Sensor-fault Tolerance using Robust MPC with Set-based State Estimation and Active Fault Isolation

Feng Xu, Sorin Olaru, *Senior Member IEEE,* Vicenç Puig, Carlos Ocampo-Martinez, *Senior Member IEEE* and Silviu-Iulian Niculescu

***Abstract*— In this paper, a sensor fault-tolerant control (FTC) scheme using robust model predictive control (MPC) and set-theoretic fault detection and isolation (FDI) is proposed. The MPC controller is used to both robustly control the plant and actively guarantee fault isolation (FI). In this scheme, fault detection (FD) is passive by interval observers, while fault isolation (FI) is active by MPC. The advantage of the proposed approach consists in using MPC to actively decouple the effect of sensor faults on the outputs such that one output component only corresponds to one sensor fault in terms of FI, which can utilize the feature of sensor faults for FI. A numerical example is used to illustrate the effectiveness of the proposed scheme.**

I. Introduction

The control systems consist of a series of different components that play different roles in global operation. Among those components, the sensors are commonly used, which are tools to acquire the real-time system-operating information. Thus, it is important to monitor the situation of sensors and tolerate the effect of sensor faults in order to provide the control systems with safety properties. In the literature, there exist two types of FTC strategies, i.e., passive FTC (PFTC) and active FTC (AFTC) [1]. Generally, PFTC, based on controller robustness, has restrictive FTC ability in terms of performance. AFTC uses a so-called FDI module to obtain fault information and then faults can be tolerated with the fault information.

In the proposed scheme, MPC is used as the control strategy, whose advantage consists in handling system constraints [2], [4]. Besides, for FDI robustness, set-based FDI is used in the scheme. In [8], a multi-sensor fault-tolerant MPC (FTMPC) scheme based invariant sets is proposed, where FDI is passively implemented. But, generally, passive fault diagnosis is more conservative. The objective of this paper is to propose a new sensor FTMPC scheme, which can deal with system constraints and tolerate sensor faults with less conservative FI conditions. The proposed scheme has three contributions. First, it proposes a novel and simple active FI technique based on MPC, which can reduce FI conservatism. Second, it proposes a robust state estimation approach for the MPC controller with feasibility guarantee. Third, it can detect, isolate and tolerate unknown but bounded sensor faults with no need of physical redundancy of sensors.

The remainder of the paper is as follows. Section II introduces the scheme. Section III presents the FDI strategy. Section IV proposes the FTC strategy. In Section V, a numerical example illustrates the effectiveness of the proposed scheme. In Section VI, some conclusions are draw.

In this paper, the inequalities are understood element-wise, the bold matrices denote interval matrices, $\text{mid}(\cdot)$ obtains the center of interval matrices, $\text{diag}[\cdot]$ denotes the diagonal matrix, $\text{center}(\cdot)$ denotes the center of a centered set, O and I denote the zero and identity matrices with suitable dimensions, respectively, $\mathbb{B}^r$ is a box composed of r unitary intervals and $\oplus$ denotes the Minkowski sum.

II. Problem Formulation

A. Plant Model

The linear discrete time-invariant plant is modelled as

$$x_{k+1} = Ax_k + Bu_k + \omega_k, \tag{1a}$$

$$y_k = \mathbf{G}Cx_k + \eta_k, \tag{1b}$$

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, $x_k \in \mathbb{R}^n$, $u_k \in \mathbb{R}^p$ and $y_k \in \mathbb{R}^q$ are state, input and output vectors at time instant k, respectively, and ω_k and η_k model unknown disturbances and noises, respectively.

In (1), $\mathbf{G}$ takes a value $\mathbf{G}_i$ ($i \in \mathbb{I} = \{0, 1, ..., q\}$) to model the i-th sensor mode, where $\mathbf{G}_0$ is the identity matrix denoting the healthy mode and $\mathbf{G}_i$ ($i \neq 0$) is a diagonal interval matrix modelling the i-th sensor fault with

$$\mathbf{G}_i = \text{diag}[1 \ \ldots \ \overset{i}{\underset{\downarrow}{f_i}} \ \ldots \ 1],$$

where the fault-modelling interval f_i satisfies $f_i \subseteq [0,\ 1)$. Additionally, a diagonal interval matrix to describe all the considered sensor faults is defined as

$$\mathbf{G}_f = \text{diag}[f_1 \ \ldots \ f_i \ \ldots \ f_q],$$

where each diagonal element of $\mathbf{G}_f$ corresponds to the considered magnitude interval of one sensor fault. Besides, the system state and input constraints are given as

$$X = \{x \in \mathbb{R}^n : \ |x - x^c| \leq \bar{x}, x^c \in \mathbb{R}^n, \bar{x} \in \mathbb{R}^n\}, \tag{2a}$$

$$U = \{u \in \mathbb{R}^p : \ |u - u^c| \leq \bar{u}, u^c \in \mathbb{R}^p, \bar{u} \in \mathbb{R}^p\}, \tag{2b}$$

respectively, where the vectors x^c, u^c, $\bar{x}$ and $\bar{u}$ are constant.

