A Game-Theoretic Control Approach to Mitigate Cyber Switching Attacks in Smart Grid Systems

Abdallah K. Farraj, Eman M. Hammad, Ashraf Al Daoud, and Deepa Kundur
Department of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario, Canada
Email: {abdallah, ehammad, ashraf, dkundur}@ece.utoronto.ca

Abstract—**A parametric game-theoretic controller is proposed to stabilize power systems during and after cyber switching attacks. The attacks are based on calculated switchings of external power sources in order to destabilize the power system. The controller relies on receiving timely information from the cyber component of the smart grid to control the output of fast-acting external power sources in order to balance the swing equation of the system. In this regard, game-theoretic analysis is applied to devise reactive strategies for the controller to drive the frequency of the system's generators to stability. The proposed controller gives system operators the flexibility to meet constraints on external power while achieving an acceptable stability time. Numerical results show the usefulness of the proposed controller in stabilizing the WECC 3-generator power system during and after a switching attack.**

I. Introduction

Smart grid systems have emerged as a result of distributed integration between the traditional power grid and cyber systems to improve the resilience and efficiency of the power delivery. The cyber component of the smart grid includes advanced control, communication networking, and sensor technologies. Specifically, system data is collected using sensors placed at particular locations over the power grid, which is then transmitted via a communication network to a control center for analysis. Smart grid systems are getting increased attention from both academic and industrial communities due to the benefits and the challenges they provide to end-user customers, electricity companies, and regulating bodies.

Because of evolving regulations and technical opportunities, cyber-physical security of smart grid systems is a sound concern for stakeholders, and thus, it creates the potential for new research directions to investigate different aspects of this topic. One specific topic of particular interest is coordinated variable structure switching attacks that target one or more components of the power system based on cyber information gained by the attacker. Another interesting aspect is concerned with designing effective control schemes that help provide system resilience during and after the attack (for example, a 3-phase fault in a feeder).

Switching attacks pose a threat to emerging smart grid systems. For example, [1]–[4] demonstrate the impact of calculated switchings of a small load on stability of power systems. The underlying assumption involves an attacker that has cyber control over a circuit breaker switching a resistive load. In order to conduct a successful attack, the attacker has to intercept the system's cyber data and must have a correct model of the local power system. Such attacks rely on using sliding-mode control theory in order to calculate when to switch the load on or off the power grid.

To address such attacks, the timely availability of power system cyber data can help in designing advanced control schemes that leverage the high granularity of real-time data for optimization and protection in the face of disturbance. The disturbance can be physical in nature via the occurrence of a fault or cyber-related through a switching attack. The work of [5]–[8] recently proposed a flocking-based scheme that controls fast-acting external power sources in order to stabilize the power system after clearance of a fault in the system.

This paper investigates a new, easy-to-conduct, cyber switching attack where the attacker has cyber control over a circuit breaker that can switch a fast-acting external power source. The only information the attacker actually needs is the frequency of the target generator, where, depending on the sign of the generator's frequency, the attacker switches the external power source to either absorb or inject power to destabilize the power system. In this regard, a novel parametric stabilizing control scheme is devised, where the controller receives frequent, but not necessarily continuous, cyber updates about frequencies of the system generator and reacts accordingly to affect the output of the external power supplies.

The interaction between the stabilizing controller and the attacker is formulated as an iterated game where in each round, the controller reacts to the action of the attacker in the previous round. A salient feature of such games is that players with longer memories of the history of the game have no advantage, in the long term, over those with shorter ones, and thus, iterated games lend themselves to Markovian strategies that are referred to as "zero-determinant" strategies [9]. This work shows that the game of mitigating cyber switching attacks admits an appealing structure that allows the stabilizing controller to mitigate such attacks using the aforementioned strategies.

The rest of this paper is organized as follows. Development of the cyber attack and the stabilizing controller is shown in Section II. Section III illustrates the development of the game-theoretic controller. Numerical results are shown in Section IV. Conclusions are shown in Section V.

978-1-4799-4934-2/14/$31.00 ©2014 IEEE

II. Development of Destabilizing Cyber Attack and Mitigation Strategies

A. Power System Overview

A schematic of the WECC 3-generator power system is shown in Fig. 1. Bus 1 is called the slack bus, buses 2 and 3 are the PV buses, and buses 7 and 8 are known as the PQ buses. Let N denote the number of generators in the power system; i.e., N = 3 for the WECC power system. The parameters of the generators of the power system are defined in Table I, where M_i and D_i are expressed in seconds, δ_i is expressed in rad/sec, and the rest are expressed in per units.

