Path Invariance of a Quadrotor System under Cyber Attacks with Theoretical Guarantees

Hamza Mahmood* Usman Ali† Adeel Akhtar*

***Abstract*—This paper presents a path-following controller for a quadrotor system to guarantee safe maneuvers, in terms of forward path invariance, in the presence of cyber-physical attacks. We assume that an adversarial agent can control any one of the rotors through a false data injection (FDI) type of attack. A feedback controller is designed using transverse feedback linearization which guarantees that the system follows a class of smooth curves under FDI attacks. Our proposed controller is computationally efficient, with a closed-form analytical expression, that not only mitigates the effect of bounded malicious signal but also ensures mission success. We provide theoretical guarantees of forward path invariance under FDI attacks with realistic assumptions and demonstrate the effectiveness of our approach through simulation.**

***Index Terms*—Path following, geometric control, adversarial agent, set invariance, cyber-physical attacks.**

I. Introduction

Unmanned aerial vehicles (UAVs) such as quadrotors have important applications in many areas such as search and rescue, emergency management, package delivery, surveillance, agriculture, and drone photography. In all these applications, a typical mission involves a high-level path planning task of finding an obstacle-free path and then a low-level control task of designing a control policy to track the planned trajectory in a safe manner [1]. One way of ensuring safety is to render the path forward-invariant [2], [3]. Achieving invariance (safe maneuver), however, in the presence of cyber-physical attacks is a challenging problem. The design of a controller that can guarantee forward path invariance in the presence of adversarial attacks is the main focus of this paper.

The problem of trajectory tracking for quadrotors has been considered in [4] in the presence of cyber-physical attacks. However, as highlighted in [5], typical trajectory tracking solutions have performance limitations; they cannot guarantee that a system stays on a trajectory once it reaches it. These limitations are overcome in [6], [7], where the authors provided an alternative path-following controller that ensures that the system sticks to the path, once it hits the trajectory, by providing guarantees on forward path invariance, and that has essentially better safety properties. These works, however, do not consider adversarial attacks. In this paper, we aim to design a controller that can ensure safety during path-following using forward path-invariance in the presence of cyber-physical attacks.

A problem somewhat similar, but fundamentally different, is considered in [8] where the authors provide a set invariance argument but it is *not* path invariance. Specifically, their controller guarantees that the system stays within a bound of the desired point or trajectory, while in our work, we want to ensure that once the system reaches the curve, it never leaves the curve. Hence, the goal of our controller design is to make the given path asymptotically stable and forward invariant.

In this paper, we consider a particular type of cyber-physical attack in UAVs, namely false data-injection (FDI) attack [9], [10], where we consider a quadrotor system with only one vulnerable input and assume that this actuator is hijacked in the sense that the adversarial agent overrides the control input and injects a malicious signal into the actuator. Our goal is then to design a control signal for the remaining actuators to ensure a safe maneuver, i.e., follow a given curve with little or no deviation. Our method does not assume an *a priori* attack model; rather, the attack is detected (for various attack detection mechanisms in CPSs, see [11] and references therein) and the instantaneous resulting motor speed is measured. The main theme of this paper is thus to design a controller that not only mitigates the effect of the malicious signal, but also fulfills some mission objectives, especially in terms of safety.

We treat the path-following problem under false data injection (PFP-FDI) as a set stabilization problem [12], where the given path is represented as a set, and then we stabilize the maximal control invariant subset of the path [2] and render it as an invariant set in the presence of adversarial attack of FDI type. Our solution is based on *transverse feedback linearization (TFL)* [13]. The problem is challenging because the quadrotor system under adversarial attack is not differentially flat and subsequently has uncontrolled internal dynamics. Despite that, we show, by designing computationally efficient closed-form controllers, that the quadrotor system with one rotor fully controlled by an adversarial agent follows the desired path in a strict sense.

While the details of our controller design and theoretical results can be found in the paper, we summarize our main contributions below:

1) A well-defined vector relative degree of a quadrotor system in case of one rotor fully controlled by an adversarial agent (Lemma 1);

This research has been supported by NJIT's startup funds.

Hamza Mahmood* and Adeel Akhtar* are with the Department of Mechanical & Industrial Engineering at the New Jersey Institute of Technology, Newark, NJ 07102 (email: {hm576, adeel.akhtar}@njit.edu). Usman Ali† is with the Faculty of Computing, Engineering and Media at the De Montfort University, Leicester, LE1 9BH, UK (email: usman.ali@dmu.ac.uk)

2) A diffeomorphism that geometrically transforms the quadrotor system into a partial linear system (Lemma 2);
3) Asymptotic stability and invariance of a given path in the presence of adversarial attacks on a single motor (Theorem 1).

A. Notation

We represent a vector $x \in \mathbb{R}^n$ with components $x_1, x_2, \ldots, x_n$ by $x = \mathrm{col}(x_1, \ldots, x_n)$. For Euclidean space, we denote the inner product and norm by $\langle \cdot, \cdot \rangle$ and $\| \cdot \|$, respectively. We abbreviate the trigonometric functions as $c_\theta := \cos\theta$, $s_\theta := \sin\theta$, $t_\theta := \tan\theta$. The point-to-set distance of a point $p \in \mathbb{R}^n$ from a nonempty set $A \subseteq \mathbb{R}^n$ is given by $\|p\|_A := \inf_{q \in A} \|p - q\|$. If $h : A \to B$ and $s : B \to C$ are two maps, then their composition is denoted by $s \circ h : A \to C$. The derivative of a C^1 map $f : \mathbb{R}^n \to \mathbb{R}^m$ at a point $p \in \mathbb{R}^n$ is written as $df_p := \frac{\partial f}{\partial x}\Big|_{x=p}$. If $f, g : \mathbb{R}^n \to \mathbb{R}^n$ and $\lambda : \mathbb{R}^n \to \mathbb{R}$ are smooth maps, the Lie derivatives are denoted by $L_g^0 \lambda := \lambda$, $L_g^k \lambda := L_g(L_g^{k-1}\lambda)$, $L_g L_f \lambda := L_g(L_f \lambda)$.

