Effects of cyber attacks on ac and high-voltage DC interconnected power systems with emulated inertia

Pan, Kaikai; Dong, Jingwei; Rakhshani, Elyas; Palensky, Peter

DOI
10.3390/en13215583

Publication date
2020

Document Version
Final published version

Published in
Energies

Citation (APA)
Pan, K., Dong, J., Rakhshani, E., & Palensky, P. (2020). Effects of cyber attacks on ac and high-voltage DC interconnected power systems with emulated inertia. *Energies*, *13*(21), 1-24. Article 5583. https://doi.org/10.3390/en13215583

energies

MDPI

Article

Effects of Cyber Attacks on AC and High-Voltage DC Interconnected Power Systems with Emulated Inertia

Kaikai Pan *, Jingwei Dong, Elyas Rakhshani and Peter Palensky

Department of Electrical Sustainable Energy, Delft University of Technology, 2600 GA Delft, The Netherlands; J.Dong-6@tudelft.nl (J.D.); E.Rakhshani@tudelft.nl (E.R.); P.Palensky@tudelft.nl (P.P.)

* Correspondence: K.Pan@tudelft.nl

Received: 12 September 2020; Accepted: 19 October 2020; Published: 26 October 2020

Abstract: The high penetration of renewable energy resources and power electronic-based components has led to a low-inertia power grid which would bring challenges to system operations. The new model of load frequency control (LFC) must be able to handle the modern scenario where controlled areas are interconnected by parallel AC/HVDC links and storage devices are added to provide virtual inertia. Notably, vulnerabilities within the communication channels for wide-area data exchange in LFC loops may make them exposed to various cyber attacks, while it still remains largely unexplored how the new LFC in the AC/HVDC interconnected system with emulated inertia would be affected under malicious intrusions. Thus, in this article, we are motivated to explore possible effects of the major types of data availability and integrity attacks—Denial of Service (DoS) and false data injection (FDI) attacks—on such a new LFC system. By using a system-theoretic approach, we explore the optimal strategies that attackers can exploit to launch DoS or FDI attacks to corrupt the system stability. Besides, a comparison study is performed to learn the impact of these two types of attacks on LFC models of power systems with or without HVDC link and emulated inertia. The simulation results on the the exemplary two-area system illustrate that both DoS and FDI attacks can cause large frequency deviations or even make the system unstable; moreover, the LFC system with AC/HVDC interconnections and emulated inertia could be more vulnerable to these two types of attacks in many adversarial scenarios.

Keywords: AC/HVDC interconnections; load frequency control; virtual inertia; Denial of Service; false data injection; attack impact

1. Introduction

In the modern power systems, there is an increasing attention on the integration of renewable energy resources (RES), energy storage devices, and high voltage direct-current (HVDC) links. In order to support frequency control in these low-inertia systems, the recent trends of research are oriented in proposing different virtual inertia emulation approaches [1–3]. To meet the changes, the conventional control scheme such as the load frequency control (LFC) is also adapting to handle the new scenario where controlled areas are interconnected by parallel alternating-current (AC) and HVDC transmission lines and energy storage systems (ESS) are added for emulating virtual inertia. On the other hand, this transformation has introduced a high dependence on data communications, as the control loops involved in the new LFC would use communication networks such as the supervisory control and data acquisition (SCADA) system to transmit measurements and control data. However, the communication channels in the SCADA network for data exchange, especially the ones for wide-area measurements, are usually unprotected, leaving the LFC system more exposed to cyber threats [4–6]. In fact, it has been reported that the conventional LFC loops of multi-area systems with pure AC interconnections can be vulnerable to a large number of malicious intrusions [7,8]. Furthermore, a deliberate attack

targeted on the LFC system can have a direct effect on the system frequency and further cause severe damages to the stability and economical operation of the grid [9].

Different from the conventional LFC, in the context of modern power systems with AC/HVDC interconnections and emulated inertia by the ESS, more controllable resources would be added in the new LFC system to enable an improvement of the dynamical response. Furthermore, having more controllable devices also increases the vulnerability to cyber attacks. Though the cyber security concerns of conventional LFC in the normal AC system have been given considerable attention, it remains insufficiently answered how the new LFC in the hybrid AC/DC grid behaves under different cyber attacks. In general, each attack can be viewed in light of corrupting one (or multiple) of the following aspects of data; confidentiality, integrity, and availability Pan2017a. From the perspective of attack impact on the physical power system, the data integrity and availability attacks are more of interest for cyber security analysis. In fact, it has been reported that both data availability and integrity attacks can corrupt the conventional LFC system; see the related work in the following subsection. Thus, in this article, we are motivated to explore the effects of the typical data availability and integrity attacks—Denial of Service (DoS) and false data injection (FDI) attacks—on the new LFC considering AC/HVDC interconnections and the matter of virtual inertia. Here, the DoS and FDI attacks are mainly considered as they are major types of data availability and integrity attacks. For the DoS attack, it is one of the major threats against the availability of data [10]. The FDI attack is also known as a major class of integrity attack. Moreover, recent incidents, like the 2015 Ukraine blackout caused by hackers, have implied the feasibilities of DoS and FDI attacks on the smart grid devices of the real world [11]. Notably in this end, we have known that a DC grid has a low tolerance to a fault; we would also like to know how the new elements of HVDC link and inertia emulation module by ESS would affect the dynamic behavior of LFC under an intentional DoS or FDI attack.

1.1. Related Work

The LFC is known as a typical automatic closed-loop system that maintains the grid frequency and scheduled tie-line power between controlled areas by tuning the setpoints of generators for active power output, based on the wide-area transmitted measurements [12]. Research activities have been carried out to look into the attack impact on conventional LFC systems with pure AC transmission lines. In the early work of the authors of [13], effects of data integrity attacks on the operating frequency stability of LFC are introduced. Then, it is demonstrated in [7] how different FDI attacks on the LFC loop can affect the system frequency and electricity market operation. The work in [14] introduced a systematic method, based on reachability, for evaluating the impact that an FDI attack can have on the LFC system. Experimental tests of various cyber attacks on LFC using Cyber-Physical Security Testbeds can be found in [8]. In [15], the modeling language Modelica is introduced to support impact assessment of FDI attacks on the LFC. There are also some studies that have started to explore the effects of data availability attacks on LFC loops. The work in [16] illustrates that DoS attacks are able to make the dynamics of a LFC system unstable. The work in [17] focuses on the impact of time-delay attacks on the dynamic behavior of a multi-area LFC, indicating that such an availability attack can be more harmful in the area where there are load changes. Other related research is about communication delay or packet loss in the LFC system. For instance, a linear discrete-time model that includes the effects of different communication delays in the LFC model is proposed in [18] to explore the stability issues. Similar studies on communication delay/packet loss in conventional LFC models of normal AC systems can be found in [19–21].

The conventional LFC models have been modified to adapt to the reformulation of traditional power systems [22]. One of such aspects is about the deployment of HVDC transmission lines between controlled areas [23,24]. Besides, new functionalities are added in the frequency control to consider the matter of virtual inertia emulation [25,26]. In the pioneering work in [27], a method for evaluating the effects of virtual inertia on the dynamic behavior of a two-area LFC system is developed. As mentioned earlier, widespread application of communication networks in the LFC-related loop could make it

vulnerable to various cyber attacks. However, as far as we know, there is still a lack of studies on the cyber security research for the new LFC system in the hybrid grid with AC/HVDC interconnections and emulated inertia by storage devices. The following references have started to evaluate the attack impact on the part of HVDC system control or the inertia emulation process; however, none of them have focused on the overall LFC loop considering new elements of HVDC links and emulated inertia by ESS. The work in [28] has studied the effects of cyber attacks on the dynamic voltage stability of a HVDC system. The authors of [29] try to evaluate the impact of cyber attacks on the HVDC transmission oscillation damping control. The work in [30] demonstrates the risk/impact of a cyber-physical attack in which loads providing emulated inertia control services are attacked. The work in [31] has interpreted the effects of FDI attacks on the LFC of a low-inertia power system. Our recent work in [32] aims to propose a comprehensive framework for vulnerability and impact analysis of stationary FDI attacks on the hybrid AC/DC grid. To conclude, research efforts are still needed to evaluate the effects of different types of data integrity and availability attacks on the LFC system with new elements of HVDC link and also ESS for virtual inertia.

1.2. Contributions and Paper Organization

In this article, we study the impact of different cyber attacks on the LFC system equipped with AC/HVDC transmission lines and bulk ESS. Two major types of data availability and integrity attacks—DoS and FDI attacks—are introduced and explored. The FDI attack scenario has been introduced in our previous work [32], where only the stationary FDI attack is considered. In this article, we move a step forward to include the dynamic (time-variant) FDI attack. We propose optimal strategies that the attacker can exploit to launch DoS or FDI attacks to corrupt the system stability. Our contributions are reflected through three aspects: (i) We have enabled to model the studied LFC system under DoS attacks as a switched linear system. Then theoretical results are obtained for switching strategies that an advanced attacker could exploit to make the targeted system unstable. (ii) The FDI attack scenario is extended to include the dynamic FDI attack. The optimal FDI attacks that can be stealthy and disruptive are characterized by optimization programs. Particularly, we introduce a type of dynamic FDI attack called zero-dynamics attack that can remain stealthy with respect to an arbitrary anomaly detector, if certain conditions are met. (iii) A comparison study is performed especially in simulation part to learn DoS and FDI attacks on different LFC models of normal AC system, AC/DC system and AC/DC system with virtual inertia. To be noted in the end, to the best of our knowledge, it is the first time that the DoS attack and the dynamic FDI attack are introduced and learned in the context of new LFC considering a hybrid AC/DC grid with virtual inertia.

The structure of this article is as follows. In Section 2, we show how the conventional LFC system model is adapting to handle the modern scenario where controlled areas are interconnected with AC/HVDC links and there is emulated inertia by ESS. Section 3 focuses on DoS attacks which corrupt the availability of the wide-area measurements data. We enable modeling of the LFC system under DoS attacks as a switched linear system and the switching strategy to make the system unstable is proposed. The dynamic FDI attacks are introduced and studied in Section 4 where the optimal stealthy and disruptive FDI attacks are characterized by optimization programs. In Section 5, we provide simulation results and discussions, and conclusions are drawn in Section 6.

2. LFC Modeling in the Hybrid AC/DC System with Virtual Inertia

We present the LFC system modeling in this section. The Kundur model in [33] is used to represent a general interconnected power system. Here, we highlight the difference between the test system of this article and the original Kundur model in [33]. First, to meet the changes in modern scenarios, the test system is equipped with AC/HVDC transmission lines and inertia emulation capabilities by ESS, based on the work in [27]. The block diagram of the system is shown in Figure 1, where two areas, four generation units (GENs), and two load demand centers are involved, and converters are installed for controlling the HVDC link and the added ESS. Second, the system model used in this

paper is modified to be suitable for LFC or automatic generation control (AGC) analysis. We consider the LFC because, as mentioned in Section 1, the high-level control of LFC with a relatively slow dynamical response would rely more on communication networks such as the SCADA system to transmit measurements and control data, while such a system is known to be vulnerable to various attacks, as reported in [4–6]. From the perspective of system modeling, considering the timescale of LFC, it is generally a linearized model with certain levels of abstraction that simplify some elements of the initial detailed Kundur model. We show the details of the system model in the following.

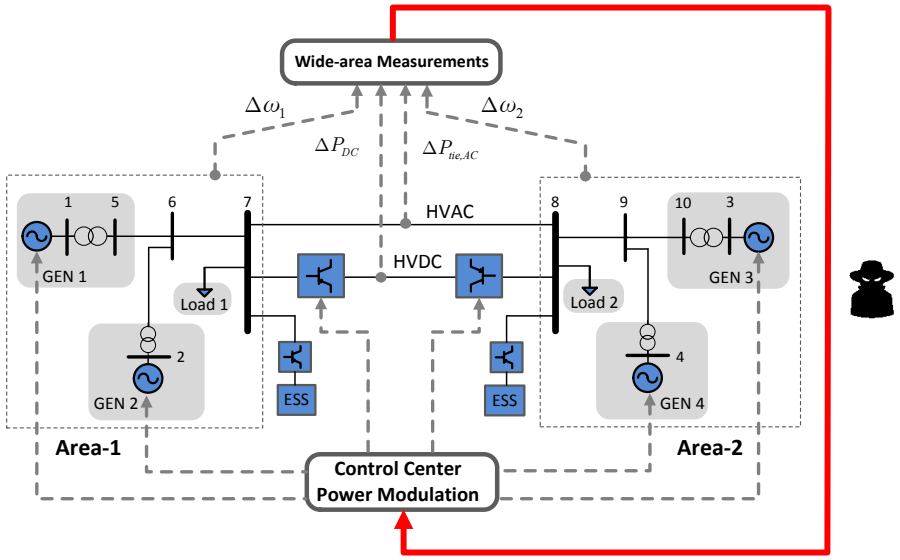


Figure 1. The block diagram of the test system. The communication channels (the red line) for the transmission of wide-area measurements are very vulnerable, and therefore the cyber attacks of Denial of Service (DoS) and false data injection (FDI) in this article are mainly on the measurements side. To be noted, we assume that the channel for control signals is equipped with advanced encryption techniques and thus not attacked.

