Fault tolerant control based on set-theoretic methods
PROST seminar

Florin Stoican

Norwegian University of Science and Technology (NTNU) - Department of Engineering Cybernetics

Wednesday, 21st March, 2012
Outline

1. Set theoretic elements
2. Fault tolerant control based on set-theoretic methods
3. Mixed integer programming elements
4. Conclusions and future directions
Outline

1. Set theoretic elements
2. Fault tolerant control based on set-theoretic methods
3. Mixed integer programming elements
4. Conclusions and future directions
Families of sets – generalities

Various families of sets in control:

- ellipsoids (Kurzhanski˘ı and Vályi [1997])
- polytopes/zonotopes (Motzkin et al. [1959])
- (B/L)MIs (Nesterov and Nemirovsky [1994])
- star-shaped sets (Rubinov and Yagubov [1986])

Issues to be considered:

- flexibility of the representation
- numerical implementation

\[ x^T Q x \leq \gamma \]

\[ \text{Kern}(S) \neq \emptyset \]

\[ G(x) \leq 0 \]
Families of sets – generalities

Various families of sets in control:

- ellipsoids (Kurzhanskii and Vályi [1997])
- polytopes/zonotopes (Motzkin et al. [1959])
- (B/L)MIs (Nesterov and Nemirovsky [1994])
- star-shaped sets (Rubinov and Yagubov [1986])

Issues to be considered:

- flexibility of the representation
- numerical implementation

\[ A_0 + \sum x_i A_i > 0 \]

\[ \text{Kern}(S) \neq \emptyset \]

\[ G(x) \leq 0 \]
Families of sets – polyhedral/zonotopic sets (more “structured”)

Best compromise: polytopic(zonotopic) sets

Polyhedral sets:
- dual representation
  - half-space:
    \[ h_i x \leq k_i, \; i = 1 \ldots N_h \]
  - vertex:
    \[ \sum_i \alpha_i v_i, \; \alpha_i \geq 0, \; \sum_i \alpha_i = 1, \; i = 1 \ldots N_v \]
- efficient algorithms for set containment problems (Gritzmann and Klee [1994])
- can approximate any convex shape (Bronstein [2008])
Families of sets – polyhedral/zonotopic sets (more “structured”)

Best compromise: polytopic/zonotopic sets

Zonotopic sets:
- obtained as
  - hypercube projection
  - Minkowski sum of generators
- additional representation
  - generator form:
    \[ \sum_{i} \lambda_i g_i, \quad |\lambda_i| \leq 1, \quad i = 1 \ldots N_g \]
- compact representation
- limited to symmetric objects
**Invariance notions**

Consider a system in $\mathbb{R}^n$

$$x^+ = f(x, \delta)$$

with disturbances bounded by the set $\Delta \subset \mathbb{R}^n$.

**Definition (RPI set)**

A set $\Omega$ is called robust positive invariant (RPI) iff

$$f(\Omega, \Delta) \subseteq \Omega.$$ 

The minimal RPI set (which is contained in all the RPI sets) can be defined as:

$$\Omega_{\infty} = f(f(\ldots, \Delta), \Delta) = \lim_{k \to \infty} f^{(k)}(0, \Delta).$$
Invariance notions

Consider a LTI system in $\mathbb{R}^n$

$$x^+ = Ax + B\delta$$

with $A$ a Schur matrix and disturbances bounded by the set $\Delta \subset \mathbb{R}^n$.

Definition (RPI set)
A set $\Omega$ is called robust positive invariant (RPI) iff

$$A\Omega \oplus B\Delta \subseteq \Omega.$$ 

The minimal RPI set (which is contained in all the RPI sets) can be defined as:

$$\Omega_\infty = \bigoplus_{i=0}^{\infty} A^i B\Delta.$$
Invariance notions – exemplification

\[ A\Omega \oplus B\Delta \subseteq \Omega \]

\[ \Omega_{\infty} = A\Omega_{\infty} \oplus B\Delta \]

\[ \Omega_{\infty} = \bigoplus_{i=0}^{\infty} A^i B\Delta \]
Ultimate bounds for zonotopic sets

Theorem (Ultimate bounds – Kofman et al. [2007])

For system $x^+ = Ax + B\delta$ with the Jordan decomposition $A = V\Lambda V^{-1}$ and assuming that $|\delta| \leq \bar{\delta}$ we have that the set $\Omega_{UB}(\epsilon)$ is RPI.

Particularities:

- explicit linear formulations
- “good” approximation of the mRPI set
- can be extended to various degenerate cases (Haimovich et al. [2008], Kofman et al. [2008])

$$\Omega_{UB}(\epsilon) = \{ x : |V^{-1}x| \leq (I - |\Lambda|)^{-1}|V^{-1}B|\bar{\delta} + \epsilon \}$$
Ultimate bounds for zonotopic sets

Theorem (Ultimate bounds – Kofman et al. [2007])

For system $x^{+} = Ax + B\delta$ with the Jordan decomposition $A = V\Lambda V^{-1}$ and assuming that $|\delta| \leq \bar{\delta}$ we have that the set $\Omega_{UB}(\epsilon)$ is RPI.

\[\delta_1 \in \Delta_1, \; |\delta_1| \leq \bar{\delta}\]
\[\delta_2 \in \Delta_2, \; |\delta_2| \leq \bar{\delta}\]

Sets with the same bounding box will give the same UBI set for a given dynamic.

Improvement (Stoican et al. [2011a]): use zonotopic sets for describing the disturbance.
Ultimate bounds for zonotopic sets

Theorem (Ultimate bounds – Kofman et al. [2007])

For system $x^+ = Ax + B\delta$ with the Jordan decomposition $A = V¹\Lambda V^{-1}$ and assuming that $|\delta| \leq \bar{\delta}$ we have that the set $\Omega_{UB}(\epsilon)$ is RPI.

$\delta_1 \in \Delta_1, |\delta_1| \leq \bar{\delta}$

$\delta_2 \in \Delta_2, |\delta_2| \leq \bar{\delta}$

Sets with the same bounding box will give the same UBI set for a given dynamic.

