A Game-Theoretic Analysis of Cyber Switching Attacks and Mitigation in Smart Grid Systems

Abdallah Farraj, *Member, IEEE,* Eman Hammad, *Student Member, IEEE,*
Ashraf Al Daoud, and Deepa Kundur, *Fellow, IEEE*

***Abstract*—We propose a framework for the analysis of cyber switching attacks and control-based mitigation in cyber-enabled power systems. Our model of the switching attack is simple, only requiring knowledge of the sign of the local relative rotor speed, which may be estimated. The controller is modeled to be resource constrained, choosing to act only during select intervals of time. We make use of an iterated game-theoretic formulation to describe the interactions of the parties and its effect on system stability. Analytic results indicate the potential of the constrained controller to achieve transient stabilization over time using zero-determinant strategies. Numerical results of the New England 39-bus power system demonstrate the potential for such a controller to increase system resilience during cyber-attacks.**

***Index Terms*—Cyber-physical systems, game theory, iterated games, smart grid, stabilizing control, switching attacks, system resilience, zero-determinant strategies.**

I. Introduction

THE RAPIDLY growing nature of the smart grid and its ever-changing threat landscape have thrust cyber-security challenges to the forefront of smart grid system development. Evolving regulations and technical alternatives provide unprecedented opportunities for stakeholders to address cyber-physical security concerns. One role research can play within this hurried environment is to provide general guidelines and strategies for identification of attack and mitigation.

In this paper, we focus on the development of an analysis framework to model the interaction of switching-based attacks on power systems and local control strategies for mitigation. Cyber switching attacks represent a growing class of cyber-physical attacks within the research community that aim to destabilize the state of a target power system component via controlled switching of circuit breakers in the proximity of the target [1], [2]. Here, an opponent would eavesdrop on local sensor readings and estimate the state of the target to compute destabilizing switching action that is implemented through false data injection of breaker control signals.

Strategies to mitigate against such cyber-physical attacks are emerging and we focus on the use of distributed control-based paradigms in this paper. Distributed controllers represent a valuable and expanding asset base from which to improve system resilience. Recent results [3]–[6] have demonstrated the usefulness of distributed control paradigms that leverage fast-acting power sources such as storage devices. The performance of the controller, however, is strongly related to its ability to receive high-granularity real-time data.

Prior art has recently begun to consider game-theoretic-based modeling of cyber-security problems within cyber-physical systems. An iterative zero-sum game is used in [7] to model security policies at the cyber-level with corresponding optimal control response at the physical layer. A zero-sum game with a mixed strategies model is developed in [8] to formulate cyber-physical systems survivability, where the attacker (defender) plays over resources being disrupted (maintained/restored). Siever *et al.* [9] formulated the placement and utilization of unified power flow controllers (UPFCs) in a power transmission system as an iterative game. In response to attackers tripping transmission lines, the defender optimizes the installation locations of the UPFCs to maximize the amount of power delivered over all attacks to which the system is most vulnerable. A game-theoretic formulation of the risk dynamics of false data injection attacks (through overcompensation) targeting automatic generation control is developed in [10], where it adopts a zero-sum Markov security game model and defines risk states as function of the probability of attack and the potential impact corresponding to the attack.

Thus, previous work has focused on strategic behavior of players who have full knowledge of the payoff matrix of each other and full system state knowledge. In addition, most of these models have prioritized formulating the player interactions at the decision-making level over integrating physical system models. While some results do hypothesize a response of optimal control, there is a need to study concrete examples of incorporating controller dynamics. The proposed work in this paper is the first to illustrate a practical smart grid stabilizing controller that makes no assumptions on attacker actions, nor on full system state knowledge. The only assumption required is that the attacker has more limited resources than the electric power utility (EPU), an assumption common in spirit

Manuscript received November 26, 2014; revised April 14, 2015; accepted May 24, 2015. Date of publication June 17, 2015; date of current version June 17, 2016. This work was supported in part by the National Science Foundation under Grant ECCS-1028246, and in part by the Natural Sciences and Engineering Research Council of Canada under Grant RGPIN 227722. Paper no. TSG-01169-2014.

A. Farraj, E. Hammad, and D. Kundur are with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: abdallah@ece.utoronto.ca; ehammad@ece.utoronto.ca; dkundur@ece.utoronto.ca).

A. Al Daoud is with TELUS Communications, Toronto, ON M5J 2V5, Canada (e-mail: ashraf.al_daoud@telus.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2015.2440095

to many security threat models in the literature. Another novel aspect of this paper is that it represents a first look at integrating a game-theoretic foundation with a smart grid dynamical system description to study the system behavior in mitigating various classes of cyber-physical attacks.

Specifically, this paper addresses an analysis of the dynamic interaction of switching attacks and distributed control for attack mitigation. In contrast to much of the former smart grid security related work that focuses on aggressive approaches of attack and mitigation, we aim to incorporate constraints of both attacker and EPU leading to more conservative interactions. The limited sampling rate of sensor readings leveraged by both opponent and EPU is explicitly modeled; thus, we do not assume the availability of a continuous-stream of data. The bound on available energy resources or cost for the opponent (controller) is articulated as the process of selective participation in the attack (mitigation) process; thus, either party can choose to be active using available resources or idle hence conserving. Moreover, the opponent is not required to know the entire state of the target component to apply the attack effectively. Similarly, the distributed controller is assumed to take action based on only local information during the attack.

This paper provides a dynamical model that describes the interaction between the EPU and the attacker and the impact of their strategies on system stability. Namely, this interaction is modeled as a 2 × 2 iterated game, where, at each round of the game, the EPU 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 memories. In this regard, iterated games lend themselves to Markovian strategies referred to as zero-determinant strategies [11]. With such strategies, players can control their own long-term payoff or that of their opponent based on the structure of the payoff matrix of the game. In this paper, we deduce such strategies that allow the EPU to stabilize the power system in light of such attacks.

The remainder of this paper is organized as follows. Section II introduces our framework of study. Game-theoretic analysis is presented in Section III followed by simulation results on the 39-bus New England system in Section IV. Discussion is found in Section V and the conclusion is drawn in Section VI.

II. Analytical Framework

We consider a cyber-physical smart grid system that is comprised of a physical component such as the power transmission network shown in Fig. 1(a) and a cyber-component that includes a set of measurement devices, their corresponding communication infrastructure, and a control center that processes measurements and makes decisions. We assume the existence of N synchronous generators each equipped with one or more local external fast-acting storage units (such as flywheels) that can effectively inject or absorb power at the generator bus based on control signals as illustrated in Fig. 1(b). Each distributed storage unit is considered to have three possible modes of operation: 1) absorbing; 2) injecting; or 3) idle.