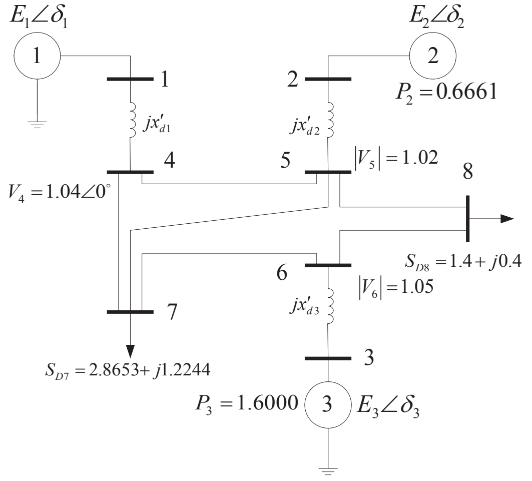

Fig. 1. WECC power system

Parameter	Description
E_i	internal voltage of Generator i, $i = 1, \ldots, N$
$P_{e,i}$	electrical power of Generator i
$P_{m,i}$	mechanical power of Generator i
M_i	inertia of Generator i
D_i	damping coefficient of Generator i
δ_i	rotor angle of Generator i
ω_i	relative normalized rotor frequency of Generator i

TABLE I
System parameters

Components of a power system are linked via a differential equation that is referred to as the *swing equation*. The transient stability of a power system can be studied by investigating the behavior of the swing equation during the instability period. However, the system parameters can be considered constant during that period and a swing equation with time-invariant parameters can be used to effectively model the dynamics of the power system.

Let $\dot{\delta}_i$ and $\dot{\omega}_i$ denote the derivatives of δ_i and ω_i with respect to time, respectively. Then, assuming a system with no power control (for example, the governor control is not activated), the swing equation for Generator i in an interconnected power system is expressed as [10], [11]

$$\begin{aligned} \dot{\delta}_i &= \omega_i \\ M_i\,\dot{\omega}_i &= -D_i\,\omega_i + P_{m,i} - P_{e,i}\,, \end{aligned} \tag{1}$$

where the electrical power of Generator i is defined as [12]

$$\begin{aligned} P_{e,i} = \sum_{k=1}^{N} \; & |E_i|\,|E_k|\,[G_{ik}\cos(\delta_i - \delta_k) + \\ & B_{ik}\sin(\delta_i - \delta_k)]\ . \end{aligned} \tag{2}$$

Here, $G_{ik} = G_{ki} \geq 0$ is the Kron-reduced equivalent conductance between Generator i and Generator k, $B_{ik} = B_{ki} > 0$ is the Kron-reduced equivalent susceptance between Generator i and Generator k, and $Y_{ik} = G_{ik} + \sqrt{-1}\,B_{ik}$ is the Kron-reduced equivalent admittance between Generator i and Generator k. All quantities Y_{ik}, G_{ik}, and B_{ik} are expressed in per unit values.

B. Cyber Attack and Stabilizing Control

Let $\Delta T = t - t_0$ be the total considered duration where the value of ω_i is calculated at time t and t_0 is the starting time of the duration, and let $\Delta P_i = P_{e,i} - P_{m,i}$ denote the difference between the electrical power and the mechanical power of Generator i. Further, define $g_i = \frac{\Delta T}{M_i} > 0$.

It is assumed that each generator in the power system is equipped by an external fast-acting power source. The power source can inject (absorb) real power in (from) the power grid, and it can be controlled using cyber commands. A flywheel is an example of such power source. A cyber-controlled switch can determine the state of the power source. In any case, the power source can be in one of three states; absorbing power, injecting power, or not interacting with the power system. The attacker affects the power system by switching the external power source at Generator i between injecting and absorbing real power with a value of $P_{A,i}$. In order to do that, it is assumed that the attacker has command over the switch that controls the external power source either by physical or cyber means.

The goal of the stabilizing controller is to asymptotically drive the frequency of the system generators into stability after the occurrence of a disturbance; i.e., it is required that $\lim_{t\to\infty} \omega_i(t) = 0\ \forall i \in \{1, \ldots, N\}$ is achieved after the activation of the controller. The stabilizing controller has cyber access to the switches that control the operation of the external power sources, and it can absorb or inject a real power of $P_{C,i}$ at Generator i. The values of $P_{A,i}$ and $P_{C,i}$ remain constants during ΔT. However, it is assumed that the stabilizing controller has more leverage than the attacker; i.e., $|P_{C,i}| > |P_{A,i}|$.

