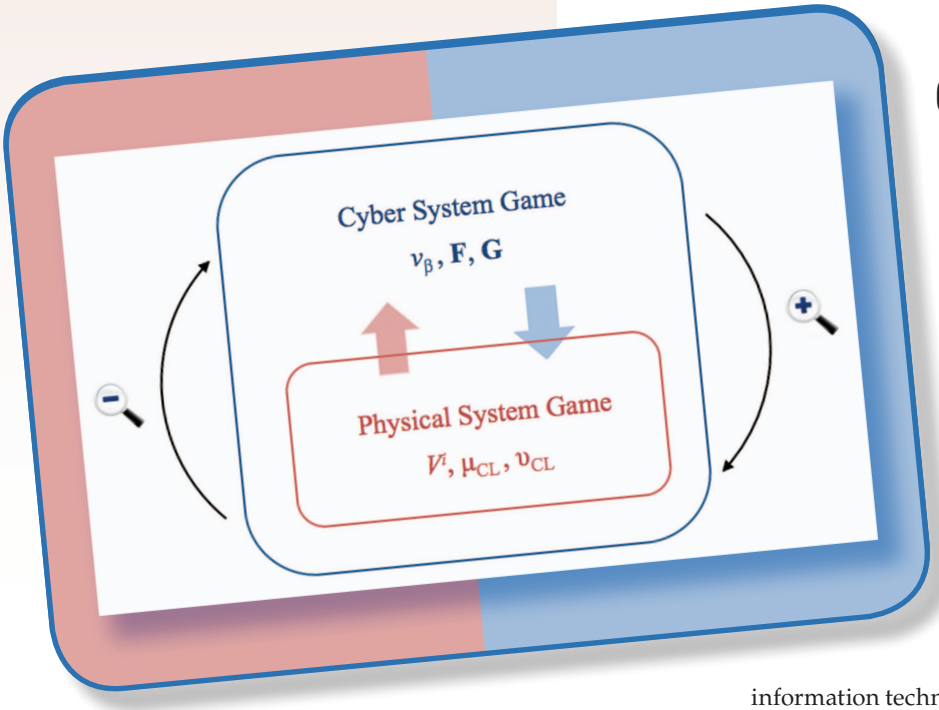
Game-Theoretic Methods for Robustness, Security, and Resilience of Cyberphysical Control Systems

QUANYAN ZHU and
TAMER BAŞAR



Digital Object Identifier 10.1109/MCS.2014.2364710
Date of publication: 19 January 2015

GAMES-IN-GAMES PRINCIPLE FOR OPTIMAL CROSS-LAYER RESILIENT CONTROL SYSTEMS

Critical infrastructures, such as power grids and transportation systems, are increasingly using open networks for operation. The use of open networks poses many challenges for control systems. The classical design of control systems takes into account modeling uncertainties as well as physical disturbances, providing 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 cybercomponents of the system. The vulnerabilities of the software deployed in the new control system infrastructure will expose the control system to many potential

1066-033X/15©2015IEEE

risks and threats from attackers. Exploitation of these vulnerabilities can lead to severe damage as has been reported in various news outlets [1], [2]. More recently, it has been reported in [3] and [4] that a computer worm, Stuxnet, was spread to target Siemens supervisory control and data acquisition (SCADA) systems that are configured to control and monitor specific industrial processes.

Uncertainties from the cybersystem are often unanticipated and more catastrophic for control systems in terms of their high impact and low effort as compared to those from the physical world. It is imperative to consider the cyber uncertainties in addition to the physical ones in the controller design. Those uncertainties can be caused by intentional malicious behaviors and/or by rare events, such as severe weather or natural disasters. Engineers are accustomed to designing systems to be reliable and robust, despite noise and disturbances. However, the cybersecurity aspect of control systems has posed new challenges for engineers and system designers.

The notion of *robustness* often refers to a system's ability to withstand a known range of uncertain parameters or disturbances, whereas *security* describes the system's ability to withstand and be protected from malicious behaviors and unanticipated events. These two system properties are *pre-event* concepts, that is, the system is designed to be robust or secure offline before it is perturbed or attacked. Despite many engineering efforts toward designing robust and secure systems, it is costly and impractical, if not impossible, to achieve perfect robustness and security against all possible attacks and events. This fact, however, renders it essential to investigate the *resilience* aspect of a system, which refers to the system's ability to recover online after adversarial events occur. It is a *post-event* concept. Hence, to provide performance guarantees, control systems should be designed to be inherently resilient, allowing them to self-recover from unexpected attacks and failures.

Resilience has been studied in many fields such as psychology [5], ecology [6], and organizational behavior [7]. The concept has also appeared in various engineering fields, such as aviation, nuclear power, oil and gas, transportation, emergency health care, and communication networks [8], [9]. The literature on resilience engineering is often found to be very diverse, qualitative, and area specific. References [10] and [11] propose the concept of resilient control systems, which emphasizes designing control systems for operation in an adversarial and uncertain environment. Resilient control systems are required to be capable of maintaining the state awareness of threats and anomalies and assuring an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature. Traditional concepts of robustness, reliability, and cybersecurity appear to be insufficient to address these emerging issues of control systems.

Metrics for robustness in control systems have been well studied in the literature [12], [13]. A game-theoretic approach has been introduced to obtain the H^∞ optimal, disturbance-attenuating minimax controllers by viewing the controller as the cost minimizer and the disturbance as the maximizer. Likewise, cybersecurity problems have been studied using game theory [14], which provides a natural framework for capturing the conflict of goals between an attacker who seeks to maximize the damage inflicted on the system and a defender who aims to minimize it. Moreover, the design of security strategies is enabled by many existing analytical and computational tools [15]. Many metrics for the resilience of control systems have been proposed recently [16]–[21].

The design of resilient control systems pivots on the fundamental system tradeoffs between robustness, resilience, and security. Perfect security could be achieved by making the system unusable, and likewise perfect robustness could be attained by making the control performance completely inadequate. The need for resilience is due to the fact that no desirable control systems exhibit perfect robustness or security. Hence, it is imperative in the control design to know what type of uncertainties or malicious events need to be considered for enhancing robustness and security and what uncertainties or malicious events need to

TABLE 1 A summary of notation.

Symbol	Meaning
$x(t)$	State of physical system
x_0	Initial state of physical system
$\theta(t)$	State of cybersystem
$u(t)$	Control input to the physical system
μ	Closed-loop control strategy
$w(t)$	Disturbance input to the physical system
$c(t,x,u;\theta)$	Instantaneous cost function
q_t	Terminal cost function
q_0	Cost function for initial condition
ν	Closed-loop strategy of disturbance
λ_{ij}	Transition rate from state i to state j
$\mathcal{A}$	Action space of the attacker
$\mathcal{L}$	Action space of the defender
$\mathbf{f}(k)$	Mixed strategy of the defender at time k
$\mathbf{g}(k)$	Mixed strategy of the attacker at time k
$J(u,w)$	Expected cost for the physical system performance
$V^i(t,x)$	Value function associated with the HJI equation
$v_\beta(i,\mathbf{f},\mathbf{g})$	Payoff for the cybersystem performance
$v^*_\beta(i)$	Value function associated with Shapley's optimality equation
γ^*_{CL}	Optimal attenuation level under closed-loop control strategies

be considered for post-event resilience. Studying these tradeoffs requires extending the control system design problem to include the cyberlayers of the system and understand the *cross-layer* issues in cyberphysical systems.

Resilient control, however, poses new challenges, different from the ones encountered in robust control and security games. Resiliency should be considered together with robustness and security since the post-event resiliency relies on the pre-event designs. Resilience builds upon robustness and security frameworks and takes a cross-layer approach by considering post-event system features. Since game theory has been successfully applied to study robustness and security, it is natural to adopt it as the main tool to build an extended and integrated framework.

The goal of this article is to introduce game-theoretic methods for resilient control design and develop a framework that studies the tradeoff between robustness, security, and resilience. A hybrid dynamic game-theoretic approach is introduced that integrates the discrete-time Markov model for modeling the evolution of cyberstates with continuous-time dynamics for describing the underlying controlled physical process. The hybrid dynamic game model provides a holistic and cross-layer viewpoint in the decision-making and design for cyberphysical systems. The continuous-time dynamics model the physical layer, that is, the plant, subject to disturbances and control efforts. The discrete-time dynamics model the cyberlayer of the system, which involves system configurations and dynamic human–machine interactions (HMIs). A zero-sum differential game is used for robust control design at the physical layer, while a stochastic zero-sum game between an administrator and an attacker is used for the design of defense mechanisms. The controlled transition between pre-event states to post-event states in the hybrid system framework leads to the design of the resilient hybrid dynamical system. The controller design at the physical layer and the security policy design at the cyberlayer of the system are intertwined. A policy made at the cyberlayer 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. For a class of system models, the overall optimal design of the cyberphysical system can be characterized by a Hamilton-Jacobi-Isaacs (HJI) equation together with a Shapley optimality criterion. The notations used in the article are summarized in Table 1 for the reader's convenience. For a brief introduction to game theory, see "Game Theory in a Nutshell".

HIERARCHICAL SYSTEMS

A cross-layer approach is pivotal for designing resilient control systems. Integrating physical control systems with cyberinfrastructure to allow for new levels of HMI has been a growing trend in the past few decades. To manage the increasing complexity of cyberphysical systems, it is essential that control designs exploit the hierarchical nature of such systems [22], [23]. Depicted in Figure 1, a cyberphysical control system can be conceptually divided into six layers: physical, control, communication, network, supervisory, and management.

Game Theory in a Nutshell

Game theory deals with strategic interactions among multiple decision makes, called players. Each player's preference ordering among multiple alternatives is captured in an objective function for that player. Players try to maximize (for utility or benefit functions) or minimize (for cost or loss functions) their respective objective functions. For a nontrivial game, the objective function of a player depends on the choices (*actions*, or equivalently *decision variables*) of at least one other player, and generally of all the players, and hence players cannot simply optimize their own objective function independent of the choices of the other players. This introduces a coupling between the actions of the players and binds them together in decision making even in a noncooperative environment.

A noncooperative game is *nonzero sum* if the sum of the players' objective functions cannot be made zero even after appropriate positive scaling and/or translation that do not depend on the players' decision variables. A two-player game is *zero sum* if the sum of the objective functions of the two players is *zero* or can be made zero by appropriate positive scaling and translation that do not depend on the decision variables of the players. A game is a *finite game* if each player has only a finite number of alternatives, that is, the players pick their actions out of finite sets (action sets); otherwise the game is an *infinite game*; finite games are also known as *matrix games*. An infinite game is said to be a *continuous-kernel game* if the actions sets of the players are subsets of finite-dimensional vector spaces, and the players' objective functions are continuous with respect to action variables of all players. A game is said to be *deterministic* if the players' actions uniquely determine the outcome, as captured in the objective functions, whereas if the objective function of at least one player depends on an additional variable (state of nature) with a known probability distribution, then the game is a *stochastic game*. A game is a *complete information* game if the description of the game [that is, the players, the objective functions, and the underlying probability distributions (if stochastic)] is common information to all players; otherwise it is an *incomplete information* game. Finally, a game is *static* if each player acts only once, and none of the players has access to information on the actions of any of the other players; otherwise it is a *dynamic game*. A dynamic game is said to be a *differential game* if the evolution of the decision process (controlled by the players over time) takes place in continuous time, and generally involves a differential equation.

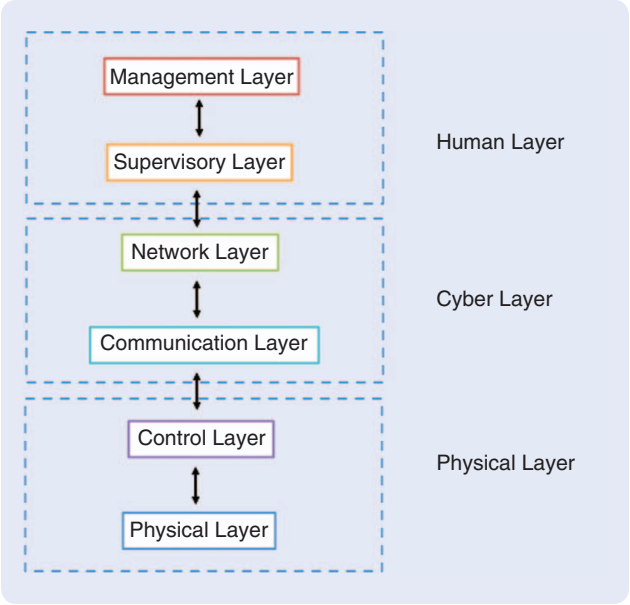


FIGURE 1 The hierarchical structure of cyberphysical control systems composed of six layers. The physical layer deals with the physical devices or chemical processes, such as electric machines and transmission lines of power system infrastructure, and electric vehicles in transportation networks. The control layer monitors and controls the physical layer system for achieving desired system performance. The communication layer provides wired or wireless data communications that enable advanced monitoring and intelligent control. The networking layer allocates network resources for routing and provides interconnections between system nodes. The supervisory layer is the executive brain of the entire system, provides human–machine interactions, and coordinates and manages lower layers through a centralized command and control. The management layer resides at the highest echelon. It deals with social and economic issues, such as market regulation, pricing, and incentives.

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 are the communication layer, which establishes physical layer wired or wireless communications, and the network layer that allocates resources and manages routing. The communication and network layers constitute the cyberworld of the system. Note that these two layers generally represent all the layers of open system interconnection (OSI) model [24], [25], which can be incorporated into the cyberlayers of the system. The supervisory layer serves as the brain of the system, coordinating all lower layers by designing and sending appropriate commands. The 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. The supervisory and management layers are often interfaced with humans, and hence they contain human factor issues and HMIs.

