A Smart Grid Vulnerability Analysis Framework for Coordinated Variable Structure Switching Attacks

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

***Abstract*—In this paper we have proposed an approach for vulnerability analysis of a class of cyber-physical reconfiguration attacks called coordinated variable structure switching. In such an attack, an opponent who gains control over a target circuit breaker, relay or switch can apply a given switching sequence to destabilize the system even if the system is stable in static switch positions. Our analysis approach is illustrated through a case study of the Western Electricity Coordinating Council 3-machine, 9-bus system. MATLAB and PSCAD® simulations are employed to validate the approach. Moreover the insights gained from the vulnerability analysis of the WECC system are consistent with intuition.**

***Index Terms*—smart grid vulnerability analysis, cyber-physical system security, coordinated variable structure switching attacks.**

I. Introduction

The smart grid is an archetypal cyber-physical system in which vulnerabilities are currently being discovered and characterized. Some vulnerabilities emerge from coupled cyber-physical interactions and others from the increased opportunity to remotely access power system components via cyber connectivity. In relation to the latter, we focus on a class of smart grid reconfiguration attacks that are termed coordinated variable structure switching. Existence of such reconfiguration vulnerabilities has been identified [1], [2]. One observation from these studies is the ease at which it was possible to destabilize the power system dynamics with a coordinated switching. The opponent would merely have to find the right parameters. Even if these parameters are selected from a linearized or low-order linear model of the complex power system, they could be successful in destabilizing a power grid.

Of importance to electrical power utilities (EPUs) is an understanding of which system components are most susceptible to such attacks and thus are best prioritized for hardening. In this paper we build upon our past work and propose a vulnerability analysis approach that identifies, assesses and priorities system components for hardening against coordinated variable structure system attacks. The success of this reconfiguration attack in disrupting power system operation is due to the selectively timed switching. In layman's terms, when a given circuit breaker, relay or switch changes state, transients that deviate the system state away from the equilibrium occur. If another change in switch state is applied when the transient is on an increase, then the state will likely be pushed further away from the equilibrium in another upswing. If this pattern of switching continues indefinitely it is possible to attract the system state away from its original equilibrium thus disrupting power system operation.

We define the relative vulnerability of a given power system component capable of switching as the ease with which the attacker can determine parameters for attack. The impact of the attack for a particular attack vector is not used to measure degree of vulnerability as we have observed that the level of disruption is essentially equivalent for all possible attack parameter values.

In the next section, we briefly review coordinated variable structure switching attacks. We present a new existence theorem assuming linear subsystem dynamics. Our vulnerability analysis approach is detailed in Section III along with an illustration of the procedure on the WECC 3-machine, 9-bus system. Section IV provides empirical data to validate the results of the proposed vulnerability assessment. Insights are derived from the assessment results that appear to agree with intuition. Section V concludes the paper with final remarks.

II. Coordinated Variable Structure Switching Attacks

A. Variable Structure Systems and Sliding Mode

Variable structure systems are a type of hybrid dynamic system consisting of a family of subsystems along with one or more rules which govern the switching among them [3]. Variable structure systems exhibit both continuous and discrete states of behavior important for modeling some underlying characteristics cyber-physical systems. For example, the switching behavior represents an important analogy for discrete-time decision-making especially involving cyber-controlled power network reconfiguration as the electromechanical switches present in a power system determine the configuration or "structure" of the system at any given time. Furthermore, the dynamical systems are a convenient paradigm to model power system physics in a static switch situation. The natural scalability of variable structure systems enables the modeling of complex interdependences in power networks. This property we leverage in our work to develop a tool for vulnerability assessment of a class of coordinated switching attacks.

978-1-4673-2729-9/12/$31.00 ©2012 IEEE

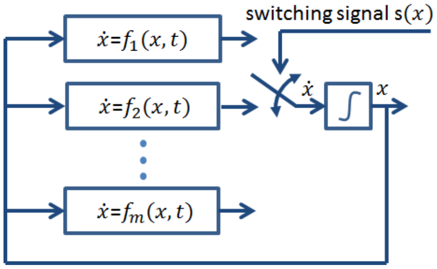

Fig. 1: General schematic of variable structure systems.

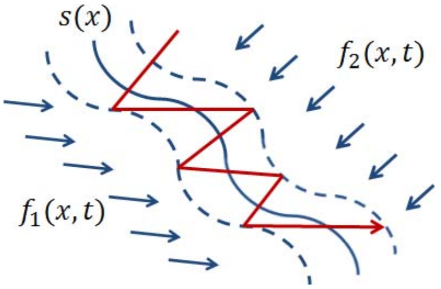

Fig. 2: Sliding surface.

