This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2581588, IEEE Transactions on Smart Grid

A Cyber-Physical Control Framework for Transient Stability in Smart Grids

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

***Abstract*—Denial of service attacks and communication latency pose challenges for the operation of control systems within power systems. Specifically, excessive delay between sensors and controllers can substantially worsen the performance of distributed control schemes. In this article, we propose a framework for delay-resilient cyber-physical control of smart grid systems for transient stability applications. The proposed control scheme adapts its structure depending on the value of the latency. As an example, we consider a parametric feedback linearization (PFL) control paradigm and make it "cyber-aware." A delay-adaptive design that capitalizes on the features of PFL control is presented to enhance the time-delay tolerance of the power system. Depending on the information latency present in the smart grid, the parameters and the structure of the PFL controller are adapted accordingly to optimize performance. The improved resilience is demonstrated by applying the PFL controller to the New England 39-bus and WECC 9-bus test power systems following the occurrence of physical and cyber disturbances. Numerical results show that the proposed cyber-physical controller can tolerate substantial delays without noticeable performance degradation.**

***Index Terms*—Cyber-physical systems, distributed control, distributed energy resources, smart grid, system resilience, time-delay tolerance, transient stability.**

I. Introduction

Modern power grids employ control, communications, and sensor technologies to improve resilience and efficiency. Such smart grid technologies can allow bidirectional information flow. In addition, the integration of more renewable energy sources into the power grid can enable nontraditional control schemes. However, reliability of the cyber and physical assets of the smart grid is a paramount priority.

Cyber and physical disturbances can affect the performance of smart grids. Events that lead to disruption include denial of service attacks, false data injection attacks, cyber-physical switching attacks, and physical faults. Resilience against attacks and faults must be addressed through a defense-in-depth paradigm whereby prevention, detection, and reaction approaches for protection are employed at various levels.

Preventative defence approaches employ mechanisms that obstruct the execution of an attack in order to limit its impact on power systems. Examples of preventative strategies include encryption and secure communication protocols that represent an initial level of defense against cyber intrusions [1], [2]; relays and circuit breakers are also a form of initial defense to prevent the propagation of a severe fault [3], [4]. Detection strategies are employed when preventive defense approaches are unsuccessful in thwarting a disturbance; these strategies use models of abnormal behavior as well as system measurements to identify anomalies. Detection techniques can be used to detect the occurrence of an unwanted system state [5], successful cyber attack [6], or a combination of both [7]. Furthermore, reaction approaches involve using strategies to recover from a disturbance and include techniques to control system operation [8]. In this work we focus on this last strategy, specifically to enhance power grid resilience through the use of distributed controllers.

Parametric feedback linearization (PFL) distributed controllers are recently proposed in [9] and [10] to address transient stability of power systems following the occurrence of a physical disturbance. The PFL controller utilizes an external energy storage system (ESS) to inject and absorb power from the system in order to stabilize rotor speed and achieve phase cohesiveness among the system generators.

For this work, we adopt a general multi-agent framework that enables system level studies and cyber-physical interaction modeling. We focus on the transient stability problem which is ideal for investigating cyber-physical dependencies within a tractable paradigm. Other relevant issues including voltage and small-signal stability and wide-area control are beyond the scope of this work. In addition, we specifically analyze and apply the PFL controller in this study. Further, the framework incorporates the effects of denial of service (DoS) and switching attacks. Specifically, we focus on control strategies to provide greater resilience to these attacks.

In this article a framework for cyber-physical control in smart grid systems is proposed where the controller adapts its structure and parameters based on communication latency and the state of the cyber component of the grid. Further, a delay-adaptive design is presented for the PFL controller. Moreover, the delay-adaptive characteristic function of the PFL controller is evaluated for the New England 39-bus and WECC 9-bus test power systems. Also the performance of the proposed cyber-physical control is numerically evaluated when the power system undergoes cyber and physical disturbances.

The rest of this paper is organized as follows. The problem setting and the proposed framework are presented in Sections II and III. A cyber-enabled PFL control is detailed in Section IV. Sections V and VI investigate the performance of the controller under the proposed design. Conclusions and final remarks are shown in Section VII.

This work was supported by the US National Science Foundation under grant ECCS-1028246 and the Natural Sciences and Engineering Research Council of Canada under grant RGPIN 227722. A. Farraj, E. Hammad, and D. Kundur are with the Department of Electrical and Computer Engineering at University of Toronto, Email: {abdallah, ehammad, dkundur}@ece.utoronto.ca.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2581588, IEEE Transactions on Smart Grid

II. Control for Resilient Smart Grids

The concept of resilience refers to the ability of a given system to bounce back from an external or internal disruption. Power system resilience is linked to the traditional concept of *power system security* that refers to the ability of a power grid to remain intact despite a physical contingency.

According to [11], power system control can be classified into mechanical and electrical. Mechanical control subsystems include fuel supply, boiler pressure, and turbine speed controls. Electrical control includes generator voltage, network, and load controls. Both categories of control are coupled through an energy control center. The associated system dynamics can be classified according to the time scale of a phenomena [11]. For example, transient stability and governor control have time scale ranges from around a fraction of a second to tens of seconds, respectively.

Transient stability describes the ability of the power system to remain in synchronism when subjected to large disturbances. Transient stability during the presence of a physical fault can be achieved by maintaining both rotor speed synchronization and phase angle cohesiveness. Speed synchronization requires the rotor speeds of all the generators to agree asymptotically with a common value typically set to 60 Hz and normalized in this paper to 0. Phase angle cohesiveness means that the difference between the phase angle of the different generators in the power system should be below a predefined threshold typically chosen to be 100°.

Circuit breakers are used as a first line of defense to clear the faults within a power system. In transient stability studies, it is of interest to compute the critical clearing time of these circuit breakers. The critical clearing time is related to the maximum power transfer in the pre-fault state of the power system [11]. A traditional way of assessing a power system's transient stability is to study transient energy functions based on Lyapunov's method. For multi-machine power systems, potential energy boundary surface (PEBS) and boundary controlling unstable equilibrium points (BCU) are widely used. More information about traditional analysis of the angle stability problem in power systems can be found in [11, Chapter 9].

The movement to a *smarter* grid involves the marriage of information technology with power delivery components. Smart grid cyber assets include the communications network infrastructure, information technology systems, computing elements, data storage, and distributed controllers. Cyber data is collected over the power grid using sensors; for example, phasor measurements units (PMUs) can be used to report time-stamped voltage and current readings from different locations around the power grid. This data is then transferred to distributed or centralized controllers via communication links. The timely availability of high-granularity system data facilities new control schemes to better stabilize the power system after the occurrence of a disturbance.

Wide-area monitoring Systems (WAMS) improve overall system reliability through situational awareness and advanced decision-making and control. PMUs are used to read current and voltage phasors at the substation bus on the transmission power network and send the readings at a specific rate to phasor data concentrators (PDCs). PMUs use global position system (GPS) clocks to synchronize and time-stamp the readings in order to enable a direct access to the state of the power grid. Further, a PDC receives 30-200 synchrophasor reports from PMUs per second, and it aligns the data from the multiple PMUs to provide a view of the overall power grid. PMU-based wide-area control and monitoring applications are of interest to the smart grid community as successful operation of such applications requires careful treatment of delays in the communication network. Examples of recent work include [12]–[17].

