MITSUBISHI ELECTRIC RESEARCH LABORATORIES
http://www.merl.com

Co-design of Safe and Efficient Networked Control Systems in Factory Automation with State-dependent Wireless Fading Channels

Hu, B.; Wang, Y.; Orlik, P.V.; Koike-Akino, T.; Guo, J.

TR2017-120 August 2017

Abstract

In factory automation, heterogeneous manufacturing processes need to be coordinated over wireless networks to achieve safety and efficiency. These wireless networks, however, are inherently unreliable due to shadow fading induced by the physical motion of the machinery. To assure both safety and efficiency, this paper proposes a state-dependent channel model that captures the interaction between the physical and communication systems. By adopting this channel model, sufficient conditions on the maximum allowable transmission interval are then derived to ensure stochastic safety for a nonlinear physical system controlled over a state-dependent wireless fading channel. Under these sufficient conditions, the safety and efficiency co-design problem is formulated as a constrained cooperative game, whose equilibria represent optimal control and transmission power policies that minimize a discounted joint-cost in an infinite horizon. This paper shows that the equilibria of the constrained game are solutions to a non-convex generalized geometric program, which are approximated by solving two convex programs. The optimality gap is quantified as a function of the size of the approximation region in convex programs, and asymptotically converges to zero by adopting a branch-bound algorithm. Simulation results of a networked robotic arm and a forklift truck are presented to verify the proposed co-design method.

arXiv

Co-design of Safe and Efficient Networked Control Systems in Factory Automation with State-dependent Wireless Fading Channels

Bin Hu, Yebin Wang, Philip Orlik, Toshiaki Koike-Akino and Jianlin Guo

***Abstract*—In factory automation, heterogeneous manufacturing processes need to be coordinated over wireless networks to achieve safety and efficiency. These wireless networks, however, are inherently unreliable due to *shadow fading* induced by the physical motion of the machinery. To assure both safety and efficiency, this paper proposes a state-dependent channel model that captures the interaction between the physical and communication systems. By adopting this channel model, sufficient conditions on the maximum allowable transmission interval are then derived to ensure *stochastic safety* for a nonlinear physical system controlled over a state-dependent wireless fading channel. Under these sufficient conditions, the safety and efficiency co-design problem is formulated as a constrained cooperative game, whose equilibria represent optimal control and transmission power policies that minimize a discounted joint-cost in an infinite horizon. This paper shows that the equilibria of the constrained game are solutions to a non-convex generalized geometric program, which are approximated by solving two convex programs. The optimality gap is quantified as a function of the size of the approximation region in convex programs, and asymptotically converges to zero by adopting a branch-bound algorithm. Simulation results of a networked robotic arm and a forklift truck are presented to verify the proposed co-design method.**

***Note to Practitioners*—This paper is motivated by problem of designing efficient communication and control policies to ensure safety for factory automation where different manufacturing processes coordinate with each other through wireless networks. One of the main challenges for this problem lies in the fact that wireless networks used for safety are highly unreliable, and can be seriously disrupted by operational machinery in the vicinity. Existing approaches that decouple the design of communication and control policies may fail to achieve efficiency for factory automation systems due to the interaction between the communication (cyber) and physical systems. By taking into account such *cyber-physical* couplings, this paper develops a novel co-design framework under which the communication and control policies are coordinated to achieve both system safety and efficiency. Under the co-design framework, this paper further shows that the communication and control policies that minimize the use of both communication and control resources in the long run while respecting safe operations, can be computed efficiently. This allows the proposed co-design method to go beyond the simple example illustrated in this paper and apply to more complex practical systems, such as automobile assembly system, manufacturing factory with automated heavy facilities, and automated warehouse with mobile industrial robots.**

***Index Terms*—Co-design method, shadow fading, stochastic safety, factory automation, networked control system.**

Yebin Wang, Philip Orlik, Toshiaki Koike-Akino and Jianlin Guo are with Mitsubishi Electric Research Laboratories (MERL), Cambridge, MA 02139, USA. yebinwang, porlik, koike, guo@merl.com

This work was performed during Bin Hu's internship at MERL. bhu2@alumni.nd.edu

I. Introduction

A. Background and Motivation

FACTORY Automation Networks (FANs) are Cyber-Physical Systems (CPS) consisting of numerous heterogeneous manufacturing processes that coordinate with each other by exchanging information over wireless networks [1]–[3]. FANs have received considerable attention due to the rapid development of wireless communication technologies, which provides efficient and cost-effective service such as increased mobility, easy scalability and maintenance for applications like automated assembly systems in manufacturing factories [4]. In many safety-critical applications, safety is always of primary concern in FANs. However, building safe and efficient FANs is challenging in two aspects. First, from a system modeling standpoint, the heterogeneous nature of FANs requires a hybrid framework that can capture system dynamics in different levels as well as their mutual interactions. Assessing the performance and safety of this "hybrid" system as a whole demands different modeling and analysis tools. Secondly, the wireless network in FANs is inherently unreliable due to channel fading [3], [5] or interference [6] caused by internal system states or external environments, such as obstacles or physical motions of machinery. The fading channel inevitably results in a severe drop in the network's quality of service (QoS) and thereby introduces a great deal of stochastic uncertainties in FANs that may cause serious safety issues. The objective of this paper is to develop a co-design paradigm for communication and control systems under which a certain level of safety and efficiency can be achieved for FANs in the presence of *shadow fading*.

Assuring safety for FANs often requires joint coordination from heterogeneous systems which may have different objectives. Such a coordination is necessary due to the interactions among the heterogeneous systems. Such interactions exist in many industrial applications, to name a few, manufacturing systems with heavy facilities mills and cranes discussed in [7], sensor network with moving robots [8] and indoor wireless networks with moving human bodies [9]. One typical example in FANs is an assembly process where an autonomous assembly arm and a forklift truck collaborate to assemble products. On the one hand, the control objective of an autonomous assembly arm is to track a specified trajectory by exchanging information between a physical plant and a remote controller via wireless networks. On the other hand, the objective of the forklift system is often related to accomplishing some

high-level tasks, such as transporting assembled products from one workstation to another. These physically separated systems, however, may have strong cyber-physical couplings. The cyber-physical couplings in the systems of networked assembly arm and forklift trucks comes from the fact that the physical motion of forklift vehicle may lead to serious *shadow fading* in the wireless network that is used by the assembly arm, thereby significantly affecting the system stability and performance. Thus, to ensure system safety for FANs, one must explicitly examine such cyber-physical couplings in communication channels.

The channel model that is used to characterize the *shadow fading* in FANs, must be carefully examined. As a type of channel fading, shadow fading is often characterized in terms of the channel gain. Traditionally, the channel gains are modeled either as *independent identical distributed* (i.i.d.) random processes [6], [10]–[12] with assumed distributions such as Rayleigh, Rician and Weibull or as Markov chains [13], [14]. These channel models are inadequate to characterize the cyber-physical couplings in FANs due to the fact that the network state is assumed to be independent from physical states in either i.i.d. or Markov chain models. With such independency, control and communication could be considered separately through the application of a separation principle [10]. This separation-principle, may be valid for networked system where the network states are independent of physical dynamics, but is clearly inappropriate for FANs where the channel state is functionally dependent on the physical states. This dependency of channel states on physical states motivates the development of a new co-design paradigm under which the communication and control policies are coordinated to achieve both system safety and efficiency.

B. Related Work

The example of an assembly process as well as the research work in [7]–[9], [15], [16] have demonstrated the importance of considering the cyber-physical couplings between communication and control systems in assuring system safety and efficiency for FANs. Similar conclusions have also been made in prior work [17], [18] where the dependency of channel states on physical states is used in the design of distributed switching control strategy to assure vehicle safety in vehicular networked systems. This paper expands the results in [18] to show that both system safety and efficiency can be achieved via a novel co-design framework. Other than these papers, we are aware of no other work formally analyzing both the system safety and efficiency *in the presence of such cyber-physical couplings*. There is, however, a great deal of related work on the co-design of communication and control systems assuming the channel states are independent of physical states. We will review these results and discuss their relationships to the work in this paper.

From a communication perspective, the impact of channel fading on the system performance can be mitigated by increasing the transmission power. This observation motivates much research on the design of optimal power strategy to achieve various objectives in both communication [19], [20] and control communities [8], [10], [21]. The objective of power control in the communication community mainly focuses on improving the communication reliability and performance in an average or asymptotic sense. In [19], [20] and relevant references therein, an adaptive power strategy combined with adaptive data-rate strategies was developed to achieve Shannon limit for fading channels. The optimal power strategy was shown to be a function of the channel gain.

The objective of power control in the control community, however, is more concerned with how the communication quality affects the system stability and performance. As shown in [22], [23], such impact is often related to the unstable modes of the dynamics in physical systems and the QoS that could be delivered by a given wireless network. The power control strategy in networked control systems is often designed to ensure a certain level of QoS under which the closed-loop system is stable. In [8], [21], sufficient conditions on the transmission power were established to ensure exponentially bounded performance for state estimation of discrete linear time-varying systems.

When considering a joint objective for the communication and control systems, recent work in [10], [24]–[26] showed that the *certainty equivalence property* holds for the optimal control policy while the optimal communication policy was adapted to the channel states and physical states. In particular, [24] showed that the joint optimization of scheduling and control can be separated into the subproblems of an optimal regulator, estimator and scheduling. Similar ideas were applied to a joint design of controller and routing redundancy over a wireless network [25]. The work in [10] considered a co-design problem for optimal control and transmission power policies for a stochastic discrete linear system controlled over a fading channel. Their results showed that the optimal control policy was a standard LQR controller while the optimal power policy was adapted to both channel and plant states. This similar structure was also discovered in a joint design problem for an optimal encoder and controller over noisy channels [26].

All of the above studies, however, were developed by assuming a state-independent channel model. From a safety standpoint, this state-independent channel model is often obtained by assuming the worst impact that the physical state can have on the network. As a result, the selected communication policy (transmission power, data rate, or scheduling) may be greater than necessary to assure the same level of performance that can be obtained by using state-dependent channel model. In other words, the conservativeness on the selection of state-independent channel model may prevent the system as a whole from achieving system efficiency.

C. Contribution

Motivated by the cyber-physical couplings in heterogeneous industrial systems, this paper develops a co-design paradigm to achieve both system safety and efficiency in the presence of *shadow fading*. The heterogeneous industrial systems are characterized by a nonlinear networked control system and a Markov decision process, which can represent a variety of realistic situations in industrial applications [7]–[9], [15],

[16]. Under this heterogeneous system framework, the first contribution of this paper is the proposal of a novel state-dependent fading channel model that captures the impact of the physical states on the channel state. Furthermore, this paper shows that the state-dependent channel model is a Markov modulated Bernoulli process [27] that generalizes the traditional i.i.d. Bernoulli channel model in two important aspects: (1) the model parameters are not constants and are stochastic processes due to their dependence on a randomly changing environment; (2) the channel parameters can be controlled by taking advantage of the cyber-physical couplings between communication and control systems.

Under the state-dependent channel model, the safety issue is examined in a stochastic setting by investigating the likelihood of the system states entering a forbidden or unsafe region. Thus, the second contribution of this paper is the sufficient condition on the maximum allowable transmission interval (MATI) under which the wireless networked system with *state-dependent fading channels* is *stochastically safe*. We also show that the MATI derived in this paper generalizes the well known results in [28] where the channel fading impact was not considered. To the best of our knowledge, the sufficient conditions presented in this paper are the first results on MATI that guarantee the stochastic safety under the *state-dependent fading channels*.

Under these safety conditions, the third contribution of this paper is the proposal of a new co-design paradigm to assure both safety and efficiency for FANs. In particular, we show that this safety-efficiency co-design can be formulated as a constrained two-player cooperative game. The equilibrium points of the constrained cooperative game represent optimal control and transmission power policies that minimize a discounted joint-cost induced by power consumption and control efforts in infinite horizon. The equilibrium of this constrained cooperative game can be obtained by solving a non-convex generalized geometric program (GGP) [29], [30]. To address the non-convexity of the GGP, this paper approximates the non-convex GGP with two relaxed convex GGPs that provide upper and lower bounds on the optimal solution. These bounds are shown to asymptotically approach the global optimum by using a branch-bound algorithm.

This paper is organized as follows. Section II describes the system model and problem formulation. Section III presents the sufficient conditions to ensure *stochastic safety*. Under the safety conditions, Section IV proposes a co-design paradigm to assure both safety and efficiency. The optimal solutions for the co-design problem are provided in Section IV-A. The main results are demonstrated via simulations of a mechanical robotic arm and a forklift truck in Sections V. Section VI concludes the paper.

Notations. Throughout the paper the n-dimensional Euclidean vector space is denoted by $\mathbb{R}^n$ and the non-negative reals and integers are denoted as $\mathbb{R}_{\geq 0}$ and $\mathbb{Z}_{\geq 0}$, respectively. The infinity norms of the vector $x \in \mathbb{R}^n$ and the matrix A are denoted by $|x|$ and $\|A\|$ respectively. The right limit value of a function $f(t)$ at time t is denoted by $f(t^+)$. Given a time interval $[t_1, t_2)$ with $t_1, t_2 > 0$, the essential supremum of a function $f(t)$ over the time interval $[t_1, t_2)$ is denoted by $|f(t)|_{[t_1,t_2)} = \operatorname{ess\,sup}_{t\in[t_1,t_2)} \|f(t)\|$ where $\|\cdot\|$ is the Euclidean norm. A function $f(t)$ is essentially ultimately bounded if $\exists M > 0$, $|f(t)|_{\mathscr{L}_\infty} = \operatorname{ess\,sup}_{t\geq 0} \|f(t)\| \leq M$. A function $\alpha(\cdot) : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is a class $\mathscr{K}$ function if it is continuous and strictly increasing, and $\alpha(0) = 0$. A function $\alpha(t)$ is a class $\mathscr{K}_\infty$ function if it is in class $\mathscr{K}$ and radially unbounded. A function $\beta(\cdot,\cdot) : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is a class $\mathscr{KL}$ function if $\beta(\cdot, t)$ is a class $\mathscr{K}_\infty$ function for each fixed $t \in \mathbb{R}_{\geq 0}$ and $\beta(s,t) \to 0$ for each $s \in \mathbb{R}_{\geq 0}$ as $t \to +\infty$. The function $\beta(\cdot,\cdot)$ is said to be of class Exp-$\mathscr{KL}$ if there exist $K_1, K_2 > 0$ such that $\beta(s,t) = K_1 \exp(-K_2 t)s$. A function $\overline{\beta}(\cdot,\cdot,\cdot) : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is said to be of class $\mathscr{KLL}$ ($\overline{\beta} \in \mathscr{KLL}$), if for each $r \geq 0$, $\overline{\beta}(\cdot,\cdot,r) \in \mathscr{KL}$ and $\overline{\beta}(\cdot, r, \cdot) \in \mathscr{KL}$.

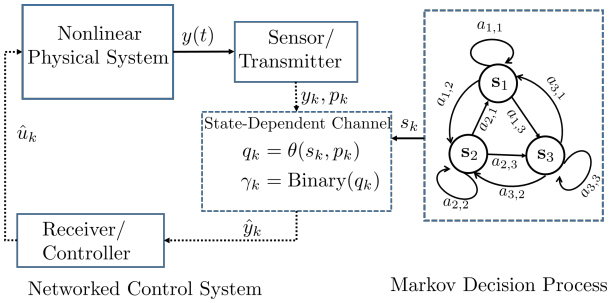


Fig. 1: Heterogeneous System Framework: Networked Control System and Markov Decision Process

II. System Model: A Heterogeneous System Framework

Fig. 1 shows a heterogeneous system framework with two subsystems. One is a networked control system ($\mathscr{G}$) that characterizes a nonlinear physical system being controlled over a wireless network. The other one is a Markov Decision Process (MDP) ($\mathscr{M}$) that models stochastic high level dynamics of a moving object in industrial systems.