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 $i \in \{1,\dots,m\}$ is the subsystem index (also known as the switch position), $x \in \mathbb{R}^{n\times 1}$ is the (time-dependent) 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*. The state vector x may represent such physical quantities as generator frequencies, phase angles or system voltages and currents. In this formulation, the position of the switch depends on the value of the switching signal $s(x)$ which is a function of system state x. For certain system parameters and selection of $s(x)$ it can be shown that Eq. 1 exhibits a form of emergent behavior known as a *sliding mode* [3], [4]. Here, the temporal trajectory of the state 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 under the conditions of Eq. 2 a state x is (locally) attracted to the surface $s(x) = 0$, and once on the sliding surface it will stay on the surface. This is because 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.

Variable structure system theory can be used to design a switching rule to achieve certain system behaviors through the selection of an appropriate sliding surface $s(x)$. Traditionally, $s(x)$ has been designed in order to stabilize the overall variable structure system [3]. Recently we have demonstrated that the theory can be applied to the modeling of power system network reconfiguration and their subsequent attack. Through judicious selection of different sliding surfaces, an attacker can construct coordinated variable structure switching attacks, which enable different sliding modes to make the system either stable or unstable [1], [2].

B. Attack Existence and Construction

Coordinated variable structure switching attacks are facilitated through cyber attack, but are designed to have a specific goal of physical disruption. This class of attacks requires that the opponent have knowledge of the local state dynamics and partial state values in order to construct and apply the attack in real-time. It also necessitates that the attacker have control over the electromechanical switching actions of one or more relay(s) and/or circuit breaker(s) of the target power system.

As power systems become increasingly cyber-enabled, cyber attack will become a possible method of accessing the state of networked electromechanical switches (unlawfully). Cyber attacks may include intrusion into the communications infrastructure that networks the switch or even into the operating system of a device that controls it. It is possible to apply these attacks to existing supervisory control and data acquisition (SCADA) systems or even centralized power system control applications via control center insiders with state knowledge and access to circuit breaker controls.

The existence of a sliding mode can be determined visually from the overlapping phase portraits [1]. Specifically, a sliding surface $s(x) = 0$ can be identified by an attacker 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 [4].

Mathematically determining the existence of a sliding mode 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 for a single switch case, we are able to provide the following theorem regarding the existence of a sliding mode.

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

$$\dot{x} = \begin{cases} A_1 x + b_1, & s(x) > 0 \\ A_2 x + b_2, & s(x) \leq 0 \end{cases} \tag{4}$$

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

$$s(x) = Cx \in \mathbb{R} \tag{5}$$

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:

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

Proof: The overall system of Eq. 4 can be represented as follows:

$$\dot{x} = \left[\frac{1+\text{sgn}(s(x))}{2}\right](A_1x+b_1)+\left[\frac{1-\text{sgn}(s(x))}{2}\right](A_2x+b_2) \tag{7}$$

for $\text{sgn}(s(x)) = 1$ for $s(x) > 0$ and $\text{sgn}(s(x)) = -1$ for $s(x) < 0$. From Eq. 2 we reinterpret that a necessary and sufficient condition for the existence of a sliding mode is:

$$s(x)\dot{s}(x) < 0. \tag{8}$$

in the neighborhood of the sliding surface. Suppose, we define a scalar positive function that is monotonically related to the distance of the state from the switching surface:

$$V = \frac{1}{2}s(x)^2. \tag{9}$$

The reader should note that V is not a Lyapunov function in the formal sense because $V = 0$ does not necessarily imply that $x = 0$. Taking the time derivative of V facilitates us to study the conditions for attraction of the state to the switching surface thus enabling it to become a sliding surface:

$$\begin{aligned} \dot{V} &= s(x)\dot{s}(x) = s(x)C\dot{x} \\ &= s(x)C\{[\frac{1+\text{sgn}(s(x))}{2}](A_1x+b_1) \\ &\quad +[\frac{1-\text{sgn}(s(x))}{2}](A_2x+b_2)\} \\ &= \frac{1}{2}(s(x)+|s(x)|)C(A_1x+b_1) \\ &\quad +\frac{1}{2}(s(x)-|s(x)|)C(A_2x+b_2) \\ &= \begin{cases} s(x)C(A_1x+b_1), & s(x) > 0 \\ s(x)C(A_2x+b_2), & s(x) < 0 \end{cases}. \end{aligned}$$

Thus, the condition of Eq. 6 is necessary and sufficient to guarantee $\dot{V} = s(x)\dot{s}(x) < 0$. ■

This theorem is useful in identifying the parameters C to construct a coordinating variable structure switching attack when power system configurations can be locally approximated as tractable low-order linear models within a local range of operating conditions. Specifically, an opponent would have to determine the vector C for a given A_i, b_i, $i \in \{1,2\}$ such that Eq. 6 holds. It can be shown that stable and unstable sliding modes exist and each one may be leveraged for a disruptive attack.