Cyber security issues of smart grid systems have recently surfaced due to the increased implementation of smart grid applications. It is observed that the shift to a cyber-enabled power grid also introduces new system vulnerabilities that exploit information systems which can lead to growing potential for cyber and physical attacks on the power grid. Common classes of cyber and physical attacks on smart grid systems include:

- False data injection attacks against state estimation: an adversary exploits the configuration of the power system to introduce an arbitrary error into certain state variables while bypassing existing techniques for bad measurement detection [18];
- Denial of service attacks: an adversary interrupts the operation of the cyber component of the power grid by jamming the communication channels, attacking networking protocols, and flooding the network traffic. This attack leads to causing communication link failure and excessive delays and consequently results in preventing the timely exchange of information between the sensors, actuators, and control systems [19];
- Switching attacks: an adversary causes physical disturbance in the power system by switching on and off one or more elements of the grid to cause instability within the power system. Effective switching attacks could be, for example, based on understanding the structure of the power system and accessing system state information [20]–[22].

Such types of attacks can lead to system instability. Given the high degree of recent research activity in false data injection attacks, we focus in this work on the lesser investigated DoS and switching attacks.

Both cyber and physical disturbances can affect the performance of smart grid systems. Distributed control schemes that rely on the availability of a cyber network present opportunities to enhance the stability and resilience of the power grid by mitigating certain types of cyber and physical disturbances. Recent research activity in this area includes [9], [10], [23]–[26]. However, the impact of cyber attacks and communication latency on the performance of such control schemes must be carefully studied in order to fully understand best practices for resilience.

We assert in this paper that resilience to cyber and physical attacks must be more carefully addressed given the intentional and targeting nature of the disturbance. Further, we believe that a distributed control paradigm is an appropriate response strategy to cyber attack. Essentially the process of control lies

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2581588, IEEE Transactions on Smart Grid

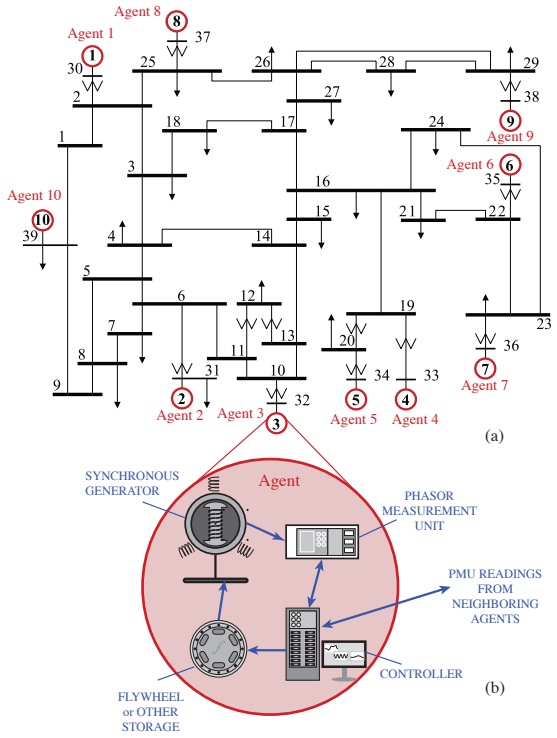


Fig. 1. Multi-agent smart grid system. (a) New England test power system (b) Cyber-physical agent

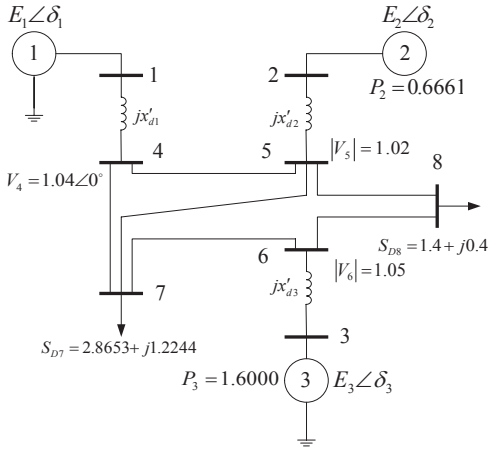


Fig. 2. WECC test power system

at the *cyber-physical interface* of the smart grid whereby it makes use of sensor information to make decisions and actuate change on the physical system. Thus the control process has the ability to inhibit the propagation of a cyber attack to the (physical) power delivery network placing it at an effective location within the overall smart grid. Consequently, we propose in this work a cyber-physical control framework to mitigate intentional disturbances (DoS and switching attacks) and achieve transient stability in the face of naturally-occurring faults.

III. A Framework for Cyber-Physical Control

In this section we adopt a general multi-agent framework to model the smart power grid. This framework enables system level studies and cyber-physical interaction modeling.We focus on control strategies that provide greater resilience against faults, DoS attacks, and switching attacks.

A. System Model

We assume that the smart grid is comprised of N cyber-physical agents where each agent contains a synchronous generator, an associated sensor that provides information on generator rotor angle and speed, a distributed controller that processes sensor data from local and neighboring agents, and a fast-acting ESS that can inject or absorb real power in the system depending on the value of the control signal. Further, a communication network connects the sensors, ESSs, and distributed controllers of the smart grid system. The overall multi-agent system is considered to be cyber-physical in nature. The physical dynamics of each agent can depend on its own state (specifically, the state of its generator) as well as the states of other agents in the system. As an example, we consider the New England 10-generator 39-bus (physical) test power system with associated cyber-physical agents as shown in Fig. 1.

Traditionally, a centralized physical controller refers to a scheme where the states of all agents need to be collected for processing and decision making; this control approach may require a significant communication overhead which leads to potential cyber attacks. On the other hand, a decentralized controller would only require the state of its own agent; this control scheme eliminates the need for significant communication infrastructure. However, a decentralized approach may experience long convergence times for the controller tasks. Furthermore, the controller makes use of its own local state and those of its neighbors in a distributed control paradigm; such scheme balances the communication requirements with convergence speed. Fig. 3 depicts the centralized, distributed, and decentralized control schemes. Mathematically, distinctions between these control approaches can be represented as [27]

$$u_i = \begin{cases} f_i(\boldsymbol{x}) & \text{centralized control} \\ f_i(x_i, \boldsymbol{x}_i^*) & \text{distributed control} \\ f_i(x_i) & \text{decentralized control} \end{cases} \quad (1)$$

where u_i is the output of the controller at agent i, x_i is the physical state of agent i, $\boldsymbol{x} = [x_1, \ldots, x_N]^T$ is the physical state of all agents in the system, and $\boldsymbol{x}_i^*$ is the state of the neighbor agents of agent i.

