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

Feng Xu[1], Sorin Olaru[2], Vicenç Puig[3], Carlos Ocampo-Martinez[3,*]
and Silviu-Iulian Niculescu[4]

[1]Center of Intelligent Control and Telescience, Graduate School at Shenzhen,
Tsinghua University, Shenzhen, China.
[2]E3S (SUPELEC Systems Sciences), Automatic Control Department,
Gif sur Yvette, Paris, France.
[3]Institut de Robòtica i Informàtica Industrial (CSIC-UPC),
Technical University of Catalonia (UPC), Barcelona, Spain.
[4]Laboratoire des Signaux et Systmes (L2S, UMR CNRS 8506), CNRS-Supélec,
Gif sur Yvette, Paris, France.

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 robust MPC controller is used to control the plant in the presence of process disturbances and measurement noises, while implementing a mechanism to tolerate faults. In the proposed scheme, fault detection (FD) is passive based on interval observers, while fault isolation (FI) is active by means of MPC and set manipulations. The basic idea is that, for a healthy or faulty mode, one can construct the corresponding output set. The size and location of the output set can be manipulated by adjusting the size and center of the set of plant inputs. Furthermore, the inputs can be adjusted on-line by changing the input-constraint set of MPC controller. In this way, one can design an input set able to separate all output sets corresponding to all considered healthy and faulty modes from each other. Consequently, all the considered healthy and faulty modes can be isolated after detecting a mode changing while preserving feasibility of MPC controller. As a case study, an electric circuit is used to illustrate the effectiveness of the proposed FTC scheme.

1 Introduction

A control system consists of a series of components that play different roles in the closed-loop operation. Among those components, sensors are used to acquire the real-time system-operating information to take proper control actions and achieve some system performance. Hence, it is important for the closed-loop system to monitor the sensor status and include mechanisms to tolerate the effect of sensor faults in order to provide the control scheme with safety properties.

In general, there exist two types of FTC approaches [2]. The first type is called passive fault-tolerant control (PFTC), whose principle consists in treating faults as uncertain factors and using the robustness of controller to cope with the effect of faults as in robust control. From the technical point of view, PFTC is relatively easy to implement but has only limited FTC capabilities. Moreover, the larger the number of faults considered in a PFTC scheme is, the higher price of performance loss the system has to face in a specific healthy or faulty mode. Comparatively, the other FTC strategy, namely active fault-tolerant control (AFTC), uses a so-called fault-diagnosis module to monitor the system. After fault occurrence, the fault-diagnosis module can extract some fault information that enables fault tolerance by means of system reconfiguration/fault accommodation[1].

[1] In order to tolerate the effect of faults, *system reconfiguration* implies that the system structure is changed, while *fault accommodation* only adjusts control laws instead of changing the system structure.

In the proposed FTC scheme, MPC is used as the control strategy, where the latest measurements are used to update the MPC controller in real time and only the first element of the optimized control sequence is injected into the system at each step [11]. As one of the successful advanced control techniques in the process industry, the major advantage of MPC for the proposed FTC scheme consists in its capability to effectively deal with system constraints [3, 10]. Moreover, for an FTC scheme, a key element is its FDI approach. Taking the robustness requirements of FDI decisions into account, the set-based FDI approach is chosen to implement the FDI objectives in the present work. Particularly, the FD approach is passive based on interval observers while the FI approach is active by making use of the constraint-handling capacity of MPC. That is, once the FD mechanism has detected a fault, the objective of MPC controller changes from tracking the nominal reference, to driving the system state to a value where FI is possible.

In the literature, there already exist several attempts of fault-tolerant model predictive control (FTMPC), such as the ones presented in [18, 22], which use set-membership estimation and Kalman filter-based FDI, respectively. In [21], an on-line optimization is used based on mixed-integer programming for the active fault isolation. In [18], the proposed FTMPC scheme used active FI, which can reduce the FI conservatism but with high price of computational complexity because the proposed active FI method required to determine on-line inputs that can separate sets associated to faults. In [17], a new method was proposed by the authors to reduce the computational complexity of the work in [18], which computed separating inputs off-line. However, since the off-line computation of separating inputs was based on partitioning an output set that included all possible outputs under all possible system modes (healthy or faulty), it was more conservative when comparing with the case of using the real-time measured outputs. Furthermore, a particularity of the works in [17, 18] was that without using the notion of invariant sets, these two methods did not provide a mechanism to check whether the considered faults were isolable or not in advance. In [22], the proposed FTMPC scheme used the Kalman filter to implement FDI. However, its main objective was to propose an FTMPC scheme. Thus, it did not rigourously consider some important features of MPC such as feasibility. The work in [24] proposed a multi-sensor FTMPC scheme, which used invariant set-based passive FDI and implemented FTC by switching among a group of sensors. Because of the use of set-based passive FDI, guaranteed FDI conditions were generally more conservative due to the pre-imposed set separation. Moreover, this FTMPC scheme tolerated faults by switching among a bank of sensors, which involved an economic price from the instrumentation point of view. Moreover, for additional references related to fault-tolerant applications of MPC, the readers are addressed to [1, 4, 5, 6, 7, 8, 20, 23], among many others.

The objective of this paper is to propose a sensor FTMPC scheme with a relatively simple system structure, which can simultaneously deal with system constraints and tolerate faults with less conservative FI conditions. Comparing with FTMPC schemes such as those aforementioned, the proposed FTMPC scheme has three main novelties. First, it proposes a novel and simple active FI technique via MPC which ensures that an output component only corresponds to one sensor fault in a pre-defined finite class of fault scenarios and simultaneously uses the concept of invariant sets to check whether the considered faults are isolable in advance. Second, it proposes a pragmatic robust state estimation approach for MPC controllers, which can provide effective feasibility guarantees of MPC open-loop optimization problem for both FI and FTC. Third, under some structural conditions (observability, disturbance and noise boundedness), the proposed scheme is able to detect, isolate and tolerate unknown but bounded sensor faults with no need of multi-sensor hardware redundancy.

The proposed FTMPC scheme is shown in Figure 1, which is composed of the *plant, MPC controller, FDI module, a bank of interval observers, switching logic and state estimator*. In Figure 1, an MPC controller is designed with a set of setpoints, considering that the setpoints may be different in different modes, and the setpoints are adjusted according to the current FDI decisions (note that the arrow on the block *MPC controller* means that the setpoints can be adjusted according to the FDI decisions). The FDI module [2] is the core of this paper and is based on the proposed FDI method that interacts with the process and obtains system-operating information to make FDI decisions. A bank of interval observers is designed to monitor the dynamical behaviours of the system, each matching a considered healthy or faulty mode and simultaneously estimating state sets. Switching logic is based on the decisions made by the FDI module, which adjusts among setpoints and interval observers and makes them match the current mode. The state estimator is designed to generate state estimations by using the estimated state set from interval observers to update the MPC controller for computing new control actions at each step.

[2] In Figure 1, the texts *FDI decision* are used twice, which are actually the same and repeated only for simplicity of drawing.

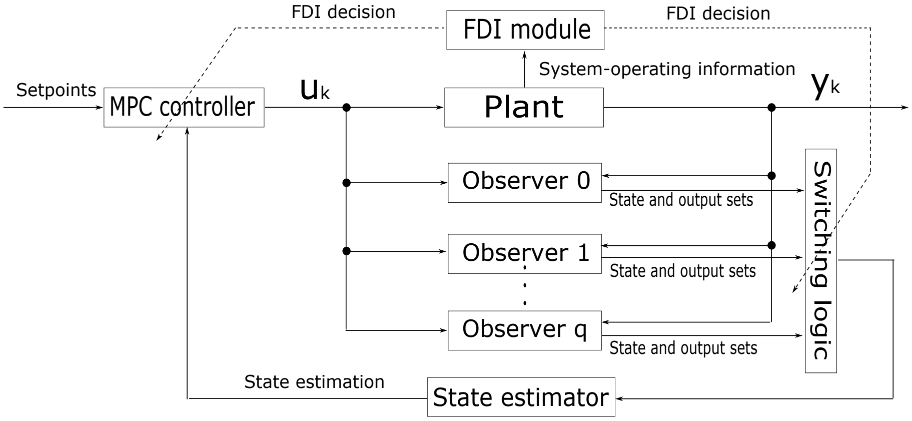

Figure 1: Sensor FTMPC scheme

The remainder of the paper is organized as follows. Section II introduces the FTMPC scheme. Section III presents the FDI strategy and FI conditions. In Section IV, the FTC strategy is proposed and the feasibility and stability of MPC are analyzed. In Section V, an example is used to illustrate the effectiveness of the proposed scheme. In Section VI, some general conclusions are drawn.

2 System Description

In this section, the objective is to introduce the proposed FTC scheme including the plant, setpoints, interval observers and robust MPC controller.

2.1 Plant Models

The linear discrete time-invariant plant under the effect of sensor faults 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 time-invariant matrices, $x_k \in \mathbb{R}^n$, $u_k \subset \mathbb{R}^p$ and $y_k \in \mathbb{R}^q$ are state, input and output vectors at time instant k, respectively, ω_k and η_k are process disturbance and measurement noise vectors, respectively.

In this paper, only sensor faults important/critical to system performance/safety are considered. That is, the matrix $\mathbf{G}$ only takes a finite number of fault scenarios into account. Furthermore, without loss of generality, only the single-fault case is considered here. But, in principle, the proposed approach can also be extended to handle the multiple faults if $\mathbf{G}$ contains the signatures of the multiple fault scenarios. In the single-fault case, $\mathbf{G}$ can take $q + 1$ values identified by $q + 1$ diagonal (interval) matrices. The diagonal elements of the matrix $\mathbf{G}$ will correspond to the statuses of sensors such that $\mathbf{G}$ can have a finite number of configurations $\mathbf{G}_i$ ($i \in \mathbb{I} = \{0, 1, ..., q\}$), where $\mathbf{G}_0$ is the identity matrix denoting the healthy sensor mode and $\mathbf{G}_i$ ($i \neq 0$) is a diagonal interval matrix to model the i-th sensor fault with

$$\mathbf{G}_i = \mathrm{diag}(1 \; \ldots \; \overset{\overset{i}{\downarrow}}{f_i} \; \ldots \; 1),$$

where diag($\cdot$) denotes the diagonal matrix and f_i denotes an interval modelling the fault magnitude in the i-the sensor and satisfying

$$f_i \subseteq [0,\ 1).$$

Furthermore, a diagonal interval matrix to describe the considered fault magnitudes corresponding to all the sensors is defined as

$$\mathbf{G}_f = \mathrm{diag}(f_1 \; \ldots \; f_i \; \ldots \; f_q),$$

where each diagonal element of $\mathbf{G}_f$ corresponds to the considered interval of fault magnitude in one sensor. Besides, the state and input constraints of the system are denoted 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 known and constant. Note that, here and in the remaining of the paper, the absolute values and the inequalities are understood element-wise. For example, it should be understood that (2a) is composed of n inequalities where the i-th one is denoted as $|x_i - x_i^c| \leq \bar{x}_i, x_i^c \in \mathbb{R}^1, \bar{x}_i \in \mathbb{R}^1$.

