Resilient Control of Cyber-Physical Systems against Denial-of-Service Attacks

Yuan Yuan, Quanyan Zhu, Fuchun Sun, Qinyi Wang and Tamer Başar

Abstract— **The integration of control systems with modern information technologies has posed potential security threats for critical infrastructures. The communication channels of the control system are vulnerable to malicious jamming and Denial-of-Service (DoS) attacks, which lead to severe time-delays and degradation of control performances. In this paper, we design resilient controllers for cyber-physical control systems under DoS attacks. We establish a coupled design framework which incorporates the cyber configuration policy of Intrusion Detection Systems (IDSs) and the robust control of dynamical system. We propose design algorithms based on value iteration methods and linear matrix inequalities for computing the optimal cyber security policy and control laws. We illustrate the design principle with an example from power systems. The results are corroborated by numerical examples and simulations.**

I. Introduction

Recent years have witnessed the migration from proprietary standards for communications towards open international standards for modern critical infrastructures. However, it is difficult to update software and hardware applications for legacy control systems. Malicious attackers, on the other hand, can easily launch an attack since the amount of knowledge needed to successfully execute an attack is decreasing. As a consequence, many incidents related to damages of cyber attacks on Industrial Control Systems (ICSs) have already been reported in [1]. In [2], the traffic air control system tower at Worchester Regional Airport (MA) USA was shut down by hacker. In [3], it has been reported that the power grid in the U.S. was penetrated by cyber spies and some key infrastructure was compromised by the intrusion. It is also reported in [3] that the Siemens Supervisory Control And Data Acquisition (SCADA) systems have been attacked by computer worm, Stuxnet. ICSs are widely used in electric, water, oil and gas industries and they are critical to the operation of the U.S. critical infrastructures. The aforementioned attacks have incurred environment and financial losses. The information technologies employed in ICSs are vastly vulnerable and have a direct effect on the physical component of the system. Hence it is essential to take into account cyber security when designing ICSs.

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. Y. Yuan and F. Sun are with Department of Computer Science and Technology, Tsinghua University, Beijing, P.R. China 100084, Email: yuanyuan@illinois.edu and fcsun@mail.tsinghua.edu.cn; Q. Zhu and T. Başar are affiliated with the Coordinated Science Laboratory and the Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, 1308. W. Main St., Urbana, IL, email:{zhu31, basar1}@illinois.edu; Q. Wang is with State Key Laboratory of Software Development Environment, Beihang University, Beijing, P.R. China 100191, Email:wqy901018@163.com.

The critical issues of cyber security in ICSs give rise to a new class of control problems which require a holistic and cross-layer design approach for controller designs of integrated cyber-physical systems. Recently, the concept of resilient control has been proposed in [4] and [5], emphasizing the controller design in an adversarial cyber environment. A resilient control system aims to maintain an acceptable level of operational normalcy in response to both the disturbance from the physical environment and malicious adversary from the cyber environment. Hence resilience represents the ability of the system to defend against adversaries and recover from cyber attacks in addition to being reliable and robust to disturbances. Design of such systems requires a system perspective towards cyber-physical systems against threats and malicious behavior. [6] discusses the state awareness of ICSs under attacks and provides some future research directions. In [7], an Adaptive Neural Control (ANC) architecture is used for control within a resilient control framework. The parameters of the attacked plant change and are controlled to match the reference model. A passivity combined with adaptive sampling approach to design a control architecture is proposed in [8], and the method shows certain robustness to network uncertainties. However, little effort has been made to consider the integrated design of defense mechanisms in the cyber layer and controller design in the physical layer. There is a need for new methodologies and principles for integrated design since the cyber systems of the ICSs are not isolated from the physical systems for defense against malicious adversaries in practical situations.

In this paper, we use dynamical systems to capture the physical layer of the system, and focus on Intrusion Detection Systems (IDSs) at the cyber layer of the system for defense against malicious behavior. IDSs are often used to detect and raise alarms for cyber attacks such as the Denial of Service (DoS) attack, which can cause delays and congestions in the communication channel. For ICSs equipped with IDSs, the integrated design involves both IDSs configuration and controller design. In [9] and [10], the authors have addressed this issue by proposing a coupled optimality criteria for designing resilient control systems. The cyber state and controlled plant are modeled as a coupled continuous Markov process and the controllers are designed via an iterative method. In this article, we consider a specific cyber defense mechanism, DoS attack, and study its impact on ICSs.

