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.

TR2019-021 May 23, 2019

Abstract

In factory automation, heterogeneous manufacturing processes need to be coordinated over wireless networks to achieve safety and efficiency. 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 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. It is shown 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.

Automatica

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

Bin Hu[a], Yebin Wang[b], Philip Orlik[b], Toshiaki Koike-Akino[b], Jianlin Guo[b]

[a]*Department of Engineering Technology, Old Dominion University, Norfolk, VA 23529, United States*
[b]*Mitsubishi Electric Research Laboratories, 201 Broadway, Cambridge, MA 02139, Unite States*

Abstract

In factory automation, heterogeneous manufacturing processes need to be coordinated over wireless networks to achieve safety and efficiency. 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 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. It is shown 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.

Keywords: Stochastic Safety, Networked Control Systems, Factory Automation, State-dependent Fading Channel

1. Introduction

1.1. 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 Zhuang et al. (2007); Rajhans et al. (2014); De Pellegrini et al. (2006). 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 Groover (2007). 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 Islam et al. (2012); De Pellegrini et al. (2006) or interference Tse & Viswanath (2005) 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 of 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 Agrawal et al. (2014), sensor network with moving robots Quevedo et al. (2013) and indoor wireless networks with moving human bodies Kashiwagi et al. (2010). One simple example in FANs is an assembly process where an autonomous assembly arm and a forklift truck collaborate to assemble products. On 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 two physically separated systems, however, may have strong cyber-physical couplings. The cyber-physical couplings come from the fact that the physical motion of forklift vehi-

☆This paper was not presented at any IFAC meeting. Corresponding author Yebin Wang. Tel. +1-617-621-7571. Fax +1-617-621-7550.

Email addresses: bhu@odu.edu (Bin Hu), yebinwang@ieee.org (Yebin Wang), porlik@merl.com (Philip Orlik), koike@merl.com (Toshiaki Koike-Akino), guo@merl.com (Jianlin Guo)

cle may lead to serious *shadow fading* in the wireless network that is used by the assembly arm, thereby significantly compromising the system stability and performance. Thus, to ensure system safety, 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 Tse & Viswanath (2005); Gatsis et al. (2014); Tatikonda & Mitter (2004); Elia (2005) with assumed distributions such as Rayleigh, Rician and Weibull or as Markov chains Zhang et al. (1999); Wang & Moayeri (1995). 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 Gatsis et al. (2014). The 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.

1.2. Related Work

The example of an assembly process as well as the research work in Agrawal et al. (2014); Quevedo et al. (2013); Kashiwagi et al. (2010); Agrawal & Patwari (2009); Leong et al. (2016) demonstrate the importance of considering the cyber-physical couplings between communication and control systems to assure safety and efficiency for FANs. Similar conclusions have been made in work Hu & Lemmon (2013, 2015) where the dependency of channel states on physical states is used in the design of distributed switching control strategy to secure safety in vehicular networked systems. This paper extends the results in Hu & Lemmon (2015) to show that both system safety and efficiency can be achieved via a novel co-design framework. We are unaware of other work which formally analyze 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. These results will be reviewed and discussed.

When considering a joint objective for the communication and control systems, recent work in Molin & Hirche (2009); Gatsis et al. (2014); Di Girolamo et al. (2015); Bao et al. (2011) 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, Molin & Hirche (2009) 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 Di Girolamo et al. (2015). The work in Gatsis et al. (2014) 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 Bao et al. (2011).

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.

1.3. 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 Agrawal et al. (2014); Quevedo et al. (2013); Kashiwagi et al. (2010); Agrawal & Patwari (2009); Leong et al. (2016). 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 physical states on the channel state. Furthermore, this paper shows that the state-dependent channel model is a Markov modulated Bernoulli process Özekici (1997) that generalizes the traditional i.i.d. Bernoulli channel model in two important aspects: (1) the model parameters are not constants but 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 derived MATI generalizes the well-known results in Nešić & Teel (2004) where the channel fading impact was not considered. To the best of our knowledge, the established sufficient conditions 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

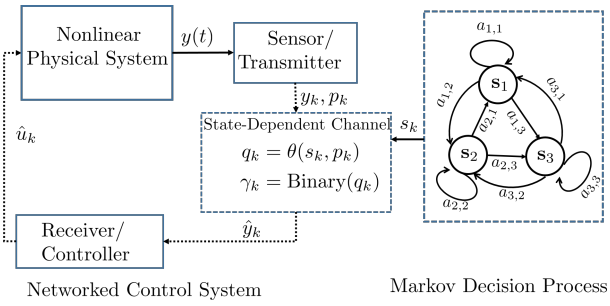


Figure 1: Heterogeneous System Framework: Networked Control System and Markov Decision Process

that the 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) Boyd et al. (2007); Maranas & Floudas (1997). 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 2 describes the system model and problem formulation. Section 3 presents the sufficient conditions to ensure *stochastic safety*. Under the safety conditions, Section 4 proposes a co-design paradigm to assure both safety and efficiency. Optimal solutions for the co-design problem are provided in Section 4.1. Main results are demonstrated via simulations of a mechanical robotic arm and a forklift truck in Sections 5. Section 6 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 $\overline{\beta}(\cdot,r,\cdot) \in \mathscr{KL}$.

2. System Model: A Heterogeneous System Framework

Fig. 1 shows a heterogeneous system framework with two subsystems: a networked control system ($\mathscr{G}$) that characterizes a nonlinear physical system being controlled over a wireless channel; 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 framework arises from 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. Such a *state-dependent* property of wireless communication in industrial systems clearly invalidates the use of traditional co-design frameworks, such as Molin & Hirche (2009); Gatsis et al. (2014); Zhang & Hristu-Varsakelis (2006), where the channel states are assumed to be decoupled from the physical states. The heterogeneous system framework in Fig. 1 is thus motivated by the co-design challenge under state-dependent fading channels.

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. The external disturbance $w \in \mathbb{R}^{n_w}$ 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 controller is remotely located and thus both 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 $\{\gamma(k)\}$ be a binary random process taking value from $\{0,1\}$. Its value 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 con-

dition 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 $e_u(t) = u(t) - \hat{u}(t_k)$. 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

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

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

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 focus on the system $\hat{\mathscr{G}}$ in the remaining of this paper.

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.

The MDP process models discrete-event decision making processes managing high-level control objectives such as transporting products from one location to another with minimum time or energy. Its state space S corresponds to a finite number of partitioned regions that the vehicle system, such as forklift trucks or cranes Agrawal et al. (2014) or robots Quevedo et al. (2013), 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. The costs in the MDP model characterizes the high level control objectives for the vehicle system. For instance, if the 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.

2.1. 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 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 $\forall s \in S, p \in \Omega_p$*

$$\Pr\{\gamma(k) = 1 | s(k) = s, p(k) = p\} = 1 - \theta(s,p) \tag{2}$$

where $s(k)$ and $p(k)$ represent the state of MDP system and the transmission power level at time instant t_k, respectively and $\theta(s,p) \in (0,1)$ is the outage probability Tse & Viswanath (2005) that monotonically decreases with respect to the transmission power level p.

