Hindawi
Mathematical Problems in Engineering
Volume 2022, Article ID 2779623, 11 pages
https://doi.org/10.1155/2022/2779623

Research Article

Security-Based Asynchronous Control for Discrete-Time Markov Switching Power Systems *

Weifeng Xu,[1] Bin Yu,[1] Liguo Weng,[1] and Jianguo Zhou[2]

[1]*State Grid Hangzhou Xiaoshan Power Supply Company, Hangzhou 311200, China*
[2]*Zhejiang Zhongxin Power Engineering Construction Co., Ltd, Hangzhou 311200, China*

Correspondence should be addressed to Liguo Weng; wlgzxdj@163.com

Received 14 December 2021; Accepted 14 March 2022; Published 5 May 2022

Academic Editor: Licheng Wang

This paper addresses the asynchronous control problem for power systems subject to abrupt variations and cyber-attacks. In the sequel, the transient faults of circuit breakers can be described as the Markov process. In light of these situations, the power systems are transmitted to discrete-time Markov switching systems. Meanwhile, the deception attacks with time-varying delays in dispatchers are regulated by a Markov process. The controller and dispatcher are mode-dependent and their modes are nonsynchronous with those of power systems, which are modeled by the hidden Markov models. On the basis of the deception attacks, sufficient conditions are presented to guarantee the stochastic mean-square stability of the closed-loop dynamic. Finally, the proposed control design strategy is testified via a simulation result.

1. Introduction

As a type of complex nonlinear system, power systems have gained considerable interest due to their spontaneous oscillation characters and high penetration [1–3]. Over the past decades, many significant methods have been devoted to power systems, such as state estimation [4–8]. For the purpose of stabilizing interconnected power systems, many efforts have been devoted to exploring the mismatch between load demand and total power generation. Following this character, many techniques are forwarded to maintain the frequency balance including the load frequency control, state feedback control [9–11]. Therefore, how to keep the frequency deviation of power systems within a certain range remains a hot topic. For instance, to overcome the low/zero inertia, stability has been studied for power systems with fluctuation and intermittency in [12]. In [13], the load frequency control technique has been utilized to balance the power exchanges among different areas. In [14], the network-induced time delay has been considered in supplying high-quality electric energy. In [15], the fuzzy-dependent power system stabilizer with uncertain factors has been investigated.

In reality, owing to many unexpected factors such as component faults, external disturbances, and unknown attacks, the power systems always experience random variations in parameters/structures, which lead to the resulting operation changes and performance degeneration [16, 17]. Markov switching is identified as an effective tool in modeling the aforementioned conditions [18]. Note that Markov switching is ubiquitous, which has been applied in many physical situations, such as tunnel-diode-circuit-model and complex networks [18–20]. However, to our knowledge, little attention has been given to Markov switching power systems (MSPSs) except for [21–23]. In [21], the random switching of power systems can be modeled as MSPSs. Lately, the continuous-time interconnected multiarea MSPSs with load frequency control are considered in [22]. In [23], the discrete-time MSPSs are studied with a hidden Markov model. Nevertheless, in contrast with the fruitful achievements of power systems, MSPSs have not gained suitable attention.

On the other hand, many valuable results have been reported on the networked power systems subjected to many network-induced factors, such as communication delays, packet losses, quantization effects, and event-triggered

protocols [24–26]. By comparison, potential cyber-attacks may destroy the stability of power systems via a shared communication network. In light of the different attack ways, cyber-attacks can be summarized into three categories: denial-of-service [27], repeat attack [28, 29], and deception attacks [30–33]. In more detail, the former aims at destroying the channel of signal exchange, and repeat attacks inject historic data into the network affect the performance, while deception attacks attempt to inject false data into the communication network to destroy the data trustworthiness. On the basis of these cyber-attacks, the conventional control law becomes untrusted. It is of significance to be concerned with cyber-attacks. Among these cyber-attacks, deception attacks are common in practice. For instance, in [34], the unified power systems against random-occurring deception attacks have been studied. In [35], on the basis of credibility, the multiarea power systems with deception attacks have been well concerned. Nevertheless, the security issues of power systems with regard to cyber-attacks have not been adequately explored, such as random occurring deception attacks with time-varying delays, not to mention power systems against Markov switching.

Through expounds of the above discussion, this work shall consider the nonsynchronous controller design issue for MSPSs with cyber-attacks. The main contributions are listed below: (1) a generalized MSPS is established, which covers asynchronous dispatcher, asynchronous controller, and deception attacks, simultaneously. (2) Deception attacks with time-varying delays are taken into consideration. The probability of each time-varying delay is different, and random-occurring deception attacks are described by a sequence of stochastic variables induced by a new Markov process. (3) A more general scenario is that the asynchronous phenomena among system mode, controller mode, and dispatcher mode are well revealed and the hidden Markov model technique is applied. Finally, the effectiveness of the gained methodology is verified via an illustrated example.

Notations: the notations in this paper is standard. $\mathbb{N}$ symbols the set of all non-negative integers. diag$\{\cdots\}$ means a block-diagonal matrix. $\mathbf{He}\{\mathscr{Z}\} = \mathscr{Z} + \mathscr{Z}^{\top}$. $\|\cdot\|$ implies the Euclidean norm of a vector. $\mathbb{R}^n$ signifies the n dimensional real space. $\mathscr{E}\{\cdot\}$ represents the mathematical expectation. $*$ describes the symmetric term.

2. Problem Formulations

As sketched in Figure 1, a type of single-machine infinite bus (SMIB) through tie line is explored in the current study. From the SMIB, we can observe the dynamic behavior of large interconnected power systems. Following this trend, the basic components of SMIB power systems (SMIBPSs) are expressed in Figure 2. Accordingly, the following formula can be established:

$$\begin{cases} \dot{\delta} = \omega_0 \omega, \\ \dot{\omega} = \dfrac{\mathfrak{T}_m - \mathfrak{T}_e}{\mathfrak{M}}, \\ \mathfrak{T}_{do}{}' \dot{\mathfrak{E}}_q{}' = \mathfrak{E}_{fd} - \dfrac{x_d + x_e}{x_d' + x_e} \mathfrak{E}_q{}' + \dfrac{x_d + x_d'}{x_d' + x_e} \mathfrak{V} \cos(\delta), \\ \mathfrak{T}_E \dot{\mathfrak{E}}_{fd} = \mathfrak{K}_E \mathfrak{E}_{ref} - \mathfrak{K}_E \mathfrak{V}_t + \mathfrak{K}_E u - \mathfrak{E}_{fd}, \end{cases} \tag{1}$$

where δ, ω, E_q', and E_{fd} refer to the generator angle, generator speed, q-axis voltage, and generator voltage, respectively. Meanwhile, other physical meanings are summarized in Table 1.

In view of the aforementioned observation, the fourth-order state-space model of SMIBPS is formulated as

$$\dot{x}(t) = Ax(t) + Bu(t), \tag{2}$$

where

$$x(t) = \begin{bmatrix} \Delta\delta \\ \Delta\omega \\ \Delta\mathfrak{E}_q{}' \\ \Delta\mathfrak{E}_{fd} \end{bmatrix},$$

$$A = \begin{bmatrix} 0 & \omega_0 & 0 & 0 \\ -\dfrac{k_1}{\mathfrak{M}} & 0 & -\dfrac{k_2}{\mathfrak{M}} & 0 \\ -\dfrac{k_4}{\mathfrak{T}_{\mathrm{do}}{}'} & 0 & -\dfrac{1}{k_3 \mathfrak{T}_{\mathrm{do}}{}'} & -\dfrac{1}{\mathfrak{T}_{\mathrm{do}}{}'} \\ -\dfrac{k_5 k_E}{\mathfrak{T}_E} & 0 & -\dfrac{k_6 k_E}{\mathfrak{T}_E} & -\dfrac{1}{\mathfrak{T}_E} \end{bmatrix}, \tag{3}$$

$$B = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \dfrac{k_E}{\mathfrak{T}_E} \end{bmatrix}.$$

Similar to the work of [10], $\mathfrak{Q}$ and $\mathfrak{P}$, respectively, represent the reactive and real power loading, whose functions are presented by the parameters $k_l (l = 1, \ldots, 6)$.

