Letter

Attack-Resilient Control Against FDI Attacks in Cyber-Physical Systems

Bo Chen, *Member, IEEE*, Yawen Tan, Zhe Sun, and Li Yu, *Member, IEEE*

Dear editor,

This letter is concerned with the control of cyber-physical systems (CPSs) in the presence of malicious false data injection (FDI) attacks on actuators. The FDI attacks on actuators may result in faults of actuators or even the instability of CPSs. To tackle this problem, an unknown input observer (UIO) is proposed to estimate the system states and attack signals. For the aim of suppressing the impact of FDI attacks, a discrete-time sliding mode control (DSMC) algorithm is correspondingly put forward, where its reaching law is constructed based on the *n*-th order difference of the estimation of attack signals. Finally, two simulation instances are presented to show the effectiveness of the proposed method.

Introduction: Cyber-physical system (CPS) plays a more and more pivotal role in the era of Industry 4.0 and attracts increasing attention from academy and industry profiting by the advantages of networks such as low cost, less wiring and convenient maintenance [1]–[3]. However, the introduction of communication networks breaks the closeness of conventional physical systems, and thus results in the threat of cyber attacks [4]–[6]. Among various cyber attacks, FDI attack is a typical and threatening one, whose working principle is to break the integrity and availability of data by injecting erroneous signals [7]. Therefore, it is of great significance to research effective defense strategies for CPSs.

In order to maintain the security and improve the robustness of CPSs under cyber attacks, the concept and methods of fault tolerant control (FTC) are proposed. According to different working principles, FTC is classified into two types, i.e., active ones and passive ones [8]. Active FTC utilizes attack-detection method to identify attacks or faults, and then appropriately manipulate the control input to compensate for the corresponding negative effect [9]. On the other hand, passive FTC normally ensures the stability of a control system by considering and addressing the worst case. In contrast with passive FTC, the active FTC input contains the estimating information of attacks or faults, which makes the control system less conservative. Hence, the investigation of active FTC has aroused keen interest from researchers and engineers.

As a robust and effective nonlinear control strategy, sliding mode control (SMC) is recognized as one of the most competent tools in dealing with uncertain systems owing to its robustness or even insensitivity to perturbations. Hence, SMC has been introduced for the purposed of ensuring the security of CPSs [10]. Specifically, Li *et al*. proposed an adaptive SMC law with a discontinuous input term to defense actuator attacks [11]. An SMC method is put forward by [12] to ensure that CPSs are stochastic finite-time bounded when subjected to random injection attacks. Note that the aforementioned studies are under the same assumption, i.e., the system states can be directly measured. Nevertheless, this strict requirement is normally difficult to be satisfied in reality. Consequently, observer-based SMC has drawn more and more attention. For instance, an observer-based event-triggered SMC method is developed for nonlinear networked control systems subjected to cyber attacks [13]. In [14], a novel technique based on neural network is presented to estimate the attack signals for attenuating the negative effect, and an adaptive SMC method is designed to guarantee the system's security.

Motivated by the aforementioned research, this letter studies the control of CPSs under FDI attacks. An unknown input observer (UIO) is designed to jointly estimate the system states and attack signals, and a DSMC law is proposed to attenuate the impact of FDI attacks and maintain the stability of the control system. Finally, the effectiveness of the proposed DSMC law is verified from two simulation examples.

The main contributions of this letter are summarized as follows:

1) For a system with unknown states, an UIO is put forward such that the system states and FDI attack signals can be accurately estimated.

2) A DSMC algorithm is accordingly designed by introducing the high-order terms with respect to the estimation of attack signals, which further reduces the width of the quasi-sliding mode domain (QSMD).

Notations: $\mathbb{R}^n$ and $\mathbb{R}^{n\times m}$ denote the *n*-dimensional and $n\times m$ dimensional Euclidean spaces, respectively; the superscript T represents the transpose operation; I_n denotes an *n*-dimensional identity matrix.

