False Data Injection Attacks on Hybrid AC/HVDC Interconnected Systems with Virtual Inertia-Vulnerability, Impact and Detection

Pan, Kaikai; Rakhshani, Elyas; Palensky, Peter

DOI
10.1109/ACCESS.2020.3013889

Publication date
2020

Document Version
Final published version

Published in
IEEE Access

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 20, 2020, accepted July 29, 2020, date of publication August 3, 2020, date of current version August 14, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3013889

False Data Injection Attacks on Hybrid AC/HVDC Interconnected Systems With Virtual Inertia–Vulnerability, Impact and Detection

KAIKAI PAN, (Member, IEEE), ELYAS RAKHSHANI, (Member, IEEE), AND PETER PALENSKY, (Senior Member, IEEE)
Department of Electrical Sustainable Energy, Delft University of Technology, 2628 CD Delft, The Netherlands
Corresponding author: Kaikai Pan (kaikaipan15@gmail.com)

ABSTRACT Power systems are moving towards hybrid AC/DC grids with the integration of HVDC links, renewable resources and energy storage modules. The load frequency control (LFC) of tomorrow has to consider the complex interactions between these components. Meanwhile, more attention should be paid to cyber security concerns as the LFC loop highly depends on data communications which may be exposed to cyber attacks. In this regard, this article aims to analyze the false data injection (FDI) attacks on the AC/DC interconnected LFC system with inertia emulation and develop advanced diagnosis tools to reveal their occurrence. We build an optimization-based framework for the purpose of vulnerability analysis. Considering the attack impact on frequency stability, it is shown that the multi-area LFC system with parallel AC/DC links and emulated inertia by storage devices is more vulnerable to FDI attacks, compared to the one without inertia emulation and the normal AC system. We then propose a detection approach to detect and isolate each FDI intrusion with a sufficient fast response, and even recover the attack value. In addition to theoretical results, the effectiveness of the proposed method is validated through simulations on the two-area AC/DC interconnected LFC system with inertia emulation capabilities.

INDEX TERMS AC/DC system, load frequency control, inertia emulation, false data injection attacks.

I. INTRODUCTION

Recent advances in power electronics have made HVDC links and renewable energy resources (RES) more popular in power system applications [1]. To better support frequency control in the modern scenarios, research activities have been carried out to develop different approaches for inertia emulation tasks [2], [3]. Such transformation does not only lead to more adaptation of conventional control schemes such as the load frequency control (LFC) to handle complex interactions between these components, but also introduce an increasing dependence on data communications. The new model of LFC must consider hybrid AC/HVDC multi-area systems incorporating virtual inertia emulation by bulk energy storage systems (ESS) [4]. Moreover, different from the control schemes which operate locally and rapidly, the high-level control of LFC loop, with a relatively slower response, would rely heavily on communication networks (e.g., the supervisory control and data acquisition (SCADA) system) to achieve wide-area data exchange [5]. However, the data in these systems are commonly transmitted through unprotected communication channels, making them more exposed to cyber intrusions including false data injection (FDI) attacks [6], [7]. We have known that a DC grid generally has a low tolerance to a fault, but it still remains largely unexplored how the hybrid AC/DC multi-area LFC system behaves under an FDI attack. Indeed, a deliberate attacker may result in severe consequences on system frequency stability [8]. Thus one need advanced tools to understand the attack strategies and detect them sufficiently fast in the context of AC/DC multi-area LFC system with emulated inertia by ESS.

A. RELATED WORK

Nowadays, the matter of virtual inertia is one of the hottest topics in the power system studies [9], [10]. Different methods for inertia emulation have been proposed for the integration of RES into the grid by using ESS [11]. In the case of multi-area AC/DC interconnected system, there are concerns

The associate editor coordinating the review of this manuscript and approving it for publication was Zhouyang Ren.

considering the virtual inertia issues. The dynamic effects of virtual inertia emulated by ESS for frequency and active power control need to be reflected in the high-level LFC loop [12], [13]. On the other hand, we can see that a lot of work has been done on the cyber security problem of pure AC multi-area LFC systems. Vulnerability and impact analysis of the AC system to cyber attacks can be found in [14], [15]. For the detection of FDI attacks which corrupt frequency stability, model-based detectors have emerged mainly from observer-based approaches in the framework of differential-algebraic equations (DAEs) [16]. For instance, an unknown input observer was employed in [17] to detect FDI attacks on the conventional AC multi-area LFC system. To be noted, these observers usually have the same degree as the system dynamics, which can cause troubles in the online implementation especially for large-scale power systems [18]. Other FDI attack detectors may come from statistical methods which always have prior assumptions on the distribution of measurement errors [19].

For the hybrid AC/DC multi-area system considering inertia emulation, however, there are still very few studies that have focused on its cyber security research [20]. To do that, it requires extensive knowledge on the dynamic behavior of the complex AC/DC system with emulated inertia and also methods or algorithms for cyber security analysis. The work in [21] studied the effect of attacks on the HVDC system and impact on the dynamic voltage stability, and proposed a predictive control based method to detect these attacks. The authors in [22] demonstrated mechanisms by which an attacker could cause system-wide unstable oscillations via loads with emulated inertia control. Recently, the literature [23] studied the possible impact of FDI attacks on the high-level LFC loop of low inertia grid under deregulated power systems, and proposed a detection approach based on the load forecasts by ensuring the availability and accuracy of such additional data. To conclude, for vulnerability and impact analysis, more efforts are still needed to learn the optimal FDI attack strategies especially in the context of AC/DC interconnected multi-area LFC system with inertia emulation capabilities. In addition, a low-order diagnosis tool for a fast response in the presence of FDI attacks is more preferred in practice. To the best of our knowledge, the following question is still not answered sufficiently,

Would it be possible to quantify the vulnerability and impact of the FDI attacks on the AC/DC interconnected LFC system with emulated inertia, and propose a diagnosis tool to detect such malicious intrusions in time?

B. CONTRIBUTIONS AND OUTLINE

In this article we aim to address the question above. For this purpose, we would first build the LFC model of the AC/DC interconnected multi-area system with added ESS for inertia emulation. A high-level control structure is presented, and possible vulnerable points of the system to FDI attacks are illustrated. Next, we introduce impact indices to evaluate the effects of FDI attacks on frequency stability. We formulate an optimization-based framework to assess the vulnerability of the AC/DC multi-area LFC system to FDI attacks. In the end, a detector in the form of residual generator with adjustable design parameters is proposed to detect, isolate and even recover each FDI intrusion. The main contributions are:

(i) Unlike many existing literature, we go beyond the study on the AC system that we explore the vulnerability and impact of the AC/DC multi-area LFC system with emulated inertia to FDI attacks. A well-constructed optimization-based framework is built to analyze the optimal attack strategies on achieving undetectability and desired impact. From both the theoretical analysis and numerical results, we have pointed out that the LFC system with AC/DC links and virtual inertial can be more vulnerable to FDI attacks, comparing with the one without virtual inertia and the normal AC system.

(ii) We further explore the attack detection problem in the AC/DC multi-area LFC system with added ESS for inertia emulation. Different from observer-based methods or other prediction-type techniques, we formulate a residual generator that can have adjustable design parameters for fast responses in attack detection. It is guaranteed that the resulting residual signal is decoupled from the system states (e.g., frequency dynamics) and load disturbances, and can recover the attack magnitude in the steady-state value of the residual. We also provide attack isolation method together with conditions of attack detectability and isolability.

In Section II, we describe the LFC model of the AC/DC interconnected multi-area system with virtual inertia emulated by added ESS, and vulnerable points on wide-area measurements are illustrated. Section III introduces the FDI attack and its optimal strategy to be disruptive and stealthy. We also propose an optimization-based framework to analyze the vulnerability and impact of the LFC system to such attacks. The FDI attack detector is developed in Section IV where we also show its capabilities of attack isolation and recovery. Numerical results are reported in Section V.

II. HYBRID AC/DC SYSTEM MODELING

In this section, the LFC system model which adapts to meet changes in the modern scenarios of parallel AC/DC lines and added ESS for inertia emulation capabilities is presented.

A. THE CONCEPT OF VIRTUAL INERTIA

For inertia emulation task, one effective way is to use the derivation of the system frequency proportionally to adjust the active power reference of a converter. Then the emulated inertia can contribute to improving the performance of the system dynamics on the inertia response. This control concept is the derivative control which calculates the rate of change of frequency (ROCOF), and can be described as

$$\Delta P_{emu} = k_a \omega_o \Delta\dot{\omega}, \tag{1}$$

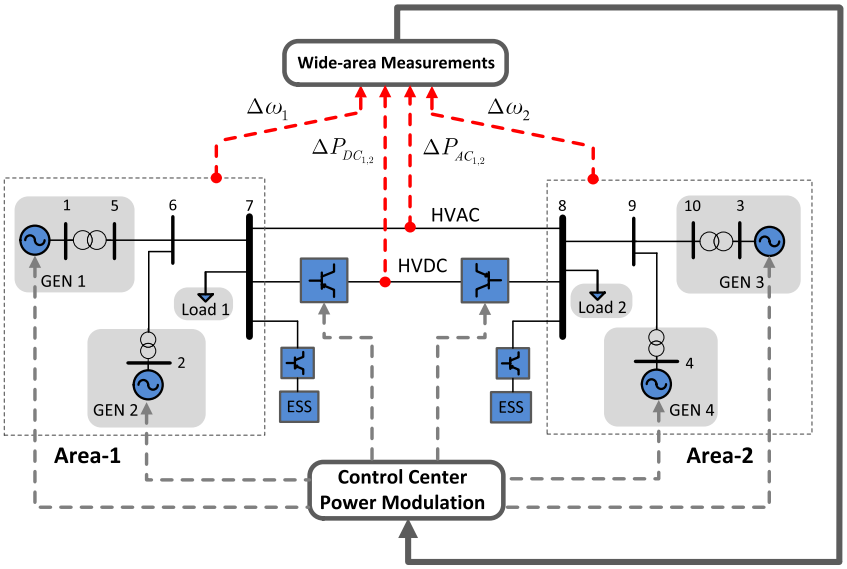


FIGURE 1. The configuration of the two-area system with parallel AC/DC links and added bulk ESS. Since the communication network between the transducers and the control center is very vulnerable, the FDI attacks of this article are mainly launched on the uploading channels (the red lines) of wide-area frequency and AC/DC power flow measurements [23].

where ΔP_{emu} is the power reference, ω_o is the nominal frequency, $\Delta\omega$ is the frequency deviation, and k_a denotes the inertial proportional conversion gain which can be selected according to an iterating tuning approach for minimizing the frequency deviations; we refer to [24] for more details.

