Secure Control of Uncertain Multi-agent Systems Under Cyber Attacks

Yajing Ma[1,2](✉), Zhanjie Li[3], and Shaohua Yang[4]

[1] Jiangsu Key Laboratory of Broadband Wireless Communication and Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
myajing517@126.com

[2] School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

[3] Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

[4] College of Engineering, Qufu Normal University, Qufu 273165, China

Abstract. This paper considers the secure control problem for a class of uncertain nonlinear multi-agent systems. To deal with the uncertainties, the adaptive laws are designed in an iterative manner. Furthermore, the auxiliary variables and Nussbaum-type functions are introduced to handle the effects caused by the attacks. By developing a common Lyapunov function, a secure control method is designed to guarantee the asymptotical consensus of the considered systems against cyber attacks. Finally, we present an example to validate the effectiveness.

Keywords: Cyber attacks · Secure control · Adaptive law · Multi-agent systems · Uncertainties

1 Introduction

In modern industrial process, physical components are connected with each other by network communication channels, such as transportation networks, UAVs, and formation of robots [1–4]. The connection by shared networks brings efficiency to control systems, but there are many vulnerabilities that could be maliciously exploited by hackers or attackers [5]. Therefor, it is paramountly important to pay more attention to the safety issue against malicious cyber attacks.

In the recent developments, denial-of-service (DoS) attacks and deception attacks are identified as two typical cyber attack and have been the subject of comprehensive research [6,7]. To handle the complex cyber attacks, many control schemes have been developed. In [8,9], the attack compensators and a dynamic surface-based resilient adaptive strategy were constructed to mitigate the effects of state-dependent actuator attacks. In [10], the Bernoulli distributed random model was introduced to characterize cyber attack, and a dynamic protocol was

Z. Ren et al. (Eds.): *Proceedings of 2021 5th Chinese Conference on Swarm Intelligence and Cooperative Control*, LNEE 934, pp. 146–154, 2023.
https://doi.org/10.1007/978-981-19-3998-3_15

designed to guarantee the security against deception attacks. For a Lipschitz-type system, [11] used a pinning method and measured the attack through a stochastic variable to achieve the synchronization under deception attacks.

In practice, switched nonlinear multi-agent systems (SNMASs) provide an general framework for modeling the man-made process involving switching behaviors [12]. Considering the importance from both theoretical and practical points of view, many results on control synthesis for the NMASs have been proposed. In the existing results, a large amount of effort has been made to solve the consensus problem of SNMASs, such as [13–15]. In [16], an adaptive robust fault-tolerant consensus protocol was designed for nonlinear fractional-order SNMASs with general directed topology. In [17,18], for MASs under fixed and switching topologies, the distributed event-triggered consensus was achieved when only the triggered information is available.

However, in the aforementioned results, the case that the control coefficients, and the constant parameters are required to be known. In addition, the time disturbances are ignored [19–21]. It is noted that many actual plants have uncertain natures, for example the automotive industry manufacturing process [22–24]. But, due to the difficulties caused by the unknown control coefficients, constant parameters, and time disturbances, the important secure control of uncertain NMASs in presence of cyber attacks has not been taken into account. This motivates the study.

2 Preliminaries

Consider the NMAS where the j-th agent is modeled as

$$\begin{aligned} \dot{\zeta}_{j,s} &= \zeta_{j,s+1} + f_{j,s}^{\sigma_j}(\zeta_{j,1}, \cdots, \zeta_{j,s}, \theta_j),\ +r_{j,s}(t),\ s = 1, \cdots, n-1, \\ \dot{\zeta}_{j,n} &= b_j u_j + f_{j,n}^{\sigma_j}(\zeta_j, \theta_j) + r_{j,n}(t), \\ z_i &= \zeta_{j,1}, \end{aligned} \tag{1}$$

where $\zeta_j = (\zeta_{j,1}, \ldots, \zeta_{j,n})^T \in R^n$, $z_i \in R$, $u_j \in R$, $j = 1, 2, \cdots, N$, are the state, output and input of the j-th agent, respectively. $\sigma_j : [0, \infty) \to \{1, 2, \cdots, m\}$ is the switching signal. The control coefficient b_j, the constant parameter θ_j and the time disturbance $r_{j,s}$ are all unknown. Assume $|r_{j,s}| \le r_0$ with r_0 being a positive constant. The nonlinear term $f_{j,s+1}^i : R^s \to R$ with $f_{j,s}^i(0) = 0$ is smooth. Consider the following sensor deception attack $\nu_j(\zeta_{j,s}, t)$ on the data information,

$$\breve{\zeta}_{j,s} = \zeta_{j,s} + \nu_j(\zeta_{j,s}, t), \quad s = 1, 2, \cdots, n, \tag{2}$$

where $\breve{\zeta}_{j,s}(t)$ is the obtained information of the j-th agent.

