Adaptive Secure Control for Uncertain Cyber–Physical Systems With Markov Switching Against Both Sensor and Actuator Attacks

Zhen Liu, Junye Zhang, and Quanmin Zhu

***Abstract*—In this article, adaptive secure controller synthesis for uncertain cyber–physical systems with Markov switching (CPSMSs), both sensor and actuator stealthy attacks as well as generally unknown transition rates (GUTRs), is under consideration via neural sliding mode control (SMC) technique. In order to resist unknown attack signals from both sensor and actuator channels, a novel neural network (NN)-based SMC design is performed, which could not only guarantee the boundedness of relevant adaptive data but also force the actual state trajectories to arrive at the proposed sliding mode surface (SMS) with limited moments almost surely. Then, a fresh stochastically stable criterion for the resultant plant is provided in spite of hidden cyber attacks, GUTRs, and structural uncertainty, relying on the arrival of the SMS and stochastic stability theory. Finally, an F-404 aircraft engine model with performance comparisons is offered to confirm the feasibleness of the theoretical result.**

***Index Terms*—Cyber–physical systems (CPSs), Markov switching parameter, neural network (NN), sensor and actuator attacks, sliding mode control (SMC).**

I. Introduction

CYBER–PHYSICAL systems (CPSs), in view of the advancement of computers and information interaction technology, have been extensively found and studied in industrial field around the heterogeneous cyber layers and physical plants [1], [2], [3], [4]. Nevertheless, upon the background of continuous development and increasing complexity of networked embedded technique, the fragility of CPSs from unknown attackers is escalated. Malicious attacks will degrade system's control precision by fabricating the sensor's measurement and/or impeding the actuator's command, which would cause unpredictable damage to physical systems [5], [6], [7], [8], [9]. It is thus of great significance, from the point of view of long-term operation, to deal with the security problem of CPSs with in-depth exploration [10].

Of special relevance for this work are a class of hybrid dynamic systems called Markov jump systems (MJSs), by which physical plants with random switching mechanism could be emulated, such as chemical reactor, DC motor, TD jump circuit, wheeled mobile manipulators, and aircraft engine system [11], [12], [13], [14], [15]. Note that the primary matter of concern for analysis and synthesis of MJSs is relevant to so-called transition rates (TRs), and research under partly unknown TRs reduces conservatism of the investigated model [16], in comparison to the case of completely known TRs. However, given the difficulty in obtaining the TRs and unknown uncertainties in practical situations, comprehensive studies on control of MJSs under generally unknown TRs (GUTRs) may be more realistic, and some remarkable control strategies have been reported in this direction [7].

As a typical robust control technique, sliding mode control (SMC) has been extensively focused around control community and engineering applications in view of its simplicity in algorithm, robustness to parametric uncertainties and disturbances [17], [18], [19], [20]. It is noteworthy that some progresses under SMC strategy have been absorbed into the synthesis of uncertain MJSs [12], [13], [15], [17], [20], [21], [22]. To cite a few, an event-triggered SMC for discrete-time MJSs was deliberated more in [20]; the stabilization for MJSs subject to actuator faults was investigated based upon adaptive SMC in [23]. It is also notable that, security control problems of CPSs have been probed further [24], [25], [26], e.g., adaptive control methods against stealthy attacks were proposed for nonlinear T–S fuzzy systems and discrete-time systems in [24] and [25], respectively.

Due to practical background of hybrid systems and signal communications between plant devices and cyber layers, recent years have witnessed the research progress of CPSs with Markov switching (CPSMSs). Apart from the GUTRs, another crucial matter in resilient control of CPSMSs is the malicious cyber attacks, and some control strategies for CPSMSs against injected attacks were investigated [7], [17], [27], [28]. Notably, the above researches focused on the actuator attacks from cyber layers only, while ignoring the general case malicious attackers pose unknown attacks to both the actuator and sensor's channels concurrently. In fact, the output signals may be contaminated due to injected sudden sensor attacks,

Received 15 August 2024; revised 28 December 2024; accepted 26 February 2025. This work was supported in part by the National Natural Science Foundation of China under Grant 61803217 and Grant 62003231; in part by the Natural Science Foundation of Shandong Province under Grant ZR2023MF029; in part by the Team Plan for Youth Innovation of Universities in Shandong Province under Grant 2022KJ142; and in part by the Taishan Scholar Special Project Fund under Grant TSON202408163. *(Corresponding author: Zhen Liu.)*

Zhen Liu and Junye Zhang are with the School of Automation and the Shandong Key Laboratory of Industrial Control Technology, Qingdao University, Qingdao 266071, China (e-mail: zhenliuzz@hotmail.com; junyezhang1@163.com).

Quanmin Zhu is with the School of Engineering, University of the West of England, BS16 1QY Bristol, U.K. (e-mail: quan.zhu@uwe.ac.uk).

which will be inaccurate for the sliding surface design and controller synthesis, then the control signal becomes invalid and the security of the system is not guaranteed, leading to the instability of the whole system. Just recently, an adaptive resilient control method for CPSMSs under sensor and actuator attacks was studied in [29], whereas the previous control results were discussed in the light of norm-bounded assumption made in system attacks. To the authors' knowledge, the above-addressed issues or limitations regarding the analysis and synthesis of CPSMSs still have not been fully inspected and solved so far. Moreover, neural network (NN), as a valid approximation technology, has been employed to identify unknown nonlinear signals, which is beneficial for the controller design to a great extent [30], however, related reports on NN-based SMC strategy of CPSMSs are relatively scarce, which generates the motivation of the work finally.

In response to the above observations, this article attempts to provide an NN-based secure control scheme for uncertain CPSMSs against structural uncertainty, GUTRs, both sensor and actuator attacks under a novel SMC framework. The main innovations and tasks are delivered as follows.

1) In contrast to [17] and [28], a simplified linear-type sliding mode surface (SMS) is established drawing upon the actual sensor measurement, from which an updated adaptive SMC framework for uncertain CPSMSs is conducted, and a novel sufficient criterion for the resultant system to be stochastically stable is derived relying on the attainability of the special SMS and stochastic stability theory.
2) In comparison to [17], [27], [28], and [29], a novel NN-based SMC strategy is exhibited to guarantee both the finite-time reachability of the proposed SMS and security performance with robustness against sensor and actuator attacks as well as the GUTRs, where previous norm boundedness assumption for unknown attacks is no longer required, which generalizes the result in previous works.
3) The resiliency of the developed control mechanism against pernicious actuator and sensor attacks is verified through simulation analysis, and the efficiency of the proposed theoretical result is justified by performance comparisons with specified indicators.

Notation: sym$\{P\}$ represents $P + P^{\mathrm{T}}$. In symmetric block matrices, "$*$" is employed to denote abbreviations of symmetry terms. Mathematical expectation is expressed by $\mathbb{E}\{\cdot\}$, and $\|\cdot\|_F$ represents the Frobenius-norm.

II. Model Description and Preparations

A. System Description

The following class of uncertain CPSMSs are considered:

$$\dot{x}(t) = (A(r_t) + \Delta A(r_t, t))x(t) + B(r_t)u_a(t) \tag{1}$$

where $x(t) = [x_1(t), x_2(t), \ldots, x_n(t)]^{\mathrm{T}} \in \mathcal{R}^n$ and $u_a(t) \in \mathcal{R}^m$ stand for state vector and control signal subject to certain actuator attacks, respectively. $A(r_t) \in \mathcal{R}^{n\times n}$ and $B(r_t) \in \mathcal{R}^{n\times m}$ represent system matrices, $\Delta A(r_t, t)$ is the structural uncertainty that fulfills $\Delta A(r_t, t) = D(r_t)\Delta Y(t)E(r_t)$, where $D(r_t)$ and $E(r_t)$ are known matrices, $\Delta Y(t)$ is an uncertain matrix and $\Delta Y^T(t)\Delta Y(t) \le I$. The right-continuous Markov process denoted by $\{r_t, t \ge 0\}$, give values in the set $\mathcal{J} = \{1, 2, \ldots, J\}$.

In what follows, attack scenarios are focused in the beginning, from which both sensor measurement and control input signal may be corrupted. The sensor attack depending on the state is defined by $\partial_s(t)$ as

$$\partial_s(t) = p(t)x(t), t \ge 0 \tag{2}$$

where $p(t)$ denotes the time-varying unknown nonlinear weight function which satisfies $0 \le p(t) \le \bar{\varrho} < 1$ and $|\dot{p}(t)| \le \bar{\varsigma} < 1$, $t \ge 0$, $\bar{\varrho}$ and $\bar{\varsigma}$ are two unknown scalars. Then, the actual state information $x_s(t)$, stemming from the compromised sensor channel for feedback, is expressed as

$$x_s(t) = x(t) + \partial_s(t), t \ge 0. \tag{3}$$

In addition, the actual control signal $u_a(t)$ received by the actuator is depicted by

$$u_a(t) = u(t) + \partial_a(x(t), t), t \ge 0 \tag{4}$$

in which $u(t)$ is the devised controller, $\partial_a(x(t), t)$ represents the actuator attack signal estimated by NN in Section II-B.

Designate $\Pi = [\eta_{ij}]_{J\times J}(i, j \in \mathcal{J})$ as TR matrix with mode transition probabilities shown by

$$\begin{aligned} \mathrm{P}_{ij} &= \Pr(r_{t+\Delta t} = j | r_t = i) \\ &= \begin{cases} \eta_{ij}\Delta t + o(\Delta t), & \text{if } i \ne j; \\ 1 + \eta_{ii}\Delta t + o(\Delta t), & \text{if } i = j \end{cases} \end{aligned}$$

where $\eta_{ij} = \hat{\eta}_{ij} + \Delta\eta_{ij}$ represents TR from mode i at moment t to mode j at moment $t + \Delta t$, $\hat{\eta}_{ij}$ denotes the TR's deterministic term, and $\Delta\eta_{ij}$ stands for uncertain term satisfying $|\Delta\eta_{ij}| \le \vartheta_{ij}$, $\vartheta_{ij} > 0$, when $i \ne j$; and $\eta_{ii} = -\sum_{j=1, j\ne i}^{J} \eta_{ij}$. For convenience, the following two index sets are introduced:

$$\begin{aligned} {\Omega_k}^i &\triangleq \left\{j{:}\hat{\eta}_{ij} \text{ is accessible for } j \in \mathcal{J}\right\} \\ {\Omega_{uk}}^i &\triangleq \left\{j{:}\hat{\eta}_{ij} \text{ is inaccessible for } j \in \mathcal{J}\right\} \end{aligned} \tag{5}$$

with the TRs divided by four categories: 1) $i \in {\Omega_k}^i$ and $j \in {\Omega_{uk}}^i \ne \oslash$; 2) $i \in {\Omega_{uk}}^i$ and ${\Omega_k}^i \ne \oslash$; 3) ${\Omega_{uk}}^i = \mathcal{J}$ and $j \in {\Omega_k}^j$ for some $j \ne i$; and 4) ${\Omega_{uk}}^i = \mathcal{J}$ and $j \notin {\Omega_k}^j$ for any $j \in \mathcal{J}$. Let $r_t = i \in \mathcal{J}$, $A(r_t)$, $\Delta A(r_t, t)$, $B(r_t)$, $D(r_t)$, $E(r_t)$ and $\Delta Y(t)$ can be shortened by A_i, $\Delta A_i(t)$, B_i, D_i, E_i, and ΔY. Consequently, (1) is reorganized as

$$\begin{aligned} \dot{x}(t) = (A_i + \Delta A_i(t))x(t) \\ + B_i[u(t) + \partial_a(x(t), t)]. \end{aligned} \tag{6}$$

B. Neural Network Architecture

As stated in [30], a three-layer feedforward NN is used to design an adaptive neural controller in this research (see Fig. 1), and the net with the input x and output y is given as $y(x) = W^T\varphi(V^T x)$, where W and V denote the connection weights between neurons with corresponding dimensions, and $\varphi(\cdot)$ represents the activation function in the hidden layer neurons.

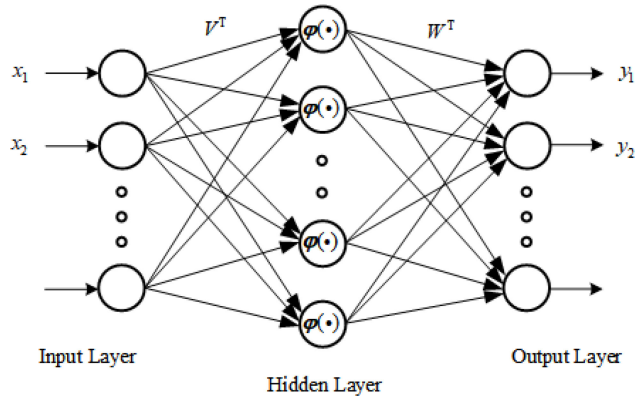

Fig. 1. NN structure.

