IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 28, 2018, accepted May 27, 2018, date of publication June 7, 2018, date of current version June 26, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2845300

An Investigation of Coordinated Attack on Load Frequency Control

CHUNYU CHEN[1], MINGJIAN CUI[2], (Member, IEEE), XINAN WANG[2], (Student Member, IEEE), KAIFENG ZHANG[1], (Member, IEEE), AND SHENGFEI YIN[2]

[1]Key Laboratory of Measurement and Control of CSE, School of Automation, Southeast University, Nanjing 210096, China
[2]Department of Electrical Engineering, Southern Methodist University, Dallas, TX 75275, USA

Corresponding author: Kaifeng Zhang (kaifengzhang@seu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 51577031 and in part by the State Grid Corporation of China (Dynamic Demand Response Control of Large-Scale Diverse Demand Side Resources).

ABSTRACT In this paper, optimal attack schemes against load frequency control (LFC) are studied by considering coordinated attack. By attacking sensor measurement (load) simultaneously, the attacker disrupts the normal operation of LFC, thus causing excess system frequency/generation excursions. From the perspective of the attacker, LFC system information availability is essential to the attack scheme design. In this paper, two scenarios, where LFC system information is and is not available to the attacker, are considered and optimal attack schemes are studied for these two scenarios, respectively. The optimal attack scheme design is modeled by an optimization problem with different objectives (attack goals): 1) maximization of frequency/generation disruption and 2) least-effort attack (minimization of attack cost). In consideration of counterattack, a threshold-based detection method is used to detect the optimal attack schemes. Two case studies, corresponding to these two scenarios, are simulated, and the results show that attack performances vary with different attack goals and the detection approach can screen out the compromised signals.

INDEX TERMS Load frequency control, false data injection, coordinated attack, optimal attack scheme, attack detection.

I. INTRODUCTION

The rapid progress in informatization of modern power grid offers many advantages including significant economic benefits and labor productivity enhancement. Nevertheless, the informatization might also give rise to unreliability problems for those information system dependent applications (e.g., wide-area control and state estimation) under potential threat of cyber intrusion. By exercising secondary control, load frequency control (LFC) system balances the active power of the control area by adjusting the reference power of the governor, thus achieving stability of frequency/tie-line power. LFC system relies on the communication between sensors and the energy management system (EMS), which faces great risks of cyber intrusion. Hence, it is necessary to investigate cyber intrusion into LFC system.

Previous studies of LFC-oriented attacks mainly focus on two aspects: 1) attack scheme design [1], [2], and 2) detection scheme design [3]. The ultimate goal of LFC-oriented attack study is to design protection measures (e.g., detection schemes), such that the negative influence of cyber attack is mitigated as much as possible. Nevertheless, attack scheme must be first analyzed to understand the motivation and behaviors of the attackers; otherwise, any detection scheme is ungrounded and detached from the potential attack strategies.

Various attack strategies have been studied in respect to different operational functions of power systems. Liu *et al.* [4] presents a bad data detection (BDD) elusion-based strategy for false data injection (FDI) attack against power system state estimation (PSSE). Subsequently, extensive research studies of PSSE-oriented attacks are investigated by using optimization methods [5], [6]. Yang *et al.* [5] models the attack goal by minimization of compromised meters for least-effort attack. Liang *et al.* [6] models attack scheme design as a bilevel optimization problem, in which the upper level is maximization of the physical line flows and the lower level is DC optimal power flow problem. Load redistribution (LR) attacks, which manipulate measurements of load bus injection and line power flow to achieve attack goals, are studied

in [7]. The most damaging LR attack is modeled by a bilevel optimization problem, in which the upper level is modeled by system loss (a weighted sum of generation and load shedding cost) maximization while the lower level is represented by a security-constraint economic dispatch (SCED) model.

As for attack schemes of LFC-oriented attack, Different attack scenarios (e.g., denial of service and delayed input attack) are simulated on LFC [8], [9]. In [2], attack scheme of FDI attack is studied. The attack goal is modeled by the minimum remaining time until the onset of disruptive remedial actions. In this paper, we also study attack strategy for LFC from the perspective of the attacker.

Previous research of LFC attack mainly focuses on falsification of area control errors (ACEs), in which the attacker falsifies sensor measurements (frequency or tie-line power measurement) to produce compromised ACEs; the compromised ACEs will disrupt the normal operation and cause excess frequency/generation excursions. Meanwhile, the upgrade of attacks means that the attacker can also implement load manipulation (through demand response program or remotely controlling smart appliances). It is necessary to investigate how this coordinated attack (by falsifying ACEs and load manipulation) influences the LFC system.

Two important questions remain to be analyzed from the perspective of the attackers. Firstly, what is the role of LFC system information availability in attack scheme design? Secondly, How does the attacker model the scheme design problem for more efficient/effective implementation? Based upon these two questions, optimal attack schemes considering LFC system information availability are presented in this paper. Two scenarios where the attacker does and does not know LFC system information, along with two main attack goals: 1) maximization of frequency/generation disruption and 2) minimization of attack cost, are used to generate four types of optimization models; then, optimal coordinated attack schemes can be achieved.

The proposed attack schemes can be used to simulate standard attack scenarios (which the attacker would most likely to produce), thus laying the ground for corresponding mitigation measure design.

The contribution of the paper includes:

1) Coordinated attack with respect to LFC is studied. That is, the attacker intrudes LFC by both compromising area control error (ACE) measurement and manipulating active power at load buses. Attack scheme design is modeled by an optimization problem, in which maximization of both frequency and generation disruption are considered as the objectives. Besides, the least-effort attack (i.e., minimization of attack cost) is studied.
2) Two scenarios are considered based on LFC system information availability to the attacker. In the first type, the attacker has complete knowledge of LFC system (structures and parameters); while he knows nothing about LFC configuration in the second type. Optimal attack schemes are designed for these two scenarios respectively.
3) Attack detection corresponding to the proposed optimal attack strategies is studied.

The remaining of the paper is as follows: Section II presents the background of LFC; Section III discusses how coordinated attack works on LFC, and gives a brief introduction of optimal attack scheme design; Section IV gives detailed analyses of optimal attack scheme design in respect to different attack goals. Attack detection corresponding to the optimal attack schemes is addressed in Section VI-D. In Section VI, two case studies are simulated for the optimal attack schemes; Concluding remarks are given in Section VII.

