Fifty-first Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
October 2 - 3, 2013

Networked Cyber-Physical Systems: Interdependence, Resilience and Information Exchange

Quanyan Zhu and Linda Bushnell

Abstract— **Ubiquitous in modern critical infrastructure, networked cyber-physical systems (CPSs) are a collection of task-oriented systems whose cyber and physical resources are conjoined and coordinated to achieve unprecedented capabilities. In this paper, we study how physically independent systems can be made interdependent in the CPS context. In order to understand such interdependencies, we establish a system framework to investigate the effect of cyber coupling on physical control systems. In particular, we study the optimal control of networked control system jointly with power control problems in wireless communication networks. We show that the information exchange between cyber and physical layers not only makes the control system more efficient but also enhances its resilience to adversarial behaviors. In addition, as a result of interdependencies, a jamming attack on one CPS can benefit the performance of the other CPS. We use a two-CPS case study to demonstrate performance of the coupled system at both the physical and cyber layers.**

I. Introduction

Modern systems are increasingly complex due to cyber and physical system integrations as well as distributed interactions among different subsystems. This class of systems is often called cyber-physical systems (CPSs), where the integration of and coordination between cyber and physical resources yield unprecedented capabilities that empower the next generation smart grid, intelligent transportation systems, and medical tele-operations. The complexity of CPS grows as a collection of task-oriented systems pool their resources and capabilities together to create a networked system which offers more functionality and performance than simply the sum of the constituent systems. We call systems of this type networked CPSs or systems of systems. A CPS network is a cyber-physical multi-agent system often seen in swarm robots, unmanned vehicles in battlefields, and power grids. The agents within the network can be interconnected physically with sensors and actuators, or coupled through the communication networks at the cyber layer of the system.

This paper aims to study the interdependence of networked CPS agents, and pinpoint the fact that two physically independent systems can become strongly coupled in the CPS context. In order to elucidate this point, we establish a system framework and specifically investigate the power control issue for the wireless communication network, and the optimal control problem of networked control systems over unreliable communication links subject to packet losses. Due to the decentralized and heterogeneous nature of multi-agent systems, we use a game-theoretic approach to design a decentralized power control algorithm that enables the transmitters to adjusts their power levels based on the signal-to-interference-and-noise ratio (SINR) of their receiver to achieve the best achievable channel quality. The optimal control of the physical layer control system relies on the knowledge of the packet drop rate, determined by the SINR of the link, which inadvertently relies on the power control scheme at the cyber layer of the system.

Traditional control design for networked control systems takes as given the network system parameters, such as the packet loss rate and time delay. The joint design of control algorithms at both cyber and physical layers of the system, however, becomes essential for CPSs, and the control performance improves as the control system can acquire real-time information from the cyber protocol. In this paper, we show that the information exchange between the cyber and physical layers not only makes the control system more efficient but also enhances its resilience to adversarial behaviors. In addition to the algorithmic design for networked CPSs, we also provide insights into some interesting phenomena as the result of cyber coupling between CPS agents. We observe that a jamming attack on one CPS can benefit the performance of the other CPSs, and the power control algorithms provide inherent resilience, which allows the CPS to recover quickly from jamming attacks.

A. Related Work

Control-theoretic and game-theoretic methods have been used for power control problems in the literature of wireless and optical communications, [1]–[4]. In [5], a hybrid technique that combines centralized optimization and game-theoretic methods is used to provide service differentiation for different channels. In addition, control of systems under unreliable communication links has also been widely studied, as in [6], [7].

Recent years have witnessed a burgeoning literature on the control for cyber-physical systems, [8]. The integration between cyber system models and control system models is recently investigated in [9]–[11] for quantifying the tradeoff between resilience and robustness using game-theoretic approaches. In [12], passivity and dissipativity methods have been used for compositional design of large-scale CPSs. In [13], L_1 adaptive control is integrated with a switching controller to form L1Simplex architecture for addressing the software failure in CPSs.

Quanyan Zhu is with the Department of Electrical Engineering, Princeton University, Princeton, NJ, USA and is supported in part by NSERC Postdoctoral Fellowship (PDF). E-mail: quanyanz@princeton.edu. Linda Bushnell is with the Department of Electrical Engineering, University of Washington, Seattle, WA, USA. E-mail: lb2@uw.edu.

978-1-4799-3410-2/13/$31.00 ©2013 IEEE

B. Paper Organization

The rest of the paper is organized as follows: Section II presents the system framework with a specific focus on the cyber layer power control game model in Subsection II-A and the physical layer optimal control of networked control system over unreliable communication links in Subsection II-B. In Section III, we use a two-CPS network as a case study to investigate the interdependencies with the CPS network and its resilience against jamming attacks. We conclude the paper in Section IV.

