Carl von Ossietzky Universität Oldenburg

Set-Based Methods for Secure State Estimation under Consideration of Cyber-Attack Scenarios

Pre-Conference Workshop European Control Conference ECC 2026 Reykjavík, Iceland

Andreas Rauh, July 07, 2026

Carl von Ossietzky Universität Oldenburg, Germany
(joint work with Nacim Meslem)

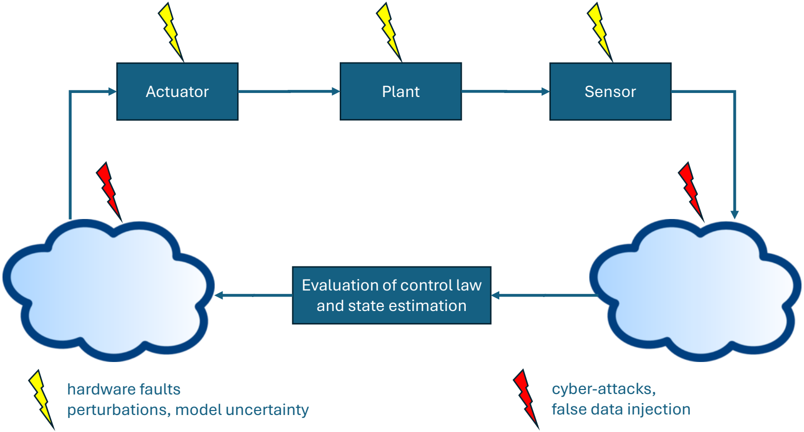
Carl von Ossietzky Universität Oldenburg

Contents

- Reliability of control and state estimation for networked cyber-physical systems
  - Robustness against inevitable model mismatch
  - Robustness against perturbations in the system dynamics
  - Robustness against sensor noise
- Resilience against cyber-attacks by exploitation of model-based approaches
- Set-valued estimation approaches
- Distinction between measurement errors and malicious attacks
- Conclusions and outlook on future work

Carl von Ossietzky Universität Oldenburg

Networked Control of Cyber-Physical Systems



Basic Challenge

Discrete-time linear system model (written as a difference inclusion)

Dynamic system model

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

where $\mathbf{x}_k \in \mathbb{R}^n$ is the state vector, $\mathbf{u}_k \in \mathbb{R}^m$ the input vector, and ${}^i\mathbf{y}_k \in \mathbb{R}^{n_i}$ the output associated with the i-th group of sensors, $i \in \{1, \dots, N\}$

In this presentation

Assumption of constant dynamics matrices $\mathbf{A}$, $\mathbf{B}$, ${}^i\mathbf{C}$, ${}^i\mathbf{D}$, $\mathbf{E}$, and ${}^i\mathbf{F}$

Carl von Ossietzky Universität Oldenburg

Basic Challenge

Discrete-time linear system model (written as a difference inclusion)

Dynamic system model

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

Uncertainties

- $[\mathbf{w}_k]$: 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

Basic Challenge

Discrete-time linear system model (written as a difference inclusion)

Dynamic system model

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

Goal

Reconstruct the state of the system even though the measurements may be corrupted by a cyber-attack in the form

$${}^{(m,i)}\mathbf{y}_k = {}^i\mathbf{y}_k + {}^i\mathbf{a}_k$$

Carl von Ossietzky Universität Oldenburg

Formulation of the Objective

State reconstruction at each time step

$$\mathcal{X}_k = \left\{ \mathbf{x}_k \;\middle|\; \begin{array}{c} \text{Consistency with system dynamics} \\ \mathbf{x}_k = \mathbf{A}\mathbf{x}_{k-1} + \mathbf{B}\mathbf{u}_{k-1} + \mathbf{E}\mathbf{w}_{k-1}, \\ \mathbf{x}_{k-1} \in [\mathbf{x}_{k-1}] \\ \mathbf{w}_{k-1} \in [\mathbf{w}_{k-1}] \end{array} \bigwedge \begin{array}{c} \text{Consistency with measurements} \\ \mathbf{x}_k \in \textbf{Set-Inversion}\left([{}^{i}\mathbf{y}_k]\right) \end{array} \right\}$$

