Covert Attack Detection for LFC Systems of Electric Vehicles: A Dual Time-Varying Coding Method

Zhihua Wu, Engang Tian, *Member, IEEE*, and Hongtian Chen, *Member, IEEE*

***Abstract*—In recent years, electric vehicles (EVs) have been widely used due to their remarkable decrease in carbon emissions and gasoline consumption. When the EVs are incorporated into the load frequency control (LFC) system, which can be seen as both the power supply and load of the power systems. However, the LFC system with EVs is vulnerable to the covert attacks and consequently the reliable operation performance and security of the power system will be affected. To solve this security issue, the real-time monitoring and detection problems are investigated in this article. First, a networked LFC system with EVs is well established, which takes load disturbances, measurement noises, and covert attacks into account so as to truly reflect the operation process of the power system. Then, an $\mathcal{H}_\infty$ sliding mode observer (SMO) is proposed to accurately estimate the internally physical state of the LFC system with EVs. In order to detect and disclose the covert attacker, a dual time-varying coding detection scheme is proposed, wherein both the control and measurement signals are encrypted before transmitting to the communication network. Subsequently, a dual time-varying coding-based detection algorithm is established, which ensures that the covert attacks can be detected without significant delay. Finally, one simulation is presented to provide tangible evidence of the effectiveness of the proposed real-time monitoring and detection methodology.**

***Index Terms*—Attack detection, load frequency control (LFC), electric vehicles (EVs), covert attacks, sliding mode observer (SMO) design.**

Manuscript received 29 May 2022; revised 25 July 2022; accepted 19 August 2022. Date of publication 9 September 2022; date of current version 18 April 2023. Recommended by Technical Editor Z. Gao and Senior Editor Z. Gao. This work was supported in part by the National Natural Science Foundation of China under Grant 62173231 and Grant 61903252, in part by Natural Science Foundation of Shanghai under Grant 21ZR444900, in part by Program for Professor of Special Appointment Eastern Scholar at Shanghai Institutions of Higher Learning, and in part by the Postgraduate Research & Practice Innovation Program of Jiangsu Province under Grant KYCX18_0299. *(Corresponding author: Hongtian Chen.)*

Zhihua Wu and Engang Tian are with the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China (e-mail: wuzhihua98@163.com; tianengang@163.com).

Hongtian Chen is with the Department of Chemical and Materials Engineering, University of Alberta, Edmonton, AB T6G 1H9, Canada (e-mail: chtbaylor@163.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TMECH.2022.3201875.

Digital Object Identifier 10.1109/TMECH.2022.3201875

I. Introduction

In RECENT years, the electric vehicle (EV) industry is developing at a high speed and has attracted more and more attention from both governments and engineering community because EVs significantly reduce carbon emissions and gasoline consumption [1], [2], which will accelerate the realization of carbon peak and carbon neutralization. Particularly, when the EVs are incorporated into the load frequency control (LFC) system, the power flow between the power system and EVs is bidirectional. That is, the discharging EVs are the power supply of the power system, while the charging EVs are the load of the power system. Consequently, EVs are a good solution to supplement the LFC to maintain the reliable operation performance of the power system [3], [4].

Generally speaking, there are two connection methods to joint different parts of the power system: the private connection and network-based connection. Compared with the private connection, the open network-based connection has the advantages of low-cost and easy expansibility, especially with the access of distributed new energy resources or EVs. Nevertheless, the implementation of the network not only brings convenience, but also makes the LFC system with EVs vulnerable to external cyber-attacks [5], [6]. It is worth noting that, once the malicious attackers successfully launch an attack, serious consequences will be resulted in, including large power outages, destruction of base facilities, data leakage, etc [7], [8]. Therefore, in order to ensure the reliable operation performance of power systems and refrain from enormous losses, it is necessary to develop corresponding real-time monitoring and detection algorithms [9], [10], [11].

In recent years, inspired by fault detection methods [12], [13], [14], a great deal of outstanding literature has been published to detect three representative cyber-attacks: denial-of-service (DoS) attack, replay attack, and false data injection attack [see [15], [16], [17], [18], [19], [20]]. Since the DoS attacks can jam the communication networks [21], they are easily detected in time. In contrast, it is more arduous to expose replay attacks and FDI attacks. Generally speaking, the detection methods for replay attacks and FDI attacks can be divided into learning-based methods [22] and model-based methods [23], [24], [25], [26], [27]. Specifically, learning-based detection methods mainly rely on machine learning technology [28]. The classical support vector machine (SVM) is usually implemented to detect the FDI

attacks [22]. For the model-based methods, an observer is often designed to estimate the state of the system, which is further used to detect the attack through the residual anomaly. For example, a noisy control authentication signal [23] is proposed to detect the replay attack for the first time. In [26], a modified unbiased finite impulse response estimator is proposed to detect deception attacks. More recently, a modified generalized likelihood ratio scheme is designed to detect and estimate the sensor deception attacks in [27].

Particularly, among various FDI attacks, a class of stealthy cyber-attacks, called covert attacks, is designed to destroy the normal running of the NCSs [29]. The covert attack is an extremely powerful attack scheme, which can degrade the system performance severely while remaining the residual under a threshold. To be more specific, attackers will first inject some input signals into the network channel from the controller to actuator so as to destroy the performance of power systems. Then, some well-designed signals are added to the channel between sensor and observer/controller in order to eliminate the effects of input attack. As a consequence, although the performance of the power systems has been damaged, the measurement signals are still identical with the healthy behavior, which makes the covert attack undetectable from the normal detection schemes proposed in the above literature.

Up to now, only few methodologies have been proposed to detect the covert attack [see [30], [31], [32], [33], [34]]. Those methods can be divided into two classes, named moving target-based methods [30], [31] and distributed model-based methods [33], [34]. The main idea of moving target-based method is to alter system dynamics fast enough such that the adversary can not accurately recognize the system models anymore. For example, in [30], a linear discrete-time auxiliary system equipped with a switched Luenberger observer is introduced to reveal covert attacks by preventing attackers from capturing perfect model knowledge. However, since the covert attack can merely be exposed when another subsystem in the auxiliary system is activated, there will be some non-negligible delay in detection. Very recently, a distributed detection strategy is proposed in [32], wherein the covert attack detection of each subsystem depends on its neighborhood. It should be pointed out that the method in [32] is used with the absence of external disturbances and measurement noises, which limits its application. Furthermore, the distributed model-based methods [33], [34] can only be used in large-scale systems.

Summarizing the above discussion, it can be perceived that the research in the area of covert attack detection is still in its infancy and most of the existing methods have their deficiencies, such as performance loss, detection delay, or dynamic coupling between the original physical plant and the auxiliary system. Especially, to the best of the authors' knowledge, the covert attack detection issue has not been thoroughly studied for the LFC systems with EVs, which motivates us to shorten this gap.

In response to above discussion, this article is devoted to making one of the very few attempts to address the covert attack detection issue for the LFC system with load disturbances and measurement noises, the considered problem is nontrivial due to the following challenges. 1) How to design a novel covert detection scheme while avoiding the existing shortcomings is a crucial challenge. Significantly, the existing detection schemes for covert attacks have some shortcomings [30], [31], [32], [33], [34], such as performance loss, detection delay, and dynamic coupling between the original physical plant and the auxiliary system. 2) How to properly handle the load disturbances and measurement noises while guaranteeing the estimation accuracy when designing the observer. Generally speaking, the estimation accuracy of the system state is extremely significant so as to effectively detect the covert attack. As shown in [35], [36], the estimation deviation of internally physical state will result in wrong judgment. In order to provide solutions to the above challenges, the key contributions of this article are highlighted as follows:

1) A networked LFC system with EVs is well established, which covers load disturbances, measurement noises, covert attacks, and dual time-varying coding mechanism in a unified framework.
2) An $\mathcal{H}_\infty$ sliding mode observer (SMO) is properly designed to accurately estimate the state of the LFC system while considering load disturbances and measurement noises. Compared with the traditional Luenberger-like observer [33], [37], the estimation error in the designed SMO can be smoothly adjusted to a boundary due to the following two reasons: one is that the influence of load disturbances are compensated, and the other is that the $\mathcal{H}_\infty$ performance constraint is satisfied.
3) A novel dual time-varying coding detection scheme (DTVCDS) is, for the first time, proposed to detect covert attacks successfully and promptly. Compared with some existing detection schemes [30], [31], [32], [33], [34], [38] the remarkable advantages of the proposed approach are that systems performance loss and dynamic coupling (between the original physical plant and the auxiliary system) are skillfully avoided, and the attack detection scheme has good scalability.

