Event-Triggered Formation Tracking Control for Unmanned Aerial Vehicles Subjected to Deception Attacks

Biao Sun 1, Zhou Gu 1,* and Tianyi Xiong 1,2

1 College of Mechanical & Electronic Engineering, Nanjing Forestry University, Nanjing 210037, China; sunbiao@njfu.edu.cn (B.S.); tianyixiong@njfu.edu.cn (T.X.)
2 School of Aeronautic Engineering, Nanjing Vocational University of Industry Technology, Nanjing 210023, China
* Correspondence: guzhou@njfu.edu.cn

Abstract: This study investigates the time-varying formation tracking (TVFT) control problem for multiple unmanned aerial vehicle (multi-UAV) systems under deception attacks by utilizing an event-triggered mechanism (ETM). First, for the sake of alleviating the communication burden, an effective ETM is designed in this paper. Second, to deal with deception attacks in the communication network, a random deception attack model under the designed ETM is constructed. Finally, a novel formation tracking control scheme for multi-UAV systems under deception attack combining the ETM is proposed to achieve the expected TVFT. The stability analysis of the formation control system is given by using the Lyapunov stability theory and linear matrix inequality (LMI) technique. Simulations are conducted to verify the effectiveness of the proposed formation control scheme.

Keywords: unmanned aerial vehicle (UAV); formation tracking control; ETM; deception attacks

1. Introduction

In the past few decades, formation flight for multiple unmanned aerial vehicle (multi-UAV) has attracted considerable research interest with the development of computer technology, sensor technology and communication networks, owing to their incomparable advantages, including low operation cost, high robustness, strong mobility and self-adaptability. Generally, one of the primary concerns of formation flight is the formation tracking control problem, which has been a research hotspot. Consequently, a large amount of results have emerged [1–3]. However, a great part of the existing formation tracking control methods are to achieve time-invariant formations, which are difficult to satisfy practical demands [4,5]. Therefore, time-varying formation control is proposed, and an increasing number of studies were conducted recently [4,6–9].

It should be pointed out that UAVs exchange information with each other through a communication network with limited energy and bandwidth in practical application. Such a situation may deteriorate the formation control performance of the multi-UAV systems. Therefore, it is necessary to design an appropriate information transmission mechanism to overcome the above drawbacks. Traditionally, an effective information transmission mechanism is periodic state sampling mechanism (so-called time-triggered mechanism (TTM)) [10], which is simple and easy to be implemented. However, the time-triggered mechanism (TTM) releases a large amount of redundant information into the communication network, even when the system is in a good condition, which will not only lead to the waste of network resources, but also decrease the battery life of the UAVs [11]. For purpose of dealing with the above problems brought by TTM s, event-triggered mechanisms (ETMs) are put forward to save network resources [12–17]. In the ETMs, whether a control task is executed or not hinges on predefined trigger criteria rather than on a time period [18,19]. For networked control systems, a new event-triggering control strategy is designed in [20]. On the basis of the work in [20], fruitful subsequent...
researches were conducted [21–35]. A position tracking control strategy based on an event-triggered mechanism for UAVs with multiple state time delays and external disturbances is designed in [36].

A communication network provides convenience and efficiency in the information exchange among UAVs. Nevertheless, it brings many challenges to the control of multi-UAV systems, such as the network security problem. Among the various factors impacting network security, cyber attacks [37,38] are able to exhaust network resources and may cause failures of important tasks. The network attack includes denial of service (DoS) attack [39,40], replay attack [41], deception attack [42–44] and so on. The DoS attack may prevent the timely information exchange [45]. With respect to the replay attack, the attackers maliciously transmit the received data repeatedly within a certain period of time, which may result in repeated unnecessary operations [46]. The deception attack will cause the incompleteness of data by replacing or stealing the information, which may result in the instability, and even executions of instructions from the attackers [47]. Compared to the aforementioned two forms of cyber-attacks, the deception attack is difficult to detect and prevent [48]. Therefore, much effort has been devoted to alleviating the negative impacts from deception attack, and great progress has been made in recent years [49–52].

As far as we know, few results are available on consensus or formation control problems for multi-UAV systems with deception attacks. Wang et al. investigate the formation control problem of multiple robots under deception attacks. Nevertheless, the ETM is not utilized to alleviate the communication burden [53]. A novel formation control law based on ETM is proposed in [54]; however, the deception attack is not considered in the proposed strategy. In addition, only time-invariant formations are realized in [54]. Therefore, the time-varying formation tracking (TVFT) control problem based on ETM for multi-UAV systems subjected to deception attacks needs more investigation.

Inspired by the observations above, we propose an integrated event-triggered formation tracking control scheme for multi-UAV systems with deception attacks. The main contributions of this study can be summarized as follows.

(1) An ETM is proposed for multi-UAV systems with time delay. Compared with the event-triggered mechanisms in Ref. [12], the information of both the leader and the formation is used to design the triggering condition, which reduces the amount of redundant data and alleviates the communication burden. Compared with the event-triggered mechanism in Ref. [54], time delay is taken into consideration, which makes the designed ETM more reasonable and realistic. The presence of time delay brings a large challenge to the theoretical analysis and finding a feasible solution by LMI since the Lyapunov function is more complicated, compared to the one in [54].

(2) A novel time-varying formation tracking control strategy is developed for multi-UAV systems under deception attacks. As far as we know, few results simultaneously take the TVFT control and deception attack problems into consideration. Different from the existing results on multi-UAV systems without cyber attacks [2,19], the problem of deception attacks is taken into account, which describes the actual situation more reasonably. The existence of deception attack increases the difficulty of the stability analysis since attackers release the inaccuracy feedback information into the communication network among the UAVs. In addition, to deal with the deception attacks, plenty of nonlinear terms are brought in the stability analysis, which needs more mathematical treatments.

Notations are as follows: \( I_n \) represents the identity matrix with \( n \times n \) dimension. \( \otimes \) describes Kronecker product. \( * \) is the terms obtained by symmetric transformation. \( \mathbb{E}\{G(t)\} \) is the mathematical expectation of \( G(t) \). \( \|X\|_2 \) denotes the 2-norm of matrix \( X \). \( Q > 0 \) represents that the matrix \( Q \) is positive definite.

2. System Description and Modeling

2.1. UAV Modeling

In this paper, we assume that \( N \) UAVs (labeled as 1, 2, \cdots, \( N \)) and one leader (denoted as UAV 0) comprise the multi-UAV systems, whose dynamics can be described as follows [2]:
\[
\begin{align*}
\dot{x}_i(t) &= Ax_i(t) + Bu_i(t), \\
x_0(t) &= Ax_0(t) + Bu_0(t),
\end{align*}
\]  
(1)

where \(x_i(t) = [x_{ix}^T(t), x_{iv}^T(t)]^T \in \mathbb{R}^{2m}\) and \(x_0(t) = [x_{ix0}^T(t), x_{iv0}^T(t)]^T \in \mathbb{R}^{2m}\) are the state vectors of UAV \(i\) and the leader, respectively. \(x_{ix}(t) \in \mathbb{R}^m\) and \(x_{iv}(t) \in \mathbb{R}^m\) are the position and velocity vector of UAV \(i\), respectively. \(x_{ix0}(t) \in \mathbb{R}^m\) and \(x_{iv0}(t) \in \mathbb{R}^m\) are the position and velocity vector of the leader, respectively. \(u_i(t) \in \mathbb{R}^m\) and \(u_0(t) \in \mathbb{R}^m\) are the control inputs of UAV \(i\) and leader, respectively. \(A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \otimes I_m, B = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes I_m\).

**Remark 1.** It is worth noting that a single UAV is regarded as a particle here, which is applied in most of the existing studies on the formation tracking control problem for multi-UAV systems [2,5,6]. As is known to all, the control of a UAV can be decoupled into attitude-loop and trajectory-loop control. Since the attitude-loop control of a UAV can be completed by UAV itself, and the formation control studied in this paper is only concerned with the position \(x_{ix}(t)\) and the velocity \(x_{iv}(t)\), the trajectory-loop control problem is addressed when dealing with the formation tracking control issue for the multi-UAV systems.

