Cyber-attack-tolerant Frequency Control of Power Systems

Chunyu Chen, Kaifeng Zhang, Ming Ni, and Ying Wang

***Abstract*—Cyber attacks are emerging threats in the Internet of Things applications, and power systems are typical cyber attack targets. As one of the most essential operation functions, frequency control is threatened by cyber intrusions, and the existing centralized control mode cannot effectively address cyber risks. In this study, a new distributed cyber-attack-tolerant frequency control scheme is designed. The distributed control mode also serves as a convenient tool for attack identification. The designed cyber-attack-tolerant frequency controller adopts the idea of passive fault attenuation, thus simplifying the design procedure. With the aid of graph theory and consensus techniques, distributed integral based and model predictive control (MPC) based controllers are designed. Compared with the integral type, the MPC-based controller can simultaneously improve the dynamic responses and the tolerance ability under attack. The proposed controller is validated via an IEEE benchmark system, and the effectiveness of its application in actual power systems is verified.**

***Index Terms*—Frequency control, cyber attack, distributed control, passive fault attenuation, cyber-attack-tolerant frequency control.**

I. Introduction

POWER system frequency stability is the vital ability of the grid to regain the equilibrium of operation states in the wake of unexpected disturbances. Many theoretical and practical products, including robust model based and computationally intelligent model-free frequency stabilizers, have been developed, mainly focusing on the physical disturbance attenuation. Nevertheless, when cyber intrusions occur, disturbances begin to dramatically take cyber-physical forms, and the disorder can even cause cascading failures of existing functions [1], [2]. Therefore, it is essential to take cyber disturbances into consideration and design cyber-attack-tolerant frequency control (CATFC) schemes to enhance the frequency regulation performance.

Except for power system frequency control, various applications (power system state estimation [3], economic dispatch [4], etc.) also face security challenges. In addition, some researchers have recently begun to study the cyber security of emerging smart grid applications, including active distribution networks [5] and electric vehicles [6]. Unlike the aforementioned cyber attack scenarios, a cyber attack on the frequency control system usually has the goal of destabilizing the system frequency. Therefore, it is essential to design countermeasures to enhance attack tolerance, so that acceptable frequency control performance under cyber attack is preserved.

Although CATFC is a comparatively new technique, a significant number of research reports have emerged about the analysis of negative influences on the system, as well as detection strategy design [7]. The attack influence under specific objective-oriented attack policies has been analyzed in two earlier studies [8], [9], both of which addressed attack policy design as optimization problems. Modeling the attack objective, e.g., the remaining time until the onset of disruptive remedial actions [8] and attack cost characterized by the energy of false data injection (FDI) [9], and operating constraints reveal the optimal attack sequences and compromised regulation performances.

The detection of cyber intrusions has also been investigated by adopting various anomaly detection (AD) techniques [10]-[14]. Reference [10] captures the compromised signal by analyzing the distribution of area control errors, among which the outliers correspond to attack scenarios. In another study, a data-driven two-tier detection framework is designed [11]. The first tier is used to flag abnormal behaviors of system variables, while the second tier detects anomalies by using correlation-based methods. A multi-perceptron neural network based detector using feature extraction and selection is presented in another report [12]. Reference [13] presents a novel unknown input observer for state estimation, which is used to calculate the residual function. The compromised scenario is indicated by a significant discrepancy between the residual and a predefined threshold value. Reference [14] proposes a dynamic watermarking-based detection method that can be implemented without upgrading generation units. Apart from investigating compromised performances and in-

Manuscript received: December 4, 2019; accepted: March 10, 2020. Date of CrossCheck: March 10, 2020. Date of online publication: October 1, 2020.

This work was supported by National Natural Science Foundation of China (No. 51977033).

C. Chen (corresponding author) is with the School of Electrical and Power Engineering, China University of Mining and Technology, Xuzhou 221116, China (e-mail: chunyuchen@cumt.edu.cn).

K. Zhang and Y. Wang are with the School of Automation, Southeast University, Nanjing 210096, China (e-mail: kaifengzhang@seu.edu.cn; wyseu@seu.edu.cn).

M. Ni is with NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211106, China, and he is also with NARI Technology Co., Ltd., Nanjing 211106, China and State Key Laboratory of Smart Grid Protection and Control, Nanjing 211106, China (e-mail: ni-ming@sgepri.sgcc.com.cn).

DOI: 10.35833/MPCE.2019.000185

trusion identification approaches, some researchers have begun to design more attack-tolerant and more secure controllers that passively or actively fight against potential cyber threats. Reference [15] proposes a game-based defense policy to minimize the expected damage. The attack defense of a frequency control system is constructed by using a two-person dynamic game model. The goal of the defender is to obtain the optimal policy at each game stage, thus minimizing the long-term loss of the defender.

An attack-tolerant or resilient frequency controller is vital to the proper functioning of the frequency stabilizing mechanism and security of power systems [16], which serves as the backbone of stable frequency-dependent equipment operation and production activities. Although the aforementioned studies involve controller renovation for security enhancement, several drawbacks might inhibit real-life application.

1) Strictly, many of these mitigation measures are not essentially attack-tolerant. These strategies are more concerned about attack mitigation and attenuation than exclusion, so they might not completely or almost completely exclude the attack from the closed frequency control loop, thus minimizing the attacker's gain and the defender's loss.

2) Some researchers have presented active attack-tolerant approaches, thus improving the attack-insensitive control schemes by combining attack identification with mitigation, e. g., isolating the attack by using an exquisitely designed state estimation program. However, the design cost is comparatively high, and the isolation program requires that special conditions hold. These conditions might not be applied to more complex actual systems. Moreover, the effectiveness of these strategies relies heavily on the success of detection, which might not always be guaranteed when considering inadvertent failure.

These active attack-tolerant approaches using identification information might not be the best options in terms of practicality and accuracy. In this study, to address this issue, a passive CATFC scheme is designed to enhance the communication robustness of the control system. Conventional frequency control schemes use all the machine speed measurement for feedback control. However, this control manner is susceptible to communication hijacking. The attacker can randomly choose one or multiple communication channels between the unit and the control center to inject false data. Thus, the frequency response deteriorates through the magnification effect of the closed loop. This performance deterioration is inevitable unless the operator can prevent each communication channel from being infiltrated by the attacker, which is quite costly when there are many frequency regulation units (e.g., distributed generators).

