Preprints of the 19th World Congress
The International Federation of Automatic Control
Cape Town, South Africa. August 24-29, 2014

A Hybrid Stochastic-Deterministic Approach For Active Fault Diagnosis Using Scenario Optimization

G.R. Marseglia * **J.K. Scott** ** **L. Magni** *** **R.D. Braatz** **** **D.M. Raimondo** *

* *Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Pavia, Italy (e-mail: davide.raimondo@unipv.it; groberto.marseglia@gmail.com)*
** *Department of Chemical and Biomolecular Engineering, Clemson University, SC, USA (e-mail: jks9@clemson.edu)*
*** *Dipartimento di Ingegneria Edile e Architettura, Università degli Studi di Pavia, Italy (e-mail: lalo.magni@unipv.it)*
**** *Massachusetts Institute of Technology, Cambridge, MA, USA (e-mail: braatz@mit.edu)*

Abstract: Active fault diagnosis can improve the diagnosability of potential faults by injecting a suitable input into the system. This input can be designed using either a stochastic or a deterministic framework. The stochastic approach aims to maximize the probability of a correct diagnosis at a certain time, whereas the deterministic approach aims to guarantee diagnosis within a certain time interval. Recently, a hybrid stochastic-deterministic approach has been developed in which all uncertainties are described by uniform probability density functions (PDFs) with finite support on zonotopes. This method is able to provide a guaranteed diagnosis at a given time N, while approximately maximizing the probability of diagnosis at some earlier time $M < N$. In this article, the hybrid stochastic-deterministic method is extended to arbitrary PDFs using a sampling approach based on scenario optimization.

Keywords: Fault Detection, Fault Diagnosis, Zonotopes, Scenario Approach

1. INTRODUCTION

Component malfunctions and other faults pose a significant threat to the safety and efficiency of complex systems, such as aircraft, power systems, and chemical plants. Over the last few decades, measurement-based methods have been developed to determine whether or not a fault has occurred (fault detection) and, if so, the nature of the fault (fault diagnosis). Disturbances, measurement noise, and other uncertainties make this task very difficult. To avoid performance degradation, it is essential that these systems provide an accurate diagnosis very quickly after the occurrence of a fault. Many methods have been proposed to address this challenge, including residual and observer-based methods (Chiang et al., 2001) and set-based approaches (Lin and Stadtherr, 2008; Stoican, 2011; Tornil-Sin et al., 2012). The vast majority of these methods are *passive*, meaning that the fault status is decided on the basis of input-output data acquired during normal control operation. However, faults are not always detectable at normal operating conditions, or are obscured by the action of the control system itself. *Active fault diagnosis* involves injecting a suitably designed input into the system to improve the detectability and diagnosability of potential faults. The inputs for active fault diagnosis can be designed using deterministic or stochastic formulations. In *deterministic formulations*, the process and measurement noises, along with any uncertainties, are assumed to be bounded. The objective is to achieve values of the measured outputs that can be shown to be consistent with exactly one potential fault scenario (including the nominal case), so that whether a fault (and which fault) has occurred is determined with certainty. Recent works in this direction are Nikoukhah (1998); Nikoukhah and Campbell (2006); Ashari et al. (2012). In contrast, *stochastic formulations* assume probability distribution functions (PDFs) for the process uncertainties, and hence the inputs are designed to maximize some measure of diagnosis probability. In this approach, there is nearly always a finite probability of an incorrect diagnosis. Despite this, stochastic methods often achieve reasonable accuracy in practice, while using much less aggressive inputs than those required by deterministic methods (see, for example, Simandl et al. (2005); Kim et al. (2013); Mesbah et al. (2012)).

Scott et al. (2013b) presents a hybrid stochastic-deterministic input design method that aims to combine the advantages of both approaches. In this work, all uncertainties are described by uniform PDFs with finite support on zonotopes, so that the noises are bounded in the deterministic sense. As in Scott et al. (2013a), these bounds are used to choose an input sequence that guarantees diagnosis on $[0, N]$. However, the approach simultaneously maximizes (in an approximate sense) the probability of an *early diagnosis* in $M < N$ steps. At both N and M, diagnosis is based on checking the consistency of the

measured output with each potential fault model using the deterministic uncertainty bounds. Thus, depending on the measured output, the test is either indeterminate, or a diagnosis can be made with certainty (note that at time N, the latter case is ensured).

The first contribution of this paper is the extension of Scott et al. (2013b) to arbitrary PDFs by an application of the scenario approach (Campi et al., 2009), which is done by first formulating the condition at time M as a deterministic guarantee of diagnosis, and then relaxing this condition through sampling. Using the theory of scenario optimization, the number of samples is then related to a guaranteed lower bound on the probability of diagnosis at M. The second contribution of the paper is a purely stochastic method, obtained from the previous method by dropping the deterministic constraint at time N. According to the above discussion, this method differs from standard stochastic formulations in that an incorrect diagnosis is impossible. Rather than maximizing the probability of a correct diagnosis, the proposed method aims to maximize the probability that sufficient information will be available to make a certain diagnosis at time M. Moreover, the scenario approach provides guaranteed bounds on this probability, rather than only estimates.

