On the Impact of Cyber Attacks on Data Integrity in Storage-Based Transient Stability Control

Abdallah Farraj, *Member, IEEE*, Eman Hammad, *Student Member, IEEE*, and Deepa Kundur, *Fellow, IEEE*

***Abstract*—Security of smart power systems is a sound concern as more cyber elements are added to the power grid. In this paper, we focus on cyber attacks that target data integrity in smart grid systems. We specifically investigate the impact of false data injection (FDI) attacks on distributed transient stability control schemes. As an example, we focus on the parametric feedback linearization (PFL) controller, and we derive closed-form expressions for the errors in rotors' speed and angle as a result of cyber attacks on data integrity. Furthermore, we investigate adaptive control strategies to eliminate or minimize the impact of FDI attacks on system dynamics. The IEEE 68-bus test power system is used to numerically evaluate the impact of example attacks and to draw valuable insights.**

***Index Terms*—Cyber attacks, distributed control, energy storage systems (ESSs), false data injection (FDI) attacks, feedback linearization control, power system dynamics, transient stability.**

I. Introduction

THE ongoing integration between traditional power system elements, renewable energy sources, and cyber systems promotes improving efficiency of smart power systems [1]–[6]. In addition, energy storage systems (ESSs) can be used to store and inject power in the power system in a controlled manner; ESSs are getting more attention as they can help facilitate the integration of renewable energy sources into the smart grid. Portrayed as a cyber-physical system, the cyber elements of a smart grid system include communication networks, sensory, and control technologies. In this paradigm, sensor readings that capture the state of the power system are transferred to the control agents through the communication network.

As smart grid elements are taking shape, reliability, and security of its cyber components are of sound concern. Specifically, hacking and cyber attacks on the power grid are more probable due to the introduction of and dependence on cyber elements. Cyber attacks can target data delivery, integrity, or confidentiality. Depending on the affected smart grid application, cyber attacks can cause financial loses to the stakeholders (for example, through theft), instability of the power grid (through disruptive attacks), or lack of access to accurate time-critical data for the control agents. Power system stability describes the ability of the power system to regain a state of operating equilibrium after being subjected to a physical disturbance [7]. Specifically, transient stability depends on the ability of the synchronous generators in the power system to maintain or restore a balance between their electrical and mechanical torques after the occurrence of a large disturbance.

Recent work in [8]–[12] propose ESS-based distributed control schemes for transient stability applications. In order to change the dynamics of the power system and achieve transient stability, a control agent utilizes sensor measurements that are received through a communication network to actuate the distributed ESSs to inject and/or absorb power from the power grid. As ESS-based control for transient stability is evolving, we assert that security should be part of controller design (and, hence, not an afterthought) and should not hinder usability. As such, we focus in this paper on cyber attacks that target data integrity for transient stability control applications. Often termed false data injection (FDI) attacks, such adverse actions manipulate the structure of the data delivery system to insert fabricated data in the data stream while bypassing bad data detection filters [13]–[17].

Specifically, we study the impact of FDI attacks on transient stability control schemes, where the data under attack is used by the control agent to actuate the distributed ESSs during transient instability periods. Recent works that address similar problems appear in [18]–[20] where the impact of FDI attacks on transient stability control is modeled as a noise term. As an example control scheme, we consider the parametric feedback linearization (PFL) control proposed in [12]. PFL control is a state-of-the-art distributed transient stability control; a PFL controller has a simple design and is flexible through a tuneable design parameter. We implement a general FDI attack that targets the controller's communication network. Further, we quantify the error introduced by the FDI attack on rotor dynamics during transient instability periods. In addition, utilizing the PFL design parameter, we investigate reactive control strategies to reduce or eliminate the impact of the cyber attacks. Finally, we numerically investigate the impact of example FDI attacks on power system dynamics.

Manuscript received January 31, 2017; revised April 21, 2017; accepted June 21, 2017. Date of publication June 28, 2017; date of current version December 1, 2017. Paper no. TII-17-0184. *(Corresponding author: Abdallah Farraj.)*

The authors are with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: abdallah@ece.utoronto.ca; ehammad@ece.utoronto.ca; dkundur@ece.utoronto.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2017.2720679

Contributions of this work include providing a framework for FDI attacks on storage-based transient stability control, deriving closed-form expressions for the impact of FDI attacks on rotor dynamics, and devising reactive control strategies to counter the effect of the FDI attacks. This is a timely problem, and to the best knowledge of the authors, the problem of FDI attacks on storage-based transient stability control has not been addressed in such detail yet.

The rest of this paper is organized as follows. The problem setting is presented in Section II. The impact of FDI attacks on transient stability control is detailed in Sections III and IV. Section V presents adaptive control strategies against FDI attacks. Section VI numerically investigates the impact of FDI attacks on PFL control scheme. Finally, conclusions are shown in Section VII.

II. Background and Problem Formulation

In this section, we present the problem setting, explain the distributed control paradigm, and introduce FDI attacks.

A. Transient Dynamics

We model the smart grid as a multiagent cyber-physical controlled system. We assume that a smart grid is comprised of cyber-physical agents where each of these agents includes a synchronous generator, a sensor that provides local measurements of the generator rotor angle and speed, a distributed control agent that processes sensor data from system agents, and a fast-acting ESS that can inject or absorb real power in the system depending on the value of the control signal. In addition, a communication network connects the different cyber-physical agents of the smart power system. Depending on the structure of the control scheme and the system state, the control agent affects the dynamics of the power system in this model by actuating the associated ESS.

Let the number of generators in the power system be denoted N. For synchronous generator i, where $i \in \{1, \ldots, N\}$, the parameters of the generator are described by using Table I. The two-axis subtransient machine model is widely used to capture the dynamics of synchronous generators during transient periods. The electrical dynamics of generator i's stator are represented as [21], [22]

$$\dot{E}'_{qi} = \frac{1}{T'_{di}}\left(-E'_{qi} - (X_{di} - X'_{di})I_{di} + E_{\mathrm{fi}}\right) \tag{1a}$$

$$\dot{E}'_{di} = \frac{1}{T'_{qi}}\left(-E'_{di} + (X_{qi} - X'_{qi})I_{qi}\right) \tag{1b}$$

$$E'_{qi} = V_{qi} + R_{\mathrm{ai}}I_{qi} + X'_{di}I_{di} \tag{1c}$$

$$E'_{di} = V_{di} + R_{\mathrm{ai}}I_{di} - X'_{qi}I_{qi} \tag{1d}$$

where $\dot{E}'_{qi}$ and $\dot{E}'_{di}$ denote the time derivative of E'_{qi} and E'_{di}, respectively. Further, the rotor dynamics can be described in this model by using [21]

$$\dot{\delta}_i = \Omega_s(\omega_i - \omega_s) \tag{2a}$$

$$\dot{\omega}_i = \frac{\omega_s}{2H_i}\left(T_{Mi} - T_{Ei} - D_i(\omega_i - \omega_s)\right) \tag{2b}$$

TABLE I
Machine Parameter Description

Parameter	Description
δ	Rotor angle
ω	Rotor angular speed
ω_s	Synchronous speed
D	Damping coefficient
E'_d	d-axis transient electromotive force (emf)
E'_q	q-axis transient emf
E_f	Field voltage
H	Machine inertia constant
I_d	d-axis component of stator current
I_q	q-axis component of stator current
R_a	Armature resistance
X_d	d-axis synchronous reactance
X_q	q-axis synchronous reactance
X'_d	d-axis transient reactance
X'_q	q-axis transient reactance
T'_d	d-axis transient open loop time constant
T'_q	q-axis transient open loop time constant
T_E	Electrical torque
T_M	Mechanical torque
V_d	d-axis terminal voltage
V_q	q-axis terminal voltage

where $\dot{\delta}_i$ and $\dot{\omega}_i$ are the time derivative of δ_i and ω_i, respectively, and Ω_s denotes the system frequency (typically equal to $60 \cdot 2\pi$ or $50 \cdot 2\pi$ depending the geographical area). For synchronous generator i, the field voltage is controlled by the excitation system, the mechanical torque is controlled by the associated speed governor, and the electrical torque is calculated according to [21]

$$T_{Ei} = E'_{di}I_{di} + E'_{qi}I_{qi} + (X'_{qi} - X'_{di})I_{di}I_{qi}. \tag{3}$$

This torque relation provides a nonlinear term in (2b). Let P_{Mi} and P_{Ei} be the mechanical and electrical powers of generator i, respectively, where $P_{Ei} = T_{Ei}$ and $P_{Mi} = T_{Mi}$ when using per units. Further, let E_i denote the internal voltage of generator i, then P_{Ei} can be expressed as [23]

$$P_{Ei} = \sum_{k=1}^{N} |E_i||E_k|\left(G_{ik}\cos(\delta_i - \delta_k) + B_{ik}\sin(\delta_i - \delta_k)\right) \tag{4}$$

where $G_{ik} = G_{ki}$ and $B_{ik} = B_{ki}$ are the Kron-reduced equivalent conductance and susceptance between generators i and k, respectively.

The swing equation describes the electromechanical dynamics of the rotor of the synchronous generator and it traditionally refers to the model in (2a) and (2b). The swing equation is useful when studying the behavior of synchronous generators when the power system is subjected to a large disturbance (i.e., during transient instability periods). Denote $P_{Ai} = P_{Mi} - P_{Ei}$, $\forall i \in \{1, \ldots, N\}$, as the accelerating power of generator i. During normal operations of the power system, the value of the accelerating power typically equals to 0. However, when a major disturbance occurs in the power system, the accelerating power of some synchronous generators deviates from 0. As a result, the speed of the rotor of such generators may increase when the accelerating power is positive, and vice versa.

