Resilient Distributed Control of Multi-agent Cyber-Physical Systems

Quanyan Zhu[1], Linda Bushnell[2], and Tamer Başar[1,⋆]

[1] Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
1308 W. Main St., Urbana, IL
{zhu31,basar1}@illinois.edu
[2] Networked Control Systems Lab
EE Dept., University of Washington
Seattle, WA, 98195, USA
lb2@uw.edu

Abstract. Multi-agent cyber-physical systems (CPSs) are ubiquitous in modern infrastructure systems, including the future smart grid, transportation networks, and public health systems. Security of these systems are critical for normal operation of our society. In this paper, we focus on physical layer resilient control of these systems subject to cyber attacks and malicious behaviors of physical agents. We establish a cross-layer system model for the investigation of cross-layer coupling and performance interdependencies for CPSs. In addition, we study a two-system synchronization problem in which one is a malicious agent who intends to mislead the entire system behavior through physical layer interactions. Feedback Nash equilibrium is used as the solution concept for the distributed control in the multi-agent system environment. We corroborate our results with numerical examples, which show the performance interdependencies between two CPSs through cyber and physical interactions.

Keywords: Cyber-Physical Systems, Network Security, Differential Games, Multi-Resolution Games, Games-in-Games, Coupled Riccati Differential Equations, Secure Control, Resilient Control Systems.

1 Introduction

Recent years have witnessed increasing integration of information technologies into modern critical infrastructures including energy systems, transportation systems and public health. The technological advancement has also brought many challenges for understanding the efficient and reliable integration of cyber and physical components of the system. Security is one of the major concerns of such

⋆ Research was supported in part by an AFSOR MURI Grant (FA9550-10-1-0573), and in part by an NSA Grant through the Information Trust Institute at the University of Illinois.

D.C. Tarraf (ed.), *Control of Cyber-Physical Systems*,
Lecture Notes in Control and Information Sciences 449,
DOI: 10.1007/978-3-319-01159-2_16,

cyber-physical systems (CPSs). With the migration from a closed network to an open and public network, adversaries can take advantage of vulnerabilities existing in cyber world in order to compromise or inflict damages on the physical system. To protect these systems, it is imperative for us to design defense schemes both at the cyber and physical layers of the system to provide security mechanisms for reliable operations.

Modern systems are increasingly complex because of multi-layer system integrations, which lead to "systems of systems". Moreover, the complexity also comes from the large scale of the system, composed of a large number of interacting distributed systems or agents that are coordinated or controlled to accomplish a certain task in a decentralized manner. Illustrated in Fig. 1, multiple CPSs are interconnected with each system autonomously controlling itself and reacting to the environment as well as cyber or physical signals of other systems. The multi-agent system architecture renders it difficult to study the security issues of such multi-agent CPSs using conventional methods. Instead, it is important to establish new frameworks for understanding the system security interdependencies. The vulnerability of the cyber component of one system can lead to insecurity of physical components of another system. Similarly, it is also possible that the physical compromise of one system can become the cyber vulnerability of another connected system.

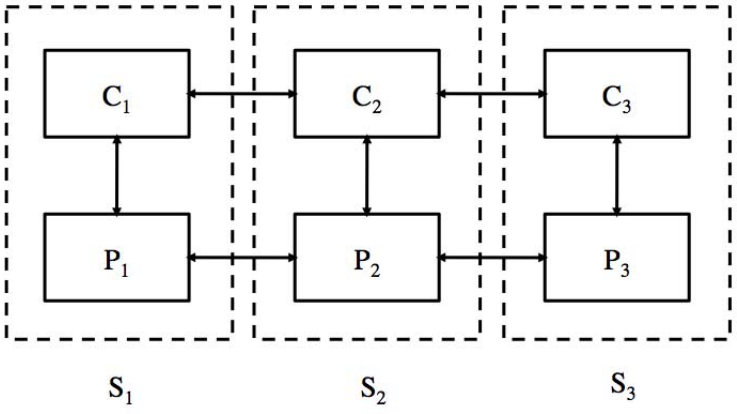

Fig. 1. Three interconnected CPSs: Each system $S_j, j = 1, 2, 3$, is composed of its cyber system C_j and physical system P_j. Three CPSs have interactions at both the physical layer and the cyber layer.

Game theory provides systematic modeling and computational tools to address these issues. Recent literature has seen a surge of interest in applying game-theoretic methods to understand cyber security and secure control systems [2,15]. In [3], static and dynamic game frameworks have been used to design equilibrium revocation strategies for defending sensor networks from node capturing and cloning attacks. In [4], a stochastic game has been used to model the

strategic interactions between an intrusion detection system (IDS) and a malicious intruder, and the authors have used online reinforcement learning methods to provide data-driven defense polices for dynamic IDS configurations.

Most of current literature have focused on problems residing at either cyber or physical components of the system. To address the system integration problem, it is essential and also inevitable to establish system models that allow detailed investigations of cross-layer coupling and performance interdependencies for CPSs. In [4, 5], we have proposed a stochastic hybrid system model, where each mode represents the condition under which physical dynamical systems evolve, and the system switches from one mode to another, depending on cyber attacks and security policies. The robust control design for the physical system against noise and disturbances is strongly coupled with the cyber defense mechanism design against cyber attacks. It has been shown that under the linear-quadratic robust control system paradigm as in [6] and the stochastic game modeling of cyber security systems as in [7, 8], the design of the CPS results in a set of coupled equations to be solved for achieving resilient and robust control of the system. This work has provided us fundamental and rich concepts in designing optimal cross-layer CPSs. The cyber system model can be further extended by including detailed models for describing attacks on cyber components based on recently developed games-in-games principle for multi-resolution games [9, 10], while the physical system model can also be extended to investigate multi-agent CPSs for understanding the multi-system interdependencies.