Problem formulation: Consider a linear discrete-time CPS where the actuator is subjected to FDI attacks. The system's expression is shown as follows:

$$\begin{cases} x(k+1) = Ax(k) + B[u(k)+a(k)] \\ y(k) = Cx(k) \end{cases} \tag{1}$$

where $x\in\mathbb{R}^{n_x}$ is the system state; $u\in\mathbb{R}^l$ denotes the control input; $y\in\mathbb{R}^{n_y}$ is the measurement signal; $a\in\mathbb{R}^l$ represents the FDI attack signal; A, B and C are constant matrices of appropriate dimensions. T and k denote the sampling period and time step, respectively. For this system, we assume that the pair (A,B) is controllable, and the pair (A,C) is observable.

A robust sliding mode controller can be designed such that the system is capable of maintaining stable and effective after being attacked, where the corresponding sliding surface s is preliminarily defined as

$$s(k) = Gx(k) \tag{2}$$

where $G\in\mathbb{R}^{l\times n_x}$ and GB is nonsingular.

Problem 1: Design a suitable UIO and a DSMC law to ensure that when the system is suffering from FDI attacks, the system trajectories can converge to the sliding surface, and subsequently converge to the origin along the sliding surface.

Control design: In this section, an UIO is designed to estimate unknown FDI attack signals, and a sliding mode controller is correspondingly designed to guarantee the stability of the control system.

Initially, the state $x(k)$ can be decoupled into a known input $\bar{x}_1(k)$ and an unknown input $\bar{x}_2(k)$. For this aim, $\Phi = [M\ B]$ and $\Lambda = [CB\ \ N]$ are construct, where $N\in\mathbb{R}^{n_y\times(n_y-l)}$ and $M\in\mathbb{R}^{n_x\times(n_x-l)}$ are matrices chosen to satisfy that Φ and Λ are nonsingular [15]. Hence, we have $\Lambda^{-1} = [\Lambda_1\ \ \Lambda_2]^T$ with $\Lambda_1\in\mathbb{R}^{l\times n_y}$ and $\Lambda_2\in\mathbb{R}^{(n_y-l)\times n_y}$. Multiplying Φ^{-1} and Λ^{-1} on both sides of the state and the measurement equation in (1) yields

Corresponding author: Zhe Sun.

Citation: B. Chen, Y. W. Tan, Z. Sun, and L. Yu, "Attack-resilient control against FDI attacks in cyber-physical systems," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 6, pp. 1099–1102, Jun. 2022.

The authors are with the Department of Automation, Zhejiang University of Technology, Hangzhou 310023, and also with the Institute of Cyberspace Security, Zhejiang University of Technology, Hangzhou 310023, China (e-mail: bchen@aliyun.com; yawentan@aliyun.com; sunzhe726@zjut.edu.cn; lyu@zjut.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2022.105641

$$\begin{cases}\bar{x}(k+1)=\bar{A}\bar{x}(k)+\bar{B}[u(k)+a(k)]\\ y(k)=\bar{C}\bar{x}(k)\end{cases} \tag{3}$$

$$\begin{cases}\Lambda_1 y(k)=\Lambda_1 CM\bar{x}_1(k)+\bar{x}_2(k)\\ \Lambda_2 y(k)=\Lambda_2 CM\bar{x}_1(k)\end{cases} \tag{4}$$

where $x=\Phi\bar{x}=\Phi[\bar{x}_1\ \ \bar{x}_2]^T$, $\bar{A}=\Phi^{-1}A\Phi=\begin{bmatrix}\bar{A}_{11} & \bar{A}_{12}\\ \bar{A}_{21} & \bar{A}_{22}\end{bmatrix}$, $\bar{B}=\Phi^{-1}B=[0\ \ I_l]^T$, $\bar{C}=C\Phi=[CM\ \ CB]$. Combining (3) and (4) yields

$$\begin{cases}\bar{x}_1(k+1)=\tilde{A}\bar{x}_1(k)+Ey(k)\\ \bar{y}(k)=\tilde{C}\bar{x}_1(k)\end{cases} \tag{5}$$

