Resilient Path Planning of UAV Formation Flight Against Covert Attacks on Ultra-Wideband Sensors

Xin Gong, *Member, IEEE*, Liqiang Gong, Tingwen Huang, *Fellow, IEEE*, and Yukang Cui, *Member, IEEE*

***Abstract*—This article proposes a resilient path planning scheme for the formation flight of the Unmanned Aerial Vehicle (UAV) swarm against covert attacks. The proposed method optimizes the time and energy consumption while navigating the UAV swarm to achieve the planned formation configuration despite the covert attacks. In particular, each UAV is moving in a three-dimensional space and equipped with a GPS sensor and an Ultra-Wideband (UWB) sensor. The covert attacker can enlarge the formation error of the UAV swarm by simultaneously spoofing the readings of the GPS sensor and corrupting control inputs without being detected by the onboard UWB sensor. To analyze and defend the attacks, we first present the essential prerequisite for the existence of covert attacks. Based on the prerequisite, an optimal covert attack scheme can be derived to maximize the terminal formation error. Correspondingly, a time-critical defense strategy is put forward to depress the above covert attacker. This defense strategy can generate a dynamically feasible polynomial trajectory for each UAV with both security and time efficiency. The effectiveness and practicality of obtained theoretical results are illustrated via two simulation examples.**

***Index Terms*—Covert attack, path planning, resilient formation, time-critical approach, UWB sensors.**

Manuscript received 9 April 2023; revised 12 June 2023; accepted 12 July 2023. Date of publication 21 July 2023; date of current version 3 August 2023. This work was supported in part by the National Natural Science Foundation of China under Grant 61903258, in part by Guangdong Basic and Applied Basic Research Foundation under Grant 2022A1515010234, in part by the Project of Department of Education of Guangdong Province under Grant 2022KTSCX105, and in part by the Start-up Research Fund of Southeast University under Grant RF1028623260. *(Xin Gong and Liqiang Gong are co-first authors.) (Corresponding author: Yukang Cui.)*

Xin Gong is with the School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China (e-mail: xingong@seu.edu.cn).

Liqiang Gong is with the Research Institute, Nanjing 6902 Technology Company, Ltd., Nanjing 210009, China, and also with the College of Mechatronics and Control Engineering, Shenzhen University, Shenzhen 518060, China (e-mail: SZUgonglq@gmail.com).

Tingwen Huang is with the Texas A&M University at Qatar, Doha 23874, Qatar (e-mail: tingwen.huang@qatar.tamu.edu).

Yukang Cui is with the Peng Cheng Laboratory, Shenzhen 518000, China, and also with the College of Mechatronics and Control Engineering, Shenzhen University, Shenzhen 518060, China (e-mail: cuiyukang@gmail.com).

Digital Object Identifier 10.1109/TICPS.2023.3297970

I. Introduction

In RECENT years, coordinated formation flight of unmanned aerial vehicles (UAVs) has gained intensive attention in academia and industry due to its extensive applications in urgent search and rescue tasks [1], military operations [2], wide-area surveillance and monitoring [3], and smart remote sensors [4]. The research on formation control and trajectory planning has been carried out mainly from two aspects: control and optimization. For formation control, a representative paper on formation consistency of UAV [5] was proposed. The authors in [6], [7], [8], [9] studied the leaderless and leader-following consensus problems. Due to the advantages of fewer control nodes and low resource consumption, it is widely used in formation control [10], [11], [12], [13]. The recent works in [14] and [15] optimized formation control from the level of communication topology optimization. Trajectory planning of UAV formation is another exploration direction of formation flight, a representative work [16], called Minimum Snap Algorithm, which can save energy within a fixed time. In [17], a kind of trajectory planning algorithm with universality and time optimization is proposed. This algorithm is used to realize multi-aircraft formation flight in complex environments. These algorithms use optimization methods to reduce the dimensions of problem solving and achieve superior performance in real-world scenarios [18], [19], [20].

However, the above algorithms need to be more safe. The safety concept in the realm of Robotics is quite diverse. To our best knowledge, two basic means of UAV safety are the robustness against unintentional and stochastic uncertainties (including disturbances) and the resilience against malicious and strategic attackers, respectively. Although a large amount of existing research (see [21] and references therein) was devoted to enhancing the robustness of the path planning algorithm, much fewer works [22], [23], [24], [25] have considered the resilience of path planning algorithms against malicious attacks, let alone covert ones [24], [25]. A novel game-theoretic framework for raising the security level of drone delivery systems was addressed in [22], where the malicious attacker tried to maximize the delivery time. In [23], the GPS spoofing attacks were depressed via cooperative localization, where each UAV can figure out its safe location via communicating with neighbours instead of believing the possibly compromised GPS channels.

Different from [22], [23], a special kind of attacks, denoted as covert (undetectable) attacks [24], [25], may also exist under some special conditions, which could deviate the nominal path of 2D robots without being detected by some well-functioning sensors. Inspired by [24], [25], here we focus on a swarm of UAVs equipped with the Ultra-Wideband (UWB) sensors [26], a special kind of 3D distance measurement units (3DMUs), which could only measure the distance among the UAVs.

The covert attacks on 3DMUs, consisting of the man-in-the-middle (MITM) attacks [27] on the GPS signal and the actuation attacks [28] on the UAV motors, are considered in this work. The danger induced by MITM attacks on GPS systems (GPS spoofing attacks) has gained substantial attention for the wide applications of GPS positioning. It was reported in [27] that a UAV capturing operation had been achieved via GPS spoofing attacks. However, the hoax of GPS spoofing attacks can be easily revealed by other onboard sensors measuring the positions or velocity w.r.t. its neighbouring UAVs, as shown in [23]. Here, we consider a special scenario in which the UAV in the swarm is equipped with 3DMUs, such as UWB sensors. It is found that a covert attacker may still achieve her aim in such a scenario. Apart from the above GPS spoofing attacks, the actuation attacks on the UAV motors are also considered. The nominal control inputs of the compromised UAV are replaced by well-designed false control inputs, such that the well-functioning UWB sensor on the attacked UAV can distinguish little difference between the readings during the nominal flight journey and the attacked one.

Unlike most of the existing works [22], [23], [27], [28], [29], [30], [31], [32] against non-covert attacks, we focus on the path planning of UAV swarms against covert attacks, which cannot be detected by some well-functioning 3DMUs. This implies that convert attacks are more strategic and flexible than non-covert ones, which are generally familiar with security vulnerabilities. This covert attack strategy is well-designed and thus cannot be easily tackled via the traditional attack detection and mitigation methods. Herein, we formulate an integrated strategy pair for both the covert attacker and the UAV swarm (defender) with time-critical targets [17], [33], [34]. The main contributions of our work are summarized as follows:

1) The definition and characteristics of covert attacks on 3DMUs are given. The prerequisite for the covert attack occurrence in the UAV swarm is further investigated.
2) An optimal attack strategy for the covert attacker is formulated such that the attacker can deform the formation configuration of the UAV swarm while keeping it undetected by well-functioning UWB sensors measuring relative distances. This kind of covert attack strategy can pose a threat to the UAV path planning in both single neighbour scenarios (SNS) and double neighbours scenarios (DNS), respectively.
3) An elaborate path planning strategy, based on time-critical idea [34], is proposed, anticipating the threat of covert attacks. More specifically, this strategy is feasible for both SNS and DNS.

Notations: In the this article, $\otimes$ represents the Kronecker product. The symbols $\mathbb{R}$, $\mathbb{N}$, $\mathbb{R}_{>0}$ and $\mathbb{R}_{\geq 0}$ denote the sets of real numbers, natural numbers, positive real numbers, and nonnegative real numbers, respectively. $\|x\|$ denotes the 2-norm of vector $x \in \mathbb{R}^n$. $0_{m\times n}$ denotes a zero matrix with m rows and n columns, while 0_m means a column vector of size m filled with 0. I_n denotes an identity matrix with n dimensions. The superscript T means the transpose of a matrix. Denote the index set of sequential integers as $\mathbf{I}[m,n] = \{m, m+1, \ldots, n\}$, where $m < n$ are two natural numbers.

II. Preliminaries

A. Graph Theory

We employ one directed graph and another undirected graph as the communication topology of the UAV swarm. For the UAV swarm, the $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \boldsymbol{A})$ is a ternary, which consists of a node set $\mathcal{V} = \{1, 2, \ldots, N\}$; an edge set $\mathcal{E} \subset \mathcal{V} \times \mathcal{V} = \{(v_j,\ v_i) \mid v_i,\ v_j \in \mathcal{V}\}$; and an adjacency matrix $\boldsymbol{A} = [a_{ij}] \in \mathbb{R}^{N\times N}$ is a weight matrix such that $a_{ij} \neq 0 \Leftrightarrow (v_j,\ v_i) \in \mathcal{E}$ and $a_{ij} = 0$, otherwise. The neighbour set of node v_i is defined by $\mathcal{N}_i = \{v_j \in \mathcal{V} \mid (v_j,\ v_i) \in \mathcal{E}\}$. The Laplacian matrix $L \in \mathbb{R}^{n\times n}$ of graph $\mathcal{G}$ with order N is defined as $[L]_{ii} = \sum_{j\in\mathcal{N}_i} a_{ij}$ and $[L]_{ij} = -a_{ij}$ for any $i \neq j$. A directed path of length m from node v_{s_0} to v_{s_m} is an ordered sequence of distinct nodes $\{v_{s_0}, v_{s_1}, \ldots, v_{s_m}\}$ where $(v_{s_i}, v_{s_{i+1}}) \in \mathcal{E},\ \forall i \in \mathbf{I}[0, m-1]$, which means that the information travels in directions from v_{s_0} to v_{s_m}. Conversely, an undirected graph of length m from node v_{s_0} to v_{s_m} is no orientation of distinct nodes $\{v_{s_0}, v_{s_1}, \ldots, v_{s_m}\}$ where $(v_{s_i}, v_{s_{i+1}}) \in \mathcal{E},\ \forall i \in \mathbf{I}[0, m-1]$, which means that nodes v_{s_0} and v_{s_m} can communicate information with each other.

