A set based probabilistic approach to threshold design for optimal fault detection

Rostampour Samarin, V.; Ferrari, Riccardo; Keviczky, Tamas

DOI
10.23919/ACC.2017.7963798

Publication date
2017

Document Version
Accepted author manuscript

Published in
Proceedings of the 2017 American Control Conference (ACC 2017)

Accepted Author Manuscript. Link to published article (IEEE): https://doi.org/10.23919/ACC.2017.7963798

A Set Based Probabilistic Approach to Threshold Design for Optimal Fault Detection

Vahab Rostampour, Riccardo Ferrari, and Tamás Keviczky

***Abstract*— Traditional deterministic robust fault detection threshold designs, such as the norm-based or limit-checking method, are plagued by high conservativeness, which leads to poor fault detection performance. On one side they are ill-suited at tightly bounding the healthy residuals of uncertain nonlinear systems, as such residuals can take values in arbitrarily shaped, possibly non-convex regions. On the other hand, they must be robust even to worst-case, rare values of the modeling and measurement uncertainties. In order to maximize performance of detection, we propose two innovative ideas. First, we introduce threshold sets, parametrized in a way to bound arbitrarily well the residuals produced in healthy condition by an observer-based residual generator. Secondly, we formulate a chance-constrained cascade optimization problem to determine such a set, leading to optimal detection performance of a given class of faults, while guaranteeing robustness in a probabilistic sense. We then provide a computationally tractable framework by using randomization techniques, and a simulation analysis where a well-known three-tank benchmark system is considered.**

I. Introduction

Advanced model-based fault diagnosis methods have emerged in important industrial sectors, such as aerospace, as fundamental tools for guaranteeing high operational readiness levels and reducing unneeded maintenance costs [1]. A key problem to be solved for widespread industrial adoption is the development of robust methods providing satisfactory, and easy to tune performances in terms of the so-called *false alarm ratio* (FAR) and *missed detection ratio* (MDR). Ideally a model-based fault diagnosis solution should be *robust* with respect to the unavoidable model and measurement uncertainties, thus having a zero or very low FAR. At the same time, it should have good *fault detection* properties, which translates into a negligible MDR.

Unfortunately, in the general case, it is not possible to simultaneously obtain both zero FAR and zero MDR, so existing designs will favor either one or the other, or seek a reasonable trade-off [1]. In the case of linear systems, and under some conditions also for nonlinear ones [2], [3], [4], geometric approaches lead to residuals that are perfectly decoupled from the uncertainties, thus making the problem of threshold design trivial. For general nonlinear systems, it is customary to assume the existence of a known, static or dynamic upper bound on the uncertainties' magnitude, thus allowing to obtain a zero FAR by design [1]. Such a powerful property often comes at the cost of very conservative thresholds, which lead to high MDR. Two key reasons stand behind this: the inability of traditional norm-based or limit-checking kind of robust deterministic thresholds to tightly bound the arbitrarily shaped, possibly non-convex regions to which healthy residuals belong; and the need to account also for large, but possibly rare values taken by the uncertainties. This last problem in practical situations is exacerbated by the fact that tight dynamic bounds on the uncertainties are seldom known, thus leading to users choosing excessively high and even static bounds.

This paper aims to address both sources of conservativeness by introducing adaptive, arbitrarily shaped threshold *sets* and by relaxing the deterministic robust zero-FAR condition, in favour of a more flexible, *probabilistic* one. Through a set-based approach to threshold design, the probability of false alarms will be defined as a user-tunable design parameter, and the detection with respect to a given class of faults will be simultaneously maximized.

The use of probabilistic thresholds in model-based fault diagnosis has been investigated previously in the literature (see [1] and the references cited therein), and recently the important case of nonlinear uncertain systems has been considered [5], [6], [7]. The use of sets in fault diagnosis has been inspired by the corpus of works on set-membership system identification [8], [9], [10], which initially addressed the inverse problem of finding, at each time step, the set of system parameters that could be able to explain current measurements, and compare it to a nominal one [11], [12]. Other works considered instead the direct problem of describing the admissible values of the residual in healthy condition using a set [13], [14], with [15] being a notable example in the field of active fault diagnosis.

To the best of the authors knowledge, no previous work considered a set-based threshold design problem for fault detection in nonlinear uncertain systems, with the goal of simultaneously guaranteeing robustness to uncertainties in a probabilistic sense, and maximizing detection of a given class of faults. In particular, the main contributions of the present paper are as follows:

- A formal definition of a novel fault detection threshold set design problem, using the concept of probabilistic set approximation through *polynomial superlevel sets* [16];
- The formulation of a cascade framework for designing threshold sets, through a two-stage chance-constrained optimization problem, in which the first step is aimed

This research was supported by the Netherlands Organization for Scientific Research (NWO) under the project grant number 408-13-030 (ATES-SGs), and by the European Union under the FP7-PEOPLE grant 324432 (AMBI).

V. Rostampour, R. Ferrari, and T. Keviczky are with Delft Center for Systems and Control, Delft University of Technology, Mekelweg 2, 2628 CD, Delft, The Netherlands. {v.rostampour, r.ferrari, t.keviczky}@tudelft.nl

at fulfilling a probabilistic robustness constraint, and the second step maximizes the performance of detection with respect to a given class of faults;
- The introduction of a computationally tractable framework for the solution of the chance constrained problem, through a randomization technique where the results of the so-called scenario approach are extended to the present case, and theoretical guarantees are given;
- An illustration of the applicability of the proposed framework, through a numerical simulation study on a three-tank uncertain nonlinear system.

A distinctive, practical advantage of the proposed randomization technique is that its implementation requires only the availability of a discrete number of samples from the healthy behaviour of the system, which can for instance be obtained from historical data.

This paper has the following structure. Section II describes the nonlinear uncertain system under study and its faults, and provides the formal definition of the proposed threshold set design problem. The proposed framework, probabilistic solution approach, is described in Section III, while the randomization technique and the theoretical results extending the scenario approach are presented in Section IV. Finally, simulation results and concluding remarks are provided in Section V and VI, respectively.

II. Problem Statement

This section provides a formal description of the fault threshold design problem. We first present the general uncertain nonlinear system dynamics, and then we introduce a fault detection observer producing a time-varying dynamic residual. Finally we provide a formulation of the problem on which our novel probabilistic framework will be based.

A. System Dynamics

Consider a nonlinear uncertain discrete time system, described as:

$$\begin{cases} x_{k+1} &= g(x_k, u_k) + \eta(x_k, u_k, w_k) + \phi(x_k, u_k, f_k) \\ y_k &= x_k + v_k \end{cases}, \quad (1)$$

where $k \in \mathbb{N}$ is the generic discrete time index and $x_k \in \mathbb{R}^n$, $u_k \in \mathbb{R}^m$ denote the state and input variables, respectively. $g : \mathbb{R}^n \times \mathbb{R}^m \mapsto \mathbb{R}^n$ represents the nominal healthy dynamics, while $\eta : \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^p \mapsto \mathbb{R}^n$ describes the effect on the system dynamics of the process modelling uncertainties $w_k \in \mathbb{R}^p$. $\phi : \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^q \mapsto \mathbb{R}^n$ is the fault function, which is characterized by an unknown time varying fault parameter vector $f_k \in \mathcal{F} \subseteq \mathbb{R}^q$, such that $\phi(x_k, u_k, 0) = 0$, $\forall\, x_k, u_k$ and the following holds.