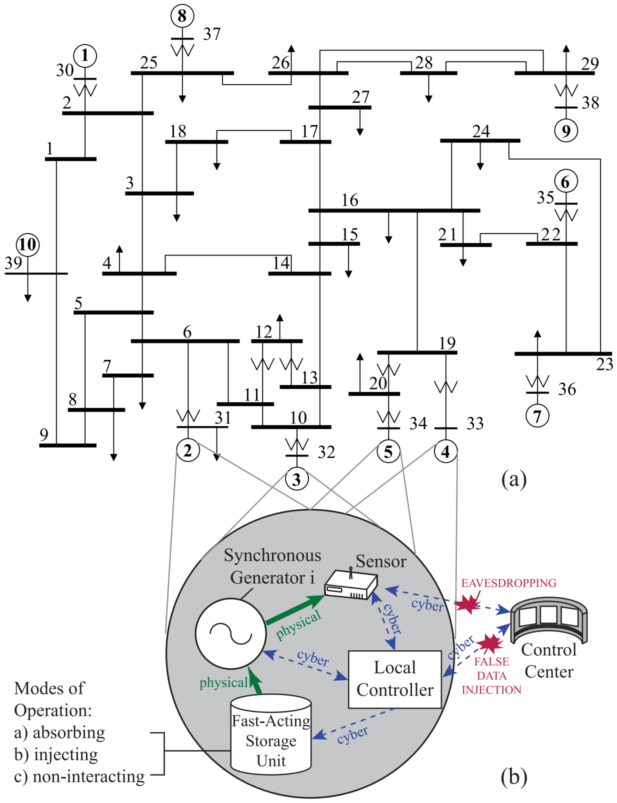

Fig. 1. (a) Traditional New England power system. (b) Cyber-enablement with local storage; possibilities for attack exist on a subset of components.

TABLE I
System Parameters

Parameter	Description
E_i	internal voltage of Generator i, $\forall i \in \{1,\ldots,N\}$
$P_{e,i}$	electrical power of Generator i
$P_{m,i}$	mechanical power of Generator i
δ_i	rotor angle of Generator i
ω_i	relative normalized rotor speed of Generator i
X'_{di}	direct-axis transient reactance of Generator i
G_{ii}	equivalent shunt conductance of Generator i
M_i	inertia of Generator i
D_i	damping coefficient of Generator i

A. Physical Power System Model

A schematic of the New England 39-bus power system is shown in Fig. 1 for $N = 10$; the system parameters are summarized in Table I, where M_i and D_i are expressed in seconds, δ_i is expressed in radians, and the remaining parameters are in per unit values. We note that the relative normalized rotor speed of generator i is defined as $\omega_i = (\omega_i^{\text{act}} - \omega^{\text{nom}})/\omega^{\text{nom}}$, where ω^{nom} is the desired nominal angular rotor speed (in radians per second) of the generator and ω_i^{act} is the actual angular rotor speed of generator i (in radians per second).

In this paper we focus, in part, on the impacts of attacks and mitigation on the transient stability of the power system. Thus, we employ a swing equation model for synchronous generators. Along with a Kron-reduced representation of physical network relationships, this model has recently demonstrated great potential for modeling issues of power system performance and stability [3], [6], [12], [13].

Let $\dot{\delta}_i$ and $\dot{\omega}_i$ denote time derivatives of δ_i and ω_i, respectively. The swing equation model for generator i (assuming no power control such as a governor) within an interconnected power system can be expressed as [12], [14]

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

where the electrical power of generator i $P_{e,i}$ is [15]

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

Here, it is assumed that $G_{ik} = G_{ki} \geq 0$ is the Kron-reduced equivalent conductance between generators i and k, $B_{ik} = B_{ki} > 0$ is the Kron-reduced equivalent susceptance between generators i and k, and $Y_{ik} = G_{ik} + \sqrt{-1}\,B_{ik}$ is the Kron-reduced equivalent admittance between generators i and k (all in per unit values). Let $\phi_{ik} = \arctan(G_{ik}/B_{ik})$ and $P_{ik} = |E_i|\,|E_k|\,|Y_{ik}|$, then

$$P_{e,i} = |E_i|^2\,G_{ii} + \sum_{k=1,\,k\neq i}^{N} P_{ik}\,\sin(\delta_i - \delta_k + \phi_{ik}). \tag{3}$$

B. Switching Attack Model

Both cyber-attack and mitigation decision-making occur in the cyber-domain as presented in Fig. 1(b). In contrast to the physical system, the cyber-infrastructure is discrete-time. Thus, each party will act (or not) based on time-sample estimates of ω_i. We let the interval between adjacent time instants employed be ΔT (ranging from the order of milliseconds to minutes depending on the type of sensor and attacker/EPU).

We consider an attacker who aims to impact a set of target synchronous generators by gaining control of their corresponding storage units using knowledge of their local rotor speed (via cyber-intrusion); several recent publications discuss the possibility of such intrusion [16], [17]. For instance, eavesdropping of local quantities can be employed to gain estimates of generator's rotor speed as recently demonstrated. Moreover, false data injection attacks may be imposed to control switches of storage units. The types of cyber-intrusion necessary to be able to execute such attacks are specific to the actual protocols, software and hardware architecture and is beyond the scope of this paper.

As discussed in the introduction, we consider a situation in which the opponent aims to balance the following objectives.

1) Imposing instability on the rotor speed of one or more target synchronous generators; in general, an attacker may aim to destabilize the system in a number of ways, but our focus in this paper is on rotor speed, which we believe will still shed some general insights on effective attack and mitigation.
2) Conserving storage resources to suit availability of local resources; an aggressive attack may drain storage rapidly thus limiting the ability of the opponent at an opportune time interval.
3) Remaining stealthy to discourage premature tripping by protection devices that would limit the attack scale; we assert that a desirable strategy would be for the attacker to subtly impose interarea oscillatory-type behavior to create a large-scale disturbance in contrast to aggressive short-term attacks that create high transients initiating relay protection.

Given the recent interest in switching attacks [18]–[20], we assume that the opponent actions impact the power system through a modulating sequence of possible injections. Specifically at time t an active attacker applies

$$P_{A,i} = \begin{cases} +\Gamma_{i,1} & \text{if } \omega_{i,0} \geq 0 \\ -\Gamma_{i,2} & \text{if } \omega_{i,0} < 0 \end{cases} \tag{4}$$

where $\Gamma_{i,1}$ and $\Gamma_{i,2} \geq 0$ are the power injected or absorbed by the storage device at generator i, respectively, based on the value of the relative normalized rotor speed at time $t_0 = t - \Delta T$ (and gleaned by the attacker through intrusion). We argue that (4) effectively models the spirit of a variety of approaches for system destabilization because (as shown in Section II-D) it promotes the deviation of ω_i from its nominal value within the time interval ΔT.

The reader should note that the opponent, to conserve energy or remain stealthy, may choose not to act, in which case the attacker is idle and $P_{A,i} = 0$.

C. EPU Stabilizing Control

An EPU can typically respond to attack impacts through a variety of technologies including fast-acting protection and distributed control. The former has the effect of power grid reduction with possible negative impacts to power delivery. The latter typically requires the attack be first detected and characterized, which may be difficult if the attack is stealthy as highlighted above.

Thus, in this paper, we consider the scenario whereby the EPU makes use of a simple local control strategy involving select (and uncorrupted) storage units that could perpetually aid in stabilization of incidental disturbances while more aggressively tackles the impacts of cyber-attack. We assume that the control is local and makes use of knowledge of the rotor speed of each associated synchronous generator as well as the attacker action (i.e., active or idle) in the previous interval; recent results have demonstrated the ability of an opponent to estimate such quantities for cyber-attack [1]. We assert that this approach provides both resilience to attack and has the potential to indicate the onset of an attack using controller statistics.