Remark 1. The SDDC model in (2) relates the channel state (packet dropout probability) to the MDP states and transmission power levels. The definition of the SDDC is closely related to the *outage probability*, which is a widely used performance metric for fading channels Tse & Viswanath (2005). It characterizes the likelihood of the Signal-to-Noise Ratio (SNR) being below a specified threshold γ_0, i.e. $\Pr\{\text{SNR} \leq \gamma_0\}$. 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 Kashiwagi et al. (2010); Agrawal et al. (2014) 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 Agrawal et al. (2014); Agrawal & Patwari (2009). See Example 2 for more details about how to construct the SDDC from the *outage probability*.

Example 2 (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 Tse & Viswanath (2005). Let h_k denote the small scale fading gain induced by multi-path 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. $h_k \sim Raleigh(1), \forall k \in \mathbb{Z}_{\geq 0}$. 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. $0 \leq \psi(s) \leq 1, \forall s \in S$. 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*

$$\Pr\{\gamma(k) = 1 | s(k) = s, p(k) = p\}$$

$$=\Pr\{\frac{p(k)h_k^2\psi(s(k))^2}{N_0}\geq\gamma_0\Big|s(k)=s,p(k)=p\}$$
$$=\int_{\frac{\gamma_0 N_0}{p}}^{\infty}\psi(s)e^{-\psi(s)x}dx=e^{-\frac{N_0\gamma_0\psi(s)}{p}}.$$

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

E1 *The* $\hat{\mathscr{G}}$ *system with* $w\equiv 0$ *is* asymptotically safe in expectation *with respect to* Ω_s*, if there exists a class* $\mathscr{KL}$ *function* $\overline{\beta}(\cdot,\cdot)$ *and a set* $\Omega_s'=\{x\in\mathbb{R}^{n_x+n_c}||x|\leq r'(r)\}$ *such that* $\forall x_0\in\Omega_s'$

$$\mathbb{E}\big[|x(t)|\big]\leq\overline{\beta}(|x_0|,t)\leq r,\quad\forall t\in\mathbb{R}_{\geq 0}\tag{3}$$

and $\lim_{t\to+\infty}\mathbb{E}\big[|x(t)|\big]=0$.

E2 *The* $\hat{\mathscr{G}}$ *system with* $|w(t)|_{\mathscr{L}_\infty}\leq M_w$ *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*

$$\mathbb{E}\big[|x(t)|\big]\leq\overline{\beta}(|x_0|,t)+\kappa(M_w),\quad\forall t\in\mathbb{R}_{\geq 0}\tag{4}$$

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* $\forall\varepsilon\in(0,1],\tau>0$*, there exists a class* $\mathscr{KLL}$ *function* $\zeta(\cdot,\cdot,\cdot)$ *and a set* $\Omega_s'=\{x\in\mathbb{R}^{n_x+n_c}||x|\leq r'(\varepsilon,r)\}$ *such that* $\forall x_0\in\Omega_s'$

$$\Pr\big\{\sup_{t\geq\tau}|x(t)|\geq r\big\}\leq\zeta(|x_0|,\tau,r)\leq\varepsilon\tag{5}$$

and $\Pr\big\{\lim_{\tau\to\infty}\sup_{t\geq\tau}|x(t)|\geq r\big\}=0$.

These safety notions are closely related to the concepts of stochastic stability in Kushner (1967); Khasminskii (2011). In particular, **E1** and **E2** characterize the system behavior on average (in the first moment) while **P1** specifies possible paths of the system. These definitions capture safety requirements on both the system's transient and steady behavior.

Remark 2. For systems without external disturbance, the definition **E1** imposes safety for the transient behavior by requiring that the expected value of the infinity norm of the system trajectories must remain within the safety region if the initial states start from a pre-defined set whose size is a function of the safety set. In addition, the system trajectories must asymptotically converge to the origin as time goes to infinity. The expected safety notion defined in terms of infinity norm $\mathbb{E}\big[|x|\big]$ as shown in **E1** implies the notion of safety in variance, i.e., $\mathbb{E}\big[\|x(t)\|_2\big]\leq\overline{\beta}(|x_0|,t)\leq r$, due to the well known condition $\|x\|_2\leq\sqrt{n_x+n_c}|x|$. The *almost sure asymptotic safety* definition **P1** is a stronger safety notion than the definition **E1** in the sense that it imposes safety requirement on almost all sample paths rather than their expected value. Regarding the transient trajectories, the definition **P1** implies that the probability of almost all sample paths leaving the safety region at any time instant $t\in[\tau,\infty)$ is strictly decreasing as either the time τ or the size of safety region r increases. Such an unsafe probability is always below a pre-selected $\varepsilon\in(0,1],\forall t\in[\tau,\infty)$ that can be considered as a safety specification discussed in Prajna et al. (2007), if the initial states start within a set whose size is a function of the safety set r and safety specification ε. Moreover, the unsafe probability reaches zero as time τ goes to infinity.

Remark 3. 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. By applying Markov inequality, the definition **E2** implies that the probability of sample paths leaving the safe region is asymptotically bounded and the probability bound is a function of the size of the external disturbance and safety region, i.e., $\lim_{t\to\infty}\Pr\big\{|x(t)|\geq r\big\}\leq\overline{\beta}(M_w,r)$.

Under the safety conditions for system $\hat{\mathscr{G}}$, the second objective of this paper is to seek optimal control and communication policies to achieve system efficiency for both system $\hat{\mathscr{G}}$ and $\mathscr{M}$. This paper focuses on seeking optimal stationary policies for MDP system and transmission power. In particular, a (randomized) stationary control policy for the MDP system $\mathscr{M}$ is a function $\pi_\infty^m:S\to Dist(A)$ where the function $Dist(A)$ is a probability distribution over a finite set of actions A. In other words, $\forall s\in S$, the stationary policy is defined as a set of probabilities with $\pi_\infty^m=\big\{\Pr\{a|s\}_{a\in A(s)}\big\}$ and $\sum_{a\in A(s)}\Pr\{a|s\}=1$. Similarly, a (randomized) stationary policy for transmission power is a function $\pi_\infty^p:S\to Dist(\Omega_p)$ where $\pi_\infty^p=\big\{\Pr\{p|s\}_{s\in S,p\in\Omega_p}\big\}$ and $\sum_{p\in\Omega_p}\Pr\{p|s\}=1$.

With the control π^m and communication π^p policies, the system efficiency resorts to a constrained infinite horizon optimization problem as follows,

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

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. Parameter $\lambda>0$ is used to trade-off communication and control costs. Solutions to the constrained infinite horizon optimization problem in (6) are optimal co-design policy for transmission power and

control to achieve both system efficiency and safety. As shown in Section 4, the main challenge to solve the above optimization problem lies in the non-convex safety constraints.

3. Sufficient Conditions for Stochastic Safety

This section presents sufficient conditions to ensure *stochastic safety* defined in Definition 3 for the $\mathscr{G}$ system. The following two assumptions are needed for the main results.

