Research Article

High-Order Observer-Based Sliding Mode Control for the Isolated Microgrid with Cyber Attacks and Physical Uncertainties

Hao Wang,1 He Jiang,1 Yan Zhao2,1 Huanxin Guan,1 Bo Hu,2 and Shunjiang Wang2

1School of Renewable Energy, Shenyang Institute of Engineering, Shenyang 110136, China
2State Grid Liaoning Electric Power Supply Co., Ltd., Shenyang 110004, China

Correspondence should be addressed to Yan Zhao; zhaoyan@sie.edu.cn

Received 22 October 2020; Revised 16 November 2020; Accepted 2 December 2020; Published 15 December 2020

Abstract
System security is essential for the operation of the island microgrid. However, the system security is generally threatened due to the presence of physical uncertainties and cyber attacks. In this article, a novel sliding mode load control strategy is proposed for the microgrid to mitigate cyber attacks and physical uncertainties. Firstly, a high-order disturbance observer (HODO) is designed to estimate the unmeasurable factors in the microgrid. Secondly, a HODO-based sliding mode control (SMC) strategy is proposed where the estimated value observed by the HODO is applied to the sliding mode surface and control law. It can better guarantee the security of the isolated microgrid. Then, the stability of the HODO-based SMC is demonstrated by Lyapunov stability theory. Finally, simulation results show that the proposed control strategy has excellent control performance.

1. Introduction

The power system is regarded as a critical factor for economic development. With the rapid development of communication equipment, power system application, and energy management system [1–3], power systems merging primary and secondary systems are promoted to transform into the cyber-physical system (CPS). Consequently, the security of the cyber-physical power system has received widespread attention.

CPS security includes the security of physical systems and cyber systems. Physical security is the security of the primary system, which can stabilize the system at scheduled operating point under physical uncertainties. Cyber security means the security of the secondary system which is vulnerable to cyber attacks [4–6]. The insecurity of the cyber-physical power system has a significant impact on the society. For example, in 2019, the primary system of Venezuelan power system became the target of an attack, resulting in a large-scale blackout. In 2003, the secondary system, computer network at the power plant, was hacked in Davis–Besse, USA. On the contrary, the security of the power grid can improve the utilization rate of clean energy power generation and enhance the reliability of the power grid [7, 8].

Because of the integration of advanced measuring devices, application software, and renewable generations, the security of the power system is threatened by serious attacks [9–12]. Multitype intelligent analysis software relies on computers and communication networks, which make the system vulnerable to cyber attacks. Meanwhile, the parameters of physical equipment including generators, turbines, and transmission lines are uncertain. Currently, many critical techniques about cyber attacks, which are the major challenge in the CPS, were studied by scholars. There are some advanced resilient control technologies for cyber attacks [13–15], such as data intrusion attacks [16, 17], nontechnical loss fraud, time-delay attacks [18], and replay attacks. Liu and Li [19] proposed a load distribution attack model with the incomplete acquisition of power system information. In [20], a detection technique was studied for uncertain systems. When the power system was attacked, it can be detected and protected immediately. In [21], a control strategy to protect distributed time-delay power systems was proposed. The method of time-delay estimation was introduced to solve time-delay switch attacks. In recent years,
2 Complexity follows: the power system and controller is considered. Proposed SMC based on the proportional-integral sliding mode surface, and this method proved that the microgrid can be immune to the attacks.

In this paper, a control strategy is investigated. Firstly, a transformed dynamics system is established combining cyber attacks and physical uncertainties as a lumped attack. Secondly, the attack is measured by a high-order nonlinear observer where the attack and its derivatives are observed. Then, compared to the linear sliding surface, an improved sliding surface including the estimation value is proposed. By employing the estimation value, system states are forced to move to the sliding mode surface with the control law. Finally, simulation results on the isolated microgrid are carried out to verify the performance of the controller.

The main contributions of the article are as follows:

1. Considering the characteristic of the power system, the presented HODO can be used to measure the cyber attacks and physical uncertainties in the power system.
2. We construct the sliding mode surface and the control law based on the output of the HODO in the corresponding state space of the microgrid.
3. Using the proposed control strategy, the security of the microgrid will be significantly improved, especially the frequency index.

This paper is organized as follows: in Section 2, the system structure of the microgrid and the dynamic equations are proposed. In Section 3, conventional SMC is illustrated. In Section 4, the control strategy is proposed. Firstly, HODO-based SMC is designed. Secondly, the stability is theoretically proved for the proposed method. The experimental simulation results are demonstrated in Section 5, while the work of this paper is summarized in Section 6.

