Resilient Event-Triggered Formation Control and Secure Estimation of Multi-UAV Systems

Zhou Gu, *Senior Member, IEEE*, Tingting Yin, Qing Lu, and Ju H. Park, *Senior Member, IEEE*

***Abstract*—This article studies the event-triggered formation control of multiple unmanned aerial vehicles (UAVs) in the presence of deception attacks. Unlike existing research focusing on deception attacks, the secure upper bound of deception attacks that the formation tracking of UAVs can tolerate is estimated to reduce the conservatism associated with the predefined upper bound of deception attacks. A dynamic event-triggered mechanism is developed by considering triggering and tracking errors to reduce data release rates while maintaining desired formation tracking performance. Leveraging information from neighboring UAVs, tracking control strategies for the multi-UAV system facing deception attacks are designed using the Lyapunov stability theory. Simulation analysis validates the effectiveness of the proposed strategies, demonstrating improved resilience in the presence of deception attacks.**

***Index Terms*—Dynamic event-triggered mechanism (DETM), formation tracking control, deception attacks, unmanned aerial vehicles (UAVs).**

I. Introduction

FORMATION control of multiple unmanned aerial vehicles (UAVs) has received significant attention in civilian and military fields due to their diverse applications, including but not limited to forest fire monitoring, film and television shooting, target search and localization, and reconnaissance and combat [1], [2], [3]. Specifically in military applications, multi-UAVs are inevitably vulnerable to malicious attacks launched by adversaries when executing high-risk tasks. Consequently, the effective control of multi-UAV systems under malicious attacks stands as a critical research challenge [4].

Numerous studies have focused on formation control analysis for multi-UAV systems, considering factors, such as stochastic noises, communication delays, and limited data rates. Among the various control frameworks, the leader-follower-based approach has been extensively studied and implemented in UAV formation control, as evidenced by the research efforts in [5], [6], and [7]. Attaining longitudinal static stability and robust formation control for heterogeneous UAVs using the nonlinear observer-based method was discussed in [8]. Significant work on formation tracking control using estimated states for unknown leader velocity has been conducted, such as in [3] and [9]. Despite these efforts, the existing research predominantly focuses on achieving time-invariant formations, limiting real-world applicability, such as obstacle avoidance. This article, therefore, emphasizes the leader-following time-varying formation tracking control of multiple UAVs.

The time-triggered communication mechanism is a prevalent assumption in most of the literature above. However, the event-triggered mechanism (ETM) for the formation tracking controllers is more productive in saving the communication bandwidth. The adoption of ETM is driven by the "necessity" to the formation tracking performance, communication and computation resources, and battery life by reducing data transmission frequency, thus rendering it more suitable for multi-UAV systems [10]. Consequently, event-based formation control has garnered significant attention in recent years [11], [12], [13], [14], [15]. Several types of ETMs, such as dynamic event-triggered mechanism (DETM), memory-ETM, and segment-weighted information-based ETM, have been explored in [16] and [17]. Under the DETM, the triggering threshold is modulated with triggering and tracking errors, thereby optimizing communication network resources more effectively, as evidenced by works in [18] and [19]. However, the corresponding results for DETM in multi-UAV formation control still need to be improved. With the increasing application of UAVs, designing an appropriate dynamic event-triggered scheme is significant and necessary further to save the UAV communication network's limited resources.

The wireless communication network is crucial in a multi-UAV system, as information interaction among neighboring UAVs relies on the network. The communication network may introduce time delay, packet loss [20], and disorder [21], and is

Received 18 June 2024; revised 12 September 2024 and 21 January 2025; accepted 16 February 2025. Date of publication 19 March 2025; date of current version 23 May 2025. This work was supported in part by the Scholarship from China Scholarship Council, in part by the National Natural Science Foundation of China under Grant 62273183 and Grant 62103193, in part by the Natural Science Foundation of Jiangsu Province, China, under Grant BK20231288, in part by the Startup Funding of Anhui Polytechnic University under Grant 2024YQQ001, and in part by the National Research Foundation of Korea (NRF), the Korea Government (Ministry of Science and Information and Communications Technology), under Grant RS-2023-00208078. Paper no. TII-24-3044. *(Corresponding authors: Zhou Gu; Ju H. Park.)*

Zhou Gu is with the School of Electrical Engineering, Anhui Polytechnic University, Wuhu 241000, China (e-mail: gzh1808@163.com).

Tingting Yin is with the School of Electrical Engineering, Anhui Polytechnic University, Wuhu 241000, China, and also with the Department of Electrical Engineering, Yeungnam University, Gyeongsan 38541, South Korea (e-mail: yttangle@163.com).

Qing Lu is with the College of Mechanical & Electronic Engineering, Nanjing Forestry University, Nanjing 210037, China (e-mail: qinglu2013@163.com).

Ju H. Park is with the Department of Electrical Engineering, Yeungnam University, Gyeongsan 38541, South Korea (e-mail: jessie@ynu.ac.kr).

Digital Object Identifier 10.1109/TII.2025.3547012

vulnerable to cyber-attacks [22]. It is evident that the system's performance may deteriorate or even lead to paralysis when the communication network of the control system is under attack. Numerous recent research has focused on developing strategies to mitigate cyber-attacks, as evidenced by works, such as [23], [24], and[25]. For instance, event-based output feedback control against deception attacks for networked systems was developed in [26], where a Bernoulli stochastic variable was introduced to describe the presence of deception attacks with predetermined upper bounds. However, in the case of an unknown system, the upper bound of the system against deception attacks needs to be estimated rather than being a preassigned parameter. Similar to the seismic rating of a building, estimating the upper bound of the system against deception attacks becomes necessary. Consequently, our study aims to analyze and model deception attacks in multi-UAV systems while estimating the upper bounds of cyber-attacks. This estimation will be used to mitigate the effects of cyber-attacks on the multi-UAV system. This is one of the primary motivations of this study.

Inspired by the discussions above, this study concentrates on designing event-based formation tracking control for multi-UAV systems under deception attacks. The key contributions of our research are as follows.

1) A novel deception attack model that targets the multi-UAV system is established. Unlike most of the conventional approaches seen in most existing works on deception attacks, where the upper bound of the attack is preassigned, as in [19] and [24], this study presents an estimation of deception attacks. This estimation allows for mitigating the adverse effects on the multi-UAV system.
2) A new adaptive law of threshold is devised for the DETM. Different from existing communication mechanisms [12] adhering to constant thresholds, the proposed approach incorporates a variable triggering rule, whose adaptability is determined by both triggering errors and tracking errors. This dynamic adjustment strategy contributes to a lower data release rate and less energy consumption.
3) A dynamic event-triggered formation tracking strategy is put forward for multi-UAV systems in the presence of deception attacks, ensuring that every UAV reaches its desired position and completes this formation.

Such a control strategy has the potential to reduce controller update frequency without compromising the tracking performance of UAVs.

The rest of this article is organized as follows. Section II presents the preliminaries and the model of dynamic event-triggered formation control for multi-UAV systems under deception attacks. Section III provides the stability analysis and the control synthesis condition. Section IV illustrates the effectiveness of our proposed strategy through a simulation example. Finally, Section V concludes this article.