II. Preliminaries

In this section, we define a class of parametric curves that can be represented as a zero-level set of a smooth function and review some elementary concepts related to curves; for details, see [14].

Definition 1 (Regular parameterized curve)**.** *A parametric curve $\sigma : I \subseteq \mathbb{R} \to \mathbb{R}^3$, for some open interval I, is called a regular curve if for each $\lambda \in I$, $\sigma'(\lambda) \neq 0$, where $\sigma'(\lambda) := d\sigma/d\lambda$.*

The following proposition shows that any regular curve has a unit-speed parameterization [14, Proposition 1.3.6].

Proposition 1 (Unit-speed parameterization of a regular curve)**.** *A parameterized curve has a unit-speed reparameterization if and only if it is regular.*

This means that every regular curve σ has a parameterization corresponding to which we have $\|\sigma'(\cdot)\| \equiv 1$. In the sections to follow, we shall always assume that a regular curve is unit-speed parameterized.

Definition 2 (L-periodic curves)**.** *Let $\sigma : \mathbb{R} \to \mathbb{R}^3$ be a parametric curve and let $L \in \mathbb{R}$. The curve σ is L-periodic if $\sigma(\lambda + L) = \sigma(\lambda)$ for all $\lambda \in \mathbb{R}$. If σ is not constant and is L-periodic for some $L \neq 0$, then σ is said to be closed.*

III. Mathematical Model of a Quadrotor

In this paper, we consider a standard quadrotor model given in [7]. Let us consider two right-handed orthonormal frames in $\mathbb{R}^3$, denoted by $\mathcal{I} = \left\{\vec{i}_1, \vec{i}_2, \vec{i}_3\right\}$ and $\mathcal{B} = \left\{\vec{b}_1, \vec{b}_2, \vec{b}_3\right\}$, called the inertial and body-fixed reference frames, respectively. The inertial frame $\mathcal{I}$ is fixed, i.e., it neither translates nor rotates. The body-fixed frame, as the name suggests, is attached to the center of gravity of the quadrotor body. The orientation of the quadrotor, also known as *attitude*, is the orientation of the frame $\mathcal{B}$ with respect to the inertial frame $\mathcal{I}$. The set of all possible orientations is given by $\mathsf{SO}(3) := \left\{R \in \mathbb{R}^{3\times 3} : R^\top R = I = RR^\top, \det(R) = +1\right\}$, which constitutes a Lie group, i.e., $\mathsf{SO}(3)$ is a smooth manifold and forms a group under matrix multiplication. The elements of $\mathsf{SO}(3)$ are called rotation matrices. One possible way to represent rotation matrices is by the three *ZYX Euler angles*, namely yaw ($\psi \in \mathbb{R}$), pitch ($\theta \in \mathbb{R}$), and roll ($\phi \in \mathbb{R}$). To obtain $\mathcal{B}$, we rotate $\mathcal{I}$ using the rotation matrix

$$R_b^i(\Phi) = \begin{bmatrix} c_\psi & -s_\psi & 0 \\ s_\psi & c_\psi & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} c_\theta & 0 & s_\theta \\ 0 & 1 & 0 \\ -s_\theta & 0 & c_\theta \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & c_\phi & -s_\phi \\ 0 & s_\phi & c_\phi \end{bmatrix}, \tag{1}$$

where the three Euler angles are denoted by $\Phi := (\phi, \theta, \psi)$. We define the domain of Euler angles with $\mathcal{E}_D := \{\Phi = (\phi, \theta, \psi) \in (-\pi, \pi) \times (-\pi, \pi) \times (-\pi, \pi) : \cos\theta > 0\}$. It is well-known that the map $R_b^i : \mathcal{E}_D \to R_b^i(\mathcal{E}_D)$ is a diffeomorphism. The inverse map $(R_b^i)^{-1}$ is a coordinate chart of the Lie group $\mathsf{SO}(3)$. While this representation is unique, it is not global, with singularities at angles $\theta = \pm\pi/2$. We define $Y(\Phi)$ and $Y^{-1}(\Phi)$ as

$$Y(\Phi) = \begin{bmatrix} 1 & 0 & -s_\theta \\ 0 & c_\phi & c_\theta s_\phi \\ 0 & -s_\phi & c_\theta c_\phi \end{bmatrix}, Y^{-1}(\Phi) = \begin{bmatrix} 1 & s_\phi t_\theta & c_\phi t_\theta \\ 0 & c_\phi & -s_\phi \\ 0 & s_\phi/c_\theta & c_\phi/c_\theta \end{bmatrix}. \tag{2}$$