Assumption 2.1 *Matrix A is a Schur matrix and the pairs $(A, \mathbf{G}_i C)$ for all $i \in \mathbb{I}$ are detectable.*

Assumption 2.2 *The disturbance and noise vectors ω_k and η_k are bounded by known sets*

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

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

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

Definition 2.1 *An r-order zonotope Z is defined as $Z = g \oplus H\mathbb{B}^r$, where g and H are called the center and segment matrix of this zonotope, respectively, $\mathbb{B}^r$ is a box composed of r unitary intervals and the symbol $\oplus$ denotes the Minkowski sum.*

Definition 2.2 *The* interval hull $\square X$ *of a zonotope $X = g \oplus H\mathbb{B}^r \subset \mathbb{R}^n$ is the smallest box that contains X (i.e., $\square X = \{x : |x_i - g_i| \leq \parallel H_i \parallel_1\}$), where H_i is the i-th row of H, and x_i and g_i are the i-th components of x and g, respectively.*

Note that Assumption 2.1 is made to guarantee that the proposed scheme can work and the corresponding details on this assumption will be explained in next sections. Moreover, under Assumption 2.2, the sets W and V can be rewritten into zonotopes.

Assumption 2.3 *The considered sensor faults can persist sufficiently long time such that the FDI module has enough time to detect and isolate the faults.*

Remark 2.1 *The interval matrix $\mathbf{G}$ in (1) models the considered fault magnitude intervals, while the actual magnitude of the i-th sensor fault is a particular but unknown value denoted as G_i with $G_i \in \mathbf{G}_i$.*

2.2 Output Setpoints

When the system operates in the i-th sensing mode, the control objective of the closed-loop system is defined to regulate around a given output setpoint y_i^*, i.e., in the absence of uncertainties,

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

where y_i^* denotes the output setpoint corresponding to the i-th sensor mode.

In this paper, a sensor FTC scheme is proposed, where the reference model for the generation of setpoints corresponding to the i-th sensor mode is given as

$$x_{k+1}^{ref} = Ax_k^{ref} + Bu_k^{ref} + \omega^c, \tag{4a}$$

$$y_k^{ref} = \text{mid}(\mathbf{G}_i)Cx_k^{ref} + \eta^c, \tag{4b}$$

where mid$(\cdot)$ computes the center of interval matrices and u_k^{ref}, x_k^{ref} and y_k^{ref} denote the reference input, state and output vectors at time instant k. Here, only the system regulation case is considered. Based on

(4), if the i-th output setpoint y_i^* is considered at steady state, the corresponding state-input setpoint pair satisfies

$$\begin{bmatrix} A-I & B \\ \mathrm{mid}(\mathbf{G}_i)C & O \end{bmatrix} \begin{bmatrix} x_i^* \\ u_i^* \end{bmatrix} = \begin{bmatrix} -\omega^c \\ y_i^* - \eta^c \end{bmatrix}, \tag{5}$$

where O and I denote the zero and identity matrices with compatible dimensions, respectively and the solution (x_i^*, u_i^*) of (5) is a state-input setpoint pair corresponding to y_i^*.

Remark 2.2 *The* steady state *of a mode describes a phase where no mode switching occurs and all system signals are in their own sets, while the* transient state *corresponds to a phase from the steady state of a mode to that of another mode, which is induced by mode switching (e.g. faults).*

Remark 2.3 *Sensor faults imply the loss of some available system-operating information. Due to some changes in the system dynamics and the existence of disturbances and noises, there will be no guarantee that the coresponding output setpoints will be exactly achieved. Note that the given output setpoints may be different in different modes. An example explaining this possibility considers that* (5) *is solvable after faults. But, the corresponding solutions may not satisfy the constraints. In this case, the setpoints can be properly changed to satisfy both solvability of* (5) *and constraints by accepting a certain degree of performance degradation.*

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

In this paper, it is assumed that (5) is solvable as in Assumption 2.4. In case that (5) is not solvable, one possible remedy is to degrade the output performance (i.e., change the corresponding output setpoint) such that (5) is solvable. Since there are $q+1$ modes (healthy or faulty) considered, $q+1$ state-input setpoint pairs should be considered. In the remaining contents of the paper, for the sake of simplicity, ω^c and η^c are considered to be zero. Additionally, notice that, since (5) may have multiple solutions (see also the case when $A-I$ is singular), in this case, one can select one solution according to particular performance specifications out of a group of solutions.

2.3 Interval Observers

Considering that there are $q+1$ sensing modes, a bank of interval observers is designed to monitor the plant, each matching one mode. In this paper, all the interval observers are designed based on the Luenberger structure. For the j-th mode, if the actual fault magnitude is denoted as G_j (i.e., $G_j \in \mathbf{G}_j$), the corresponding Luenberger observer is designed as

$$\hat{x}_{k+1}^j = (A - L_j G_j C)\hat{x}_k^j + Bu_k + L_j y_k + (-L_j)\hat{\eta}_k + \hat{\omega}_k, \tag{6a}$$
$$\hat{y}_k^j = G_j C \hat{x}_k^j + \hat{\eta}_k, \tag{6b}$$

where $\hat{x}_k^j$ and $\hat{y}_k^j$ are the estimated state and output vectors and $\hat{\eta}_k$ and $\hat{\omega}_k$ are artificial signals that emulate the effect of η_k and ω_k on the plant (1) with $\hat{\eta}_k \in V$ and $\hat{\omega}_k \in W$, respectively. Thus, by introducing $\mathbf{G}_j$, W and V into (6) to replace G_j, ω_k and η_k, respectively, the corresponding interval observer can be obtained as

$$\hat{X}_{k+1}^j = (A - L_j \mathbf{G}_j C)\hat{X}_k^j \oplus \{Bu_k\} \oplus \{L_j y_k\} \oplus (-L_j)V \oplus W, \tag{7a}$$
$$\hat{Y}_k^j = \mathbf{G}_j C \hat{X}_k^j \oplus V, \tag{7b}$$

where $\hat{X}_k^j$ and $\hat{Y}_k^j$ are the corresponding estimated state and output sets. Note that, since the real fault magnitude G_j is unknown, $\mathbf{G}_j$ is used to replace G_j in the interval observer (7).

Assumption 2.5 *For the* j*-th observer, the observer gain* L_j *can be designed to guarantee that* $A - L_j G_j C$ *is a Schur matrix for all* $G_j \in \mathbf{G}_j$.

Note that, under Assumption 2.1, Assumption 2.5 can always be satisfied. However, an example method allowing this observer gain design can be referred to [16].

Assumption 2.6 *The initial state x_0 of the plant belongs to the initial set $\hat{X}_0^j$ corresponding to the j-th interval observer for $j \in \mathbb{I}$.*

From the computational point of view, the implementation of interval observers is based on zonotopes. Actually, (7) is the ideal form of interval observer. Practically, in order to propagate the dynamics of the j-th interval observer with a zonotope, it is needed to approximate the product of an interval matrix and a zonotope generated during the propagation with a zonotope by using Properties A.3 and A.4 in Appendix A. This is because sensor fault magnitude $\mathbf{G}_i$ is considered as an interval matrix instead of a particular value in this paper, which results in that, at each step, the generated output set is an union of a group of zonotopes originated from the product of an interval matrix and a zonotope (see the term $(A - L_j\mathbf{G}_jC)\hat{X}_k^j$ in (7)). Additionally, since at each iteration of the interval observer dynamics (7), the order of the estimated state and output zonotopes increases, it is necessary to control the explosion of zonotope order. This can be done by using Property A.5 that can over-approximate a high-order zonotope with a low-order zonotope avoiding the problem.

2.4 Robust MPC Controller

In the proposed FTC scheme, the min-max robust MPC technique is used as the control strategy because it allows to consider system uncertainties and constraints. The advantage of the min-max MPC technique consists in that it can directly deal with the plant input constraints allowing easily to manipulate their bounds, which is the key for the proposed sensor active FI approach. In this paper, the design of the min-max MPC controller is based on [10] and the details of the min-max MPC technique and the associated properties are omitted here. In the following, two important concepts of sets used for robust MPC are introduced.

Definition 2.3 *A set $\mathcal{X} \subseteq X$ is a* robust control invariant *(RCI) set of the dynamics $x_{k+1} = Ax_k + Bu_k + \omega_k$ if for any $x_k \in \mathcal{X}$, there always exists $u_k \in U$ such that $x_{k+1} \in \mathcal{X}$ holds for all $\omega_k \in W$ and $k \geq 0$.*

Definition 2.4 *A set $\mathcal{X}_\mathcal{M} \subseteq X$ is said to be the* maximal robust control invariant *(MRCI) set of the dynamics $x_{k+1} = Ax_k + Bu_k + \omega_k$, if it is a RCI and contains all RCI sets inside X.*

When the proposed FTC scheme is in the i-th mode, the i-th state-input setpoint pair and interval observer should be chosen. Thus, according to [3, 10], an MPC controller corresponding to the i-th mode can be designed as

$$J_k = \min_{\mathbf{u}} \max_{\mathbf{w}} \sum_{j=0}^{N-1} \|(x_{k+j|k} - x_i^*)\|_Q^2 + \|(u_{k+j|k} - u_i^*)\|_R^2 + \|(x_{k+N|k} - x_i^*)\|_P^2$$

$$\text{subject to} \quad \left.\begin{array}{r} x_{k+j|k} \in X, \\ u_{k+j|k} \in U, \\ x_{k+N|k} \in X_M, \\ x_{k|k} = \hat{x}_k, \end{array}\right\} \forall \omega_{k+j|k} \in W, \tag{8}$$

with the MPC controller internal model

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

where N denotes the prediction horizon, X_M is the terminal state constraint set that is the MRCI set of the dynamics (1a) under the constraints (2), $\hat{x}_k$ is the system state estimation that is obtained in real time and used to update the MPC controller to generate new control actions, $\mathbf{u} = [u_{k|k}, u_{k+1|k}, \cdots, u_{k+N-1|k}]$ is the optimized control sequence over the prediction horizon, Q, R and P are positive-definite weighting matrices, and $\mathbf{w} = [\omega_{k|k}, \omega_{k+1|k}, \cdots, \omega_{k+N-1|k}]$ is the sequence of process disturbances over the prediction horizon.

