Switched System Models for Coordinated Cyber-Physical Attack Construction and Simulation

Shan Liu, Xianyong Feng, 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, fxy8410, dkundur, takis, klbutler}@tamu.edu

***Abstract*—Effective simulation of large-scale power system disturbances especially those stemming from intentional attack represents an open engineering and research problem. Challenges stem from the need to develop intelligent models of cyber-physical attacks that produce salient disruptions, to appropriately portray meaningful cyber-physical interdependencies, and balance precision, scale and complexity. In this paper, we present a foundation for the development of a class of intelligent cyber-physical attacks that we term *coordinated switching attacks*. Our approach, based on variable structure systems theory, is amenable to implementation in well known power system simulators. We provide a method to construct such attack models and demonstrate their utility in the simulation of extensive system disturbances. Our results demonstrate the potential for coordinated switch attacks to enable large-scale power system disturbances.**

I. Introduction

The smart grid promises increased capacity, security and reliability through the integration of advanced communications, computation and control within the power grid. Designing for a future smart grid is challenging on several fronts. Asset owners must understand how to best prioritize investment while operators must be aware of emergent behaviors stemming from the increased dependence on information technology.

Tools for modeling and simulation of such systems are of paramount importance in enabling the judicious planning and preparedness for contingencies. It is well known that simulations are a cost-effective and safer alternative to conducting experiments with prototype or real systems. They can also be conducted faster than in real-time for efficient what-if analysis.

According to a recent report published by the U.S. Department of Homeland Security, Science and Technology Directorate [1] several open challenges exist for developing power grid modeling and simulation capabilities that can meet known and emerging challenges. These include:

1) addressing large-scale disturbances such as accidents, cascading failures and coordinated cyber-physical attacks;
2) accounting for interdependencies between the power grid and other critical infrastructures; and
3) planning and design of distributed generation sources for power grid deployment.

In this paper we focus on a component of the first challenge through the development of intelligent models for coordinated cyber-physical attacks that are easily amenable to the simulation of worst-case power system disruptions. In particular, we focus on *coordinated switching attacks* whereby an attacker aims to destabilize the power grid by leveraging corrupted communication channels and/or control signaling to hijack relevant circuit breakers. Use of such models is imperative for vulnerability analysis in order for stakeholders to prioritize system hardening resources.

Existing empirical approaches [2]–[6] that simulate power system attacks harness well-developed communications and power systems software. Essentially, these simulators, developed separately, are combined such that a cyber attack is implemented in the communication simulator that transfers synthetic sensor or control data to the power system simulator which then takes virtual action based on the possibly corrupted information. Typical power system reliability metrics are then employed to characterize the effects of the attack.

Such approaches are valuable in providing indications of attack impacts, but motivations exist for more intelligent attack models and the tighter integration of the information technology (cyber) and power system (physical) models. It is important that the attack models enable worst-case contingency analysis bound impacts and identify critical system weaknesses. The interface between the information and power system must be well coordinated to allow for the characterization of cyber-physical cascading failures and interactions. Variable granularity of system description is needed to balance precision, scale and complexity. Ideally, models should make use of well developed mathematical constructions in order to enable fundamental insights such as an understanding of global stability behavior from local parameters to promote secure system planning [7], [8].

Our work aims to meet the need for more intelligent attack models amenable to software implementation and testing. We model cyber-physical interactions using a class of hybrid systems known as switched systems. Attacks are constructed by employing variable structure systems theory such that they are ideally coordinated to create large-scale system disturbances. The attacks, easily implemented and tested in simulation for vulnerability analysis, are low-cost requiring simple computations on local state information.

The next section provides background and introduces our coordinated switching attack constructions. Section III demonstrates the utility of our cyber-physical attack models for simulating worst-case disturbances in PSCAD simulations.

978-1-4673-0195-4/11/$26.00 ©2011 IEEE

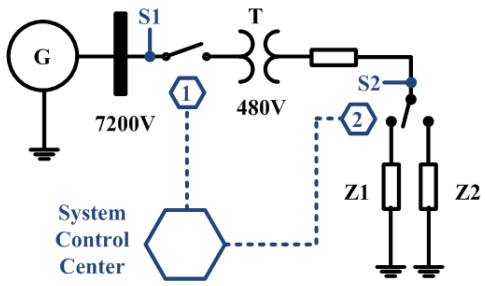

Fig. 1. Elementary switched system example. Two different dynamics describe behavior depending on the status of switch $S2$.

