2011 50th IEEE Conference on Decision and Control and
European Control Conference (CDC-ECC)
Orlando, FL, USA, December 12-15, 2011

Robust and Resilient Control Design for Cyber-Physical Systems with an Application to Power Systems

Quanyan Zhu and Tamer Başar

Abstract— **The tradeoff between robustness and resilience is a pivotal design issue for modern industrial control systems. The trend of integrating information technologies into control system infrastructure has made resilience an important dimension of the critical infrastructure protection mission. It is desirable that systems support state awareness of threats and anomalies, and maintain acceptable levels of operation or service in the face of unanticipated or unprecedented incidents. In this paper, we propose a hybrid theoretical framework for robust and resilient control design in which the stochastic switching between structure states models unanticipated events and deterministic uncertainties in each structure represent the known range of disturbances. We propose a set of coupled optimality criteria for a holistic robust and resilient design for cyber-physical systems. We apply this method to a voltage regulator design problem for a synchronous machine with infinite bus and illustrate the solution methodology with numerical examples.**

I. Introduction

The migration of many current critical infrastructures such as power grids and transportations systems into open public networks has posed many challenges in control systems. The classical design of control systems takes into account modeling uncertainties as well as physical disturbances and encompasses a multitude of control design methods such as robust control, adaptive control, and stochastic control. With the growing level of integration of control systems with new information technologies, modern control systems face uncertainties not only from the physical world but also from the cyber space. IT uncertainties are often unanticipated and more catastrophic as compared to the ones from the physical world. It is imperative to consider such IT uncertainties in addition to the physical ones in the controller design. In [1], [**?**], the concept of a resilient control system has been proposed, which emphasizes the control system design in an adversarial and uncertain cyber environment. A resilient control system needs to maintain the state awareness of threats and anomalies and assure an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature. Traditional concepts of robustness, reliability and defense in depth need to be broadened to include the consideration of cyber and physical security and threats from malicious behaviors.

Resilient control design pivots on the inherent system tradeoff between *robustness* and *resilience*. In [2] and [3], the distinctions between these two concepts are discussed and elaborated in the context of power systems. Robustness refers to the operation of a system under a given range of perturbations or disturbances whereas resilience refers to the restoration of a system under unexpected extreme and rare events. As pointed out in [2], robustness and resilience are not general properties of a system but are relative to specific classes of perturbations. A system that is resilient or robust to a certain type of perturbations may be brittle or fragile to another. Centralized systems are often more robust yet less resilient than decentralized systems. Systems with a global coordination can withstand a larger range of uncertainties or disturbances, but may fail to respond to unforeseen attacks or faults. Such tradeoff is essential to the design of system architecture and its control.

The metric of robustness in control systems has been well studied in [4] and [5]. In [5], a game-theoretical approach has been used to yield a minimax, disturbance attenuating control by viewing the controller as the cost minimizer and the disturbance as the cost maximizer. A metric for resilient control systems has recently been introduced and discussed in [6], [7]. However, not much effort has been expended in studying the resilient control design, and almost none on a holistic approach to resilient and robust control design. In this paper, we address this design issue using a hybrid dynamic game-theoretic approach, combining Markov chain dynamics with continuous-time H^∞ control.

The hybrid model provides a holistic and cross-layer viewpoint to decision-making and design for cyber-physical systems. The continuous-time dynamics model the physical layer plant subject to disturbances and control efforts. The discrete-time dynamics model the cyber layer of the system, which involves human factors. We use a zero-sum differential game for the optimal control design at the physical layer and a stochastic zero-sum game between an administrator (or defender) and an attacker for the design of the defense mechanisms. The designs at the physical and the cyber layers are intertwined. A policy made at the cyber layer can influence the optimal control design for the physical system; and the optimal control design at the lower level needs to be taken into account when security policies are determined. The overall optimal design of the cyber-physical system is characterized by a Hamilton-Jacobi-Isaacs (HJI) equation together with a Shapley-like optimality criterion. Our framework connects the resilient control for the cyber system with the robust control for the physical system.

The rest of the paper is organized as follows. In Section II, we first motivate the combined approach to resilient and robust control by introducing a hierarchical layered view-

Q. Zhu and T. Başar are with the Department of Electrical & Computer Engineering and Coordinated Science Laboratory, University of Illinois, 1308 West Main St., Urbana, IL, 61801, USA., University of Illinois at Urbana-Champaign. {zhu31, basar1}@illinois.edu. Research supported in part by grants from DOE and an AFOSR MURI.

978-1-61284-799-3/11/$26.00 ©2011 IEEE

point of cyber-physical systems. In Section II-A, we present the hybrid system model, and we describe the optimality conditions in Section II-B and Section II-C. In Section III, we characterize the solution for the special class of linear-quadratic problems. In Section IV, we present an application in power systems and illustrate with numerical examples. We conclude the paper in Section V with some general remarks and identification of future work.