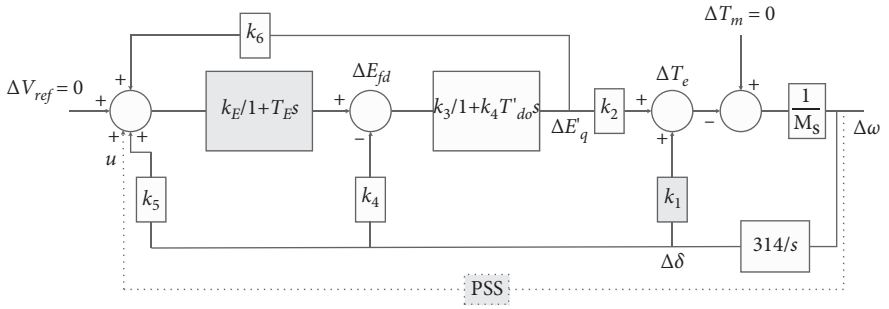

Figure 1: Signal model of SMIBPSs.

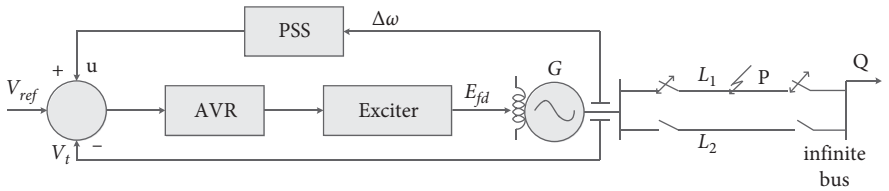

Figure 2: Basic components of SMIBPSs with faults.

Table 1: The parameters of power systems.

x'_d	Generator d-axis transient reactance
x_d, x_q	$d-q$ axis synchronous reactance
$\mathfrak{T}_e, \mathfrak{T}_m$	Electrical, mechanical torque
$k_E, \mathfrak{T}_E$	Exciter gain and time constant
$\mathfrak{V}$	Infinite busbar voltage
$\mathfrak{V}_t$	Terminal voltage
$\mathfrak{P}, \mathfrak{Q}$	Real and reactive power loadings
$\mathfrak{M}$	Inertia coefficient
$\mathfrak{T}'_{\mathrm{do}}$	Open circuit d-axis transient time constant
u	Stabilizing signal
x_e	External reactance
Δw	Speed deviation
$k_1, \ldots, k_6$	Linearized model constants of the synchronous machine

More specifically, the values of parameters in Table 1 are given by $x_q = 1.55$pu, $x_d = 1.6$pu, $x'_d = 0.32$pu, $\mathfrak{T}'_{\mathrm{do}} = 6$s, $\mathfrak{M} = 10$s, $x_e = 0.4$pu, $\omega_0 = 50\pi$rad/s, $\mathfrak{T}_E = 0.05$s, $k_E = 50$, and $\mathfrak{L}_l = 0.8\,(l = 1, 2)$.

By resorting to a discretization period T, the discrete-time SMIBPS (2) can be established as

$$x(k+1) = Ax(k) + Bu(k), \tag{4}$$

where $A = e^{\mathrm{AT}}$ and $B = \int_0^T e^{At} B \mathrm{d}t$.

In light of the unreliability of the network medium, the abrupt variations of SMIBPS cannot be avoided. To model the variation of SMIBPS in a suitable way, a stochastic variable $\sigma(k)$ takes values within a space $\mathscr{M} = \{1, \ldots, \mathscr{M}\}$, is presented to depict the Markov switching SMIBPSs as follows:

$$x(k+1) = A_{\sigma(k)} x(k) + B_{\sigma(k)} u(k),\ k = 0, 1, \ldots, \tag{5}$$

where $\sigma(k)$ refers to a Markov chain, whose transition probability matrix (TPM) $\Pi = [\pi_{mn}]_{\mathscr{M}\times\mathscr{M}}$ is inferred as

$$\pi_{mn} = \Pr\{\sigma(k+1) = n \mid \sigma(k) m\}, \tag{6}$$

where $0 \le \pi_{mn} \le 1$ and $\sum_{n=1}^{\mathscr{M}} \pi_{mn} = 1$ for all $m, n \in \mathscr{M} = \{1, 2, \ldots, \mathscr{M}\}$.

Notice that the data are transmitted to controllers via an unencrypted communication network, which is always being attacked on the sensor-to-controller channels. It is well-known that deception attacks are commonly encountered, which launch some deception signals to destroy the information authenticity of $x(k)$. Thus, as depicted in Figure 1, we consider the random occurring deception attacks in power systems, which damage/destroy the performance to the data integrity. Therefore, the real system information is modeled as

$$\overline{x}(k) = x(k) + \alpha_{\varepsilon(k)}(k)\zeta(k), \tag{7}$$

where $\zeta(k) = -x(k) + f(x(k - \tau_{\varepsilon(k)}(k)))$. $\tau_{\varepsilon(k)}(k)$ stand for the jump-mode-dependent time-varying delay of deception attacks, and $\tau_{\varepsilon(k)}(k) \in [\tau_1, \tau_2]$. τ_1 and τ_2 are two constants, which satisfies $0 \le \tau_1 \le {}_2$. $f(x(k)) = [f(x_1(k - \tau_{\varepsilon(k)}(k)))$ $, f(x_2(k - \tau_{\varepsilon(k)}(k))), \ldots, f(x_n(k - \tau_{\varepsilon(k)}(k)))]^{\top}$ being the nonlinear function of deception attacks subject to random occurring time-varying delays. $\alpha_{\varepsilon(k)}(k)$ implies the Bernoulli variable, in which $\alpha_{\varepsilon(k)}(k) = 1$ and $\alpha_{\varepsilon(k)}(k) = 0$ signify the transmission channel with and without attack. It yields

$$\begin{aligned} \mathscr{E}\left\{\alpha_{\varepsilon(k)}(k) = 1\right\} &= \overline{\alpha}_{\varepsilon(k)}, \mathscr{E}\left\{\alpha_{\varepsilon(k)}(k) = 0\right\} \\ &= 1 - \overline{\alpha}_{\varepsilon(k)}, \\ \mathscr{E}\left\{\left(\alpha_{\varepsilon(k)}(k) - \overline{\alpha}_{\varepsilon(k)}\right)^2\right\} &= \overline{\alpha}_{\varepsilon(k)}\left(1 - \overline{\alpha}_{\varepsilon(k)}\right) \\ &= \widehat{\alpha}^2_{\varepsilon(k)}. \end{aligned} \tag{8}$$

In particularly, $\varepsilon(k)$ is a Markov process having values over a set $\mathscr{S} = \{1, \ldots, \mathscr{S}\}$, whose TPM $\Omega = [\psi_{\mathrm{ms}}]_{\mathscr{M}\mathrm{s}}$ with

$$\psi_{\mathrm{ms}} = \Pr\{\varepsilon(k) = s|\sigma(k) = m\}, \tag{9}$$

where $0 \le \psi_{ms} \le 1$ and $\sum_{s=1}^{\mathcal{S}} \psi_{\mathrm{ms}} = 1$ for any $m \in \mathcal{M}$ and $s \in \mathcal{S}$.

Accordingly, the actual system information can be reformulated as

$$\overline{x}(k) = \left(1 - \alpha_{\varepsilon(k)}(k)\right)x(k) + \alpha_{\varepsilon(k)}(k) f\left(x\left(k - \tau_{\varepsilon(k)}(k)\right)\right). \tag{10}$$

Remark 1. In contrast to the reporting literature with mode-independent deception attacks [30–33], the deception attacks have the Markov behavior, and the attack indication scalar $\alpha_{\varepsilon(k)}(k)$ is presented to describe the dynamic behavior. Meanwhile, in the current study, time-varying delays against Markov behavior are considered in the deception attacks, which covers the existing deception attacks as special cases [30–33].