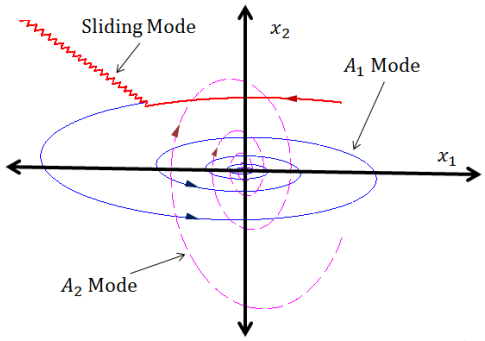

Fig. 2. Phase portraits of individual stable subsystems $\dot{x} = A_1 x$ and $\dot{x} = A_2 x$, and unstable switched system for $s(x) = x_1 + x_2$; $\varepsilon = 0.5$.

Conclusions and future directions of research are provided in Section V.

II. Coordinated Switching Attacks

Switched systems are a type of variable structure system that consist of a family of subsystems and a rule that governs the switching among them. For example, the elementary power system of Fig. 1, which represents a load shedding scenario, can be described using two different sets of dynamics depending on the location of the load switch $S2$. Specifically, we can write

$$\dot{x}(t) = \begin{cases} A_1(x,t), & s(x) > 0 \\ A_2(x,t), & s(x) < 0 \end{cases} \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state vector, $A_i(x,t) \in \mathbb{R}^n$ is the subsystem dynamics when $S2$ connects Z_i, and $s(x) \in \mathbb{R}$; $s(x) = 0$ 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 emergent behavior known as a *sliding mode* [9], [10]. Here, the trajectory of the state $x(t)$ 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*.

Consider a specific case of Fig. 1 in which we assume linear models and $n = 2$; where $x = [x_1, x_2]^T$. Suppose,

$$\dot{x}(t) = \begin{cases} A_1 x, & s(x) > 0 \\ A_2 x, & s(x) < 0 \end{cases} \tag{2}$$

for $A_1 = \begin{bmatrix} -1 & -10 \\ 2 & -0.2 \end{bmatrix}$ and $A_2 = \begin{bmatrix} -0.2 & 2 \\ -10 & -1 \end{bmatrix}$ and some $s(x)$. The phase portrait of each individual subsystem $\dot{x} = A_i x$, $i = 1, 2$ is shown in Fig. 2 demonstrating the stability of the power system example in each static switch position.

We assert that variable structure system theory can be leveraged to design a method of switching (equivalent to selection of an appropriate sliding surface $s(x)$) to destabilize Eq. 2 even if each subsystem alone is stable. For example, suppose that the sliding surface is selected to be $s(x) = x_1 + x_2$. The corresponding phase portrait is shown in Fig. 2 demonstrating the trajectory of the state away from the origin.

This form of attack requires that switching be coordinated such that it occurs when the state attempts to intersect the sliding surface $s(x) = 0$. The attacker must therefore be intelligent ideally knowing the local state information in order to induce a worst-case disruption. To apply a coordinated switching attack, a sliding surface $s^\dagger(x)$ that destabilizes the switched system must be known to the attacker. The attack can be orchestrated through a combination of cyber-physical corruptions that is beyond the scope of this paper.

The stages of such an attack construction can be described as follows: *Step (1):* Represent the system under attack as a switched system whereby $s(x)$ remains general; *Step (2):* Determine the phase portraits of each subsystem identifying stable focii and saddle points (necessary for nonlinear systems) and overlap them on the same plot; *Step (3):* Using the overlapping phase portrait, search for a sliding surface $s(x) = 0$ when a sliding mode exists if $s\dot{s} < 0$. An unstable sliding mode exists if, in the vicinity of $s(x) = 0$, the trajectory vectors of the subsystems point toward the switching surface in opposite directions and away from the origin; this ensures that the state trajectory of the switched system will be driven to the switching surface, will stay within a neighborhood of it and move away from the origin for instability. The interested reader is referred to [10]; *Step (4):* Assign the identified unstable sliding surface to $s^\dagger(x)$ for attack implementation or modify it systematically in simulation to identify a worst-case attack impact. The latter may be necessary when the model of *Step (1)* is distinct from (i.e., usually lower order than) the simulator models.