Assumption 1. No fault acts on the system, that is $f_k = 0$, for $0 \leq k < k_f$, with k_f being the fault occurrence time. Moreover, the variables x_k and u_k remain bounded before and after the occurrence of a fault, i.e., there exist some stability regions $\mathcal{S} = \mathcal{S}^x \times \mathcal{S}^u \subset \mathbb{R}^n \times \mathbb{R}^m$, such that $(x_k, u_k) \in \mathcal{S}, \forall\, k$. □

Remark 1. As in this paper we consider only fault detection, and not fault isolation, it suffices to consider a fault class containing the single fault function ϕ and assume its parameterization is capable of representing any possible fault to which the system can be subjected.

Finally, $y_k \in \mathbb{R}^n$ is the measurement vector, where it is assumed for the sake of simplicity that the state vector is completely measurable, with the extension to input-output systems being addressable as in [17]. We also assume the presence of a measurement noise $v_k \in \mathbb{R}^n$.

Assumption 2. w_k and v_k are random variables defined on some probability spaces $(\mathcal{W}, \mathfrak{B}(\mathcal{W}), \mathbb{P}_\mathcal{W})$, and $(\mathcal{V}, \mathfrak{B}(\mathcal{V}), \mathbb{P}_\mathcal{V})$, respectively, where $\mathcal{W} \subseteq \mathbb{R}^p$, $\mathcal{V} \subseteq \mathbb{R}^n$, $\mathfrak{B}(\cdot)$ denotes a Borel σ-algebra, and $\mathbb{P}_\mathcal{W}$, $\mathbb{P}_\mathcal{V}$ are a probability measure defined over $\mathcal{W}$, $\mathcal{V}$, respectively. Furthermore, w_k and v_k are not correlated and are independent from x_k, u_k and f_k. □

Remark 2. It is important to note that, as in [16], [18], we do not require the sample spaces $\mathcal{W}$, $\mathcal{V}$ and the probability measures $\mathbb{P}_\mathcal{W}, \mathbb{P}_\mathcal{V}$ to be known explicitly, as it will be explained in Section IV.

B. Residual Generator

We will adopt a model-based fault detection approach such as in [19], and will generate a dynamic residual $r_k := y_k - \hat{y}_k$ as the state measurement error of the following nonlinear estimator

$$\begin{cases} \hat{x}_{k+1} &= g(y_k, u_k) + \Lambda\,(\hat{y}_k - y_k) \\ \hat{y}_k &= \hat{x}_k \end{cases}, \quad (2)$$

where $\Lambda \triangleq \text{diag}(\lambda^i,\, i = 1 \dots n)$ is a diagonal matrix, and $|\lambda^i| \leq 1$ denotes a filtering parameter chosen to guarantee the stability of the estimator.

By using eqs. (1),(2), we can then compute the residual generator dynamics as

$$r_{k+1} = \Lambda\, r_k + \delta_k + \phi(x_k, u_k, f_k)\ , \quad (3)$$

where we introduced the stochastic process δ_k, which is the *random total uncertainty* influencing the residual generator:

$$\delta_k := g(x_k, u_k) - g(y_k, u_k) + \eta(x_k, u_k, w_k) + v_{k+1}\ . \quad (4)$$

Thanks to Ass. 1, 2 and eq. (4), it follows that δ_k is a random variable on a probability space $(\Delta_k, \mathfrak{B}(\Delta_k), \mathbb{P}_{\delta_k})$, where Δ_k is produced by letting w_k vary over $\mathcal{W}$, and v_k and v_{k+1} vary over $\mathcal{V}$. We can now introduce a compact notation for the residual generator described by eqs. (2),(3),(4), through a mapping function $\Sigma : \mathbb{R}^n \times \mathbb{R}^n \times \mathbb{R}^n \mapsto \mathbb{R}^n$ defined as

$$\Sigma(r_k, \delta_k, \phi(x_k, u_k, f_k)) := r_{k+1}. \quad (5)$$

Remark 3. From (3),(5) it follows that the mapping from the uncertain variable $\delta_k \in \Delta_k$ to the residual variables r_{k+1} is measurable, so that the residual signal r_{k+1} can be viewed as a random variable on the same probability space as δ_k. □

Given these preliminaries, and for analysis purposes, it is now possible to write the following two fundamental concepts (see Fig. 1).

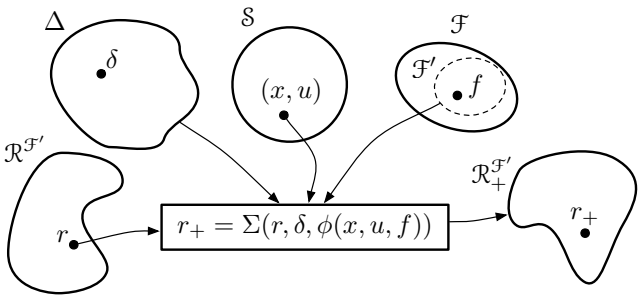


Fig. 1. The faulty residual set $\mathcal{R}_+^{\mathcal{F}'}$ can be thought as the image obtained by computing the output Σ for the actual values r, x, u, respectively, of the residual, state and input, and letting δ and f vary over Δ and $\mathcal{F}'$, respectively. The healthy residual set $\mathcal{R}_+^0$ can be obtained by restricting to $\mathcal{F}' = \{0\}$.

Definition 1. The time varying $\mathcal{F}'$*–faulty residual set* $\mathcal{R}_{k+1}^{\mathcal{F}'}$ at time index $k+1$ is defined as the image of the sets Δ_k and $\mathcal{F}' \subseteq \mathcal{F}$ through Σ and ϕ, respectively, that is

$$\begin{aligned}\mathcal{R}_{k+1}^{\mathcal{F}'} :=& \Sigma(r_k, \Delta_k, \phi(x_k, u_k, \mathcal{F}')) \\ =& \{r \,|\, r = \Sigma(r_k, \delta, \phi(x_k, u_k, f)),\, \delta \in \Delta_k,\, f \in \mathcal{F}'\}.\end{aligned}$$

Consider now a special case of the above definition.

Definition 2. The time varying *healthy residual set* $\mathcal{R}_{k+1}^0$ at time index $k+1$ is defined as the $\mathcal{F}'$–faulty residual set in the case $\mathcal{F}' = \{0\}$.

Furthermore, the notation $r_k^0 \in \mathcal{R}_k^0$ denotes the generic element of the healthy residual set. When there is no ambiguity, in the rest of the paper we will drop the index k, and instead employ the index "+" to denote the value of a set or variable at next time index, such as in $r_+ = \Sigma(r, \delta, \phi)$.