The reader should note that the linear formulation of our model in Theorem 1 is not as restrictive as it may first appear. The coordinated switching attack aims to create power system disruption through local system destabilization. We assert that in many cases our linear models are sufficient to provide this damaging information to attackers; once disruption has begun the non-local nonlinear nature can in fact aid in destabilization. We show via simulation later in this paper that this is indeed the case.

Next, we will demonstrate how variable structure system theory and coordinated variable structure switching attacks can help us identify, quantify, and prioritize the vulnerabilities in smart grid systems.

III. Vulnerability Analysis

Vulnerability assessment is a critical step in establishing a system's trade-offs and its priorities for evolution. In this paper, we employ the results from our analysis of coordinated variable structure switching attacks to better characterize this vulnerability in smart grid systems. Our approach considers a single switch in turn to identify the existence of a switching attack and quantify the breadth of possible attacks possible at that switch. Linearized system models are employed in order to keep the evaluation tractable.

A. Approach

In general, our vulnerability analysis framework can be described through the application of following steps *for each* of the k target switches, relays or circuit breakers. An *initial switch configuration* is assumed for which the power system is at equilibrium prior to application of an attack.

1) Model the power system under consideration as a variable structure system. This involves obtaining analytic expressions (typically nonlinear) to describe the system dynamics for the open and closed target switch positions. Appropriate expressions for $f_i(x,t)$, $i \in \{1,2\}$ in Eq. 3 must be assigned such that they correspond to opened/closed positions of the target switch while keeping $s = Cx$ general. The remaining $k-1$ switches are assumed to follow the initial switch configuration.
2) Apply linearization techniques to the system above in order to derive the linear representation of Eq. 4 for specific values of A_i, b_i, $i \in \{1,2\}$.
3) Employ Eq. 6 of Theorem 1 to determine the range of attack vectors C for which a sliding mode exists and the associated region of attraction includes the pre-attack equilibrium point. The later requirement is necessary as it is must be possible to first attract the system state to the sliding surface. The reader should note that in general $s = Cx$ is assumed to be a function of all system states. In the case that only partial state information is known to

apply the attack, C can be constrained to be appropriately sparse such that only known states are functions of s.

In cases where $n = 2$, it is possible to verify the analytic results visually. For unstable (stable) sliding modes the trajectory vectors of the subsystems in the neighborhood of the sliding surface will point in opposite directions toward the sliding surface and away (toward) the origin in the phase portrait.

4) Rank the degree of vulnerability for the target switch by quantifying the range of attack vectors C possible to generate the sliding mode. Unstable and stable sliding modes exist. As discussed in [1], [2], if persistent attacker switching is assumed then only unstable sliding modes need to be considered. If attacker switching occurs within a finite period of time in the order of seconds, then both stable and unstable sliding modes can be used for disruption and should be considered.

Typically, the ranked results can give one measure of the degree of vulnerability. Thus, switches that have been quantified as being highly susceptible to the coordinated variable structure switching attack (thus ranked highly) may undergo hardening including the application of additional security controls/mechanisms against cyber attacks that would grant control over the switch.

To illustrate our vulnerability assessment approach, we demonstrate how it can be employed to study the well known Western Electricity Coordinating Council (WECC) 3-machine, 9-bus system [5], see Fig. 3. We assess our results in part by comparing the ranking established using the above approach (with linearized analytical power system models) with nonlinear and practical high order models of PSCAD®.

B. Case Study: WECC 3-machine, 9-bus system

Fig. 3 presents the cyber-enabled smart power system under consideration. The physical system (shown in solid lines) is based on the 3-machine 9-bus WECC system and is comprised of typical components such as generators G_i, loads Z_i, circuit breakers (illustrated as indexed squares) and transmission lines. The cyber components correspond to communication channels (distinguished with shaded dashed lines) and measurement devices (represented as indexed hexagons). The communication channels are employed to transmit sensor data between the measurement devices and control center and also control signals from the control center to the corresponding switches and circuit breakers. Nine possible target switches are delineated in Fig. 3. In our case study we assume that the initial state of all nine switches is that of being closed and unless otherwise stated we consider the steps for vulnerability analysis for the target Switch 1.