F. Xu, V. Puig and C. Ocampo-Martinez are with the Institut de Robòtica i Informàtica Industrial (CSIC-UPC), Technical University of Catalonia (UPC), Llorens i Artigas, 4-6, 08028 Barcelona, Spain, {fxu, vpuig, cocampo}@iri.upc.edu.

S. Olaru is with the E3S (SUPELEC Systems Sciences), Automatic Control Department, Gif sur Yvette, France, sorin.olaru@supelec.fr.

S. Niculescu is with L2S, CNRS-Supelec, Gif sur Yvette, France, silviu.niculescu@lss.supelec.fr.

This work has been partially supported by the EU project i-Sense (FP7-ICT-2009-6-270428), China Scholarship Council, CNRS-Supélec and Automatic Control Department, Supélec, France.

Assumption 2.1: ω_k and η_k are bounded by known sets

$$W = \{\omega \in \mathbb{R}^n : |\omega - \omega^c| \leq \bar{\omega}, \omega^c \in \mathbb{R}^n, \bar{\omega} \in \mathbb{R}^n\}, \quad (3a)$$

$$V = \{\eta \in \mathbb{R}^q : |\eta - \eta^c| \leq \bar{\eta}, \eta^c \in \mathbb{R}^q, \bar{\eta} \in \mathbb{R}^q\}, \quad (3b)$$

respectively, where the vectors ω^c, η^c, $\bar{\omega}$ and $\bar{\eta}$ are constant. ■

Assumption 2.2: The matrix A is a Schur matrix and the pairs $(A, \mathbf{G}_i C)$ are detectable for all $i \in \mathbb{I}$. ■

Remark 2.1: For brevity, only single fault is considered in the paper. But, theoretically, the proposed approach can also be extended for multiple faults with $\mathbf{G}$ modelling multiple faults important/critical to system performance/safety. ◊

Assumption 2.3: The considered faults should persist sufficiently long time such that the FDI module has enough responsive time to cope with them. ■

B. Set-point Tracking

In the i-th mode, the control objective is to track an output set-point, i.e., in the absence of uncertainties and/or faults,

$$\lim_{k\to\infty} (y_k - y_i^*) \to 0,$$

where y_i^* denotes the output set-point of the i-th mode.

Remark 2.2: Sensor faults imply the loss of available system information. Thus, there perhaps exist situations, where one has to degrade the expected performance. ◊

In the proposed scheme, the tracking references for the i-th sensor mode are generated by the i-th nominal model

$$x_{k+1}^{ref} = Ax_k^{ref} + Bu_k^{ref}, \quad (4a)$$

$$y_k^{ref} = \text{mid}(\mathbf{G}_i) C x_k^{ref}, \quad (4b)$$

where u_k^{ref}, x_k^{ref} and y_k^{ref} are the reference input, state and output at time instant k. Using (4), at steady state, one has

$$\begin{bmatrix} A - I & B \\ \text{mid}(\mathbf{G}_i) C & O \end{bmatrix} \begin{bmatrix} x_i^* \\ u_i^* \end{bmatrix} = \begin{bmatrix} O \\ y_i^* \end{bmatrix}. \quad (5)$$

where (x_i^*,u_i^*) is the state-input set-point pair corresponding to y_i^*. But, the solution of (5) may not be unique. Thus, for $q+1$ modes, $q+1$ set-point pairs should be obtained.

Assumption 2.4: Under the constraints (2), the equation (5) is solvable for all $i \in \mathbb{I}$. ■

Remark 2.3: if needed, ω^c and η^c can be added into (4).◊

III. Fault Detection and Isolation

A. Fault Detection

A bank of interval observers are designed to monitor the plant, each of which matches one mode. The j-th ($j \in \mathbb{I}$) interval observer matching the j-th mode is designed as

$$\hat{X}_{k+1}^j = (A - L_j \mathbf{G}_j C)\hat{X}_k^j \oplus \{Bu_k\} \oplus \{L_j y_k\} \oplus (-L_j)V \oplus W, \quad (6a)$$

$$\hat{Y}_k^j = \mathbf{G}_j C \hat{X}_k^j \oplus V, \quad (6b)$$

where $\hat{X}_k^j$ and $\hat{Y}_k^j$ are the estimated state and output sets, and L_j is the observer gain that assures $A - L_j \mathbf{G}_j C$ is a Schur matrix.

