SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

June 2022, Vol. 65 162204:1–162204:13
https://doi.org/10.1007/s11432-020-3148-x

Secure output synchronization of heterogeneous multi-agent systems against false data injection attacks

Shicheng HUO[1,3], Dalin HUANG[2,3] & Ya ZHANG[1,3*]

[1]*School of Automation, Southeast University, Nanjing* 210096*, China;*
[2]*School of Cyber Science and Engineering, Southeast University, Nanjing* 210096*, China;*
[3]*Key Laboratory of Measurement and Control of Complex Systems of Engineering, Ministry of Education, Nanjing* 210096*, China*

Received 5 August 2021/Revised 5 October 2021/Accepted 1 December 2021/Published online 19 May 2022

Abstract This paper studies secure output synchronization for heterogeneous multi-agent systems against false data injection (FDI) attacks. Both the sensors and actuators of agents may be injected into FDI attacks. To mitigate the malicious impact of these attacks on synchronization performance, a desired reference model, which is combined with an auxiliary system, is first designed for each agent to simulate its normal system dynamics. Then, based on this reference model, a state feedback cooperative controller and a static output feedback cooperative controller, which consist of adaptive compensators, are proposed, respectively. The integrated control protocols can ensure that the output synchronization error is small by adjusting some designed parameters even in the presence of FDI attacks. An illustrative example is employed to demonstrate the effectiveness of the proposed method.

Keywords output synchronization, false data injection attacks, adaptive compensators, heterogeneous multi-agent systems, secure control

Citation Huo S C, Huang D L, Zhang Y. Secure output synchronization of heterogeneous multi-agent systems against false data injection attacks. Sci China Inf Sci, 2022, 65(6): 162204, https://doi.org/10.1007/s11432-020-3148-x

1 Introduction

Previously, multi-agent systems (MASs) have been widely used in various practical engineering applications, such as intelligent energy management [1], swarm robots [2, 3], distributed estimation [4, 5] and formation control [6, 7]. The synchronization of MASs has been a popular research topic [8], and thus various synchronization algorithms have been constructed, such as fault-tolerant controllers [9,10], event-triggered control laws [11,12], and robust group synchronization controllers [13]. In practical applications, because it is difficult or impossible to ensure that all agents have identical system dynamics, synchronization of heterogeneous MASs have attracted increasing attention. Moreover, due to the extensive use of network communication in networked MASs, they are vulnerable to malicious cyber attacks, such as false data injection (FDI) attacks. Therefore, the problem of secure synchronization of heterogeneous MASs is a concern.

For heterogeneous MASs, output synchronization has been studied in [14–20]. For example, the novel distributed proportional-integral-derivative (PID)-like control protocols were designed in [14] for output containment and synchronization of heterogeneous high-order MASs. Both state feedback and output feedback controllers were designed for output synchronization of heterogeneous MASs in [15]. An observer-based sliding-mode consensus law was proposed in [16] to ensure that the output consensus error could converge to zero even in the case of external disturbances. Based on event-triggered communication among agents, [17] designed an output synchronization controller to guarantee that synchronization error can be globally bounded. More general nonlinear heterogeneous MASs were studied in [18–20].

* Corresponding author (email: yazhang@seu.edu.cn)

The above synchronization protocols were designed for attack-free networks. They may be ineffective for systems in the presence of FDI attacks where attackers directly inject false data into agents' sensors and/or actuators to cause synchronization performance to degrade or even to prevent synchronization among agents. Secure control for cyber-physical systems under sensor and actuator attacks has attracted increasing attention [21–23]. In recent years, several researchers have investigated synchronization control of MASs under FDI attacks. The commonly used methods to eliminate or mitigate the malicious effects of FDI attacks can be primarily classified into four types. The first method is that attacked agents are isolated from the entire communication network [24–27]. Before removing the attacked agent, it is necessary to detect and identify which agent is under an FDI attack. To ensure that state synchronization can be achieved, some fraction of the neighbors of any attacked agent need to be assumed to be secure. The second method is based on attack detection and on developing control protocols by neglecting information that was detected to be attacked [28]. The third method is based on robust control techniques. In [29–32] the attacks are assumed to be randomly injected into the agents where the probabilities of random attacks and the amplitudes of attack signals are relatively small. Otherwise, bounded state synchronization errors of the homogeneous MASs cannot be guaranteed. The fourth method is based on mitigating adverse impacts of FDI attacks. Several research papers have established resilient state synchronization protocols for homogeneous MASs to mitigate FDI attacks [33–35]. Specifically, a resilient adaptive synchronization protocol was constructed in [33] by designing novel state simulators to emulate the ideal state trajectories of the agents. Then, based on [33], Modares et al. [34] investigated leader-following synchronization for a more general high-order system model subject to dynamic disturbances and leaderless synchronization was studied in [35].

Based on the above discussion, most studies of the synchronization of networks under FDI attacks [24–27, 29–36] have focused on homogeneous MASs, while few have investigated the synchronization of heterogeneous MASs. Because heterogeneous MASs have been widely applied in practical applications, it is important to investigate the synchronization of heterogeneous MASs under FDI attacks. The primary challenges for addressing this, in contrast to homogeneous MASs, are that adaptive attack compensators cannot be directly designed and only using an adaptive compensator in homogeneous MASs is not enough for a system to achieve output synchronization. This paper investigates secure output synchronization for heterogeneous MASs against FDI attacks. The primary contributions are as follows:

• Both an auxiliary system and a reference model are constructed simultaneously for the first time for each agent where the auxiliary system needs to use a neighbors' information and the reference model is the prerequisite for designing a resilient control protocol. However, only the reference models were designed for homogeneous MASs under FDI attacks in [33–35] and only the auxiliary systems were designed for the heterogeneous MASs in the absence of FDI attacks in [15–17].

• Unlike [29–32] where random attacks were considered, this paper studies successive attack signals and proposes adaptive compensators to mitigate the impact of successive FDI attack signals on output synchronization performance. Based on such compensators, a resilient state feedback cooperative controller and a resilient static output feedback cooperative controller are designed, respectively.

Organization. In Section 2, the heterogeneous MASs under attacks are described and the form of resilient control protocol is provided. In Section 3, the reference models are designed and the secure output synchronization problems are addressed by using the developed resilient control protocols. A simulation example is provided in Section 4 to verify the validity of our proposed techniques. The content of this paper is concluded in Section 5.

Notations. $\lambda(\cdot)$ and $\lambda_{\min}(\cdot)$ represent the eigenvalue and the minimum eigenvalue of a matrix, respectively. $\mathbb{R}^n$ represents the set of n-dimensional column vectors. $\mathrm{Re}(\cdot)$ represents the real part of a number. $\otimes$ represents the Kronecker product. $\mathrm{diag}\{\cdot\}$ represents the block-diagonal matrix. $\mathrm{col}(\eta_1, \eta_2, \ldots, \eta_N)$ denotes a column vector with η_i as its elements. $\|\cdot\|_2$ represents the 2-norm. Δ^{T} represents the transpose of matrix Δ.

