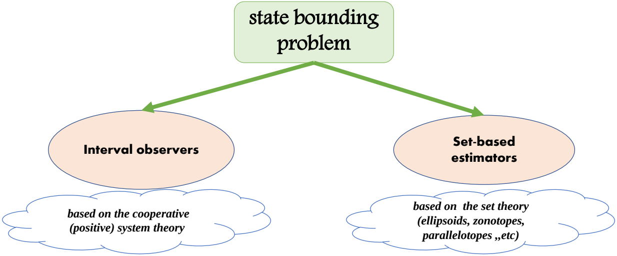
Secure state estimation algorithm for discrete-time linear systems: A set-valued approach

Nacim Meslem

29 February 2024



Moving Horizon-like set-valued state estimator

- **Correction stage**: based on the observability matrix.
- **Prediction stage**: based on non recursive formula.

Deals with sensor anomalies

- Faulty sensors.
- Malicious sensor attacks.

Outline

Outline

Discrete-Time Systems with multiple sensors

$$\begin{cases} \mathbf{x}_{k+1} & \in & \mathbf{A}\mathbf{x}_k + \mathbf{B}\mathbf{u}_k + \mathbf{E}[\mathbf{w}_k], & \mathbf{x}_0 \in [\mathbf{x}_0] \\ {}^{i}\mathbf{y}_k & \in & {}^{i}\mathbf{C}\mathbf{x}_k + {}^{i}\mathbf{D}\mathbf{u}_k + {}^{i}\mathbf{F}[{}^{i}\mathbf{v}_k], & i \in \{1, \ldots, N\} \end{cases}$$

N : Is the number of the considered sensors.

Assumption 1 (Bounded sets)

- $[\mathbf{w}_k]$: Is the worst-case domain of the modeling error, which includes the state disturbances and process noise;
- $[{}^{i}\mathbf{v}_k]$: Stands for the feasible domain of the output error, which includes measurement noise and sensor inaccuracy;
- $[\mathbf{x}_0]$: Is the feasible set of the system initial state.

Assumption 2 (Observability)

The matrix pairs $(\mathbf{A}, {}^{i}\mathbf{C})$ are observable for all $i \in \{1, \ldots, N\}$.

Sensors subject to cyber-attacks or faults

$${}^{(m,i)}\mathbf{y}_k = {}^{i}\mathbf{y}_k + {}^{i}\mathbf{a}_k, \quad i \in \{1, \ldots, N\},$$

where ${}^{i}\mathbf{a}_k$ stands for additive sensor faults or malicious attacks.

Objective

- **Design robust state estimator** with the following properties:
  - Guarantee: based on the available data, this state estimator has to provide a tight enclosure of the actual state vector of the system

$$\underline{\mathbf{x}}_k \leq \mathbf{x}_k \leq \overline{\mathbf{x}}_k.$$

  - Resilience: even in the presence of a cyber-attack or a sensor fault, the estimated interval has to keep framing the actual state vector of the system.

Proposed Approach: Prediction-Correction strategy

Prediction

- Open loop interval predictor.
- Explicit reachability method.

Correction

- Based on the observability matrix of the pairs $(\mathbf{A}, {}^{i}\mathbf{C})$.
- Correction at past time instants

Set-membership consistency tests

- Detect sensor anomalies.
- Distinguish between sensor faults and malicious attacks.

Outline

Interval prediction:

General solution of the state equation

$$\mathbf{x}_k = \mathbf{A}^{k-s}\mathbf{x}_s + \sum_{j=0}^{k-s-1} \mathbf{A}^{k-s-j-1}\mathbf{B}\mathbf{u}_{s+j} + \sum_{j=0}^{k-s-1} \mathbf{A}^{k-s-j-1}\mathbf{E}\mathbf{w}_{s+j},$$

where k is the current time instant and s stands for the initial time instant.

Interval extension

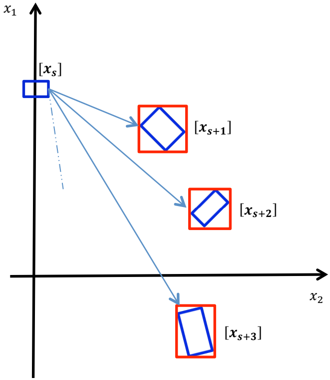
$$[\mathbf{x}_k] = \mathbf{A}^{k-s}[\mathbf{x}_s] \oplus \sum_{j=0}^{k-s-1} \mathbf{A}^{k-s-j-1}\mathbf{B}\mathbf{u}_{s+j} \oplus \sum_{j=0}^{k-s-1} \mathbf{A}^{k-s-j-1}\mathbf{E}[\mathbf{w}_{s+j}].$$