Assumption 1. (see [36]). The embedded function $f(x(k - \tau_{\varepsilon(k)}(k)))$, which is adopted to restrain deception attacks with random occurring time-varying delays, satisfies the following condition:

$$\left\| f\left(x\left(k - \tau_{\varepsilon(k)}(k)\right)\right)\right\|^2 \le \left\| Qx\left(k - \tau_{\varepsilon(k)}(k)\right)\right\|^2, \tag{11}$$

where Q indicates a known matrix implying an upper bound of embedded function $f(x(k - \tau_{\varepsilon(k)}(k)))$.

It is noteworthy that the resulting mode information determines the controller design and effects the performance. With respect to the mode information that cannot be observed when an attack occurs, in the current study, an asynchronous controller was developed as follows:

$$u(k) = K_{\theta(k)}\overline{x}(k), \tag{12}$$

where $K_{\theta(k)}$ being the controller gains. Stochastic variable $\theta(k)$ implies a Markov chain having values in a space $\mathcal{D} = \{1, 2, \ldots, \mathcal{D}\}$, whose TPM $\Xi = [\varphi_{md}]_{\mathcal{M}\mathrm{D}}$ with

$$\varphi_{md} = \Pr\{\theta(k) = d|\sigma(k) = m\}, \tag{13}$$

where $0 \le \varphi_{md} \le 1$ and $\sum_{d=1}^{\mathcal{D}} \varphi_{md} = 1$ for any $m \in \mathcal{M}$ and $d \in \mathcal{D}$.

Let $\sigma(k) = m \in \mathcal{M}$, $\varepsilon(k) = s \in \mathcal{S}$, and $\theta(k) = d \in \mathcal{D}$, combining (5), (10), and (12), we have

$$\begin{aligned} x(k+1) = {} & \mathcal{A}_{msd}x(k) + \overline{\alpha}_s B_m K_d f\left(x\left(k - \tau_s(k)\right)\right) \\ & + \left(\alpha_s(k) - \overline{\alpha}_s\right)B_m K_d\left(-x(k) + f\left(x\left(k - \tau_s(k)\right)\right)\right), \end{aligned} \tag{14}$$

where $\mathcal{A}_{msd} = A + (1 - \overline{\alpha}_s)B_m K_d$.

Remark 2. Actually, the mode information of the SMIBPSs is difficult to achieve due to many factors, including higher costs and time-wasting. In order to describe the dynamic behavior of random occurring deception attacks and control laws, the hidden Markov models are adopted to model these asynchronous phenomena. More specifically, we get the two-independent conditional probabilities as follows:

$$\begin{aligned} & \Pr\{\varepsilon(k) = s, \theta(k) = d|\sigma(k) = m\} \\ & \quad = \Pr\{\varepsilon(k) = s|\sigma(k) = m\} \times \Pr\{\theta(k) = d|\sigma(k) = m\} \\ & \quad = \psi_{ms}\varphi_{md}. \end{aligned} \tag{15}$$

For the convenience of presentation, the following definition is recalled:

Definition 1. (see [37]). The closed-loop dynamic (14) is stochastically mean-square stable (SMSS), if under any initial condition $\alpha(t_0)$, $\varphi(t_0) \in \mathcal{L}$, and $\upsilon(t_0) \in \mathcal{M}$, such that

$$\mathcal{E}\left\{\sum_{0}^{\infty} \|x(k)\|^2 | x(k_0), \sigma(k_0)\right\} < \infty. \tag{16}$$

3. Main Results

In the current section, the SMSS criteria for the closed-loop dynamic (14) and controller design method will be established in Theorem 1 and Theorem 2, respectively.

Theorem 1. *For given scalars $\tau_2 \ge \tau_1 \ge 0$, and $\overline{\alpha}_s (s \in \mathcal{S})$., and gain matrix K_d, the closed-loop dynamic (14) is SMSS, if there exist matrices $P_m > 0 (m \in \mathcal{M})$, $R > 0$, such that for any $(m, n \in \mathcal{M}, s \in \mathcal{S}, d \in \mathcal{D})$,*

$$\sum_{s=1}^{\mathcal{S}} \psi_{ms} \sum_{d=1}^{\mathcal{D}} \varphi_{md} U_{msd}^{-1} < P_m^{-1}, \tag{17}$$

$$\widehat{\Sigma}_{msd} = \Upsilon_{msd}^1 + \Upsilon_{msd}^{2\top} \mathrm{P}_m \Upsilon_{msd}^2 + \widehat{\alpha}_s^2 \Upsilon_{msd}^{3\top} \mathrm{P}_m \Upsilon_{msd}^3 < 0, \tag{18}$$

where

$$\begin{aligned} \Upsilon_{msd}^1 &= \mathrm{diag}\left\{-U_{msd}^{-1} + (\tau_2 - \tau_1 + 1)R, -R + \overline{\alpha}_s Q^\top Q, -\overline{\alpha}_s I\right\}, \\ \Upsilon_{msd}^2 &= \left[A_m + \left(1 - \overline{\alpha}_s\right)B_m K_d 0 \overline{\alpha}_s B_m K_d\right], \\ \Upsilon_{msd}^3 &= \left[-B_m K_d 0 B_m K_d\right]. \end{aligned} \tag{19}$$

Proof. Let us construct the following Lyapunov functional:

$$V(x(k), \sigma(k)) = \sum_{\iota=1}^{3} V_\iota(\alpha(t), \varphi(t), \upsilon(t)), \tag{20}$$

where

$$\begin{aligned} V_1(x(k), \sigma(k)) &= x^\top(k) P_{\sigma(k)}^{-1} x(k), \\ V_2(x(k), \sigma(k)) &= \sum_{\delta=k-\tau_s(k)}^{k-1} x^\top(\delta) R x(\delta), \\ V_3(x(k), \sigma(k)) &= \sum_{l=-\tau_2+2}^{-\tau_1+1} \sum_{\delta=k+l-1}^{k-1} x^\top(\delta) R x(\delta). \end{aligned} \tag{21}$$

Calculating the derivation of $V(x(k), \sigma(k))$ along the trajectories (14), yields

$$\begin{aligned}\mathscr{E}\{\Delta V(k)\} &= \mathscr{E}\{V(x(k+1),\sigma(k+1)=n)|x(k),\sigma(k)=m\} - V(x(k),\sigma(k))\\ &= \mathscr{E}\{x^{\top}(k+1)\mathrm{P}_m x(k+1)\} - x^{\top}(k)P_m^{-1}x(k)\\ &= \left[\mathscr{A}_{msd}x(k) + \overline{\alpha}_s B_m K_d f(k-\tau_s(k))\right]^{\top}\sum_{s=1}^{\mathscr{S}}\psi_{ms}\sum_{d}^{\mathscr{D}}\varphi_{md}\mathrm{P}_m\\ &\quad\times\left[\mathscr{A}_{msd}x(k) + \overline{\alpha}_s B_m K_d f(k-\tau_s(k))\right]\\ &\quad+\widehat{\alpha}_s^2\left[B_m K_d(-x(k)+f(k-\tau_s(k)))\right]^{\top}\sum_{s=1}^{\mathscr{S}}\psi_{ms}\sum_{d}^{\mathscr{D}}\varphi_{md}\mathrm{P}_m\\ &\quad\times\left[B_m K_d(-x(k)+f(k-\tau_s(k)))\right] - x^{\top}(k)P_m^{-1}x(k).\end{aligned} \tag{22}$$

$$\begin{aligned}\mathscr{E}\{\Delta V_2(k)\} &= \mathscr{E}\{V_2(x(k+1),\sigma(k+1))\} - V_2(x(k),\sigma(k))\\ &\le x^{\top}(k)Rx(k) - x^{\top}(k-\tau_s(k))Rx(k-\tau_s(k)) + \sum_{k+1-\tau_2}^{k-\tau_1}x^{\top}(\delta)Rx(\delta).\end{aligned} \tag{23}$$

$$\begin{aligned}\mathscr{E}\{\Delta V_3(k)\} &= \mathscr{E}\{V_3(x(k+1),\sigma(k+1))\} - V_3(x(k),\sigma(k))\\ &\le (\tau_2-\tau_1)x^{\top}(k)Rx(k) - \sum_{k+1-\tau_2}^{k-\tau_1}x^{\top}(\delta)Rx(\delta).\end{aligned} \tag{24}$$

