International Journal of Mathematics Trends and Technology
ISSN: 2231 – 5373 /doi:10.14445/22315373/IJMTT-V67I2P511
Volume 67 Issue 2, 74-82, Februray, 2021
© 2021 Seventh Sense Research Group®

Security Control of Multi-agent Systems Under Cooperative Attacks With Flexible Switching Mechanism

Xuemei Zhang

College of Information Science and Technology, Jinan University, Guangzhou 510632, China

Abstract *- This paper investigates the security control problem of nonlinear leader-following multi-agent systems based on distributed adaptive state observers in the purpose of finding some sensors that are attacked by anattacker. At first, a flexible switching mechanism is proposed in designing the observers such that the security problem is effectively solved with the consideration of sensor attacks, process disturbances and output disturbances in the systems' dynamics. Then, the tracking error control strategy is constructed based on the agents' dynamics and state estimation. Moreover, both the state estimation and the attack tolerance control performance can be guaranteed regardless of multiple attacks and other external disturbances. What's more, the unknown feedback matrix of the distributed control protocol and the unknown gain matrix of the proposed observer are determined by solving only two linear matrix inequalities (LMIs). Finally, a simulation example is given to illustrate the effectiveness of the theoretical analysis.*

Keywords — *multi-agent systems (MASs), security control, sensor attacks, distributed controller, switching mechanism*

I. INTRODUCTION

The multi-agent systems (MASs), which consist of autonomous dynamical systems and each dynamical system represents an agent communicating and interacting with other agents, are interpreted in application of modern control theory. Many researches concentrating on the application of MASs such as unmanned aerial vehicle formation cooperation, satellite formation flying, sensor network, have been published in [1–4]. However, if the sensors of agents are attacked by an attacker, the measured data may be inaccurate or incorrect. The attack signals can even disrupt the control performance of the system through the communication topology. Thus, the security control problem of MASs becomes the focus in the future.

In recent years, a lot of researches subject to security issues of MASs under sensor attacks are published (e.g., [5–8]). In most existing works, many effective approaches have been proposed to decrease the effect of sensors attacks. In [9], two novel distributed control protocols are proposed based on the adaptive control strategy and the event-triggered transmission scheme. A kind of distributed H_∞ controllers is introduced to attenuate the effects of disturbances or attacks in [10]. Authors in [11] construct an individual high-gain observer in order to observe the portion of the system state. Although all the methods mentioned above can effectively reach good control performance, it is hard to observe all the agent state in reality when sensor

attacks occur. In addition, uncertain external disturbances are inevitable in the process of information interaction, which usually cause poor performance, instability of the systems. Therefore, appropriate distributed controller can better deal with the safety control problem of the systems. Refs [12] introduces a novel hybrid distributed control scheme to reduce the impact of denial-of-service attacks and state estimation for observing the followers' position, which is one of our motivations for designing the controllers in this paper.

To solve the security control problem of MASs , suitable adaptive state observers need to be established to effectively recover the agents state by utilizing the observability Gramian and the Luenberger observer. In [13], a novel intermediate observer design method is proposed to estimate the system states, actuator faults, and sensor faults. literature [14] studies the distributed resilient observer-based fault-tolerant control problem for heterogeneous linear multiagent systems under actuator faults and denial-of-service (DoS) attacks. It is worth mentioning that there are some limitations in the exiting output feedback security control protocol. On one hand, the attacks signals are distinguished by the performance index in verifying the proposed security control approach, but it is difficult to achieve good control performance when the cooperative attacks occur and the attack signals becomes larger [5, 15, 16]. On the other hand, observer based control method are used to estimate the attack signals and the measured data are probably inaccurate, then the security control performance can not be guaranteed [17]. Therefore, in order to effectively search all the attacked sensors, a novel flexible switching mechanism is proposed for a single linear system such that the secure control method is truly verified in [18]. Unlike the principles of traditional observer, this switching mechanism is established and every agent used the same one in designing observer. Therefore, the attack tolerant control performance can be better verified by a switching function matrix. In this paper, this flexible switching mechanism is further improved and the consensus of nonlinear MASs can be achieved by a better protocol.

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

Motivated by the above discussions, this article develops an adaptive state observer for nonlinear leader following MASs under sensor attacks and external disturbances, in which the systems works both in normal condition and attacked conditions. A switching function matrix is proposed in the state observer for searching all the attacked sensors and the agent state is reconstructed such that the tracking error is close to zero. Based on Lyapunov stability analysis, the stability of the system is realized if attacks occur [19]. The main contributions of this paper are concluded as threefold. Firstly, the security control problem of nonlinear leader-following MASs is investigated under cooperative attacks and external disturbances, which are practical in practice. Secondly, a flexible switching mechanism is proposed to search all the attacked sensors of agents, in which the state can be recovered by an observer with a changed function matrix. Due to this effective scheme, the security control performance can be better verified. Finally, the unknown parameters matrix of the proposed methods is determined by solving two linear matrix inequalities (LMIs).

The rest of this papers are summarized as follows. The problem statement is detailed with some given preliminaries in section II. Several sufficient conditions can be obtained for the consensus of nonlinear leader-following MASs in section III. From section IV, a numerical application illustrates the practicability of the proposed systems. Section V is the conclusion of this article.

Notations: Denote $\mathbb{R}^n$, $\mathbb{R}^{n\times n}$ as the set of n-dimensional vectors, space of $n\times n$ matrices, respectively; $P=P^{\mathrm{T}}\in\mathbb{R}^n$ and $P>0$ means that the matrix P are symmetric and positive definite. T, -1 and I_n are the transpose of the vector (or matrix), the inverse of a matrix and n-dimensional identity matrix; any vector $M\in\mathbb{R}^n$ is a norm which can be defined as $\|M\|^2=M^{\mathrm{T}}M$. $*$ represents the symmetric elements of the symmetric matrix; C_a^b denotes the binomial coefficient with $a,b,\in\mathbb{R}^+$. The support of a vector $s\in\mathbb{R}^n$ is defined as $\mathrm{supp}(s)$. A vector $b\in\mathbb{R}^n$ is s-sparse if $|\mathrm{supp}(b)|=s$ with $s\le n$. The Kronecker product $\otimes$ has the following propertion $(A\otimes B)(C\otimes D)=(AC\otimes BD)$, $(A\otimes B)^{\mathrm{T}}=(A^{\mathrm{T}}\otimes B^{\mathrm{T}})$. The other matrices or vectors without explicitly stated are assumed to have appropriate dimensions.