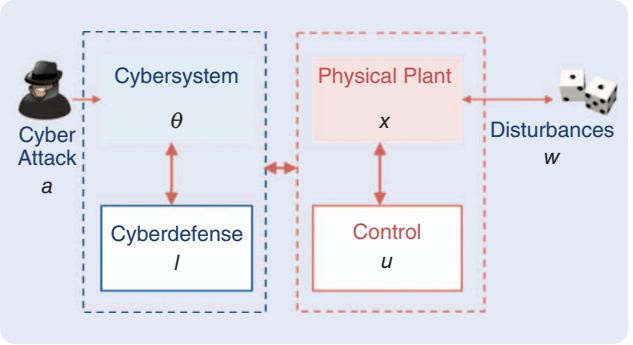


FIGURE 2 The interactions between the cyber and physical systems are captured by their dynamics. The physical system state $x(t)$ is controlled by u with the presence of disturbances and noises. The cyberstate $\theta(t)$ is controlled by the defense mechanism l used by the network administrator as well as the attacker's action a. A cyberattack can compromise the controller and the plant through their coupling with the cybersystem.

The layered architecture can facilitate the understanding of the cross-layer interactions between the physical layers and the cyberlayers. In Figure 2, $x(t)$ and $\theta(t)$ denote the continuous physical state and the discrete cyberstate 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 cyberstate $\theta(t)$ 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 the adoption of a class of hybrid system models, as will be seen later.

PHYSICAL LAYER CONTROL SYSTEM PROBLEM

Resilient control requires a cross-layer control design. The control problem at the physical layer of the system is described below. Consider a general class of systems subject to two types of uncertainty: 1) a continuous deterministic uncertainty that models the known parametric uncertainties and disturbances and 2) 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

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

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

The state of the cybersystem is described by θ. The evolution of θ depends on the cyberdefense action l and the attacker's action a, which are also functions of time. $\theta(t)$ is a shorthand notation in place of $\theta(t, a, l)$ if the pair of actions (a, l) is fixed. For a given pair (a, l), $\theta(t), t \in [0, t_f]$, is 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 $\mathcal{S} := \{1,2,\ldots,s\}$ 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 [3]. An administrator can enforce security by dynamically updating the security policy of the control systems [26], [27]. Once an attack occurs, the administrator can restore the system back to normal operation. Different from conventional computer networks, control systems are reported to experience lower rates of attacks [28], and the software updates are less frequent than the ones in computer networks. Hence, the transition between structural states are at a different time scale from the evolution of physical states. The systems are assumed to have reached their physical steady states when the structural transition happens. This assumption is validated from the fact that the attack rate on control systems is often lower than the one on information systems [29], [30] and the fact that the time scale of the failure rate of devices and components in control systems is higher than the one of the system dynamics and operations [31].

Cyberstrategy

Let $\bar{k} = t/\varepsilon, \varepsilon > 0$, be the time scale on which cyberevents 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 cyberattack chosen by the attacker from his attack space $\mathcal{A} := \{a_1, a_2, \ldots, a_M\}$ composed of all M possible actions. $l \in \mathcal{L}$ is the cyberdefense mechanism that can be employed by the network administrator, where $\mathcal{L} := \{l_1, l_2, \ldots, l_N\}$ is the set of all the possible defense actions. Without loss of generality, $\mathcal{A}$ and $\mathcal{L}$ do not change with time even though, in practice, they can change due to technological updates and advances. The mixed strategies $\mathbf{f}(k) = [f_i(k)]_{i=1}^N \in \mathcal{F}_k, \mathbf{g}(k) = [g_j(k)]_{j=1}^M \in \mathcal{G}_k$ of the defender and the attacker, respectively, are considered here, 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

$$\mathcal{F}_k := \left\{ \mathbf{f}(k) \in [0,1]^N : \sum_{i=1}^N f_i(k) = 1 \right\}, \tag{2}$$

$$\mathcal{G}_k := \left\{ \mathbf{g}(k) \in [0,1]^M : \sum_{j=1}^M g_j(k) = 1 \right\}. \tag{3}$$

The transition law of the cybersystem 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

$$\text{Prob}\{\theta(k+\Delta) = j | \theta(k) = i\} = \begin{cases} \lambda_{ij}(\mathbf{f}(k), \mathbf{g}(k)), & j \neq i, \\ \lambda_{ii}(\mathbf{f}(k), \mathbf{g}(k)), & j = i, \end{cases} \tag{4}$$

where $\Delta > 0$, which is on the same time scale as k (for example, 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

$$\lambda_{ij}(\mathbf{f}(k), \mathbf{g}(k)) = \sum_{i=1}^N \sum_{j=1}^M f_i(k) g_j(k) \tilde{\lambda}_{ij}(a_i(k), l_j(k)). \tag{5}$$

Equations (1) and (4) describe hybrid systems [32]–[34] with both continuous and discrete states. Let $\mathcal{F}_t$ be the sigma-field generated by $\theta_{[t_0,t]} := \{\theta(s), s \leq t\}$. The admissible control and disturbance processes, $u(\cdot)$ and $w(\cdot)$, are taken to be $\mathbb{F}_t$ measurable and piecewise continuous, with the corresponding spaces denoted by $\mathcal{U}$ and $\mathcal{W}$, respectively. f is taken to be 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 cyberattacks or component failure. These events result in random structural changes in the dynamics of the system. For each $u \in \mathcal{U}, w \in \mathcal{W}$, the state process $x(\cdot)$ is continuous with probability one, and if (u,w) is chosen to be memoryless, then the pair (x,θ) is a Markov process.

Closed-Loop, Perfect-State Feedback Control

A closed-loop, perfect-state information structure is considered for control design. The controller has access to $x_{[t_0,t]}$ at time t, which can be written as

$$u(t) = \mu(t, x_{[t_0,t]}; \theta_{[t_0,t]}), \qquad t \in [t_0, t_f], \tag{6}$$

where μ is an admissible closed-loop control strategy, piecewise continuous in its first argument, and Lipschitz continuous in its second argument. The class of all such control strategies is denoted by $\mathcal{M}_{\text{CL}} \subseteq \mathcal{U}$. Analogously, let $\mathcal{N}_{\text{CL}} \subseteq \mathcal{W}$ denote the class of all closed-loop disturbance strategies

$$w(t) = \nu(t, x_{[t_0,t]}; \theta_{[t_0,t]}), \qquad t \in [t_0, t_f]. \tag{7}$$

The performance index for the hybrid control system is given by the expected cost over the statistics of θ

$$J(u,w) := \mathbb{E}_\theta\{L(x,u,w;\theta)\}, \tag{8}$$

with the cost function L given as

$$L(x,u,w;\theta) = q_f(x(t_f); \theta(t_f)) + \int_{t_0}^{t_f} c(t, x(t), u(t), w(t); \theta(t))\,dt + c_0(x_0; \theta(t_0)), \tag{9}$$

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 dropped out,

and $t_f \to \infty$. For each $\mu_{\mathrm{CL}} \in \mathcal{M}_{\mathrm{CL}}$ and $\nu_{\mathrm{CL}} \in \mathcal{N}_{\mathrm{CL}}$, the stochastic differential equation will admit a well-defined solution (as a piecewise deterministic process), which will induce corresponding unique elements in $\mathcal{U}$ and $\mathcal{W}$, which is the "open-loop representations" of μ and ν, respectively.

The H^∞-optimal control problem in the time domain is in fact a minimax optimization problem, and hence a zero-sum game, where the controller can be viewed as the minimizing player and the disturbance as the maximizing player [13], [35]. Here, the objective is to find a minimax closed-loop controller $\mu^*_{\mathrm{CL}} \in \mathcal{M}_{\mathrm{CL}}$ that infimizes the supremum of J over all closed-loop disturbance policies

$$\sup_{\nu \in \mathcal{N}_{\mathrm{CL}}} J(\mu^*_{\mathrm{CL}}, \nu) = \inf_{\mu \in \mathcal{M}_{\mathrm{CL}}} \sup_{\nu \in \mathcal{N}_{\mathrm{CL}}} J(\mu, \nu). \tag{10}$$

A cost structure of interest is the separable one

$$c(t,x,u,w;\theta) = c_0(t,x,u;\theta) - \gamma^2 r(w;\theta). \tag{11}$$

The solution of (10) parameterized in γ is denoted by μ^*_γ, and γ_{CL} denotes the smallest value of $\gamma > 0$ such that for $\gamma > \gamma_{\mathrm{CL}}$ the right-hand side of (10) is bounded. Then μ^*_γ for $\gamma > \gamma_{\mathrm{CL}}$ is an H^∞ controller for the hybrid system, with respect to the performance index

$$\sup_{w \in \mathcal{W}} \left\{ \frac{\mathbb{E}_\theta\{q_f(x_f;\theta(t_f)) + \int_{t_0}^{t_f} c_0(t,x(t),u(t);\theta(t))\,dt\}}{\mathbb{E}_\theta\{\|w\|^2 + q_0(x_0;\theta(t_0))\}} \right\}, \tag{12}$$

where $\|\cdot\|$ denotes the $\mathcal{L}_2$-norm of w for each sample path of θ. The minimum value of (12) is γ^2_{CL}. It defines a measure of disturbance attenuation in the nonlinear hybrid system. Note that in (10), x_0 is considered as part of the disturbance.

What has been formulated above, as described by (10), is a differential game. Let $V(\cdot): \mathbb{R} \times \mathbb{R}^n \times \mathcal{S}$ denote the cost-to-go function associated with this differential game, that is, $V(t,x,i)$ is the upper value of a similar game defined on the shorter interval $[t,t_f]$, with initial state x, and initial structure $\theta(t) = i$. The following assumptions are quite standard.

A1): The differential game defined by (10) 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 **A**1), the infinitesimal generator of the upper-value function is

$$\begin{aligned}\mathcal{L}V(t,x;\theta)|_{\theta=i} &:= \lim_{h\to 0} \frac{1}{h} \mathbb{E}\{V(t+h, x(t+h);\theta(t+h)) \\ &\quad - V(t,x(t),\theta(t))|x(t) = x, \theta(t) = i\} \\ &= V_t(t,x;i) + V_x(t,x;i) f(t,x,u,w;i) + \sum_{j=1}^{s} \lambda_{ij} V_{t,x;j},\end{aligned} \tag{13}$$

with $u \in \mathcal{U}$ and $w \in \mathcal{W}$ chosen to be memoryless, which in fact is not a restriction as further elaborated below. From (13), the associated HJI equation is

$$\begin{aligned}-V^i_t(t,x) = \inf_{u \in \mathbb{R}^r} \sup_{w \in \mathbb{R}^p} \Big\{ & V^i_x(t,x) f(t,x,u,w,i) \\ & + c(t,x,u,w,i) + \sum_{j \in \mathcal{S}} \lambda_{ij} V^j(t,x) \Big\},\end{aligned} \tag{14}$$

$$V^i(t_f,x) = q_f(x(t_f);i), \qquad i \in \mathcal{S}, \tag{15}$$

where the simpler notation $V^i(t,x)$ is used in place of $V(t,x;\theta(t) = i)$. Denoting any such control by $\mu^{\mathrm{F}} \in \mathcal{M}_{\mathrm{CL}}$, (14) and (15) can be rewritten as

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

Furthermore, if the Isaacs condition [on interchangeability of infimum and supremum in (14)] holds and if there exists a disturbance policy, $\nu^{\mathrm{F}} \in \mathcal{N}_{\mathrm{CL}}$, that achieves the maximum in (14), 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 partial differential equation (PDE)

$$\begin{aligned}-V^i_t(t,x) = {} & V^i_x(t,x) f(t,x,\mu^{\mathrm{F}}(t,x,i),\nu^{\mathrm{F}}(t,x,i),i) \\ & + c(t,x,\mu^{\mathrm{F}}(t,x,i),\nu^{\mathrm{F}}(t,x,i),i) + \sum_{j \in \mathcal{S}} \lambda_{ij} V^j(t,x).\end{aligned} \tag{16}$$

For details on the equilibrium concepts of games, see "General Game Model and Equilibrium Concept." The preceding discussion and the ensuing result are now summarized in the theorem below.

Theorem 1

Let the cyberstrategy pair $(\mathbf{f}(k), \mathbf{g}(k))$ be fixed, **A**1) hold, and $\mu^{\mathrm{F}} \in \mathcal{M}_{\mathrm{CL}}$ be defined as above. Then, μ^{F} is a closed-loop minimax controller. If, furthermore, the Isaacs condition holds and $\nu^{\mathrm{F}} \in \mathcal{N}_{\mathrm{CL}}$ is defined above, the pair of Markov policies $(\mu^{\mathrm{F}}, \nu^{\mathrm{F}})$ provides a saddle-point solution on the product space $\mathcal{M}_{\mathrm{CL}} \times \mathcal{N}_{\mathrm{CL}}$. The corresponding saddle-point value function solves (16) subject to (15). □

The optimal cost $V^i(t_0,x_0)$ yields the physical layer control performance under the minimax controller. Note that this cost depends on the cyberstrategy pair $(\mathbf{f},\mathbf{g})$ since the transition rate λ_{ij} is a function of mixed strategies. The cyberstrategies are determined by analyzing a security game at the cyberlayer.

CYBERLAYER DEFENSE SYSTEM

At the cyberlayer, a zero-sum game framework can be used to capture the strategic interactions between an attacker and a defender. The game takes different forms depending on the information available to the defender, the targets of the attacker, and the security mechanism. For example, a zero-sum stochastic game has been used for dynamic configurations of a network of IDSs [36], [37], in which the state

General Game Model and Equilibrium Concept

Consider an N-player game, with $\mathcal{N} := \{1, \ldots, N\}$ denoting the players set. The decision or action variable of Player i is denoted by $x_i \in X_i$, where X_i is the action set of Player i. Let x denote the N-tuple of actions variables of all players, $x := (x_1, \ldots, x_N)$. Allowing for possibly coupled constraints, let $\Omega \subset X$ be the constraint set for the game, where X is the N-product of $X_1, \ldots, X_N$; hence for an N-tuple of action variables to be feasible, $x \in \Omega$. The players are minimizers, with the objective function (loss function or cost function) of Player i denoted by $L_i(x_i, x_{-i})$, where x_{-i} stands for the action variables of all players except the ith one.

