Ph.D. Defense Presentation:

Privacy and Utility Preserving Sensing for Filtering Systems

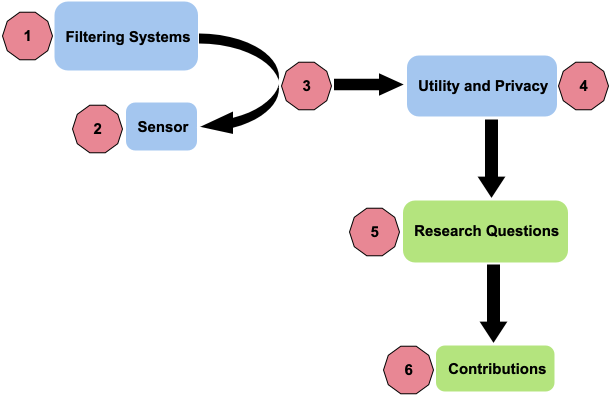
Niladri Das
Department of Aerospace Engineering

Adviser: Dr. Raktim Bhattacharya
Committee Members: Dr. S. R. Vadali, Dr. S. Chakravorty, & Dr. P. R. Kumar
Texas A&M University , College Station, TX, USA

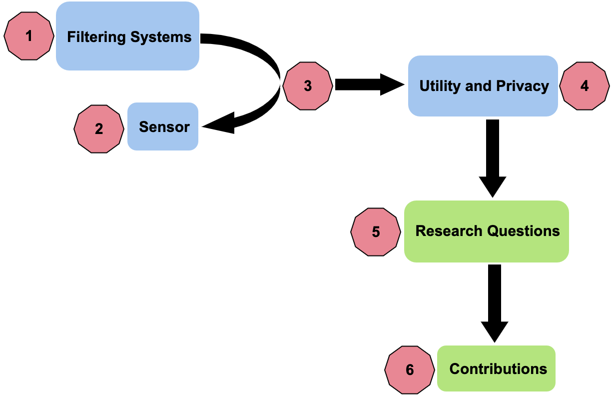
October 15, 2020

Outline

Privacy and Utility Preserving Sensing for **Filtering Systems**

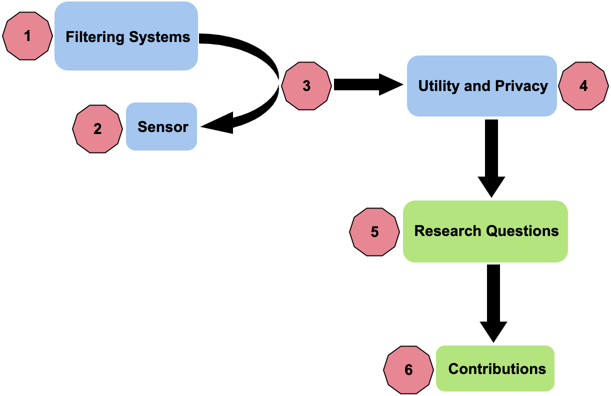


Privacy and Utility Preserving **Sensing** for Filtering Systems



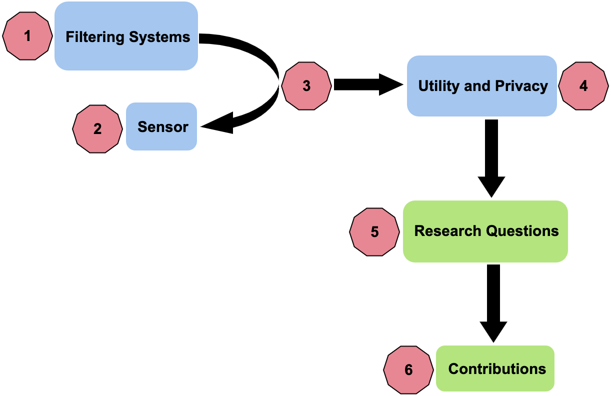
Outline

Privacy and Utility Preserving Sensing for Filtering Systems



Outline

Privacy and Utility Preserving Sensing for Filtering Systems



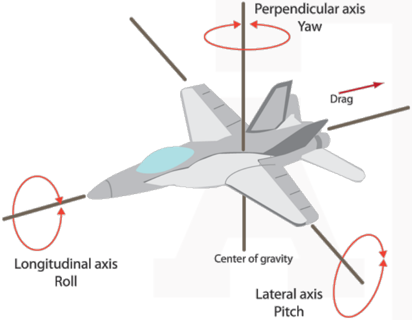


Figure 1: An Aircraft! : How can we estimate the velocity ?