Given that the EPU control may be persistent and aims to locally push the rotor speed to its nominal value, it is important to conserve storage resources especially when being fed by a highly variable renewable resource and when operating costs are limited. Thus, the EPU control may not always choose to be active. If active, we model the impact of EPU control at time t as

$$P_{C,i} = \begin{cases} -\Lambda_{i,2} & \text{if } \omega_{i,0} > 0 \\ +\Lambda_{i,1} & \text{if } \omega_{i,0} < 0 \end{cases} \tag{5}$$

where $\Lambda_{i,1}$ and $\Lambda_{i,2} \geq 0$ are the amount of power the stabilizing controller is injecting into (absorbing from) the power grid at generator i based on the value of the rotor speed at time t_0 (acquired by the EPU). As shown in Section II-D, this action has the effect of helping move ω_i to its desired nominal value and thus represents in spirit the local time action of a broad class of mitigation strategies. If idle, we set $P_{C,i} = 0$.

D. Switching Attack and Stabilizing Controller Models

We let $\Delta P_i = P_{e,i} - P_{m,i}$ and $g_i = (\Delta T / M_i) > 0$. The impact of attack and mitigation at generator i can be modeled as terms on the right side of (1) [3], [6]

$$\begin{aligned} \dot{\delta}_i &= \omega_i \\ \dot{\omega}_i &= \frac{1}{M_i}\left[-D_i\omega_i - \Delta P_i + P_{A,i} + P_{C,i}\right] \end{aligned} \tag{6}$$

where $P_{A,i}$ and $P_{C,i}$ represent the effect of the attacker and the EPU controller, respectively. A positive value of $P_{A,i}$ ($P_{C,i}$) implies that the attacker (EPU controller) injects real power at the bus of generator i, and a negative value indicates absorption.

Given that the attacker and the EPU controller may each be active or idle, we consider four possibilities for action within the sampling interval ΔT and model the overall impact on relative normalized rotor speed of generator i. Specifically, we compute $\omega_i(t)$ where t is the current sample instant relative to $\omega_i(t_0)$ for $t_0 = t - \Delta T$.

1) Case 1 (Idle Attack and Control): Here, we set $P_{A,i} = P_{C,i} = 0$ in (6) and integrate from t_0 to $t = t_0 + \Delta T$ to give

$$\omega_i(t) = \int_{t_0}^{t} \frac{[-D_i\omega_i - \Delta P_i]}{M_i}\, dt + \omega_i(t_0) := \omega_{i,0}. \tag{7}$$

Thus, $|\omega_i(t)| = |\omega_{i,0}|$.

2) Case 2 (Active Attack and Idle Control): We set $P_{A,i}$ as in (4) and $P_{C,i} = 0$; integrating from t_0 to $t = t_0 + \Delta T$ gives

$$\omega_i(t) = \int_{t_0}^{t} \frac{\left[-D_i\omega_i - \Delta P_i + P_{A,i}\right]}{M_i}\, dt + \omega_i(t_0) \tag{8}$$

$$= \omega_{i,0} + g_i\, P_{A,i} \tag{9}$$

$$|\omega_i(t)| = |\omega_{i,0}| + g_i|P_{A,i}| > |\omega_{i,0}| \tag{10}$$

because $\omega_{i,0}$ and $P_{A,i}$ have the same sign in (4). It is noted that the action of the attacker moves the rotor speed away from its nominal value decreasing the stability margin as intended.

3) Case 3 (Idle Attack and Active Control): Similarly, $P_{A,i} = 0$ and $P_{C,i}$ is represented by (5). As a result

$$\omega_i(t) = \int_{t_0}^{t} \frac{\left[-D_i\omega_i - \Delta P_i + P_{C,i}\right]}{M_i}\, dt + \omega_i(t_0) \tag{11}$$

$$= \omega_{i,0} + g_i\, P_{C,i} \tag{12}$$

$$|\omega_i(t)| = |\omega_{i,0}| - g_i|P_{C,i}| \tag{13}$$

because $P_{C,i}$ and $\omega_{i,0}$ have opposite signs in (5). Accordingly, the EPU controller drives the power system closer to stability.

Attacker Controller	$n_2 = 1$ (Active)	$n_2 = 2$ (Idle)
$n_1 = 1$ (Active)	$X_{1,1}$	$X_{1,2}$
$n_1 = 2$ (Idle)	$X_{2,1}$	$X_{2,2}$

Fig. 2. Generic payoff matrix.

4) Case 4 (Active Attack and Control): Here, $P_{A,i}$ and $P_{C,i}$ are given by (4) and (5), respectively, to give

$$\omega_i(t) = \omega_{i,0} + g_i P_{A,i} + g_i P_{C,i} \tag{14}$$

$$|\omega_i(t)| = |\omega_{i,0}| - g_i\big(|P_{C,i}| - |P_{A,i}|\big). \tag{15}$$

The reader should note that if $|P_{C,i}| < |P_{A,i}|$, then the net effect on rotor speed is to deviate further from the nominal value (i.e., $|\omega_i(t)| > |\omega_{i,0}|$). For $|P_{C,i}| \geq |P_{A,i}|$, we have $|\omega_i(t)| \leq |\omega_{i,0}|$. However, the gain achieved by the controller as not as great as in case 3.

In our formulation, we assert that to conserve energy both attacker and EPU would selectively choose to remain idle. The question naturally arises as to what the long-term effects of such a mixed strategy would be on the behavior of the system. In the next section, we consider this question using a game-theoretic formulation for the case of $|P_{C,i}| \geq |P_{A,i}|$, which we believe is most relevant given that the opponent often corrupts only a small fraction of resources in comparison to the EPUs resources.

III. Game-Theoretic Analysis

A. Zero-Determinant Strategies for Iterated Games

Consider a 2×2 iterated game with the one stage game of Fig. 2. The game has two players: 1) the EPU controller (row player); and 2) the attacker (column player). At each round of the game, a player chooses from two actions $\{1, 2\}$. Let n_1 and n_2 denote an actions of the EPU controller and attacker, respectively. A value of $n_1 = 1$ or $n_1 = 2$ refers to an active or idle EPU control in a given round of the game, respectively. We have similar interpretations for $n_2 = 1$ (active attacker) and $n_2 = 2$ (idle attacker). The value $X_{j,k}$, where $j, k \in \{1, 2\}$, denotes the relative normalized rotor speed of the power generator if the EPU controller chooses $n_1 = j$ and the attacker chooses $n_2 = k$ during the current play interval.

It is shown in [11] that, in iterated games, where the same actions and the same payoff matrices are repeated, for any strategy of the player with the longer memory, the player with the shorter memory can achieve the same long-term outcome if the opponent has played a shorter memory strategy. Thus, any history outside what is shared between the two players can be disregarded; consequently, the game can be modeled as a Markov chain taken here to be a single memory step process.

