Privileged Estimate Fusion With Correlated Gaussian Keystreams

Conference on Decision and Control (CDC) 2022

Marko Ristic, Benjamin Noack

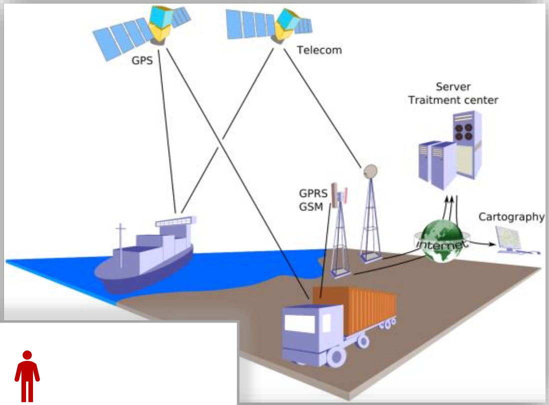
Autonomous Multisensor Systems Group
Institute for Intelligent Cooperating Systems
Faculty of Computer Science
Otto von Guericke University, Magdeburg

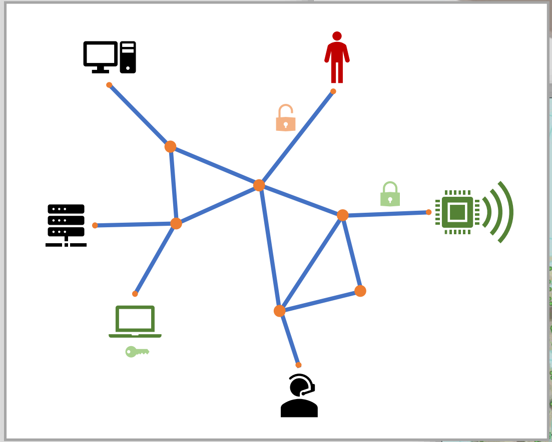
9.12.2021

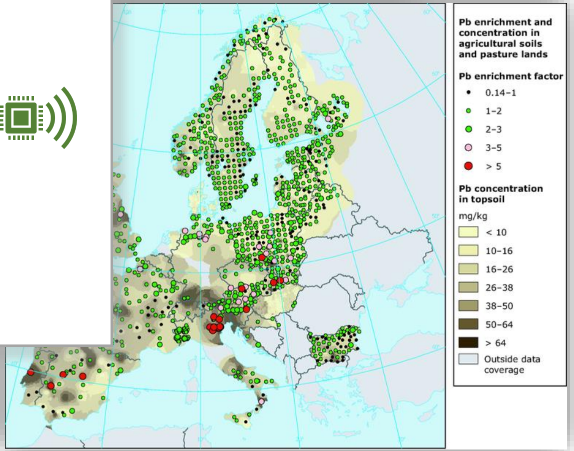
Security in Networks

- Growing number of public networks
- Increasingly used by distributed sensors, IoT devices, cloud computing, etc
- Greater need for security guarantees
- Affected users
  - Private
  - Commercial
  - Government

https://fr.wikipedia.org/wiki/G%C3%A9olocalisation#/media/Fichier:Geolocation.png