Graph theory. The communication topology is described by a directed graph $\mathscr{G} = (\mathscr{V}, \mathscr{E}, \mathscr{A})$. where $\mathscr{V} = \{1, 2, \ldots, N\}$ denotes the node set, $\mathscr{E} = \mathscr{V} \times \mathscr{V}$ denotes the edge set, and $\mathscr{A} = [a_{ij}]_{N\times N}$ denotes the weighted adjacency matrix, where $a_{ii} = 0$. If there exists a directed edge from agent j to agent i, i.e., $(j, i) \in \mathscr{E}$, $a_{ij} > 0$; else, $a_{ij} = 0$. The set of nodes with edges incoming to node i is called the neighbor set of node i, i.e., $\mathscr{N}_i = \{j : (j, i) \in \mathscr{E}\}$. The Laplacian matrix $\mathcal{L} = [l_{ij}]_{N\times N}$ is obtained as $\mathcal{L} = \mathscr{D} - \mathscr{A}$ where the sum of each row equals zero. $\mathscr{D} = \mathrm{diag}(d_i)$ is called the in-degree matrix, where $d_i = \sum_{j\in\mathscr{N}_i} a_{ij}$ is the weighted in-degree of node i. A directed graph has a directed spanning tree if there exists at least one node called the root node, which has a directed path to all other nodes. A diagonal

matrix $\mathcal{G} = \text{diag}\{g_{10}, g_{20}, \ldots, g_{N0}\}$ is the leader adjacency matrix, where $g_{i0} = 1$ if node i can receive information from the leader, and $g_{i0} = 0$ otherwise.

2 Problem formulation and preliminaries

2.1 Heterogeneous multi-agent systems under attacks

Consider a group of agents which are described by N heterogeneous linear systems

$$\begin{cases} \dot{x}_i = A_i x_i + B_i u_i^d, \\ y_i = C_i x_i, \end{cases} \tag{1}$$

where $x_i \in \mathbb{R}^{n_i}$, $y_i \in \mathbb{R}^m$, and $u_i^d \in \mathbb{R}^{p_i}$ respectively denote state, output and damaged control input of agent i, $i = 1, 2, \ldots, N$. The matrices A_i, B_i, and C_i are known with compatible dimensions which may be different for all agents.

Let the leader dynamics be described as follows:

$$\begin{cases} \dot{\tau} = S\tau, \\ \psi = D\tau, \end{cases} \tag{2}$$

where $\tau \in \mathbb{R}^{n_0}$ and $\psi \in \mathbb{R}^m$ are the state and output of the leader, respectively.

Assumption 1. The directed graph $\mathscr{G}$ contains a spanning tree with the leader as its root.

Assumption 2. The matrix pairs (A_i, B_i), $i = 1, 2, \ldots, N$, are stabilizable.

Assumption 3. The matrix pair (S, D) is detectable.

Assumption 4. For all $i = 1, 2, \ldots, N$, there exist matrix pairs (Ξ_i, Λ_i) satisfying the following linear matrix equations

$$\begin{cases} \Xi_i S = A_i \Xi_i + B_i \Lambda_i, \\ C_i \Xi_i = D. \end{cases} \tag{3}$$

Remark 1. Assumption 1 is the necessary topology condition to guarantee that MASs can achieve synchronization. Stabilizability in Assumption 2 and detectability in Assumption 3 are two basic properties of control systems, which are satisfied in many practical system models. Assumption 4 is the output regulation equation [15], which is necessary for output synchronization of heterogeneous MASs and can be satisfied in some practical system models. In general, synchronization is used to describe the common behavior of nonlinear coupling complex networks and consensus is used to describe the common behavior among multiple agents. Inspired by [8], consensus of linear MASs can be considered a special case of synchronization of complex networks. There is some literature [17, 34] calling the consensus of MASs as synchronization of MASs. Therefore, synchronization of MASs means consensus of MASs throughout the paper.

In this paper, the attack model in the networked MASs is that the attacker continuously injects false data into the sensors and actuators of agents rather than intermittently as [29–32], which are shown in Figures 1 and 2. The communication links among agents are assumed to be secure. It can be seen from Figures 1 and 2 that the purpose of the attacker is to inject false data such that the actuators and controllers cannot obtain true control inputs and system states/outputs, respectively, thus degrading the output synchronization performance of the system.

The actuators of the agents are attacked and the mathematical model of the attack on actuator is given as

$$u_i^d = u_i + \mu_i^a, \tag{4}$$

where u_i is the resilient control protocol to be designed, μ_i^a is the injected attack signal into the actuator and u_i^d is the damaged control input which is used by the actuator of agent i.

When the state information is available, the attacker injects attack signal to agents' states, which is shown as Figure 1. Under the attack, the state that the agent obtains can be described as

$$x_i^d = x_i + \chi_i^a, \tag{5}$$

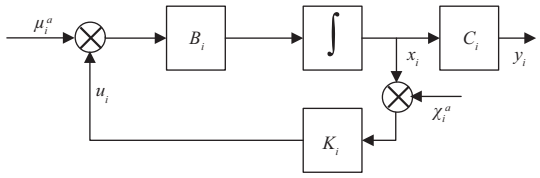

Figure 1 Attack modeling under state feedback control strategy.

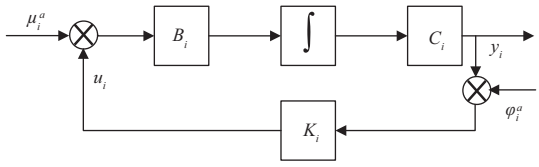

Figure 2 Attack modeling under static output feedback control strategy.

where x_i is the state, χ_i^a is the attack signal injected into the sensor of agent i, and x_i^d is the damaged state information which is actually used by the controller.

In some practical applications, state information are not usually available and only the measurement output information can be used. Thus, when the output information is available, the attacker injects attack signal into agents' outputs, which is shown as Figure 2. Under the attack, the output that the agent obtains can be depicted as

$$y_i^d = y_i + \varphi_i^a, \tag{6}$$

where y_i is the output, φ_i^a is the attack signal, and y_i^d is the damaged output information employed by the controller.

Assumption 5. The attack signals in (4)–(6) are bounded and differentiable.

Remark 2. The attack signal is bounded since the energy of the attack is limited as it happens in some real situations. For instance, a number of electronic devices operate at batteries of limited power, and if they are employed as the attack emitters, the attack signal is consequently bounded. There is also differentiable attack signal in practice. For example, harmonic sinusoidal oscillator is commonly used as signal generation machine, which can generate sinusoidal wave by self-oscillating circuit without additional input signal. If the harmonic sinusoidal oscillator is used as the attack emitter, the attack signal is differentiable.

2.2 Resilient control protocols

To mitigate the malicious impacts of FDI attacks, for the state feedback (SF) control strategy, the resilient control protocol is designed as

$$u_i = u_{s,i} + u_{cs,i}, \tag{7}$$

where $u_{s,i} = K_i(x_i^d - \Xi_i\pi_i) + \Lambda_i\pi_i$ is a standard SF controller which uses corrupted state information x_i^d, π_i is the state of the auxiliary system, Ξ_i and Λ_i can be calculated by using regulation equations (3), and K_i is the gain matrix to be designed. $u_{cs,i} = -z_i$ is the adaptive compensator to be designed later.

