Journal of Intelligent & Robotic Systems (2024) 110:68
https://doi.org/10.1007/s10846-024-02086-3

REGULAR PAPER

# Attack Detection and Security Control for UAVs Against Attacks on Desired Trajectory

**Kunpeng Pan[1,2] · Yang Lyu[1] · Feisheng Yang[1,2] · Zheng Tan[1] · Quan Pan[1]**

Received: 14 April 2023 / Accepted: 1 March 2024


**Abstract**
The paper presents a security control scheme for unmanned aerial vehicles (UAVs) against desired trajectory attacks. The key components of the proposed scheme are the attack detector, attack estimator, and integral sliding mode security controller (ISMSC). We focus on malicious tampering of the desired trajectory sent by the ground control station (GCS) to the UAV by attackers. Firstly, we model attacks by analyzing the characteristics of desired trajectory attacks. Secondly, an integrated attack detection scheme based on an unknown input observer (UIO) and an interval observer is presented. Subsequently, a robust adaptive observer (RAO) is employed to compensate for the impact of attacks on the control system. Thirdly, an ISMSC with an attack compensation mechanism is established. Finally, simulation results are provided to verify the effectiveness of the proposed scheme. The proposed detection scheme can not only detect desired trajectory attacks but also distinguish them from abrupt unknown disturbances (AUDs). By utilizing ISMSC method, UAVs under desired trajectory attacks can fly safely. The proposed comprehensive framework of detection, estimation and compensation provides a theoretical basis for ensuring cyber security in UAVs.

**Keywords** Unmanned aerial vehicle · Desired trajectory attack · Attack detection · Integral sliding mode · Security controller

## 1 Introduction

Unmanned systems, such as unmanned aerial vehicles (UAVs) [1, 2], unmanned marine vehicles [3–5], and industrial control systems [6, 7], have been widely used in both military and civilian fields. UAV is a typical unmanned system, and the related technology is constantly improving. However, with the development of network communication, UAVs are also becoming the focus of cyber attackers. To mention a few, the Iranian military successfully hijacked an American RQ-170 UAV in 2011 by launching a global position system (GPS) spoofing attack [8]. A U.S. UAV fleet at Creech Air Force Base in Nevada is infected by the "keylogging" virus (September 2011), which stole a lot of telemetry and real-time reconnaissance intelligence data from UAV [9]. A South Korean S-100 Camcopter suffered a GPS jamming attack during a flight test, resulting in the death of an engineer (2012) [10]. The above examples show that the research of the past on UAVs risk identification and reinforcement is far from sufficient.

Generally, UAVs consist of a base system, flight managers, communication links, navigation systems, payloads, and other units. The vulnerable points include (a) the channels from the GCS to the UAVs, (b) from the navigation system to the UAVs, and (c) the communication link between UAVs. Attackers steal system information from the ground control station (GCS), such as desired trajectory and system state. They then use this information to design attack signals and inject them into the system, thereby affecting the flight performance of UAVs [11]. This paper specifically focuses on addressing tampering with the desired trajectory sent by

✉ Yang Lyu
lyu.yang0326@gmail.com

Kunpeng Pan
pankunpeng@mail.nwpu.edu.cn

Feisheng Yang
yangfeisheng@nwpu.edu.cn

Zheng Tan
tanzheng@mail.nwpu.edu.cn

Quan Pan
quanpan@nwpu.edu.cn

[1] School of Automation, Northwestern Polytechnical University, Xi'an 710129, Shaanxi, China

[2] Innovation Center NPU Chongqing, Northwestern Polytechnical University, Chongqing 400000, China

Published online: 29 April 2024

GCS to UAVs. In the field of UAVs, malicious attackers gain unauthorized access to a UAV system through network communications which causes deviations from set trajectories. An attack detector is designed to identify whether an attack has occurred. Once an attack is detected, an attack estimation and compensation unit is activated in order to achieve integrated detection, estimation and compensation within the UAV system for effective attack detection and security control measures. This provides strong theoretical support for ensuring safe flights of UAVs under network security threats.

Attack detection is the most basic step of our proposed scheme. Existing research results of attack detection can be divided into data-driven and knowledge-based detection methods. Model-free-based detection methods are widely studied [12, 13]. Two kinds of data mining methods, artificial neural network and support vector machine, are used for intrusion detection. However, this approach imposes a heavy computation burden, and training a fully connected network is very difficult. In addition to the above data-driven approaches, some model-based ones have also been proposed. A scheme based on state estimation is proposed to achieve attack detection, such as the weighted least squares method [14, 15]. Although this method can detect basic attacks, it may fail to detect well-designed attacks. To solve this problem, observer-based state estimation methods have also been proposed, such as the Lunberger observer and sliding mode observer [16]. Based on erroneous measurements, $\chi^2$ detectors are given to detect bad data [17]. However, this scheme is no longer applicable when the injected data matches the historical distribution. To improve the accuracy of attack detection, a new detector based on historical information is proposed, that is, the summation detector [18]. With the help of traditional fault detection ideas, the attack detection scheme is also proposed based on the comparison of residual and threshold [16, 19, 20]. However, the selection of the threshold is difficult and is easy to affect the detection accuracy.

Recently, important advances have been achieved in security control. Security state estimation is a common method to achieve security control [21–24]. Shaunak et al. [21] propose a secure state estimation method and give the maximum number of sensor channels that could be attacked. Based on prior information, a secure state estimation scheme under malicious sensor attacks is designed in [22]. Ao et al. [23] further extend to interconnected systems, a distributed observer is proposed to achieve secure state estimation. Nevertheless, the above algorithms use all the information in batches, making the calculation complex. To reduce the computational complexity, an adaptive state observer with the switching mechanism is introduced. This method can adaptively truncate the attack channel, establish the attack tolerance strategy, and realize the secure state estimation [24]. In addition, security control schemes based on attack estimation and compensation have been studied to ensure the safe flight of UAVs [11, 25, 26]. Inspired by fault estimation, Su et al. [16] design a sliding model observer for attack detection and reconstruction without security control. Inevitably, the upper bound of the attack needs to be known in advance under such an estimation scheme, and the condition of strictly positive realness needs to be satisfied. These conditions are very strict, thus greatly limiting its application. To address these issues, Gu et al. propose a compensation scheme based on attack signal reconstruction using disturbance observer [11]. In addition, a combined learning observer and attack observer scheme is proposed in [26], which effectively achieves attack estimation and compensation. However, the design process of the iterative learning observer is complicated and lacks generality.

The proportional-integral-differential controller and the linear quadratic regulation controller are developed for UAVs in [27, 28], respectively. However, with the above methods, external disturbances and uncertainties inevitably affect the performance of the controllers. One of the most common methods for dealing with disturbances and uncertainties is the adaptive control approach [29]. Sliding mode control is a good technique to handle uncertainties and disturbances so that the system can reach the desired state in finite time. The major advantage of sliding mode control is its ability to effectively reject matched uncertainty. Later on, integral sliding mode control technique has been extensively investigated [30]. By using integral sliding mode control technique, disturbances are eliminated and the system trajectory starts on the sliding surface. To the best of our knowledge, there are few conclusions regarding the detection and security problems associated with desired trajectory attacks. The research on how to detect these attacks, distinguish them from abrupt unknown disturbances (AUDs), estimate the attacks without equality constraints, and design an integral sliding mode security controller (ISMSC) in cases where the upper bound of desired trajectory attacks is unknown remains open, which motivates this article.

The motivation of this article is summarized as:

1. The existing work on desired trajectory attacks is insufficient, and it is worth studying how to detect, estimate, and compensate for such attacks.
2. The schemes of [16, 19, 20] can achieve attack detection, but they cannot differentiate attacks from AUDs. It is worth investigating how to distinguish attacks from AUD.
3. The sliding mode observer (SMO) [16] needs to determine the upper bound of the attack. Investigating how to address this limitation is worthwhile.

In this article, a scheme for detecting attacks and controlling the security of UAVs under desired trajectory attacks

is proposed. Compared to existing related works, the main contributions of this article can be summarized as follows:

1. Different from false data injection attacks [11, 16], desired trajectory attacks are considered in this paper, which are converted to control input channels by analyzing the transmission mechanism and characteristics of attacks. In other words, desired trajectory attacks are translated into malicious tampering of the input signal.
2. The scheme [26] can realize attack detection and distinguish attacks from AUDs, but it is limited when attacks and AUDs occur simultaneously. The proposed detection scheme based on unknown input observer (UIO) and interval observer can avoid the missing detection caused by the simultaneous occurrence of attacks and AUDs.
3. Compared with the SMO [16], a robust adaptive observer (RAO) is proposed to estimate attacks without an equality constraint. Then, we present an ISMSC controller with attack compensation that incorporates the desired position information.

The mathematical model of UAVs and the desired trajectory attack model are described in Section 2. Section 3 proposes the attack detection logic based on a UIO and an interval observer. A RAO is employed with a performance index to carry out attack estimation in Section 4. After attack detection and reconstruction, an ISMSC strategy is developed to achieve UAV security control in Section 5. To demonstrate the feasibility and superiority of the attack detection and security control strategy, simulation results are provided in Section 6. Finally, conclusions are drawn in Section 7.

The abbreviations in the Introduction are organized as in Table 1.

**Notation** $\mathbb{R}^n$ denotes the n-dimensional Euclidean space. The superscript $T$ stands for matrix transposition, and $S > 0$, $S < 0$ denote positive-definiteness and negative-definiteness. $\lambda_{\max}(A)$ and $\lambda_{\min}(A)$ denote the largest and smallest eigenvalues of $A$, respectively. $\mathbf{C}$ represents the set of a complex number. Given a vector $v_i \in \mathbb{R}^n$, $\|v_i\|$ is the Euclidean norm of $v_i$. $\underline{a}$ and $\overline{a}$ are the upper and lower bounds of $a$. $\mathbf{0}$ and $\mathbf{I}$ denote a zero matrix and unit matrix with appropriate dimensions.

**Table 1** List of abbreviations

| Abbreviations | Definition |
|---|---|
| UAV | Unmanned aerial vehicle |
| GCS | Ground control station |
| UIO | Unknown input observer |
| AUD | Abrupt unknown disturbance |
| RAO | Robust adaptive observer |
| GPS | Global position system |
| SMO | Sliding mode observer |
| ISMSC | Integral sliding mode security controller |

## 2 Preliminaries and Problem Formulation

In what follows, we first introduce models for the UAVs and the desired trajectory attacks model. Then, we propose an overall security control framework.

### 2.1 UAV System Description

In this paper, the UAV is assumed to be a rigid body. In the inertial reference frame $F_I$, the position, velocity, and attitude Euler angles of UAV are defined as $p = [p_x, p_y, p_z]^T$, $v = [v_x, v_y, v_z]^T$, and $\xi = [\phi, \theta, \psi]^T$. $\phi, \theta$ and $\psi$ represent the roll angles, pitch angles, and yaw angles that denote the rotation around $x-$, $y-$ and $z-$ axes, respectively. The UAV dynamic model is characterized as [11]:

$$\begin{aligned} &\dot{p} = v, \\ &m\dot{v} = F - G, \\ &M(\xi)\ddot{\xi} + N(\xi, \dot{\xi})\dot{\xi} = \vartheta, \end{aligned} \tag{1}$$

where $G = [0, 0, mg]$ is the gravity vector of the UAV. $m$ and $g$ are the mass and gravitational acceleration. $\vartheta = [\vartheta_\phi, \vartheta_\theta, \vartheta_\psi]^T$ are the magnitude of the torque of the propeller. $M(\xi)$ and $N(\xi, \dot{\xi})$ denote the diagonal moment of inertia tensor and centrifugal and Coriolis matrix, respectively. Details can be founded in [11]. $F = [F_x, F_y, F_z]^T$ is the equivalent control force input, which is described as

$$F = f \begin{bmatrix} \cos\psi \sin\theta \cos\phi + \sin\psi \sin\phi \\ \sin\psi \sin\theta \cos\phi - \cos\psi \sin\phi \\ \cos\phi \cos\theta \end{bmatrix}. \tag{2}$$

$f$ is the magnitude of the thrust. $I_{xx}$, $I_{yy}$, and $I_{zz}$ denote the moments of inertia. Let $p_d$ be the desired trajectory. It follows from Eq. 2 that the desired attitude angles are derived as:

$$\begin{aligned} \theta_d &= arctan(\frac{F_x \cos\psi + F_y \sin\psi}{F_z}), \\ \phi_d &= arctan(\cos\theta \frac{F_x \sin\psi - F_y \cos\psi}{F_z}). \end{aligned} \tag{3}$$

Notice that, the desired attitude $\xi_d = [\phi_d, \theta_d, \psi_d]^T$, where the desired yaw angle $\psi_d$ is assumed to be 0.

The errors of position, velocity, and attitude Euler angles are defined as:

$$e_p = p - p_d, e_v = v - \dot{p}_d, e_\xi = \xi - \xi_d. \tag{4}$$

Considering that there are no attack in the system, the controllers based on PID can be designed as:

$$F = m(K_p e_p + K_v e_v + \ddot{p}_d) + G, \vartheta = K_\xi e_\xi + K_\omega \dot{\xi}, \quad (5)$$

where $K_p$ and $K_v$ represent the controller gain of position loop gain. $K_\xi$ and $K_\omega$ are the controller gains in the attitude loop.

## 2.2 Attack Analysis and Modeling

The UAV needs to receive the GCS remote signal in real time. It is important to ensure the safe transmission of desired trajectory. However, UAVs are vulnerable when receiving wireless data transmissions. Define $p_a$ as the attacked desired trajectory. Inspired by [26, 31], bias attacks and hybrid attacks are investigated in this paper.