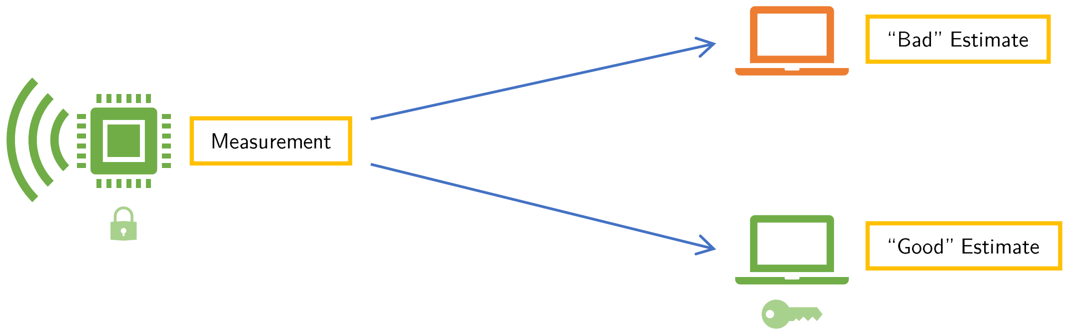




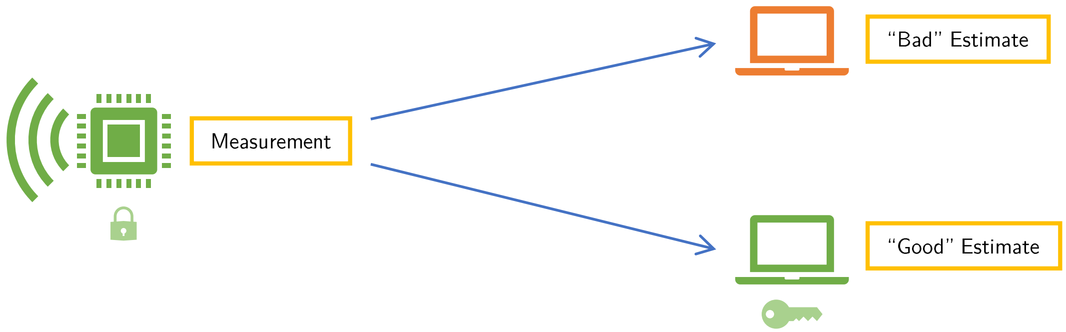
https://www.eea.europa.eu/data-and-maps/figures/soil-contamination-by-heavy-metals

Privilege in Estimation

- Public measurements useable for state estimation
- Trusted or special users may be granted *privilege*
- Privileged users should perform *better* than unprivileged ones



- Public measurements useable for state estimation
- Trusted or special users may be granted *privilege*
- Privileged users should perform *better* than unprivileged ones



- Security guarantee concerns proving the minimum difference in performance

Single Sensor Privilege

- Add generated Gaussian keystream to measurements
- Anyone holding generation key can remove added noise

Single Sensor Privilege

- Add generated Gaussian keystream to measurements
- Anyone holding generation key can remove added noise

    - System

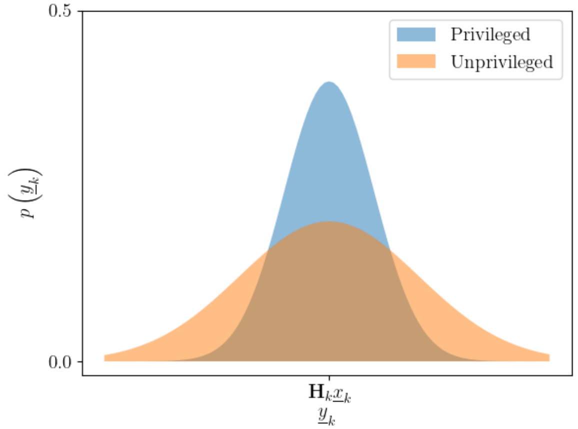
$$\underline{x}_k = \mathbf{F}_k \underline{x}_{k-1} + \underline{w}_k \qquad \underline{w}_k \sim \mathcal{N}(\underline{0}, \mathbf{Q}_k)$$

    - Measurement

$$\underline{y}_k = \mathbf{H}_k \underline{x}_k + \underline{v}_k \qquad \underline{v}_k \sim \mathcal{N}(\underline{0}, \mathbf{R}_k)$$

    - Modified measurement

$$\underline{y}'_k = \underline{y}_k + \underline{g}_k = \mathbf{H}_k \underline{x}_k + \underline{v}_k + \underline{g}_k \qquad \underline{v}_k \sim \mathcal{N}(\underline{0}, \mathbf{R}_k)\,,\ \underline{g}_k \dot{\sim} \mathcal{N}(\underline{0}, \mathbf{Z})$$



Cryptographic Definition for Performance

- Algorithms

$$\mathsf{Setup}\left(\mathcal{M}_S, \mathcal{M}_M, \kappa\right),$$
$$\mathsf{Noise}\left(\mathsf{pub}, \mathsf{sk}, k, \mathcal{M}_S, \mathcal{M}_M, \underline{y}_1, \ldots, \underline{y}_k\right)$$

- Definitions

$$\mathit{estimator},$$
$$\mathsf{neglCov}_m(\kappa) : \mathbb{N} \to \mathbb{R}^{m \times m}$$