The rest of this article is organized as follows. In Section II, we present the dynamic model of the LFC system with EVs, the characteristics of the covert attack, and the stealthy effects of the covert attacks. In Section III, an $\mathcal{H}_\infty$ SMO and DTVCDS are proposed. In Section IV, simulation results are presented to testify the validity of the proposed detection mechanism. Finally, Section V concludes this article.

II. Preliminaries

In this section, we will first establish the dynamic model of the LFC systems with EVs. The considered system model takes the load disturbances and measurement noises into consideration in this article in order to truly reflect the actual operation of the power system [39]. Then, the attack scheme and the concealment of covert attacks are presented. Finally, the addressing detection problem of covert attacks is formulated.

A. The Dynamic Model of the LFC System With EVs

The structure of the considered system is shown in Fig. 1. The power system consists of turbines, generators, governors,

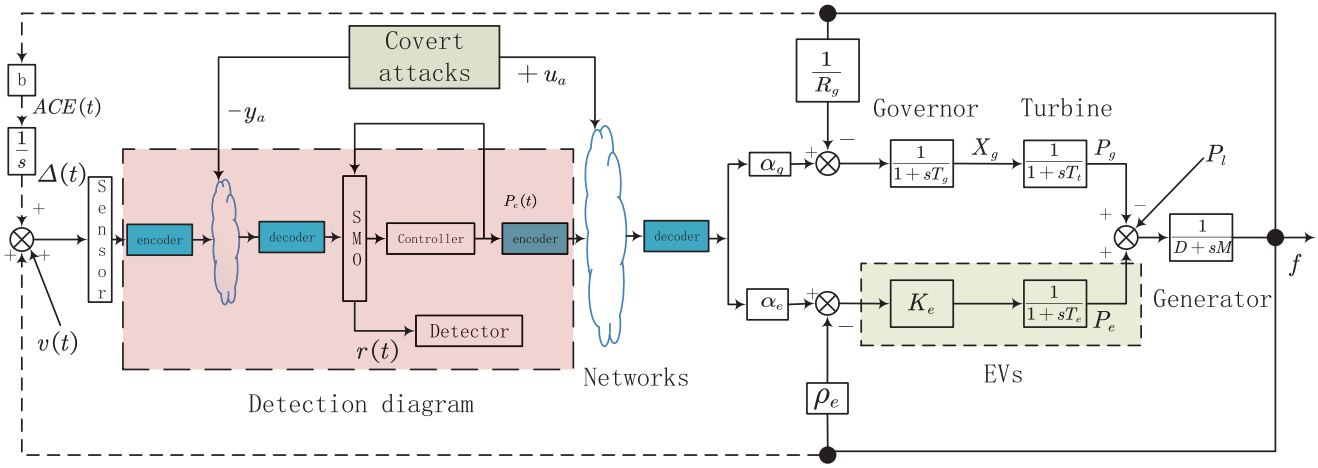

Fig. 1. Diagram of the LFC system with EVs under covert attacks.

and EVs, wherein the EVs participate in the LFC scheme in the second frequency control (SFC) of the power system and quickly compensate for the imbalance between load and power generation to improve the operation flexibility and the frequency stability of power system.

According to the information flow and transfer function presented in Fig. 1, the following equations are deduced:

$$\begin{cases} f(s) = \frac{1}{D+sM}(P_g(s) + P_e(s) - P_l(s)) \\ X_g(s) = \frac{1}{1+sT_g}(\alpha_g P_c(s) - \frac{1}{R_g} f(s)) \\ P_g(s) = \frac{1}{1+sT_t} X_g(s) \\ P_e(s) = \frac{K_e}{1+sT_e}(\alpha_e P_c(s) - \rho_e f(s)) \\ \Delta(s) = \frac{1}{s} ACE(s) = \frac{1}{s} b f(s). \end{cases} \tag{1}$$

where f, X_g, P_g, P_e, P_l, P_c, α_g, and α_e denote the frequency deviation, governor valve position, turbine output power, incremental change in EVs, load disturbance, control input, thermal turbine, and EVs participation factor, respectively. D, M, R_g, ρ_e, T_g, T_t, K_e, T_e, and b are the load damping coefficient, inertia constant, governor, and EVs droop characteristic, speed governor, and turbine time constant, EVs gain constant, time constant, and frequency bias constant, respectively. $\mathrm{ACE}(s) = bf(s)$ is the area error control, which is used to maintain zero steady-state error for frequency deviation, and $\Delta(s)$ is the integration of the area control error. By using the inverse Laplace transform with (1) and defining $x^T(t) = [f(t), X_g(t), P_g(t), P_e(t), \Delta(t)]$, $y^T(t) = [f(t), \Delta(t)]$, $u(t) = P_c(t)$, and $\omega(t) = P_l(t)$ as the state vector, measurement output, control input, and load disturbances, respectively, the state-space representation of the LFC system with EVs can be expressed as

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + H\omega(t) \\ y(t) = Cx(t) + v(t) \end{cases} \tag{2}$$

where

$$A = \begin{bmatrix} -\frac{D}{M} & 0 & \frac{1}{M} & \frac{1}{M} & 0 \\ -\frac{1}{R_g T_g} & -\frac{1}{T_g} & 0 & 0 & 0 \\ 0 & \frac{1}{T_t} & -\frac{1}{T_t} & 0 & 0 \\ -\frac{\rho_e K_e}{T_e} & 0 & 0 & -\frac{1}{T_e} & 0 \\ b & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$B^T = \begin{bmatrix} 0 & \frac{\alpha_g}{T_g} & 0 & \frac{\alpha_e K_e}{T_e} & 0 \end{bmatrix} \tag{3}$$

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$H^T = \begin{bmatrix} -\frac{1}{M} & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Assumption 1: Load disturbance $\omega(t)$ is unknown but bounded and measurement noise $v(t)$ is square integrable, i.e., $\forall t \geq 0$, there exist known scalars $\bar{\omega}$ satisfying that

$$\|\omega(t)\| \leq \bar{\omega}, \int_0^\infty v^T(s) v(s) ds < \infty. \tag{4}$$

A static output feedback (SOF) controller is chosen as

$$u(t) = -Ky(t). \tag{5}$$

It is not difficult to find that the SOF controller merely needs the output information rather than the state information whose true value is usually difficult to obtain. Therefore, the SOF controller is easier to be implemented. Moreover, the control gain K is a constant matrix, which can be designed by the pole placement method.

B. Model of Covert Attacks

The covert attack is an extremely powerful attack scheme, which is assumed to have the capability of intercepting the transmitted data (disclosure capability), capturing model knowledge, and arbitrary changing the transmitted data into a new compatible vector. The main threaten of covert attack lies in its stealthiness, that is, it can degrade the system performance while cannot be detected by traditional methods. Actions of the covert

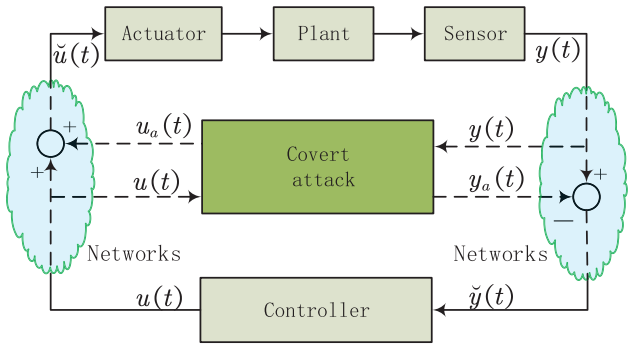

Fig. 2. Structure of covert attacks for linear plants.

attack operate as follows (see Fig. 2): in the forward channel, an attack signal $u_a(t)$ is added to destroy the performance of the systems, while, in the feedback channel, an appropriately designed signal $y_a(t)$ is injected to eliminate the influence of the bad effect of the attack signal $u_a(t)$ on the measurement output. As shown in Fig. 2, the covert attack on the communication channels are modeled as follows:

$$\begin{aligned}\breve{u}(t) &= u(t) + u_a(t)\\ \breve{y}(t) &= y(t) - y_a(t)\end{aligned} \tag{6}$$

where $u_a(t) \in \mathbb{R}$, $y_a(t) \in \mathbb{R}^2$, $\breve{u}(t) \in \mathbb{R}$, and $\breve{y}(t) \in \mathbb{R}^2$ denote arbitrary attack signals injected in forward channel, well-designed attack signals added to feedback channel, the control input signals received by power systems, the measured output signals received by LFC, respectively.