### 2.2.1 Bias Attack

Define $\delta_{ba}$ as the bias attack signal. The attacked desired trajectory signal is represented as $p_{ba} = p_d + \delta_{ba}$. The asymptotic convergence attack model is employed as

$$\dot{\delta}_{ba} = -\varpi \delta_{ba} + \varpi \delta_{b\infty}, \quad (6)$$

where $\delta_{ba}$ and $\delta_{b\infty}$ are transient components and desired deviations with known upper bound. $\varpi$ is a known constant and $\delta_{ba}(0) = 0$. The attack signal can be delivered to the control channel along the desired trajectory, and the attack model $F_\delta^{ba}$ on the control channel can be expressed.

$$F_\delta^{ba} = m(K_p \delta_{ba} + K_v \dot{\delta}_{ba} + \ddot{\delta}_{ba}), \quad (7)$$

where $F_\delta^{ba} = [F_{\delta x}^{ba}, F_{\delta y}^{ba}, F_{\delta z}^{ba}]^T$, $\dot{\delta}_{ba}$ and $\ddot{\delta}_{ba}$ are the time derivative.

### 2.2.2 Hybrid Attack

Define $\delta_{ha}$ as hybrid attack signal. The desired trajectory attacked is deceloped as $p_{ha} = p_d + \delta_{ha}$, where

$$\delta_{ha} = \delta_{ba} + \chi_{ha}. \quad (8)$$

$\chi_{ha}$ is the periodic attack signal, which is described by the following exogenous system model:

$$\chi_{ha} = \mathcal{V}_{ha}\varphi_{ha}, \dot{\varphi}_{ha} = \mathcal{W}_{ha}\varphi_{ha}, \quad (9)$$

where $\mathcal{V}_{ha}$ and $\mathcal{W}_{ha}$ are known matrices. $\varphi_{ha}$ is intermediate variable. The exogenous system Eq. 9 can not only describe a periodic attack, but also be seen as a generalized bias attack. In addition, many kinds of attacks can be described by model Eq. 9, such as harmonic attack with unknown phase and unknown amplitude [32].

It follows from Eq. 8 that the attack model is mapped to the control input channel as $F_\delta^{ha}$, where

$$F_\delta^{ha} = m((K_p \delta_{ba} + K_v \dot{\delta}_{ba} + \ddot{\delta}_{ba}) + K_p \chi_{ha} + K_v \dot{\chi}_{ha} + \ddot{\chi}_{ha}), \quad (10)$$

where $F_\delta^{ha} = [F_{\delta x}^{ha}, F_{\delta y}^{ha}, F_{\delta z}^{ha}]^T$, $\dot{\chi}_{ha}$ and $\ddot{\chi}_{ha}$ are the time derivative.

According to the above analysis, the attack can be mapped to the input channel. In the two types of attack cases, the input channels under attacks are transformed into:

$$u_f(t) = u_0(t) + \frac{F_a}{m} = \begin{cases} u_0(t) + \dfrac{F_\delta^{ba}}{m}, \ Bias\ attacks \\ u_0(t) + \dfrac{F_\delta^{ha}}{m}, \ Hybrid\ attacks, \end{cases} \quad (11)$$

where

$$u_0(t) = (F - G)/m. \quad (12)$$

**Assumption 1** *The desired bias vector $\delta_{b\infty}$ satisfies the bounded constraint of $\|\delta_{b\infty}\| \le \bar{\delta}_b$.*

**Remark 1** *The capability of attackers is limited* [33]. *Therefore, the assumption that the attack is bounded is given. Generally speaking, if the amplitude of the attack is too large, it becomes easy to detect. To avoid detection, bias attacks gradually increase towards the desired bias.*

**Property 1** *Since $\delta_{ba}$ converges asymptotically, it is bounded. Referring to* Eq. 7, *both the norms of $F_\delta^{ba}$ and its derivative are bounded, that is,*

$$\begin{aligned} \|F_\delta^{ba}\| &= \|m(K_p \delta_{ba} + (K_v \varpi - \varpi^2)(-\delta_{ba} + \delta_{b\infty}))\| \\ &\le \bar{\delta}_b \|m\|(\|K_p\| + 2\|K_v \varpi - \varpi^2\|), \\ \|\dot{F}_\delta^{ba}\| &= \|m(-K_p \varpi + K_v \varpi^2 - \varpi^3)(\delta_{ba} - \delta_{b\infty})\| \\ &\le 2\bar{\delta}_b \|m\|\| - K_p \varpi + K_v \varpi^2 - \varpi^3\|. \end{aligned} \quad (13)$$

**Property 2** *According to* Eqs. 8 *and* 9, *one has*

$$F_\delta^{ha} = F_\delta^{ba} + m\Psi\varphi_{ha}, \dot{F}_\delta^{ha} = \dot{F}_\delta^{ba} + m\dot{\Psi}\varphi_{ha} \quad (14)$$

*where $\Psi_{\varphi_{ha}} = (K_p \mathcal{V}_{ha} + K_v \mathcal{V}_{ha}\mathcal{W}_{ha} + \mathcal{V}_{ha}\mathcal{W}_{ha}^2)\varphi_{ha}$, $\dot{\Psi}_{\varphi_{ha}} = (K_p \mathcal{V}_{ha}\mathcal{W}_{ha} + K_v \mathcal{V}_{ha}\mathcal{W}_{ha}^2 + \mathcal{V}_{ha}\mathcal{W}_{ha}^3)\varphi_{ha}$ and $\dot{\varphi}_{ha} = \mathcal{W}_{ha}\varphi_{ha}$. $\Psi_{\varphi_{ha}}$ represents the harmonic attack with unknown phase and unknown amplitude in this paper. The harmonic attack and its derivative is bounded, that is, $\|\Psi_{\varphi_{ha}}\| < \bar{\Psi}_{\varphi_{ha}}$ and $\|\Psi_{\varphi_{ha}}\| < \bar{\dot{\Psi}}_{\varphi_{ha}}$.*

**Property 3** *Due to $K_p, K_v, \mathcal{W}_{ha}, \mathcal{V}_{ha}$ are constant matrices, $K_p\mathcal{V}_{ha} + K_v\mathcal{V}_{ha}\mathcal{W}_{ha} + \mathcal{V}_{ha}\mathcal{W}_{ha}^2$ is a constant matrix, that is, $\Psi_{\varphi_{ha}} \leq \bar{\Psi}_{\varphi_{ha}}$. Accordingly, $F_\delta^{ha}$ and $\dot{F}_\delta^{ha}$ are bounded, that is,*

$$\|F_\delta^{ha}\| \leq \bar{F}_\delta^{ha}, \|\dot{F}_\delta^{ha}\| \leq \bar{\dot{F}}_\delta^{ha} \tag{15}$$

*where $\bar{F}_\delta^{ha} = \bar{\delta}_b\|m\|(\|K_p\| + 2\|K_v\varpi - \varpi^2\|) + \|m\|\bar{\Psi}_{\varphi_{ha}}$, $\bar{\dot{F}}_\delta^{ha} = 2\bar{\delta}_b\|m\|\| - K_p\varpi + K_v\varpi^2 - \varpi^3\| + \|m\|\bar{\dot{\Psi}}_{\varphi_{ha}}$.*

**Remark 2** *Once the desired trajectory is compromised, the security and performance of the UAV may be reduced, potentially leading to a crash. By analyzing injection attack characteristics, attack models can be mapped onto the control channel, providing a basis for subsequent detection and compensation.*

**Remark 3** *The desired trajectory attacks are modeled as attack signals on the control input channel, considering bias attacks and hybrid attacks with unknown upper bounds.*

### 2.3 Security Control Framework

The effects of the two types of attacks on the control input channel are $F_\delta^{ba}$ and $F_\delta^{ha}$, which are uniformly characterized as $F_a \in \mathbb{R}^a$. Define the system state $x = [p^T, v^T]^T \in \mathbb{R}^n$. Under attacks and AUDs, it has

$$\begin{aligned} \dot{x}(t) =& Ax(t) + B(u_f(t) + u_c(t)) + D\Delta d, \\ z(t) =& C_z x(t) + D_z(u_f(t) + u_c(t)), \\ y(t) =& Cx(t), \end{aligned} \tag{16}$$

where

$$A = \begin{bmatrix} 0 & I \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 \\ I \end{bmatrix},$$

and $u_c(t)$ is the security controller with attack compensation mechanism. $y(t) \in \mathbb{R}^p$ and $z(t) \in \mathbb{R}^z$ are measured output and regulated output, respectively. $\Delta d \in \mathbb{R}^q$ denotes AUDs. $p < n, A, B, C, C_z, D_z$ are the constant matrices with appropriate dimensions. For convenience, here, we assume that $C = [I_p, 0_{p\times(n-p)}]$.

Let $\omega(t) = [F_a^T, \Delta^T d]^T \in \mathbb{R}^r$, $(r = a + q)$, , $E = [B, D]$, then the system Eq. 16 can be rewritten as

$$\begin{aligned} \dot{x}(t) =& Ax(t) + B(u_0(t) + u_c(t)) + E\omega(t), \\ z(t) =& C_z x(t) + D_z(u_f(t) + u_c(t)), \\ y(t) =& Cx(t). \end{aligned} \tag{17}$$

Regarding the overall security framework, all the input signals are listed in Table 2.

**Table 2** Input signals

| Symbol | Equation | Definition |
|---|---|---|
| $F$ | Eq. 5 | Equivalent control force input |
| $F_\delta^{ba}$ | Eq. 7 | Equivalent input produced by bias attacks |
| $F_\delta^{ha}$ | Eq. 10 | Equivalent input produced by hybrid attacks |
| $u_0(t)$ | Eq. 12 | Input signal without attacks effect |
| $u_f(t)$ | Eq. 11 | Input signal with attacks effect |
| $u_c(t)$ | Eq. 39 | Input signal with attack compensation |

The main purpose of the presented paper is to test a security scheme that is based on attack detection, estimation, and compensation. The security control framework comprises three subsystems: 1) the attack detection subsystem (ADs); 2) the attack estimation subsystem (AEs) based on a RAO; and 3) the security control subsystem (SCs) with attack compensation. The security control framework is illustrated in Fig. 1.

The above subsystems are presented separately in the following sections. However, before these procedures, we need to present some preliminaries as follows.

**Assumption 2** *The observer matching condition is*

$$rank(CE) = rank(C).$$

**Assumption 3**

$$rank\begin{bmatrix} sI_n - A & E \\ C & 0 \end{bmatrix} = n + r, \forall s \in \mathbb{C}, Re(s) \geqslant 0.$$

**Assumption 4** *The initial state $x(0)$ has upper and lower bounds, $\bar{x}(0)$ and $\underline{x}(0)$, that is, $\underline{x}(0) \leq x(0) \leq \bar{x}(0)$. The AUDs $\Delta d$ satisfies $\underline{\Delta}d \leq \Delta d \leq \bar{\Delta}d$, where $\underline{\Delta}d$ and $\bar{\Delta}d$ are known vectors.*

**Definition 1** *A Metzler matrix is considered as a square matrix in which all the off-diagonal components are non-negative.*

**Definition 2** *$D^+$ and $D^-$ are defined as $max(0, D)$ and $max(0, -D)$, where $D$ is the constant matrix with appropriate dimensions.*

**Lemma 1** [34] *Assume that three vector variables: $x(t), \bar{x}(t), \underline{x}(t)$ satisfy $\underline{x}(t) \leq x(t) \leq \bar{x}(t)$. If there exist any constant matrix $Q$, one has: $Q^+\underline{x}(t) - Q^-\bar{x}(t) \leq Qx(t) \leq Q^+\bar{x}(t) - Q^-\underline{x}(t)$, where $Q^+$ and $Q^-$ are defined under* Definition 2.

