Robust MPC design for fault tolerance of constrained multisensor linear systems

Alain Yetendje, Maria M. Seron, José A. De Doná

Abstract—In this paper, a robust fault-tolerant control strategy for constrained multisensor linear systems, subject to sensor faults and in the presence of bounded state and output disturbances is proposed. The scheme verifies that for each sensors-estimator combination, suitable residual variables lie inside pre-computed sets and selects the more appropriate combination based on a chosen criterion. An active fault tolerant output feedback controller yields an MPC-based control law and by means of the notion of “tube” of trajectories, we ensure robust closed-loop exponential stability and good performance in the fault-free case and under the occurrence of abrupt sensor faults.

I. INTRODUCTION

Model predictive control (MPC) is one of the most successful approaches for designing non-linear controllers for linear systems with constraints. The idea of developing fault tolerant control (FTC) approaches based on MPC control has been discussed in the last few years within the research community. In [3], the foundations of a possible theory were discussed and simulations on an aircraft system showed that MPC offers the possibility to achieve fault tolerance by reconfiguring the controller in response to a fault. In [4], it was shown that when knowledge of the fault is available one can increase fault tolerance by modifying parameters of the optimisation problem which is solved at each sampling instant in MPC. Faults that affect the internal model or system constraints can be incorporated into an MPC controller in a straightforward way. Other possibilities consist of degrading the control objective by changing the constraints in order to represent certain kind of faults, and/or modifying the internal system model used by the MPC controller. In [8], a fault tolerant scheme using the explicit characterisation of the stability region, together with the constraint handling capabilities and optimality properties of MPC is proposed for nonlinear systems subject to uncertainty, constraints, and faults in the control actuators. In [9], the problem of achieving fault tolerance in the presence of uncertainty was addressed, where a robust hybrid predictive controller was used to characterise the stability region under each control configuration. Most of these approaches tackle the problem of FDI and reconfiguration separately and are usually carried out on simulation examples, experimental systems, or real applications, but very few of them provide analytical proofs that guarantee fault tolerance for constrained systems.

In this paper, we consider a sensor FDI strategy which employs a bank of sensors-estimator combinations and verifies that for each of these combinations, the updated estimation tracking errors lie inside pre-computed “healthy” sets. Those combinations for which the latter set-containment property holds are considered within a chosen selection criterion (e.g.: switching of sensors-estimator combinations [12], sensors-estimation fusion [1]), to be used by the controller. We propose an active fault-tolerant control scheme based on the output feedback problem for constrained linear discrete-time systems subject to state and measurement disturbances [7]. The output feedback controller yields a “tube”, whose center is generated by using conventional MPC with tighter constraints on the nominal system, and whose size is restricted by using a local feedback that attempts to steer all trajectories of the uncertain system to the central trajectory [10]. Proofs of fault tolerance of the resulting closed-loop system and robust exponential stability of a robust invariant set are given under a set of conditions on the system parameters (disturbance bounds, etc.) in the fault-free case and under the occurrence of abrupt sensor faults.

II. PLANT AND TRACKING OBJECTIVE

Consider the discrete-time linear time-invariant plant

\[ x^+ = Ax + Bu + Ew \]  

(1)

where \( x \in \mathbb{R}^n \) is the system state, \( u \in \mathbb{R}^m \) is the control input, \( x^+ \in \mathbb{R}^n \) is the successor state and \( w \in \mathbb{R}^r \) is an unknown state disturbance. \( A \in \mathbb{R}^{n \times n}, B \in \mathbb{R}^{n \times m}, E \in \mathbb{R}^{n \times r} \) are constant matrices, the pair \((A, B)\) is assumed to be controllable. We assume that \( w \in \mathbb{W} \subset \mathbb{R}^r \), where \( \mathbb{W} \) is a known C-set\(^1\).

The control objective is for the state \( x_t \) to track the setpoint \( x_s \) such that the controlled plant (1) fulfills hard constraints \( x \in \mathcal{X}, u \in \mathcal{U} \), where \( \mathcal{X} \subset \mathbb{R}^n \) is a closed set that contains \( x_s \) in its interior and \( \mathcal{U} \subset \mathbb{R}^m \) is a compact set that contains \( u_t \) in its interior, where \( x_t \) and \( u_t \) satisfy \( x_t = Ax_t + Bu_t \).

III. MEASUREMENT SYSTEM AND SENSOR FAULT MODEL

We consider a bank of output equations that combine several sensor measurements as follows:

\[ y_i = \Pi_i(C_ix + \eta_i) + (I_p - \Pi_i)\eta_i^F \]  

(2)

for \( i = 1, \ldots, M \), where \( y_i \in \mathbb{R}^p \) is the measured output of the \( i \)-th group of sensors; \( \eta_i, \eta_i^F \in \mathbb{R}^p \) are unknown measurement noises, and \( I_p \) is the \( p_i \times p_i \) identity matrix. \( C_i \in \mathbb{R}^{p_i \times n} \) are constant matrices, and \((A, C_i)\) are observable.

\(^1\)A C-set is a compact, convex set that contains the origin in its (non empty) interior.
The measurement noises $\eta_i, \eta_{F}^i$ are known to the extent that they lie, respectively, in the C-sets $N_i \subset \mathbb{R}^{p_i}$ and $N_{F}^i \subset \mathbb{R}^{p_i}$ for $i = 1, \ldots, M$. Although not explicitly considered in this paper, sensor bias can also be included in the foregoing analysis by considering the “under-fault” noises $\eta_{F}^i$ to have the form $\eta_{F}^i = \eta_{i, \text{bias}} + \eta_{F}^i$ where $\eta_{i, \text{bias}}$ is constant and $\eta_{F}^i$ belongs to a known C-set.

