Progressive Switching Attacks for Instigating Cascading Failures in Smart Grid

Shan Liu*, Bo Chen*, Deepa Kundur†, Takis Zourntos*‡, Karen Butler-Purry*

*Department of Electrical and Computer Engineering, Texas A&M University
{liu2712, boboychn, takis, klbutler}@tamu.edu
†Department of Electrical and Computer Engineering, University of Toronto
dkundur@comm.utoronto.ca
‡Ontario College of Art and Design University
takis.zourntos@gmail.com

***Abstract*—In this paper we present a progressive strategy for applying a multi-switch cyber-physical attack on emerging smart grid systems. In contrast to a single switch attack, recently studied, we demonstrate how the additional degrees of freedom available to an opponent can be used to induce cascading failures throughout a power system in a stealthy way. A framework based on variable structure system theory is presented in which targeted attacks can be constructed. Attack execution is simulated on the New England 10-generator 39-bus test system using DSA*Tools*™ to demonstrate the potential of the approach to achieve high impact disruption.**

***Index Terms*—Smart grid modeling, sliding mode, coordinated variable structure switching attacks.**

I. Introduction

There has been recent emphasis on studying the cyber-physical interactions of smart grid systems in the context of security assessment [1]–[4]. Recently, a class of cyber-physical *coordinated variable structure switching* attacks have been proposed in which a power system, with a corrupted circuit breaker, is modeled as a variable structure system. From this model, a switching sequence is deduced using sliding mode theory such that instability of a target synchronous generator can be induced by an opponent through application of that switching sequence to the corrupted breaker [5]–[7]. In this paper, we aim to provide a more comprehensive assessment of the security posture of a smart grid system by considering additional degrees of freedom available to an opponent for stealthy attack. Specifically, we focus on exploring a non-trivial extension to the coordinated switching attack, which makes use of multiple breaker corruptions and collusion to create cascading failures within multiple targets of the system for wider-scale disruption.

II. Distributed Multi-Switch Attacks

A. Variable Structure Systems

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

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

For certain forms of dynamics and selections of $s(x,t)$, it can be shown that the overall switched system exhibits *sliding mode* behavior. In the sliding mode, while switching persists, the state of the overall switched system is attracted to and stays on the $s(x,t) = 0$ manifold termed a *sliding surface* of the variable structure system. Existence of the sliding mode (i.e., attraction to and invariance on) is guaranteed if and only if $s\dot{s} < 0$ and typically represents a local results in state-space.

Recently, the authors have modeled smart grid transmission systems under reconfiguration (e.g., circuit breaker switching) as variable structure systems. We have demonstrated how transient *instability* of a target synchronous generator can be induced by an opponent who has corrupted a circuit breaker and switches it open or closed depending on the sign of an appropriately defined $s(x,t)$ [5], [6]. The system state x represents the phase and frequency of the target generator and the switching has the effect of disrupting both the generator frequency and phase desynchronizing it.

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

B. Distributed Switching for Attack

We consider a power system consisting of $M > 0$ circuit breakers. We assume that an opponent (or a colluding collective of opponents) has control over $0 < m \leq M$ breakers through, say, corruption of breaker control signals via attacks

978-1-4799-1303-9/13/$31.00 ©2013 IEEE

on the associated communication network, as discussed in [5], [6]. The objective of the opponent is to disrupt power system operation through transient destabilization of one or more target synchronous generators denoted $\{G_t\}$, $t = 1, 2, \ldots, T$ assuming that the opponent has some knowledge of the target generator states. Such destabilization will cause generator protection relays to trip taking the corresponding generators off-line. We say that the attack is collusive as the corrupted breakers must work together to achieve the overall attack.

Strategies that involve *simultaneous* switching of corrupted breakers are possible to destabilize the system. However, in this work we consider the situation in which the strategy of the opponent is to start coordinated switching of the corrupted breakers in tandem such that Switch 1 begins at time t_1, Switch 2 at t_2 and so on until finally Switch m begins at t_m where $t_1 < t_2 < \cdots < t_m$; all switches continue to switch persistently until the attack is completed. We assert that such progressive switching enables greater control over the timing of destabilization to synchronize the attack with other assaults.