Compact form

$$[{}^{p}\mathbf{x}_k] = \mathbf{A}^{\sigma(k)}[\mathbf{x}_s] \oplus \mathbf{N}_{\sigma(k)}[\mathbf{P}_{\sigma(k):k-1}] \oplus \mathbf{B}_{\sigma(k)}\mathbf{U}_{\sigma(k):k-1},$$

where

$$\begin{array}{lcl}
\sigma(k) & = & k - s \\
\mathbf{N}_{\sigma(k)} & = & (\mathbf{A}^{\sigma(k)-1}\mathbf{E},\ \mathbf{A}\mathbf{E},\ \ldots,\ \mathbf{E}) \\
\mathbf{B}_{\sigma(k)} & = & (\mathbf{A}^{\sigma(k)-1}\mathbf{B},\ \mathbf{A}\mathbf{B},\ \ldots,\ \mathbf{B}) \\
[\mathbf{P}_{\sigma(k):k-1}] & = & \{[\mathbf{w}_{\sigma(k)}];\ [\mathbf{w}_{\sigma(k)+1}];\ \ldots;\ [\mathbf{w}_{k-1}]\} \\
\mathbf{U}_{\sigma(k):k-1} & = & \{\mathbf{u}_{\sigma(k)};\ \mathbf{u}_{\sigma(k)+1};\ \ldots;\ \mathbf{u}_{\sigma(k)+k-1}\}.
\end{array}$$



- One computes directly the upcoming state enclosures, $[\mathbf{x}_k]$, $k > s$ from a given time instant s.
- There is no *wrapping effect* or *dependence phenomenon* in this interval expression.

Interval prediction:

Illustrative example

Consider the rotation system,

$$\mathbf{x}_{k+1} = \mathbf{A}\mathbf{x}_k,$$

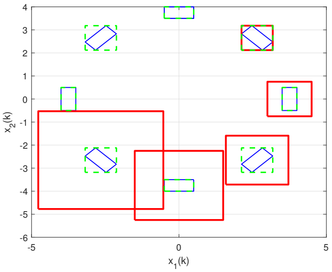
where A is defined by,

$$\mathbf{A} = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}.$$

- Initial box $[\mathbf{x}_0] = \{[-0.5, 0.5]; \ [3.5, \ 4]\}$.
- At each iteration this box undergo a rotation of an angle $\theta = \frac{\pi}{4}$
- The volume of reached set stays constant for all time instant $k \geq 0$.

Explicit solution (no recursive set-valued computation)

$$\mathbf{x}_k = \mathbf{A}^k \mathbf{x}_0.$$



- Blue parallelograms represent the exact reachable sets.
- Red rectangles correspond to the outer approximations obtained by the iterative interval method.
- Green rectangles show the outer approximations provided by the non-iterative interval method.

Correction

Point-valued expressions

For all $k > s = n - 1$ **and for all** $i \in \{1, \ldots, N\}$

Sequence of system output in function of the past state vector $\mathbf{x}_{\sigma(k)}$

$$^{i}\mathbf{Y}_{\sigma(k):\sigma(k)+n-1} = {}^{i}\mathcal{O}\mathbf{x}_{\sigma(k)} + {}^{i}\mathcal{O}_u\mathbf{U}_{\sigma(k):\sigma(k)+n-1} + {}^{i}\mathcal{O}_d\mathbf{P}_{\sigma(k):\sigma(k)+n-2} + {}^{i}\mathcal{H}\mathbf{Z}_{\sigma(k):\sigma(k)+n-1},$$

where

Vectors

- $\mathbf{U}_{\sigma(k):\sigma(k)+n-1} = \left\{\mathbf{u}_{\sigma(k)}; \mathbf{u}_{\sigma(k)+1}; \ldots; \mathbf{u}_{\sigma(k)+n-1}\right\}$
- $^{i}\mathbf{Y}_{\sigma(k):\sigma(k)+n-1} = \left\{^{(m,i)}\mathbf{y}_{\sigma(k)};^{(m,i)}\mathbf{y}_{\sigma(k)+1}; \ldots;^{(m,i)}\mathbf{y}_{\sigma(k)+n-1}\right\}$
- $^{i}\mathbf{Z}_{\sigma(k):\sigma(k)+n-1} = \left\{^{i}\mathbf{v}_{\sigma(k)};^{i}\mathbf{v}_{\sigma(k)+1}; \ldots;^{i}\mathbf{v}_{\sigma(k)+n-1}\right\}$
- $\mathbf{P}_{\sigma(k):\sigma(k)+n-2} = \left\{\mathbf{w}_{\sigma(k)}; \mathbf{w}_{\sigma(k)+1}; \ldots; \mathbf{w}_{\sigma(k)+n-2}\right\}$