The fault matrix $\Pi_i \in \mathbb{R}^{p_i \times p_i}$ in (2) characterizes the sensor fault situation, and is described as follows:

\[
\Pi_i = \begin{cases} 
I_{p_i} & \text{if all sensors are healthy} \\
\text{diag} \{ \pi_1, \ldots, \pi_{p_i} \} & \text{otherwise}
\end{cases} \tag{3}
\]

where $\pi_j \in [0, 1]$, for $j = 1, \ldots, p_i$. From (2), $\pi_j < 1$ indicates that the $j$th sensor of the $i$th sensor group has lost effectiveness, and $\pi_j = 0$ signifies outage of the sensor.

IV. ESTIMATORS

In accordance with the measurement equations (2), we consider a bank of $M$ estimators, where each estimator is associated with one group of sensors and is designed in order to estimate the states of the system (1). The estimators are described by the following equations, for $i = 1, \ldots, M$:

\[
\hat{x}_i^+ = A \hat{x}_i + Bu + L_i[y - C_i \hat{x}_i] \tag{4}
\]

\[
\hat{x}_{i}^{UP} = \hat{x}_i + G_i[y - C_i \hat{x}_i] \tag{5}
\]

where $\hat{x}_i \in \mathbb{R}^n$ is the current estimator state, and $\hat{x}_{i}^{UP} \in \mathbb{R}^n$ is the updated estimator state. The estimator gains $L_i \in \mathbb{R}^{n \times p_i}$ are such that:

\[
A_{L_i} \triangleq A - L_i C_i \tag{6}
\]

are Schur matrices, for $i = 1, \ldots, M$. The update gains $G_i \in \mathbb{R}^{n \times p_i}$ are arbitrary real matrices of appropriate dimensions.

Provided the $i$th group of sensors is “healthy” (i.e., $\Pi_i = I_{p_i}$), the estimated states $\hat{x}_i$ satisfy, using (2), (4)

\[
\hat{x}_i^+ = A \hat{x}_i + Bu + L_i[y - C_i \hat{x}_i] \tag{7}
\]

with the state estimation error

\[
\tilde{x}_i = x - \hat{x}_i \tag{8}
\]

satisfying

\[
\tilde{x}_i = A_{L_i} \tilde{x}_i + (Ew - L_i \eta_i) \tag{9}
\]

V. ESTIMATE RECONFIGURATION

Every estimator (4), (5) independently estimates the states of system (1) and gives the unbiased updated state estimate $\hat{x}_{i}^{UP}$ to be evaluated by an FDI mechanism. Only “healthy” updated estimates, as diagnosed by the FDI unit (described in Section IX below) are used at the reconfiguration stage, which will then provide an adequate “reconfigured” updated estimate for use by the feedback controller. We consider two different methodologies for the reconfiguration stage. The first methodology switches between the available sensors-estimator combinations by means of a suitable criterion [12]. In the second methodology, employed by the authors in [1], the estimates deemed “healthy” by means of the FDI test are fused based on an optimal fusion steady-state Kalman filter. The choice of the reconfiguration technique is left at the user discretion, therefore for the remainder of the paper, the “reconfigured” updated estimate provided by either technique is generically denoted by

\[
x^{UP} = \sum_{\ell \in H} \lambda_{\ell} \hat{x}_{\ell}^{UP} \tag{10}
\]

where $H$ is defined as

\[
H \triangleq \{ \ell \in \{1, \ldots, M\} : \text{sensor group } \ell \text{ is diagnosed as healthy} \} \tag{11}
\]

and $\sum_{\ell \in H} \lambda_{\ell} = 1$. We will later explain in Section IX how the set $H$ is constructed and updated at each time step by the FDI unit. For details on how the coefficients $\lambda_{\ell}, \ell \in H$, are computed see [12], for switching; and [1], for fusion. For each possible $H \in \mathbb{P}_M$ (the set of all subsets of $\{1, \ldots, M\}$), the corresponding coefficients $\lambda_{\ell}, \forall \ell \in H$, can be precomputed and stored so that the on-line reconfiguration task simply amounts to employing the pre-stored set of coefficients corresponding to the current index set $H$.

For future reference, we define the “reconfigured” updated state estimation error as

\[
x^{UP} - \hat{x} = \sum_{\ell \in H} \lambda_{\ell} (\hat{x}_{\ell}^{UP} - \hat{x}_{\ell}) \tag{12}
\]

where we have used (2) with $\Pi_{\ell} = I_{p_{\ell}}$, (5), (8), and (10).

VI. ROBUST TUBE-MPC CONTROLLER AND TRACKING ERRORS

Following [10], we consider as “reference model” the nominal system obtained from (1) by neglecting $w$

\[
\hat{x}^+ = A \hat{x} + B \bar{u} \tag{13}
\]

where $\hat{x} \in \mathbb{R}^n$ denotes the nominal system state and $\bar{u} \in \mathbb{R}^m$ is the input to the nominal system. Choosing an initial state $\hat{x} = \hat{x}(0)$ and a nominal control sequence $\hat{u} \triangleq \{\hat{u}(0), \hat{u}(1), \ldots\}$ yields a nominal state sequence $\hat{x} \triangleq \{\hat{x}(0), \hat{x}(1), \ldots\}$ solution of (13), which constitutes the center of a tube. Since the real system may be disturbed, the future trajectory of the disturbed plant will probably differ from the nominal prediction. To counteract the effect of the disturbances, we force the trajectory to lie as close as possible to the nominal trajectory, by combining in the control $u$ a feed-forward part, given by the tube based model predictive controller and a feedback part as in [6]:

\[
u = \bar{u} + K(x^{UP} - \hat{x}) \tag{14}
\]

where $K \in \mathbb{R}^{n \times n}$ is such that $A_K = A + BK$ is a Schur matrix.