In view of the approximation capability of the three-layer NN for continuous functions [30], [31], [32], one has

$$\partial_a(x(t),t) = W_d^{\mathrm{T}}\varphi\left(\mathcal{O}_d^{\mathrm{T}}\bar{\mathcal{X}}_d\right) + \phi_d(x), x(t) \in \Im \tag{7}$$

where $W_d \in \mathcal{R}^{r\times m}$ and $\mathcal{O}_d \in \mathcal{R}^{(n+1)\times r}$ are the optimization weights of hidden-to-output layer and input-to-hidden layer with r neurons, $\mathcal{O}_d \triangleq [\mathcal{O}_{d1}, \mathcal{O}_{d2}, \ldots, \mathcal{O}_{dr}]$, contains the threshold; $\bar{\mathcal{X}}_d = [x^{\mathrm{T}}(t), -1]^{\mathrm{T}}$ represents the neural input vector with input bias -1, $\varphi(\mathcal{O}_d^{\mathrm{T}}\bar{\mathcal{X}}_d) \triangleq [\varphi_1(\mathcal{O}_{d1}^{\mathrm{T}}\bar{\mathcal{X}}_d), \varphi_2(\mathcal{O}_{d2}^{\mathrm{T}}\bar{\mathcal{X}}_d), \ldots, \varphi_r(\mathcal{O}_{dr}^{\mathrm{T}}\bar{\mathcal{X}}_d)]^T$, in which $\varphi_l(\mathcal{O}_{dl}^{\mathrm{T}}\bar{\mathcal{X}}_d) = [1/1+e^{-\mathcal{O}_{dl}^{\mathrm{T}}\bar{\mathcal{X}}_d}]$ is a sigmoid function, $l = 1, \ldots, r$, $\Im$ is a compact set; $\phi_d(x)$ indicates the estimation error vector meeting $\|\phi_d(x)\| \le \bar{\phi}_d$, $\bar{\phi}_d > 0$ is an unknown constant [30]. However, considering that the original state signal $x(t)$ may not be acquired due to the sensor attack, we redefine the actuator attack by NN as follows:

$$\begin{aligned}\partial_a(x(t),t) &= W^{\mathrm{T}}\varphi\left(\mathcal{O}^{\mathrm{T}}\bar{\mathcal{X}}\right) + \phi(x_s(t)) \\ &\triangleq \partial_a(x_s(t),t), x_s(t) \in \Im\end{aligned} \tag{8}$$

in which $\bar{\mathcal{X}} = (x_s^{\mathrm{T}}(t), -1)^{\mathrm{T}}$; similarly, $W \in \mathcal{R}^{r\times m}$ and $\mathcal{O} \in \mathcal{R}^{(n+1)\times r}$ are the optimization weights, and the approximation error vector is described by $\phi(x_s(t))$ with $\|\phi(x_s(t))\| \le \bar{\phi}$, $\bar{\phi} > 0$.

Lemma 1 [30], [31], [32]: The attack signal $\partial_a(x_s(t),t)$ is estimated by $\hat{\partial}_a(x_s(t),t) = \hat{W}^{\mathrm{T}}\varphi(\hat{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}})$ based on NN. Then, the approximated error $\hat{\partial}_a(x_s(t),t) - \partial_a(x_s(t),t)$ shown by $\tilde{\partial}_a(x_s(t),t)$, is rebuilt as

$$\begin{aligned}\tilde{\partial}_a(x_s(t),t) &= \tilde{W}^{\mathrm{T}}\left(\hat{\varphi} - \hat{\varphi}'\hat{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}}\right) \\ &\quad + \hat{W}^{\mathrm{T}}\hat{\varphi}'\tilde{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}} + v(x_s(t))\end{aligned} \tag{9}$$

where the estimation error matrices of the weights are provided by $\tilde{W} = \hat{W} - W$, and $\tilde{\mathcal{O}} = \hat{\mathcal{O}} - \mathcal{O}$, in which $\hat{W} \in \mathcal{R}^{r\times m}$ and $\hat{\mathcal{O}} \in \mathcal{R}^{(n+1)\times r}$ indicate the hidden-output and input-hidden weight matrices, and r refers to the number of hidden neurons. Moreover, the residual term $v(x_s(t))$ is described as

$$v(x_s(t)) = \tilde{W}^{\mathrm{T}}\hat{\varphi}'\mathcal{O}^{\mathrm{T}}\bar{\mathcal{X}} + W^{\mathrm{T}}o\left(\tilde{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}}\right) + \phi(x_s(t)) \tag{10}$$

where $\hat{\varphi}' \triangleq \mathrm{diag}\{\varphi_1'(\hat{\mathcal{O}}_1^{\mathrm{T}}\bar{\mathcal{X}}), \varphi_2'(\hat{\mathcal{O}}_2^{\mathrm{T}}\bar{\mathcal{X}}), \ldots, \varphi_r'(\hat{\mathcal{O}}_r^{\mathrm{T}}\bar{\mathcal{X}})\} \in \mathcal{R}^{r\times r}$, $\varphi_l'(\hat{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}})$ means the derivative of the lth neuron in the hidden layer of NN related to the input signal, $l = 1, 2, \ldots, r$, $\hat{\varphi} \triangleq [\varphi_1(\hat{\mathcal{O}}_1^{\mathrm{T}}\bar{\mathcal{X}}), \varphi_2(\hat{\mathcal{O}}_2^{\mathrm{T}}\bar{\mathcal{X}}), \ldots, \varphi_r(\hat{\mathcal{O}}_r^{\mathrm{T}}\bar{\mathcal{X}})]^T \in \mathcal{R}^{r\times 1}$, and $o(\cdot)$ represents the infinitesimal.

Lemma 2 [32]: The norm of $v(x_s(t))$ satisfies $\|v(x_s(t))\| < \alpha^{\mathrm{T}}\omega$, in which the vector $\alpha \in \mathcal{R}^4$ is unknown, and ω is denoted by $\omega \triangleq (1, \|\bar{\mathcal{X}}\|, \|\bar{\mathcal{X}}\|\|\hat{W}\|_F, \|\bar{\mathcal{X}}\|\|\hat{\mathcal{O}}\|_F)^{\mathrm{T}}$. Herein, denote $\hat{\alpha}$ and $\tilde{\alpha}$ as the estimation vector and error of α, respectively, and $\tilde{\alpha} = \hat{\alpha} - \alpha$.

Lemma 3 [7]: For a matrix $T > 0$, given any real scalar ϵ and a matrix Q, one has $\epsilon(Q + Q^{\mathrm{T}}) \le \epsilon^2 T + QT^{-1}Q^{\mathrm{T}}$.

III. Main Results

A. Reachability Analysis of SMS

This part is focused on a simplified SMS design first, and the reachability of the SMS is confirmed with the developed NN-based adaptive controller then. In this position, the SMS is proposed as

$$S(x_s(t)) \triangleq {B_i}^{\mathrm{T}}P_i x_s(t) = 0 \tag{11}$$

where $P_i > 0$ will be computed later.

Remark 1: In contrast to [17] and [28], a linear SMS function is designed for the CPSMSs, which is computed with the actual measurement $x_s(t)$ from the impaired sensor channel.

Theorem 1: If a NN-based SMC law is developed as

$$u(t) = -\hat{W}^{\mathrm{T}}\varphi\left(\hat{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}}\right) - \mathcal{F}_i(t) \tag{12}$$

where $\mathcal{F}_i(t) = ({B_i}^{\mathrm{T}}P_iB_i)^{-1}[\overline{\zeta}\Upsilon(\hat{\alpha}^{\mathrm{T}}\omega + \hat{\beta}(t) + \sigma) + \|{B_i}^{\mathrm{T}}P_i\|(\|A_i\| + \|D_i\|\|E_i\|)\|x_s(t)\|]\mathrm{sgn}(S(x_s(t)))$, and the adaptive rules are shown by

$$\dot{\hat{\mathcal{W}}} = \begin{cases} {\hbar_1}^{-1}\underline{\zeta}\left(\hat{\varphi} - \hat{\varphi}'\hat{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}}\right)S^{\mathrm{T}}(x_s(t))\left({B_i}^{\mathrm{T}}P_iB_i\right), & \text{if } \Lambda_i > 0 \\ 0, & \text{if } \Lambda_i = 0 \\ {\hbar_1}^{-1}\overline{\zeta}\left(\hat{\varphi} - \hat{\varphi}'\hat{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}}\right)S^{\mathrm{T}}(x_s(t))\left({B_i}^{\mathrm{T}}P_iB_i\right), & \text{if } \Lambda_i < 0 \end{cases}$$

$$\dot{\hat{\mathcal{O}}} = \begin{cases} {\hbar_2}^{-1}\underline{\zeta}(\bar{\mathcal{X}}S^{\mathrm{T}}(x_s(t))\left({B_i}^{\mathrm{T}}P_iB_i\right)\hat{\mathcal{W}}^{\mathrm{T}}\hat{\varphi}'), & \text{if } \Lambda_i > 0 \\ 0, & \text{if } \Lambda_i = 0 \\ {\hbar_2}^{-1}\overline{\zeta}(\bar{\mathcal{X}}S^{\mathrm{T}}(x_s(t))\left({B_i}^{\mathrm{T}}P_iB_i\right)\hat{\mathcal{W}}^{\mathrm{T}}\hat{\varphi}'), & \text{if } \Lambda_i > 0 \end{cases}$$

$\dot{\hat{\alpha}} = {\hbar_3}^{-1}\overline{\zeta}\Upsilon\|S(x_s(t))\|\omega$; $\dot{\hat{\beta}}(t) = {\hbar_4}^{-1}\overline{\zeta}\Upsilon\|S(x_s(t))\|$, where $\Lambda_i = S^{\mathrm{T}}(x_s(t))({B_i}^{\mathrm{T}}P_iB_i)(\hat{W}^{\mathrm{T}}\hat{\varphi}'\tilde{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}} + \tilde{W}^{\mathrm{T}}(\hat{\varphi} - \hat{\varphi}'\hat{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}}))$, $\Upsilon = \max_{i\in\mathcal{J}}\|({B_i}^{\mathrm{T}}P_iB_i)\|$, $\hbar_1$, $\hbar_2$, $\hbar_3$ and $\hbar_4$ represent the coefficients of the adaptive rules, $\hat{\beta}(0) \ge 0$ denotes the initial condition of $\hat{\beta}(t)$ by the designer, σ is a positive constant, $\overline{\zeta} \triangleq \max\left(1/(1-q(t))\right)$, $\underline{\zeta} \triangleq \min\left(1/(1-q(t))\right)$, and $q(t) = p(t)/(p(t)+1)$, then the finite-time reachability of the proposed SMS can be guaranteed almost surely.