Assumption 3.1: The initial state x_0 belongs to an initial set $\hat{X}_0$ for all interval observers. ■

As defined in (3), W and V can be rewritten as zonotopes[1]. By defining $\hat{X}_0$ as a zonotope, $\hat{X}_{k+1}^j$ and $\hat{Y}_k^j$ are zonotopes as well. Using zonotope operations, interval observers (6) can be propagated on-line with preserving zonotopic structure and guaranteeing containment. If the j-th interval observer matches the current mode, at steady state, one has

$$x_k \in \hat{X}_k^j \text{ and } y_k \in \hat{Y}_k^j.$$

In the i-th mode, $\mathbf{G}$ takes the value $\mathbf{G}_i$ ($i \in \mathbb{I}$) and the i-th interval observer monitors the plant. To detect faults, the residual[2] (in terms of zonotopes) is defined as

$$R_k^{ii} = y_k - \hat{Y}_k^i. \quad (8)$$

Remark 3.1: Although a bank of interval observers operate concomitantly, only residual zonotopes of the interval observer matching the current mode is used for FD. ◊

Thus, when the system is in the i-th mode, the FD task is implemented by testing whether or not

$$\mathbf{0} \in R_k^{ii} \quad (9)$$

is violated in real time. If a violation is detected, it means that the system has become faulty[3]. Otherwise, it is considered that the system is still in the i-th mode. The satisfaction of (9) does not always imply the system is healthy because the FD strategy cannot be sensitive to all faults. For the faults undetectable by (9), only potential PFTC ability of the proposed scheme can tolerate them to some extent.

B. Fault Isolation

1) Fault Isolation Conditions: To explain the proposed FI approach, it is assumed that the inputs are bounded by a set

$$U_f = \{u \in \mathbb{R}^p : \left|u - u_f^c\right| \leq \bar{u}_f, u_f^c \in \mathbb{R}^p, \bar{u}_f \in \mathbb{R}^p\},$$

where U_f satisfies the input constraint of the plant. i.e.,

$$U_f \subseteq U. \quad (10)$$

Additionally, the output equation (1a) can be rewritten as

$$x_{k+1} = Ax_k + \begin{bmatrix} B & I \end{bmatrix} \begin{bmatrix} u_k \\ \omega_k \end{bmatrix}. \quad (11)$$

By considering $u_k \in U_f$ and $\omega_k \in W$, a *robust positively invariant* (RPI) set of (11) can be computed (see [3], [5], [6] for the notion of RPI sets and constructive algorithms), which is denoted as X_f centered at

$$x_f^c = (I - A)^{-1}(Bu_f^c + \omega^c). \quad (12)$$

Furthermore, according to (1b), in the i-th mode, the corresponding output set can be obtained as

$$Y_f^i = \mathbf{G}_i C X_f \oplus V,$$

[1]Please see [7] for the notion of zonotopes and all relevant properties of zonotopes used to implement interval observers in this paper.

[2]For analysis, R_k^{ii} is used to denote residual zonotopes of the i-th interval observer in the i-th mode at time instant k. But, realistically, one should only use R_k^i to denote residual zonotopes from the i-th interval.

[3]In this paper, "become faulty" generally denotes mode switching including fault occurrence and system recovery.

where Y_f^i is centered at $y_f^{c,i} = \text{mid}(\mathbf{G}_i)Cx_f^c + \eta^c$. If $\mathbf{G}_i$ takes the value $\mathbf{G}_0$, the corresponding healthy output set is

$$Y_f^0 = CX_f \oplus V,$$

where Y_f^0 is centered at $y_f^{c,0} = Cx_f^c + \eta^c$. The output set has q components, each of which is an interval that can be obtained by projecting the output set towards the corresponding dimension. In terms of $u_k \in U_f$, only the i-th component of Y_f^i is different from that of Y_f^0 because of the effect of the i-th fault, while all the other components are the same. Furthermore, in contrast to Y_f^0, one defines a set

$$Y_f = \mathbf{G}_f CX_f \oplus V,$$

where Y_f is centered at $y_f^c = \text{mid}(\mathbf{G}_f)Cx_f^c + \eta^c$. By comparing Y_f^0 and Y_f^i with Y_f, one knows:

- All the interval components of Y_f^0 are different from those of Y_f, respectively.
- Only the i-th interval component of Y_f^i ($i \neq 0$) is the same with that of Y_f, while all the others are different.

For brevity, the i-th interval components of Y_f^0, Y_f^i and Y_f are denoted as $Y_f^0(i)$, $Y_f^i(i)$ and $Y_f(i)$, which are centered at $y_f^{c,0}(i)$, $y_f^{c,i}(i)$ and $y_f^c(i)$ (the i-th components of $y_f^{c,0}$, $y_f^{c,i}$ and y_f^c), respectively.

Proposition 3.1: For the plant (1) under the constraints (2), if there exists a set U_f that satisfies (10) such that

$$Y_f^0(i) \cap Y_f(i) = \emptyset, \text{ for all } i \in \mathbb{I} \setminus \{0\}, \tag{13}$$

all the considered sensor modes are isolable after detection.

Proof : If the inputs are bounded by U_f, because of the separation of the i-th interval component, i.e, $Y_f^0(i) \cap Y_f(i) = \emptyset$, after the i-th fault occurs, the i-th output component finally enters into the i-th interval of Y_f instead of Y_f^0, while all the other output components enter into the corresponding components of Y_f^0 instead of Y_f, respectively, which indicates the i-th fault. Thus, if all the interval components of Y_f^0 and Y_f are separate from each other, it implies that all the considered sensor modes are isolable after their detection.□

Assumption 3.2: There exists a set $U_f \subseteq U$ such that all the considered sensor faults satisfy (13). ■

2) Fault Isolation Strategy: If a sensor fault is detected at time instant k_d, the state is still inside X_M (the *maximal robust control invariant* (MRCI) set of (1a) under the constraints (2)) at this time instant because sensor faults do not affect the system dynamics, i.e.,

$$x_{k_d} \in X_M, \tag{14}$$

where X_M is the terminal state constraint set of the MPC controller in the proposed scheme.

