Received 24 March 2013; revised 8 August 2013 and 14 November 2013; accepted 21 November 2013.
Date of publication 2 January 2014; date of current version 21 January 2014.

Digital Object Identifier 10.1109/TETC.2013.2296440

A Framework for Modeling Cyber-Physical Switching Attacks in Smart Grid

SHAN LIU[1], SALMAN MASHAYEKH[2], DEEPA KUNDUR[3], TAKIS ZOURNTOS[2], AND KAREN BUTLER-PURRY[2]

[1]Department of Network Engineering, Communication University of China, Beijing 100024, China
[2]Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843 USA
[3]Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON L5L 1C6, Canada

CORRESPONDING AUTHOR: S. LIU (liushan2009@gmail.com)

This work was supported by the National Science Foundation under NSF Grant EECS-1028246 and the Norman Hackerman Advanced Research Program under Project 000512-0111-2009.

ABSTRACT Security issues in cyber-physical systems are of paramount importance due to the often safety-critical nature of its associated applications. A first step in understanding how to protect such systems requires an understanding of emergent weaknesses, in part, due to the cyber-physical coupling. In this paper, we present a framework that models a class of cyber-physical switching vulnerabilities in smart grid systems. Variable structure system theory is employed to effectively characterize the cyber-physical interaction of the smart grid and demonstrate how existence of the switching vulnerability is dependent on the local structure of the power grid. We identify and demonstrate how through successful cyber intrusion and local knowledge of the grid an opponent can compute and apply a coordinated switching sequence to a circuit breaker to disrupt operation within a short interval of time. We illustrate the utility of the attack approach empirically on the Western Electricity Coordinating Council three-machine, nine-bus system under both model error and partial state information.

INDEX TERMS Cyber-physical systems, security modeling, variable structure systems, coordinated switching attacks.

I. INTRODUCTION

We are witnessing the rapid technological evolution of numerous application fields including power systems, robotics and social networking. These systems will evolve into next-generation *cyber-physical systems* providing a spectrum of advantages over their predecessors. However, cyber-enablement of these systems naturally leads to issues of security requiring approaches to resilient system design. Tools for modeling cyber-physical systems are of paramount importance in enabling the judicious planning and vulnerability analysis.

A vulnerability in a system exists when there is a *weakness* in the system, *access* to the weakness and a *capability* by an opponent to exploit the weakness. We investigate a novel theoretical modeling framework based on variable structure system theory that enables the identification of a class of reconfiguration-based *weaknesses* in the power grid employing formal mathematical principles. Such an approach provides a prescriptive strategy to identify possible ways to trigger rotor angle instability in synchronous generators of power systems. Moreover, our model allows us to deduce steps for practical attack construction that are amenable to simulation demonstrating the potential *capability* of an opponent to exploit the flaw.

We assume that *access* to the flaw is facilitated through smart grid communication channels providing opponent(s) opportunities for remotely controlling physical power system components such as modern circuit breakers possibly via illicit security breaches and intrusion. Thus, our vulnerability is applicable to a smart grid system with remotely connected circuit breakers and one or more synchronous generators used as targets making it relevant to a broad class of modern and future power transmission systems.

We name the class of attacks that stems from our framework *coordinated variable structure switching attacks* whereby an opponent aims to destabilize the power grid by

leveraging corrupted communication channels and/or control signaling to hijack relevant circuit breakers. Our work represents a novel departure from existing smart grid vulnerability analysis research in that it represents the first use of variable structure system theory for attack performance analysis. This enables a prescriptive approach to vulnerability identification in contrast to methods that make use of reverse-engineering or ad hoc "what-if" analysis [1]–[12] leading to the identification of a new class of *reconfiguration-based* vulnerabilities. Moreover, we extend our recent work [13]–[15] by enhancing the theoretical foundation to better characterize the impact of attacks and perform necessarily robustness analysis of the attack construction under practical constraints of model error and partial information.

In the next section we focus on our attack development. Attack existence and characterization are presented in Section III. Attack construction and impact are studied in Sections IV and V. We then address issues involving limitations on attacker capability in Section VI followed by final remarks in Section VIII.

II. COORDINATED SWITCHING ATTACKS

A. SLIDING MODE IN VARIABLE STRUCTURE SYSTEMS

Variable structure systems are nonlinear systems characterized by discontinuous dynamics [16]. Such systems are considered to exhibit both continuous and discrete forms of behavior much needed for the modeling cyber-physical systems while being conducive to software implementation. Consider the following elementary variable structure system described as:

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

where $x \in \mathbb{R}^{n\times 1}$ is the system state vector, $f_i(x,t) \in \mathbb{R}^{n\times 1}$ represents *subsystem* dynamics for $i = 1, 2$, $s(x) \in \mathbb{R}$ is a state-dependent switching signal (sometimes denoted simply as s), and $s(x) = 0$ is called the n-dimensional *switching surface*. The state is a time-dependent quantity and therefore could also be denoted $x(t)$. The evolution of x in time through *state space* is called the *state trajectory* of the system.

Eq. (1) represents a system which abruptly switches dynamics between $f_1(x,t)$ and $f_2(x,t)$ according to the sign of $s(x)$ and is effective in modeling the action of a circuit breaker in power systems. A block diagram linking a simple power system to Eq. (1) is provided in Fig. 1 to elucidate; here, the state vector x represents the physical quantities of generator phase angle and frequency. When the power system switch changes positions between loads Z_1 (Position 1) and Z_2 (Position 2) it has the effect of changing between system dynamics denoted $f_1(x,t)$ and $f_2(x,t)$, respectively.

Analysis of the system in Eq. (1) leads to a number of interesting properties one of which is termed *sliding mode* behavior [16], [17]. In the sliding mode, the state trajectory of the system of (1) is attracted and subsequently confined to the switching surface $s(x) = 0$, which in this case is also termed the *sliding surface*.

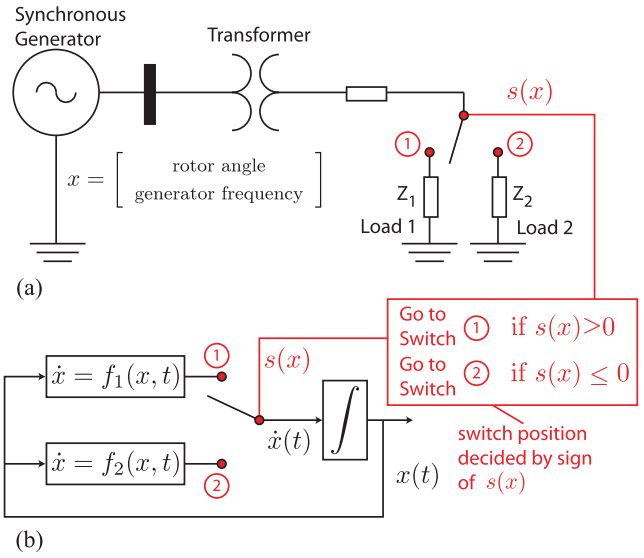

FIGURE 1. Elementary variable structure system example. (a) Elementary power system. (b) Block diagram.

There are two crucial aspects to this phenomenon. The first necessary condition is that the switching surface is attractive meaning that within some subset of state space, trajectories converge to the switching surface making it a sliding surface. The second requirement is that the variable structure system behavior, confined to the sliding surface, exhibits certain desired properties such as asymptotic stability, exponential growth or oscillation. We assert that this collective behavior can be used to steer the state into a position of instability for attack.

Consider a specific case of Eq. (1) assuming linear dynamics, $n = 2$ and $x = [x_1, x_2]^T$:

$$\dot{x} = \begin{cases} A_1 x, & s(x) > 0, \text{ where } A_1 = \begin{bmatrix} -1 & -10 \\ 3 & -0.3 \end{bmatrix} \\ A_2 x, & s(x) \leq 0, \text{ where } A_2 = \begin{bmatrix} -0.3 & 3 \\ -10 & -1 \end{bmatrix} \end{cases} \tag{2}$$

for some $s(x)$. The state trajectory $x(t)$, as governed by its dynamics, can be viewed geometrically in a *phase portrait*. The phase portraits of the individual subsystems A_1 and A_2 (i.e., assuming static switch positions of 1 and 2, respectively) are shown in both Fig. 2(a) and (b) as dashed and dash-dot lines, respectively. As can be observed, both subsystem trajectories converge to the stable equilibrium point $(0, 0)$ from the initial condition $(25, -25)$. Moreover, it can be shown that because the subsystems are linear they are each *globally asymptotically stable* meaning that the trajectories will always converge to $(0, 0)$ from any initial condition in $\mathbb{R}^2$ [18]. Thus, in this example, we can deduce that the system of Eq. (2) is stable when the switch is static in either position. This is analogous to a well-designed power system which will be stable for either an open or closed static breaker condition.