3 Fault Detection and Isolation

This section presents the FD and FI methods used in the proposed FTC scheme. Both of them are based on the notions of interval observers and set theory.

3.1 Fault Detection

It can be observed that, based on Assumption 2.2, W and V can be rewritten in zonotopic form. Moreover, $\hat{X}_0^j$ can be initialized according to Assumption 2.6 that allows to approximate $\hat{X}_{k+1}^j$ and $\hat{Y}_k^j$ by means of zonotopes as well. As aforementioned, by using zonotope operations, the computational complexity of interval observers can be managed along the state dynamics evolution. Thus, the interval observer (7) can be propagated on-line by preserving the zonotopic structure and guaranteeing the containment of system states. If the j-th interval observer matches the current sensor mode, as long as the initial state and initial set satisfy Assumption 2.6, it is guaranteed that

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

In the i-th sensor mode, the fault-modeling matrix $\mathbf{G}$ should take a value $G_i \in \mathbf{G}_i$ ($i \in \mathbb{I}$) and the i-th interval observer is used to monitor the plant if the switching logic of the FDI mechanism in Figure 1 accurately chooses it. In order to detect faults, the residual (in terms of zonotopes) of the i-th interval observer corresponding to the i-th sensor mode is defined as

$$R_k^{ii} = y_k - \hat{Y}_k^i, \tag{10}$$

where the first superscript of R_k^{ii} corresponds to the i-th sensor mode while the second superscript corresponds to the i-th interval observer.

Although all the interval observers in the bank operate simultaneously, only residual zonotopes of the interval observer matching the current sensor mode is chosen for FD in real time. Therefore, when the system is in the i-th sensor mode, the FD task is implemented by testing whether or not

$$\mathbf{0} \in R_k^{ii} \tag{11}$$

is violated in real time. If a violation is detected, it means that a sensor fault has occurred. Otherwise, it is considered that the system still operates in the i-th sensor mode.

The sensitivity of the criterion (11) to faults is related to the design of interval observers and the sizes of sets such as W and V. The satisfaction of (11) does not always imply that the system is healthy because the FD strategy cannot be sensitive to all faults. For faults undetectable by (11), the AFTC strategy of the proposed scheme cannot be started up to deal with the faults. Instead, only the potential PFTC ability of the proposed scheme will be able to handle them to some extent under specific conditions. In this case, the faults are treated as unknown uncertain factors by MPC and the robustness of MPC is used to passively tolerate such faults.

3.2 Fault Isolation

3.2.1 Guaranteed FI Conditions.

At a time instant when a sensor fault occurs, the fault only affects one component of the system output at that time instant. However, due to the feedback loop, the effect of the sensor fault on the remaining outputs will be coupled after fault occurrence (i.e., more output components will be affected by the fault afterwards), which increases difficulties of FI.

Different from the passive FI approaches in references and therein, the proposed FI approach in this paper is active by modifying the effect of controller on the plant to decouple the fault effect on the different output components. Thus, in order to explain the proposed FI approach, it is assumed that the plant input vector is bounded by a set U_f after FD:

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

where the set U_f should satisfy the input constraint of the plant:

$$U_f \subseteq U. \tag{12}$$

Remark 3.1 *U_f is an artificially defined input set used for FI. Note that U_f is different from the hard input-constraint set U and must be a subset of U. In this paper, the basic idea is that, during the steady-state operation, U is used as the input-constraint set of MPC controller to maximize control performance, while after FD, the MPC input-constraint set is adjusted from U to U_f to actively isolate faults.*

Since only sensor faults are considered in this paper, the output equation will be affected while the state-space equation dynamics will not be affected by sensor faults. In this case, if the input vector is bounded by a set, a state invariant set can be constructed by considering the inputs as disturbances. In this way, the dynamics (1a) can be rewritten as

$$x_{k+1} = Ax_k + \begin{bmatrix} B & I \end{bmatrix} \begin{bmatrix} u_k \\ \omega_k \end{bmatrix}. \tag{13}$$

Remark 3.2 *The invariant set of* (13) *will be used to establish guaranteed FI conditions for the proposed approach. In general, considering u_k as disturbances will increase the size of invariant set (i.e., the conservatism of FI conditions) in the traditional passive set-based FDI approaches. But, since this paper aims to propose an active FI approach by designing an input set U_f and adjusting the input-constraint set of MPC to U_f for FI on-line, we can known that U_f is a controllable design freedom, whose size and location can be determined by designers. Thus, the least conservative case is to design U_f as a point instead of a set and adjust the location of this point to satisfy the FI conditions. Obviously, with respect to the traditional passive approaches, the proposed active FI approach actually can have less FI conservatism. The details will be given in the following contents.*

In order to construct the state invariant set, some additional definitions on the set-invariance theory are recalled, which are collected in Definitions 3.1 and 3.2.

Definition 3.1 *A set $\mathcal{X}$ is a* robust positively invariant *(RPI) set of the dynamics $x_{k+1} = Ax_k + E\omega_k$ if for $x_k \in \mathcal{X}$ and $\omega_k \in W$, one always has $x_{k+1} \in A\mathcal{X} + EW \subseteq \lambda\mathcal{X}$ $(0 < \lambda \leq 1)$. When $0 < \lambda < 1$, the RPI set $\mathcal{X}$ is* λ-contractive.

Definition 3.2 *The* minimal robust positively invariant *(mRPI) set of the dynamics $x_{k+1} = Ax_k + E\omega_k$ is an RPI set contained in any closed RPI set and the mRPI set is unique and compact.*

Thus, by considering $u_k \in U_f$ and $\omega_k \in W$, an RPI set of the dynamics (13) can be computed (see [9, 15, 19] for the details of the RPI sets), which is denoted as X_f centered at

$$x_f^c = (I - A)^{-1}(Bu_f^c + \omega^c). \tag{14}$$

Furthermore, in the i-th mode, the corresponding output set can be obtained as

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

where Y_f^i is centered at

$$y_f^{c,i} = \mathrm{mid}(\mathbf{G})_i C x_f^c + \eta^c.$$

If $\mathbf{G}$ takes the value $\mathbf{G}_0$, the output set corresponding to the healthy sensor mode is

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

where Y_f^0 is centered at

$$y_f^{c,0} = Cx_f^c + \eta^c.$$

It is known that the output set is q-dimensional. Since the aim of this paper is to implement that one component of the output set is only matched to the status of a single sensor, this set is projected into each dimension of the q dimensions and evaluated in a component-wise manner taking into account that each component is bounded by an interval. Theoretically, considering $u_k \in U_f$, only the i-th component of Y_f^i is different from that of Y_f^0 due to the effect of the i-th fault, while all the other components of Y_f^0 and Y_f^i should be the same. Furthermore, with respect to Y_f^0, another set is defined for the proposed FI strategy as

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

where Y_f is centered at

$$y_f^c = \mathrm{mid}(\mathbf{G}_f) C x_f^c + \eta^c.$$

By comparing Y_f^0, Y_f^i with Y_f, one can identify the two following situations:

- comparing $\mathbf{G}_0$ with $\mathbf{G}_f$, due to the effect of the faults, all the components of Y_f are different from those of Y_f^0 by considering that Y_f is used to model the effect of faults over all sensors,
- only the i-th component of Y_f^i ($i \neq 0$) coincides with that of Y_f, while all the others do not coincide with the corresponding components of Y_f. This is because of the effect of the i-th fault over Y_f^i, which can be observed by comparing $\mathbf{G}_i$ and $\mathbf{G}_f$.

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

It can be observed that the size and position of the output set are affected by the set of inputs and the magnitudes of faults as also emphasized in Remark 3.2. Thus, by choosing different U_f inside U, one can obtain different output sets in different modes (healthy or faulty). This implies that one can separate the output sets corresponding to different modes by designing U_f. Based on this idea, one gives the FI conditions of the proposed FI approach in Proposition 3.1.

Proposition 3.1 *For the plant* (1) *under the constraints* (2)*, if there exists a set U_f that satisfies* (12) *such that*

$$Y_f^0(l) \cap Y_f(l) = \emptyset, \textit{ for all } l \in \mathbb{I} \setminus \{0\}, \tag{15}$$

all the considered sensor faults are isolable after detection in the case of persistent faults.

Proof : If the inputs are bounded by a set U_f, which can guarantee the separation of the l-th component, i.e, $Y_f^0(l) \cap Y_f(l) = \emptyset$, after the l-th fault occurs, the l-th output component converges to the l-th interval component of Y_f instead of Y_f^0, while all the other output components converge to the corresponding components of Y_f^0 instead of Y_f, respectively, which indicates that the l-th fault has occurred. Thus, if all the components of Y_f^0 and Y_f are separated from each other, it implies that all the considered sensor faults are isolable after they are detected. □

Assumption 3.1 *There exists a set $U_f \subseteq U$ such that all the considered sensor faults satisfy their corresponding output-interval separation conditions described by* (15)*.*

Note that, based on Proposition 3.1 and Assumption 3.1, it can be guaranteed that the considered sensor faults can be isolated if the inputs are bounded in U_f. Thus, U_f is a key set for the implementation of the proposed FI method in this paper. In order to help the readers understand the role of the set U_f, Remark 3.3 is made.

