# A DER Attack-Mitigation Differential Game for Smart Grid Security Analysis

Pirathayini Srikantha, *Student Member, IEEE*, and Deepa Kundur, *Fellow, IEEE*

***Abstract*—Information and communication infrastructure will be extensively deployed to monitor and control electric power delivery components of today's power grid. While these cyber elements enhance a utility's ability to maintain physical stability, if a subset are compromised by adversaries, disruption may occur. In this paper, a novel framework based on the principles of differential games is proposed that demonstrates stealthy worst-case strategies for attackers to disrupt transient stability by leveraging control over distributed energy resources. We demonstrate that if the electric power utility is able to identify uncompromised components, countermeasures can exist that effectively reduce the impact of attack for a fixed time interval. Based on our results, we develop insights to construct safety margin recommendations for cyber-physical smart grid actuation elements that promote system resilience during a cyber attack.**

***Index Terms*—Cyber-physical systems, distributed algorithms, power system security.**

## I. Introduction

THE ELECTRIC power grid is a vital infrastructure that facilitates fundamental operations in modern society. As a complex entity composed of tightly interconnected elements, the corruption of even a small subset of components has the potential to trigger cascading failures leading to system-wide disruptions. In order to enhance grid resilience, electric power utilities (EPUs) are increasingly integrating advanced (cyber) information systems with the (physical) power infrastructure to enable wide area monitoring, protection, and control (WAMPAC). We are thus witnessing the traditional power system evolve into an emergent cyber-physical entity comprised of a diverse set of WAMPAC devices including phasor measurement units (PMUs), smart circuit breakers and distributed energy resources (DERs) that utilize communication networks to synergistically promote system robustness.

One major pitfall associated with this amalgamation is that the cyber-enabled power system will inherit well-documented cyber vulnerabilities stemming from intelligent devices utilizing standard communication protocols. These vulnerabilities can be leveraged by adversaries to launch insidious attacks on the integrity, confidentiality, and availability of cyber data generated in the power system. Examples include false data injection into measurement devices [1], estimation of system state via eavesdropping [2], and denial of service attacks on the communication network [3]. Risk analysis frameworks have been developed to empirically study the potential physical impact of these cyber attacks [4]–[6]. In recent work, more sophisticated attack models facilitated by the aforementioned cyber attacks are proposed to specifically target physical system weaknesses. For example, Liu *et al.* [7] demonstrated that attackers having remote access to a subset of smart circuit breakers can successfully trip target generators by designing an effective sequence of binary on–off signals that drive the system into sliding mode instability. In another work, Liu *et al.* [8] incorporated information such as system intrusion obtained from the cyber network into the physical laws of the power grid to improve state estimations of the power grid.

False data injection is an example of a data oriented stealthy attack model in the context of the smart grid. Typically, a stealthy attack is one in which the actions of the attacker go unnoticed until a significant degree of disruption has occurred, thus preventing timely mitigation from occurring. Bad data injection attacks corrupt PMU data in such a manner that evades traditional false data detection schemes in the power grid. These will cause the EPU to make incorrect operational decisions that can inevitably lead to blackouts and/or major economical losses [9], [10]. A coordinated switching attack is an example of a binary control-oriented stealthy attack model that utilizes corrupt smart circuit breakers to progressively build physical instability at various points in the power grid in order to instigate widespread cascading failures [11].

In this paper, we explore an attack-mitigation model of similar flavor in which attacks instigated by means of data corruption and communication network sabotage via devices capable of continuous actuation are engineered based on the underlying physics of the power infrastructure represented mathematically as a nonlinear dynamical system. This paper represents a novel departure from existing research as it, for the first time, considers the use of DERs for attack. Given the growing diversity of attack models in the smart grid literature, we begin our exploration of this field by first focussing on a possible DER-based attack with the intent of building upon this framework in the future to include a broad spectrum of other attacks. DERs are fast acting external energy

Manuscript received October 23, 2014; revised May 29, 2015; accepted August 3, 2015. Date of publication August 23, 2015; date of current version April 19, 2016. This work was supported in part by the National Science Foundation under Grant ECCS-1028246, in part by the Natural Sciences and Engineering Research Council of Canada under Grant RGPIN 227722, and in part by the Hatch Graduate Scholarship for Sustainable Energy Research. Paper no. TSG-01059-2014.

The authors are with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: pirathayini.srikantha@ece.utoronto.ca; dkundur@ece.utoronto.ca).

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.2015.2466611

sources employed by EPUs (in lieu of circuit breakers that reduce system topology) to add resilience into the system by aiding with generator frequency synchronization when faults occur [12]. In our attack model, cyber-actuators controlling DERs serve as instruments for perpetrating the attacks. Due to the nature of DERs, switched system theory can no longer be applied for analysis. Moreover, we assert that corrupt DERs enable adversaries to conduct stealthy attacks which can evade fault detection mechanisms and yet succeed in disrupting the system. As stealthy attacks are difficult to detect, attack mitigation can be challenging even if counter-strategies exist. Hence, natural research questions arise: what is the worst-case damage possible by an opponent? What effect does a best-effort mitigation by an EPU have? Are there component safety margins that aid in promoting system resilience?

We consider these questions in the context of maintaining transient stability of a cyber-physical smart grid system with DERs. Thus, our first contribution is a novel attack-mitigation model in which opponents harness a subset of DERs to steer normal grid operation away from stability while the EPU aims to regain stability using another subset of system resources. Interactions between the opponents and the EPU is formulated as a nonlinear differential game theoretic problem. The solution to this problem represents our second contribution, the development of a novel algorithm linking robust control and linear quadratic game theory to generate worst-case attack vectors that aim to bypass circuit breakers as well as best-effort counterstrategies to minimize attack impact. We show that the derived countermeasures are effective in suppressing system disruption. As this is an ideal case, comprehensive analysis is performed to identify how the counterstrategies can reduce system disruption risks for various delays encountered in the attack identification process. We demonstrate that when the EPU is unable to identify corrupt DERs in a timely manner, coordinated attacks on even a subset of DERs can cause transient instability in a system as large as a 10-machine, 39-bus New England power grid. In our third contribution, we show how insights from this analysis enable vulnerability assessment to highlight safety margin recommendations for complex cyber-physical actuating elements of the smart grid like the DERs.

The remainder of this paper is organized as follows. Section II details the proposed attack-mitigation model and introduces the game theoretic problem formulation. Section III provides an overview of the novel algorithm proposed to solve nonlinear differential games. Next, in Section IV, attack and countermeasure vectors are constructed and the impact of these on power system dynamics is demonstrated. Final remarks are presented in Section V. The Appendix contains detailed proofs of the theorems and the lemma presented in this paper.

## II. System Framework

### A. Cyber-Physical System

We consider a power grid in which DERs are deployed at close proximity to each synchronous generator in the system.

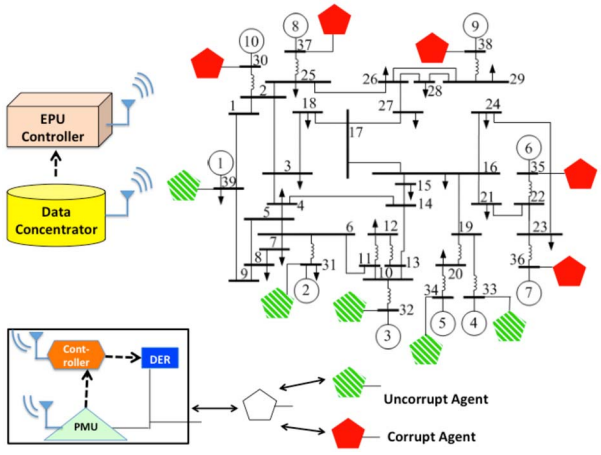


Fig. 1. Diagram of system model.