Variable structure system theory can be used to design a switching signal $s(x)$ to achieve certain desired system behaviors in Eq. (1). Traditionally, $s(x)$ has been designed

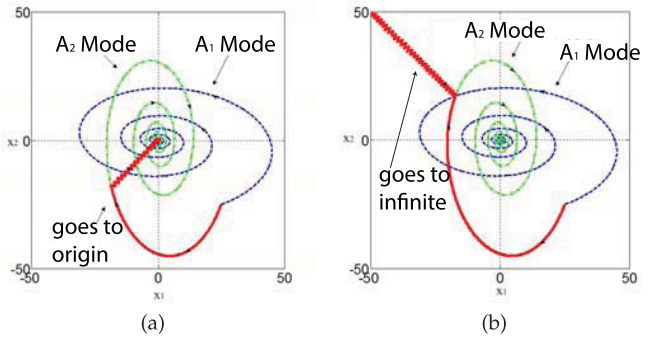

FIGURE 2. Sliding mode system trajectories of Eq. 2 in the presence of variable structure switching. (a) For $s(x) = -x_1 + x_2$. (b) For $s(x) = x_1 + x_2$.

to stabilize the variable structure system [16]. In this paper, we deviate from this philosophy and study how $s(x)$ may be selected by an attacker to steer the trajectory of Eq. (1) to instability thus enabling large-scale disruption in the associated power system. In Fig. 1(a) this would equate to destabilizing the generator angle and frequency resulting in *transient instability* of the smart grid system.

Consider the linear subsystem example of Eq. 2. We consider the following two selections for the switching signal $s(x)$, $s(x) = -x_1 + x_2$ and $s(x) = x_1 + x_2$, with associated phase portraits shown in Fig. 2(a) and (b), respectively. As is evident both selections instigate sliding mode behavior as convergence to the $s(x) = 0$ line is clearly observed. The former however results in stable sliding mode behavior while the latter results in instability. Making a simple analogy to smart grid systems, we thus purport that it may be possible for an opponent who can control the state of a circuit breaker to determine an $s(x)$, and hence a switching sequence, that can destabilize the overall switched power system even though it is designed to exhibit stable behavior when the breaker is static.

B. ATTACK ASSUMPTIONS AND OVERVIEW

To leverage variable structure system theory for cyber-physical attack development in a smart grid, an opponent would therefore need:

(A) to first identify a (physical) target component to attack (i.e., destabilize);
(B) electromechanical switching control over a corrupted circuit breaker (or equivalent) in the target's proximity;
(C) a local model of the smart grid system in the vicinity of the target and breaker; and
(D) knowledge of the target's state x.

Knowledge of a local model of the smart grid is a common assumption made in other attack literature [19], [20]. Conditions (A) and (C) collectively enable the identification of a variable structure system model of the smart grid to design a switching signal $s(x)$, if one exists, that instigates unstable sliding mode behavior; this establishes the first stage of *attack construction*. Conditions (B) and (D) allow implementation of the attack in the second stage of *attack execution*. In Sec. VI we relax Conditions (C) and (D).

The reader should note that to achieve Conditions (B) and (D), an opponent would have to remotely access communication systems related to the breaker and the synchrophasor sensor of the target generator, respectively. In protected information systems, this would require that the attacker illicitly infiltrate the corresponding data transmission systems. For Condition (B), the opponent would have to inject fabricated breaker control signals into the communication network. For Condition (D), the opponent would have to infiltrate the associated SCADA or synchrophasor network to intercept generator state information.

Cyber intrusion or corruption of distributed systems is a necessary assumption for vulnerability analysis especially when studying system resilience. Numerous practical examples of cyber weaknesses in smart grid communication networks have been documented [21] that range from exploiting holes in well known operating systems used by measurement and control devices to distribution-area attacks such as the hijacking of smart meters that can enable the effective shutting on/off of loads to provide the type of switching attack presented in this paper. The types of cyber intrusions necessary to be able to execute a coordinated variable structure switching attack are specific to the actual protocols, software and hardware architecture and is beyond the scope of this work.

III. ATTACK EXISTENCE AND DYNAMICS

Assuming Conditions (A) to (D) of Section II-B hold, the existence of a coordinated variable-structure switching vulnerability for a given smart grid is directly related to the existence of a sliding mode for the associated breaker switched system. Sliding mode existence for the general class of systems in Eq. (1) is an open problem. Thus, in this section we provide existence conditions for *incrementally linear* subsystems to facilitate attack construction in Section IV. Moreover, we characterize the dynamics and stability properties of this class of systems during sliding mode behavior to better understand the impact of the attack. Our formulation conveniently represents the switching of a single corrupted circuit breaker or switch, but can be naturally scaled to multiple switches by increasing the number of subsystems.

The reasons for the incrementally linear assumption are three-fold. First, because many power system configurations can be approximated as linear about a local range of operating conditions, it allows for representation of a useful class; in Section V we demonstrate how one can successfully construct and execute attacks even on nonlinear power system models using this linearized model. Second, the linear approximation does not carry the same limitations for system destabilization as it would for stabilization. For stabilization, model linearization expands the region of convergence over the original nonlinear system making the system appear more stable than it really is. In contrast, we contend that such

approximations for destabilization provide conservative impacts often demonstrating richer disruptions in the actual nonlinear systems. Finally, demonstrating the construction of an attack using linearized models provides intuition as to the practical feasibility of identifying such attacks with only approximate information.

A. SLIDING MODE EXISTENCE

In general, the sliding mode existence condition is given by [16] (note: $\dot{s}(x)$ is the time derivative of $s(x)$):

$$s(x)\dot{s}(x) < 0 \qquad \text{for } s(x) \neq 0. \tag{3}$$

1) NONLINEAR SUBSYSTEMS

Typically, sliding mode existence is local for nonlinear time-varying dynamics. Determining analytic existence conditions, in the form of parameter ranges for a structure of nonlinear dynamics, is often intractable. However, a visual approach employing overlapping phase portraits of the subsystems can be used based on the following interpretation. Eq. (3) is equivalent to the following:

$$\lim_{s(x)\to 0^+} \dot{s}(x) < 0 \text{ and } \lim_{s(x)\to 0^-} \dot{s}(x) > 0. \tag{4}$$

The above equation implies that if we consider the state space to be partitioned into two regions corresponding to $s(x) > 0$ and $s(x) < 0$ then if the state is on, say, the $s(x) > 0$ ($s(x) < 0$) side, its trajectory will be attracted to the other side (and across $s(x) = 0$) due to the requirement on the rate of change of $s(x)$ that $\dot{s}(x) < 0$ ($\dot{s}(x) > 0$). The overall effect is an attraction to the $s(x) = 0$ surface whereby once the state crosses $s(x) = 0$ from one side to the other, it crosses right back. Visually in state-space, Eq. (3) can be evaluated by employing overlapping phase portraits of the subsystems and analyzing whether the state trajectories of the appropriate subsystems on either side of the surface push the state back to the sliding surface. Of course, the visual approach is limited to situations in which dimensionality is small.

2) (INCREMENTALLY) LINEAR SUBSYSTEMS

Analytically, we present the following theorem regarding the existence of a sliding mode for incrementally linear subsystem dynamics.

Theorem 1 (Existence of a Sliding Mode). *Given the variable structure system:*

$$\dot{x} = \begin{cases} A_1 x + b_1, & s(x) > 0 \\ A_2 x + b_2, & s(x) \leq 0 \end{cases} \tag{5}$$

where $x \in \mathbb{R}^{n\times 1}$, $A_i \in \mathbb{R}^{n\times n}$, $b_1 \in \mathbb{R}^{n\times 1}$ and $s(x) = Cx \in \mathbb{R}$ for constant row vector $C = [c_1\ c_2\ \cdots\ c_n] \in \mathbb{R}^{1\times n}$ the necessary and sufficient conditions for existence of the sliding mode are:

$$\begin{cases} C(A_1 x + b_1) < 0, & s(x) > 0 \\ C(A_2 x + b_2) > 0, & s(x) < 0 \end{cases}. \tag{6}$$

Proof: The overall system of Eq. (5) can be represented as (for simplicity we denote $s(x)$ as s):

$$\dot{x} = \left[\frac{1+\text{sgn}(s)}{2}\right](A_1 x + b_1) + \left[\frac{1-\text{sgn}(s)}{2}\right](A_2 x + b_2) \tag{7}$$

where $\text{sgn}(s) = 1$ for $s > 0$ and $\text{sgn}(s) = -1$ for $s \leq 0$. From Eq. (3) a sliding mode exists if and only if $s\dot{s} < 0$; we determine the conditions to guarantee this inequality where we make use that $s\ \text{sgn}(s) = |s|$:

$$\begin{aligned} s\dot{s} = sC\dot{x} &= sC\left\{\left[\frac{1+\text{sgn}(s)}{2}\right](A_1 x + b_1) \right. \\ &\qquad \left. + \left[\frac{1-\text{sgn}(s)}{2}\right](A_2 x + b_2)\right\} \\ &= \frac{1}{2}sC(A_1 + A_2)x + \frac{1}{2}|s|C(A_1 - A_2)x \\ &= \frac{1}{2}(s+|s|)C(A_1 x + b_1) + \frac{1}{2}(s-|s|)C(A_2 x + b_2) \end{aligned}$$

which is equivalent to (6) if we impose $s\dot{s} < 0$ and where we make use of the fact that $s + |s| > 0$ and $s - |s| = 0$ for $s > 0$, and $s + |s| = 0$ and $s - |s| < 0$ for $s < 0$. ■

Thus, Condition (6) is necessary and sufficient to guarantee that $s\dot{s} < 0$ and represents a convenient test for the existence of a sliding mode. An opponent would have to determine a vector $C = [c_1\ c_2\ \cdots\ c_n]$ (or an associated vector range) such that (6) holds for a region in state space.