II. PRELIMINARIES AND PROBLEM DESCRIPTION

A. Graph theory

The MASs is considered as a directed graph with *N* agents. The communication topology is denoted as $\bar{G}(\mathrm{V},\mathrm{E},\mathrm{A})$, where $V=\{V_1,V_2,\ldots,V_N\}$ is the set of all nodes, $\mathrm{E}\in\mathrm{V}\times\mathrm{V}$ represents the set of all edges. The weighted adjacent matrix is $A=[a_{ij}]_{N\times N}$ with $a_{ij}>0$ if there is a directed edge from agent V_i to agent V_j and V_i can get information from V_j; otherwise, $a_{ij}=0$. The Laplacian matrix can be defined as $L=[l_{ij}]_{N\times N}$, $l_{ij}=-a_{ij}(i\neq j)$ and $l_{ii}=\sum_{j=1}^{N}a_{ij},i=1,2,\ldots,N$. The pinning matrix can be denoted as $Q=\{q_i\}\in\mathbb{R}^{N\times N}$, if the *i*th node is connected to the leader, $q_i=1$, otherwise $q_i=0$.

B. Problem description

Consider the following MASs under sensor attacks, the system model of leader node is described as:

$$\begin{cases}\dot{x}_0(t)=Ax_0(t)+B_2f(x_0(t)),\\ y_0(t)=Cx_0(t).\end{cases}\tag{1}$$

Assume that from 1 to *N* of agents are followers. The dynamics of *i*th follower are given as

$$\begin{cases}\dot{x}_i(t)=Ax_i(t)+B_1u_i(t)+B_2f(x_i(t))+D_ww_i(t),\\ y_i(t)=Cx_i(t)+E(d_i(t)+v_i(t)),\end{cases}\tag{2}$$

where $x_i(t)\in\mathbb{R}^n$, $u_i(t)\in\mathbb{R}^n$, $\mathrm{y}_i(t)\in\mathbb{R}^n$ represent the state vector, control input and measurement output, respectively. $w_i(t)\in\mathbb{R}^n$, $d_i(t)\in\mathbb{R}^n$, $v_i(t)\in\mathbb{R}^n$ are the process disturbances, measurement disturbances, the sensor attacks injected by attackers, respectively. the nonlinear function $f(\cdot)\in\mathbb{R}^n$ satisfies the global Lipschitz condition $\|f(x)-f(y)\|\le l\|x-y\|$ with constant $l>0$. A,B_1,B_2,C,E are known constant matrices with appropriate

dimensions.

Remark 1. As a non-negligible factor, it is of great practical significance to consider disturbances in the dynamics of MASs. The process disturbances, output disturbances and sensor attacks are considered in (2) like other articles [13,18,20]. Compared with many works [9,21], systems (2) are more general in practical application.

Assumption 1. The sensor attacks $v_i(t) \in \mathbb{R}^n$ is a *s*-sparse vector and $v(t) = (v_1^{\mathrm{T}}(t), v_2^{\mathrm{T}}(t), \ldots, v_N^{\mathrm{T}}(t))^{\mathrm{T}}$; $\mathrm{supp}(v(t))$ satisfies $\|v(t)\| \le \sigma_v$, where $\sigma_v > 0$ is known constant. Given constants $\sigma_w > 0$ and $\sigma_d > 0$, the other disturbances $w(t) = (w_1^{\mathrm{T}}(t), w_2^{\mathrm{T}}(t), \ldots, w_N^{\mathrm{T}}(t))^{\mathrm{T}}$ and $d(t) = (d_1^{\mathrm{T}}(t), d_2^{\mathrm{T}}(t), \ldots, d_N^{\mathrm{T}}(t))^{\mathrm{T}}$ satisfy $\|w(t)\| \le \sigma_w$ and $\|d(t)\| \le \sigma_d$.

The most important objective is to design a reasonable control protocol based on the flexible switching mechanism. The system state is estimated by the state observer, and the system's attack tolerance control performance can be guaranteed.

III. MAIN RESULTS

A. Construct the adaptive state observer

In this section, the unmeasurable state can be estimated by an adaptive state observer. Based on the analysis of [5,18], a flexible switching mechanism was proposed to solve the problem of difficult identification of attack signals. The switching function matrix is used to detect the sensor that is attacked and switch autonomously due to the change of switching element.

Definition 1 (See the work of [5]).

System (2) is *s*-sparse observable if for every set $S \subset 1, 2, \ldots, n$ with $|S| = s$, the pair (A, C_S) is observable. $|S|$ is the cardinality of S.

$v_i(t)$ is nonzero element if the *i*th sensor is attacked; otherwise $v_i(t)$ is zero. Constructing the flexible switching matrix $L_\xi = \mathrm{diag}\{l_1, \ldots, l_i, \ldots, l_n\}$. $l_i = 0$ means the *i*th sensor is not attacked, otherwise $l_i = 1$. The attack mode $\xi = C_n^0 + C_n^1 + \ldots + C_n^s$ and will defined later. Then the distributed state observer is defined as

$$\dot{\hat{x}}_i(t) = A\hat{x}_i(t) + B_1 u_i(t) + B_2 f(\hat{x}_i(t)) + \hat{\rho}\hat{K}L_\xi \delta_i, \tag{3}$$

where

$$\delta_i = \sum_{j=1}^{N} a_{ij}(y_i(t) - y_j(t)) + q_i(y_i(t) - y_0(t)), \quad \hat{\delta}_i = \sum_{j=1}^{N} a_{ij}(C\hat{x}_i(t) - C\hat{x}_j(t)) + q_i(C\hat{x}_i(t) - C\hat{x}_0(t)).$$

$\hat{\rho}$, $\hat{K}$ are the observer coupling strength and the observer gain matrix. It is assumed that the reference signal from the leader is (called "pinned") available to the controlled followers[22]. Define $x_0(t) = \hat{x}_0(t)$ and $\delta_{L\xi_i} = L_\xi(\delta_i - \hat{\delta}_i)$, The energy function $\delta(t) = N^{-\frac{1}{2}}(\sum_{i=1}^{N} \|\delta_{L\xi_i}\|^2)^{\frac{1}{2}}$, the observed performance index ψ is denoted as

$$\Delta\psi(t) = \mu N_\theta^2(\delta(t)) = \begin{cases} 0, & \delta(t) < \theta, \\ \mu(\delta(t) - \theta)^2, & \delta(t) \ge \theta, \end{cases} \tag{4}$$

where Δ represents the time derivative; μ and θ are constants to be determined later. Denote the switching index

$$\xi(\psi) = \left\lceil \mathrm{mod}(\psi, C_n^0 + C_n^1 + \ldots + C_n^s) \right\rceil, \tag{5}$$

where $\lceil \cdot \rceil$ is the ceiling function, mod(·) is the residual operator or known as the modulus.

