A Distributed Control Paradigm for Smart Grid to Address Attacks on Data Integrity and Availability

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

***Abstract*—In this paper, we propose an adaptive cyber-enabled parametric feedback linearization (PFL) control scheme for transient stability of smart grids. Based on feedback linearization control theory, the distributed PFL controller utilizes a distributed energy storage system to modify the dynamics of the power system during transients. We consider cyber attacks on data integrity and availability in the smart grid, and propose to adapt the PFL controller's parameter to the cyber state of the smart grid. Specifically, the PFL control scheme adapts its aggressiveness parameter to the level of noise, communication latency, and data injection attacks. Further, depending on the severity of the physical disturbance, the controller adjusts the value of its parameter to speed up the stabilization process. The performance of the proposed control scheme is validated on the IEEE 68-bus test power system, where the adaptive PFL controller is shown to efficiently stabilize the power system during physical and cyber disturbances.**

***Index Terms*—Smart grid, data integrity, data availability, cyber attacks, cyber-physical control, swing equation, feedback linearization control, transient stability, power system dynamics.**

I. Introduction

CYBER-PHYSICAL systems involve interacting networks of physical and computational components. Security of networked cyber-physical systems is of particular recent interest given the critical dependence of advanced societies on such systems (which include smart grid, autonomous transportation, and advanced healthcare) leading to concerns of safety and privacy. In this paper, we focus on smart grid systems and their operational security. It is well known that defense-in-depth security approaches involve the stages of prevention, detection and reaction. We focus on latter process of reaction providing opportunities to add resilience into cyber-physical system design. In particular, we argue that an effective approach to react to a cyber attack is to mitigate its impact on the physical system component. Since control lies at the cyber-physical boundary, it represents an effective component to deter the propagation of cyber attack impacts. Smart power systems are characterized, in part, by their high degree of cyber enablement and incorporation of alternative energy sources, which has facilitated advanced forms of operational control as well as the use of energy storage systems (ESSs). Control schemes that specifically utilize ESSs for system actuation provide opportunities to change power system dynamics to provide greater stability and resilience. As more sensors and communication networks are installed in the smart grid, the potential for distributed control schemes becomes more visible.

We consider the application of distributed control to transient stability problems. Transient stability is concerned with the ability of the power system to maintain synchronism when subjected to severe disturbance [1]; physical disturbances include loss of generators or transmission lines, faults, or switching attacks [2]–[4]. Transient stability is related to the ability of the synchronous generators to balance input mechanical torque with output electrical torque. If the torque difference persists to be nonzero, the generators experience angular swings leading to loss of synchronism. In this context, a distributed control scheme can aid the power system to regain transient stability after the onset of disturbances. The distributed control (by employing the associated communication network to receive frequent system measurement updates) can affect the dynamics of the power system via ESS actuation subsequently enabling the synchronous generators to achieve transient stability. New distributed control schemes have recently been proposed for stability applications [5]–[12]. Such approaches, however, are typically activated after the occurrence of a *physical* disruption and have been developed for "ideal" conditions.

A. Contributions

Distributed controllers face real environments where cyber attacks, noisy channels, and excessive communication latency are present. Cyber attacks that target data integrity and availability include false data injection (FDI) attacks against state estimation where an adversary introduces stealthy errors into specific measurements used for state estimation [13], denial of service (DoS) attacks against communication links where an adversary interrupts the operation of the cyber network to cause communication link failure and excessive delays and consequently results in preventing the timely exchange of information between the sensors, actuators, and control systems [14], and interference attacks against signals where an adversary jams communications links with undesired electromagnetic signals. Such attacks and issues can contribute to measurement distortions and

Manuscript received December 19, 2016; revised April 9, 2017; accepted May 28, 2017. Date of publication July 5, 2017; date of current version February 19, 2018. The guest editor coordinating the review of this manuscript and approving it for publication was Dr. Arash Mohammadi. *(Corresponding author: Abdallah Farraj.)*

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

Digital Object Identifier 10.1109/TSIPN.2017.2723762

uncertainties that degrade the performance of distributed ESS-based control schemes.

Robust control implementations are traditionally used to contain the effects of measurement uncertainties; however, such designs are usually complicated and might not perform well for all operating points. For example, complex solutions for real-time delay-adaptive control appear in [15], [16], and excessive communication delay poses a challenge for wide-area damping control schemes [16]–[18]. Furthermore, the targeted nature of cyber attacks render some robust control approaches ineffective. Thus, in this work we propose a simple adaptive control scheme to address attacks on data integrity and availability by strengthening the results of [19], [20] on parametric feedback linearization (PFL) control. PFL control is a distributed paradigm that removes the nonlinearity in the system dynamics while enhancing the stability of the synchronous generators. Cyber attacks affect the quality of the received measurements at the controller; hence, we study of impact of measurement uncertainties on the eigenvalues and the steady-state values of the closed-loop power system. We propose to adapt the controller parameter to reflect the quality of the received measurement. The proposed control scheme is tractable, has simple design, and efficiently stabilizes the power grid under ideal conditions and during measurement uncertainties and attacks on data integrity and availability.

B. Comparative Study

In this work we build on the PFL controller proposed in [21]; we enhance the controller by making it more adaptive to measurements uncertainty. The PFL controller is designed in [21] to address physical disturbances; however, in this work we adapt the controller's parameter (α_i) as a response to the cyber state of the smart grid. Further, we conduct in this work a detailed analysis of the system dynamics and we derive expressions for steady-state rotor speed values.

The work in [22] presents a control paradigm for frequency regulation in power system; in this work we consider the transient stability problem. Further, we propose to have control agents on the generator buses; however, all buses are controlled in [22]. A complete model that includes reactive power and voltage dynamics is used in this work; but [22] uses a lossless system model and does not include voltage dynamics or reactive powers.

A power system robustness framework is presented in [23] to incorporate different attack scenarios into the conventional security-constrained optimal power flow-based dispatch scheme; the model integrates generation operation cost in normal state, $N-1$ contingency risks caused by random failures, and the risks caused by deliberate attacks. It is argued in [23] that system defenders should minimize the worst consequences that can be caused by attackers. The proposed controller in this work complements the framework proposed in [23] by adapting the controller's design parameter in order to mitigate the consequences of attacks.

The rest of this paper is organized as follows. The problem setting is presented in Section II. The proposed adaptive PFL control scheme is detailed in Sections III and IV. Sections V and VI investigate the performance of the adaptive control scheme using the IEEE 68-bus test power system followed by conclusions in Section VII.

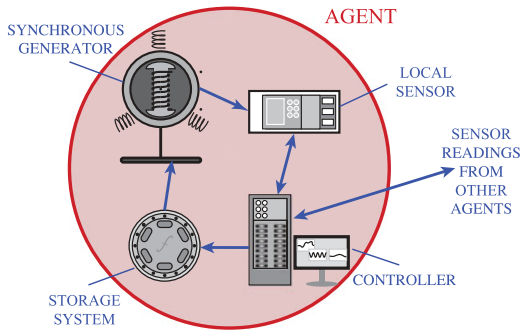

Fig. 1. Cyber-physical agent.

II. ESS-Based Control

In this section we define the goals of this work. We introduce a multi-agent formulation for smart grids. We then overview the transient stability problem, and we include the cyber-enabled ESS-based distributed control paradigm.

A. Problem Formulation

In this work we propose an adaptive ESS-based control scheme to address attacks on data integrity and availability, and we focus on the recently-published PFL control for transient stability applications. The objectives of this work include:

1) developing a measure to quantify the levels of measurement uncertainty;
2) studying the impact of measurements uncertainties on the dynamics of the controlled system;
3) studying the relation between the PFL controller's design parameter and measurements uncertainty levels;
4) proposing a piece-wise linear relationship for the design parameter depending on the corruption level; and
5) verifying the performance of the adaptive PFL control versus latency and noise levels.

B. Multi-Agent Representation

We model the smart grid as a multi-agent system comprised of N cyber-physical agents as depicted in Fig. 1. In this model, cyber-physical Agent i consists of a synchronous Generator i, an associated sensor that provides local measurements of the generator rotor angle δ_i and rotor speed ω_i, communication transceivers to connect different smart grid agents for the transmission of δ_i and ω_i, a local fast-acting ESS (such as a flywheel), and a distributed control agent. The distributed controller processes sensor data from system agents (received locally at the agent generator and through the communication network) to calculate the control signal u_i. The distributed controller affects the dynamics of the power system by utilizing the local ESS to inject or absorb real power at the ith generator bus depending on the value of the control signal u_i.