II. System Model

A cyber-physical system (CPS) is an integrated system consisting of a physical subsystem that implements the system's functionality and a cyber subsystem that enables data communications and provides applications and services for the physical components of the system. A networked CPS is composed of multiple CPSs whose cyber or physical systems interact with each other. For notational convenience, we let the networked CPS denoted by S, which comprises a set of N CPSs $\mathcal{S} = \{S_1, S_2, \cdots, S_N\}$. A system S_i is composed of a physical subsystem P_i and cyber system C_i, $i = 1, 2, \cdots, N$. Hence, the physical layer of S is denoted by the set $\mathcal{P} := \{P_1, P_2, \cdots, P_N\}$, and its cyber counterpart is denoted as $\mathcal{C} := \{C_1, C_2, \cdots, C_N\}$. The interactions within S can be found between components within and across $\mathcal{C}$ and $\mathcal{P}$. The system performance of independent physical components of the system can be made interdependent through its cyber interactions, and vice versa. We use Fig. 1 as an example to illustrate the scenario where two CPSs S_1 and S_2 interact with each other through the coupling between their cyber components C_1 and C_2. The physical components P_1 and P_2 are often designed independently without taking into account the coupling at the cyber layer of the system. Hence, it is interesting to raise the following question: *How does the coupling affect the system performances of P_1 and P_2 and the efficiency of the entire system?*

In this paper, we study this issue by establishing an integrated theoretical framework for a specific class of CPSs where its physical infrastructure consists of a control system, supported by wireless communications. In particular, we consider the scenario where C_i, $i = 1, 2, \cdots, N$, seeks to perform power control to achieve the best Signal to Noise and Interference Ratio (SINR) for communications between sensors, remote controllers and the plant, while at the physical layer, P_i $i = 1, 2, \cdots, N$ optimally regulates the control system over unreliable communication channels. The scenario is motivated by an electronic warfare system in which the operation of networked heterogeneous agents on a battlefield, such as unmanned ground vehicles (UGV), unmanned aerial vehicles (UAVs), convoys, and a tactical operations center, heavily rely on wireless communication systems that are vulnerable to intentional and unintentional interference between legitimate agents and malicious jammers. The control of physical agents and the management of communication systems need to be performed at the same time to ensure the reliability and security of entire battlefield system.

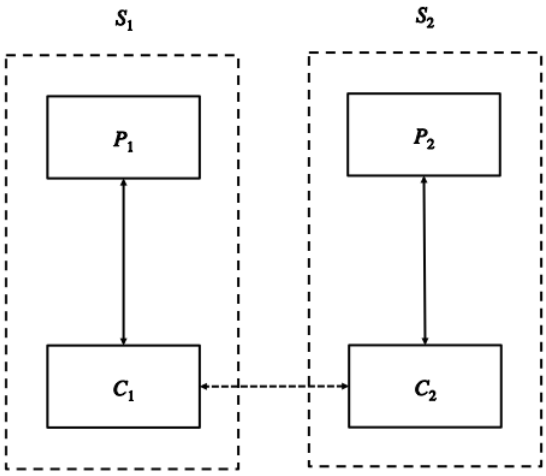

Fig. 1. Interactions between two CPSs S_1 and S_2: The physical layer of the system is $\mathcal{P} = \{P_1, P_2\}$ and the cyber layer of the system is $\mathcal{C} = \{C_1, C_2\}$. The coupling between C_1 and C_2 affects the performances of independently designed P_1 and P_2.

Fig. 2 illustrates a two-UAV scenario, where two UAVs are remotely controlled by two independent operators by sending control and command messages through a wireless network using power levels p_1 and p_2. The communication between C_1 and P_1 interferes with the communication between C_2 and P_2. To address this issue, the following two subsections are organized as follows: In Subsection II-A, we introduce a game-theoretic model for distributed power control for heterogeneous CPS networks. In Subsection II-B, we present the optimal control of LTI systems subject to packet loss over communication links. Since the power levels used in the wireless network determine the packet drop rate, it is natural to integrate the two models and study the performance interdependencies between distributed agents in a networked CPS.

A. Decentralized Power Control

Power management is an essential component to achieve effective wireless communications in the presence of interference and noise. Consider the cyber layer $\mathcal{C}$ of a CPS network, where $C_i, i = 1, 2, \cdots, N$, is equipped with two transmitters s_i^1, s_i^2 and two receivers r_i^1, r_i^2. They form two communication links (s_i^1, r_i^1) and (s_i^2, r_i^2). The link (s_i^1, r_i^1) sends the measurement data from the transmitter s_i^1 on the sensor of the physical system P_i to the receiver r_i^1 on its controller. The link (s_i^2, r_i^2) sends the control signal from the transmitter s_i^2 on the controller to the receiver r_i^2 on the actuator of the plant of P_i. We consider Raleigh-fading channels for the signal propagation. Let $p_i^k \in [0, p_{i,\max}^k]$, $i = 1, 2, \cdots, N, k = 1, 2$, be the transmission power of s_i^k, where $p_{i,\max}^k$ is an upper bound imposed by physical limitation of the transmitter. Let $h_{i,j}^{k,l} \in \mathbb{R}_+$ and $f_{i,j}^{k,l} \in \mathbb{R}_+$ be the slow-varying channel gain and the fast time-scale Rayleigh fading between transmitter

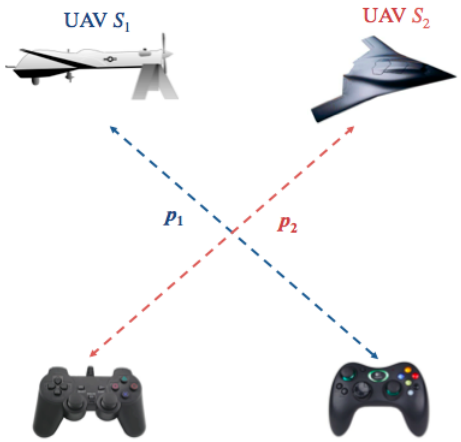

Fig. 2. Operation of two UAV systems as a motivating example: Two UAVs are remotely controlled by two independent operators. The inferences between two communication links, with power levels p_1 and p_2, affect the control performance of the two UAVs.