Using the above relationship, the kinematic equation of a rotating rigid body can be described as $\dot{\Phi} = Y^{-1}(\Phi)\Omega$, where $\Omega(t) := (p(t), q(t), r(t)) \in \mathbb{R}^3$ are body rates of the rotating rigid body. Let $x_q(t) := (x_I(t), y_I(t), z_I(t)) \in \mathbb{R}^3$ denote the quadrotor's position, and $v_q(t) = (v_x(t), v_y(t), v_z(t)) \in \mathbb{R}^3$ be its velocity with respect to the inertial frame $\mathcal{I}$. Let $J := \mathrm{diag}(I_x, I_y, I_z) \in \mathbb{R}^{3\times 3}$ be the inertia matrix of the quadrotor expressed in body-fixed frame $\mathcal{B}$. Let m and g be the mass of the quadrotor and acceleration due to gravity, respectively. The input torque about the three body axes is denoted by $\tau(t) := \mathrm{col}(\tau_p(t), \tau_q(t), \tau_r(t)) \in \mathbb{R}^3$, which, together with the combined thrust $u_f(t)$, defines the four control inputs of the UAV system. The translational and rotational drag coefficients are denoted by k_t and k_r, respectively, and are assumed to be the same in all directions. The dynamics of the quadrotor can be locally represented[1] using Euler angles as

$$\begin{aligned} \dot{\Phi} &= Y^{-1}(\Phi)\Omega, \\ \dot{\Omega} &= J^{-1}\left(\tau - k_r\Omega - (\Omega \times J\Omega)\right), \\ \dot{x}_q &= v_q, \\ \dot{v}_q &= \frac{u_f}{m} R_b^i(\Phi)\vec{b}_3 - g\vec{i}_3 - \frac{k_t}{m} v_q. \end{aligned} \tag{3}$$

It can be seen that the input of the quadrotor model (3) is $\mathcal{U}_\tau(t) := (u_f(t), \tau(t)) \in \mathbb{R}^4$. However, the inputs of a physical quadrotor are forces generated by each propeller. Let the force generated by the i-th propeller be $f_i(t) \in \mathbb{R}$, and we denote all forces of the quadrotor by $\mathcal{U}_f(t) := (f_1(t), f_2(t), f_3(t), f_4(t)) \in \mathbb{R}^4$. We assume that these thrust

[1] note that the argument t is dropped for notational simplicity

forces are nonnegative, twice differentiable, and bounded above by some $M < \infty$. The force inputs $\mathcal{U}_f$ are related to $\mathcal{U}_\tau$ by an invertible linear map, whose matrix representation is given by

$$\begin{bmatrix} u_f \\ \tau_p \\ \tau_q \\ \tau_r \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & -l & 0 & l \\ -l & 0 & l & 0 \\ d & -d & d & -d \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \end{bmatrix}, \tag{4}$$

where l is the distance of each rotor from the quadrotor's center of gravity and d is the ratio between the drag and the thrust coefficients of the blade.

Let $x(t) = \mathrm{col}(\Phi(t), \Omega(t), x_q(t), v_q(t)) \in \mathbb{R}^{12}$ be the state of the quadrotor. We take the output $y \in \mathbb{R}^3$ of the system (3) to be the position x_q of the quadrotor

$$y = h(x) = x_q. \tag{5}$$

Next, we consider a quadrotor model under an adversarial attack.

A. Quadrotor under Adversarial Attack

We assume that only one rotor is vulnerable and without loss of generality, let us assume that f_2 is the vulnerable input. Meanwhile, the other three control inputs f_1, f_3, f_4 are secure and cannot be attacked. We also assume that the adversarial agent completely controls the second motor and can inject a malicious FDI signal, i.e., the thrust force generated by the second motor is now fully under the control of the adversarial agent.

Definition 3 (Adversarial Signal)**.** *An adversarial signal is a smooth bounded map $\mathcal{A} : \mathbb{R}_{\geq 0} \times \mathbb{R}^3 \to [0, M_a] \subset \mathbb{R}$, $(t, x_q) \mapsto \mathcal{A}(t, x_q)$ for some $M_a < \infty$.*

We assume that there exists an attack detection mechanism that detects the instantaneous value of the adversarial signal $\mathcal{A}(t, x_q)$; its value for each instant $t \geq 0$ is known to us. Since actuator two is under attack, it follows from Definition 3 that $f_2 = \mathcal{A}(t, x_q)$. By substituting $f_2 = \mathcal{A}(t, x_q)$ in (4), we obtain

$$\tau_p = \left(u_f - \frac{\tau_r}{d}\right)\left(\frac{l}{2}\right) - 2l\mathcal{A}(t, x_q). \tag{6}$$

Under this adversarial attack on the second motor, the thrust forces f_1, f_3, f_4, can alternatively be represented by (u_f, τ_q, τ_r) using (4). Before formally stating the problem, we make the following mild assumption:

Assumption 1. *For all time $t \geq 0$, the combined thrust force $u_f \neq 0$ and $\phi, \theta \neq \pm\pi/2$, i.e., the system does not go into gimbal lock situation.*

Note that this assumption is reasonable: in order for the quadrotor to be in the air, it needs to have a nonzero combined thrust force. Also, we highlight that the singularity associated with gimbal lock is an artifact of the local parameterization, i.e., Euler angles, on $\mathsf{SO}(3)$.