The swing equation of Generator i, including the effects of both the attacker and the stabilizing controller, becomes

$$\begin{aligned} \dot{\delta}_i &= \omega_i \\ \dot{\omega}_i &= \tfrac{1}{M_i}\left[-D_i\omega_i - \Delta P_i + P_{A,i} + P_{C,i}\right]\ . \end{aligned} \tag{3}$$

A positive value of $P_{A,i}$ ($P_{C,i}$) implies that the attacker (controller) injects real power into the power system at Generator i, and a negative value indicates that real power is absorbed at the external power source of Generator i.

The following four combinations of attack and control are investigated:

1) Case 1: Both Attack and Control Are Not Active: Both $P_{A,i}$ and $P_{C,i}$ are zeros in this case. Consequently, $\dot{\omega}_i = \frac{1}{M_i}\left[-D_i\omega_i - \Delta P_i\right]$. Then, the relative normalized frequency of Generator i at time t can be represented as

$$\begin{aligned} \omega_i(t) &= \frac{1}{M_i}\int_{t_0}^{t}\left[-D_i\omega_i - \Delta P_i\right]\,\mathrm{d}t + \omega_i(t_0) \\ &:= \omega_{i,0}(t)\,, \end{aligned} \tag{4}$$

where $\omega_i(t_0)$ is the frequency of the generator at the beginning of the interval. The absolute value of Generator i's frequency in this case is $|\omega_i(t)| = |\omega_{i,0}(t)|$.

2) Case 2: Attack Is Active and Control Is Not Active: The value of $P_{C,i}$ is zero in this case, so $\dot{\omega}_i = \frac{1}{M_i}\left[-D_i\omega_i - \Delta P_i + P_{A,i}\right]$. The value of $P_{A,i}$ is assumed to be constant during the ΔT duration. Moreover, the sign of $\omega_{i,0}(t)$ in Eq. (4) is calculated at the beginning of ΔT, and $P_{A,i}$ is given the same sign. In other words

$$P_{A,i} = \begin{cases} U_{A,i} & \text{if } \omega_{i,0}(t) \geq 0 \\ -U_{A,i} & \text{if } \omega_{i,0}(t) < 0\,, \end{cases} \tag{5}$$

where $U_{A,i} > 0$ is the amount of power the attacker can control at the external power source of Generator i. The external power source actually injects power in the system if $P_{A,i}$ is positive while it absorbs power from the grid if $P_{A,i}$ is negative. Accordingly, the frequency of the generator at the end of ΔT will be

$$\begin{aligned} \omega_i(t) &= \frac{1}{M_i}\int_{t_0}^{t}\left[-D_i\omega_i - \Delta P_i + P_{A,i}\right]\,\mathrm{d}t + \omega_i(t_0) \\ &= \omega_{i,0}(t) + g_i\,P_{A,i}\,, \end{aligned} \tag{6}$$

and because $\omega_{i,0}(t)$ and $P_{A,i}$ have the same sign, the absolute value of the normalized frequency of Generator i becomes

$$|\omega_i(t)| = |\omega_{i,0}(t)| + g_i\,U_{A,i}\,. \tag{7}$$

It is noted here that $|\omega_i(t)| > |\omega_{i,0}(t)|$ because of the action of the attacker. However, the relative normalized frequency of a generator is zero during normal operations; consequently, the attacker increases the instability of the power system by increasing the deviation of the system generators from the stability margin.

3) Case 3: Attack Is Not Active and Control Is Active: There is no disturbance from the attacker in this case, and so $\dot{\omega}_i = \frac{1}{M_i}\left[-D_i\omega_i - \Delta P_i + P_{C,i}\right]$. The value of $P_{C,i}$ is constant during the ΔT interval, and it has an opposite sign to that of $\omega_{i,0}(t)$ in Eq. (4) (i.e., the opposite action to that of the attacker). Mathematically, $P_{C,i}$ is represented as

$$P_{C,i} = \begin{cases} -U_{C,i} & \text{if } \omega_{i,0}(t) > 0 \\ U_{C,i} & \text{if } \omega_{i,0}(t) < 0\,, \end{cases} \tag{8}$$