2. Model of the Cyber-Physical Power System

In this paper, a typical cyber-physical system composed of the power system and controller is considered. The matrix form of the cyber-physical power system is expressed as follows:

\[
\dot{x}(t) = A_n x(t) + B_n u(t) + F_n \Delta P_d,
\]

where

\[
x(t) = \begin{bmatrix} \Delta f(t) \\ \Delta P_g(t) \\ \Delta X_g(t) \end{bmatrix},
\]

\[
A_n = \begin{bmatrix} -\frac{1}{T_p} & \frac{K_p}{T_p} & 0 \\ 0 & -\frac{1}{T_T} & \frac{1}{T_T} \\ \frac{1}{R T_g} & 0 & -\frac{1}{T_g} \end{bmatrix},
\]

\[
B_n = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}^T,
\]

\[
F_n = \begin{bmatrix} K_p & 0 & 0 \end{bmatrix}^T,
\]

\[
\overline{C} = [1 \ 0 \ 0]^T,
\]

where \(x(t)\) is the system state vector; \(A_n, B_n\), and \(F_n\) are system matrices; \(\Delta f(t), \Delta P_g(t), \text{and} \Delta X_g(t)\) are the deviations of frequency, power output, and governor valve position, respectively; \(T_p, T_T, \text{and} T_g\) are the time constants of the power system, turbine, and governor, respectively; \(K_p\) denotes the power system, \(R\) is speed drop; and \(u(t)\) and \(\Delta P_g(t)\) denote the control vector and the cyber attacks, respectively. The formulated cyber-physical power system is similar to that of the literature [25].

Considering the physical uncertainties of the system dynamic model, equation (1) is written as

\[
\dot{x}(t) = (A' + \Delta A)x(t) + (B' + \Delta B)u(t) + (F' + \Delta F)\Delta P_d,
\]

\[
y = \overline{C}x(t),
\]

where \(A', B', \text{and} F'\) are the determined physical system and \(\Delta A, \Delta B, \text{and} \Delta F\) denote the uncertainties of the physical system. Equation (4) is the detailed representation of system dynamics (3):
Complexity

where $k_{mn}$ denotes physical uncertainties.

The system dynamic model with cyber attacks and physical uncertainties can be represented as follows:

$$\Delta f(t) = -\frac{1}{T_p} \Delta f(t) + \frac{K_p}{T_p} \Delta P_g(t) + d_1(x, t),$$

$$\Delta \dot{P}_g(t) = -\frac{1}{T_T} \Delta P_g(t) + \frac{1}{T_T} \Delta X_g(t) + d_2(x, t),$$

$$\Delta X_g(t) = -\frac{1}{RT_g} \Delta f(t) + \frac{1}{T_g} \Delta X_g(t) + \frac{1}{T_g} u(t) + d_3(x, u, t),$$

where

$$d_1(x, t) = k_{11} \Delta f(t) + k_{12} \Delta P_g(t) - \left( \frac{K_p}{T_p} + k_{13} \right) \Delta P_d(t),$$

$$d_2(x, t) = k_{21} \Delta P_g(t) + k_{22} \Delta X_g(t),$$

$$d_3(x, u, t) = k_{31} \Delta f(t) + k_{32} \Delta X_g(t) + k_{33} u(t).$$

Assumption 1. Pair A is observable.

In order to design the observer conveniently, let us transform system dynamics (5) using the transformation matrix. The structure is

$$\dot{\eta}_1 = \eta_2 + d_{11},$$

$$\dot{\eta}_2 = \eta_3 + d_{12},$$

$$\dot{\eta}_3 = \mathcal{C}A^3 T^{-1} \eta + \mathcal{C}A^2 B u + d_{13},$$

where $\eta = T x(t)$ and $T = [\mathcal{C}, \mathcal{C}A, \mathcal{C}A^2]^T$.

The aforementioned system is represented as

$$\dot{\eta} = \mathcal{A}\eta + \mathcal{B} u + F_d d,$$

where $\mathcal{A} = T A T^{-1}$, $\mathcal{B} = T B$, $F_d = T F_d$, and $[d_{11}, d_{12}, d_{13}] = T$.

Assumption 2. The attacks $d_{1i}$ are continuous, and their higher-order derivative with respect to time satisfies

$$\frac{\partial^q d_{1i}(x, t)}{\partial t^q} \leq \chi, \quad q = 0, 1, 2, 3, \ldots, r, \quad i = 1, 2, 3,$$

where $\chi$ is a positive number.

Remark 2. Using a linear nonsingular transformation, system dynamic model (5) can be transformed into system (9). It should be noted that system (9) facilitates the design of HODO-based SMC. Meanwhile, $\eta$ is equivalent to $x(t)$ in simulation analysis.

3. Conventional SMC Design

In the microgrid, the conventional SMC was proposed to ensure system security through secondary frequency regulation of the generator, which adjusts the system to the normal working range with the attacks.