B. Transient Stability

Using the previously-described multi-agent framework of the smart system, let N denote the number of generators in the power system. Also, for Generator i, where $i \in \{1, \ldots, N\}$, let $P_{e,i}$, $P_{m,i}$, ω_i, X'_{di}, δ_i, M_i, and D_i denote its electrical power (in pu), mechanical power (in pu), relative normalized rotor speed (in pu), direct-axis transient reactance (in pu), rotor angle (in radians), inertia (in seconds), and damping coefficient (in seconds), respectively. The relative normalized rotor speed of Generator i is calculated here as $\omega_i = (\omega_i^{act} - \omega^{nom})/\omega^{nom}$, where ω^{nom} is the nominal

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2581588, IEEE Transactions on Smart Grid

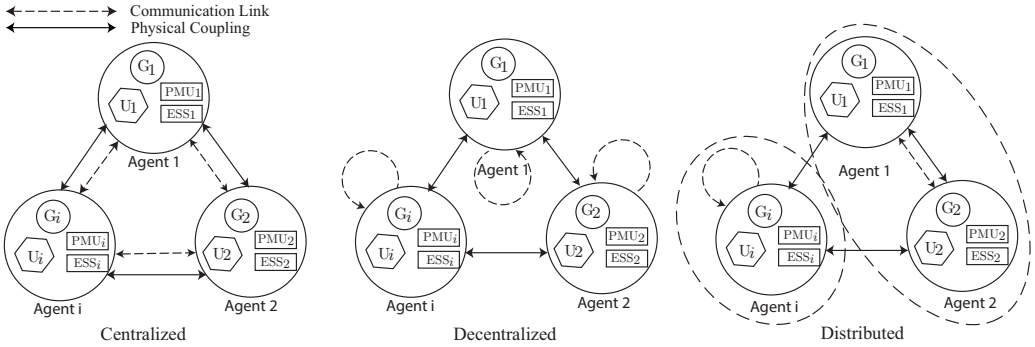


Fig. 3. Centralized vs. decentralized vs. distributed control

angular rotor speed of the power system and ω_i^{act} is the actual angular rotor speed of Generator i.

We employ the swing equation model to describe the dynamics of coupled synchronous generators in the power system. The swing equation links the rotor acceleration of a synchronous generator to the difference between the mechanical torque supplied by the prime mover and electromagnetic torque output of that generator. As such, this model is used to describe the effects of any imbalance between mechanical input and electrical output powers during disturbances. Further, the Kron reduction technique [28] can be used to eliminate bus nodes in a power system and reduce the power network into nodes of dynamic generators; consequently, Kron reduction is used in this work to scale down the order of the interconnections and determine effective mutual couplings between synchronous generator pairs. The combination of these models has recently been shown to effectively characterize transient stability within power systems [9].

Let $\dot{\delta}_i$ and $\dot{\omega}_i$ denote the derivatives of δ_i and ω_i with respect to time, respectively. The swing equation model of Generator i is expressed as [29], [30]

$$\begin{array}{rcl} \dot{\delta}_i & = & \omega_i \\ \dot{\omega}_i & = & \frac{1}{M_i}\left(-D_i\,\omega_i + P_{a,i}\right) \end{array} \tag{2}$$

where $P_{a,i} = P_{m,i} - P_{e,i}$ denotes the accelerating power of Generator i.

A Synchronous generator is typically equipped with power control schemes to help adjust its internal settings in response to changes and faults in the power grid. However, these local power controls have slow reaction to rapid changes. As such, without external power control, synchronous generators cannot alone achieve transient stability in the presence of a switching attack or during a severe fault. Thus, through possible application of control strategies, transient stability can be achieved and/or the stability time can be enhanced. Consequently, external distributed controllers can represent a critical asset for the protection and stability of smart grid systems. Applying a controlled fast-acting stabilizing ESS at Generator i's bus modifies the swing equation to

$$\begin{array}{rcl} \dot{\delta}_i & = & \omega_i \\ \dot{\omega}_i & = & \frac{1}{M_i}\left(-D_i\,\omega_i + P_{a,i} + u_i\right) \end{array} \tag{3}$$

where u_i is the output of the ESS at Generator i's bus. The controlled ESS affects the dynamics of the synchronous generator by injecting and/or absorbing real power at the associated generator's bus.

C. Cyber-Aware Control Scheme

Communication latency is an aggregate result of processing and propagation delays in the communication network. Delay also depends on the communication medium, topology, and protocols. Generally, sensor sampling and quantization delay, possible cryptographic delay if security processing is employed, channel propagation delay, and queueing delay contribute to the overall latency. Furthermore, DoS attacks can cripple communications links to cause excessive delays. In addition, delay can be affected by intermediate nodes between the source and destination (such as data and traffic concentrators and other controllers). We emphasize that the delay that we study in this work is the total delay between the sensors and the controllers.

Communication delay poses a challenge for wide-area damping controllers in power systems as shown in [31]–[33]. Several works consider the development of a delay-adaptive control; for example, [34]–[37] demonstrate that communication latency complicates the design of real-time control systems. To damp inter-area oscillations, [33] explores a two-level control system that implements a second order Padé approximation of communication delay. A similar approach using a predictor-based H_∞ control with a fourth order Padé approximation of communication delay is investigated in [32]. Because the measurements of the power system take certain time before they affect the input of the controller, the closed-loop control system is termed a dead-time system [32].

Furthermore, [21] and [38] demonstrate how communication latency impacts the performance of recently-developed transient stability control schemes in smart grid systems. For example, it is demonstrated in [38] that the performance of the flocking-based controllers deteriorates with increasing latency between sensors and controllers.

In contrast to (1) where the output of the controller is function of the physical state of the system (i.e., $\boldsymbol{x}$), a "cyber-aware" controller of Generator i takes into consideration the cyber state of the network as demonstrated by

$$u_i = f_i(\boldsymbol{x}, \boldsymbol{y}) \tag{4}$$

where in this case $\boldsymbol{y}$ represents the cyber state of the smart grid system. Further, time-delay tolerance is defined as the longest

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2581588, IEEE Transactions on Smart Grid

lag that a closed-loop control system can tolerate to keep the system stable [31]. One goal of the cyber-aware controller is to enhance the time-delay tolerance of the power system especially during DoS attacks.

Variable-structure systems are nonlinear control systems characterized by ordinary differential equations with discontinuous state functions [39], [40]. Such systems can be useful in modeling and analyzing the behavior of smart grids. We take a simple, yet effective, approach to design a cyber-aware controller that mitigates the effects of long communication delays and lost cyber connectivity between system agents. Specifically, building on the variable-structure concept, latency is categorized into discrete ranges, based on which the controller switches between predefined corresponding configurations depending on the delay range of the measurements.

Let the communication latency between the sensors and the controller be termed τ. Then, a cyber-aware controller for Generator i can take the following form

$$u_i = \begin{cases} f_1(\boldsymbol{x}, \boldsymbol{y}) & \tau \leq \tau_1 \\ f_2(\boldsymbol{x}, \boldsymbol{y}) & \tau_1 < \tau \leq \tau_2 \\ \vdots & \vdots \end{cases} \tag{5}$$

where $f_1, f_2, \cdots$ are predefined configurations of the controller.