Since DERs are able to rapidly absorb or inject power into the grid, they are employed in our framework for restoring frequency synchronization in the event of a fault or disruption as studied in [12]. Common types of DERs include renewable sources, batteries, and flywheels. DERs are more flexible than traditional synchronous generators and are less disruptive than circuit breakers that reduce the system topology when faults occur. As shown in Fig. 1, each DER is integrated with a local controller that translates cyber data into DER actuation signals. The local controller can make distributed decisions based on measurements transmitted by a local PMU at close proximity or can act according to control data transmitted by the centralized EPU controller. The EPU controller performs computations to maintain grid stability using insights extracted from the data concentrator which amasses measurement data transmitted by all PMUs. Communication takes place via a network overlay connecting all cyber elements in the system.

We represent the cyber-physical interactions through dynamical system models. Such (possibly nonlinear) models are applicable to a variety of cyber-actuating system elements and cyber-physical mixes. Thus, we first develop a mathematical framework assuming generalized dynamics $f(\cdot)$ as listed in (2). Our intent is to first consider a general formulation so that our analysis can be applied for a broader context. In Section IV, we consider a specific 10-machine 39-bus system illustrated in Fig. 1 whose dynamics are governed by (9).

### B. Attack-Mitigation Model

A vulnerability is defined to be a system flaw or susceptibility for which means are available to access and exploit it [3]. For the specific problem, we consider in this paper the smart grid system is physically susceptible to transient instability of its synchronous generators in the face of stealthy DER cyber corruption. Here, the term stealthy takes into account the impact of the attack, which needs to be lower initially to prevent detection via traditional safety mechanisms in place. The DER-based attack will postpone the activation of these detection mechanisms in order to maximize the impact on the system. We specifically consider the tripping of circuit

breakers which are prevalent in the power grid (although breakers will trip during the onset of transient instability). Transient stability of the grid is maintained when generator frequencies lie within $\pm 2\%$ of the nominal 60 Hz frequency and the phase angle difference between any generator pair lies within 100° [13]. Any deviation in these conditions will trip the corresponding generator resulting in topology reduction and cascading failures.

This physical flaw can be accessed by leveraging the widespread cyber connectivity necessary for measurement and control within the smart grid system in addition to weaknesses in the cyber components including operating system holes and communication protocol limitations. The adversary can exploit the physical flaw and promote transient instability through interception, modification, and/or fabrication cyber attacks that actuate change on the system through corrupt local actuating DER controllers. Moreover, an adversary can either eavesdrop or intercept cyber data to learn about the system topology to facilitate more effective disruption.

Hence, in our attack-mitigation model we assume the following for the attacker and EPU.

1) The attacker is aware of the local physical system topology and initial state of the system prior to attack.
2) The attacker is capable of corrupting or applying other forms of denial-of-service on a subset of PMU data.
3) The attacker has control over a subset of DERs via intrusion of appropriate cyber resources.
4) The EPU has control over the remaining DERs.
5) The EPU has knowledge of the physical topology and system state during regular operation.

Assumption 1 credits the attacker with physical topology information. Such information may be gleaned through eavesdropping of local communications and is consistent with recent papers on smart grid attacks [1], [7]. Assumptions 2 and 3 can be implemented effectively through a variety of known cyber attacks on the communications infrastructure by exploiting flaws in protocols or operating systems [14]. Assumption 4 requires the EPU to employ detection mechanisms such as in [15] and [16] to identify uncompromised DERs; thus, the proposed research represents an orthogonal contribution to detection schemes by providing a framework for reaction and resilience. Assumption 5 removes the EPUs dependency on possibly corrupt current grid state data for making countermeasure decisions. This assumption is feasible as the EPU monitors the grid state at regular intervals. We would like to emphasize again that this is a DER-based attack model. As there is a growing trend in harnessing DERs for resilience in the smart grid [12], [17], it is necessary to investigate vulnerabilities that may result from the integration of these devices. As this is a new formulation, studying DER attacks in isolation is a necessary first step before integrating these into a general framework that includes other attack models such as false data injection.

For tractability in our problem formulation, we assume that detection of the attack and identification of corrupt resources are immediate. We, however, explore the impact of delay during this attack characterization in Section IV.

### C. Mathematical Description

The system state is represented by the collection of frequencies and phase angles of each synchronous generator in the grid, reflecting the overall transient stability. Since state measurements and control occur at discrete intervals of time with sampling frequency often ranging from 50 to 60 Hz [18], we describe the dynamics in discrete-time. The discrete-time state $x_k$ of the overall power system containing $g$ synchronous generators of the index set $G = \{1, 2, \ldots, g\}$ is

$$x_k = \big(\omega_1(k), \ldots, \omega_g(k), \theta_1(k), \ldots, \theta_g(k)\big)' \tag{1}$$

where $\omega_i(k)$ and $\theta_i(k)$ represent the frequency and phase angle of generator $i$ at time step $k$ and $(\cdot)'$ is the transpose operator. The system state at stable equilibrium is denoted $x_k^s$.

As discussed, each generator effectively has a corresponding fast acting DER (for example, in the form of storage) of the same index. An adversary having compromised a set $E \subset \{1, 2, \ldots, g\}$ of DERs will construct an attack vector $u_k^e$ at time step $k$. This vector, of length $g$, has at most $|E|$ nonzero elements at locations $i \in E$ corresponding to the compromised DERs. In contrast, the EPU will construct a countermeasure vector $u_k^p$ by leveraging the remaining uncorrupted elements $P = \{1, 2, \ldots, g\} \backslash E$ to enhance resilience to attack. Thus $u_k^p$ will be a vector of length $g$ with nonzero elements possible at locations $i \in P$. Each component value of $u_k^e$ and $u_k^p$ represents the amount of power that is absorbed or injected into the system by the corresponding DER. Due to physical constraints, power injection or absorption by DER $i$ is bounded by $[l_i, c_i]$ where $l_i \leq c_i$. If $l_i$ is a negative value then $|l_i|$ is the maximum power that DER $i$ can absorb from the system. Otherwise, it represents a lower limit on the power that it can inject into the grid. Similarly, $|c_i|$ is the maximum power injection capacity of DER $i$ if $c_i$ is positive; otherwise, it is the minimum power that can be absorbed from the grid. Section IV considers various scenarios that explore these limits.

The overall system dynamics that accounts for attack and countermeasure vectors is expressed as

$$x_{k+1} = f\big(x_k, u_k^p, u_k^e\big). \tag{2}$$

To represent the system in a sufficiently realistic manner, the above dynamics are considered to be nonlinear in this paper.

Fig. 1 illustrates a New England 10-machine, 39-bus power system integrated with DERs and corresponding cyber elements. In this example, DERs 1–5 are corrupt and DERs 6–10 are unaffected. The attacker and EPU will apply control policies to their corresponding DERs to achieve their individual objectives.