II. Preliminaries and Problem Formulation

A. Preliminaries

The communication topology among all UAVs in a system could be described as a directed graph $\mathbb{F} = (\mathbb{V}, \mathbb{B}, \mathbb{C})$, in which $\mathbb{B} \subseteq \{(i,j), i,j \in \mathbb{V}\}$ and $\mathbb{V} \in \{1, 2, \ldots, N\}$ stand for the set of edges and nodes. Edge $(i,j) \in \mathbb{B}$ denotes that the jth UAV can gain data from the ith UAV. The adjacency matrix is denoted as $\mathbb{C} = [c_{ij}]_{N\times N}$, wherein $c_{ii} = 0$ and $c_{ij} = 1$ if $(j,i) \in \mathbb{B}$, and $c_{ij} = 0$, otherwise. The Laplacian matrix is defined as $\mathcal{L} = [\mathfrak{L}_{ij}]_{N\times N}$ with $\mathfrak{L}_{ii} = \sum_{j=1, j\neq i}^{N} c_{ij}$, $\mathfrak{L}_{ij} = -c_{ij}$ for $i \neq j$. Let $\mathbb{A}_i = \{j | (i,j) \in \mathbb{B}\}$ for the ith UAV, which is a set involving all its neighbors.

In a leader-following configuration, the follower UAVs are represented as $1, 2, \ldots, N$, and the leader is labeled by an extra node 0. These data of the leader could be acquired by the ith follower UAV, which is described as $b_i = 1$; otherwise, $b_i = 0$. Denote $\mathcal{B} = \text{diag}\{b_1, \ldots, b_N\}$. Besides, there exists a directed spanning tree in topology graph $\mathbb{F}$ with UAV 0 as the root node.

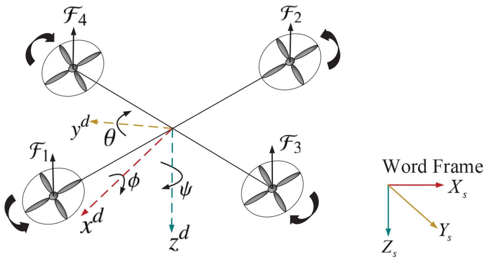


Fig. 1. Quadrotor configuration frame system.

B. Modeling of a Multi-UAV System

The structure of a quadrotor UAV, including four rotors and one rigid cross frame, is illustrated in Fig. 1. The relationship between the four inputs (the lifts $\mathcal{F}_q$, $q \in \{1, 2, 3, 4\}$ produced by four motors) and six output variables [position coordinates (x, y, and z), pitch θ, roll ϕ, and yaw ψ] is elaborated in [6]. The control scheme of the quadrotor UAV is composed of inner loop and outer loop controls [6]. This research concentrates on the formation tracking control (outer loop control) of multiple quadrotor UAVs.

Let us consider a multi-UAV system comprising one leader and N followers, with their dynamic equations described as

$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t) \tag{1}$$

where $x_i^T(t) = [\zeta_i^T(t) \;\; v_i^T(t)]$, $i = 0, 1, 2, \ldots, N$, in which $\zeta_i(t) \in \mathbb{R}^q$ and $v_i(t) = \zeta_i(t)$ stand for the position and the velocity of the ith UAV, respectively; $u_i(t)$ denotes the input of the controller; $A = \begin{bmatrix} 0 & I_3 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 \\ I_3 \end{bmatrix}$.

Remark 1: In this study, we mainly focus on the kinematic model of multi-UAV systems, which involves position $\zeta_i(t)$ and velocity $v_i(t)$, whereas the dynamic model, which studies the attitude of UAVs (describing changes in pitch, roll, and yaw), can be seen in [1].

The time-varying formation for the followers is described by $f(t) = [f_1^T(t), f_2^T(t), \ldots, f_N^T(t)]^T$ with $f_i(t) = [f_{\zeta i}^T(t), f_{vi}^T(t)]^T$ and $f_{vi}(t) = \dot{f}_{\zeta i}(t)$. For the ith follower ($i \in \{1, 2, \ldots, N\} \triangleq \Gamma$), $f_{\zeta i}(t)$ ($f_{vi}(t)$) represents its relative position (velocity). Denote $\Psi_i(t) = f_i(t) + x_0(t)$ as its desired state, where $\Psi_i(t) = \left[\Psi_{\zeta i}^T(t), \Psi_{vi}^T(t)\right]^T$. The tracking error is represented as $\bar{x}_i(t) = x_i(t) - \Psi_i(t)$.

C. Deception Attacks

The data transmission among neighboring UAVs is via the communication network. The vulnerability of the communication network gives rise to various security threats, such as deception attacks. In the absence of deception attacks, the relative information received by the ith UAV could be stated as

$$\xi_i(t) = \sum_{j \in \mathbb{A}_i} \xi_{ij}(t) \tag{2}$$

where $\xi_{ij}(t) = c_{ij}[x_i(t) - f_i(t) - (x_j(t) - f_j(t))]$.

Given the presence of potential deception attacks launched by malicious adversaries, the actual relative information received by the ith UAV is rewritten as

$$\xi_i(t) = \sum_{j \in \mathbb{A}_i} [\xi_{ij}(t) + \mu_{ij}(t)\xi_{ij}(t)] \tag{3}$$

where $\mu_{ij}(t)$ $(i, j \in \Gamma, i \neq j)$ is composed by unknown time-varying continuous functions to undermine the formation tracking performance.

For real constant $\bar{\mu} > 0$, $\mu_{ij}(t)$ satisfies

$$-\bar{\mu} \leq \mu_{ij}(t) \leq \bar{\mu}. \tag{4}$$

Remark 2: From (3), it is evident that $\mu_{ij}(t) \neq 0$ implies the occurrence of deception attacks. In such a scenario, the relative signal acquired by the ith UAV is paraded in (3). On the other hand, $\mu_{ij}(t) = 0$ signifies the absence of any deception attacks, enabling each UAV to receive the actual relative states, as described in (2).

Define a Laplacian matrix as $\mathcal{W} = [w_{ij}]_{N\times N}$, wherein $w_{ii} = \sum_{j=1, j\neq i}^{N} \tilde{c}_{ij}$ with $\tilde{c}_{ij} = c_{ij}\mu_{ij}(t) = -w_{ij}$.

The following lemma is essential to obtain the main results.

Lemma 1: Under the inequalities in (4), for a given directed graph $\mathbb{F}$, the following inequality is satisfied:

$$\|\mathcal{W}\| \leq \bar{\mu}\gamma \tag{5}$$

where $\gamma = (\sup_{i=1}^{N} \sup_{j=1}^{N} |\mathfrak{L}_{ij}|^2)^{\frac{1}{2}}$ is a constant for the graph $\mathbb{F}$.

Proof: Recollect the matrix $\mathcal{W}$ in the form

$$\mathcal{W} = \begin{bmatrix} w_{11} & \cdots & w_{1N} \\ \vdots & \vdots & \vdots \\ w_{N1} & \cdots & w_{NN} \end{bmatrix}.$$

On the basis of the definition of $\mathcal{L}$, it is easy to obtain that

$$\|\mathcal{W}\| = \left(\sum_{i=1}^{N}\sum_{j=1}^{N} w_{ij}^2\right)^{\frac{1}{2}} \leq \bar{\mu}\left(\sum_{i=1}^{N}\sum_{j=1}^{N} \mathfrak{L}_{ij}^2\right)^{\frac{1}{2}} \leq \bar{\mu}\gamma. \tag{6}$$

That ends the proof.■

D. Design of the DETM

In this research, the DETM is employed to update control input signals, achieving the purpose of minimizing redundant transmission data. The threshold of the designed mechanism is adaptable and relies on tracking and triggering errors. For a clear description of the DETM, we define the triggering instants of the ith UAV as $0 \leq t_0^i < t_1^i < \cdots < t_\delta^i < t_{\delta+1}^i < \cdots$. The event generator functions $\Pi_i(\cdot,\cdot) : \mathbb{R}^q \times \mathbb{R} \to \mathbb{R}$ $(i \in \Gamma)$ are chosen as follows:

$$\Pi_i(\varphi_i(t), \bar{x}_i(t_\delta^i)) = \varphi_i^T(t)W_i\varphi_i(t) - \varsigma_i(t)\bar{x}_i^T(t_\delta^i)W_i\bar{x}_i(t_\delta^i) \tag{7}$$

where the triggering error $\varphi_i(t) = \bar{x}_i(t_\delta^i) - \bar{x}_i(t)$, $t \in [t_\delta^i, t_{\delta+1}^i)$; matrix $W_i > 0$ will be determined via Algorithm 1; the threshold $\varsigma_i(t) = \phi_i e^{-\alpha_i\|\bar{x}_i(t) - \bar{x}_i(t_\delta^i)\|} + \beta_i$ with constants $\alpha_i \geq 0$, $\phi_i > 0$, and $\beta_i \geq 0$, and they satisfy $\phi_i + \beta_i \in [0, 1]$, which yields that $\varsigma_i(t) \in [0, \phi_i + \beta_i] \in [0, 1]$. It is assumed that the leader UAV does not employ such a communication mechanism in this research.