B. Problem Formulation

For a UAV swarm with N agents, we consider the dynamics model of ith UAV as

$$\underbrace{\begin{bmatrix}\dot{p}_i^n\\ \dot{v}_i^n\\ \dot{a}_i^n\end{bmatrix}}_{\dot{x}_i^n} = \underbrace{\begin{bmatrix}0_{3\times3} & I_3 & 0_{3\times3}\\ 0_{3\times3} & 0_{3\times3} & I_3\\ 0_{3\times3} & 0_{3\times3} & 0_{3\times3}\end{bmatrix}}_{A_{veh}} \underbrace{\begin{bmatrix}p_i^n\\ v_i^n\\ a_i^n\end{bmatrix}}_{x_i^n} + \underbrace{\begin{bmatrix}0_{3\times3}\\ 0_{3\times3}\\ I_3\end{bmatrix}}_{B_{veh}} u_i^n, i \in \mathbf{I}[1, N] \tag{1}$$

where $\bullet_i^n = [\bullet_{i,x}^n, \bullet_{i,y}^n, \bullet_{i,z}^n]^{\mathrm{T}} \in \mathbb{R}^3$ and $\bullet \in \{p, v, a, u\}$ denotes the nominal position, velocity, acceleration and the control input (jerk) of the attacked ith UAV in formation, respectively. Instead, in this work, we define

$$\underbrace{\begin{bmatrix}\dot{p}_i\\ \dot{v}_i\\ \dot{a}_i\end{bmatrix}}_{\dot{x}_i} = \underbrace{\begin{bmatrix}0_{3\times3} & I_3 & 0_{3\times3}\\ 0_{3\times3} & 0_{3\times3} & I_3\\ 0_{3\times3} & 0_{3\times3} & 0_{3\times3}\end{bmatrix}}_{A_{veh}} \underbrace{\begin{bmatrix}p_i\\ v_i\\ a_i\end{bmatrix}}_{x_i} + \underbrace{\begin{bmatrix}0_{3\times3}\\ 0_{3\times3}\\ I_3\end{bmatrix}}_{B_{veh}} u_i, i \in \mathbf{I}[1, N] \tag{2}$$

where $\bullet_i = [\bullet_{i,x}, \bullet_{i,y}, \bullet_{i,z}]^{\mathrm{T}} \in \mathbb{R}^3$ with $\bullet \in \{p, v, a, u\}$ denotes the real position, velocity, acceleration and the control input of the ith UAV in formation, respectively. Herein, the UAV is equipped with two kinds of sensors: a GPS sensor measuring the UAV's absolute position and a UWB sensor measuring the relative distances between itself and its neighbours without the

attacks, the sensor readings are

$$y_i^{n,\mathrm{GPS}} = p_i^n, \quad y_{i,j}^{n,\mathrm{UWB}} = (p_i^n - p_j^n)^{\mathrm{T}}(p_i^n - p_j^n). \tag{3}$$

Considering that a covert attacker exists in the flight of the UAV formation, which deceives the reading signal of GPS and UWB sensors. The attacked sensor readings are given as

$$y_i^{\mathrm{GPS}} = p_i + u_i^{\mathrm{GPS}}, \quad y_{i,j}^{\mathrm{UWB}} = (p_i - p_j^n)^{\mathrm{T}}(p_i - p_j^n). \tag{4}$$

where $u_i^{\mathrm{GPS}} \in \mathbb{R}^3$ is the spoofing GPS signal.

The relationship between attacker and defender is described as follows. The covert attacker attempts to change the flight track of the attacked UAV, such that the formation error of the UAV swarm is enlarged, and thus the predefined formation pattern cannot be achieved. Correspondingly, the defenders prepare their defenses in advance for any possible covert attack, making it difficult for convert attacks to succeed. More specifically, the attack targets are listed as:

1) Maximizing the deviation between the nominal and the attacked path of the UAV and thus preventing the UAV swarm from achieving the predefined formation pattern;
2) Evading detection by the well-functioning onboard UWB sensors.

Correspondingly, the defense targets are listed as:

1) The UAV swarm can minimize its integrated objective functions, including energy consumption and formation error;
2) Each UAV in the swarm could detect the abnormality when a non-covert attack occurs.

Inspired by [24], we define covert attacks on UWB sensors in a 3D environment.

Definition 1: Under the above setting, the attack $(u_i, u_i^{\mathrm{GPS}})$ is called covert if and only if the measurements satisfy

$$y_i^{\mathrm{GPS}} = y_i^{n,\mathrm{GPS}}, \forall i, \tag{5}$$

$$y_{i,j}^{\mathrm{UWB}} = y_{i,j}^{n,\mathrm{UWB}}, \forall j \in \mathcal{N}_i, \tag{6}$$

during the whole flight journey.

C. Covert Attack Characteristics

Denote that $s_{i,j}^n(t) = p_i^n(t) - p_j^n(t)$ and $s_{i,j}(t) = p_i(t) - p_j^n(t)$ which represent UAV's nominal and attacked relative positions w.r.t. the j-th neighbour, respectively. Denote that $R(p_i^n(t)) = [s_{i,1}^n(t), s_{i,2}^n(t), \ldots, s_{i,m}^n(t)] \in \mathbb{R}_{3\times m}$, $m = |\mathcal{N}_i|$.

Lemma 1: The covert attacks in definition exists under the condition that $\mathrm{rank}(R(p_i^n(t))) \leq 2, \exists t$.

Proof: Lemma 1 is proven via Reduction to Absurdity. We show that all covert attacks subject to $u_i = u_i^n$ under the condition that $\mathrm{rank}(R(p_i^n(t))) \geq 3, \forall t$. From the assumption that $x_n(0) = x(0)$, we have $s_{i,j}(0) = s_{i,j}^n(0), \forall i = \mathbf{I}(1,j)$. By recalling Definition 1, covert attacks require that

$$\dot{y}_{i,j}^{\mathrm{UWB}} - \dot{y}_{i,j}^{n,\mathrm{UWB}} = {v_i}^{\mathrm{T}} s_{i,j} - {v_i^n}^{\mathrm{T}} s_{i,j}^n = 0.$$

Or equivalently, $\forall a, b, c \in \mathbf{I}(1,j)$,

$$(v_i(\tau) - v_i^n(\tau))^{\mathrm{T}}[s_{i,a}^n(\tau)\, s_{i,b}^n(\tau)\, s_{i,c}^n(\tau)] = 0.$$

Since $\mathrm{rank}(R(p_i^n(t))) \geq 3$, it follows that $s_{i,a}^n(\tau)$, $s_{i,b}^n(\tau)$ and $s_{i,c}^n(\tau)$ are linearly independent to each other. Hence, we have

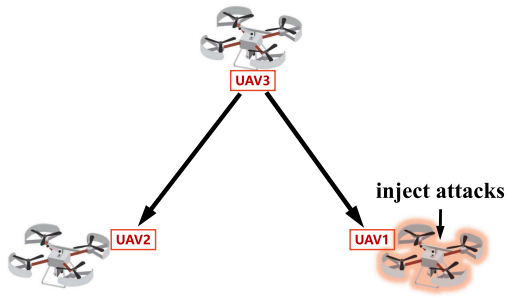


Fig. 1. Swarm of three UAVs in SNS: the UAV1 is subjected to covert attacks.

$v_i(\tau) = v_i^n(\tau)$ and thus $s_{i,j}(\tau_+) = s_{i,j}^n(\tau_+)$. By repeating the above process, we obtain that $u_i = u_i^n, \forall t$, which means that no covert attack exists. This arouses a contradiction, which finishes the proof. ■

Remark 1: According to Lemma 1, we present two situations in which a UAV formation is vulnerable to covert attack:

1) single neighbour scenarios (SNS);
2) double neighbours scenarios (DNS).

When the attacked drone has three or more neighbours, it follows from Lemma 1 that a covert attack exists if and only if all the neighbours are collinear. In fact, this special condition is also applicable to the case of DNS. The optimal attack and defense strategies under collinearity of neighbours are essentially the same as those in DNS to be described in Section IV later, which are thus omitted. □

III. Attack and Defense Trajectory Generation in SNS

A. Optimal Covert Attacks in SNS

In this section, we discuss the problems of the covert attack trajectory of the SNS, and how to design a good initial value to solve the problem quickly. For simplicity, we consider a swarm of three UAVs for example. As shown in Fig. 1, each UAV has only one neighbour. Without loss of generality, the attacked UAV is indexed by 1. Based on (5) and (6), the covert attack in SNS exists when the attacked path p_1 and the spoofing GPS signal u_1^{GPS} satisfy:

$$(p_1 - p_3^n)^2 = (p_1^n - p_3^n)^2, \quad u_1^{\mathrm{GPS}} = p_1 - p_1^n. \tag{7}$$

Lemma 2: Every covert attack $(u_i, u_i^{\mathrm{GPS}})$ subjects to

$${p_1}^{\mathrm{T}} p_1 - 2{p_1}^{\mathrm{T}} p_3^n = {p_1^n}^{\mathrm{T}} p_1^n - 2{p_1^n}^{\mathrm{T}} p_3^n, \tag{8}$$

$$u_1^{\mathrm{T}}(p_1 - p_3^n) = (u_1^n)^{\mathrm{T}}(p_1^n - p_3^n). \tag{9}$$

Proof: First, it can be computed from $(s_{i,j}^n)^{\mathrm{T}} s_{i,j}^n = s_{i,j}^{\mathrm{T}} s_{i,j}$ that (8) is right. By taking the time derivative on both sides of $y_{1,3}^{n,\mathrm{UWB}} = y_{1,3}^{\mathrm{UWB}}$, one can obtain

$$v_1^{\mathrm{T}}(p_1 - p_3^n) = (v_1^n)^{\mathrm{T}}(p_1^n - p_3^n). \tag{10}$$

By taking the time derivative on both sides of (10), we obtain

$$a_1^{\mathrm{T}}(p_1 - p_3^n) = (a_1^n)^{\mathrm{T}}(p_1^n - p_3^n). \tag{11}$$

By taking the time derivative on both sides of (11), one has (9). ■

Based on (8) and (9), the following objective function is considered

$$\max_{u_1} \quad \| (p_1(T) - h_{p,i}) - \frac{1}{|\mathcal{N}_i|} \sum_{j \in J_i} (p_j^n(T) - h_{p,j}) \|^2, \tag{12}$$

$$\text{s.t.} \quad {p_1}^{\mathrm{T}} p_1 - 2{p_1}^{\mathrm{T}} p_3^n = {p_1^n}^{\mathrm{T}} p_1^n - 2{p_1^n}^{\mathrm{T}} p_3^n, \tag{12a}$$

$$u_1^{\mathrm{T}}(p_1 - p_3^n) = (u_1^n)^{\mathrm{T}}(p_1^n - p_3^n), \tag{12b}$$

$$\|u_a\| \le \bar{u}, \tag{12c}$$

$$x(0) = x_1^n(0). \tag{12d}$$

where $h_{p,j}$ represents formation pattern associated with jth UAV. In (12), (12a) denotes covert constraint on UWB sensors, (12b) denotes constraint on input signals, and (12c) means the constraint on the upper bound of the input signals.

