A Class of Cyber-Physical Switching Attacks for Power System Disruption

[Extended Abstract]

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

In this paper, we present the development of a new class of intelligent cyber-physical attacks termed *coordinated switching attacks* whereby opponents aim to destabilize the power grid through controlled switching. Such switching is facilitated by cyber attack and corruption of communication channels and control signals of the associated switch(es). The attack employs a variable structure systems theory model of a smart grid. The sliding mode theory is employed to leverage emergent system properties to identify state-dependent switching sequences to disrupt power flow. Our results demonstrate the potential for coordinated switch attacks to enable large-scale power system disturbances.

Categories and Subject Descriptors

B.2.2 [**Hardware**]: Performance Analysis and Design Aids—*Simulation, worst-case analysis*; I.6.5 [**Computing Methodologies**]: Model Development—*Modeling methodologies*; K.6.5 [**Computing Milieux**]: Security and Protection—*physical security, unauthorized access*

General Terms

Algorithms, security, theory

Keywords

switched system, coordinated switching attacks, smart grid

1. INTRODUCTION

Contingency analysis of power systems is a well understood problem to aid in securing the power grid. However, as the power system today evolves into a smarter grid, there will be increased threats of intentional cyber attack. Cyber attacks target the cyber assets of a system in order to compromise confidentiality, integrity and availability (C-I-A). Specifically, cyber assets are a collection of computing system components including hardware, software, storage, communication media, and data that directly support information-related activities. In a smart grid, they typically facilitate monitoring, communications, computation and control. They often include supervisory control and data acquisition (SCADA) system components, intelligent electronic devices (IEDs), programmable logic controllers (PLCs), remote terminal units (RTUs), advanced metering infrastructure (AMI), phasor measurements units (PMUs), phasor data concentrators (PDCs) and associated communications infrastructure.

The greater dependence on this type of information technology coupled with their increased connectivity will make the need for cyber security of paramount importance. However, before cyber security solutions can be comprehensively developed, it is important to understand the system vulnerabilities. In a smart grid, with increased interaction between the underlying physical power system and the information system theses vulnerabilities may arise from emergent properties that are not well understood.

In this paper we study the vulnerability of power systems to coordinated state-dependent switching attacks. Specifically, we propose a new class of coordinated attacks that are designed to destabilize a power system through switching. Thus, the cyber attack takes a cyber-physical flavor as it is constructed by making use of state-dependent information of the physical power system components, but is implemented through cyber corruptions of the associated communication channels or control signals of the target switch(es).

We model our problem and develop a cyber-physical attack 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, can be easily implemented for vulnerability analysis and are low-cost requiring simple computations on local state information.

2. COORDINATED SWITCHING ATTACKS

Consider an elementary power system shown in Fig. 1. This single generator system can serve one of two loads $Z1$ or $Z2$ depending on the status of switch $S2$. Two sensor/actuator devices denoted with enumerated hexagons observe local voltages and currents around each switch and communicate this information to the system control center

CSIIRW '11, October 12-14, Oak Ridge, Tennessee, USA

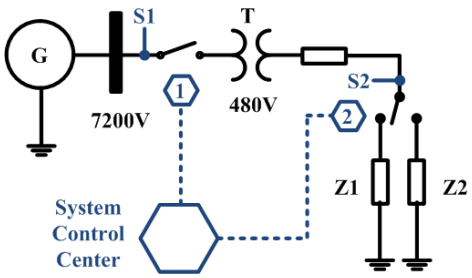

Figure 1: Elementary switched system example. Two different dynamics describe behavior depending on the status of switch $S2$.

and the associated switch itself for remote and local decision-making, respectively. We consider a situation in which the communication link between the system control center and sensor/actuator device 2 is corrupted allowing arbitrary control signals to be injected to control the status of $S2$.

If the status of $S2$ is ideally controlled we assert that it may be possible to destabilize the overall *switched system*. Formally, 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* [1, 4]. 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.

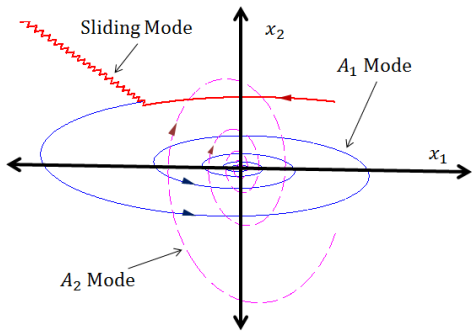

Figure 2: Phase portraits of individual stable subsystems $\dot{x} = A_1 x$ and $\dot{x} = A_2 x$, and unstable switched system for $s(x) = x_1 + x_2$; $\varepsilon = 0.5$.