For the output feedback (OF) control strategy, the resilient control protocol is designed as

$$u_i = u_{o,i} + u_{co,i}, \tag{8}$$

where $u_{o,i} = K_i\left(y_i^d - C_i\Xi_i\pi_i\right) + \Lambda_i\pi_i$, π_i is the state of the auxiliary system to be designed, Ξ_i and Λ_i can be calculated from regulation equations (3). $u_{co,i} = -\bar{z}_i$ is the compensator to be designed later,

In both SF and OF control strategy of the MAS, the agents transmit their auxiliary system states to their neighbors and the auxiliary system of π_i is designed as

$$\begin{aligned} \dot{\pi}_i &= S\pi_i - \epsilon H\beta_i, \\ \beta_i &= \sum_{j=1}^{N} a_{ij}\left(\pi_i - \pi_j\right) + g_{i0}\left(\pi_i - \tau\right), \end{aligned} \tag{9}$$

where H and ϵ need to be designed.

Remark 3. It is worth mentioning that the standard SF and OF controllers cannot synchronize the output of the agents with that of the leader in the presence of FDI attacks. In detail, under the attack models (4)–(6), the heterogeneous MASs (1) under the standard SF controller is deteriorated into

$$\dot{x}_i = A_ix_i + B_iu_i^d = A_ix_i + B_iu_{n,i} + B_if_i, \tag{10}$$

where

$$\begin{aligned} u_{n,i} &= u_{n,i}^s = K_i\left(x_i - \Xi_i\pi_i\right) + \Lambda_i\pi_i, \\ f_i &= f_i^s = \mu_i^a + K_i\chi_i^a. \end{aligned} \tag{11}$$

The heterogeneous MASs (1) under the standard OF controller is deteriorated into system (10) with

$$\begin{aligned} u_{n,i} &= u_{n,i}^o = K_i\left(y_i - C_i\Xi_i\pi_i\right) + \Lambda_i\pi_i, \\ f_i &= f_i^o = \mu_i^a + K_i\varphi_i^a. \end{aligned}$$

If there is only the normal parts $(A_ix_i + B_iu_{n,i})$ in (10), the output synchronization can be achieved as demonstrated in [37]. However, due to the existence of the injected attack term B_if_i, the output synchronization cannot be achieved without the introduction of the adaptive compensators. Therefore, it is necessary to introduce the adaptive compensators to suppress the detrimental impacts of sustained FDI attacks.

Remark 4. It is easy to see from (10) that the attack signal injected into one agent can only affect that agent's dynamics. This is because if the agent is under attack, i.e., if f_i is nonzero, it can only affects the state of the corresponding agent, but not the auxiliary system state π_i in (9). The corrupted state of an agent is not transmitted to other agents. β_i defined in (9) is the only part in the agent dynamics (10) that requires neighbor information. Since the auxiliary state π_i is secure, the attacks can only affect the attacked agents such that they cannot track the leader's output, but cannot cause the output synchronization error of other secure agents to be nonzero. Therefore, the designed compensator only needs to use the information of each agent, not the distributed information.

3 Secure output synchronization against attacks

In this section, the resilient control protocols consisting of standard control protocols and adaptive compensators are designed to guarantee that output synchronization for heterogeneous MASs can be achieved in the presence of FDI attacks.

3.1 Heterogeneous reference models

Before designing the resilient control protocols, a reference model, which operates in an expected normal system dynamics in the absence of attacks, needs to be constructed for each agent. Let the state of reference model for agent i be $\bar{x}_i$. Then, the reference model is designed as

$$\begin{cases} \dot{\bar{x}}_i = A_i\bar{x}_i + B_i\bar{u}_i, \\ \bar{y}_i = C_i\bar{x}_i, \end{cases} \tag{12}$$

where $\bar{u}_i = K_i(\bar{x}_i - \Xi_i\pi_i) + \Lambda_i\pi_i$ for the case of SF control, $\bar{u}_i = K_i(\bar{y}_i - C_i\Xi_i\pi_i) + \Lambda_i\pi_i$ for the case of static OF control, and π_i is defined in (9).

Before proving that the standard control protocols can enable the heterogeneous reference models to track the outputs of leaders, Lemma 1 is given.

Lemma 1 ([38])**.** Suppose that Assumption 1 holds. Let symmetric matrices X and T be positive definite. The gain matrix H in (9) is designed as $H = T^{-1}P$, where P is the unique symmetric positive-definite solution of the following algebraic Riccati equation (ARE):

$$S^{\mathrm{T}}P + PS + X - PT^{-1}P = 0. \tag{13}$$

Then, the following equation holds:

$$\lim_{t\to\infty}\left(\pi_i(t) - \tau(t)\right) = 0, \tag{14}$$

if

$$\epsilon \geqslant \frac{1}{2\underline{\lambda}_m}, \tag{15}$$

where $\underline{\lambda}_m = \min(\mathrm{Re}(\lambda(\mathcal{L} + \mathcal{G})))$.

Then, we give a condition on the output synchronization for the reference model (12) with leader (2).

Theorem 1. Suppose that Assumptions 1–4 hold. Output synchronization for the heterogeneous reference system (12) with leader (2) can be achieved under the SF regulation protocol, if $A_i + B_iK_i$ is Hurwitz, Ξ_i and Λ_i are solutions of regulation equations (3), and H and ϵ are designed in Lemma 1.

Proof. For $i = 1, 2, \ldots, N$, define $\bar{\eta}_i \triangleq \bar{x}_i - \Xi_i\pi_i$ and $\varpi_i \triangleq \pi_i - \tau$. Then, we have

$$\begin{aligned}\dot{\bar{\eta}}_i &= \dot{\bar{x}}_i - \Xi_i\dot{\pi}_i\\ &= A_i\bar{x}_i + B_i\bar{u}_i - \Xi_i\left(S\pi_i + \epsilon H\beta_i\right)\\ &= A_i\bar{x}_i + B_iK_i\bar{\eta}_i + B_i\Lambda_i\pi_i - A_i\Xi_i\pi_i - B_i\Lambda_i\pi_i - \epsilon\Xi_iH\beta_i.\end{aligned}$$

Based on Kronecker product, one has

$$\dot{\bar{\eta}} = \left(A + BK\right)\bar{\eta} - \epsilon\Xi\left(\mathcal{L} + \mathcal{G}\right)\otimes H\varpi,$$

where $\Delta \triangleq \mathrm{diag}(\Delta_i, i = 1, 2, \ldots, N)$, $(\Delta = A,\ B,\ K,\ \Xi)$, $\bar{\eta} \triangleq \mathrm{col}(\bar{\eta}_1, \bar{\eta}_2, \ldots, \bar{\eta}_N)$, and $\varpi \triangleq \mathrm{col}(\varpi_1, \varpi_2, \ldots, \varpi_N)$.

According to Lemma 1, it is obtained that

$$\lim_{t\to\infty}\varpi(t) = 0.$$

Subsequently, it is easy to know that $\lim_{t\to\infty}\bar{\eta}_i(t) = 0$ if $A_i + B_iK_i$ is Hurwitz. Then, we have $\lim_{t\to\infty}\bar{y}_i(t) = \lim_{t\to\infty}C_i\Xi_i\pi_i(t) = \lim_{t\to\infty}D\tau(t) = \lim_{t\to\infty}\psi(t)$. This means that output synchronization for heterogeneous reference system (12) with leader (2) can be achieved under SF control protocol. This proof is completed.

Similarly, under static OF control protocol, it can be obtained that output synchronization can be achieved if $A_i + B_iK_iC_i$ is Hurwitz.