In this study, the conventional centralized control manners are changed by reformulating the communication methods and designing a distributed controller that uses the local machine speed measurement as the feedback signal. The main advantage of this policy is that it can effectively evade FDI with secure estimation of the protected measurement. Moreover, it can address a situation in which the attacker manipulates the reference of the feedback control system. This issue is seldom addressed but is highly likely in practice. The main contributions of this study are as follows:

1) A new distributed frequency control mode is developed to enhance the self-healing ability under cyber attacks from the perspective of passive fault attenuation. An effective yet convenient detector is given as the by-product of the distributed controller, avoiding the computational burdens of intelligent AD methods.

2) An integral-based CATFC is designed with the aid of graph and consensus theories. It is capable of resisting both FDI and denial of service (DoS) attacks by using indirect estimation of the control reference value and machine speed measurement.

3) A model predictive control (MPC) based CATFC is presented to improve the dynamic responses while guaranteeing the attack tolerance. The proposed method can be applied to more-practical power system models instead of simplified equivalent unit-based models. This lays foundation for wide application in actual power systems.

The remainder of this paper is organized as follows. Section II provides a formal analysis on the vulnerability of the conventional centralized mode to cyber attacks. Section III presents the distributed CATFC design procedures. Specifically, they can be categorized according to two aspects. Section III-A describes the working principle of the resistance of the distributed mode to cyber attacks. Section III-B gives the detailed procedure of integral-based and MPC-based CATFC design. Case studies are discussed in Section IV. The conclusions are presented in Section V.

II. Conventional Centralized Frequency Control Scheme and Its Cyber Security Vulnerability

In this section, through a brief introduction, the conventional centralized frequency control scheme is presented. Then, the cyber security vulnerability of this existing control mode is analyzed by imitating the probable policies of an attacker, laying the foundations for the attack-tolerant controller design in the following subsections.

A. Conventional Centralized Frequency Control Scheme

The control scheme itself is not the focus of this subsection. Thus, only the centralized control architecture is discussed. A schematic diagram of the centralized control mode under cyber attack is shown in Fig. 1.

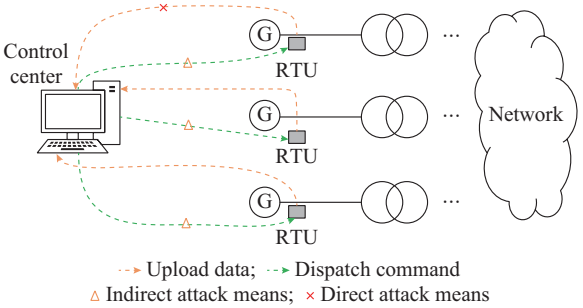

Fig. 1. Schematic diagram of centralized frequency control mode under cyber attack.

As shown in Fig. 1, if the data collected from a certain unit are attacked by a direct attack means (e. g., FDI) through the upper-level center computation, it is equivalent to executing an indirect attack means (compromised control commands) on each lower-level unit. Thus, the main drawback of the centralized control mode under cyber attack is that all the participating units would receive and then execute compromised commands once the data of any remote terminal unit (RTU) sent to the upper-level center are compromised.

All the plants (units) possess bi-directional communication channels with the upper-level control center, which either sends down orders (through the communication channels indicated by the green dotted lines in Fig. 1) or receives machine speed measurement (through the communication channels indicated by the orange dotted lines in Fig. 1). The control center serves as a "brain center" in which the orders and measurements are uniformly processed.

B. Attack Impact of Two-equivalent-unit System Using Centralized Mode

Under the circumstances of cyber intrusions, there are mainly two localities that might suffer from the attack. The first is the measurement uploading channels (indicated by the orange dotted lines in Fig. 1) and the second is the order issuing channels (indicated by the green dotted lines in Fig. 1). The attacker might infiltrate the channels, implement an element of sabotage (FDI) [17], and cause instability (frequency deviation).

To illustrate the impact of an FDI attack on a centralized frequency controller, a system comprising two equivalent units is tested. A schematic diagram of the two-equivalent-unit system based on the system frequency response model is shown in Fig. 2. The red cross symbol represents the implementation of the FDI attack by the attacker. α_1 and α_2 are the allocation coefficients. T_{12} is the synchronous coefficient. Detailed descriptions of the system frequency response model are given in previous work [18]. Supposing that the FDI attack is used to falsify the machine speed measurement of unit 1, the dynamic response is shown in Fig. 3. As can be seen, explicit deviations occur under the FDI attack.

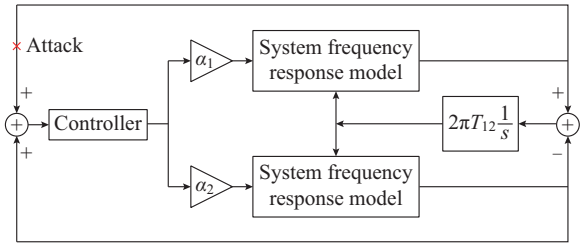

Fig. 2. Schematic diagram of two-equivalent-unit system.

III. CATFC Scheme Under New Distributed Control Framework

In the previous section, the vulnerability of the centralized mode is demonstrated. To overcome this problem, a distributed CATFC is designed.

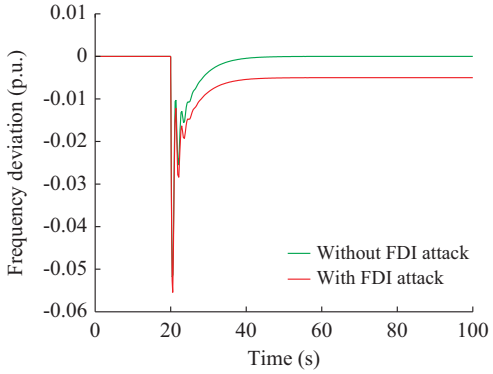

Fig. 3. Dynamic frequency response with and without FDI attack.

Specifically, the working principle and benefit of the distributed mode are discussed first. Then, the design procedure of a proportional-integral (PI) based CATFC is presented. Finally, an MPC-based CATFC is proposed.