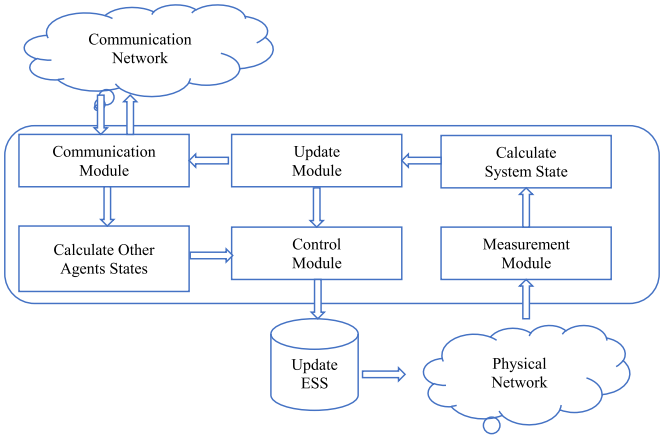

Fig. 2. Logical modules of a control agent.

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

As shown in Fig. 2, a control agent has a measurements module to acquire power system sensor readings, a system state module to estimate the generator rotor speed, rotor angle, and accelerating power, a communication module to transmit (receive) local state information to (from) other agents, and a control module that computes the control signal using system state variables, latency, noise levels, and other flags. In addition, an update module extracts the local generator's rotor speed and angle values; this module also labels any corrupted measurement with the appropriate flags (e.g., noise, interference or FDI) and estimates latency values that are also added to the labels.

C. System Dynamics

Let N denote the number of synchronous generators in the power system under consideration. The parameters for Generator i, $i \in \{1, \ldots, N\}$ are defined in Table I. The two-axis sub-transient machine model is widely used to describe the dynamics of synchronous generators during large disturbances. In this model, the transient electrical dynamics of the stator of Generator i are described as [24], [25]:

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

$$\dot{E}'_{di} = \frac{1}{T'_{qi}}\left(-E'_{di} + (X_{qi} - X'_{qi})I_{qi}\right) \tag{2}$$

$$E'_{qi} = V_{qi} + R_{ai}I_{qi} + X'_{di}I_{di} \tag{3}$$

$$E'_{di} = V_{di} + R_{ai}I_{di} - X'_{qi}I_{qi} \tag{4}$$

where $\dot{E}'_{qi}$ and $\dot{E}'_{di}$ denote the time derivatives of E'_{qi} and E'_{di}, respectively. In addition, let Ω_s denote the system frequency (typically equal to $60 \cdot 2\pi$ or $50 \cdot 2\pi$ depending the geographical location), and let $\dot{\delta}_i$ and $\dot{\omega}_i$ be the time derivatives of δ_i and ω_i, respectively. The rotor dynamics of the synchronous generator can be expressed by [24]:

$$\dot{\delta}_i = \Omega_s(\omega_i - \omega_s) \tag{5}$$

$$\dot{\omega}_i = \frac{\omega_s}{2H_i}\left(T_{Mi} - T_{Ei} - D_i(\omega_i - \omega_s)\right). \tag{6}$$

Equations (5) and (6) are typically referred to as the *swing equation* and collectively describe the electromechanical dynamics of the synchronous generator's rotor and thus can be useful in studying the behavior of the generators when the power system is subjected to large disturbances. In this model, the field voltage of a generator is controlled by the excitation system, the mechanical torque is controlled by the speed governor, and the nonlinear electrical torque T_{Ei} is calculated as [24]:

$$T_{Ei} = E'_{di}I_{di} + E'_{qi}I_{qi} + (X'_{qi} - X'_{di})I_{di}I_{qi}. \tag{7}$$

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. Let E_i denote the internal voltage of Generator i, and $G_{ik} = G_{ki}$ and $B_{ik} = B_{ki}$ represent the Kron-reduced equivalent conductance and susceptance between Generators i and k, respectively. The value of P_{Ei} can be directly calculated as [26]:

$$P_{Ei} = \sum_{k=1}^{N} |E_i||E_k|\left(G_{ik}\cos(\delta_i - \delta_k) + B_{ik}\sin(\delta_i - \delta_k)\right). \tag{8}$$

Let $P_{Ai} = P_{Mi} - P_{Ei}$ denote the accelerating power of Generator i. During normal operation of the power system, the accelerating power typically equals 0. However, when a major disturbance occurs, the accelerating power of some generators deviate from 0, and the rotor will increase its speed when $P_{Ai} > 0$ and vice versa. However, the synchronous generator might be damaged if there is a large deviation in its rotor speed which, for safety reasons, might lead to disconnecting the machine from the power grid. The goal of a control scheme for transient stability is to regain the balance between the mechanical and electrical torques of a synchronous generator in order to achieve constant and acceptable rotor speeds fast. In other words, the controller tries to restore the synchronism between the system generators. In this work, we label a generator as stabilized if its rotor speed is driven back to the acceptable range;

thus, stability time is a performance metric that quantifies the time the controller takes to stabilize the synchronous generators in the power system.

D. Distributed Control Paradigm

The cyber network of the smart grid enables the design and implementation of new control schemes. In this paradigm, sensors can communicate their measurements to the distributed controllers through the communication network, and the distributed controllers can affect the dynamics of the power system by injecting or absorbing power from the grid through actuating the ESSs. An ESS has the ability to respond to load variations and control signals by injecting or absorbing power [27]. There are many types of ESSs, including mechanical, electrical, thermal, biological, and chemical systems. Popular ESS technologies include flywheels, pumped hydro, solid state, compressed air, and capacitor systems. As power systems transform into smarter grids, ESSs can help in maintaining system stability and reliability. We model the distribution of the ESSs in the power system by incorporating an ESS at each generator bus. The capacity of each ESS is determined as a percentage of the associated generator mechanical power. Let the output of the ESS at the bus of Generator i be denoted u_i. Depending on the sign of u_i, the associated ESS absorbs or injects an amount of power equal to $|u_i|$. Thus, the swing equation of Generator i at time t becomes

$$\begin{aligned} rll\dot{\delta}_i(t) &= \Omega_s(\omega_i(t) - \omega_s) \\ \dot{\omega}_i(t) &= \frac{\omega_s}{2H_i}\left(P_{Ai}(t) - D_i(\omega_i(t) - \omega_s) + u_i(t)\right). \end{aligned} \tag{9}$$

ESS-based control (u_i) affects the operation of the associated storage device to achieve transient stability; a positive (negative) u_i value in (9) indicates that the ESS injects (absorbs) real power from the bus of Generator i.

Flywheels store energy in rotating mass. The stored kinetic energy depends on the flywheel moment of inertia and rotational speed [28]. The kinetic energy is transferred to/from the flywheel using an electrical machine that works as a motor/generator set. When the electrical machine acts as a motor, the electric energy supplied to the stator is converted to positive torque which will cause the flywheel rotor to rotate faster and store kinetic energy. In the generator mode, the kinetic energy stored in the rotor applies a negative torque to slow down the rotor and convert the kinetic energy into an electric energy that can be released. With the help of power electronics, a flywheel can serve connected loads at its power rating for few tens of seconds. Flywheels have longer lifetime and high degree of efficiency, which makes them suitable for short-term energy charge/discharge operations. The fast response time also makes flywheels useful for frequency regulation. With sufficent capacity, flywheels can be beneficial in enhancing the electric power quality [29].

Let m_F be the mass of the flywheel, it has a radius r_F and is rotating with an angular speed of ω_F. Further, the polar moment of inertia of the flywheel is $J_F = m_F.{r_F}^2$. Then, the stored energy in the flywheel (termed E_F) is described as

$$E_F = \frac{1}{2} m_F.(r_F.\omega_F)^2 . \tag{10}$$

The kinetic energy in a flywheel rotating at a maximum angular speed of ω_{Fm} can be given by $\frac{1}{2} J_F.{\omega_{Fm}}^2$. Let T_F be the period of operation of the flywheel, K_F denotes its torque conversion factor value, and P_{Fm} is its maximum nominal power rating. The design of the rotor/stator system and field windings determines the value of K_F [30]. Then,

$$T_F = \frac{1}{2}\frac{J_F}{P_{Fm}}{\omega_{Fm}}^2 . \tag{11}$$

The rotation of the flywheel yields to a piece-wise defined function [31], and its discharging characteristic has constant spin and exponential reduction in speed regions as

$$\omega_F(t) = \begin{cases} \omega_{Fm} & t < T_F \\ \omega_{Fm}.\exp\left(-\frac{K_F}{J_F}(t - T_F)\right) & t \geq T_F . \end{cases} \tag{12}$$

The power of the flywheel at the exponential region is the derivative of the stored kinetic energy with respect to time. Then, the flywheel discharge power is expressed as

$$P_F = \begin{cases} P_{Fm} & t < T_F \\ P_{Fm}.\exp\left(-\frac{K_F}{J_F}(t - T_F)\right) & t \geq T_F . \end{cases} \tag{13}$$

As T_F is in the order of few tens of seconds, the power fast power injection/absorption can appear instantaneous from the controller's point of view.