Remark 2. The switching scheme are proposed in [18]. Different from the previous works, the switching index ξ switches between 1 and $C_n^0 + C_n^0 + \ldots + C_n^s$ and finally ξ will switch to the right mode [5] . $\xi = 1$ and $L_1 = I_n$ is the initial condition, at which system (2) is not attacked.

The cooperative attacks tolerant control input is proposed due to the analysis above.

$$u_i(t) = -\rho K\left(\sum_{j=1}^{N} a_{ij}(\hat{x}_i(t) - \hat{x}_j(t)) + q_i(\hat{x}_i(t) - \hat{x}_0(t))\right), \tag{6}$$

where ρ, K are the coupling strength and the undetermined control feedback matrix.

B. Stability analysis of global tracking error systems

Define the tracking error $e_i(t) = x_i(t) - x_0(t)$ and the estimation error $\hat{e}_i(t) = x_i(t) - \hat{x}_i(t),$ we have

$$\begin{cases} \dot{e}(t) = (I_N \otimes A)e(t) - (H \otimes \rho B_1 K)e(t) + (H \otimes \rho B_1 K)\hat{e}(t) + (I_N \otimes B_2)F(t) + (I_N \otimes D_w)w(t), \\ \dot{\hat{e}}(t) = (I_N \otimes A)\hat{e}(t) - (H \otimes \hat{\rho}\hat{K}L_\xi C)\hat{e}(t) + (I_N \otimes B_2)\hat{F}(t) + (I_N \otimes D_w)w(t) \\ \qquad -(H \otimes \hat{\rho}\hat{K}L_\xi E)d(t) - (H \otimes \hat{\rho}\hat{K}L_\xi E)v(t), \end{cases} \tag{7}$$

where $H = \mathrm{L} + \mathrm{Q}$, $e(t) = (e_1^{\mathrm{T}}(t), e_2^{\mathrm{T}}(t), \ldots, e_N^{\mathrm{T}}(t))^{\mathrm{T}}$, $\hat{e}(t) = (\hat{e}_1^{\mathrm{T}}(t), \hat{e}_2^{\mathrm{T}}(t), \ldots, \hat{e}_N^{\mathrm{T}}(t))^{\mathrm{T}}$ and

$$F(t) = ((f(x_1) - f(x_0))^{\mathrm{T}}, (f(x_2) - f(x_0))^{\mathrm{T}}, \ldots, (f(x_N) - f(x_0))^{\mathrm{T}})^{\mathrm{T}},$$

$$\hat{F}(t) = ((f(x_1) - f(\hat{x}_1))^{\mathrm{T}}, (f(x_2) - f(\hat{x}_2))^{\mathrm{T}}, \ldots, (f(x_N) - f(\hat{x}_N))^{\mathrm{T}}).$$

Before showing the results, the following lemmas are introduced.

Lemma 1 (See the work of Lin et al [21]).

There exits a positive vector $\chi = [\chi_1, \chi_2, \ldots, \chi_N]^{\mathrm{T}}$ and the diagonal matrix $\Xi = \mathrm{diag}\{\chi_1, \chi_2, \ldots, \chi_N\}$ such that

$$\Xi H + H^{\mathrm{T}}\Xi > 0,$$

where $H^{\mathrm{T}}\chi = 1_N$ and H is defined in (7).

Lemma 2 (See the work of Cao et al [23]).

For any $\kappa > 0,$ $x \in \mathbb{R}^n$, $y \in \mathbb{R}^n$ and matrix $M \in \mathbb{R}^{n\times n}$, the following inequality holds

$$2x^{\mathrm{T}}y \le \kappa x^{\mathrm{T}}M^{-1}x + \kappa^{-1}y^{\mathrm{T}}My.$$

Lemma 3 (See the work of Hou et al [25]).

For continuous functions $V(t) > 0$, any positive constants α, β, the following inequalities holds

$$\dot{V}(t) \le -\alpha V(t) + \beta,$$

Then

$$V(t) \le e^{-\alpha t}V(t) + \alpha^{-1}\beta(1 - e^{-\alpha t}).$$

Theorem 1. Suppose that Assumptions 1 holds, the tracking error systems (7) are uniformly ultimately bounded if for given positive scalars $\varepsilon,$ $\tilde{\varepsilon},$ $\gamma,$ $\tilde{\gamma},$ there exits positive symmetric matrices $P,$ Q such that

$$\begin{pmatrix} \Omega & lP \\ * & -I \end{pmatrix} < 0, \tag{8}$$

$$\begin{pmatrix} \hat{\Omega} & QB_2 & QD_w \\ * & -I & 0 \\ * & * & -\chi_{\min}\chi_{\max}^{-2}I \end{pmatrix} < 0, \tag{9}$$

where $\Omega = AP + PA^{\mathrm{T}} + B_2B_2^{\mathrm{T}} + \chi_{\max}^2\chi_{\min}^{-1}D_wD_w^{\mathrm{T}} - \lambda_1\rho\chi_{\max}^{-1}B_1B_1^T + (\varepsilon + \tilde{\varepsilon})P,$

$\hat{\Omega} = \mathrm{Q}A + A^{\mathrm{T}}Q + l^2I_n - \lambda_1\hat{\rho}\chi_{\max}^{-1}C^{\mathrm{T}}L_\xi C^{\mathrm{T}} + 2\lambda_{\max}(\Xi HH^{\mathrm{T}}\Xi)\hat{\rho}\chi_{\min}^{-1}C^{\mathrm{T}}L_\xi EE^{\mathrm{T}}L_\xi^{\mathrm{T}}C + (\gamma + \tilde{\gamma})Q.$

Proof. We construct the Lyapunov functions as

$$V(t) = e^{\mathrm{T}}(t)(\Xi \otimes P^{-1})e(t) + \varsigma\hat{e}^{\mathrm{T}}(t)(\Xi \otimes Q)\hat{e}(t), \tag{10}$$