The reader should note that (6) implies that the range of C for which the inequalities exist is in general dependent on the values of the state x. This implies that the attraction condition exists for a given neighborhood of x and hence is *local*. To employ this criterion, an opponent would consider the neighborhood about the current equilibrium point x^*, $x \in \mathcal{N}(x^*)$, and select a C such that $sC(A_1 x + b_1) < 0$ for $s > 0$ and $sC(A_2 x + b_2) > 0$ for $s < 0$ for $x \in \mathcal{N}(x^*)$.

We emphasize that the conditions above only guarantee *attraction to the $s = 0$ surface* and do not imply stability properties of the system. The next theorem characterizes the behavior of the state once attracted to the sliding surface thus providing insight on its stability properties.

B. SLIDING MODE DYNAMICS

A sliding mode provides a steering quality to an opponent to shift a grid to a more vulnerable state. If a sliding mode is unstable, the state will attract to $s = 0$ and then continue on the surface to infinity. In the stable case, it will eventually converge to an equilibrium point on the $s = 0$ surface. To characterize the sliding mode dynamics and stability properties, we present the following theorem.

Theorem 2 (Sliding Mode Dynamics). *For the variable structure system:*

$$\dot{x} = \begin{cases} A_1 x + b_1, & s(x) > 0 \\ A_2 x + b_2, & s(x) \leq 0 \end{cases}$$

where $x \in \mathbb{R}^{n\times 1}$, $A_i \in \mathbb{R}^{n\times n}$ and $b_i \in \mathbb{R}^{n\times 1}$, assume that a sliding mode for $s = Cx$, $C \in \mathbb{R}^{1\times n}$, exists. Then, the sliding mode dynamics can be characterized by $G(x)$ as follows:

$$\dot{x} = G(x) \tag{8}$$

where

$$G(x) = \frac{1}{2}\left[(A_1 + A_2)x + (b_1 + b_2)\right] - \frac{1}{2}[(A_1 - A_2)x + (b_1 - b_2)] \cdot \frac{C\left[(A_1 + A_2)x + (b_1 + b_2)\right]}{C\left[(A_1 - A_2)x + (b_1 - b_2)\right]}$$

Moreover, the local stability properties of the system about a neighborhood of the equilibrium point $x^* \in \mathbb{R}^{n\times 1}$ can be determined stable if all non-trivial eigenvalues of $G(x^*)$ are on the left half plane and unstable otherwise.

proof: We assign: $G_a(x) = \frac{1}{2}[(A_1 + A_2)x + (b_1 + b_2)]$ and $G_d(x) = \frac{1}{2}[(A_1 - A_2)x + (b_1 - b_2)]$. Then, the variable structure system can be represented in the form of a control system:

$$\begin{cases} \dot{x} = G_a(x) + G_d(x)u \\ s = Cx \\ u = \text{sgn}(s). \end{cases} \tag{9}$$

where $u \in \mathbb{R}$ is defined for a given $s = Cx$. Given sliding mode existence, we can characterize its traversal along $s(x) = 0$ using the method of equivalent control [17]. Here, we have:

$$\dot{s} = C\dot{x} = CG_a(x) + CG_d(x)u. \tag{10}$$

For the state confined on the sliding surface, $s = \dot{s} = 0$. We solve for the equivalent control u_{eq} by setting Eq. (10) to zero and solving for u. This gives $u_{eq} = -[CG_d(x)]^{-1}CG_a(x)$ where the reader should note that $CG_a(x), CG_d(x) \in \mathbb{R}$. The effective system dynamics on the sliding mode is therefore:

$$\begin{aligned} \dot{x} &= G_a(x) + G_d(x)u_{eq} \\ &= \frac{1}{2}\left[(A_1 + A_2)x + (b_1 + b_2)\right] \\ &\quad -\frac{1}{2}[(A_1 - A_2)x + (b_1 - b_2)] \\ &\quad \cdot\frac{C\left[(A_1 + A_2)x + (b_1 + b_2)\right]}{C\left[(A_1 - A_2)x + (b_1 - b_2)\right]} \\ &= G(x). \end{aligned}$$

The local stability properties easily follow by applying linearization and Theorems 15 and 27 of [18]. □

Eqs. 8 and 9 of Theorem III-B describe the sliding mode dynamics as a combination of the *average* (i.e., $\frac{1}{2}\left[(A_1 + A_2)x + (b_1 + b_2)\right]$) and *difference* (i.e, $\frac{1}{2}\left[(A_1 - A_2)x + (b_1 - b_2)\right]$) of the individual subsystem dynamics. The state- and sliding surface-dependent weight $\frac{C[(A_1+A_2)x+(b_1+b_2)]}{C[(A_1-A_2)x+(b_1-b_2)]} \in \mathbb{R}$ scales the difference dynamics relative to the average dynamics to maintain the system on the sliding surface. Selection of C and hence the particular sliding mode to use for switching will have an effect on the behavior of the state. If C is more aligned (via the dot product measure) to the average dynamics, then the difference dynamics have greater influence than the average and vice versa.

For an attack, an opponent is concerned with power flow disruption and may be most interested in the stability properties of the sliding mode. Thus, unstable sliding modes can be leveraged through persistent switching until significant disruption results. Although perhaps not immediately obvious, stable sliding modes can also be leveraged as we demonstrate in Section V to steer the system across the stability boundary of one of the subsystems and then terminate switching to enable passive disruption.

IV. ATTACK CONSTRUCTION

Employing our framework, we provide the steps necessary for attack construction and apply it to a case study involving the Western Electricity Coordinating Council (WECC) 3-machine system, 9-bus system. The reader should note that, from our experience, existence of a sliding mode and hence ability to construct the attack for a target generator in the proximity of a corrupted breaker is typically high for most test systems considered.

A. STAGES OF ATTACK CONSTRUCTION

The stages of an attack construction are as follows.

1) Mathematically represent the system under the switching attack as a variable structure system whereby the switching rule $s(x)$ remains general.
2) For general nonlinear systems, identify the equilibrium points and linearize the system about the equilibrium points.
3) Determine the existence of and identify a class of sliding modes using Theorem III-A.2.
4) Characterize the dynamical and stability properties of the sliding modes using Theorem III-B.
5) Select and assign an identified sliding surface to $s(x)$ for attack implementation.

We contend that the steps above apply to general nonlinear models of power system dynamics; the linearization stage is critical to make use of Theorems III-A.2 and III-B. However, for general nonlinear systems, pictorial approaches for identification of sliding modes are also possible as mentioned in Section III-A. A phase portrait of each nonlinear subsystem must be determined identifying stable foci and saddle points. These phase portraits must then be overlapped. A sliding surface $s(x) = 0$ may be identified visually if in the vicinity of $s(x) = 0$, the trajectory vectors of the subsystems point toward the switching surface in opposite directions; this ensures that the state trajectory of the switched system will be driven to the switching surface and will stay within a neighborhood of it. The interested reader is referred to [17]. We employ the visual approach to sliding mode identification as a brief check to verify our linearized model results, but would not typically be used by an opponent for attack construction.

A natural approach to attacking a power grid would be to exploit the unstable sliding mode of a system whereby the state is steered to an arbitrarily large value. However, the reader should note that it is possible to exploit both unstable and stable sliding modes for effective power system disruption.