The set inversion produces an **outer enclosure** of the state vector $[{}^{\mathrm{inv}}\mathbf{x}_k]$ from the feasible domain of system outputs

$$[{}^{i}\mathbf{y}_k] = {}^{(m,i)}\mathbf{y}_k \oplus (-{}^{i}\mathbf{F}[{}^{i}\mathbf{v}_k]), i \in \{1, \dots N\}$$

Carl von Ossietzky Universität Oldenburg

Interval Predictor (1)

State prediction between the time instants s and k

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

with the corresponding interval formulation

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

Note – Reduction of *wrapping and dependency effect* similar to:

I. Krasnochtanova, A. Rauh, M. Kletting, H. Aschemann, E.P. Hofer, K.-M. Schoop: *Interval methods as a simulation tool for the dynamics of biological wastewater treatment processes with parameter uncertainties.* Applied Mathematical Modelling. Vol 34, pp.744–762, 2010. DOI:10.1016/j.apm.2009.06.019.

Interval Predictor (2)

State prediction between the time instants s and k

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

$$\begin{aligned}
\sigma(k) &= k - s \\
\mathbf{N}_{\sigma(k)} &= \left(\mathbf{A}^{\sigma(k)-1}\mathbf{E},\ \mathbf{AE},\ \ldots,\ \mathbf{E}\right) \\
\mathbf{B}_{\sigma(k)} &= \left(\mathbf{A}^{\sigma(k)-1}\mathbf{B},\ \mathbf{AB},\ \ldots,\ \mathbf{B}\right) \\
[\mathbf{P}_{s:s+\sigma(k)-1}] &= \left([\mathbf{w}_s]^T,\ [\mathbf{w}_{s+1}]^T,\ \ldots,\ [\mathbf{w}_{s+\sigma(k)-1}]^T]\right)^T \\
[\mathbf{U}_{s:s+\sigma(k)-1}] &= \left(\mathbf{u}_s^T,\ \mathbf{u}_{s+1}^T,\ \ldots,\ \mathbf{u}_{s+\sigma(k)-1}^T]\right)^T
\end{aligned}$$

Carl von Ossietzky Universität Oldenburg

Interval-Based State Correction at Past Time Instants

Consideration of the simplified case $n_i = 1$

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

where

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

and

$${}^{i}\Xi_p = -\left({}^{i}\mathcal{O}\right)^{-1}\,{}^{i}\mathcal{O}_d\,,\quad {}^{i}\Xi_z = -\left({}^{i}\mathcal{O}\right)^{-1}\,{}^{i}\mathbf{H}\,,\quad {}^{i}\mathbf{H}\ \text{depends on}\ {}^{i}\mathbf{F}$$

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

Interval-Based State Correction at Past Time Instants

Consideration of the simplified case $n_i = 1$

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

where

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

and

$${}^{i}\Xi_p = -\left({}^{i}\mathcal{O}\right)^{-1}\,{}^{i}\mathcal{O}_d\ ,\quad {}^{i}\Xi_z = -\left({}^{i}\mathcal{O}\right)^{-1}\,{}^{i}\mathbf{H}\ ,\quad {}^{i}\mathbf{H}\ \text{depends on}\ {}^{i}\mathbf{F}$$

$${}^{i}\mathcal{O}_u = \begin{pmatrix} {}^{i}\mathbf{D} & \mathbf{0} & \dots & \mathbf{0} & \mathbf{0} \\ {}^{i}\mathbf{C}\mathbf{B} & {}^{i}\mathbf{D} & \dots & \vdots & \vdots \\ \vdots & \vdots & \dots & \vdots & \vdots \\ {}^{i}\mathbf{C}\mathbf{A}^{n-2}\mathbf{B} & {}^{i}\mathbf{C}\mathbf{A}^{n-3}\mathbf{B} & \dots & {}^{i}\mathbf{C}\mathbf{B} & {}^{i}\mathbf{D} \end{pmatrix}$$

