A Coordinated Multi-Switch Attack for Cascading Failures in Smart Grid

Shan Liu, Bo Chen, Takis Zourntos, Deepa Kundur, and Karen Butler-Purry

***Abstract*—This paper explores distributed smart grid attack strategies to destabilize power system components using variable structure system theory. Here, an opponent is able to remotely control multiple circuit breakers within a power system, say through data corruption or communication network attack, to destabilize target synchronous generators through application of state-dependent breaker switching. In contrast to attack via a single breaker, the multi-switch case provides additional degrees of freedom that can lead to stealthier and wide-scale cascading failures. We provide a dynamical systems context for formulating distributed multi-switch strategies and execute such attacks on the New England 10-generator 39-bus test system.**

***Index Terms*—Coordinated multi-switch attacks, cyber-physical system security, sliding mode theory, smart grid attacks, variable structure system modeling.**

I. Introduction

IT IS WELL known that the smart grid promises increased reliability, efficiency and sustainability through the use of advanced information (cyber) and energy (physical) infrastructure. This greater dependence on information systems however raises concerns as to how its integration will affect the cyber and physical security of future power systems.

Historically, such cyber-enablement of classical application fields including commerce, entertainment, and social interactions has led to improved functionality and efficiency at the cost of security. Thus, we assert the importance of addressing cyber and physical security issues of emerging cyber-enabled power systems. A first step in such a study will require the exploration of novel vulnerabilities stemming from cyber-physical integration, which we aim to address in this paper, to better develop strategies for their mitigation.

There has been a movement toward addressing cyber-physical aspects of system security. For instance, information confidentiality has been addressed by studying cyber-to-physical leakage via clues about cyber protocol activity in power system voltage and current measurements [1], [2]. Novel risk analysis frameworks that account for the physical impacts of cyber attacks have been presented [3], [4]. To more comprehensively account for the interaction between the power system and information network, empirical approaches have been developed that harness realistic communications and power systems simulators [5].

We argue that to identify insidious weaknesses stemming from cyber-physical interaction and evaluate mitigation approaches, it is crucial that the physical notion of time be incorporated into the modeling framework. Furthermore, we believe that for the results to have useful meaning to electric power utilities and for risk analysis, the model should loosely represent select aspects of the system physics with appropriate granularity. For this reason, our work represents a departure from prior art by formulating the smart grid security problem within a hybrid dynamical system context that is mathematically representable and relates attack impacts to disturbances on quantifiable power system performance metrics.

Our past work has focused on the application of variable structure system theory to address a class of reconfiguration attacks in power transmission systems called coordinated variable structure switching attacks [6]–[11]. We have been able to identify a novel class of vulnerabilities unique to smart power systems that leverages the potential of an opponent to obtain estimates of localized state information and remotely control an associated circuit breaker. Here, an opponent can employ the local state information to design a switching sequence for the breaker that can cause transient instability of a target synchronous generator leading to power disruption. One key observation from these studies is the ease with which it is possible to destabilize the power system dynamics (through the exploitation of vulnerabilities in cyber infrastructure) by using short-duration cyber-controlled switching of a single breaker.

In this paper, we aim to provide a more comprehensive assessment of the security posture of a smart grid system by focusing on a non-trivial extension to the single-switch coordinated switching attack that makes use of multiple breaker corruptions and collusion to create cascading failures within multiple targets of the system. This shifts the vulnerability analysis problem from one that can be visualized in a two-dimensional plane to one in higher-order dimensions. Moreover, construction of an attack has significantly greater degrees of freedom that we explore by considering *simultaneous*, *concurrent* and *progressive* approaches to switching. We therefore test our attack framework for the first time on the 10-machine, 39-bus New England power system in DSATools™ providing an opportunity to study the effectiveness of the coordinated switching attack on generators with local controllers.

In the next section, we present our multi-switch hybrid dynamical systems modeling framework. Section III provides mathematical examples to give insight on the different ways in

Manuscript received November 21, 2012; revised May 02, 2013, August 08, 2013; accepted January 22, 2014. Date of publication April 11, 2014; date of current version April 17, 2014. Paper no. TSG-00808-2012.

S. Liu is with the Department of Network Engineering, Communication University of China, Beijing 100024, China.

B. Chen, T. Zourntos, and K. Butler-Purry are Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843 USA.

D. Kundur is with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON L5L 1C6, Canada.

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.2014.2302476

which multiple switching can be harnessed for system disruption. In Section IV we demonstrate how the multi-switch attack principles can be applied to the popular 39-bus New England test power system for targeted and more global power system disruptions through transient destabilization of select system generators. Final remarks and avenues for future research are presented in Section V.

II. Distributed Multi-Switch Framework

A. Variable Structure Systems

Variable structure systems represent an elegant hybrid dynamical systems framework in which to study the behavior of systems with switched dynamics. Here, the dynamics of a system with state $x \in \mathbb{R}^{n\times 1}$ change (or switch) to one of a set of predefined subsystems depending on the value of a *switching signal* $s(x,t)$ that is time and/or state-dependent. In the case of scalar $s(x,t)$ and two subsystems a general structure for a variable structure system can be given by:

$$\dot{x} = \begin{cases} f_1(x,t) & s(x,t) \geq 0 \\ f_2(x,t) & s(x,t) < 0 \end{cases}. \tag{1}$$

For certain structures and parameters of system dynamics and selections of $s(x,t)$, it can be shown that the overall switched system exhibits *sliding mode* behavior. In the sliding mode, while switching persists, the state of the overall switched system is attracted to and stays on the $s(x,t) = 0$ manifold termed a *sliding surface* of the variable structure system. The sliding mode property of variable structure systems has been useful classically for system stabilization to steer the system state from possible instability to a desirable equilibrium position. An excellent background on sliding mode control can be found in [12], [13] and references therein; moreover, [14] provides an excellent tutorial on the subject.

Recently, the authors have modeled smart grid transmission systems under reconfiguration (e.g., remotely controlled "smart" circuit breaker switching) as variable structure systems. We have demonstrated how, in contrast, transient instability of a target synchronous generator can be induced by an opponent who has corrupted a circuit breaker and switches it open or closed depending on the sign of an appropriately defined $s(x,t)$ [6], [7]. The system state x represents the phase and frequency of the target generator and the switching has the effect of disrupting both the generator frequency and phase thus desynchronizing it.

Much of the analysis of variable structure systems within the existing literature assumes a single scalar switching signal $s(x,t) \in \mathbb{R}$. In this vein, the authors' past work has considered the application of sliding mode theory when a *single* circuit breaker is corrupted and employed for transient instability of a *sole* target synchronous generator. Such a formulation is valuable for identifying local cyber-physical vulnerabilities within smart grid systems, but by nature cannot model potential distributed attacks that can lead to cascading failures.

B. Distributed Switching for Attack

We consider a power system consisting of $M > 0$ circuit breakers or switches. We assume that an opponent (or possibly a colluding collective of opponents) has control over $0 < m \leq M$ breakers through, say, corruption of breaker control signals via attacks on the associated communication network, as discussed in [6], [7]. The objective of the opponent is to disrupt the operation of the power system through transient destabilization of one or more target synchronous generators denoted $\{G_t\}, t = 1, 2, \ldots, T$ assuming that the opponent has some knowledge of the target generator states. Such destabilization will cause generator protection relays to trip taking the corresponding generators off-line. Although loss of a single generator may not be of significant concern, in our distributed multi-switch framework we investigate the effects of possible cascading outages.

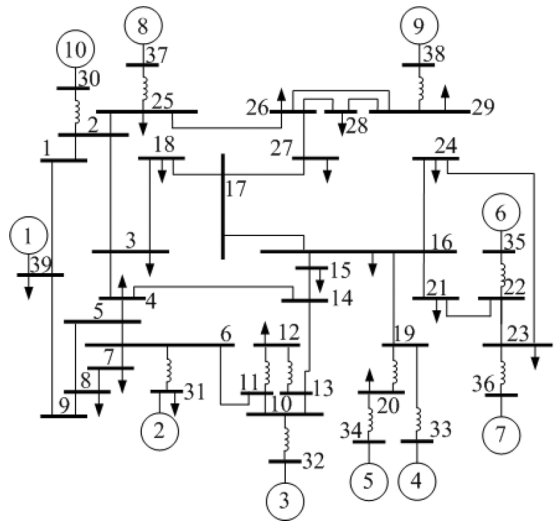


Fig. 1. New England 10-machine, 39-bus power system.

We consider the situation in which the strategy of the opponent is to model the overall system as a variable structure system and apply state-dependent switching to the corrupted switches such that sliding mode behavior is manifested. If the particular sliding mode is unstable, then transient instability of target synchronous generators will be induced. Consider for example the 39-bus New England test system of Fig. 1. Suppose that an opponent has control over the breakers connecting Lines 26–28 and 28–29 and has established Generators 8 and 9 as targets. The task of the opponent would be to construct a switching sequence based on variable structure system theory using knowledge of the phase and frequencies of Generators 8 and 9 for each of the switches at Line 26–28 and Line 28–29. If successful, the switching would induce sliding mode behavior and thus transient destabilization of its targets. Questions naturally arise regarding how multi-switching should be strategized.

Thus, part of our focus in this paper is to explore different ways to incorporate multiple corrupted switches to target multiple synchronous generators. In the next section, we provide a general variable structure system framework. The model is somewhat general so that the attack may be readily applicable to other forms of instability (e.g., frequency and voltage) and for other types of target components such as transformers or transmission lines beyond the scope of this paper. Moreover, it enables us to consider different multi-switch attack strategies within the same system to assess the various compromises. In

Section IV we specifically focus on transient destabilization and our models are more specific.