2. PROBLEM STATEMENT

Consider a system that on each time step k is described by one of n_m discrete-time linear time-invariant models with state $x_k \in \mathbb{R}^{n_x}$, output $y_k \in \mathbb{R}^{n_y}$, input $u_k \in U \subset \mathbb{R}^{n_u}$, disturbance $v_k \in V \subset \mathbb{R}^{n_v}$, and measurement noise $w_k \in W \subset \mathbb{R}^{n_w}$. Each model is identified with the index $i \in \mathbb{I} = \{1, 2, \ldots, n_m\}$ and evolves according to

$$x_k = A^{[i]}x_{k-1} + B^{[i]}u_{k-1} + r^{[i]} + B_w^{[i]}w_{k-1}, \quad (1)$$

$$y_k = C^{[i]}x_k + s^{[i]} + D_v^{[i]}v_k. \quad (2)$$

The vectors $r^{[i]}$ and $s^{[i]}$ are constant and are used to model additive faults (e.g., actuator or sensor bias). One of these models is considered to be the nominal model; the rest represent different faults. It is assumed that our method provides a diagnosis sufficiently rapidly to guarantee that a single model is active until the diagnosis is provided.

3. PRELIMINARIES

3.1 Sequence Notation

A tilde designates a sequence on $[0, N]$ associated with (1)–(2), for example, $\tilde{u} \equiv (u_0, \ldots, u_{N-1}) \in \tilde{U}$. Another shorthand is $\lambda \equiv (x_0, \tilde{w}, v_N)$, where λ is a random variable distributed according to an arbitrary PDF in the set $\Delta = X_0 \times \tilde{W} \times V$, where $\tilde{W} \equiv W \times \ldots \times W$ denote the sets of disturbances on $[0, N]$ (the number of Cartesian products is N). Note that λ contains all random variables that affect the output at time N, y_N.

3.2 Zonotopes

The supports X_0, W, and V are assumed to be zonotopes, which are centrally symmetric convex polytopes that can be described as Minkowski sums of line segments called *the generators of the zonotope* (Guibas et al., 2003). In *generator representation*, a zonotope Z is fully characterized by its *center* $c \in \mathbb{R}^n$ and *generators* $g_1, \ldots, g_{n_g} \in \mathbb{R}^n$ as

$$Z = \left\{ c + \sum_{i=1}^{n_g} \xi_i g_i : \|\xi\|_\infty \leq 1 \right\}.$$

We use the notation $Z = \{G, c\}$, where $G \equiv [g_1 \ \cdots \ g_{n_g}]$, and note that Z can be equivalently defined as the image of the unit hypercube in $\mathbb{R}^{n_g}$ under the affine mapping $\xi \mapsto G\xi + c$. The *order* of a zonotope is defined as n_g/n. Given Z, $Y \subset \mathbb{R}^n$ and $R \in \mathbb{R}^{m \times n}$,

$$RZ \equiv \{Rz : z \in Z\},$$
$$Z + Y \equiv \{z + y : z \in Z,\ y \in Y\},$$
$$-Z \equiv \{-z \in \mathbb{R}^n : z \in Z\}.$$

For $Z = \{G_z, c_z\}$ and $Y = \{G_y, c_y\}$, these operations can be computed efficiently, even in high dimension by

$$RZ = \{RG_z, Rc_z\}, \quad (3)$$
$$Z + Y = \{[G_z \ G_y], c_z + c_y\}, \quad (4)$$
$$-Z = \{G_z, -c_z\}. \quad (5)$$

Because zonotopes are convex polytopes, they can always be represented as an intersection of a finite number of halfspaces, $Z = \{z : Hz \leq k\}$, which is called the (H,k)-*representation* of Z. An algorithm for converting a zonotope from generator to (H,k)-representation is given by Althoff et al. (2010). The (H,k)-representation makes verifying the membership $z \in Z$ very simple, and will be advantageous for the methods presented in §5. On the other hand, generator representation is often much more compact, and makes the operations (3)–(5) very efficient to perform. Moreover, it is simple and efficient to compute a reduced order zonotope containing the original zonotope (Althoff et al., 2010).

3.3 Reachable Sets

For each model $i \in \mathbb{I}$ and time $k \geq 0$, define the *state solution map* $\phi_k^{[i]} : \mathbb{R}^{kn_u} \times \mathbb{R}^{n_x + kn_w + n_v} \to \mathbb{R}^{n_x}$ and the *output solution map* $\psi_k^{[i]} : \mathbb{R}^{kn_u} \times \mathbb{R}^{n_x + kn_w + n_v} \to \mathbb{R}^{n_y}$, so that $\phi_k^{[i]}(\tilde{u}, \lambda)$ is the state of (1) and $\psi_k^{[i]}(\tilde{u}, \lambda)$ is the output of (2) at k given the initial state x_0, input $\tilde{u}$, disturbance $\tilde{w}$, and measurement noise v_k (the dependence of $\phi_k^{[i]}$ on v_k is trivial, but simplifies notation).

Definition 1. Define the *state reachable set* and *output reachable set* for model i at time k, respectively, as

$$\Phi_k^{[i]}(\tilde{u}, \Delta) \equiv \{\phi_k^{[i]}(\tilde{u}, \lambda) : \lambda \in \Delta\}, \quad (6)$$
$$\Psi_k^{[i]}(\tilde{u}, \Delta) \equiv \{\psi_k^{[i]}(\tilde{u}, \lambda) : \lambda \in \Delta\}. \quad (7)$$

For brevity, explicit dependence of the reachable sets on Δ will be omitted. Iterating (1)–(2) k times yields matrices $\tilde{A}^{[i]}, \tilde{B}^{[i]}$, etc. such that

$$\phi_k^{[i]}(\tilde{u}, \lambda) = \tilde{A}^{[i]}x_0 + \tilde{B}^{[i]}\tilde{u} + \tilde{r}^{[i]} + \tilde{B}_w^{[i]}\tilde{w}.$$

It follows that

$$\Phi_k^{[i]}(\tilde{u}) = \tilde{A}^{[i]}X_0 + \tilde{B}^{[i]}\tilde{u} + \tilde{r}^{[i]} + \tilde{B}_w^{[i]}\tilde{W},$$
$$\Psi_k^{[i]}(\tilde{u}) = C^{[i]}\Phi_k^{[i]}(\tilde{u}) + s^{[i]} + D_v^{[i]}V.$$