IV. Problem Formulation

We consider a regular, smooth curve γ in $\mathbb{R}^3$ as the desired path for our quadrotor to follow. Let $\sigma : \mathbb{R} \to \mathbb{R}^3$ be the unit-speed parameterization of γ. The curve γ can be either closed (see Definition 2), e.g., a circle, or not closed, e.g., a straight line. It can be shown that there exists a smooth map $s : \mathbb{R}^3 \to \mathbb{R}^2$, $s := (s_1, s_2)$, such that $\gamma = s^{-1}(0)$ with $\mathrm{rank}(ds_y) = 2$ for each point y on γ. Since $\gamma = s^{-1}(0)$, the path in the output space (5) can be represented by its zero-level set representation as

$$\gamma := s^{-1}(0) = \left\{y \in \mathbb{R}^3 : s_1(y) = s_2(y) = 0\right\} \subset \mathbb{R}^3. \tag{7}$$

We lift the path γ to the quadrotor's state space:

$$\Gamma := \left\{x \in \mathbb{R}^{12} : s_1(h(x)) = s_2(h(x)) = 0\right\}.$$

We can now state the path-following control problem in the presence of adversarial agent:

Problem 1. *Consider a quadrotor model (3) satisfying Assumption 1, an adversarial agent $\mathcal{A}$ given in Definition 3, a desired path γ defined in (7), and a set of initial conditions in the neighborhood of Γ. Design a controller $\kappa : \mathbb{R}^{12} \times \mathbb{R}^k \to \mathbb{R}^3$ (where $k \in \mathbb{Z}^+$ is the dimension of the augmented state) such that the output of the system converges to the set γ, i.e., $\|y(t)\|_\gamma \to 0$, as $t \to \infty$, such that Γ or some subset of Γ becomes asymptotically stable and forward invariant.*

It should be noted that the output $y \in \mathbb{R}^3$ approaches the curve γ if and only if the state x of the system approaches Γ [12]. However, in general, the set Γ cannot be made forward invariant, so we aim to stabilize a subset of Γ and denote it by $\Gamma^\star$ (see [6], [7]). We observe that the path invariance of a set is a necessary condition for its stability. This means that asymptotic stability of a set implies its forward invariance. Next, we present our path-following controller.

V. Path-Following Controller Design

In general, we cannot stabilize the set Γ, as highlighted previously, and we seek to stabilize the largest controlled invariant subset $\Gamma^\star$ contained in Γ. We call $\Gamma^\star$ the path following manifold (see [2], [7], [15]). For any trajectory of the system that is in the path-following manifold, there exists a suitable choice of control input such that the output associated with the trajectory can be made to remain on the desired path. By rendering $\Gamma^\star$ attractive and invariant, Problem 1 can be solved. To obtain $\Gamma^\star$, by using the map $s : \mathbb{R}^3 \to \mathbb{R}^2$, we define the following:

$$\alpha = \begin{bmatrix} \alpha_1(x) \\ \alpha_2(x) \end{bmatrix} := s \circ h(x) = \begin{bmatrix} s_1 \circ h(x) \\ s_2 \circ h(x) \end{bmatrix}. \tag{8}$$

We see that α in (8) has only two component functions. Since we have only three control inputs for our attacked quadrotor, we augment α with one additional function to have the number of component functions of the output equal to the number of control inputs. We then check if the augmented output has a well-defined vector relative degree. For this, let $\pi : \mathbb{R}^3 \to \mathbb{R}$

be any smooth real-valued function. It can be easily shown (see [7]) that the virtual output $\hat{y} = (\alpha, \pi \circ h)$ does not have a well-defined relative degree because the decoupling matrix is not full rank.

As in [6], we can solve this problem by delaying the appearance of the control input u_f using two integrators which are included through two additional states: $x_{13} := u_f, x_{14} := \dot{u}_f$. Define $u_d := \ddot{u}_f$ and $u := \text{col}(u_d, u_r, u_q) \in \mathbb{R}^3$, where $u_r := \tau_r$ and $u_q := \tau_q$. We write the extended model, with a slight abuse of notation, as

$$\dot{x} = f(x) + g_1(x)u_d + g_2(x)u_r + g_3(x)u_q, \tag{9}$$

where $x = \text{col}(\Phi, \Omega, x_q, v_q, x_{13}, x_{14}) \in \mathbb{R}^{14}$, and $f(x)$ is as follows:

$$f(x) = \begin{bmatrix} Y^{-1}(\Phi)\Omega \\ -\frac{k_r p - l x_{13}/2 + 2\mathcal{A}(t,x_q) l - I_y q r + I_z q r}{I_x} \\ -\frac{k_r q + I_x p r - I_z p r}{I_y} \\ -\frac{k_r r - I_x p q + I_y p q}{I_z} \\ v_q \\ \frac{x_{13}}{m} R_b^i(\Phi)\vec{b}_3 - g\vec{i}_3 - \frac{k_t}{m} v_q \\ x_{14} \\ 0 \end{bmatrix}. \tag{10}$$

The vectors $g_1(x)$, $g_2(x)$, and $g_3(x)$ are as follows:

$$\begin{aligned} g_1(x) &= \text{col}(0,0,0,0,0,0,0,0,0,0,0,0,0,1), \\ g_2(x) &= \text{col}(0,0,0,-l/(2I_x d),0,1/I_z,0,0,0,0,0,0,0,0), \\ g_3(x) &= \text{col}(0,0,0,0,1/I_y,0,0,0,0,0,0,0,0,0). \end{aligned} \tag{11}$$

To obtain the largest control invariant subset of Γ, we apply the zero dynamics algorithm [16] and obtain

$$\Gamma^\star = \left\{ x \in \mathbb{R}^{14} : L_f^i \alpha(x) = 0,\ i = 0,1,2,3,4 \right\} \subset \Gamma. \tag{12}$$

Having a well-defined vector relative degree is key to our controller design. To achieve a well-defined vector relative degree, we choose a function similar to the one used in [6], [7]. Let $U_\gamma \subset \mathbb{R}^3$ be a tubular neighbourhood of the path γ and define the function

$$\begin{aligned} \varpi : U_\gamma &\to \mathbb{R} \\ y &\mapsto \arg\inf_{\lambda \in \mathbb{R}} \|y - \sigma(\lambda)\|. \end{aligned} \tag{13}$$

The function defined above is smooth as long as U_γ is a sufficiently small "tube" around the curve γ. With this definition, the virtual output function $\hat{y}$ becomes

$$\hat{y} = \begin{bmatrix} \alpha_1(x_q) \\ \alpha_2(x_q) \\ \pi(x_q) \end{bmatrix} = \begin{bmatrix} s_1 \circ h(x) \\ s_2 \circ h(x) \\ \varpi \circ h(x) \end{bmatrix}. \tag{14}$$

We now prove that at each point of $\Gamma^\star$, the extended quadrotor system (9) under the bounded adversarial attack $\mathcal{A}$ has a well-defined vector relative degree.