Assumption 1. *The attacks $\nu_j(\zeta_{j,s}, t)$, $j = 1, 2, \cdots, n$, are modeled as $\nu_j(\zeta_{j,s}, t) = \delta(t)\zeta_{j,s}$, where signals $\delta(t)$ are unknown. Denote $\varrho(t) = (1 + \delta(t))$ and $\zeta_{j,s} = \varrho(t)^{-1}\breve{\zeta}_{j,s}$. For $j = 1, 2, \cdots, n$, there are uncertain constants ϱ_0, $\bar{\varrho}_1$ and $\bar{\varrho}_2$ such that $|\dot{\varrho}(t)\varrho^{-1}(t)| \le \varrho_0$ and $0 < \bar{\varrho}_1 \le |\varrho(t)| \le \bar{\varrho}_2$.*

Lemma 1 [25,26]**.** *For the vectors ζ, y with suitable dimension, and the real-valued continuous function $f(y,\zeta)$, there are smooth functions $\psi(y)$ and $\bar{f}(\zeta)$ such that $|f(\zeta,y)| \leq \psi(y)\bar{f}(\zeta)$.*

By Lemma 1, there exist functions $\psi_{j,s}(\breve{\zeta}_{j,1},\cdots,\breve{\zeta}_{j,s})$ and constant ϖ such that

$$|f_{j,s}^{i}(\zeta_{j,1},\cdots,\zeta_{j,s},\theta_j)| \leq \varpi\psi_{j,s}(\breve{\zeta}_{j,1},\cdots,\breve{\zeta}_{j,s}). \tag{3}$$

3 Main Result

3.1 Design of Consensus Protocol

Step 1: For $j=1,\cdots,N$, introduce the auxiliary variables as

$$\begin{aligned}\dot{\eta}_j &= -\sum_{k=1}^{N} b_{j,k}(\breve{z}_i - \breve{z}_k),\\ z_{j,1} &= \breve{\zeta}_{j,1} - \eta_j,\end{aligned} \tag{4}$$

where $\breve{z}_i = \breve{\zeta}_{j,1}$, $\eta_j(0) = \breve{\zeta}_j(0)$. Choose the Lyapunov function candidate as

$$V_1 = \frac{1}{2}\sum_{j=1}^{N} z_{j,1}^2 + \frac{1}{2}\tilde{\varrho}^2 + \frac{1}{2}\tilde{\vartheta}^2, \tag{5}$$

where $\tilde{\varrho} = \varrho - \hat{\varrho}$, $\tilde{\vartheta} = \vartheta - \hat{\vartheta}$, and $\hat{\varrho}$, $\hat{\vartheta}$ are the estimation of ϱ_0, ϑ, respectively. By taking $\vartheta = \bar{\varrho}\varpi \max_{j=1,2,\cdots,N}|\theta_j|$ and by using (3), one can calculate that

$$z_{j,1}\varrho f_{j,1}^{i}(\zeta_{j,1},\theta_j) \leq \vartheta\pi + \vartheta\frac{(z_{j,1}\psi_{j,1})^2}{\sqrt{(z_{j,1}\psi_{j,1})^2+\pi^2}}. \tag{6}$$

Construct the virtual protocol $\breve{\zeta}_{j,2}^{*}$ as

$$\breve{\zeta}_{j,2}^{*} = -\mu_{j,1}z_{j,1} + \dot{\eta}_j - \hat{\varrho}\bar{\omega}_{\varrho,j,1} - \hat{\vartheta}\bar{\omega}_{\theta,j,1}, \tag{7}$$

where $\mu_{j,1}$ a positive constant, $\bar{\omega}_{\varrho,j,1} = \frac{z_{j,1}\breve{\zeta}_{j,1}^2}{\sqrt{(z_{j,1}\breve{\zeta}_{j,1})^2+\pi^2}}$, $\bar{\omega}_{\theta,j,1} = \frac{z_{j,1}\psi_{j,1}^2}{\sqrt{(z_{j,1}\psi_{j,1})^2+\pi^2}}$. Then, it follows from (4)–(7) that