where $\tilde{A}=\bar{A}_{11}-\bar{A}_{12}\Lambda_1 CM$, $E=\bar{A}_{12}\Lambda_1$, $\bar{y}(k)=\Lambda_2 y(k)$, and $\tilde{C}=\Lambda_2 CM$. A Luenberger observer can be designed while the system matrices $(\tilde{A},\tilde{C})$ is observable, In addition, the observability of this system has been examined and affirmed in [16]. According to the concept of UIO proposed in [17], a Luenberger observer is constructed to estimate $\bar{x}_1(k)$ with $\hat{\bar{x}}_1$, which signifies that $\hat{\bar{x}}_1\to\bar{x}_1$ as $t\to\infty$. The observer is shown as follows:

$$\begin{cases}\hat{\bar{x}}_1(k+1)=(\tilde{A}-L\tilde{C})\hat{\bar{x}}_1(k)+(L\Lambda_2+E)y(k)\\ \hat{\bar{x}}_2(k+1)=\Lambda_1 y(k+1)-\Lambda_1 CM\hat{\bar{x}}_1(k+1)\end{cases} \tag{6}$$

where $L\in\mathbb{R}^{(n_x-l)\times(n_y-l)}$. Then, the estimated state can be obtained as $\hat{x}(k)=\Phi\hat{\bar{x}}(k)$. Thus, by substituting (6) into (3), we achieve the estimation of the FDI attack signal $a(k)$ as

$$\begin{aligned}\hat{a}(k)=\ &\Lambda_1 y(k+1)-\Lambda_1 CM\hat{\bar{x}}_1(k+1)-\bar{A}_{21}\hat{\bar{x}}_1(k)\\ &-\bar{A}_{22}\Lambda_1 y(k)+\bar{A}_{22}\Lambda_1 CM\hat{\bar{x}}_1(k)-u(k).\end{aligned} \tag{7}$$

Rearranging (7), we can get a simplified equation as

$$\hat{a}(k)=K_1 y(k+1)+K_2\hat{\bar{x}}_1(k)+K_3 y(k)+K_4 u(k) \tag{8}$$

where $K_2=\Lambda_1 CML\Lambda_2 CM-\Lambda_1 CM\bar{A}_{11}+\Lambda_1 CM\bar{A}_{12}\Lambda_1 CM-\bar{A}_{21}+\bar{A}_{22}\Lambda_1 CM$, $K_3=-\Lambda_1 CML\Lambda_2-\Lambda_1 CM\bar{A}_{12}\Lambda_1-\bar{A}_{22}\Lambda_1$, $K_1=\Lambda_1$, $K_4=-I_l$. The estimated state $\hat{x}(k)$ and the estimated FDI attack signal $\hat{a}(k)$ will be utilized in the compensating procedure of the subsequent SMC design.

For the SMC design, the first step is to construct an appropriate sliding surface, which has been accomplished and embodied in (2). Not only a suitable sliding variable is required, but also a reaching law is of great importance. Herein, a reaching law based on [18] is adopted in our case, which is with the following expression:

$$s(k+1)=(1-qT)s(k)-\lambda\,\mathrm{sign}[s(k)]+\nabla^n a(k) \tag{9}$$

where $\nabla a(k)=CB\hat{a}(k)$; $\nabla^n a(k)=\nabla^{n-1}a(k)-\nabla^{n-1}f(k-1)$; $\mathrm{sign}[s(k)]\triangleq[\mathrm{sign}s_1(k),\ldots,\mathrm{sign}s_l(k)]^T$; q is chosen to satisfy $q>0$ and $0<1-qT<1$; $\lambda>0$ and $n>0$ are control parameters to be selected.

According to [19], we have the following lemma for the FDI attack signal $a(k)$:

Lemma 1: $a(k)=O(T), a(k)-a(k-1)=O(T^2)$, and $a(k)-2a(k-1)+a(k-2)=O(T^3)$, T is the sampling time.