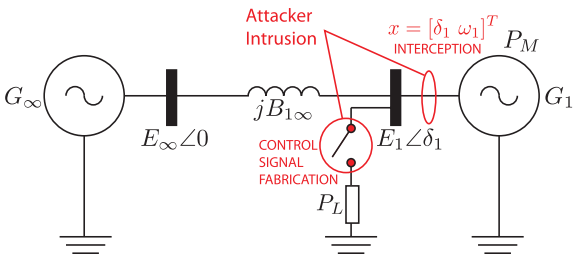

FIGURE 3. Single machine infinite bus system model. The opponent coordinates switching of the load P_L based on the values of Generator G_1's state $x = [\delta_1 \omega_1]^T$.

To illustrate the use of our variable structure theory approach, we demonstrate the construction of an attack for the well known single machine infinite bus (SMIB) power system model presented in Fig. 3.

B. VARIABLE STRUCTURE REPRESENTATION

A typical power system is piecewise time-invariant; that is, within a short window of time representing the attack duration before disruption, the system parameters can be considered to be constant. Thus, for the purposes of our modeling for attack construction, we make use of time-invariant parameters in a swing equation-based model of the power system. Thus, the SMIB model can be expressed as [22]:

$$\begin{cases} \dot{\delta}_1 = \omega_1 \\ M_1\dot{\omega}_1 = P_{M1} - E_1^2 G_{11} \\ \qquad\quad - s_L P_L - E_1 E_\infty B_{1\infty}\sin\delta_1 - D_1\omega_1 \\ \qquad = P_1 - C_{1\infty}\sin\delta_1 - D_1\omega_1 \end{cases} \tag{11}$$

where δ_1 and ω_1 are the rotor angle and rotor speed deviation of Generator G_1, respectively, and collectively form the state $x = [\delta_1\ \omega_1]^T$, M_1, D_1, E_1, P_{M1} are the moment of inertia, damping coefficient, internal voltage and mechanical power of G_1, respectively, E_∞ is the voltage at the infinite bus, P_L is the local load at Bus 1, s_L is the load switch status ($s_L = 1$, if the load is connected; $s_L = 0$, otherwise), and $B_{1\infty}$ is the transfer susceptance of the line between Bus 1 and the infinite bus. We assign $P_1 = P_{M1} - E_1^2 G_{11} - s_L P_L$ and $C_{1\infty} = E_1 E_\infty B_{1\infty}$.

Assuming that $C_{1\infty} = 1, D_1 = 0.1, M_1 = 0.1, P_{M1} - E_1^2 G_{11} - P_L = 0, P_{M1} - E_1^2 G_{11} = 0.9$, the overall variable structure system can be represented as:

$$A_1 : \begin{cases} \dot{\delta}_1 = \omega_1 \\ \dot{\omega}_1 = -10\sin\delta_1 - \omega_1 \end{cases} \quad \text{if } s_L = 1$$
$$A_2 : \begin{cases} \dot{\delta}_1 = \omega_1 \\ \dot{\omega}_1 = 9 - 10\sin\delta_1 - \omega_1 \end{cases} \quad \text{if } s_L = 0 \tag{12}$$

It is straightforward to determine from Eq. (12) that system A_1's stable foci are at $(2n\pi, 0)$ and the saddle points are at $(2n\pi + \pi, 0)$ where $n \in \mathbb{Z}$ as shown in the phase portrait of Fig. 4(a). Any point within a stability boundary will converge to the corresponding stable focus. Similarly, for system A_2, the stable foci are at $(2n\pi + 1.1198, 0)$ and $(2n\pi + 2.0218, 0)$, and the saddle points are at $(2n\pi + 2.0218, 0)$ as shown in the phase portrait of Fig. 4(b).

As discussed in Section IV-A, for a general nonlinear system the existence of a sliding mode can be determined pictorially from the overlapping phase portraits. Here, one interprets Eq. (3) visually in state space whereby a sliding surface $s(x) = 0$ must be found such that in the neighborhood of this surface the trajectory vectors of each subsystem point toward the switching surface but in opposite directions. The switching between subsystems would be assigned such that when on one side of the sliding surface $s(x) = 0$, the system would switch to the subsystem with trajectories pointing toward that surface. This ensures that the state trajectory of the variable structure system will be driven to the switching surface and will stay within a region of it [17].

To determine the possibility of a sliding mode in this way, the overlapping phase portraits are shown in Fig. 4(c). Visual inspection suggests there are multiple possibilities for linear sliding surfaces such as $s = 6\delta_1 + \omega_1$. However, in the next section we demonstrate the utilization of Theorems III-A.2 and III-B on the linearized system to determine the range of possible sliding surfaces for attack. In this way, we demon-

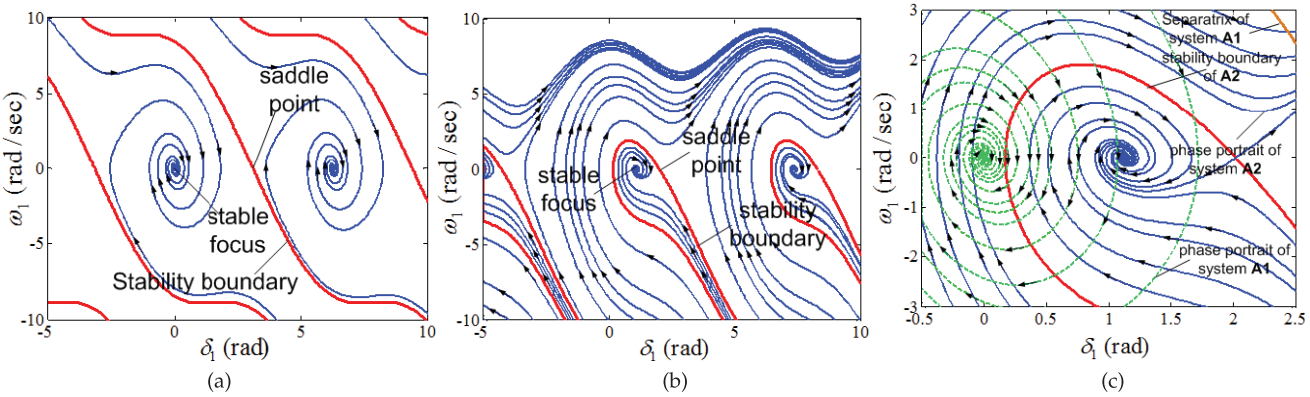

FIGURE 4. Individual and overlapping phase portraits of subsystems of Eq. (12). (a) Phase portrait of system A_1. (b) Phase portrait of system A_2. (c) Close-up of overlapping phase portraits.

strate the mathematical and numerical ease in determining such a vulnerability.

C. SMIB ATTACK CONSTRUCTION

To apply Theorems III-A.2 and III-B to our SMIB power system model of Eq. (12), we must linearize its representation. Approximating $\sin\delta_1 \approx \delta_1$ for δ_1 small and assuming $s > 0$ ($s \leq 0$) corresponds to the load switch being closed to give A_1 (open to give A_2), we obtain:

$$\begin{aligned} \dot{\delta}_1 &= \omega_1 \\ \dot{\omega}_1 &= \begin{cases} -10\delta_1 - \omega_1, & s > 0 \\ 9 - 10\delta_1 - \omega_1, & s \leq 0 \end{cases} \end{aligned} \tag{13}$$

corresponding to $A_1 = A_2 = \begin{bmatrix} 0 & 1 \\ -10 & -1 \end{bmatrix}$, $b_1 = \begin{bmatrix} 0 & 0 \end{bmatrix}^T$ and $b_2 = \begin{bmatrix} 0 & 9 \end{bmatrix}^T$ in (5). Theorem III-A.2 provides the following sliding mode existence conditions for $s = c_1\delta_1 + c_2\omega_1$:

$$\begin{cases} c_1\omega_1 - 10c_2\delta_1 - c_2\omega_1 < 0 & \text{for } c_1\delta_1 + c_2\omega_1 > 0 \\ c_1\omega_1 - 10c_2\delta_1 - c_2\omega_1 + 9c_2 > 0 & \text{for } c_1\delta_1 + c_2\omega_1 < 0 \end{cases}. \tag{14}$$

Fig. 5 illustrates this overall region; the regions delineated $s < 0$ and $s > 0$ denote the values of (c_1, c_2) for which $c_1\omega_1 - 10c_2\delta_1 - c_2\omega_1 < 0$ and $c_1\omega_1 - 10c_2\delta_1 - c_2\omega_1 + 9c_2 > 0$ about $x^* = [1.1198 \;\; 0]^T$, respectively. We can construct an attack by selecting $C = [6\ 1]$ corresponding to $s = 6\delta_1 + \omega_1$. Applying Theorem III-B, we find that it is a stable sliding mode.