### D. Game-Theoretic Pursuer-Evader Formulation

Computation of control policies for both parties can be naturally formulated as a game theoretic problem. The adversary will construct attack vector $u_k^e$ that attempts to maximize state deviations from stable setpoints to instigate transient instability. We assert that, in essence, the adversary behaves like an evader attempting to deviate the system from stability. Upon detecting the onset of an attack, the EPU will design a countermeasure vector $u_k^p$ that aims to minimize state deviations

for a fixed time $K$ ($k \in \{1 \dots K\}$) by which time the incident can be isolated. The EPU therefore functions like a pursuer. If the EPU takes no counteraction, then there is potential for the system to move in the direction favorable to the adversary. Assumptions 1–3 (listed earlier) lead to both parties being forced to employ an open-loop information structure for control decisions. This particular information structure eliminates the need for an adversary to constantly intercept measurement data to construct an effective attack vector (i.e., less resources are required). On the other hand, this structure prevents the EPU from relying on possibly corrupt measurements for devising countermeasures. Since both pursuer and evader have opposing goals and each will execute a series of control actions over a finite time period to achieve individual objectives, this in effect represents a finite time two-player zero sum (2PZS) noncooperative differential game. The reader should note that throughout this paper we employ variable/parameter annotations $P$ or $p$ to denote pursuer (i.e., EPU) and $E$ or $e$ to denote evader (i.e., attacker).

One main assumption made in this formulation is that both the EPU and the attacker behave in a rational but selfish manner. Due to this assumption, both players will use best-response (no-regret) policy to devise their strategies. A no-regret policy for the attacker is to maximize the minimum possible state deviations for all combinations of control actions by the EPU while for the EPU it is minimizing the maximum possible state deviations from $x_k^s$ for all possible attacks. As both players behave rationally, each party can distributively compute individual control strategies by solving the corresponding optimization problem listed in $P_P$ and $P_E$ (i.e., the 2PZS smart grid attack-mitigation game) over $k = 1, 2, \dots, K$ discrete time steps

$$\begin{aligned} &\textbf{(P}_P\textbf{):} && \textbf{(P}_E\textbf{):} \\ &\min_{U^e} \max_{U^p} J(U^p, U^e, X) && \max_{U^p} \min_{U^e} J(U^p, U^e, X) \\ &\text{s.t. } x_{k+1} = f\big(x_k, u_k^p, u_k^e\big) && \forall\ k = 1, 2, \dots, K \end{aligned}$$

where $U^e \in \mathbb{R}^{GXK}$ and $U^p \in \mathbb{R}^{GXK}$ are the control actions of the attacker and EPU on $E$ compromised and $P$ uncompromised cyber-physical DER elements, $X \in \mathbb{R}^{NXK}$ is the state trajectory of $N = 2G$ state variables, and $J(U^p, U^e, X)$ represents the cost function for each party.

Many types of equilibrium can exist in a differential game. Since the players take a best-response approach to devise their strategies, the Nash equilibrium (NE), defined as follows, is specifically considered.

*Definition 1:* NE results when both players having chosen strategies $U^{p*}$ and $U^{e*}$ cannot choose a strategy that is better than the current strategy as indicated by the following:

$$J\big(U^{p*}, U^e, X\big) \le J\big(U^{p*}, U^{e*}, X\big) \le J\big(U^p, U^{e*}, X\big). \quad (3)$$

The NE control strategy $U^{p*}$ of the EPU is the best effort countermeasure and the NE control strategy $U^{e*}$ of the attacker is the worst-case attack vector.

## III. Attack and Mitigation Strategy Construction

Attack and mitigation construction requires solving (3). However, in contrast to its linear counterpart, the 2PZS game with nonlinear dynamics cannot be solved analytically. Therefore, we develop a novel iterative algorithm for deriving open-loop strategies for the 2PZS smart grid attack-mitigation game with quadratic cost and nonlinear system dynamics over a finite time horizon. The iterative algorithm proposed in this paper is a differential game counterpart to the iterative linear quadratic regulator proposed in the optimal control literature (see [19], [20]) for deriving locally optimal feedback control laws in nonlinear systems.

Our algorithm improves the computation of the attack/mitigation strategies (which we in general call control policy) of each player in an iterative manner. Both players are first initialized with control policies $u_k^{p*}$ and $u_k^{e*}$ $\forall\ k \in \{1 \dots K\}$. The $k$th nonzero component of the control policy is initialized randomly but in a conservative manner to reduce chances of deriving control policies with noticeably large DER inputs or outputs. The corresponding state-input trajectory $x_k^*$ $\forall\ k \in \{1 \dots K\}$ is obtained by applying $u_k^{p*}$ and $u_k^{e*}$ to the original system dynamics of (2). At each iteration, the algorithm obtains a linear approximation of the original nonlinear game around this state-input trajectory. The linearized game is solved to analytically compute the improvement to the current NE strategy for each player. Thus, the update can be interpreted as an incremental best-response of each player in the linearized game. The iterations are repeated until the cost of the game no longer changes.

### A. Linearizing System Dynamics

The nonlinear system dynamics of the 2PZS game listed in (2) is linearly approximated around $x_k^*$, $u_k^{p*}$, and $u_k^{e*}$ by applying first-order Taylor Series expansion, which results in

$$\delta x_{k+1} = A_k \delta x_k + B_k^p \delta u_k^p + B_k^e \delta u_k^e \quad (4)$$

where $\delta x_{k+1} = x_{k+1} - f(x_k^*, u_k^{p*}, u_k^{e*})$, $\delta x_k = x_k - x_k^*$, $\delta u_k^p = u_k^p - u_k^{p*}$, $\delta u_k^e = u_k^e - u_k^{e*}$, $A_k = (\partial f)/(\partial x_k)|_{x_k^*}$, $B_k^p = (\partial f)/(\partial u_k^p)|_{u_k^{p*}}$, and $B_k^e = (\partial f)/(\partial u_k^e)|_{u_k^{e*}}$. Thus, $\delta u_k^p$ and $\delta u_k^e$ can be interpreted as the incremental improvement to the current control policies $u_k^{p*}$ and $u_k^{e*}$, and $\delta x_{k+1}$ as the deviation from the state trajectory $x_{k+1}^*$ induced by $\delta u_k^p$ and $\delta u_k^e$. From this point on, $\delta x_k$, $\delta u_k^p$, and $\delta u_k^e$ will be considered the new state and control variables.