1) Variable Structure System Modeling: Borrowing from the structure of the classical swing equations, the dynamic equations of the system can be expressed as:

$$\begin{cases} \dot{\delta}_i = \omega_i - \omega_s \\ \dot{\omega}_i = \frac{1}{M_i}[P_{mi} - \sum_{k=1}^{3} E_i E_k |Y_{ik}| \cos(\delta_i - \delta_k - \angle Y_{ik})] \end{cases} . \tag{10}$$

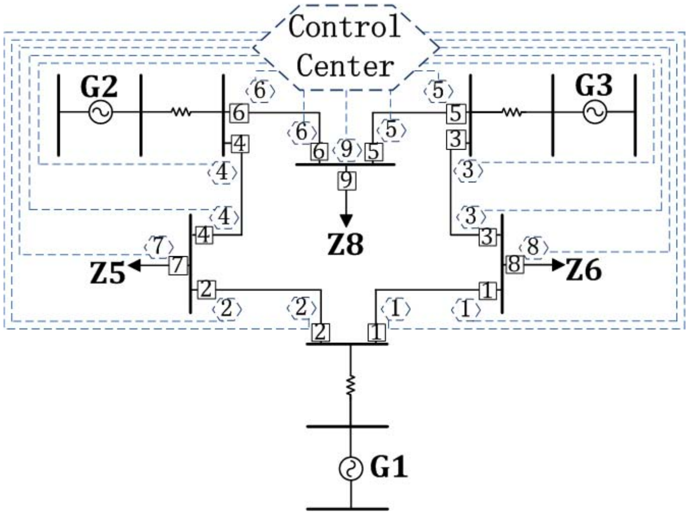

Fig. 3: Western Electricity Coordinating Council (WECC) 3-machine, 9-bus system.

where δ_i and ω_i are the rotor angle and rotor speed of Generator G_i, $i = \{1, 2, 3\}$, respectively, M_i is the moment of inertia of Generator G_i, E_i is the constant internal voltage, P_{mi} is the mechanical power, and Y_{ik} is the Kron reduced admittance matrix for the network. The parameters of the system are detailed in Table I. Using this model, we represent the WECC network as a variable structure system.

TABLE I: WECC System Parameters.

Name	Value
ω_s	120π rad/s
H_1	10 s
H_2	3.01 s
H_3	6.4 s
E_1	1.1426 pu
E_2	1.2164 pu
E_3	1.2196 pu
P_{m1}	2.0531 pu
P_{m2}	0.6860 pu
P_{m3}	1.6340 pu
X_{d1}	0.08 pu
X_{d2}	0.18 pu
X_{d3}	0.12 pu
X_{line}	0.3 pu

Given there are three generators, we define the state of the system with vector $x = [\delta_1, \delta_2, \delta_3, \omega_1, \omega_2, \omega_3]^T \in \mathbb{R}^{6\times1}$. From Eq. 10 and Table I, when all switches are closed, the system dynamic equations can be described as:

$$\begin{cases} \dot{\delta}_1 &= \omega_1 - 120\pi \\ \dot{\delta}_2 &= \omega_2 - 120\pi \\ \dot{\delta}_3 &= \omega_3 - 120\pi \\ \dot{\omega}_1 &= -1.63 - 10.6\cos\left(\delta_1 - \delta_3 - 1.41\right) \\ & \quad -13.2\cos\left(\delta_1 - \delta_2 - 1.38\right) \\ \dot{\omega}_2 &= 34.2 - 36.0\cos\left(\delta_2 - \delta_3 - 1.38\right) \\ & \quad -48.8\cos\left(\delta_2 - \delta_1 - 1.38\right) \\ \dot{\omega}_3 &= 34.1 - 76.5\cos\left(\delta_3 - \delta_2 - 1.38\right) \\ & \quad -83.4\cos\left(\delta_3 - \delta_1 - 1.41\right) \end{cases} . \quad (11)$$

It can also be shown that when Switch 1 is open, the system dynamic equations are given by:

$$\begin{cases} \dot{\delta}_1 &= \omega_1 - 120\pi \\ \dot{\delta}_2 &= \omega_2 - 120\pi \\ \dot{\delta}_3 &= \omega_3 - 120\pi \\ \dot{\omega}_1 &= 0.04 - 4.81\cos\left(\delta_1 - \delta_3 - 1.34\right) \\ & \quad -11.8\cos\left(\delta_1 - \delta_2 - 1.42\right) \\ \dot{\omega}_2 &= 33.4 - 38.9\cos\left(\delta_2 - \delta_3 - 1.33\right) \\ & \quad -43.6\cos\left(\delta_2 - \delta_1 - 1.42\right) \\ \dot{\omega}_3 &= 22.6 - 82.8\cos\left(\delta_3 - \delta_2 - 1.33\right) \\ & \quad -37.8\cos\left(\delta_3 - \delta_1 - 1.34\right) \end{cases} . \quad (12)$$

