Security and Safety, Vol. 2, 2023017 (2023)
https://doi.org/10.1051/sands/2023017
sands.edpsciences.org

Security and Safety in Unmanned Systems

Research Article

OPEN ACCESS

Industrial Control

Event-triggered resilient consensus control of multiple unmanned systems against periodic DoS attacks based on state predictor

Haichuan Yang[1], Ziquan Yu[1], and Youmin Zhang[2,*]

[1] *College of Automation Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China*

[2] *Department of Mechanical, Industrial and Aerospace Engineering, Concordia University, Montreal, Quebec H3G 1M8, Canada*

Received: 30 January 2023 / Revised: 26 April 2023 / Accepted: 28 June 2023 / Published online: 23 August 2023

Abstract This paper develops an event-triggered resilient consensus control method for the nonlinear multiple unmanned systems with a data-based autoregressive integrated moving average (ARIMA) agent state prediction mechanism against periodic denial-of-service (DoS) attacks. The state predictor is used to predict the state of neighbor agents during periodic DoS attacks and maintain consistent control of multiple unmanned systems under DoS attacks. Considering the existing prediction error between the actual state and the predicted state, the estimated error is regarded as the uncertainty system disturbance, which is dealt with by the designed disturbance observer. The estimated result is used in the design of the consistent controller to compensate for the system uncertainty error term. Furthermore, this paper investigates dynamic event-triggered consensus controllers to improve resilience and consensus under periodic DoS attacks and reduce the frequency of actuator output changes. It is proved that the Zeno behavior can be excluded. Finally, the resilience and consensus capability of the proposed controller and the superiority of introducing a state predictor are demonstrated through numerical simulations.

Keywords Multiple unmanned systems, denial-of-service, event-triggered, consensus control, state predictor

Citation Yang H, Yu Z and Zhang Y. Event-triggered resilient consensus control of multiple unmanned systems against periodic DoS attacks based on state predictor. Security and Safety 2023; **2**: 2023017. https://doi.org/10.1051/sands/2023017

1 Introduction

Multiple unmanned systems are gradually replacing human work in many fields such as collaborative task execution, large-scale environmental monitoring, and high-risk industry work due to their advantages of high efficiency, intelligence, security, and strong scalability [1, 2]. In order to improve the collaboration capability and security of unmanned systems, extensive research has been carried out on the consensus control of unmanned systems, which has become a hot spot in recent years [3]. Consensus control is the basis of unmanned systems cooperative formation control. The key to consensus is the information interaction between unmanned systems. However, as the scale of unmanned systems deployment expands, the communication network between agents will become complex. Therefore, the shortcomings of the unmanned system network vulnerabilities will gradually be exposed.

* Corresponding author (email: ymzhang@encs.concordia.ca)

In the applications of the control systems *via* networks, cyberattacks can disrupt network connections on a large scale, which degrades the execution efficiency of the cyber system and even causes task failure. Cybersecurity has attracted more and more attention in the field of automatic control [4, 5]. Considering the followers with the unmodeled dynamics in the communication network, a fully distributed adaptive control strategy is designed in [6] based on neural networks for achieving the followers synchronized to the leader. For guaranteeing the cyber security of the unmanned system under network attacks, using resilient control methods to ensure security has become an important research direction [7]. In the network control system, network attacks refer to attacks on the controlled object at the network level. They can illegally hinder and damage the information interaction in the unmanned system network. It includes two main types of cyberattacks, denial-of-service (DoS) attacks and deception attacks [8]. In this paper, the distributed event-triggered resilient consensus control is investigated for unmanned systems against periodic DoS attacks.

DoS is one of the common types of cyberattacks, which has been widely studied [9]. The purpose of the DoS attack is to destroy the network link between neighboring agents and disconnect the information exchange, thereby hindering the consensus of the unmanned system. DoS attacks can have devastating effects on the unmanned system, which reflect the urgent need to solve the DoS attack problem. In [10], an asynchronous DoS description model is proposed, which is close to the network attacks that occur in reality. In [11], a periodic DoS attack model is introduced into the output feedback control of cyber-physical systems and can be easily combined with asynchronous attacks on different channels. In [3] the transmission nonlinearities with gain and bias in the network link are considered for the leader-following consensus problem of multi-agent systems. The consensus can be achieved by designing distributed adaptive control schemes. The research scenario is similar to cyber-attacks.

Considering with distributed and resilient control of the unmanned systems against DoS attacks, linear systems were mainly used as investigated objects in the early stage [12]. In this field, robust control methods were the main measures to resist DoS attacks. For resilient control of linear systems, the linear matrix inequality (LMI) method is a tool for solving the feedback controller parameters [13, 14]. However, practical unmanned systems are nonlinear dynamic models such that linear control methods are not applicable in most cases. In addition, the input-to-state stable (ISS) control methods are widely used to study the resilient control method against DoS attacks [15, 16]. But for many nonlinear unmanned systems, the ISS stability condition is difficult to satisfy. Recently, more and more researchers focus on the resilient control of nonlinear unmanned systems [17, 18]. Recently, type-2 fuzzy logic systems are widely used for dynamic model transformation. In [19], based on the type-2 fuzzy logic system approximating the unknown smooth function. A distributed adaptive supervisory control method is proposed in the paper. Although excellent control performance is obtained in these papers, the stability of the system cannot be guaranteed during a cyberattack due to the broken feedback loop.

Recently, event-triggered control is one of the hotspots in the field of network attack resilient control [20]. Event-triggered control aims to decrease the waste of communication resources for agents and reduce the frequency of controller updates [21, 22]. Through the action of the event-triggered mechanism (ETM), the feedback control loop will be closed when the state of the agent exceeds the designed event-triggered setting threshold [12, 23]. The controller output will not change until the conditions for triggering the next event are met. When a DoS attack occurs, the ETM works and the actuator of the agent maintains a constant output state until the network attack disappears. Although the control performance will be reduced, the stability of the system can be guaranteed. In the field of consensus control, a large number of applications combine distributed control with ETM. In [24], based on dynamic ETM, a distributed control protocol is proposed to ensure the consensus of linear agents. Due to the Zeno behavior in the ETM, it can be excluded by presetting the minimum trigger interval [25].

The core issue of defending against cyberattacks is to maintain the stability of the system under attacks and to quickly recover consensus after the attacks. Although some switching control methods can be introduced into resilient control to mitigate the effect of DoS attacks [26, 27], they must rely on system model features and reference commands. Furthermore, the feedback loop is still broken under DoS attacks. In order to maintain the feedback loop, some scholars use the method of state holding or safety observer to reconstruct virtual reference information [28, 29].

However, the observer can only obtain the last information of the neighbor agents before the attack in practical application situations. Model-based observers will not be able to obtain a satisfactory estimate if the state of the neighbor agents is variable. Many existing methods of state predictors have been developed

for dealing with communication transmission issues. In [30], for the power system, an optimal wide-area controller is designed with the state predictor for compensating the error caused by transport lags. In [31], a predictor-based extended-state-observer is designed for estimating the state of neighbor agents. A leader-follower consensus protocol is proposed against communication delays and disturbances efficiently. Considering data-based prediction methods, an active communication delay compensation mechanism with a data-driven state predictor is proposed in [32] to estimate the current states of neighbor agents using the delayed state information. Combined with the prescribed performance method and neural networks, a kind of back-stepping control method is developed for autonomous underwater vehicle formation control. Many existing methods have been developed related to the state predictor for compensating communication delays. However, many existing states predicted methods rely on the model of agents and do not involve the resilient control method against cyber-attacks. The autoregressive integrated moving average (ARIMA) model [33] is widely used for trend and data prediction. Many predicting methods related to ARIMA have been proposed for applications [34–36]. Compared with other data-based intelligent prediction methods, ARIMA has the advantage that it does not require pre-training. Therefore, real-time predictions can be made using historical data.

Motivated by the above existing works, combined with the ETM and the resilient control method, a distributed control method is proposed for the unmanned systems against the periodic asynchronous multi-channel DoS attacks. ARIMA is introduced into the control scheme to predict the state information of the neighbor unmanned system in real-time during DoS attacks. The prediction mechanism will play a key role when the communication network suffers from DoS attacks. The main contributions of this paper are summarized as follows.

1. Compared with the existing work of ARIMA to classify network attacks [37], this is different from the research field of this paper. Aiming at the issue that the feedback loop is broken by the DoS attacks, to the best of the authors' knowledge, the proposed data-based state predictor is introduced for the first time into the model-based resilient control against the DoS attacks in this paper.
2. Since ARIMA is a data-based state prediction method, it is difficult to prove the convergence of differences between the real state and predicting state for unmanned systems. In this paper, a disturbance observer is proposed to estimate the uncertain disturbance of the system caused by state estimation.
3. Comparing with the existing works related to ETM and resilient control against DoS attacks, a control scheme is proposed for a nonlinear unmanned system to guarantee the system consensus under the periodic DoS attack. Besides, the dynamic ETM is designed to reduce the actuator triggering frequency.

The paper structure is arranged as follows. The preliminaries about the unmanned systems model, graph theory, the DoS attack model, and the proposed ARIMA prediction method are shown in Section 2. The main results related to the proposed ETM, disturbance observer, and resilient controller are proposed in Section 3. Further, the simulation has been carried out to verify the resilient capacity against DoS attacks of the proposed method in Section 4. Finally, the conclusion of the paper is given in Section 5.

2 Preliminaries and problem statement

2.1 Unmanned system model description

Consider using the following typical second-order dynamic system to describe a single agent to constitute the unmanned system

$$\begin{cases} \dot{x}_1(t) = F_1 + G_1 x_2(t) \\ \dot{x}_2(t) = F_2 + G_2 u(t) \end{cases} \tag{1}$$

where $x_1(t) \in \mathbb{R}^n$ and $x_2(t) \in \mathbb{R}^n$ represent the dynamic state of an individual in the unmanned system. In this paper, the individual in unmanned systems is named an agent. $u(t)$ is the control signal of the agent. F_1, G_1, F_2, and G_2 reflect the dynamics characteristics of the agent. F_1 and F_2 are the nonlinear differentiable terms correlating with the dynamic of the agent. G_1 and G_2 are the nonlinear control input matrices for the agent, defined by the physical parameters of the system. G_1 and G_2 are bounded and nonsingular, rendering the agent dynamics controllable.

2.2 Preliminaries for graph theory

The set of agents can be defined as the virtual nodes v_N. Furthermore, the set can be described as $\mathcal{V} = (v_1, v_2, \ldots, v_N)$. The edge set can be denoted as $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$. $\mathcal{A} = [a_{ij}] \in R^{N\times N}$ is the adjacency matrix. If $e_{ij} = (v_i, v_j) \in \mathcal{E}$, there is $a_{ij} = 1$. It means that agent i can acquire the information from the agent j, otherwise, $a_{ij} = 0$. It is noticed that $a_{ij}(t_0) = 0$ will exist constrainedly when the edge e_{ij} suffers from a DoS attack at t_0. The interaction communication among agents can be described as the directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$. Define the degree matrix $\mathcal{D} = \mathrm{diag}(d_i) \in R^{N\times N}$, where $d_i = \sum_{j=1}^{N} a_{ij}$. There is the Laplacian matrix $\mathcal{L} = \mathcal{D} - \mathcal{A}$.