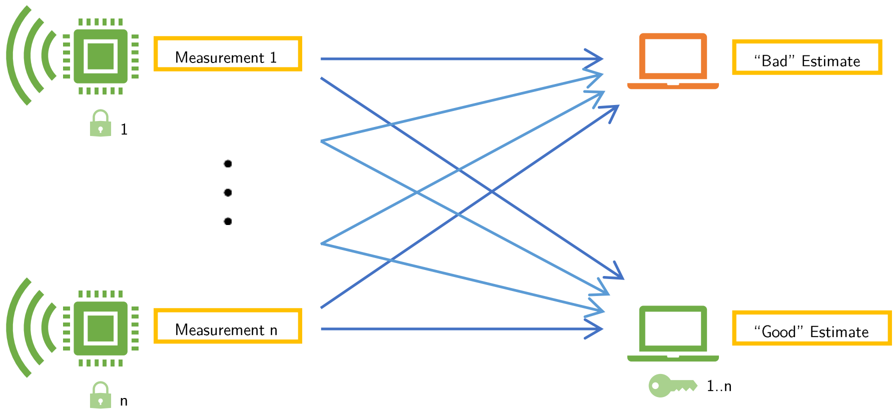
- Covariance Privilege

$(\mathsf{Setup}, \mathsf{Noise})$ meets $\{\mathbf{D}_1, \mathbf{D}_2, \ldots\}$-*Covariance Privilege for Models* $\mathcal{M}_S$ *and* $\mathcal{M}_M$

if for any PPT estimator $\mathcal{A}$, there exists a PPT estimator $\mathcal{A}'$, such that

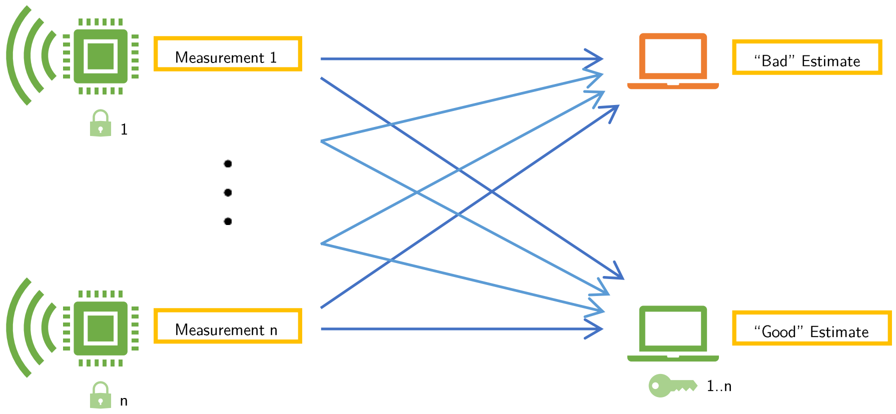
$$\begin{aligned}
&\mathsf{Cov}\left[\mathcal{A}\left(k, \kappa, \mathsf{pub}, \mathcal{M}_S, \mathcal{M}_M, \underline{y}'_1, \ldots, \underline{y}'_k\right) - \underline{x}_k\right] \\
&- \mathsf{Cov}\left[\mathcal{A}'\left(k, \kappa, \mathsf{pub}, \mathcal{M}_S, \mathcal{M}_M, \underline{y}_1, \ldots, \underline{y}_k\right) - \underline{x}_k\right] \\
&\succeq \mathbf{D}_k + \mathsf{neglCov}_m(\kappa)
\end{aligned}$$

- Multiple privileged sensors each adding Gaussian keystream



Complication of Fusion

- Multiple privileged sensors each adding Gaussian keystream



- Two ways of getting better estimates
  - Hold keys to remove added noises (desired)
  - Fuse more measurements (desired only when keys are held as well)

Multisensor Estimation Problem

- Linear models considered
- Kalman Filter optimality in proofs

  - System

$$\underline{x}_k = \mathbf{F}_k \underline{x}_{k-1} + \underline{w}_k \qquad \underline{w}_k \sim \mathcal{N}(\underline{0}, \mathbf{Q}_k)$$

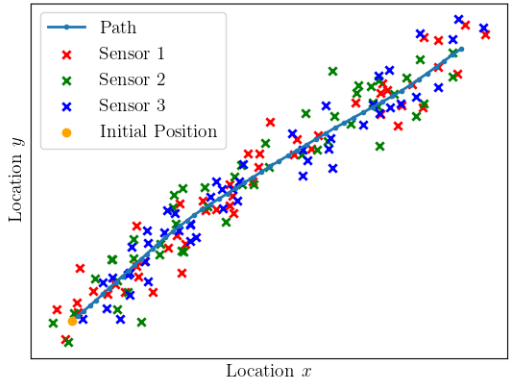
  - Measurements

$$\underline{y}_{k,i} = \mathbf{H}_{k,i} \underline{x}_k + \underline{v}_{k,i} \qquad \underline{v}_{k,i} \sim \mathcal{N}(\underline{0}, \mathbf{R}_{k,i}), \; 1 \leq i \leq n$$

  - Modified measurements and keys

$$\underline{y}'_{k,i}, \; \mathsf{sk}_i \qquad 1 \leq i \leq n$$

Example: Linear Constant Velocity Model ($n = 3$)