II. Resilient and Robust Control

In this section, our aim is to establish a theoretical framework for designing resilient controllers. To address this challenge, we first need to understand the architecture of industrial control systems (ICSs). Here, we adopt a layering perspective toward ICSs. This view-point has been adopted in many large scale system designs such as the Internet, power systems and nuclear power plants. For example, in smart grids, the hierarchical architecture includes economy grid, regulatory grid, electricity market grid, transmission grid and distribution grid, etc. We hierarchically separate ICSs into 6 layers, namely, physical layer, control layer, communication layer, network layer, supervisory layer and management layer.

The physical layer comprises the physical plant to be controlled. The control layer consists of multiple control components, including observers/sensors, intrusion detection systems (IDSs), actuators and other intelligent control components. The physical layer together with the control layer can be viewed as the physical world of the system. On top of these two layers, the communication layer is where we have physical communication channels that can be in the form of wireless channels, the Internet, etc., and the network layer is where the topology and routing of the architecture live. The communication and network layers constitute the cyber world of the system. Supervisory layer coordinates all lower layers by designing and sending appropriate commands. It can be viewed as the brain of the system. Management layer is a higher level decision-making engine, where the decision-makers take an economic perspective towards the resource allocation problems in control systems. Supervisory and management layers are interfaces with humans and hence they contain many human factors and human-made decisions.

The layered architecture can facilitate the understanding of the cross-layer interactions between the physical world and the cyber world. In Fig. 1, we use $x(t)$ and $\theta(t)$ to denote the continuous physical state and the discrete cyber state of the system, which are governed by the laws f and Λ, respectively. The physical state $x(t)$ is subject to disturbances w and can be controlled by u. The cyber state $\theta(t)$ is controlled by the defense mechanism l used by the network administrator as well as the attacker's action a. The hybrid nature of the cross-layer interaction leads to adoption of the hybrid system model described later through (1) and (2).

As mentioned earlier, in this section our goal is to establish a framework for designing a resilient controller for the hybrid system model described. We view resilient control as a cross-layer control design, which takes into account the given range of deterministic uncertainties at each state as well as the random unexpected events that trigger the transition from one system state to another. Hence, it has the property of disturbance attenuation or rejection to physical uncertainties as well as damage mitigation or resilience to sudden cyber attacks. We first derive resilient control for the closed-loop perfect-state measurement information structure in a general setting with the transition law dependent on the control action, and then we simplify the result to the special case of the linear quadratic problem.

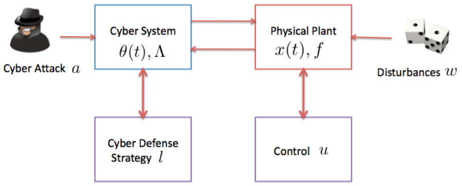

Fig. 1. The interactions between the cyber and physical systems are captured by their dynamics governed by the transition law Λ and the dynamical system f.

A. Control Framework

We consider a general class of systems subject to two types of uncertainties: a continuous deterministic uncertainty that models the known parametric uncertainties and disturbances, and a discrete stochastic uncertainty that models the unknown and unanticipated events that lead to a change in the system operation state at random times. Let the system state evolve according to the piecewise deterministic dynamics:

$$\dot{x}(t) = f(t, x, u, w; \theta(t, a, l)), \quad x(t_0) = x_0, \qquad (1)$$

where $x(t) \in \mathbb{R}^n$, x_0 is a fixed (known) initial state of the physical plant at starting time t_0, $u \in \mathbb{R}^r$ is the control input, $w \in \mathbb{R}^p$ is the disturbance. x, u, w are quantities that lie at the physical and control layers of the entire system.

The state of the cyber system is described by θ. We model the process $\theta(t), t \in [0, t_f]$, by a Markov jump process with right-continuous sample paths, with initial distribution π_0, and with rate matrix $\lambda = \{\lambda_{ij}\}_{i,j \in \mathcal{S}}$, where $\mathcal{S} := \{1, 2, \cdots, s\}$ is the state space; $\lambda_{ij} \in \mathbb{R}_+$ are the transition rates such that for $i \neq j, \lambda_{ij} \geq 0$, and $\lambda_{ii} = 1 - \sum_{j \neq i} \lambda_{ij}$ for $i \in \mathcal{S}$.

Transitions between the structural states are controlled by the attacker and the system administrator. An attacker can exploit the vulnerabilities in the control system software and launch an attack to bring down the operation. An example is Stuxnet, a Windows-based worm that was recently discovered to target industrial software and equipment [10]. An administrator can enforce the security by dynamically updating the security policy of control systems [11], [12]. Once an attack occurs, the administrator can restore the system to normal operation. Different from conventional computer networks, control systems are reported to experience lower rates of attacks [7] and the software updates are less frequent than the ones in computer networks. Hence, the transition between structural states are on a different time scale from the evolution of the physical states. We assume that the systems have reached their physical steady states when the structural transition takes place. This assumption can be validated by two facts. The first is that the attack rate on control systems is often lower than the one on information systems, [17], and the second one is that the time scale of the failure rate of devices and components in control systems is larger than the one of the system dynamics and operations [18].