A. Distributed Control Mode with Immunity to Cyber Attack

In this subsection, the working principle of the distributed mode resistance to an FDI attack is addressed. The distributed feature means that every generation unit only uses the integral (supposing that the controller is integral-type) of the machine speed deviation measured at its local generator internal bus [19]. The distributed controller is:

$$u_i = k_i \int \left(\omega_i(t) - \omega_0\right) \mathrm{d}t \tag{1}$$

where u_i is the distributed control law; k_i is the integral coefficient; ω_i is the local machine speed measurement; and ω_0 is the nominal machine speed.

As (1) shows, the information of other machine speed measurements is not required. This means that the communication burden is reduced. Moreover, the most essential benefit of this distributed mode is that the FDI attack scenario can be easily distinguished by a residual function. If the k^{th} unit is compromised by an FDI attack, the resulting control equation is:

$$u_k = k_i \int \left(\omega_k(t) - \omega_0 - att\right) \mathrm{d}t \tag{2}$$

where *att* is the false injection.

Because every unit tracks its own perceived reference, some unscathed ones track the real ω_0, while other compromised ones track the false $\omega_0 + att$. This causes the nonsynchronization of the machine speeds of different generation units. This nonsynchronization is a good indicator of FDI attack identification. For example, the operator can calculate the residual frequency deviation as:

$$dev = \sum_{i=1}^{N} \left| \omega_i - \frac{1}{N} \sum_{i=1}^{N} \omega_i \right| \tag{3}$$

where *dev* is the threshold of total frequency deviations.

By comparing *dev* with the predefined threshold value, the detection can be realized. Another approach is to directly use the angle difference between any pair of units. Because the machine speed difference always exists, the angle difference continuously increases over time. To verify this phenome-

non, the two-equivalent-unit system shown in Fig. 2 is used. In the distributed mode, the dynamic frequency response and machine angle difference are shown in Fig. 4 and Fig. 5, respectively. As can be seen, there exists an explicit difference of the speed deviation of the two units, and the angle difference abruptly increases when an FDI attack occurs at 20 s. The theoretical and simulation analyses show that the distributed controller can naturally identify an FDI attack by observing the respective response. This does not mean that other data-based AD-based cyber attack detection schemes are not worth investigating. In many applications where a centralized mode is preferred, AD could still wield great power.

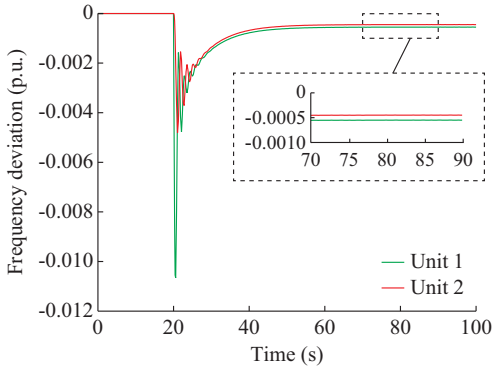

Fig. 4. Dynamic frequency response under distributed control scheme with FDI attack.

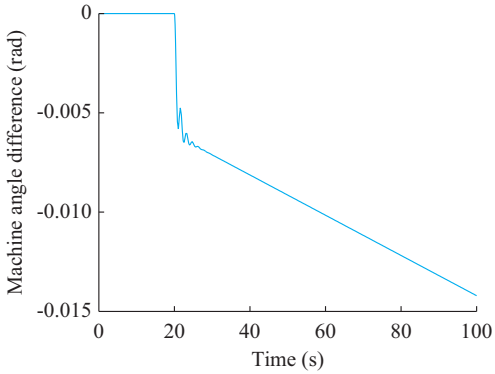

Fig. 5. Machine angle difference under distributed control scheme with FDI attack.

B. CATFC Scheme Using Distributed Control Mode

In Section III-A, the distributed control mode and the new attack detection approach using this mode are addressed. Nevertheless, the distributed controller shown in (1) still cannot exclude the FDI in its current form. An analysis shows that the main factor of its ineffectiveness for attack resistance is the failure of eliminating *att* in the closed loop. Hence, if the true measurement ω_k can be extracted from the false one, i. e., $\omega_k + att$ shown in (2), the influence of the FDI attack can be completely avoided.

1) Cyber Attack and Some Technical Backgrounds

Under the guidance of the true measurement reconstruction idea, a novel state estimator is designed by using a consensus algorithm. Before the detailed design procedure is presented, some important remarks are given with respect to cyber attack scenarios.

Remark 1: the field sensors are susceptible to cyber intrusions, and the attacker can easily hack into sensors that perform local machine speed measurement. Nevertheless, one machine speed measurement is processed through the private channel, which is deemed to be invulnerable to attack by a sufficiently high level of security.

Remark 2: the reference value for distributed control (tracking) in this study is assumed to be vulnerable to cyber intrusion, which means that the attacker can infiltrate the distributed system and falsify this reference value.

Remark 1 explains the situation (position) in which the attacker can implement attacks. Remark 1 is understandable and pragmatic in that field sensors for machine speed measurement are the most-critical elements for frequency destabilization, whether in a distributed or centralized control mode, and the rudimentary protection measures of sensors are likely to be considered by this type of attack, which can be easily penetrated.

Remark 2 further pushes the boundary of attack scenarios into control parameter (reference value) distortion on the basis of misrepresentation of feedback state information. It must be remembered that the control parameter is another important element for guaranteeing the success of controller execution. It becomes a natural and primary target of cyber attacks.

In the procedure of CATFC design, the techniques repeatedly used are graph and consensus theories. Hence, a basic introduction is given in advance. Supposing that the set of generation units is $\mathcal{N} = \{1, 2, \ldots, |\mathcal{N}|\}$, where $|\mathcal{N}|$ declares its cardinality. It is assumed that the communication is bi-directional, which means that if $(n_i, n_j) \in \mathcal{E}$, then $(n_j, n_i) \in \mathcal{E}$, where (n_i, n_j) means the possible communication signal transmit direction from n_i to n_j; and $\mathcal{E} \subseteq \mathcal{N} \times \mathcal{N}$ denotes communication channels that connect two units. $\boldsymbol{\mathcal{A}}$ with nonnegative elements a_{ij} declares the on-off status of the connection between n_i and n_j. $G = (\mathcal{N}, \mathcal{E}, \boldsymbol{\mathcal{A}})$ is called the "communication graph", and it is supposed that the graph is connected under no attack, which means that any two distinct nodes can be connected via a path that follows the direction of $\boldsymbol{\mathcal{A}}$.