### B. Cost Function

We formulate the 2PZS smart grid attack-mitigation game by accounting for the objectives of both players. The overall cost of the game is represented as the sum of a per-stage cost $h_k$ incurred over the control horizon $k = 1, 2, \dots, K$. Moreover, as discussed in Section II-D both players optimize with respect to the degree of state deviation from the stable trajectory and the magnitude of individual control policies. As discussed in the introduction, a stealthy attack is one that must go unnoticed for a period of time and therefore should not trigger commonly deployed safety mechanisms such as circuit breakers that can alert the EPU to a possible concern. Circuit breaker opening can result from excessive DER energy flow which can be caused by discontinuous high magnitude actuation by the attacker. If these detection mechanisms are alerted prematurely, then the attacker will be prevented from inflicting

more damage on the system. Thus, the attacker would prefer to limit this type of system reaction by employing smaller continuous magnitude control policies. Additionally, the EPU would also prefer a control policy with lower magnitude in order to conserve resources until the attack can be isolated. Thus, we let

$$J\big(\delta u^p, \delta u^e\big) = \sum_{k=1}^{K} h_k\big(\delta x_k, \delta u_k^p, \delta u_k^e\big) \tag{5}$$

where

$$\begin{aligned} h_k(\delta x_k, \delta u_k^p, \delta u_k^e) = \frac{1}{2}\Big[&\big(x_{k+1}^D + \delta x_{k+1}\big)' Q_{k+1}\big(x_{k+1}^D + \delta x_{k+1}\big) \\ &+ \big(u_k^{p*} + \delta u_k^p\big)'\big(u_k^{p*} + \delta u_k^p\big) \\ &- \big(u_k^{e*} + \delta u_k^e\big)'(\alpha_k I)\big(u_k^{e*} + \delta u_k^e\big)\Big] \end{aligned} \tag{6}$$

$x_k^D = x_k^* - x_k^s$, and $Q_k$ and $\alpha_k$ are cost matrices. The first term of (6) reflects the deviation of current state-input trajectory from the stable trajectory. The EPU will select $\delta u_k^p$ that minimizes $J$ and the attacker will select $\delta u_k^e$ that maximizes $J$. Since both players will desire to minimize their control policy magnitudes, the second and third terms have opposite signs. For a unique local NE to exist, $J$ must satisfy Theorem 1.

*Theorem 1 [21]:* If the cost function $J(\delta u^p, \delta u^e)$ is strictly convex in $\delta u^p$ and strictly concave in $\delta u^e$, a unique NE solution $(\delta u^{p*}, \delta u^{e*})$ exists.

Due to the quadratic form of $J$, conditions listed in Lemma 1 allowing $J$ to satisfy Theorem 1 can be derived.

*Lemma 1:* Necessary and sufficient conditions for strict convex-concavity of the quadratic cost function $J(\delta u^p, \delta u^e)$

$$\begin{aligned} \text{Convexity:}\quad & C_k \succ 0 \ \forall k \in K \\ \text{where}\quad & C_k = B_k^{p'} Q_{k+1} B_k^p + I \\ \text{Concavity:}\quad & D_k \succ 0 \ \forall\ k \in K \\ \text{where}\quad & D_k = \alpha_k I - B_k^{e'} S_{k+1} B_k^e \\ & S_k = Q_k + A_k' S_{k+1} A_k + \\ & A_k' S_{k+1} B_k^e \Big(\alpha_k I - B_k^{e'} S_{k+1} B_k^e\Big)^{-1} B_k^{e'} S_{k+1} A_k \\ & S_{K+1} = Q_{K+1}. \end{aligned}$$

Derivation of Lemma 1 is listed in the Appendix. Restricting $Q_k$ to be positive definite allows $J$ to be strictly convex as $C_k \succ 0$. For $J$ to be strictly concave, $\alpha_k$ is adjusted so that $D_k$ is diagonally dominant. This adjustment of $\alpha_k$ can be interpreted as a penalty on $\delta u_k^e$ for deviating from the strict concavity condition. The structuring of $\alpha_k$ that allows $J$ to meet the strict concavity condition is listed in the Appendix.

### C. Attack and Mitigation Vectors

With the aid of $Q_k$ and $\alpha_k$, the cost function is structured to guarantee the existence of a unique local NE solution for the linearized system. As $J$ is strictly convex-concave, the solution for $\delta u_k^e$ and $\delta u_k^p$ can be computed in closed-form as listed in Theorem 2 via the minimum principle extended for two-player games [21]. Now, equipped with a method to compute $\delta u_k^p$ and $\delta u_k^e$, these updates can be applied to iteratively improve the control policies $u_k^{p*}$ and $u_k^{e*}$. This process is repeated until the change in cost $J$ between iterations is less than a threshold $\tau$. The attacker applies the resulting $u_k^{e*}$ to the compromised DERs and the EPU applies $u_k^{p*}$ on the remaining DERs as a countermeasure.

TABLE I
ALGORITHM FOR 2PZS GAME WITH NONLINEAR DYNAMICS

Initialization:
- Set the iteration count: $i \leftarrow 0$.
- Randomly but conservatively select values for $u_k^{e*(0)}$, $u_k^{p*(0)}$.

Algorithm: ($\forall\ k = 1...K$)
1) $x_1^* \leftarrow x_1^s$; $x_{k+1}^* \leftarrow f(x_k^*, u_k^{p*(i)}, u_k^{e*(i)})$.
2) Evaluate $A_k$, $B_k^p$, $B_k^e$ using $x_k^{*(i)}$, $u_k^{p*(i)}$, $u_k^{e*(i)}$.
3) Evaluate $\alpha_k$ using backward recursion.
4) Evaluate $N_k$, $M_k$, $v_k$, $\Delta_k$ via backward recursion.
5) Compute $\delta x_k$, $\delta u_k^p$ and $\delta u_k^e$ using Theorem 2.
6) Evaluate whether $u_k^{e*}$ and $u_k^{p*}$ heed DER actuation limits $[l_d, c_d]\ \forall\ d \in \{1 \dots G\}$ and reset these values to the corresponding limits if necessary.

If $|J^i - J^{i-1}| < \tau$ is met then terminate. Else, repeat Algorithm.

*Theorem 2:* If the cost function $J$ is strictly convex-concave, the following are the closed-form expressions for the incremental NE solution:

$$\begin{aligned} \delta x_{k+1} &= \Delta_k^{-1}\big[A_k \delta x_k - N_k M_{k+1} - B_k^e u_k^{e*} - B_k^p u_k^{p*}\big];\ \delta x_1 = 0 \\ \delta u_k^p &= -B_k^{p'}\big[Q_{k+1} x_{k+1}^D + v_{k+1} + M_{k+1}\delta x_{k+1}\big] - u_k^{p*} \\ \delta u_k^e &= \alpha_k^{-1} B_k^{e'}\big[Q_{k+1} x_{k+1}^D + v_{k+1} + M_{k+1}\delta x_{k+1}\big] - u_k^{e*} \end{aligned}$$

where

$$\begin{aligned} \Delta_k &= I + N_k M_{k+1} \\ N_k &= B_k^p B_k^{p'} - B_k^e \alpha_k^{-1} B_k^{e'} \\ M_k &= Q_k + A_k' M_{k+1} \Delta^{-1} A_k;\ M_{K+1} = Q_{K+1} \\ v_k &= A_k'\Big[v_{k+1} + Q_{k+1} x_{k+1}^D - M_{k+1}\Delta^{-1} \\ &\qquad \times\big(N_k\big(Q_{k+1} x_{k+1}^D + v_{k+1}\big) + B_k^e u_k^e + B_k^p u_k^p\big)\Big]; \\ v_{K+1} &= 0 \end{aligned} \tag{7}$$

### D. Summary of Algorithm

A summary of the iterative algorithm proposed to compute the open-loop control strategies of the 2PZS game with nonlinear system dynamics is presented in Table I.