Proof:

Step 1: The following Lyapunov function is constructed as:

$$\begin{aligned}\mathcal{V}_1(S(x_s(t)),i) &= \frac{1}{2}S^{\mathrm{T}}(x_s(t))S(x_s(t)) \\ &\quad + \frac{1}{2}\mathrm{tr}\{\tilde{W}^{\mathrm{T}}\hbar_1\tilde{W}\} + \frac{1}{2}\mathrm{tr}\{\tilde{\mathcal{O}}^{\mathrm{T}}\hbar_2\tilde{\mathcal{O}}\} + \frac{1}{2}\tilde{\alpha}^{\mathrm{T}}\hbar_3\tilde{\alpha}.\end{aligned} \tag{13}$$

Note that the weight function $q(t)$ is provided as $q(t) = p(t)/(p(t)+1)$. Then, the SMS function can be rewritten as

$$S(x_s(t)) = {B_i}^{\mathrm{T}}P_i x_s(t) = \frac{S(x(t))}{1-q(t)} \tag{14}$$

in which $S(x(t)) \triangleq B_i^{\mathrm{T}} P_i x(t)$. Thus, the following can be derived:

$$\dot{S}(x_s(t)) = B_i^{\mathrm{T}} P_i [\frac{\dot{x}(t)}{1-q(t)} - \frac{(1-\dot{q}(t))x(t)}{(1-q(t))^2}]. \tag{15}$$

Then, the infinitesimal operator $\mathcal{L}$ on $\mathcal{V}_1(S(x_s(t)), i)$ yields

$$\mathcal{L}\mathcal{V}_1(S(x_s(t)\ ), i) = \mathcal{R}_{1,i} + \mathcal{R}_{2,i} \tag{16}$$

where $\mathcal{R}_{1,i} = (1/(1-q(t)))S^{\mathrm{T}}(x_s(t))B_i^{\mathrm{T}}P_i\dot{x}(t) + \mathrm{tr}\{\tilde{W}^{\mathrm{T}}\hbar_1\dot{\tilde{W}}\} + \mathrm{tr}\{\tilde{\mathcal{O}}^{\mathrm{T}}\hbar_2\dot{\tilde{\mathcal{O}}}\} + \tilde{\alpha}^{\mathrm{T}}\hbar_3\dot{\tilde{\alpha}}$, $\mathcal{R}_{2,i} = -((1-\dot{q}(t))/((1-q(t))^2))S^{\mathrm{T}}(x_s(t))B_i^{\mathrm{T}}P_i x(t)$. Further, $\mathcal{R}_{1,i}$ is converted into

$$\begin{aligned}\mathcal{R}_{1,i} = &\frac{S^{\mathrm{T}}(x_s(t))}{1-q(t)}B_i^{\mathrm{T}}P_i(A_i + \Delta A_i(t))x(t)\\ &+ \frac{S^{\mathrm{T}}(x_s(t))}{1-q(t)}(B_i^{\mathrm{T}}P_iB_i)(u(t) + \partial_a(x_s(t), t))\\ &+ \mathrm{tr}\{\tilde{W}^{\mathrm{T}}\hbar_1\dot{\tilde{W}}\} + \mathrm{tr}\{\tilde{\mathcal{O}}^{\mathrm{T}}\hbar_2\dot{\tilde{\mathcal{O}}}\} + \tilde{\alpha}^{\mathrm{T}}\hbar_3\dot{\tilde{\alpha}}.\end{aligned} \tag{17}$$

Substituting (12) into (17), it yields

$$\begin{aligned}\mathcal{R}_{1,i} \le &\frac{S^{\mathrm{T}}(x_s(t))}{1-q(t)}B_i^{\mathrm{T}}P_i(A_i. + \Delta A_i(t))x(t)\\ &+ \frac{S^{\mathrm{T}}(x_s(t))}{1-q(t)}(B_i^{\mathrm{T}}P_iB_i)(\partial_a(x_s(t), t)\\ &- \hat{W}^{\mathrm{T}}\varphi(\hat{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}}) - \mathcal{F}_i(t)) + \mathrm{tr}\{\tilde{W}^{\mathrm{T}}\hbar_1\dot{\tilde{W}}\}\\ &+ \mathrm{tr}\{\tilde{\mathcal{O}}^{\mathrm{T}}\hbar_2\dot{\tilde{\mathcal{O}}}\} + \tilde{\alpha}^{\mathrm{T}}\hbar_3\dot{\tilde{\alpha}}.\end{aligned} \tag{18}$$

Considering the actuator attack in (8) and Lemma 1, (18) can be derived as

$$\begin{aligned}\mathcal{R}_{1,i} \le &\frac{S^{\mathrm{T}}(x_s(t))}{1-q(t)}B_i^{\mathrm{T}}P_i(A_i + \Delta A_i(t))x(t)\\ &+ \frac{S^{\mathrm{T}}(x_s(t))}{1-q(t)}(B_i^{\mathrm{T}}P_iB_i)(-\nu(x_s(t))\\ &- \tilde{W}^{\mathrm{T}}(\hat{\varphi} - \hat{\varphi}'\hat{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}}) - \hat{W}^{\mathrm{T}}\hat{\varphi}'\tilde{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}} - \mathcal{F}_i(t))\\ &+ \mathrm{tr}\{\tilde{W}^{\mathrm{T}}\hbar_1\dot{\tilde{W}}\} + \mathrm{tr}\{\tilde{\mathcal{O}}^{\mathrm{T}}\hbar_2\dot{\tilde{\mathcal{O}}}\} + \tilde{\alpha}^{\mathrm{T}}\hbar_3\dot{\tilde{\alpha}}.\end{aligned} \tag{19}$$

Noting that all variables have finite dimensions, $x_s(t) = x(t)/(1-q(t))$ and $\|\cdot\| \le \|\cdot\|_1$, (19) is further shown as

$$\begin{aligned}\mathcal{R}_{1,i} \le\ & S(x_s(t))B_i^{\mathrm{T}}P_i(A_i + \Delta A_i(t))x_s(t)\\ &- \|S(x_s(t))\|_1\|B_i^{\mathrm{T}}P_i\|(\|A_i\| + \|D_i\|\|E_i\|)\|x_s(t)\|\\ &+ \bar{\zeta}\Upsilon\|S(x_s(t))\|\|B_i^{\mathrm{T}}P_iB_i\|\alpha^{\mathrm{T}}\omega - \frac{\Lambda_i}{1-q(t)}\\ &- \bar{\zeta}\Upsilon\|S(x_s(t))\|_1(\sigma + \hat{\beta}(t) + \hat{\alpha}^{\mathrm{T}}\omega)\\ &+ \mathrm{tr}\{\tilde{W}^{\mathrm{T}}\hbar_1\dot{\tilde{W}}\} + \mathrm{tr}\{\tilde{\mathcal{O}}^{\mathrm{T}}\hbar_2\dot{\tilde{\mathcal{O}}}\} + \tilde{\alpha}^{\mathrm{T}}\hbar_3\dot{\tilde{\alpha}}\\ \le\ & S(x_s(t))B_i^{\mathrm{T}}P_i(A_i + \Delta A_i(t))x_s(t)\\ &- \|S(x_s(t))\|\|B_i^{\mathrm{T}}P_i\|(\|A_i\| + \|D_i\|\|E_i\|)\|x_s(t)\|\\ &+ \bar{\zeta}\|S(x_s(t))\|\|B_i^{\mathrm{T}}P_iB_i\|\alpha^{\mathrm{T}}\omega - \frac{\Lambda_i}{1-q(t)}\\ &- \bar{\zeta}\Upsilon\|S(x_s(t))\|(\hat{\alpha}^{\mathrm{T}}\omega + \hat{\beta}(t) + \sigma)\\ &+ \mathrm{tr}\{\tilde{W}^{\mathrm{T}}\hbar_1\dot{\tilde{W}}\} + \mathrm{tr}\{\tilde{\mathcal{O}}^{\mathrm{T}}\hbar_2\dot{\tilde{\mathcal{O}}}\} + \tilde{\alpha}^{\mathrm{T}}\hbar_3\dot{\tilde{\alpha}}.\end{aligned} \tag{20}$$

In view of $\dot{\hat{\beta}}(t) = \hbar_4^{-1}\bar{\zeta}\Upsilon\|S^{\mathrm{T}}(x_s(t))\| \ge 0$ and $\dot{\hat{\beta}}(0) \ge 0$, one also gives

$$\begin{aligned}\mathcal{R}_{1,i} \le\ & S(x_s(t))B_i^{\mathrm{T}}P_i(A_i + \Delta A_i(t))x_s(t)\\ &- \|S(x_s(t))\|\|B_i^{\mathrm{T}}P_i\|(\|A_i\| + \|D_i\|\|E_i\|)\|x_s(t)\|\\ &+ \bar{\zeta}\Upsilon\|S(x_s(t))\|\alpha^{\mathrm{T}}\omega - \frac{\Lambda_i}{1-q(t)}\\ &- \bar{\zeta}\Upsilon\|S(x_s(t))\|(\hat{\alpha}^{\mathrm{T}}\omega + \sigma)\\ &+ \mathrm{tr}\Big\{\tilde{W}^{\mathrm{T}}\hbar_1\dot{\tilde{W}}\Big\} + \mathrm{tr}\Big\{\tilde{\mathcal{O}}^{\mathrm{T}}\hbar_2\dot{\tilde{\mathcal{O}}}\Big\} + \tilde{\alpha}^{\mathrm{T}}\hbar_3\dot{\tilde{\alpha}}\\ \le\ & \bar{\zeta}\Upsilon\|S(x_s(t))\|\alpha^{\mathrm{T}}\omega - \frac{\Lambda_i}{1-q(t)}\\ &- \bar{\zeta}\Upsilon\|S(x(t))\|(\hat{\alpha}^{\mathrm{T}}\omega + \sigma) + \tilde{\alpha}^{\mathrm{T}}\hbar_3\dot{\tilde{\alpha}}\\ &+ \mathrm{tr}\Big\{\tilde{W}^{\mathrm{T}}\hbar_1\dot{\tilde{W}}\Big\} + \mathrm{tr}\Big\{\tilde{\mathcal{O}}^{\mathrm{T}}\hbar_2\dot{\tilde{\mathcal{O}}}\Big\}.\end{aligned} \tag{21}$$

In the position, for the case $\Lambda_i > 0$, it follows that:

$$\begin{aligned}\mathcal{R}_{1,i} \le\ & \bar{\zeta}\Upsilon\|S(x_s(t))\|(\alpha^{\mathrm{T}}\omega - \hat{\alpha}^{\mathrm{T}}\omega) - \bar{\zeta}\Upsilon\|S(x_s(t))\|\sigma\\ &- \zeta\Lambda_i + \mathrm{tr}\Big\{\tilde{W}^{\mathrm{T}}\hbar_1\dot{\tilde{W}}\Big\} + \mathrm{tr}\Big\{\tilde{\mathcal{O}}^{\mathrm{T}}\hbar_2\dot{\tilde{\mathcal{O}}}\Big\} + \tilde{\alpha}^{\mathrm{T}}\hbar_3\dot{\tilde{\alpha}}\\ \le\ & \bar{\zeta}\Upsilon\|S(x_s(t))\|\big(\alpha^{\mathrm{T}}\omega - \hat{\alpha}^{\mathrm{T}}\omega\big)\\ &- \bar{\zeta}\Upsilon\|S(x_s(t))\|\sigma + \tilde{\alpha}^{\mathrm{T}}\hbar_3\dot{\tilde{\alpha}}\\ =\ & -\delta_1\|S(x_s(t))\| < 0\end{aligned} \tag{22}$$

where $\delta_1 = -\bar{\zeta}\sigma\Upsilon$. Then, for the case that Λ_i is less than 0, the following inequality can be obtained:

$$\begin{aligned}\mathcal{R}_{1,i} \le\ & \bar{\zeta}\Upsilon\|S(x_s(t))\|(\alpha^{\mathrm{T}}\omega - \hat{\alpha}^{\mathrm{T}}\omega) - \bar{\zeta}\Lambda_i\\ &- \bar{\zeta}\Upsilon\|S(x_s(t))\|\sigma + \mathrm{tr}\Big\{\tilde{W}^{\mathrm{T}}\hbar_1\dot{\tilde{W}}\Big\}\\ &+ \mathrm{tr}\Big\{\tilde{\mathcal{O}}^{\mathrm{T}}\hbar_2\dot{\tilde{\mathcal{O}}}\Big\} + \tilde{\alpha}^{\mathrm{T}}\hbar_3\dot{\tilde{\alpha}}\\ \le\ & \bar{\zeta}\Upsilon\|S(x_s(t))\|\big(\alpha^{\mathrm{T}}\omega - \hat{\alpha}^{\mathrm{T}}\omega\big)\\ &- \bar{\zeta}\Upsilon\|S(x_s(t))\|\sigma + \tilde{\alpha}^{\mathrm{T}}\hbar_3\dot{\tilde{\alpha}}\\ =\ & -\delta_1\|S(x_s(t))\| < 0.\end{aligned} \tag{23}$$

In like manner, if $\Lambda_i = 0$, then the inequality $\mathcal{R}_{1,i} \le -\delta_1\|S(x_s(t))\| < 0$ still holds. Moreover, $\mathcal{R}_{2,i}$ can be calculated as

$$\mathcal{R}_{2,i} \le -\frac{1-\dot{q}(t)}{(1-q(t))^2}\|S(x_s(t))\|^2 < 0. \tag{24}$$

From the above discussion, we have $\mathcal{L}\mathcal{V}_1(S(x_s(t)), i) < 0$. Then, it can be obtained that $S(x_s(t))$, $\tilde{\mathcal{W}}$, $\tilde{\mathcal{O}}$ and $\tilde{\alpha}$ are bounded, which gives the boundedness of $\tilde{\partial}_a(x_s(t), t)$ further, i.e., $\|\tilde{\partial}_a(x_s(t), t)\| \le \beta$, where $\beta > 0$ is an unknown scalar, and its estimation is defined by $\hat{\beta}(t)$.