C. Multiple Switching Signals

The multi-switch investigation necessitates that the switching signal of Section II-A be a *switching vector* signal $s(x,t) \in \mathbb{R}^{m\times 1}$ where $m > 1$ is the number of corrupted switches; the sign of each element of $s(x,t)$ provides information to an opponent on whether to open or close a specific breaker for attack. There is limited variable structure system theory literature dedicated to this extended multi-switch situation. We do not provide theoretical foundations for this underdeveloped class of problems. In contrast, we aim to explore through examples how the multiple switch problem can be constructed and exploited for system destabilization. For the remainder of the paper we consider only time-invariant state-dependent vector switching signals and denote it for simplicity as either $s(x)$ or s.

Consider a nth order linear time invariant variable structure system model with m control inputs:

$$\dot{x} = Ax + Bu, \tag{2}$$

where $x \in \mathbb{R}^{n\times 1}$ is the time-dependent state vector, $u \in \mathbb{R}^{m\times 1}$ is the input vector, $A \in \mathbb{R}^{n\times n}$ is the system transformation matrix and $B \in \mathbb{R}^{n\times m}$ is the input matrix. The time-invariant state-dependent switching signal is defined as

$$s(x) = Cx \in \mathbb{R}^{m\times 1}, \tag{3}$$

where $s(x) = 0$ is called the *switching surface* and $C \in \mathbb{R}^{m\times n}$ is the corresponding coefficient matrix; we denote the ith element of s as $s_i \in \mathbb{R}$ such that $s = [s_1\ s_2\ \ldots\ s_m]^T$. For tractability, most switching signals are assumed to be linear combinations of the system states. In our interpretation of the problem a single circuit breaker, say called Switch i, is controlled via the sign of the ith element of s. Therefore, our framework implicitly assumes that m controllable breakers exist in the system.

The role of u in our formulation is two-fold. First, it represents an appropriate step change in dynamics due to a sign change in the elements of $s(x)$; thus we expect $\mathrm{sgn}(s_i)$ components in u to have the desired effect of switching the nature of the dynamics as the signs of the switching signal elements change. Second, it modifies the system dynamics Ax in our instructive example of Section III using a second order linear feedback component to guarantee an appropriate sliding mode exists for a given $s = Cx$ and multi-switch strategy. The reader should note that in an actual power system attack scenario addressed in Section IV, the action of an opponent would result only in the first s-dependent component.

Consider switching surfaces $s_i = 0$ for $i = 1, 2, \ldots, m$ whereby their *intersection* is compactly denoted $s = \mathbf{0}$ meaning $s = [s_1\ s_2\ \ldots\ s_m]^T = [0\ 0\ \ldots\ 0]^T$. To determine the existence of the sliding surface $s = \mathbf{0}$ for a general class of variable structure systems it is *sufficient* to establish that the following condition holds (for $s \neq \mathbf{0}$) [14]:

$$s^T \dot{s} < 0. \tag{4}$$

Typically, the guarantee that (4) holds occurs for a local region of state space. Thus a state trajectory would have to enter this local region to guarantee attraction to the sliding surface $s = \mathbf{0}$; once the state is within the region of attraction persistent sliding mode switching will guarantee that the state is attracted to $s = \mathbf{0}$ and remains on that surface.

Condition (4) does not guarantee that the individual sliding surfaces $s_i = 0$ exist for $i = 1, 2, \ldots, m$. If they exist for a subset $j \in \mathcal{S} \subseteq \{1, 2, \ldots, m\}$ then the following additional conditions must hold, again, for a possibly local region about the sliding surface:

$$s_j \dot{s}_j < 0 \qquad j \in \mathcal{S}. \tag{5}$$

In the multi-switch cases that follow, we consider the scenario in which each of the m switches open and close according to the sign of a particular element of $s = [s_1\ s_2\ \ldots s_m]^T$. For example, the ith switch would open for $s_i < 0$ and close when $s_i \geq 0$. The terminal sliding surface for attack is the intersection of all of the *individual switching surfaces* $s = \mathbf{0}$. Moreover we assume that individual sliding surfaces exist for $s_j = 0$ for $j \in \mathcal{S}$. The existence of individual sliding surfaces provided by (5) enables the possibility of employing a variety of multi-switch strategies that we investigate for power system attack in this paper.

Throughout the paper the authors adopt a compact notation common to systems theory to describe the dynamical representations and variables. However such a convention, albeit simpler, may not readily provide information on temporal or state dependencies that could better elucidate the concepts and relationships in a power systems context. Therefore, we provide a summary in Table I of the key variables of this paper and their associated dependencies.

D. Attack Assumptions and Overview

A vulnerability in a system exists when there is a flaw in the system, access to the flaw and a capability by an opponent to exploit the flaw. We consider the vulnerability we address in this paper to be cyber-physical in nature because a *physical* weakness is exploited through access provided by *cyber* (communications) means.

In order to study a worst-case scenario for disruption we assume that attacker communication is ideal and that corrupted breakers are temporally synchronized in their switching. Moreover, we assume that physical catastrophe instigated by the proposed attack does not affect the performance of the associated communication system.

1) Attacker Knoweldge: To leverage variable structure system theory to construct a smart grid attack, an opponent would need:

1) to identify a set of (physical) target synchronous generators to attack denoted $\{G_t\}, t = 1, 2, \ldots, T$;
2) electromechanical switching control over $m > 1$ corrupted circuit breakers in the targets' proximity;
3) knowledge of the targets' states x; and
4) a local model of the smart grid system encompassing the targets.

TABLE I
VARIABLE DIMENSIONS, DEPENDENCIES AND NOTATION. PLEASE NOTE THAT MODEL PARAMETERS SUCH AS C, c_i, A_i AND b_i ARE CONSTANTS WITH NO TEMPORAL OR STATE DEPENDENCIES

Quantity	Dependencies	Common notation(s) used	Dimensions	Other possible description(s)
state	time	x	$\mathbb{R}^{n\times 1}$	$x(t)$
state trajectory/derivative	time	$\dot{x}$	$\mathbb{R}^{n\times 1}$	$\dot{x}(t)$
state element	time	x_i	$\mathbb{R}$	$x_i(t)$
state element derivative	time	$\dot{x}_i$	$\mathbb{R}$	$\dot{x}_i(t)$, $\frac{dx_i(t)}{dt}$
switching vector	state (for this paper)	$s(x)$ or s	$\mathbb{R}^{m\times 1}$	$s(x(t))$
switching signal	state (for this paper)	$s_i(x)$ or s_i	$\mathbb{R}$	$s_i(x(t))$
derivative of switching vector	state and time	$\dot{s}$	$\mathbb{R}^{m\times 1}$	$\dot{s}(x)$
derivative of switching signal	state and time	$\dot{s}_i$	$\mathbb{R}$	$\dot{s}_i(x)$, $\dot{s}_i(x(t))$
equivalent control	state and switching vector	u	$\mathbb{R}^{m\times 1}$	$u(t)$, $u(x,s)$
system transformation matrix	n/a (constant)	A	$\mathbb{R}^{n\times n}$	
input matrix	n/a (constant)	B	$\mathbb{R}^{n\times m}$	
sliding mode coefficients	n/a (constant)	C	$\mathbb{R}^{m\times n}$	
switching surface	state	$s=0$		$s(x)=0$
linear sliding surface	state	$s=Cx=0$		$Cx(t)=0$
rotor angle of G_i	time	δ_i	$\mathbb{R}$	$\delta_i(t)$
rotor angle derivative	time	$\dot{\delta}_i$	$\mathbb{R}$	$\dot{\delta}_i(t)$
rotor speed of G_i	time	ω_i	$\mathbb{R}$	$\omega_i(t)$
rotor speed derivative	time	$\dot{\omega}_i$	$\mathbb{R}$	$\dot{\omega}_i(t)$

Physical means to obtain such measurement data and control switching actions requires that the opponent employ geographically proximal and perhaps even distributed and unstealthy techniques, which is impractical for resource constrained opponents. However, with the increased dependence on information technology and its proposed large-scale connectivity, it is feasible that such approaches will be implemented remotely through an effective sequence of cyber intrusions.

In order to implement the attack remotely an opponent must exploit one or more cyber vulnerabilities within the associated communications and computing devices. Numerous practical examples of current and expected cyber weaknesses in power deliver networks have been documented [15] that range from exploiting the lack of cyber security mechanisms in legacy technology to exploiting holes in well known operating systems used by measurement and control devices. The types of cyber intrusions necessary to be able to execute a coordinated variable-structure switching attack will be specific to the actual system hardware and software and is beyond the scope of this work. However, common approaches may involve data interception, modification and fabrication. Direct means of cyber attack could involve the eavesdropping of local state information from phasor measurement units along communication links and the fabrication of circuit breaker control signals to implement the switching attack. Indirect means could entail the interception of related measurement information to estimate the current state and subsequent false data injection attacks on state estimators [16] to induce incorrect decision-making to force switching.

False data injection attacks are one form of cyber attack that can be exploited for coordinated switching attacks; they have recently been investigated by Liu *et al.* [16] in the context of state estimation. We highlight that indeed such attacks may be exploited to facilitate our proposed attack. Our work, in contrast, is focused on how cyber attacks such as these on the information system can be harnessed to exploit a physical weakness such as sliding mode instability to establish a new form of *cyber-physical* vulnerability that has the potential to bring about cascading failures.

2) Attack Construction and Execution: Based on this information an opponent would model the local grid as a variable structure system where x is given by the states of $\{G_t\}, t = 1, 2, \ldots, T$ and switching occurs at the corrupted breaker(s). An opponent would then construct an attack by determining an appropriate sliding mode surface $s = \mathbf{0}$ for system destabilization. The attack would be executed using knowledge of x such that the opponent would close (open) Breaker j for $s_j(x) > 0$ ($s_j(x) \leq 0$). The stages of attack construction (conducted off-line a priori) and execution can be represented as follows:

1) Select the target generators $\{G_t\}, t = 1, 2, \ldots, T$ for which state information is available or can be estimated.
2) Select the m corrupted or corruptible breakers.
3) Mathematically represent the associated target smart grid system as a variable structure system keeping the switching rule $s(x) \in \mathbb{R}^{m\times 1}$ general, where the jth breaker status is controlled by the value of the jth element of s for $j = 1, 2, \ldots, m$.
4) Test the existence of sliding mode surfaces according to (4) and (5). If a range of C exists for attack then select a value analytically or empirically; details beyond the scope of this paper are provided in [8].
5) Based on the existence of the overall and individual switching surfaces, design a strategy for multiple switching as we will discuss in Section III.