Correction

Point-valued expressions

For all $k > s = n - 1$ **and for all** $i \in \{1, \ldots, N\}$

Sequence of system output in function of the past state vector $\mathbf{x}_{\sigma(k)}$

$$^{i}\mathbf{Y}_{\sigma(k):\sigma(k)+n-1} = {}^{i}\mathcal{O}\mathbf{x}_{\sigma(k)} + {}^{i}\mathcal{O}_u\mathbf{U}_{\sigma(k):\sigma(k)+n-1} + {}^{i}\mathcal{O}_d\mathbf{P}_{\sigma(k):\sigma(k)+n-2} + {}^{i}\mathcal{H}\mathbf{Z}_{\sigma(k):\sigma(k)+n-1},$$

where

Matrices

$$^{i}\mathcal{O} = \begin{pmatrix} ^{i}\mathbf{C} \\ ^{i}\mathbf{C}\mathbf{A} \\ \vdots \\ ^{i}\mathbf{C}\mathbf{A}^{n-1} \end{pmatrix}, \qquad ^{i}\mathcal{O}_d = \begin{pmatrix} \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} \\ ^{i}\mathbf{C}\mathbf{E} & \mathbf{0} & \ldots & \vdots \\ \vdots & \vdots & \ldots & \vdots \\ ^{i}\mathbf{C}\mathbf{A}^{n-2}\mathbf{E} & ^{i}\mathbf{C}\mathbf{A}^{n-3}\mathbf{E} & \ldots & ^{i}\mathbf{C}\mathbf{E} \end{pmatrix},$$

$$^{i}\mathcal{O}_u = \begin{pmatrix} ^{i}\mathbf{D} & \mathbf{0} & \ldots & \mathbf{0} & \mathbf{0} \\ ^{i}\mathbf{C}\mathbf{B} & ^{i}\mathbf{D} & \ldots & \vdots & \vdots \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ ^{i}\mathbf{C}\mathbf{A}^{n-2}\mathbf{B} & ^{i}\mathbf{C}\mathbf{A}^{n-3}\mathbf{B} & \ldots & ^{i}\mathbf{C}\mathbf{B} & ^{i}\mathbf{D} \end{pmatrix}, \qquad ^{i}\mathcal{H} = \mathrm{diag}(n, {}^{i}\mathbf{F})$$

Correction
Set inversion

For all $k > s = n - 1$ **and for all** $i \in \{1, \ldots, N\}$

Set inversion

$$[{}^{(\mathrm{inv},i)}\mathbf{x}_{\sigma(k)}] = {}^{(\mathrm{inv},i)}\hat{\mathbf{x}}_{\sigma(k)} \oplus {}^{i}\Xi_p[\mathbf{P}_{\sigma(k):\sigma(k)+n-2}] \oplus {}^{i}\Xi_z[{}^{i}\mathbf{Z}_{\sigma(k):\sigma(k)+n-1}],$$

where

Point-valued estimate

$${}^{(\mathrm{inv},i)}\hat{\mathbf{x}}_{\sigma(k)} = ({}^{i}\mathcal{O})^{-1}({}^{i}\mathbf{Y}_{\sigma(k):\sigma(k)+n-1} - {}^{i}\mathcal{O}_u\mathbf{U}_{\sigma(k):\sigma(k)+n-1}),$$

and

Uncertainties

$${}^{i}\Xi_p = -({}^{i}\mathcal{O})^{-1}\,{}^{i}\mathcal{O}_d \quad \text{and} \quad [\mathbf{P}_{\sigma(k):\sigma(k)+n-2}] = \{[\mathbf{w}_{\sigma(k)}];[\mathbf{w}_{\sigma(k)+1}];\ldots;[\mathbf{w}_{\sigma(k)+n-2}]\}$$

$${}^{i}\Xi_z = -({}^{i}\mathcal{O})^{-1}\,{}^{i}\mathcal{H} \quad \text{and} \quad [{}^{i}\mathbf{Z}_{\sigma(k):\sigma(k)+n-1}] = \{[{}^{i}\mathbf{v}_{\sigma(k)}];[{}^{i}\mathbf{v}_{\sigma(k)+1}];\ \ldots;[{}^{i}\mathbf{v}_{\sigma(k)+n-1}]\}$$

Correction

Set-filtering

For all $k > s = n - 1$

Correction at the past time instant $\sigma(k)$

$$[{}^{c}\mathbf{x}_{\sigma(k)}] := [{}^{(\mathrm{inv},i)}\mathbf{x}_{\sigma(k)}] \cap [{}^{p}\mathbf{x}_{\sigma(k)}].$$

where

Interval predictor

$$[{}^{p}\mathbf{x}_{k+1}] := \mathbf{A}^{n}[{}^{c}\mathbf{x}_{\sigma(k)}] \oplus \mathbf{N}_{n}[\mathbf{P}_{\sigma(k):k}] \oplus \mathbf{B}_{n}\mathbf{U}_{\sigma(k):k},$$

with

$$\begin{array}{lcl} \mathbf{N}_n & = & \left(\mathbf{A}^{n-1}\mathbf{E},\ \mathbf{AE},\ \ldots\ \mathbf{E}\right) \\ \mathbf{B}_n & = & \left(\mathbf{A}^{n-1}\mathbf{B},\ \mathbf{AB},\ \ldots\ \mathbf{B}\right). \end{array}$$