IV. Parametric Feedback Linearization Control

A PFL controller is a tunable distributed controller that easily integrates with generator governors. When a power system undergoes transient instability due to faults or switching attacks, the PFL controller utilizes the physical state information of the power system to execute a feedback linearization action that synchronizes the generators more aggressively.

The utilization of PFL control for power systems (fully or partially) decouples the dynamics of the physical system resulting in an interesting system response against communication delays. Specifically, a piecewise linear delay-adaptive characteristic function can be used to describe the behavior of the power system under PFL control. Utilizing this characteristic function, a parameter of the PFL control is adjusted to account for the degree of information lag in the cyber components of the smart grid system.

A. "Physical" PFL Control

Centralized and decentralized PFL schemes are recently proposed in [9] and [10], respectively. A distributed flavor of this controller is also proposed in [23]. A centralized PFL (CPFL) controller relies on collecting the power system data before taking a stabilizing action. On the other hand, a decentralized PFL (DPFL) controller only requires local measurements to compute the control signal. Further, a distributed PFL (DiPFL) control scheme utilizes the sensor readings of a cluster of agents.

The CPFL controller requires receiving timely measurements of the rotor speed and phase angle of all synchronous generators in the power system in order to calculate the control signal. Mathematically, the CPFL control signal is expressed as [9]

$$u_{ci} = -\left(P_{a,i} + \alpha_i\, \omega_i\right) \tag{6}$$

where $\alpha_i > 0$ is called the frequency stability parameter of Generator i. The $\alpha_i\omega_i$ term will asymptotically drive the normalized rotor speed of Generator i to 0. The CPFL controller fully cancels the nonlinear terms in the swing equation of Generator i provided that all system measurements are obtained. Consequently, the swing equation of the interconnected power system reduces into decoupled linear equations after implementing the CPFL controller.

Since the communication channels relaying the system measurements from the sensors to the controllers are vulnerable to cyber attacks and long communication delays, the DPFL controller only utilizes the measurements from the sensors situated near the local generator bus. As a result, the accelerating power term (i.e., $P_{a,i}$) cannot be estimated and consequently cannot be cancelled, resulting in a partially linearized control system. Mathematically, the DPFL control signal is expressed as [10]

$$u_{di} = -\alpha_i\omega_i. \tag{7}$$

Consider a power system that has been partitioned into non-overlapping areas $S_j \subseteq N$, where $j = 1, 2, 3, \cdots$. The power system can be partitioned into clusters depending on the mutual physical coupling between generator pairs of the system. Thus, generators within an area have higher mutual coupling. Then, following [41], a DiPFL control can be formulated for each area as a two-level control scheme. In the first control level, a feedback linearization controller is used to affect the rotor speed against a dynamic reference speed, termed as $\bar{\omega}$. The first-level DiPFL control signal for Generator i in area S_j is formulated as [23]

$$u_{D_i i} = -\alpha_i(\omega_i - \bar{\omega})\,. \tag{8}$$

To eliminate static errors due to noise, false data injections, and equipment bias errors, $\bar{\omega}$ is controlled with a proportional controller at the second control level as

$$\dot{\bar{\omega}} = -\frac{\gamma_i}{N_j} \sum_{k \in S_j} \omega_k \tag{9}$$

where $\gamma_i > 0$ is called the control update ratio and N_j is the number of generators in area S_j.

B. Robustness Analysis

We investigate the robustness of the PFL controller in the presence of measurement uncertainty or unavailability. Some of the causes of measurement unreliability include:

- Excessive communication latency between the sensors and the controllers during DoS attacks;
- Noisy measurements due to interference and noise in communication channels;
- Sensor equipment bias and saturation;
- False data injections;
- Missing measurements due to unavailable sensors.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2581588, IEEE Transactions on Smart Grid

Here, the measurements must be estimated at the controller side resulting in a possible difference between the actual and estimated values.

Let the estimated measurements of the relative normalized rotor speed (ω_i) and rotor angle (δ_i) be denoted as $\hat{\omega}_i$ and $\hat{\delta}_i$, respectively. We also model the uncertainty in the nonlinear component of the swing equation using $\hat{P}_{a,i}$. The overall relationships between the actual and estimated quantities are represented as

$$\begin{array}{rcl} \hat{\delta}_i & = & (1+e_{\delta_i})\delta_i \\ \hat{\omega}_i & = & (1+e_{\omega_i})\omega_i \\ \hat{P}_{a,i} & = & (1+e_{P_i})P_{a,i} \end{array} \tag{10}$$

where the parameters e_{δ_i}, e_{ω_i}, and e_{P_i} capture the degree of uncertainty in the rotor phase angle, rotor speed, and accelerating power of Generator i, respectively.

The value of the feedback control signal for Generator i in the presence of measurement uncertainty is then given by

$$\hat{u}_{ci} = -\left(\hat{P}_{a,i} + \alpha_i\,\hat{\omega}_i\right) \tag{11}$$

which leads to closed-system dynamics of the form

$$\dot{x}_i = \hat{A}_i\,x_i + \hat{f}_{NL}(x_i) \tag{12}$$

where

$$\hat{A}_i = \left[\begin{array}{cc} 0 & 1 \\ 0 & -\frac{1}{M_i}\left[D_i + \alpha_i(1+e_{\omega_i})\right] \end{array}\right] \tag{13}$$

and

$$\hat{f}_{NL}(x_i) = [0, -e_{P_i}P_{a,i}]^T\ . \tag{14}$$

We focus on the effects of measurement error by neglecting model uncertainty, and so we assume $e_{P_i} \ll 1$. Thus, the system dynamics can be approximated as

$$\dot{x}_i = \hat{A}_i\,x_i\,. \tag{15}$$

It can be shown that the eigenvalues of $\hat{A}_i$ are given by 0 and $\frac{-1}{M_i}\left[D_i + \alpha_i(1+e_{\omega_i})\right]$. A sufficient condition to ensure that the nonzero eigenvalue lies in the left-hand plane is

$$e_{\omega_i} > -\frac{D_i + \alpha_i}{\alpha_i} \tag{16}$$

where we assume $\alpha_i > 0$ which is necessary for a stabilizing controller. Reformulating (16), we observe that

$$1 + e_{\omega_i} = \frac{\hat{\omega}_i}{\omega_i} > -\frac{D_i}{\alpha_i}\,. \tag{17}$$

This implies that as long as the rotor speed estimate, $\hat{\omega}_i$, has the correct sign as ω_i, stabilization will occur. In fact, even if the sign of $\hat{\omega}_i$ is reversed, stabilization is possible as long as $|\hat{\omega}_i|$ is bounded to be less than $|\omega_i|D_i/\alpha_i$. The reader is reminded that both ω_i and $\hat{\omega}_i$ represent incremental rotor speeds where 0 corresponds to the utility frequency of 50 or 60 Hz.

The result in (17) indicates that the margin of stability is affected by the inverse of α_i. As such, when the communication delay is substantial, the estimation of the system state variables becomes less accurate, then decreasing the value of α can enhance the system stability. Accordingly, varying the value of α can extend the time-delay tolerance of the system especially when the communication links between the sensors and the controller experience excessive delays or during DoS attacks.