Recalling Assumption 1, the following formula can be acquired:

$$\begin{aligned}&-\overline{\alpha}_s x^{\top}(k-\tau_s(k))Q^{\top}Qx(k-\tau_s(k))\\ &\quad+\overline{\alpha}_s f^{\top}(k-\tau_s(k))f(k-\tau_s(k))\le 0.\end{aligned} \tag{25}$$

If follows from (20)–(25), it can be obtained that

$$\begin{aligned}\mathscr{E}\{\Delta V(k)\} &= \mathscr{E}\{\Delta V_1(k)\} + \mathscr{E}\{\Delta V_2(k)\} + \mathscr{E}\{\Delta V_3(k)\}\\ &= \mathscr{E}\left\{\eta^{\top}(k)\sum_{s=1}^{\mathscr{S}}\psi_{ms}\sum_{d=1}^{\mathscr{D}}\varphi_{md}\widehat{\Sigma}_{msd}\eta(k) - x^{\top}(k)P_m^{-1}x(k)\right\}\\ &\le \mathscr{E}\left\{\eta^{\top}(k)\sum_{s=1}^{\mathscr{S}}\psi_{ms}\sum_{d=1}^{\mathscr{D}}\varphi_{md}\overline{\Sigma}_{msd}\eta(k) - x^{\top}(k)P_m^{-1}x(k)\right\}\\ &= \mathscr{E}\left\{x^{\top}(k)\left(\sum_{s=1}^{\mathscr{S}}\psi_{ms}\sum_{d=1}^{\mathscr{D}}\varphi_{md}U_{msd}^{-1} - P_m^{-1}\right)x(k)\right\},\end{aligned} \tag{26}$$

where $\eta^{\top}(k) = [x^{\top}(k)x^{\top}(k-\tau_s(k))f^{\top}(x(k-\tau_s(k)))]$, $\overline{\Sigma}_{\mathrm{msd}} = \mathrm{diag}\{U_{msd}^{-1},0,0\}$.

In light of condition (17), the above inequality equivalents to

$$\mathscr{E}\{\Delta V(k)\} \le -\lambda_{\min}(-\overline{\Sigma}_{msd})\eta^{\top}(k)\eta(k) \le -\upsilon x^{\top}(k)x(k), \tag{27}$$

where $\upsilon = \inf\{\lambda_{\min}(-\overline{\Sigma}_{msd})\}$. Obviously, it yielded $\mathscr{E}\{\Delta V(k)\} < 0$, which means

$$\begin{aligned}\mathscr{E}\left\{\sum_{k=0}^{\infty}\|x(k)\|^2\right\} &\le \frac{1}{\upsilon}\{\mathscr{E}V(x(0),\sigma(0))\} - \mathscr{E}\{V(x(\infty),\sigma(\infty))\}\\ &\le \frac{1}{\upsilon}\mathscr{E}\{V(x(0),\sigma(0))\} < \infty.\end{aligned} \tag{28}$$

Based on Definition 1, the closed-loop dynamic (14) achieves SMSS, which completes the proof.□ □

Theorem 2. *For given scalars $\tau_2 \ge \tau_1 \ge 0$, and $\overline{\alpha}_s\,(s\in\mathscr{S})$, and gain matrix $\overline{K}_d$, the closed-loop dynamic (14) is SMSS, if there exist matrices $P_m > 0\,(m\in\mathscr{M})$., $U_{msd} > 0\,(m,n\in\mathscr{M}, s\in\mathscr{S}, d\in\mathscr{D})$., $\overline{R} > 0$, and matrix $Y_d\,(d\in\mathscr{D})$ such that for any $(m,n\in\mathscr{M}, s\in\mathscr{S}, d\in\mathscr{D})$,*

$$\begin{bmatrix}-P_m & \Phi_{msd}\\ * & \mathrm{diag}\{-U_{m11},\ldots,-U_{msd},\ldots-U_{m\mathrm{SD}}\}\end{bmatrix} < 0, \tag{29}$$

where

$$\begin{aligned}\Phi_{msd} &= \left[\sqrt{\psi_{m1}\varphi_{m1}}\,P_m\cdots\sqrt{\psi_{ms}\varphi_{md}}\,P_m\cdots\sqrt{\psi_{m\mathscr{S}}\varphi_{m\mathscr{D}}}\,P_m\right],\\ \overrightarrow{\Upsilon}_{msd}^{1} &= \mathrm{diag}\{U_{msd} - \mathbf{sym}\{Y_d\} + (\tau_2-\tau_1+1)\overline{R}_d,\\ &\quad -\overline{R}_d, \overline{\alpha}_s(I - \mathbf{sym}\{Y_d\})\},\\ \overrightarrow{\Upsilon}_{msd}^{2} &= \left[\varpi_m\overrightarrow{\Upsilon}_{msd}^{2,1\top}\varpi_m\overrightarrow{\Upsilon}_{msd}^{2,2\top}\overrightarrow{\Upsilon}_{msd}^{2,3}\right],\\ \overrightarrow{\Upsilon}^{3} &= \mathrm{diag}\{\Upsilon^{3,1},\Upsilon^{3,1},-I\},\\ \overrightarrow{\Upsilon}_{msd}^{2,1} &= [A_m Y_d + (1-\overline{\alpha}_s)B_m\overline{K}_d 0\overline{\alpha}_s B_m\overline{K}_d],\\ \overrightarrow{\Upsilon}_{msd}^{2,2} &= [-B_m\overline{K}_d 0 B_m\overline{K}_d],\\ \overrightarrow{\Upsilon}_{msd}^{2,3} &= [0\sqrt{\alpha_s}QY_d 0]^{\top},\\ \varpi_m &= [\sqrt{\pi_{m1}}\,I\sqrt{\pi_{m2}}\,I\cdots\sqrt{\pi_{m\mathscr{M}}}\,I],\\ \Upsilon^{3,1} &= \mathrm{diag}\{-P_1,-P_2,\ldots,-P_{\mathscr{M}}\}.\end{aligned} \tag{30}$$

Furthermore, the controller gains are achieved as

$$K_d = \overline{K}_d Y_d^{-1}, \quad \forall d \in \mathscr{D}. \tag{31}$$

Proof. Firstly, premultiplying and postmultiplying the condition (29) by term $\mathrm{diag}\{P_m^{-1}, I, \ldots, I\}$ and its transpose, we can get that

$$\begin{bmatrix} -P_m^{-1} & \overline{\Phi}_{msd} \\ * & \mathrm{diag}\{-U_{m11}, \ldots, -U_{msd}, \cdots - U_{m\mathrm{SD}}\} \end{bmatrix} < 0, \tag{32}$$

where

$$\overline{\Phi}_{msd} = \left[\sqrt{\psi_{m1}\varphi_{m1}}\, I \cdots \sqrt{\psi_{ms}\varphi_{md}}\, I \cdots \sqrt{\psi_{m\mathscr{S}}\varphi_{m\mathscr{D}}}\, I\right]. \tag{33}$$

According to Schur complement, one can derive (33) is equivalent to (17).