The UAVs are supposed to maintain a desired formation and track the leader’s trajectories in the meantime under the proposed control scheme. The expected formation is specified by \(p_{iF}(t) = [p_{iF1}^T(t), p_{iF2}^T(t), \ldots, p_{iFK}^T(t)]^T\), where \(p_{i0}(t) = [p_{i01}^T(t), p_{i02}^T(t)]^T\) with \(p_{i0}(t) = p_{i0}(t)\) is the piecewise continuously differentiable formation vector for UAV \(i\) with \(p_{i0}(t)\) being the corresponding position and velocity term in vector \(p_{i0}(t)\), respectively [55]. We define the formation tracking error as follows:

\[
\Psi_i(t) = x_i(t) - x_0(t) - p_{i0}(t),
\]  
(2)

where \(\Psi_i = [\Psi_{ix}^T, \Psi_{iv}^T]^T, \Psi_{ix}(t) = x_{ix}(t) - x_{ix0}(t) - p_{ix}(t)\) and \(\Psi_{iv}(t) = x_{iv}(t) - x_{iv0}(t) - p_{iv}(t)\) are denoted as the formation tracking position and velocity error vector, respectively.

This article aims at proposing a novel event-triggered formation tracking control scheme so that \(\Psi_i(t)\) is able to converge to the origin, that is, the desired TVFT of multi-UAV system (1) subjected to deception attacks can be achieved. Figure 1 shows the framework of the overall formation control scheme.

![Figure 1](image-url)  
**Figure 1.** The framework of the overall formation control scheme.

### 2.2. Event-Triggered Communication Scheme

The information exchanges among the UAVs are implemented by a communication network. To solve the problem of unnecessary network resource consumption brought by periodic sampling, ETMs are adopted to decide whether the real-time local control data should be released or not. The event-trigger function is as follows:

\[
\ell(t) = e_i^T(t)\Omega_i e_i(t) - \lambda_i \Psi_i^T(t^i_p h + \mu^i h)\Omega_i \Psi_i(t^i_p h + \mu^i h),
\]  
(3)
where \( e_i(t) = \Psi_i(t_{i}^p h) - \Psi_i(t_{i}^p h + \mu_i h) \) represents the \( i \)-th UAV’s error between the last event-triggered data and current sampling data; \( \lambda_i \in [0, 1] \) and \( \Omega_i \) are positive symmetric matrices to be designed; \( h \) is the sampling period; \( \mu_i = 1, 2, \ldots; t_{i}^p h \subseteq \{ t_{i}^0 h, t_{1}^1 h, t_{2}^2 h, \ldots \} \) represents the latest releasing instant of the \( i \)-th UAV in which \( t_0 \) is the initial time; \( t_{i}^p h + \mu_i h \) denotes the current sampling instant of the \( i \)-th UAV. Then the next releasing instant of the \( i \)-th UAV can be defined by the following:

\[
t_{i}^{p+1} h = t_{i}^{p} h + \max \left\{ (\mu^i + 1)h \mid \ell(t) < 0 \right\}.
\]

(4)

According to (4), if the event-triggered condition \( \ell(t) > 0 \), the data packet at this sampling instant is delivered to the controller of the \( i \)-th UAV, while the packets at instants \( t_{i}^p h + \mu_i h \) are discarded with \( \mu_M^i \triangleq \max \{ \mu^i \} \) for \( t \in [t_{i}^p h, t_{i}^{p+1} h) \).

2.3. Deception Attacks

Due to the intrinsic properties of the communication network among the UAVs, the network is vulnerable to cyber attacks. The deception attack as a common attack mode is considered in this paper, which may modify the data transmitted through the network. It can be expressed by a nonlinear function \( f(\Psi_i(t)) \). In view of the fact that the deception attack occurs randomly, the random variable \( \omega(t) \in \{0, 1\} \) is used to describe whether the deception attack occurs or not, which satisfies the Bernoulli distribution. In detail, if \( \omega(t) = 1 \), the attack occurs; if \( \omega(t) = 0 \), the attack does not happen. Then, the signal under deception attacks for UAV \( i \) received from UAV \( j \) is presented as the following:

\[
\hat{\Psi}_j(t) = \omega(t)f(\Psi_j(t - \varsigma_j(t))) + (1 - \omega(t))\Psi_j(t_{i}^p h),
\]

(5)

where \( 0 \leq \varsigma_j(t) \leq \varsigma_M^i \) with \( \varsigma_M^i \) being a maximum attack delay. Denote \( \varsigma_M = \max\{\varsigma_M^1, \varsigma_M^2, \ldots, \varsigma_M^N\} \). Besides, \( \mathbb{E}\{\omega(t)\} = \bar{\omega} \) and \( \mathbb{E}\{(\omega(t) - \bar{\omega})^2\} = \sigma^2 \).

**Assumption 1.** Assume that the deception attack function \( f(x) \) satisfies the following conditions:

\[
\|f(\Psi(t))\|_2 \leq \|F\Psi(t)\|_2,
\]

(6)

where \( F \) is a real constant matrix with appropriate dimensions.

**Remark 2.** Note that the deception attacks may be undetectable since the attack signals are strategically generated by malicious adversaries and may relate to system information. In this paper, we assume that the full state information transmitted in the network is available to the attackers. In addition, the deception attack is supposed to be modeled as a nonlinear function \( f(\Psi_j(t - \varsigma_j(t))) \) associated with the system state.

**Remark 3.** It should be pointed out that the error signal under deception attack \( \hat{\Psi}_j(t) \) can be acquired through the corresponding sensors and network in real control. In detail, the ideal error signal without deception attack \( \Psi_j(t) \) is obtained through corresponding local sensors. Then, it may encounter deception attacks, and \( \hat{\Psi}_j(t) \) may be delivered to UAV \( i \) through the communication network.

**Remark 4.** It should be mentioned that the energy of deception attack is limited in practice, and deception attacks may be difficult to be detected. Thus, we can assume the deception attack nonlinear function \( f(\Psi_j(t - \varsigma_j(t))) \) is constrained by condition (6) in Assumption 1, which is really of practical significance and also made in [23,56,57].

**Remark 5.** To avoid being detected, the deception attack is usually an intermittent signal. Thus, we can assume that \( \omega(t) \) satisfies the Bernoulli distribution, which also conforms to reality. Similar assumptions are also made in [58,59].
Remark 6. In recent years, due to the widespread application of UAVs, the network security of multi-UAV systems has attracted widespread attention from scholars. In the existing literature, researchers have deeply investigated the control problems of single systems under deception attacks. However, the research on the network security control issues for multi-UAV systems is not sufficient at present. As a result, this study investigates the secure formation control for multi-UAV systems (1) with deception attacks (5).

2.4. Control Law and Formation Tracking Error Systems

Invoking the dynamics (1) and taking the derivative of (2), the dynamics of the formation tracking error is the following:

\[
\dot{\Psi}_i(t) = Ax_i(t) + Bu_i(t) - Ax_0(t) - Bu_0(t) - \dot{p}_i(t).
\]

(7)

According to the above equation and adopting state feedback control method, a general formation tracking control law can be derived as follows:

\[
a_i(t) = -K \sum_{j=1}^{N} a_{ij} \left[ (x_i(t) - x_j(t) - p_i(t)) - (x_j(t) - x_0(t) - p_j(t)) \right] \\
+ b_i (x_i(t) - x_0(t) - p_i(t)) + \dot{p}_i + \dot{x}_0,
\]

(8)

where \( K \in \mathbb{R}^{n \times m} \) is the control gain matrix with the elements being positive. \( a_{ij} \geq 0 \) and \( b_i \geq 0 \) are the coupling weights among the followers and leader. In detail, \( a_{ij} > 0 \) if and only if UAV \( j \) can deliver information to UAV \( i \); otherwise, \( a_{ij} = 0 \). \( b_i > 0 \) if and only if the leader can deliver information to UAV \( i \); if not, \( b_i = 0 \).

