A Class of Switching Exploits Based on Inter-Area Oscillations

Eman Hammad, *Student Member, IEEE*, Ahmed M. Khalil, *Member, IEEE*, Abdallah Farraj, *Member, IEEE*, Deepa Kundur, *Fellow, IEEE*, and Reza Iravani, *Fellow, IEEE*

***Abstract*—This work presents a new class of cyber-physical switching attacks that targets power transmission systems. The proposed approach relies on exciting inter-area oscillation modes in a coordinated manner to drive groups of system generators out of step. Our paradigm targets inter-area oscillations by switching a relatively small part (in the order of 2%) of the system load at a (low) frequency that resonates with one of the inter-area oscillation modes observed in the power system. The switching frequency of the targeted mode is chosen through measurement-based analysis of the frequency deviation at a select bus that is observable by the adversary. The inter-area switching attack is implemented as single-load switching and coordinated multi-load switching and is studied with a variety of switching signals. Numerical results show the potential and characteristics of the proposed switching exploitation when applied to the four-machine two-area power system and the Northeast Power Coordinating Council 68-bus system.**

***Index Terms*—Cyber-physical security, inter-area oscillations, power system stability, smart grid, switching attacks.**

I. Introduction

There has been recent focus on the development of research results, design principles and government guidelines addressing smart grid cyber security concerns [1], [2]. The evolving integration of cyber technology in emerging power systems has increased exposure to cyber and cyber-physical attacks. The significant impact of such onslaughts is evidenced by the series of recent attacks targeting critical infrastructures including Stuxnet (2010) [3], German steel mill (2014) [4], and the Ukraine power grid (2015) [5]. One class of cyber-physical attacks that has received attention is that of *switching attacks* aimed at disrupting operation by exploiting priori knowledge of the power grid structure and current state information to modulate system components to enhance disruption.

Initial work [6]–[9] investigated the effects of *sliding-mode*-based switching attacks on the transient stability of power systems. Here, the power system under assault is modeled as a variable-structure control system [10]. To be effective, this attack employs calculated state-based switchings of a given load to create an unstable sliding-mode that drives a target synchronous generator outside its stability boundary. A linear model of the local power grid and full knowledge of the target generator state are necessary for attack success.

More recently, a state-based switching attack employing a fast-acting energy storage system (ESS) was proposed to destabilize parts of the power grid [11]. Here, an adversary is assumed to have physical/cyber control of a circuit breaker, access to the current state of the ESS (by, for example, interception), and knowledge of the power system model under the binary (open/closed) states of the circuit breaker. The opponent, using this knowledge, computes a switching signal that determines control of the ESS circuit breaker to instigate power system disruption.

Another switching attack was presented as part of the Idaho National Laboratory's Aurora experiment [12]. This undertaking showcased the impact of switching a synchronous machine out of synchronism. The associated threat model assumed by the Aurora attack places an adversary at a capacity of gaining control over one of the most protected components in a power system thus arguably decreasing the practical attack feasibility. Switching attacks have also been included in vulnerability and anomaly detection frameworks [13].

Although a number of thrusts have examined switching-based attacks, few methodologies have been developed to address their mitigation; investigations have focused on approaches to counteract switching using ESSs via a game-theoretic control [14] and a feedback-linearization control [15].

In this paper we propose a new class of switching attacks, termed *inter-area switching attacks*, that addresses the limitations of existing attack strategies. Specifically, our approach enables stealthy reconnaissance and execution without the need for full knowledge of power system topology or state providing greater feasibility. The practical advantage of our scheme stems from the exploitation of inter-area mode oscillations within the power system that are easily estimated through measurement-based techniques.

Inter-area oscillations characterize how a group of coherent synchronous generators swing against other generator groups. The proposed switching attack has two phases: reconnaissance and execution. During reconnaissance, an adversary probes

Manuscript received September 21, 2016; revised December 23, 2016; accepted January 30, 2017. Date of publication February 8, 2017; date of current version August 21, 2018. This work was supported by the Natural Sciences and Engineering Research Council of Canada under Grant RGPIN 227722. Paper no. TSG-01296-2016.

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

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

Digital Object Identifier 10.1109/TSG.2017.2666046

and estimates inter-area oscillation modes of the power system. Based on this knowledge, the adversary then selects a mode and subsequently, during execution, switches a small part of the load under his/her control near an inter-area link. A low switching frequency is selected to stimulate one of the system inter-area oscillation modes thus over-exciting it. Hence, with sufficient switching, the attack will resonate the targeted mode resulting in driving a group of generators to instability. The size of the switched load is relatively small, where for the case of the four-generator two-area power system, a successful inter-area switching attack was conducted by switching $2 - 16\%$ of one load ($L7$). Noting that switching a smaller size load would require a longer switching time to successfully carry the attack. Further, as shown for the case of coordinated switching attack, an adversary could resort to switching multiple smaller loads in a coordinated manner.

The main contributions of this paper are three-fold. We first present a model and a general methodology for inter-area switching attacks. Next, we implement specific types of inter-area switching attacks demonstrating the design flexibility available by varying the switching signals and number of loads controlled. Finally, we study the degree of vulnerability of power systems to the proposed attack through simulations on the four-machine two-area power system and the Northeast Power Coordinating Council (NPCC) 68-bus system; we demonstrate how the nonlinearity of the underlying power system dynamics results in interesting attack characteristics that can be exploited for high impact disruption.

The remainder of this paper is organized as follows. We discuss our threat model and inter-area switching attacks in Section II. Section III provides a brief review of the small-signal analysis and inter-area oscillations in power systems. The estimation of the inter-area modes oscillating frequencies using the spectral Independent Component Analysis (ICA) approach is presented in Section IV. Section V presents the simulation setup, results and analysis. Conclusions and final remarks are discussed in Section VI.

II. Inter-Area Mode Switching Attacks

Switching attacks represent an archetypal cyber-physical attack in which cyber-enabled system elements are exploited to disrupt targeted physical power system components. The primary goal of switching attacks is to impact power availability, typically by causing instability of one or more target components, by reconfiguring the grid topology in some way. Specifically, an adversary capable of gaining cyber-enabled access to circuit breakers initiates open/close actions that affect system dynamics to instigate instability of a target entity such as a generator. Previously proposed switching attacks provoke disruption by modulating the power system topological structure to instigate an unwanted dynamic response causing the component to be tripped out. For example the work in [6] relied on variable structure systems theory and sliding mode control to rapidly destabilize a target generator, while the proposed attack in this work targets inter-area oscillatory modes. Switching attacks, in contrast to other forms of cyber-physical attacks on power systems, have been shown to be capable of high impact disruptions within very short time intervals using limited knowledge of power system topology. Moreover, there can be greater control over the physical components targeted for disruption.

Thus, an important function of existing power system monitoring and protection schemes has been to constrain the range of possible attacks and restrict the degree of attack impact by limiting cascading failures and regulating impending instability. The application of such protection is facilitated by the ability to monitor and detect anomalous physical states, which is greatly enhanced when aggressive switching is applied by an opponent to carry out a successful attack.