When implementing the attack, switch "chattering" will result, which is not realistic for circuit breakers that exhibit practical delays and hysteresis between switching. Thus, we employ a *boundary layer* for switching [11]. Here, for $\varepsilon > 0$, an attack is implemented as follows:

$$\dot{x}(t) = \begin{cases} A_1 x, & s^\dagger(x) > \varepsilon \\ A_2 x, & s^\dagger(x) < -\varepsilon \end{cases}. \tag{3}$$

The sliding mode trajectory in Fig. 2 makes use of $\varepsilon = 0.5$.

Although general nonlinear switching surfaces are possible, for simplicity, we focus on identification of linear sliding surfaces. We next go through the steps of attack construction for an example system.

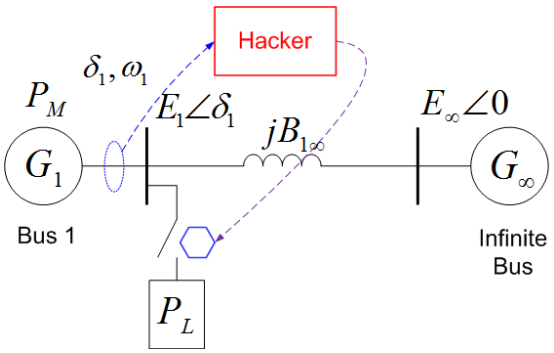

Fig. 3. Single machine infinite bus system used for attack construction.

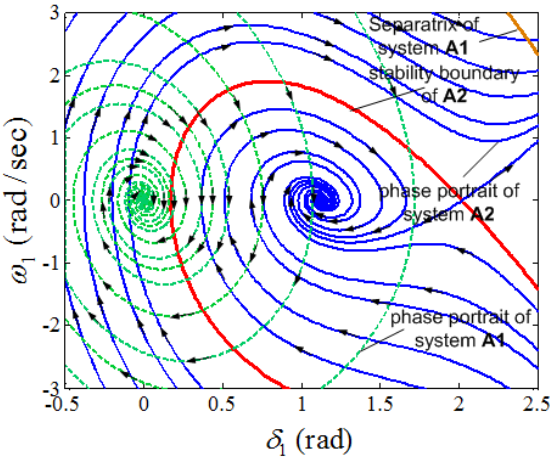

Fig. 4. Overlapping phase portraits of system A_1 and A_2.

III. Attack Construction: Case Study

Step (1): During attack construction, we consider the single machine infinite bus (SMIB) system model of Fig. 3 with a switch at load P_L. It is straightforward to show for an appropriate parameter set and from the swing equations that a switched system representation is given by:

$$A_1 : \begin{cases} \dot{\delta}_1 = \omega_1 \\ \dot{\omega}_1 = -10\sin\delta_1 - \omega_1 \end{cases} \quad \text{if } P_L \text{ connected}$$

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

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

Step (2): Setting the left hand side of the dynamics to zero, the equilibrium points of A_1 and A_2 are found to be $(2k\pi, 0), (2k\pi + \pi, 0)$, and $(2k\pi + 1.1198, 0), (2k\pi + 2.0218, 0)$, respectively, for any integer k. Employing Jacobians and system separatrices, the appropriate stable equilibria and saddle points are found to determine the overall phase portrait shown in Fig. 4.