Step 2: The arrival of the SMS can be justified further with a selected Lyapunov function as follows:

$$\mathcal{V}_2(S(x_s(t)), i) = \frac{1}{2}S^{\mathrm{T}}(x_s(t))S(x_s(t)) + \frac{\hbar_4}{2}\tilde{\beta}^2(t) \tag{25}$$

in which $\tilde{\beta}(t) = \hat{\beta}(t) - \beta$. The infinitesimal operator $\mathcal{L}\mathcal{V}_2(S(x_s(t)), i)$ can be redefined as

$$\mathcal{L}\mathcal{V}_2(S(x_s(t)), i) = \mathcal{R}_{3,i} \tag{26}$$

where $\mathcal{R}_{3,i} = S^{\mathrm{T}}(x_s(t))B_i^{\mathrm{T}}P_i[\dot{x}(t)/1-q(t)] + \hbar_4\tilde{\beta}(t)\dot{\tilde{\beta}}(t)$. Substituting (12) into (26), one has

$$\mathcal{R}_{3,i} \le \frac{S^{\mathrm{T}}(x_s(t))}{1-q(t)}B_i^{\mathrm{T}}P_i(A_i + \Delta A_i(t))x(t)$$

$$
\begin{aligned}
&+\frac{S^{\mathrm{T}}(x_s(t))}{1-q(t)}\big(B_i{}^{\mathrm{T}}P_iB_i\big)\big(\partial_a(x_s(t),t)\\
&-\hat{W}^{\mathrm{T}}\varphi\big(\hat{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}}\big)-\mathcal{F}_i(t)\big)+\hbar_4\tilde{\beta}(t)\dot{\tilde{\beta}}(t)\\
\le&\frac{S^{\mathrm{T}}(x_s(t))}{1-q(t)}B_i{}^{\mathrm{T}}P_i(A_i+\Delta A_i(t))x(t)\\
&+\frac{S^{\mathrm{T}}(x_s(t))}{1-q(t)}\big(B_i{}^{\mathrm{T}}P_iB_i\big)\big(-\tilde{\partial}_a(x_s(t),t)\\
&-\mathcal{F}_i(t)\big)+\hbar_4\tilde{\beta}(t)\dot{\tilde{\beta}}(t)
\end{aligned}
\tag{27}
$$

Meanwhile, in view of $\|\cdot\|\le\|\cdot\|_1$, one has

$$
\begin{aligned}
\mathcal{R}_{3,i}\le&\|S(x(t))\|\big\|B_i{}^{\mathrm{T}}P_i(A_i+\Delta A_i(t))\big\|\|x_s(t)\|\\
&-\|S(x_s(t))\|\|B_i{}^{\mathrm{T}}P_i\|(\|A_i\|+\|D_i\|\|E_i\|)\\
&\cdot\|x_s(t)\|-\bar{\zeta}\Upsilon\|S(x_s(t))\|(\hat{\alpha}^{\mathrm{T}}\omega+\hat{\beta}(t)+\sigma)\\
&+\bar{\zeta}\Upsilon\|S(x_s(t))\|\big\|\tilde{\partial}_a(x_s(t),t)\big\|+\hbar_4\tilde{\beta}(t)\dot{\tilde{\beta}}(t)\\
\le&-\bar{\zeta}\Upsilon\|S(x_s(t))\|(\hat{\alpha}^{\mathrm{T}}\omega+\sigma).
\end{aligned}
\tag{28}
$$

It is noteworthy that, based upon the adaptive rule $\dot{\hat{\alpha}}$, there exists an instant $T^*>0$ such that $\hat{\alpha}^{\mathrm{T}}\omega>0$ for $t\ge T^*$. Then, it further follows:

$$
\mathcal{R}_{3,i}\le-\delta_1\|S(x_s(t))\|<0,\ \text{ for } t\ge T^*. \tag{29}
$$

Moreover, introduce the function $\mathcal{V}_3(S(x_s(t)),i)=[1/2]S^{\mathrm{T}}(x_s(t))S(x_s(t))$. Considering the case that $\tilde{\beta}(t)=\hat{\beta}(t)>0$, there exists a finite instant $T'>0$ such that $\hbar_4\tilde{\beta}(t)\dot{\tilde{\beta}}(t)\ge0$ for $t\ge T_f=\max\{T^*,T'\}$. In view of (29), one can get

$$
\mathcal{L}\mathcal{V}_3(S(x_s(t)),i)\le-\delta_1\|S(x_s(t))\|<0\ \forall t\ge T_f. \tag{30}
$$

Further, one has

$$
\mathcal{L}\mathcal{V}_3(S(x_s(t)),i)\le-\zeta\sqrt{\mathcal{V}_3(S(x_s(t)),i)}\forall t\ge T_f \tag{31}
$$

where $\zeta=\sqrt{2}\delta_1$. By Itô's formula, it yields

$$
\mathcal{L}\|S(x_s(t))\|=\mathcal{L}\sqrt{\mathcal{V}_3(S(x_s(t)),i)}\le-\zeta/2 \tag{32}
$$

and hence

$$
\mathbb{E}\|S(x_s(t))\|\le\mathbb{E}\|S\big(x_s\big(T_f\big)\big)\|-(\zeta/2)(t-T_f) \tag{33}
$$

which concludes there exists an instant $t_f=T_f+2m_0/\zeta$ satisfying $\mathbb{E}\|S(x_s(t))\|=0$ for all $t\ge t_f$, where $m_0=\mathbb{E}\|S(x_s(T_f))\|<\infty$. Thus, the arrival of the devised SMS can be determined almost surely. ■

Remark 2: In contrast to the existing control strategy [17], [19] that guaranteed the uniform boundedness of sliding variable only, the proposed NN-based adaptive SMC design can not only satisfy the boundedness of related data but also admit the state onto the proposed SMS $S(x_s(t))=0$ in finite time almost surely.

Remark 3: Differing from the projection operator approach to handle the attack signals in [29], the NN-based control method is introduced herein. It is worth mentioning that the norm-bounded assumption is not required in this work, which indicates the control design in (12) generalizes the result proposed in [29].

B. Performance Analysis

In this part, a new stochastically stable criterion of the resultant CPSMSs subject to GUTRs on the sliding motion is put forward.

Theorem 2: The system (6) is stochastically stable during the sliding phase if there exist matrices $P_i>0$, $\mathcal{U}_{g,i}>0$, $\mathcal{V}_{g,i}>0$, $\mathcal{W}_i>0$ and $\mathcal{X}_{i,j_\alpha}>0$, K_i and a positive scalar ι such that the conditions in the following are held.

Case 1: $i\in\Omega_k{}^i$ and $g\in\Omega_{uk}{}^i$

$$
\begin{bmatrix}\Xi_{i,1}+\Xi_1 & (P_iD_i)^{\mathrm{T}} & \psi_1\\ * & -\iota I & 0\\ * & * & -\mathcal{U}_{g,i}\end{bmatrix}<0. \tag{34}
$$

Case 2: $i\in\Omega_{uk}^i$, $g\in\Omega_{uk}{}^i$ and $\Omega_k^i\neq\oslash$

$$
\begin{cases}\begin{bmatrix}\Xi_{i,2}+\Xi_2 & (P_iD_i)^{\mathrm{T}} & \psi_2\\ * & -\iota I & 0\\ * & * & -\mathcal{V}_{g,i}\end{bmatrix}<0\\ P_i-P_j\ge0.\end{cases} \tag{35}
$$

Case 3: $\Omega_{uk}{}^i=\mathcal{J}$, $g\in\Omega_{uk}{}^i$ and $j\in\Omega_k{}^j$ for some $j\neq i$

$$
\begin{bmatrix}\Xi_{i,3}+\Xi_3 & (P_iD_i)^{\mathrm{T}} & P_i-P_g\\ * & -\iota I & 0\\ * & * & -\mathcal{W}_i\end{bmatrix}<0. \tag{36}
$$

Case 4: $\Omega_{uk}{}^i=\mathcal{J}$, $g\in\Omega_{uk}{}^i$ and $j\notin\Omega_k{}^j$ for any $j\in\mathcal{J}$

$$
\begin{cases}\begin{bmatrix}\Xi_{i,4}+\Xi_4 & (P_iD_i)^{\mathrm{T}} & P_{j_\alpha}-P_j\\ * & -\iota I & 0\\ * & * & -\mathcal{X}_{i,j_\alpha}\end{bmatrix}<0\\ P_i-P_j\ge0.\end{cases} \tag{37}
$$

where the matrix K_i is set for $A_i-B_iK_i$ is Hurwitz, and

$$
\begin{aligned}
\Xi_{i,\varpi}&=\mathrm{sym}\{P_i(A_i-B_iK_i)\}+\iota E_i{}^{\mathrm{T}}E_i,\ \varpi\in\{1,2,3,4\}\\
\Xi_1&=\sum_{j\in\Omega_k^i}\Big[\hat{\eta}_{ij}\big(P_j-P_g\big)+\frac{1}{4}\big(\vartheta_{ij}\big)^2\mathcal{U}_{g,i}\Big]\\
\Xi_2&=\sum_{j\in\Omega_k^i}\Big[\hat{\eta}_{ij}\big(P_j-P_g\big)+\frac{1}{4}\big(\vartheta_{ij}\big)^2\mathcal{V}_{g,i}\Big]\\
\Xi_3&=\alpha_i\hat{\eta}_{jj}\big(P_i-P_g\big)+\frac{1}{4}\big(\vartheta_{jj}\big)^2\mathcal{W}_i,\\
\Xi_4&=\hat{\eta}_{jj_\alpha}\big(P_{j_\alpha}-P_g\big)+\frac{1}{4}\big(\vartheta_{jj_\alpha}\big)^2\mathcal{X}_{i,j_\alpha}\\
\psi_1&=\big[\big(P_{j,1}-P_g\big),\big(P_{j,2}-P_g\big),\ldots,\big(P_{j_1}-P_g\big)\big]\\
\psi_2&=\big[\big(P_{j,1}-P_g\big),\big(P_{j,2}-P_g\big),\ldots,\big(P_{j_2}-P_g\big)\big].
\end{aligned}
$$

Proof: The Lyapunov function candidate is selected as

$$
\mathcal{V}_4(x,i)=x^{\mathrm{T}}(t)P_ix(t). \tag{38}
$$

The infinitesimal generator of $\mathcal{V}_4(x,i)$ along system (6) gives

$$
\begin{aligned}
\mathcal{L}\mathcal{V}_4(x,i)&=2x^{\mathrm{T}}(t)P_i\dot{x}(t)+\sum_{j=1}^{J}\eta_{ij}x^{\mathrm{T}}(t)P_jx(t)\\
&=x^{\mathrm{T}}(t)\cdot\mathrm{sym}\{P_i(A_i-B_iK_i)\}x(t)\\
&\quad+2x^{\mathrm{T}}(t)P_i\Delta A_ix(t)+2x^{\mathrm{T}}(t)P_iB_i\\
&\quad\cdot\big(u_a(t)+K_ix(t)\big)+\sum_{j=1}^{J}\eta_{ij}x^{\mathrm{T}}(t)P_jx(t).
\end{aligned}
$$

Besides, the following inequality is held:

$$2x^{\mathrm{T}}(t)P_i\Delta A_i x(t) \le \iota^{-1}x^{\mathrm{T}}(t)P_iD_iD_i{}^{\mathrm{T}}P_ix(t) + \iota x^{\mathrm{T}}(t)E_i{}^{\mathrm{T}}E_ix(t) \tag{39}$$

for a positive scalar ι. By taking reachability of the SMS into account, we get $S^{\mathrm{T}}(x_s(t)) = x^{\mathrm{T}}(t)P_iB_i/(1-q(t)) = 0$, yielding $x^{\mathrm{T}}(t)P_iB_i = 0$. Thus, it follows that:

$$\mathcal{L}\mathcal{V}_4(x,i) \le x^{\mathrm{T}}(t)\mathcal{H}_ix(t) \tag{40}$$

where $\mathcal{H}_i = \mathrm{sym}\{P_i(A_i - B_iK_i)\} + \iota^{-1}P_iD_iD_i^{\mathrm{T}}P_i + \iota E_i{}^{\mathrm{T}}E_i + \sum_{j=1}^{J}\eta_{ij}P_j$.