However, a large deviation in rotor speed might damage the synchronous machine and consequently force the generator to be disconnected from the power system.

In this paper, a synchronous generator is said to be stabilized if its rotor speed is driven back to an acceptable range and when the differences between the rotor angle of the different generators are below a predefined threshold. In this context, the goal of a transient stability control is to regain the balance between the mechanical and electrical torques of the synchronous generators in order to stabilize the power system. In other words, the actions of the distributed control agents should restore the synchronism between the system generators and drive back the rotor speeds to within an acceptable range.

B. Distributed Control Paradigm

The presence of a communication network in smart grid systems enables the periodic exchange of sensor readings between the different cyber-physical agents. The sensors take periodic readings of the system state parameters (the rotor speeds and angles in this case) and transmit such measurements to the distributed controllers in the cyber-physical agents through the communication network. Based on the received measurements and their attributes (for example, delay, amount of noise, and reliability of measurements), the control agents calculate control signals to actuate the local ESS at the associated synchronous generator's bus. Thus, by injecting or absorbing calculated amounts of power through the ESSs, the control agents can affect the dynamics of the power system. The ESS is controlled in [8] as a function of the level of frequency deviation in the power system, and the mechanical power of the synchronous generators is actuated in [24] to regulate the rotor speed. Optimal control theory is used in [3] and [25] to calculate the control signal, and nonlinear control schemes are used in [26]–[29].

Let u_i denotes the output of the controlled ESS at the bus of generator i, and let $\theta_i = \omega_i - \omega_s$ be the rotor speed of generator i relative to the synchronous speed in per units. Then, incorporating the control action at time t modifies the swing equation of generator i to

$$\begin{aligned} \dot{\delta}_i(t) &= \Omega_s \theta_i(t) \\ \dot{\omega}_i(t) &= \frac{\omega_s}{2H_i}\left(P_{Ai}(t) - D_i\theta_i(t) + u_i(t)\right). \end{aligned} \tag{5}$$

Here, ω_s, P_{Ai}, θ_i, and u_i are in per units. Also, let $\bar{\delta}_i$ and $\bar{\theta}_i$ denote the steady-state values of δ_i and θ_i, respectively, where

$$\begin{aligned} \bar{\delta}_i &= \lim_{t\to\infty} \delta_i(t) \\ \bar{\theta}_i &= \lim_{t\to\infty} \theta_i(t). \end{aligned} \tag{6}$$

Based on the feedback linearization control theory, a distributed PFL control scheme is proposed in [12] for transient stability applications. The PFL control agent actuates the associated ESS of generator i at time t according to [12]

$$u_i(t) = -P_{Ai}(t) - \alpha_i\theta_i(t) \tag{7}$$

where $\alpha_i \geq 0$ is a design parameter. Through adjusting the value of α_i, the PFL control actuation reshapes the dynamics of the controlled power system to resemble the dynamics of a series of stable and decoupled linear control systems with tunable eigenvalues.

C. FDI Threats to Smart Power Grids

Securing smart power systems against cyber attacks is a paramount challenge for system operators as increased implementations of smart grid applications bring new challenges and vulnerabilities. It is observed that exploiting smart grid data delivery systems can lead to potentially damaging cyber and physical attacks [28]. Common classes of cyber and physical attacks on smart grid systems include interference, FDI, denial of service, and switching attacks [30]–[35]. An adversary exploits the configuration of the cyber and physical elements of the power system in an FDI attack in order to introduce an error into certain system state variables. The adversary designs the FDI attack vector such that it bypasses any existing schemes for bad measurement detection. By launching an FDI attack, the adversary may disrupt the normal energy distribution of power system, affect the estimation of the state variables, or achieve financial gains.

FDI attacks modify information that is generated by supervisory control and data acquisition (SCADA) systems. FDI attacks are distinct from naturally-occurring errors because the modified data is altered in an intelligent way such that it still fulfills, for example, physical laws such that it is not detected by typical bad data detection schemes [36]. Bad data detection represents a class of signal processing techniques that aim to identify anomalies in power system telemetry readings such that they can be rejected during computation of the power system state. Hence, if FDI data goes undetected by bad data detection filters, incorrect state estimation may result enabling incorrect actions, for example, by the power system operator. Even if an FDI attack is detected, a system operator may not be able to estimate the true state; hence, part of the grid remains unobservable which enhances the vulnerability of the power system to further attacks [36].

To launch a successful FDI attack, the modified data should appear "correct" in order to pass through bad data detection filters. To achieve this, the adversary requires knowledge of the topology of the power system and must, in some cases, conduct the process of state estimation [36]. Simplified approaches to conduct state estimation can be used through dc power flow approximation [37].

1) DC State Estimation: Consider the state estimation problem in power systems; let $\boldsymbol{x}$, $\boldsymbol{z}$, and $\boldsymbol{n}$ represent the true states of the system, sensor measurements received at the estimator, and errors in measurements, respectively. By using the dc power flow approximation, the relation between these variables is governed by the work in [38] and [39]

$$\boldsymbol{z} = \boldsymbol{H}_s\boldsymbol{x} + \boldsymbol{n} \tag{8}$$

where $\boldsymbol{H}_s$ is a Jacobian matrix, and $\boldsymbol{H}_s\boldsymbol{x}$ links sensor measurements to system states. The goal in state estimation is to find an estimate $\hat{\boldsymbol{x}}$ that is the best fit of the measurement vector $\boldsymbol{z}$. Several approaches can be utilized to find $\hat{\boldsymbol{x}}$, including

maximum likelihood criterion, weighted least-square criterion, and minimum variance criterion [39]. Specifically, when $\boldsymbol{n}$ has a Gaussian distribution with zero mean, then $\hat{\boldsymbol{x}}$ is found as [39]

$$\hat{\boldsymbol{x}} = (\boldsymbol{H}_s \boldsymbol{W}_s \boldsymbol{H}_s)^{-1} \boldsymbol{H}_s^T \boldsymbol{W}_s \boldsymbol{z} \tag{9}$$

where $\boldsymbol{W}_s$ is a diagonal matrix whose elements can be the reciprocals of the measurement errors variance.

2) Bad Measurement Detection: The measurements used in state estimation might be inaccurate because of device errors and failures, malicious actions by adversaries, or other noise signals. Inaccurate measurements can affect the state estimation process; thus, bad measurement detection schemes can be helpful in detecting, identifying, or correcting corrupted measurements [17], [31], [38], [40], [41]. A common approach to detect bad measurements is to look at the measurement residue $||\boldsymbol{z} - \boldsymbol{H}_s \hat{\boldsymbol{x}}||$. This metric shows the difference between received sensor measurements and estimated measurements. Then, $||\boldsymbol{z} - \boldsymbol{H}_s \hat{\boldsymbol{x}}||$ is compared to a threshold ε. If $||\boldsymbol{z} - \boldsymbol{H}_s \hat{\boldsymbol{x}}|| > \varepsilon$, then the bad measurement detection scheme declares that at least one faulty (or bad) measurement is present in the received measurement $\boldsymbol{z}$.

3) FDI Attack Vector: In stealthy FDI attacks against state estimation, the adversary manipulates the sensor readings in order to cause arbitrary errors in the estimated values of the system state (i.e., $\hat{\boldsymbol{x}}$) without being detected by the bad data detection scheme. For example, let $\hat{\boldsymbol{x}}_a$ denotes the estimate of $\boldsymbol{x}$ when there is an FDI attack, where $\hat{\boldsymbol{x}}_a = \hat{\boldsymbol{x}} + \boldsymbol{e}_a$ and $\boldsymbol{e}_a$ is the estimation error introduced by the adversary. Let the received measurement vector during the attack be denoted as $\boldsymbol{z}_a$. If $\boldsymbol{z}_a = \boldsymbol{z} + \boldsymbol{H}_s \boldsymbol{e}_a$, where an error of $\boldsymbol{H}_s \boldsymbol{e}_a$ is injected by the adversary, then the residue of the corrupted data appears as [31]

$$\begin{aligned} ||\boldsymbol{z}_a - \boldsymbol{H}_s \hat{\boldsymbol{x}}_a|| &= ||\boldsymbol{z} + \boldsymbol{H}_s \boldsymbol{e}_a - \boldsymbol{H}_s (\hat{\boldsymbol{x}} + \boldsymbol{e}_a)|| \\ &= ||\boldsymbol{z} - \boldsymbol{H}_s \hat{\boldsymbol{x}}||. \end{aligned} \tag{10}$$

As this residue is the same with the case of no FDI attack, an adversary injecting an attack vector of $\boldsymbol{z}_a = \boldsymbol{z} + \boldsymbol{H}_s \boldsymbol{e}_a$ can bypass the bad data detection scheme.

D. FDI Threat Model

Our threat model follows standard assumptions employed in the FDI attacks literature [31], [38], [41]. The threat model assumes that the adversary has:

1) eavesdropping capabilities on the sensor readings;
2) knowledge about power system topology and model;
3) sufficient computational power to compute system state variables; and
4) capability to inject fabricated measurements in the communication network.

The adversary conducts the cyber attack, while the power system undergoes transient stability analysis and control, which may coincide with a major disturbance.

One goal of the adversary is to conduct a stealthy FDI attack in which data modification goes undetected. Further, slowing down the stabilization process (by invoking a less aggressive control) is another objective of the attacker if the modified data is detected by the control agent. The attack process is divided in two steps: reconnaissance and execution. In the reconnaissance stage, the adversary designs an attack vector $\boldsymbol{z}_a$ to bypass the bad data detection schemes as shown in (10). In the execution stage, the adversary identifies the SCADA environment, locates control and monitoring devices, accesses the measurements $\boldsymbol{z}$, and injects the malicious data $\boldsymbol{z}_a$ instead of $\boldsymbol{z}$ [41]. The threat model can be justified following an example in [42], where attackers use authentication and restart communications option vulnerabilities in Modbus/TCP protocols to conduct IP spoofing and denial-of-service attacks in order to inject malicious data and change the target addresses of SCADA traffic.