At time instant k_d, the proposed FI approach switches the input constraint of the MPC controller from U to U_f to start active FI. After constraint switching, if the MPC controller is still feasible, the generated control action satisfies

$$u_{k_d} \in U_f. \tag{15}$$

To isolate the fault during the transition induced by faults, at time instant k_d, one initializes a set-based dynamics

$$X_{k+1} = AX_k \oplus Bu_k \oplus W, \tag{16a}$$
$$Y_k = \mathbf{G}_f CX_k \oplus V, \tag{16b}$$

with $X_{k_d} = X_M$ and $u_k \in U_f$ ($k \geq k_d$). Afterwards, the state and output set sequences can be generated by (16). Moreover, by using $\check{X}_{k_d} = X_M$ at time instant k_d to initialize the other set-based dynamics

$$\check{X}_{k+1} = A\check{X}_k \oplus BU_f \oplus W, \tag{17a}$$
$$\check{Y}_k = \mathbf{G}_f C\check{X}_k \oplus V, \tag{17b}$$

the other state and output set sequences can be obtained.

As per [5], the state set sequence generated by (17a) will converge to the *minimal robust positively invariant* (mRPI) set of system states with respect to $u_k \in U_f$, enter into and stay inside X_f, and the output set sequence generated by (17b) will enter into and stay inside Y_f.

Proposition 3.2: At time instant k_d, by using X_M to initialize (16) and (17), for all $k \geq k_d$, $X_k \subseteq \check{X}_k$ and $Y_k \subseteq \check{Y}_k$ will always hold. □

Proposition 3.3: Given the plant (1), the state and output set sequences generated by (16), starting from time instant k_d, $x_k \in X_k$ can hold for all $k \geq k_d$. If the plant is healthy, no components of y_k and Y_k can persistently satisfy $y_k(i) \in Y_k(i)$ ($i \in \mathbb{I} \setminus \{0\}$) for all $k \geq k_d$, while if the i-th fault occurs, the i-th components of y_k and Y_k can persistently satisfy $y_k(i) \in Y_k(i)$ for all $k \geq k_d$ but all the other components of y_k and Y_k cannot.

Proof : First, because of (14), (15) and $u_k \in U_f$ for all $k > k_d$, comparing (1) and (16), $x_k \in X_k$ will hold for all $k \geq k_d$. Second, under Proposition 3.2, comparing (17) with (16), X_k and Y_k finally enter into X_f and Y_f and stay inside, respectively. Considering Y_f^0, Y_f^i and Y_f, for the i-th mode, i.e., $\mathbf{G}$ in (1b) takes a value inside $\mathbf{G}_i$ ($i \neq 0$), under Proposition 3.1, starting from time instant k_d, only $y_k(i) \in Y_k(i)$ will hold for all $k \geq k_d$ with the initialization $X_{k_d} = X_M$, while all the other components of y_k do not have the same conclusion. For the healthy mode, since all the components of Y_f^0 are separate from the corresponding components of Y_f, no components of y_k can be contained by the corresponding interval of Y_k for all $k \geq k_d$. □

Thus, under Proposition 3.1, 3.3 and Assumption 3.2, if a considered sensor fault is detected, by using the output set sequence generated by (16), the fault can be isolated by real-time testing whether or not

$$y_k(i) \in Y_k(i),\ k \geq k_d \tag{18}$$

is violated for all $i \in \mathbb{I} \setminus \{0\}$. With the real-time testing of (18) for all the components, one has the FI conclusions:

- If the plant recovers to the health from a faulty mode, for $k \geq k_d$, by testing (18), at a time instant, if all the output components violate (18), it implies that the healthy mode is isolated at this time instant.
- If the plant changes into another fault from a faulty mode or the healthy mode, only the output component

corresponding to the current mode can always respect (18) while all the others will finally diverge from their corresponding interval components of Y_k, respectively. Thus, the proposed FI approach consists in searching this unique component that indicates the fault and the corresponding time instant indicates the FI time.