Where constant $\varepsilon > 0$ to be determined later. Calculating the derivative of $V(t)$ yields

$$\begin{aligned}\dot{V}(t) &= 2e^{\mathrm{T}}(t)(\Xi \otimes P^{-1})\dot{e}(t) + 2\hat{e}^{\mathrm{T}}(t)(\Xi \otimes Q)\dot{\hat{e}}(t)\\ &= e^{\mathrm{T}}(t)(\Xi \otimes (P^{-1}A + A^{\mathrm{T}}P^{-1}))e(t) - \rho e^{\mathrm{T}}(t)((\Xi H + H^{\mathrm{T}}\Xi) \otimes P^{-1}B_1K)e(t)\\ &\quad + 2\rho e^{\mathrm{T}}(t)(\Xi H \otimes P^{-1}B_1K)\hat{e}(t) + 2e^{\mathrm{T}}(t)(\Xi \otimes P^{-1}B_2)F(t) + 2e^{\mathrm{T}}(t)(\Xi H \otimes P^{-1}D_w)w(t)\\ &\quad + \varsigma\hat{e}^{\mathrm{T}}(t)(\Xi \otimes (QA + A^{\mathrm{T}}Q))\hat{e}(t) - \varsigma\hat{\rho}\hat{e}^{\mathrm{T}}(t)((\Xi H + H^{\mathrm{T}}\Xi) \otimes Q\hat{K}L_{\xi}C)\hat{e}(t) + 2\varsigma\hat{e}^{\mathrm{T}}(t)(\Xi \otimes QB_2)\hat{F}(t)\\ &\quad + 2\varsigma\hat{e}^{\mathrm{T}}(t)\left(\Xi \otimes QD_w\right)w(t) - 2\varsigma\hat{e}^{\mathrm{T}}(t)(\Xi H \otimes \hat{\rho}Q\hat{K}L_{\xi}E)d(t) - 2\varsigma\hat{e}^{\mathrm{T}}(t)(\Xi H \otimes \hat{\rho}Q\hat{K}L_{\xi}E)v(t).\end{aligned}$$

(11)

Let $K = B_1^{\mathrm{T}}P^{-1}$, $\hat{K} = Q^{-1}C^{\mathrm{T}}$, $\lambda_1 = \lambda_{\min}(\Xi H + H^{\mathrm{T}}\Xi) > 0$, $\chi_{\max} = \max\{\chi_1, \ldots, \chi_N\}$, $\chi_{\min} = \min\{\chi_1, \ldots, \chi_N\}$.

Based on Assumption 1 and Lemmas 1, 2, the following inequalities hold

$$2e^{\mathrm{T}}(t)(\Xi \otimes P^{-1}B_2)F(t) \le e^{\mathrm{T}}(t)(\Xi \otimes (P^{-1}B_2 + l^2 I_n))e(t). \tag{12}$$

$$2e^{\mathrm{T}}(t)(\Xi \otimes P^{-1}D_w)w(t) \le e^{\mathrm{T}}(t)(\Xi \otimes \chi_{\max}^2\chi_{\min}^{-1}P^{-1}D_wD_w^{\mathrm{T}}P^{-1})e(t) + \sigma_w^2. \tag{13}$$

$$-\rho e^{\mathrm{T}}(t)\left(t\right)((\Xi H + H^{\mathrm{T}}\Xi) \otimes P^{-1}B_1K)e(t) \le -e^{\mathrm{T}}(t)(\Xi \otimes \lambda_1\rho\chi_{\max}^{-1}P^{-1}B_1B_1^{\mathrm{T}}P^{-1})e(t). \tag{14}$$

$$2\varsigma\hat{e}^{\mathrm{T}}(t)(\Xi \otimes QB_2)\hat{F}(t) \le \varsigma\hat{e}^{\mathrm{T}}(t)(\Xi \otimes (QB_2B_2^{\mathrm{T}}Q + l^2 I_n))\hat{e}(t). \tag{15}$$

$$2\varsigma\hat{e}^{\mathrm{T}}(t)(\Xi \otimes QD_w)w(t) \le \varsigma\hat{e}^{\mathrm{T}}(t)(\Xi \otimes (\chi_{\max}^2\chi_{\min}^{-1}QD_wD_w^{\mathrm{T}}Q))\hat{e}(t) + \sigma_w^2. \tag{16}$$

$$-\varsigma\hat{e}^{\mathrm{T}}(t)((\Xi H + H^{\mathrm{T}}\Xi) \otimes \hat{\rho}Q\hat{K}L_{\xi}C)\hat{e}(t) \le -\varsigma\hat{e}^{\mathrm{T}}(t)(\Xi \otimes \lambda_1\beta_{\max}^{-1}\hat{\rho}C^{\mathrm{T}}L_{\xi}C)\hat{e}(t). \tag{17}$$

$$-\varsigma 2\hat{e}^{\mathrm{T}}(t)(\Xi H \otimes \hat{\rho}Q\hat{K}L_{\xi}E)d(t) \le \varsigma\hat{e}^{\mathrm{T}}(t)(\Xi \otimes \lambda_{\max}(\Xi HH^{\mathrm{T}}\Xi)\hat{\rho}\chi_{\min}^{-1}C^{\mathrm{T}}L_{\xi}EE^{\mathrm{T}}L_{\xi}^{\mathrm{T}}C)\hat{e}(t) + \sigma_d^2. \tag{18}$$

$$-2\varsigma\hat{e}^{\mathrm{T}}(t)(\Xi H \otimes \hat{\rho}Q\hat{K}L_{\xi}E)v(t) \le \varsigma\hat{e}^{\mathrm{T}}(t)(\Xi \otimes \lambda_{\max}(\Xi HH^{\mathrm{T}}\Xi)\chi_{\min}^{-1}\hat{\rho}C^{\mathrm{T}}L_{\xi}EE^{\mathrm{T}}L_{\xi}^{\mathrm{T}}C)\hat{e}(t) + \sigma_v^2. \tag{19}$$