Then, the next triggering instant is developed as

$$t_{\delta+1}^i = \inf_{t > t_\delta^i} \{t | \Pi_i(\varphi_i(t), \bar{x}_i(t_\delta^i)) > 0\}. \tag{8}$$

Moreover, the triggered signal is

$$\bar{x}_i(t_\delta^i) = \bar{x}_i(t) + \varphi_i(t). \tag{9}$$

Remark 3: The threshold $\varsigma_i(t)$ of the DETM in (8) relies on the dynamic error between the current input data $\bar{x}_i(t)$ and the latest released data $\bar{x}_i(t_\delta^i)$. As the error converges to 0, signifying the asymptotic stability of the UAV system upon completion of the formation task, the threshold $\varsigma_i(t)$ remains constant. Consequently, the threshold remains modulated based on the dynamic error until it reaches zero.

Remark 4: In the DETM (8), setting $\alpha_i = 0$ and $\beta_i \neq 0$ reduces to the case, as described in [12], while setting $\alpha_i = 0$ and $\beta_i = 0$ will turn to the general time-triggered scheme.

Remark 5: Some novel ETMs, such as those in [13] and [17], have been investigated in previous studies. In this study, the DETM is employed as the primary focus is on estimating the secure upper bound for deception attacks in formation tracking.

E. Formation Control Strategies

This research proposes a formation control strategy for the system (1) to achieve the desired formation. Thanks to the DETM, the control input $u_i(t) = u_i(t_\delta^i)$ for $t \in [t_\delta^i, t_{\delta+1}^i)$, $i \in \Gamma$. Moreover, the dynamic event-based formation control strategies are designed as

$$\begin{aligned} u_i(t) = {} & b_iK_1\bar{x}_i(t_\delta^i) + \dot{\Psi}_{vi}(t) \\ & + K_2 \sum_{j \in \mathbb{A}_i} (c_{ij} + \tilde{c}_{ij})[\bar{x}_i(t_\delta^i) - \bar{x}_j(t_{\delta'}^j)] \end{aligned} \tag{10}$$

where K_1 and K_2 are controller gains to be determined; $\dot{\Psi}_{vi}(t)$ is the desired acceleration; $\bar{x}_j(t_{\delta'}^j)$ represents the latest delivered measurements from the jth UAV; $\delta' \triangleq \operatorname{argmin}_{\delta'}\{t - t_{\delta'}^j | t > t_{\delta'}^j, \delta' = 0, 1, 2, 3, \cdots\}$.

Invoking (10) into (1) yields the following tracking error system:

$$\begin{aligned}\dot{\bar{x}}_i(t) &= (A + BK_1 b_i)\bar{x}_i(t)\\ &\quad + BK_2 \sum_{j\in\mathbb{A}_i} (c_{ij} + \tilde{c}_{ij})[\bar{x}_i(t^i_\delta) - \bar{x}_j(t^j_{\delta'})].\end{aligned} \tag{11}$$

Combining (9) and (11) and using the Kronecker product follow the closed-loop formation tracking system:

$$\begin{aligned}\dot{\bar{x}}(t) &= (\tilde{A} + \tilde{\mathcal{B}}\tilde{B}\tilde{K}_1)\bar{x}(t) + \tilde{\mathcal{L}}\tilde{B}\tilde{K}_2[\bar{x}(t) + \varphi(t)]\\ &\quad + \tilde{\mathcal{R}}\tilde{B}\tilde{K}_2[\bar{x}(t) + \varphi(t)]\end{aligned} \tag{12}$$

where $\tilde{A} = I_N \otimes A$, $\tilde{B} = I_N \otimes B$, $\tilde{K}_\iota = I_N \otimes K_\iota$, $\iota = 1, 2$, $\tilde{\mathcal{L}} = \mathcal{L} \otimes I_6$, $\tilde{\mathcal{B}} = \mathcal{B} \otimes I_6$, $\tilde{\mathcal{R}} = \mathcal{R} \otimes I_6$, $\bar{x}(t) = \text{col}_N\{\bar{x}_i(t)\}$, and $\varphi(t) = \text{col}_N\{\varphi_i(t)\}$. Here, col ${}_N\{\cdot\}$ stands for N-columns vector; $\text{col}^i_N\{\cdot\}$ indicates N-columns vector with only the i th nonzero column. I_N represents the $(N \times N)$-dimensional identity matrix, and it is abbreviated as I occasionally.

III. Main Results

In this section, the stability of event-triggered formation control for multi-UAV systems under deception attacks will be analyzed first.

Theorem 1: For known controller gains K_1 and K_2, system (12) is asymptotically stable if there exists positive definite matrix $\tilde{P}$ such that the following inequality holds:

$$\Theta = \begin{bmatrix} \Theta_{11} & * \\ \tilde{K}_1^T\tilde{B}^T\tilde{\mathcal{B}}^T\tilde{P} + \tilde{K}_2^T\tilde{B}^T\tilde{\mathcal{L}}^T\tilde{P} & -W \end{bmatrix} \leq -I. \tag{13}$$

Moreover, the upper bound of the attack signal is estimated by

$$|\mu_{ij}(t)| \leq \bar{\mu} = \frac{1}{2\gamma\|P\|\|B\|\|K_2\|\|H_3\|} \tag{14}$$

for $i \in \Gamma$ and $j \in \mathbb{A}_i$, where

$$\begin{aligned}\Theta_{11} &= \text{sym}\{\tilde{P}\tilde{\mathcal{B}}\tilde{B}\tilde{K}_1 + \tilde{P}\tilde{A} + \tilde{P}\tilde{\mathcal{L}}\tilde{B}\tilde{K}_2\} + (\phi + \beta)W\\ \phi &= \phi_0 \otimes I_6, \phi_0 = \text{diag}\{\phi_1, \phi_2, \ldots, \phi_N\}\\ \beta &= \beta_0 \otimes I_6, \beta_0 = \text{diag}\{\beta_1, \beta_2, \ldots, \beta_N\}\\ W &= \text{diag}\{W_1, W_2, \ldots, W_N\}.\end{aligned}$$

Proof: The proof comprises two parts: The stability of the discussed system is analyzed in Step A, and the exclusion of Zeno phenomenon in the DETM is outlined in Step B.

Step A: The time-varying Lyapunov function candidate in the following form is selected for system (12):

$$V(t) = \bar{x}^T(t)\tilde{P}\bar{x}(t) \tag{15}$$

with $\tilde{P} = I_N \otimes P$.