Assumption 4. *The networked control 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 $t \in \mathbb{R}_{\geq 0}$.*

Assumption 5. *The networked control system $\dot{x} = f(t,x,e,w)$ is* exponential input to state stable (Exp-ISS) *w.r.t. e and w, if the system is* ISS *and the function $\beta(s,t)$ 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 6. *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*

$$\underline{w}|e| \leq W(e) \leq \overline{w}|e|, \tag{7}$$

$$\left\langle \frac{\partial W(e)}{\partial e}, g(t,x,e,w) \right\rangle \leq L_1 W(e) + L_2|x| + L_3|w|. \tag{8}$$

Assumption 6 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 process $\{e(t_k^+)\}$ forms a stochastic jump process and its discrete dynamic is governed by the outage probability of the fading channels $\theta(s,p)$ which depends on the MDP's state $s \in S$ and the transmission power level $p \in \Omega_p$.

Proposition 7. *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*

$$\mathbb{E}\{W(e(t_k^+))\Big| s(k) = s, p(k) = p\} = \theta(s,p) W(e(t_k)). \tag{9}$$

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 (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 8. *Let $T_k = t_{k+1} - t_k$ denote the transmission time interval, P_m denote the transition matrix defined in* (11) *and $p \in \Omega_p$ denote the transmission power level. Suppose the ISS assumption in Assumption 4 and Assumption 6 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*

$$\tau^* = \frac{1}{L_1} \ln \frac{L_2\overline{\gamma}_1 + L_1\overline{w}}{L_2\overline{\gamma}_1 + \overline{w}L_1 \|P_m(\pi_\infty^m, \pi_\infty^p) diag(\theta(s,p))\|} > 0 \tag{10}$$

is the MATI. The system parameters L_1, and L_2 come from (7) and (8) respectively and

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

$$P_m(\pi_\infty^m, \pi_\infty^p) = \begin{bmatrix} \Pr(s_1,p_1|s_1,p_1) & \cdots & \Pr(s_1,p_1|s_N,p_M) \\ \Pr(s_1,p_2|s_1,p_1) & \cdots & \Pr(s_2,p_1|s_N,p_M) \\ \vdots & \vdots & \vdots \\ \Pr(s_N,p_M|s_1,p_1) & \cdots & \Pr(s_N,p_M|s_N,p_M) \end{bmatrix} \tag{11}$$

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. Proof is based on the small gain theorem in Isidori (1995) and Markovian jump system theory in Costa et al. (2006). The stochastic hybrid system (1) can be viewed 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 $\mathbb{I}_k$. Given the error dynamics over $\mathbb{I}_k$ and Assumption 6, 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

$$\begin{aligned} &W(e(t_{k+1})) \\ &\quad\leq e^{L_1(t_{k+1}-t_k)}W(e(t_k^+)) + \int_{t_k}^{t_{k+1}} e^{L_1(t_{k+1}-s)}L_2|x|ds \\ &\quad\leq e^{L_1T_k}W(e(t_k^+)) + L_2|x|_{[t_k,t_{k+1})}\int_{t_k}^{t_{k+1}} e^{L_1(t_{k+1}-s)}ds \\ &\quad= e^{L_1T_k}W(e(t_k^+)) + \frac{L_2}{L_1}(e^{L_1T_k}-1)|x|_{[t_k,t_{k+1})} \end{aligned} \tag{12}$$

Since $|x|_{[t_k,t_{k+1})} = \sup_{t_k\leq t<t_{k+1}}|x| \geq |x(\tau)|, \forall \tau \in \mathbb{I}_k$, the second inequality holds. Note that the inequality (12) 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 (12) without changing the sign,

$$\begin{aligned}
&W_{k+1}(s,p)\\
&\leq e^{L_1T_k}\mathbb{E}\{W(e(t_k^+))\mathbb{1}_{s,p}\}+\frac{L_2}{L_1}(e^{L_1T_k}-1)\mathbb{E}\{|x|_{[t_k,t_{k+1})}\mathbb{1}_{s,p}\}\\
&=e^{L_1T_k}\sum_{s'\in S,p'\in\Omega_p}\mathbb{E}\{W(e(t_k^+))\mathbb{1}_{s',p'}\}\Pr\{s,p|s',p'\}\\
&\quad+\frac{L_2}{L_1}(e^{L_1T_k}-1)|x|_{[t_k,t_{k+1})}\mathbb{E}\{\mathbb{1}_{s,p}\} \qquad (13)\\
&=e^{L_1T_k}\sum_{s'\in S,p'\in\Omega_p}W_k(s',p')\theta(s',p')\Pr\{s,p|s',p'\}\\
&\quad+\frac{L_2}{L_1}(e^{L_1T_k}-1)|x|_{[t_k,t_{k+1})}\mathbb{E}\{\mathbb{1}_{s,p}\} \qquad (14)
\end{aligned}$$

The equality (13) holds due to the Markovian property of the MDP and power processes. The second Equality (14) holds as a result of Proposition 7 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 $W_k\coloneqq[W_k(s_1,p_1),W_k(s_1,p_2),\ldots,W_k(s_{|S|,|\Omega_p|})]^T$, then

$$\begin{aligned}
W_{k+1}\leq& e^{L_1T_k}P_m\text{diag}(\theta(s,p))W_k\\
&+\frac{L_2}{L_1}(e^{L_1T_k}-1)|x|_{[t_k,t_{k+1})}[\mathbb{E}\{\mathbb{1}_{s,p}\}] \qquad (15)
\end{aligned}$$

where $\text{diag}(\theta(s,p)),P_m(\pi_\infty^m,\pi_\infty^p)$ are defined in (11) and $[\mathbb{E}\{\mathbb{1}_{s,p}\}]\coloneqq[\mathbb{E}\{\mathbb{1}_{s_1,p_1}\}\cdots\mathbb{E}\{\mathbb{1}_{s_i,p_j}\}\cdots\mathbb{E}\{\mathbb{1}_{s_{|S|},p_{|\Omega_p|}}\}]^T$. Since both sides of (15) are positive, taking the ∞-norm on both sides of (15) leads to

$$\begin{aligned}
&|W_{k+1}|\\
&\leq e^{L_1T_k}\underbrace{\|P_m\text{diag}(\theta(s,p))\|}_{P_\infty}|W_k|\\
&\quad+\frac{L_2}{L_1}(e^{L_1T_k}-1)|\underbrace{[\mathbb{E}\{|x|_{[t_k,t_{k+1})}\mathbb{1}_{s,p}\}]}_{X_{[k,k+1)}}|\\
&\leq\frac{L_2}{L_1}(e^{L_1T^*}-1)\Big(|X_{[k,k+1)}|+e^{L_1T^*}P_\infty|X_{[k-1,k)}|+\cdots\\
&\quad+\left(e^{L_1T^*}P_\infty\right)^k|X_{[0,1)}|\Big)+\left(e^{L_1T^*}P_\infty\right)^{k+1}|W_0|\\
&\leq\frac{L_2}{L_1}(e^{L_1T^*}-1)\sum_{i=0}^{\infty}\left(e^{L_1T^*}P_\infty\right)^i|X_{[0,k+1)}|+\left(e^{L_1T^*}P_\infty\right)^{k+1}|W_0|\\
&=\frac{L_2}{L_1}\frac{e^{L_1T^*}-1}{1-e^{L_1T^*}P_\infty}|X_{[0,k+1)}|+\left(e^{L_1T^*}P_\infty\right)^{k+1}|W_0| \qquad (16)
\end{aligned}$$