Interval estimation: A bundle of estimators

Prediction-Correction Principle

Phase 1: Interval-based predictor

- **For** $k := 1$ to $k := n-1$
  1. $[{}^p\mathbf{x}_k] := \mathbf{A}^k[\mathbf{x}_0] \oplus \mathbf{N}_k[\mathbf{P}_{0:k-1}] \oplus \mathbf{B}_k\mathbf{U}_{0:k-1}$
  2. $[\mathbf{x}_k] := [{}^p\mathbf{x}_k]$
- **end**

Phase 2: Interval-based predictor-corrector

- **For** $k \geq n-1$ to ∞
  3. $\sigma(k) := k - (n-1)$
  4. **Set-inversion: For** $i = 1$ **to** $i = N$

$$[{}^{(\mathrm{inv},i)}\mathbf{x}_{\sigma(k)}] = {}^{(\mathrm{inv},i)}\hat{\mathbf{x}}_{\sigma(k)} \oplus {}^i\,\Xi_p[\mathbf{P}_{\sigma(k):\sigma(k)+n-2}] \oplus {}^i\,\Xi_z[{}^i\mathbf{Z}_{\sigma(k):\sigma(k)+n-1}]$$

  5. **Set-intersection**

$$[{}^c\mathbf{x}_{\sigma(k)}] := \cap_{i=1}^{N}[{}^{(\mathrm{inv},i)}\mathbf{x}_{\sigma(k)}] \cap [{}^p\mathbf{x}_{\sigma(k)}]$$

  6. **Set-propagation**

$$[{}^p\mathbf{x}_{k+1}] := \mathbf{A}^n[{}^c\mathbf{x}_{\sigma(k)}] \oplus \mathbf{N}_n[\mathbf{P}_{\sigma(k):k}] \oplus \mathbf{B}_n\mathbf{U}_{\sigma(k):k}$$

  7. $[\mathbf{x}_{k+1}] := [{}^p\mathbf{x}_{k+1}]$
- **end**
- **Return** $[\mathbf{x}_k],\ k \in \{1, 2, \ldots, \infty\}$

Convergence property

Proposition:

Under the observability assumption of the pairs

$$(\mathbf{A}, {}^{i}\mathbf{C}), \;\; i \in \{1, \dots N\},$$

and the boundedness assumption of the boxes

$${}^{i}\mathbf{v}_k \in [{}^{i}\mathbf{v}_k], \;\; \mathbf{w}_k \in [\mathbf{w}_k], \;\; \forall k \geq 0$$

the proposed algorithm provides an interval sequence $[\mathbf{x}_k], \;\; k \in \{1, 2, \dots\}$, such that:

- For all $k \geq (n-1)$, the width of the state enclosure $[\mathbf{x}_k]$ is lower than,

$$w([\mathbf{x}_k]) \leq \beta_v \min_{i \in \{1, \dots N\}} \{ \max_{j \in \{\sigma(k), \dots \sigma(k)+n-1\}} \{ w([{}^{i}\mathbf{v}_j]) \} \} + \beta_d \max_{j \in \{\sigma(k), \dots \sigma(k)+n-1\}} \{ w([\mathbf{w}_j]) \},$$

where

- $\beta_v = \|\mathbf{A}^n\|_\infty \min_{i \in \{1, \dots N\}} \{ \|{}^{i}\Xi_z\|_\infty \}$ and
- $\beta_d = \|\mathbf{N}_n\|_\infty + \|\mathbf{A}^n\|_\infty \min_{i \in \{1, \dots N\}} \{ \|{}^{i}\Xi_p\|_\infty \}$.

Sketch of the proof

For $k \geq n-1$, the state enclosure $[{}^p\mathbf{x}_{k+1}]$ can be computed from the corrected box $[{}^c\mathbf{x}_{\sigma(k)}]$ at the time instant $\sigma(k)$

$$[{}^p\mathbf{x}_{k+1}] := \mathbf{A}^n[{}^c\mathbf{x}_{\sigma(k)}] \oplus \mathbf{N}_n[\mathbf{P}_{\sigma(k):k}] \oplus \mathbf{B}_n\mathbf{U}_{\sigma(k):k}$$

Then, one can outer approximate it as follows:

$$[{}^p\mathbf{x}_{k+1}] \quad \subseteq \quad \mathbf{A}^{n-1}[{}^{(\mathrm{inv},i)}\mathbf{x}_{\sigma(k)}] \oplus \mathbf{N}_n[\mathbf{P}_{\sigma(k):k}] \oplus \mathbf{B}_n\mathbf{U}_{\sigma(k):k}$$