Remark 5. It is worth noting that according to (10), attacks can adversely affect the agent dynamics such that the output synchronization cannot be achieved, while they cannot influence the dynamics of the reference model (12). Therefore, the standard regulation protocols can be designed to ensure that the output of reference model $\bar{y}_i$ can converge to the leader's output ψ. What is more important is that we can take advantage of the difference between the agent's state under attacks and the state of the reference model (which operates in an expected normal system dynamics in the absence of attack) to estimate the FDI attacks and compensate for them.

In the following, based on the reference model (12), the resilient control protocols are designed to deal with the attacked term in order to mitigate the adverse influence of the attacks on output synchronization. Accordingly, the output synchronization errors can be very small even in the presence of FDI attacks.

3.2 State feedback control protocol

Firstly, let K_i in the resilient SF regulation protocol (7) and the reference model (12) be calculated as

$$K_i = -R_i^{-1}B_i^{\mathrm{T}}P_i, \tag{16}$$

where the symmetric positive definite matrix $P_i > 0$ is the solution to

$$A_i^{\mathrm{T}}P_i + P_iA_i + Q_i - P_iB_iR_i^{-1}B_i^{\mathrm{T}}P_i = 0, \tag{17}$$

and $R_i > 0$ and $Q_i > 0$ are symmetric positive definite matrices that can be selected to adjust the synchronization error.

Now, recall the resilient SF control protocol

$$u_i = K_i(x_i^d - \Xi_i\pi_i) + \Lambda_i\pi_i - z_i, \tag{18}$$

where the adaptive compensation term z_i is updated as

$$\dot{z}_i = -\vartheta_iK_i(x_i^d - \bar{x}_i) - \vartheta_iz_i, \tag{19}$$

and $\vartheta_i > 0$ is a scalar design parameter to adjust the synchronization error.

Theorem 2. Consider the heterogeneous MASs (10) under FDI attacks as shown in Figure 1. Suppose that Assumptions 1–5 hold. Let the control input be constructed as (18) and (19), Ξ_i and Λ_i be the solution of regulation equations (3). Then, the output synchronization of MASs (10) can be achieved with bounded synchronization error, which can be adjusted by selecting matrices R_i, Q_i and scalar ϑ_i.

Proof. From Theorem 1, it is easy to obtain that the output of reference model $\bar{y}_i$ can track the leader output ψ. Hence, if the actual state x_i can converge to the state of reference model $\bar{x}_i$, then by using the regulation equations (3), the output synchronization is ensured. Define tracking error between the agent i's state and the reference state as

$$\hat{x}_i = x_i - \bar{x}_i. \tag{20}$$

Then, according to (10), (12), (18), and (19), we obtain

$$\dot{\hat{x}}_i = (A_i + B_i K_i)\,\hat{x}_i - B_i \hat{z}_i, \tag{21}$$

where $\hat{z}_i = z_i - f_i^s$ and the dynamics of z_i becomes

$$\begin{aligned}\dot{z}_i &= -\vartheta_i K_i (x_i^d - \bar{x}_i) - \vartheta_i z_i \\ &= -\vartheta_i K_i \hat{x}_i - \vartheta_i z_i - \vartheta_i K_i \chi_i^a \\ &= -\vartheta_i K_i \hat{x}_i - \vartheta_i \hat{z}_i - \vartheta_i \bar{f}_i \\ &= \vartheta_i R_i^{-1} B_i^{\mathrm{T}} P_i \hat{x}_i - \vartheta_i \hat{z}_i - \vartheta_i \bar{f}_i,\end{aligned} \tag{22}$$

where $\bar{f}_i = 2f_i^s - \mu_i^a$. It is not difficult to find that $\bar{f}_i = f_i^s$ when the attacker only injects the attack into the actuator.

Then, we choose the following Lyapunov function

$$V_i = \hat{x}_i^{\mathrm{T}} P_i \hat{x}_i + \vartheta_i^{-1} \hat{z}_i^{\mathrm{T}} R_i \hat{z}_i. \tag{23}$$

Based on (21) and (22), the derivative of the Lyapunov function is

$$\begin{aligned}\dot{V}_i =& \hat{x}_i^{\mathrm{T}} (A_i^{\mathrm{T}} P_i + P_i A_i - 2P_i B_i R_i^{-1} B_i^{\mathrm{T}} P_i)\hat{x}_i - 2\hat{x}_i^{\mathrm{T}} P_i B_i \hat{z}_i + 2\hat{x}_i^{\mathrm{T}} (P_i B_i R_i^{-1}) R_i \hat{z}_i - 2\hat{z}_i^{\mathrm{T}} R_i \hat{z}_i \\ & - 2\hat{z}_i^{\mathrm{T}} R_i (\bar{f}_i + \vartheta_i^{-1} \dot{f}_i^s) \\ =& \hat{x}_i^{\mathrm{T}} (A_i^{\mathrm{T}} P_i + P_i A_i - 2P_i B_i R_i^{-1} B_i^{\mathrm{T}} P_i)\hat{x}_i - 2\hat{z}_i^{\mathrm{T}} R_i \hat{z}_i - 2\hat{z}_i^{\mathrm{T}} R_i (\bar{f}_i + \vartheta_i^{-1} \dot{f}_i^s).\end{aligned} \tag{24}$$

From (17), we have

$$\dot{V}_i = -\hat{x}_i^{\mathrm{T}} Q_i \hat{x}_i - \hat{x}_i^{\mathrm{T}} (P_i B_i R_i^{-1} B_i^{\mathrm{T}} P_i)\hat{x}_i - 2\hat{z}_i^{\mathrm{T}} R_i \hat{z}_i - 2\hat{z}_i^{\mathrm{T}} R_i (\bar{f}_i + \vartheta_i^{-1} \dot{f}_i^s). \tag{25}$$

Due to the fact that the second term in (25) is negative, we have

$$\dot{V}_i \leqslant -\hat{x}_i^{\mathrm{T}} Q_i \hat{x}_i - 2\hat{z}_i^{\mathrm{T}} R_i \hat{z}_i - 2\hat{z}_i^{\mathrm{T}} R_i (\bar{f}_i + \vartheta_i^{-1} \dot{f}_i^s). \tag{26}$$

Then, using Young's inequality to the last term of (26) deduces

$$\dot{V}_i \leqslant -\hat{x}_i^{\mathrm{T}} Q_i \hat{x}_i + (\bar{f}_i + \vartheta_i^{-1} \dot{f}_i^s)^{\mathrm{T}} R_i (\bar{f}_i + \vartheta_i^{-1} \dot{f}_i^s). \tag{27}$$

From (27), we can obtain that $\dot{V}_i < 0$, if

$$\|\hat{x}_i\|_2 > \frac{\lambda_{\max}(R_i)}{\lambda_{\min}(Q_i)} \|(\bar{f}_i + \vartheta_i^{-1} \dot{f}_i^s)\|_2. \tag{28}$$

Then, one has $\lim_{t\to\infty} \|\hat{x}_i(t)\|_2 = \lim_{t\to\infty} \|x_i(t) - \bar{x}_i(t)\|_2 \leqslant \theta_i$, θ_i is a small parameter which denotes the bound of the tracking error between the x_i and the reference model $\bar{x}_i$. The error bound θ_i can be adjusted by increasing ϑ_i in the update equation (19), increasing the parameter Q_i or decreasing R_i in ARE (17). Based on $\lim_{t\to\infty} \bar{\eta}_i(t) = \lim_{t\to\infty} \bar{x}_i(t) - \Xi_i \pi_i(t) = 0$, one has $\lim_{t\to\infty} \|\eta_i(t)\|_2 = \lim_{t\to\infty} \|x_i(t) - \Xi_i \pi_i(t)\|_2 \leqslant \theta_i$. Then, we have $\lim_{t\to\infty} \|y_i(t) - C_i \Xi_i \pi_i(t)\|_2 \leqslant C_i \theta_i \triangleq \varsigma_i$, i.e., $\lim_{t\to\infty} \|y_i(t) - D\tau(t)\|_2 = \lim_{t\to\infty} \|y_i(t) - \psi(t)\|_2 \leqslant \varsigma_i$. Therefore, the output synchronization error bound can be made very small by adjusting the parameters in (28), which shows that the adaptive compensator can mitigate the impact of the FDI attacks. This completes the proof.