Dynamics of Motion:

$$\boldsymbol{x}_{k+1} = \boldsymbol{f}(\boldsymbol{x}_k) + \boldsymbol{n}_k, \quad (1)$$

Measurement Equation:

$$\boldsymbol{y}_k = \boldsymbol{h}(\boldsymbol{x}_k) + \boldsymbol{v}_k, \quad (2)$$

$\boldsymbol{n}_k$: **Process noise**

$\boldsymbol{v}_k$: **Measurement noise**

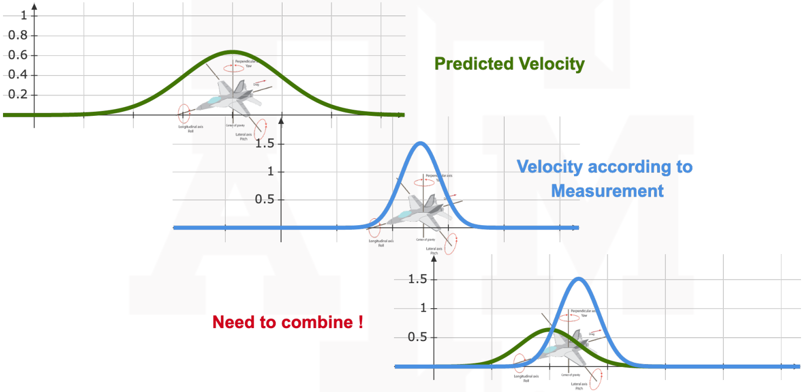


Figure 2: Estimate the Velocity !

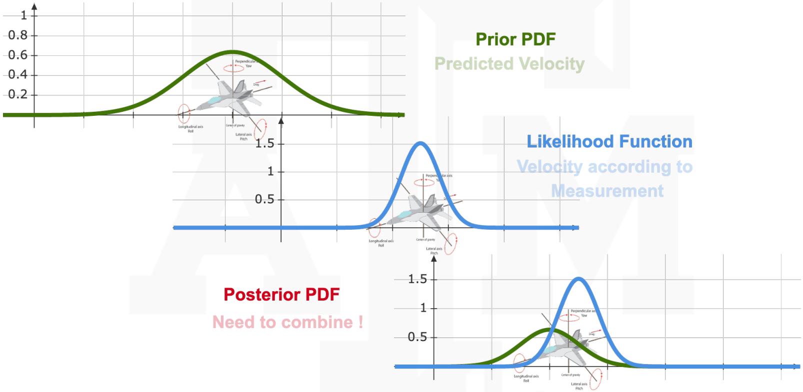
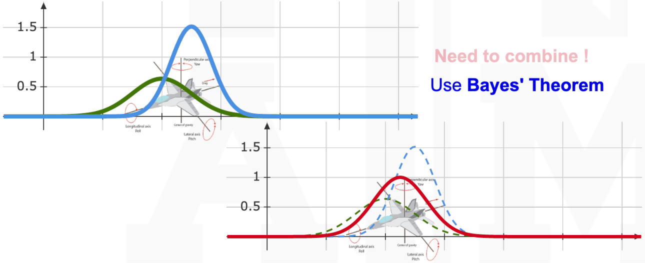


Figure 3: Estimate the Velocity !



Need to combine !

Use **Bayes' Theorem**

Posterior PDF

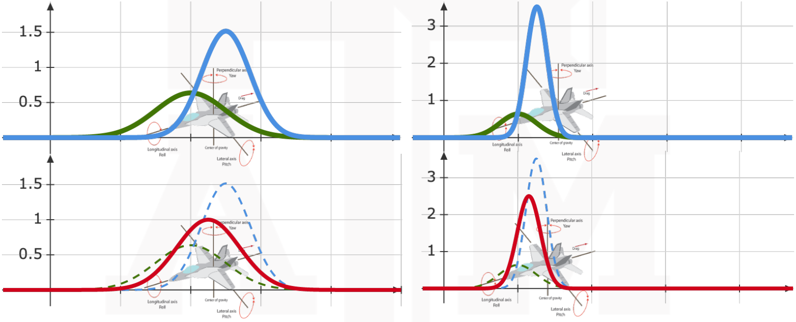
Figure 4: Calculating the Velocity !