s_i^k and receiver r_j^l, respectively, $i,j = 1,2,\cdots,N$ and $k,l = 1,2$. The SINR obtained at receiver r_i^k is affected by other transmitters in the neighborhood and background noise. We let $\mathcal{N}_i$ denote the set of CPS systems in the neighborhood of S_i whose communication systems interfere with C_i, and σ_i^k the variance of the background noise. Thus, in accordance with the interference model considered, the SINR at the receiver r_i^k is given by

$$\gamma_i^k = \frac{Lh_{j,i}^{l,k} f_{j,i}^{l,k} p_i^k}{\sum_{j\in\mathcal{N}_i}\sum_{k=1}^{2} h_{j,i}^{l,k} f_{j,i}^{l,k} p_j^l + (\sigma_i^k)^2}, \tag{1}$$

where $L := W/R > 1$ is the spreading gain; W is the chip rate, and R is the data rate of each transmitter. Note that as defined in (1), the two communication channels of C_i can interfere with each other. The goal of power control in wireless networks is to find optimal power levels p_i^k that yield the best SINRs at r_i^k. It is natural for us to adopt a game-theoretic framework for power control in CPS networks, since a CPS network can comprise of a diverse number of devices or agents that are designed and manufactured by different sources, and the coordination between a large number of them can be a daunting task.

Each link engages in its own power management to maximize its payoff function $J_i^k := U_i^k - W_i^k$, where U_i^k and W_i^k are the utility function and cost function for the communication link (s_i^k, r_i^k), respectively. Denote the power vector $\mathbf{p} = \{p_i^k, i = 1,2,\cdots,N, k = 1,2\} \in \mathbb{R}_+^{2N}$, and let $\mathbf{p}_{-i}^{-k} = \{p_j^l, j \neq i, j = 1,2,\cdots,N, l = 1,2\} \cup \{p_i^l, l \neq k\}$ be the set of power levels other than p_i^k. We define a linear pricing function $W_i^k := \omega_i^k p_i^k$, where $\omega_i^k \in \mathbb{R}$ is the unit cost on the power, and a utility function U_i^k that reflects the channel's preference for maximizing γ_i^k, given by

$$U_i^k(p_i^k, \mathbf{p}_{-i}^{-k}) = \ln\left(1 + a_i^k \tilde{\gamma}_i^k\right).$$

Here, a_i^k is a positive parameter, and

$$\tilde{\gamma}_i^k = \frac{Lh_{j,i}^{l,k} f_{j,i}^{l,k} p_i^k}{\sum_{(k,l)\in\mathcal{M}_i^k} h_{j,i}^{l,k} f_{j,i}^{l,k} p_j^l + (\sigma_i^k)^2},$$

where $\mathcal{M}_i^k$ is the index set of interfering channels given by

$$\mathcal{M}_i^k := \{(j,l) : j \in \mathcal{N}_i,\ l = 1,2\}\backslash\{(i,k)\}.$$

It is easy to verify that $\tilde{\gamma}_i^k = \frac{\gamma_i^k}{L-\gamma_i^k}$. In the noncooperative power control game, each link maximizes the following payoff function

$$\max_{p_i^k \in [0, p_{i,\max}^k]} J_i^k(p_i^k, \mathbf{p}_{-i}^{-k}) := \ln\left(1 + a_i^k \tilde{\gamma}_i^k\right) - \omega_i^k p_i^k \tag{2}$$

for $i = 1,2,\cdots,N, k = 1,2$.

The Nash equilibrium (NE) is an equilibrium solution concept for the continuous-kernel $2N$-person noncooperative game described in (2), which is defined as follows:

Definition 1 ([14]). *A strategy profile $(\bar{\mathbf{p}})$ is a Nash equilibrium (NE) of the noncooperative game with payoff function J_i^k defined in (2) if for every $i = 1,2,\cdots,N, k = 1,2$,*

$$J_i^k(\bar{\mathbf{p}}) \geq J_i^k(p_i^k, \bar{\mathbf{p}}_{-i}^{-k}), \quad p_i^k \in [0, p_{i,\max}^k].$$

Proposition 1. *Let the maximization problem in (2) yields an inner solution for all values of $\mathbf{p}_{-i}^{-k}$. Then, the $2N$-player game problem described by (2) admits a unique Nash equilibrium $\bar{\mathbf{p}}$ if for all $i = 1,2,\cdots,N$, $k = 1,2$, a_i^k are selected such that*

$$\frac{1}{Lh_{i,i}^{k,k} f_{i,i}^{k,k}} \sum_{(k,l)\in\mathcal{M}_i^k} h_{j,i}^{l,k} f_{j,i}^{l,k} < a_i^k. \tag{3}$$

□

Sketch of the proof. Due to the concavity of J_i^k in p_i^k, a unique best-response function can be obtained for each (i,k). Finding the fixed point of $2N$ best-response functions, under the assumptions above, leads to solving a linear system of equations. Using strict diagonal dominance ensures the existence and uniqueness of the NE. □

Based on the NE solution, a distributed best-response algorithm can be implemented to adjust power levels online. Consider the following discrete time iterative dynamics:

$$p_i^k(t+1) = \frac{1}{\omega_i^k} - \frac{1}{a_i^k}\left(\frac{1}{\gamma_i^k(t)} - \frac{1}{L}\right) p_i^k(t), \quad i = 1,2,\cdots,N; k = 1,2, \tag{4}$$

where $p_i^k(t), \gamma_i^k(t)$ are the transmitting power levels at s_i^k and the SINR at r_i^k at time step $t \in \mathbb{N}_+$, respectively. The algorithm adjusts the power level based on the measured SINR level at each step.