In contrast, in this paper, we demonstrate the existence of a successful class of stealthy inter-area switching attacks that exhibit the following properties that enable them to be a more insidious threat:

- low switching frequency that can readily go undetected;
- low switching power that cannot be easily distinguished from regular load changes; and
- lack of the need for a full power system model or knowledge to construct and apply the attack.

As we discuss next, the proposed attack makes use of the presence of inter-area modes and the ability to switch loads in the system to excite these modes to intensify disruption.

A. Power System Characteristics

Power systems comprised of multiple synchronous machines exhibit complex properties and phenomena. One such characteristic is termed generator *coherency*, which describes how groups of generators in the power system naturally cluster in terms of frequency when a disturbance is applied. Synchronous machine coherency can be modeled as interactions of coupled oscillators where the different machines are coherent if they oscillate in synchronism [16]. Inter-area mode oscillations are one manifestation of interactions between groups of generators in a power system, typically observed when the groups of generators that are interconnected by weak lines swing against each other [17].

There are two distinct types of inter-area oscillations: very low frequency modes ($0.1 - 0.3$ Hz) involving all generators of the power system, and higher frequency modes ($0.4 - 0.8$ Hz) involving subgroups of generators swinging against each other. An inter-area oscillation mode is a characteristic of a specific power system for a given operating condition. A detailed representation of the interconnected power system enables the analysis of inter-area oscillations as detailed in Section III.

Switching loads represent a stealthy way to introduce subtle disruptions in the power grid that can be masked as normal load changes. Power system loads are typically classified as one of three types: constant current, constant power, and constant impedance. From an adversarial perspective, heating loads (which have constant impedance) present a convenient class to exploit for switching, as these loads undergo switching during normal operation. In contrast, constant power and constant current loads are, in many cases, motor loads and converter-based loads, respectively, whose switching would be more apparent to consumers and system operators.

B. Threat Model

The proposed attack relies on a threat model in which the targeted power system exhibits inter-area modes that are exploited via limited access to cyber-enabled infrastructure. The salient components of the threat model can be summarized as follows.

1) The power system exhibits inter-area modes that can be exploited for disruption.
2) The adversary can:
    a) control part of the system's load denoted the *switching load* L_{sw}.
    b) observe the line measurements (for a few seconds) at the switching load L_{sw} bus.

It is important to emphasize that no previous system knowledge (such as the $\boldsymbol{A}$ matrix) is required to construct or apply the proposed attack. In addition, the existence of inter-area modes is evident in most multi-machine power systems.

The proposed threat model deconstructs the attack into two stages: reconnaissance and execution. This model is observed in recent cyber-physical attacks with proven consequences on cyber-enabled industrial systems as in the case of Stuxnet [3], and power systems as in the case of the cyber-attack on the Ukrainian power grid [5]. Moreover, the proposed level of access assumed by the presented threat model can be obtained by an adversary with limited resources as is evident in the attack on the Ukranian power grid.

For example, the ability to control part of the system's load is possible through intrusion of associated smart meters or home area networks that appropriately shed/excite loads via control signals that may be spoofed. In another potential scenario, an adversary obtains limited substation access to, for example, de-energize the circuit breaker of the line connected to L_{sw}. Yet another alternative enables an adversary with limited resources to cause a transient fault from the switching load L_{sw} side. Practically, such infiltrations may be possible by exploiting one or more of a variety of weaknesses in specific device operating systems, communication protocols, physical security in use and using insider information [18]; the details and associated investigation are beyond the scope of this paper.

Similarly, ability to observe appropriate line measurements is possible through intrusion of associated sensor devices or communication links to glean information directly about line measurements or estimate them from related data [18]. This enables measurements to be collected and analyzed by an adversary to deduce the characteristic inter-area oscillation frequencies. An adversary then selects one of the inter-area frequency modes denoted f_{sw} and (at a select time) switches the load under control at frequency f_{sw}. The reader should note that f_{sw} is typically less than 1 Hz. The existence of inter-area modes enables the switching to cause coherent generators in the system areas to swing against each other; hence their phase difference would eventually be outside the tolerated range, resulting in either generator tripping or islanding of the system areas if islanding mechanisms are installed.

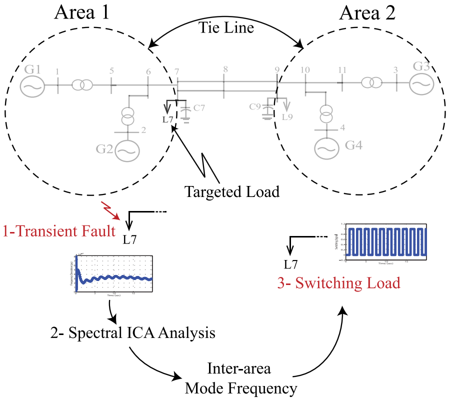


Fig. 1. Inter-area switching attack.

C. Attack: Reconnaissance and Execution

To launch an effective inter-area switching attack, the adversary conducts the following steps (see also Fig. 1).

1) As consistent with the threat model, gains access to:
    - Part of the constant-impedance load L_{sw} with the ability to switch L_{sw} on and off.
    - Line measurements at the L_{sw} bus.
    - Short circuiting control, such as the built-in de-energization circuit breaker or a method of imposing a fault at the load side.
2) Imposes a transient short circuit on the power system at time t_0 to excite system inter-area oscillation modes.
3) Records line measurements for few seconds following the fault until the system enters steady-state.
4) Performs spectral ICA analysis on the recorded data to extract the frequencies of the inter-area modes (collectively denoted F_m).
5) Select the target mode frequency $f_m \in F_m$.
6) At time $t_0 + T$, applies switching of L_{sw} at frequency $f_{\text{sw}} = f_m$, where $T > 0$ is the time the adversary waits before launching the switching attack.
7) Concludes switching after power system instability arises.

Steps 1 to 4 represent a reconnaissance phase, while steps 5 to 7 occur during the execution phase.

D. Forms of Inter-Area Switching Attacks

An adversary may consider different implementations of switching attacks based on the number of loads under attacker control, switching frequency, and intended stealthiness. The switching signal $S(t)$ at frequency f_{sw} can be expressed as

$$S(t) = \frac{1}{2}\left[\text{sgn}(\sin(2\pi f_{\text{sw}} t)) + 1\right] \tag{1}$$

where $S(t) = 1$ ($S(t) = 0$) denotes a closed (open) switch.

Using the estimated target inter-area frequency f_{sw}, realization of the inter-area switching attack can take different forms of which we consider two:

1) Single Switching Load: In this form of the attack, a single switching action via (1) is initiated on part of the system load L_{sw}, with a switching frequency the same as the estimated targeted inter-area mode f_{sw}.