Filters such as

- Kalman Filter
- Ensemble Kalman Filter
- Unscented Kalman Filter
- Particle Filter

approximates the process of combining prior PDF and likelihood function

Filtering and Sensing



More Sensor Noise

Less Sensor Noise

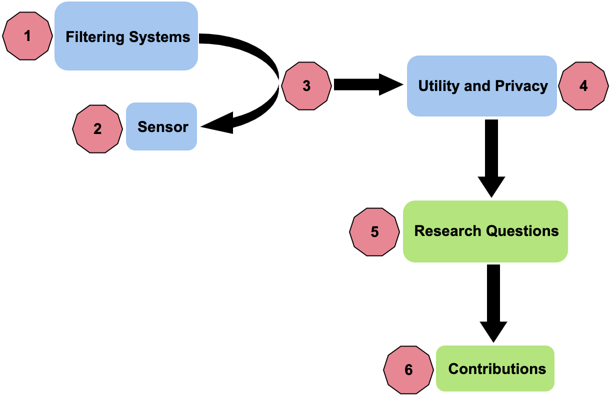
Figure 5: Estimate the Velocity !

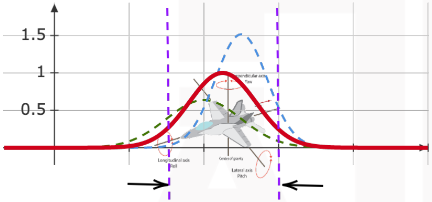
- Sensor/measurement noise ($\boldsymbol{v}_k$) is **zero mean independent Gaussian noise**

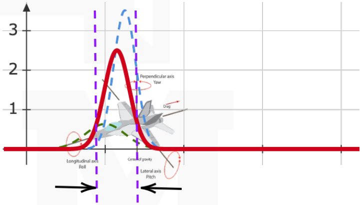
$$\boldsymbol{v}_k \sim \mathcal{N}(0, \boldsymbol{R}_k)$$

  $\boldsymbol{R}_k$ is the noise intensity or noise co-variance matrix
- Filter variables:
  - Prior PDF mean and co-variance : $\boldsymbol{\mu}_k^-, \boldsymbol{\Sigma}_k^-$
  - Posterior PDF mean and co-variance : $\boldsymbol{\mu}_k^+, \boldsymbol{\Sigma}_k^+$

Privacy and Utility Preserving Sensing for Filtering Systems



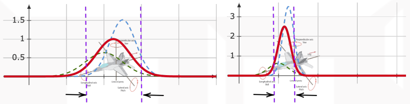




Less Accurate Predictions	**More** Accurate Predictions
More Sensor Noise	**Less** Sensor Noise
More Privacy	**More** Utility

Figure 6: Estimate the Velocity !

Utility and Privacy



Less Accurate Predictions

More Sensor Noise

More Privacy

More Accurate Predictions

Less Sensor Noise

More Utility

- Utility requirement is prescribed as an **upper bound** on posterior co-variance

$$\mathbf{\Sigma}_k^+ \leq \mathbf{\Sigma}^{ub}, \text{ or } \mathbf{tr}\left[\mathbf{\Sigma}_k^+\right] \leq \gamma_u$$

- Privacy requirement is prescribed as a **lower bound** on posterior co-variance

$$\mathbf{\Sigma}_k^+ \geq \mathbf{\Sigma}_{lb}, \text{ or } \mathbf{tr}\left[\mathbf{\Sigma}_k^+\right] \geq \gamma_u$$

Research Questions:

If we know $\boldsymbol{R}_k$ we can calculate $\boldsymbol{\Sigma}_k^+$ for a given filter — Forward problem

Main Question:
Can we solve the inverse problems

1. Calculate $\boldsymbol{R}_k$ such that $\boldsymbol{\Sigma}_k^+ \leq \boldsymbol{\Sigma}^{ub}$, or $\mathbf{tr}\left[\boldsymbol{\Sigma}_k^+\right] \leq \gamma_u$ (**Utility Problem**)
2. Calculate $\boldsymbol{R}_k$ such that $\boldsymbol{\Sigma}_k^+ \geq \boldsymbol{\Sigma}_{lb}$, or $\mathbf{tr}\left[\boldsymbol{\Sigma}_k^+\right] \geq \gamma_u$ (**Privacy Problem**)