Case 1 ($i \in \Omega_k{}^i$): Denote $\lambda_{i,k} \triangleq \sum_{i\in\Omega_k^i}\eta_{ij}$. Due to $\Omega_k^i \neq \oslash$, it gives $\lambda_{i,k} < 0$. Note that $\sum_{j=1}^{J}\eta_{ij}P_j$ could be expressed as

$$\begin{aligned}\sum_{j=1}^{J}\eta_{ij}P_j &= \Big(\sum_{j\in\Omega_k{}^i} + \sum_{j\in\Omega_{uk}{}^i}\Big)\eta_{ij}P_j \\ &= \sum_{j\in\Omega_k{}^i}\eta_{ij}P_j - \lambda_{i,k}\sum_{j\in\Omega_{uk}{}^i}\frac{\eta_{ij}}{-\lambda_{i,k}}P_j\end{aligned} \tag{41}$$

in which $\sum_{j\in\Omega_{uk}{}^i}(\eta_{ij}/-\lambda_{i,k}) = 1$ and $0 < (\eta_{ij}/-\lambda_{i,k}) < 1, j \in \Omega_{uk}{}^i$. Hence, for any $g \in \Omega_{uk}{}^i$, one also gives

$$\begin{aligned}&\Xi_{i,1} + \sum_{j\in\Omega_k^i}\eta_{ij}\big(P_j - P_g\big) \\ &= \sum_{g\in\Omega_{uk}^i}\frac{\eta_{ij}}{-\lambda_{i,k}}\Big[\Xi_{i,1} + \sum_{j\in\Omega_k^i}\eta_{ij}\big(P_j - P_g\big)\Big].\end{aligned} \tag{42}$$

Evidently, one has

$$\begin{aligned}&\sum_{j\in\Omega_k^i}\eta_{ij}\big(P_j - P_g\big) \\ &= \sum_{j\in\Omega_k^i}\hat{\eta}_{ij}\big(P_j - P_g\big) + \sum_{j\in\Omega_k^i}\Delta\eta_{ij}\big(P_j - P_g\big).\end{aligned} \tag{43}$$

In addition, for any $\mathcal{U}_{g,i} > 0$, it yields by Lemma 3 that

$$\begin{aligned}&\sum_{j\in\Omega_k^i}\Delta\eta_{ij}\big(P_j - P_g\big) \\ &= \sum_{j\in\Omega_k^i}\Big[\frac{1}{2}\Delta\eta_{ij}\big(\big(P_j - P_g\big) + \big(P_j - P_g\big)\big)\Big] \\ &\le \sum_{j\in\Omega_k^i}\Big[\frac{1}{4}\big(\vartheta_{ij}\big)^2\mathcal{U}_{g,i} + \big(P_j - P_g\big)\mathcal{U}_{g,i}{}^{-1}\big(P_j - P_g\big)^{\mathrm{T}}\Big].\end{aligned} \tag{44}$$

Via Schur complement and (34), it gives $\mathcal{L}\mathcal{V}_4(x,i) < 0$, which shows system (6) during the sliding motion is stochastically stable.

Case 2 ($i \in \Omega_{uk}^i$ and $\Omega_k^i \neq \oslash$): Denote $\lambda_{i,k} \triangleq \sum_{j\in\Omega_k^i}\eta_{ij}$. Since $\Omega_{uk}^i \neq \oslash$, one has $\lambda_{i,k} > 0$ and

$$\begin{aligned}&\sum_{j=1}^{J}\eta_{ij}P_j \\ &= \sum_{j\in\Omega_k^i}\eta_{ij}P_j + \eta_{ii}P_i + \sum_{j\in\Omega_{uk}^i}\eta_{ij}P_j \\ &= \sum_{j\in\Omega_k^i}\eta_{ij}P_j + \eta_{ii}P_i - \big(\eta_{ii} + \lambda_{i,k}\big)\sum_{j\in\Omega_{uk}^i,j\neq i}\frac{\eta_{ij}}{-\eta_{ii} - \lambda_{i,k}}P_j\end{aligned} \tag{45}$$

where $\sum_{j\in\Omega_{uk}^i,j\neq i}(\eta_{ij}/-\eta_{ii} - \lambda_{i,k}) = 1$, $0 \le \eta_{ij}/(-\eta_{ii} - \lambda_{i,k}) \le 1$ and $g \in \Omega_{uk}^i$. For any $j \in \Omega_{uk}^i$, one gives

$$\begin{aligned}&\Xi_{i,2} + \sum_{j=1}^{J}\eta_{ij}P_j \\ &= \sum_{g\in\Omega_{uk}^i,j\neq i}\frac{\eta_{ij}}{-\eta_{ii} - \lambda_{i,k}}[\Xi_{i,2} + \mathrm{diag}\{\eta_{ii}\big(P_i - P_g\big) \\ &+ \sum_{j\in\Omega_k^i}\eta_{ij}\big(P_j - P_g\big), \eta_{ii}\big(P_i - P_g\big) + \sum_{j\in\Omega_k^i}\eta_{ij}\big(P_j - P_g\big)\}].\end{aligned} \tag{46}$$

Since $0 \le \eta_{ij} \le -\eta_{ii} - \lambda_{i,k}$, the inequality $\Xi_{i,2} + \sum_{j=1}^{J}\eta_{ij}P_j < 0$ is equivalent to

$$\Xi_{i,2} + \eta_{ii}\big(P_i - P_g\big) + \sum_{j\in\Omega_k^i}\eta_{ij}\big(P_j - P_g\big) < 0. \tag{47}$$

From $\eta_{ii} < 0$, (47) holds if

$$\begin{cases} P_i - P_g \ge 0, \\ \Xi_{i,2} + \sum_{j\in\Omega_k^i}\eta_{ij}\big(P_j - P_g\big) < 0. \end{cases} \tag{48}$$

Moreover, for any $\mathcal{V}_{i,g} > 0$, by Lemma 3, one has

$$\begin{aligned}&\sum_{j\in\Omega_k^i}\eta_{ij}\big(P_j - P_g\big) \\ &= \sum_{j\in\Omega_k^i}\hat{\eta}_{ij}\big(P_j - P_g\big) + \sum_{j\in\Omega_k^i}[\frac{1}{4}\big(\vartheta_{ij}\big)^2\mathcal{V}_{g,i} \\ &+ \big(P_j - P_g\big)\mathcal{V}_{g,i}{}^{-1}\big(P_j - P_g\big)^{\mathrm{T}}].\end{aligned} \tag{49}$$

Recalling the similar line and condition (35), one also has $\mathcal{L}\mathcal{V}_4(x,i) < 0$.

Case 3 ($\Omega_{uk}{}^i = \mathcal{J}$ and $j \in \Omega_k{}^j$ for Some $j \neq i$): In such case, η_{ii} is estimated by $\alpha_i\eta_{jj}$. Denote $\lambda_{i,k} \triangleq \eta_{ii}$. Therefore, $\sum_{j=1}^{J}\eta_{ij}P_j$ is changed into

$$\begin{aligned}\sum_{j=1}^{J}\eta_{ij}P_j &= \eta_{ii}P_i + \sum_{j\in\Omega_{uk}{}^i}\eta_{ij}P_j \\ &= \eta_{ii}P_i - \lambda_{i,k}\sum_{j\in\Omega_{uk}{}^i}\frac{\eta_{ij}}{-\lambda_{i,k}}P_j.\end{aligned} \tag{50}$$

Since $\sum_{j\in\Omega_{uk}{}^i}\eta_{ij} = -\eta_{ii} = -\lambda_{i,k} > 0$, it follows that for $\forall g \in \Omega_{uk}{}^i$

$$\begin{aligned}&\Xi_{i,3} + \sum_{j=1}^{J}\eta_{ij}P_j \\ &= \sum_{g\in\Omega_{uk}{}^i}\frac{\eta_{ig}}{-\lambda_{i,k}}\big[\Xi_{i,3} + \eta_{ii}\big(P_i - P_g\big)\big] \\ &= \Xi_{i,3} + \eta_{ii}\big(P_i - P_g\big) = \Xi_{i,3} + \alpha_i\eta_{jj}\big(P_i - P_g\big).\end{aligned} \tag{51}$$

Further, by recalling $\eta_{ij} = \hat{\eta}_{ij} + \Delta\eta_{ij}$, one has

$$\alpha_i\eta_{jj}\big(P_i - P_g\big) = \alpha_i\big(\hat{\eta}_{jj} + \Delta\eta_{jj}\big)\big(P_i - P_g\big). \tag{52}$$

Then, by Lemma 3, for any $\mathcal{W}_i > 0$, one has

$$\begin{aligned}\Delta\eta_{jj}(P_i - P_g) &= \frac{1}{2}\cdot 2\Delta\eta_{jj}(P_i - P_g)\\ &\le \left[\frac{(\vartheta_{jj})^2}{4}\mathcal{W}_i + (P_i - P_g)(\mathcal{W}_i)^{-1}(P_i - P_g)^{\mathrm{T}}\right].\end{aligned} \tag{53}$$

Combining (51), (52) and (53), it also yields $\mathcal{L}\mathcal{V}_4(x,i) < 0$ by Schur complement and condition (36).

Case 4 ($\Omega_{uk}{}^i = \mathcal{J}$ and $j \notin \Omega_k{}^j$ for any $j \in \mathcal{J}$): In this case, denote $\lambda_{i,k} \triangleq \eta_{ij_a}(j_a \neq i)$, and η_{ij_a} is estimated by η_{jj_a}. Then, $\sum_{j=1}^{J}\eta_{ij}P_j$ is changed into

$$\begin{aligned}&\sum_{j=1}^{J}\eta_{ij}P_j\\ &= \eta_{ij_a}P_{j_a} + \eta_{ii}P_i + \sum_{j\in\Omega_{uk}{}^i, j\neq i}\eta_{ij}P_j\\ &= \eta_{ij_a}P_{j_a} + \eta_{ii}P_i - (\eta_{ii} + \lambda_{i,k})\sum_{j\in\Omega_{uk}{}^i, j\neq i}\frac{\eta_{ij}P_j}{-\eta_{ii} - \lambda_{i,k}}\end{aligned} \tag{54}$$

thus one has

$$\begin{aligned}&\Xi_{i,4} + \sum_{j=1}^{J}\eta_{ij}P_j\\ &= \sum_{g\in\Omega_{uk}{}^i, j\neq i}\left[\Xi_{i,4} + \eta_{ii}(P_i - P_g) + \eta_{ij_a}(P_{j_a} - P_g)\right].\end{aligned} \tag{55}$$

Since $0 \le \eta_{ij} \le -\eta_{ii} - \lambda_{i,k}$, the inequality $\Xi_{i,4} + \eta_{ii}(P_i - P_g) + \eta_{ij_a}(P_{j_a} - P_g) < 0$ is equivalent to

$$\Xi_{i,4} + \eta_{ii}(P_i - P_g) + \alpha_i\eta_{jj_a}(P_{j_a} - P_g) < 0. \tag{56}$$

Due to $\eta_{ii} < 0$, (56) < 0 holds if

$$\begin{cases} P_i - P_g \ge 0,\\ \Xi_{i,4} + \alpha_i\eta_{jj_a}(P_{j_a} - P_g) < 0.\end{cases} \tag{57}$$

Further, by Lemma 3, for any $\mathcal{X}_{ij_\alpha} > 0$, it gives

$$\begin{aligned}&\eta_{jj_a}(P_{j_a} - P_g)\\ &= \hat{\eta}_{jj_a}(P_{j_a} - P_g) + \Delta\eta_{jj_a}(P_{j_a} - P_g)\\ &\le \hat{\eta}_{jj_a}(P_{j_a} - P_g) + \left[\frac{(\vartheta_{jj_a})^2}{4}\mathcal{X}_{ij_a}\right.\\ &\quad \left. + (P_{j_a} - P_g)(\mathcal{X}_{ij_a})^{-1}(P_{j_a} - P_g)^{\mathrm{T}}\right].\end{aligned} \tag{58}$$

From the similar line and condition (37), $\mathcal{L}\mathcal{V}_4(x,i) < 0$ still holds, which implies the stochastic stability of system (6) on the sliding motion. ■

Remark 4: As seen, a novel NN-based secure controller design is developed for the underlying CPSMSs, where the control diagram against potential sensor and actuator attacks is displayed in Fig. 2, and the main components of the whole CPSMS, i.e., the physical layer, cyber layer, and control layer, are integrated, in which both the sensor and actuator attack signals described through the communication channels may endanger the system security, and the effects of the two malicious cyber attacks can be well suppressed by the current adaptive control method.

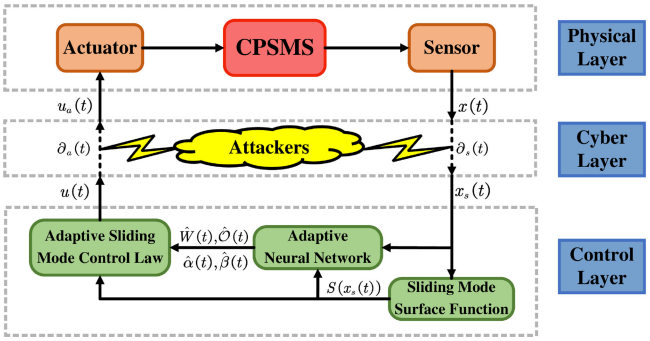

Fig. 2. Control diagram against both sensor and actuator attacks.

