

## TOWARDS FAULT-TOLERANT OPTIMAL CONTROL

Howard J. Chizeck  
 Laboratory for Information and  
 Decision Systems  
 Massachusetts Institute of Technology  
 Cambridge, Massachusetts 02139

Alan S. Willsky  
 Laboratory for Information and  
 Decision Systems  
 Massachusetts Institute of Technology  
 Cambridge, Massachusetts 02139

## ABSTRACT

Questions regarding the design of fault-tolerant controllers that may endow systems with dynamic reliability are addressed here. Results for jump linear quadratic Gaussian (JLQG) control problems are extended to include random jump costs, trajectory discontinuities, and a simple case of non-Markovian mode transitions.

## 1. INTRODUCTION

Regardless of how well they are designed and manufactured, engineering systems occasionally fail to function as expected due to component failures and environmental disturbances. As a result, unacceptably high costs may be incurred. Ideally, systems should be designed to be dynamically reliable. That is, they should function "acceptably well" despite various component failures and environmental disturbances. Many complex engineering systems currently in use do not possess this property of fault-tolerance. For example, electrical power systems have been known to experience complete blackouts resulting from the failure of a few components (such as switches), or as a consequence of abrupt disturbances (such as lightning bolts, and sudden loads).

The design of fault-tolerant controllers involves a number of subjective questions. Among these are modelling issues, particularly with respect to failure events, and clarification of different control tasks such as: the detection of failures, the adaptation and reorganization of controllers both in response to detected failures and in anticipation of them, and the prevention of certain failures. Various costs must be quantified and compared, including those relating to operation under different failure conditions, costs incurred at failure instants, and costs related to improper failure detection. The goal is to find objective approaches for the design of fault-tolerant systems; to formulate and solve problems that capture and quantify the subjective issues of fault-tolerant control.

In this paper, some extensions to basic results [1],[2] concerning the control of systems having randomly jumping parameters are presented, as an initial step towards fault-tolerant optimal control.

\* This work was supported in part by the Office of Naval Research under Contract No. N00014-77-C-0224 and in part by NASA Ames Research Center under Grant NGL-22-009-124. The work of the first author was also supported in part by a National Science Foundation Fellowship.

## 2. JUMP LINEAR QUADRATIC GAUSSIAN PROBLEM

Our approach is to model component failures by randomly and abruptly changing parameters (see [3] for a survey of problems of this type). Assume that a given system can operate in  $N < \infty$  different modes, each corresponding to a particular set of component and environmental conditions. Motivated by concerns of robustness and implementability, as well as mathematical tractability, a linear quadratic Gaussian problem formulation can be chosen for operation in each mode.

Let  $\rho(t) \in \{1, \dots, N\}$  denote the mode of the system at time  $t$ , where  $\{\rho(t); t \leq T\}$  is a finite state Markov process having transition probabilities

$$(1) \Pr\{\rho(t+dt)=j | \rho(t)=i\} = \begin{cases} q_{ij}(t)dt + o(dt) & i \neq j \\ 1 - q_j(t)dt + o(dt) & i = j \end{cases}$$

and initial probability distribution  $P(t_0)$ . The

$q_{ij}$  and  $q_j$  are continuous nonnegative functions, and  $q_j(t) = \sum_{k \neq j} q_{jk}(t)$ .

In between jumps in  $\rho$ , the system state trajectory  $x(t)$  satisfies a vector stochastic differential equation

$$(2) \dot{x} = [A(t,k)x(t) + B(t,k)u(t)]dt + C(t,k)dw(t) \\ x(t_0) = x_0$$

for each mode  $k$ , where  $x \in \mathbb{R}^n$ ,  $u \in \mathbb{R}^m$  is the control,  $w(t)$  is a separable Wiener process and  $x_0$  is a Gaussian random variable independent of the  $dw$  increments. Assume that  $A(t,k), B(t,k), C(t,k)$  are piecewise-continuous in  $t$  on the known finite interval  $[t_0, T]$ , for each  $k \in \{1, \dots, N\}$ .