In this regard, let $\boldsymbol{n}(t) = (n_1, n_2)$ denote the state of the game at round t and $\boldsymbol{S} = \{(1,1), (1,2), (2,1), (2,2)\}$ be the state space of the game. Also, let $\mathbb{P}(\cdot)$ denote the probability operator and $\boldsymbol{k} = (k_1, k_2)$, then

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

represents the probability that the EPU controller takes action 1 ($n_1 = 1$) in round $t + 1$ if in the previous round

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

Fig. 3. Payoff matrix of generator i.

the controller took action k_1 and the attacker took action k_2. In the same manner, the probability that the attacker takes action 1 ($n_2 = 1$) in round $t + 1$ is represented as

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

The Markov chain has a unique stationary distribution $\boldsymbol{\pi}^T = (\pi_{1,1}, \pi_{1,2}, \pi_{2,1}, \pi_{2,2})$, where for each $\pi_{j,k}$, j refers to an action by the EPU controller and k refers to an action by the attacker. Further, the average long-term outcome of the game, denoted as u_X, is given by [21] as $u_X = \boldsymbol{\pi}^T\hat{\boldsymbol{X}}$, where $\hat{\boldsymbol{X}} = (X_{1,1}, X_{1,2}, X_{2,1}, X_{2,2})^T$. It is shown in [11] that if the $p_C^{\boldsymbol{k}}$'s are chosen such that

$$a\hat{\boldsymbol{X}} + b = \left(-1 + p_C^{1,1}, -1 + p_C^{1,2}, p_C^{2,1}, p_C^{2,2}\right)^T \tag{16}$$

where a and b are arbitrary nonzero real numbers, then the row player can fix the value of u_X regardless of the actions of the column player (the attacker) if and only if the minimum value of one row in the payoff matrix of Fig. 2 exceeds the maximum value of the other row. In such case, as shown in [21] that the row player (i.e., the EPU controller) can fix the long-term average payoff u_X to any value in the range between the minimum and the maximum values representing a profound advantage to the EPU in an attack situation. To achieve a specific u_X, the controller has to take an action in the current interval according to the following likelihoods [21]:

$$\begin{aligned} p_C^{1,1} &= 1 + \left(1 - \frac{X_{1,1}}{u_X}\right)b, & p_C^{1,2} &= 1 + \left(1 - \frac{X_{1,2}}{u_X}\right)b \\ p_C^{2,1} &= \left(1 - \frac{X_{2,1}}{u_X}\right)b, & p_C^{2,2} &= \left(1 - \frac{X_{2,2}}{u_X}\right)b. \end{aligned} \tag{17}$$

B. Long-Term Mitigation Control

Given the objectives of system destabilization (or stabilization) by the attacker (EPU controller), we make use of the value of $|\omega_i(t)|$ to represent the payoff at the end of the interval ΔT for each party. Thus, the EPU controller aims to minimize this payoff (i.e., drive $|\omega_i(t)|$ to zero) while the attacker aims to increase payoff of targeted generators.

Let $\boldsymbol{X} = [X_{j,k}]$ denote the payoff matrix of generator i at the end of ΔT. Then, following the development of Section II-D, the values of $\boldsymbol{X}$ are shown in Fig. 3.

It is important to note that the payoff matrix of the game is nonstatic since the value of $|\omega_{i,0}|$ changes every ΔT; however, because all the elements of the matrix are shifted by a fixed value, $|\omega_{i,0}|$, it is shown in the Appendix that the strategy of the EPU controller, as will be subsequently derived, does not depend on the temporal value of $|\omega_{i,0}|$ and thus, the results of [21] still apply.

Let $X_{j,\max}$ and $X_{j,\min}$ denote the maximum and minimum values of row j in the payoff matrix of generator i, respectively. Because $|P_{C,i}| \geq |P_{A,i}|$, the maximum and minimum values of the rows of $\boldsymbol{X}$ are found in this case as

$$\begin{aligned} X_{1,\max} &= |\omega_{i,0}| - g_i\big(|P_{C,i}| - |P_{A,i}|\big) \\ X_{1,\min} &= |\omega_{i,0}| - g_i|P_{C,i}| \\ X_{2,\max} &= |\omega_{i,0}| + g_i|P_{A,i}| \\ X_{2,\min} &= |\omega_{i,0}|. \end{aligned} \tag{18}$$

It is observed that $X_{1,\max} < X_{2,\min}$ while $X_{2,\max} \not< X_{1,\min}$. Consequently, because $X_{1,\max} < X_{2,\min}$, the average long-term payoff attained by using the zero-determinant control strategy lies in $[X_{1,\max}\ , X_{2,\min}] = |\omega_{i,0}| - [g_i(|P_{C,i}| - |P_{A,i}|), 0]$. Let the specific value of the average long-term payoff at generator i be parameterized as

$$u_X = |\omega_{i,0}| - \alpha g_i\big(|P_{C,i}| - |P_{A,i}|\big) \tag{19}$$

where $0 \leq \alpha \leq 1$ is called the persistence factor; a high value of α moves u_X closer to $|\omega_{i,0}| - g_i(|P_{C,i}| - |P_{A,i}|)$, indicating that the EPU controller is more aggressive in driving the rotor speed of generator i to stability.

Further, following the development in [21], the range of valid values of b in (16) can be found as

$$\max\left(\frac{-u_X}{u_X - X_{1,\min}}, \frac{u_X}{u_X - X_{2,\max}}\right) \leq b < 0. \tag{20}$$

Given the results of (18) and (19), and for the case of an aggressive stabilizing controller (i.e., $\alpha \geq (1/2)$), it can be shown that $u_X - X_{1,\min} \geq X_{2,\max} - u_X$. Consequently, for $\alpha \geq (1/2)$, $b_{\min} \leq b < 0$, where $b_{\min} = (u_X/(u_X - X_{2,\max}))$ simplifying to

$$b_{\min} = \frac{-1}{g_i}\frac{|\omega_{i,0}| - g_i\big(|P_{C,i}| - |P_{A,i}|\big)}{\alpha\big(|P_{C,i}| - |P_{A,i}|\big) + |P_{A,i}|}. \tag{21}$$

Let the specific value of b be expressed as $b = \beta b_{\min}$, where $0 < \beta \leq 1$ is called the steering factor. Then

$$b = \frac{-\beta}{g_i}\frac{|\omega_{i,0}| - g_i\big(|P_{C,i}| - |P_{A,i}|\big)}{\alpha\big(|P_{C,i}| - |P_{A,i}|\big) + |P_{A,i}|}. \tag{22}$$

A high value of β means that the EPU controller is more probable to take a stabilizing action; i.e., p_C increases with increasing β.