B. AC/DC INTERCONNECTED SYSTEM WITH ESS FOR INERTIA EMULATION

A typical model for presenting a general interconnected system is a modified Kundur model with two areas and four generation units (GENs). Different from the original Kundur system in [25] where the two areas are interconnected with pure AC lines, the test system in this article is equipped with parallel AC/HVDC links and also added bulk ESS for providing virtual inertia. This modified power system is built based on the work of [13], and its block diagram is illustrated in Figure 1. We can see that two converters are added as interfaces for controlling the behavior of the bulk ESS modules in accordance with load frequency control and HVDC coordination signals to reduce the deviations of system frequency during contingencies.

The wide-area frequency and AC/DC power flow measurements are collected in each area and tie line, and sent to the control center via communication networks for power modulation. The wide-area measurements are transmitted through communication networks such as the SCADA system whose protocols (e.g., DNP3, IEC61850) are always not equipped with adequate cyber security features [26]. Considering the vulnerabilities within these communication channels, the FDI attack scenario of this article mainly focuses on the uploading paths of wide-area frequency and AC/DC power flow measurements, as depicted in Figure 1. In Section III-A, we will discuss how such FDI attacks can effect the two-area AC/DC interconnected LFC system in Figure 1.

Next, we describe the adopted LFC system model of this article. The LFC concept is known as high-level control application at the transmission level. The conventional LFC model needs to be modified to meet the the necessary changes in modern power system scenarios of parallel AC/HVDC links and added ESS for the matter of inertia emulation, as shown in Figure 1. In the work of LFC, we are interested in collective performance of all generators in the system, and hence the inter-machine oscillations and transmission system performance are not considered [25]. Each area of a power system is usually represented by a simplified/linearized model comprised of equivalent governors, turbines and generators [18]. Additionally, as indicated in [13], [15], [17] and [25], the LFC loop for active power and frequency stability analysis can be decoupled from the excitation part or the automatic voltage regulator (AVR) loop, since the time constant of AVR for each individual generator is quite smaller than the one of the high-level LFC control. It is feasible to use a quasi-state model that considers only the steady-state point of the voltage control loop ignoring its fast dynamics [5]. Till this end, it results in the high-level control structure in Figure 2 for the LFC model of the two-area AC/DC system with added ESS for inertia emulation. This system model has been introduced in [13] and different from the detailed model of Kundur, the parameters of this model are made for LFC purpose with slower dynamics.

As we can see from Figure 2, the frequency deviation of Area i in the Laplace domain can be expressed as

$$\Delta\omega_i(s) = \frac{K_{p_i}}{1+sT_{p_i}}\big[\Delta P_{m_i} - \Delta P_{L_i} - (\Delta P_{AC_{i,j}} + \Delta P_{DC_{i,j}} + \Delta P_{ESS_i})\big], \quad (2)$$

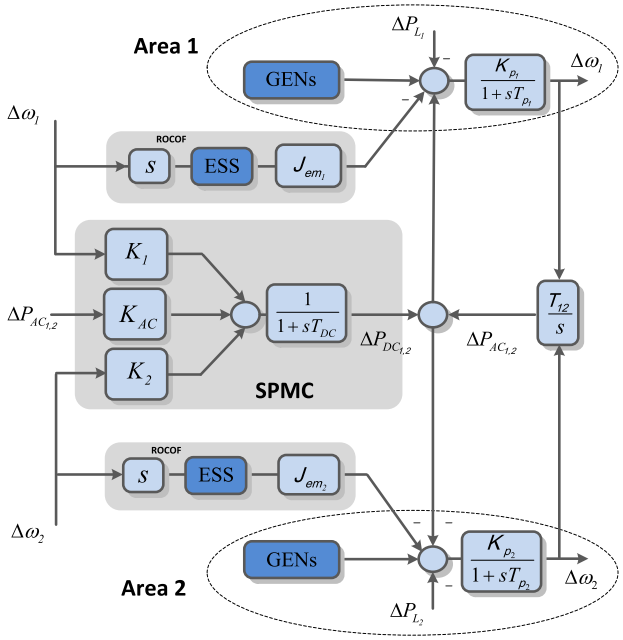


FIGURE 2. A high-level control structure for the LFC model of the two-area AC/DC interconnected system with added ESS for inertia emulation.

where K_{p_i} is the system gain associated with the damping coefficient and T_{p_i} is the system time constant related to both the equivalent inertia and the damping. ΔP_{m_i} is the total active power from all GENs within Area i, i.e., $\Delta P_{m_i} = \sum_{g=1}^{G_i} \Delta P_{m_{i,g}}$ where G_i denotes the number of participated GENs. In (2), the total load variation in Area i is mentioned by ΔP_{L_i}, and $\Delta P_{AC_{i,j}}$ is the AC power flow deviations between Area i and Area j. Comparing with the conventional LFC for AC systems, the LFC model here is adapting to consider the elements from the HVDC link and the added ESS, i.e., $\Delta P_{DC_{i,j}}$ and ΔP_{ESS_i} in (2). $\Delta P_{DC_{i,j}}$ is the power modulation by HVDC link and ΔP_{ESS_i} is the emulated power from ESS of Area i, both of which will be described later in this section. Before that, we first have

$$\Delta P_{m_{i,g}}(s) = \frac{1}{1+sT_{ch_{i,g}}}\Big[\frac{\Delta\omega_i}{R_{i,g}\times 2\pi} - \phi_{i,g}\Delta P_{agc_i}\Big], \quad (3)$$

$$\Delta P_{AC_{i,j}}(s) = \frac{T_{AC_{i,j}}}{s}\big[\Delta\omega_i - \Delta\omega_j\big]. \quad (4)$$

In (3) and (4), $R_{i,g}$ denotes the droop of each generation unit, $T_{ch_{i,g}}$ is the overall time constant of the turbine-governor model. The LFC loop generates the automatic generation control (AGC) signal ΔP_{agc_i} for active power reference of each GEN in Area i, and $\phi_{i,g}$ is an area participating factor of each GEN such that $\sum_{g=1}^{G_i} \phi_{i,g} = 1$. Besides, $T_{AC_{i,j}}$ denotes the power coefficient of the AC line between Area i and Area j. The AGC signal is to tune the setpoints of participated GENs to maintain the system frequency as its nominal value and the tie-line power as the scheduled one. The computation of ΔP_{agc_i} will be based on the Area Control Error (ACE) of Area i. Different from the typical AC multi-area system, the ACE signal of the system with parallel AC/HVDC links contains the deviations of frequency in that area and both AC/DC power flows, and acts as an input for the integral control action, i.e.,

$$ACE_i = \frac{\beta_i}{2\pi}\Delta\omega_i + (\Delta P_{AC_{i,j}} + \Delta P_{DC_{i,j}}), \quad (5)$$

$$\Delta P_{agc_i} = K_{I_i}\frac{ACE_i}{s}, \quad (6)$$

where β_i is the frequency bias and K_{I_i} represents the integral gain of the AGC controller.

To model the HVDC link for dynamic analysis on the interconnected LFC system, we use the concept of Supplementary Power Modulation Controller (SPMC). As illustrated in Figure 2, the SPMC is designed as a high-level damping controller to improve the performance of power system during load changes. The inputs of SPMC consist of frequency deviations in the interconnected areas and deviations of the transmitted power in the AC line. Then the output of SPMC is used for the HVDC link to generate the desired DC power by changing the duty cycles of converters. Thus the coordinated control strategy acting as a supplementary power modulation for this DC link can be described by

$$\Delta P_{DC_{ref}} = K_i\Delta\omega_i + K_j\Delta\omega_j + K_{AC}\Delta P_{AC_{i,j}}, \quad (7)$$

$$\Delta P_{DC_{i,j}}(s) = \frac{1}{1+sT_{DC}}\Delta P_{DC_{ref}}, \quad (8)$$

where $\Delta P_{DC_{ref}}$ is the desired DC power reference, K_i, K_j, K_{AC} are used as control gains, and T_{DC} is the time constant of the HVDC link. For this type of high-level control, the proper time response could be between 100 ms to 500 ms [13]. In this article, it is assumed 100 ms for T_{DC}.

For the inertia emulation process, according to the control law in Section II-A, the deviation of active power output from the ESS in each area, namely ΔP_{ESS_i}, can be written as

$$\Delta P_{ESS_i}(s) = \frac{J_{em_i}}{1+sT_{ESS_i}}[s\Delta\omega_i(s)], \quad (9)$$

where T_{ESS_i} is the time constant of the derivative-based components. Notably, in practice, the derivative based control strategy might be sensitive to the noise especially during the measurements of frequency signals. Therefore, a low-pass filter can be added to the model for eliminating the effects of noise. In this study, the dynamics of such a filter with storage elements is considered by the time constant T_{ESS_i}. From (9), there will be two gains (J_{em_1} and J_{em_2}) representing the virtual inertia for these two areas. As stated in Section II-A, the values of these two gains can be obtained from the iterating optimization approach in [24]. For the inertia emulation control of this article, it is assumed that we have enough energy stored in the DC side of the converter station, and the stored energy from ESS is only used for a short period of time (2 s to 5 s) to provide virtual inertia. We have simplified the ESS model in this article as only the dynamic effects of inertia emulation on high-level LFC loop have been considered. The detail of state of the charge is not modeled but its value is assumed to be always brought back close to the higher limit during off-peak period.

Thus finally, based on the equations (2) to (9), the LFC system model under the high-level control structure for the exemplary two-area system with parallel AC/DC links and added bulk ESS for virtual inertia emulation can be presented by the following state equation,

$$\dot{\boldsymbol{X}}(t) = \boldsymbol{A}_c\boldsymbol{X}(t) + \boldsymbol{B}_{c,d}\boldsymbol{d}(t), \tag{10}$$

where $\boldsymbol{X} \in \mathbb{R}^{n_X}$ represents the vector of all state variables and $\boldsymbol{d} \in \mathbb{R}^{n_d}$ is the system input of load variations, namely,

$$\boldsymbol{X} := \Big[\Delta\omega_1\ \Delta\omega_2\ \Delta P_{m_{1,1}}\ \Delta P_{m_{1,2}}\ \Delta P_{m_{2,1}}\ \Delta P_{m_{2,2}}\ \Delta P_{agc_1}\ \Delta P_{agc_2}\ \Delta P_{AC_{1,2}}\ \Delta P_{DC_{1,2}}\ \Delta P_{ESS_1}\ \Delta P_{ESS_2}\Big]^\top,$$

$$\boldsymbol{d} = \Big[\Delta P_{L_1}\ \Delta P_{L_2}\Big]^\top.$$

In (10), $\boldsymbol{A}_c$ and $\boldsymbol{B}_{c,d}$ are constant matrices with appropriate dimensions. Overall, in the LFC model of the two-area AC/DC interconnected system which also has two inertia emulators, there are three new state variables ($\Delta P_{DC_{1,2}}$, ΔP_{ESS_1} and ΔP_{ESS_2}) of synchronous controllers that would be added, comparing with the one of a normal AC system. In addition to (10), we can also derive an output model where the wide-area measurements of frequencies and AC/DC power flows are available in the control center of Figure 1. Thus we can have

$$\boldsymbol{Y}(t) = \boldsymbol{C}\boldsymbol{X}(t), \tag{11}$$

where $\boldsymbol{Y} \in \mathbb{R}^{n_Y}$ represents the system output and $\boldsymbol{C}$ is the output matrix. The formulations of these matrices $\boldsymbol{A}_c$, $\boldsymbol{B}_{c,d}$ and $\boldsymbol{C}$ in the equations (10) and (11) of continuous-time model of LFC are given in Appendix A. In the end, for the purpose of numerical analysis, (10) and (11) need to be discretized. To obtain the analytical solution for the discretization, the matrices $\boldsymbol{A}$ and $\boldsymbol{B}_d$ of sampled discrete-time model with a sampling-period T_s become [27],

$$\boldsymbol{A} = e^{\boldsymbol{A}_c T_s}, \quad \boldsymbol{B}_d = \int_{t=0}^{T_s} e^{\boldsymbol{A}_c(T_s-t)}\boldsymbol{B}_{c,d}\mathrm{d}t. \tag{12}$$

III. FDI ATTACKS ON THE AC/DC MULTI-AREA LFC SYSTEM

As discussed in the preceding, we consider a high-level structure of control and security for the AC/DC multi-area LFC system with inertia emulation by added ESS.