In this work, we use polynomials to represent trajectories to improve computational efficiency. The covert attack polynomials trajectory is defined as

$$p_i = \left\{ \begin{bmatrix} 1 & t & t^2 & t^3 & \cdots & t^n \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right\} \underbrace{\begin{bmatrix} P_{i,x} & P_{i,y} & P_{i,z} \end{bmatrix}}_{P}, \tag{13}$$

where $P \in \mathbb{R}^{(n+1)\times 3}$ is the polynomials coefficient. Notice that in our paper that $n = 5$ is a fifth-order polynomial.

Based on (8), (12) and (13), this optimization problem is reformulated as a Quadratic Constraint Quadratic Programming (QCQP) problem in (14) by substituting the above definition of polynomial trajectories into (12), we solve the (x, y, z) of the UAV1, and then derive the control input u according to the differential flat characteristics of the UAV,

$$\max_{X_1} \quad X_1^{\mathrm{T}} Q X_1 - 2X_1^{\mathrm{T}}(E_{px}C_1 + E_{py}C_2 + E_{pz}C_3)Q_T + {E_p}^2, \tag{14}$$

$$\text{s.t.} \quad X_1^{\mathrm{T}} Q X_1 - 2(X_1^{\mathrm{T}} Q_T p_3^n - {p_1^n}^{\mathrm{T}} p_3^n) - {p_1^n}^{\mathrm{T}} p_1^n = 0, \tag{14a}$$

$$X_1^{\mathrm{T}} Q_T Q_u^{\mathrm{T}} X_1 - X_1^{\mathrm{T}} Q_u p_3^n - u_1^n(p_1^n - p_3^n) = 0, \tag{14b}$$

$$-\bar{u} \le Q_u^{\mathrm{T}} X_1 \le \bar{u}, \tag{14c}$$

$$x(0) = x_1^n(0), \tag{14d}$$

where

$$E = h_i + \frac{1}{|\mathcal{N}_i|} \sum_{j \in \mathcal{N}_i} (x_j(T) - h_j),$$

$$E_p = h_{p,i} + \frac{1}{|\mathcal{N}_i|} \sum_{j \in \mathcal{N}_i} (p_j^n(T) - h_{p,j}),$$

$$E_v = h_{v,i} + \frac{1}{|\mathcal{N}_i|} \sum_{j \in \mathcal{N}_i} (x_{vj}(T) - h_{v,j}),$$

Algorithm 1 Covert Attack Algorithm.

Initialization: $\mathbf{X}_1^0 \leftarrow$ **random**
Input: $(\mathbf{X}_1^0, \mathbf{T})$, $(\mathbf{h}_p, \mathbf{h}_v, \mathbf{h}_a)$.
Output: $(\mathbf{X}_1)$, **Trajectory**
1: $(\mathbf{X}_1^{bad}) \leftarrow$ **mini snap + mini formation**
2: $(\mathbf{X}_1^{good}) \leftarrow$ **based on geometric**
3: $(\mathbf{X}_1) \leftarrow$ **Interior point method**
4: **return** $(\mathbf{X}_1, u_1)$

$$E_a = h_{ai} + \frac{1}{|\mathcal{N}_i|} \sum_{j \in \mathcal{N}_i} (x_{aj}(T) - h_{aj}).$$

In (14), denote $P_{1,x}, P_{1,y}, P_{1,z}$ as the polynomial coefficients of X-axis, Y-axis and Z-axis for UAV_1, respectively,

$$X_1 = \begin{bmatrix} P_{1,x}^{\mathrm{T}} & P_{1,y}^{\mathrm{T}} & P_{1,z}^{\mathrm{T}} \end{bmatrix}^{\mathrm{T}} \in \mathbb{R}^{3(n+1)},$$

$$Q = \mathrm{blkdiag}[Q_1 \quad Q_2 \quad Q_3] \in \mathbb{R}^{3(n+1)\times 3(n+1)},$$

$$Q_1 = C_1 Q_t Q_t^{\mathrm{T}} C_1^{\mathrm{T}} \in \mathbb{R}^{(n+1)\times(n+1)},$$

$$Q_t = [1 \quad t \quad t^2 \quad t^3 \quad \dots \quad t^n]^{\mathrm{T}} \in \mathbb{R}^{(n+1)\times 1},$$

$C_1 \in \mathbb{R}^{3(n+1)\times(n+1)}$ represents the mapping matrix satisfying $P_{1,x} = C_1^{\mathrm{T}} X_1 \in \mathbb{R}^{n+1}$. Similarly, we have $P_{1,y} = C_2^{\mathrm{T}} X_1$, $P_{1,z} = C_3^{\mathrm{T}} X_1$.

Moreover, we have $Q_2 = C_2 Q_t Q_t^{\mathrm{T}} C_2^{\mathrm{T}}$, $Q_3 = C_3 Q_t Q_t^{\mathrm{T}} C_3^{\mathrm{T}}$, where Q_u and Q_T are defined as

$$Q_u = [0 \quad 0 \quad 0 \quad 6 \quad \dots \quad n(n-1)(n-2)t^{(n-3)}]^{\mathrm{T}} \otimes [1 \quad 1 \quad 1]^{\mathrm{T}} \in \mathbb{R}^{3(n+1)\times 1},$$

$$Q_T = Q_t \otimes [1 \quad 1 \quad 1]^{\mathrm{T}} \in \mathbb{R}^{3(n+1)\times 1}.$$

Remark 2: A good initial value strategy based on geometric features for SNS.

For a non-convex problem like (14), the optimal solution can be obtained quickly by relying on a good initial value. Therefore, we give a condition to get a good initial value based on geometric information to solve the problem of covert attacks under SNS.

The idea of a good initial value: First of all, three initial value points are calculated, namely the initial value point, the nominal trajectory point at $\frac{T}{2}$, and the point where the formation error is the largest when the spatial constraint is satisfied at the last moment.

$$\max_{p_{\text{init}}} \quad \| (p_{\text{init}} - h_{p,i}) - \frac{1}{|\mathcal{N}_i|} \sum_{j \in J_i} (p_j^n(T) - h_{p,j}) \|^2,$$

$$\text{s.t.} \quad {p_{\text{init}}}^{\mathrm{T}} p_{\text{init}} - 2{p_{\text{init}}}^{\mathrm{T}} p_3^n = {p_1^n}^{\mathrm{T}} p_1^n - 2{p_1^n}^{\mathrm{T}} p_3^n.$$

Then according to the T_0 moment position, velocity, acceleration, $\frac{T}{2}$ moment position, velocity, T moment position, solve six equations of six unknowns to get the initial values. The good initial value is shown in Fig. 2. □

How to select a good initial value algorithm for SNS is summarized in Algorithm 1

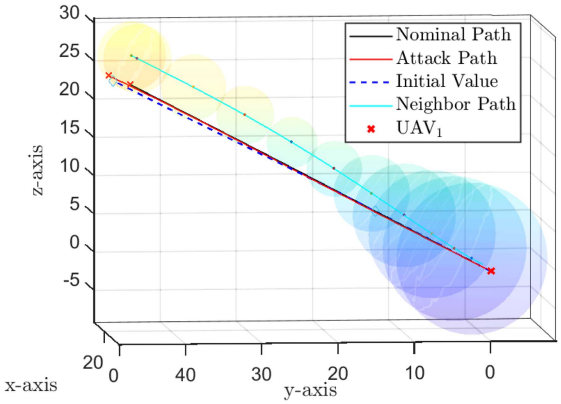


Fig. 2. Covert attack path and good initial value: The blue dotted line is the trajectory represented by the good initial value obtained, and the green line represents the trajectory of the neighbour of the trajectory being attacked, and the ball on the trajectory forms a spatial constraint of the concealed attack trajectory, and the concealed attack trajectory must be on these continuous spheres. The solid red line represents the attack trajectory, which does not fully coincide with the maximum formation error point due to the constraint of (9).

B. Time-Critical Defense Strategy in SNS

This section addresses the formation secure trajectory planning problem in the SNS case. First, we give the input description of the absolute secure trajectory; then, we design the generation of the secure trajectory according to this input. We say that if each UAV's u satisfies one of the following mutually exclusive conditions, the formation trajectory is safe.

1) $p = p_n$ at all times;
2) if $p \neq p_n$ at some time, the attack u is detectable.