2.1. The Conventional LFC Structure

The LFC loop is a typical high-level control application. To regulate the power grid frequency, the LFC module in each controlled area receives wide-area measurements of frequency and tie-line power and sends control signals of set points for the output power of the participating generators in that area (e.g., GEN 1 and GEN 2 in Area 1 of Figure 1). To understand the LFC concept, we first introduce an area control error (ACE) signal as follows,

$$ACE_i = \beta_i \Delta\omega_i + \Delta P_{tie_{ij}}\,, \tag{1}$$

where β_i, $\Delta\omega_i$, and $\Delta P_{tie_{ij}}$ are the frequency bias factor, the frequency deviation of Area i, and the net tie-line power flow variation between Area i and Area j, respectively; for a two-area power system, like the one in Figure 1, $\Delta P_{tie_{ij}} = -\Delta P_{tie_{ji}}$. Thus, for a normal AC system where there are only pure AC transmission lines, let ω_0 be the nominal value of frequency, and we have

$$\Delta P_{tie_{ij}} = \Delta P_{tie,AC}\,,\ \Delta\omega_i = \omega_i - \omega_0\,. \tag{2}$$

To be mentioned, the ACE value in (1) defines the frequency to restore and the power to compensate in the event of load-generation imbalance.

As noted earlier, the LFC system is a high-level control application, and we pay more attention to the collective performance of all generators [33]. Then, we can do certain levels of abstraction and suppose that each area consists of equivalent governors, turbines, and generators. The dynamics of

each area is represented by a linearized model. In this regard, the frequency dynamics of Area i in the two-area system can be described in the Laplace domain,

$$\Delta\omega_i(s) = \frac{K_{p_i}}{1+sT_{p_i}}\Big[\sum_{g=1}^{G_i}\Delta P_{m_{i,g}} - \Delta P_{d_i} - \Delta P_{tie,AC}\Big], \tag{3}$$

where K_{p_i} and T_{p_i} are the system gain and the time constant, respectively. The gain K_{p_i} is related to the damping coefficient. The time constant T_{p_i} is associated with both the equivalent inertia and the damping. $\Delta P_{m_{i,g}}$ is the output power of each participated generator in Area i, and G_i denotes the number of these generators. ΔP_{d_i} represents the total load variation in Area i. For the variables $\Delta P_{m_{i,g}}$ and $\Delta P_{tie,AC}$, we have

$$\Delta P_{m_{i,g}}(s) = \frac{1}{1+sT_{ch_{i,g}}}\Big[\frac{\Delta\omega_i}{R_{i,g}\times 2\pi} - \phi_{i,g}\Delta P_{agc_i}\Big], \tag{4}$$

$$\Delta P_{tie,AC}(s) = \frac{T_{AC_{i,j}}}{s}\big[\Delta\omega_i - \Delta\omega_j\big], \tag{5}$$

where $R_{i,g}$ is considered as droop for each participated generator in Area i. $T_{ch_{i,g}}$ is the time constant of the whole turbine-governor unit (we assume that each dynamic generator model consists of its turbine-governor model). ΔP_{agc_i} denotes the AGC signal generated by the LFC control loop in Area i. $\phi_{i,g}$ is an area participating factor satisfying $\sum_{g=1}^{G_i}\phi_{i,g} = 1$. $T_{AC_{i,j}}$ is the coefficient for the power flow on the AC transmission line between these two areas.

The AGC signal ΔP_{agc_i} is used to regulate the set points of participated generators for active power output. The goal is to guarantee that the system frequency restores to nominal value in a load-generation imbalance event. Meanwhile, the tie-line power flow between controlled areas should act as the scheduled one. Here, ΔP_{agc_i} is generated by an integral control law, with the inputs of frequency deviations and tie-line power flow variations as parts of the ACE signal, that is,

$$\Delta P_{agc_i} = K_{I_i}\frac{ACE_i}{s}, \tag{6}$$

where K_{I_i} is the integral gain of the AGC controller and ACE_i is the ACE of Area i mentioned in (1). In the following, we show how the conventional LFC model adapts to meet the changes of parallel AC/HVDC links and the matter of inertia emulation.

2.2. LFC for AC/HVDC Interconnected System

Next, we consider the scenario where the controlled areas now are interconnected by AC/HVDC transmission lines. There are usually two converters in the HVDC system: one converter controls the active power flow, and the other one would be responsible to control the level of DC link voltage [27]. Here, we introduce the concept of Supplementary Power Modulation Controller (SPMC) to model the effects of HVDC link on the dynamic performance of the overall LFC loop. Note that the dynamics of fast transient HVDC power electronic parts is neglected when we analyze the dynamic effects of the HVDC link on LFC. This is because of the fact that the time constant of electronic parts is much smaller than that of mechanical parts in the analysis of dynamic behavior of the power system.

As a high-level supervisory control loop, the SPMC is able to improve the performance of the power system when there are load changes. To construct the SPMC, one needs the frequency deviations in each area, i.e., ω_i and ω_j, and the power flow variations in the AC line, i.e., $\Delta P_{tie,AC}$. Then, the HVDC link generates the desired DC power based on the output of SPMC, by changing the duty cycles of converters. The SPMC strategy as a damping controller can be expressed as

$$\Delta P_{DC_{ref}} = K_i\Delta\omega_i + K_j\Delta\omega_j + K_{AC}\Delta P_{tie,AC}, \tag{7}$$

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

where $\Delta P_{DC_{ref}}$ denotes the reference of the DC power; K_i, K_j, and K_{AC} represent control gains; and T_{DC} denotes the time constant of the HVDC link. According to the work in [27], the proper time response of this kind of supervisory controller could range from 100 ms to 500 ms. Here, we assume that T_{DC} is 100 ms.

In (8), ΔP_{DC} is the generated power by the HVDC link. Then, the deviations of total tie-line power flows on both AC and HVDC transmission lines become

$$\Delta P_{tie_{ij}} = \Delta P_{tie,AC} + \Delta P_{DC}\,. \tag{9}$$

Note the difference between Equations (9) and (2) which is for the normal AC system. Then, considering the new added DC power in the total tie-line power flow variation, the ACE signal of each area now needs to be adjusted to

$$ACE_i = \beta_i \Delta\omega_i + \Delta P_{tie,AC} + \Delta P_{DC}\,. \tag{10}$$

2.3. LFC for AC/HVDC System with Emulated Inertia by ESS

In this part, we continue to model the LFC in the test system equipped with not only AC/HVDC transmission lines but also bulk ESS for inertia emulation. Note that a virtual inertia could be emulated by the added bulk ESS to improve the inertia response of conventional generators to load variations. In this article, the inertia emulation is realized by derivative control. Then, the emulated power from ESS for Area i can be written as

$$\Delta P_{ESS_i}(s) = \frac{J_{em_i}}{1+sT_{ESS_i}}[s\Delta\omega_i(s)]\,, \tag{11}$$

where T_{ESS_i} denotes the time constant of the derivative control loop and J_{em_i} is the control gain representing the emulated inertia. We can see that the above derivative control loop calculates the rate of change of frequency (ROCOF). To be highlighted, instead of wide-area frequency data for the supervisory AGC and SPMC loops in the proceeding, only the local frequency information would be used for a relatively faster response in the derivative control-based inertia emulation. The selection of control gain J_{em_i} is based on an iterating tuning approach where the frequency deviations are minimized; we refer to the work in [34] for details. Considering that the derivative control loop could be sensitive to the noise, one may add a low-pass filter to the model to eliminate the effects of noise [32] (here we consider the filter's effects through the time constant T_{ESS_i}). The storage part of ESS will remain charged during normal operation, and it starts to help the system once contingencies occur. Note that the ESS mainly works for a short period of time (2 s to 5 s) to emulate inertia.

In the end, adding the emulated active power from ESS and also the power modulated by the HVDC link in Section 2.2, the Equation (3) of frequency dynamics in Area i will be changed to

$$\Delta\omega_i(s) = \frac{K_{p_i}}{1+sT_{p_i}}\Big[\sum_{g=1}^{G_i}\Delta P_{m_{i,g}} - \Delta P_{d_i} - \Delta P_{tie,AC} - \Delta P_{DC} + \Delta P_{ESS_i}\Big]\,. \tag{12}$$

2.4. LFC System Model in the State-Space Form

As shown in Figure 1, the wide-area measurements are mainly frequencies in the two areas and power flows on both AC and HVDC lines. These measurements would act as inputs for supervisory controllers in LFC, i.e., the AGC and SPMC loops; recall Sections 2.1 and 2.2. For the virtual inertia emulation part, it uses local frequency information only for a relatively faster response, as indicated in Section 2.3. Given the above explanations and the system descriptions in Sections 2.1–2.3, the open-loop

LFC model for the test two-area system interconnected by AC and HVDC transmission lines and equipped with added ESS can be compactly described by a continuous-time state-space form:

$$\begin{aligned} \dot{\bar{\boldsymbol{x}}}(t) &= \bar{\boldsymbol{A}}_c \bar{\boldsymbol{x}}(t) + \bar{\boldsymbol{B}}_{c,u} \boldsymbol{u}(t) + \bar{\boldsymbol{B}}_{c,d} \boldsymbol{d}(t), \\ \bar{\boldsymbol{y}}(t) &= \bar{\boldsymbol{C}} \bar{\boldsymbol{x}}(t), \end{aligned} \tag{13}$$

where the state vector $\bar{\boldsymbol{x}}$, the control input vector $\boldsymbol{u}$, the disturbance input vector $\boldsymbol{d}$, and the output vector $\bar{\boldsymbol{y}}$ of wide-area measurements can be expressed as

$$\begin{aligned} \bar{\boldsymbol{x}} &:= \left[\Delta\omega_1 \ \Delta\omega_2 \ \Delta P_{m_{1,1}} \ \Delta P_{m_{1,2}} \ \Delta P_{m_{2,1}} \ \Delta P_{m_{2,2}} \ \Delta P_{tie,AC} \ \Delta P_{DC} \ \Delta P_{ESS_1} \ \Delta P_{ESS_2}\right]^\top, \\ \boldsymbol{u} &:= \left[\Delta P_{DC_{ref}} \ \Delta P_{agc_1} \ \Delta P_{agc_2}\right]^\top, \\ \boldsymbol{d} &:= \left[\Delta P_{d_1} \ \Delta P_{d_2}\right]^\top, \\ \bar{\boldsymbol{y}} &:= \left[\Delta\omega_1 \ \Delta\omega_2 \ \Delta P_{tie,AC} \ \Delta P_{DC}\right]^\top. \end{aligned} \tag{14}$$

We note that the control input vector $\boldsymbol{u}$ consists of control signals from supervisory AGC and SPMC controllers. Besides, the disturbance input vector $\boldsymbol{d}$ corresponds to load changes in each area.

