Closed-loop Actuator-fault Detection and Isolation using Invariant Sets and Tubes

Feng Xu [*] **Vicenç Puig** [*] **Carlos Ocampo-Martinez** [*]
Florin Stoican [**] **Sorin Olaru** [***]

[*] *Institut de Robòtica i Informàtica Industrial (CSIC-UPC), Technical University of Catalonia, Llorens i Artigas, 4-6, Barcelona, Spain,* {*fxu, vpuig, cocampo*}*@iri.upc.edu*
[**] *Politehnica University of Bucharest (PUB), Department of Automatic Control and Systems Engineering, Bucharest, Romania, florin.stoican@acse.pub.ro*
[***] *SUPELEC Systems Sciences, Automatic Control Department and EPI INRIA DISCO, France, sorin.olaru@supelec.fr*

Abstract: This paper proposes a new actuator-fault detection and isolation (FDI) strategy for closed-loop discrete time-invariant systems by using invariant sets and tubes. In this approach, invariant sets are used for fault detection (FD) and the establishment of FDI conditions, while the tubes are generated for fault isolation (FI) at transient state. Comparing with the existing set-theoretic FDI techniques, the advantage of this approach consists in that it exhibits a balance between the conservativeness of FDI conditions, the fast FI response and the computational complexity. The effectiveness of the proposed technique is illustrated by a numerical example.

1. INTRODUCTION

Fault occurrence always implies the switching of the system functioning modes (see [Blanke et al., 2006]). With respect to each mode of the system, an invariant set can be constructed to confine the residual of the mode and as long as all invariant sets (one healthy invariant set and at least one faulty invariant set) are disjoint from each other, the fault can be isolated [Ocampo-Martinez et al., 2010].

In the literature, the features of the set-theoretic actuator FDI techniques are that they are generally based on a bank of observers and that only the observer selected by the FDI module is used for FDI [Ocampo-Martinez et al., 2010, Seron and Doná, 2010], e.g., if the i-th observer is chosen to reconfigure the closed-loop system, then only the residual generated by the i-th observer is real-time tracked for FDI. Thus, once the residual corresponding to the i-th observer leaves its corresponding invariant set, it implies that a fault is detected. Then, FI is based on finding an after-fault invariant set corresponding to the i-th observer, which the residual of the i-th observer finally enters into.

Actually, these existing approaches waste some useful system information, i.e., the information provided by the other observers not matching the mode. In principle, if the system information obtained by all the observers can be used, the guaranteed FDI conditions will be at least not more conservative than those proposed in [Ocampo-Martinez et al., 2010, Seron and Doná, 2010].

Besides, the FI techniques proposed in [Ocampo-Martinez et al., 2010] have to observe a waiting time until the transit state between the modes elapses, which delays the FI decision. To avoid this waiting time, [Seron and Doná, 2010] proposed a technique to implement FDI one step after faults by considering one-step-after-fault sets.

However, considering the contractiveness of observers, the one-step-after-fault sets (transient sets) are generally bigger than the corresponding invariant sets (steady limit sets). Note that any increase in set size implies an increase in the conservativeness of FDI conditions.

The objective of this paper is to propose a new technique to obtain a balance among the existing invariant set-based approaches. The main contribution lies in that it uses the process information provided by all the observers to implement FDI by establishing less conservative FDI conditions and generating tubes to make FI decisions during the transient state induced by faults.

The notation $|\cdot|$ denotes the elementwise absolute value, $\mathbf{B}^r$ is a box composed of r unitary intervals, the inequalities are understood elementwise, O and I denote the zero and the identity matrices with compatible dimensions, respectively, the notation $\text{diag}(\cdot)$ denotes the diagonal matrix, and for a vector a, its transpose is denoted as a^T.

2. PROBLEM FORMULATION

The discrete time-invariant plant is modeled by

$$x_{k+1} = Ax_k + BF_iu_k + \omega_k, \tag{1a}$$
$$y_k = Cx_k + \eta_k, \tag{1b}$$

where $A \in \mathbb{R}^{n \times n}$, $B \in \mathbb{R}^{n \times p}$ and $C \in \mathbb{R}^{q \times n}$ are constant matrices, $x_k \in \mathbb{R}^n$, $u_k \subset \mathbb{R}^p$ and $y_k \in \mathbb{R}^q$ are states, inputs and outputs at time instant k, respectively, and ω_k and η_k denote process disturbances and measurement noises, respectively. The matrix F_i ($i \in \mathbb{I} = \{0, 1, \cdots N\}$) is a diagonal matrix modeling the i-th actuator mode [1], where F_0 is the identity matrix describing the healthy mode.

---

[1] The set $\mathbb{I}$ represents a finite range of actuator modes (healthy or faulty) critical to the system performance and/or safety.

Assumption 2.1. The pairs (A, BF_i) and (A, C) are stabilizable and detectable, respectively. ∎

Assumption 2.2. Only one fault occurs at a time and the fault is persistent such that the FDI module has enough time to detect and isolate it. ∎

According to (1), the j-th ($j \in \mathbb{I}$) observer matching the j-th mode is designed as

$$\hat{x}_{k+1}^j = (A - L_j C)\hat{x}_k^j + BF_j u_k + L_j y_k, \tag{2a}$$

$$\hat{y}_k^j = C\hat{x}_k^j, \tag{2b}$$

where $\hat{x}_k^j$ and $\hat{y}_k^j$ are the states and output estimations, respectively, and L_j is the observer gain.