Proposition 2. *Let the assumptions in Proposition 1 hold and (3) hold. Then, the distributed algorithm in (4) converges to the unique NE.* □

Proof. The result follows from the fact that the map $\mathbf{\Pi}$ such that $\mathbf{p}(t+1) := \mathbf{\Pi}\mathbf{p}(t)$ is contractive under the assumptions made above. □

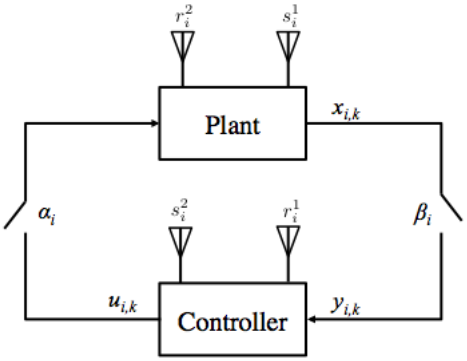

Fig. 3. System model for CPS S_i: The physical system P_i is described by a feedback control system, and the cyber system is described by two communication links: (s_i^1, r_i^1) between the plant sensor and the controller, and (s_i^2, r_i^2) between the controller and the plant actuator. The plant is controlled over unreliable communication links with packet loss rates β_i, α_i for the two links, respectively. The power levels of the wireless system are also controlled to achieve best possible SINR in the presence of intentional and unintentional interferences.

B. Optimal Control over Unreliable Communication Links

The physical layer of the CPS network can be modeled by a networked control system as illustrated in Fig. 3, where the links connecting the sensor to the controller, and the controller to the actuator are prone to failure. We use the following discrete-time linear time-invariant (LTI) dynamics to describe the physical plant P_i for $i = 1, 2, \cdots, N$:

$$x_{i,t+1} = A_i x_{i,t} + \alpha_{i,t} B_i u_{i,t} + w_{i,t}, \quad (5)$$

$$y_{i,t} = \beta_{i,t} x_{i,t}, \quad t = 0, 1, \cdots \quad (6)$$

where $x_{i,t} \in \mathbb{R}^n$ is the state of P_i; $x_{i,0} \in \mathbb{R}^n$ is the initial state with probability distribution P_{x_0}; $u_{i,t} \in \mathbb{R}^m$ is the control input of P_i; and $w_{i,t} \in \mathbb{R}^n$ is the additive disturbances on the system, which are independent zero-mean second-order random vectors. The stochastic processes $\{\alpha_{i,t}\}_{t\in\mathbb{N}_+}$ and $\{\beta_{i,t}\}_{t\in\mathbb{N}_+}$ model the link failures from the controller to the actuator (C-A), and from the sensors to the controller (S-C), respectively. We let $\{\alpha_{i,t}\}_{t\in\mathbb{N}_+}$ and $\{\beta_{i,t}\}_{t\in\mathbb{N}_+}$ be i.i.d. Bernoulli process independent of the process $\{w_{i,t}\}_{t\in\mathbb{N}_+}$, with

$$\mathbb{P}[\alpha_{i,t} = 0] = 1 - \bar{\alpha}_{i,t}, \quad \mathbb{P}[\alpha_{i,t} = 1] = \bar{\alpha}_{i,t}, \quad (7)$$

$$\mathbb{P}[\beta_{i,t} = 0] = 1 - \bar{\beta}_{i,t}, \quad \mathbb{P}[\beta_{i,t} = 1] = \bar{\beta}_{i,t}, \quad (8)$$

where $\bar{\alpha}_{i,t}, \bar{\beta}_{i,t} \in [0, 1]$ are probabilities of successful transmission of the C-A and S-C links, respectively. As illustrated in Fig. 3, $\alpha_{i,t} = 0$ when the C-A link fails, i.e., the control packet is lost and $\alpha_{i,t} = 1$, otherwise. Similarly, $\beta_{i,t} = 0$ when the S-C fails, i.e., the measurement data is lost and $\beta_{i,t} = 1$, otherwise.

The power control in wireless networks affects the reliability of communication links. The probability of successful transmission of S-C link (s_i^1, r_i^1) and C-A link (s_i^2, r_i^2) for Rayleigh fading channels depends on the SINR level γ_i^k and a target SINR level $\bar{\gamma}_i^k$ [15]. They can be approximated by

$$\bar{\beta}_{i,t} = e^{-\frac{\bar{\gamma}_i^1}{\gamma_i^1(t)}}, \quad \bar{\alpha}_{i,t} = e^{-\frac{\bar{\gamma}_i^2}{\gamma_i^2(t)}}. \quad (9)$$