2) Linearization: Using small angle approximation we linearize Eqs. 11 and 12 to give

$$\dot{x} = \begin{cases} A_0 x + b_0, & s(x) > 0 \text{ (Switch 1 closed)} \\ A_1 x + b_1, & s(x) < 0 \text{ (Switch 1 open)} \end{cases} , \quad (13)$$

where

$$A_0 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -23.5 & 13.0 & 10.5 & 0 & 0 & 0 \\ 47.9 & -83.3 & 35.3 & 0 & 0 & 0 \\ 82.3 & 75.1 & -157.0 & 0 & 0 & 0 \end{pmatrix}, \quad b_0 = \begin{pmatrix} -120\pi \\ -120\pi \\ -120\pi \\ -5.83 \\ 18.3 \\ 5.89 \end{pmatrix}$$

and

$$A_1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -16.4 & 11.7 & 4.68 & 0 & 0 & 0 \\ 43.1 & -81.0 & 37.8 & 0 & 0 & 0 \\ 36.8 & 80.4 & -117.0 & 0 & 0 & 0 \end{pmatrix}, \quad b_1 = \begin{pmatrix} -120\pi \\ -120\pi \\ -120\pi \\ -2.86 \\ 17.6 \\ -5.81 \end{pmatrix}.$$

3) Application of the Existence Theorem: Assuming $s = Cx = c_1\delta_1 + c_2\delta_2 + c_3\delta_3 + c_4\omega_1 + c_5\omega_2 + c_6\omega_3$, the existence conditions for a sliding mode can be rewritten as:

$$\begin{cases} \begin{cases} CA_0 x + b_0 < 0 \\ Cx > 0 \end{cases} \\ \begin{cases} CA_1 x + b_1 > 0 \\ Cx < 0 \end{cases} \end{cases} . \quad (14)$$

Typically, the attacker may only have partial state information. In this example, we assume the attacker has access to the local state information of a particular generator, say G_1. This adds a sparsity constraint on C such that $C = [c_1\ 0\ 0\ c_4\ 0\ 0]$ making $s = c_1\delta_1 + c_4\omega_1$. The unstable attraction region for the sliding mode to exist can be described analytically in Eq. 15:

$$\begin{cases} \begin{cases} -c_1(120\pi - \omega_1) - c_4(23.5\delta_1 + 5.83) < 0 \\ c_1\delta_1 + c_4\omega_1 > 0 \end{cases} \\ \begin{cases} -c_1(120\pi - \omega_1) - c_4(16.4\omega_1 + 2.86) > 0 \\ c_1\delta_1 + c_4\omega_1 < 0 \end{cases} \end{cases} . \quad (15)$$

Therefore, as long as for a particular parameter set (c_1, c_4) Eq. 15 results in the equilibrium point of the system (for the initial switch configuration) being in the region of attraction, there exists an opportunity for an opponent to apply a switching attack and drive the state to the sliding surface. Figs. 4, 5 and 6 illustrate the ranges of (c_1, c_4) such that the pre-attack equilibrium point lies in the region of attraction.

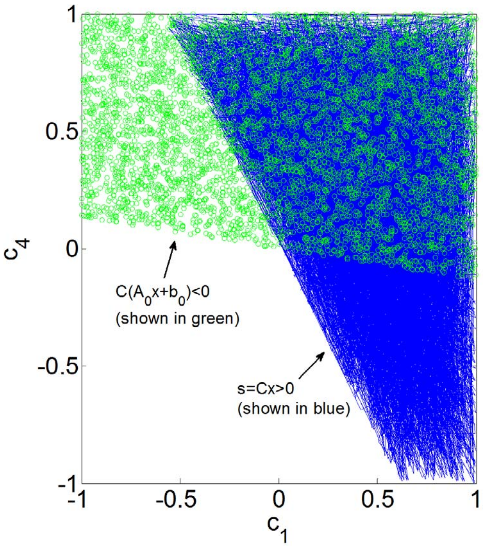

Fig. 4: Range of attack vector (c_1, c_4) for $s > 0$. $C(A_0x + b_0) < 0$ and $s = Cx > 0$ are shown in green and blue, respectively.

In our example, it is possible to also visually find the range of sliding mode parameters by using the phase portrait graphs to verify the analytical results. Recall that to have an unstable sliding mode exist, the trajectory vectors of the subsystems need to point toward the sliding surface in opposite directions and away from the origin. Originally, the system is stable as shown in Fig. 7 which provides the phase portrait when Switch 1 is closed. When Switch 1 opened, the system is still stable as seen in Fig. 8. The overlapping phase portrait for both switch configurations is shown in Fig. 9. An unstable sliding mode is identified for $s = 0.0095\delta_1 - \omega_1$ (i.e., $c_1 = 0.0095$ and $c_4 = -1$) by visual inspection.