III. Impact of Measurement Uncertainty

In this section we introduce the distributed PFL control scheme and study its performance in an ideal environment and in the presence of measurements uncertainties. We quantify the impact on the eigenvalues of the closed-loop system and on the steady-state values.

A. Feedback Linearization Control

The distributed PFL controller of [21] achieves transient stability after the onset of disturbances in smart grid systems. Let the capacity of the ESS of Agent i at time t be denoted $C_i(t)$. Then, to account for the capacity limits of the local storage device, u_i is given by:

$$u_i(t) = \begin{cases} C_i(t) & \hat{u}_i(t) > C_i(t) \\ \hat{u}_i(t) & -C_i(t) \leq \hat{u}_i(t) \leq C_i(t) \\ -C_i(t) & \hat{u}_i(t) < -C_i(t) \end{cases} \tag{14}$$

where $\hat{u}_i$ is the preprocessed signal computed by the PFL controller to achieve transient stability. The controller changes the output of the corresponding ESS for Generator i as [21]:

$$\hat{u}_i(t) = -P_{Ai}(t) - \alpha_i(\omega_i(t) - \omega_s) \tag{15}$$

to shape the system dynamics as described in (9) and (14). Here, $\alpha_i = \beta_i D_i > 0$ is a measure of the agility of the PFL controller, whereby a higher value of α_i indicates a more aggressive controller. After applying the PFL control signal, the rotor dynamics

of Generator i becomes:

$$\begin{aligned} rll\dot{\delta}_i(t) &= \Omega_s(\omega_i(t)-\omega_s) \\ \dot{\omega}_i(t) &= \frac{-\omega_s}{2H_i}(D_i+\alpha_i)\,(\omega_i(t)-\omega_s) \\ &= \frac{-\omega_s D_i}{2H_i}(1+\beta_i)\,(\omega_i(t)-\omega_s)\,. \end{aligned} \tag{16}$$

Once a disturbance is detected, the PFL controller receives periodic measurements of the different sensors in the smart grid. The controller utilizes (15) to calculate the control signal and it actuates the associated ESS accordingly. As a result, the rotor speeds of the different synchronous generators are driven back to around ω_s, and the rotor angles are stabilized.

Define $\boldsymbol{x}_i = [\delta_i, \omega_i - \omega_s]^T$ as the state variable of Generator i. Then, applying the PFL control reduces the *resultant* rotor dynamics of Generator i to a set of decoupled linear equations as follows:

$$\dot{\boldsymbol{x}}_i(t) = \boldsymbol{A}_i\,\boldsymbol{x}_i(t) \tag{17}$$

where

$$\boldsymbol{A}_i = \begin{bmatrix} 0 & \Omega_s \\ 0 & \frac{-\omega_s D_i}{2H_i}(1+\beta_i) \end{bmatrix}. \tag{18}$$

The eigenvalues of $\boldsymbol{A}_i$ are 0 and $\frac{-\omega_s D_i}{2H_i}(1+\beta_i)$ corresponding to the left-hand complex plane; hence, $\lim_{t\to\infty}\omega_i(t) = \omega_s$ is achieved [32]. The zero eigenvalue indicates that there is no direct control over the rotor angle. However, (6) indicates that the fluctuations in rotor angle are stopped once the rotor speed is asymptotically stabilized. Under ideal conditions, the PFL controller reshapes the rotor dynamics of the closed-loop power system to resemble a series of stable decoupled linear systems with tunable eigenvalues. Thus, the PFL controller achieves transient stability.

In (17), the mechanical power is considered constant during the stabilization process (which is usually few seconds). This is justified as the reaction time of the speed governor is typically much slower than that of the PFL controller. Given the change in mechanical power is negligible during this short period, $\dot{P}_{Mi} = 0$ is used. The reader should note that the PFL controller complements and enhances the operation of existing power control schemes.

B. Measurement Uncertainty

As a result of cyber disturbances on data integrity and availability, noise, interference, and communication latency, the measurements received by the control agent can be different from the actual physical values. Let the received measurements of δ_i, ω_i, and P_{Ai} be denoted $\hat{\delta}_i$, $\hat{\omega}_i$, and $\hat{P}_{Ai}$, respectively, which are employed by the PFL controller to compute $u_i(t)$. We model the relationship between these estimates and their original values as [19], [20]:

$$\begin{aligned} \hat{\delta}_i(t) &= \delta_i(t) + n_{\delta_i}(t) \\ &= (1+e_{\delta_i}(t))\delta_i(t) \\ \hat{\omega}_i(t)-\omega_s &= \omega_i(t)-\omega_s+n_{\omega_i}(t) \\ &= (1+e_{\omega_i}(t))(\omega_i(t)-\omega_s) \\ \hat{P}_{Ai}(t) &= P_{Ai}(t)+n_{p_i}(t) \\ &= (1+e_{p_i}(t))P_{Ai}(t) \end{aligned} \tag{19}$$

where $n_{\delta_i}(t) = e_{\delta_i}(t)\delta_i(t)$, $n_{\omega_i}(t) = e_{\omega_i}(t)(\omega_i(t)-\omega_s)$, and $n_{p_i}(t) = e_{p_i}(t)P_{Ai}(t)$ are the additive uncertainties of the rotor angle, rotor speed, and accelerating power of Generator i at time t, respectively, and are interrelated through (5) and (8).

We revisit (8) in order to explore the relation between the uncertainties in rotor angle and electrical power. We employ the standard DC power flow approximation in [33] to linearize the electrical power formula. This process of linearization is particularly applicable to power transmission systems, which is the focus of our study [34]. Starting from (8), the electrical power of Generator i can be approximated as

$$\begin{aligned} P_{Ei} &\overset{(a)}{\approx} \sum_{k=1}^{N} |E_i|\,|E_k|B_{ik}\sin(\delta_i-\delta_k) \\ &\overset{(b)}{\approx} \sum_{k=1}^{N} |E_i|\,|E_k|\,B_{ik}(\delta_i-\delta_k) \end{aligned} \tag{20}$$

where (a) assumes that line resistances are negligible compared to the reactances in all Kron-reduced transmission lines; also, (b) assumes that rotor angle differences $(\delta_i-\delta_k)$ are small between Generators i and k, which leads to $\sin(\delta_i-\delta_k) \approx \delta_i-\delta_k$. Instead of using δ_i to calculate P_{Ei}, assume that the controller applies $\hat{\delta}_i$ from (19) due to measurement uncertainties. This leads to $\hat{P}_{Ei}$ of the form

$$\begin{aligned} \hat{P}_{Ei} &\overset{(a)}{\approx} \sum_{k=1}^{N} |E_i|\,|E_k|\,B_{ik}((1+e_{\delta_i})\delta_i-(1+e_{\delta_k})\delta_k) \\ &\overset{(b)}{\approx} (1+e_{\delta_i})\sum_{k=1}^{N} |E_i|\,|E_k|\,B_{ik}(\delta_i-\delta_k) \\ &= (1+e_{\delta_i})P_{Ei} \end{aligned} \tag{21}$$

where (a) is from (20) and (b) assumes different uncertainties in rotor angles are approximately equal. Consequently, the impact of rotor angle uncertainty on accelerating power can be approximated as $\hat{P}_{Ei} = (1+e_{\delta_i})P_{Ei}$.

C. Closed-Loop System under Uncertainty

The signal-to-noise ratio (SNR) is a measure traditionally used to quantify the level of noise in a received measurement. In this work we extend this concept to include the effect of interference, communication latency, FDI, and other cyber attacks. From (19), the instantaneous SNR value of the rotor speed

measurement at time t is:

$$\text{SNR}_{\omega_i}(t) = \frac{(\omega_i(t)-\omega_s)^2}{n_{\omega_i}(t)^2} = \frac{1}{e_{\omega_i}(t)^2} \tag{22}$$

where we used $n_{\omega_i}(t) = e_{\omega_i}(t)(\omega_i(t)-\omega_s)$ and simplified. Similar expressions can be found for the other two quantities ($\hat{\delta}_i$ and $\hat{P}_{Ai}$). Given the uncertainty in the received measurement, the PFL control signal becomes $\hat{u}_i(t) = -\hat{P}_{Ai}(t) - \alpha_i(\hat{\omega}_i(t) - \omega_s)$. Consequently, the measurement uncertainty modifies the swing equation of the closed-loop system to be:

$$\dot{\boldsymbol{x}}_i(t) = \hat{\boldsymbol{A}}_i(t)\,\boldsymbol{x}_i(t) + \boldsymbol{c}_i(t) \tag{23}$$

where

$$\hat{\boldsymbol{A}}_i(t) = \begin{bmatrix} 0 & \Omega_s \\ 0 & -\frac{D_i+\alpha_i(1+e_{\omega_i}(t))}{2H_i/\omega_s} \end{bmatrix}$$

$$\boldsymbol{c}_i(t) = \begin{bmatrix} 0 \\ -\frac{e_{p_i}(t)P_{Ai}(t)}{2H_i/\omega_s} \end{bmatrix}. \tag{24}$$

D. Analysis of Measurement Uncertainty

In the following we investigate the impact of measurement uncertainties on the eigenvalues of $\hat{\boldsymbol{A}}_i(t)$ and quantify the steady-state behavior of the system-state variable due to the existence of the bias vector $\boldsymbol{c}_i(t)$.