3.3 Static output feedback control protocol

Firstly, consider that the coupled gain K_iC_i in the control protocol (8) and the reference model (12) is calculated as

$$K_iC_i = -R_i^{-1}(B_i^{\mathrm{T}}P_i + M_i), \tag{29}$$

where $R_i > 0$ is a given symmetric positive definite matrix that can be selected to adjust the synchronization error, and the symmetric positive definite matrix $P_i > 0$ is the solution to

$$A_i^{\mathrm{T}}P_i + P_iA_i + C_i^{\mathrm{T}}C_i - P_iB_iR_i^{-1}B_i^{\mathrm{T}}P_i + M_i^{\mathrm{T}}R_i^{-1}M_i = 0. \tag{30}$$

Then, recall the resilient OF control protocol

$$u_{o,i} = K_i(y_i^d - C_i\Xi_i\pi_i) + \Lambda_i\pi_i - \bar{z}_i, \tag{31}$$

where $\bar{z}_i$ is updated as

$$\dot{\bar{z}}_i = -\vartheta_iR_i^{-1}B_i^{\mathrm{T}}P_i(C_i^{\mathrm{T}}C_i)^{\dagger}C_i^{\mathrm{T}}(y_i^d - \bar{y}_i) - \vartheta_i\bar{z}_i, \tag{32}$$

$\vartheta_i > 0$ is a scalar design parameter to adjust the synchronization error, and $\dagger$ denotes the pseudo inverse.

Remark 6. In the SF control, the controller gain K_i can be directly calculated by using ARE (16) and (17). However, in the static OF control, K_i cannot be solved directly due to the introduction of matrix C_i. Therefore, inspired by [39], an iterative algorithm is provided to find the gain of static OF controller.

(1) Initialize: Set $\hbar = 0$, $M_i^0 = 0$, and choose R_i and a feasible gain K_i^0.

(2) $\hbar$th iteration: given $K_i^{\hbar}$, solve the $P_i^{\hbar}$ by using the following equation:

$$(A_i + B_iK_i^{\hbar}C_i)^{\mathrm{T}}P_i^{\hbar} + P_i^{\hbar}(A_i + B_iK_i^{\hbar}C_i) + C_i^{\mathrm{T}}(K_i^{\hbar})^{\mathrm{T}}R_iK_i^{\hbar}C_i + C_i^{\mathrm{T}}C_i + (M_i^{\hbar})^{\mathrm{T}}R_i^{-1}M_i^{\hbar} = 0.$$

(3) Update the gain $K_i^{\hbar}$ and the matrix $M_i^{\hbar}$ by the following equation:

$$\begin{aligned} K_i^{\hbar+1} &= -R_i^{-1}(B_i^{\mathrm{T}}P_i^{\hbar} + M_i^{\hbar})C_i^{\mathrm{T}}(C_iC_i^{\mathrm{T}})^{-1}, \\ M_i^{\hbar+1} &= -R_iK_i^{\hbar+1}C_i - B_i^{\mathrm{T}}P_i^{\hbar}. \end{aligned}$$

If $K_i^{\hbar+1}$ and $K_i^{\hbar}$ are sufficiently approximate, go to step (4); otherwise, set $\hbar = \hbar + 1$ and rerun step (2).

(4) Terminate: Set $K_i = K_i^{\hbar}$.

Theorem 3. Consider the heterogeneous MASs (10) under FDI attacks shown as Figure 2. Suppose that Assumptions 1–5 hold. Let the control input be designed as (31) and (32), Ξ_i and Λ_i be the solution of regulation equations (3). Then, the output synchronization of MASs (10) can be achieved with bounded synchronization error, which can be adjusted by selecting matrix R_i and scalar ϑ_i.

Proof. According to (10), (12), (20), (31), and (32), we have

$$\dot{\hat{x}}_i = (A_i + B_iK_iC_i)\hat{x}_i - B_i\tilde{z}_i, \tag{33}$$

where $\tilde{z}_i = \bar{z}_i - f_i^o$ and the dynamics of $\bar{z}_i$ becomes

$$\dot{\tilde{z}}_i = -\vartheta_iR_i^{-1}B_i^{\mathrm{T}}P_i\hat{x}_i - \vartheta_i\tilde{z}_i - \vartheta_i\tilde{f}_i, \tag{34}$$

where $\tilde{f}_i = 2f_i^o - \mu_i^a$.

Choose the Lyapunov function candidate as

$$V_i = \hat{x}_i^{\mathrm{T}}P_i\hat{x}_i + \vartheta_i^{-1}\tilde{z}_i^{\mathrm{T}}R_i\tilde{z}_i. \tag{35}$$

Then, based on (33) and (34), the derivative of the Lyapunov function is

$$\dot{V}_i = \hat{x}_i^{\mathrm{T}}((A_i + B_iK_iC_i)^{\mathrm{T}}P_i + P_i(A_i + B_iK_iC_i))\hat{x}_i - 2\tilde{z}_i^{\mathrm{T}}R_i\tilde{z}_i - 2\tilde{z}_i^{\mathrm{T}}R_i(\tilde{f}_i + \vartheta_i^{-1}\dot{f}_i^o). \tag{36}$$

According to (29) and (30), it is obtained that $A_i + B_iK_iC_i$ is Hurwitz and $P_i > 0$. Then there exists a positive definite matrix Ψ_i such that

$$\dot{V}_i \leqslant -\hat{x}_i^{\mathrm{T}}\Psi_i\hat{x}_i - 2\tilde{z}_i^{\mathrm{T}}R_i\tilde{z}_i - 2\tilde{z}_i^{\mathrm{T}}R_i(\tilde{f}_i + \vartheta_i^{-1}\dot{f}_i^o). \tag{37}$$

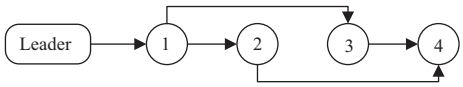

Figure 3 Communication topology.

After some operations similar to Theorem 2, the premise of $\dot{V}_i < 0$ is that

$$\|\hat{x}_i\|_2 > \frac{\lambda_{\max}(R_i)}{\lambda_{\min}(\Psi_i)}\|(\tilde{f}_i + \vartheta_i^{-1}\dot{f}_i^o)\|_2. \tag{38}$$

Then, similar to the proof of Theorem 2, the output synchronization error can be small by adjusting the parameters in (38), which shows that the adaptive compensator can mitigate the impact of the FDI attacks. This completes the proof.