**Lemma 2** [34] *Under* Assumptions 2 *and* 3, *the observer gain matrix can be obtained by the following LMI*

$$PA + A^TP - \mathcal{W}C - C^T\mathcal{W}^T < 0, PE = C^TF^T$$

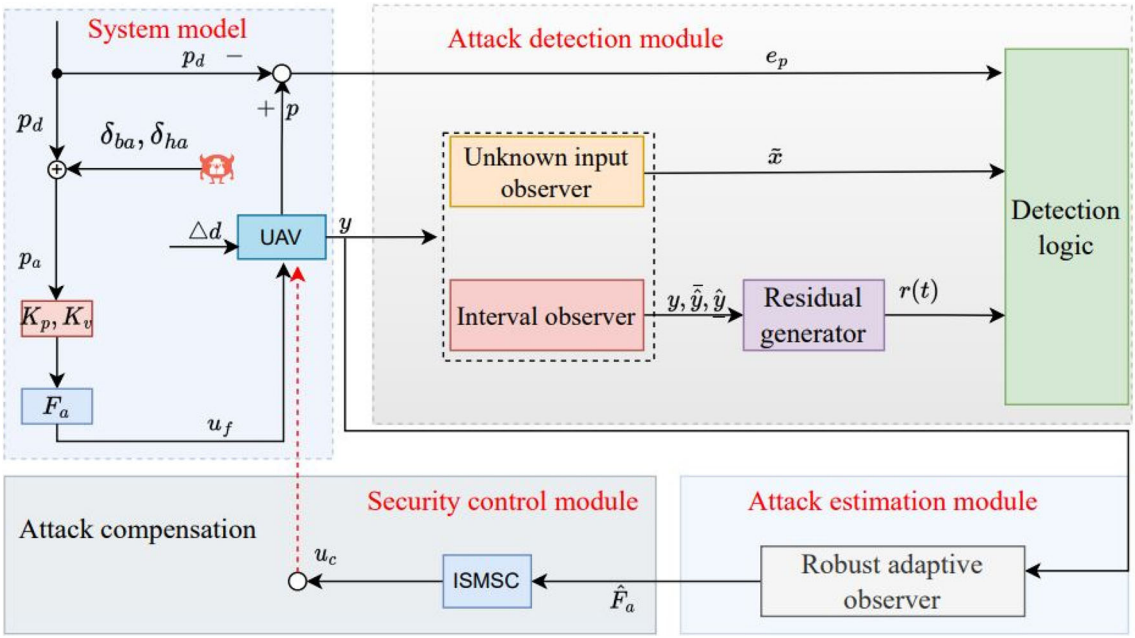



**Fig. 1** Block diagram of security control for the UAVs

*where $P$ is a symmetric positive definite matrix. $L = P^{-1}\mathcal{W}$ is a observer gain matrix. $F$ is a parameter matrix.*

**Lemma 3** [35] *The matrix $V$ is both Metzler and Hurwitz in the system $\dot{x}(t) = Vx(t) + d(t)$. If there satisfies $d(t) > 0$ and $x(0) > 0$, we have $x(t) > 0$ for all $t > 0$.*

## 3 Attack Detection Subsystem

In practice, UAVs suffer from AUDs, which can lead to performance degradation. Typical disturbances include wind shear, turbulence, electromagnetic interference, and so on. These disturbances, along with attacks, cause flight performance degradation that makes it difficult to distinguish between attacks and AUDs. In this section, a UIO and an interval observer are employed to detect and differentiate attacks from AUDs.

### 3.1 UIO Observer Design

Inspired by [26], an UIO is built for system Eq. 16 as:

$$\begin{aligned} \dot{z}_{dec} &= RA\hat{x}_{uio} + L_{uio}C(x - \hat{x}_{uio}), \\ \hat{x}_{uio} &= z_{dec} + Hx, \end{aligned} \tag{18}$$

where $\hat{x}_{uio} \in \mathbb{R}^n$ is the state estimation. $R \in \mathbb{R}^{n\times n}$, $H \in \mathbb{R}^{n\times n}$ and $L_{uio} \in \mathbb{R}^{n\times n}$ denote the observer gains to be designed. $z_{dec} \in \mathbb{R}^n$ is the auxiliary intermediate variable. Let $\tilde{x} = x - \hat{x}_{uio} = [\tilde{p}, \tilde{v}]^T$. To get the observer gain, the Theorem 1 is given.

**Theorem 1** *With respect of the UIO* Eq. 18*, if there exist matrices $P > 0 \in \mathbb{R}^{n\times n}$, $R \in \mathbb{R}^{n\times n}$, $H \in \mathbb{R}^{n\times n}$ and $L \in \mathbb{R}^{n\times n}$ satisfying*

$$R + H = I, RB = 0, \tag{19}$$

*the state estimation error is obtained as*

$$\dot{\tilde{x}} = (RA - L_{uio}C)\tilde{x} + R\Delta d, \tag{20}$$

*Further, $L_{uio}$ is chosen such that*

$$P(RA - L_{uio}C) + (RA - L_{uio}C)^T P < 0. \tag{21}$$

*It follows from* Eq. 20 *that if no AUDs is injected into UAV ($\Delta d = 0$), the state estimation error $\tilde{x}(t)$ converges to 0 asymptotically.*

***Proof*** See Appendix A for details. □

### 3.2 Interval Observer Design

An interval observer is designed for estimating the upper and lower boundary of the measurement output $y(t)$. The estimation is robust to disturbance but sensitive to desired trajectory attacks. The system matrices $A$, $B$, $D$ and $E$ into block vectors or matrices as follows:

$$A = \left[\begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array}\right], B = \left[\begin{array}{c} B_1 \\ \hline B_2 \end{array}\right], D_z = \left[\begin{array}{c} D_1 \\ \hline D_2 \end{array}\right], E = \left[\begin{array}{c} E_1 \\ \hline E_2 \end{array}\right],$$

where $A_{11} \in \mathbb{R}^{p\times p}$,$A_{12} \in \mathbb{R}^{p\times(n-p)}$, $A_{21} \in \mathbb{R}^{(n-p)\times p}$, $A_{22} \in \mathbb{R}^{(n-p)\times(n-p)}$, $B_1 \in \mathbb{R}^{p\times m}$, $B_2 \in \mathbb{R}^{p\times m}$, $D_1 \in \mathbb{R}^{p\times r}$, $D_2 \in \mathbb{R}^{(n-p)\times r}$, $E_1 \in \mathbb{R}^{p\times r}$, $E_2 \in \mathbb{R}^{(p-r)\times r}$. $E_1 = [B_1, D_1]$, $E_2 = [B_2, D_2]$.

Define $U = \left[\begin{array}{c|c} I_p & 0_{p\times(n-p)} \\ \hline G & I_{n-p} \end{array}\right]$, where $G \in \mathbb{R}^{(n-p)\times p}$ is the observer gain matrix to be designed later. By letting $h = [h_1^T, h_2^T]^T = Ux$, the system Eq. 17 can be rewritten as

$$\dot{h}(t) = U_A h(t) + U_B(u_0(t) + u_c(t)) + U_E\omega(t), \tag{22}$$

where

$$U_A = \left[\begin{array}{c|c} A_{11} - A_{12}G & A_{12} \\ \hline GA_{11} + A_{21} - GA_{12}G - A_{22}G & GA_{12} + A_{22} \end{array}\right],$$
$$U_B = \left[\begin{array}{c} B_1 \\ \hline GB_1 + B_2 \end{array}\right], U_E = \left[\begin{array}{c} E_1 \\ \hline GE_1 + E_2 \end{array}\right].$$

Since $y(t) = h_1(t)$, we can obtain

$$\begin{aligned}\dot{y}(t) = &(A_{11} - A_{12}G)y(t) + A_{12}\hat{h}_2 + B_1(u_c(t) \\ &+ u_0(t) + F_a) + D_1\Delta d(t),\end{aligned} \tag{23}$$

Based on Lemma 2, the matrices $L, P$ are decomposed into block matrix as $L = \left[\begin{array}{c} L_1 \\ L_2 \end{array}\right]$, $P = \left[\begin{array}{cc} P_{11} & P_{12} \\ P_{21} & P_{22} \end{array}\right]$, where $L_1 \in \mathbb{R}^{p\times p}, L_2 \in \mathbb{R}^{(n-p)\times p}, P_{11} \in \mathbb{R}^{p\times p}, P_{12} \in \mathbb{R}^{p\times(n-p)}$, $P_{22} \in \mathbb{R}^{(n-p)\times(n-p)}$. Further, we have $[P_{21}, P_{22}]E = 0$. By multiplying the left by $P_{22}^{-1}$, we get $[P_{22}^{-1}P_{21}, I_{n-p}]E = 0$. Let $G = P_{22}^{-1}P_{21}$. The $\dot{h}_2$ can be written as

$$\begin{aligned}\dot{h}_2(t) = &(GA_{12} + A_{22})h_2 + (GB_1 + B_2)(u_0(t) + u_c(t) + F_a) \\ &+ (GA_{11} + A_{21} - GA_{12}G - A_{22}G)y(t).\end{aligned} \tag{24}$$

With respect of Eqs. 23 and 24, the interval observer is employed as

$$\begin{aligned}\dot{\bar{\hat{y}}}(t) = &(A_{11} - A_{12}G)\bar{\hat{y}}(t) + A_{12}\hat{h}_2 + L_{io}\bar{e}_y \\ &+ B_1(u_0(t) + u_c(t)) + D_1^+\bar{\Delta}d - D_1^-\underline{\Delta}d. \\ \dot{\underline{\hat{y}}}(t) = &(A_{11} - A_{12}G)\underline{\hat{y}}(t) + A_{12}\hat{h}_2 + L_{io}\underline{e}_y \\ &+ B_1(u_0(t) + u_c(t)) + D_1^+\bar{\Delta}d - D_1^-\underline{\Delta}d. \\ \dot{\hat{h}}_2(t) = &(GA_{12} + A_{22})\hat{h}_2 + (GB_1 + B_2)(u_0(t) + u_c(t)) \\ &+ (GA_{11} + A_{21} - GA_{12}G - A_{22}G)y(t)\end{aligned} \tag{25}$$

where $L_{io}$ is the observer gain matrix. $\bar{\hat{y}}, \underline{\hat{y}}$ are denoted as the upper and lower bounded estimations of $y(t)$. $\bar{e}_y = \bar{\hat{y}}(t) - y(t)$ and $\underline{e}_y = y(t) - \underline{\hat{y}}(t)$ denote the upper and lower bounded of estimation errors, respectively. $D_1^+$ and $D_1^-$ are given by Definition 2. $\hat{h}_2$ is the estimation of $h_2$. Due to $Ux(t) = h(t)$, we obtain $x(t) = [h_1^T, h_2^T - h_1^T G^T]^T$, which further implies $\hat{x}(t) = [y^T, h_2^T - y^T G^T]^T$. Let $e_x = x(t) - \hat{x}(t)$, $e_{h2} = h_2 - \hat{h}_2$.

**Theorem 2** *With respect of the interval observer* Eq. 24*, if the observer gain matrix is chosen as* $L_{io} = A_{11} - A_{12}G - \Psi$*, where* $\Psi \in \mathbb{R}^{p\times p}$ *is a known Hurwitz and Metzler matrix, there exists a scalar* $t_w > 0$ *such that* $\underline{y}(t) \le y(t) \le \bar{y}(t)$ *holds when* $F_a = 0$*. Here, the initial values are set as*

$$\bar{\hat{y}}(0) = C^+\bar{x}(0) - C^-\underline{x}(0),\ \underline{\hat{y}}(0) = C^+\underline{x}(0) - C^-\bar{x}(0) \tag{26}$$

*where* $C^+$ *and* $C^-$ *are defined under* Definition 2*.*

***Proof*** See Appendix B for details. □

### 3.3 Attack Detection Logic

This part proposes a comprehensive detection logic based on the trajectory tracking error $e_p$, the state estimation error $\tilde{x}(t)$, and the upper and lower bounds $[\bar{\hat{y}}, \underline{\hat{y}}(t)]$ of the output estimation.

1) The trajectory tracking error $e_p$ is generated through the GCS. When the UAV is in the presence of attacks, the trajectory tracking error $e_p$ is not asymptotically stable. Similarly, AUDs will lead to the decrease in tracking performance, meaning that the tracking error $e_p$ does not converge to zero.

2) The state estimation error $\tilde{x}(t)$ is generated by UIO, which can converge to zero under attacks. Since the desired trajectory attacks are mapped into the control input channel, by special construction, the input channel is masked such that the state estimation error converges to zero under attacks. However, the injection of AUDs causes the state estimation error $\tilde{x}(t)$ to be no longer asymptotically stable.

3) Notice that the interval observer contains the boundary information of the $\Delta d$. Thus, the interval observer is robust to the AUDs but sensitive to attacks. In other words, when no attack occurs, the output $y(t)$ of the system is within the range of interval estimation.

Based on the above analysis, the attack detection logic is described as:

$$flag = \begin{cases} 0,\ e_p \to 0 & \text{Safe} \\ 1,\ e_p \nrightarrow 0 \& \tilde{x} \to 0 & \text{Under attacks} \\ 2,\ e_p \nrightarrow 0 \& \tilde{x} \nrightarrow 0 \& y(t) \in [\bar{\hat{y}}(t), \underline{\hat{y}}(t)] & \text{Under AUDs} \\ 3,\ e_p \nrightarrow 0 \& \tilde{x} \nrightarrow 0 \& y(t) \notin [\bar{\hat{y}}(t), \underline{\hat{y}}(t)] & \text{Under AUDs and attacks} \end{cases} \tag{27}$$

where $flag = 0$, $flag = 1$, $flag = 2$ and $flag = 3$ denote that the UAV is safe, under attacks, under AUDs, under AUDs and attacks, respectively.

**Remark 4** *The proposed detection scheme will lead to missed detection when attacks and AUDs occur simultaneously if it only considers both* $e_p$ *and* $\tilde{x}$*. When the system output signal falls within the interval estimation range of the output vector, it indicates that the system is free from attacks. Thus, the proposed attack detection scheme can avoid the problem of missed detection when attacks and AUDs occur together.*

**Property 4** *The detection logic* Eq. 27 *is not straightforward for us to verify. Thus, an impoved logic is given based on the above detection logic. Firstly, given a small positive constant* $\epsilon$*, we consider* $e_p$ *and* $\tilde{x}(t)$ *to be asymptotically stable if* $|e_p| < \epsilon, |\tilde{x}(t)| < \epsilon$ *is satisfied. Next, define the* $\bar{\tilde{e}}_y(t) = -\bar{e}_y(t), \underline{\tilde{e}}_y(t) = -\underline{e}_y(t)$*, and then define* $\bar{\tilde{e}}_y^{\max}(t), \underline{\tilde{e}}_y^{\max}(t)$ *as the maximal elements of* $\bar{\tilde{e}}_y(t), \underline{\tilde{e}}_y(t)$*. The residual estimation function is given as* $r(t) = \max\{\bar{\tilde{e}}_y^{\max}, \underline{\tilde{e}}_y^{\max}\}$*. The attack detection logic is rewritten as*

$$flag = \begin{cases} 0, & |e_p| \le \epsilon & Safe \\ 1, & |e_p| > \epsilon \& |\tilde{x}| \le \epsilon & Under\ attacks \\ 2, & |e_p| > \epsilon \& |\tilde{x}| > \epsilon \& r(t) \le 0 & Under\ AUDs \\ 3, & |e_p| > \epsilon \& |\tilde{x}| > \epsilon \& r(t) > 0 & Under\ AUDs\ and\ attacks. \end{cases} \tag{28}$$

The variables associated with attack detection are summarized in Table 3.