Later in Section VIII, we will explain how the control action $\hat{u}$ is obtained by means of MPC.

We define the plant tracking error, $z$, the estimation tracking errors $e_i$, and the updated estimation tracking errors, $e_{i}^{UP}$, for $i = 1, \ldots, M$, as

\[
z \triangleq x - \hat{x} \tag{15}
\]

\[
e_i \triangleq \hat{x}_i - \hat{x} \tag{16}
\]

\[
e_{i}^{UP} \triangleq \hat{x}_{i}^{UP} - \hat{x} = e_i + \eta_i \tag{17}
\]
where, from (5),
\[ \gamma_i \triangleq G_i[y_i - C_i \hat{x}_i] \]  
(18)

Using (8), and substituting (2) \([\Pi_i = I_{pi}]\) in (18), we have that, under healthy operation of the \(i\)th group of sensors,
\[ \gamma_i = G_i C_i \hat{x}_i + G_i \eta_i \]  
(19)

Note from (1), (12)–(15), that we can express the dynamics of the plant tracking error as:
\[ z^+ = A_k z - B K U_{i^*} + E w \]  
(20)

Also using (12), (15), the “reconfigured” updated estimate tracking error \(e_{i^*}^{UPs}\) satisfies
\[ e_{i^*}^{UPs} \triangleq x_{i^*}^{UPs} - \hat{x} = z - x_{i^*}^{UPs} \]  
(21)

Using (14) and (21) in (7), the closed-loop estimator states \(\hat{x}_i\) corresponding to healthy sensors satisfy
\[ \hat{x}_i^+ = A_k \hat{x}_i + B \hat{u} + BK(z - x_{i^*}^{UPs}) + L_C \hat{x}_i + L_e \eta_i \]  
(22)

Using (8), (13), (15), (16), and (22), each estimation tracking error \(e_i\) satisfies the difference equation
\[ e_i^+ = A_k e_i + (B K + L_C) \hat{x}_i - B K x_{i^*}^{UPs} + L_e \eta_i \]  
(23)

VII. INVARIANT SETS FOR THE CLOSED-LOOP SYSTEM DYNAMICS

In this section, we derive invariant sets for the closed-loop system dynamics. In this analysis, we will assume that the FDI unit (described in Section IX) correctly identifies the faulty groups of sensors, so that the “reconfigured” updated estimate (10) is only formed by estimations corresponding to healthy groups of sensors. Later, in Section IX, we validate this analysis by providing conditions that guarantee that the FDI unit correctly discards faulty groups of sensors.

A. Estimation errors analysis

The difference equation (9) can be rewritten in the form
\[ \hat{x}_i^+ = A_k \hat{x}_i + \delta_i, \quad \delta_i \triangleq E w - L_e \eta_i \]  
(24)

Each “disturbance” \(\delta_i\) lies in the C-set \(\Delta_i \triangleq E \mathbb{W} \oplus (-L_e \mathbb{N}_i)\) (where the symbol \(\oplus\) denotes the Minkowski sum of sets).

Since \(A_k\) are Schur matrices, there exist a C-set \(\bar{S}\) that is finite time computable and RPI\(^4\) for the system (24) and constraint set \((\mathbb{R}^n, \Delta_i)\) \([10]\).

Using (12), we can compute the C-set \(\bar{S}_{i^*}^{UPs}\), where \(x_{i^*}^{UPs}\) lies whenever each estimation error \(\hat{x}_i \in \bar{S}\), \(\ell \in \mathbb{H}\), as:
\[ \bar{S}_{i^*}^{UPs} \triangleq \text{Conv hull} \left( \bigcup_{i \in \mathbb{H}} \left\{ \bigcup_{\ell \in \mathbb{H}} \mathcal{A}_i \left[ (I_h - G_i C_i) \bar{S}_i \oplus (-G_i \mathbb{N}_i) \right] \right\} \right) \]  
(25)

where \(\text{Conv hull}\) denotes the convex hull, and \(\mathbb{P}_M\) is the set of all subsets of \(\{1, \ldots, M\}\) (see Section V).

B. Plant tracking error analysis

The dynamics of the plant tracking error \(z\) defined in (20) can be rewritten in the form:
\[ z^+ = A_k z + z_\delta, \quad z_\delta = -B K x_{i^*}^{UPs} + E w \]  
(26)

where \(x_{i^*}^{UPs}, w\) are bounded respectively by \(S_{i^*}^{UPs}, \mathbb{W}\), and \(z_\delta\) lies in the set \(Z_\delta\) defined by
\[ Z_\delta = (-B K) S_{i^*}^{UPs} \oplus E \mathbb{W} \]  
(27)

Since \(A_k\) is a Schur matrix, there exists a C-set \(\mathbb{Z}\) that is finite time computable and RPI for system (26) and constraint set \((\mathbb{R}^n, Z_\delta)\).

C. Estimation and updated estimation tracking errors analysis in case of healthy sensors

The dynamics of the estimation tracking errors \(e_i\) (under healthy operation of the \(i\)th group of sensors) given in (23) can be rewritten in the form:
\[ e_i^+ = A_k e_i + \delta_i, \quad \delta_i \triangleq (B K + L_C) \hat{x}_i - B K x_{i^*}^{UPs} + L_e \eta_i \]  
(28)

where each \(\delta_i\) lies in \(\Delta_i\) defined by
\[ \Delta_i \triangleq (B K + L_C) \bar{S}_i \oplus (-B K) S_{i^*}^{UPs} \oplus L \mathbb{N}_i \]  
(29)

Since \(A_k\) is a Schur matrix, there exists a C-set \(\bar{S}\) that is finite time computable and RPI for system (23) (equivalently, (28)) and constraint set \((\mathbb{R}^n, \bar{S})\).