IV. Fault-tolerant Control

A. Robust MPC Controller

In this proposed scheme, the robust MPC controller is implemented by using min-max MPC. In the steady-state operation of the i-th mode, the i-th state-input set-point pair and the i-th interval observer are used and the corresponding robust MPC controller is designed as

$$\begin{aligned} J_k = \min_{\mathbf{u}} \max_{\mathbf{w}} & \sum_{j=0}^{N-1} \|(x_{k+j|k} - x_i^*)\|_Q^2 + \|(u_{k+j|k} - u_i^*)\|_R^2 \\ & + \|(x_{k+N|k} - x_i^*)\|_P^2 \\ \text{subject to} \quad & \left.\begin{array}{r} x_{k+j|k} \in X, \\ u_{k+j|k} \in U, \\ x_{k+N|k} \in X_M, \\ x_{k|k} = \hat{x}_k, \end{array}\right\} \forall \omega_{k+j|k} \in W, \end{aligned} \tag{19}$$

where N is the prediction horizon, $\hat{x}_k$ is the system state estimation, $\mathbf{u} = [u_{k|k}, u_{k+1|k}, \cdots, u_{k+N-1|k}]$, Q, R and P are positive-definite weighting matrices, $\mathbf{w} = [\omega_{k|k}, \omega_{k+1|k}, \cdots, \omega_{k+N-1|k}]$ and the internal model of the MPC controller is given as

$$x_{k+j+1|k} = Ax_{k+j|k} + Bu_{k+j|k} + \omega_{k+j|k}.$$

In the i-th mode, if no fault is detected, the MPC controller (19) is used to robustly control the system to track the i-th output set-point y_i^*. If a fault is detected, at the FD time, active FI is started by switching the input and terminal state constraints of (19) from U and X_M to U_f and X_{M_f} (X_{M_f} is the MRCI set of (1a) under $x_k \in X$ and $u_k \in U_f$), respectively. By using active FI, the fault can be isolated and the controller can be reconfigured with the state-input set-point pair and interval observer corresponding to the new mode. Simultaneously, the input and terminal state constraints of the MPC controller must be switched back to U and X_M in the operation of the new mode, respectively.

B. Robust State Estimation

Under the constraints (2), one can compute the MRCI set X_M for the dynamics (1a). Since X_M is used as the terminal state constraint of the MPC controller (19), ideally, if the initial state is inside X_M and the real states are available for the MPC controller updating, the states can always be confined inside X_M and the MPC controller can be always feasible (see [4] for min-max MPC). Unfortunately, it is impossible to obtain the real states. Instead, one has to estimate the states for the MPC controller.

1) State Estimation: For feasibility and stability of the MPC controller with state estimation, one still uses X_M as the terminal state constraint in the steady-state operation.

Remark 4.1: In the steady-state operation, as long as the MPC controller (19) is always updated by a point inside X_M at each time instant, i.e., $\hat{x}_k \in X_M$, it can keep feasible such that the generated control actions always satisfy $u_k \in U$. $\Diamond$

For constraint satisfaction during the transition induced by faults, one makes the following assumption.

Assumption 4.1: The mRPI set (denoted as X_m) corresponding to $u_k \in U$ and $\omega_k \in W$ for the dynamics (11) is contained in the state constraint set X. ■

Assumption 4.2: There exists $\alpha \geq 1$ such that the initial state x_0 of (1a) satisfies $x_0 \in \bar{X} = \alpha X_m$ and $\bar{X} \subset X_M$. ■

Under Assumption 4.1 and 4.2, $\bar{X}$ is an RPI set corresponding to $u_k \in U$ and $\omega_k \in W$ for the dynamics (11). Thus, if $u_k \in U$, the states always stay inside $\bar{X}$. Furthermore, if the system is in the steady-state operation of the i-th mode, the i-th interval observer can real-time estimate sets to contain the current states, i.e., $x_k \in \hat{X}_k^i$. Thus, based on $\bar{X}$ and $\hat{X}_k^i$, one has

$$x_k \in \bar{X} \cap \hat{X}_k^i. \tag{20}$$

In the i-th mode, the following method is proposed to obtain state estimation, i.e.,

$$\hat{x}_k = \text{center}(\bar{X} \cap \hat{X}_k^i), \tag{21}$$

where $\hat{x}_k$ is used to update the MPC controller (19).

Proposition 4.1: Under Assumption 4.1 and 4.2, the MPC controller (19) with the state estimation (21) is recursively feasible in the steady-state operation. Moreover, the real states x_k are always confined inside $\bar{X}$.

Proof : Under Assumption 4.1 and 4.2, $\bar{X}$ is contained inside X_M, which implies $\hat{x}_k \in X_M$. Thus, at each step, by using (21), the MPC controller (19) is always feasible. As long as the MPC controller is feasible, $u_k \in U$ always holds, which always implies $x_k \in \bar{X} \subseteq X$. □

2) Stability with State Estimation: When using the state estimation (21) to update the MPC controller, there always exist state estimation errors defined as

$$\tilde{x}_k = x_k - \hat{x}_k, \tag{22}$$

Since both x_k and $\hat{x}_k$ are confined in the intersection $\bar{X} \cap \hat{X}_k^i$, $\tilde{x}_k$ should be bounded. In the worst case, i.e., $\bar{X}$ coincides with $\hat{X}_k^i$, the bound of $\tilde{x}_k$ can be obtained as

$$\tilde{x}_k \in \bar{X} \oplus (-\bar{X}). \tag{23}$$

Note that because the coincidence of $\bar{X}$ and $\hat{X}_k^i$ is a low probability event, the real-time bound of $\tilde{x}_k$ should be less conservative than (23). Since the plant is stable as in Assumption 2.2, the bounding of $\tilde{x}_k$ implies stability of the system with the state estimation (21).