6) Execute the attack by employing switching of the m corrupted breakers such that Breaker j is closed (open) for $s_j(x) > 0 (s_j(x) \leq 0)$.

The reader should note that for a given smart grid system, set of target generators $\{G_t\}, t = 1, 2, \ldots, T$ and set of m corrupted breakers, a range of C may be valid for attack although it is possible that no value for C exists to instigate sliding mode behavior. In the former situation, typically the attack can achieve its goal within the order of seconds for any valid value of C, but depending on the specific value of C, the particular system state behavior toward instability would be different. In the latter case, no coordinated variable structure switching attack is possible. In such a situation, the opponent could attempt to change the set of target generators or expand the set of corrupt breakers. The reader should note that existence of the sliding mode thus provides a convenient way to assess the existence of vulnerabilities and prioritize system components for hardening as discussed by the authors in [8].

III. Multiple Switching and the Sliding Mode

We consider three approaches to illustrate how multiple corrupted switches can be exploited by an opponent for system disruption. For simplicity we focus on a two-swxitch situation in which $s = [s_1 \ s_2]^T$; the general m-switch case would represent a natural extension to this multi-switch foundation. We first consider a case, called *synchronized switching*, whereby the switches have the same switching surfaces $s_1 = s_2 = C^1 x = 0$ thus are synchronized with switching occurring simultaneously. Next, we focus on the case of *concurrent switching*, in which the switches have distinct switching surfaces $s_1 = C^1 x = 0$ and $s_2 = C^2 x = 0$ with switching occurring simultaneously. Last, we focus on *progressive switching* where switches with distinct switching surfaces begin in tandem.

To demonstrate the application of different strategies for multi-switch variable structure system attacks, we make use of the following fundamental third-order canonical form realization of the linear time-invariant system of (2):

$$\dot{x}(t) = \underbrace{\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}}_{x} + \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}}_{B} \underbrace{\begin{bmatrix} u_1 \\ u_2 \end{bmatrix}}_{u}. \tag{6}$$

As discussed in Section II-C, we assign the input $u = [u_1 \ u_2]^T$ to be not only s-dependent to represent the effects of switching, but also x-dependent to adjust the system dynamics such that appropriate sliding modes exist to illustrate various switching strategies within the same context.

The two switching surfaces are represented as:

$$s = Cx = \begin{bmatrix} c_1^1 & c_2^1 & c_3^1 \\ c_1^2 & c_2^2 & c_3^2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}, \tag{7}$$

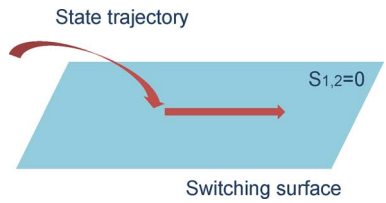


Fig. 2. State trajectory for synchronized switching.

where $C^i = [c_1^i \ c_2^i \ c_3^i]$ is the coefficient vector of $s_i, i = 1, 2$. In Section IV, the opponent-corrupted switches are operated such that when switching is applied, Switch i opens if $s_i < 0$ and closes if $s_i \geq 0$ for $i = 1, 2$.

A. Synchronized Switching

We first consider the synchronized switching case where $C^1 = C^2$ because it provides a natural bridge between our former single switch work [6], [7] and the multi-switch extension in this paper. For the synchronized case, by definition $s_1 = s_2 = s_{1,2}$ which implies that the sliding surface $s = [s_1 \ s_2]^T = \mathbf{0}$ can also be represented as $s_{1,2} = 0$ and that $s_{1,2} = c_1^1 x_1 + c_2^1 x_2 + c_3^1 x_3$. We assume that the sliding surface $s_{1,2} = 0$ exists. The strategy here is to simultaneously and persistently apply synchronized switching (i.e., having both switches open and close at the same time) to Switches 1 and 2. To be effective switching must occur when $x(t)$ is in the region of attraction of the $s_{1,2} = 0$ sliding surface and consequently the state will be driven to $s_{1,2} = 0$ as illustrated in Fig. 2. In this case the existence of $s_{1,2} = 0$ (equivalent to $s = \mathbf{0}$) also implies the existence of the individual sliding surfaces.

To develop an illustrative example of the effects of simultaneous switching, we consider our canonical system of (6) and determine a $u_{1,2} = u_1 = u_2$ to guarantee $s_{1,2}\dot{s}_{1,2} < 0$. Consider:

$$s_{1,2}\dot{s}_{1,2} = s_{1,2}C^1\dot{x} = s_{1,2}C^1(Ax + Bu) < 0, \tag{8}$$

where $u = [u_{1,2} \ u_{1,2}]^T$. There are a variety of strategies to assign $u_{1,2}$ to guarantee sliding mode existence. In this paper we assign $u_{1,2}$ such that $s_{1,2}\dot{s}_{1,2} = -|s_{1,2}| < 0$, a common approach within the sliding mode community. We therefore determine $u_{1,2}$ such that $s_{1,2}C^1Ax + s_{1,2}C^1Bu = -|s_{1,2}| = -s_{1,2} \cdot \mathrm{sgn}(s_{1,2})$ which simplifies to give

$$u_{1,2} = -\frac{c_1^1 x_2 + c_2^1 x_3 + c_3^1(\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3) + \mathrm{sgn}(s_{1,2})}{c_2^1 + c_3^1}. \tag{9}$$

and an overall description of the system dynamics with concurrent switching:

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = \frac{-c_3^1\alpha_1 x_1 - (c_1^1 + c_3^1\alpha_2)x_2 + (c_3^1 - c_3^1\alpha_3)x_3 - \mathrm{sgn}(s_{1,2})}{c_2^1 + c_3^1} \\ \dot{x}_3 = \frac{c_2^1\alpha_1 x_1 + (c_2^1\alpha_2 - c_1^1)x_2 + (c_2^1\alpha_3 - c_2^1)x_3 - \mathrm{sgn}(s_{1,2})}{c_2^1 + c_3^1} \end{cases}. \tag{10}$$

The dynamics of (10) describes the system's evolution (attraction) toward $s_{1,2} = 0$.

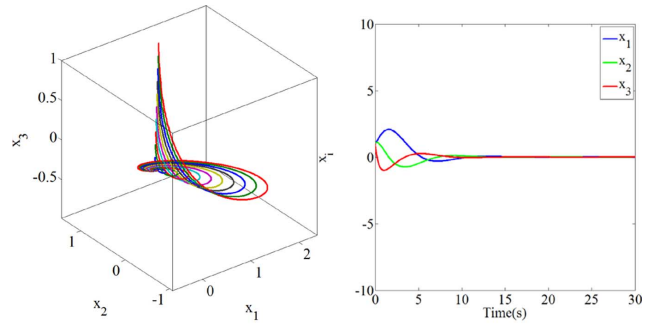


Fig. 3. State trajectories and states values for canonical system. (a) System trajectories. (b) System states versus time.

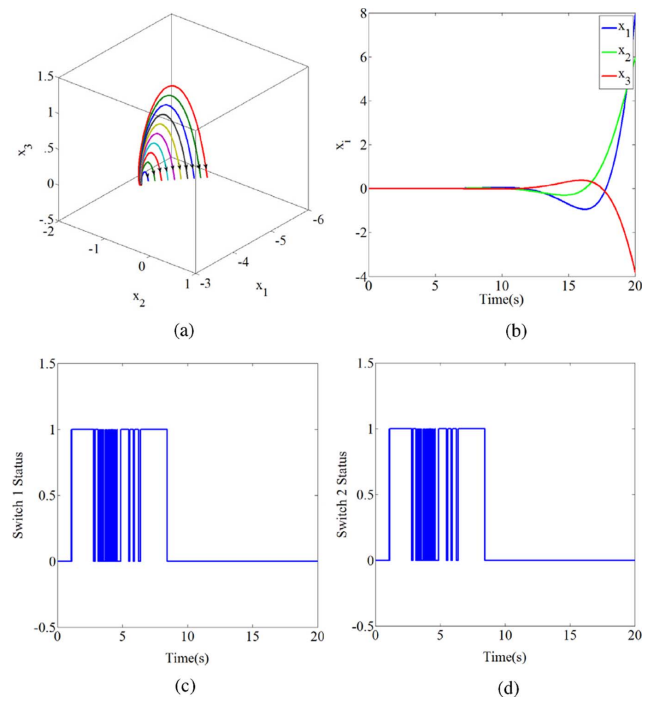


Fig. 4. System trajectories and states for synchronized switching. (a) System trajectories. (b) System states. (c) Switch 1 status. (d) Switch 2 status.

1) Numerical Illustration: Consider the canonical system for $\alpha_1 = -1, \alpha_2 = -2$ and $\alpha_3 = -3$. The original system state trajectories and state values as a function of time are shown in Figs. 3(a) and (b), respectively, demonstrating the stable nature of the overall system. To apply a switching attack, C^1 is selected such that:

$$C^1 = [-1 \ -2 \ 1]. \tag{11}$$

The corresponding simulation results are shown in Fig. 4. As can be observed, the system achieves instability demonstrating the how the simultaneous switching case can disrupt system operation.