Carl von Ossietzky Universität Oldenburg

Interval-Based State Correction at Past Time Instants

Consideration of the simplified case $n_i = 1$

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

where

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

and

$${}^{i}\Xi_p = -\left({}^{i}\mathcal{O}\right)^{-1}\,{}^{i}\mathcal{O}_d\,, \quad {}^{i}\Xi_z = -\left({}^{i}\mathcal{O}\right)^{-1}\,{}^{i}\mathbf{H}\,, \quad {}^{i}\mathbf{H} \text{ depends on } {}^{i}\mathbf{F}$$

$$\mathbf{U}_{\sigma(k):\sigma(k)+n-1} = \begin{pmatrix} \mathbf{u}_{\sigma(k)} \\ \mathbf{u}_{\sigma(k)+1} \\ \vdots \\ \mathbf{u}_{\sigma(k)+n-1} \end{pmatrix}, \quad {}^{i}\mathbf{Y}_{\sigma(k):\sigma(k)+n-1} = \begin{pmatrix} {}^{(m,i)}\mathbf{y}_{\sigma(k)} \\ {}^{(m,i)}\mathbf{y}_{\sigma(k)+1} \\ \vdots \\ {}^{(m,i)}\mathbf{y}_{\sigma(k)+n-1} \end{pmatrix}$$

$$\left[{}^{i}\mathbf{Z}_{\sigma(k):\sigma(k)+n-1}\right] = \left(\left[{}^{i}\mathbf{v}_{\sigma(k)}\right]^T,\ \left[{}^{i}\mathbf{v}_{\sigma(k)+1}\right]^T,\ \ldots,\ \left[{}^{i}\mathbf{v}_{\sigma(k)+n-1}\right]^T\right)^T$$

Carl von Ossietzky Universität Oldenburg

Interval-Based State Correction at Past Time Instants

Consideration of the simplified case $n_i = 1$

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

where

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

and

$${}^{i}\Xi_p = -\left({}^{i}\mathcal{O}\right)^{-1}\,{}^{i}\mathcal{O}_d\,,\quad {}^{i}\Xi_z = -\left({}^{i}\mathcal{O}\right)^{-1}\,{}^{i}\mathbf{H}\,,\quad {}^{i}\mathbf{H}\ \text{depends on}\ {}^{i}\mathbf{F}$$

Note

Kalman's observability criterion and the Theorem of Cayley-Hamilton provide an **upper bound** for the required previous time instants for set inversion in the case of linear systems. However, this is **generally not true** in the nonlinear case:

T. Paradowski, S. Lerch, M. Damaszek, R. Dehnert, B. Tibken: *Observability of Uncertain Nonlinear Systems Using Interval Analysis*. Algorithms, vol. 13, no. 3, paper 66, 2020. DOI:10.3390/a13030066

Interval-Based State Estimator (1)

Correction of the predicted state enclosure

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

Interval-Based State Estimator (1)

Correction of the predicted state enclosure

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

Prediction of the corrected enclosure

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

where

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

Interval-Based State Estimator (2)

Proposition

Under the observability assumption of the pairs

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

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,

$$w\big([\mathbf{x}_k]\big) \leq \beta_v \min_{i \in \{1,\dots N\}} \{w\big([{}^{i}\mathbf{Z}_{\sigma(k):\sigma(k)+n-1}]\big)\} + \beta_d w\big([\mathbf{P}_{\sigma(k):\sigma(k)+n-1}]\big),$$

where

– $\beta_v = \left\|\mathbf{A}^n\right\|_\infty \min_{i \in \{1,\dots N\}}\{\left\|{}^{i}\Xi_z\right\|_\infty\}$ and

– $\beta_d = \left\|\mathbf{N}_n\right\|_\infty + \left\|\mathbf{A}^n\right\|_\infty \min_{i \in \{1,\dots N\}}\{\left\|{}^{i}\Xi_p\right\|_\infty\}$.

Consideration of Sensor Anomalies

Decomposition of the measurements

$$ {}^{(m,i)}\mathbf{y}_k = {}^{i}\mathbf{y}_k + {}^{i}\mathbf{a}_k $$

Implementation of a bank of filters (consistency of predicted measurements)

For ${}^{i}\mathbf{a}_k = \mathbf{0}$, we have the inclusions

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

with

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

Fault Detection and Isolation

Detection of the occurrence of an anomaly

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

All sensors for which the consistency test of the predicted measurements fails, are guaranteed to be faulty (i.e., behave anomalously)