$$\bar{\boldsymbol{A}}_{11} = \begin{bmatrix} \frac{-1}{T_{p_1}} & 0 & \frac{K_{p_1}}{T_{p_1}} & \frac{K_{p_1}}{T_{p_1}} & 0 & 0 & \frac{-K_{p_1}}{T_{p_1}} \\ 0 & \frac{-1}{T_{p_2}} & 0 & 0 & \frac{K_{p_2}}{T_{p_2}} & \frac{K_{p_2}}{T_{p_2}} & \frac{K_{p_1}}{T_{p_1}} \\ \frac{-1}{2\pi R_{1,1} T_{ch_{1,1}}} & 0 & \frac{-1}{T_{ch_{1,1}}} & 0 & 0 & 0 & 0 \\ \frac{-1}{2\pi R_{1,2} T_{ch_{1,2}}} & 0 & 0 & \frac{-1}{T_{ch_{1,2}}} & 0 & 0 & 0 \\ 0 & \frac{-1}{2\pi R_{2,1} T_{ch_{2,1}}} & 0 & 0 & \frac{-1}{T_{ch_{2,1}}} & 0 & 0 \\ 0 & \frac{-1}{2\pi R_{2,2} T_{ch_{2,2}}} & 0 & 0 & 0 & \frac{-1}{T_{ch_{2,2}}} & 0 \end{bmatrix}_{(6\times 7)},$$

$$\bar{\boldsymbol{A}}_{12} = \begin{bmatrix} \frac{-K_{p_1}}{T_{p_1}} & \frac{-K_{p_1}}{T_{p_1}} & 0 \\ \frac{K_{p_2}}{T_{p_2}} & 0 & \frac{-K_{p_2}}{T_{p_2}} \\ 0 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 0 \end{bmatrix}_{(6\times 3)}, \quad \bar{\boldsymbol{A}}_{21} = \begin{bmatrix} \frac{T_{AC_{1,2}}}{2\pi} & \frac{-T_{AC_{1,2}}}{2\pi} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}_{(2\times 7)}, \tag{15}$$

$$\bar{\boldsymbol{A}}_{22} = \begin{bmatrix} 0 & 0 & 0 \\ \frac{-1}{T_{DC}} & 0 & 0 \end{bmatrix}_{(2\times 3)}, \quad \bar{\boldsymbol{A}}_{32} = \begin{bmatrix} \frac{J_{em_1} K_{p_1}}{T_{ESS_1} T_{p_1}} & -\frac{1}{T_{ESS_1}} - \frac{J_{em_1} K_{p_1}}{T_{ESS_1} T_{p_1}} & 0 \\ \frac{-J_{em_2} K_{p_2}}{T_{ESS_2} T_{p_2}} & 0 & -\frac{1}{T_{ESS_2}} - \frac{J_{em_2} K_{p_2}}{T_{ESS_2} T_{p_2}} \end{bmatrix}_{(2\times 3)},$$

$$\bar{\boldsymbol{A}}_{31} = \begin{bmatrix} \frac{-J_{em_1}}{T_{ESS_1} T_{p_1}} & 0 & \frac{J_{em_1} K_{p_1}}{T_{ESS_1} T_{p_1}} & \frac{J_{em_1} K_{p_1}}{T_{ESS_1} T_{p_1}} & 0 & 0 & \frac{J_{em_1} K_{p_1}}{T_{ESS_1} T_{p_1}} \\ 0 & \frac{-J_{em_2}}{T_{ESS_2} T_{p_2}} & 0 & 0 & \frac{J_{em_2} K_{p_2}}{T_{ESS_2} T_{p_2}} & \frac{J_{em_2} K_{p_2}}{T_{ESS_2} T_{p_2}} & \frac{-J_{em_2} K_{p_2}}{T_{ESS_2} T_{p_2}} \end{bmatrix}_{(2\times 7)}.$$

$$\bar{\boldsymbol{B}}_{c,u} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{T_{DC}} & 0 & 0 \\ 0 & 0 & \frac{-\phi_{1,1}}{T_{ch_{1,1}}} & \frac{-\phi_{1,2}}{T_{ch_{1,2}}} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{-\phi_{2,1}}{T_{ch_{2,1}}} & \frac{-\phi_{2,2}}{T_{ch_{2,2}}} & 0 & 0 & 0 & 0 \end{bmatrix}^\top_{(10\times 3)}. \tag{16}$$

$$\bar{\boldsymbol{B}}_{c,d} = \begin{bmatrix} \frac{-K_{p_1}}{T_{p_1}} & 0 & 0 & \cdots & 0 & \frac{-J_{em_1} K_{p_1}}{T_{ESS_1} T_{p_1}} & 0 \\ 0 & \frac{-K_{p_2}}{T_{p_2}} & 0 & \cdots & 0 & 0 & \frac{-J_{em_2} K_{p_2}}{T_{ESS_2} T_{p_2}} \end{bmatrix}^\top_{(10\times 2)}. \tag{17}$$

The matrices $\bar{\boldsymbol{A}}_c$, $\bar{\boldsymbol{B}}_{c,u}$, $\bar{\boldsymbol{B}}_{c,d}$, and $\bar{\boldsymbol{C}}$ in (13) are constant with appropriate dimensions. For a better illustration of the system state matrix $\bar{\boldsymbol{A}}_c$, we use the following expression,

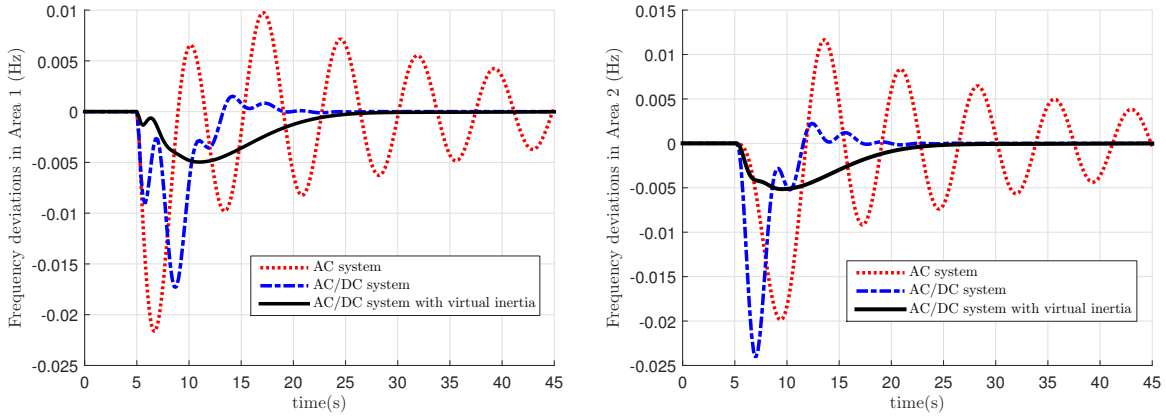
$$\bar{\boldsymbol{A}}_c = \begin{bmatrix} \bar{\boldsymbol{A}}_{11} & \bar{\boldsymbol{A}}_{12} \\ \bar{\boldsymbol{A}}_{21} & \bar{\boldsymbol{A}}_{22} \\ \bar{\boldsymbol{A}}_{31} & \bar{\boldsymbol{A}}_{32} \end{bmatrix}_{(10\times 10)}.$$

Each sub-matrix of $\bar{\boldsymbol{A}}_c$ is presented in Equation (15). In addition, the system input matrices $\bar{\boldsymbol{B}}_{c,u}$ and $\bar{\boldsymbol{B}}_{c,d}$ that relate control signals and load changes to the system states are given in (16) and (17), respectively. We omit the detail of the output matrix $\bar{\boldsymbol{C}}$ in (13) as its formulation is straightforward considering that the output vector $\bar{\boldsymbol{y}}$ corresponds to wide-area measurements of frequency in each area and power lows on both AC and HVDC transmission lines. In the end, the parameters of the two-area system and also associated control loops, i.e., the parameters appeared in Equations (1)–(12) for LFC purpose, are referred to Table 1, based on the work in [27].

Table 1. Parameters of the two-area system and associated control loops.

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

As mentioned, it is easy to observe that the open-loop LFC models for the normal AC system and the AC/DC system, but without inertia emulation functionalities, can also be derived in the form of (13). For instance, for the conventional LFC structure in a normal AC system, there would be no such state variables of $\Delta P_{DC_{1,2}}$, ΔP_{ESS_1} and ΔP_{ESS_2}. Besides, the variable $\Delta P_{DC_{ref}}$ related to the control input of DC link is not included in $\boldsymbol{u}$, and there is no wide-area measurement for the DC power flow in the output vector $\bar{\boldsymbol{y}}$. Before looking into the effects of cyber attacks, we first validate the LFC system models. To do that, as a common approach, we launch a step load change for the input of the system. The load change happens in Load 1 of Area 1 at $t = 5$ s with an increase of 0.03 p.u. Figure 2 provides the results of frequency deviations in both areas. It is easy to observe that the expansion of the interconnected system using HVDC link and especially the strategy of inertia emulation can help in improving the LFC system dynamics. The improvements are significant in damping frequency oscillations in a load change, which indicates a good performance when the overall LFC system model is equipped with HVDC link by SPMC control and also ESS for virtual inertia emulation.



(**a**) (**b**)

Figure 2. Results of both areas when there is a step load change in Load 1 of Area 1 in the two-area power system. (**a**) Frequency deviation of Area 1. (**b**) Frequency deviation of Area 2.

3. DoS Attacks on the AC/DC Multi-Area LFC System with Virtual Inertia

In this section, we study the effects of data availability attacks on the LFC system developed in the previous section. The DoS attack is mainly considered as it is one of the major threats against the availability of data [10]. In a DoS attack, it typically causes periods of time at which the communication is not possible, thus preventing measurements or control data from reaching the respective destinations [35]. To launch DoS attacks, there are many strategies that an attacker can exploit. For instance, the attacker can jam the communication channels, compromise devices and prevent them from sending data, attack the routing protocols, and flood the network traffic [36]. To be illustrative, one can consider a man-in-the-middle (MITM) attack scenario on the communication channels between the substations and the control center. Then, the attacker is capable of interfering with the transmitted measurements using the MITM tool to block the measurements, either by attacking the routing scheme or flooding the network traffic [37]. In this article, we aim to model DoS attacks on the developed LFC mathematical model in Section 2 such that the behavior of data absence caused by DoS attacks is considered in the modeling process. We refer to the work in [10] for the specific strategies for launching such DoS attacks.

3.1. The Test LFC System under DoS Attacks

First, we need to modify the LFC system model developed in Section 2 to include DoS attacks into the control loop. As illustrated in Figure 1, we consider the attack scenario where communication channels for the transmission of wide-area measurements are attacked by DoS. To help in model analysis, one needs to modify the state-space representation in (13) by defining the following new "virtual" state and output vectors,

$$\begin{aligned} \boldsymbol{x} &:= \left[\Delta\omega_1 \;\; \Delta\omega_2 \;\; \Delta P_{m_{1,1}} \;\; \Delta P_{m_{1,2}} \;\; \Delta P_{m_{2,1}} \;\; \Delta P_{m_{2,2}} \;\; \Delta P_{tie,AC} \;\; \Delta P_{DC} \;\; \Delta P_{ESS_1} \;\; \Delta P_{ESS_2} \;\; \int ACE_1 \;\; \int ACE_2\right]^\top, \\ \boldsymbol{y} &:= \left[\Delta\omega_1 \;\; \Delta\omega_2 \;\; \Delta P_{tie,AC} \;\; \Delta P_{DC} \;\; \int ACE_1 \;\; \int ACE_2\right]^\top, \end{aligned} \tag{18}$$

where $\int ACE_i$ is the integration of the ACE signal in Area i. Note that $\int ACE_i$ in $\boldsymbol{y}$ is a virtual variable and the practical wide-area measurements in the output vector $\boldsymbol{y}$ are frequencies ($\Delta\omega_i$) and AC/DC power flows ($\Delta P_{tie,AC}$, ΔP_{DC}). Then, the integral action in the supervisory AGC loop can be transformed into a static output feedback control problem [20]. We still use definitions of input vectors $\boldsymbol{u}$ and $\boldsymbol{d}$ in (14). Then, we can obtain the following "modified" dynamic model for the test LFC system

interconnected by AC/HVDC links and equipped with bulk ESS, by considering the "virtual" state vector $\boldsymbol{x}$ and output vector $\boldsymbol{y}$ in (18),

$$\begin{aligned} \dot{\boldsymbol{x}}(t) &= \boldsymbol{A}_c\boldsymbol{x}(t) + \boldsymbol{B}_{c,u}\boldsymbol{u}(t) + \boldsymbol{B}_{c,d}\boldsymbol{d}(t)\,, \\ \boldsymbol{y}(t) &= \boldsymbol{C}\boldsymbol{x}(t)\,. \end{aligned} \tag{19}$$

Note that now $\boldsymbol{u}$ represents the input signal from the resulted static output feedback control in the above open-loop LFC system model of (19).

By using the "virtual" output vector $\boldsymbol{y}$ in (18), the static output feedback control process can be expressed as $\boldsymbol{u} = \boldsymbol{K}\boldsymbol{y}$ where $\boldsymbol{K}$ is the gain of the static output feedback control and we can have

$$\boldsymbol{K} = \begin{bmatrix} K_1 & K_2 & K_{AC} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & K_{I_1} & 0 \\ 0 & 0 & 0 & 0 & 0 & K_{I_2} \end{bmatrix}. \tag{20}$$

For the matrices $\boldsymbol{A}$, $\boldsymbol{B}_{c,u}$, $\boldsymbol{B}_{c,d}$, and $\boldsymbol{C}$ in the model (19), it is easy to derive their formulations based on $\bar{\boldsymbol{A}}_c$, $\bar{\boldsymbol{B}}_{c,u}$, $\bar{\boldsymbol{B}}_{c,d}$ and $\bar{\boldsymbol{C}}$ given in the original open-loop LFC model in Section 2.4.