So, its width can be upper bounded by

$$\begin{aligned}
w([{}^p\mathbf{x}_{k+1}]) \quad &\leq \quad \|\mathbf{A}^{n-1}\|_\infty w([{}^{(\mathrm{inv},i)}\mathbf{x}_{\sigma(k)}]) + \|\mathbf{N}_n\|_\infty w([\mathbf{P}_{\sigma(k):k}]) \\
&\leq \quad \|\mathbf{A}^{n-1}\|_\infty w(({}^i\mathcal{O})^{-1}([{}^i\mathbf{Y}_{\sigma(k):k}] - {}^i\mathcal{O}_d[\mathbf{P}_{\sigma(k):k-1}])) + \|\mathbf{N}_n\|_\infty w([\mathbf{P}_{\sigma(k):k}]) \\
&\leq \quad \|\mathbf{A}^{n-1}\|_\infty w(-({}^i\mathcal{O})^{-1}({}^i\mathcal{H}[{}^i\mathbf{Z}_{\sigma(k):k}] + {}^i\mathcal{O}_d[\mathbf{P}_{\sigma(k):k-1}])) + \|\mathbf{N}_n\|_\infty w([\mathbf{P}_{\sigma(k):k}]) \\
&\leq \quad \|\mathbf{A}^{n-1}\|_\infty \|{}^i\mathcal{O}^{-1}\,{}^i\mathcal{H}\|_\infty w([{}^i\mathbf{Z}_{\sigma(k):k}]) + \|\mathbf{A}^{n-1}\|_\infty \|{}^i\mathcal{O}^{-1}\,{}^i\mathcal{O}_d\|_\infty w([\mathbf{P}_{\sigma(k):k-1}]) + \\
&\qquad \|\mathbf{N}_n\|_\infty w([\mathbf{P}_{\sigma(k):k}]) \\
&\leq \quad \|\mathbf{A}^{n-1}\|_\infty \|{}^i\Xi_z\|_\infty w([{}^i\mathbf{Z}_{\sigma(k):k}]) + \|\mathbf{A}^{n-1}\|_\infty \|{}^i\Xi_p\|_\infty w([\mathbf{P}_{\sigma(k):k-1}]) + \\
&\qquad \|\mathbf{N}_n\|_\infty w([\mathbf{P}_{\sigma(k):k}]) \\
&\leq \quad \beta_v \min_{i\in\{1,\ldots N\}}\{\max_{j\in\{\sigma(k),\ldots\sigma(k)+n-1\}}\{w([{}^i\mathbf{v}_j])\}\} + \\
&\qquad\qquad \beta_d \max_{j\in\{\sigma(k),\ldots\sigma(k)+n-1\}}\{w([\mathbf{w}_j])\}.
\end{aligned}$$

Outline

Fault detection:

For each sensor $i \in \mathcal{P} = \{1, \ldots, p\}$, with $p < N$

Set-membership detection tests

$$^{(m,i)}\mathbf{y}_k \in [^{(p,i)}\mathbf{y}_k], \begin{cases} \text{True} \Rightarrow s_i = 1 \text{ (Healty sensor)} \\ \text{False} \Rightarrow s_i = 0 \text{ (Faulty sensor)}, \end{cases}$$

where

$$[^{(p,i)}\mathbf{y}_k] = {}^i\mathbf{C}[^p\mathbf{x}_k] + {}^i\mathbf{D}\mathbf{u}_k + {}^i\mathbf{F}[^i\mathbf{v}_k], \ i \in \mathcal{P}.$$

Set of valid sensors

Based on the results of the set-membership tests all sensors with $s_i = 0$ are discarded and those with $s_i = 1$ are retained,

$$\mathcal{S} = \{i \in \mathcal{P} \mid s_i = 1\}$$

Prevention and Resilience strategy:

- From $\mathcal{S}$ select randomly a subset $\mathcal{S}^\star$ of valid sensors to perform several set-inversion operation.

$$\forall l \in \mathcal{S}^\star, \; [^{(\mathrm{inv},l)}\mathbf{x}_{\sigma(k)}]. \tag{1}$$

- Discard all inconsistent boxes $[^{(\mathrm{inv},l)}\mathbf{x}_{\sigma(k)}]$ that satisfy

$$[^{(\mathrm{inv},l)}\mathbf{x}_{\sigma(k)}] \cap [^{p}\mathbf{x}_{\sigma(k)}] = \emptyset \tag{2}$$

  and form a new subset

$$\mathcal{S}^{\star\star} = \{l \in \mathcal{S}^\star \mid (2) \text{ is false}\}. \tag{3}$$

- Correct the predicted state enclosure at the past time instant $\sigma(k)$ by intersecting all valid inverted state enclosures. That is,

$$[^{c}\mathbf{x}_{\sigma(k)}] = \left(\cap_{l \in \mathcal{S}^{\star\star}} [^{(\mathrm{inv},l)}\mathbf{x}_{\sigma(k)}]\right) \cap [^{p}\mathbf{x}_{\sigma(k)}] \tag{4}$$

Remark:

All unknown signals $^{i}\mathbf{a}_k$ that satisfy the intersection test (2) are considered as malicious attacks.