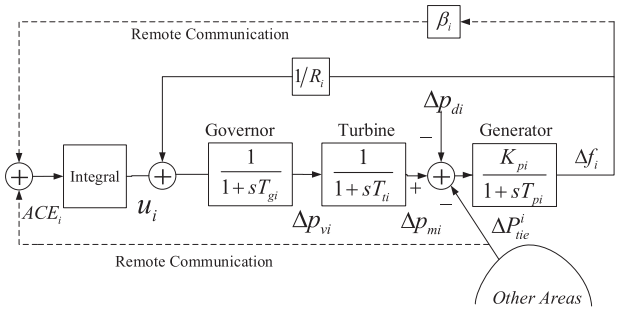


FIGURE 1. Diagram of load frequency control model.

II. BASICS OF LOAD FREQUENCY CONTROL

For simplicity, classic equivalent unit-based LFC model is given to illustrate how LFC works. The diagram of LFC model of area i (containing one equivalent unit) is shown in Fig. 1 [10]. Δp_{vi} represents the valve position change; Δp_{mi} represents the mechanical power change; Δp_{di} represents the load variation, and R_i is the droop coefficient. Let:

$$x_i = \left[\Delta f_i \quad \Delta P^i_{tie} \quad \Delta p_{mi} \quad \Delta p_{vi} \quad \int ACE_i \right]^T$$

the state-space representation of the transfer function-based model can be written by [11]:

$$\begin{cases} \dot{x}_i = A_i x_i + B_i u_i + \sum_{j \in N_i} E_{ij} \Delta f_j + F_i \Delta p_{di} \\ y_i = C_i x_i \end{cases} \tag{1}$$

The controlled output y_i represents the area control error (ACE_i):

$$y_i = ACE_i = \beta_i \Delta f_i + \Delta P^i_{tie} \tag{2}$$

where Δf_i (ΔP^i_{tie}) represents the frequency (tie-line power) deviation; β_i represents the bias coefficient. ACE_i evaluates the active power imbalance of the control area i and is used as the feedback signal. By replacing u_i in (1) with the integral controller $u_i = K_i \int ACE_i$, $B_i u_i$ can be merged into $A_i x_i$, thus achieving $\bar{A}_i x_i$:

$$\dot{x}_i = \bar{A}_i x_i + \Delta_i \tag{3}$$

where $\Delta_i = \sum_{j \in N_i} E_{ij} \Delta f_j + F_i \Delta p_{di}$. The definitions of matrices (e.g., E_{ij} and F_i) can be found in [11].

III. BASICS OF COORDINATED ATTACK ON LOAD FREQUENCY CONTROL

By aggregating each subsystem (3), it follows that the overall system can be written as:

$$\dot{x} = \bar{A}x + \Delta \tag{4}$$

where

$$\Delta = diag\begin{pmatrix} F_1 & \cdots & F_n \end{pmatrix}\begin{bmatrix} \Delta p_{d1} & \cdots & \Delta p_{dn} \end{bmatrix}^T$$

Furthermore, suppose the attacker injects false signal Δp_{ai} into ACE_i, (4) can be rewritten by:

$$\dot{x} = \bar{A}x + \Delta + \Gamma \tag{5}$$

where

$$\Gamma = diag\begin{pmatrix} G_1 & \cdots & G_n \end{pmatrix}\begin{bmatrix} \Delta p_{a1} & \cdots & \Delta p_{an} \end{bmatrix}^T$$

Based on (5), it can be learned that the attacker can disrupt the system responses by injecting Δp_{ai} and manipulating Δp_{di} simultaneously.

Assumption 1: Δp_{di} contains normal load variation Δp_{dni} and malicious load manipulation Δp_{dai}; Δp_{dai} is tens even hundreds of times more than Δp_{dni} in magnitudes (in order to produce explicit frequency excursions). Hence, Δp_{di} is regarded as Δp_{dai} approximately.

A. POSITIONING OF COORDINATED ATTACK ON LFC

Suppose the attacker has limited capability and can only exercise one certain Δp_{di} and Δp_{ai}. It means the attacker desires to find the best location (bus) to inject Δp_{di} and the best area to inject Δp_{ai}, thus causing maximal damages (e.g., maximal frequency excursions).

From the perspective of quasi-steady state analysis, injecting Δp_{ai} into any ACE_i would produce approximately the same frequency/generation excursions (though the transient behaviors might be slightly different). The proof is omitted here. Hence, the search problem is transformed into computation of the optimal bus for Δp_{di} injection:

$$bus^* = \arg\max_{bus_i} G\left(bus_i\right) \tag{6}$$

where bus^* represent the optimal bus; G is selected as frequency Δf_o or generation Δu_o excursions. $\Delta f_o = \left(\sum_j H_{ij}\Delta f_{ij}\right)/\sum_j H_{ij}$ represents the deviation of center-of-inertia (COI) frequency for the overall system; $\Delta u_o = \sum_i \sum_j \Delta u_{ij}/m$ denotes the average generation excursion of all generators. And these two variables are interchangeable without influencing the optimal bus selection.

B. DESIGN OF OPTIMAL ATTACK SCHEME (Δp^*_{di} & Δp^*_{ai})

Besides the positioning problem, how the attacker chooses $\Delta p_{ai}/\Delta p_{di}$ should be investigated. In this paper, attack scheme design is modeled by the optimization problem:

$$\left(\Delta p^*_{ai}, \Delta p^*_{di}\right) = \arg\max_{\Delta p_{di}, \Delta p_{ai}} G\left(\Delta p_{di}, \Delta p_{ai}\right) \tag{7}$$

(7) means that the attacker would design $\left(\Delta p^*_{ai}, \Delta p^*_{di}\right)$ to achieve maximal damage ($\Delta f_o/\Delta u_o$):

$$\left(\Delta p^*_{ai}, \Delta p^*_{di}\right) = \arg\min_{\Delta p_{di}, \Delta p_{ai}} G\left(\Delta p_{di}, \Delta p_{ai}\right) \tag{8}$$

(8) means that the attacker would design $\left(\Delta p^*_{ai}, \Delta p^*_{di}\right)$ to minimize attack cost.

From (6), it is known that the attacker should establish the mapping between (Δp_{ai}, Δp_{di}) and $\Delta f_o/\Delta u_o$. As is mentioned in the Abstract and Introduction, LFC information availability influences the attack scheme design. In this case, the information availability or unavailability requires different mapping computation technique. In the remaining of this section, optimization models using two mappings (corresponding to the two scenarios) are presented. In the first scenario, the mapping is based on precise computation of $\Delta f_o/\Delta u_o$ under the input of $\Delta p_{di}/\Delta p_{ai}$; while the second one uses fitting method to estimate $\Delta f_o/\Delta u_o$.