From Lemma 1 it can be further concluded that $\nabla a(k)=O(T)$; $\nabla^2 a(k)=O(T^2)$; $\nabla^n a(k)=O(T^n)$. Therefore, the upper bound of the disturbance term in (9) can be decreased by augmenting the order of $\nabla a(k)$. Subsequent analysis will further prove that the width of QSMD can get reduced.

Combining (1), (2) and the reaching law (9), a DSMC law is obtained, and the corresponding control input $u(k)$ can be expressed as

$$\begin{aligned}u(k)=-(GB)^{-1}\Big[&GAx(k)-(1-qT)s(k)\\ &+\lambda\,\mathrm{sign}(s(k))+\sum\nolimits_{i=1}^{n-1}\nabla^i a(k-1)\Big].\end{aligned} \tag{10}$$

Remark 1: As the order of $\nabla a(k)$ increases, the width of QSMD will be shorten. Nevertheless, the constraint requirement for unknown signals will also be higher. It can be seen that the proposed DSMC law's working principle is based on the statistical characteristics of unknown signals.

Up to now, we have designed a DSMC law for the CPS under unknown FDI attacks. However, the stability of the control system is required to be proved. Specifically, in our case, we need to substantiate that the switch function $s(k)$ from any initial state can reach the QSMD and subsequently remain in the QSMD.

Theorem 1: For the discrete-time CPS as shown in (1) with the following assumption:

$$\xi=\max\nabla^n a(k)\le\lambda \tag{11}$$

the system trajectories will converge to an $O(T^n)$ QSMD by the proposed DSMC law, where the expression of Ω_Δ is shown as below:

$$\Omega_\Delta=\{s_i(k)\,|\,|s_i(k)|<\lambda+\xi\}. \tag{12}$$

Proof: Two cases of $s_i(k)>0$ and $s_i(k)<0$ are discussed here, respectively.

For the first case $s_i(k)>0$, from (9) we can obtain

$$\begin{aligned}s_i(k+1)&=(1-qT)s_i(k)-\lambda+\nabla^n a_i(k)\\ &<s_i(k)-\lambda+\nabla^n a_i(k)<s_i(k).\end{aligned} \tag{13}$$

As shown in (13), when $s_i(k)>0$, the sliding variable $s_i(k)$ is monotonically decreasing. Hence, there exists a situation where $s_i(k^*)>0$, and $s_i(k^*+1)<0$. It is of necessity to investigate whether $s_i(k^*+1)$ will exceed Ω_Δ in this case, i.e., whether $s_i(k^*+1)-(-\lambda-\xi)>0$. The deduction is shown as follows:

$$\begin{aligned}s_i(k^*+1)-(-\lambda-\xi)&=(1-qT)s_i(k^*)-\lambda+\nabla^n a_i(k^*)+\lambda+\xi\\ &=(1-qT)s_i(k^*)+\nabla^n a_i(k^*)+\xi\\ &>(1-qT)s_i(k^*)>0.\end{aligned} \tag{14}$$

It can be seen that when $s_i(k)>0$, the sliding variable $s_i(k)$ will converge into Ω_Δ.

For the second case $s_i(k)<0$, we can prove in the same way. ■

Though it has been verified that the switch function $s(k)$ from any initial state will finally converge into the QSMD, it is of great necessity to prove that the trajectories will stay in the QSMD and not escape from it.

Theorem 2: For the system (1) with the assumption (11) and under the DSMC law (10), when the switch function $s(k)$ enters QSMD Ω_Δ, it will always stay in it.

Proof: When $s(k)$ enters the QSMD, there exist two situations, namely, $0\le s(k)\le\lambda+\xi$ and $-\lambda-\xi\le s(k)\le 0$. Hence, we discuss this issue in two cases.