Using (21), we can compute the C-set \(S_{i^*}^{UPs}\), where the “reconfigured” updated estimation tracking error \(e_{i^*}^{UPs}\) lies whenever \(z \in \mathbb{Z} \) and \(x_{i^*}^{UPs} \in S_{i^*}^{UPs}\), with \(S_{i^*}^{UPs}\) defined in (25), as:
\[ S_{i^*}^{UPs} \triangleq Z \oplus (-\bar{S}_{i^*}^{UPs}) \]  
(30)

The following result establishes the existence of, and characterises, the invariant tubes where the system trajectories lie. The assumption that initial values are in the corresponding invariant sets is satisfied if, e.g., enough time elapses at the beginning of system operation without change in the fault situation, since those sets are attractive and convergence in finite time is ensured.

Theorem 7.1 (Tube for system’s trajectories): Assume the initial system state, \(x(0)\), the nominal system state, \(\bar{x}(0)\), and the initial value of the estimators associated with healthy groups of measurements, \(\hat{x}_i(0) = x(0) - \bar{x}_i(0) \in \bar{S}_i\), \(z(0) = x(0) - \bar{x}(0) \in Z\), \(e_i(0) = \hat{x}_i(0) - \bar{x}_i(0) \in \bar{S}_i\). Let \(u(k) = \bar{u}(k) + K (\hat{x}_{i^*}^{UPs}(k) - \bar{x}(k))\) \(\forall k \geq 0\), where \(\hat{x}_{i^*}^{UPs}\) is defined in (10). Then \(\forall k \geq 0,\)
1) \(\hat{x}_{i^*}^{UPs}(k) \in S_{i^*}^{UPs}\),
2) \(z(k) \in Z\) and \(x(k) \in \{\bar{x}(k)\} \oplus Z\); \(e_i(k) \in S_i\) and \(e_{i^*}^{UPs}(k) \in S_{i^*}^{UPs}\).

Proof:
1) Since \(\bar{S}\) is an RPI set, the assumption on the initial conditions \(\hat{x}_i(0) \in \bar{S}_i\) implies \(\hat{x}_i(k) \in \bar{S}_i, \forall k \geq 0\). Therefore, from (12) and (25), \(\hat{x}_{i^*}^{UPs}(k) \in S_{i^*}^{UPs}, \forall k \geq 0\).
2) Since \(\hat{x}_{i^*}^{UPs}(k) \in S_{i^*}^{UPs}\), then \(z(k) \in Z_\delta\) in (26)–(27), \(\forall k \geq 0\). Combining this result with the assumption \(z(0) \in Z\), together with the invariance of \(Z\), we have
\(z(k) \in \mathbb{Z}, \forall k \geq 0\). Moreover, from (15), we have that \(x = \bar{x} + z\), and it follows that the system state, \(x(k)\), satisfies \(x(k) \in \{\bar{x}(k)\} \oplus \mathbb{Z}, \forall k \geq 0\).

3) Since \(\bar{x}(k) \in S_{\bar{x}}\) and \(\tilde{u}(u(k)) \in \mathbb{S}_{U}^p\), we have that \(S_{\bar{x}} \subset \Delta_l\) in (28)-(29), \(\forall k \geq 0\). With the assumption on the initial condition \(e_i(0) \in S_{\bar{x}}\), and the invariance of \(S_{\bar{x}}\), it follows that \(e_i(k) \in S_{\bar{x}}, \forall k \geq 0\). Moreover, \(z(k) \in \mathbb{Z}, \forall k \geq 0\) implies, from (21) and (30), that \(\bar{e}(k) \in \mathbb{S}_{U}^p, \forall k \geq 0\).

\[\begin{align*}
\text{VIII. NOMINAL MPC DESIGN}
\end{align*}\]

We define the nominal optimal control problem for the reference system (13) to track the setpoint \((x_s, u_s)\) as

\[\begin{align*}
\mathcal{P}_N(x, u) : & \quad V_0(x, u) = \min_{u} \{V_0(x, u, x_s) \mid u \in \mathcal{O}(x)\} \\
& \text{in which } N \text{ is the prediction horizon, } \bar{x} = \bar{x}(0) \text{ is the initial condition of the nominal system (13) at the current time, and}
\end{align*}\]

and the cost \(V_N(x, \bar{u}, x_s, u_s)\) is defined by

\[\begin{align*}
V_N(x, \bar{u}, x_s, u_s) = \sum_{k=0}^{N-1} \ell(\bar{x}(k), \bar{u}(k), x_s, u_s) + V_f(\bar{x}(N), x_s)
\end{align*}\]

where \(V_f(\bar{x}(N), x_s)\) is the terminal cost function and \(\ell(\bar{x}(k), \bar{u}(k), x_s, u_s)\) is the stage cost defined by

\[\begin{align*}
\ell(\bar{x}, \bar{u}, x_s, u_s) = \|\bar{x} - x_s\|_Q + \|\bar{u} - u_s\|_R + V_f(\bar{x}, x_s) = \|\bar{x} - x_s\|_p
\end{align*}\]

with \(Q, R, P\) positive definite weighting matrices.