III. Progressive Switching

The multi-switch investigation necessitates that the switching signal of Section II-A be a *switching vector* $s(x,t) \in \mathbb{R}^{m\times 1}$; the sign of each element of $s(x,t)$ dictates when to open or close a specific breaker for attack. Existence of a sliding mode at $s(x,t) = [s_1\ s_2\ \cdots\ s_m]^T = [0\ 0\ \cdots\ 0]^T = \mathbf{0}$ is guaranteed if [8]:

$$s^T \dot{s} < 0. \tag{2}$$

We say that an *individual* sliding mode for $s_i = 0$ exists if and only if it can be shown that:

$$s_i \dot{s}_i < 0. \tag{3}$$

Thus, the sliding surface $s = \mathbf{0}$ is at the intersection of all individual sliding surfaces $s_i = 0$ for $i = 1, 2, \ldots, m$.

For simplicity we first demonstrate the progressive switching idea on an example system and focus on a two-switch situation in which $s = [s_1\ s_2]^T$; the general m-switch case would represent a natural extension. We consider the following fundamental third-order canonical form realization of a linear time-invariant system:

$$\dot{x}(t) = \underbrace{\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}}_{x} + \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}}_{B} \underbrace{\begin{bmatrix} u_1 \\ u_2 \end{bmatrix}}_{u}. \tag{4}$$

The switching vector is represented as:

$$s = [s_1\ s_2]^T = Cx = \begin{bmatrix} c_1^1 & c_2^1 & c_3^1 \\ c_1^2 & c_2^2 & c_3^2 \end{bmatrix} [x_1\ x_2\ x_3]^T, \tag{5}$$

where $C^i = [c_1^i\ c_2^i\ c_3^i]$ is the coefficient vector of s_i, $i = 1, 2$.

For this example, we model the effects of switching using a switched input $u = [u_1\ u_2]^T$. Here u will naturally be s-dependent to represent the change in dynamics due to switching. However, for our canonical example, we also allow u to contain a linear state-dependent feedback component to guarantee that the system of Eq. (4) indeed has an appropriate sliding mode for a given set of switching surfaces. The reader should note that in an actual power system attack scenario addressed in Section IV, the action of an opponent would result only in the first s-dependent component.

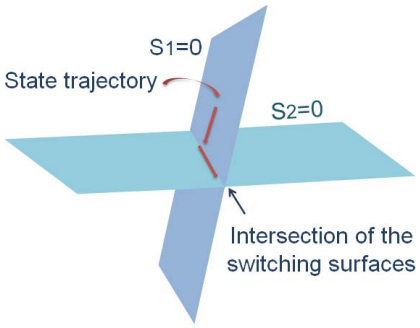


Fig. 1: State trajectory for progressive switching.

Progressive switching works as follows. Suppose that the individual sliding surface $s_1 = 0$ exists and is *stable*; that is, Switch 1 can be switched according to the sign of s_1 and the state trajectory will be attracted to the $s_1 = 0$ manifold and converge to an equilibrium position. Suppose also that the intersection of surfaces $s_1 = 0$ and $s_2 = 0$ denoted $s = \mathbf{0}$ is also a valid sliding surface and represents an *unstable* sliding mode. Here, Switches 1 and 2 are simultaneously switched according to the signs of s_1 and s_2, respectively and the state converges to the $s = \mathbf{0}$ surface at which point it moves to infinity destabilizing the system.

The progressive switching strategy requires first that switching of Switch 1 begin at some t_1 and then simultaneous switching of Switches 1 and 2 be applied at some $t_2 > t_1$ to first attract the system state to $s_1 = 0$ in a stable (and hence stealthy) way and then attract it to $s = \mathbf{0}$ at t_2 such that it moves along the sliding surface to infinity; figure 1 illustrates. For a state to be attracted to a sliding mode, it must be within the region of attraction as given by assessing the conditions for Eq. (2) and (3). Thus, t_1 and t_2 must be appropriately selected such that the state x is within an appropriate region of attraction in state space. We consider the progressive switching attack to have the following three stages.