A. FDI ATTACK BASICS: VULNERABILITY AND IMPACT

An FDI attack can modify the wide-area measurement to a lower or higher value. Thus the discrete-time model of system output under FDI attacks can be described by

$$\tilde{\boldsymbol{Y}}[k] = \boldsymbol{C}\boldsymbol{X}[k] + \boldsymbol{f}[k], \tag{13}$$

where $\tilde{\boldsymbol{Y}}[\cdot]$ is the corrupted output and $\boldsymbol{f}[\cdot]$ denotes FDI attacks. In this article, we mainly consider the general "stationary" FDI attack where it occurs as a constant bias injection $\boldsymbol{f}$ at an unknown time instance $k_{\min}$. Other scenarios such as scaling, ramp, pulse and random FDI attacks are referred to [19]. These corruptions on the wide-area measurements would affect the dynamics of the controllers and consequently the involved system. As shown in Figure 1, the FDI attacks are mainly on the wide-area frequency and AC/DC power flow measurements, which would corrupt the AGC operation and HVDC coordination as the wide-area measurements are acting as inputs for these supervisory control loops. Note that instead of the external wide-area measurements, the virtual inertial emulator is using the local information only for a faster response and thus not attacked. For instance, an FDI attack on the AC power flow measurement between Areas i and j, say $f_{AC_{i,j}}$, can manipulate the supervisory loops of both AGC and SPMC. This attack can change (5) and (7) into the following equations respectively,

$$ACE_i = \frac{\beta_i}{2\pi}\Delta\omega_i + (\Delta P_{AC_{i,j}} + f_{AC_{i,j}} + \Delta P_{DC_{i,j}}),$$
$$\Delta P_{DC_{ref}} = K_i\Delta\omega_i + K_j\Delta\omega_j + K_{AC}(\Delta P_{AC_{i,j}} + f_{AC_{i,j}}).$$

Thus the state equation under FDI attacks in the discrete-time mode can be expressed as

$$\boldsymbol{X}[k+1] = \boldsymbol{A}\boldsymbol{X}[k] + \boldsymbol{B}_d\boldsymbol{d}[k] + \boldsymbol{B}_f\boldsymbol{f}[k], \tag{14}$$

where the matrix $\boldsymbol{B}_f$ relates FDI attacks to the system states. Note that $\boldsymbol{B}_f$ is obtained through the same matrix transformation as $\boldsymbol{B}_d$ in (12), while the matrix $\boldsymbol{B}_{c,f}$ in the continuous-time model depends on the specific attack scenario. In Appendix A, we also provide an instance where all the vulnerable wide-area frequency and AC/DC power flow measurements are attacked by FDI attacks to illustrate how the matrix $\boldsymbol{B}_{c,f}$ is formulated.

Remark 1 (Vulnerability of Different LFC System Models Under FDI Attacks): Consider the LFC models of the following systems under FDI attacks,

- *normal AC system,*
- *AC/DC interconnected system,*
- *AC/DC interconnected system with inertia emulation.*

We can see that, different from the pure AC system, the hybrid system with parallel AC/HVDC links and added ESS for inertia emulation would have more vulnerable points to FDI attacks. Intruders can manipulate the wide-area measurements of frequencies and both AC and DC power flows. According to the high-level control structure, corruptions on these wide-area measurements can affect the supervisory control - both the AGC and SPMC loops. In Section V-B we would present simulation results for this analysis.

An advanced FDI attacker also considers the impact of various attack strategies. The frequency properties that can be influenced by FDI attacks are mainly maximum frequency deviation (MFD) or steady-state frequency deviation (SSFD). In this article, we use the former MFD during the transients as the attack impact index. Intuitively, for a univariate FDI attack where only one measurement is compromised, a larger constant injection is more desired to cause the maximum damage. In this article, the attack is said to be disruptive to the system when the impact index MFD arrives at a certain value. For instance, in Figure 3, this (absolute) value is selected

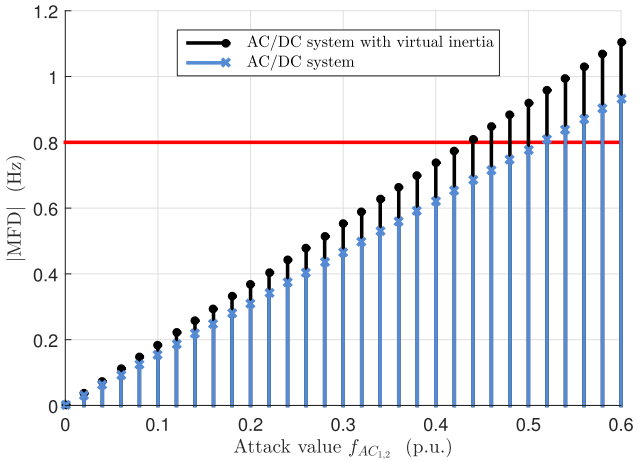


FIGURE 3. The MFD of Area 1 under various values of a univariate attack $f_{AC_{1,2}}$. The red line indicates the MFD limit for having a disruptive FDI attack.

to be 0.8 Hz, as it may mislead to trigger a possible load shedding scheme when the frequency reaches 59.2 Hz (for a 60 Hz system) according to [28]. In Figure 3, we can see that with the increase of the univariate attack value, the MFD becomes larger. To be disruptive, it can be inferred from Figure 3 that the univariate attack value on the AC power flow measurement of the two-area AC/DC interconnected LFC system with emulated inertia should be a minimum of 0.44 p.u. (for the base of 100 MW), while it is 0.52 p.u. in the AC/DC system without considering virtual inertia. These values are obtained by simulations on the LFC models of different systems under the univariate attack $f_{AC_{1,2}}$.

B. DISRUPTIVE STEALTHY FDI ATTACK STRATEGIES

The univariate attack for a large impact in Figure 3 may be detectable since it may go beyond possible thresholds and trigger data quality alarms. An intelligent attack should attend to pursue a desired impact and also satisfy the undetectability criterion [29]. In this regard, the attacker may be required to have vast attack resources to manipulate multiple data channels (i.e., multivariate attacks) and enough knowledge of the targeted system operations (e.g., the parameters of the LFC system model in Section II and also the data quality checking programs). Then the attacker can select "appropriate" injection values. This ensures that the worst-case attack scenario is considered in the vulnerability analysis. The vulnerability of a multi-area LFC system to such optimal FDI attacks can be quantified by computing the attack resources needed by the attacker to achieve the targets on attack impact and undetectability, which can be formalized in the following definition.

Definition 2 (Vulnerability to Disruptive Stealthy Attacks): Consider an FDI attack with $\boldsymbol{f}$. *We call it a* disruptive stealthy attack *if* $\boldsymbol{f}$ *takes values from the set*

$$\mathcal{F} := \left\{ \boldsymbol{f} \in \mathbb{R}^{n_Y} : \boldsymbol{b_{min}} \leq \boldsymbol{F_f f} \leq \boldsymbol{b_{max}} \right\}, \tag{15}$$

where the vectors $\boldsymbol{b_{min}}, \boldsymbol{b_{max}} \in \mathbb{R}^{n_b}$ *and the matrix* $\boldsymbol{F_f} \in \mathbb{R}^{n_b \times n_Y}$ *are scenario specific. The following Remark 3 shows that the selections of* $\boldsymbol{b_{min}}$, $\boldsymbol{b_{max}}$, $\boldsymbol{F_f}$ *may be adjusted according to different national grid codes. Thus, to describe the vulnerability of multi-area LFC systems to the disruptive stealthy attacks, one can formulate an optimization program to compute the needed attack resources by the adversary to achieve its targets on attack impact and undetectability,*

$$\begin{aligned} \alpha_i^\star := \min_{\boldsymbol{f}} \quad & \| \boldsymbol{f} \|_0 \\ s.t. \quad & \boldsymbol{f} \in \mathcal{F}, \ \boldsymbol{f}(i) = \mu, \\ & \boldsymbol{f}(j) = 0, \ \text{for all } j \in \mathcal{P}. \end{aligned} \tag{16}$$

where $\| \cdot \|_0$ *denotes the zero vector norm (the number of non-zero elements in a vector),* $\boldsymbol{f}(i)$ *is the injection with value* μ *on a specific measurement that the attacker can already access. We also add the constraint that some well-protected data channels (in the set* $\mathcal{P}$*) cannot be attacked. The multi-area LFC system is more vulnerable to the attack with a smaller* $\alpha_i^\star$ *as it requires fewer data channels to be manipulated to achieve its targets.*

The optimization program (16) is NP-hard. We can use the big M method to express (16) as a mixed integer linear program (MILP) which can be solved by appropriate solvers. We omit the details and refer to [14] for a similar reformulation.

Remark 3 ($\boldsymbol{b_{min}}$, $\boldsymbol{b_{max}}$ *and* $\boldsymbol{F_f}$ *Selection for Disruptive Stealthy Attacks): For an effective attack strategy, the selection of parameters* $\boldsymbol{b_{min}}$, $\boldsymbol{b_{max}}$ *and* $\boldsymbol{F_f}$ *in* (15) *are critical. To be precise, the disruptive stealthy attacks need to satisfy the following criteria [17], [19],*

(i) *To avoid triggering data quality alarms, the frequency deviation after attack corruptions should remain within a range,*

$$\Delta\omega_{min} \leq \Delta\omega_{i,f} \leq \Delta\omega_{max}.$$

(ii) *The calculated ACE of Area i during attacks,* $ACE_{i,f}$*, should not exceed a permitted value,*

$$|ACE_{i,f}| \leq ACE_{max}.$$

(iii) *Similarly, the computed power reference signal for the HVDC link under FDI attack,* $\Delta P_{DC_{ref,f}}$*, should not exceed an acceptable value,*

$$|\Delta P_{DC_{ref,f}}| \leq \Delta P_{DC_{ref,max}}.$$

(iv) *To be disruptive to the frequency stability, the MFD after FDI corruptions should reach a certain value.*

It is worth mentioning that the limits of (i) - (iv) are system dependent as reflected in the different national grid codes. In this article, the values of $\Delta\omega_{min}$, $\Delta\omega_{max}$, ACE_{max} and $\Delta P_{DC_{ref,max}}$ in (i) - (iii) are set to be -0.1 Hz, 0.1 Hz, 0.05 p.u. and 0.1 p.u., respectively, according to the references [25], [30]–[32]. For (iv), as mentioned earlier, the (absolute) value of MFD should reach 0.8 Hz for a disruptive FDI attack from the grid code in [28].