Let the status of the EPU controller and attacker be j and k, respectively, in the previous time interval ΔT and be known to the EPU controller. Let $p_i^{j,k}$ denote the probability that the controller is active at generator i in the current time interval given knowledge that $n_1 = j$ and $n_2 = k$ in the previous interval. Using the results of (17), (19), and (22), the probabilities of the EPU controller taking a stabilizing action are

$$\begin{aligned} p_i^{1,2} &= \frac{(\alpha - \beta + \alpha\beta)|P_{C,i}| + (1 - \alpha - \alpha\beta)|P_{A,i}|}{\alpha|P_{C,i}| + (1-\alpha)|P_{A,i}|} \\ p_i^{1,1} &= p^{1,2} + \frac{\beta|P_{A,i}|}{\alpha|P_{C,i}| + (1-\alpha)|P_{A,i}|} \\ p_i^{2,1} &= \beta \\ p_i^{2,2} &= \frac{\alpha\beta(|P_{C,i}| - |P_{A,i}|)}{\alpha|P_{C,i}| + (1-\alpha)|P_{A,i}|}. \end{aligned} \tag{23}$$

Moreover, let $\rho_i = (|P_{C,i}|/|P_{A,i}|) \geq 1$ denote the ratio of the control power and the attack power at generator i. Then the probabilities of action can be expressed as

$$\begin{aligned} p_i^{1,1} &= 1 + \beta - \beta \frac{\rho_i}{\alpha\rho_i - \alpha + 1} \\ p_i^{1,2} &= 1 - \beta \frac{(1-\alpha)\rho_i + \alpha}{\alpha\rho_i - \alpha + 1} \\ p_i^{2,1} &= \beta \\ p_i^{2,2} &= \beta \frac{\alpha\rho_i - \alpha}{\alpha\rho_i - \alpha + 1}. \end{aligned} \tag{24}$$

For the special case of $\rho_i = \infty$; i.e., $P_{A,i} = 0$ and there is no attack at generator i, the probabilities that the EPU controller takes a stabilizing action become

$$p_i^{1,2} = 1 + \beta - \frac{\beta}{\alpha}, \quad p_i^{2,2} = \beta. \tag{25}$$

Similarly, when $\alpha = 1$ (i.e., the EPU controller is very aggressive), the controller action probabilities are

$$\begin{aligned} p_i^{1,1} &= 1, \quad p_i^{1,2} = 1 - \beta \frac{1}{\rho_i} \\ p_i^{2,1} &= \beta, \quad p_i^{2,2} = \beta - \beta \frac{1}{\rho_i}. \end{aligned} \tag{26}$$

In other words, $p_i^{1,2} = p_i^{1,1} - (\beta/\rho_i)$ and $p_i^{2,2} = p_i^{2,1} - (\beta/\rho_i)$. This means that if the attacker is not active at generator i during a specific time interval, the EPU controller will reduce the probability of taking an action to stabilize the power system by β/ρ_i in the subsequent interval. The controller's behavior in this scenario reflects the case where as a result of no action from the attacker, the deviation of $\omega_{i,0}$ is small, if existed; hence, it is not in the best interest of the EPU controller to take aggressive actions that would over-correct the deviation.

It is to be noted that if the EPU stabilizing controller chooses to act all the time, regardless of the actions of the attacker, the average long-term payoff will be in the range $|\omega_{i,0}| - g_i|P_{C,i}| + [0\,,\, g_i|P_{A,i}|]$, 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 constraints on the availability or the cost of the storage units.

IV. Numerical Results

We demonstrate the validity of our analysis insights on the 39-bus New England power system of Fig. 1 with parameters of Table II and values of M_i's and X'_{di}'s taken from [22] and [23]. To provide a conservative assessment of the attack mitigation, we do not activate governor control in our simulations.

The power system is assumed to be running normally from $0 \leq t < 0.5$ s. Then, a cyber switching attack that targets both generators 2 and 9 from $0.5 \leq t \leq 10.5$ s is applied. The attacker injects or absorbs (depending on the sign of $\omega_{i,0}$) 0.15 p.u. of power at the external storage units of generators 2 and 9 every $\Delta T = 50$ ms during the attack duration.

TABLE II
New England Power System Parameters

Generator	M_i (s)	D_i (ms)	X'_{di} (pu)
1	0.2228	20	0.0310
2	0.1607	20	0.0697
3	0.1899	20	0.0531
4	0.1517	20	0.0436
5	0.1379	20	0.1320
6	0.1846	20	0.0500
7	0.1401	20	0.0490
8	0.1289	20	0.0570
9	0.1830	20	0.0570
10	2.6526	20	0.0060

TABLE III
Load Flow Analysis

Generator	$P_{e,i}$ (pu)	$\lvert E_i \rvert$ (pu)	δ_i (degree)
1	5.7066	1.0837	30.7002
2	6.4762	1.2421	29.8521
3	6.3105	1.1340	27.7721
4	5.0777	1.4645	39.0375
5	6.4909	1.2602	30.1499
6	5.5930	1.1797	31.3045
7	5.3773	1.1024	28.1576
8	8.2919	1.2031	40.5242
9	2.4471	1.1181	10.4393
10	9.2693	1.0434	3.5338

The EPU stabilizing controller is activated on the system generators at t = 0.75 s (i.e., the EPU controller is activated after 250 ms from the start of the switching attack). The stabilizing control is deactivated when both cyber-attack is finished and power system is stable. The power of each storage unit is limited to 10% of the mechanical power of the corresponding generator. Further, the EPU controller can inject or absorb a real power of 0.3 p.u. at the storage unit every $\Delta T = 50$ ms as well. In other words, the amount of power the EPU controller can use at any specific storage unit is limited to the minimum of 0.3 p.u. and 10% of the mechanical power of the corresponding generator.

Before the occurrence of the cyber-attack, load flow analysis of the power system yields the results tabulated in Table III; here, the mechanical and electrical powers of each generator are equal due to the steady-state nature.

Generator stability time is measured as the difference between the time after which generator's relative normalized rotor speed is restricted to a 0.8333% threshold (i.e., the maximum rotor speed is within ± 0.5 Hz of the nominal value) and t = 0.75 s, the time when the stabilizing controller is activated. Further, let the $\Delta T = 50$ ms interval be called the game interval, $|P_{A,i}|$ = 0.15 p.u., $i \in \{2, 9\}$, and $|P_{C,i}| = \min(0.3 \text{ pu}, (P_{m,i}/10)) \; \forall i \in \{1, \ldots, N\}$.

The activity ratio of the controller ξ represents the percentage of time that the EPU controller is active ($n_1 = 1$) within the stabilization period. It can be shown that this measure is approximated by $100 \times p_i^{2,2}/(1 + p_i^{2,2} - p_i^{1,2})$ for nonattacked generators. Using (24) and given that $P_{A,i}$ = 0 (i.e., $\rho_i = \infty$), $\forall i \notin \{2, 9\}$, we can approximate

$$\xi_i \approx 100 \times \alpha, \forall i \notin \{2, 9\}. \tag{27}$$

The attacker targets fast-acting storage units at generators 2 and 9. At the end of each game interval,

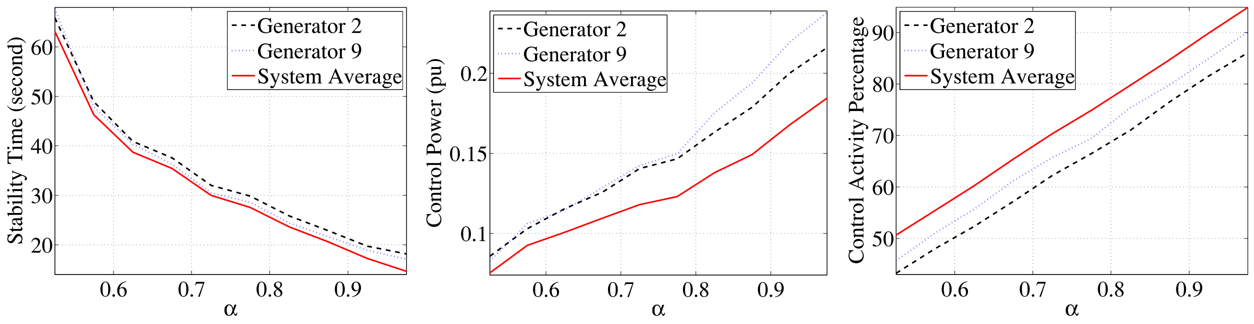

Fig. 4. Performance versus the persistence factor α.