The goal of this paper is to focus on the latter part of the extension. We first discuss a general framework for designing distributed control schemes for multi-agent CPSs, and then establish a stochastic hybrid differential game model for studying the impact of a malicious physical system on the physical dynamics of other systems. In particular, we study a two-person synchronization problem where S_1 aims to achieve synchrony with S_2, while S_2 intends to mislead S_1 to an unfavorable system state. We provide a set of coupled Riccati differential equations to characterize the feedback Nash equilibrium solution of an N-person stochastic hybrid differential game. This investigation provides an initial step toward addressing more complex scenarios where cyber systems can be reconfigured in response to physical systems. We also see that this work serves as the inner-most game within the games-in-games framework for large scale hierarchical systems.

The paper is organized as follows. In Section 2, we discuss related work to our problem. In Section 3, we present the general system model for multi-agent cyber-physical systems. In Section 4, we study the feedback Nash equilibrium strategies for a two-person game problem. Section 5 provides numerical examples to illustrate the equilibrium solutions, and we conclude in Section 6.

2 Related Works

Our work falls into many different research areas in the literature. Our system model for describing CPSs is based on the continuous-time Markov jump linear

systems, which has been widely studied in the literature in [11–13]. In [11], zero-sum differential game frameworks are used to study H-infinity robust control of Markovian jump systems. [13] has studied the minimax control of randomly switching systems under sampled state information. In this work, we build our multi-agent system model based on systems of similar structures, and investigate distributed control using N-person nonzero-sum differential games.

This work focuses on the physical component under the larger framework of resilient control established in [4, 5]. With the parameters of the cyber components fixed, we investigate the control of multi-agent systems at different system modes. This includes the design of distributed controllers at critical systems states, which allows to provide certain level of system performance after cyber attacks.

Adversarial behaviors reside at multiple layers of the system. [14] has proposed a hierarchical security framework for CPS, in particular for the emerging smart grid, and discussed security issues at the control, communications, and information management layers of the system. The goal of resilient control of CPS is to adopt first a divide-and-conquer approach and then integrate the layer-specific solutions together as the system-level solution. Following this methodology, this work considers malicious behaviors at the physical layer, where some agents intend to mislead or inflict damage on the agents through physical interactions. Solution to this problem can be interfaced with solutions from the other layers, such as those in [15, 16], through recently developed games-in-games principle for multi-resolution games [9, 10].

3 System Model for Multi-agent CPSs

In this section, we present a general system model for describing the interactions between multi-agent CPSs. Let $\mathcal{N} = \{1, 2, \cdots, N\}$ be the index set, and $\mathcal{S} = \{S_1, S_2, \cdots, S_N\}$ the set of N interconnected CPSs. Each system $S_j \in \mathcal{S}$ is composed of a cyber system C_j and a physical system P_j. We let $\mathcal{C} = \{C_1, C_2, \cdots, C_N\}$ be the N cyber systems associated with $\mathcal{S}$, and $\mathcal{P} = \{P_1, P_2, \cdots, P_N\}$ be the set of N physical dynamical systems. The cyber systems are often described by graphical models and their modeling can be found in many recent literature on decision and control at cyber-level of CPS [9, 15], while the physical systems are often modeled through dynamical systems governed by physical laws and constraints. The focus of this paper will be on the interconnected physical systems $\mathcal{P}$ and the impact of cyber systems $\mathcal{C}$ on the performance of $\mathcal{P}$. The multi-agent interactions between N systems can be represented by two graphs. One is $\mathcal{G}_P := \langle \mathcal{N}, \mathcal{E}_P \rangle$ that represents the cyber relations among N systems. Such relations can exist at multiple levels within the cyber system, ranging from communication links between two work stations [16] to security interdependencies through economic investment [17]. The other graph is denoted by $\mathcal{G}_C := \langle \mathcal{N}, \mathcal{E}_C \rangle$, which captures the interconnections between physical systems. It can represent the underlying information flow of sensing or actuation signals. In Fig. 1, both cyber and physical parts of the systems are interconnected in the same fashion, i.e., $\mathcal{E}_C = \mathcal{E}_P := \{(1, 2), (2, 3)\}$.

We describe the dynamics of each CPS S_j by a continuous-time Markov jump linear system as follows:

$$\dot{x}_j = A_j(t, \theta_j(t))x_j + B_j(t, \theta_j(t))u_j; \quad x_j(t_0) = x_{j,0}, \tag{1}$$

where $x_j \in \mathbb{R}^{n_j}$ is the n_j-dimensional system state vector of system $P_j \in \mathcal{P}$; $u_j \in \mathbb{R}^{p_j}$ is the p_j-dimensional control input determined by P_j; θ_j is a finite state Markov chain defined on the state space $\Theta_j = \{\theta_{j,1}, \theta_{j,2}, \cdots, \theta_{j,M}\}$ with a positive initial distribution $\pi_j^0 := [\pi_{j,1}^0, \pi_{j,2}^0, \cdots, \pi_{j,M}^0]$ and the infinitesimal generator matrix $\Lambda_j = (\lambda_{i,i'}(t))_{i\in\Theta_j, i'\in\Theta_j}$, such that $\lambda_{ii'} \geq 0$ for $i \neq i'$ and

$$\mathbb{P}\{\theta_j(t+h) = i' | \theta_j(t) = i\} = \begin{cases} \lambda_{ii'}h + o(h), & i' \neq i \\ 1 + \lambda_{ii}h + o(h), & i' = i \end{cases}.$$

The system states x_j and inputs u_j each belong to appropriate Hilbert spaces $\mathcal{H}_{x_j}$ and $\mathcal{H}_{u_j}$, respectively, defined on the time interval $[0, t_f]$. The system P_j is stochastic due to the switching between different modes or forms governed by Λ_j. Here, we assume that $A_j(t, i) \in \mathbb{R}^{n_j \times n_j}$ and $B_j(t, i) \in \mathbb{R}^{n_j \times p_j}$ are piecewise continuous in t for each $i \in \Theta$.