E. Problem Formulation

In this paper, we study the impact of FDI attacks on storage-based transient stability control schemes. As an example, we focus on PFL control proposed in [12]. The objectives of this paper include the following:

1) providing a general framework for FDI attacks on storage-based transient stability control;
2) quantifying the error introduced by FDI attack on rotor dynamics;
3) devising reactive control strategies to counter the effect of the FDI attacks; and
4) investigating the impact of example attacks on power system dynamics and drawing conclusions.

III. FDI Attacks on Transient Stability Control

In this section, we investigate the effect of a general FDI attack on transient stability control. Specifically, we consider the PFL control in (7) as an example, and we derive expressions for the deviation in rotor speed and angle due to the attack. We assume the FDI attack bypasses the existing bad measurement detection filter; thus, the control agent "does not know" that the received data is corrupt with intentional errors.

A. FDI Attack Representation

Assume, a general representation for FDI attacks on the system state parameters δ, θ, P_A. Because of the false data introduced by the adversary, the received measurements at the controller of cyber-physical agent i (termed as $\tilde{\delta}_i, \tilde{\theta}_i, \tilde{P}_{Ai}$) can be represented as

$$\begin{aligned} \tilde{\theta}_i(t) &= \theta_i(t) + f_{\theta i}(t) \\ \tilde{P}_{Ai}(t) &= P_{Ai}(t) + f_{Pi}(t) \\ \tilde{\delta}_i(t) &= \delta_i(t) + f_{\delta i}(t) \end{aligned} \tag{11}$$

where a general FDI attack signal is expressed using

$$\begin{aligned} f_{\theta i}(t) &= \epsilon_{i1} \theta_i(t) + \kappa_{i1}(t) + \mu_{i1} \\ f_{Pi}(t) &= \epsilon_{i2} P_{Ai}(t) + \kappa_{i2}(t) + \mu_{i2} \\ f_{\delta i}(t) &= \epsilon_{i3} \delta_i(t) + \kappa_{i3}(t) + \mu_{i3}. \end{aligned} \tag{12}$$

In this context, the ϵ_i term introduces an amplification component, κ_i represents a general time-varying additive signal,

and μ_i denotes a constant bias in the received system state variables. The model in (11) provides a general representation that can capture different types of FDI attacks. Following (4), the rotor angle values determine P_{Ei}. Thus, an attack on rotor angle measurements can indirectly affect the value of $P_{Ai}(t)$. Since the PFL controller utilizes the values of $P_{Ai}(t)$ and $\theta_i(t)$ to calculate $u_i(t)$, the following discussion will focus on FDI attacks on rotor speed and accelerating power; however, an FDI attack on δ_i implicitly leads to an attack on P_{Ai} as demonstrated by (4).

Since it is assumed that the FDI attack vector bypasses the bad measurement detection scheme, the PFL controller will, unknowingly, utilize the received (and corrupted) measurements to calculate the control action. Using the corrupt received measurements in $\tilde{\theta}_i$ and $\tilde{P}_{Ai}$, the PFL control signal at time t becomes $u_i(t) = -\tilde{P}_{Ai}(t) - \alpha_i\tilde{\theta}_i(t)$. Given the values of the control signal, $\tilde{P}_{Ai}$, and $\tilde{\theta}_i$, the rotor dynamics of generator i, thus, becomes

$$\begin{aligned}\dot{\theta}_i(t) =& -\frac{D_i+\alpha_i}{2H_i/\omega_s}\theta_i(t) - \frac{\alpha_i\epsilon_{i1}}{2H_i/\omega_s}\theta_i(t) - \frac{\alpha_i\mu_{i1}+\mu_{i2}}{2H_i/\omega_s} \\ & - \frac{\alpha_i\kappa_{i1}(t)+\kappa_{i2}(t)+\epsilon_{i2}P_{Ai}(t)}{2H_i/\omega_s} \\ =:& \; a_i\theta_i(t) + b_i\theta_i(t) + c_i + g_i(t) \end{aligned} \tag{13}$$

where

$$\begin{aligned} a_i =& -(D_i+\alpha_i)/(2H_i/\omega_s) \\ b_i =& -(\alpha_i\epsilon_{i1})/(2H_i/\omega_s) \\ c_i =& -(\alpha_i\mu_{i1}+\mu_{i2})/(2H_i/\omega_s) \\ g_i(t) =& -(\alpha_i\kappa_{i1}(t)+\kappa_{i2}(t)+\epsilon_{i2}P_{Ai}(t))/(2H_i/\omega_s). \end{aligned}$$

In this formulation, $a_i\theta_i(t)$ represents the dynamics of the rotor when there is no FDI attack, and the impact of the FDI attack on rotor speed appears in $b_i\theta_i(t) + c_i + g_i(t)$.

B. Impact on Rotor Speed and Angle

Building on the results in (13), the rotor speed dynamics at time t becomes $\dot{\theta}_i(t) = (a_i+b_i)\theta_i(t) + c_i + g_i(t)$. Solving this differential equation leads to

$$\begin{aligned}\theta_i(t) =& \; \theta_i(t_0)\exp((a_i+b_i)t) \\ & + \frac{c_i}{a_i+b_i}\left(\exp((a_i+b_i)t) - 1\right) \\ & + \int_{t_0}^{t} g_i(\tau)\exp((a_i+b_i)(t-\tau))\,\mathrm{d}\tau \end{aligned} \tag{14}$$

where $g_i(\tau)$ is defined in (13), t_0 is the starting time of the controller, and $\theta_i(t_0)$ is the rotor relative speed at t_0. Then, applying the values of a_i, b_i, and c_i from (13) reveals the value of the rotor relative speed as a function of time as shown in (16). In addition, let $\delta_i(t_0)$ denotes the rotor angle at t_0. Then, using $\dot{\delta}_i(t) = \Omega_s\theta_i(t)$ and (14) to study the impact of FDI attacks on the rotor angle of generator i, we find that the rotor angle can be expressed as a function of time as

$$\begin{aligned}\delta_i(t) =& \; \delta_i(t_0) - \frac{\theta_i(t_0)(a_i+b_i)+c_i}{(a_i+b_i)^2}\Omega_s - \frac{c_i}{a_i+b_i}\Omega_s t \\ & + \frac{\theta_i(t_0)(a_i+b_i)+c_i}{(a_i+b_i)^2}\Omega_s\exp((a_i+b_i)t) \\ & + \frac{1}{a_i+b_i}\Omega_s\int_{t_0}^{t} g_i(\tau)\left(\exp((a_i+b_i)(t-\tau)) - 1\right)\mathrm{d}\tau. \end{aligned} \tag{15}$$

Similarly, expanding this result using the values of a_i, b_i, and c_i leads to the expression of $\delta_i(t)$ in (17).

$$\begin{aligned}\theta_i(t) =& \; \theta_i(t_0)\exp\left(-\frac{D_i+\alpha_i+\alpha_i\epsilon_{i1}}{2H_i/\omega_s}t\right) + \frac{\alpha_i\mu_{i1}+\mu_{i2}}{D_i+\alpha_i+\alpha_i\epsilon_{i1}} \\ & \times \left(\exp\left(-\frac{D_i+\alpha_i+\alpha_i\epsilon_{i1}}{2H_i/\omega_s}t\right) - 1\right) \\ & + \int_{t_0}^{t} g_i(\tau)\exp\left(-\frac{D_i+\alpha_i+\alpha_i\epsilon_{i1}}{2H_i/\omega_s}(t-\tau)\right)\mathrm{d}\tau. \end{aligned} \tag{16}$$

$$\begin{aligned}\delta_i(t) =& \; \delta_i(t_0) - \frac{\alpha_i\mu_{i1}+\mu_{i2}}{D_i+\alpha_i+\alpha_i\epsilon_{i1}}\Omega_s t - \frac{\Omega_s 2H_i/\omega_s}{D_i+\alpha_i+\alpha_i\epsilon_{i1}} \\ & \times \int_{t_0}^{t} g_i(\tau)\left(\exp\left(-\frac{D_i+\alpha_i+\alpha_i\epsilon_{i1}}{2H_i/\omega_s}(t-\tau)\right) - 1\right)\mathrm{d}\tau \\ & + \frac{\Omega_s 2H_i/\omega_s}{(D_i+\alpha_i+\alpha_i\epsilon_{i1})^2}\left(\theta_i(t_0)(D_i+\alpha_i+\alpha_i\epsilon_{i1})\right. \\ & \left. +\alpha_i\mu_{i1}+\mu_{i2}\right)\left(1-\exp\left(-\frac{D_i+\alpha_i+\alpha_i\epsilon_{i1}}{2H_i/\omega_s}t\right)\right). \end{aligned} \tag{17}$$

C. Rotor Speed and Angle When There is no FDI Attack

This is the case of normal operation where $f_{\theta i}(t) = 0$ and $f_{Pi}(t) = 0$. From (16), the rotor relative speed will appear as

$$\theta_i(t) = \theta_i(t_0)\exp\left(-\frac{D_i+\alpha_i}{2H_i/\omega_s}t\right). \tag{18}$$

In addition, following (17), the rotor angle during the normal control operation becomes

$$\delta_i(t) = \delta_i(t_0) + \frac{\Omega_s 2H_i/\omega_s}{D_i+\alpha_i}\theta_i(t_0)\left(1-\exp\left(-\frac{D_i+\alpha_i}{2H_i/\omega_s}t\right)\right). \tag{19}$$

It is to be reminded that $\frac{D_i+\alpha_i}{2H_i/\omega_s} > 0$. Thus, following the results in (18) and (19), the steady-state values of the rotor speed and angle can be expressed as

$$\bar{\theta}_i = 0 \tag{20a}$$

$$\bar{\delta}_i = \delta_i(t_0) + \frac{\Omega_s 2H_i/\omega_s}{D_i+\alpha_i}\theta_i(t_0). \tag{20b}$$

Consequently, the rotor speed of generator i will exponentially converge to the synchronous speed (i.e., $\lim_{t\to\infty}\omega_i(t) = \omega_s$), and that means the synchronous generator is stabilized due to the actions of the PFL controller.