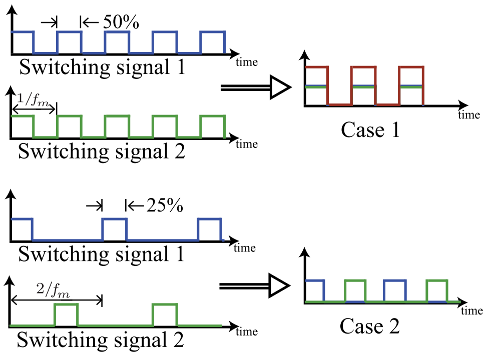


Fig. 2. Proposed cases of coordinated attack.

2) Coordinated Switching Loads: In this attack form, we consider the situation where the adversary has access to more than one load, and investigate how this would impact attack structure and characteristics. Within this context two options prevail for load switching coordination (see also Fig. 2):

- Case 1: Switching both loads at f_{sw} with a 50% duty cycle[1] via (1) and with the quantity of switching load distributed between the two loads.
- Case 2: Switching both loads at a frequency that is half the targeted mode frequency $f_{\text{sw}} = \frac{f_m}{2}$ with a 25% duty cycle and a phase shift between the two switching signals as

$$
\begin{aligned}
S_1(t) &= \frac{1}{4}\left[\operatorname{sgn}(\sin(2\pi f_{\text{sw}} t)) + 1\right] \\
&\quad \times \left[\operatorname{sgn}\left(\sin\left(2\pi f_{\text{sw}}\left(t - \frac{1}{4f_{\text{sw}}}\right)\right)\right) + 1\right] \\
S_2(t) &= S_1(t + \tau_0)
\end{aligned}
\tag{2}
$$

where τ_0 represents an appropriate phase shift, and a switch value of 1 or 0 represents a closed or open switch position, respectively.

The nonlinear power system characteristics preclude the use of superposition theory to predict system behavior. Thus, later in the paper, we empirically investigate the effects of coordinated switching as a function of phase difference and frequency range to determine the stealthier implementations.

E. Stealthiness

In the context of cyber-physical systems, a stealthy attack is defined as one that cannot be observed using existing detection measures during an active phase of attack until significant physical disruption ensues. For example, the well-known class of false data injection attacks is considered stealthy if bad data detection cannot flag measurement corruption [19]. Hence, stealthy attacks can be particularly worrisome due to the potential damage possible before identification.

For the proposed inter-area switching attack, system operators are usually aware of the system state and the changes that occur including variations in the load. We assert, however, that slow load switching at a frequency less than 1 Hz will not alarm the system operator as it resembles natural load variations. Moreover, coordinated attacks further increase stealthiness by decreasing the switching frequency and quantity of load switched at each attack location. To further mask the attack from system operators, an adversary could also consider simultaneously inducing a fault into the system.

III. Small-Signal Stability and Inter-Area Oscillations

In this section, we introduce a high level summary of power systems small signal stability concept and how it relates to inter-area oscillatory modes exploited in the proposed attack model. Small-signal stability refers to maintaining synchronism between synchronous machines when subjected to small disturbances and has been considered an important aspect of power system analysis. In current power systems, small-signal stability problems are often related to insufficient damping of system electromechanical oscillations [17]. Eigenvalue analysis of a linearized power system model is a well-known and commonly used approach to investigate the properties of inter-area oscillations in multi-machine power system models [17], [20], [21].

A. System Model

The dynamics of a multi-machine power system can be described using a nonlinear state-space representation:

$$\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{u})\boldsymbol{y} = \boldsymbol{g}(\boldsymbol{x}, \boldsymbol{u}) \tag{3}$$

where $\boldsymbol{x}, \boldsymbol{u}, \boldsymbol{y}$ are the state vector, system input vector and system output vector, respectively, and $\boldsymbol{f}, \boldsymbol{g}$ are nonlinear functions mapping the state and input vectors to the system dynamics and output, respectively. Small-signal stability considers the stability of the power system under small perturbations; hence, system dynamics can be linearized around an equilibrium point. Let $(\boldsymbol{x_0}, \boldsymbol{u_0})$ be the initial state vector and the initial input vector, respectively, corresponding to the equilibrium point of interest; thus, $\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x_0}, \boldsymbol{u_0}) = 0$.

For a small deviation $(\boldsymbol{\Delta x}, \boldsymbol{\Delta u})$, we represent the state and input as $\boldsymbol{x} = \boldsymbol{x_0} + \boldsymbol{\Delta x}$ and $\boldsymbol{u} = \boldsymbol{u_0} + \boldsymbol{\Delta u}$, respectively. Then, the linearized form of (3) can be formulated as

$$
\begin{aligned}
\boldsymbol{\Delta \dot{x}} &= \boldsymbol{A \Delta x} + \boldsymbol{B \Delta u} \\
\boldsymbol{\Delta y} &= \boldsymbol{C \Delta x} + \boldsymbol{D \Delta u}
\end{aligned}
\tag{4}
$$

where $\boldsymbol{A}$ is the state matrix, which is also the Jacobian matrix with elements a_{ij} corresponding to the partial derivatives $\partial f_i / \partial x_j$ (where f_i, x_j are the ith and jth element of $\boldsymbol{f}, \boldsymbol{x}$, respectively) evaluated at the equilibrium point of interest.

B. Eigenvalues and Stability

For small-signal stability study of the power system, eigenvalue analysis is conducted on the state matrix $\boldsymbol{A}$ of the linearized system model. The results of this eigenvalue analysis is presented in the form of right and left eigenvectors $(\boldsymbol{\psi}, \boldsymbol{\phi})$ [17]:

$$
\begin{aligned}
\boldsymbol{\psi_i A} &= \lambda_i \boldsymbol{\psi_i} \\
\boldsymbol{A \phi_i} &= \lambda_i \boldsymbol{\phi_i} .
\end{aligned}
\tag{5}
$$

Let $\boldsymbol{\Phi} = [\boldsymbol{\phi_1}, \boldsymbol{\phi_2}, \ldots, \boldsymbol{\phi_n}]$, then the following quadratic form results:

$$\boldsymbol{\Phi^{-1} A \Phi = \Lambda} \tag{6}$$

[1] The duty cycle of a pulse wave signal is defined as the ratio of the active signal time over the overall time for one waveform cycle.

where $\mathbf{\Lambda}$ is a diagonal matrix with eigenvalues λ_i as the diagonal elements. Stability of the power system is determined by λ_i where a real eigenvalue would correspond to a non-oscillatory mode, a negative real eigenvalue represents a decaying mode, and a positive real eigenvalue represents instability. Moreover, complex eigenvalues, that usually occur in conjugate pairs, correspond to oscillatory modes.

For a complex pair of eigenvalues expressed as $\lambda = \sigma \pm j\varpi$, the corresponding frequency of oscillation f in Hz is calculated by

$$f = \frac{\varpi}{2\pi} \tag{7}$$

and the damping ratio ξ is given by

$$\xi = \frac{-\sigma}{\sqrt{\sigma^2 + \varpi^2}}\,. \tag{8}$$

In the next section, we illustrate how to obtain an estimate of the targeted inter-area oscillatory mode.