Stage 1: The system state x is driven to the $s_1 = 0$ sliding surface. We make use of our canonical system of Eq. (4) and illustrate this behavior by assigning an input u as follows:

$$u = -(C^1 B)^{-1}(C^1 A x) - (C^1 B)^{-1} \cdot \mathrm{sgn}(s_1), \tag{6}$$

that guarantees the existence of the $s_1 = 0$ sliding surface: $s_1 \dot{s}_1 = s_1 C^1 \dot{x} = C^1(Ax + Bu) = -s_1 \cdot \mathrm{sgn}(s_1) = -|s_1| < 0$ to obtain the following overall Stage 1 dynamics:

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = \frac{1}{(c_3^1)^2 + (c_2^1)^2} \Big[c_2^1 c_3^1 \alpha_1 x_1 + c_2^1 (c_1^1 + c_3^1 \alpha_2) x_2 + ((c_3^1)^2 \\ \qquad + 2(c_2^1)^2 + c_2^1 c_3^1 \alpha_3) x_3 - c_2^1 \cdot \mathrm{sgn}(s_1) \Big] \\ \dot{x}_3 = \frac{1}{(c_3^1)^2 + (c_2^1)^2} \Big[((c_3^1)^2 \alpha_1 + (c_2^1)^2 \alpha_1) x_1 + (2(c_3^1)^2 \alpha_2 + (c_2^1)^2 \alpha_2 \\ \qquad + c_3^1 c_1^1) x_2 + (2(c_3^1)^2 \alpha_3 + (c_2^1)^2 \alpha_3 + c_3^1 c_2^1) x_3 - c_3^1 \cdot \mathrm{sgn}(s_1) \Big] \end{cases} \tag{7}$$

Stage 2: The system state x enters and remains on the $s_1 = 0$ sliding surface. Here, the method of equivalent control can be employed to describe the effective dynamics in the presence of Switch 1 switching. We set $\dot{s}_1 = C^1\dot{x} = C^1(Ax+Bu) = 0$ to give $u_{eq} = -(C^1B)^{-1}(C^1Ax)$. Substituting this into Eq. (4) gives overall Stage 2 dynamics:

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = \dfrac{-c_2^1c_3^1\alpha_1x_1 - c_2^1(c_1^1 + c_3^1\alpha_2)x_2 + c_3^1(c_3^1 - c_2^1\alpha_3)x_3}{(c_3^1)^2 + (c_2^1)^2} \\ \dot{x}_3 = \dfrac{(c_2^1)^2\alpha_1x_1 + ((c_2^1)^2\alpha_2 - c_3^1c_1^1)x_2 + c_2^1(c_2^1\alpha_3 - c_3^1)x_3}{(c_3^1)^2 + (c_2^1)^2} \end{cases}. \quad (8)$$

Stage 3: The system state x is driven to the $s = \mathbf{0}$ sliding surface at the intersection of $s_1 = 0$ and $s_2 = 0$. To illustrate this behavior, we assign u to guarantee $s^T\dot{s} < 0$. Consider $u = -(CB)^{-1}(CAx) - (CB)^{-1}\cdot\text{sgn}(s)$ which implies $s^T\dot{s} = -|s| < 0$, to provide an overall dynamics:

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = \dfrac{(c_3^2c_1^1 - c_3^1c_1^2)x_2 + c_3^2\cdot\text{sgn}(s_1) - c_3^1\cdot\text{sgn}(s_2)}{c_3^1c_2^2 - c_2^1c_3^2} \\ \dot{x}_3 = \dfrac{(c_2^1c_1^2 - c_2^2c_1^1)x_2 - c_2^2\cdot\text{sgn}(s_1) + c_2^1\cdot\text{sgn}(s_2)}{c_3^1c_2^2 - c_2^1c_3^2} \end{cases}. \quad (9)$$

1) Numerical Illustration: We consider $\alpha_1 = -1$, $\alpha_2 = -2$ and $\alpha_3 = -3$ which corresponds to a stable canonical system, which we demonstrate can be destabilized using our switching control framework. The two switching surfaces are selected as:

$$C = \begin{bmatrix} 1 & 2 & -1 \\ -2 & -1 & -1 \end{bmatrix}. \quad (10)$$

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

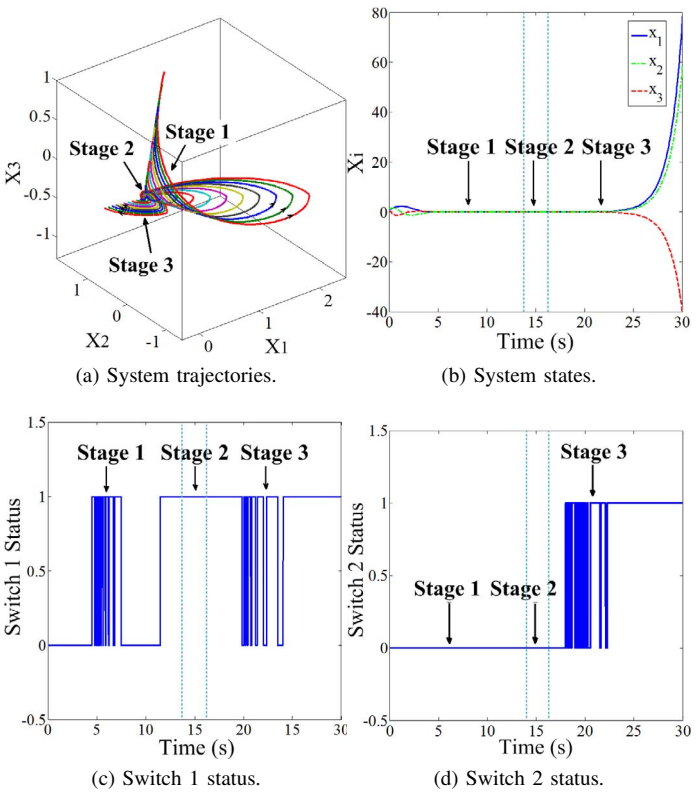
IV. Application to Test System

We apply the progressive switching principles to the New England 10-machine, 39-bus system of Fig. 3 employing DSA*Tools*^{TM}. The overall system can be modeled via the swing equations with the following dynamics:

$$\begin{cases} \dot{\delta}_i = \omega_i - \omega_s \\ \dot{\omega}_i = \dfrac{1}{M_i}[P_{mi} - \Sigma_{k=1}^{10}E_iE_k|Y_{ik}|\cos(\delta_i - \delta_k - \angle Y_{ik})] \end{cases}, \quad (11)$$

where δ_i, ω_i, M_i, P_{mi} and E_i are the phase angle, frequency (with nominal frequency being 60 Hz), moment of inertia, mechanical power and terminal voltage of the ith generator. Y_{ik} is the Kron-reduced equivalent admittance between the ith and kth generators. Typical parameter values for the New England system are assumed. The jth (corrupted) breaker in the system is assumed to target Generator t and incorporate the following switching signal with coefficients c_{j_1} and c_{j_2}:

$$s_j = c_{j_1}\delta_t + c_{j_2}\omega_t. \quad (12)$$



(a) System trajectories. (b) System states. (c) Switch 1 status. (d) Switch 2 status.

Fig. 2: System trajectories and states for progressive switching.

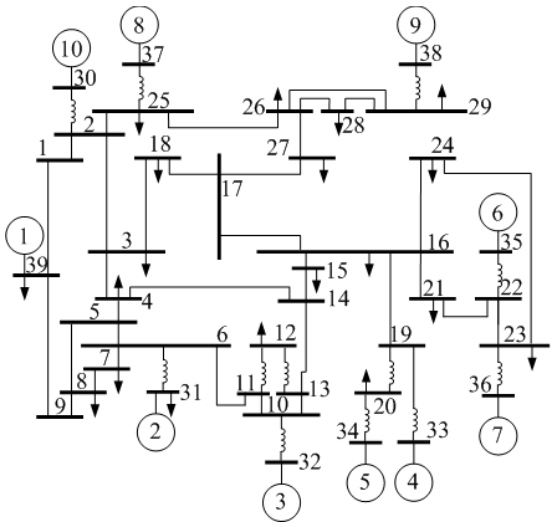


Fig. 3: New England 10-machine, 39-bus Power System.

The opponent is assumed to have access to δ_t and ω_t through vulnerable sensors or via state estimation as discussed [9].

The overall system is assumed to be initially at a stable equilibrium point. The task of an opponent in control of the jth corrupted breaker would be to select the parameters c_{j_1} and c_{j_2} judiciously to induce instability in Generator t; this can be conducted empirically or analytically [9], [10] using the model of Eq. 11. Execution of the attack on Generator t requires knowledge of δ_t and ω_t. The opponent-corrupted switches are operated such that when switching is applied,

TABLE I: Cascading failure sequence for test system.