Since X_0, W, and V are zonotopes, these equations imply that $\Phi_k^{[i]}(\tilde{u})$ and $\Psi_k^{[i]}(\tilde{u})$ are zonotopes and can be com-

puted efficiently using (3)–(5). In particular, with $X_0 \equiv \{G_0, c_0\}$, $\tilde{W} \equiv \{G_{\tilde{W}}, 0\}$, and $V \equiv \{G_V, 0\}$,

$$\Phi_k^{[i]}(\tilde{u}) = \left\{ \left[\tilde{A}^{[i]} G_0 \tilde{B}_w^{[i]} G_{\tilde{W}}\right], \overline{\phi}_k^{[i]}(\tilde{u}, c_0) \right\} \text{ and}$$

$$\Psi_k^{[i]}(\tilde{u}) = \left\{ \left[C^{[i]} \left[\tilde{A}^{[i]} G_0 \ \tilde{B}_w^{[i]} G_{\tilde{W}}\right] D_v^{[i]} G_V\right], \overline{\psi}_k^{[i]}(\tilde{u}, c_0) \right\},$$

where $\overline{\phi}_k^{[i]}(\tilde{u}, c_0) \equiv \tilde{A}^{[i]} c_0 + \tilde{B}^{[i]} \tilde{u} + \tilde{r}^{[i]}$ and $\overline{\psi}_k^{[i]}(\tilde{u}, c_0) \equiv C^{[i]} \overline{\phi}_k^{[i]} + s^{[i]}$ (i.e., the state and output of (3)–(5) when $\lambda = (c_0, 0, 0)$). Note that u affects the center of these sets, but not their generator matrices (i.e., their shapes). It follows by applying the algorithm of Althoff et al. (2010), that $\Phi_k^{[i]}(\tilde{u})$ and $\Psi_k^{[i]}(\tilde{u})$ can be described by (H,k)-representations of the form $\{z : Hz \leq k(\tilde{u})\}$.

4. REVIEW OF THE DETERMINISTIC APPROACH

This section briefly reviews the method of Scott et al. (2013a) for computing an input $\tilde{u} = (u_0, ..., u_{N-1})$ that guarantees diagnosis at time N. Specifically, diagnosis is performed online by checking the inclusion $y_N \in \Psi_N^{[i]}(\tilde{u})$, for each $i \in \mathbb{I}$. Noting that this must hold for at least one i, *diagnosis* is said to occur if

$$\exists i \in \mathbb{I} : y_N \in \Psi_N^{[i]}(\tilde{u}),\ y_N \notin \Psi_N^{[j]}(\tilde{u}),\ \forall j \in \mathbb{I}, i \neq j. \quad (8)$$

The objective is to design an input that guarantees this condition, which may be stated equivalently as

$$\Psi_N^{[i]}(\tilde{u}) \bigcap \Psi_N^{[j]}(\tilde{u}) = \emptyset,\ \forall (i,j) \in \mathbb{I},\ i \neq j. \quad (9)$$

To identify a minimally invasive input of this type, consider the optimization

$$\min_{\tilde{u}} \ \tilde{u}^{\mathrm{T}} R \tilde{u},\ \text{s.t. } \tilde{u} \in \tilde{U},\ (9) \text{ holds},$$

where and $\tilde{u}^{\mathrm{T}} R \tilde{u}$ is a positive semidefinite quadratic function representing the harmful effect of the active input on the system that needs to be minimized, and $\tilde{U} \equiv U \times ... \times U$ is a polyhedral input constraint. In order to solve this problem, the constraints (9) have to be rewritten in a suitable way. To this end, rewrite the reachable sets in the generator representation $\Psi_N^{[i]}(\tilde{u}) = \{G_N^{[i]}, c_N^{[i]}(\tilde{u})\}$ and observe that (9) is equivalent to the condition $\nexists (\xi, \gamma) \in \mathbb{R}^{n_g \times n_g} : c_N^{[i]}(\tilde{u}) + G_N^{[i]} \xi = c_N^{[j]}(\tilde{u}) + G_N^{[j]} \gamma,\ \|\xi\|_\infty \leq 1$, and $\|\gamma\|_\infty \leq 1$. This condition can be written as $\delta_N^{[ij]}(\tilde{u}) > 1$ where

$$\delta_N^{[ij]}(\tilde{u}) \equiv \min \delta^{[ij]} \quad (10)$$

$$\text{s.t. } G_N^{[i]} \xi + c_N^{[i]}(\tilde{u}) = G_N^{[j]} \gamma + c_N^{[j]}(\tilde{u}), \quad (11)$$

$$\|\xi\|_\infty \leq \delta^{[ij]}, \|\gamma\|_\infty \leq \delta^{[ij]}. \quad (12)$$

The optimization becomes

$$\inf_u \ \tilde{u}^{\mathrm{T}} R \tilde{u},\ s.t.\ \tilde{u} \in U,\ 1 < \delta_N^{[ij]}(\tilde{u}),\ \forall (i,j), i \neq j. \quad (13)$$

Since (10)–(12) define a linear program (LP), the constraints in (13) can be replaced by their necessary and sufficient conditions of optimality. After further reformulations, the problem can be rewritten as a MIQP that can be easily solved with, for example, CPLEX. The details of this optimization problem can be found in Scott et al. (2013a). Although this method guarantees diagnosis, it can result in very aggressive inputs. Moreover, because (13) does not consider the distribution of uncertainties, it can lead to inputs that consistently require all N steps for diagnosis in simulations. For these reason, the following sections reformulate the problem in a sample-based framework with the aim of maximizing the probability of early diagnosis for uncertainties described by arbitrary PDFs.