Let $k = t/\epsilon, \epsilon > 0$, be the time scale on which cyber events happen, which is often on the order of days, in contrast to the one of the physical systems which evolve on the time scale of seconds. Denote by $a \in \mathcal{A}$ a cyber attack chosen by the attacker from his attack space $\mathcal{A} := \{a_1, a_2, \cdots, a_M\}$ composed of all possible actions. $l \in \mathcal{L}$ is the cyber defense mechanism that can be employed by the network administrator where $\mathcal{L} := \{l_1, l_2, \cdots, l_N\}$ is the set of all the possible defense actions. Without loss of generality, we assume that $\mathcal{A}$ and $\mathcal{L}$ do not change in time even though, in practice, they can change due to technological updates and advances. We consider the mixed strategies $\mathbf{f}(k) = [f_i(k)]_{i=1}^N \in \mathcal{F}_k, g(k) \in \mathcal{G}_k$ of the defender and the attacker, respectively, where $f_i(k)$ and $g_j(k)$ are the probabilities of choosing $l_i \in \mathcal{L}$ and $a_j \in \mathcal{A}$, respectively, where $\mathcal{F}_k$ and $\mathcal{G}_k$ are sets of admissible strategies, defined by $\mathcal{F}_k := \{\mathbf{f}(k) \in [0,1]^N : \sum_{i=1}^N f_i(k) = 1\}$ and $\mathcal{G}_k := \{\mathbf{g}(k) \in [0,1]^M : \sum_{j=1}^M g_j(k) = 1\}$. The transition law of the cyber system state $\theta(k)$ at time k depends on the actions of the attacker as well as the defense mechanism employed by the administrator. More precisely, the rate matrix has the form

$$\text{Prob}\{\theta(k+\Delta) = j | \theta(k) = i\} = \begin{cases} \lambda_{ij}(\mathbf{f}(k), \mathbf{g}(k)), & j \neq i, \\ \lambda_{ii}(\mathbf{f}(k), \mathbf{g}(k)), & j = i, \end{cases} \tag{2}$$

where $\Delta > 0$ which is on the same time scale as k, i.e., in days, and $\lambda_{ij}(\mathbf{f}(k), \mathbf{g}(k))$ are the average transition rates in terms of the transition rates $\tilde{\lambda}_{ij}(a(k), l(k)),\ i, j \in \mathcal{S}$, defined by $\lambda_{ij}(\mathbf{f}(k), \mathbf{g}(k)) = \sum_{i=1}^N \sum_{j=1}^M f_i(k) g_j(k) \tilde{\lambda}_{ij}(a_i(k), l_j(k))$.

B. H^∞ Optimal Control

Systems described by (1) and (2) are hybrid ones with continuous and discrete states and they have been investigated earlier in [8], [9]. Let $\mathcal{F}_t$ be the sigma-field generated by $\theta_{[t_0,t]} := \{\theta(s), s \leq t\}$. Denote by $\mathcal{U}$ and $\mathcal{W}$ the sets of admissible controls and disturbance processes, respectively, which are $\mathcal{F}_t-$measurable, and piecewise continuous. We assume that f is piecewise continuous in t and Lipschitz continuous in (x, u, w), for each fixed sample path of θ, with probability one. The process θ models the unanticipated or rare uncertainties that arise from cyber attacks or component failures. These events result in random structural changes in the dynamics of the system. We consider a closed-loop perfect state information structure for the control design. The controller has access to $x_{[t_0,t]}$ and $\theta_{[t_0,t]}$ at time t and has the form $u(t) = \mu(t, x_{[t_0,t]}; \theta_{[t_0,t]}),\ t \in [t_0, t_f]$, where μ is an admissible closed-loop control strategy, piecewise continuous in its first argument, and Lipschitz continuous in its second argument. We denote the class of all such control strategies by $\mathcal{M}_{\text{CL}}$. Analogously, denote by $\mathcal{N}_{\text{CL}}$ the class of all closed-loop disturbance strategies $v(t) = \nu(t, x_{[t_0,t]}; \theta_{[t_0,t]}),\ t \in [t_0, t_f]$. The performance index for the hybrid control system is the expected cost over the statistics of θ, given by

$$J(u, v) := \mathbb{E}_\theta\{L(x, u, w; \theta)\}, \tag{3}$$

with the cost function L given as

$$\begin{aligned} L(x, u, w; \theta) &= q_0(x_0; \theta(t_0)) + q_f(x(t_f); \theta(t_f)) \\ &\quad + \int_{t_0}^{t_f} g(t, x(t), u(t), w(t); \theta(t)) dt, \end{aligned} \tag{4}$$

where q_f is continuous in x, and g is jointly continuous in (t, x, u, w). In the infinite-horizon case, q_f is absent and $t_f \to \infty$. The objective is to find a minimax closed-loop controller $\mu^*_{\text{CL}} \in \mathcal{M}_{\text{CL}}$ that infimizes the supremum of J over all closed-loop disturbance policies:

$$\sup_{\nu \in \mathcal{N}_{\text{CL}}} J(\mu^*_{\text{CL}}, \nu) = \inf_{\mu \in \mathcal{M}_{\text{CL}}} \sup_{\nu \in \mathcal{N}_{\text{CL}}} J(\mu, \nu). \tag{5}$$