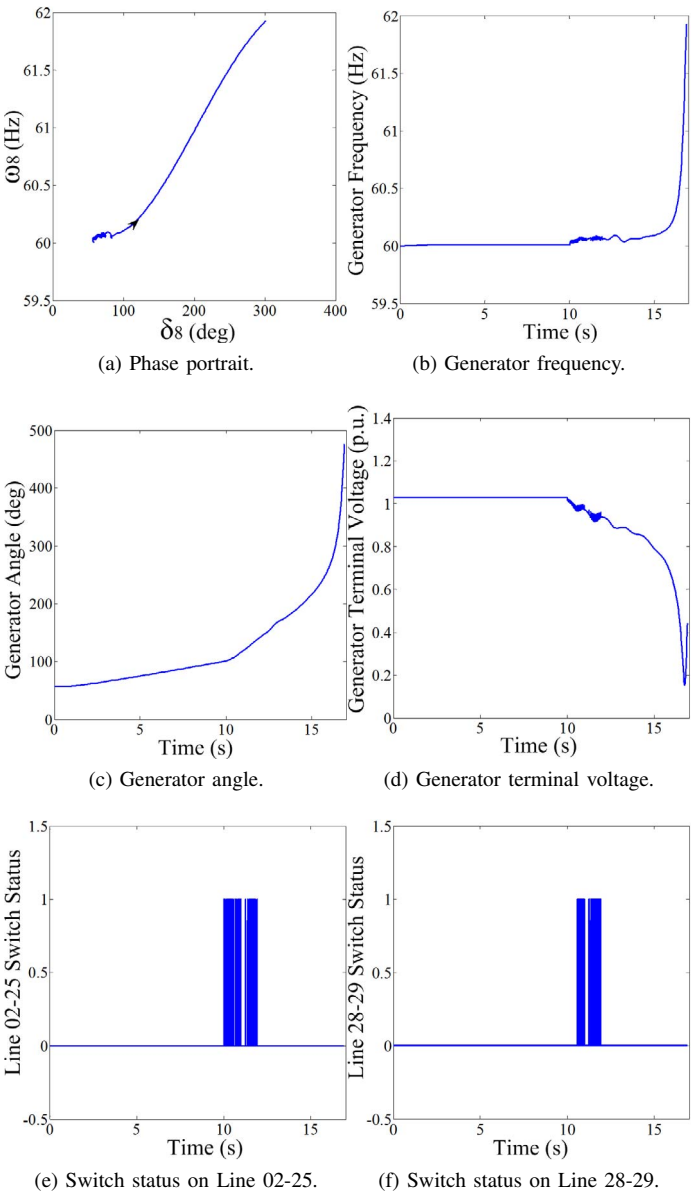
Time (s)	Event Recording
0-10	Normal operating
10-11	Switching attacks implemented on Generator 9
11-16.38	Generator 9 loses synchronous, and is tripped by over-frequency relay at 16.38 second
16.38-20	System is operating at 59.8 HZ after tripping Generator 9
20-21	Switching attacks implemented on Generator 8
21-26.9	Generator 8 loses synchronous, and is tripped by over-frequency relay at 26.9 second
26.9-31.3	Generator 5 loses synchronous, and is tripped by over-frequency relay at 31.3 seccond
31.3-50	Line 21-22 active power increases, and is tripped by overload transmission line protection relay at 50 second
50-50.74	Generator 7 loses synchronous, and is tripped by over-frequency relay at 50.74 second
50.74-50.78	Generator 6 loses synchronous, and is tripped by over-frequency relay at 50.78 second
50.78-50.82	Bus 3 frequency decreases, the load on Bus 3 is tripped by UFLS at 50.82 second
50.82-51.03	Bus 16 frequency decreases, the load on Bus 16 is tripped by UFLS aT 51.03 second
51.03-51.15	Generator 4 loses synchronous, and is tripped by over-frequency relay at 51.15 second
51.15-51.26	Bus 15 and 18 frequencies decrease, the loads on Bus 15 and 18 are tripped by UFLS at 51.26 second
51.26-51.28	Generator 2 loses synchronous, and is tripped by over-frequency relay at 51.28 second
51.28-51.29	Generator 3 loses synchronous, and is tripped by over-frequency relay at 51.29 second
51.29-51.47	Bus 7 frequency decreases, the load on Bus 7 is tripped by UFLS at 51.47 second
51.47-53.66	Bus 25, 26 and 28 frequencies decrease, the loads on Bus 25, 26 and 28 are tripped by UFLS at 53.66 second
53.66-62.1	Generator 1 loses synchronous, and is tripped by over-frequency relay at 62.1 second
62.1-80	Generator 10 provides power to the remaining loads under fairly low frequency and voltage, which can not meet the normal power requirements.