IV. Probing the Targeted Inter-Area Modes

Success of the proposed class of attacks depends, at its core, on the effectiveness of the reconnaissance phase; i.e., effectively identifying the frequencies of inter-area mode of oscillation through offline analysis of line measurements following an induced fault. Several measurement-based approaches to estimate the frequency of different inter-area modes exist in literature [22]. Examples include masking signal-based empirical mode decomposition [22], spectral ICA [23], [24], Prony analysis [25], Yule-Walker methods [26], least squares algorithms [27], and subspace methods [28].

In this paper, we adopt the spectral ICA method due to its invariance to time delays and phase lag, and it's immunity to noise in the measured data [23], [24]; nevertheless, we believe that other methods could be easily applied. In our setup, the input data to this method is the frequency deviation signal recorded at the L_{sw} bus. Once the adversary induces a fault, this data is gathered over the time following the fault until the system settles to steady state. The output of the spectral ICA method is the frequency of oscillation of the targeted inter-area mode. This frequency is used to identify the switching frequency of the proposed switching attack.

The ICA approach is used to separate/recover unobserved signals or sources from an observed mixture without previous knowledge of the system properties or specifications [24], [29]. ICA assumes that the observed signal is a mixture of independent non-gaussian components, and seeks to maximize the statistical independence between the components, e.g., maximize kurtosis (non-Gaussianity). Mathematically, ICA aim to decompose an input matrix $\boldsymbol{X}$ into independent non-Gaussian components (ICs) such that:

$$\boldsymbol{X} = \boldsymbol{W}\boldsymbol{C} \tag{9}$$

where the rows of $\boldsymbol{C}$ are the ICs of the system and $\boldsymbol{W}$ is the *mixing matrix* that relates the ICs to the measured signal. For spectral ICA method, the power spectral densities of the measured time series are used as the rows of $\boldsymbol{X}$. ICA decomposition on the power spectra of signal measurements such as frequency deviation signal in our setup is able to separate the signals into their frequency components and estimate the inter-area oscillatory modes. Therefore, the identified ICs in our setup constitutes the modes of oscillation characterizing the power system. A set of these ICs are the inter-area modes, of which one is selected to be targeted in the proposed class of attacks [23]. To estimate the mixing matrix and the ICs, a fast fixed point algorithm is employed, which maximizes the Kurtosis of the different ICs [30]. Further implementation details are found in [23], [30], and [31].

V. Numerical Results

To illustrate the analysis, model, and impact of the inter-area switching attack we consider two power system models. We start with the four-machine two-area power system [17] as an illustrative example to help arrive at insights, and we then verify our observations on the Northeast Power Coordinating Council 68-bus system.

The index adopted for this study is the *time-to-instability*. This measure is defined as the time difference between the start of the switching attack and the time that the first system generator's angular speed exceeds 1.025 pu [32]; this threshold signifies when over-speeding protection is activated resulting in generator tripping and subsequent considerable mismatch between system generation and load.

A. Four-Machine Two-Area Power System

As an illustrative example we consider the small-signal stability of a two-area four-machine power system [17], shown in Fig. 3. The system is composed of two similar areas connected via a weak tie; each area consists of two coupled synchronous generators. Each generator has a rating of 900 MVA and 20 kV.

Further, each generator circuitry is represented by a fourth-order rotor electrical dynamic model. The stator electrical circuit is represented in the network steady-state model. For each generator, the magnetic saturation effects of both axes are included in the model. Input mechanical power to each generator is assumed to remain unchanged and the governor system dynamics are not considered. All generators are equipped with DC excitation systems. The system data is available in [17].

Simulation time step is 1.667 msec and each simulation case provides 20 seconds of dynamic response of the system subsequent to a disturbance [33]. The simulated response is sampled at the rate of 120 Hz. An analytical eigenvalue analysis of the four-machine two-area system, given the knowledge of the system state matrix $\boldsymbol{A}$, shows that the power system exhibits the eigenvalues and modes of oscillation shown in Table I [17].

Based on the above identified modes of oscillation, the first mode corresponding to $f_m = 0.5293$ Hz could be considered as an effective target frequency candidate. This choice is attractive for two reasons:

- the $f_m = 0.5293$ mode represents the lowest inter-area switching frequency, which aids in achieving stealth; and
- the oscillatory mode is the least-damped (i.e., has smallest σ value) potentially making it the easiest mode to drive the system to instability.

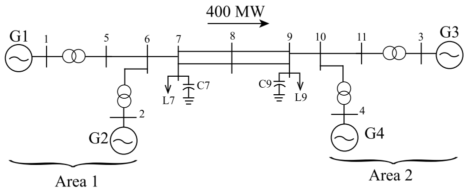


Fig. 3. The four-machine two-area power system.

TABLE I
FOUR-MACHINE TWO-AREA SYSTEM OSCILLATORY MODES

No.	Eigenvalue		Frequency (Hz)	Damping Ratio
	σ	ϖ		
1	**-0.0447**	**±3.3256**	**0.5293**	**1.3%**
2	-0.5575	±6.7107	1.0680	8.3%
3	-0.5638	±6.9352	1.1038	8.1%
4	-0.3793	±0.3334	0.0531	75.1%
5	-0.3984	±0.3300	0.0525	77.0%
6	-0.7400	±0.4663	0.0742	84.6%
7	-5.0527	±1.7660	0.2811	94.4%
8	-4.3874	±1.3211	0.2103	95.8%
9	-6.2695	±1.5562	0.2477	97.1%
10	-6.3100	±1.5564	0.2477	97.1%
11	-34.5597	±0.0817	0.0130	100%

1) Inter-Area Mode Frequency Estimation: Following the threat model and reconnaissance phase presented in Section II, a 3-phase fault is imposed at Bus 7 at which the switching load is connected for a duration of 80 msec. After clearing the fault, the power system is left to settle down with its own dynamics, while the frequency deviation signal at Bus 7 is recorded. The frequency deviation signal is calculated from the rate of change of the phase angle of the bus voltage as

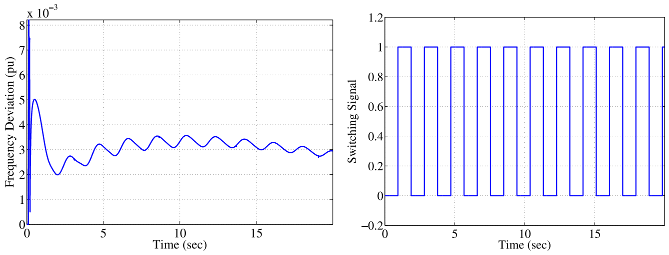
$$\Delta f_7\Big|_{t+\Delta t} = \frac{1}{\omega_0}\left(\frac{\theta_7\Big|_{t+\Delta t} - \theta_7\Big|_{t}}{\Delta t}\right) \tag{10}$$

where ω_0 is the system nominal frequency, θ_7 is the voltage phase angle of Bus 7, and t and $t + \Delta t$ are time instants. Fig. 4(a) shows the recorded signal used as the input data to the spectral ICA method.