A cost structure of interest is the separable one:

$$g(t, x, u; \theta) = g_0(t, x, u; \theta) - \gamma^2 r(w; \theta). \tag{6}$$

The solution of (5) parameterized in γ is denoted by μ^*_γ and γ_{CL} is the smallest value of $\gamma > 0$ for which the right hand side of (5) is bounded. Then $\mu^*_{\gamma,\text{CL}}$ is the H^∞ controller for the hybrid system, with respect to the performance index:

$$\sup_{w \in \mathcal{W}} \left\{ \frac{\mathbb{E}_\theta\{q_f(x_f; \theta(t_f)) + \int_{t_0}^{t_f} g_0(t, x(t), u(t); \theta(t)) dt\}}{\mathbb{E}_\theta\{\|w\|^2 + q_0(x_0; \theta(t_0))\}} \right\},$$

where $\|\cdot\|$ denotes the $\mathcal{L}_2$-norm of w for each sample path of θ. The minimum value of the performance index is γ^2_{CL}. It defines a measure of disturbance attenuation in the nonlinear hybrid system. Note that in (5), we have considered x_0 as part of disturbance.

Consider the differential game described by (5). Let $V(\cdot) : \mathbb{R} \times \mathbb{R}^n \times \mathcal{S}$ denote the cost-to-go function associated with this differential game, i.e., $V(t, x, i)$ is the upper value of a similar game defined on the shorter interval $[t, t_f]$, with initial state x, and initial structure $\theta(t) = i$. We assume that the differential game defined by (5) has an upper value V for every initial time t, state $x(t)$, and structure $\theta(t)$, which is jointly continuously differentiable in (t, x). Under this assumption, we have the associated Isaacs equation:

$$\begin{aligned} -V^i_t(t, x) &= \inf_{u \in \mathbb{R}^r} \sup_{w \in \mathbb{R}^p} \{V^i_x(t, x) f(t, x, u, w, i) + \\ &\quad g(t, x, u, w, i) + \sum_{j \in \mathcal{S}} \lambda_{ij} V^j(t, x)\}, \quad (7) \\ V^i(t_f, x) &= q_f(x(t_f); i); \quad i \in \mathcal{S}. \quad (8) \end{aligned}$$

Any control $u \in \mathbb{R}^r$ that achieves the minimum on the right hand of (7) correspond to a control policy that is a memoryless function of (x, θ). Denote any such control law by $\mu^{\mathrm{F}} \in \mathcal{M}_{\mathrm{CL}}$ and (7) can be rewritten as

$$\begin{aligned}-V_t^i(t,x) &= \sup_{w\in\mathbb{R}^p} \{V_x^i(t,x)f(t,x,\mu^{\mathrm{F}}(t,x,i),w,i) \\ &\qquad +g(t,x,\mu^{\mathrm{F}}(t,x,i),w,i) + \sum_{j\in\mathcal{S}} \lambda_{ij}V^j(t,x)\}.\end{aligned}$$

Furthermore, if Isaacs condition holds and if there exists a disturbance policy, $\nu^{\mathrm{F}} \in \mathcal{N}_{\mathrm{CL}}$, that achieves the maximum in (7), then ν^{F} is also a Markov policy, and $(\mu^{\mathrm{F}}, \nu^{\mathrm{F}})$ are in saddle-point equilibrium. In this case, the upper value is also the value function, satisfying the PDE:

$$\begin{aligned}-V_t^i(t,x) &= \sup_{w\in\mathbb{R}^p} \{V_x^i(t,x)f(t,x,\mu^{\mathrm{F}}(t,x,i),\nu^{\mathrm{F}}(t,x,i),i) \\ &\qquad +g(t,x,\mu^{\mathrm{F}}(t,x,i),\nu^{\mathrm{F}}(t,x,i),i) + \sum_{j\in\mathcal{S}} \lambda_{ij}V^j(t,x)\}.\end{aligned}$$

The optimal cost $V^i(t_0,x_0)$ generates a measure on the resilience and robustness of the system. It is desirable that the costs on faulty structure states are kept relatively lower than the normal operation states. The tradeoff between resilience and robustness can be seen from the two-fold controller design in which one goal is to spend control effort to bring the system back to normal operation mode following the occurrence of unanticipated events and the other goal is to yield optimal performance for the control system in each operating state.

C. Optimal Defense

The defense against attacks happens on a longer time scale and involves decision-making at the human and cyber levels of the system. Using time-scale separation, the optimal defense mechanism can be designed by viewing the physical control system at its steady state at each cyber state θ at a given time k. The interaction between an attacker and a defending administrator can be captured by a zero-sum stochastic game with the defender aiming to maximize the long-term system performance or payoff function and the attacker aiming to minimize it [13]. We use a discounted payoff criterion $V_\beta(s,\mathbf{f},\mathbf{g})$, defined as

$$V_\beta(i,\mathbf{f}(k),\mathbf{g}(k)) := \int_0^\infty e^{-\beta k}\mathbb{E}_i^{\mathbf{f}(k),\mathbf{g}(k)} V^i(k,\mathbf{f}(k),\mathbf{g}(k))dk,$$