C. Fault-tolerant Control Approach

1) Active Fault Isolation: Once a fault (indexed by $j \neq i$) is detected at time instant k_d, the proposed FI approach relies on switching the constraints of the MPC controller from U and X_M to U_f and X_{M_f} to start active FI.

Proposition 4.2: Under Assumption 3.2, 4.1 and 4.2, the mRPI set (denoted as X_{m_f}) for the dynamics (11) corresponding to $u_k \in U_f$ is contained in X_m. Moreover, X_{M_f} is a *robust control invariant* (RCI) set for the dynamics (11) corresponding to $u_k \in U$.

Proof : Because of $U_f \subseteq U$, the mRPI set for the dynamics (11) corresponding to $u_k \in U_f$ is contained in that corresponding to $u_k \in U$. Because of $\bar{X} \subseteq X$, both mRPI sets are contained in X. For $U_f \subseteq U$, X_{M_f} can satisfy the definition as an RCI set of the dynamics (11) under $u_k \in U$, which indicates $X_{M_f} \subseteq X_M$ (See [2] for the RCI sets). □

During active FI, $x_k \in \hat{X}_k^i$ cannot always hold, which implies that (21) cannot guarantee feasibility of the MPC controller. Thus, it is necessary to propose a new strategy to update the MPC controller to guarantee both active FI and transient-state feasibility after faults. To avoid infeasibility during active FI, for each step $k \geq k_d$, one uses

$$\hat{x}_k = \text{center}(X_{M_f}) \tag{24}$$

to update the MPC controller for generating control actions.

By (24), during active FI, the feasibility of the MPC controller can always be guaranteed such that $u_k \in U_f$, which implies that the satisfaction of the FI conditions in Proposition 3.1 on-line. Furthermore, FI can be implemented by using the FI approach (18). Then, at time instant k_i when the fault is isolated, the constraints of the MPC controller are switched to U and X_M from U_f and X_{M_f} for performance.

Proposition 4.3: At the FI time k_i, $x_{k_i} \in \bar{X}$ (i.e., $x_{k_i} \in X_M$). Furthermore, as long as the MPC controller is feasible, $x_k \in X_M$ for all $k \geq k_i$.

Proof : Under Assumption 4.2, $x_k \in \bar{X} \subseteq X_M$ in the steady-state operation. At time instant k_d, although the constraints U and X_M are switched into U_f and X_{M_f}, one still has $u_k \in U_f \subseteq U$ with (24), which implies that the states still stay inside $\bar{X}$. At time instant k_i when the constraints are switched back to U and X_M, $x_{k_i} \in \bar{X}$ still holds and the feasibility of (19) assures $x_k \in X_M$ for all $k \geq k_i$. □

Remark 4.2: It is assumed that the j-th mode ($j \neq i$) is isolated. Under Proposition 4.3, for $k \geq k_i$, if the intersection $\bar{X} \cap \hat{X}_k^j$ is not empty, $\hat{x}_k = \text{center}(\bar{X} \cap \hat{X}_k^j)$ is used for the MPC controller. Otherwise, (24) continues to be used. After reconfiguration, it is guaranteed that, several steps later, $\bar{X} \cap \hat{X}_k^j \neq \emptyset$ can persistently hold.

D. Fault-tolerant Control Algorithm

An FTC algorithm is summarized for the FTC scheme.

1) It is assumed that the system is in the i-th mode, i.e., the i-th state-input set-point pair and the i-th interval observer are used for the system.
2) When a fault is detected at time instant k_d, the constraints of the MPC controller are simultaneously switched from U and X_M to U_f and X_{M_f} to start active FI. (24) is used to guarantee active FI and MPC feasibility during active FI stage, (16) is initialized by X_M to generate the output set sequence for FI and the FI strategy (18) is used to isolate the fault.
3) Once the fault is isolated (it is assumed that the index is $j \neq i$), the system is reconfigured and the strategy proposed in Remark 4.2 is specially used for the initial stage of the new mode. Afterwards, the whole algorithm is repeated to monitor this new mode.

V. Illustrative Numerical Example

A numerical example is used to show the effectiveness of the proposed scheme, whose parameters are given as