Next, by means of Schur complement, it can be easily obtained from (17)as follows:

$$\begin{bmatrix} \overline{\Upsilon}_{msd}^1 & \varpi_m \Upsilon_{msd}^2 \\ * & \overrightarrow{\Upsilon}^3 \end{bmatrix} < 0, \tag{34}$$

where

$$\begin{aligned} \overline{\Upsilon}_{msd}^1 &= \mathrm{diag}\left\{-U_{msd}^{-1} + (\tau_2 - \tau_1 + 1)R, -R, -\overline{\alpha}_s I\right\}, \\ &\quad \left[\varpi_m \Upsilon_{msd}^{2\top} \varpi_m \Upsilon_{msd}^{3\top} \Upsilon_{msd}^4\right], \\ \overline{\Upsilon}_{msd}^2 &= \Upsilon_{msd}^4 \\ &= \left[\sqrt{\alpha_s}\, Q00\right]^\top. \end{aligned} \tag{35}$$

Premultiplying and postmultiplying (35) by $\mathrm{diag}\{Y_d, Y_d, Y_d, I, I, \ldots, I\}$ and its transpose, respectively. It yields

$$\begin{bmatrix} \widehat{\Upsilon}_{msd}^1 & \widehat{\Upsilon}_{msd}^2 \\ * & \overrightarrow{\Upsilon}_m^3 \end{bmatrix} < 0, \tag{36}$$

where

$$\begin{aligned} \widehat{\Upsilon}_{msd}^1 &= \mathrm{diag}\left\{-Y_d U_{msd}^{-1} Y_d^\top + (\tau_2 - \tau_1 + 1)\overline{R}_d, -\overline{R}_d, -Y_d \overline{\alpha}_s Y_d^\top\right\}, \\ \widehat{\Upsilon}_{msd}^2 &= \left[\varpi_m \widehat{\Upsilon}_{msd}^{2,1\top} \varpi_m \widehat{\Upsilon}_{msd}^{2,2\top} \overrightarrow{\Upsilon}_{msd}^{2,3}\right], \\ \widehat{\Upsilon}_{msd}^{2,1} &= \left[A_m Y_d + (1 - \overline{\alpha}_s) B_m K_d Y_d 0 \overline{\alpha}_s B_m K_d Y_d\right], \\ \widehat{\Upsilon}_{msd}^{2,2} &= \left[-B_m K_d Y_d 0 B_m K_d Y_d\right], \\ \overline{R}_d &= Y_d R Y_d^\top. \end{aligned} \tag{37}$$

On the other hand, with respect to $U_{msd} > 0$, it can be derived that

$$(U_{msd} - Y_d) U_{msd}^{-1} (U_{msd} - Y_d)^\top \geq 0, \tag{38}$$

which equivalents to

$$U_{msd} - \mathbf{sym}\{Y\}_d \geq -Y_d U_{msd}^{-1} Y_d^\top. \tag{39}$$

Similarly, in light of $\overline{\alpha}_s \geq 0$, one can also obtain

$$\overline{\alpha}_s (I - \mathbf{sym}\{Y_d\}) \geq -Y_d (\overline{\alpha}_s I) Y_d^\top. \tag{40}$$

Substituting (40) and (41) into (37) and utilizing Schur complement, (30) can be guaranteed. This completes the proof.

4. Numerical Examples

In the current section, to evaluate the efficiency of the attained methodology, the off-on jumping of circuit breakers subject to Markov switching that is associated with two modes, similar to [9, 11], the parameters are listed as follows:

For Mode $m = 1$

$$A_1 = \begin{bmatrix} 0.9833 & 9.368 & -0.01264 & -1.833 \times 10^{-5} \\ -3.529 \times 10^{-3} & 0.9833 & -2.655 \times 10^{-3} & -5.542 \times 10^{-6} \\ 6.39 \times 10^{-3} & -2.936 \times 10^{-2} & 0.955 & 3.681 \times 10^{-3} \\ -0.2263 & -1.253 & -11.31 & 0.5231 \end{bmatrix},$$
$$B_1 = \left[-1.417 \times 10^{-4} - 5.836 \times 10^{-5} 6.133 \times 10^{-2} 22.27\right]^\top. \tag{41}$$

For Mode $m = 2$

$$A_2 = \begin{bmatrix} 0.9866 & 9.378 & -8.638 \times 10^{-3} & -1.253 \times 10^{-5} \\ -2.837 \times 10^{-3} & 0.9866 & -1.812 \times 10^{-3} & -3.878 \times 10^{-6} \\ 2.054 \times 10^{-3} & -1.243 \times 10^{-2} & 0.9443 & 3.67 \times 10^{-3} \\ -0.6894 & 3.545 & -16.25 & 0.5118 \end{bmatrix},$$
$$B_2 = \left[-9.692 \times 10^{-5} - 3.99 \times 10^{-5} 6.123 \times 10^{-2} 22.15\right]^\top. \tag{42}$$

As stated in [11], a Markov chain is adopted to describe the fault switching in power lines, the transition probabilities are illustrated in Table 2. From which, it is clear that $\Pi = \begin{bmatrix} -0.07 & 0.93 \\ -0.2 & 0.8 \end{bmatrix}$.

Furthermore, the condition TPM Ω with two modes and condition TPM Ξ with three modes are selected as

$$\Omega = \begin{bmatrix} 0.4 & 0.6 \\ 0.5 & 0.5 \end{bmatrix}, \quad \Xi = \begin{bmatrix} 0.1 & 0.4 & 0.5 \\ 0.6 & 0.2 & 0.2 \end{bmatrix}. \tag{43}$$

Meanwhile, choosing $\alpha_1 = 0.5$, $\alpha_2 = 0.2$, $\tau_1 = 1$, and $\tau_2 = 2$. The embedded function of deception attacks is chosen as

$$f\left(x\left(k - \tau_{\varepsilon(k)}(k)\right)\right) = \begin{bmatrix} -\tanh\left(\varrho_1 x_1\left(k - \tau_{\varepsilon(k)}(k)\right)\right) \\ -\tanh\left(\varrho_2 x_1\left(k - \tau_{\varepsilon(k)}(k)\right)\right) \\ -\tanh\left(\varrho_3 x_1\left(k - \tau_{\varepsilon(k)}(k)\right)\right) \\ -\tanh\left(\varrho_4 x_1\left(k - \tau_{\varepsilon(k)}(k)\right)\right) \end{bmatrix}, \tag{44}$$

with $\varrho_1 = 10^{-4}$, $\varrho_2 = 5 * 10^{-4}$, $\varrho_3 = 2 * 10^{-4}$, and $\varrho_4 = 3 * 10^{-4}$. From which, we get the upper bound $Q = 10^{-4} \times \{1, 5, 2, 3\}$. On the basis of conditions in Theorem 2, the controller gains can be computed as

$$\begin{aligned} K_1 &= [\,-0.0546 \;\; 2.0486 \;\; 0.0083 \;\; -0.0010\,], \\ K_2 &= [\,-0.0492 \;\; 1.7493 \;\; 0.0296 \;\; -0.0013\,], \\ K_3 &= [\,-0.0482 \;\; 1.6955 \;\; 0.0334 \;\; -0.0013\,]. \end{aligned} \tag{45}$$

The simulations are plotted in Figure 3, which presents the uncontrolled curves of $x(k)$. The evolution of system mode $\sigma(k)$, dispatcher mode $\varepsilon(k)$, and controller mode $\theta(k)$ are depicted in Figure 4. The random occurring deception attacks and evolution of time-varying delays $\tau_\varepsilon(k)$ are described in Figures 5 and 6, respectively. Under the aforementioned control gains, the state trajectories of the closed-loop dynamic (14) is displayed in Figure 7, and the control input $u(k)$ is exhibited in Figure 8. It can be seen from Figure 8 that the developed methodology works well.

Meanwhile, when $\mathscr{M} = \mathscr{S} = \mathscr{D} = \{2\}$ and TPMs $\Pi = \Omega = \Xi = \begin{bmatrix} -0.07 & 0.93 \\ -0.2 & 0.8 \end{bmatrix}$, the asynchronous controller degrades into the synchronous case. Similarly, the controller gains can be acquired as

$$\begin{aligned} K_1 &= [\,-0.0082 \;\; 0.3773 \;\; 0.0391 \;\; -0.0044\,], \\ K_2 &= [\,-0.0459 \;\; 1.9166 \;\; -0.0047 \;\; -0.0006\,]. \end{aligned} \tag{46}$$

On the basis of the abovementioned controller gains, the state trajectories of closed-loop dynamic (14) are plotted in

Table 2: The transition probabilities.