Step (3): Observation of the overlapping phase portraits as detailed in Section II reveals a sliding mode surface of the form:

$$s = \delta_1 + \omega_1. \tag{4}$$

To model breaker delays and hysteresis, we employ $\varepsilon = 0.2$

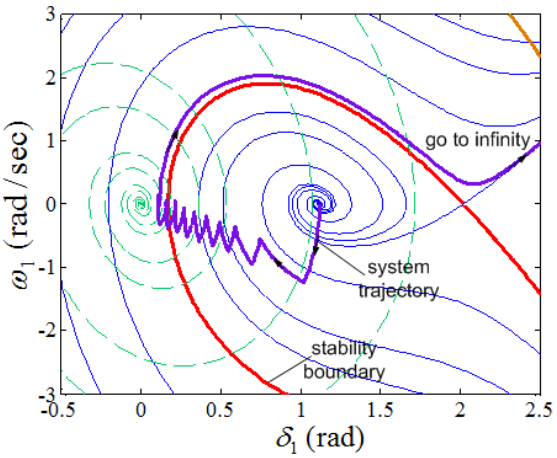

Fig. 5. System trajectory of coordinated switching attack of Eq. 5.

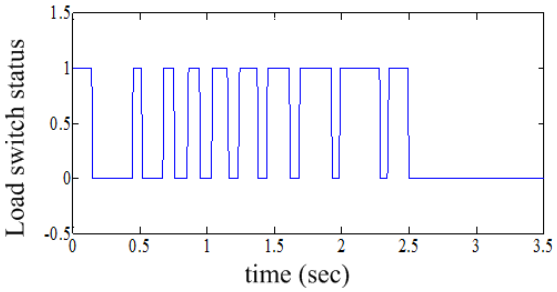

Fig. 6. Load switch status for system of Eq. 5; 0 represents open switch (i.e., P_L not connected) and 1 represents closed switch (P_L connected).

implementing the switching attack for $s^\dagger = \delta_1 + \omega_1$:

$$\begin{aligned} \dot{\delta}_1 &= \omega_1 \\ \dot{\omega}_1 &= \begin{cases} -10\sin\delta_1 - \omega_1, & s^\dagger > \varepsilon \\ 9 - 10\sin\delta_1 - \omega_1, & s^\dagger < -\varepsilon \end{cases} \end{aligned} \tag{5}$$

Fig. 5 presents the corresponding phase portrait showing the unstable system trajectory away from the origin. The load switch status is shown in Fig. 6. Switching occurs from 0 to 2.5 seconds, which drives the system over the stability boundary of A_2. At this point, the attacker may continue to apply the switching attack or to save effort may leave the switch open; to minimize cost, the latter is applied.

Step (4): Thus, $s^\dagger = \delta_1 + \omega_1$ is identified as an unstable sliding surface for the SMIB switched system of Fig. 3. The second order swing equations have been used for system modeling during this attack construction phase and MATLAB/Simulink is employed for the phase trajectory plots. In the next section, we demonstrate how for more realistic simulators such as PSCAD, the identified $s^\dagger = \delta_1 + \omega_1$ represents a search starting point to identify a severely disrupting attack during simulation.

IV. PSCAD Simulation

In this section we study two power system examples that can be modeled as the SMIB switched system of the previous section. Thus, we start with the unstable sliding mode $s^\dagger$ constructed in the previous section and modify it through search (specifically through slope modification) to account for the high order system differences.

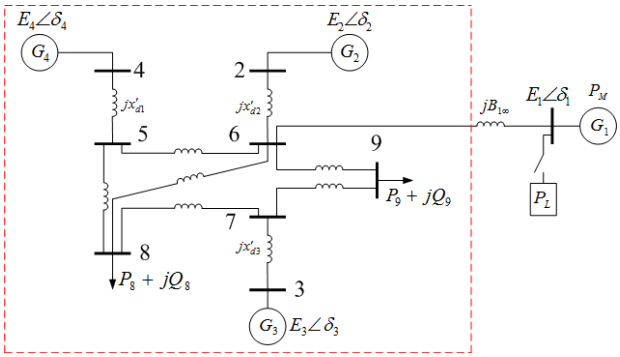

Fig. 7. One line diagram of the Case 1 study power system. The dashed rectangle can be approximated as an SMIB system.

TABLE I
GENERATOR PARAMETERS FOR FIG. 7 SYSTEM.