Switch i opens if $s_i < 0$ and closes if $s_i \geq 0$ for $i = 1, 2$. We consider the progressive multi-switch attack approach as well as consider how the multi-switch framework can be leveraged by an opponent to initiate cascading failures within the system.

The target switches are selected based on the conclusion of [7] which provided guidelines on selection of generators and through power flow analysis. Theoretically, any two switches of the system can be employed to perform attack, as long as the measurement information is available. But the cascading effect will perform successfully only when the combination of switches sequence selected properly.

A. Progressive Switching

We consider corruption of breakers on Line 02-25 (Switch 1) and Line 28-29 (Switch 2) with target Generator 8. Although it can be shown that an individual sliding mode does not exist for Switch 2, it does for Switch 1. Thus we employ progressive switching starting with Switch 1. We assume an opponent employs $s_1 = -7\delta_8 + \omega_8$ and $s_2 = -5\delta_8 + \omega_8$ and Switch 1 begins at 10.0 s and Switch 2 joins at 10.5 s appropriately coordinating with Switch 1. Fig. 4 demonstrates the effectiveness of the approach for system destabilization.



(a) Phase portrait. (b) Generator frequency.

(c) Generator angle. (d) Generator terminal voltage.

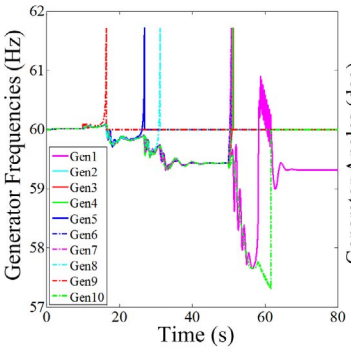
(e) Switch status on Line 02-25. (f) Switch status on Line 28-29.

Fig. 4: System trajectories and states for a coordinated progressive multi-switch attack.

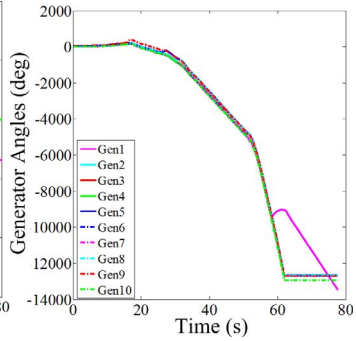
B. Cascading Failure

We aim to address cascading failures dynamically, in the context of our proposed multi-switch analysis framework. We consider how corruption of a subset of breakers within the New England 10-machine test system of Fig 3 can be exploited to strain the system sufficiently to result in a sequence of trips and failures resulting in the loss of a substantial amount of load. We model the presence of protection as detailed in [11] and [12]. The overload protection on transmission lines is assumed to trigger when the active power over a line is more than 800 MW for 5 seconds.

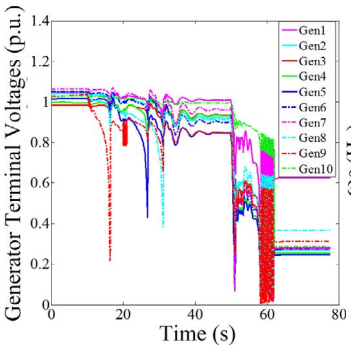
We consider the corruption of Line 26-28 (Switch 1), Line 28-29 (Switch 2). In the first phase of the attack, an opponent targets Generator 9 employing $s_1 = -5\delta_9 + \omega_9$ and $s_2 = -8\delta_9 + \omega_9$. After Generator 9 is tripped by protection devices, a



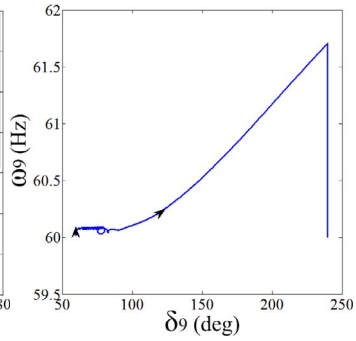
(a) Generator frequencies.