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 $s(x) = 0$, a sliding mode would 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 [1]; *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* [2] for switching. 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.

3. ATTACK CONSTRUCTION

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

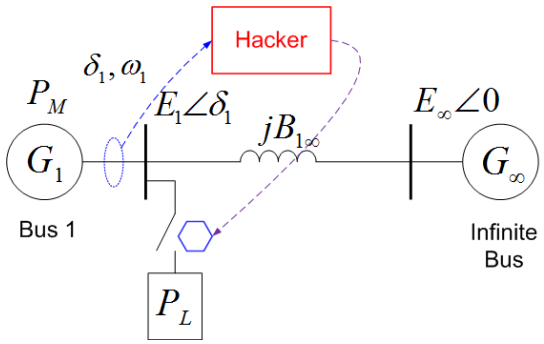

Figure 3: Single machine infinite bus system used for attack construction.

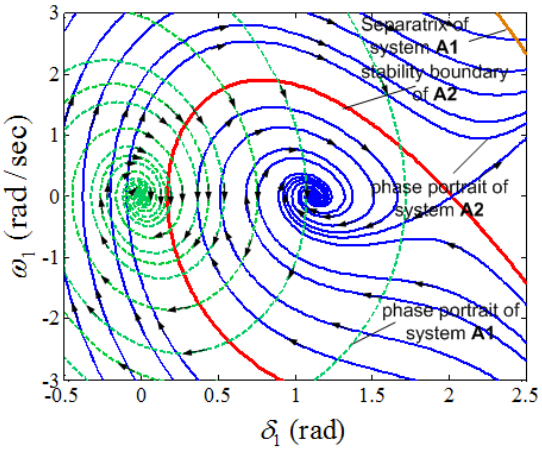

Figure 4: Overlapping phase portraits of system A_1 and A_2.

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 2 reveals a sliding mode surface of the form:

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

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

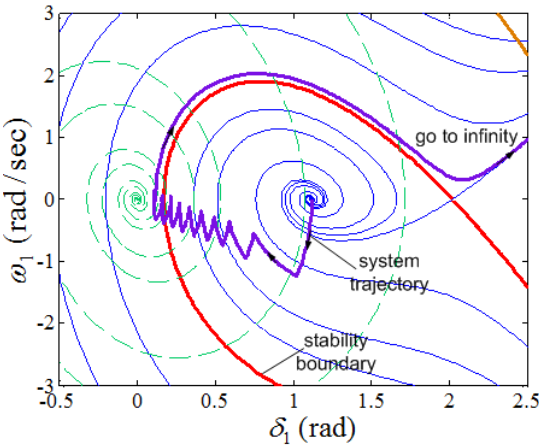

Figure 5: System trajectory of coordinated switching attack of Eq. 5.

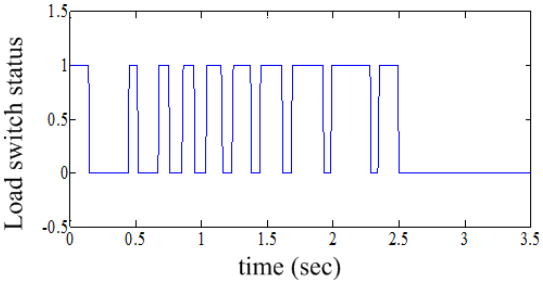

Figure 6: Load switch status for system of Eq. 5; 0 represents open switch (i.e., P_L not connected) and 1 represents closed switch (P_L connected).

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.

4. IMPLEMENTATION AND SIMULATION

In this section we study through PSCAD simulations the impact of an attack. We employ a power system example that can be modeled as the SMIB switched system of the previous section. 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.