4) Ranking: To assess the relative vulnerabilities at the different switches of Fig. 3, Steps 1) to 3) are repeated for the remaining eight target switches. Table II summarizes the results. Without loss of generality and to avoid scale ambiguity, $c_4 = -1$ is set leaving the task to be that of identifying the range of c_1 such that the equilibrium point occurs in attraction region of the sliding mode $s = c_1\delta_1 - \omega_1$.

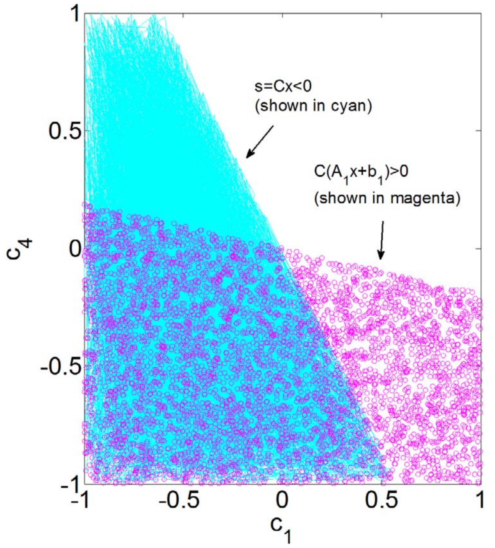

Fig. 5: Range of attack vector (c_1, c_4) for $s < 0$. $C(A_1x + b_1) > 0$ and $s = Cx < 0$ are shown in magenta and cyan, respectively.

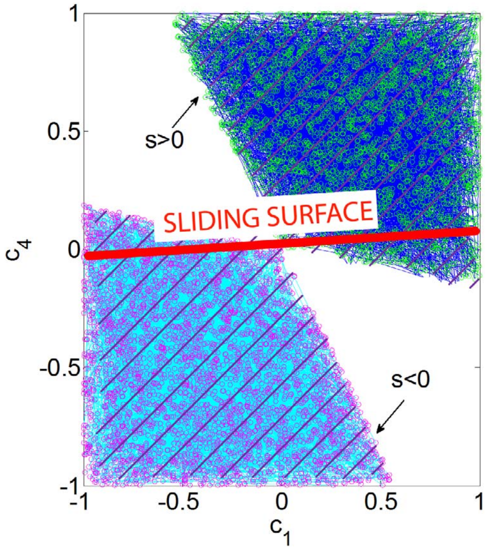

Fig. 6: Overall attack vector range (c_1, c_4). Overlapping regions of attraction are shown in shaded areas.

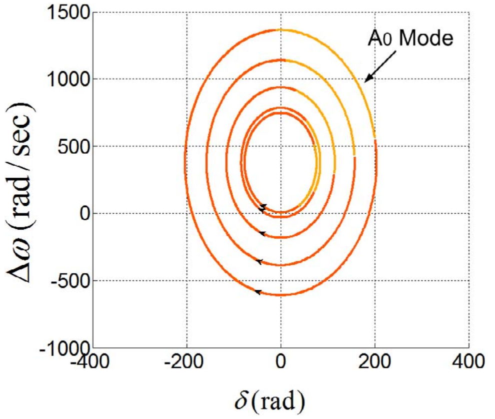

Fig. 7: Phase portrait for Switch 1 closed in Fig. 3.

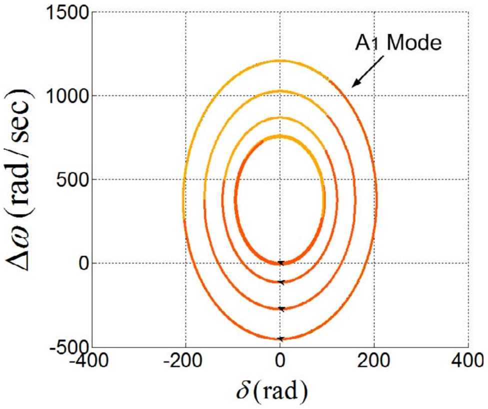

Fig. 8: Phase portrait for Switch 1 open in Fig. 3.

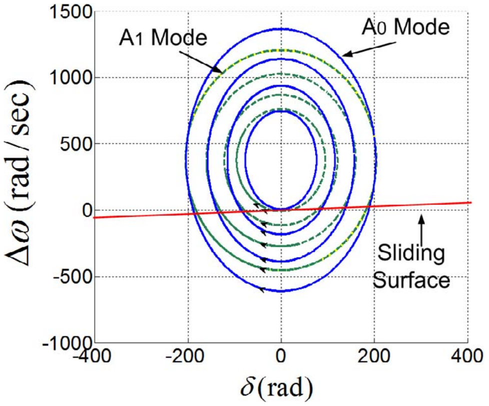

Fig. 9: Overlapping phase portraits for target Switch 1 in Fig. 3. Sliding surface $s = 0.0095\delta_1 - \omega_1$

The switches are first separated into the different classes of line switches and load switches and then ranked according to the size of these regions. Thus, the most vulnerable switch to coordinated switching is the one with the largest range of C (equivalent to the range of c_1 in this example). Results are presented in the first two columns of Table III.