B. Concurrent Switching

We next consider the situation in which the sliding surface $s = \mathbf{0}$ exists and the strategy is to simultaneously and persistently apply sliding mode switching to Switches 1 and 2. To be effective, switching must begin when $x(t)$ is in the region of attraction of the $s = \mathbf{0}$ sliding surface and consequently the state

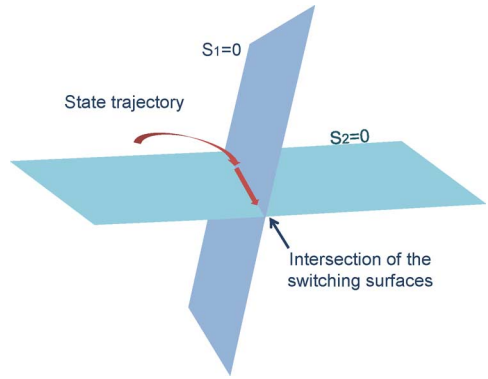


Fig. 5. State trajectory for concurrent switching.

will be driven to $s = \mathbf{0}$ as illustrated in Fig. 5. In this concurrent switching case, individual sliding modes do not have to exist.

To develop an illustrative example of the effects of such concurrent switching, we once again consider our canonical system of (6) and determine a u to guarantee $s^T\dot{s} < 0$. Such a system will have resulting dynamics that we will use to demonstrate the effects of system disruption due to multi-switch attacks. Consider:

$$s^T\dot{s} = s^TC\dot{x} = s^TC(Ax + Bu) < 0. \tag{12}$$

There are a variety of strategies to assign u to guarantee sliding mode existence. We once again assign u such that $s^T\dot{s} = -|s| < 0$ as common and therefore determine u such that $s^TCAx + s^TCBu = -|s| = -s^T \cdot \mathrm{sgn}(s)$ to give $u = -(CB)^{-1}(CAx) - (CB)^{-1} \cdot \mathrm{sgn}(s)$ and an overall description of the system dynamics with concurrent switching:

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = \frac{\left(c_3^2c_1^1 - c_3^1c_1^2\right)x_2 + c_3^2 \cdot \mathrm{sgn}(s_1) - c_3^1 \cdot \mathrm{sgn}(s_2)}{c_3^1c_2^2 - c_2^1c_3^2} \\ \dot{x}_3 = \frac{\left(c_2^1c_1^2 - c_2^2c_1^1\right)x_2 - c_2^2 \cdot \mathrm{sgn}(s_1) + c_2^1 \cdot \mathrm{sgn}(s_2)}{c_3^1c_2^2 - c_2^1c_3^2} \end{cases}. \tag{13}$$

1) Unstable Sliding Modes: Sliding mode control has been conventionally employed for stabilization. Thus, the resulting dynamics after the state reaches the sliding surface and remains there are stable. In contrast, for power system disruption, opponents aim to identify unstable sliding modes through appropriate selection of C.

We employ the method of equivalent control to determine an effective set of system dynamics on the $s = \mathbf{0}$ sliding surface. Therefore we set:

$$\dot{s} = C\dot{x} = C(Ax + Bu) = 0. \tag{14}$$

Solving for u gives us the equivalent control $u_{\mathrm{eq}} = -(CB)^{-1}CAx$. Thus, the effective system dynamics on the sliding surface becomes:

$$\dot{x} = Ax + Bu_{\mathrm{eq}} = Ax - B(CB)^{-1}CAx \tag{15}$$

$$= (I - B(CB)^{-1}C)Ax \tag{16}$$

$$= \underbrace{\begin{bmatrix} 0 & 1 & 0 \\ 0 & \frac{c_3^1c_1^2 - c_1^1c_3^2}{c_3^1c_2^2 - c_2^1c_3^2} & 0 \\ 0 & \frac{c_2^1c_1^2 - c_2^2c_1^1}{c_3^1c_2^2 - c_2^1c_3^2} & 0 \end{bmatrix}}_{(I - B(CB)^{-1}C)A} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}. \tag{17}$$

It is easy to see from the structure of matrix $(I-B(CB)^{-1}C)A$ that the eigenvalues are 0, 0 and $(c_3^1c_1^2 - c_1^1c_3^2)/(c_3^1c_2^2 - c_2^1c_3^2)$. Thus to guarantee instability of this linear system it is necessary that the non-zero eigenvalue be positive. Thus, C should be selected such that

$$\frac{c_3^1c_1^2 - c_1^1c_3^2}{c_3^1c_2^2 - c_2^1c_3^2} > 0. \tag{18}$$

It is clear that such a C exists with appropriately selected parameters. Thus a multi-switch attack is feasible in this case.

2) Numerical Illustration: Consider the canonical system for $\alpha_1 = -1, \alpha_2 = -2$ and $\alpha_3 = -3$. The original system state trajectories and state values as a function of time are shown in Figs. 3(a) and (b), respectively, demonstrating the stable nature of the overall system. To apply a switching attack, C is selected to fulfill Condition (18) by assigning:

$$C = \begin{bmatrix} c_1^1 & c_2^1 & c_3^1 \\ c_1^2 & c_2^2 & c_3^2 \end{bmatrix} = \begin{bmatrix} -1 & 2 & 1 \\ -2 & -1 & 1 \end{bmatrix}. \tag{19}$$

which provides eigenvalues for $(I-B(CB)^{-1}C)A$ at 0, 0 and $(1)/(3) > 0$ as desired. (13) describes the system's evolution to $s = \mathbf{0}$. Figs. 6(a) and (b) demonstrate the system state behavior and Figs. 6(c) and (d) give the switch status. It is clear that the switching induces system instability within a short period of time even when the original system is stable.

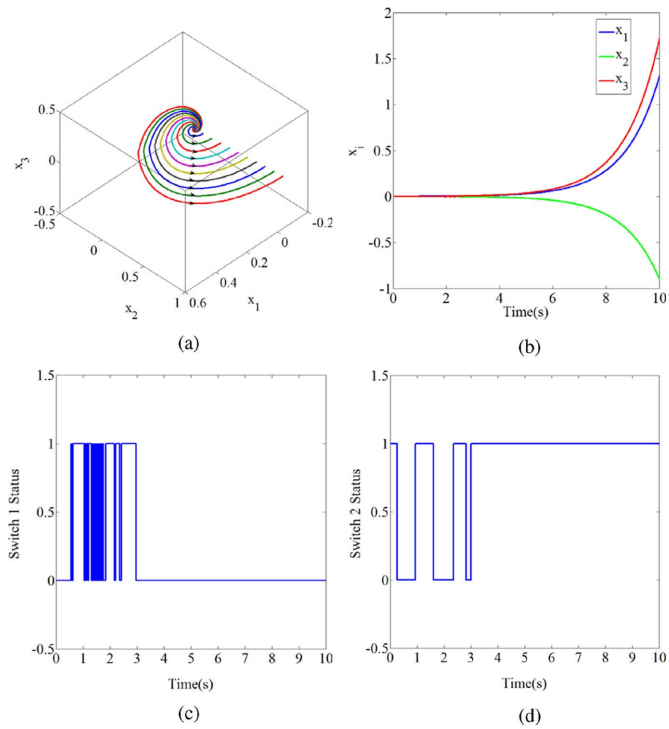


Fig. 6. System trajectories and states for concurrent switching. (a) System trajectories. (b) System states. (c) Switch 1 status. (d) Switch 2 status.

C. Progressive Switching

Consider the case in which the sliding surface $s = \mathbf{0}$ and an individual sliding surface $s_1 = 0$, say, both exist. For such a situation, it is possible for an opponent to apply concurrent switching as discussed in the previous section. There however may be disadvantages to this for a successful attack. First, the region of convergence for the $s = \mathbf{0}$ sliding surface may be difficult to reach for certain system conditions in which say the equilibrium position is distant from the region of convergence. Furthermore, the opponent may prefer to be stealthy for a period of time slowly moving the trajectory to a seemingly stable but vulnerable position prior to an appropriately timed disruption. The additional timing control that this provides to an opponent may be beneficial when intending to apply synchronized cyber-physical attacks on the overall system.

We demonstrate in this section how an opponent can apply *progressive* switching and appropriately leverage the existence of an individual sliding surface to improve the stealthiness of an attack. If we consider the two-switch case as illustrated in Fig. 7, the opponent's aim is to first apply Switch 1 to attract a state $x(t)$ that is within the region of attraction of the $s_1 = 0$ sliding surface and then, while $x(t)$ is moving on this individual sliding surface, add Switch 2 as well to attract the overall system to the $s = \mathbf{0}$ sliding surface. If the individual $s_1 = 0$ sliding mode is stable and the $s = \mathbf{0}$ sliding mode is unstable an initially stealthy but subsequently high impact attack is realized. We consider the progressive switching attack to have the following three stages.

Stage 1: The system state x is driven to the $s_1 = 0$ sliding surface. We make use of our canonical form system of (6) and illustrate this behavior by assigning an input u as follows:

$$u = -(C^1B)^{-1}(C^1Ax) - (C^1B)^{-1} \cdot \mathrm{sgn}(s_1), \tag{20}$$

that guarantees the existence of the $s_1 = 0$ sliding surface:$s_1\dot{s}_1 = s_1C^1\dot{x} = C^1(Ax+Bu) = -s_1 \cdot \mathrm{sgn}(s_1) = -|s_1| < 0$ to obtain the overall Stage 1 dynamics, shown in (21) at the bottom of the page.