where $T^*=\max_{0\leq i\leq k}T_k$. Clearly, (16) shows that the W system is ISS 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 $\underline{w}|e|\leq W(e)\leq\overline{w}|e|$, it is straightforward to conclude that the error dynamic system is also ISS in expectation as follows,

$$\begin{aligned}
|E_{k+1}|\leq&\frac{L_2}{L_1\overline{w}}(e^{L_1T^*}-1)\frac{1}{1-e^{L_1T^*}P_\infty}|X_{[0,k+1)}|\\
&+\frac{\underline{w}\left(e^{L_1T^*}P_\infty\right)^{k+1}}{\overline{w}}|E_0| \qquad (17)
\end{aligned}$$

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

Similarly, let $X_t(s,p)\coloneqq\mathbb{E}\{|x(t)|\mathbb{1}_{s,p}\}$ denote the expectation of $|x(t)|$ over the set s,p. By Assumption 4 and $\gamma_1(s)\leq\overline{\gamma}_1 s,\forall s>0$, one has

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

Similar to the derivation of (17), one has

$$|X_t|\leq\beta(|X_0|,t-t_0)+\overline{\gamma}_1|E_{[t_0,t)}| \qquad (18)$$

Consider the ISS characterizations of subsystem X in (18) and subsystem E in (17), from the well-established small gain theorem Jiang et al. (1994), the interconnected system X and E is asymptotically stable if the small gain condition $\frac{L_2}{L_1\overline{w}}(e^{L_1T^*}-1)\frac{1}{1-e^{L_1T^*}\|P_m\text{diag}(\theta(s,p))\|}\overline{\gamma}_1<1$ holds. The small-gain condition leads to the sufficient condition in (10). Since $\mathbb{E}\{|x(t)|\}\leq|X_t|,\forall t\geq 0$ and the subsystem X is asymptotically stable, there exists a class $\mathscr{KL}$ function $\overline{\beta}(s,t)$ such that $\mathbb{E}\{|x(t)|\}\leq\overline{\beta}(|x(0)|,t)$. Then, we select $r'>0$ to satisfy $\overline{\beta}(r',0)=r$ and if the initial states $|x_0|\leq r'$, we know that $\mathbb{E}\{|x(t)|\}\leq\overline{\beta}(|x(0)|,t)\leq\overline{\beta}(r',0)=r$. The proof is complete. □

Remark 4. The MATI in (10) generalizes the result in Nešić & Teel (2004). In particular, the MATI in Nešić & Teel (2004) is recovered if the shadow fading is absent, i.e., $\theta(s,p)=0,\forall s\in S,p\in\Omega_p$.

Theorem 9. *Let the hypothesis in Theorem 8 and the Exp-ISS Assumption 4 hold . System $\mathscr{G}$ is almost surely asymptotically safe (**P1** in Definition 3) with respect to the origin.*

PROOF. Under the Exp-ISS assumption in Assumption 4, by following the same argument used in proving Theorem 8, 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 $\forall x(0)\in\Omega_s$, $\mathbb{E}[|x(t)|]\leq K_1\exp(-K_2t)|x(0)|,\forall t\in\mathbb{R}_{\geq 0}$. Let $\tau'>\tau\geq 0$ denote any time instants such that $\tau\leq t<\tau'$ holds, then for any given $\varepsilon>0$ and the safe set $\Omega_s=\{x\in\mathbb{R}^{n_x+n_c}||x|\leq r\}$ with $r\geq 0$, consider the following probability bound $\Pr\{\sup_{\tau\leq t<\tau'}|x(t)|\geq r\}\leq\Pr\left\{\int_\tau^{\tau'}|x(t)|dt\geq r\right\}\stackrel{(a)}{\leq}\mathbb{E}\left\{\int_\tau^{\tau'}|x(t)|dt\right\}/(\varepsilon+r)\stackrel{(b)}{\leq}\int_\tau^{\tau'}\mathbb{E}\{|x(t)|\}dt/r\leq\int_\tau^{\tau'}K_1\exp(-K_2t)|x(0)|dt/r\leq$

$\frac{K_1|x(0)|}{K_2\varepsilon'}[\exp(-K_2\tau) - \exp(-K_2\tau')]$. The inequality (a) holds due to the Markov inequality; and the 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

$$\Pr\{\sup_{\tau<t}|x(t)| \geq r\} \leq \frac{K_1|x(0)|}{K_2 r}\exp(-K_2\tau) \leq \frac{K_1|x(0)|}{K_2 r}.$$

Let $\varepsilon' := \frac{K_1|x(0)|}{K_2 r}$, and then there exists a function $\delta(\varepsilon', r) = \frac{\varepsilon' K_2 r}{K_1}$ such that $\Pr\{\sup_{\tau\leq t}|x(t)| \geq r\} \leq \varepsilon', \forall |x(0)| \leq \delta(\varepsilon', r)$. Taking the integral of the probability $\Pr\big\{\sup_{\tau<t}|x(t)| \geq r\big\}$ with time instant τ from 0 to ∞, one has

$$\begin{aligned}\int_0^\infty \Pr\big\{\sup_{\tau<t}|x(t)| \geq r\big\}d\tau \\ \leq \int_0^\infty \frac{K_1|x(0)|}{K_2 r}\exp(-K_2\tau)d\tau = \frac{K_1|x(0)|}{K_2^2 r} < \infty.\end{aligned}$$

Then, by the Borel Cantelli lemma, one knows that $\Pr\big\{\lim_{\tau\to\infty}\sup_{\tau<t}|x(t)| \geq r\big\} = 0$. The proof is complete. □

Theorem 10. *Suppose that the MATI condition in* (10) *holds and consider the system in* (1) *with* $|w|_{\mathscr{L}_\infty} \leq M_w$.. *Then the system* $\hat{\mathscr{G}}$ *is asymptotically bounded in expectation (**E2** in Definition 3) with respect to a bounded safe set* $\Omega_s = \{x \in \mathbb{R}^{n_x+n_c} | |x| \leq r\}$, *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* $\mathbb{E}\big[|x(t)|\big] \leq \overline{\beta}(|x_0|,t) + \kappa(M_w), \forall t \in \mathbb{R}_{\geq 0}$ *and* $\lim_{t\to+\infty}\mathbb{E}\big[|x(t)|\big] = \kappa(M_w)$.