5. MAXIMIZING THE PROBABILITY OF DIAGNOSIS

This section considers the problem of computing an input $\tilde{u}$ that maximizes the probability of diagnosis at time N (i.e., maximizes the probability of observing y_N such that (8) holds). As a first step, §5.1 considers inputs that satisfy a specified lower bound on the probability of diagnosis. This formulation is then extended in §5.2 so that $\tilde{u}$ is chosen so as to approximately maximize this bound within a single optimization.

5.1 Satisfying an a priori *Probability Bound*

In order to establish a lower bound on the probability of diagnosis, begin with the deterministic formulation for guaranteed diagnosis in §4, and subsequently relax this condition through sampling. Using the theory of scenario optimization (Campi et al., 2009), the number of samples can then be rigorously related to the probability of diagnosis. To begin, it is necessary to reformulate the diagnosis condition (9) in a form compatible with the results in Campi et al. (2009). To this end, first note that (9) is equivalent to $\psi_N^{[i]}(\tilde{u}, \lambda) \notin \Psi_N^{[j]}(\tilde{u}),\ \forall \lambda \in \Delta,\ \forall (i,j) \in \mathbb{I}^2, i \neq j$. Next, recall that each zonotope $\Psi_N^{[j]}(\tilde{u}) = \{G_N^{[j]}, c_N^{[j]}(\tilde{u})\}$ has an (H,k)-representation of the form $\Psi_N^{[j]}(\tilde{u}) = \{z : H_N^{[j]} z \leq k_N^{[j]}(\tilde{u})\}$, where $k_N^{[j]}$ is an affine function of $\tilde{u}$ (see §3). Thus, the condition that $\psi_N^{[i]}(\tilde{u}, \lambda) \notin \Psi_N^{[j]}(\tilde{u})$ is equivalent to requiring that at least one of the conditions $-h_{N,t}^{[j]} \psi_N^{[i]}(\tilde{u}, \lambda) < -k_{N,t}^{[j]}(\tilde{u})$, $t \in \{1, \ldots, n_h\}$ is satisfied, where $h_{N,t}^{[j]}$ is the t^{th} row of $H_N^{[j]}$ and $k_{N,t}^{[j]}$ is the t^{th} element of $k_N^{[j]}$. This equivalence leads to the reformulation of (9):

$$-h_{N,t}^{[j]} \psi_N^{[i]}(\tilde{u}, \lambda) < -k_{N,t}^{[j]}(\tilde{u}) + \alpha(1 - p_t^{[ij]}),\ \forall \lambda \in \Delta \quad (14)$$

$$\sum_{t=1}^{n_h^{[j]}} p_t^{[ij]} \geq 1, \quad p_t^{[ij]} \in \{0,1\},\ \forall t \in \{1, .., n_h^{[j]}\}, \quad (15)$$

$$\forall (i,j) \in \mathbb{I}^2,\ i \neq j. \quad (16)$$

The binary variables $p_t^{[ij]}$ determine whether or not the corresponding constraint (14) is active: if $p_t^{[ij]} = 1$, then (14) is active; if $p_t^{[ij]} = 0$, then, provided that α is sufficiently large, (14) is trivially satisfied. For $\tilde{u} \in \tilde{U}$ with $\tilde{U}$ bounded, a sufficiently large α exists because the function $(\tilde{u}, \lambda) \mapsto -h_{N,t}^{[j]} \psi_N^{[i]}(\tilde{u}, \lambda) + k_{N,t}^{[j]}(\tilde{u})$ is continuous. To see that conditions (14)–(16) imply (9), choose $\tilde{u} \in \tilde{U}$ and suppose that there exist $p_t^{[ij]}$ such that (14)–(16) hold. Then, for each pair (i,j), t may be chosen such that $p_t^{[ij]} = 1$, and for this t, (14) clearly implies that $\Psi_N^{[i]}(\tilde{u})$ and $\Psi_N^{[j]}(\tilde{u})$ are disjoint. On the other hand, the conditions (14)–(16) are not equivalent to (9) because they require that $\Psi^{[i]}(\tilde{u})$ is separated from $\Psi^{[j]}(\tilde{u})$ by a single hyperplane $h_{N,t}^{[j]}$.

Thus, (14)–(16) is a conservative reformulation of (9). However, the conservatism can be reduced by augmenting the (H,k)-representation of $\Psi^{[j]}(\tilde{u})$ with additional redundant constraints $h_{N,t}^{[j]} z \leq k_{N,t}^{[j]}(\tilde{u})$, $t{=}n_h^{[j]}{+}1,\ldots,n_h^{[j]}{+}\ell$. In particular, we choose additional constraints corresponding to the hyperplanes defining the facets of $\Psi^{[i]}(\tilde{u})$, so that $h^{[j]}_{N,n_h^{[j]}+t}{=}h^{[i]}_{N,t}$, $t{=}1,\ldots,n_h^{[i]}$. Briefly making use of the generator representation of $\Psi^{[i]}(\tilde{u})$, the corresponding k values are given by $k^{[j]}_{N,n_h^{[j]}+t}(\tilde{u}) = h^{[i]}_{N,t}c^{[j]}_N(\tilde{u}){+}\|h^{[i]}_{N,t}G^{[j]}_N\|_1$. Now consider replacing the diagnosis constraint in (13) with (14)–(16), which results in a mixed-integer program with the following property. For each fixed realization of the binary variables, the program has robust constraints of the general form $f(\tilde{u},\lambda) \leq 0$, $\forall\lambda \in \Delta$, where $f(\cdot,\lambda)$ is linear, and hence convex on $\tilde{U}$, for each fixed $\lambda \in \Delta$. This mathematical form is compatible with the theory of scenario optimization of Campi et al. (2009); Campi and Garatti (2008), which relates the solution of such robust optimizations with the solution obtained by replacing Δ with a subset Ω of finite cardinality. Thus, we consider the scenario optimization corresponding to (13):