IV. ATTACK DETECTION, ISOLATION AND RECOVERY

In this section, a detector in the form of residual generator is developed for the detection, isolation and recovery of the FDI attack that corrupts the two-area LFC system with parallel AC/DC links and added ESS for inertia emulation. To do that, let us first reformulate the LFC system model under FDI attacks in the state-space representation of Section II into a general DAE description. Consider a time-shift operator q that $q\boldsymbol{x}[k] \rightarrow \boldsymbol{x}[k+1]$. One can fit (13) and (14) into,

$$\boldsymbol{H}(q)\boldsymbol{x}[k] + \boldsymbol{L}(q)\boldsymbol{y}[k] + \boldsymbol{F}(q)\boldsymbol{f}[k] = 0, \tag{17}$$

where $\boldsymbol{x} := [\boldsymbol{X}^\top \ d^\top]^\top$ contains all the unknown signals of system states and "disturbances" (load variations of this article), $\boldsymbol{y} := \tilde{\boldsymbol{Y}}$ denotes the available system output for a detector. Let n_x, n_y and n_r be the dimensions of $\boldsymbol{x}[\cdot]$, $\boldsymbol{y}[\cdot]$ and the row number of (17). Then $\boldsymbol{H}(\cdot)$, $\boldsymbol{L}(\cdot)$ and $\boldsymbol{F}(\cdot)$ are polynomial matrices in terms of q such that

$$\boldsymbol{H}(q) := \begin{bmatrix} -q\boldsymbol{I} + \boldsymbol{A} & \boldsymbol{B}_d \\ \boldsymbol{C} & \boldsymbol{0} \end{bmatrix}, \boldsymbol{L}(q) := \begin{bmatrix} \boldsymbol{0} \\ -\boldsymbol{I} \end{bmatrix}, \boldsymbol{F}(q) := \begin{bmatrix} \boldsymbol{B}_f \\ \boldsymbol{I} \end{bmatrix}.$$

A. FDI ATTACK DETECTOR CONSTRUCTION

The principle of an FDI attack detector is to generate a diagnosis signal to reveal the presence of the attack, giving the available data $\boldsymbol{y}[k]$. Definition 4 characterizes its task.

Definition 4 (FDI Attack Detection): The diagnosis signal from the detector differentiates whether the system output is a consequence of normal disturbances or FDI attacks. Thus ideally it relates a non-zero mapping from the attack to the diagnosis signal, while it is decoupled from the effects of unknown system states and disturbances.

In this article, we restrict the attack detector to a type of residual generator with linear transfer operations [18], i.e., $r[k] := \boldsymbol{R}(q)\boldsymbol{y}[k]$, where $r[\cdot]$ is called the residual signal for diagnosis, $\boldsymbol{R}(q)$ is the transfer function that needs to be designed. Considering that $\boldsymbol{y}[\cdot]$ is associated with $\boldsymbol{L}(q)$ in (17), we propose a formulation of $\boldsymbol{R}(q) := \boldsymbol{a}(q)^{-1}\boldsymbol{N}(q)\boldsymbol{L}(q)$. Now the task of detector construction comes to the design of $\boldsymbol{N}(q)$ whose dimension and predefined order are n_r and d_N, if the denominator $\boldsymbol{a}(q)$ with sufficient order to make $\boldsymbol{R}(q)$ physically realizable is determined. Multiplying the left of (17) by $\boldsymbol{a}(q)^{-1}\boldsymbol{N}(q)$ would lead to

$$\begin{aligned} r[k] &= \boldsymbol{a}(q)^{-1}\boldsymbol{N}(q)\boldsymbol{L}(q)\boldsymbol{y}[k] \\ &= \underbrace{-\boldsymbol{a}(q)^{-1}\boldsymbol{N}(q)\boldsymbol{H}(q)\boldsymbol{x}[k]}_{\text{(I)}} \underbrace{-\boldsymbol{a}(q)^{-1}\boldsymbol{N}(q)\boldsymbol{F}(q)\boldsymbol{f}[k]}_{\text{(II)}}. \end{aligned} \tag{18}$$

Term (I) is the part from the effect of unknown system states and load disturbances $\boldsymbol{x}[\cdot]$. Term (II) corresponds to the FDI attack. Thus according to Definition 4, the desired detector would generate the residual signal $r[\cdot]$ that can be decoupled from $\boldsymbol{x}[\cdot]$ but keep sensitive to $\boldsymbol{f}[\cdot]$. We would expect

$$\boldsymbol{N}(q)\boldsymbol{H}(q) = 0, \quad \boldsymbol{N}(q)\boldsymbol{F}(q) \neq 0. \tag{19}$$

Inspired by (19), the following theoretical result shows an effective way for attack detection and also recovery.

Theorem 5 (FDI Attack Detection and Recovery): It can be observed that $\boldsymbol{H}(q) := \sum_{i=0}^{1}\boldsymbol{H}_i q^i$, $\boldsymbol{N}(q) := \sum_{i=0}^{d_N}\boldsymbol{N}_i q^i$ and $\boldsymbol{F}(q) := \boldsymbol{F}$. Consider an FDI attack in the set (15). A residual generator with the following linear program characterizations for (19) can have non-zero steady-state residual output that recovers the attack value $\boldsymbol{f}$,

$$\begin{cases} \bar{\boldsymbol{N}}\bar{\boldsymbol{H}} = 0, \\ -\boldsymbol{a}(1)^{-1}\sum_{i=0}^{d_N}\boldsymbol{N}_i\boldsymbol{F} = 1, \end{cases} \tag{20}$$

where the matrices $\bar{\boldsymbol{N}}$, $\bar{\boldsymbol{H}}$ are defined as

$$\bar{\boldsymbol{N}} := \begin{bmatrix} \boldsymbol{N}_0 & \boldsymbol{N}_1 & \cdots & \boldsymbol{N}_{d_N} \end{bmatrix},$$

$$\bar{\boldsymbol{H}} := \begin{bmatrix} \boldsymbol{H}_0 & \boldsymbol{H}_1 & 0 & \cdots & 0 \\ 0 & \boldsymbol{H}_0 & \boldsymbol{H}_1 & 0 & \vdots \\ \vdots & 0 & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \boldsymbol{H}_0 & \boldsymbol{H}_1 \end{bmatrix}.$$

Proof: Note that $\boldsymbol{N}(q)\boldsymbol{H}(q) = \bar{\boldsymbol{N}}\bar{\boldsymbol{H}}[\boldsymbol{I}, \ q\boldsymbol{I}, \cdots, q^{d_N+1}\boldsymbol{I}]^\top$. If $\bar{\boldsymbol{N}}\bar{\boldsymbol{H}} = 0$ as stated in (20), then the diagnosis filter becomes $r[k] = -\boldsymbol{a}(q)^{-1}\boldsymbol{N}(q)\boldsymbol{f}[k]$. The steady-state value of the residual signal under the FDI attack would become $-\boldsymbol{a}(q)^{-1}\boldsymbol{N}(q)\boldsymbol{F}(q)\boldsymbol{f} \mid_{q=1}$. To track the FDI attack magnitude, one can simply make $-\boldsymbol{a}(1)^{-1}\boldsymbol{N}(1)\boldsymbol{F}(1) = 1$. Due to that $\boldsymbol{N}(1)\boldsymbol{F}(1) = \sum_{i=0}^{d_N}\boldsymbol{N}_i\boldsymbol{F}$, the residual signal from (20) recovers the exact attack value $\boldsymbol{f}$ in the steady-state behavior of the residual generator. ■

Next, the residual generator design becomes to find a feasible $\bar{\boldsymbol{N}}$ satisfying (20). To increase the sensitivity of the residual to the attack, in addition to (20), the detector may also aim to let the coefficients of $\boldsymbol{N}(q)\boldsymbol{F}(q)$ in (19) achieve the maximum value. Then we can characterize the attack detection and recovery problem as the optimization program,

$$\begin{aligned} \gamma^\star = \max_{\bar{\boldsymbol{N}}} \quad & \left\|\bar{\boldsymbol{N}}\bar{\boldsymbol{F}}\right\|_\infty \\ \text{s.t.} \quad & \bar{\boldsymbol{N}}\bar{\boldsymbol{H}} = 0, \quad \left\|\bar{\boldsymbol{N}}\right\|_\infty \leq \eta, \\ & -\boldsymbol{a}(1)^{-1}\sum_{i=0}^{d_N}\boldsymbol{N}_i\boldsymbol{F} = 1, \end{aligned} \tag{21}$$

where the constraint $\|\bar{\boldsymbol{N}}\|_\infty \leq \eta$ is added to avoid possible unbounded solutions and it does not affect the performance of the detector. The matrix $\bar{\boldsymbol{F}}$ has a similar definition with $\bar{\boldsymbol{H}}$ in Theorem 5. Thus if we have a resulted $\gamma^\star > 0$, then the solution to (21) offers a residual generator that detects the FDI attack and also tracks the attack value.

Strictly speaking, the proposed optimization program (21) is not a linear program (LP) due to the non-convex objective function. However, as explained by a similar argument in [33, Lemma 4.3], one can view (21) as a family of n standard LPs where n is the number of columns of $\bar{\boldsymbol{F}}$.

Remark 6 (Attack Isolation): The residual generator from (21) is mainly designed for one univariate attack. For multivariate attacks ($\alpha_i^\star > 1$ from (16)), an alternative is to build a bank of residual generators where each of them aims to

detect one particular intrusion and keep insensitive to others, by considering the following "reconstructed" DAE,

$$\left[\boldsymbol{H}(q)\ \boldsymbol{F}_{-j}(q)\right]\begin{bmatrix}\boldsymbol{x}[k]\\ \boldsymbol{f}_{-j}[k]\end{bmatrix}+\boldsymbol{L}(q)\boldsymbol{y}[k]+\boldsymbol{F}_j(q)\boldsymbol{f}_j[k]=0,$$

where $\boldsymbol{F}_{-j}(q)$ is the polynomial matrix that includes all columns of $\boldsymbol{F}(q)$ except the j-th one, and similarly $\boldsymbol{f}_{-j}[k]$ contains all the elements of $\boldsymbol{f}[k]$ except the j-th one. Then the j-th residual generator can be designed using the same approach in Theorem 5 and (21) *for the j-th intrusion while isolating the effects from others. The j-th attack can be identified by the j-th residual generator since the other residual generators keep insensitive to this attack. In the end, with* (21)*, it can also recover the j-th attack's value in the steady-state behavior of the j-th residual generator.*

Remark 6 shows that the attack isolation problem can be treated as an attack detection task effectively. In the end, we provide sufficient and necessary conditions for the feasibility of attack detection and isolation.