Stage 2: The system state x enters and remains on the $s_1 = 0$ sliding surface. Here, the method of equivalent control can be employed to describe the effective dynamics in the presence of Switch 1 switching. We set $\dot{s}_1 = C^1\dot{x} = C^1(Ax+Bu) = 0$ to

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = \frac{1}{(c_3^1)^2+(c_2^1)^2}\left[c_2^1c_3^1\alpha_1x_1 + c_2^1\left(c_1^1+c_3^1\alpha_2\right)x_2 + \left(\left(c_3^1\right)^2\right.\right. \\ \left.\left. +2\left(c_2^1\right)^2 + c_2^1c_3^1\alpha_3\right)x_3 - c_2^1 \cdot \mathrm{sgn}(s_1)\right] \\ \dot{x}_3 = \frac{1}{(c_3^1)^2+(c_2^1)^2}\left[\left(2\left(c_3^1\right)^2\alpha_1 + \left(c_2^1\right)^2\alpha_1\right)x_1 + \left(2\left(c_3^1\right)^2\alpha_2 + \left(c_2^1\right)^2\alpha_2\right.\right. \\ \left.\left. +c_3^1c_1^1\right)x_2 + \left(2\left(c_3^1\right)^2\alpha_3 + \left(c_2^1\right)^2\alpha_3 + c_3^1c_2^1\right)x_3 - c_3^1 \cdot \mathrm{sgn}(s_1)\right] \end{cases}. \tag{21}$$

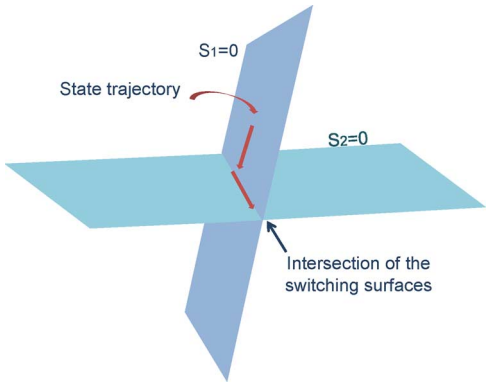


Fig. 7. State trajectory for progressive switching.

give $u_{\text{eq}} = -(C^1B)^{-1}(C^1Ax)$. Substituting this into (6) gives overall Stage 2 dynamics:

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = \frac{-c_2^1 c_3^1 \alpha_1 x_1 - c_2^1\left(c_1^1 + c_3^1\alpha_2\right)x_2 + c_3^1\left(c_3^1 - c_2^1\alpha_3\right)x_3}{\left(c_3^1\right)^2 + \left(c_2^1\right)^2} \\ \dot{x}_3 = \frac{\left(c_2^1\right)^2\alpha_1 x_1 + \left(\left(c_2^1\right)^2\alpha_2 - c_3^1 c_1^1\right)x_2 + c_2^1\left(c_2^1\alpha_3 - c_3^1\right)x_3}{\left(c_3^1\right)^2 + \left(c_2^1\right)^2} \end{cases}. \quad (22)$$

Analogous to Section III-B we can select C to guarantee, in contrast, the stability of the $s_1 = 0$ sliding surface.

Stage 3: The system state x is driven to the $s = \mathbf{0}$ sliding surface at the intersection of $s_1 = 0$ and $s_2 = 0$. To illustrate this behavior, we once again set $s^T\dot{s} < 0$ to give the Stage 3 dynamics of (13).

1) Numerical Illustration: Once again, we consider the stable canonical system for $\alpha_1 = -1, \alpha_2 = -2$ and $\alpha_3 = -3$. Using parallel reasoning to the concurrent switching example, the two switching surfaces are selected as:

$$C = \begin{bmatrix} 1 & 2 & -1 \\ -2 & -1 & -1 \end{bmatrix}. \quad (23)$$

The corresponding simulation results of system trajectories, system states, switches are shown in Fig. 8. As shown, during Stages 1 and 2, the system trajectory is attracted to the $s_1 = 0$ sliding surface and remains stable as Switch 1 is applied. However, when Switch 2 is applied the joint switching has the effect of destabilization the overall system when it is attracted to the $s = \mathbf{0}$ sliding surface.

IV. Simulations

In this section, we apply the multi-switch principles of the previous section to the New England 10-machine, 39-bus system of Fig. 1 employing DSA*Tools*™. The first step requires identification of attack parameters from our variable structure system model of the corresponding smart grid. Specifically, we make use of the swing equation model in which generators are not equipped with local controllers. The second step implements the designed attack in a simulation model that includes these controllers. The reader should note that although our swing equation model does not include generator control, our simulation model in DSA*Tools*™ includes excitation and governor control for more realistic assessment. The automatic voltage regulator (AVR) data is derived from

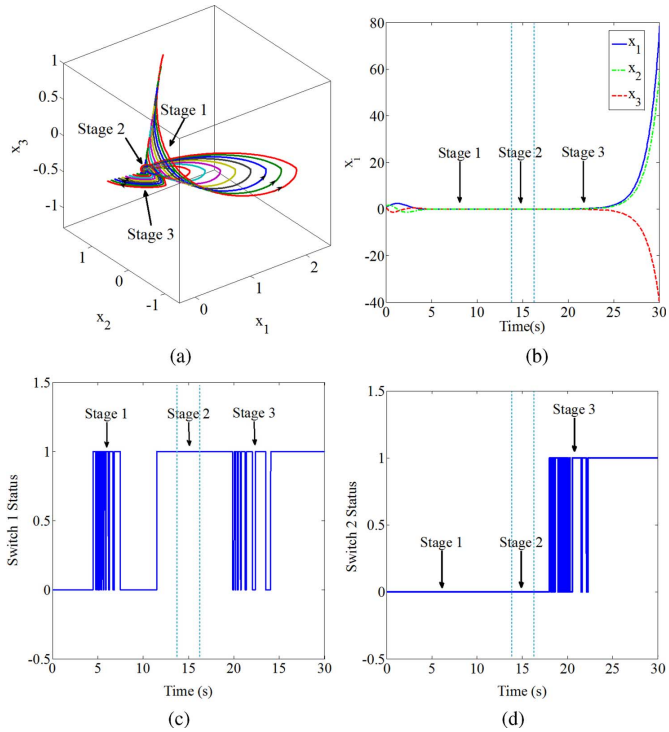


Fig. 8. System trajectories and states for progressive switching. (a) System trajectories. (b) System states. (c) Switch 1 status. (d) Switch 2 status.

`http://electrica.uc3m.es/pablole/new_england.html` (in PSS/E format), where the static and dynamic data have been obtained from the example files of PST toolbox (`http://www.ecse.rpi.edu/pst/PST.html`). The turbine governor data is from the PSS/E program application guide. Thus, our approach allows construction of an attack using idealized analytical models that can effectively execute under more realistic conditions.

Under non-attack conditions, the systems with AVR and turbine governors are robust and stable to disturbance. However, as we demonstrate in this section after our coordinated switching attack is applied, the system can become unstable within the order of seconds.

A. Attack Construction

An opponent's objective is to first construct an attack by selecting a multi-switch strategy and determining the parameters of C to disrupt power delivery using a model of the power system, and then execute the attack using local state information of target generators. Moreover, it can be shown that this attack is robust to model error and noisy states [10].

The overall system can be modeled via the swing equations with the following dynamics:

$$\begin{cases} \dot{\delta}_i = \omega_i - \omega_s \\ \dot{\omega}_i = \frac{1}{M_i}\left[P_{mi} - \Sigma_{k=1}^{10} E_i E_k |Y_{ik}| \cos\left(\delta_i - \delta_k - \angle Y_{ik}\right)\right] \end{cases}, \quad (24)$$

where $\delta_i, \omega_i, M_i, P_{mi}$ and E_i are the phase angle, frequency (with nominal frequency being 60 Hz), moment of inertia, mechanical power and terminal voltage of the ith generator. Y_{ik} is the Kron-reduced equivalent admittance between the ith and

kth generators. Typical parameter values for the New England system are assumed. The jth (corrupted) breaker in the system is assumed to target Generator t and incorporate the following switching signal with coefficients c_{j_1} and c_{j_2}:

$$s_j = c_{j_1}\delta_t + c_{j_2}\omega_t. \tag{25}$$

The overall system is assumed to be initially at a stable equilibrium point. The task of an opponent in control of the jth corrupted breaker would be to select the parameters c_{j_1} and c_{j_2} judiciously to induce instability in Generator t; this can be conducted empirically or analytically [8] using the model of (24). Execution of the attack on Generator t requires knowledge of δ_t and ω_t.

We consider the concurrent and progressive approaches to multi-switch attack and then consider how the multi-switch framework can be leveraged by an opponent to initiate cascading failures within the system. We do not provide results for the synchronized switching case, which is somewhat analogous to a single switch case since one common switching surface is used for all switches. Instead for comparative purposes, we provide results for the single switch case and compare it to our multi-switch case to see the attack performance gains possible.

B. Single Switch Attack

We first assume an opponent corrupts the breaker corresponding to Line 26–28 of Fig. 1 and targets Generator 9 to induce instability employing the sliding surface $s = -5\delta_9 + \omega_9$. Fig. 9 illustrates the corresponding effects on the system when switching is applied starting at 10 s for only a 2–3 second duration. Fig. 9(a) shows the state trajectory leading to instability while Figs. 9(b), (c), and (d) demonstrate the time scale upon which disruption occurs. The switch status used is presented in Fig. 9(e).

Next we consider the situation in which the breaker of Line 28–29 is corrupted and targets Generator 9 once again to induce instability using $s = -8\delta_9 + \omega_9$. Fig. 10 presents the results of the attack starting at 10 s demonstrating once again instability within 2–3 seconds of switching.

C. Concurrent Switching

We next consider the scenario in which an opponent simultaneously corrupts the breakers corresponding to Line 26–28 (Switch 1) and Line 28–29 (Switch 2) of Fig. 1 and targets Generator 9 once again to induce instability. The opponent is assumed to employ $s_1 = -5\delta_9 + \omega_9$ and $s_2 = -8\delta_9 + \omega_9$ for attack as in Section IV-B. Fig. 11 illustrates the corresponding effects on the system when concurrent switching is applied starting at 10 s for only a 1 second duration. Instability is clearly evident in frequency, angle, and voltage. It should be noted that the use of both switches in contrast to either single switch for attack results in faster instability with a shorter switch duration.

D. Progressive Switching

In this case we consider corruption of breakers on Line 02–25 (Switch 1) and Line 28–29 (Switch 2) with target Generator 8. Although it can be shown that an individual sliding mode does not exist for Switch 2, it does for Switch 1. Thus we employ progressive switching starting with Switch 1. We assume an opponent employs $s_1 = -7\delta_8 + \omega_8$ and $s_2 = -5\delta_8 + \omega_8$ and Switch 1 begins at 10.0 s and Switch 2 joins at 10.5 s appropriately coordinating with Switch 1. Fig. 12 demonstrates the effectiveness of the approach for system destabilization.