Note that the process θ_j in stochastic hybrid dynamics (1) captures structural changes of the physical system caused by successful cyber attacks, while x_j models the evolution of physical states of P_j. For example, the attack on circuit breakers in energy systems will change the system from being in normal mode to restorative or emergency mode, where partial load is lost or power flow constraint is violated. It is important to design contingent voltage or frequency control strategies in response to mode changes at the physical layer. However, it is also necessary to take appropriate cyber control actions to restore the system to its normal state [14,18].

For each system S_j, input u_j directly controls the physical state x_j, while the defense in the cyber domain determines the rate matrix Λ. In this paper, we assume that Λ is given and find distributed control strategies of each system when centralized coordination is not possible. In particular, we study the case where malicious behaviors are present in the physical component of the system. These adversarial effects can be caused by physical compromise of a normal system or manual placement of malicious agents into the network, which is in the same spirit as the node capturing and cloning attacks in sensor networks [3]. In addition, the malicious behavior can also be induced through cyber attacks, where normal system behavior can be altered by Stuxnet-like worms through the enterprise and process control networks [19].

The goal of each system S_j can be captured by the performance index L_j given as:

$$L_j(x_j, u_j; \theta_j, t_0) = q_j^f(x(t_f); \theta(t_f)) + \int_{t_0}^{t_f} g_j(t, x_j(t), u_j(t); \theta(t))dt,$$

where $x(t) = [x_1^T(t), x_2^T(t), \cdots, x_N^T(t)]'$, $\theta(t) = [\theta_1, \theta_2, \cdot, \theta_N]^T$, q_j^f is continuous in x, and g_j is jointly continuous in (t, x_j, u_j). We consider the feedback

perfect-state measurement information structure for all systems and design controller in the form of

$$u_j(t) = \gamma_j(t, x(t); \theta(t)), \tag{2}$$

where γ_j is an admissible feedback control strategy, piecewise continuous in its first argument, and Lipschitz continuous in its second argument. We denote the class of all such control strategies by $\mathcal{M}_j^{\text{FB}}$. Note that each P_j can observe the state information of other systems through interconnection graph $\mathcal{G}$. Hence in general, the control and its performance index will be dependent on the aggregate state vector x.

Under the above assumptions and with controls picked as in (2), the system (1) admits a well-defined solution, which will induce corresponding "open-loop" representations of γ_j. By taking the expected value of the resulting stochastic cost L_j over the statistics of θ will lead to the average cost corresponding to the inputs generated by γ_j, which we write as:

$$J_j(\gamma_j, \gamma_{-j}; t_0) = \mathbb{E}_\theta\{L_j(x_j, u_j; \theta)\}, \tag{3}$$

where $\gamma_{-j} := \{\gamma_1, \cdots, \gamma_{j-1}, \gamma_{j+1}, \cdots, \gamma_N\}$ denotes the set of control strategies other than γ_j.

Since each system computes its own optimal control, the objective of each system S_j is to minimize the cost J_j over all its own feedback control policies:

$$\min_{\gamma_j \in \mathcal{M}_j^{\text{FB}}} J_j(\gamma_j, \gamma_{-j}; t_0). \tag{4}$$

This will lead to an $N-$person differential game model with each system solving (4), and its solution is characterized by feedback Nash equilibrium (FBNE) defined as follows.

Definition 1 (Feedback Nash Equilibrium, [1]). *The strategy profile* $(\gamma_1^*, \gamma_2^*, \cdots, \gamma_N^*)$ *is a feedback Nash equilibrium (FBNE) for the* N*-person stochastic differential game described by (1) and (3) if for all* $j \in \mathcal{N}$ *and* $\gamma_j \in \mathcal{M}_j^{FB}$,

$$J_j(\gamma_j^*, \gamma_{-j}^*; t_0) \leq J_j(\gamma_j, \gamma_{-j}^*; t_0).$$

In addition, the equilibrium strategies are strongly time-consistent if for all $j \in \mathcal{N}$, $t \in [t_0, t_f)$, *and* $\gamma_j \in \mathcal{M}_j^{FB}$,

$$J_j(\gamma_j^*, \gamma_{-j}^*; t) \leq J_j(\gamma_j, \gamma_{-j}^*; t).$$

4 Two-System Problem

In this section, we consider the case of two interconnected systems $S_1 = \langle C_1, P_1 \rangle$, and $S_2 = \langle C_2, P_2 \rangle$. Each system $S_j, j \in \mathcal{N}$, has two modes. We let $\theta_{j,1}$ refer to the normal or safe operation state, while $\theta_{j,2}$ refers to the compromised state after

the success of cyber attacks. The goal of S_1 is to achieve physical synchronization with S_2 and its finite-horizon cost function (3) can be rewritten as

$$J_1 = \mathbb{E}\left\{ \frac{1}{2}|x_1(t_f) - x_2(t_f)|^2_{Q_1^f(\theta(t_f))} + \frac{1}{2}\int_0^{t_f} \Big(|x_1(t) - x_2(t)|^2_{Q_1(t,\theta(t))} + |u_1(t)|^2_{R_1(t,\theta(t))} \Big)\, dt \right\}, \quad (5)$$