Set of valid sensors

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

and discard all sensors with $s_i = 0$

Carl von Ossietzky Universität Oldenburg

Prevention of Faulty Estimates due to Attacks: Ensure Resilience

– From $\mathcal{S}$ select randomly a subset $\mathcal{S}^\star$ of valid sensors to perform several set-inversion stages. Based on the interval inversion formula we obtain

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

Prevention of Faulty Estimates due to Attacks: Ensure Resilience

- From $\mathcal{S}$ select randomly a subset $\mathcal{S}^\star$ of valid sensors to perform several set-inversion stages. Based on the interval inversion formula we obtain

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

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

$$\left[{}^{(\mathrm{inv},l)}\mathbf{x}_{\sigma(k)}\right] \cap \left[{}^{p}\mathbf{x}_{\sigma(k)}\right] = \emptyset \qquad (\star)$$

  and form a new subset

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

Prevention of Faulty Estimates due to Attacks: Ensure Resilience

- From $\mathcal{S}$ select randomly a subset $\mathcal{S}^\star$ of valid sensors to perform several set-inversion stages. Based on the interval inversion formula we obtain

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

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

$$\left[{}^{(\mathrm{inv},l)}\mathbf{x}_{\sigma(k)}\right] \cap \left[{}^{p}\mathbf{x}_{\sigma(k)}\right] = \emptyset \qquad (\star)$$

  and form a new subset

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

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

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

Illustrating Example

Dynamic system model

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

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

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

Measurement noise

$$^{i}\mathbf{v}_k \in [-0.01, 0.01], \; i \in \{1, 2\}, \; \forall k \geq 0$$

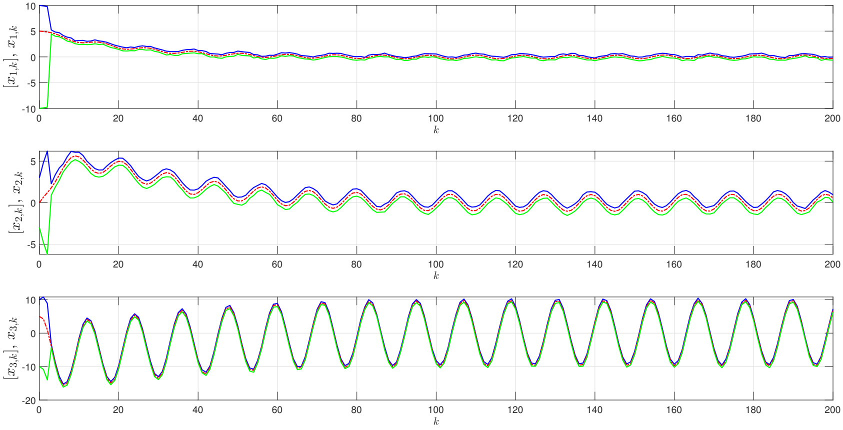
Process noise

$$\mathbf{w}_k \in ([-0.1, 0.1], [-0.1, 0.1])^T, \; \forall k \geq 0$$

Initial uncertainty of the estimator

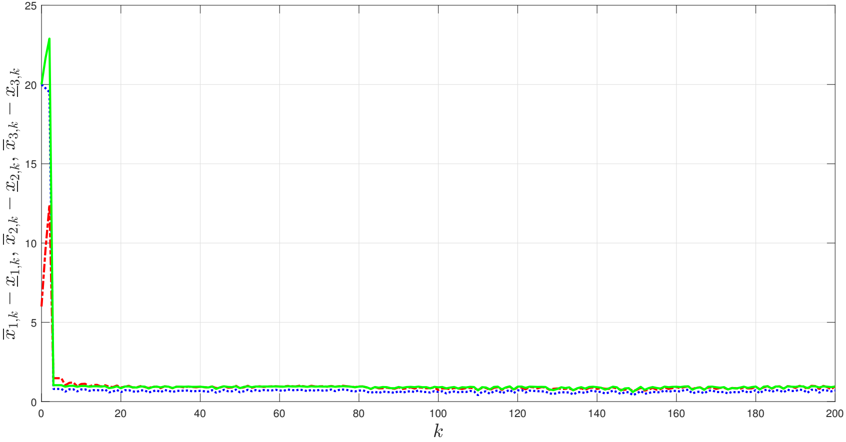
$$\mathbf{x}_0 \in ([-10, 10], [-3, 3], [-10, 10])^T$$