Remark 3.3 *Assumption 3.1 can guarantee that the proposed FI approach is able to implement FI. However, there always exist faults, for which, one cannot find an input set that satisfies Assumption 3.1. Thus, one needs at least a method to judge whether there exist subsets inside U, which satisfies Assumption 3.1. It is known that the size and center of U_f directly affect the separation of the output sets. If one considers U_f as points instead of sets, then the extreme points of U will have the highest possibility to satisfy Assumption 3.1. If all extreme points of U cannot satisfy Assumption 3.1, it means that inside U, one cannot find an useful input set U_f. This method can be used to test whether the proposed method can be used for a sensor FTC application based on the proposed FTC scheme. Besides, even though there exists satisfactory U_f, in the current paper, one only uses the trial and error method to design U_f. However, the methods proposed in [12, 13, 20] can be used as references.*

3.2.2 Fault Isolation Strategy.

It is assumed that a fault is detected at time instant k_d. At this time instant, the proposed FI approach switches the input constraint of the MPC controller from U to U_f to start an active FI phase. According to the MPC controller formulation (8), after the input-constraint switching, if the MPC controller is still feasible, the generated control action must satisfy

$$u_k \in U_f,\ k > k_d. \tag{16}$$

In the proposed FI method, one needs to confine the state x_{k_d} at the FD time instant inside a set that is denoted as $\bar{X}_{k_d}$, i.e.,

$$x_{k_d} \in \bar{X}_{k_d}. \tag{17}$$

Remark 3.4 *In order to introduce the principle of the proposed FI method, for simplicity, we do not explain at this moment how to obtain $\bar{X}_{k_d}$. Instead, the details about $\bar{X}_{k_d}$ will be presented in Section 4.*

In order to isolate a fault during the transition induced by the fault, one initializes a set-based dynamics at time instant k_d, i.e.,

$$X_{k+1} = AX_k \oplus Bu_k \oplus W, \tag{18a}$$

$$Y_k = \mathbf{G}_f CX_k \oplus V, \tag{18b}$$

with

$$X_{k_d} = \bar{X}_{k_d} \text{ and } u_k \text{ for } k \geq k_d.$$

Afterwards, the state and output set sequences can be generated by (18). In addition to the generated state and output set sequences, due to (16), by using $\check{X}_{k_d+1} = X_{k_d+1}$ at time instant $k_d + 1$ to initialize the other set-based dynamics

$$\check{X}_{k+1} = A\check{X}_k \oplus BU_f \oplus W, \tag{19a}$$

$$\check{Y}_k = \mathbf{G}_f C\check{X}_k \oplus V, \tag{19b}$$

the other state and output set sequences can be obtained.

According to [15], the state set sequence generated by (19a) will converge to the mRPI set of the dynamics (13) with respect to $u_k \in U_f$ and $\omega_k \in W$, enter into and stay inside X_f. Correspondingly, the output set sequence generated by (19b) will finally converge to Y_f.

Remark 3.5 *According to Definitions 3.1 and 3.2, the mRPI set is contained in any RPI set. Thus, the state and output set sequences generated by (19a) and (19b) will enter into X_f and Y_f, respectively.*

Proposition 3.2 *Given the plant (1) and let (18) and (19) be initialized by $X_{k_d} = \bar{X}_{k_d}$ and $\check{X}_{k_d+1} = X_{k_d+1}$ at time instants k_d and $k_d + 1$, for all $k > k_d$, $X_k \subseteq \check{X}_k$ and $Y_k \subseteq \check{Y}_k$ will always hold.*

Proof : Comparing (18) with (19), it can be observed that (19) is a set-based dynamics of (18) by considering the input set U_f. Moreover, with X_{k_d+1} to initialize (19) at time instant $k_d + 1$, i.e., $X_{k_d+1} \subseteq \check{X}_{k_d+1}$, it can be obtained that, for all $k > k_d$, $X_k \subseteq \check{X}_k$ and $Y_k \subseteq \check{Y}_k$ will always hold. □

Proposition 3.3 *Given the plant (1) and the state and output set sequences generated by (18) and (19), $x_k \in X_k$ can hold for all $k > k_d$. If the plant is healthy, no components of y_k and Y_k can persistently satisfy $y_k(l) \in Y_k(l)$ $(l \in \mathbb{I} \setminus \{0\})$ for all $k > k_d$, while if the l-th fault occurs, the l-th components of y_k and Y_k can satisfy $y_k(l) \in Y_k(l)$ for all $k > k_d$ but all the other components of y_k and Y_k cannot satisfy the similar inclusions.*

Proof : First, due to (16) and (17), comparing (1) and (18), $x_k \in X_k$ will hold for all $k > k_d$. Second, under Proposition 3.2, comparing (19) with (18), X_k and Y_k will finally converge to X_f and Y_f and remain inside, respectively. Considering Y_f^0, Y_f^i and Y_f, for the l-th mode, i.e., $\mathbf{G}$ in (1b) takes a value inside $\mathbf{G}_l$ $(l \neq 0)$, under Proposition 3.1, starting from $k = k_d$, only $y_k(l) \in Y_k(l)$ will hold for all $k > k_d$ with $X_{k_d} = \bar{X}_{k_d}$, on the other hand, all the other components of y_k do not lead to the same conclusion because only the l-th component of y_k is affected by the l-th fault while all the others are not affected by the l-th fault. For the healthy mode, since all the components of Y_f^0 are separate from the corresponding components of Y_f, respectively, no components of y_k can persistently be contained by the corresponding interval of Y_k for all $k > k_d$. □

Thus, under Propositions 3.1, 3.3 and Assumption 3.1, if a considered fault is detected, using the output set sequence generated by (18), the fault can be isolated by testing whether or not

$$y_k(l) \in Y_k(l),\ k > k_d \tag{20}$$

is violated for all $l \in \mathbb{I} \setminus \{0\}$ in real time. By the real-time testing of (20) for all the components, one can obtain the following FI criteria:

- if the plant recovers to the healthy mode after functioning in a faulty mode, for $k > k_d$, by testing (20), at a time instant, if all the output components violate (20), it implies that the healthy mode is isolated at this time instant.
- if the plant changes into another fault after functioning in a faulty mode or the healthy mode, only the output component corresponding to the current mode can always respect (20) while all the others will finally diverge from their corresponding 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.

Remark 3.6 *The proposed FI method is based on a precondition that the MPC controller is always feasible after the input-constraint switching. This condition will be detailedly explained in Section 4.*

4 Fault-tolerant Control

This section first proposes a pragmatic state-estimation method for the proposed FTC scheme by using the state-estimation sets from interval observers and presents ways to guarantee the MPC feasibility and system-constraint satisfaction. Additionally, this section also describes an FTC algorithm to explain the proposed FTC scheme from a global point of view.

4.1 Robust State Estimation

For the proposed FTC scheme, in the i-th sensor mode, if no fault is detected, the MPC controller (8) is used to robustly control the closed-loop system to reach the i-th output setpoint y_i^*. According to the proposed active FI approach in the previous section, if a fault is detected, the active FI procedure is triggered at the FD time instant by adjusting the input and terminal state constraints of the MPC controller (8) from U and X_M to U_f and X_{M_f}, respectively. By means of this active FI method, the fault can be isolated and simultaneously, the controller can be reconfigured with the state-input setpoint pair and interval observer corresponding to this new mode (healthy or faulty). Note that, in order to obtain an expected performance, at the FI time instant, the input and terminal state constraints of the MPC controller are adjusted back to U and X_M again during the operation of the new mode, respectively.

Remark 4.1 *The aforementioned set X_{M_f} for active FI should the MRCI set of the dynamics (1a) under the constraints $x_k \in X$ and $u_k \in U_f$.*

As in (8), to implement the proposed FTMPC scheme, a basic condition is to construct proper state estimations for the MPC controller. The state estimations should be able to guarantee the feasibility of open-loop optimization problem. Considering that, under the constraints (2), the MRCI set X_M can be constructed for the dynamics (1a) and one can obtain Proposition 4.1.

Proposition 4.1 *Let X_M, the terminal constraint of the MPC controller (8), be defined as the MRCI set for the dynamics and state-input constraints (2). Then, if the initial state is inside X_M and the state measurements are available for updating the MPC controller, the system states can always be confined inside X_M and the recursive feasibility of MPC optimization problem can be ensured.*

Proof : This result can be obtained using the definition of the MRCI set and its properties. □

Proposition 4.1 is based on an ideal situation that the system states are completely measurable.Unfortunately, it is impossible to obtain the real states if the system is under the effect of process disturbances and measurement noises. Instead, one has to estimate the system states and use the state estimations to update the MPC controller for the real-time generation of control actions. In order to guarantee the feasibility with state estimations, one still uses the MRCI set X_M as the terminal state constraint during the steady-state operation. Furthermore, the state estimations can be constructed based on the conclusion in Proposition 4.2.

Proposition 4.2 *As long as the MPC controller (8) is updated by a point inside X_M at each time instant, i.e., $\hat{x}_k \in X_M$, the feasibility of the receding horizon optimization is preserved such that the generated control actions always satisfy the input constraint, i.e., $u_k \in U$.*

Proof : Since X_M is the MRCI set, (8) is always feasible if $\hat{x}_k \in X_M$ and the feasibility of optimization problem always implies that the generated control actions satisfy $u_k \in U$. □

For the system with disturbances and noises, even though the feasibility of MPC open-loop optimization problem can be guaranteed, it only implies that one can guarantee the input-constraint satisfaction and the state constraint may still be violated. The reason is that, under the effect of disturbances and noises, the state estimations always have errors, which means that the generated control actions (based on those state estimations) may not be able to steer the states to satisfy the constraints. Thus, in order to guarantee that the system states are always inside X, one makes Assumptions 4.1 and 4.2.

Assumption 4.1 *The mRPI set, denoted as X_m, with respect to unknown but bounded signals $u_k \in U$ and $\omega_k \in W$ for the dynamics (13), is contained in the state-constraint set X, i.e., $X_m \subseteq X$.*

Assumption 4.2 *There exists a scalar $\alpha \geq 1$ such that the initial state x_0 satisfies $x_0 \in \bar{X} = \alpha X_m$ and $\bar{X} \subseteq X_M$.*

Under Assumptions 4.1 and 4.2, $\bar{X}$ is an RPI set corresponding to additive uncertainties $u_k \in U$ and $\omega_k \in W$ for the dynamics (13) due to the fact that the positive invariance is preserved by scaling in the case of linear time-invariant dynamics. Thus, as long as $u_k \in U$ holds, the system states always stay inside $\bar{X}$ if the previous states are also inside $\bar{X}$.