2) Integral-based CATFC Scheme

From the description above, it is known that the attacker can implement an FDI attack in two ways: ① through field sensor measurement distortion; ② through reference value distortion. Hence, if the real measurement can be reconstructed, the attack loss can be avoided. For this purpose, a distributed integral-based frequency controller is designed as:

$$u_i = k_i \int \left(\hat{\omega}_i(t) - \hat{\omega}_{i0} \right) \mathrm{d}t \tag{4}$$

where $\hat{\omega}_i$ and $\hat{\omega}_{i0}$ are the estimators of real measurement for the state (machine speed) and reference value, respectively.

Specifically, the estimator of the protected measurement is written as (5) or (6).

$$\dot{\hat{\omega}}_i = \sum_{j \in N_j} a_{ij} \left(\hat{\omega}_j - \hat{\omega}_i \right) + a_{i0} \left(\omega_r - \hat{\omega}_i \right) \tag{5}$$

$$\dot{\hat{\omega}}_i = sig\left(\sum_{j\in N_j} a_{ij}\left(\hat{\omega}_j - \hat{\omega}_i\right) + a_{i0}\left(\omega_{\mathrm{r}} - \hat{\omega}_i\right)\right)^{\frac{1}{2}} \tag{6}$$

where ω_{r} is the protected measurement of the unit speed, which is always of real value under protection (the attacker cannot change this value); $sig(\cdot)^b = sig(\cdot)|\cdot|^b (b>0)$ is the sign function; and a_{i0} is a 0-1 variable, which represents whether $\hat{\omega}_i$ has direct access to the machine speed measurement ω_i. If the direct access exists, $a_{i0}=1$; otherwise, $a_{i0}=0$.

Equations (5) and (6) are designed to minimize the impact of an FDI attack on state measurement by a dynamically calibrated consensus module, i. e., each unit tracks the virtual leader (ω_{r}) and obtains $\hat{\omega}_i$. It uses $\hat{\omega}_i$ rather than the directly measured machine speed ω_i as the feedback signal. Consequently, the impact of the compromised measurement $\omega_i + att$ is attenuated.

The main difference between (5) and (6) is that (6) can realize tracking in finite time. By some mathematic transformations, (5) can be expressed by:

$$\dot{\hat{\boldsymbol{\omega}}} - \dot{\boldsymbol{\omega}}_{\mathrm{r}} = -\left(\boldsymbol{\mathcal{L}} + \boldsymbol{\mathcal{A}}_0\right)\left(\hat{\boldsymbol{\omega}} - \boldsymbol{\omega}_{\mathrm{r}}\right) \tag{7}$$

where $\hat{\boldsymbol{\omega}}$ and $\boldsymbol{\omega}_{\mathrm{r}}$ are the vectors of the estimated machine speed of the follower and the reference speed of the leader, respectively; $\boldsymbol{\mathcal{A}}_0 = \mathrm{diag}\{a_{i0}\}$; and $\boldsymbol{\mathcal{L}} = \boldsymbol{D} - \boldsymbol{\mathcal{A}}$ is the graph Laplacian associated with G [20], $\boldsymbol{D}$ represents the degree matrix of the follower agents, $\boldsymbol{\mathcal{A}}$ represents the adjacency matrix of the follower agents. It can be proven that $-\left(\boldsymbol{\mathcal{L}} + \boldsymbol{\mathcal{A}}_0\right)$ is negatively definite if the graph is connected, so that $\hat{\omega}_i - \dot{\omega}_{\mathrm{r}}$ is asymptotically stable under the assumption that $\dot{\omega}_{\mathrm{r}} \to 0$. Furthermore, the convergence of the finite-time estimator can be proven. The detailed proof can be found in previous work [21].

The estimator of reference value is expressed as (8) or (9).

$$\dot{\hat{\omega}}_{i0} = \sum_{j\in N_j} a_{ij}\left(\hat{\omega}_{j0} - \hat{\omega}_{i0}\right) + a_{i0}\left(\omega_0 - \hat{\omega}_{i0}\right) \tag{8}$$

$$\dot{\hat{\omega}}_{i0} = sig\left(\sum_{j\in N_j} a_{ij}\left(\hat{\omega}_{j0} - \hat{\omega}_{i0}\right) + a_{i0}\left(\omega_0 - \hat{\omega}_{i0}\right)\right)^{\frac{1}{2}} \tag{9}$$

Similarly, (8) and (9) are designed to minimize the impact of an FDI attack on the reference value by a dynamically calibrated consensus module, i.e., each unit tracks the virtual leader (ω_0) and obtains $\hat{\omega}_{i0}$. It uses $\hat{\omega}_{i0}$ rather than the direct reference value ω_0 as the feedback signal. Consequently, the impact of the compromised reference value $\omega_0 + att$ is attenuated.

With this newly-developed distributed frequency controller, the focus of cyber attacks changes from infiltrating and damaging the system (through injecting false data) to destroying the communication channels (through DoS attack), which aims at debilitating the connectivity of the communication graph. Nevertheless, when considering the multifold channels and limitedness of the attack means, the attacker can barely break off all the connections, which would certainly result in the system collapse. Even if some of the connections are disconnected, as long as the connectivity condition holds (the graph has at least one path between any pair of vertices), the consensus and ensuing control performance can be ensured.

Remark 3: in practice, the defender could strengthen the communication graph by adding additional channels between two vertices, so that the connectivity is unscathed under DoS attack.

3) MPC-based CATFC Scheme

In the description above, the working principle of the resistance of the distributed frequency controller to cyber attacks is meticulously explained. The designed controller is essentially integral-type. Constrained by the low reacting velocity, an improved yet engineering-application-friendly approach needs to be found. A variety of frequency controllers using advanced control theories have been investigated [22]-[26]; nevertheless, the practicality and convenience are restricted by their special application scenarios, which might not effectively comply with the requirements of more practical systems. In this subsection, the MPC method is adopted to improve the dynamic performance. MPC is one of the most practical control methods for offsetting the disadvantage of PI-based controllers [27], and it is widely used in industrial system control [28], [29]. The goal of MPC is to obtain control actions in a sequential manner, so that the predicted responses (machine speed ω_i) converge to the reference value ω_0 optimally.