Combining (2) and (8), we have the following:

\[
a_i(t) = -K \sum_{j=1}^{N} a_{ij} \left[ \Psi_i(t) - \Psi_j(t) \right] + b_i \Psi_i(t) + \dot{p}_i + \dot{x}_0.
\]

(9)

Then, by taking the designed ETM (3) and deception attack into consideration, the actual control law can be obtained as follows:

\[
u_i(t) = -K \sum_{j=1}^{N} a_{ij} \left[ \Psi_i(t) - \Psi_j(t) \right] + b_i \Psi_i(t) + \dot{p}_i + \dot{x}_0, t \in [t^i_{\varphi h}, t^i_{\varphi +1 h}].
\]

(10)

Remark 7. As a matter of fact, the term \(-K \sum_{j=1}^{N} a_{ij} \left[ \Psi_i(t) - \Psi_j(t) \right] + b_i \Psi_i(t)\) in (9) denotes the feedback control with respect to the local neighborhood error \( \sum_{j=1}^{N} a_{ij} \left[ \Psi_i(t) - \Psi_j(t) \right] + b_i \Psi_i(t) \). The last two terms \( \dot{p}_i \) and \( \dot{x}_0 \) are designed to compensate the corresponding terms in (7). Furthermore, the formation tracking error signal of UAV \( i \) at instant \( t^i_{\varphi h} \) adopts the packets generated by ETM, which is represented by \( \Psi_i(t^i_{\varphi h}) \). In addition, with the help of the zero-order-holder which is equipped in the local controller, the control input holds until a new triggered signal is delivered. \( \Psi_j(t) \) refers to the formation tracking error state of UAV \( j \) suffering from the deception attack. Compared with the traditional formation control law in [2,19], the multi-UAV system can achieve the desired formation by using the event-based control strategy (10), even if the multi-UAV systems suffer from the deception attacks.

Time delay is inevitable during the communication among the UAVs. We assume that time delay of the the \( i \)-th UAV at the instant of \( t^i_{\varphi h} \) is denoted as \( \tau^i_{\varphi} \) with an upper bound \( \tau^i_{\text{max}} \). It holds that \( [t^i_{\varphi h} + \tau^i_{\varphi}, t^i_{\varphi + 1 h} + \tau^i_{\varphi + 1}] = \bigcup_{\mu^i=0}^{\tau^i_{\text{max}}} x^i_{\varphi h} [\mu^i h] \) with \( x^i_{\varphi h} [\mu^i h] = [t^i_{\varphi h} + \mu^i h, \ldots] \).
\[ \pi_{\phi} = \pi_{\phi+1} + h + \mu' h + h + \pi'_{\phi+1}. \] Define \( \pi'(t) = t - t'_{\phi} h - \mu' h \) for \( t \in X_{t_{\phi}} \). It yields the following:

\[ 0 \leq \pi'(t) \leq h + \pi'_{\max} = \pi_M. \] (11)

To facilitate analysis, \( \pi'_M = \max\{\pi'_1, \pi'_2, \ldots, \pi'_N\} \).

From (3) and (11), the event-triggered data at the current time can be expressed as the following:

\[ \Psi'_i(t_{\phi} h) = \Psi'_i(t - \pi'(t)) + e_i(t). \] (12)

Define

\[
\begin{align*}
\Psi(t) &= [\Psi_1^T(t), \Psi_2^T(t), \ldots, \Psi_N^T(t)]^T, \\
F(\Psi(t - \psi(t))) &= [f^T(\Psi_1(t - \psi(t))), f^T(\Psi_2(t - \psi(t))), \ldots, f^T(\Psi_N(t - \psi(t)))]^T, \\
e(t) &= [e_1^T(t), e_2^T(t), \ldots, e_N^T(t)]^T, \\
\Psi(t - \pi(t)) &= [\Psi_1^T(t - \pi^2(t)), \Psi_2^T(t - \pi^2(t)), \ldots, \Psi_N^T(t - \pi^2(t))]^T, \\
\hat{B} &= \text{diag}\{b_1, b_2, \ldots, b_N\}, \\
L &= L + \hat{B},
\end{align*}
\]

where matrix \( L = D - W \) is the Laplacian matrix among the UAVs with \( D = \text{diag}\{\Sigma_{i=1}^N a_{1i}, \Sigma_{i=1}^N a_{2i}, \ldots, \Sigma_{i=1}^N a_{N_i}\} \) and \( W = [a_{ij}]_{N \times N} \).

Combining Equations (1)–(3), (5), (10), (12) and definition in (13), the formation tracking error system can be rewritten as the following:

\[
\begin{align*}
\Psi'(t) = & (I_N \otimes A)\Psi(t) - (\tilde{L} \otimes BK)\Psi(t - \pi(t)) - (\tilde{L} \otimes BK)e(t) \\
& - \omega(t)(W \otimes BK)e(t) + \omega(t)(W \otimes BK)F(\Psi(t - \psi(t))) \\
& - \omega(t)(W \otimes BK)\Psi(t - \pi(t)).
\end{align*}
\] (14)

Next, an assumption is made for the subsequent theoretical analysis.

**Assumption 2.** Assume that the communication graph among the UAVs and the leader is a digraph containing a spanning tree, in which the leader is the root node.

**Remark 8.** Based on Assumption 2, the overall formation trajectory can be determined by the leader dynamics, while other followers follow the leader’s trajectory.

### 3. Main Results

In this section, we present the main results of this paper; the stability criterion for the closed-loop control system is derived.

**Theorem 1.** For given event trigger parameter \( \lambda \), the delay upper \( \pi_M, \psi_M \), scalar \( \mu \), the probability expectation of deception attack \( \bar{\omega} \), the gain matrix \( K \) and the attack upper bound matrix \( F \), the formation tracking error system (14) is asymptotically stable if there exist positive definite matrices \( P > 0, Q_1 > 0, Q_2 > 0, R_1 > 0, R_2 > 0, \Omega_i > 0 (i = 1, 2, \ldots, N), \) and the matrices \( M, N \) with appropriate dimensions such that the following matrix inequalities hold:

\[
\Gamma = \begin{bmatrix}
\Gamma_{11} & * & * & * & * \\
\Gamma_{21} & -I & * & * & * \\
\Gamma_{31} & 0 & -R_1^{-1} & * & * \\
\Gamma_{41} & 0 & 0 & -R_2^{-1} & * \\
\Gamma_{51} & 0 & 0 & 0 & -R_1^{-1} \\
\Gamma_{61} & 0 & 0 & 0 & 0 & -R_2^{-1}
\end{bmatrix} < 0,
\] (15)
\[ \begin{bmatrix} R_1 & * \\ M & R_2 \end{bmatrix} \geq 0, \quad \begin{bmatrix} R_2 & * \\ N & R_2 \end{bmatrix} \geq 0, \quad (16) \]

where

\[
\Gamma_{11} = \begin{bmatrix}
\Phi_{11} & * & * & * & * & * \\
\Phi_{21} & \Phi_{22} & * & * & * & * \\
\Phi_{31} & \Phi_{32} & \Phi_{33} & * & * & * \\
\Phi_{41} & 0 & 0 & \Phi_{44} & * & * \\
\Phi_{51} & 0 & 0 & \Phi_{54} & \Phi_{55} & * \\
\Phi_{61} & 0 & 0 & 0 & 0 & -\Omega \\
\Phi_{71} & 0 & 0 & 0 & 0 & -I
\end{bmatrix},
\]

\[
\Phi_{11} = \Phi_{11}^1 + \Phi_{11}^2,
\]

\[
\Phi_{11}^1 = I_N \otimes (PA + A^T P), \quad \Phi_{11}^2 = Q_1 + Q_2 - R_1 - R_2,
\]

\[
\phi_{21} = -L^T \otimes K TB^P - \phi(W \otimes KTB^P) + R_1 + M,
\]

\[
\phi_{22} = -2R_1 - M - M^T + \lambda(L^T \otimes I_2)\Omega(L \otimes I_2),
\]

\[
\phi_{31} = -M, \quad \phi_{32} = R_1 + M, \quad \phi_{33} = -Q_1 - R_1,
\]

\[
\phi_{41} = R_2 + N, \quad \phi_{44} = -2R_2 - N - N^T,
\]