C. "Cyber-Physical" PFL Control

Under PFL control, we anticipate that the decoupling of the power system dynamics would result in a direct piecewise linear relationship between communication delay and the optimal frequency stability parameter, where the parameters of this linear relationship are characteristic of the power system under study. It is to be noted that if δ is delayed, then the accelerating power term cannot be estimated correctly and so it may not cancel out perfectly. However, even though there is an incomplete cancellation of $P_{a,i}$ because of the communication delay, we can assume that if the delay is bounded, there is a bound on this error. So if we neglect this error, the dominant dynamics of the closed-control system are linear and decoupled.

A gain-scheduling control design is an approach to design non-linear control systems. In this approach, rather than seeking a single robust controller for the entire operating range of a specific input parameter, the design parameters of the controller are made dependent on the specific value of that input parameter. Building on this concept, the "cyber-physical" PFL controller is proposed to have a gain-scheduling design. Consequently, the PFL controller for Generator i is proposed to be adaptive to a delay value of τ at time t as

$$u_{ci}(t) = -P_{a,i}(t-\tau) - \alpha_i(\tau)\omega_i(t-\tau)\,. \tag{18}$$

In other words, the frequency stability parameter of the PFL controller is made adaptive to latency rather than being a fixed-value parameter.

Let $\alpha_i^*(\tau)$ denote the values of the frequency stability parameter that optimize the performance of the PFL controller for the various values of delay. Given the values of the communication latency are known to the controller for each sensor measurement, then once a measurement is received by the PFL controller, the controller can apply the corresponding optimal value of the frequency stability parameter.

A cyber-physical PFL control that is robust to delays and extends the time-delay tolerance is proposed in this work to combine the philosophies of variable-structure systems and gain-scheduling control design. The gain-scheduling approach is utilized where the frequency stability parameter is made adaptive to the value of delay between the sensors and the controllers. Further, the variable-structure design means that the cyber-physical PFL controller switches between predefined control schemes depending on the value of delay.

In this case we specify the control signal of the cyber-physical PFL controller as

$$u_i = \left\{\begin{array}{ll} u_{ci}\left(\boldsymbol{x}, \alpha_c^*\right) & \tau \le \tau_{opt} \\ u_{ci}\left(\boldsymbol{x}, \alpha^*(\tau)\right) & \tau_{opt} < \tau \le \tau_{max} \\ u_{di}\left(\boldsymbol{x}_i, \alpha_d^*\right) & \tau_{max} < \tau \end{array}\right. \tag{19}$$

where α_d^* is the optimum value of the DPFL controller's frequency stability parameter, and α_c^* is the optimum value of CPFL controller's parameter when the latency is not greater

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2581588, IEEE Transactions on Smart Grid

than τ_{opt}; further, the frequency stability parameter is made adaptive to the communication latency when the delay is up to τ_{max}. As obvious from (19) the cyber-physical controller utilizes the centralized form for $\tau \leq \tau_{max}$. However, when the delay exceeds τ_{max}, the controller switches to the decentralized mode. Consequently, the proposed cyber-physical controller employs the variable-structure and gain-scheduling design concepts. It is to be noted that τ_{opt}, τ_{max}, and the optimal values of α are dependent on the power system.

The work in [24] proposes a two-tier smart grid control based on flocking concepts. To minimize communication overhead amongst the generators, different generators are grouped into homogeneous clusters. Further, full communication connectivity amongst the generators of a cluster is assumed; however, inter-cluster connectivity is assumed in [24] to occur between the head generators in each cluster.

Our work is similar to that of [24] in that both contributions consider the problem transient stability of the power system. However, the proposed work is different in several ways; for example, our controller changes its structure and parameters depending on the value of the communication latency. In addition, we employ feedback-linearization control instead of the flocking-based control. Moreover, our model adapts to the situation of complete communication network loss by switching to a decentralized mode of control. Finally, we assert that our framework is general and thus does not solely apply to a specific power system.

D. Unavailable Sensors Case

Further, we propose a modified DiPFL controller to address the case when some cyber-physical agents do not possess their own local sensors. Consequently, such agents do not have measurements of their local rotor angle and speed. Thus, to control the output of the local ESS we employ available readings from other agents within the cluster. Given that the physical coupling is strong within each area, the different agents are expected to share close dynamics. As such, the state of an agent without a local sensor can be inferred from the other agents in the cluster.

Specifically, consider the case when agent $\tilde{i}$ in area S_j does not have an associated sensor; consequently, the values of $\delta_{\tilde{i}}$ and $\omega_{\tilde{i}}$ are unknown. However other agents in S_j have sensors and so the values of their rotor speed and angle are known and shared with all agents of S_j. Define the set $S_{\tilde{j}}$ to be the set of all agents in S_j except agent $\tilde{i}$; i.e., $S_{\tilde{j}}$ has $N_j - 1$ agents. Following the results of (8) and (9), we propose that the control signal of the different agents in area S_j be calculated as

$$u_i = \begin{cases} -\alpha_i(\omega_{\tilde{j}} - \bar{\omega}) & i = \tilde{i} \\ -\alpha_i(\omega_i - \bar{\omega}) & i \neq \tilde{i} \end{cases} \tag{20}$$

where

$$\begin{aligned} \omega_{\tilde{j}} &= \tfrac{1}{N_j - 1} \sum_{k \in S_{\tilde{j}}} \omega_k \\ \dot{\bar{\omega}} &= -\gamma_i \omega_{\tilde{j}} \,. \end{aligned} \tag{21}$$

In this case the available readings from the agents of the area determine the control signal for each agent.

TABLE I
NEW ENGLAND SYSTEM FAULT DETAILS

Case Study	Faulted Bus	Tripped Line
1	17	17–18
2	11	10–11
3	22	21–22
4	5	5–8

TABLE II
WECC SYSTEM FAULT DETAILS

Case Study	Faulted Bus	Tripped Line
1	6	8–6
2	8	5–8
3	5	4–5
4	4	7–4
5	7	6–7

V. LATENCY CHARACTERISTIC FUNCTION

Here we try to find the latency characteristic function of the CPFL controller (i.e., the optimal values of α for the corresponding values of τ). The results of this study will be used in building the cyber-physical PFL controller of (19). We consider both the New England and WECC test power systems.

For the following results, stability time of a generator is measured by finding the difference between the time after which the relative normalized rotor speed of the generator is restricted to a 0.8333% threshold (i.e., the time when the actual rotor speed of the generator is limited to $\pm$ 0.5 Hz) and the time when the stabilizing controller is activated. Further, for the New England test power system, the average stability time and control power values do not take into account Generator 10's results because it represents an equivalent generator cluster.