Sequential Assumption

- Estimators can access q measurements $(1 \leq q \leq n)$
- Estimators have privilege p (the number of keys they hold) $(0 \leq p \leq n)$

$$\mathsf{e}^{[\text{privilege, access}]}$$

Sequential Assumption

- Estimators can access q measurements $(1 \leq q \leq n)$
- Estimators have privilege p (the number of keys they hold) $(0 \leq p \leq n)$

$$\mathsf{e}^{[\text{privilege, access}]}$$

- Estimators have access to sequential measurements
- Estimators have access to *all* measurements for which they hold a key

Sequential Assumption

- Estimators can access q measurements $(1 \leq q \leq n)$
- Estimators have privilege p (the number of keys they hold) $(0 \leq p \leq n)$

$$\mathsf{e}^{[\text{privilege, access}]}$$

- Estimators have access to sequential measurements
- Estimators have access to *all* measurements for which they hold a key

$\mathsf{e}^{[0,q]}$	Access to:	$\underline{y}'_{k,i}\,,\ 1 \leq i \leq q$
$\mathsf{e}^{[p,p]}$	Access to:	$\underline{y}'_{k,i}\,,\ \mathsf{sk}_i\,,\ 1 \leq i \leq p$
$\mathsf{e}^{[p,q]}$	Access to:	$\underline{y}'_{k,i}\,,\ 1 \leq i \leq q \qquad \mathsf{sk}_j\,,\ 1 \leq j \leq p$

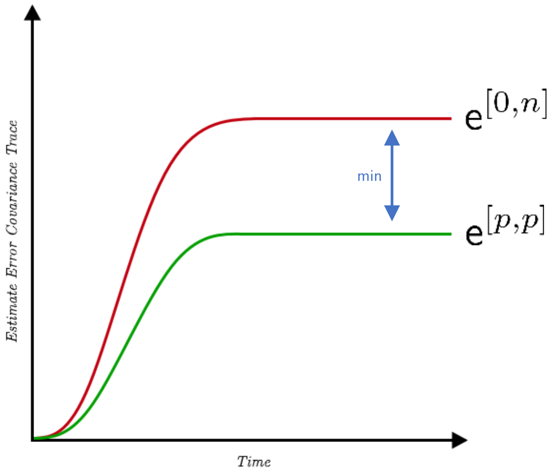
Bounds on Performance Loss and Gain

- Capture desired performance differences in multisensor environment

Bounds on Performance Loss and Gain

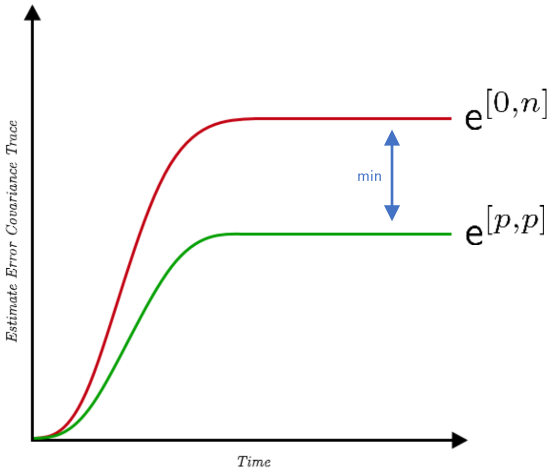
- Capture desired performance differences in multisensor environment