Now, an N-tuple of action variables $x^* \in \Omega$ is a *Nash equilibrium* (or *noncooperative equilibrium*) if, for all $i \in \mathcal{N}$, $x_i \in X_i$,

$$L_i(x_i^*, x_{-i}^*) \le L_i(x_i, x_{-i}^*), \text{ such that } (x_i, x_{-i}^*) \in \Omega.$$

If $N = 2$ and $L_1 \equiv -L_2 =: L$, then the game is a two-player zero-sum game, with Player 1 minimizing L and Player 2 maximizing the same quantity. In this case, the Nash equilibrium becomes the *saddle-point equilibrium*, which is formally defined as follows, where the coupling constraint Ω is left out (or simply assumed to be equal to the product set $X := X_1 \times X_2$): A pair of actions $(x_1^*, x_2^*) \in X$ is in *saddle-point equilibrium* for a game with cost function L, if for all $(x_1, x_2) \in X$,

$$L(x_1^*, x_2) \le L(x_1^*, x_2^*) \le L(x_1, x_2^*).$$

This also implies that the order in which minimization and maximization are carried out is inconsequential, that is,

$$\min_{x_1 \in X_1} \max_{x_2 \in X_2} L(x_1, x_2) = \max_{x_2 \in X_2} \min_{x_1 \in X_1} L(x_1, x_2), \tag{S1}$$

$$= L(x_1^*, x_2^*) =: L^*, \tag{S2}$$

where the first expression in (S1) is known as the *upper value* of the game, the second expression in (S1) is the *lower value* of the game, and L^* is known as the value of the game. Upper and lower values are, in fact, defined in more general terms using infimum (inf) and supremum (sup) replacing minimum and maximum, respectively, to account for the facts that minima and maxima may not exist. When the action sets are finite, however, the latter always exists. Note that the value of a game, whenever it exists (which certainly does if there exists a saddle point), is *unique*. Hence, if there exists another saddle-point solution, say $(\hat{x}_1, \hat{x}_2)$, then $L(\hat{x}_1, \hat{x}_2) = L^*$. Moreover, these multiple saddle points are *orderly interchangeable*, that is the pairs $(x_1^*, \hat{x}_2)$ and $(\hat{x}_1, x_2^*)$ are also in saddle-point equilibrium. This property of saddle-point equilibria does not extend to multiple Nash equilibria (for nonzero-sum games). Multiple Nash equilibria are generally not interchangeable, and further they do not lead to the same values for the players' cost functions, the implication being that when players switch from one equilibrium to another, some players may benefit from that (in terms of reduction in cost) while others may see an increase in their costs. Further, if the players pick randomly (for their actions) from the multiple Nash equilibria of the game, then the resulting N-tuple of actions may not be in Nash equilibrium.

of the system evolves according to transition rules determined by the actions taken by the players, and dynamic system configuration policy has been developed for IDSs to optimally defend against intrusions. In [38] and [39], a multistage Stackelberg game has been studied for developing deceptive routing strategies for nodes in a multihop wireless communication network. The framework is convenient to model the scenario where the defender first deploys a proactive defense, and the attacker follows the protocol. A stochastic repeated game and an iterative learning mechanism have been adopted for moving target defense [40], [41]. Due to the lack of complete information of the attacker and the system itself, the players update their strategies in a feedback manner driven by the data they have observed from the system.

In this article, a general stochastic game formulation is introduced in which the state space coincides with $\mathcal{S}$. This class of models captures the uncertainties in cybersystem dynamics and the time evolution of system states and player strategies. Moreover, in the absence of decision making of the players (that is, the costs and the transitions are independent of player strategies), the framework would be reduced to a Markov-chain model which has been used for reliability analysis [42].

At time $k \in \mathbb{R}_+$, the action pair (a, l) is chosen by the attacker and the defender according to a mixed strategy pair $(\mathbf{f}(k), \mathbf{g}(k))$ as introduced in (2) and (3). The joint actions affect the transition rates λ_{ij} in (4) and also incur a cost $c^i(a, l; \mu_{\mathrm{CL}}, \nu_{\mathrm{CL}})$, where c^i is a bounded cost function that incorporates the physical layer control system performance under the closed-loop strategies $\mu_{\mathrm{CL}}, \nu_{\mathrm{CL}}$. The cost c^i has two components: the cost inflicted on the cyberlayer and the resulting impact-aware, physical-layer performance index from the action pair (a, l).

The defense against attacks involves HMIs, which occur at the human and cyberlayers of the system. Hence, defense often evolves on a longer time-scale than the physical layer processes. Using time-scale separation, the optimal defense mechanism can be designed by viewing the physical control system at its steady state at each cyberstate 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 whereas the attacker aiming to minimize it [43]. A discounted payoff criterion $v_\beta(i, \mathbf{f}, \mathbf{g})$ is used and it is defined as

$$v_\beta(i, \mathbf{f}, \mathbf{g}) := \int_0^\infty e^{-\beta k} \mathbb{E}_i^{\mathbf{f}(k), \mathbf{g}(k)} c^i(a, l; \mu_{\mathrm{CL}}, \nu_{\mathrm{CL}})\, dk,$$

where β is the discount factor. The operator $\mathbb{E}_i^{\mathbf{f},\mathbf{g}}$ is the expectation operator. Here a class of mixed stationary strategies $\mathbf{f}^i \in \mathcal{F}^i$ and $\mathbf{g}^i \in \mathcal{G}^i, i \in \mathcal{S}$, is considered that are only dependent on the current cyberstate 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 $\mathcal{F}_S := \Pi_{i\in\mathcal{S}}\mathcal{F}^i$ and $\mathcal{G}_S := \Pi_{i\in\mathcal{S}}\mathcal{G}^i$. The following theorem characterizes the stationary saddle-point equilibrium of the stochastic zero-sum game in a similar fashion as in [43]–[46] .

Theorem 2 [18]

Let the strategy pair $(\mu_{\mathrm{CL}}, \nu_{\mathrm{CL}})$ be fixed. Assume that $\lambda_{ij}(k)$ are continuous in $\mathbf{f}^i$, and $\mathbf{g}^i$ and the cost functions c^i are bounded. Then, 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

$$\begin{aligned}
\beta v_\beta^*(i) &= \tilde{c}^i(\mathbf{F}^*, \mathbf{G}^*) + \sum_{j\in\mathcal{S}} \lambda_{ij}(\mathbf{F}^*, \mathbf{G}^*) v_\beta^*(j) \\
&= \sup_{\mathbf{F}\in\mathcal{F}_S} \left\{ \tilde{c}^i(\mathbf{F}, \mathbf{G}^*) + \sum_{j\in\mathcal{S}} \lambda_{ij}(\mathbf{F}, \mathbf{G}^*) v_\beta^*(j) \right\} \\
&= \inf_{\mathbf{G}\in\mathcal{G}_S} \left\{ \tilde{c}^i(\mathbf{F}^*, \mathbf{G}) + \sum_{j\in\mathcal{S}} \lambda_{ij}(\mathbf{F}^*, \mathbf{G}) v_\beta^*(j) \right\} \\
&= \sup_{\mathbf{F}\in\mathcal{F}_S} \inf_{\mathbf{G}\in\mathcal{G}_S} \left\{ \tilde{c}^i(\mathbf{F}, \mathbf{G}) + \sum_{j\in\mathcal{S}} \lambda_{ij}(\mathbf{F}, \mathbf{G}) v_\beta^*(j) \right\} \\
&=: L_\beta(i) \\
&= \inf_{\mathbf{G}\in\mathcal{G}_S} \sup_{\mathbf{F}\in\mathcal{F}_S} \left\{ \tilde{c}^i(\mathbf{F}, \mathbf{G}) + \sum_{j\in\mathcal{S}} \lambda_{ij}(\mathbf{F}, \mathbf{G}) v_\beta^*(j) \right\} \\
&=: U_\beta(i), \qquad (17)
\end{aligned}$$

where $\tilde{c}^i(\mathbf{F}, \mathbf{G})$ is a shorthand notation for $\mathbb{E}_{\mathbf{F},\mathbf{G}} c^i(a, l; \mu_{\mathrm{CL}}, \nu_{\mathrm{CL}})$, and $L_\beta(i), U_\beta(i)$ are defined to be respectively the lower value and the upper value of the game. In addition, $(\mathbf{F}^*, \mathbf{G}^*)$ from (17) 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 above result is also known as the Shapley optimality criterion for stochastic games. For more details on the properties of saddle points of zero-sum games, see "Minimax Theorem." The saddle-point equilibrium strategies can be computed using a value iteration scheme [44], [45]. Let $\{v_\beta^n(i)\}_{n=1}^\infty$ be a sequence of values of the game which obeys the following update law

$$\begin{aligned}
v_\beta^{n+1}(i) &= \tilde{c}^i(\mathbf{F}_n^*, \mathbf{G}_n^*) + \sum_{j\in\mathcal{S}} \lambda_{ij}(\mathbf{F}_n^*, \mathbf{G}_n^*) v_\beta^n(j) \\
&= \sup_{\mathbf{F}\in\mathcal{F}_S} \left\{ \tilde{c}^i(\mathbf{F}_n, \mathbf{G}_n^*) + \sum_{j\in\mathcal{S}} \lambda_{ij}(\mathbf{F}_n, \mathbf{G}_n^*) v_\beta^n(j) \right\} \\
&= \inf_{\mathbf{G}\in\mathcal{G}_S} \left\{ \tilde{c}^i(\mathbf{F}_n^*, \mathbf{G}_n) + \sum_{j\in\mathcal{S}} \lambda_{ij}(\mathbf{F}_n^*, \mathbf{G}_n) v_\beta^n(j) \right\}. \qquad (18)
\end{aligned}$$

The following theorem provides a convergence result on the iterative algorithm in (18).

Theorem 3

Let $\{\mathbf{F}_n^*, \mathbf{G}_n^*\}$ be the sequence of strategies in $\mathbf{F}_S \times \mathbf{G}_S$ produced by the value iteration scheme described in (18). Then, any limit point $(\mathbf{F}_n, \mathbf{G}_n)$ of the sequence is a pair of saddle-point equilibrium strategies. Moreover, the limit point yields the unique game value $v_\beta^*(i), i \in \mathcal{S}$. □

Note that the equilibrium solution $\{\mathbf{F}^*, \mathbf{G}^*\}$ depends on the physical layer minimax control $(\mu_{\mathrm{CL}}^*, \nu_{\mathrm{CL}}^*)$, while finding the control policy $(\mu_{\mathrm{CL}}^*, \nu_{\mathrm{CL}}^*)$ using (14) and (15) relies on the security policy $\{\mathbf{F}^*, \mathbf{G}^*\}$ taken at the cyberlayer. The optimality criterion (17) in Theorem 2 together with the HJI equation in (14) defines a set of coupled optimality conditions that are used to solve for obtaining the cyberpolicy $\mathbf{F}^*$ and the robust controller μ_{CL}^* and its associated performance index γ^*.

The coupling between the cybersystem game (CSG) and the physical system game (PSG) captures the essential tradeoffs between robustness, resilience, and security. To ensure that the system operates in a normal condition, either a perfect secure system is designed so that no attack can succeed or the system is capable of recovering back to its normal condition quickly once it fails. However, given limited resources, perfect security is not possible, and the solution to the cybergame (for good states) provides a fundamental limit for the best-effort security strategies. Hence, it is essential to allocate resources to the cybersystem to recover from the failure states. This security and resilience tradeoff is captured by the stochastic CSG introduced in this section, which yields strategies balancing the level of security that prevents the cybersystem from failure, and the level of resilience that brings the system quickly back to its normal state of operation.

On the other hand, to achieve a higher level of robustness, the control effort has to be distributed across different cyberstates. Robustness of the control system is high if the system is perfectly secure, that is, the system does not fail and does not move to a compromised state, because control effort only needs to be expended for the good states. However, perfect security does not exist, and the control effort has to be expended on the bad states as well in case the system fails to ensure robustness at the failure states. Hence, there is a tradeoff between security and robustness. The formulation of the PSG captures this tradeoff.

In addition, the coupling between the CSG and PSG yields a design relationship between the level of robustness against w in the physical system and the cost for security defense against $\mathbf{G}$ in the cybersystem. A higher demand of robustness at the physical level will lead to a higher control cost and a higher impact cost for the cybersystem once the system is compromised, which in turn requires a stronger level of security and resilience to prevent or recover from the failure. Given limited resources for defense, physical-level robustness will dictate the tradeoff relationship between security and resilience. Hence, as a result of this framework, a balance of security, resilience, and robustness is achieved for the cyberphysical control system.

LINEAR-QUADRATIC PROBLEM WITH CASCADING FAILURES

Linear Quadratic Problem

The set of optimality equations can be simplified by considering the special case of the linear quadratic problem defined as

Minimax Theorem

Consider two-person, zero-sum finite games, or equivalently matrix games, where Player 1 is the minimizer and Player 2 the maximizer. Let X_1 and X_2 be Player 1's and Player 2's action sets, respectively. Let card $(X_1) = m$ and card $(X_2) = n$ be the cardinality of action sets, that is the minimizer has m choices and the maximizer has n choices. The objective function $L(x_1, x_2)$ is defined on $X_1 \times X_2$. Equivalently, an $m \times n$ matrix A can be associated with this game, whose entries are the values of $L(x_1, x_2)$, following the same ordering as that of the elements of the action sets, that is ijth entry of A is the value of $L(x_1, x_2)$ when x_1 is the ith element of X_1 and x_2 is the jth element of X_2. Player 1's choices are then the rows of the matrix A and Player 2's are its columns.

In general, a saddle point may not exist in pure strategies for all zero-sum games. One example is the game known as *Matching Pennies*. Each player has a penny and can choose heads or tails. The players then reveal their choices simultaneously. If the two choices are identical (that is, if they match), then Player 1 wins and is given the other player's penny. If the choices do not match, then Player 2 wins and is given the other player's penny. This is an example of a zero-sum game, where one player's gain is exactly equal to the other player's loss. The game matrix associated with the game is

$$A = \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}.$$

The entries of this matrix are losses to Player 1 (and thus gain to Player 2). The first row corresponds to the choice of heads for Player 1, and the second row corresponds to the choice of tails for him. Symmetrically, the first column corresponds to heads for Player 1, and the second column is tails for him. Here there is no row-column combination at which the players would not have an incentive to unilaterally deviate and improve their returns.