TABLE II: Attack vector ranges derived from Theorem 1; $c_4 = -1$ to avoid scale ambiguity.

Switch	Sliding Mode Range for c_1
1	(-1, 0.575)
2	(-1, 0.550)
3	(-1, 0.598)
4	(-1, 0.600)
5	(-1, 0.592)
6	(-1, 0.595)
7	(-1, 0.560)
8	(-1, 0.575)
9	(-1, 0.590)

TABLE III: Target Switch Ranking for System of Fig. 3.

Linearized Results		PSCAD® Results	
Switch Type		Switch Type	
Line	Load	Line	Load
4	9	4	8
3	8	3	9
6	7	6	7
5		5	
1		2	
2		1	

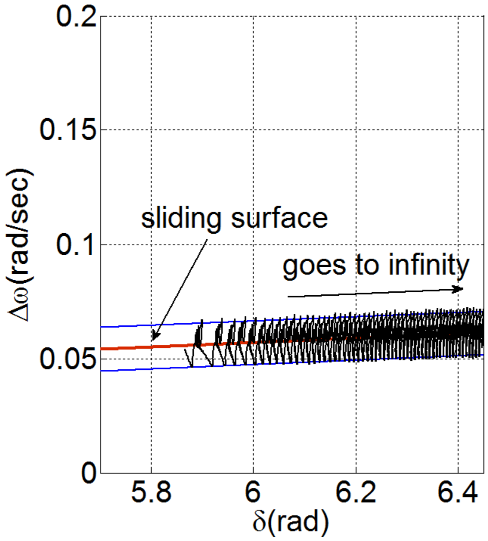

Fig. 10: MATLAB/Simulink phase portrait for $s = 0.0095\delta_1 - \omega_1$.

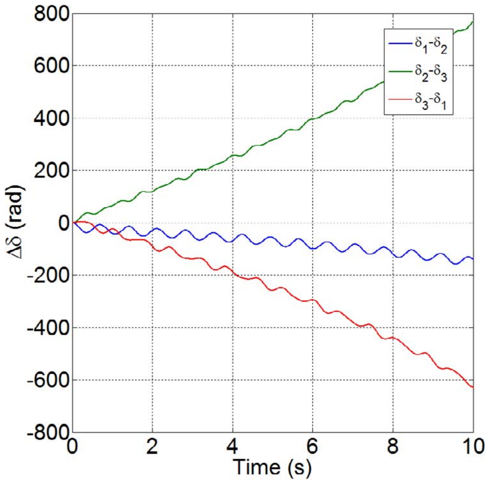

Fig. 11: System phase for unstable sliding mode $s = 0.0095\delta_1 - \omega_1$.

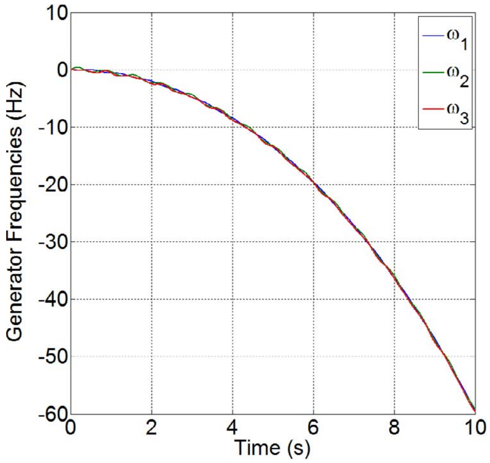

Fig. 12: Generator frequencies for unstable sliding mode $s = 0.0095\delta_1 - \omega_1$. All three generators are unstable.

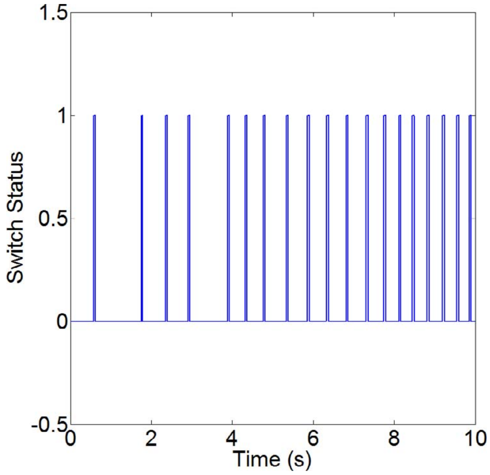

Fig. 13: Switch status for unstable sliding mode $s = 0.0095\delta_1 - \omega_1$.