Anomaly-Free Case (1)



Carl von Ossietzky Universität Oldenburg

Anomaly-Free Case (2)



Case of Sensor Faults (1)

Faulty behavior of sensor 1

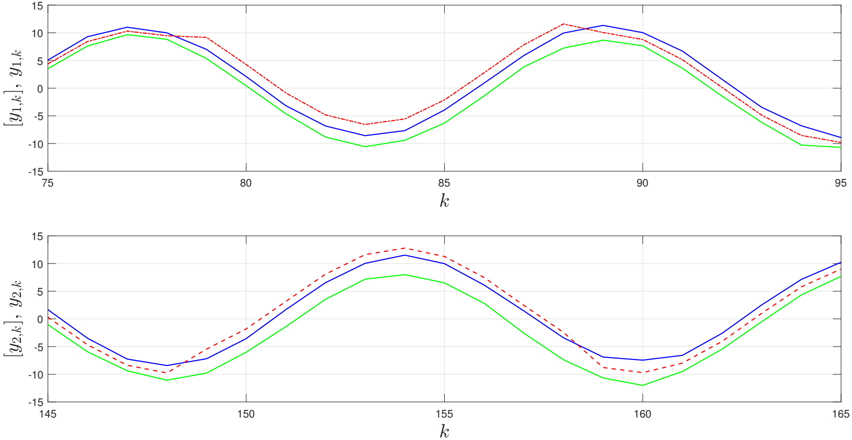
$$^{1}a_k = \begin{cases} 3 & \text{if } 79 \leq k \leq 88 \\ 0 & \text{otherwise} \end{cases}$$

Faulty behavior of sensor 2

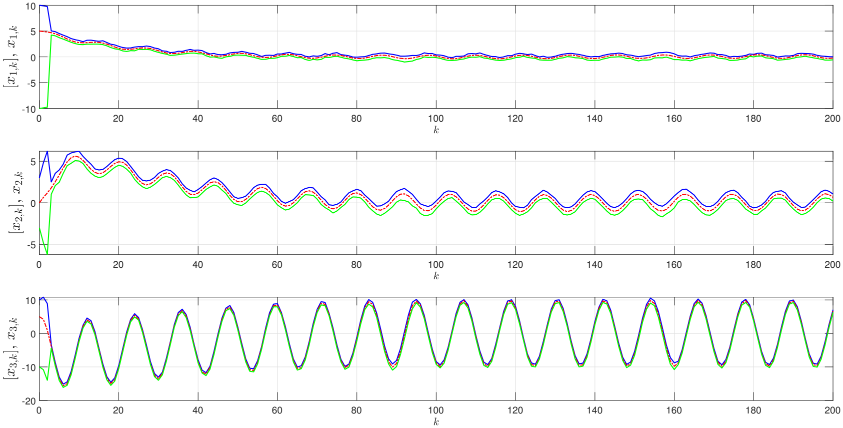
$$^{2}a_k = \begin{cases} 3 & \text{if } 149 \leq k \leq 158 \\ 0 & \text{otherwise} \end{cases}$$

The magnitude of the fault is that large that the sensor validation test succeeds: Measured values are inconsistent with their predictions

Case of Sensor Faults (2)

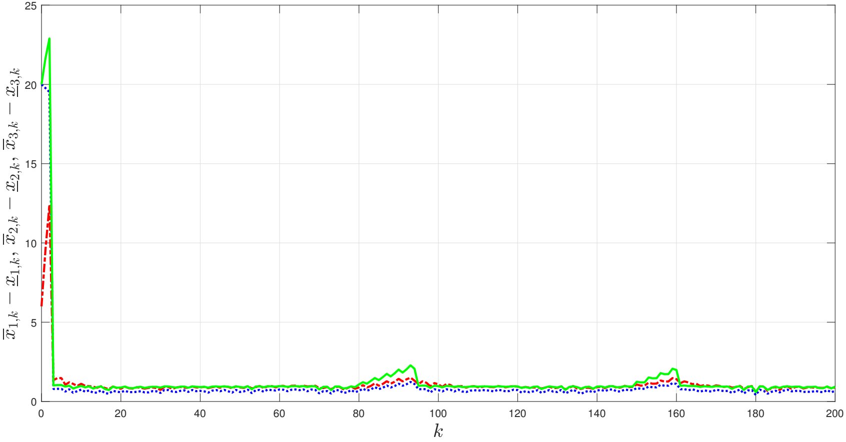


Case of Sensor Faults (3)