This opens the door for looking for a *mixed-strategy* equilibrium. A *mixed strategy* for Player i is a probability distribution over his action set X_i, which is denoted by p_i for Player i. If X_i is finite, which is the case here, then p_i will be a probability vector, taking values in the probability simplex determined by X_i, which is denoted by $\mathcal{P}_i$. A pair (p_1^*, p_2^*) constitutes a *saddle point in mixed strategies* (or a *mixed-strategy saddle-point equilibrium*), if for all $(p_1, p_2) \in \mathcal{P}$,

$$J(p_1^*, p_2) \le J(p_1^*, p_2^*) \le J(p_1, p_2^*),$$

where $J(p_1, p_2) = E_{p_1,p_2}[L(x_1, x_2)]$, and $\mathcal{P} := \mathcal{P}_1 \times \mathcal{P}_2$. Here $J^* = J(p_1^*, p_2^*)$ is the value of the zero-sum game in mixed strategies.

In terms of the matrix A, and the probability vectors p_1 and p_2 (both column vectors), which were introduced earlier (note that in this case p_1 is of dimension m and p_2 is of dimension n, and components of each are nonnegative and add up to one), the expected cost function can be rewritten as

$$J(p_1, p_2) = p_1' A p_2.$$

By the *minimax theorem* [52], J admits a saddle point, which means that the matrix game A has a saddle point in mixed strategies, that is there exists a pair (p_1^*, p_2^*) such that for all other probability vectors p_1 and p_2, of dimensions m and n, respectively, the following pair of saddle-point inequalities hold

$$p_1^{*\prime} A p_2 \le p_1^{*\prime} A p_2^* \le p_1' A p_2^*.$$

The quantity $p_1^{*\prime} A p_2^*$ is the *value* of the game in mixed strategies. This result is now captured in the following theorem.

THEOREM S1 (MINIMAX THEOREM)
Every finite two-person, zero-sum game has a saddle point in mixed strategies.

The extension of this result to N-player finite games was first obtained in [49], as captured in the following theorem.

THEOREM S2
Every finite N-player nonzero-sum game has a Nash equilibrium in mixed strategies.

A standard proof for this result uses Brouwer's fixed point theorem; see [35].

$$f(t, x, u, w; i) = A^i x + B^i u + D^i w, \tag{19}$$

$$q_f(t_f; i) = |x(t_f)|^2_{Q^i_f}, \tag{20}$$

$$q_0(x_0, i) = |x_0|^2_{Q^i_0}, \tag{21}$$

$$c_0(t, x, u, i) = |x|^2_{Q^i_f} + |u|^2_{R^i}, \tag{22}$$

$$r(w; \theta) = |w|^2, \tag{23}$$

where $i \in \mathcal{S}$, $|\cdot|$ denotes the Euclidean norm with appropriate weighting, and A^i, B^i, D^i, Q^i, R^i are matrices of appropriate dimensions, whose entries are continuous functions of time t. Further, $Q^i(\cdot) \ge 0, R^i(\cdot) > 0$, and $Q^i_0 > 0$ and $Q^i_f \ge 0$.

Consider the infinite horizon case with the cost function defined by

$$L(x, u, w; \theta) = \mathbb{E} \int_{t_0}^{\infty} (|x(t)|^2_{Q^i} + |u(t)|^2_{R^i} - \gamma^2 |w(t)|^2) dt. \tag{24}$$

Before stating Theorem 4, the following assumptions are made

A2): The Markov chain θ is irreducible for any admissible strategies [47, p. 78].

A3): The pair (A^i, B^i) is stochastically stabilizable [48, see its definition on p. 59].

A4): The pair (A^i, Q^i) is observable for each $i \in \mathcal{S}$.

Theorem 4 [33]

Consider the soft-constrained, zero-sum differential game with perfect measurements in the infinite-horizon case

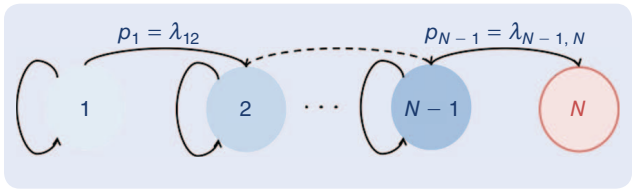


FIGURE 3 A system progresses from a normal operating state $\theta = 1$ to the failure state N. The intermediate states are the ones in which part of the system is exploited and attacked due to the launch of a multistage attack. The transition between the cyberstates follows a Markov process with rate $\lambda_{i,i+1} = p_i, 1 \le i \le N-1$, and $\lambda_{ii} = 1 - p_i, 1 \le i \le N-1, \lambda_{NN} = p_N$.

defined by (10), (19)–(23), (24), (6), and (7), with λ_{ij}s fixed. Let assumptions A2)–A4) hold. Then, $\gamma^*_{\mathrm{CL},\infty} < +\infty$, and for any $\gamma_{\mathrm{CL}} > \gamma^*_{\mathrm{CL},\infty}$, there exists a set of minimal positive definite solutions $Z_i, i \in \mathcal{S}$, to generalized algebraic Riccati equations (GAREs),

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

which further satisfy the condition

$$\gamma^2_{\mathrm{CL}}Q^i_0 - Z_i \ge 0,\ \ i \in \mathcal{S}, \tag{25}$$

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

$$u^*_{\gamma\infty}(t) = \mu^*_{\gamma\infty}(t, x(t), \theta(t)) = -(R^i)^{-1}B^{i\top}Z_ix(t). \tag{26}$$

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

$$\dot{x}(t) = \left(A^i - (B^i(R^i)^{-1}B^{i\top} - \frac{1}{\gamma^2}D^iD^{i\top})Z_i\right)x(t), \tag{27}$$

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

For $\gamma < \gamma^*_{\mathrm{CL},\infty}$, on the other hand, either condition (25) 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 2. Let $\tilde{g}^i = V^i$ be the cost function which describes the physical layer system performance. Then, the fixed-point equation (17) can be written as

$$\beta v^*_\beta(i) = x_0'Z_i(\mathbf{F}^*,\mathbf{G}^*)x_0 + \sum_{j\in\mathcal{S}}\lambda_{ij}(\mathbf{F}^*,\mathbf{G}^*)v^*_\beta(j). \tag{28}$$

The optimal control u^* and the optimal defense strategy $\mathbf{F}^*$ need to be found by solving the coupled equations (28) and GAREs in Theorem 4.

Cascading Failures

Cascading failure is kind of failure in a system comprised of interconnected parts in which the failure of a part can trigger the failure of successive parts. Such a failure is common in computer networks and power systems. In the case of cascading failures, state $\theta = 1$ is the normal operating state and state $\theta = N$ is the terminal failure state. The states $i, 2 \le i \le N-1$, are intermediate compromised states in which one system component failure leads to another. The failure and compromised states are taken to be irreversible, that is, the system cannot be fixed or brought back to its normal state immediately after faults occur. This is usually due to the fact that the time scale for critical cascading failures is much shorter than the time scale for system maintenance. In our modeling framework, the transition between the failure states follows a Markov jump process with rate matrix $\lambda = \{\lambda_{ij}\}_{i,j\in\mathcal{S}}$ such that for $i \ne j$, $\lambda_{ij} \ge 0$, $\lambda_{ii} = 1 - \sum_{j\ne i}\lambda_{ij}$, and $i > j$ and $j > i+1$, $\lambda_{ij} = 0$. For simplicity, the notation $\lambda_{i,i+1} = p_i, 1 \le i \le N-1$, denotes the transition rates between adjacent states, and hence $\lambda_{ii} = 1 - p_i, 1 \le i \le N-1$, $p_N = \lambda_{NN}$. Here, $p_i, i = 1, \cdots, N-1$, are dependent on the cyberstrategy pair $(\mathbf{F},\mathbf{G})$, which has been introduced earlier. An effective cyberdefense action will lead to lower transition rates, and a power cyberattack will increase them. The structure of state transition of cascading failures is depicted in Figure 3.

Following (28), the optimality criteria for the cybersystem under cascading cyberstates can be further simplified to

$$\beta v^*_\beta(N) = V^N, \tag{29}$$

$$\beta v^*_\beta(i) = \mathrm{val}\{c^i + p_iv^*_\beta(i+1) - p_iv^*_\beta(i)\}, \tag{30}$$

$$(\mathbf{f}_i,\mathbf{g}_i) \in \arg\ \mathrm{val}\{c^i + p_iv^*_\beta(i+1) - p_iv^*_\beta(i)\},\ \ i = 1,\cdots,N-1, \qquad c^i = x_0^\top Z_ix_0. \tag{31}$$

Here, $p_i = \lambda_{i,i+1}, 1 \le i \le N-1$, and V^i is dependent on p_i through Z_i in Theorem 4. Note that (30) and (31) find the game value v^i_β and stationary saddle-point equilibrium strategies $(\mathbf{F},\mathbf{G})$, respectively. Since both players have a finite number of choices for each k, the existence of a saddle-point solution is guaranteed for the zero-sum stochastic game [35], [49].

In addition, the optimality criteria for the H^∞ optimal control in the linear quadratic case can be reduced to

$$A^{N\top}Z_N + Z_NA^N - Z_N\left(B^N(R^N)^{-1}B^{N\top} - \frac{1}{\gamma^2}D^ND^{N\top}\right)Z_N + Q^N = 0, \tag{32}$$

$$A^{i\top}Z_i + Z_iA^i - Z_i\left(B^i(R^i)^{-1}B^{i\top} - \frac{1}{\gamma^2}D^iD^{i\top}\right)Z_i + Q^i + p_iZ_{i+1} = 0,\ \ i = 1,\ldots,N-1. \tag{33}$$

Here, γ is a chosen level of attenuation. Under the regularity conditions in [13], there exists a finite scalar $\gamma^\infty > 0$ such

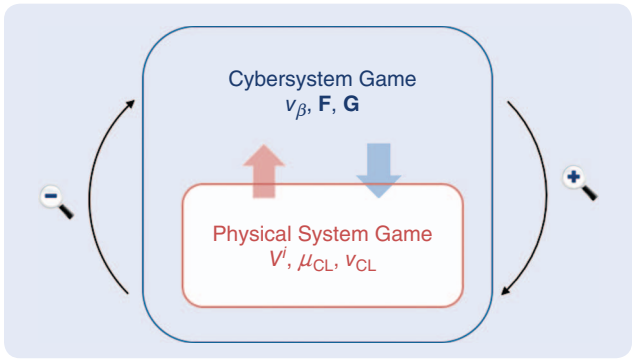


FIGURE 4 A games-in-games structure for cross-layer resilient control design. At the physical layer control system, a zero-sum differential game between the robust controller and the disturbance is used to design an H^∞ controller for achieving robust performance for uncertain parameters or disturbances. At the cyberlayer defense system, a zero-sum stochastic game between a defender and an attacker is used to design an optimal cyberpolicy for ensuring system security. The cross-layer solution $(\mu_{CL}, \nu_{CL}, \mathbf{F}, \mathbf{G})$ has to satisfy a Hamilton–Jacobi–Isaacs equation and a Shapley optimality criterion. V^i is the value function for the physical system at cybermode i, and $v_\beta(i)$ is the value function for the cybersystem. The solution process is composed of a zooming-in process and a zooming-out process. The zooming-in operation goes from the cyberlayer decision process to the physical layer one, while the zooming-out operation refers to the reverse.

that for all $\gamma > \gamma^\infty$, (32) and (33) admit unique minimal nonnegative definite solutions.

In (30), p_is are dependent on $\mathbf{F}$ and $\mathbf{G}$. At the same time, as a result of solving (33), the value V^i is dependent on p_is and B_is, which are in turn functions of $\mathbf{F}$ and $\mathbf{G}$. The above set of coupled equations can be solved by starting with (32) for obtaining the value of the terminal state V^N. From (29), the value v_N^* is calculated and then in the next step use (30) and (33) to find the stationary saddle-point equilibrium strategies $\mathbf{f}_{N-1}^*, \mathbf{g}_{N-1}^*$ at state $\theta = N-1$, their corresponding transition rate $p_{N-1}^* = \lambda_{N-1,N}(\mathbf{f}_{N-1}^*, \mathbf{g}_{N-1}^*)$ and the Riccati solution Z_{N-1}. The process is iterated again by using Z_{N-1} in (30) for $i = N-2$, and the obtained strategy pair $(\mathbf{f}_{N-2}^*, \mathbf{g}_{N-2}^*)$ is used in (33) to solve Z_{N-2}. Hence backward induction is used to obtain Z_1 and $(\mathbf{f}_1^*, \mathbf{g}_1^*)$.

Note that the coupling between (32), (33) and (29), (30) demonstrates the interdependence between security at the cyberlevel and the robustness at the physical level. The holistic viewpoint toward these system properties is essential in addressing the resilience of cyberphysical control systems. The coupling between cyber and physical levels of the system is not one directional but rather reciprocal. The upward resilience from the physical level to the cyberlevel results from the function c^i while the downward resilience from the cyberlevel to the physical level follows from the dependence of λ_{ij} on the cyberpolicies.

GAMES-IN-GAMES STRUCTURE

The cross-layer, game-theoretic model captures the coupling between the cyber and the physical layers of the system dynamics. In the framework, robustness of the cyberphysical control system is studied under an H^∞ optimal control model, while its security is studied using a two-person zero-sum cybersecurity game. The control and defense strategy designs are extended to incorporate post-event system states, where resilient control and cyberstrategies are developed to deal with uncertainties and events that are not taken into account in pre-event robustness and security designs. Under the assumptions made in Theorems 1 and 2, a secure, resilient, and robust control and cyberstrategy pair $(\mu_{CL}, \mathbf{F})$ has to satisfy the general optimality criteria (14), (15), and (17). In the linear quadratic problem with cascading states, they are reduced to (32), (33), (29), and (30). They are derived from the optimality criteria of two dynamic games. One is the zero-sum differential game for the H^∞ robust control design, and the other one is the zero-sum stochastic game for equilibrium defense policy. Due to the layering architecture and the time-scale separation, the CSG can been seen as the one on top of the PSG. The two games are coupled and exhibit a *games-in-games* structure as illustrated in Figure 4. The outcome of the PSG affects the cost structure of the CDG. In addition, the solution to the PSG depends on the equilibrium solution $(\mathbf{F}^*, \mathbf{G}^*)$ from the CSG. Solutions to this game structure define the tradeoff between robust and resilient control of cyberphysical control systems.