where $U_{C,i} > 0$ is the amount of real power the stabilizing controller can inject in (absorb from) the power grid at Generator i. Further, in order for the controller to be effective, the power injected or absorbed by the controller should not change the sign of the generator's frequency at the end of ΔT; i.e., $U_{C,i} \leq \frac{1}{g_i}|\omega_{i,0}(t)|$ for each ΔT. Accordingly, the relative normalized frequency of the generator is expressed as

$$\begin{aligned} \omega_i(t) &= \frac{1}{M_i}\int_{t_0}^{t}\left[-D_i\omega_i - \Delta P_i + P_{C,i}\right]\,\mathrm{d}t + \omega_i(t_0) \\ &= \omega_{i,0}(t) + g_i\,P_{C,i}\,. \end{aligned} \tag{9}$$

Because $P_{C,i}$ and $\omega_{i,0}(t)$ have opposite signs, the absolute value of Generator i's frequency is found as

$$|\omega_i(t)| = |\omega_{i,0}(t)| - g_i\,U_{C,i}\,. \tag{10}$$

Accordingly, $|\omega_i(t)| < |\omega_{i,0}(t)|$ due to the action of the stabilizing controller. Because $|\omega_i(t)|$ is getting smaller, the controller is actually driving the power system closer to stability.

4) Case 4: Both Attack and Control Are Active: Contributions from both the attacker and the stabilizing controller affect the dynamics of the power system in this case. Consequently, $\dot{\omega}_i = \frac{1}{M_i}\left[-D_i\omega_i - \Delta P_i + P_{A,i} + P_{C,i}\right]$. During the interval ΔT, the value of $P_{A,i}$ is constant and has the same sign to that of $\omega_{i,0}(t)$ while the value of $P_{C,i}$ is constant and has an opposite sign to that of $\omega_{i,0}(t)$ as previously shown in Eqs. (5) and (8). As a result, the relative normalized frequency of Generator i at the end of ΔT will be equal to

$$\omega_i(t) = \omega_{i,0}(t) + g_i\,P_{A,i} + g_i\,P_{C,i}\,, \tag{11}$$

and the absolute value of $\omega_i(t)$ will in this case be

$$|\omega_i(t)| = |\omega_{i,0}(t)| - g_i\,\left(U_{C,i} - U_{A,i}\right)\,. \tag{12}$$

Because $U_{C,i} > U_{A,i}$, then $|\omega_i(t)| < |\omega_{i,0}(t)|$. This result means that the power system gets closer to stability in this case even though the attacker is active in this interval; however, the gain achieved by the controller in stabilizing the frequency of Generator i in *Case 4* (i.e., $g_i\,U_{C,i} - g_i\,U_{A,i}$) is less than that achieved in *Case 3* (i.e., $g_i\,U_{C,i}$).

III. Game-Theoretic Control Approach

Consider a 2×2 iterated game with the one stage game shown in Fig. 2. The game is formulated for each generator under attack and it has two players; the controller (the row player) and the attacker (the column player). Each round of the game corresponds to a time interval ΔT. In each round, the players choose from two actions $\{1, 2\}$. Let n_1 denote an action of the controller and n_2 denote an action of the attacker. For the controller, a value of $n_1 = 1$ refers to an action to stabilize the power system via injecting (absorbing) power in (from) the generator, while $n_1 = 2$ indicates that the controller stays idle in that round. For the attacker, a value of $n_2 = 1$ means that the attacker injects (absorbs) power to destabilize the generator, and stays idle otherwise.

In any given round, payoff of the game is defined as the absolute value of the generator's frequency at the end of that round. The payoff matrix for all possible action combinations is shown in Fig. 2. As discussed in the previous section, whenever the attacker injects (absorbs) power according to Eq. (7), the frequency of the generator drifts away from the stability margin. On the other hand, an action by the controller drives the frequency closer to that margin as indicated by Eq. (8). In the face of such attacks, the controller aims at driving the power system into stability using a reactive strategy that will be presented in the sequel.

