Reference governor for tracking with fault detection capabilities

F. Stoican†, S. Olaru†, M.M. Seron‡ and J.A. De Doná‡

Abstract— **This paper presents a fault tolerant multisensor strategy for feedback control of a class of nonlinear systems upon a geometrical approach. A key point to ensure fault tolerance is the separation between healthy and faulty closed-loop behavior. Here we achieve this through set theoretic operations upon sets describing the healthy/faulty behavior of the system. The results rely both on an appropriate choice for the exogenous signals and on fixed point conditions for a nonlinear mapping which describes the gap between the nonlinear system and a linearized model in the functioning interval. A reference governor is employed such that, under a receding horizon technique, only feasible exogenous signals are provided to the system.**

I. Introduction

Nowadays the use of redundant sensors in applications is becoming ubiquitous. In modern applications there are strict requirements on the stability and performance criteria. Malfunctions in actuator, sensors or other systems components might lead to unsatisfactory performance or even instability. There are safety-critical systems in which this behavior is not merely inconvenient but can become catastrophic (well known examples of malfunctioning in aircraft incidents are discussed in [1]). As a consequence, a great deal of effort has been put into developing closed-loop systems which can tolerate faults, while maintaining desirable performance and stability properties [2]. Any fault tolerant control (FTC) scheme relies on two fundamental mechanisms, the fault detection and isolation (FDI) and the control reconfiguration mechanisms. The solutions employed usually implement *active* FTC schemes which react to a detected fault and reconfigure the control actions so that stability and performance can be satisfied.

Lately, set membership techniques for fault detection were proposed in the literature. In [3] parameter variances and bounded disturbances are considered in order to obtain a robust detection of faults. A new approach was proposed in [4], which uses a deterministic description of the sensor behavior in order to obtain fault tolerance guarantees upon invariant set separation. The approach utilizes bounded disturbance and noise descriptions, and derives a switching control which ensures closed-loop fault tolerant stabilization.

In the present paper, the technique is extended to systems with *nonlinear* dynamics, a reference governor employing a *receding horizon* optimization procedure to deliver a reference which permits fault detection, and a switching scheme enhanced to include all healthy sensors in designing the control action. The basic ingredients for the fault tolerant design are adapted to this general case as follows:

- Bounds for the region of ultimate convergence with respect to a pre-stabilizing control law are obtained (using the results in [5]) in order to construct sets associated to the healthy and faulty sensor behavior.
- The reference signals are provided through a reference governor which uses receding horizon techniques [6].
- Once the separation is achieved, the switch between the estimations can be handled using on-line optimization.

The following notations will be used throughout the paper. $\mathbb{N}$ denotes the set of non negative integers; $\mathbb{N}^+$ denotes the set $\mathbb{N} \setminus \{0\}$. Whenever time is unspecified, a variable x stands for $x(k)$ for some (unspecified) $k \in \mathbb{N}$, x^+ stands for the *successor* variable, that is, $x(k+1)$. Inequalities and absolute values of vectors and matrices are taken elementwise.

II. Problem statement

Consider the problem of trajectory tracking for the discrete-time nonlinear system

$$x^+ = f(x) + Bu + w \tag{1}$$

where $x \in \mathbb{R}^n$ is the state, $u \in \mathbb{R}^m$ is the control input, $w \in \mathbb{R}^n$ is an additive noise bounded as $|w| \leq \bar{w}$, $f : \mathbb{R}^n \to \mathbb{R}^n$ and $B \in \mathbb{R}^{n\times m}$ is a constant matrix. In this nonlinear setting, the tracking problem implies the existence of a reference state trajectory $\bar{x}(k)$ and a reference control action $\bar{u}(k)$ that satisfy

$$\bar{x}^+ = f(\bar{x}) + B\bar{u} \tag{2}$$

and are provided by a reference governor (R.G.), as shown in Figure 1. In the following sections we will design a fault tolerant control scheme based on the following assumption:

Assumption 1: The reference trajectories $(\bar{x}, \bar{u})$ are bounded, that is, $\bar{x}(k) \in \bar{X}$, $\bar{u}(k) \in \bar{U}$ for all $k \geq 0$, where $\bar{X} \subset \mathbb{R}^n$ and $\bar{U} \subset \mathbb{R}^m$ are compact sets. ♦

Then, a stabilizing controller can be designed for the dynamical system describing the *tracking error*

$$z^+ = F(z, \bar{x}) + Bv + w \tag{3}$$

with variables $z = x - \bar{x}$ and $v = u - \bar{u}$, where

$$F(z, \bar{x}) \triangleq f(z + \bar{x}) - f(\bar{x}). \tag{4}$$

† SUPELEC Systems Sciences (E3S) - Automatic Control Department, Gif sur Yvette, France {florin.stoican,sorin.olaru}@supelec.fr
‡ CDSC, The University of Newcastle, NSW 2308, Australia {maria.seron,jose.dedona}@newcastle.edu.au