C. Fault Detection Threshold Design Problem

Having built a residual generator, the remaining central problem in fault detection is designing a threshold with suitable robustness and detection performance guarantees. Traditional solutions to the deterministic robust threshold design problem (see [20] for a survey) seek a threshold bounding all possible values of the healthy residual r^0, thus guaranteeing zero FAR by design. In the norm-based approach, a scalar threshold τ bounding $\|r^0\|$ is sought, whereas in the limit checking approach a vector is found such that its j–th component $\tau_{(j)}$ bounds $|r_{(j)}^0|$. In order to minimize the MDR, such thresholds should be made as small as possible, a goal which we may express as

$$\text{(I)} \begin{cases} \min\limits_{\tau \in \mathbb{R}} & \tau \\ \text{s.t.} & \|r^0\| \le \tau \end{cases}, \quad \text{(II)} \begin{cases} \min\limits_{\tau_{(j)} \in \mathbb{R}} & \tau_{(j)} \\ \text{s.t.} & |r_{(j)}^0| \le \tau_{(j)} \end{cases},$$

where problem (II) should be solved for each $j = 1 \dots n$ independently. If we interpret the thresholds resulting from (I) and (II) in a set theoretic setting, it is easy to see that they lead, respectively, to the smallest ball and axis-aligned box in $\mathbb{R}^n$ containing the healthy residual set $\mathcal{R}^0$ (Fig. 2–a and 2–b). Such solutions are clearly over-conservative, for two reasons. First, they use simple and convex manifolds to bound the set $\mathcal{R}^0$, which in general can have an arbitrary shape and be non–convex, because of the assumed nonlinearity of both the system nominal dynamics g and uncertainty function η. Secondly, bounding the entire set $\mathcal{R}^0$ does indeed lead to a deterministic guarantee on the FAR, but ignores the fact that in real applications some values of r^0 may have a negligible probability of being produced, and as such they could be excluded in the threshold design procedure.

It is the stated objective of the present paper to address both the aforementioned sources of conservativeness. First of all we will introduce an adaptive, parameterized set-based threshold, which could *approximate* arbitrarily well the shape of the set $\mathcal{R}^0$. In second place we will relax the deterministic, hard constraints of problems (I) and (II) with a probabilistic guarantee, thus reaching a desired level of FAR. Finally, thanks to our assumption on the knowledge of the functional dependence of the fault function ϕ on the unknown but bounded fault parameter f, we will propose a threshold design framework, which will aim at the same time to reducing the MDR.

In order to formalize the above ideas, we first define $\mathcal{T}_k \subseteq \mathbb{R}^n$ as an adaptive *threshold set* at time index k for fault detection, and then introduce the following novel concept.

Definition 3. Given the residual generator function Σ and a fixed $\alpha \in [0,1]$, an adaptive threshold set $\mathcal{T}_k$ is said to be *probabilistically* α*–robust* with respect to the random total uncertainty $\delta \in \Delta$, if

$$\mathcal{V}(\mathcal{T}_+) := \mathbb{P}\left[r_+^0 \notin \mathcal{T}_+\right] < 1 - \alpha\,, \tag{6}$$

where $\mathcal{V}(\mathcal{T}_+)$ is the *violation probability* of the healthy residuals $r_+^0 \in \mathcal{R}_+^0$.

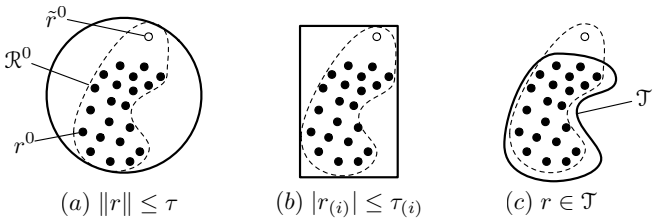
Definition 4. A fault function ϕ is said to be *detectable over* $\mathcal{F}' \subseteq \mathcal{F}$ *by an adaptive threshold set* $\mathcal{T}_k$ *and a residual generator* Σ if $\forall\, f \in \mathcal{F}'$, $\exists\, r \in \mathcal{R}$, $(x,u) \in \mathcal{S}$ and $\delta \in \Delta$ such that $r_+ \notin \mathcal{T}_+$, with $r_+ = \Sigma(r, \delta, \phi(x,u,f))$.

We now describe the adaptive threshold set $\mathcal{T}_k$, using a *generalized indicator function* $\mathcal{I}_{\mathcal{T}}(r, \theta_k) : \mathbb{R}^n \times \mathbb{R}^t \mapsto \mathbb{R}$ parametrized by a time varying vector $\theta_k \in \mathbb{R}^t$, as follows:

$$\mathcal{T}_k := \{r \in \mathbb{R}^n \,|\, \mathcal{I}_{\mathcal{T}}(r, \theta_k) \ge c\}\,. \tag{7}$$

This yields a *c–superlevel set* [21] of $\mathcal{I}_{\mathcal{T}}$, for any value of c, as the adaptive threshold set $\mathcal{T}_k$, while Def. 3 leads to an expected FAR better then $1 - \alpha$. The following remark describes better our idea into the above definitions and the proposed probabilistic framework.

Remark 4. A fundamental point in understanding Def. 3, is that the probabilistic condition (6) is expressed in terms of the *future* healthy residual belonging to the *future* threshold set. In fact, while at a given time the actual residual r is a computable and as such deterministic quantity, its future value r_+ is a random variable, as it linearly depends on the random variable δ. It thus makes sense to consider the probability, measured with respect to the probability space on which δ is defined, that in healthy conditions r_+ will belong to the set $\mathcal{T}_+$. The latter is a deterministic set that shall be computed at the current time, as will be highlighted



$(a)\ \|r\| \leq \tau$ $(b)\ |r_{(i)}| \leq \tau_{(i)}$ $(c)\ r \in \mathcal{T}$

Fig. 2. A pictorial, intuitive comparison of different robust threshold and residual evaluation approaches. Representative healthy values r^0 of the residual are drawn as filled black circles, while rare ones $\tilde{r}^0$ are drawn as empty circles. For convenience, in all cases the evaluation condition is represented as membership in a set drawn with a tick line. a) Norm based. b) Limit checking. c) The proposed, probabilistic set-based approach.

in the next sections. We stress again the fact that Def. 3 does not require $\mathcal{T}_+$ to be a (proper) subset of $\mathcal{R}^0_+$, but only that $\mathcal{T}_+$ approximates it in the given probabilistic sense. This distinction will be the key in designing the solution proposed in Sect. III.

III. Proposed Probabilistic Framework

This section proposes a unified framework to design a threshold set that is *probabilistically α–robust* and at the same time maximizes the detectability over a given fault parameter set $\mathcal{F}'$. The threshold set $\mathcal{T}$ will be obtained as the solution of the cascade of two chance-constrained optimization problems.

A. Probabilistic Threshold Set Design

In the proposed approach we will assume the indicator function $\mathcal{I}_{\mathcal{T}}(r,\theta)$ to be a polynomial function of given degree d, with θ containing the polynomial coefficients in a suitable order. Denoting $\pi_\xi(r)$ a vector of monomials of degree up to $\xi := \lceil d/2 \rceil$[1], we can conveniently define $\mathcal{I}_{\mathcal{T}}(r,\theta) := \pi_\xi(r)^\top G(\theta)\, \pi_\xi(r)$, where $G(\theta)$ is a matrix depending on the coefficients contained in θ, which eventually is the quantity to be solved for during the proposed design procedure.