For the first case $0\le s(k)\le\lambda+\xi$, it can be derived that

$$\begin{aligned}s_i(k+1)&=(1-qT)s_i(k)-\lambda+\nabla^n a_i(k)\\ &\ge-\lambda+\nabla^n a_i(k)\\ &\ge-(\lambda+\xi)\end{aligned} \tag{15}$$

and

$$\begin{aligned}s_i(k+1)&=(1-qT)s_i(k)-\lambda+\nabla^n a_i(k)\\ &\le\lambda+\xi-(\lambda-\nabla^n a_i(k))\\ &\le\lambda+\xi.\end{aligned} \tag{16}$$

For the second case $-\lambda-\xi\le s_i(k)\le 0$, the proof can be completed by a similar procedure.

Consequently, we achieve the conclusion that when the sliding variable $s(k)$ enters the QSMD Ω_Δ, it stays inside Ω_Δ and is unable to escape from it. ■

To this end, we have presented the selection of the control parameters of the DSMC.

1) Selection of λ: The parameter λ determines the width of QSMD and the capacity of the system to resist attacks. Increasing λ enhances the attack-resistance ability but at the cost of bringing more chattering. Considering this tradeoff, we set $\lambda=0.2$.

2) Selection of q: The parameter q determines the convergence rate

of the system. A larger q leads to a faster convergence rate but at the cost of augmenting the risk of instability. To achieve a balance, the parameter q is set as $q = 5$.

3) Selection of n: The parameter n denotes the order of the attack signal. From Lemma 1, it can be seen that a larger n leads to a narrower QSMD. However, increasing n also means more strict conditions to be satisfied. Taking this tradeoff into consideration, we set $n = 5$.

Simulation results: A fourth-order inverted pendulum system [20] is adopted as the controlled object whose dynamic model is as (1), where the system matrix, input matrix and measurement matrix are set as $A = \begin{bmatrix} 1 & 0.0991 & 0.0136 & 0.0004 \\ 0 & 0.9818 & 0.2789 & 0.0136 \\ 0 & -0.0023 & 1.1598 & 0.1053 \\ 0 & -0.0474 & 3.2764 & 1.1598 \end{bmatrix}$, $B = \begin{bmatrix} 0.0091 \\ 0.1822 \\ 0.0232 \\ 0.4732 \end{bmatrix}$ and $C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, respectively. The initial state and the sampling period are set as $x(0) = [0.98\ \ 0\ \ 0.2\ \ 0]^T$ and $T = 0.1$ s. Two simulations are carried out, where various FDI attack signals are adopted to test the effectiveness and robustness of the UIO-based SMC law. In Case 1, the FDI attack signal $a(k)$ is set as

$$\begin{cases} a(k) = -2\cos(k\pi T), & k < 50 \\ a(k) = 2, & 50 \le k < 125 \\ a(k) = 5\sin(k\pi T), & 125 \le k < 200. \end{cases} \tag{17}$$

Another relatively complicated FDI attack signal $a(k)$ in Case 2 is designed as

$$\begin{cases} a(k) = \sin(k\pi T), & k < 50 \\ a(k) = \sin(k\pi T) + e^{1-\frac{1}{[(k-50)T]^2}}, & 50 \le k < 125 \\ a(k) = \sin(k\pi T) + e^{1-\frac{1}{[(k-50)T]^2}} \\ \qquad -e^{1-\frac{1}{[(k-125)T]^2}}, & 125 \le k < 200. \end{cases} \tag{18}$$

By implementing the proposed algorithm, the simulation results are obtained and shown in Figs. 1–4. Specifically, the estimation performance of the proposed UIO is shown in the upper parts of Figs. 1 and 3, which turns out to be satisfactory. Under different attacks, the estimated FDI attack signals are able to track the actual ones precisely. As shown in Fig. 2, when the attack signal changes, namely, when $k = 125$, the sliding variable deviates from the QSMD for a pretty short time but then immediately converges back to the QSMD and stays in it. The width of the QSMD is approximately 0.2. From Fig. 4 we can see that the proposed DSMC law is able to guarantee the convergence within the QSMD, where the width of the QSMD is approximately 0.17. The lower parts of Figs. 1 and 3 reveal that the system trajectories under the action of the presented method converge to zero in a pretty short time and maintain stable thereafter.