V. ATTACK EXECUTION AND IMPACT

In this section we execute a coordinated variable structure switching attack using our sliding mode selection of $s = 6\delta_1 + \omega_1$ on the nonlinear SMIB and a more realistic test system to demonstrate the value of Theorems III-A.2 and III-B for attack construction on linearized models. Our target in both cases is Generator G_1 and the corrupted breaker is that associated with load switching.

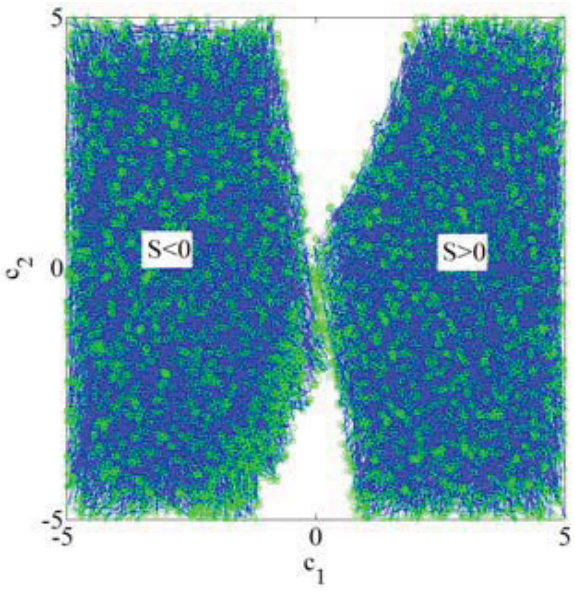

FIGURE 5. Valid sliding mode parameter region about neighborhood of $x^* = [1.1198 \;\; 0]^T$.

A. NONLINEAR SMIB CASE STUDY

Consider application of a switching attack on the *nonlinear* SMIB model of Eq. (12). We assume that the load is initially disconnected (i.e., is at A_2) and apply the attack from 0 to 2.5 seconds, which drives the system trajectory across the stability boundary of subsystem A_2 at which time the attack finally switches the system dynamics to A_2 permanently as observed in Fig. 6(a). Thus, G_1 is destabilized within seconds by steering its state over the stability boundary via the switching attack. The reader should note that as discussed $s = 6\delta_1 + \omega_1$ is a stable sliding mode. Thus, persistent switching (opposed to that limited to 2.5 s) will result in steering the power system from the initial stable focus of (1.1198, 0) to the stable focus of (0, 0) as presented in Fig. 6(b).

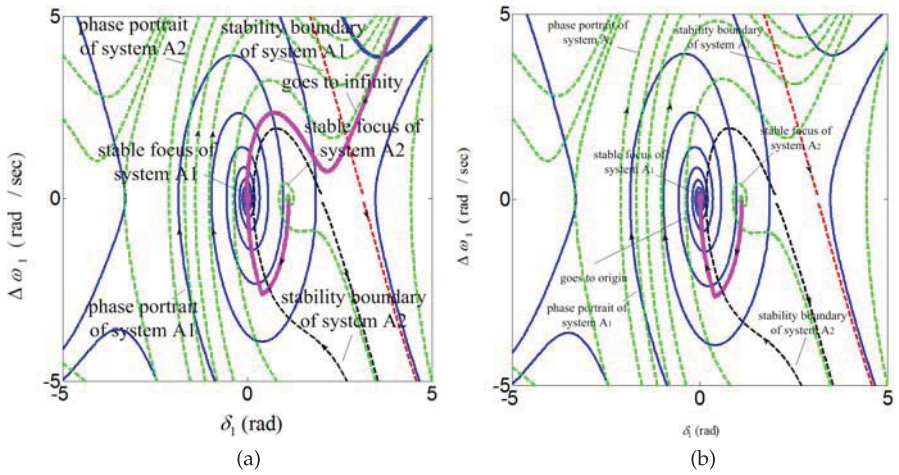

FIGURE 6. Switching attack on System (12) for $s = 6\delta_1 + \omega_1$. (a) Stop time of 2.5 seconds. (b) No stop time.

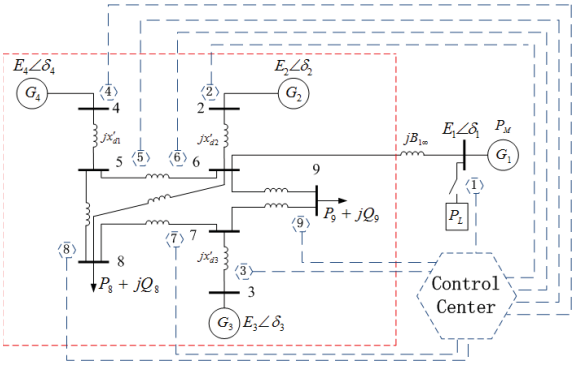

FIGURE 7. One-line diagram of revised WECC system.

B. WECC 3-GENERATOR, 9-BUS CASE STUDY

To further demonstrate the utility of the attack, we consider a variant of the well-known Western Electricity Coordinating Council (WECC) 3-machine, 9-bus system [23] presented in Fig. 7. This system can be approximated with the second order nonlinear SMIB model of Eq. (12). Thus, we apply the same sliding surface $s = 6\delta_1 + \omega_1$ for attack.

The test system in question is simulated in PSCAD (Power System Computer Aided Design, https://hvdc.ca/pscad/) software, one of the most popular power system simulation tools. PSCAD enables the modeling of generator controls including governors and exciters as well as protective relays to demonstrate the potential of our approach to disrupt real power system operation. The test system is based on the WECC system, with the addition of a transmission line, a local load, and a gas turbine generator. Here, the base MVA is 100, the system normal frequency is 60 Hz and the generator parameters are shown in Table 1. The transmission line connecting Generator G_1 and the infinite bus are modeled using an inductor of 0.014 H. The local load P_L is chosen to be 32.4 MW modeled using a constant resistor. The PSCAD step size was chosen to be 50 μs.

For consistent comparison, simulations of the WECC system are presented for the same system initial conditions and stop time as employed for the second order nonlinear SMIB model of the previous section. Specifically, the initial state of the WECC system is set to to the stable focus of (1.1198, 0). If $s > 0$, the system dynamics switch to system A_1 and if $s \leq 0$, they switch to A_2. The switching attack is applied from 0.2248 to 2.7248 seconds (the non-zero start time is necessary for PSCAD implementation of the attacked system), which once again drives the system trajectory across the stability boundary of A_2 at which point the switch is permanently set to A_2 making the system unstable. The frequency relays of all generators including G_1 are set to trip for a deviation more than $\pm 5\%$ of the nominal frequency (of $2\pi \times 60 = 377$ rad/s), which corresponds to 18.8 rad/sec; in this way we also take into account the response of the non-corrupted breakers to the switching attack. PSCAD simulations demonstrate in Fig. 8(a) how at time 2.7248 seconds (which corresponds to 2.5 seconds in the SMIB simulation due to the delayed start time), the system state diverges. The deviation from nominal frequency, phase angle and output voltage of Generator G_1 during the attack is shown in Fig. 8(b)–(d), respectively. As observed, the frequency and voltage of G_1 become unstable right after application of the attack.

To illustrate how the sliding mode exploited for the attack is in fact stable, the same coordinated switching is applied indefinitely with results presented in Fig. 9.

TABLE 1. Generator parameters for Fig. 7 system.

Name	Parameter	Gen 1	Gen 2
Rated RMS Line-Line Volatge	V_{gl-l}	13.8 kV	16.5 kV
Active Power	P_g	36 MW	100 MW
Power Factor	p_{fg}	0.8	0.8
Frequency	f	60 Hz	60 Hz
Direct axis unsaturated reactance	Xd	1.55	0.146
D axis unsaturated transient reactance	Xd′	0.22	0.0608
D axis open circuit unsaturated transient time constant	Tdo′	8.95 sec	8.96
Q axis unsaturated reactance	Xq	0.76	0.0969
Q axis unsaturated transient reactance	Xq′	N.A	0.0969
Q axis open circuit unsaturated transient time constant	Tqo′	N.A	0.31
Inertia Constant	H	0.5 sec	23.64
Name	Parameter	Gen 3	Gen 4
Rated RMS Line-Line Volatge	V_{gl-l}	18.0 kV	13.8 kV
Active Power	P_g	163 MW	85MW
Power Factor	p_{fg}	0.8	0.8
Frequency	f	60 Hz	60 Hz
Direct axis unsaturated reactance	Xd	0.8958	1.3125
D axis unsaturated transient reactance	Xd′	0.1198	0.1813
D axis open circuit unsaturated transient time constant	Tdo′	6.0	5.89
Q axis unsaturated reactance	Xq	0.8645	1.2578
Q axis unsaturated transient reactance	Xq′	0.1969	0.25
Q axis open circuit unsaturated transient time constant	Tqo′	0.539	0.6
Inertia Constant	H	6.4	3.01

C. EFFICACY OF LINEARIZED RESULTS

We assert that the attack theory and analysis presented in this paper has the potential to be employed, in part, as a tool to understand possibility vulnerabilities in future smart grid systems as well as the worst-case impact of switching attacks. One measure of the degree of weakness exhibited by a system could relate to the range of possible sliding modes available for an opponent to exploit.