In order to deal with the above covert attack, we propose a time-critical defense scheme in this subsection. The defense target is to minimize the mixed objective function of formation error, time consumption, and attack resilience. We formulate the trajectory generation as an unconstrained optimization problem:

$$\begin{aligned} J_i &= \min_{X_i,T} \sum_{\epsilon} \lambda_\epsilon J_{i,\epsilon}, \\ &= \min_{X_i,T} \lambda_r J_{i,r} + \lambda_t J_{i,t} + \lambda_d J_{i,d} + \lambda_e J_{i,e} + \lambda_f J_{i,f}, \end{aligned} \tag{15}$$

where $J_{i,r}$, $J_{i,t}$, $J_{i,d}$, $J_{i,e}$, and $J_{i,f}$ denote the attack resilience term, execution time term, dynamical feasibility term, control effort term, and formation shape term for the ith UAV, respectively; and $\lambda_\bullet$, $\bullet \in \{r, t, d, e, f\}$, denote the associated weights to adjust the importance of the above different terms.

$$J = \min_{X,T} \sum_{i}^{M} J_i, \tag{16}$$

$$\frac{\partial J}{\partial c} = \left[\frac{\partial J}{\partial X}, \frac{\partial J}{\partial T}\right]^{\mathrm{T}}. \tag{17}$$

Where $M = 3$ represents the number of UAV in the swarm, $X = [X_1, X_2, X_3] \in \mathbb{R}^{9(n+1)}$ and $c = [X, T]^{\mathrm{T}}$ in our case. Commonly, a sufficiently large weight suffices for penalties. The problem is solved via unconstrained nonlinear optimization.

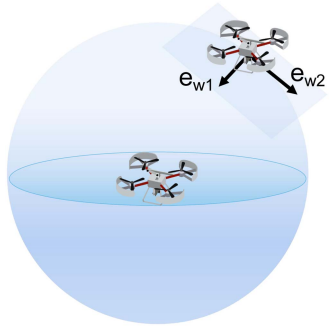


Fig. 3. Attack direction in SNS: the UAV on the top right corner is subjected to attacks.

1) Attack Resilience J_r: The suppression of attacks is achieved by punishing inputs in the offensive direction. Define that

$$\begin{cases} F_{1,i} = (p_{i,x}(t) - p_{j,x}(t), p_{i,y}(t) - p_{j,y}(t), p_{i,z}(t) - p_{j,z}(t)), \\ F_{2,i} = (p_{j,x}(t), p_{j,y}(t), p_{j,z}(t)), \\ W_{1,i} = F_{1,i} \times F_{2,i}, \\ W_{2,i} = W_{1,i} \times F_{1,i}, \\ W_1 = [W_{1,1}, W_{1,2}, W_{1,3}], \\ W_2 = [W_{2,1}, W_{2,2}, W_{2,3}]. \end{cases} \tag{18}$$

It can be verified that $W_{1,i} \perp (F_{1,i}, F_{2,i})$ and, $W_{2,i} \perp (W_{1,i}, F_{1,i})$. Define that $e_{w1} = [\frac{W_{1,1}}{\|W_{1,1}\|}, \frac{W_{1,2}}{\|W_{1,2}\|}, \frac{W_{1,3}}{\|W_{1,3}\|}]^{\mathrm{T}} \in \mathbb{R}^{1\times 9}$ and $e_{w2} = [\frac{W_{2,1}}{\|W_{2,1}\|}, \frac{W_{2,2}}{\|W_{2,2}\|}, \frac{W_{2,3}}{\|W_{2,3}\|}]^{\mathrm{T}} \in \mathbb{R}^{1\times 9}$. The above attack directions e_{w1} and e_{w2} are vivid represented in Fig. 3. Based on the above attack directions e_{w1} and e_{w2}, we define the penalty for i-th UAV as:

$$J_r = \sum_{k=0}^{T/\delta t} |(e_{w1}(k) + e_{w2}(k))U|, \tag{19}$$

where $U = [u_{1,x}, u_{1,y}, u_{1,z}, u_{2,x}, u_{2,y}, u_{2,z}, u_{3,x}, u_{3,y}, u_{3,z}]^{\mathrm{T}} \in \mathbb{R}^{9\times 1}$ represents the input of each UAV in the swarm. A frequently-used derivative formula is given as follows:

$$\frac{\partial \frac{Px}{\|Px\|}}{\partial x} = \frac{P^{\mathrm{T}}}{\|Px\|} - \frac{P^{\mathrm{T}}(Px)(Px)^{\mathrm{T}}}{\|Px\|^3} \triangleq \Gamma_x(P), \tag{20}$$

and its derivatives with respect to X and T are

$$\begin{aligned} \frac{\partial J_r}{\partial X} &= \sum_{k=0}^{T/\delta t} \frac{(e_{w1}(k) + e_{w2}(k))U}{|(e_{w1}(k) + e_{w2}(k))U|} (\Gamma_x(F_1) + \Gamma_x(F_2))U \\ &\quad + \frac{\partial U}{\partial t}(e_{w1}^{\mathrm{T}} + e_{w2}^{\mathrm{T}}), \end{aligned} \tag{21}$$

$$\frac{\partial J_r}{\partial T} = |(e_{w1}(T/\delta) + e_{w2}(T/\delta))U(T)|. \tag{22}$$

We defined that

$$\begin{aligned} &t_v = \dot{t}_p,\ t_a = \ddot{t}_p,\ t_u = \dddot{t}_p, \\ &t_p = [1 \quad t \quad t^2 \quad t^3 \quad \cdots \quad n(n-1)(n-2)t^{n-3}]^{\mathrm{T}}, \end{aligned}$$

$$\frac{\partial U}{\partial t} = \text{blkdiag}[t_u^{\mathrm{T}} \quad \cdots \quad t_u^{\mathrm{T}}] \in \mathbb{R}^{9(n+1)\times 9}.$$

Then, $F_1 = \partial W_1/\partial X$ and $F_2 = \partial W_2/\partial X$.

2) Execution Time J_t: A shorter execution time is desirable, so we also minimize the weighted total execution time $J_t = T$. Obviously, its gradient $\partial J_{i,t}/\partial X = 0_{9(n+1)\times 1}$, $\partial J_t/\partial T = 1$.

3) Dynamical Feasibility Penalty J_d: For the trajectory generation of the dynamic feasibility is always guaranteed by limiting the trajectory's derivatives. In our work, we limit the amplitude of velocity, acceleration, and jerk. Note that the dynamical feasibility penalty is acquired constraints of time $T > 0$. The constraints of velocity, acceleration, and jerk are denoted as

$$J_{i,dv} = \sum_{k=0}^{T/\delta t} \max\{v(t_k)^2 - v_{\max}^2, 0\}^2, \tag{23}$$

$$J_{i,da} = \sum_{k=0}^{T/\delta t} \max\{a(t_k)^2 - a_{\max}^2, 0\}^2, \tag{24}$$

$$J_{i,du} = \sum_{k=0}^{T/\delta t} \max\{u(t_k)^2 - u_{\max}^2, 0\}^2, \tag{25}$$

$$J_d = \sum_{i}^{M} (J_{i,dv} + J_{i,da} + J_{i,dj}). \tag{26}$$

where $v_{\max}$, $a_{\max}$, $j_{\max}$ are maximum allowed velocity, acceleration and jerk. The corresponding gradients are

$$\frac{\partial J_{i,\mathrm{dv}}}{\partial X} = \sum_{k=0}^{T/\delta t} \begin{bmatrix} v_{v,1}^T & v_{v,2}^T & v_{v,3}^T \end{bmatrix}^T, \tag{27}$$

where

$$v_{v,1} = \max\{4(v_{i,x}^3 + v_{i,x}v_{i,y}^2 + v_{i,x}v_{i,z}^2 - v_{i,x}v_{\max}^2)t_v^{\mathrm{T}}, 0_{18\times 1}\},$$
$$v_{v,2} = \max\{4(v_{i,y}^3 + v_{i,y}v_{i,x}^2 + v_{i,y}v_{i,z}^2 - v_{i,y}v_{\max}^2)t_v^{\mathrm{T}}, 0_{18\times 1}\},$$
$$v_{v,3} = \max\{4(v_{i,z}^3 + v_{i,z}v_{i,y}^2 + v_{i,z}v_{i,x}^2 - v_{i,z}v_{\max}^2)t_v^{\mathrm{T}}, 0_{18\times 1}\},$$

and

$$\frac{\partial J_{i,\mathrm{da}}}{\partial X} = \sum_{k=0}^{T/\delta t} \begin{bmatrix} v_{a,1}^T & v_{a,2}^T & v_{a,3}^T \end{bmatrix}^T, \tag{28}$$

where

$$v_{a,1} = \max\{4(a_{i,x}^3 + a_{i,x}a_{i,y}^2 + a_{i,x}a_{i,z}^2 - a_{i,x}a_{\max}^2)t_a^{\mathrm{T}}, 0_{18\times 1}\},$$
$$v_{a,2} = \max\{4(a_{i,y}^3 + a_{i,y}a_{i,x}^2 + a_{i,y}a_{i,z}^2 - a_{i,y}a_{\max}^2)t_a^{\mathrm{T}}, 0_{18\times 1}\},$$
$$v_{a,3} = \max\{4(a_{i,z}^3 + a_{i,z}a_{i,y}^2 + a_{i,z}a_{i,x}^2 - a_{i,z}a_{\max}^2)t_a^{\mathrm{T}}, 0_{18\times 1}\},$$

and

$$\frac{\partial J_{i,\mathrm{du}}}{\partial X} = \sum_{k=0}^{T/\delta t} \begin{bmatrix} v_{u,1}^T & v_{u,2}^T & v_{u,3}^T \end{bmatrix}^T, \tag{29}$$

where

$$v_{u,1} = \max\{4(u_{i,x}^3 + u_{i,x}u_{i,y}^2 + u_{i,x}u_{i,z}^2 - u_{i,x}u_{\max}^2)t_u^{\mathrm{T}}, 0_{18\times 1}\},$$
$$v_{u,2} = \max\{4(u_{i,y}^3 + u_{i,y}u_{i,x}^2 + u_{i,y}u_{i,z}^2 - u_{i,y}u_{\max}^2)t_u^{\mathrm{T}}, 0_{18\times 1}\},$$
$$v_{u,3} = \max\{4(u_{i,z}^3 + u_{i,z}u_{i,y}^2 + u_{i,z}u_{i,x}^2 - u_{i,z}u_{\max}^2)t_u^{\mathrm{T}}, 0_{18\times 1}\}.$$