$$\begin{aligned}\dot{V}_1 \leq &-\sum_{j=1}^{N}\mu_{j,1}z_{j,1}^2 + \sum_{j=1}^{N} z_{j,1}(\breve{\zeta}_{j,2} - \breve{\zeta}_{j,2}^{*})\\ &- \tilde{\varrho}(\dot{\hat{\varrho}} - \omega_{\varrho,1}) - \tilde{\vartheta}(\dot{\hat{\vartheta}} - \omega_{\theta,1}) + c_1,\end{aligned} \tag{8}$$

where $\omega_{\varrho,1} = \sum_{j=1}^{N} z_{j,1}\bar{\omega}_{\varrho,j,1}$, $\omega_{\theta,1} = \sum_{j=1}^{N} z_{j,1}\bar{\omega}_{\theta,j,1}$ and c_1 is a positive constant.

Step s $(2 \leq s \leq n-1)$: Construct the auxiliary variable $z_{j,s} = \breve{\zeta}_{j,s} - \breve{\zeta}^*_{j,s}$ with $\breve{\zeta}^*_{j,s}$ being the virtual protocol. By (1), the following inequality holds,

$$\dot{z}_{j,s} = \dot{\varrho}\varrho^{-1}\breve{\zeta}_{j,s} + \breve{\zeta}_{j,s+1} + \varrho f^i_{j,s}(\zeta_{j,1}, \cdots, \zeta_{j,s}, \theta_j) - \dot{\breve{\zeta}}^*_{j,s}. \tag{9}$$

Choose the Lyapunov function candidate as

$$V_s = V_{s-1} + \frac{1}{2}\sum_{j=1}^{N} z^2_{j,s}. \tag{10}$$

Similar to step 1, one can design the virtual protocol $\breve{\zeta}^*_{j,s+1}$ such that

$$\begin{aligned}\dot{V}_s \leq & -\sum_{j=1}^{N}\mu_{j,1}(z^2_{j,1} + \cdots + z^2_{j,s}) + \sum_{j=1}^{N} z_{j,s}z_{j,s+1} \\ & - \tilde{\varrho}(\dot{\hat{\varrho}} - \omega_{\varrho,s}) - \tilde{\vartheta}(\dot{\hat{\vartheta}} - \omega_{\theta,s}) - \sum_{j=1}^{N}\sum_{l=2}^{s} z_{j,l}\frac{\partial\breve{\zeta}^*_{j,l}}{\partial\hat{\varrho}}(\dot{\hat{\varrho}} - \omega_{\varrho,s}) \\ & - \sum_{j=1}^{N}\sum_{l=2}^{s} z_{j,l}\frac{\partial\breve{\zeta}^*_{j,l}}{\partial\hat{\vartheta}}(\dot{\hat{\vartheta}} - \omega_{\theta,s}) + c_s, \end{aligned} \tag{11}$$

where c_s is some a positive constant, $\omega_{\theta,s}$ and $\omega_{\varrho,s}$ are some functions.

Step n: At the finial step, the Lyapunov function is constructed as

$$V_n = V_{n-1} + \sum_{j=1}^{N}\frac{1}{2}z^2_{j,n}. \tag{12}$$

Design the control protocol as

$$u_j = -\mathcal{C}_j(\xi_j)\breve{\zeta}^*_{j,n+1}, \quad \dot{\xi}_j = \breve{\zeta}^*_{j,n+1}z_{j,n}, \tag{13}$$

and the adaptive laws as

$$\dot{\hat{\varrho}} = \omega_{\varrho,n}, \quad \dot{\hat{\vartheta}} = \omega_{\theta,n}, \tag{14}$$

where $\mathcal{C}_j(\xi_j) = \cosh(g_1\xi_j)\sin\left(\frac{\xi_j}{g^j_2}\right), j = 1, 2, \cdots, N$, with $g_1 > 0$ and $g_2 > 0$, and the structures of $\breve{\zeta}^*_{j,n+1}$, $\omega_{\varrho,n}$, $\omega_{\theta,n}$ are same as that in previous steps. Then, after calculation, we can obtain that

$$\dot{V}_n \leq -\sum_{j=1}^{N}\mu_{j,1}(z^2_{j,1} + \cdots + z^2_{j,n}) + \sum_{j=1}^{N}(\varrho b_j\mathcal{C}_j(\xi_j) - 1)\dot{\xi}_j + c_n, \tag{15}$$

where $c_n > 0$ is a constant.