Improvement (Stoican et al. [2011a]): use zonotopic sets for describing the disturbance.
Ultimate bounds for zonotopic sets

Theorem (Ultimate bounds – Kofman et al. [2007])

For system $x^+ = Ax + B\delta$ with the Jordan decomposition $A = V\Lambda V^{-1}$ and assuming that $|\delta| \leq \bar{\delta}$ we have that the set $\Omega_{UB}(\epsilon)$ is RPI.

For a zonotopic perturbation

$$\Delta = C B_m^n$$

the dynamics become

$$x^+ = Ax + B\delta = Ax + BCw$$

and the UBI set becomes:

$$\tilde{\Omega}_{UB}(\epsilon) = \left\{ x : |V^{-1}x| \leq (I - |\Lambda|)^{-1}|V^{-1}B\ C\ |1 + \epsilon \right\}$$
Other set theoretic topics

- set separation between sets
  - through a separating hyperplane
  - through a barrier function

- upper bound for the inclusion time
  - particular bounds for a given attractive set

- RPI description for particular dynamics
  - switched/with delay
  - cyclic invariance
Outline

1 Set theoretic elements

2 Fault tolerant control based on set-theoretic methods
   - Problem statement
   - FDI mechanism
   - RC strategies
   - Extensions

3 Mixed integer programming elements

4 Conclusions and future directions
The need for FTC in control applications

- **Bhopal chemical spill**
  - (~4000 casualties)

- **Flight 1862 crash**
  - (43 casualties)

- **Fukushima meltdown**
  - (~40 km exclusion zone)

- **BP oil spill**
  - (~60000 barrels/day)
Fault tolerant control requirements
Fault tolerant control based on set-theoretic methods

FTC generalities

Legend

- $u =$ inputs
- $w =$ disturbances
- $r =$ references
- $v =$ noise
- $z =$ tracking error

FTC characterization
- passive (robust control)
- active (adaptive control)
  - FDI and RC blocks
  - link and reciprocal influences between FDI and RC

FDI directions
- stochastic (Kalman filters, sensor fusion)
- artificial intelligence
- set theoretic methods
Multisensor scheme
Problem statement

Multisensor scheme – plant

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

- LTI system
- bounded noise: \( w \in W \)
Fault tolerant control based on set-theoretic methods

Problem statement

Multisensor scheme – sensors

\[ y_i = C_i x + \eta_i \]

- static and redundant sensors
- bounded noise: \( \eta_i \in \mathbb{N}_i \)
Fault tolerant control based on set-theoretic methods

Problem statement

Multisensor scheme – fault scenario

\[ y_i = C_i x + \eta_i \]

\[ y_i = 0 \cdot x + \eta_i^F \]

- bounded noise: \( \eta_i^F \in N_i^F \)
- abrupt faults
- known model of the fault
Multisensor scheme – estimates

\[ \begin{align*}
\hat{x}_i^+ &= A\hat{x}_i + Bu + L_i (y_i - C_i \hat{x}_i) 
\end{align*} \]
Multisensor scheme – tracking error

\[
\hat{z}_i = \hat{x}_i - x_{\text{ref}}
\]

- minimize tracking error
Fault tolerant control based on set-theoretic methods

Problem statement

Multisensor scheme – controller

\[ u = u_{\text{ref}} + v \]

- switch (and not fusion)
- fix gain + reference governor
- MPC strategies

Florin Stoican
Modeling equations

- **plant dynamics**
  \[ x^+ = Ax + Bu + Ew \]

- **reference signal**
  \[ x_{\text{ref}}^+ = Ax_{\text{ref}} + Bu_{\text{ref}} \]

- **plant tracking error**
  \[ z^+ = x - x_{\text{ref}} = Az + B(u - u_{\text{ref}}) + Ew \]

- **estimations of the state**
  \[ \hat{x}_i^+ = (A - L_i C_i) \hat{x}_i + Bu + L_i (y_i - C_i \hat{x}_i) \]

- **estimations of the tracking error**
  \[ \hat{z}_i = \hat{x}_i - x_{\text{ref}} \]
Set separation conditions

Reminder:
- \( z = x - x_{ref} \)
- \( y_i = C_i x + \eta_i \)  \(\xrightarrow{\text{FAULT}}\) \( y_i = 0 \cdot x + \eta_i^F \)
- \( \eta_i \in N_i, \eta_i^F \in N_i^F \)

Consider the residual signal

\[
 r_i = y_i - C_i x_{ref},
\]
\[
\begin{aligned}
 r_i^H &= C_i z + \eta_i \\
 r_i^F &= -C_i x_{ref} + \eta_i^F
\end{aligned}
\]

Set separation condition:

\[
(\{C_i z\} \oplus N_i) \cap (\{-C_i x_{ref}\} \oplus N_i^F) = \emptyset
\]
Set separation conditions

Reminder:
- \( z = x - x_{\text{ref}} \)
- \( y_i = C_i x + \eta_i \) \( \xrightarrow{\text{FAULT}} \) \( y_i = 0 \cdot x + \eta_i \)
- \( \eta_i \in N_i, \eta_i^F \in N_i^F \)

Consider the residual signal

\[
\begin{align*}
  r_i &= y_i - C_i x_{\text{ref}}, \\
  \left\{ 
    \begin{array}{l}
      r_i^H \in R_i^H = C_i S_z \oplus N_i \\
      r_i^F \in R_i^F = -C_i X_{\text{ref}} \oplus N_i^F
    \end{array}
  \right.
\end{align*}
\]

Set separation condition:

\[
\left( C_i S_z \oplus N_i \right) \cap \left( -C_i X_{\text{ref}} \oplus N_i^F \right) = \emptyset
\]

Assume that:
- \( z \in S_z \)
- \( x_{\text{ref}} \in X_{\text{ref}} \)
Set separation conditions