Consider introducing the reference command into the unmanned system, which can be defined as a virtual node v_N. The adjacency matrix is defined as $\left[a'_{ij}\right] \in R^{(N-1)\times(N-1)}$ for $N-1$ agents. The augmented adjacency matrix $\bar{\mathcal{A}}$ including the virtual command can then be described as

$$\bar{\mathcal{A}} = \begin{bmatrix} \left[a'_{ij}\right] & {\beta_i}^T \\ 0^{1\times(N-1)} & 0^{1\times 1} \end{bmatrix} \tag{2}$$

where $\beta_i \in R^{1\times(N-1)}$ represents that the information transfers from the virtual node to the following agents. There is no information transmitted from followers to the virtual node. Therefore, the last row of the matrix $\bar{\mathcal{A}}$ is the zero vector. In addition, the element in $\bar{\mathcal{A}}$ including β_i is defined as $\bar{a}_{ij} \in R^{N\times N}$. The initial directed graph $\bar{\mathcal{G}} = \left(\bar{\mathcal{V}}, \bar{\mathcal{E}}, \bar{\mathcal{A}}\right)$ denotes the communication relationship of the unmanned systems, where $\bar{\mathcal{V}} = (v_1, v_2, \ldots, v_N)$ denotes the nodes set including followers and the virtual node, and $\bar{\mathcal{E}} \subseteq \bar{\mathcal{V}} \times \bar{\mathcal{V}}$. For satisfying resilient controller design requirements, assumed that the original communication topology is the strong connection, which will suffer from the DoS attack to affect the information interaction. DoS attacks would be discussed and dealt with in the following sections. Moreover, it is necessary for each agent to have access to at least one neighboring agent to receive consensus reference information related to the virtual node.

Assumption 1. *[6] For the communication relationship of unmanned systems, the graph $\bar{\mathcal{G}}$ has a spanning tree. The virtual lead node is the root node with no incoming edges from the followers, and at least one follower can get the information of the leader.*

2.3 DoS attacks model

For the periodic DoS attacks, a period can be described as T_n, with $T_n \geqslant 0$, including a duration of DoS-on and duration of DoS-off. By defining the attack period as $T_p = T_{i+1} - T_i$, the attack duration can be denoted as T_d, with the initial time h_n. The attack rate is $F_a = T_d/T_p$.

For the periodic DoS attacks, the attack sequence can be described as follows:

$$H_n = [h_n, h_n + T_d). \tag{3}$$

The sets of DoS-on and DoS-off on each channel can be described as $\mathcal{T}(T_i)$ and $\bar{\mathcal{T}}(T_i)$,

$$\begin{aligned} \mathcal{T}(T_i) &= \bigcup_{n\in\mathbb{N}_0} H_n \cap T_i \\ \bar{\mathcal{T}}(T_i) &= T_i \backslash \mathcal{T}(T_i). \end{aligned} \tag{4}$$

According to the description of the DoS attacks model by (4), a kind of periodic DoS attack sequence on a channel is shown as follows.

As shown in Figure 1, a new period of DoS begins with T_n at a DoS-off moment. The network attack DoS-on lasts for T_d, which is represented by the gray region. The period of the DoS attack is T_p.

2.4 Agent states predictor under DoS attacks

In this paper, for predicting the states of agents under DoS attacks, the ARIMA model is used to design the state predictor. The model can be described as

$$x_t^p = \epsilon + \varepsilon_t + \sum_{i=1}^{p} a_i x_{t-i} + \sum_{i=1}^{q} b_i \varepsilon_{t-i} \tag{5}$$

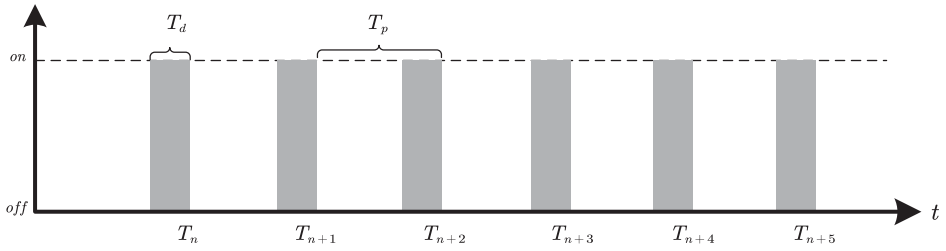


Figure 1. A classical periodic DoS attack

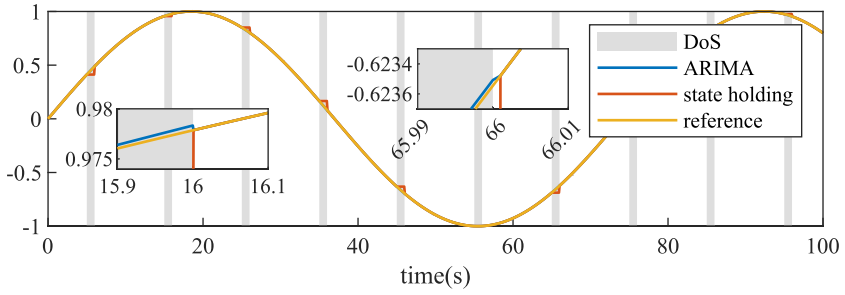


Figure 2. Comparison of the two methods for state prediction

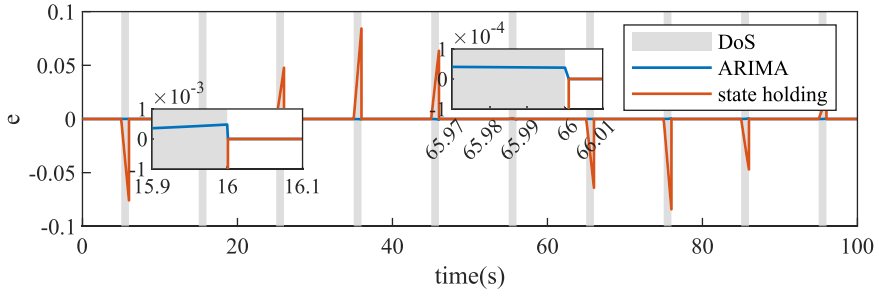


Figure 3. State prediction error of two methods

where ϵ is the estimation constant term. ε_t is the estimation error sequence. p and q represent the autoregressive number and moving average number in ARIMA, respectively. a and b are the autocorrelation and partial autocorrelation coefficients, respectively.

The states of unmanned systems can be estimated recursively by historical data. In addition, the prerequisite for the effectiveness of ARIMA is that the estimated agent should not be an "anti-predictive behavior". Considering the consensus control of the unmanned system with the limitation of kinematic characteristics, it is assumed that there is a cooperative relationship between unmanned systems. Assumed that under the control of reference commands, large state changes, such as highly dynamic behaviors, would not be undergone by the cooperative unmanned systems during DoS attacks. The prerequisite is satisfied.

As a numerical simulation, define $p = 2$ and $q = 2$. The historical state is used to predict the future state during DoS attacks. Compared with state holding, the prediction ability of ARIMA is shown in the following figures.

Figures 2 and 3 show the prediction ability of ARIMA. By using a sine signal as the simulated state, the error is much less than that of state holding. Therefore, this paper uses the ARIMA as the predictor for the agent state against the DoS attack. The numerical simulation and comparison are carried out in Section 4.

Combining DoS attacks with state estimation, the states of neighbor unmanned systems for an agent can be defined as a switching function

$$\hat{x}_i(t) = \begin{cases} x_i(t), t \in \bar{\mathcal{T}}(T_i) \\ x_{ti}^p(t), t \in \mathcal{T}(T_i) \end{cases} \tag{6}$$

where $x_i(t)$ represents the states of the ith neighbor agent in the case of DoS-off. $x_{ti}^p(t)$ is the estimation states of neighbor agent i in the case of DoS-on according to the state prediction method in (5) or state holding method. Noted that $\hat{x}_i$ is a switching function caused by the DoS attack. The derivative term $\dot{\hat{x}}_1^j$ is hard to obtain and introduced into the controller design. In the actual operation process of the unmanned system, the state time series of the neighbor agent can be obtained. The $\dot{\hat{x}}_1^j$ can be calculated using the following equation.

$$\dot{\hat{x}}_1^i(t_k) = \frac{\hat{x}_1^i(t_k) - \hat{x}_1^i(t_{k-1})}{t_k - t_{k-1}} \tag{7}$$

where t_k and t_{k-1} represent the sampling times, respectively. $\hat{x}_1^i(t_k)$ and $\hat{x}_1^i(t_{k-1})$ denote the states of the ith neighbor agent at t_k and t_{k-1}. Considering the error between the real state and the estimated state, the states of neighbor agent j can be rewritten as

$$x_j(t) = \hat{x}_j(t) + \varepsilon_j \tag{8}$$

where ε_j represents an uncertain term for describing the error, which will be addressed in the following steps. The term ε_j emerges as a result of DoS attacks, which represents the discrepancy between the real state $x_j(t)$ and estimated state $\hat{x}_j(t)$ under the DoS attacks. The boundedness of ε_j should be discussed. Therefore, an existing assumption is introduced in the paper.

Assumption 2. *[38] Because the energy of the attacker is limited, DoS attacks are commonly considered intermittent attacks, which are necessary conditions to ensure the controllability of the system.*

The periodic DoS attack is investigated in the paper. Therefore, the attack duration is finite time. According to Assumption 2, ε_j is bounded under existing conditions. By the proposed estimation mechanism in this paper, the feedback control loop can be held during the DoS attacks.

In addition, some existing lemmas that are necessary for designing the resilient controller in this paper are presented as follows:

Lemma 1. *[39] For any $\theta \in \mathbb{R}$ and $\epsilon > 0$, there is $0 \leqslant |\theta| - \theta \tanh(\theta/\epsilon) \leqslant 0.2785\epsilon$.*

Lemma 2. *[40] For any $a, b \in \mathbb{R}^n$ and $h \neq 0$, there is $a^T b \leqslant \frac{h^2}{2} a^T a + \frac{1}{2h^2} b^T b$.*

3 Main results

3.1 Consensus control protocol

According to the definition of communication topology nodes, the reference command information can be regarded as a virtual node in the augmented adjacency matrix (2). The consensus protocol for MAS can be achieved if $\lim_{t\to\infty} \sum_{i,j=1}^{N} \|x_1^i(t) - x_1^j(t)\| \to 0$ is satisfied. To develop the distributed controller for agents, the consensus control measurement error function can be defined as

$$\boldsymbol{\xi} = \sum_{i=1}^{N} \xi_i \tag{9}$$

$$\xi_i = \sum_{j=1}^{N} \bar{a}_{ij} \left(x_1^i - x_1^j \right) \tag{10}$$

where x_1^i is the states of the ith agent. x_1^j represents the states of the neighbor agent j. N represents the number of neighbor agents. $\bar{a}_{ij}$ is the communication topology.