The assumptions listed in Section II-B provide sufficient knowledge and means for both attacker and EPU to distributively compute their respective control policies using this iterative algorithm. As the literature dedicated to 2PZS games with nonlinear dynamics is limited, we do not provide theoretical guarantees for the convergence of the proposed algorithm to the solution of the nonlinear game and therefore the resulting control policies can be suboptimal. However, we are able to demonstrate through case studies in the following section that this algorithm remains effective in designing attack and mitigation vectors that adequately meet the objectives of each

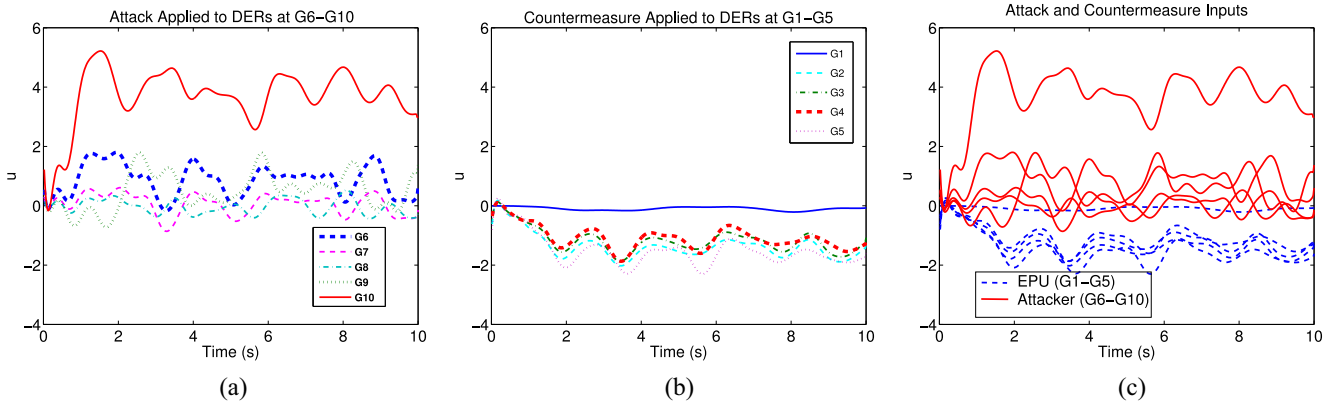


Fig. 2. Attack and countermeasure vectors applied to DERs. (a) Attack vectors. (b) Countermeasure vectors. (c) Attack and countermeasure vectors.

player in a realistic power system configuration. More specifically, when only the attacker applies his/her control policy on only a subset of DERs, we show that the system states move into transient instability as expected. On the other hand, when both the attack and counter strategies are applied simultaneously, the EPU is able to contain state deviations within the tolerance margins of transient stability.

## IV. Results

The impact of control policies designed using the iterative algorithm in Table I is studied under various settings for an IEEE ten machine 39-bus system implemented in MATLAB/Simulink. In all simulations, the control time horizon is set to 10 s as it is assumed that the attack can be isolated within this period. The frequency at which control signals are transmitted to DERs is 50 Hz ($K = 500$), which is the assumed rate at which PMUs communicate with the grid. Initial states of the system before an attack are at stable values.

### A. Cyber-Physical Model

So far, a generalized dynamical system listed in (2) has represented the underlying cyber-physical interactions in the power system. Here, we make use of a specific model proposed in [22] and extended in [12], that is adapted for our problem given our impact focus on transient stability. The power network with $g$ synchronous generators is simplified using Kron reduction and the generators are modeled via swing equations. Fast acting power absorbing and injecting DERs such as flywheels that are cyber controlled are assumed to be present at the vicinity of each synchronous generator for improved resilience. The physical state of the $i$th synchronous generator is represented by its frequency $\omega_i$ and phase angle $\theta_i$. Cyber and physical coupling affecting the state of the $i$th power generator is modeled as

$$\dot{\omega}_i = \frac{1}{M_i}\left[u_i + P_i\right] \text{ and } \dot{\theta}_i = \omega_i \tag{8}$$

for $i = 1, 2, \ldots, g$ where $u_i$ is the impact on the dynamics introduced by cyber-controlled DER actuation related to the $i$th synchronous generator and $P_i$ is the set of

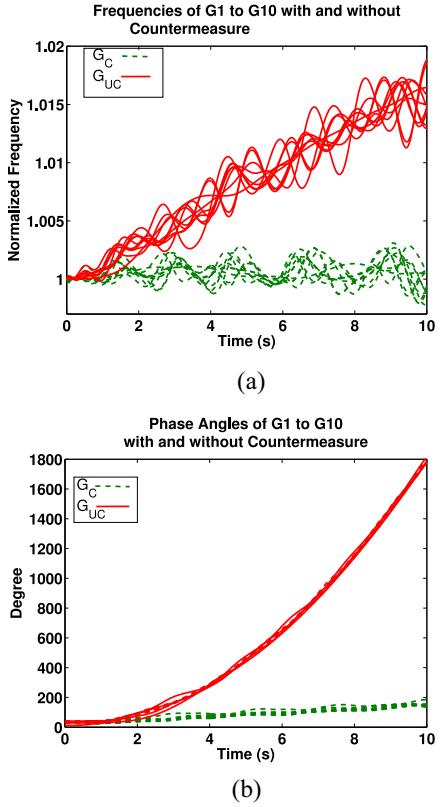


Fig. 3. Transient stability of G1–G10. (a) Normalized frequency. (b) Phase angle (°).

interconnected swing equations derived from the Kron-reduced power grid

$$P_i = -D_i\omega_i + P_{m,i} - |E_i|^2 G_{ii} - \sum_{j=1, j\neq i}^{g} P_{ij}\sin\left(\theta_i - \theta_j + \psi_{ij}\right) \tag{9}$$

where $P_{ij}$ reflects the equivalent admittance, conductance, and susceptance between the $i$th and the $j$th generators and $\psi_{ij}$ is the loss of energy due to transfer conductance between generator $i$ and $j$ [22].

It is clear that this dynamical system is highly nonlinear. Moreover, the reader should note that for the purpose of

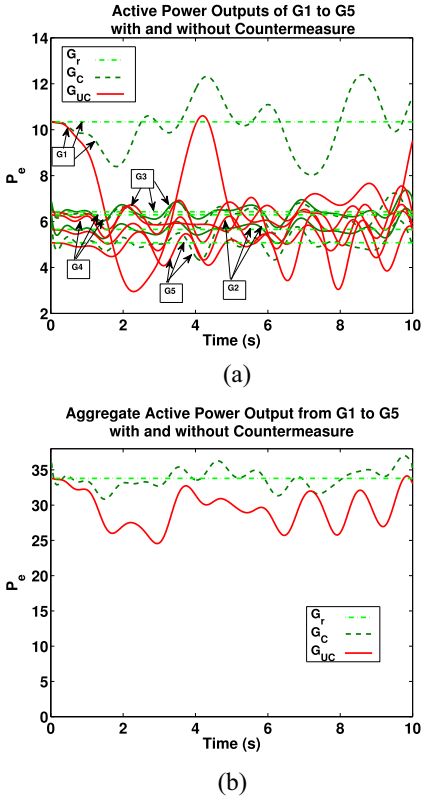


Fig. 4. EPU controlled systems. (a) Active generation. (b) Aggregate active generation.