According to the inequalities (11)-(19), we have

$$\dot{V}(t) \le e^{\mathrm{T}}(t)(\Xi \otimes \Pi_1)e(t) + \varsigma\hat{e}^{\mathrm{T}}(t)(\Xi \otimes \Pi_2)\hat{e}(t) + 2e^{\mathrm{T}}(t)(\Xi H \otimes \rho P^{-1}B_1B_1^{\mathrm{T}}P^{-1})\hat{e}(t) + \tau, \tag{20}$$

where $\tau = 2\sigma_w^2 + \sigma_d^2 + \sigma_v^2$,

$$\Pi_1 = P^{-1}A + A^{\mathrm{T}}P^{-1} + P^{-1}B_2B_2^{\mathrm{T}}P^{-1} + l^2 I_n + \chi_{\max}^2\chi_{\min}^{-1}P^{-1}D_wD_w^{\mathrm{T}}P^{-1} - \lambda_1\rho\chi_{\max}^{-1}P^{-1}B_1B_1^{\mathrm{T}}P^{-1},$$

$$\Pi_2 = QA + A^{\mathrm{T}}Q + QB_2B_2^{\mathrm{T}}Q + l^2 I_n + \chi_{\max}^2\chi_{\min}^{-1}QD_wD_w^{\mathrm{T}}Q - \lambda_1\hat{\rho}\chi_{\max}^{-1}C^{\mathrm{T}}L_{\xi}C + 2\lambda_{\max}(\Xi HH^{\mathrm{T}}\Xi)\hat{\rho}\chi_{\min}^{-1}C^{\mathrm{T}}L_{\xi}EE^{\mathrm{T}}L_{\xi}^{\mathrm{T}}C.$$

Inequalities $\Pi_1 \le -(\varepsilon + \tilde{\varepsilon})P^{-1}$ and $\Pi_2 \le -(\gamma + \tilde{\gamma})Q$ are supported by conditions (8) and (9) for the given positive constants ε, $\tilde{\varepsilon}$, γ, $\tilde{\gamma}$. Inequality (20) can be written as

$$\dot{V}(t) \le -\varepsilon e^{\mathrm{T}}(t)(\Xi \otimes P^{-1})e(t) - \varsigma\gamma\hat{e}^{\mathrm{T}}(t)(\Xi \otimes Q)\hat{e}(t) + \tau + \eta^{\mathrm{T}}(t)\Theta\eta(t), \tag{21}$$

where $\eta(t) = (e^{\mathrm{T}}(t), \hat{e}^{\mathrm{T}}(t))^{\mathrm{T}}$, $\Theta = \begin{pmatrix} -\Xi \otimes \tilde{\varepsilon}P^{-1} & \Xi H \otimes \rho P^{-1}B_1B_1^{\mathrm{T}}P^{-1} \\ * & -\Xi \otimes \varsigma\tilde{\gamma}Q \end{pmatrix}$. Obviously, $-\Xi \otimes \tilde{\varepsilon}P^{-1} < 0$ and $\Theta < 0$ are established if and only if ς satisfies

$$\Xi \otimes \tilde{\varepsilon}P^{-1} > \varsigma(\Xi H \otimes \rho P^{-1}B_1B_1^{\mathrm{T}}P^{-1})^{\mathrm{T}}(\Xi \otimes \tilde{\gamma}Q)^{-1}(\Xi H \otimes \rho P^{-1}B_1B_1^{\mathrm{T}}P^{-1}).$$

Let $\alpha = \min\{\varepsilon, \gamma\}$, $\beta = \tau$, then it is concluded from (21) that

$$\dot{V}(t) \le -\alpha V(t) + \beta. \tag{22}$$

According to **Lemma 3**, one gets

$$V(t) \le e^{-\alpha t}V(t) + \alpha^{-1}\beta(1-e^{-\alpha t}). \tag{23}$$

Thus, it is derived from inequality (23) that the states dynamics of tracking error systems (7) are uniformly bounded when $t \to \infty$, and the consensus tracking error converges to a small neighborhood of the origin, which means the consensus of the proposed MASs can be realized.

According to artice [5], it is easy to obtain that the convergence $\dot{\psi}(t)$ satisfies $\int_{t^*}^{+\infty} \dot{\psi}(t)dt \le 1$ for a certain time t^*. Obviously, it holds

$$\tilde{\lambda}\|\hat{e}(t)\|^2 \le \tilde{\lambda}(\|\hat{e}(t)\|^2 + \|e(t)\|^2) \le V(t) \le e^{-\alpha(t-t^*)}V(t^*) + \alpha^{-1}\beta(1-e^{-\alpha(t-t^*)}), \tag{24}$$

where $\tilde{\lambda}=\min\{\lambda_{\min}(\Xi \otimes P^{-1}), \lambda_{\min}(\Xi \otimes Q)\}$. Then from (24), we obtain

$$\|\hat{e}(t)\| \le \tilde{\lambda}^{-\frac{1}{2}} e^{-\frac{\alpha}{2}(t-t^*)} V^{\frac{1}{2}}(t^*) + \alpha^{-\frac{1}{2}}\tilde{\lambda}^{-\frac{1}{2}}\beta^{\frac{1}{2}}. \tag{25}$$

Let $\delta_{L\xi}(t) = (H \otimes L_\xi C)\hat{e}(t) + (H \otimes L_\xi E)d(t) + (H \otimes L_\xi E)v(t)$. The energy function $\delta(t)=N^{-\frac{1}{2}}(\sum_{i=1}^{N}\|\delta_{L\xi_i}\|^2)^{\frac{1}{2}}$ satisfies

$$\delta(t) \le N^{-\frac{1}{2}}\|H \otimes L_\xi C\|[\tilde{\lambda}^{-\frac{1}{2}} e^{-\frac{\alpha}{2}(t-t^*)} V^{\frac{1}{2}}(t^*) + \alpha^{-\frac{1}{2}}\tilde{\lambda}^{-\frac{1}{2}}\beta^{\frac{1}{2}}] + N^{-\frac{1}{2}}\|H \otimes L_\xi E\|\sigma_d + N^{-\frac{1}{2}}\|H \otimes L_\xi E\|\sigma_v. \tag{26}$$