Together the joint process  $\{x(t), \rho(t)\}$  is assumed to be Markov, and it is assumed that both  $x(t)$  and  $\rho(t)$  are perfectly observed at each  $t$ . The "jump linear quadratic Gaussian" control problem involves minimization of the quadratic cost functional

$$(3) E\{J[u]\} = E \left\{ \int_{t_0}^T [x'(s)Q(s, \rho(s))x(s) + u'(s)R(s, \rho(s))u(s)] ds + x'(T)K_T(\rho(T))x(T) \right\}$$

where  $u(t)$  is specified by a feedback control law satisfying certain technical conditions (see [1]). The matrices  $Q(t,j) = Q(t,j)'$   $\geq 0$  and  $R(t,j) = R(t,j)'$   $\geq \epsilon I$  ( $\epsilon > 0$ ) are piecewise continuous in  $t$ , and  $K_T(j) = K_T'(j) \geq 0$ , for each  $j$ . Using either dy-

dynamic programming methods [1] or a stochastic maximum principle [2], it can be shown that the optimal feedback control law for operation in each mode  $\rho(t)=j$  has the linear form

$$(4) \quad u^*(t) = -R^{-1}(t,j)B'(t,j)K(t,j)x(t)$$

where the symmetric  $n \times n$  matrices  $K(t,j) \geq 0$  are specified by  $N$  coupled matrix Riccati differential equations.

This problem captures some aspects of fault-tolerant control. Changes in parameters  $A, B, C$  model abrupt failure events such as actuator failures, broken connections, and the like. Different relative weightings can be assigned to quantities such as performance tolerance and expended control energy in various modes, through  $Q, R$  and  $K_T$  values.

When the mode of the system changes, there may be random jump costs incurred that reflect "start-up" or "shut-down" costs, and transient costs resulting from the need to switch controls. One way to incorporate them in the optimal control problem is to charge costs  $x'(t)Z_{ij}(t)x(t)$  when the mode shifts from  $i$  to  $j$  at time  $t$ , where the  $Z_{ij}(t) \geq 0$  are independent  $n \times n$ -valued symmetric matrices of stochastic processes with mean value functions  $Z_{ij}(t) = Z_{ij}'(t) \geq 0$  and finite variances (and are independent of  $x_0, \rho_0, w(t)$ ). The cost functional then becomes

$$(5) \quad E\{J_1[u]\} = E\{J[u] + \sum_{i,j \neq i} \int_{t_0}^T x'(t) Z_{ij}(t) x(t) q_{ij}(t) dt\}.$$

When the mode of the system shifts, there may also be random discontinuities in trajectory  $x(t)$ , resulting from impulsive external disturbances, or phenomena such as changes in amplifier biases. If the modes represent different linearized models of a nonlinear system, jumps in  $x(t)$  might correspond to initialization along different nominal paths. Deterministic discontinuities linear in  $x(t)$  are considered in [4]. Here we assume that the trajectory jumps are described by

$$(6) \quad x(t^+) = F_{ij}(t)x(t^-) + H_{ij}(t)v_{ij}(t)$$

when the mode shifts from  $i$  to  $j$  at  $t$ .  $F_{ij}(t) \in R^{n \times n}$  and  $H_{ij} \in R^{n \times q}$  are continuous in  $t$  and deterministic; the  $v_{ij}(t)$  are independent  $R^q$ -valued zero-mean stochastic processes, with finite variances  $V_{ij}(t)$ , independent of  $x_0, \rho_0, w(t)$  and the  $Z_{ij}(t)$ . The

cost functional (5), for a system described by (1), (2) and (6), is minimized by a linear feedback control law of form (4), where the  $K(t,j) \geq 0$  are specified by the  $N$  coupled equations on  $[t_0, T]$ :

$$\begin{aligned} -\dot{K}(t,j) &= A(t,j)'K(t,j) + K(t,j)A(t,j) + Q(t,j) \\ &- K(t,j)B'(t,j)R^{-1}(t,j)B(t,j)K(t,j) - q_j(t)K(t,j) \\ &+ \sum_{i \neq j} q_{ji}(t) [F_{ji}(t)K(t,i)F_{ji}(t) + Z_{ji}(t)] \end{aligned} \quad (7)$$

