Coordinated Variable Structure Switching in Smart Power Systems: Attacks and Mitigation

Shan Liu, Deepa Kundur, Takis Zourntos and Karen Butler-Purry
Department of Electrical and Computer Engineering
Texas A&M University
College Station, Texas 77843-3128, USA
{liu2712, dkundur, takis, klbutler}@tamu.edu

ABSTRACT

Recently, a class of cyber-physical attacks termed coordinated variable structure switching attacks has been identified for future smart grid systems. Here, an attacker who has remotely gained access to a circuit breaker or switch is able to disrupt power system operation by applying a state-dependent switching sequence. The sequence can be effectively designed employing variable structure systems theory. In this work, we extend this research to demonstrate an approach to mitigation within this variable structure system framework. Specifically, we study strategies employed by a power system operator in the face of a switching attack to steer the system to a stable equilibrium through persistent co-switching and by leveraging the existence of a stable sliding mode. We demonstrate how such co-switching can be designed for a variant of the WECC 3-machine, 9-bus system using linearized models and then employ simulations in MATLAB/Simulink and PSCAD to demonstrate its potential in practice.

Categories and Subject Descriptors

C.4 [**Computer Systems Organization**]: Performance of Systems—*Modeling techniques*; G.1.7 [**Mathematics of Computing**]: Ordinary Differential Equations—*Convergence and stability*; I.6.5 [**Computing Methodologies**]: Model Development—*Modeling methodologies*

General Terms

Performance, security, theory

Keywords

cyber-physical system security, coordinated variable structure switching, smart grid attack mitigation

HiCoNS'12, April 17–18, 2012, Beijing, China.

1. INTRODUCTION

It is well known that future smart grid systems aim to enable greater reliability, efficiency, economics, sustainability and security. This is achieved through the marriage of information technology with the power generation and delivery network. Within such a cyber-physical system increased autonomy and functionality is enabled, in part, through situational awareness and distributed control. A physical-to-cyber bridge manifests at measurement devices such as phasor measurement units (PMUs) and intelligent electronic devices (IEDs) to enable the acquisition of highly granular data for use in decision-making. A cyber-to-physical bridge arises at actuators including circuit breakers and switches which can be remotely controlled by system operators and distributed control devices.

Recently, the authors have demonstrated how an opponent can leverage the future connectivity of these breakers and switches to disrupt power delivery. Specifically, we have identified the existence of a class of cyber-physical system attacks entitled *coordinated variable structure switching attacks* in which an opponent can employ local state information to design a switching sequence that can destabilize synchronous generators leading to various forms of instability and power loss [2, 3].

In this work, we extend our research to demonstrate an approach to mitigation within this variable structure system framework. Specifically, we study strategies employed by a power system operator in the face of a switching attack to steer the system to a stable equilibrium through persistent co-switching and by leveraging a stable *sliding mode*. In the next section, we provide a necessary background to variable structure systems and the sliding mode. We highlight the conditions for the existence of a sliding mode and demonstrate how the concept can be employed by either an attacker or system operator to achieve diverse objectives. In Section 3 we detail a mathematical approach to design a mitigation technique against the class of switching attacks and apply it to the Western Electricity Coordinating Council (WECC) 3-machine, 9-bus system. Simulations are employed to verify our design results in Section 4. The paper concludes with final remarks in Section 5.

2. COORDINATED VARIABLE STRUCTURE SWITCHING

2.1 Variable Structure Systems and the Sliding Mode

Variable structure systems are a class of hybrid dynamical systems that consist of a family of subsystems and one or more rules that govern the switching among them [6]. Such systems exhibit both continuous and discrete states of behavior important for modeling some underlying characteristics of cyber-physical systems. For example, the switching behavior represents an important analogy for discrete-time decision-making especially involving power network reconfiguration as determined by the state of associated circuit breakers and switches. Moreover, the subsystem dynamics represent a convenient structure from which to model power system physics under a static switch condition. The natural scalability of variable structure systems enables the modeling of complex interdependencies in cyber-enabled power systems.

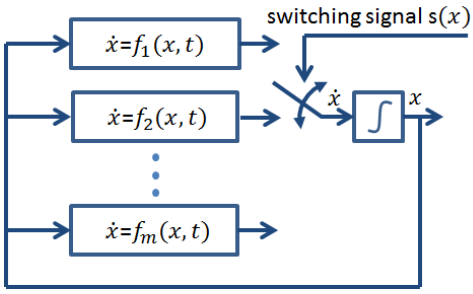

Figure 1: State-dependent variable structure system.

Fig. 1 is a pictorial representation of a variable structure system with *state-dependent* switching. Here, the subsystem dynamics are described as:

$$\dot{x} = f_i(x,t) \tag{1}$$

where $i \in \{1,\ldots,m\}$ is the subsystem index (also known as the switch position), $x \in \mathbb{R}^{n\times 1}$ is the state vector, $f_i(x,t) \in \mathbb{R}^{n\times 1}$ is the subsystem dynamics corresponding to switch position i and $s(x) \in \mathbb{R}^{1\times n}$ is the switching signal where $s(x) = 0$ is called the *switching surface*. For certain system parameters and selection of $s(x)$ it can be shown that Eq. 1 exhibits a form of behavior known as a *sliding mode* [1, 6]. Here, the trajectory of x is attracted and subsequently confined to the n-dimensional surface $s(x) = 0$, which in the case of a sliding mode is also termed the *sliding surface*.