What's more, from (4), there exits time t^* such that

$$\int_{t^*}^{+\infty} \dot{\psi}(t)dt \le \int_{t^*}^{+\infty} \mu\left(N^{-\frac{1}{2}}\|H \otimes L_\xi C\|\tilde{\lambda}^{-\frac{1}{2}} e^{-\frac{\alpha}{2}(t-t^*)} V^{\frac{1}{2}}(t^*)\right)^2 dt \le \mu N^{-1}\|H^{\mathrm{T}}H \otimes C^{\mathrm{T}}L_\xi^{\mathrm{T}}L_\xi C\|\tilde{\lambda}^{-1}\alpha^{-1}V(t^*), \tag{27}$$

where $\theta=N^{-\frac{1}{2}}\|H \otimes L_\xi C\|\alpha^{-\frac{1}{2}}\tilde{\lambda}^{-\frac{1}{2}}\beta^{\frac{1}{2}} + N^{-\frac{1}{2}}\|H \otimes L_\xi E\|\sigma_d + N^{-\frac{1}{2}}\|H \otimes L_\xi E\|\sigma_v$. It is obtained from (22) that

$$V(t^*) \le e^{-\alpha(t-t^*)}V(0) + \alpha^{-1}\beta. \tag{28}$$

Combine (27) and (28) that

$$\int_{t^*}^{+\infty} \dot{\psi}(t)dt \le \mu N^{-1}\|H^{\mathrm{T}}H \otimes C^{\mathrm{T}}L_\xi^{\mathrm{T}}L_\xi C\|\tilde{\lambda}^{-1}\alpha^{-1}(e^{-\alpha(t-t^*)}V(0) + \alpha^{-1}\beta). \tag{29}$$

Let $\mu=N\|H^{\mathrm{T}}H \otimes C^{\mathrm{T}}L_\xi^{\mathrm{T}}L_\xi C\|^{-1}\tilde{\lambda}\alpha(\varpi + \alpha^{-1}\beta)^{-1}$ for the determined parameter $\varpi > 0$. Thus, there always exits t^* satisfying $e^{-\alpha t^*} \le \varpi$ and $\int_{t^*}^{+\infty} \dot{\psi}(t)dt \le 1$. From Barbalat's lemma, it holds $\lim_{t\to\infty} N_\theta^2(\delta(t)) = 0$ and $\lim_{t\to\infty}\delta(t) < \theta$.

When the system is attacked, it can be proved that the performance index ψ drives the switching index ξ to change between 1 and $C_n^0 + C_n^1 + \ldots + C_n^s$ continuously until the index is reached to the correct mode, the performance index ψ will continue to increase in this process, and will eventually remain stable. At that time, sensor attacks $v_i(t) = 0$. The proof is complete.

Remark 3. In the paper, security control problem of MASs under multiple attacks is solved by a flexible switching mechanism. Compared with most exiting literature [11,13,24], the switching scheme proposed in this paper is more practical and flexible. Thus when systems are attacked, the switching performance index can be guaranteed such that the security control problem can be solved in a better strategy.

IV. NUMERICAL SIMULATION

In this section, a numerical example is provided to verify the theoretical results. The MASs with followers' dynamics (2) and leader dynamics (1) are denoted as a graph with one leader and three followers, which can be shown in **Fig 1**.

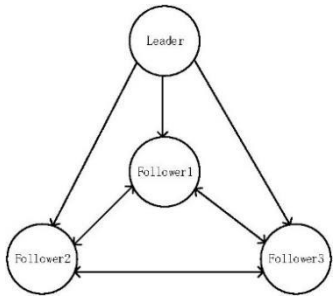


Fig 1: The graph of leader-following MASs.

Table 1: Sensor attacks.

	Follower 1	Follower 2	Follower 3
Sensor 1	0.2sin(t)	0.2sin(t)	0
Sensor 2	0	0	0

Example. The MASs topology of corresponding augmented Laplacian matrix is defined as

$$H=\begin{pmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{pmatrix}.$$

Based on Lemma 1, it is easy to obtain that $\Xi=I_3$, $\chi_{\max}=\chi_{\min}=1$ and $\lambda_1=\lambda_{\min}(\Xi H+H^{\mathrm{T}}\Xi)=2.$ The mainly problem is to choose the proper parameters such that the security tracking control method proposed in this paper can be verified. The nonlinear function is described as $f(x_i(t))=\tanh(x_i(t)),$ and Lipschitz constant can be chosen as $l=1.$

For the given parameters $\rho=\hat{\rho}=0.2,$ $\varepsilon=8.5,$ $\tilde{\varepsilon}=0.6,$ $\gamma=10.5,$ $\tilde{\gamma}=0.4$. Both the process disturbances and measurement disturbances are defined as $w_i(t)=d_i(t)=0.2\sin(t),$ $\sigma_w=\sigma_d=0.2$ satisfy **Assumption 1.** Choose the known matrices as

$$A=\begin{pmatrix} -8 & -40 \\ 30 & -9 \end{pmatrix},\ B_1=\begin{pmatrix} 2.7 & -5 \\ 4 & 3 \end{pmatrix},\ B_2=\begin{pmatrix} -2 & 0 \\ 1 & 1 \end{pmatrix},$$

$$D_w=\begin{pmatrix} 0.1 & 0 \\ 0 & 0.5 \end{pmatrix},\ C=\begin{pmatrix} 0.1 & 0.2 \\ 0.1 & 0.3 \end{pmatrix},\ E=\begin{pmatrix} 0.1 & 0 \\ -0.1 & 0 \end{pmatrix}.$$

Based on **Theorem 1.** it yields

$$P=\begin{pmatrix} 1.0697 & -0.0273 \\ -0.0273 & 0.8304 \end{pmatrix},\ Q=\begin{pmatrix} 1.1935 & 0.0365 \\ 0.0365 & 0.8472 \end{pmatrix},$$

$$K=\begin{pmatrix} 2.6495 & 4.9043 \\ -4.5858 & 3.4618 \end{pmatrix},\ \hat{K}=\begin{pmatrix} 0.0767 & 0.0730 \\ 0.2328 & 0.3510 \end{pmatrix}.$$

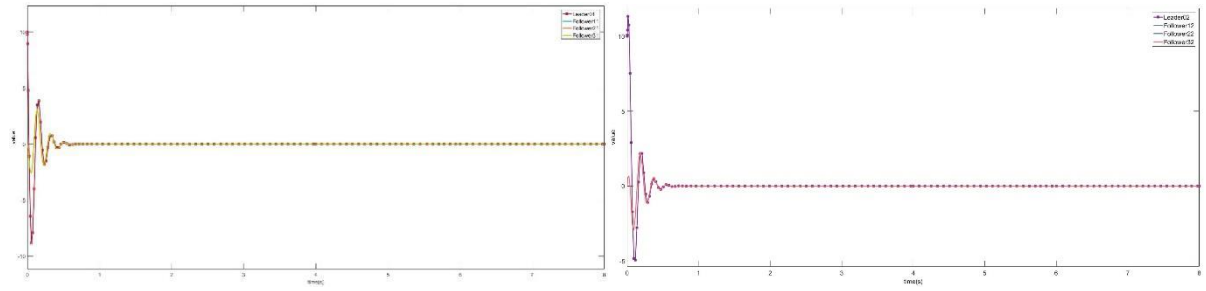


Fig 2. The state trajectories of leader-following MASs.