\[
\phi_{51} = -N, \quad \phi_{54} = R_2 + N, \quad \phi_{55} = -Q_2 - R_2,
\]

\[
\phi_{61} = -L^T \otimes K TB^P - \phi(W \otimes KTB^P), \quad \phi_{71} = \phi(W \otimes KTB^P),
\]

\[
\Gamma_{21} = [0 \quad 0 \quad 0 \quad F \quad 0 \quad 0 \quad 0], \quad \Gamma_{31} = [\Gamma_{31}^1 \quad \Gamma_{31}^2 \quad 0 \quad 0 \quad 0 \quad 0 \quad \Gamma_{31}^3 \quad \Gamma_{31}^4],
\]

\[
\Gamma_{31} = \pi_M(I_N \otimes \Lambda), \quad \Gamma_{33} = -\pi_M/[L \otimes BK + \phi(W \otimes BK)], \quad \Gamma_{33} = \pi_M\phi(W \otimes BK),
\]

\[
\Gamma_{41} = [\Gamma_{41}^1 \quad \Gamma_{41}^2 \quad 0 \quad 0 \quad 0 \quad \Gamma_{41}^3 \quad \Gamma_{41}^4],
\]

\[
\Gamma_{41} = eM(I_N \otimes \Lambda), \quad \Gamma_{41} = -eM/[L \otimes BK + \phi(W \otimes BK)], \quad \Gamma_{41} = eM\phi(W \otimes BK),
\]

\[
\Gamma_{51} = [0 \quad \Gamma_{51}^1 \quad 0 \quad 0 \quad 0 \quad \Gamma_{51}^2 \quad -\Gamma_{51}^3 \quad \Gamma_{51}^4], \quad \Gamma_{51} = e\pi_M(W \otimes BK),
\]

\[
\Omega = \text{diag}\{\Omega_1, \Omega_2, \ldots, \Omega_N\}, \quad \lambda = \text{diag}\{I_2 \otimes \lambda_1, I_2 \otimes \lambda_2, \ldots, I_2 \otimes \lambda_N\}.
\]

**Proof.** Choose a Lyapunov–Krasovskii candidate as follows:

\[
V(t) = \Psi^T(t)(I_N \otimes P)\Psi(t) + \int_{t-\pi_M}^t \Psi^T(s)Q_1\Psi(s)ds + \int_{t-\pi_M}^t \Psi^T(s)Q_2\Psi(s)ds + \int_{t-\pi_M}^t \Psi^T(s)R_1\Psi(s)ds + \int_{t-\pi_M}^t \Psi^T(s)R_2\Psi(s)ds.
\]

(17)

Time-differentiate (17) and compute its mathematical expectation to obtain the following:

\[
\mathbb{E}\{V(t)\} = 2\Psi^T(t)(I_N \otimes P)\Psi(t) + \Psi^T(t)(Q_1 + Q_2)\Psi(t) - \Psi^T(t - \pi_M)Q_1\Psi(t - \pi_M)
\]

\[
-\Psi^T(t - \pi_M)Q_2\Psi(t - \pi_M) + \mathbb{E}\{\Psi^T(t)[\pi_M^2R_1 + \pi_M^2R_2]\Psi(t)\}
\]

\[
- \pi_M \int_{t-\pi_M}^t \Psi^T(s)R_1\Psi(s)ds - \pi_M \int_{t-\pi_M}^t \Psi^T(s)R_2\Psi(s)ds,
\]

(18)

where the following holds:

\[
\Psi(t) = \mathcal{A}(t) + (\phi - \omega(t))\mathcal{B}(t),
\]

\[
\mathcal{A}(t) = (I_N \otimes A)\Psi(t) - [L \otimes BK + \phi(W \otimes BK)]\Psi(t - \pi(t))
\]

\[
- [L \otimes BK + \phi(W \otimes BK)]\eta(t) + \phi(W \otimes BK)F(\Psi(t - \phi(t))),
\]

\[
\mathcal{B}(t) = (W \otimes BK)\Psi(t - \pi(t)) + (W \otimes BK)e(t) - (W \otimes BK)F(\Psi(t - \phi(t))).
\]
Letting $\mathcal{R} = \pi_M^2 \mathcal{R}_1 + \varepsilon_M^2 \mathcal{R}_2$ yields the following:

$$
\mathbb{E}\{\Psi^T(t)(\pi_M^2 \mathcal{R}_1 + \varepsilon_M^2 \mathcal{R}_2)\Psi(t)\} = \mathcal{A}^T(t)\mathcal{R}(t) + e^2 \mathcal{B}^T(t)\mathcal{R}(t).
$$

Using the Jessen inequality in [21], it follows that

$$
-\pi_M \int_{t-\pi_M}^t \Psi^T(s)\mathcal{R}_1\Psi(s)ds \leq \mathcal{Z}_1^2(t)\Pi_1\mathcal{Z}_1(t),
$$

$$
-\varphi_M \int_{t-\varphi_M}^t \Psi^T(s)\mathcal{R}_2\Psi(s)ds \leq \mathcal{Z}_2^2(t)\Pi_2\mathcal{Z}_2(t),
$$

where

$$
\mathcal{Z}_1(t) = \begin{bmatrix}
\Psi(t) \\
\Psi(t-\pi(t)) \\
\Psi(t-\pi_M)
\end{bmatrix},
\mathcal{Z}_2(t) = \begin{bmatrix}
\Psi(t) \\
\Psi(t-\varphi(t)) \\
\Psi(t-\varphi_M)
\end{bmatrix},
$$

$$
\Pi_1 = \begin{bmatrix}
-R_1 & 0 & 0 \\
\mathcal{R}_1 + \mathcal{M} & -2\mathcal{R}_1 - \mathcal{M} - \mathcal{M}^T & 0 \\
-M & \mathcal{R}_1 + \mathcal{M} & -R_1
\end{bmatrix},
$$

$$
\Pi_2 = \begin{bmatrix}
-R_2 & 0 & 0 \\
\mathcal{R}_2 + \mathcal{N} & -2\mathcal{R}_2 - \mathcal{N} - \mathcal{N}^T & 0 \\
-N & \mathcal{R}_2 + \mathcal{N} & -R_2
\end{bmatrix}.
$$

According to ETM (3), it can be obtained the following:

$$
\lambda \Psi^T(t-\pi(t))\Omega \Psi(t-\pi(t)) - e^T(t)\Omega e(t) > 0.
$$

(20)

Based on the inequality (6), the constraint conditions of deception attack can be obtained as follows:

$$
\Psi^T(t-\varphi(t))F^T F\Psi(t-\varphi(t)) - F^T(\Psi(t-\varphi(t)))F(\Psi(t-\varphi(t))) > 0.
$$

(21)

Combining the above Equations (18)–(21) yields the following:

$$
\mathbb{E}\{\dot{\mathcal{V}}(t)\} \leq 2\Psi^T(t)(I_N \otimes P)\Psi^T(t) + \Psi^T(t)(Q_1 + Q_2)\Psi(t) - \Psi^T(t-\pi(t))\mathcal{Q}_1\Psi(t-\pi_M) - \Psi^T(t-\varphi_M)\mathcal{Q}_2\Psi(t-\varphi_M) + \mathcal{Z}_1^2(t)\Pi_1\mathcal{Z}_1(t) + \mathcal{Z}_2^2(t)\Pi_2\mathcal{Z}_2(t) + \mathcal{A}^T(t)\mathcal{A}(t) + e^2 \mathcal{B}^T(t)\mathcal{B}(t) + \lambda \Psi^T(t-\pi(t))\Omega \Psi(t-\pi(t)) - e^T(t)\Omega e(t) + \Psi^T(t-\varphi(t))F^T F\Psi(t-\varphi(t)) - F^T(\Psi(t-\varphi(t)))F(\Psi(t-\varphi(t)))).
$$

Define $\zeta^T(t) = [\mathcal{Z}_1^2(t), \Psi^T(t-\varphi(t)), \Psi^T(t-\varphi_M), e^T(t), F^T(\Psi(t-\varphi(t)))],$ and then applying inequality (21) and the Schur complement yields the following:

$$
\mathbb{E}\{\dot{\mathcal{V}}(t)\} \leq \zeta^T(t)\Gamma\zeta(t).
$$

(23)

According to the above analysis, the condition $\Gamma < 0$ is sufficient to guarantee $\mathbb{E}\{\dot{\mathcal{V}}(t)\} \leq 0$. Therefore, we can conclude from Equations (15) and (23) that all UAVs in the multi-UAV system can track the trajectories of the leader while forming the designed formation under the proposed control scheme. This completes the proof.