1) OPTIMIZATION CONSIDERING COMPLETE LFC MODEL

In this section, it is assumed that the attacker has sufficient computational capability and complete information of LFC system. The attacker knows the structure as well as the parameters of the LFC system exactly, and he can exercise the attack scheme (in the form of attack sequence) in the time step T as small as possible.

In practice, the attacker can compute $\Delta f_o(kT)$ or $\Delta u_o(kT)$ as a linear function of attack sequence $\Delta p_{di} = [\Delta p_{di}(0T)\Delta p_{di}(1T) \cdots \Delta p_{di}(kT)]^T$, $\Delta p_{ai} = [\Delta p_{ai}(0T)\ \Delta p_{ai}(1T) \cdots \Delta p_{ai}(kT)]^T$ through discretization:

$$\Delta f_o\left(kT\right) = F_f^d \Delta p_{di} + F_f^a \Delta p_{ai} \tag{9}$$

Derivation of F_d^d and F_d^a can simply be realized through triangle approximation or Euler methods, which are omitted due to space limits.

Based upon (7), the frequency maximization-oriented optimization model is presented as:

$$\begin{aligned} \max_{\Delta p_{di}, \Delta p_{ai}} \ & \Delta f_o\left(kT\right) \\ s.t.\ & \Delta f_o\left(kT\right) = F_f^d \Delta p_{di} + F_f^a \Delta p_{ai} \\ & \Delta p_{dl} \le \Delta p_{di}\left(jT\right) \le \Delta p_{du} \\ & \Delta p_{al} \le \Delta p_{ai}\left(jT\right) \le \Delta p_{au} \end{aligned} \tag{10}$$

where Δp_{dl} (Δp_{du}) is the lower (upper) limits of Δp_{di}; Δp_{al} Δp_{au} is the lower (upper) limits of Δp_{ai}.

Assumption 2: Throughout this paper, it is assumed that the attacker cannot inject false data with arbitrary values; Δp_{di} and Δp_{ai} are bounded by lower and upper boundaries.

Similarly, the average generation disruption Δu_o can be calculated by:

$$\Delta u_o\left(kT\right) = F_u^d \Delta p_{di} + F_u^a \Delta p_{ai} \tag{11}$$

By replacing the objective function in (10) with $\Delta u_o\left(kT\right)$, generation maximization-oriented model is

Algorithm 1 The Procedure of Regression

1: **Set** regression horizon H
2: **For** $i = j : length(\Delta p_{di}) - H + 1$
3: $y(j) = \Delta f_o(j + H - 1)$
4: $x(1 : H, j) = \Delta p_{di}(j : j + H - 1)$
5: $x(H + 1 : 2H, j) = \Delta p_{ai}(j : j + H - 1)$
6: **End**
7: $(R_d, R_a) = regress(y, x)$

given by:

$$\begin{aligned} &\max_{\Delta p_{di}, \Delta p_{ai}} \ \Delta u_o\,(kT) \\ &s.t.\ \Delta f_o\,(kT) = F_u^d\,\Delta p_{di} + F_u^a \Delta p_{ai} \\ &\quad \Delta p_{dl} \le \Delta p_{di}\,(jT) \le \Delta p_{du} \\ &\quad \Delta p_{al} \le \Delta p_{ai}\,(jT) \le \Delta p_{au} \end{aligned} \tag{12}$$

Δf_o and Δu_o are no longer interchangeable in the objective function when considering Δp_{di} and Δp_{ai} simultaneously. It means that optimal attack sequences in these two cases would be different.

Based upon (8), the attack cost minimization model is presented as:

$$\begin{aligned} &\min_{\Delta p_{di}, \Delta p_{ai}} \ Q\,(\Delta p_{di}, \Delta p_{ai}) \\ &s.t.\ \left| F_d^d\,\Delta p_{di} + F_d^a \Delta p_{ai} \right| \ge \Delta f_t \\ &\quad \Delta p_{dl} \le \Delta p_{di}\,(jT) \le \Delta p_{du} \\ &\quad \Delta p_{al} \le \Delta p_{ai}\,(jT) \le \Delta p_{au} \end{aligned} \tag{13}$$

where Q is the cost function, which is modeled by the energy of attack signals since the attacker wants to achieve the goal (Δf_o exceeds the threshold Δf_t) with the minimum signal energy:

$$E_s = \sum_{k=0}^{n} |x\,(n)|^2 \tag{14}$$

where x is $\Delta p_{di}/\Delta p_{ai}$.

2) OPTIMIZATION CONSIDERING REGRESSION BASED LFC MODEL

In this section, It is assumed that the attacker does not know the exact configuration of LFC system; hence, he cannot compute exact Δf_o or Δu_o as in (10) or (13). Moreover, the attacker can only change Δp_{di} or Δp_{ai} above certain time step due to limited computational capability, which is equivalent to the much bigger time step T compared with that in (10) or (13).

In this situation, the attacker can resort to regression technique to fit input data (Δp_{di} and Δp_{ai}) to output data (Δf_o and Δu_o), thus obtaining the estimation of $\Delta f_o/\Delta u_o$ even he does not know the exact model of LFC.

The operator *regress* in Algorithm 1 can be realized through least squares or absolute deviation methods, the detail is omitted here. By the aid of Algorithm 1, the regression coefficient vector R_d (R_a) for Δp_{di} (Δp_{ai}) can be obtained.

$$\Delta f_o \approx R_d^f \Delta p_{di} + R_a^f \Delta p_{ai} \tag{15}$$

By replacing $y(j)$ by $\Delta u_o(j + H - 1)$, Algorithm 1 can be used to calculate the regression coefficients for Δu_o. As with (10)-(13), frequency/generation disruption maximization-oriented or attack cost minimization-oriented optimization models can be defined.

IV. ANALYSIS OF OPTIMAL ATTACK SCHEME FOR LOAD FREQUENCY CONTROL

In this section, the positioning problem in (6) is first studied. Then, based on optimization models in Section III, optimal attack schemes and the influence on LFC performance are studied.