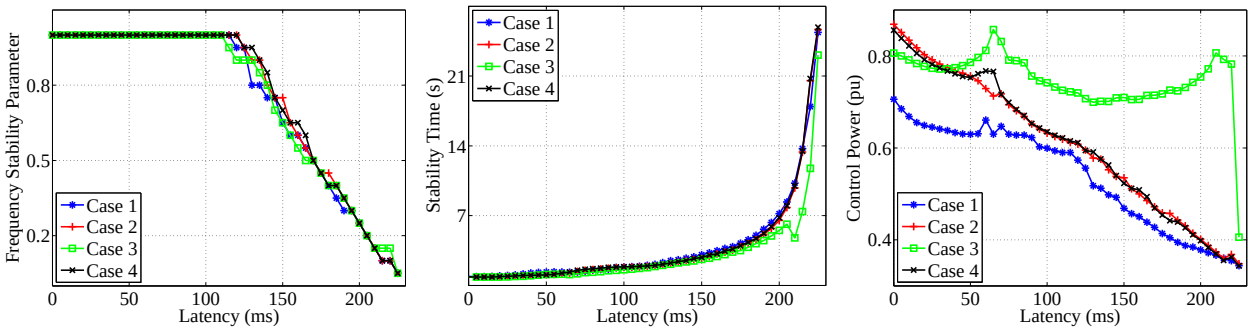
A. New England Power System

The New England 10-generator 39-bus test power system (shown in Fig. 1) is considered. The values of M_i's and X'_{di}'s are found from [42], [43] and the damping coefficients are set to 20 ms. Four case studies are considered in this work as shown in Table I. The power system is assumed to be running in normal state from $t = 0$ to $t = 0.5$ s. A three-phase fault occurs at the faulted bus at $t = 0.5$ s, then the tripped line is removed to clear the fault at $t = 0.6$ s. Finally, the CPFL controller is activated on all generators at $t = 0.7$ s.

We evaluate the latency characteristic function for the New England power system for communication latencies up to 225 ms. Fig. 4 displays the relation between the communication latency and the optimum values of the frequency stability parameter, stability time, and control power for this test system. For the results in this figure, the optimum values of α refer to the set of frequency stability parameters that yield the lowest mean stability time for a certain communication latency.

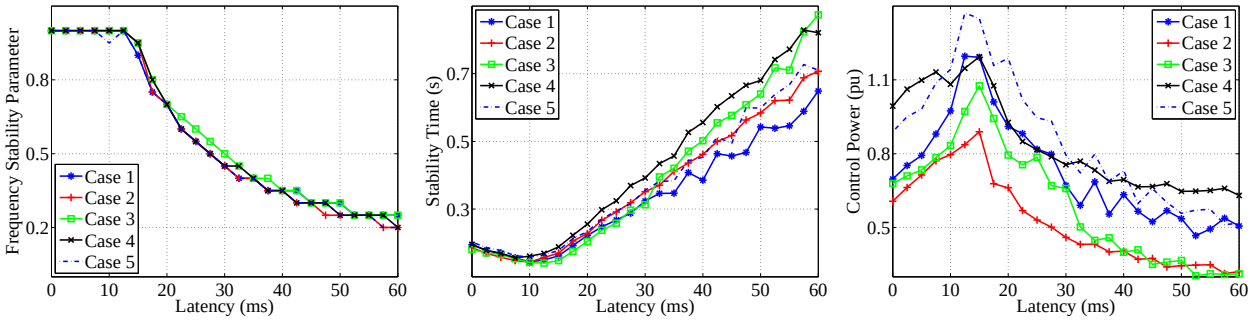
It is noted from Fig. 4 that a high value of α makes the stability time lowest for latency values up to 115 ms. However, for higher values of latency, a better strategy is to let the value of α decline with increasing the value of latency. This observation aligns with the results of (17) where it is observed

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2581588, IEEE Transactions on Smart Grid



(a) Optimum α (b) Stability time (c) Control power

Fig. 4. Optimal performance versus latency in the New England test power system



(a) Optimum α (b) Stability time (c) Control power

Fig. 5. Optimal performance versus latency in the WECC test power system

that decreasing the value of α can enhance the system stability when there is a substantial communication latency.

Considering the four case studies mentioned in Table I, a curve fitting approach is used to find the optimal values of α as a function of τ. Interestingly, it is found that the CPFL controller can adapt its frequency stability parameter using a piecewise linear characteristic function as

$$\alpha^*(\tau) = \begin{cases} 1 & \tau \leq 115 \text{ ms} \\ -8.86\,\tau + 2.02 & 115 \text{ ms} < \tau \leq 225 \text{ ms}\,. \end{cases} \tag{22}$$

As a result of (6), (19), and (22), the cyber-physical PFL controller is proposed for the New England test power system as

$$u_i = \begin{cases} -P_{a,i} - \omega_i & \tau \leq 115 \text{ ms} \\ -P_{a,i} + (8.86\tau - 2.02)\omega_i & 115 \text{ ms} < \tau \leq 225 \text{ ms} \\ -\alpha_d^*\omega_i & 225 \text{ ms} < \tau\,. \end{cases} \tag{23}$$

B. WECC Power System

Extending the above approach to the WECC 9-bus 3-generator test power system (shown in Fig. 2), five case studies are considered as shown in Table II. For simulating this power system, $D_1 = 5$ ms, $D_2 = 1$ ms, $D_3 = 2$ ms, $X'_{d1} = 0.08$ pu, $X'_{d2} = 0.18$ pu, $X'_{d3} = 0.12$ pu, $M_1 = 50$ ms, $M_2 = 15$ ms, and $M_3 = 35$ ms. A three-phase fault occurs at the faulted bus at $t = 0.5$ s, then the tripped line is removed to clear the fault at $t = 0.6$ s, and the CPFL controller is activated on all generators at $t = 0.7$ s. Fig. 5 displays the relation between τ and the optimum values of α, stability time, and control power for the five test cases.

Considering the results of Fig. 5, and similar to the approach taken in (22), curve fitting is employed to find the latency characteristic function for the CPFL controller as

$$\alpha^*(\tau) = \begin{cases} 1 & \tau \leq 15 \text{ ms} \\ -12.8\,\tau + 0.92 & 15 \text{ ms} < \tau \leq 62.5 \text{ ms}\,. \end{cases} \tag{24}$$

Consequently, the cyber-physical PFL controller is proposed for the WECC test power system as

$$u_i = \begin{cases} -P_{a,i} - \omega_i & \tau \leq 15 \text{ ms} \\ -P_{a,i} + (12.8\tau - 0.92)\omega_i & 15 \text{ ms} < \tau \leq 62.5 \text{ ms} \\ -\alpha_d^*\omega_i & 62.5 \text{ ms} < \tau\,. \end{cases} \tag{25}$$

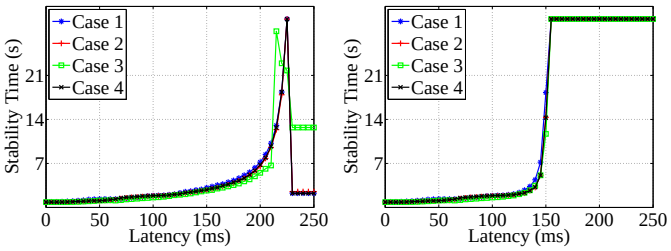
VI. Numerical Results

In this section we numerically evaluate the performance of the proposed controller and compare the results with the traditional "physical" PFL controller. For this study we apply both controllers to the New England test power system; however, it is to be noted that similar results can be obtained for the WECC test power system.