Name	Parameter	Value
Rated RMS Line-Line Volatge	V_{gl-l}	13.8 kV
Active Power	P_g	36 MW
Power Factor	p_{fg}	0.8
Frequency	f	60 Hz
Armature Resistance @ 95°C	R_a	0.010 Ω
Potier reactance	X_p	0.17
Direct axis unsaturated reactance	Xd	1.55
Direct axis unsaturated transient reactance	Xd'	0.22
Direct axis unsaturated sub-transient reactance	Xd"	0.14
Direct axis open circuit unsaturated transient time constant	Tdo'	8.95 sec
Direct axis open circuit unsaturated sub-transient time constant	Tdo"	0.036 sec
Quadrature axis unsaturated reactance	Xq	0.76
Quadrature axis unsaturated transient reactance	Xq'	N.A
Quadrature axis unsaturated sub-transient reactance	Xq"	0.20
Quadrature axis open circuit unsaturated transient time constant	Tqo'	N.A
Quadrature axis open circuit unsaturated sub-transient time constant	Tqo"	0.12 s
Inertia Constant	H	0.5 sec

A. Case 1 Study

Consider the system of Fig. 7 where we assume that the inertia of Generator G_1 is smaller than that of Generators G_2, G_3 and G_4. Thus, in contrast to G_1 the total system inertia is large and can be approximated as an infinite inertia system. Thus, the overall system of Fig. 7 can be modeled as the SMIB switched system of Fig. 3 and the attack construction of Section III represents a starting point to search for an appropriate $s^\dagger$ in PSCAD simulation for system destabilization.

The system of Fig. 7 is modeled and simulated in PSCAD using the generator parameters of Table I. The transmission line connecting the generator and the infinite bus is modeled using an inductor with inductance 0.014 H and the local load P_L is chosen as 32.4 MW modeled as a constant resistor. Varying the slope of the candidate unstable sliding mode of Section III reveals that the following switching logic serves to destabilize the system for a large-scale system disruption:

$$s^\dagger = \delta_1 + 0.2 \cdot \omega_1. \tag{6}$$

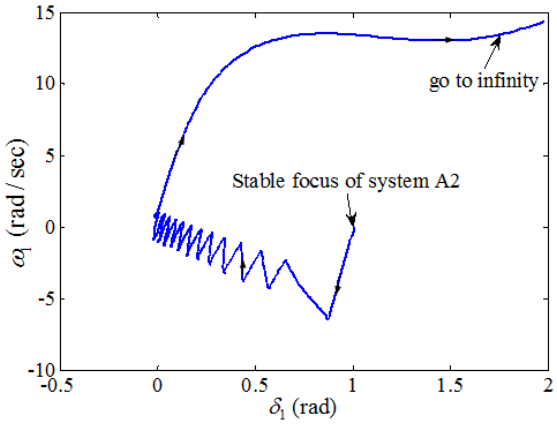

Fig. 8. System trajectory of the the switched system of Fig. 7 in the presence of a coordinated switching attack using $s^\dagger = \delta_1 + 0.2 \cdot \omega_1$.

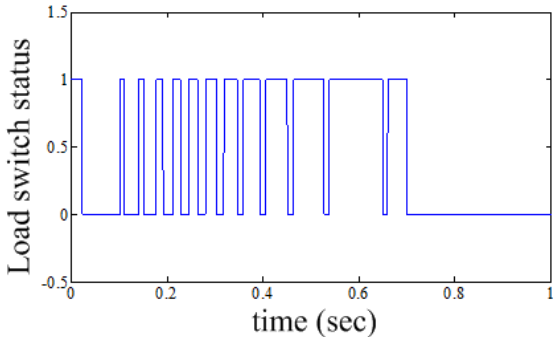

Fig. 9. Load switch status of Fig. 7 in the presence of an attack with $s^\dagger = \delta_1 + 0.2 \cdot \omega_1$; 0 represents open switch (i.e., P_L not connected) and 1 represents closed switch (P_L connected).