In a realistic framework, the wide-area measurements are applied to the supervisory AGC and SPMC controllers in discrete-time samples. Thus we would like to express the dynamic LFC system model in a discrete-time framework. To do that, (19) needs to be discretized. Taking a sampling period T_s, we have the following discretization results for a zero-order hold (ZOH) [38],

$$\boldsymbol{A} = e^{\boldsymbol{A}_c T_s}\,, \quad \boldsymbol{B}_u = \int_{t=0}^{T_s} e^{\boldsymbol{A}_c(T_s-t)}\boldsymbol{B}_{c,u}\mathrm{d}t\,, \quad \boldsymbol{B}_d = \int_{t=0}^{T_s} e^{\boldsymbol{A}_c(T_s-t)}\boldsymbol{B}_{c,d}\mathrm{d}t\,. \tag{21}$$

To be noted, (21) can be explained as the analytical solution of the ZOH discretization. Then, after discretization of (19), the discrete-time version of the open-loop LFC model for the two-are system equipped with AC/HVDC transmission lines and bulk ESS can be described by

$$\begin{aligned} \boldsymbol{x}[k+1] &= \boldsymbol{A}\boldsymbol{x}[k] + \boldsymbol{B}_u\boldsymbol{u}[k] + \boldsymbol{B}_d\boldsymbol{d}[k]\,, \\ \boldsymbol{y}[k] &= \boldsymbol{C}\boldsymbol{x}[k]\,. \end{aligned} \tag{22}$$

As noted earlier, vulnerabilities within the wide-area communication network (e.g., SCADA system) may allow cyber attacks. In this section, we focus on the following DoS attack scenario; the adversary has compromised the communication channels of wide-area measurements, preventing these measurements from being transmitted to the control center for power modulation (i.e., supervisory AGC and SPMC loops); recall Figure 1. According to the authors of [39], it is reasonable to assume that the channel for AGC and SPMC control signals is equipped with advanced encryption techniques; therefore, we mainly focus on the uploading channels of wide-area measurements instead of control signals on the feedback loop. As stated in Section 2.3, we know that the control loop of inertia emulation is using local information only and thus not attacked directly by DoS. Due to the DoS attack, the missing measurements are typically replaced with the last received ones. By properly designing the DoS attack sequences, the attacker can corrupt the normal operation of the controllers and consequently the involved physical system, e.g., the system stability. We show such effects of DoS attacks in what follows. According to the authors of [16], the DoS attack on the output vector $\boldsymbol{y}$ can be treated as a switching on/off event. Let $\tilde{\boldsymbol{y}}$ denote the output vector under DoS attacks, and the control signal becomes

$$\boldsymbol{u}[k] = K\tilde{\boldsymbol{y}}[k]\,. \tag{23}$$

We also consider that the controllers are equipped with ZOH. Hence the wide-area measurements in the LFC loop under DoS attacks can be further expressed as

$$\tilde{\boldsymbol{y}}[k] = \begin{cases} \boldsymbol{y}[k] = \boldsymbol{C}\boldsymbol{x}[k] & \text{if, } S_1\,; \\ \tilde{\boldsymbol{y}}[k-1] = \boldsymbol{C}\tilde{\boldsymbol{x}}[k-1] & \text{if, } S_2\,. \end{cases} \tag{24}$$

where S_1 and S_2 are "positions" indicating whether the wide-area measurements are under DoS attacks or not, $\tilde{\boldsymbol{x}}$ is an introduced auxiliary vector that satisfies

$$\tilde{\boldsymbol{x}}[k] = \begin{cases} \boldsymbol{x}[k] & \text{if, } S_1\,; \\ \tilde{\boldsymbol{x}}[k-1] & \text{if, } S_2\,. \end{cases} \tag{25}$$

Next, to include DoS attacks into the control loop, let us augment the state vector with the introduced vector $\tilde{\boldsymbol{x}}^\top[k-1]$, i.e., $\boldsymbol{z}[k] := \begin{bmatrix}\boldsymbol{x}^\top[k] & \tilde{\boldsymbol{x}}^\top[k-1]\end{bmatrix}^\top$. Then, one can integrate (23) with (22) to derive the closed-loop model of the test LFC system under DoS attacks,

$$\boldsymbol{z}[k+1] \;=\; \Phi_j \boldsymbol{z}[k] \;+\; \boldsymbol{B}_{d,cl}\boldsymbol{d}[k]\,, \tag{26}$$

where j indicates the switch position such that $j = 1$ for position of S_1 (no DoS attacks), and $j = 2$ for position of S_2 (under DoS attacks), and the corresponding matrices are

$$\Phi_1 = \begin{bmatrix} \boldsymbol{A} + \boldsymbol{B}_u\boldsymbol{K}\boldsymbol{C} & \boldsymbol{0} \\ \boldsymbol{I} & \boldsymbol{0} \end{bmatrix}, \quad \Phi_2 = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{B}_u\boldsymbol{K}\boldsymbol{C} \\ \boldsymbol{0} & \boldsymbol{I} \end{bmatrix}, \quad \boldsymbol{B}_{d,cl} = \begin{bmatrix} \boldsymbol{B}_d \\ \boldsymbol{0} \end{bmatrix}. \tag{27}$$

Remark 1 (DoS attacks on "selected" measurements)**.** *In the attack scenario above, we can observe that all the system outputs are assumed to be attacked by DoS; see* (24)*. This is mainly for the simplicity of illustrating the formulations of closed-loop system matrices. However, the developed framework can subsume the scenario where only part of measurements are attacked. One can introduce diagonal matrices with the elements of binary vectors sitting on the main diagonals to indicate which wide-area measurement is under a DoS attack. For instance, let us introduce* $\tilde{\boldsymbol{y}}[k] = \boldsymbol{P}_{1,m}\boldsymbol{C}\boldsymbol{x}[k] + \boldsymbol{P}_{2,m}\boldsymbol{C}\tilde{\boldsymbol{x}}[k-1]$ *for the switch position* S_2 *when the m-th measurement is attacked by DoS, and* $\boldsymbol{P}_{1,m}$, $\boldsymbol{P}_{2,m}$ *are such diagonal matrices that characterize the "position" of the attacked measurement.*

3.2. Stability of the Test LFC System under DoS Attacks

In the following, we show how the DoS attacks can affect the stability of the closed-loop LFC system in the hybrid AC/DC grid with emulated inertia. We have modeled the LFC under DoS attacks as a switched linear system in the proceeding. The stability issue of a switched system has been extensively investigated; one look in [21,40] for a detailed analysis. From the viewpoint of an attacker, the whole system may be made unstable by choosing a proper switching strategy.

To study the stability of the test system in (26), let us consider a scenario where the loads keep constant, namely, $\boldsymbol{d}[k] = 0$ for all $k \in \mathbb{N}$. The following Lemma 1 indicates that there exist possible switching strategies that the attacker can exploit to launch DoS attacks to make the underlying two-area LFC system unstable.

Lemma 1. *We introduce a constant* $0 \leq \lambda \leq 1$*. Then, the switched linear system of* (26)*, where* $\Phi_i \in \{\Phi_1, \Phi_2\}$*, is unstable, if there exists* λ *such that the equivalent system with system matrix* $\Phi_1^{\lambda}\Phi_2^{(1-\lambda)}$ *has an eigenvalue with magnitude outside the unity circle.*

Proof of Lemma 1. Let us introduce a time interval $[T_0,\, T_d)$ and $n_T = T_d - T_0$. Similar to the work in [16] (Theorem 2), we can assume that the test system operates normally from T_0, i.e., the switched linear system of (26) with $\Phi_i \in \{\Phi_1, \Phi_2\}$ stays at Φ_1 for a time period of λn_T. Then, afterwards,

the test system is attacked by DoS and (26) stays at Φ_2 for a time period of $(1-\lambda)n_T$. In the end, the state of the test LFC system at T_d would become

$$\boldsymbol{z}[T_d] = \Phi_1^{\lambda n_T}\Phi_2^{(1-\lambda)n_T}\boldsymbol{z}[T_0]\,. \tag{28}$$

Let us define $\Phi(\lambda) := \Phi_1^{\lambda}\Phi_2^{(1-\lambda)}$. We will have $\boldsymbol{z}[T_d] = (\Phi(\lambda))^{n_T}\boldsymbol{z}[T_0]$. Thus the switched linear system of (26) would be unstable, if its "equivalent" system matrix $\Phi(\lambda)$ has eigenvalues with magnitude outside the unity circle. □

Based on Lemma 1, we can see that if an advanced attacker can choose a proper constant λ, it may make the closed-loop LFC system for the AC/HVDC interconnected power system with emulated inertia unstable. To be noted, here we mainly consider the optimal DoS attack strategy that can corrupt the system stability, and thus the attacker is assumed to be with extensive attack resources to corrupt multiple wide-area measurements and also full knowledge of the underlying system (e.g., the parameters of the test system in (22)). Besides, the mitigation and detection schemes that the power systems are usually equipped with are not included in the framework of this article; we leave the possible complex "interactions" between DoS attacks and mitigation/detection schemes in the LFC system for the future work.

4. FDI Attacks on the AC/DC Multi-Area LFC System with Virtual Inertia

Vulnerabilities within the communication channels for wide-area measurements may also make the test LFC system exposed to data integrity attacks. FDI attack, known as a major class of integrity attack, can modify the values of measurements to corrupt the normal operation of controllers and further the physical system. Then next we study FDI attacks on the test LFC system in the hybrid AC/DC grid with virtual inertia. We extend our previous work [32] to include both stationary and dynamic FDI attacks in this article. Particularly, we show a specific type of dynamic FDI attack that can remain stealthy with respect to an arbitrary anomaly detector, while in the mean time cause severe damages to system frequency stability.

4.1. The Test LFC Sytem under FDI Attacks: Basics

As noted in Section 3.1, in this article we focus on the attack scenario where the uploading communication channels of wide-area measurements are attacked. Thus, the system output after FDI corruptions would become

$$\tilde{\boldsymbol{y}}[k] = \begin{cases} \boldsymbol{y}[k] & \text{if, } k \notin \mathcal{T}_f; \\ \boldsymbol{y}[k] + \boldsymbol{D}_f\boldsymbol{f}[k] & \text{if, } k \in \mathcal{T}_f, \end{cases} \tag{29}$$

where $\boldsymbol{f}[\cdot] \in \mathbb{R}^{n_f}$ represents the FDI attack signal, $\mathcal{T}_f$ denotes the FDI attack period, and $\boldsymbol{D}_f$ characterizes the part of measurements that are attacked by FDI. Again, as illustrated in Figure 1, FDI attacks on wide-area measurements would mainly corrupt the supervisory AGC and SPMC controls as these loops use the wide-area measurements as the controller inputs, which also implies that the virtual inertia emulator is not compromised directly by FDI. Based on (22) and (29), the closed-loop model of the test LFC system under FDI attacks can be expressed as

$$\begin{aligned} \boldsymbol{x}[k+1] &= \boldsymbol{A}_{cl}\boldsymbol{x}[k] + \boldsymbol{B}_d\boldsymbol{d}[k] + \boldsymbol{B}_f\boldsymbol{f}[k]\,, \\ \tilde{\boldsymbol{y}}[k] &= \boldsymbol{C}\boldsymbol{x}[k] + \boldsymbol{D}_f\boldsymbol{f}[k]\,, \end{aligned} \tag{30}$$

where $\boldsymbol{A}_{cl} := \boldsymbol{A} + \boldsymbol{B}_u\boldsymbol{K}\boldsymbol{C}$ and $\boldsymbol{B}_f := \boldsymbol{B}_u\boldsymbol{K}\boldsymbol{D}_f$. We can see that the corruptions on the supervisory control loops by FDI attacks would further affect the involved physical system.

To illustrate the attack strategy that an FDI attacker can exploit to be disruptive to the LFC system, let us start from the stationary FDI attack scenario where the attack occurs as a constant bias injection

on wide-area measurements during the attack period, i.e., $\boldsymbol{f}[k] = \boldsymbol{f}$ for $k \in \mathcal{T}_f$ and $\boldsymbol{f}$ is a constant vector while $\boldsymbol{f}[k] = \mathbf{0}$ for $k \notin \mathcal{T}_f$. We say such attack is "stationary" as the attack value remains unchanged during the attack period. As a typical FDI scenario, the stationary FDI attack has been studied in a large amount of literature work [12,39,41]. According to the number of manipulated wide-area measurements, stationary FDI attacks can be classified into two types in general, i.e., univariate attack ($n_f = 1$) and multivariate attack ($n_f > 1$).

Similar to the advanced DoS attack which aims to corrupt the system stability with an optimal strategy, an intelligent FDI attack with full system knowledge also would seek to maximize its impact on the targeted LFC system. To evaluate the attack impact, the indices of maximum frequency deviation (MFD) and steady-state frequency deviation (SSFD) for frequency stability are commonly deployed. In the univariate FDI attack scenario, intuitively, the attacker would prefer a larger constant bias injection to have the maximum impact from the perspective of MFD or SSFD. However, a large constant injection may also trigger data quality alerts. In general, data quality alerts would be triggered if the calculated ACE in the control center exceeds 0.05 p.u., according to the grid code in [7].