Lemma 7: (Necessary and Sufficient Conditions of Attack Detectability and Isolability): For a univariate FDI attack ($\alpha_i^\star = 1$), it is detectable that satisfies (19) *if, and only if,*

$$Rank\left(\left[\boldsymbol{H}(q)\ \boldsymbol{F}(q)\right]\right) > Rank\left(\boldsymbol{H}(q)\right). \tag{22}$$

Next, for multivariate FDI attacks ($\alpha_i^\star > 1$), one particular intrusion $\boldsymbol{f}_j$ is isolable from others if, and only if,

$$Rank\left(\left[\boldsymbol{H}(q)\ \boldsymbol{F}(q)\right]\right) > Rank\left(\left[\boldsymbol{H}(q)\ \boldsymbol{F}_{-j}(q)\right]\right). \tag{23}$$

Proof: The detectability condition (22) is adopted from [16, Theorem 3]. Alternatively, (22) can be rewritten as $\boldsymbol{F}(q) \notin \mathrm{Im}\left(\boldsymbol{H}(q)\right)$. It ensures that the residual signal keeps sensitive to the FDI attack but decoupled from the unknown system states and disturbances. For the isolability criterion, note that from Remark 6, the $\boldsymbol{H}(q)$ in (17) has been "replaced" by $\left[\boldsymbol{H}(q)\ \boldsymbol{F}_{-i}(q)\right]$ in the reconstructed DAE. Then it is easy to obtain (23) extended from (22). Similarly, the condition (23) can be rewritten as $\boldsymbol{F}_j(q) \notin \mathrm{Im}\left(\left[\boldsymbol{H}(q)\ \boldsymbol{F}_{-j}(q)\right]\right)$. ■

V. NUMERICAL RESULTS

A. PRELIMINARIES

To evaluate the vulnerability and impact of the multi-area LFC system to FDI attacks and also validate the effectiveness of the proposed attack detection methodology, in this section, we study the exemplary two-area system with parallel AC/DC links and added ESS for inertia emulation, and provide numerical results. As shown in Figure 1, there are two GENs and one load demand center in each area. The system and control parameters of the studied case has been provided in Appendix A. Considering the characterizations of the time responses of controllers (especially inertia emulators) in the high-level structure, the sampling period T_s is given as 0.04 s [24]. We can obtain a 12-order discrete-time LFC system model which can be fitted into the DAE form of (17).

In the detector design, the degree of the residual generator is set to $d_N = 3$ which is much less than the order of the LFC system. We give the denominator a determined formulation of $\boldsymbol{a}(q) := (q-p)^{d_N}/(1-p)^{d_N}$ where p can be treated as the pole of $R(q)$, and it is normalized in steady-state value for all feasible poles. It should be mentioned that the parameters d_N and p are adjustable for a fast response of attack detection in the context of load frequency dynamics considering inertia issues. Particularly, as a general rule, the smaller the poles, the faster the residual responds, and the more sensitive the residual responds to system noise [18]. We use CPLEX to solve all the corresponding optimization programs.

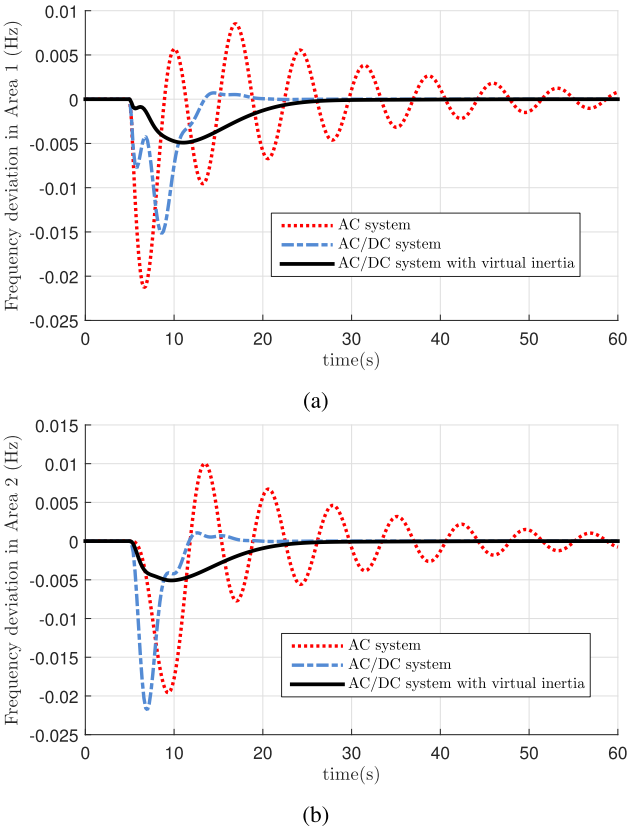


FIGURE 4. Frequency deviations under a step load change of 0.03 p.u. increase at $t = 5$ s in Load 1 of Area 1, i.e., $\Delta P_{L_1} = 0$ for $t \le 5$ s and $\Delta P_{L_1} = 0.03$ p.u. for all $t > 5$ s. (a) $\Delta\omega_1$ of Area 1; (b) $\Delta\omega_2$ of Area 2.

B. VULNERABILITY OF LFC SYSTEMS TO FDI ATTACKS

First, we present the results of frequency deviations in Figure 4 where the system input is only a step load change of 0.03 p.u. increase at $t = 5$ s in Load 1 of Area 1. The comparisons are made on LFC models of the normal AC system, the AC/DC interconnected system and the AC/DC interconnected system with inertia emulation. To be mentioned, we have introduced the supervisory frequency control of high-level LFC loop in this article. The result of Figure 4 is obtained by simulating the proposed LFC system model. The oscillations seen in Figure 4 is indeed due to the dynamics of the LFC loop which is always with a relatively slower response, comparing with the low-frequency oscillation phenomena inherent to power systems. From Figure 4, we can

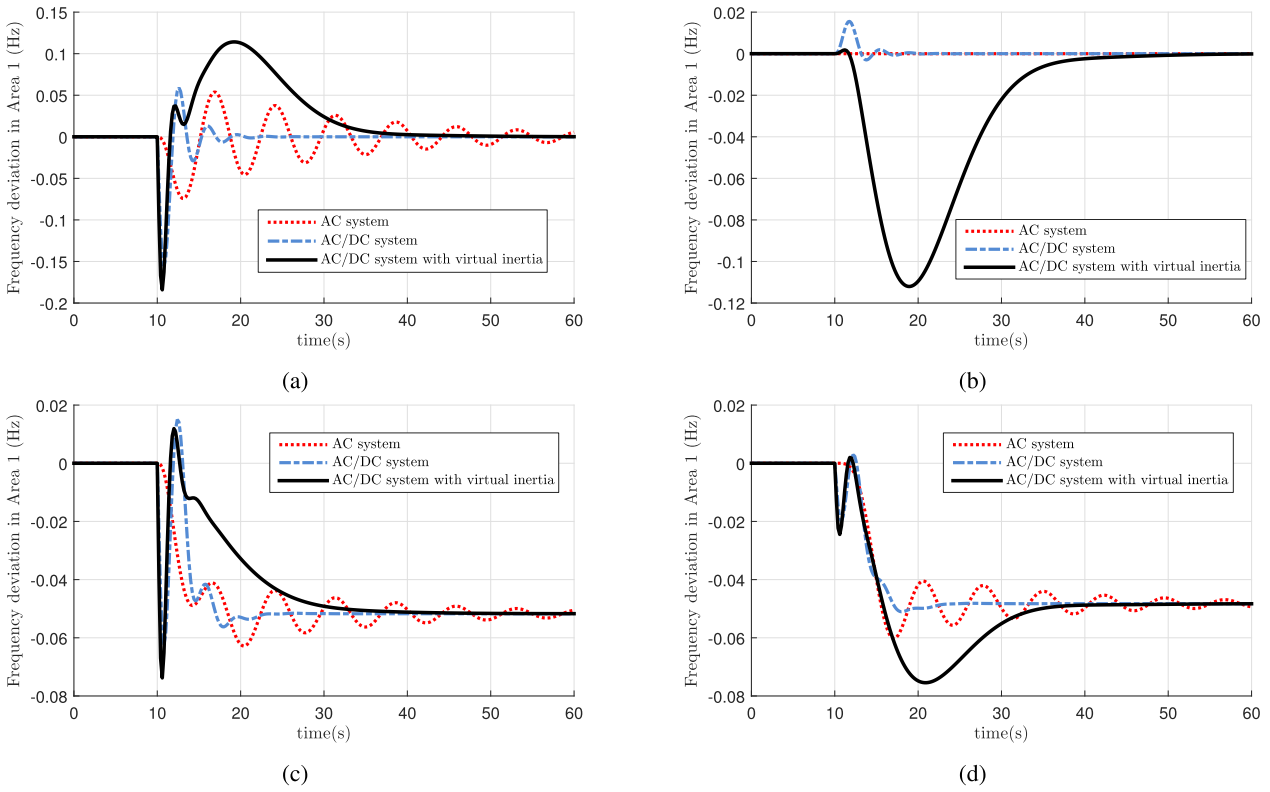


FIGURE 5. Frequency deviations of Area 1 under univariate attacks (a) on the AC link, $f_{AC_{1,2}} = 0.1$ p.u.; (b) on the DC link, $f_{DC_{1,2}} = -0.1$ p.u.; (c) on the frequency of Area 1, $f_{\omega_1} = 0.1$ Hz; (d) on the frequency of Area 2, $f_{\omega_2} = 0.1$ Hz at $t = 10$ s.

see that the HVDC link and especially, the inertia emulation provided by the added ESS, can improve the LFC system dynamics significantly in damping frequency oscillations during the step-load fault, which proves the effectiveness of the high-level LFC control structure of this article.

Next, to evaluate the vulnerability of LFC models of different systems (normal AC system, AC/DC system and AC/DC system with inertia emulation) to FDI attacks, we launch univariate attacks on the wide-area measurements of frequencies and AC/DC power flows, separately. Recall Figure 1 which shows vulnerable measurement channels. The simulation results are shown in Figure 5 for Area 1. The additional results of frequency deviations of Area 2 under these univariate attacks are provided in Figure 8 of Appendix B. In these scenarios, the univariate attack with the same attack value can cause the most severe ''damage'' to the AC/DC interconnected LFC system with virtual inertia emulated by added ESS. Comparing with LFC models of the normal AC system and the system with parallel AC/DC links but without emulated inertia, the model of AC/DC system with inertia emulation capabilities is always with larger MFDs under each univariate attack. This observation is consistent with Remark 1 of Section III-A. In fact, as stated in Remark 1, FDI corruptions on the wide-area frequencies and AC/DC power flows would affect both supervisory control loops of AGC and SPMC as these measurements are inputs to these controllers in the LFC system model. To be highlighted, even though the inertia emulator is not being attacked directly as it uses local information only, the inertia emulation task still affect the dynamic performance of the overall LFC system under FDI attacks on the wide-area measurements. This can be seen from the simulation results of Figure 5 and Figure 8 (in Appendix B). The reason could be that the inertia emulation is being ''misled'' by the frequency variations caused by the FDI attacks on the supervisory control loops, and in turn contributes to a larger MFD value.