Assumption 2.3. The observer gain L_j assures that $A - L_j C$ is a Schur matrix. ∎

This paper only considers FDI (from healthy to faulty) and does not discuss mode switching (from faulty to healthy/faulty to faulty), since the principles are similar. Thus, the system is considered healthy at the beginning and the corresponding reference system is designed as

$$x_{k+1}^{\text{ref}} = Ax_k^{\text{ref}} + Bu_k^{\text{ref}}, \tag{3}$$

where x_k^{ref} and u_k^{ref} denote the reference states and inputs.

The control objective of the closed-loop system is to make the states asymptotically track the reference state trajectory. Since the system is healthy, the state estimation of the nominal observer is used for the closed-loop system design. Using (1), (2) and (3), the control law is given as

$$u_k = u_k^{\text{ref}} - K(\hat{x}_k^0 - x_k^{\text{ref}}), \tag{4}$$

where $\hat{x}_k^0$ is the estimated state from the nominal observer and K is the feedback gain such that the closed-loop system is always stable.

Assumption 2.4. u_k^{ref}, ω_k and η_k are bounded, i.e.,

$U_{\text{ref}} = \{u_k^{\text{ref}} \in \mathbb{R}^p : \left| u_k^{\text{ref}} - u_{\text{ref}}^c \right| \le \bar{u}_{\text{ref}}, u_{\text{ref}}^c \in \mathbb{R}^p, \bar{u}_{\text{ref}} \in \mathbb{R}^p \}$,

$W = \{\omega_k \in \mathbb{R}^n : |\omega_k - \omega^c| \le \bar{\omega}, \omega^c \in \mathbb{R}^n, \bar{\omega} \in \mathbb{R}^n \}$,

$V = \{\eta_k \in \mathbb{R}^q : |\eta_k - \eta^c| \le \bar{\eta}, \eta^c \in \mathbb{R}^q, \bar{\eta} \in \mathbb{R}^q \}$,

where the vectors u_{ref}^c, ω^c, η^c, $\bar{u}_{\text{ref}}$, $\bar{\omega}$ and $\bar{\eta}$ are constant. ∎

Note that, considering the structure of U_{ref}, W and V, they can be rewritten as zonotopes: $U_{\text{ref}} = u_{\text{ref}}^c \oplus H_{\bar{u}_{\text{ref}}} \mathbf{B}^p$, $W = \omega^c \oplus H_{\bar{\omega}} \mathbf{B}^n$ and $V = \eta^c \oplus H_{\bar{\eta}} \mathbf{B}^q$, where $H_{\bar{u}_{\text{ref}}} \in \mathbb{R}^{p \times p}$, $H_{\bar{\omega}} \in \mathbb{R}^{n \times n}$ and $H_{\bar{\eta}} \in \mathbb{R}^{q \times q}$ are diagonal matrices with the main diagonals being $\bar{u}_{\text{ref}}$, $\bar{\omega}$ and $\bar{\eta}$, respectively.

3. SYSTEM ANALYSIS

3.1 Residuals

The components given in (1), (2), (3) and (4) constitute the closed-loop system and, $\hat{x}_k^j$, x_k^{ref}, $\hat{y}_k^j$ and y_k are obtainable signals, which convey the real-time system information. To implement the proposed technique, one defines the residual corresponding to the j-th observer as

$$r_k^j = x_k^{\text{ref}} - \hat{x}_k^j. \tag{5}$$

In the fault-free situation, as indicated in (4), the state estimation of the nominal observer is used to generate the closed-loop control laws. Even though the system becomes faulty, the nominal observer will still be used for the closed-loop control before the fault is isolated.

Moreover, according to (2), (3), (4) and (5), the dynamics of r_k^j are obtained as

$$r_{k+1}^j = Ar_k^j - BF_j K r_k^0 - L_j C \tilde{x}_k^j + (B - BF_j)u_k^{\text{ref}} - L_j \eta_k, \tag{6}$$

where $\tilde{x}_k^j$ is the state estimation error of the j-th observer, which is defined as $\tilde{x}_k^j = x_k - \hat{x}_k^j$. As per (6), whichever mode the system is in, the residual dynamics corresponding to a certain observer have the same structure.

However, for different modes, the dynamics of $\tilde{x}_k^j$ are generally different. For example, in the i-th mode, the dynamics of $\tilde{x}_k^j$ are derived as

$$\tilde{x}_{k+1}^j = (A - L_j C)\tilde{x}_k^j + B(F_i - F_j)K r_k^0 + B(F_i - F_j)u_k^{\text{ref}} + \omega_k - L_j \eta_k, \tag{7}$$

where F_i and F_j correspond to the i-th mode active at the current situation and the j-th observer, respectively.

Since $N + 1$ observers are used, at each time instant, one can obtain $N + 1$ residuals and $N + 1$ state estimation errors. Thus, in order to collect all useful process information, one defines the following vectors:

$$\mathbf{z}_k^i = \begin{bmatrix} \mathbf{r}_k^i \\ \tilde{\mathbf{x}}_k^i \end{bmatrix}, \mathbf{r}_k^i = \begin{bmatrix} r_k^0 \\ r_k^1 \\ \vdots \\ r_k^N \end{bmatrix}, \tilde{\mathbf{x}}_k^i = \begin{bmatrix} \tilde{x}_k^0 \\ \tilde{x}_k^1 \\ \vdots \\ \tilde{x}_k^N \end{bmatrix}, \tag{8}$$

where $\mathbf{r}_k^i$ and $\tilde{\mathbf{x}}_k^i$ collect all the residuals and state estimation errors corresponding to all the observers in the i-th mode, respectively. Moreover, according to (6) and (7), the dynamics of $\mathbf{z}_k^i$ are derived as

$$\mathbf{z}_{k+1}^i = A_{\mathbf{z}}^i \mathbf{z}_k^i + B_{\mathbf{z}}^i u_k^{\text{ref}} + E_\omega^{\mathbf{z}} \omega_k + E_\eta^{\mathbf{z}} \eta_k, \tag{9}$$