The optimal control of LTI systems over unreliable communications links has been studied in [7] for TCP and UDP networks. Here we summarize the result presented in [7] for finite horizon optimal control over TCP networks, where acknowledgement packets are generated by the receivers to signal the successful receipt of packets. Let $I_{i,t}$ denote the information available to the controller at time t. For TCP networks,

$$I_{i,t}^{\text{TCP}} = \{y_{i,0}, \cdots, y_{i,t}\ ; u_{i,0}, \cdots, u_{i,t-1}\ ; \beta_{i,0}, \cdots, \beta_{i,t}\ ; \alpha_{i,0}, \cdots, \alpha_{i,t}\}, \quad t = 1, 2, \cdots$$

$$I_{i,0}^{\text{TCP}} = \{y_{i,0}, \beta_{i,0}\}.$$

We consider the class of policies consisting of a sequence of functions $\pi_i = \{\mu_{i,0}, \mu_{i,1}, \cdots, \mu_{i,T-1}\}$, where T is the decision horizon, and $\mu_{i,t} : I_{i,t}^{\text{TCP}} \to \mathbb{R}^m$ yields control actions $u_{i,t} = \mu_{i,t}(I_{i,t}^{\text{TCP}})$. The goal of optimal control over TPC networks is to find an admissible policy that minimize the quadratic cost function

$$J_i^P = \mathbb{E}\left\{ x_{i,T}' F_i x_{i,T} + \sum_{t=1}^{T-1} x_{i,t}' Q_i x_{i,t} + \alpha_{i,t} u_{i,t}' R_i u_{i,t} \right\}, \quad (10)$$

subject to (5) and (6). Here $R_i > 0, Q_i \geq 0, F_i \geq 0$ with appropriate dimensions. The following result can be found in [7].

Proposition 3 ([7])**.** *For the optimal control problem (10) subject to dynamics (5) and (6) and $t \in [0, T]$, the optimal policy is*

$$u_{i,t}^* = G_{i,t} \hat{x}_{i,t}, \quad (11)$$

where $\hat{x}_{i,t}$ is the estimator of the state described by

$$\hat{x}_{i,t} = \begin{cases} A_i \hat{x}_{i,t-1} + \alpha_{i,t-1} B_i u_{i,t-1}, & \beta_{i,t} = 0, \\ x_{i,t}, & \beta_{i,t} = 1. \end{cases} \quad (12)$$

with initial condition

$$\hat{x}_{i,0} = \begin{cases} \mathbb{E}_{P_{x_0}}[x_0], & \beta_{i,t} = 0, \\ x_{i,0}, & \beta_{i,t} = 1. \end{cases}, \quad (13)$$

and the matrix G_k is given by

$$G_{i,t} = -(R_i + B_i' K_{i,t+1} B_i)^{-1} B_i' K_{i,t+1} A_i, \quad (14)$$

with matrices $K_{i,t}$ given recursively by the Riccati equation

$$P_{i,t} = (1 - \bar{\alpha}_{i,t}) A_i' K_{i,t+1} B_i (R_i + B_i' K_{i,t+1} B_i)^{-1} * B_i' K_{i,t+1} A_i,$$

$$K_{i,t} = A_i' K_{i,t+1} A_i - P_{i,t} + Q,$$

with terminal condition $K_{i,T} = F_i, P_{i,T} = 0$. □

Since there is no measurement noise in (6), the separation principle between estimation and control holds, and (12) yields the optimal estimator $\hat{x}_{i,t}$. Hence, optimal total cost achieved by the control (11) is $\hat{x}_{i,0}' K_{i,T} \hat{x}_{i,0}$ which is only dependent on the packet loss rate on C-A link $\bar{\alpha}_{i,t}$.

The optimal control obtained in (11), (12), (13), and (14) depends on the knowledge of $\bar{\alpha}_{i,t}, \bar{\beta}_{i,t}$. With the power control model described in Subsection II-A, the probability

of packet loss can be analytically expressed using (9), which is determined by the power levels used for the S-C and C-A links. The control algorithm (11) can be coupled with the power control algorithm (4) to study the interdependencies of agents within a networked CPS. The coupled algorithm is a forward and backward system where finding optimal control requires solving Riccatti equations backwards in time, while the update of power levels is made forward in time.

III. Case Study: Remote Control of Two Agents

In this section, we illustrate the interdependencies of a networked CPS using numerical examples. In order to implement the coupled system in practice, we consider two scenarios: (i) One is time scale separation where the power control cyber dynamics are faster than the physical system dynamics so that the optimal control can be found at NE $\bar{\mathbf{p}}$; (ii) Another scenario is to consider an infinite horizon control problem as in Theorem 3 of [7] so that the controller gain can be obtain by solving an algebraic Riccatti equation.

We consider two identical, unstable, scalar, open-loop systems for P_1 and P_2 as in [7]:

$$x_{i,t+1} = 2x_{i,t} + \alpha_{i,t}u_{i,t} + w_{i,t}, \quad i = 1, 2, \tag{15}$$

where $A_i = 2, B_i = 1$, $x_{i,t} \in \mathbb{R}$, and $\alpha_{i,t}$ are the packet loss rates between the controller and the actuator of system S_i. Let the noise process, $\{w_{i,t}\}$, be zero-mean with variance $\sigma_w^2 = 1$. The initial state $x_{i,0}$ is also zero-mean with variance $\sigma_{x_{i,0}}^2 = 1$. With $Q_i = R_i = 1$, the optimal control for infinite horizon case under TCP information structure is given by

$$u_{i,t}^* = -G_i x_{i,t}, \tag{16}$$

where the controller gain

$$G_i = -\frac{2K_i}{1 + K_i}, \quad K_i = \frac{2 + \sqrt{4\bar{\alpha}_i + 1}}{4\bar{\alpha}_i - 3}.$$