1) Eigenvalue Study: Inspection of (24) reveals that the eigenvalues of $\hat{\boldsymbol{A}}_i(t)$ are 0 and $\frac{-\omega_s}{2H_i}(D_i + \alpha_i(1+e_{\omega_i}(t)))$. The nonzero eigenvalue has to be in the left-hand complex plane for the ith generator to stabilize during disturbances. This requires that $D_i + \alpha_i(1+e_{\omega_i}(t)) > 0$, or:

$$e_{\omega_i}(t) > -\frac{D_i+\alpha_i}{\alpha_i} = -\frac{1+\beta_i}{\beta_i}. \tag{25}$$

When $e_{\omega_i}(t) > 0$, both $\hat{\omega}_i(t) - \omega_s$ and $\omega_i(t) - \omega_s$ have the same sign and $|\hat{\omega}_i(t) - \omega_s| > |\omega_i(t) - \omega_s|$. Hence, as a result of the measurement uncertainty, the PFL controller over-compensates for the speed deviation, but the generator is stable as $e_{\omega_i}(t) > 0 > -\frac{1+\beta_i}{\beta_i}$. On the other hand, for the case when $e_{\omega_i}(t) < 0$, the measurement and its estimate may have different signs, and that means the controller under-compensates the rotor speed difference. Consequently, we need to investigate the possibility that $e_{\omega_i}(t) \not> -\frac{1+\beta_i}{\beta_i}$ in order to guarantee generator stability.

Specifically, when $e_{\omega_i}(t) < 0$, we can deduce from (22) that $e_{\omega_i}(t) = \frac{-1}{\sqrt{\text{SNR}_{\omega_i}(t)}}$. In order to keep the generators stable, we follow the results in (25) to find the required relation between the SNR values and the controller design parameter as:

$$\frac{-1}{\sqrt{\text{SNR}_{\omega_i}(t)}} > -\frac{1+\beta_i}{\beta_i}.$$

Rearranging this expression leads to the following constraint:

$$\sqrt{\text{SNR}_{\omega_i}(t)} > \frac{\beta_i}{1+\beta_i}. \tag{26}$$

It is to be noted that $0 < \frac{\beta_i}{1+\beta_i} < 1$. Thus, if the power in the "noise" component is limited compared to the original signal, the SNR is large and any value of β_i (and correspondingly α_i) works. However, to reduce stabilization time, a high value of β_i would be preferred when the SNR is high. On the other hand, if the SNR value is low and less than 0 dB, the value of β_i should be restricted in order not to move the nonzero eigenvalue to the right-hand complex plane. Consequently, the PFL control scheme should be less aggressive for low SNR values. From (26), this objective can be accomplished by limiting β_i according to:

$$\beta_i < \frac{\sqrt{\text{SNR}_{\omega_i}(t)}}{1-\sqrt{\text{SNR}_{\omega_i}(t)}}. \tag{27}$$

2) Steady-State Value: Another consequence of measurement uncertainties appears as a potential bias in the steady-state values of state variables. If we approximate the uncertainty in the accelerating power as a constant independent of the other two state variables, the steady-state value of the rotor speed, denoted ω_i^*, can be found. In steady state, $\dot{\omega}_i^* = 0$, thus ω_i^* can be extracted from (23) as

$$-\frac{D_i+\alpha_i(1+e_{\omega_i}^*)}{2H_i/\omega_s}(\omega_i^*-\omega_s) - \frac{e_{p_i}^* P_{Ai}^*}{2H_i/\omega_s} = 0 \tag{28}$$

where $e_{p_i}^*, P_{Ai}^*, e_{\omega_i}^*$ are the steady-state values of the corresponding variables. Then, the steady-state rotor speed value is expressed as

$$\omega_i^* - \omega_s = -\frac{e_{p_i}^* P_{Ai}^*}{D_i+\alpha_i(1+e_{\omega_i}^*)}. \tag{29}$$

One objective of the PFL control scheme is to change the dynamics of the power system such that $\omega_i^* - \omega_s = 0$ is realized rapidly. However, this target might not be achieved due to measurement uncertainties as shown above. It is observed that a higher value of α_i reduces the effect of e_{p_i} but it amplifies the effect of e_{ω_i}.

E. Observations

It is apparent from (26) and (27) that to keep the generators stable, the value of β_i (and correspondingly α_i) can be varied in response to the level of uncertainty in the received measurements. Specifically, the value of the SNR decreases when the cyber system suffers from higher degrees of noise, interference, FDI infiltration, and communication latency. The smart grid system can be pushed toward stability during disturbances by decreasing the value of α_i when SNR decreases. In other words, when the PFL controller is less certain about the fidelity of the received measurements, the controller should become less aggressive. On the other hand, the results of (29) show that α_i has a mixed effect when it comes to reducing the error in the steady-state values. However, since $|P_{Ai}| \gg |\omega_i - \omega_s|$ in traditional faults, a higher value of α_i will help in pushing $\omega_i^* - \omega_s$ to 0 especially when SNR values are high. Further, for the low-SNR scenario, the requirements of low α_i for eigenvalue placement and high α_i for steady-state values should be satisfied. Consequently, a relatively moderate value of α_i can be utilized when the SNR is low.

IV. Adaptive Control Paradigm

In this section we propose a simple cyber-adaptive PFL control scheme that takes into consideration the findings in (17), (26), and (29). In this work, measurement uncertainty represents the effect of attacks on data integrity, and (excessive) communication delay between the sensors and the controllers is used to capture the effect of cyber attacks on data availability. For tractability, the PFL controller reacts to cyber attacks on data integrity and availability by varying the value of its aggressiveness parameter.

A. Defense-in-Depth Approach to Security

Cyber attacks can lead to system malfunctioning, safety, or instability problems, financial losses for the system operators, or gains for the intruders. Dealing with cyber attacks on smart grids is different from the treatment of traditional sensor noise issues due to the targeted nature of these attacks. Traditionally, the first line of defense against attacks is intrusion detection and possible prevention. However, cyber-security studies in smart grids now focus on stealthy attacks that bypass these lines of defenses. Consequently, there is a shift from attack prevention into attack mitigation via control.

The cyber-physical disturbances can be addressed through a defense-in-depth paradigm where prevention, detection and reaction strategies for protection against attacks are simultaneously employed at various levels. Preventative approaches aim to obstruct the impact of a disturbance by making it impossible to be carried out or by immediately isolating the associated fault. Detection schemes are employed when prevention is unsuccessful in thwarting a disturbance; such strategies use system measurements and models for the identification of anomalies. A reaction approch uses strategies to recover from a disturbance and includes the design of control systems [35].

B. SNR Estimation

In this section we apply the method of moments to estimate the SNR of the received measurements. Let $x(t)$ denote the transmitted sensor signal at time t, $y(t)$ is the received signal at the controller, $n(t)$ is a zero-mean noise Gaussian signal measured at the controller side, and $\mathbb{E}[\cdot]$ is the expectation operator. $\mathbb{E}\big[x^2(t)\big]$, $\mathbb{E}\big[y^2(t)\big]$ and $\mathbb{E}\big[n^2(t)\big]$ represent the power of the transmitted, received, and noise signals, respectively. Let $\hat{\mathbb{E}}\big[x^2(t)\big]$ and $\hat{\mathbb{E}}\big[y^2(t)\big]$ denote the estimates to $\mathbb{E}\big[x^2(t)\big]$ and $\mathbb{E}\big[y^2(t)\big]$, respectively; $\hat{\mathbb{E}}\big[y^2(t)\big]$ is measured at the controller side by time-averaging the power of the received signal; $x(t)$ is also assumed to be an ergodic signal, thus $\hat{\mathbb{E}}\big[x^2(t)\big]$ can be estimated from the typical properties of the sensor signal. Assume that $\mathbb{E}[x(t)] = 0$, which is valid for many signals, including the rotor relative speed $(\omega_i - \omega_s)$. Further, $x(t)$ and $n(t)$ are assumed to be independent signals (i.e., $\mathbb{E}[x(t) \cdot n(t)] = \mathbb{E}[x(t)] \cdot \mathbb{E}[n(t)]$), which is valid given that $n(t)$ is a noise signal. The following cases are considered:

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

$$y(t) = x(t) + n(t)\,. \tag{30}$$

Thus, $\mathbb{E}[y(t)] = \mathbb{E}[x(t)] + \mathbb{E}[n(t)] = 0$ and $\mathbb{E}\big[y^2(t)\big] = \mathbb{E}\big[x^2(t)\big] + \mathbb{E}\big[n^2(t)\big]$. The actual SNR value is expressed as

$$\text{SNR} = \frac{\mathbb{E}\big[x^2(t)\big]}{\mathbb{E}[n^2(t)]}\,. \tag{31}$$

The noise power is estimated from $\hat{\mathbb{E}}\big[y^2(t)\big] - \hat{\mathbb{E}}\big[x^2(t)\big]$. Hence, the estimated SNR value is calculated from $\hat{\mathbb{E}}\big[x^2(t)\big] / \Big(\hat{\mathbb{E}}\big[y^2(t)\big] - \hat{\mathbb{E}}\big[x^2(t)\big]\Big)$. Since $\hat{\mathbb{E}}\big[y^2(t)\big]$ is measured at the controller side and $\hat{\mathbb{E}}\big[x^2(t)\big]$ is known from the typical properties of the sensor signal, then SNR can be estimated for this case as shown above.