3.2 Consensus Analysis

Theorem 1. *For the SNMASs (1), consider the cyber attacks (2) with Assumption 1. The consensus protocol (13) and the adaptive laws (14), guarantee the asymptotical consensus of all outputs under arbitrary switching.*

Proof: Integrating both sides of (15), it is deduced that

$$V_n(t) \leq \int_0^t \sum_{j=1}^{N} (\varrho b_j \mathcal{C}_j(\xi_j) - 1)\dot{\xi}_j \mathrm{d}\omega + c, \tag{16}$$

where $c > 0$ is a constant. By (16) and Barbalat's Lemma, we have $\lim_{t\to\infty} z_{j,s}(t) = 0$. Denote $\eta = (\eta_1, \cdots, \eta_N)^T$, $z_1 = (z_{1,1}, \cdots, z_{N,1})$, $\zeta_1 = (\zeta_{1,1}, \cdots, \zeta_{N,1})^T$ and $\varsigma = P^{-1}\eta$. Then, we obtain that

$$\dot{\varsigma} = -J\varsigma - JP^{-1}z_1, \tag{17}$$

where $P = [1_N; v_2; \cdots; v_N]$ and $L_A = PJP^{-1}$. $J = \mathrm{diag}\{0, J_1\}$ is the Jordan canonical form. Let $\bar{\varsigma} = (\varsigma_2, \cdots, \varsigma_N)$. By using Barbalat's Lemma, it follows from (17) that $\lim_{t\to\infty} |\bar{\varsigma}| = 0$. Furthermore, we can deduce that

$$\lim_{t\to\infty} (y_i(t) - z_i(t)) = 0, \tag{18}$$

which means that the output of agents reach consensus asymptotically under arbitrary switching.

4 An Illustrative Example

To illustrate the effectiveness, this section presents a numerical simulation. Consider the following uncertain SNMAS whose communication graph is shown in Fig. 1.

$$\begin{aligned} \dot{\zeta}_{j,1} &= b_j u_j + f_{j,1}^{\sigma_j}(\zeta_{j,1}, \theta_j) + r_{j,1}(t), \\ z_i &= \zeta_{j,1}, \end{aligned} \tag{19}$$

where $j = 1, 2, 3, 4$, $\sigma_j : [0, \infty) \to M = \{1, 2\}$. $f_{j,1}^i$, $f_{j,2}^i$, $f_{j,3}^i$ and $f_{j,4}^i$, $i \in 1, 2$, are selected as $f_{1,1}^1 = \sin(\zeta_{1,1})\theta_1$, $f_{1,1}^2 = \frac{\zeta_{1,1}\theta_1}{10+\zeta_{1,1}^2}$, $f_{2,1}^1 = \sin(\zeta_{2,1})\theta_2$, $f_{2,1}^2 = \zeta_{2,1}\theta_2$, $f_{3,1}^1 = \zeta_{3,1}\sin(\zeta_{3,1})$, $f_{3,1}^2 = \zeta_{3,1}^2$, $f_{4,1}^1 = \zeta_{4,1}$, $f_{4,1}^2 = 1 - \cos(\zeta_{4,1}^2)$, $r_{1,1} = r_{2,1} = r_{3,1} = r_{4,1} = 0.1\sin(t)$.

According to the design method in Sect. 3, we design the consensus protocol and the adaptive laws as follows

$$\begin{aligned} u_j &= -\mathcal{C}_j(\xi_j)\breve{\zeta}_{j,2}^*, \quad \dot{\xi}_j = \breve{\zeta}_{j,2}^* z_{j,1}, \\ \dot{\hat{\varrho}} &= \omega_{\varrho,1}, \quad \dot{\hat{\vartheta}} = \omega_{\theta,1}, \end{aligned} \tag{20}$$