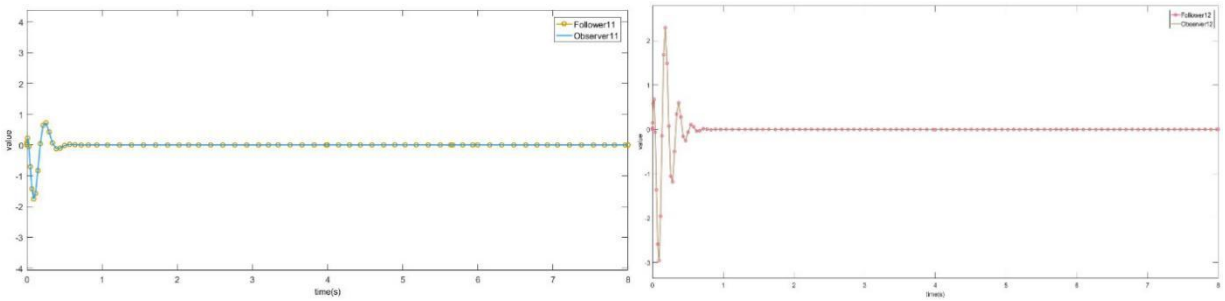


Fig 3. The state estimation of follow 1.

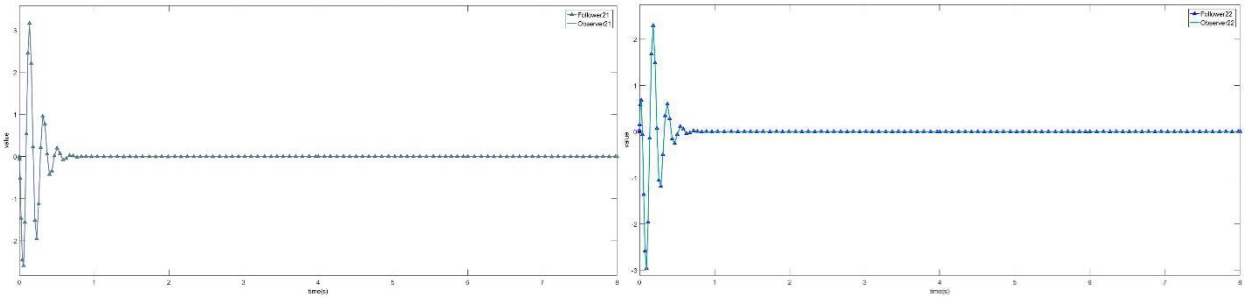


Fig 4. The state estimation of follow 2.

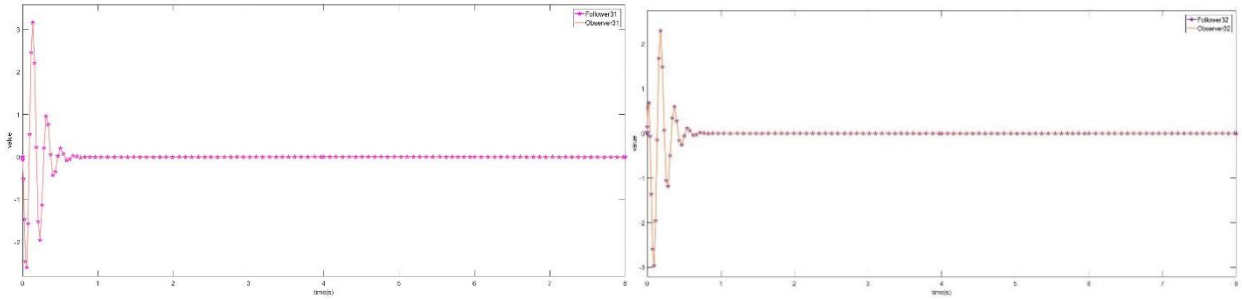
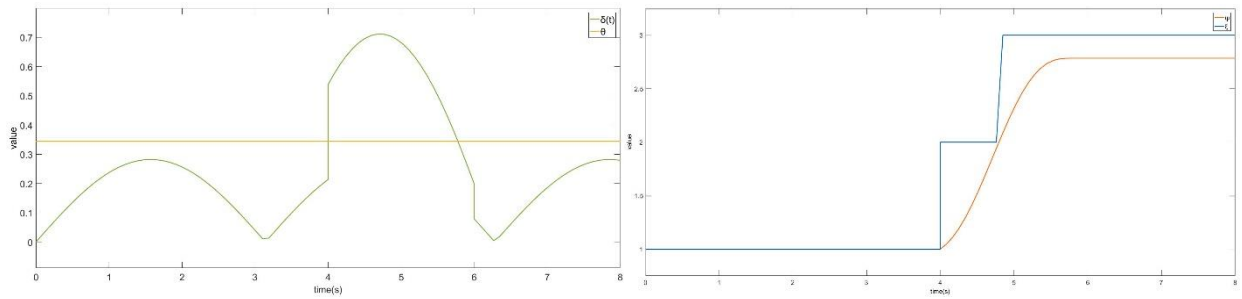


Fig 5. The state estimation of follow 3.



(a) **(b)**

Fig 6. The flexible switching mechanism.

In 4s, sensor attacks occur on sensor 1 of motor 1 and motor 2, which can be seen in **Table 1**. $\sigma_v = 0.4$ satisfies

Assumption 1. Choose the initial condition of leader as $(10,10)^{\mathrm{T}}$ and the others are zero conditions, the state trajectories are shown in **Fig 2** and their estimation are shown in **Fig 3-Fig 5.** Define the initial condition of the switching index $\xi = 1$, and the observed performance index $\psi = 1$. **Fig 6(a)** plots the energy function $\delta(t)$ and constant θ, **Fig 6(b)** shows the switching index ξ and the observed performance index ψ. Since the energy function $\delta(t)$ keeps changing in the time interval 4-6s, the flexible switching mechanism is stimulated for searching the attack mode. At about t=6s, the switching index ξ reaches to the right mode and the observed performance index ψ is stable. Then the flexible switching mechanism can be effectively verified. Therefore, we conclude that all the agents achieve agreement. That is, the security control of nonlinear leader-following MASs can be effectively verified.