**Remark 5** *The proposed detection logic is an integrated scheme that contains trajectory tracking errors* $e_p$*, state estimation errors* $\tilde{x}$ *produced by UIO, and residual signals produced by interval observer. However, the above logical determination* Eq. 27 *is not straightforward for us to verify.* $\epsilon$ *is chosen as the threshold to judge whether* $e_p$ *and* $\tilde{x}$ *are approaching* 0*. If* $e_p$ *and* $\tilde{x}$ *are less than* $\epsilon$*, we consider* $e_p$ *and* $\tilde{x}$ *approaching* 0*. Thus, a new equivalent logical determination is given in* Eq. 28*.*

**Remark 6** *The proposed scheme can realize attack detection, when attack and disturbance occur simultaneously. However, for the case that attack added into the same channel with the disturbance, the detection logic is invalid.*

## 4 Attack Estimation Subsystem

After the attack is detected, attack estimation is the key to security control for UAV. According to Eq. 16, we obtain

$$\begin{aligned} \dot{\hat{x}}_{rao}(t) =& A\hat{x}_{rao} + B(u_0(t) + u_c(t)) + L_{rao}z_y(t) + B\hat{F}_a(t), \\ \hat{F}_a(t) =& \Gamma(H_1\dot{z}_y(t) + H_2 z_y(t)), \\ \hat{y}_{rao}(t) =& C\hat{x}_{rao}(t), \end{aligned} \tag{29}$$

where $\hat{x}_{rao}(t)$, $\hat{y}_{rao}(t)$ and $\hat{F}_a(t)$ are the estimation of system state $x(t)$, system output $y(t)$ and attack signal $F_a(t)$. $z_y(t) = y(t) - \hat{y}_{rao}(t)$ is the output estimation error. The matrix $L_{rao}$ is the attack estimation observer gain to be designed. $\Gamma > 0$ is the known adaptive learning rate. $H_1$ and $H_2$ are the parameters matrices used to attack reconstruction. Substituting Eqs. 16 and 29 into $e_{rao}(t) = x(t) - \hat{x}_{rao}(t)$, we obtain

$$\dot{e}_{rao}(t) = (A - L_{rao}C)e_{rao} + B(F_a(t) - \hat{F}_a(t)) + D\Delta d. \tag{30}$$

Consider the robust performance index

$$J(t) = \int_0^{+\infty} (z_y^T(t)z_y(t) - \gamma^2 \Delta^T d\Delta d)dt. \tag{31}$$

To achieve attack estimation accurately, the following theorem is given.

**Lemma 4** [36] *Given the symmetric matrix* $\Pi \in \mathbb{R}^{n\times n}$*,* $\theta \in \mathbb{R}^{n\times m}$*,* $\Xi \in \mathbb{R}^{m\times m}$ *and* $\varphi \in \mathbb{R}^{m\times n}$ *with the appropriate dimensions, it has*

$$\Pi + \theta\Xi\varphi + \varphi^T\Xi^T\theta^T < 0.$$

*There is a necessary and sufficient condition for* $\Xi$ *to be true for* $\Xi^T\Xi \le \mathbf{I}$ *is that exist* $\varepsilon$ *and satisfy*

$$\Pi + \varepsilon\theta\theta^T + \varepsilon^{-1}\varphi^T\varphi < 0.$$

**Theorem 3** *If there exists a symmetric matrix* $Q > 0 \in \mathbb{R}^n$ *and matrices* $Y \in \mathbb{R}^{n\times p}$*,* $S \in \mathbb{R}^m$*,* $H_1 \in \mathbb{R}^{m\times p}$ *and* $H_2 \in \mathbb{R}^{m\times p}$ *such that*

$$\begin{bmatrix} \mathbf{I} & Q^{-1} \\ * & \mathbf{I} \end{bmatrix} \ge 0, \tag{32}$$

$$\begin{bmatrix} \psi_{11} & \psi_{12} & 0 & C^TY^T & QD \\ * & \psi_{22} & H_1C & 0 & H_1CD \\ * & * & -\varepsilon I & 0 & 0 \\ * & * & * & -\varepsilon^{-1}I & 0 \\ * & * & * & * & -\gamma^2 I \end{bmatrix} < 0, \tag{33}$$

*where* $\psi_{11} = QA + A^TQ - YC - C^TY^T + C^TC$*,* $\psi_{12} = QB - C^TH_2^T - A^TC^TH_1^T$*,* $\psi_{22} = -H_1CB - B^TC^TH_1^T +$

**Table 3** Attack detection related variables

| Symbol | Definition | Symbol | Definition |
|---|---|---|---|
| $x(t)$ | UAV system state | $y(t)$ | UAV system output |
| $\hat{x}_{uio}$ | UIO state | $[\bar{\tilde{y}}(t), \underline{\tilde{y}}(t)]$ | Output estimation interval |
| $F_a$ | Attack signal | $\Delta d$ | AUD |
| $\tilde{x}(t)$ | State estimation error | $e_p$ | Trajectory tracking error |
| $REF$ | Residual estimation function | $\epsilon$ | Threshold value |

*S, then the observer gain* $L_{rao} = P^{-T}Y$ *is obtained and the robust performance is guaranteed, that is,* $\|z_y(t)\| \leq \gamma\|\Delta d(t)\| + \sqrt{\kappa}$, *with* $\kappa = \dot{\bar{F}}_a^2\lambda_{max}(\Gamma^{-1}S^{-1}\Gamma^{-1})$.

***Proof*** See Appendix C for details. □

Since Eqs. 32 and 33 contain both $Q, Q^{-1}, \varepsilon$ and $\varepsilon^{-1}$, which are not strictly linear matrix inequalities. Define $\bar{Q} = Q^{-1}, \bar{\varepsilon} = \varepsilon^{-1}$. The inequality solving problem is transformed into an optimization problem as follows:

$$\min_{Q,\varepsilon} \ trace(Q\bar{Q} + \varepsilon\bar{\varepsilon}I), \tag{34}$$

s.t.

$$\begin{bmatrix} \psi_{11} & \psi_{12} & 0 & C^TY^T & 0 \\ * & \psi_{22} & H_1C & 0 & 0 \\ * & * & -\varepsilon I & 0 & 0 \\ * & * & * & -\bar{\varepsilon}I & 0 \\ * & * & * & * & -\gamma^2 I \end{bmatrix} < 0, \tag{35}$$

$$\begin{bmatrix} \mathbf{I} & \bar{Q} \\ * & \mathbf{I} \end{bmatrix} \geq 0, \begin{bmatrix} Q & \mathbf{I} \\ * & Q \end{bmatrix} \geq 0, \begin{bmatrix} \varepsilon & 1 \\ * & \bar{\varepsilon} \end{bmatrix} \geq 0. \tag{36}$$

To solve Eqs. 34-36, Algorithm 1 is summarized as follows:

**Algorithm** 1 Solve the optimization problems Eqs. 34-36.

1. Initialization, set the maximum number of iterations, N;
2. Compute a set of feasible solutions $(Q_0, \bar{Q}_0, S_0, Y_0, H_{10}, H_{20}, \varepsilon_0, \bar{\varepsilon}_0, \gamma_0)$ satisfying Eqs. 35-36;
3. Let $k = 0$;
4. Calculate the optimal solution $(Q, S, Y, H_1, H_2, \varepsilon, \gamma)$, make $min \ trace(Q_k\bar{Q} + Q\bar{Q}_k + \varepsilon_k\bar{\varepsilon}I + \varepsilon\bar{\varepsilon}_k I + \gamma I)$, s.t. Eqs. 35-36;
5. If the Eqs. 32 and 33 hold or $k > N$, the iteration ends;
6. Let $k = k + 1$, compute the next iteration value and return to the Step 4;
7. Compute iteration values and return Step 4;

## 5 Integral Sliding Mode Security Control

In the previous section, we obtain the attack estimation signal through a robust adaptive observer. Subsequently, an ISMSC with an attack compensation mechanism is designed to eliminate the impact of the attack team system inspired by [30]. Let $x_d = [p_d^T, v_d^T]^T, e = [e_p, e_v] = x - x_d$. It follows from Eq. 16 that the closed error system considering attack estimation and compensation is rewritten as

$$\begin{aligned} \dot{e}(t) =& Ax + B(m(K_pe_p + K_ve_v + \ddot{p}_d) + F_a + u_c) + D\Delta d - \dot{x}_d \\ =& \bar{A}e + B(F_a + u_c) + D\Delta d, \end{aligned} \tag{37}$$

where $\bar{A} = \begin{bmatrix} 0 & I \\ K_p & K_v \end{bmatrix}$ and $u_c$ is the secure controller with compensation mechanism, which is designed below. Firstly, a sliding manifold for UAV system is defined as

$$\sigma(t) = We(t) - We(0) - W\int_0^t \bar{A}e(\tau)d(\tau), \tag{38}$$

where $W = (B^TB)^{-1}B^T$ is the given matrix. Furthermore, the term $-We(0)$ is designed to eliminate the reaching phase by ensuring that $\sigma = 0$. We choose the $u_c(t)$ as

$$\begin{aligned} u_c(t) =& -\rho(t)(WB)^{-1}\frac{\sigma(t)}{\|\sigma(t)\|} - \hat{F}_a, \rho(t) \\ \geq& \|WD\bar{\Delta}d\| + \|WB\bar{e}_f(t)\| + \varrho \end{aligned} \tag{39}$$

where $\rho(t)$ is the modulation gain to keep the system trajectories sliding along the sliding surface in Eq. 38. $\hat{F}_a$ is the attack estimation signal. $\varrho > 0$ is a known constant.

Then, the stability of the closed system Eq. 16 with ISMSC Eq. 39 is analyzed. See Appendix D for details.

## 6 Simulation and Analysis

In an effort to verify the effectiveness of proposed detection, estimation and security control schemes, the simulation verification in this paper is based on Matlab R2019b software platform. The UAV system and PID controller gains are given as shown in Table 4. The desired trajectory $p_d(t) = [0.75\sin(\pi t/5), 0.75\cos(\pi t/5), 1]$.

### 6.1 Attack Detection Simulation Results

To examine the detection capability of the proposed methods, bias attacks, hybrid attacks and AUDs are involved. The parameters involved in the simulation for attack detection are shown in Table 5. The upper and lower bounds of AUDs are set as $\bar{\Delta}d = 0.8$ and $\underline{\Delta}d = -0.8$. Using Theorem 1, the gain matrix $L_{uio}$ of the UIO is obtained as

$$L_{uio} = \begin{bmatrix} 0.5\mathbf{I} & 0.5\mathbf{I} \\ 0.5\mathbf{I} & 1.5\mathbf{I} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}.$$

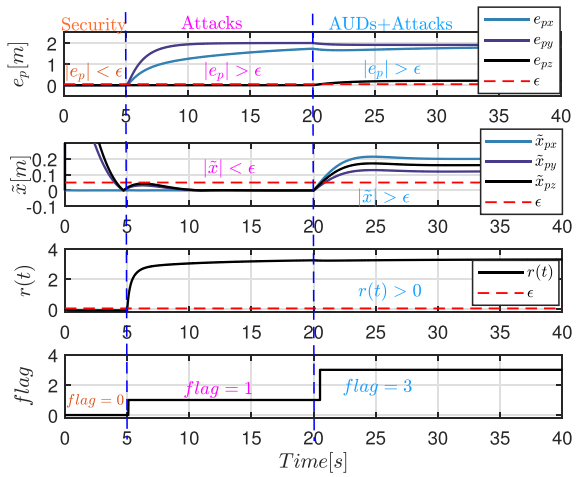
By the introduction of Lemma 2, the matrix $P$ can be calculated, and then $G$ can be obtained $G = \begin{bmatrix} -0.1053 & -0.1053 & 0.3146 & -0.0077 & -0.0154 \end{bmatrix}$. The gain matrix of the interval observers with

$$L_{io} = \begin{bmatrix} 6 & -1 & -1 & 0 & -1 \\ -1 & 6 & -1 & -1 & 0 \\ -0.8946 & -0.8946 & 5.6853 & -0.9923 & -0.9846 \\ -7 & -1 & -1 & -2 & -1 \\ -1 & -7 & -1 & -1 & -2 \end{bmatrix}$$

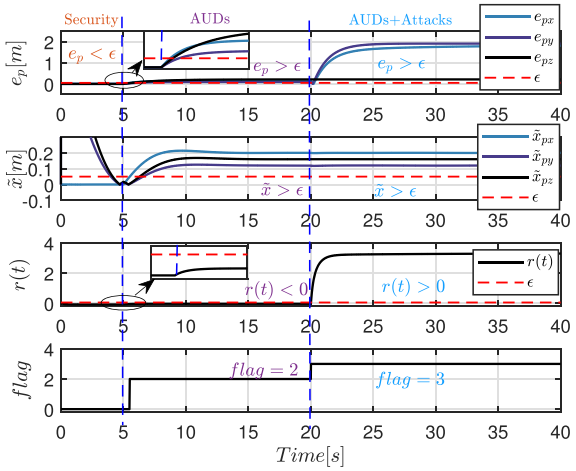
by choosing

$$\Phi = \begin{bmatrix} -6 & 1 & 1 & 1 & 1 \\ 1 & -6 & 1 & 1 & 1 \\ 1 & 1 & -6 & 1 & 1 \\ 1 & 1 & 1 & -6 & 1 \\ 1 & 1 & 1 & 1 & -6 \end{bmatrix}.$$

Set the parameter $\epsilon = 0.05$. When the simulation time reaches $5s$, bias attacks are injected, and after $15s$, both attacks and AUDs are simultaneously injected. The detection results are shown in Fig. 2(a). In another case, AUDs are added between 5 to $20s$, and at $t = 20s$, bias attacks and AUDs are simultaneously injected. Figure 2(b) illustrates the simulation results. Similarly, the detection results of hybrid attacks are shown in Fig. 3.