Lemma 1. *Given the extended system in (9) with a virtual output map defined in (14), and an adversarial attack signal $\mathcal{A}$ defined in Definition 3, the system has a well-defined vector relative degree of $\{4,4,4\}$ for all $x \in \Gamma^\star \cap \{x \in \mathbb{R}^{14} : x_{13} \neq 0\}$ under Assumption 1.*

Proof: Consider any arbitrary $x^\star \in \Gamma^\star \cap \{x \in \mathbb{R}^{14} : x_{13} \neq 0\}$. Since $\Gamma^\star \subseteq \Gamma$, $x^\star \in \Gamma$ and so, the output $h(x^\star)$ lies on the path γ. This implies that there exists a $\lambda^\star \in \mathbb{R}$ such that $h(x^\star) = \sigma(\lambda^\star)$. By the definition of vector relative degree, we first show that $L_{g_i} L_f^j \pi(x) = L_{g_i} L_f^j \alpha_k(x) \equiv 0$ for $i \in \{1,2,3\}$, $j \in \{0,1,2\}$, $k \in \{1,2\}$ in a neighbourhood of $x^\star$. It is easy to see that this holds by simply computing these Lie derivatives. Then, we need to show that the 3×3 decoupling matrix

$$D(x^\star) = \begin{bmatrix} L_{g_1} L_f^3 \alpha_1(x^\star) & L_{g_2} L_f^3 \alpha_1(x^\star) & L_{g_3} L_f^3 \alpha_1(x^\star) \\ L_{g_1} L_f^3 \alpha_2(x^\star) & L_{g_2} L_f^3 \alpha_2(x^\star) & L_{g_3} L_f^3 \alpha_2(x^\star) \\ L_{g_1} L_f^3 \pi(x^\star) & L_{g_2} L_f^3 \pi(x^\star) & L_{g_3} L_f^3 \pi(x^\star) \end{bmatrix}, \tag{15}$$

is invertible. Interestingly, the adversarial attack signal $\mathcal{A}$ does not appear in any entry of the decoupling matrix $D(x^\star)$ and so, the determinant of $D(x^\star)$ is as follows:

$$\det\left(D(x)\right) = \frac{l(x_{13})^2}{I_x I_y m^3 d} \left\langle -d_\chi \alpha_1, (d_\chi \alpha_2 \times \sigma') \right\rangle, \tag{16}$$

where $d_\chi \alpha_i := \text{col}(\frac{\partial \alpha_i}{\partial x_I}, \frac{\partial \alpha_i}{\partial y_I}, \frac{\partial \alpha_i}{\partial z_I})$ for $i \in \{1,2\}$ and $\sigma' := \text{col}(\frac{d\sigma_x}{d\lambda}, \frac{d\sigma_y}{d\lambda}, \frac{d\sigma_z}{d\lambda})$. The determinant is zero if and only if any term in the numerator of (16) is zero. Since $x^\star \in \Gamma^\star \cap \{x \in \mathbb{R}^{14} : x_{13} \neq 0\}$, the combined thrust $x_{13} \neq 0$ under Assumption 1. Also, $\text{span}\{d_\chi \alpha_1, d_\chi \alpha_2, \sigma'\}(x^\star) = \mathbb{R}^3$ (see [6, Lemma V.2]) and so, $\langle -d_\chi \alpha_1, (d_\chi \alpha_2 \times \sigma') \rangle \neq 0$ at $x^\star$ (see [6, Lemma V.1]). Hence, we have shown that for each $x^\star \in \Gamma^\star \cap \{x \in \mathbb{R}^{14} : x_{13} \neq 0\}$, $\det\left(D(x^\star)\right) \neq 0$, and therefore, the extended system has a well-defined vector relative degree at $x^\star$. ∎

The well-defined vector relative degree of $\{4,4,4\}$ for the extended system means that the internal dynamics has dimension $14 - (4+4+4) = 2$. So, we require two additional functions to define a complete coordinate transformation.

Lemma 2. *(Diffeomorphism) Suppose Assumption 1 holds, then for each $x^\star \in \Gamma^\star$, there exists a neighbourhood $U_x \subset \mathbb{R}^{14}$ of $x^\star$ such that the map $\mathscr{T} : U_x \to \mathscr{T}(U_x) \subset \mathbb{R}^{14}$, defined by*

$$\begin{bmatrix} \xi_{ji} \\ \eta_i \\ \mu_k \end{bmatrix} = \mathscr{T}(x) = \begin{bmatrix} L_f^{i-1} \alpha_j(x) \\ L_f^{i-1} \pi(x) \\ \mu(x) \end{bmatrix}, \tag{17}$$

for $i \in \{1,2,3,4\}$, $j \in \{1,2\}$ and $k \in \{1,2\}$, is a diffeomorphism.