A. IDENTIFICATION OF OPTIMAL BUS FOR LOAD MANIPULATION

As previously mentioned, the goal of optimal bus identification is to find the bus where the attacker manipulates Δp_{di} to achieve the maximal $\Delta f_o/\Delta u_o$, and Δu_o and Δf_o are equivalent in terms of optimal bus identification. Hence, Δf_o is chosen as the evaluation criterion. It is known that Jacobian matrix is useful for quantifying the relation between angle and power deviation. Angle deviation $\Delta\theta$ in some sense can be equivalent to Δf_o; hence a sensitivity based method is used for optimal bus identification. Firstly, the relation between $\Delta P/Q$ and $\Delta V/\theta$ around nominal states are obtained as:

$$\begin{bmatrix} \Delta P \\ \Delta Q \end{bmatrix} = \begin{bmatrix} J_{11} & J_{12} \\ J_{21} & J_{22} \end{bmatrix} \begin{bmatrix} \Delta\theta \\ \Delta V \end{bmatrix} \tag{16}$$

where J is the Jacobian matrix around nominal states. Let $Q = 0$ (since only active power is considered), it follows that:

$$\Delta\theta = S\Delta P \tag{17}$$

where $S = \left(-J_{12}(J_{22})^{-1}J_{21} + J_{11}\right)^{-1}$. Column $S(:, j)$ of S represents the coefficient when the attacker manipulates Δp_d at load bus j; by summing the entries $\sum_i S(i, j)$ which correspond to the angle deviation $\Delta\theta_{gi}$ at the generator bus i, the optimal bus can be expressed by:

$$bus^* = \arg\max_{j \in N_l} \sum\nolimits_i S(i, j) \tag{18}$$

where N_l represents the set of load buses. In most cases, the utility operator rather than the attacker knows power flow calculations. In other words, J is unknown to the attacker; nevertheless, the attacker knows the topology of the power systems (e.g., drone surveillance), based upon which he can identify a set of load buses N_{lg} which are the most physically close to the generators. In practise, the attacker can find the optimal bus^* from N_{lg} through exhaustive search (e.g., in the test phase, the attacker can manipulate a small Δp_d at each element in N_{lg} to find the one which produces the maximum Δf_o).

B. DESIGN OF OPTIMAL ATTACK SEQUENCE Δp^*_{di} & Δp^*_{ai}

Based on (10), (12) and (13) defined in Section III-B1 and III-B2, four optimization models: 1) $\Delta f_o/\Delta u_o$ maximization in Scenario 1 (model I), 2) attack cost minimization in Scenario 1 (model II), 3) $\Delta f_o/\Delta u_o$ maximization in Scenario 2 (model III), 2) attack cost minimization in Scenario 2 (model IV) are generated. In the following, how to calculate the optimal attack sequence of these four models is presented.

1) OPTIMAL ATTACK SEQUENCE FOR OPTIMIZATION MODEL I

The objective of model I is the maximization of : 1) Δf_o 2) Δu_o. From (10)/(12), it can be learned that the terminal time kT determines the value of the objective function apart from parameters of LFC system.

Based upon the characteristics of dynamic systems, it is known that the older system inputs has much less influence on current states than newer system inputs. Hence, a fixed time horizon/window W is used to estimate the $\Delta f_o(kT)$/ $\Delta u_o(kT)$.

This curtailment can significantly improve computational efficiency without significantly compromising the accuracy of computation. By implementing time window W, (10) can be rewritten as

$$\begin{aligned} &\max \Delta f_o\,(W) \\ &s.t.\ \Delta f_o\,(W) = F_d^d\,\Delta p_{di} + F_d^a \Delta p_{ai} \\ &\quad \Delta p_{dl} \le \Delta p_{di}\,(jT) \le \Delta p_{du} \\ &\quad \Delta p_{al} \le \Delta p_{ai}\,(jT) \le \Delta p_{au} \end{aligned} \tag{19}$$

By substituting Δf_o in (9) into the objective function in (19), the objective function can be written as a linear function $S\Delta p^T$ of combinatorial vector of $\Delta p = \left[\Delta p_{di}\ \Delta p_{ai}\right]$. The convexity/concavity of S determines what methods can be used to calculate the optimum. Since S in this case is a linear function, then (19) is a linear programming (LP) problem, various algorithms including simplex-based or interior point methods can be used for optimum calculation. The same approach applies for (12) and is omitted here.

2) OPTIMAL ATTACK SEQUENCE FOR OPTIMIZATION MODEL II

Similar to Section IV-B1, time window W is used to improve computational efficiency. (13) can be thus rewritten as:

$$\begin{aligned} &\min \Delta p Q \Delta p^T \\ &s.t.\ \left|F_d^d\,\Delta p_{di} + F_d^a \Delta p_{ai}\right| \ge \Delta f_t(W) \\ &\quad \Delta p_{dl} \le \Delta p_{di}\,(jT) \le \Delta p_{du} \\ &\quad \Delta p_{al} \le \Delta p_{ai}\,(jT) \le \Delta p_{au} \end{aligned} \tag{20}$$

where Q is set the identity matrix based upon (14), which means that (20) is convex quadratic programming (QP) problem. It can be solved using ellipsoid method.

3) OPTIMAL ATTACK SEQUENCE FOR OPTIMIZATION MODEL III

As with Section IV-B1, $\Delta f_o/\Delta u_o$ maximization-oriented attack optimization model can be constructed using the regression model in (15). The details are omitted due to space limits.

4) OPTIMAL ATTACK SEQUENCE FOR OPTIMIZATION MODEL IV

As with Section IV-B2, attack cost minimization-oriented attack optimization model can be constructed using the regression model in (15). The details are omitted due to space limits.

V. REMEDIAL MEASURE DESIGN FOR OPTIMAL ATTACKS

In previous sections, optimal attack schemes with respect to different attack models: 1) (10) for Δf_o ((12) for Δu_o) maximization, 2) the model in (13) for attack cost minimization are discussed. Correspondingly, we study the possibility of cyber attack detection of these two attack scenarios.

A. ATTACK DETECTION OF OPTIMAL ATTACKS

Attack detection plays an essential role in distinguishing between compromised (caused by attacks) and normal system responses (e.g., system frequency), thus laying the groundwork for follow-up mitigation scheme design. Current detection techniques (e.g., classification and clustering based methods) depend on appropriate sample/feature selection and require off-line training/processing. When considering the uncertainty of system responses caused by the uncertainty of the boundary Δp_{dl} & Δp_{du} (Δp_{al} & Δp_{au}), it is even more difficult to use existing anomaly detection methods.

The key to solving attack detection is to extract the differences between compromised and normal system responses. It is intuitively obvious that maximization of Δf_o (Δu_o) will incur excess frequency (generation) excursions, which contrasts with normal low-magnitude damped responses. Hence, by programmed thresholds which are achieved through statistical analysis of normal data, compromised signals can be detected. Compared with other anomaly detection methods, threshold-based methods not only do not demand sample/feature selection and off-line training, but also require no memory to compute and have fast speed, which is very suitable for industrial applications.