We first formulate a chance-constrained optimization problem to obtain the minimum volume threshold set $\mathcal{T}$ that fulfills Def. 3 for a user-designed α:

$$\begin{cases} \min\limits_{\theta} & \textbf{vol}\ \mathcal{T} \\ \text{s.t.} & \mathcal{V}(\mathcal{T}) < 1-\alpha\ , \end{cases} \tag{8}$$

where $\textbf{vol}\ \mathcal{T} := \int_{\mathcal{T}} dr$ is the volume or Lebesgue measure of $\mathcal{T}$. The proposed optimization problem (8) is in general non-convex and hard to solve, due to the numerical complexity arising from the minimum volume objective, and the probabilistic constraint. Following [22] and [23] to proceed further, we restrict the range of our indicator function to be non-negative which yields $\mathcal{I}_{\mathcal{T}}$ to be a polynomial sum-of-squares (SoS) and $G(\theta)$ to be a symmetric Gram matrix. We are now able to bound the objective function using the relation:

$$\textbf{vol}\ \mathcal{T} = \int_{\mathcal{T}} dr\ \leq \int_{\mathcal{B}} \mathcal{I}_{\mathcal{T}}(r,\theta)\, dr\ =\ \text{trace}(G(\theta)M)\ , \tag{9}$$

[1] $\lceil\cdot\rceil$ is the ceiling operator which returns the smallest integer greater than or equal to its argument.

where $\mathcal{B} \in \mathbb{R}^n$ is an arbitrary compact set so that $\mathcal{T} \subseteq \mathcal{B}$ and $M := c^{-1} \int_{\mathcal{B}} \pi_\xi(r)\pi_\xi(r)^\top dr$ denotes the matrix of moments of the Lebesgue measure on $\mathcal{B}$ in basis $\pi_\xi(r)$. Thanks to (9) and Def. 3, we can reformulate (8) as

$$\begin{cases} \min\limits_{\theta,\gamma} & \gamma & \text{(10a)} \\ \text{s.t.} & G(\theta) \succeq 0\ , & \text{(10b)} \\ & \text{trace}(G(\theta)M) \leq \gamma\,, & \text{(10c)} \\ & \mathbb{P}\left[\mathcal{I}_{\mathcal{T}}(r^0_+,\theta) \geq c\right] \geq \alpha\,. & \text{(10d)} \end{cases}$$

Remark 5. Constraint (10b) imposes the positive semidefiniteness of $G(\theta)$ in order to constrain $\mathcal{I}_{\mathcal{T}}$ to be SoS. Moreover, in (10c) we introduced the auxiliary variable γ to allow us to upper bound the objective function, using epigraphical reformulation [24]. Finally note that, as explained in Remark 4 the probabilistic constraint in (10d) is measured with respect to the underlying random variable δ.

It is intuitive that a minimum volume threshold set is an effective, albeit heuristic strategy for maximizing fault detection. A more rigorous investigation of this problem will be presented in next section.

B. Maximization of Fault Detection

By looking at Ass. 1 and at Def. 1 and 4, the following can be shown, justifying the quest for the smallest $\mathcal{T}$.

Theorem 1 (Detectability)**.** *A necessary condition for the fault function ϕ to be detectable over $\mathcal{F}'$ during the evolution of system (1) is that $\exists\, k \geq k_f$ so that $\mathcal{R}^{\mathcal{F}'}_{k+1} \cap \overline{\mathcal{T}_{k+1}} \neq \emptyset$, where $\overline{\mathcal{T}}$ denotes the complement of set $\mathcal{T}$.*

Anyway, this is not sufficient, as in general it may still hold $\mathcal{R}^{\mathcal{F}'}_{k+1} \cap \mathcal{T}_{k+1} \neq \emptyset$, which means that at least one of the possible realizations of the random variable δ_k will keep the residual r_{k+1} inside $\mathcal{T}_{k+1}$, even for $k \geq k_f$. Eq. (3) reveals that this can easily happen when the fault and the uncertainty have similar magnitude and opposite direction, as in the trivial case $\delta_k = -\phi_k$. Our approach in the present paper will be to maximize the probability of a successful detection at each time step k, by making $\mathcal{T}_k$ as much distant as possible from $\mathcal{R}^{\mathcal{F}'}_k$, in the sense that is described next.

We will assume the availability[2] of a description of the set $\mathcal{R}^{\mathcal{F}'}$ through a polynomial SoS generalized indicator function $\mathcal{I}_{\mathcal{R}^{\mathcal{F}'}}(r,\psi) := \pi_\xi(r)^\top G(\psi)\, \pi_\xi(r)$ with the same degree d and the same monomial basis $\pi_\xi(r)$ as $\mathcal{I}_{\mathcal{T}}$. By denoting ψ^* the actual value of ψ so that $\mathcal{I}_{\mathcal{R}^{\mathcal{F}'}}(r,\psi) \geq c$ for all $r \in \mathcal{R}^{\mathcal{F}'}$, we are now in a position to formulate an optimization problem for maximizing the distance between the threshold set $\mathcal{T}$ and the faulty residual set $\mathcal{R}^{\mathcal{F}'}$:

$$\begin{cases} \max\limits_{\theta} & \|\, \mathcal{I}_{\mathcal{T}}(r,\theta) - \mathcal{I}_{\mathcal{R}^{\mathcal{F}'}}(r,\psi^*)\,\|_\infty \\ \text{s.t.} & \|\theta\|_\infty \leq \bar{c}\ , \end{cases} \tag{11}$$

where $\bar{c}$ is a given constant parameter. The objective function aims at maximizing the Chebyshev distance between $\mathcal{I}_{\mathcal{T}}$ and

[2] A simple way to obtain it is to solve a problem analogous to (10), where the constraint (10d) is imposed deterministically on all elements of $\mathcal{R}^{\mathcal{F}'}$.

$\mathcal{I}_{\mathcal{R}^{\mathcal{F}'}}$, which is also known as the polynomial height [25]. Since both of them share the same monomial basis vector $\pi_\xi(r)$, this leads to the maximization of the distance $\|G(\theta) - G(\psi^*)\|_\infty$ between their Gram matrices [25]. Notice that the second constraint in (11) is added to ensure that the solutions remain bounded. We now propose a cascade of two chance-constrained optimization problems (10) and (11), which is in general hard to solve.

C. Cascade Problem Formulation Scheme

In order to attain our stated goal of obtaining a probabilistically α–robust threshold set which also maximizes detecttion of the fault function ϕ in the sense of Def. 4 and of Subsect. III-B, we propose a cascade of two chance-constrained optimization problems as follows:

$$\begin{cases} \min\limits_{\theta,\gamma} & \gamma \\ \text{s.t.} & G(\theta) \succeq 0\,, \quad \text{trace}(G(\theta)M) \leq \gamma\ , \\ & \mathbb{P}\left[\mathcal{I}_{\mathcal{T}}(r_+^0, \theta) \geq c\right] \geq \alpha \end{cases} \tag{12a}$$

$$\begin{cases} \max\limits_{\theta} & \|G(\theta) - G(\psi^*)\|_\infty \\ \text{s.t.} & G(\theta) \succeq 0\,, \quad \text{trace}(G(\theta)M) \leq \gamma^*\ , \\ & \mathbb{P}\left[\mathcal{I}_{\mathcal{T}}(r_+^0, \theta) \geq c\right] \geq \alpha \end{cases} \tag{12b}$$

where the quantity γ^* is the optimal cost obtained by solving the first stage (12a), while (12) has to be solved sequentially in a *lexicographic* (multi-objective) sense [26]. Note that the unnecessary constraint in (11) is dropped due to the introduced bound in (12b).