where β is the discount factor. The operator $\mathbb{E}_i^{\mathbf{f},\mathbf{g}}$ is the expectation operator and $V^i(k,\mathbf{f}(k),\mathbf{g}(k))$ is the value function at state i with starting time at k in (4) and its dependence on $\mathbf{f}(k),\mathbf{g}(k)$ is from the state transition between states in (2). We consider a class of mixed stationary strategies $\mathbf{f}^i \in \mathcal{F}^i$ and $\mathbf{g}^i \in \mathcal{G}^i, i \in \mathcal{S}$, that are only dependent on the current cyber state i. Let $\mathbf{F} = \{\mathbf{f}_i\}_{i\in\mathcal{S}} \in \mathcal{F}_S$ and $\mathbf{G} = \{\mathbf{g}_i\}_{i\in\mathcal{S}} \in \mathcal{G}_S$, where $\mathcal{F}_S := \prod_{i\in\mathcal{S}} \mathcal{F}^i$ and $\mathcal{G}_S := \prod_{i\in\mathcal{S}} \mathcal{G}^i$. The following theorem characterizes the stationary saddle-point equilibrium of the stochastic zero-sum game in a similar fashion as in [13], and [14].

Theorem 1: Assume that $\lambda_{ij}(k)$ are continuous in $\mathbf{f}^i$ and $\mathbf{g}^i$ and the value functions $V^i(k)$ are bounded. There exists a pair of stationary strategies $(\mathbf{F}^*,\mathbf{G}^*) \in \mathcal{F}_S \times \mathcal{G}_S$ such that, for all $i \in \mathcal{S}$, the following fixed-point equation is satisfied.

$$\begin{aligned}\beta v_\beta^*(i) &= V^i(\mathbf{F}^*,\mathbf{G}^*) + \sum_{j\in\mathcal{S}} \lambda_{ij}(\mathbf{F}^*,\mathbf{G}^*)v_\beta^*(j) \qquad (9)\\ &= \sup_{\mathbf{F}\in\mathcal{F}_S} \{V^i(\mathbf{F},\mathbf{G}^*) + \sum_{j\in\mathcal{S}} \lambda_{ij}(\mathbf{F},\mathbf{G}^*)v_\beta^*(j)\} \\ &= \inf_{\mathbf{G}\in\mathcal{G}_S} \{V^i(\mathbf{F}^*,\mathbf{G}) + \sum_{j\in\mathcal{S}} \lambda_{ij}(\mathbf{F}^*,\mathbf{G})v_\beta^*(j)\} \\ &= \sup_{\mathbf{F}\in\mathcal{F}_S} \inf_{\mathbf{G}\in\mathcal{G}_S} \{V^i(\mathbf{F},\mathbf{G}) + \sum_{j\in\mathcal{S}} \lambda_{ij}(\mathbf{F},\mathbf{G})v_\beta^*(j)\} \\ &=: L_\beta(i) \\ &= \inf_{\mathbf{G}\in\mathcal{G}_S} \sup_{\mathbf{F}\in\mathcal{F}_S} \{V^i(\mathbf{F},\mathbf{G}) + \sum_{j\in\mathcal{S}} \lambda_{ij}(\mathbf{F},\mathbf{G})v_\beta^*(j)\} \\ &=: U_\beta(i)\end{aligned}$$

where $v_\beta(i) = V_\beta(i,\mathbf{F},\mathbf{G})$ and $L_\beta(i)$, $U_\beta(i)$ are defined to be the lower value and the upper value of the game. In addition, $(\mathbf{F}^*,\mathbf{G}^*)$ from (9) is a pair of saddle-point equilibrium strategies and the value of game $v_\beta^*(i)$ is unique and has the property that $v_\beta^*(i) = L_\beta(i) = U_\beta(i)$.

The saddle-point equilibrium strategies can be computed using a value iteration scheme [13]. Let $\{v_\beta^n(i)\}_{n=1}^\infty$ be a sequence of values of the game which obeys the following update law:

$$\begin{aligned}v_\beta^{n+1}(i) &= V^i(\mathbf{F}_n^*,\mathbf{G}_n^*) + \sum_{j\in\mathcal{S}} \lambda_{ij}(\mathbf{F}_n^*,\mathbf{G}_n^*)v_\beta^n(j) \qquad (10)\\ &= \sup_{\mathbf{F}\in\mathcal{F}_S} \{V^i(\mathbf{F}_n,\mathbf{G}_n^*) + \sum_{j\in\mathcal{S}} \lambda_{ij}(\mathbf{F}_n,\mathbf{G}_n^*)v_\beta^n(j)\}, \\ &= \inf_{\mathbf{G}\in\mathcal{G}_S} \{V^i(\mathbf{F}_n^*,\mathbf{G}_n) + \sum_{j\in\mathcal{S}} \lambda_{ij}(\mathbf{F}_n^*,\mathbf{G}_n)v_\beta^n(j)\}.\end{aligned}$$

It is clear that if this set of update laws converges from every starting point, then the limit is the unique saddle-point solution of the game.

D. Coupled Design

The design of robust and resilient control system needs to adopt a holistic viewpoint in which the physical layer robust control design needs to consider the cyber layer security mechanism, and the cyber defense protocol design needs to take into account the physical layer control performance.

Definition 1: Under the information structures specified in Sections II-B and II-C, a robust and resilient control for the cyber-physical system described by (1) is a set of optimal control policies $\{(\mathbf{F}^*,\mathbf{G}^*),(\mu^*,\nu^*)\}$ that satisfy the optimality criterion (9) coupled with HJI conditions (7).