Reminder:
- \( z = x - x_{\text{ref}} \)
- \( y_i = C_i x + \eta_i \) \( \xrightarrow{\text{FAULT}} y_i = 0 \cdot x + \eta_i^F \) \( \xleftarrow{\text{RECOVERY}} \)
- \( \eta_i \in N_i, \eta_i^F \in N_i^F \)

Consider the residual signal

\[
 r_i = y_i - C_i x_{\text{ref}}, \quad \begin{cases} r_i^H \in R_i^H = C_i S_z \oplus N_i \\ r_i^F \in R_i^F = -C_i x_{\text{ref}} \oplus N_i^F \end{cases}
\]

Set separation condition:

\[
 \left( C_i S_z \oplus N_i \right) \cap \left( -C_i x_{\text{ref}} \oplus N_i^F \right) = \emptyset
\]

Assume that:
- \( z \in S_z \)
- \( x_{\text{ref}} \in X_{\text{ref}} \)

\[
 R_i^H \cap R_i^F = \emptyset \quad \begin{cases} r_i \in R_i^H \leftrightarrow y_i = C_i x + \eta_i \\ r_i \in R_i^F \leftrightarrow y_i = 0 \cdot x + \eta_i^F \end{cases}
\]
Auxiliary sets

- boundedness assumptions: $N_i, N_i^F, W$
- $X_{\text{ref}}$ – set for the reference signal
- $\tilde{S}_i$ – invariant set for the state estimation error
- $S_z$ – invariant set for the plant tracking error

State estimation error:

$$\tilde{x}_i^+ = x^+ - \hat{x}_i^+ = (A - L_i C_i) \tilde{x}_i + \begin{bmatrix} E & -L_i \end{bmatrix} \begin{bmatrix} w \\ \eta_i \end{bmatrix}$$

Plant tracking error (for fix gain $v = -K \hat{z}_l$):

$$z^+ = (A - BK) z + \begin{bmatrix} E & BK \end{bmatrix} \begin{bmatrix} w \\ \tilde{x}_l \end{bmatrix}$$
Fault tolerant control based on set-theoretic methods

FDI mechanism

Auxiliary sets

- boundedness assumptions: $N_i, N_i^F, W$
- $X_{ref}$ – set for the reference signal
- $\tilde{S}_i$ – invariant set for the state estimation error
- $S_z$ – invariant set for the plant tracking error

State estimation error:

$$\tilde{x}_i^+ = x^+ - \hat{x}_i^+ = (A - L_iC_i) \tilde{x}_i + [E \quad -L_i] \begin{bmatrix} w \\ \eta_i \end{bmatrix}$$

Plant tracking error (for fix gain $v = -K\hat{z}_l$):

$$z^+ = (A - BK) z + [E \quad BK] \begin{bmatrix} w \\ \tilde{x}_l \end{bmatrix}$$
Fault tolerant control based on set-theoretic methods

FDI mechanism

Auxiliary sets

- boundedness assumptions: $N_i, N_i^F, W$
- $X_{ref}$ – set for the reference signal
- $\tilde{S}_i$ – invariant set for the state estimation error
- $S_z$ – invariant set for the plant tracking error

State estimation error:

$$\tilde{x}_i^+ = x^+ - \hat{x}_i^+ = (A - L_i C_i) \tilde{x}_i + \begin{bmatrix} E & -L_i \end{bmatrix} \begin{bmatrix} w \\ \eta_i \end{bmatrix}$$

Plant tracking error (for fix gain $v = -K\hat{z}_i$):

$$z^+ = (A - BK) z + \begin{bmatrix} E & BK \end{bmatrix} \begin{bmatrix} v \\ \tilde{x}_l \end{bmatrix}$$
Sensor partitioning

- $I_H = \{ i \in I^-_H : r_i \in R^H_i \} \cup \{ i \in I^-_R : S^R_i \subseteq \tilde{S}_i, \ r_i \in R^H_i \}$
- $I_F = \{ i \in I : r_i \notin R^H_i \}$
- $I_R = I \setminus (I_H \cup I_F)$.

$I = I_H \cup I_F \cup I_R$

<table>
<thead>
<tr>
<th></th>
<th>$I_H$</th>
<th>$I_F$</th>
<th>$I_R$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\tilde{x}_i \in \tilde{S}_i$</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$r_i \in R^H_i$</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
</tr>
</tbody>
</table>
Sensor partitioning

- $I_H = \{ i \in I_H : r_i \in R_i^H \} \cup \{ i \in I_R : S_i^R \subseteq \tilde{S}_i, r_i \in R_i^H \}$
- $I_F = \{ i \in I : r_i \notin R_i^H \}$
- $I_R = I \setminus (I_H \cup I_F)$.

$I = I_H \cup I_F \cup I_R$

$r_i \in R_i^H \rightarrow r_i \notin R_i^H$

<table>
<thead>
<tr>
<th></th>
<th>$I_H$</th>
<th>$I_F$</th>
<th>$I_R$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\tilde{x}_i \in \tilde{S}_i$</td>
<td>✓</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>$r_i \in R_i^H$</td>
<td>✓</td>
<td>→</td>
<td>X ←</td>
</tr>
</tbody>
</table>
Sensor partitioning

- $I_H = \{ i \in I_H : r_i \in R_i^H \} \cup \{ i \in I_R : S_i^R \subseteq \tilde{S}_i, \ r_i \in R_i^H \}$
- $I_F = \{ i \in I : r_i \notin R_i^H \}$
- $I_R = I \setminus (I_H \cup I_F)$.