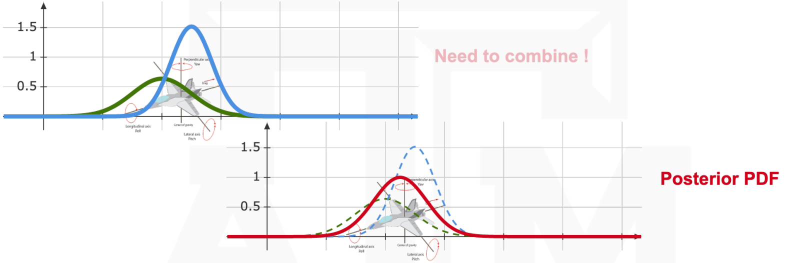


Figure 7: Posterior PDF depends upon which filter we use

Results on how to solve the **Utility Problem** and **Privacy Problem** for specific filters

1. **Kalman Filter**
2. **Ensemble Kalman Filter** and **Unscented Kalman Filter**

Large-scale spatio-temporal problems including

- For space situational awareness where space objects are tracked using ground/space based sensor networks
  - What $\boldsymbol{R}_k$ is allowed satisfying **utility** while sensing ?
  - How much additional noise with noise intensity $\boldsymbol{R}_k$, can be added to the measurements to satisfy **privacy** requirement ?
- Health monitoring,
- Power-system monitoring.

Without analytical approach

- Conservatively noise is added to measurement data to increase **privacy**
  - The US military adds synthetic noise to the public domain SSA data, which impacts how accurately the space objects can be tracked.
- Choose the best sensors satisfying a budget constraint to increase **utility**.

How can we calculate the noise for privacy and the sensor precision for utility ?

1. **Kalman Filter** (KF)
2. **Ensemble Kalman Filter** (EnKF) & **Unscented Kalman Filter** (UKF)

How to solve the utility problem for Kalman Filter?

What do we need

- Kalman Filter equations — equation connecting $\boldsymbol{R}_k$ and $\boldsymbol{\Sigma}_k^+$
- Prescribed utility $\boldsymbol{\Sigma}_k^+ \leq \boldsymbol{\Sigma}^{ub}$, or $\mathbf{tr}\left[\boldsymbol{\Sigma}_k^+\right] \leq \gamma_u$

Calculate $\boldsymbol{R}_k$ that satisfies utility and optimize over the feasible set of $\boldsymbol{R}_k$

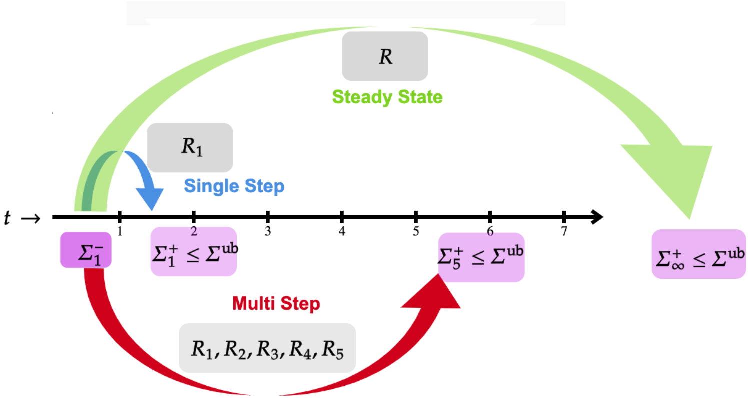


Figure 8: Three scenarios for calculating $\boldsymbol{R}$; single step is special case of multi step; multi step allows us to model multi-rate sensing, with m being the least-common-multiple of the various sensing intervals.