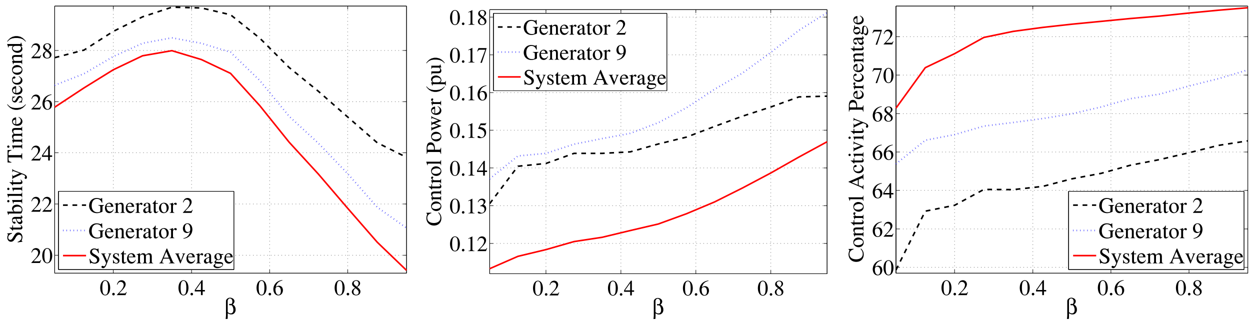

Fig. 5. Performance versus the steering factor β.

TABLE IV
PERFORMANCE BENCHMARK

Generator	Stability Time (second)	Control Power (pu)
1	12.1021	0.1881
2	13.6828	0.2900
3	12.2603	0.2125
4	12.2402	0.1721
5	13.3902	0.1486
6	11.5588	0.1684
7	11.2565	0.1543
8	10.6682	0.1854
9	11.8557	0.2907
Average	12.1128	0.2011

the attacker uses (4) to determine whether it needs to absorb or inject power in the next game interval; the attacker does not change the value of attack power during the 50-ms interval. In contrast, the mitigation strategy of the EPU controller relies on (23) to calculate its probability of taking action in the next game interval. If the EPU controller must be active, (5) is used to determine the specific action.

A. Stabilizing Control Without Zero-Determinant Strategies

As a benchmark, Table IV displays the performance measures of the power system when the stabilizing controller does not implement the game-theoretic approach (i.e., when the EPU controller always takes a stabilizing action regardless of the actions of the attacker in the previous game interval). This represents an extreme "best case" for stabilization irrespective of cost and energy conservation. It is noted the average stability time of the system generators is approximately 12.1 s, which means that the power system is driven to stability within about 2.36 s from the end of the cyber attack.

B. Stabilizing Control Using Zero-Determinant Strategies

The stability time of the system generators, the average control power, and the controller's activity ratio versus the controller's persistence factor, α, are shown in Fig. 4; in this case, a value of $\beta = 0.5$ is used. As noted in (19), the value of α determines the long-term payoff of the power system during and after the cyber switching attack, and a high value of α means the controller is more aggressive and so the system generators will be driven to stability faster. Furthermore, the value of the persistence factor directly affects the EPU controller's activity as shown in (27). The tradeoff between the stability time and the average power required by the EPU controller is well demonstrated in this figure.

Fig. 5 shows the performance measures versus the steering factor of the controller, β, for a value of $\alpha = 0.75$. It is observed that varying the value of β does not have substantial effects on the performance measures. Because β affects the controller's likelihood of action as shown in (24), higher values of β means the EPU controller is more likely to take a stabilizing action. Moreover, results of this figure confirm that the controller meets its target long-term average payoff as long as the value of $b = \beta b_{\min}$ lies in the range $b_{\min} \leq b < 0$. This result also suggests that the system operator has flexibility in designing the stabilizing controller.

The relation between the power ratio, ρ, and the system performance is shown in Fig. 6 for $\alpha = 0.75$, $\beta = 0.5$, and $|P_{C,i}| = \min(0.3 \text{ pu}, (P_{m,i}/10))$ $\forall i \in \{1, \ldots, N\}$. In this figure, the attack power is found from $|P_{A,i}| = (|P_{C,i}|/\rho_i)$. Because ρ represents the ratio of the control power and the attack power, a higher value of ρ indicates a higher capability of the EPU stabilizing controller compared to that of

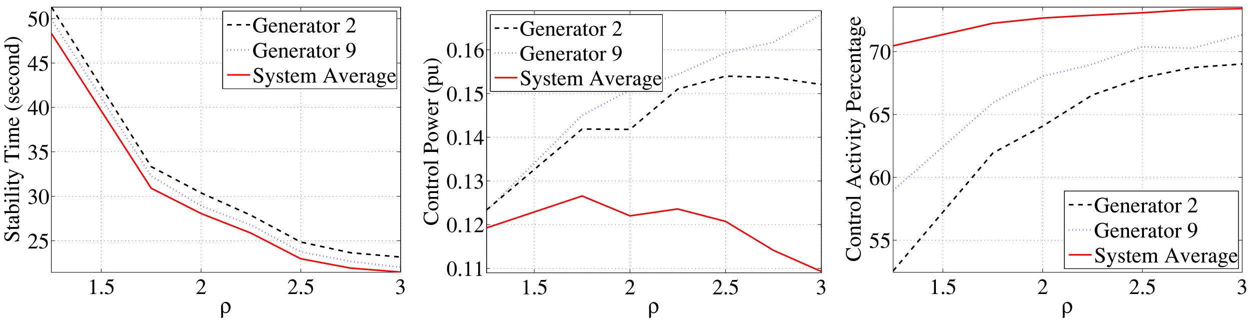

Fig. 6. Performance versus the power ratio ρ.

the attacker. Consequently, the effect of ρ on the system performance resembles that of α. It is observed that the stability time decreases steadily with increasing the power ratio. On the other hand, the average control power that is used to stabilize the power system slightly increases for the attacked generators. Consequently, a higher value of ρ will drive the system quicker to stability; however, the average control power will not substantially increase.

The results of Figs. 4–6 demonstrate the tradeoff amongst the parameters of the EPU controller, the stability time, and average control power. Consequently, the system operator can choose the appropriate values of α, β, and ρ, such that an acceptable stability time is achieved while the budget for external storage (cost or availability) is met.