Proof: Since the dimension of the internal dynamics is 2, we choose two real-valued functions μ_1, μ_2 to complete the definition of $\mathscr{T}$ similar to [6]:

$$\mu_1 := \psi, \quad \mu_2 := -\frac{p}{I_z} - \frac{lr}{2I_x d}. \tag{18}$$

Next, we check the rank of the Jacobian matrix $\frac{\partial \mathscr{T}}{\partial x}$ to see whether it defines a local diffeomorphism. The determinant of $\frac{\partial \mathscr{T}}{\partial x}$ is given by

$$\frac{-l(x_{13})^4 c_\phi}{2I_x m^6 d} \langle -d_\chi \alpha_1, (d_\chi \alpha_2 \times \sigma') \rangle. \tag{19}$$

Now, this determinant equals zero if and only if any term in the numerator equals zero. However, by our hypothesis and Assumption 1, $x_{13} \neq 0$ and $\phi \neq \pm\frac{\pi}{2}$. Moreover, as in the proof of Lemma 1, we have $\langle -d_\chi \alpha_1, (d_\chi \alpha_2 \times \sigma') \rangle \neq 0$ at $x^\star$. Thus, the Jacobian of $\mathscr{T}$ is invertible in a neighbourhood of $x^\star$. By [16, Proposition 1.2.3], $\mathscr{T}$ defines a local diffeomorphism. ■

The equivalent transformed system after applying $\mathscr{T}$ to the extended system (9) becomes

$$\begin{aligned}
\dot{\xi}_{ij} &= \xi_{ij+1} \\
\dot{\eta}_j &= \eta_{j+1} \\
\dot{\xi}_{14} &= L_f^4\alpha_1 + L_{g_1}L_f^3\alpha_1 u_d + L_{g_2}L_f^3\alpha_1 u_r + L_{g_3}L_f^3\alpha_1 u_q\Big|_{x=T^{-1}(\xi,\eta,\mu)} \\
\dot{\xi}_{24} &= L_f^4\alpha_2 + L_{g_1}L_f^3\alpha_2 u_d + L_{g_2}L_f^3\alpha_2 u_r + L_{g_3}L_f^3\alpha_2 u_q\Big|_{x=T^{-1}(\xi,\eta,\mu)} \\
\dot{\eta}_4 &= L_f^4\pi + L_{g_1}L_f^3\pi u_d + L_{g_2}L_f^3\pi u_r + L_{g_3}L_f^3\pi u_q\Big|_{x=T^{-1}(\xi,\eta,\mu)} \\
\dot{\mu}_k &= b_k(\xi,\eta,\mu)|_{x=T^{-1}(\xi,\eta,\mu)}
\end{aligned} \tag{20}$$

for $i \in \{1,2\}$, $j \in \{1,2,3\}$, $k \in \{1,2\}$ and where b_k are smooth maps. From (20), one can define a regular feedback of the form

$$\begin{bmatrix} u_d \\ u_r \\ u_q \end{bmatrix} := D^{-1}(x)\left(\begin{bmatrix} -L_f^4\alpha_1 \\ -L_f^4\alpha_2 \\ -L_f^4\pi \end{bmatrix} + \begin{bmatrix} v^{\xi_1} \\ v^{\xi_2} \\ v^{\eta} \end{bmatrix}\right), \tag{21}$$

where $(v^{\xi_1}, v^{\xi_2}, v^{\eta})$ are auxiliary control inputs. Using Lemma 1 and the regular feedback law (21), the extended quadrotor model (9) transformed to 3 decoupled chain of integrators and two-dimensional internal dynamics is given as follows:

$$\begin{array}{llll}
\dot{\xi}_{11} = \xi_{12} & \dot{\xi}_{21} = \xi_{22} & \dot{\eta}_1 = \eta_2 & \dot{\mu} = b(\xi,\eta,\mu). \\
\dot{\xi}_{12} = \xi_{13} & \dot{\xi}_{22} = \xi_{23} & \dot{\eta}_2 = \eta_3 & \\
\dot{\xi}_{13} = \xi_{14} & \dot{\xi}_{23} = \xi_{24} & \dot{\eta}_3 = \eta_4 & \\
\dot{\xi}_{14} = v^{\xi_1} & \dot{\xi}_{24} = v^{\xi_2} & \dot{\eta}_4 = v^{\eta} &
\end{array} \tag{22}$$

Since (22) is a partial linear system, designing a controller for the linear subsystems is straightforward. For the ξ-subsystem, we design the following linear controller:

$$v^{\xi_1} = -\sum_{i=1}^{4} k_{1i}^{\xi}\xi_{1i}, \quad v^{\xi_2} = -\sum_{i=1}^{4} k_{2i}^{\xi}\xi_{2i}, \tag{23}$$

for some strictly positive gains k_{1i}^{ξ} and k_{2i}^{ξ}, $i \in \{1,\cdots,4\}$, which renders the resulting closed-loop linear system Hurwitz. We underscore that by stabilizing the origin of the ξ-subsystem, the system state converges to the set $\Gamma^\star$. Similarly, a linear control law is designed for the $\eta-$subsystem

$$v^{\eta} = -k_2^{\eta}(\eta_2 - \dot{\eta}_1^{ref}) - k_3^{\eta}(\eta_3 - \ddot{\eta}_1^{ref}) - k_4^{\eta}(\eta_4 - \dddot{\eta}_1^{ref}) \tag{24}$$

for some appropriate gains k_i^{η} for $i \in \{2,3,4\}$ to ensure stability.

Next, we show that the internal state $\mu \in \mathbb{R}^2$ remains bounded under bounded adversarial attacks.