$$\min_{\tilde{u},p_t^{[ij]}} \tilde{u}^{\mathrm{T}} R \tilde{u} \tag{17}$$

$$\text{s.t. } \tilde{u} \in \tilde{U} \tag{18}$$

$$-h^{[j]}_{N,t}\psi^{[i]}_N(\tilde{u},\lambda) < -k^{[j]}_{N,t}(\tilde{u}) + \alpha(1-p_t^{[ij]}), \tag{19}$$

$$\sum_{t=1}^{n_h^{[j]}} p_t^{[ij]} \geq 1,\ t=1,..,n_h^{[j]} \tag{20}$$

$$\forall (i,j) \in \mathbb{I}^2,\ i \neq j, \forall\lambda \in \Omega \subset \Delta. \tag{21}$$

Choose any *violation parameter* $\epsilon \in (0,1)$ and *confidence parameter* $\beta \in (0,1)$, and let N_{samp} satisfy

$$\sum_{j=1}^{k}\sum_{i=0}^{d-1} \binom{N_{samp}}{i} \epsilon^i (1-\epsilon)^{N_{samp}-i} \leq \beta, \tag{22}$$

where d and k are the numbers of continuous and binary variables in (17)–(21), respectively. The results of Calafiore et al. (2012), and more recently of Esfahani et al. (2012), show that the solution of (17)–(21) with $|\Omega| = N_{samp}$ satisfies the subsequent condition with probability at least $1-\beta$. The solution violates the constraints (14)–(16) for a subset of Δ that has probability at most ϵ. Choosing β very small (e.g. $\beta = 10^{-20}$), this implies that it is sufficient to solve (17)–(21) with $|\Omega| = N_{samp}$ in order to guarantee diagnosis with probability at least $1-\epsilon$ with practical certainty (the expression "*with practical certainty*" shall be used in the rest of this note as a synonym of "*with probability larger than* $1-\beta$", where $\beta > 0$ is some extremely small value). This remarkable result is an extension to mixed-integer programs of the results for convex programs originally presented by Campi and Garatti (2008) and Campi et al. (2009).

5.2 Maximization of the Probability Bound

The main disadvantage of the method in the previous section is that ϵ has to be tuned *a priori*, which has two consequences. The first is that feasibility is not guaranteed. Moreover, if the problem is feasible, the probability bound $1-\epsilon$ is not necessarily the best possible. In order to overcome these problems, this section extends the approach by presenting a method that can approximately modify this probability bound during the optimization of $\tilde{u}$. Moreover, a method is given for computing a guaranteed probability bound for the computed input *a posteriori*. As done by Calafiore and Fagiano (2013), introduce a slack variable ρ to make the optimization feasible for all possible N and for all possible sample sets Ω as

$$\min_{\tilde{u},\rho,p_t^{[ij]}} \tilde{u}^{\mathrm{T}} R \tilde{u} + \gamma\rho \tag{23}$$

$$\text{s.t. } \tilde{u} \in \tilde{U} \tag{24}$$

$$-h^{[j]}_{N,t}\psi^{[i]}_N(\tilde{u},\lambda) < -k^{[j]}_{N,t}(\tilde{u}) + \alpha(1-p_t^{[ij]}) + \rho, \tag{25}$$

$$\sum_{t=1}^{n_h^{[j]}} p_t^{[ij]} \geq 1, \quad \rho \geq 0, \qquad \forall\lambda \in \Omega \subset \Delta, \tag{26}$$

$$\forall t \in \{1,..,n_h^{[j]}\},\ \forall (i,j) \in \mathbb{I}^2,\ i \neq j. \tag{27}$$

where γ represents a weighting scalar that can be chosen by the designer and is in most cases set as a very large number (exceeding the upper bound of $\tilde{u}^{\mathrm{T}} R \tilde{u}$, $\forall\tilde{u} \in U$). We can also provide a bound $\overline{\rho}$ on ρ, since $\tilde{u}$ lies in a bounded set and the samples are taken from bounded sets. Thus, the problem (23)–(27) is always feasible having $\rho \leq \overline{\rho}$, and we choose α such that $\alpha \geq \overline{\rho}$. In practical uses, α will be set equal to a very large number, say 10^6, and ρ can be bounded to be $\rho \leq \alpha$. As in the previous section, the above program is in a mathematical form compatible with the results of Calafiore et al. (2012). Thus, if (22) holds, the same probabilistic guarantees follow. However, when the optimal value ρ^* of ρ is nonzero, the conclusion that the constraints will be satisfied for a subset of Δ with probability at least $1-\epsilon$ does not imply that diagnosis will occur with probability $1-\epsilon$. This situation can be overcome either by solving this problem with increasing N until $\rho^* = 0$, or by computing a valid lower bound on the probability of diagnosis for the optimal input *a posteriori*. Similarly to Campi and Garatti (2011), the latter can be achieved by pruning all of the samples $\lambda \in \Omega$ that violate the constraints (14)–(16) as follows. Compute

$$\rho_\lambda \equiv \min_{\rho,p_t^{[ij]}} \rho \tag{28}$$

$$\text{s.t. } \rho \geq 0, \tag{29}$$

$$-h^{[j]}_t\psi^{[i]}_N(\tilde{u},\lambda) < -k^{[j]}_t(\tilde{u}) + \alpha(1-p_t^{[ij]}) + \rho \tag{30}$$

$$\sum_{t=1}^{n_h^{[j]}} p_t^{[ij]} \geq 1, \forall t \in \{1,\ldots,n_h^{[j]}\}, \forall (i,j) \in \mathbb{I},\ i \neq j. \tag{31}$$

