACM MobiHoc workshop on Airborne Networks and Communications*, (South Carolina, USA, 2012), pp. 31–36. https://doi.org/10.1145/2248326.2248334
22. L. Zomlot, S. Chandran, Sundaramurthy, X. Ou, and S. R. Rajagopalan, Prioritizing Intrusion Analysis Using Dempster-Shafer Theory, *ACM workshop on Security and artificial intelligence*, (Chicago, Illinois, USA, 2011), pp. 59–70. https://doi.org/10.1145/2046684.2046694

23. R. Mitchell, I.-R. Chen, Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 44(5), 593–604 (2014). https://doi.org/10.1109/TSMC.2013.2265083
24. Jp. Yaacoub, H. Noura, O. Salman and A. Chehab, Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations, *Internet of Things*, 11(100218), (2020). https://doi.org/10.1016/j.iot.2020.100218
25. Y. Yang, Y. Xiao and T. Li, Attacks on Formation Control for Multiagent Systems, *IEEE Transactions on Cybernetics*, 52(120), 12805–12817 (2022). https://doi.org/10.1109/TCYB.2021.3089375
26. Y. Gu, K. Guo, L. Guo, J. Qiao, J. Jia, X. Yu, and L. Xie, An enhanced UAV safety control scheme against attacks on desired trajectory, *Aerospace Science and Technology*, 119, 107212 (2021). https://doi.org/10.1016/j.ast.2021.107212
27. S. Jadidi, H. Badihi, and Y. Zhang, Hybrid Fault-Tolerant and Cyber-Resilient Control for PV System at Microgrid Framework, *Annual Conference of the IEEE Industrial Electronics Society*, (Toronto, Canada, 2021). https://doi.org/10.1109/IECON48115.2021.9589054
28. M. Saied, H. Shraim, C. Francis, A review on recent development of multirotor UAV fault-tolerant control systems, *IEEE Aerospace and Electronic Systems Magazine*, 39, 9 (2024). https://doi.org/10.1109/MAES.2023.3327697
29. A. T. Hafez, M. A. Kamel, Fault-Tolerant Control for Cooperative Unmanned Aerial Vehicles Formation Via Fuzzy Logic, *International Conference on Unmanned Aircraft Systems (ICUAS)*, (Arlington, VA, USA, 2016). https://doi.org/10.1109/ICUAS.2016.7502660
30. D. Karaboga, *An Idea Based On Honey Bee Swarm for Numerical Optimization*, Tech. Report TR06, Kayseri, Turkey: Dept. Comput. Eng., Erciyes Univ., 2005.
31. M. Saied, H. Shraim, H. Mazeh, C. Francis, Fault-Tolerant Control of an Hexarotor Unmanned Aerial Vehicle Applying Outdoor Tests and Experiments, IFAC-PapersOnLine, 51(22), 312–317 (2018). https://doi.org/10.1016/j.ifacol.2018.11.560
32. M. Saied, M. Slim, H. Mazeh, C. Francis and H. Shraim, Unmanned Aerial Vehicles Fleet Control via Artificial Bee Colony Algorithm, *4th Conference on Control and Fault Tolerant Systems (SysTol)*, Casablanca, Morocco, 2019, pp. 80–85. https://doi.org/ 10.1109/SYSTOL.2019.8864752