V. Discussion

The reader should note that game-theoretic analysis commonly focuses on identifying and analyzing equilibrium strategies assuming strategic rational players. Our formulation deviates from this classical formulation to include playing against a nonstrategic opponent; thus making the notion of equilibrium invalid. In essence, we assume the actions of the attacker (i.e., whether or not the attacker would access the system in the next round) to be random and not necessarily strategic. Thus, our analysis focuses on the long-term average outcome of the game from the standpoint of the controller. In this regard, we deduce reactive strategies of the controller to achieve a targeted long-term outcome without assumptions on the attacker's strategy or the payoff matrix.

To further emphasize how the game converges to the long-term average outcome, the strategies of the defender (i.e., EPU controller) in the aforementioned game dictates that the controller takes an action to correct for any existing deviation in the system state from nominal desired state. In this framework, the controller continues to work in a series of actions to maintain system desired state. The game-theoretic formulation provides guarantees that over time the EPU is able to mitigate any set of strategies of the attacker.

The numerical results show that the attack mitigation strategy is successful in bringing the power system to stability even though the switching attack is an aggressive one. In addition, as we show that a suitable set of design parameters can lead to an acceptable performance (i.e., stability time) while meeting a budget constraint (i.e., an average control power). This type of proposed defense can be thought of as a first-line-of-defense scheme against cyber switching attacks till the system operators isolate and remove the attacked devices from the system to prevent the adversary from continuing the attack.

Our results show strategic implications for an effective control-based attack mitigation scheme. First, the formulation demonstrates how the EPU does not have to act aggressively or persistently in order to stabilize the power system. Further, because of the zero-determinant feature of the game, players with longer memories of the history of the game have no advantage in the long run over those with shorter memories; consequently, the EPU controller does not need to know the whole history of the attack in order to mitigate it efficiently, and it is actually sufficient for the EPU controller to know only the previous act of the attacker.

As evident from the analysis and the numerical results, the proposed framework provides a flexibility for the system operator in choosing a suitable set of values for α, β, and ρ in order to meet a specific stability time. This flexibility enriches the tunability of the attack mitigation strategy and helps the EPU to meet different resource constraints. Further, although the storage unit model is used in this paper; the model in (4) is flexible and our analysis will also hold for modulating distributed generators and loads.

As a final note, it can be deduced that if the attacker has more leverage over the stabilizing controller (i.e., $|P_{A,i}| \geq |P_{C,i}| \, \forall i$), then the attacker can utilize the game structure to fix the long-term outcome of the game; other defense mechanisms should be activated by the EPU in this case. Otherwise, the EPU controller will determine the long-term result of the game regardless of the actions of the attacker.

VI. Conclusion

This paper presents an analysis framework to determine the effects of cost or availability-constrained mitigation controllers in the presence of cyber switching attacks. We focus on a class of switching attacks and control actions that are simple making use of only the sign of the target generator's relative normalized rotor speed. The stabilizing controller relies on receiving timely system updates in order to determine the strategy for mitigation. Our controller model makes use of zero-determinant strategies for iterated games to determine when the controller is active. The merits of the proposed controller are investigated on the New England 39-bus power system. Numerical results detail the system performance metrics versus the parameters of the stabilizing controller. We assert that our models provide insight into a broad class of attack and mitigation strategies thus demonstrating that it is possible for stabilizing controllers that are not always active to stabilize a power grid under attack over time. Future work will include addressing mitigation in the face of multiple random attacks as well as investigating strategies for effective mitigation when $|P_{A,i}| > |P_{C,i}|$. In the latter, we will study how more aggressive attacks are conducive to early detection, notification and subsequent intervention by system operators.

Appendix

Here, we extend the work of Al Daoud *et al.* [21] to consider the case when the elements of the payoff matrix include a fixed bias that can change from one interval to another.

Theorem 1: Consider the game described in Fig. 2. Assume a fixed payoff matrix at each stage of the game and consider a set of zero-determinant strategies for this game as described in (17). If at any round of the game, the elements of the payoff matrix are shifted by a fixed value, the set of zero-determinant strategies for the game still holds.

Proof: Let the values of the payoff matrix, $\boldsymbol{X}$, before the bias be $\boldsymbol{X} = [X_{j,k}]$, where $j, k \in \{1, 2\}$. First, assume that $X_{1,\max} < X_{2,\min}$.

The average long-term payoff, u_X, can lie in the range of $[X_{1,\max}, X_{2,\min}]$. Let the exact value of u_X be represented as $u_X = X_{1,\max} + \sigma(X_{2,\min} - X_{1,\max})$ where $0 \leq \sigma \leq 1$. Further, the minimum value of b is $(u_X/(u_X - X_{2,\max}))$, and let the exact value of b be represented as $b = \eta(u_X/(u_X - X_{2,\max}))$ where $0 < \eta \leq 1$. Using the definition of $p_C^{1,1}$ in (17), the following is found:

$$\begin{aligned} p_C^{1,1} &= 1 + \left(1 - \frac{X_{1,1}}{u_X}\right)b \\ &= 1 + \eta\left(\frac{u_X - X_{1,1}}{u_X}\right)\frac{u_X}{u_X - X_{2,\max}} \\ &= 1 + \eta\left(\frac{u_X - X_{1,1}}{u_X - X_{2,\max}}\right). \end{aligned}$$

Let $\boldsymbol{X}'$ be the new payoff matrix after introducing a bias of Θ to all the elements of $\boldsymbol{X}$; i.e., $X'_{j,k} = X_{j,k} + \Theta\ \forall j, k \in \{1, 2\}$. The value of u'_X is found as

$$\begin{aligned} u'_X &= X'_{1,\max} + \sigma\left(X'_{2,\min} - X'_{1,\max}\right) \\ &= X_{1,\max} + \Theta + \sigma\left(X_{2,\min} - X_{1,\max}\right) \\ &= u_X + \Theta. \end{aligned} \tag{28}$$

Further, the value of b' is expressed as

$$b' = \eta\frac{u'_X}{u'_X - X'_{2,\max}} = \eta\frac{u_X + \Theta}{u_X - X_{2,\max}}. \tag{29}$$

The value of $p_C^{1,1'}$ is consequently found as

$$\begin{aligned} p_C^{1,1'} &= 1 + \left(1 - \frac{X'_{1,1}}{u'_X}\right)b' \\ &= 1 + \eta\left(\frac{u_X - X_{1,1}}{u_X + \Theta}\right)\frac{u_X + \Theta}{u_X - X_{2,\max}} \\ &= 1 + \eta\left(\frac{u_X - X_{1,1}}{u_X - X_{2,\max}}\right) = p_C^{1,1}. \end{aligned} \tag{30}$$

Similar results can be found for the values of $p_C^{1,2'}$, $p_C^{2,1'}$, and $p_C^{2,2'}$. Further, analogous analysis can be conducted for the case when $X_{2,\max} < X_{1,\min}$. Accordingly, the values of the probability of taking an action do not change if all the elements of the payoff matrix undergo the same value of bias. Hence, the structure of the game does not change. ■

The mitigation philosophy of the controller in this game is to mitigate any resulting bias on estimated system nominal state; thus, actions of the EPU controller are relative to this value and include this as a bias in the 2 × 2 game. But as Theorem 1 shows, it is proven that regardless of the fluctuations of ω_i during the game, the controller will be able to stabilize the power generator as long the game is played according to (24).