The goal of S_2 is a malicious system which intends to mislead the state of S_1 to its preferred state $\bar{x}_2 \in \mathbb{R}$. Hence its associated performance index is described by

$$J_2 = \mathbb{E}\left\{ \frac{1}{2}|x_2(t_f) - \bar{x}_2|^2_{Q_2^f(\theta(t_f))} + \frac{1}{2}\int_0^{t_f} \Big(\alpha|x_1(t) - x_2(t)|^2_{Q_2(t,\theta(t))} + (1-\alpha)|x_2(t) - \bar{x}_2|^2_{Q_2(t,\theta(t))} + |u_2(t)|^2_{R_2(t,\theta(t))} \Big)\, dt \right\}, \quad (6)$$

where $\alpha \in (0,1)$ is a weighting parameter. In (5) and (6), $Q_j^f(\cdot), Q_j(\cdot,\cdot), j = 1,2$, are non-negative definite matrices of proper dimensions, and $R_j(\cdot,\cdot)$ is positive definite. In addition, we assume that $Q_j(t,i), R_j(t,i)$ are piece-wise continuous in t for each $i \in \Theta$.

We assume that each system S_j has perfect observation of its own physical states x_j and system mode θ_j as well as the state and the mode of the other system. Hence we have $\mathcal{E}_C = \mathcal{E}_P := \{(1,2)\}$. Let the aggregate state and mode vectors be given by $x := [x_1^T, x_2^T]^T \in \mathbb{R}^2$ and $\theta := [\theta_1, \theta_2]^T \in \Theta := \Theta_1 \times \Theta_2$. The control input u_j of P_j is generated by a feedback strategy γ_j^F, according to (2).

4.1 Feedback Nash Equilibrium Solution

In this subsection, we characterize the feedback Nash equilibrium of the game associated with (1), (5), (6), and (2). The evolution of aggregated system $\mathcal{S}$ is described by

$$\dot{x} = \tilde{A}(t,\theta(t))x + \sum_{j=1}^{N} \tilde{B}_j(t,\theta(t))u_j, \quad (7)$$

where the system parameters $\tilde{A} \in \mathbb{R}^{(n_1+n_2)\times(n_1+n_2)}$ and $\tilde{B}_1 \in \mathbb{R}^{(n_1+n_2)\times n_1}, \tilde{B}_2 \in \mathbb{R}^{(n_1+n_2)\times n_2}$ are given by

$$\tilde{A}(t,\theta(t)) = \begin{bmatrix} A_1(t,\theta(t)) & 0_{n_1\times n_2} \\ 0_{n_2\times n_1} & A_2(t,\theta(t)) \end{bmatrix},$$

$$\tilde{B}_1(t,\theta(t)) = \begin{bmatrix} B_1 \\ 0_{n_2\times n_1} \end{bmatrix} \text{ and } \tilde{B}_2(t,\theta(t)) = \begin{bmatrix} 0_{n_1\times n_2} \\ B_2 \end{bmatrix}.$$

In addition, we define the following quantities:

$$\tilde{Q}_1(t,\theta(t)) := \begin{bmatrix} Q_1(t,\theta(t)) & -Q_1(t,\theta(t)) \\ -Q_1(t,\theta(t)) & Q_1(t,\theta(t)) \end{bmatrix},$$

$$\tilde{Q}_2(t,\theta(t)) := \begin{bmatrix} \alpha Q_2(t,\theta(t)) & -\alpha Q_2(t,\theta(t)) \\ -\alpha Q_2(t,\theta(t)) & Q_2(t,\theta(t)) \end{bmatrix},$$

$$\tilde{Q}_1^f(\theta(t)) = \begin{bmatrix} Q_1^f(\theta(t)) & -Q_1^f(\theta(t)) \\ -Q_1^f(\theta(t)) & Q_1^f(\theta(t)) \end{bmatrix},$$

$$\tilde{Q}_2^f(\theta(t)) = \begin{bmatrix} 0_{n_1\times n_1} & 0_{n_1\times n_2} \\ 0_{n_2\times n_1} & Q_2^f(\theta(t)) \end{bmatrix}, \quad \text{and}$$

$$p_1^T(t,\theta(t)) = 0_{1\times(n_1+n_2)}, \quad p_2^T(t,\theta(t)) = \begin{bmatrix} 0_{1\times n_1} & (1-\alpha)\bar{x}_2^T(Q_2^T+Q_2) \end{bmatrix}$$

We can rewrite (5) and (6) into the following equivalent cost functions:

$$\tilde{J}_1 = \mathbb{E}\left\{ \frac{1}{2}x^T\tilde{Q}_1^f(\theta(t_f))x + \frac{1}{2}\int_0^{t_f} \Big(x^T\tilde{Q}_1(t,\theta(t))x - p_1^T(t,\theta(t))x + u_1^T R_1(t,\theta(t))u_1 \Big)\, dt \right\}, \tag{8}$$

$$\tilde{J}_2 = \mathbb{E}\left\{ \frac{1}{2}x^T\tilde{Q}_2^f(\theta(t_f))x + \frac{1}{2}\int_0^{t_f} \Big(x^T\tilde{Q}_2(t,\theta(t))x - p_2^T(t,\theta(t))x + u_2^T R_2(t,\theta(t))u_2 \Big)\, dt \right\}, \tag{9}$$

Note that the direct coupling between two systems in this problem comes from the cost function while the indirect coupling enters in the dynamics though the feedback control strategies based on the information flow topology $\mathcal{G}_C, \mathcal{G}_P$. Following [20], to characterize the equilibrium solution, we let value functions V_j take the form of

$$V_j(t,x,\theta(t)) = \frac{1}{2}x^T Z_j(t,\theta(t))x + c_j^T(t,\theta(t))x + \eta_j(t,\theta(t)). \tag{10}$$

In addition, denote by $Z_j^l(t) := Z_j(t,\theta(t))$, $c_j^l(t) := c_j(t,\theta(t)), p_j^l(t) := p_j(t,\theta(t))$, $\eta_j^l(t) := \eta_j(t,\theta(t))$, when $\theta(t) = l, l \in \Theta$.