When the current sampling instant is c, MPC, which is modeled as an optimization problem, is used to calculate the future input $\left[u(c), u(c+1), \ldots, u(c+M-1)\right]$ within the control horizon of M. Then, the actual control input keeps constant during this horizon with $u = u(c)$. Meanwhile, the predicted output $\left[\hat{y}(c), \hat{y}(c+1), \ldots, \hat{y}(c+P-1)\right]$ is calculated within the prediction horizon of P. In the calculation process, through a bias correction function that diminishes the errors between the predicted output $\hat{y}$ and actual output y, the corrected prediction $\tilde{y}$ is obtained and used to calculate the objective function in the optimization problem.

A detailed power system model is used to design this distributed MPC-based frequency controller. The power system model can be written by a set of differential algebraic equations:

$$\begin{cases} \dot{\boldsymbol{x}} = \boldsymbol{f}\left(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{u}\right) \\ \boldsymbol{0} = \boldsymbol{g}\left(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{u}\right) \end{cases} \tag{10}$$

where $\boldsymbol{x}$ is the vector of states of power systems; $\boldsymbol{u}$ is the vector of the control inputs and disturbances term; and $\boldsymbol{y}$ is the vector of outputs.

The resulting small-signal stability model is achieved by linearizing (10), which can be expressed as:

$$\begin{cases} \Delta\dot{\boldsymbol{x}} = \boldsymbol{A}_{11}\Delta\boldsymbol{x} + \boldsymbol{C}_{12}\Delta\boldsymbol{y} + \boldsymbol{B}_{12}\Delta\boldsymbol{u} \\ \boldsymbol{0} = \boldsymbol{A}_{21}\Delta\boldsymbol{x} + \boldsymbol{C}_{22}\Delta\boldsymbol{y} + \boldsymbol{B}_{22}\Delta\boldsymbol{u} \end{cases} \tag{11}$$

where Δ represents the deviation of the variable from the equilibrium point; and $\boldsymbol{A}_{11}$, $\boldsymbol{A}_{21}$, $\boldsymbol{C}_{12}$, $\boldsymbol{C}_{22}$, $\boldsymbol{B}_{12}$, and $\boldsymbol{B}_{22}$ are the coefficient matrices via linearization.

Usually, $\boldsymbol{A}_{21}$ is invertible. By substituting $\Delta\boldsymbol{x}$ and $\Delta\boldsymbol{u}$ for

$\Delta \boldsymbol{y}$ and setting the controlled output by $y=\omega_i=\boldsymbol{C}^{\mathrm{T}}\boldsymbol{x}$, (11) can be transformed into each subsystem (corresponding to each agent):

$$\begin{cases}\dot{\boldsymbol{x}}_i=\boldsymbol{A}_{\mathrm{e}}\boldsymbol{x}_i+\boldsymbol{B}_{\mathrm{e}}u_{\mathrm{c},i}+\boldsymbol{F}_{\mathrm{e}}u_{\mathrm{d},i}\\ y_i=\boldsymbol{C}^{\mathrm{T}}\boldsymbol{x}_i\end{cases} \tag{12}$$

where $\boldsymbol{A}_{\mathrm{e}}$, $\boldsymbol{B}_{\mathrm{e}}$, $\boldsymbol{F}_{\mathrm{e}}$, and $\boldsymbol{C}$ are the coefficient matrices of the subsystem; Δ are removed for simplicity; $u_{\mathrm{c},i}$ is the control variable; and $u_{\mathrm{d},i}$ is the disturbance. $\boldsymbol{u}_i=\left[u_{\mathrm{c},i},u_{\mathrm{d},i}\right]$.

After obtaining the differential form in (12), the design procedure is as follows.

First, the crude predicted response $\left[\hat{y}_i(c),\hat{y}_i(c+1),\ldots,\hat{y}_i(c+P-1)\right]$ from the current instant to the future P sampling instant beyond is:

$$\hat{y}_i(c+j)=\sum_{i=1}^{j}S_i\Delta u_{\mathrm{c},i}(c+j-i)+\sum_{i=j+1}^{N-1}S_i\Delta u_{\mathrm{c},i}(c+j-i)+S_N u_{\mathrm{c},i}(c+j-N) \tag{13}$$

where $\Delta u_{\mathrm{c},i}(k)=u_{\mathrm{c},i}(k)-u_{\mathrm{c},i}(k-1)$ is the control input change; N is the time span; and S_i is the step-response coefficient.

Second, the corrected prediction $\tilde{y}(c+j)$ is written as:

$$\tilde{y}_i(c+j)=\hat{y}_i(c+j)+b(c+j) \tag{14}$$

The correction terms satisfy:

$$b(c+j)=y_i(c)-\hat{y}_i(c) \tag{15}$$

where $y_i(c)$ is the real measurements, which is calculated by (12).

Third, the optimization model is defined as:

$$\min_{\Delta U(c)} J=\boldsymbol{E}^{\mathrm{T}}(c)\boldsymbol{Q}\boldsymbol{E}(c)+\Delta\boldsymbol{U}^{\mathrm{T}}(c)\boldsymbol{R}\Delta\boldsymbol{U}(c) \tag{16}$$

where $\boldsymbol{E}(c)=\left[y_{\mathrm{r}}(c+1)-\tilde{y}_i(c+1),y_{\mathrm{r}}(c+2)-\tilde{y}_i(c+2),\ldots,y_{\mathrm{r}}(c+P)-\tilde{y}_i(c+P)\right]$; $\Delta\boldsymbol{U}(c)=\left[\Delta u_{\mathrm{c},i}(c),\Delta u_{\mathrm{c},i}(c)+1,\ldots,\Delta u_{\mathrm{c},i}(c)+M-1\right]$; $\boldsymbol{Q}$ and $\boldsymbol{R}$ are the weighted coefficient matrices; and y_{r} is calculated either by (5) and (6) for machine speed estimation or (8) and (9) for reference value estimation. The remainder of the optimization procedure is trivial and omitted because of space limitations.

IV. Case Studies

The distributed CATFC is verified with Kundur's 4-unit 13-bus system, the single-line diagram of which is shown in Fig. 6.