Remark 6. The first stage problem (12a) aims at determining the minimum volume threshold set $\mathcal{T}$ subject to the probabilistic α–robust constraint, but in doing so is ignoring any information on the faulty residual set $\mathcal{R}^{\mathcal{F}'}$. This could possibly lead to unsatisfactory detection properties due to a large intersection $\mathcal{T} \cap \mathcal{R}^{\mathcal{F}'}$. The goal of the second stage problem (12b) is then to find a new parameter θ, leading to a new threshold set $\mathcal{T}$ with the same robustness guarantee and a volume which is not worse than the one resulting from the solution of problem (12a), but which is as distant as possible from the set $\mathcal{R}^{\mathcal{F}'}$. The effectiveness of such improvement may, anyway, be limited by the degree ξ of the monomial basis used by $\mathcal{I}_{\mathcal{T}}$ and $\mathcal{I}_{\mathcal{R}^{\mathcal{F}'}}$ [23, Lemma 1].

The proposed optimization problem (12) is however non-convex and hard to solve due to chance constraints being in general difficult to enforce. In the following section, we provide a computationally tractable randomized approach, together with a rigorous theoretical analysis of its properties.

IV. Computationally Tractable Methodology

Chance-constrained optimization problems are known to be non-convex and hard to solve [27], [28], however they received increasing attention due to recent developments toward computationally tractable approaches [29]. In particular, randomization techniques allow to approximate chance constraints in an equivalent sense without imposing any restriction on the probability distribution and geometric information of uncertain variables. The basic idea is very simple: chance constraints are substituted with finitely many hard constraints that correspond to samples from the uncertainty realizations [30]. Using this approach, we are now able to formulate the following tractable optimization problem:

$$\begin{cases} \min\limits_{\theta,\gamma} & \gamma \\ \text{s.t.} & G(\theta) \succeq 0\,, \quad \text{trace}(G(\theta)M) \leq \gamma\,, \\ & \mathcal{I}_{\mathcal{T}}(r_+^{0,(i)}, \theta) \geq c\,, \quad i = 1, 2, \cdots, N \end{cases} \tag{13a}$$

$$\begin{cases} \max\limits_{\theta} & \|G(\theta) - G(\psi^*)\|_\infty \\ \text{s.t.} & \theta \succeq 0\,, \quad \text{trace}(G(\theta)M) \leq \gamma^*\,, \\ & \mathcal{I}_{\mathcal{T}}(r_+^{0,(i)}, \theta) \geq c\,, \quad i = 1, 2, \cdots, N \end{cases} \tag{13b}$$

where $r_+^{0,(i)} = \Sigma(r, \delta^{(i)}, \phi(x, u, 0))$, and $\delta^{(i)} \in \Delta$ are samples of the random variable δ. We assume to be able to generate samples based on the knowledge of η, and availability of the uncertainty samples from $\mathcal{W}$ and $\mathcal{V}$. Should this knowledge be not available, samples can still be obtained using historical data recorded in healthy conditions from system (1) and by inverting eq. (3).

The link between the chance-constrained program and the quality of its approximation is the number of samples N that should be considered in order to reach a given level of confidence. This has been rigorously investigated in the *scenario approach*, a powerful randomized method developed recently (see [31] and the references therein). The crucial requirement to invoke these results is the convexity of the optimization problem in the decision variables, but unfortunately in the present case this does not hold due to use of the Chebyshev distance in the objective (13b). It is, however, easy to show that (13b) can be transformed into a number of different convex programs. As it has been shown in [5, Lemma 4.3], the set of the solutions of (13b) is equivalent to the union of the solution sets of ξ different convex programs, where we recall that 2ξ is the degree of $\mathcal{I}_{\mathcal{T}}(r, \theta)$. The following remark highlights some issues to be addressed in order to extend the theoretical results in [31] and the experimental two-step solution of [32] to the cascade structure of the optimization formulation (13).

Remark 7. Applying the results in [31, Th. 1] leads to computing the number N of samples as a function of the total degrees of freedom of problem (13a) and of the confidence level with which it is desired to approximate (12a). Solving (13a) then yields an optimal solution (θ_a^*, γ^*), the last term of which is used as a fixed constraint for solving (13b). Based on [31, Th. 1], there exists theoretical guarantee for feasibility of solution (θ_a^*, γ^*), however here we compute θ_b^* which might not be feasible for (12a) together with γ^*. It is important that the same N is used for both (13a) and (13b): otherwise, there are no guarantees that the program (13b), which is based on the solution of (13a), is feasible. This is due to γ_a^* being a random variable and depend on the specific value of N.

In [31] the existence and uniqueness of the tractable program solution is assumed. This was later relaxed by

applying a tie-break rule (e.g., lexicographic rule) and selecting among the optimal solutions the one with the best Euclidean distance [31, Section 2.1.5]. This is, however, not true in general for differently structured problems, such as the cascade formulation in (13), since in [31] a single tractable optimization program was considered. More specifically, a tie-break rule can be employed if the non–unique optimal solutions are obtained regardless of the number N of samples of the uncertain variable. As it is explained in the above remark, this cannot be guaranteed here in (13) due to the fact that the optimal solution γ^* is a random variable and depends on N. The following extends the result obtained in [31] to the present setting.

Theorem 2. *Consider* $\upsilon := [\theta, \gamma]^\top \in \mathbb{R}^\ell$ *to be the augmented vector of all the decision variables of* (13). *Let* $\beta \in [0,1]$ *and* $N \geq N(\varepsilon, \beta, \ell)$, *where*

$$N(\alpha, \beta, \ell) := \min \left\{ N \in \mathbb{N} \,\middle|\, d \sum_{i=0}^{\ell-1} \binom{N}{i} (1-\alpha)^i \alpha^{N-i} \leq \beta \right\}.$$

Then, the optimizer $\upsilon^* := [\theta_b^*, \gamma^*]^\top$ *of the randomized cascade convex program* (13) *is a feasible solution of the chance-constrained cascade optimization problem* (12) *with confidence level* $(1-\beta)$, *in the average.*

Proof. Due to the non-convexity introduced by the Chebyshev distance, we have to recast the second stage problem (13b) into ξ sub-programs. By denoting with Ψ_j the feasible solution set of the j–th subproblem it is clear that the optimizer of (13b) can be found in $\bigcup_{j=1}^{\xi} \Psi_j$ [5]. For clarity the proof will be broken down into three steps: a) application of the scenario approach of [31] to each individual sub-program; b) extension to the ξ sub-programs; c) theoretical conditions for the optimizer $\upsilon^* := [\theta_b^*, \gamma^*]^\top$ to be a feasible solution of (12). Let us now denote with $\mathcal{T}(\theta_b^*)$ the threshold set $\mathcal{T}$ obtained when $\mathcal{I}_{\mathcal{T}}$ is parameterized by a given θ_b^*, and recall that $\mathcal{V}(\mathcal{T}(\theta_b^*))$ is the violation probability (Def. 3).