$I = I_H \cup I_F \cup I_R$

$r_i \notin R_i^H \rightarrow r_i \in R_i^H$

<table>
<thead>
<tr>
<th></th>
<th>$I_H$</th>
<th>$I_F$</th>
<th>$I_R$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\tilde{x}_i \in \tilde{S}_i$</td>
<td>✓</td>
<td>—</td>
<td>X</td>
</tr>
<tr>
<td>$r_i \in R_i^H$</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
Sensor partitioning

- \( I_H = \{ i \in \overline{I}_H : r_i \in R_i^H \} \cup \{ i \in \overline{I}_R : S_i^R \subseteq \tilde{S}_i, r_i \in R_i^H \} \)
- \( I_F = \{ i \in I : r_i \notin R_i^H \} \)
- \( I_R = I \setminus (I_H \cup I_F) \).

\[ \mathcal{I} = I_H \cup I_F \cup I_R \]

\[ \tilde{x}_i \notin \tilde{S}_i \rightarrow \tilde{x}_i \in \tilde{S}_i \]

<table>
<thead>
<tr>
<th></th>
<th>( I_H )</th>
<th>( I_F )</th>
<th>( I_R )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \tilde{x}_i \in \tilde{S}_i )</td>
<td>✓</td>
<td>‾</td>
<td>X</td>
</tr>
<tr>
<td>( r_i \in R_i^H )</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
</tr>
</tbody>
</table>
Recovery – preliminaries

Conditions for recovery acknowledgment ($I_R \rightarrow I_H$)

- $r_i \in R_i^H$ – residual
- $\tilde{x}_i \in \tilde{S}_i$ – estimation error

$\tilde{x}_i = x - \hat{x}_i$ is not measurable but we construct $S_i^R$ such that $\tilde{x}_i \in S_i^R$

Strategies:
- necessary conditions
- sufficient conditions

- $\tilde{x}_i \in S_i^R$, a necessary condition for $\tilde{x}_i \in \tilde{S}_i$ is $S_i^R \cap \tilde{S}_i \neq \emptyset$
- $\tilde{x}_i \in S_i^R$, a sufficient condition for $\tilde{x}_i \in \tilde{S}_i$ is $S_i^R \subseteq \tilde{S}_i$
Fault tolerant control based on set-theoretic methods

FDI mechanism

Recovery – validation

\[ I_R \xrightarrow{i} I_H : (i \in I_R^-) \land (S_i^R \subseteq ˜S_i) \land (r_i \in R_i^H) \]

Issues:
- gap time
- inclusion validation

Strategies (during faulty functioning):
- gap time
  - keep the original dynamics of the estimator (Olaru et al. [2009])
  - change the dynamics of the estimator (Stoican et al. [2010b])
  - reset the estimation (\( \hat{x}_i^o = x_{ref} \) or \( \hat{x}_i^o = ˜x_i \))
- inclusion validation
  - wait for the validation of the inclusion
  - compute the reachable set of \( S_i^R \) and observe when the inclusion is validated
Recovery – validation

\[ I_R \xrightarrow{i} I_H : \ (i \in I_R^-) \land (S_i^R \subseteq \tilde{S}_i) \land (r_i \in R_i^H) \]

Issues:
- gap time
- inclusion validation

Strategies (during faulty functioning):
- gap time
  - keep the original dynamics of the estimator (Olaru et al. [2009])
  - change the dynamics of the estimator (Stoican et al. [2010b])
  - reset the estimation (\( \hat{x}_i^o = x_{ref} \) or \( \hat{x}_i^o = \hat{x}_l \))
- inclusion validation
  - wait for the validation of the inclusion
  - compute the reachable set of \( S_i^R \) and observe when the inclusion is validated
Illustrative example

Consider the interdistance example with dynamics

\[
\begin{align*}
\dot{x} &= \begin{bmatrix} 1 & 0.1 \\ 0 & 1 \end{bmatrix} x + \begin{bmatrix} 0 \\ 0.5 \end{bmatrix} u + \begin{bmatrix} 0 \\ 0.1 \end{bmatrix} w \\
& \quad \text{where } W = \{ w : |w| \leq 0.2 \}.
\end{align*}
\]

with \( W = \{ w : |w| \leq 0.2 \} \).

\( C_1 = \begin{bmatrix} 0.35 & 0.25 \end{bmatrix} \), \( |\eta_1| \leq 0.15 \), \( |\eta_1^F| \leq 1 \)

\( C_2 = \begin{bmatrix} 0.30 & 0.80 \end{bmatrix} \), \( |\eta_2| \leq 0.1 \), \( |\eta_2^F| \leq 1 \)

\( C_3 = \begin{bmatrix} 0.35 & 0.25 \end{bmatrix} \), \( |\eta_3| \leq 0.1 \), \( |\eta_3^F| \leq 0.3 \).
Illustrative example – FDI validation

Consider the interdistance example with dynamics

\[
\begin{bmatrix}
1 & 0.1 \\
0 & 1
\end{bmatrix} x + \begin{bmatrix}
0 \\
0.5
\end{bmatrix} u + \begin{bmatrix}
0 \\
0.1
\end{bmatrix} w
\]

with \( W = \{w : |w| \leq 0.2\} \).

\[
R_1^H = \{r_1 : -22.9 \leq r_1 \leq 22.9\},
\]

\[
R_2^H = \{r_2 : -19.8 \leq r_1 \leq 19.8\},
\]

\[
R_3^H = \{r_3 : -22.9 \leq r_1 \leq 22.9\}.
\]

\[
R_1^F = \{r_1 : -58.9 \leq r_1 \leq -49.8\},
\]

\[
R_2^F = \{r_2 : -53.9 \leq r_1 \leq -39.2\},
\]

\[
R_3^F = \{r_3 : -58.1 \leq r_1 \leq -50.5\}.
\]
Illustrative example – recovery validation

Sensors estimations for test case when 3\textsuperscript{th} sensor fails twice at \( f_1 \) and \( f_3 \) respectively:

\[
\begin{align*}
    f_1 &= 6s \\
    f_2 &= 9s \\
    f_3 &= 14s \\
    f_4 &= 16s \\
    f_5 &= 26.5s \\
    t_1 &= 13.1s \\
    t_2 &= 25.5s \\
    t_3 &= 30.9s
\end{align*}
\]

set transitions for sensor with index 3
Control strategies

For all control strategies we use the separation condition as a design constraint:

\[
(\{ C_i z \} \oplus N_i) \cap (\{- C_i x_{\text{ref}}\} \oplus N^F_i) = \emptyset
\]

to assure exact FDI.