Conclusions: This letter investigates the control of CPSs under FDI attacks. An UIO is designed to estimate the system states and attack signals, and a DSMC algorithm is accordingly developed to attenuate the impact of FDI attacks, where the stability of the control system is mathematically substantiated in detail. The simulation results evidently demonstrate the effectiveness and superiority of the presented UIO-based DSMC method. Note that our study in this letter is concerned with a linear CPS model. However, most of the CPSs in reality are nonlinear ones. Hence, our future work is to study nonlinear CPSs and put forward more robust and effective control strategies.

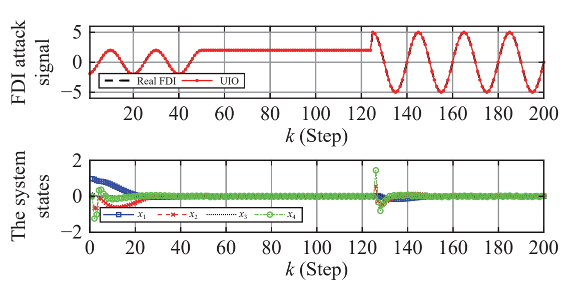

Fig. 1. Estimation of FDI attack signal and system states in Case 1.

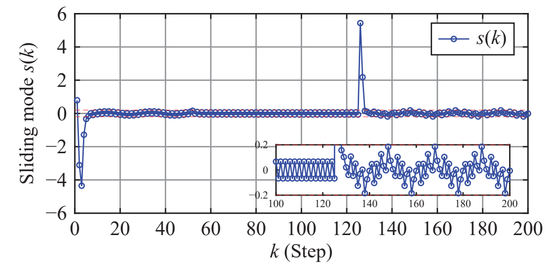

Fig. 2. Sliding mode dynamics in Case 1.

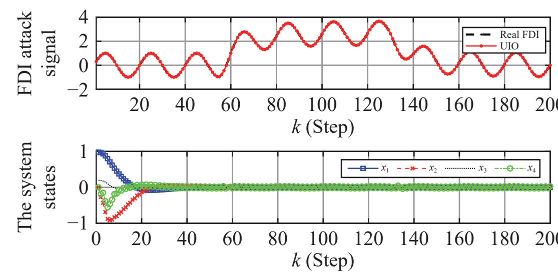

Fig. 3. Estimation of FDI attack signal and system states in Case 2.

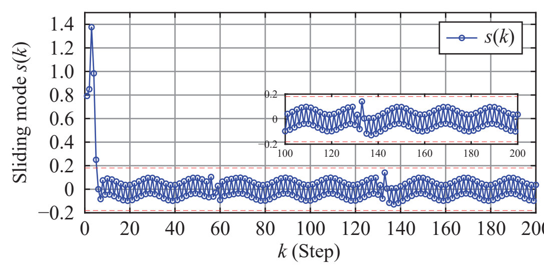

Fig. 4. Sliding mode dynamics in Case 2.

Acknowledgments: This work was supported in part by the National Natural Science Funds of China (61973277, 62073292) and the Zhejiang Provincial Natural Science Foundation of China (LR20F030004, LY20F020030).

References

[1] D. Ding, Q. Han, X. Ge, and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey," *IEEE Trans. Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 176–190, 2020.

[2] B. Chen, D. W. C. Ho, G. Hu, and L. Yu, "Delay-dependent distributed Kalman fusion estimation with dimensionality reduction in cyber-physical systems," *IEEE Trans. Cybernetics*, 2021. DOI: 10.1109/TCYB.2021.3119461.

[3] S. Lai, B. Chen, T. Li, and L. Yu, "Packet-based state feedback control under DOS attacks in cyber-physical systems," *IEEE Trans. Circuits and Systems II: Express Briefs*, vol. 66, no. 9, pp. 1421–1425, 2019.