In order to preserve the temporal features of the signals (which are useful to identify the initial time of the attack), a sliding window would move over the data to calculate the moving statistics of the streaming signals. The variance operator is executed to evaluate the deviation of the input data in each window. The variance operator can remove the negativeness in the original data, and thus the statistics are all positive and convenient for comparison. Specifically, the procedure for detection is as shown in Algorithm 2, where

var (*exp*) represents variance (exponential) operator; ς_f is the threshold for detection.

B. MITIGATION OF OPTIMAL ATTACKS

Once the the compromised signal (the initial time of the optimal attack) is detected, the utility (defender) should take quick action before any further deterioration of LFC performance. Mitigation of optimal attacks in some sense is equivalent to active fault tolerant control (AFTC) [12], which reacts to the fault (attack) in an attempt to maintain the stability in real-time. An AFTC system mainly contains two main parts: 1) a fault detection scheme and 2) controller reconfiguration. In Section V-A, the cyber attack (fault) detection scheme is presented; and the remaining question is the design of reconfigurable controller.

Many advanced reconfiguration mechanisms (e.g., optimization and compensation) have been presented [12]; nevertheless, they require accurate information (e.g., the magnitude of $\Delta p_d/\Delta p_a$) from the detection and considerable computation, which places heavy demands on the detector and is undesirable in engineering applications. Besides, reconfiguration methods usually have strict requirements on the system model and may only be applied to certain scenarios. They usually cannot effectively deal with more complex systems of power grids.

In this paper, a simple mitigation scheme is presented in attempt to attenuate the influence of Δp_d & Δp_a on LFC. When the detector senses the attack, EMS will 1) switch to redundant measurements and 2) restore the load. By switching to redundant measurements (from redundant sensors), the influence of Δp_a on *ACE* is attenuated; by restoring the load, the influence of Δp_d from the consumption side is attenuated.

VI. CASE STUDIES

A. CONFIGURATION OF TWO LFC SYSTEMS

Previously, two scenarios considering whether the attacker knows exact LFC system information are discussed. Optimization models (including the solution methods) in respect to specific objectives (attack goals) are addressed. In this section, two test LFC systems are tested for the optimal attack schemes.

The first LFC system (System I) is the classic LFC system, which uses the equivalent generator-based LFC model. By considering the simplicity of the classic model, it is assumed that the attacker has complete information of classic LFC system; hence, optimization models in Section IV-B1 and IV-B2 are used for case studies. The diagram of the classic model-based two-area system is shown in Fig. 2. The second LFC system is based on the Kundur's two-area four-machine system, which has complete models of the generators (including the frequency/voltage regulators) and the networks. The complexity of the system structure means that the attacker can hardly grasp LFC system information; hence, optimization models in Section IV-B3 and IV-B4 are used for case studies. The diagram is shown in Fig. 3. In both systems (Fig. 2 and 3), the tie-line interchange power ΔP_{tie} is compromised by FDI Δp_a, thus the compromised ACE would disrupt LFC system from generation side. Meanwhile, load manipulation Δp_d occurs at specific bus. As for System I, since it is based on simplified equivalent model and there exists only one aggregated load bus, positioning problem is not considered.

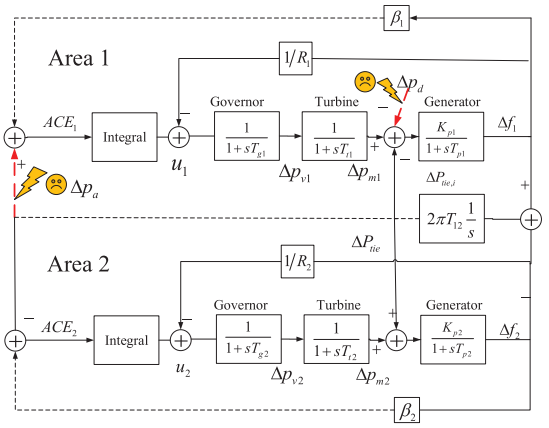


FIGURE 2. Classic model-based two-area LFC system (System I).

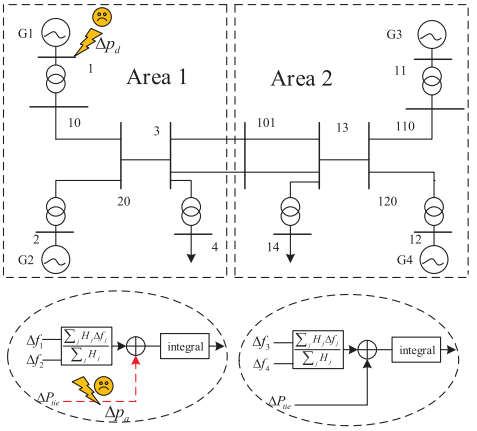


FIGURE 3. LFC based on Kundur's two-area four-machine system (System II).

B. CASE STUDY FOR SYSTEM I

In this section, System I in Fig. 2 is simulated for optimal attacks. Based on model I (II) in Section IV-B1 (IV-B2), the following three scenarios are considered.

- **Scenario 1**: The attacker tries to maximize Δf_o. The lower (upper) bound for Δp_d (Δp_a) is -0.002 *p.u.* (0.002 *p.u.*).
- **Scenario 2**: The attacker tries to maximize Δu_o. The lower (upper) bound for Δp_d (Δp_a) is -0.002 *p.u.* (0.002 *p.u.*).
- **Scenario 3**: The attacker tries to minimize $\Delta p Q \Delta p^T$ under the condition $|\Delta f_o| \geq \varepsilon_f$, where the threshold

Algorithm 2 Procedure for Attack Detection

1: **Sample** $\Delta f_o/\Delta u_o$ (the sampling rate is f_s, duration of inspection is T_s, the length of the signals is $L_s = T_s f_s$)
2: **Set** sliding window width $sw_1 = l_1$
3: **For** $i = 1 : L_s - l_1 + 1$
4: $y(i) = \Delta f_o(i : i + l_1 - 1)$
5: $x(i) = exp(var(y(i)))$
6: **End**
7: **If** $x(i) >= \varsigma_f$
8: **Then** Δf_o is compromised
9: **End**