Control strategies:

- **z** fixed and **x_{\text{ref}}** a decision variable:
  - fix gain feedback + reference governor

- **z** a decision variable and **x_{\text{ref}}** fixed:
  - MPC strategy for the feedback action

- both **z** and **x_{\text{ref}}** as decision variables:
  - MPC strategy involving both the reference and the feedback action
Fixed gain feedback

Assume a fixed feedback gain: such that a cost function is minimized:

\[ v = -K\hat{z}_l \]

\[ l = \arg\min_{i \in I_H} J(\hat{z}_i) \]

use only current information (classical case):

\[ v^* = -K\hat{z}_l \]

\[ l = \arg\min_{i \in I_H} \{||\hat{z}_i||_Q + ||v||_R\} \]
Fixed gain feedback

Assume a fixed feedback gain:

\[ \nu = -K\hat{z}_l \]

such that a cost function is minimized:

\[ l = \arg \min_{i \in I_H} J(\hat{z}_i) \]

use a prediction horizon:

- **individual merit**: keep the same sensor during the prediction horizon

\[ \nu = -K\hat{z}_{i^*} \]

\[ i^* = \arg \min_{i \in I_H} \left\{ \sum_{j=0}^{\tau-1} \left( ||\hat{z}_{i[j]}||_Q + ||v_{[j]}||_R \right) + ||\hat{z}_{i[\tau]}||_P \right\} \]

s.t.:

\[ \hat{z}_{i[j]}^+ = A\hat{z}_{i[j]} + Bv_{[j]} . \]

- **relay race**: check the sensor index at each iteration

- **collaborative scenario**: consider a convex sum of the sensors (at least in the terminal step)
Fixed gain feedback

Assume a fixed feedback gain:

\[ v = -K \hat{z}_l \]

such that a cost function is minimized:

\[ l = \arg \min_{i \in I_H} J(\hat{z}_i) \]

use a prediction horizon:

- **individual merit**: keep the same sensor during the prediction horizon
- **relay race**: check the sensor index at each iteration

\[ v = -K \hat{z}_{i^*} \]

\[ \{i^*_0, \ldots, i^*_{\tau-1}\} = \arg \min_{i \in I_H} \left\{ \sum_{j=0}^{\tau-1} (\|\hat{z}_{i[j]}\|Q + \|v_{[j]}\|R) + \|\hat{z}_{i[\tau]}\|P \right\} \]

s.t.:

\[ \hat{z}^+_{i[j]} = A\hat{z}_{i[j]} + Bv_{[j]} . \]

- **collaborative scenario**: consider a convex sum of the sensors (at least in the terminal step)
Fixed gain feedback

Assume a fixed feedback gain: $v = -K \hat{z}_i$

such that a cost function is minimized:

$$l = \arg\min_{i \in I_H} J(\hat{z}_i)$$

use a prediction horizon:

- **individual merit**: keep the same sensor during the prediction horizon
- **relay race**: check the sensor index at each iteration
- **collaborative scenario**: consider a convex sum of the sensors (at least in the terminal step)

$$v = -K \hat{z}_{i_0^*}$$

$$\{i_0^*, \ldots, i_{\tau-1}^*\} = \arg\min_{i \in I_H} \left\{ \sum_{j=0}^{\tau-1} \left( ||\hat{z}_{i[j]}||Q + ||v_{[j]}||R \right) + ||\hat{z}_{[\tau]}||P \right\}$$

s.t.:

$$\hat{z}_{i[j]}^+ = A \hat{z}_{i[j]} + B v_{[j]}$$

$$\hat{z}_{[\tau]}^* \in \text{conv} \left\{ \hat{z}_{[\tau]}^* \right\}_{i \in I_H}.$$
FDI adjusted reference governor

Fix \( z \in S_z \) and let \( x_{\text{ref}} \) be the decision variable:

\[
D_{x_{\text{ref}}} \triangleq \left\{ x_{\text{ref}} : \left( \{-C_i x_{\text{ref}}\} \oplus N_i^F \right) \cap \left( C_i S_z \oplus N_i \right) = \emptyset, \ i = 1 \ldots N \right\}.
\]

Reference governor (Stoican et al. [2010d]):

\[
u^{\ast}_{\text{ref}[0,\tau-1]} = \arg \min_{u_{\text{ref}[0,\tau-1]}} \sum_{i=0}^{\tau-1} \left( \| r[i] - x_{\text{ref}[i]} \|^2_{Q_r} + \| u_{\text{ref}[i]} \|^2_{R_r} \right)
\]

subject to:

\[
x_{\text{ref}[i]}^+ = A x_{\text{ref}[i]} + B u_{\text{ref}[i]}
\]

\[
x_{\text{ref}[i]}^+ \in D_{x_{\text{ref}}}
\]

Characteristics:
- fix gain
- flexible reference
MPC with FDI feasibility guarantees

Fix \( x_{\text{ref}} \) (\( x_{\text{ref}} \in X_{\text{ref}} \)) and let \( z \) be the decision variable:

\[
D_z \triangleq \left\{ z : (\{ C_i z \} \oplus N_i) \cap (\{-C_i x_{\text{ref}}\} \oplus N_i^F) = \emptyset, \ i = 1 \ldots N \right\}
\]

into the MPC formulation:

\[
v_{[0,\tau-1]}^* = \arg \min_{v_{[0,\tau-1]}} \left\{ \sum_{i=0}^{\tau-1} \left( ||z[i]||Q + ||v[i]||R \right) + ||z[\tau]||P \right\}
\]

subject to:

\[
z_{[i]}^+ = Az[i] + Bv[i] + Ew[i]
\]

\( z_{[i]}^+ \in D_z \)

Issues:

• stability guarantees
• numerical complexity (reachable sets)
MPC with FDI feasibility guarantees