In order to achieve the covert purpose, the malicious attacker executes the following dynamic system:

$$\begin{cases}\dot{\breve{x}}(t) = A\breve{x}(t) + Bu_a(t)\\ y_a(t) = C\breve{x}(t)\end{cases} \tag{7}$$

where $\breve{x}(t) \in \mathbb{R}^5$ is the attacker's own system state.

Assuming that the attack starts at time $t_a \geq 0$, motivated by [33], the following proposition will demonstrate the principle of the stealthiness of the covert attack.

Proposition 1: Suppose that the attacker has perfect knowledge of (A, B, C), 1) if A is Hurwitz, the existence of $y_a(t)$ can be properly designed by the attacker to make the attack covert as $t \to \infty$. 2) If the attacker chooses $\breve{x}(t_a) = 0$, the attack will be covert for all the moments and for any $\forall A \in \mathbb{R}^{5\times 5}$.

Proof: For $0 < t < t_a$, since the attack is not launched, i.e., $u_a(t) = y_a(t) = 0$, it is obvious that

$$\begin{aligned}y(t) = \breve{y}(t) = Ce^{At}x(0) + C\int_0^t e^{A(t-s)}\\ \times [Bu(s) + H\omega(s)]\,\mathrm{d}s + v(t)\end{aligned} \tag{8}$$

For $t \geq t_a$, if there are no cyber attack, the measured output signal should be

$$\begin{aligned}y_{att-free}(t) = Ce^{A(t-t_a)}x(t_a) + C\int_{t_a}^t e^{A(t-s)}\\ \times [B(u(s) + H\omega(s)]\,\mathrm{d}s + v(t).\end{aligned} \tag{9}$$

On the other side, the measured output under covert attacks can be written as

$$\begin{aligned}y_{att}(t) = Ce^{A(t-t_a)}x(t_a) + C\int_{t_a}^t e^{A(t-s)}\\ \times [B(u(s) + u_a(s)) + H\omega(s)]\,\mathrm{d}s + v(t).\end{aligned} \tag{10}$$

Subsequently, recalling the attack model (7), $y_a(t)$ can be computed as

$$y_a(t) = Ce^{A(t-t_a)}\breve{x}(t_a) + C\int_{t_a}^t e^{A(t-s)}Bu_a(s)\,\mathrm{d}s. \tag{11}$$

Then, if we subtract (11) from (10), the measured output signal received by LFC can be written as

$$\begin{aligned}\breve{y}(t) = Ce^{A(t-t_a)}(x(t_a) - \breve{x}(t_a))\\ + C\int_{t_a}^t e^{A(t-s)}[Bu(s) + H\omega(s)]\,\mathrm{d}s + v(t).\end{aligned} \tag{12}$$

The purpose of the covert attacker is make the attacked signal $\breve{y}(t)$ equal to the measured output signal without attack $y_{\text{att}-\text{free}}(t)$. If this is true, the attack effect on the measured output can be eliminated. Comparing (9) with (12), we can found that, first, if $\breve{x}(t_a)) = 0$, we are ready to reach the conclusion that $\breve{y}(t) = y_{\text{att}-\text{free}}(t)$. Else, if A is Hurwitz, we can conclude that $\breve{y}(t) = y_{\text{att}-\text{free}}(t)$ when $t \to \infty$. ■

Remark 1: Proposition 1 illustrates that by properly designing the attack signal $y_a(t)$, the covert attack does not affect the measured output signals, i.e., the attack is stealth for the detection method depending on the measured output. Since the attack dynamic system (7) is designed by the attacker, it is natural to choose the initial state as $\breve{x}(t_a) = 0$ to highlight the stealthy characteristics of the attack. Therefore, in practical engineering practice, the covert attack is easier to launch attacks, avoid detection, and cause serious system damages.

C. Effects of Covert Attack

In this part, we will demonstrate that the covert attack is invisible through the traditional residual-based detection method. First, the physical dynamic model of the LFC system with EVs under the covert attack can be expressed as follows:

$$\begin{cases}\dot{\tilde{x}}(t) = A\tilde{x}(t) + B(u(t) + u_a(t)) + H\omega(t)\\ \breve{y}(t) = C\tilde{x}(t) - y_a(t) + v(t)\end{cases} \tag{13}$$

where $\tilde{x}(t) \in \mathbb{R}^5$ is the attacked system state, $u_a(t) \in \mathbb{R}$ is the attack signal to destroy the performance of power system, and $y_a(t) \in \mathbb{R}^2$ is produced by (7) to eliminate the input attack effect on the measurement.

In order to detect cyber-attacks from the perspective of cybernetics, the classical means is to introduce an observer to estimate the current state $\hat{x}(t)$, the output $\hat{y}(t)$, and generate a residual signal $r(t)$, a residual-based detection logic is provided as [40]

$$\begin{cases}r(t) = y(t) - \hat{y}(t)\\ \|r(t)\| \leq \bar{r} \Rightarrow \text{nominal}\\ \|r(t)\| > \bar{r} \Rightarrow \text{attacked}\end{cases} \tag{14}$$

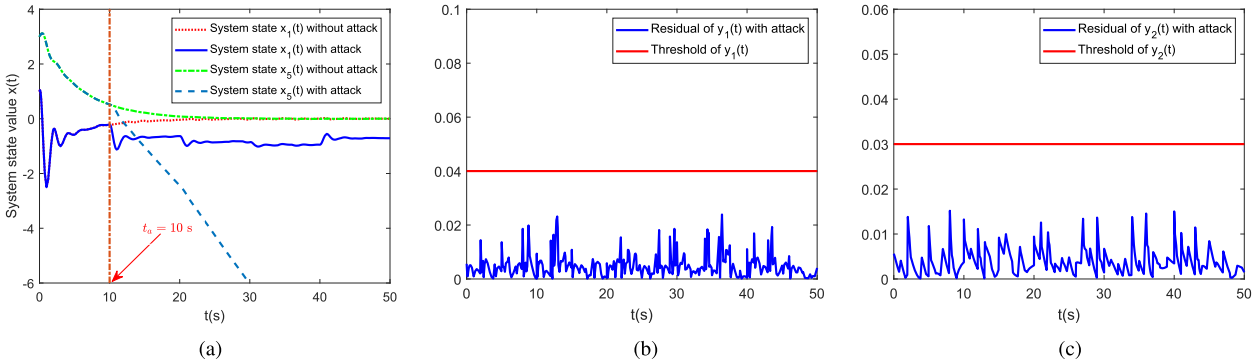

Fig. 3. Simulation results of Example 1: detection of covert attacks for the LFC system with EVs under the residual-based detection technique. (a) Change of state under covert attacks. (b) Detection residual r_1 under covert attacks. (c) Detection residual r_2 under covert attacks.

where $y(t)$ is the actual measured output, $\hat{y}$ is the estimated output, and $\bar{r}$ is the upper bound of $r(t)$. If the residual signal is larger than $\bar{r}$, we believe that the system is under attack.

Remark 2: In order to avert a high false alarm rate, let us select $\bar{r} = \tilde{r} + \vec{r}$, where $\tilde{r}$ represents a threshold acquired by considering the generated residual in attack-free conditions. $\vec{r}$ is a constant, which is chosen to reduce the false alarm rate. Generally speaking, the threshold $\bar{r}$ is often obtained by Monte Carlo experiments under different operating conditions in engineering practice [14]. Furthermore, supposing that at minimum one component j of $r(t)$, $\bar{r}$ subject to $|r_j| > \bar{r}_j$, we assume that the system is under cyber attack, which makes detection logic more sensitive to offsets of each component.

Next, to show the concealment of the covert attack, the following example is proposed.