2) Additive FDI Attack: Let the additive FDI signal be denoted as $f_a(t)$, then the received signal is expressed as $y(t) = x(t) + n(t) + f_a(t)$. The attack signal is assumed to be independent of the transmitted signal $x(t)$. Calculating the second moment of the received signal yields $\mathbb{E}\big[y^2(t)\big] = \mathbb{E}\big[x^2(t)\big] + \mathbb{E}\big[n^2(t)\big] + \mathbb{E}\big[f_a^2(t)\big]$. This leads to an SNR value of

$$\text{SNR} = \frac{\mathbb{E}\big[x^2(t)\big]}{\mathbb{E}[n^2(t)] + \mathbb{E}[f_a^2(t)]}\,. \tag{32}$$

Noting that $\hat{\mathbb{E}}\big[n^2(t)\big] + \hat{\mathbb{E}}\big[f_a^2(t)\big] = \hat{\mathbb{E}}\big[y^2(t)\big] - \hat{\mathbb{E}}\big[x^2(t)\big]$, the SNR is estimated as $\hat{\mathbb{E}}\big[x^2(t)\big] / \Big(\hat{\mathbb{E}}\big[y^2(t)\big] - \hat{\mathbb{E}}\big[x^2(t)\big]\Big)$.

3) Multiplicative FDI Attack: This is a case where the FDI attack amplifies the transmitted signal by a gain factor. Denote $f_m(t) = c.x(t)$ as the multiplicative FDI signal, then the received signal is $y(t) = x(t) + n(t) + f_m(t) = (1 + c)x(t) + n(t)$. Thus, the SNR value is calculated from

$$\text{SNR} = \frac{(1+c)^2\mathbb{E}\big[x^2(t)\big]}{\mathbb{E}[n^2(t)]}\,. \tag{33}$$

To estimate the SNR value, we calculate the second and fourth central moments of $y(t)$ as

$$\begin{aligned}\mathbb{E}\big[y^2(t)\big] &= (1+c)^2\mathbb{E}\big[x^2(t)\big] + \mathbb{E}\big[n^2(t)\big]\\ \mathbb{E}\big[y^4(t)\big] &= (1+c)^4\mathbb{E}\big[x^4(t)\big] + \mathbb{E}\big[n^4(t)\big]\\ &\quad + 6(1+c)^2\mathbb{E}\big[x^2(t)\big]\mathbb{E}\big[n^2(t)\big]\end{aligned} \tag{34}$$

where $\mathbb{E}\big[n^4(t)\big] = 3(\mathbb{E}\big[n^2(t)\big])^2$ [36]. The second and fourth moments of $y(t)$ can be estimated by time-averaging the received measurements power and fourth moments. Solving for $\mathbb{E}\big[n^2(t)\big]$ and $(1+c)^2$ in (34) enables estimating the SNR value in (33). More information about the moment-based SNR estimation can be found in [37].

C. Design Parameter versus Measurement Uncertainty

As shown in (17) and (18), a higher value of the parameter α_i makes the PFL controller more aggressive and it moves the nonzero eigenvalue deeper in the left-hand complex plane; thus, high α_i speeds up the transient stability of the system generators (i.e., it reduces the stability time). However, higher values of α_i require more control power as (15) shows. Consequently, when the cyber system has no disturbance issues, the PFL controller can be made as aggressive as possible as long as it satisfies

the control power constraints. Further, when the PFL controller receives measurements with higher degrees of noise, FDI infiltration, interference, or communication latency, the controller can adapt its parameter according to the level of uncertainty in the measurements. The results in (27) emphasize the relationship between the uncertainty and α_i, where the PFL controller becomes less aggressive and reduces the value of α_i when it faces lower-fidelity measurements. However, as the uncertainty about the accelerating power can be more pronounced compared to that of the rotor speed, the PFL controller can be made more aggressive with a higher value of α_i as observed in (29); thus, this leads to relatively moderate values of α_i in the low-SNR region.

Specifically, we start with a "potential" piece-wise linear relationship between α_i and SNR. When considering the SNR scale in dBs, the relationship between α_i and SNR_i can be approximated as a constant line for low SNR values. Furthermore, for the medium-SNR region, the value of α_i increases as a function of SNR, and it is approximated as a line with a positive slope. When SNR is high, the value of α_i can exceed the maximum allowed due to the constraints on control power; consequently, α_i can be set as the maximum allowed when the SNR value is high. Hence, the PFL control is proposed to adapt α_i against SNR according to:

$$\alpha_i = \begin{cases} \alpha_u & \text{SNR}_i \geq \text{SNR}_{\max} \\ a_s + b_s\,\text{SNR}_i & \text{SNR}_{\min} < \text{SNR}_i < \text{SNR}_{\max} \\ \alpha_l & \text{SNR}_i \leq \text{SNR}_{\min} \end{cases} \quad (35)$$

where a_s, b_s, $\text{SNR}_{\max}$, $\text{SNR}_{\min}$, and $\alpha_l < \alpha_u$ are specific to the power system, α_u depends on the control power constraint, and all SNR values are in dBs.

D. Design Parameter versus Measurement Latency

Communication latency between sensors and controllers is an aggregate result of processing and propagation delays in the communication network, and it can vary depending on the communication protocols, communication medium, and topology. Sensor sampling, quantization, and cryptographic delays can add to queueing delays to contribute to the overall latency. DoS attacks can also degrade communications links and cause excessive delays. Total latency is also affected by intermediate nodes (for example, data concentrators) between sensors and controllers. A phasor measurement unit (PMU) is a sensing device that can provide time-stamped periodic measurements at a high rate. Assuming all devices have GPS clocks, estimating latency between the sensors and the controller can be accomplished by observing the time when the measurement is received and the time-stamp when the measurement was created. This measure can give an estimate of the total delay between the sensors and the controllers.

Denote communication latency as τ; then, following the recommendations of [19], [20], the PFL controller updates α_i as a function of τ as:

$$\alpha_i(\tau) = \begin{cases} \alpha_u & \tau_i \leq \tau_{\min} \\ a_\tau + b_\tau\,\tau_i & \tau_{\min} < \tau_i \leq \tau_{\max} \end{cases} \quad (36)$$

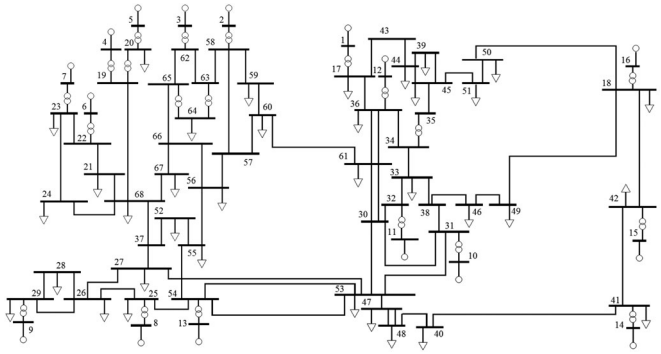

Fig. 3. Single line diagram of the IEEE 68-bus 16-machine test power system.

where a_τ, b_τ, $\tau_{\min}$, and $\tau_{\max}$ are specific to the power system under study. However, if τ exceeds $\tau_{\max}$ and the controller cannot efficiently stabilize the power grid, then the it switches to a decentralized PFL control mode where it relies only on local measurements of the rotor speed; in this case, the local-mode control signal appears as $\hat{u}_i(t) = -\alpha_i(\omega_i(t) - \omega_s)$.