Fix $x_{ref}$ ($x_{ref} \in X_{ref}$) and let $z$ be the decision variable:

$$D_z \triangleq \{ z : (\{C_i z\} \oplus N_i) \cap (\{-C_i X_{ref}\} \oplus N_i^F) = \emptyset, \ i = 1 \ldots N \}$$

into the tube-MPC formulation ($z \in \{z_{nom}\} \oplus S_z$):

$$v_{nom[0,\tau-1]}^* = \arg \min_{v_{nom[0,\tau-1]}} \left\{ \sum_{i=0}^{\tau-1} \left( ||z_{nom[i]}||_Q + ||v_{nom[i]}||_R \right) + ||z_{nom[\tau]}||_P \right\}$$

subject to:

$$z_{nom[i]}^+ = Az_{nom[i]} + Bv_{nom[i]}$$
$$z_{nom[i]}^+ \in D_z \ominus S_z$$

Issues:

- stability guarantees
- numerical complexity
  (reachable sets)
The estimation error as residual signal

Consider the residual signal as

\[ r_i = \hat{z}_i \]

The residual sets for healthy to faulty transitions are:

- \( R_{i}^{H} = \hat{S}_{i}^{H} \) (the invariant set of dynamics \( \hat{z}_i \) under healthy functioning)
- \( R_{i}^{F} = \hat{S}_{i}^{H \rightarrow F} \) (the one-step reachable set of \( \hat{S}_{i}^{H} \) under faulty functioning for \( \hat{z}_i \))

Particularities:
- requires persistent faults
- recovers the entire information
- permits passive FTC
- has filter behavior
The estimation error as residual signal

Consider the residual signal as

\[ r_i = \hat{z}_i \]

The residual sets for faulty to healthy transitions are:

- \( R^H_i = \hat{S}^F_i \) (the invariant set of dynamics \( \hat{z}_i \) under faulty functioning)
- \( R^F_i = \hat{S}^{F\rightarrow H}_i \) (the one-step reachable set of \( \hat{S}^F_i \) under healthy functioning for \( \hat{z}_i \))

Particularities:

- requires persistent faults
- recovers the entire information
- permits passive FTC
- has filter behavior
Passive FTC implementation

For a cost function \( J(\cdot) \) passive FTC is possible if:

\[
\max_{i \in I_H} J(\hat{z}_i) < \min_{i \in \mathcal{I} \setminus I_H} J(\hat{z}_i)
\]

\[
J(\hat{z}_i) = \hat{z}_i^T P \hat{z}_i
\]

\[
J(\hat{z}_i) = J^* \left\{ \left\lfloor \rho_H(\hat{z}_i) \right\rfloor - 1 \right\} + J^* \left[ \rho_H(\hat{z}_i) \right]
\]
Passive FTC implementation

For a cost function $J(\cdot)$ passive FTC is possible if:

$$\max_{i \in I_H} J(\hat{z}_i) < \min_{i \in I \setminus I_H} J(\hat{z}_i)$$

Not always possible!
Extended residual

Consider a receding observation horizon of length $\tau$ with extended residual

$$r_i = y_i[-\tau,0] - C_{i,\tau} x_{ref}[-\tau,0] - \Gamma_{i,\tau} v[-\tau,0]$$

which leads to:

$$r_i^H = \Theta_{i,\tau} z[-\tau] + \Phi_{i,\tau} w[-\tau,0] + \eta_i[-\tau,0]$$

$$r_i^F = -\Theta_{i,\tau} x_{ref}[-\tau] - \Gamma_{i,\tau} \left( u_{ref}[-\tau,0] + v[-\tau,0] \right) + \eta_i^F[-\tau,0]$$

Set separation guarantee for FDI:

$$-\Theta_{i,\tau} \left( z + x_{ref}[-\tau] \right) - \Gamma_{i,\tau} \left( u_{ref}[-\tau,0] + v[-\tau,0] \right) \not\in P_i$$
Extended residual

Consider a receding observation horizon of length $\tau$ with extended residual

$$r_i = y_i[-\tau,0] - C_{i,\tau} x_{\text{ref}}[-\tau,0] - \Gamma_{i,\tau} v[-\tau,0]$$

which leads to:

$$r_i^H = \Theta_{i,\tau} z[-\tau] + \Phi_{i,\tau} w[-\tau,0] + \eta_i[-\tau,0]$$

$$r_i^F = -\Theta_{i,\tau} x_{\text{ref}}[-\tau] - \Gamma_{i,\tau} \left( u_{\text{ref}}[-\tau,0] + v[-\tau,0] \right) + \eta_i^F[-\tau,0]$$

Set separation guarantee for FDI:

$$-\Theta_{i,\tau} \left( z + x_{\text{ref}}[-\tau] \right) - \Gamma_{i,\tau} \left( u_{\text{ref}}[-\tau,0] + v[-\tau,0] \right) \notin P_i$$

All control parameters influence the capacity of fault detection
Extended residual (II)

Particularities:
- requires persistent faults (only for \( \tau \) instants)
- recovers the entire information
- enhances the separation conditions
- adds delay in the control design
  - stability harder to enforce
  - maximizes FDI admissible space
Influences of extended residuals in RC design

General condition for FDI validation:

\[ \mathbb{D}_{\text{ref}} \triangleq \left\{ -\Theta_{i,\tau} \left( z + x_{\text{ref}[-\tau]} \right) - \Gamma_{i,\tau} \left( u_{\text{ref}[-\tau,0]} + v_{[-\tau,0]} \right) \notin P_i \right\} \]