Applying the spectral ICA method to the above signal resulted in identifying a dominant IC of frequency $f_m = 0.55$ Hz. This value is very close to the frequency of the inter-area mode identified from the small-signal analysis of the system. However, since the estimated frequency is not exactly the same as the calculated one, the sensitivity of the attack strength to the change of the estimated value of the inter-area mode will be studied further in Section. V-A4.

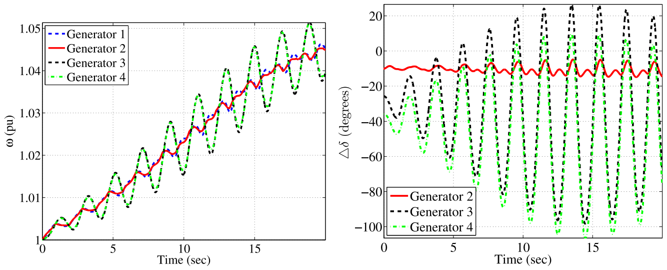
2) Switching at the Targeted Mode Frequency: Using the estimated value of the inter-area mode of oscillation, the switching attack is initiated on the test system. Fig. 4(b) shows the switching signal used in the attack, which represents the control signal to the circuit breaker of L_{sw} (at Bus 7).

Fig. 5 illustrates the impact of the switching attack on the generators' angular speed ω and relative internal angle $\Delta\delta$. In this attack, 5% of the total system load is switched (i.e., 14% of the load connected at Bus 7). It is clear that the proposed attack quickly drives the power system to instability. Although we have not included the models of speed governors and turbines, it is important to state that the system was driven to instability before traditional speed governors and the turbines would have reacted. As shown, the attack is able to destabilize the system at around 10 seconds, which is typically less than such devices time constants [34]. Thus, speed governors and turbines would begin to respond after the generators would have been tripped by the out-of-step protection.



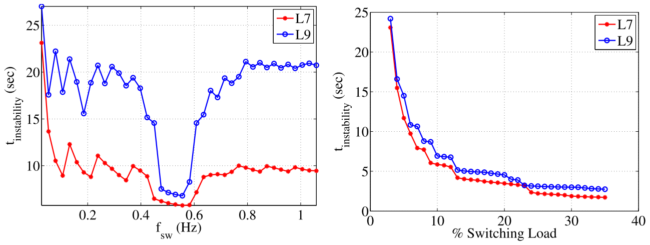
(a) frequency deviation signal recorded at Bus 7 (b) controlled load switching signal

Fig. 4. Single load attack.



(a) rotor speed (b) rotor relative angle

Fig. 5. Impact of single load attack on angular speed and internal angle of system generators.



(a) Impact of f_{sw} for 10% switching load (b) Impact of percentage of switching load at $f_{\mathrm{sw}} = 0.5293$ Hz

Fig. 6. Time-to-instability of single load attack on *L*7 and *L*9.

3) Load Selection: Given the target mode and previous analysis, we compare the attack impact when conducted using *L*7 or *L*9 on either side of the tie-line. The goal of this investigation is to assess the sensitivity of attack success to load selection. Results of Fig. 6 demonstrate that switching either load exhibits similar time-to-instability behavior at the targeted mode frequency.

4) Sensitivity Analysis: The sensitivity of the proposed attack to the switching frequency and the portion of the load being switched are studied here. Several simulation cases are considered where the load switching frequency f_{sw} is varied through the range of inter-area oscillations. Results of this

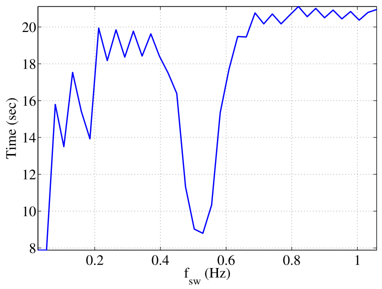


Fig. 7. Time-to-instability vs. switching frequency.

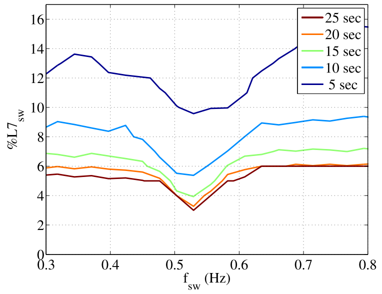


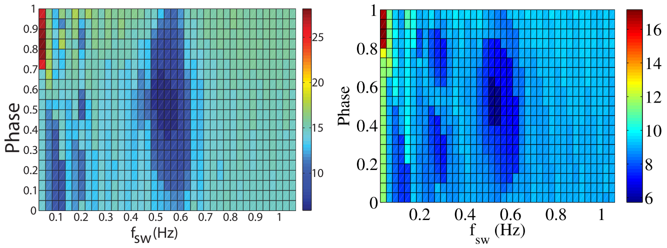
Fig. 8. Contour map of time-to-instability of different switching loads vs. switching frequency.

study are shown in Fig. 7. It is clear that the lowest time-to-instability in the range of frequencies [0.4−0.7] Hz is achieved at a switching frequency of $f_{\text{sw}} = 0.529$ Hz. This is the same frequency as the inter-area mode extracted by the eigenvalue analysis of Table I. Further, it is noted that an adversary with an estimated switching frequency of $f_m = 0.55$ Hz, extracted through the ICA analysis, is able to successfully conduct the attack as confirmed by these results.

Moreover, the lowest time-to-instability is achieved at $f_{\text{sw}} = 0.05$ Hz. This is actually a frequency of another oscillatory mode in the system as shown in Table I. However, the frequency of this mode is not estimated by the ICA method due to its high damping ratio (∼ 75%). Additionally, this mode is not an inter-area mode but a mode related to the flux linkage of the synchronous generators.

We further study the sensitivity of the attack (with respect to time-to-instability) to the percentage of switching load $\%L7_{\text{sw}}$ and the switching frequency f_{sw}. Fig. 8 depicts these results as a contour map showing time-to-instability curves as boundaries. While this figure emphasizes the previous observation, it further describes the relationship between the time-to-instability and $\%L7_{\text{sw}}$, where it shows that to achieve instability in a shorter time the adversary would need to control and switch a higher percentage of the load.

5) Coordinated Switching Loads: We next investigate the possible cases of coordinated switching loads previously described in Section II-D2, where an adversary has an access to more than one load. For the simulation setup these loads are *L*7 and *L*9. Due to the non-linearity of the power system, we study the impact of varying the frequency of the switching signals, as well as the phase difference between them.



(a) 50% duty cycle

(b) 25% duty cycle

Fig. 9. Coordinated attack on *L*7 and *L*9 with variable phase difference between the switching signals.