The constraint set \(\mathcal{O}(\bar{x})\) is defined by

\[\begin{align*}
\mathcal{O}(\bar{x}) = \{\bar{u} \mid \bar{u}(k) \in \mathbb{U} \cap \mathbb{K}_{U}^{p}, x_s, u_s, x_s, u_s\}
\end{align*}\]

where \(x_s \in X \cap \mathbb{Z}\) is the terminal constraint set. Note that \(\bar{u}\) is forced to satisfy the tighter constraints \(\bar{u} \in \mathbb{U} \cap \mathbb{K}_{U}^{p}\), which from (14), (21) and Theorem 7.1 item 3), ensure \(u \in \mathbb{U}\).

Similarly, in order to ensure that the unknown state \(x = \bar{x} + z\) [see (15) and Theorem 7.1 item 2) satisfies state constraints \(x \in X\), we must ensure that \(\bar{x} \in X \cap \mathbb{Z}\).

The solution of \(\mathcal{P}_N(x, u)\) is

\[\begin{align*}
\tilde{u}^0(x, x_s, u_s) = \arg \min_{\bar{u}} \{V_0(x, \tilde{u}, x_s, u_s) \mid \bar{u} \in \mathcal{O}(\bar{x})\}
\end{align*}\]

and the model predictive control law \(\kappa_N\) is obtained as

\[\begin{align*}
\bar{u} = \kappa_N(x, u) = \tilde{u}^0(x, x_s, u_s)
\end{align*}\]

where \(\tilde{u}^0(x, x_s, u_s)\) is the first element in the sequence \(\tilde{u}^0(x, x_s, u_s)\).

We next establish the stability properties of the above nominal controller. We require three standard assumptions. Assumptions 8.1, 8.2 below specify properties which, if possessed by the terminal cost function \(V_f(\bar{x}(N), x_s)\) and terminal constraint set \(X_f\), enable the use of the value function \(V_0(x, x_s, u_s)\), solution of the optimal control problem \(\mathcal{P}_N(x, u)\), defined in (31) as a Lyapunov function [10].

**Assumption 8.1 (Basic stability assumption):**

\[\begin{align*}
\min_{\bar{u} \in \mathbb{U} \cap \mathbb{K}_{U}^{p}, x_s} \{V_f(\bar{x} + \bar{B} u, x_s) + \ell(\bar{x}, \bar{u}, x_s, u_s)\} \\
A \bar{x} + \bar{B} u \in X_f \quad \forall x_s \in X_f
\end{align*}\]

The above assumption implicitly requires that for each \(\bar{x} \in X_f\), there exists a \(\bar{u} \in \mathbb{U} \cap \mathbb{K}_{U}^{p}\) such that \(A \bar{x} + \bar{B} u \in X_f\), i.e., it implies the following assumption.

**Assumption 8.2 (Implied invariance):** The set \(X_f\), is control invariant for the system \(\dot{x} = Ax + Bu, \bar{u} \in \mathbb{U} \cap \mathbb{K}_{U}^{p}\), that is, \(\forall x \in X_f\) there exists a \(\bar{u} \in \mathbb{U} \cap \mathbb{K}_{U}^{p}\) such that \(\dot{x} = Ax + \bar{B} u \in X_f\). The following assumption requires the disturbances and noises to be “small enough” so that the constraint set (34) is not empty.

**Assumption 8.3 (Tighter set for constraint satisfaction):** The disturbance sets \(W, N\), for \(i = 1, \ldots, M\), are sufficiently small to ensure that \(Z \subset X \cap \mathbb{K}_{U}^{p} \subset \mathbb{U}\).

Let

\[\begin{align*}
\mathcal{X}_N \triangleq \{\bar{x} \mid \forall \bar{u} \in \mathbb{U} \cap \mathbb{K}_{U}^{p}, x_s \in X_f\}
\end{align*}\]

where \(\mathcal{X}_N\) is the constraint set defined in (34). We then have the following result.

**Lemma 8.4 (Exponential stability of the nominal system):**

Consider the system

\[\dot{x} = Ax + Bu\]

where \(u\) is the nominal MPC law (36). Suppose \(\mathcal{X}_N\) is compact. Then, the setpoint \(x_s\) is exponentially stable with a region of attraction \(\mathcal{X}_N\) for the system (38).

**Proof:** If Assumptions 8.1–8.3, are satisfied for the optimal control problem \(\mathcal{P}_N(x, u)\), and \(\mathcal{X}_N\) is compact, then there exist constants \(c_1\) and \(c_2\) such that the value function \(V_0(x, x_s, u_s)\) satisfies (see [10]):

\[\begin{align*}
V_0(x, x_s, u_s) & \geq c_1 \|x - x_s\|^2, \quad \forall x_s \in \mathcal{X}_N \\
\Delta V_0(x, x_s) & \leq -c_1 \|x - x_s\|^2, \quad \forall x_s \in \mathcal{X}_N \\
V_0(x, x_s) & \leq c_2 \|x - x_s\|^2, \quad \forall x_s \in \mathcal{X}_N
\end{align*}\]

where \(\Delta V_0(x, x_s) = V_0(x, x_s, u_s) - V_0(x, x_s, u_s)\).

Hence \(x_s\) is exponentially stable for the nominal system \(\dot{x} = Ax + B\kappa_N(x, u)\) with a region of attraction \(\mathcal{X}_N\), i.e., there exist constants \(c > 0\) and \(\gamma \in (0, 1)\) such that \(\|x(k) - x_s\| \leq c \|x(0) - x_s\|^\gamma, \forall k \geq 0\) [10].

**Corollary 8.5:** The nominal state \(\dot{x}\) in (38) is bounded such that for constant vectors \(x_s \in \mathbb{R}^n\) and \(\delta_{\text{max}} \in \mathbb{R}^n\) (where \(x_s\) is the setpoint defined in Section II), \(\bar{x} \in \mathcal{X}_N \triangleq \{x \in \mathbb{R}^n \mid \|x - x_s\| \leq \delta_{\text{max}}\}\). Later in Section IX-B we will show exponential stability of the fault tolerant output MPC based on the above nominal controller results.