Control strategies:
- fix gain with delayed information \((v_{[-\tau,0]} = -K\hat{z}_{i[-2\tau,-\tau]})\) leads to condition:

\[ -\Theta_{i,\tau} x_{\text{ref}[-\tau]} - \Gamma_{i,\tau} u_{\text{ref}[-\tau,0]} \notin P_i \ominus \left\{ -KS_{z[-2\tau,-\tau]} \right\} \ominus S_z \]

to be used in a reference governor.
- MPC formulation:

\[
(u^*_\text{ref}, v^*) = \arg \min_{u_{\text{ref}[0,\sigma], v[0,\sigma]}} \sum_{j=0}^{\sigma} f \left( x_{\text{ref}[j]}, z[j], u_{\text{ref}[j]}, v[j] \right)
\]

subject to:

\[
\begin{align*}
x_{\text{ref}^+[j]} &= Ax_{\text{ref}[j]} + Bu_{\text{ref}[j]} \\
z_{[j]}^+ &= Az[j] + Bv[j] + Ew[j]
\end{align*}
\]

\[
\left( x_{\text{ref}[j-\tau]}, u_{\text{ref}[j-\tau,j]}, v_{[j-\tau, j]}, z[j] \right) \in \mathbb{D}_{\text{ref}[j]}
\]
FDI adjustment for fix gain control

Control strategy for fix gain feedback:
- instead of computing the set invariant for a given dynamics we try to determine the dynamics that make a given set invariant
- for a bounded reference $x_{ref} \in X_{ref}$ the feasible tracking error region is given by

$$D_z \triangleq \left\{ z : \left( \{C_iz\} \oplus N_i \right) \cap \left( \{-C_iX_{ref}\} \oplus N_i^F \right) = \emptyset, i = 1 \ldots N \right\}$$

Take $S_z \subseteq D_z$ and enforce its invariance as a parameter after $K$ (Stoican et al. [2010a]):

$$S_z = \{ z : Hz \leq K \} \subseteq D_z$$

$$z^+ = (A - BK)z + \begin{bmatrix} E & B & K \end{bmatrix} \begin{bmatrix} w \\ \bar{x}_l \end{bmatrix}$$

$$\epsilon^* = \max_l \min_{K, H, \epsilon} \epsilon \\
\quad \epsilon \geq 0 \\
\quad HF_z = F_z(A - BK) \\
\quad H\theta_z + F_z B_z l \delta_z, l \leq \epsilon \theta_z \\
\quad \delta_z, l \in \Delta_z, l$$

if $\epsilon^* \leq 1$ the solution is feasible
FDI adjustment for fix gain control

Control strategy for fix gain feedback:
- instead of computing the set invariant for a given dynamics we try to determine the dynamics that make a given set invariant
- for a bounded reference $x_{\text{ref}} \in X_{\text{ref}}$ the feasible tracking error region is given by

$$D_z \triangleq \{ z : (\{C_i z\} \oplus N_i) \cap (\{-C_i x_{\text{ref}}\} \oplus N_i^{F}) = \emptyset, \ i = 1 \ldots N \}$$

Take $S_z \subseteq D_z$ and enforce its invariance as a parameter after $K$ (Stoican et al. [2010a]):

$$S_z = \{ z : H z \leq K \} \subseteq D_z$$

$$z^+ = (A - B K)z + \begin{bmatrix} E & B & K \end{bmatrix} \begin{bmatrix} w \\ \tilde{x}_l \end{bmatrix}$$

$$
\epsilon^* = \max_l \min_{K,H,\epsilon} \epsilon \\
K, H, \epsilon \geq 0 \\
H F_z = F_z (A - B K) \\
H \theta_z + F_z B_z, l \delta_z, l \leq \epsilon \theta_z \\
\delta_z, l \in \Delta_z, l
$$

if $\epsilon^* \leq 1$ the solution is feasible
From multisensor to multiple loops

- the same principles hold for actuator/subsystems faults
- issues to be considered:
  - computations more difficult (star-shaped sets)
  - the system becomes switched
Switched systems particularities

Note ([Branicky [1994]]): A switched system may not be stable even if all its subsystems are stable:

\[
\begin{align*}
\dot{x}_1 &= f_1(x_1, x_2) \\
\dot{x}_2 &= f_2(x_1, x_2)
\end{align*}
\]

then the system is globally stable for any switch occurring at moments greater or equal with \( T \).
Switched systems particularities

Theorem (Geromel and Colaneri [2006])

Let there be the switched system $x^+ = A_i x$ and assume that:

$$
\begin{align*}
P_i &> 0 \\
A'_i P_i A_i + P_i &\leq 0 \\
A'_i T P_j A_i T &< P_i \quad \forall j \neq i
\end{align*}
$$

then the system is globally stable for any switch occurring at moments greater or equal with $T$.

Difficulty: RPI construction for switched systems (Stoican et al. [2010c])
Outline

1. Set theoretic elements
2. Fault tolerant control based on set-theoretic methods
3. Mixed integer programming elements
4. Conclusions and future directions
Mixed integer programming elements

MIP – Preliminaries

Set separation problems usually lead to nonconvex feasible regions for optimization problems (usually, the complement of a polyhedral set):

$$x^* = \arg \min_{x \notin P} J(x)$$

where

$$P = \{x : h_i x \leq k_i, \ i = 1 \ldots N\}.$$

The goal is to reduce the number of binary variables in the extended representation.
MIP – Basic idea

Linear extended representation:

\[-h_i x \leq -k_i + M \alpha_i, \quad i = 1 : N\]

\[\sum_{i=1}^{N} \alpha_i \leq N - 1\]

with \((\alpha_1, \ldots, \alpha_N) \in \{0, 1\}^N\)
MIP – Basic idea

Linear extended representation:

\[-h_i x \leq -k_i + M \alpha_i, \quad i = 1 : N\]

\[\sum_{i=1}^{N} \alpha_i \leq N - 1\]

with \((\alpha_1, \ldots, \alpha_N) \in \{0, 1\}^N\)

Any of the regions \(\mathcal{R}^- (\mathcal{H}_i)\) of \(\mathcal{C}(P)\) can be obtained by a suitable choice of binary variables

\[\mathcal{R}^- (\mathcal{H}_i) \leftrightarrow (\alpha_1, \ldots, \alpha_N)^i \triangleq (1, \ldots, 1, \underbrace{0}_{i}, 1, \ldots, 1)\]
Mixed integer programming elements