A. Internal Dynamics

The internal dynamics of the uncontrolled μ-subsystem is as follows:

$$\begin{aligned}
\dot{\mu}_1(\xi,\eta,\mu) &= \dot{\psi} = \frac{1}{c_\theta}\left(qs_\phi + rc_\phi\right)\Big|_{x=T^{-1}(\xi,\eta,\mu)}, \\
\dot{\mu}_2(\xi,\eta,\mu) &= -\frac{lx_{13}}{2I_xI_z} + \frac{lk_r r + pql(I_y - I_x)}{2I_xI_z d} + \\
&\qquad \frac{k_r p + 2\mathcal{A}(t,x_q)l + qr(I_z - I_y)}{I_xI_z}\Big|_{x=T^{-1}(\xi,\eta,\mu)}.
\end{aligned} \tag{25}$$

We now prove the boundedness of internal dynamics:

Lemma 3. *If the quadrotor system has bounded control inputs $(u_f, u_r, u_q) \in \mathbb{R}^3$ and Assumption 1 holds, then the derivatives of the internal states, i.e., $\dot{\mu}_1$ and $\dot{\mu}_2$ given in (25) are bounded. Also, μ_2 is bounded.*

Proof: It can be shown that bounded control inputs imply bounded body rates p, q, r. By Assumption 1, the system is bounded away from singularities $(\phi, \theta = \pm\pi/2)$. From (25), we get

$$\begin{aligned}
|\dot{\mu}_1| &\leq \left|\frac{1}{c_\theta}\right|(|q| + |r|), \\
|\dot{\mu}_2| &\leq \frac{l|x_{13}|}{2I_xI_z} + \frac{lk_r|r| + |pql(I_y - I_x)|}{2I_xI_z d} + \\
&\qquad \frac{k_r|p| + 2|\mathcal{A}(t,x_q)|l + |qr(I_z - I_y)|}{I_xI_z}, \\
|\mu_2| &\leq \frac{|p|}{I_z} + \frac{l|r|}{2I_x d},
\end{aligned} \tag{26}$$

which are bounded because the body rates p, q, r, the thrust forces f_1, f_3, f_4, and the adversarial signal $\mathcal{A}$ are all bounded. ■

We are now ready to prove the main result.

Theorem 1. *(Main Result) Given the extended system (9), the virtual output function (14), an adversarial attack signal $\mathcal{A}$ defined in Definition 3, the regular feedback given in (21) along with the controllers in (23), the path following manifold $\Gamma^\star$ given in (12) is asymptotically stable and forward-invariant.*

Proof: The feedback transformation (21) is well-defined in a neighbourhood of the path-following manifold $\Gamma^\star$. By Lemma 2, the function $\mathscr{T}$ is a diffeomorphism of a neighbourhood of $\Gamma^\star$ onto its image. In (ξ,η,μ) coordinates, the set $\Gamma^\star$ becomes $\mathscr{T}(\Gamma^\star) = \{(\xi,\eta,\mu) : \xi = 0\}$. The ξ-subsystem in (22), after the feedback transformation, is linear time-invariant, and the feedback (23) makes the set $\Gamma^\star$ exponentially stable. Thus, for any $x(0)$ close to $\Gamma^\star$, or equivalently, for any $\xi(0)$ close to 0, $\xi(t) \to 0$ exponentially. Therefore, $\mathscr{T}(\Gamma^\star)$ is exponentially stable, and since $\mathscr{T}$ is a local diffeomorphism, this implies that $\Gamma^\star$ is exponentially stable as well and hence, is asymptotically stable and also forward-invariant. ■

It is immediate to see that stability of $\Gamma^\star$ implies that the output of the system converges to the set γ, i.e., $\|y(t)\|_\gamma \to 0$, as $t \to \infty$, and by construction, γ becomes a forward invariant set. Hence, Problem 1 is solved in the presence of bounded

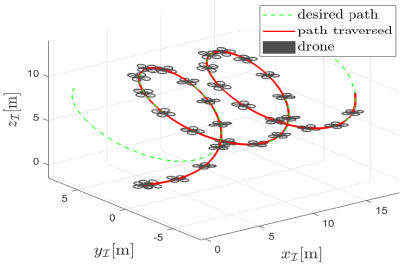
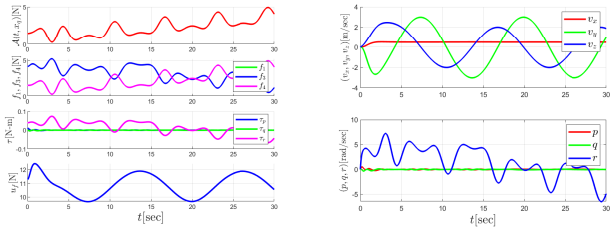


Fig. 1. Quadrotor following the path



(a) Adversarial agent, input forces, torques, and thrust forces

(b) Quadrotor's velocities

Fig. 2. System's input and velocities

adversarial attacks. Moreover, the controller (24) makes the quadrotor follow a desired speed profile along the path, even in the presence of adversarial attacks.

VI. Numerical Simulation

We assume, without loss of generality, that rotor two is under a bounded attack and the quadrotor has a weight-to-thrust ratio of $1:4$, i.e., each propeller is capable of producing at least 8N of force [17]. It is assumed that the rotors cannot produce negative thrust, hence the actuator limits are between zero and eight, i.e., $f_i(t) \in [0, 8]$ for $i \in \{1, 3, 4\}$. The mass of the quadrotor is 1.1 kg and the inertias of the quadrotor are $I_x = 0.0020066$ kg.m^2, $I_y = 0.0020038$ kg.m^2, $I_z = 0.0013323$ kg.m^2. The length of each arm of the quadrotor is $l = 0.2656$ m.