Furthermore, if the system is in the steady-state operation of the i-th mode, the i-th interval observer can estimate sets containing the states in real time, i.e.,

$$x_k \in \hat{X}_k^i.$$

Thus, based on the state inclusions of the sets $\bar{X}$ and $\hat{X}_k^i$, one has

$$x_k \in \bar{X} \cap \hat{X}_k^i. \tag{21}$$

In this paper, for practical reasons, the following pragmatic method is proposed to obtain the state estimation for the MPC controller (8) during the steady-state operation of the i-th sensor mode

$$\hat{x}_k = \text{center}(\bar{X} \cap \hat{X}_k^i), \tag{22}$$

where center$(\cdot)$ denotes the center of a set. Considering that the intersection of zonotopes is not always a zonotope. In the case that the set $\bar{X} \cap \hat{X}_k^i$ is not centered, center$(\bar{X} \cap \hat{X}_k^i)$ represents the center of the largest inscribed hyperbox in $\bar{X} \cap \hat{X}_k^i$. (the hyperbox is an interval vector whose elements are intervals and center$(\bar{X} \cap \hat{X}_k^i)$ is the middle-point vector of the interval vector).

Remark 4.2 *Theoretically, any point inside the set $\bar{X} \cap \hat{X}_k^i$ can be used to update the MPC controller and preserve its recursive feasibility. For simplicity, the proposed approach chooses the center of the intersection as in (22). Thus, if better performance can be obtained by choosing another point in $\bar{X} \cap \hat{X}_k^i$, it is allowed under the framework of the proposed FTC scheme.*

Proposition 4.3 *Under Assumptions 4.1 and 4.2, the MPC controller (8) with the state estimation (22) is recursively feasible during the steady-state operation. Moreover, the states x_k are always confined inside $\bar{X}$.*

Proof : Under Assumption 4.1 and 4.2, it is known that $\bar{X}$ is contained inside X_M, which implies that $\hat{x}_k \in X_M$ holds. At each time step, by using (22), the MPC controller (8) is always feasible. Moreover, as long as the MPC controller is always feasible, $u_k \in U$ always holds, which always implies $x_k \in \bar{X} \subseteq X$. □

When using the state estimation (22) to update the MPC controller, there always exist state estimation errors, which are defined as

$$\tilde{x}_k = x_k - \hat{x}_k. \tag{23}$$

Moreover, since both x_k and $\hat{x}_k$ are bounded by the intersection $\bar{X} \cap \hat{X}_k^i$, $\tilde{x}_k$ will also belong to a bounding set. In the worst case (i.e., $\bar{X}$ coincides with $\hat{X}_k^i$), the bound of $\tilde{x}_k$ can be obtained as

$$\tilde{x}_k \in \bar{X} \oplus (-\bar{X}). \tag{24}$$

Note that because the coincidence of $\bar{X}$ and $\hat{X}_k^i$ is a low probability event, the real-time bound of $\tilde{x}_k$ is generally less conservative than (24). Since it is assumed that the plant is stable as in Assumption 2.1 (this assumption is necessary to assure the existence of the RPI sets of the system), the bounding of $\tilde{x}_k$ implies the system stability with the state estimation (22).

4.2 Fault-tolerant Control

As an important part of the proposed FTC strategy, it has been emphasized that, once a fault (indexed by $j \neq i$) is detected at time instant k_d, the constraints of the MPC controller will be adjusted from U and X_M to U_f and X_{M_f} to start up the proposed active FI mechanism to isolate the fault. Then, after FI, the proposed fault-tolerant mechanism will be further initiated to tolerate the fault.

Proposition 4.4 *Under Assumptions 3.1 and 4.1, the mRPI set, denoted as X_{m_f}, for the dynamics (13) corresponding to $u_k \in U_f$ is contained in the set X_m. Moreover, X_{M_f} is an RCI set corresponding to $u_k \in U$.*

Proof : Due to $U_f \subseteq U$, the mRPI set for the dynamics (13) corresponding to $u_k \in U_f$ is contained in the mRPI sets with respect to $u_k \in U$. Due to $\bar{X} \subseteq X$, 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 under $u_k \in U$, which indicates $X_{M_f} \subseteq X_M$. □

During active FI, the constraints $x_k \in X_{M_f}$ and $x_k \in \hat{X}_k^i$ may be violated because the mode has changed and the obtained information is corrupted, which implies that (22) may not guarantee the feasibility of MPC optimization problem after a mode changing. Thus, it is necessary to propose a new state-estimation strategy to update the MPC controller for guaranteeing both active FI and feasibility during the transient-state operation induced by the mode changing. Thus, during active FI, different from (22), a pragmatic state-estimation method to satisfy the input constraints and serve the FI objectives is proposed as

$$\hat{x}_k = \text{center}(X_{M_f}). \tag{25}$$

Note that, during the FI phase, in order to establish the FI conditions on-line, one has to satisfy $u_k \in U_f$ for $k \geq k_d$. According to the proposed FI approach, at the FD time k_d, one adjusts the input and terminal constraints from U and X_M to U_f and X_{M_f}, respectively. But, if at the FD time k_d+1, $\hat{x}_{k_d+1} = \text{center}(\bar{X} \cap \hat{X}_{k_d+1}^i)$ is outside X_{M_f}, i.e., $\hat{x}_{k_d} \notin X_{M_f}$, the MPC controller may become infeasible. Thus, in order to avoid this problem, one proposes to use (25) as a pragmatic state-estimation method during the whole FI phase.

Remark 4.3 *Any point inside X_{M_f} can be used as the state estimation. But for simplicity, the center is used. However, one can also select different points inside X_{M_f} instead of the center as the state estimation according to possible requirements such as energy constraints or similar.*

By using (25), during the active FI phase, the feasibility of MPC open-loop optimization problem can always be guaranteed, which implies the satisfaction of the FI conditions presented in Proposition 3.1 on-line. It should be considered that when using the state estimations (25) to update the MPC controller instead of using the real states, there always exist errors between the estimations and real states. In spite of the errors, there are several reasons that support the use of this pragmatic strategy as follows:

- as a consequence of using (25) to initialize the MPC controller during the period from FD to FI, the generated control signal u_k will be constant during the transition. Since the plant is stable (see Assumption 2.1), the state estimation errors will not grow unbounded and the system remains stable in the BIBO (bounded-input, bounded-output) sense.
- during active FI, the feasibility of MPC open-loop optimization problem implies $u_k \in U_f$. Thus, the system states finally converge to X_f and stay inside, which proves the boundedness of state estimation errors.

- the proposed FI strategy can isolate faults and reconfigure the system during the transition, which implies that the use of (25) only persists a short time. Generally, the short FI time implies the limiting of the effect of state estimation errors.

Algorithm 1: FTC algorithm

```
Initialization (system mode $i$, interval observers, state estimator, etc);
At time instant $k$: FD $\leftarrow$ FALSE, FI $\leftarrow$ FALSE, $\mathbf{0} \in R_k^{ii}$, $\hat{x}_k \leftarrow$ center($\bar{X} \cap \hat{X}_k^i$), $\mathbb{I}_i$=$\mathbb{I} \setminus \{i\}$;
(Fault detection)
while FD $\neq$ TRUE do
  $k \leftarrow k+1$;
  Obtain $R_k^{ii}$;
  if $\mathbf{0} \notin R_k^{ii}$ then
    FD $\leftarrow$ TRUE;
  end if
end while
(Fault isolation)
At time instant $k_d$:
1. Adjust $U$ and $X_M$ to $U_f$ and $X_{M_f}$;
2. $\hat{x}_k \leftarrow$ center($X_{M_f}$);
3. Initialize (18) with $\bar{X}_{k_d} = X_M$;
while FI $\neq$TRUE do
  $k \leftarrow k+1$;
  Obtain $y_k$, $Y_k$;
  for $l \in \mathbb{I}_i$ do
    if $y_k(l) \notin Y_k(l)$ then
      Remove $l$ from $\mathbb{I}_i$;
    end if
    if Length($\mathbb{I}_i$)=1 then
      $f \leftarrow \mathbb{I}_i$;
      Break;
    end if
  end for
end while
(Fault-tolerant control)
At time instant $k_i$:
1. Adjust $U_f$ and $X_{M_f}$ to $U$ and $X$;
2. Choose setpoint pair $(x_f^*, u_f^*)$;
3. Select interval observer $f$;
for $k \geq k_i$ do
  if $\bar{X} \cap \hat{X}_k^f \neq$ Empty then
    $\hat{x}_k \leftarrow$ center($\bar{X} \cap \hat{X}_k^f$);
  else
    $\hat{x}_k \leftarrow$ center($X_{M_f}$);
  end if
end for
return
```

The aforementioned points can prove the effectiveness of the FI mechanism. Moreover, for the proposed FTC scheme, if one assumes that a fault is isolated at time instant k_i, the MPC constraints will be adjusted back to U and X_M from U_f and X_{M_f} at time instant k_i for making full use of the potential control performance of the scheme, respectively.

Proposition 4.5 *At the FI time k_i, $x_{k_i} \in \bar{X} \subseteq X_M$ holds, and as long as the MPC controller is feasible, $x_k \in X_M$ will always hold for all $k \geq k_i$.*

Proof : Under Assumption 4.2, $x_k \in \bar{X} \subseteq X_M$ during the steady-state operation. At the FD time k_d, although the constraints U and X_M are adjusted to U_f and X_{M_f}, respectively, one still has $u_k \in U_f \subseteq U$ with (25), which implies that the system states are contained in $\bar{X}$. At the FI time k_i when the constraints are adjusted back to U and X_M, $x_{k_i} \in \bar{X}$ still holds and the feasibility of (8) guarantees $x_k \in X_M$ for all $k \geq k_i$. □

Remark 4.4 *Under Assumptions 4.1 and 4.2, $x_k \in \bar{X}$ and $x_k \in X_M$ can always hold based on Propositions 4.3 and 4.5. Thus, the set $\bar{X}_{k_d}$ (introduced in Section 3.2.2) can be defined as $\bar{X}_{k_d} = \bar{X}$ or $\bar{X}_{k_d} = X_M$. Additionally, without Assumptions 4.1 and 4.2, a more conservative alternative can be $\bar{X}_{k_d} = X$. Note that, any of these three sets can be used to do the initialization for the proposed FI method.*

It is assumed that the j-th (healthy or faulty) mode ($j \neq i$) is isolated, at time instant k_i, the system should be reconfigured. Furthermore, under Proposition 4.5, 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 as the estimation of the current state, otherwise, (25) should continue to be used. Note that, after reconfiguration, it is guaranteed that, along system functioning, $\bar{X} \cap \hat{X}_k^j \neq \emptyset$ will persistently hold after a specific time instant as long as no any other mode switching occurs.