a) Applying the existing results in [31] to each sub-program, we have for all $j \in \{1, \cdots, \xi\}$:

$$\mathbb{P}^N \left[\mathcal{V}(\mathcal{T}(\theta_{b_j}^*)) \leq 1-\alpha \right] \leq \sum_{i=0}^{\ell-1} \binom{N}{i} (1-\alpha)^i \alpha^{N-i}.$$

b) Considering that $\mathcal{V}(\mathcal{T}(\theta_b^*)) \subseteq \bigcup_{j=1}^{\xi} \mathcal{V}(\mathcal{T}(\theta_{b_j}^*))$, we can readily extend the aforesaid results to ξ sub-programs as follows:

$$\begin{aligned} &\mathbb{P}^N \left[\mathcal{V}(\mathcal{T}(\theta_b^*)) \leq 1-\alpha \right] \leq \\ &\quad \leq \mathbb{P}^N \left[\bigcup_{j=1}^{\xi} \mathcal{V}(\mathcal{T}(\theta_{b_j}^*)) \leq 1-\alpha \right] \\ &\quad \leq \sum_{j=1}^{\xi} \mathbb{P}^N \left[\mathcal{V}(\mathcal{T}(\theta_{b_j}^*)) \leq 1-\alpha \right] \\ &\quad < \xi \sum_{i=0}^{\ell-1} \binom{N}{i} (1-\alpha)^i \alpha^{N-i} \leq \beta. \end{aligned}$$

Notice that the obtained bound is the desired assertion as it is stated in the theorem. However, the most important part of the proof is to extend this result to the cascade setup of the present optimization problem in (13).

c) In order to proceed let us first define an indicator function $\mathbb{1}_{\{\cdot\}} : [0,1] \mapsto \{0,1\}$ that indicates whether the inequality in its argument, which is a function of a random variable, holds or not. We now have to provide a new bound for the following N-fold product conditional probability $\mathbb{P}^N \left[\mathcal{V}(\mathcal{T}(\theta_b^*)) \leq 1-\alpha \middle| \gamma^* \right]$ which is a random variable with respect to γ^* due to the fact that γ^* is an optimal solution of the first step optimization problem and it depends on specific random samples. To this end consider the following N-fold product conditional expectation problem:

$$\begin{aligned} &\mathbb{E}^N \left[\mathbb{1}_{\{\mathcal{V}(\mathcal{T}(\theta_b^*)) \leq 1-\alpha\}} \middle| \gamma^* \right] \\ &\quad = 1 \cdot \mathbb{P}^N \left[\mathcal{V}(\mathcal{T}(\theta_b^*)) \leq 1-\alpha \middle| \gamma^* \right] \\ &\qquad + 0 \cdot \mathbb{P}^N \left[\mathcal{V}(\mathcal{T}(\theta_b^*)) \leq 1-\alpha \middle| \gamma^* \right] \\ &\quad = \mathbb{P}^N \left[\mathcal{V}(\mathcal{T}(\theta_b^*)) \leq 1-\alpha \middle| \gamma^* \right]. \end{aligned} \tag{14}$$

The best approximation of $\mathbb{P}^N \left[\mathcal{V}(\mathcal{T}(\theta_b^*)) \leq 1-\alpha | \gamma^* \right]$ is given by $\mathbb{E}^N \left[\mathbb{1}_{\{\mathcal{V}(\mathcal{T}(\theta_b^*)) \leq 1-\alpha\}} \middle| \gamma^* \right]$ which is a function of random variable γ^*. The best here means that one cannot do any better than this due to the fact that $\mathbb{P}^N \left[\mathcal{V}(\mathcal{T}(\theta_b^*)) \leq 1-\alpha | \gamma^* \right]$ is itself a function of random variable γ^*. Finally, we calculate the above quantity by the law of the unconscious [33] as follows:

$$\begin{aligned} &\mathbb{E}^N \left[\mathbb{E}^N \left[\mathbb{1}_{\{\mathcal{V}(\mathcal{T}(\theta_b^*)) \leq 1-\alpha\}} \middle| \gamma^* \right] \right] \\ &= \sum\nolimits_{\nu} \mathbb{E}^N \left[\mathbb{1}_{\{\mathcal{V}(\mathcal{T}(\theta_b^*)) \leq 1-\alpha\}} \middle| \gamma^* = \nu \right] \mathbb{P}^N \left[\gamma^* = \nu \right] \\ &= \mathbb{E}^N \left[\mathbb{1}_{\{\mathcal{V}(\mathcal{T}(\theta_b^*)) \leq 1-\alpha\}} \right] = \mathbb{P}^N \left[\mathcal{V}(\mathcal{T}(\theta_b^*)) \leq 1-\alpha \right], \end{aligned} \tag{15}$$

where the last equation is due to the partition theorem. The proof is completed by noting that the final expression in (15) is already bounded in part (b) of the proof. □

V. Simulation Study

In this section a demonstration of the proposed scheme will be given, by using the well known three-tank benchmark system [19]. Using the proposed approach in [23], that translates the problem (13) into linear programs, at each time step the problem (13) will be solved using the Matlab Optimization Toolbox (linprog), and the fault detection condition $\mathcal{I}_{\mathcal{T}}(r, \theta) < c = 1$ will be tested.

A. Description of system and faults parameters

For simulating the nominal dynamics function g in the observer (2), the following nominal values have been chosen: $A = [1 \;\; 1.3 \;\; 2]$ m^2 for the tanks' cross-section, $A^p = [0.2 \;\; 0.1]$ m^2 with unitary outflow coefficients for the pipes one, and $A^d = [0.1 \;\; 0.1 \;\; 0.1]$ m^2 with outflow coefficients equal to 0.5 for the drains. Instead, when simulating the physical system (1), we assumed w and the function η to account for a uniformly distributed uncertainty in the parameters, ranging up to 5% for the tanks' cross section, 15% for the pipes' and drains' cross section and levels, and up to 20% for the pipes' outflow coefficient. The initial levels

of the tanks were set to $x(0) = [6\ 7\ 3]$ m while the pump inflows were computed as $u_1(k) = 0.2 \cdot \cos(0.5 \cdot kT_s) + 0.8$ and $u_2(k) = 0.1 \cdot \sin(0.1 \cdot kT_s) + 1$. The sampling time was $T_s = 0.1$ s, and the filter coefficients $\lambda^i = 0.85$. A 30% partial shutdown of pump no. 1 is introduced at time $T_f = 20$ s, by defining a fault function $\phi(x, u, f) = [-u \cdot f\ 0\ 0]^\top$ with $f \in \mathcal{F}' = \{0.3\}$.