The consensus of MAS can be achieved if $\sum_{i=1}^{N}\xi_i$ is bounded. According to the definition of x_j in (8), it can be obtained that

$$\xi_i = \sum_{j=1}^{N}\bar{a}_{ij}\Big(x_1^i - \hat{x}_1^j - \varepsilon_1^j\Big). \tag{11}$$

Taking the derivative of (11) and by virtue of (1), it can be obtained that

$$\begin{aligned}\dot{\xi}_i &= \sum_{j=1}^{N}\bar{a}_{ij}\Big(\dot{x}_1^i - \dot{\hat{x}}_1^j - \dot{\varepsilon}_1^j\Big)\\ &= \sum_{j=1}^{N}\bar{a}_{ij}\Big(F_1^i + G_1^i x_2^i - \dot{\hat{x}}_1^j - \dot{\varepsilon}_1^j\Big)\\ &= \bar{d}_i\big(F_1^i + G_1^i x_2^i\big) - \sum_{j=1}^{N}\bar{a}_{ij}\dot{\hat{x}}_1^j - \sum_{j=1}^{N}\bar{a}_{ij}\dot{\varepsilon}_1^j\end{aligned} \tag{12}$$

where $\bar{d}_i = \sum_{j=1}^{N}\bar{a}_{ij}$ is obtained by the augmented degree matrix.

3.2 Disturbance observer for DoS attacks

According to (11), the uncertain term ε_j caused by the state predictor is treated as the disturbances that the degrade system performance under the DoS attack. Noted that $\dot{\varepsilon}$ is hard to obtain since the state of the neighbor agents is defined as the switching function. Compared with the intrinsic disturbances in agents, ε_j is only discovered under the DoS attacks and caused by the state predictor leading to a signal vibration. Developing a disturbance observer to compensate for the error term ε_j and degrade the signal vibration is crucial for improving the system's resiliency. An estimation term can be immediately integrated into the resilient controller to compensate for the disturbance and protect the system security.

According to (12), the system uncertain disturbance term can be denoted as

$$\Delta_i = -\sum_{j=1}^{N}\bar{a}_{ij}\dot{\varepsilon}_1^j. \tag{13}$$

According to the above analysis, it is noticed that the disturbance does not always exist since the DoS attack cannot always occur. For dealing with the issue, define the observer $\hat{\Delta}_i$ of Δ_i as

$$\hat{\Delta}_i = \hat{\mathscr{D}}_i + \sum_{j=1}^{N}\bar{a}_{ij}\dot{\hat{x}}_1^j \tag{14}$$

where $\hat{\mathscr{D}}_i$ represents the estimation term of $\mathscr{D}_i$ which is defined as

$$\mathscr{D}_i = \Delta_i - \sum_{j=1}^{N}\bar{a}_{ij}\dot{\hat{x}}_1^j. \tag{15}$$

In the proposed disturbance observer, $\hat{\mathscr{D}}_i$ is an indirect estimator related to Δ_i for dealing with the issue that the disturbance does not always exist. $\sum_{j=1}^{N}\bar{a}_{ij}\dot{\hat{x}}_1^j$ is a given term by neighbor agents information *via* communication topological network. $\hat{\Delta}_i$ can be acquired by (14). Substituting $\mathscr{D}_i$ into (12) one yields

$$\dot{\xi}_i = \bar{d}_i\big(F_1^i + G_1^i x_2^i\big) + \mathscr{D}_i. \tag{16}$$

The observer error can be calculated as

$$\tilde{\Delta}_i = \Delta_i - \hat{\Delta}_i = \mathscr{D}_i + \sum_{j=1}^{N}\bar{a}_{ij}\dot{\hat{x}}_1^j - \hat{\mathscr{D}}_i - \sum_{j=1}^{N}\bar{a}_{ij}\dot{\hat{x}}_1^j = \mathscr{D}_i - \hat{\mathscr{D}}_i. \tag{17}$$

Furthermore, define the error term between $\mathscr{D}_i$ and $\hat{\mathscr{D}}_i$ as $\tilde{\mathscr{D}}_i = \mathscr{D}_i - \hat{\mathscr{D}}_i$. By virtue of (16), it can be obtained that

$$\tilde{\mathscr{D}}_i = \dot{\xi}_i - \bar{d}_i\left(F_1^i + G_1^i x_2^i\right) - \hat{\mathscr{D}}_i. \tag{18}$$

Assume $\left|\dot{\mathscr{D}}_i\right| < \delta_i$, where δ_i represents the unknown upper bound of $\dot{\mathscr{D}}_i$. The update law $\dot{\hat{\mathscr{D}}}_i$ of $\mathscr{D}_i$ and estimation adaptive law $\dot{\hat{\delta}}_i$ of δ_i are designed as

$$\dot{\hat{\mathscr{D}}}_i = k_d\left(\dot{\xi}_i - \bar{d}_i(F_1 + G_1 x_2)\right) - k_d\hat{\mathscr{D}}_i + u_\delta \tag{19}$$

$$u_\delta = sign\left(\tilde{\mathscr{D}}_i\right)\hat{\delta}\tanh\left(\left|\tilde{\mathscr{D}}_i\right|^T k_\delta\hat{\delta}/\varepsilon_\delta\right) \tag{20}$$

$$\dot{\hat{\delta}}_i = k_\delta\left|\tilde{\mathscr{D}}_i\right| \tag{21}$$

$$\dot{\varepsilon}_\delta = \varepsilon^* - k_\varepsilon e^{\left|\tilde{\mathscr{D}}_i\right|}\varepsilon_\delta \tag{22}$$

where k_d represents a diagonal matrix. k_δ, k_ε, and ε^* are the positive parameters.

3.3 Event-triggered control protocol

Considering the agent model (1) and the consensus control protocol (10), design the virtual control signal $\varphi(\xi_i)$ and the control signal $u_i(t)$ for the ith agent to realize the consensus of unmanned systems.

By substituting agent model (1), the consensus control differences (12) can be rewritten as

$$\dot{\xi}_i = \bar{d}_i\left(F_1^i + G_1^i\varphi(\xi_i) + G_1^i\left(x_2^i - \varphi(\xi_i)\right)\right) - \sum_{j=1}^{N}\bar{a}_{ij}\dot{\hat{x}}_1^j - \sum_{j=1}^{N}\bar{a}_{ij}\dot{\varepsilon}_1^j. \tag{23}$$

For the stability of agent, the virtual control signal $\varphi\left(\xi^i\right)$ for x_2^i is designed as

$$\varphi\left(\xi_1^i\right) = \left(\bar{d}_i G_1\right)^{-1}\left(-k_\varphi\xi_1^i - \bar{d}_i F_1 - \frac{k_\eta^2}{2h_\eta^2}\xi_1^i - \sum_{j=1}^{N}\bar{a}_{ij}\dot{\hat{x}}_j + \hat{\Delta}_i\right) \tag{24}$$

in which

$$\dot{k}_\varphi = -k_c k_\varphi + sign\left(\xi_1^i\right)k_\eta\xi_1^i + k_c k^*. \tag{25}$$

Noted that G_1 is nonsingular, and $\bar{d}_i = 0$ is avoided as every following agent has a neighbor agent or the virtual node at least to receive the information according to Assumption 1 established about communication topology with a spanning tree in the paper. Therefore, $\varphi\left(\xi_1^i\right)$ can be calculated. Furthermore, defined the adaptive gain error term

$$\tilde{k}_\varphi = k_\varphi - k^* \tag{26}$$

where k^*, k_η, and k_c are positive definite matrices. k_φ is an adaptive control matrix related to ξ_i for improving the ability of resilience. It is noted that $\text{sign}(\xi_i)k_\eta\xi_i \geqslant 0$ is expected. There is $\tilde{k} \geqslant \tilde{k}(0)e^{-k_c t}$. It can be obtained $k_\varphi \geqslant \tilde{k}(0)e^{-k_c t} + k^*$. If $\tilde{k}(0) > 0$, and $k_\varphi(0) > k^*$, there is $k_\varphi > k^* > 0$.

Define virtual control error

$$\zeta_i = x_2^i - \varphi(\xi_i). \tag{27}$$

By virtue of (1), the derivative of (27) is derived as

$$\dot{\zeta}_i = \dot{x}_2^i - \dot{\varphi}(\xi_i) = F_2 + G_2 u(t_k) - \dot{\varphi}(\xi_i) \tag{28}$$

where the actuator control signal $u_i(t_k)$ of the event-triggering time sequence is defined as $t_k = \{t_0, t_1, \ldots, t_n\}$. The purpose of introducing the ETM into the proposed resilient controller is to reach an equilibrium between control performance and service life of actuators under DoS attack in practical design and to make the controller resilient under DoS attacks. In the proposed resilient controller, the ETM can decrease the actuator triggering frequency under the DoS attacks. Under normal conditions,

actuators would be triggered at a fixed maximum frequency for the optimal control performance. However, the controller is threatened by the reference signal vibration due to the DoS attacks. By using the ETM, the controller acting on the actuator will decrease the triggering frequency, making the controller insensitive to the reference signal involving the cyber-attack. The resiliency can be reflected in the process of consensus control under the DoS attacks. By reducing the actuator trigger frequency, the service life of agents can be prolonged. It is a way to ensure the security of the systems.

The measurement error for ETM is defined as

$$e_i(t) = \zeta_i(t_k) - \zeta_i(t). \tag{29}$$

The event time instants for actuator controller $u(t_k)$ are determined by the following approach

$$t_{k+1} = \inf\{t > t_k | f(t) \geqslant 0\} \tag{30}$$

where $f(t)$ satisfies the following definition

$$f(t) = e_i(t)^T \Pi e_i(t) - \zeta_i(t)^T \Lambda \zeta_i(t) - \mu_i. \tag{31}$$

In the paper, a dynamic ETM method is designed to improve system performance. Compared with some existing work such as [24], the proposed dynamic ETM term μ_i is updated by the virtual control error (27) without measurement error for ETM. The coupling between event trigger error and condition is decreased. The dynamic triggering term μ_i is designed as

$$\dot{\mu}_i = {\zeta_i}^T k_{\zeta\mu} \zeta_i - k_\mu \mu_i. \tag{32}$$

The control signal $u(t_k)$ can be designed as the function related to $\zeta_i(t_k)$, which is represented as $u(\zeta_i(t_k))$. According to ETM (29), $u(t_k)$ can be rewritten as $u(e_i(t) + \zeta_i(t))$. The controller input can be carried out by

$$u(t_k) = G_2^{-1}(-k_\zeta(e_i + \zeta_i(t)) - F_2 + \dot{\varphi}(\xi_i)) \tag{33}$$

where $\varphi(\xi_i)$ is designed by (24) and (28). However, it is noticed that $\dot{\varphi}(\xi_i)$ is hard to acquire. For solving the difficulty, the high-order-differentiator (HOD) is introduced.