The necessary and sufficient conditions for the existence of a sliding mode are given by:

$$\lim_{s(x)\to 0^+} \dot{s}(x) < 0 \quad \text{and} \quad \lim_{s(x)\to 0^-} \dot{s}(x) > 0. \tag{2}$$

For $m = n = 2$ and

$$\dot{x}(t) = \begin{cases} f_1(x,t), & s(x) > 0 \\ f_2(x,t), & s(x) \le 0 \end{cases}, \tag{3}$$

Fig. 2 pictorially describes how the sliding surface partitions two distinct regions in state-space given by $s(x) > 0$ and $s(x) < 0$. When in either one of these regions local to the sliding surface, the state is attracted back to it as governed by the complementary sign of $\dot{s}(x)$ in Eq. 2.

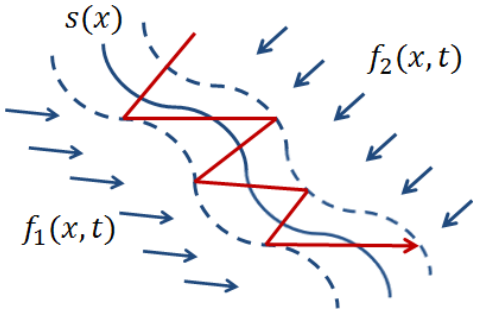

Figure 2: Under the conditions of Eq. 2 a state x is (locally) attracted to the sliding surface $s(x) = 0$, and once on this surface it will stay on the surface.

Recently we have demonstrated how variable structure system theory can be applied to the modeling of power system reconfiguration and its subsequent attack. Through judicious selection of a sliding surface, an attacker can construct switching attacks on select breakers to destabilize power system components [2, 3].

2.2 Cyber-Physical Attack via Variable Structure Theory

As power systems become increasingly cyber-enabled, cyber attack will become a possible method of wrongly gaining control of networked electromechanical switches. Forms of cyber attack may include intrusion into the communications infrastructure that networks the switch or the operating system of a device that controls it. Coordinated variable structure switching attacks are facilitated through cyber attack, but are designed to have a specific goal of physical disruption. They require that the opponent have control over the electromechanical switching actions of one or more relay(s) and/or circuit breaker(s) of the target power system as well as knowledge of the local state dynamics and partial state values.

An approach to construct a coordinated variable structure switching attack involves modeling the power system under consideration as a variable structure system and then identifying an appropriate sliding surface $s(x)$ that when applied as state-dependent switching, will destabilize the system; details are found in [2, 3].

We illustrate attack construction through the elementary example of Fig. 3, which represents a load shedding scenario. The (blue) dashed lines and hexagons represent (cyber) communication channels, sensors, breaker actuators and the system control center. The (black) solid lines correspond to physical power system devices such as generators, loads, switches and transmission lines. In this example, the generator G can serve one of two possible loads $Z1$ or $Z2$ controlled through load switch $S2$. Employing information from sensors $S1$ and $S2$, the control center makes decisions on the position of $S2$ and hence the serviced load. The overall, switched system of Fig. 3 can be modeled as:

$$\dot{x} = \begin{cases} f_1(x,t), & s(x) > 0 \\ f_2(x,t), & s(x) \le 0 \end{cases} \tag{4}$$

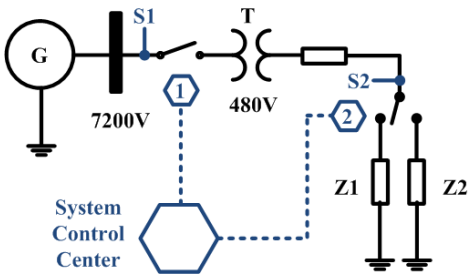

Figure 3: Elementary variable structure system example. Two different dynamics describe behavior of the power system depending on the status of switch $S2$.

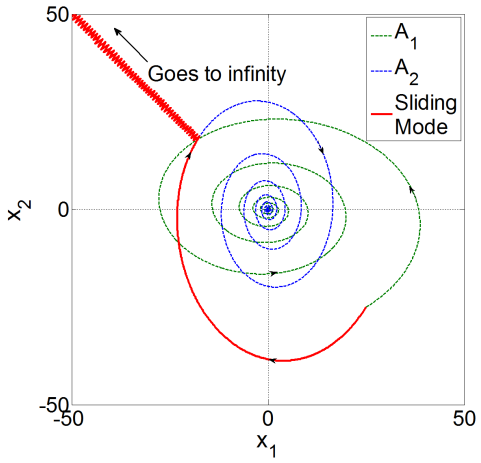

Figure 4: Phase portraits of switched system with $s = x_1 + x_2$.

where $x \in \mathbb{R}^{n\times 1}$ is the state vector, $f_i(x,t) \in \mathbb{R}^{n\times 1}$, $i \in \{1,2\}$ is the subsystem dynamics when $S2$ connects Z_i, and $s(x) \in \mathbb{R}^{1\times n}$ where $s(x) = 0$ is the switching surface.