The cyber-physical coupling within this heterogeneous framework is due to the fact that the physical states (e.g., locations) of the moving object modeled by MDP's states may lead to *shadow fading* on the wireless channel that is used by the networked control system. Such a coupling has been shown to be critical for performance guarantee in a variety of realistic situations in industrial applications, to name a few, such as robotic arms and forklift trucks, heavy facilities mills and cranes [7], sensor network with moving robots [8], [16] and indoor wireless networks with moving human bodies [9]. Under such industrial settings, the radio channel characteristics are non-stationary and may experience abrupt changes due to the motion of the moving object. Such *state-dependent* property of these wireless communications in industrial systems clearly invalidates the use of traditional co-design frameworks, such as [10], [24], [31], that rely on the assumption that the channel states are decoupled from the physical states. The heterogeneous system framework depicted in Fig. 1 is thus motivated by the co-design challenge under state-dependent fading channels.

A. The $\mathscr{G}$ System Model

The dynamics of the $\mathscr{G}$ system are modeled as follows,

$$\mathscr{G} := \begin{cases} \dot{x}_p &= f_p(t,x_p,\hat{u},w) \\ y &= g_p(t,x_p), \quad \text{Physical Plant} \\ \dot{x}_c &= f_c(t,x_c,\hat{y}) \\ u &= g_c(t,x_c), \quad \text{Remote Controller.} \end{cases}$$

where $x_p \in \mathbb{R}^{n_x}$ and $y \in \mathbb{R}^{n_y}$ are the physical states and measurements, respectively. $x_c \in \mathbb{R}^{n_c}$ and $u \in \mathbb{R}^{n_u}$ are the internal state and output for the remote controller, respectively. $w \in \mathbb{R}^{n_w}$ is the external disturbance that is assumed to be essentially ultimately bounded, i.e., $\exists M_w > 0$, $|w|_{\mathscr{L}_\infty} \leq M_w$. $f_p(\cdot,\cdot,\cdot,\cdot) : \mathbb{R}_{\geq 0} \times \mathbb{R}^{n_x} \times \mathbb{R}^{n_u} \times \mathbb{R}^{n_w} \to \mathbb{R}^{n_x}$, $g_p(\cdot,\cdot) : \mathbb{R}_{\geq 0} \times \mathbb{R}^{n_x} \to \mathbb{R}^{n_y}$, $f_c(\cdot,\cdot,\cdot) : \mathbb{R}_{\geq 0} \times \mathbb{R}^{n_c} \times \mathbb{R}^{n_u} \to \mathbb{R}^{n_c}$ and $g_c(\cdot,\cdot) : \mathbb{R}_{\geq 0} \times \mathbb{R}^{n_x} \to \mathbb{R}^{n_u}$ are Lipschitz functions for the physical plant and remote controller respectively. Without loss of generality, we assume the origin is the unique equilibrium for system $\mathscr{G}$, i.e. $f_p(0,0,0,0) = 0^{n_x}, f_c(0,0,0) = 0^{n_c}, g_p(0,0) = 0^{n_y}, g_c(0,0) = 0^{n_u}$.

Let $\{t_k\}$ denote an increasing sequence of time instants where $t_k < t_{k+1}$ for all $k \in \mathbb{Z}_{\geq 0}$. Let $\Omega_p = \{p_i\}_{i=1}^M$ be a transmission power set including M power levels where $p_i \in \mathbb{R}_{\geq 0}$ is the power level. As shown in Figure 1, the measurement y and controller output u are sampled and transmitted over an unreliable communication channel with a selected power level $p_k \in \Omega_p$ at time instant t_k. The wireless network is subject to fading and randomly drops the sampled information at each time instant. Let $\{\gamma(k)\}$ denote a binary random process taking value from $\{0,1\}$. The value of the process $\gamma(k)$ at the kth consecutive sampling instant indicates whether or not a packet dropout has occurred. In particular,

$$\gamma(k) = \begin{cases} 1 & , \quad \text{packet successfully decoded without error} \\ 0 & , \quad \text{packet is dropped.} \end{cases}$$

Let $\hat{y}(t_k)$ and $\hat{u}(t_k)$ denote the estimates of the corresponding variables at time instant t_k. Note that we assume the time used for communication and computing control action is negligible compared to the sampling time interval and the network condition is unchanged during this small time interval. The estimation error induced by the communication during the sampling time interval $[t_k, t_{k+1})$ is defined as $e_y(t) = y(t) - \hat{y}(t_k)$ and $e_u = u(t) - \hat{u}(t_k)$. Let $e(t) = [e_y(t); e_u(t)]^T$ denote the aggregated estimation error at time t. After the information is successfully received, this aggregated estimation error will be reset to zero. Let t_k^+ denote the real time immediately after the sampling instant, t_k. The estimation error $e(t_k^+)$ will be reset to zero immediately after each successful transmission. So we may formally express $e(t_k^+)$ as $e(t_k^+) = (1-\gamma(k))e(t_k)$. Let $x := [x_p; x_c]$ denote the aggregated state for the closed loop system $\mathscr{G}$, and then one has the following equivalent system representation in terms of x and e,

$$\hat{\mathscr{G}} := \begin{cases} \dot{x} &= f(t,x,e,w) \\ \dot{e} &= g(t,x,e,w), \forall t \in (t_k, t_{k+1}) \\ e(t_k^+) &= (1-\gamma(k))e(t_k), \quad k \in \mathbb{N}^+. \end{cases} \tag{1}$$

where

$$f(t,x,e,w) := \begin{bmatrix} f_p(t,x_p,g_c(t,x_c)-e_u(t),w) \\ f_c(t,x_c,g_p(t,x_p)-e_p(t)) \end{bmatrix}$$

$$g(t,x,e,w) := \begin{bmatrix} \frac{\partial g_p(x_p,t)}{\partial x_p} f_p(t,x_p,g_c(t,x_c)-e_u(t),w) + \frac{\partial g_p(x_p,t)}{\partial t} \\ \frac{\partial g_c(x_c,t)}{\partial x_c} f_c(t,x_c,g_p(t,x_p)-e_u(t)) + \frac{\partial g_c(x_c,t)}{\partial t} \end{bmatrix}.$$

Note that we further assume that the functions $g_p(\cdot,\cdot)$ and $g_c(\cdot,\cdot)$ are continuously differentiable and thus the function $g(\cdot,\cdot,\cdot,\cdot)$ in (1) is well defined. Since the (set) stability of the system $\hat{\mathscr{G}}$ implies the (set) stability of the system $\mathscr{G}$, we will only discuss the stability of the system $\hat{\mathscr{G}}$ in the remaining of this paper.

B. The $\mathscr{M}$ System Model

The $\mathscr{M}$ system is modeled by an MDP process. An MDP is defined by a five tuple $\mathscr{M} = \{S, s_0, A, P, c\}$, where

- $S = \{s_i\}_{i=1}^N$ is the state space for the MDP.
- $s_0 \subset S$ is the set of initial states.
- $A = \{a_i\}_{i=1}^{M_a}$ is the action set.
- $P : S \times A \times S \to [0,1]$ is the transition probability , i.e. $P(s_i, a, s_j) = \Pr\{s_j | a, s_i\}$.
- $c : S \times A \to \mathbb{R}_{\geq 0}$ is the reward function.

Unlike system $\mathscr{G}$ that models low level physical dynamics, the MDP process is used to model discrete-event decision making processes managing high-level control objectives such as transporting products from one location to another with minimum time or energy. The state space S in the MDP system corresponds to a finite number of partitioned regions that the vehicle system, such as forklift trucks or cranes [7] or robots [8], can operate by taking actions from an action set A. The transition probability matrix P is used to model the stochastic uncertainties caused by sensor or actuation noises when the actions are physically implemented. The costs in the MDP model are defined to characterize the high level control objectives for the vehicle system. For instance, if the control objective is to transport the products to a target region, then small costs will be assigned in the minimization optimization problem, to the situation when the vehicle is transitted to the target region.

C. State Dependent Dropout Channel Model

As shown in Fig. 1, the wireless channel used by the networked control system $\mathscr{G}$ is functionally dependent on the state of the MDP system. This relationship corresponds to the situation that vehicle's physical positions directly lead to shadow fading, thereby generating a great deal of stochastic uncertainties in system $\mathscr{G}$. Equation (1) shows that the stochastic uncertainty in system $\hat{\mathscr{G}}$ is governed by a binary random process $\{\gamma(k)\}$, which characterizes the stochastic variations in channel conditions.

The state-dependency in the shadow fading channel is captured by a novel *State-Dependent Dropout Channel* (SDDC) model that is formally defined as follows.

Definition II.1. *Given a binary random process $\{\gamma(k)\}_{k=0}^\infty$, an MDP system $\mathscr{M} = \{S, s_0, A, P_m, c\}$ and a transmission power*

set $\Omega_p = \{p_i\}_{i=1}^M$, the wireless channel is SDDC if

$$\Pr\{\gamma(k)=1|s(k)=s,p(k)=p\} = 1-\theta(s,p), \forall s\in S, p\in\Omega_p. \tag{2}$$

where $\theta(s,p)\in(0,1)$ is the outage probability [6] that monotonically decreases with respect to the transmission power level p.

Remark II.2. *The definition of the SDDC is closely related to the* outage probability*, which is a widely used performance metric for fading channels [6]. It characterizes the likelihood of the Signal-to-Noise Ratio (SNR) being below a specified threshold γ_0, i.e.* $\Pr\{SNR \le \gamma_0\}$*. The difference between the SDDC model and traditional* outage probability *lies in the state-dependent feature of* (2) *where the probability is defined for each each MDP state (partitioned region). The probability defined in* (2) *can be obtained by measuring the SNR for each MDP state, see [7], [9] and reference therein for details about the statistical methods. In practice, the transmitter can estimate the probability by either directly using the visual sensor to observe the positions of the controlled moving object, or using the estimation techniques discussed in [7], [15]. See Example II.4 for more details about how to construct the SDDC from the* outage probability.

Remark II.3. *The SDDC model in* (2) *relates the channel state (packet dropout probability) to the MDP states and transmission power levels. From a control standpoint, this correlation enables that the channel conditions can be controlled by designing different control and transmission power strategies. By using such a freedom in the channel model, this paper develops a co-design framework that coordinates control and communication strategies to achieve both safety and efficiency for the entire heterogeneous system. The co-design idea of using the state-dependent channel model distinguishes our work from other results, such as [7]–[9], [16] where the channel state is assumed a fixed and uncontrollable random process.*

Example II.4 (SDDC model with Raleigh fading)**.** *Channel fading is often the result of the superimposition of signal attenuation in both large (shadowing) and small scale levels [6]. Let h_k denote the small scale fading gain induced by multipath propagation at time instant t_k. Suppose $\{h_k\}_{k=0}^{\infty}$ is an* i.i.d *process that satisfies a Raleigh distribution with a scale parameter* 1*, i.e. $h_k \sim Raleigh(1), \forall k\in\mathbb{Z}_{\ge 0}$. Let $\psi(\cdot): S\to[0,1]$ denote a shadow level function that characterizes the level of shadowing effect on the channel gain for each MDP state, i.e. $0\le\psi(s)\le 1, \forall s\in S$. Thus, the state dependent channel gain is $\bar{h}_k(s) := \psi(s)h_k$, and for a given transmission power level p and noise power N_0, the SNR is $p\bar{h}_k(s)^2/N_0$. With the assumption that the small scale fading gain is conditionally independent on shadowing state $s\in S$, for a given SNR threshold γ_0, one has*

$$\begin{aligned}&\Pr\{\gamma(k)=1|s(k)=s,p(k)=p\}\\ =&\Pr\{\frac{p(k)h_k^2\psi(s(k))^2}{N_0}\ge\gamma_0\Big|s(k)=s,p(k)=p\}\\ =&\int_{\frac{\gamma_0 N_0}{p}}^{\infty}\psi(s)e^{-\psi(s)x}dx = e^{-\frac{N_0\gamma_0\psi(s)}{p}}.\end{aligned}$$

Then, we have the explicit function form $\theta(s,p) = 1 - e^{-\frac{N_0\gamma_0\psi(s)}{p}}$ for SDDC model.

The SDDC in (2) characterizes a *cyber-physical coupling* between the networked control system $\mathscr{G}$ and the MDP system $\mathscr{M}$. In the presence of such coupling, the first objective of this paper is to find conditions under which system $\mathscr{G}$ achieves *stochastic safety* that is formally defined as belows.

Definition II.5 (Stochastic Safety)**.** *Consider the networked control system $\hat{\mathscr{G}}$ in (1) and the SDDC model in (2), let $\Omega_s = \{x\in\mathbb{R}^{n_x+n_c}||x|\le r\}$ with $r\ge 0$ denote a safe set for $\hat{\mathscr{G}}$ system, and $x_0 = x(0)$ denote the initial state of the networked control system,*

- **E1** *The $\hat{\mathscr{G}}$ system with $w\equiv 0$ is* asymptotically safe in expectation *with respect to Ω_s, if $\forall x(0)\in\Omega_s$, there exists a class $\mathscr{KL}$ function $\overline{\beta}(\cdot,\cdot)$ such that*
$$\mathbb{E}\big[|x(t)|\big] \le \overline{\beta}(|x_0|,t), \quad \forall t\in\mathbb{R}_{\ge 0} \tag{3}$$
and thereby $\lim_{t\to+\infty}\mathbb{E}\big[|x(t)|\big]=0$.
- **E2** *The $\hat{\mathscr{G}}$ system with $|w(t)|_{\mathscr{L}_\infty}\le M_w$ is* asymptotically bounded in expectation *with respect to Ω_s, if $\forall x(0)\in\Omega_s$, there exists a class $\mathscr{KL}$ function $\overline{\beta}(\cdot,\cdot)$ and a class $\mathscr{K}$ function $\kappa(\cdot)$ such that*
$$\mathbb{E}\big[|x(t)|\big] \le \overline{\beta}(|x_0|,t)+\kappa(M_w), \quad \forall t\in\mathbb{R}_{\ge 0} \tag{4}$$
and $\lim_{t\to+\infty}\mathbb{E}\big[|x(t)|\big]=\kappa(M_w)$.
- **P1** *The $\hat{\mathscr{G}}$ system with $w\equiv 0$ is* almost surely asymptotically safe *with respect to Ω_s, if $\forall\varepsilon,\tau>0$ and $x_0\in\Omega_s$, there exists a class $\mathscr{KLL}$ function $\beta_\varepsilon(\cdot,\cdot,\cdot)$ such that*
$$\Pr\big\{\sup_{t\ge\tau}|x(t)|\ge\varepsilon+r\big\}\le\beta_\varepsilon(|x_0|,\tau,r) \tag{5}$$
and $\lim_{\tau\to\infty}\Pr\big\{\sup_{t\ge\tau}|x(t)|\ge\varepsilon+r\big\}=0$.
- **P2** *The $\hat{\mathscr{G}}$ system with $|w(t)|_{\mathscr{L}_\infty}\le M_w$ is* stochastically safe in probability *with respect to Ω_s, if $\forall\varepsilon_1>0$, there exists a class $\mathscr{KL}$ function $\overline{\beta}_{\varepsilon_2}(M_w,r)$ such that*
$$\lim_{t\to\infty}\Pr\big\{|x(t)|\ge\varepsilon_1+r\big\}\le\overline{\beta}_{\varepsilon_2}(M_w,r). \tag{6}$$

Remark II.6. *The safety notions **E1** and **E2** are concerned with system behavior on average (in the first moment) while the safety notions **P1** and **P2** focus on the specification on the sample path of the system. Note that these two types of safety definitions specify both the system's transient and steady behavior. For systems without external disturbance, the safety definition **E1** requires that the first moment of the norm of the system trajectories must asymptotically converge to the origin if the initial states start within the safety set while the* almost sure asymptotic safety *definition **P1** is a stronger safety notion than the definition **E1** in the sense that it requires*

*almost all sample paths starting from the safety set Ω_s stay in the safe region with probability asymptotically going to one. For systems with non-vanishing but ultimately bounded disturbance, the definition **E2** requires that the first moment of the system trajectories is asymptotically bounded with its bound depending on the magnitude of external disturbance. The safety notion **P2** basically means that the probability of sample paths of the system leaving the safe region is asymptotically bounded and the probability bound is a function of the size of the external disturbance and safety region. These safety notions are closely related to the concepts of stochastic stability defined in [32], [33].*

Under the safety conditions for system $\mathscr{G}$, the second objective of this paper is to seek optimal control and communication policies to achieve system efficiency for both system $\mathscr{G}$ and $\mathscr{M}$. A control policy for the MDP system $\mathscr{M}$ is an infinite sequence $\pi^m = \{u_1^m, u_2^m, \ldots\}$ where u_k^m is the decision made at time instant k. The decision making u_k^m is defined as a probability distribution over the action set A given the history information, i.e., $u_k^m = \Pr\{a|s_k, a_{k-1}, \ldots, s_0\}, \forall a \in A$. Similarly, a power policy for system $\mathscr{G}$ can be defined as $\pi^p = \{u_1^p, u_2^p, \ldots,\}$ with $u_k^p = \Pr\{p|s_k, a_{k-1}, \ldots, s_0\}$. The policy is *stationary* if $\pi_\infty^m = \{u_\infty^m, u_\infty^m, \ldots\}$ ($\pi_\infty^p = \{u_\infty^p, u_\infty^p, \ldots\}$) with $u_\infty^m = \Pr\{a|s\}$ ($u_\infty^p = \Pr\{p|s\}$), $\forall a \in A, s \in S$ and $p \in \Omega_p$. This paper will focus on the stationary policy space.