P_1 and P_2 are remotely controlled by two independent operators who send command and control messages using wireless communications. Note that there is no coupling between the two systems at the physical layer of the CPS network, i.e., the control objectives of P_1 and P_2 are independent of each other. The interference between two C-A communication links, however, affects the SINRs of two physically independent systems, and hence leads to the coupling of two CPS systems. We let the channel gain of the receiver r_i^k be determined by the Rayleigh fast-fading and log-normal shadowing path loss model, given by

$$h_{i,j}^{k,l} = (0.1/d_{i,j})^{\frac{1}{4}} \cdot Y_\sigma^{-1} \cdot f_{i,j}^{k,l},$$

where $d_{i,j}^{k,l}$ denotes the distance between the transmitter s_i^k and the receiver $r_{i,j}^{k,l}$; $\log(Y_\sigma)$ is a zero-mean Gaussian random variable with a standard deviation of $\sigma = 0.1$; and $f_{i,j}^{k,l}$ is a random variable with Rayleigh distribution which models the fast-fading channel. We assume that S-C channels (s_i^1, r_i^1) and C-A channels (s_i^2, r_i^2) use different frequency bands and do not interfere with each other. Interference occurs, however, between S-C links and between C-A links. The system parameters are chosen as $L = 128$, $\sigma_i^k = 0.1$, for all $i = 1, 2, \cdots, N$, and $k = 1, 2$. As illustrated in Fig. 2, we set the distance between the controller and the actuator of S_1 and S_2 to be $d_{1,1} = d_{2,2} = 100$ m. The distance between the controller of S_1 and the actuator of S_2 and the one between the controller of S_2 and the actuator of S_1 to be $d_{12} = d_{21} = 80$ m.

Algorithm 1 : Online Optimal Control of Networked Cyber-Physical Systems

1: Initialize the system parameters $x_{i,0}, p_i^k(0), a_i^k, \omega_i^k$ of S_i for $i = 1, 2$
2: For each time step $t = 1, 2, \cdots$
3: s_i^2 uses (4) to update $p_i^k(t)$ based on SINR $\gamma_i^2(t)$
4: P_i computes packet drop rates (7), (8)
5: P_i uses the real-time packet drop rates and $I_{i,t}^{\text{TCP}}$ to find
optimal control (16) and sends the control signal to r_i^2
6: r_i^2 sends the acknowledgement to s_i^2
7: r_i^2 measures the SINR value γ_i^2 and sends to s_i^2
8: s_i^1 sends the state measurement to r_i^1
9: Return to step 3

In the first numerical experiment, the decentralized power control algorithm adaptively chooses the optimal power level in response to to the measured SINR level. We set the initial power level as 10 mW for each link, $p_{i,\max}^k = 50$ mW, $\bar{\gamma}_i^k = 7$ dB. We simulate the coupled dynamics of the decentralized control algorithm (4) and the system dynamics (15) under optimal control (16). The details of the algorithm are described in Algorithm 1. In Figs. 4 and 5, we present the SINR and the power level of each C-A communication link over time, respectively. It can be seen that the channel quality of S_1 is better than the one of S_2, and hence S_1 has a lower probability of packet drop. Within 40 iterations, the decentralized algorithm yields the NE of the power control game at the steady state. In Fig. 6, the system states x_1 an x_2 evolve according the dynamics (15) under the optimal control (16) with the parameter $\bar{\alpha}_i$ obtained using SINR in Fig. 4 at each time step. It can be seen that at the NE of the game, S_2 experiences more spikes in its controlled dynamics as it suffers a higher loss rate of C-A signal. We also found that when no control inputs are applied to the plant, the state of uncontrolled system dynamics blows up exponentially. We observe that S_1 experiences a spike at $t = 10$ due to relative low SINR when power levels are adjusted online.

In the second numerical experiment, we introduce a jammer who attacks the communication channels of S_1 and S_2. To study the effect of jamming on the networked CPS, we let the adversary jam S_1 from $t = 60$ to $t = 70$ and S_2 from $t = 120$ to $t = 130$. In Figs. 7 and 8, we show the SINR and the power levels of two C-A channels, respectively. It can be seen that when the jammer attacks S_1, SINR of S_1 degrades 2 dB, while the S_2 benefits from the jamming and improves its SINR by 0.5 dB. This phenomenon occurs due to the fact that the jammer reduces the interference of S_1 on S_2 by

attacking S_1. A similar situation occurs when S_2 is jammed, which leads to a roughly 4 dB degradation for S_2 but 2 dB improvement for S_1. We observe that the power control algorithm provides some degree of resilience to the CPS network. The channels tend to restore their performances once being attacked, and the channel qualities are recovered once the jammer disappears. Eventually, the steady state of the power control algorithm is reached which corresponds to the NE of the two-person noncooperative game. In Fig. 9, we show the evolution of system states under the jamming attacks. We observe that on average, S_2 has has a smaller number of spikes due to the fact that the channel quality of S_2 is better than the one of S_1. The attack on S_1 leads to two spikes of x_1 for the period between $t = 60$ and $t = 70$.

From these experiments, we can see that the two physically independent systems S_1 and S_2 become strongly coupled in the CPS network. The coupling at the cyber communication layer plays a significant role in the physical layer control system. The optimal control over unreliable links requires the parameter knowledge of packet drop rates. These parameters can be learned and assessed online based on the channel quality parameters at the cyber layer. In the case of a jamming attack, we observe an interesting phenomena where one system's "meat" is another channel's "poison", i.e., one system can benefit from other system's attack. This lesson allows us to design deceptive CPSs that are capable of proactive defense of critical infrastructures against known or unknown attacks.