The design of the SMC is composed of two processes: firstly, to design a sliding surface; secondly, to design the control law. The designed sliding surface drives system states to the desired equilibrium asymptotically and remain on it. The system state can be driven to the sliding surface by the designed control law after sufficient time.

3.1. Linear SMC. Based on system dynamic (8), the linear SMC is designed as

$$s_1 = C_1 \eta = \sum_{i=1}^{3} c_i \eta_i,$$

where $C_1 = [c_1, c_2, c_3]$ are constants, and $c_1 = 1$. $c_i$ meets that the polynomial $c_1 + c_2 p + c_3 p^2$, which is Hurwitz, such that the eigenvalues of the polynomial are less than zero.

According to the literature [27], the reaching condition is chosen as $s_1 \eta \eta < 0$. The equality reaching condition is selected as follows:

$$\dot{s}_1 = -k_{d1} s_1 - k_{d2} \text{sign}(s_1),$$

where $k_{d1}$ and $k_{d2}$ are positive numbers and $\text{sign}(\cdot)$ is the sign function.

The control law is designed based on (8), (11), and (12), which drives the system state to the sliding surface:

$$u(t) = -(C_1 \mathcal{B}) \left[ C_1 \mathcal{A} \eta + C_1 \dot{x} + k_{d1} s + k_{d2} \text{sign}(s) \right].$$

3.2. Proportional-Integral SMC. The proportional-integral SMC is presented in this section. The proportional-integral sliding surface is selected as

$$s_2 = C_1 \eta - \int_0^t (C_1 \mathcal{A} - C_1 \mathcal{B} K) \eta dt,$$

where matrix $K$ is designed as $\lambda (C_1 \mathcal{A} - C_1 \mathcal{B} K) < 0$.

Similar to (12), we have

$$\dot{s}_2 = -k_{d3} s_2 - k_{d4} \text{sign}(s_2).$$

The control law is designed as follows:

$$u(t) = -(C_1 \mathcal{B}) \left[ C_1 \mathcal{B} K \eta + C_1 \dot{x} + k_{d3} s_2 + k_{d4} \text{sign}(s_2) \right].$$

However, there are two obvious drawbacks including large overshoot and the lack of estimation for the attack.
4. Methodology

4.1. High-Order Observer for Cyber Attacks and Physical Uncertainties. In this section, an observer is proposed to estimate the attack [28]. In Figure 1, physical attacks $k_{mn}$ appear in the governing system, turbine, and power system. Meanwhile, cyber attacks $\Delta r_{c}(t)$ corrupt the power system. When the system is attacked, the boundaries of the undetectable attack will be directly used in SMC without the HODO. Thus, the control is conservative. The proposed control strategy where the HODO can accomplish the detection of unknown attacks compensates this shortcoming to make the controller output more accurate.

The HODO can estimate the attacks for system (9) as follows:

\[
\begin{bmatrix}
\dot{d}_{11}^{(q-1)} \\
\dot{d}_{12}^{(q-1)} \\
\dot{d}_{13}^{(q-1)} \\
\end{bmatrix} = \begin{bmatrix}
P_{11q} & P_{12q} & P_{13q}
\end{bmatrix} \begin{bmatrix}
\eta_1 \\
\eta_2 \\
\eta_3 \\
\end{bmatrix},
\]

\[
\begin{bmatrix}
\dot{\eta}_1 \\
\dot{\eta}_2 \\
\dot{\eta}_3 \\
\end{bmatrix} = -L_q [\bar{A}\eta + \bar{B}u(t) + \bar{P}_d \tilde{d}] + \begin{bmatrix}
\tilde{d}_{11}^{(q-1)} \\
\tilde{d}_{12}^{(q-1)} \\
\tilde{d}_{13}^{(q-1)} \\
\end{bmatrix},
\]

\[q = 1, 2, 3, \ldots, r - 1,
\]

\[
\begin{bmatrix}
\dot{d}_{11}^{(r-1)} \\
\dot{d}_{12}^{(r-1)} \\
\dot{d}_{13}^{(r-1)} \\
\end{bmatrix} = \begin{bmatrix}
P_{11r} & P_{12r} & P_{13r}
\end{bmatrix} \begin{bmatrix}
\eta_1 \\
\eta_2 \\
\eta_3 \\
\end{bmatrix},
\]

\[
\begin{bmatrix}
\dot{\eta}_1 \\
\dot{\eta}_2 \\
\dot{\eta}_3 \\
\end{bmatrix} = -L_r [\bar{A}\eta + \bar{B}u(t) + \bar{P}_d \tilde{d}]
\]

where $L_q = \begin{bmatrix}
l_{11q} & 0 & 0 \\
0 & l_{12q} & 0 \\
0 & 0 & l_{13q}
\end{bmatrix}$, $q = 1, 2, 3, \ldots, r$, are constant matrices which are necessary to select $L_q > 0$ for the stability of the HODO; $\tilde{d}_{11}^{(q-1)}$ and $\tilde{d}_{1r}^{(r-1)}$ are estimations of $d_{11}^{(q-1)}$ and $d_{1r}^{(r-1)}$, respectively, and $P_{1iq}$ are auxiliary variables ($i = 1, 2, 3; q = 1, 2, 3, \ldots, n$).