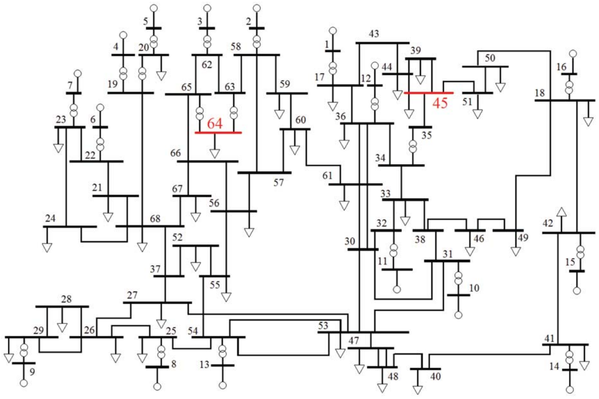


Fig. 10. A schematic diagram of the NPCC equivalent system.

Fig. 9 shows these results for the cases of 50% and 25% duty cycle. Time-to-instability is shown in color-coded surface rendering for a variable phase difference and a variable switching frequency.

For Case 1 (i.e., 50% duty cycle), the lowest time-to-instability is observed for a wide range of phase difference values between 35% and 70%, and a switching frequency in the range of (0.5 − 0.58) Hz. These observations suggest that to target the oscillation mode of interest, a coordinated attack is very possible with little coordination between the two switching loads. A conservative 50% phase difference could be assumed by the adversary at the two loads.

In Case 2 (i.e., 25% duty cycle), we arrive at two distinct interesting observations:

- at the targeted oscillatory mode $f_{\text{sw}} = f_m = 0.529$ Hz, we have a more sensitive range of phase difference values around (35 − 65)%; and
- at a switching frequency $f_{sw} = \frac{f_m}{2} = 0.264$ Hz, we notice that we can actually obtain a low time-to-instability in two ranges of phase shifts centered around 25% and 75%, which results in targeting the mode of 0.529 Hz. This is interesting due to the increased stealthiness of this approach as it uses half of the target mode frequency.

B. NPCC 68-Bus System

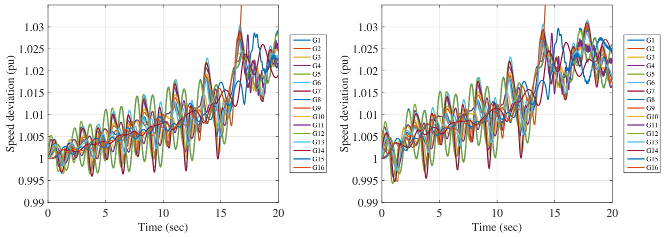
The proposed attack is applied on a study system representing an equivalent of the Northeast Power Coordinating Council (NPCC) system [35], shown in Fig. 10, which includes 16 conventional power plants, 68 high-voltage buses, 66 transmission lines, and 35 loads. Each conventional power plant (GEN)

TABLE II
NPCC SYSTEM OSCILLATORY MODES

Control Oscillatory Modes			Electromechanical Oscillatory Modes			
#	Freq. (Hz)	Damping ξ (%)	#	Freq. (Hz)	Damping ξ (%)	Mode Type
1	0.0264	100%	12	1.8831	6.91%	Local Modes
2	0.0451	99.69%	13	1.5631	8.01%	
3	0.0955	88.23%	14	1.5492	5.48%	
4	0.1332	85.93%	15	1.5373	7.48%	
5	1.6200	85.67%	16	1.4216	2.71%	
6	0.1585	84.31%	17	1.3385	3.61%	
7	0.0882	83.93%	18	1.2637	7.52%	
8	0.0907	79.69%	19	1.2227	6.53%	
9	0.0977	78.99%	20	1.2148	4.76%	
10	0.0946	77.65%	21	1.2051	6.40%	
11	0.3361	61.42%	22	1.0740	6.51%	
			23	0.8104	5.52%	Inter-Area Modes
			24	0.7653	4.29%	
			25	0.5602	6.66%	
			26	0.4242	7.71%	

TABLE III
NPCC SYSTEM ANALYTICAL INTER-AREA OSCILLATORY MODES AND ICA ESTIMATED MODES

Mode	Analytical (Hz)	ICA Estimated (Hz)	Error
23	0.8104	0.831	2.5%
24	0.7653	0.732	4.3%
25	0.5602	0.534	4.6%
26	0.4242	0.445	4.9%



(a) without masking fault

(b) with masking fault

Fig. 11. Angular speed of system generators.

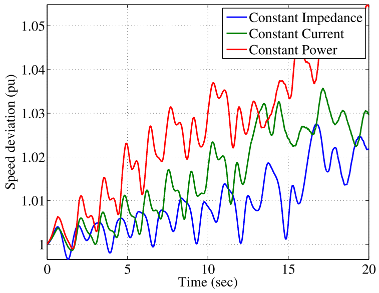


Fig. 12. Angular Speed of GEN2 for different system load models, and coordinated switching of loads at Bus 64 and Bus 45.

is represented by the same electro-mechanical model of generators of the two-area power system of Fig. 3. Generators connected to Buses $2-8$ and 13 are equipped with DC excitation systems and the unit connected at Bus 9 (GEN-9) is equipped with a static exciter [20], while the remaining generators are under constant excitation. In addition, GEN-9 is equipped with a Power System Stabilizer (PSS) driven by the rotor speed deviation signal [20]. Further, each transmission line is modeled as an equivalent π model with lumped parameters in the network phasor model. Finally, each load is modeled as constant impedance and included in the network phasor model.

Based on eigen analysis [36], the study system includes 26 oscillatory modes as shown in Table II. By inspecting the different modes, the following is observed in relation to the context of this paper:

- the least-damped modes (16 and 17) are primarily affected by the power system stabilizer of GEN-9;
- mode 26 represents oscillations of GEN-9 and GEN-13 against those of the New York system;
- mode 24 represents oscillations of generators $(2-7)$ of the New England system against generators of New York system. Therefore, New England system can be divided into two groups, one includes GEN-8, GEN-9 and GEN-13 and the other includes generators $(2-7)$. These two groups do not oscillate against each other; and
- the other two inter-area modes represent oscillations of New York system generators against GEN-14 (Ontario), GEN-15 (Michigan) and GEN-16 (PJM).

Initially the study system is at steady state, and a 5-cycle, 3-ph-G fault is imposed at Bus-64 to identify the frequency of oscillation of the targeted inter-area mode. Table III enumerates the identified inter-area modes estimated through ICA with reasonable accuracy. The estimated frequency of the targeted mode is found to be $f_m = 0.732$ Hz which is very close to the frequency of mode 24 in Table II. The value of $f_m = 0.732$ Hz is used as the inter-area switching attack frequency. The single load and coordinated load switching attacks are studied in the system, where similar results are observed to those of the four-machine two-area power system. Due to space limitation, we only include results for the coordinated attack.

The switching loads are at Bus 64 and Bus 45. The coordinated switching attack begins at $t = 0$ sec with a switching frequency of 0.366 Hz for each load and a switching signal of duty cycle equal to 25% and a phase shift of 25% between the two switching signals. This switching is conducted to verify the observation obtained based on the four-machine two-area coordinated attack. Fig. 11(a) shows the angular speed of system generators for the coordinated switching attack, where the targeted inter-area mode is excited due to the imposed switching and GEN-16 is driven to instability at $t = 16.5$ s.