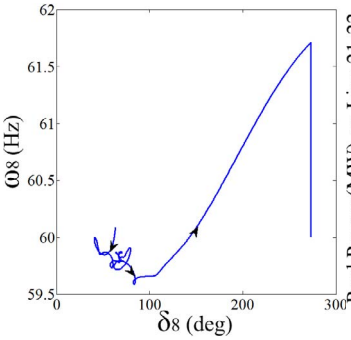
(b) Generator angles.



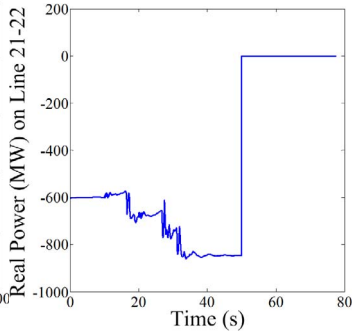
(c) Generator terminal voltages.



(d) Phase portrait of Generator 9.



(e) Phase portrait of Generator 8.



(f) Real power (MW) on line 21-22 for overload protective relay.

Fig. 5: Trajectories and states for cascading failure case.

second phase is applied. Here, the opponent targets Generator 8 employing $s_1 = -2\delta_8 + \omega_8$ and $s_2 = -8\delta_8 + \omega_8$. The attack results in a series of critical component trips and a resulting domino effect presented in Table I and Fig. 5. Eventually, the entire system works under power provided by Generator 10 only, which is clearly sufficient to meet the normal demand requirements.

An opponent only needs to apply switching from 10 s to 11 s and 20 s to 21 s to have devastating effects within 80 s even with the use of protection. This impact is significant in contrast to use of a single switch and demonstrates the potential of coordinated variable structure switching attacks for large-scale system disruption.

V. Final Remarks

We have presented a multi-switch approach to instigate significant power system disruption using variable structure system theory. We employ a modeling framework that elegantly merges cyber-physical aspects of operation. Our research represents a departure from prior work by formulating the smart grid security problem within dynamical system contexts that are mathematically representable and relate attack impacts to disturbances on quantifiable power system performance metrics. In larger systems that are more robust, we content that a greater number of switches must be employed for a progressive attack. The increased flexibility will enable a higher degree of disruption. Future work focuses on identifying the minimum number of switches to cause a cascading effect.

Acknowledgment

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

References

[1] H. Tang and B. McMillin, "Security property violation in CPS through timing," in *Proc. 28th International Conference on Distributed Computing Systems Workshops*, 2008, pp. 519–524.

[2] C.-C. Liu, C.-W. Ten, and M. Govindarasu, "Cybersecurity of SCADA systems: Vulnerability assessment and mitigation," in *Proc. IEEE Power Systems Conference and Exposition*, March 2009, pp. 1–3.

[3] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, January 2012.

[4] H. Lin, S. Sambamoorthy, S. Shukla, J. Thorp, and L. Mili, "Power system and communicaiton network co-simulation for smart grid applications," in *Proc. IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, Anaheim, California, January 2011, pp. 1–6.

[5] 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 2011, pp. 49–54.

[6] ——, "A class of cyber-physical switching attacks for power system disruption," in *7th ACM Annual Cyber Security and Information Intelligence Research Workshop*, Oak Ridge, Tennessee, October 2011.

[7] 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 Society General Meeting*, San Diego, California, July 2012.

[8] R. DeCarlo, S. Zak, and G. Matthews, "Variable structure control of nonlinear multibariable systems: A tutorial," *Proceedings of the IEEE*, vol. 76, no. 3, pp. 212–232, March 1988.

[9] S. Liu, D. Kundur, T. Zourntos, and K. Butler-Purry, "Coordinated variable structure switching attack in the presence of model error and state estimation," in *Third IEEE International Conference on Smart Grid Communications*, Tainan City, Taiwan, November 2012.

[10] ——, "Coordinated variable structure switching in smart power systems: Attacks and mitigation," in *1st International Conference on High Confidence Networked Systems at CPSWeek*, Beijing, China, April 2012, pp. 21–30.

[11] WECC, "WECC off-nominal frequency load shedding plan," 2010.

[12] ——, "Application of zone 3 distance relays on transmission lines," 1997.