MIP – Basic idea

Linear extended representation:

\[-h_i x \leq -k_i + M \alpha_i(\lambda), \quad i = 1 : N\]
\[0 \leq \beta_i(\lambda)\]

with \(\alpha_i(\lambda) : \{0, 1\}^{N_0} \to \{0\} \cup [1, \infty)\)

and

\[N_0 = \lceil \log_2 N \rceil\]

Any of the regions \(\mathcal{R}^-(\mathcal{H}_i)\) of \(\mathcal{C}(P)\) can be obtained by a suitable choice of binary variables (Stoican et al. [2011b])

\[\mathcal{R}^-(\mathcal{H}_i) \leftrightarrow (\lambda_1, \ldots, \lambda_{N_0})^i\]
Mixed integer programming elements

MIP – Basic idea

Linear extended representation:

\[-h_i x \leq -k_i + M \alpha_i(\lambda), \quad i = 1: N\]

\[0 \leq \beta_1(\lambda)\]

with \(\alpha_i(\lambda) : \{0, 1\}^{N_0} \to \{0\} \cup [1, \infty)\)

and

\[N_0 = \lceil \log_2 N \rceil\]

For any \(\lambda \in \{0, 1\}^{N_0}\) unallocated to a region \(\mathcal{R}^-(\mathcal{H}_i)\), the MI representation degenerates to the entire space \(\mathbb{R}^n\).

Solution: add constraints that make the unallocated tuples infeasible
Exemplification of the approach

Consider a polytope \( P \subset \mathbb{R}^2 \) given by

\[
\begin{bmatrix}
-1 & 0 \\
1 & 0 \\
0 & -1 \\
0 & 1
\end{bmatrix} \mathbf{x} \leq \begin{bmatrix}
1 \\
1 \\
1 \\
1
\end{bmatrix}
\]
Exemplification of the approach

and its complement $C(P)$ by

$$\begin{bmatrix} 1 & 0 \\ -1 & 0 \\ 0 & 1 \\ 0 & -1 \end{bmatrix} \times \begin{bmatrix} -1 + M\alpha_1 \\ -1 + M\alpha_2 \\ -1 + M\alpha_3 \\ -1 + M\alpha_4 \end{bmatrix}$$

in the classical MI formulation.
Exemplification of the approach

and its complement $C(P)$ by

$$\begin{bmatrix} 1 & 0 \\ -1 & 0 \\ 0 & 1 \\ 0 & -1 \end{bmatrix} x \leq \begin{bmatrix} -1 + M(\lambda_1 + \lambda_2) \\ -1 + M(1 - \lambda_1 + \lambda_2) \\ -1 + M(1 + \lambda_1 - \lambda_2) \\ -1 + M(2 - \lambda_1 - \lambda_2) \end{bmatrix}$$

in the reduced MI formulation.

In the reduced representation only $N_0 = \lceil \log_2 4 \rceil = 2$ binary variables are needed.

For region $R^-(H_2)$ associate tuple $(\lambda_1^2, \lambda_2^2) = (0, 1)$ which leads to the mapping

$$\alpha_2 = 1 + \lambda_1 - \lambda_2$$
MIP – Non-connected regions

Consider the complement $C(P) = cl(\mathbb{R}^n \setminus P)$ of a union of polyhedral sets $P = \bigcup_j P_j$.

$$A(H) = \bigcup_{l=1,\ldots,\gamma(N)} \left( \bigcap_{i=1}^{N} R^{\sigma_l(i)}(H_i) \right)_{A_l}$$

Using the hyperplanes $H_i$ we partition the space into disjoint cells $A_l$. 
MIP – Non-connected regions

Consider the complement \( \mathcal{C}(\mathbb{P}) = \text{cl}(\mathbb{R}^n \setminus \mathbb{P}) \) of a union of polyhedral sets \( \mathbb{P} = \bigcup_j P_j \).

\[
\begin{align*}
A_l & \left\{ \begin{array}{l}
\sigma_l(1)h_1x_1 & \leq \sigma_l(1)k_1 + M\alpha_l(\lambda) \\
\vdots & \\
\sigma_l(N)h_Nx_N & \leq \sigma_l(N)k_N + M\alpha_l(\lambda) \\
\vdots & \\
0 & \leq \beta_l(\lambda)
\end{array} \right.
\end{align*}
\]

Using the same procedure we associate a linear combination of binary variables \( \alpha_l(\lambda) \) to each cell (Stoican et al. [2011c]).
MIP – Non-connected regions

Consider the complement $C(P) = cl(\mathbb{R}^n \setminus P)$ of a union of polyhedral sets $P = \bigcup_j P_j$.

\[
\begin{align*}
A_I \begin{cases}
\sigma_I(1)h_1x & \leq \sigma_I(1)k_1 + M\alpha_I(\lambda) \\
\vdots & \\
\sigma_I(N)h_Nx & \leq \sigma_I(N)k_N + M\alpha_I(\lambda) \\
0 & \geq \beta_I(\lambda)
\end{cases}
\end{align*}
\]

The number of cells can be reduced through merging procedures (Karnaugh maps, espresso heuristic minimizer).
Outline

1. Set theoretic elements
2. Fault tolerant control based on set-theoretic methods
3. Mixed integer programming elements
4. Conclusions and future directions
Conclusions

- invariant sets offer a robust FTC approach
- a countable number of sensor fault scenarios can be arbitrary chosen
- a global view in considering the effects of the FDI mechanism
- extensions to MPC
- good balance between computational effort and precision
- robust fault detection
Future directions – set theoretic elements

- invariance computations
  - explicit formula for the boundary of the mRPI set
  - RPI sets for switched/with delay systems
- optimization problem which returns an RPI set for given dynamics and constraints (+ fix structure)
- faster algorithms for set operations (treat degenerate polyhedral cases)
- comprehensive framework for zonotopes
- bridge the gap with stochastic FTC by the use of probabilistic invariance
References


Florin Stoican, Ionela Prodan, and Sorin Olaru. Enhancements on the hyperplane arrangements in mixed integer techniques. Accepted to the 50th IEEE Conference on Decision and Control and European Control Conference, 2011c.
Thank you!
Questions ?