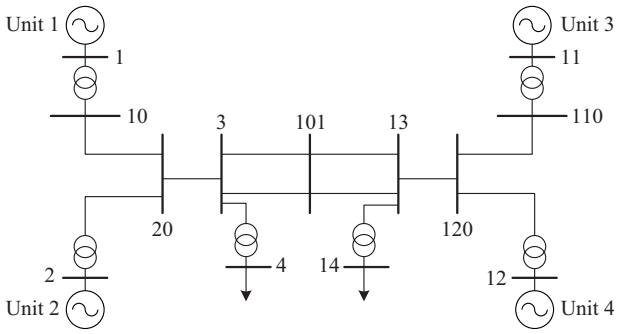

Fig. 6. Diagram of Kundur's 4-unit 13-bus system.

The system in Fig. 6 is modeled by using MATLAB/Simulink, and it contains complete models of the synchronous generator, power system stabilizer, primary frequency control, and excitation block, as well as the network model. Therefore, the resulting dynamic model written in (12), of which the order is 58, is much more practical and complex than the equivalent unit based model in Fig. 2.

A. Communication Graph and Cyber Attack Simulation

Before testing the designed CATFC, how different units communicate with each other and how the attacker implements attacks must be explained. The communication graph is shown in Fig. 7. Unit 1 is regarded as the protected unit, of which the machine speed measurement always has true values. In addition, it is assumed that unit 1 has direct access to the virtual leader (reference value ω_0). For simplicity, the edge set $\boldsymbol{\mathcal{A}}$ for ω_0 and machine speed measurement tracking of unit 1 are the same. Another benefit of this configuration is that any pair of nodes has connection, which reduces the risks of nonconnectivity under cyber attacks.

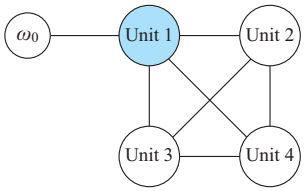

Fig. 7. Communication graph of units in Kundur's 4-unit 13-bus system.

Based on Fig. 7, cyber attacks are simulated by the two scenarios in Fig. 8 and Fig. 9. In scenario 1, the attacker implements FDI attacks on the measurement of units 2, 3, and 4 (the measurement of unit 1 is protected), as well as compromising the control reference value of all units. The attacker implements DoS attacks by breaking the three connections shown in Fig. 8. In scenario 2, the attacker implements FDI attacks on the measurement of units 2, 3, and 4 (the measurement of unit 1 is protected), as well as compromising the control reference value of all units. The attacker implements DoS attacks by breaking the three connections shown in Fig. 9.

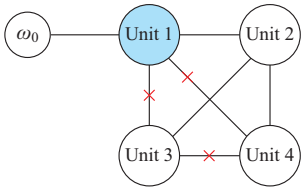

Fig. 8. Cyber attack scenario 1 of Kundur's 4-unit 13-bus system.

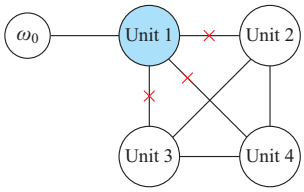

Fig. 9. Cyber attack scenario 2 of Kundur's 4-unit 13-bus system.

It can be proven that, for the node set $\mathcal{N}$ with any pair of nodes connected, the minimal number of connections that the attacker must break to influence the tracking is $|\mathcal{N}|-1$. Hence, in the two attack scenarios, it is assumed that the attacker can disconnect three connections simultaneously. In attack scenario 1, the Laplacian matrix is:

$$-\left(\mathcal{L}+\mathcal{A}_0\right)=\begin{bmatrix}2&-1&0&0\\-1&3&-1&-1\\0&-1&1&0\\0&-1&0&1\end{bmatrix} \tag{17}$$

It can be found that $-\left(\mathcal{L}+\mathcal{A}_0\right)$ is negatively definite in scenario 1, and the tracking can be ensured. Nevertheless, $-\left(\mathcal{L}+\mathcal{A}_0\right)$ in scenario 2 is:

$$-\left(\mathcal{L}+\mathcal{A}_0\right)=\begin{bmatrix}1&0&0&0\\0&2&-1&-1\\0&-1&2&-1\\0&-1&-1&2\end{bmatrix} \tag{18}$$

The matrix is not negatively definite in scenario 2. Thus, the tracking cannot be achieved.

B. CATFC Simulation Under Cyber Attack Scenario 1

The integral-based and MPC-based CATFCs are tested. For brevity, only the finite-time tracker is tested. It is supposed that the load variation 0.05 p.u. occurs on bus 4 in Fig. 6 at 0 s. The simulation results are shown in Fig. 10.