The parameter $\varepsilon = 0.2$ is employed to model breaker delays and hysteresis. The coordinated switching attack is applied from 0 to 0.7 seconds which drives the system across the stability boundary of subsystem A_2 (i.e., when the switch is open and no load is connected). At this time the state trajectory approaches infinity as demonstrated in the phase portrait of Fig. 8 generated from the PSCAD simulation. The switch status of the load, system frequency and output voltage are shown in Figs. 9, 10 and 11, respectively, demonstrating the disruptiveness of the attack. As can be observed, the frequency and voltage were unstable after the coordinated switching attack was applied to the system.

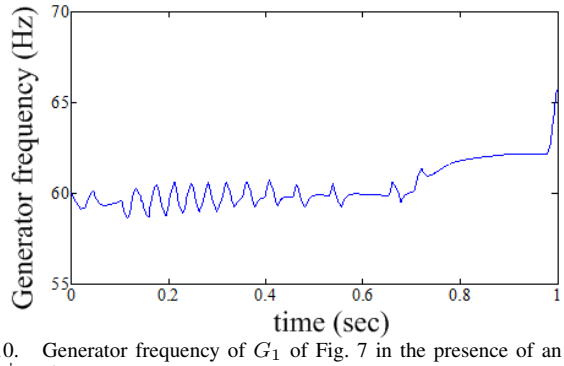

Fig. 10. Generator frequency of G_1 of Fig. 7 in the presence of an attack with $s^\dagger = \delta_1 + 0.2 \cdot \omega_1$.

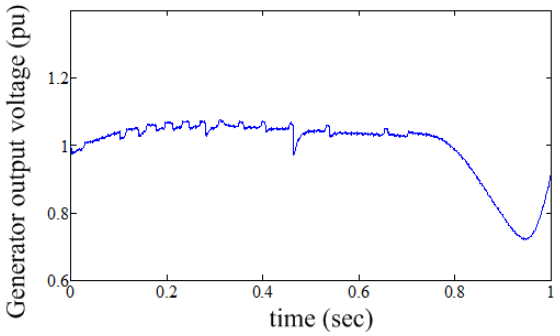

Fig. 11. Generator G_1 of Fig. 7 output voltage in the presence of an attack with $s^\dagger = \delta_1 + 0.2 \cdot \omega_1$.

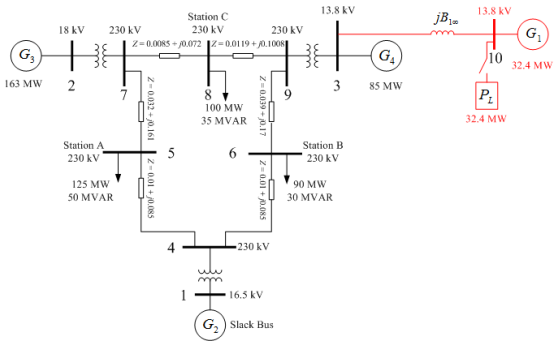

Fig. 12. One line diagram of revised WECC system.

B. 3-Generator, 9-Bus Case Study

We also demonstrate of the ability of the coordinated switching attack to cause large-scale disruptions a variant of the well-known Western Electricity Coordinating Council (WECC) 3-machine, 9-bus system [12]. Based on the WECC system, we add a transmission line, a local load, and a gas turbine generator to produce the revised WECC system shown in Fig. 12. Here, the base MVA is 100, the system normal frequency is 60 Hz. and the generator parameters are shown in Table II. The transmission line connecting Generator G_1 and the infinite bus is modeled using an inductor of 0.014 H. The local load P_L is chosen to be 32.4 MW modeled using constant resistor. The PSCAD step size was chosen to be 50 μs. We assert that the insights from the SMIB system can also be employed to determine a unstable sliding mode in this case.