A. Attacks on ICSs

According to [1], attacks on the ICSs can be summarized in Fig. 1. A_3 and A_5 represent deception attacks, where the

978-1-4799-0503-4/13/$31.00 ©2013 IEEE

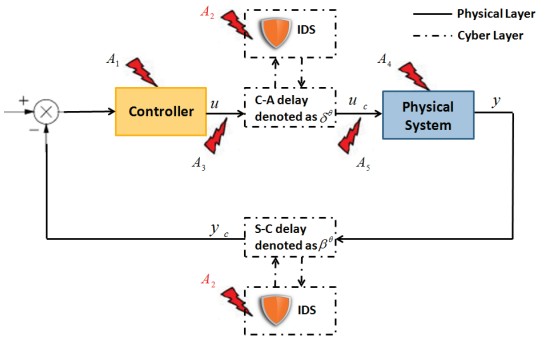


Fig. 1. The control system can be subject to many attacks. They can be on the controller, the plant and the communication networks. The IDSs are used for defending the networked control system.

false information $\tilde{y} \neq y$ and $\tilde{u} \neq u$ are sent from sensors and controllers. A_1 and A_4 represent direct attacks against the actuators or the plant. A_2 is the DoS attack, where the controller is prevented from receiving sensor measurement and actuator from receiving control signals. Note that DoS attacks are most commonly used by the adversary which involve jamming the communication channels, compromising devices and attacking the routing protocols, etc. We will restrict our attention to DoS attacks in this article, leaving the deception attacks to a future study. Since IDSs is often designed to detect unauthorized uses of networks [12], we will use IDSs configuration as the defense mechanism.

B. Contributions

In this paper, we propose a methodology to co-design the IDSs configuration policy at the cyber layer and the controller at the physical layer. The contributions are summarized as follows:

1) We use a discrete-time hybrid system model to study the effect of the IDSs cyber security policies on the control system under DoS attacks.
2) We use a stochastic game to capture interactions between the IDSs and the adversary. We find the optimal configuration of IDSs by taking into account its impact on the underlying control performance.
3) We couple the design at cyber and physical layers of the system and propose a co-design algorithm based on value iteration and linear matrix inequalities (LMIs) to compute the H^∞ optimal control for physical dynamical system and the optimal IDSs configuration policy.
4) The interdependencies of the cyber system and the underlying physical layer control system is studied.

C. Organizations

The rest of the paper is organized as follows. We first describe the system framework in Section II-A and then establish a game-theoretic model for studying defense mechanism against DoS attacks in Section II-B. In Section II-C, H^∞ optimal control problem is formulated and addressed. A co-design algorithm is proposed in Section II-D. In Section III, the method proposed is applied to the control of a power

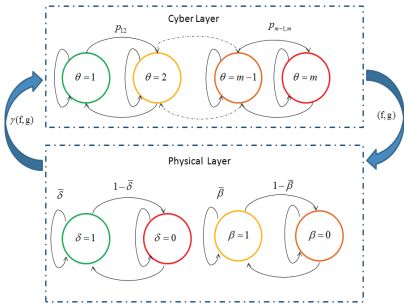


Fig. 2. The system framework contains two decision problems. (i) The decision problem at the cyber layer is a competitive Markov decision problem, capturing the interactions between an attacker and a defender whose actions $(\mathbf{f}, \mathbf{g})$ affect the cyber state θ and the transition probabilities. (ii) The decision problem at the physical layer is to design an optimal controller of a dynamical system with S-C delay δ^θ and C-A delay β^θ for achieving control performance γ^θ. The two decision problems are interleaved and coupled.

system and the results are corroborated by numerical simulations. In Section IV, conclusions are drawn and directions for future study are identified.