Attacker / Controller	$n_2 = 1$	$n_2 = 2$
$n_1 = 1$	$\lvert\omega_{i,0}(t)\rvert + g_i\left(U_{A,i} - U_{C,i}\right)$	$\lvert\omega_{i,0}(t)\rvert - g_i U_{C,i}$
$n_1 = 2$	$\lvert\omega_{i,0}(t)\rvert + g_i U_{A,i}$	$\lvert\omega_{i,0}(t)\rvert$

Fig. 2. Payoff matrix of Generator i

Zero-Determinant Strategies for Iterated Games

Zero-determinant games refer to strategies used in iterated 2×2 games in which the players can control their own long-term payoff or the payoff of their opponent [9]. Consider the previous game and define the state of the game in any given round by the actions of the players in that round. Let the number of the current game round be termed as q, let $\boldsymbol{n}(q) = (n_1, n_2)$ denote the state of the game in round q, and let $\boldsymbol{S} = \{(1,1), (1,2), (2,1), (2,2)\}$ denote the state space of the game. It is shown in [9] that, for any iterated game, a player with longer memory of the history of the game has no advantage over the player with shorter memory. Thus, players can condition their moves on the state of the game in the previous round and the game can be modeled as a Markov chain, where

$$p_C^{\boldsymbol{k}} = \mathbb{P}(n_1(q+1) = 1 \mid \boldsymbol{n}(q) = \boldsymbol{k}),\ \forall \boldsymbol{k} \in \boldsymbol{S}$$

denote the probability that the controller takes action 1 in round $q+1$ if the state of the game was $\boldsymbol{k}$ in the previous round. In the same manner, the conditional probability for the attacker is

$$p_A^{\boldsymbol{k}} = \mathbb{P}(n_2(q+1) = 1 \mid \boldsymbol{n}(q) = \boldsymbol{k}),\ \forall \boldsymbol{k} \in \boldsymbol{S}\,.$$

The Markov chain has a unique stationary distribution $\boldsymbol{\pi}^T = (\pi_{1,1}, \pi_{1,2}, \pi_{2,1}, \pi_{2,2})$, where $\pi_{k,j}$ is the probability that the game is in state (k,j). In this regard, let $X_{k,j}$ denote the payoff of the game if the controller chooses $n_1 = k$ and the attacker chooses $n_2 = j$. The average long-term payoff is thus given by

$$u_X = \boldsymbol{\pi}^T \hat{\boldsymbol{X}}\,,$$

where $\hat{\boldsymbol{X}} = (X_{1,1}, X_{1,2}, X_{2,1}, X_{2,2})^T$. It is shown in [9] that if the $p_C^{\boldsymbol{k}}$'s are chosen such that

$$a\hat{\boldsymbol{X}} + b = \left(-1 + p_C^{1,1}, -1 + p_C^{1,2}, p_C^{2,1}, p_C^{2,2}\right)^T\,,$$

where a and b are arbitrary real numbers, then the row player (i.e., the controller) can achieve u_X regardless of the actions of the column player (the attacker). The range of values of u_X that can be achieved is defined in [13]. Namely, for 2×2 games that admit a structure where the minimum value of one row of the payoff matrix exceeds the maximum value of the other row, it is shown that u_X can be fixed at any value in the range between those two values. In specific, let $X_{l,max}$ and $X_{l,min}$ denote the maximum and minimum values of the row of the payoff matrix with $n_1 = l$. Then, if $X_{l,max} < X_{m,min}$ for $l \neq m$, then u_X can be fixed at any value in the interval $[X_{l,max}, X_{m,min}]$.

Note that in the game in Fig. 2, $|P_{C,i}| > |P_{A,i}|$ and thus,

$$\begin{array}{rcl} X_{1,max} & = & |\omega_{i,0}(t)| + g_i\, U_{A,i} - g_i\, U_{C,i} \\ X_{1,min} & = & |\omega_{i,0}(t)| - g_i\, U_{C,i} \\ X_{2,max} & = & |\omega_{i,0}(t)| + g_i\, U_{A,i} \\ X_{2,min} & = & |\omega_{i,0}(t)|\,. \end{array} \tag{13}$$

Furthermore, note that $X_{1,max} < X_{2,min}$ and thus, u_X can be fixed at any value in the range $[X_{1,max}, X_{2,min}]$ (i.e., $|\omega_{i,0}(t)| + [g_i\, U_{A,i} - g_i\, U_{C,i}\,,\, 0]$). To achieve a specific u_X, the controller has to apply the following strategy in each round [13]

$$\begin{array}{rcl} p_C^{1,1} & = & 1 + \left(1 - \frac{X_{1,1}}{u_X}\right) b \\ p_C^{1,2} & = & 1 + \left(1 - \frac{X_{1,2}}{u_X}\right) b \\ p_C^{2,1} & = & \left(1 - \frac{X_{2,1}}{u_X}\right) b \\ p_C^{2,2} & = & \left(1 - \frac{X_{2,2}}{u_X}\right) b\,, \end{array} \tag{14}$$

where b is such that

$$\max\left(\frac{-1}{1 - \frac{X_{1,min}}{u_X}}\,,\, \frac{1}{1 - \frac{X_{2,max}}{u_X}}\right) \leq b < 0\,. \tag{15}$$

It is important to emphasize that the game under consideration is dynamic, i.e., the payoff matrix can change over the course of the game. This can be observed since $|\omega_{i,0}(t)|$ changes every ΔT; however, the previous strategy does not depend on $|\omega_{i,0}(t)|$ as will be seen in Eq. (18).