One interesting aspect of the games-in-games structure is that its solution is featured by *zooming-in* and *zooming-out* operations. The zooming-out operation refers to the fact that the solution of the PSG provides an input to the CSG, which leads to a solution of the CSG. The zooming-in operation refers to the reverse fact, that is, the PSG also affects the CSG. As depicted in Figure 4, solutions to the coupled optimality criteria precisely involve these two procedures. *zooming in* is defined as the operation of passing the parameters from higher level CSG to lower level PSG, and *zooming out* as the operation of passing the parameters from the lower-level PSG to the higher level CSG. A sequence of structured zooming-in and zooming-out operations is observed in the linear-quadratic problem with cascading states. The procedure for finding the solution starts with finding Z_{N-1} using (33) and then zooming out to the CSG to find $(v_\beta^*(N-1), \mathbf{f}_i, \mathbf{g}_i)$. This is followed by zooming in to the PSG again and find Z_{N-2}. The zooming-in and zooming-out operations alternate until reaching the initial state $\theta = 1$.

A Numerical Example

Consider the following two-state linear system that arises from a single-machine infinite bus power system linearized around its operation point [18]. Let $x \in \mathbb{R}^3$ be the state vector that includes the power angle, the relative speed, and the active power delivered by the generator. Let $u \in \mathbb{R}^3$ be the control variable that determines the amplifier of the generator. At the normal operating state $\theta = 1$, its dynamics are described by

$$\dot{x} = A^1 x + B^1 u + D^1 w, \tag{34}$$

where

$$A^1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & -0.625 & -39.2699 \\ -0.156627 & 1.65884 & -0.738602 \end{bmatrix},$$
$$B^1 = \begin{bmatrix} 0 \\ 0 \\ -0.271287 \end{bmatrix}, \; D^1 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

With an unanticipated fault caused by a cyberattack at the rate λ_{12}, the system is compromised and its dynamics at the failed state $\theta = 2$ are given by

$$\dot{x} = A^2 x + B^2 u + D^2 w, \tag{35}$$

where

$$A^2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & -0.625 & -39.2699 \\ -0.0691878 & 0.960155 & -0.407174 \end{bmatrix},$$
$$B^2 = \begin{bmatrix} 0 \\ 0 \\ -0.119837 \end{bmatrix}, \; D^2 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

The design strategy based on the linear quadratic criterion described above could be used here, by choosing the weighting matrices

$$Q^1 = Q^2 = \begin{bmatrix} 1000 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 10 \end{bmatrix}, \; R^1 = 10, \; R^2 = 1,$$

where the weights of 1000 are used in Q_1 and Q_2 to emphasize the willingness to use more control in a post-attack state.

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

	A	NA
D	0.1	0.05
ND	0.95	0.05

.

In the above table, a higher transition rate has been attached to a failure state if the attacker launches an attack while the cybersystem does not have proper measures to defend itself. On the other hand, the probability is lower if the cybersystem can defend itself from attacks. In the above table, a base transition rate of 0.05 has been assumed to capture the inherent reliability of the physical system without exogenous attacks. The optimality criterion (28) and GAREs in Theorem 4 are used to obtain the discounted value functions $v^*_\beta(i), i = 1,2$, with the discount factor chosen to be $\beta = 1$, and yield $V^2 = 7.2075 \times 10^4$ independent of the parameter p. Hence, $v^*_\beta(2) = V^2$ and v^*_β satisfies the following fixed-point equation:

$$v^*_\beta(1) = \text{val}\{\mathbf{H} - v^*_\beta(1)\mathbf{G}\}, \tag{36}$$

where

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

and

$$\mathbf{G} = \begin{bmatrix} 0.1 & 0.05 \\ 0.95 & 0.05 \end{bmatrix},$$

where val is the value operator for a matrix game [44], [45]. Using value iteration, it is possible to compute $v^*_\beta(1) = 1.3087 \times 10^4$, 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 informs that the defender should always be defending and the attacker should not be attacking. At $p = 0.05$, the physical layer robust feedback control at each state i is obtained by

$$u^{\text{F}}(t,x,1) = -(R^1)^{-1} B^{1\top} Z^1, \quad u^{\text{F}}(t,x,2) = -(R^2)^{-1} B^{2\top} Z^2,$$

where

$$Z^1 = \begin{bmatrix} 399.3266 & 31.8581 & -162.2334 \\ 31.8581 & 5.7083 & -15.2963 \\ -162.2334 & -15.2963 & 149.7459 \end{bmatrix},$$

and

$$Z^2 = \begin{bmatrix} 2.8512 & 0.1066 & -2.8575 \\ 0.1066 & 0.0345 & -0.1041 \\ -2.8575 & -0.1041 & 4.1506 \end{bmatrix},$$

and the optimum performance index is $\gamma^*_\infty = 8.5$.

CASE STUDY: DEFENSE AGAINST DENIAL-OF-SERVICE ATTACK

The games-in-games principle for the special case of the linear-quadratic problem with cascading failures has been applied to study the resilience of the power energy system in [18]. The principle can be further extended to discrete-time systems where the physical layer game is a discrete-time minimax design problem with perfect state measurements and the cyberlayer game is a discrete-time stochastic Markov game. In parallel to the results developed for continuous-time systems, a similar set of coupled equations for discrete-time systems can be developed. Interested readers can refer to [13] and [21] for results on the

discrete-time minimax design problem with perfect and imperfect state measurements. To further illustrate this, a case study of denial-of-service (DoS) attack is discussed below, which can cause delays and congestion in the communication channel of the cyberphysical systems.

Control System Model

A networked control system is vulnerable to different types of cyberattacks, including false data injection, DoS, and sensor node capture and cloning attack, as depicted in Figure 5. Here, the games-in-games principle is used to study a class of DoS attacks on control systems. The controlled plant under DoS attacks is described by a discrete-time model for computational convenience

$$\begin{cases} x_{k+1} = Ax_k + B_2 u_{c,k} + B_1 \omega_k, \\ z_k = Dx_k, \end{cases} \tag{37}$$

where $x_k \in \mathbb{R}^n$ and $u_{c,k} \in \mathbb{R}^m$ are, respectively, the state variable and the control signal received by the actuator, ω_k is the disturbance belonging to $l_2[0,\infty)$. A, B_1, B_2, and D are matrices with appropriate dimensions. The measurement with randomly varying communication delays is described by

$$\begin{cases} y_k = Cx_k, \\ y_{c,k} = (1-\delta^\theta) y_k + \delta^\theta y_{k-1}, \end{cases} \tag{38}$$

where $y_{c,k} \in \mathbb{R}^p$ is the measured output and $y_k \in \mathbb{R}^p$ is the actual output. $\theta \in \mathcal{S} := \{\theta_1, \theta_2, \ldots, \theta_s\}$ is the state space of the cybersystem. The stochastic variable δ^θ is distributed according to a Bernouli distribution:

$$\begin{aligned} &\bar{\delta}^\theta := \Pr\{\delta^\theta = 1\} = \mathbb{E}\{\delta^\theta\}, \\ &\Pr\{\delta^\theta = 0\} = 1 - \mathbb{E}\{\delta^\theta\} = 1 - \bar{\delta}^\theta. \end{aligned} \tag{39}$$

When $\delta^\theta = 1$, the measured output is $y_{c,k} = y_{k-1}$, that is, the measured output has a one-step time delay. When $\delta^\theta = 0$, the measured output is $y_{c,k} = y_k$, that is, there is no delay between the measured output and the actual system output. An observer-based control strategy takes the form of

$$\begin{cases} \hat{x}_{k+1} = A\hat{x}_k + B_2 u_{c,k} + L^\theta (y_{c,k} - \bar{y}_{c,k}), \\ \bar{y}_{c,k} = (1-\delta^\theta) C\hat{x}_k + \delta^\theta C\hat{x}_{k-1}, \end{cases} \tag{40}$$

$$\begin{cases} u_k = K^\theta \hat{x}_k, \\ u_{c,k} = (1-\beta^\theta) u_k + \beta^\theta u_{k-1}, \end{cases} \tag{41}$$

where $u_k \in \mathbb{R}^m$ is the control signal generated by the controller and $u_{c,k}$ is the signal received by the actuator. $K^\theta \in \mathbb{R}^{m\times n}$ and $L^\theta \in \mathbb{R}^{n\times p}$ denote the controller gains and observer gains that are to be designed. The stochastic variable β^θ, mutually independent of δ^θ, is also a Bernoulli distributed white sequence with expected value $\bar{\beta}^\theta$. Note that the sensor-to-controller (S-C) delay is described by the situation that $\delta^\theta = 1$, and the controller-to-actuator (C-A) delay is described by $\beta^\theta = 1$.

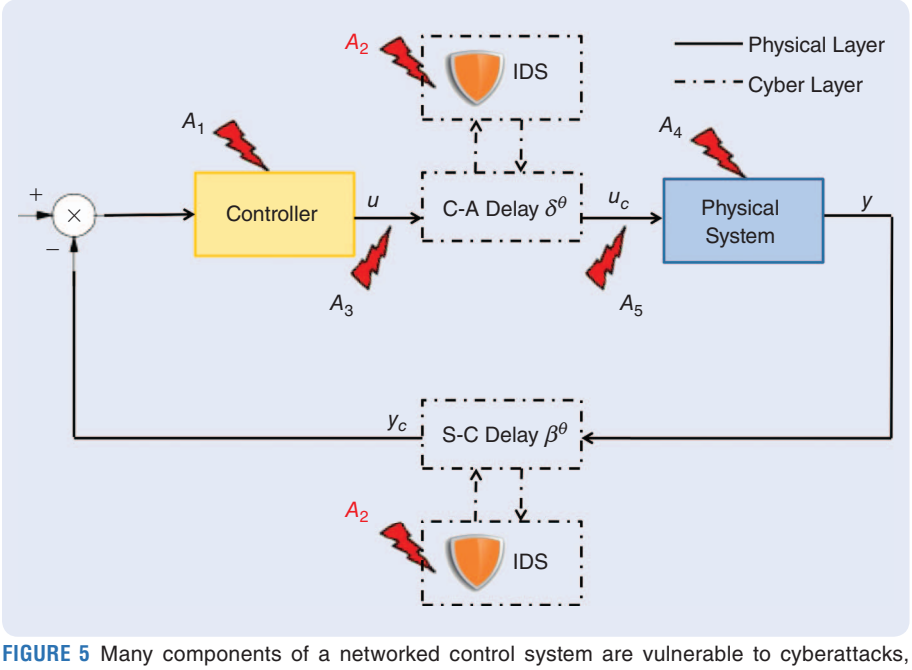


FIGURE 5 Many components of a networked control system are vulnerable to cyberattacks, including the controller, the physical plant, and the communication networks [51]. In the diagram, dotted blocks constitute the cyberlayer of the system while blocks with solid lines are components at the physical layer. A_1 and A_4 represent direct attacks against the actuators or the plant. A_2 is the denial of service attack, where the controller is prevented from receiving sensor measurements and the actuator from receiving control signals. A_3 and A_5 represent deception attacks, where the false information $\tilde{y} \neq y$ and $\tilde{u} \neq u$ is sent from sensors and controllers. Intrusion detection systems (IDSs) are detection devices used to defend the control system from intruders but may cause C-A delay between controller (C) and actuator (A) and/or S-C delay between sensor (S) and controller (C). The probabilities of incurring a one time-step delay are denoted by parameters δ^θ and β^θ, which depend on the cyberstate θ. An IDS is configured optimally as a tradeoff between physical layer control system performance and cyber-level security enhancement.

Intrusion Detection Systems

IDSs are deployed in communication networks for detecting unauthorized system access. They are passive devices that receive and evaluate information sent over a network against a set of signatures. IDS signatures have been developed for most published vulnerabilities and for potentially dangerous activity in common IT protocols. The C-A and S-C delays depend on the configurations of the IDSs. A configuration providing high information assurance can result in significant delays for control system applications since a large number of signatures have to be checked for each incoming

Uncertainties from the cybersystem are often unanticipated and more catastrophic for control systems in terms of their high impact and low effort as compared to those from the physical world.

packet. The configuration of IDSs is not a trivial task. The current version of the Snort IDS, for example, has approximately 10,000 signature rules located in 50 categories. Each IDS also comes with a default configuration to use when no additional information or expertise is available. It is not trivial to determine the optimal configuration of an IDS because of the need to understand the quantitative relationships between a wide range of analyzers and tuning parameters.

For industrial control systems, a set of SCADA IDS signatures that parallel Snort rules for enterprise IT systems have been designed by Digital Bond's Quickdraw, which leverages the existing IDS equipment by developing signatures for control system protocols, devices, and vulnerabilities [50]. In Figure 6, a typical SCADA IDS rule is illustrated, which is used to detect a buffer overflow attack. The rule is specifically designed for Siemens Tecnomatix FactoryLink software, which is used for monitoring, supervising, and controlling industrial processes. FactoryLink is commonly used to build applications such as HMI systems and SCADA systems. The logging function of FactoryLink is vulnerable to a buffer overflow caused by the usage of `vsprintf` with a stack buffer of 1024 B. The vulnerability can be exploited remotely in various ways like the passing of a big path or filter string in the file related operations [50].

```
alert tcp any any -> any 7580 (msg:"ETPRO SCADA
Siemens Tecnomatix FactoryLink CSService GetFile
path Buffer Overflow"; flow:to_server, established;
content:"LEN|00|"; depth:4; byte_test:4,>,
1028,0,little; content:"|99|"; distance:8; within:1;
content:"|99 00 00 00 08 00 00 00 02 06|"; distance:
0; byte_test:4,>,1024,0,big; classtype:attempted-
user;reference:url,digitalbond.com/tools/quickdraw/
vulnerability-rules; sid:1111675; rev:1;)
```

FIGURE 6 A supervisory control and data acquisition (SCADA) intrusion detection system rule to detect CSService CSMSG GetFile buffer overflow in a Siemens Tecnomatix FactoryLink: Siemens Tecnomatix FactoryLink software is used for monitoring, supervising, and controlling industrial processes. FactoryLink can be used to build applications such as human–machine interface systems and SCADA systems. The logging function of the software is vulnerable to a buffer overflow caused by `vsprintf` with a stack buffer of 1024 B. An attacker can exploit the vulnerability remotely to cause application crash and obtain illegitimate access to arbitrary memory.