Notation: The standard notation is used throughout this paper. For a matrix M, $M > 0$ ($M < 0$) means that M is positive definite (negative definite). M^T stands for the transpose of M. The element in the ith row and jth column of matrix M is denoted as $[M]_{ij}$. we use $*$ as an ellipsis for the terms that are introduced by symmetry. $l_2[0,\infty)$ is the space of square-integrable vector functions over $[0,\infty)$.

II. Resilient and H^∞ Optimal Control

In this section, we consider the problem where the adversary launches DoS attacks on a networked control system. A hybrid discrete-time dynamical system model is established consisting of IDSs at the cyber layer and the underlying physical layer dynamical system. Fig. 2 illustrates the interplay between cyber and physical layers of the system. A Markov chain is used to capture the dynamics of the cyber state, while the physical layer dynamics under DoS attacks are captured by a discrete-time model with sensor-to-controller (S-C) and controller-to-actuator (C-A) delays, which are distributed according to a Bernouli Distribution. The configuration policies against the attacker at the cyber layer affect the control system through S-C and C-A delays. In addition, the control system performance under best-effort controller at the physical layer needs to be taken into account when designing a configuration policy. The resilient control design involves the co-design of the cyber configuration policy as well as the optimal controller for the physical dynamical system.

A. System Framework

This subsection provides the system framework of resilient control. The controlled plant under DoS attacks is described by the model as follows.

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

where $x_k \in \mathbb{R}^n$ and $u_{c,k} \in \mathbb{R}^m$ are 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

$$\begin{cases} y_k = Cx_k, \\ y_{c,k} = (1-\delta^\theta)y_k + \delta^\theta y_{k-1}, \end{cases} \tag{2}$$

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

$$\begin{aligned} &\bar{\delta}^\theta := \Pr\{\delta^\theta = 1\} = E\{\delta^\theta\}, \\ &\Pr\{\delta^\theta = 0\} = 1 - E\{\delta^\theta\} = 1 - \bar{\delta}^\theta \end{aligned} \tag{3}$$

In this paper, we propose an observer-based control strategy described by

$$\begin{cases} \hat{x}_{k+1} = A\hat{x}_k + B_2 u_{c,k} + L^\theta(y_{c,k} - \bar{y}_{c,k}), \\ \bar{y}_{c,k} = (1-\bar{\delta}^\theta)C\hat{x} + \bar{\delta}^\theta C\hat{x}_{k-1}, \end{cases} \tag{4}$$

$$\begin{cases} u_k = K^\theta \hat{x}_k, \\ u_{c,k} = (1-\beta^\theta)u_k + \beta^\theta u_{k-1}, \end{cases} \tag{5}$$

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. $K \in \mathbb{R}^{m\times n}$ and $L \in \mathbb{R}^{n\times p}$ denote the controller gains and observer gains which 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 S-C delay is described by the situation that $\delta^\theta = 1$ and the C-A delay is described by $\beta^\theta = 1$. In the sequel, the optimal strategy designed in different layers will be shown and the coupled design for the holistic hybrid model will be presented at the end.

B. Optimal Defense Mechanism

Since IDSs are designed to detect unauthorized uses of systems and networks, we use them to defend the networked control system. In practice, IDSs are deployed at different levels to monitor the traffic of applications and networks, that is, the IDSs is configured with different security enforcement. In this paper, we use the IDSs configuration to represent the cyber defense strategy.

An attacker launches its attack from his attack space $\mathcal{A} := \{a_1, a_2, \cdots, a_M\}$. The set $\mathcal{L} := \{L_1, L_2, \cdots, L_N\}$ denotes the defense library and $\bar{\mathcal{L}}$ denotes the set of all possible sets of $\mathcal{L}$, with cardinality $|\bar{\mathcal{L}}| = 2^N$. Let $F_i \in \bar{\mathcal{L}}, i \in \{1, 2, \cdots, 2^N\}$ be a configuration set of all libraries. As shown in Fig. 3, we need different configurations of libraries to detect different attacks. Stationary mixed strategy is used in which $f(\theta, F_i)$ and $g(\theta, a_j)$ are the probabilities of the detector and attacker choosing actions $F_i \in \bar{\mathcal{L}}$ and $a_j \in \mathcal{A}$, respectively. We denote $f(\theta, F_i)$ and $g(\theta, a_j)$ as $f_i(\theta)$ and $g_j(\theta)$. Note that $f_i(\theta)$ and $g_j(\theta))$ are functions of the random jump process $\{\theta_n\}$. $\{\theta_n\}$ is a finite state discrete Markov jump process, that is, θ takes discrete values in a given finite set $\Theta := \{\theta_1, \theta_2, \cdots, \theta_s\}$. Functions $f_i : \Theta \longrightarrow [0,1], i \in \{1, 2, \cdots, 2^N\}$ and $g_j : \Theta \longrightarrow [0,1], j \in \{1, 2, \cdots, M\}$, need to satisfy $\sum_{i=1}^{2^N} f_i(\theta) = 1$ and $\sum_{j=1}^{M} g_j(\theta) = 1$. The cyber system switches among different states and the transition