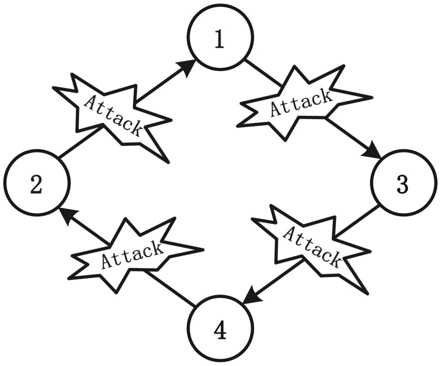

Fig. 1. Communication graph.

where $z_{j,1} = \breve{\zeta}_{j,1} - \eta_j$, $\breve{\zeta}^*_{j,2} = -\mu_{j,1} z_{j,1} + \dot{\eta}_j - \hat{\varrho}\bar{\omega}_{\varrho,j,1} - \hat{\vartheta}\bar{\omega}_{\theta,j,1}$, $\omega_{\varrho,1} = \sum_{j=1}^{N} z_{j,1}\bar{\omega}_{\varrho,j,1}$, $\omega_{\theta,1} = \sum_{j=1}^{N} z_{j,1}\bar{\omega}_{\theta,j,1}$, $\bar{\omega}_{\varrho,j,1} = \frac{z_{j,1}\breve{\zeta}_{j,1}^2}{\sqrt{(z_{j,1}\breve{\zeta}_{j,1})^2+\pi^2}}$, $\bar{\omega}_{\theta,j,1} = \frac{z_{j,1}\psi_{j,1}^2}{\sqrt{(z_{j,1}\psi_{j,1})^2+\pi^2}}$, $\psi_{1,1} = 2$, $\psi_{2,1} = |\breve{\zeta}_{2,1}|$, $\psi_{3,1} = 2\breve{\zeta}_{3,1}^2 + 1$, $\psi_{4,1} = |\breve{\zeta}_{4,1}| + 1$.

For Simulation, the parameters are selected as $\theta_1 = \theta_2 = 0.2$, $\theta_3 = \theta_4 = 1$, $b_1 = 0.9$, $b_2 = b_3 = 0.6$, $b_4 = -0.5$, $\mu_{1,1} = 2$, $\mu_{2,1} = 5$, $\mu_{3,1} = 2$, $\mu_{4,1} = 4$, $g_1 = 20$, $g_2 = 0.26$, $a = 1$, $\delta = 0.5 + 0.2\sin(t)$, $(\zeta_{1,1}(0), \zeta_{2,1}(0), \zeta_{3,1}(0), \zeta_{4,1}(0)) = (-0.2, 0.5, 0.1, 0.2)$, and the other initial states are set as zero. The switching signal is described in Fig. 2. For convenience, we let $z_y = (y_1 - y_2, y_2 - y_3, y_3 - y_4)$, and we will make a comparison to the control scheme in [24].

Figures 3 and 4 show the simulation results. Figure 3 shows the consensus error $\|z_y\|$ using the methods in the paper. It can be seen that the proposed control method can effectively deal with the cyber attacks of the uncertain MAS.

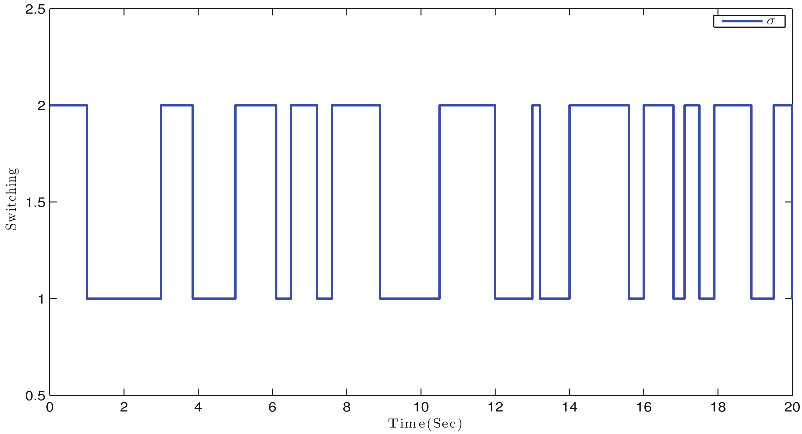

Fig. 2. Switching law.

Figure 4 show the adaptive laws of agents. The asymptotical consensus control objective is achieved under the proposed adaptive method.