Using a similar procedure to Section IV-A the following unstable sliding mode has been found in simulations (by varying the slope of linear switching surface in increments) to destabilize the system:

$$s^\dagger = \delta_1 + 0.1 \cdot \omega_1. \tag{7}$$

Employing $\varepsilon = 0.05$ the coordinated switching attack of Eq. 3 is applied. The switching attack is applied from 0 to 0.7 seconds, which drives the system trajectory across the stability boundary of the subsystem A_2 (i.e., P_L not connected). The attacker then switches to subsystem A_2 at 0.7 seconds to destabilize the system. Generator G_1 is tripped at 1 second causing a significant disturbance. The system state gradually approaches infinity as shown in Fig. 13. The switch status, Generator G_1 frequency and output voltage are shown in Figs. 14, Figs. 15 and 16, respectively. The frequency and voltage of Generator G_1 destabilized after the coordinated switching attack was applied to the system. As shown in Fig. 17, the frequency of Generators G_2, G_3 and G_4 exhibit large oscillations due to the instability of Generator G_1 prior to tripping. After Generator G_1 was tripped at 1 second, the frequency of G_2, G_3 and G_4 gradually converged back to 60 Hz.

TABLE II
GENERATOR PARAMETERS FOR FIG. 12 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	
Q axis unsaturated reactance	Xq	0.76	0.0969
Q axis unsaturated transient reactance	Xq'	N.A	0.0969
Q axis open circuit unsaturated transient time constant	Tqo'	N.A	0.31
Inertia Constant	H	0.5 sec	23.64
Name	Parameter	Gen 3	Gen 4
Rated RMS Line-Line Volatge	V_{gl-l}	18.0 kV	13.8 kV
Active Power	P_g	163 MW	85MW
Power Factor	p_{fg}	0.8	0.8
Frequency	f	60 Hz	60 Hz
Direct axis unsaturated reactance	Xd	0.8958	1.3125
D axis unsaturated transient reactance	Xd'	0.1198	0.1813
D axis open circuit unsaturated transient time constant	Tdo'	6.0	5.89
Q axis unsaturated reactance	Xq	0.8645	1.2578
Q axis unsaturated transient reactance	Xq'	0.1969	0.25
Q axis open circuit unsaturated transient time constant	Tqo'	0.539	0.6
Inertia Constant	H	6.4	3.01

V. CONCLUSIONS

This paper introduces a class of coordinated switching attacks to enable the modeling and simulation of large-scale disruptions due to coordinated cyber-physical attacks. Attack construction makes use of variable structure systems theory in order to produce a state-dependent switching rule to implement the attack. The potential of this class of attacks in the simulation of system disturbances is shown through study of two systems including a variant of the WECC 3-maching, 9-bus system.

This paper represents a work in progress toward the development of a class of attacks to aid in contingency and

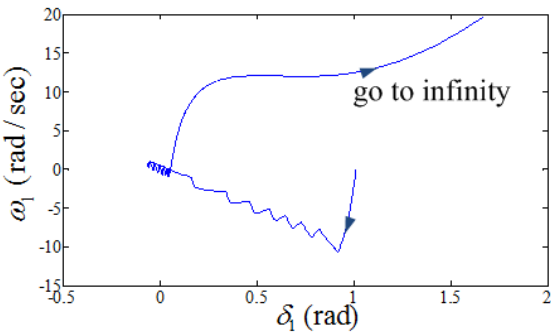

Fig. 13. System trajectory of the switched system of Fig. 12 in the presence of a coordinated switching attack using $s^\dagger = \delta_1 + 0.1 \cdot \omega_1$.

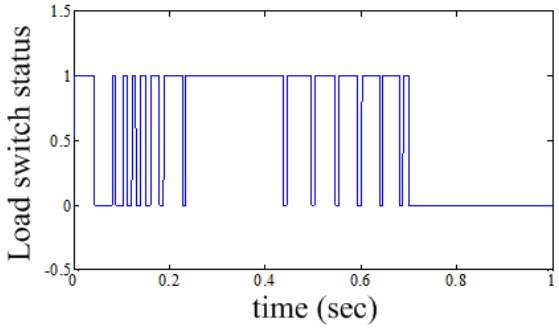

Fig. 14. Load switch status of Fig. 12 in the presence of an attack with $s^\dagger = \delta_1 + 0.1 \cdot \omega_1$; 0 represents open switch (i.e., P_L not connected) and 1 represents closed switch (P_L connected). To reduce effort the attack is only applied from 0 to 0.7 s after which the system destabilizes tripping G_1.