Example 1: Supposing that the attacker starts injecting covert attacks at $t_a = 10$ s, the attack signal is the same as (43) of Case 1 in the Section IV. The corresponding matrix parameters are taken in [39]. As depicted in Fig. 3 , the simulation results testify the powerful destructive and stealthy characteristics of the covert attack. According to Fig. 3(a), we can perceive that the state of LFC system with EVs has changed significantly after $t = 10$ s (due to space constraints, we only present the change of $x_1(t)$ and $x_5(t)$ here). Nevertheless, the corresponding residual does not exceed the precomputed threshold $\bar{r}$, as shown in Fig. 3(b) and (c). That is to say, covert attacks easily alter the internally physical state of the LFC system with EVs and spoof the detection scheme triumphantly.

Compared with the traditional cyber-attacks, the above attacks are more destructive and stealthy. Therefore, the purpose of this article is to promptly detect the covert attack via designing a SMO and constructing a DTVCDS to avoid damaging the normal operation of the system.

III. Detection Procedure

In this section, a dual coding attack detection framework is established for the covert attack. First, an $\mathcal{H}_\infty$ SMO is proposed, which can estimate the system state more accurately than the Luenberger-like one [37]. Furthermore, the observer gains can be computed by solving a set of linear matrix inequalities. Then, a DTVCDS is proposed to expose the covert attacks. Two pairs of encoder–decoder are preprogrammed in the forward and feedback communication channels, which is not affected by load disturbances and external noises. Both the measured output signals and control input signals are coded before they are sent to the network, and which are decoded after they are used by the next nodes (i.e., observer and control nodes). In this way, the covert attack can be exposed successfully. The design details of the SMO and DTVCDS are presented in the following sections.

A. SMO Design

For the LFC systems with EVs in (2), we design the following SMO:

$$\begin{cases} \dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + L(y(t) - \hat{y}(t)) + \alpha(t) \\ \hat{y}(t) = C\hat{x}(t) \end{cases} \tag{15}$$

where $\hat{x}(t)$ is the estimated state vector, $L \in \mathbb{R}^{5\times 2}$ is the observer gain to be designed later, and $\alpha(t) \in \mathbb{R}^5$ is a function to compensate for the load disturbance $P_l(t)$ (i.e., $\omega(t)$).

Defining the estimation error as $e(t) = x(t) - \hat{x}(t)$, if there is no attacks in the system, the estimation error dynamics can be written as

$$\dot{e}(t) = (A - LC)e(t) + H\omega(t) - Lv(t) - \alpha(t). \tag{16}$$

The main objectives of the $\mathcal{H}_\infty$ SMO are listed as follows:

1) Design the observer gain such that the estimation error system (16) is asymptotically stable when the external disturbance is zero.
2) Design the function $\alpha(t)$ to compensate the influence of the load disturbance $P_l(t)$ (i.e., $\omega(t)$).
3) The influence from the measurement noise $v(t)$ to the estimation error $e(t)$ is constrained as

$$\int_0^\infty e^T(t)e(t)dt < \gamma^2 \int_0^\infty v^T(t)v(t)dt \tag{17}$$

where γ is $\mathcal{H}_\infty$ performance index.

To facilitate the derivation of the main results, we present the following lemma.

Lemma 1: The $\mathcal{H}_\infty$ performance constraint (17) is satisfied if for a Lyapunov candidate function $V(t)$, $J = \dot{V}(t) + e^T(t)e(t) - \gamma^2 v^T(t)v(t)$ is negative definite [41].

For given observer gain L, by using Lemma 1, sufficient conditions for the asymptotically stable and the $\mathcal{H}_\infty$ performance of the estimation error system in (16) are derived in the following theorem.

Theorem 1: For given parameters L and $\gamma > 0$, system (16) is asymptotically stable with $\mathcal{H}_\infty$ norm bound γ, if there exist matrix $P > 0$ and scalar $\beta > 0$ such that the following condition is satisfied:

$$\begin{bmatrix} \Xi & -PL & I \\ * & -\gamma^2 I & 0 \\ * & * & -I \end{bmatrix} < 0 \tag{18}$$

where

$$\Xi = P(A - LC) + (A - LC)^T P + \beta I \tag{19}$$

$$\begin{cases} \alpha(t) = \bar{\omega}^2 \beta^{-1} \frac{\|PH\|^2}{2r^T(t)r(t)} P^{-1} C^T r(t), if\ r(t) \neq 0 \\ \alpha(t) = 0, if\ r(t) = 0 \end{cases} \tag{20}$$

and $r(t)$ is the residual signal defined in (14).

Proof: According to Lemma 1, to satisfy the asymptotically stable and the $\mathcal{H}_\infty$ performance of the estimation error system, we should have

$$J = \dot{V}(t) + e^T(t)e(t) - \gamma^2 v^T(t)v(t) < 0. \tag{21}$$

By selecting $V = e^T(t)Pe(t)$ and taking derivative of V, we have

$$\begin{aligned} J = {} & e^T(t)P(A - LC)e(t) + e^T(t)(A - LC)^T Pe(t) \\ & + \omega^T(t)H^T Pe(t) + e(t)^T PH\omega(t) + e^T(t)e(t) \\ & - v^T(t)L^T Pe(t) - e^T(t)PLv(t) - \alpha^T(t)Pe(t) \\ & - e^T(t)P\alpha(t) - \gamma^2 v^T(t)v(t). \end{aligned} \tag{22}$$

If $r(t) = 0$, $r(t) = 0$ implies that $e(t) = 0$ since the system is observable. Therefore, (21) is established.

Next, we analyze the case where $r(t) \neq 0$.

By utilizing Assumption 1, one obtains

$$\begin{aligned} & \omega^T(t)H^T Pe(t) + e(t)^T PH\omega(t) \\ & \leq \beta e^T(t)e(t) + \beta^{-1}\omega^T(t)H^T PPH\omega(t) \\ & \leq \beta e^T(t)e(t) + \beta^{-1}\|PH\|^2\bar{\omega}^2. \end{aligned} \tag{23}$$

According to (20), we have the following expressions:

$$-\alpha^T(t)Pe(t) - e^T(t)P\alpha(t) = -\bar{\omega}^2\beta^{-1}\|PH\|^2. \tag{24}$$

Subsequently, combining (22)–(24), we have

$$\begin{aligned} J \leq {} & e^T(t)P(A - LC)e(t) + e^T(t)(A - LC)^T Pe(t) \\ & + \beta e^T(t)e(t) - 2e^T(t)PLv(t) + e^T(t)e(t) \\ & - \gamma^2 v^T(t)v(t) \\ = {} & \begin{bmatrix} e^T(t) & v^T(t) \end{bmatrix} \begin{bmatrix} \Xi_1 & -PL \\ * & -\gamma^2 I \end{bmatrix} \begin{bmatrix} e(t) \\ v(t) \end{bmatrix} \end{aligned} \tag{25}$$

where $\Xi_1 = P(A - LC) + (A - LC)^T P + \beta I + I$. By using Schur complement, we can conclude that if the condition (18) is established, condition (21) is also satisfied. The proof of this theorem is now complete. ■

Now, we are in a position to calculate the observer gain L, which is shown in the following theorem.

Theorem 2: For given scalar $\gamma > 0$, system (16) is asymptotically stable with $\mathcal{H}_\infty$ norm bound γ, if there exist matrix $P > 0$, matrix S with appropriate dimension and scalar $\beta > 0$ such that the following condition is satisfied:

$$\begin{bmatrix} \Xi_2 & -S & I \\ * & -\gamma^2 I & 0 \\ * & * & -I \end{bmatrix} < 0 \tag{26}$$

where $\Xi_2 = PA - SC + A^T P - C^T S^T + \beta I$. Additionally, The observer gain can be computed as

$$L = P^{-1}S. \tag{27}$$

Proof: Define $S = PL$, condition (26) can be easily obtained from (18). ■

Remark 3: We can perceive from (20) that the magnitude of $\alpha(t)$ may increase without bound when the residual $r(t)$ is quite small. This phenomenon is overcame as follows [42]:

$$\begin{cases} \alpha(t) = \bar{\omega}^2 \beta^{-1} \frac{\|PH\|^2}{2r^T(t)r(t)} P^{-1} C^T r(t), if\ \|r(t)\| \geq \epsilon \\ \alpha(t) = 0, if\ \|r(t)\| < \epsilon \end{cases} \tag{28}$$

where ϵ is a threshold chosen by utilizing the cut-and-try approach. Therefore, the residual $r(t)$ can be bound to ϵ, which will improve the sensitivity of the residual-based detection technology to cyber attacks.