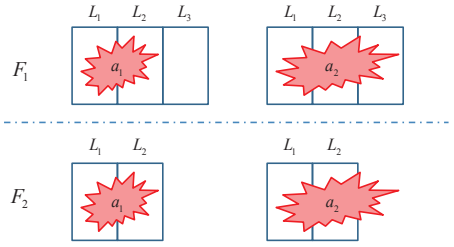


Fig. 3. An example to illustrate the necessity of different IDSs configurations: Library configurations F_1 and F_2 are used to detect different attacks a_1 and a_2; F_2 outperforms F_1 for detecting a_1 since F_1 uses more libraries than F_2 does, and degrades the system performance. However, F_1 can detect a_2 better than F_2 does, since a_2 is not fully detectable by F_2.

probabilities $\mathbb{P}(\theta'(n+1)\,|\theta(n), a_j, F_i),\ \theta'(n+1), \theta(n) \in \Theta$ are dependent on the defense mechanism and attack strategy and

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

Function $r : \Theta \times \mathcal{A} \times \bar{\mathcal{L}} \longrightarrow \mathbb{R}$ defines the cost of the possible action pair (F_i, a_j) for a certain cyber state θ. The defender can be seen as the minimizer, who minimizes the cost function $r(\theta, F_i, a_j)$, and the attacker can be seen as the maximizer, who maximizes the cost function, Assuming that the game between the attacker and the defender is zero-sum, we have the relation

$$\begin{aligned} r(\theta, F_i, a_j) &= r^a(\theta, F_i, a_j) \\ &= -r^l(\theta, F_i, a_j). \end{aligned} \tag{6}$$

We augment the distribution vectors over all the cyber states Θ and have

$$\begin{aligned} \mathbf{f}(\theta) &:= [f_1(\theta), \cdots, f_{2^N}(\theta)]^T, \\ \mathbf{g}(\theta) &:= [g_1(\theta), \cdots, g_M(\theta)]^T, \\ \mathbf{F}_s &:= [\mathbf{f}(\theta_1), \cdots, \mathbf{f}(\theta_s)]^T \in \mathbf{F}, \\ \mathbf{G}_s &:= [\mathbf{g}(\theta_1), \cdots, \mathbf{g}(\theta_s)]^T \in \mathbf{G}, \\ \theta \in \Theta &:= \{\theta_1, \theta_2, \cdots \theta_s\}. \end{aligned}$$

$v_\beta : \Theta \times \mathbf{F} \times \mathbf{G} \longrightarrow \mathbb{R}$ is the β-discounted payoff if

$$v_\beta = \sum\nolimits_{n=0}^{\infty} \beta^n E^{\mathbf{f}(\theta), \mathbf{g}(\theta)} r(\theta, F_i, a_j),$$

where $\beta \in (0,1)$ is a discount factor.