Remark 4.5 *Even though after the system is reconfigured at time instant k_i, one cannot assure that, at the first several time instants after $k = k_i$, $\bar{X} \cap \hat{X}_k^j$ is always non-empty due to a transition before entering the steady-state operation of the j-th mode. Thus, during the transition, one can still use (25) as a remedy if $\bar{X} \cap \hat{X}_k^j$ is empty. However, after the transition, $\bar{X} \cap \hat{X}_k^j$ can always be non-empty and be used for state estimations during the new steady-state operation.*

In order to summarize the proposed FTC scheme, the whole FTC procedure has been formalized as Algorithm 1. Note that, in Algorithm 1, Length$(\cdot)$ denotes to obtain the number of elements in a set, Break is to terminate a loop and $f \leftarrow \mathbb{I}_i$ means to assign the only remaining element inside $\mathbb{I}_i$ to f. Additionally, although this paper mainly focuses on FDI, the sensor recovery process from healthy to faulty can also be detected and isolated as explained in Section 3.2.2. Thus, the terms *fault detection and isolation* and *fault-tolerant control* generally describe all the considered mode transition (from healthy to faulty, faulty to faulty and faulty to healthy).

5 Illustrative Example

In this section, an electric circuit taken from [14] is used as the case study of the proposed FTC approach. This circuit is shown in Figure 2, where the inputs are the power sources $V_1(t)$ and $V_2(t)$, the states are composed of the capacitor voltage $v_C(t)$ and the inductor currency $i_L(t)$, and the outputs are the voltages of the capacitor and the resistor R_3.

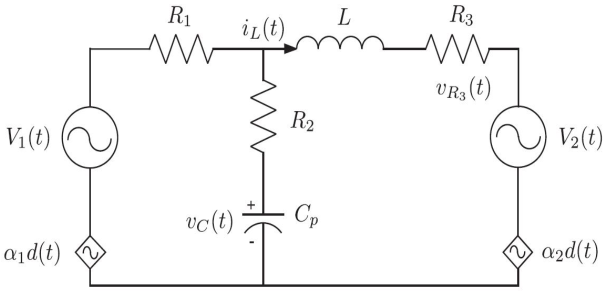

Figure 2: Circuit chart

The dynamics of this circuit are given in [14], whose system matrices are as follows:

$$A = \begin{bmatrix} -\frac{1}{R_{eq}C_p} & \frac{R_1}{R_{eq}C_p} \\ \frac{1}{L}(\frac{R_2}{R_{eq}} - 1) & -\frac{1}{L}(\frac{R_1R_2}{R_{eq}} - R_3) \end{bmatrix}, B = \begin{bmatrix} \frac{1}{R_{eq}C_p} & 0 \\ -\frac{R_2}{LR_{eq}} & \frac{1}{L} \end{bmatrix},$$

$$E = \begin{bmatrix} \frac{\alpha_1}{R_{eq}C_p} \\ \frac{1}{L}(\alpha_2 - \frac{R_2}{R_{eq}}\alpha_1) \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \\ 0 & R_3 \end{bmatrix},$$

where the values of the relevant parameters are given as $R_1 = 30\Omega$, $R_2 = 1000\Omega$, $R_3 = 20\Omega$, $L = 80$mH, $C_p = 50\mu$F, $R_{eq} = R_1 + R_2$ and $\alpha_1 = \alpha_2 = 1$. The only difference of this current case study from that in [14] is that the measurement noises are considered in this example in order to better illustrate the proposed FTC scheme. With a sampling time of 1/15s, the dynamics of the circuit can be discretized as

$$x_{k+1} = A_d x_k + B_d u_k + E_d w_k, \tag{26a}$$

$$y_k = \mathbf{G} C_d x_k + \eta_k, \tag{26b}$$

with

$$A_d = \begin{bmatrix} 0.8706 & 3.8835 \\ -0.0024 & 0.2395 \end{bmatrix}, B_d = \begin{bmatrix} 0.1294 & 0.0667 \\ -0.0809 & 0.0833 \end{bmatrix}, E_d = \begin{bmatrix} 0.1294 \\ 0.0024 \end{bmatrix}, C_d = \begin{bmatrix} 1 & 0 \\ 0 & 20 \end{bmatrix},$$

where $\mathbf{G}$ models sensor modes. In this example, three modes are considered, which are denoted as $\mathbf{G}_0$, $\mathbf{G}_1$ and $\mathbf{G}_2$, respectively. Moreover, in (26), the process disturbances and measurement noises of the circuit are bounded, which are denoted as $|\omega| \leq 1.5$ and $|\eta| \leq \begin{bmatrix} 0.1 & 0.1 \end{bmatrix}^T$. Besides, all the relevant designing parameters in this example are presented as follows:

- observer gains[3]:

$$L_0 = \begin{bmatrix} 0.4706 & 0.1942 \\ -0.0024 & -0.013 \end{bmatrix}, L_1 = \begin{bmatrix} 9.4110 & 0.1942 \\ -0.0485 & -0.013 \end{bmatrix}, L_2 = \begin{bmatrix} 0.4706 & 3.8835 \\ -0.0024 & -0.2605 \end{bmatrix}.$$

- considered fault magnitudes:
  $\mathbf{G}_1 = \begin{bmatrix} [0, 0.1] & 0 \\ 0 & 1 \end{bmatrix}$, $\mathbf{G}_2 = \begin{bmatrix} 1 & 0 \\ 0 & [0, 0.1] \end{bmatrix}$, $\mathbf{G}_f = \begin{bmatrix} [0, 0.1] & 0 \\ 0 & [0, 0.1] \end{bmatrix}$.

- real fault magnitudes[4]: $G_1 = \begin{bmatrix} 0.05 & 0 \\ 0 & 1 \end{bmatrix}, G_2 = \begin{bmatrix} 1 & 0 \\ 0 & 0.05 \end{bmatrix}$.

- output setpoints: $y_0^* = \begin{bmatrix} 4 & 2 \end{bmatrix}^T, y_1^* = \begin{bmatrix} 0 & 2 \end{bmatrix}^T, y_2^* = \begin{bmatrix} 4 & 0 \end{bmatrix}^T$.

- state-input setpoint pairs:

$$u_0^* = \begin{bmatrix} 0.313 & 1.333 \end{bmatrix}^T, u_1^* = \begin{bmatrix} -2.313 & -1.333 \end{bmatrix}^T, u_2^* = \begin{bmatrix} 2.627 & 2.667 \end{bmatrix}^T,$$
$$x_0^* = \begin{bmatrix} 4 & 0.1 \end{bmatrix}^T, x_1^* = \begin{bmatrix} 0 & 0.1 \end{bmatrix}^T, x_2^* = \begin{bmatrix} 4 & 0 \end{bmatrix}^T.$$

- initial conditions: $x_0 = \begin{bmatrix} 0 & 0 \end{bmatrix}^T, \hat{X}_0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 0.1 & 0 \\ 0 & 0.1 \end{bmatrix} \mathbb{B}^2$.

- system constraints:
  $U = \{u : \begin{bmatrix} -3 & -3 \end{bmatrix}^T \leq u \leq \begin{bmatrix} 3 & 3 \end{bmatrix}^T\}$, $X = \{x : \begin{bmatrix} -20 & -10 \end{bmatrix}^T \leq x \leq \begin{bmatrix} 20 & 10 \end{bmatrix}^T\}$.

- input set for active FI: $U_f = \{u : \begin{bmatrix} 0 & 2 \end{bmatrix}^T \leq u \leq \begin{bmatrix} 1 & 3 \end{bmatrix}^T\}$.

- prediction horizon: $N = 2$,

- MPC controller parameters: $Q = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, R = \begin{bmatrix} 0.1 & 0 \\ 0 & 0.1 \end{bmatrix}. P = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

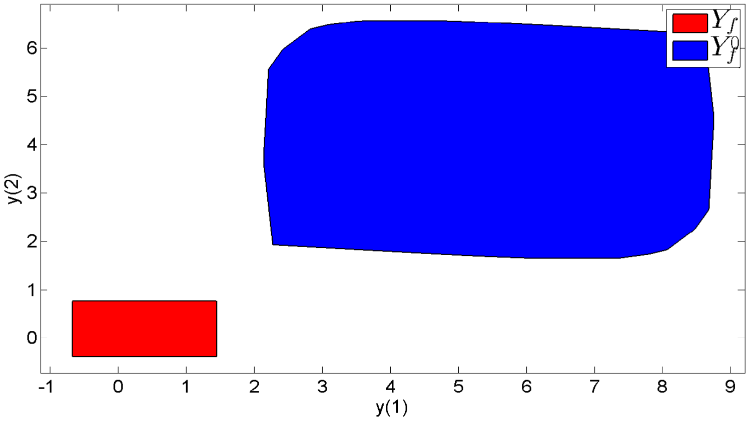

Figure 3: Output sets of active FI

For the three modes, three interval observers are designed as in (7). Considering that $u_k \in U_f$ and $\omega_k \in W$, the output sets corresponding to the FI conditions in Proposition 3.1 can be constructed, which are presented in Figure 3. Since Y_f is generated from the multiplication of an interval matrix and a zonotope, it is quite difficult to accurately compute it. Thus, as a pragmatic idea, a box outer-bounding Y_f (i.e., the red set in the figure) instead of Y_f is used to check the FI conditions. In Figure 3, it can be observed that two components of Y_f are disjoint from those of Y_f^0, respectively, which means that the considered sensor faults can be isolated by the proposed FI approach.