The PFL control is proposed to be adaptive to the cyber state of the smart grid in (35) and (36). However, to take the physical state of the smart grid into consideration, the PFL controller can adapt its design parameter according to the severity of the disturbance. Specifically, the controller can be made more aggressive by employing a higher value of α_i for longer physical disturbances or for delayed activation of the controller. When the power system is subjected to a longer disturbance, its dynamics move farther from the steady-state stable values. Accordingly, the smart grid system needs a more aggressive controller to bring it back to stability. Similarly, when the PFL controller is not activated immediately after the onset of the disturbance, the system dynamics change fast and move away from the stability margin. Consequently, given it is already activated late, a more aggressive PFL controller can stabilize the already-in-severe-state power system faster.

V. Analysis of the Controller Parameter

In this section we quantify the design parameter of the adaptive PFL controller to enhance its performance against cyber attacks on data integrity and availability. The IEEE New York-New England 68-bus test power system (shown in Fig. 3) is used for numerical simulations in order to verify the control scheme. Six faults are considered on the test power system at Buses 24, 26, 30, 37, 38, and 66, where each fault lasts for 5 cycles (i.e., 83.3 ms). The PFL control is activated immediately following the disturbance, and every ESS in the system has a maximum capacity of 2.5% of the mechanical power of the corresponding generator.

A. Adaptive Control to Data Integrity Disturbances

Given $\alpha_i = \beta_i D_i$ as defined in (15), Fig. 4(a) illustrates the optimal values of β_i that achieve the lowest stability time for any given SNR value. Consistent with the observations above, the general trend for the optimal β_i is that it is relatively low for low SNR values and it increases when the SNR values increase.

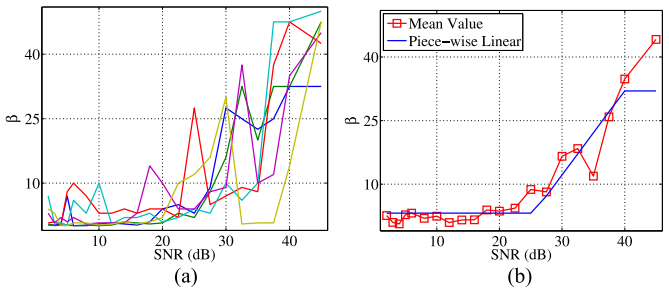

Fig. 4. Relation between β and SNR. (a) Optimal β_i versus SNR for different faults. (b) Piece-wise linear relationship between β_i and SNR.

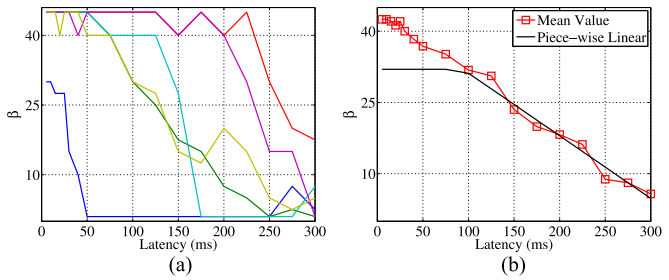

Fig. 5. Relation between β and latency. (a) Optimal β_i versus latency for different faults. (b) Piece-wise linear relationship between β_i and latency.

Fig. 4(b) shows the average β_i value for the six faults from Fig. 4(a). Further, a curve-fitting approach is used to find the piece-wise linear relationship between β_i and SNR as suggested in (35). Assuming the maximum value of β_i is 32, the value of β_i can then be varied versus SNR (in dBs) as:

$$\beta_i(\text{SNR}_i) = \begin{cases} 32 & \text{SNR}_i \geq 40 \\ -47.5 + 2\,\text{SNR}_i & 25 < \text{SNR}_i < 40 \\ 3.2 & \text{SNR}_i \leq 25\,. \end{cases} \tag{37}$$

Consequently, the PFL controller adapts to measurement uncertainties by being less aggressive when the measurements are corrupted to a greater degree with noise, interference, FDI attacks, and communication latencies. Conversely, with higher measurement quality, the SNR value becomes higher and the PFL controller increases its aggressiveness.

B. Adaptive Control to Data Availability Disturbances

The optimal values of β_i versus communication latency are shown in Fig. 5(a) for the six faults; it is shown that the optimal β_i generally decreases as τ increases. Observing the mean value of the optimal β_i s and following (36), the piece-wise linear relationship between β_i and τ is displayed in Fig. 5(b). In this case, the relation between the control design parameter and the latency (in ms) is expressed as:

$$\beta_i(\tau_i) = \begin{cases} 32 & \tau_i \leq 95 \\ 44 - 0.132\,\tau_i & 95 < \tau_i \leq 310\,. \end{cases} \tag{38}$$

Consistent with our SNR findings, the controller is most aggressive when the communication latency (and subsequent measurement uncertainty) is small. As the delay increases, the PFL controller becomes less aggressive in a linear fashion. If the latency exceeds the maximum limit, the PFL controller can switch to a local control mode that relies on local measurements of rotor speed as

$$\hat{u}_i(t) = -\alpha_i(\omega_i(t) - \omega_s)\,. \tag{39}$$

Due to the missing accelerating power component, this mode of control usually takes longer time to stabilize the associated synchronous generator.

C. Adaptive Control to Integrity and Availability Disturbances

The case of simultaneous data integrity and availability attacks is considered in this section. Observing (37), the design parameter generally increases with increasing SNR values; further, the controller adapts to increased values of communication latency in (38) by decreasing the design parameter value. Consequently, to address simultaneous SNR and latency issues, the PFL controller implements the same approach (i.e., it increase β_i for increasing SNR_i or decreasing τ_i). The controller can select the design parameter to be the minimum value of both separate cases. In other words, the PFL is proposed to vary β_i as a function of SNR_i and τ_i as

$$\beta_i(\text{SNR}_i, \tau_i) = \min\left(\beta_i(\text{SNR}_i), \beta_i(\tau_i)\right) \tag{40}$$

where $\beta_i(\text{SNR}_i)$ and $\beta_i(\tau_i)$ are the piece-wise linear relationships defined in (37) and (38), respectively.

VI. Numerical Results

In this section we evaluate the performance of the adaptive PFL controller against SNR and communication latency using the IEEE 68-bus test power system. The design parameter (α_i) is varied depending on the state of the cyber network as presented in Section V.

A. Simulation Environment

The test power system has 16 synchronous generators and 68 buses. The parameters of this power system are extracted from [38], and the simulation environment follows the guidelines in [24]; more details are found in [39]. Generators 14, 15, and 16 of the test power system represent equivalences of other interconnected power networks; thus, these generators along with Generator 13 (the slack-bus generator) have high inertia constants. Further, Generators 1 to 12 are equipped with fast excitation systems, and Generator 9 is equipped with a power system stabilizer. In addition, there are three double-circuit tie-lines connecting Buses $60-61$, $53-54$, and $27-53$.

The test power system is simulated using Matlab and Simulink tools, and the two-axis sub-transient machine model is used. Fourth-order Runge-Kutta method is used to solve the differential equations in (1)–(6) along with other power control schemes. The system state is measured periodically and transmitted to the control agents. The value of the control design parameter is adapted depending on the cyber state. The control signal u_i is calculated and fed to the nonlinear simulator periodically. For each simulation test, the stability time is calculated following the recommendations in [40].

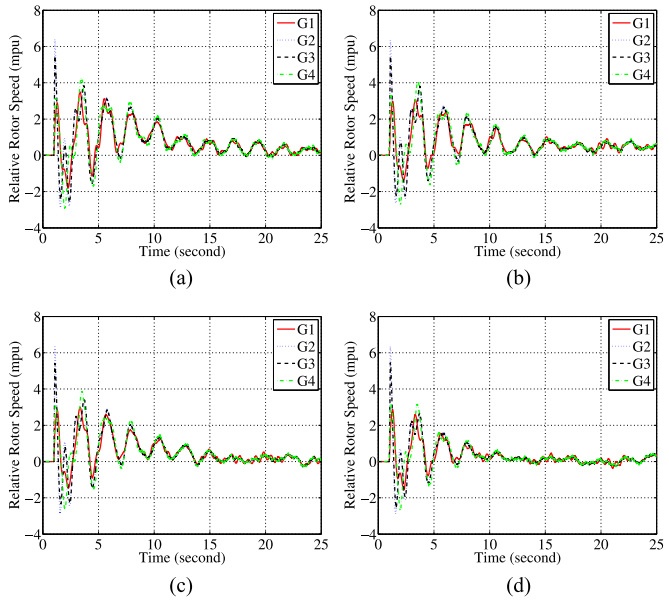

Fig. 6. Sample rotor speed for different values of SNR for a fault at Bus 60. (a) SNR = 10 dB, (b) SNR = 20 dB, (c) SNR = 30 dB, (d) SNR = 40 dB.