Outline

Secure state estimation algorithm:

Phase 2: Secure predictor-corrector estimator

3. **Get** $\mathcal{S}$ from Phase 1 (based on the output set-membership tests)
4. **Select** randomly a subset $\mathcal{S}^\star$ from $\mathcal{S}$

- **For** $k \geq n-1$ to ∞

   5. $\sigma(k) := k - (n-1)$
   6. **Set-inversion**: $\forall l \in \mathcal{S}^\star$, **compute**

$$[{}^{(\mathrm{inv},l)}\mathbf{x}_{\sigma(k)}] = {}^{(\mathrm{inv},l)}\hat{\mathbf{x}}_{\sigma(k)} \oplus {}^{l}\Xi_p[\mathbf{P}_{\sigma(k):\sigma(k)+n-2}] \oplus {}^{l}\Xi_z[{}^{l}\mathbf{Z}_{\sigma(k):\sigma(k)+n-1}]$$

   7. **Form** the subset $\mathcal{S}^{\star\star}$ (based on the set-membership tests (2)-(3))
   8. **Correction step**

$$[{}^{c}\mathbf{x}_{\sigma(k)}] = \left(\cap_{l\in\mathcal{S}^{\star\star}} [{}^{(\mathrm{inv},l)}\mathbf{x}_{\sigma(k)}]\right) \cap [{}^{p}\mathbf{x}_{\sigma(k)}]$$

   9. **Set-propagation**

$$[{}^{p}\mathbf{x}_{k+1}] := \mathbf{A}^n[{}^{c}\mathbf{x}_{\sigma(k)}] \oplus \mathbf{N}_n[\mathbf{P}_{\sigma(k):k}] \oplus \mathbf{B}_n\mathbf{U}_{\sigma(k):k}$$

   10. $[\mathbf{x}_{k+1}] := [{}^{p}\mathbf{x}_{k+1}]$
   11. **Form** a new valid sensors set $\mathcal{S}$
   12. **Select** randomly a subset $\mathcal{S}^\star$ from $\mathcal{S}$

- **end**
- **Return** $[\mathbf{x}_k], \ k \in \{1, 2, \ldots, \infty\}$

Outline

Illustrative example:

Considered system

System Matrices

$$\mathbf{A} = \begin{pmatrix} 0.9630 & 0.0181 & 0.0187 \\ 0.1808 & 0.8195 & -0.0514 \\ -0.1116 & 0.0344 & 0.95861 \end{pmatrix}, \ \mathbf{B} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \mathbf{E} = \begin{pmatrix} 0.0996 & 0.0213 \\ 0.0050 & 0.1277 \\ 0.1510 & 0.0406 \end{pmatrix},$$

$$^{1}\mathbf{C} = \begin{pmatrix} 1 & 0 & -1 \end{pmatrix}, \ ^{2}\mathbf{C} = \begin{pmatrix} -1 & 1 & 1 \end{pmatrix},$$

$$^{1}\mathbf{F} = {}^{2}\mathbf{F} = 1, \ ^{1}\mathbf{D} = {}^{2}\mathbf{D} = 0.$$

System input and initial condition

- System input: $\mathbf{u}_k = 5\sin(100k)$
- Initial condition: $\mathbf{x}_0 = (5, 0, 5)^T$

Observability conditions

- The matrix pairs $(\mathbf{A}, {}^{1}\mathbf{C})$ and $(\mathbf{A}, {}^{2}\mathbf{C})$ are observable
- The used number of sensors $p = N = 2$.

Illustrative example:

Initial state box

$$[\mathbf{x}_0] = \{[-10,\ 10]; [-3,\ 3]; [-10,\ 10]\}$$

Feasible box of state disturbance

$$\mathbf{w}_k \in [\mathbf{w}_k] = \{[-0.1,\ 0.1]; [-0.1,\ 0.1]\}, \forall k \geq 0$$

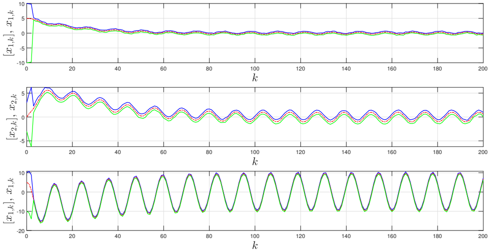
Feasible boxes of measurement noises

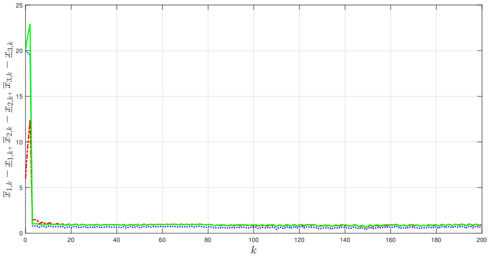
$$^1\mathbf{v}_k \in [\mathbf{v}_k] = [-0.01, 0.01], \forall k \geq 0$$

$$^2\mathbf{v}_k \in [\mathbf{v}_k] = [-0.01, 0.01], \forall k \geq 0$$

Illustrative example:

Simulation results: First test (Sensors Free From Anomalies)





- **Interval estimation of each state variable.**
- Blue and green lines correspond to the estimated upper and lower bounds.
- Red dashed lines correspond to actual state variables of the system.