In addition, we also observe that the information exchange of SINR between the cyber and physical layers as depicted in Algorithm 1 is critical for the CPS to defend against jamming attacks. Without the real-time knowledge of SINR, the physical layer computes its optimal control (16) at the predetermined packet loss rate. In this case, the control fails to respond to an increased packet loss rate, which can lead to instability of the control system. On the contrary, when the controller adapts its control signal when jamming occurs, the system becomes more resilient to the attack even though it suffers a temporary loss of performance and incurs a higher cost on control.

IV. Conclusion and Future Work

In this paper, we have studied a network of cyber-physical systems (CPSs) and the interdependency between CPSs. The performances of physically independent networked control system become heavily coupled due to the interference in the wireless communication network that delivers sensor data and control signals between the plants and the controllers. This phenomenon informs us that it is essential to move from the classical design of networked control system to a new paradigm of co-design between cyber and physical layers of the CPS. The former aims at designing control systems with given parameters of packet loss and time delay, while the later aims at the joint design of communication network and control system, and enables information exchange between control and communication layers of the system. As we have observed in the case study, this approach allows the CPS to respond more quickly to the change of system parameters and become more resilient to adversarial behaviors.

Specifically, we have studied the coupling between the cyber layer power control and the physical layer optimal control of the networked control system. Due to the heterogeneity of agents and complexity of the CPS, we have introduced a decentralized power control algorithm that allows the transmitters at the sensors and the controllers to adjust their power levels in real-time according to SINR levels at the receiver. A game-theoretic approach was used to model the independent decision-making at each transmitters, and the designed distributed algorithm was shown to converge to the Nash equilibrium of the noncooperative power control game. The optimal control over the unreliable communication links is coupled with the power control algorithm through the real-time packet drop rates. We have observed that the interferences caused between two CPSs account for the interdependencies between the two systems. We have also seen that with the presence of an adversary, one system can benefit from the other system's loss. This insight provides us theoretical basis for designing proactive and adaptive defense in the regime of cyber-physical systems as future work.

References

[1] T. Alpcan, T. Başar, R. Srikant, and E. Altman, "CDMA uplink power control as a noncooperative game," *Wireless Networks*, vol. 8, pp. 659-670, 2002.

[2] T. Alpcan, T. Başar, and S. Dey, "A power control game based on outage probabilities for multicell wireless data networks," *IEEE Transactions on Wireless Communications*, vol. 5, no. 4, pp. 890-899, April 2006.

[3] Q. Zhu and L. Pavel, "State-space approach to pricing design in OSNR Nash game," in *Proc. of the IFAC World Congress*, pp. 12001-12006, July 2008.

[4] S. Kandukuri and S. Boyd, "Optimal power control in interference-limited fading wireless channels with outage-probability specifications," *IEEE Transactions on Wireless Communications*, vol. 1, no. 1, pp. 46-55, Jan. 2002.

[5] Q. Zhu and L. Pavel, "Enabling differentiated services using generalized power control model in optical networks," *IEEE Transactions on Communications*, vol. 57, no. 9, pp. 2570-2575, Sept. 2009.

[6] S. Yüksel and T. Başar, *Stochastic Networked Control Systems: Stabilization and Optimization under Information Constraints*, Systems & Control: Foundations and Applications Series, Birkhäuser, Boston, MA, June 2013.

[7] O. C. Imer, S. Yüksel, and T. Başar, "Optimal control of LTI systems over unreliable communication links," *Automatica*, vol. 42, no. 9, pp. 1429-1440, Sept. 2006.

[8] D. C. Tarraf (Editor), *Control of Cyber-Physical Systems: Workshop Held at The Johns Hopkins University, March 2013*, Lecture Notes in Control and Information Sciences (LNCIS), vol. 449, March 2013.

[9] Q. Zhu, L. Bushnell, and T. Başar, "Resilient distributed control of multi-agent cyber-physical systems," *Proc. of the Annual Conference on Information Sciences and Systems (CISS) Workshop on Control of Cyber-Physical Systems*, LNCIS 449, pp. 301 - 316, March 2013.

[10] Q. Zhu and T. Başar, "A dynamic game-theoretic approach to resilient control system design for cascading failures," *Proc. of the 1st Conference on High Confidence Networked Systems (HiCoNS), part of CPSWeek 2012*, pp. 41-46, April 2012.

[11] Q. Zhu and T. Başar, "Toward robust and resilient control design for cyber-physical systems with an application to power systems," *Proc. of the 50th IEEE Conference on Decision and Control and European Control Conference* (CDC/ECC), pp. 4066-4072, Dec. 2011.

[12] P. J. Antsaklis, B. Goodwine, V. Gupta, M. J. McCourt, Y. Wang, P. Wu, M. Xia, H. Yu, and F. Zhu, "Control of cyberphysical systems using passivity and dissipativity based methods", *European Journal of Control*, vol. 19, no. 5, pp. 379-388, Sept. 2013.

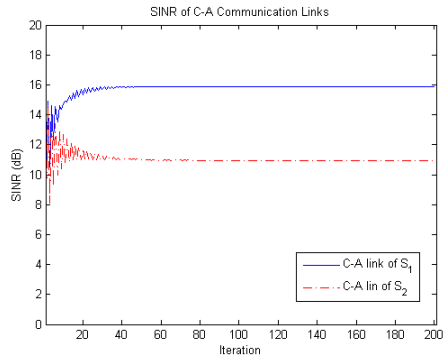

Fig. 4. Evolution of SINR of C-C-A communication links of S_1 (solid blue) and S_2 (dotted red): S_1 has a higher SINR than S_2 at the equilibrium, and hence S_1 yields a lower packet loss rate for the control messages.