The desired path is a non-closed curve given by $\gamma = \{y \in \mathbb{R}^3 : y_2 - \cos y_1 = 0, y_3 + 4\cos y_1 - 8 = 0\}$, and the adversarial signal is dependent on both time and system state $x_q = (x_I, y_I, z_I)$, namely $\mathcal{A}(t, x_q) = 0.1t + \sin z_I$. We highlight that the system only knows the instantaneous value of $\mathcal{A}(t, x_q)$ using a speed sensor attached to each motor of the quadrotor and not the whole attack model. Using a known motor constant k_m and the measured motor speed ω_m, one can measure the force exerted at the i-th motor by $f_i = k_m\omega_m$. Moreover, we assume 10% of parametric uncertainty in the quadrotor's inertia and 2% of uncertainty in mass. A small uncertainty in mass is considered because the mass of the quadrotor can be accurately measured within grams. On the other hand, the system's inertia is difficult to measure accurately. Figure 1 shows that the quadrotor is following the curve starting from an initial position of $x_q = (1.5, 0.3.0.5)$m despite parametric uncertainties. The bounded adversarial signal $\mathcal{A}(t, x_q)$ is plotted against time in the top plot of Figure 2a. It can also be seen in the remaining plots of Figure 2a that all the inputs remain bounded and well within the actuators' limit of 8N. To watch the animation of this maneuver, click here.[2] Finally, Figure 2b shows the linear and angular velocities of the quadrotor, and it can be seen that since the adversarial agent is bounded, the body rates are also bounded. In summary, the effectiveness of the proposed controller is shown through successful simulation. In the case of one rotor completely controlled by an adversarial agent, we have shown that even in the case of parametric uncertainties, the system can follow the given path accurately.

[2]https://youtu.be/orp1g-pIFrM

References

[1] S. M. LaValle, *Planning Algorithms*. Cambridge, U.K.: Cambridge University Press, 2006, available at http://planning.cs.uiuc.edu/.

[2] C. Nielsen, C. Fulford, and M. Maggiore, "Path following using transverse feedback linearization: Application to a maglev positioning system," *Automatica*, vol. 46, pp. 585–590, March 2010.

[3] A. Akhtar, C. Nielsen, and S. L. Waslander, "Path following using dynamic transverse feedback linearization for car-like robots," *IEEE Transactions on Robotics*, vol. 31, no. 2, pp. 269–279, 2015.

[4] B. Li, H. Liu, C. K. Ahn, and W. Gong, "Optimized intelligent tracking control for a quadrotor unmanned aerial vehicle with actuator failures," *Aerospace Science and Technology*, vol. 144, p. 108803, 2024.

[5] A. Aguiar, J. Hespanha, and P. Kokotović, "Path-following for nonminimum phase systems removes performance limitations," *IEEE Transactions on Automatic Control*, vol. 50, no. 2, pp. 234–239, 2005.

[6] A. Akhtar, S. L. Waslander, and C. Nielsen, "Fault tolerant path following for a quadrotor," in *52nd IEEE Conference on Decision and Control*, 2013, pp. 847–852.

[7] ——, "Path following for a quadrotor using dynamic extension and transverse feedback linearization," in *51st IEEE Conference on Decision and Control (CDC)*, Dec. 2012, pp. 3551 –3556.

[8] K. Garg, R. G. Sanfelice, and A. A. Cardenas, "Control barrier function-based attack-recovery with provable guarantees," in *2022 IEEE 61st Conference on Decision and Control (CDC)*, 2022, pp. 4808–4813.

[9] L. Xu, H. Zhu, K. Guo, Y. Gao, and C. Wu, "Output-based secure control under false data injection attacks," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 2, pp. 43–50, 2024.

[10] S. Gao, H. Zhang, C. Huang, Z. Wang, and H. Yan, "Optimal injection attack strategy for nonlinear cyber-physical systems based on iterative learning," *IEEE Transactions on Automation Science and Engineering*, vol. 21, no. 1, pp. 56–68, 2024.

[11] Z. Gong, F. Yang, and D. Wu, "Zero-sum game based secure tracking control of uav against fdi attacks using fixed-time convergent reinforcement learning," in *2023 62nd IEEE Conference on Decision and Control (CDC)*, 2023, pp. 1841–1846.

[12] C. Nielsen and M. Maggiore, "Maneuver regulation via transverse feedback linearization: Theory and examples," *Symposium on Nonlinear Control Systems (NOLCOS)*, September 2004.

[13] R. S. D'Souza and C. Nielsen, "An algorithm for local transverse feedback linearization," *SIAM Journal on Control and Optimization*, vol. 61, no. 3, pp. 1248–1272, 2023.

[14] A. N. Pressley, *Elementary differential geometry*. Springer Science & Business Media, 2010.

[15] L. Consolini, M. Maggiore, C. Nielsen, and M. Tosques, "Path following for the pvtol aircraft," *Automatica*, vol. 46, pp. 1284–1296, August 2010.

[16] A. Isidori, *Nonlinear Control Systems*. Secaucus, NJ, U.S.A: Springer-Verlag New York, Inc., 1995.

[17] L. Bauersfeld, E. Kaufmann, P. Foehn, S. Sun, and D. Scaramuzza, "Neurobem: Hybrid aerodynamic quadrotor model," *Robotic Science and System (RSS), July 12–16*, 2021.