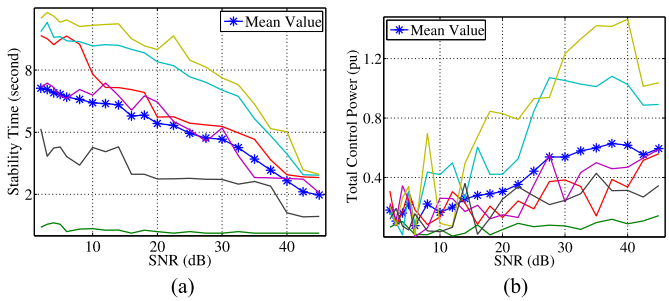

Fig. 7. Performance versus SNR (adaptive control). (a) Stability time versus SNR. (b) Control power versus SNR.

B. Performance Versus Data Integrity Attacks

First, we investigate the performance of the PFL controller versus disturbances against data integrity of the cyber network, which can be translated into measurement uncertainties. The findings of (37) are used to adapt the value of β_i given a specific SNR value. The values of $\omega_i - \omega_s$ for the first four generators are shown in Fig. 6 for sample SNR values. It is shown that as the SNR value increases, the relative rotor speed decays faster to zero, which is an indication of stability. Further, Fig. 7 displays the stability time and required control power for the six faults mentioned above. It is shown here that because the PFL controller adapts its design parameter, the controller effectively stabilizes the power system during a wide range of SNR values.

Fig. 8 demonstrates the performance when the PFL controller's design parameter is not adapted to SNR, where the value of $\alpha_i = 3.2D_i$ is used. Comparing the findings in Fig. 8 with those of the proposed case in Fig. 7, it is observed that the controller takes longer times to stabilize and it uses more ESS power during the stabilization process. The value of the proposed PFL control is evident since it is a good merit of the controller to achieve stability faster and with less power.

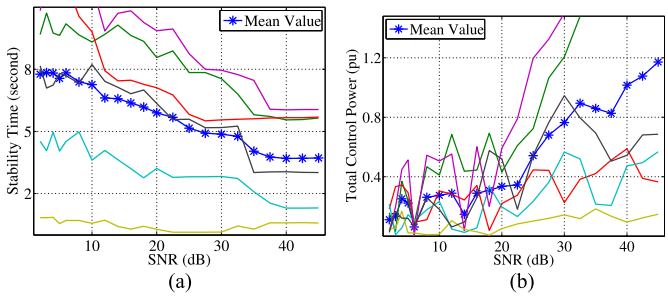

Fig. 8. Performance versus SNR (non-adaptive control). (a) Stability time versus SNR. (b) Control power versus SNR.

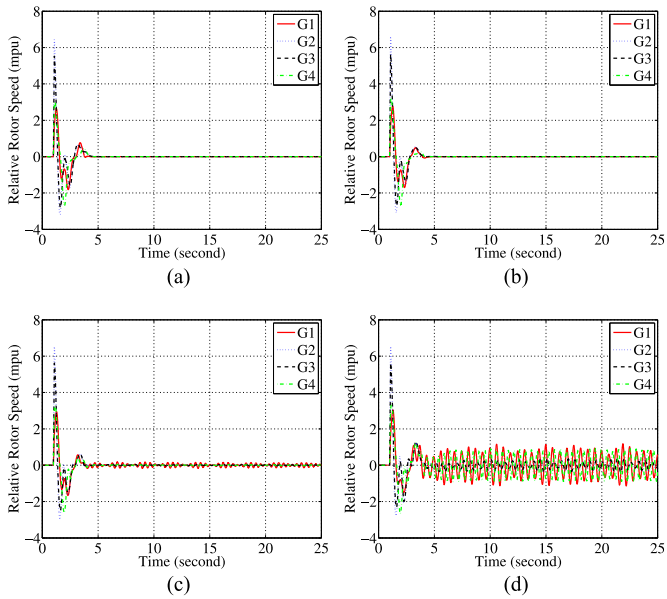

Fig. 9. Sample rotor speed for different values of latency for a fault at Bus 60. (a) τ = 50 ms. (b) τ = 100 ms. (c) τ = 200 ms. (d) τ = 300 ms.

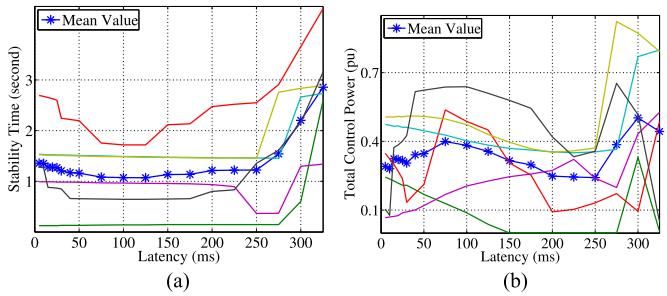

Fig. 10. Performance versus latency (adaptive control). (a) Stability time versus latency. (b) Control power versus latency.

C. Performance Versus Data Availability Attacks

Next, we capture the performance of the proposed controller versus cyber attacks on data availability, which is represented in this work as communication latency. Thus, following the design recommendations for β_i in (38), Fig. 9 shows the relative rotor speed for sample latency values, and it is observed that increasing the value of τ leads to longer times to stabilize the generators. Fig. 10 also illustrates the performance of the adaptive PFL controller versus latency (τ). The controller efficiently stabilizes the power system generators, and both stability time

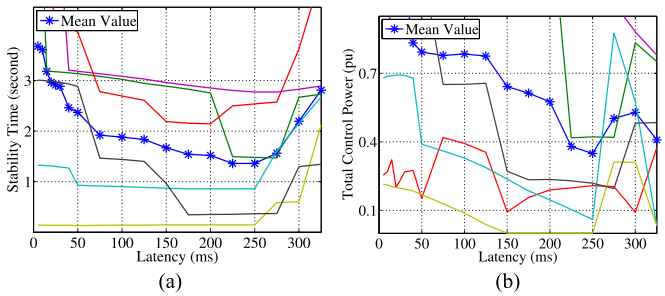

Fig. 11. Performance versus latency (non-adaptive control). (a) Stability time versus latency. (b) Control power versus latency.

and control power do not vary extensively over a wide range of τ. It is observed that the PFL controller adapts well up to delays of 300 ms; as the latency far exceeds this threshold, the PFL controller switches to a local control mode.

For the sake of comparison, Fig. 11 shows the controller's performance when $\alpha_i = 3.2D_i$ is used for all values of latency. It is observed that the non-adaptive controller requires more control power and takes more time to stabilize the power system. Thus, by comparing Figs. 10 and 11, the advantage of the proposed adaptive control scheme is evident.

D. Discussion

As expected from the controller design, stability time is enhanced (i.e., becomes shorter) with increasing α_i; this happens when the PFL controller receives high-fidelity measurements at the high-SNR and the low-latency regions as shown in (37) and (38), respectively. Further, as the controller becomes more aggressive, more control power is generally required to stabilize the power system. The PFL control scheme is proposed to be less aggressive when SNR is low or when communication latency is high; thus, the adaptive controller typically takes longer time to achieve stability. The above results demonstrate that the adaptive PFL controller can efficiently react to cyber attacks on the communication network that target data integrity and availability.

It is observed in Fig. 4 that the optimum value of β_i increases with the increasing SNR. However, instead of adapting the controller to each specific fault, we propose to look at the average behavior of different faults and infer a useful pattern. The general approach (i.e., taking the average) works nicely with all faults as seen in Fig. 7 where stability time keeps going down with increasing SNR values. Exhausting all possible types of faults can fine tune the adaption equation in (37). A small dip is noted around SNR $= 35$ dB in Fig. 4(b); however, applying the piece-wise linear curve in (37) yields a smooth stability time as shown in Fig. 7(a). Similar observations can be drawn for the results of communication latency.

It is to be noted that total control power is usually a function of the aggressiveness of the controller, stability time, and location of the fault. We observe that as the PFL controller becomes more aggressive with increasing SNR values as described in (37), total control power generally increases as observed in Fig. 7(b). On the other hand, control power starts to slightly increase with increasing latency for the first 95 ms, which is when the design parameter is constant; however, with increasing values of latency, the PFL controller starts to become less aggressive as defined in (38), and so less control power is generally utilized. Finally, for higher values of latency ($\tau_i \geq 250$ ms), the controller takes longer times to stabilize the system generator and thus it requires more ESS power.

VII. Conclusion

In this work we consider a distributed control paradigm to aid in the security of cyber-physical smart grid systems. We focus on the problem of transient stability and propose a tractable cyber-enabled adaptive control scheme based on feedback linearization control. The distributed control scheme affects the dynamics of the power system through power injection and absorbtion via ESSs, and it is parameterized through an aggressiveness design parameter. We consider the problem of attacks on data integrity and availability in the cyber component of the smart grid. The cyber state includes information about the noise level, interference, false data injections, and communication latency. The distributed controller is proposed to adapt its design parameter as a function of the cyber state of the smart grid and also depending on the severity of the physical disturbance.