Remark 1: Note that the distribution of stochastic variables δ^θ and β^θ, which reflect the Quality-of-Service (QoS) of the communication network, is actually dependent on the attack and defense mechanism in the cyber layer. Let us define four mappings $H_1 : \Theta \times \mathbf{F} \times \mathbf{G} \to \mathbb{R}$, $W_1 : \Theta \times \mathbf{F} \times \mathbf{G} \to \mathbb{R}$, $H_2 : \Theta \times \bar{\mathcal{L}} \times \mathcal{A} \to \mathbb{R}$ and $W_2 : \Theta \times \bar{\mathcal{L}} \times \mathcal{A} \to \mathbb{R}$. $\bar{\delta}^\theta$ and $\bar{\beta}^\theta$can be seen as the result of these mappings;

$$\begin{aligned} \bar{\delta}^\theta &:= H_1(\theta, \mathbf{f}(\theta), \mathbf{g}(\theta)) = \ \mathbf{f}(\theta)^T H(\theta)\ \mathbf{g}(\theta), \\ \bar{\beta}^\theta &:= W_1(\theta, \mathbf{f}(\theta), \mathbf{g}(\theta)) = \ \mathbf{f}(\theta)^T W(\theta)\ \mathbf{g}(\theta), \end{aligned}$$

where $[H(\theta)]_{ij} = H_2(\theta, F_i, a_j)$ and $[W(\theta)]_{ij} = W_2(\theta, F_i, a_j)$.
The following definition captures the characterization of the optimal defense mechanism.

Definition 1: (Saddle-Point Equilibrium) Let

$$\mathbf{v}_\beta = [v_\beta(\theta_1), \cdots, v_\beta(\theta_s)]^T,$$

A pair $(\mathbf{F}_s^*, \mathbf{G}_s^*)$ is a saddle-point of the β-discounted game if

$$\mathbf{v}_\beta(\mathbf{F}_s^*, \mathbf{G}_s) \leq \mathbf{v}_\beta(\mathbf{F}_s^*, \mathbf{G}_s^*) \leq \mathbf{v}_\beta(\mathbf{F}_s, \mathbf{G}_s^*), \tag{7}$$

in which $\mathbf{F}_s^*, \mathbf{G}_s^*$ are the saddle-point equilibrium defense and attack strategies.

The algorithm to find the optimal defence mechanism $\boldsymbol{F}_s^*$ iteratively is presented in the following theorem.

Theorem 1: The discounted zero-sum stochastic game possesses a value $\mathbf{v}_\beta$ for $\forall F_i \in \bar{\mathcal{L}},\ a_j \in \mathcal{A}$, which is the unique solution of equations

$$v_\beta^{N+1}(\theta) = \mathbf{val}\{R(\theta)\}, \tag{8}$$

$$[R(\theta)]_{ij} = r(\theta, F_i, a_j) + \beta \sum_{\theta' \in \Theta} \mathbb{P}(\theta' \,|\theta, F_i, a_j)\, v_\beta^N(\theta')]. \tag{9}$$

where **val** is a function that yields the game value of a zero-sum matrix game. Then, we can obtain the saddle-point equilibrium strategies to achieve the value with

$$(\mathbf{f}^*(\theta), \mathbf{g}^*(\theta)) \in \mathbf{arg\ val}\{R(\theta)\},$$

where **arg val** yields the mixed strategies that yield the value of the game.

C. H^∞ Optimal Control

Dynamic system model described by (1)-(5) is a hybrid discrete model which has been investigated earlier in [11]. We extend the idea and propose H^∞ index for the discrete hybrid model which is the expectation over $\mathbf{f}(\theta)$ and $\mathbf{g}(\theta)$ for a given θ. If the initial condition is zero, the H^∞ index γ_θ satisfies

$$E^{\,\mathbf{f}(\theta),\,\mathbf{g}(\theta)} \left\{ \sum_{k=0}^{\infty} \{\|z_k\|^2\} \right\} < \gamma_\theta^2 \sum_{k=0}^{\infty} \{\|\omega_k\|^2\} \tag{10}$$

for all $\theta \in \Theta$. The theorem below indicates how to convert the conditions satisfying H^∞ index into linear matrix inequalities (LMIs) which are easy to calculate using available tools.