Next, eliminate from Ω every λ such that $\rho_\lambda > 0$, so that only N^* elements are left in Ω. Let $P = N_{samp} - N^*$. Then, following the proof of Algorithm 4.1 in Esfahani et al. (2012), we can extend the results in Campi and Garatti (2011) and say with practical certainty (probability $1-\beta$) that the probability of diagnosis in N steps with input $\tilde{u}^*$ is at least $1-\epsilon$, with $\epsilon > 0$ the smallest value satisfying

$$\sum_{j=1}^{k} \binom{P+d-1}{P} \sum_{i=0}^{P+d-1} \binom{N_{samp}}{i} \epsilon^i (1-\epsilon)^{N_{samp}-i} \leq \beta. \tag{32}$$

The addition of ρ in (23)–(27) provides a heuristic method for modifying the probability level ϵ during optimization, whereas a true lower bound on the probability of diagnosis

for the computed $\tilde{u}$ is only computed a posteriori. Thus, the computed $\tilde{u}$ is suboptimal in the sense that it may not maximize the probability bound $1-\epsilon$. This approach can be improved by the algorithm:

Algorithm 1. Solve the optimization (23)–(27) (or run Algorithm 2) to obtain ρ^* and $\tilde{u}^*$:

WHILE $\rho^* > 0$ ***AND*** $\Omega \neq \emptyset$
(1) Calculate all the ρ_λ as described in (28)–(31) and eliminate all $\lambda \in \Omega$ with $\rho_\lambda = \rho^*$.
(2) With the updated sample set, solve (23)–(27) to obtain ρ^* and $\tilde{u}^*$.
END WHILE

With the N^* samples remaining after termination of Algorithm 1, the probability of diagnosis in N steps with input $\tilde{u}^*$ can be computed as before. Note that the optimization (23)–(27) can potentially be very large and could pose some computational issues due to the potentially large number of samples, but more so due to the large number of binary variables that may be required in the reformulation (14)–(16). However, the primary reason for this reformulation was to demonstrate that the theoretical results of scenario optimization are applicable. For the purposes of numerical simulation, an alternative formulation is proposed in which $\rho = \rho(\tilde{u}, \Omega)$ is computed for each $\tilde{u}$ via an embedded algorithm that removes the need for any binary variables and allows a standard gradient-based approach to be used to find a solution $\tilde{u}$ minimizing $u^{\mathrm{T}}Ru + \rho(\tilde{u}, \Omega)$. This algorithm can check *in parallel*, thus alleviating complexity, for each sample in the output space $\psi^{[i]}(\tilde{u}, \lambda)$ which is the minimum constraint violation $\rho(\psi^{[i]}(\tilde{u}, \lambda))$ so that $\psi^{[i]}(\tilde{u}, \lambda) \notin \Psi^{[j]}(\tilde{u}), \forall (i,j) \in \mathbb{I}$. It then returns the maximum of these constraint violations $(\rho(\tilde{u}, \Omega) \equiv \max(\rho(\psi^{[i]}(\tilde{u}, \lambda))), \forall i \in \mathcal{M}, \forall \lambda \in \Omega)$.

Algorithm 2. ***INPUT*** $\tilde{u}$, Ω ***OUTPUT*** $\tilde{u}^{\mathrm{T}}R\tilde{u} + \gamma\rho(\tilde{u}, \Omega)$:
(1) Compute all $\psi_N^{[i]}(\tilde{u}, \lambda)$, $\forall i \in \mathbb{I}$, $\forall \lambda \in \Omega$
(2) For each $(i,j) \in \mathbb{I}^2$, $i \neq j$, compute the (H,k)-representation of $\Psi_N^{[j]}(\tilde{u})$ (with redundant halfspace constraints from $\Psi_N^{[i]}(\tilde{u})$ as per §5.1).
(3) ***FORALL*** $i \in \mathbb{I}, j \in \mathbb{I}, i \neq j$
(4) $\rho(i,j) = 10^6$
(5) ***FORALL*** $t \in \{1, \ldots, n_h^{[j]}\}$
  (a) $\rho_{temp} = 0$
  (b) ***FORALL*** $\lambda \in \Omega$
    $\rho_{temp} = \max\{\rho_{temp}, -h_{N,t}^{[j]}\psi_N^{[i]}(\tilde{u}, \lambda) + k_{N,t}^{[j]}(\tilde{u})\}$
  (c) ***ENDFORALL***
  (d) $\rho(i,j) = \min\{\rho(i,j), \rho_{temp}\}$
(6) ***ENDFORALL***
(7) ***ENDFORALL***
(8) $\rho(\tilde{u}, \Omega) = \max\{\rho(i,j)\}$
(9) Compute $\tilde{u}^{\mathrm{T}}R\tilde{u} + \gamma\rho(\tilde{u}, \Omega)$

Remark 2. Algorithm 2 can be also used to solve the problem (17)–(21) by just adding the constraint $\rho = 0$ in the outer program.