The estimation errors are defined as

\[
\tilde{e} = \begin{bmatrix}
\tilde{d}_{11,1} & \tilde{d}_{12,1} & \tilde{d}_{13,1} & \tilde{d}_{11,2} & \tilde{d}_{12,2} & \tilde{d}_{13,2} & \ldots & \tilde{d}_{11,q} & \tilde{d}_{12,q} & \tilde{d}_{13,q}
\end{bmatrix}
\]

where

\[
\tilde{d}_{1i} = d_{1i} - \tilde{d}_{1i},
\]

and $\tilde{d}_{1i}^{(q-1)}$ is the error in the estimation of $d_{1i}^{(q-1)}$. From (8), (17), and (18), it follows that

\[
\begin{bmatrix}
\dot{\tilde{d}}_{11}^{(q-1)} \\
\dot{\tilde{d}}_{12}^{(q-1)} \\
\dot{\tilde{d}}_{13}^{(q-1)} \\
\end{bmatrix} = L_q \begin{bmatrix}
\tilde{d}_{11}^{(q-1)} \\
\tilde{d}_{12}^{(q-1)} \\
\tilde{d}_{13}^{(q-1)} \\
\end{bmatrix}, \quad q = 1, 2, 3, \ldots, r - 1.
\]

Obviously, $[\tilde{d}_{11}^{(q-1)}, \tilde{d}_{12}^{(q-1)}, \tilde{d}_{13}^{(q-1)}]^T = [d_{11}^{(q)}, d_{12}^{(q)}, d_{13}^{(q)}]^T$. Subtracting both sides of equation (23) from $[\tilde{d}_{11}^{(q)}, \tilde{d}_{12}^{(q)}, \tilde{d}_{13}^{(q)}]^T$ yields

\[
\begin{bmatrix}
\dot{\tilde{d}}_{11}^{(q-1)} \\
\dot{\tilde{d}}_{12}^{(q-1)} \\
\dot{\tilde{d}}_{13}^{(q-1)} \\
\end{bmatrix} = L_q \begin{bmatrix}
\tilde{d}_{11}^{(q-1)} \\
\tilde{d}_{12}^{(q-1)} \\
\tilde{d}_{13}^{(q-1)} \\
\end{bmatrix}, \quad q = 1, 2, 3, \ldots, r - 1.
\]

From (19) and (20), we can get
where \( L_q \) is bounded as Assumption 2, the stability of estimation error dynamics can be expressed in the matrix form as

\[
\begin{bmatrix}
\frac{d}{dt} \bar{d}_{11} \\
\frac{d}{dt} \bar{d}_{12} \\
\frac{d}{dt} \bar{d}_{13}
\end{bmatrix} = -L_q \begin{bmatrix}
\bar{d}_{11} \\
\bar{d}_{12} \\
\bar{d}_{13}
\end{bmatrix} + \begin{bmatrix}
d_{11} \\
d_{12} \\
d_{13}
\end{bmatrix} \tag{26}
\]

Differentiating (25) and using (26) give

\[
\begin{bmatrix}
\frac{d}{dt} \bar{d}_{11} \\
\frac{d}{dt} \bar{d}_{12} \\
\frac{d}{dt} \bar{d}_{13}
\end{bmatrix} = - \sum_{q=1}^{r} L_q \begin{bmatrix}
\frac{d^{(r-q)} \bar{d}_{11}}{dt^{(r-q)}} \\
\frac{d^{(r-q)} \bar{d}_{12}}{dt^{(r-q)}} \\
\frac{d^{(r-q)} \bar{d}_{13}}{dt^{(r-q)}}
\end{bmatrix} + \begin{bmatrix}
\frac{d^{(r)} d_{11}}{dt^r} \\
\frac{d^{(r)} d_{12}}{dt^r} \\
\frac{d^{(r)} d_{13}}{dt^r}
\end{bmatrix} \tag{27}
\]