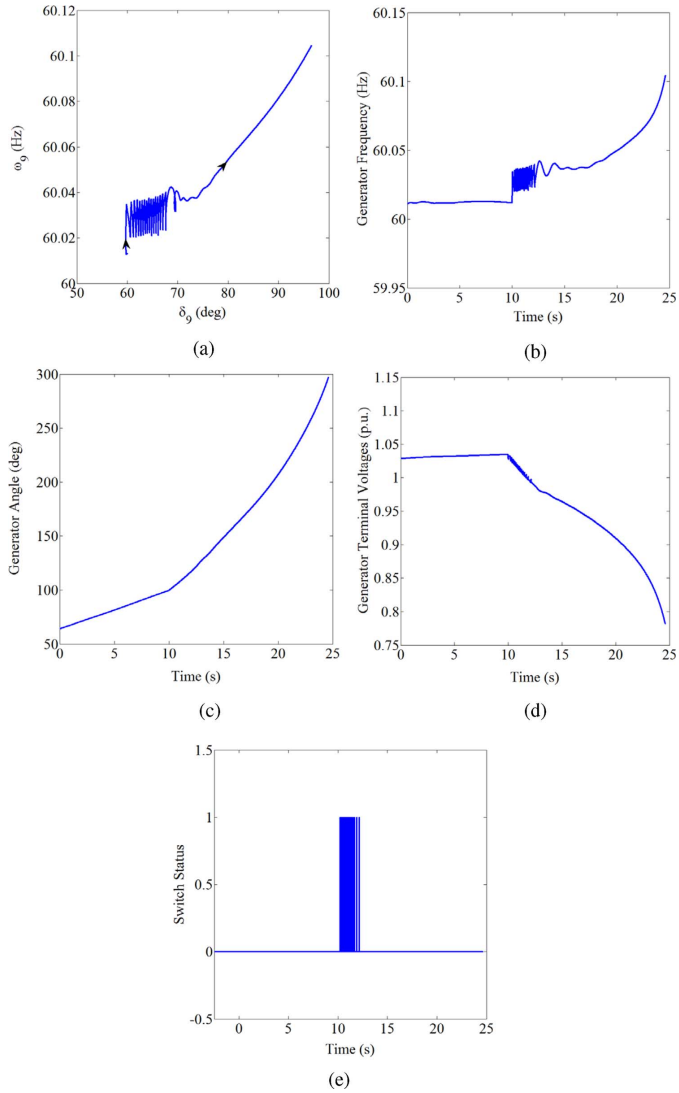


Fig. 9. System trajectories and states for a single switch attack on Line 26–28. (a) Phase portrait. (b) Generator 9 frequency. (c) Generator 9 angle. (d) Generator 9 terminal voltage. (e) Switch status.

E. Cascading Failure

Traditionally, cascading failure analysis focuses on steady state system characteristics about an initial equilibrium state using static power flow methods; dynamic analysis is considered in general to be difficult to model and complex to assess. In this section we aim to address cascading failures dynamically but in the context of our proposed multi-switch analysis framework. We consider how corruption of a subset of breakers within the New England 10-machine test system of Fig. 1 can be exploited to strain the system sufficiently to result in a sequence of trips and failures resulting in the loss of a substantial amount of load. We model the presence of protection as detailed in [17]–[19]. The overload protection on transmission lines is

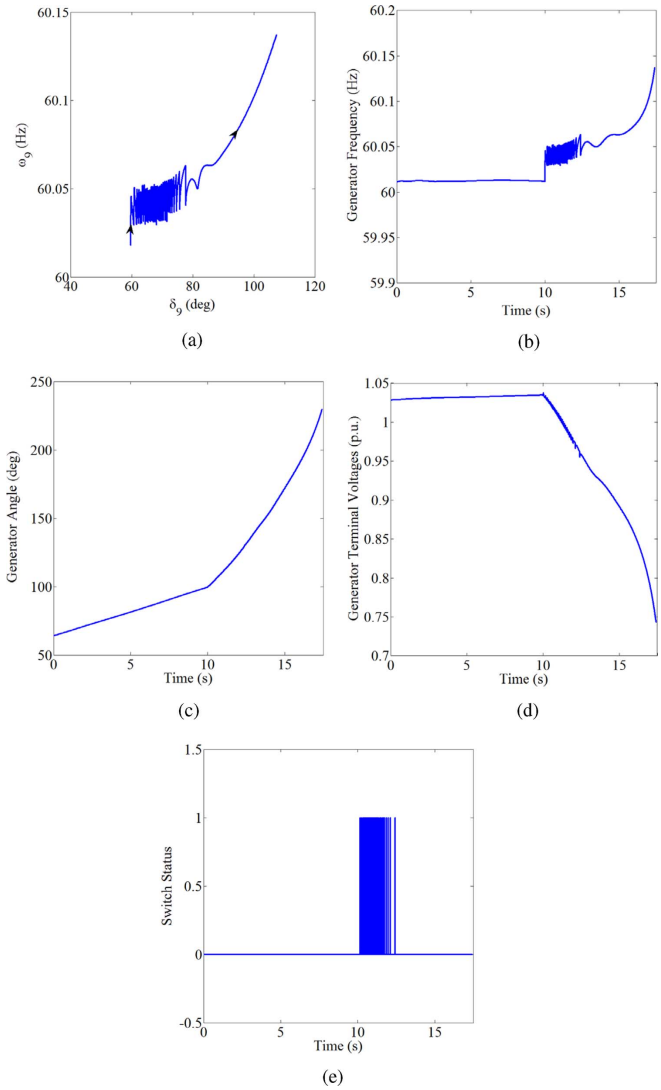


Fig. 10. System trajectories and states for a single switch attack on Line 28–29. (a) Phase portrait. (b) Generator 9 frequency. (c) Generator 9 angle. (d) Generator 9 terminal voltage. (e) Switch status.

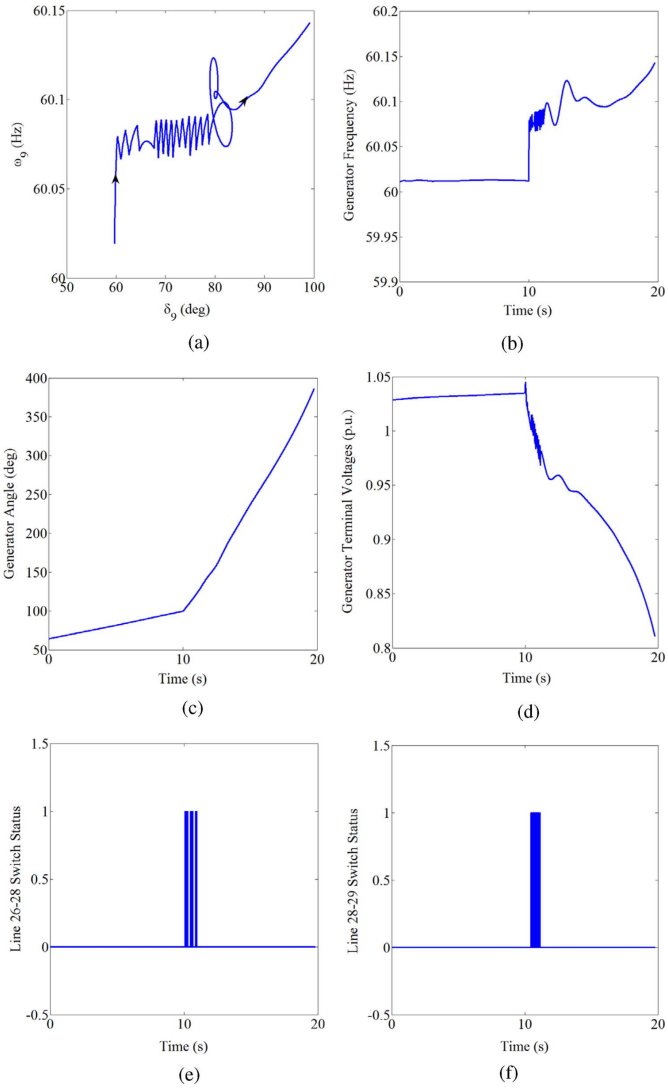


Fig. 11. System trajectories and states for a coordinated concurrent multi-switch attack. (a) Phase portrait. (b) Generator 9 frequency. (c) Generator 9 angle. (d) Generator 9 terminal voltage. (e) Switch 1 status (Line 26–28). (f) Switch 2 status (Line 28–29).

assumed to trigger when the active power over a line is more than 800 MW for 5 seconds.

We consider the corruption of Line 26–28 (Switch 1), Line 28–29 (Switch 2). In the first phase of the attack, an opponent targets Generator 9 employing $s_1 = -5\delta_9 + \omega_9$ and $s_2 = -8\delta_9 + \omega_9$. After Generator 9 is tripped by protection devices, a second phase is applied. Here, the opponent targets Generator 8 employing $s_1 = -2\delta_8 + \omega_8$ and $s_2 = -8\delta_8 + \omega_8$. The attack results in a series of critical component trips and a resulting domino effect presented in Table II and Fig. 13. Eventually, the entire system works under power provided by Generator 10 only, which is clearly sufficient to meet the normal demand requirements.

An opponent only needs to apply switching from 10 s to 11 s and 20 s to 21 s to have devastating effects within 100 s even with the use of protection. This impact is significant in contrast to use of a single switch and demonstrates the potential of coordinated variable structure switching attacks for large-scale system disruption.