where

$$A_{\mathbf{z}}^i = \begin{bmatrix} A - BF_0 K & O & \cdots & O & -L_0 C & O & \cdots & O \\ -BF_1 K & A & \cdots & O & O & -L_1 C & \cdots & O \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ -BF_N K & O & \cdots & A & O & O & \cdots & -L_N C \\ B(F_i - F_0)K & O & \cdots & O & A - L_0 C & O & \cdots & O \\ B(F_i - F_1)K & O & \cdots & O & O & A - L_1 C & \cdots & O \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ B(F_i - F_N)K & O & \cdots & O & O & O & \cdots & A - L_N C \end{bmatrix},$$

$$B_{\mathbf{z}}^i = \begin{bmatrix} B - BF_0 \\ B - BF_1 \\ \vdots \\ B - BF_N \\ B(F_i - F_0) \\ B(F_i - F_1) \\ \vdots \\ B(F_i - F_N) \end{bmatrix}, E_\omega^{\mathbf{z}} = \begin{bmatrix} O \\ O \\ \vdots \\ O \\ I \\ I \\ \vdots \\ I \end{bmatrix}, E_\eta^{\mathbf{z}} = \begin{bmatrix} -L_0 \\ -L_1 \\ \vdots \\ -L_N \\ -L_0 \\ -L_1 \\ \vdots \\ -L_N \end{bmatrix}.$$

In the i-th mode, the behavior of the closed-loop system can be described by (9). Considering u_k^{ref}, ω_k and η_k are bounded, by substituting their bounding sets into (9), one can obtain a set-based dynamics of (9) as

$$\mathbf{Z}_{k+1}^i = A_{\mathbf{z}}^i \mathbf{Z}_k^i \oplus B_{\mathbf{z}}^i U_{\text{ref}} \oplus E_\omega^{\mathbf{z}} W \oplus E_\eta^{\mathbf{z}} V. \tag{10}$$

In order to reduce computational complexity and the consequences of the wrapping effect [Neumaier, 1993], (9) is equivalently split into two different lower-order dynamics that are presented as

$$\mathbf{r}_{k+1}^i = A_{\mathbf{r}} \mathbf{r}_k^i + B_{\mathbf{r}} u_k^{\text{ref}} + E_{\tilde{\mathbf{x}}} \tilde{\mathbf{x}}_k^i + E_\eta \eta_k, \tag{11}$$

where

$$A_{\mathbf{r}} = \begin{bmatrix} A-BF_0K & O & O & \cdots & O \\ -BF_1K & A & O & \cdots & O \\ -BF_2K & O & A & \cdots & O \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ -BF_NK & O & O & \cdots & A \end{bmatrix}, \quad B_{\mathbf{r}} = \begin{bmatrix} B-BF_0 \\ B-BF_1 \\ B-BF_2 \\ \vdots \\ B-BF_N \end{bmatrix},$$

$$E_{\tilde{\mathbf{x}}} = \begin{bmatrix} -L_0C & O & O & \cdots & O \\ O & -L_1C & O & \cdots & O \\ O & O & -L_2C & \cdots & O \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ O & O & O & \cdots & -L_NC \end{bmatrix}, \quad E_{\eta} = \begin{bmatrix} -L_0 \\ -L_1 \\ -L_2 \\ \vdots \\ -L_N \end{bmatrix},$$

and

$$\tilde{\mathbf{x}}_{k+1}^i = A_{\tilde{\mathbf{x}}}\tilde{\mathbf{x}}_k^i + B_{\tilde{\mathbf{x}}}^i u_k^{\mathrm{ref}} + E_{\mathbf{r}}^i r_k^0 + E_{\omega}^{\tilde{x}}\omega_k + E_{\eta}\eta_k, \quad (12)$$

where

$$A_{\tilde{\mathbf{x}}} = \begin{bmatrix} A-L_0C & O & \cdots & O \\ O & A-L_1C & \cdots & O \\ \vdots & \vdots & \cdots & \vdots \\ O & O & \cdots & A-L_NC \end{bmatrix}, \quad B_{\tilde{\mathbf{x}}}^i = \begin{bmatrix} B(F_i-F_0) \\ B(F_i-F_1) \\ \vdots \\ B(F_i-F_N) \end{bmatrix},$$

$$E_{\mathbf{r}}^i = \begin{bmatrix} B(F_i-F_0)K \\ B(F_i-F_1)K \\ \vdots \\ B(F_i-F_N)K \end{bmatrix}, \quad E_{\omega}^{\tilde{x}} = \begin{bmatrix} I \\ I \\ \vdots \\ I \end{bmatrix}.$$

Thus, by considering (11) and (12) together and substituting the sets of ω_k and η_k into them, one can obtain another set-based description of the dynamics:

$$\mathbf{R}_{k+1}^i = A_{\mathbf{r}}\mathbf{R}_k^i \oplus \{B_{\mathbf{r}}u_k^{\mathrm{ref}}\} \oplus E_{\tilde{\mathbf{x}}}\tilde{\mathbf{X}}_k^i \oplus E_{\eta}V, \quad (13a)$$

$$\tilde{\mathbf{X}}_{k+1}^i = A_{\tilde{\mathbf{x}}}\tilde{\mathbf{X}}_k^i \oplus \{B_{\tilde{\mathbf{x}}}^i u_k^{\mathrm{ref}}\} \oplus \{E_{\mathbf{r}}^i r_k^0\} \oplus E_{\omega}^{\tilde{x}}W \oplus E_{\eta}V. \quad (13b)$$