We continue with disruptive stealthy attacks introduced in Section III-B. These FDI attacks with optimal attack strategies can be multivariate to achieve the targets on attack impact and undetectability, and are obtained by solving the optimization program (16) for vulnerability analysis. From the results of (16), an ''optimal'' multivariate attack ($\alpha_i^\star = 2$) that can manipulate both AC and DC power lines with $f_{AC_{1,2}} = 0.44$ p.u. and $f_{DC_{1,2}} = -0.39$ p.u. is a disruptive stealthy attack in the set of (15) for the proposed LFC model of the two-area AC/DC interconnected system with emulated inertia by added ESS. Figure 6 shows the frequency deviations of both areas under this multivariate attack. The MFD of Area 1 reaches -0.8 Hz at around $t = 10.6$ s while the attack is launched at $t = 10$ s, which implies a disruptive attack as defined in this article. The MFD in Area 1 of the AC/DC system without emulated inertia has

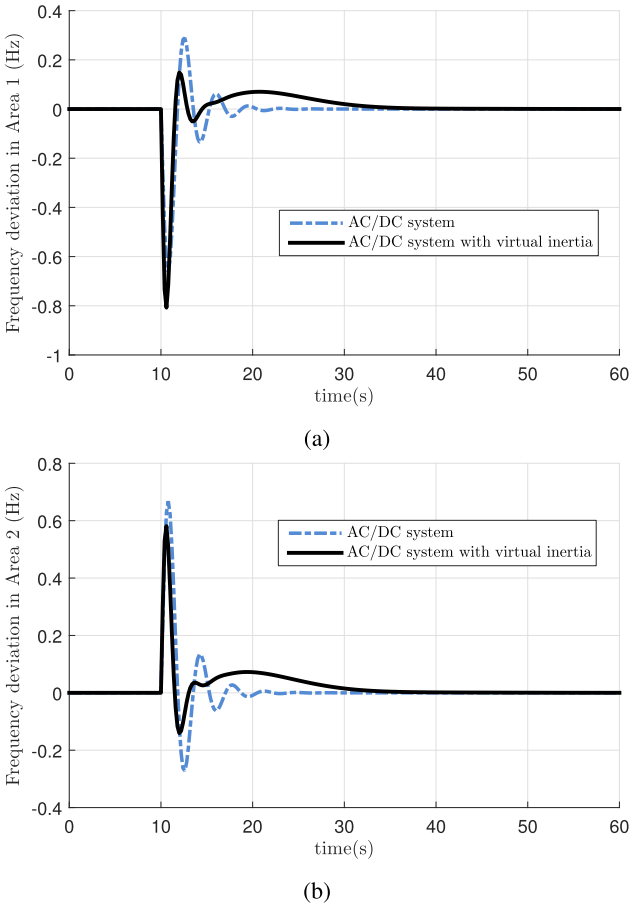


FIGURE 6. Frequency deviations under the multivariate attacks on both AC and DC links, i.e., $f_{AC_{1,2}} = 0.44$ p.u. and $f_{DC_{1,2}} = -0.39$ p.u.. (a) $\Delta\omega_1$ of Area 1; (b) $\Delta\omega_2$ of Area 2.

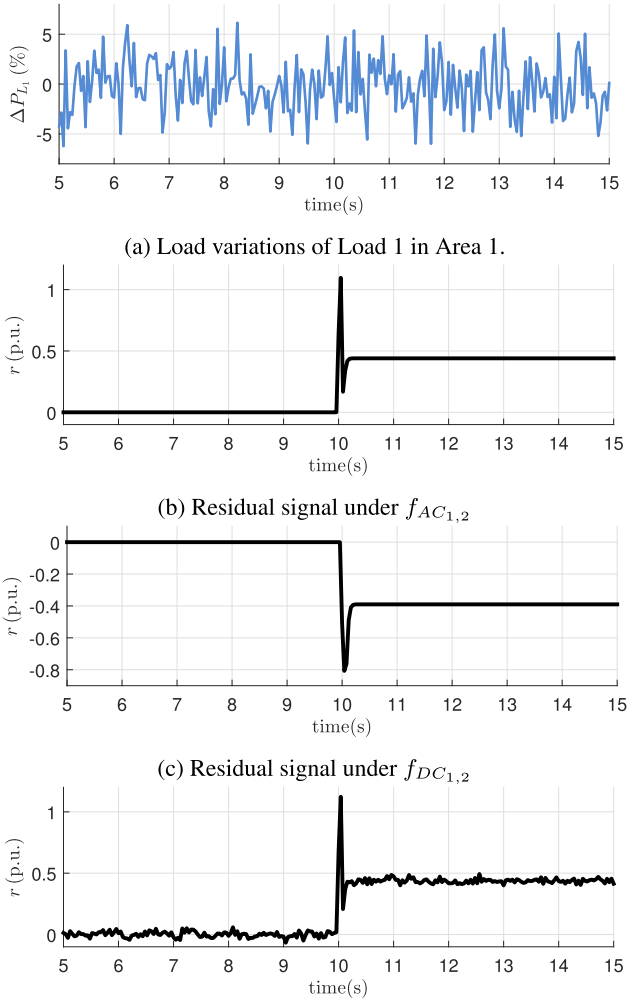


FIGURE 7. Residual responses under multivariate attacks.

reached -0.66 Hz under the same multivariate attack. To be noted, there is no disruptive stealthy attack in the type of Definition 2 when solving (16) for the LFC model of normal AC system, i.e., no multivariate attack can achieve both targets on attack impact and undetectability in such scenario. Thus from all of these observations, it is reasonable to conclude that the AC/DC interconnected LFC system considering inertia emulation is more vulnerable to FDI attacks, comparing with the one without virtual inertia and the normal AC system.

C. FDI ATTACK DETECTION AND RECOVERY

In the third simulation, we validate the proposed method for attack detection, isolation and recovery. To challenge the detector, now the system input $\boldsymbol{d}$ is modeled as stochastic load patterns; see Figure 7a for Load 1 in Area 1. The adversarial case comes from the disruptive stealthy attack obtained in the above subsection. We build a bank of two residual generators to detect and isolate the multivariate attacks $f_{AC_{1,2}}$ and $f_{DC_{1,2}}$ on the parallel AC/DC links in the two-area LFC system, using the approach in (21) and Remark 6. The optimal value of (21) achieves $\gamma^\star = 4.440$ in the residual generator construction for detecting $f_{AC_{1,2}}$ and $\gamma^\star = 2.649$ in another residual generator for detecting $f_{DC_{1,2}}$, which implies a successful detection and isolation as indicated by Lemma 7.

In Figure 7, the results of the residual generators under load disturbances and multivariate attacks are presented. Both detectors have generated a residual signal for the presence of each FDI intrusion in the multivariate attack scenario. To be noted, we can see that the resulted residual generators with designed capabilities from Theorem 5 can recover the attack values; the steady-state residual values in Figure 7b and Figure 7c are equal to 0.44 p.u. and -0.39 p.u., respectively. The residual signals are also decoupled from each other and stochastic load disturbances. Next, to test the residual generators in a more realistic setting, we also provide the simulation results where there exists noise in the system process and measurements. Zero-mean Gaussian noise with the covariance 0.0009 to the frequency and 0.03 to the other states was applied according to [17]. Figure 7d shows one instance of the residual signals under the noisy setting and it still works effectively in detecting and tracking the attack value of $f_{AC_{1,2}}$. In the end, it should be mentioned that in these

simulations the adjustable parameter, i.e., the pole of $a(q)$, is set to be $p = 0.1$ for a fast response of attack detection. The residual signal under $f_{AC_{1,2}}$ can recover the attack value from $t = 10.36$ s in Figure 7b before the MFD reaches the maximum value (at around $t = 10.6$ s) in Figure 6a. This indicates that the developed residual generator can detect the FDI intrusions sufficiently fast in the inertia context.

D. FURTHER DISCUSSIONS: ATTACK DETECTION METHOD COMPARISON

As mentioned in Section I-A, observer-based approach is another major technique for attack detection when the system models are described by DAEs. In general, the observer-based methods include state observers where an estimate of the system state is a prior, and more general output observers where the observer order can be lower (or higher) than the system state [34]. Here we try to provide a comparison of these two methods on the order of the residual generator, the design variable of complexity and the response time.

- A low-order residual generator is more desired in the on-line implementation due to its reduced computation complexity. An output observer can have a reduced order in some specific cases, while our method can have a user-defined order $d_N = 3$ versus the system dynamics $n_x = 12$.
- State observer-based method needs a precondition of system observability. The output observers have relaxed such constraints, but usually need to satisfy the so-called Luenberger-type conditions [35]. Our diagnosis tool provides an existence of a residual generator with a lower order dynamics but without these constraints.
- Comparing to the state observer, the output observer has a more general form that one has more design freedom, but also more involved design with complexity. Instead of a state-space representation, we proposed a more straightforward transfer operation in our method.
- We admit that an observer-based residual generator may also be able to detect the FDI attacks of this article. However, to the best of our knowledge, using adjustable design parameters for a fast response of attack detection especially in the inertia context has not been well studied, while our method builds on such a perspective.

VI. CONCLUSION

In this article, we investigated FDI attacks on the AC/DC interconnected LFC system with emulated inertia. We offer an optimization-based vulnerability and attack impact analysis framework. Our study shows that the AC/DC multi-area LFC system can be more vulnerable to FDI attacks. We also propose a diagnosis tool to detect, isolate and recover all the FDI intrusions. The effectiveness of these methods was validated by simulations in the two-area system with parallel AC/DC links and added ESS for providing virtual inertia. The future research includes the study of other types of cyber attacks on the hybrid AC/DC grids with virtual inertia emulation capabilities.

TABLE 1. Parameters of the generation units.

Parameters	Area 1		Area 2	
	GEN 1	GEN 2	GEN 3	GEN 4
$T_{ch_{i,g}}$ (s)	0.38	0.38	0.36	0.39
$R_{i,g}$ (Hz/p.u.)	2.4	2.5	2.5	2.7
$\phi_{i,g}$	0.5	0.5	0.5	0.5

TABLE 2. Parameters of the two-area system.

Parameters	Area 1	Area 2
K_{p_i} (p.u./Hz)	102	102
T_{p_i} (s)	20	25
β_i (p.u./Hz)	0.425	0.396
K_{I_i}	0.7	0.7
T_{ESS_i} (s)	0.026	0.026
$T_{AC_{i,j}}$ (s)	0.245	

TABLE 3. Control parameters of the studied case.