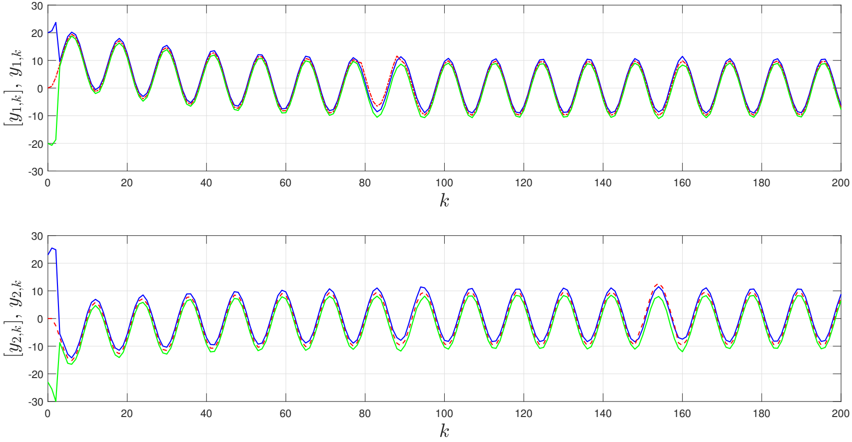
Carl von Ossietzky Universität Oldenburg

Case of Sensor Faults (4)



Carl von Ossietzky Universität Oldenburg

Case of Sensor Faults (5)



Carl von Ossietzky Universität Oldenburg

Malicious Attacks (1)

Attack on sensor 1

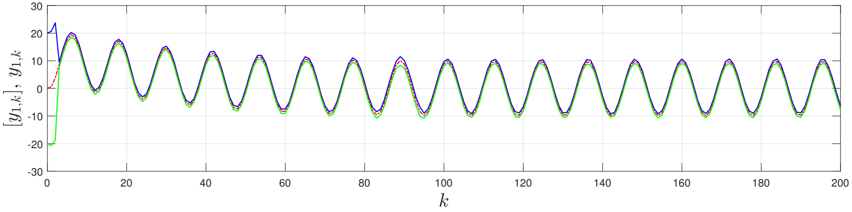
$$^{1}a_k = \begin{cases} 0.1 & \text{if } 79 \leq k \leq 80 \\ 0 & \text{otherwise} \end{cases}$$

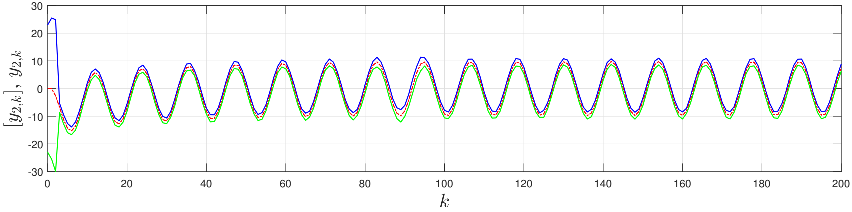
Attack on sensor 2

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

Malicious Attacks (2)

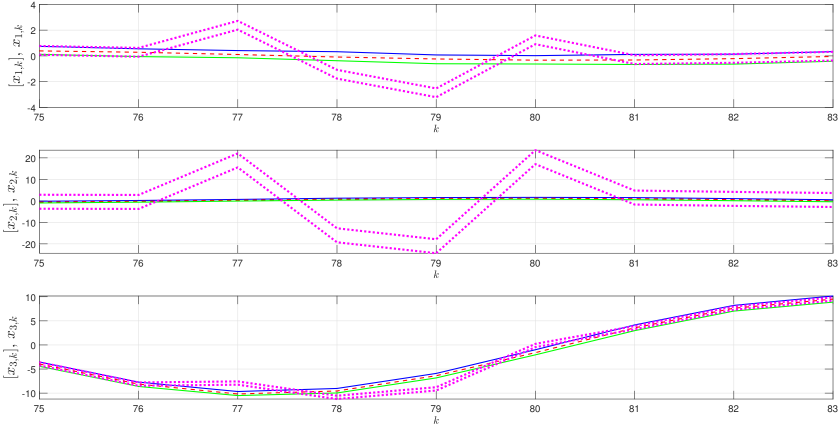
Measured (dashed) vs. predicted outputs: Sensor validation test fails