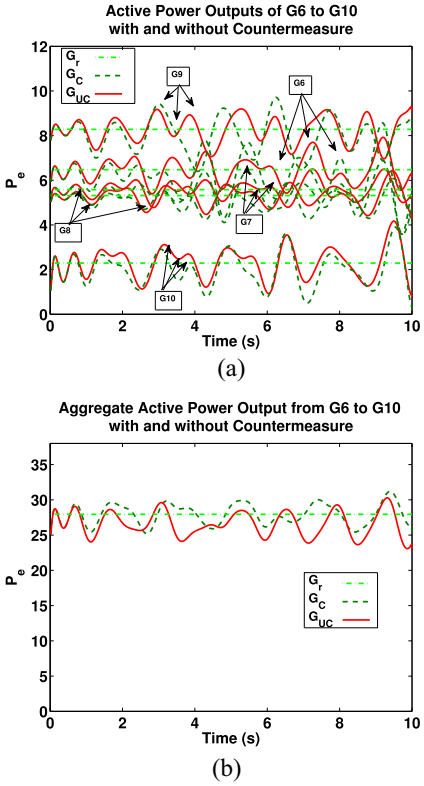


Fig. 5. Attacker controlled systems. (a) Active generation. (b) Aggregate active generation.

constructing a tractable differential game model, we have limited ourselves to a swing equation-based model of generators. We do not believe this poses a significant concern. Since we have not included the dynamics of other stabilizing controls such as a governor or exciter in the formulation, our analysis provides a conservative vulnerability assessment. Thus, successful strategies to counteract attacks, we believe, will be at least as successful as our results in this paper show and the guidelines gleaned from this analysis will still be of value for improving resilience and security.

### B. Validation

Attack and countermeasure strategies are constructed using the method outlined in Table I. In the IEEE 39-bus system, we consider a scenario where only a subset of DERs is corrupted. More specifically, as illustrated in Fig. 1, DERs associated with generators 6–10 are compromised while the remaining five DERs are not; the corresponding power absorption and injection limits $[l_i, c_i]$ of DERs 1–5 and 6–10 are $[-6, 1]$ and $[-1, 6]$, respectively.

Fig. 3(a) and (b) illustrates the impact of applying the attack and countermeasure vectors on the normalized frequencies and phase angles of generators 1–10 in the IEEE 39-bus system for two cases. In the first case, the DERs 6–10 are under attack and the EPU takes no action to circumvent this. In the second case, the EPU applies its countermeasure vector on DERs 1–5 right after the onset of the attack. Fig. 3(a) and (b) illustrates how the normalized frequencies and phase angles of generators evolve over the control horizon from the time the attack has commenced (at 0 s) to the time of isolation (at 10 s). When no countermeasure is applied, it is evident that the generator frequencies denoted by $G_{UC}$ diverge away from the stable value 1. Similarly, the phase angles digress significantly when only the attack is applied to the system. When the EPU applies the countermeasure to the system under attack, it is able to maintain the normalized frequencies and phase angles of all generators within the tolerable transient stability margins.

The impact of the attacks on active power generation is presented in Figs. 4 and 5. $G_r$ denotes regular active power inputs of generators when there is no attack. When the system is under attack and countermeasures are not in place (i.e., $G_{UC}$), the active power inputs are highly oscillatory and this behavior is clearly evident in the aggregate active power input plots in Figs. 4(b) and 5(b). These oscillations can significantly damage inductive loads due to the ringing effects caused by the harmonic content introduced by these oscillations [23]. On the other hand, when the EPU applies the countermeasure during the attack (i.e., $G_C$), it is able to reduce oscillation amplitudes and prevent active power inputs from diverging from $G_r$.

The attack and countermeasure vectors utilized for this particular set of results are illustrated in Fig. 2. The attack vector does not contain sharp bursts of power injection or absorption that may trip safety mechanisms such as circuit breakers and control inputs lie within the imposed limits. These DER actuation vectors are distinct from one another as these are highly dependent on the physical properties of the power system and

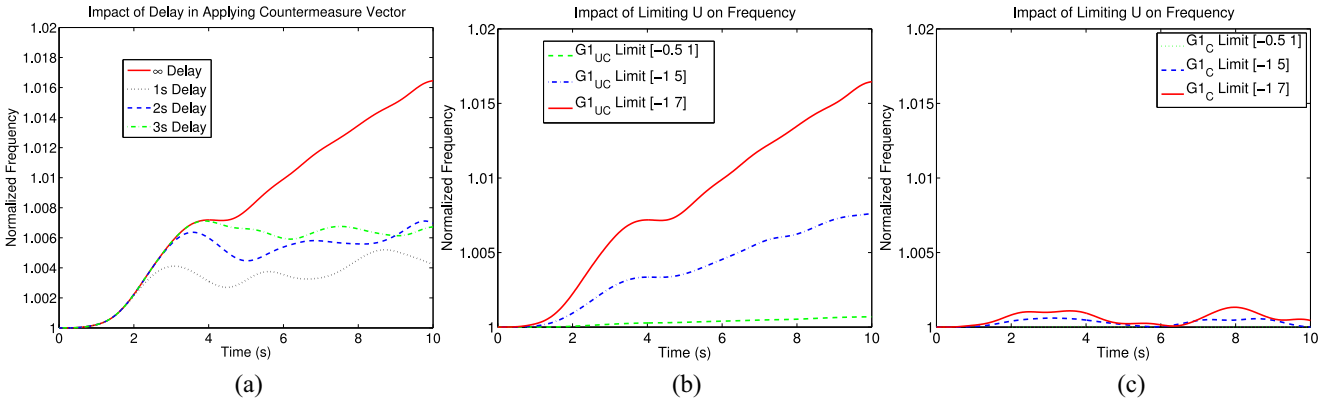


Fig. 6. Impacts of delay and limits on cyber actuation on generator frequencies. (a) Varying delay. Varying $U$ (b) without countermeasure and (c) with countermeasure.

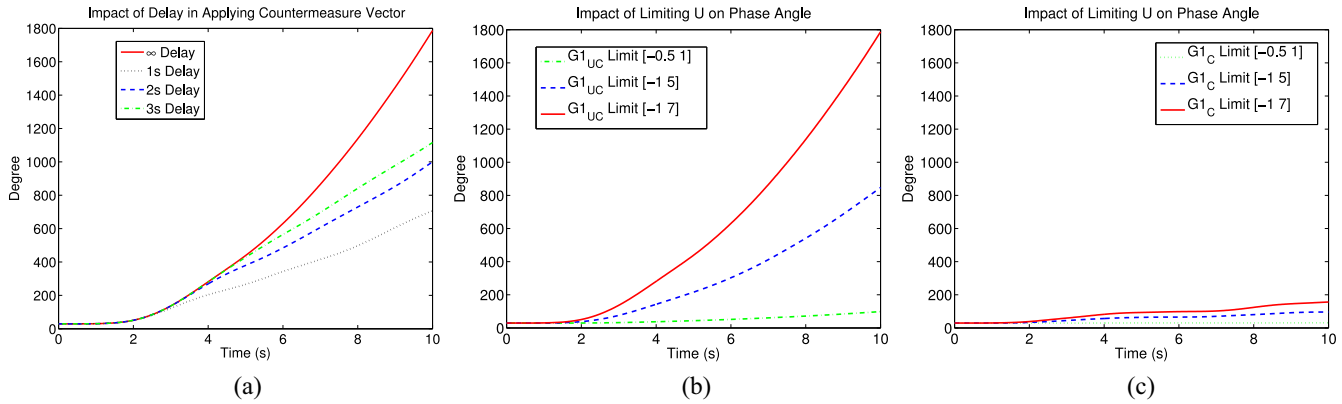


Fig. 7. Impacts of delay and limits on cyber actuation on generator phase angles. (a) Varying delay. Varying $U$ (b) without countermeasure and (c) with countermeasure.