Consider a specific case of Fig. 3 in which we assume linear models and $n = 2$; where $x = [x_1, x_2]^T$. Suppose,

$$\dot{x} = \begin{cases} A_1 x, & s(x) > 0, \text{ where } A_1 = \begin{bmatrix} -1 & -10 \\ 5 & -0.5 \end{bmatrix} \\ A_2 x, & s(x) \leq 0, \text{ where } A_2 = \begin{bmatrix} -0.5 & 5 \\ -10 & -1 \end{bmatrix} \end{cases} \quad (5)$$

for some $s(x)$. It can be shown that both subsystems (i.e., in a static switch position) are globally asymptotically stable. However, under the following switching rules

$$s(x) = x_1 + x_2 \quad \text{and} \quad s(x) = -x_1 + x_2$$

the switched system trajectories of Fig. 4 and Fig. 5 are exhibited. The first switching rule exhibits unstable sliding mode behavior and would be appropriate to be employed by an attacker for system destabilization. The second switching rule enables the system to converge to the stable equilibrium point.

We have shown in [2, 3] how variable structure system theory can be used to design switching rules for attack to destabilize the system through the selection of an appropriate sliding surface $s(x)$. In this work, we focus on the

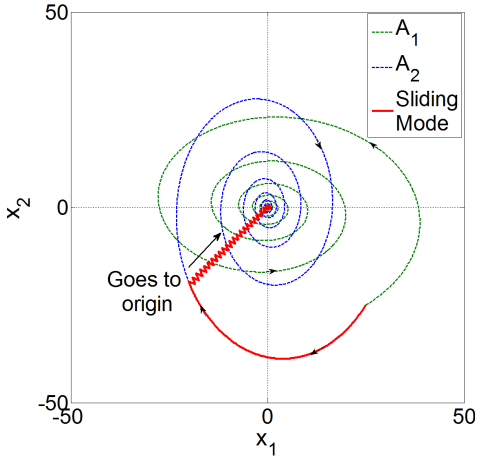

Figure 5: Phase portraits of switched system with $s = -x_1 + x_2$.

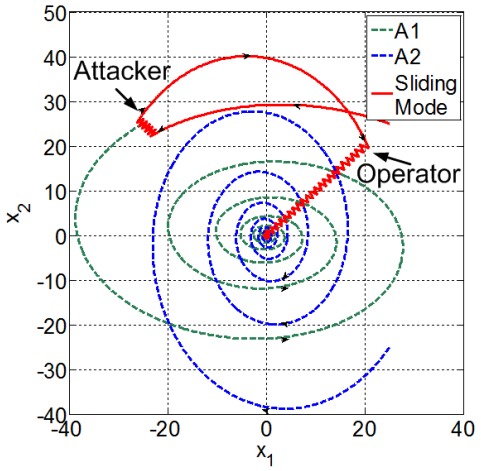

Figure 6: State trajectory for attack (at $t = 0$) using $s(x) = x_1 + x_2$ and attacker lockout and operator control (at $t = 1$s) using $s(x) = -x_1 + x_2$.

properties of *stable* sliding modes and leverage their existence to equip operators with a means of mitigation against such attacks once detected.

To illustrate our idea, consider the situation whereby a switching attack is remotely applied to a system described by Eq. 5 using $s(x) = x_1 + x_2$ at time $t = 0$ seconds. Suppose through cyber and physical means of intrusion detection, an operator is able to identify the the attack and remove remote access capability of the opponent. In order to steer the system back to a stable equilibrium point, the operator can exploit the stable sliding mode of $s(x) = -x_1 + x_2$ at say time $t = 1$ second. The resulting state trajectory of the limited-time attack and operator control is shown in Fig. 6 with corresponding switch status in Fig. 7. We observe that the system travels along the unstable sliding mode until the attacker lockout and subsequent trajectory steering back to the equilibrium by the operator.

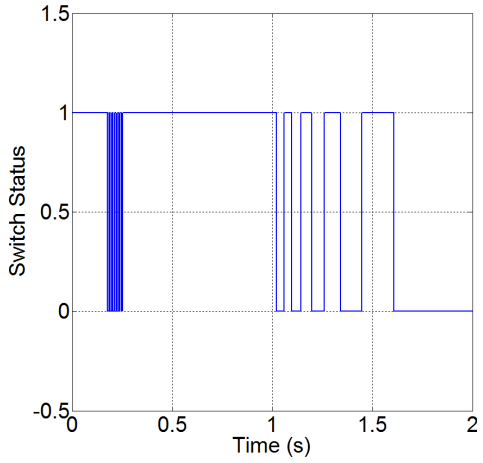

Figure 7: Switch status during attack and mitigation.

2.3 Sliding Mode Existence for Linear Dynamics

Mathematically determining the existence of a sliding mode (for either attack or mitigation) for a general class of variable structure systems is equivalent to establishing that the conditions of Eq. 2 hold. Analytic results are difficult to determine for general subsystem dynamics, functions $s(x)$ and problem dimensionality. However, assuming linear models of dynamics and the switching surface and for a single switch case, the following theorem has been derived by the authors in [4] regarding the existence of such sliding modes.