Theorem 2: Given scalars $\gamma_\theta > 0$ and the strategy pair $(\mathbf{f}(\theta),\ \mathbf{g}(\theta))$ or all $\theta \in \Theta$. The hybrid model described by (1)-(5) 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 $P_2^\theta \in \mathbb{R}^{n\times n}$ 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 the following LMIs hold, where

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

and $U_1 \in \mathcal{R}^{m\times n}$ and $U_2 \in \mathcal{R}^{(n-m)\times n}$ satisfies

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

and $\sigma_i (i = 1, 2, \cdots, m)$ are eignvalues of B_2. The controller gain and observer gain are given by:

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

$$\Pi^\theta = \begin{bmatrix} \Pi_{11}^\theta & * \\ \Pi_{21}^\theta & \Pi_{22}^\theta \end{bmatrix} < 0, \tag{12}$$

where

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

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

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

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

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

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

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

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

Proof: The proof follows the steps described in [11] and hence is omitted here due to page limitation. ■

Note that the LMIs in Theorem 2 lead to the convex optimization problem as follows:

$$\begin{aligned} \hat{\gamma}_\theta := \min_{\substack{P_{11}>0, P_{22}>0, P_2>0 \\ S_1>0, S_2>0, M, \bar{M}}} \quad & \gamma_\theta \\ \text{subject to} \quad & (12) \end{aligned} \tag{13}$$

Since γ_θ is influenced by the cyber state and strategy, it is actually dependent on the triple $(\theta,\ \mathbf{f}(\theta),\ \mathbf{g}(\theta))$. Let us define two mappings $C_1 : \Theta \times \mathbf{F} \times \mathbf{G} \to \mathcal{R}$ and $C_2 : \Theta \times \bar{\mathcal{L}} \times \mathcal{A} \to \mathcal{R}$. $\hat{\gamma}_\theta$ can be seen as the value of the mapping:

$$\hat{\gamma}_\theta = C_1(\theta, \mathbf{f}(\theta), \mathbf{g}(\theta)) = \ \mathbf{f}(\theta)^T C(\theta)\ \mathbf{g}(\theta),$$

where $[C(\theta)]_{ij} = C_2(\theta, F_i, a_j)$. Since the design in the physical layer and cyber layer have been specified, respectively. the co-design procedure will be discussed in the next section.

D. Coupled Design

In this subsection, we provide a cross layer design based on the previous results to demonstrate how to design the resilient controller using a holistic view. The main problem we address is formulated as below:

Problem 1: The resilient control of the cyber-physical system against the DoS attack is to find a set of control and observer gains K^θ and L^θ in (4) and (5) satisfying H^∞

optimal performance $\hat{\gamma}_\theta$, and the optimal cyber policy $\mathbf{F}_s^*$ and $\mathbf{G}_s^*$.

The coupled design here means that, on the one hand, cyber defense mechanism takes into account the H^∞ index, in which $r(\theta, F_i, a_j) = C_2(\theta, F_i, a_j)$. On the other hand, the H^∞ optimal controller is designed with $\bar{\delta}^\theta = \mathbf{f}^*(\theta)^T H(\theta)\ \mathbf{g}(\theta)^*$ and $\bar{\beta}^\theta = \mathbf{f}^*(\theta)^T W(\theta)\ \mathbf{g}(\theta)^*$. We propose the following algorithm for the coupled design. Note

Algorithm 1 Algorithm for Coupled Design

Given: $H_2(\theta, F_i, a_j)$ and $W_2(\theta, F_i, a_j)$ for all $\theta \in \Theta, F_i \in \bar{\mathcal{L}}, a_j \in \mathcal{A}$,

Output: K^θ and L^θ for all $\theta \in \Theta$; $\mathbf{F}_s^*$ and $\mathbf{G}_s^*$.

1) **Initialization**:
2) Initialize v_β^0 and $\beta = 0.5$.
3) **Iterative update**:
4) **while** $(\mathbf{v}_\beta^{h+1} - \mathbf{v}_\beta^h > [\varepsilon, \varepsilon, \cdots, \varepsilon]')$ **do**
5) Solve the convex optimization problem (13) and obtain $C_2(\theta, F_i, a_j)$ to establish $r(\theta, F_i, a_j) = C_2(\theta, F_i, a_j)$.
6) Calculate the cost matrix $R(\theta)$ using (9)
7) Find $v_\beta^{h+1}(\theta)$ using the following LMIs

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

8) **end while**
9) Obtain $\mathbf{F}_s^*$ using $\mathbf{f}^*(\theta) = \tilde{y} v_\beta(\theta)$ and solve the dual problem of (LMG), which can be found in [14] 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

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

that the proposed algorithm above involves a value iteration method for computing the stationary mixed saddle-point equilibrium for the stochastic game, in which a linear program (LMG) is solved at each step. "LMG" stands for linear program for matrix games. The mixed Nash equilibrium of a matrix game is computed by solving a linear program (LMG). The algorithm also invokes the computational tools for solving a set of LMIs for obtaining H^∞ robust controller in the form of (4) and (5) that achieve optimal control system performances.