In order to have enough attack impact and remain undetected with respect to data quality checking programs, an adversary may have to compromise multiple wide-area measurements with vast attack resources to launch multivariate stationary attacks. Let us still consider an intelligent attack scenario where the attacker is also equipped with full knowledge of the underlying system (i.e., all the system parameters in Section 2 and possible data quality checking programs). Then, the multivariate attack can choose an appropriate injection of $\boldsymbol{f}$. In the following, we characterize the optimal strategy for stationary FDI attacks where the attacker aims to have enough attack impact and remain undetected from the data quality checking program, and in the mean time try to compromise as less measurements as possible. This strategy can be described by the optimization program,

$$\begin{aligned} \alpha_i^\star := \min_{\boldsymbol{f}} \quad & \| \boldsymbol{f} \|_0 \\ \text{s.t.} \quad & \boldsymbol{f} \in \mathcal{F}, \ \ \boldsymbol{f}(i) = \mu\,, \\ & \boldsymbol{f}(j) = 0, \ \ \text{for all } j \in \mathcal{P}\,, \end{aligned} \tag{31}$$

where $\| \cdot \|_0$ is the zero vector norm that quantifies the number of non-zero elements in the vector. The attack values which reflect the attack targets on impact and undetectability are taken from the set $\mathcal{F} := \{\boldsymbol{f} \in \mathbb{R}^{n_f} : \ \boldsymbol{b_{min}} \leq \boldsymbol{F_f f} \leq \boldsymbol{b_{max}}\}$ where the vectors $\boldsymbol{b_{min}}, \boldsymbol{b_{max}} \in \mathbb{R}^{n_b}$ and the matrix $\boldsymbol{F_f} \in \mathbb{R}^{n_b \times n_f}$ are scenario-specific and should be taken based on the criterion reflected in different national grid codes. For instance, to be disruptive of attack impact, the (absolute) MFD value should reach 0.8 Hz, as a possible load shedding scheme could be triggered when the frequency decreases to 59.2 Hz; we refer to our previous work in [32] for a detailed discussion on the selections of $\boldsymbol{b_{min}}$, $\boldsymbol{b_{max}}$ and $\boldsymbol{F_f}$. In (31), $\boldsymbol{f}(i)$ denotes the i-th FDI on the measurement that the attacker has already been able to compromise; this constraint is to make (31) feasible [37]. The last constraint in (31) is introduced to show that some protected measurements in the set $\mathcal{P}$ could not be attacked.

By using a so-called big M approach in [37], the problem of (31) can be translated into a mixed integer linear program (MILP). A MILP can be usually solved by a solver like CPLEX. The obtained index $\alpha_i^\star$ in the optimal attack strategy of (31) in some sense can also access "how hard" it is for the attacker to attack the test LFC system with significant impact and also undetectability, and it is of interest to both the attacker and the system operator: if $\alpha_i^\star$ is large, it requires extensive coordinated attack resources by the attacker to accomplish; if $\alpha_i^\star$ is small, some of the measurements are critical as they require fewer corruptions to be altered.

4.2. A Type of Stealthy FDI Attack on the Test LFC System: Zero-Dynamics Attack

For the stationary FDI attacks above, though the intelligent ones with enough system knowledge and vast attack resources can remain undetected from data quality checking programs, advanced

detection schemes can still be developed to reveal their occurrence. In [32], we have proposed an anomaly detector for the detection, isolation, and even recovery of both stationary univariate and multivariate FDI attacks. In this subsection, we further explore the possibility of a type of FDI attack that can be stealthy with respect to arbitrary anomaly detectors. This comes to a type of dynamic (time-variant) FDI attack called *zero-dynamics attack*. Within a zero-dynamic attack strategy, the attacker can make the system outputs zero but drive the state (e.g., frequency of each area) trajectory of the underlying system (i.e., the test LFC system interconnected by AC/HVDC transmission lines and equipped with ESS for inertia emulation) to a possible unsafe set (e.g., the MFD defined in the previous subsection reaches a certain value that can mislead to wrong system operations). As the system outputs also act as inputs to an arbitrary anomaly detector, the diagnostic signal of the anomaly detector would not be able to trigger alerts for this type of attack when the system outputs are zero. To formalize the attack scenario, we introduce the following definition based on the work in [42].

Definition 1. *[Zero-dynamics attack] An FDI attack $\boldsymbol{f}[k]$ is called zero-dynamics attack if the corrupted system output $\tilde{\boldsymbol{y}}$ in (29) satisfies $\tilde{\boldsymbol{y}}[k] = 0$ for $k \in \mathcal{T}_f$. Without less of generality, we let $\mathcal{T}_f$ be the time interval $[0,\ T_f)$.*

That is to say, one cannot decouple such an FDI attack from the system outputs, and therefore it can not be detected by an arbitrary anomaly detector. It has been shown in [42] that the attack sequence that makes the outputs identically zero for all $k \in T_f$ is given by

$$\boldsymbol{f}[k] = z_0^k \boldsymbol{f}_0\,, \tag{32}$$

where z_0 is the system zero and $\boldsymbol{f}_0$ is the corresponding input zero direction. Considering the LFC system model in (30) under FDI attacks, such a signal $\boldsymbol{f}[\cdot]$ in (32) can be checked by using the Rosenbrock system matrix and correspondingly the input zero direction for a system zero $z_0 \in \mathbb{C}$ can be obtained, according to the work in [42]. This can be written as

$$\boldsymbol{P}(z) = \begin{bmatrix} \boldsymbol{A}_{cl} - z\boldsymbol{I} & \boldsymbol{B}_d & \boldsymbol{B}_f \\ \boldsymbol{C} & \boldsymbol{0} & \boldsymbol{D}_f \end{bmatrix}, \quad \boldsymbol{P}(z_0) \begin{bmatrix} \boldsymbol{x}_0 \\ \boldsymbol{d}_0 \\ \boldsymbol{f}_0 \end{bmatrix} = \boldsymbol{0}\,. \tag{33}$$

It can be observed that $\boldsymbol{f}[k] = z_0^k \boldsymbol{f}_0$ is a zero-dynamics attack if and only if there exists $\boldsymbol{x}_0 \in \mathbb{C}^{n_x}$ and $\boldsymbol{d}_0 \in \mathbb{C}^{n_d}$ that satisfies (33). This implies that the zero-dynamics attack $\boldsymbol{f}[k] = z_0^k \boldsymbol{f}_0$ is stealthy only if there is a simultaneous disturbance signal $\boldsymbol{d}[k] = z_0^k \boldsymbol{d}_0$ and initial state $\boldsymbol{x}[0] = \boldsymbol{x}_0$. Note the fact that the disturbance signal in the LFC system model of (30) represents load changes. Thus it may be infeasible for the case $\boldsymbol{d}[k] = z_0^k \boldsymbol{d}_0$ in practice. However, one can consider a scenario where the loads keep constant while a zero-dynamics attack $\boldsymbol{f}[k] = z_0^k \boldsymbol{f}_0$ is launched by the attacker to make system outputs zero. Such a zero-dynamics attack can be obtained from the following equation,

$$\begin{bmatrix} \boldsymbol{A}_{cl} - z_0\boldsymbol{I} & \boldsymbol{B}_f \\ \boldsymbol{C} & \boldsymbol{D}_f \end{bmatrix} \begin{bmatrix} \boldsymbol{x}_0 \\ \boldsymbol{f}_0 \end{bmatrix} = \boldsymbol{0}\,. \tag{34}$$

If there exist solutions to (34), then the zero-dynamics attack exists and the system operator would also be misled to believe that there is no load change and hence the system outputs are zero, while, in fact, the dynamic FDI attack may have driven the system states of frequencies in both areas to unsafe sets. Notably, if the test system (30) is assumed to be with zero initial state and there exists a large difference between $\boldsymbol{x}_0$ from (34) and zero initial condition, then the zero-dynamics attack from (34) may be detectable especially in the beginning period of the attack sequence [42].

To this end, similar to the case of stationary FDI attack, we can also consider an intelligent attack scenario where the attacker tries to compromise as less measurements as possible, which would lead to the following optimization program,

$$\begin{aligned} \beta_i^\star := \min_{z_0, \boldsymbol{x}_0, \boldsymbol{f}_0^i} \quad & \|\boldsymbol{f}_0^i\|_0 \\ \text{subject to} \quad & \begin{bmatrix} \boldsymbol{A}_{cl} - z_0 \boldsymbol{I} & \boldsymbol{B}_f \\ \boldsymbol{C} & \boldsymbol{D}_f \end{bmatrix} \begin{bmatrix} \boldsymbol{x}_0 \\ \boldsymbol{f}_0^i \end{bmatrix} = \boldsymbol{0}, \\ & \boldsymbol{f}_0(i) = \eta. \end{aligned} \tag{35}$$

One can also let $|z_0| \geq 1$ in (35) such that the attack signal can be persistent (if $|z_0| < 1$, the attack signal will asymptotically vanish to zero). We also add the last constraint about $\boldsymbol{f}_0(i)$ to make (35) feasible. In general, similar to (31) for a stationary FDI attack, (35) is a combinatorial problem and is hard to solve. However, it can have simple solutions if there is finite number of system zeros of z_0. For instance, if there is a single z_0, then the null-space of $\boldsymbol{P}(z_0)$ has dimension 1, and there is only one unitary vector $[\boldsymbol{x}_0^\top, \boldsymbol{f}_0^\top]^\top$ that is the solution to (34). If the null-space of $\boldsymbol{P}(z_0)$ has dimension n, then there are n unitary vectors that are solutions to (34). A linear combination of these n unitary vectors is also a solution, and similar to (31), one can use big M method to translate (35) into a MILP problem which can be solved by the solver CPLEX.

5. Simulation Results

In this section, we evaluate the effects of these two types of data integrity and availability attacks-DoS and FDI attacks-on the test LFC system through simulations. As shown in Figure 1, the two-area system is interconnected with AC/HVDC transmission lines and equipped with bulk ESS for inertia emulation. The parameters of the two-area system and also associated control loops, i.e., the parameters appeared in Equations (1)–(12), are referred to Table 1 in Section 2.4. Then, the matrices involved in the original state-space model of (13) for the two-area LFC system can be obtained through (15) to (17). In particular, we are interested in the difference between effects of these two types of data integrity and availability attacks on the LFC models of the following studied systems in this article:

- Normal AC system.
- AC/DC interconnected system.
- AC/DC interconnected system with virtual inertia.

From Section 2, we have seen that the LFC model in the system interconnected by AC/HVDC lines and equipped with ESS has more controllable devices, comparing with the one in the normal AC system. Intuitively, an attacker can manipulate more vulnerable measurements as it can attack frequencies of both areas and also power flows on both AC and HVDC transmission lines. Furthermore, the DoS and FDI attacks on all of these measurements would affect not only the supervisory AGC loop but also the SPMC for power modulation in control center. Thus, in this section, we perform a comparison study through simulations to explore the difference of attack impact on these three LFC system models.

5.1. DoS Attack Results

We start with DoS attacks. In Section 3.2, we have introduced a constant $\lambda \in [0, 1]$ such that if an advanced attacker can choose a proper λ, the "equivalent" closed-loop LFC system under DoS attacks on measurements (with system matrix $\Phi(\lambda) = \Phi_1^\lambda \Phi_2^{(1-\lambda)}$) can be made unstable. From the proof of Lemma 1, we would note that the smaller λ is, the earlier the DoS attack occurs. Then, we let γ_m denote the maximum real part of eigenvalues of $\Phi(\lambda) = \Phi_1^\lambda \Phi_2^{(1-\lambda)}$. To study how the DoS attack would affect the stability of the underlying LFC systems, we compute γ_m with λ ranging between 0 and 1 for the three LFC system models. The results are shown in Figure 3. It can be seen form Figure 3

that $\gamma_m > 1$ when λ is close to 0 for all of these systems, which implies that there exists an eigenvalue with magnitude outside the unity circle and the systems are unstable. With the increase of λ, γ_m may decrease and be smaller than 1 later. This result is straightforward since the LFC systems become unstable more easily when DoS attacks occur at an early period. For the LFC of normal AC system, $\gamma_m < 1$ when $\lambda \geq 0.6$. For AC/DC system, $\gamma_m < 1$ when $\lambda \geq 0.33$. For AC/DC system but with virtual inertia, γ_m is around 1 when λ is small, and is smaller than 1 when $\lambda \geq 0.53$.