Theorem 1 provides a sufficient criterion of realizing TVFT. Based on this, the design of control gain $K$ is presented in Theorem 2.

**Theorem 2.** Suppose that Assumptions 1 and 2 hold. For given event-triggering parameter $\lambda_i$, the delay upper bound $\pi_M, \varphi_M$, scalar $\mu, \gamma_1, \gamma_2, \gamma_3$, the probability expectation of deception
attack $\varphi$, and the matrix $F$, the formation tracking error system (14) is asymptotically stable if there are positive definite matrices $\hat{P} > 0, \hat{Q}_1 > 0, \hat{Q}_2 > 0, \hat{R}_1 > 0, \hat{R}_2 > 0, \Omega > 0$ ($i = 1, 2, \ldots, N$), $X > 0, Y > 0$ and the matrices $\mathcal{M}, \mathcal{N}$ so that the following linear matrix inequalities hold:

$$\hat{\Gamma} = \begin{bmatrix}
\hat{\Gamma}_{11} & * & * & * & * \\
\hat{\Gamma}_{21} & -I & * & * & * \\
\hat{\Gamma}_{31} & 0 & Z_1 & * & * \\
\hat{\Gamma}_{41} & 0 & Z_2 & * & * \\
\hat{\Gamma}_{51} & 0 & 0 & Z_1 & * \\
\hat{\Gamma}_{61} & 0 & 0 & 0 & Z_2
\end{bmatrix} < 0, \quad (24)$$

$$\begin{bmatrix}
\hat{\mathcal{R}}_1 & * \\
\mathcal{M} & \hat{\mathcal{R}}_1
\end{bmatrix} \geq 0, \quad \begin{bmatrix}
\hat{\mathcal{R}}_2 & * \\
\mathcal{N} & \hat{\mathcal{R}}_2
\end{bmatrix} \geq 0, \quad (25)$$

where

$$\hat{\Gamma}_{11} = \begin{bmatrix}
\Phi_{11} & * & * & * & * \\
\Phi_{21} & \Phi_{22} & * & * & * \\
\Phi_{31} & \Phi_{32} & \Phi_{33} & * & * \\
\Phi_{41} & 0 & 0 & \Phi_{44} & * \\
\Phi_{51} & 0 & 0 & \Phi_{54} & \Phi_{55} \\
\Phi_{61} & 0 & 0 & 0 & 0
\end{bmatrix}, \quad \Phi_{11} = \Phi_{11} + \Phi_{11}^2, \quad \Phi_{21} = A_1X_1 + X_1^T A_1^T, \quad \Phi_{11} = \tilde{Q}_1 + \tilde{Q}_2 - \tilde{R}_1 - \tilde{R}_2,$$

$$\Phi_{21} = -Y_1^T L_1^T - \tilde{\varphi}(Y_1^T W_1^T) + \hat{\mathcal{R}}_1 + \mathcal{M}, \quad \Phi_{22} = -2\tilde{R}_1 - \mathcal{M} - \mathcal{M}^T + \Lambda(L^T \otimes I_2)\hat{\Omega}(L \otimes I_2),$$

$$\Phi_{31} = -\mathcal{M}, \quad \Phi_{32} = \hat{\mathcal{R}}_1 + \mathcal{M}, \quad \Phi_{33} = -\tilde{Q}_1 - \tilde{R}_1,$$

$$\Phi_{41} = \hat{\mathcal{R}}_2 + \mathcal{N}, \quad \Phi_{44} = -2\tilde{R}_2 - \mathcal{N} - \mathcal{N}^T,$$

$$\Phi_{51} = -\mathcal{N}, \quad \Phi_{54} = \hat{\mathcal{R}}_2 + \mathcal{N}, \quad \Phi_{55} = -\tilde{Q}_2 - \tilde{R}_2,$$

$$\Phi_{61} = -Y_1^T L_1^T - \tilde{\varphi}(Y_1^T W_1^T), \quad \Phi_{71} = \tilde{\varphi}(Y_1^T W_1^T),$$

$$\hat{\Gamma}_{21} = [0 \ 0 \ 0 \ FX_1 \ 0 \ 0 \ 0], \quad \hat{\Gamma}_{31} = [\hat{\Gamma}_{31}^1 \hat{\Gamma}_{31}^2 \hat{\Gamma}_{31}^3 \hat{\Gamma}_{31}^4 \hat{\Gamma}_{31}^5 \hat{\Gamma}_{31}^6 \hat{\Gamma}_{31}^7],$$

$$\hat{\Gamma}_{31}^1 = \pi_M A_1 X_1, \quad \hat{\Gamma}_{31}^2 = \pi_M \tilde{\varphi}(W_1 Y_1), \quad \hat{\Gamma}_{31}^3 = -\pi_M [L_1 Y_1 + \tilde{\varphi}(W_1 Y_1)],$$

$$\hat{\Gamma}_{31}^4 = [\hat{\Gamma}_{41}^1 \hat{\Gamma}_{41}^2 \hat{\Gamma}_{41}^3 \hat{\Gamma}_{41}^4 \hat{\Gamma}_{41}^5 \hat{\Gamma}_{41}^6 \hat{\Gamma}_{41}^7],$$

$$\hat{\Gamma}_{41}^1 = \tilde{\varphi}(A_1 X_1), \quad \hat{\Gamma}_{41}^2 = \tilde{\varphi}(W_1 Y_1), \quad \hat{\Gamma}_{41}^3 = -\tilde{\varphi}(L_1 Y_1 + \tilde{\varphi}(W_1 Y_1)),$$

$$\hat{\Gamma}_{51} = [0 \ \hat{\Gamma}_{51}^1 \ 0 \ 0 \ \hat{\Gamma}_{51}^2 \ -\hat{\Gamma}_{51}^3 \ \hat{\Gamma}_{51}^4],$$

$$\hat{\Gamma}_{51}^1 = [0 \ \hat{\Gamma}_{51}^1 \ 0 \ 0 \ \hat{\Gamma}_{51}^2 \ -\hat{\Gamma}_{51}^3 \ \hat{\Gamma}_{51}^4],$$

$$\hat{\Gamma}_{61} = [0 \ \hat{\Gamma}_{61}^1 \ 0 \ 0 \ \hat{\Gamma}_{61}^2 \ -\hat{\Gamma}_{61}^3 \ \hat{\Gamma}_{61}^4],$$

$$A_1 = I_N \otimes A, \quad X_1 = I_N \otimes X, \quad Y_1 = I_N \otimes Y, \quad W_1 = W \otimes B, \quad L_1 = L \otimes B,$$

$$Z_1 = -2\gamma_1 (I_N \otimes X) + \gamma_1^2 \tilde{R}_1, \quad Z_2 = -2\gamma_2 (I_N \otimes X) + \gamma_2^2 \tilde{R}_2.$$

Proof. Define $X = P^{-1} \tilde{X}, \quad \tilde{X} = \begin{bmatrix}
\tilde{X} \\
\tilde{X} \tilde{Q}_1 \tilde{X} \\
\tilde{X} \tilde{Q}_2 \tilde{X} \\
\tilde{X} \tilde{R}_1 \tilde{X} \\
\tilde{X} \tilde{R}_2 \tilde{X} \\
\tilde{X} \mathcal{M} \tilde{X} \\
\tilde{X} \mathcal{N} \tilde{X} \\
\tilde{X} \tilde{\Omega} \tilde{X} \\
\tilde{X} \Omega \tilde{X} \tilde{Y} = K \tilde{X}
\end{bmatrix},$ then we can obtain that

$$-\mathcal{R}_1^{-1} = -\tilde{X} \mathcal{R}_1^{-1} \tilde{X}, \quad -\mathcal{R}_2^{-1} = -\tilde{X} \mathcal{R}_2^{-1} \tilde{X}, \quad -I = -\tilde{X} \tilde{I} \tilde{X}. \quad (26)$$