Remark 4: It is worth noting that the discontinuous function $\alpha(t)$ is used to compensate for the load disturbance, and the $\mathcal{H}_\infty$ technique is employed to damp measurement noises. Thus, the estimation effect of SMO in (15) is better than the conventional Luenberger-like observer.

In the simulation part, we compare the estimation effects of SMO with conventional Luenberger-like observer from two perspectives. Although it is common to reconstruct the state of the system using SMO [42], [43], [44], it is the first attempt to develop the SMO for the LFC system with EVs while considering the load disturbances and measurement noises, and combine the SMO with DTVCDS to reveal the covert attacks. Furthermore, it should be pointed out that (16) holds in the case of attack-free. Next, we will analyze the estimation error dynamics for the SMO (15) when the LFC system with EVs is under covert attacks.

Proposition 2: Supposing LFC system with EVs (2) be under the covert attack described in (6) and (7), the residual signal $r'(t)$ and the error dynamics for the SMO (15) are expressed as follows:

$$r'(t) = C\check{e}(t) + v(t) \tag{29}$$

$$\dot{\check{e}}(t) = (A - LC)\check{e}(t) + H\omega(t) - Lv(t) - \alpha(t). \tag{30}$$

Proof: By combining (2), (6), and (7), we obtain

$$r'(t) = \check{y}(t) - C\hat{x}(t) = C\check{e}(t) + v(t). \tag{31}$$

By utilizing (15), one obtain

$$\begin{aligned}\breve{e}(t) &= \dot{x}(t) - \dot{\breve{x}}(t) - \dot{\hat{x}}(t)\\ &= Ax(t) + B(u(t) + u_a(t)) + H\omega(t) - A\breve{x}(t) - Bu_a(t)\\ &\quad - A\hat{x}(t) - Bu(t) - L(\breve{y}(t) - \hat{y}(t)) - \alpha(t)\\ &= (A - LC)\breve{e}(t) + H\omega(t) - Lv(t) - \alpha(t).\end{aligned} \tag{32}$$

The proof of this proposition is now completed. ■

We observe that (16) and (30) are identical, which once again shows the concealment of the attack.

In the next section, a DTVCDS is proposed to successfully detect the covert attacks.

B. Dual Time-Varying Coding Detection Scheme

In Proposition 2, we have demonstrated that covert attacks can be designed to bypass the detector (14). Motivated by [45], a DTVCDS is proposed to expose covert attacks. Our main idea is to design two pairs of encoders and decoders to limit the attacker's disclosure capability. Then, the attackers can not completely eliminate the influence of the additive attack signal $u_a(t)$ by calculating the resulting output and subtracting $y_a(t)$ from the sensor readings. Hence, the corrupted measurement output $\breve{y}(t)$ is distinguishable from the healthy response $y(t)$, i.e., the output residual $r(t)$ will change significantly and exceed the predesigned threshold.

As show in Fig. 1, a pair of time-varying encoder and decoder are established in the forward channel. The control signal $u(t)$ is coded into $U(t)$ before sending to the network

$$U(t) = \Phi(t)u(t) \tag{33}$$

where $\Phi(t)$ is a time-varying coding matrix with proper dimension, and for any fixed t, $\Phi(t)$ is invertible. In practice, owing to the time-varying property of $\Phi(t)$, the coding matrix $\Phi(t)$ can not be accurately distinguished by the attacker. When the malicious attacker starts injecting attack signals as (6) and (7) without the knowledge of the time-varying coding matrix, the corrupted control signal changes to

$$\breve{U}(t) = \Phi(t)u(t) + u_a(t). \tag{34}$$

Before the control signal enters the power system, $\breve{U}(t)$ is decoded as

$$\breve{U}'(t) = u(t) + \Phi^{-1}(t)u_a(t). \tag{35}$$

Similarly, a pair of time-varying encoder and decoder are established in the feedback channel, and the measured output signal is coded before it is transmitted to the network. Therefore, the corrupted measured output is

$$\breve{Y}(t) = y(t) \otimes \varphi(t) - y_a(t) \tag{36}$$

where $\varphi(t)$ is the time-varying coding matrix and $\otimes$ denotes the Hadamard vector product.

Before the measurement signal enters the LFC controller, $\breve{Y}(t)$ is decoded as

$$\breve{Y}'(t) = \breve{Y}(t) \oslash \varphi(t) = y(t) - y_a(t) \oslash \varphi(t) \tag{37}$$

where $\oslash$ denotes the Hadamard vector division.

Next, we will prove that, if there are no attacks in the closed-loop system, the proposed DTVCDS will not disturb the normal running of the LFC systems with EVs, i.e., the system performance degradation caused by the noise control detection scheme in [23] is effectively eliminated.

Proposition 3: Considering the structure architecture in Fig. 1, if there are no cyber attacks in the LFC systems with EVs, the proposed DTVCDS has no effect on the normal operation of the considered systems.

Proof: Under an attack-free scenario, that is, $u_a(t) \equiv 0$ and $y_a(t) \equiv 0$. According to (35), the signal $\breve{U}'(t)$ is recovered as

$$\breve{U}'(t) = u(t) + \Phi^{-1}(t)u_a(t) \equiv u(t) \tag{38}$$

and according to (37), we can write the signal $\breve{Y}'(t)$ as

$$\breve{Y}'(t) = \breve{Y}(t) \oslash \varphi(t) = y(t) - y_a(t) \oslash \varphi(t) \equiv y(t). \tag{39}$$

This completes the proof.

Theorem 3: Considering the LFC systems with EVs, if there are covert attacks in the systems, the estimation error dynamic is expressed as follows:

$$\dot{\breve{e}}'(t) = (A - LC)\breve{e}'(t) + H\omega(t) - Lv(t) - \alpha(t) + \Sigma(t) \tag{40}$$

where $\Sigma(t) = B(\Phi^{-1}(t) - I)u_a(t) + LC\breve{x}' \oslash \varphi(t) - LC\breve{x}'$, that is, by using of the DTVCDS, the estimation error in (40) is different from that in (30). In another word, if we appropriate select the functions $\Phi(t)$ and $\varphi(t)$, $\Sigma(t)$ will be big enough such that the residual signal will be detected by the attack detector, which makes the covert attack reveal.

Proof: By combining (2), (15), (35), and (37), we have

$$\begin{aligned}\dot{\breve{e}}'(t) &= \dot{x}'(t) - \dot{\breve{x}}'(t) - \dot{\hat{x}}'(t)\\ &= Ax'(t) - A\breve{x}'(t) - A\hat{x}'(t) + B(\Phi^{-1} - I)u_a(t)\\ &\quad - L(y'(t) - y_a(t) \oslash \varphi(t) - \hat{y}'(t)) + H\omega(t) - \alpha(t)\\ &= (A - LC)\breve{e}'(t) + H\omega(t) - Lv(t) - \alpha(t) + \Sigma(t).\end{aligned} \tag{41}$$

It should be noted that (41) is different from (16) and (30). In other words, by using the DTVCDS, the estimation error is different after the covert attack. Since $r'(t) = C\breve{e}'(t) + v(t)$, the residual will change correspondingly, which makes the covert attack loses its stealth features. ■

Remark 5: Covert attacks will be successful if the attacker can eliminate the influence to output $y(t)$ caused by $u_a(t)$. However, in the proposed detection diagram, time-varying coding matrices $\Phi(t)$ and $\varphi(t)$ are both unknown to the attacker. The attack signal entering the power system changes from $u_a(t)$ to $\Phi^{-1}(t)u_a(t)$. Therefore, the attacker cannot simply exploit $y_a(t)$ to perfectly cancel the influence of $u_a(t)$, not to mention relying on $y_a(t) \oslash \varphi(t)$. Furthermore, the time-varying coding matrices $\Phi(t)$ and $\varphi(t)$ can be designed as $C\tilde{x}(t) - y_a(t) \oslash \varphi(t) \gg Cx(t)$ in order to enhance the residual signal sensitivity to $u_a(t)$. Ultimately, the attacker's actions will be exposed before the residual-based detector (14). In addition, it is worth mentioning that the above DTVCDS is not affected by the system uncertainty

and the $\mathcal{H}_\infty$ SMO has strong robustness, which ensures the scalability of the proposed detection scheme.