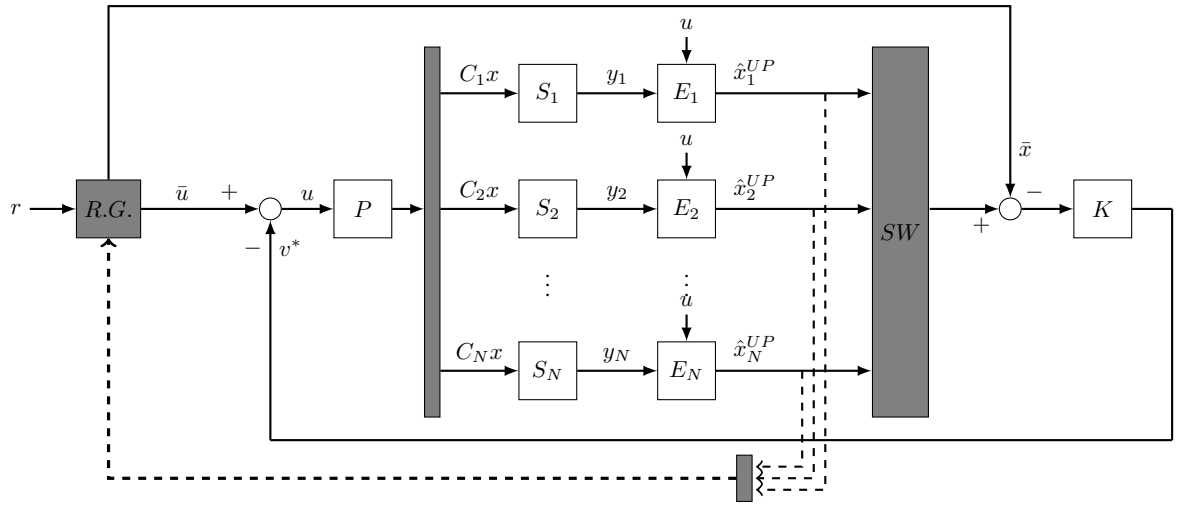


Fig. 1: Multisensor scheme with plant P, sensors S_i, estimators E_i and feedback gain K. The shaded blocks are the reference governor (R.G.) and the switching mechanism (SW)

For further use we consider F as a decomposition of linear[1] and nonlinear components, thus rewriting (3) as:

$$\begin{aligned} z^+ &= Az + Bv + \gamma(z,\bar{x}) + w \\ \gamma(z,\bar{x}) &\triangleq F(z,\bar{x}) - Az \\ &= \underbrace{(f(x) - Ax)}_{\theta(x)} - \underbrace{(f(\bar{x}) - A\bar{x})}_{\theta(\bar{x})} \end{aligned} \tag{5}$$

Different combinations of plant states are measured via a family of N sensors, as illustrated in Figure 1. We denote by $\mathcal{I} \triangleq \{1,\ldots,N\}$ the set of all sensor indices.

Definition 1 (Healthy sensor): The ith sensor, for $i \in \mathcal{I}$, is healthy if its output $y_i \in \mathbb{R}^{p_i}$ is given by

$$y_i = C_i x + \eta_i, \tag{6}$$

where $\eta_i \in \mathbb{R}^{p_i}$ is a bounded measurement disturbance satisfying $\eta_i \in N_i \subset \mathbb{R}^{p_i}$. ♦

Definition 2 (Faulty sensor): The jth sensor, for $j \in \mathcal{I}$, is faulty if its output is given by

$$y_j = \eta_j^F, \tag{7}$$

where η_j^F is a bounded measurement noise satisfying $\eta_j^F \in N_j^F \subset \mathbb{R}^{p_i}$, uncorrelated with the system's states. ♦

The sensors supply information which can be used for the estimation of the state. Assuming that the pairs (A, C_i) are detectable for $i = 1,\ldots,N$, we can use the following estimators:

$$\hat{x}_i^+ = A\hat{x}_i + Bu + \theta(\bar{x}) + L_i(y_i - C_i\hat{x}_i), \tag{8}$$

where the gains L_i are such that $A - L_iC_i$ are Schur matrices (their eigenvalues are strictly inside the unit circle). The nonlinear term $\theta(\bar{x})$ (see (5)) is introduced in order to counteract the nonlinearity of the plant model.

[1]Obtained for example as a first term of a Taylor expansion around an equilibrium point x_0: $A = \left.\frac{\partial f(x)}{\partial x}\right|_{x=x_0}$

An estimation update is considered in order to acknowledge the failure of a sensor at the very moment of occurrence

$$\hat{x}_i^{UP} = \hat{x}_i + M_i(y_i - C_i\hat{x}_i) \tag{9}$$

with matrix $M_i \in \mathbb{R}^{n\times p_i}$ arbitrarily taken (the usual choice being $M_i = A^{-1}L_i$). Additionally, we define the updated estimation tracking error for further use in the control action:

$$\hat{z}_i^{UP} = \hat{x}_i^{UP} - \bar{x} \tag{10}$$

For all estimators (8) taking measurements (6) from healthy sensors, the dynamics of the estimation error $\tilde{x}_i \triangleq x - \hat{x}_i$ can be expressed, using (1), (5), (6) and (8), as

$$\begin{aligned} \tilde{x}_i^+ &= (Ax + Bu + \theta(x) + w) \\ &\quad - (A\hat{x}_i + Bu + \theta(\bar{x}) + L_iC_i\tilde{x}_i + L_i\eta_i) \\ &= (A - L_iC_i)\tilde{x}_i + \gamma(z,\bar{x}) + w - L_i\eta_i. \end{aligned} \tag{11}$$