THEOREM 1 (EXISTENCE OF A SLIDING MODE). *Given the variable structure system:*

$$\dot{x} = \begin{cases} A_1 x + b_1, & s(x) > 0 \\ A_2 x + b_2, & s(x) \leq 0 \end{cases} \tag{6}$$

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*

$$s(x) = Cx \in \mathbb{R} \tag{7}$$

for constant row vector $C = [c_1\ c_2\ \cdots\ c_n] \in \mathbb{R}^{1\times n}$ *the necessary and sufficient conditions for the existence of a sliding mode are:*

$$\begin{cases} C(A_1 x + b_1) < 0, & s(x) > 0 \\ C(A_2 x + b_2) > 0, & s(x) < 0 \end{cases}. \tag{8}$$

We assert that this theorem is useful for identifying the parameters C to construct coordinating variable structure switching attacks or mitigation strategies because many power system configurations can be approximated as tractable low-order linear models within a local range of operating conditions. Specifically, an opponent or operator would have to determine the vector C for a given A_i, b_i, $i \in \{1, 2\}$ such that Eq. 8 holds. It can be shown that stable and unstable sliding modes exist and the operator can leverage such stable modes of behavior.

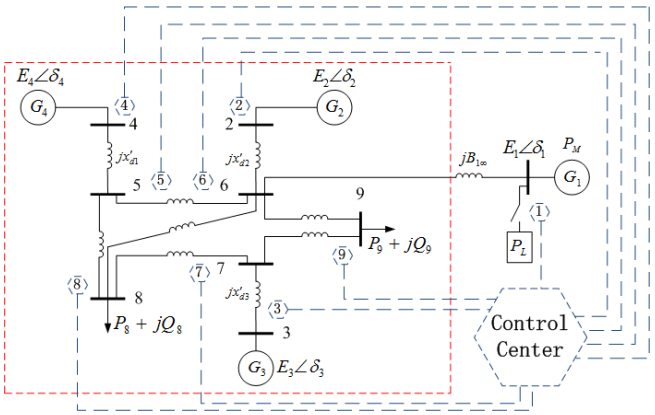

Figure 8: One line diagram of revised Western Electricity Coordinating Council (WECC) 3-machine, 9-bus system. The (red) dashed rectangle is approximated as a SMIB system.

3. COORDINATED VARIABLE STRUCTURE SWITCHING FOR MITIGATION

In this section, we demonstrate the utility of Theorem 1 in determining a strategy for switching-based operator mitigation through study of a variant of the well known Western Electricity Coordinating Council (WECC) 3-machine, 9-bus system.

3.1 System Modeling and Variable Structure Representation

Fig. 8 shows both cyber and physical components of the WECC 3-machine, 9-bus system. The (blue) dashed lines represent the cyber components which correspond to communication channels, sensors, breaker actuators and the control center. The (black) solid lines illustrate physical power system elements including generators, loads, switches, transmission lines.

We approximate this system using the following second order nonlinear single-machine infinite bus (SMIB) model:

$$\begin{cases} \dot{\delta}_1 &= \omega_1 \\ M_1\dot{\omega}_1 &= P_{M1} - E_1^2 G_{11} - s_L P_L \\ & \quad -E_1 E_\infty B_{1\infty} \sin\delta_1 - D_1\omega_1 \end{cases} \tag{9}$$

where δ_1 and ω_1 are the rotor angle and rotor speed deviation of Generator G_1, respectively, and collectively form the system state vector $x = [\delta_1\ \omega_1]^T$. The parameters M_1, D_1 and E_1 represent the moment of inertia, damping coefficient, and internal voltage of Generator G_1, respectively, E_∞ is the voltage magnitude 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 infinite bus.

For simplicity, we may rewrite Eq. 9 as:

$$\begin{cases} \dot{\delta}_1 = \omega_1 \\ M_1\dot{\omega}_1 = P_1 - C_{1\infty}\sin\delta_1 - D_1\omega_1 \end{cases} \tag{10}$$

where $P_1 = P_{M1} - E_1^2 G_{11} - s_L P_L$ 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:

$$A_1 : \begin{cases} \dot{\delta}_1 = \omega_1 \\ \dot{\omega}_1 = -10 \sin \delta_1 - \omega_1 \end{cases} \quad \text{if } P_L \text{ connected}$$
$$A_2 : \begin{cases} \dot{\delta}_1 = \omega_1 \\ \dot{\omega}_1 = 9 - 10 \sin \delta_1 - \omega_1 \end{cases} \quad \text{if } P_L \text{ not connected} \tag{11}$$

where the system state $[\delta_1 \ \omega_1]^T$ represents the phase angle and frequency of Generator G_1.