IV. Simulation and Discussion

Table III provides a ranking of the target switches according to our vulnerability analysis approach. However, to evaluate the quality of our results and hence the validity of our vulnerability analysis philosophy we must consider two issues. First, our approach leverages Theorem 1 and is therefore based, in part, on linearized models of the system. Thus a question arises as to the accuracy of the ranking results due to model approximation. Second, the figure of merit that we use for ranking is the area of the associated region of attraction of the sliding mode. Our intuition is that this provides a measure of the ease at which an attack can be applied and hence a degree of vulnerability, but one may ask what useful information does it tell us about the system?

A. Comparison to Higher Order Models

To validate the ranking of Table III using the linearized models, we conduct MATLAB/Simulink simulations of the nonlinear swing equation model in part given by Eqs. 11

and 12 and high order PSCAD® simulations. Fig. 10 shows the phase portrait of the system when a switching attack is applied for $s = 0.0095\delta_1 - \omega_1$ (previously identified as an unstable sliding mode from the linear models). As observed, even with nonlinear swing-equation based models the system state is attracted to the surface and travels away from the origin causing instability in G_1 and overall system disruption.

PSCAD® results for the WECC system and attack $s = 0.0095\delta_1 - \omega_1$ are presented in Figs.11, 12 and 13. Here, the base MVA of the system is 100, the system normal frequency is 60 Hz and the generator parameters are shown in Table IV. We see that the system becomes unstable at 1.593 s along with the selected unstable sliding mode. All three generator frequencies for unstable sliding mode are shown in Fig. 12, and switch status is shown in Fig. 13.

TABLE IV: Generator parameters for PSCAD® simulation of WECC system.

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

TABLE V: Attack vector ranges determined by brute force PSCAD® simulation; $c_4 = -1$ to avoid scale ambiguity.

Switch	Sliding Mode Range for c_1
1	(0.001, 0.01)
2	(0.01, 0.02)
3	(0.07, 0.095)
4	(0.07, 0.1)
5	(0.07, 0.085)
6	(0.07, 0.09)
7	(0.001, 0.01)
8	(0.001, 0.02)
9	(0.001, 0.015)

In Table III, the ranking of the switches via brute force PSCAD® simulation to determine c_1 ranges is compared to the linearized models. Strong correlation is shown. For both line and load switches, except for a deviation of a single switch, the ordering is the same.

B. Ranking and Intuition

Table III provides insight into vulnerabilities present in the WECC system of Fig. 3. The ranking of the switches we assert is consistent with intuition. We make the following observations useful as rules of thumb for vulnerability assessment smart grid system security:

1) Transmission line switches are typically more susceptible to coordinated switching attack than load switches. We argue that switching at the transmission line causes disruptions at critical internal components of the network causing overall system instability in contrast to switches at the edges of the power grid.
2) Transmission line switches in close proximity to larger generators and loads tend to be more vulnerable to coordinated switching. Naturally, if larger components are switched in an out, greater disruption arises enabling disruption.
3) Load switches at larger loads are more vulnerable.
4) Switches associated with longer transmission lines are more vulnerable to coordinated switching. Longer transmission lines imply less coupling between associated system components. If switching is applied at an already weak position of the network, disruption of phase and frequency is more likely.

V. Final Remarks

In this paper, we present a vulnerability analysis framework for coordinated variable structure switching attacks. For tractability and ease of computation our approach makes use of linear models of power system dynamics for ranking the degree of vulnerability of the various switches. MATLAB/Simulink simulations of nonlinear swing equation-based models and PSCAD® simulations of the 3-generator, 9-bus WECC system help validate the overall approach. Furthermore, insights derived from our vulnerability analysis appear to agree with intuition. Future work focuses on developing complementary measures to rank system vulnerability to cyber-physical reconfiguration attacks.

Acknowledgment

Funding was provided through NHARP Project 000512-0111-2009 and NSF grants EECS-1028246 and EEC-1062603.

References

[1] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. Butler-Purry, "Switched system models for coordinated cyber-physical attack construction and simulation," in *First IEEE International Workshop on Smart Grid Modeling and Simulation*, Brussels, Belgium, October 17 2011.

[2] ——, "A class of cyber-physical switching attacks for power system disruption," in *7th ACM Annual Cyber Security and Information Intelligence Research Workshop*, Oak Ridge National Laboratory. Oak Ridge, Tennessee: ACM International Conference Proceedings Series, October 12-14 2011.

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

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

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