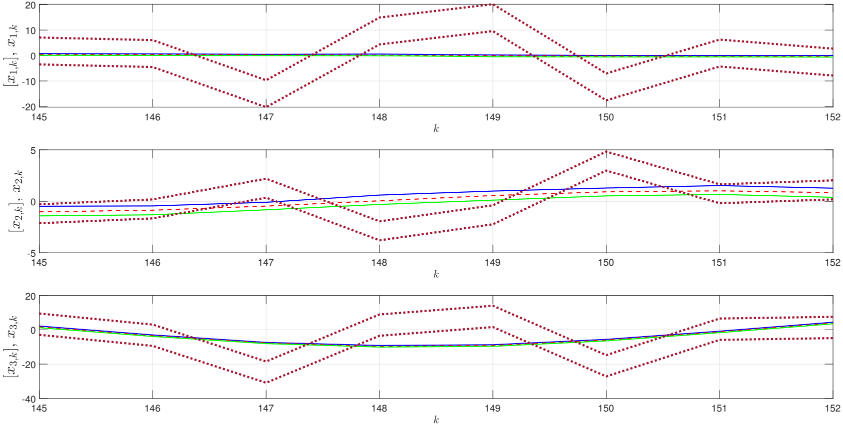
Malicious Attacks (3)

Solid lines correspond to the predicted state enclosure while the dotted lines represent the inverted state enclosure from the data generated by the first sensor

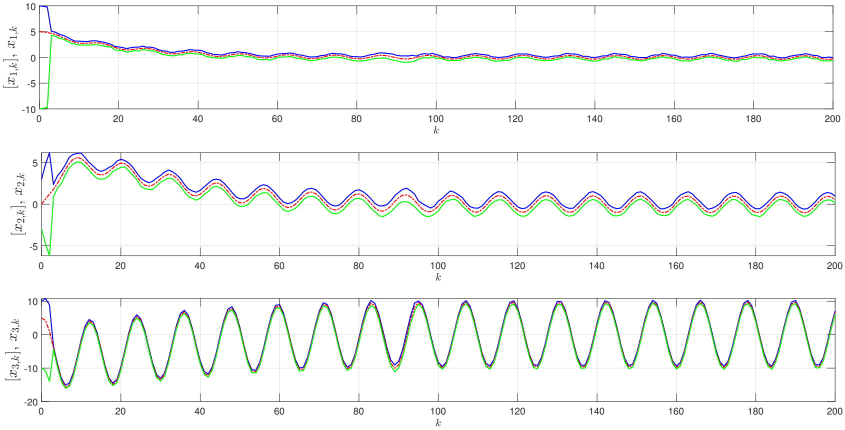


Malicious Attacks (4)

Solid lines correspond to the predicted state enclosure while the dotted lines represent the inverted state enclosure from the data generated by the second sensor



Malicious Attacks (5)



Conclusions and Future Work

- Set-based state estimation based on prediction–correction scheme
- Handling of faulty sensor data
- Resilience against malicious attacks

- Generalization to more complex cyber-physical systems
- Treatment of nonlinear models

N. Meslem, A. Rauh, Andreas. *Secure State Estimation Algorithm for Discrete-Time Linear Systems: A Set-Valued Approach*. In: T.N. Dinh, A. Rauh, S.Z. Yong, Z. Wang (Eds.): *Set-Valued Approaches to Control and Estimation of Uncertain Systems*, Springer, 2025. DOI:10.1007/978-3-031-94239-6_1.

Carl von Ossietzky Universität Oldenburg

Thank you!

Andreas Rauh

andreas.rauh@uni-oldenburg.de

www.interval-methods.de/seminars

Carl von Ossietzky
Universität
Oldenburg

Thank you!

Andreas Rauh
andreas.rauh@uni-oldenburg.de

www.uol.de/en/computingscience/dcis