The differentiator can be designed with a compact form

$$\dot{\hat{\boldsymbol{\varphi}}} = \boldsymbol{A}\hat{\boldsymbol{\varphi}} + \boldsymbol{B}\varphi \tag{34}$$

where $\hat{\boldsymbol{\varphi}} = [\hat{\varphi}, \dot{\hat{\varphi}}]^T$, $\varphi = \varphi(\xi_i)$, and $\boldsymbol{A} = \begin{bmatrix} 0 & a_0 \\ -a_0 a_1^2 & -2a_0 a_1 \end{bmatrix}$, $\boldsymbol{B} = \begin{bmatrix} 0 \\ a_0 a_1^2 \end{bmatrix}$.

3.4 Stability analysis

Theorem. *Consider the unmanned systems described by* (1) *under the directed communication topology* (2). *The state predictor is designed as* (5). *The consensus error is constructed as* (10). *The dynamic ETM is defined as* (30). *A disturbance observer focusing on DoS attacks is developed as* (14) *following the update laid by* (19)–(22). *Furthermore, the virtual control signal is designed as* (24) *with the adaptive laws* (25) *and* (26), *and the control signal is designed as* (33). *The consensus of unmanned systems can be guaranteed, and errors are uniformly ultimately bounded (UUB).*

Proof. For the disturbance observer, define the observer estimation error $\tilde{\delta}_i = \delta_i - \hat{\delta}_i$. Since δ_i is a constant, $\dot{\delta}_i = 0$. For the agent i in the MAS, the Lyapunov function candidate is defined as follows:

$$V_d = \frac{1}{2}\tilde{\mathscr{D}}_i^T k_\delta \tilde{\mathscr{D}}_i + \frac{1}{2}\tilde{\delta}_i^T \tilde{\delta}_i + \varepsilon_\delta. \tag{35}$$

According to (22), it is noticed that $k_\varepsilon e^{|\tilde{\mathscr{D}}_i|} > 0$ and $\varepsilon^* > 0$. It is easy to verify that $\varepsilon_\delta > 0$. The derivative of V_d is derived as

$$\dot{V}_d = \tilde{\mathscr{D}}_i^T k_\delta \dot{\tilde{\mathscr{D}}}_i + \tilde{\delta}^T \dot{\delta} + \varepsilon^* - k_\varepsilon e^{|\tilde{\mathscr{D}}|} \varepsilon_\delta$$

$$
\begin{aligned}
&= -\tilde{\mathscr{D}}_i^T k_\delta k_d\Big(\Big(\dot{\xi}_i - \bar{d}_i\big(F_1^i + G_1^i x_2\big)\Big) - \hat{\mathscr{D}}_i\Big) + \tilde{\mathscr{D}}_i^T k_\delta\Big(\dot{\mathscr{D}}_i - u_\delta\Big) - \tilde{\delta}^T\dot{\hat{\delta}}_i + \varepsilon^* - k_\varepsilon e^{|\tilde{\mathscr{D}}_i|}\varepsilon_\delta \\
&= -\tilde{\mathscr{D}}_i^T k_d k_\delta \tilde{\mathscr{D}}_i - \Big(\delta_i - \hat{\delta}_i\Big)k_\delta\Big|\tilde{\mathscr{D}}_i\Big| + \tilde{\mathscr{D}}_i^T k_\delta\dot{\mathscr{D}}_i - k_\varepsilon e^{|\tilde{\mathscr{D}}_i|}\varepsilon_\delta + \varepsilon^* \\
&\quad - \tilde{\mathscr{D}}_i^T k_\delta sign\Big(\tilde{\mathscr{D}}_i\Big)\hat{\delta}\tanh\Big(\Big|\tilde{\mathscr{D}}_i\Big|^T k_\delta\hat{\delta}/\varepsilon_\delta\Big) \\
&\leqslant -\tilde{\mathscr{D}}_i^T k_d k_\delta \tilde{\mathscr{D}}_i + \Big|\tilde{\mathscr{D}}_i\Big|^T k_\delta\delta_i - \Big(\delta_i - \hat{\delta}_i\Big)k_\delta\Big|\tilde{\mathscr{D}}\Big| - k_\varepsilon e^{|\tilde{\mathscr{D}}_i|}\varepsilon_\delta + \varepsilon^* \\
&\quad - \tilde{\mathscr{D}}_i^T k_\delta sign\Big(\tilde{\mathscr{D}}\Big)\hat{\delta}\tanh\Big(\Big|\tilde{\mathscr{D}}_i\Big|^T k_\delta\hat{\delta}/\varepsilon_\delta\Big) \\
&\leqslant -\tilde{\mathscr{D}}_i^T k_d k_\delta \tilde{\mathscr{D}}_i - k_\varepsilon e^{|\tilde{\mathscr{D}}_i|}\varepsilon_\delta + \varepsilon^* + \Big|\tilde{\mathscr{D}}_i\Big|^T k_\delta\delta_i - \Big(\delta_i - \hat{\delta}_i\Big)k_\delta\Big|\tilde{\mathscr{D}}_i\Big| \\
&\quad - \Big|\tilde{\mathscr{D}}_i\Big|^T k_\delta\hat{\delta}_i\tanh\Big(\Big|\tilde{\mathscr{D}}_i\Big|^T k_\delta\hat{\delta}/\varepsilon_\delta\Big) \\
&\leqslant -\tilde{\mathscr{D}}_i^T k_d k_\delta \tilde{\mathscr{D}}_i - k_\varepsilon e^{|\tilde{\mathscr{D}}_i|}\varepsilon_\delta + \Big|\tilde{\mathscr{D}}_i\Big|^T k_\delta\Big|\hat{\delta}_i\Big| - \Big|\tilde{\mathscr{D}}_i\Big|^T k_\delta\hat{\delta}_i\tanh\Big(\Big|\tilde{\mathscr{D}}_i\Big|^T k_\delta\hat{\delta}/\varepsilon_\delta\Big) + \varepsilon^*.
\end{aligned} \tag{36}
$$

Define $\kappa_i = |\tilde{\mathscr{D}}_i|^T k_\delta$, it is noticed that $\kappa_i > 0$. Furthermore, there is $\varepsilon_\delta > 0$. According to Lemma 1, one yields

$$
\Big|\tilde{\mathscr{D}}_i\Big|^T k_\delta\Big|\hat{\delta}_i\Big| - \Big|\tilde{\mathscr{D}}_i\Big|^T k_\delta\hat{\delta}_i\tanh\Big(\Big|\tilde{\mathscr{D}}_i\Big|^T k_\delta\hat{\delta}/\varepsilon_\delta\Big) = \Big|\kappa_i\hat{\delta}_i\Big| - \kappa_i\hat{\delta}_i\tanh\Big(\kappa_i\hat{\delta}/\varepsilon_\delta\Big) \leqslant 0.2785\varepsilon_\delta. \tag{37}
$$

Substituting (37) into (36) has

$$
\dot{V}_d \leqslant -\tilde{\mathscr{D}}_i^T k_d k_\delta \tilde{\mathscr{D}}_i - k_\varepsilon e^{|\tilde{\mathscr{D}}_i|}\varepsilon_\delta + 0.2785\varepsilon_\delta + \varepsilon^* \leqslant -\tilde{\mathscr{D}}_i^T K_d\tilde{\mathscr{D}}_i - \Big(k_\varepsilon e^{|\tilde{\mathscr{D}}_i|} - 0.2785\Big)\varepsilon_\delta + \varepsilon^* \tag{38}
$$

where $K_d = k_d k_\delta$. Therefore, $k_\varepsilon e^{|\tilde{\mathscr{D}}_i|} \geqslant k_\varepsilon$. If there is $k_\varepsilon \geqslant 0.2785$, such that $k_\varepsilon e^{|\tilde{\mathscr{D}}_i|} - 0.2785 \geqslant 0$.

According to $\varepsilon_\delta > 0$, one yields

$$
\dot{V}_d \leqslant -\alpha_d V_d + \varepsilon^* \tag{39}
$$

where $\alpha_d = 2\lambda_{\min}(K_d)$. It can be obtained that

$$
V_d \leqslant \Big(V_d(0) - \frac{\varepsilon^*}{\alpha_d}\Big)e^{-\alpha_d t} + \frac{\varepsilon^*}{\alpha_d}. \tag{40}
$$

According to (35), it means that $\tilde{\mathscr{D}}_i$ and $\tilde{\delta}_i$ are UUB. The error convergence of the state predictor can be proved. □

For the proof of the event-triggered consensus control protocol, choose the following candidate Lyapunov function for the ith agent as

$$
V_i = \frac{1}{2}{\xi_i}^T\xi_i + \frac{1}{2}\tilde{k}_i^T\tilde{k}_i + \frac{1}{2}{\zeta_i}^T\zeta_i + \mu_i. \tag{41}
$$

According to (31) and (32), one has

$$
\dot{\mu}_i(t) \geqslant \frac{k_{\zeta\mu}}{h_1^2 k_e}\Big(e_i(t)^T\Pi e_i(t) - \mu_i\Big) - k_\mu\mu_i. \tag{42}
$$

It is noticed that $\frac{k_{\zeta\mu}}{h_1^2 k_e}e_i(t)^T\Pi e_i(t) \geqslant 0$, it has

$$
\begin{aligned}
&\dot{\mu}_i(t) \geqslant -\Big(\frac{k_{\zeta\mu}}{h_1^2 k_e} + k_\mu\Big)\mu_i \\
&\mu_i(t) \geqslant \mu_{ik}\exp\Big\{-\Big(\frac{k_{\zeta\mu}}{h_1^2 k_e} + k_\mu\Big)(t - t_k)\Big\} > 0.
\end{aligned} \tag{43}
$$

Hence, the condition $V_i \geqslant 0$ is always satisfied. Taking the derivative of (41), one has

$$\dot{V}_i = {\xi_i}^T \dot{\xi}_i + \tilde{k}_i^T \dot{\tilde{k}}_i + {\zeta_i}^T \dot{\zeta}_i + \dot{\mu}_i. \tag{44}$$