Since \([(d_{11}^T (x, t)/dt^p), (d_{12}^T (x, t)/dt^q), (d_{13}^T (x, t)/dt^r)]^T\) is bounded as Assumption 2, the stability of estimation errors depends on the selection of matrices \( L_q \). The HODO error dynamics can be expressed in the matrix form as

\[
\bar{e} = D_r \bar{e} + E \omega, \tag{28}
\]

where

\[
D_r = \begin{bmatrix}
-L_1 & I_3 & 0 & \cdots & 0 \\
-L_2 & 0 & I_3 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
-L_{p-1} & 0 & 0 & \cdots & I_3 \\
-L_p & 0 & 0 & 0 & 0
\end{bmatrix},
\]

\[
E = \begin{bmatrix}
0 \\
0 \\
\vdots \\
0 \\
I_2 
\end{bmatrix},
\]

\[
\omega = \begin{bmatrix}
d_{11}^T \\
d_{12}^T \\
\frac{d}{dt} d_{13} \\
\frac{d}{dt} d_{13}
\end{bmatrix},
\]

\[
I_3 = \begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{bmatrix}.
\]

In equation (28), the estimation error vector \( \bar{e} \) is illuminated in (21). The derivatives of all vectors in the estimation error vector can be calculated from (25) and (26). From (28), obviously, we can choose appropriate matrix \( L_q (q = 1, 2, 3, \ldots, r) \) such that the eigenvalues of \( D_r \) can be placed arbitrarily. Assume that \( L_q \) are designed to guarantee the eigenvalues of \( D_r \) less than zero. A positive symmetric matrix can be selected as follows:

\[
D_r^T P + PD_r = -Q. \tag{30}
\]

Define a Lyapunov functional, and \( \lambda_{\text{min}} \) is the smallest eigenvalue; then,

\[
V (\bar{e}) = \bar{e}^T P \bar{e}. \tag{31}
\]

Substituting (28) into the derivative of \( V (\bar{e}) \) becomes

\[
\dot{V} (\bar{e}) = \bar{e}^T (D_r^T P + PD_r) \bar{e} + 2 \bar{e}^T P E \omega
\leq -\bar{e}^T Q \bar{e} + 2 \| P E \| \| \bar{e} \| \| \omega \|
\leq -\lambda_{\text{min}} \| \bar{e} \|^2 + 2 \| P E \| \| \bar{e} \| \| \omega \|
= -\| \bar{e} \| \left( \lambda_{\text{min}} \| \bar{e} \| - 2 \| P E \| \| \omega \| \right). \tag{32}
\]

Consequently, for (8), (25), and (26), after sufficiently long time, the norm of the estimation error is ultimately bounded by

\[
\| \bar{e} \| \leq \frac{2 \| P E \| \| \omega \|}{\lambda_{\text{min}}}. \tag{33}
\]

When the error state trajectory enters into the closed ball centered at \( \bar{e} = 0 \) with radius \( q \) and the smallest eigenvalue \( \lambda_{\text{min}} > 0 \), the Lyapunov function satisfies \( \dot{V} (\bar{e}) < 0 \). It implies that the estimation error system is stable. The bound of the estimation error can be lowered by the appropriate choice of the parameter \( L_q (q = 1, 2, 3, \ldots, r) \).

4.2 SMC Based on the HODO. When the system is attacked, SMC is an effective control strategy to guarantee the security of the system. However, the shortcoming is that the conventional SMC method would bring some adverse effects such as introducing overshoot. In this section, a HODO-based SMC is presented. It should be noted that SMC and HODO are designed, respectively.

To be immune to attacks, a linear sliding surface based on the HODO is applied to improve the stability of the power system.

The sliding surface is selected as follows:

\[
s^* = \sum_{i=1}^{3} c_i \eta_i + c_2 \bar{d}_{11} + \bar{d}_{12} + \bar{d}_{13}. \tag{34}\]

**Theorem 1.** Using HODO (17)–(20) and the designed controller law (35), all the states of (9) are ultimately bounded; therefore, the closed-loop system is asymptotically stable around equilibrium with the following control law:
where
\[ \zeta = k_d s^* + k_s \text{sign}(s^*), \]
\[ k_s = \left( \left| c_1 + c_2 l_{111} + l_{112} \right| + (c_2 + l_{121}) + 4 \left\| \bar{e}_1 \right\| + 3 \chi + \theta \right), \]
and \( k_d \) and \( \theta \) are positive constants.