In the present paper we consider the regulation loop to have a fixed feedback gain[2] $v = -K\hat{z}_l^{UP}$, for some $l \in \mathcal{I}$ determined from a switch among any of the estimations associated with healthy sensors. The tracking error then satisfies

$$\begin{aligned} z^+ &= Az - BK\hat{z}_l^{UP} + \gamma(z,\bar{x}) + w \\ &= (A - BK)z + BK(I - M_lC_l)\tilde{x}_l \\ &\quad -BKM_l\eta_l + \gamma(z,\bar{x}) + w. \end{aligned} \tag{12}$$

In the following sections we will establish conditions that one has to impose in order to assure the selection of healthy estimations in the presence of faults.

III. Invariant set construction

To compute invariant sets we will use the *ultimate bounds* construction. This construction provides a computationally inexpensive description of robust positive invariant (RPI)

[2]K chosen such that $A - BK$ is a Schur matrix.

$$\zeta_{\mathcal{I}}^{+}=\underbrace{\begin{bmatrix}A-BK & & \\ & \ddots & \\ & & A-L_iC_i \\ & & & \ddots\end{bmatrix}}_{A_{\mathcal{I}}}\zeta_{\mathcal{I}}+\underbrace{\begin{bmatrix}\gamma(z,\bar{x})+BK(I-M_lC_l)\tilde{x}_l \\ \vdots \\ \gamma(z,\bar{x}) \\ \vdots\end{bmatrix}}_{\gamma_{\mathcal{I}}(\zeta_{\mathcal{I}},\bar{x})}+\underbrace{\left[\begin{array}{c|ccc}I & 0 & \cdots & -BKM_l \quad \cdots \quad 0 \\ \hline \vdots & & \ddots & 0 \\ I & & -L_i & \\ \vdots & 0 & & \ddots\end{array}\right]}_{E_{\mathcal{I},l}}\cdot\underbrace{\begin{bmatrix}w \\ \vdots \\ \eta_i \\ \vdots\end{bmatrix}}_{w_{\mathcal{I}}} \quad (13)$$

sets associated to a dynamical system affected by additive bounded disturbances ([5], [7], [8]).

Theorem 1: Consider the system $\xi^+ = \Phi\xi + \gamma(\xi) + w$, where $\xi \in \mathbb{R}^n$, $|w| \leq \bar{w}$ and $\Phi \in \mathbb{R}^{n\times n}$ has its eigenvalues strictly inside the unit circle and Jordan canonical form $\Lambda = V^{-1}\Phi V$. Suppose that a continuous map $\delta : \mathbb{R}^n_{+,0} \to \mathbb{R}^n_{+,0}$ exists such that $|\gamma(\xi)| \leq \delta(|\xi|)$ and $|\xi_1| \leq |\xi_2| \Rightarrow \delta(|\xi_1|) \leq \delta(|\xi_2|)$. Consider the map $T : \mathbb{R}^n_{+,0} \to \mathbb{R}^n_{+,0}$ defined by

$$T(\xi) = |\Lambda|\xi + |V^{-1}|\left[\delta(|V|\xi) + \bar{w}\right]. \quad (14)$$

Suppose that a fixed point b exists for $T(\xi)$. Then the set

$$S = \{\xi : |V^{-1}\xi| \leq b\} \quad (15)$$

is invariant.

Proof: The proof follows the lines of Theorem 4 in [5]. ■

It can be observed that equations (11)–(12) are interdependent and they cannot be decoupled as is the case for linear dynamics (see [4]). Thus, for the class of nonlinear dynamics in (1), the construction of invariant sets has to be performed in the augmented *tracking error + estimation error* state space. Denoting the augmented state vector by

$$\zeta_{\mathcal{I}} \triangleq \left[\begin{array}{c|ccc} z^T & \ldots & \tilde{x}_i^T & \ldots \end{array}\right]^T, \quad i \in \mathcal{I}, \quad (16)$$

we have that the augmented dynamics satisfy (13) where $A_{\mathcal{I}}$ is a Schur matrix and $l \in \mathcal{I}$ is the index of the estimation selected by the switching mechanism for the construction of the feedback control action.