III. Numerical Simulation

In this section, we investigate the resilient control problem associated with the uninterrupted power system (UPS). UPS usually provides uninterrupted, high quality and reliable power for vital loads, such as life supporting system, data storage systems or emergency equipment. Thus, the resilience and robustness of the UPS is essential. We perform an integrated design of the optimal defense mechanism for IDSs and the optimal control strategy for PWM inverter such that the output AC voltage can maintain desired setting under the influence of DoS attacks. The discrete-time model at half-load operating point can be found in [11]:

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

For the cyber layer, two states are considered: a normal state θ_1 and a compromised state θ_2. We use library l_1 to detect a_1 and use l_2 to detect a_2. Suppose that the system can only load one library at a time. We provide the following tables with elements to be the action pairs ($H_2(\theta, F_i, a_j)$,$W_2(\theta, F_i, a_j)$). At θ_1, we have

	a_1	a_2
F_1	(0.01,0.01)	(0.05,0.05)
F_2	(0.03,0.03)	(0.01,0.01)

and the transition probabilities are

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

At state θ_2, we have

	a_1	a_2
F_1	(0.06,0.06)	(0.1,0.1)
F_2	(0.08,0.08)	(0.06,0.06)

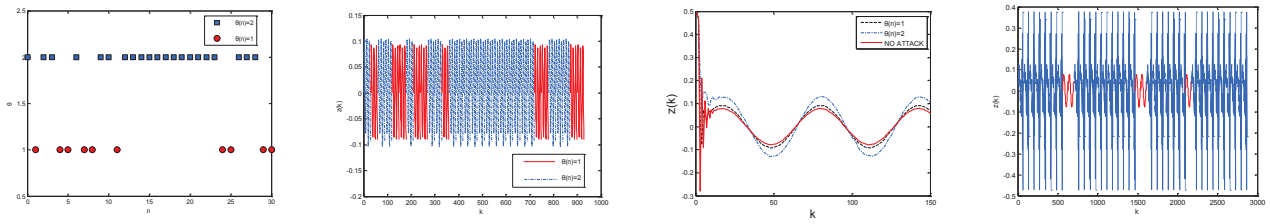
and the transition probabilities are the same as in θ_1. Then, using Theorem 1, we have the cost/reward table for state θ_1,

	a_1	a_2
F_1	0.0994	0.1641
F_2	0.1232	0.0994

and for state θ_2,

	a_1	a_2
F_1	0.1961	0.8084
F_2	0.3148	0.1961

respectively. Using Algorithm 1, we obtain the game values at states θ_1 and θ_2 to be $\mathbf{v}_{0.5} = [0.3370 \quad 0.5299]^T$ 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 $\mathbf{g}^*(\theta_2) = [0.7671\ 0.2329]^T$. In Fig. 4, we show the cyber states and physical system performance when an attacker launches an attack a_1. Fig. 4(a) shows cyber state of the system under the saddle-point configuration policy. Fig. 4(b) shows the steady-state performance of the dynamical system under co-designed controller when it switches between two cyber states. Fig. 4(c) shows the H^∞ control result under different cyber states, and Fig. 4(d) shows the performance under an H_∞ robust controller without considering cyber-layer of the system. Comparing Fig. 4(d) with Fig. 4 (b),



(a) (b) (c) (d)

Fig. 4. Control performance under resilient control against DoS attack: Fig. 4(a) shows cyber state of the system under the saddle-point configuration policy. Fig. 4(b) shows the steady-state performance of the dynamical system under co-designed controller when it switches between two cyber states. Fig. 4(c) shows the H^∞ control result under different cyber states, and Fig. 4(d) shows the performance under an H_∞ robust controller without considering cyber-layer of the system.

we can see that the H_∞ performance in Fig. 4(b) is much better than the one in Fig. 4(d), and the system in Fig. 4(d) is more vulnerable to attacks and moves to the compromised state more frequently.