IV. Study of Special Cases of FDI Attacks

In this section, we consider special cases of FDI attacks. We build on the results in (16) and (17) to simplify the expressions for the generator's rotor speed and angle in order to gain more direct insights.

A. Attack Targets Rotor Speed Variable

Consider the case of an FDI attack that only targets the rotor speed variable (θ_i); thus, $f_{Pi}(t) = 0$. The following is a detailed study of the impact of some specific attack vectors.

1) $\mu_{i1} \neq 0$, Other Terms are Zeros: This is the case of a constant bias in the rotor speed measurements. In this FDI attack, the rotor relative speed and angle, respectively, appear as

$$\begin{aligned}\theta_i(t) &= \theta_i(t_0)\exp\left(-\frac{D_i+\alpha_i}{2H_i/\omega_s}t\right)\\ &\quad+\frac{\alpha_i\mu_{i1}}{D_i+\alpha_i}\left(\exp\left(-\frac{D_i+\alpha_i}{2H_i/\omega_s}t\right)-1\right)\\ \delta_i(t) &= \delta_i(t_0)+\frac{\Omega_s 2H_i/\omega_s}{D_i+\alpha_i}\theta_i(t_0)\left(1-\exp\left(-\frac{D_i+\alpha_i}{2H_i/\omega_s}t\right)\right)\\ &\quad+\frac{\alpha_i\mu_{i1}}{D_i+\alpha_i}\Omega_s\left(\frac{2H_i/\omega_s}{D_i+\alpha_i}-t\right)\\ &\quad\times\left(1-\exp\left(-\frac{D_i+\alpha_i}{2H_i/\omega_s}t\right)\right).\end{aligned} \tag{21}$$

Then, the steady-state value of the rotor relative speed is shown as

$$\bar{\theta}_i = -\frac{\alpha_i\mu_{i1}}{D_i+\alpha_i}. \tag{22}$$

However, the magnitude of the rotor angle increases with time because of the $\frac{\alpha_i\mu_{i1}}{D_i+\alpha_i}\Omega_s t$ term.

2) $\epsilon_{i1} \neq 0$, Other Terms are Zeros: The FDI attack in this scenario provides only an amplification term of ϵ_{i1}, and thus $\tilde{\theta}_i(t) = \theta_i(t) + \epsilon_{i1}\theta_i(t)$. Consequently, this attack affects the rotor dynamics as

$$\begin{aligned}\theta_i(t) &= \theta_i(t_0)\exp\left(-\frac{D_i+\alpha_i+\alpha_i\epsilon_{i1}}{2H_i/\omega_s}t\right)\\ \delta_i(t) &= \delta_i(t_0)+\frac{\Omega_s 2H_i/\omega_s}{D_i+\alpha_i+\alpha_i\epsilon_{i1}}\theta_i(t_0)\\ &\quad-\frac{\Omega_s 2H_i/\omega_s}{D_i+\alpha_i+\alpha_i\epsilon_{i1}}\theta_i(t_0)\exp\left(-\frac{D_i+\alpha_i+\alpha_i\epsilon_{i1}}{2H_i/\omega_s}t\right).\end{aligned} \tag{23}$$

Consider the situation when $\epsilon_{i1} > -(D_i+\alpha_i)/\alpha_i$, and in this case $D_i+\alpha_i+\alpha_i\epsilon_{i1} > 0$. This leads the steady-state values to be expressed as

$$\begin{aligned}\bar{\theta}_i &= 0\\ \bar{\delta}_i &= \delta_i(t_0)+\frac{\Omega_s 2H_i/\omega_s}{D_i+\alpha_i+\alpha_i\epsilon_{i1}}\theta_i(t_0).\end{aligned} \tag{24}$$

However, if $\epsilon_{i1} < -(D_i+\alpha_i)/\alpha_i$, then the magnitude of the rotor speed and angle will increase with time, and so transient stability is lost.

3) $\mu_{i1} \neq 0, \epsilon_{i1} \neq 0$, Other Terms are Zeros: In this case, the FDI attack adds amplification and constant bias terms to the rotor speed variable. Hence, the rotor speed and angle of generator i are described as

$$\begin{aligned}\theta_i(t) &= -\frac{\alpha_i\mu_{i1}}{D_i+\alpha_i+\alpha_i\epsilon_{i1}}+\left(\theta_i(t_0)+\frac{\alpha_i\mu_{i1}}{D_i+\alpha_i+\alpha_i\epsilon_{i1}}\right)\\ &\quad\times\exp\left(-\frac{D_i+\alpha_i+\alpha_i\epsilon_{i1}}{2H_i/\omega_s}t\right)\\ \delta_i(t) &= \delta_i(t_0)-\frac{\alpha_i\mu_{i1}}{D_i+\alpha_i+\alpha_i\epsilon_{i1}}\Omega_s t\\ &\quad+\frac{\Omega_s 2H_i/\omega_s}{D_i+\alpha_i+\alpha_i\epsilon_{i1}}\left(\theta_i(t_0)+\frac{\alpha_i\mu_{i1}}{D_i+\alpha_i+\alpha_i\epsilon_{i1}}\right)\\ &\quad\times\left(1-\exp\left(-\frac{D_i+\alpha_i+\alpha_i\epsilon_{i1}}{2H_i/\omega_s}t\right)\right).\end{aligned} \tag{25}$$

The steady-state behavior depends on the value of the amplification term. Specifically, if $\epsilon_{i1} > -(D_i+\alpha_i)/\alpha_i$, then

$$\bar{\theta}_i = -\frac{\alpha_i\mu_{i1}}{D_i+\alpha_i+\alpha_i\epsilon_{i1}}. \tag{26}$$

However, the magnitude of the rotor angle increases with time. On the other hand, both rotor speed and angle diverge when $\epsilon_{i1} < -(D_i+\alpha_i)/\alpha_i$.

B. Attack Targets Accelerating Power Variable

Consider the case of an FDI attack that only targets P_{Ai} with a constant bias ($\mu_{i2} \neq 0$). This attack leads the rotor dynamics to be

$$\begin{aligned}\theta_i(t) &= \left(\theta_i(t_0)+\frac{\mu_{i2}}{D_i+\alpha_i}\right)\exp\left(-\frac{D_i+\alpha_i}{2H_i/\omega_s}t\right)-\frac{\mu_{i2}}{D_i+\alpha_i}\\ \delta_i(t) &= \delta_i(t_0)-\frac{\mu_{i2}}{D_i+\alpha_i}\Omega_s t+\frac{\Omega_s 2H_i/\omega_s}{D_i+\alpha_i}\\ &\quad\times\left(\theta_i(t_0)+\frac{\mu_{i2}}{D_i+\alpha_i}\right)\left(1-\exp\left(-\frac{D_i+\alpha_i}{2H_i/\omega_s}t\right)\right).\end{aligned} \tag{27}$$

In this case, the steady-state value of the rotor speed is shown as

$$\bar{\theta}_i = -\frac{\mu_{i2}}{D_i+\alpha_i}. \tag{28}$$

However, the magnitude of the rotor angle keeps increasing with time.

C. Attack Is Only a Constant Bias

In this scenario, the values of ϵ_i and $\kappa_i(t)$ are zeros. Thus, the FDI attack signal appears as

$$\begin{aligned}f_{\theta i}(t) &= \mu_{i1}\\ f_{Pi}(t) &= \mu_{i2}.\end{aligned}$$

This type of FDI attack changes the rotor speed into

$$\theta_i(t) = \theta_i(t_0)\exp\left(-\frac{D_i+\alpha_i}{2H_i/\omega_s}t\right) + \frac{\alpha_i\mu_{i1}+\mu_{i2}}{D_i+\alpha_i}\left(\exp\left(-\frac{D_i+\alpha_i}{2H_i/\omega_s}t\right)-1\right). \quad (29)$$

Here, the first component of $\theta_i(t)$ represents the normal behavior of the rotor speed when there is no attack [i.e., the term in (18)], and the second component represents the impact of the FDI attack on θ_i. Thus, $\frac{\alpha_i\mu_{i1}+\mu_{i2}}{D_i+\alpha_i}(\exp(-\frac{D_i+\alpha_i}{2H_i/\omega_s}t)-1)$ represents the deviation in rotor speed due to the FDI attack. From (29), the steady-state value of the rotor relative speed becomes

$$\bar{\theta}_i = -\frac{\alpha_i\mu_{i1}+\mu_{i2}}{D_i+\alpha_i}. \quad (30)$$

Likewise, the rotor angle expression during this type of FDI attack is expressed as

$$\delta_i(t) = \delta_i(t_0) - \frac{\alpha_i\mu_{i1}+\mu_{i2}}{D_i+\alpha_i}\Omega_s t + \frac{\Omega_s 2H_i/\omega_s}{(D_i+\alpha_i)^2}\left(1-\exp\left(-\frac{D_i+\alpha_i}{2H_i/\omega_s}t\right)\right) \times (\theta_i(t_0)(D_i+\alpha_i)+\alpha_i\mu_{i1}+\mu_{i2}). \quad (31)$$

It is observed here that this FDI attack causes a deviation of $\frac{\alpha_i\mu_{i1}+\mu_{i2}}{D_i+\alpha_i}[\frac{\Omega_s 2H_i/\omega_s}{D_i+\alpha_i}(1-\exp(-\frac{D_i+\alpha_i}{2H_i/\omega_s}t))-\Omega_s t]$ in the rotor angle. Also, if $\alpha_i\mu_{i1}+\mu_{i2}=0$, the steady-state rotor angle in this case is shown as

$$\bar{\delta}_i = \delta_i(t_0) + \frac{\Omega_s 2H_i/\omega_s}{D_i+\alpha_i}\theta_i(t_0). \quad (32)$$

Otherwise, the magnitude of rotor angle increases with time.