For this reason, Theorem III-A.2 can be a useful tool when applied to a linearized smart grid system. To demonstrate the

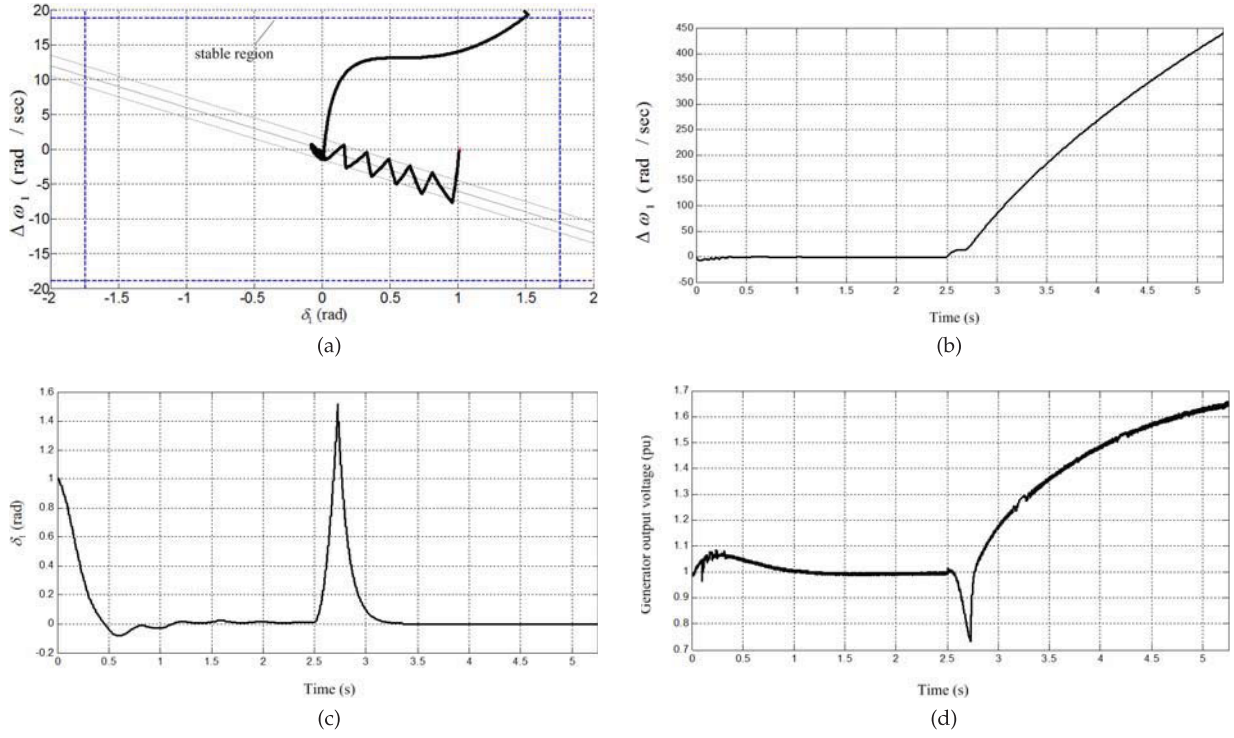

FIGURE 8. PSCAD simulation results of WECC system for $s = 6\delta_1 + \omega_1$ switching from 0 to 2.5 seconds. (a) System state trajectory. (b) G_1 deviation from nominal frequency. (c) G_1 phase angle. (d) G_1 output voltage.

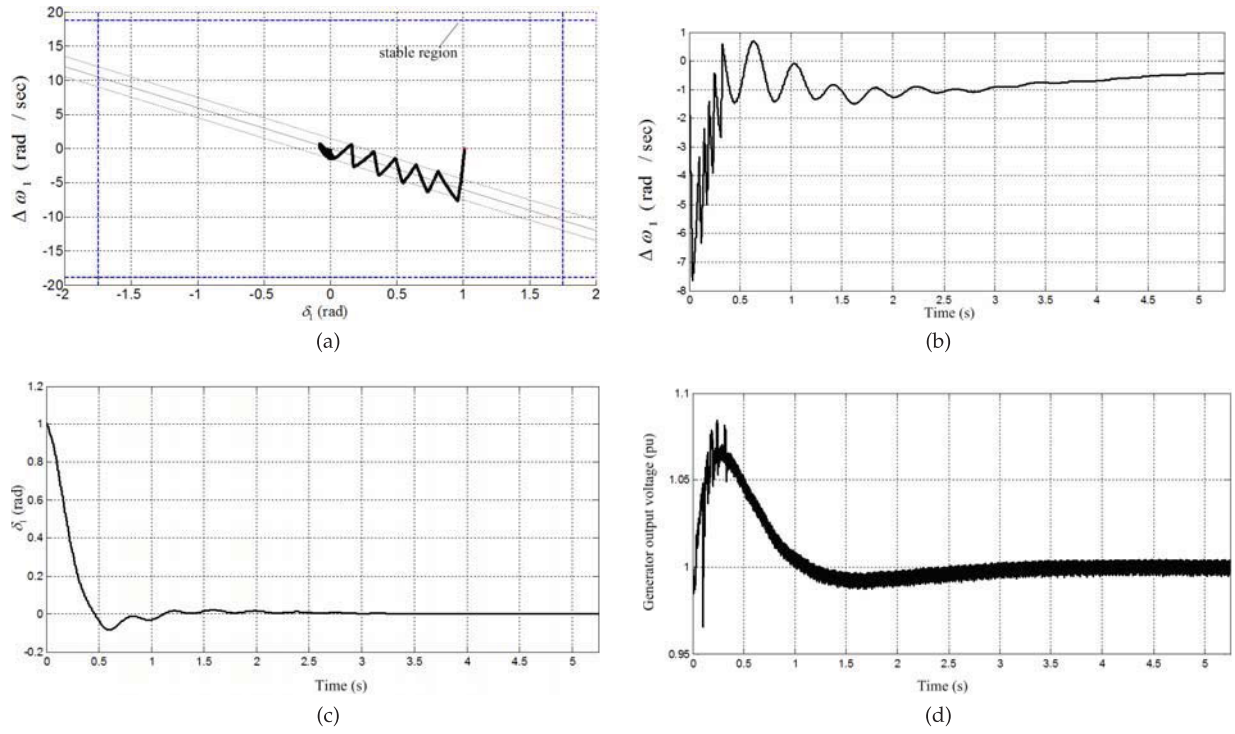

FIGURE 9. PSCAD simulation results of WECC system in the presence of persistent variable structure switching for $s = 6\delta_1 + \omega_1$ from 0 seconds. (a) System state trajectory. (b) G_1 deviation from nominal frequency. (c) G_1 phase angle. (d) G_1 output voltage.

value of the linearized results, we present in Table 2 the ranges of c_1 corresponding to the existence or lack of sliding mode for the three systems: linearized SMIB, nonlinear SMIB and high-order WECC. It is clear that there is a large overlap in

TABLE 2. Empirical existence of sliding surface $s = c_1\delta_1 + \omega_1$ for linearized SMIB, nonlinear SMIB, nonlinear SMIB with parameter errors and WECC test system. Simulation tests were conducted for $c_1 \in Z$ and $-20 \le c_1 \le 20$.

	Linearized SMIB	Nonlinear SMIB
No sliding mode	$-20 \le c_1 < 0.7$	$-20 \le c_1 < 0.6$
Sliding mode exists	$0.7 \le c_1 \le 20$	$0.6 \le c_1 \le 20$
	Nonlinear SMIB w/ parameter error	WECC
No sliding mode	$-20 \le c_1 < 0.6$	$-20 \le c_1 < 0.7$
Sliding mode exists	$0.6 \le c_1 \le 20$	$0.7 \le c_1 \le 20$

the existence of a sliding mode in both the nonlinear and linearized versions demonstrating how our approximation does not significantly affect the degree of vulnerability present in the system.

VI. LIMITATIONS ON ATTACKER KNOWLEDGE

To construct and apply a successful coordinated variable structure switching attack, an opponent would need to leverage cyber intrusion to enable Conditions (B) and (D) of Section II-B as well as have a local model of the smart grid in the proximity of the target and corrupt breaker.