Performance Loss Lower Bound

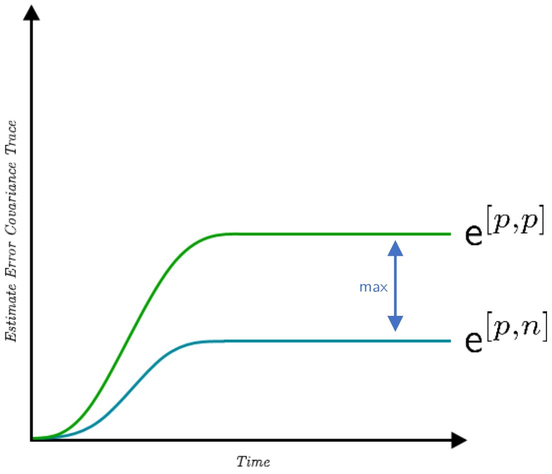


- Capture desired performance differences in multisensor environment

Performance Loss Lower Bound

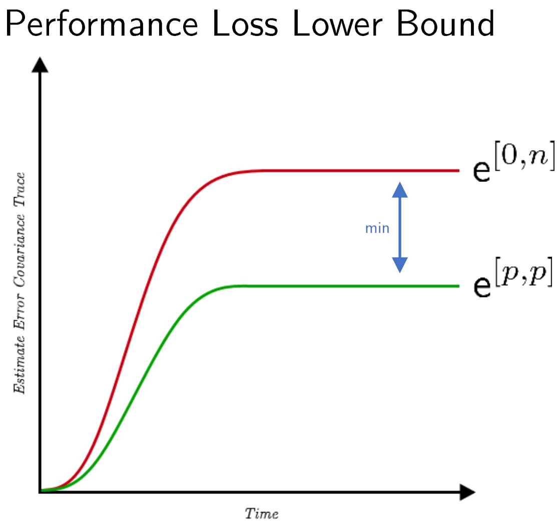


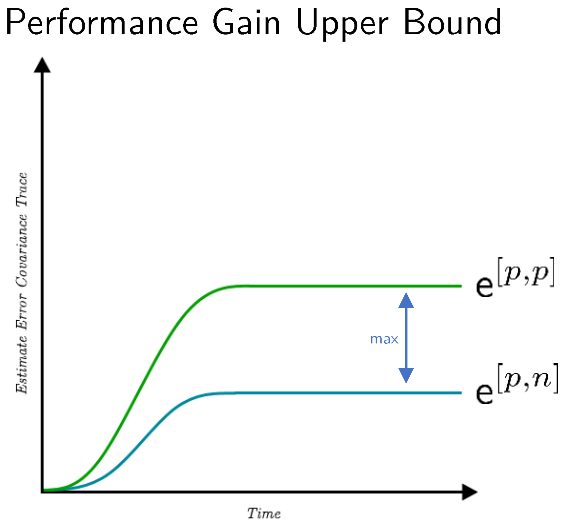
Performance Gain Upper Bound



Bounds on Performance Loss and Gain

- Capture desired performance differences in multisensor environment





- Both bounds desired for each privilege p

Correlated Noise Generation

- Generate uniform keystreams from sk_i for $1 \leq i \leq n$
- Correlated uniform keystreams with Box-Muller transform

$$\begin{bmatrix} \underline{g}_{k,1} \\ \vdots \\ \underline{g}_{k,n} \end{bmatrix} \sim \mathcal{N}\left(\underline{0}, \mathbf{S}^{(n)}\right) \qquad \mathbf{S}^{(n)} = \underbrace{\begin{bmatrix} \mathbf{Z} & \cdots & \mathbf{Z} \\ \vdots & \ddots & \vdots \\ \mathbf{Z} & \cdots & \mathbf{Z} \end{bmatrix}}_{\text{Correlated component}} + \underbrace{\begin{bmatrix} \mathbf{Y} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \ddots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{Y} \end{bmatrix}}_{\text{Uncorrelated component}}$$

Correlated Noise Generation

- Generate uniform keystreams from sk_i for $1 \leq i \leq n$
- Correlated uniform keystreams with Box-Muller transform

$$\begin{bmatrix} \underline{g}_{k,1} \\ \vdots \\ \underline{g}_{k,n} \end{bmatrix} \sim \mathcal{N}\left(\underline{0}, \mathbf{S}^{(n)}\right) \qquad \mathbf{S}^{(n)} = \underbrace{\begin{bmatrix} \mathbf{Z} & \cdots & \mathbf{Z} \\ \vdots & \ddots & \vdots \\ \mathbf{Z} & \cdots & \mathbf{Z} \end{bmatrix}}_{\text{Correlated component}} + \underbrace{\begin{bmatrix} \mathbf{Y} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \ddots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{Y} \end{bmatrix}}_{\text{Uncorrelated component}}$$

- Add generated keystreams to measurements

$$\underline{y}'_{k,i} = \underline{y}_{k,i} + \underline{g}_{k,i} = \mathbf{H}_{k,i}\underline{x}_k + \underline{v}_{k,i} + \underline{g}_{k,i} \qquad \underline{v}_k \sim \mathcal{N}(\underline{0}, \mathbf{R}_{k,i})$$

Correlated Noise Reconstruction

- Each added noise depends on multiple keys!
- Need to correctly reconstruct partial noises when $p < n$
- Lower-triangular decomposition (e.g. Cholesky) in Box-Muller transform ensures

$$\underline{g}_{k,i} \quad \text{depends on} \quad \mathsf{sk}_j \,, \; 1 \leq j \leq i$$