Define $\dot{V}_i = \dot{V}_{i1} + \dot{V}_{i2}$, where $\dot{V}_{i1} = \frac{1}{2}{\xi_i}^T \xi_i + \frac{1}{2}\tilde{k}_i^T \tilde{k}_i$ and $\dot{V}_{i2} = {\zeta_i}^T \dot{\zeta}_i + \dot{\mu}$. Substituting (23), (27) into $\dot{V}_1$ and according to Lemma 2, one has

$$\begin{aligned}\dot{V}_{i1} &= {\xi_i}^T \dot{\xi}_i + \tilde{k}_i^T \dot{\tilde{k}}_i \\ &= -{\xi_i}^T k_\varphi \xi_i - {\xi_i}^T \frac{\eta^2}{2h_\eta^2}\xi_i + {\xi_i}^T G_1^i \zeta_i + {\xi_i}^T \Delta_i - {\xi_i}^T \hat{\Delta}_i + \tilde{k}_i^T (sign(\xi_i) k_\eta \xi_i - k_c(k_i - k^*)).\end{aligned} \tag{45}$$

According to Lemma 2 and (17), one has

$$\begin{aligned}\dot{V}_{i1} =& -{\xi_i}^T k_\varphi \xi_i - {\xi_i}^T \frac{\eta^2}{2h_\eta^2}\xi_i + {\xi_i}^T G_1^i \zeta_i - \tilde{k}_i^T k_c \tilde{k}_i + \tilde{k}_i^T sign(\xi_i) k_\eta \xi_i + {\xi_i}^T \tilde{\mathscr{D}}_i \\ \leqslant& -{\xi_i}^T k_\varphi \xi_i - \tilde{k}_i^T k_c \tilde{k}_i + \frac{h_\eta^2}{2}\tilde{k}_i^T \tilde{k}_i + {\xi_i}^T \xi_i + \frac{\left\|G_1^i\right\|_F^2}{2}{\zeta_i}^T \zeta_i + \frac{1}{2}\tilde{\mathscr{D}}_i{}^T \tilde{\mathscr{D}}_i \\ \leqslant& -\xi_i(k_\varphi - 1)\xi_i - \tilde{k}_i^T \left(k_c - \frac{h_\eta^2}{2}\right)\tilde{k}_i + \frac{\left\|G_1^i\right\|_F^2}{2}{\zeta_i}^T \zeta_i + \frac{1}{2}\tilde{\mathscr{D}}_i{}^T \tilde{\mathscr{D}}_i\end{aligned} \tag{46}$$

where $\|\cdot\|_F$ represents Frobenius norm.

Furthermore, substituting (28) and (33) into $\dot{V}_2$, and according to Lemma 2, one has

$$\begin{aligned}\dot{V}_{i2} &= {\zeta_i}^T \dot{\zeta}_i + \dot{\mu} \\ &= {\zeta_i}^T (F_2 + G_2 u(e_i + \zeta_i(t)) - \dot{\varphi}(\xi_i)) + {\zeta_i}^T k_{\zeta\mu} \zeta_i - k_\mu \mu \\ &= -{\zeta_i}^T k_\zeta \zeta - {\zeta_i}^T k_\zeta e_i + {\zeta_i}^T k_{\zeta\mu} \zeta_i - k_\mu \mu \\ &\leqslant -{\zeta_i}^T k_\zeta \zeta + \frac{h_1^2}{2}{\zeta_i}^T k_\zeta \zeta_i + \frac{1}{2h_1^2}{e_i}^T k_\zeta e_i + {\zeta_i}^T k_{\zeta\mu} \zeta_i - k_\mu \mu.\end{aligned} \tag{47}$$

By virtue of ETM (30)–(32), the matrix Π and Λ can be selected as k_ζ and $h_1^2 k_e$, respectively, such that

$$\begin{aligned}\dot{V}_{i2} &\leqslant -{\zeta_i}^T k_\zeta \zeta + \frac{1}{2h_1^2}\left(h_1^2 {\zeta_i}^T k_e \zeta_i + \mu\right) + \frac{h_1^2}{2}{\zeta_i}^T k_\zeta \zeta_i + {\zeta_i}^T k_{\zeta\mu} \zeta_i - k_\mu \mu \\ &\leqslant -{\zeta_i}^T \left(k_\zeta - \frac{h_1^2}{2}k_\zeta - \frac{1}{2}k_e - k_{\zeta\mu}\right)\zeta_i - \left(k_\mu - \frac{1}{2h_1^2}\right)\mu.\end{aligned} \tag{48}$$

Substituting (46) and (48) into (44), then one can obtain

$$\begin{aligned}\dot{V}_i &= \dot{V}_{i1} + \dot{V}_{i2} \\ &\leqslant -{\xi_i}^T (k_\varphi - 1)\xi_i - \tilde{k}_i^T \left(k_c - \frac{h_\eta^2}{2}\right)\tilde{k}_i - {\zeta_i}^T \left(k_\zeta - \frac{h_1^2}{2}k_\zeta - \frac{1}{2}k_e - k_{\zeta\mu}\right)\zeta_i \\ &\quad + \frac{\left\|G_1^i\right\|_F^2}{2}{\zeta_i}^T \zeta_i + \frac{1}{2}\tilde{\mathscr{D}}^T \tilde{\mathscr{D}} - \left(k_\mu - \frac{1}{2h_1^2}\right)\mu \\ &\leqslant -\lambda_{\min}(k_\varphi - 1){\xi_i}^T \xi_i + \frac{1}{2}\tilde{\mathscr{D}}^T \tilde{\mathscr{D}} - \lambda_{\min}\left(k_\zeta - \frac{h_1^2}{2}k_\zeta - \frac{1}{2}k_e - k_{\zeta\mu}\right){\zeta_i}^T \zeta_i \\ &\quad + \frac{\left\|G_1^i\right\|_F^2}{2}{\zeta_i}^T \zeta_i - \lambda_{\min}\left(k_\mu - \frac{1}{2h_1^2}\right)\mu - \lambda_{\min}\left(k_c - \frac{h_\eta^2}{2}\right)\tilde{k}_i^T \tilde{k}_i \\ &\leqslant -\varsigma_1 V_i + \varsigma_2\end{aligned} \tag{49}$$

where ς_1, ς_2 are given as

$$\varsigma_1 = \min\left\{\begin{array}{c} 2\lambda_{\min}(k_\varphi - 1), \\ 2\lambda_{\min}\left(k_c - \frac{h_\eta^2}{2}\right), \\ 2\lambda_{\min}(K_V) - \left\|G_1^i\right\|_F^2, \\ 2\lambda_{\min}\left(k_\mu - \frac{1}{2h_1^2}\right) \end{array}\right\}, \varsigma_2 = \frac{1}{2}\tilde{\mathscr{D}}^T\tilde{\mathscr{D}} \tag{50}$$

where $K_V = k_\zeta - \frac{h_1^2}{2}k_\zeta - \frac{1}{2}k_e - k_{\zeta\mu}$. Further, G_1^i is the control matrix of MAS, which is bounded on the basis of the system characteristics. According to (40), ς_2 is bounded. Therefore, ξ_i, $\tilde{k}_i$, and ζ_i are UUB.

Considering the consensus error of MAS for all agents, according to (9), (10) and (49), the system consensus error satisfies

$$\boldsymbol{\xi} = \sum_{i=1}^{N}\xi_i \leqslant \sum_{i=1}^{N}V_i \leqslant \sum_{i=1}^{N}\left(\left(V_i(0) - \frac{\varsigma_{i2}}{\varsigma_{i1}}\right)e^{-\varsigma_{i1}t} + \frac{\varsigma_{i2}}{\varsigma_{i1}}\right). \tag{51}$$

It can be concluded that $\sum_{i=1}^{N}\xi_i$ is uniformly convergent. Furthermore, the stability of the system consensus can be demonstrated.

3.5 Excluding Zeno behavior

In this subsection, it has been proved that there will be no Zeno behavior in the proposed dynamic ETM (30). For verifying that there is no Zeno behavior, the inequality $t_{k+1} - t_k > 0$ must be satisfied.

By defining $e_i = \zeta_i(t_k) - \zeta_i(t)$ during one trigger interval, it is noticed that $\zeta_i(t_k)$ is a constant in $[t_k, t_{k+1}]$.

$$\frac{\mathrm{d}e_i}{\mathrm{d}t} \leqslant \frac{\mathrm{d}}{\mathrm{d}t}\sqrt{{e_i}^T e_i} \leqslant |\dot{e}_i| \leqslant \left|\dot{\zeta}_i(t_k) - \dot{\zeta}_i(t)\right| \leqslant \left|\dot{\zeta}_i(t)\right| \leqslant \mathcal{K} \tag{52}$$

where $\mathcal{K}$ is a positive constant.

According to (52), the integral of $\frac{\mathrm{d}e_i}{\mathrm{d}t}$ satisfies

$$e_i \leqslant \int_{t_k}^{t_{k+1}} \mathcal{K}\,\mathrm{d}t \leqslant \mathcal{K}(t_{k+1} - t_k). \tag{53}$$

Furthermore, the following constraint exists

$$t_{k+1} - t_k \geqslant \frac{e_i}{\mathcal{K}}. \tag{54}$$

According to dynamic ETM (30), (31), and (43), there are $e_i \geqslant \sqrt{\frac{1}{k_\zeta}(h_1^2{\zeta_i}^T k_e\zeta_i + \mu)}$ and $\mu > 0$. It can be obtained that $e_i > 0$. One yields

$$t_{k+1} - t_k \geqslant \frac{\sqrt{\frac{1}{k_\zeta}\left(h_1^2{\zeta_i}^T k_e\zeta_i + \mu\right)}}{\mathcal{K}} > 0. \tag{55}$$

According to (55), there is a minimum time interval between the trigger of two events. The condition that inequality $t_{k+1} - t_k > 0$ is satisfied. Therefore, the Zeno behavior is excluded.