The goal of the network administrator is to configure an optimal set of detection rules to protect the cybersystem from attackers. To model the interaction between an attacker and a defender, a dynamic game approach is used. Let $\mathcal{L}^*$ be a finite set of possible system configurations in the network and $\mathcal{A}$ be the finite action set of the attacker. The mixed strategies $\mathbf{f}(k)$ and $\mathbf{g}(k)$ are defined on the action spaces $\mathcal{L}^*$ and $\mathcal{A}$, respectively.

The distributions of random variables δ^θ and β^θ are dependent on the states and attack and defense mechanism in the cyberlayer. Let $\mathbf{H} \in \mathbb{R}^{N\times M}$ and $\mathbf{W} \in \mathbb{R}^{N\times M}$ be two state-dependent matrices whose entries H_{ij} and W_{ij} reflect the S-C and C-A delays for different attack and defense action pairs (F_i, a_j). The parameters of the Bernoulli random variables are determined by mixed strategies $\mathbf{f}_\theta, \mathbf{g}_\theta$ as

$$\bar{\delta}^\theta := \mathbf{f}_\theta^T \mathbf{H}(\theta)\mathbf{g}_\theta, \qquad \bar{\beta}^\theta := \mathbf{f}_\theta^T \mathbf{W}(\theta)\mathbf{g}_\theta.$$

The cybersystem transitions between different states and its transition probabilities

$$\mathbb{P}(\theta'(n+1)|\theta(n), a_j, F_i),\ \theta'(n+1), \qquad \theta(n) \in \Theta,$$

are dependent on the defense and attack action pair (F_j, a_j) at time n, and

$$\sum_{\theta' \in \Theta} \mathbb{P}(\theta'|\theta(n), F_i, a_j) = 1.$$

Cross-Layer Control Design

The H^∞ index is the expectation over $\mathbf{f}_\theta$ and $\mathbf{g}_\theta$ for a given θ. Without loss of generality, let $x_0 = 0$; then

$$\mathbb{E}^{\mathbf{f}(\theta),\mathbf{g}(\theta)}\left\{\sum_{k=0}^{\infty} \{\| z_k \|^2\}\right\} < \gamma_\theta^2 \sum_{k=0}^{\infty} \{\| \omega_k \|^2\}, \tag{42}$$

for all $\theta \in \Theta$. The goal of the physical layer control design is to find optimal $K^\theta, L^\theta, \theta \in \mathcal{S}$. The theorem below indicates how to convert the conditions satisfying the H^∞ index into linear matrix inequalities (LMIs) that are easy to solve numerically using available tools.

Theorem 5 [21]

Given scalars $\gamma_\theta > 0$ and a strategy pair $(\mathbf{f}_\theta, \mathbf{g}_\theta)$ for all $\theta \in \Theta$, the hybrid model described by (37)–(41) is exponentially mean-square stable and the H^∞-norm constraint (10) is achieved for all nonzero ω_k if there exist positive definite matrices $P_{11}^\theta \in \mathbb{R}^{m\times m}$, $P_{22}^\theta \in \mathbb{R}^{(n-m)\times(n-m)}$, $S_1^\theta \in \mathbb{R}^{n\times n}$ and $P_2^\theta \in$

ALGORITHM 1 An algorithm for coupled design.

Given: $\mathbf{H}(\theta)$ and $\mathbf{W}(\theta)$ for all $\theta \in \Theta, F_i \in \mathcal{L}^*, a_j \in \mathcal{A}$,
Output: K^θ and L^θ for all $\theta \in \Theta$; $\mathbf{F}_s^*$ and $\mathbf{G}_s^*$.

1) **Initialization:**
2) Initialize $\mathbf{v}_\beta^0$ and $\beta = 0.5$.
3) **Iterative update:**
4) **while** $(\|\mathbf{v}_\beta^{h+1} - \mathbf{v}_\beta^h\| > \varepsilon)$ **do**
5) Solve the convex optimization problem (46) and obtain $\mathbf{C}(\theta)$.
6) Calculate the cost matrix $\mathbf{R}(\theta) := [R_{ij}(\theta)]$ using

$$R_{ij}(\theta) = C_{ij}(\theta) + \beta \sum_{\theta' \in \Theta} \mathbb{P}(\theta' \mid \theta, F_i, a_j) v^h(\theta'). \tag{47}$$

7) Find the value $v_\beta^{h+1}(\theta)$ of the matrix game $\mathbf{R}(\theta)$ using the following linear program

$$\text{(LPMG)} \quad v_\beta^{h+1}(\theta) = \max_{\tilde{y}} \tilde{y}' \mathbf{1}_m$$
$$\text{s.t} \quad R^T(\theta)\tilde{y} \le \mathbf{1}_n$$
$$\tilde{y} \ge 0.$$

8) **end while**
9) Obtain $\mathbf{F}_s^*$ using $\mathbf{f}_\theta^* = \tilde{y} v_\beta(\theta)$ and solve the dual problem of (LPMG) to get $\mathbf{G}_s^*$ and $\mathbf{g}_\theta^*$
10) Use Theorem 2 to obtain the controller gain and the observer gain for all $\theta \in \Theta$ with

$$K^\theta = V\Sigma^{-1} P_{11}^{\theta\,-1} \Sigma V^T M^\theta, \quad L^\theta = S_1^{\theta\,-1} N^\theta.$$

$\mathbb{R}^{n\times n}$ and $S_2^\theta \in \mathbb{R}^{n\times n}$, and real matrices $M^\theta \in \mathbb{R}^{m\times n}, N^\theta \in \mathbb{R}^{n\times p}$ such that

$$P_1^\theta := U_1^T P_{11}^\theta U_1 + U_2^T P_{22}^\theta U_2,$$

where $U_1 \in \mathbb{R}^{m\times n}$ and $U_2 \in \mathbb{R}^{(n-m)\times n}$ satisfy

$$\begin{bmatrix} U_1 \\ U_2 \end{bmatrix} B_2 V = \begin{bmatrix} \Sigma \\ 0 \end{bmatrix}, \quad \Sigma = \operatorname{diag}\{\sigma_1, \sigma_2, \ldots, \sigma_m\},$$

and $\sigma_i, i = 1,2,\ldots,m$, are eigenvalues of B_2. In addition, the controller gain and observer gain satisfy the following LMIs:

$$K^\theta = V\Sigma^{-1} P_{11}^{\theta\,-1} \Sigma V^T M^\theta, \quad L^\theta = S_1^{\theta\,-1} N^\theta, \tag{43}$$

$$\Pi^\theta = \begin{bmatrix} \Pi_{11}^\theta & * \\ \Pi_{21}^\theta & \Pi_{22}^\theta \end{bmatrix} < 0, \tag{44}$$

where

$$\Pi_{11}^\theta = \begin{bmatrix} P_2^\theta - P_1^\theta & * & * & * & * \\ 0 & S_2^\theta - S_1^\theta & * & * & * \\ 0 & 0 & -P_2^\theta & * & * \\ 0 & 0 & 0 & -S_2^\theta & * \\ 0 & 0 & 0 & 0 & -\gamma_\theta^2 I \end{bmatrix},$$

$$\Pi_{22}^\theta = \begin{bmatrix} -P_1^\theta & * & * & * & * \\ 0 & -S_1^\theta & * & * & * \\ 0 & 0 & -P_1^\theta & * & * \\ 0 & 0 & 0 & -S_1^\theta & * \\ 0 & 0 & 0 & 0 & -I \end{bmatrix}, \tag{45}$$

$$\Pi_{21}^\theta = \begin{bmatrix} \Pi_{21}^\theta(1,1) & \Pi_{21}^\theta(1,2) \\ \Pi_{21}^\theta(2,1) & \Pi_{21}^\theta(2,2) \end{bmatrix},$$

$$\Pi_{21}^\theta(1,1) = \begin{bmatrix} P_1^\theta A + (1-\bar{\beta}^\theta) B_2 M^\theta & -(1-\bar{\beta}^\theta) B_2 M^\theta \\ 0 & S_1^\theta A - (1-\bar{\delta}^\theta) N^\theta \mathbf{C}(\theta) \end{bmatrix},$$

$$\Pi_{21}^\theta(1,2) = \begin{bmatrix} \bar{\beta}^\theta B_2 M^\theta & -\bar{\beta}^\theta B_2 M^\theta & P_1^\theta B_1 \\ 0 & -\bar{\delta}^\theta N^\theta C(\theta) & S_1^\theta B_1 \end{bmatrix},$$

$$\Pi_{21}^\theta(2,1) = \begin{bmatrix} \alpha_1^\theta B_2 M^\theta & -\alpha_1^\theta B_2 M^\theta \\ \alpha_2^\theta N^\theta \mathbf{C}(\theta) & 0 \\ D & 0 \end{bmatrix},$$

$$\Pi_{21}^\theta(2,2) = \begin{bmatrix} -\alpha_1^\theta B_2 M^\theta & \alpha_1^\theta B_2 M^\theta & 0 \\ -\alpha_2^\theta N^\theta \mathbf{C}(\theta) & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

$$\alpha_1^\theta = [(1-\bar{\beta}^\theta)\bar{\beta}^\theta]^{1/2},$$
$$\alpha_2^\theta = [(1-\bar{\delta}^\theta)\bar{\delta}^\theta]^{1/2}.$$

Note that (43) and (44) in Theorem 5 lead to a convex optimization problem

$$\hat{\gamma}_\theta := \min_{\substack{P_{11}^\theta > 0,\, P_{22}^\theta > 0,\, P_2^\theta > 0 \\ S_1^\theta > 0,\, S_2^\theta > 0,\, M^\theta,\, N^\theta}} \gamma_\theta \tag{46}$$
$$\text{subject to} \quad (42).$$

Since γ_θ is influenced by the cyberstate and strategy, it is actually dependent on the triple $(\theta, \mathbf{f}(\theta), \mathbf{g}(\theta))$. Let $\mathbf{C}(\theta) \in \mathbb{R}^{N\times M}$ be the performance matrix with its entry $C_{ij}(\theta)$ corresponding to the physical layer H^∞ performance index under the action pair (F_i, a_j). $\hat{\gamma}_\theta$ can be seen as the value of the mapping:

$$\hat{\gamma}_\theta = \mathbf{f}_\theta^T \mathbf{C}(\theta)\, \mathbf{g}_\theta.$$

The coupled design here means that the cyberdefense mechanism takes into account the H^∞ index, and the H^∞ optimal controller is designed with $\bar{\delta}^\theta = \mathbf{f}^*{}_\theta^T \mathbf{H}(\theta) \mathbf{g}_\theta^*$ and $\bar{\beta}^\theta = \mathbf{f}^*{}_\theta^T \mathbf{W}(\theta) \mathbf{g}_\theta^*$. Algorithm 1 is proposed for the coupled design. The algorithm involves a value iteration for computing the stationary mixed saddle-point equilibrium for the stochastic game, in which a linear program for matrix games (LPMG) is solved at each step. For computation of the saddle-point equilibrium using linear programming, see "Linear Programming for Computing the Saddle-Point Equilibrium." Since the game here is zero-sum and finite, the value iteration method converges to stationary saddle-point equilibrium strategies. Readers interested in a proof of convergence of value iteration in zero-sum finite games can refer to [44] and [45]. The algorithm also invokes the computational tools for solving a set of LMIs for obtaining the H^∞ robust controller in the form of (40) and (41) that achieves optimal control system performance.

A Numerical Example

An uninterrupted power system (UPS) model is used to illustrate the design procedures. A UPS usually provides uninterrupted, high quality, and reliable power for vital loads, such as life support systems, data storage systems, or emergency equipment. Thus, the resilience and robustness

A cyberphysical control system can be conceptually divided into six layers: physical, control, communication, network, supervisory, and management.

of the UPS are essential. An integrated design of the optimal defense mechanism for IDSs and the optimal control strategy for a pulse-width modulation (PWM) inverter is performed such that the output ac voltage can maintain its desired setting under the influence of DoS attacks. Let the system parameters be

$$A = \begin{bmatrix} 0.9226 & -0.6330 & 0 \\ 1.0 & 0 & 0 \\ 0 & 1.0 & 0 \end{bmatrix},$$
$$B_1 = \begin{bmatrix} 0.5 \\ 0 \\ 0.2 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix},$$
$$D = [0.1 \;\; 0 \;\; 0],$$
$$C = [23.738 \;\; 20.287 \;\; 0].$$

For the cyberlayer, two states are considered: a normal state θ_1 and a compromised state θ_2. When there are no attacks and the system is in normal state, the communication network is taken to be delay free, that is, $\bar{\delta}^{\theta} = \beta^{\theta} = 0$. The IDS system contains two libraries l_1, l_2 for defending against two attacks a_1, a_2. Library l_1 is used for detecting a_1 whereas library l_2 for a_2. Let $\mathcal{A} = \{a_1, a_2\}$, $\mathcal{L}^* = \{F_1, F_2\}$, where F_1 is the configuration where l_1 is loaded and F_2 is the configuration where l_2 is loaded. Figure 7 illustrates the performance of IDS configurations under different attack scenarios.

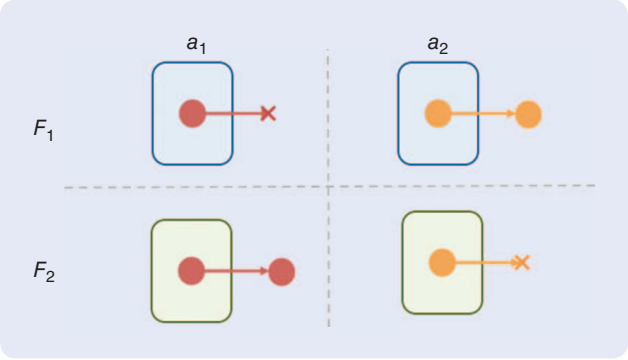


FIGURE 7 An example to illustrate the necessity of different intrusion detection system (IDS) configurations. Library l_1 is used to detect a_1 while library l_2 is used to detect a_2. Configurations $F_1 := \{l_1\}$ and $F_2 := \{l_2\}$ are used to detect a sequence of attacks composed of a_1 and a_2. Each configuration leads to a different physical layer probability of delay in S-C and C-A communication channels. The diagram shows IDS performance under four action pairs $(a_1, F_1), (a_1, F_2), (a_2, F_1)$, and (a_2, F_2) in a two-by-two matrix style, where the row corresponds to configurations, while the column refers to different attack actions. A circle refers to an attack. A box refers to a configuration. A successful defense thwarts an attack. An X denotes a successful defense that prevents the attack from propagating further. The attacks a_1 and a_2 can be successfully detected in the case of (a_1, F_1) and (a_2, F_2), respectively. The attacks will penetrate the system for the scenarios corresponding to (a_1, F_2) and (a_2, F_1).