With the definitions of control π^m and communication π^p policies, the system efficiency is defined as a constrained infinite horizon optimization problem as follows,

$$\begin{aligned} \min_{\pi^p, \pi^m} \quad & J_\alpha(s_0, \pi^m, \pi^p) = (1-\alpha) \sum_{k=0}^{\infty} \alpha^k \mathbb{E}\{\lambda c_p(p_k) + c(s_k, a_k)\} \\ \text{s.t.} \quad & \text{Safety conditions assuring (3) or (4) or (5) or (6).} \end{aligned} \tag{7}$$

where $c_p(\cdot): \Omega_p \to \mathbb{R}_{\geq 0}$ is the power cost and $c(\cdot,\cdot)$ is the cost defined in the MDP system. $\alpha \in (0,1)$ is the discounted factor that provides a weight between short term rewards and rewards that might be obtained in a more distance future. $\lambda > 0$ is a parameter used to adjust the weight between communication and control costs.

III. Stochastic Safety

This section presents sufficient conditions to ensure *stochastic safety* defined in Definition II.5 for the $\mathscr{G}$ system. The following two assumptions are needed for the main results.

Assumption III.1. *The system $\dot{x} = f(t,x,e,w)$ is input to state stable (ISS) w.r.t. e and w, i.e. there exist a class $\mathscr{KL}$ function $\beta(\cdot,\cdot)$, a class $\mathscr{K}$ function $\gamma_2(\cdot)$ and a positive real $\overline{\gamma}_1 \in \mathbb{R}_{\geq 0}$ such that $|x(t-t_0)| \leq \beta(|x(t_0)|, t-t_0) + \overline{\gamma}_1 |e|_{[t_0,t)} + \gamma_2(|w|_{[t_0,t)})$ and $\beta(\cdot,t)$ is a concave function for any fixed $t \in \mathbb{R}_{\geq 0}$. The system is* exponential input to state stable (Exp-ISS) *w.r.t. e and w, if $\beta(s,t)$ is a class Exp-$\mathscr{KL}$ function and $\gamma_2(s) = \overline{\gamma}_2 s$ is a linear function with $\overline{\gamma}_2 > 0$.*

Assumption III.2. *There exists a Lyapunov function $W(\cdot)$ and $\underline{w}, \overline{w}, L_1, L_2, L_3 > 0$ for the estimation error dynamics $\dot{e} = g(t,x,e,w)$ in system (1) such that*

$$\underline{w}|e| \leq W(e) \leq \overline{w}|e|, \tag{8}$$

$$\left\langle \frac{\partial W(e)}{\partial e}, g(t,x,e,w) \right\rangle \leq L_1 W(e) + L_2|x| + L_3|w|. \tag{9}$$

Assumption III.2 basically requires that the estimation error e is exponentially bounded and the couplings of x, w in the error dynamics are linear. The following proposition shows that for a given transmission time sequence $\{t_k\}_{k=0}^{\infty}$, the estimation error $e(t_k)$ forms a stochastic jump process whose jump size is $\theta(s,p)$ and depends on the MDP's state $s \in S$ and the transmission power level $p \in \Omega_p$.

Proposition III.3. *Consider a random dropout process $\{\gamma(k)\}$ associated with the channel's SDDC model in* (2) *and let $\{t_k\}$ denote the transmission time sequence. Let $W(e)$ be a Lyapunov function for the error dynamic system in* (1)*, then one has*

$$\mathbb{E}\{W(e(t_k^+))\Big| s(k) = s, p(k) = p\} = \theta(s,p) W(e(t_k)). \tag{10}$$

where the conditional expectation operator $\mathbb{E}(\cdot|\cdot)$ is taken with respect to the random process $\gamma(k)$.

Proof: The proof is easily completed by combining $W(e(t_k^+)) = (1-\gamma(k))W(e(t_k))$ and the SDDC model in (2). ∎

Under a *state dependent shadow fading channel*, the following theorem presents a sufficient condition on the Maximum Allowable Transmission Interval (MATI) under which the system $\hat{\mathscr{G}}$ achieves *almost sure asymptotic safety*. In particular, we show that the MATI is a function of the control (π_∞^m) and transmission power (π_∞^p) policies.

Theorem III.4. *Let $T_k = t_{k+1} - t_k$ denote the transmission time interval, P_m denote the transition matrix defined in* (12) *and $p \in \Omega_p$ denote the transmission power level. Suppose the ISS assumption in Assumption III.1 and Assumption III.2 hold, for a given stationary control policy π_∞^m and a given stationary transmission power policy π_∞^p, the $\hat{\mathscr{G}}$ system with $w = 0$ is asymptotically safe in expectation (asymptotically stable in expectation) with respect to the origin, if $T_k \in (0, \tau^*]$ where*

$$\tau^* = \frac{1}{L_1} \ln \frac{L_2 \overline{\gamma}_1 + L_1 \overline{w}}{L_2 \overline{\gamma}_1 + \overline{w} L_1 \| P_m(\pi_\infty^m, \pi_\infty^p) diag(\theta(s,p)) \|} > 0 \tag{11}$$

is the MATI. The system parameters L_1, and L_2 come from (8) and (9) respectively and

$$diag(\theta(s,p)) = \begin{bmatrix} \theta(s_1,p_1) & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & \theta(s_i,p_j) & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & \theta(s_N,p_M) \end{bmatrix}$$

$$P_m(\pi_\infty^m, \pi_\infty^p) = \begin{bmatrix} \Pr(s_1,p_1|s_1,p_1) & \cdots & \Pr(s_1,p_1|s_N,p_M) \\ \Pr(s_1,p_2|s_1,p_1) & \cdots & \Pr(s_2,p_1|s_N,p_M) \\ \vdots & \vdots & \vdots \\ \Pr(s_N,p_M|s_1,p_1) & \cdots & \Pr(s_N,p_M|s_N,p_M) \end{bmatrix} \tag{12}$$

with $\Pr\{s_i,p_i|s_j,p_j\}=\sum_{a\in A(s_j)}\Pr\{s_i|a,s_j\}\Pr\{a|s_j\}\Pr\{p_i|s_i\}$.

Proof: The proof is provided in Appendix A. ∎

Remark III.5. *The MATI in* (11) *generalizes the result in [28]. In particular, one can see that the MATI in [28] is recovered if the shadow fading is absent, i.e.,* $\theta(s,p)=0,\forall s\in S,p\in\Omega_p$.

Theorem III.6. *Let the hypothesis in Theorem III.4 and the Exp-ISS assumption in Assumption III.1 hold , then the system* $\mathscr{G}$ *is almost surely asymptotically safe (**P1** in Definition II.5) with respect to the origin.*

Proof: The proof is provided in Appendix A. ∎

Theorem III.7. *Suppose the MATI condition in* (11) *holds and consider the system in* (1) *with* $|w|_{\mathscr{L}_\infty}\le M_w$*, then the system* $\hat{\mathscr{G}}$ *is asymptotically bounded in expectation (**E2** in Definition II.5) with respect to a bounded safe set* $\Omega_s=\{x\in\mathbb{R}^{n_x+n_c}\big||x|\le r\}$*, i.e.,* $\forall x(0)\in\Omega_s$*, there exists a class* $\mathscr{KL}$ *function* $\overline{\beta}(\cdot,\cdot)$ *and a class* $\mathscr{K}$ *function* $\kappa(\cdot)$ *such that*

$$\mathbb{E}\big[|x(t)|\big]\le\overline{\beta}(|x_0|,t)+\kappa(M_w),\quad\forall t\in\mathbb{R}_{\ge0}$$

and $\lim_{t\to+\infty}\mathbb{E}\big[|x(t)|\big]=\kappa(M_w)$.

Proof: The proof is provided in Appendix A. ∎

Theorem III.8. *Suppose the hypothesis in Theorem III.7 holds, then the system* $\hat{\mathscr{G}}$ *is stochastically safe in probability (**P2** in Definition II.5) with respect to a bounded safe set* $\Omega_s=\{x\in\mathbb{R}^{n_x+n_c}\big||x|\le r\}$.

Proof: The result can be straightforwardly obtained by Markov inequality. ∎

IV. Safety and Efficiency: A Two-player Constrained Cooperative Game

The *system efficiency* in this paper is defined as an optimization problem where optimal transmission power and control policies are sought to minimize a joint communication and control cost in an infinite horizon. To assure both system efficiency and safety, the control (π^m) and communication (π^p) policies must be carefully coordinated due to their tight couplings as suggested by the safety condition in (11). This collaboration between communication and control systems can be naturally formulated as a *two-player constrained cooperative game* where the players' strategy spaces are constrained and coupled. The equilibrium of the game represents the optimal transmission power and control policies to achieve both *system safety* and *efficiency*.

Problem IV.1 (Two-player Constrained Cooperative Game)**.** *Let* $c_p(\cdot):\Omega_p\to\mathbb{R}_{\ge0}$ *denote the power cost and* $c(\cdot,\cdot):S\times A\to\mathbb{R}_{\ge0}$ *denote the control cost for the MDP system, the safety and efficiency problem is to find the optimal control* π^{m^*} *and transmission power* π^{p^*} *policies to the following two-player constrained cooperative game,*

$$\begin{aligned}\min_{\pi^p,\pi^m}\quad & J_\alpha(s_0,\pi^m,\pi^p)\\ s.t.\quad & \|P_m(\pi^m,\pi^p)diag(\theta(s,p))\|\le\xi(T).\end{aligned}\tag{13}$$

where $\alpha\in(0,1)$ *and* T *is the transmission time interval and* $\xi(T)\in(0,1)$ *is a monotonically decreasing function with respect to* T.

Remark IV.2. *The inequality* (13) *is a safety constraint reformulated by the sufficient condition* (11)*. In order to see how this safety constraint is derived from* (11)*, let* (π^p,π^m) *denote the feasible policies such that* $T\le\tau^*(\pi^p,\pi^m)$*. Thus*

$$T\le\frac{1}{L_1}\ln\frac{L_2\overline{\gamma}_1+L_1}{L_2\overline{\gamma}_1+L_1\|P_m(\pi^p,\pi^m)diag(\theta(s,p))\|}.$$

By arranging the inequality, one has

$$\|P_m(\pi_p,\pi_m)diag(\theta(s,p))\|\le\underbrace{\frac{1}{L_1}\left[e^{-L_1T}(L_2\overline{\gamma}_1+L_1)-L_2\overline{\gamma}_1\right]}_{\xi(T)}.$$

Since $T\le\tau^*$*, one always has* $\xi(T)>0$*. Thus, for any given control* π^m *and power* π^p *policies that satisfy the above inequality, the sufficient condition in* (11) *assures system safety.*

Under the stationary policy space, we show that the two-player constrained cooperative game Problem IV.1 can be solved by solving the following constrained nonlinear optimization problem.

Problem IV.3. Constrained Nonlinear Optimization Problem: *Suppose the state S and action A spaces in the MDP system* $\mathscr{M}$ *are finite sets, and transmission power set* Ω_p *is finite. Let* $u^p_\infty(p|s)=\Pr\{p|s\}$ *and* $\delta(s,a)$ *where* $p\in\Omega_p,s\in S$ *and* $a\in A$*, denote the decision variables to the following nonlinear constrained optimization problem.*

$$\min_{u^p_\infty(p|s),\delta(s,a)}\sum_{(s,a)\in S\times A(s)}\big(\lambda\sum_{p\in\Omega_p}c_p(p)u^p_\infty(p|s)+c(s,a)\big)\delta(s,a)\tag{14a}$$

subject to

$$\sum_{s\in S}\frac{\sum_{a\in A(s)}\Pr\{s'|s,a\}\delta(s,a)}{\sum_{a\in A(s)}\delta(s,a)}\sum_{p\in\Omega_p}u^p_\infty(p|s')\theta(s,p)\le\xi(T),\tag{14b}$$

$$\sum_{a\in A(s)}\delta(s,a)=D_0(s)(1-\alpha)+\alpha\sum_{s'\in S}\sum_{a'\in A(s')}\delta(s',a')\Pr\{s|s',a'\},\tag{14c}$$

$$\sum_s\sum_a\delta(s,a)=1,\ \sum_{p\in\Omega_p}u^p_\infty(p|s)=1,\delta(s,a)\ge0,\ u^p_\infty(p|s)\ge0.\tag{14d}$$

The following Lemma shows that Problems IV.3 and IV.1 are equivalent in the sense that they have the same optimal solutions and objectives.

Lemma IV.4. *Let* δ^* *and* $u^{p^*}_\infty$ *denote the optimal solutions to Problem IV.3, then the policies* $u^{p^*}_\infty=\pi^{p^*}_\infty$ *and* $\pi^{m^*}_\infty(a|s)=\Pr\{a|s\}=\frac{\delta^*(s,a)}{\sum_{a\in A(s)}\delta^*(s,a)}$ *are the optimal solutions to Problem IV.1.*

Proof: The proof can be obtained by examining the equivalence between Problem IV.3 and Problem IV.1 in terms of objective function, decision variables and feasible set imposed by the constraints. We have already shown that

the objective function in Problem IV.1 can be rewritten as a function of the new decision variables $\{u_p(s,a)\}$ and $\{\delta(s,a)\}$ in Problem IV.3. According to the definition of $\delta(s,a)$, one has $\Pr\{a|s\} = \frac{\Pr\{a,s\}}{\Pr\{s\}} = \frac{\delta(s,a)}{\sum_{a\in A(s)}\delta(s,a)}$. Thus, the decision variable $\delta(s,a)$ uniquely defines the control strategy π^m. The constraints in (14d) are introduced to enforce the probability law (i.e. non-negativity and total probability being 1). The constraint in (14c) is a reformulation of the Markovian dynamics for the MDP in terms of new decision variables $\delta(s,a)$ and $u_p(s,a)$ (see [34] for more details). Therefore, one has established the equivalence and the proof is complete. ■

Remark IV.5. *Problem IV.3 is a polynomial optimization problem where the objective function and safety constraints in* (14b) *are polynomial functions. The main challenge to solve this polynomial optimization problem is the fact that the safety constraints are non-convex. The presence of non-convex constraint* (14b) *in the optimization problem is due to the couplings between communication and control policies in industrial settings with* state-dependent fading wireless channels.