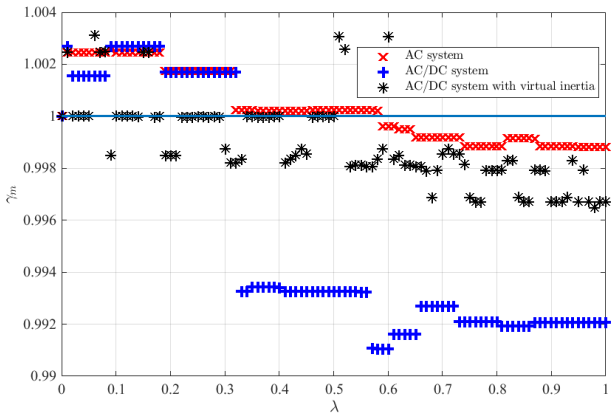
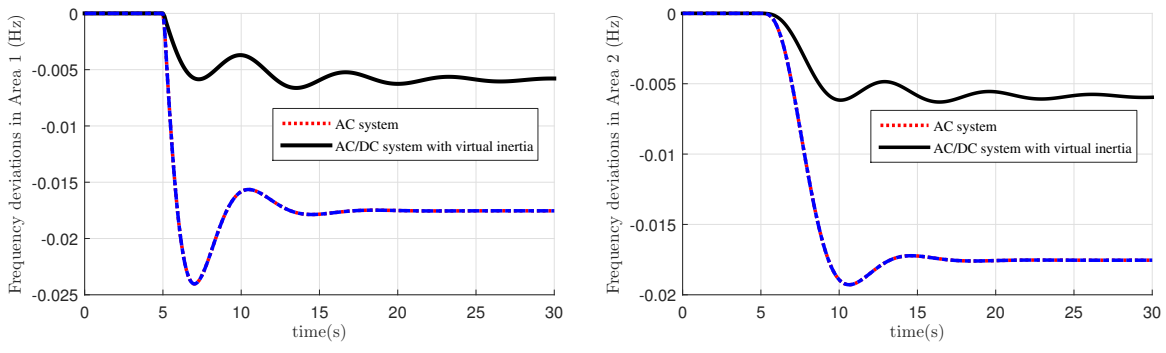


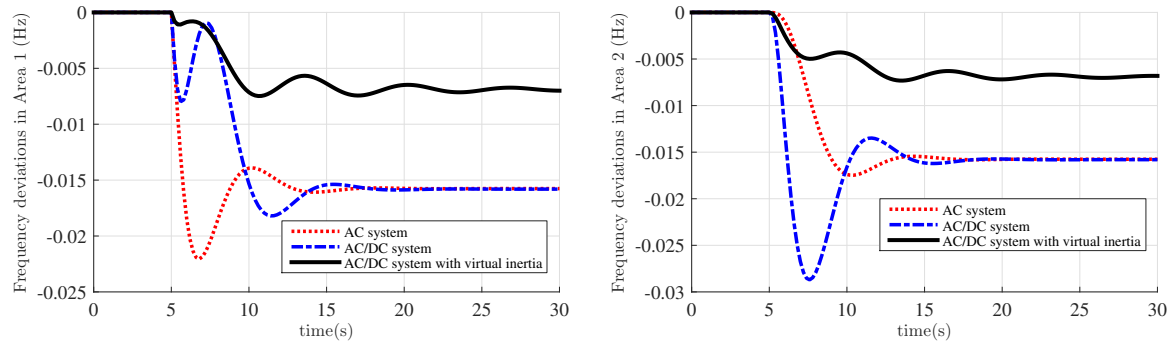
Figure 3. The maximum real part of the eigenvalues of $\Phi(\lambda) = \Phi_1^{\lambda}\Phi_2^{(1-\lambda)}$ for the three load frequency control (LFC) systems.

We let the time interval in the proof of Lemma 1 be $[0, 30)$ (in seconds). Then, three case studies are considered in the simulations of DoS attacks: (i) Case 1: $\lambda = 0.033$, the three LFC systems are under DoS attacks which start from $t = 1$ s; (ii) Case 2: $\lambda = 0.2$, the three LFC systems are under DoS attacks which start from $t = 6$ s; (iii) Case 3: $\lambda = 0.4$, the three LFC systems are under DoS attacks which start from $t = 12$ s. For all the cases, similar to Figure 2, we add a step load input to the test LFC systems that there is an increase of 0.03 p.u. in Load 1 of Area 1, at $t = 5$ s. The simulation results of the three case studies are presented in Figures 4–6. For Case 1 in Figure 4, the DoS attacks occur at $t = 1$ s, which is before the load change. It can be observed that there are large steady-state frequency deviations (SSFDs) because the controller is attacked by DoS completely. For Case 2 in Figure 5, the DoS attacks occur right after the event of step-load change and we still see large SSFDs. Comparing the results of Figures 4–6, it is reasonable to conclude that from the viewpoint of the attacker, it is optimal to launch DoS attacks as early as the dynamics of the LFC system does not converge. When the attacks occur in a late stage, the DoS attacks might not have big impact; see the results of Case 3 where $\lambda = 0.4$. It can be also expected that as long as the LFC system dynamics has converged, the DoS attacks would not have effects any more.



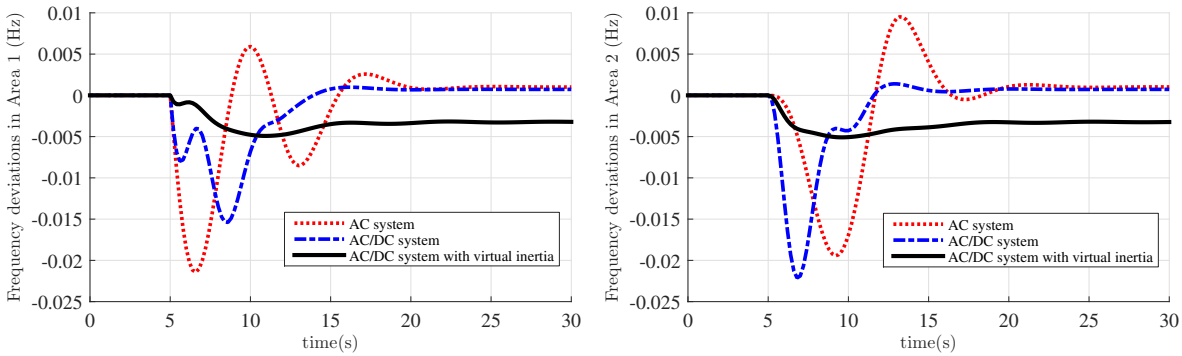
(**a**) (**b**)

Figure 4. Case 1: results of both areas under a step-load change at 5 s and also DoS attacks that start from 1 s. (**a**) Frequency deviation of Area 1. (**b**) Frequency deviation of Area 2.



(**a**) (**b**)

Figure 5. Case 2: results of both areas under a step-load change at 5 s and also DoS attacks that start from 6 s. (**a**) Frequency deviation of Area 1. (**b**) Frequency deviation of Area 2.



(**a**) (**b**)

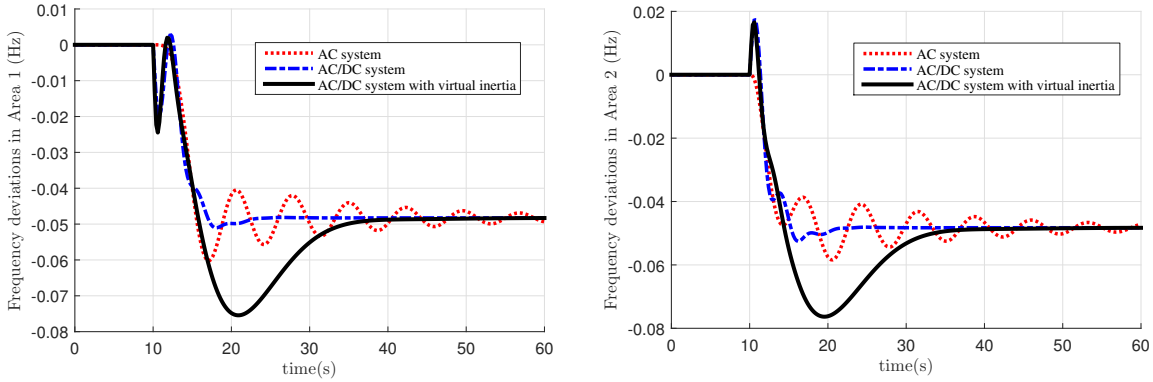
Figure 6. Case 3: results of both areas under a step-load change at 5 s and also DoS attacks that start from 12 s. (**a**) Frequency deviation of Area 1. (**b**) Frequency deviation of Area 2.

When looking into the frequency deviations of the three system LFC models in Figures 4 and 5, we can also see that the impact of early DoS attacks on the LFC models of normal AC system and AC/DC system but without virtual inertia can be more significant from the perspective of SSFD, comparing with the one of the AC/DC interconnected system with virtual inertia. This is due to the fact that the control loop of inertia emulation is not attacked directly by DoS as it is using local frequency information only, while the DoS attacks are mainly on measurements for supervisory AGC and SPMC loops. The emulated inertia still works to damp frequency oscillations even during these DoS attacks. However, as shown in Figure 6, for the DoS attacks that occur at $t = 12$ s, there would be a larger SSFD in the LFC of the system with AC/HVDC transmission lines and virtual inertia. This is because the ESS is mainly used for a short period of time (2 s to 5 s) to emulate virtual inertia (recall Section 2.3), while the load step event starts from $t = 5$ s. To conclude, the frequency dynamics of the LFC system under DoS attacks would become worse comparing with the scenario where there is no DoS attack, while the effects of DoS attacks (quantified by attack impact index, e.g., SSFD) on the three LFC system models of this article depend to the time that the DoS attack occurs.

5.2. FDI Attack Results

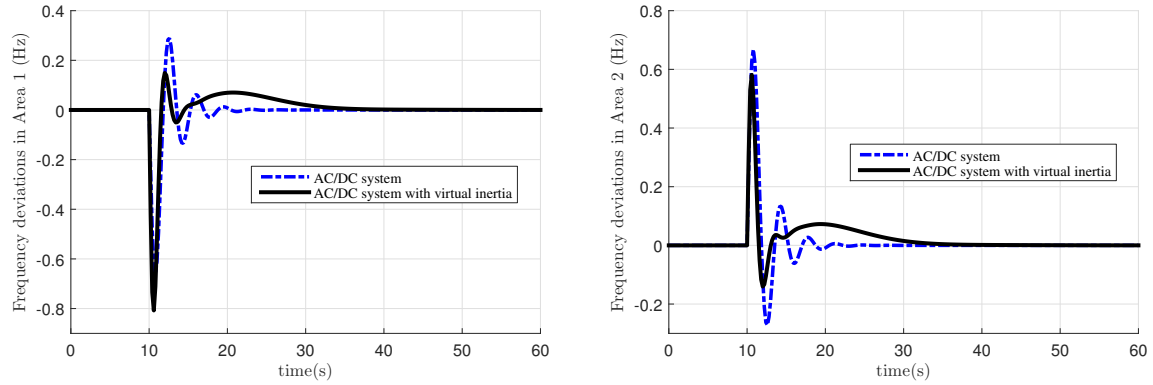
Next, we evaluate the effects of FDI attacks on the three LFC system models. To begin with, stationary univariate and multivariate attacks are launched. The frequency deviation results under a univariate attack on the frequency measurement of Area 2 are shown in Figure 7. We can see that regarding the attack impact index of MFD (maximum frequency deviation) during the transients, there would be a larger MFD in the LFC of the system interconnected by AC/HVDC lines and equipped with ESS to emulate inertia. This observation is consistent with the result of [32], and we refer to [32] for a more detailed analysis of univariate attacks on the other wide-area measurements (e.g., frequency

of Area 1, AC/DC power flow). Then, we move to stationary multivariate attacks where multiple measurements are attacked simultaneously to be disruptive and undetectable (with respect to data quality checking programs). The optimal strategies for these attacks can be obtained from (31) by solving the resulted MILP using the solver CPLEX. It turns out that a multivariate attack ($\alpha_i^\star = 2$) that can attack power flows on both AC and HVDC lines with a attack magnitude vector $\boldsymbol{f} = [0.44 \ -0.39]^\top$ (in p.u.) is able to disrupt the LFC system and avoid data quality alarms. The frequency deviations under this multivariate attack are shown in Figure 8. The MFD of Area 1 in the AC/DC interconnected system with emulated inertia arrives at -0.8 Hz after the occurrence of multivariate attack, which may mislead wrong system operations of load shedding. To be noted, when solving solving (31) for the normal AC system, there is no such kind of multivariate FDI attack that can have enough impact regarding the index MFD but remain undetected from data quality checking programs. From the observations above, the inertia emulation functionality plays a key role in affecting the dynamic behavior of the test LFC system under FDI attacks. Due to the frequency variations caused by FDI attacks on supervisory controls, the inertia emulator is also being "misled" as it calculates rate of change of frequency (ROCOF) from local frequency information in its derivative control loop (recall Section 2.3), which in turn would contribute to a larger MFD.



(**a**) (**b**)

Figure 7. Results of both areas under a univariate attack with a magnitude of 0.1 Hz on the measurement of frequency in Area 2, at $t = 10$ s. (**a**) Frequency deviation of Area 1. (**b**) Frequency deviation of Area 2.