System Model:

$$\boldsymbol{x}_{k+1} = \boldsymbol{A}_k \boldsymbol{x}_k + \boldsymbol{B}_k \boldsymbol{w}_k,$$
$$\boldsymbol{y}_k = \boldsymbol{C}_k \boldsymbol{x}_k + \boldsymbol{n}_k,$$

Augmented System Model:

$$\boldsymbol{X}_k = \boldsymbol{\mathcal{A}}_k \boldsymbol{x}_{km} + \boldsymbol{\mathcal{B}}_k \boldsymbol{W}_k,$$
$$\boldsymbol{Y}_k = \boldsymbol{\mathcal{C}}_k \boldsymbol{X}_k + \boldsymbol{N}_k,$$

where,

- $\boldsymbol{X}_k := [\boldsymbol{x}_{km+1}^T, ..., \boldsymbol{x}_{(k+1)m^T}]^T, \boldsymbol{Y}_k := [\boldsymbol{y}_{km+1}^T, ..., \boldsymbol{y}_{(k+1)m}^T]^T$
- $\mathbb{E}\left[(\boldsymbol{X}_k - \bar{\boldsymbol{X}}_k)(\boldsymbol{X}_k - \bar{\boldsymbol{X}}_k)^T\right] := \boldsymbol{P}_k \rightarrow \boxed{\boldsymbol{P}_k^- \text{ and } \boldsymbol{P}_k^+}$
- $\boldsymbol{\mathcal{R}}_k := \mathbf{diag}\left(\boldsymbol{R}_{km}, \cdots, \boldsymbol{R}_{km+m-1}\right)$

Optimize over the feasible set of $\boldsymbol{\mathcal{R}}_k$ that satisfies
$$\boldsymbol{\Sigma}_{(k+1)m}^+ \leq \boldsymbol{\Sigma}^{ub}$$

Utility Problem:

$$\text{Optimize } c_1(\boldsymbol{R}_k) \text{ such that } \boldsymbol{\Sigma}^{+}_{(k+1)m} \leq \boldsymbol{\Sigma}^{ub}$$

- Choice of objective function $c_1(.)$ is influenced by the constraints on the communication bandwidth and sensor battery life,
- Precision of a sensor $(\boldsymbol{R}_k^{-1})$ is explicitly related to its cost, thus having economical implications — weighted l_1 norm.

Kalman Filter equations

$$\begin{aligned}
\boldsymbol{K}_k &= \boldsymbol{\Sigma}_k^- \boldsymbol{C}_k^T \left[\boldsymbol{C}_k \boldsymbol{\Sigma}_k^- \boldsymbol{C}_k^T + \boldsymbol{R}_k \right]^{-1}, && \text{(Kalman Gain)} \\
\boldsymbol{\mu}_k^- &= \boldsymbol{A}_k \boldsymbol{\mu}_{k-1}^+, && \text{(Mean Propagation)} \\
\boldsymbol{\Sigma}_k^- &= \boldsymbol{A}_k \boldsymbol{\Sigma}_{k-1}^+ \boldsymbol{A}_k^T + \boldsymbol{B}_k \boldsymbol{Q}_k \boldsymbol{B}_k^T, && \text{(Variance Propagation)} \\
\boldsymbol{\mu}_k^+ &= \boldsymbol{\mu}_k^- + \boldsymbol{K}_k (\boldsymbol{y}_k - \boldsymbol{C}_k \boldsymbol{\mu}_k^-), && \text{(Mean Update)} \\
\boldsymbol{\Sigma}_k^+ &= (\boldsymbol{I}_{n_x} - \boldsymbol{K}_k \boldsymbol{C}_k) \boldsymbol{\Sigma}_k^-, && \text{(Variance Update)}
\end{aligned}$$

Equation connecting $\boldsymbol{R}_k$ and $\boldsymbol{\Sigma}_k^+$:

$$\boxed{\boldsymbol{\Sigma}_k^+ = (\boldsymbol{I}_{n_x} - \boldsymbol{K}_k \boldsymbol{C}_k) \boldsymbol{\Sigma}_k^-}$$

Assuming $\boldsymbol{R}_k$ to be diagonal, i.e. $\boldsymbol{R}_k := \mathbf{diag}\left(\boldsymbol{r}_k\right)$, where $\boldsymbol{r}_k := \begin{bmatrix} r_1 & r_2 & \cdots & r_{n_{y_k}} \end{bmatrix}^T$, with $r_i > 0$

- It is convenient to formulate the problem in terms of sensor precisions, defined by $\boldsymbol{S}_k := \boldsymbol{R}_k^{-1}$, resulting in $s_i := 1/r_i$.