- Parameter matrices:
  $A = \begin{bmatrix} 0.6 & 0 \\ 0 & 0.7 \end{bmatrix}, B = \begin{bmatrix} 0.5 & 0.1 \\ 0.2 & -0.3 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$
- Process disturbances: $\bar{w} = \begin{bmatrix} 0.1 & 0.1 \end{bmatrix}^T, w^c = \begin{bmatrix} 0 & 0 \end{bmatrix}^T.$
- Measurements noises: $\bar{\eta} = \begin{bmatrix} 0.1 & 0.1 \end{bmatrix}^T, \eta^c = \begin{bmatrix} 0 & 0 \end{bmatrix}^T.$
- Observer gains[4]:
  $L_0 = \begin{bmatrix} 0.2 & 0 \\ 0 & 0.2 \end{bmatrix}, L_1 = \begin{bmatrix} 2 & 0 \\ 0 & 0.2 \end{bmatrix}, L_2 = \begin{bmatrix} 0.2 & 0 \\ 0 & 2 \end{bmatrix}.$
- Considered sensor faults:
  $\mathbf{G}_1 = \begin{bmatrix} [0, 0.2] & 1 \\ 0 & 1 \end{bmatrix}, \mathbf{G}_2 = \begin{bmatrix} 1 & 0 \\ 0 & [0, 0.2] \end{bmatrix},$
  $\mathbf{G}_f = \begin{bmatrix} [0, 0.2] & 0 \\ 0 & [0, 0.2] \end{bmatrix}.$
- Fault magnitudes[5]: $G_1 = \begin{bmatrix} 0.1 & 1 \\ 0 & 1 \end{bmatrix}, G_2 = \begin{bmatrix} 1 & 0 \\ 0 & 0.1 \end{bmatrix}.$
- Output set-points: $y_0^* = \begin{bmatrix} 1.5 \\ 1 \end{bmatrix}, y_1^* = \begin{bmatrix} 0.5 \\ 1 \end{bmatrix}, y_2^* = \begin{bmatrix} 1.5 \\ 0.5 \end{bmatrix}.$
- State-input set-point pairs:
  $u_0^* = \begin{bmatrix} 1.2353 \\ -0.1765 \end{bmatrix}, u_1^* = \begin{bmatrix} 3.7059 \\ 1.4706 \end{bmatrix}, u_2^* = \begin{bmatrix} 1.9412 \\ -3.7059 \end{bmatrix},$
  $x_0^* = \begin{bmatrix} 1.5 \\ 1 \end{bmatrix}, x_1^* = \begin{bmatrix} 5 \\ 1 \end{bmatrix}, x_2^* = \begin{bmatrix} 1.5 \\ 5 \end{bmatrix}.$
- Initial conditions:
  $x_0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \hat{X}_0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 0.1 & 0 \\ 0 & 0.1 \end{bmatrix} \mathbb{B}^2.$
- System constraints:
  $U = \{u : \begin{bmatrix} -10 & -10 \end{bmatrix}^T \leq u \leq \begin{bmatrix} 10 & 10 \end{bmatrix}^T\},$
  $X = \{x : \begin{bmatrix} -20 & -20 \end{bmatrix}^T \leq x \leq \begin{bmatrix} 20 & 20 \end{bmatrix}^T\}.$
- Input set for active FI:
  $U_f = \{u : \begin{bmatrix} 6.5 & 6.5 \end{bmatrix}^T \leq u \leq \begin{bmatrix} 7.5 & 7.5 \end{bmatrix}^T\}.$
- Sampling time: $T = 0.1$s.
- Prediction horizon: $N = 2$.
- MPC controller parameters:
  $Q = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, R = \begin{bmatrix} 0.1 & 0 \\ 0 & 0.1 \end{bmatrix}, P = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$

For the three modes (healthy and faulty), three corresponding interval observers are designed as in (6). Furthermore, using $u_k \in U_f$ and $\omega_k \in W$, the output sets corresponding to the three mode can be presented in Figure 1.

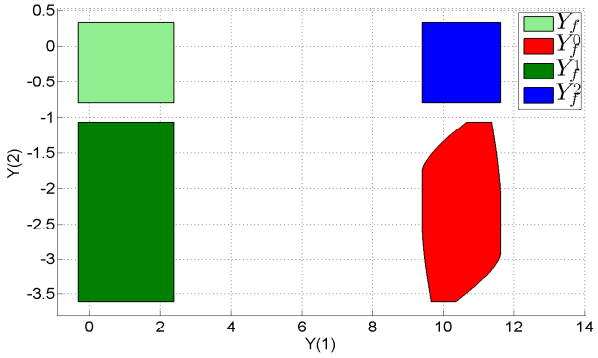

Fig. 1. Output sets for active FI

In Figure 1, all the interval components of Y_f are disjoint from those of Y_f^0, respectively, and both of Y_f^1 and Y_f^2 have

[4] L_1 and L_2 are obtained using mid($\mathbf{G}_1$) and mid($\mathbf{G}_2$), respectively.

[5] G_1 and G_2 denote actual fault magnitudes, i.e., $G_1 \in \mathbf{G}_1$ and $G_2 \in \mathbf{G}_2$. Note that fault occurrence of any magnitude inside $\mathbf{G}_1$ and $\mathbf{G}_2$ can be isolated if they can be detected.

an interval component that is the same with Y_f. The scenarios for both faults are: from time instants 1 to 10, the system is healthy, while from time instants 11 to 30, a fault occurs.