**Proof.** Construct a Lyapunov candidate function as
\[ V(s^*) = \frac{1}{2} s^* s^* . \]

It obviously elicits
\[ \dot{V}(s^*) = s^* s^* . \]

From (9) and (34), it follows that
\[ s^* = c_1 \dot{\eta}_1 + c_2 \dot{\eta}_2 + \dot{\eta}_3 + c_d \dot{d}_{11} + \dot{d}_{11} + \dot{d}_{12} - \zeta. \]

Inserting (35) into (39), we obtain
\[ s^* = (c_1 + c_2 l_{111} + l_{112}) \dot{d}_{11} + (c_2 + l_{121}) \dot{d}_{12} \]
\[ + \dot{d}_{13} + \dot{d}_{11} + \dot{d}_{12} + \dot{d}_{12} - \zeta. \]

According to (24), we have
\[ \begin{align*}
\dot{d}_{11} &= l_{111} \dot{d}_{11} + \ddot{d}_{11} \\
\dot{d}_{12} &= l_{112} \dot{d}_{12} + \ddot{d}_{12} \\
\dot{d}_{13} &= l_{121} \dot{d}_{13} + \ddot{d}_{13} \\
\dot{d}_{11} &= l_{122} \dot{d}_{11} + \ddot{d}_{11} \\
\dot{d}_{12} &= l_{131} \dot{d}_{12} + \ddot{d}_{12} \\
\dot{d}_{13} &= l_{132} \dot{d}_{13} + \ddot{d}_{13}.
\end{align*} \]

Then, substituting (41) to (40), we have
\[ s^* = (c_1 + c_2 l_{111} + l_{112}) \ddot{d}_{11} + (c_2 + l_{121}) \ddot{d}_{12} + \ddot{d}_{13} \]
\[ + \dot{d}_{11} - \ddot{d}_{11} + \dot{d}_{12} - \ddot{d}_{12} + \dot{d}_{11} - \ddot{d}_{11} - \zeta. \]

Substituting (42) into (38), it follows that
\[ \dot{V}(s^*) = s^* \dot{s}^* \leq -k_s \left| s^* \right| - k_d \left| s^* \right|^2 + \left[ (c_1 + c_2 l_{111} + l_{112}) \right] \]
\[ + (c_2 + l_{121}) + 4 \left\| \bar{e}_1 \right\| + 3 \left| s^* \right| \]
\[ < - \theta \left| s^* \right| - k_d \left| s^* \right|^2 < 0. \]

According to (21), \( \bar{e}_1 = [\ddot{d}_{11}, \ddot{d}_{12}, \ddot{d}_{13}, \ddot{d}_{11}, \ddot{d}_{12}, \ddot{d}_{11}] \) is bounded as follows:
\[ \| \bar{e}_1 \| < \| \bar{e}_1 \| \leq \frac{2\| \bar{e}_1 \| \omega}{\lambda_m} . \]
Table 1: The parameters of power systems.

| Parameters | R     | Kp    | Tp    | TR    | TG    |
|------------|-------|-------|-------|-------|-------|
| Values     | 2.7   | 112.5 | 25    | 0.33  | 0.072 |

\[
\begin{align*}
\ddot{d}_{13} &= p_{131} + \dot{l}_{131} \eta_3, \\
\dot{p}_{131} &= -l_{131} (-77.4 \eta_1 - 42.8 \eta_2 - 17 \eta_3 + 189.4u + \ddot{d}_{13}) + \ddot{d}_{13}, \\
\ddot{d}_{13} &= p_{132} + l_{132} \eta_3, \\
\dot{p}_{132} &= l_{132} (-77.4 \eta_1 - 42.8 \eta_2 - 17 \eta_3 + 189.4u + \ddot{d}_{13}) + \ddot{d}_{13}, \\
\ddot{d}_{13} &= p_{133} + l_{133} \eta_3, \\
\dot{p}_{133} &= l_{133} (-77.4 \eta_1 - 42.8 \eta_2 - 17 \eta_3 + 189.4u + \ddot{d}_{13}).
\end{align*}
\]

The control parameters and the initial variables are selected as

\[
c_1 = 8, \\
c_2 = 3, \\
c_3 = 1, \\
k_d = k_{d1} \\
k_e = k_{e1}
\]

\[
x(0) = [0.1, 0, 0]^T.
\]

5.1. Step Cyber Attack. In this case, a step cyber attack is applied without physical uncertainties. Cyber attack is executed to the microgrid, which is 0.1 pu. And the cyber attack is added at the initial time and ends at 5 s. The attack boundary is \( \chi = 0.1 \).

The values are considered as follows:

Parameter 1 (P1): \( l_{111} = l_{121} = l_{131} = 10000 \) and \( l_{112} = l_{122} = l_{132} = 1500 \)

Parameter 2 (P2): \( l_{111} = l_{121} = l_{131} = 10000 \) and \( l_{112} = l_{122} = l_{132} = 1000 \)
We can see that the proposed SMC can ensure system security (especially, frequency deviation). The simulation result is presented in Figure 3. Moreover, it has a small overshoot compared with the conventional SMC at the initial time.