System reliability	Mode 1	Mode 2
Model 1 (maximum)	0.826	0.174
Model 2 (minimum)	0.00116	0.99884

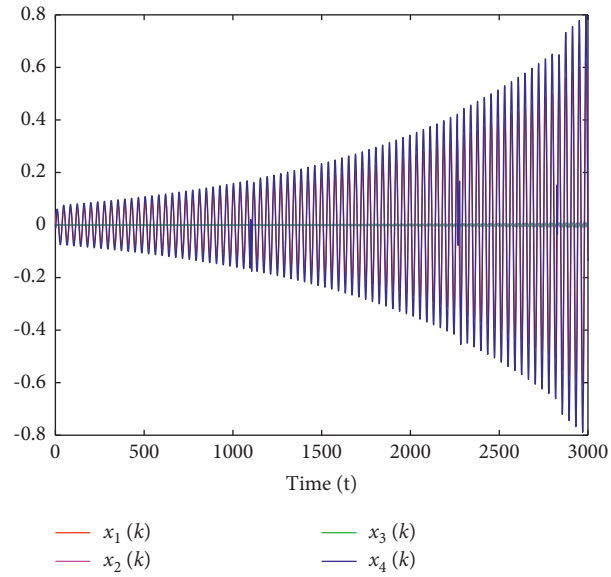

Figure 3: State trajectories of open-loop dynamic (14).

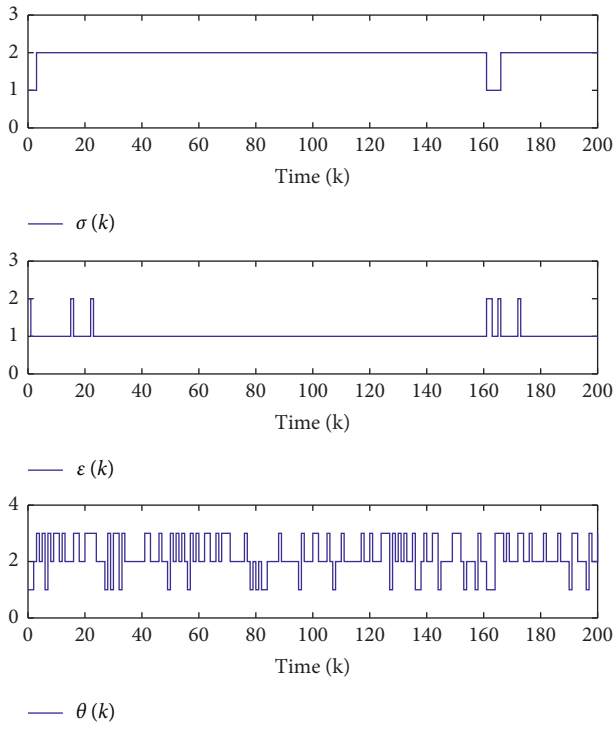

Figure 4: Evolution of modes.

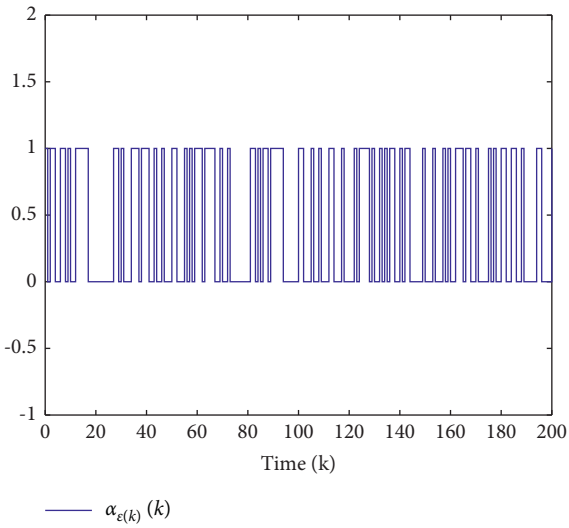

Figure 5: Evolution of $\alpha_{\varepsilon(k)}(k)$.

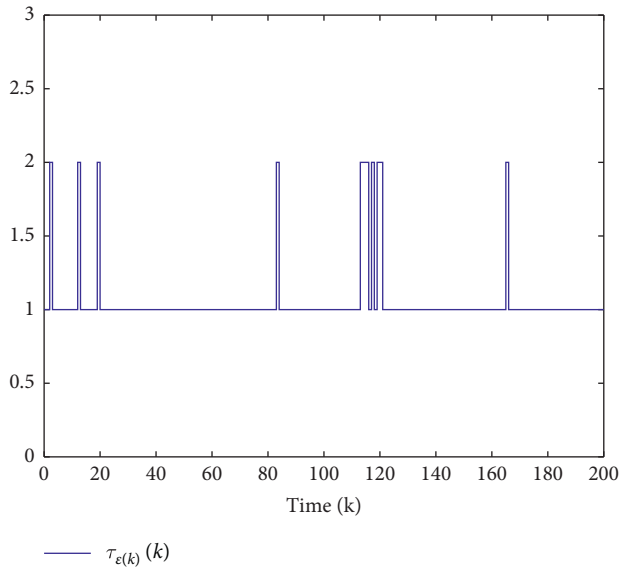

Figure 6: Evolution of time-varying delay.

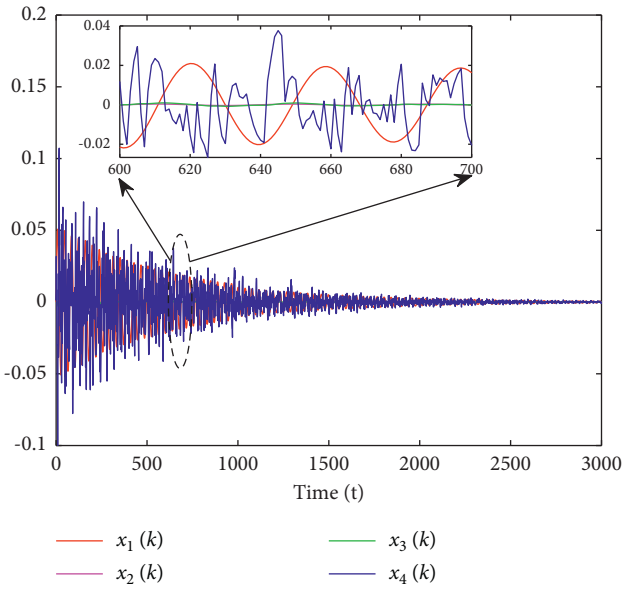

Figure 7: State trajectories of closed-loop dynamic (14).

Figure 9 and the control input $u(k)$ is shown in Figure 10. Clearly, it can be seen from Figures 9 and 10 that the ideal control situation (synchronous control) can achieve better performance.