B. Numerical implementation

A degree $d = 4$ was chosen for the polynomials $\mathcal{I}_\mathcal{T}$ and $\mathcal{I}_{\mathcal{R}^{\mathcal{F}'}}$, and without loss of generality the boundary value of the superlevel set c was fixed to be one. Following Theorem 2, at each time step, two sets of $N = 512$ samples of the residual r_+ one step ahead were generated by a Monte Carlo method, one in the healthy ($f = 0$) and one in the faulty ($f = 0.3$) hypothesis, using the available information on the function η and on the domains $\mathcal{W}$ and $\mathcal{V}$ to which w and v belong. In order to approximate an hyper-rectangle deterministic threshold set, against which to compare our results, an additional simulation was run with a higher number $N' = 2^{16}$ of samples per each time step.

The faulty samples, denoted by $r_+^{\mathcal{F}',(i)}$, are used to find the parameter ψ^* needed to describe the faulty residual set $\mathcal{R}^{\mathcal{F}'}$ (Subsect. III-C), by solving the additional problem:

$$\begin{cases} \min\limits_{\psi,\lambda} & \lambda \\ \text{s.t.} & G(\psi) \succeq 0\,, \quad \text{trace}(G(\psi)M) \leq \lambda\,, \\ & \mathcal{I}_{\mathcal{R}^{\mathcal{F}'}}(r_+^{\mathcal{F}',(i)}, \psi) \geq c\,, \quad \forall\, i = 1 \dots N \end{cases} \cdot \tag{16}$$

The healthy samples, denoted by $r_+^{0,(i)}$, are instead used to solve problem (13). Both (13) and (16) are indeed a semidefinite program on the polynomial coefficients θ and ψ, but for numerical efficiency they can be converted to linear programs by introducing an additional set of artificial constraints requiring the polynomials to be positive on a dense grid of points in the integration domain $\mathcal{B}$, as described in [23]. The moment matrix M is computed only once for both polynomials, as long as $\mathcal{B}$ is of a suitable size as to be held constant during the simulation. This is another advantage of having chosen the same monomial basis for both $\mathcal{I}_\mathcal{T}$ and $\mathcal{I}_{\mathcal{R}^{\mathcal{F}'}}$.

C. Simulation Results

In Figure 3 it is possible to see an example of the resulting faulty residual set $\mathcal{R}^{\mathcal{F}'}$ obtained from solving (16), and of the threshold set $\mathcal{T}$ obtained first from (13a) and then from (13b).

It is very interesting, in order to show the advantage of the proposed scheme with respect to an adaptive, but deterministic approach leading to hyperrectangular sets, to analyze the ratio of the volume of the proposed polynomial superlevel set to a deterministic hyperrectangular one, as mentioned earlier. As it can be seen in Figure 4, before the fault occurrence time on average the obtained probabilistic threshold set volume is always smaller than about 57% of the hyper-rectangular one, a fact allowing for better detectability

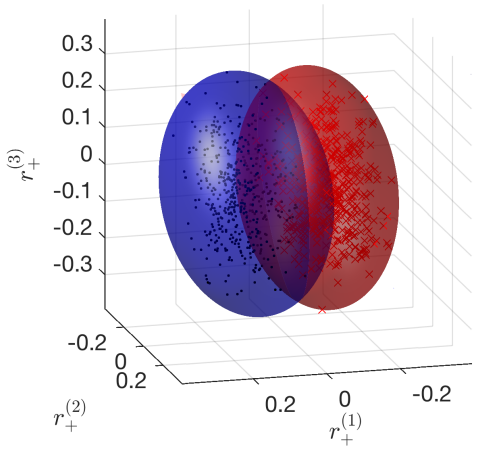


Fig. 3. An example of the sets obtained using 4th order polynomials as indicator functions. The blue color denotes the threshold set $\mathcal{T}$ obtained by solving problem (13b). The red color shows the faulty residual set $\mathcal{R}^{\mathcal{F}'}$ obtained by solving problem (16).

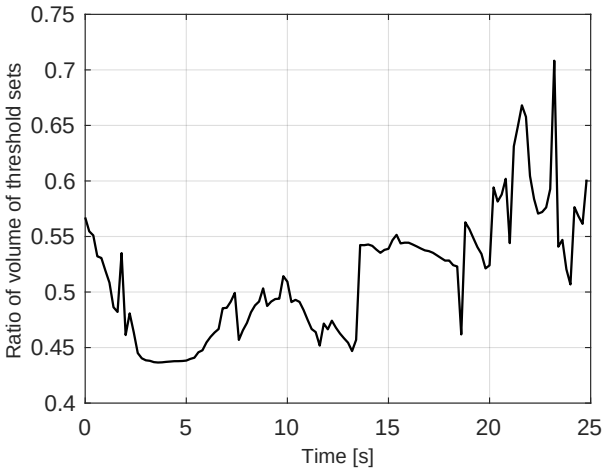


Fig. 4. Ratio between the volume of the proposed polynomial superlevel threshold set and of an equivalent deterministic hyperrectangular set.

performances with all other conditions being kept equal. Finally, the behavior of the polynomial $\mathcal{I}_\mathcal{T}(r, \theta_b^*)$ applied to the actual computed residual r_+ is shown in Figure 5, where the correctness of the detection decision using the proposed scheme is testified by the polynomial dropping below the boundary value ($c = 1$) after the fault onset time $T_f = 20$ s. No false alarms are reported before this time.

VI. Conclusions

In this paper a novel approach to the design of robust detection thresholds for uncertain nonlinear systems was proposed, leading to theoretically sound probabilistic guarantees on the performance level in terms of expected false alarm ratio and fault detection. This problem was cast as a bi-level cascade convex optimization program, where in the first stage the volume of the resulting polynomial threshold set is minimized while meeting a desired bound on the probability of false alarms. In the second stage, the previous solution is used as a starting point for optimizing the threshold sensitivity to a given class of faults, while maintaining the

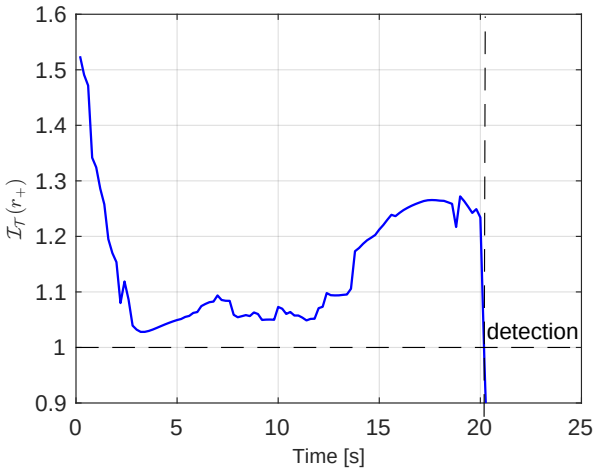


Fig. 5. Time behavior of the polynomial $\mathcal{I}_{\mathcal{T}}(r, \theta_b^*)$ applied to the residual r_+. The drop below the boundary value c = 1 after the fault time (20 s) indicates a successful detection.

desired level of false alarm probability. The complete chance-constrained problem is then solved in a tractable scheme by relying on randomization techniques, while providing theoretical guarantees on the feasibility of the solution with high confidence level in the average. Finally, simulation results on the well known three-tank benchmark are provided along with useful insights on the advantages with respect to established deterministic robust thresholds.

REFERENCES

[1] S. Ding, *Model-based fault diagnosis techniques: design schemes, algorithms, and tools*. Berlin, Heidelberg: Springer-Verlag, 2008.