Given the need for timed coordination in the attack, switching control is imperative for success. However, in this section, we assess the effect of limitations on opponent knowledge to the ability to construct and execute an attack. We focus on model error, which affects the ability to construct a feasible attack and strategies to contend with only partial state information, which affects attack execution.

A. MODEL PARAMETER ERROR

Questions naturally arise as to the effects of model error on attack construction. Consider the system of (12) with parameter error:

$$A_1 : \begin{cases} \dot{\delta}_1 = 0(1+\varepsilon_{11}) + (1+\varepsilon_{12})\omega_1 \\ \dot{\omega}_1 = (-10+\varepsilon_{13})\sin\delta_1 + (-1+\varepsilon_{14})\omega_1 \end{cases}$$
$$A_2 : \begin{cases} \dot{\delta}_1 = 0(1+\varepsilon_{21}) + (1+\varepsilon_{22})\omega_1 \\ \dot{\omega}_1 = 9 + (-10+\varepsilon_{23})\sin\delta_1 + (-1+\varepsilon_{24})\omega_1. \end{cases} \quad (15)$$

where $\{\varepsilon_{ij}\}$ are specific parameter error values. The existence conditions of Theorem III-A.2 become:

$$c_1(1+\varepsilon_{12})\omega_1 - 10c_2(1+\varepsilon_{13})\delta_1 - c_2(1+\varepsilon_{14})\omega_1 < 0 \quad \text{for } c_1\delta_1 + c_2\omega_1 > 0$$
$$c_1(1+\varepsilon_{22})\omega_1 - 10c_2(1+\varepsilon_{23})\delta_1 - c_2(1+\varepsilon_{24})\omega_1 + 9c_2 > 0 \quad \text{for } c_1\delta_1 + c_2\omega_1 < 0$$

Fig. 10 illustrates the effects of errors; the associated change in slope of the region boundaries due to parameter errors result in both false positives and false negatives for the determination of C. Study of Fig. 10 reveals that a robust strategy for the selection of C would be to select a value *internal* to the region boundaries. If bounds on ε_{ij} are available, then it is possible guarantee a robust selection of C that is far enough from the boundaries.

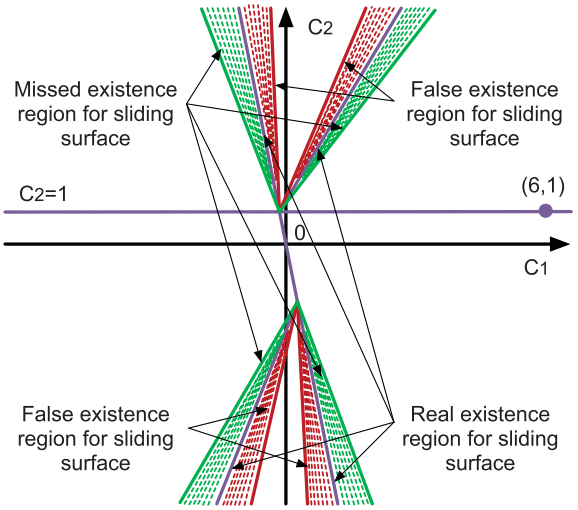

FIGURE 10. Effect of model error on sliding mode identification. Selection of C = [6 1] is internal to the boundaries and guarantees robustness against a degree of model error.

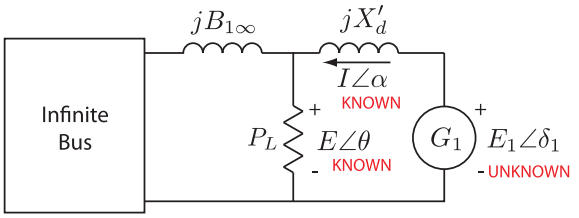

FIGURE 11. SMIB system approximation for partial state estimation.

B. PARTIAL STATE INFORMATION

The opponent may gain target state information through cyber intrusion and eavesdropping. The feasibility of this depends on the communication media and protocols used; further discussion is beyond the scope of this paper.

In this section, we investigate the efficacy of our attack approach when only partial state information is available. Here, we assume that the opponent aims to estimate the missing state information, from say other available information, resulting in an increase in attack complexity.

We consider the case in which an attack is applied to the revised WECC test system of Fig. 7. We assume that the Generator G_1 frequency ω_1 is known to the opponent, but the rotor angle δ_1 must be estimated in some way. Specifically, we assume as an example the terminal voltage and current of an associated transmission line is known and must be used in the estimation of δ_1.

Modeling the standard WECC system in relation to G_1 as a SMIB system, we obtain the system in Fig. 11. Applying Kirchoff's law gives:

$$\begin{aligned} E_1\angle\delta_1 &= jX'_dI\angle\alpha + E\angle\theta \\ &= (E\cos\theta - X'_dI\cdot\sin\alpha) + j(E\sin\theta - X'_dI\cos\alpha) \end{aligned}$$

where $E_1\angle\delta_1$ is the generator internal voltage, jX'_d is the impedance of transmission line, $I\angle\alpha$ is the current of transmission line and $E\angle\theta$ is the terminal voltage. Thus, the generator internal voltage E_1 and phase angle δ_1 can be estimated using the following equations:

$$E_1 = \sqrt{(E\cos\theta - X'_d I\cdot\sin\alpha)^2 + (E\sin\theta - X'_d I\cos\alpha)^2} \tag{16}$$

and $\tan\delta_1 = \frac{E\sin\theta + X'_d I\cos\alpha}{E\cos\theta - X'_d I\sin\alpha}$.

Given the approximation that $\tan\delta_1 \approx \delta_1$ when δ_1 is small, we have

$$\delta_1 \approx \tan\delta_1 = \frac{E\sin\theta + X'_d I\cos\alpha}{E\cos\theta - X'_d I\sin\alpha}. \tag{17}$$

Therefore, δ_1 can be estimated via the terminal voltage $E\angle\theta$ and current $I\angle\alpha$ of transmission line as follows:

$$\begin{bmatrix}\hat{\delta}_1\\ \omega_1\end{bmatrix} = \begin{bmatrix}\frac{E\sin\theta + X'_d I\cos\alpha}{E\cos\theta - X'_d I\sin\alpha}\\ \omega_1\end{bmatrix}. \tag{18}$$

Using this estimation approach, we apply the attack from 0 to 2.5 seconds on a PSCAD simulation of the test system of Fig 7; as shown in Fig. 12, the system dynamics follow the sliding mode to subsequently produce instability and disruption.

VII. RELATED WORK

Our work builds on the body of recent research that has focused on the interaction between the cyber and physical aspects of a smart grid to aid in vulnerability analysis takes on a variety of flavors. These techniques can be classified into a number of categories. *Static approaches* [1] consider the topological information about the smart grid in order to study vulnerabilities often using graph-theoretic means. Compact relationships between system components that can lead to cascading corruption and failure are identified. *Empirical approaches* [12]–[15] harness research and development of realistic communications and power systems simulators. These two forms of simulators are combined such that an attack is applied in the communication simulator that transfers data to the power systems simulator which makes decisions based on this possibly corrupt information. Typical traditional power system reliability metrics are used to assess impact of the cyber attacks. Such approaches are valuable in providing indications of attack impacts, but often require exhaustive 'what-if' forms of attack case analysis that are limited from providing general principles for grid design. In *cyber-physical leakage approaches* [24], [25] confidentiality of the cyber network is studied by identifying how voltage and current measurements of the physical power system can be successfully analyzed for any clues about cyber protocol activity. *Testbed research* addresses the exploration of practical vulnerabilities through SCADA testbed development and construction [11], [12]. Although some insights on how to protection industrial control systems for SCADA are provided. There exists room to develop more prescriptive approaches to provide more general design guidelines for future smart grid systems.

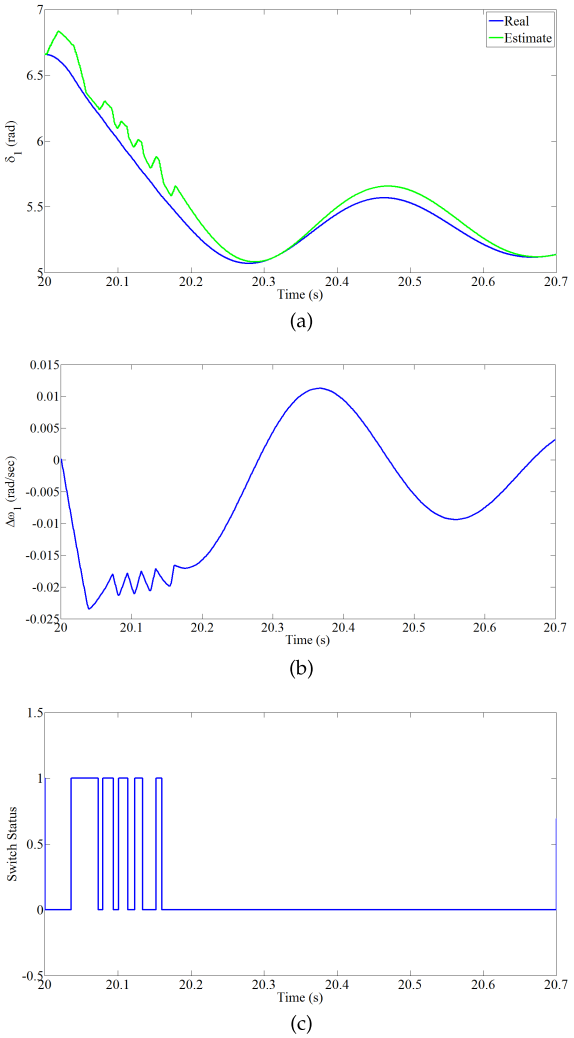

FIGURE 12. Coordinated switching attack with partial state knowledge on test system of Fig. 7. (a) G1 phase angle. (b) G1 deviation from nominal frequency. (c) Switch Status.