PROOF. Following the argument and notation in the proof of Theorem 8, similar to inequalities (17) and (18) one has the interconnected systems with $|w|_{\mathscr{L}_\infty} \leq M_w$ defined as follows

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

Since the small gain condition holds for any transmission time interval $T^* \leq \tau^*$ where τ^* is defined in (10), one can conclude that the composite system state $C_k := [E_k, X_k]$ is ISS 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 $|C_k| \leq \overline{\beta}(|C_0|, kT^*) + \kappa(M_w)$. Given a safe set $\Omega_s := \{x \in \mathbb{R}^n | |x| \leq r\}$, then for any $\varepsilon > 0$, the stochastic safety in probability can be characterized as

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

The first Inequality holds due to the Markov's inequality. The second inequality holds because $\mathbb{E}(|x(t)|) = \sum_{s\in S, p\in\Omega_p} X_t(s,p) \leq |S||\Omega_p||X_t|$ and $|X_t| \leq |C_t|$. One has $\lim_{t\to\infty}\Pr\{|x(t)| \geq r+\varepsilon\} \leq |S||\Omega_p|\frac{\kappa(M_w)}{r+\varepsilon}$. □

4. 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 (10). 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 11 (Two-player Constrained Cooperative Game). *Let* $c_p(\cdot) : \Omega_p \to \mathbb{R}_{\geq 0}$ *denote the power cost and* $c(\cdot,\cdot) : S \times A \to \mathbb{R}_{\geq 0}$ *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,*

$$\begin{aligned}\min_{\pi^p,\pi^m} \quad & J_\alpha(s_0,\pi^m,\pi^p) \\ s.t. \quad & \|P_m(\pi^m,\pi^p)diag(\theta(s,p))\| \leq \xi(T).\end{aligned} \tag{19}$$

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 5. The inequality (19) is a safety constraint reformulated by the sufficient condition (10). In order to see how this safety constraint is derived from (10), let (π^p,π^m) denote the feasible policies such that $T \leq \tau^*(\pi^p,\pi^m)$. Thus $T \leq \frac{1}{L_1}\ln\frac{L_2\overline{\gamma}_1+L_1}{L_2\overline{\gamma}_1+L_1\|P_m(\pi^p,\pi^m)\mathrm{diag}(\theta(s,p))\|}$. Rearrangement of the inequality gives $\|P_m(\pi_p,\pi_m)\mathrm{diag}(\theta(s,p))\| \leq \frac{1}{L_1}\big[e^{-L_1T}(L_2\overline{\gamma}_1 + L_1) - L_2\overline{\gamma}_1\big] \triangleq \xi(T)$. Since $T \leq \tau^*$, 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 (10) assures system safety.

Under the stationary policy space, we show that Problem 11 is equivalent to the following constrained nonlinear optimization problem.

Problem 12. Constrained Nonlinear Optimization Problem: *Suppose that the state S and action A spaces in the MDP system* $\mathscr{M}$ *are finite sets, and the transmission power set* Ω_p *is finite. Let* $u_\infty^p(p|s) = \Pr\{p|s\}$ *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.*

$$\min_{u_\infty^p(p|s),\delta(s,a)} \sum_{(s,a)\in S\times A(s)}\big(\lambda\sum_{p\in\Omega_p}c_p(p)u_\infty^p(p|s) + c(s,a)\big)\delta(s,a) \tag{20a}$$

subject to

$$\sum_{s\in S}\frac{\sum_{a\in A(s)}\Pr\{s'|s,a\}\delta(s,a)}{\sum_{a\in A(s)}\delta(s,a)}\sum_{p\in\Omega_p}u_\infty^p(p|s')\theta(s,p)\le\xi(T), \tag{20b}$$

$$\sum_{a\in A(s)}\delta(s,a)=D_0(s)(1-\alpha)+\alpha\sum_{s'\in S}\sum_{a'\in A(s')}\delta(s',a')\Pr\{s|s',a'\}, \tag{20c}$$

$$\sum_s\sum_a\delta(s,a)=1,\ \sum_{p\in\Omega_p}u_\infty^p(p|s)=1,\delta(s,a)\ge 0,\ u_\infty^p(p|s)\ge 0. \tag{20d}$$

The following Lemma shows that Problems 12 and 11 are equivalent in the sense that they have the same optimal solutions and objectives.

Lemma 13. *Let δ^* and $u_\infty^{p^*}$ denote the optimal solutions to Problem 12, then the policies $u_\infty^{p^*}=\pi_\infty^{p^*}$ and $\pi_\infty^{m^*}(a|s)=\Pr\{a|s\}=\frac{\delta^*(s,a)}{\sum_{a\in A(s)}\delta^*(s,a)}$ are the optimal solutions to Problem 11.*

PROOF. The proof can be obtained by examining the equivalence between Problem 12 and Problem 11 in terms of objective function, decision variables and feasible set imposed by the constraints. We have already shown that the objective function in Problem 11 can be rewritten as a function of the new decision variables $\{u_p(s,a)\}$ and $\{\delta(s,a)\}$ in Problem 12. 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 (20d) are introduced to enforce the probability law (i.e. non-negativity and total probability being 1). The constraint in (20c) 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 Altman (1999) for more details). Therefore, one has established the equivalence and the proof is complete. □

Remark 6. Problem 12 is a polynomial optimization problem where the objective function and safety constraints in (20b) are polynomial. It involves the non-convex safety constraints (20b), thanks to the couplings between communication and control policies through *state-dependent fading wireless channels*.

4.1. Relaxed Generalized Geometrical Programming

Problem 12 falls into one type of non-convex optimization problem, called Generalized Geometric Program (GGP) Maranas & Floudas (1997) 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. Problem 12 can be formulated as a GGP as follows,

$$\begin{aligned}\underset{X}{\text{minimize}}\quad & G_0(X)=G_0^+(X)\\ \text{subject to}\quad & G_i(X)=G_i^+(X)-G_i^-(X)\le 0,\quad i=1,\ldots,N\\ & G_{\text{linear}}(X)\le 0,\quad X\in\Omega_X\end{aligned} \tag{21}$$

where $G_i^+,G_i^-,i=1,2,\ldots,N$ are posynomials and G_{linear} are linear functions. To see how safety constraints in (20b) can be written as the difference of two posynomials, multiplying both sides of (20b) 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, $X=\exp(Z)$,

$$\begin{aligned}\underset{Z}{\text{minimize}}\quad & \tilde{G}_0(Z)=\tilde{G}_0^+-\tilde{G}_0^-\\ \text{subject to}\quad & \tilde{G}_i(Z)=\tilde{G}_i^+(Z)-\tilde{G}_i^-(Z)\le 0,\quad i=1,\ldots,M\\ & G_{\text{linear}}(Z)\le 0,\quad Z\in\Omega_Z.\end{aligned} \tag{22}$$

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 Maranas & Floudas (1997). To address the non-convexity issues, this paper approximates the second terms $\tilde{G}_i^-$ in the non-convex safety constraints using linear functions. 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.