In summary, its derivatives with respect to X is

$$\frac{\partial J_d}{\partial X} = \begin{bmatrix} \frac{\partial J_{i,dv}}{\partial X} + \frac{\partial J_{i,da}}{\partial X} + \frac{\partial J_{i,du}}{\partial X} \\ \vdots \\ \frac{\partial J_{M,dv}}{\partial X} + \frac{\partial J_{M,da}}{\partial X} + \frac{\partial J_{M,du}}{\partial X} \end{bmatrix} \in \mathbb{R}^{9(n+1)\times 9}, \tag{30}$$

and its derivatives with respect to T is

$$\frac{\partial J_d}{\partial T} = \max\{v(T)^2 - v_{\max}^2, 0\}^2 + \max\{a(T)^2 - a_{\max}^2, 0\}^2 + \max\{u(T)^2 - u_{\max}^2, 0\}^2.$$

4) Formation Shape J_f: Formation shape generation is generated by a formation error penalty term, which is defined as a formation error penalty term

$$J_f = \sum_{i}^{M} \| (x_i(T) - h_i) - \frac{1}{|\mathcal{N}_i|} \sum_{j\in\mathcal{N}_i} (x_j(T) - h_j) \|^2, \tag{31}$$

and its derivatives with respect to X and T are

$$\frac{\partial J_f}{\partial X} = 2\sum_{i}^{M} (x_i(T) - h_i) - \frac{1}{|\mathcal{N}_i|} \sum_{j\in\mathcal{N}_i} (x_j(T) - h_j) t_p^{\mathrm{T}}, \tag{32}$$

$$\frac{\partial J_f}{\partial T} = \sum_{i}^{M} \| (\dot{x}_i(T) - h_i) - \frac{1}{|\mathcal{N}_i|} \sum_{j\in\mathcal{N}_i} (\dot{x}_j(T) - h_j) \|^2. \tag{33}$$

5) Control Effort J_e: The Control effort is considered to minimize the sum of swarm jerk:

$$J_e = \sum_{k=0}^{T/\delta t} U(k)^{\mathrm{T}} U(k). \tag{34}$$

And its derivatives with respect to X and T are

$$\frac{\partial J_e}{\partial X} = 2\sum_{k=0}^{T/\delta t} \frac{\partial U(k)}{\partial t} U(k), \tag{35}$$

$$\frac{\partial J_e}{\partial T} = 2\sum_{k=0}^{T/\delta t} \frac{\partial U(k)}{\partial t} U(k). \tag{36}$$

6) Time Constraint Elimination: Time T is an open set of $T > 0$, which is eliminated by a differential isomorphism

$$T = e^{\tau}, \tag{37}$$

$$\frac{\partial J}{\partial \tau} = \left(\frac{\partial J}{\partial T}\right) e^{\tau}. \tag{38}$$

7) Equation Constraint Elimination: The state of the UAV swarm at the moment of discovery of a potential covert attack is known to both attacker and defender. X_1, X_2, X_3 are first three coefficients determined by $x_1(0), x_2(0), x_3(0)$. For

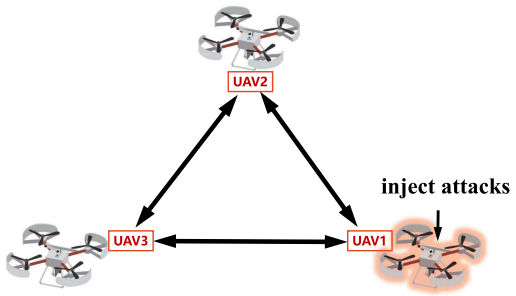


Fig. 4. Undirected: the UAV1 is attacked.

Algorithm 2 Defense Trajectory Generation Algorithm.

Initialization: $(\mathbf{X}_0, \mathbf{T}_0)$, $\mathbf{g}_0 \leftarrow \frac{\partial J}{\partial c}$, $\mathbf{B}_0 \leftarrow \mathbf{I}$, $\mathbf{k} \leftarrow 0$, $\delta \leftarrow 1.0 \times 10^{-8}$, $\eta = 0$

Input: Initial guess solution $(\mathbf{X}_0, \mathbf{T}_0)$, expected formation matrix $(\mathbf{h_p}, \mathbf{h_v}, \mathbf{h_a})$, dynamics parameter $(\mathbf{v_{max}}, \mathbf{a_{max}}, \mathbf{u_{max}})$, penalty coefficient$(\lambda_\mathbf{r}, \lambda_\mathbf{t}, \lambda_\mathbf{e}, \lambda_\mathbf{d}, \lambda_\mathbf{f})$.

Output: Polynomial coefficient and optimal time horizon $(\mathbf{X}, \mathbf{T})$

while $\eta = 0$ **do** Determine whether the trajectory satisfies the dynamic constraints
  while $\| g^k \| \leq \delta$ **do**
    $d \leftarrow \mathbf{B}^k \mathbf{g}^k$.
    $t \leftarrow lewis(Overton - Line - Search)$Improved line search method.
    $x^{k+1} \leftarrow x^k + td$ Update the search values.
    $g^{k+1} \leftarrow \frac{\partial J}{\partial c}(c = c^{k+1})$.
    $B^{k+1} \leftarrow (Cautious - Limited - Memory - BFGS(g^{k+1} - g^k, x^{k+1} - x^k))$.
    $k \leftarrow k + 1$ Update the search steps.
  if $v < v_{\max} + \varepsilon, a < a_{\max} + \varepsilon, u < u_{\max} + \varepsilon, \forall t$ **then**
    $\eta = 1$
  else if Dynamics is not satisfied **then**
    $T = T + \varepsilon$
    L-BFGS slove $\sum_i^M J_i$ Until the dynamics constraints are satisfied
    $\eta = 1$
return $(\mathbf{X}, \mathbf{T})$

example,the first three items of $P_{1,x}$ are uniquely determined is $[x_{1,p_x}(0), x_{1,v_x}(0), \frac{1}{2}x_{1,a_x}(0)]$.

The defense algorithm in SNS can be summarized in Algorithm 2 .

IV. Attack and Defense Trajectory Generation in DNS

A. Optimal Covert Attacks in DNS

For simplicity, we consider a swarm of three UAVs in DNS as shown in Fig. 4. Without loss of generality, we assume that UAV_1 is the drone under attack, and UAV_2 and UAV_3 are its two neighbours. According to (5) and (6), covert attack exists when the position of the attacked UAV and the spoofing GPS signal u_1^{GPS} satisfy:

$$\begin{cases} (p_1(t) - p_2^n(t))^2 = (p_1^n(t) - p_2^n(t))^2, \\ (p_1(t) - p_3^n(t))^2 = (p_1^n(t) - p_3^n(t))^2, t \in [0, T], \\ u_1^{\text{GPS}} = p_1 - p_1^n. \end{cases} \tag{39}$$

Lemma 3: Covert attack exists under the condition that every covert attack (u_i, u_i^{GPS}) must satisfy

$$\begin{cases} {p_1}^{\mathrm{T}} p_1 - 2{p_1}^{\mathrm{T}} p_2^n = {p_1^n}^{\mathrm{T}} p_1^n - 2{p_1^n}^{\mathrm{T}} p_2^n, \\ {p_1}^{\mathrm{T}} p_3^n - {p_1}^{\mathrm{T}} p_2^n = {p_1^n}^{\mathrm{T}} p_3^n - {p_1^n}^{\mathrm{T}} p_2^n. \end{cases} \tag{40}$$

$$\begin{cases} u_1(p_1 - p_3^n) = u_1^n(p_1^n - p_3^n), \\ u_1(p_1 - p_2^n) = u_1^n(p_1^n - p_2^n). \end{cases} \tag{41}$$

Proof: The proof is similar to Lemma 2 and thus omitted here. ■

Based on (40), the optimization scheme for optimal covert attacks is formulated as

$$\max_P \quad \| (p_1(T) - h_{p,i}) - \frac{1}{|\mathcal{N}_i|} \sum_{j \in \mathcal{N}_i} (p_j^n(T) - h_{p,j}) \|^2, \tag{42}$$

$$\text{s.t.} \quad {p_1}^{\mathrm{T}} p_1 - 2{p_1}^{\mathrm{T}} p_2^n = {p_1^n}^{\mathrm{T}} p_1^n - 2{p_1^n}^{\mathrm{T}} p_2^n, \tag{42a}$$

$${p_1}^{\mathrm{T}} p_3^n - {p_1}^{\mathrm{T}} p_2^n = {p_1^n}^{\mathrm{T}} p_3^n - {p_1^n}^{\mathrm{T}} p_2^n, \tag{42b}$$

$$u_1(p_1 - p_3^n) = u_1^n(p_1^n - p_3^n), \tag{42c}$$

$$u_1(p_1 - p_2^n) = u_1^n(p_1^n - p_2^n), \tag{42d}$$

$$\|u\| \leq \bar{u}, \tag{42e}$$

$$x(0) = x_1^n(0). \tag{42f}$$

Similar to section III, we could reformulate (42) as a QCQP problem:

$$\max_{X_1} \quad X_1^{\mathrm{T}} Q X_1 - 2X_1^{\mathrm{T}}(E_x^F C_1 + E_y^F C_2 + E_z^F C_3) Q_T + E^2, \tag{43}$$

$$\text{s.t.} \quad X_1^{\mathrm{T}} Q X_1 - 2(X_1^{\mathrm{T}} Q_T p_3^n - {p_1^n}^{\mathrm{T}} p_3^n) - {p_1^n}^2 = 0, \tag{43a}$$

$$X_1^{\mathrm{T}} Q X_1 - 2(X_1^{\mathrm{T}} Q_T p_2^n - {p_1^n}^{\mathrm{T}} p_2^n) - {p_1^n}^2 = 0, \tag{43b}$$

$$X_1^{\mathrm{T}} Q_T Q_u^{\mathrm{T}} X_1 - X_1^{\mathrm{T}} Q_u p_3^n - u_1^n(p_1^n - p_3^n) = 0, \tag{43c}$$

$$X_1^{\mathrm{T}} Q_T Q_u^{\mathrm{T}} X_1 - X_1^{\mathrm{T}} Q_u p_2^n - u_1^n(p_1^n - p_2^n) = 0, \tag{43d}$$

$$-\bar{u} \leq Q_u^{\mathrm{T}} X_1 \leq \bar{u}, \tag{43e}$$

$$x(0) = x_1^n(0). \tag{43f}$$

Remark 3 (A good initial value strategy based on geometric features for DNS): Like the method of getting the initial value in SNS. The initial value point at the T is satisfied:

$$\max_{p_{\text{init}}} \quad \| (p_{\text{init}} - h_{p,i}) - \frac{1}{|\mathcal{N}_i|} \sum_{j \in J_i} (p_j^n(T) - h_{p,j}) \|^2,$$

$$\text{s.t.} \quad {p_{\text{init}}}^{\mathrm{T}} p_{\text{init}} - 2{p_{\text{init}}}^{\mathrm{T}} p_3^n = {p_1^n}^{\mathrm{T}} p_1^n - 2{p_1^n}^{\mathrm{T}} p_3^n,$$