Assumption 2: There exists a continuous map $\delta : \mathbb{R}^n_{+,0} \to \mathbb{R}^n_{+,0}$ satisfying $|z_1| \leq |z_2| \Rightarrow \delta(|z_1|) \leq \delta(|z_2|)$ such that $\forall z \in \mathbb{R}^n$, $|\gamma(z,\bar{x})| \leq \delta(|z|)$, $\forall \bar{x} \in \bar{X}$. ♦

Remark 1: Using Assumption 2, it can be shown that the function

$$\delta_{\mathcal{I}}(\zeta_{\mathcal{I}}) \triangleq \Big[(\delta(z) + \max_{i\in\mathcal{I}}|BK(I-M_iC_i)|\tilde{x}_i)^T, \delta(z)^T, \ldots, \ldots, \delta(z)^T\Big]^T \quad (17)$$

satisfies $|\zeta_{\mathcal{I}1}| \leq |\zeta_{\mathcal{I}2}| \Rightarrow \delta_{\mathcal{I}}(|\zeta_{\mathcal{I}1}|) \leq \delta_{\mathcal{I}}(|\zeta_{\mathcal{I}2}|)$ and, moreover, $\gamma_{\mathcal{I}}(\zeta_{\mathcal{I}}, \bar{x})$ defined in (13) can be bounded as

$$|\gamma_{\mathcal{I}}(\zeta_{\mathcal{I}}, \bar{x})| \leq \delta_{\mathcal{I}}(|\zeta_{\mathcal{I}}|), \forall \bar{x} \in \bar{X}. \quad (18)$$

In addition, using the bounds $\bar{w}$ for the disturbance term w in (1) and the bounds on the measurement noises described in Definitions 1 and 2, we have that the disturbance signal $w_{\mathcal{I}}$ defined in (13) can be bounded, for $k = 0, 1, \ldots,$ as

$$|w_{\mathcal{I}}(k)| \leq \bar{w}_{\mathcal{I}} \triangleq \left[\begin{array}{c|ccc} \bar{w}^T & \ldots & \bar{\eta}_i^T & \ldots \end{array}\right]^T. \quad \blacklozenge$$

We are now ready to use Theorem 1 to construct an invariant set for the augmented system (13).

Proposition 1: Let $A_{\mathcal{I}} = V_{\mathcal{I}}\Lambda_{\mathcal{I}}V_{\mathcal{I}}^{-1}$ be a Jordan decomposition of $A_{\mathcal{I}}$ defined in (13) and suppose the map $T_{\mathcal{I}} : \mathbb{R}^{(N+1)n}_{+,0} \to \mathbb{R}^{(N+1)n}_{+,0}$ defined as

$$T_{\mathcal{I}}(\zeta) = |\Lambda_{\mathcal{I}}|\zeta + |V_{\mathcal{I}}^{-1}|\delta_{\mathcal{I}}(|V_{\mathcal{I}}|\zeta) + \max_{l\in\mathcal{I}}|V_{\mathcal{I}}^{-1}E_{\mathcal{I},l}|\bar{w}_{\mathcal{I}} \quad (19)$$

with $E_{\mathcal{I},l}$ defined in (13) and $\delta_{\mathcal{I}}$, $\bar{w}_{\mathcal{I}}$ defined in Remark 1, has a fixed point $b_{\mathcal{I}}$. Then, the set

$$S_{\mathcal{I}} = \left\{\zeta_{\mathcal{I}} : \left|V_{\mathcal{I}}^{-1}\zeta_{\mathcal{I}}\right| \leq b_{\mathcal{I}}\right\} \quad (20)$$

is invariant for the closed-loop system (13) resulting from the switching control law $v = -K\hat{z}_l^{UP}, l \in \mathcal{I}$. ■

Using (16), projections on the tracking error and the estimation error spaces result, respectively, in the sets

$$S_z = \big[I\underbrace{0\ \ldots\ 0}_{N}\big]S_{\mathcal{I}}; \quad \tilde{S}_i = \big[0\ \underbrace{0\ \ldots\ I\ \ldots\ 0}_{N}\big]S_{\mathcal{I}},$$

which are such that z remains in S_z and $\tilde{x}_i$ remains in $\tilde{S}_i$, for $i \in \mathcal{I}$, whenever $\zeta_{\mathcal{I}}$ belongs to the invariant set $S_{\mathcal{I}}$.

IV. Fault tolerant scheme

A. Separation principle for FDI

In the current paper we propose a control scheme which is fault tolerant to sensor outages. Consequently we will use a fault detection and isolation mechanism that will acknowledge a faulty sensor and will remove it from the pool of available sensors for the reconfiguration of the control law.

We require the detection of faults to be robust with respect to the bounded/state-dependent disturbances considered. As such, we will see that the signals of interest are restricted to either "healthy" or "faulty" polytopic sets, denoted as R_i^H and R_i^F, respectively. These sets will be computed in an offline procedure and the actual fault detection reduces itself to a fast online set membership evaluation which will differentiate between the healthy/faulty cases as long as the separation condition

$$R_i^H \cap R_i^F = \emptyset, \quad \forall i \in \mathcal{I} \quad (21)$$

is verified. The variables and associated sets used for acknowledging the fault occurrence can be chosen through a variety of methods. In the following we present a method which constructs an appropriate residual signal [9] sensitive to fault occurrences. Indeed, the presence of a fault implies a

modification in the sensor output, as shown in Definitions 1 and 2, which will manifest itself in the residual signal

$$r_i = \hat{x}_i^{UP} - (I - M_i C_i)\,\hat{x}_i \tag{22}$$

composed from measurable quantities associated to the i^{th} sensor. From Definitions 1 and 2 the following forms are obtained for the healthy and faulty cases, respectively:

$$r_i^H = M_i C_i (z + \bar{x}) + M_i \eta_i \tag{23}$$
$$r_i^F = M_i \eta_i^F \tag{24}$$