IV. Simulation Validation

In this section, a representative example is taken, from which the viability of the presented control method is substantiated with simulation comparisons.

Example 1: As a simulation object, the linearized F-404 aircraft engine plant model in [15] is borrowed, in which the relevant state vector with physical data is written as

$$x(t) = \begin{bmatrix}\text{sideslip angle}(^{\mathrm{o}}/\mathrm{s})\\ \text{roll rate}(^{\mathrm{o}}/\mathrm{s})\\ \text{yaw rate}(^{\mathrm{o}}/\mathrm{s})\end{bmatrix}.$$

The corresponding matrix A_i is described as

$$A_i = \begin{bmatrix}-1.46 & 0 & 2.48\\ 0.1643 + 0.5\tau_i & -0.4 + \tau_i & -0.3788\\ 0.3107 & 0 & -2.23\end{bmatrix}$$

where $\tau_i, i = 1,2,3$, are unknown parameters of the system model and set by -1, -2 and -3, respectively, then it follows:

$$A_1 = \begin{bmatrix}-1.46 & 0 & 2.428\\ -0.3357 & -1.4 & -0.3788\\ 0.3107 & 0 & -2.23\end{bmatrix}, B_1 = \begin{bmatrix}-0.1\\ 0.2\\ -0.2\end{bmatrix},$$

$$A_2 = \begin{bmatrix}-1.46 & 0 & 2.428\\ -0.8357 & -2.4 & -0.3788\\ 0.3107 & 0 & -2.23\end{bmatrix}, B_2 = \begin{bmatrix}-0.2\\ 0.1\\ -0.1\end{bmatrix},$$

$$A_3 = \begin{bmatrix}-1.46 & 0 & 2.428\\ -1.3357 & -3.4 & -0.3788\\ 0.3107 & 0 & -2.23\end{bmatrix}, B_3 = \begin{bmatrix}-0.2\\ 0.1\\ -0.2\end{bmatrix};$$

$$D_1 = \begin{bmatrix}0.2 & 0.2 & 0.1\\ 0 & 0.2 & 0\\ 0 & 0.2 & 0.1\end{bmatrix}, E_1 = \begin{bmatrix}0.2 & 0.3 & 0.1\\ 0 & 0.2 & 0.1\\ 0 & 0.3 & 0.3\end{bmatrix},$$

$$D_2 = \begin{bmatrix}0.2 & 0.1 & 0.1\\ 0.1 & 0.2 & 0.1\\ 0.1 & 0.2 & 0.1\end{bmatrix}, E_2 = \begin{bmatrix}0.1 & 0.2 & 0.2\\ 0 & 0.2 & 0.2\\ 0.1 & 0.2 & 0.3\end{bmatrix},$$

$$D_3 = \begin{bmatrix}0.1 & 0.2 & 0\\ 0.1 & 0.2 & 0\\ 0.2 & 0.2 & 0.1\end{bmatrix}, E_3 = \begin{bmatrix}0.2 & 0.2 & 0.2\\ 0 & 0.2 & 0.1\\ 0.1 & 0.2 & 0.3\end{bmatrix}.$$

The TR matrix is set as

$$\Pi = \begin{bmatrix}-0.45 + \Delta\eta_{11} & ? & 0.27 + \Delta\eta_{13}\\ ? & ? & 0.38 + \Delta\eta_{23}\\ ? & ? & ?\end{bmatrix}$$

where "?" indicates the totally unavailable TRs. The parametric matrices K_1, K_2 and K_3 are chosen as

$$K_1 = \begin{bmatrix} -0.8234 & 8.6907 & -0.4476 \end{bmatrix}$$
$$K_2 = \begin{bmatrix} -0.4853 & 1.4484 & 7.1411 \end{bmatrix}$$
$$K_3 = \begin{bmatrix} -1.2797 & -0.3621 & -3.2277 \end{bmatrix}$$

and ΔY is taken as $\Delta Y = 0.3\cos(100t)$. From Theorem 2, the feasible parameters are obtained as follows:

$$P_1 = \begin{bmatrix} 16.3642 & 4.2610 & 6.6614 \\ 4.2610 & 18.2106 & 8.0298 \\ 6.6614 & 8.0298 & 22.4143 \end{bmatrix}$$
$$P_2 = \begin{bmatrix} 10.4125 & 3.1423 & 6.7523 \\ 3.1423 & 14.0692 & 3.3443 \\ 6.7523 & 3.3443 & 22.4143 \end{bmatrix}$$
$$P_3 = \begin{bmatrix} 15.5899 & 0.1647 & 4.9571 \\ 0.1647 & 12.3043 & 1.5121 \\ 4.9571 & 1.5121 & 18.4719 \end{bmatrix}.$$

Then, the established sliding surface function is shown by

$$S(x_s(t)) = \begin{cases} [-2.1165, 1.6101, -3.5430]x_s(t), & i = 1 \\ [-2.4435, 0.4440, -4.2573]x_s(t), & i = 2 \\ [-4.0929, 0.8951, -4.5346]x_s(t), & i = 3 \end{cases}$$

and the related SMC law is designed as

$$u(t) = \begin{cases} -\hat{W}^{\mathrm{T}}\varphi(\hat{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}}) - 0.8050[1.0429(\hat{\alpha}^{\mathrm{T}}\omega + \hat{\beta}(t) \\ +1) + 3.5604\|x_s(t)\|]\mathrm{sgn}(S(x_s(t))), & i = 1 \\ -\hat{W}^{\mathrm{T}}\varphi(\hat{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}}) - 1.0429[1.0429(\hat{\alpha}^{\mathrm{T}}\omega + \hat{\beta}(t) \\ +1) + 3.6651\|x_s(t)\|]\mathrm{sgn}(S(x_s(t))), & i = 2 \\ -\hat{W}^{\mathrm{T}}\varphi(\hat{\mathcal{O}}^{\mathrm{T}}\bar{\mathcal{X}}) - 0.5510[1.0429(\hat{\alpha}^{\mathrm{T}}\omega + \hat{\beta}(t) \\ +1) + 4.8566\|x_s(t)\|]\mathrm{sgn}(S(x_s(t))), & i = 3 \end{cases}$$

where the updating gains are set as $\hbar_1 = 0.2$, $\hbar_2 = 0.5$, $\hbar_3 = 0.3$ and $\hbar_4 = 0.1$. Besides, the utilized NN consists of nine neurons, where the relevant initial values of $\hat{W}$, $\hat{\mathcal{O}}$, and $\hat{\alpha}$ are set as $[0.1]_{9\times1}$, $[0.1]_{4\times9}$ and $[0.3]_{4\times1}$, respectively. In addition, the values of the learning rate and batch size of the NN are chosen as 0.1 and 4, respectively. Simulation experiments with comparisons of specified performance measures are conducted under the current method and the algorithms of [17], [28] in the following three cases.

Case 1 (Performance Comparison Under Sensor Attacks): The sensor attack denoted by $\partial_s(t) = p(t)x(t)$, is imposed on the communication channel, where the time-varying function $p(t)$ is given as

$$p(t) = \begin{cases} 0.5 + 0.25\sin(t), & 0 \le t \le 2 \\ 0.5 + 0.25\cos(2t), & 2 < t \le 6 \\ 0.5 + 0.45\cos(5t), & 6 < t \le 40. \end{cases}$$

By the same system settings, the associated gain matrices $K_{\mathrm{com,i}}(i = 1, 2, 3)$ in [17, Th. 2] are computed as

$$K_{\mathrm{com},1} = [6.4313, 0.4782, 2.5813]$$
$$K_{\mathrm{com},2} = [7.7995, 6.4901, 1.2767]$$
$$K_{\mathrm{com},3} = [3.6903, 6.7520, 3.9376].$$

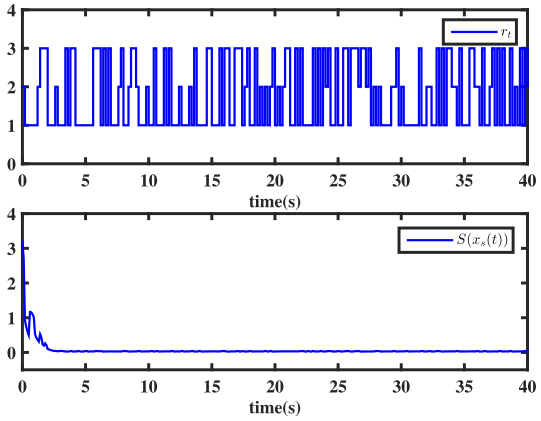

Fig. 3. Jump mode r_t and SMS variable $S(x_s(t))$.

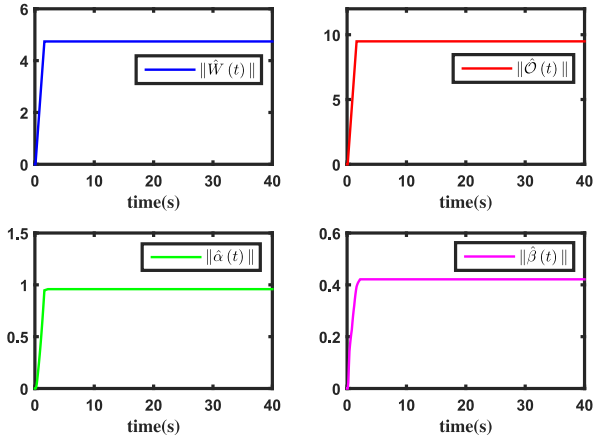

Fig. 4. Norm curves of adaptive parameters $\hat{W}(t)$, $\hat{\mathcal{O}}(t)$, $\hat{\alpha}(t)$, and $\hat{\beta}(t)$.

Then, the devised sliding surface function $S(t)$ in [17] is exhibited by

$$S(t) = \begin{cases} [-0.1, 0.2, -0.2]x_s(t) \\ -\int_0^t [0.5955, -0.2370, -0.1049]x_s(\kappa)\mathrm{d}\kappa, & i = 1 \\ [-0.2, 0.1, -0.1]x_s(t) \\ -\int_0^t [0.6453, 0.1494, -0.2239]x_s(\kappa)\mathrm{d}\kappa, & i = 2 \\ [-0.2, 0.1, -0.2]x_s(t) \\ -\int_0^t [0.4284, 0.2677, 0.2769]x_s(\kappa)\mathrm{d}\kappa, & i = 3 \end{cases}$$

and the synthesized controller is utilized as same as that in [17, Th. 3]. For simulation experiment, Fig. 3 displays the evolution of jump mode and SMS variable via the current method, and norm curves of the adaptive parameters $\hat{W}(t)$, $\hat{\mathcal{O}}(t)$, $\hat{\alpha}(t)$ and $\hat{\beta}(t)$ are shown in Fig. 4, respectively. The plots of the system response and control input under the two control methods are provided in Fig. 5 based on the initial condition $x(0) = [2 \ \ -1 \ \ -2]^{\mathrm{T}}$. As observed from Fig. 5, the control signal becomes invalid, and the security of the system can not be guaranteed due to the potential sensor attack signal under the method in [17], leading to the instability of the closed-loop system, while the influence of the sensor attack can be restrained via the developed control algorithm.

Case 2 (Performance Comparison Under Actuator Attacks): As observed from [28], the specific form of actuator attack signal is shown by $\partial_a(x(t), t) = \delta(t)Q(t)\Psi(x(t), t), t \ge 5s$,

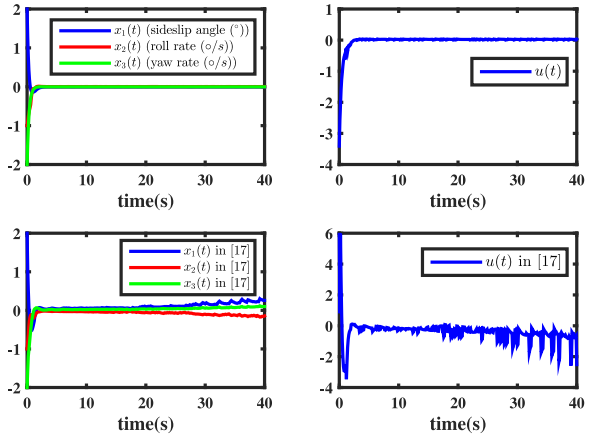

Fig. 5. State response and control signal under two methods.