By calculating the derivation of (15), one can get

$$\begin{aligned}\dot{V}(t) &= 2\bar{x}^T(t)\tilde{P}\dot{\bar{x}}(t)\\ &= 2\bar{x}^T(t)\tilde{P}(\tilde{A} + \tilde{\mathcal{B}}\tilde{B}\tilde{K}_1)\bar{x}(t)\\ &\quad + 2\bar{x}^T(t)\tilde{P}(\tilde{\mathcal{B}}\tilde{B}\tilde{K}_1 + \tilde{\mathcal{L}}\tilde{B}\tilde{K}_2)\varphi(t)\\ &\quad + 2\bar{x}^T(t)\tilde{P}\tilde{\mathcal{R}}\tilde{B}\tilde{K}_2[\bar{x}(t) + \varphi(t)]\\ &\leq 2\bar{x}^T(t)\tilde{P}(\tilde{A} + \tilde{\mathcal{B}}\tilde{B}\tilde{K}_1 + \tilde{\mathcal{L}}\tilde{B}\tilde{K}_2)\bar{x}(t)\\ &\quad + 2\bar{x}^T(t)\tilde{P}(\tilde{\mathcal{B}}\tilde{B}\tilde{K}_1 + \tilde{\mathcal{L}}\tilde{B}\tilde{K}_2)\varphi(t)\\ &\quad + 2\bar{\mu}\gamma\bar{x}^T(t)\tilde{P}\tilde{B}\tilde{K}_2[\bar{x}(t) + \varphi(t)].\end{aligned} \tag{16}$$

Based on (8), we have

$$(\phi + \beta)\bar{x}^T(t)W\bar{x}(t) - \varphi^T(t)W\varphi(t) < 0. \tag{17}$$

Combining (16) and (17) and leveraging Schur complement follow that:

$$\dot{V}(t) \leq \chi^T(t)\Theta\chi(t) - 2\bar{\mu}\gamma\|P\|\|B\|\|K_2\|[\bar{x}(t) + \varphi(t)] \tag{18}$$

where $\chi(t) = [\bar{x}^T(t), \varphi^T(t)]^T$.

Employing Lemma 1 and (13), one has

$$\dot{V}(t) \leq\ - (1 - 2\bar{\mu}\gamma\|P\|\|B\|\|K_2\|\|H_3\|)\chi^T(t)\chi(t)$$

where $H_3 = H_1^T H_1 + H_1^T H_2$, $H_1 = [I\ 0]$, and $H_2 = [0\ I]$.

It follows from (14) that

$$\dot{V}(t) \leq -\chi^T(t)\chi(t). \tag{19}$$

Furthermore, one can get $x_i(t) \to f_i(t) + x_0(t)$ as $t \to +\infty$, which means that all the UAVs can achieve the desired formation.

Step B: The avoidance of the Zeno behavior will be discussed in the following.

Denote $\varrho = \arg\max_i \parallel \varphi_i(t) \parallel (i \in \Gamma)$. Then, one can get $\parallel \varphi_i(t) \parallel \leq \parallel \varphi(t) \parallel$. Moreover, we have $\parallel \varphi_\varrho(t) \parallel / \parallel \bar{x}_\varrho(t) \parallel \leq (\sqrt{N} \parallel \varphi(t) \parallel)/\parallel \bar{x}(t) \parallel$. ε_ϱ signifies the time interval for $\parallel \varphi_\varrho(t) \parallel / \parallel \bar{x}_\varrho(t) \parallel$ increasing from zero to $(\phi_i + \beta_i)$, and ε^* is the time interval from zero to $(\sqrt{N} \parallel \varphi(t) \parallel)/\parallel \bar{x}(t) \parallel$. Calculating the time derivative of $\parallel \varphi(t) \parallel/\parallel \bar{x}(t) \parallel$ yields that

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}t}\frac{\parallel \varphi(t) \parallel}{\parallel \bar{x}(t) \parallel} &= -\frac{\varphi^T(t)\dot{\bar{x}}(t)}{\parallel \varphi(t) \parallel\parallel \bar{x}(t) \parallel} - \frac{\varphi(t)\bar{x}^T(t)\dot{\bar{x}}(t)}{\parallel \bar{x}(t) \parallel^2\parallel \bar{x}(t) \parallel}\\ &\leq \left(1 + \frac{\parallel \varphi(t) \parallel}{\parallel \bar{x}(t) \parallel}\right)\\ &\quad \times \left(\parallel \Phi_1 \parallel + \parallel \Phi_2 \parallel \frac{\parallel \varphi(t) \parallel}{\parallel \bar{x}(t) \parallel} + \tau_{\text{sup}}\right)\end{aligned} \tag{20}$$

where $\Phi_1 = \tilde{A} + \tilde{\mathcal{B}}\tilde{B}\tilde{K}_1 + \tilde{\mathcal{L}}\tilde{B}\tilde{K}_2 + \tilde{\mathcal{R}}\tilde{B}\tilde{K}_2$, $\Phi_2 = \tilde{\mathcal{L}}\tilde{B}\tilde{K}_2 + \tilde{\mathcal{R}}\tilde{B}\tilde{K}_2$, and $\tau_{\text{sup}} = \sup\{\frac{\|(\tilde{\mathcal{L}}\tilde{B}\tilde{K}_2 + \tilde{\mathcal{R}}\tilde{B}\tilde{K}_2)\varphi(t)\|}{\|\bar{x}(t)\|}\}$ $(\parallel \bar{x}(t) \parallel \neq 0)$.

Let $\kappa = \parallel \varphi(t) \parallel/\parallel \bar{x}(t) \parallel$, then (20) can be rewritten as $\dot{\kappa} \leq (1 + \kappa)(\parallel \Phi_1 \parallel + \parallel \Phi_2 \parallel \kappa + \tau_{\text{sup}})$. Assume that $\dot{\sigma} = (1 + \sigma)(\parallel \Phi_1 \parallel + \parallel \Phi_2 \parallel \sigma + \tau_{\text{sup}})$ has a solution $\sigma(t, \sigma_0)$ with $\sigma(0, \sigma_0) = \sigma_0$. As a result, one has $\kappa \leq \sigma(t, \sigma_0)$. Suppose that the system begins at the first triggered, we can get $\sigma_0 = 0$. Then, the smallest time interval could be derived through calculating the time of the following equality: $\frac{\mathrm{d}\sigma}{(1+\sigma)(\|\Phi_1\|+\|\Phi_2\|\sigma+\tau_{\text{sup}})} = \mathrm{d}t$. Denoting ε as the solution of the equality yields that

$$\begin{aligned}\varepsilon &= \frac{1}{\parallel \Phi_1 \parallel + \parallel \Phi_2 \parallel \sigma + \tau_{\text{sup}}}\\ &\quad \times \ln\left[\frac{(\parallel \Phi_1 \parallel + \tau_{\text{sup}})\sigma(t, 0) + \parallel \Phi_1 \parallel + \tau_{\text{sup}}}{\parallel \Phi_2 \parallel \sigma(t, 0) + \parallel \Phi_1 \parallel + \tau_{\text{sup}}}\right].\end{aligned} \tag{21}$$

Algorithm 1: Controller Gains and the Estimation of Upper Bound of Deception Attack.

```
Input: the communication topology information $\mathcal{L}, \mathcal{B}$, the
       initial value of attack $\bar{\mu}_0$, triggering parameters
       $\phi_i, \alpha_i, \beta_i, i \in \Gamma$
Output: controller gains $K_\iota$, triggering matrices $W_i$, and
        the upper bound of deception attacks $\bar{\mu}$
Combining (16), (17) and applying Schur complement
follow that (23). Defining $Y_\iota = PBK_\iota$, $\tilde{Y}_\iota = I_N \otimes Y_\iota$
($\iota = 1, 2$) yields (24).
initialization: $\bar{\mu}_0$, $\phi_i, \alpha_i, \beta_i, i \in \Gamma$
while $\bar{\mu} \neq \bar{\mu}_0$ do
    $\bar{\mu}_0 \leftarrow \bar{\mu}$
    obtain $P$ and $Y_\iota$ by solving (24)
    obtain $K_\iota$ by calculating $K_\iota = B^T P^{-1} Y_\iota$
    then obtain $\bar{\mu}$ accodding to (14)
end
return $K_\iota (\iota = 1, 2)$, $W_i$ $(i \in \Gamma)$, and $\bar{\mu}$
```