Remark 1. Comparing (9) with (13), as long as $\mathbf{r}_{k^*}^i \in \mathbf{R}_{k^*}^i$ and $\tilde{\mathbf{x}}_{k^*}^i \in \tilde{\mathbf{X}}_{k^*}^i$ are satisfied at time instant k^*, $\mathbf{r}_k^i \in \mathbf{R}_k^i$ and $\tilde{\mathbf{x}}_k^i \in \tilde{\mathbf{X}}_k^i$ always hold for all $k \geq k^*$. $\diamond$

Proposition 3.1. Comparing (10) with (13), if $\mathbf{R}_{k^*}^i \times \tilde{\mathbf{X}}_{k^*}^i \subseteq \mathbf{Z}_{k^*}^i$, where $\times$ denotes the Cartesian product, then $\mathbf{R}_k^i \times \tilde{\mathbf{X}}_k^i \subseteq \mathbf{Z}_k^i$ always holds for all $k > k^*$.

Proof: Substituting the sets of u_k^{ref}, ω_k and η_k into (9), one can obtain (10), while (13) is obtained by only substituting the sets of ω_k and η_k into (11) and (12). Since (9) is equivalent to (11) and (12), (13) should be bounded by (10) after k^*, as long as the sets of the two set-based dynamics satisfy the condition in Proposition 3.1 at k^*. $\square$

3.2 Real-time Bounds for State Estimation Errors

Since the state estimation errors are unmeasurable, this paper aims to obtain their bounds by using available signals. According to (1b) and (2b), the output estimation error $\tilde{y}_k^j$ of the j-th observer is defined as

$$\tilde{y}_k^j = y_k - \hat{y}_k^j = C\tilde{x}_k^j + \eta_k. \quad (14)$$

Similarly, when the system is in the i-th mode, one defines the output estimation error vector as

$$\tilde{\mathbf{y}}_k^i = \left[(\tilde{y}_k^0)^T \ (\tilde{y}_k^1)^T \ \cdots \ (\tilde{y}_k^N)^T \right]^T, \quad (15)$$

where, according to (14), $\tilde{\mathbf{y}}_k^i$ is derived as

$$\tilde{\mathbf{y}}_k^i = C_{\tilde{\mathbf{x}}}\tilde{\mathbf{x}}_k^i + F_{\eta}\eta_k, \quad (16)$$

where $C_{\tilde{\mathbf{x}}} = \mathrm{diag}([\,C \ C \ \cdots \ C\,])$ and $F_{\eta} = [\,I \ I \ \cdots \ I\,]^T$.

According to (16) and considering the bound of η_k, at time instant k, one always has the relationship

$$C_{\tilde{\mathbf{x}}}\tilde{\mathbf{x}}_k^i \in \{\tilde{\mathbf{y}}_k^i\} \oplus (-F_{\eta}V). \quad (17)$$

By using (17), since the output estimation error $\tilde{\mathbf{y}}_k^i$ is available, the set of $\tilde{\mathbf{x}}_k^i$ can always be computed.

Remark 2. If $C_{\tilde{\mathbf{x}}}$ is invertible, the set of $\tilde{\mathbf{x}}_k^i$ can be directly computed with (17). If $C_{\tilde{\mathbf{x}}}$ is not invertible, the set of $\tilde{\mathbf{x}}_k^i$ can be obtained by intersecting all the strips determined by componentwise inequalities of (17) with a set of $\tilde{\mathbf{x}}_k^i$ determined by the physical constraints. $\diamond$

Remark 3. Although the set of $\tilde{\mathbf{x}}_k^i$ is obtained, considering the use of set-based propagation in this paper, a box of the set of $\tilde{\mathbf{x}}_k^i$ is more useful, which can be obtained and be written as $\tilde{\mathbf{X}}_k^i = [\underline{\mathbf{b}}_k^i, \overline{\mathbf{b}_k^i}]$, where $\underline{\mathbf{b}}_k^i$ and $\overline{\mathbf{b}_k^i}$ denotes the lower and upper bounds of the box. $\diamond$

3.3 Invariant Sets of Residuals

Theorem 3.1. [Kofman et al., 2007, Olaru et al., 2010]. Considering the system $x_{k+1} = A_{\circ}x_k + B_{\circ}\delta_k$ where $A_{\circ}$ is a Schur matrix and $\delta_k \in \Delta = \{\delta : |\delta - \delta^{\circ}| \leq \bar{\delta}\}$, and $A_{\circ} = V\Lambda V^{-1}$ as the Jordan decomposition, the set

$$\Phi(\theta) = \{x \in \mathbb{R}^n : |V^{-1}x| \leq (I - |\Lambda|)^{-1}|V^{-1}B_{\circ}|\bar{\delta} + \theta\} \oplus \xi^{\circ} \quad (18)$$

is *robust positively invariant* (RPI) and attractive for the system trajectories with θ any vector with positive components and $\xi^{\circ} = (I - A_{\circ})^{-1}B_{\circ}\delta^{\circ}$.

(1) For any θ, the set $\Phi(\theta)$ is (positively) invariant, that is, if $x_0 \in \Phi(\theta)$, then $x_k \in \Phi(\theta)$ for all $k \geq 0$.