Let a feasible value of u_X be represented as

$$u_X = |\omega_{i,0}(t)| + \alpha\left(g_i\, U_{A,i} - g_i\, U_{C,i}\right), \tag{16}$$

where $0 \leq \alpha \leq 1$ is referred to as the persistence factor. A high value of α means that u_X is closer to $|\omega_{i,0}(t)| + g_i\, U_{A,i} - g_i\, U_{C,i}$ indicating that the controller is more aggressive in driving the frequency of the generator to stability.

Given the results of Eqs. (13) and (16), and for the case of an aggressive stabilizing controller (i.e., $\alpha \geq \frac{1}{2}$), it can be shown that

$$1 - \frac{X_{1,min}}{u_X} \geq \frac{X_{2,max}}{u_X} - 1\,.$$

Consequently, for $\alpha \geq \frac{1}{2}$, the valid range for b in Eq. (15) can be represented as

$$b_{min} \leq b < 0\,,$$

where

$$b_{min} = \frac{1}{g_i} \frac{|\omega_{i,0}(t)| + \alpha g_i \left(U_{A,i} - U_{C,i}\right)}{\alpha \left(U_{A,i} - U_{C,i}\right) - U_{A,i}} \, .$$

The system operator can specify a fixed value of b within the valid range as $b = \beta b_{min}$, where $0 < \beta \leq 1$ is referred to as the steering factor. Therefore, the exact value of b can be expressed as

$$b = \frac{\beta}{g_i} \frac{|\omega_{i,0}(t)| + \alpha g_i \left(U_{A,i} - U_{C,i}\right)}{\alpha \left(U_{A,i} - U_{C,i}\right) - U_{A,i}} \, . \tag{17}$$

At the beginning of a new round, the controller is assumed to know the action of the attacker in the previous round (i.e., whether the attacker was active or idle). Using the results of Eqs. (14), (16), and (17), the strategy of the controller is given as

$$\begin{array}{rcl} p_i^{1,2} & = & \frac{(\alpha-\beta+\alpha\beta)U_{C,i}+(1-\alpha-\alpha\beta)U_{A,i}}{\alpha U_{C,i}+(1-\alpha)U_{A,i}} \\ p_i^{1,1} & = & p^{1,2} + \frac{\beta U_{A,i}}{\alpha U_{C,i}+(1-\alpha)U_{A,i}} \\ p_i^{2,1} & = & \beta \\ p_i^{2,2} & = & \frac{\alpha\beta(U_{C,i}-U_{A,i})}{\alpha U_{C,i}+(1-\alpha)U_{A,i}} \, . \end{array} \tag{18}$$

Furthermore, for the special case of $\alpha = 1$, the strategy can be expressed as

$$\begin{array}{rcl} p_i^{1,1} & = & 1 \\ p_i^{1,2} & = & 1 - \beta\frac{U_{A,i}}{U_{C,i}} \\ p_i^{2,1} & = & \beta \\ p_i^{2,2} & = & \beta(1 - \frac{U_{A,i}}{U_{C,i}}) \, . \end{array} \tag{19}$$

In other words, $p_i^{1,2} = p_i^{1,1} - \beta\frac{U_{A,i}}{U_{C,i}}$ and $p_i^{2,2} = p_i^{2,1} - \beta\frac{U_{A,i}}{U_{C,i}}$. This means that if the attacker does not take a destabilizing action against Generator i during a specific time interval, the controller reduces the probability of taking an action to stabilize the power system by $\beta\frac{U_{A,i}}{U_{C,i}}$ in the subsequent round.

It is to be noted that if the controller takes a stabilizing action all the time regardless of the actions of the attacker (i.e., the probability of taking a stabilizing action is always 1 regardless of the value of n_2), then the average long-term payoff will be in the range $|\omega_{i,0}(t)| - g_i U_{C,i} + [0, g_i U_{A,i}]$, which can be better than the average long-term payoff attained by using the game-theoretic approach. However, the game-theoretic control approach gives the system operators a guarantee of an acceptable system performance while meeting constrains on the availability or the cost of the external power sources.