DER power limits. For instance, the countermeasure vector of DER 1 which is associated with generator 1 is not high in magnitude (i.e., $u_1$ is close to 0) and this maybe due to the power limitation of $[-6, 1]$ imposed on DER 1 and/or the physical properties and interactions in the vicinity of generator 1 which are captured by the swing equations in (9). These results demonstrate that once an adversary is able to compromise a set of DERs with sufficient capacities, these can be manipulated to move the grid away from equilibrium when the attacker acts alone. These also show that successful countermeasures that aim to reduce the impact of the attack do potentially exist in practice when effective attack detection and identification schemes are in place.

### C. Design Considerations

From the above results, it is clear that when the EPU applies no countermeasure, the attacker can successfully introduce significant deviation to system states which inevitably leads to the tripping of synchronous generators. In accordance with the attacker's goals, consequences of the attack will be cascading failures and system-wide disruptions. Hence, it is critical for the EPU to identify the onset of the attack as soon as possible. Another important factor is the power limits imposed on the DERs. The larger the bounds are, the better equipped will the attacker be to inflict lasting damage on the system. The degree of damage inflicted on the grid due to delays in identifying an attack can be limited by imposing safety margins on the capacity of cyber-actuating elements. We present detailed analyses investigating these tradeoffs for an IEEE 39-bus system and demonstrate how these results are useful for constructing a comprehensive vulnerability assessment framework.

First, the impact of delay in applying the countermeasure is investigated. Figs. 6(a) and 7(a) illustrate the normalized frequency and phase angle of the generator 1 when the countermeasure vector is dispatched with a delay of 1–3 s. For comparison, the normalized frequency and phase angle of the generator when the countermeasure is not applied (i.e., delay is $\infty$) is also included. The power limits on DERs 1–5 and 6–10 are fixed to $[-6, 1]$ and $[-1, 6]$ for results in Figs. 6(a) and 7(a). When there is a delay in applying the countermeasure, the attacker has an advantage over the EPU as the system states have already begun to deviate by the time the countermeasure is dispatched. Since the EPU does not have a head start and does not utilize the current snapshot of the grid due to possible loss of integrity in the reported measurements, it is forced to manage with the available information and resources. In general, regardless of the delay, the application of the countermeasure results in the normalized frequency of the generator returning toward the stable value 1. When the countermeasure is not applied, the phase angle diverges in an exponential manner. When the countermeasure is applied after

a delay, the phase angle increases slowly in a linear manner. As the delay increases, the normalized frequency of the system takes longer to return to 1 and the slope of the phase angle trajectory increases. Even though repercussions of the delay are evident, the countermeasure vector is able to somewhat reduce the impact of the attack on state deviations. It is clear that the EPU must be able to identify the onset of the attack as soon as possible to maximally reduce its impact.

Next, the impact of various power limits imposed on DERs 6–10 on system states when the attacker is the only active participant is illustrated in Figs. 6(b) and 7(b). For these results, the power limits on DERs 6–10 is set to one of $[-0.5, 1]$, $[-1, 5]$, and $[-1, 7]$. It is clear that as the limit increases, the attacker has greater potential to move the grid into transient instability faster. For instance, when the limit is set to $[-1, 7]$, the attack vector can move the normalized frequency to almost 1.02. The system will succumb into transient instability when the normalized frequency exceeds $\pm 2\%$ of the nominal value. When the limit on cyber actuation has higher restrictions, the maximum state deviations that the adversary can perpetuate within the control horizon also decreases. This gives a larger time window for the EPU to identify and dispatch its protection mechanisms. These observations also apply to the phase angle plot in Fig. 7(b). When the limit on DERs 6–10 is $[-1, 7]$, the phase angle of generator 1 increases rapidly to very high magnitudes. The impact on these attacked systems when countermeasures are applied via DERs 6–10 is depicted in Figs. 6(c) and 7(c). These plots indicate that when the countermeasure vector is applied in parallel to the attack, it is able to suppress the state deviations for all three power limits.

A vulnerability assessment framework requires the identification and assessment of all possible risks introduced by assets in a system. In the attack-mitigation model introduced in this paper, we consider risks originating from cyber elements integrated with the DERs. The degree of the risk can be gauged by evaluating its likelihood and severity. Risk likelihood can be estimated using the Delphi approach [3]. Given that an approximation of the time required for the EPU to detect the onset of an attack is available, the risk severity of each DER in the system can be determined. If the delay incurred to identify an attack is greater than the time window within which the DER can be manipulated to cause the system states to diverge into transient instability, then the risk associated with the DER is high. Based on this information, risk prioritization can be performed to deduce appropriate safety margin recommendations for cyber-actuation elements to deal with time-critical cyber security breaches.

## V. Conclusion

In this paper, we study how an attacker can construct stealthy attack vectors to manipulate compromised cyber-physical DERs to perpetuate physical instability in a smart grid. We also demonstrate that an EPU can devise countermeasure vectors by formulating its interactions with the attacker as a 2PZS differential game. Since analytical principles cannot be applied to solve a highly nonlinear 2PZS game, a new iterative algorithm is proposed here to overcome this difficulty. It is shown that when only the attack vector is applied to a system as large as the 10-machine 39-bus IEEE power grid, the system moves away from a stable equilibrium enabling the attacker to win. When the countermeasure vector is simultaneously applied to the system, the EPU is able to successfully circumvent the attack and subdue the system states to lie within a stability threshold. The results of this research also facilitate risk assessment to establish safety margins that allow the deployment of mechanisms that adequately protect the system during a security breach. As future work, the integration of other cyber-actuating elements and attack models that include distributed generation systems, false injection, and switching attacks is imperative for a comprehensive vulnerability assessment framework that further extends the safety margin analysis presented in this paper.

## Appendix

### A. Proof for Lemma 1

$\delta u_k^p$ is present in the first and second terms of the per stage cost function $h_k(.)$ in (6). Expanding $\delta x_{k+1}$ and grouping like terms results in $C_k$ being the quadratic form matrix of $\delta u_k^p$. For $h_k(.)$ to be strictly convex, $C_k$ must be positive definite [24]. $C_k \succ 0\ \forall k = 1 \ldots K$ forces all $h_k(.)$ to be strictly convex. Since convexity is preserved in linear combinations of convex functions, $J(.)$ results in being a strictly convex function.