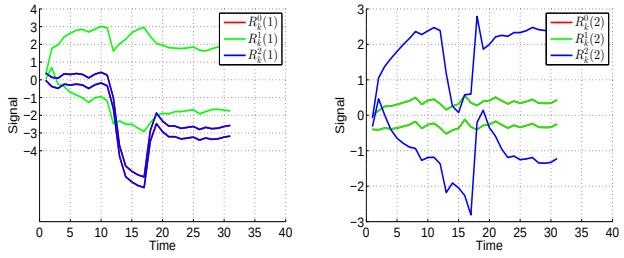

Fig. 2. FD of the first fault

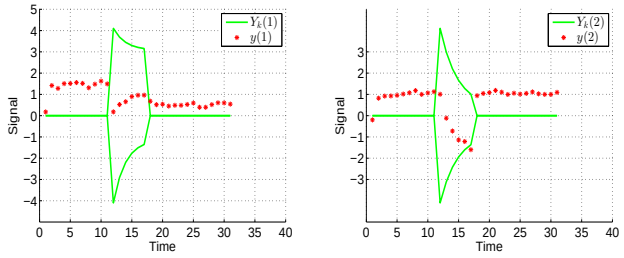

Fig. 3. FI of the first fault

The FD and FI results of the first fault are shown in Figure 2 and 3, respectively. In Figure 2, a fault is detected at $k = 12$, i.e., $\mathbf{0} \notin R_{12}^0$ (note that $R_k^0(1)$ and $R_k^0(2)$ respectively coincides with $R_k^2(1)$ and $R_k^1(2)$ in Figure 2). Thus, active FI is started at $k = 12$, i.e., (16) is initialized and (18) is tested in real time for FI. In Figure 3, at $k = 17$, the first component of y_k respects its bound $Y_k(1)$, i.e., $y_{17}(1) \in Y_{17}(1)$, while the second component violates its bound, i.e., $y_{17}(2) \notin Y_{17}(2)$, which indicates the first sensor fault is isolated. Thus, the first state-input set-point pair is used to reconfigure the system at $k = 17$. The output of the system is shown in Figure 3 as the red stars. Before the first fault, the expected output y_0^* is well tracked, while after the first fault, the tracking performance becomes poor until the time instant $k = 17$ when the system is reconfigured. After $k = 17$, the expected y_1^* can be well tracked again.

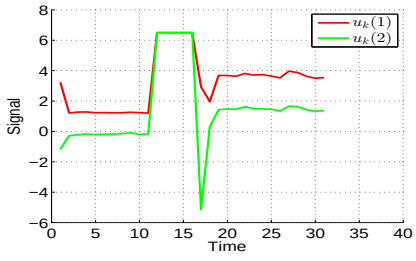

Fig. 4. Control inputs for the first fault

The control actions are presented in Figure 4, where before fault occurrence, the control inputs satisfy their constraints.

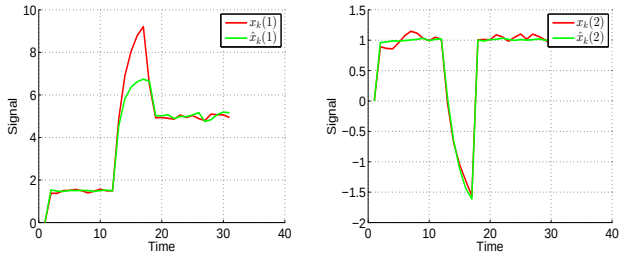

Fig. 5. Comparison of states and state estimations

During active FI, because of the strategy (24), the generated inputs are constant, which satisfy the constraint set U_f. After system reconfiguration, the control inputs to tolerate the first fault are generated, which also satisfy the constraint U. Besides, to show the effectiveness of the state estimation (21), a comparison between the real states and their estimations is shown in Figure 5. It can be observed that (21) can give satisfactory state estimations in steady state.

Remark 5.1: Although two sensor faults are considered in this example, due to the length of this paper, only the results related to the first sensor fault are presented here. ◊

VI. Conclusions

The paper propose a sensor FTC scheme using MPC, interval observer-based FD and set-based active FI. By combining MPC with set-based FDI approaches it is shown that sensor FDI and the corresponding FI conditions can be simplified. For the MPC feasibility guarantees, the FTC scheme rely on relationships between invariant sets characterizing the autonomous dynamics and resumed by 4.1. If alternative on-line state-estimation schemes can be implemented by exploiting plant information, the FTC scheme proposed in the present paper can be used with possible relaxed assumptions.

References

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

[2] F. Borrelli, A. Bemporad, and M. Morari. *Predictive Control for Linear and Hybrid Systems*. Model Predictive Control Lab, UC-Berkeley, USA, 2013.

[3] 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.

[4] Johan Löfberg. *Min-max Approaches to Robust Model Predictive Control*. PhD thesis, Department of Electrical Engineering, Linköping University, Sweden, 2003.

[5] 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.

[6] F. Stoican and S. Olaru. *Set-theoretic Fault-tolerant Control in Multisensor Systems*. John Wiley & Sons, Inc., 2013.

[7] F. Xu, V. Puig, C. Ocampo-Martinez, F. Stoican, and S. Olaru. Actuator-fault detection and isolation based on set-theoretic approaches. *Journal of Process Control*, 24(2):947 – 956, 2014.

[8] A. Yetendje, M. M. Seron, and J. A. De Doná. Robust MPC design for fault tolerance of constrained multisensor linear systems. In *Proceedings of the International Conference on Control and Fault-Tolerant Systems*, Nice, France, October 6-8 2010.