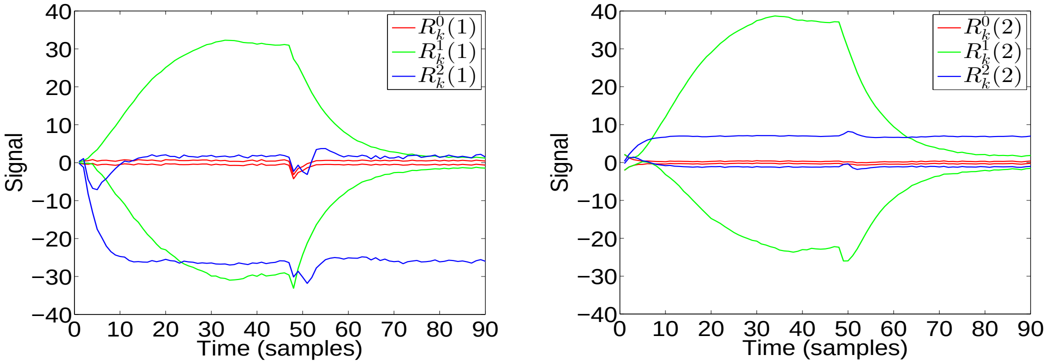

Figure 4: FD of fault 1

In this simulation, for simplicity, one only illustrates the process from the healthy mode to a faulty mode and omits the process of sensor recovery from a faulty mode to the healthy mode because they are using the same principle. Thus, the same scenario is defined for both faults: from time instants $k = 1$ to 45, the plant is healthy, while from time instants $k = 46$ to 90, a sensor fault occurs.

Remark 5.1 *In Figures 4 and 8, $R_k^i(1)$ and $R_k^i(2)$ denote the first and second components of R_k^i from the i-th interval observer at time instant k, respectively. For the remaining figures, the notations $Y_k(1)$, $Y_k(2)$, $y(1)$, $y(2)$, $x_k(1)$, $x_k(2)$, $u_k(1)$ and $u_k(2)$ have the similar meaning.*

The FD and FI simulation results of the first sensor fault are shown in Figures 4 and 5, respectively. In Figure 4, it is shown that a fault is detected at $k = 47$, i.e., $\mathbf{0} \notin R_{47}^0$. Then, the active FI process is started,

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

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

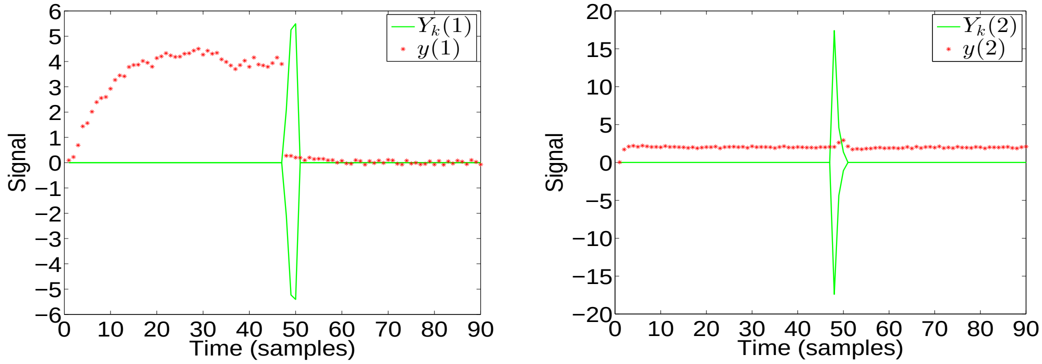

Figure 5: FI of fault 1

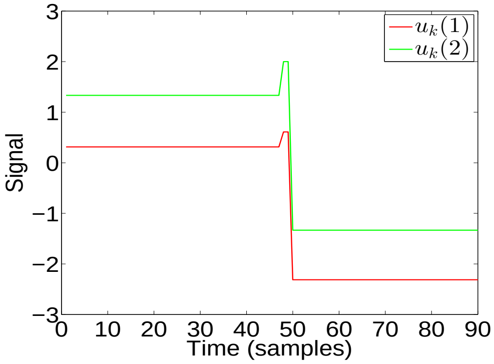

Figure 6: Control inputs of Scenario 1

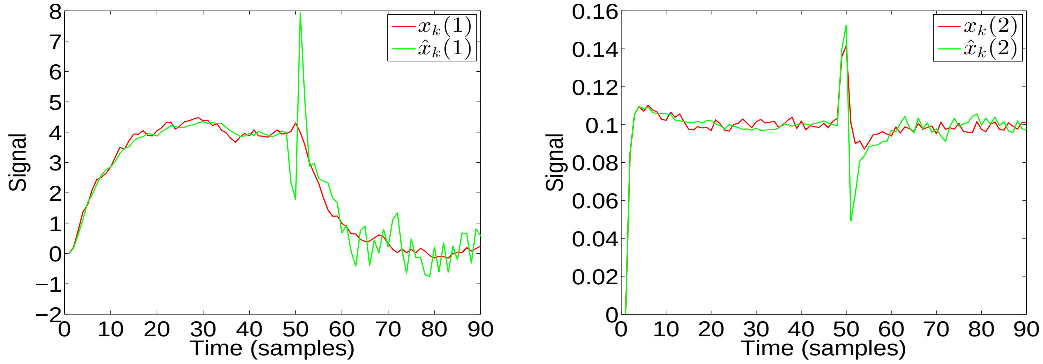

Figure 7: Comparison of states and state estimations 1

i.e., (18) is initialized and (20) is tested in real time for FI (see Figure 5). At $k = 50$, the first component of y_k respects its bound $Y_k(1)$, i.e., $y_{50}(1) \in Y_{50}(1)$, while the second component violates its bound, i.e., $y_{50}(2) \notin Y_{50}(2)$, which indicates that the first sensor fault is isolated. Finally, the first state-input setpoint pair is used for FTC at $k = 50$.

In Figure 5, before the occurrence of the first fault, it can be observed that the expected output y_0^* is well regulated (the outputs are shown in Figure 5 as the red stars), while after the first fault, we degrade the performance specification from y_0^* to y_1^*. Then, after system reconfiguration at $k = 50$, the output setpoint y_1^* can be well regulated as well. In Figure 6, the generated inputs u_k are presented, where we can see that the input constraints can be well satisfied during the whole process. Besides, in order to show the effectiveness of the proposed state-estimation method (22), a comparison between the real states and their estimations is shown in Figure 7.

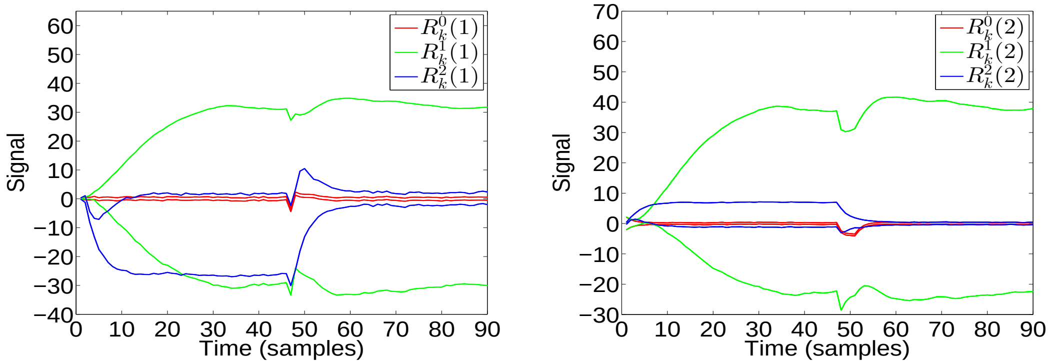

Figure 8: FD of fault 2

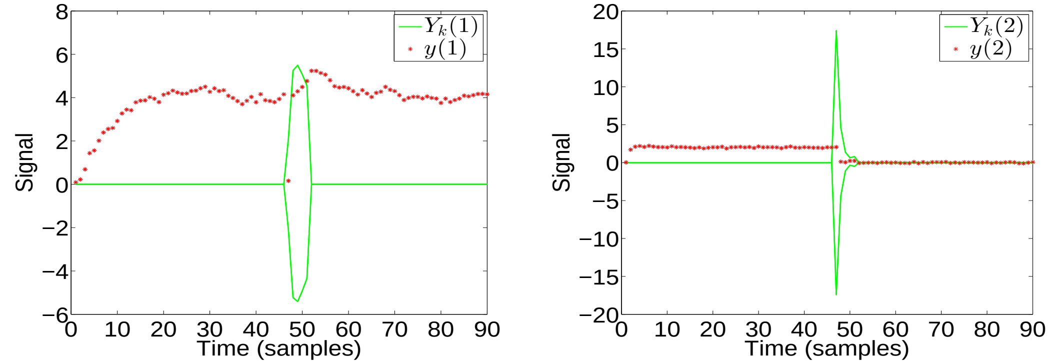

Figure 9: FI of fault 2

Similar to the first scenario, the FD and FI simulation results of the second fault are shown in Figures 8 and 9, respectively. In Figure 8, it is shown that a fault is detected at $k = 46$. In Figure 9, the second sensor fault is isolated at time instant $k = 51$ and simultaneously the controller is updated with the second state-input pair corresponding to the second scenario. Similarly, the outputs are shown in Figure 9 as the red stars, where y_0^* and y_2^* are well regulated before the second fault and after reconfiguration, respectively. The generated control inputs for the second scenario are shown in Figure 10, which presents that the input constraints are always satisfied. In Figure 10, during active FI, it is seen that only five control actions are generated and only five steps are needed to isolate the second fault. In Figure 11, a comparison between the real states and their estimations is shown. According to these results, we can see the effectiveness of the proposed sensor FTC scheme.