The optimality criterion (9) in Theorem 1 together with HJI equation in (7) defines a set of coupled optimality conditions for cyber-physical systems that we need to solve to obtain the cyber policy $\mathbf{F}^*$ and the robust controller u and its associated performance index γ^*.

III. Linear-Quadratic Problem

In this section, we consider a special case of linear quadratic problem in which λ_{ij}'s are constant in x,u but can be time-varying, and $f(t,x,u,w;i) =$

$A^i x + B^i u + D^i w$, $q_f(t_f;i) = |x(t_f)|^2_{Q^i_{t_f}}$, $q_0(x_0,i) = |x_0|^2_{Q^i_0}$, $g_0(t,x,u,i) = |x|^2_{Q^i_{t_f}} + |u|^2_{R^i}$, $r(w;\theta) = |w|^2$, where $i \in \mathcal{S}$, $|\cdot|$ denotes the Euclidean norm with appropriate weighting, A^i, B^i, D^i, Q^i, R^i are matrices of appropriate dimensions, whose entries are continuous functions of time t. $Q^i(\cdot) \geq 0, R^i(\cdot) > 0$, and Q^i_0 is a positive-definite matrix and Q^i_f is a constant nonnegative-definite matrix. We consider an infinite horizon case with the cost function defined by $L(x,u,w;\theta) = \int_{t_0}^{\infty}(|x(t)|^2_{Q^i} + |u(t)|^2_{R^i} - \gamma^2|w(t)|^2)dt$. Before stating Theorem 2, we make the following assumptions:

(**A**1): Matrix functions R^i and Q^i_0 are positive definite for $i \in \mathcal{S}$.

(**A**2): The Markov chain θ is irreducible for any admissible strategies.

(**A**3): The pair (A^i, B^i) is stochastically stabilizable.

(**A**4): The pair (A^i, Q^i) is observable for each $i \in \mathcal{S}$.

***Theorem** 2 ([8]):* Consider the soft-constrained zero-sum differential game with perfect measurements in the infinite-horizon case. Let assumptions (**A**1)-(**A**4) hold. Then, $\gamma^*_{\text{CL},\infty} < +\infty$, and for any $\gamma_{\text{CL}} > \gamma^*_{\text{CL},\infty}$, there exists a set of minimal positive definite solutions $Z_i, i \in \mathcal{S}$, to GAREs,

$$A^{i'} Z_i + Z_i A^i - Z_i \left(B^i (R^i)^{-1} B^{i'} - \frac{1}{\gamma^2} D^i D^{i'} \right) Z_i + Q^i + \sum_{j=1}^{s} \lambda_{ij}(\mathbf{F}, \mathbf{G}) Z_j = 0; \quad i \in \mathcal{S}. \quad (11)$$

which further satisfy the condition

$$\gamma^2_{\text{CL}} Q^i_0 - Z_i \geq 0, \quad i \in \mathcal{S}, \quad (12)$$

and a strategy $\mu^*_{\gamma\infty}$ for P1 that guarantees the zero upper value is:

$$u^*_{\gamma\infty}(t) = \mu^*_{\gamma\infty}(t, x(t), \theta(t)) = -(R^i)^{-1} B^{i'} Z_i x(t). \quad (13)$$

For almost all $\gamma > \gamma^*_{\infty}$, the jump linear system driven by both the optimal control and the optimal disturbance,

$$\dot{x}(t) = \left(A^i - \left(B^i (R^i)^{-1} B^{i'} - \frac{1}{\gamma^2} D^i D^{i'} \right) Z_i \right) x(t) \quad (14)$$

is also mean-square stable, i.e., $\lim_{t \to \infty} \mathbb{E}\{|x(t)|^2\} = 0$.

For $\gamma < \gamma^*_{\text{CL},\infty}$, on the other hand, either condition (12) is not satisfied or the set of GAREs does not admit nonnegative definite solutions, and in both cases, the upper value of the game is $+\infty$.

On a longer time scale, the continuous-time zero-sum game between the attacker and the administrator has the stationary saddle-point equilibrium characterized by Theorem 1. More specifically, the fixed-point equation (9) can be written as

$$\beta v^*_{\beta}(i) = x_0' Z_i(\mathbf{F}^*, \mathbf{G}^*) x_0 + \sum_{j \in \mathcal{S}} \lambda_{ij}(\mathbf{F}^*, \mathbf{G}^*) v^*_{\beta}(j). \quad (15)$$

The optimal control u^* and the optimal defense strategy $\mathbf{F}^*$ need to be found by solving the coupled equations (15) and GAREs in Theorem 2. A demonstration of this is provided in the next section within the context of an application to power systems.