D. Attack is an Amplification and a Constant Bias

In this type of FDI attacks, the received measurements at agent i will appear as

$$\tilde{\theta}_i(t) = \theta_i(t) + \epsilon_{i1}\theta_i(t) + \mu_{i1}$$
$$\tilde{P}_{Ai}(t) = P_{Ai}(t) + \epsilon_{i2}P_{Ai}(t) + \mu_{i2}$$

which leads to $g_i(t) = -\frac{\epsilon_{i2}}{2H_i/\omega_s}P_{Ai}(t)$ in (13). Thus, the rotor speed and angle can be expressed as in (16) and (17), respectively, with $g(\tau)$ is replaced with $-\frac{\epsilon_{i2}}{2H_i/\omega_s}P_{Ai}(\tau)$. Since the expression of the accelerating power over time is typically very complicated and depends on many factors, the deviation in rotor speed and angle values can be numerically calculated during a simulation. To investigate the steady-state behavior under this type of attacks, define

$$\Delta_{\theta_i} = \lim_{t\to\infty}\int_{t_0}^{t} P_{Ai}(\tau)\exp\left(\frac{D_i+\alpha_i+\alpha_i\epsilon_{i1}}{2H_i/\omega_s}(\tau-t)\right)\mathrm{d}\tau$$
$$\Delta_{\delta_i} = \Delta_{\theta_i} - \lim_{t\to\infty}\int_{t_0}^{t} P_{Ai}(\tau)\,\mathrm{d}\tau \quad (33)$$

to denote a steady-state residue in the rotor speed and angle, respectively. Consequently, the steady-state value of the rotor relative speed becomes

$$\bar{\theta}_i = -\frac{\alpha_i\mu_{i1}+\mu_{i2}}{D_i+\alpha_i+\alpha_i\epsilon_{i1}} - \frac{\epsilon_{i2}}{2H_i/\omega_s}\Delta_{\theta_i} \quad (34)$$

for the case when $\epsilon_{i1} > -(D_i+\alpha_i)/\alpha_i$; otherwise, the rotor speed diverges over time. In addition, the steady-state value for the rotor angle can be shown as

$$\bar{\delta}_i = \delta_i(t_0) + \frac{\Omega_s 2H_i/\omega_s}{D_i+\alpha_i}\theta_i(t_0) + \frac{\Omega_s\epsilon_{i2}}{D_i+\alpha_i+\alpha_i\epsilon_{i1}}\Delta_{\delta_i} \quad (35)$$

for the case when $\alpha_i\mu_{i1}+\mu_{i2}=0$. However, when $\alpha_i\mu_{i1}+\mu_{i2}\neq 0$, the value of $|\delta_i(t)|$ increases with time.

V. Adaptive PFL Control Against FDI Attacks

In this section, we investigate some reactive strategies to reduce the impact of FDI attacks on PFL control. We revisit the findings of Section IV to get insights that help in devising a reaction mechanism to offset or minimize the steady-state error in rotor speed.

A. Observations

Let $\alpha_{\max} > 0$ denotes the maximum possible value of α_i. The following can be observed from the results of Section IV.

1) Time varying FDI components can result in steady-state residues in (16) and (17).
2) A high value of α_i can increase the value of g_i in (13) for a general FDI attack that includes time-varying signals.
3) Increasing the value of α_i can decrease the difference between the initial and final values of the rotor angle as shown in (20b).
4) A positive amplification value on rotor speed measurements does not affect the steady-state rotor speed values as shown in (24).
5) If $\alpha_{\max} \geq -\mu_{i2}/\mu_{i1} > 0$, then the PFL control design parameter can be selected as $\alpha_i = -\mu_{i2}/\mu_{i1}$ to eliminate the effect of the FDI attack on rotor speed and angle for the case when the FDI attack is a constant bias in (30) and (32). However, such approach does not remove the steady-state residue in (33) when the FDI attack includes also an amplification term.
6) Rotor angles divergence is possible if $\alpha_i\mu_{i1}+\mu_{i2}\neq 0$ in (32) and (35); thus, synchronism can possibly be lost.

Consider the steady-state values of θ_i (i.e., $\bar{\theta}_i$) under the different types of FDI attacks. The value of the PFL design parameter (α_i) can be varied in response to FDI attacks as the following.

1) Decreasing the value of α_i can reduce the magnitude of $\bar{\theta}_i$ in (22).
2) A smaller value of α_i can enhance the stability margin in (24) and, thus, the PFL controller can tolerate more FDI attacks; furthermore, a lower value of α_i reduces the impact of attacks on the rotor angle steady-state value.
3) Reducing α_i enhances the stability margin in (26) and can decrease the magnitude of $\bar{\theta}_i$.

4) The results in (30) show that $|\bar{\theta}_i| \to \mu_{i2}/D_i$ as $\alpha_i \to 0$, and $|\bar{\theta}_i| \to \mu_{i1}$ as $\alpha_i \to \infty$; thus, α_i can be made smaller if μ_{i2}/D_i lies in the acceptable range for θ_i.
5) It is observed in (30) and (32) that:
   a) if $\mu_{i1} = 0$, then increasing the value of α_i reduces the impact of FDI attacks;
   b) if $\mu_{i2} = 0$, then decreasing α_i reduces the impact of the attack; and
   c) if the control agent can precisely estimate the FDI attack parameters and if $-\mu_{i2}/\mu_{i1} > 0$, then a value of $\alpha_i = -\mu_{i2}/\mu_{i1} > 0$ eliminates the impact of the FDI attack on rotor dynamics.
6) A smaller value of α_i reduces the value of Δ_{θ_i} in (33); thus, decreasing the impact of $\epsilon_{i2}/(2H_i/\omega_s)\Delta_{\theta_i}$ term in the steady-state value of θ_i in (34).

The above results indicate that in some cases the PFL controller can eliminate the impact of the FDI attack. For example, if $\alpha_i = -\mu_{i2}/\mu_{i1}$ is a valid option (i.e., $\alpha_{\max} \geq -\mu_{i2}/\mu_{i1} > 0$), then the PFL controller can eliminate the error in rotor speed and angle if this ratio is estimated correctly.

B. Adaptive Control Reaction to FDI Attacks

Unless there is a strong bias in the accelerating power component, the PFL controller should generally decrease the value of its design parameter α_i in (7) as a result of the FDI attack. Specifically, decreasing α_i enhances the stability margin for the case of a multiplier FDI component, and it also reduces the magnitude of the steady-state rotor speed. However, the eigenvalues of the controlled system are directly affected by the value of α_i, and it usually takes longer times to stabilize the system generators with decreasing values of α_i. Hence, there is a trade-off between stability time and the PFL controller's ability to offset the impact of FDI attacks. Consequently, the value of the design parameter should be selected in a way to balance the aggressiveness of the PFL controller and its resilience to corrupt measurements.

C. Attack Estimation

In this section, we overview techniques to estimate the FDI attack parameters; we apply the method of moments to estimate the signal-to-noise ratio (SNR) of the corrupted measurements [43]. We focus on the rotor speed variable; however, similar analysis can be conducted for the accelerating power. In this context, θ_i, $\tilde{\theta}_i$, and $\hat{\theta}_i$ represent the transmitted, FDI-corrupted, and received measurements of rotor speed, respectively. The model in (11) presents the relation between θ_i and $\tilde{\theta}_i$; further, $\hat{\theta}_i(t) = \tilde{\theta}_i(t) + n_i(t)$, where $n_i(t)$ is a zero-mean Gaussian noise signal that corrupts the received measurements at time t at agent i's side.

1) Notation and Assumptions: $\mathbb{E}[\cdot]$ denotes the statistical expectation operator, which can be estimated for a specific variable by averaging its value over time. $\mathbb{E}[\theta_i(t)] = 0$ can be assumed from the properties of the rotor speed variable. Furthermore, $\mathbb{E}[\theta_i^2(t)]$, $\mathbb{E}[\hat{\theta}_i^2(t)]$, and $\mathbb{E}\left[n_i^2(t)\right]$ represent the power of the transmitted, received, and noise signals, respectively. The estimated value of $\mathbb{E}[\hat{\theta}_i^2(t)]$ (denoted $\hat{\mathbb{E}}[\hat{\theta}_i^2(t)]$) is calculated at the controller side by time-averaging the power of the received signal. In addition, $\theta_i(t)$ is assumed to be an ergodic signal; thus, the estimate to $\mathbb{E}\left[\theta_i^2(t)\right]$ (denoted $\hat{\mathbb{E}}\left[\theta_i^2(t)\right]$) can be calculated from the typical properties of the rotor speed signal. Further, $\theta_i(t)$ and $n_i(t)$ are assumed to be independent signals (i.e., $\mathbb{E}[\theta_i(t) \cdot n_i(t)] = \mathbb{E}[\theta_i(t)] \cdot \mathbb{E}[n_i(t)]$), which is valid given that $n_i(t)$ is a noise signal. The following cases are considered.