According to $(\gamma R - P) R^{-1} (\gamma R - P) \geq 0$, where $\gamma$ is a positive real number, $R, P$ are positive definite matrix, we have the following:

$$-PR^{-1} P \leq -2\gamma P + \gamma^2 R. \quad (27)$$
Combining (26) and (27), we can obtain the following:

\[
\begin{cases}
-\hat{X}R_1^{-1}\dot{\hat{X}} \leq -2\gamma_1\dot{\hat{X}} + \gamma_1^2\dot{\bar{X}}, \\
-\hat{X}R_2^{-1}\dot{\bar{X}} \leq -2\gamma_2\dot{\bar{X}} + \gamma_2^2\dot{\bar{X}}, \\
\hat{X}\hat{X} \leq -2\gamma_3\dot{\hat{X}} + \gamma_3^2\dot{L}.
\end{cases}
\]

(28)

Pre-multiplying and post-multiplying inequalities (15) and (16) with \(\Lambda\) and \(\bar{\Lambda}\), respectively, where \(\Lambda = \text{diag}\{I_N \otimes X, I_N \otimes \dot{X}, I_N \otimes \dot{X}, I_N \otimes X, I_N \otimes X, I_N \otimes X, I, I, I, I, I\}\) and \(\bar{\Lambda} = \text{diag}\{I_N \otimes X, I_N \otimes X\}\), it is obvious that (15) and (16) are equivalent to (24) and (25). According to Theorem 1 and Equation (23), we can draw the conclusion that the goal of expected formation tracking under deception attacks is realized for system (1). Moreover, the control gain of controller (10) is \(K = YX^{-1}\). This completes the proof. □

4. Simulation Example

In the simulation, we construct a multi-UAV system composed of four UAVs and a virtual leader described by Equation (1). As stated in Remark 1, each UAV in the multi-UAV system is deemed as a particle, and only the trajectory-loop control of UAV \(i\) is studied to achieve the expected formation tracking control for the multi-UAV systems [2,54].

The communication topology is exhibited in Figure 2, which describes the information sharing among the UAVs and the leader in the multi-UAV systems. From Figure 2, one has the Laplacian matrix and adjacency matrix as follows:

\[
L = \begin{bmatrix}
0 & 0 & 0 & 0 \\
-1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & -1 & 1 \\
\end{bmatrix},
\]

\[
W = \begin{bmatrix}
0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
\end{bmatrix}.
\]

The initial states are chosen as follows:

\[
x_0 = [0 \ 0 \ 0 \ 0]^T, x_1 = [-20 \ 10 \ 0 \ 0]^T, x_2 = [20 \ -20 \ 0 \ 0]^T,
\]

\[
x_3 = [-20 \ 20 \ 0 \ 0]^T, x_4 = [15 \ 15 \ 0 \ 0]^T.
\]

The deception attack \(f(\Psi(t))\) \((i = 1, 2, 3, 4)\) is set as the following:

\[
f(\Psi(t)) = \begin{bmatrix}
-tanh(0.15\Psi_{ix}(t)) \\
tanh(0.3\Psi_{ix}(t))
\end{bmatrix}.
\]

We set \(F = \text{diag}\{0.15, 0.3\}\), which means that the condition (6) can be guaranteed.

Next, considering the random property of the deception attacks, two possible cases of different values of \(\varpi(t)\) are given in this section.

**Case 1:** The probability of deception attack occurrence is \(\varpi = 0.2\). Let \(\varpi_M = 0.2, \theta_M = 0.1, h = 0.01\), the scalars \(\gamma_1 = \gamma_2 = \gamma_3 = 1, \mu = 0.1, \lambda_1 = 0.01, \lambda_2 = 0.02, \lambda_3 = 0.015, \lambda_4 = 0.025\). Through solving the LMI in Theorem 2 by MATLAB, the following triggering parameters and control gain are obtained:

\[
\begin{align*}
\Omega_1 &= \begin{bmatrix}
0.1635 & 0.3702 \\
0.3702 & 1.2485
\end{bmatrix}, \\
\Omega_2 &= \begin{bmatrix}
0.2008 & 0.4793 \\
0.4793 & 1.5662
\end{bmatrix}, \\
\Omega_3 &= \begin{bmatrix}
0.1549 & 0.3506 \\
0.3506 & 1.2018
\end{bmatrix}, \\
\Omega_4 &= \begin{bmatrix}
0.2009 & 0.4829 \\
0.4829 & 1.5835
\end{bmatrix}, \\
K &= \begin{bmatrix}
0.3579 \\
1.0710
\end{bmatrix}.
\end{align*}
\]

The simulation results are shown by Figures 3–11. The formation tracking position error \(\Psi_{ix}\) is exhibited by Figures 3 and 4, respectively, which show that the control system performs well in this case. The varying formations at \(t = 30, 40, 50, 60\) s are pre-
sented in Figure 5, from which it can be observed that the four UAVs realize the desired time-varying square formation with rotating around and tracking the trajectories of the leader. Figures 6–9 represent the release time intervals of four UAVs, respectively. It can be seen in Figures 6–9 that a large amount sampled data are abandoned by utilizing the proposed ETM, which implies that the network communication burden is alleviated effectively. Figures 10 and 11 represent the control input of four UAVs on the X- and Y-axes, respectively.

**Figure 2.** The communication graph.

**Case 2:** In this case, \( \bar{\omega} \) is set as \( \bar{\omega} = 0.5 \). In addition, the other parameters in this simulation case are chosen as the same as those in Case 1. According to Theorem 2, the triggering parameters and control gain are calculated as follows:

\[
\Omega_1 = \begin{bmatrix} 0.1292 & 0.2148 \\ 0.2148 & 0.6170 \end{bmatrix}, \quad \Omega_2 = \begin{bmatrix} 0.1562 & 0.2810 \\ 0.2810 & 0.7759 \end{bmatrix}, \\
\Omega_3 = \begin{bmatrix} 0.1264 & 0.2104 \\ 0.2104 & 0.6092 \end{bmatrix}, \quad \Omega_4 = \begin{bmatrix} 0.1553 & 0.2810 \\ 0.2810 & 0.7782 \end{bmatrix}, \\
K = \begin{bmatrix} 0.4496 & 1.0639 \end{bmatrix}.
\]

The simulation results in Case 2 are shown in Figures 12 and 13, which depict the formation position tracking errors \( \Psi_{ix}, i = 1, 2, 3, 4 \). It can be observed that \( \Psi_{ix} \) converges to the origin about 20 s, even when the probability of the deception attack occurrence is 0.5 in Figures 12 and 13.

**Figure 3.** Responses of \( \Psi_{ix} \) on X-axis.
Furthermore, to show the superiority of the proposed ETM, a comparative simulation is conducted between the TTM and our proposed ETM based formation control under deception attacks. The simulation results are shown by Table 1, which presents the average numbers of released data packets of four UAVs on X- and Y-axes with sampling period $h = 0.01$ under ETM and TTM, respectively. From Table 1, it can be observed that the average numbers of released data packets under the proposed ETM are significantly fewer than those under TTM, which indicates that the proposed ETM-based formation control scheme in this paper can effectively alleviate network burden.

Figure 4. Responses of formation tracking error on Y-axis.

Figure 5. Position of four UAVs and the leader at $t = 30, 40, 50, 60s$. 
Figure 6. Triggering instants of UAV 1.

Figure 7. Triggering instants of UAV 2.

Figure 8. Triggering instants of UAV 3.
Figure 9. Triggering instants of UAV 4.

Figure 10. Control inputs of the four UAVs on X-axis.

Figure 11. Control inputs of the four UAVs on Y-axis.
Figure 12. Responses of $\Psi_{ix}$ on X-axis.

Figure 13. Responses of $\Psi_{iy}$ on Y-axis.