4.1.1. 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,

$$\begin{aligned}&\tilde{G}_i^-(Z)\le A_iZ+B_i\\ &A_i=\sum_{j\in L_i^-}a_{ij}A_{ij}[b_{ij1},\ldots,b_{ijn}],\quad B_i=\sum_{j\in L_i^-}a_{ij}B_{ij}\\ &A_{ij}=\frac{\exp(Y_{ij}^H)-\exp(Y_{ij}^L)}{Y_{ij}^H-Y_{ij}^L},\quad B_{ij}=\frac{Y_{ij}^H\exp(Y_{ij}^L)-Y_{ij}^L\exp(Y_{ij}^H)}{Y_{ij}^H-Y_{ij}^L}\\ &Y_{ij}^L=\sum_{l=1}^n\min(b_{ijl}z_l^L,b_{ijl}z_l^H),\quad Y_{ij}^H=\sum_{l=1}^n\max(b_{ijl}z_l^L,b_{ijl}z_l^H)\end{aligned} \tag{23, 24}$$

By replacing $\tilde{G}_i^-(Z)$ with $A_iZ+B_i, \forall i=0,1,\ldots,M$ in the transformed GGP (22), one has the convex optimization problem as follows,

$$\begin{aligned} \underset{Z}{\text{minimize}} \quad & \tilde{G}_0^U(Z) = \tilde{G}_0^+(Z) \\ \text{subject to} \quad & \tilde{G}_i^U(Z) = \tilde{G}_i^+(Z) - (A_iZ+B_i) \le 0, \quad i=1,\ldots,N \\ & G_{\text{linear}}(Z) \le 0, \quad Z \in \Omega_Z \end{aligned} \tag{25}$$

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,

Lemma 14. *Maranas & Floudas (1997) 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 $\Delta_i^*, \forall i=1,\ldots,N$ 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 similar to the one in Maranas & Floudas (1997) and is therefore omitted in this paper. Please see Maranas & Floudas (1997) or Hu et al. (2017) for details. □

4.1.2. 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 determined by $\tilde{G}_i^-(Z) \ge A_iZ+B_i^L$ where $B_i^L = \sum_{j\in L_i^-} a_{ij}A_{ij}(1-\log(A_{ij}))$. By replacing $\tilde{G}_i^-(Z)$ with $A_iZ+B_i^L, \forall i=0,1,\ldots,M$ in the transformed GGP (22), one has the following convex optimization with linear lower bounds,

$$\begin{aligned} \underset{Z}{\text{minimize}} \quad & \tilde{G}_0^L(Z) = \tilde{G}_0^+(Z) - (A_0Z+B_0^L) \\ \text{subject to} \quad & \tilde{G}_i^L(Z) = \tilde{G}_i^+(Z) - (A_iZ+B_i^L) \le 0, \quad i=1,\ldots,M \\ & G_{\text{linear}}(Z) \le 0, \quad Z \in \Omega_Z \end{aligned} \tag{26}$$

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

Lemma 15. *Consider the GGP problem (22) and the relaxed GGP (26) 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 (25), (26) are lower and upper bounds to the original non-convex problem in (22).

Lemma 16. *Let Z^{H^*}, Z^* and Z^{L^*} denote the optimal solution to the optimization problems in (25), (22) and (26) respectively, the optimal objective functions then satisfy $\tilde{G}_0^H(Z^{H^*}) \le \tilde{G}_0(Z^*) \le \tilde{G}_0^L(Z^{L^*})$ and the solution Z^{L^*} is a suboptimal solution to the non-convex optimization problem in (22). 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 (25), (22) and (26) 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 $\tilde{G}_0^H(Z^{H^*}) \le \tilde{G}_0(Z^*)$. The proof is complete. □

4.2. Sub-optimality and Distance to Global Optimality

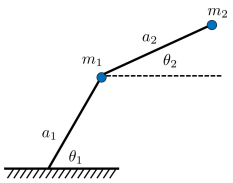
Obtaining an exact global optimum for a non-convex optimization problem is generally NP-hard Vandenberghe & Boyd (1996), which means that "brute force" type of searching algorithms are necessary to find global solutions. Hence, it is reasonable to expect suboptimal solutions but with certain performance guarantee. This paper adopts a *Branch-Bound* method under which the lower and upper bounds of the non-convex GGP Problem in (22) asymptotically approaches the optimal solutions. 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 17. *Consider the non-convex GGP problem in (22), relaxed convex problems in (25) and (26) and the Branch-Bound algorithm, let Z^*, Z^{H^*} and Z^{L^*} denote the optimal solutions for the optimization problems (22), (25) and (26) 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*

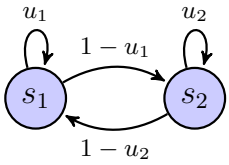
$$|Z^{H^*} - Z^*| = \mathscr{O}(\delta) \quad \text{as } \delta\to 0 \tag{27}$$

$$|Z^* - Z^{L^*}| = \mathscr{O}(\delta) \quad \text{as } \delta\to 0 \tag{28}$$

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



(a) Two Link Planar Elbow Arm



(b) Forklift Truck: Two-state MDP

Figure 2: Simulation example of robotic manipulator and forklift truck

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 omitted. Interested readers are referred to Hu et al. (2017) for more details.

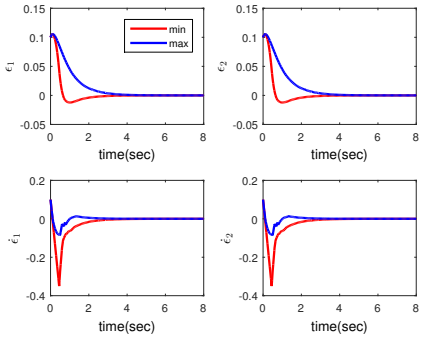
5. Simulation Results

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 system dynamic of a two-link planar elbow arm is modeled by a nonlinear ODE [1] $G(q)+M(q)\ddot{q}+V(q,\dot{q})=\tau$ where $q=[\theta_1;\theta_2]$ are the angles for the upper and lower links of the planar elbow arm as shown in Figure 2a and $\dot{q},\ddot{q}$ are the corresponding angular velocities and accelerations. $\tau=[\tau_1;\tau_2]\in\mathbb{R}^2$ is the system input with $\tau_i, i=1,2$ representing the external torque forces generated by either motors or hydraulic actuators. The angular states $q,\dot{q}$ are measured by local sensors and are transmitted through a wireless communication channel to a remote controller that determines the values of forces $\tau_i, i=1,2$. In this simulation, the control objective of the robotic arm is to track a predefined desired trajectory 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 in Lewis et al. (2003), $F=M(\hat{q})(\ddot{q}_d-K[\hat{q}-q_d;\hat{\dot{q}}-\dot{q}_d])+V(\hat{q},\hat{\dot{q}}+G(\hat{q}))$ 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 other parameters in the simulation are the length a_i and mass weight $m_i, i=1,2$ of the upper and lower links, which are set to be $m_1=1, a_1=2, m_2=0.1, a_2=10$.