Remark 7. It can be seen from Remark 6 that the design of static OF control gain is more complicated than that of SF control gain. Both the adaptive compensation term and the design of control gain in OF control are more complex. Meanwhile, for the case of SF control, the parameters ϑ_i, Q_i, and R_i in (28) can be adjusted to make the output synchronization error smaller. However, due to that the static OF control reduces the degree of freedom of the ARE (30), the introduction of static OF control results in fewer adjustable parameters in (38). This may give rise to worse output synchronization performance compared to SF control.

Remark 8. It can be seen from (28) and (38) that the faster the attack signals change, i.e., the larger the $\dot{f}_i^s$ and $\dot{f}_i^o$ are, the larger the ϑ_i is required. Therefore, $\dot{f}_i^s$ and $\dot{f}_i^o$ are not demanded to be small as [36] due to compensation term z_i and $\bar{z}_i$ in the resilient control protocols. On the other hand, because the results are given in 2-norm form in (28) and (38), the attack signals need to be Lebesgue square integrable such that the right side of (28) and (38) can be finite. This leads to a certain conservatism in the considered attack models.

4 An illustrative example

In this section, a numerical example is used to demonstrate that the proposed method can achieve secure output synchronization against FDI attacks. Consider that the heterogeneous MASs consists of four followers and one leader, and the communication among them is represented by a directed graph shown as Figure 3.

Refer to [40], the ith follower's dynamics are given as

$$\begin{cases} \dot{x}_i = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & -l_i & -k_i \end{bmatrix} x_i + \begin{bmatrix} 0 \\ 0 \\ b_i \end{bmatrix} u_i, \\ y_i = [1\ 0\ 0]\, x_i, \end{cases}$$

where the parameters satisfy b_i, k_i, $l_i > 0$ and the three state variables represent position, velocity, and acceleration, respectively. For each follower, the corresponding parameters are specified as $\{1, 2, 10\}$, $\{2, 1, 3\}$, $\{1, 2, 5\}$, $\{2, 3, 1\}$. The dynamics of the leader are given by

$$\dot{\tau} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \tau, \quad \psi = [1\ 0]\, \tau.$$

Let $X = \mathrm{diag}\{1, 1\}$ and $T = \mathrm{diag}\{3, 2\}$. Then, based on ARE (13), $H = [0.4553, 0.2899; 0.4349, 1.1152]$ can be obtained and choose $\epsilon = 0.6$. According to regulation equations (3) and the given parameters, the pairs Ξ_i and Λ_i can be calculated as $\Xi_i = [1, 0; 0, 1; 0, 0]$ and $\Lambda_i = [0\ l_i/b_i]$. Given $Q_i = \mathrm{diag}\{1, 1, 1\}$ and $R_i = 0.8$ for all the followers, then the SF control gains can be obtained from (16) as

$$K_1 = -[1.5811\ 0.5458\ 0.7553], \quad K_2 = -[1.5811\ 1.9015\ 1.6567],$$
$$K_3 = -[1.5811\ 1.0655\ 0.9379], \quad K_4 = -[1.5811\ 2.8898\ 1.2640].$$

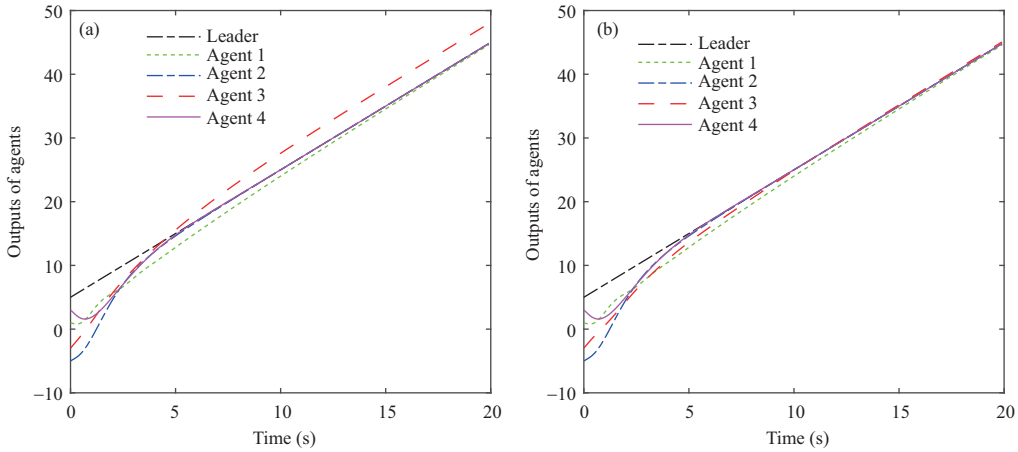

Figure 4 (Color online) Agents' outputs under the biasing attack signal in the actuator of agent 3 using the standard SF control protocol (a) and the improved resilient control protocol (b), respectively.

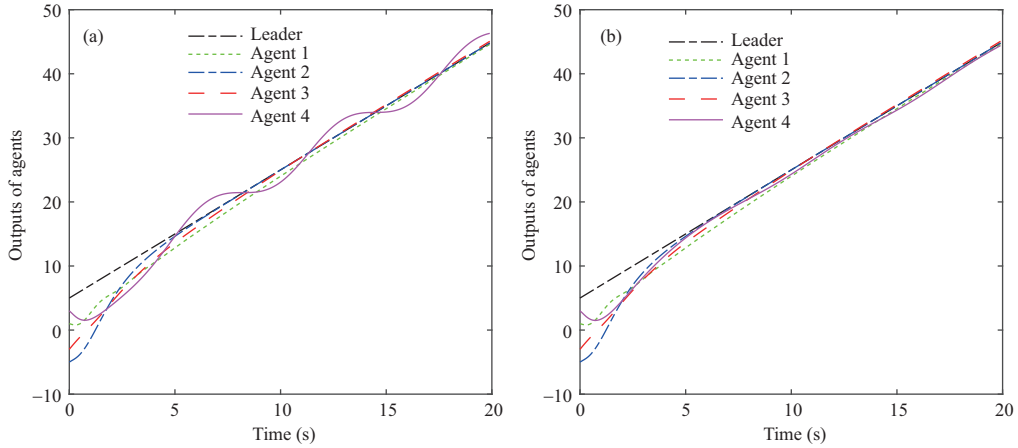

Figure 5 (Color online) Agents' outputs under the harmonic sinusoidal attack signal in the sensor of agent 4 using the standard SF control protocol (a) and the improved resilient control protocol (b), respectively.

Now, three types of successive attack signals (i.e., biasing attack, harmonic sinusoidal attack, and compound attack) are used to demonstrate the effectiveness of the proposed control protocol. These attacks affect the control signal and system state signal, respectively. The initial conditions are $\tau(0) = [5\ 2]^{\mathrm{T}}$, $x_1(0) = [1\ -1\ 2]^{\mathrm{T}}$, $x_2(0) = [-5\ 2\ -1]^{\mathrm{T}}$, $x_3(0) = [-3\ 4\ -1]^{\mathrm{T}}$, and $x_4(0) = [3\ -3\ -2]^{\mathrm{T}}$.