4 Simulation result

4.1 Experimental simulation model

In this section, the effectiveness of the proposed ETM consensus control method with predictor is verified by simulation scenarios as follows. A multiple unmanned aerial vehicles (multi-UAV) system is used to

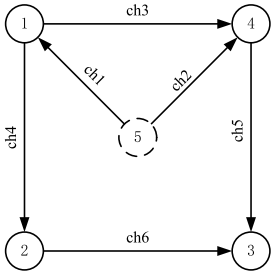


Figure 4. Directed communication topology of MAS

represent the MAS in this paper. The multi-UAV system consists of 4 UAVs as 4 nodes labeled as 1 to 4 and a virtual reference node labeled as 5. The directed communication topology is established as (2) in Figure 4. The derivation process and specific system parameters of the UAV model used can be found in [41]. The dynamic model of the ith UAV is shown as follows:

$$\begin{cases} \dot{V}_i = (-D_i + T_i c_{\alpha_i} c_{\beta_i})/m_i - g s_{\gamma_i} \\ \dot{\chi}_i = (L_i s_{\mu_i} + Y_i c_{\mu_i})/(m_i V_i c_{\gamma_i}) - (c_{\alpha_i} s_{\beta_i} c_{\mu_i} - s_{\alpha_i} s_{\mu_i}) T_i/(m_i V_i c_{\gamma_i}) \\ \dot{\gamma}_i = (L_i c_{\mu_i} - Y_i s_{\mu_i})/(m_i V_i) + (c_{\alpha_i} s_{\beta_i} s_{\mu_i} + s_{\alpha_i} c_{\mu_i}) T_i/(m_i V_i) - g c_{\gamma_i}/V_i \end{cases} \tag{56}$$

$$\begin{cases} \dot{\mu}_i = (p_i c_{\alpha_i} + r_i s_{\alpha_i})/c_{\beta_i} + \dot{\gamma}_i c_{\mu_i} t_{\beta_i} + \dot{\chi}_i (s_{\gamma_i} + c_{\gamma_i} s_{\mu_i} t_{\beta_i}) \\ \dot{\alpha}_i = q_i - t_{\beta_i} (p_i c_{\alpha_i} + r_i s_{\alpha_i}) - (\dot{\chi}_i c_{\gamma_i} s_{\mu_i} + \dot{\gamma}_i c_{\mu_i})/c_{\beta_i} \\ \dot{\beta}_i = p_i s_{\alpha_i} - r_i c_{\alpha_i} + \dot{\chi}_i c_{\gamma_i} c_{\mu_i} - \dot{\gamma}_i s_{\mu_i} \end{cases} \tag{57}$$

$$\begin{cases} \dot{p}_i = (c_{i1} r_i + c_{i2} p_i) q_i + c_{i3} \mathcal{L}_i + c_{i4} \mathcal{N}_i \\ \dot{q}_i = c_{i5} p_i r_i - c_{i6} (p_i^2 - r_i^2) + c_{i7} \mathcal{M}_i \\ \dot{r}_i = (c_{i8} p_i - c_{i2} r_i) q_i + c_{i4} \mathcal{L}_i + c_{i9} \mathcal{N}_i \end{cases} \tag{58}$$

where V_i, χ_i, and γ_i represent the velocity, flight path angle, and heading angle of the ith UAV, respectively. μ_i, α_i, and β_i represent its angle of attack, sideslip angle, and bank angle, respectively. p_i, q_i, and r_i denote its angular rate, respectively. For fitting in the proposed second-order MAS consensus control model (1) to design the resilient consensus controller in the paper, the multi-UAV attitude consensus control is considered to verify the effectiveness of the controller. By defining $x_1^i(t) = [\mu_i, \alpha_i, \beta_i]$ and $x_2^i(t) = [p_i, q_i, r_i]$, the dynamic model of UAV can be rewritten as the form of (1).

In Figure 4, ch$i$, $i = 1, 2, \ldots, 6$, represents the communication channel, in which the state information transforms from the UAV that sends out commands to the object UAV. The dotted circle represents the virtual reference node signal. The arrows of channels represent the direction of transmission. The communication between nodes is carried out by directed routing. Parameters of the DoS attack model for every channel are $T_n = 10\,\text{s}$ and $F_a = 9\%$. Further, $T_d = 0.9\,\text{s}$. The delay times for every channel are set as $T_{\text{delay}} = 1.3\,\text{s}$ to realize the asynchronous DoS attacks. The beginning time of the DoS attacks $T_{\text{begin}} = 5\,\text{s}$. The timing sequences of DoS attacks on six channels are shown in Figure 5.

For researching consensus control based on dynamic ETM under the DoS attacks, the time-varying reference command must be considered. Because the consensus control and ETM will not work if the command is a constant when MAS has been stable. In addition, the system stability will not suffer from the DoS attacks, since the desired state is constant whether it exists or not a DoS attack.

In the proposed event-triggered resilient controller with the DoS attack disturbance observer scheme, the actuator control signal for each agent is adopted as (33). The virtual control signal is adopted as (24), which follows the updated laws as (25) and (26). The disturbance observer is designed as (14) and (19). Observer parameters are updated by (20)–(22). The actuator triggers follow the dynamic ETM as (30) and (31), where the dynamic parameters are satisfied (32).

The initial states of agents are taken as $x_{11}^1(0) = 0.02$, $x_{12}^1(0) = -0.05$, $x_{13}^1(0) = 0.05$, $x_{21}^1(0) = 0.001$, $x_{22}^1(0) = 0.001$, $x_{23}^1(0) = -0.001$, $x_{11}^2(0) = -0.02$, $x_{12}^2(0) = -0.01$, $x_{13}^2(0) = 0.04$, $x_{21}^2(0) = 0.001$, $x_{22}^2(0) = -0.001$, $x_{23}^2(0) = -0.001$, $x_{11}^3(0) = -0.03$, $x_{12}^3(0) = -0.05$, $x_{13}^3(0) = -0.05$, $x_{21}^3(0) = -0.001$, $x_{22}^3(0) = 0.001$, $x_{23}^3(0) = -0.001$, $x_{11}^4(0) = 0.03$, $x_{12}^4(0) = -0.03$, $x_{13}^4(0) = -0.02$, $x_{21}^4(0) = 0.001$, $x_{22}^4(0) = 0.001$,

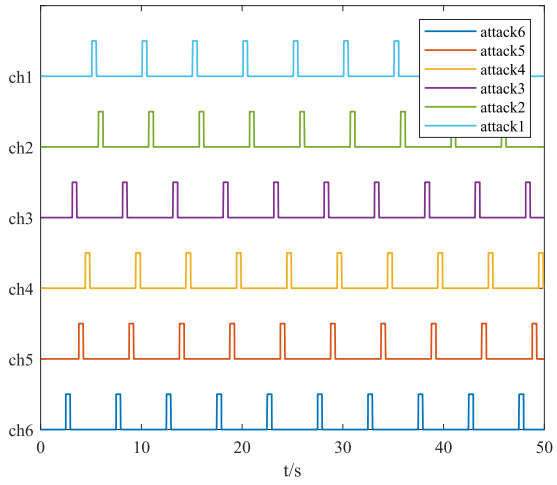


Figure 5. DoS attack on six channels

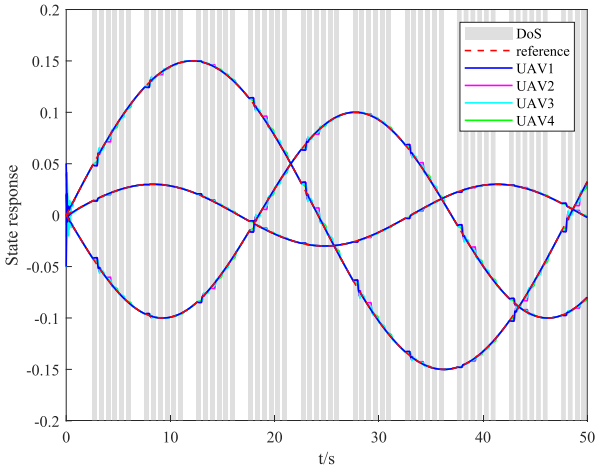


Figure 6. Attitude response of multi-UAV with state holding under DoS attacks

$x_{23}^4(0) = 0.001$. For the disturbance observer, $k_d = \text{diag}(1,1,1)$, $k_\delta = \text{diag}(1,1,1)$, $\varepsilon^* = 0.2$, and $k_\varepsilon = 0.3$. For the virtual control signal, $k^* = \text{diag}(10,10,12)$, $k_c = \text{diag}(5,5,5)$, $k_\eta = \text{diag}(1,1,1)$, and $h_\eta = 0.5$. For the HOD, $a_0 = 2$, $a_1 = 10$. For the actuator control signal, $k_\zeta = \text{diag}(10,20,10)$. For the ETM, $h_1 = 0.5$, $k_\mu = 5$, and $k_{\zeta\mu} = \text{diag}(0.5,0.5,0.5)$.

4.2 Simulation scenario 1

Considering periodic DoS attacks, we use the time-varying reference command in the control scheme to verify the resilient capability of the proposed controller without introducing the state predictor in the first step. By using the state holding of the agent during the DoS attacks proposed in Section 2, the resilient control effect is as Figure 6.

In order to show the MAS tracking effect by the proposed resilient controller, UAVs attitude tracking effectiveness simulation results on three attitude angles $[\mu, \alpha, \beta]$ from $x_1^i(t)$ to reference signal are shown in Figure 7. It shows that the tracking performance on three attitudes can be guaranteed by the proposed resilient controller. The tracking error will exist during the DoS attack as the reference command is unavailable, after which the tracking error will be eliminated.

The tracking error between agent state signal $x_1^i(t)$ and reference state signal $x^0(t)$ is defined as $e_i(t) = x_1^i(t) - x^0(t)$. The attitude tracking error $[\mu_i, \alpha_i, \beta_i]$ of UAVs are shown in Figure 8. It can be shown that the maximum of the tracking error is close to 0.01 in the simulation due to the periodic

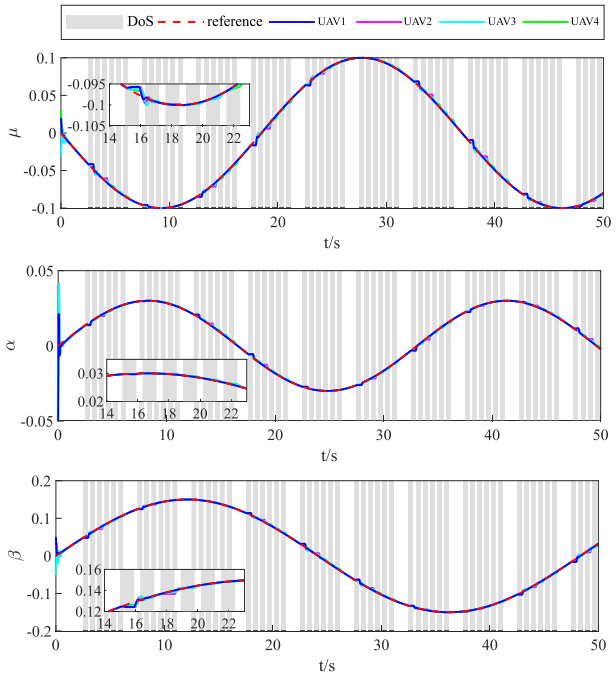


Figure 7. State response on three attitudes under DoS attacks

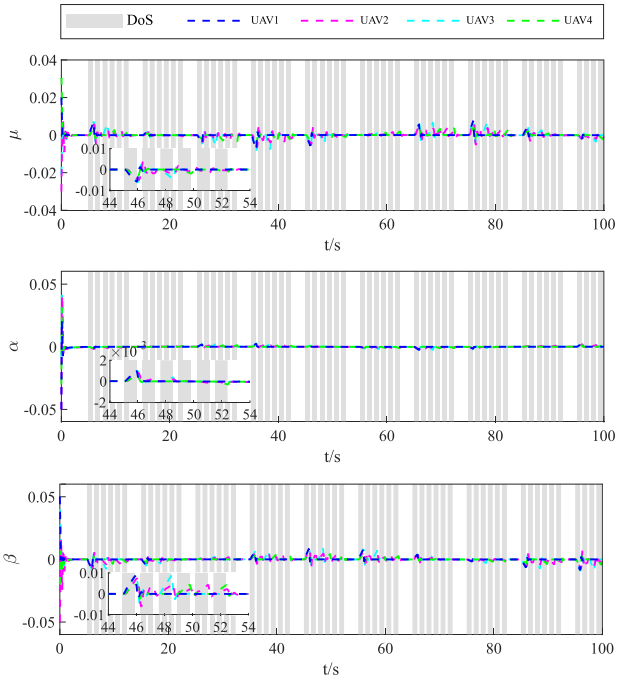


Figure 8. Attitude tracking error of multi-UAV with state holding

DoS attacks. Besides, the error will approach zero during the duration of DoS-off. The resilient ability can be verified.