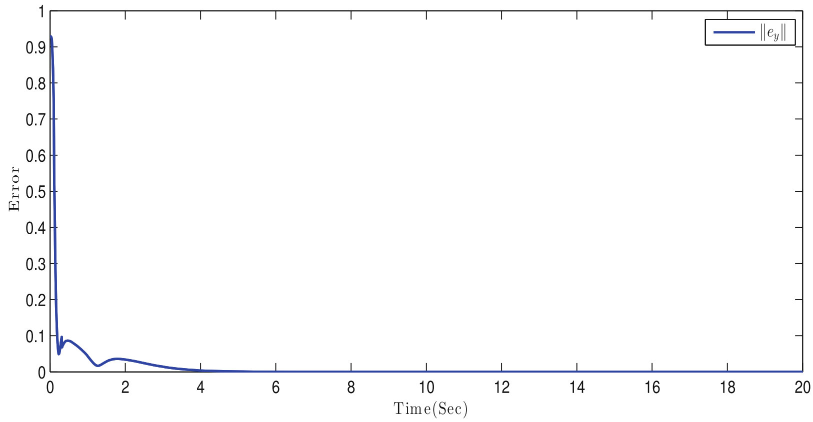

Fig. 3. Consensus error.

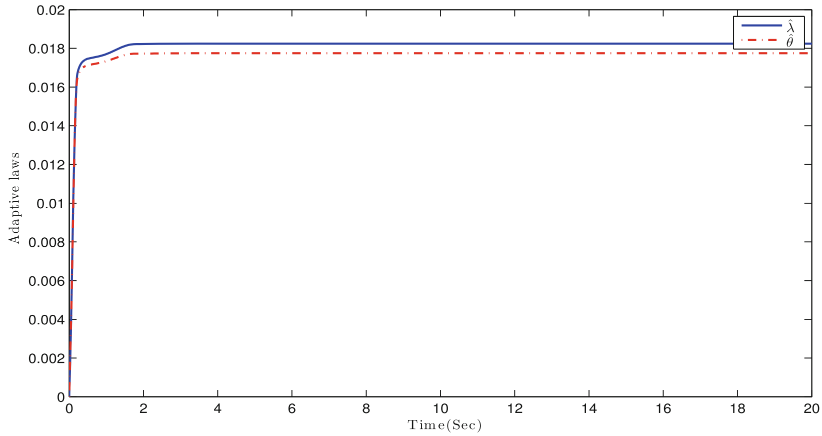

Fig. 4. Adaptive laws.

5 Conclusion

This paper has established a consensus method for uncertain NMASs against cyber attacks. We introduce Nussbaum-type functions and auxiliary variables to handle the uncertainties and cyber attacks. How to extend the designed consensus protocol to the cases of more general cyber attacks is worthy of further study.

Acknowledgement. This work was supported in part by National Natural Science Foundation of China under Grants 62103199, 62103201, in part by the Natural Science Foundation of Jiangsu Province under Grant BK20210590, in part by the College Science Research Program of Jiangsu Province under Grant 21KJB510043, and in part by the Research Grants of the Nanjing University of Posts and Telecommunications (NY220158 and NY220177).