References

[1] S. Liu, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "Coordinated variable structure switching in smart power systems: Attacks and mitigation," in *Proc. Int. Conf. High Confid. Netw. Syst. (HiCoNS)*, Berlin, Germany, Apr. 2012, pp. 21–30.

[2] 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 *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, San Diego, CA, USA, Jul. 2012, pp. 1–6.

[3] J. Wei, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "A flocking-based dynamical systems paradigm for smart power system analysis," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, San Diego, CA, USA, Jul. 2012, pp. 1–8.

[4] J. Wei and D. Kundur, "Two-tier hierarchical cyber-physical security analysis framework for smart grid," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, San Diego, CA, USA, Jul. 2012, pp. 1–5.

[5] 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 *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Tainan, Taiwan, Nov. 2012, pp. 372–377.

[6] J. Wei, D. Kundur, T. Zourntos, and K. Butler-Purry, "A flocking-based paradigm for hierarchical cyber-physical smart grid modeling and control," *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2687–2700, Nov. 2014.

[7] Q. Zhu and T. Başar, "A dynamic game-theoretic approach to resilient control system design for cascading failures," in *Proc. Int. Conf. High Confid. Netw. Syst.*, Berlin, Germany, Apr. 2012, pp. 41–46.

[8] C. Y. Ma, N. S. Rao, and D. K. Yau, "A game theoretic study of attack and defense in cyber-physical systems," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Shanghai, China, Apr. 2011, pp. 708–713.

[9] W. M. Siever, A. Miller, and D. R. Tauritz, "Blueprint for iteratively hardening power grids employing unified power flow controllers," in *Proc. IEEE Int. Conf. Syst. Syst. Eng. (SoSE)*, San Antonio, TX, USA, Apr. 2007, pp. 1–7.

[10] Y. W. Law, T. Alpcan, M. Palaniswami, and S. Dey, "Security games and risk minimization for automatic generation control in smart grid," in *Decision and Game Theory for Security*. Berlin, Germany: Springer-Verlag, 2012, pp. 281–295.

[11] W. H. Press and F. J. Dyson, "Iterated prisoner's dilemma contains strategies that dominate any evolutionary opponent," *Proc. Nat. Acad. Sci.*, vol. 109, no. 26, pp. 10409–10413, Jun. 2012.

[12] F. Dörfler and F. Bullo, "Synchronization and transient stability in power networks and non-uniform Kuramoto oscillators," in *Proc. Amer. Control Conf. (ACC)*, Baltimore, MD, USA, Jun./Jul. 2010, pp. 930–937.

[13] F. Dorfler and F. Bullo, "Kron reduction of graphs with applications to electrical networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 60, no. 1, pp. 150–163, Jan. 2013.

[14] P. M. Anderson and A. A. Fouad, *Power System Control and Stability* (IEEE Power Systems Engineering Series). Piscataway, NJ, USA: IEEE-Press, 1994.

[15] A. R. Bergen and V. Vittal, *Power Systems Analysis*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2000.

[16] T. Flick and J. Morehouse, *Securing the Smart Grid: Next Generation Power Grid Security*. Boston, MA, USA: Syngress, 2011.

[17] S. M. Amin, "For the good of the grid," *IEEE Power Energy Mag.*, vol. 6, no. 6, pp. 48–59, Nov./Dec. 2008.

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

[19] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 273–285, Dec. 2013.

[20] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, "A coordinated multi-switch attack for cascading failures in smart grid," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1183–1195, May 2014.

[21] A. Al Daoud, G. Kesidis, and J. Liebeherr, "Zero-determinant strategies: A game-theoretic approach for sharing licensed spectrum bands," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2297–2308, Nov. 2014.

[22] T. Athay, R. Podmore, and S. Virmani, "A practical method for the direct analysis of transient stability," *IEEE Trans. Power App. Syst.*, vol. PAS-98, no. 2, pp. 573–584, Mar. 1979.

[23] B. Pal and B. Chaudhuri, *Robust Control in Power Systems* (Power Electronics and Power Systems Series). New York, NY, USA: Springer, 2006.

Abdallah Farraj (S'11–M'12) received the B.Sc. and M.Sc. degrees from the University of Jordan, Amman, Jordan, in 2000 and 2005, respectively, and the Ph.D. degree from Texas A&M University, College Station, TX, USA, in 2012, all in electrical engineering.

He is currently a Postdoctoral Fellow with the University of Toronto, Toronto, ON, Canada. He is a Fulbright Scholar. His current research interests include cognitive communications, cyber-security of smart grids, downhole telemetry systems, wireless communications, and signal processing applications.

Eman Hammad (GSM'14) received the B.Sc. degree from the University of Jordan, Amman, Jordan, in 2000, and the M.Sc. degree from Texas A&M University, College Station, TX, USA, in 2011, both in electrical engineering. She is currently pursuing the Ph.D. degree with the Department of Electrical Engineering, University of Toronto, Toronto, ON, Canada.

She has professional experience in the IT industry in Jordan. Her current research interests include cyber-physical systems in particular cyber-security, resilient control, and cooperative game theory in the context of smart grids.

Ms. Hammad was a recipient of the Hatch Graduate Scholarship for Sustainable Energy Research and the Best Poster Award at the Institute for Sustainable Energy 2014 Symposium. She is currently with the IEEE Toronto Computer Society Chapter Chair. She was a Technical Program Committee and an Organizing Committee Member for several conferences and workshops.

Ashraf Al Daoud received the Ph.D. degree in computer engineering from Boston University, Boston, MA, USA, in 2010.

From 2011 to 2013, he was on the faculty with the Department of Computer Engineering, German-Jordanian University, Amman, Jordan. From 2013 to 2014, he was a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada. He is currently with the Economic Decision Support Group, TELUS Communications, Toronto. His current research interests include telecom economics, game theory, and network optimization.

Deepa Kundur (S'91–M'99–SM'03–F'15) received the B.A.Sc., M.A.Sc., and Ph.D. degrees from the University of Toronto, Toronto, ON, Canada, in 1993, 1995, and 1999, respectively, all in electrical and computer engineering.

She is a Professor with the Edward S. Rogers, Sr. Department of Electrical and Computer Engineering, University of Toronto. She is a recognized authority on cyber-security issues and has appeared as an expert in popular television, radio, and print media. Her current research interests include interface of cyber-security, signal processing, and complex dynamical networks.

Prof. Kundur was a recipient of Best Paper Recognitions from the 2008 INFOCOM Workshop on Mission Critical Networks, the 2011 Cyber Security and Information Intelligence Research Workshop, and the 2012 IEEE Canadian Conference on Electrical and Computer Engineering. She is currently an Associate Editor of the IEEE Transactions on Information Forensics and Security, an Associate Chair with the Division of Engineering Science, and a General Chair of the IEEE GlobalSIP'15 Symposium on Signal and Information Processing for Optimizing Future Energy Systems, the 2015 International Conference on Smart Grids for Smart Cities, and the 2015 Smart Grid Resilience Workshop at IEEE GLOBECOM 2015. She has participated on several editorial boards.