A. New England Power System

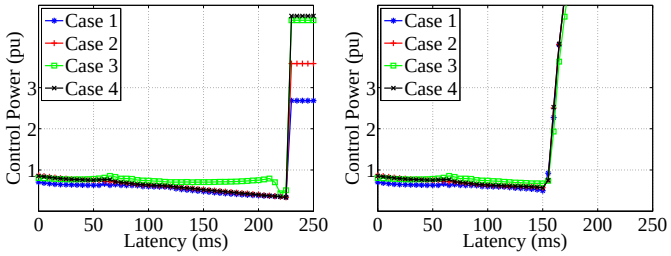
The four test cases of Table I are considered for the New England test power system. Stability time of the system generators and the average control power are the measures that are used to evaluate the performance of the proposed

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2581588, IEEE Transactions on Smart Grid



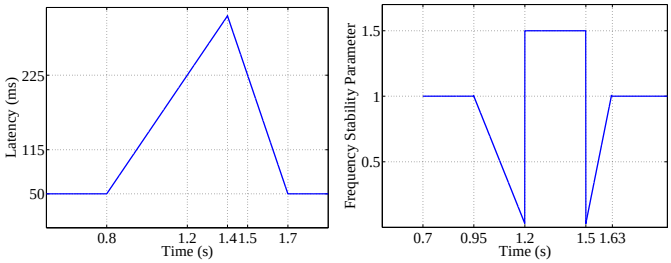
(a) Cyber-Physical Controller (b) Delay-Inadaptive Controller

Fig. 6. Stability time of the PFL controller



(a) Cyber-Physical Controller (b) Delay-Inadaptive Controller

Fig. 7. Control power of the PFL controller



(a) Communication Latency (b) Frequency Stability Parameter

Fig. 8. Response to concurrent physical and cyber disturbances

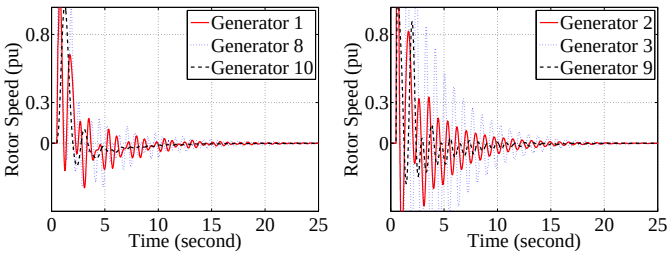


Fig. 9. Performance when Generators 3 and 8 do not have associated sensors

cyber-physical PFL controller. The strategy of (23) is used, and $\alpha_d^* = 30$ is applied when the controller is in the decentralized mode. Further, the performance is compared to that of the delay-inadaptive traditional PFL controller where α is set to 1 regardless of delay values.

Fig. 6 illustrates the average stability time of the PFL controller. It is observed that when the frequency stability parameter is constant regardless of the value of latency, the PFL controller can stabilize the New England power system as long as the communication latency is below about 150 ms. However, when α is varied to accommodate the communication latency as shown in (22), the cyber-physical PFL controller can stabilize the power system's generators provided that the latency is less than 225 ms. Further, for higher values of latency, the cyber-physical PFL controller can switch to the decentralized mode and still be able to stabilize the power system.

Further, Fig. 7 displays the average external power used by the PFL controller. It is observed that the proposed cyber-physical PFL controller has a substantial power gain over the delay-inadaptive controller especially for high values of communication latency. Consequently, the proposed cyber-physical control scheme increases the robustness of the PFL controller to communication delays and increases the time-delay tolerance.

B. Numerical Example

Consider the New England test power system with an estimated average latency of 50 ms during normal operations. Assume that a three-phase fault occurs at Bus 17, Line 17-18 is removed, and the PFL controller is activated at $t = 0.5$ s, 0.6 s, and 0.7 s, respectively. Further, assume a DoS attack targets the communication network at $t = 0.8$ s; consequently, the communication latency starts to increase. At $t = 1.4$ s, the DoS attack is stopped and the latency quickly starts to drop to normal values. As a result of the DoS attack, the communication latency changes as shown in Fig. 8(a).

The cyber-physical PFL controller responds to the varying nature of latency by adapting its α parameter as described in (23) and shown in Fig. 8(b). When $\tau > 225$ ms (for $1.2 \leq t < 1.5$ s in this example), the controller switches to the decentralized mode and α_d^* = 1.5 is used.

C. Unavailable Sensors Case

Consider the case when Generators 3 and 8 do not have their own local sensors. Consequently, the proposed cyber-physical controller utilizes the structure of (20) and (21). The power system generators are clustered in three separate areas as $\{1, 8, 10\}$, $\{2, 3, 9, 4, 5\}$, and $\{6, 7\}$. Assume that a three-phase fault occurs at Bus 11, Line 11-10 is removed, and the PFL controller is activated at $t = 0.5$ s, 0.6 s, and 0.7 s, respectively. Fig. 9 displays the relative normalized rotor speed for selected generators in the system. Results of this figure show that the different generators stabilize quickly; however, as expected, the generators that do not have local sensors take relatively longer time to achieve stability.

VII. Conclusions

This article proposes a framework for cyber-physical control to improve system resilience in smart grids. Specifically, the proposed control scheme adapts its structure and parameters depending on communication latency values between the sensors and the controllers in the power grid. A delay-adaptive design that capitalizes on the features of parametric feedback linearization (PFL) control is presented in this work in order to enhance the time-delay tolerance of the power system and to react to cyber and physical attacks.

The performance of the proposed cyber-physical control scheme is demonstrated when the PFL controller is applied

to the New England 39-bus and WECC 9-bus test power systems following the occurrence of a physical disturbance. Numerical results also show that the proposed controller can tolerate substantial delays without noticeable degradation in performance and is able to stabilize the power system effectively. Future directions of this work include investigating other types of control schemes, incorporating other types of cyber attacks, and investigating cyber-aware wide-area control schemes.

REFERENCES

[1] T. Flick and J. Morehouse, *Securing the Smart Grid: Next Generation Power Grid Security*. Syngress, 2011.

[2] W. Stallings, *Network Security Essentials: Applications and Standards, 5th edition*. Pearson, 2013.

[3] S. Horowitz and A. Phadke, *Power System Relaying, 4th Ed.* Wiley, 2014.

[4] B. Ravindranath and M. Chander, *Power System Protection and Switchgear*. New Age International Pvt Ltd. Publishers, 2011.

[5] A. Abur and A. Expósito, *Power System State Estimation: Theory and Implementation*. CRC Press, 2004.

[6] R. Berthier, W. Sanders, and H. Khurana, "Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 350–355, October 2010.

[7] S. Zonouz, K. Rogers, R. Berthier, R. Bobba, W. Sanders, and T. Overbye, "SCPSE: security-oriented cyber-physical state estimation for power grid critical infrastructures," *IEEE Transactions on Smart Grid*, 2012.