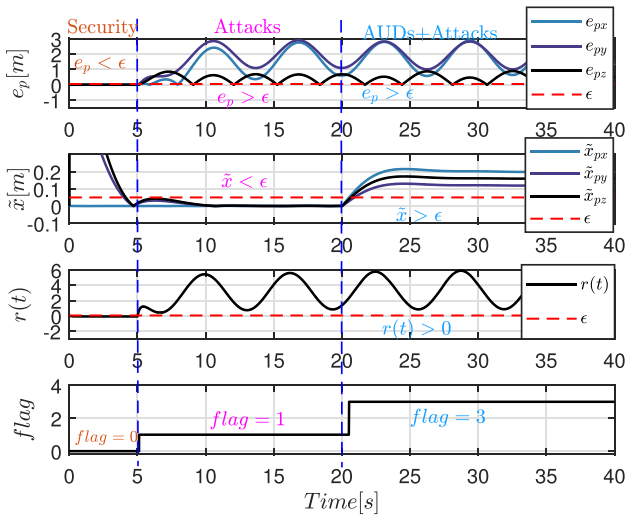

(a) Response of $e_p, \tilde{x}, r(t)$ and alarm under bias attacks /bias attacks and AUDs.



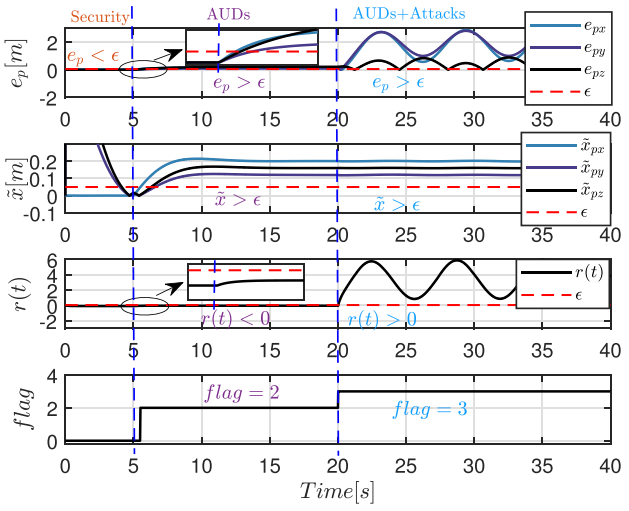

(b) Response of $e_p, \tilde{x}, r(t)$ and alarm under AUDs/bias attacks and AUDs.

**Fig. 2** Response of the state estimation error, tracking error, residual estimation function and alarm under attacks and AUDs. $e_{px}, e_{py}, e_{pz}$ and $\tilde{x}_{px}, \tilde{x}_{py}, \tilde{x}_{pz}$ are the components of the trajectory tracking error and the state estimation error in the X,Y and Z direction, respectively

From Fig. 2(a), it can be observed that: 1) the trajectory tracking error $|e_p| < \epsilon$ for $t < 5s$, indicating the safety of the UAV system; 2) for $5s < t < 20s$, both the trajectory tracking error $|e_p| > \epsilon$ and state estimation error $|\tilde{x}| < \epsilon$, suggesting attacks on the UAV system; and 3) when both conditions of $|e_p| > \epsilon, |\tilde{x}| > \epsilon$, and $r(t) > 0$ are met for $t > 20s$, it indicates simultaneous encounters with attacks and AUDs. From Fig. 2(b), it can be seen that from 5 seconds to 10 seconds, all conditions of $|e_p| > \epsilon, |\tilde{x}| > \epsilon$, and $r(t) < 0$ are satisfied, which implies that only AUDs affect the UAV system during this period. Similarly, Fig. 3 suggests that the detection mechanism is capable of distinguishing hybrid attacks (bias attacks and harmonic attacks) from AUDs




(a) Attack detection under hybrid attacks/hybrid attacks and AUDs.




(b) Attack detection under AUDs/ hybrid attacks and AUDs.

**Fig. 3** Response of the state estimation error, tracking error, residual estimation function and alarm under attacks and AUDs. $e_{px}, e_{py}, e_{pz}$ and $\tilde{x}_{px}, \tilde{x}_{py}, \tilde{x}_{pz}$ are the components of the trajectory tracking error and the state estimation error in the X, Y and Z direction, respectively

**Table 4** UAV and PID controller parameters

| Symbols | Values | Symbols | Values |
|---|---|---|---|
| $m$ | 1.121 $kg$ | $K_p$ | -diag([6,6,6]) |
| $I_{xx}$ | 0.01 $kg \cdot m^2$ | $K_v$ | -diag([8,8,15]) |
| $I_{yy}$ | 0.0082 $kg \cdot m^2$ | $K_\xi$ | diag([2.25,1.85,0.59]) |
| $I_{zz}$ | 0.0148 $kg \cdot m^2$ | $K_\omega$ | diag([0.2,0.16,0.12]) |

With the proposed attack detection mechanism, not only the attack detection can be effectively realized under the two attack types of bias attacks and hybrid attacks, but also the bias/hybrid attacks can be distinguished from the AUDs.

## 6.2 Attack Estimation Simulation Results

The proposed attack estimation scheme is further verified by considering bias attacks and hybrid attacks, respectively. It is assumed that the attacks are injected at $t = 5s$.

Following Algorithm 1, set the maximum number of iterations N=100. Using the LMI toolbox, initial variable values $(Q_0, \bar{Q}_0, S_0, Y_0, H_{10}, H_{20}, \varepsilon_0, \bar{\varepsilon}_0, \gamma_0)$ satisfying Eqs. 35-36 are computed. Then, iterate from $k = 0$ until Eqs. 32 and 33 are satisfied. When $k = 28$, the iteration ends and the optimal solution is obtained as follows:

$$\varepsilon = 0.5917, \gamma = 0.7776$$

$$Q = \begin{bmatrix} 0.3243 & 0 & 0 & 0.0275 & 0 & 0 \\ 0 & 0.3243 & 0 & 0 & 0.0275 & 0 \\ 0 & 0 & 0.5490 & 0 & 0 & -0.0534 \\ 0.0275 & 0 & 0 & 0.4121 & 0 & 0 \\ 0 & 0.0275 & 0 & 0 & 0.4121 & 0 \\ 0 & 0 & -0.0534 & 0 & 0 & 0.2316 \end{bmatrix},$$

$$L_{rao} = \begin{bmatrix} 5.2415 & 0 & 0 & -0.3501 & 0 \\ 0 & 5.2415 & 0 & 0 & -0.3501 \\ 0 & 0 & 3.0362 & 0 & 0 \\ -0.3501 & 0 & 0 & 4.1212 & 0 \\ 0 & -0.3501 & 0 & 0 & 4.1212 \\ 0 & 0 & -0.4383 & 0 & 0 \end{bmatrix},$$

$$H_1 = \begin{bmatrix} 0.0000 & 0 & 0 & 0.0001 & 0 \\ 0 & 0.0001 & 0 & 0 & 0.0000 \\ 0 & 0 & 0.0323 & 0 & 0 \end{bmatrix},$$

**Table 5** Attack detection parameters

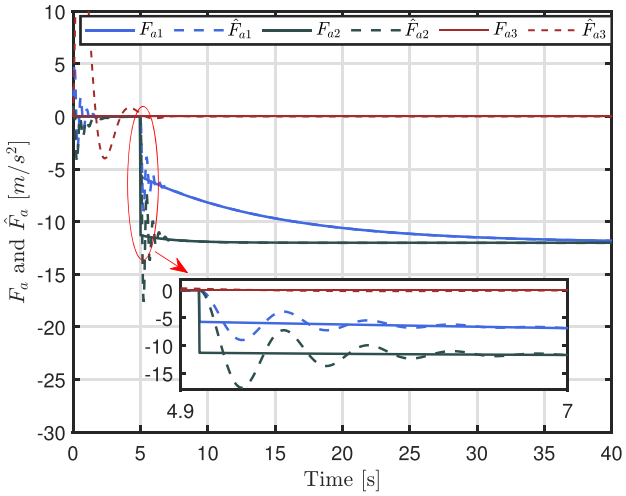
| Section | Parameters |
|---|---|
| Bias attack | $\varpi = diag([0.5, 0.6, 0]), \delta_{b\infty}=[5, 5, 5]^T$ |
| Harmonic attack | $W = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, V = \begin{bmatrix} 543 \\ 000 \end{bmatrix}$ |
| $AUDs$ | $\Delta d = [0.5, 0.3, 0.4]^T$ |
| Matrix $D$ | $[0.2, 0.2, 0.1, 0.1, 0.2, 0.1]^T$ |

$$H_2 = \begin{bmatrix} -0.0275 & 0 & 0 & -0.4121 & 0 \\ 0 & -0.0275 & 0 & 0 & -0.4121 \\ 0 & 0 & 0.0861 & 0 & 0 \end{bmatrix}.$$

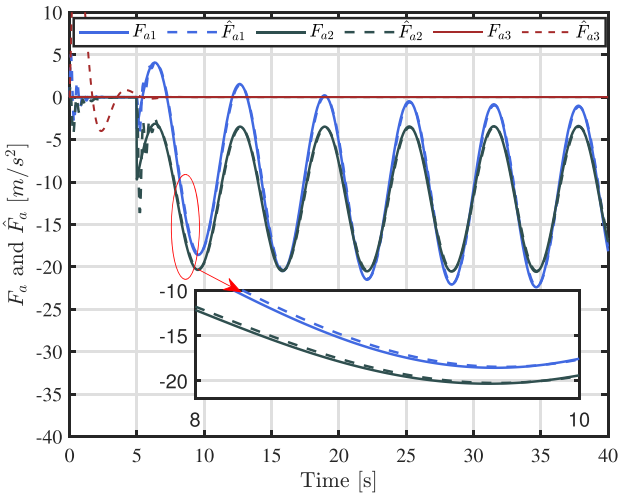
Figure 4(a) and (b) describe the estimation results of biased and hybrid attacks, respectively. The results show that the reconstruction of two attack types, bias attacks, and hybrid attacks, can be achieved using the proposed attack estimation method.

## 6.3 Security Control Simulation Results

After attack detection and estimation, security control is verified in this subsection. Figures 5-8 show the results of security control under two types of attacks. Figure 5 depicts the input signals $u_0, u_f, u_c$ under two attack sce-

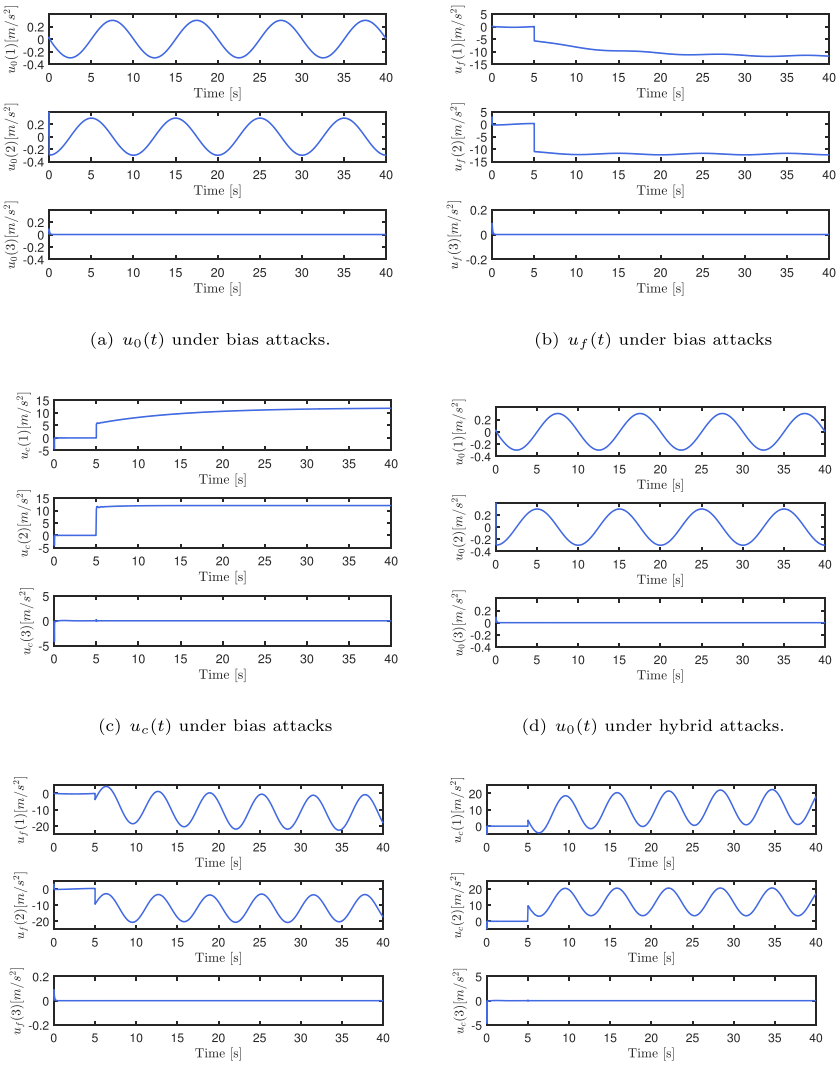



(a) Bias attack signals and their estimations.