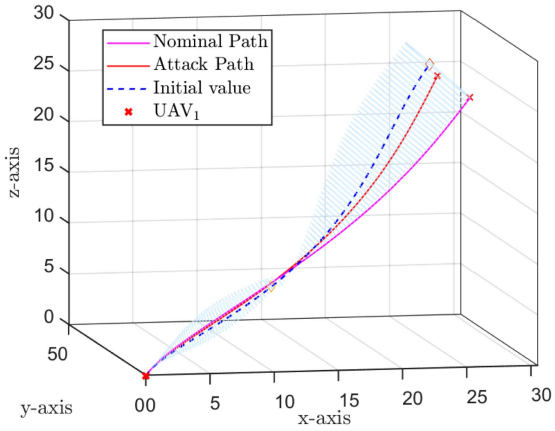


Fig. 5. Undirected: the UAV with red shading is subjected to attacks.

$$p_{\text{init}}{}^{\mathrm{T}} p_{\text{init}} - 2p_{\text{init}}{}^{\mathrm{T}} p_2^n = p_1^{n\mathrm{T}} p_1^n - 2p_1^{n\mathrm{T}} p_2^n.$$

Then according to the T_0 moment position of nominal trajectory, velocity, acceleration, $\frac{T}{2}$ moment position of nominal trajectory, velocity, T moment position, solve six equations six unknowns to get the initial values. The good initial value is shown in Fig. 5. □

B. Time-Critical Defense Strategy in DNS

We also propose a time-critical defense scheme for the covert attack problem in DNS. We require this trajectory to have as little error at the end as possible, as little energy, and as little time as possible, and u_i does not follow the attack direction. In this case, the $J_{\{t,d,e,f\}}$ are same as the $J_{\{t,d,e,f\}}$ in the SNS, the difference is attack resilience J_r.

1) Attack Resilience J_r: To illustrate the input attack direction at any point on the attack trajectory, we define

$$\begin{cases} F_{1,i} = (p_{i,x}(t) - p_{j_1,x}(t), p_{i,y}(t) - p_{j_1,y}(t), p_{i,z}(t) - p_{j_1,z}(t)), \\ F_{2,i} = (p_{i,x}(t) - p_{j_2,x}(t), p_{i,y}(t) - p_{j_2,y}(t), p_{i,z}(t) - p_{j_2,z}(t)), \\ W_{1,i} = F_{1,i} \times F_{2,i}, \\ W = [W_{1,1}, W_{1,2}, W_{1,3}], \\ e_w = [\frac{W_{1,1}}{\|W_{1,1}\|}, \frac{W_{1,2}}{\|W_{1,2}\|}, \frac{W_{1,3}}{\|W_{1,3}\|}]^{\mathrm{T}}. \end{cases}$$

It can be verified that $W_{1,i} \perp (F_{1,i}, F_{2,i})$, the attack direction vivid represented in Fig. 6.

Based on the above attack directions e_{w1} and e_{w2}, we define the penalty for i-th UAV as:

$$J_r = \sum_{k=0}^{T/\delta t} |(e_w(k))U|, \tag{44}$$

and its derivatives with respect to X and T are

$$\frac{\partial J_r}{\partial X} = \sum_{k=0}^{T/\delta t} \frac{(e_w(k))U}{|(e_w(k))U|}(\Gamma_x(F))U + \frac{\partial U}{\partial t}(e_w^{\mathrm{T}}), \tag{45}$$

$$\frac{\partial J_r}{\partial T} = |e_w(T/\delta)U(T)|. \tag{46}$$

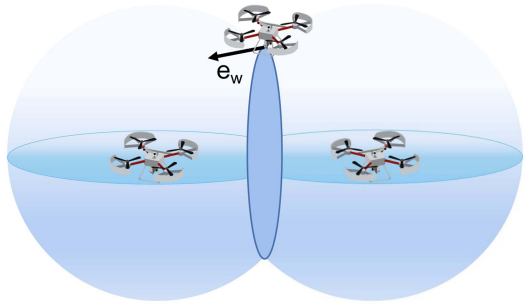


Fig. 6. Attack direction in DNS: the UAV with transparent processing is subjected to attacks.

Similar to section III-B, the problem can be solved via unconstrained nonlinear optimization.

Remark 4: This work mainly focuses on the secure path planning scheme against cyber threats, such as covert attacks, rather than physical threats, such as collision avoidance. The group collision avoidance of UAV swarms can be resolved within our framework, since the distance measurement achieved by the well-functioned UWB sensors is free from covert attacks. Specifically, the safety-related physical constraints, such as group collision avoidance, can be ensured by introducing near-field emergency mechanisms additionally, such as the fuzzy logic in the previous work [35]. For example, a UAV equipped with UWB sensors could make an emergency stop when it detects other UAVs and waits for their departure after setting a priority order.

V. Numerical Simulation

A. Case 1 (Attack and Defense in SNS)

In this section, we show that the attack and defense strategies in the SNS. The simulation parameters are selected as $T_0 = 5$ s,

$$x_1(0) = \begin{bmatrix} 0 & 0 & 0 & 1 & 2 & 1 & 1 & 2 & 1 \end{bmatrix}^{\mathrm{T}},$$

$$x_2(0) = \begin{bmatrix} 1 & 0 & 0 & 1 & 2 & 1 & 1 & 2 & 1 \end{bmatrix}^{\mathrm{T}},$$

$$x_3(0) = \begin{bmatrix} 2 & 0 & 0 & 1 & 2 & 1 & 1 & 2 & 1 \end{bmatrix}^{\mathrm{T}},$$

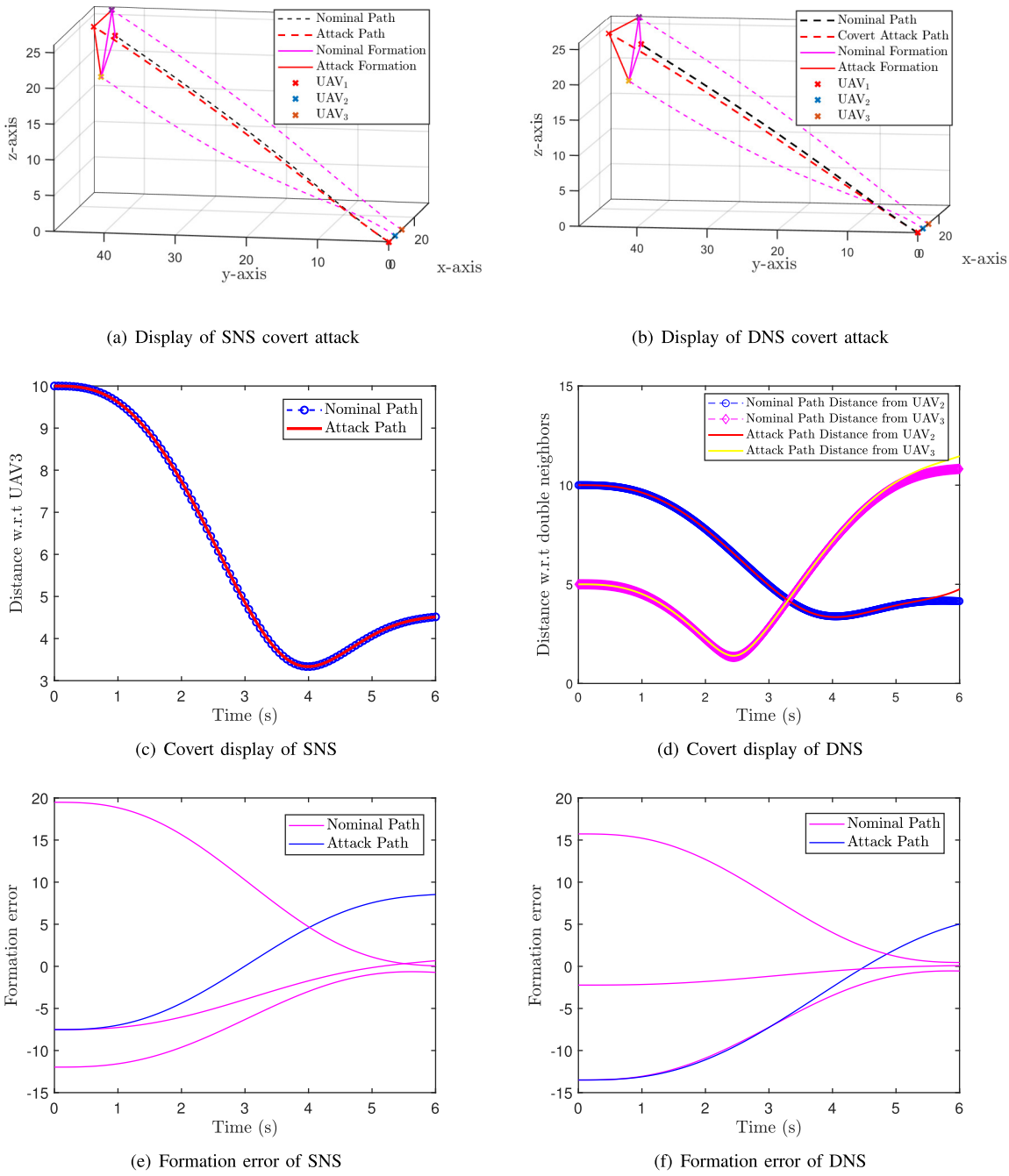
$$h_p = \begin{bmatrix} 10 & 0 & 0 & -5\sqrt{2} & 0 & -5\sqrt{2} & 5\sqrt{2} & 0 & 5\sqrt{2} \end{bmatrix}^{\mathrm{T}},$$

$$h_v = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}^{\mathrm{T}},$$

$$h_a = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}^{\mathrm{T}}.$$

The weight coefficients of each item are $\lambda_r = 1000$, $\lambda_t = 10$, $\lambda_d = 5$, $\lambda_e = 1$ and $\lambda_f = 8500$.