Theorem 1. *For the N-person stochastic differential game described above, let there exist a set of matrix valued functions $Z_j^l(t) \geq 0, j \in \mathcal{N}, l \in \Theta$, satisfying the following N coupled matrix Riccati differential equations:*

$$\dot{Z}_j^l + Z_j^l F_j^l + (F_j^l)^T Z_j^l + \tilde{Q}_j^l + Z_j^l \tilde{B}_j^l (R_j^l)^{-1}(\tilde{B}_j^l)^T Z_j^l + \sum_{l'\in\Theta} \lambda_{ll'} Z_j^{l'} = 0, \tag{11}$$

$$Z_j^l(t_f) = \tilde{Q}_j^f, \quad l \in \Theta \tag{12}$$

where

$$F_j^l := A^l - \sum_{j'=1,2} \tilde{B}_{j'}^l (R_{j'}^l)^{-1}(\tilde{B}_{j'}^l)^T Z_{j'}^l.$$

Then, the differential game admits a FBNE solution, affine in the current value of the aggregate state $x(t)$, given by

$$\begin{aligned} u_j^*(t) &= \gamma_j^*(t, x(t), \theta(t)) \\ &= -R_j^{-1}(t,\theta(t))\tilde{B}_j^T(t,\theta(t))[Z_j(t,\theta(t))x(t) + c_j(t,\theta(t))], \quad j \in \mathcal{N}, \end{aligned} \tag{13}$$

where $c_j(t,\theta(t))$ are obtained as the unique solution of the coupled linear differential equations:

$$\dot{c}_j^l + (F_j^l)^T c_j^l - Z_j^l \left\{ \sum_{j' \neq j} \tilde{B}_{j'}^l (R_{j'}^l)^{-1} (\tilde{B}_{j'}^l)^T c_{j'}^l \right\} - \frac{1}{2} p_j^l + \sum_{l' \in \Theta} \lambda_{ll'} c_j^{l'} = 0 \tag{14}$$

$$c_1^l(t_f) = 0, \quad l \in \Theta \tag{15}$$

$$c_2^l(t_f) = -\frac{1}{2}\bar{x}_2^T((Q^f)^T + Q^f), \quad l \in \Theta \tag{16}$$

The corresponding values of the cost functionals associated with each mode are

$$V_j^l(0, x_0) = \frac{1}{2} x_0^T Z_i^l(0) x_0 + (c_j^l)^T x_0^T + \eta_j^l(0),$$

where $\eta_j^l,\ j \in \mathcal{N},\ l \in \Theta$ are obtained from

$$\begin{aligned} &\dot{\eta}_j^l - (c_j^l)^T \left\{ \sum_{j'=1,2} \tilde{B}_{j'}^l (R_{j'}^l)^{-1} (\tilde{B}_{j'}^l)^T c_{j'}^l \right\} \\ &+ \frac{1}{2}(c_j^l)^T \tilde{B}_j^l (R_j^l)^{-1} (\tilde{B}_j^l)^T c_j^l + \sum_{l' \in \Theta} \lambda_{ll'} \eta_j^{l'} = 0, \end{aligned} \tag{17}$$

$$\eta_j^l(t_f) = 0, \quad l \in \Theta \tag{18}$$

Proof (Sketch of Proof). With γ_2^* fixed, the sufficient condition for the feedback strategy γ_1^* to be optimal is that the cost-to-go function $V_1(t,x,\theta(t))$ satisfies the following partial differential equations [20]:

$$\begin{aligned} \min_{u_1} \Bigg\{ &\frac{\partial}{\partial t} V_1(t,x,i) + \frac{\partial}{\partial x} V_1(t,x,i) \cdot \Big(\tilde{A}(t,i)x + \tilde{B}_1(t,i)u_1 \\ &+ \tilde{B}_2(t,i)\gamma_2^*(t,x,i) \Big) + \sum_{i' \in \Theta} \lambda_{ii'} V_1(t,x,i') \Bigg\} = 0. \end{aligned} \tag{19}$$

Likewise, with γ_1^* fixed, the sufficient condition for γ_2^* is that $V_2(t,x,\theta(t))$ satisfies

$$\begin{aligned} \min_{u_2} \Bigg\{ &\frac{\partial}{\partial t} V_2(t,x,i) + \frac{\partial}{\partial x} V_2(t,x,i) \cdot \Big(\tilde{A}(t,i)x + \tilde{B}_1(t,i)\gamma_1^* \\ &+ \tilde{B}_1(t,i)u_1 \Big) + \sum_{i' \in \Theta} \lambda_{ii'} V_2(t,x,i') \Bigg\} = 0. \end{aligned} \tag{20}$$

The results follow from using (19) and (20) and the value function in the form of (10).

Note that the FBNE obtained above is also strongly-time consistent. The equilibrium control strategies retain the same form for any initial conditions of the game. This leads to a robust and optimal solution in case of disturbances and errors.