3.2 Sliding Mode Existence

To apply Theorem 1 to our WECC system model of Eq. 11, we must linearize its representation. We make the simple approximation that $\sin \delta_1 \approx \delta_1$ when δ_1 is small. Assuming $s > 0$ and $s \leq 0$ corresponds to the load switch being closed (subsystem A_1) and open (subsystem A_2), respectively, we therefore obtain:

$$\begin{aligned} \dot{\delta}_1 &= \omega_1 \\ \dot{\omega}_1 &= \begin{cases} -10\delta_1 - \omega_1, & s > 0 \\ 9 - 10\delta_1 - \omega_1, & s \leq 0 \end{cases} \end{aligned} \tag{12}$$

which corresponds to:

$$A_1 = A_2 = \begin{bmatrix} 0 & -1 \\ -10 & -1 \end{bmatrix},$$

$$b_1 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

and

$$b_2 = \begin{bmatrix} 0 \\ 9 \end{bmatrix}$$

in Eq. 6.

We may use Theorem 1 and leverage the linearity of the inequality boundaries to analytically determine the existence and parameter range of a linear sliding surface of the form $s(x) = Cx$. Specifically, we determine the range of C that guarantees the equilibrium point x^* is in the region of attraction given by:

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

For the linearized system of Eq. 12, the following existence conditions for the sliding mode $s = c_1\delta_1 + c_2\omega_1$ are determined:

$$\begin{cases} \begin{cases} c_1\omega_1 - 10c_2\delta_1 - c_2\omega_1 < 0 \\ c_1\delta_1 + c_2\omega_1 > 0 \end{cases} \\ \begin{cases} c_1\omega_1 - 10c_2\delta_1 - c_2\omega_1 + 9c_2 > 0 \\ c_1\delta_1 + c_2\omega_1 < 0 \end{cases} \end{cases}. \tag{13}$$

The results for $x^* = [\delta_1^* \ \omega_1^*]^T = [1.1198 \ 0]^T$ (at the equilibrium of system A_2) are presented in Fig. 9.

As discussed in our previous work [2,3], a sliding mode can also be selected through visual inspection of the overlapping phase portraits of A_1 and A_2. Specifically, an attacker must identify a line whereby the trajectories of the active switched subsystem are pointing towards $s(x) = 0$. Fig. 10 shows the individual and overlapping phase portraits of the linearized subsystems of Eq. 12. Using both techniques (Theorem 1 and visual inspection) we, for example, can determine that the following sliding modes exist: an unstable sliding mode at $s = \delta_1 + 0.5\omega_1$ appropriate for an attacker and a stable sliding mode at $s = \delta_1 + 10\omega_1$ appropriate for an operator trying to stabilize the system.

In the next section employing the attack and mitigation parameters identified here using linearized models, we execute our operator co-switching in the face of a coordinated variable structure switching attack on the lower order nonlinear model of Eq. 11 using MATLAB/Simulink and on a higher order model implemented in PSCAD®. We demonstrate how the identified parameters prove to result in an effective approach for operator restabilization.

4. SIMULATION RESULTS

4.1 SMIB Swing Equation Model

4.1.1 Phase Portraits

The nonlinear second order system model of Eq. 11 is characterized in Fig. 11, which presents the individual phase portraits for the switch in the closed and open position, and the overlapping phase portraits useful in identify a feasible sliding surface $s(x) = 0$. To determine the individual phase portraits, the equilibrium and saddle points are identified by setting the left hand side of the corresponding subsystem dynamics to zero. The system Jacobian matrix is employed to distinguish between the two.

The Jacobin matrix of subsystem A_1 can be expressed as:

$$J_1 = \begin{bmatrix} 0 & 1 \\ -10\cos\delta_1 & -1 \end{bmatrix}. \tag{14}$$

Based on the Jacobian matrix, we identify that the equilibrium points $(2n\pi, 0)$ are stable focus (as all of the resulting eigenvalues of J_1 are all in the left hand plane) and $(2n\pi + \pi, 0)$ are saddle points (one or more eigenvalues of J_1 is in the right hand plane). The stability boundary of the system can be obtained based on the saddle points and inverse time system dynamics. The stability boundary partitions the 2-dimensional space into "smaller" periodically repeating spaces. Each such space includes one stable focus. If the initial state of the system lies in this space, the system will converge to the stable focus within this more compact space shown in the left graph of Fig. 11.

Similarly, we can identify that the equilibrium points of subsystem A_2 are $(2n\pi + 1.1198, 0)$ and $(2n\pi + 2.0218, 0)$, where n is an integer. The Jacobin matrix can be expressed as:

$$J_2 = \begin{bmatrix} 0 & 1 \\ -10\cos\delta_1 & -1 \end{bmatrix}. \tag{15}$$

Thus, we identify that the equilibrium points $(2n\pi+1.1198, 0)$ are stable focus and $(2n\pi+2.0218, 0)$ are saddle points. The stability boundary of the system is obtained similarly to the case of A_1 above.

Using the overlapping phase portrait of Fig. 11, visual inspection can be employed to determine that $s = \delta_1+0.5\omega_1$ and $s = \delta_1 + 10\omega_1$ are indeed sliding modes of the system.