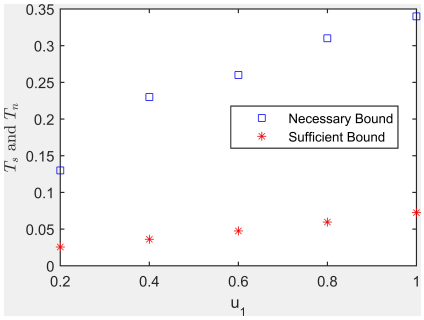
The wireless communication channel used by the robotic arm is subject to shadow fading which is directly related to the physical position of the forklift truck. In the simulation, the autonomous forklift system is modeled as a two state MDP as shown in Figure 2b with s_1 representing the physical region that leads to a good channel condition and s_2 denoting the region that causes a shadow fading. The transitions between these two states are controlled by two actions 'stay' and 'go' and $u_i, i=1,2$ 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 the two-state MDP model, the transmitter in the robotic arm can select either high power p_H level or low power p_L level (i.e., $\Omega_p=\{p_H,p_L\}$), to adjust the outage probability $\theta(s,p), s\in\{s_1,s_2\}, p\in\{p_H,p_L\}$ as shown in the channel model (2). The outage probabilities under different power levels and MDP states are set to be $\theta(s_1,p_L)=0.4, \theta(s_1,p_H)=0.1, \theta(s_2,p_L)=0.9$ and $\theta(s_2,p_H)=0.4$.

The first simulation result is to show almost sure safety for the two-link planar elbow arm system under the MATI in (10) 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 3a 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 3a 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



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



(b) Sufficient T_s and necessary T_n bounds on MATI

Figure 3: Almost surely convergence of tracking error on angular states (Left Figure 3a); 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 3b).

[1] Pleaser refer to Lewis et al. (2003) or Hu et al. (2017) for details about the functions $G(q), M(q)$ and $V(q,\dot{q})$ for the two link planar elbow arm.

if the system is almost surely asymptotically stable. These results, therefore, seem to confirm our sufficient condition in (10) for almost sure safety.

Figure 3b shows the comparison of the sufficient MATI bounds (red stars) obtained by (10) and necessary MATI bounds (blue squares) generated by the exhaustive search method [2] 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 Nešić & Teel (2004). Our results can apply to a more general stochastic networked system but with similar gaps.

The second simulation results are to verify the effectiveness and advantages of the proposed co-design paradigm to achieve both safety and efficiency by comparing it against the separation design framework proposed in Gatsis et al. (2014). The co-design optimization problem for the example of forklift and robotic arm is formulated as follows,

$$\begin{aligned}
\underset{\{x_i\}_{i=1}^4,\{y_i\}_{i=1}^4}{\textbf{Minimize}} \quad & \sum_{i=1}^{4} c_i x_i + 2\lambda \sum_{j=1}^{2} (y_{2j-1} c_p(p_H) \\
& + y_{2j} c_p(p_L))(x_{2j-1} + x_{2j}) \qquad (29a) \\
\textbf{subject to} \quad & \begin{cases} (1-\alpha)x_1 + x_2 - \alpha x_4 = (1-\alpha)\delta_0 \\ x_1 + x_2 + x_3 + x_4 = 1, \\ y_{2j-1} + y_{2j} = 1, j = 1,2 \\ y_i \geq 0, x_i \geq 0, \quad i = 1,2,3,4 \end{cases} \qquad (29b) \\
& \begin{cases} \frac{x_1 y_1}{x_1+x_2}\theta(s_1) + \frac{x_4 y_3}{x_3+x_4}\theta(s_2) \leq c(T) \\ \frac{x_1 y_2}{x_1+x_2}\theta(s_1) + \frac{x_4 y_4}{x_3+x_4}\theta(s_2) \leq c(T) \\ \frac{x_2 y_1}{x_1+x_2}\theta(s_1) + \frac{x_3 y_3}{x_3+x_4}\theta(s_2) \leq c(T) \\ \frac{x_2 y_2}{x_1+x_2}\theta(s_1) + \frac{x_3 y_4}{x_3+x_4}\theta(s_2) \leq c(T) \end{cases} \qquad (29c)
\end{aligned}$$

where $\{x_i\}$ and $\{y_i\}$ represent the decision variables related to the control and transmit power policies defined in Problem 12 $x_1 := \delta(s_1, \text{“Stay”}), y_1 := \Pr\{p_H|s_1\}, x_2 := \delta(s_1, \text{“Go”}), y_2 := \Pr\{p_L|s_1\}, x_3 := \delta(s_2, \text{“Stay”}), y_3 := \Pr\{p_H|s_2\}, x_4 := \delta(s_2, \text{“Go”}), y_4 := \Pr\{p_L|s_2\}$. The inequalities (29c) 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. As discussed in Section 4, the parameter $c(T)$ is a function of the transmission time interval T and system parameters in the arm system (See Remark 5). Once T is selected, $c(T)$ is a fixed value. c_i is the system cost induced by the state in x_i, i.e., $c_1 = c(s_1, \text{“Stay”}) = 1.5, c_2 = c(s_1, \text{“Go”}) = .5, c_3 = c(s_2, \text{“Stay”}) = 1$ and $c_2 = c(s_2, \text{“Go”}) = 1$. The power costs are $c_p(p_L) = 0.5$ and $c_p(p_H) = 2$. The other parameters in the simulation are: $\delta_0 = \Pr\{s(0) = s_1\} = 0.5$, $\alpha = 0.8$, and $\lambda = 1$.

[2] The exhaustive search method starts with the sufficient MATI τ^* bound in (10), and increase the value of τ^* until the the maximum and minimum value of the sample path fail to converge to zero.

By using the GGP formulation and the branch-bound algorithm discussed in Section 4.1, Figure 4 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 17 which state that the global optimal solution is asymptotically achieved by the branch-bound algorithm.

Figure 5 shows the performance comparison between the proposed co-design framework and the separation design method under different transmission time intervals T (Figure 5a) and different fading levels (Figure 5b). 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 (29c) in the optimization problem (29) 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,

$$\begin{aligned}
\underset{\{y_i\}_{i=1}^4}{\textbf{Minimize}} \quad & (0.2y_1 + 1.8y_3)c_p(p_H) + (0.2y_2 + 1.8y_4)c_p(p_L) \\
\textbf{subject to} \quad & \begin{cases} y_1 + y_2 = 1 \\ y_3 + y_4 = 1 \\ y_1\theta(s_1) + y_3\theta(s_2) \leq c(T) \\ y_2\theta(s_1) + y_4\theta(s_2) \leq c(T) \\ y_i \geq 0, \quad i = 1,2,3,4 \end{cases} \qquad (30)
\end{aligned}$$

Note that the safe region generated by the constraints (30) in the separation design problem is two times smaller than that generated by the co-design framework (29c). 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 5a 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

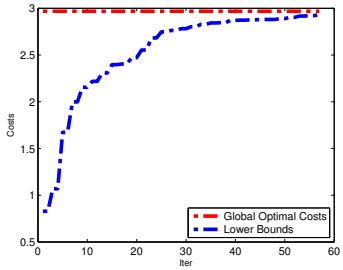
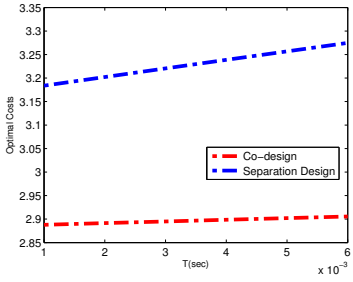
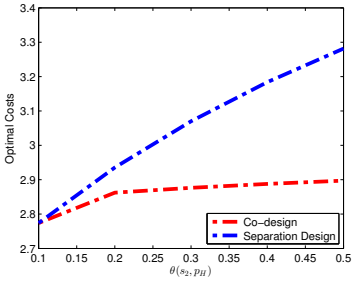


Figure 4: Asymptotic Convergence of Lower Bounds to Global Optimum with $T = 0.01$ sec



(a) Optimal costs under different T



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

Figure 5: 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 5a) and shadow fading levels $\theta(s_2, p_H) = 0.1 : 0.1 : 0.5$ (Figure 5b)

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 (30) for the separation design method will be infeasible if T is larger than 0.006 sec.