Letting $\sigma(t^*, 0) = \sqrt{\sum_{i=1}^{N} \phi_i / N}$ follows that

$$\varepsilon^* = \frac{1}{\| \Phi_1 \| + \| \Phi_2 \| \sigma + \tau_{\text{sup}}} \times \ln \left[\frac{(\| \Phi_1 \| + \tau_{\text{sup}}) \sigma(t^*, 0) + \| \Phi_1 \| + \tau_{\text{sup}}}{\| \Phi_2 \| \sigma(t^*, 0) + \| \Phi_1 \| + \tau_{\text{sup}}} \right]. \quad (22)$$

Based on the above analysis, it can be deduced that $0 < \varepsilon^* \leq \varepsilon_\varrho$, indicating the avoidance of Zeno behavior of the proposed DETM. This ends the proof.■

Remark 6: $\bar{\mu}$ in (4) denotes the estimated upper bound for deception attacks. Unlike most existing research, such as in [19] and [24], the upper bound is assumed to be satisfied a Lipschitz condition with a given upper bounded. As seen in (14), the upper bound can be estimated and incorporated into the formation control design, playing a critical role in secure formation tracking. While Theorem 1 provides a sufficient condition to ensure secure formation tracking, more precise estimates of the secure upper bound will be explored in future work.

Following the outcomes in Theorem 1, Algorithm 1 presents the process of obtaining the controller gains, triggering matrices, and estimating the upper bound of deception attacks.

The matrices mentioned in Algorithm 1 are presented as follows:

$$\tilde{\Theta} = \begin{bmatrix} \tilde{\Theta}_{11} & * \\ \tilde{\Theta}_{21} & -W \end{bmatrix} \quad (23)$$

$$\bar{\Theta} = \begin{bmatrix} \bar{\Theta}_{11} & * \\ \tilde{Y}_1^T \tilde{\mathcal{B}}^T + \tilde{Y}_2^T \tilde{\mathcal{L}}^T + \bar{\mu}\gamma \tilde{Y}_2^T & -W \end{bmatrix} < 0 \quad (24)$$

where

$$\tilde{\Theta}_{11} = \text{sym}\{\tilde{P}\tilde{\mathcal{B}}\tilde{B}\tilde{K}_1 + \tilde{P}\tilde{A} + \tilde{P}\tilde{\mathcal{L}}\tilde{B}\tilde{K}_2 + \bar{\mu}\gamma\tilde{P}\tilde{B}\tilde{K}_2\} + (\phi + \beta)W$$

$$\tilde{\Theta}_{21} = \tilde{K}_1^T \tilde{B}^T \tilde{\mathcal{B}}^T \tilde{P} + \tilde{K}_2^T \tilde{B}^T \tilde{\mathcal{L}}^T \tilde{P} + \bar{\mu}\gamma \tilde{K}_2^T \tilde{B}^T \tilde{P}$$

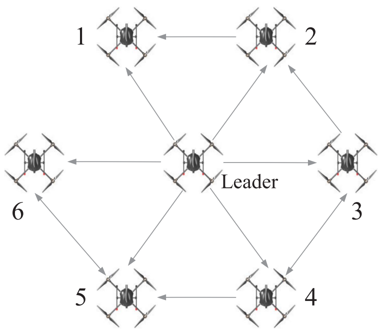


Fig. 2. Topology graph.

$$\bar{\Theta}_{11} = \text{sym}\{\tilde{P}\tilde{A} + \tilde{\mathcal{B}}\tilde{Y}_1 + \tilde{\mathcal{L}}\tilde{Y}_2 + \bar{\mu}\gamma\tilde{Y}_2\} + (\phi + \beta)W.$$

IV. Example

This section provides a multi-UAV system comprising follower UAVs 1–6 and a single leader. The topology graph describing the data communication among these UAVs is displayed in Fig. 2, from which one knows that $\mathcal{B} = I_6$ and

$$\mathcal{L} = \begin{bmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & -1 & 1 \end{bmatrix}.$$

Remark 7: Fig. 2 presents one type of communication topology of the multi-UAV system, where there exists a directed spanning tree with the leader UAV as the root node. In such a situation, controller gains, triggering matrices, and the estimated upper bound of deception attacks are obtained by employing Algorithm 1 with appropriate parameter values in MATLAB. Other topologies satisfying this condition could be discussed and simulated similarly.

Six UAVs are configured to maintain a time-varying hexagonal formation on the XOY plane, revolving around the leading UAV with the trajectory $[-2\cos(0.2t), 2t, 3t]^T$. The state $x_i(t)$ and control input $u_i(t)$ for the ith UAV are represented as $x_i(t) = [\zeta_{iX}(t), \zeta_{iY}(t), \zeta_{iZ}(t), v_{iX}(t), v_{iY}(t), v_{iZ}(t)]^T$ and $u_i(t) = [u_{iX}(t), u_{iY}(t), u_{iZ}(t)]^T$ $(i \in \{1, 2, 3, 4, 5, 6\} \triangleq \Gamma_6)$. The time-varying formation is specified by

$$f_{\zeta i}(t) = \begin{bmatrix} 3\cos(0.8t + \frac{\pi}{3}(i-1)) \\ 3\sin(0.8t + \frac{\pi}{3}(i-1)) \\ 0 \end{bmatrix}.$$

Let $\phi_1 = 0.01$, $\phi_2 = 0.012$, $\phi_3 = 0.013$, $\phi_4 = 0.008$, $\phi_5 = 0.011$, $\phi_6 = 0.015$, $\alpha_1 = 0.2$, $\alpha_2 = 0.3$, $\alpha_3 = 0.1$, $\alpha_4 = 0.25$, $\alpha_5 = 0.4, \alpha_6 = 0.15, \beta_1 = 0.01, \beta_2 = 0.012, \beta_3 = 0.013, \beta_4 = 0.008$, $\beta_5 = 0.011$, and $\beta_6 = 0.015$. Using Algorithm 1, we can get the following parameters:

$$K_l = K_{l0} \otimes I_3, l \in \{1, 2\}$$

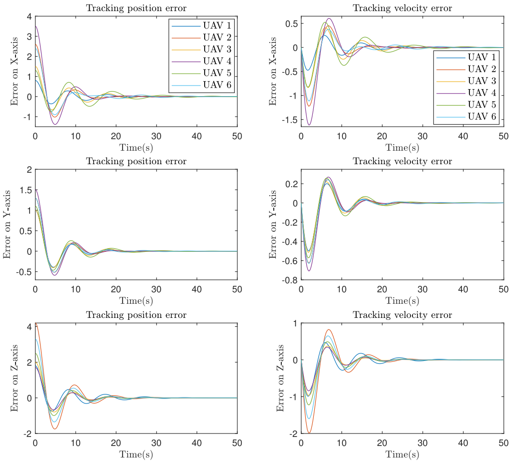


Fig. 3. Tracking position/velocity errors of six UAVs.

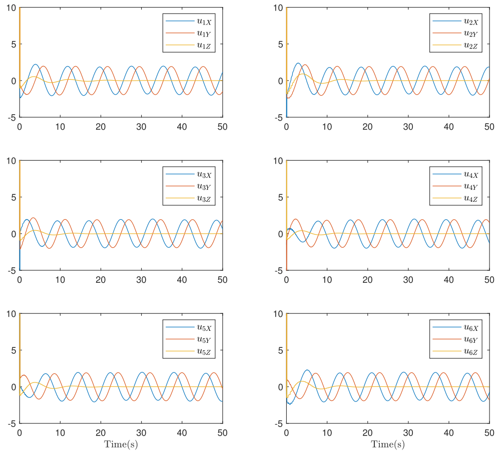


Fig. 5. Control inputs of six UAVs.