Based on the above parameters, the simulation results concerned about the optimal attack strategy are shown in Fig. 7(a). The covert of the attack is shown by showing that



(a) Display of SNS covert attack

(b) Display of DNS covert attack

(c) Covert display of SNS

(d) Covert display of DNS

(e) Formation error of SNS

(f) Formation error of DNS

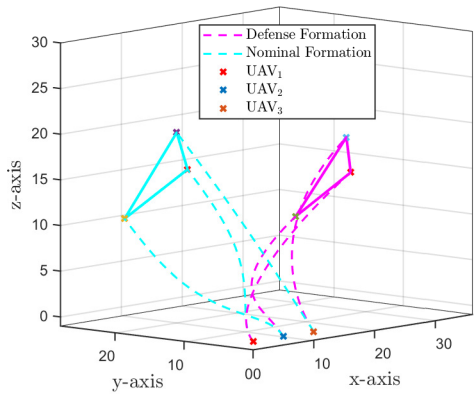
Fig. 7. Generation of covert attacks in SNS and DNS.

the UWB sensor reading on the attack trajectory of the attacked UAV equals the sensor reading on the nominal trajectory in Fig. 7(c). Where Fig. 7(e) shows the formation error generated by the covert attack. The formation error of the nominal trajectory tends to zero, while the formation error of the attacked UAV tends to be the maximum at the end time.

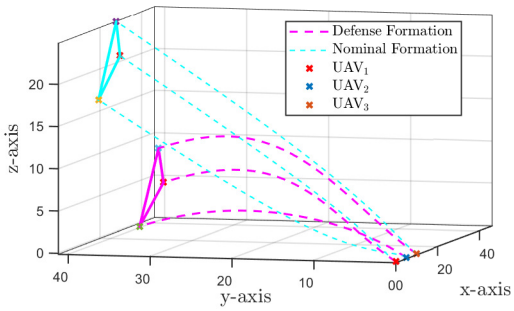
Then we consider the optimization of defense strategy to deal with the above covert attack and generate the defense trajectory of the whole formation in Fig. 8(a). Because for an attacker, every drone that meets Lemma 1 is attackable. In our results, the defense trajectory of time optimization will still spend more time and energy than the nominal trajectory. Although it spent more consumption resistance, it guarantees the convergence of formation errors, and the result is shown in Fig. 8(c).

B. Case 2 (Attack and Defense in DNS)

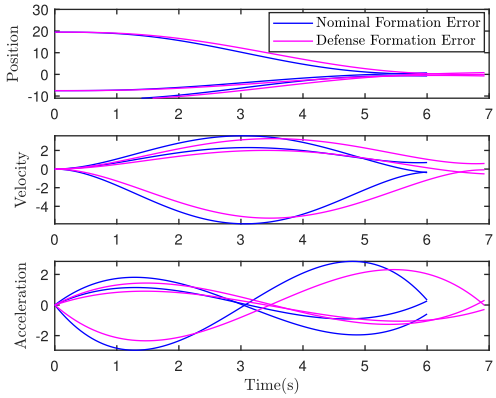
Choose the same simulation parameters as the case of SNS. We conduct another simulation example in DNS, the covert



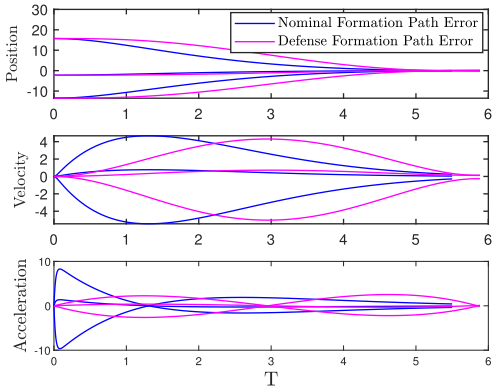
(a) Display of SNS defense



(b) Display of DNS defense



(c) Display of SNS defense formation error



(d) Display of DNS defense formation error

Fig. 8. Generation of defense for covert attacks in SNS and DNS.

attack strategy performance in DNS is shown in Fig. 7(b). Fig. 7(d) shows the concealment of the attack of the double neighbours. The reading of the distance between the two base stations on the attack track of the attacked UAV is always equal to the distance between the two base stations on the nominal track, so the concealed attack here will not be detected. Hence, we compare the formation error of the nominal trajectory and that of concealed attack trajectory. In Fig. 7(f), the nominal trajectory formation error of dual neighbours tends to zero over time, and the error of the attack trajectory is maximum at the end.

Then we consider optimizing the defense strategy to deal with the above covert attack in DNS. Fig. 8(b) and (d) show the resilient defense trajectory against the double neighbours in the entire formation. The resilient path with a larger λ_t and λ_c value is more energy efficient but less safe, as shown in Table I. Comparing the defense performances in Table I, the optimal defense strategy in DNS is both more energy efficient and safer than the counterpart in SNS under the same settings.

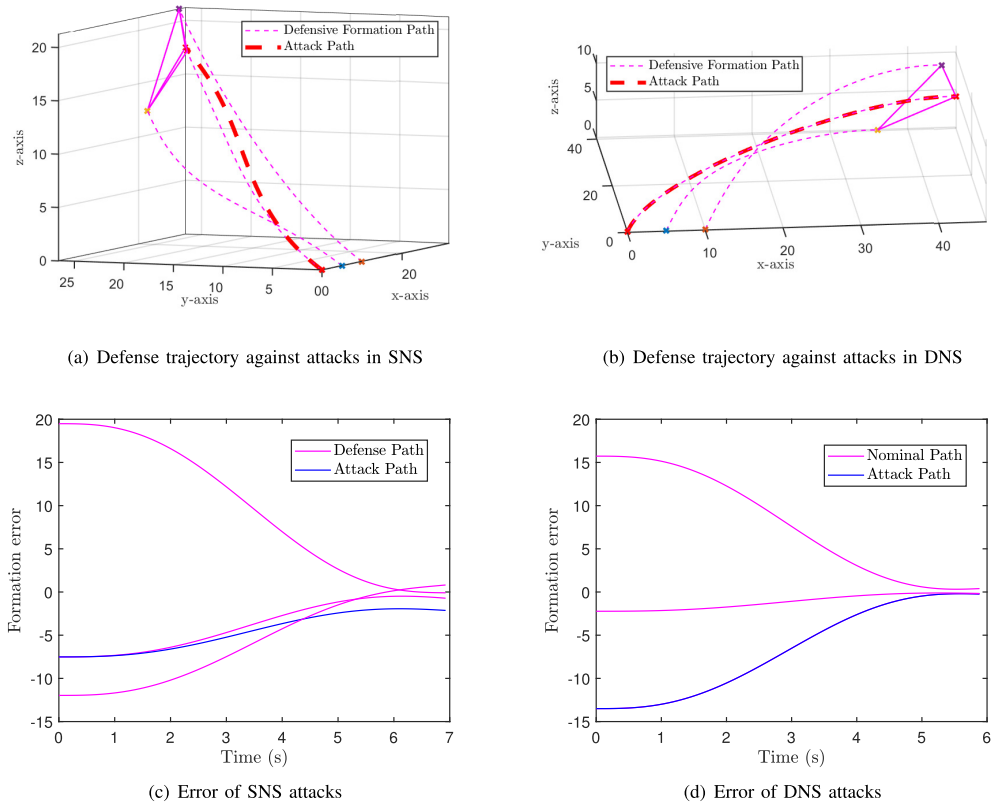
C. Case 3 (Verification of the Defense Strategy)

The effectiveness of the defense is verified by attacking our proposed attack method against our proposed defense method.

TABLE I
OPTIMAL TIME HORIZON AND ASSOCIATED DEVIATION

	λ_{others}	λ_r	$T^*(s)$	J_c
Defense in SNS	invariant	0	4.2715	2.6532×10^3
	invariant	10	4.3695	2.9562×10^3
	λ_{others}	λ_c	$T^*(s)$	J_c
Defense in DNS	invariant	0	5.8842	3.2178×10^3
	invariant	10	6.9408	5.409×10^3

In the simulations, the defense of SNS is more challenging because it has more freedom of space to attack. Hence, the defense trajectory is still attackable, but the error is significantly reduced. The results are shown in Fig. 9(a) and (c). In the DNS, the defense is easier to achieve than in SNS, as shown in Fig. 9(b) and (d). For more details of the simulation results in Cases 1 and 3, please refer to the following link https://www.bilibili.com/video/BV11W4y1R7Ah/.



(a) Defense trajectory against attacks in SNS

(b) Defense trajectory against attacks in DNS

(c) Error of SNS attacks

(d) Error of DNS attacks

Fig. 9. Defense trajectory against attacks in SNS and DNS.

VI. Conclusion

This work proposes a resilient path planning scheme against covert attacks for the formation flight of the UAV swarm. First, we give the definition and the prerequisite for the covert attacks against 3DMUs. Based on this prerequisite, an optimal covert attack strategy is formulated, which targets maximizing the UAV swarm's formation error without being detected by the well-functioning UWB sensors equipped on each UAV. A time-critical defense strategy is proposed to depress the above covert attacks, which could generate a safe and time-efficient polynomial trajectory for each UAV with both dynamic feasibility and security. The effectiveness and practicality of our theoretical results have been illustrated via numerical simulation examples. The proposed resilient path planning scheme can be extended to secure path planning against general covert attacks toward other information-incomplete sensors (such as monocular cameras) and has potential applications in anti-UAV technology [36].

References

[1] P. Yao, Z. Xie, and P. Ren, "Optimal UAV route planning for coverage search of stationary target in river," *IEEE Trans. Control Syst. Technol.*, vol. 27, no. 2, pp. 822–829, Mar. 2019.