A. Relaxed Generalized Geometrical Programming

Problem IV.3 falls into one type of non-convex optimization problem, called Generalized Geometric Program (GGP) [30] where the objective function and constraints are the difference of two *posynomials*. A posynomial is a function such that $G_i(x_1,x_2,\ldots,x_n) = \sum_{j=1}^{L} a_{ij} x_1^{b_{ij1}} x_2^{b_{ij2}} \ldots x_n^{b_{ijn}}$ where $a_l > 0, \forall l$ and $b_{ij} \in \mathbb{R}$.

Let $X = [\delta(s_1,a_1), u_\infty^p(p_1|s_1), \ldots, \delta(s_N,a_M), u_\infty^p(p_\ell|s_N)]^T$ denote the decision vector and $\Omega_X \subset \mathbb{R}_+^{NM\ell\times 1}$ denote the feasible region for X. The constrained optimization Problem IV.3 can be formulated as a GGP as follows,

$$\begin{aligned} \underset{X}{\text{minimize}} \quad & G_0(X) = G_0^+(X) \\ \text{subject to} \quad & G_i(X) = G_i^+(X) - G_i^-(X) \le 0, \quad i = 1,\ldots,N \\ & G_{\text{linear}}(X) \le 0, \quad X \in \Omega_X \end{aligned} \tag{15}$$

where $G_i^+, G_i^-, i = 1,2,\ldots,N$ are posynomials and G_{linear} are linear functions. To see how safety constraints in (14b) can be written as the difference of two posynomials, multiplying both sides of (14b) by $\prod_{s\in S}\sum_{a\in A(s)}\delta(s,a)$ leads to

$$\underbrace{\sum_{a\in A(s)} \Pr\{s'|a,s\}\delta(s,a) \sum_{p\in\Omega_p} u_\infty^p(p|s')\theta(s,p) \prod_{\tilde{s}\neq s,\tilde{s}\in S} \sum_{a\in A(s)} \delta(\tilde{s},a)}_{G_i^+(X)} - \underbrace{\xi(T)\prod_{s\in S}\sum_{a\in A(s)}\delta(s,a)}_{G_i^-(X)} \le 0.$$

The above GGP can be further reformulated by introducing an exponential transformation, $X = \exp(Z)$,

$$\begin{aligned} \underset{Z}{\text{minimize}} \quad & \tilde{G}_0(Z) = \tilde{G}_0^+ - \tilde{G}_0^- \\ \text{subject to} \quad & \tilde{G}_i(Z) = \tilde{G}_i^+(Z) - \tilde{G}_i^-(Z) \le 0, \quad i = 1,\ldots,M \\ & G_{\text{linear}}(Z) \le 0, \quad Z \in \Omega_Z. \end{aligned} \tag{16}$$

where $\Omega_Z = \log(\Omega_X) \subset \mathbb{R}^{NM\ell\times 1}$, $G_i^- = \sum_{j\in L_i^-} a_{ij}\exp\sum_{l=1}^n b_{ijl}z_l$ and $G_i^+ = \sum_{j\in L_i^+} a_{ij}\exp\sum_{l=1}^n b_{ijl}z_l$.

Since $\exp(Z)$ is a convex function in terms of Z, $\tilde{G}_i^+, \tilde{G}_i^-, i = 0,1,\ldots,N$ and G_{linear} are convex functions as well. However, the function $\tilde{G}_i^+(Z) - \tilde{G}_i^-(Z)$ in the safety constraint is generally not convex [30]. To address the non-convexity issues, this paper approximates the second terms $\tilde{G}_i^-$ in the non-convex safety constraints using a linear function. The basic idea is illustrated in Figure 2a using a simple exponential function. In Figure 2a, the linear function shown by the solid line upper approximates the exponential function while the linear function shown by the dashed line approximates the exponential function from below. These two functions can be viewed as upper and lower bounds on the exponential function. The following two subsections are devoted to demonstrate how to construct the upper and lower linear functions for a general multivariate exponential function $\tilde{G}_i^-(Z)$ for a given domain.

1) Relaxed GGP with Linear Upper Bound: For a given bounded domain $\Omega_Z = \{Z | Z \in [Z^L, Z^H]\}$ with $Z^L = [z_1^L,\ldots,z_n^L]$ and $Z^H = [z_1^H,\ldots,z_n^H]$, one can construct a linear function such that,

$$\begin{aligned} & \tilde{G}_i^-(Z) \le A_i Z + B_i \\ & A_i = \sum_{j\in L_i^-} a_{ij}A_{ij}[b_{ij1},\ldots,b_{ijn}], \quad B_i = \sum_{j\in L_i^-} a_{ij}B_{ij} \\ & A_{ij} = \frac{\exp(Y_{ij}^H) - \exp(Y_{ij}^L)}{Y_{ij}^H - Y_{ij}^L}, \quad B_{ij} = \frac{Y_{ij}^H\exp(Y_{ij}^L) - Y_{ij}^L\exp(Y_{ij}^H)}{Y_{ij}^H - Y_{ij}^L} \end{aligned} \tag{17}$$

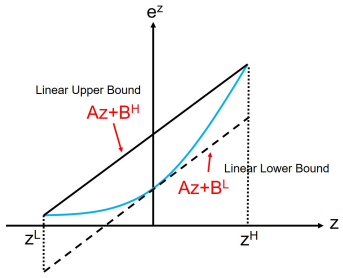
$$Y_{ij}^L = \sum_{l=1}^n \min(b_{ijl}z_l^L, b_{ijl}z_l^H), \quad Y_{ij}^H = \sum_{l=1}^n \max(b_{ijl}z_l^L, b_{ijl}z_l^H) \tag{18}$$

By replacing $\tilde{G}_i^-(Z)$ with $A_iZ+B_i, \forall i = 0,1,\ldots,M$ in the transformed GGP (16), one has the convex optimization problem as follows,

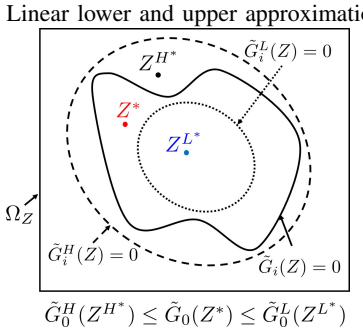
$$\begin{aligned} \underset{Z}{\text{minimize}} \quad & \tilde{G}_0^U(Z) = \tilde{G}_0^+(Z) \\ \text{subject to} \quad & \tilde{G}_i^U(Z) = \tilde{G}_i^+(Z) - (A_iZ + B_i) \le 0, \quad i = 1,\ldots,N \\ & G_{\text{linear}}(Z) \le 0, \quad Z \in \Omega_Z \end{aligned} \tag{19}$$

Let $\delta_{ij} = Y_{ij}^H - Y_{ij}^L$ denote the interval width associated with term j in $\tilde{G}_i^-$ and $\delta_i = \max_{j\in L_i^-}\delta_{ij}$ denote the maximum interval width over all terms in $\tilde{G}_i^-$. Let $\Delta_i(Z) = A_iZ + B_i - G_i^-(Z)$ denote the gap between $\tilde{G}_i^-$ and A_iZ+B_i and $\Delta_i^* = \max_{Z\in\Omega_Z}\Delta_i(Z)$ denote the maximum gap. The following lemma characterizes the explicit relationship between the maximum gap Δ_i^* and the size of the region of approximation δ_i [30],

Lemma IV.6. *Consider the transformed posynomial functions $\tilde{G}_i^-(Z)$ and its upper approximation A_iZ+B_i with the region of approximation Ω_Z, then, for all $Z \in \Omega_Z$, the maximum gap*



(a) Linear lower and upper approximation



(b) Inner and outer convex regions

Fig. 2: Lower and upper bounds by two relaxed convex GGPs

$\Delta_i^*, \forall i = 1,\ldots,N$ *defined over* Ω_Z *is a function of* δ_i *as follows,*

$$\begin{aligned}\Delta_i^* &\le \sum_{j\in L_i^-} e^{Y_{ij}^L}\Big(1-\Theta(\delta_{ij})+\Theta(\delta_{ij})\log(\Theta(\delta_{ij}))\Big)\\ &\le |L_i^-|e^{Y_i^L}\Big(1-\Theta(\delta_i)+\Theta_i\log(\Theta(\delta_i)\Big)\end{aligned}$$

where $e^{Y_i^L} = \max_{j\in L_i^-} e^{Y_{ij}^L}$ *and* $\Theta(\delta) = \frac{e^\delta - 1}{\delta}$. *Furthermore, one has* $\Delta_i^* \sim \mathscr{O}(\delta_i^2)$.

Proof: The proof is included in Appendix A. ■

2) Relaxed GGP with Linear Lower Bound: Similar to the case of upper bound,a lower bound for the transformed monomial function $\tilde{G}_{ij}^-(Z)$ can also be constructed as follows,

$$\begin{aligned}&\tilde{G}_i^-(Z) \ge A_i Z + B_i^L\\ &B_i^L = \sum_{j\in L_i^-} a_{ij}A_{ij}\Big(1-\log(A_{ij})\Big)\end{aligned} \tag{20}$$

By replacing $\tilde{G}_i^-(Z)$ with $A_iZ+B_i^L, \forall i = 0,1,\ldots,M$ in the transformed GGP (16), one has the following convex optimization with linear lower bounds,

$$\begin{aligned}\underset{Z}{\text{minimize}}\quad & \tilde{G}_0^L(Z) = \tilde{G}_0^+(Z) - (A_0Z+B_0^L)\\ \text{subject to}\quad & \tilde{G}_i^L(Z) = \tilde{G}_i^+(Z) - (A_iZ+B_i^L) \le 0, \quad i=1,\ldots,M\\ & G_{\text{linear}}(Z) \le 0, \quad Z\in\Omega_Z\end{aligned} \tag{21}$$

The following lemma shows that the maximum gap of for the lower bound case is the same as the upper bound case.

Lemma IV.7. *Consider the GGP problem (16) and the relaxed GGP (21) with lower bound linear function* $A_iZ+B_i^L, i = 0,1,\ldots,M$. *Let* $\Delta_i^{L^*}$ *denote the maximum gap defined over the domain* Ω_Z, *then* $\Delta_i^{L^*} = \Delta_i^*$ *and* $\Delta_i^{L^*} = \mathscr{O}(\delta_i^2)$ *as* $\delta \to 0$.

Proof: The proof is similar to the upper bound case and is omitted here. ■

The following lemma shows that the optimal solutions to the two convex optimizations in (19), (21) are lower and upper bounds to the original non-convex problem in (16).

Lemma IV.8. *Let* Z^{H^*}, Z^* *and* Z^{L^*} *denote the optimal solution to the optimization problems in (19), (16) and (21) respectively, the optimal objective functions then satisfy*

$$\tilde{G}_0^H(Z^{H^*}) \le \tilde{G}_0(Z^*) \le \tilde{G}_0^L(Z^{L^*}) \tag{22}$$

and the solution Z^{L^*} *is a suboptimal solution to the non-convex optimization problem in (16). Let* $\overline{\Delta}_0 := \tilde{G}_0(Z^{L^*}) - \tilde{G}_0(Z^*)$ *denote the gap between the suboptimal and optimal solutions, this gap then has upper upper bound as* $\overline{\Delta}_0 \le \tilde{G}_0^L(Z^{L^*}) - \tilde{G}_0^H(Z^{H^*})$.

Proof: Let $\mathscr{C}_v^H$, $\mathscr{C}_v$ and $\mathscr{C}_v^L$ denote the feasible sets that are generated by the constraints in optimization problems (19), (16) and (21) respectively. Since $\mathscr{C}_v^L \subset \mathscr{C}_v \subset \mathscr{C}_v^H$ and $\tilde{G}_0^H(Z) \le \tilde{G}_0(Z) \le \tilde{G}_0^L(Z)$ hold for any $Z\in\Omega_Z$, then one has $\tilde{G}_0(Z^{L^*}) \le \tilde{G}_0^L(Z^{L^*})$. By the definition of Z^* and $\mathscr{C}_v^L \subset \mathscr{C}_v$, one further has $\tilde{G}_0(Z^*) \le \tilde{G}_0(Z^{L^*}) \le \tilde{G}_0^L(Z^{L^*})$. The same argument can also be applied to prove $\tilde{G}_0^H(Z^{H^*}) \le \tilde{G}_0(Z^*)$. By Inequality (22), the final result holds. ■

B. Branch-Bound Algorithm

This section presents a *Branch-Bound* method under which the lower and upper bounds of the non-convex GGP Problem in (16) asymptotically approaches the optimal solutions.

1) Branch Procedure: The branch procedure involves partitioning the hyper-rectangular domain Ω_Z into two small sub-regions under which two convex optimization problems in (21) and (19) are solved. Let $\Omega_Z^{i,j} = \{Z\in\mathbb{R}^n | Z\in[Z^{L,ij}, Z^{H,ij}]\}$ denote the j^{th} $(j=1,2)$ sub-region at the i^{th} stage, where $Z^{L,ij}$ and $Z^{H,ij}$ represent the boundaries of the rectangular constraint $\Omega_Z^{i,j}$. For the sub-region $\Omega_Z^{i,j}$, let $Z^{H^*,ij}, Z^{L^*,ij}$ denote the optimal solutions to the problems in (19) and (21). Then, $\tilde{G}_0(Z^{H^*,ij})$ and $\tilde{G}_0(Z^{L^*,ij})$ are the corresponding lower bound and upper bound on $\tilde{G}_0(Z^*)$. Clearly, the upper bound solutions $Z^{L^*,ij}$ are always feasible for the original GGP problem while the lower bounds $Z^{H^*,ij}$ are not necessarily feasible solutions. In order to obtain tight bounds, the upper and lower bounds are iteratively updated by

$$\tilde{G}_0^{UB} = \begin{cases}\min\Big\{\tilde{G}_0^{UB,i-1}, \tilde{G}_0^{LB,i-1}, \{\tilde{G}_0(Z^{L^*,ij})\}_{j=1,2}\Big\}, \\ \qquad\qquad\qquad \text{if } \tilde{G}^{LB,i-1} \text{ is feasible}\\ \min\Big\{\tilde{G}_0^{UB,i-1}, \{\tilde{G}_0(Z^{L^*,ij})\}_{j=1,2}\Big\}, \quad \text{Otherwise}\end{cases} \tag{23}$$

$$\tilde{G}_0^{LB,i} = \begin{cases}\big\{\tilde{G}_0^{LB,i-1}, \tilde{G}_0(Z^{H^*,ij})\big\}, & \text{if } \tilde{G}_0(Z^{H^*,ij}) < \tilde{G}_0^{UB}, j=1,2\\ \tilde{G}_0^{LB,i-1}, & \text{Otherwise}\end{cases} \tag{24}$$

The upper bound $\tilde{G}_0^{UB}$ in (23) is the minimum feasible solutions up to stage i. The $\tilde{G}_0^{LB,i}$ is a set of all possible lower bounds that could be used to approach the global optimum.

At each stage, the branch procedure selects the region that has the minimum lower bounds, i.e.

$$(l, j) = \arg \min_{0 \le l \le i, j=1,2} \tilde{G}_0^{LB,i} \tag{25}$$

where (l, j) represents the index of the selected region. Thus, the "best" lower bound up to stage i is

$$\tilde{G}_0^{LB} = \tilde{G}_0(Z^{H^*,lj}) \tag{26}$$

The selected region is then partitioned into two smaller regions $\Omega_Z^{i+1,j}, j = 1,2$ by a bisection of the longest side of the hyper-rectangular. Two convex optimization problems in (21) and (19) are then constructed based on the new regions $\Omega_Z^{i+1,j}, j = 1,2$. The lower bound set $\tilde{G}_0^{LB,i}$ is further updated by removing current "best" lower bound $\tilde{G}_0(Z^{H^*,lj})$,

$$\tilde{G}_0^{LB,i} \leftarrow \tilde{G}_0^{LB,i} \setminus \tilde{G}_0(Z^{H^*,lj}) \tag{27}$$

This branch procedure repeats until the gap between the lower and upper bounds is smaller than some specified threshold ε_c.