Remark 6: As analyzed in Remark 5, by selecting proper parameters in the proposed DTVCDS, residual signals will increase abruptly and timely. Then, the covert attack is exposed instantaneously by the detection scheme. In [30], a linear discrete-time auxiliary system equipped with a switched Luenberger observer is proposed to expose covert attacks. The covert attack can merely be exposed after another subsystem in the auxiliary system is activated. Therefore, the detection speed is highly dependent on the switching speed of the subsystem. In other words, the detection is realized with some delay when the switching point of the subsystem is different from the starting point of the attack. As shown in [30], the covert attack can be detected with a time delay 2000s after the attack occurred. Therefore, our detection mechanism is more sensitive than the existing approach in [30].

Remark 7: In the proposed DTVCDS, the encoders and decoders should have the knowledge of the time-varying coding signal simultaneously. For the simplicity of implementation, the time-varying parameters can be replaced by periodic varying ones taking values in a finite set. In a word, this periodic coding scheme is not only easy to implement in engineering, but also difficult to be recognized by attackers, which can successfully detect covert attacks and is obviously superior to the random coding scheme.

C. Dual Time-Varying Coding Detection Algorithm

By means of above discussion, a residual-based dual time-varying coding detection algorithm against covert attacks is summarized in Algorithm 1.

Algorithm 1: Dual Time-Varying Coding Detection Algorithm.

Input: the initial values $x(0)$, γ, $\bar{\omega}$, ϵ, $\bar{r}$, $a=0$, T, T', $t_i(i=1,2,\ldots,T)$, $t'_j(j=1,2,\ldots,T')$, $\Phi(t)$ and $\varphi(t)$.

Construct the physical dynamic equations of the LFC system with EVs in (2)→parameters (A,B,C,H,ω,v,x,y) and design the SOF controller in (5);
Design the SMO in (15) that satisfies the $\mathcal{H}_\infty$ performance constraint simultaneously;
Design DTVCDS as (33), (35), (36) and (37);
Based on (15), state parameters of the LFC system with EVs are obtained;
Computer the residuals r_i for all components of $y(t)$;
for $l \in (1,2)$ **do**
  if $|r_l| > \bar{r}_l$ **then**
    $a = a+1$,
  else
    $a = a$,
  end if
end for
if $a > 0$ **then**
  There exist attacks in the LFC system with EVs;
else
  No attacks in the LFC system with EVs;
end if

Output: Record the attacked LFC system with EVs.

IV. Illustrative Example

In this part, for the sake of demonstrating the validity of the designed detection mechanism, a power system with LFC is considered under the covert attack. Some electrical parameters of the system are chosen from [39], the initial state is set to $x(0)=[1,0,0.2,0,3]^T$, and other parameters are $\gamma=2.5$, $\beta=2$, and $\epsilon=0.01$. In the progress of actual operations, the load disturbance $\omega(t)$ and sensor noise $v(t)$ are random variables for $t\in[0,50]$ independently uniformly distributed in the following interval: $\omega(t),v_1(t),v_2(t)\in[-0.01,0.01]$. When $t\in[50,\infty)$, the load disturbance $\omega(t)$ still obeys the uniform distribution of the above interval and the sensor noise $v(t)$ is 0.

A SOF controller is designed to maintain the power system nominal frequency (for instance, 60 Hz in China and North America). The controller gain is designed as $K=[0.0775,0.3872]$. By solving the LMI (26), a steady-state gain L is computed as:

$$L^T=\begin{bmatrix} 2.7883 & -2.0964 & -0.8793 & 0.4089 & 0.1749 \\ 0.9212 & -0.6489 & -0.3910 & 0.1345 & 0.6185 \end{bmatrix}.$$

The corresponding simulation results of the proposed SMO and Luenberger observer are displayed in Fig. 4 (due to space constraints, we only show the estimation effect of $x_1(t)$ here).

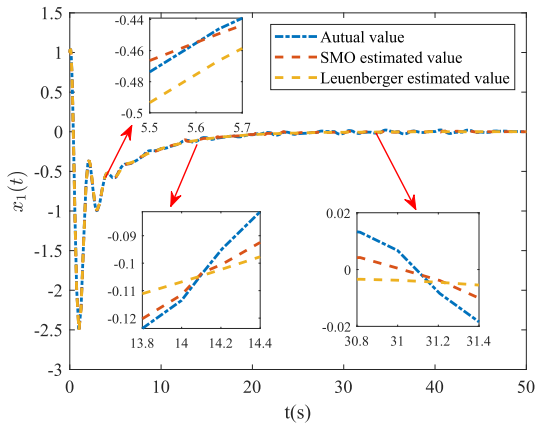

Fig. 4. State trajectories of $x_1(t)$ by using different observers.

From the simulation, it can be found that the estimation accuracy of SMO in (15) is better than the Luenberger observer [37].

Furthermore, we employ the root-mean-square error (RMSE) as a measure to evaluate the accuracy of two observers. The RMSE is defined as follows:

$$\mathrm{RMSE}(x_i)=\sqrt{\frac{1}{N}\sum_{t=1}^{N}(x_i-\hat{x}_i)^2},\quad i=1,2,\cdots,5 \quad (42)$$

where x_i, $\hat{x}_i$ and $\mathrm{RMSE}(x_i)$ are the ith state, the ith estimated state and the RMSE of the ith state, respectively. N is the total number of samples time. Table I lists the comparison results of $\mathrm{RMSE}(x_1)$, $\mathrm{RMSE}(x_2)$, and $\mathrm{RMSE}(x_3)$ for the proposed

TABLE I
COMPARISON OF RMSE FOR THE TWO OBSERVERS

Method	RMSE(x_1)	RMSE(x_2)	RMSE(x_3)
Luenberger observer [37]	0.012053	0.005421	0.004465
Proposed SMO	0.008967	0.004613	0.003985
Relative improvement	25.59%	14.90%	10.75%

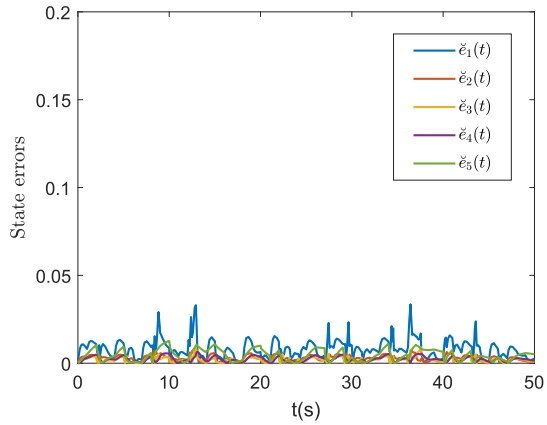

Fig. 5. State errors received by the SMO without DTVCDS.

SMO and the Luenberger observer [37]. We observe that the proposed SMO can produce better performance and the relative improvements are 25.59%, 14.90%, and 10.75%, respectively. Obviously, by using the proposed SMO, more accurate residuals are obtained, which will be conducive in detecting covert attacks.

For the sake of validating the effectiveness of the proposed DTVCDS for different covert attack signals, the following two cases are considered.

Case 1: Suppose the covert attacker launches an attack at $t_a = 10$ s, and the injected attack $u_a(t)$ is as follows:

$$u_a(t) = \begin{cases} 0, & 0 \le t < 10 \\ -0.5, & 10 \le t < 20 \\ -0.7, & 20 \le t < 30 \\ -0.8, & 30 \le t < 40 \\ -0.6, & 40 \le t \le 50 \end{cases}. \tag{43}$$

The attack signal $y_a(t)$ is generated by (7).

A residual-based detector shown in (14) is used in the simulation scenario. The detector thresholds are $\bar{r}_1 = 0.04$ and $\bar{r}_2 = 0.03$. To show the effectiveness of the proposed detection mechanism, first, if the DTVCDS is not employed, the state error with covert attacks are shown in Fig. 5. Obviously, as shown in Fig. 5, there is no evident change trend before and after the attack. That is, the covert attack can not be detected by using the residual signals.