(2) Given $\theta \in \mathbb{R}^n, \theta > 0$, and $x_0 \in \mathbb{R}^n$, there exists $k^* \geq 0$ such that $x_k \in \Phi(\theta)$ for all $k \geq k^*$. ▼

Remark 4. [Olaru et al., 2010]. Considering the same system in Theorem 3.1 and denoting X_0 as an RPI initial set of the system, each of the set iterations

$$X_{j+1} = A_{\circ}X_j \oplus B_{\circ}\Delta, \quad j \in \mathbb{N},$$

is an RPI approximation of the minimal RPI (mRPI) set of the system (X_j denotes the j-th element of the set sequence and $\mathbb{N}$ is the set of natural numbers). As j tends to infinity, the set sequence converges to the mRPI set. $\diamond$

Remark 5. For any initial set X_0, as j tends to infinity, the set sequence always converges to the mRPI set. The difference from Remark 4 is that the set X_j may not be a RPI approximation of the mRPI set. $\diamond$

According to Remark 5, one knows that, as k tends to infinity, (10) will converge to the mRPI set of $\mathbf{z}_k^i$. Thus, according to Proposition 3.1, the set iterations of (13) are contractive and bounded by the mRPI set of $\mathbf{z}_k^i$.

Moreover, since u_k^{ref}, ω_k and η_k are bounded, for the i-th mode, an RPI set, denoted as $\mathbf{Z}^i$, can be constructed to confine the corresponding $\mathbf{z}_k^i$. By definition, the mRPI is always contained in any RPI set. Thus, for the i-th mode, the corresponding tube generated by (13) will ultimately enter into $\mathbf{Z}^i$. Since $\mathbf{z}_k^i$ is composed of $\mathbf{r}_k^i$ and $\tilde{\mathbf{x}}_k^i$, the corresponding sets of $\mathbf{r}_k^i$ and $\tilde{\mathbf{x}}_k^i$ (denoted as $\mathbf{R}^i$ and $\tilde{\mathbf{X}}^i$, respectively) can be obtained by projecting $\mathbf{Z}^i$ to the spaces of $\mathbf{r}_k^i$ and $\tilde{\mathbf{x}}_k^i$, respectively.

4. FDI APPROACH

4.1 Fault Detection and Isolation

Once the i-th ($i \in \mathbb{I}_0 = \mathbb{I} \setminus \{0\}$) fault occurs, the residual vector [2] $\mathbf{r}_k$ will enter into and stay inside the set $\mathbf{R}^i$.

When the system is in the healthy functioning, if a sufficient amount of time has passed since the start of the system, $\mathbf{r}_k$ should always be inside $\mathbf{R}^0$. Thus, a fault is detected whenever a violation of

$$\mathbf{r}_k \in \mathbf{R}^0 \qquad (19)$$

is confirmed under the assumption of persistent faults. Otherwise, it is considered that the system is still healthy.

It is assumed a fault is detected at time instant k_d, $\mathbf{r}_{k_d}^f$ and $\tilde{\mathbf{y}}_{k_d}^f$ can be obtained, where f denotes a new but unknown mode. Thus, at time instant k_d, by (17), one can obtain

$$\tilde{\mathbf{X}}_{k_d}^f = [\underline{\mathbf{b}_{k_d}^f}, \overline{\mathbf{b}_{k_d}^f}], \qquad (20a)$$

$$\mathbf{R}_{k_d}^f = \mathbf{r}_{k_d}^f \oplus O\mathbf{B}^s, \ f \in \mathbb{I}_0. \qquad (20b)$$

Moreover, at time instant k_d, using $\tilde{\mathbf{X}}_{k_d}^f$ and $\mathbf{R}_{k_d}^f$ to initialize N set-based faulty dynamics described by (13), then all the residual tubes $\mathbb{T}^i$ ($i \in \mathbb{I}_0$) corresponding to the N faults are generated, each of which corresponds to a faulty mode. The i-th tube is denoted as

$$\mathbb{T}^i = \{\mathbf{R}_{k_d}^i, \mathbf{R}_{k_d+1}^i, \mathbf{R}_{k_d+2}^i, \dots \}.$$

According to Remark 1, it is known that at least one residual tube out of the N tubes $\mathbb{T}^i$ ($i \in \mathbb{I}_0$) can always bound $\mathbf{r}_k^f$ after time instant k_d. If one and only one residual tube can always bound $\mathbf{r}_k^f$, FI can be guaranteed by searching that tube, i.e., testing if

$$\mathbf{r}_k^f \in \mathbf{R}_k^i, \ i \in \mathbb{I}_0, \ k > k_d. \qquad (21)$$

Eventually, by real-time testing the inclusion (21) between $\mathbf{r}_k^f$ and the N faulty tubes, at a time instant k_i when there is one and only one tube that respects (21), it implies that the fault is isolated at this time instant and indicated by the index of that tube. The conditions to guarantee this fact will be detailed in Section 5.

4.2 Computation of Tubes

The FI key is to compute tubes. As per Section 3.2, at the FD time k_d, $\tilde{\mathbf{X}}_{k_d}^f$ and $\mathbf{R}_{k_d}^f$ indicated in Remark 3 and (20) should be constructed to generate tubes. Since a box can be expressed as a zonotope, the set $\tilde{\mathbf{X}}_k^f$ is rewritten as

$$\tilde{\mathbf{X}}_k^f = \tilde{\mathbf{x}}_k^{f,c} \oplus H_k^{f,\tilde{\mathbf{x}}} \mathbf{B}^{s_{\tilde{\mathbf{x}}}},$$

where $\tilde{\mathbf{x}}_k^{f,c}$ and $H_k^{f,\tilde{\mathbf{x}}}$ are the corresponding center and segment matrix, respectively.