[2] Y. Jia, Y. Yang, Q. Li, and W. Zhang, "Aerial escort task using networked miniature unmanned aerial vehicles," *Int. J. Control*, vol. 94, no. 6, pp. 1556–1566, 2021.

[3] H. Huang and A. V. Savkin, "An algorithm of reactive collision free 3-D deployment of networked unmanned aerial vehicles for surveillance and monitoring," *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 132–140, Jan. 2020.

[4] T. M. Cabreira, C. Di Franco, P. R. Ferreira, and G. C. Buttazzo, "Energy-aware spiral coverage path planning for UAV photogrammetric applications," *IEEE Robot. Automat. Lett.*, vol. 3, no. 4, pp. 3662–3668, Oct. 2018.

[5] X. Dong, B. Yu, Z. Shi, and Y. Zhong, "Time-varying formation control for unmanned aerial vehicles: Theories and applications," *IEEE Trans. Control Syst. Technol.*, vol. 23, no. 1, pp. 340–348, Jan. 2015.

[6] J. Qin, C. Yu, and B. D. Anderson, "On leaderless and leader-following consensus for interacting clusters of second-order multi-agent systems," *Automatica*, vol. 74, pp. 214–221, 2016.

[7] H. Du, G. Wen, D. Wu, Y. Cheng, and J. Lü, "Distributed fixed-time consensus for nonlinear heterogeneous multi-agent systems," *Automatica*, vol. 113, 2020, Art. no. 108797.

[8] Z. Li, Z. Duan, and L. Huang, "Leader-follower consensus of multi-agent systems," in *Proc. Amer. Control Conf.*, 2009, pp. 3256–3261.

[9] R. Olfati-Saber and R. M. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1520–1533, Sep. 2004.

[10] G. Wen, Y. Zhao, Z. Duan, W. Yu, and G. Chen, "Containment of higher-order multi-leader multi-agent systems: A dynamic output approach," *IEEE Trans. Autom. Control*, vol. 61, no. 4, pp. 1135–1140, Apr. 2016.

[11] X. Gong, Y. Cui, J. Shen, Z. Shu, and T. Huang, "Distributed prescribed-time interval bipartite consensus of multi-agent systems on directed graphs: Theory and experiment," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 1, pp. 613–624, Jan.–Mar. 2021.

[12] Y. Mao, Q. Shan, T. Li, S. Yang, and Q. Yi, "Adaptive containment control for unmanned surface vessels," in *Proc. IEEE Int. Conf. Secur., Pattern Anal., Cybern.*, 2021, pp. 99–104.

[13] Y. Cui, Y. Chen, D. Yang, Z. Shu, T. Huang, and X. Gong, "Resilient formation tracking of spacecraft swarm against actuation attacks: A distributed lyapunov-based model predictive approach," *IEEE Trans. Syst., Man, Cybern. Syst.*, 2023, doi: 10.1109/TSMC.2023.3292426.

[14] C. Wang and L. Guo, "Adaptive cooperative tracking control for a class of nonlinear time-varyingmulti-agent systems," *J. Franklin Inst.*, vol. 354, no. 15, pp. 6766–6782, 2017.

[15] Y. Yuan, Y. Wang, and L. Guo, "Sliding-mode-observer-based time-varying formation tracking for multispacecrafts subjected to switching topologies and time-delays," *IEEE Trans. Autom. Control*, vol. 66, no. 8, pp. 3848–3855, Aug. 2021.

[16] D. Mellinger and V. Kumar, "Minimum snap trajectory generation and control for quadrotors," in *Proc. IEEE Int. Conf. Robot. Automat.*, 2011, pp. 2520–2525.
[17] Z. Wang, X. Zhou, C. Xu, and F. Gao, "Geometrically constrained trajectory optimization for multicopters," *IEEE Trans. Robot.*, vol. 38, no. 5, pp. 3259–3278, Oct. 2022.
[18] X. Zhou, Z. Wang, X. Wen, J. Zhu, C. Xu, and F. Gao, "Decentralized spatial-temporal trajectory planning for multicopter swarms," 2021, arXiv:2106.12481.
[19] X. Zhou et al., "Swarm of micro flying robots in the wild," *Sci. Robot.*, vol. 7, no. 66, 2022, Art. no. eabm5954.
[20] Y. Cui, Y. Huang, M. Basin, and Z. Wu, "Geometric programming for nonlinear satellite buffer networks with time delays under L_1-gain performance," *IEEE/CAA J. Automatica*, 2023, doi: 10.1109/JAS.2023.123726.
[21] N. Dadkhah and B. Mettler, "Survey of motion planning literature in the presence of uncertainty: Considerations for UAV guidance," *J. Intell. Robotic Syst.*, vol. 65, no. 1, pp. 233–246, 2012.
[22] A. Sanjab, W. Saad, and T. Başar, "Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game," in *Proc. IEEE Int. Conf. Commun.*, 2017, pp. 1–6.
[23] A. Eldosouky, A. Ferdowsi, and W. Saad, "Drones in distress: A game-theoretic countermeasure for protecting UAVs against GPS spoofing," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2840–2854, Apr. 2020.
[24] G. Bianchin, Y.-C. Liu, and F. Pasqualetti, "Secure navigation of robots in adversarial environments," *IEEE Contr. Syst. Lett.*, vol. 4, no. 1, pp. 1–6, Jan. 2020.
[25] Y.-C. Liu, G. Bianchin, and F. Pasqualetti, "Secure trajectory planning against undetectable spoofing attacks," *Automatica*, vol. 112, 2020, Art. no. 108655.
[26] H. Xu, L. Wang, Y. Zhang, K. Qiu, and S. Shen, "Decentralized visual-inertial-UWB fusion for relative state estimation of aerial swarm," in *Proc. IEEE Int. Conf. Robot. Automat.*, 2020, pp. 8776–8782.
[27] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *J. Field Robot.*, vol. 31, no. 4, pp. 617–636, 2014.
[28] S. Zuo and D. Yue, "Resilient output formation containment of heterogeneous multigroup systems against unbounded attacks," *IEEE Trans. Cybern.*, vol. 52, no. 3, pp. 1902–1910, Mar. 2022.
[29] J. Wang, J. Gao, and P. Wu, "Attack-resilient event-triggered formation control of multi-agent systems under periodic DoS attacks using complex laplacian," *ISA Trans.*, vol. 128, pp. 10–16, 2022.
[30] W. He, X. Gao, W. Zhong, and F. Qian, "Secure impulsive synchronization control of multi-agent systems under deception attacks," *Inf. Sci.*, vol. 459, pp. 354–368, 2018.
[31] X. Li, Q. Zhou, P. Li, H. Li, and R. Lu, "Event-triggered consensus control for multi-agent systems against false data-injection attacks," *IEEE Trans. Cybern.*, vol. 50, no. 5, pp. 1856–1866, May 2020.
[32] X. Zhang, Q. Han, X. Ge, and L. Ding, "Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3616–3626, Aug. 2020.
[33] M. W. Mueller, M. Hehn, and R. D'Andrea, "A computationally efficient motion primitive for quadrocopter trajectory generation," *IEEE Trans. Robot.*, vol. 31, no. 6, pp. 1294–1310, Dec. 2015.
[34] F. Gao, W. Wu, J. Pan, B. Zhou, and S. Shen, "Optimal time allocation for quadrotor trajectory generation," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst.*, 2018, pp. 4715–4722.
[35] X. Gong, J. J. Liu, Y. Wang, and Y. Cui, "Distributed finite-time bipartite consensus of multi-agent systems on directed graphs: Theory and experiment in nano-quadcopters formation," *J. Franklin Inst.*, vol. 357, no. 16, pp. 11953–11973, 2020.
[36] D. He, G. Yang, H. Li, S. Chan, Y. Cheng, and N. Guizani, "An effective countermeasure against UAV swarm attack," *IEEE Netw.*, vol. 35, no. 1, pp. 380–385, Jan./Feb. 2021.

Xin Gong (Member, IEEE) received the B.Sc. degree from Wuhan University, Wuhan, China, in 2015 and the M.Sc. degree from Shanghai Jiaotong University, Shanghai, China, in 2018. He received the Ph.D. degree in control theory and engineering from the University of Hong Kong, Hong Kong, in 2022, In 2020, he was a Research Associate with the College of Aeronautics and Engineering, Kent State University, Kent, OH, USA. He is currently a Research Associate Professor with the School of Cyber Science and Engineering, Southeast University, Nanjing, China. His research interests include efficient and resilient control of multi-agent systems, distributed optimization, game theory, and their applications in UAV swarms.

Liqiang gong received the M.S. degree in mechanical engineering from Shenzhen University, Shenzhen, China, in 2023. he joined Nanjing 6902 Technology Co., Ltd, Nanjing, China, as an algorithm Engineer of UAV flight control. His research interests include path planning and distributed control of UAV swarms.

Tingwen Huang (Fellow, IEEE) received the B.S. degree in mathematics from Southwest Normal University (now Southwest University), Chongqing, China, 1990, the M.S. degree in applied mathematics from Sichuan University, Chengdu, China, in 1993, and the Ph.D. degree in applied mathematics from Texas A&M University, College Station, TX, USA, in 2002. where he was a Visiting Assistant Professor. He was with Texas A&M University, Qatar (TAMUQ), Ar-Rayyan, Qatar, as an Assistant Professor in August 2003, then he was promoted to Professor in 2013. His research research interests include computational intelligence, smart grid, dynamical systems, optimization, and control.

Yukang Cui (Member, IEEE) received the B.Eng. degree in automation from the Harbin Institute of Technology, Harbin, China, in 2012 and the Ph.D. degree in mechanical engineering from the University of Hong Kong, Pokfulam, Hong Kong, in 2017. In 2017, he was a Research Associate with the Department of Mechanical Engineering, the University of Hong Kong. Since 2018, he has been with the College of Mechatronics and Control Engineering, Shenzhen University, Shenzhen, China, where he is currently an Associate Professor. His research interests include nonlinear time-delay systems, multi-agent systems, multi-robot cooperative sensing, and swarm-robot path planning.