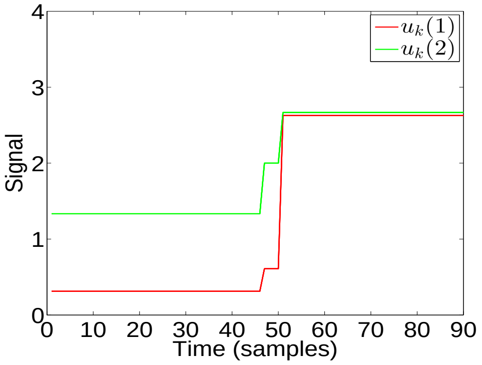

Figure 10: Control inputs of Scenario 2

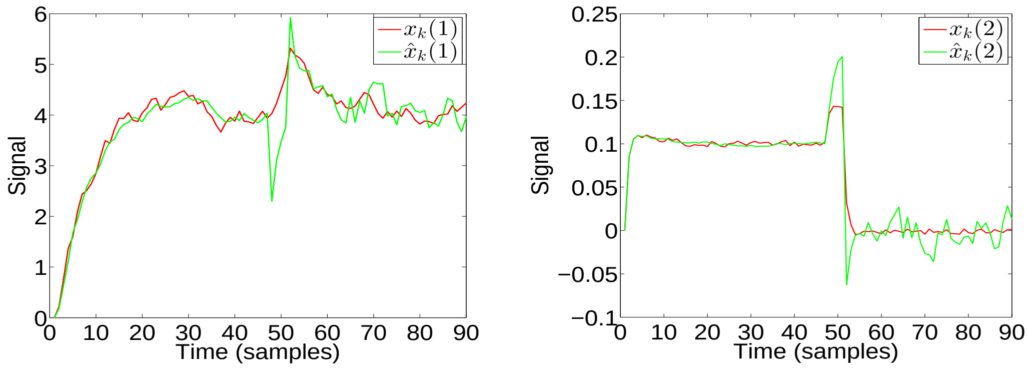

Figure 11: Comparison of states and state estimations 2

6 Conclusions

In this paper, a sensor and actuator FTC scheme using robust MPC, interval observer-based FD and set-based active FI is proposed. In this FTMPC scheme, the FI conditions are established on-line by the MPC controller. With MPC, in comparison with the passive methods, the FI conditions can be simplified by the active FI method proposed in this paper. In order to make the proposed FTMPC scheme work, one has to obtain the feasibility, stability and constraint satisfaction and also to propose a state-estimation method for the robust MPC controller. Currently, several pragmatic methods have been developed based on several assumptions to obtain the feasibility, stability, constraint satisfaction and state estimations such as (22), (25), Assumptions 2.1, 4.1 and 4.2. For example, for invariant set construction and feasibility guarantees, the proposed FTC scheme relies on Assumption 4.1. Thus, there still exists space to improve the performance of this FTMPC scheme and reduce different types of conservatism such as relaxing the assumptions and developing more efficient state-estimation methods during both transient-state and steady-state phases.

The main contribution of this paper has been to propose a novel FTMPC framework based on MPC and interval observers. Additionally, as aforementioned, a novel state-estimation method has been proposed to guarantee the recursive feasibility of MPC open-loop optimization problem. This means that, if better state-estimation approaches can be found, Assumption 4.1 can potentially be removed and the FTC scheme can further be improved with those state-estimation approaches. In the future research, aside the faulty state estimation improvements, the key points are to find better ways to relax the assumptions, apply U_f directly as the input-constraint set of the MPC controller during the active FI phase instead of using a fixed point inside U_f and develop a systematic method to compute the set U_f instead of the current trial and error method to find a satisfactory U_f.

Acknowledgements

This work has been supported by the DGR of Generalitat de Catalunya (SAC group Ref. Ref. 2014/SRG/374), European Commission through contract CICYT SHERECS DPI- 2011-26243 of the Spanish Ministry of Education, China Scholarship Council, CNRS-Supélec and Automatic Control Department, Supélec, France.

A Appendix

Property A.1 *Given two zonotopes* $X_1 = g_1 \oplus H_1\mathbb{B}^{r_1} \subset \mathbb{R}^n$ *and* $X_2 = g_2 \oplus H_2\mathbb{B}^{r_2} \subset \mathbb{R}^n$*, their Minkowski sum is* $X_1 \oplus X_2 = \{g_1 + g_2\} \oplus [H_1 \quad H_2]\mathbb{B}^{r_1+r_2}$*.*

Property A.2 *Given a zonotope* $X = g \oplus H\mathbb{B}^r \subset \mathbb{R}^n$ *and a suitable matrix* K*,* $KX = Kg \oplus KH\mathbb{B}^r$*.*

Property A.3 *Given a family of zonotopes denoted by* $X = g \oplus \mathbf{M}\mathbb{B}^r$ *(*$g \in \mathbb{R}^n$ *is a real vector and* $\mathbf{M} \in \mathbb{R}^{n\times r}$ *is an interval matrix), a zonotope inclusion* $\diamond(X)$ *is defined by*

$$\diamond(X) = g \oplus [mid(\mathbf{M}) \;\; H]\mathbb{B}^{r+n},$$

where H *is a diagonal matrix that satisfies*

$$H_{ii} = \sum\nolimits_{j=1}^{r} \frac{diam(\mathbf{M})_{ij}}{2}, i = 1, 2, \cdots, n,$$

where $diam(\cdot)$ *obtains the diameter of an interval matrix.*

Property A.4 *Given the dynamics* $X_{k+1} = \mathbf{A}X_k \oplus \mathbf{B}u_k$*, where* $\mathbf{A}$ *and* $\mathbf{B}$ *are interval matrices and* u_k *is the input at step* k*, if* X_k *is a zonotope with the center* g_k *and segment matrix* H_k*,* X_{k+1} *is bounded by*

$$X^e_{k+1} = g_{k+1} \oplus H_{k+1}\mathbb{B}^r,$$

with

$$\begin{aligned} g_{k+1} =& mid(\mathbf{A})g_k + mid(\mathbf{B}))u_k, \\ H_{k+1} =& [J_1 \quad J_2 \quad J_3], \\ J_1 =& seg(\diamond(\mathbf{A}H_k)), \\ J_2 =& \frac{diam(\mathbf{A})}{2} g_k, \\ J_3 =& \frac{diam(\mathbf{B})}{2} u_k, \end{aligned}$$

where $seg(\cdot)$ *obtains the segment (or generator) matrix of a zonotope.*

Property A.5 *Given a zonotope* $X = g \oplus H\mathbb{B}^r \subset \mathbb{R}^n$ *and an integer* s *(with* $n < s < r$*), denote by* $\hat{H}$ *the matrix resulting from the reordering of the columns of the matrix* H *in decreasing Euclidean norm.* $X \subseteq g \oplus [\hat{H}_T \quad Q]\mathbb{B}^s$ *where* $\hat{H}_T$ *is obtained from the first* $s - n$ *columns of matrix* $\hat{H}$ *and* $Q \in \mathbb{R}^{n\times n}$ *is a diagonal matrix whose elements are* $Q_{ii} = \sum_{j=s-n+1}^{r} \mid \hat{H}_{ij} \mid$*,* $i = 1, \ldots, n$*.*

References

[1] M. Abdel-Geliel, E. Badreddin, and A. Gambier. Application of model predictive control for fault tolerant system using dynamic safety margin. In *Proceedings of the American Control Conference*, Minneapolis, MN, USA, June, 2006.

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

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

[4] J.D. Boskovic and R.K. Mehra. Fault accommodation using model predictive methods. In *Proceedings of the American Control Conference*, volume 6, pages 5104–5109, Woburn, MA, USA, May, 2002.

[5] E.F. Camacho, T. Alamo, and D.M. de la Pena. Fault-tolerant model predictive control. In *Proceedings of the IEEE Conference on Emerging Technologies and Factory Automation (ETFA)*, Sevilla, Spain, September, 2010.

[6] F.A. de Almeida and D. Leissling. Fault-tolerant flight control system using model predictive control. In *Proceedings of the Brazilian Symposium on Aerospace Eng.& Applications*, São Paulo, Brazil, September 2009.

[7] D.A. Joosten, T.J.J. van den Boom, and T.J.J. Lombaerts. Fault-tolerant control using dynamic inversion and model-predictive control applied to an aerospace benchmark. In *Proceedings of the 17th IFAC World Congress*, Seoul, South Korea, July 2008.

[8] M. Kettunen and S-L. Jämsä-Jounela. Fault tolerant MPC with an embedded FDI system. In *Proceedings of the 1st IFAC Workshop on Applications of Large Scale Industrial Systems*, Helsinki, Finland, August 2006.

[9] 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.

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

[11] J.M. Maciejowski. *Predictive Control with Constraints.* Prentice Hall, 2002.

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

[13] R. Nikoukhah, S.L. Campbell, K.G Horton, and F. Delebecque. Auxiliary signal design for robust multimodel identification. *IEEE Transactions on Automatic Control*, 47(1):158–164, Jan 2002.

[14] 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.

[15] 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.

[16] M.C. De Oliveira, J.C. Geromel, and J. Bernussou. Extended h 2 and h norm characterizations and controller parametrizations for discrete-time systems. *International Journal of Control*, 75(9):666–679, 2002.

[17] D.M. Raimondo, R.D. Braatz, and J.K. Scott. Active fault diagnosis using moving horizon input design. In *Proceedings of the European Control Conference (ECC)*, Zürich, Switzerland, July 17-19 2013.

[18] D.M. Raimondo, G.R. Marseglia, R.D. Braatz, and J.K. Scott. Fault-tolerant model predictive control with active fault isolation. In *Proceedings of the International Conference on Control and Fault-Tolerant Systems (SysTol)*, pages 6567 – 6572, Nice, France, October 9-11 2013.

[19] S.V. Rakovic, E.C. Kerrigan, K.I. Kouramas, and D.Q. Mayne. Invariant approximations of the minimal robust positively invariant set. *Automatic Control, IEEE Transactions on*, 50(3):406 – 410, March 2005.

[20] Joseph K. Scott, Rolf Findeisen, Richard D. Braatz, and Davide M. Raimondo. Input design for guaranteed fault diagnosis using zonotopes. *Automatica*, 50(6):1580 – 1589, 2014.

[21] Florin Stoican, Sorin Olaru, María M Seron, and José A De Doná. Reference governor design for tracking problems with fault detection guarantees. *Journal of Process Control*, 22(5):829–836, 2012.

[22] Shengqi Sun, Liang Dong, Lin Li, and Shusheng Gu. Fault-tolerant control for constrained linear systems based on MPC and FDI. *International Journal of Information and Systems Sciences*, 4(4):512 –23, 2008.

[23] X. Yang and J.M. Maciejowski. Fault-tolerant model predictive control of a wind turbine benchmark. In *Proceedings of the 8th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, Mexico City, Mexico, August 2012.

[24] A. Yetendje, M. Seron, and J. De Doná. Robust multisensor fault tolerant model-following MPC design for constrained systems. *International Journal of Applied Mathematics and Computer Science*, 22(1):211–223, 2012.