Initializing (13) by using $\tilde{\mathbf{X}}_{k_d}^f$ and $\tilde{\mathbf{R}}_{k_d}^f$ at time instant k_d, one obtains the zonotopic form of residual tubes

---

[2] $\mathbf{r}_k$ is the general denotation of the residual vector while $\mathbf{r}_k^i$ denotes the residual vector under the i-th mode.

$$\mathbf{r}_{k+1}^{i,c} = A_r \mathbf{r}_k^{i,c} + B_r u_k^{\text{ref}} + E_{\tilde{\mathbf{x}}} \tilde{\mathbf{x}}_k^{i,c} + E_\eta \eta_c, \qquad (22a)$$

$$H_{k+1}^{i,r} = [A_r H_k^{i,r} \quad E_{\tilde{\mathbf{x}}} H_k^{i,\tilde{\mathbf{x}}} \quad E_\eta H_{\bar{\eta}}], \qquad (22b)$$

$$\tilde{\mathbf{x}}_{k+1}^{i,c} = A_{\tilde{\mathbf{x}}} \tilde{\mathbf{x}}_k^{i,c} + B_{\tilde{\mathbf{x}}}^i u_k^{\text{ref}} + E_r^i r_k^0 + E_\omega^{\tilde{\mathbf{x}}} \omega_c + E_\eta \eta_c, \qquad (22c)$$

$$H_{k+1}^{i,\tilde{\mathbf{x}}} = [A_{\tilde{\mathbf{x}}} H_k^{i,\tilde{\mathbf{x}}} \quad E_\omega^{\tilde{\mathbf{x}}} H_{\bar{\omega}} \quad E_\eta H_{\bar{\eta}}], \qquad (22d)$$

where $\mathbf{r}_k^{i,c}$ and $H_k^{i,r}$ denotes the center and segment matrix of $\mathbf{R}_k^i$, respectively.

Using (22), N residual tubes $\mathbb{T}_k^i$ ($i \in \mathbb{I}_0$) corresponding to the N considered faults can be obtained. Additionally, an FDI algorithm is used to summarize the proposed FDI techniques in Section 4.1, where length($\cdot$) denotes the number of elements in a set.

Algorithm 1 FDI algorithm

Require: Fault index set $\mathbb{I}_0$;
Ensure: Faulty index f;
  1: Initialize a bank of observers (2) and $f = 0$;
  2: At time instant k: $\mathbf{r}_k \in \mathbf{R}^0$ and fault $\leftarrow$ FALSE;
  3: **while** fault $\neq$ TRUE **do**
  4:   $k \leftarrow k + 1$;
  5:   Compute $\mathbf{r}_k$;
  6:   **if** $\mathbf{r}_k \notin \mathbf{R}^0$ **then**
  7:     fault $\leftarrow$ TRUE, $f \neq 0$;
  8:     Obtain $\mathbf{r}_{k_d}^f$ and $\tilde{\mathbf{y}}_{k_d}^f$ to construct $\mathbf{R}_{k_d}^f$ and $\tilde{\mathbf{X}}_{k_d}^f$;
  9:     Initialize (13) to generate N tubes $\mathbb{T}^i$ ($i \in \mathbb{I}_0$);
 10:   **end if**
 11: **end while**
 12: **while** length($\mathbb{I}_0$)$\neq 1$ **do**
 13:   **for** $i \in \mathbb{I}_0$ **do**
 14:     **if** $\mathbf{r}_k^f \notin \mathbf{R}_k^i$ **then**
 15:       Remove i from $\mathbb{I}_0$;
 16:     **end if**
 17:   **end for**
 18:   $k \leftarrow k + 1$;
 19: **end while**
 20: $f \leftarrow \mathbb{I}_0$ (finally only one element inside $\mathbb{I}_0$);
 21: **return** f;

---

5. FDI CONDITIONS

5.1 Guaranteed FDI Conditions

To assure the considered faults are detectable and isolable by the proposed technique, one establishes FDI conditions based on the residual invariant sets.

According to Remark 5 and Proposition 4, once a fault occurs, after initialization, the tube $\mathbb{T}^i$ ($i \in \mathbb{I}_0$) will enter into the set $\mathbf{R}^i$ in accordance with the fault.

To guarantee FDI at transient state, one should assure that, after initialization, there is one and only one tube that can always bound $\mathbf{r}_k^i$, i.e., the sets $\mathbf{R}^i$ ($i \in \mathbb{I}$) should be separate from each other. For this objective, the FDI conditions are established as follows.

Theorem 5.1. For any two modes i_1 and i_2 out of the $N+1$ modes, as long as

$$\mathbf{R}^{i_1} \cap \mathbf{R}^{i_2} = \emptyset, \ i_1 \neq i_2 \text{ and } i_1, i_2 \in \mathbb{I} \qquad (23)$$

holds, it is guaranteed that all the considered faults are detectable and then isolable during the transition.

Proof : If (23) is satisfied, the residual $\mathbf{r}_k$ must leave the healthy invariant set after fault occurrence and one and only one tube can always contain the residual $\mathbf{r}_k$ during the transition, which guarantees FD and FI. □

5.2 Comparison of FDI Conditions

In the i-th mode, the RPI set of r_k^j is obtained by the corresponding projection of $\mathbf{R}^i$ and is denoted as $R^{i,j}$. As mentioned in Section 1, the existing works are based on the residual corresponding to the observer matching the current mode, i.e., only the residual r_k^0 corresponding to the nominal observer is used for FDI and the FDI conditions are based on the complete separation of all after-fault invariant sets of r_k^0 under all modes, i.e.,

$$R^{i_1,0} \cap R^{i_2,0} = \varnothing, \ i_1, i_2 \in \mathbb{I}. \qquad (24)$$

Comparatively, instead of using the system information only from one observer, the proposed approach utilizes all the process information from all the observers for FDI (see (23)). Considering the structure of $\mathbf{r}_k^i$, it is known that the set $\mathbf{R}^i$ is equivalent to the composition of $N+1$ sets corresponding to the residuals of the $N+1$ observers, i.e., $\mathbf{R}^i = R^{i,0} \times R^{i,1} \times \cdots \times R^{i,N}$. Thus, $R^{i,j}$ is the component of $\mathbf{R}^i$ corresponding to r_k^j.