Fig. 2. System mode transitions from normal mode to failure mode. Such mode switch is dictated by cyber defense mechanisms, and it has impact on evolution of the physical state of the system.

5 A Numerical Example

In this section, we use a numerical example to illustrate the solution outlined in the section above. In Fig. 2, we depict the transition of individual systems from their normal operation ($\theta_j = 1$) to failure mode ($\theta_j = 2$). In the two-system case, this leads to a total four aggregate modes, i.e., $\Theta = \{\theta_1, \theta_2, \theta_3, \theta_4\}$ with $\theta_1 = (1,1), \theta_2 = (1,2), \theta_3 = (2,1), \theta_4 = (2,2)$. We let θ_4 be the absorbing mode, where no cyber recovery mechanisms are available at the same time scale of the state evolution at the physical layer. The rate matrix Λ is chosen as follows:

$$\Lambda = \begin{bmatrix} -\frac{3}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ 0 & -\frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{21}$$

Fig. 3 illustrates the transition between different modes.

The transition from one mode to another corresponds to the system failure due to cyber attacks. As a result, the aggregate system $\mathcal{S}$ has different system dynamics at each mode. In this example, we let x_j be scalars, and let $A^l, l \in \Theta$, be the only quantities that are mode-dependent and take the following values:

$$\tilde{A}^1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \ \tilde{A}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \tilde{A}^3 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \ \tilde{A}^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{22}$$

It is easy to see that each failure causes the corresponding system "less stable" by switching the diagonal entry from 0 to 1. We let other parameters in the

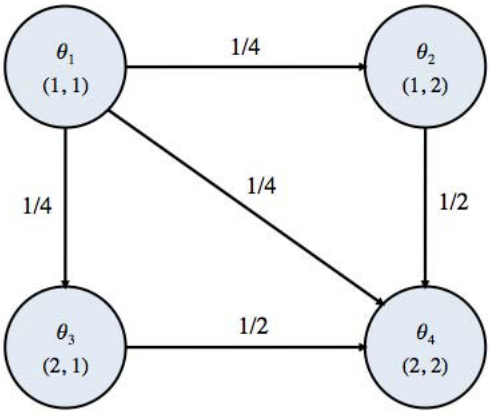

Fig. 3. Rate matrix Λ: θ_1 is the normal operating state. The entire system can fail and transition to another mode at equal rates to $\theta_1, \theta_2, \theta_3$. The intermediate failure modes θ_2, θ_3 switch to θ_4 when cyber attack occurs. θ_4 is the absorbing state. The system can not recover immediately once damaged.

system to be independent of modes, i.e., for all $l \in \Theta$, $j = 1, 2$, $B_j^l = 1$, $R_j^l = 1$, $\alpha = 1/2$, and

$$\tilde{Q}_1 = \tilde{Q}_1^f = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}, \quad \tilde{Q}_2^f = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad \tilde{Q}_2 = \begin{bmatrix} \alpha & -\alpha \\ -\alpha & 1 \end{bmatrix}. \tag{23}$$

We obtain the FBNE solution in the form of

$$u_1^*(t) = K_1^1(t, \theta(t))x_1 + K_1^2(t, \theta(t))x_2 + \xi_1(t, \theta(t)) \tag{24}$$
$$u_2^*(t) = K_2^1(t, \theta(t))x_1 + K_2^2(t, \theta(t))x_2 + \xi_2(t, \theta(t)) \tag{25}$$

and the resulting system dynamics are given by

$$\dot{x}(t) = (\tilde{A}(t, \theta(t)) + K_1(t, \theta(t)) + K_2(t, \theta(t)))x(t) + \xi(t, \theta(t)), \tag{26}$$

where $K_j = [K_j^1, K_j^2]^T, j = 1, 2$, and $\xi = [\xi_1, \xi_2]^T$. We set the initial condition as $\theta(0) = \theta_1$ and $x(0) = [0, 1/2]^T$. In Figs. 4 and 5, we show the feedback control gains K_1^1 and K_2^2 for systems S_1 and S_2 for the time interval $[0, 2.5]$. We can see that the feedback gain K_1^1 at modes θ_1, θ_2 are close and its behavior at modes θ_3, θ_4 are similar to each other. It is easy to see that in modes θ_1 and θ_2, the system S_1 is in normal operation mode. The difference in the gains $K_1^1(t, 1), K_1^1(t, 2)$ is due to the coupling from the malfunctioning of system S_2. We see here how the security mode of one system leads to different behavior of another system. In addition, the numerical solutions for the affine terms ξ_1, ξ_2 are illustrated in Figs. 6 and 7. These feedforward terms allow the system to