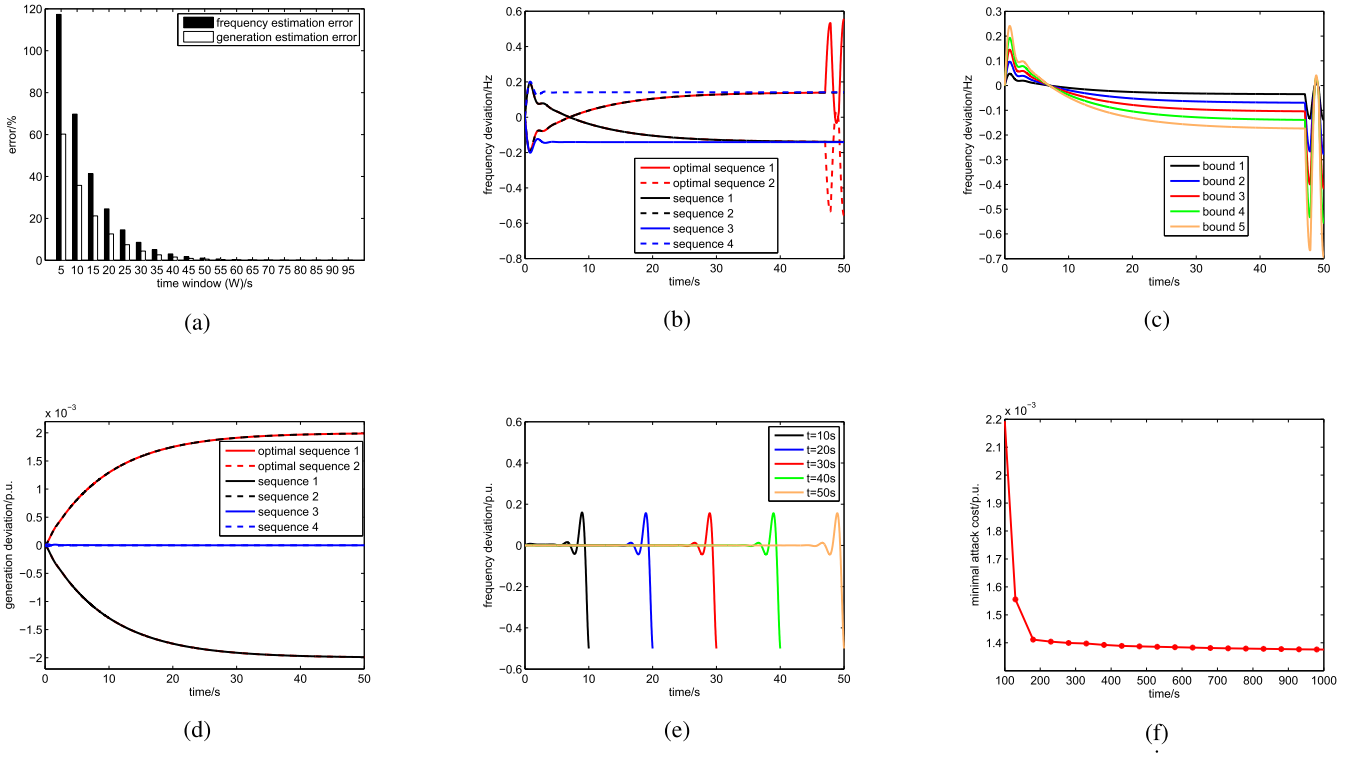


FIGURE 4. Simulation results of case study of System I. (a) Estimation errors under different time window W. (b) frequency excursions under $\Delta p_{d,a}$ and $\Delta p^*_{d,a}$. (b) frequency excursions under $\Delta p^*_{d,a}$ (with different boundaries of injection). (c) generation excursions under $\Delta p_{d,a}$ and $\Delta p^*_{d,a}$. (d) frequency excursions under minimal attack cost. (d) minimal attack cost for different execution time of attacks.

ε_f is chosen as 0.5 Hz. The lower (upper) bound for Δp_d (Δp_a) is -0.005 $p.u.$ (0.005 $p.u.$).

Before calculating the optimal attack sequence, the time window W should be first obtained. The step size for discretization is 0.01s; the time span of test data is 100s. Estimation errors under different W are shown in Fig. 4a.

As can be seen, estimation errors of both Δf_o and Δu_o decrease with the increase of W. When W reaches 50s or beyond, the reduction of errors is not so significant; hence, in the simulation, W is set 50s.

The simulation results of scenario 1 are shown in Fig. 4b. For comparison, frequency excursions under four other non-optimal attack sequences (sequence 1: $\Delta p_d = \Delta p_{dl}$, $\Delta p_a = \Delta p_{au}$; sequence 2: $\Delta p_d = \Delta p_{du}$, $\Delta p_a = \Delta p_{al}$; sequence 3: $\Delta p_d = \Delta p_{du}$, $\Delta p_a = \Delta p_{au}$; sequence 4: $\Delta p_d = \Delta p_{dl}$, $\Delta p_a = \Delta p_{al}$;) are also simulated. As can be seen, the two optimal sequences produce symmetric frequency excursions, which correspond to the maximal frequency deviations in positive and negative directions, respectively. Similarly, frequency excursions show symmetric patterns when the non-optimal sequences are mutually opposite (sequence 1 & 2, sequence 3 & 4).

From Fig. 4b, it can also be learned the steady-state frequency deviations under sequence 1 & 3 (2 & 4) are the same. This is because Δp_a are the same in sequence 1 & 3 (2 & 4). That is, Δp_a weigh more than Δp_d in disrupting Δf_o in the long term.

Furthermore, frequency excursions under optimal attack sequence (Δp^*_d, Δp^*_a) (under different bounds ($\Delta p_{dl,al}$, $\Delta p_{du,au}$)) are shown in Fig. 4c. The five bounds for (Δp_{dl}, Δp_{du}) (Δp_{al}, Δp_{au}) are: 1) ± 0.0015 $p.u.$, 2) ± 0.002 $p.u.$, 3) ± 0.0025 $p.u.$, 4) ± 0.0030 $p.u.$, and 5) ± 0.0035 $p.u.$. As can be seen, frequency excursion profiles under five bounds show a scaling relation.