2) No FDI Attack: Consider the following model of the received signal

$$\hat{\theta}_i(t) = \theta_i(t) + n_i(t)\,. \tag{36}$$

Thus, $\mathbb{E}[\hat{\theta}_i(t)] = \mathbb{E}[\theta_i(t)] + \mathbb{E}[n_i(t)] = 0$ from the properties of the signals, and $\mathbb{E}[\hat{\theta}_i^2(t)] = \mathbb{E}[\theta_i^2(t)] + \mathbb{E}[n_i^2(t)]$ from the independence assumption. The actual SNR value is then expressed as

$$\text{SNR} = \frac{\mathbb{E}\left[\theta_i^2(t)\right]}{\mathbb{E}\left[n_i^2(t)\right]}\,. \tag{37}$$

The noise power is estimated at the controller side from $\hat{\mathbb{E}}[\hat{\theta}_i^2(t)] - \hat{\mathbb{E}}\left[\theta_i^2(t)\right]$. Hence, the estimated SNR value is calculated from

$$\hat{\mathbb{E}}\left[\theta_i^2(t)\right] / \left(\hat{\mathbb{E}}\left[\hat{\theta}_i^2(t)\right] - \hat{\mathbb{E}}\left[\theta_i^2(t)\right]\right).$$

Since $\hat{\mathbb{E}}[\hat{\theta}_i^2(t)]$ is measured by the controller by time-averaging the received signal power, and because $\hat{\mathbb{E}}\left[\theta_i^2(t)\right]$ is assumed to be known from the typical properties of the rotor speed signal, then the SNR can be estimated as shown above.

3) Constant-Bias FDI Attack: The received (corrupted) rotor speed variable appears as $\hat{\theta}_i(t) = \theta_i(t) + n_i(t) + \mu_{i1}$, where μ_{i1} is the constant bias that the adversary injects in the transmitted signal as in (11). Thus, $\mathbb{E}[\hat{\theta}_i(t)] = \mu_{i1}$, and $\mathbb{E}[\hat{\theta}_i^2(t)] = \mathbb{E}[\theta_i^2(t)] + \mathbb{E}[n_i^2(t)] + \mu_{i1}^2$. The constant bias is estimated in this attack from $\hat{\mathbb{E}}[\hat{\theta}_i(t)]$. The SNR of the received signal also appears as

$$\text{SNR} = \frac{\mathbb{E}\left[\theta_i^2(t)\right]}{\mathbb{E}\left[n_i^2(t)\right] + \mu_{i1}^2}\,. \tag{38}$$

However, $\hat{\mathbb{E}}[n_i^2(t)] + \mu_{i1}^2 = \hat{\mathbb{E}}[\hat{\theta}_i^2(t)] - \hat{\mathbb{E}}[\theta_i^2(t)]$. Consequently, the controller can estimate the SNR value from

$$\hat{\mathbb{E}}\left[\theta_i^2(t)\right] / \left(\hat{\mathbb{E}}\left[\hat{\theta}_i^2(t)\right] - \hat{\mathbb{E}}\left[\theta_i^2(t)\right]\right).$$

4) Additive FDI Attack: As shown in (11), the received signal is expressed for this attack as $\hat{\theta}_i(t) = \theta_i(t) + n_i(t) + \kappa_{i1}(t) + \mu_{i1}$. The attack signal is assumed to be independent of the transmitted signal $\theta_i(t)$, and that κ_{i1} has zero mean. The constant-bias term is estimated using the first moment as $\mathbb{E}[\hat{\theta}_i(t)] = \mu_{i1}$; calculating the second moment of the received signal also yields $\mathbb{E}[\hat{\theta}_i^2(t)] = \mathbb{E}[\theta_i^2(t)] + \mathbb{E}[n_i^2(t)] + \mathbb{E}[\kappa_{i1}^2(t)] + \mu_{i1}^2$. This attack leads to an SNR value of

$$\text{SNR} = \frac{\mathbb{E}\left[\theta_i^2(t)\right]}{\mathbb{E}\left[n_i^2(t)\right] + \mathbb{E}\left[\kappa_{i1}^2(t)\right] + \mu_{i1}^2}\,. \tag{39}$$

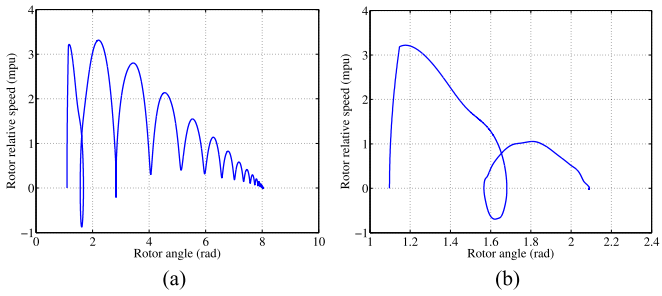

Fig. 1. Phase portrait when there is no FDI attack. (a) PFL control is not activated. (b) PFL control is activated.

Noting that $\hat{\mathbb{E}}[n_i^2(t)] + \hat{\mathbb{E}}[\kappa_{i1}^2(t)] + \mu_{i1}^2 = \hat{\mathbb{E}}[\hat{\theta}_i^2(t)] - \hat{\mathbb{E}}[\theta_i^2(t)]$, the SNR value is estimated as

$$\hat{\mathbb{E}}\left[\theta_i^2(t)\right] / \left(\hat{\mathbb{E}}\left[\hat{\theta}_i^2(t)\right] - \hat{\mathbb{E}}\left[\theta_i^2(t)\right]\right).$$

5) Multiplicative FDI Attack: This is a case where the FDI attack amplifies the transmitted signal by a gain factor. From (11), the received signal is $\hat{\theta}_i(t) = \theta_i(t) + n_i(t) + \epsilon_{i1}\theta_i(t) = (1+\epsilon_{i1})\theta_i(t) + n_i(t)$. Thus, $\mathbb{E}[\hat{\theta}_i(t)] = 0$, and the SNR value is calculated from

$$\text{SNR} = \frac{(1+\epsilon_{i1})^2 \mathbb{E}\left[\theta_i^2(t)\right]}{\mathbb{E}\left[n_i^2(t)\right]}. \tag{40}$$

To estimate the SNR for this type of attack, we calculate the second and fourth central moments of $\hat{\theta}_i(t)$ as

$$\begin{aligned}\mathbb{E}\left[\hat{\theta}_i^2(t)\right] &= (1+\epsilon_{i1})^2 \mathbb{E}\left[\theta_i^2(t)\right] + \mathbb{E}\left[n_i^2(t)\right] \\ \mathbb{E}\left[\hat{\theta}_i^4(t)\right] &= (1+\epsilon_{i1})^4 \mathbb{E}\left[\theta_i^4(t)\right] + \mathbb{E}\left[n_i^4(t)\right] \\ &\quad + 6(1+\epsilon_{i1})^2 \mathbb{E}\left[\theta_i^2(t)\right] \mathbb{E}\left[n_i^2(t)\right] \end{aligned} \tag{41}$$

where $\mathbb{E}[n_i^4(t)] = 3(\mathbb{E}[n_i^2(t)])^2$ for Gaussian noise [44]. The second and fourth moments of $\hat{\theta}_i(t)$ can be estimated from the received measurement. Solving for $\mathbb{E}[n_i^2(t)]$ and $(1+\epsilon_{i1})^2$ in (41) enables the controller to estimate the SNR value in (40).

VI. Numerical Results

In this section, we numerically evaluate the impact of example FDI attacks on the transient stability control. The IEEE New York–New England 68-bus test power system is used for numerical simulations. The test system has 16 synchronous generators and 68 buses. The parameters of this power system are extracted from [45], and the simulation environment follows the guidelines in [21]. More details about this test system can be found in [46]. As an illustrative example, consider a three-phase fault that occurs at Bus 30 at $t = 1$ s for 5 cycles (i.e., a fault duration of 83.3 ms), and the fault is cleared after that; thus, the test power system undergoes a major disturbance enabling transient stability studies. To facilitate achieving transient stability, PFL control is activated in all agents at $t = 2$ s, and the control design parameter $\alpha_i = 9D_i$ is used for Figs. 2 and 3. Further, the capacity of each ESS in the cyber-physical agents is limited to $5\%P_{Mi}$, which means that $\max_{t\geq 2}(|u_i(t)|) \leq 5\%P_{Mi}, \forall i \in \{1,\ldots,N\}$.

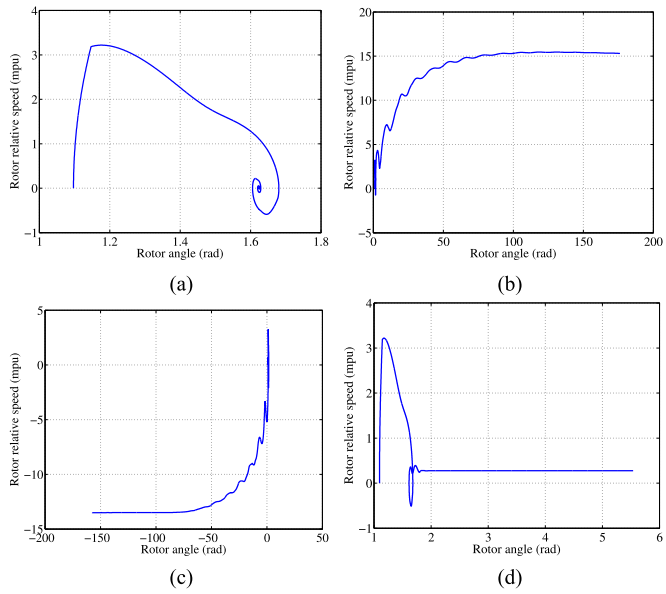

Fig. 2. Phase portrait for different FDI attacks on rotor speed variable (PFL control is activated). (a) $\epsilon_{i1} = 5$, others are zeros. (b) $\epsilon_{i1} = -1.5$, others are zeros. (c) $\mu_{i1} = 0.015$, others are zeros. (d) $\epsilon_{i1} = 2.5, \mu_{i1} = -0.001$, others are zeros.