IV. Numerical Results

In this section, the WECC power system in Fig. 1 is considered where it is assumed that each generator is equipped with an external fast-acting power source. Stability time of a generator is measured by finding the difference between the time after which the frequency of the generator is restricted to a 2% threshold (i.e., time when the maximum relative normalized frequency of the generator is limited to ±0.02 pu) and the time when the stability controller is activated.

The power system is assumed to be attack-free from $t = 0$ to $t = 0.5$ seconds. Then, a cyber switching attack targets Generator 2 for 7 seconds (i.e., from t = 0.5 to t = 7.5 seconds). The stabilizing controller is activated on the three generators at t = 0.7 seconds. The controller is deactivated when both the power system is stable and the cyber attack is finished. The attacker injects or absorbs 0.1-pu real power at the external power source of Generator 2 every 50 msec during the attack duration. Further, the controller is limited to inject or absorb real power of 0.2 pu at the external power sources every 50 msec as well. Each round of the game is a 50-msec interval which will be called the game interval. Consequently, ΔT = 0.05, $U_{A,2}$ = 0.1, and $U_{C,i}$ = 0.2, where i = $1, 2, 3$.

In order to fulfill its destabilizing switching attack, the attacker controls the switch of the fast-acting power source at Generator 2. At the end of each interval, the attacker employs Eq. (5) to determine if it needs to absorb or inject power, using the external power source, in the next interval. In addition, the attacker does not change the value of $P_{A,2}$ during the interval (i.e., the attacker uses a step-wise function during each interval). The strategy of the controller is characterized by Eq. (18). Moreover, if the stabilizing controller has to take an action in the next interval, the controller uses Eq. (8) to calculate its contribution to the power system generators. The controller affects the fast-acting external power sources at the system generators in order to stabilize the power system.

As a benchmark, Fig. 3 shows the normalized relative frequency and phase of the system generators when the stabilizing controller constantly takes an action regardless of the action of the attacker in the previous interval (i.e., the probability of the controller taking an action in each game interval is 1 regardless of the value of n_2). Table II displays the performance measures of the power system. It is noted the average stability time of the three generators is around 7.19 second, which means that the power system is driven to stability within about 390 msec from the end of the cyber attack.

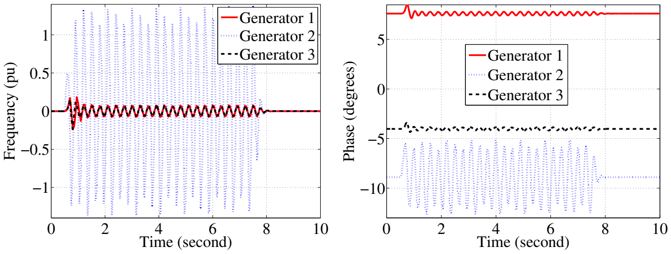

Fig. 3. System performance when controller acts all the time

Stability time of the system generators and the average power used by the stabilizing controller versus the controller's persistence factor (α) are shown in Fig. 4; in this case, a value of β = 0.5 is used. As noted in Eq. (16), the value of α determines the long-term payoff of the game, where a high value of α means that the system generators will be stabilized faster. The results of this figure demonstrate the

Measure Generator	Stability Time (second)	Control Power (pu)
Generator 1	7.208	0.100
Generator 2	7.247	0.191
Generator 3	7.119	0.060

TABLE II
PERFORMANCE BENCHMARK

tradeoff between the stability time and the required control power. Further, the system operator can choose the value of α such that an acceptable stability time is achieved while the budget of the external power sources (for example, cost or availability) is met.

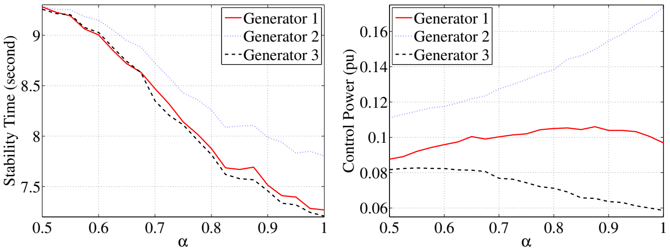

Fig. 4. System performance versus the persistence factor

Fig. 5 shows the performance measures versus the steering factor of the controller (i.e., β) for a value of $\alpha = 0.75$. It is observed that β does not have a substantial effect on the performance. Because β affects the controller's action probability as shown in Eq. (14), results of this figure show that the controller achieves the target long-term average (i.e., $\lim_{t\to\infty} \omega_i(t) = 0$) as long as $b_{min} \leq b < 0$. The results also show that the system operator has more flexibility in designing the stabilizing controller.