VI. CONCLUSIONS

This paper studies the security control problem of MASs under sensor attacks and other external disturbances. a flexible switching mechanism is proposed to search the attack mode modeled by a suitable adaptive state observer. Also, the tracking error control strategy is constructed based on the followers dynamics and the corresponding state estimation. Both the state estimation and the attack tolerance control performance is guaranteed regardless of multiple attacks and disturbances. By lyapunov stability theory, sufficient conditions for the consensus of the considered MASs are obtained. Finally, An experimental results verify the effectiveness of the proposed scheme.

REFERENCES

[1] Z. Obdržálek, Mobile agents and their use in a group of cooperating autonomous robots. In Proceedings of the 2017 22nd International Conference on Methods and Models in Automation and Robotics (MMAR): (2017) 125-130.

[2] Y. Gao, and L. Wang, Sampled-data based consensus of continuous-time multi-agent systems with time-varying topology, IEEE Transactions on Automatic Control. 56(5) (2011)1226–1231..

[3] Y. Xu, W. Liu, and J. Gong, Stable multi-agent-based load shedding algorithm for power systems, IEEE Transactions on Power Systems. 26(4)(2011) 2006–2014.

[4] J. Lu, X. Guo, T. Huang, and Z. Wang, Consensus of signed networked multi-agent systems with nonlinear coupling and communication delays, Applied Mathematics and Computation. 350 (2019) 153–162.

[5] J.-W. Zhu, Y.-P. Yang, W.-A. Zhang, L. Yu, and X. Wang, Cooperative attack tolerant tracking control for multi-agent system with a resilient switching scheme, Neurocomputing. 409 (2020) 372–380.

[6] A. Mustafa, and H. Modares, Attack analysis and resilient control design for discrete-time distributed multi-agent systems, IEEE Robotics and Automation Letters. 5(2)(2019) 369–376.

[7] X.Jin, and W.M.Haddad, An adaptive control architecture for leader–follower multiagent systems with stochastic disturbances and sensor and actuator attacks, International Journal of Control. 92(11) (2019) 2561–2570.

[8] R. Gao, J. Huang, and L. Wang, Leaderless consensus control of uncertain multi-agents systems with sensor and actuator attacks, Information Sciences. 505 (2019) 144–156.

[9] R. Yang, H. Zhang, G. Feng, H. Yan, and Z. Wang, Robust cooperative output regulation of multi-agent systems via adaptive event-triggered control, Automatica. 102 (2019) 129–136.

[10] H. Modares, B. Kiumarsi, F. L. Lewis, F. Ferrese, and A. Davoudi, Resilient and robust synchronization of multiagent systems under attacks on sensors and actuators, IEEE transactions on cybernetics. 5(3)(2019) 1240–1250.

[11] J. Kim, C. Lee, H. Shim, Y. Eun, and J. H. Seo, Detection of sensor attack and resilient state estimation for uniformly observable nonlinear systems having redundant sensors, IEEE Transactions on Automatic Control. 64(3)(2018) 1162–1169.

[12] Y. Wang, J. Lu, and J. Liang, Security control of multiagent systems under denial-of-service attacks, IEEE Transactions on Cybernetics. (2020).

[13] J. Han, X. Liu, X. Gao, and X. Wei, Intermediate observer based robust distributed fault estimation for nonlinear multi-agent systems with directed graphs, IEEE Transactions on Industrial Informatics. 16(12)(2019) 7426-7436.

[14] C. Deng, and C. Wen, Distributed resilient observer-based fault-tolerant control for heterogeneous multi-agent systems under actuator faults and dos attacks, IEEE Transactions on Control of Network Systems. 7(3)(2020) 1308-1318.

[15] H. Ni, Z. Xu, J. Cheng, and D. Zhang, Robust stochastic sampled-data-based output consensus of heterogeneous multi-agent systems subject to random dos attack: a markovian jumping system approach, International Journal of Control, Automation and Systems. 17(7) (2019) 1687–1698.

[16] D. Zhang, L. Liu, and G. Feng, Consensus of heterogeneous linear multiagent systems subject to aperiodicsampled-dataanddosattack, IEEEtransactionsoncybernetics. 49(4) (2018) 1501–1511.

[17] Y. Yang, H. Xu, and D. Yue, Observer-based distributed secure consensus control of a class of linear multi-agent systems subject to random attacks, IEEE Transactions on Circuits and Systems I: Regular Papers. 66(8)(2019) 3089–3099.

[18] L. An, and G.-H. Yang, Secure state estimation against sparse sensor attacks with adaptive switching mechanism, IEEE Transactions on Automatic Control. 63(8)(2017) 2596–2603.

[19] M. Tan, Z. Song, and X. Zhang, Robust leader-following consensus of cyber–physical systems with cyber attack via sampled-data control, ISA transactions. (2020).

[20] R. Gao, and J. Huang, Leader-following consensus of uncertain strict feedback multiagent systems subject to sensor and actuator attacks, International Journal of Robust and Nonlinear Control. 30(17) (2020) 7635–7654.

[21] H. Chu, L. Gao, D. Yue, and C. Dou, Consensus of lipschitz nonlinear multiagent systems with input delay via observer-based truncated prediction feedback, IEEE Transactions on Systems, Man, and Cybernetics: Systems. 50(10) (2019) 3784-3794.

[22] Y. Wan, J. Cao, G. Chen, and W. Huang, Distributed observer-based cyber-security control of complex dynamical networks, IEEE Transactions on Circuits and Systems I: Regular Papers. 64(11)(2017) 2966–2975.

[23] J. Cao, and D. W. Ho, A general framework for global asymptotic stability analysis of delayed neural networks based on lmi approach, Chaos, Solitons & Fractals. 24(5) (2005) 1317–1329.

[24] Y. Yang, Q. Liu, Y. Qian, D. Yue, and X. Ding, Secure bipartite tracking control of a class of nonlinear multi-agent systems with nonsymmetric input constraint against sensor attacks, Information Sciences. 539 (2020) 504-521.

[25] Z G. Hou, L. Cheng, M. Tan, Decentralized Robust Adaptive Control for the Multiagent System Consensus Problem Using Neural Networks[J]. IEEE Transactions on Systems Man & Cybernetics Part B. 39(3)(2009) 636-647.