4.1.2 Empirical Results

In order to determine the validity of our proposed approach for mitigation, we simulate the nonlinear swing equation model of Eq. 11 in MATLAB/Simulnk. We first assume that the load is disconnected from the system (i.e., the variable structure system is switched initially to A_2). Therefore,

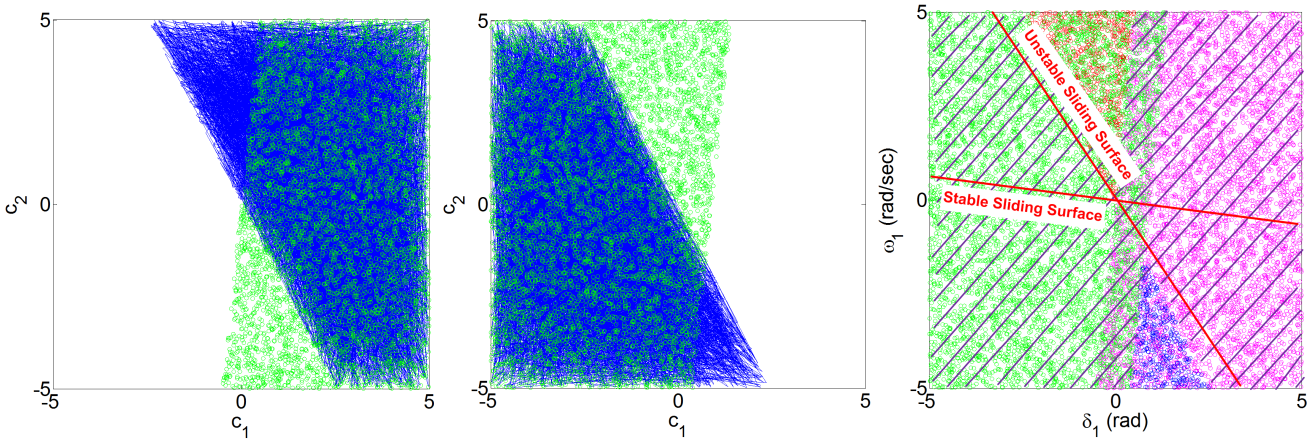

Figure 9: [left] **Range of** C **for** $s > 0$. [middle] **Range of** C **for** $s < 0$. [right] **Overall range of** C **for existence of sliding mode;** $s = \delta_1 + 0.5\omega_1$ **(unstable) and** $s = \delta_1 + 10\omega_1$ **(stable) are highlighted.**

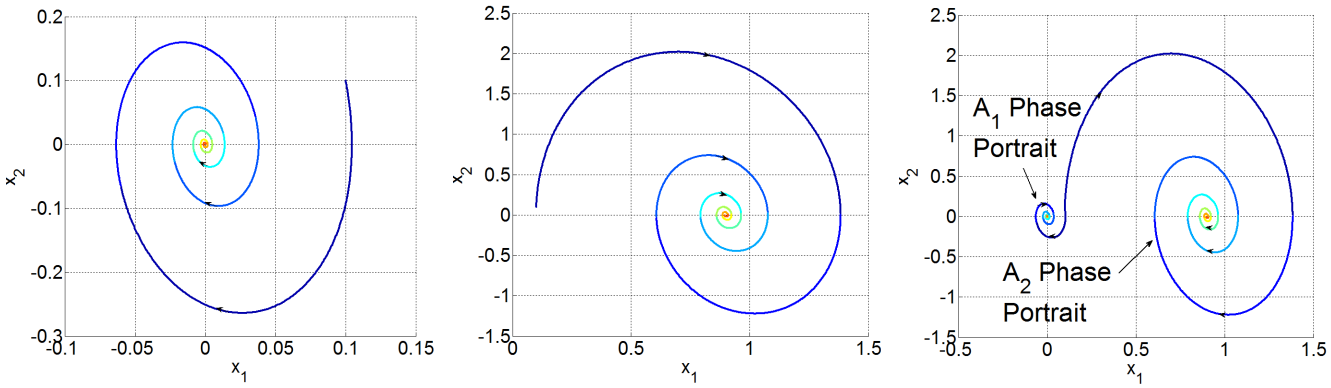

Figure 10: [left] **Linearized phase portrait of system** A_1. [middle] **Linearized phase portrait of system** A_2. [right] **Overlapping linearized phase portraits.**