\footnote{If \(X\) in (34) is not compact, compactness of \(\mathcal{X}_N\) can be ensured by substituting \(X\) in (34) by its intersection with an arbitrarily large bounded box.}
IX. FAULT DETECTION AND IDENTIFICATION

In this section we describe the proposed fault detection and identification principle. The principle is based on the separation of “healthy” sets, where the updated estimation tracking errors (17) remain under healthy operation, from “under-fault” sets, towards which the updated estimation tracking errors jump when abrupt sensor faults occur in one or more groups of sensors.

A. Condition for fault tolerance

Suppose a \( j \)th group of sensors is healthy and such that its associated estimation error, \( \tilde{x}_j \), defined in (8), and estimation tracking error, \( e_j \), defined in (16), satisfy \( \tilde{x}_j \in \tilde{S}_j \) and \( e_j \in S_j \), where \( \tilde{S}_j \), \( S_j \) are the RPI sets defined in Sections VII-A and VII-C, respectively. Using (17), (19), we can then compute the C-set

\[
S_{j}^{\text{UP}} \triangleq \tilde{S}_j \circledast (G_j C_j) \tilde{S}_j \circledast G_j N_j
\]

where the updated estimation tracking error \( e_j^{\text{UP}} \) belongs whenever \( e_j \in S_j \), \( \tilde{x}_j \in \tilde{S}_j \), \( \eta_j \in N_j \). We know from Theorem 7.1, item 3), that this condition will hold for as long as the \( j \)th group of sensors remains healthy.

Consider next a fault in the \( j \)th group of sensors, characterised by a change of the fault matrix \( \Pi_j \) in (2) from the identity matrix (healthy case, see (3)) to a new “under fault” value. At the time of the fault, substituting (2) into (17), (18) and using (8) and (16) we have that the “under fault” updated estimation tracking error, \( e_j^{\text{UP}} \), satisfies

\[
e_j^{\text{UP}} = [I_n + G_j (\Pi_j - I_{p_j}) C_j] e_j + G_j (\Pi_j - I_{p_j}) C_j \tilde{x}_j
+ G_j \Pi_j C_j \eta_j + G_j [\Pi_j N_j + (I_{p_j} - \Pi_j) \eta_j^P]
\]

Since, at the time of the fault, the estimation tracking error \( e_j \) still belongs to \( S_j \) and the estimation error \( \tilde{x}_j \) still is in \( \tilde{S}_j \), then the updated estimation tracking error \( e_j^{\text{UP}} \) at the time of the fault will belong to the set

\[
S_{j}^{\text{UP}}(\Pi_j) = [I_n + G_j (\Pi_j - I_{p_j}) C_j] S_j \circledast G_j (\Pi_j - I_{p_j}) C_j \tilde{S}_j \circledast G_j (\Pi_j - I_{p_j}) N_j \circledast N_j
\]

where \( \tilde{X} \) is as in Corollary 8.5, and \( N_j \), \( N_j^P \) are the C-sets associated with the measurement noises.

In order to ensure an effective fault detection and identification, we need to verify that the sets \( S_{j}^{\text{UP}} \) and \( S_{j}^{\text{UP}}(\Pi_j) \) are separated.

**Assumption 9.1:** The condition \( S_{j}^{\text{UP}} \cap S_{j}^{\text{UP}}(\Pi_j) = \emptyset \) holds for all \( j = 1, \ldots, M \), for any of the possible values\(^8\) of the fault matrix \( \Pi_j \) characterising the considered fault situations for the \( j \)th group of sensors.

Note that the healthy updated estimation tracking error sets \( S_{j}^{\text{UP}} \) defined in (40) are centred at 0 (this is so because the sets \( \tilde{S}_j \) associated to the dynamics (24); \( S_j \) associated to the dynamics (28); and \( N_j \) defined in Section III, are all centred at 0). The set \( S_{j}^{\text{UP}}(\Pi_j) \) defined in (42), on the other hand, is offset around a centre point \( c_j(\Pi_j) \) given by

\[
c_j(\Pi_j) = G_j (\Pi_j - I_{p_j}) C_j x_0
\]

where \( x_0 \) is the center of \( \tilde{X} \) as expressed in Corollary 8.5. Thus, the reference offset \( x_0 \)—which in turn shifts the centre \( c_j(\Pi_j) \) in (43)—provides a mechanism to achieve the set separation condition of Assumption 9.1.

We require the following assumption which describes the initialisation condition of the FTC scheme.

**Assumption 9.2:** Before the occurrence of the first sensor fault, the system has been operating under healthy condition for a sufficiently long time such that all the estimation error trajectories are inside the RPI sets \( \tilde{S}_j \) defined in Section VII-A, for \( i = 1, \ldots, M \) and the estimation tracking errors are inside the RPI sets \( S_j \) defined in Section VII-C. Moreover, we assume that at least one group of sensors (which may consist of just one sensor) is operational at all times.

**Remark 9.3:** Notice that Assumption 9.2 guarantees that when the fault in the \( j \)th sensor group occurs at some time instant \( k \), \( \tilde{x}_j(k) \) is in \( \tilde{S}_j \) and \( e_j(k) \) is in \( S_j \). Hence we have, at the time of the fault, \( e_j^{\text{UP}} \in S_{j}^{\text{UP}}(\Pi_j) \). Combining this condition with Assumption 9.1, we conclude that the \( j \)th group of sensors, for \( j \in \{1, \ldots, M\} \), is healthy at any time \( k \) (and thus can be combined and used for reconfiguration in (10)) if \( e_j^{\text{UP}}(k) \in S_{j}^{\text{UP}} \); and that the moment \( e_j^{\text{UP}}(k) \) leaves the set \( S_{j}^{\text{UP}} \) allows us to detect a fault in that sensor group which, in consequence, must be discarded.