2) Bound Procedure: The bound procedure is to cut those branches that have no feasible solutions or do not contain the global optimum. The criteria to determine which branch can be safely fathomed are based on the monotonicity analysis for the structure of the constraint and objective functions in the relaxed GGP formulation (21). To be specific, consider the following lower bounds for the original $\tilde{G}_i^U(Z), \forall i = 0,1,\ldots,m$ and $\forall Z \in \Omega_Z^{\ell,j}$

$$\tilde{G}_i^U(Z) \ge \underline{\tilde{G}}_i^U \tilde{G}_i^+(Y_i^{L,\ell j}) - \sum_{k \in L_{-i}} a_{ik} A_{ik}^{\ell j} Y_i^{H,\ell j} - B_i. \tag{28}$$

where $Y_i^{L,\ell j}, Y_i^{H,\ell j}$ and $A_{ik}^{\ell j}$ are defined in (18) for the region $\Omega_Z^{\ell,j}$. B_i is defined in (17). A branch associated with the above bounds can be removed if

- there exists any ℓ such that for any $i \in [1,2,\ldots,m], j \in \{1,2\}$, the bounds in (28) are positive
- there exists any ℓ such that $\underline{\tilde{G}}_0^U \ge \tilde{G}_0^{UB}$

Remark IV.9. *The first condition is used to test whether the convex domain generated by the branch procedure contains any feasible solutions, which is a necessary condition for feasibility test. The second condition is used to eliminate branches that do not contain the global optimum.*

3) Sub-optimality and Distance to Global Optimality: Obtaining an exact global optimum for a non-convex optimization problem is generally NP-hard [35], which means that "brute force" type of searching algorithms are necessary to find global solutions. Hence, it is reasonable to expect suboptimal solutions but with certain performance guarantee. Here, the performance refers to the explicit distance characterization between optimal solutions and suboptimal solutions generated by the branch-bound method. Specifically, we show that the optimality gap can be predicted by measuring the maximum size of the super-rectangular where the sub-optimal solutions locate. This prediction gives rise to an upper bound on the maximum number of stages needed in the Branch-Bound algorithm to achieve the desired optimality gap.

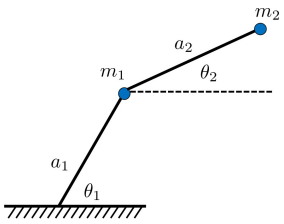
Theorem IV.10. *Consider the non-convex GGP problem in (16), relaxed convex problems in (19) and (21) and the Branch-Bound algorithm, let Z^*, Z^{H^*} and Z^{L^*} denote the optimal solutions for the optimization problems (16), (19) and (21) respectively, let $\delta := \max_{1 \le i \le m, j \in L_{-i}} (Y_{ij}^H - Y_{ij}^L)$ denote the maximum size of the super-rectangular region, then the suboptimal solutions Z^{H^*} and Z^{L^*} asymptotically converge to optimal solution Z^* as the maximum size $\delta \to 0$. Moreover, if the constraint qualification $\exists h_i \in \mathbb{R}^n, \nabla \tilde{G}_i(Z^*) h_i < 0, \forall i = 1,2,\ldots,M$ holds at Z^*, then, one has*

$$|Z^{H^*} - Z^*| = \mathcal{O}(\delta) \quad as \ \delta \to 0 \tag{29}$$

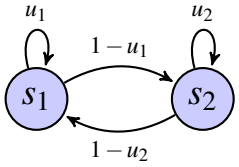
$$|Z^* - Z^{L^*}| = \mathcal{O}(\delta) \quad as \ \delta \to 0 \tag{30}$$

Furthermore, let D_B denote the depth of a full binary tree generated by the BB algorithm, then the maximum D_B to achieve a desired optimality gap δ^* is $D_B \sim \log_2(\left\lceil \frac{\delta^0}{\delta^*} \right\rceil^n + 1)$ where δ^0 is the maximum size of the initial super-rectangular region.

Proof: The proof is provided in Appendix A. ■



(a) Two Link Planar Elbow Arm



(b) The forklift truck: a two-state MDP

Fig. 3: Simulation example of networked robotic manipulator and forklift truck

V. Simulation Results

This section uses the example of a two-link planar elbow arm and a forklift truck to demonstrate the effectiveness of our co-design framework in assuring safety and efficiency for factory automation systems. The *almost sure safety* is demonstrated via Monte Carlo simulations using the sufficient conditions in Theorem III.4. Under the safety constraint, optimal results regarding the power management for robotic arm system and decision making in forklift trucks are provided to show the system's efficiency as a whole and the necessity of the co-design paradigm.

Consider the system dynamics of a nonlinear two-link

(Power, State)	s_1	s_2
p_L	0.4	0.9
p_H	0.1	0.4

TABLE I: Outage Probability $\theta(s,p)$ in SDDC (2)

planar elbow arm as follows [36],

$$\underbrace{\begin{bmatrix}(m_1+m_2)ga_1\cos\theta_1+m_2ga_2\cos(\theta_1+\theta_2)\\ m_2ga_2\cos(\theta_1+\theta_2)\end{bmatrix}}_{G(q)}+$$

$$\underbrace{\begin{bmatrix}(m_1+m_2)a_1^2+a_2m_2(a_2+2a_1\cos\theta_2) & m_2a_2(a_2+a_1\cos\theta_2)\\ m_2(a_2^2+a_1a_2\cos\theta_2) & m_2a_2^2\end{bmatrix}}_{M(q)}\begin{bmatrix}\ddot{\theta}_1\\ \ddot{\theta}_2\end{bmatrix}$$

$$=\begin{bmatrix}\tau_1\\ \tau_2\end{bmatrix}-\underbrace{\begin{bmatrix}-m_2a_1a_2(2\dot{\theta}_1\dot{\theta}_2+\dot{\theta}_2^2)\sin\theta_2\\ m_2a_1a_2\dot{\theta}_1{}^2\sin\theta_2\end{bmatrix}}_{V(q,\dot{q})}$$

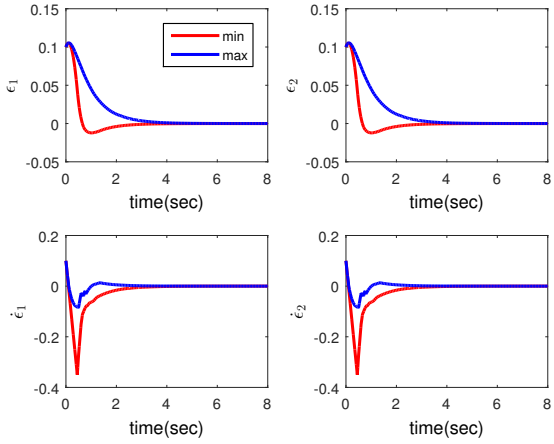
where $q=[\theta_1;\theta_2]$ are the angles for the upper and lower links of the planar elbow arm as shown in Figure 3a and $\dot{q},\ddot{q}$ are the corresponding angular velocities and accelerations. The system inputs $\tau_i, i=1,2$ are the external torque forces that are provided by either motors or hydraulic actuators [36]. These forces $\tau_i, i=1,2$ are assumed to be generated by a remote controller, which uses the angular information $q,\dot{q}$ transmitted through a wireless communication channel. With the received angular information, the control objective of the robotic arm is to track a predefined desired trajectory.

In the simulation, the length a_i and mass weight $m_i, i=1,2$ for the upper and lower links are set to be $m_1=1, a_1=2, m_2=0.1, a_2=10$. The desired angular trajectories are defined as two sinusoidal signal: $q_d=[g_1\sin(2\pi f_d t); g_2\sin(2\pi f_d t)]$ with desired amplitude $g_1=g_2=.1$ and frequency $f_d=.5s^{-1}$. The control input $F=[\tau_1;\tau_2]$ is computed by the following feedback linearization method [36], $F=M(\hat{q})(\ddot{q}_d-K[\hat{q}-q_d;\hat{\dot{q}}-\dot{q}_d])+V(\hat{q},\hat{\dot{q}}+G(\hat{q}))$ where $\hat{q},\hat{\dot{q}}$ are the estimates of the angular information depending on the real time channel conditions and K is the controller matrix gain $K=[5,0,5,0;0,5,0,5]$.

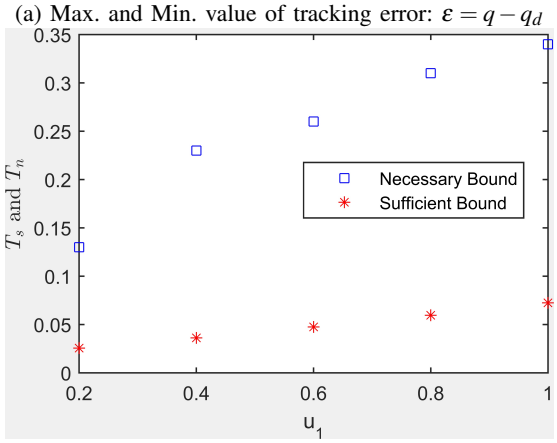
The wireless communication channel used by the robotic arm is subject to shadow fading which is directly related to the physical position of the forklift truck. In the simulation, the autonomous forklift system is modeled as a two state MDP as shown in Figure 3b where s_1 is the state representing the good channel region while the state s_2 characterizes the region causing shadow fading. $u_i, i=1,2$ are control strategies characterizing the probabilities of staying in state s_i given the current state s_i, i.e. $u_i=\Pr\{\text{“stay”}|s_i\}, i=1,2$. With this state-dependent fading channel, the transmitter in the robotic arm can select high power p_H level or low power p_L level, to adjust the outage probability as shown in the channel model (2). Table I shows the outage probabilities $\theta(s,p)$ for different power levels and MDP states

A. Almost Sure Safety

The first simulation result is to show almost sure safety for the two-link planar elbow arm system under the MATI in (11)



(a) Max. and Min. value of tracking error: $\varepsilon=q-q_d$



(b) Sufficient T_s and necessary T_n bounds on MATI

Fig. 4: Almost surely convergence of tracking error on angular states (Left Figure 4a); Comparison of sufficient and necessary MATI bounds under power and control strategies $\Pr\{p_H|s_i, i=1,2\}=1$ and $u_1=0.2,0.4,0.6,0.8,1$ (Right Figure 4b).

as well as to investigate the tightness of the MATI. A Monte Carlo simulation method is used to generate 1000 sample paths with each path being evolved over the same time interval from 0 to 8 seconds.

The transmission time interval $T=0.05\ s$ is selected to be smaller than the MATI bound τ^* under the control strategy $u_1=0.6, u_2=0.4$ and the power strategy $\Pr\{p_H|s_i, i=1,2\}=1$. Figure 4a shows the maximum value marked by the blue line, and the minimum value marked by the blue line of the tracking errors $(e_i,\dot{e}_i, i=1,2)$ over the 1000 sample paths. One can see from Figure 4a that the maximum and minimum values of the tracking errors asymptotically converge to zero as time increases. This is precisely the behavior that one would expect if the system is almost surely asymptotically stable. These results, therefore, seem to confirm our sufficient condition in (11) for almost sure safety.

The tightness of the sufficient conditions is investigated by comparing them against “necessary” bounds, which are obtained by an exhaustive search method. This exhaustive search method is to find a lower bound on the MATI such that the system violates the almost sure safety property. The procedure of this searching method starts with the sufficient

(Action, State)	s_1	s_2
Stay	1.5	1.
Go	.5	1
Power Level	p_H	p_L
Cost	2	.5

TABLE II: Control and Power Cost

MATI τ^* bound in (11), and then increases the value of τ^* until the maximum and minimum value of the sample path fail to converge to zero. The maximum value of τ that guarantees almost sure convergence in this search procedure would be the heuristic "necessary" bounds.

Figure 4b shows the comparison of the sufficient MATI bounds (red stars) obtained by (11) and necessary MATI bounds (blue squares) generated by the exhaustive search method under different control strategies $u_1 = 0.2, 0.4, 0.6, 0.8, 1$ and $u_2 = 1 - u_1$. As shown in the plot, the theoretical sufficient bounds are approximately 5 times conservative than the heuristic necessary bounds. This performance gap is reasonably close provided that the robotic arm networked system is highly nonlinear. In fact, similar conservativeness (around $6-8$ times) were also reported for deterministic networked systems in [28]. Our results can apply to a more general stochastic networked system but with similar gaps.

Note that u_1 represents the probability of staying in the good channel region while u_2 is the probability for the bad channel region where shadow fading occurs. Figure 4b also shows that the MATI increases when the probability of a good channel increases. This observation matches precisely with the argument that the control strategies from one system do have strong impacts on the network reliability of other systems. This finding motivates our co-design paradigm where the sufficient bound derived in (11) is a safety constraint that both the robotic arm system and the forklift system must satisfy, to achieve system safety and efficiency.

B. Safety and Efficiency: A Co-design Paradigm

This section demonstrates the effectiveness of the co-design paradigm by solving the constrained optimization problem in (14). In particular, the simulations in this section consist of two parts. The first part is to show that the optimal solutions of the constrained optimization problem (14) can be achieved asymptotically by solving relaxed convex GGPs using the branch-bound algorithm. The second part of the simulation is to show the necessity of our proposed co-design framework to achieve both system safety and efficiency by comparing it against the separation design framework proposed in [10].

In the simulation setup, the costs $c(s,a)$ and $c_p(p)$ defined in the constrained optimization problem (14) are shown in Table II to simulate a nontrivial scenario where the forklift truck is driven to the bad channel region s_2 to achieve its best interest. The co-design framework for the example of forklift and robotic arm is formulated as follows,

$$\underset{\{x_i\}_{i=1}^4,\{y_i\}_{i=1}^4}{\textbf{Minimize}} \quad \sum_{i=1}^{4} c_i x_i + 2\lambda \sum_{j=1}^{2} (y_{2j-1}c_p(p_H) + y_{2j}c_p(p_L))(x_{2j-1}+x_{2j}) \tag{31a}$$

$$\textbf{subject to} \quad \begin{cases} (1-\alpha)x_1 + x_2 - \alpha x_4 = (1-\alpha)\delta_0 \\ x_1 + x_2 + x_3 + x_4 = 1, \\ y_{2j-1} + y_{2j} = 1, j = 1,2 \\ y_i \geq 0, x_i \geq 0, \quad i = 1,2,3,4 \end{cases} \tag{31b}$$

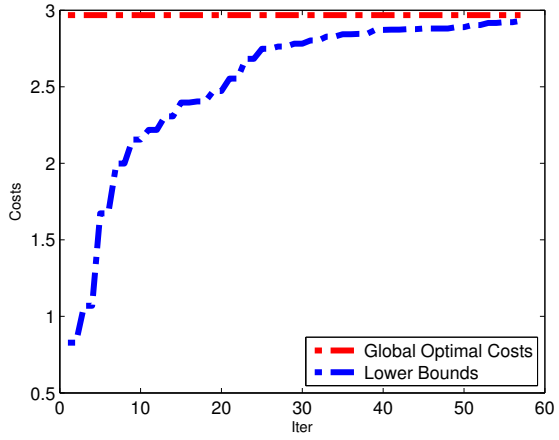
$$\begin{cases} \frac{x_1 y_1}{x_1+x_2}\theta(s_1) + \frac{x_4 y_3}{x_3+x_4}\theta(s_2) \leq c(T) \\ \frac{x_1 y_2}{x_1+x_2}\theta(s_1) + \frac{x_4 y_4}{x_3+x_4}\theta(s_2) \leq c(T) \\ \frac{x_2 y_1}{x_1+x_2}\theta(s_1) + \frac{x_3 y_3}{x_3+x_4}\theta(s_2) \leq c(T) \\ \frac{x_2 y_2}{x_1+x_2}\theta(s_1) + \frac{x_3 y_4}{x_3+x_4}\theta(s_2) \leq c(T) \end{cases} \tag{31c}$$

where $\{x_i\}$ and $\{y_i\}$ represent the decision variables related to the control and transmit power policies defined in Problem IV.3 $x_1 := \delta(s_1, \text{"Stay"}), y_1 := \Pr\{p_H|s_1\}, x_2 := \delta(s_1, \text{"Go"}), y_2 := \Pr\{p_L|s_1\}, x_3 := \delta(s_2, \text{"Stay"}), y_3 := \Pr\{p_H|s_2\}, x_4 := \delta(s_2, \text{"Go"}), y_4 := \Pr\{p_L|s_2\}$. The inequalities (31c) are the safety constraints and $\theta(s_i) = \theta(s_i, p_H) + \theta(s_i, p_L)$ is the dropout probability at state s_i whose value is shown in Table I. As discussed in Section IV, the parameter $c(T)$ is a function of the transmission time interval T and system parameters in the arm system (See Remark IV.2). Once T is selected, $c(T)$ is a fixed value. c_i is the system cost induced by the state in x_i, e.g. $c_2 = c(s_1, \text{"Go"})$ (See Table II). The other parameters in the simulation are: $\delta_0 = \Pr\{s(0) = s_1\} = 0.5$, $\alpha = 0.8$, and $\lambda = 1$.