[4] B. Chen, D. W. C. Ho, G. Hu, and L. Yu, "Secure fusion estimation for bandwidth-constrained cyber-physical systems under replay attacks," *IEEE Trans. Cybernetics*, vol. 48, no. 6, pp. 1862–1876, 2018.

[5] X. Ge, Q. Han, M. Zhong, and X. Zhang, "Distributed krein space-based attack detection over sensor networks under deception attacks," *Automatica*, vol. 109, p. 108557, 2019. DOI: 10.1016/j.automatica.2019.108557.

[6] B. Chen, G. Hu, D. W. Ho, and L. Yu, "Distributed estimation and control for discrete time-varying interconnected systems," *IEEE Trans. Automatic Control*, 2021. DOI: 10.1109/TAC.2021.3075198

[7] L. Gao, B. Chen, and L. Yu, "Fusion-based FDI attack detection in cyberphysical systems," *IEEE Trans. Circuits and Systems II: Express Briefs*, vol. 67, no. 8, pp. 1487–1491, 2019.

[8] A. Abbaspour, S. Mokhtari, A. Sargolzaei, and K. K. Yen, "A survey on active fault-tolerant control systems," *Electronics*, vol 9, no. 9, p. 1513, 2020. DOI: 10.3390/electronics9091513.

[9] X. Yu and J. Jiang, "A survey of fault-tolerant controllers based on safety-related issues," *Annual Reviews in Control*, vol. 39, pp. 46–57, 2015.

[10] X. Huang, D, Zhai, and J. Dong, "Adaptive integral sliding-mode control strategy of data-driven cyber-physical systems against a class of actuator attacks," *IET Control Theory* & *Applications*, vol. 12, no. 10, pp. 1440–1447, 2018.

[11] M. Li, Y. Chen, Y. Zhang, and Y. Liu, "Adaptive sliding-mode tracking control of networked control systems with false data injection attacks," *Information Sciences*, vol. 585, pp. 194–208, 2022.

[12] Z. Cao, Y. Niu, and J. Song, "Finite-time sliding-mode control of Markovian jump cyber-physical systems against randomly occurring injection attacks," *IEEE Trans. Automatic Control*, vol. 65, no. 3, pp. 1264–1271, 2019.

[13] L. Zhang and G. Guo, "Observer-based adaptive event-triggered sliding mode control of saturated nonlinear networked systems with cyberattacks," *Information Sciences*, vol. 543, pp. 180–201, 2021.

[14] Z. Cao, Y. Niu, and Y. Zou, "Adaptive neural sliding mode control for singular semi-Markovian jump systems against actuator attacks," *IEEE Trans. Systems*, *Man*, *and Cybernetics: Systems*, vol. 51, no. 3, pp. 1523–1533, 2019.

[15] M. Hou and P. Muller, "Design of observers for linear systems with unknown inputs," *IEEE Trans. Automatic Control*, vol. 37, no. 6, pp. 871–875, 1992.

[16] M. R. Khalghani, J. Solanki, S. K. Solanki, M. H. Khooban, and A. Sargolzaei, "Resilient frequency control design for microgrids under false data injection," *IEEE Trans. Industrial Electronics*, vol. 68, no. 3, pp. 2151–2162, 2020.

[17] J. Chen, R. J. Patton, and H. Zhang, "Design of unknown input observers and robust fault detection filters," *Int. J. Control*, vol. 63, no. 1, pp. 85–105, 1996.

[18] W. Gao, Y. Wang, and A. Homaifa, "Discrete-time variable structure control systems," *IEEE Trans. Industrial Electronics*, vol. 42, no. 2, pp. 117–122, 1995.

[19] H. Ma, J. Wu, and Z. Xiong, "A novel exponential reaching law of discrete-time sliding-mode control," *IEEE Trans. Industrial Electronics*, vol. 64, no. 5, pp. 3840–3850, 2017.

[20] H. Yang, Y. Xu, and J. Zhang, "Event-driven control for networked control systems with quantization and Markov packet losses," *IEEE Trans. Cybernetics*, vol. 47, no. 8, pp. 2235–2243, 2017.