Based on the above developments, the fault diagnosis criterion proposed for the FDI unit is as follows:

**Criterion 9.4 (FDI):** At each time step \( k \), for each \( i = 1, \ldots, M \): if the updated estimation tracking error satisfies \( e_i^{\text{UP}}(k) \in S_{i}^{\text{UP}} \), with \( S_{i}^{\text{UP}} \) defined in (40), then the \( i \)th group of sensors is deemed healthy and considered for reconfiguration in (10)–(11); if \( e_i^{\text{UP}}(k) \notin S_{i}^{\text{UP}} \) then the \( i \)th group of sensors is deemed faulty and discarded for all future times.

B. Stability analysis

The tube MPC controller (14), steers the trajectories of the uncertain system (1), toward the central trajectory \( \tilde{x} \) generated by the nominal system (38). The following theorem uses the properties of this nominal system to establish closed-loop stability of the overall fault tolerant control scheme based on the tube MPC controller reconfigured by the use of the FDI Criterion 9.4.

**Theorem 9.5:** Consider the system (1), where \( u \) is computed as in (14), with \( \tilde{u} \) given by (36), \( U^{\text{UP}} \) given by (10) and \( \tilde{x} \) generated by the nominal system (38). Suppose the conditions stated in Assumptions 8.3, 9.1 and 9.2 hold. Moreover, consider that the stage cost \( f(\tilde{x}(N), x_N) \) given in (33) are selected so that the matrices \( Q, R, P \) satisfy the discrete algebraic Riccati equation \( A^T P A - P - (A^T B P + B^T P B)^{-1} (A^T B P) + Q = 0 \). The terminal constraint set \( \mathbb{X}_T \) given in (34), is chosen to be the maximal positively invariant constraint admissible set for the system \( \tilde{x}^T = A \tilde{x} + B \tilde{u} \) under the tighter constraints \( \tilde{x} \in \mathbb{X} \circledast \mathbb{Z} \) and \( \tilde{u} \in U \circledast K^{\text{UP}} \). Then,
1) System (1) reconfigured by the use of the FDI Criterion 9.4 to select the index set $H$ in (11) [used to compute the “reconfigured” updated estimates (10)] preserves exponential stability with a region of attraction $\mathcal{X}_N \oplus \mathbb{Z}$, whenever a $j$th group of sensors fails with fault matrix $\Pi_j$.

2) The state of the system (1), $x$, converges robustly and exponentially fast to $\{x_0\} \oplus \mathbb{Z}$ while satisfying the state and control hard constraints $x \in \mathcal{X}$, $u \in \mathcal{U}$.

Proof: As explained in Remark 9.3, Assumptions 9.2 and 9.1 guarantee that the FDI Criterion 9.4 only selects healthy groups of sensors to compute the “reconfigured” updated estimates (10) used in the control law (14).

While $\hat{x}_i \in \hat{\mathcal{S}}_i, \forall i \in \mathbb{N}$, then $\hat{x}^{UP*} \in \mathcal{S}^{UP*}$ and hence $z \in \mathbb{Z}$ (see Theorem 7.1 items 1) and 2)). The proposed choices for $\ell(\bar{x}(k), \bar{u}(k), x_0, u_0)$, $V_f(\bar{x}(N), x_0)$ and $\mathcal{X}_f$ guarantee that Assumptions 8.1 and 8.2 are satisfied [10]. Thus the result in Lemma 8.4 holds. As explained in the latter lemma, the region of attraction for $\hat{x}$ is the feasibility region of the optimisation problem $\mathcal{X}_N$. Since $x = \hat{x} + z$, the domain of attraction for $x$ is $\mathcal{X}_N \oplus \mathbb{Z}$. Therefore, the system is exponentially stable with a region of attraction $\mathcal{X}_N \oplus \mathbb{Z}$, and $x$ converges robustly and exponentially fast to $\{x_0\} \oplus \mathbb{Z}$.

In addition, using the fact that $x = \hat{x} + z$, $\hat{x} \in \mathcal{X} \oplus \mathbb{Z}$ and $z \in \mathbb{Z}$, yields $x \in \mathcal{X}$. Similarly, using (14), (21), $\bar{u} \in \mathcal{U} \oplus \mathcal{S}^{UP*}$, and $e^{UP*} \in \mathcal{S}^{UP*}$, we have that $u \in \mathcal{U}$. The result then follows. ■

X. ILLUSTRATIVE EXAMPLE

We consider the automotive longitudinal control problem under a stop-and-go scenario, discussed in [5], to illustrate the effectiveness of the proposed fault tolerant constrained control approach. In this problem, the vehicle interdistance dynamics are typically represented by the discretisation of a double integrator plant which, for a sampling period $T_s = 0.1s$, satisfy (1) with

$$A = \begin{bmatrix} 1 & 0.1 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0.1 \end{bmatrix},$$

where the first state represents the interdistance (in m) and the second state its time derivative (in m/s). The process disturbance $w$ represents an error in the estimation of the leader vehicle acceleration [5] and belongs to the C-set $\mathcal{W} = \{w \in \mathbb{R}^2 : |w| \leq 0.1\}$. We consider four position sensors $S_i$ with the following characteristics in the measurement equations (2): $C_i = [1 \ 0]$ for $i = 1, \ldots, 4$, and the measurement noises lie respectively in the C-sets $N_1 = N^F_1 \triangleq \{\eta \in \mathbb{R} : |\eta| \leq 0.001\}$, $N_p = N^F_p \triangleq \{\eta \in \mathbb{R} : |\eta| \leq 0.1\}$, $p = 2, 3, 4$. The state, and control constraint sets are $\mathcal{X} \triangleq \{x \in \mathbb{R}^2 : |x_2| \leq 6\}$ and $\mathcal{U} \triangleq \{u \in \mathbb{R} : |u| \leq 25\}$.