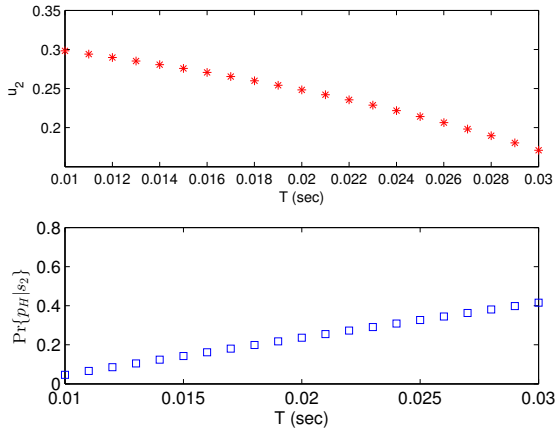
By using the GGP formulation and the branch-bound algorithm discussed in Section IV-A, Figure 5a shows that the lower bounds (blue dashed line) obtained by solving the relaxed convex GGP problem asymptotically approaches the optimal point (red dashed line) as the number of the iteration increases. This result confirms the arguments made in Theorem IV.10 which state that the global optimal solution is asymptotically achieved by the branch-bound algorithm.

The feasible region enclosed by the safety constraints (31c) shows a tight coupling between the control policies, the transmit power policies, and the transmission time interval T. Figure 5b shows the changes of the optimal control and power strategies as a function of the transmission time interval T. In particular, the upper plot of Figure 5b shows that the optimal control policies $u_2 := \Pr\{\text{"Stay"}|s_2\}$ (marked by red stars) for the forklift truck to stay at shadowing state s_2 monotonically decreases as the transmission time interval T increases. The bottom plot of Figure 5b shows that the optimal probabilities (marked by blue squares) of using high-level transmission power at bad channel region ($\Pr\{p_H|s_2\}$) increase monotonically as the transmission time interval T increases. These results imply that the overall system safety and efficiency is obtained by active coordinations between communication and control strategies.

Figure 6 shows the performance comparison between the proposed co-design framework and the separation design



(a) Asymptotic Convergence of Lower Bounds to Global Optimum with $T = 0.01$ sec



(b) Optimal control ($u_2 :=$ Pr{"Stay"$|s_2$}) and power policies (Pr$\{p_H|s_2\}$) at shadowing state s_2 for different transmission time intervals $T = 0.01 : 0.001 : 0.03$.

method under different transmission time intervals T (Figure 6a) and different fading levels (Figure 6b). In this separation design framework, the control and communication polices are designed separately to optimize their own individual interests. In particular, the optimal control policies $u_i^*, i = 1,2$ for the forklift truck are obtained by solving a linear program that is generated by eliminating the decision variables $y_i, i = 1,2,3,4$ and safety constraint (31c) in the optimization problem (31) and the optimal solutions are $x_1^* = 0, x_2^* = 0.1, x_3^* = 0.9, x_4^* = 0$. Thus, the optimal control policies are $u_2^* = 1, u_1^* = 0$ with the optimal cost 0.55. On the other hand, the optimal power policies for the robotic arm system are obtained by solving a linear programming problem as below that assumes the worst case impact of the forklift truck system,

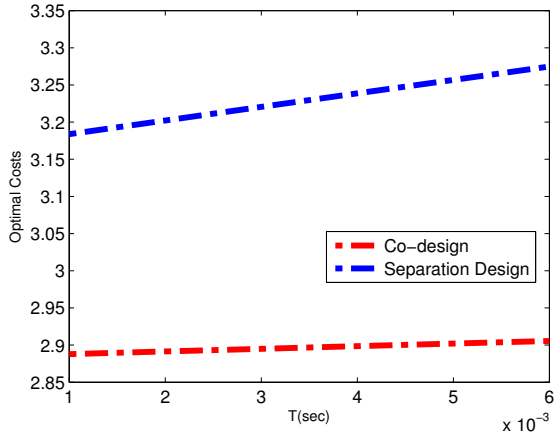
$$\underset{\{y_i\}_{i=1}^4}{\textbf{Minimize}} \quad (0.2y_1 + 1.8y_3)c_p(p_H) + (0.2y_2 + 1.8y_4)c_p(p_L) \tag{32a}$$

$$\textbf{subject to} \quad \begin{cases} y_1 + y_2 = 1 \\ y_3 + y_4 = 1 \\ y_1\theta(s_1) + y_3\theta(s_2) \le c(T) \\ y_2\theta(s_1) + y_4\theta(s_2) \le c(T) \\ y_i \ge 0, \quad i = 1,2,3,4 \end{cases} \tag{32b}$$

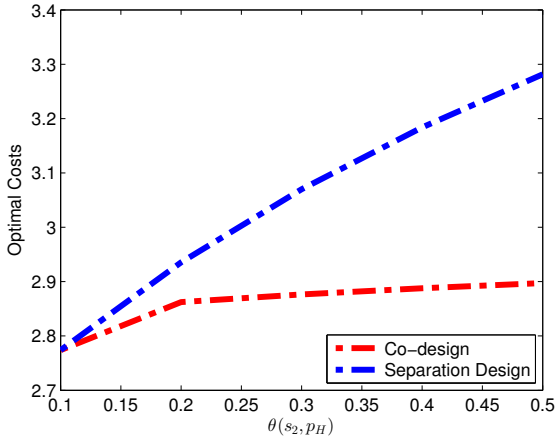
Note that the safe region generated by the constraints (32b) in the separation design problem is two times smaller than that generated by the co-design framework (31c). Indeed, the selected transmission time interval T in the co-design framework must satisfy $4c(T) > \theta(s_1) + \theta(s_2)$ to assure that the safe region is nonempty while the condition for the safe region to be nonempty in separation design is $2c(T) > \theta(s_1) + \theta(s_2)$. From the optimization's standpoint, although the co-design framework will for sure lead to better system performance than the separation design method due to its larger safe region, we are interested in investigating how the performance gap evolves as a function of T and the outage probability $\theta(s_2)$ under the co-design and separation design framework. The sensitivity analysis for these two frameworks is critical to ensuring a robust system design.

Figure 6a shows the overall optimal performance (power costs + system costs in MDP) achieved by the co-design (marked by red dashed line) and separation design (marked by blue dashed line) methods under the transmission time intervals T ranged from 0.001 *sec* to 0.006 *sec*. As expected, the optimal costs generated by the co-design method over the entire time interval are smaller than that under the separation method. Moreover, the performance gap between these two methods increases as the T increases from 0.001 sec to 0.006 sec. These results imply that the optimal performance achieved by the co-design method is less sensitive to the changes of T than that achieved by the separation design method. It is worth noting that the constrained optimization problem in (32) for the separation design method will be infeasible if T is larger than 0.006 sec.

Figure 6b shows the optimal performance comparison under different fading levels. In particular, the shadow fading level is categorized by different outage probability at the shadow state s_2. The value of the outage probability $\theta(s_2, p_H)$ at state s_2 is selected from 0.1 to 0.5 to simulate different levels of shadow fading. As shown in Figure 6b, the optimal costs achieved by the co-design framework (marked by red dashed line) are smaller than the those obtained by the separation design method (marked by blue dashed line) under all fading levels. Furthermore, the performance gap between these two methods is enlarged as the outage probability $\theta(s_2)$ in the bad channel region s_2 increases. In particular, the increase in optimal costs under the co-design framework flattens out even when the fading levels increases dramatically from 0.2 to 0.5.



(a) Optimal costs under different T



(b) Optimal costs under different fading levels $\theta(s_2, p_H)$

Fig. 6: The comparison of the optimal performance achieved by co-design and separation design frameworks under different transmission time intervals T from 0.001 sec to 0.006 sec (Figure 6a) and shadow fading levels $\theta(s_2, p_H) = 0.1 : 0.1 : 0.5$ (Figure 6b)

This simulation result suggests that the co-design method is more robust against the shadow fading than the separation method, and is resilient to significant communication degrations. The resilience of the co-design framework is particularly important and useful in factory automation systems where serious shadow fading is often present in wireless links.

VI. Conclusion

This paper examines the safety and efficiency of FANs in the presence of a *shadow fading channel* that varies as a function of the physical states. Sufficient conditions on MATI are presented to assure *almost sure asymptotic stability* without external disturbance and *stochastic stability in probability* with non-vanishing external disturbance. These safety conditions are shown to be dependent on the transmission power and the control policies. This observation motivates us to develop a co-design paradigm to ensure system efficiency under the safety constraint. The problem of safety-efficiency co-design is then addressed by solving a two-player constrained cooperative game. Furthermore, we show that the optimal solution to the constraint cooperative game is equivalent to the solution of a non-convex GGP problem. Two relaxed convex GGP were formulated to provide upper and lower bounds on the optimal solution. These bounds asymptotically converge to the global optima by using a branch-bound algorithm. The simulation results of a networked robotic arm and a forklift truck are used to illustrate our findings.

Our current paper focuses on the safety guarantee for the networked control system ($\mathscr{G}$ system) by co-designing efficient power policies and motion planning policies. It is, however, beyond the scope of this paper, if the objective of the co-design problem also includes ensuring system performance more than safety, e.g., optimal tracking control for the networked robotic arms. It is an important and interesting topic that will be pursued in our future work.

Appendix

Proof of Theorem III.4: The techniques used to prove the main results are based on the small gain theorem [37] and Markovian jump system theory [38]. One may view the stochastic hybrid system (1) as two interconnected subsystems (e and x) modulated with a stochastic jump process ($\{e(t_k)\}$). Let $\mathbb{I}_k := [t_k, t_{k+1})$ denote the k^{th} transmission time interval and $T_k := \tau_{k+1} - \tau_k, \forall k \in \mathbb{N}^+$ denote the transmission time interval for $\mathbb{I}_k$. Consider the error dynamics over $\mathbb{I}_k$ and suppose Assumption III.2 holds, one can use comparison principle to bound the error trajectory as $W(e(t)) \leq e^{L_1(t-t_k)}W(e(t_k^+)) + \int_{t_k}^{t} e^{L_1(t-s)}L_2|x|ds$. Then, one has

$$\begin{aligned} W(e(t_{k+1})) &\leq e^{L_1(t_{k+1}-t_k)}W(e(t_k^+)) + \int_{t_k}^{t_{k+1}} e^{L_1(t_{k+1}-s)}L_2|x|ds \\ &\leq e^{L_1 T_k}W(e(t_k^+)) + L_2|x|_{[t_k,t_{k+1})}\int_{t_k}^{t_{k+1}} e^{L_1(t_{k+1}-s)}ds \\ &= e^{L_1 T_k}W(e(t_k^+)) + \frac{L_2}{L_1}(e^{L_1 T_k}-1)|x|_{[t_k,t_{k+1})} \quad (33) \end{aligned}$$

The second inequality holds because $|x|_{[t_k,t_{k+1})} := \sup_{t_k \leq t < t_{k+1}}|x| \geq |x(\tau)|, \forall \tau \in \mathbb{I}_k$. Note that the inequality (33) holds for any given initial value $e(t_k^+)$. Moreover, $\{e(t_k^+)\}$ is a stochastic jump process that is governed by stochastic variations on the fading channel. Since the fading channel state in (2) depends on the probability measure of MDP state s and power state p, let $\mathbb{1}_A$ denote the indicator function that takes value 1 when sample value falls in set A and takes value 0 otherwise, then define the operator $W_{k+1}(s,p) \stackrel{\text{def}}{=} \mathbb{E}\{W(e(t_{k+1}))\mathbb{1}_{s_{k+1}=s, p_{k+1}=p}\}$ as the expectation of the $W(e(t_{k+1}))$ over the set $\{s_{k+1} = s, p_{k+1} = p\}$. Since $W(e) \geq 0, \forall e \in \mathbb{R}^n$, one can take this expectation operator on

both sides of (33) without changing the sign,

$$
\begin{aligned}
&W_{k+1}(s,p)\\
&\le e^{L_1T_k}\mathbb{E}\{W(e(t_k^+))\mathbb{1}_{s_{k+1}=s,p_{k+1}=p}\}+\frac{L_2}{L_1}(e^{L_1T_k}-1)\mathbb{E}\{|x|_{[t_k,t_{k+1})}\mathbb{1}_{s,p}\}\\
&=e^{L_1T_k}\sum_{s'\in S,p'\in\Omega_p}\mathbb{E}\{W(e(t_k^+))\mathbb{1}_{s',p'}\}\Pr\{s,p|s',p'\}\\
&\quad+\frac{L_2}{L_1}(e^{L_1T_k}-1)|x|_{[t_k,t_{k+1})}\mathbb{E}\{\mathbb{1}_{s,p}\} \qquad (34)\\
&=e^{L_1T_k}\sum_{s'\in S,p'\in\Omega_p}W_k(s',p')\theta(s',p')\Pr\{s,p|s',p'\}\\
&\quad+\frac{L_2}{L_1}(e^{L_1T_k}-1)|x|_{[t_k,t_{k+1})}\mathbb{E}\{\mathbb{1}_{s,p}\} \qquad (35)
\end{aligned}
$$

The first Equality (34) holds due to the Markovian property of the MDP and power processes. The second Equality (35) holds as a result of Proposition III.3 and $\mathbb{E}\{W(e(t_k^+))\mathbb{1}_{s_k=s',p_k=p'}\}=\mathbb{E}\{W(e(t_k^+))|s_k=s,p_k=p'\}\Pr\{s_k=s',p_k=p'\}$. Let $W_k:=[W_k(s_1,p_1),W_k(s_1,p_2),\dots,W_k(s_{|S|},|\Omega_p|)]^T$, then

$$
W_{k+1}\le e^{L_1T_k}P_m\mathrm{diag}(\theta(s,p))W_k+\frac{L_2}{L_1}(e^{L_1T_k}-1)|x|_{[t_k,t_{k+1})}[\mathbb{E}\{\mathbb{1}_{s,p}\}] \qquad (36)
$$

where

$$
\mathrm{diag}(\theta(s,p)):=\begin{bmatrix}\theta(s_1,p_1)&\cdots&0&\cdots&0\\ \vdots&\ddots&\vdots&\ddots&\vdots\\ 0&\cdots&\theta(s_i,p_j)&\cdots&0\\ \vdots&\ddots&\vdots&\ddots&\vdots\\ 0&\cdots&0&\cdots&\theta(s_N,p_M)\end{bmatrix},
$$

$$
[\mathbb{E}\{\mathbb{1}_{s,p}\}]:=\begin{bmatrix}\mathbb{E}\{\mathbb{1}_{s_1,p_1}\}\\ \vdots\\ \mathbb{E}\{\mathbb{1}_{s_i,p_j}\}\\ \vdots\\ \mathbb{E}\{\mathbb{1}_{s_{|S|},p_{|\Omega_p|}}\}\end{bmatrix}
$$

and

$$
P_m(\pi_\infty^m,\pi_\infty^p):=\begin{bmatrix}\Pr(s_1,p_1|s_1,p_1)&\cdots&\Pr(s_1,p_1|s_N,p_M)\\ \Pr(s_1,p_2|s_1,p_1)&\cdots&\Pr(s_2,p_1|s_N,p_M)\\ \vdots&\vdots&\vdots\\ \Pr(s_N,p_M|s_1,p_1)&\cdots&\Pr(s_N,p_M|s_N,p_M)\end{bmatrix}_{NM\times NM}
$$