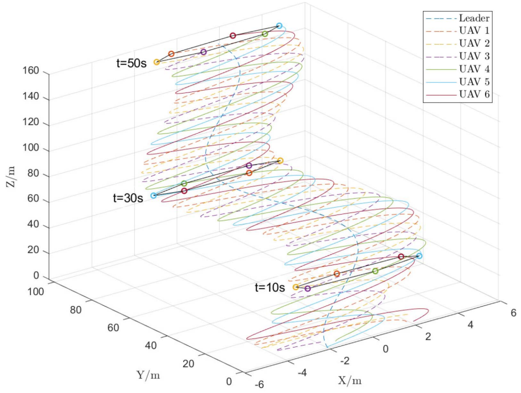


Fig. 4. Tracking trajectories of UAVs 1–6 and the leader with position snapshots at $t = 10$, 30, and 50 s.

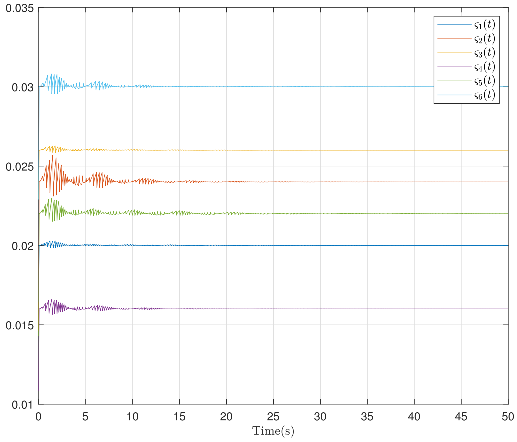


Fig. 6. Thresholds $\varsigma_i(t)$ $(i \in \Gamma_6)$ of the DETM.

$$K_{10} = \begin{bmatrix} -0.4768 & -0.4290 \end{bmatrix}, K_{20} = \begin{bmatrix} 0.0804 & 0.0724 \end{bmatrix}$$

$$W_i = W_{i0} \otimes I_3, i \in \Gamma_6$$

$$W_{10} = \begin{bmatrix} 8.7536 - 0.0142 \\ -0.01428.7617 \end{bmatrix}, W_{20} = \begin{bmatrix} 8.7487 - 0.0170 \\ -0.01708.7584 \end{bmatrix}$$

$$W_{30} = \begin{bmatrix} 8.7462 - 0.0184 \\ -0.01848.7568 \end{bmatrix}, W_{40} = \begin{bmatrix} 8.7584 - 0.0113 \\ -0.01138.7648 \end{bmatrix}$$

$$W_{50} = \begin{bmatrix} 8.7351 - 0.0257 \\ -0.02578.7497 \end{bmatrix}, W_{60} = \begin{bmatrix} 8.7411 - 0.0213 \\ -0.02138.7533 \end{bmatrix}.$$

The initial position of six UAVs are assumed by $\zeta_1(0) = [4, 2, 2.2]^T$, $\zeta_2(0) = [5, 1, 1.2]^T$, $\zeta_3(0) = [6, 4.5, 4.8]^T$, $\zeta_4(0) = [3, 2.5, 2.9]^T$, $\zeta_5(0) = [3, 2.49, 2.91]^T$, and $\zeta_6(0) = [3, 2.51, 2.89]^T$. Based on the above control gains, the simulation results shown in Figs. 3–8 can be generated, wherein Fig. 5 displays the control input. Under such a designed control, the tracking position/velocity errors are presented in Fig. 3, indicating the asymptotic stability of the UAV system despite the deception attacks. Each UAV reaches its designated position and successfully completes the formation task. The tracking trajectories of each UAV are shown in Fig. 4 with position snapshots captured at time intervals of 10, 30, and 50 s. Fig. 6 exhibits the trajectories of the thresholds $\varsigma_i(t)$ $(i \in \Gamma_6)$ of the DETM, from which one can see that the thresholds $\varsigma_i(t)$ $(i \in \Gamma_6)$ are adaptively modulated based on the tracking errors and triggering errors rather than preset constants and finally converge to 0.02, 0.024, 0.026, 0.016, 0.022, and 0.03, respectively. Figs. 7 and 8 depict the six UAVs' triggering instants and releasing intervals. These figures demonstrate the effectiveness of the designed DETM in saving network resources by discarding data that violates triggering conditions, while ensuring UAV tracking performance.

Theorem 1 not only presents the conditions for ensuring the tracking performance, but also evaluates the upper bound of deception attacks. In this example, the estimated upper bound is calculated as 0.1187. This estimation serves as a reference of secure value, as exceeding this secure value poses a risk to the UAV formation. This is illustrated in Fig. 9.

Furthermore, a comparison is made between our proposed method and the secure formation control method in [25], which

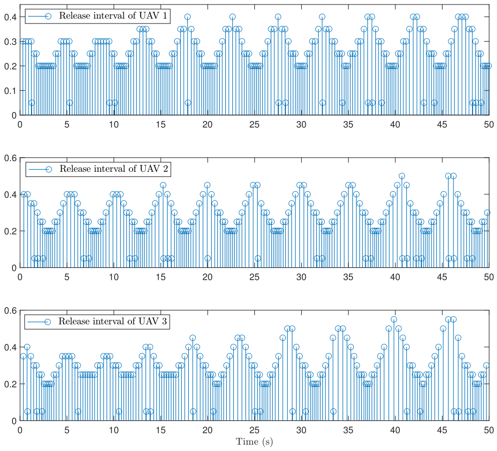


Fig. 7. Release instants and intervals of UAVs 1–3.

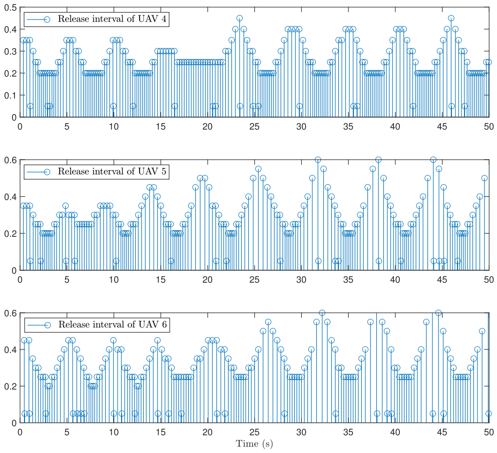


Fig. 8. Release instants and intervals of UAVs 4–6.

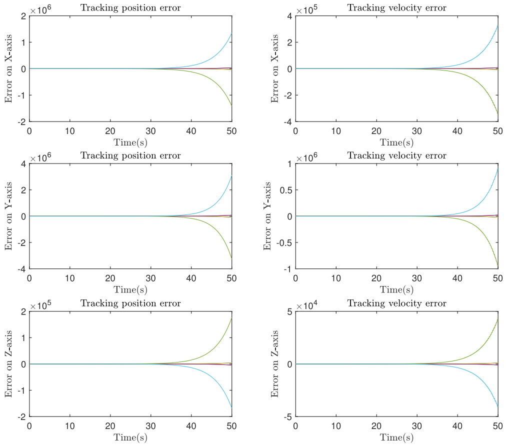


Fig. 9. Tracking position/velocity errors of six UAVs with $\bar{\mu} = 0.15$.