Table 1. The average number of released data packets of four UAVs on X- and Y-axes.

|       | On X-Axis | On Y-Axis |
|-------|-----------|-----------|
| ETM   | 151.5     | 174.25    |
| TTM   | 6001      | 6001      |

Consequently, the ETM designed in this paper leads to less data released into the network and saves network resources. Meanwhile, the multi-UAV systems subjected to deception attacks is able to realize the desired TVFT by utilizing the proposed formation control scheme.

5. Conclusions

In this paper, we propose a novel event-triggered formation tracking control scheme for multi-UAV systems subjected to deception attacks. A novel ETM is put forward to alleviate the communication burden, in which the information of both the leader and the formation is involved in the triggering condition. To deal with the problems of limited network bandwidth and insecure control for the wireless networked multi-UAV systems,
a novel formation control strategy is developed for multi-UAV systems subjected to deception attacks. Under this strategy, the desired formation tracking for multi-UAV systems with deception attacks can be guaranteed, and the burden of the network can be reduced. Finally, two simulation examples with different probabilities of deception attack occurrence and a comparative simulation are conducted to verify the validity and superiority of the presented control scheme. The future work aims to propose an adaptive ETM-based control strategy to improve communication efficiency.

Author Contributions: Conceptualization, T.X. and Z.G.; methodology, B.S.; software, T.X.; validation, Z.G., T.X. and B.S.; formal analysis, B.S.; investigation, B.S.; resources, T.X.; writing—original draft preparation, B.S.; writing—review and editing, T.X.; visualization, T.X.; supervision, Z.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by National Natural Science Foundation of China Grant No.52005266 and No.62103193.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lin, Z.; Wang, L.; Han, Z.; Fu, M. Distributed formation control of multi-agent systems using complex laplacian. IEEE Trans. Autom. Control 2014, 59, 1765–1777. [CrossRef]
2. Dong, X.; Hua, Y.; Zhou, Y.; Ren, Z.; Zhong, Y. Theory and experiment on formation-containment control of multiple multrotor unmanned aerial vehicle systems. IEEE Trans. Autom. Sci. Eng. 2019, 16, 229–240. [CrossRef]
3. Zhang, J.; Yan, J.; Zhang, P. Multi-uav formation control based on a novel back-stepping approach. IEEE Trans. Veh. Technol. 2020, 69, 2437–2448. [CrossRef]
4. Xiong, T.; Gu, Z. Observer-based adaptive fixed-time formation control for multi-agent systems with unknown uncertainties. Neurocomputing 2021, 423, 506–517. [CrossRef]
5. Xiong, T.; Pu, Z.; Yi, J.; Tao, X. Fixed-time observer based adaptive neural network time-varying formation tracking control for multi-agent systems via minimal learning parameter approach. IET Control Theory Appl. 2020, 14, 1147–1157. [CrossRef]
6. Dong, X.; Zhou, Y.; Ren, Z.; Zhong, Y. Time-varying formation tracking for second-order multi-agent systems subjected to switching topologies with application to quadrotor formation flying. IEEE Trans. Ind. Electron. 2016, 64, 5014–5024. [CrossRef]
7. Wang, R.; Dong, X.; Li, Q.; Ren, Z. Distributed time-varying formation control for multiagent systems with directed topology using an adaptive output-feedback approach. IEEE Trans. Ind. 2019, 15, 4676–4685. [CrossRef]
8. Wang, R.; Dong, X.; Li, Q.; Ren, Z. Distributed time-varying output formation control for general linear multiagent systems with directed topology. IEEE Trans. Control Netw. Syst. 2019, 6, 609–620. [CrossRef]
9. Wang, Z.; Zhuang, Z.; Liu, Y.; Ding, F.; Tang, M. Color Classification and Texture Recognition System of Solid Wood Panels. Forests. 2021, 12, 1154. [CrossRef]
10. Yue, D.; Won, S. Delay-dependent robust stability of stochastic uncertain systems with time delay and markovian jump parameters. Circuits Syst. Signal Process. 2003, 22, 351–365. [CrossRef]
11. Li, X.; Dong, X.; Li, Q.; Ren, Z. Event-triggered time-varying formation control for general linear multi-agent systems. J. Franklin Inst. 2019, 356, 10179–10195. [CrossRef]
12. Gu, Z.; Park, J.H.; Yue, D.; Wu, Z.-G.; Xie, X. Event-triggered security output feedback control for networked interconnected systems subject to cyber-attacks. IEEE Trans. Syst. Man Cybern. 2020, 51, 6197–6206. [CrossRef]
13. Gu, Z.; Shi, P.; Yue, D. An adaptive event-triggering scheme for networked interconnected control system with stochastic uncertainty. Int. J. Robust Nonlinear Control. 2017, 27, 236–251. [CrossRef]
14. Hu, S.; Yue, D.; Yin, X.; Xie, X.; Ma, Y. Adaptive event-triggered control for nonlinear discrete-time systems. Int. J. Robust Nonlinear Control 2016, 26, 4104–4125. [CrossRef]
15. Li, J.; Li, C.; Yang, X.; Chen, W. Event-triggered containment control of multi-agent systems with high-order dynamics and input delay. Electronics 2018, 7, 343. [CrossRef]
16. Kwon, W.; Baek, J. Novel summation-type triggering condition on event-based memory output feedback control for networked control systems. Electronics 2020, 9, 779. [CrossRef]
17. Zheng, B.-C.; Fei, S.; Liu, X. Event-triggered and memory-based sliding mode variable structure control for memristive systems. Electronics 2018, 7, 253. [CrossRef]
18. Yang, J.; Xiao, F.; Chen, T. Event-triggered formation tracking control of nonholonomic mobile robots without velocity measurements. Automatica 2020, 112, 108671. [CrossRef]
19. Yin, X.; Yue, D.; Hu, S.; Zhang, H. Distributed adaptive model-based event-triggered predictive control for consensus of multiagent systems. Int. J. Robust Nonlinear Control 2018, 28, 6180–6201. [CrossRef]
20. Yue, D.; Tian, E.; Han, Q.-L. A delay system method for designing event-triggered controllers of networked control systems. IEEE Trans. Autom. Control 2012, 58, 475–481. [CrossRef]
21. Liu, J.; Wei, L.; Xie, X.; Tian, E.; Fei, S. Quantized stabilization for t-s fuzzy systems with hybrid-triggered mechanism and stochastic cyber-attacks. *IEEE Trans. Fuzzy Syst.*, 2018, 26, 3820–3834. [CrossRef]

22. Ye, D.; Chen, M.; Yang, H. Distributed adaptive event-triggered fault-tolerant consensus of multiagent systems with general linear dynamics. *IEEE Trans. Cybern.*, 2018, 49, 757–767. [CrossRef]

23. Tian, E.; Peng, C. Memory-based event-triggering $H\infty$ load frequency control for power systems under deception attacks. *IEEE Trans. Cybern.*, 2020, 50, 4610–4618. [CrossRef]

24. Zhang, J.; Zhang, H.; Cai, Y.; Wang, W. Consensus control for nonlinear multi-agent systems with event-triggered communications. *Appl. Math. Comput.*, 2021, 408, 126341.