Since both sides of (36) are positive, taking the ∞-norm on both sides of (36) leads to

$$
\begin{aligned}
&|W_{k+1}|\\
&\le e^{L_1T_k}\underbrace{\|P_m\mathrm{diag}(\theta(s,p))\|}_{P_\infty}|W_k|+\frac{L_2}{L_1}(e^{L_1T_k}-1)|\underbrace{[\mathbb{E}\{|x|_{[t_k,t_{k+1})}\mathbb{1}_{s,p}\}]}_{X_{[k,k+1)}}|\\
&\le\frac{L_2}{L_1}(e^{L_1T^*}-1)\Big(|X_{[k,k+1)}|+e^{L_1T^*}P_\infty|X_{[k-1,k)}|+\cdots\\
&\quad+\big(e^{L_1T^*}P_\infty\big)^k|X_{[0,1)}|\Big)+\Big(e^{L_1T^*}P_\infty\Big)^{k+1}|W_0|\\
&\le\frac{L_2}{L_1}(e^{L_1T^*}-1)\sum_{i=0}^{\infty}\Big(e^{L_1T^*}P_\infty\Big)^i|X_{[0,k+1)}|+\Big(e^{L_1T^*}P_\infty\Big)^{k+1}|W_0|\\
&=\frac{L_2}{L_1}(e^{L_1T^*}-1)\frac{1}{1-e^{L_1T^*}P_\infty}|X_{[0,k+1)}|+\Big(e^{L_1T^*}P_\infty\Big)^{k+1}|W_0| \qquad (37)
\end{aligned}
$$

where $T^*=\max_{0\le i\le k}T_k$. Clearly, (37) shows that the W system is input to state stable with respect to $X_{[0,k+1]}$ with linear gain $\frac{L_2}{L_1}(e^{L_1T^*}-1)\frac{1}{1-e^{L_1T^*}P_\infty}$ if $e^{L_1T^*}P_\infty<1$.

Since $\underline{w}|e|\le W(e)\le\overline{w}|e|$, it is straightforward to conclude that the error dynamic system is also input to state stable in expectation as follows,

$$
|E_{k+1}|\le\frac{L_2}{L_1\overline{w}}(e^{L_1T^*}-1)\frac{1}{1-e^{L_1T^*}P_\infty}|X_{[0,k+1)}|+\frac{\underline{w}\Big(e^{L_1T^*}P_\infty\Big)^{k+1}}{\overline{w}}|E_0| \qquad (38)
$$

where $E_{k+1}:=[E_{k+1}(s_1,p_1),\dots,E_{k+1}(s_i,p_j),\dots,E_{k+1}(s_{|S|},p_{|\Omega_p|})]$ with $E_{k+1}(s_i,p_j)=\mathbb{E}\{|e(t_{k+1})|\mathbb{1}_{s_i,p_j}\}$.

Similarly, let $X_t(s,p):=\mathbb{E}\{|x(t)|\mathbb{1}_{s,p}\}$ denote the expectation of $|x(t)|$ over the set s,p. By Assumption III.1 and $\gamma_1(s)\le\overline{\gamma}_1 s,\forall s>0$, one has

$$
\begin{aligned}
X_t(s,p)&\le\mathbb{E}\{\beta(|x(t_0)|,t-t_0)\mathbb{1}_{s,p}\}+\overline{\gamma}_1\mathbb{E}\{|e|_{[t_0,t)}\mathbb{1}_{s,p}\}\\
&\le\beta(\mathbb{E}\{|x(t_0)|\mathbb{1}_{s,p}\},t-t_0)+\overline{\gamma}_1\mathbb{E}\{|e|_{[t_0,t)}\mathbb{1}_{s,p}\}\\
&=\beta(X_0(s,p),t-t_0)+\overline{\gamma}_1E_{[t_0,t)}(s,p)
\end{aligned}
$$

then similar to the derivation of (38), one has

$$
|X_t|\le\beta(|X_0|,t-t_0)+\overline{\gamma}_1|E_{[t_0,t)}| \qquad (39)
$$

Consider the ISS characterizations of subsystem X in (39) and subsystem E in (38), from the well-established small gain theorem [39], the interconnected system X and E is asymptotically stable if

$$
\frac{L_2}{L_1\overline{w}}(e^{L_1T^*}-1)\frac{1}{1-e^{L_1T^*}\|P_m\mathrm{diag}(\theta(s,p))\|}\overline{\gamma}_1<1 \qquad (40)
$$

It is easy to show that the small-gain condition in (40) leads to the sufficient condition in (11). Since $\mathbb{E}\{|x(t)|\}\le|X_t|,\forall t\ge0$ and the subsystem X is asymptotically stable, there exists a class $\mathscr{KL}$ function $\overline{\beta}(s,t)$ such that $\mathbb{E}\{|x(t)|\}\le\overline{\beta}(|x(0)|,t)$. The proof is complete. ■

Proof of Theorem III.6: Under the Exp-ISS assumption in Assumption III.1, by following the same argument used in proving Theorem III.4, one can show that the networked control system $\mathscr{G}$ is exponentially stable in expectation with respect to origin, i.e., there exists a class Exp-$\mathscr{KL}$ function $\beta(s,t)=K_1\exp(-K_2t)s$ such that $\forall x(0)\in\Omega_s$, $\mathbb{E}[|x(t)|]\le K_1\exp(-K_2t)|x(0)|,\forall t\in\mathbb{R}_{\ge0}$. Let $\tau'>\tau\ge0$ denote any time instants such that $\tau\le t<\tau'$ holds, then for any given $\varepsilon>0$ and the safe set $\Omega_s=\{x\in\mathbb{R}^{n_x+n_c}||x|\le r\}$ with $r\ge0$, consider

the following probability bound

$$\begin{aligned}\Pr\{\sup_{\tau\le t<\tau'}|x(t)|\ge\varepsilon+r\}&\le\Pr\left\{\int_\tau^{\tau'}|x(t)|dt\ge\varepsilon+r\right\}\\&\overset{(a)}{\le}\mathbb{E}\left\{\int_\tau^{\tau'}|x(t)|dt\right\}/(\varepsilon+r)\overset{(b)}{\le}\int_\tau^{\tau'}\mathbb{E}\{|x(t)|\}dt/(\varepsilon+r)\\&\le\int_\tau^{\tau'}K_1\exp(-K_2t)|x(0)|dt/(\varepsilon+r)\\&\le\frac{K_1|x(0)|}{K_2\varepsilon'}[\exp(-K_2\tau)-\exp(-K_2\tau')]\end{aligned}$$

where inequality (a) holds due to the Markov inequality and inequality (b) holds by exchanging the expectation and integration due to the measurability and boundedness of $|x(t)|$ over time interval $[\tau,\tau')$. Let $\tau'\to+\infty$, then one has

$$\Pr\{\sup_{\tau<t}|x(t)|\ge\varepsilon+r\}\le\frac{K_1|x(0)|}{K_2(\varepsilon+r)}\exp(-K_2\tau)\le\frac{K_1|x(0)|}{K_2(\varepsilon+r)}.$$

Let $\varepsilon':=\frac{K_1|x(0)|}{K_2(\varepsilon+r)}$, and then there exists a function $\delta(\varepsilon,\varepsilon',r)=\frac{\varepsilon'K_2(\varepsilon+r)}{K_1}$ such that

$$\Pr\{\sup_{\tau\le t}|x(t)|\ge\varepsilon+r\}\le\varepsilon',\forall|x(0)|\le\delta(\varepsilon,\varepsilon',r).$$

Since $\tau\ge0$ is arbitrarily chosen, by taking $\tau\to+\infty$, the networked system $\mathscr{G}$ is almost surely asymptotically stable due to

$$\lim_{\tau\to\infty}\Pr\{\sup_{\tau\le t}|x(t)|\ge\varepsilon+r\}\le\lim_{\tau\to\infty}\frac{K_1|x(0)|}{K_2(\varepsilon+r)}\exp(-K_2\tau)=0.$$

The proof is complete. ∎

Proof of Theorem III.7: Following the argument and notation in the proof of Theorem III.4, similar to inequalities (38) and (39) one has the interconnected systems with $|w|_{\mathscr{L}_\infty}\le M_w$ defined as follows

$$\begin{aligned}|E_{k+1}|&\le\frac{\underline{w}\left(e^{L_1T^*}P_\infty\right)^{k+1}}{\overline{w}}|E_0|+\frac{L_2(e^{L_1T^*}-1)}{L_1\overline{w}(1-e^{L_1T^*}P_\infty)}|X_{[0,k+1)}|\\&+\frac{L_3(e^{L_1T^*}-1)}{L_1\overline{w}(1-e^{L_1T^*}P_\infty)}|[\mathbb{E}\{|w|_{[t_k,t_{k+1})}\mathbb{1}_{s,p}\}]|\\|X_t|&\le\beta(|X_0|,t-t_0)+\overline{\gamma}_1|E_{[t_0,t)}|+|[\mathbb{E}\{\gamma_2|w|_{[t_k,t_{k+1})}\mathbb{1}_{s,p}\}]|\end{aligned}$$

Since the small gain condition holds for any transmission time interval $T^*\le\tau^*$ where τ^* is defined in (11), one can apply the argument in [39] to conclude that the composite system state $C_k:=[E_k,X_k]$ is input to state stable with respect to w, i.e., there exists a class $\mathscr{KL}$ function $\overline{\beta}(\cdot,\cdot)$ and a class $\mathscr{K}$ function $\kappa(\cdot)$ such that $|C_k|\le\overline{\beta}(|C_0|,kT^*)+\kappa(M_w)$. Let $\Omega_s:=\{x\in\mathbb{R}^n||x|\le\Delta_s\}$ denote the bounded safe set, then for any $\varepsilon>0$, the stochastic safety in probability can be characterized as

$$\begin{aligned}\Pr\{|x(t)|\ge\Delta_s+\varepsilon\}&\le\frac{\mathbb{E}(|x(t)|)}{\Delta_s+\varepsilon}\le\frac{|S||\Omega_p||C_k|}{\Delta_s+\varepsilon}\\&\le|S||\Omega_p|\frac{\overline{\beta}(|C_0|,kT^*)+\kappa(M_w)}{\Delta_s+\varepsilon}\end{aligned}$$

The first Inequality holds due to the Markov's inequality. The second inequality holds because $\mathbb{E}(|x(t)|)=\sum_{s\in S,p\in\Omega_p}X_t(s,p)\le|S||\Omega_p||X_t|$ and $|X_t|\le|C_t|$. One thus has $\lim_{t\to\infty}\Pr\{|x(t)|\ge\Delta_s+\varepsilon\}\le\underbrace{|S||\Omega_p|\frac{\kappa(M_w)}{\Delta_s+\varepsilon}}_{\delta}$. The proof is complete. ∎

Proof of Lemma IV.6:

1) Proof of First Part: : Let $\Delta_i=A_iZ+B_i-\tilde{G}_i^-(Z)$ denote the gap and $\Delta_{ij}=\overline{A}_{ij}Z+\overline{B}_{ij}-\tilde{G}_{ij}^-(Z)$ denote the gap for each term in $\tilde{G}_i^-(Z)$ where $\overline{A}_{ij}:=a_{ij}A_{ij}[b_{ij1},\dots,b_{ijn}],\overline{B}_{ij}:=a_{ij}B_{ij}$ and $\tilde{G}_{ij}^-(Z):=a_{ij}\exp\sum_{l=1}^n b_{ijl}z_l,\forall j\in L_i^-$. Since

$$\begin{aligned}A_i=\sum_{j\in L_i^-}\overline{A}_{ij},\quad B_i=\sum_{j\in L_i^-}\overline{B}_{ij}\\\tilde{G}_i^-(Z)=\sum_{j\in L_i^-}\tilde{G}_{ij}^-(Z),\quad\Delta_i=\sum_{j\in L_i^-}\Delta_{ij}\end{aligned}$$

and $\Delta_i^*:=\max_{Z\in\Omega_Z}\Delta_i=\max_{Z\in\Omega_Z}(A_iZ+B_i-\tilde{G}_i^-(Z))\le\sum_{j\in L_i^-}\max_{Z\in\Omega_Z}\Delta_{ij}:=\sum_{j\in L_i^-}\Delta_{ij}^*$, one can evaluate the maximum gap between the posynomial function and its linear approximation by examining the maximum gap for each term in the posynomial function. Specifically, the maximum point in Δ_{ij} can be obtained by $Z^*=\arg\max_{Z\in\Omega_Z}\Delta_{ij}(Z)\Leftrightarrow\frac{\partial\Delta_{ij}}{\partial Z}=0$. with $\frac{\partial\Delta_{ij}}{\partial Z}=\overline{A}_{ij}-\frac{\partial\tilde{G}_{ij}^-(Z)}{\partial Z},\frac{\partial\tilde{G}_{ij}^-(Z)}{\partial Z}=a_{ij}[b_{ij1},b_{ij2},\dots,b_{ijn}]e^{\sum_{j\in L_i^-}b_{ijl}z_l}$ and $\overline{A}_{ij}:=a_{ij}A_{ij}[b_{ij1},\dots,b_{ijn}]$.

Since $\sum_{j\in L_i^-}b_{ijl}z_l^*=\log A_{ij},\Delta_{ij}^*=a_{ij}\left(A_{ij}(\log A_{ij}-1)+B_{ij}\right)$ with $A_{ij}=\frac{\exp(Y_{ij}^L+\delta_{ij})-\exp Y_{ij}^L}{\delta_{ij}},B_{ij}=\frac{(Y_{ij}^L+\delta_{ij})\exp(Y_{ij}^L)-Y_{ij}^L\exp(Y_{ij}^L+\delta_{ij})}{\delta_{ij}}$, one has $\Delta_{ij}^*=e^{Y_{ij}^L}\left(1-\Theta_{ij}+\Theta_{ij}\log(\Theta_{ij})\right)$ with $\Theta_{ij}=\frac{e^{\delta_{ij}}-1}{\delta_{ij}}$. Because $\Delta_i^*\le\sum_{j\in L_i^-}\Delta_{ij}^*$, one finally has

$$\begin{aligned}\Delta_i^*&\le\sum_{j\in L_i^-}e^{Y_{ij}^L}\left(1-\Theta(\delta_{ij})+\Theta(\delta_{ij})\log(\Theta(\delta_{ij}))\right)\\&\le|L_i^-|e^{Y_i^L}\left(1-\Theta(\delta_i)+\Theta_i\log(\Theta(\delta_i)\right)\end{aligned}$$

where $e^{Y_i^L}=\max_{j\in L_i^-}e^{Y_{ij}^L}$ and $\Theta(\delta)=\frac{e^\delta-1}{\delta}$. The second inequality holds because $\Theta(\delta)$ is a monotonically increasing function with respect to any $\delta\in\mathbb{R}_{\ge0}$ and $\Theta(\delta_{ij})\le\Theta(\delta_i)$ due to $\delta_i=\max_{j\in L_i^-}\delta_{ij}$. The first part of the proof is complete.