Parameters	Value
K_1	0.3
K_2	0.1
K_{AC}	4.7
J_{em_1}	0.87
J_{em_2}	0.093

APPENDIX

A. PARAMETERS OF THE TWO-AREA TEST SYSTEM

In this subsection, we provide the parameters of the two-area LFC system with parallel AC/DC links and ESS for inertia emulation. First, for the involved parameters in the equations from (2) to (9), the exact values used in the studied case of this article are listed in Table 1, Table 2 and Table 3. These values are given based on [13]. Next, we provide the detailed formulations of the matrices in the continuous-time LFC system model. This state-space model representation is derived based on the equations from (2) to (9). The system state matrix $\boldsymbol{A}_c$ can be partitioned as follows,

$$\boldsymbol{A}_c = \begin{bmatrix} \boldsymbol{A}_{11} & \boldsymbol{A}_{11} \\ \boldsymbol{A}_{21} & \boldsymbol{A}_{22} \\ \boldsymbol{A}_{31} & \boldsymbol{A}_{32} \end{bmatrix}_{(12\times 12)}.$$

Each sub-matrix of $\boldsymbol{A}_c$ and the matrix $\boldsymbol{B}_{c,d}$ related to load variations inputs are shown in the equations (24)-(25) at the bottom of the next page. As we have assumed an output model where the wide-area measurements of frequencies and AC/DC power flows are collected and transmitted to the

control center, the output matrix $\boldsymbol{C}$ becomes

$$\boldsymbol{C} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 & 0 \end{bmatrix}_{(4\times 12)}.$$

Next, we illustrate the formulation of the matrix $\boldsymbol{B}_{c,f}$ which relates the FDI attacks to the system states in the state-space model. As mentioned in Section III-A, $\boldsymbol{B}_{c,f}$ depends on the specific attack scenario. Let us consider an instance that all the vulnerable wide-area measurements are attacked by FDI attacks. These corruptions affect the supervisory control loops of both the AGC operation and the SPMC control, but not the inertia emulation task as the emulators are using local information only. Then the multivariate attacks can be described by

$$\boldsymbol{f} = \begin{bmatrix} f_{\Delta\omega_1} & f_{\Delta\omega_2} & f_{AC_{1,2}} & f_{DC_{1,2}} \end{bmatrix}^T_{(4\times 1)},$$

$$\boldsymbol{A}_{11} = \begin{bmatrix} \frac{-1}{T_{p_1}} & 0 & \frac{K_{p_1}}{T_{p_1}} & \frac{K_{p_1}}{T_{p_1}} & 0 & 0 & 0 & 0 & \frac{-K_{p_1}}{T_{p_1}} \\ 0 & \frac{-1}{T_{p_2}} & 0 & 0 & \frac{K_{p_2}}{T_{p_2}} & \frac{K_{p_2}}{T_{p_2}} & 0 & 0 & \frac{K_{p_2}}{T_{p_2}} \\ \frac{-1}{2\pi R_{1,1} T_{ch_{1,1}}} & 0 & \frac{-1}{T_{ch_{1,1}}} & 0 & 0 & 0 & \frac{-\phi_{1,1}}{T_{ch_{1,1}}} & 0 & 0 \\ \frac{-1}{2\pi R_{1,2} T_{ch_{1,2}}} & 0 & 0 & \frac{-1}{T_{ch_{1,2}}} & 0 & 0 & \frac{-\phi_{1,2}}{T_{ch_{1,2}}} & 0 & 0 \\ 0 & \frac{-1}{2\pi R_{2,1} T_{ch_{2,1}}} & 0 & 0 & \frac{-1}{T_{ch_{2,1}}} & 0 & 0 & \frac{-\phi_{2,1}}{T_{ch_{2,1}}} & 0 \\ 0 & \frac{-1}{2\pi R_{2,2} T_{ch_{2,2}}} & 0 & 0 & 0 & \frac{-1}{T_{ch_{2,2}}} & 0 & \frac{-\phi_{2,2}}{T_{ch_{2,2}}} & 0 \end{bmatrix}_{(6\times 9)},$$

$$\boldsymbol{A}_{12} = \begin{bmatrix} \frac{-K_{p_1}}{T_{p_1}} & \frac{-K_{p_1}}{T_{p_1}} & 0 \\ \frac{K_{p_2}}{T_{p_2}} & 0 & \frac{-K_{p_2}}{T_{p_2}} \\ 0 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 0 \end{bmatrix}_{(6\times 3)}, \quad \boldsymbol{A}_{21} = \begin{bmatrix} \frac{\beta_1 K_{I_1}}{2\pi} & 0 & 0 & \cdots & 0 & K_{I_1} \\ 0 & \frac{\beta_1 K_{I_2}}{2\pi} & 0 & \cdots & 0 & -K_{I_2} \\ \frac{T_{AC_{1,2}}}{2\pi} & \frac{-T_{AC_{1,2}}}{2\pi} & 0 & \cdots & 0 & 0 \end{bmatrix}_{(3\times 9)},$$

$$\boldsymbol{A}_{22} = \begin{bmatrix} K_{I_1} & 0 & 0 \\ -K_{I_2} & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}_{(3\times 3)}, \quad \boldsymbol{A}_{32} = \begin{bmatrix} \frac{-1}{T_{DC}} & 0 & 0 \\ \frac{J_{em_1} K_{p_1}}{T_{ESS_1} T_{p_1}} & -\frac{1}{T_{ESS_1}} - \frac{J_{em_1} K_{p_1}}{T_{ESS_1} T_{p_1}} & 0 \\ \frac{-J_{em_2} K_{p_2}}{T_{ESS_2} T_{p_2}} & 0 & -\frac{1}{T_{ESS_2}} - \frac{J_{em_2} K_{p_2}}{T_{ESS_2} T_{p_2}} \end{bmatrix}_{(3\times 3)}, \tag{24}$$

$$\boldsymbol{A}_{31} = \begin{bmatrix} \frac{K_1}{T_{DC}} & \frac{K_2}{T_{DC}} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{K_{AC}}{T_{DC}} \\ \frac{-J_{em_1}}{T_{ESS_1} T_{p_1}} & 0 & \frac{J_{em_1} K_{p_1}}{T_{ESS_1} T_{p_1}} & \frac{J_{em_1} K_{p_1}}{T_{ESS_1} T_{p_1}} & 0 & 0 & 0 & 0 & \frac{J_{em_1} K_{p_1}}{T_{ESS_1} T_{p_1}} \\ 0 & \frac{-J_{em_2}}{T_{ESS_2} T_{p_2}} & 0 & 0 & \frac{J_{em_2} K_{p_2}}{T_{ESS_2} T_{p_2}} & \frac{J_{em_2} K_{p_2}}{T_{ESS_2} T_{p_2}} & 0 & 0 & \frac{-J_{em_2} K_{p_2}}{T_{ESS_2} T_{p_2}} \end{bmatrix}_{(3\times 9)}.$$

$$\boldsymbol{B}_{c,d} = \begin{bmatrix} \frac{-K_{p_1}}{T_{p_1}} & 0 & 0 & \cdots & 0 & \frac{-J_{em_1} K_{p_1}}{T_{ESS_1} T_{p_1}} & 0 \\ 0 & \frac{-K_{p_2}}{T_{p_2}} & 0 & \cdots & 0 & 0 & \frac{-J_{em_2} K_{p_2}}{T_{ESS_2} T_{p_2}} \end{bmatrix}^\top_{(12\times 2)}, \tag{25}$$

$$\boldsymbol{B}_{c,f} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \frac{K_{I_1}\beta_1}{2\pi} & 0 & 0 & \frac{K_1}{T_{DC}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{K_{I_2}\beta_2}{2\pi} & 0 & \frac{K_2}{T_{DC}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & K_{I_1} & -K_{I_2} & 0 & \frac{K_{AC}}{T_{DC}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & K_{I_1} & -K_{I_2} & 0 & 0 & 0 & 0 \end{bmatrix}^\top_{(12\times 4)}. \tag{26}$$

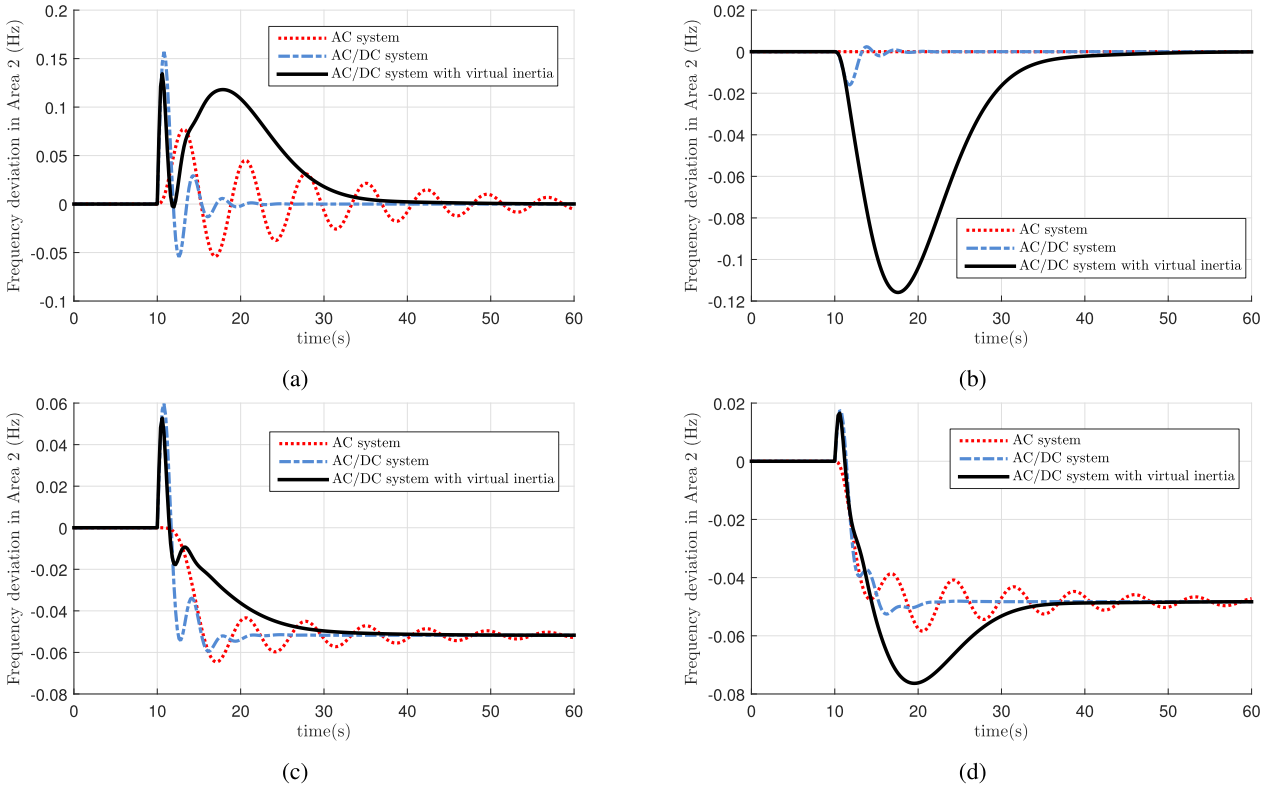


FIGURE 8. Frequency deviations of Area 2 under univariate attacks (a) on the AC link, $f_{AC_{1,2}} = 0.1$ p.u.; (b) on the DC link, $f_{DC_{1,2}} = -0.1$ p.u.; (c) on the frequency of Area 1, $f_{\omega_1} = 0.1$ Hz; (d) on the frequency of Area 2, $f_{\omega_2} = 0.1$ Hz at $t = 10$ s.

and the matrix $\boldsymbol{B}_{c,f}$ is presented in the equation (26) at the bottom of the previous page.