25. Zhang, A.; Zhou, D.; Yang, P.; Yang, M. Event-triggered finite-time consensus with fully continuous communication free for second-order multi-agent systems. *Int. J. Control. Autom. Syst.*, 2019, 17, 836–846. [CrossRef]

26. Gu, Z.; Yue, D.; Tian, E. On designing of an adaptive event-triggered communication scheme for nonlinear networked interconnected control systems. *Inf. Sci.*, 2018, 422, 257–270. [CrossRef]

27. Hu, S.; Yue, D.; Chen, X.; Cheng, Z.; Xie, X. Resilient $H\infty$ filtering for event-triggered networked systems under nonperiodic dos jamming attacks. *IEEE Trans. Syst. Man Cybern. Syst.*, 2019, 51, 1392–1403. [CrossRef]

28. Liu, J.; Wang, Y.; Cao, J.; Yue, D.; Xie, X. Secure adaptive-event-triggered filter design with input constraint and hybrid cyber attack. *IEEE Trans. Cybern.*, 2021, 51, 4000–4010. [CrossRef]

29. Peng, C.; Yue, D.; Yang, T.-C.; Tian, E.G. On delay-dependent approach for robust stability and stabilization of t-s fuzzy systems with constant delay and uncertainties. *IEEE Trans. Fuzzy Syst.*, 2009, 17, 1143–1156. [CrossRef]

30. Peng, C.; Han, Q.-L.; Yue, D. Communication-delay-distribution-dependent decentralized control for large-scale systems with ip-based communication network. *IEEE Trans. Control Syst. Technol.*, 2013, 21, 820–830. [CrossRef]

31. Yang, Y.; Yue, D.; Xue, Y. Decentralized adaptive neural output feedback control of a class of large-scale time-delay systems with input saturation. *J. Frankl. Inst.*, 2015, 352, 2129–2151. [CrossRef]

32. Xie, X.; Yue, D.; Zhang, H.; Xue, Y. Fault estimation observer design for discrete-time takagi–sugeno fuzzy systems based on homogeneous polynomially parameter-dependent lyapunov functions. *IEEE Trans. Cybern.*, 2017, 47, 2504–2513. [CrossRef]

33. Gu, Z.; Sun, X.; Lam, H.-K.; Yue, D.; Xie, X. Event-based secure control of t-s fuzzy based 5-dof active semi-vehicle suspension systems subject to dos attacks. *IEEE Trans. Cybern.*, 2021. to be published. [CrossRef]

34. Gu, Z.; Ahn, C.K.; Yue, D.; Xie, X. Event-triggered $H\infty$ filtering for t-s fuzzy-model-based nonlinear networked systems with multisensors against dos attacks. *IEEE Trans. Cybern.*, 2020. to be published. [CrossRef] [PubMed]

35. Yan, S.; Gu, Z.; Nguang, S.K. Memory-event-triggered $H\infty$ output control of neural networks with mixed delays. *IEEE Trans. Neural Netw. Learn. Syst.*, 2021. to be published. [CrossRef] [PubMed]

36. Zhang, M. Tracking control for unmanned aerial vehicles with time-delays based on event-triggered mechanism. *J. Control Eng. Appl. Inf.*, 2019, 21, 12–19.

37. Zhang, D.; Ling, R.; Wang, Q.; Yu, L.; Feng, Y. Sensor-network-based distributed stabilization of nonlinear large-scale systems with energy constraints and random sensor faults. *J. Frankl. Institute*, 2015, 352, 3345–3365. [CrossRef]

38. Gu, Z.; Shi, P.; Yue, D.; Yan, S.; Xie, X. Memory-based continuous event-triggered control for networked t-s fuzzy systems against cyber-attacks. *IEEE Trans. Fuzzy Syst.*, 2020, 29, 3118–3129. [CrossRef]

39. Hu, S.; Yue, D.; Han, Q.-L.; Xie, X.; Chen, X.; Dou, C. Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks. *IEEE Trans. Cybern.*, 2019, 50, 1952–1964. [CrossRef]

40. Sun, H.; Peng, C.; Zhang, W.; Yang, T.; Wang, Z. Security-based resilient event-triggered control of networked control systems under denial of service attacks. *J. Frankl. Inst.*, 2019, 356, 10277–10295. [CrossRef]

41. Ye, D.; Zhang, T.-Y.; Guo, G. Stochastic coding detection scheme in cyber-physical systems against replay attack. *Inf. Sci.*, 2019, 481, 432–444. [CrossRef]

42. Wang, H.; Ying, Y.; Lu, R.; Xue, A. Network-based $H\infty$ control for singular systems with event-triggered sampling scheme. *Inf. Sci.*, 2016, 329, 540–551. [CrossRef]

43. Ding, D.; Wang, Z.; Ho, D.W.; Wei, G. Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks. *Automatica*, 2017, 78, 231–240. [CrossRef]

44. Han, F.; Dong, H.; Wang, Z.; Li, G. Local design of distributed $H\infty$-consensus filtering over sensor networks under multiplicative noises and deception attacks. *Int. J. Robust Nonlinear Control*, 2019, 29, 2296–2314. [CrossRef]

45. Zhang, D.; Liu, L.; Feng, G. Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and dos attack. *IEEE Trans. Cybern.*, 2018, 49, 1501–1511. [CrossRef] [PubMed]

46. Porter, M.; Hespanhol, P.; Aswani, A.; Johnson-Roberson, M.; Vasudevan, R. Detecting generalized replay attacks via time-varying dynamic watermarking. *IEEE Trans. Autom. Control*, 2020, 66, 3502–3517. [CrossRef]

47. Zhang, D.; Wang, Q.; Feng, G.; Shi, Y.; Vasilakos, A.V. A survey on attack detection, estimation and control of industrial cyber–physical systems. *Int. J. Syst. Sci.*, 2021, 11, 1–16. [CrossRef]

48. Yao, W.; Nan, J.; Zhao, Y.; Fang, J.; Ai, X.; Zuo, W.; Wen, J.; Cheng, S. Resilient wide-area damping control for inter-area oscillations to tolerate deception attacks. *IEEE Trans. Smart Grid*, 2021, 12, 4238–4249. [CrossRef]

49. Rong, N.; Wang, Z. Event-based impulsive control of it2 t-s fuzzy interconnected system under deception attacks. *IEEE Trans. Fuzzy Syst.*, 2021, 29, 1615–1628. [CrossRef]
50. Yoo, S.J. Neural-network-based adaptive resilient dynamic surface control against unknown deception attacks of uncertain nonlinear time-delay cyberphysical systems. *IEEE Trans. Neural Netw. Learn. Syst.* 2020, 31, 4341–4353. [CrossRef]
51. Gu, Z.; Zhou, X.; Zhang, T.; Yang, F.; Shen, M. Event-triggered filter design for nonlinear cyber–physical systems subject to deception attacks. *ISA Trans.* 2020, 104, 130–137. [CrossRef] [PubMed]
52. Cui, Y.; Liu, Y.; Zhang, W.; Alsaadi, F.E. Sampled-based consensus for nonlinear multiagent systems with deception attacks: The decoupled method. *IEEE Trans. Syst. Man Cybern. Syst.* 2021, 51, 561–573. [CrossRef]
53. Wang, W.; Han, Z.; Liu, K.; Lü, J. Distributed adaptive resilient formation control of uncertain nonholonomic mobile robots under deception attacks. *IEEE Trans. Circuits Syst. Regul. Pap.* 2021, 68, 3822–3835. [CrossRef] [PubMed]
54. Wei, L.; Chen, M.; Li, T. Dynamic event-triggered cooperative formation control for uavs subject to time-varying disturbances. *IET Control Appl.* 2020, 14, 2514–2525. [CrossRef]
55. Xiong, T.; Gu, Z.; Yi, J.; Pu, Z. Fixed-time adaptive observer-based time-varying formation control for multi-agent systems with directed topologies. *Neurocomputing* 2021, 463,483–494. [CrossRef]
56. Liu, J.; Yin, T.; Cao, J.; Yue, D.; Karimi, H.R. Security control for ts fuzzy systems with adaptive event-triggered mechanism and multiple cyber-attacks. *IEEE Trans. Syst. Man Cybern. Syst.* 2021, 51, 6544–6554. [CrossRef]
57. Liu, J.; Gu, Y.; Xie, X.; Yue, D.; Park, J.H. Hybrid-driven-based $H_\infty$ control for networked cascade control systems with actuator saturations and stochastic cyber attacks. *IEEE Trans. Syst. Man Cybern. Syst.* 2019, 49, 2452–2463. [CrossRef]
58. Liu, J.; Gu, Y.; Zha, L.; Liu, Y.; Cao, J. Event-triggered $H_\infty$ load frequency control for multiarea power systems under hybrid cyber attacks. *IEEE Trans. Syst. Man Cybern. Syst.* 2019, 49, 1665–1678. [CrossRef]
59. Zhou, X.; Gu, Z.; Yang, F. Resilient event-triggered output feedback control for load frequency control systems subject to cyber attacks. *IEEE Access* 2019, 7, 58951–58958. [CrossRef]