Figure 5b 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 5b, 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. 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.

6. 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 and the optimal solutions are then obtained by solving two relaxed convex GGP. 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.

References

Agrawal, P., Ahlén, A., Olofsson, T., & Gidlund, M. (2014). Long term channel characterization for energy efficient transmission in industrial environments. *IEEE Transactions on Communications*, *62*, 3004–3014.

Agrawal, P., & Patwari, N. (2009). Correlated link shadow fading in multi-hop wireless networks. *IEEE Transactions on Wireless Communications*, *8*, 4024–4036.

Altman, E. (1999). *Constrained Markov Decision Processes* volume 7. CRC Press.

Bao, L., Skoglund, M., & Johansson, K. H. (2011). Iterative encoder-controller design for feedback control over noisy channels. *IEEE Transactions on Automatic Control*, *56*, 265–278.

Boyd, S., Kim, S.-J., Vandenberghe, L., & Hassibi, A. (2007). A tutorial on geometric programming. *Optimization and Engineering*, *8*, 67–127.

Costa, O. L. V., Fragoso, M. D., & Marques, R. P. (2006). *Discrete-time Markov Jump Linear Systems*. Springer Science & Business Media.

De Pellegrini, F., Miorandi, D., Vitturi, S., & Zanella, A. (2006). On the use of wireless networks at low level of factory automation systems. *IEEE Transactions on Industrial Informatics*, *2*, 129–143.

Di Girolamo, G., D'Innocenzo, A., & Di Benedetto, M. (2015). Co-design of controller and routing redundancy over a wireless network. *IFAC-PapersOnLine*, *48*, 100–105.

Elia, N. (2005). Remote stabilization over fading channels. *Systems & Control Letters*, *54*, 237–249.

Gatsis, K., Ribeiro, A., & Pappas, G. J. (2014). Optimal power management in wireless control systems. *IEEE Transactions on Automatic Control*, *59*, 1495–1510.

Groover, M. P. (2007). *Automation, Production Systems, and Computer-Integrated Manufacturing*. Prentice Hall Press.

Hu, B., & Lemmon, M. D. (2013). 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* (pp. 41–48). ACM.

Hu, B., & Lemmon, M. D. (2015). Distributed switching control to achieve almost sure safety for leader-follower vehicular networked systems. *IEEE Transactions on Automatic Control*, *60*, 3195–3209.

Hu, B., Wang, Y., Orlik, P., Koike-Akino, T., & Guo, J. (2017). Co-design of safe and efficient networked control systems in factory automation with state-dependent wireless fading channels. *arXiv preprint arXiv:1708.06468*, . URL: `https://arxiv.org/pdf/1708.06468.pdf`.

Isidori, A. (1995). *Nonlinear control systems*. Springer Science & Business Media.

Islam, K., Shen, W., & Wang, X. (2012). Wireless sensor network reliability and security in factory automation: A survey. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, *42*, 1243–1256.

Jiang, Z.-P., Teel, A. R., & Praly, L. (1994). Small-gain theorem for ISS systems and applications. *Mathematics of Control, Signals and Systems*, *7*, 95–120.

Kashiwagi, I., Taga, T., & Imai, T. (2010). Time-varying path-shadowing model for indoor populated environments. *IEEE Transactions on Vehicular Technology*, *59*, 16–28.

Khasminskii, R. (2011). *Stochastic Stability of Differential Equations* volume 66. Springer Science & Business Media.

Kushner, H. (1967). *Stochastic Stability and Control*. Academic Press, New York.

Leong, A. S., Quevedo, D. E., Ahlén, A., & Johansson, K. H. (2016). On network topology reconfiguration for remote state estimation. *IEEE Transactions on Automatic Control*, *61*, 3842–3856.

Lewis, F. L., Dawson, D. M., & Abdallah, C. T. (2003). *Robot Manipulator Control: Theory and Practice*. CRC Press.

Maranas, C. D., & Floudas, C. A. (1997). Global optimization in generalized geometric programming. *Computers & Chemical Engineering*, *21*, 351–369.

Molin, A., & Hirche, S. (2009). On LQG joint optimal scheduling and control under communication constraints. In *Proceedings of the IEEE Conference on Decision and Control* (pp. 5832–5838). IEEE.

Nešić, D., & Teel, A. R. (2004). Input-output stability properties of networked control systems. *IEEE Transactions on Automatic Control*, *49*, 1650–1667.

Özekici, S. (1997). Markov modulated bernoulli process. *Mathematical Methods of Operations Research*, *45*, 311–324.

Prajna, S., Jadbabaie, A., & Pappas, G. J. (2007). A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Transactions on Automatic Control*, *52*, 1415–1428.

Quevedo, D. E., Ahlen, A., & Johansson, K. H. (2013). State estimation over sensor networks with correlated wireless fading channels. *IEEE Transactions on Automatic Control*, *58*, 581–593.

Rajhans, A., Bhave, A., Ruchkin, I., Krogh, B. H., Garlan, D., Platzer, A., & Schmerl, B. (2014). Supporting heterogeneity in cyber-physical systems architectures. *IEEE Transactions on Automatic Control*, *59*, 3178–3193.

Tatikonda, S., & Mitter, S. (2004). Control over noisy channels. *IEEE Transactions on Automatic Control*, *49*, 1196–1201.

Tse, D., & Viswanath, P. (2005). *Fundamentals of Wireless Communication*. Cambridge University Press.

Vandenberghe, L., & Boyd, S. (1996). Semidefinite programming. *SIAM Review*, *38*, 49–95.

Wang, H. S., & Moayeri, N. (1995). Finite-state markov channel-a useful model for radio communication channels. *IEEE Transactions on Vehicular Technology*, *44*, 163–171.

Zhang, L., & Hristu-Varsakelis, D. (2006). Communication and control co-design for networked control systems. *Automatica*, *42*, 953–958.

Zhang, Q., Kassam, S. et al. (1999). Finite-state markov model for Rayleigh fading channels. *IEEE Transactions on Communications*, *47*, 1688–1692.

Zhuang, L., Goh, K. M., & Zhang, J.-B. (2007). The wireless sensor networks for factory automation: issues and challenges. In *Proceedings of the IEEE Conference on Emerging Technologies and Factory Automation* (pp. 141–148). IEEE.