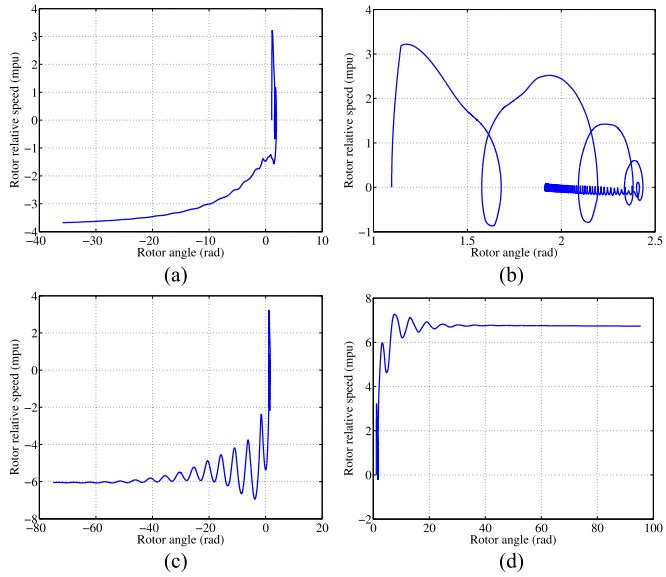

Fig. 3. Phase portrait for different FDI attacks on accelerating power variable (PFL control is activated). (a) $\epsilon_{i2} = 5$, others are zeros. (b) $\epsilon_{i2} = -5$, others are zeros. (c) $\mu_{i2} = 5$, others are zeros. (d) $\epsilon_{i2} = -1.5, \mu_{i2} = -5$, others are zeros.

We consider the phase portrait as a geometrical representation of the weighted trajectories of the system generators' rotor speed and angle.

A. Performance When There are no FDI Attacks

The phase portrait is shown in Fig. 1 for the case when there is no FDI attack. Fig. 1(a) displays the results when the PFL control is not activated, while the phase portrait when the PFL controller is activated is depicted in Fig. 1(b). It is shown that without distributed control, the power system trajectory keeps

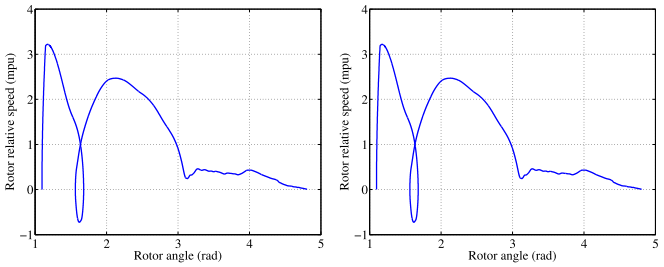

Fig. 4. Phase portrait showing PFL controller completely eliminating the impact of FDI attack. (a) No FDI attack: $\alpha_i = 10$. (b) FDI attack: $\alpha_i = 10$, $\mu_{i1} = -0.05$, $\mu_{i2} = 0.5$.

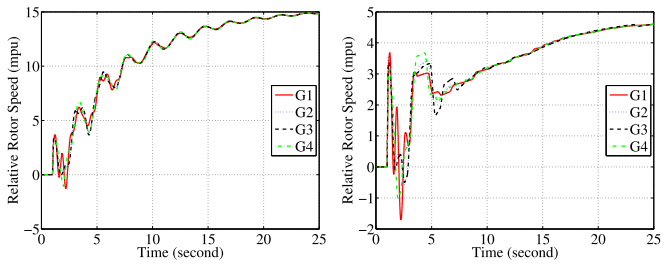

Fig. 5. Adaptive PFL control for $\mu_{i1} = -0.5$. (a) $\alpha_i = 9D_i$. (b) $\alpha_i = 0.01D_i$.

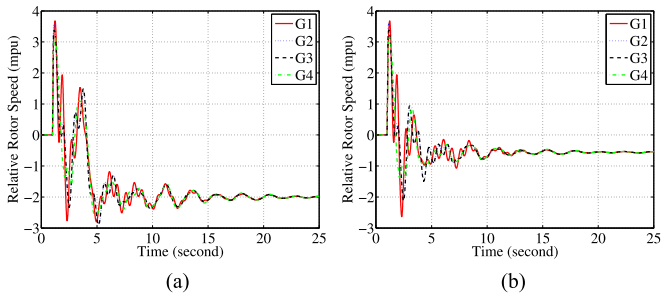

Fig. 6. Adaptive PFL control for $\mu_{i2} = 1$. (a) $\alpha_i = 9D_i$. (b) $\alpha_i = 35D_i$.

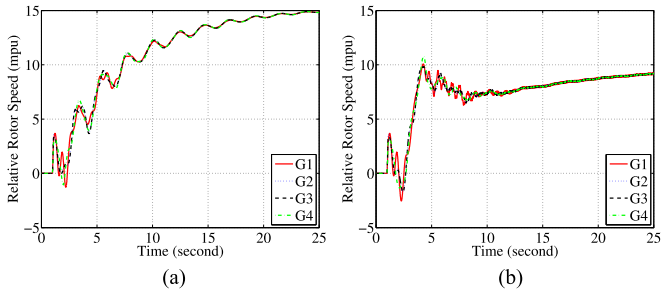

Fig. 7. Adaptive PFL control for $\mu_{i1} = -0.5, \mu_{i2} = -3, \epsilon_{i1} = 5, \epsilon_{i2} = 2$. (a) $\alpha_i = 9D_i$. (b) $\alpha_i = 0.5D_i$.

"swinging" till the system finally settles in (if it is stable); however, the PFL control speeds up the stabilization process and the phase portrait converges faster.

B. Impact of FDI Attacks

As a demonstration, we display in Fig. 2 the impact of example FDI attacks on the rotor speed variable. The impact of such attacks on transient stability is shown to depend on the details of the FDI attack vector. For example, a large positive multiplier term ($\epsilon_{i1} \gg 1$) may not cause a large variation in the power system trajectory; however, a negative multiplier, even if relatively small, can cause noticeable divergence for the transient stability control. Considering a simple amplification plus constant bias FDI attack in Fig. 2(d) demonstrates the easiness of tricking the distributed control on settling the synchronous generator on a nonzero rotor relative speed. Furthermore, the weighted phase portrait is shown in Fig. 3 for sample attacks on the accelerating power variable. As $P_{Ai}(t)$ usually decreases with time after the end of the disturbance, the impact of multiplier terms becomes smaller over time. Similarly, an additive FDI term moves the steady-state value of the rotor speed according to (28) and shown in Fig. 3(c).

C. Adaptive PFL Control

The PFL controller can be made adaptive to reduce the impact of the FDI attacks as detailed in Section V. For example, the value of the design parameter can be set to $-\mu_{i2}/\mu_{i1}$ for constant bias attacks if this ratio is within the acceptable margin for α_i. Assuming that the PFL controller can accurately estimate such ratio, utilizing $\alpha_i = -\mu_{i2}/\mu_{i1}$ completely eliminates the impact of this type of FDI attacks as demonstrated in Fig. 4.

Further, following the results of Section V, Figs. 5–7 demonstrate sample performance results (for the first four generators in the test power system) for the adaptive PFL control for different types of FDI attacks. For example, in Fig. 5, the steady-state rotor value decreases from about 15 to 4.6 mpu when α_i is decreased from $9D_i$ to $0.01D_i$ for a constant-bias attack on the rotor speed parameter. Also, Fig. 6 shows the results of adapting the PFL controller for a bias attack on the accelerating power variable; it is observed that $\bar{\theta} \approx -2$ mpu when $\alpha_i = 9D_i$, but $\bar{\theta} \approx -0.6$ mpu when $\alpha_i = 35D_i$. Similarly for a more general FDI attack, reducing the value of α_i to $0.5D_i$ improves the steady-state rotor speed in Fig. 7 from about 15 to 9 mpu.

D. Discussion

The phase portrait can be used to show the impact of cyber attacks on data integrity. The numerical results in Fig. 1(b) demonstrate the aggressive stabilization by the PFL controller. However, it is observed in Figs. 2 and 3 that the details of the attack vector greatly affect the impact of the FDI attacks. For example, a positive value of ϵ_{i1} yields a limited impact on the synchronous generator transient stability. However, the PFL controller shows resilience to different combinations of attacks. In addition, adapting the value of the PFL controller's design parameter (α_i) can enhance the stability of the power system during the FDI attack.

VII. Conclusion

We aim in this paper to investigate the impact of FDI attacks on storage-based transient stability control schemes. We

consider a general formulation for an FDI attack on PFL control, and we derive closed-form expressions for the values of rotor speed and angle as a result of this cyber attack. Then, we investigate reactive mechanisms to enhance the performance of the PFL controller during FDI attacks. We numerically evaluate the impact of example FDI attacks using the IEEE 68-bus test power system and we draw observations on the impact and limitations of such attacks.

It is observed from the numerical results that the PFL control scheme handles various FDI attacks reasonably well. Further, adapting the PFL design parameter can enhance the performance of the controller during these cyber attacks. Future directions of this paper include investigating detailed detection strategies of FDI attacks on storage-based transient stability control.

Acknowledgment

The authors would like to thank Dr. A. M. Khalil at the University of Toronto for his help in simulating the power system.