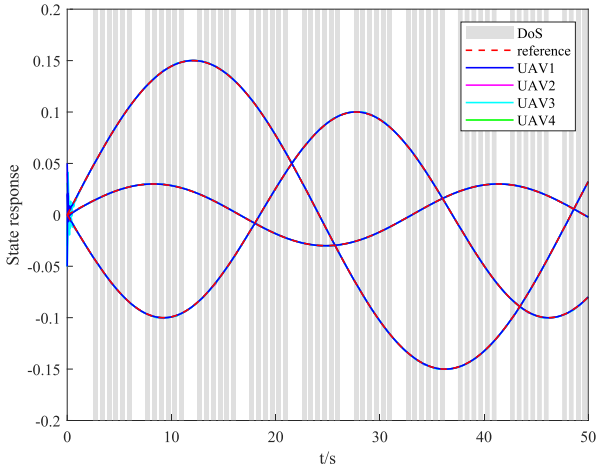


Figure 9. Attitude response of multi-UAV with ARIMA under DoS attacks

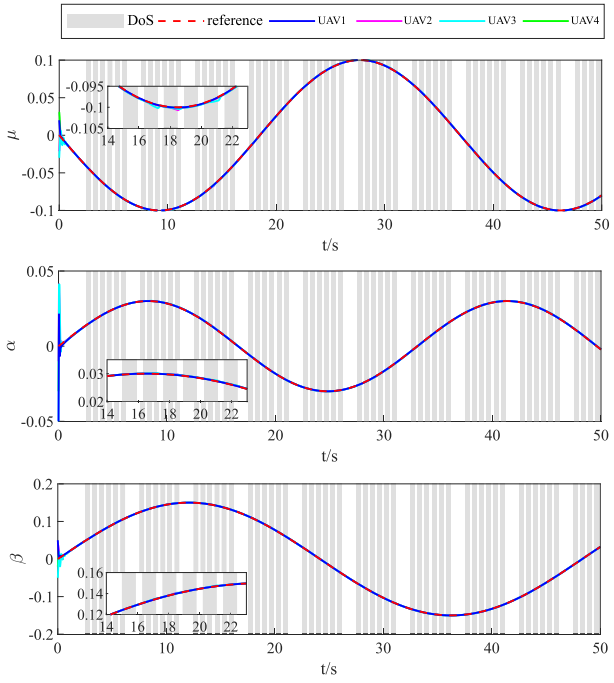


Figure 10. State response on three attitudes under DoS attacks

4.3 Simulation scenario 2

For comparison, using the same reference signal, the resilient controller is utilized with the state predictor in the second step. The control performance of the three attitude angles $[\mu, \alpha, \beta]$ from $x_1^i(t)$ is shown as Figure 9. The tracking performance on three attitudes is shown in Figure 10.

Compared with the resilient control scheme without a state predictor, state tracking trajectories of followers are smoother during the duration of the DoS-on attack. This means that the system has better security. The error of attitude tracking is given in Figure 11.

The attitude tracking error is less than 1×10^{-3} by utilizing the ARIMA under the periodic DoS attacks, which is much lower than that without the ARIMA state predictor. The merit of introducing ARIMA into the resilient control scheme can be verified.

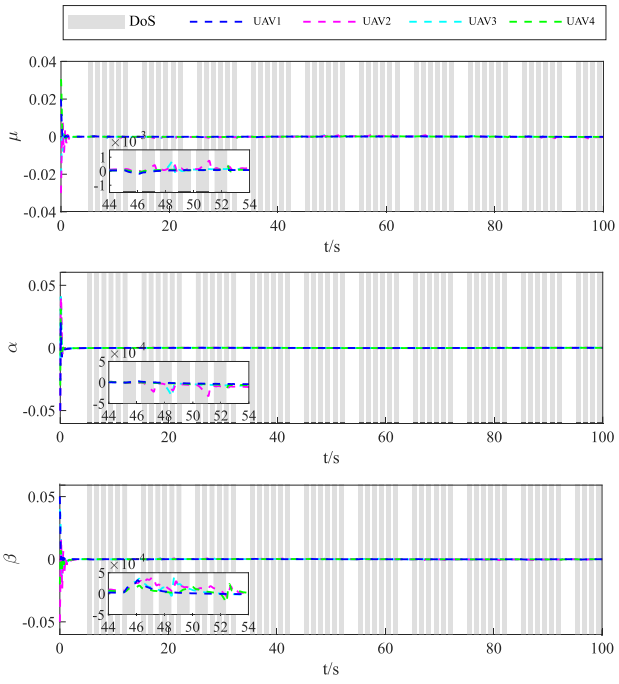


Figure 11. Attitude tracking error of multi-UAV with ARIMA

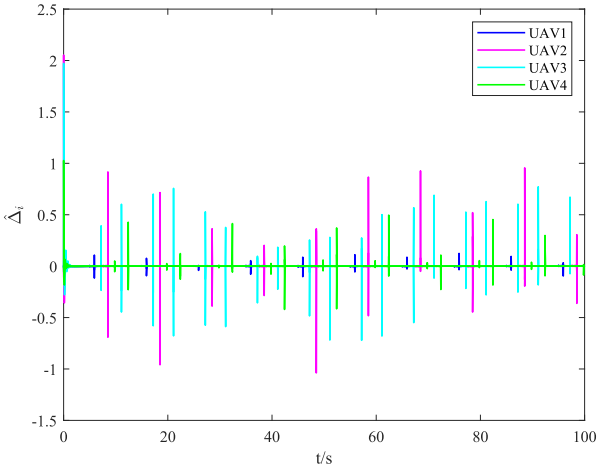


Figure 12. Disturbance observation results for attitudes of multi-UAV

For demonstrating the estimation effectiveness of the proposed indirect disturbance observer, the reconstruction result of the disturbance from the observer in the situation of the proposed controller by introducing the predictor is shown in Figure 12.

In order to verify the consensus control effectiveness of the proposed control scheme, define the consensus evaluating indicator as

$$e_i^c(t) = x_1^i(t) - \frac{1}{N}\sum_{j=1}^{N} x_1^j(t) \tag{59}$$

where $\frac{1}{N}\sum_{j=1}^{N} x_1^j(t)$ respects the average states information of all follower UAVs. According to the consensus control measurement error (10), the evaluating indicator (59) can be used to describe the consensus measurement error of an agent.

Figure 13 shows the simulation results about consensus error by using the evaluation indicator (59). It can be seen from Figure 13 that there is an obvious consensus deviation at the initial moment of simulation

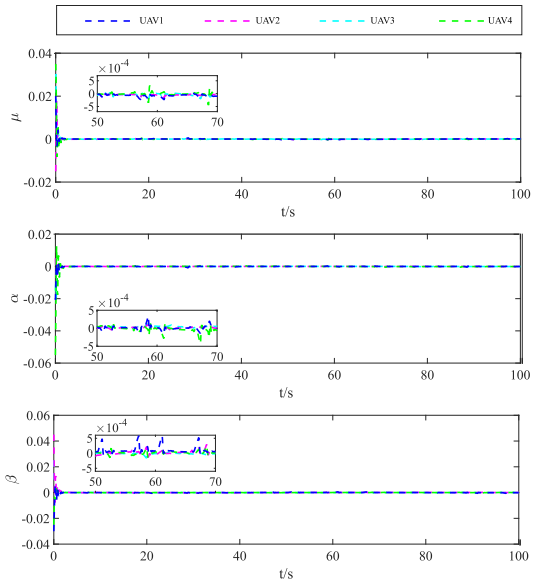


Figure 13. Attitude tracking consensus error of multi-UAV

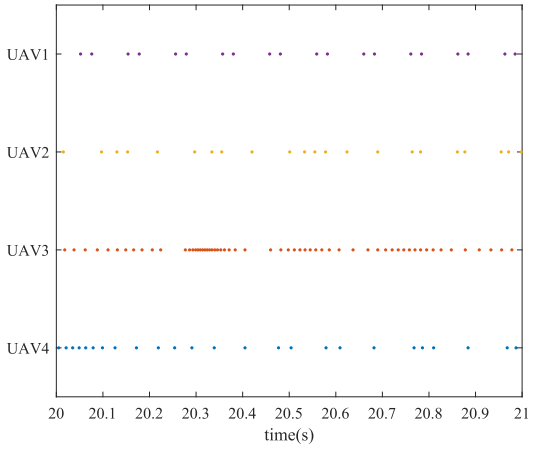


Figure 14. Responses of triggered time for multi-UAV

due to the different initial states of the multi-UAV. After a short adjustment by the proposed controller, MAS can achieve convergence of consensus. Further, the consensus errors of multi-UAV in three attitudes $[\mu_i, \alpha_i, \beta_i]$ are less than 5×10^{-4} even by utilizing a time-varying reference command following ETM under the periodic DoS attacks. The consensus performance is never compromised by network attacks and time-varying reference commands. The attitude tracking performance can be ensured simultaneously. It can be illustrated that the proposed resilient controller has the ability to maintain the tracking performance while ensuring the consensus under the periodic DoS attacks.

The sequence of events triggered by four agents during 1 s is described in Figure 14. In the simulation scenarios, the initial controller refresh frequency is set as 1×10^3 Hz. As shown in Figure 14, the controller trigger frequency is far less than the control system refresh frequency. As the time-varying attitude reference command is deployed, the controller trigger must exist for guaranteeing the system consensus and tracking capability.