TABLE I

TABLE OF PARAMETERS

Symbol	Meaning
$k_c = 1$	Gain of the excitation amplifier
$D = 5.0$	Per unit damping constant
$H = 4.0$	Per unit inertia constant
$\omega_0 = 100\pi$	Synchronous machine speed
$P_m = 0.9$	Mechanical input power
$T_{d0} = 6.9$	Direct axis transient short circuit time constant
$V_s = 0.91$	Infinite bus voltage
$x_d = 1.863$	Direct axis reactance of the generator
$x'_d = 0.257$	Direct axis transient reactance of the generator
$x_T = 0.127$	Reactance of the transformer
$x_L = 0.4853$	Reactance of the transmission line

IV. APPLICATION TO POWER SYSTEMS

In this section, we apply the framework in Section II to the voltage regulation problem of a power generator subject to sudden faults or attacks. A power system has multiple generators interconnected through a large dynamic network. A common approach to designing control systems for generators is to model the dynamics of a single generator and to approximate everything else as an infinite bus, i.e., the voltage and the phase of the entire network are not affected by the input power or field excitation of the generator. We design a stabilizing control, called the power system stabilizer (PSS), used to damp out the low-frequency oscillations for a single-machine infinite-bus (SMIB) system [16]. A fault can occur as a result of an unexpected cyber attack. For example, an attacker can break into the IT system and damage the circuit breakers in a power grid, leading to an operation under a faulty state. It is important that we design a controller to regulate the system to equilibrium as quickly as possible if such a failure occurs [15], and at the same time a defense mechanism to protect the systems from possible attacks. We define a two-state operation: one is under the normal state ($\theta = 1$) and the other is the post-attack state ($\theta = 2$).

Denote by δ the power angle, ω the relative speed, P_e the active electrical power delivered by generator; and u_f the input of the amplifier of the generator as the control variable. The system equations to model SMIB are:

$$\begin{aligned}
\dot{\delta}(t) &= \omega(t); \\
\dot{\omega}(t) &= -\frac{D}{2H}\omega(t) + \frac{\omega_0}{2H}(P_m(t) - P_e(t)); \\
\dot{P}_e(t) &= -\frac{1}{T'_{d0}} P_e(t) + \frac{1}{T'_{d0}} \left\{ \frac{V_s}{x_{ds}} \sin(\delta(t)) \left[k_c u_f + \right.\right. \\
&\quad \left.\left. T'_{d0}(x_d - x'_d) \frac{V_s}{x'_{ds}} \omega(t) \sin(\delta(t)) \right] + T'_{d0} \omega(t) \text{cot}(\delta(t)) \right\} + w,
\end{aligned}$$

where w is the disturbance, $T'_{d0} = \frac{x'_{ds}}{x_{ds}} T_{d0}$; $x_{ds} = x_T + x_L + x_d$; $x'_{ds} = x_T + x_L + x'_d$; the main parameters listed in Table I and their values are chosen based on [16].

Under normal operation ($\theta = 1$), the control objective is to regulate the synchronous machine state $x := [x_1, x_2, x_3]' =$

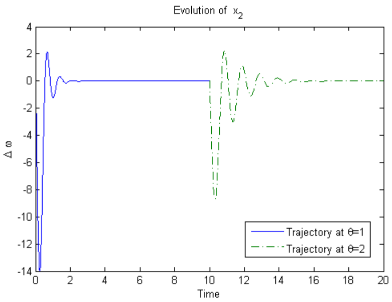

Fig. 2. Evolution of state x_2(i.e., ω) with failure happening at $t = 10$.

$[\delta, \omega, P_e]'$ to the level of $[\delta_0, 0, P_m]'$. We can linearize the system around the desired levels to achieve the goal.

The transition rates $\tilde{\lambda}_{ij}, i, j = 1, 2$, take the following parametrized form: $\tilde{\lambda}_{12} = p$, $\tilde{\lambda}_{11} = -p$, $\tilde{\lambda}_{21} = \tilde{\lambda}_{22} = 0$, where we have assumed that the operation after the attacker cannot immediately be recovered. At the cyber layer, the administrator (or the defender) can take two actions, namely, to defend ($l_1 =$ D) or not to defend ($l_2 =$ ND). The attacker can also take two actions, i.e, to attack ($a_1 =$ A) or not to ($a_2 =$ NA). The parameter p determines the transition law with respect to pure strategies and its values are tabulated as follows.

	A	NA
D	0.1	0.05
ND	0.95	0.05

In the above table, we have assumed a higher transition rate to a failure state if the attacker launches an attack while the cyber system does not have proper measures to defend itself. On the other hand, the rate is lower if the cyber system can defend itself from attacks. In the above table, we have assumed a base transition rate 0.05 to denote the inherent reliability of the physical system without exogenous attacks. We use the fixed-point equation (15) and GAREs in Theorem (2) to obtain the discounted value functions $v^*_\beta(i), i = 1, 2$, with the discount factor chosen to be $\beta = 1$. We set $x_0 = [\delta_0, 0, P_m]'$ and obtain $V^2 = 7.2075 \times 10^4$ independent of the parameter p. Hence, $v^*_\beta(2) = V^2$ and v^*_β obeys the following fixed-point equation $v^*_\beta(1) = \text{val}\,\{\mathbf{H} - v^*_\beta(1)\mathbf{G}\}$, where

$$\mathbf{H} = \begin{bmatrix} 1.4396 & 0.9994 \\ 8.4867 & 0.9994 \end{bmatrix} \times 10^4, \mathbf{G} = \begin{bmatrix} 0.1 & 0.05 \\ 0.95 & 0.05 \end{bmatrix},$$