4.1 Biasing attack signal on actuator

The biasing attack is assumed to be injected into actuator of follower 3, i.e., $\mu_3^a = 5$ and let $\vartheta_3 = 0.5$. Consequently, the output of each agent is shown in Figure 4(a), where the standard SF control protocol $u_{s,i}$ in (7) without the adaptive compensator is employed. It is easy to find that the output synchronization cannot be achieved and the bounds of synchronization errors maintain relatively large. If we apply the resilient control protocol u_i in (7) to counter FDI attacks, the trajectories of the agents are shown in Figure 4(b). It is obvious that compared to the case under the standard control protocol $u_{s,i}$, the improved resilient control protocol u_i can achieve a much better synchronization performance.

4.2 Harmonic sinusoidal attack signal on system state

The attack signal generated by the harmonic sinusoidal oscillator is injected into state signal of follower 4, i.e., $\chi_4^a = \sin(0.1t)$ and let $\vartheta_4 = 16.4$. Accordingly, the output of each agent is shown as (a) under the standard SF control protocol $u_{s,i}$ and (b) under the resilient control protocol u_i in Figure 5. It is shown that the attacked agent cannot keep output synchronization with the leader under the standard

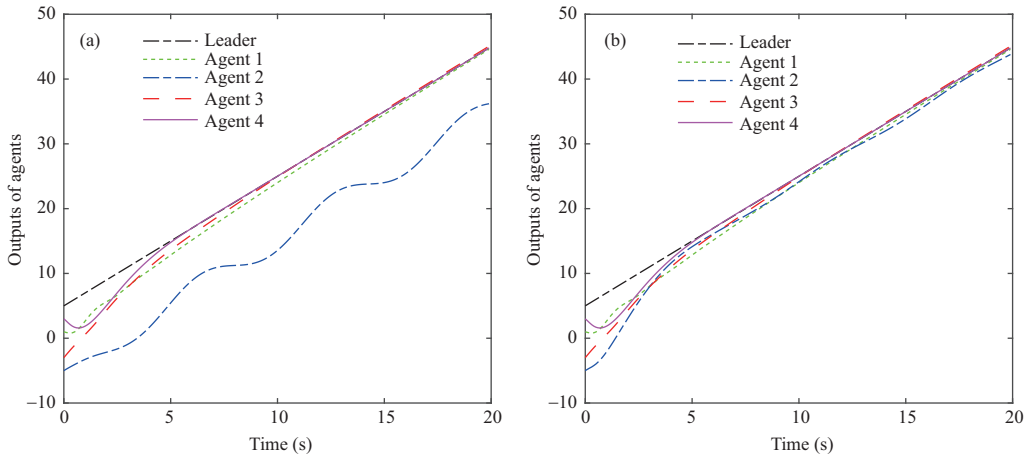

Figure 6 (Color online) Agents' outputs under the compound attack signal in the sensor of agent 2 using the standard SF control protocol (a) and the improved resilient control protocol (b), respectively.

control protocol; however, by using the resilient control protocol, the output synchronization error can be reduced well.

4.3 Compound attack signal on system state

The compound attack signal is injected into state signal of follower 2, i.e., $\chi_2^a = \sin(0.1t) + 3$ and let $\vartheta_2 = 15$. It is clear from Figure 6 that the proposed resilient control protocol is effective. In [24–27], attacked agents are isolated from the entire communication network to guarantee that other secure agents can synchronize with the leader. This method has a restriction on the number of agents or neighbors under attacks. For example, if agent 1 in this example is identified as an attacked agent. Removing this agent will prevent other secure agents from synchronizing to the leader, since it is the only agent with a direct access to the leader. However, the method we proposed has no restriction on the number of attacked agents. Moreover, in [28], measurement information is detected first, the attacked measurement information will not be used and the secure measurement information will be used by the controller. This method is not applicable for this paper because the attack signal continuously exists, and if the attacked signal does not apply, the controller will never have the signal available.

4.4 Resilient static OF control strategy

In the following, the static OF control strategy is considered for output synchronization. Let $R_1 = 0.3$, $R_2 = 0.5$, $R_3 = 0.8$, and $R_4 = 0.9$. Then, the gain matrices can be obtained based on ARE (29). Consider the attack scenario as $\chi_2^a = 2\sin(0.1t)$ and $\mu_4^a = -6$ and let $\vartheta_2 = 15$ and $\vartheta_4 = 0.5$. The output trajectories of agents under the standard OF control protocol and the resilient control protocol are given as Figures 7(a) and (b), respectively. It can be seen that the controller based on the adaptive compensator can guarantee better synchronization performance for heterogeneous MASs.

5 Conclusion

The secure output synchronization of heterogeneous MASs against sensor and actuator attacks was studied in this paper. First, the desired reference models were designed based on auxiliary systems, which have been shown to synchronize output with the leader. On the basis of the difference between the reference models and the agents' systems, the adaptive compensators were developed to mitigate the adverse effect of attacks. The SF controller and static OF controller based on the adaptive compensators were proposed to reduce synchronization errors. In this paper, the signal was transmitted continually, which may lead to the emergence of network-induced phenomena and the waste of communication resources. Meanwhile, the attacks were assumed to be differentiable and bounded, and the static OF controller was used when only output information was available. Future research may include secure synchronization control under event-triggered transmission mechanisms, secure output synchronization control under

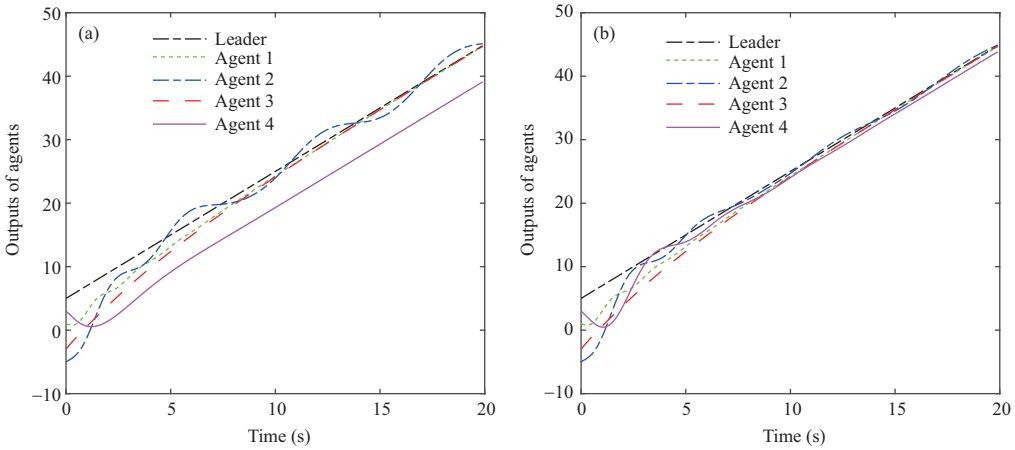

Figure 7 (Color online) Agents' outputs under the FDI attacks in the sensor of agent 2 and the actuator of agent 4 using the standard OF control protocol (a) and the improved resilient control protocol (b), respectively.

more general attacks, and dynamic OF controllers.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61973082), Six Talent Peaks Project in Jiangsu Province (Grant No. XYDXX-005).