We demonstrate of the ability of the coordinated switching attack to cause large-scale disruptions on a variant of the well-known Western Electricity Coordinating Council (WECC) 3-machine, 9-bus system [3]. Based on the WECC system, we add a transmission line, a local load, and a

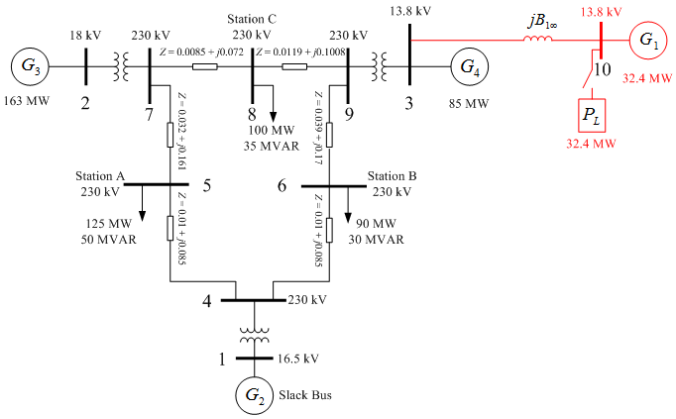

Figure 7: One line diagram of revised WECC system.

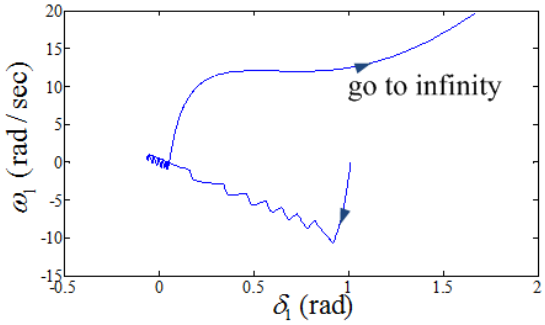

Figure 8: System trajectory of the switched system of Fig. 7 in the presence of a coordinated switching attack using $s^\dagger = \delta_1 + 0.1 \cdot \omega_1$.

gas turbine generator to produce the revised WECC system shown in Fig. 7. Here, the base MVA is 100, the system normal frequency is 60 Hz. 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 study how the insights from the SMIB system can be employed to determine a unstable sliding mode to exploit for attack.

The following unstable sliding mode has been found in simulations (by varying the slope of linear switching surface in increments) to destabilize the system:

$$s^\dagger = \delta_1 + 0.1 \cdot \omega_1. \tag{6}$$

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. 8. The switch status, is shown in Fig. 9.

As shown in Fig. 10, 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 where the attack causing system disruption, the frequency of G_2, G_3 and G_4 gradually converged back to 60 Hz a producing a reduced operational state.

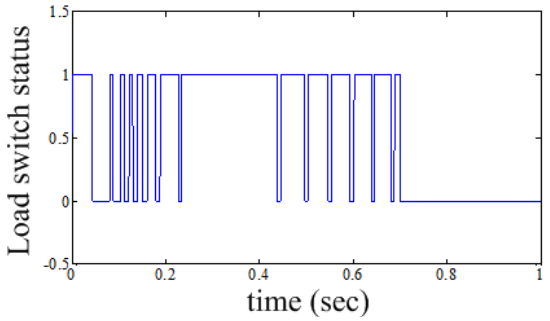

Figure 9: Load switch status of Fig. 7 in the presence of an attack with $s^\dagger = \delta_1 + 0.1 \cdot \omega_1$; 0 represents open switch (i.e., P_L not connected) and 1 represents closed switch (P_L connected). To reduce effort the attack is only applied from 0 to 0.7 s after which the system destabilizes tripping G_1.

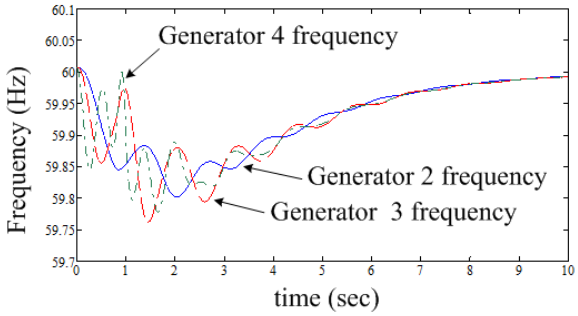

Figure 10: Frequencies of G_2, G_3 and G_4 before and after G_1 tripping.

5. CONCLUSIONS

This paper introduces a class of cyber-physical attacks to analyze the vulnerability of emerging power systems to state-dependent opponent-controlled coordinated switching. 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 to enable large-scale system disturbances is demonstrated through simulation of the well known Western System Coordinating Council 3-machine, 9-bus system. Future work will extend the the research to include multiple corrupted switches to optimize disruption.

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.

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

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

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