For the proposed scenario in the 68 bus system, the switching load is comprised of the loads at Bus 45 (208 MW) and at Bus 64 (9 MW), where the two loads combined represent 1.23% of the total system load (17620.7 MW). This may collectively may represent heating loads of commercial blocks or urban high rise buildings during, say, cold winter days when exterior temperatures reach $-15°$C degrees. Therefore, an adversary can possibly carry the attack by controlling the supply point of urban centers.

Different power system load models, i.e., constant impedance, constant power and constant current representations were considered. All the three representations result in similar system behavior in response to inter-area switching attacks, with varying time-to-instability. Figure 12 illustrates the angular speed deviation of GEN2 for the three system load models, where the constant impedance load model exhibits the lowest time-to-instability. The simulation results represent the limiting cases of the system behavior for the different load models. We assert that any composite load model of the system will exhibit behaviors that are within the characteristics captured by these limiting cases thus enabling similar conclusions on attack impact.

Further, an adversary could consider "hiding" the load switching action from the system operator by introducing a fault concurrently with the load switching. Introducing the fault would "mask" the adversary action from the system operator such that the source of instability is unidentified during the attack; resulting in increased stealthiness. The "masking" fault is imposed at the beginning of the inter-area switching attack at $t = 0$ sec. A similar system response with slightly lower time-to-instability is observed with the "masking" fault as is illustrated in Fig. 11(b).

C. Prevention and Detection

As can be concluded from results above, the proposed class of attacks could pose a serious threat to power systems exhibiting inter-area oscillatory modes. The work presented in this paper aims to highlight existing power systems vulnerabilities that can be exploited with increasingly stealthy attacks, hence encouraging system operator to re-evaluate existing measures for prevention and detection. The stealthiness of the proposed attack challenges existing mechanisms for alarming suspicious behaviour in the power system. One possible deterrence against inter-area switching attacks is to enhance the power system's inherit inter-area oscillatory modes damping thus limiting the impact of such attacks. The proposed attack, in addition to previous switching attacks, suggest the need for new mechanisms for close monitoring of loads in the evolving power system. An alarm would be raised if systematic switching at a frequency close to an inter-area oscillation mode is observed. If such systematic switching is observed at the frequencies of concern (or at fractions of these frequencies), then possible countermeasures could involve actuation of an energy storage system to reverse the impact of the switching in each area.

VI. Conclusion

A new class of cyber-physical smart grid switching attacks is presented in this paper. The proposed inter-area switching attack is of particular interest due to its low switching frequency (supporting stealth) and the lack of knowledge of the full system state (promoting practicality). The attack targets the inter-area modes of a power system driving coherent groups of generators out of step. During reconnaissance, an adversary conducting the attack estimates a low-damping inter-area mode by imposing a transient fault, and utilizing a measurements based signal analysis approach to identify and estimate the frequency of an inter-area mode of oscillation. During execution, the adversary switches part of the system load on and off at an estimated inter-area mode target frequency driving the power system to instability.

Results of this work show that low-frequency switching of a small percentage of the load can quickly drive the power system to instability. Further, we show that the proposed attack can be successfully conducted through switching a single load or a coordinated switching of two loads. Increased stealthiness of the coordinated form of the attack was observed through switching the two loads at half the frequency of the targeted mode. Impact, characteristics and forms of the attack are illustrated using the four-machine two-area power system and verified using the NPCC 68-bus system.

References

[1] *Guidelines for Smart Grid Cybersecurity NISTIR 7628 Revision 1*, document NISTIR 7628, Nat. Inst. Stand. Technol., Sep. 2014, pp. 1–668.

[2] *Energy Sector Cybersecurity Framework Implementation Guidance*, U.S. Dept. Energy Office Elect. Del. Energy Rel., Washington, DC, USA, Jan. 2015, pp. 1–53.

[3] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, May/Jun. 2011.

[4] K. Zetter. (2015). *A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever*. Accessed on Feb. 2016. [Online]. Available: http://www.wired.com/2015/01/german-steel-mill-hack-destruction/

[5] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," SANS Ind. Control Syst., Mar. 2016. [Online]. Available: https://pdfs.semanticscholar.org/8d21/ac4f42533126c4449c10c3ae6f5709d319f2.pdf

[6] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "Switched system models for coordinated cyber-physical attack construction and simulation," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Brussels, Belgium, Oct. 2011, pp. 49–54.

[7] S. Liu, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "Coordinated variable structure switching attack in the presence of model error and state estimation," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Tainan, Taiwan, Nov. 2012, pp. 318–323.

[8] 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. Gener. Meeting (PESGM)*, San Diego, CA, USA, Jul. 2012, pp. 1–6.

[9] A. K. Farraj, E. M. Hammad, D. Kundur, and K. L. Butler-Purry, "Practical limitations of sliding-mode switching attacks on smart grid systems," in *Proc. IEEE Power Energy Soc. Gener. Meeting (PESGM)*, National Harbor, MD, USA, Jul. 2014, pp. 1–5.

[10] D. Liberzon, *Switching in Systems and Control* (Systems & Control: Foundations & Applications). Boston, MA, USA: Birkhäuser, 2003.

[11] A. K. Farraj and D. Kundur, "On using energy storage systems in switching attacks that destabilize smart grid systems," in *Proc. IEEE PES Conf. Innov. Smart Grid Technol. (ISGT)*, Washington, DC, USA, Feb. 2015, pp. 1–5.

[12] J. Meserve. (Sep. 26, 2007). *Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid*. Accessed on Jul. 2016. [Online]. Available: http://www.cnn.com/2007/US/09/26/power.at.risk/index.html

[13] J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1643–1653, Jul. 2014.

[14] A. K. Farraj, E. M. Hammad, A. Al Daoud, and D. Kundur, "A game-theoretic control approach to mitigate cyber switching attacks in smart grid systems," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Venice, Italy, Nov. 2014, pp. 958–963.

[15] A. Farraj, E. Hammad, and D. Kundur, "On using distributed control schemes to mitigate switching attacks in smart grids," in *Proc. IEEE Can. Conf. Elect. Comput. Eng. (CCECE)*, Halifax, NS, Canada, May 2015, pp. 1578–1582.

[16] F. Dörfler, M. Chertkov, and F. Bullo, "Synchronization in complex oscillator networks and smart grids," *Proc. Nat. Acad. Sci. USA*, vol. 110, no. 6, pp. 2005–2010, 2013.

[17] P. Kundur, N. J. Balu, and M. G. Lauby, *Power System Stability and Control* (EPRI Power System Engineering Series). New York, NY, USA: McGraw-Hill, 1994.

[18] T. Flick and J. Morehouse, *Securing the Smart Grid: Next Generation Power Grid Security*. Burlington, MA, USA: Elsevier, 2010.

[19] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Security (TISSEC)*, vol. 14, no. 1, 2011, Art. no. 13.