2) Proof of Second Part: : Note that $\Theta_{ij}\to1\Leftrightarrow\delta_{ij}\to0$ and the Taylor expansion of function $\log(\Theta_{ij})$ at $\Theta_{ij}=1$ is $\log(\Theta_{ij})=(\Theta_{ij}-1)-\frac{1}{2}(\Theta_{ij}-1)^2+\frac{1}{3}(\Theta_{ij}-1)^3-\cdots$, then

$$\begin{aligned}&1-\Theta_{ij}+\Theta_{ij}\log(\Theta_{ij})\\&=(\Theta_{ij}-1)^2\underbrace{(1-\frac{1}{2}\Theta_{ij})}_{>0\text{ around }\Theta_{ij}=1}+\Theta_{ij}(\Theta_{ij}-1)^3\underbrace{(\frac{7}{12}-\frac{1}{4}\Theta_{ij})}_{>0\text{ around }\Theta_{ij}=1}+\cdots\end{aligned}$$

Taking the Taylor expansion for function $e^{\delta_{ij}}$ at point 0, one further has $\Theta_{ij}(\delta_{ij})-1=\frac{1}{2!}\delta_{ij}+\frac{1}{3!}\delta_{ij}^2+\cdots$. Thus, $\Delta_{ij}^*\sim\mathscr{O}(\delta_{ij}^2)$. Since $\Delta_i^*\le\sum_{j\in L_i^-}\Delta_{ij}^*$, then $\Delta_i^*\sim\mathscr{O}(\delta_i^2)$. The second part of the proof is complete. ∎

Proof of Theorem IV.10: The proof is based on the

perturbation analysis for the non-convex optimization problem [40]. Let the non-convex GGP problem in (16) denote the unperturbed nominal optimization and the relaxed convex problems (19) and (21) denote the perturbed optimization defined as follows,

$$\begin{aligned} \underset{Z}{\text{minimize}} \quad & \tilde{G}_0(Z,u_0) \\ \text{subject to} \quad & \tilde{G}_i(Z,u_i) \leq 0, \quad i=1,\ldots,M \\ & Z \in \Omega_Z \end{aligned} \tag{41}$$

where $u_i = \tilde{G}_i^s(Z) - \tilde{G}_i(Z), s = H,L$ represents the perturbation term and $|u_i| \leq \Delta_i^*(\delta_i)$ with Δ_i^* defined in Lemma IV.6. Let $\nu(u)$ denote the optimal value of the perturbed optimization problem in (41) which is a function of u. By Lemma IV.6 and IV.7, let $\Phi(\delta) = \{u \in \mathbb{R}^{M+1} \big| |u| \leq \Delta(\delta)\}$ denote a compact set with $\delta = \max_{0\leq i\leq M} \delta_i$, the objective is to show how optimal solutions $Z^*(u)$ of the perturbed optimization problem in (41) and optimal value $\nu(u)$ for any $u \in \Phi(\delta)$ converge to the optimal solutions of the unperturbed problem when $\delta \to 0$. First, it is easy to show that $Z^*(0) = \lim_{\delta\to 0} Z^*(u)$ and $\nu(0) = \lim_{\delta\to 0}\nu(u)$ since $\delta \to 0 \Longrightarrow u \to 0$ and $\tilde{G}_i(Z,u_i), \forall i = 0,1,\ldots,M$ is smooth with respect to both Z and u. Furthermore, one knows that $|u| = \mathscr{O}(\delta^2)$ as $\delta \to 0$ by Lemma IV.6. Thus, one can define the perturbation path, along a direction $d \in \mathbb{R}^{M+1}$, in the parameter space $\Phi(\delta)$ as $u(\delta) = u_0 + \delta^2 d + \mathscr{O}(\delta^3)$. The vector d characterizes the perturbation directions for the constraint functions and objective function in optimization problem in (41). For example, $d = [0,0,\ldots,\underbrace{+1}_{i+1},\ldots,M]^T$ represents the positive perturbation occurring at i^{th} constraint function. Note that the branch procedure defined in the branch-bound algorithm defines the perturbation direction d. Let Z^* denote the optimal solution for the unperturbed problem and $\tilde{G}_0(Z^*,u_0)$ denote the optimal value. Let h_i denote any feasible direction such that the directional regularity $DG_i(Z^*,u_0)(h_i,d_i) < 0, i = 1,2,\ldots,M$ holds (see Section 4.2 in [40]). Since $u_0 = 0$ represents the unperturbed problem, for any perturbed problem along the path $u(t) = \delta^2 d + \mathscr{O}(\delta^3)$, one has $|Z^*(u) - Z^*| = \mathscr{O}(\delta)$ by Theorem 4.53 in [40]. It is easy to verify that the lower and upper bounds Z^{H^*} and Z^{L^*} generated by the branch-bound algorithm correspond to the cases $Z^*(u)$ when perturbation directions d are selected oppositely.

The branch-bound algorithm is a bisection method whose data structure forms a binary tree. By (29) or (30), one can define desired optimality gap as δ^*, then for a given initial gap $\delta_0 > \delta^*$, the maximum number of bisections Nb that are needed to achieve δ^* for a n-dimensional variable Z is $Nb = \left\lceil \frac{\delta^0}{\delta^*} \right\rceil^n$. Note that the relationship between binary tree depth and the number of bisections is $Nb = 2^{DB} - 1$. One has $DB = \log_2\left(\left\lceil \frac{\delta^0}{\delta^*} \right\rceil^n + 1\right)$. Since optimality gap satisfies (29) and (30), one has the final conclusion and the proof is complete. ■

REFERENCES

[1] L. Zhuang, K. M. Goh, and J.-B. Zhang, "The wireless sensor networks for factory automation: issues and challenges," in *Emerging Technologies and Factory Automation, 2007. ETFA. IEEE Conference on*. IEEE, 2007, pp. 141–148.

[2] A. Rajhans, A. Bhave, I. Ruchkin, B. H. Krogh, D. Garlan, A. Platzer, and B. Schmerl, "Supporting heterogeneity in cyber-physical systems architectures," *Automatic Control, IEEE Transactions on*, vol. 59, no. 12, pp. 3178–3193, 2014.

[3] F. De Pellegrini, D. Miorandi, S. Vitturi, and A. Zanella, "On the use of wireless networks at low level of factory automation systems," *Industrial Informatics, IEEE Transactions on*, vol. 2, no. 2, pp. 129–143, 2006.

[4] M. P. Groover, *Automation, production systems, and computer-integrated manufacturing*. Prentice Hall Press, 2007.

[5] K. Islam, W. Shen, and X. Wang, "Wireless sensor network reliability and security in factory automation: A survey," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 42, no. 6, pp. 1243–1256, 2012.

[6] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[7] P. Agrawal, A. Ahlén, T. Olofsson, and M. Gidlund, "Long term channel characterization for energy efficient transmission in industrial environments," *IEEE Transactions on Communications*, vol. 62, no. 8, pp. 3004–3014, 2014.

[8] D. E. Quevedo, A. Ahlen, and K. H. Johansson, "State estimation over sensor networks with correlated wireless fading channels," *Automatic Control, IEEE Transactions on*, vol. 58, no. 3, pp. 581–593, 2013.

[9] I. Kashiwagi, T. Taga, and T. Imai, "Time-varying path-shadowing model for indoor populated environments," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 1, pp. 16–28, 2010.

[10] K. Gatsis, A. Ribeiro, and G. J. Pappas, "Optimal power management in wireless control systems," *Automatic Control, IEEE Transactions on*, vol. 59, no. 6, pp. 1495–1510, 2014.

[11] S. Tatikonda and S. Mitter, "Control over noisy channels," *Automatic Control, IEEE Transactions on*, vol. 49, no. 7, pp. 1196–1201, 2004.

[12] N. Elia, "Remote stabilization over fading channels," *Systems & Control Letters*, vol. 54, no. 3, pp. 237–249, 2005.

[13] Q. Zhang, S. Kassam *et al.*, "Finite-state markov model for Rayleigh fading channels," *Communications, IEEE Transactions on*, vol. 47, no. 11, pp. 1688–1692, 1999.

[14] H. S. Wang and N. Moayeri, "Finite-state markov channel-a useful model for radio communication channels," *Vehicular Technology, IEEE Transactions on*, vol. 44, no. 1, pp. 163–171, 1995.

[15] P. Agrawal and N. Patwari, "Correlated link shadow fading in multi-hop wireless networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 8, 2009.

[16] A. S. Leong, D. E. Quevedo, A. Ahlén, and K. H. Johansson, "On network topology reconfiguration for remote state estimation," *IEEE Transactions on Automatic Control*, vol. 61, no. 12, pp. 3842–3856, 2016.

[17] B. Hu and M. D. Lemmon, "Using channel state feedback to achieve resilience to deep fades in wireless networked control systems," in *Proceedings of the 2nd ACM international conference on High confidence networked systems*. ACM, 2013, pp. 41–48.

[18] ——, "Distributed switching control to achieve almost sure safety for leader-follower vehicular networked systems," *IEEE Transactions on Automatic Control*, vol. 60, no. 12, pp. 3195–3209, 2015.

[19] G. Caire, G. Taricco, and E. Biglieri, "Optimum power control over fading channels," *Information Theory, IEEE Transactions on*, vol. 45, no. 5, pp. 1468–1489, 1999.

[20] A. J. Goldsmith and S.-G. Chua, "Variable-rate variable-power MQAM for fading channels," *Communications, IEEE Transactions on*, vol. 45, no. 10, pp. 1218–1230, 1997.

[21] D. E. Quevedo, J. Ostergaard, and A. Ahlen, "Power control and coding formulation for state estimation with wireless sensors," *Control Systems Technology, IEEE Transactions on*, vol. 22, no. 2, pp. 413–427, 2014.

[22] S. Tatikonda and S. Mitter, "Control under communication constraints," *Automatic Control, IEEE Transactions on*, vol. 49, no. 7, pp. 1056–1068, 2004.

[23] B. G. N. Nair, F. Fagnani, S. Zampieri, and R. J. Evans, "Feedback control under data rate constraints: An overview," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 108–137, 2007.

[24] A. Molin and S. Hirche, "On LQG joint optimal scheduling and control under communication constraints," in *Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference. CDC/CCC 2009. Proceedings of the 48th IEEE Conference on*. IEEE, 2009, pp. 5832–5838.

[25] G. Di Girolamo, A. D'Innocenzo, and M. Di Benedetto, "Co-design of controller and routing redundancy over a wireless network," *IFAC-PapersOnLine*, vol. 48, no. 22, pp. 100–105, 2015.

[26] L. Bao, M. Skoglund, and K. H. Johansson, "Iterative encoder-controller design for feedback control over noisy channels," *IEEE Transactions on Automatic Control*, vol. 56, no. 2, pp. 265–278, 2011.
[27] S. Özekici, "Markov modulated bernoulli process," *Mathematical Methods of Operations Research*, vol. 45, no. 3, pp. 311–324, 1997.
[28] D. Nešić and A. R. Teel, "Input-output stability properties of networked control systems," *Automatic Control, IEEE Transactions on*, vol. 49, no. 10, pp. 1650–1667, 2004.
[29] S. Boyd, S.-J. Kim, L. Vandenberghe, and A. Hassibi, "A tutorial on geometric programming," *Optimization and engineering*, vol. 8, no. 1, pp. 67–127, 2007.
[30] C. D. Maranas and C. A. Floudas, "Global optimization in generalized geometric programming," *Computers & Chemical Engineering*, vol. 21, no. 4, pp. 351–369, 1997.
[31] L. Zhang and D. Hristu-Varsakelis, "Communication and control co-design for networked control systems," *Automatica*, vol. 42, no. 6, pp. 953–958, 2006.
[32] H. Kushner, *Stochastic stability and control*. Academic Press, New York, 1967.
[33] R. Khasminskii, *Stochastic stability of differential equations*. Springer Science & Business Media, 2011, vol. 66.
[34] E. Altman, *Constrained Markov decision processes*. CRC Press, 1999, vol. 7.
[35] L. Vandenberghe and S. Boyd, "Semidefinite programming," *SIAM Review*, vol. 38, no. 1, pp. 49–95, 1996. [Online]. Available: http://dx.doi.org/10.1137/1038003
[36] F. L. Lewis, D. M. Dawson, and C. T. Abdallah, *Robot manipulator control: theory and practice*. CRC Press, 2003.
[37] A. Isidori, *Nonlinear control systems*. Springer Science & Business Media, 1995.
[38] O. L. V. Costa, M. D. Fragoso, and R. P. Marques, *Discrete-time Markov jump linear systems*. Springer Science & Business Media, 2006.
[39] Z.-P. Jiang, A. R. Teel, and L. Praly, "Small-gain theorem for ISS systems and applications," *Mathematics of Control, Signals and Systems*, vol. 7, no. 2, pp. 95–120, 1994.
[40] J. F. Bonnans and A. Shapiro, *Perturbation analysis of optimization problems*. Springer Science & Business Media, 2013.

PLACE PHOTO HERE

Bin Hu received the B.S. degree in automation from Hefei University of Technology, Hefei, China, in 2007, the M.S. degree in control and system engineering from Zhejiang University, Hangzhou, China, in 2010, and the Ph.D. degree in electrical engineering from the University of Notre Dame, Notre Dame, IN, USA in 2016. His research interests include stochastic networked control systems, information theory, switched control systems, distributed control and optimization, and human machine interaction.

PLACE PHOTO HERE

Yebin Wang received the B.Eng. degree in Mechatronics Engineering from Zhejiang University, China, in 1997, M.Eng. degree in Control Theory & Engineering from Tsinghua University, China, in 2001, and Ph.D. in Electrical Engineering from the University of Alberta, Canada, in 2008. Dr. Wang has been with Mitsubishi Electric Research Laboratories in Cambridge, MA, USA, since 2009, and now is a Senior Principal Research Scientist. From 2001 to 2003 he was a Software Engineer, Project Manager, and R&D Manager in industries, Beijing, China. His research interests include nonlinear control and estimation, optimal control, adaptive systems and their applications including mechatronic systems.

PLACE PHOTO HERE

Philips Orlik was born in New York, NY in 1972. He received the B.E. degree in 1994 and the M.S. degree in 1997 both from the State University of New York (SUNY) at Stony Brook. In 1999 he earned his Ph. D. in electrical engineering also from SUNY Stony Brook. He is currently the Group Manager of Electronics & Communications at Mitsubishi Electric Research Laboratories Inc. located in Cambridge, MA. His primary research focus is on advanced wireless and mobile cellular communications, sensor networks, ad-hoc networking and UWB. Other research interests include vehicular/car-to-car communications, mobility modeling, performance analysis, and queuing theory.

PLACE PHOTO HERE

Toshiaki Koike-Akino (M'05-SM'11) received the B.S. degree in electrical and electronics engineering, M.S. and Ph.D. degrees in communications and computer engineering from Kyoto University, Kyoto, Japan, in 2002, 2003, and 2005, respectively. During 20062010, he has been a Postdoctoral Researcher at Harvard University, and joined Mitsubishi Electric Research Laboratories, Cambridge, MA, USA, since 2010. His research interest includes digital signal processing for data communications and sensing. He received the YRP Encouragement Award 2005, the 21st TELECOM System Technology Award, the 2008 Ericsson Young Scientist Award, the IEEE GLOBECOM'08 Best Paper Award in Wireless Communications Symposium, the 24th TELECOM System Technology Encouragement Award, and the IEEE GLOBECOM'09 Best Paper Award in Wireless Communications Symposium.

PLACE PHOTO HERE

Jianlin Guo is a Senior Principal Research Scientist at Mitsubishi Electric Research Laboratories in Cambridge, Massachusetts, USA. He received his Ph.D. in Applied Mathematics in 1995 from University of Windsor, Windsor, Ontario, Canada. His research interests include routing and resource management in wireless IoT networks, coexistence of the heterogeneous wireless networks, control over wireless networks, wireless sensor networks, smart grid networks, safety and handover in vehicular communications, nonlinear stability of convection in porous medium.