(b) Hybrid attacks and their estimations.

**Fig. 4** Response of attacks and their estimations




(a) $u_0(t)$ under bias attacks.

(b) $u_f(t)$ under bias attacks

(c) $u_c(t)$ under bias attacks

(d) $u_0(t)$ under hybrid attacks.

(e) $u_f(t)$ under hybrid attacks.

(f) $u_c(t)$ under hybrid attacks.

**Fig. 5** Input signals under attacks

narios. Figure 5(a)-(c) are the results under bias attacks. Figure 5(d)-(f) denote the input signal under hybrid attacks.

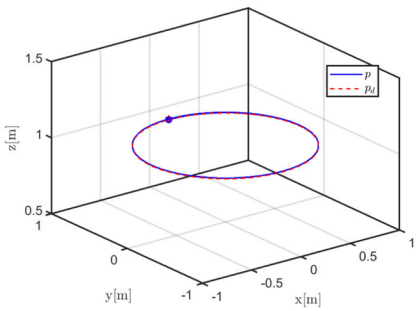
The UAV flight trajectory with bias attacks is depicted in Fig. 6, where Fig. 6(a) describes the trajectory under safe condition, Fig. 6(b) shows the trajectory under bias attacks, Fig. 6(c) describes the UAV flight trajectory $p_c$ under only compensation mechanism, and Fig. 6(d) is the flight trajectory $p_{sc}$ under the proposed ISMSC with compensation mechanism. In the hybrid attack case, similar results are shown in Fig. 7. Figure 8 shows the response of attitude angles and thrust $f$ with bias attacks. $\phi$ is the roll angle under attacks. $\phi_c$ represents roll angle under the attack compensation, $\phi_{sc}$ denotes the roll angle with ISMSC. $\theta, \theta_c, \theta_{sc}, \psi, \psi_c, \psi_{sc}, f, f_c, f_{sc}$ have similar definitions. Figure 9 denotes attitude angles and $f$ under hybrid attacks. It can be concluded that: 1) the flight trajectory of UAV under attack cannot fly according to the desired trajectory; 2) the proposed ISMSC scheme with compensation mechanism has better security performance than the general attack compensation.

## 6.4 Quantitative Assessments

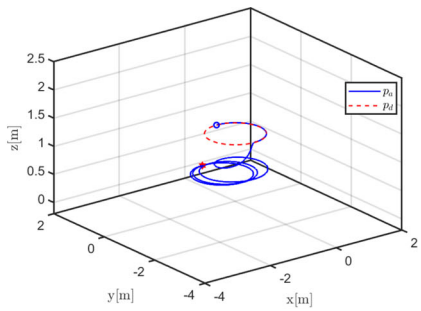
After verifying the feasibility of the proposed scheme, the next step is to provide quantitative assessments that describe the superiority of the proposed scheme. The mean absolute error (MAE) and standard deviation (STD) of both position trajectory and attitude angle tracking are defined as

$$\Upsilon_p = \frac{1}{n}\sum_{i=1}^{n}\|p - p_d\|, \Gamma_p = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(\|p - p_d\| - \Upsilon_p)^2},$$

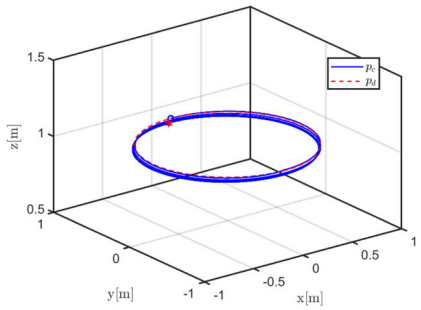
**Fig. 6** UAV trajectory with bias attack



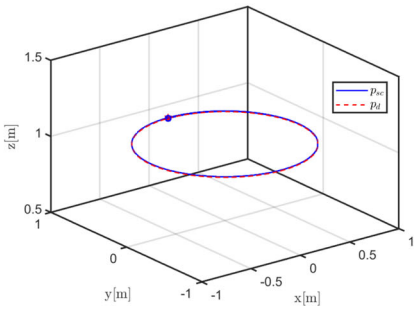

(a) UAV trajectory under safe condition.




(b) UAV trajectory under bias attack.

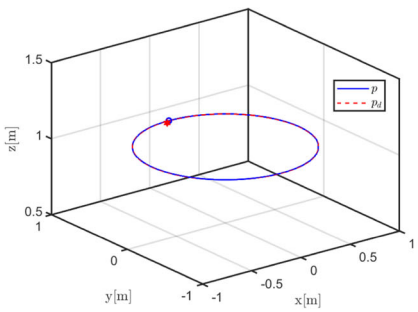



(c) UAV trajectory with compensation.

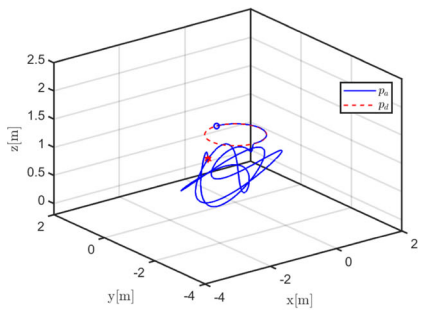



(d) UAV trajectory with our scheme.

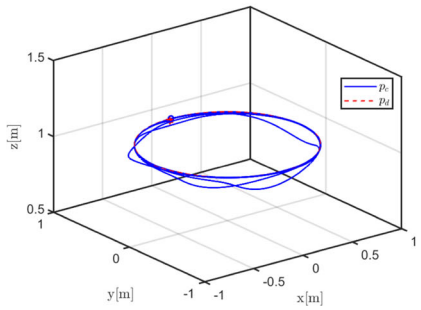
**Fig. 7** UAV trajectory with hybrid attacks



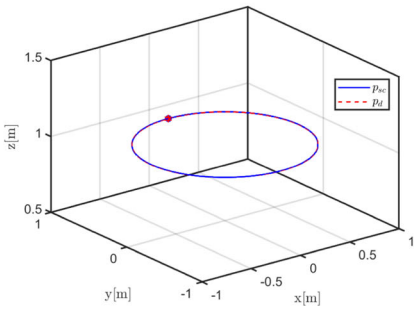

(a) UAV trajectory under safe condition.




(b) UAV trajectory under hybrid attack.

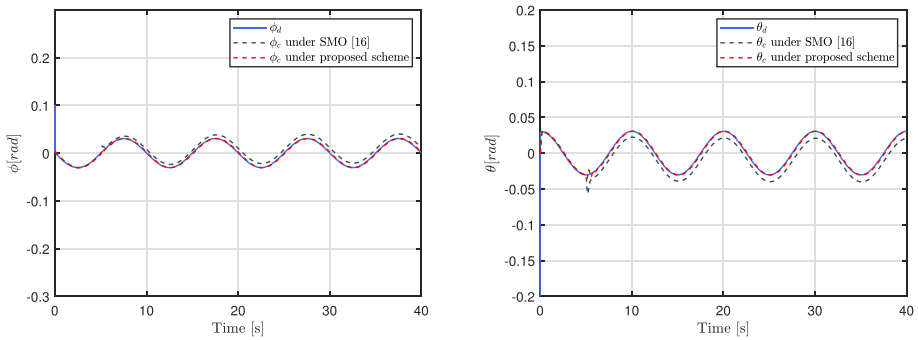



(c) UAV trajectory with compensation.

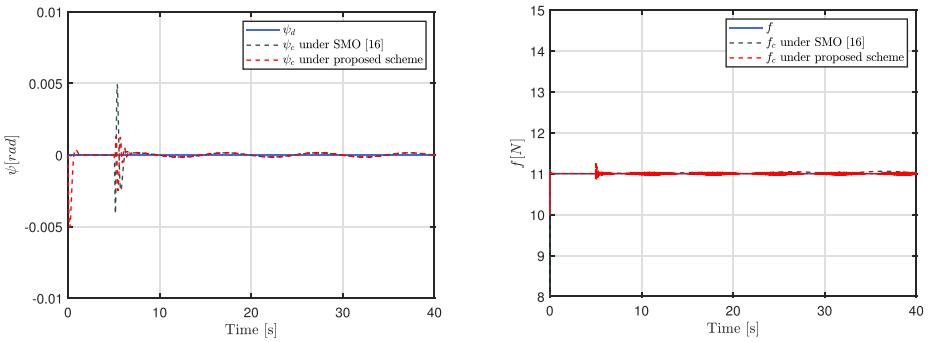



(d) UAV trajectory with our scheme.

**Fig. 8** Response of attitude angles and $f$ under bias attacks

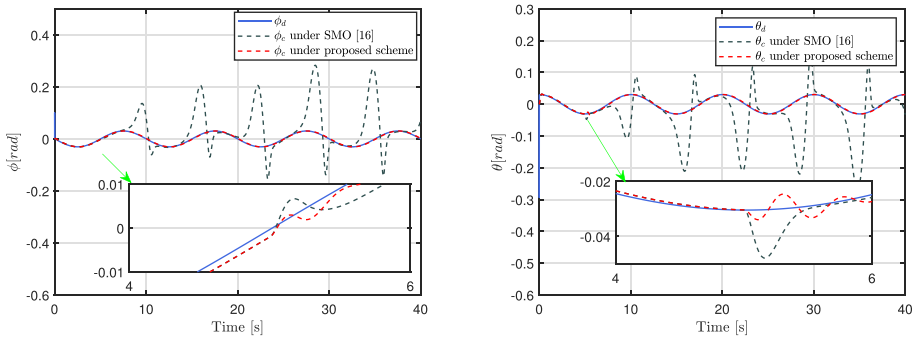



(a) Response of $\phi$ under bias attack. (b) Response of $\theta$ under bias attack.

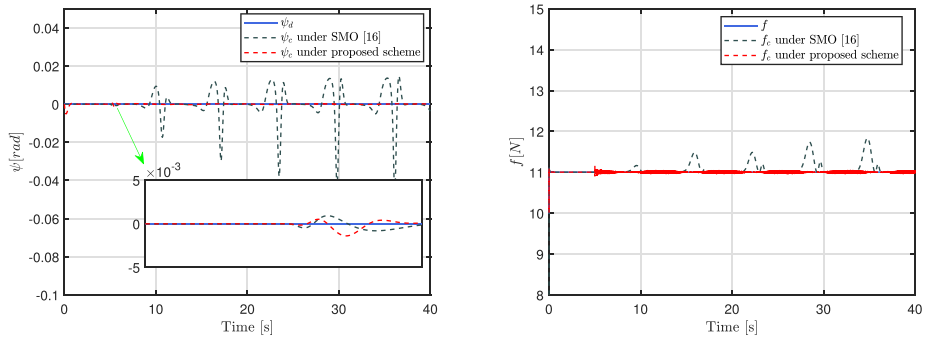



(c) Response of $\psi$ under bias attack. (d) Response of $f$ under bias attack.

**Fig. 9** Response of attitude angles and $f$ under hybrid attacks




(a) Response of $\phi$ under hybrid attacks. (b) Response of $\theta$ under hybrid attacks.




(c) Response of $\psi$ under hybrid attacks. (d) Response of $f$ under hybrid attacks.

**Table 6** Mean absolute error and standard deviation under bias attacks

| Parameters | $\varpi$ | $diag(0.9, 0.8, 0)$ | $diag(0.7, 0.6, 0)$ | $diag(0.4, 0.5, 0)$ | $diag(0.5, 0.5, 0)$ | $diag(0.1, 0.4, 0)$ |
|---|---|---|---|---|---|---|
| | $\delta_\infty$ | $[5, 5, 5]^T$ | $[4, 4, 4]^T$ | $[3, 3, 3]^T$ | $[2, 2, 2]^T$ | $[2, 2, 2]^T$ |
| Proposed scheme | $\Upsilon_p$ | 0.0013 | 0.0012 | 0.0012 | 0.0012 | 0.0012 |
| | $\Gamma_p$ | 0.0025 | 0.0025 | 0.0025 | 0.0025 | 0.0025 |
| | $\Upsilon_\xi$ | 0.0011 | 0.0009 | 0.0008 | 0.0006 | 0.0006 |
| | $\Gamma_\xi$ | 0.0056 | 0.0050 | 0.0045 | 0.0042 | 0.0041 |
| The method of [16] | $\Upsilon_p$ | 2.0573 | 0.8946 | 0.3040 | 0.0220 | 0.0191 |
| | $\Gamma_p$ | 0.8292 | 0.3557 | 0.1007 | 0.0058 | 0.0061 |
| | $\Upsilon_\xi$ | 0.0164 | 0.0143 | 0.0340 | 0.0092 | 0.0086 |
| | $\Gamma_\xi$ | 0.9566 | 0.5181 | 0.0499 | 0.0240 | 0.0238 |

$$\Upsilon_\xi = \frac{1}{n}\sum_{i=1}^{n}\|\xi - \xi_d\|, \Gamma_\xi = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(\|\xi - \xi_d\| - \Upsilon_\xi)^2},$$

where $\Upsilon_p$, $\Upsilon_\xi$ and $\Gamma_p$, $\Gamma_\xi$ are the MAE and STD of position and angel trajectory tracking, respectively. The results of the calculations are listed in Tables 6 and 7.