Proving the concavity condition is more involved as the third term of $h_k(.)$ in (6) is negative. Since the control-strategies are computed in the open-loop and values that $\delta u_k^p$ take do not affect the structure of $\delta u_k^e$, the original game is treated as a single player optimal control problem [21]. Hence, without loss of generality, the following variables are set to 0: $\delta u_k^p$, $x_{k+1}^D$ and $u_k^p$ resulting in the per-stage cost being $g(\delta x_k, \delta u_k^e) = 1/2[\delta u_k^{e'}(\alpha_k I)\delta u_k^e - \delta x'_{k+1} Q_{k+1} \delta x_{k+1}]$. Since the game is now converted into an optimal control problem, dynamic programming can be applied to obtain the conditions for strict concavity. In dynamic programming, value function is defined as $V(k, \delta x) = \min_{\delta u_k^e}[g(\delta x_k, \delta u_k^e) + V(k+1, \delta x_{k+1})]$. According to [21], the value function of a linear quadratic optimal control problem has a quadratic form $V(k, \delta x) = \delta x'_k S_k \delta x_k$. For $V(k, \delta x)$ to exist, the expression minimized above must be convex. This is true only if $D_k \succ 0$ is satisfied. The expression for $S_k$ is precisely the reverse algebraic Riccatti equation used in linear quadratic regulator optimal control problem and is derived in a similar manner here [25].

### B. Structuring $\alpha_k$

$\alpha_k$ is a diagonal matrix and varying $\alpha_k$ will modify the diagonal elements of $D_k$. According to the Gershgorin theorem, if each diagonal entry in a real matrix is greater than the sum of other elements in the same row, then the real part of all eigenvalues of the matrix will be positive [26]. This is a sufficient condition to ensure the positive definiteness of a matrix. Values for $\alpha_k$ can be obtained by via backward recursion. $S_{K+1} = Q_{K+1}$ is the boundary condition on $S_k$. Starting at $k = K$, the $i$th entry of $\alpha_k$ is set to $\sum_{l=j; l\neq i}^{n} -[B_k^{e'} S_{k+1} B_k^e]_{ij} + \epsilon$ for $\epsilon > 0$.

## ACKNOWLEDGMENT

The authors would like to thank Prof. L. Pavel for providing feedback on the initial development of this paper.

## REFERENCES

[1] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Security*, Chicago, IL, USA, 2009, pp. 21–32.

[2] M. El-Halabi, A. Farraj, H. Ly, and D. Kundur, "A distortion-theoretic perspective for redundant metering security in smart grid," in *Proc. IEEE Can. Conf. Elect. Comput. Eng. (CCECE)*, Montreal, QC, Canada, Apr./May 2012, pp. 1–5.

[3] D. Kundur, "Power system reliability, security and stability, class notes for ECE1518: Seminar in identity, privacy and security," Dept. Elect. Comput. Eng., Univ. Toronto, Toronto, ON, Canada, 2014.

[4] S. Sridhar, A. Hahn, and G. Manimaran, "Cyber-physical security for electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[5] A. Hahn and G. Manimaran, "Cyber attack exposure evaluation framework for the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 835–843, Dec. 2011.

[6] P. Rezaei, P. Hines, and M. Eppstein, "Estimating cascading failure risk with random chemistry," *IEEE Trans. Power Syst.*, vol. 30, no. 5, pp. 2726–2735, Sep. 2015.

[7] 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.

[8] T. Liu *et al.*, "Abnormal traffic-indexed state estimation: A cyber–physical fusion approach for smart grid attack detection," *Future Gener. Comput. Syst.*, vol. 49, pp. 94–103, Aug. 2015.

[9] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, DOI: 10.1109/JSYST.2014.2341597.

[10] M. Esmalifalak, Z. Han, and L. Song, "Effect of stealthy bad data injection on network congestion in market based power system," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Shanghai, China, 2012, pp. 2468–2472.

[11] S. Liu, B. Chen, D. Kundur, T. Zourntos, and K. Butler-Purry, "Progressive switching attacks for instigating cascading failures in smart grid," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Vancouver, BC, Canada, 2013, pp. 1–5.

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

[13] P. Kundur *et al.*, "Definition and classification of power system stability: IEEE/CIGRE joint task force on stability terms and definitions," *IEEE Trans. Power Syst.*, vol. 19, no. 3, pp. 1387–1401, Aug. 2004.

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

[15] S. Backhaus *et al.*, "Cyber-physical security: A game theory model of humans interacting over control systems," *IEEE Trans. Smart Grid*, vol. 4, no. 4, pp. 2320–2327, Dec. 2013.

[16] G. Andersson *et al.*, "Cyber-security of SCADA systems," in *Proc. IEEE PES Innov. Smart Grid Technol.*, Washington, DC, USA, 2012, pp. 1–2.

[17] E. Hammad, A. Farraj, and D. Kundur, "A resilient feedback linearization control scheme for smart grids under cyber-physical disturbances," in *Proc. IEEE PES Innov. Smart Grid Technol.*, Washington, DC, USA, 2015, pp. 1–5.

[18] Y. J. Kim, M. Thottan, V. Kolesnikov, and W. Lee, "A secure decentralized data-centric information infrastructure for smart grid," *IEEE Commun. Mag.*, vol. 48, no. 11, pp. 58–65, Nov. 2010.

[19] P. Abbeel, "Optimal control for linear dynamical systems and quadratic cost, class notes for CS 287: Advanced robotics," Dept. Elect. Eng., Univ. California, Berkeley, CA, USA, 2013.

[20] E. Todorov and W. Li, "Optimal control methods suitable for biomechanical systems," in *Proc. 25th Annu. Int. Conf. IEEE EMBS*, vol. 2. Cancún, Mexico, 2003, pp. 1758–1761.

[21] T. Basar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, 2nd ed. Philadelphia, PA, USA: SIAM, 1999.

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

[23] P. Srikantha, C. Rosenberg, and S. Keshav, "An analysis of peak demand reductions due to elasticity of domestic appliances," in *Proc. Future Energy Syst.*, Madrid, Spain, 2012, pp. 1–10.

[24] D. Bertsekas, A. Nedic, and A. E. Ozdaglar, *Convex Analysis and Optimization*. Belmont, MA, USA: Athena Scientific, 2003.

[25] R. Kwong, "Linear quadratic optimal control," *Lect. Notes Univ. Toronto*, 2013.

[26] E. A. Carlen, "The symmetric eigenvalue problem, class notes for MATH2605: Calculus III," Dept. Comput. Sci., Georgia Tech University, Atlanta, GA, USA, 2003.

**Pirathayini Srikantha** (S'14) received the B.A.Sc. degree in systems design engineering with distinction (Dean's Honours List), and the M.A.Sc. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2009 and 2013, respectively. She is currently pursuing the Ph.D. degree with the Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON.

Her current research interests include investigating how effective solutions can be designed for current applications in the electric smart grid such as cyber-security, sustainable power dispatch, demand response using convex optimization, and game theoretic techniques.

Ms. Srikantha was a recipient of the Best Paper Award Recognition at the Third IEEE International Conference on Smart Grid Communications in 2012 for the Symposium of Demand Side Management, Demand Response, and Dynamic Pricing.

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

From 1999 to 2002, she was an Assistant Professor with the Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, where she became a Professor in 2012. She currently serves as the Associate Chair of the Division of Engineering Science. From 2003 to 2012, she was a Faculty Member of Electrical and Computer Engineering, Texas A&M University, College Station, TX, USA. Her current research interests include cyber-security of the electric smart grid, cyber-physical system theory, security and privacy of social and sensor networks, multimedia security, and computer forensics.

Prof. Kundur was a recipient of the Best Paper/Poster Recognitions from various venues and Teaching Awards from both the University of Toronto and Texas A&M University. She has participated on several editorial boards and currently serves as an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. She serves as the General Chair for the IEEE GlobalSIP 2015 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.