[8] P. Kundur, *Power System Stability and Control*. EPRI Power System Engineering Series, McGraw-Hill, 1994.

[9] A. Farraj, E. Hammad, and D. Kundur, "A Cyber-Enabled Stabilizing Controller for Resilient Smart Grid Systems," in *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, pp. 1–5, February 2015.

[10] E. Hammad, A. Farraj, and D. Kundur, "A Resilient Feedback Linearization Control Scheme for Smart Grids under Cyber-Physical Disturbances," in *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, pp. 1–5, February 2015.

[11] P. W. Sauer and M. A. Pai, *Power System Dynamics and Stability*. Prentice-Hall, 1998.

[12] K. Zhu, M. Chenine, and L. Nordström, "Ict architecture impact on wide area monitoring and control systems' reliability," *IEEE Transactions on Power Delivery*, vol. 26, no. 4, pp. 2801–2808, 2011.

[13] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2444–2453, 2015.

[14] J. W. Stahlhut, T. J. Browne, G. T. Heydt, and V. Vittal, "Latency viewed as a stochastic process and its impact on wide area power system control signals," *IEEE Transactions on Power Systems*, vol. 23, no. 1, pp. 84–91, 2008.

[15] M. Mokhtari, F. Aminifar, D. Nazarpour, and S. Golshannavaz, "Wide-area power oscillation damping with a fuzzy controller compensating the continuous communication delays," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1997–2005, 2013.

[16] G. N. Ericsson, "Information security for electric power utilities (epus)cigre developments on frameworks, risk assessment, and technology," *IEEE Transactions on Power Delivery*, vol. 24, no. 3, pp. 1174–1181, 2009.

[17] M. Chenine, J. Ullberg, L. Nordstrom, Y. Wu, and G. Ericsson, "A framework for wide-area monitoring and control systems interoperability and cybersecurity analysis," *IEEE Transactions on Power Delivery*, vol. 29, no. 2, pp. 633–641, 2014.

[18] Y. Liu, P. Ning, and M. K. Reiter, "False Data Injection Attacks Against State Estimation in Electric Power Grids," *ACM Transactions on Information and System Security*, vol. 14, pp. 13–33, June 2011.

[19] S. Liu, X. P. Liu, and A. El Saddik, "Denial-of-Service (DoS) Attacks on Load Frequency Control in Smart Grids," in *IEEE PES Innovative Smart Grid Technologies (ISGT)*, pp. 1–6, 2013.

[20] E. Hammad, A. Khalil, A. Farraj, D. Kundur, , and R. Iravani, "Tuning Out of Phase: Resonance Attacks," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 1–6, November 2015.

[21] A. Farraj, E. Hammad, D. Kundur, and K. Butler-Purry, "Practical Limitations of Sliding-Mode Switching Attacks on Smart Grid Systems," in *IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–5, July 2014.

[22] 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 *IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–6, July 2012.

[23] E. Hammad, A. Farraj, and D. Kundur, "Paradigms and Performance of Distributed Cyber-Enabled Control Schemes for the Smart Grid," in *IEEE Power & Energy Society General Meeting (PESGM)*, pp. 1–5, IEEE, 2015.

[24] J. Wei and D. Kundur, "Two-tier hierarchical cyber-physical security analysis framework for smart grid," in *IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–5, 2012.

[25] J. Wei and D. Kundur, "A Flocking-Based Model for DoS-Resilient Communication Routing in Smart Grid," in *IEEE Global Communications Conference (GLOBECOM)*, pp. 3519–3524, December 2012.

[26] J. Wei, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "A Flocking-Based Dynamical Systems Paradigm for Smart Power System Analysis," in *IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–8, July 2012.

[27] M. Andreasson, "Control of Multi-Agent Systems with Applications to Distributed Frequency Control of Power Systems." Licentiate Thesis, KTH School of Electrical Engineering, March 2013.

[28] F. Dörfler and F. Bullo, "Kron Reduction of Graphs With Applications to Electrical Networks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 60, pp. 150–163, January 2013.

[29] P. M. Anderson and A. A. Fouad, *Power System Control and Stability*. IEEE Power Systems Engineering Series, IEEE Press, 1994.

[30] F. Dörfler and F. Bullo, "Synchronization and Transient Stability in Power Networks and Non-Uniform Kuramoto Oscillators," in *American Control Conference (ACC)*, pp. 930–937, June/July 2010.

[31] H. Wu, K. S. Tsakalis, and G. T. Heydt, "Evaluation of Time Delay Effects to Wide-Area Power System Stabilizer Design," *IEEE Transactions on Power Systems*, vol. 19, pp. 1935–1941, November 2004.

[32] B. Chaudhuri, R. Majumder, and B. C. Pal, "Wide-Area Measurement-Based Stabilizing Control of Power System Considering Signal Transmission Delay," *IEEE Transactions on Power Systems*, vol. 19, pp. 1971–1979, November 2004.

[33] S. Zhang and V. Vittal, "Design of Wide-Area Power System Damping Controllers Resilient to Communication Failures," *IEEE Transactions on Power Systems*, vol. 28, pp. 4292–4300, November 2013.

[34] B. Wittenmark, J. Nilsson, and M. Törngren, "Timing Problems in Real-Time Control Systems," in *American Control Conference (ACC)*, vol. 3, pp. 2000–2004, June 1995.

[35] J. Nilsson and B. Bernhardsson, "Analysis of Real-Time Control Systems with Time Delays," in *IEEE Conference on Decision and Control (CDC)*, vol. 3, pp. 3173–3172, December 1996.

[36] J. Nilsson and B. Bernhardsson, "LQG Control over a Markov Communication Network," in *IEEE Conference on Decision and Control (CDC)*, vol. 5, pp. 4586–4591, December 1997.

[37] 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, January 1998.

[38] A. Farraj, E. Hammad, J. Wei, D. Kundur, and K. Butler-Purry, "Performance Evaluation of Flocking-Based Distributed Cyber-Physical Control for Smart Grid," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 970–975, November 2014.

[39] D. Liberzon, *Switching in Systems and Control*. Systems & Control: Foundations & Applications Series, Birkhäuser, 2003.

[40] A. Sabanovic, L. Fridman, and S. Spurgeon, *Variable Structure Systems: From Principles to Implementation*. IET Control Engineering Series 66, The Institution of Engineering and Technology, 2004.

[41] M. Andreasson, D. V. Dimarogonas, H. Sandberg, and K. H. Johansson, "Distributed Control of Networked Dynamical Systems: Static Feedback and Integral Action and Consensus," *IEEE Transactions on Automatic Control*, vol. 59, pp. 1750–1764, July 2014.

[42] T. Athay, R. Podmore, and S. Virmani, "A Practical Method for the Direct Analysis of Transient Stability," *IEEE Transactions on Power Apparatus and Systems*, vol. 98, pp. 573–584, March/April 1979.

[43] B. Pal and B. Chaudhuri, *Robust Control in Power Systems*. Power Electronics and Power Systems Series, Springer, 2006.