The fault detection reduces then to the study of the sets R_i^H and R_i^F of all the possible values in the healthy, respectively faulty, case of the residual signal:

$$\begin{aligned} R_i^H &= M_i C_i S_z \oplus M_i C_i \bar{X} \oplus M_i N_i \\ R_i^F &= M_i N_i^F \end{aligned} \tag{25}$$

If sets (25) do not overlap (i.e., conditions (21) hold, which can be verified by an offline analysis) one can always guarantee fault detection at the moment of occurrence. Note also that the online test reduces itself to a low complexity set membership evaluation and that *a priori* knowledge of the current value of the reference signal $\bar{x}$ is not required.

Remark 2: If $0 \in N_i^F$ then the separation of the sets (25) is achieved by means of an offset in the reference signal (2) which implies the existence of an offset for the polytopic set $\bar{X}$ in Assumption 1. We can then define a maximal admissible region in which the reference signal $\bar{x}$ can take values:

$$\bar{X}_{max} = \{\bar{x} : \quad (21) \text{ are verified for all } i \in \mathcal{I}\} \tag{26}$$

Note that, although we require $\bar{X} \subseteq \bar{X}_{max}$, the set $\bar{X}$ may not always be chosen to be equal to $\bar{X}_{max}$ since this may adversely affect the nonlinear term $\gamma(z, \bar{x})$, rendering the invariant set computation more difficult (i.e., the iterative application of map (19) may not converge to a fixed point).♦

B. Fault tolerance guarantees

With the FDI mechanism outlined in Subsection IV-A we are now ready to treat the appearance of a fault.

Theorem 2: Consider the multisensor scheme described in Section II and the associated sets R_i^H and R_i^F defined as in Subsection IV-A. Suppose $R_i^H \cap R_i^F = \emptyset$ for all $i \in \mathcal{I}$ and let the initial augmented state $\zeta_{\mathcal{I}}(0)$ in (13) satisfy $\zeta_{\mathcal{I}}(0) \in S_{\mathcal{I}}$. If at all future instants there exists at least one sensor which is healthy (in order for the switching mechanism to have at least one choice), then there exists a control law that preserves the invariance of the signals corresponding to the sensors that remain healthy (as per Definition 1).

Proof: Let the set $\mathcal{I}$ be split in two disjoint sets $\mathcal{I} = \mathcal{H}(k) \cup \mathcal{F}(k)$ corresponding to indices of healthy and faulty sensors, respectively, at each sampling time $k > 0$. Since $\zeta_{\mathcal{I}}(0) \in S_{\mathcal{I}}$ by assumption, we then initialize the multisensor scheme with $\mathcal{H}(0) = \mathcal{I}$. At each $k > 0$, the control law $v(k) = -K\hat{z}_l^{UP}(k), l \in \mathcal{H}(k)$ is applied and there exist "fictitious" values for $\tilde{x}_j(k), \forall j \in \mathcal{F}(k)$ (e.g. $\tilde{x}_j(k) = 0$) such that the extended vector $\zeta_{\mathcal{I}}(k+1) \in S_{\mathcal{I}}$. Recalling the definitions (25) of the "healthy/faulty residual sets" R_j^H, R_j^F, fault detection is then immediate by using property (21) that R_j^H and R_j^F are disjoint. Indeed, the detection mechanism has to update the set $\mathcal{F}(k+1) = \mathcal{F}(k) \cup \{j\}$ for all indices j which satisfy $r_j(k) \in R_j^F$. Finally, $\mathcal{H}(k+1) = \mathcal{I} \setminus \mathcal{F}(k+1)$ and the proof is complete. ■

We observe that the hypothesis that $\zeta_{\mathcal{I}}(0) \in S_{\mathcal{I}}$ (which prompts us to initialize $\mathcal{H}(0) = \mathcal{I}$) is not restrictive, any combination $\mathcal{I} = \mathcal{H}(0) \cup \mathcal{F}(0)$ with $\mathcal{H}(0) \neq \emptyset$ can be handled similarly.

C. Control law design

The design of the control law $u = \bar{u} + v$ consists of the separate construction of both feedforward ($\bar{u}$) and feedback (v) control actions for the system.