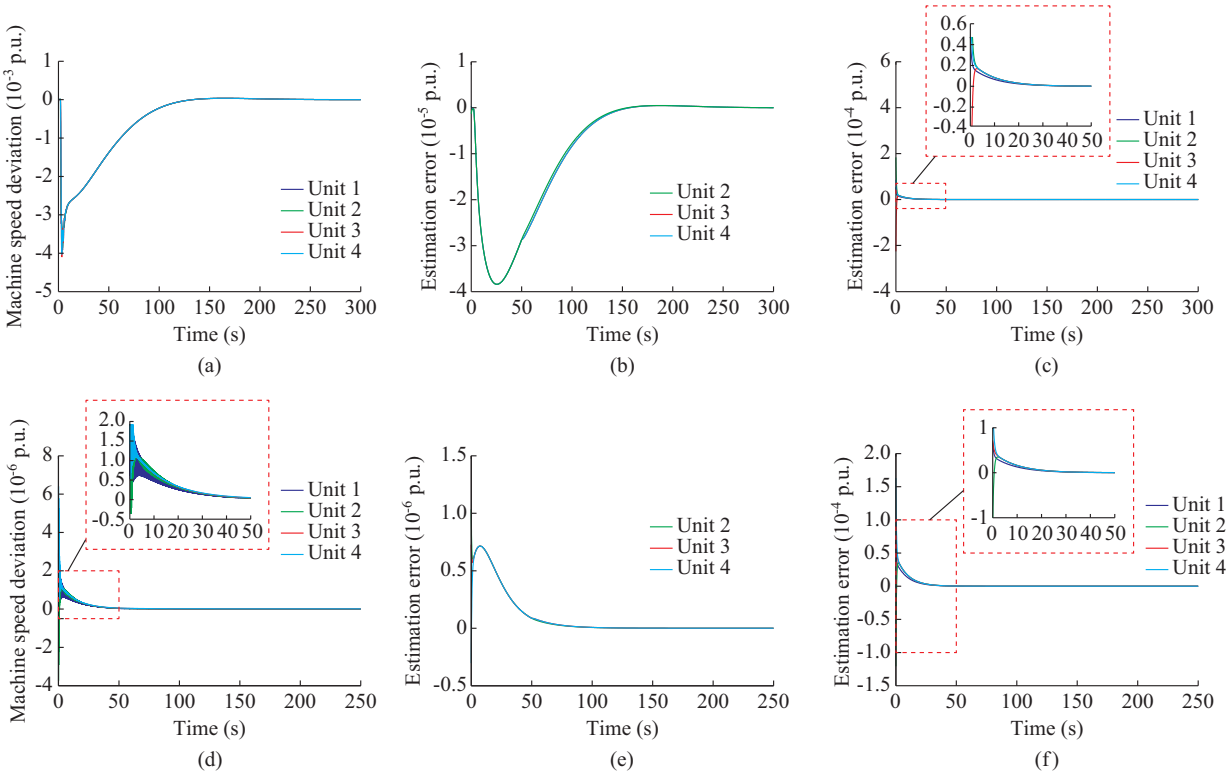

Fig. 10. Simulation results of case study under cyber attack scenario 1. (a) Machine speed deviation using integral-based CATFC. (b) Machine speed measurement tracking using integral-based CATFC. (c) Nominal control reference value tracking using integral-based CATFC. (d) Machine speed deviation using MPC-based CATFC. (e) Machine speed measurement tracking using MPC-based CATFC. (f) Nominal control reference value tracking using MPC-based CATFC.

As shown in Fig. 10, the proposed distributed CATFC can resist FDI and DoS attacks. Moreover, MPC-based CATFC shows better control performance than integral-based CATFC.

C. CATFC Simulation Under Cyber Attack Scenario 2

The integral-based and MPC-based CATFCs are tested. For brevity, only the finite-time tracker is tested. It is supposed that the cyber attack occurs after normal load variation, and the time difference is 50 s. The simulation results using the integral-based and MPC-based controllers are shown in Fig. 11(a) and (b), respectively. Furthermore, the near-simultaneous load variation and cyber attack scenario are simulated by setting the time difference to be a small number (0 s in this case), and the simulation results using the MPC-based controller are shown in Fig. 11(c).

The machine speeds diverge with the integral-based controller, while, in Fig. 11(b), machine speed deviations still converge to zero. This is because the time difference 50 s is larger than the settling time of the MPC-based controller, which means each generator learns the true reference speed ω_0 before the connection is cut off. Therefore, each can track the true speed, and thus the global convergence is guaranteed. Nevertheless, from the perspective of the integral-based controller, the settling time is larger than 50 s , which means some generators do not learn the true speed at all. Therefore, the machine speed diverges from the true speed. As shown in Fig. 11(c), when the time difference 0 s is much smaller than the settling time, even the MPC-based

controller cannot maintain global convergence.

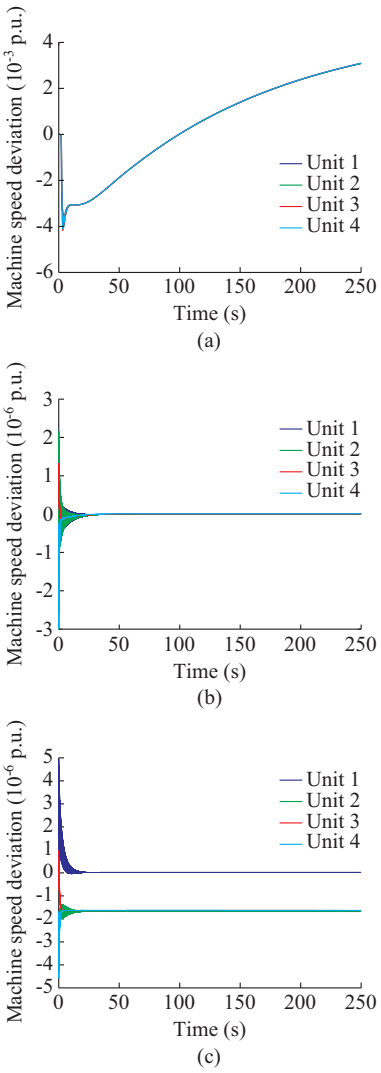

Fig. 11. Simulation results of case study under cyber attack scenario 2. (a) Machine speed deviation using integral-based CATFC. (b) Machine speed deviation using MPC-based CATFC I. (c) Machine speed deviation using MPC-based CATFC II.

When a DoS attack with complete nonconnectivity occurs before normal load variation and the initial reference value of other generators (except the one that always knows the true reference speed value) is compromised, other generators can never learn this true value through the consensus mechanism, and global convergence cannot be guaranteed.

V. Conclusion

A new distributed frequency control mode is presented to enhance the cyber security of power systems. Unlike the centralized control mode, which uniformly processes and then sends the control orders, the distributed mode uses local information without extensively exchanging information with the upper-level control centers, thus offering improved privacy and autonomy. Instead of using direct local measurement or the control reference value, the designed controller uses estimation through communicating with its neighboring units. Hence, the negative influence of cyber attacks can always be excluded if the estimation is always correct, which is equivalent to the consensus of the estimation. Through the simulations using a more practical model based on Kundur's 4-unit 13-bus system, it is proven that the designed CATFC can defend against cyber attacks as long as the connectivity of the communication graph is ensured. Moreover, the performance of the MPC-based controller is explicitly better than that of the integral-based one in terms of overall control performance under cyber attack. Moreover, it is learned that the characteristics of distributed controllers (integral-based or MPC-based) and the temporal relation between normal load variation and DoS attack could influence the global convergence of machine speeds in some extreme cyber attack scenarios, e.g., the connectivity of the communication graph is destroyed. In future work, it is planned to investigate further how to improve cyber attack tolerance in extreme cyber attack scenarios by considering the temporal relation and modifying the structure of the distributed controller.

References

[1] Z. Li, M. Shahidehpour, A. Alabdulwahab *et al.*, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 5, pp. 2260-2272, Sept. 2016.