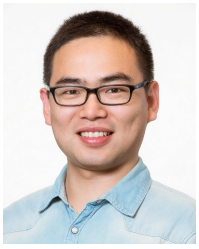
B. ADDITIONAL SIMULATION RESULTS

In Figure 8, the frequency deviations of Area 2 under each univariate attack on the wide-area measurements of AC power flow, DC power flow, frequency of Area 1 and frequency of Area 2 are plotted. We provide these additional simulation results in accordance with Figure 5 to support the observations in Section V-B.

REFERENCES

[1] E. Rakhshani, D. Remon, and P. Rodriguez, "Effects of PLL and frequency measurements on LFC problem in multi-area HVDC interconnected systems," *Int. J. Electr. Power Energy Syst.*, vol. 81, pp. 140–152, Oct. 2016.
[2] T. Xu, W. Jang, and T. Overbye, "Commitment of fast-responding storage devices to mimic inertia for the enhancement of primary frequency response," *IEEE Trans. Power Syst.*, vol. 33, no. 2, pp. 1219–1230, Mar. 2018.
[3] K. Dhingra and M. Singh, "Frequency support in a micro-grid using virtual synchronous generator based charging station," *IET Renew. Power Gener.*, vol. 12, no. 9, pp. 1034–1044, Jul. 2018.
[4] C. Mosca, F. Arrigo, A. Mazza, E. Bompard, E. Carpaneto, G. Chicco, and P. Cuccia, "Mitigation of frequency stability issues in low inertia power systems using synchronous compensators and battery energy storage systems," *IET Gener., Transmiss. Distrib.*, vol. 13, no. 17, pp. 3951–3959, Sep. 2019.
[5] M. Vrakopoulou, P. M. Esfahani, K. Margellos, J. Lygeros, and G. Andersson, "Cyber-attacks in the automatic generation control," in *Cyber Physical Systems Approach to Smart Electric Power Grid*. Berlin, Germany: Springer-Verlag, 2015, pp. 303–328.
[6] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.
[7] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *Proc. IEEE PES Gen. Meeting*, Jul. 2010, pp. 1–6.
[8] R. Tan, H. H. Nguyen, E. Y. S. Foo, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "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.
[9] J. Fang, R. Zhang, H. Li, and Y. Tang, "Frequency derivative-based inertia enhancement by grid-connected power converters with a Frequency-Locked-Loop," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 4918–4927, Sep. 2019.
[10] L. Ruttledge and D. Flynn, "Short-term frequency response of power systems with high non-synchronous penetration levels," *Wiley Interdiscipl. Rev., Energy Environ.*, vol. 4, no. 5, pp. 452–470, Sep. 2015.
[11] M. Datta and T. Senjyu, "Fuzzy control of distributed PV inverters/energy storage systems/electric vehicles for frequency regulation in a large power system," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 479–488, Mar. 2013.
[12] I. Dudurych, M. Burke, L. Fisher, M. Eager, and K. Kelly, "Operational security challenges and tools for a synchronous power system with high penetration of non-conventional sources," *CIGRE Sci. Eng.*, no. 7, pp. 91–101, 2017.
[13] E. Rakhshani and P. Rodriguez, "Inertia emulation in AC/DC interconnected power systems using derivative technique considering frequency measurement effects," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3338–3351, Sep. 2017.
[14] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson, "Secure control systems: A quantitative risk management approach," *IEEE Control Syst.*, vol. 35, no. 1, pp. 24–45, Feb. 2015.
[15] P. Mohajerin 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.

[16] M. Nyberg and E. Frisk, "Residual generation for fault diagnosis of systems described by linear differential-algebraic equations," *IEEE Trans. Autom. Control*, vol. 51, no. 12, pp. 1995–2000, Dec. 2006.
[17] A. Ameli, A. Hooshyar, E. F. El-Saadany, and A. M. Youssef, "Attack detection and identification for automatic generation control systems," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4760–4774, Sep. 2018.
[18] K. Pan, P. Palensky, and P. M. Esfahani, "From static to dynamic anomaly detection with application to power system cyber security," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1584–1596, Mar. 2020.
[19] 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.
[20] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber risk analysis of combined data attacks against power system state estimation," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3044–3056, May 2019.
[21] A. Gholami, M. Mousavi, A. K. Srivastava, and A. Mehrizi-Sani, "Cyber-physical vulnerability and security analysis of power grid with HVDC line," in *Proc. North Amer. Power Symp. (NAPS)*, Wichita, Kansas, Oct. 2019, pp. 1–6.
[22] H. E. Brown and C. L. Demarco, "Risk of cyber-physical attack via load with emulated inertia control," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5854–5866, Nov. 2018.
[23] S. D. Roy and S. Debbarma, "Detection and mitigation of cyber-attacks on AGC systems of low inertia power grid," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2023–2031, Jun. 2020.
[24] E. Rakhshani, P. Rodriguez, A. M. Cantarellas, and D. Remon, "Analysis of derivative control based virtual inertia in multi-area high-voltage direct current interconnected power systems," *IET Gener., Transmiss. Distrib.*, vol. 10, no. 6, pp. 1458–1469, Apr. 2016.
[25] P. Kundur, N. Balu, and M. Lauby, *Power System Stability and Control* (Discussion Paper Series). New York, NY, USA: McGraw-Hill, 1994. [Online]. Available: https://books.google.nl/books?id=2cbvyf8Ly4AC
[26] K. Pan, A. Teixeira, C. D. López, and P. Palensky, "Co-simulation for cyber security analysis: Data attacks against energy management system," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2017, pp. 253–258.
[27] K. Ogata, *Discrete-time Control Systems*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 1995.
[28] *Continental Europe Operation Handbook, Policy 1: Load-Frequency Control and Performance–Appendix*, ENTSO-E, Brussels, Belgium, Mar. 2016.
[29] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Trans. Ind. Informat.*, vol. 14, no. 5, pp. 1932–1941, May 2018.
[30] H. Weng and Z. Xu, "WAMS based robust HVDC control considering model imprecision for AC/DC power systems using sliding mode control," *Electr. Power Syst. Res.*, vol. 95, pp. 38–46, Feb. 2013.
[31] *Frequency Stability Evaluation Criteria for the Synchronous Zone of Continental Europe*, ENTSO-E, Brussels, Belgium, 2016.
[32] *MIGRATE Project, Type-3 and Type-4 EMT—Model Documentation Model Version: V7*, Energynautics, Darmstadt, Germany, 2017.
[33] P. Mohajerin Esfahani and J. Lygeros, "A tractable fault detection and isolation approach for nonlinear systems with probabilistic performance," *IEEE Trans. Autom. Control*, vol. 61, no. 3, pp. 633–647, Mar. 2016.
[34] X. Gao, X. Liu, and J. Han, "Reduced order unknown input observer based distributed fault detection for multi-agent systems," *J. Franklin Inst.*, vol. 354, no. 3, pp. 1464–1483, Feb. 2017.
[35] V. Andrieu and L. Praly, "On the existence of a Kazantzis-Kravaris/Luenberger observer," *SIAM J. Control Optim.*, vol. 45, no. 2, pp. 432–456, Jan. 2006.



KAIKAI PAN (Member, IEEE) received the B.Sc. and M.Sc. degrees (Hons.) in information engineering, measuring, and control from Beihang University, Beijing, China, in 2012 and 2015, respectively, and the Ph.D. degree in electrical engineering from the Delft University of Technology (TU Delft), The Netherlands. He is currently a Smart Grid Cyber Security Researcher with the Electrical Sustainable Energy Department, TU Delft. His current research interests include cyber risk analysis of advanced data attacks, attack or anomaly detection with model-based or data-driven approaches, cyber-physical systems modeling, the Internet of Things, and co-simulation techniques. He also served as a Reviewer for various journals and conferences mainly at the Power and Energy Society.

ELYAS RAKHSHANI (Member, IEEE) was born in 1982. He received the Ph.D. degree in electrical engineering *(cum laude)* from the Technical University of Catalonia (UPC), Barcelona, Spain, in 2016. From 2013 to 2016, he was a Junior Researcher with the Research Department, ABENGOA Company, Seville, Spain, working on different projects related to power electronics applications and the flexible operation of modern power systems. Since 2017, he has been working as a Postdoctoral Researcher with the IEGP Research Center, Delft University of Technology (TU Delft), The Netherlands. He joined the IEPG Center since the beginning of 2017 working on European H2020 projects related to control and dynamic stability assessment of low-inertia renewable-based power systems. His research interests include power system control and dynamic stability, HVDC control and power converter applications in power systems, wind power integration, frequency control, and optimal intelligent control. Based on his research, he has published and presented several scientific works/articles in the most distinguished journals and international conferences in electrical engineering. He has two book chapters, one patent, and several journal articles. He served as a Reviewer for various journals and the IEEE conferences and also served as the Technical Program Committee (TPC) Member for different conferences in Power and Energy Society (PES).

PETER PALENSKY (Senior Member, IEEE) was born in Austria, in 1972. He received the M.Sc. degree in electrical engineering and the Ph.D. degree from the Vienna University of Technology, Austria, in 1997 and 2001, respectively. After that, he co-founded an Envidatec, a German startup on energy management and analytics, and joined the Lawrence Berkely National Laboratory, CA, USA, as a Researcher, and the University of Pretoria, South Africa, in 2008. In 2009, he became the Head of business unit on sustainable building technologies at the Austrian Institute of Technology (AIT), and later the first Principle Scientist for complex energy systems at AIT. In 2014, he was appointed as a Full Professor for intelligent electric power grids at TU Delft. His main research interests include energy automation networks, smart grids, and modeling intelligent energy systems. He is active in international committees like ISO or CEN and serves an IEEE IES AdCom member-at-large in various functions for the IEEE. He is the Editor-in-Chief of the *IEEE Industrial Electronics Magazine*, an Associate Editor of the several other IEEE publications, and regularly organizes the IEEE conferences.