Correlated Noise Reconstruction

- Each added noise depends on multiple keys!
- Need to correctly reconstruct partial noises when $p < n$
- Lower-triangular decomposition (e.g. Cholesky) in Box-Muller transform ensures

$$\underline{g}_{k,i} \quad \text{depends on} \quad \mathsf{sk}_j\,,\ 1 \leq j \leq i$$

- Can reconstruct first p noises with $\mathsf{sk}_i\,,\ 1 \leq i \leq p$ exactly (recall sequential assumption)

$$\begin{bmatrix} \underline{g}_{k,1} \\ \vdots \\ \underline{g}_{k,p} \end{bmatrix} \sim \mathcal{N}\left(\underline{0}, \mathbf{S}^{(p)}\right) \qquad \mathbf{S}^{(p)} = \begin{bmatrix} \mathbf{Z} & \cdots & \mathbf{Z} \\ \vdots & \ddots & \vdots \\ \mathbf{Z} & \cdots & \mathbf{Z} \end{bmatrix} + \begin{bmatrix} \mathbf{Y} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \ddots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{Y} \end{bmatrix}$$

Observable Measurement Models

- Gaussian keystream indistinguishable from random without key
- Leads to three observable measurement models

Observable Measurement Models

Notation

$$\mathbf{R}_k^{(1:q)} = \begin{bmatrix} \mathbf{R}_{k,1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \mathbf{R}_{k,q} \end{bmatrix}$$

$$\bar{\mathbf{Z}} = \begin{bmatrix} \mathbf{Z} & \cdots & \mathbf{Z} \\ \vdots & \ddots & \vdots \\ \mathbf{Z} & \cdots & \mathbf{Z} \end{bmatrix}$$

- Gaussian keystream indistinguishable from random without key
- Leads to three observable measurement models

$$\mathsf{e}^{[0,q]} \qquad \underline{y}_k = \mathbf{H}_k^{(1:q)} \underline{x}_k + \underline{v}'_k \qquad \underline{v}'_k \sim \mathcal{N}\left(\underline{0}, \mathbf{R}_k^{(1:q)} + \mathbf{S}^{(q)}\right)$$

$$\mathsf{e}^{[p,p]} \qquad \underline{y}_k = \mathbf{H}_k^{(1:p)} \underline{x}_k + \underline{v}'_k \qquad \underline{v}'_k \sim \mathcal{N}\left(\underline{0}, \mathbf{R}_k^{(1:p)}\right)$$

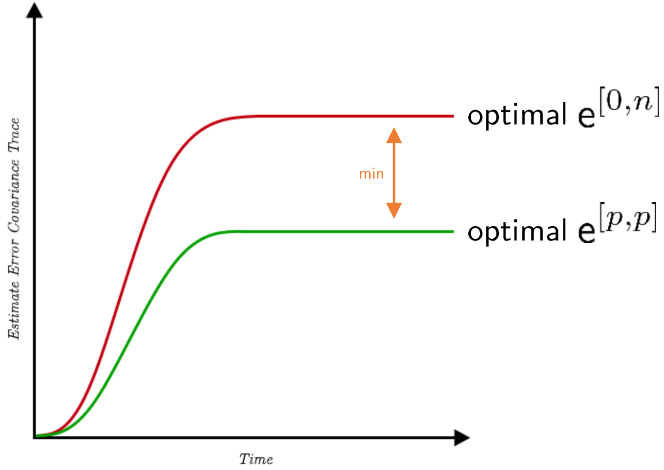
$$\mathsf{e}^{[p,q]} \qquad \underline{y}_k = \mathbf{H}_k^{(1:q)} \underline{x}_k + \underline{v}'_k \qquad \underline{v}'_k \sim \mathcal{N}\left(\underline{0}, \begin{bmatrix} \mathbf{R}_k^{(1:p)} & \mathbf{0} \\ \mathbf{0} & \mathbf{S}^{(q-p)} - \bar{\mathbf{Z}}\left(\mathbf{S}^{(p)}\right)^{-1} \bar{\mathbf{Z}} + \mathbf{R}_k^{(p+1:q)} \end{bmatrix}\right)$$