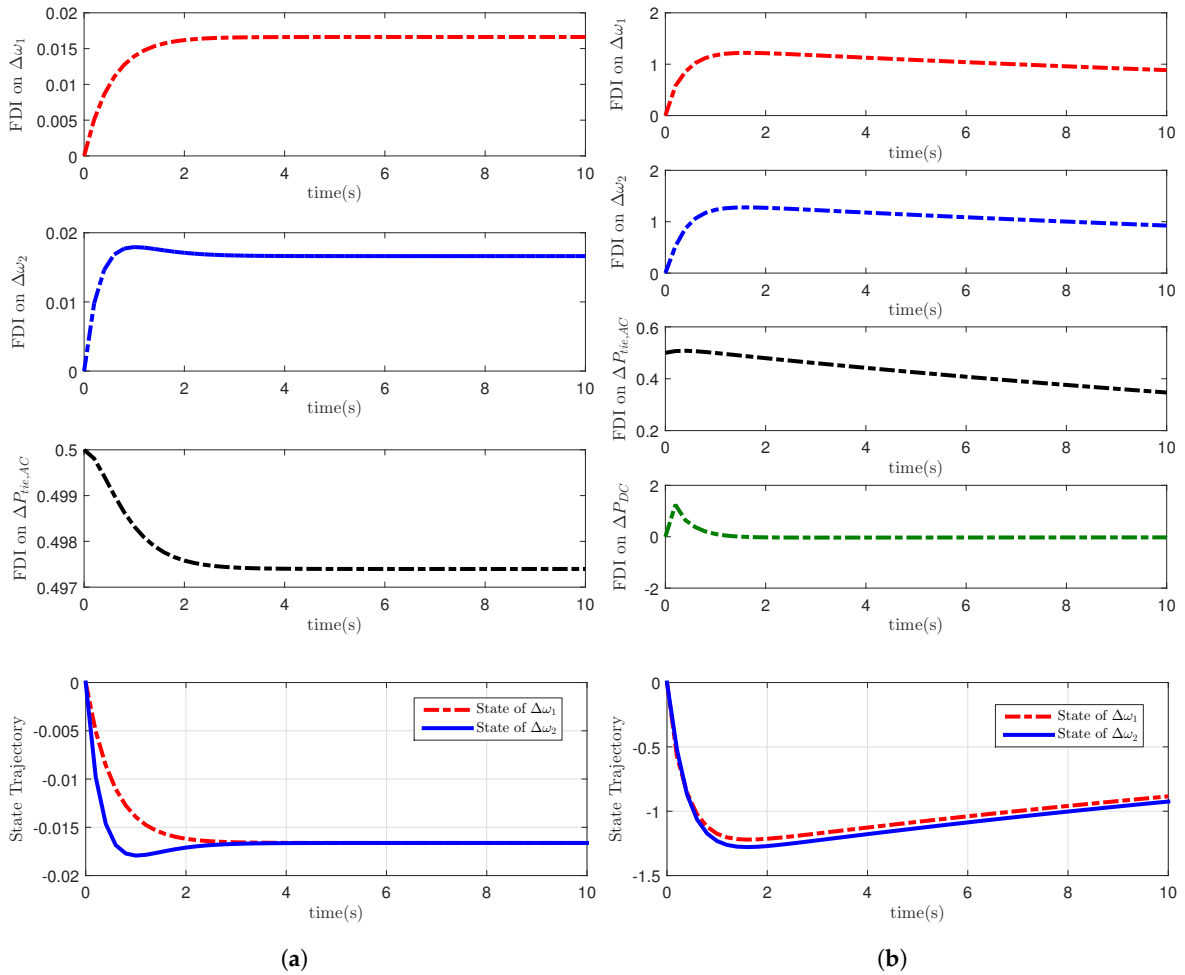
(**a**) (**b**)

Figure 8. Results of both areas under multivariate attacks on power flow measurements of both AC and HVDC lines with magnitudes of 0.44 p.u. and -0.39 p.u., respectively, at $t = 10$ s. (**a**) Frequency deviation of Area 1. (**b**) Frequency deviation of Area 2.

The stationary FDI attacks above can be detected by an advanced anomaly detector. However, as illustrated in Section 4.2, the so-called zero-dynamics attack can lead to zero system outputs and thus remain hidden with respect to arbitrary anomaly detectors. To the end, we move to the simulations of such an attack scenario. From the calculations of system zeros, we see that for the LFC of normal AC

system, there are four system zeros (0.5850, 0.5908, 0.6927, 1) of real values and correspondingly four unitary vectors that are solutions to (34). For the LFC of AC/DC system but without virtual inertia, there are five system zeros (−0.0250, 0.5856, 0.5908, 0.8087, 1) of real values and correspondingly five unitary vectors that are solutions in the null-space of $\boldsymbol{P}(z_0)$. For the LFC of AC/DC system with virtual inertia provided by ESS, there are eight system zeros (−0.0622, 0.5846, 0.5908, 0.6008, 0.6661, 0.9332, 0.9779, 0.9920) of real values and correspondingly 8 unitary vectors.

To compare the three LFC system models under zero-dynamics attacks, first we let $\boldsymbol{f}_0(i)$ in (35) be the injection on the AC power flow measurement with a value of 0.5 p.u. and solve (35) for all the LFC systems. Figure 9 depicts the state trajectory of frequency under the resulted zero-dynamics attacks on the normal AC system and the AC/DC system with emulated inertia. We can observe that the zero-dynamics attack is able to drive the state of frequency in the LFC of the system interconnected by AC/HVDC lines and equipped with ESS to outside the safe set; see Figure 9b where the MFD can reach a certain value to mislead wrong system operations of load shedding. Besides, we can notice that different from the stationary univariate/multivariate attack, the false data injections in the zero-dynamics attack are "dynamic" (time-variant) and coordinated to remain stealthy to an arbitrary anomaly detector. To be noted, in the zero-dynamics attack scenario, the operator believes that there are no load changes as the system outputs are "made" zero by attacks, while the system states of frequencies in both areas have been driven to unsafe sets. This implies that the zero-dynamics attack can cause severe damages to the system frequency stability.



(**a**) (**b**)

Figure 9. State trajectory under zero-dynamics attacks on wide-area measurements with $\boldsymbol{f}_0(i)$ in (35) being the injection on the AC power flow measurement with a value of 0.5 p.u.. (**a**) normal AC system; (**b**) AC/DC system with virtual inertia.

Similarly, Figure 10 shows the state trajectory of the AC/DC system and AC/DC system with virtual inertia under zero-dynamics attacks where $f_0(i)$ in (35) is the injection on the DC power flow measurement with a value of 0.5 p.u. (the normal AC system is not attacked in this scenario as it does not have DC power flow measurement). The zero-dynamics attack can still result in large (frequency) state deviations especially in the context of LFC in a hybrid AC/DC system with virtual inertia. Notably, the impact index MFD would be made more large under such zero-dynamics attack if one increases the initial attack value of $f_0(i)$ in (35). To conclude, the stealthy zero-dynamics attack can be very impactful to the LFC systems when the loads are constant during a specific time period and the null-space of $\boldsymbol{P}(z_0)$ has multiple dimensions. Besides, the LFC model considering the added elements of HVDC link and ESS for virtual inertia can be more vulnerable to such attacks when the three LFC system models have the same initial attack value of $f_0(i)$ in (35).

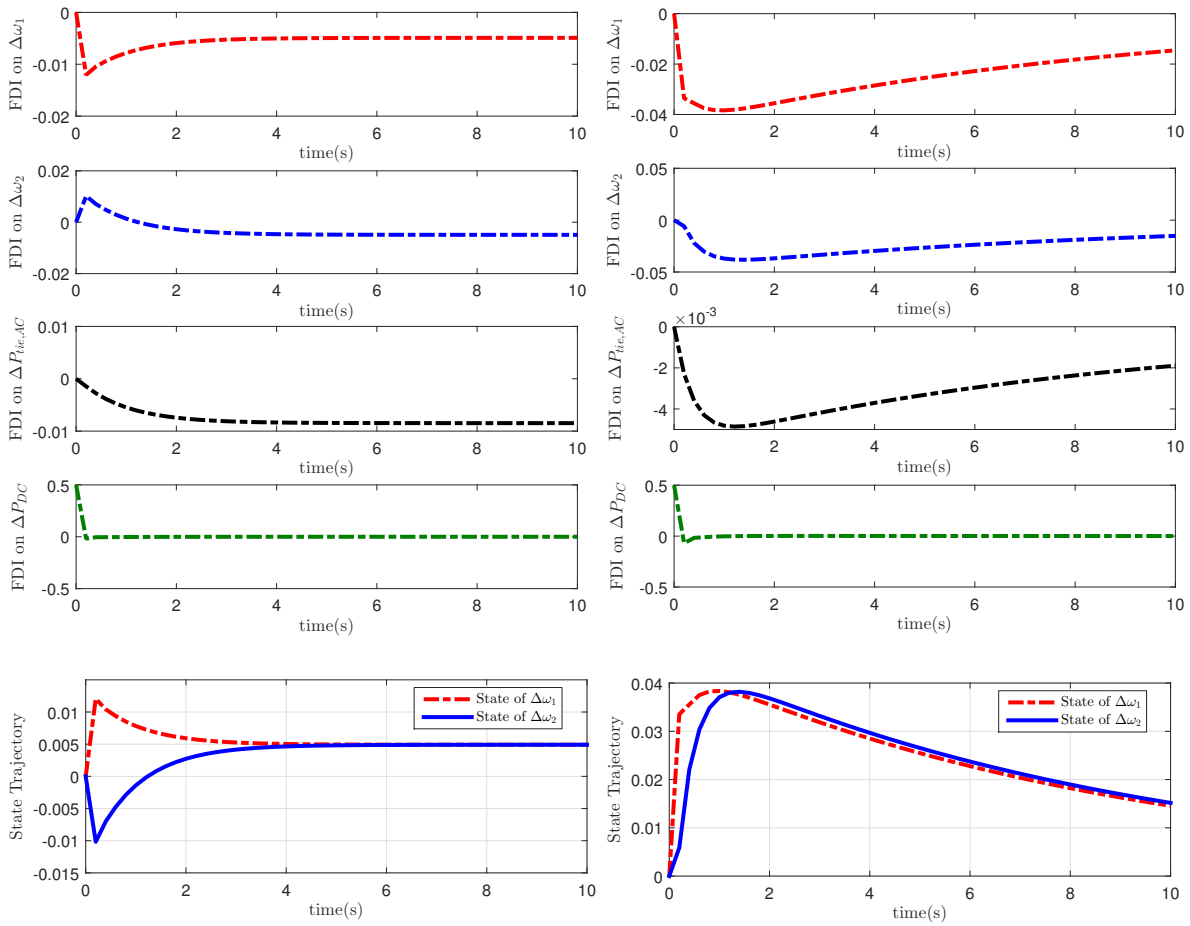


Figure 10. State trajectory under zero-dynamics attacks on wide-area measurements with $f_0(i)$ in (35) being the injection on the DC power flow with a value of 0.5 p.u. (**a**) AC/DC system; (**b**) AC/DC system with virtual inertia.

5.3. Discussions

In this article, both DoS and FDI attacks are studied in the new LFC considering AC/HVDC links and inertia emulation module by added ESS. From the results above, we see that the LFC system with AC/HVDC interconnections and emulated inertia could be more vulnerable to the two types of attacks in many adversarial scenario. Here we provide a brief discussion on how these attacks can be detected.

The DoS attacks are trivially detectable as the absence of data can be treated as an anomaly [42]. However, they can also be misdiagnosed as a poor communication network condition. To detect such attacks, one may utilize the statistical properties of the missing data: we can assume that,

under normal conditions, each wide-area measurement may be missing with a given small probability. Then, the Bernoulli distributed random variables can be introduced to indicate whether the measurements data are available or not, and one can differentiate between cases of low probability of missing data under normal conditions, versus cases where missing data occurs with higher probability due to DoS attacks.

For the FDI attacks, it is relatively easier to reveal the occurrence of the stationary ones. For instance, in our work [32], we have proposed a detector with adjustable design variables to have a fast response in the inertia context when the stationary FDI attacks occur. One can also detect the multivariate stationary attack which is equipped with vast attack resources and full knowledge of the targeted system, by designing a bank of detectors where each of them is responsible to detect a particular FDI intrusion. When it comes to the extremely powerful dynamic attack, the detection task becomes much more difficult. The zero-dynamics attack could keep stealthy to an arbitrary detector if certain conditions are satisfied. However, it is noteworthy that this is a rather conservative viewpoint, and for attacks not satisfying all the conditions in Section 4.2, one can still have a successful detection. To this end, we note that many of attacks discussed in this article could trigger alerts on communication network specific measures (e.g., Intrusion Detection System). This give us opportunities to design cross-domain detection schemes to improving the overall cyber attacks detection.