[2] M. Tian, Z. Dong, M. Cu *et al.*, "Energy-supported cascading failure model on interdependent networks considering control nodes," *Physica A: Statistical Mechanics and Its Applications*, vol. 522, pp. 195-204, Feb. 2019.

[3] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 4868-4877, Sept. 2018.

[4] P. Li, Y. Liu, H. Xin *et al.*, "A robust distributed economic dispatch strategy of virtual power plant under cyber-attacks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4343-4352, Oct. 2018.

[5] Z. Li, M. Shahidehpour, F. Aminifar, *et al.*, "Networked microgrids for enhancing the power system resilience," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1289-1310, May 2017.

[6] S. Mousavian, M. Erol-Kantarci, L. Wu *et al.*, "A risk-based optimization model for electric vehicle infrastructure response to cyber attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6160-6169, Nov. 2018.

[7] F. Zhang, H. A. D. E. Kodituwakku, W. Hines *et al.*, "Multi-layer data-driven cyber-attack detection system for industrial control systems based on network, system and process data," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4362-4369, Jul. 2019.

[8] R. Tan, H. H. Nguyen, E. Y. Foo *et al.*, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1609-1624, Jul. 2017.

[9] C. Chen, M. Cui, X. Wang *et al.*, "An investigation of coordinated attack on load frequency control," *IEEE Access*, vol. 6, pp. 30414-30423, Jun. 2018.

[10] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580-591, Mar. 2014.

[11] M. Q. Ali, R. Yousefian, E. Al-Shaer *et al.*, "Two-tier data-driven intrusion detection for automatic generation control in smart grid," in *Proceedings of 2014 IEEE Conference on Communications and Network Security*, San Francisco, USA, Dec. 2014, pp. 292-300.

[12] C. Chen, K. Zhang, K. Yuan *et al.*, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 1932-1941, May 2018.

[13] A. Ameli, A. Hooshyar, E. F. El-Saadany *et al.*, "Attack detection and identification for automatic generation control systems," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 4760-4774, Sept. 2018.

[14] T. Huang, B. Satchidanandan, P. Kumar *et al.*, "An online detection

framework for cyber attacks on automatic generation control," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 6816-6827, Nov. 2018.

[15] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for risk minimization in automatic generation control," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 223-232, Jan. 2015.

[16] S. Liu, Z. Hu, X. Wang *et al.*, "Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4066-4075, Jul. 2019.

[17] Q. Wang, W. Tai, Y. Tang *et al.*, "Review of the false data injection attack against the cyber-physical power system," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 2, pp. 101-107, Jun. 2019.

[18] C. Chen, K. Zhang, K. Yuan *et al.*, "Disturbance rejection-based LFC for multi-area parallel interconnected AC/DC system," *IET Generation, Transmission & Distribution*, vol. 10, no. 16, pp. 4105-4117, Dec. 2016.

[19] C. Zhao, E. Mallada, and F. Dorfler, "Distributed frequency control for stability and economic dispatch in power networks," in *Proceedings of American Control Conference (ACC)*, Chicago, USA, Jul. 2015, pp. 2359-2364.

[20] R. Olfati-Saber and R. M. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1520-1533, Sept. 2004.

[21] C. Gang and G. Zhijun, "Distributed secondary control for droop-controlled autonomous microgrid," in *Proceedings of 34th Chinese Control Conference (CCC)*, Hangzhou, China, Jul. 2015, pp. 9008-9013.

[22] H. Shabani, V. Behrooz, and E. Majid, "A robust PID controller based on imperialist competitive algorithm for load frequency control of power systems," *ISA Transactions*, vol. 52, no. 1, pp. 88-95, Jan. 2013.

[23] M. H. Khooban and N. Taher, "A new intelligent online fuzzy tuning approach for multi-area load frequency control: self adaptive modified bat algorithm," *International Journal of Electrical Power Energy Systems*, vol. 71, no. 1, pp. 254-261, Oct. 2015.

[24] C. Peng, Z. Jin, and H. Yan, "Adaptive event-triggering H_∞ load frequency control for network-based power systems," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 2, pp. 1685-1694, Feb. 2018.

[25] L. Xiong, H. Li, and W. Jie, "LMI based robust load frequency control for time delayed power system via delay margin estimation," *International Journal of Electrical Power Energy Systems*, vol. 100, no. 1, pp. 91-103, Sept. 2018.

[26] K. Lu, W. Zhou, G. Zeng *et al.*, "Constrained population extremal optimization-based robust load frequency control of multi-area interconnected power system," *International Journal of Electrical Power Energy Systems*, vol. 105, no. 1, pp. 249-271, Feb. 2019.

[27] S. J. Qin and A. B. Thomas, "A survey of industrial model predictive control technology," *Control Engineering Practice*, vol. 11, no. 7, pp. 733-764, Jul. 2003.

[28] R. Zhang, A. Xue, and F. Gao, "Temperature control of industrial coke furnace using novel state space model predictive control," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2084-2092, Nov. 2014.

[29] R. P. Aguilera, P. Lezana, and D. E. Quevedo, "Switched model predictive control for improved transient and steady-state performance," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 4, pp. 968-977, Aug. 2015.

Chunyu Chen received the Ph.D. degree from Southeast University, Nanjing, China, in 2019. He is currently with School of Electrical Power and Engineering, China University of Mining and Technology, Xuzhou, China. His research interests include safety and stability control of power systems, security of electrical cyber-physical systems, power system optimization, and artificial intelligence in power systems.

Kaifeng Zhang received the Ph.D. degree from Southeast University, Nanjing, China, in 2004, and joined the faculty of the same university, where he is currently a Professor with the School of Automation. His research interests include power system dispatch and control, wind power, and nonlinear control.

Ming Ni received the B.S. and Ph.D. degrees from Southeast University, Nanjing, China, in 1991 and 1996, respectively. He is currently the Chief Expert of power system planning and analysis with the State Grid Electric Power Research Institute, a Researcher-level Senior Engineer with NARI Group Corporation, and an Adjunct Professor with the School of Electrical Engineering, Southeast University. His research interests include power system planning, analysis and control, and cyber-physical systems.

Ying Wang received the Ph.D. degree from Southeast University, Nanjing, China, in 2018, and joined the faculty of the same university, where she is currently a Lecturer with the School of Automation. Her research interests include power system dispatch and electricity market.