The condition (23) implies that the separation between $\mathbf{R}^{i_1}$ and $\mathbf{R}^{i_2}$ can be guaranteed as long as there exists one component of $\mathbf{R}^{i_1}$ that is disjoint from that of $\mathbf{R}^{i_2}$, i.e., $\exists i_1, i_2 \in \mathbb{I}$ such that $R^{i_1,j} \cap R^{i_2,j} = \varnothing$, where j could not only be 0 but also any other index inside $\mathbb{I}$. This means the FDI condition (24) is only a particular case of the FDI condition (23), which implies the reduced conservativeness and enhanced fault sensitiveness of this proposed FDI approach.

6. NUMERICAL EXAMPLE

An example modeled as (1) is presented. Two actuator faults, F_1 and F_2, are considered and the parameters are

- system matrices:
$$A = \begin{bmatrix} 0.6 & 0.05 \\ 0.1 & 0.7 \end{bmatrix}, B = \begin{bmatrix} 0.5 & 0.1 \\ 0.2 & -0.3 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

- disturbances: $\bar{w} = [0.1\ 0.1]^T,\ w^c = [0\ 0]^T,$

- noises: $\bar{\eta} = [0.01\ 0.01]^T, \eta^c = [0\ 0]^T,$

- observer gains: $L_0 = L_1 = L_2 = \begin{bmatrix} 1 & 0.05 \\ 0.1 & 0.2 \end{bmatrix},$

- feedback gain: $K = \begin{bmatrix} 0.2353 & -0.1765 \\ 0.1471 & -0.2353 \end{bmatrix},$

- fault magnitudes: $F_1 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, F_2 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},$

- reference input (sinusoidal signal) set:
$$U_{\text{ref}} = \begin{bmatrix} 5 \\ 5 \end{bmatrix} \oplus \begin{bmatrix} 0.3 & 0 \\ 0 & 0.3 \end{bmatrix} \mathbf{B}^2,$$

- initial conditions:
$$x_0 = [0\ 0]^T, \hat{x}_0 = \hat{x}_1 = \hat{x}_2 = [0\ 0]^T,$$
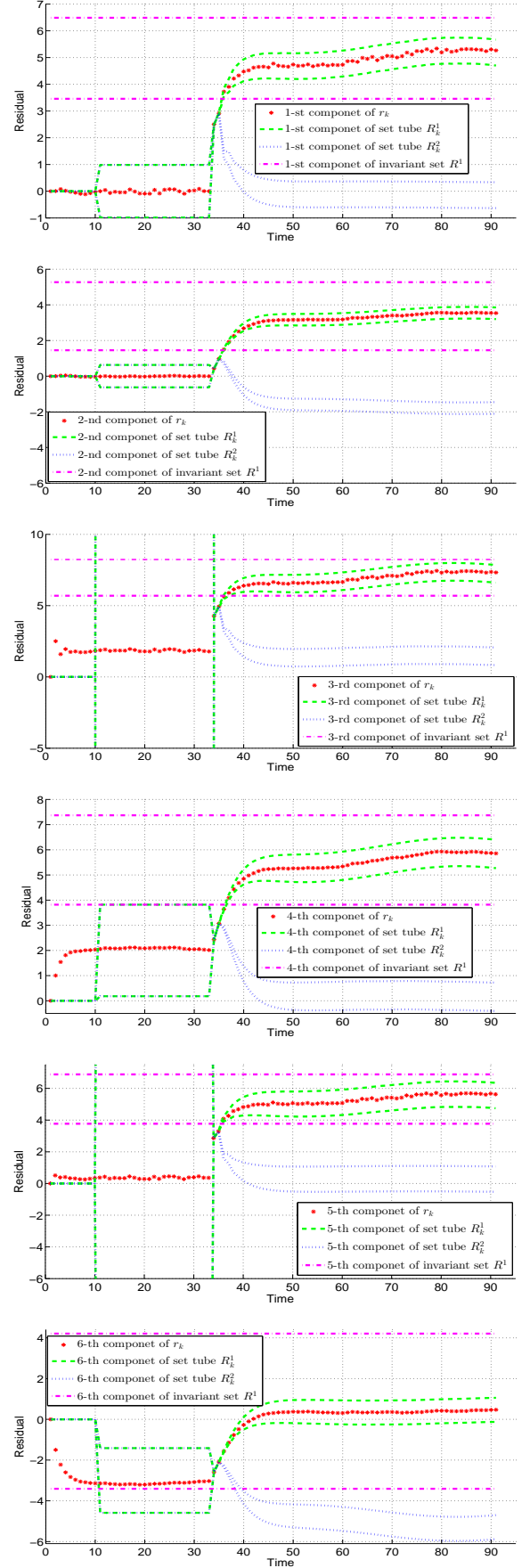

Fig. 1. FDI of the fault 1

- sampling time: $T = 0.1s$.

The RPI sets of the residual under three different modes are computed. For simplicity, they are written as boxes:

$$\mathbf{R}^0 = ([-0.9844, 0.9844], [-0.6294, 0.6294], [-302.4385, 306.01],$$
$$[0.1809, 3.8191], [-41.0474, 41.7616], [-4.588, -1.412]),$$

$$\mathbf{R}^1 = ([3.45780, 6.48780], [1.45490, 5.2730], [5.69540, 8.23340],$$
$$[3.8186, 7.3705], [3.7696, 6.8816], [-3.4091, 4.2094]),$$

$$\mathbf{R}^2 = ([-1.2622, 0.9716], [-2.8069, -0.9243], [-2.8646, 6.3562],$$
$$[-3.4321, 3.9370], [-0.8232, 1.3066], [-6.1596, -4.0726]),$$

which shows that $\mathbf{R}^0$, $\mathbf{R}^1$ and $\mathbf{R}^2$ are separate from each other (the satisfaction of the FDI conditions (23)).