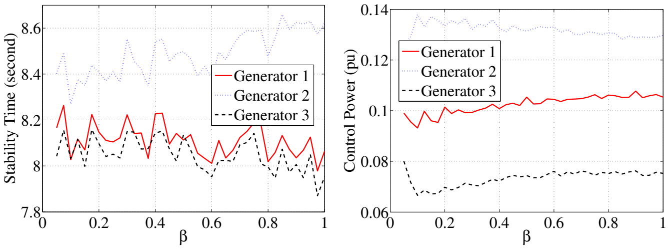

Fig. 5. System performance versus the steering factor

V. CONCLUSIONS

This paper proposed a parametric game-theoretic controller to stabilize power systems during and after a switching attack. The attacker conducts its destabilizing act by switching an external power source between injecting and absorbing real power, and the attacker only needs to calculate the frequency of the targeted generator in order to run the attack. Further, the stabilizing controller relies on receiving timely system updates in order to affect the output of external power sources. In this regard, we modeled the interaction between the attacker and the controller as an iterated game and devised reactive strategies to stabilize the power system.

The strategy of the stabilizing controller was characterized for this setup. The merits of the proposed controller were investigated on the WECC 3-generator power system. Numerical results detailed the system performance metrics versus the parameters of the stabilizing controller. The results of this work show the effectiveness of the proposed controller in keeping the power system stable during and after the switching attack.

ACKNOWLEDGMENT

This work was supported in part by the National Science Foundation under grant ECCS-1028246 and the Natural Sciences and Engineering Research Council of Canada.

REFERENCES

[1] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "Switched System Models for Coordinated Cyber-Physical Attack Construction and Simulation," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 49–54, 2011.

[2] S. Liu, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "Coordinated Variable Structure Switching Attack in the Presence of Model Error and State Estimation," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 318–323, 2012.

[3] S. Liu, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "Coordinated Variable Structure Switching in Smart Power Systems: Attacks and Mitigation," in *International Conference on High Confidence Network Systems (HiCoNS) at Cyber Physical Systems Week (CPSWeek)*, pp. 21–30, 2012.

[4] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "A Smart Grid Vulnerability Analysis Framework for Coordinated Variable Structure Switching Attacks," in *IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–6, 2012.

[5] J. Wei, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "A Flocking-Based Dynamical Systems Paradigm for Smart Power System Analysis," in *IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–8, 2012.

[6] J. Wei and D. Kundur, "Two-Tier Hierarchical Cyber-Physical Security Analysis Framework For Smart Grid," in *IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–5, 2012.

[7] J. Wei, D. Kundur, and T. Zourntos, "On the Use of Cyber-Physical Hierarchy for Smart Grid Security and Efficient Control," in *IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, pp. 1–6, 2012.

[8] J. Wei, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "Probing the Telltale Physics: Towards a Cyber-Physical Protocol to Mitigate Information Corruption in Smart Grid Systems," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 372–377, 2012.

[9] W. H. Press and F. J. Dyson, "Iterated Prisoner's Dilemma contains strategies that dominate any evolutionary opponent," *Proceedings of the National Academy of Sciences*, vol. 109, pp. 10409–10413, June 2012.

[10] F. Dörfler and F. Bullo, "Synchronization and Transient Stability in Power Networks and Non-Uniform Kuramoto Oscillators," in *American Control Conference (ACC)*, pp. 930–937, 2010.

[11] P. M. Anderson and A. A. Fouad, *Power System Control and Stability*. IEEE Power Systems Engineering Series, IEEE Press, 1994.

[12] A. R. Bergen and V. Vittal, *Power Systems Analysis*. Prentice-Hall, second ed., 2000.

[13] A. Al Daoud, G. Kesidis, and J. Liebeherr, "An Iterated Game of Uncoordinated Sharing of Licensed Spectrum Using Zero-Determinant Strategies," *arXiv preprint arXiv:1401.3373, 2014*. To appear at IEEE Journal on Selected Areas in Communications (J-SAC) - Cognitive Radio Series, November 2014 Issue.