Utility Problem:

Minimize $\mathbf{tr}\left[\boldsymbol{S}_k\right]$ such that $\boldsymbol{\Sigma}^+_{(k+1)m} \leq \boldsymbol{\Sigma}^{ub}$

- **Multi-step Utility Theorem** (Theorem 1)
  - Outline of the proof.
  - How to promote sparsity?
- **Steady State Utility Theorem** (Theorem 2)
  - Outline of the proof.
  - How to improve the solution?
- **Numerical Example** : Satellite Tracking Problem

TEXAS A&M UNIVERSITY

Multi-step Utility Theorem

Theorem 1

Optimal sensor precision $\boldsymbol{s}_k \in \mathbb{R}^{n_{y_{k,m}}} \geq 0$, *which satisfies* $\boldsymbol{\Sigma}^+_{(k+1)m} \leq \boldsymbol{\Sigma}^d$, *is given by the solution of the following optimization problem,*

$$\left.\begin{array}{l} \min\limits_{\boldsymbol{s}_k} \mathbf{tr}\left[\boldsymbol{W}\boldsymbol{\mathcal{S}}_k\right], \ \textit{subject to} \\ \begin{bmatrix} \boldsymbol{M}_{11} & \boldsymbol{M}_m\boldsymbol{P}_k^- \\ (*)^T & \boldsymbol{L} + \boldsymbol{L}\boldsymbol{\mathcal{S}}_k\boldsymbol{L} \end{bmatrix} \geq 0, \\ 0 \leq \boldsymbol{s}_k \leq \boldsymbol{s}_k^{max}, \end{array}\right\} \tag{3}$$

where $(*)^T$ *represents symmetric terms, and*

$$\boldsymbol{\mathcal{S}}_k := \mathbf{diag}\left(\boldsymbol{s}_k\right), \ \boldsymbol{L} := \boldsymbol{\mathcal{C}}_k\boldsymbol{P}_k^-\boldsymbol{\mathcal{C}}_k^T, \ \boldsymbol{x}_{(k+1)m} := \boxed{\boldsymbol{M}_m}\boldsymbol{X}_k,$$

$$\boldsymbol{M}_{11} := \boldsymbol{\Sigma}^d - \boldsymbol{M}_m\boldsymbol{P}_k^-\boldsymbol{M}_m^T + \boldsymbol{M}_m\boldsymbol{P}_k^-\boldsymbol{L}^{-1}\boldsymbol{P}_k^-\boldsymbol{M}_m^T,$$

The variable $\boldsymbol{W}$ *is a diagonal matrix, which is user defined and serves as a normalizing weight on* $\boldsymbol{\mathcal{S}}_k$.

Outine of the Proof :

- Inequality $\Sigma^{+}_{(k+1)m} \leq \Sigma^{d}$ is written as a function of P^{-}_{k} using Variance Update equation, where $\boxed{\Sigma^{-}_{km} := M_m P^{-}_{k} M^{T}_{m}}$.
- Use Matrix Inversion Lemma, followed by Schur complement —

$$\begin{bmatrix} M_{11} & M_m P^{-}_{k} \\ (*)^T & L + L\mathcal{S}_k L \end{bmatrix} \geq 0. \tag{4}$$

- Optimal precision can be determined by minimizing the cost function $\mathbf{tr}\left[W\mathcal{S}_k\right]$.
- Practical considerations may upper-bound maximum precision, which is incorporated in the formulation using the constraint

$$s_k \leq s^{\text{max}}_{k}. \tag{5}$$

Inequalities (4), (5), along with minimization of $\mathbf{tr}\left[W\mathcal{S}_k\right]$, result in the optimization problem in (3).

If utility is given as a bound on the trace:

With the relaxation $\mathbf{tr}\left[\boldsymbol{\Sigma}^{+}_{(k+1)m}\right] \leq \gamma_d$, the optimization problem in (3) modifies to

$$\left.\begin{aligned} &\min_{\boldsymbol{s}_k, \boldsymbol{F}} \mathbf{tr}\left[\boldsymbol{W}\boldsymbol{\mathcal{S}}_k\right], \text{ subject to} \\ &\begin{bmatrix} \boldsymbol{M}_{11} & \boldsymbol{M}_m \boldsymbol{P}_k^- \\ (*)^T & \boldsymbol{L} + \boldsymbol{L}\boldsymbol{\mathcal{S}}_k \boldsymbol{L} \end{bmatrix} \geq 0, \\ &0 \leq \boldsymbol{s}_k \leq \boldsymbol{s}_k^{\text{max}},\ \boldsymbol{F} \geq 0,\ \mathbf{tr}\left[\boldsymbol{F}\right] \leq \gamma_d, \end{aligned}\right\} \tag{6}$$