- Exact linear models mean optimal estimates

Proving Performance Loss and Gain Bounds

- Exact linear models mean optimal estimates

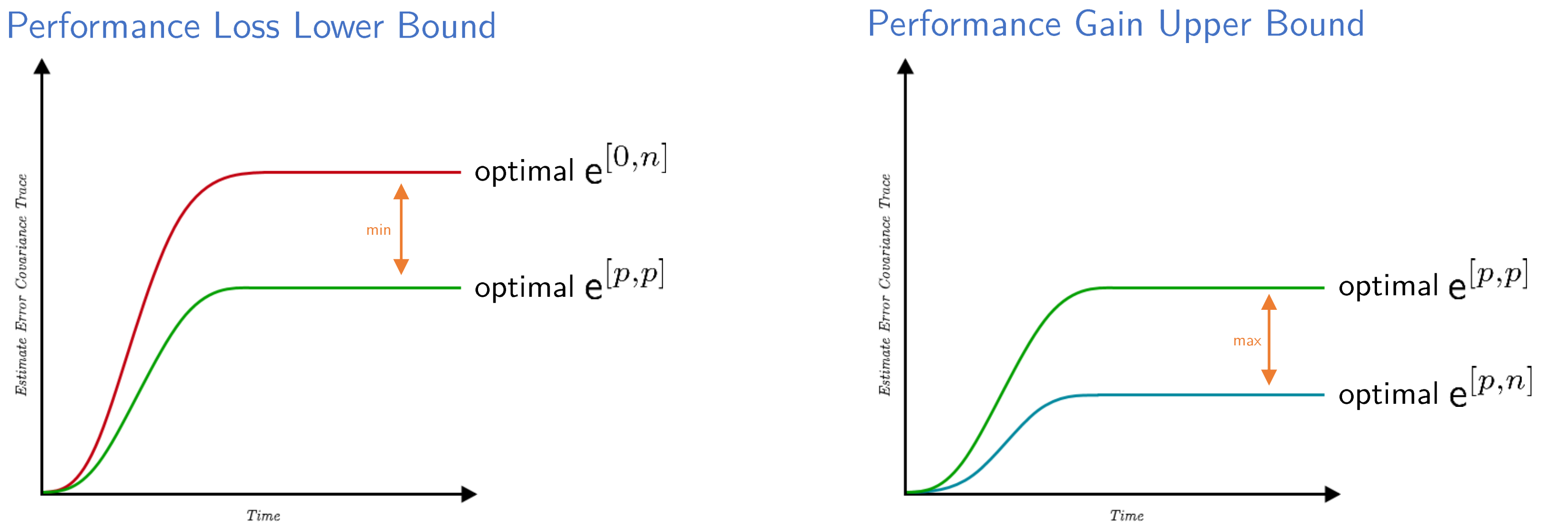
Performance Loss Lower Bound



$$\mathbf{P}_0 = \mathbf{0} \implies \text{Lowest possible } \operatorname{tr}\left(\mathbf{P}_k\right)$$

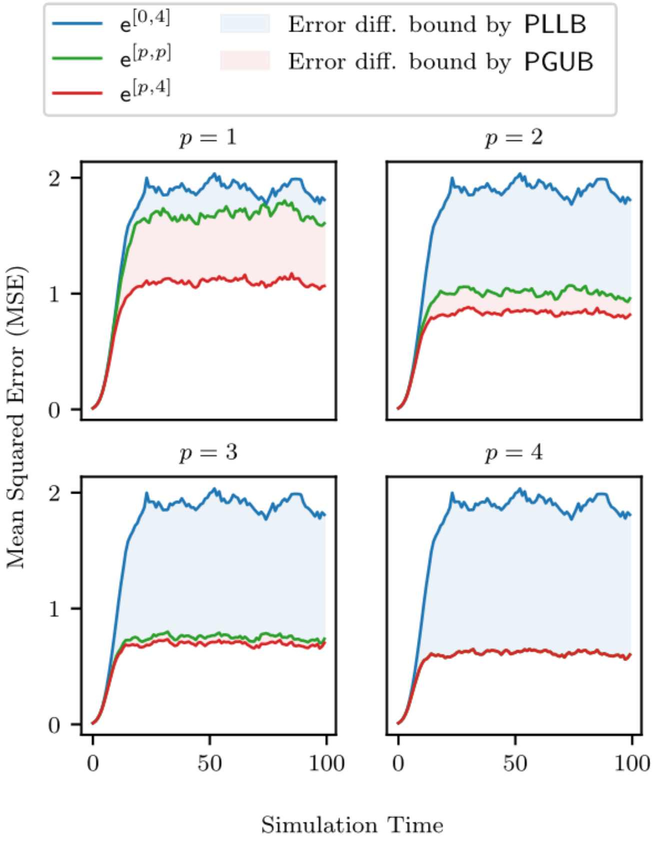
Proving Performance Loss and Gain Bounds