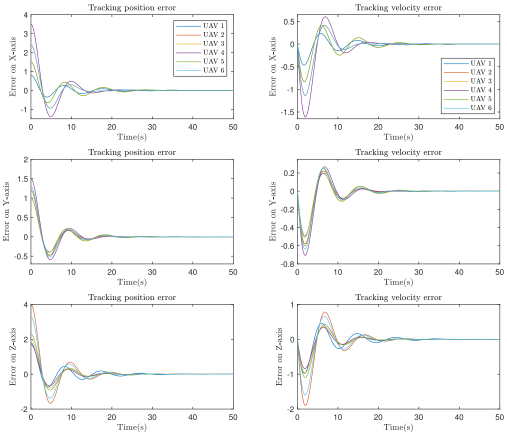


Fig. 10. Tracking position/velocity errors of six UAVs with the secure formation control method in [25].

TABLE I
NTE FOR UAV 1 UNDER DIFFERENT TRIGGERING PARAMETERS

Triggering parameters		NTE
$\alpha_1 = 0.2$, $\phi_1 = 0.01$	$\beta_1 = 0.005$	219
	$\beta_1 = 0.01$	201
	$\beta_1 = 0.03$	162
$\alpha_1 = 0.2$, $\beta_1 = 0.01$	$\phi_1 = 0.005$	214
	$\phi_1 = 0.01$	201
	$\phi_1 = 0.03$	161
$\beta_1 = 0.01$, $\phi_1 = 0.01$	$\alpha_1 = 0.02$	204
	$\alpha_1 = 0.2$	201
	$\alpha_1 = 0.4$	199

relies on predefined upper limits of deception attacks. In implementing the control method from [25], the upper bound of the deception attack is set to 0.08. Under conditions identical to those depicted in Figs. 3 and 10 exhibit the tracking position/velocity errors for six UAVs with the secure formation control method in [25]. Figs. 3 and 10 demonstrate that the multi-UAV system achieves the formation flight objective using these formation control methods. However, the estimated upper bound for deception attacks, which is calculated as 0.1187, exceeds the upper bound of 0.08 set in [25]. This highlights the proposed method's ability to mitigate the adverse effects on the UAV system and reduce the conservatism in the design of the formation control strategy.

By setting different values for the triggering parameters α_i, β_i, and ϕ_i $(i \in \Gamma_6)$, the number of triggering events (NTE) generated by the ETMs is recorded in Table I, while keeping the other parameters the same, as in Fig. 3. For brevity, only the results for UAV 1 are presented, as the findings for UAVs 2–6 are similar. From Table I, it can be observed that larger values of β_i, ϕ_i, and α_i result in fewer triggering events. Furthermore, β_i and ϕ_i significantly affect the NTE, while α_i has a relatively smaller impact.

Next, we aimed to demonstrate the effectiveness of the proposed DETM in reducing redundant triggering events compared to the ETM with constant thresholds proposed in [12]. In the ETM in [12], the sampling period is 0.05 s. Under the same conditions and parameters as the previous simulation, Fig. 11 displays the responses of the tracking position/velocity error

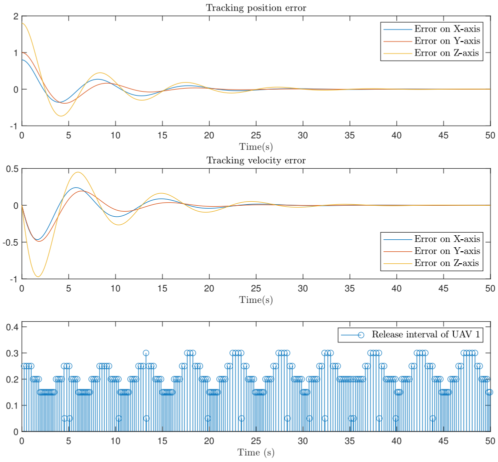


Fig. 11. Tracking position/velocity error and release intervals for the first UAV with the ETM in [12].

TABLE II
NTE for Six UAVs Under Different ETMs

	ETM in [12]	Our DETM (8)
NTE for UAV 1	302	201
NTE for UAV 2	279	190
NTE for UAV 3	259	183
NTE for UAV 4	312	204
NTE for UAV 5	265	173
NTE for UAV 6	242	162

and release intervals of UAV 1 under the ETM. For brevity, only the results for UAV 1 are presented, as those for UAVs 2–6 have analogous results. Table II presents the NTE generated by the ETMs above for all six UAVs.

The results depicted in Figs. 3 and 11 indicate that the trajectories of the tracking position/velocity errors for UAV 1 using both ETMs were similar. However, as shown in Table II, the NTE for UAVs 1–6 under the developed DETM (8) were significantly reduced by 33.4%, 31.9%, 29.3%, 34.6%, 34.7%, and 33.1%, respectively, compared to that generated by the ETM in [12] with the sampling period $h = 0.05$ s. This reduction in triggering events illustrates the effectiveness of our DETM in mitigating the bandwidth burden of the UAV communication network.

V. Conclusion

In this study, we have tackled the challenge of dynamic event-based formation control for multi-UAVs operating under deception attacks, taking into account an estimated upper bound on deception attacks. Distinguishing our methodology from existing literature focused on deception attacks with predetermined upper bounds, we estimate the maximum attack redundancy capable of ensuring the tracking performance of multi-UAVs. The formulated formation control strategies for UAVs under deception attacks were tailored to fulfill the specific formation tasks assigned to each UAV. Simulation results effectively showcase the effectiveness of the proposed approach in achieving formation stabilization and precise tracking control. In this study, the estimated upper bound of deception attacks serves as a reference of secure for maintaining UAV formation under the designed control strategy. Future research will focus on finding a more accurate estimation of the secure upper bound for deception attacks.

References

[1] B. Tian, J. Cui, H. Lu, L. Liu, and Q. Zong, “Attitude control of UAVs based on event-triggered supertwisting algorithm,” *IEEE Trans. Ind. Informat.*, vol. 17, no. 2, pp. 1029–1038, Feb. 2021.

[2] B. U. Meinen and D. T. Robinson, “Mapping erosion and deposition in an agricultural landscape: Optimization of UAV image acquisition schemes for SfM-MVS,” *Remote Sens. Environ.*, vol. 239, Mar. 2020, Art. no. 111666.

[3] B. Wang, “A time-varying observer design for synchronization with an uncertain target and its applications in coordinated mission rendezvous,” *Automatica*, vol. 136, Feb. 2022, Art. no. 109931.

[4] V. P. Tran, F. Santoso, M. A. Garratt, and S. G. Anavatti, “Distributed artificial neural networks-based adaptive strictly negative imaginary formation controllers for unmanned aerial vehicles in time-varying environments,” *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 3910–3919, Jun. 2021.

[5] T. Yin, Z. Gu, and J. H. Park, “Event-based intermittent formation control of multi-UAV systems under deception attacks,” *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 35, no. 6, pp. 8336–8347, Jun. 2024.

[6] J. Wang, L. Han, X. Dong, Q. Li, and Z. Ren, “Distributed sliding mode control for time-varying formation tracking of multi-UAV system with a dynamic leader,” *Aerosp. Sci. Technol.*, vol. 111, Apr. 2021, Art. no. 106549.

[7] B. An, B. Wang, H. Fan, L. Liu, H. Hu, and Y. Wang, “Fully distributed prescribed performance formation control for UAVs with unknown maneuver of leader,” *Aerosp. Sci. Technol.*, vol. 130, Nov. 2022, Art. no. 107886.

[8] B. Wang, W. Chen, B. Zhang, P. Shi, and H. Zhang, “A nonlinear observer-based approach to robust cooperative tracking for heterogeneous spacecraft attitude control and formation applications,” *IEEE Trans. Autom. Control*, vol. 68, no. 1, pp. 400–407, Jan. 2023.

[9] S. Baldi, D. Sun, G. Zhou, and D. Liu, “Adaptation to unknown leader velocity in vector-field UAV formation,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 1, pp. 473–484, Feb. 2022.