6. HYBRID STOCHASTIC-DETERMINISTIC INPUT DESIGN

In this section, similarly to what is done by Scott et al. (2013b), the deterministic input design method in Scott et al. (2013a) is combined with the stochastic method considered in the previous section. The result of this combination is the formulation of a *hybrid stochastic-deterministic* input design approach. In particular, an optimization is formulated that chooses an input of minimum norm such that two conditions hold: (1) diagnosis is guaranteed at time N, (2) the probability of diagnosis at a specified time $M < N$ is greater than a lower probability bound. In order to write the whole optimization, an input sequence $\tilde{u}$ is needed so that (23)–(27) holds at time step M and the intersection between the output reachable sets at time N of all the possible couples of models $(i,\ j)$ is the empty set. Recalling that the latter condition is equivalent to ask $\delta_N^{[ij]}(\tilde{u}) > 1$, the problem can be rewritten as

$$\min_{\tilde{u}, p_t, \rho} u^{\mathrm{T}}Ru + \gamma\rho(\tilde{u}, \Omega), \text{s.t. } \tilde{u} \in \tilde{U},\ \min_{i,j \in \mathbb{I}: i \neq j} \delta_N^{[ij]}(\tilde{u}) > 1.$$

The resulting optimization is a bilevel program. However, the inner LPs can replaced with their KKT conditions as in Scott et al. (2013a). The resulting MIQP can be solved efficiently using Algorithm 1. Because the problem has linear constraints and quadratic cost, the conditions described by Esfahani et al. (2012) are satisfied and thus (22) holds.

7. NUMERICAL RESULTS

Consider the four models defined by

$$A^{[1]} = \left[\begin{smallmatrix} 0.60 & 0.20 \\ -0.20 & 0.70 \end{smallmatrix}\right],\ A^{[2]} = A^{[3]} = A^{[4]} = \left[\begin{smallmatrix} 0.84 & 0.28 \\ -0.28 & 0.98 \end{smallmatrix}\right],$$
$$B^{[1]} = B^{[2]} = \left[\begin{smallmatrix} -0.3861 & 0.1994 \\ -0.1994 & 0.3861 \end{smallmatrix}\right],\ B^{[3]} = \left[\begin{smallmatrix} -0.3861 & 0 \\ -0.1994 & 0 \end{smallmatrix}\right],$$
$$B^{[4]} = \left[\begin{smallmatrix} 0 & 0.1994 \\ 0 & 0.3861 \end{smallmatrix}\right],\ B_w^{[i]} = \left[\begin{smallmatrix} 0.1215 & 0.0598 \\ 0.0598 & 0.1215 \end{smallmatrix}\right],\ C^{[i]} = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right],$$
$$D_v^{[i]} = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right],\ r^{[i]} = s^{[i]} = \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right],\ i = 1, \ldots, 4.$$

Model 2 is considered to be the nominal model; Model 1 has system faults while Models 3 and 4 have faulty actuators. The support of the PDF for λ is $X_0 \times \tilde{W} \times V$, where X_0, $\tilde{W}$, and V are zonotopes defined, in generator notation, as

$$X_0 = \{0.4\mathbf{I}, [1\ \ 1]^{\mathrm{T}}\};\quad V = W = \{0.4\mathbf{I}, [0\ \ 0]^{\mathrm{T}}\}.$$

$\lambda = (x_0, \tilde{w}, v_N) \in X_0 \times \tilde{W} \times V$ is a random variable distributed according to

$$x_0 = c_{X_0} + G_{X_0}\left[\sum_{i=1}^{3}\sigma_i/3,\ \sum_{i=1}^{4}\sigma_i/4\right]^{\mathrm{T}},$$
$$v_k = w_k = c_W + G_W\left[\sum_{i=1}^{3}\sigma_i/3,\ \sum_{i=1}^{4}\sigma_i/4\right]^{\mathrm{T}},$$

where each σ_i is uniformly distributed in $[-1, 1]$, and each of the above equations uses different values so that x_0, w_k, and v_k are independent. The goal of the first example is to synthesize an input $\tilde{u}_1$ that maximizes the probability of separation in $M = 3$ steps and to provide a lower bound on the probability of diagnosis. Given that $\tilde{u}_1$ was synthesized using $N_{samp} = 800$ samples and $P = 10$ of them were pruned, a probability bound ϵ was computed according to (32). For $\beta = 10^{-20}$, this results in $\epsilon = 0.12$, so that, with practical certainty, diagnosis will occur with a probability of at least 0.88. To verify this bound, Monte Carlo simulation was carried out with 10^4 samples, and $\tilde{u}_1$ was observed to provide a diagnosis in 3 steps in 99% of cases. As another example, consider imposing a deterministic guarantee of diagnosis at $N = 5$, while simultaneously maximizing the probability of diagnosis at $M = 3$ (see §6). The result is shown in Figure 2 while Figure 1 reports the result with only the deterministic constraint at $N = 5$. The comparison of the two figures clearly shows, for time $k = 3$, that the stochastic approach

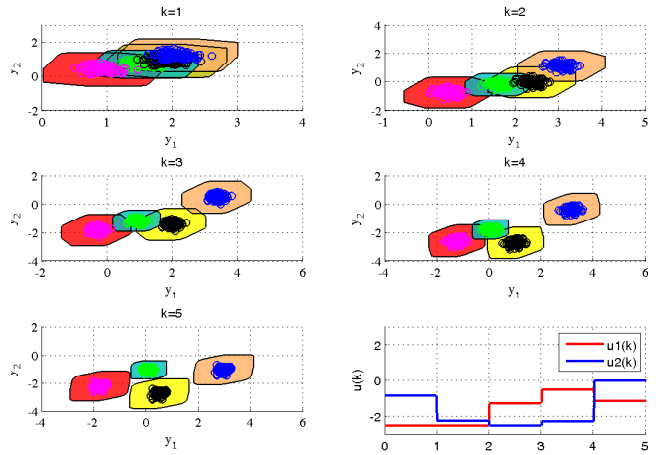

Fig. 1. *Deterministic approach*: Output reachable sets of nominal and faulty models using the input $\tilde{u}_2$ that guarantees diagnosis in 5 steps. Colored circles represent 200 samples.