On the other hand, to further verify the impact of the deception attacks, let $\alpha_{\varepsilon(k)}(k) = 0$, which signifies no deception attacks occur. Similarly, by solving the conditions of Theorem 2, the corresponding gains can be calculated as

$$\begin{aligned} K_1 &= [\,-0.0571 \quad 1.8693 \quad 0.3956 \quad -0.0407\,], \\ K_2 &= [\,-0.0598 \quad 1.9824 \quad 0.3964 \quad -0.0453\,], \\ K_3 &= [\,-0.0597 \quad 2.0021 \quad 0.3918 \quad -0.0458\,]. \end{aligned} \tag{47}$$

Under the aforementioned control gains, the state trajectories of the closed-loop dynamic (14) are displayed in Figure 11 and the control input $u(k)$ is exhibited in

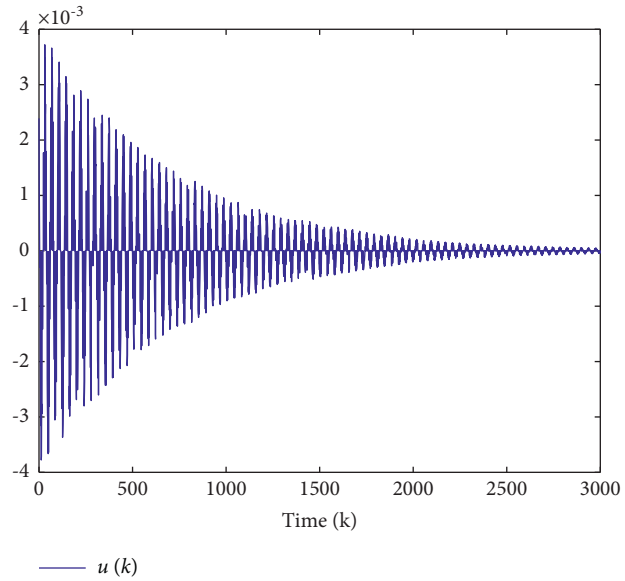

Figure 8: Curve of control input with deception attacks.

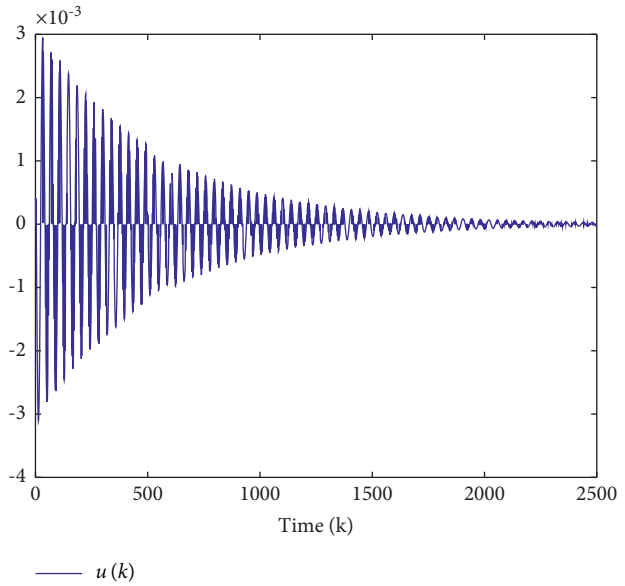

Figure 10: Curve of synchronous control input.

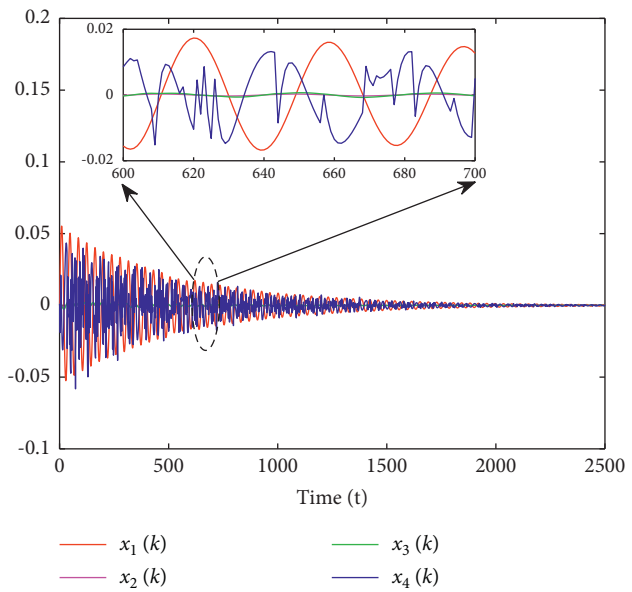

Figure 9: State trajectories of synchronous closed-loop dynamic (14).

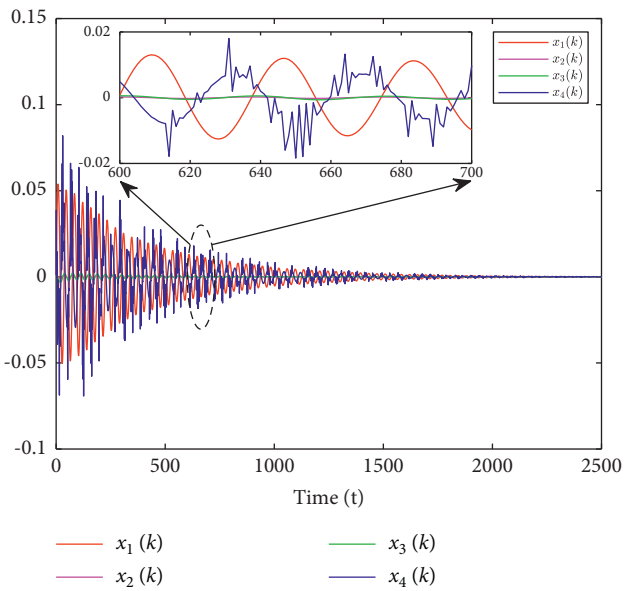

Figure 11: State trajectories of closed-loop dynamic (14) without deception attacks.

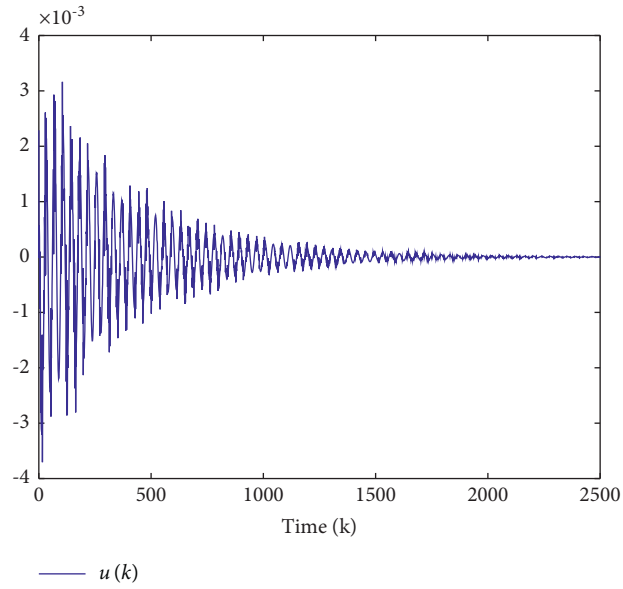

Figure 12: Curve of control input without deception attacks.

Figure 12. From the figures, it is clear that a better performance can be achieved without considering the deception attacks. From which, one concludes that deception attacks degrade the dynamic performance to a certain extent.

5. Conclusion

The problem of power systems being subject to abrupt variations and cyber-attacks has been addressed in the current study. Two hidden Markov models are expressed to characterize the asynchronous phenomena among system mode, dispatcher mode, and controller mode. Furthermore, unlike the existing cyber-attacks, the deception attacks with time-varying delays are regulated by a Markov process. Based on the Lyapunov theory, sufficient conditions are presented to guarantee the stochastic mean-square stability of the closed-loop dynamic. Finally, the proposed control design strategy is testified via a simulation result.

Data Availability

All the data are included within this manuscript.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] W. Kai, F. Xiao, P. Jinbo, R. Jun, D. Chongxiong, and L. Liwei, "State of charge (soc) estimation of lithium-ion battery based on adaptive square root unscented kalman filter," *International Journal of Electrochemical Science*, vol. 15, no. 9, pp. 9499–9516, 2020.

[2] K. Wang, W. Wang, L. Wang, and L. Li, "An improved soc control strategy for electric vehicle hybrid energy storage systems," *Energies*, vol. 13, no. 20, p. 5297, 2020.

[3] X. Feng, Q. Li, and K. Wang, "Waste plastic triboelectric nanogenerators using recycled plastic bags for power generation," *ACS Applied Materials & Interfaces*, vol. 13, no. 1, pp. 400–410, 2020.