Thus, the proposed approach can be used to detect and isolate the faults. In this example, the time span of simulation for both faults is 90 time instants. The time instants from 1 to 10 are used to initialize the system so that the residuals stay inside the healthy invariant sets, those from 11 to 30 represent the healthy functioning, and those from 31 to 91 represent the faulty functioning.

In the simulation, both faults occur at time instant 31. However, because of space limits of this paper, only the results of the fault 1 are presented. In Figure 1, the first residual component leaves its invariant set at time instant 34, which means the fault 1 is detected at that time. Except the first component, all the other components of the residual vector still stay inside their invariant sets. Besides, all the residual components indicate the fault 1 is isolated at time instant 36. Note that, in Figure 1, the constant bounds from 11 to 30 labelled with blue-green mixed color denote the healthy invariant sets of residuals.

Since the tubes are computed by zonotopes and the residual zonotopes are reordered by Property A.3 in the Appendix to reduce the order of the zonotopes at each time instant, the tubes cannot be accurately computed and always include some approximate errors. But the computation of invariant sets (i.e., RPI approximations of the mRPI set) is generally accurate (generally, the mRPI set cannot be computed). Thus, if the accumulation of errors in zonotope overapproximation is too big with respect to the corresponding ideal tubes, the generated tubes may fail to converge into their corresponding invariant sets.

Actually, the FI task of this approach can be divided into two different and independent phases. The first phase is based on the tubes for the transient-state FI while the second phase is based on invariant set separation for the steady-state FI. As long as the FDI conditions in Theorem 5.1 are satisfied, the fault can be isolated at latest when the system enters into the steady state, even though the first phase of the proposed FI approach fails to isolate the fault at transient state.

Thus, in the case that the tubes do not accurately converge into their corresponding invariant sets because of the accumulation errors, tube-based transient-state FI is perhaps affected. But the invariant set-based steady-state FI can still work normally (i.e., the whole availability of the proposed FDI approach is not affected). Additionally, since this approach uses the tubes, when designing the observers and controllers, the wrapping effect should be avoided as far as possible [Neumaier, 1993].

7. CONCLUSIONS

This paper proposes an actuator FDI strategy by using invariant sets and tubes. The first advantage of this technique is that it uses all the available system-operating information to reduce the conservativeness of FDI conditions and isolate the faults during the transition. The other advantage is that if the FDI conditions cannot be fully satisfied, the approach can still be used. The difference consists in that perhaps the FI result is not unique but it can reliably isolate the real fault, which implies the extension of the effectiveness of the FDI framework.

APPENDIX

Definition A.1. The Minkowski sum of two sets A and B is defined by $A \oplus B = \{a + b : a \in A, b \in B\}$. $\qquad \triangledown$

Property A.1. Given zonotopes $X_1 = g_1 \oplus G_1 \mathbf{B}^{r_1} \subset \mathbb{R}^n$ and $X_2 = g_2 \oplus G_2 \mathbf{B}^{r_2} \subset \mathbb{R}^n$, the *Minkowski sum* of them is $X_1 \oplus X_2 = \{g_1 + g_2\} \oplus [G_1 \quad G_2] \mathbf{B}^{r_1+r_2}$. $\qquad \blacklozenge$

Property A.2. Given a zonotope $X = g \oplus G \mathbf{B}^r \subset \mathbb{R}^n$ and a compatible matrix K, $KX = Kg \oplus KG \mathbf{B}^r$. $\qquad \blacklozenge$

Property A.3. Given $X = g \oplus G \mathbf{B}^r \subset \mathbb{R}^n$ and an integer s $(n < s < r)$, denote by $\hat{G}$ the matrix resulting from the recording of the columns of G in decreasing Euclidean norm. $X \subseteq g \oplus [\hat{G}_T \quad Q] \mathbf{B}^s$ where $\hat{G}_T$ is obtained from the first $s - n$ columns of matrix $\hat{G}$ and $Q \in \mathbb{R}^{n \times n}$ is a diagonal matrix whose elements are computed by $Q_{ii} = \sum_{j=s-n+1}^{r} | \hat{G}_{ij} |, i = 1, \dots, n$. $\qquad \blacklozenge$

ACKNOWLEDGMENT

REFERENCES

M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki. *Diagnosis and Fault-Tolerant Control*. Springer-Verlag, Berlin, Germany, 2006.

E. Kofman, H. Haimovich, and M.M. Seron. A systematic method to obtain ultimate bounds for perturbed systems. *International Journal of Control*, 80(2):167–178, 2007.

Arnold Neumaier. The wrapping effect, ellipsoid arithmetic, stability and confidence regions. In *Validation Numerics*, Computing Supplementum, pages 175–190. Springer, 1993.

C. Ocampo-Martinez, J.A. De Doná, and M.M Seron. Actuator fault-tolerant control based on set separation. *International Journal of Adaptive Control and Signal Processing*, 24(12):1070– 1090, 2010.

S. Olaru, J.A. De Doná, M.M. Seron, and F. Stoican. Positive invariant sets for fault tolerant multisensor control schemes. *International Journal of Control*, 83 (12):2622–2640, 2010.

M.M. Seron and J.A. De Doná. Actuator fault tolerant multi-controller scheme using set separation based diagnosis. *International Journal of Control*, 83(11):2328–2339, 2010.