[2] C. De Persis and A. Isidori, "A geometric approach to nonlinear fault detection and isolation," *IEEE Transaction on Automatic Control*, vol. 46, no. 6, pp. 853–865, Jun. 2001.

[3] E. Evangelia Tiniou, P. Mohajerin Esfahani, and J. Lygeros, "Fault detection with discrete-time measurements: an application for the cyber security of power networks," in *52nd IEEE Conference Decision and Control*, Dec 2013, pp. 194–199.

[4] B. Svetozarevic, P. Mohajerin Esfahani, M. Kamgarpour, and J. Lygeros, "A robust fault detection and isolation filter for a horizontal axis variable speed wind turbine," in *American Control Conference (ACC), 2013*, June 2013, pp. 4453–4458.

[5] P. Mohajerin Esfahani and J. Lygeros, "A tractable fault detection and isolation approach for nonlinear systems with probabilistic performance," *IEEE Transactions on Automatic Control*, vol. 61, no. 3, pp. 633–647, March 2016.

[6] P. Mohajerin Esfahani, M. Vrakopoulou, G. Andersson, and J. Lygeros, "A tractable nonlinear fault detection and isolation technique with application to the cyber-physical security of power systems," in *51st IEEE Conference Decision and Control*, Dec 2012, pp. 3433–3438, full version: http://control.ee.ethz.ch/index.cgi?page=publications;action=details;id=4196.

[7] F. Boem, R. M. G. Ferrari, T. Parisini, and M. M. Polycarpou, "Optimal topology for distributed fault detection of large-scale systems," *IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes*, vol. 48, no. 21, pp. 60–65, 2015.

[8] M. Milanese, J. Norton, H. Piet-Lahanier, and É. Walter, *Bounding approaches to system identification*. Springer Science & Business Media, 2013.

[9] C. Combastel, "An extended zonotopic and gaussian kalman filter (ezgkf) merging set-membership and stochastic paradigms: Toward non-linear filtering and fault detection," *Annual Reviews in Control*, vol. 42, pp. 232–243, 2016.

[10] R. M. Fernández-Cantí, J. Blesa, V. Puig, and S. Tornil-Sin, "Set-membership identification and fault detection using a bayesian framework," *International Journal of Systems Science*, vol. 47, no. 7, pp. 1710–1724, 2016.

[11] J. Blesa, V. Puig, and J. Saludes, "Robust fault detection using polytope-based set-membership consistency test," *IET Control Theory & Applications*, vol. 6, no. 12, pp. 1767–1777, 2012.

[12] A. Ingimundarson, J. M. Bravo, V. Puig, T. Alamo, and P. Guerra, "Robust fault detection using zonotope-based set-membership consistency test," *International Journal of Adaptive Control and Signal Processing*, vol. 23, no. 4, 2009.

[13] I. Fagarasan, S. Ploix, and S. Gentil, "Causal fault detection and isolation based on a set-membership approach," *Automatica*, vol. 40, no. 12, pp. 2099–2110, 2004.

[14] S. Zhai, Y. Wan, and H. Ye, "A set-membership approach to integrated trade-off design of robust fault detection system," *International Journal of Adaptive Control and Signal Processing*, 2016.

[15] G. R. Marseglia, J. K. Scott, L. Magni, R. D. Braatz, and D. M. Raimondo, "A hybrid Stochastic-Deterministic approach for active fault diagnosis using scenario optimization," in *IFAC World Congress*, vol. 19, 2014, pp. 1102–1107.

[16] F. Dabbene, D. Henrion, C. Lagoa, and P. Shcherbakov, "Randomized approximations of the image set of nonlinear mappings with applications to filtering," *IFAC Symposium on Robust Control Design*, vol. 48, no. 14, pp. 37–42, 2015.

[17] R. M. Ferrari, T. Parisini, and M. M. Polycarpou, "A robust fault detection and isolation scheme for a class of uncertain input-output discrete-time nonlinear systems," in *American Control Conference, 2008*, June 2008, pp. 2804–2809.

[18] V. Rostampour and T. Keviczky, "Robust randomized model predictive control for energy balance in smart thermal grids," in *European Control Conference (ECC)*. IEEE, 2016, pp. 1201–1208.

[19] R. M. Ferrari, T. Parisini, and M. Polycarpou, "A fault detection and isolation scheme for nonlinear uncertain discrete-time sytems," in *46th IEEE Conference on Decision and Control*, Dec 2007, pp. 1009–1014.

[20] P. M. Frank and X. Ding, "Survey of robust residual generation and evaluation methods in observer-based fault detection systems," *Journal of process control*, vol. 7, no. 6, pp. 403–424, 1997.

[21] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[22] L. J. Guibas, A. Nguyen, and L. Zhang, "Zonotopes as bounding volumes," in *Proceedings of the fourteenth annual ACM-SIAM symposium on Discrete algorithms*, ser. SODA '03. Philadelphia, PA, USA: Society for Industrial and Applied Mathematics, 12 Jan. 2003, pp. 803–812.

[23] F. Dabbene and D. Henrion, "Set approximation via minimum-volume polynomial sublevel sets," in *European Control Conference*, July 2013, pp. 1114–1119.

[24] D. P. Bertsekas, *Convex optimization theory*. Athena Scientific Belmont, 2009.

[25] R. Zippel, *Effective polynomial computation*. Springer Science & Business Media, 2012, vol. 241.

[26] R. T. Marler and J. S. Arora, "Survey of multi-objective optimization methods for engineering," *Structural and multidisciplinary optimization*, vol. 26, no. 6, pp. 369–395, 2004.

[27] V. Rostampour, K. Margellos, M. Vrakopoulou, M. Prandini, G. Andersson, and J. Lygeros, "Reserve requirements in ac power systems with uncertain generation," in *Innovative Smart Grid Technologies Europe (ISGT EUROPE)*. IEEE, 2013, pp. 1–5.

[28] K. Margellos, V. Rostampour, M. Vrakopoulou, M. Prandini, G. Andersson, and J. Lygeros, "Stochastic unit commitment and reserve scheduling: A tractable formulation with probabilistic certificates," in *European Control Conference (ECC)*. IEEE, 2013, pp. 2513–2518.

[29] V. Rostampour and T. Keviczky, "Probabilistic energy management for building climate comfort in smart thermal grids with seasonal storage systems," *arXiv preprint arXiv:1611.03206*, 2016.

[30] V. Rostampour, P. Mohajerin Esfahani, and T. Keviczky, "Stochastic nonlinear model predictive control of an uncertain batch polymerization reactor," *IFAC Conference on Nonlinear Model Predictive Control (NMPC)*, vol. 48, no. 23, pp. 540–545, 2015.

[31] M. C. Campi and S. Garatti, "The exact feasibility of randomized solutions of uncertain convex programs," *SIAM J. Optim.*, vol. 19, no. 3, pp. 1211–1230, 2008.

[32] L. Deori, S. Garatti, and M. Prandini, "Stochastic constrained control: trading performance for state constraint feasibility," *European Control Conference*, pp. 2740–2745, 2013.

[33] O. Kallenberg, *Foundations of Modern Probability*, ser. Probability and its Applications (New York). New York: Springer-Verlag, 1997.