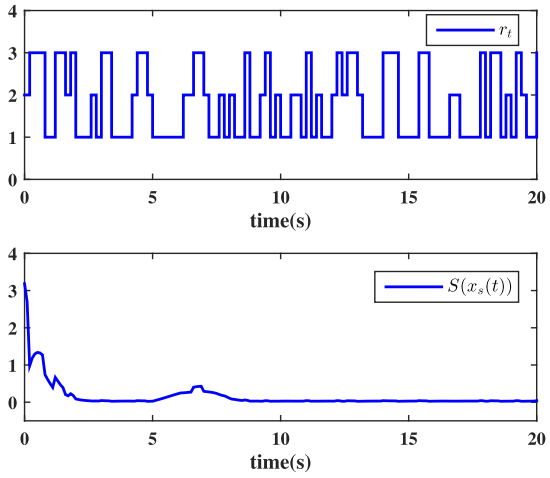

Fig. 6. Jump mode r_t and SMS variable $S(x_s(t))$.

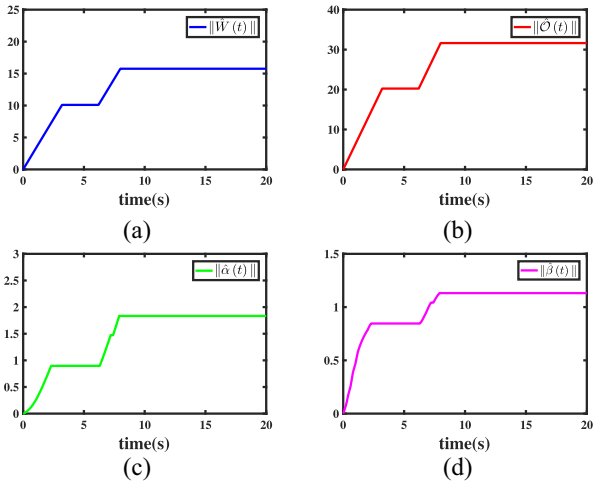

Fig. 7. Norm curves of adaptive parameters $\hat{W}(t)$, $\hat{\mathcal{O}}(t)$, $\hat{\alpha}(t)$, and $\hat{\beta}(t)$.

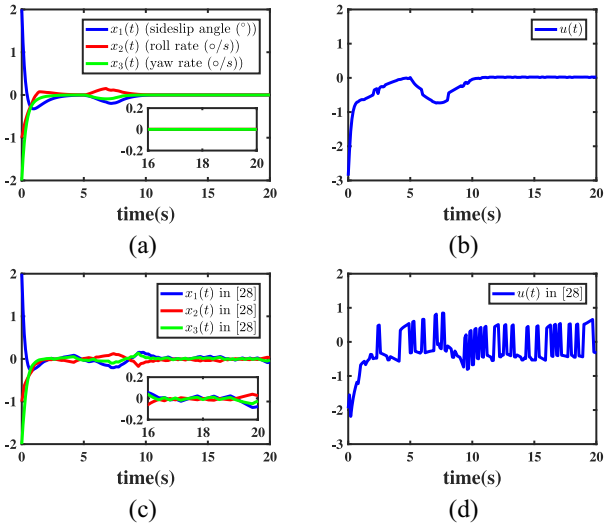

Fig. 8. State response and control signal under two methods.

where $\delta(t)$ stands for the Bernoulli variable, $Q(t)$ denotes an unknown weight matrix, and $\Psi(x(t),t)$ represents the system information used by the adversaries. In such case, $Q(t)$ and $\Psi(x(t),t)$ are chosen as $Q(t) = \cos(t)$ and $\Psi(x(t),t) = \sqrt{x_2^2 + x_3^2 + 2}$. By the same system settings, the matching matrices $M_{\text{com,i}}(i = 1, 2, 3)$ in [28] are shown as

$$\begin{aligned} M_{\text{com},1} &= [-0.8234, 8.6907, -0.4476] \\ M_{\text{com},2} &= [-0.4853, 1.4484, 7.1411] \\ M_{\text{com},3} &= [-1.2797, -0.3621, -3.2277]. \end{aligned}$$

In the position, the corresponding sliding surface variable $s(t)$ in [28] is computed as

$$s(t) = \begin{cases} [-0.5794, 0.4886, -0.8849]x_s(t) \\ -\int_0^t [0.1330, 2.2068, 0.2326]x_s(\kappa)\mathrm{d}\kappa, & i = 1 \\ [-0.6536, 0.1247, -1.2177]x_s(t) \\ -\int_0^t [0.3431, 0.0844, 2.9735]x_s(\kappa)\mathrm{d}\kappa, & i = 2 \\ [-1.3144, 0.4353, -1.1282]x_s(t) \\ -\int_0^t [0.3062, -1.6726, -2.5576]x_s(\kappa)\mathrm{d}\kappa, & i = 3 \end{cases}$$

while the developed controller is provided as same as that in [28, Th. 3]. In simulation, Fig. 6 displays evolution of the jump mode and SMS variable, and norm curves of the adaptive parameters $\hat{W}(t)$, $\hat{\mathcal{O}}(t)$, $\hat{\alpha}(t)$ and $\hat{\beta}(t)$ are shown in Fig. 7, respectively. The plots of the system response and control input are provided in Fig. 8 between the current control method and that in [28] under the same initial condition in Case 1.

In order to further illustrate the availability of the proposed result more clearly, data exploration including tracking precision performance [e.g., integral absolute error (IAE), integral time-weighted absolute error (ITAE), integral square error (ISE)] and energy consumption (EC) taken from [33], is carried out, i.e., IAE $\triangleq \int_0^{20} \|x_s(t)\|\mathrm{d}t$, ITAE $\triangleq \int_0^{20} t\|x_s(t)\|\mathrm{d}t$ and ISE $\triangleq \int_0^{20} \|x_s(t)\|^2\mathrm{d}t$, EC $\triangleq \int_0^{20} u^2(t)\mathrm{d}t$ are introduced herein. Comparison results of the four indicators are provided in Fig. 9. It is observed that the resultant system via the proposed control method can be resilient against attacks with better control accuracy under lower EC.

Case 3 (Performance Comparison Under Both Sensor and Actuator Attacks): In this case, the actuator attack $\partial_a(x(t),t)$ is taken as

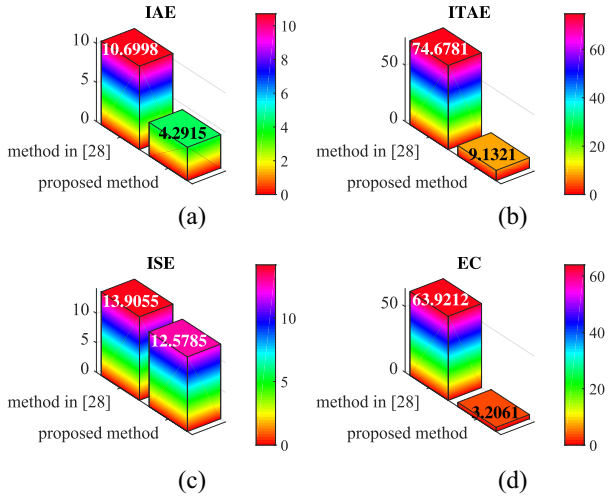

Fig. 9. Comparison of performance measures.

$$\partial_a(x(t),t) = \begin{cases} \mathcal{M}(t) + \mathcal{N}_1(t)\mathcal{N}_2(t), & 0 \le t < 3 \\ 0, & 3 \le t < 8 \\ (1 + 1.2\sin(200t)), & 8 \le t < 15 \\ 0, & 15 \le t < 20 \end{cases}$$

where $\mathcal{M}(t) = 0.4\sin(3t)$, $\mathcal{N}_1(t) = 0.2\cos(3t)$ and $\mathcal{N}_2(t) = \sin(x_2(t))\cos(x_3(t))$, and the time-varying function $p(t)$ of the sensor attack is chosen as

$$p(t) = \begin{cases} 0, & 0 \le t < 4 \\ 0.6 + 0.25\sin(2t), & 4 \le t < 10 \\ 0.5 + 0.45\sin(2t), & 10 \le t \le 20. \end{cases}$$

Then, the evolutions of transfer mode r_t and SMS variable are shown by Fig. 10, the norm curves of the adaptive parameters $\hat{W}(t)$, $\hat{\mathcal{O}}(t)$, $\hat{\alpha}(t)$ and $\hat{\beta}(t)$ are provided in Fig. 11, and the curves of the state response and control signal, based on the two different methods, are described in Fig. 12.

Moreover, differing from the case in [28] that just takes actuator attacks into consideration, the proposed method deals with a more general case that the sensor and actuator are simultaneously interfered. As seen from Fig. 12, although the system is obviously affected by both the actuator and sensor attacks during [0s, 3s] and [8s, 10s], the state response will return to stable status more robustly and quickly by virtue of the proposed NN-based SMC than the method in [28], which shows the former is more efficient in achieving desirable operation while withstanding complicated threats.

Furthermore, the analysis of the above quantitative data indicators is carried out, see Fig. 13, which demonstrates the resultant system using the current method is also resilient against both attacks with better control accuracy and lower EC. At last, the statistical results under 30 sets of repeated experiments have been performed to further validate the efficiency and advantage of the current control approach with other peer methods, where the corresponding curves of state response are shown in Fig. 14, which indicates the closed-loop system has better control accuracy with more robustness under the proposed algorithm in contrast to the method in [28].

Remark 5: It should be mentioned that the results of this article are obtained based on the premise of that the modes of

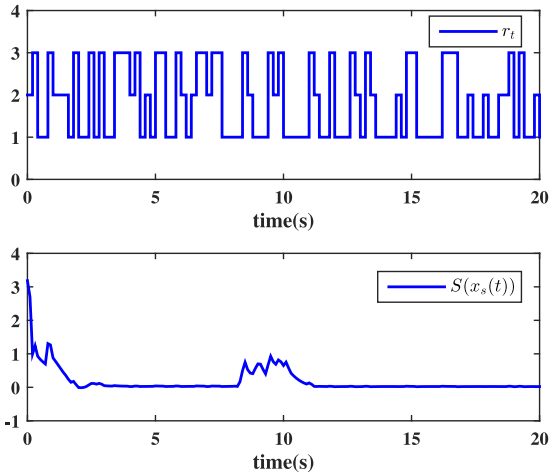

Fig. 10. Jump mode r_t and SMS variable $S(x_s(t))$.

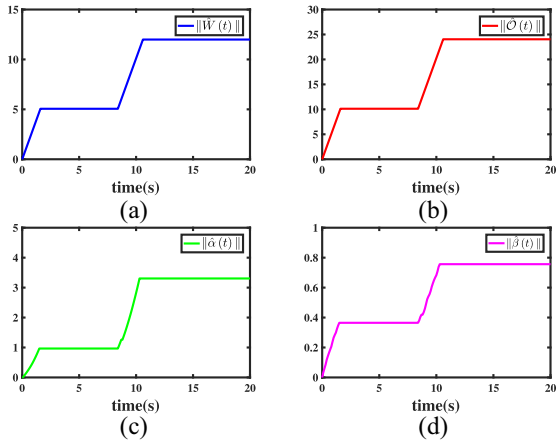

Fig. 11. Norm curves of adaptive parameters $\hat{W}(t)$, $\hat{\mathcal{O}}(t)$, $\hat{\alpha}(t)$, and $\hat{\beta}(t)$.