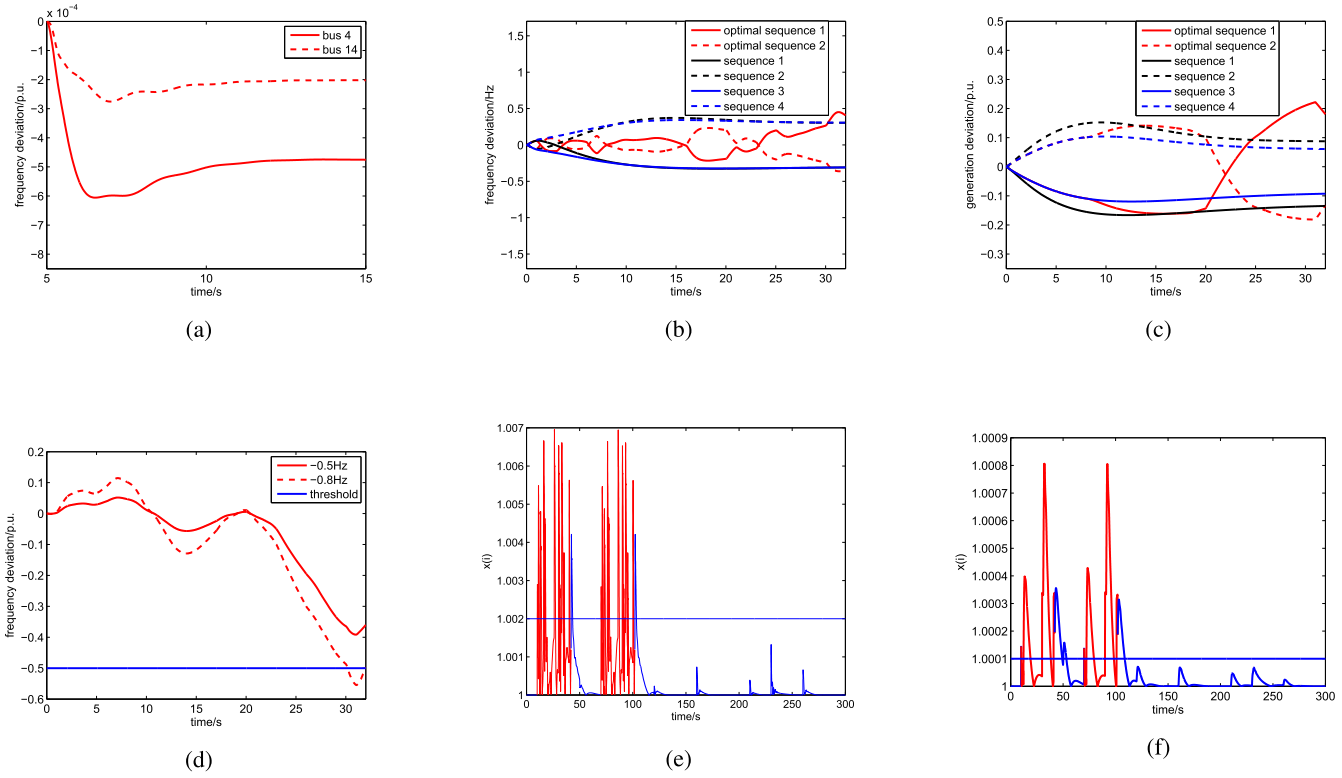


FIGURE 5. Simulation results of case study of System II. (a) frequency excursions under Δp_d into different load buses. (b) frequency excursions under $\Delta p_{d,a}$ and $\Delta p^*_{d,a}$. (c) generation excursions under $\Delta p_{d,a}$ and $\Delta p^*_{d,a}$. (d) minimal attack cost. (e) Detection of frequency optimization-oriented attacks. (f) Detection of generation optimization-oriented attacks.

The simulation results of scenario 2 are shown in Fig. 4d. As can be seen, optimal sequence 1 and sequence 2 (optimal sequence 2 and sequence 1) produce the same generation excursions; while sequence 3 & 4 almost do not disrupt the generation. This is because Δp_d and Δp_a are opposing to each other in generation disruption. Take sequence 3 ($\Delta p_a = \Delta p_{au}$, $\Delta p_d = \Delta p_{du}$) as an example. ($\Delta p_a = \Delta p_{au}$ causes $ACE < 0$, which indicates the generation deviation $\Delta u_{o1} < 0$; $\Delta p_d = \Delta p_{du}$ causes $ACE > 0$, which indicates the generation deviation $\Delta u_{o2} > 0$. Moreover, since in the classic model there exists no power loss and $\Delta p_{du} = \Delta p_{au}$. Hence, $\Delta u_o = \Delta u_{o1} + \Delta u_{o2} = 0$.

The simulation results of scenario 3 are shown in Fig. 4e and 4f. As can be seen, with the increase of execution time of the attack, the minimal attack cost also decreases (quite significantly at the inception). That is, the attacker can sacrifice attack time for cost reduction at the inception of the attack; nevertheless, this approach does not work with the passage of attack execution time.

C. CASE STUDY FOR SYSTEM II

In this section, System II in Fig. 3 is simulated for optimal attack sequence. Based on model III (IV) in Section IV-B3 (IV-B4), the following three scenarios are considered.

- **Scenario 4**: The attacker tries to maximize Δf_o. The boundaries for Δp_d are $(-0.9\ p.u., 0.9\ p.u.)$, Δp_a are $(-0.5\ p.u., 0.5\ p.u.)$.
- **Scenario 5**: The attacker tries to maximize Δu_o. The boundaries are the same as in Scenario 4.
- **Scenario 6**: The attacker tries to minimize $\Delta p Q \Delta p^T$ under the condition $|\Delta f_o| \geq \varepsilon_f$, where the threshold ε_f is chosen as 0.5 Hz. The lower (upper) bound for Δp_d (Δp_a) is $-1\ p.u.$ ($1\ p.u.$).

The simulation results of optimal bus identification are shown in Fig. 5a. It can be seen that load manipulation at bus 4 has explicit frequency excursions than at bus 14.

The simulation results for scenario 4, 5 and 6 are shown in Fig. 5b, 5c and 5d, respectively. Curves in Fig. 4b and 5b (4d and 5c) have different profiles. This is due to the difference of the boundaries and system configuration. Besides, in classic LFC model (System I), the base power for the generator and load are the same; while they are not the same for System II (the base power of the generator is much bigger than the load). Hence, in Fig. 4d, generation under ($\Delta p_d = 0.002\ p.u.$, $\Delta p_a = 0.002\ p.u.$) completely offsets with each other $\Delta u_o = 0$. generation under ($\Delta p_d = 0.9\ p.u.$, $\Delta p_a = 0.5\ p.u.$) becomes negative since $\Delta u_d > 0$ (caused by Δp_d) cannot completely offset $\Delta u_d < 0$ (caused by Δp_a) due to the inequality of base power.

As can be seen in Fig. 5b and 5c, the frequency/generation excursions under two optimal attack sequences are not symmetric as in Fig. 4b and 4d. This phenomenon is due to the cumulation of estimation errors at each execution point, which would enhance the errors between scheduled optimum

and the real excursions. Due to the errors, it can also be found that when the threshold ε_f is set exactly 0.5 Hz, the real frequency excursion (at scheduled execution time) under the minimum attack cost does not surpass the threshold (as the solid line shows in Fig. 5d). In practice, the attacker would reset the theoretical ε_f (e.g., $\varepsilon_f = 0.8\ Hz$) to make real frequency excursions surpass the desired threshold $\varepsilon_f = 0.5\ Hz$.