References

1 Bidram A, Lewis F L, Davoudi A. Distributed control systems for small-scale power networks: using multiagent cooperative control theory. IEEE Control Syst Mag, 2014, 34: 56–77
2 Fang H, Shang C S, Chen J. An optimization-based shared control framework with applications in multi-robot systems. Sci China Inf Sci, 2018, 61: 014201
3 Qin J H, Gao H J, Zheng W X. Exponential synchronization of complex networks of linear systems and nonlinear oscillators: a unified analysis. IEEE Trans Neural Netw Learn Syst, 2015, 26: 510–521
4 Ding D R, Wang Z D, Han Q L. A set-membership approach to event-triggered filtering for general nonlinear systems over sensor networks. IEEE Trans Autom Control, 2020, 65: 1792–1799
5 Zhang Y, Tian Y P. A fully distributed weight design approach to consensus Kalman filtering for sensor networks. Automatica, 2019, 104: 34–40
6 Zhang Y, Sun L C, Hu G Q. Distributed consensus-based multitarget filtering and its application in formation-containment control. IEEE Trans Control Netw Syst, 2020, 7: 503–515
7 Chen W, Ding D R, Ge X H, et al. $\mathcal{H}_\infty$ containment control of multiagent systems under event-triggered communication scheduling: the finite-horizon case. IEEE Trans Cybern, 2020, 50: 1372–1382
8 Li Z K, Duan Z S, Chen G R, et al. Consensus of multiagent systems and synchronization of complex networks: a unified viewpoint. IEEE Trans Circ Syst I, 2010, 57: 213–224
9 Wang Y J, Song Y D, Lewis F L. Robust adaptive fault-tolerant control of multiagent systems with uncertain nonidentical dynamics and undetectable actuation failures. IEEE Trans Ind Elec, 2015, 62: 3978–3988
10 Qin J H, Fu W M, Zheng W X, et al. On the bipartite consensus for generic linear multiagent systems with input saturation. IEEE Trans Cybern, 2017, 47: 1948–1958
11 Yi X L, Liu K, Dimarogonas D V, et al. Dynamic event-triggered and self-triggered control for multi-agent systems. IEEE Trans Autom Control, 2018, 64: 3300–3307
12 Xu W Y, Ho D W C, Zhong J, et al. Event/self-triggered control for leader-following consensus over unreliable network with DoS attacks. IEEE Trans Neural Netw Learn Syst, 2019, 30: 3137–3149
13 Yu W W, Wang H, Hong H F, et al. Distributed cooperative anti-disturbance control of multi-agent systems: an overview. Sci China Inf Sci, 2017, 60: 110202
14 Lui D G, Petrillo A, Santini S. An optimal distributed PID-like control for the output containment and leader-following of heterogeneous high-order multi-agent systems. Inf Sci, 2020, 339: 166–184
15 Yaghmaie F A, Lewis F L, Su R. Output regulation of linear heterogeneous multi-agent systems via output and state feedback. Automatica, 2016, 67: 157–164
16 Zhang J C, Zhu F L. Observer-based output consensus of a class of heterogeneous multi-agent systems with unmatched disturbances. Commun Nonlinear Sci Numer Simul, 2018, 56: 240–251
17 Almeida J, Silvestre C, Pascoal A. Event-triggered output synchronization of heterogeneous multi-agent systems. Int J Robust Nonlinear Control, 2017, 27: 1302–1338
18 Du H B, Wen G H, Wu D, et al. Distributed fixed-time consensus for nonlinear heterogeneous multi-agent systems. Automatica, 2020, 113: 108797
19 Feng Y Z, Zheng W X. Adaptive tracking control for nonlinear heterogeneous multi-agent systems with unknown dynamics. J Franklin Inst, 2019, 356: 2780–2797
20 Shi S, Feng H Y, Liu W H, et al. Finite-time consensus of high-order heterogeneous multi-agent systems with mismatched disturbances and nonlinear dynamics. Nonlinear Dyn, 2019, 96: 1317–1333
21 Tan S, Guerrero J M, Xie P L, et al. Brief survey on attack detection methods for cyber-physical systems. IEEE Syst J, 2020, 14: 5329–5339
22 Zhou Y Q, Vamvoudakis K G, Haddad W M, et al. A secure control learning framework for cyber-physical systems under sensor and actuator attacks. IEEE Trans Cybern, 2021, 51: 4648–4660

23 Gao Y B, Sun G H, Liu J X, et al. State estimation and self-triggered control of CPSs against joint sensor and actuator attacks. Automatica, 2020, 113: 108687
24 Zeng W T, Chow M Y. Resilient distributed control in the presence of misbehaving agents in networked control systems. IEEE Trans Autom Control, 2014, 44: 2038–2049
25 Teixeira A, Shames I, Sandberg H, et al. Distributed fault detection and isolation resilient to network model uncertainties. IEEE Trans Cybern, 2014, 44: 2024–2037
26 Pasqualetti F, Bicchi A, Bullo F. Consensus computation in unreliable networks: a system theoretic approach. IEEE Trans Autom Control, 2011, 57: 90–104
27 Sundaram S, Hadjicostis C N. Distributed function calculation via linear iterative strategies in the presence of malicious agents. IEEE Trans Autom Control, 2010, 56: 1495–1508
28 Zuo Z Q, Cao X, Wang Y J. Security control of multi-agent systems under false data injection attacks. Neurocomputing, 2020, 404: 240–246
29 Ding D R, Wang Z D, Ho D W, et al. Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks. IEEE Trans Cybern, 2016, 47: 1936–1947
30 He W L, Gao X Y, Zhong W M, et al. Secure impulsive synchronization control of multi-agent systems under deception attacks. Inf Sci, 2018, 459: 354–368
31 Cui Y, Liu Y R, Zhang W B, et al. Sampled-based consensus for nonlinear multiagent systems with deception attacks: the decoupled method. IEEE Trans Syst Man Cybern Syst, 2021, 51: 561–573
32 Li X M, Zhou Q, Li P S, et al. Event-triggered consensus control for multi-agent systems against false data-injection attacks. IEEE Trans Cybern, 2019, 50: 1856–1866
33 Torre G D L, Yucelen T. Adaptive architectures for resilient control of networked multiagent systems in the presence of misbehaving agents. Int J Control, 2018, 91: 495–507
34 Modares H, Kiumarsi B, Lewis F L, et al. Resilient and robust synchronization of multiagent systems under attacks on sensors and actuators. IEEE Trans Cybern, 2019, 50: 1240–1250
35 Mustafa A, Modares H. Attack analysis and resilient control design for discrete-time distributed multi-agent systems. IEEE Robot Autom Lett, 2019, 5: 369–376
36 Chen C, Lewis F L, Xie S L, et al. Resilient adaptive and H_∞ controls of multi-agent systems under sensor and actuator faults. Automatica, 2019, 102: 19–26
37 Ma Q, Miao G Y. Output consensus for heterogeneous multi-agent systems with linear dynamics. Appl Math Comput, 2015, 271: 548–555
38 Zhang H W, Lewis F L, Das A. Optimal design for synchronization of cooperative systems: state feedback, observer and output feedback. IEEE Trans Autom Control, 2011, 56: 1948–1952
39 Gadewadikar J, Lewis F L, Abu-Khalaf M. Necessary and sufficient conditions for H_∞ static output-feedback control. J Guidance Control Dyn, 2006, 29: 915–920
40 Wieland P, Sepulchre R, Allgöwer F. An internal model principle is necessary and sufficient for linear output synchronization. Automatica, 2011, 47: 1068–1074