5 Conclusion and future work

This paper investigates a resilient control method for MAS under periodic DoS attacks. A data-based state prediction method is introduced into a model-based controller scheme to combat DoS attacks. The prediction method adopted in this paper is to design a state predictor to estimate the state of neighbor agents under the DoS attacks. State predictors can connect the feedback loop that is disrupted by DoS attacks. For the prediction error caused by the data-based state prediction method, this paper proposes a disturbance observer to compensate for the error which is regarded as an uncertain disturbance. Furthermore, in order to guarantee the security and consensus of MAS, this paper proposes a resilient controller based on dynamic ETM. Finally, the effectiveness of the proposed resilient consensus control method is shown by numerical simulations. Meanwhile, the resilient capability of the proposed controller against the periodic DoS attacks has been demonstrated by the comparative simulations. In this paper, a resilient control method is developed against network attacks with constraint conditions without considering more general types of attacks. In our future study $\dot{\hat{\delta}}_i$ will be designed by using the switching function form. Then, more general DoS attacks and other kinds of network attacks will be considered, such as random DoS attacks and false data injection attacks to expand the application of the proposed resilient control method.

Conflict of Interest

The authors declare that they have no conflict of interest.

Data Availability

No data are associated with this article.

Authors' Contributions

Haichuan Yang: Conceptualization, Methodology, Draft. Ziquan Yu: Writing – review & editing. Youmin Zhang: Writing – review & editing.

Acknowledgements

We thank the anonymous reviewers for their helpful comments.

Funding

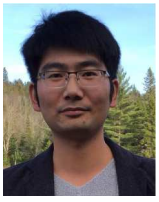
This work was supported by the National Natural Science Foundation of China (Nos. 61833013, 62003162, 62233009), Natural Science Foundation of Jiangsu Province of China (Nos. BK20200416, BK20222012), China Postdoctoral Science Foundation (Nos. 2020TQ0151, 2020M681590), Fundamental Research Funds for the Central Universities (No. NS2021025), Industry-University Research Innovation Foundation for the Chinese Ministry of Education (No. 2021ZYA02005), Science and Technology on Space Intelligent Control Laboratory (No. HTKJ2022KL502015), Aeronautical Science Foundation of China (No. 20200007018001), and Natural Sciences and Engineering Research Council of Canada.

References

[1] Zhang YM and Jiang J. Bibliographical review on reconfigurable fault-tolerant control systems. Ann Rev Control 2008; **32**: 229–52.
[2] Yu ZQ, Zhang YM and Jiang J et al. A review on fault-tolerant cooperative control of multiple unmanned aerial vehicles. Chin J Aeronaut 2022; **35**: 1–18.
[3] Shen QK, Shi P and Zhu JW et al. Adaptive consensus control of leader-following systems with transmission nonlinearities. Int J Control 2019; **92**: 317–28.
[4] Ding SX. A note on diagnosis and performance degradation detection in automatic control systems towards functional safety and cyber security. Secur Saf 2022; **1**: 2022004.
[5] Wu JX. Problems and solutions regarding generalized functional safety in cyberspace. Secur Saf 2022; **1**: 2022001.
[6] Shen QK, Shi P and Zhu JW et al. Neural networks-based distributed adaptive control of nonlinear multiagent systems. IEEE Trans Neural Networks Learn Syst 2020; **31**: 1010–21.
[7] Fattahi M and Afshar A. Resilient sampled-data control of networked control systems against cyber attacks. Int J Dyn Control 2020; **8**: 205–17.
[8] Gao S, Zhang H and Wang ZP et al. Optimal injection attack strategy for cyber-physical systems: a dynamic feedback approach. Secur Saf 2022; **1**: 2022005.
[9] He WL, Xu WY and Ge XH et al. Secure control of multiagent systems against malicious attacks: a brief survey. IEEE Trans Ind Inf 2022; **18**: 3595–608.
[10] Liu H and Wang ZJ. Sampled-data-based consensus of multi-agent systems under asynchronous denial-of-service attacks. Nonlinear Anal Hybrid Syst 2021; **39**: 100969.
[11] Zhu YZ and Zheng WX. Observer-based control for cyber-physical systems with periodic DoS attacks via a cyclic switching strategy. IEEE Trans Autom Control 2020; **65**: 3714–21.
[12] Feng Z and Hu GQ. Distributed secure average consensus for linear multi-agent systems under DoS attacks. In: 2017 American Control Conference (ACC). Seattle, WA: IEEE, 2017, 2261–66.

[13] Gu Z, Huan Z and Yue D et al. Event-triggered dynamic output feedback control for networked control systems with probabilistic nonlinearities. Inf Sci 2018; **457, 458**: 99–112.
[14] Hu SL, Yue D and Xie XP et al. Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks. IEEE Trans Cybern 2019; **49**: 4271–81.
[15] Lu AY and Yang GH. Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service. IEEE Trans Autom Control 2018; **63**: 1813–20.
[16] Persis CD and Tesi P. Input-to-state stabilizing control under denial-of-service. IEEE Trans Autom Control 2015; **60**: 2930–44.
[17] Dong T and Gong YL. Leader-following secure consensus for second-order multi-agent systems with nonlinear dynamics and event-triggered control strategy under DoS attack. Neurocomputing 2020; **416**: 95–102.
[18] Li ZJ, Hua CC and Li K et al. Event-triggered control for high-order uncertain nonlinear multiagent systems subject to denial-of-service Attacks. IEEE Trans Syst Man Cybern Syst 2022; **52**: 6129–38.
[19] Shen QK, Shi Y and Jia RF et al. Design on type-2 fuzzy-based distributed supervisory control with Backlash-Like hysteresis. IEEE Trans Fuzzy Syst 2021; **29**: 252–261.
[20] Sun YC and Yang GH. Periodic event-triggered resilient control for cyber-physical systems under denial-of-service attacks. J Franklin Inst 2018; **355**: 5613–31.
[21] Zhang XM, Han QL and Yu XH. Survey on recent advances in networked control systems. IEEE Trans Ind Inf 2016; **12**: 1740–1752.
[22] Xu WY, Ho DWC and Li LL et al. Event-triggered schemes on leader-following consensus of general linear multiagent systems Under different topologies. IEEE Trans Cybern 2017; **47**: 212–23.
[23] Astrom KJ and Bernhardsson BO. Comparison of periodic and event based sampling for first-order stochastic systems. IFAC Proceedings Vol 1999, **32**: 5006–11.
[24] Hu WF, Yang CH and Huang TW et al. A distributed dynamic event-triggered control approach to consensus of linear multiagent systems with directed networks. IEEE Trans Cybern 2020; **50**: 869–74.
[25] Fan Y, Liu L and Feng G et al. Self-triggered consensus for multi-agent systems with zeno-free triggers. IEEE Trans Autom Control 2015; **60**: 2779–84.
[26] Pan KP, Lyu Y and Pan Q. Adaptive formation for multiagent systems subject to denial-of-service attacks. IEEE Trans Circuits Syst I Regul Pap 2022; **69**: 3391–3401.
[27] Wen GH, Duan ZS and Chen GR et al. Consensus tracking of multi-agent systems with Lipschitz-type node dynamics and switching topologies. IEEE Trans Circuits Syst I Regul Pap 2014; **61**: 499–511.
[28] Lu AY and Yang GH. Event-triggered secure observer-based control for cyber-physical systems under adversarial attacks. Inf Sci 2017; **420**: 96–109.
[29] Yang Y, Li YF and Yue D et al. Distributed secure consensus control with event-triggering for multiagent systems under DoS attacks. IEEE Trans Cybern 2021, **51**: 2916–28.
[30] Mohagheghi S, Venayagamoorthy GK and Harley RG. Optimal wide area controller and state predictor for a power system. IEEE Trans Power Syst 2007, **22**: 693–705.
[31] Wang CY, Zuo ZY and Qi ZQ et al. Predictor-based extended-state-observer design for consensus of MASs with delays and disturbances. IEEE Trans Cybern 2019, **49**: 1259–69.
[32] Du J, Li J and Lewis FL. Distributed 3D time-varying formation control of underactuated AUVs with communication delays based on data-driven state predictor. IEEE Trans Ind Inf 2023; **19**: 6963–71.
[33] Alfaki MMA and Masih S. Modeling and forecasting by using time series ARIMA models. Int J Eng Res Technol 2015; **4**: 914–18.
[34] Fan DY, Sun H and Yao J et al. Well production forecasting based on ARIMA-LSTM model considering manual operations. Energy 2021; **220**: 119708.
[35] Andres HM, Fujita H and Hayashi T et al. Forecasting of COVID19 per regions using ARIMA models and polynomial functions. Appl Soft Comput 2020; **96**: 106610.
[36] Xie YL, Jin MP and Zou ZP et al. Real-time prediction of docker container resource load based on a hybrid model of ARIMA and triple exponential smoothing. IEEE Trans Cloud Comput. 2022; **10**: 1386–1401.
[37] Tabatabaie Nezhad SM, Nazari M and Gharavol EA. A novel DoS and DDoS attacks detection algorithm using ARIMA time series model and chaotic system in computer networks. IEEE Commun Lett 2016; **20**: 700–3.
[38] Hao RL, Wang HB and Zhou MH et al. Distributed adaptive command filtered resilient event-triggered secure consensus control for multiagent systems under double DoS attacks. Expert Syst App 2023; **224**: 120016.
[39] Ma BX, Wang YF and Chen G. Event-triggered type-2 fuzzy-based sliding mode control for steer-by-wire systems. Mechatronics 2022; **82**: 102704.
[40] Hassan L, Zemouche A and Boutayeb M. A new observer-based controller design method for a class of time-varying delay systems with Lipschitz nonlinearities. In: 2014 American Control Conference. Portland, OR: IEEE, 2014, 4163–68.
[41] Yu ZQ, Zhang YM and Liu ZX et al. Distributed adaptive fractional-order fault-tolerant cooperative control of networked unmanned aerial vehicles via fuzzy neural networks. IET Control Theory App 2019; **13**: 2917–29.

Haichuan Yang received the M.S. degree in control theory and control engineering from Xi'an University of technology, Xi'an, China, in 2020. He is currently pursuing the Ph.D. degree in control science and engineering with Nanjing University of Aeronautics and Astronautics, Nanjing, China. His current research interests include resilient cooperative control of unmanned aerial vehicles and their applications.



Ziquan Yu received the Ph.D. degree in control science and engineering from Northwestern Polytechnical University, Xi'an, China, in 2019. From 2017 to 2019, he was a joint Ph.D. student supported by the China Scholarship Council with the Department of Mechanical, Industrial and Aerospace Engineering, Concordia University, Montreal, QC, Canada. He is currently with the College of Automation Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China. His current research interests include fault-tolerant cooperative control of safety-critical systems, and guidance, navigation, and control of unmanned aerial vehicles.

Youmin Zhang received the B.S., M.S., and Ph.D. degrees in automatic control from Northwestern Polytechnical University, Xi'an, China, in 1983, 1986, and 1995, respectively. He is currently a Professor with the Department of Mechanical, Industrial and Aerospace Engineering and the Concordia Institute of Aerospace Design and Innovation, Concordia University, Montreal, QC, Canada. His current research interests include guidance, navigation, and control, fault detection and diagnosis, fault-tolerant control, and remote sensing with applications to unmanned aerial/space/ground/marine vehicles, smart grids, smart cities, and cyber-physical systems.