The feedforward action is provided by the reference governor, which has to choose a feasible reference signal (such that (21) will be verified) and, at the same time, follow an *ideal* reference as close as possible. This problem can be cast as the optimization of a cost function under constraints, and it will be solved here in a model predictive control (MPC) formulation:

$$\bar{u}^*(k) = \underset{\bar{u}(k),\ldots,\bar{u}(k+\tau)}{argmin} \sum_{i=0}^{i=\tau} (||r(k+i) - \bar{x}(k+i)||_{Q_r} + ||\bar{u}(k+i)||_{R_r})$$

subject to:

$$\begin{aligned} \bar{x}(k+i+1) &= f(\bar{x}(k+i)) + B\bar{u}(k+i) \\ \bar{x}(k+i) &\in \bar{X}_{max} \end{aligned} \tag{27}$$

where $r \in \mathbb{R}^n$ is the ideal reference to be followed, τ is the prediction horizon, and $Q_r \in \mathbb{R}^{n \times n}$ and $R_r \in \mathbb{R}^{m \times m}$ are weighting matrices. The feedforward control action is then set to $\bar{u} = \bar{u}^*(k)$.

A refinement can be applied if we use the information provided by the sensors to estimate the tracking error at the current time, by employing a technique described in [10]:

Lemma 1: The tracking error of the plant is described at the current time instant k by the set

$$Z_{\mathcal{H}(k)} = \bigcap_{l \in \mathcal{H}(k)} \left(\{\hat{z}_l^{UP}\} \oplus (I - M_l C_l)\tilde{S}_l \oplus (-M_l N_l) \right) \tag{28}$$

Proof: The tracking error is rewritten as a sum of unmeasurable disturbances and the measurable updated estimation tracking error associated with any healthy sensor l:

$$z = \hat{z}_l^{UP} + (I - M_l C_l)\tilde{x}_l - M_l \eta_l \tag{29}$$

Considering the sets that define $\tilde{x}_l$ and η_l one obtains that

$$z \in \{\hat{z}_l^{UP}\} \oplus (I - M_l C_l)\tilde{S}_l \oplus (-M_l N_l) \tag{30}$$

and taking into account all the values proposed by the acknowledged healthy sensors it follows that z belongs to the set defined in (28), thus concluding the proof. ■

Thus, at the current instant k, the tracking error will reside in $S_z \cap Z_{\mathcal{H}(k)}$ and then the optimization problem (27) can be reformulated as:

$$\bar{u}^*(k) = \underset{\bar{u}(k),\ldots,\bar{u}(k+\tau)}{argmin} \sum_{i=0}^{i=\tau} (||r(k+i) - \bar{x}(k+i)||_{Q_r} + ||\bar{u}(k+i)||_{R_r})$$

subject to:

$$\begin{aligned} \bar{x}(k+i+1) &= f(\bar{x}(k+i)) + B\bar{u}(k+i) \\ M_j \left\{C_j \left\{\bar{x}(k+i)\right\} \oplus C_j(S_z \cap Z_{\mathcal{H}(k+i|k)}) \oplus N_j\right\} & \\ \cap M_j N_j^F = \emptyset, \quad \forall j \in \mathcal{I} & \quad (31) \end{aligned}$$

where $Z_{\mathcal{H}(k|k)} = Z_{\mathcal{H}(k)}$ is the set defined in (28) and $Z_{\mathcal{H}(k+i|k)}$ for $i \geq 1$ is a prediction of $Z_{\mathcal{H}(k)}$ based on the prediction of the updated estimation tracking error $\hat{z}_l^{UP}$.

A few remarks concerning the computational aspects are in order:

Remark 3: Problem (31), although less conservative than (27), is difficult to implement since it requires the prediction of the updated tracking errors $\hat{z}_l^{UP}$. Due to noise presence the future values will be set-valued and, in consequence, (28) will increase exponentially, reducing the degree to which it is relevant in approximating the tracking error. ♦

Remark 4: Even when the sets N_i, N_i^F and S_z employed in (21) to describe the residuals sets are convex and contain the origin, $\bar{X}_{max}$ will in general be nonconvex. This will involve solving the problem (27) in the framework of mixed-integer logic. ♦

We now turn to the feedback component v of the control action $u = \bar{u} + v$. As mentioned before, one alternative is to use a switching among the healthy updated estimation tracking errors. The following Lemma with prove that the choice of the feedback control law by switching between the healthy estimations can be relaxed to any point residing inside their convex hull.

Lemma 2: Any convex combination of healthy updated estimation tracking errors used to construct the control action will preserve the invariance of the tracking error set S_z.

Proof: Consider a convex combination of healthy updated tracking errors $z_*^{UP} = \sum_{l \in \mathcal{H}} \alpha_l \hat{z}_l^{UP}$, with $\sum_{l \in \mathcal{H}} \alpha_l = 1$, $\alpha_l \geq 0$. Applying $v_* = -Kz_*^{UP}$ in (5) we obtain

$$\begin{aligned} z^+ &= Az - BKz_*^{UP} + \gamma(z, \bar{x}) + w \\ &= Az - BK \sum_{l \in \mathcal{H}} \alpha_l \hat{z}_l^{UP} + \gamma(z, \bar{x}) + w \\ &= \sum_{l \in \mathcal{H}} \alpha_l \underbrace{\left(Az - BK\hat{z}_l^{UP} + \gamma(z, \bar{x}) + w\right)}_{z_l^+} \quad (32) \end{aligned}$$

where, by z_l^+ we denoted the next value of the tracking error if at the current moment the control action was provided by the l^{th} sensor. As it can be seen, z^+ will be a convex combination of interior points z_l^+ of S_z (by the invariance property) and, as a consequence, will be itself inside the set, since by construction (see (20)) the sets $S_{\mathcal{I}}$ and $S_z = \begin{bmatrix} I & 0 & \ldots & 0 \end{bmatrix} S_{\mathcal{I}}$ are convex, thus concluding the proof.■