Linear Programming for Computing Saddle-Point Equilibrium

Let A and B be two $(m \times n)$-dimensional matrices related to each other by the relation

$$A = B + c\mathbf{1}_m \mathbf{1}'_n, \tag{S3}$$

where $\mathbf{1}_m$ stands for the m-dimensional column vector whose entries are all ones and c is some constant. Denote by $V_m(A)$ and $V_m(B)$ the saddle-point values in mixed strategies for matrix games A and B, respectively. Then

1) every mixed strategy saddle-point equilibrium (MSSPE) for matrix game A also constitutes a MSSPE for the matrix game B, and vice versa
2) $V_m(A) = V_m(B) + c$.

Matrix games that satisfy (S3) are *strategically equivalent* matrix games. For a given matrix game A, a strategically equivalent matrix game can be found with all entries positive by adding a constant c.

Based on this fact, the complete equivalence between a matrix game and a linear program (LP) is used to compute its MSSPE. The following proposition captures this result, a proof of which can be found in [35].

PROPOSITION S1

Given a zero-sum matrix game described by the $m \times n$ matrix A, let B be another matrix game (strategically equivalent to A), obtained from A by adding an appropriate positive constant to make all its entries positive. Introduce the two LPs:

Primal LP: $\max y'\mathbf{1}_m$ such that $B'y \le \mathbf{1}_n$, $y \ge 0$,

Dual LP: $\min z'\mathbf{1}_n$ such that $Bz \ge \mathbf{1}_m$, $z \ge 0$,

with their optimal values (if they exist) denoted by V_p and V_d, respectively. Then

1) Both LPs admit solutions, and $V_p = V_d = 1/V_m(B)$.
2) If (y^*, z^*) solves matrix game B, $y^*/V_m(B)$ solves the primal LP, and $z^*/V_m(B)$ solves the dual LP.
3) If $\tilde{y}^*$ solves the primal LP, and $\tilde{z}^*$ solves the dual LP, the pair $(\tilde{y}^*/V_p, \tilde{z}^*/V_d)$ constitutes a MSSPE for the matrix game B, and hence for A, and $V_m(B) = 1/V_p$.

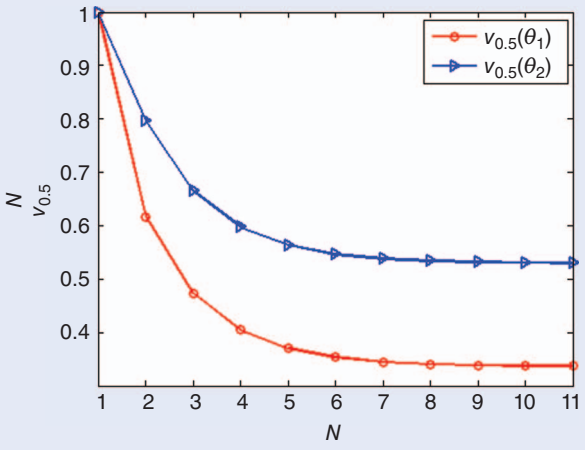


FIGURE 8 The value iteration method for finding the value of the zero-sum stochastic game using the iterative steps 4–8 in Algorithm 1. The game values at states θ_1 and θ_2 are found to be $\mathbf{v}_{0.5} = [0.3370 \;\; 0.5299]^T$. The optimal mixed strategies are $\mathbf{f}^*_{\theta_1} = [0.4273 \; 0.5726]^T$, $\mathbf{f}^*_{\theta_2} = [0.2329 \; 0.7671]^T$, $\mathbf{g}^*_{\theta_1} = [0.5726 \; 0.4273]^T$, and $\mathbf{g}^*_{\theta_2} = [0.7671 \; 0.2329]^T$.

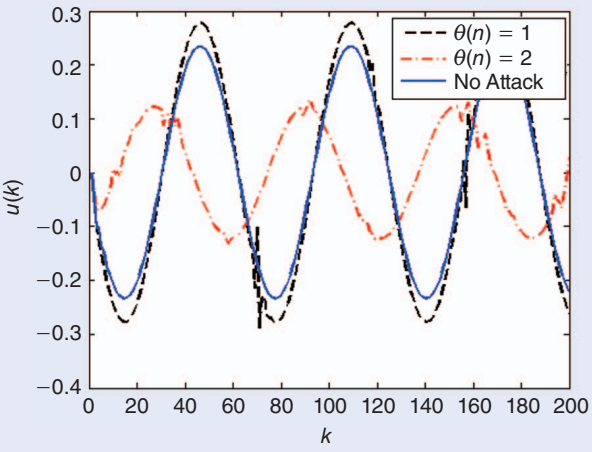


FIGURE 9 The minimax optimal controller design for the uninterrupted power system. The observer and the controller gains at state θ_1 are $L^{\theta_1} = [0.0283 \; 0.0296 \; 0.0125]^T$, and $K^{\theta_1} = [-0.9357 \; 0.6424 \; 0]$, respectively, and for θ_2, the gains are $L^{\theta_2} = [-0.7075 \; 0.7663 \; -0.0003]^T$, and $K^{\theta_2} = [0.0142 \; 0.0238 \; 0.0118]$. The controller signal at the compromised state has higher magnitude than the one at state θ_1. Under no attack (that is, the S-C and C-A delays are zero), the optimal gains are found to be $L = [0.0658 \; 0.0421 \; 0.0108]^T$, $K = [-0.9226 \; 0.6330 \; 0]$.

The following tables describe the payoff matrix pairs $(\mathbf{H}(\theta), \mathbf{W}(\theta))$ that correspond to the scenarios in Figure 7. At cyberstate θ_1,

$$\mathbf{H}(\theta_1) = \mathbf{W}(\theta_1) = \begin{array}{c|cc} & a_1 & a_2 \\ \hline F_1 & 0.01 & 0.05 \\ F_2 & 0.03 & 0.01 \end{array},$$

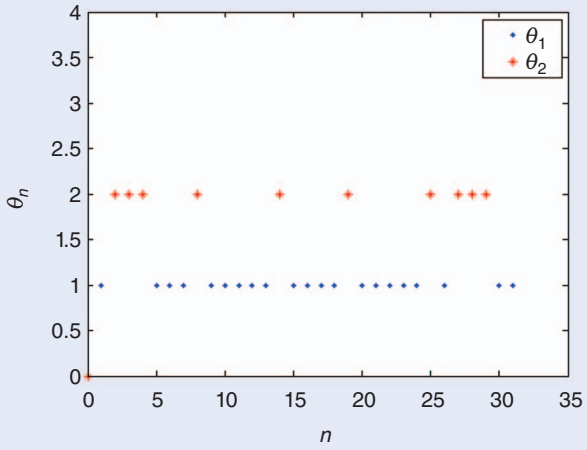


FIGURE 10 The evolution of cyberstate of the system under the saddle-point configuration policy. The cybersystem stochastically switches between two cyberstates based on the saddle-point mixed strategy of the cybergame.

and the matrix of transitions between states under different action pairs (F_i, a_j), $i = 1,2$, $j = 1,2$, is

	a_1	a_2
F_1	(1,0)	(0,1)
F_2	(0,1)	(1,0)

When IDSs are configured in a correct way to defend against attacks, the system remains safe at its normal state θ_1. When attacks cannot be defended against by the IDS, the system transitions to a failure state θ_2. Likewise, at cyberstate θ_2 the transition matrix takes the same form as in state θ_1. It captures the fact that the system can be recovered manually if intrusions are detected correctly; otherwise, the system remains in failure state θ_2.

$$\mathbf{H}(\theta_2) = \mathbf{W}(\theta_2) = \begin{array}{c|cc} & a_1 & a_2 \\ \hline F_1 & 0.06 & 0.1 \\ F_2 & 0.08 & 0.06 \end{array}.$$

The cost/reward table lists the H^∞ performance index under action pairs (F_i, a_j), $i = 1,2$, $j = 1,2$. At state θ_1,

	a_1	a_2
F_1	0.0994	0.1641
F_2	0.1232	0.0994

and at state θ_2,

	a_1	a_2
F_1	0.1961	0.8084
F_2	0.3148	0.1961

respectively.

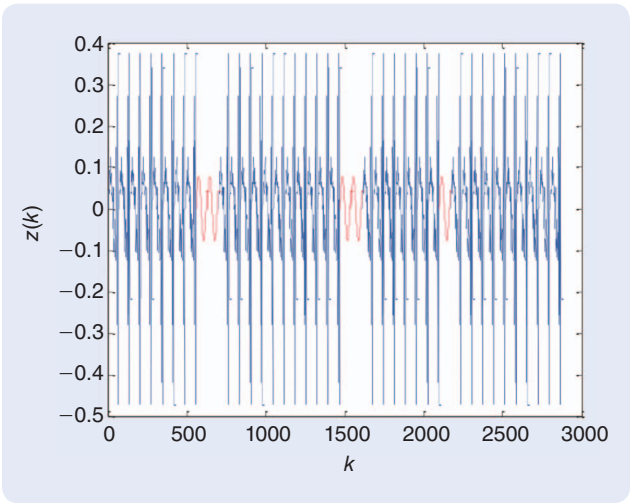


FIGURE 11 The performance when a conventional H^∞ optimal controller is used to control the physical dynamical system. The blue curve is the system output under state θ_2 whereas the red curve is the output under state θ_1. The physical-layer system performance switches randomly between the two cyberstates. The performances are shown for sinusoidal inputs for each cyberstate. In comparison to Figure 12, the resilient control allows the system to be more secure with less probability of being in a compromised state and more robust even when the system is compromised.

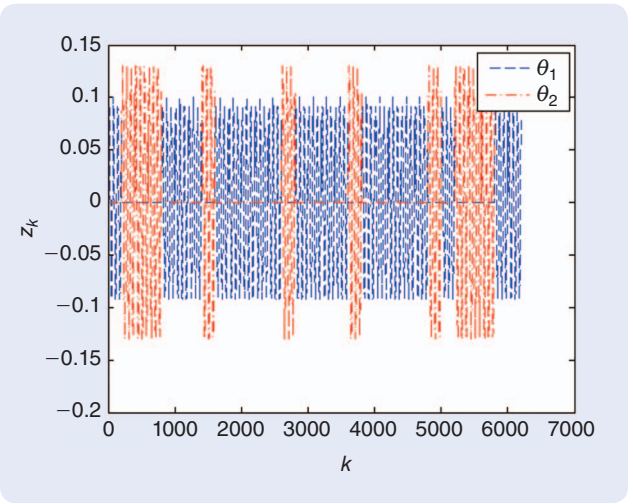


FIGURE 12 The performance of the dynamical system under the codesigned controller when it switches between two cyberstates. With a sinusoidal input into the physical layer system and the cyberswitching depicted in Figure 10, the output from the physical system is observed. At the failure state, the system has a high attenuation rate than at normal state.

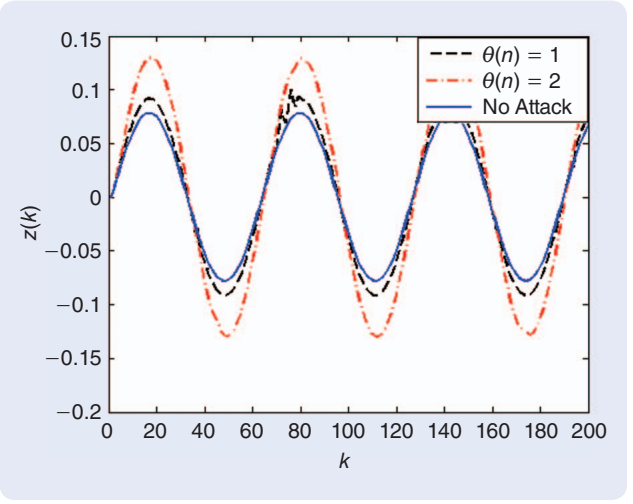


FIGURE 13 The H^∞ control result under different cyberstates. The control input signal at state θ_1 has a lower magnitude than its counterpart at state θ_2. The control system requires a higher control effort at a compromised state as it is subjected to a higher probability of S-C and C-A delays. Under no attack, the control system experiences no delays, that is, $\delta^\theta = \beta^\theta = 0$, and the control effort is the minimum among the three cases.

Using Algorithm 1, the game values with $\beta = 0.5$ at states θ_1 and θ_2 are $\mathbf{v}_{0.5} = [0.3370 \;\; 0.5299]^T$. The optimal mixed strategies are $\mathbf{f}^*_{\theta_1} = [0.4273 \; 0.5726]^T$, $\mathbf{f}^*_{\theta_2} = [0.2329 \; 0.7671]^T$, $\mathbf{g}^*_{\theta_1} = [0.5726 \; 0.4273]^T$ and $\mathbf{g}^*_{\theta_2} = [0.7671 \; 0.2329]^T$. Figure 8 shows the iterative process to find the value of the game in Algorithm 1. It can be seen that the value function of the zero-sum stochastic game converges within ten steps using the value iteration method. It can be seen from the obtained equilibrium mixed strategies that, at a compromised state, more expensive defense mechanisms are used by the system, which leads to recovery of its normal operation. Figure 9 shows the minimax control signal under minimax closed-loop optimal control. The controller signal at the compromised state has a higher magnitude than at the normal state. The system tends to spend more control effort to recover the system from instability after attacks. Figure 10 shows the evolution of cyberstates under the saddle-point configuration policy and H^∞ optimal control. The cybersystem stochastically switches between two cyberstates based on the saddle-point mixed strategies. At the equilibrium strategies, the occurrence of a compromised state is less frequent than the normal operating state. Figure 11 compares the steady-state performance of a conventional H^∞ design and its performance under resilient control design. In the failure state, the system has a higher attenuation rate than the one that occurs at the normal state due to the larger control effort (seen in Figure 9). This is how the system is designed to recover from its failure mode. Figure 12 shows the stable oscillation of the physical system under switching between two cyberstates θ_1 and θ_2. Figure 13 shows the control action from the H^∞ optimal controller for the physical layer under different cyberstates. Resilient control keeps the system more often in a normal state, and makes the system more robust even when the system is compromised.