It follows from results that the MAE and STD of the proposed method are much smaller than the contrast simulation [16]. It can be concluded that the MAE and STD are smaller than the case with only attack compensation.

## 7 Conclusion

This paper presents a security control scheme for UAVs under desired trajectory attack with detection, estimation, and compensation. Firstly, most of the existing works only consider attack detection, but the proposed scheme can not only detect attacks but also identify attacks and AUDs. Secondly, the RAO is designed to estimate the effects of attacks on control systems without equality constraint compared with the SMO. Finally, the ISMSC scheme is designed based on reconstructed attacks to solve the problem of unknown upper bound uncertainty.

The future work will focus on addressing secure control for UAVs facing simultaneous attacks such as DoS attacks and GPS deception attacks

## Appendix A Proof of Theorem 1

Let $R + H = I$. It follows from Eq. 16 that

$$\dot{x} = RAx + RD\Delta d + RB(F + F_a + u_c(t)) + H\dot{x}. \quad \text{(A.1)}$$

The state estimation error $\tilde{x}$ can be obtained as

$$\begin{aligned}\dot{\tilde{x}} &= RAx + RD\Delta d + RB(F + F_a + u_c(t)) \\ &\quad + H\dot{x} - RA\hat{x}_{uio} - L_{uio}C(x - \hat{x}_{uio}) - H\dot{x} \\ &= (RA - L_{uio}C)\tilde{x} + RB(F + F_a + u_c(t)) + RD\Delta d.\end{aligned}$$

**Table 7** Mean absolute error and standard deviation under hybrid attacks

| Parameters | $\varpi$ | $diag(0.9, 0.8, 0)$ | $diag(0.7, 0.6, 0)$ | $diag(0.4, 0.5, 0)$ | $diag(0.5, 0.5, 0)$ | $diag(0.1, 0.4, 0)$ |
|---|---|---|---|---|---|---|
| | $\delta_\infty$ | $[5, 5, 5]^T$ | $[4, 4, 4]^T$ | $[3, 3, 3]^T$ | $[2, 2, 2]^T$ | $[2, 2, 2]^T$ |
| | $\mathcal{W}_{ha}$ | $\begin{bmatrix}0 & 3\\ -3 & 0\end{bmatrix}$ | $\begin{bmatrix}0 & 0.5\\ -0.5 & 0\end{bmatrix}$ | $\begin{bmatrix}0 & 2\\ -2 & 0\end{bmatrix}$ | $\begin{bmatrix}0 & 1.5\\ -1.5 & 0\end{bmatrix}$ | $\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$ |
| | $\mathcal{V}_{ha}$ | $\begin{bmatrix}0.8 & 0.9 & 0\\ 0 & 0 & 0\end{bmatrix}$ | $\begin{bmatrix}0.5 & 0.6 & 0\\ 0 & 0 & 0\end{bmatrix}$ | $\begin{bmatrix}1 & 2 & 0\\ 0 & 0 & 0\end{bmatrix}$ | $\begin{bmatrix}4 & 2 & 0\\ 0 & 0 & 0\end{bmatrix}$ | $\begin{bmatrix}5 & 4 & 0\\ 0 & 0 & 0\end{bmatrix}$ |
| Proposed scheme | $\Upsilon_p$ | 0.0013 | 0.0012 | 0.0012 | 0.0012 | 0.0012 |
| | $\Gamma_p$ | 0.0025 | 0.0025 | 0.0025 | 0.0025 | 0.0025 |
| | $\Upsilon_\xi$ | 0.0013 | 0.0008 | 0.0009 | 0.0007 | 0.0006 |
| | $\Gamma_\xi$ | 0.0052 | 0.0046 | 0.0044 | 0.0040 | 0.0039 |
| The method of [16] | $\Upsilon_p$ | 2.0562 | 0.9033 | 0.2791 | 0.0740 | 0.0678 |
| | $\Gamma_p$ | 0.8488 | 0.3706 | 0.1798 | 0.0727 | 0.0859 |
| | $\Upsilon_\xi$ | 0.0557 | 0.0160 | 0.0462 | 0.0513 | 0.0417 |
| | $\Gamma_\xi$ | 0.9142 | 0.5263 | 0.2718 | 0.1081 | 0.0963 |

Submitting $RB = 0$ into the above formula renders:

$$\dot{\tilde{x}} = (RA - L_{uio}C)\tilde{x} + RD\Delta d. \tag{A.2}$$

The Lyapunov function candidate is chosen as : $V_1(t) = \tilde{x}^T P\tilde{x}$. Calculating the time derivatives of $V_1(t)$ with respect to time $t$, we obtain

$$\dot{V}_1(t) = \tilde{x}^T(P(RA - L_{uio}C) + (RA - L_{uio}C)^T P)\tilde{x}.$$

Consequently, if Eq. 21 holds, the state estimation error of $\tilde{x}$ is asymptotically stable. The proof is completed.

## Appendix B Proof of Theorem 2

Denote $\bar{\underline{e}}_y(t) = [\bar{e}_y^T(t), \underline{e}_y^T(t)]^T$. Based on Eqs. 23 and 24, it can obtain

$$\dot{\bar{\underline{e}}}_y(t) = \bar{\Psi}\bar{\underline{e}}_y(t) + \bar{A}_{12}e_{h2}(t) + D_d, \tag{B.1}$$

where $e_{h2}(t) = h_2(t) - \hat{h}_2(t)$ and

$$\begin{aligned} \bar{\Psi} &= \begin{bmatrix} \Psi & 0 \\ 0 & \Psi \end{bmatrix}, \bar{A}_{12} = \begin{bmatrix} -A_{12} \\ A_{12} \end{bmatrix}, \\ D_d &= \begin{bmatrix} D_1^+\bar{\Delta}_d - D_1^-\underline{\Delta}_d - D_1\Delta_d \\ -D_1^+\underline{\Delta}_d + D_1^-\bar{\Delta}_d + D_1\Delta_d \end{bmatrix}. \end{aligned} \tag{B.2}$$

According to Lemma 1 and Eq. 25, it has $\underline{y}(0) \le y(0) \le \bar{y}(0)$ which implies $\bar{\underline{e}}_y(t) > 0$, $D_d > 0$. By Lemma 2, one has

$$\begin{bmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{bmatrix}\begin{bmatrix} A_{11} - L_1 & A_{12} \\ A_{21} - L_2 & A_{22} \end{bmatrix} + \begin{bmatrix} A_{11} - L_1 & A_{12} \\ A_{21} - L_2 & A_{22} \end{bmatrix}^T \begin{bmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{bmatrix}^T < 0, \tag{B.3}$$

which implies

$$\Lambda = \begin{bmatrix} \Lambda_{11} & \Lambda_{12} \\ * & \Lambda_{22} \end{bmatrix} < 0, \tag{B.4}$$

where $\Lambda_{11} = P_{11}(A_{11} - L_1) + (A_{11} - L_1)^T P_{11}^T + P_{12}(A_{21} - L_2) + (A_{21} - L_2)^T P_{12}^T$, $\Lambda_{12} = P_{11}A_{12} + A_{12}^T P_{11}^T + P_{12}A_{22} + A_{22}^T P_{12}^T$, $\Lambda_{22} = P_{21}A_{12} + A_{12}^T P_{21}^T + P_{22}A_{22} + A_{22}^T P_{22}^T$. Let $G = P_{22}^{-1}P_{21}$. Since $\Lambda_{22} < 0$, we have

$$P_{22}(A_{22} + KA_{12}) + (A_{22} + KA_{12})^T P_{22}^T < 0. \tag{B.5}$$

The state estimation error is calculated

$$e_x = \begin{bmatrix} h_1 \\ h_2 - Gh_1 \end{bmatrix} - \begin{bmatrix} h_1 \\ \hat{h}_2 - Gh_1 \end{bmatrix} = \begin{bmatrix} 0 \\ e_{h2} \end{bmatrix}. \tag{B.6}$$

Based on Eqs. 24 and 25, the estimation error is obtained as

$$\dot{e}_{h2}(t) = (A_{22} + KA_{12})e_{h2}(t). \tag{B.7}$$

If the inequality Eq. B.5 holds, the error system Eq. B.7 is asymptotically stable, that is, $\lim_{t\to\infty} e_{h2}(t) = 0$. Thus, $\bar{A}_{12}e_{h2}(t) + D_d > 0$ holds for all $t > t_w$. Combing Lemma 3, it follows taht $\bar{\underline{e}}_y(t) > 0$, that is, $\underline{y}(t) \le y(t) \le \bar{y}(t)$. Theorem 2 is proved.

## Appendix C Proof of Theorem 3

To make analysis on the stability of system Eq. 30, the Lyapunov function is taken

$$V_2 = e_{rao}^T Q e_{rao} + e_F^T \Gamma^{-1} e_F, \tag{C.1}$$

where $Q$ is the Lyapunov matrix to be designed. The time derivative Lyapunov function along with Eq. 30 can be computed by

$$\begin{aligned} \dot{V}_2(t) &= 2e_{rao}^T Q\dot{e}_{rao} + 2e_F^T\Gamma^{-1}\dot{e}_F \\ &\le 2e_{rao}^T Q[(A - L_{rao}C)e_{rao} + Be_F(t) + D\Delta d] \\ &+ 2e_F^T(t)\Gamma^{-1}\dot{F}_a - 2e_F^T H_1\dot{z}_y - 2e_F^T H_2 z_y \end{aligned} \tag{C.2}$$

It has

$$\begin{aligned} 2e_F^T(t)\Gamma^{-1}\dot{F}_a \le e_F^T S e_F + \dot{F}_a^T\Gamma^{-1}S^{-1}\Gamma^{-1}\dot{F}_a \le e_F^T S e_F \\ + \dot{\bar{F}}_a^2\lambda_{max}(\Gamma^{-1}S^{-1}\Gamma^{-1}). \end{aligned} \tag{C.3}$$

Defining $\kappa = \dot{\bar{F}}_a^2\lambda_{max}(\Gamma^{-1}S^{-1}\Gamma^{-1})$ and substituting Eq. C.3 into Eq. C.2 yields that

$$\begin{aligned} \dot{V}_2(t) \le\ & 2e_{rao}^T Q[(A - L_{rao}C)e_{rao} + Be_F + D\Delta d] \\ & - 2e_F^T H_1 C(A - L_{rao}C)e_{rao} \\ & - 2e_F^T H_1 CBe_F + 2e_F^T H_2 Ce_{rao} + e_F^T S e_F \\ & - 2e_F^T H_2 Ce_{rao} + \kappa. \end{aligned} \tag{C.4}$$

In the zero initial condition, Eq. 31 can be rewritten as

$$\begin{aligned} & J(t) - \gamma^2 F_a^T(\tau)F_a(\tau) + \dot{V}(\tau))d\tau - V_2(t) \\ &= \int_0^{+\infty} (z_y^T(\tau)z_y(\tau) - \gamma^2\Delta d^T\Delta d \\ &+ \dot{V}_2(\tau))d\tau - \int_0^{+\infty} \dot{V}_2(\tau)d\tau \\ &= \int_0^{+\infty} (z_y^T(\tau)z_y(\tau) - \gamma^2\Delta d^T\Delta d \\ &+ \dot{V}_2(\tau))d\tau - V(\infty) + V(0) \\ &\le \int_0^{+\infty} (z_y^T(\tau)z_y(\tau) - \gamma^2\Delta d^T\Delta d + \dot{V}_2(\tau))d\tau \end{aligned} \tag{C.5}$$

Defining $\eta(t) = [e_{rao}^T, e_F^T, \Delta^T d]^T$, it follows from Eq. C.4 that one can obtain $z_y^T(\tau)z_y(\tau) - \gamma^2\Delta d^T\Delta d + \dot{V}_2(\tau) = \eta^T(\tau)\Theta\eta(\tau) + \kappa$,where

$$\Theta = \begin{bmatrix} \Theta_{11} & \Theta_{12} & \Theta_{13} \\ * & \Theta_{22} & \Theta_{23} \\ * & * & \Theta_{33} \end{bmatrix} \tag{C.6}$$

with $\Theta_{11} = Q(A - L_{rao}C) + (A - L_{rao}C)^T Q^T + C^T C$, $\Theta_{12} = QB - (A - L_{rao}C)^T C^T H_1^T - C^T H_2^T$, $\Theta_{13} = QD$, $\Theta_{22} = S - He(H_1CB)$, $\Theta_{23} = H_1CD$, $\Theta_{33} = -\gamma^2 I$. Define the $Y = QL_{rao}$. Furthermore, it has:

$$\begin{aligned}\Theta = &\begin{bmatrix} QA + A^TQ - YC - C^TY^T & QB - C^TH_2^T - A^TC^TH_1^T & QD \\ * & S - He(H_1CB) & H_1CD \\ * & * & -\gamma^2 I \end{bmatrix} \\ &+ \begin{bmatrix} 0 \\ H_1C \\ 0 \end{bmatrix} Q^{-1} \begin{bmatrix} YC & 0 & 0 \end{bmatrix} + \begin{bmatrix} C^TY^T \\ 0 \\ 0 \end{bmatrix} Q^{-1} \begin{bmatrix} 0 & C^TH_1^T & 0 \end{bmatrix}.\end{aligned} \tag{C.7}$$

By Lemma 4, if $Q^{-2} \leq I$, there exists $\varepsilon > 0$, $\Theta$ is rewritten as

$$\begin{aligned}\Theta = &\begin{bmatrix} QA + A^TQ - YC - C^TY^T & QB - C^TH_2^T - A^TC^TH_1^T - C^TC & QD \\ * & S - H_1CB - B^TC^TH_1^T & H_1CD \\ * & * & -\gamma^2 I \end{bmatrix} \\ &+ \varepsilon^{-1} \begin{bmatrix} 0 \\ H_1C \\ 0 \end{bmatrix} \begin{bmatrix} YC & 0 & 0 \end{bmatrix} + \varepsilon \begin{bmatrix} C^TY^T \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & C^TH_1^T & 0 \end{bmatrix}.\end{aligned} \tag{C.8}$$

Using the projection theorem and Schur complement lemma, the Eq. 33 is obtained. If Eqs. 32 and 33 hold, it implies $J < \kappa$.