[10] B. Zhang, X. Sun, M. Lv, and S. Liu, “Distributed coordinated control for fixed-wing UAVs with dynamic event-triggered communication,” *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 4665–4676, May 2022.

[11] H. Guo, M. Chen, Y. Jiang, and M. Lungu, “Distributed adaptive human-in-the-loop event-triggered formation control for QUAVs with quantized communication,” *IEEE Trans. Ind. Informat.*, vol. 19, no. 6, pp. 7572–7582, Jun. 2023.

[12] X.-M. Zhang and Q.-L. Han, “A decentralized event-triggered dissipative control scheme for systems with multiple sensors to sample the system outputs,” *IEEE Trans. Cybern.*, vol. 46, no. 12, pp. 2745–2757, Dec. 2016.

[13] Z. Gu, Y. Fan, X. Sun, C. K. Ahn, and X. Xie, “Event-based two-step transmission mechanism for the stabilization of networked T-S fuzzy systems with random uncertaintie,” *IEEE Trans. Cybern.*, vol. 54, no. 2, pp. 1283–1293, Feb. 2024.

[14] J. Luo, L. Tang, Q. Chen, and Z. Zhang, “Trajectory design and bandwidth allocation considering power-consumption outage for UAV communication: A machine learning approach,” *IEEE Trans. Ind. Informat.*, vol. 20, no. 2, pp. 2519–2528, Feb. 2024.

[15] J. Wang, C. Bi, D. Wang, Q. Kuang, and C. Wang, “Finite-time distributed event-triggered formation control for quadrotor UAVs with experimentation,” *ISA Trans.*, vol. 126, pp. 585–596, Jul. 2022.

[16] X. Sun, Z. Gu, D. Yue, and X. Xie, “Event-triggered H_∞ filtering for cyber–physical systems against DoS attacks,” *IEEE Trans. Syst. Man Cybern.: Syst.*, vol. 53, no. 5, pp. 2705–2715, May 2023.

[17] Z. Gu, X. Huang, X. Sun, X. Xie, and J. H. Park, “Memory-event-triggered tracking control for intelligent vehicle transportation systems: A leader-following approach,” *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 5, pp. 4021–4031, May 2024.

[18] W. Gai, S. Li, J. Zhang, Y. Zheng, and M. Zhong, “Dynamic event-triggered H_i/H_∞ optimization approach to fault detection for unmanned aerial vehicles,” *IEEE Trans. Instrum. Meas.*, vol. 71, 2022, Art. no. 3512211.

[19] X. Sun, Z. Gu, F. Yang, and S. Yan, "Memory-event-trigger-based secure control of cloud-aided active suspension systems against deception attacks," *Inf. Sci.*, vol. 543, pp. 1–17, Jan. 2021.

[20] M. Zhang, W. X. Zheng, X. Song, and H. Yuan, "Two efficient Kalman filter algorithms for measurement packet dropping systems under maximum correntropy criterion," *Syst. Control Lett.*, vol. 175, May 2023, Art. no. 105515.

[21] X. Xie, F. Yang, L. Wan, J. Xia, and K. Shi, "Enhanced local stabilization of constrained N-TS fuzzy systems with lighter computational burden," *IEEE Trans. Fuzzy Syst.*, vol. 31, no. 3, pp. 1064–1070, Mar. 2023.

[22] X. Xie, J. Lu, D. Yue, and D.-W. Ding, "Enhanced fuzzy fault estimation of discrete-time nonlinear systems via a new real-time gain-scheduling mechanism," *IEEE Trans. Cybern.*, vol. 53, no. 3, pp. 1607–1617, Mar. 2023.

[23] Y. Guo, M. Wu, K. Tang, J. Tie, and X. Li, "Covert spoofing algorithm of UAV based on GPS/INS-integrated navigation," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6557–6564, Jul. 2019.

[24] E. Tian, H. Chen, C. Wang, and L. Wang, "Security-ensured state of charge estimation of lithium-ion batteries subject to malicious attacks," *IEEE Trans. Smart Grid*, vol. 14, no. 3, pp. 2250–2261, May 2023.

[25] T. Yin, Z. Gu, and S. Yan, "Event-based formation control for multiple unmanned aerial vehicles under directed topology," *ISA Trans.*, vol. 137, pp. 111–121, Jun. 2023.

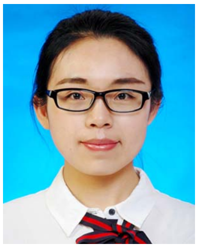
[26] L. Zha, R. Liao, J. Liu, X. Xie, E. Tian, and J. Cao, "Dynamic event-triggered output feedback control for networked systems subject to multiple cyber attacks," *IEEE Trans. Cybern.*, vol. 52, no. 12, pp. 13800–13808, Dec. 2022.

Zhou Gu (Senior Member, IEEE) received the B.S. degree in automation from North China Electric Power University, Beijing, China, in 1997, and the M.S. and Ph.D. degrees in control science and engineering from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2007 and 2010, respectively.

From 1999 to 2013, he was with the School of Power engineering, Nanjing Normal University as an Associate Professor. He is currently a Professor with Anhui Polytechnic University, Wuhu, China. His current research interests include networked control systems, time-delay systems, reliable control, and their applications.

Tingting Yin received the Ph.D. degree in mechanical engineering from Nanjing Forestry University, Nanjing, China, in 2024.

From 2023 to 2024, she was a Visiting Ph.D. Student with the Department of Electrical Engineering, Yeungnam University, Gyeongsan, South Korea. Her research interests include networked control systems, multiagent systems, cooperative control, reliable control, and their applications.



Qing Lu received the Ph.D. degree in control science and engineering from the Harbin Institute of Technology, Harbin, China, in 2021.

From 2017 to 2019, she was a Visiting Student with the School of Electrical and Electronic Engineering, University of Adelaide, Adelaide, SA, Australia. She is currently a Lecturer with the College of Mechanical and Electronic Engineering, Nanjing Forestry University, Nanjing, China. Her research interests include networked control systems, fuzzy control, model predictive control, and event-triggered control.

Ju H. Park (Senior Member, IEEE) received the Ph.D. degree in electronics and electrical Engineering from the Pohang University of Science and Technology (POSTECH), Pohang, South Korea, in 1997.

From 1997 to 2000, he was a Research Associate with the Engineering Research Center-Automation Research Center, POSTECH. In March 2000, he was with Yeungnam University, Gyeongsan, South Korea, where he is currently the Chuma Chair Professor. He is the coauthor of the monographs *Recent Advances in Control and Filtering of Dynamic Systems with Constrained Signals* (Springer-Nature, 2018) and *Dynamic Systems With Time Delays: Stability and Control* (Springer-Nature, 2019) and is the Editor of an edited volume *Recent Advances in Control Problems of Dynamical Systems and Networks* (Springer-Nature, 2020). He has authored or coauthored a number of articles in his research fields, which include robust control and filtering, neural/complex networks, fuzzy systems, multiagent systems, and chaotic systems.

Dr. Park was the recipient of the Highly Cited Researchers Award by Clarivate Analytics (formerly, Thomson Reuters), since 2015 and listed in three fields, Engineering, Computer Sciences, and Mathematics, from 2019 to 2022. He is the Receiving Editor, a Subject Editor, an Advisory Editor, and an Associate Editor of several international journals, including *Nonlinear Dynamics, Franklin Open, IET Control Theory and Applications, Engineering Reports, Cogent Engineering*, IEEE TRANSACTIONS ON FUZZY SYSTEMS, IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, and IEEE TRANSACTIONS ON CYBERNETICS. He is a Fellow of the Korean Academy of Science and Technology.