D. ATTACK DETECTION OF OPTIMAL ATTACK SEQUENCE

In this section, attack detection using Algorithm 2 is demonstrated. Sampling rate f_s is set 100 Hz; duration of inspection T_s is 300s; $l_1 = 10$. The optimal attack sequences in Scenario 4 and 5 occur at 10s and 70s, enduring for $H = 32s$. Normal disturbances occur intermittently during the inspection time span. By running Algorithm 2 only under normal disturbances, the threshold for detection can be achieved using the distribution of normal $x(i)$ (e.g., 97.5% confidence interval). ς_f (ς_g) for frequency (generation) maximization oriented attacks herein is set 1.002 (1.0001). The simulation results are shown in Fig. 5(e) and 5(f). As can be seen, the proposed detection methods can locate the inception of attack (10s and 70s) with explicit jump of $x(i)$. Moreover, $x(i)$ during the attack (as the red curves show), are not always above the threshold, since some parts of both frequency and generation excursions would cross equilibrium (as can be seen in Fig. 5b and 5f). The optimal H (to minimize regression errors) can be computed by both the attacker and the defender; hence, H is regarded as a known constant. It means the defender knows the duration of the optimal attacks, he just needs to calculate the inception of the attacks.

VII. CONCLUSION

In this paper, coordinated attack against LFC is considered from the perspective attack scheme, detection and mitigation. Coordinated attack scheme design is modeled as the optimization problem, in which the objective is frequency/generation maximization and attack cost minimization. The LFC system information availability to the attacker is considered in building the optimization model, based upon which two attack scenarios are used to generated to three optimization-based attack models. Through numerical studies, it is shown that attack performances vary with different attack objectives, under different situations depending on whether attackers know LFC system information or not. The results lay the groundwork for subsequent remedial measure design (e.g., the proposed threshold-based detection methods), which can assist the defender in grasping the knowledge of the attacker behaviors for better-directed mitigation scheme design.

ACKNOWLEDGMENT

(Mingjian Cui is co-corresponding author.)

REFERENCES

[1] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two-area power system: Impact identification using reachability," in *Proc. Amer. Control Conf.*, Jun. 2010, pp. 962–967.

[2] R. Tan *et al.*, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1609–1624, Jul. 2017.

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

[4] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, p. 13, 2011.

[5] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.

[6] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3864–3872, Sep. 2016.

[7] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012.

[8] S. Liu, X. P. Liu, and A. El Saddik, "Denial-of-Service (DoS) attacks on load frequency control in smart grids," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf.*, Feb. 2013, pp. 1–6.

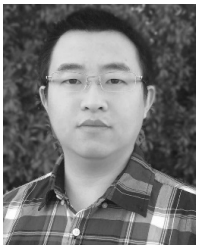
[9] A. Sargolzaei, K. Yen, and M. Abdelghani, "Delayed inputs attack on load frequency control in smart grid," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf.*, Feb. 2014, pp. 1–5.

[10] P. Kundur, N. J. Balu, and M. G. Lauby, *Power System Stability and Control*, vol. 7. New York, NY, USA: McGraw-Hill, 1994.

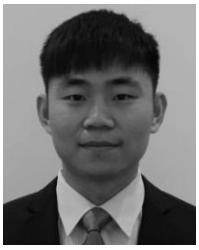
[11] C. Chen, K. Zhang, K. Yuan, Z. Gao, X. Teng, and Q. Ding, "Disturbance rejection-based LFC for multi-area parallel interconnected AC/DC system," *IET Gener., Transmiss. Distrib.*, vol. 10, no. 16, pp. 4105–4117, 2016.

[12] Y. Zhang and J. Jiang, "Issues on integration of fault diagnosis and reconfigurable control in active fault-tolerant control systems," *Fault Detection, Supervision Saf. Tech. Process.*, vol. 2, pp. 1437–1448, Aug./Sep. 2007.

CHUNYU CHEN received the B.S. degree in electrical engineering from the China University of Mining and Technology, Xuzhou, China, in 2012. He is currently pursuing the Ph.D. degree with Southeast University, Nanjing, China, and the Joint-Ph.D. degree with Southern Methodist University, Dallas, TX, USA. He is also a Visiting Student with Southern Methodist University. His research interests include power system operation and control and power system cyber security.



MINGJIAN CUI (S'12–M'16) received the B.S. and Ph.D. degrees in electrical engineering and automation from Wuhan University, Wuhan, China, in 2010 and 2015, respectively. From 2014 to 2015, he was a Visiting Scholar with the National Renewable Energy Laboratory, Transmission and Grid Integration Group, Golden, CO, USA. From 2016 to 2017, he was a Post-Doctoral Research Associate with The University of Texas at Dallas, Richardson, TX, USA. He is currently a Post-Doctoral Research Associate with Southern Methodist University, Dallas, TX, USA. He has published over 50 journal and conference papers. His research interests include power system operation, wind and solar forecasts, machine learning, data analytics, and statistics.



XINAN WANG (S'15) received the B.S. degree in electrical engineering from Northwestern Polytechnical University, Xi'an, China, in 2013, and the M.S. degree in electrical engineering from Arizona State University, Tempe, AZ, USA, in 2016. He is currently pursuing the Ph.D. degree in electrical engineering with Southern Methodist University, Dallas, TX, USA. From 2016 to 2017, he was a Research Assistant with the Advanced Power System Analytics Group, GEIRI North America, Santa Clara, CA, USA. His research interests include WAMS-related application in power system, data-driven load monitoring, and renewable energy integration.

KAIFENG ZHANG (M'10) received the Ph.D. degree from Southeast University, Nanjing, China, in 2004. From 2004 to 2006, he was a Post-Doctoral Fellow in control science and engineering with Southeast University, where he has been with the Faculty since 2006. From 2013 to 2014, he was a Visiting Scholar with Lehigh University. In 2016, he was a Visiting Scholar with the Argonne National Laboratory, Energy Systems Division. His research interests include the area of power systems dispatch and control, wind power, electricity market, and nonlinear control.

SHENGFEI YIN received the B. Eng. degree from the College of Electrical and Information Engineering, Hunan University, Changsha, China, in 2016, and the M.S. degree from the Illinois Institute of Technology, Chicago, IL, USA, in 2017. He is currently pursuing the Ph.D. degree in electrical engineering with Southern Methodist University, Dallas, TX, USA. His research interests include power market operation/optimization and data analysis in power systems.