By using the proposed DTVCDS, the time-varying coding parameters are designed as follows:

$$\varphi(t) = \begin{cases} [1.254\ 1]^T; & 0 \le t < 10s \\ [1.205\ 1]^T; & 10s \le t < 30s \\ [1.123\ 1]^T; & 30s \le t < 50s \end{cases}$$

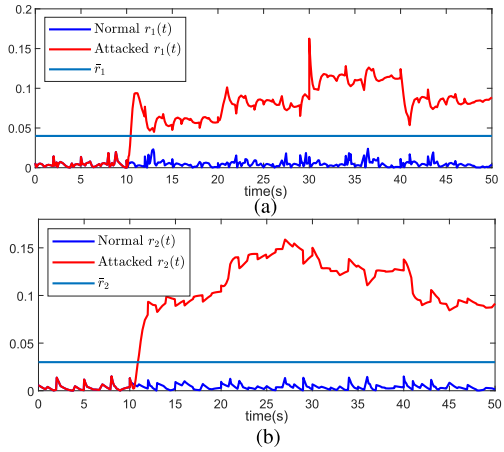

Fig. 6. Simulation results of the DTVCDS (a) Case 1: Trajectory of $r_1(t)$. (b) Case 1: Trajectory of $r_2(t)$.

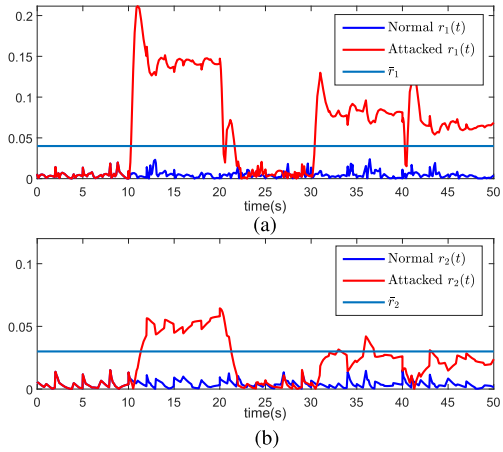

Fig. 7. Simulation results of the UTVCDS (a) Case 1: Trajectory of $r_1(t)$. (b) Case 1: Trajectory of $r_2(t)$.

$$\Phi(t) = \begin{cases} 0.837; & 0 \le t < 10s \\ 0.725; & 10s \le t < 30s \\ 0.755; & 30s \le t < 50s \end{cases}$$

The simulation results based on the detection method proposed in this article are shown in Fig. 6. In the attack-free case, the residuals of $y_1(t)$ and $y_2(t)$ (i.e., $|r_1|$ and $|r_2|$) are close to zero and do not exceed the threshold. It means that the proposed SMO and DTVCDS will not influence the residual signals without cyber attacks.

In case of a covert attack (43), we perceive that the threshold is exceeded for the residuals $|r_1|$ and $|r_2|$ at approximately $t_1 = 10.45$ and $t_2 = 10.88$ s, respectively. That is, the attack is detected less than 1s. In order to further highlight the advantages of DTVCDS, we implement a set of comparison experiments, that is, only using unilateral time-varying coding schemes (UTVCDS). The corresponding simulation results are shown in Fig. 7. We can perceive that the UTVCDS can also detect attacks, but there are many missed alarms that are usually prohibited in

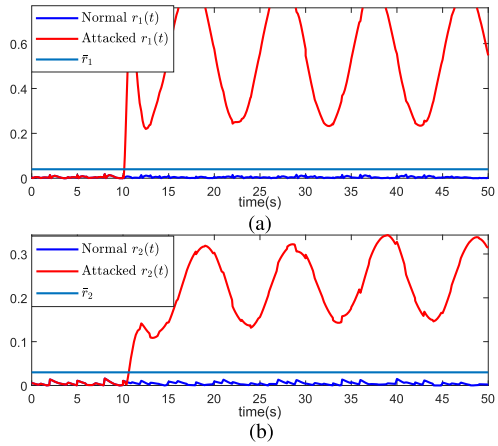

Fig. 8. Simulation results of the DTVCDS (a) Case 2: Trajectory of $r_1(t)$. (b) Case 2: Trajectory of $r_2(t)$.

engineering practice. Then, we can conclude that our detection scheme is effective and sensitive to the covert attacks.

Case 2: Consider a time-varying attack signal $u_a(t)$ as

$$u_a(t) = \begin{cases} 0, & 0 \le t < 10 \\ 0.3sin(\frac{\pi}{5}t) - 0.6, & 10 \le t \le 50. \end{cases} \tag{44}$$

Meanwhile, a well-designed attack signal $y_a(t)$ is generated by (7). The corresponding simulation results are displayed in Fig. 8. When there is no cyber-attack in the system, the residuals of $y_1(t)$ and $y_2(t)$ (i.e., blue lines in Fig. 8) do not exceed the threshold. Nevertheless, when there are covert attacks in the system, the residuals of $y_1(t)$ and $y_2(t)$ (i.e., red lines in Fig. 8) exceed the threshold rapidly. As a consequence, the time-varying covert attack in this case can be detected by the proposed detector.

From the above two cases, the validity of the proposed real-time monitoring and detection mechanism for the two kinds of covert attacks can be illustrated.

V. Conclusion

In this article, we have established a networked LFC system with EVs model in which the EVs have been embedded in the power system to hoist the support ability of load balance. Subsequently, an $\mathcal{H}_\infty$ SMO has been designed to accurately estimate the internally physical state of the power system, which is more effective than the Luenberger-like observer in some existing works. In order to restrict the attacker's disclosure capability, a dual time-varying coding detection algorithm has been proposed to reveal the attack. At last, a power system instance has demonstrated that the designed real-time monitoring and detection scheme can successfully expose covert attacks and is sensitive to covert attacks.

References

[1] S. Kim and S. B. Choi, "Cooperative control of drive motor and clutch for gear shift of hybrid electric vehicles with dual-clutch transmission," *IEEE/ASME Trans. Mechatronics*, vol. 25, no. 3, pp. 1578–1588, Jun. 2020.

[2] J. Guo et al., "Takagi–Sugeno fuzzy-based robust $\mathcal{H}_\infty$ integrated lane-keeping and direct yaw moment controller of unmanned electric vehicles," *IEEE/ASME Trans. Mechatronics*, vol. 26, no. 4, pp. 2151–2162, Aug. 2021.

[3] H. Yang, C. Y. Chung, and J. Zhao, "Application of plug-in electric vehicles to frequency regulation based on distributed signal acquisition via limited communication," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1017–1026, May 2013.

[4] S. Izadkhast et al., "An aggregate model of plug-in electric vehicles including distribution network characteristics for primary frequency control," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 2987–2998, Jul. 2016.

[5] C. Peng, J. Li, and M. Fei, "Resilient event-triggering $\mathcal{H}_\infty$ load frequency control for multi-area power systems with energy-limited DoS attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 4110–4118, Sep. 2017.

[6] E. Tian and C. Peng, "Memory-based event-triggering $\mathcal{H}_\infty$ load frequency control for power systems under deception attacks," *IEEE Trans. Cybern.*, vol. 50, no. 11, pp. 4610–4618, Nov. 2020.

[7] F. Farivar et al., "Covert attacks through adversarial learning: Study of lane keeping attacks on the safety of autonomous vehicles," *IEEE/ASME Trans. Mechatronics*, vol. 26, no. 3, pp. 1350–1357, Jun. 2021.

[8] S. Hu et al., "Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks," *IEEE Trans. Cybern.*, vol. 49, no. 12, pp. 4271–4281, Dec. 2019.

[9] L. Liu et al., "Distributed non-fragile set-membership filtering for nonlinear systems under fading channels and bias injection attacks," *Int. J. Syst. Sci.*, vol. 52, no. 6, pp. 1192–1205, 2021.

[10] J. Hu et al., "A survey on sliding mode control for networked control systems," *Int. J. Syst. Sci.*, vol. 52, no. 6, pp. 1129–1147, 2021.

[11] D. Ding et al., "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 5, pp. 779–789, May 2018.

[12] H. Chen et al., "Data-driven designs of fault detection systems via neural network-aided learning," *IEEE Trans. Neural Netw. Learn. Syst.*, early access, Apr. 14, 2021, doi: 10.1109/TNNLS.2021.3071292.