F. Discussion

In our empirical results, we have presented switch statuses to demonstrate the switching action required by circuit breakers. Questions natural arise as to the feasibility of switching at the dense rates demonstrated in plots such as Figs. 12(e) and (f). Upon closer inspection, a zoomed-in plot of Figs. 12(e) and (f), shown in Figs. 14(a) and (b) respectively, demonstrate the connect and trip pulses required by a circuit breaker for the switching attack between time instants 10 s and 11 s. Tables III and IV detail the switch times numerically. As shown in the tables, the smallest interval for a breaker to connect after a trip is 16 ms. Moreover, the breaker must be capable of frequent on-and-off operation.

We provide a brief review of circuit breaker technology that has the potential to be applicable to the switching attacks detailed in this paper. Fast operation breakers, suitable for the frequent action, characteristic of our attack, include air blast circuit breakers [20] and SF_6 breakers [21] for high voltage (e.g., 345 kV) systems such as the 39-bus test system employed in the

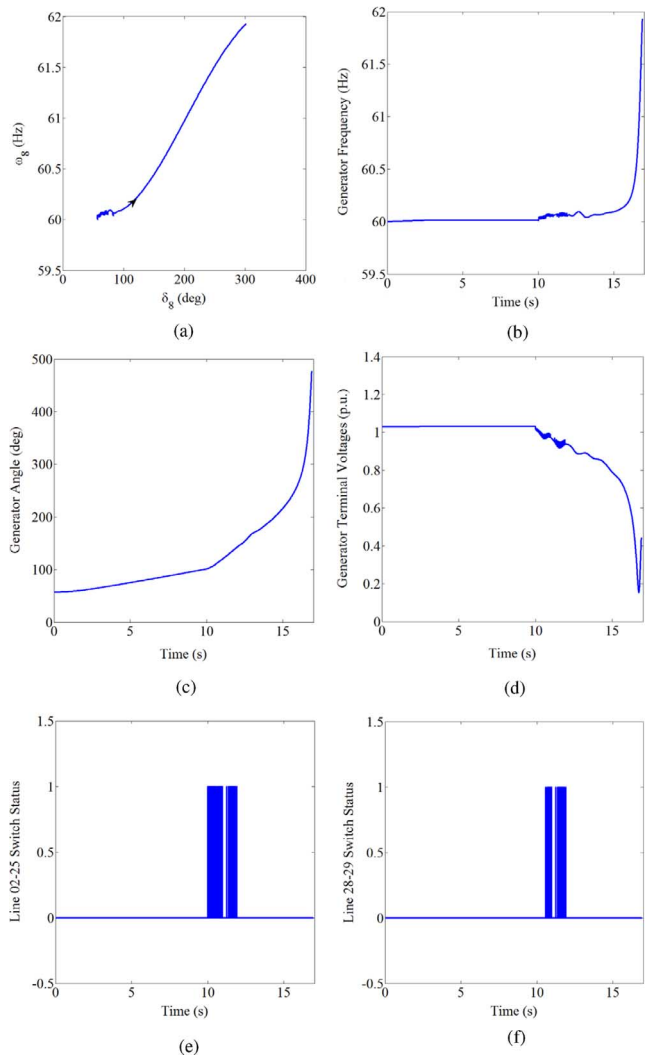


Fig. 12. System trajectories and states for a coordinated progressive multi-switch attack. (a) Phase portrait. (b) Generator frequency. (c) Generator angle. (d) Generator terminal voltage. (e) Switch status on Line 02–25. (f) Switch status on Line 28–29.

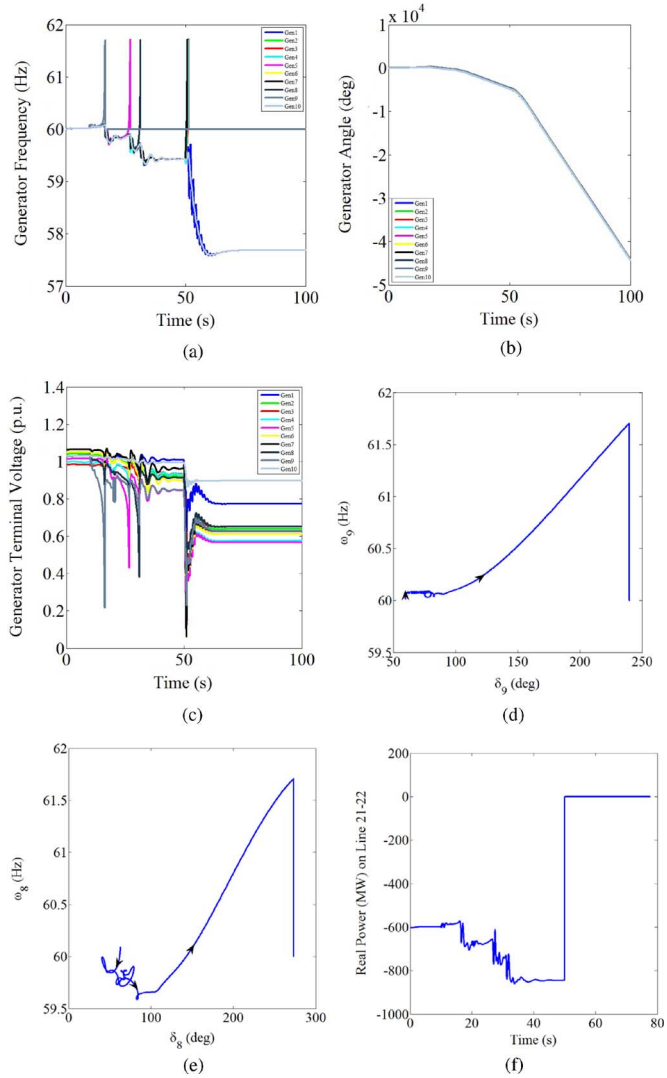


Fig. 13. System trajectories and states of cascading failure analysis. (a) Generator frequencies. (b) Generator angles. (c) Generator terminal voltages. (d) Phase portrait of Generator 9. (e) Phase portrait of Generator 8. (f) Real power (MW) on line 21–22 for overload protective relay.

paper. For both types of breakers, the air/gas is compressed to enable high velocity flow to dissipate arcing quickly as needed by our attack. Within arc interruption technology, the classic synchronous air blast circuit breaker proposed by FUJI Electric [22] can extinguish the arc in 1.2 ms, comparably faster than non-synchronous interruption; we expect that the duty cycles of current technology have become considerably faster than reported thus enabling switching attacks. The ultra-fast earthing switch (UFES) produced by ABB in 2011 is capable of extinguishing arc fault within 4 ms, compared to traditional protection which takes 140 ms [23], [24]. These specifications fulfill the 16 ms minimum timing requirement.

More recently, focus as been placed on the development of semiconductor-enabled solid-state breakers [25], in which there is no mechanical component, in order to perform higher frequency operation. Here, arc interruption is inherently integrated. We assert that such technology, currently under development, is very suitable for application of our switching attack. Thus, we conclude that there are strong indications within current breaker specifications and future goals that our proposed attack has strong practical application. One avenue of future work will be to investigate the feasibility of applying the attack to solid-state circuit breaker apparatuses.

V. Final Remarks and Future Work

In this environment of rushed development and rapid deployment, we contend that there is a timely and critical need for research that takes a systematic view of smart grid vulnerability analysis and protection in order to provide engineering principles of more general use. This paper presented a worst-case scenario for a multi-switch attack making use of variable structure system theory for power system disruption. We have demonstrated the utility of employing multiple switches for creating transient instability in target generators of a power grid.

Future work will focus on developing analytical bounds on the time to "catastrophe" in the presence of ideal and non-ideal inter-attacker communications. Based on these results we will aim develop adaptive distributed control strategies that

TABLE II
CASCADING FAILURE PROCESS OF NEW ENGLAND 10-MACHINE, 39-BUS POWER SYSTEM

Time (s)	Event Recording
0-10	Normal operating
10-11	Switching attacks implemented on Generator 9
11-16.38	Generator 9 loses synchronous, and is tripped by over-frequency relay at 16.38 second
16.38-20	System is operating at 59.8 HZ after tripping Generator 9
20-21	Switching attacks implemented on Generator 8
21-26.9	Generator 5 loses synchronous, and is tripped by over-frequency relay at 26.9 second
21-31.3	Generator 8 loses synchronous, and is tripped by over-frequency relay at 31.3 second
31.3-50	Line 21-22 active power increases, and is tripped by overload transmission line protection relay at 50 second
50-50.58	Generator 7 loses synchronous, and is tripped by over-frequency relay at 50.58 second
50.58-50.68	Generator 6 loses synchronous, and is tripped by over-frequency relay at 50.68 second
50.58-52.70	UFLS is activated, first load block is tripped (13%)
50.62-52.80	UFLS is activated, second load block is tripped (13%)
50.70-53.30	UFLS is activated, third load block is tripped (13%)
51-51.15	Generator 4 loses synchronous, and is tripped by over-frequency relay at 51.15 second
51.04-53.97	UFLS is activated, forth load block is tripped (13%)
51.12-54.82	UFLS is activated, fifth load block is tripped (13%)
51.26-51.27	Generator 2 loses synchronous, and is tripped by over-frequency relay at 51.27 second
51.27-51.30	Generator 3 loses synchronous, and is tripped by over-frequency relay at 51.30 second
54.82-100	Generator 1 and Generator 10 provide power to the remaining loads under fairly low frequency and voltage, which can not meet the normal power requirements.

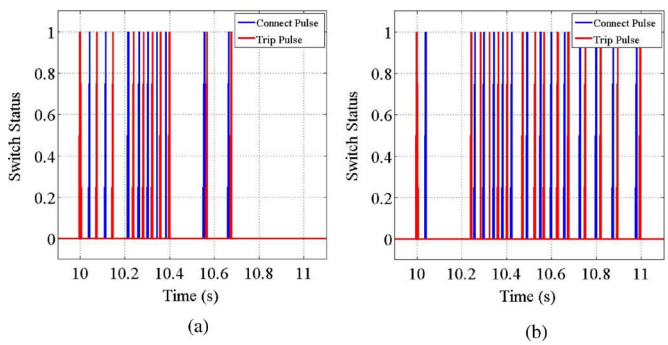


Fig. 14. Close-up of switch statuses for Fig. 12 example between time 10 s and 11 s. (a) Switch status on Line 02–25. (b) Switch status on Line 28–29.