where "val" is the value operator for a matrix game [13]. Using value iteration with initial value of $v^*_\beta(1)$ set to 0, we find $v^*_\beta(1) = 1.3087 \times 10^4$ and the corresponding stationary saddle-point strategy $\mathbf{f}^* = [1, 0]', \mathbf{g}^* = [0, 1]'$, which is a pure strategy leading to an optimal value of $p = 0.05$. The stationary saddle-point equilibrium strategy says that the defender should always be defending and the attacker should not be attacking. In Fig. 2, we show the evolution of state x_2 with failure happening at time $t = 10$. The optimal control design allows the state x_2 to stabilize after fault occurs. Note that our design methodology can be used to meet given resilient control design specifications such as degrading time, recovery time, performance loss, etc. [6], by choosing appropriate weighting matrices.

V. Conclusion

Control design in many critical infrastructures is challenged by the uncertainties from the cyber world. The goal of resilient control is to maintain an acceptable level of operation or service in face of undesirable incidents. In this paper, we have proposed a holistic theoretical framework for the robust and resilient control design problem for cyber-physical systems. We have applied the design methodology to a synchronous machine with infinite bus and obtained a robust and resilient feedback control strategy. Our future work will aim to investigate the impact of information structures on the control design. In particular, we are interested in systems with imperfect and delayed measurements.

References

[1] C.G. Rieger, D.I. Gertman, and M. A. McQueen, "Resilient control systems: next generation design research," In Proc. of the 2nd Conf. on Human System interactions, Catania, Italy, May 21 - 23, 2009, pp. 629 – 633.

[2] L. Mili, "Taxonomy of the characteristics of power system operating states," NSF-VT Resilient and Sustainable Critical Infrastructures (RESIN) Workshop, Tuscon, Arizona, Dec. 2010, URL: `http://www.nvc.vt.edu/lmili/publications.html`

[3] L. Mili, "Power and communications systems as integrated cyber-physical systems," in Proc. of 48th Allerton Conference on Communication, Control, and Computing, Allerton, IL, Sept. 2010, URL: `http://www.nvc.vt.edu/lmili/publications.html`

[4] K. Zhou and J. Doyle, *Essentials of Robust Control*, Prentice Hall, 1997.

[5] T. Başar and P. Bernhard, *H-infinity Optimal Control and Related Minimax Design Problems: A Dynamic Game Approach*, Birkhäuser, 1995.

[6] D. Wei and K. Ji, "Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights", in Proc. of 3rd Intl. Symp. on Resilient Control Systems (ISRCS), 2010.

[7] W. Boyer and M. McQueen, "Ideal based cyber security technical metrics for control systems", in Proc. of 2nd Intl. Workshop on Critical Information Infrastructures Security, Oct. 2007.

[8] Z. Pan and T. Başar, "H-infinity control of large scale jump linear systems via averaging and aggregation", *Intl. Journal of Control*, vol. 72, no. 10, pp. 866–881, 1999.

[9] T. Başar, "Minimax control of switching systems under sampling," *Systems and Control Letters*, vol. 25, no. 5, pp. 315–325, Aug. 1995.

[10] R. McMillan, Siemens: Stuxnet worm hit industrial systems, *Computerworld*, Sept. 16, 2010, `http://www.computerworld.com/s/article/print/9185419`, Retrieved Aug. 16, 2011.

[11] Q. Zhu, H. Tembine and T. Başar, "Network security configuration: a nonzero-sum stochastic game approach," in Proc. of 2010 American Control Conference (ACC 2010), Baltimore, Maryland, June 30 - July 2, 2010, pp. 1059–1064.

[12] Q. Zhu and T. Başar, "Dynamic policy-based IDS configuration," in Proc. of 48th IEEE Conf. on Decision and Control (CDC'09), Dec. 16-18, 2009; Shanghai, China, pp. 8600–8605.

[13] J. Filar and K. Vrieze, *Competitive Markov Decision Processes*, Springer-Verlag, 1996.

[14] O. Hernandez-Lerma and J. B. Lasserre, "Zero-sum stochastic games in Borel spaces: average payoff criterion," SIAM J. Control Optim., vol. 39, pp. 1520-1539.

[15] P. W. Sauer and M. A. Pai, *Power System Dynamics and Stability*, Prentice Hall, 1st edition, 1997.

[16] Y. Wang, D. J. Hill, R. H. Middleton and L. Gao, "Transient stability enhancement and voltage regulation of power systems," *IEEE Trans. on Power Systems*, vol. 8, no. 2, pp. 620–627, May 1993.

[17] Q. Zhu, M. McQueen, C. Rieger and T. Başar, "Management of control system information security: control system patch management," in Proc. of Workshop on the Foundations of Dependable and Secure Cyber-Physical Systems (FDSCPS-11), CPSWeek 2011, Chicago.

[18] A. D. Dominguez-Garcia, J. G. Kassakian, and J. E. Schindall, "A generalized fault coverage model for linear time-invariant systems," *IEEE Transactions on Reliability*, vol. 58, no. 3, pp. 553–567, Sept. 2009.