[13] Z. Gao, C. Cecati, and S. X. Ding, "A survey of fault diagnosis and fault-tolerant techniques—Part I: Fault diagnosis with model-based and signal-based approaches," *IEEE Trans. Ind. Electron.*, vol. 62, no. 6, pp. 3757–3767, Jun. 2015.

[14] H. Chen et al., "Data-driven fault diagnosis for traction systems in high-speed trains: A survey, challenges, and perspectives," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 1700–1716, Mar. 2022.

[15] J. Cao et al., "Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks," *Inf. Sci.*, vol. 548, pp. 69–84, 2021.

[16] S. Zhu et al., "An adaptive torus-event-based controller design for networked T-S fuzzy systems under deception attacks," *Int. J. Robust Nonlinear Control*, vol. 32, no. 6, pp. 3425–3441, Apr. 2022.

[17] X. Xu et al., "Robust reset speed synchronization control for an integrated motor-transmission powertrain system of a connected vehicle under a replay attack," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5524–5536, Jun. 2021.

[18] D. Ding et al., "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, Jan. 2018.

[19] X. Ge et al., "Distributed Krein space-based attack detection over sensor networks under deception attacks," *Automatica*, vol. 109, Nov. 2019, Art. no. 108557.

[20] F. Qu, E. Tian, and X. Zhao, "Chance-constrained $\mathcal{H}_\infty$ state estimation for recursive neural networks under deception attacks and energy constraints: The finite-horizon case," *IEEE Trans. Neural Netw. Learn. Syst.*, early access, Jan. 7, 2022, doi: 10.1109/TNNLS.2021.3137426.

[21] X.-M. Zhang et al., "Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3616–3626, Aug. 2020.

[22] M. Esmalifalak et al., "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.

[23] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396–1407, Jul. 2014.

[24] Z.-H. Pang et al., "Detection of stealthy false data injection attacks against networked control systems via active data modification," *Inf. Sci.*, vol. 546, pp. 192–205, 2021.

[25] X. Wang et al., "Detection and isolation of false data injection attacks in smart grid via unknown input interval observer," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3214–3229, Apr. 2020.
[26] Z. Ju, H. Zhang, and Y. Tan, "Deception attack detection and estimation for a local vehicle in vehicle platooning based on a modified UFIR estimator," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3693–3705, May 2020.
[27] Z. Ju, H. Zhang, and Y. Tan, "Distributed deception attack detection in platoon-based connected vehicle systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 4609–4620, May 2020.
[28] S. Liu et al., "Online active learning for drifting data streams," *IEEE Trans. Neural Netw. Learn. Syst.*, early access, Jul. 21, 2021, doi: 10.1109/TNNLS.2021.3091681.
[29] R. Smith, "Covert misappropriation of networked control systems: Presenting a feedback structure," *IEEE Control Syst.*, vol. 35, no. 1, pp. 82–92, Feb. 2015.
[30] C. Schellenberger and P. Zhang, "Detection of covert attacks on cyber-physical systems by extending the system dynamics with an auxiliary system," in *Proc. IEEE 56th Annu. Conf. Decis. Control*, 2017, pp. 1374–1379.
[31] M. Ghaderi, K. Gheitasi, and W. Lucia, "A blended active detection strategy for false data injection attacks in cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 1, pp. 168–176, Mar. 2021.
[32] A. Barboni et al., "Distributed detection of covert attacks for interconnected systems," in *Proc. 18th Eur. Control Conf.*, 2019, pp. 2240–2245.
[33] A. Barboni et al., "Detection of covert cyber-attacks in interconnected systems: A distributed model-based approach," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3728–3741, Sep. 2020.
[34] A. J. Gallo et al., "A distributed cyber-attack detection scheme with application to DC microgrids," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3800–3815, Sep. 2020.
[35] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, 2010, pp. 226–231.
[36] J. Hu, Z. Wang, and H. Gao, "Joint state and fault estimation for time-varying nonlinear systems with randomly occurring faults and sensor saturations," *Automatica*, vol. 97, pp. 150–160, 2018.
[37] X. Luo et al., "Observer-based cyber attack detection and isolation in smart grids," *Int. J. Elect. Power Energy Syst.*, vol. 101, pp. 127–138, 2018.
[38] P. Griffioen, S. Weerakkody, and B. Sinopoli, "An optimal design of a moving target defense for attack detection in control systems," in *Proc. IEEE Amer. Control Conf.*, 2019, pp. 4527–4534.
[39] T. N. Pham et al., "Static output feedback frequency stabilization of time-delay power systems with coordinated electric vehicles state of charge control," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3862–3874, Sep. 2017.
[40] K. Manandhar et al., "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.
[41] E. Tian et al., "Chance-constrained $\mathcal{H}_\infty$ control for a class of time-varying systems with stochastic nonlinearities: The finite-horizon case," *Automatica*, vol. 107, pp. 296–305, 2019.
[42] H. Zhang, G. Zhang, and J. Wang, "$\mathcal{H}_\infty$ observer design for LPV systems with uncertain measurements on scheduling variables: Application to an electric ground vehicle," *IEEE/ASME Trans. Mechatronics*, vol. 21, no. 3, pp. 1659–1670, Jun. 2016.
[43] A. Akhenak et al., "Design of sliding mode unknown input observer for uncertain Takagi–Sugeno model," in *Proc. IEEE Mediterranean Conf. Control Automat.*, 2007, pp. 1–6.
[44] B. Xiao and S. Yin, "Velocity-free fault-tolerant and uncertainty attenuation control for a class of nonlinear systems," *IEEE Trans. Ind. Electron.*, vol. 63, no. 7, pp. 4400–4411, Jul. 2016.
[45] F. Miao et al., "Coding schemes for securing cyber-physical systems against stealthy data injection attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 106–117, Mar. 2017.

Zhihua Wu received the B.Sc. degree in mathematics and applied mathematics from Anhui University of Technology, Ma'anshan, China, in 2020. He is currently working toward the M.Sc. degree in operations research and cybernetics with the University of Shanghai for Science and Technology, Shanghai, China.

His research interests include cyber attack and robust control.

Engang Tian (Member, IEEE) received the B.Sc. degree in mathematics from Shandong Normal University, Jinan, China, in 2002, the M.Sc. degree in operations research and cybernetics from Nanjing Normal University, Nanjing, China, in 2005, and the Ph.D. degree in control theory and control engineering from Donghua University, Shanghai, China, in 2008.

From 2011 to 2012, he was a Postdoctoral Research Fellow with the Hong Kong Polytechnic University, Hong Kong. From 2015 to 2016, he was a Visiting Scholar with the Department of Information Systems and Computing, Brunel University London, U.K. From 2008 to 2018, he was an Associate Professor and then a Professor with the School of Electrical and Automation Engineering, Nanjing Normal University, Nanjing, China. In 2018, he was appointed as an Eastern Scholar by the Municipal Commission of Education, Shanghai, China, and joined University of Shanghai for Science and Technology, Shanghai, China. He is currently a Professor with the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai, China. He has authored or coauthored more than 100 papers in refereed international journals. His research interests include networked control systems, cyber attack, as well as nonlinear stochastic control and filtering.

Hongtian Chen (Member, IEEE) received the B.S. and M.S. degrees in electrical automation from the School of Electrical and Automation Engineering, Nanjing Normal University, Nanjing, China, China, in 2012 and 2015, respectively, the Ph.D. degree in control theory and control engineering from the College of Automation Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2019.

He had ever been a Visiting Scholar with the Institute for Automatic Control and Complex Systems, University of Duisburg-Essen, Duisburg, Germany, in 2018. Now, he is a Post-Doctoral Fellow with the Department of Chemical and Materials Engineering, University of Alberta, Edmonton, AB, Canada. His research interests include process monitoring and fault diagnosis, data mining and analytics, machine learning, and quantum computation; and their applications in high-speed trains, new energy systems, and industrial processes.

Dr. Chen was a recipient of the Grand Prize of Innovation Award of Ministry of Industry and Information Technology of the People's Republic of China in 2019, the Excellent Ph.D. Thesis Award of Jiangsu Province in 2020, and the Excellent Doctoral Dissertation Award from Chinese Association of Automation (CAA) in 2020.