VIII. FINAL REMARKS

A grand challenge in cyber-physical systems research is the development of models that elegantly interface the discrete-time characteristics of the cyber infrastructure with the analog nature of the physical system. We believe that our use of variable structure system theory conveniently interfaces the switching cyber-control within power systems to provide a novel way to understand the cyber-physical interaction and in the case of this paper gain insight into new forms of vulnerability. In addition, it lends itself to a natural mathematical framework and formalism useful for automatic identification of vulnerabilities. The use of dynamical systems allows for flexible granularity and can conveniently be implemented for simulation.

Our work demonstrates the efficacy of coordinated variable structure switching attacks by demonstrating how attack con-

struction on a linearized version of the system still executes on nonlinear and realistic models of the system. Moreover, the attack can be successful even under conditions of model error and partial state knowledge. Future work will aim to apply variable structure system theory to model robotics systems as discussed in [26] and [27] and generalized social networking contexts when switched dynamics may be appropriate for representing simple cyber-assisted human decision-making amongst finite choices such as those made when gambling or in elections.

REFERENCES

[1] D. Conte de Leon, J. Alves-Foss, A. Krings, and P. Oman, "Modeling complex control systems to identify remotely accessible devices vulnerable to cyber attack," in *Proc. 1st Workshop Sci. Aspects Cyber Terrorism*, Nov. 2002, pp. 1–3.

[2] D. D. Dudenhoeffer, M. R. Permann, S. Woolsey, R. Timpany, C. Miller, A. McDermott, and M. Manic, "Interdependency modeling and emergency response," in *Proc. Summer Comput. Simul. Conf.*, Jul. 2007, pp. 1230–1237.

[3] B. Rozel, M. Viziteu, R. Caire, N. Hadjsaid, and J.-P. Rognon, "Towards a common model for studying critical infrastructure interdependencies," in *Proc. IEEE Power Energy Soc. General Meeting Convers. Del. Electr. Energy 21st Century*, Jul. 2008, pp. 1–6.

[4] N. HadjSaid, C. Tranchita, B. Rozel, M. Viziteu, and R. Caire, "Modeling cyber and physical interdependencies—Application in ICT and power grids," in *Proc. IEEE Power Syst. Conf. Exposit.*, Mar. 2009, pp. 1–6.

[5] J. Stamp, A. McIntyre, and B. Ricardson, "Reliability impacts from cyber attack on electric power systems," in *Proc. IEEE Power Syst. Conf. Exposit.*, Mar. 2009, pp. 1–8.

[6] S. Sheng, W. L. Chan, K. K. Li, D. Xianzhong, and Z. Xiangjun, "Context information-based cyber security defense of protection system," *IEEE Trans. Power Delivery*, vol. 22, no. 3, pp. 1477–1481, Jul. 2007.

[7] D. Edwards, S. K. Srivastava, D. A. Cartes, S. Simmons, and N. Wilde, "Implementation and validation of a multi-level security model architecture," in *Proc. Int. Conf. Intell. Syst. Appl. Power Syst.*, Nov. 2007, pp. 1–4.

[8] T. Mander, F. Nabhani, L. Wang, and R. Cheung, "Integrated network security protocol layer for open-access power distribution systems," in *Proc. IEEE Power Eng. Soc. General Meeting*, Jun. 2007, pp. 1–8.

[9] K. Xiao, N. Chen, S. Ren, L. Shen, X. Sun, K. Kwiat, and M. Macalik, "A workflow-based non-intrusive approach for enhancing the survivability of critical infrastructures in cyber environment," in *Proc. 3rd Int. Workshop Softw. Eng. Secure Syst.*, May 2007, pp. 1–4.

[10] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol, "SCADA cyber security testbed development," in *Proc. 38th North Amer. Power Symp.*, Sep. 2006, pp. 483–488.

[11] A. Giani, G. Karsai, T. Roosta, A. Shah, B. Sinopoli, and J. Wiley, "A testbed for secure and robust SCADA systems," *SIGBED Rev.*, vol. 5, no. 2, pp. 1–4, Jul. 2008.

[12] G. Dondossola, F. Garrone, and J. Szanto, "Supporting cyber risk assessment of power control systems with experimental data," in *Proc. IEEE Power Syst. Conf. Expo.*, Mar. 2009, pp. 1–3.

[13] 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 1st Int. Conf. Smart Grid Commun.*, Oct. 2011, pp. 49–54.

[14] 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 CSIIRW*, Oct. 2011, pp. 1–4.

[15] 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 *Proc. IEEE Power Energy Soc. General Meeting*, Jul. 2012, pp. 1–6.

[16] Z. Sun and S. S. Ge, *Switched Linear Systems: Control and Design*. New York, NY, USA: Springer-Verlag, 2005.

[17] R. A. DeCarlo, S. H. Zak, and G. P. Matthews, "Variable structure control of nonlinear multivariable systems: A tutorial," *Proc. IEEE*, vol. 76, no. 3, pp. 212–232, Mar. 1988.

[18] M. Vidyasagar, *Nonlinear Systems Analysis*. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.

[19] 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*, Nov. 2009, pp. 21–32.

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

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

[22] P. Kundur, *Power System Stability and Control*. New York, NY, USA: McGraw-Hill, 1994.

[23] P. W. Sauer and M. A. Pai, *Power System Dynamics and Stability*. Champaign, IL, USA: Stipes Publishing, 2007.

[24] 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.

[25] B. McMillin, "Complexities of information security in cyber-physical power systems," in *Proc. IEEE Power Syst. Conf. Exposit.*, Mar. 2009, pp. 1–2.

[26] V. Utkin, J. Guldner, and J. Shi, *Sliding Mode Control in Electro-Mechanical Systems*. New York, NY, USA: Taylor & Francis, 1999.

[27] A. Sabanovic, "Variable structure systems with sliding modes in motion control—A survey," *IEEE Trans. Ind. Inf.*, vol. 7, no. 2, pp. 212–223, May 2011.

SHAN LIU received her Ph.D. degree in electrical and computer engineering from Texas A&M University, in 2013. 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. She is currently an Assistant Professor at the Communication University of China.

SALMAN MASHAYEKH is currently pursuing the Ph.D. degree in electrical and computer engineering with Texas A&M University. His research interests include power management systems, and physical security and cyber security of power systems.

DEEPA KUNDUR is a Professor of electrical and computer engineering with the University of Toronto. She is an Appointed Member of the NERC Smart Grid Task Force, was an Elected Member of the IEEE Information Forensics and Security Technical Committee, and was the Inaugural Vice-Chair of the Security Interest Group of the IEEE Multimedia Communications Technical Committee. She was a Chair of the Trustworthy Cyber-Physical Systems and Infrastructures Track of the NSF and PNNL-sponsored 2011 Workshop on Cooperative Autonomous Resilient Defenses in Cyberspace and was an invited speaker to the NSF-sponsored 2011 Workshop on Cyber-Physical Applications in Smart Grids. She is the author of several widespread tutorial papers, including two articles in the IEEE SIGNAL PROCESSING MAGAZINE in 1996 and 2004 and three articles in the PROCEEDINGS OF THE IEEE in 1999, 2004, and 2008.

TAKIS ZOURNTOS is with Texas A&M University and OCAD University. He received the B.A.Sc., M.A.Sc., and Ph.D. degrees in electrical and computer engineering from the University of Toronto in 1993, 1996, and 2003, respectively. He has over 15 years of 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 Magazine*'s 2009 Best of What's New: Security Innovation and wired.com.

KAREN BUTLER-PURRY is a Professor of electrical and computer engineering and an Associate Provost Graduate Studies with Texas A&M University. She is a well-known authority 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.