Using Lemma 2 one can apply the control action

$$u = \bar{u} - Kz^* \quad (33)$$

with z^* selected by minimizing a suitable cost function, e.g.,

$$z^* = \underset{z \in ConvexHull(\hat{z}_l^{UP},\, l \in \mathcal{H})}{argmin} z^T P z \quad (34)$$

for some appropriate weighting matrix P (e.g., the solution to the Riccati equation associated to the weighting matrices Q and R used to design the feedback gain K in an LQR sense).

V. Example

Consider the nonlinear discrete-time system

$$x^+ = \begin{bmatrix} 1 & 0.1 \\ 0 & 1 \end{bmatrix} x + \begin{bmatrix} \frac{\sqrt{|x_1|}}{60} \\ 0 \end{bmatrix} + \begin{bmatrix} 0.1 \\ 0.1 \end{bmatrix} u + \begin{bmatrix} 0 \\ 0.1 \end{bmatrix} w$$

with the plant noise w bounded by $|w| \leq 0.2$.

We consider three sensors defined by

$$C_{1,2,3} = \left\{\begin{bmatrix} 1 & 0 \end{bmatrix}, \begin{bmatrix} 0.5 & 1 \end{bmatrix}, \begin{bmatrix} 0.75 & 0.25 \end{bmatrix}\right\}$$

and affected by noises bounded by

$$\bar{\eta}_{1,2,3} = 0.1, \bar{\eta}_{1,2,3}^F = 1.$$

The poles of $A - L_i C_i$,

$$p_{1,2,3} = \left\{\begin{bmatrix} 0.93 & 0.80 \end{bmatrix}, \begin{bmatrix} 0.95 & 0.85 \end{bmatrix}, \begin{bmatrix} 0.96 & 0.80 \end{bmatrix}\right\}$$

are assigned through gain matrices

$$L_{1,2,3} = \left\{\begin{bmatrix} 0.27 & 0.14 \end{bmatrix}^T, \begin{bmatrix} 0.10 & 0.15 \end{bmatrix}^T, \begin{bmatrix} 0.28 & 0.11 \end{bmatrix}^T\right\}.$$

The update matrices in (9) are computed as $M_{1,2,3} = A^{-1}L_{1,2,3}$.

Using tuning parameters $Q = \begin{bmatrix} 0.10 & 0 \\ 0 & 6.32 \end{bmatrix}$, $R = 7.26$, we select $K = \begin{bmatrix} 0.11 & 1 \end{bmatrix}$ as the optimal feedback gain (in the LQR sense) which will be used to construct the closed loop system, as in (12).

Using the fact that $\left|\sqrt{|b|} - \sqrt{|a|}\right| \leq \sqrt{|b-a|}$ is valid for any $a, b \in \mathbb{R}$ one can bound the tracking error nonlinear component, as $|\gamma(z, \bar{x})| \leq \delta(|z|)$ with $\delta(z) \triangleq \begin{bmatrix} \frac{\sqrt{|z_1|}}{60} \\ 0 \end{bmatrix}$ respecting Assumption 2.

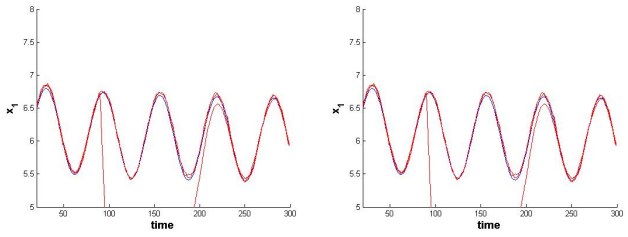
Since $\delta(z)$ does not depend on the values taken by $\bar{x} \in \bar{X}$ it follows that, in the sense of Remark 2, we can maximize the range of available references to $\bar{X} = \bar{X}_{max}$ with $\bar{X}_{max}$ defined as in (26). Using this function $\delta(z)$ in (17) we can apply Proposition 1 to obtain, for the augmented system (13), the invariant set (20) where the fixed point

$$b_{\mathcal{I}} = 10^{-2} \cdot \begin{bmatrix} 0.4 & 0.5 & 13.3 & 19.8 & 3.9 & 13.9 & 7.7 & 12.4 \end{bmatrix}^T$$

is computed by iteration of mapping (19).

Using the projection of the set on the z axis, S_z, the healthy and faulty residual sets (25) are constructed for the three sensors.