where  $K(T,j) = K_T(j)$ . The optimal cost-to-go from  $(t_0, x(t_0), \rho(t_0))$  is

$$(8) \quad x'(t_0)K(t_0, \rho(t_0))x(t_0) + r(t_0, \rho(t_0))$$

where the scalar term  $r$  satisfies, with  $r(T,j) = 0$ ,

$$\begin{aligned} \dot{r}(t,j) &= -\text{tr}\{C'(t,j)'K(t,j)C(t,j)\} + q_k(t)r(t,j) \quad (9) \\ &- \sum_{i \neq j} q_{ji}(t) [r(t,i) + \text{tr}\{H_{ji}'(t)K(t,i)H_{ji}(t)V_{ji}(t)\}]. \end{aligned}$$

The proof of this result involves a straightforward application of the Bellman equation, as in [1].

### 3. FURTHER CONSIDERATIONS

There are many other aspects of fault-tolerant control that are not captured by the above formulation. For example,  $x(t)$  and  $\rho(t)$  are often not perfectly observable. If a linear function of  $x(t)$  is observed in the presence of additive Gaussian white noise (but  $\rho(t)$  is perfectly observed), then a separation (certainty equivalence) result follows, due to the linear quadratic formulation. In each mode, a Kalman filter generates the best (conditional mean) estimate of  $x(t)$  which is then used by the optimal feedback control law as the true value. If  $\rho(t)$  is also not perfectly observed, then the combined filtering and control problem is much harder because of 'adaptive-dual' difficulties; that is,  $u(t)$  can be used both to control the system, and to "probe" for information useful in estimating  $x$  and  $\rho$ .

The  $\{\rho(t)\}$  process need not be Markov; for example, in some systems past mode values and  $x(t)$  histories may affect mode transition rates. Suppose there exists a stochastic process  $\{\beta(t)\}$  such that the joint process  $\{\rho(t), \beta(t)\}$  is Markov, and the intensities in (1) are of the form  $q_j(t, \beta(t))$ ,  $q_{ij}(t, \beta(t))$ . If  $\beta(t)$  changes values only when  $\rho(t)$  jumps (and not in between), then the optimal control law has the form (4), where the gains  $K(t, \rho(t), \beta(t))$  are given by (7)-(8) but are parameterized by  $\beta$ .  $\beta(t)$  might correspond to the past order of mode shifts (thus taking values in a finite set) or to mode shift times. These can be used to incorporate models of component failures that are dependent upon elapsed times of operation.

If  $\beta(t)$  changes values between  $\rho(t)$  jumps, the control problem appears to be much more difficult. Another problem formulation (currently under study) includes voluntary changes in  $\rho(t)$ , as control actions with associated costs. Some limited results of this type are given in [5], [6].

#### REFERENCES

1. Wonham, W.M., "Random Differential Equations in Control Theory," in Probabilistic Methods in Applied Mathematics, Vol. 2, A.T. Bharucha-Reid, Ed., Academic Press (New York), 1970, pp. 132-212.
2. Sworder, D.D., "Feedback Control of a Class of Linear Systems with Jump Parameters," IEEE Trans. A.C., Vol. AC-14, No. 1, pp. 9-14.
3. Sworder, D.D., "Control of Systems Subject to a Sudden Change in Characters," Proc. of the IEEE, Vol. 64, No. 8, pp. 1219-1225, Aug. 1976.
4. Sworder, D.D., "Control of Jump Parameter Systems with Discontinuous State Trajectories," IEEE Trans. AC, Vol. AC-17, pp. 740-741.
5. Ratner, R.S. and Luenberger, D.G., "Performance Adaptive Renewal Policies for Linear Systems," IEEE Trans. on Aut. Cont., Vol. AC-14.
6. Sworder, D.D., "Uniform Performance-Adaptive Renewal Policies for Linear Systems," IEEE Trans. A.C., Vol. AC-15, pp. 581-583, Oct. 1970.