An evaluation index based on frequency deviation is employed to demonstrate HODO’s control performance, which is

\[ f_D = \int_0^t |\Delta f| \, dt. \]  \hspace{1cm} (48)

Table 2 shows the evaluation index of frequency deviation between the conventional SMC and the second-order disturbance observer with different parameters. It can be concluded from Table 2 that the adjustment ability of the second-order disturbance observer is superior to the conventional SMC. Furthermore, the selection of the parameter in the second-order disturbance observer has an improvement on the overshoot.

5.2. Random Cyber Attacks. In this case, the designed SMC with the second-order disturbance observer and third-order disturbance observer is tested in the microgrid. The random external attack is injected into the microgrid, which is \( \Delta P_d(t) = 0.2 \sin(t) \) and ends at 15 s. The parameters of the disturbance observer are as follows:

(a) The second-order disturbance observer:
\[
\begin{align*}
I_{111} &= I_{121} = I_{131} = 500, \\
I_{112} &= I_{122} = I_{132} = 100.
\end{align*}
\]  \hspace{1cm} (49)

(b) The third-order disturbance observer:
\[
\begin{align*}
I_{111} &= I_{121} = I_{131} = 500, \\
I_{112} &= I_{122} = I_{132} = 100, \\
I_{113} &= I_{123} = I_{133} = 25.
\end{align*}
\]  \hspace{1cm} (50)

The plot of the estimation values \( \Delta P_d(t) \) is shown in Figure 4. The disturbance can be tracked in 8 s, while the estimated value accurately estimates the reference disturbance after 10 s. The frequency deviation with the HODO-based SMC is presented in Figure 5.

Using equation (48), we get
\[
\begin{align*}
I_{D1} &= \int_{20}^{22} |\Delta f| \, dt = 0.007, \\
I_{D2} &= \int_{20}^{22} |\Delta f| \, dt = 0.003, \\
I_{D3} &= \int_{20}^{22} |\Delta f| \, dt = 0.0017.
\end{align*}
\]  \hspace{1cm} (51)

where \( I_{D1}, I_{D2}, \) and \( I_{D3} \) represent the evaluation index of the second- and third-order disturbance observer.

It can be concluded that it quickly converges to 0 with the third-order disturbance observer, compared with the effect of the second-order disturbance observer.

5.3. Physical Uncertainties with Cyber Attacks. The stochastic step attack is executed to the microgrid (see Figure 6). Adjust the uncertainty time constant \( T_r \), the governor time constant \( T_g \), and the speed drop \( R \) to 0.38, 0.08, and 2.5 in 20 s, respectively. System uncertainties and cyber attacks occur simultaneously between 15 and 20 seconds. When physical uncertainties appear in the secondary system, the system variables of the microgrid are gradually stable within the limited time by using HODO-based SMC, which are shown in Figure 7.
Figure 4: Actual and estimated attack.

Figure 5: Frequency deviation with the disturbance observer.

Figure 6: Stochastic attack.
6. Conclusion

In this paper, a HODO-based SMC is employed to guarantee the security of the cyber-physical power system. Firstly, HODO is applied to measure cyber attacks and physical uncertainties with matching and unmatching. Secondly, the SMC with the estimated value obtained by the HODO effectively stabilizes the system, furthermore, as compared with the conventional SMC and the proposed control strategy, and the advantage of the HODO-based SMC is small overshoot. In future, further research will be extended to the power-interconnected and time-delay system.

Data Availability

The data used in the research of this article are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by Liaoning Revitalization Talents Program (XLYC1907138), the Natural Science Foundation of Liaoning Province (2019-MS-239), the Doctoral Scientific Research Foundation of Liaoning Province (2020-B5-181), the Key R&D Program of Liaoning Province (2018220017), and the Technology Innovation Talent Fund of Shenyang (RC190360).

References

[1] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber-physical system security for the electric power grid,” *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[2] M. Govindarasu, A. Hann, and P. Sauer, “Cyber-physical systems security for smart grid,” in *Future Grid Initiative White Paper* PSERC Arizona State University, Tempe, AZ, USA, 2012.

[3] Q. Sun, Y. Zhang, H. He, D. Ma, and H. Zhang, “A novel energy function-based stability evaluation and nonlinear control approach for energy internet,” *IEEE Transactions on Smart Grid*, vol. 8, no. 3, pp. 1195–1210, 2017.

[4] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, “A review of false data injection attacks against modern power systems,” *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2017.

[5] B. M. Horowitz and K. M. Pierce, “The integration of diversely redundant designs, dynamic system models, and state estimation technology to the cyber security of physical systems,” *Systems Engineering*, vol. 16, no. 4, pp. 401–412, 2013.