Convergence characteristics

- Convergence reached at

$$k = 3$$

- For all $k \geq 3$,

$$w([\mathbf{x}_k]) < 1$$

Illustrative example:

Simulation results: second test (Sensors Subject to Faults)

The considered fault on the first sensor

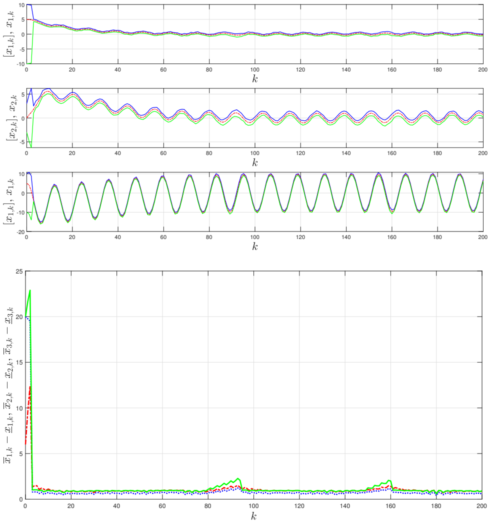
$$ {}^{1}a_k = \begin{cases} 3 & \text{if} \quad 79 \leq k \leq 88 \\ 0 & \quad\;\; \text{otherwise} \end{cases} $$

The considered fault on the second sensor

$$ {}^{2}a_k = \begin{cases} 3 & \text{if} \quad 149 \leq k \leq 158 \\ 0 & \quad\;\; \text{otherwise.} \end{cases} $$

Illustrative example:

Simulation results: (Sensors Subject to Faults)



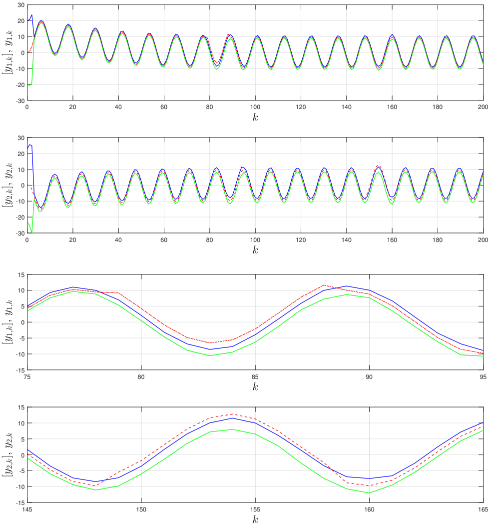
- **Interval estimation of each state variable**.
- Blue and green lines correspond to the estimated upper and lower bounds.
- Red dashed lines correspond to actual state variables of the system.

Characteristics

- The framing property is still guaranteed
- The faults cause inflation on the estimated intervals.

Illustrative example:

Simulation results: second test (Sensors Subject to Faults)



- **Interval prediction of each system output**.
- Blue and green lines correspond to the estimated upper and lower bounds.
- Red dashed lines correspond to the measured system output.

Output set-membership tests

- There is no intersection between $^{(m,1)}\mathbf{y}_k$ and $[^{(p,1)}\mathbf{y}_k]$ over the time sequence $k \in \{79, \ldots, 88\}$

$$^{(m,1)}\mathbf{y}_k \notin [^{(p,1)}\mathbf{y}_k]$$

- There is no intersection between $^{(m,2)}\mathbf{y}_k$ and $[^{(p,2)}\mathbf{y}_k]$ over the time sequence $k \in \{149, \ldots, 158\}$

$$^{(m,1)}\mathbf{y}_k \notin [^{(p,1)}\mathbf{y}_k]$$

Illustrative example:

Simulation results: third test (Sensors Subject to Malicious Attacks)

The considered attack on the first sensor

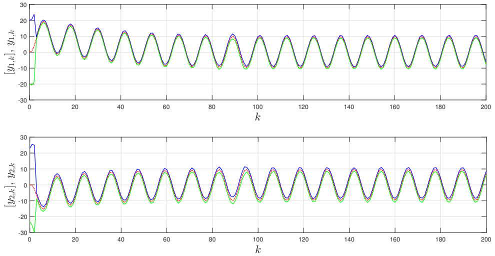
$$ {}^{1}a_k = \begin{cases} 0.1 & \text{if} \quad 79 \leq k \leq 80 \\ 0 & \quad\quad \text{otherwise} \end{cases} $$

The considered attack on the second sensor

$$ {}^{2}a_k = \begin{cases} 0.1 & \text{if} \quad 149 \leq k \leq 150 \\ 0 & \quad\quad \text{otherwise.} \end{cases} $$

Illustrative example:

Simulation results: third test (Sensors Subject to Malicious Attacks)



- **Interval prediction of each system output**.
- Blue and green lines correspond to the estimated upper and lower bounds.
- Red dashed lines correspond to the measured system output.