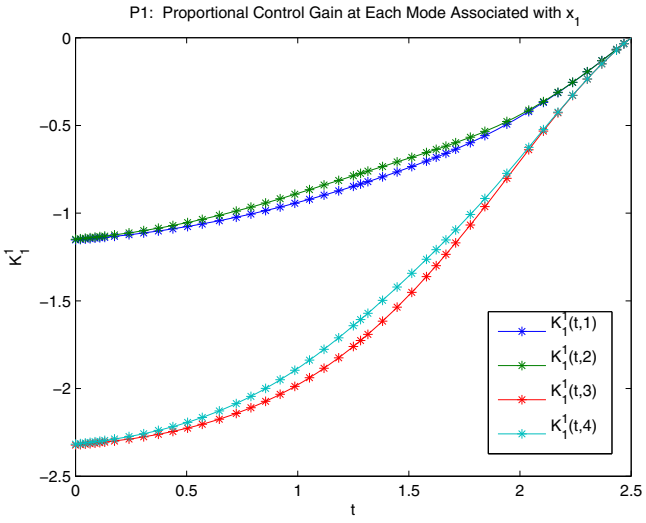

Fig. 4. Individual feedback control term of P_1 with respect to state x_1

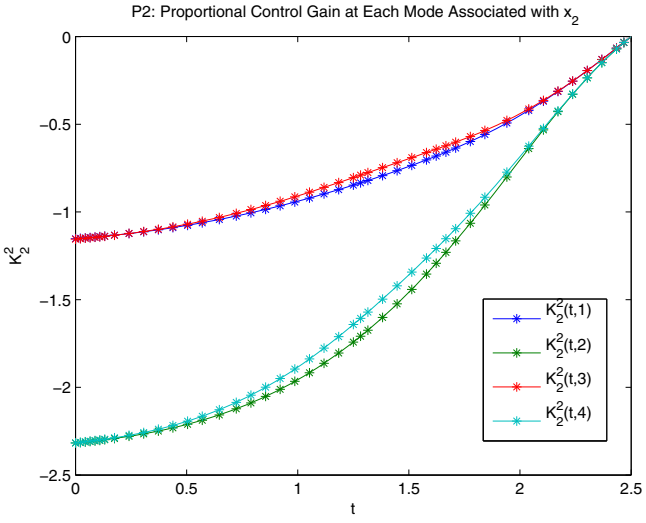

Fig. 5. Individual feedback control term of P_2 with respect to state x_2

track the desired trajectory. In Figs. 8 and 9, we show the sample state and mode trajectories. We see that the system mode eventually goes to the failure state θ_4. In Fig. 8, we observe that the malicious system S_2 first attracts S_1 for synchronization, and then misleads it to reach a value $\bar{x}_2 = 1$.