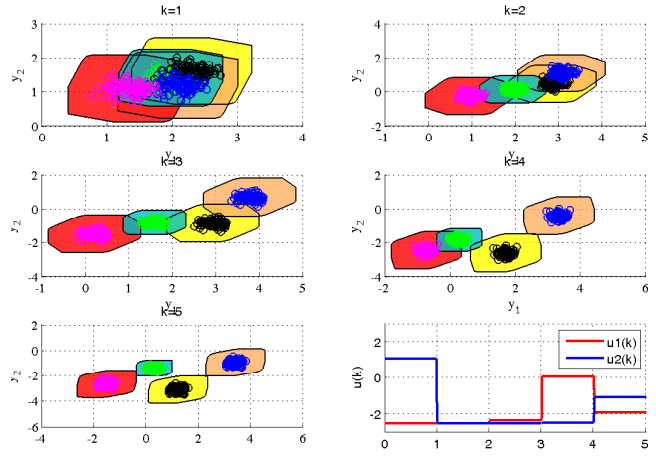

Fig. 2. *Hybrid stochastic-deterministic approach*: Output reachable sets of nominal and faulty models using the input $\tilde{u}_1$ that guarantees separation in 5 steps and approximately maximizes the probability of diagnosis in 3 steps.

leads to less overlapped output reachable sets. On the other side, in order to have a greater probability of early diagnosis, the input needs to be more aggressive and in fact $\frac{\|u_{hybrid}\|_2}{\|u_{deterministic}\|_2} = 1.18$.

REFERENCES

Althoff, M., Stursberg, O., and Buss, M. (2010). Computing reachable sets of hybrid systems using a combination of zonotopes and polytopes. *Nonlinear Analysis–Hybrid Systems*, 4(2), 233–249.

Ashari, A., Nikoukhah, R., and Campbell, S.L. (2012). Effects of feedback on active fault detection. *Automatica*, 48, 866–872.

Calafiore, G. and Fagiano, L. (2013). Robust model predictive control via scenario optimization. *IEEE Trans. Automat. Contr.*, 58(1), 219–224.

Calafiore, G.C., Lyons, D., and Fagiano, L. (2012). On mixed-integer random convex programs. In *Proc. of the 51st IEEE Conference on Decision and Control*, 3508–3513.

Campi, M.C. and Garatti, S. (2008). The exact feasibility of randomized solutions of uncertain convex programs. *SIAM J. on Optimization*, 19(3), 1211–1230.

Campi, M.C. and Garatti, S. (2011). A sampling-and-discarding approach to chance-constrained optimization: Feasibility and optimality. *J. Optim. Theor. Appl.*, 148(2), 257–280.

Campi, M.C., Garatti, S., and Prandini, M. (2009). The scenario approach for systems and control design. *Annu. Rev. Control*, 33(2), 149–157.

Chiang, L.H., Russell, E.L., and Braatz, R.D. (2001). *Fault Detection and Diagnosis in Industrial Systems*. Springer-Verlag, London.

Esfahani, P.M., Sutter, T., and Lygeros, J. (2012). Performance bounds for the scenario approach and an extension to a class of non-convex programs. *arXiv preprint arXiv:1307.0345*.

Guibas, L.J., Nguyen, A., and Zhang, L. (2003). Zonotopes as bounding volumes. In *Proc. of the 14th ACM-SIAM Symposium on Discrete Algorithms*, 803–812.

Kim, K.K.K., Raimondo, D.M., and Braatz, R.D. (2013). Optimum input design for fault detection and diagnosis: Model-based prediction and statistical distance measures. In *Proc. of the European Control Conference*, 1940–1945.

Lin, Y. and Stadtherr, M.A. (2008). Fault detection in nonlinear continuous-time systems with uncertain parameters. *AIChE Journal*, 54(9), 2335–2345.

Mesbah, A., Bombois, X., Forgione, M., Ludlage, J.H., Modén, P.E., Hjalmarsson, H., and Van den Hof, P.M. (2012). A unified experiment design framework for detection and identification in closed-loop performance diagnosis. In *Proc. of the 51st IEEE Conference on Decision and Control*, 2152–2157.

Nikoukhah, R. (1998). Guaranteed active failure detection and isolation for linear dynamical systems. *Automatica*, 34(11), 1345–1358.

Nikoukhah, R. and Campbell, S.L. (2006). Auxiliary signal design for active failure detection in uncertain linear systems with a priori information. *Automatica*, 42(2), 219–228.

Scott, J.K., Findeisen, R., Braatz, R.D., and Raimondo, D.M. (2013a). Design of active inputs for set-based fault diagnosis. *Proc. of the American Control Conference*, 3561–3566.

Scott, J.K., Marseglia, G.R., Magni, L., Braatz, R.D., and Raimondo, D.M. (2013b). A hybrid stochastic-deterministic input design method for active fault diagnosis. *Proc. of the IEEE Conference on Decision and Control*, 5656–5661.

Simandl, M., Puncochar, I., and Kralovec, J. (2005). Rolling horizon for active fault detection. In *Proc. of the IEEE Conf. on Decision and Control*, 3789–3794.

Stoican, F. (2011). *Fault Tolerant Control Based on Set-theoretic Methods*. Ph.D. thesis, Ecole Superieure Delectricite, France.

Tornil-Sin, S., Ocampo-Martinez, C., Puig, V., and Escobet, T. (2012). Robust fault detection of non-linear systems using set-membership state estimation based on constraint satisfaction. *Engineering Applications of Artificial Intelligence*, 25(1), 1–10.