## Appendix D Stability analysis of the ISMSC

Using Eqs. 37, 38 and 39, one has

$$\begin{aligned}\dot{\sigma}(t) =& W\dot{e}(t) - W\bar{A}e(t) \\ =& W(Ae(t) + B(F_a + u_c(t) + D\Delta d) - WAe(t) \\ =& W(Ae(t) + B(F_a - \rho(t)\frac{\sigma(t)}{\|\sigma(t)\|} - \hat{F}_a + D\Delta d) - WAe(t) \\ =& -\rho(t)\frac{\sigma(t)}{\|\sigma(t)\|} + WBe_f(t) + WD\Delta d.\end{aligned} \tag{D.1}$$

Choose the Lyapunov function as $V_3(t) = \frac{1}{2}\sigma^T(t)\sigma(t)$. By taking the derivative, it yields

$$\begin{aligned}\dot{V}_3(t) =& \sigma(t)^T\dot{\sigma}(t) = -\rho(t)\|\sigma(t)\| + \sigma(t)^T WBe_f(t) \\ &+ \sigma(t)^T WD\Delta d \\ \leq& \|\sigma(t)\|(-\rho(t) + \|WEe_f(t)\| + \|WD\Delta d\|).\end{aligned} \tag{D.2}$$

Following Theorem 3, the attack error $e_f(t)$ is bounded. Note that if we choose $\rho(t) \geq \|WD\bar{\Delta}d\| + \|WB\bar{e}_f(t)\| + \varrho$, where $\varrho > 0$ is a known constant, one has

$$\dot{V}_3(t) \leq -\varrho\|\sigma(t)\| = -\varrho\sqrt{2V_3(t)}. \tag{D.3}$$

It follows from Eq. D.3 that $\sqrt{2V_3(t)} - \sqrt{2V_3(0)} \leq -\varrho t$. In finite time $\frac{\sqrt{2V_3(0)}}{\varrho}$, the Lyapunov function approaches 0.

**Author Contributions** All authors contributed to the study conception and design. Methodology, software, formal analysis, validation and supervision were performed by [Kunpeng Pan], [Yang Lyu], [Feisheng Yang], [Zheng Tan] and [Quan Pan]. The first draft of the manuscript was written by [Kunpeng Pan] and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

**Funding** This work was supported by the National Natural Science Foundation of China (grant numbers 62073269, 61790552, 62203358, 62233014), the Key Research & Development Project in Shaanxi Province (Program No. 2022GY-244), the Aeronatical Science Foundation of China (grant number 2020Z034053002),the Natural Science Foundation of Chongqing, China, (grant number CSTB2022NSCQ-MSX0963) and Guangdong Basic and Applied Basic Research Foundation (grant number 2023A1515011220).

## Declarations

**Competing Interests** The authors have no relevant financial or non-financial interests to disclose.

## References


1. Guo, K., Jia, J., Yu, X., Guo, L., Xie, L.: Multiple observers based anti-disturbance control for a quadrotor uav against payload and wind disturbances. Control. Eng. Pract. **102**, 104560 (2020)
2. Li, Y., et al.: Angular acceleration estimation-based incremental nonlinear dynamic inversion for robust flight control. Control. Eng. Pract. **117**, 104938 (2021)
3. Hao, L.-Y., Zhang, H., Li, T.-S., Lin, B., Chen, C.L.P.: Fault tolerant control for dynamic positioning of unmanned marine vehicles based on t-s fuzzy model with unknown membership functions. IEEE Trans. Veh. Technol. **70**, 146–157 (2021)
4. Hao, L.-Y., Zhang, H., Guo, G., Li, H.: Quantized sliding mode control of unmanned marine vehicles: various thruster faults tolerated with a unified model. IEEE Transactions on Systems, Man, and Cybernetics: Systems **51**, 2012–2026 (2021)
5. Hao, L.-Y., Yu, Y., Li, T.-S., Li, H.: Quantized output-feedback control for unmanned marine vehicles with thruster faults via sliding-mode technique. IEEE Transactions on Cybernetics **52**, 9363–9376 (2022)
6. Pan, K., Yang, F., Feng, Z. Pan, Q.: Attack estimation–based resilient control for cyber-physical power systems. Trans Ins Meas Control (2022)
7. Su, Q., Wang, H., Sun, C., Li, B., Li, J.: Cyber-attacks against cyber-physical power systems security: state estimation, attacks reconstruction and defense strategy. Appl. Math. Comput. **413**, 126639 (2022)
8. Pajic, M., et al.: Design and implementation of attack-resilient cyberphysical systems: with a focus on attack-resilient state estimators. IEEE Control Syst. Mag. **37**, 66–81 (2017)
9. Hartmann, K. Steup, C.: The vulnerability of uavs to cyber attacks-an approach to the risk assessment. Paper presented at 5th international conference on cyber conflict (CYCON 2013) 1–23 (2013)
10. Krishna, C.G.L., Murphy, R.R.A., review on cybersecurity vulnerabilities for unmanned aerial vehicles. notePaper presented at,: IEEE International Symposium on Safety. Secur Res Robot (SSRR) **194–199**, 2017 (2017)
11. Gu, Y., Yu, X., Guo, K., Qiao, J., Guo, L.: Detection, estimation, and compensation of false data injection attack for uavs. Inf. Sci. **546**, 723–741 (2021)
12. Chen, W.-H., Hsu, S.-H., Shen, H.-P.: Application of svm and ann for intrusion detection. Comput. Oper. Res. **32**, 2617–2634 (2005)
13. Hamedani, K., et al.: Detecting dynamic attacks in smart grids using reservoir computing: a spiking delayed feedback reservoir based approach. IEEE Trans Emerg Topics Comput Intell **4**, 253–264 (2019)
14. Deng, R., Xiao, G., Lu, R.: Defending against false data injection attacks on power system state estimation. IEEE Trans. Industr. Inf. **13**, 198–207 (2015)
15. Liu, L., Esmalifalak, M., Ding, Q., Emesih, V.A., Han, Z.: Detecting false data injection attacks on power grid by sparse optimization. IEEE Transactions on Smart Grid **5**, 612–621 (2014)
16. Su, Q., Li, S., Gao, Y., Huang, X., Li, J.: Observer-based detection and reconstruction of dynamic load altering attack in smart grid. J. Franklin Inst. **358**, 4013–4027 (2021)
17. Guo, Z., Shi, D., Johansson, K.H., Shi, L.: Optimal linear cyber-attack on remote state estimation. IEEE Trans. Control Netw. Syst. **4**, 4–13 (2017)
18. Ye, D., Zhang, T.-Y.: Summation detector for false data-injection attack in cyber-physical systems. IEEE Trans. Cybern. **50**, 2338–2345 (2020)
19. Zhong, M., Song, Y., Ding, S.X.: Parity space-based fault detection for linear discrete time-varying systems with unknown input. Automatica **59**, 120–126 (2015)
20. Ao, W., Song, Y., Wen, C.: Adaptive cyber-physical system attack detection and reconstruction with application to power systems. IET Control Theory Appl. **10**, 1458–1468 (2016)
21. Mishra, S., Shoukry, Y., Karamchandani, N., Diggavi, S.N., Tabuada, P.: Secure state estimation against sensor attacks in the presence of noise. IEEE Trans. Control of Netw. Syst. **4**, 49–59 (2017)
22. Shinohara, T., Namerikawa, T., Qu, Z.: Resilient reinforcement in secure state estimation against sensor attacks with a priori information. IEEE Trans. Autom. Control **64**, 5024–5038 (2019)
23. Ao, W., Song, Y., Wen, C.: Distributed secure state estimation and control for cpss under sensor attacks. IEEE Trans. Cybern. **50**, 259–269 (2020)
24. An, L., Yang, G.-H.: Secure state estimation against sparse sensor attacks with adaptive switching mechanism. IEEE Trans. Autom. Control **63**, 2596–2603 (2018)
25. Guan, Y., Ge, X.: Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks. IEEE Trans. Signal Inform. Process. over Netw. **4**, 48–59 (2017)
26. Gu, Y., et al.: An enhanced uav safety control scheme against attacks on desired trajectory. Aerosp. Sci. Technol. **119**, 107212 (2021)
27. Salih, A.L., Moghavvemi, M., Mohamed, H.A., Gaeid, K.S.: Modelling and pid controller design for a quadrotor unmanned air vehicle. Paper presented at 2010 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), 1–5 (2010)
28. Argentim, L.M., Rezende, W.C., Santos, P.E. Aguiar, R.A.: Pid, lqr and lqr-pid on a quadcopter platform. Paper presented at 2013 International Conference on Informatics, Electronics and Vision (ICIEV), pp. 1–6 (2013)
29. Dydek, Z.T., Annaswamy, A.M., Lavretsky, E.: Adaptive control of quadrotor uavs: a design trade study with flight evaluations. IEEE Trans. Control Syst. Technol. **21**, 1400–1406 (2012)
30. Mu, B., Zhang, K., Shi, Y.: Integral sliding mode flight controller design for a quadrotor and the application in a heterogeneous multi-agent system. IEEE Trans. Industr. Electron. **64**, 9389–9398 (2017)
31. Teixeira, A., Shames, I., Sandberg, H., Johansson, K.H.: A secure control framework for resource-limited adversaries. Automatica **51**, 135–148 (2015)
32. Guo, L., Chen, W.-H.: Disturbance attenuation and rejection for systems with nonlinearity via dobc approach. Int. J. Robust Nonlinear Control: IFAC-Affiliated J. **15**, 109–125 (2005)
33. Zhu, Y., Qiao, J., Guo, L. Han, C.: Observer-based attitude control for flexible spacecrafts under actuator fault and actuator saturation. Paper presented at the 27th Chinese Control and Decision Conference (2015 CCDC), pp. 508–513 (2015)
34. Shan, Y., Zhu, F.: Interval observer-based fault tolerant control strategy with fault estimation and compensation. Asian J. Control **24**, 895–906 (2022)
35. Farina, L. Rinaldi, S.: Positive linear systems: theory and applications Wiley, vol. 50, (2000)
36. Pan, K., Yang, F., Feng, Z. Pan, Q.: Attack reconstruction for a class of cyber-physical systems with altering load. Paper presented at 2021 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS), pp. 78–83 (2021)

**Kunpeng Pan** received the B.Sc. degree in automation in 2017 from Dalian Ocean University, China, and the M.Sc. degree in control theory and application in 2020 from Northeast Electric Power University, China. He is currently working toward the Ph.D. degree in control theory and applications with the School of Automation, Northwestern Polytechnical University, China. His research interests include switched systems, cyber-physical-systems, and secure control.

**Yang Lyu** received the Ph.D. degree in control theory and applications from Northwestern Polytechnical University, Xi'an, China, in 2019. He was a Research Fellow with Nanyang Technological University Singapore, under the STE-NTU Corporate Lab from 2019 to 2021. He is currently an Associate Professor with Northwestern Polytechnical University. His current research interests include information fusion for robotic systems and resilient robotic systems.

**Feisheng Yang** received the Ph.D. degree in control theory and control engineering from Northeastern University, Shenyang, China, in 2013. He was a Postdoctoral Fellow with Xi'an Jiaotong University, Xi'an, China, in 2018, an Associate Professor with the Northwestern Polytechnical University (NPU), Xi'an, China, in 2014, and a Visiting Associate Professor with the Department of Computer Science and Information Technology, La Trobe University, Melbourne, VIC, Australia, in 2015. From 2016 to 2017, he was a Visiting Scholar with the Department of Mechanical and Aerospace Engineering, University of California at San Diego, La Jolla, CA, USA. Since 2018, he has been the Deputy Director of the Institute of Control, Privacy and Security for Cyber-physical Systems (iCPS2) with NPU. He is currently a Ph.D supervisor. His research interests include event-triggered communication and networked control, distributed optimization and resource allocation, and cyber security and intelligent control.

**Zheng Tan** is a PhD candidate in control theory and applications from Northwestern Polytechnical University, Xi'an, China. He graduated from Civil Aviation University of China with a master's degree from 2017 to 2020. He is currently a PhD candidate with Northwestern Polytechnical University. His research interests include information fusion for robotic systems and UAV control and navigation.

**Quan Pan** was born in China, in 1961. He received the bachelor's degree in automatic control from the Huazhong University of Science and Technology, Wuhan, China, in 1982, and the master's and Ph.D. degrees in control science and engineering from Northwestern Polytechnical University (NPU), Xi'an, China, in 1991 and 1997, respectively. He has been a professor with the School of Automation, NPU, since 1998. His main research interests include pattern recognition and information fusion.