TABLE III
TRIP TIME INTERVALS FOR EXAMPLE OF FIG. 14(A)

Trip Time (sec)	Connect Time (sec)	Duration (sec)
10.000	10.044	0.044
10.076	10.116	0.040
10.144	10.216	0.072
10.240	10.260	0.020
10.284	10.304	0.020
10.324	10.344	0.020
10.360	10.384	0.024

TABLE IV
TRIP TIME INTERVALS FOR EXAMPLE OF FIG. 14(B)

Trip Time (sec)	Connect Time (sec)	Duration (sec)
10.000	10.040	0.040
10.244	10.260	0.016
10.284	10.300	0.016
10.324	10.340	0.016
10.360	10.384	0.016
10.404	10.424	0.020
10.468	10.492	0.024
10.524	10.552	0.028
10.564	10.600	0.036
10.624	10.660	0.036
10.672	10.728	0.056
10.752	10.800	0.038

aim to minimize damage through effective system reconfiguration such as islanding. Moreover, we will aim to identify peer-to-peer-type strategies within groups of microgrid systems to rebalance and create resilience to switching attacks. Another avenue of future work will identify strategies to measure the effectiveness of a multi-switch attack to identify optimal values of the sliding mode coefficient matrix C.

ACKNOWLEDGMENT

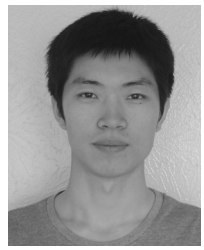
Funding for this work was provided through the U.S. National Science Foundation Project ECCS-1028246 and the Norman Hackerman Advanced Research Program Project 000512-0111-2009.

REFERENCES

[1] H. Tang and B. McMillin, "Security property violation in CPS through timing," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops*, 2008, pp. 519–524.
[2] B. McMillin, "Complexities of information security in cyber-physical power systems," in *Proc. IEEE Power Syst. Conf. Expo.*, Mar. 2009, pp. 1–2.
[3] C.-C. Liu, C.-W. Ten, and M. Govindarasu, "Cybersecurity of SCADA systems: Vulnerability assessment and mitigation," in *Proc. IEEE Power Syst. Conf. Expo.*, Mar. 2009, pp. 1–3.
[4] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.
[5] H. Lin, S. Sambamoorthy, S. Shukla, J. Thorp, and L. Mili, "Power system and communicaiton network co-simulation for smart grid applications," in *Proc. IEEE PES Conf. Innov. Smart Grid Technol. (ISGT)*, Anaheim, CA, USA, Jan. 2011, pp. 1–6.
[6] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. Butler-Purry, "Switched system models for coordinated cyber-physical attack construction and simulation," in *Proc. 1st IEEE Int. Workshop Smart Grid Model. Simul.*, Brussels, Belgium, Oct. 17, 2011, pp. 49–54.
[7] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. Butler-Purry, "A class of cyber-physical switching attacks for power system disruption," in *Proc. 7th ACM Annu. Cyber Security Inf. Intell. Res. Workshop*, Oak Ridge, TN, USA, Oct. 12–14, 2011.
[8] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A smart grid vulnerability analysis framework for coordinated variable structure switching attacks," in *2012 IEEE Power Energy Soc. Gen. Meet.*, San Diego, CA, USA, Jul. 22–26, 2012.

[9] S. Liu, D. Kundur, T. Zourntos, and K. Butler-Purry, "Coordinated variable structure switching in smart power systems: Attacks and mitigation," in *Proc. 1st Int. Conf. High Confidence Netw. Syst. Cyber Phys. Syst. Week*, Beijing, China, Apr. 17–18, 2012, pp. 21–30.
[10] S. Liu, D. Kundur, T. Zourntos, and K. Butler-Purry, "Coordinated variable structure switching attack in the presence of model error and state estimation," in *Proc. 3rd IEEE Int. Conf. Smart Grid Commun.*, Tainan City, Taiwan, Nov. 5–8, 2012.
[11] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans. Emerging Topics Comput.*, vol. 1, no. 2, pp. 273–285, 2013.
[12] D. Liberzon*, Switching in Systems and Control*. Boston, MA, USA: Birkhauser, 2003.
[13] V. Utkin*, Sliding Modes and Their Applications in Variable Structure Systems*. Moscow, USSR: MIR Publishers, 1978.
[14] R. DeCarlo, S. Zak, and G. Matthews, "Variable structure control of nonlinear multivariable systems: A tutorial," *Proc. IEEE*, vol. 76, no. 3, pp. 212–232, Mar. 1988.
[15] T. Flick and J. Morehouse*, Securing the Smart Grid: Next Generation Power Grid Security*. Burlington, MA, USA: Syngress, 2011.
[16] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Security*, Chicago, IL, USA, Nov. 2009, pp. 21–32.
[17] WECC, WECC "Off-nominal frequency load shedding plan," 2010.
[18] WECC, "Application of Zone 3 distance relays on transmission lines," 1997.
[19] WECC, "WECC coordinated off-nominal frequencyload shedding and restoration requirements," 1997.
[20] PKG Air-blast generator circuit breaker [Online]. Available: http://www.alstom.com/grid/products-and-services/high-voltage-power-products/circuit-breakers/PKG-Air-blast-generator-circuit-breaker/
[21] FKG SF6 generator circuit breaker [Online]. Available: http://www.alstom.com/grid/products-and-services/high-voltage-power-products/circuit-breakers/FKG-SF6-generator-circuit-breaker/
[22] N. Kiyokuni and M. Miyazima, "Synchronous air-blast circuit breaker for one cycle interruption delivered to Hokuriku Electrical Power Co., Inc. and Kyushu Electric Power Co., Inc.," Fuji Electric, Kawasaki, Tech. Rep. UDC 621.316.57.064.45, 1967.
[23] "ABB introduces record-breaking switchgear arc interrupter to China," [Online]. Available: http://www.abb.us/cawp/seitp202/f178fd61bb963bf5482578c30032c781.aspx
[24] "Ultra-fast earthing switch (UFES)—active internal arc protection for switchgear," [Online]. Available: http://www.abb.ca/product/db0003db004279/05d1e893194566e9c1257799003303d7.aspx
[25] C. Meyer and R. De Doncker, "Solid-state circuit breaker based on active thyristor topologies," *IEEE Trans. Power Electron.*, vol. 21, no. 2, pp. 450–458, Mar. 2006.

Shan Liu received the B.E. degree in electrical engineering from University of Science and Technology Beijing, China, in 2004, and the Ph.D. degree in electrical engineering from Texas A&M University, College Station, TX, USA, in 2013. She is an Assistant Professor at Communication University of China. She has worked as an intern at Siemens and engineer at Honeywell. Her research interests focus on the cyber security of the electric smart grid and cyber-physical system theory. She has received the ACM CSIIRW 11 best paper and multiple travel grant awards.



Bo Chen received the B.Sc. Eng. and M.Sc. Eng. degrees from North China Electric Power University, China, in 2008 and 2011, respectively, all in electrical engineering. He is currently pursuing the Ph.D. degree in the Department of Electrical and Computer Engineering at Texas A&M University, College Station, TX, USA. His research interests are optimization, power system stability analysis, and cyber security of smart grid.

Takis Zourntos received the B.A.Sc., M.A.Sc. and Ph.D. degrees in electrical engineering at the University of Toronto, Canada, in 1993, 1996, and 2003, respectively. He is a research faculty at Texas A&M University, College Station, TX, USA, and has over 15 years experience at the interface of microelectronics and control theory, which he currently applies to cyber-physical systems applications such as power systems and robotics. His recent cyber-physical systems robotics research has been featured in *Popular Science*'s 2009 Best of What's New: Security Innovation and wired.com.

Deepa Kundur received the B.A.Sc., M.A.Sc., and Ph.D. degrees all in electrical and computer engineering from the University of Toronto, ON, Canada in 1993, 1995, and 1999, respectively. From September 1999 to December 2002 she was an Assistant Professor in The Edward S. Rogers Sr. Department of Electrical & Computer Engineering at the University of Toronto and returned in September 2012 to hold the title of Professor. From January 2003 to December 2012 she was a Faculty Member in Electrical & Computer Engineering at Texas A&M University, College Station, TX, USA. Dr. Kundur's research interests include cybersecurity of the electric smart grid, cyber-physical system theory, security and privacy of social and sensor networks, multimedia security, and computer forensics. She has been an appointed member of the NERC Smart Grid Task Force and the Technical Program Co-Chair for the 2012 IEEE International Workshop on Information Forensics and Security. She has been on several editorial boards and is the recipient of numerous teaching awards at both the University of Toronto and Texas A&M University. Her research has received best paper recognitions at the 2008 IEEE INFOCOM Workshop on Mission Critical Networks, the 2011 Cyber Security and Information Intelligence Research Workshop, the 2012 IEEE Canadian Conference on Electrical and Computer Engineering, and the 2013 IEEE Power & Energy Society General Meeting.

Karen Butler-Purry received her B.S. (*summa cum laude*) in electrical engineering from Southern University, Baton Rouge, LA, USA, in 1985, the M.S. degree from the University of Texas at Austin, TX, USA, in 1987, and her Ph.D. in electrical engineering from Howard University, Washington, DC, USA, in 1994. She is a Professor in Electrical & Computer Engineering and Associate Provost for Graduate and Professional Studies at Texas A&M University, College Station, TX, USA. Her research interests are in the areas of computer and intelligent systems application to power distribution systems, distribution automation and management, fault diagnosis, estimation of remaining life of transformers, intelligent reconfiguration, and modeling and simulation for hybrid vehicles.