The tube MPC controller is required to steer the nominal system from the locally stable initial state $\bar{x} = \bar{x}(0) = [0 \ 0]$ at time 0, to, alternatively (following a square-like wave pattern), the setpoints $x_s = x_{s0} = [2 \ 0]^T$ and $x_s = x_{s10} = [10 \ 0]^T$, with a horizon $N = 30$. The matrices $Q, R, P$ in (33) are computed as explained in Theorem 9.5, with $Q = I_2$, $R = 10^{-5}$ and $P = \begin{bmatrix} 11.5134 & 1.0523 \\ 1.0523 & 1.1063 \end{bmatrix}$.

With the above data, we computed the domains of attraction $\mathcal{X}_N(x_{s0})$, $\mathcal{X}_N(x_{s10})$ of the nominal system under tighter constraints as depicted in Figure 1 (respectively red set and green set). The constant setpoints $x_{s1}, x_{s10}$ (dot markers), the terminal constraint sets respectively $\mathcal{X}_f(x_{s1})$, $\mathcal{X}_f(x_{s10})$ (blue and yellow sets), together with the initial state $\bar{x}$ (square marker) are also plotted on the same figure. Note that $x_{s1} \in \mathcal{X}_f(x_{s2})$, $x_{s10} \in \mathcal{X}_f(x_{s10})$ and starting from the initial condition $\bar{x}$, the states of the nominal system can be steered to the desired constant setpoint in $N$ steps while satisfying the tighter control constraints. To achieve the reference tracking goal we slightly modify the feedback part of the control $u$ in (14), by adding integral action. Thus, $u$ is now expressed by the following equation $u = \bar{u} + K_i \hat{x}^{UP*}$, where $K_i = [K_i \ K_{i\sigma}^T] = [6.3608 \ 8.0362 \ -0.8830]$ is a stabilising gain computed using LQR and $\sigma \in \mathbb{R}$ denotes the integral action state, defined by $\sigma^+ = \sigma + T_i (C^* \bar{x} - y^*)$ with $C^* = [1 \ 0]$, and $y^* = C^* \bar{x} + \eta^* \in \mathbb{R}$ is a system measured output which we assume not affected by faults.

The estimators (4), (5) are designed as steady state Kalman estimators whose equations can be found in, e.g., [11]. We chose the following parameters in those equations:

$$G_1 = \begin{bmatrix} 0.9991 \\ 0.9503 \end{bmatrix}, \quad G_2 = G_3 = G_4 = \begin{bmatrix} 0.6875 \\ 0.6250 \end{bmatrix}, \quad L_i = AG_i, \forall i \in \{1, \ldots, 4\}.$$  

The “reconfigured” updated estimate $\hat{x}^{UP*}$ presented in Section V, is obtained by using an optimal fusion steady state Kalman filter technique, as explained in [1].

Using the procedure in [2], we compute the RPI sets described in Section VII as well as the “healthy” and “faulty” sets (40) and (42). We consider a simulation scenario where all the sensors start under healthy operation, and total outage of sensor $S_1$ occurs at time $t_f = 17s$, characterised by $\Pi_1 = 0$ in (2). The separation condition of Assumption 9.1 holds for sensor $S_1$, as depicted in Fig. 2. When a fault occurs in sensor $S_1$, the corresponding updated estimation tracking error trajectories jump from the RPI set $\mathcal{S}^{UP}$ defined in (40) (top set centred at zero) to the “shifted” RPI set $\mathcal{S}^{UP*}$ (Pi1) defined in (42) (bottom set centred away from zero), making fault diagnosis possible. According to Theorem 9.5, we can conclude that the system preserves exponential stability with
a region of attraction $\mathbb{X}_N \oplus \mathbb{Z}$ whenever $S_1$ fails. At time $t_F - T_s$, $e_{UP}^1$ belongs to $S_{UP}^{\Pi_1}$, and at the time of the fault, $t_F$, $e_{UP}^1$ jumps to the set $S_{UP}^{\Pi_1}(\Pi_1)$. Fig. 3 shows the effectiveness of the fault tolerant constrained scheme. The first subplot displays the reference signal (dash-dotted red line) which is tracked by the actual vehicle interdistance (dotted blue line) under the fault situation considered. The second subplot depicts the reference and the system velocity which satisfy the constraints previously defined. Input constraint satisfaction is ensured, and shown in the third subplot where the reference and the system acceleration (control action) are plotted.

**Fig. 3.** Interdistance position, velocity and acceleration for a given reference signal. Bounds for tighter velocity: $[-4.6247, 4.6247]$. Bounds for tighter acceleration: $[-4.3503, 4.3503]$. 

**XI. CONCLUSION**

We have proposed a robust fault tolerant control scheme for constrained multisensor linear systems subject to sensor faults and in the presence of bounded state and output disturbances. An FDI unit provides a mechanism where the updated estimation tracking error of each sensor-estimator combination is tested for containment in a pre-computed healthy set. An active fault tolerant output feedback MPC controller guarantees robust closed-loop exponential stability of the system in normal operation and under abrupt faults in some of the sensors. An illustrative example shows the effectiveness of the scheme in those situations.

**REFERENCES**