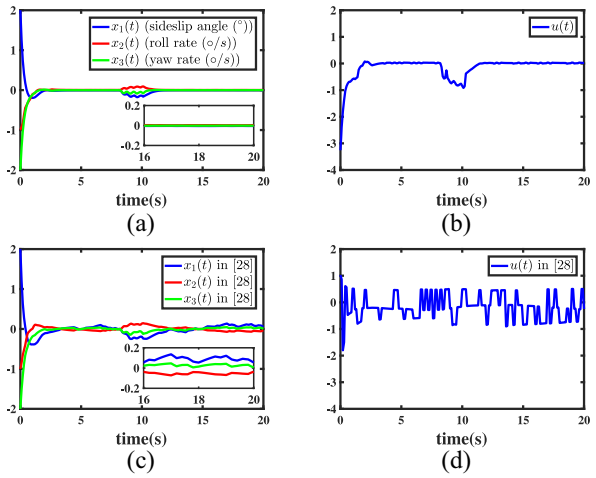

Fig. 12. State response and control signal under two methods.

the controller and sensor can always be synchronized with the system mode. However, some limitations using the proposed methodology may exist in a real system. For instance, in practical engineering, identification errors of system mode, certain delays in switching signals, etc., may lead to asynchronous switching phenomenon among the modes of the controller,

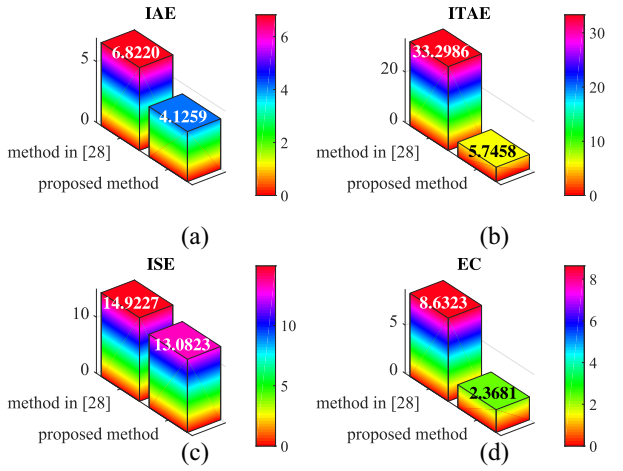

Fig. 13. Comparison of performance measures.

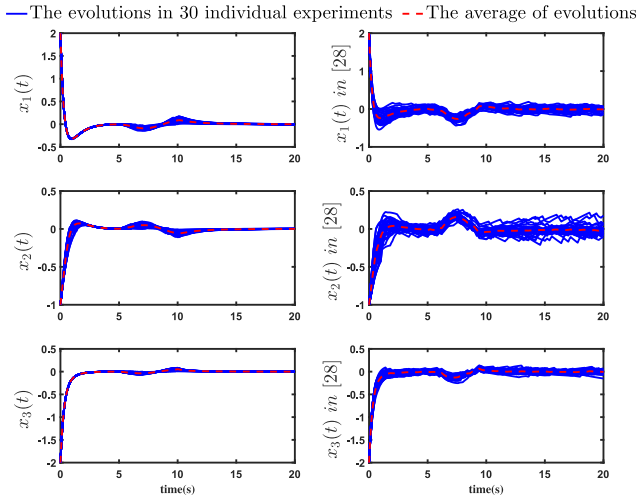

Fig. 14. Comparative curves of state responses under two methods.

the sensor, and the system [34], [35]. Asynchronous switching often results in a decrease in system performance, and as the switching signal lags severely and/or fast switching occurs, it will cause the whole system to be unstable. Hence, the difficulties that asynchronous switching occurs during system operation, may be encountered in deploying the methodology, and the asynchronous control measures for the system are not probed, which deserves further investigation in future work.

V. Conclusion

In this article, the NN-based adaptive secure control issue for uncertain CPSMSs against GUTRs, structural uncertainty, both sensor and actuator attacks have been addressed via the SMC technique. A special NN-based SMC law has been established to ensure the attainability of the devised SMS. A fresh stochastically stable condition for the CPSMSs has been derived relying on the attainability of the SMS and stochastic stability theory. Finally, the feasibleness of the proposed control algorithm has been verified by simulation experiments with performance comparisons.

References

[1] K. D. Kim and P. R. Kumar, "Cyber-physical systems: A perspective at the centennial," *Proc. IEEE*, vol. 100, pp. 1287–1308, May 2012.

[2] D. Pan, D. Ding, X. Ge, Q.-L. Han, and X.-M. Zhang, "Privacy-preserving platooning control of vehicular cyber-physical systems with saturated inputs," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 53, no. 4, pp. 2083–2097, Apr. 2023.

[3] X.-L. Wang and G.-H. Yang, "Piecewise attack strategy design for T-S fuzzy cyber-physical systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 10, pp. 6477–6486, Oct. 2022.

[4] L. W. An and G.-H. Yang, "Enhancement of opacity for distributed state estimation in cyber-physical systems," *Automatica*, vol. 136, Feb. 2022, Art. no. 110087.

[5] Y. Joo, Z. Qu, and T. Namerikawa, "Resilient control of cyber-physical system using nonlinear encoding signal against system integrity attacks," *IEEE Trans Autom. Control*, vol. 66, no. 9, pp. 4334–4341, Sep. 2021

[6] F. Santoso and A. Finn, "A data-driven cyber-physical system using deep-learning convolutional neural networks: Study on false-data injection attacks in an unmanned ground vehicle under fault-tolerant conditions," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 53, no. 1, pp. 346–356, Jan. 2023.

[7] Z. Liu, X. Chen, and J. Yu, "Adaptive sliding mode security control for stochastic Markov jump cyber-physical nonlinear systems subject to actuator failures and randomly occurring injection attacks," *IEEE Trans. Ind. Informat.*, vol. 19, no. 3, pp. 3155–3165, Mar. 2023.

[8] M. Meng, G. Xiao, and B. Li, "Adaptive consensus for heterogeneous multi-agent systems under sensor and actuator attacks," *Automatica*, vol. 122, Dec. 2020, Art. no. 109242.

[9] D. Meng, W. Niu, X. Ding, and L. Zhao, "Network-to-network control over heterogeneous topologies: A dynamic graph approach," *IEEE Trans. Syst. Man, Cyber. Syst.*, vol. 50, no. 5, pp. 1885–1896, May 2020.

[10] S. Nateghi, Y. Shtessel, and C. Edwards, "Resilient control of cyber-physical systems under sensor and actuator attacks driven by adaptive sliding mode observer," *Int. J. Control*, vol. 31, no. 15, pp. 7425–7443, Jul. 2021.

[11] S. Li and Z. Xiang, "Stochastic stability analysis and L_∞-gain controller design for positive Markov jump systems with time-varying delays," *Nonlinear Anal. Hybrid Syst.*, vol. 22, pp. 31–42, Nov. 2016.

[12] J. Yu, Z. Liu, and P. Shi, "Robust state-estimator-based control of uncertain semi-Markovian jump systems subject to actuator failures and time-varying delay," *IEEE Trans. Automat. Control*, vol. 69, no. 1, pp. 487–494, Jan. 2024.

[13] B. Jiang, Z. Wu, Z. Liu, and B. Li, "Adaptive sliding mode security control of wheeled mobile manipulators with Markov switching joints against adversarial attacks," *Control Eng. Pract.*, vol. 137, Aug. 2023, Art. no. 105558.

[14] E.-K. Boukas, *Stochastic Switching Systems: Analysis and Design*. Boston, MA, USA: Birkhauser, 2006.

[15] M. Liu, L. Zhang, P. Shi, and Y. Zhao, "Sliding mode control of continuous-time Markovian jump systems with digital data transmission," *Automatica*, vol. 80, pp. 200–209, Jun. 2017.

[16] C. Park, N. Kwon, I. Park, and P. Park, "H_∞ filtering for singular Markovian jump systems with partly unknown transition rates," *Automatica*, vol. 109, Nov. 2019, Art. no. 108528.

[17] M. Li, Y. Chen, and Y. Z. Liu, "Sliding-mode secure control for jump cyber–physical systems with malicious attacks," *J. Frank. Inst.*, vol. 358, no. 7, pp. 3424–3440, May 2021.

[18] X. Zhao, H. Yang, and G. Zong, "Adaptive neural hierarchical sliding mode control of nonstrict-feedback nonlinear systems and an application to electronic circuits," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 7, pp. 1394–1404, Jul. 2017.

[19] Y. Niu, J. Lam, X. Wang, and D. W. Ho, "Neural adaptive sliding mode control for a class of nonlinear neutral delay systems," *J. Dyn. Sys., Meas., Control.*, vol. 130, no. 6, Nov. 2008, Art. no. 61011.

[20] R. Ma, X. Shao, J. Liu, and L. Wu, "Event-triggered sliding mode control of Markovian jump systems against input saturation," *Syst. Control. Lett.*, vol. 134, Dec. 2019, Art. no. 104525.

[21] B. Chen, Y. Niu, and Y. Zou, "Adaptive sliding mode control for stochastic Markovian jumping systems with actuator degradation," *Automatica*, vol. 49, no. 6, pp. 1748–1754, Jun. 2013.

[22] Z. Cao, Y. Niu, and Y. Zou, "Adaptive neural sliding mode control for singular semi-Markovian jump systems against actuator attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 3, pp. 1523–1533, Mar. 2021.

[23] H. Yang, S. Yin, and O. Kaynak, "Neural network-based adaptive fault-tolerant control for Markovian jump systems with nonlinearity and actuator faults," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 6, pp. 3687–3698, Jun. 2021.
[24] J. Song, X.-H. Chang, and Z.-M. Li, "Secure P2P nonfragile sampled-data controller design for nonlinear networked system under sensor saturation and DoS attack," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 3, pp. 1575–1585, May/Jun. 2023.
[25] C. Wu, X. Li, W. Pan, J. Liu, and L. Wu, "Zero-sum game-based optimal secure control under actuator attacks," *IEEE Trans. Autom. Control*, vol. 66, no. 8, pp. 3773–3780, Aug. 2021.
[26] Z. Kazemi, A. A. Safavi, M. M. Arefi, and F. Naseri, "Finite-time secure dynamic state estimation for cyber–physical systems under unknown inputs and sensor attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 8, pp. 4950–4959, Aug. 2022.
[27] 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. Automat. Control*, vol. 65, no. 3, pp. 1264–1271, Mar. 2020.
[28] W. Qi, C. Lv, J. H. Park, G. Zong, J. Cheng, and K. Shi, "SMC for semi-Markov jump cyber-physical systems subject to randomly occurring deception attacks," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 1, pp. 159–163, Jan. 2022.
[29] H. Yang, H. Han, S. Yin, H. Han, and P. Wang, "Sliding mode-based adaptive resilient control for Markovian jump cyber–physical systems in face of simultaneous actuator and sensor attacks," *Automatica*, vol. 142, Aug. 2022, Art. no. 110345.
[30] A. Yeşildirek and F. L. Lewis, "Feedback linearization using neural networks," *Automatica*, vol. 31, no. 11, pp. 1659–1664, Nov. 1995.
[31] S. Mohammad-Hoseini, M. Farrokhi, and A. J. Koshkouei, "Robust adaptive control of uncertain non-linear systems using neural networks," *Int. J. Control*, vol. 81, no. 8, pp. 1319–1330, Nov. 2008.
[32] L. C. Fu, "Neural network approach to variable structure based adaptive tracking of SISO systems," in *Proc. IEEE Workshop Variable Struct. Syst.*, Tokyo, Japan, 1996, pp. 148–153.
[33] S. Mobayen and V. J. Majd, "Robust tracking control method based on composite nonlinear feedback technique for linear systems with time-varying uncertain parameters and disturbances," *Nonlinear Dyn.*, vol. 70, no. 1, pp. 171–180, 2012.
[34] Z.-G. Wu, P. Shi, Z. Shu, H. Su, and R. Lu, "Passivity-based asynchronous control for Markov jump systems," *IEEE Trans. Autom. Control*, vol. 62, no. 4, pp. 2020–2025, Apr. 2017.
[35] X. Li, C. K. Ahn, W. Zhang, and P. Shi, "Asynchronous event-triggered-based control for stochastic networked Markovian jump systems with FDI attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 53, no. 9, pp. 5955–5967, Sep. 2023.

Zhen Liu received the Ph.D. degree in control theory and applications from the Ocean University of China, Qingdao, China, in 2017.

He was a joint Ph.D. candidate with the School of Engineering, University of the West of England, Bristol, U.K., and a Visiting Scholar with the College of Engineering, University of Kentucky, Lexington, KY, USA. He is currently a Distinguished Professor with the School of Automation, Qingdao University, Qingdao. His current research interests include intelligent control and robot, cyber–physical systems, UAV Control, and sliding mode control.

Dr. Liu was the recipient of the Shandong Province Taishan Scholar Special Project Fund.

Junye Zhang received the B.S. degree in automation from Jinan University, Jinan, China, in 2021. He is currently pursuing the M.Sc. degree in control science and engineering with the School of Automation, Qingdao University, Qingdao, China.

His research interests include stochastic systems and intelligent control.

Quanmin Zhu received the M.Sc. degree from the Harbin Institute of Technology, Harbin, China, in 1983, and the Ph.D. degree from the Faculty of Engineering, University of Warwick, Coventry, U.K., in 1989.

He is a Professor of Control Systems with the School of Engineering, University of the West of England, Bristol, U.K. His main research interest is in the area of nonlinear system modeling, identification, and control.

Prof. Zhu is acting as a member of Editorial Committee of *Chinese Journal of Scientific Instrument*, and the President of International Conference of Modeling, Identification and Control.