[4] Y. Hua, N. Wang, and K. Zhao, "Simultaneous unknown input and state estimation for the linear system with a rank-deficient distribution matrix," *Mathematical Problems in Engineering*, vol. 2021, Article ID 6693690, 11 pages, 2021.

[5] K. Wang, C. Liu, J. Sun et al., "State of charge estimation of composite energy storage systems with supercapacitors and lithium batteries," *Complexity*, vol. 2021, Article ID 8816250, 15 pages, 2021.

[6] C. Liu, Q. Li, and K. Wang, "State-of-charge estimation and remaining useful life prediction of supercapacitors," *Renewable and Sustainable Energy Reviews*, vol. 150, Article ID 111408, 2021.

[7] C. Liu, Y. Zhang, J. Sun, Z. Cui, and K. Wang, "Stacked bidirectional lstm rnn to evaluate the remaining useful life of supercapacitor," *International Journal of Energy Research*, vol. 46, no. 3, 2022.

[8] Z. Cui, L. Wang, Q. Li, and K. Wang, "A comprehensive review on the state of charge estimation for lithium-ion battery based on neural network," *International Journal of Energy Research*, vol. 46, no. 5, 2022.

[9] V. Ugrinovskii and H. R. Pota, "Decentralized control of power systems via robust control of uncertain Markov jump parameter systems," *International Journal of Control*, vol. 78, no. 9, pp. 662–677, 2005.

[10] P. Kundur, "Power system stability," *Power system stability and control*, vol. 10, pp. 7–1, 2007.

[11] F. A. El-Sheikhi, H. M. Soliman, R. Ahshan, and E. Hossain, "Regional pole placers of power systems under random failures/repair Markov jumps," *Energies*, vol. 14, no. 7, p. 1989, 2021.

[12] K. Dehghanpour and S. Afsharnia, "Electrical demand side contribution to frequency control in power systems: a review on technical aspects," *Renewable and Sustainable Energy Reviews*, vol. 41, pp. 1267–1276, 2015.

[13] H. Shayeghi, H. A. Shayanfar, and A. Jalili, "Load frequency control strategies: a state-of-the-art survey for the researcher," *Energy Conversion and Management*, vol. 50, no. 2, pp. 344–353, 2009.

[14] C.-K. Zhang, L. Jiang, Q. H. Wu, Y. He, and M. Wu, "Delay-dependent robust load frequency control for time delay power systems," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 2192–2201, 2013.

[15] H. Shokouhandeh and M. Jazaeri, "Robust design of fuzzy-based power system stabiliser considering uncertainties of loading conditions and transmission line parameters," *IET Generation, Transmission & Distribution*, vol. 13, no. 19, pp. 4287–4300, 2019.

[16] T. Yang, Y. Zhang, W. Li, and A. Y. Zomaya, "Decentralized networked load frequency control in interconnected power systems based on stochastic jump system theory," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 4427–4439, 2020.

[17] J. Cheng, J. H. Park, and Z.-G. Wu, "A hidden Markov model based control for periodic systems subject to singular perturbations," *Systems & Control Letters*, vol. 157, Article ID 105059, 2021.

[18] Y. Wang, H. Pu, P. Shi, C. K. Ahn, and J. Luo, "Sliding mode control for singularly perturbed Markov jump descriptor systems with nonlinear perturbation," *Automatica*, vol. 127, Article ID 109515, 2021.

[19] J. Cheng, L. Liang, J. H. Park, H. Yan, and K. Li, "A dynamic event-triggered approach to state estimation for switched memristive neural networks with nonhomogeneous sojourn probabilities," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 12, pp. 4924–4934, 2021.

[20] J. Cheng, Y. Wang, J. H. Park, J. Cao, and K. Shi, "Static output feedback quantized control for fuzzy Markovian switching singularly perturbed systems with deception attacks," *IEEE Transactions on Fuzzy Systems*, vol. 30, no. 4, pp. 1036–1047, 2022.

[21] A. Ameli, A. Hooshyar, A. H. Yazdavar, E. F. El-Saadany, and A. Youssef, "Attack detection for load frequency control systems using stochastic unknown input estimators," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2575–2590, 2018.

[22] A. Kazemy and M. Hajatipour, "Event-triggered load frequency control of Markovian jump interconnected power systems under denial-of-service attacks," *International Journal of Electrical Power & Energy Systems*, vol. 133, Article ID 107250, 2021.

[23] S. Kuppusamy, Y. H. Joo, and H. S. Kim, "Asynchronous control for discrete-time hidden Markov jump power systems," *IEEE Transactions on Cybernetics*, 2021.

[24] M. Chi, X.-L. Wang, Y. Dou, and Z.-W. Liu, "Intermittent Sampled Data Control for Time-Varying Formation-Containment of the Multiagent System With/without Time Delay," *Complexity*, vol. 2021, Article ID 9971855, 9 pages, 2021.

[25] J. Cheng, J. J. H. Park, Z. G. Wu, and H. Yan, "Ultimate Boundedness Control for Networked Singularly Perturbed Systems with Deception Attacks: A Markovian Communication Protocol Approach," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 2, pp. 445–456, 2022.

[26] W. Zhou, J. Fu, H. Yan, X. Du, Y. Wang, and H. Zhou, "Event-triggered approximate optimal path-following control for unmanned surface vehicles with state constraints," *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–15, 2021.

[27] D. Zhang, Z. Ye, G. Feng, and H. Li, "Intelligent event-based fuzzy dynamic positioning control of nonlinear unmanned marine vehicles under dos attack," *IEEE Transactions on Cybernetics*, pp. 1–14, 2021.

[28] E. I. Bilis, W. Kröger, and C. Cen Nan, "Performance of electric power systems under physical malicious attacks," *IEEE Systems Journal*, vol. 7, no. 4, pp. 854–865, 2013.

[29] Z. Ye, D. Zhang, Z.-G. Wu, and H. Yan, "A3c-based intelligent event-triggering control of networked nonlinear unmanned marine vehicles subject to hybrid attacks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–14, 2021.

[30] D. Ding, Z. Wang, D. W. C. Ho, and G. Wei, "Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks," *Automatica*, vol. 78, pp. 231–240, 2017.

[31] Y. Wu, J. Cheng, X. Zhou, J. Cao, and M. Luo, "Asynchronous filtering for nonhomogeneous Markov jumping systems with deception attacks," *Applied Mathematics and Computation*, vol. 394, Article ID 125790, 2021.

[32] S. Huo and F. Li, "Hidden Markov model-based control for networked fuzzy Markov jump systems against randomly occurring multichannel attacks," *International Journal of Robust and Nonlinear Control*, vol. 31, no. 5, pp. 1657–1673, 2021.

[33] Y. Xu, Z.-G. Wu, and J. Sun, "Security-based passivity analysis of Markov jump systems via asynchronous triggering control," *IEEE Transactions on Cybernetics*, pp. 1–10, 2021.

[34] E. Tian and C. Peng, "Memory-Based event-triggering H ∞ load frequency control for power systems under deception attacks," *IEEE Transactions on Cybernetics*, vol. 50, no. 11, pp. 4610–4618, 2020.

[35] Z. Hu, S. Liu, W. Luo, and L. Wu, "Credibility-based secure distributed load frequency control for power systems under false data injection attacks," *IET Generation, Transmission & Distribution*, vol. 14, no. 17, pp. 3498–3507, 2020.

[36] J. Liu, L. Wei, X. Xie, E. Tian, and S. Fei, "Quantized stabilization for T-S fuzzy systems with hybrid-triggered mechanism and stochastic cyber-attacks," *IEEE Transactions on Fuzzy Systems*, vol. 26, no. 6, pp. 3820–3834, 2018.

[37] Z. Xu, Z.-G. Wu, H. Su, P. Shi, and H. Que, "Energy-to-peak filtering of semi-markov jump systems with mismatched modes," *IEEE Transactions on Automatic Control*, vol. 65, no. 10, pp. 4356–4361, 2019.