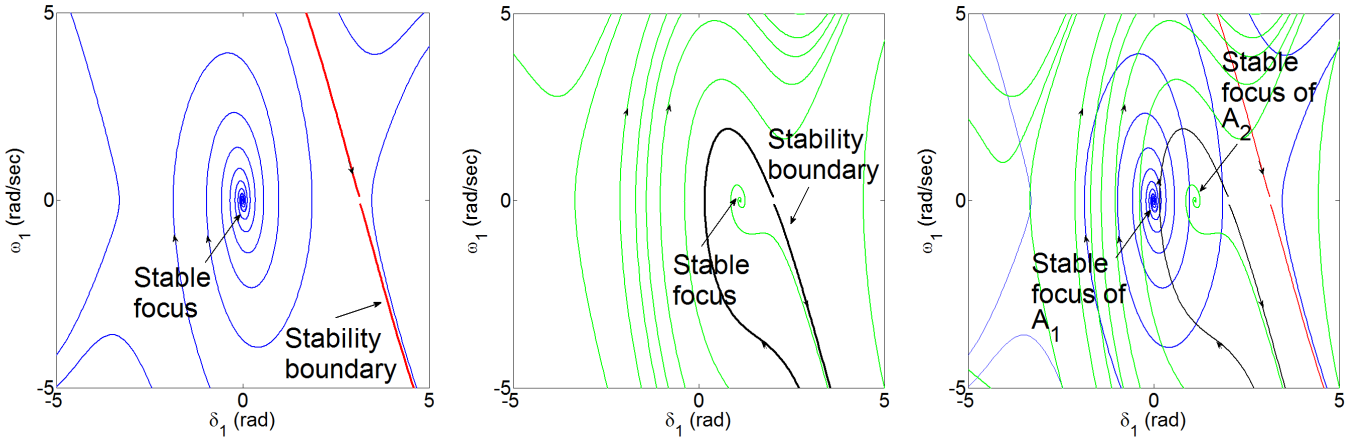

Figure 11: Phase portraits of Eq. 11 subsystems [left] for switch in closed position (A_1)**, [middle] for switch in open position** (A_2)**, [right] shown overlapping.**

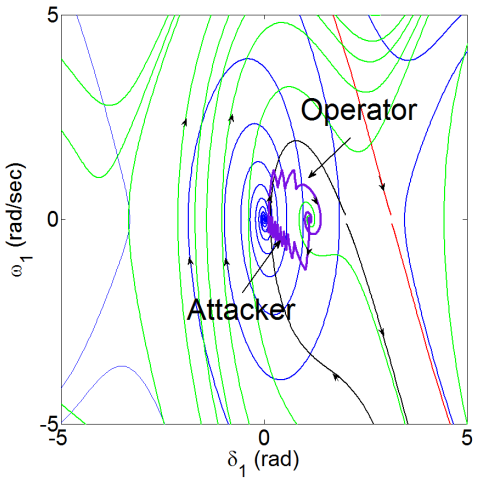

Figure 12: State trajectory employing the SMIB swing equation model in the presence of an attack (0-2.5 s) and operator co-switching (starting at 2.5s) for re-stabilization.

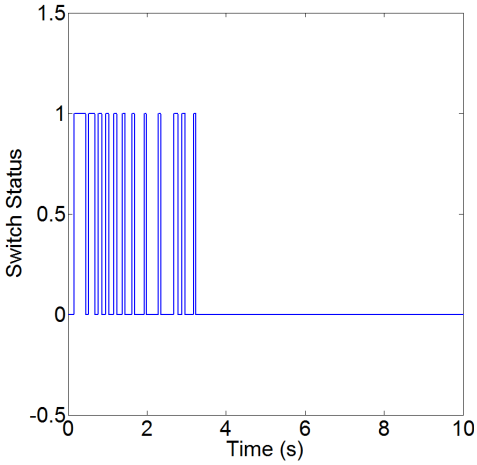

Figure 13: Load switch status during attack and mitigation.

the initial state of the system is chosen as the stable focus of A_2 given by $(1.1198, 0)$. If $s > 0$, the system dynamics switch to system A_1; otherwise, the system dynamics switch to system A_2. Due to the chattering effects, as detailed in [3] we employ a hysteresis effect to make the switching frequency finite.

We assume that an attacker applies a switching attack from 0 to 2.5 seconds employing the unstable sliding mode $s = \delta_1 + 0.5\omega_1$, which aims to drive the system trajectory across the stability boundary of the system A_2, to cause power system instability. Assuming that the operator is notified through intrusion detection systems of the attack, he/she can employs means to disconnect the attacker's remote access and re-steer the system trajectory back to the equilibrium point using the sliding surface $s = \delta_1 + 10\omega_1$ at 2.5 seconds. As can be seen in Fig. 12, the attacker is able to move the state over the stability boundary, but the operator successfully restabilizes the system. The corresponding load switch status is shown in Fig. 13.

4.2 PSCAD® Model

To further demonstrate the potential of our sliding mode design approach, we study applying the attack and mitigation switching strategies to a high order nonlinear PSCAD® model of the WECC 3-machine, 9-bus system of Fig. 8 [5]. Here, the base MVA is 100, the system normal frequency is 60 Hz and the generator parameters are detailed 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. As in the former studies, the P_L load switch is used to attack the system.

Table 1: Generator parameters for WECC 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 sec
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 sec	5.89 sec
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

For consistent comparison, the initial state of the WECC

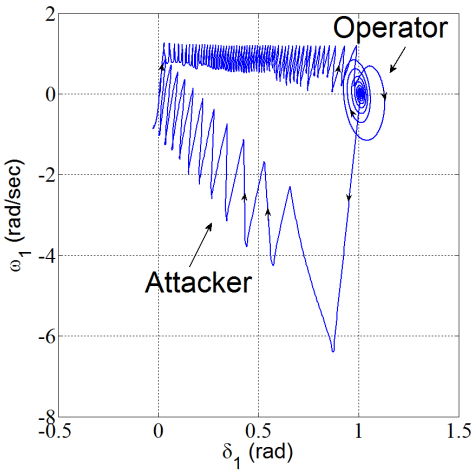

Figure 14: State trajectory employing the PSCAD® model in the presence of an attack (0-0.7s) and operator co-switching (starting at 0.7s) for re-stabilization.