6. Conclusions

In this article, we aim to explore the effects of two major types of data integrity and availability attacks-DoS and FDI attacks on the new LFC system that could be equipped with AC/HVDC transmission lines and also ESS for inertia emulation in the modern scenarios. We have modeled the test LFC system under DoS attacks as a switched linear system, and theoretical results are provided for switching strategies that an advanced DoS attacker can exploit to make the system unstable. For the FDI attack scenario, both stationary and dynamic FDI attacks are studied and their optimal strategies to achieve attack impact and undetectability are proposed. Particularly, the zero-dynamics FDI attack is introduced, and we show that it can remain stealthy with respect to arbitrary anomaly detectors and drive the system states of frequencies to unsafe sets. We hope that our work provides inspirations for moving in that direction: the complexity of the attack scenario and also the modern power system itself has introduced more challenges in the system operation.

In addition to theoretical results, a comparison study is performed by simulations on the exemplary two-area system to learn DoS and FDI attacks on three different LFC system models. The numerical results illustrate that in many adversarial scenarios, the LFC system with AC/HVDC transmission lines and added ESS can be more vulnerable to the cyber attacks of this article. In particular, the inertia emulation part is key to the performance of LFC system dynamics under both types of DoS and FDI attacks. This requires more advanced mitigation or detection schemes in the context of LFC system with new elements of HVDC link and inertia emulation block. We have a discussion above on a possible detection scheme as we can envision, and we leave it for future work.

Author Contributions: Conceptualization, K.P., E.R. and P.P.; methodology, K.P.; software, K.P. and J.D.; validation, K.P., J.D. and E.R.; formal analysis, K.P.; investigation, K.P. and E.R.; resources, E.R. and P.P.; data curation, K.P.; writing—original draft preparation, K.P. and J.D.; writing—review and editing, K.P., J.D., E.R. and P.P.; visualization, K.P.; supervision, P.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript.

LFC	Load frequency control
HVDC	High-voltage direct-current
AC	Alternating-current

DoS	Denial of service
FDI	False data injection
RES	Renewable energy resources
ESS	Energy storage systems
SCADA	Supervisory control and data acquisition
GEN	Generation unit
ACE	Area control error
AGC	Automatic generation control
SPMC	Supplementary power modulation controller
ROCOF	Rate of change of frequency
MITM	Man-in-the-middle
ZOH	Zero-order hold
MFD	Maximum frequency deviation
SSFD	Steady-state frequency deviation
MILP	Mixed integer linear program

References

1. Alipoor, J.; Miura, Y.; Ise, T. Power System Stabilization Using Virtual Synchronous Generator With Alternating Moment of Inertia. *IEEE J. Emerg. Sel. Top. Power Electron.* **2015**, *3*, 451–458. [CrossRef]
2. Castro, L.M.; Acha, E. On the Provision of Frequency Regulation in Low Inertia AC Grids Using HVDC Systems. *IEEE Trans. Smart Grid* **2016**, *7*, 2680–2690. [CrossRef]
3. Zhang, W.; Rouzbehi, K.; Luna, A.; Gharehpetian, G.B.; Rodriguez, P. Multi-terminal HVDC grids with inertia mimicry capability. *IET Renew. Power Gener.* **2016**, *10*, 752–760. [CrossRef]
4. Ten, C.W.; Liu, C.C.; Manimaran, G. Vulnerability Assessment of Cybersecurity for SCADA Systems. *IEEE Trans. Power Syst.* **2008**, *23*, 1836–1846. [CrossRef]
5. Vrakopoulou, M.; Esfahani, P.M.; Margellos, K.; Lygeros, J.; Andersson, G. Cyber-attacks in the automatic generation control. In *Cyber Physical Systems Approach to Smart Electric Power Grid*; Springer: New York, NY, USA, 2015; pp. 303–328. [CrossRef]
6. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber-Physical System Security for the Electric Power Grid. *Proc. IEEE* **2012**, *100*, 210–224. [CrossRef]
7. Sridhar, S.; Govindarasu, M. Model-Based Attack Detection and Mitigation for Automatic Generation Control. *IEEE Trans. Smart Grid* **2014**, *5*, 580–591. [CrossRef]
8. Ashok, A.; Wang, P.; Brown, M.; Govindarasu, M. Experimental evaluation of cyber attacks on Automatic Generation Control using a CPS Security Testbed. In Proceedings of the IEEE Power Energy Society General Meeting, Denver, CO, USA, 26–30 July 2015; pp. 1–5. [CrossRef]
9. Khalaf, M.; Youssef, A.; El-Saadany, E. Joint Detection and Mitigation of False Data Injection Attacks in AGC Systems. *IEEE Trans. Smart Grid* **2019**, *10*, 4985–4995. [CrossRef]
10. Beitollahi, H.; Deconinck, G. Analyzing well-known countermeasures against distributed denial of service attacks. *Comput. Commun.* **2012**, *35*, 1312–1332. [CrossRef]
11. Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. *IEEE Trans. Power Syst.* **2017**, *32*, 3317–3318. [CrossRef]
12. Pan, K.; Palensky, P.; Esfahani, P.M. From Static to Dynamic Anomaly Detection With Application to Power System Cyber Security. *IEEE Trans. Power Syst.* **2020**, *35*, 1584–1596. [CrossRef]
13. Sridhar, S.; Manimaran, G. Data integrity attacks and their impacts on SCADA control system. In Proceedings of the IEEE Power Energy Society General Meeting, Providence, RI, USA, 25–29 July 2010; pp. 1–6. [CrossRef]
14. Esfahani, P.M.; Vrakopoulou, M.; Margellos, K.; Lygeros, J.; Andersson, G. Cyber attack in a two-area power system: Impact identification using reachability. In Proceedings of the American Control Conference (ACC), Baltimore, MD, USA, 30 June–2 July 2010; pp. 962–967. [CrossRef]
15. Pan, K.; Gusain, D.; Palensky, P. Modelica-Supported Attack Impact Evaluation in Cyber Physical Energy System. In Proceedings of the IEEE 19th International Symposium on High Assurance Systems Engineering (HASE), Hangzhou, China, 3–5 January 2019; pp. 228–233. [CrossRef]

16. Liu, S.; Liu, X.P.; El Saddik, A. Denial-of-Service (dos) attacks on load frequency control in smart grids. In Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24–27 February 2013; pp. 1–6. [CrossRef]
17. Rahimi, K.; Parchure, A.; Centeno, V.; Broadwater, R. Effect of communication Time-Delay attacks on the performance of Automatic Generation Control. In Proceedings of the North American Power Symposium (NAPS), Charlotte, NC, USA, 4–6 October 2015; pp. 1–6. [CrossRef]
18. Zhang, J.; Domínguez-García, A.D. On the impact of communication delays on power system automatic generation control performance. In Proceedings of the North American Power Symposium (NAPS), Pullman, WA, USA, 7–9 September 2014; pp. 1–6. [CrossRef]
19. Bevrani, H.; Hiyama, T. On Load–Frequency Regulation With Time Delays: Design and Real-Time Implementation. *IEEE Trans. Energy Convers.* **2009**, *24*, 292–300. [CrossRef]
20. Jiang, L.; Yao, W.; Wu, Q.H.; Wen, J.Y.; Cheng, S.J. Delay-Dependent Stability for Load Frequency Control With Constant and Time-Varying Delays. *IEEE Trans. Power Syst.* **2012**, *27*, 932–941. [CrossRef]
21. Liu, S.; Liu, P.X.; Saddik, A.E. Modeling and Stability Analysis of Automatic Generation Control Over Cognitive Radio Networks in Smart Grids. *IEEE Trans. Syst. Man Cybern. Syst.* **2015**, *45*, 223–234. [CrossRef]
22. Rakhshani, E.; Remon, D.; Rodriguez, P. Effects of PLL and frequency measurements on LFC problem in multi-area HVDC interconnected systems. *Int. J. Electr. Power Energy Syst.* **2016**, *81*, 140–152. [CrossRef]
23. Vural, A.M. Contribution of high voltage direct current transmission systems to inter-area oscillation damping: A review. *Renew. Sustain. Energy Rev.* **2016**, *57*, 892–915. [CrossRef]
24. Rouzbehi, K.; Zhang, W.; Ignacio Candela, J.; Luna, A.; Rodriguez, P. Unified reference controller for flexible primary control and inertia sharing in multi-terminal voltage source converter-HVDC grids. *Transm. Distrib. IET Gener.* **2017**, *11*, 750–758. [CrossRef]
25. Bevrani, H.; Hiyama, T. *Intelligent Automatic Generation Control*; CRC Press: Boca Raton, FL, USA, 2017.
26. Chamorro, H.R.; Sevilla, F.R.S.; Gonzalez-Longatt, F.; Rouzbehi, K.; Chavez, H.; Sood, V.K. Innovative primary frequency control in low-inertia power systems based on wide-area RoCoF sharing. *IET Energy Syst. Integr.* **2020**, *2*, 151–160. [CrossRef]
27. Rakhshani, E.; Rodriguez, P. Inertia Emulation in AC/DC Interconnected Power Systems Using Derivative Technique Considering Frequency Measurement Effects. *IEEE Trans. Power Syst.* **2017**, *32*, 3338–3351. [CrossRef]
28. Gholami, A.; Mousavi, M.; Srivastava, A.K.; Mehrizi-Sani, A. Cyber-Physical Vulnerability and Security Analysis of Power Grid with HVDC Line. In Proceedings of the North American Power Symposium (NAPS), Wichita, KS, USA, 13–15 October 2019; pp. 1–6. [CrossRef]
29. Fan, R.; Lian, J.; Kalsi, K.; Elizondo, M. Impact of Cyber Attacks on High Voltage DC Transmission Damping Control. *Energies* **2018**, *11*, 1046. [CrossRef]
30. Brown, H.E.; Demarco, C.L. Risk of Cyber-Physical Attack via Load With Emulated Inertia Control. *IEEE Trans. Smart Grid* **2018**, *9*, 5854–5866. [CrossRef]
31. Roy, S.D.; Debbarma, S. Detection and Mitigation of Cyber-Attacks on AGC Systems of Low Inertia Power Grid. *IEEE Syst. J.* **2019**, *14*, 1–9. [CrossRef]
32. Pan, K.; Rakhshani, E.; Palensky, P. False Data Injection Attacks on Hybrid AC/HVDC Interconnected Systems With Virtual Inertia—Vulnerability, Impact and Detection. *IEEE Access* **2020**, *8*, 141932–141945. [CrossRef]
33. Kundur, P.; Balu, N.; Lauby, M. *Power System Stability and Control*; Discussion Paper Series; McGraw-Hill Education: New York, NY, USA, 1994. [CrossRef]
34. Rakhshani, E.; Remon, D.; Mir Cantarellas, A.; Rodriguez, P. Analysis of derivative control based virtual inertia in multi-area high-voltage direct current interconnected power systems. *Transm. Distrib. IET Gener.* **2016**, *10*, 1458–1469. [CrossRef]
35. Dolk, V.S.; Tesi, P.; De Persis, C.; Heemels, W.P.M.H. Event-Triggered Control Systems under Denial-of-Service Attacks. *IEEE Trans. Control Netw. Syst.* **2017**, *4*, 93–105. [CrossRef]
36. Amin, S.; Cárdenas, A.A.; Sastry, S.S. Safe and secure networked control systems under denial-of-service attacks. In *International Workshop on Hybrid Systems: Computation and Control*; Springer: New York, NY, USA, 2009; pp. 31–45.
37. Pan, K.; Teixeira, A.; Cvetkovic, M.; Palensky, P. Cyber Risk Analysis of Combined Data Attacks Against Power System State Estimation. *IEEE Trans. Smart Grid* **2018**, *10*, 3044–3056. [CrossRef]

38. Ogata, K. *Discrete-time Control Systems*, 2nd ed.; Prentice-Hall, Inc.: Upper Saddle River, NJ, USA, 1995.
39. Chen, C.; Zhang, K.; Yuan, K.; Zhu, L.; Qian, M. Novel Detection Scheme Design Considering Cyber Attacks on Load Frequency Control. *IEEE Trans. Ind. Inform.* **2018**, *14*, 1932–1941. [CrossRef]
40. Lin, H.; Antsaklis, P.J. Stability and Stabilizability of Switched Linear Systems: A Survey of Recent Results. *IEEE Trans. Autom. Control* **2009**, *54*, 308–322. [CrossRef]
41. Teixeira, A.; Sou, K.C.; Sandberg, H.; Johansson, K.H. Secure control systems: A quantitative risk management approach. *IEEE Control Syst.* **2015**, *35*, 24–45. [CrossRef]
42. Teixeira, A.; Shames, I.; Sandberg, H.; Johansson, K.H. A secure control framework for resource-limited adversaries. *Automatica* **2015**, *51*, 135–148. [CrossRef]