References

[1] R. Deng, Z. Yang, M.-Y. Chow, and J. Chen, "A Survey on demand response in smart grids: Mathematical models and approaches," *IEEE Trans. Ind. Informat.*, vol. 11, no. 3, pp. 570–582, Jun. 2015.

[2] A. Sabbah, A. El-Mougy, and M. Ibnkahla, "A survey of networking challenges and routing protocols in smart grids," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 210–221, Feb. 2014.

[3] A. Farraj, E. Hammad, and D. Kundur, "On the use of energy storage systems and linear feedback optimal control for transient stability," *IEEE Trans. Ind. Inform.*, to be published.

[4] W. Li, M. Ferdowsi, M. Stevic, A. Monti, and F. Ponci, "Cosimulation for smart grid communications," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2374–2384, Nov. 2014.

[5] V. Güngör *et al.*, "Smart grid technologies: Communication technologies standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529–539, Nov. 2011.

[6] R. Deng, R. Lu, G. Xiao, and J. Chen, "Fast distributed demand response with spatially-and temporally-coupled constraints in smart grid," *IEEE Trans. Ind. Informat.*, vol. 11, no. 6, pp. 1551–1606, Dec. 2015.

[7] P. Kundur *et al.*, "Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions," *IEEE Trans. Power Syst.*, vol. 19, no. 3, pp. 1387–1401, Aug. 2004.

[8] P. Mercier, R. Cherkaoui, and A. Oudalov, "Optimizing a battery energy storage system for frequency control application in an isolated power system," *IEEE Trans. Power Syst.*, vol. 24, no. 3, pp. 1469–1477, Aug. 2009.

[9] A. Farraj, E. Hammad, and D. Kundur, "A cyber-enabled stabilizing controller for resilient smart grid systems," in *Proc. IEEE PES Conf. Innovative Smart Grid Technol.*, Feb. 2015, pp. 1–5.

[10] J. Wei, D. Kundur, T. Zourntos, and K. Butler-Purry, "A flocking-based paradigm for hierarchical cyber-physical smart grid modeling and control," *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2687–2700, Nov. 2014.

[11] E. Hammad, A. Farraj, and D. Kundur, "Paradigms and performance of distributed cyber-enabled control schemes for the smart grid," in *Proc. IEEE Power Energy Soc. General Meeting*, 2015, pp. 1–5.

[12] A. Farraj, E. Hammad, and D. Kundur, "A cyber-enabled stabilizing control scheme for resilient smart grid systems," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1856–1865, Jul. 2016.

[13] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2010, pp. 226–231.

[14] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2010, pp. 220–225.

[15] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *Proc. IEEE Global Commun. Conf.*, 2012, pp. 3153–3158.

[16] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[17] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106–115, Sep. 2012.

[18] A. Farraj, E. Hammad, and D. Kundur, "A systematic approach to delay-adaptive control design for smart grids," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Nov. 2015, pp. 768–773.

[19] A. Farraj, E. Hammad, and D. Kundur, "Enhancing the performance of controlled distributed energy resources in noisy communication environments," in *Proc. IEEE Can. Conf. Elect. Comput. Eng.*, 2016, pp. 1–4.

[20] A. Farraj, E. Hammad, and D. Kundur, "A cyber-physical control framework for transient stability in smart grids," *IEEE Trans. Smart Grid*, to be published.

[21] P. Sauer and M. Pai, *Power System Dynamics and Stability*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1998.

[22] J. Glover, M. Sarma, and T. Overbye, *Power System Analysis & Design*, 5th ed. Boston, MA, USA: Cengage Learning, 2011.

[23] A. Bergen and V. Vittal, *Power Systems Analysis*, 2nd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2000.

[24] M. Andreasson, D. Dimarogonas, H. Sandberg, and K. Johansson, "Distributed control of networked dynamical systems: Static feedback and integral action and consensus," *IEEE Trans. Autom. Control*, vol. 59, no. 7, pp. 1750–1764, Jul. 2014.

[25] A. Farraj, E. Hammad, and D. Kundur, "On using distributed energy resources to reshape the dynamics of power systems during transients," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2015, pp. 756–761.

[26] E. Hammad, A. Farraj, and D. Kundur, "On the effects of distributed control area design for the stabilization of cyber-enabled smart grids," in *Proc. Workshop Model. Simul. Cyber, Phys. Energy Syst.*, 2015, pp. 1–6.

[27] F. Kazempour, E. Hammad, A. Farraj, and D. Kundur, "Frequency-stabilizing control scheme for islanded microgrids," in *Proc. IEEE Power Energy Soc. General Meeting*, 2015, pp. 1–5.

[28] A. Farraj, E. Hammad, A. Al Daoud, and D. Kundur, "A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1846–1855, Jul. 2016.

[29] A. Farraj, E. Hammad, and D. Kundur, "Robustness analysis of feedback linearization distributed control schemes in smart grid systems," in *Proc. IEEE Power Energy Soc. General Meeting*, 2015, pp. 1–5.

[30] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, 2013.

[31] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Security*, vol. 14, no. 1, pp. 13–33, Jun. 2011.

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

[33] E. Hammad, A. Khalil, A. Farraj, D. Kundur, and R. Iravani, "Tuning out of phase: Resonance attacks," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Nov. 2015, pp. 1–6.

[34] A. Farraj, E. Hammad, D. Kundur, and K. Butler-Purry, "Practical limitations of sliding-mode switching attacks on smart grid systems," in *Proc. IEEE Power Energy Soc. General Meeting*, Jul. 2014, pp. 1–5.

[35] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "A smart grid vulnerability analysis framework for coordinated variable structure switching attacks," in *Proc. IEEE Power Energy Soc. General Meeting*, Jul. 2012, pp. 1–6.

[36] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-Attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[37] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proc. Workshop Secure Control Syst.*, 2010, pp. 1–6.

[38] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *Proc. Workshop Secure Control Syst.*, 2010, pp. 1–9.

[39] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Conf. Comput. Commun. Security*, 2009, pp. 21–32.

[40] Y. Huang *et al.*, "Bad data injection in smart Grid: Attack and defense mechanisms," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 27–33, Jan. 2013.

[41] C. Konstantinou and M. Maniatakos, "A case study on implementing false data injection attacks against nonlinear state estimation," in *Proc. ACM Workshop Cyber, Phys. Syst. Security Privacy*, 2016, pp. 81–92.

[42] C. Liu, J. Wu, C. Long, and Y. Wang, "Dynamic state recovery for cyber-physical systems under switching location attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 14–22, Mar. 2017.

[43] A. Stéphenne, F. Bellili, and S. Affes, "Moment-based SNR estimation over linearly-modulated wireless SIMO channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 2, pp. 714–722, Feb. 2010.
[44] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Processes*. New York, NY, USA: Tata McGraw-Hill Education, 2002.
[45] B. Pal and B. Chaudhuri, *Robust Control in Power Systems* (Power electronics and power systems series). New York, NY, USA: Springer, 2006.
[46] A. Singh and B. Pal, "IEEE PES task force on benchmark systems for stability controls report on the 68-Bus, 16-Machine, 5-Area system," IEEE Power and Energy Society, Tech. Rep., Dec. 2013. [Online]. Available: http://eioc.pnnl.gov/benchmark/ieeess/NETS68/New_England_New_York_68_Bus_System_study_report.pdf

Abdallah Farraj (S'11–M'12) received the B.Sc. and M.Sc. degrees in electrical engineering from the University of Jordan, Amman, Jordan, and the Ph.D. degree in electrical engineering from Texas A&M University, College Station, TX, USA.

His research interests include modeling and analysis of cyber-physical systems, cyber security and resilience of smart grids, cognitive communications, and downhole telemetry systems.

Eman Hammad (S'14) received the B.Sc. degree from the University of Jordan, Amman, Jordan, and the M.Sc. degree from Texas A&M University, College Station, TX, USA, both in electrical engineering. She is currently working toward the Ph.D. degree in the Department of Electrical Engineering, University of Toronto, Toronto, ON, Canada.

Her current research interests include cyber-physical systems with particular interest in cyber-security, resilient control, and cooperative game theory in the context of smart grids. She currently serves as the IEEE Toronto Communication Society Chapter Chair.

Deepa Kundur (S'91–M'99–SM'03–F'15) is a native of Toronto, Canada. She received the B.A.Sc., M.A.Sc., and Ph.D. degrees all in electrical and computer engineering from the University of Toronto, Toronto, ON, Canada, in 1993, 1995, and 1999, respectively.

She currently serves as the Chair of the Division of Engineering Science and as a Professor and the Director of the Centre for Power & Information in The Edward S. Rogers Sr. Department of Electrical & Computer Engineering, the University of Toronto. From January 2003 to December 2012, she was a faculty member in electrical & computer engineering at Texas A&M University, College Station, TX, USA, and from September 1999 to December 2002, she was a faculty member in electrical & computer engineering at the University of Toronto. She is an author of more than 150 journal and conference papers. She is also a recognized authority on cyber security issues and has appeared as an expert in popular television, radio, and print media. She has participated on several editorial and conference executive boards, and currently serves on the Advisory Board of the IEEE Spectrum. Her research interests include interface of cyber security, signal processing, and complex dynamical networks.

Dr. Kundur's research has received best paper recognitions at numerous venues including the 2015 IEEE Smart Grid Communications Conference, the 2015 IEEE Electrical Power and Energy Conference, the 2012 IEEE Canadian Conference on Electrical & Computer Engineering, the 2011 Cyber Security and Information Intelligence Research Workshop, and the 2008 IEEE INFOCOM Workshop on Mission Critical Networks. She has also received the teaching awards at both the University of Toronto and Texas A&M University. She is a Fellow of the Canadian Academy of Engineering.