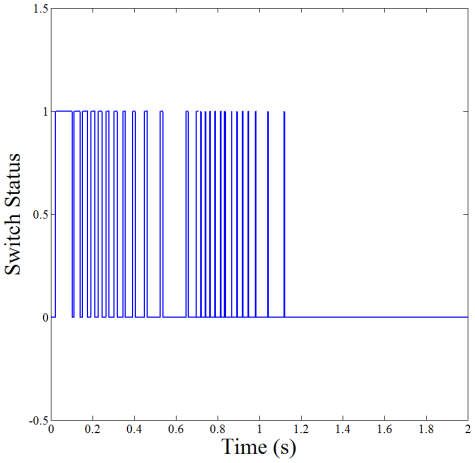

Figure 15: Load switch status during attack and mitigation.

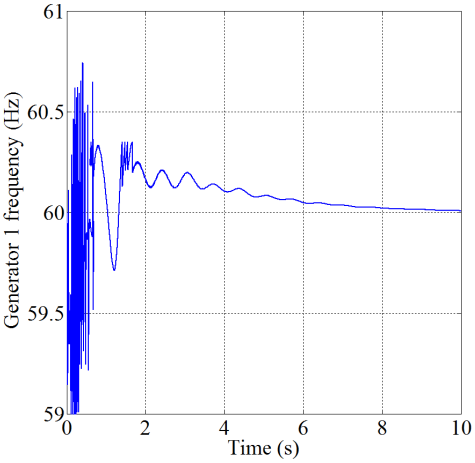

Figure 16: Generator G_1 frequency during attack and mitigation.

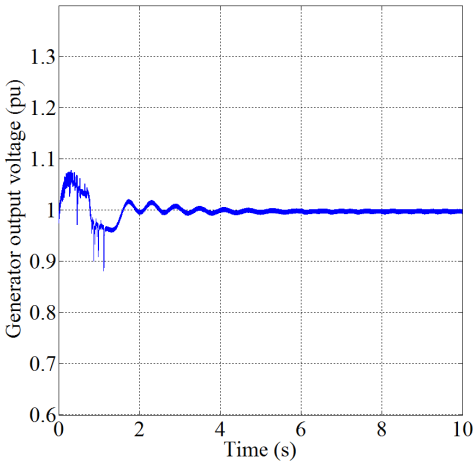

Figure 17: Generator G_1 output voltage during attack and mitigation.

system is set to to the stable focus of $(1.1198, 0)$ and the same sliding modes are employed by the attacker and operator. If $s > 0$, the system dynamics switch to system A_1 and if $s < 0$, they switch to A_2. The attacker applies the sliding mode attack from 0 to 0.7 seconds, which aims to drive 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. At 0.7 seconds, we assume the operator is notified of the attack the thus locks out the attacker by removing other forms of remote access to the switch and then applies switching to the load switch employing the stable sliding mode to drive the system trajectory back to the stable focus of system A_2.

Fig. 14 illustrates how the attacker moves the system over the stability boundary and the operator is subsequently able to redirect the state back to the stable equilibrium. The specific load switch status during both attack and mitigation is shown in Fig. 15. The Generator G_1 frequency and output voltage are displayed in Figs. 16 and 17 to show how operator co-switching enables transient, frequency and voltage stability in the power system.

5. CONCLUSIONS

This paper has extended our recent research identifying a class of power system reconfiguration vulnerabilities termed coordinated variable structure switching attacks by providing strategies for operators to re-stabilize the system (also through switching) once switch control is re-gained from the attacker. We propose a co-switching approach that exploits the existence of *stable* sliding modes that are then used to redirect the system trajectory back to an appropriate stable equilibrium point. Both analytic and empirical results are used to design and verify the potential of coordinated variable structure switching for mitigation.

6. ACKNOWLEDGMENTS

Funding for this work was provided through the Norman Hackerman Advanced Research Program Project 000512-0111-2009 and NSF grants EECS-1028246 and EEC-1062603. The authors also would like to thank Xianyong Feng for pro-

viding a preliminary version of the files for the PSCAD® simulations.

7. REFERENCES

[1] R. A. Decarlo, S. H. Zak, and G. P. Matthews. Variable structure control of nonlinear multivariable systems: A tutorial. *Proceedings of the IEEE*, 76(3):212–232, 1988.

[2] 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 Cyber Security and Information Intelligence Research Workshop*, Oak Ridge National Laboratory, October 2011.

[3] 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. Second IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Brussels, Belgium, October 2011.

[4] 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 Engineering Society General Meeting*, page under review, 2012.

[5] P. W. Sauer and M. A. Pai. *Power System Dynamics and Stability*. Stipes Publishing Co., 2007.

[6] Z. Sun and S. S. Ge. *Switched Linear Systems: Control and Design*. Springer-Verlag, London, 2005.