SUMMARY AND CONCLUSION

With the increasing integration of information technologies into industrial systems and networks, such as the

To provide performance guarantees, control systems should be designed to be inherently resilient, allowing them to self-recover from unexpected attacks and failures.

power grid, robust and resilient control system design is essential for assuring the robust performance of cyberphysical control systems in the face of adversarial attacks. This article has presented a hybrid game-theoretic framework whereby the occurrence of unanticipated events is modeled by stochastic switching, and deterministic uncertainties are represented by the known range of disturbances. The design of a robust controller at the physical layer takes into account risks of failures due to the cybersystem, while the design of the security policies is based on its potential impact on the control system. The cross-layer coupled design introduced in this article results in solving a zero-sum differential game for robust control coupled with a zero-sum stochastic game for the security policy. The two games are intertwined and coupled together through cyber and physical system variables. The solution to the two coupled games requires a zooming-in process, which uses variables from the cyberlevel to solve the physical layer game, and a zooming-out process, which uses physical system variables to solve the cyberlayer game. The joint design results in a robust and resilient controller switching between different modes for guaranteeing performance in the face of unexpected events.

This article has presented a general class of system models, where the physical system is described by nonlinear ordinary differential equations, and the cybersystem is captured by Markov models. The framework can be further extended to other classes of systems including sampled-data systems, systems with delayed measurements, and model predictive control systems. The optimal design of new classes of systems can follow the same games-in-games principle discussed here and can be characterized by a new set of optimality conditions. Interesting future research includes the study of problems with stronger coupling, in which control and defense strategies depend on both cyberstates and physical states, and the development of advanced computational tools to compute the control and defense strategies. The article has also discussed offline computational methods to compute the equilibria. In addition, learning algorithms and adaptive mechanisms can be developed within this framework to provide online adaptation to changes, which will enhance the resilience of the system. Study of a distributed network of cyberphysical systems is another possible research direction. The networking effects in the cybersystem can lead to performance interdependencies of distributed physical layer control systems.

AUTHOR INFORMATION

Quanyan Zhu (quanyan.zhu@nyu.edu) is an assistant professor in the Department of Electrical and Computer Engineering at New York University. He received the B.Eng. in honors electrical engineering with distinction from McGill University in 2006, the M.A.Sc. from the University of Toronto in 2008, and the Ph.D. from the University of Illinois at Urbana-Champaign in 2013. From 2013 to 2014, he was a postdoctoral research associate in the Department of Electrical Engineering, Princeton University. He is a recipient of many awards including the NSERC Canada Graduate Scholarship, the Mavis Future Faculty Fellowships, and the NSERC Postdoctoral Fellowship. He spearheaded the INFOCOM workshop on Communications and Control on Smart Energy Systems and the Midwest Workshop on Control and Game Theory. His current research interests include optimal control, game theory, reinforcement learning, network security and privacy, resilient control systems, and cyberphysical systems. He is a Member of the IEEE. He can be contacted at LC200A, 5 MetroTech Center, Brooklyn, NY 11201 USA.

Tamer Başar is with the University of Illinois at Urbana-Champaign, where he holds the positions of Swanlund Endowed Chair, Center for Advanced Study Professor of Electrical and Computer Engineering; research professor at the Coordinated Science Laboratory; and research professor at the Information Trust Institute. He received the B.S.E.E. from Robert College, Istanbul, and the M.S., M.Phil, and Ph.D. from Yale University. He is a member of the U.S. National Academy of Engineering, a Life Fellow of IEEE, and a fellow of International Federation of Automatic Control (IFAC) and the Society for Industrial and Applied Mathematics. He has served as president of IEEE Control Systems Society (CSS), the International Society of Dynamic Games (ISDG, and the American Automatic Control Council (AACC). He has received several awards and recognitions over the years, including the highest awards of IEEE CSS, IFAC, AACC, and ISDG, and a number of international honorary doctorates and professorships. He has over 600 publications in systems, control, communications, and dynamic games, including books on noncooperative dynamic game theory, robust control, network security, wireless and communication networks, and stochastic networked control. He is on editorial boards of several journals and is editor of several book series. His current research interests include stochastic teams, games, and networks; security; and cyberphysical systems.

REFERENCES

[1] S. Gorman. (2009, Apr. 8). Electricity grid in U.S. penetrated by spies. *Wall Str. J.* [Online]. Available: http://online.wsj.com/article/SB123914805204099085.html

[2] B. Krebs. (2008, June 5). Cyber incident blamed for nuclear power plant shutdown. *Washington Post*. [Online]. Available: http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html

[3] S. Greengard, "The new face of war," *Commun. ACM*, vol. 53, no. 12, pp. 20–22, Dec. 2010.

[4] R. McMillan. (2010, Sept. 16). Siemens: Stuxnet worm hit industrial systems. [Online]. Available: http://www.computerworld.com/s/article/print/9185419

[5] L. Gunderson and C. S. Holling, *Panarchy: Understanding Transformations in Human and Natural Systems*. Washington, D.C.: Island Press, Dec. 2001.

[6] B. Walker, D. Salt, and W. Reid, *Resilience Thinking: Sustaining Ecosystems and People in a Changing World*. Washington, D.C.: Island Press, Aug. 2006.

[7] J. P. Kotter, "Accelerate!" *Harv. Bus. Rev.*, vol. 90, no. 11, pp. 45–58, Nov. 2012.

[8] E. Hollnagel, D. D. Woods, and N. Leveson, *Resilience Engineering: Concepts and Precepts*. Farnham, U.K.: Ashgate Publishing, Sept. 2006.

[9] E. Hollnagel, J. Pariès, D. D. Woods, and J. Wreathall, *Resilience Engineering in Practice: A Guide Book*. Farnham, U.K.: Ashgate Publishing, Jan. 2011.

[10] C. Rieger, D. Gertman, and M. McQueen, "Resilient control systems: Next generation design research," in *Proc. 2nd Conf. Human System Interactions*, 2009, pp. 632–636.

[11] C. Rieger, "Notional examples and benchmark aspects of a resilient control system," in *Proc. 3rd Int. Symp. Resilient Control Systems*, 2010, pp. 64–71.

[12] K. Zhou and J. Doyle, *Essentials of Robust Control*, 1st ed. Englewood Cliffs, NJ: Prentice-Hall, 1997.

[13] T. Başar and P. Bernhard, *H-Infinity Optimal Control and Related Minimax Design Problems: A Dynamic Game Approach*, 1st ed. Switzerland: Birkhäuser, 1995.

[14] M. Manshaei, Q. Zhu, T. Alpcan, T. Başar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, pp. 1–39, June 2013.

[15] T. Alpcan and T. Başar, *Network Security: A Decision and Game Theoretic Approach*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[16] D. Wei and K. Ji, "Resilient industrial control system: Concepts, formulation, metrics, and insights," in *Proc. 3rd Int. Symp. Resilient Control Systems*, 2010, pp. 15–22.

[17] W. Boyer and M. McQueen, "Ideal based cyber security technical metrics for control systems," in *Proc. 2nd Int. Conf. Critical Information Infrastructures Security*, Berlin, Heidelberg: Springer-Verlag, 2008, pp. 246–260.

[18] Q. Zhu and T. Başar, "Robust and resilient control design for cyber-physical systems with an application to power systems," in *Proc. 50th IEEE Conf. Decision Control European Control*, 2011, pp. 4066–4071.

[19] Q. Zhu and T. Başar, "A dynamic game-theoretic approach to resilient control system design for cascading failures," in *Proc. 1st Conf. High Confidence Networked Systems, CPSWeek*, Beijing, China, Apr. 16, 2012, pp. 41–46.

[20] Q. Zhu, L. Bushnell, and T. Başar, "Resilient distributed control of multi-agent cyber-physical systems," in *Proc. Workshop Control Cyber-Physical Systems*, Baltimore, MD, Mar. 20–21, 2013, pp. 301–316.

[21] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Başar, "Resilient control of cyber-physical systems against denial-of-service attacks," in *Proc. 6th Int. Symp. Resilient Control Systems*, 2013, pp. 54–59.

[22] M. Ilic, "From hierarchical to open access electric power systems," *Proc. IEEE*, vol. 95, no. 5, pp. 1060–1084, 2007.

[23] Q. Zhu and T. Başar, "A hierarchical security architecture for the smart grid," in *Smart Grid Communications and Networking*, E. Hossain, Z. Han, and H. V. Poor, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2012, ch. 18.

[24] H. Zimmermann, "OSI reference model–The ISO model of architecture for open systems interconnection," *IEEE Trans. Commun.*, vol. 28, no. 4, pp. 425–432, 1980.

[25] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 6th ed. Upper Saddle River, NJ: Pearson Education, 2012.

[26] Q. Zhu, H. Tembine, and T. Başar, "Distributed strategic learning with application to network security," in *Proc. American Control Conf.*, San Francisco, CA, June 29–July 1, 2011, pp. 4057–4062.

[27] Q. Zhu, H. Tembine, and T. Başar, "Heterogeneous learning in zero-sum stochastic games with incomplete information," in *Proc. 49th IEEE Conf. Decision Control*, 2010, pp. 219–224.

[28] M. Fabro and T. Nelson, "Control systems cyber security: Defense in depth strategies," ISA Expo, Houston, TX, INL Tech. Rep. INL/CON-07-12804, 2007.

[29] Q. Zhu, M. McQueen, C. Rieger, and T. Başar, "Management of control system information security: Control system patch management," in *Proc. Workshop Foundations Dependable Secure Cyber-Physical Systems, CPSWeek*, Apr. 2011, pp. 51–54.

[30] J. Eisenhauer, P. Donnelly, M. Ellis, and M. O'Brien, "Roadmap to secure control systems in the energy sector," Energ. Incorp., U.S. Dept. Energy and the U.S. Dept. Homeland Secur., 2006.

[31] A. Dominguez-Garcia, J. Kassakian, and J. Schindall, "A generalized fault coverage model for linear time-invariant systems," *IEEE Trans. Reliab.*, vol. 58, no. 3, pp. 553–567, 2009.

[32] A. Haidar and E. K. Boukas, "Robust stability criteria for Markovian jump singular systems with time-varying delays," in *Proc. 47th IEEE Conf. Decision Control*, 2008, pp. 4657–4662.

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

[34] T. Başar, "Minimax control of switching systems under sampling," *Int. J. Control*, vol. 25, no. 5, pp. 315–325, Aug. 1995.

[35] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory* (Classics in Applied Mathematics), 2nd ed. Philadelphia, PA: Soc. Ind Appl. Math., 1999.

[36] Q. Zhu and T. Başar, "Dynamic policy-based IDS configuration," in *Proc. 48th IEEE Conf. Decision Control, Held Jointly with the 28th Chinese Control Conf.*, 2009, pp. 8600–8605.

[37] Q. Zhu, H. Tembine, and T. Başar, "Network security configurations: A nonzero-sum stochastic game approach," in *Proc. American Control Conf.*, 2010, pp. 1059–1064.

[38] Q. Zhu, A. Clark, R. Poovendran, and T. Başar, "Deceptive routing games," in *Proc. IEEE 51st Annu. Conf. Decision Control*, 2012, pp. 2704–2711.

[39] A. Clark, Q. Zhu, R. Poovendran, and T. Başar, "Deceptive routing in relay networks," in *Proc. Conf. Decision Game Theory Security* (Lecture Notes in Computer Science), J. Grossklags and J. C. Walrand, Eds. Berlin Heidelberg, Germany: Springer-Verlag, 2012, pp. 171–185.

[40] Q. Zhu and T. Başar, "Feedback-driven multi-stage moving target defense," in *Proc. Conf. Decision Game Theory Security* (Notes in Computer Science). Berlin Heidelberg, Germany: Springer-Verlag, 2013.

[41] Q. Zhu, H. Tembine, and T. Başar, "Hybrid learning in stochastic games and its application in network security," in *Reinforcement Learning and Approximate Dynamic Programming for Feedback Control* (Computational Intelligence Series), F. L. Lewis and D. Liu, Eds. Piscataway, NJ: IEEE Press, 2012, ch. 14, pp. 305–329.

[42] B. Randell, P. Lee, and P. C. Treleaven. (1978, June). Reliability issues in computing system design. *ACM Comput. Surv.* [Online]. *10(2)*, pp. 123–165. Available: http://doi.acm.org/10.1145/356725.356729

[43] L. S. Shapley, "Stochastic games," *Proc. Natl. Acad. Sci.*, vol. 39, no. 10, pp. 1095–1100, 1953.

[44] J. Filar and K. Vrieze, *Competitive Markov Decision Processes*, 1st ed. Berlin Heidelberg, Germany: Springer-Verlag, 1996.

[45] T. E. S. Raghavan and J. A. Filar, "Algorithms for stochastic games—A survey," *Methods Models Oper. Res.*, vol. 35, no. 6, pp. 437–472, 2003.

[46] O. Hernandez-Lerma and J. Lasserre, "Zero-sum stochastic games in Borel spaces: Average payoff criteria," *SIAM J. Control Optim.*, vol. 39, no. 5, pp. 1520–1539, 2000.

[47] S. Meyn and R. L. Tweedie, *Markov Chains and Stochastic Stability*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, Apr. 2009.

[48] O. do Valle Costa, M. Fragoso, and M. Todorov. (2012). *Continuous-Time Markov Jump Linear Systems* (Probability and its applications). Berlin Heidelberg, Germany: Springer-Verlag. [Online]. Available: http://books.google.com/books?id=Lal5ECvti-0C

[49] J. Nash, "Equilibrium points in N-person games," *Proc. Natl. Acad. Sci.*, vol. 36, no. 1, pp. 48–49, 1950.

[50] D. Bond. (2012, Feb. 20). Quickdraw SCADA IDS. [Online]. Available: http://www.digitalbond.com/tools/quickdraw/

[51] R. A. Kisner, "Cybersecurity through real-time distributed control systems," Oak Ridge Natl. Lab., Tech. Rep. ORNL/TM-2010/30, 2010, pp. 4–5.

[52] J. von Neumann, "Zur Theorie der Gesellschaftsspiele," *Math. Annalen*, vol. 100, no. 1, pp. 295–320, 1928.