[6] Z. Qu, Y. Zhang, N. Qu, L. Wang, Y. Li, and Y. Dong, “Method for quantitative estimation of the risk propagation threshold in electric power CPS based on seepage probability,” *IEEE Access*, vol. 6, pp. 68813–68823, 2018.

[7] Q. Sun, R. Han, H. Zhang, J. Zhou, and J. M. Guerrero, “A multiagent-based consensus algorithm for distributed coordinated control of distributed generators in the energy internet,” *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 3006–3019, 2015.

[8] A. Giani, E. Bitar, M. Garcia, M. Mcqueen, P. Khargonekar, and K. Poolla, “Smart grid data integrity attacks,” *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1244–1253, 2013.

[9] J. P. Lopes, N. Hatzigiannakis, J. Mutale, P. Dijapic, and N. Jenkins, “Integrating distributed generation into electric power systems: a review of drivers, challenges and opportunities,” *Electric Power Systems Research*, vol. 77, no. 5, pp. 1189–1203, 2007.

[10] Y. Li, H. Zhang, X. Liang, and B. Huang, “Event-triggered-based distributed cooperative energy management for multienergy systems,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 4, pp. 2008–2022, 2019.

[11] F. Blaabjerg, R. Teodorescu, M. Liserre, and A. V. Timbus, “Overview of control and grid synchronization for distributed
power generation systems,” *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1398–1409, 2006.

[12] R. Wang, Q. Sun, D. Ma, and Z. Liu, “The small-signal stability analysis of the droop-controlled converter in electromagnetic timescale,” *IEEE Transactions on Sustainable Energy*, vol. 10, no. 3, pp. 1459–1469, 2019.

[13] L. An and G.-H. Yang, “Improved adaptive resilient control against sensor and actuator attacks,” *Information Sciences*, vol. 423, pp. 145–156, 2018.

[14] W. Ao, Y. Song, and C. Wen, “Adaptive cyber-physical system attack detection and reconstruction with application to power systems,” *IET Control Theory & Applications*, vol. 10, no. 12, pp. 1458–1468, 2016.

[15] Y. Wu, Z. Wei, J. Weng, X. Li, and R. H. Deng, “Resonance attacks on load frequency control of smart grids,” *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4490–4502, 2018.

[16] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, “The 2015 Ukraine blackout: implications for false data injection attacks,” *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.

[17] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, “Evaluation of reinforcement learning-based false data injection attack to automatic voltage control,” *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2158–2169, 2019.

[18] A. Sargolzaei, K. K. Yen, and M. N. Abdelghani, “Control of nonlinear heartbeat models under time-delay-switched feedback using emotional learning control,” *International Journal on Recent Trends in Engineering & Technology*, vol. 10, no. 2, pp. 85–91, 2014.

[19] X. Liu and Z. Li, “Local load redistribution attacks in power systems with incomplete network information,” *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1665–1676, 2014.

[20] H. Wang, J. Ruan, B. Zhou et al., “Dynamic data injection attack detection of cyber physical power systems with uncertainties,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 10, pp. 5505–5518, 2019.

[21] A. Sargolzaei, K. K. Yen, and M. N. Abdelghani, “Preventing time-delay switch attack on load frequency control in distributed power systems,” *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 1176–1185, 2016.

[22] L. Jiang, W. Yao, Q. H. Wu, J. Y. Wen, and S. J. Cheng, “Delay-dependent stability for load frequency control with constant and time-varying delays,” *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 932–941, 2012.

[23] A. Y. Siaramakrishna, M. V. Hariharam, and M. C. Srisailam, “Design of variable structure load-frequency controller using pole assignment technique,” *International Journal of Control*, vol. 40, no. 3, pp. 487–498, 1984.

[24] C.-T. Pan and C.-M. Liaw, “An adaptive controller for power system load-frequency control,” *IEEE Transactions on Power Systems*, vol. 4, no. 1, pp. 122–128, 1989.

[25] C. Mu, W. Liu, W. Xu, and M. Rabiu Islam, “Observer-based load frequency control for island microgrid with photovoltaic power,” *International Journal of Photoenergy*, vol. 2017, Article ID 2851436, 11 pages, 2017.

[26] Y. Mi, Y. Fu, C. Wang, and P. Wang, “Decentralized sliding mode load frequency control for multi-area power systems,” *IEEE Transactions on Power Systems*, vol. 28, no. 4, pp. 4301–4309, 2013.

[27] V. I. Utkin, *Sliding Modes in Control Optimization*, Springer, Berlin, Germany, 1992.

[28] D. Ginoya, P. D. Shendge, and S. B. Phadke, “Sliding mode control for mismatched uncertain systems using an extended disturbance observer,” *IEEE Transactions on Industrial Electronics*, vol. 61, no. 4, pp. 1983–1992, 2014.