In Figure 3 the maximal reference set $\bar{X}_{max}$ is depicted. An ideal reference r (continuous blue line) is provided which will be tracked by the reference governor through a receding horizon procedure with $\tau = 5$ prediction steps as in (27). The result is the reference pair $(\bar{u}, \bar{x})$ ($\bar{x}$ shown in dashed



(a) convex sum selection (b) single sensor selection

Fig. 2: Scenario of functioning for multisensor scheme (blue for reference, red for state estimations) – the first component of the state.

blue line) which will be provided to the plant for reference tracking.

A scenario of functioning is depicted in Figure 2. For comparison purposes, the strategy described in (33)–(34) (with the choice of P mentioned after (34)), is shown in Figure 2(a), and a switching strategy that also applies the control (33), but with z^* being the minimizer of the cost function $z^T P z$ over $z \in \{\hat{z}_1^{UP}, \ldots, \hat{z}_N^{UP}\}$, is shown in Figure 2(b). In both cases one can see that the reference is accurately followed, even under a fault occurring in the 2^{nd} sensor at step $k = 90$ (also shown are the estimates of x_1 based on the second sensor, which fails at $k = 90$ and later recovers at $k = 150$). Moreover, even if not visually noticed in this comparison, it is to be expected that the enhanced command design (33)–(34) will have superior performance, in the sense that it minimizes the same cost function over a larger set of values. In effect, an integral cost over the simulation window of 15.159 was reached for the first method and 25.318 for the second one.

VI. Conclusions

The paper has presented a fault tolerant control scheme based on a reconfigurable control action for a class of nonlinear multisensor systems. The detection of abrupt faults was realized through set membership testing. The reference followed by the system was obtained through a reference governor which employs a receding horizon technique in order to determine a reference which enables the fault detection mechanism. The construction of the feedback control law was redesigned to take into account the information provided by all the healthy sensors. The nonlinear case presents interesting challenges, including the tightening of the invariant sets which allows fault detection and the effect of the structure of the optimization problems on real-time performance.

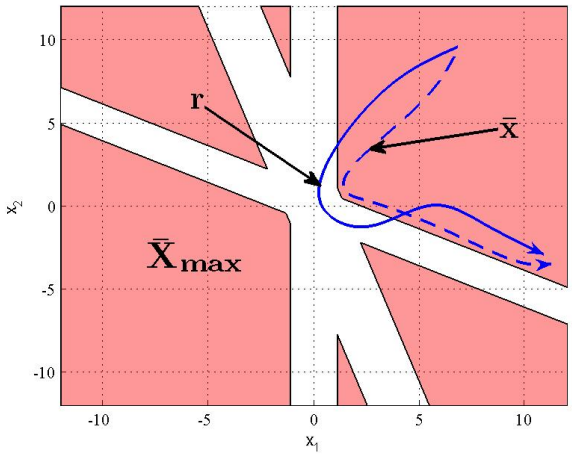


Fig. 3: Maximal reference set $\bar{X}_{max}$ with ideal reference r (continuous blue line) and feasible reference $\bar{x}$ (dashed blue line)

References

[1] J. Maciejowski and C. Jones, "MPC fault-tolerant flight control case study: Flight 1862," in *Proc. of the 4th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, Washington, DC, USA, June 2003.

[2] Y. Zhang and J. Jiang, "Bibliographical review on reconfigurable fault-tolerant control systems," *Annual Reviews in Control*, vol. 32, no. 2, pp. 229–252, 2008.

[3] P. Planchon and J. Lunze, "Diagnosis of linear systems with structured uncertainties based on guaranteed state observation," *Int. Journal of Control Automation and Systems*, vol. 6, no. 3, pp. 306–319, Jun. 2008.

[4] M. M. Seron, X. W. Zhuo, J. A. De Doná, and J. J. Martínez, "Multisensor switching control strategy with fault tolerance guarantees," *Automatica*, vol. 44, no. 1, pp. 88–97, 2008.

[5] E. Kofman, H. Haimovich, and M. M. Seron, "A systematic method to obtain ultimate bounds for perturbed systems," *Int. Journal of Control*, vol. 80, no. 2, pp. 167–178, 2007.

[6] S. Olaru and D. Dumur, "Compact explicit MPC with guarantee of feasibility for tracking," in *Proc. of the 44th IEEE Conf. on Decision and Control and European Control Conf.*, Seville, Spain, 12-15 December 2005, pp. 969–974.

[7] H. Haimovich, E. Kofman, and M. M. Seron, "Systematic ultimate bound computation for sampled-data systems with quantization," *Automatica*, vol. 43, no. 6, pp. 1117–1123, 2007.

[8] E. Kofman, "Non-conservative ultimate bound estimation in LTI perturbed systems," *Automatica*, vol. 41, no. 10, pp. 1835–1838, 2005.

[9] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and fault-tolerant control*. Springer-Verlag, 2006.

[10] S. Olaru, F. Stoican, J. A. De Doná, and M. M. Seron, "Necessary and sufficient conditions for sensor recovery in a multisensor control scheme," in *Proc. of the 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, Barcelona, Spain, 30 June-3 July 2009, pp. 977–982.