References

1. Cao, Y., Ren, W.: Finite-time consensus for multi-agent networks with unknown inherent nonlinear dynamics. Automatica **50**(10), 2648–2656 (2014)
2. Ding, L., Han, Q.-L., Ge, X., Zhang, X.-M.: An overview of recent advances in event-triggered consensus of multiagent systems. IEEE Trans. Cybern. **48**(4), 1110–1123 (2018)
3. Zhang, Z., Mishra, Y., Dou, C., Yue, D., Zhang, B., Tian, Y.-C.: Delay-tolerant predictive power compensation control for photovoltaic voltage regulation. IEEE Trans. Indust. Inform. **17**(7), 4545–4554 (2021)
4. Li, Z., Zhao, J.: Output feedback stabilization for a general class of nonlinear systems via sampled-data control. Int. J. Robust Nonlinear Control **28**(7), 2853–2867 (2018)
5. Fei, Y., Shi, P., Lim, C.-C.: Neural network adaptive dynamic sliding mode formation control of multi-agent systems. Int. J. Syst. Sci. **51**(11), 2025–2040 (2020)
6. De Persis, C., Tesi, P.: Networked control of nonlinear systems under denial-of-service. Syst. Control Lett. **96**, 124–131 (2016)
7. Mahmoud, M.S., Hamdan, M.M., Baroudi, U.A.: Secure control of cyber physical systems subject to stochastic distributed dos and deception attacks. Int. J. Syst. Sci. **51**(9), 1653–1668 (2020)
8. Zha, L., Liu, J., Cao, J.: Resilient event-triggered consensus control for nonlinear muti-agent systems with dos attacks. J. Franklin Inst. **356**(13), 7071–7090 (2019)
9. Ma, Y., Li, Z., Zhao, J.: Output consensus for switched multi-agent systems with bumpless transfer control and event-triggered communication. Inf. Sci. **544**, 585–598 (2021)
10. Zhao, D., Wang, Z., Wei, G., Han, Q.L.: A dynamic event-triggered approach to observer-based PID security control subject to deception attacks. Automatica **120**, 109128 (2020)
11. He, W., Mo, Z., Han, Q., Qian, F.: Secure impulsive synchronization in Lipschitz-type multi-agent systems subject to deception attacks. IEEE/CAA J. Autom. Sinica **7**(5), 1326–1334 (2020)
12. Ma, Y., Zhao, J.: Distributed integral-based event-triggered scheme for cooperative output regulation of switched multi-agent systems. Inf. Sci. **457**, 208–221 (2018)
13. Yang, H., Han, Q.L., Ge, X., Ding, L., Zhou, D.: Fault-tolerant cooperative control of multiagent systems: a survey of trends and methodologies. IEEE Trans. Ind. Inform. **16**(1), 4–17 (2020)
14. Yuan, C., Wu, F.: Cooperative output regulation of multi-agent systems with switched leader dynamics. Int. J. Syst. Sci. **49**(7), 1463–1477 (2018)
15. Li, Z., Ma, Y., Zhao, J.: Control design of switched nonlinear systems: an intermittent compensation switching strategy. SIAM J. Control. Optim. **58**(6), 3684–3708 (2020)

16. Gong, P., Lan, W., Han, Q.-L.: Robust adaptive fault-tolerant consensus control for uncertain nonlinear fractional-order multi-agent systems with directed topologies. Automatica **117**, 109011 (2020)
17. Chen, W., Hu, J., Wu, Z., Yu, X., Chen, D.: Finite-time memory fault detection filter design for nonlinear discrete systems with deception attacks. Int. J. Syst. Sci. **51**(8), 1464–1481 (2020)
18. Ma, Y., Zhao, J.: Distributed event-triggered consensus using only triggered information for multi-agent systems under fixed and switching topologies. IET Control Theory Appl. **12**(9), 1357–1365 (2018)
19. Li, Z., Zhao, J.: Fuzzy adaptive robust control for stochastic switched nonlinear systems with full-state-dependent nonlinearities. IEEE Trans. Fuzzy Syst. **28**(9), 2035–2047 (2020)
20. Zhang, Z., Dou, C., Yue, D., Zhang, B.: Predictive voltage hierarchical controller design for islanded microgrids under limited communication. IEEE Trans. Circuits Syst. I Regul. Pap. **69**(2), 933–945 (2021). https://doi.org/10.1109/TCSI.2021.3117048
21. Li, Z., Yue, D., Ma, Y., Zhao, J.: Neural-networks-based prescribed tracking for nonaffine switched nonlinear time-delay systems. IEEE Trans. Cybern. (2021). https://doi.org/10.1109/TCYB.2020.3042232
22. Li, Z., Zhao, J.: Co-design of controllers and a switching policy for nonstrict feedback switched nonlinear systems including first-order feedforward paths. IEEE Trans. Autom. Control **64**(4), 1753–1760 (2019)
23. Zhao, J., Hill, D.J.: Dissipativity theory for switched systems. IEEE Trans. Autom. Control **53**(4), 941–953 (2008)
24. Huang, J., Song, Y., Wang, W., Wen, C., Li, G.: Fully distributed adaptive consensus control of a class of high-order nonlinear systems with a directed topology and unknown control directions. IEEE Trans. Cybern. **48**(8), 2349–2356 (2018)
25. Wei, L., Qian, C.: Adaptive control of nonlinearly parameterized systems: the smooth feedback case. IEEE Trans. Autom. Control **47**(8), 1249–1266 (2002)
26. Li, Z., Zhao, J.: Adaptive consensus of non-strict feedback switched multi-agent systems with input saturation. IEEE/CAA J. Automatica Sinica **8**(11), 1752–1761 (2021)