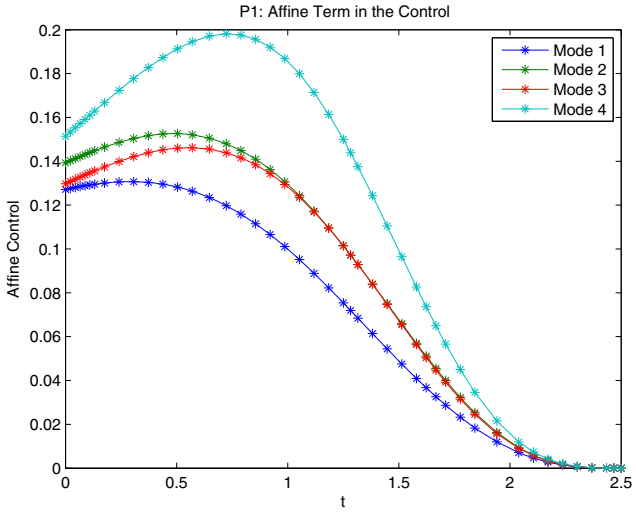

Fig. 6. Feedforward control term of P_1

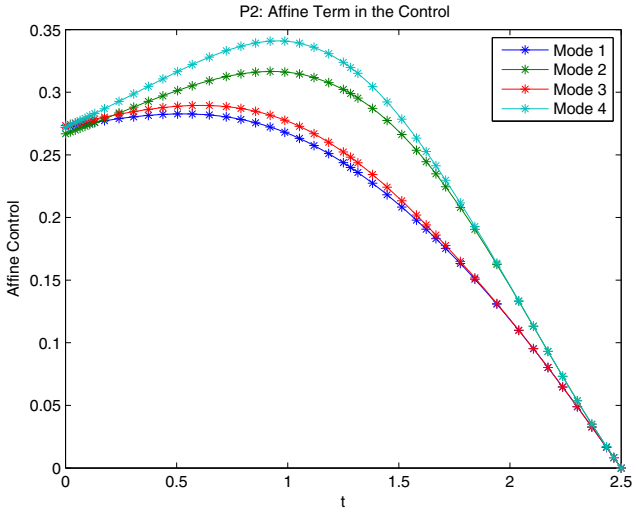

Fig. 7. Feedforward control term of P_2

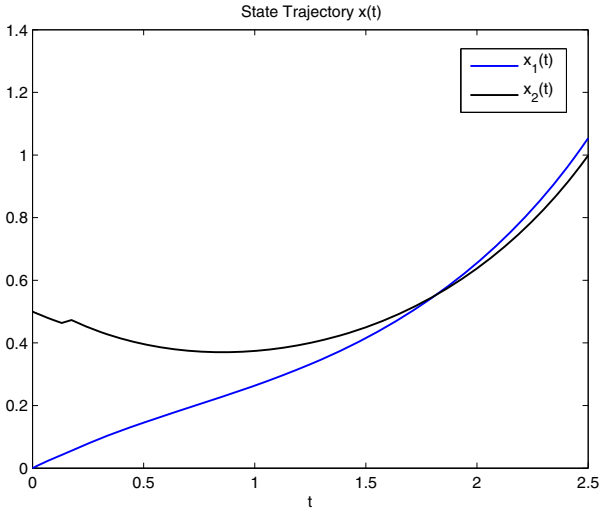

Fig. 8. Sample state trajectory

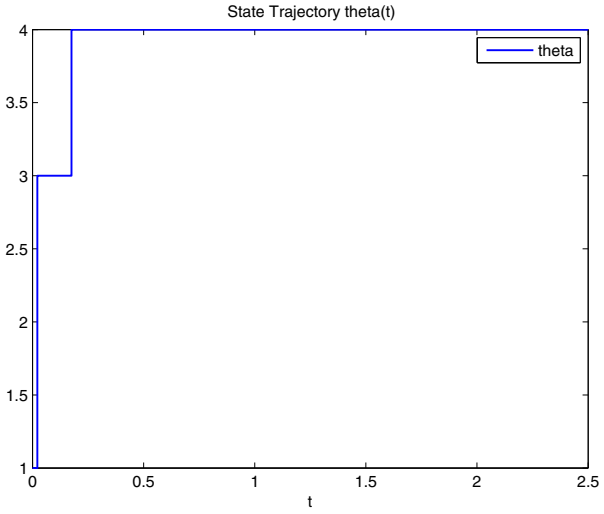

Fig. 9. Sample mode trajectory

6 Conclusion

Modern systems are increasingly complex due to cyber and physical system integrations as well as distributed interactions among different subsystems. This paper investigates resilient control design for multi-agent cyber-physical systems (CPSs). We have established a general system framework for describing the interactions between cyber and physical components within a CPS, as well as the interdependencies among multiple CPSs. We have focused on the physical layer control design and have studied a two-system problem with one malicious agent who intends to mislead and compromise the physical behaviors of the systems. We have designed distributed controllers based on feedback Nash equilibrium solutions. From the numerical example, we have observed that the performance of the systems are coupled at both physical and cyber layers. As for future work, we would extend this work to nonlinear and stochastic systems with additive noise. In addition, it would be interesting to study distributed cyber defense mechanisms based on this framework and employ tools from multi-resolution games to provide interface for cyber and physical decision problems in order to achieve required specifications for security and resilience.

References

1. Başar, T., Olsder, G.J.: Dynamic Noncooperative Game Theory. SIAM Series in Classics in Applied Mathematics (January 1999)
2. Alpcan, T., Başar, T.: Network Security: A Decision and Game Theoretic Approach. Cambridge University Press (January 2011)
3. Zhu, Q., Bushnell, L., Başar, T.: Game-theoretic analysis of node capture and cloning attack with multiple attackers in wireless sensor networks. In: Proc. 51st IEEE Conference on Decision and Control, CDC 2012, Maui, Hawaii, December 10-13 (2012)
4. Zhu, Q., Başar, T.: Robust and resilient control design for cyber-physical systems with an application to power systems. In: Proc. of 50th IEEE Conference on Decision and Control and European Control Conference (CDC/ECC), Orlando, Florida, December 12-15, pp. 4066–4071 (2011)
5. Zhu, Q., Başar, T.: A dynamic game-theoretic approach to resilient control system design for cascading failures. In: Proc. of International Conference on High Confidence Networked Systems (HiCoNS) at CPSWeek 2012, Beijing, China, pp. 41–46 (2012)
6. Başar, T., Bernhard, P.: H-infinity Optimal Control and Related Minimax Design Problems: A Dynamic Game Approach. Birkhäuser, Boston (August 1995)
7. Lye, K., Wing, J.M.: Game strategies in network security. International Journal of Information Security 4(1-2), 71–86 (2005)
8. Zhu, Q., Başar, T.: Dynamic policy-based IDS configuration. In: Proc. 48th IEEE Conference on Decision and Control, CDC 2009, Shanghai, China, December 16-18 (2009)
9. Zhu, Q., Başar, T.: Toward a theory of multi-resolution games. Submitted to SIAM Conference on Control and Its Applications (CT13)
10. Zhu, Q., Başar, T.: Multi-layer and multi-resolution large population stochastic games. In: 2012 SIAM Annual Meeting, Minneapolis, Minnesota, July 9-13 (2012)

11. Pan, Z., Başar, T.: H-infinity control of Markovian jump systems and solutions to associated piecewise-deterministic differential games. In: Olsder, G.J. (ed.) New Trends in Dynamic Games and Applications, pp. 61–94. Birkhäuser, Boston (1995)
12. Ji, Y., Chizeck, H.J.: Controllability, stabilizability, and continuous-time Markov jump linear quadratic control. IEEE Trans. on Automatic Control AC-35, 777–788 (1990)
13. Başar, T.: Minimax control of switching systems under sampling. Systems and Control Letters 25(5), 315–325 (1995)
14. Zhu, Q., Başar, T.: A hierarchical security architecture for smart grid. In: Hossain, E., Han, Z., Poor, H.V. (eds.) Smart Grid Communications and Networking. Cambridge University Press (2012)
15. Manshaei, M.H., Zhu, Q., Alpcan, T., Başar, T., Hubaux, J.-P.: Game theory meets network security and privacy. ACM Computing Survey 45(3) (2013, to appear)
16. Zhu, Q., Tembine, H., Başar, T.: Network security configuration: A nonzero-sum stochastic game approach. In: Proc. 2010 American Control Conference (ACC 2010), Baltimore, Maryland, June 30-July 2, pp. 1059–1064 (2010)
17. Kunreuther, H., Heal, G.: Interdependent security. Journal of Risk and Uncertainty 26(2), 231–249 (2003)
18. Liacco, T.D.: The adaptive reliability control system. IEEE Trans. on Power Apparatus & Systems PAS-86(5), 517–523 (1967)
19. Falliere, N., Murchu, L.O., Chien, E.: W32. Stuxnet Dossier. Symantec Reports (February 2011)
20. Başar, T., Haurie, A.: Feedback equilibria in differential games with structural and modal uncertainties. In: Cruz Jr., J.B. (ed.) Advances in Large Scale Systems, vol. 1, pp. 163–201. JAI Press Inc., Connecticut (1984)