[20] P. W. Sauer and M. A. Pai, *Power System Dynamics and Stability*. Upper Saddle River, NJ, USA: Prentice-Hall, 1998.

[21] Y. Chompoobutrgool, "Concepts for power system small signal stability analysis and feedback control design considering synchrophasor measurements," Licentiate thesis, KTH School Elect. Eng., KTH Roy. Inst. Technol., Stockholm, Sweden, 2012.

[22] A. R. Messina, *Inter-Area Oscillations in Power Systems: A Nonlinear and Nonstationary Perspective*. New York, NY, USA: Springer, 2009.

[23] M. A. M. Ariff and B. C. Pal, "Coherency identification in interconnected power system—An independent component analysis approach," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1747–1755, May 2013.

[24] J. Thambirajah, N. F. Thornhill, and B. C. Pal, "A multivariate approach towards interarea oscillation damping estimation under ambient conditions via independent component analysis and random decrement," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 315–322, Feb. 2011.

[25] J. F. Hauer, C. J. Demeure, and L. L. Scharf, "Initial results in Prony analysis of power system response signals," *IEEE Trans. Power Syst.*, vol. 5, no. 1, pp. 80–89, Feb. 1990.

[26] R. W. Wies, J. W. Pierre, and D. J. Trudnowski, "Use of ARMA block processing for estimating stationary low-frequency electromechanical modes of power systems," *IEEE Trans. Power Syst.*, vol. 18, no. 1, pp. 167–173, Feb. 2003.

[27] R. W. Wies, A. Balasubramanian, and J. W. Pierre, "Combining least mean squares adaptive filter and auto-regressive block processing techniques for estimating the low-frequency electromechanical modes in power systems," in *Proc. IEEE Power Energy Soc. Gener. Meeting (PESGM)*, Montreal, QC, Canada, 2006, p. 8.

[28] M. Larsson and D. S. Laila, "Monitoring of inter-area oscillations under ambient conditions using subspace identification," in *Proc. IEEE Power Energy Soc. Gener. Meeting (PESGM)*, Calgary, AB, Canada, 2009, pp. 1–6.

[29] J.-F. Cardoso, "Blind signal separation: Statistical principles," *Proc. IEEE*, vol. 86, no. 10, pp. 2009–2025, Oct. 1998.

[30] A. Hyvärinen and E. Oja, "A fast fixed-point algorithm for independent component analysis," *Neural Comput.*, vol. 9, no. 7, pp. 1483–1492, 1997.

[31] C. Xia and J. Howell, "Isolating multiple sources of plant-wide oscillations via independent component analysis," *Control Eng. Pract.*, vol. 13, no. 8, pp. 1027–1035, 2005.

[32] B. J. Kirby *et al.*, *Frequency Control Concerns in the North American Electric Power System*. Washington, DC, USA: U.S. Dept. Energy, 2003.

[33] 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.

[34] P. M. Anderson and A. A. Fouad, *Power System Control and Stability*. Piscataway, NJ, USA: Wiley, 2008.

[35] B. Pal and B. Chaudhuri, *Robust Control in Power Systems* (Power Electronics and Power Systems). New York, NY, USA: Springer, 2006.

[36] A. Mohammed, "Impacts of high-depth of penetration of wind power on interconnected power systems dynamics," Ph.D. dissertation, The Edward S. Rogers Sr. Dept. Elect. Comput. Eng., Univ. Toronto, Toronto, ON, Canada, 2016.

Eman Hammad (S'14) received the B.Sc. degree in electrical engineering from the University of Jordan and the M.Sc. degree in electrical engineering from Texas A&M University. She is currently pursuing the Ph.D. degree with the Department of Electrical Engineering, University of Toronto. Her current research interests include cyber-physical systems with particular interest in cyber-security, resilient control, and cooperative game theory in the context of smart grids. She was a recipient of many awards, and is currently serving as the IEEE Toronto Communication Society Chapter Chair.

Ahmed M. Khalil (S'13–M'16) received the B.Eng. and M.Sc. degrees in electrical engineering from Cairo University and the Ph.D. degree in electrical engineering from the University of Toronto. He is currently with the Electrical Power and Machines Department, Faculty of Engineering, Cairo University, Cairo, Egypt, and also with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada. His research interests include large-scale integration of renewable energy resources and power systems dynamics and control.

Abdallah Farraj (S'11–M'12) received the B.Sc. and M.Sc. degrees in electrical engineering from the University of Jordan in 2000 and 2005, respectively, and the Ph.D. degree in electrical engineering from Texas A&M University in 2012. He is a Fulbright Scholar. He is currently a Post-Doctoral Fellow with the University of Toronto. His research interests include modeling and analysis of cyber-physical systems, cyber security of smart grids, cognitive communications, and downhole telemetry systems.

Deepa Kundur (F'15) received the B.A.Sc., M.A.Sc., and Ph.D. degrees in electrical and computer engineering from the University of Toronto in 1993, 1995, and 1999, respectively. She currently serves as the Chair of the Division of Engineering Science and a Professor of Electrical and Computer Engineering with the University of Toronto. From 1999 to 2002, she was a Faculty Member with Electrical and Computer Engineering, University of Toronto, and from 2003 to 2012, she was a Faculty Member with Electrical and Computer Engineering, Texas A&M University.

She has authored over 150 journal and conference papers. Her research interests lie at the interface of cyber security, signal processing, and complex dynamical networks. She has participated on several editorial boards and currently serves on the Advisory Board of IEEE Spectrum. She currently serves as the Symposium Co-Chair for the Communications for the Smart Grid Track of ICC 2017 and the TPC Co-Chair for IEEE SmartGridComm 2018. Recently, she also served as the General Chair for the Workshop on Communications, Computation and Control for Resilient Smart Energy Systems at ACM e-Energy 2016, the Workshop on Cyber-Physical Smart Grid Security and Resilience at Globecom 2016, the Symposium on Signal and Information Processing for Smart Grid Infrastructures at GlobalSIP 2016, the 2015 International Conference on Smart Grids for Smart Cities, the 2015 Smart Grid Resilience (SGR) Workshop at IEEE GLOBECOM 2015, and the IEEE GlobalSIP 15 Symposium on Signal and Information Processing for Optimizing Future Energy Systems.

Dr. Kundurs was a recipient of the Best Paper Recognitions at numerous venues including the 2015 IEEE Smart Grid Communications Conference, the 2015 IEEE Electrical Power and Energy Conference, the 2012 IEEE Canadian Conference on Electrical & Computer Engineering, the 2011 Cyber Security and Information Intelligence Research Workshop, and the 2008 IEEE INFOCOM Workshop on Mission Critical Networks and the Teaching Awards at both the University of Toronto and Texas A&M University. She is a fellow of the Canadian Academy of Engineering.

Reza Iravani (M'87–SM'00–F'03) received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering. Currently, he is a Professor with the University of Toronto, Toronto, Canada. His research interests include power system dynamics and applications of power electronics in power systems.