The adaptive controller is proposed to be aggressive in stabilizing the power system when it receives high-fidelity measurements and when communication delay is low. However, when the measurements are highly-corrupted or when the latency is excessive, the control scheme becomes less aggressive. The numerical results, simulated on the IEEE 68-bus test power system, demonstrate that the proposed adaptive control scheme is efficient, yet simple, in stabilizing the power system during cyber and physical disturbances.

Acknowledgment

The authors thank Dr. Ahmed M. Khalil at the University of Toronto for his help in simulating the power system.

References

[1] 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.

[2] 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. Gen. Meet.*, Jul. 2012, pp. 1–6.

[3] 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. Gen. Meet.*, Jul. 2014, pp. 1–5.

[4] 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.

[5] A. Vahidnia, G. Ledwich, and E. W. Palmer, "Transient stability improvement through wide-area controlled SVCs," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 3082–3089, Jul. 2016.

[6] M. Andreasson, D. Dimarogonas, K. Johansson, and H. Sandberg, "Distributed vs. centralized power systems frequency control," in *Proc. Eur. Control Conf.*, Jul. 2013, pp. 3524–3529.

[7] 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.

[8] 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, pp. 1750–1764, Jul. 2014.

[9] A. Farraj, E. Hammad, and D. Kundur, "A cyber-enabled stabilizing controller for resilient smart grid systems," in *Proc. IEEE PES Conf. Innov. Smart Grid Technol.*, Feb. 2015, pp. 1–5.
[10] 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.
[11] R. Hadidi and B. Jeyasurya, "A real-time multiagent wide-area stabilizing control framework for power system transient stability enhancement," in *Proc. IEEE Power Energy Soc. Gen. Meet.*, pp. 1–8, 2011.
[12] 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. Informat.*, to be published.
[13] 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, pp. 13–33, Jun. 2011.
[14] S. Liu, X. P. Liu, and A. El Saddik, "Denial-of-Service (DoS) attacks on load frequency control in smart grids," in *IEEE PES Innov. Smart Grid Technol.*, 2013, pp. 1–6.
[15] J. Nilsson, B. Bernhardsson, and B. Wittenmark, "Stochastic analysis and control of real-time systems with random time delays," *Automatica*, vol. 34, pp. 57–64, Jan. 1998.
[16] S. Zhang and V. Vittal, "Design of wide-area power system damping controllers resilient to communication failures," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4292–4300, Nov. 2013.
[17] H. Wu, K. S. Tsakalis, and G. T. Heydt, "Evaluation of time delay effects to wide-area power system stabilizer design," *IEEE Trans. Power Syst.*, vol. 19, no. 4, pp. 1935–1941, Nov. 2004.
[18] B. Chaudhuri, R. Majumder, and B. C. Pal, "Wide-area measurement-based stabilizing control of power system considering signal transmission delay," *IEEE Trans. Power Syst.*, vol. 19, no. 4, pp. 1971–1979, Nov. 2004.
[19] 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.*, pp. 768–773, Nov. 2015.
[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] 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.
[22] F. Dörfler and S. Grammatico, "Amidst centralized and distributed frequency control in power systems," in *Proc. Amer. Control Conf.*, 2016, pp. 5909–5914.
[23] Y. Xiang, L. Wang, and N. Liu, "A robustness-oriented power grid operation strategy considering attacks," *IEEE Trans. Smart Grid*, to be published.
[24] P. Sauer and M. Pai, *Power System Dynamics and Stability*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1998.
[25] J. Glover, M. Sarma, and T. Overbye, *Power System Analysis and Design*, 5th ed. Independence, KY, USA: Cengage Learn., 2011.
[26] A. Bergen and V. Vittal, *Power Systems Analysis*, 2nd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2000.
[27] P. F. Ribeiro, B. K. Johnson, M. L. Crow, A. Arsoy, and Y. Liu, "Energy storage systems for advanced power applications," *Proc. IEEE*, vol. 89, no. 12, pp. 1744–1756, Dec. 2001.
[28] A. Ruddell, "Investigation on storage technologies for intermittent renewable energies: Evaluation and recommended R&D strategy," CCLRC-Rutherford Appleton Laboratory, Chilton, U.K., Storage Technol. Rep. ST6: Flywheel, 2003. [Online]. Available: www.itpower.co.uk/investire/pdfs/flywheelrep.pdf
[29] G. O. Cimuca, C. Saudemont, B. Robyns, and M. M. Radulescu, "Control and performance evaluation of a flywheel energy-storage system associated to a variable-speed wind generator," *IEEE Trans. Ind. Electron.*, vol. 53, no. 4, pp. 1074–1085, Jun. 2006.
[30] E. Furlong and W. Wiltsch, "Performance and operational characteristics of an advanced power system," GE Library, 2010.
[31] T. T. Leung, "Concept of a modified flywheel for megajoule storage and pulse conditioning," *IEEE Trans. Magn.*, vol. 27, no. 1, pp. 403–408, Jan. 1991.
[32] H. Khalil, *Nonlinear Systems*, 3rd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2002.
[33] K. Purchala, L. Meeus, D. Van Dommelen, and R. Belmans, "Usefulness of DC power flow for active power flow analysis," in *IEEE Power Eng. Soc. Gen. Meet.*, Jun. 2005, pp. 454–459.
[34] E. Sjödin, "The price of synchrony: evaluating transient power losses in renewable energy integrated power networks." M.S. thesis, KTH School of Electrical Engineering, Stockholm, Sweden, Aug. 2013.
[35] P. Kundur, *Power System Stability Control* (EPRI Power System Engineering Ser.), New York, NY, USA: McGraw-Hill, 1994.
[36] A. Papoulis and S. U. Pillai, *Probability, Random Variables Stochastic Processes*, Columbus, OH, USA, Tata McGraw-Hill Education, 2002.
[37] 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, 2010.
[38] B. Pal and B. Chaudhuri, *Robust Control Power System*. Power Electronics and Power Systems Series, Springer, 2006.
[39] 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," Tech. Rep., IEEE Power and Energy Society, Dec. 2013.
[40] Ontario Independent Electricity System Operator (IESO), "Ontario Power System Restoration Plan." http://www.ieso.ca. Issue 11.0: 31 Jan. 2016, Accessed: 28 Jul. 2016.

Abdallah Farraj (S'11–M'12) received the B.Sc. and M.Sc. degrees from the University of Jordan, Amman, Jordan, in 2000 and 2005, respectively, and the Ph.D. degree in from Texas AM University, College Station, TX, USA in 2012, all electrical engineering . He is currently a Postdoctoral Fellow at the University of Toronto. He is also a Fulbright Scholar. His research interests include modeling and analysis of cyber-physical systems, cyber security 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 AM University, College Station, TX, USA, both in electrical engineering. She is working toward the Ph.D. degree in the Department of Electrical Engineering, University of Toronto, Toronto, ON, Canada. Her 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 received many awards, and is currently 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 in electrical and computer engineering from the University of Toronto, Toronto, ON, Canada, in 1993, 1995, and 1999, respectively.

She is currently the Chair of the Division of Engineering Science and a Professor of electrical and computer engineering at the University of Toronto. From January 2003 to December 2012, she was a Faculty Member in the Department of Electrical and Computer Engineering, Texas A&M University, and from September 1999 to December 2002, she was a Faculty Member in the Department of Electrical and Computer Engineering, University of Toronto. She is an author of more than 150 journal and conference papers. Her research interests include interface of cyber security, signal processing, and complex dynamical networks.

Prof. Kundur has participated on several editorial boards and currently serves on the Advisory Board of IEEE Spectrum. She is currently the Symposium Co-Chair of the Communications for the Smart Grid Track of ICC 2017 and the TPC Co-Chair of the IEEE SmartGridComm 2018. Recently, she was also the General Chair of the Workshop on Communications, Computation and Control for Resilient Smart Energy Systems at ACM e-Energy 2016, General Chair of the Workshop on Cyber-Physical Smart Grid Security and Resilience at Globecom 2016, General Chair of the Symposium on Signal and Information Processing for Smart Grid Infrastructures at GlobalSIP 2016, General Chair of the 2015 International Conference on Smart Grids for Smart Cities, General Chair of the 2015 Smart Grid Resilience Workshop at IEEE GLOBECOM 2015, and General Chair of the IEEE GlobalSIP'15 Symposium on Signal and Information Processing for Optimizing Future Energy Systems. Her 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 and 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 awards at both the University of Toronto and Texas A&M University. She is a Fellow of the Canadian Academy of Engineering.