IV. Conclusion

Industrial control systems in many critical infrastructures are subject to malicious cyber attacks. The goal of resilient control system is to protect the system from such attacks and maintain an acceptable level of operation in the face of cyber attacks and uncertainties. In this paper, we have proposed a methodology to design the IDSs configuration policy at the cyber-layer and the controller for the physical layer dynamical system. We have used a co-design algorithm based on value iterations and LMIs to compute the H^∞ optimal control and the cyber security policy. Using numerical examples, we have shown that the design methodology yield a controller that outperforms the H^∞ controller without taking cyber defense into account. The paper has focused on the denial-of-service attacks and their impact on the cyber security policies and performance of the dynamical system. As future work, we can consider different cyber attack models and study more sophisticated defense strategies. In addition, H^∞ control problem can also be viewed as a game problem between disturbances and controller [14]. By adopting a game-theoretic perspective, we will employ the concepts and tools from our recent initiative on multi-resolution and multi-layer games.

References

[1] R. A. Kisner, "Cybersecurity through Real-Time Distributed Control Systems", Oak Ridge National Laboratories report, ORNL/TM-2010/30, 2010, pp. 4-5.

[2] S. Gorman, "Electricity Grid in U.S. Penetrated by Spies", Wall Street Journal, April 8, 2009, `http://online.wsj.com/article/SB123914805204099085.html`, Retrieved March. 27, 2013.

[3] E. M. Tieghi, "Integrating Electronic Security into the Control Systems Environment: differences IT vs. Control Systems", CNN, March 18, 1998, `http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html`, Retrieved March. 27, 2013.

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

[5] L. Mili, "Power and communications systems as integrated cyberphysical systems", *in Proc. of 48th Allerton Conference on Communication, Control, and Computing*, Allerton, IL, 2010.

[6] A. Melin, R. Kisner, D. Fugate, and T. McIntyre, "Minimum State Awareness for Resilient Control Systems Under Cyber-Attack", *in Future of Instrumentation International Workshop* , Gatlinburg, Tennessee, 2012, pp. 978-982.

[7] S. Giorgi, F. Saleheen, F. Ferrese, and C. H. Won, "Adaptive Neural Replication and Resilient Control Despite Malicious Attacks", *in Proc. of the 5th Intl. Symp. on Resilient Control Systems*, Salt Lake, Utah, 2012, pp. 112-117.

[8] E. Eyisi, X. Koutsoukos, and N. Kottenstette, "Passivity-Based Trajectory Tracking Control with Adaptive Sampling Over a Wireless Network", *in Proc. of the 5th Intl. Symp. on Resilient Control Systems*, Salt Lake, Utah, 2012, pp. 130-136.

[9] Q. Zhu and T. Başar, "Robust and Resilient Control Design for Cyber-Physical Systems with an Application to Power Systems", *in Proc. of the IEEE Conference on Decision and Control*, Orlando, FL, 2011, pp. 4066-4071.

[10] Q. Zhu and T. Başar, "A Dynamic Game-Theoretic Approach to Resilient Control System Design for Cascading Failures", *in Proc. of the 1st Intl. conference on High Confidence Networked Systems*, Beijing, China, 2012, pp. 41-46.

[11] F. W. Yang, Z. D. Wang, Y. S. Hung, and M. Gani, "H_∞ Control for Networked Systems With Random Communication Delays", *in IEEE Transactions on Automatic Control*, vol. 51, no. 3, pp. 511-518, Mar, 2006.

[12] Q. Zhu and T. Başar, "Dynamic Policy-Based IDS Configuration", *in Proc. of the 48th IEEE Conference on Decision and Control and 28th Chinese Control Conference*, Shanghai, China, 2009, pp. 8600-8605

[13] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory, 2nd ed*, Society for Industrial and Applied Mathematics, 1999.

[14] T. Başar and P. Bernhar, *H^∞ Optimal Control and Related Minmax Design Problems*, Birkhauser, 1995.