- Exact linear models mean optimal estimates



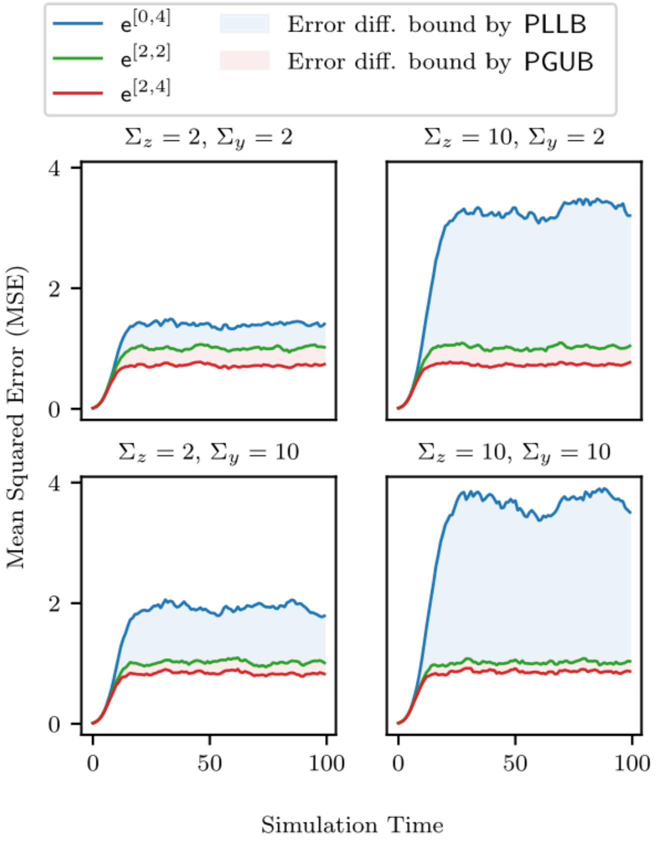
$\mathbf{P}_0 = \mathbf{0} \implies$ Lowest possible $\mathrm{tr}\left(\mathbf{P}_k\right)$

Simulation Results

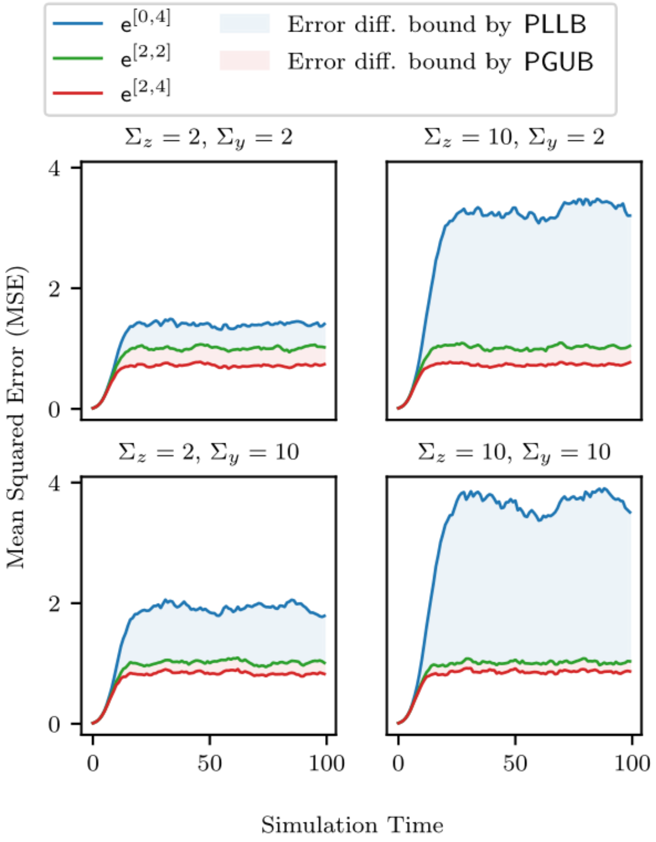


- $n = 4$
- Fixed fully correlated component $\mathbf{Z}$ and uncorrelated component $\mathbf{Y}$

Simulation Results



- $n = 4$
- Varied $\mathbf{Z} = \Sigma_z \times \mathbf{I}$ and $\mathbf{Y} = \Sigma_y \times \mathbf{I}$



- $n = 4$
- Varied $\mathbf{Z} = \Sigma_z \times \mathbf{I}$ and $\mathbf{Y} = \Sigma_y \times \mathbf{I}$

- Effect of $\mathbf{Z}$ and $\mathbf{Y}$ on bounds?

Future Work

- Search for correlation matrix parameters that affect bounds independently
- Relaxations of sequential assumption

Phone: +49 391 67 57591
Email: marko.ristic@ovgu.de
Web: https://ams.ovgu.de

Thank you!