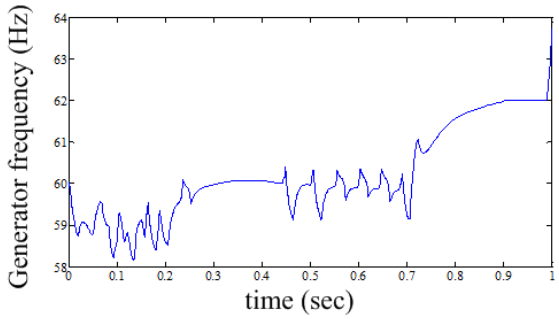

Fig. 15. Generator frequency of G_1 of Fig. 12 in the presence of an attack with $s^\dagger = \delta_1 + 0.1 \cdot \omega_1$. G_1 destabilizes tripping out at 1 second.

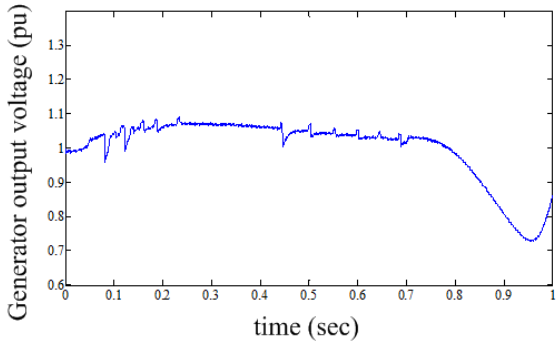

Fig. 16. Generator G_1 of Fig. 12 output voltage in the presence of an attack with $s^\dagger = \delta_1 + 0.1 \cdot \omega_1$.

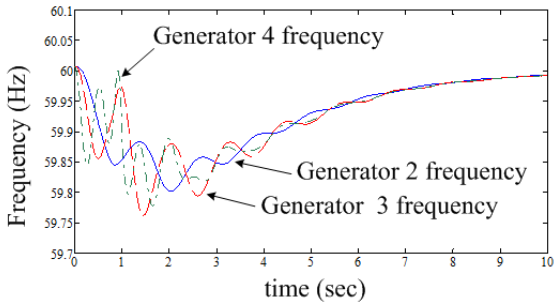

Fig. 17. Frequencies of G_2, G_3 and G_4 before and after G_1 tripping.

vulnerability analysis of current and future power systems. Future work will extend the attack for multiple switches and generalize the theory to develop necessary and sufficient conditions for a system to be susceptible to such attacks. In addition, we will test larger test systems in DSA*Tools*™.

Acknowledgment

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.

References

[1] National Power Grid Simulator Workshop Participants, "National power grid simulation capability: Needs and issues," U.S. Department of Homeland Security, Science and Technology Directorate, Tech. Rep., December 9-10 2008.

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

[3] D. D. Dudenhoeffer, M. R. Permann, S. Woolsey, R. Timpany, C. Miller, A. McDermott, and M. Manic, "Interdependency modeling and emergency response," in *Proc. 2007 Summer Computer Simulation Conference*, July 2007, pp. 1230–1237.

[4] B. Rozel, M. Viziteu, R. Caire, N. Hadjsaid, and J.-P. Rognon, "Towards a common model for studying critical infrastructure interdependencies," in *Proc. IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century*, Pittsburgh, Pennsylvania, July 2008, pp. 1–6.

[5] N. HadjSaid, C. Tranchita, B. Rozel, M. Viziteu, and R. Caire, "Modeling cyber and physical interdependencies – application in ICT and power grids," in *Proc. IEEE Power Systems Conference and Exposition*, March 2009, pp. 1–6.

[6] J. Stamp, A. McIntyre, and B. Ricardson, "Reliability impacts from cyber attack on electric power systems," in *Proc. IEEE Power Systems Conference and Exposition*, March 2009, pp. 1–8.

[7] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *Proc. IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, Maryland, October 2010, pp. 244–249.

[8] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. Butler-Purry, "Towards modeling the impact of cyber attacks on a smart grid," *International Journal of Security and Networks*, vol. 6, no. 1, pp. 2–13, 2011.

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

[10] 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.

[11] D. Liberzon, *Switching in Systems and Control*. Boston: Birkhauser, 2003.

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