Output set-membership tests

- This test fails to detect the presence of the attack over the time sequence $k \in \{80, 81\}$

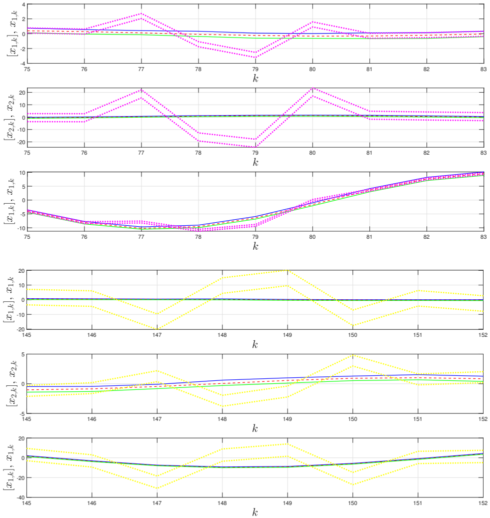
$$^{(m,1)}\mathbf{y}_k \in [^{(p,1)}\mathbf{y}_k]$$

- This test fails to detect the presence of the attack over the time sequence $k \in \{150, 151\}$

$$^{(m,2)}\mathbf{y}_k \in [^{(p,2)}\mathbf{y}_k]$$

Illustrative example:

Simulation results: third test (Sensors Subject to Malicious Attacks)



- **Interval estimation of each state variable.**
- Blue and green lines correspond to the estimated upper and lower bounds.
- Red dashed lines correspond to actual state variables of the system.
- Magenta and yellow lines correspond to the estimated upper and lower bounds.

State set-membership tests

- There is no intersection between $[^{(\mathrm{inv},1)}\mathbf{x}_{\sigma(k)}]$ and $[^{(p,1)}\mathbf{x}_{\sigma(k)}]$ over the time sequence $k \in \{77, \ldots, 80\}$

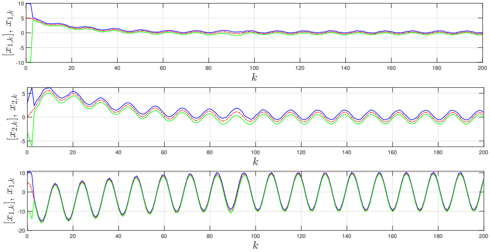
$$[^{(\mathrm{inv},1)}\mathbf{x}_{\sigma(k)}] \cap [^{(p,1)}\mathbf{x}_{\sigma(k)}] = \emptyset$$

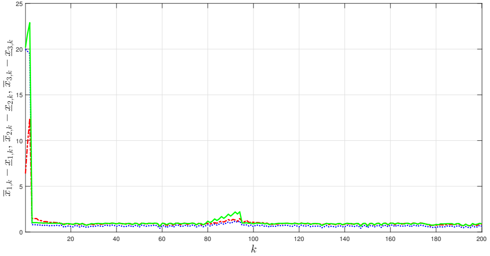
- There is no intersection between $[^{(\mathrm{inv},2)}\mathbf{x}_{\sigma(k)}]$ and $[^{(p,2)}\mathbf{x}_{\sigma(k)}]$ over the time sequence $k \in \{147, \ldots, 150\}$

$$[^{(\mathrm{inv},2)}\mathbf{x}_{\sigma(k)}] \cap [^{(p,2)}\mathbf{x}_{\sigma(k)}] = \emptyset$$

Illustrative example:

Simulation results: third test (Sensors Subject to Malicious Attacks)





- **Interval estimation of each state variable**.
- Blue and green lines correspond to the estimated upper and lower bounds.
- Red dashed lines correspond to actual state variables of the system.

Characteristics

- The framing property is still guaranteed
- The attacks cause inflation on the estimated intervals.

Conclusion

Some conclusion remarks:

- In bounded error context, set computations should be applied at the last step.
- Consistency techniques is a natural way to detect and isolate sensors anomalies

Perspectives:

- Applied advanced Moving Target Defense strategy
- Consider the case of Faults and Attacks on system actuators

Some references

- N. Meslem and A. Hably, *Robust set-membership state estimator against outliers in data*, IET Control Theory & Applications 14 (13), 1752-1761, 2020.
- N. Meslem and N. Ramdani, *A new approach to design set-membership state estimators for discrete-time linear systems based on the observability matrix*, International Journal of Control 93 (11), 2541-2550, 2020.
- N. Meslem and N. Ramdani, *Forward-backward set-membership state estimator based on interval analysis*, 2018 Annual American Control Conference (ACC), 5161-5166, 2018.
- N. Meslem and N. Ramdani, *A comparison of two methods for state estimation: A statistical Kalman filter, and a deterministic interval-based approach*, 2018 26th Mediterranean Conference on Control and Automation (MED), 127-132, 2018.