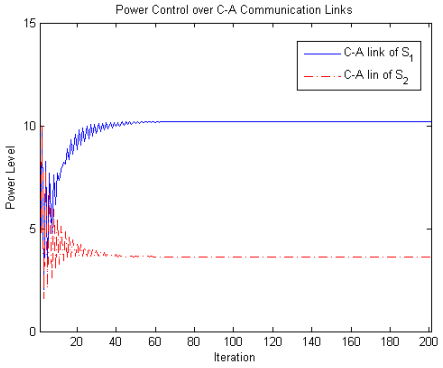

Fig. 5. The power levels over C-A communication links evolve under decentralized power control algorithms: The steady-state power levels are 10.5 and 4.05, respectively, for S_1 and S_2, corresponding to a Nash equilibrium of the power control game.

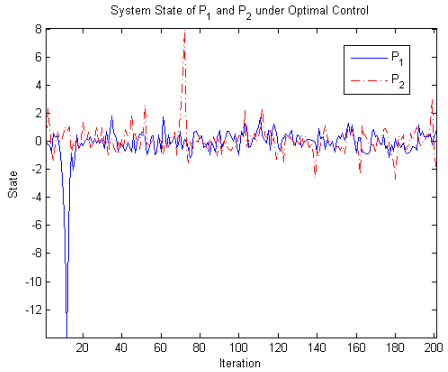

Fig. 6. Evolution of the system states $x_{1,t}$ and $x_{2,t}$ under optimal control over unreliable communication links: S_2 experiences more spikes than S_1 due to its low SINR at the equilibrium; S_1 starts with a low SINR, and hence experiences a higher rate of packet loss, resulting in a spike at $t = 10$.

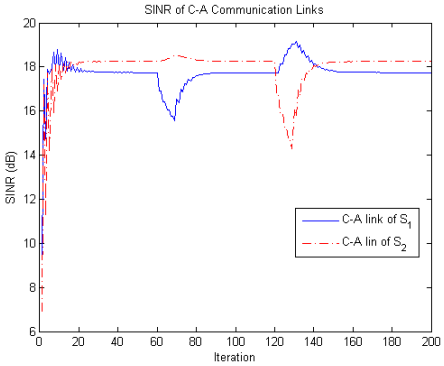

Fig. 7. Evolution of SINR of C-A communication links of S_1 (solid blue) and S_2 (dotted red) under jamming attacks: The jammer attacks S_1 from $t = 60$ to $t = 70$ and S_2 from $t = 120$ to $t = 130$. The channel qualities degrade and then reach steady states of 17.8dB and 18.1dB for S_1 and S_2, respectively.

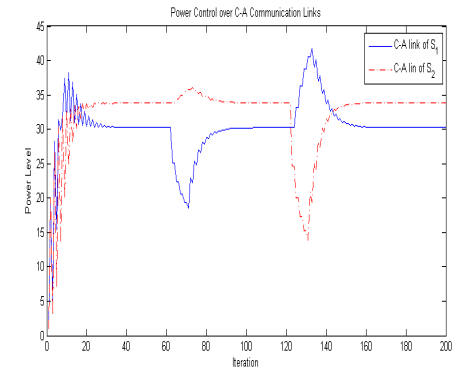

Fig. 8. The power levels over C-A communication links evolve over time under jamming attacks: The jammer attacks S_1 from $t = 60$ to $t = 70$ and S_2 from $t = 120$ to $t = 130$. The equilibrium power levels are 30.5 and 33.8 for S_1 (solid blue) and S_2 (dotted red), respectively.

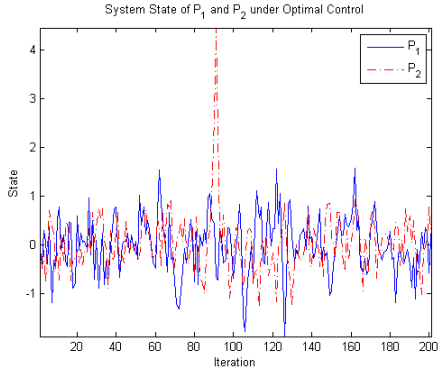

Fig. 9. Evolution of the system states $x_{1,t}$ and $x_{2,t}$ under optimal control over insecure communication links: S_1 has a lower SINR and hence a higher packet loss rate at the steady-state of power control.

[13] X. Wang, N. Hovakimyan, and L. Sha, "L1Simplex: fault-tolerant control of cyber-physical systems," In *Proc. of the ACM/IEEE 4th International Conference on Cyber-Physical Systems (ICCPS), part of CPSWeek 2013*, pp. 41-50, April 2013.

[14] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, SIAM Series in Classics in Applied Mathematics, Jan. 1999.

[15] J. Proakis, *Digital Communications*, McGraw-Hill, 4th edition, Aug. 2000.

[16] R. Poovendran, "Cyber-Physical Systems: Close Encounters Between Two Parallel Worlds [Point of View]," *Proceedings of the IEEE*, vol. 98, no. 8, pp.1363-1366, Aug. 2010.

[17] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*, Cambridge University Press, 2005.