where

$$\boldsymbol{\mathcal{S}}_k := \mathbf{diag}\left(\boldsymbol{s}_k\right),\ \boldsymbol{L} := \boldsymbol{\mathcal{C}}_k \boldsymbol{P}_k^- \boldsymbol{\mathcal{C}}_k^T,$$
$$\boldsymbol{M}_{11} := \boldsymbol{F} - \boldsymbol{M}_m \boldsymbol{P}_k^- \boldsymbol{M}_m^T + \boldsymbol{M}_m \boldsymbol{P}_k^- \boldsymbol{L}^{-1} \boldsymbol{P}_k^- \boldsymbol{M}_m^T,$$

and $\boldsymbol{W}$ is the normalizing weight on $\boldsymbol{\mathcal{S}}_k$, as in theorem 1. In (6), a new variable $\boldsymbol{F} \in \mathbb{S}_+^{n_x}$ is introduced to impose the trace bound, where $\mathbb{S}_+^{n_x}$ — space of symmetric positive definite matrices of dimension $n_x \times n_x$.

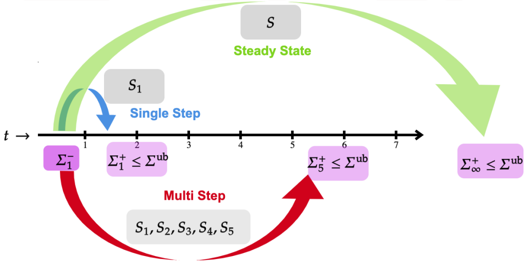
Improving Sparseness:

In Theorem 1 the sparseness of the solution can be improved by iteratively solving the optimization problem (3) with weights

$$\boldsymbol{W}_{j+1} := (\boldsymbol{\mathcal{S}}_k^* + \epsilon \boldsymbol{I})_j^{-1}, \tag{7}$$

with $\boldsymbol{W}_1 := \boldsymbol{I}_{n_{y_{k,m}}}$, where subscript j denotes the iteration index

m-Periodic Systems:



Instead of $\Sigma^+_{(k+1)m} \leq \Sigma^d$ we talk about $\boxed{\Sigma_\infty \leq \Sigma^{ub}}$ $\leftarrow$ Steady State

Example: If the period of the system is 5, calculate $\boldsymbol{\mathcal{S}}_1, \boldsymbol{\mathcal{S}}_2, \boldsymbol{\mathcal{S}}_3, \boldsymbol{\mathcal{S}}_4, \boldsymbol{\mathcal{S}}_5$ so that $\Sigma_\infty \leq \Sigma^{ub}$

TEXAS A&M UNIVERSITY

Steady State Utility Theorem

Theorem 2

Optimal sensor precision $\boldsymbol{s}_m \in \mathbb{R}^{n_{y_{k,m}}} \geq 0$, *which satisfies* $\mathbf{tr}\left[\boldsymbol{M}_x \boldsymbol{P}^d_\infty \boldsymbol{M}_x^T\right] \leq \gamma_d$ *is given by the solution of the following optimization problem,*

$$\min_{\boldsymbol{s}_m, \boldsymbol{Z}, \boldsymbol{P}^d_\infty, \boldsymbol{\mathcal{K}}_\infty} \quad \mathbf{tr}\left[\boldsymbol{W}\boldsymbol{\mathcal{S}}_m\right] \textit{ subject to} \tag{8a}$$

$$\begin{bmatrix} \boldsymbol{M}_{11} & \boldsymbol{M}_x \boldsymbol{\mathcal{A}}_m (\boldsymbol{I}_{N_x} - \boldsymbol{\mathcal{K}}_\infty \boldsymbol{\mathcal{C}}_m) & \boldsymbol{M}_x \boldsymbol{\mathcal{A}}_m \boldsymbol{\mathcal{K}}_\infty \\ (*)^T & \boldsymbol{Z} & \mathbf{0}_{N_x \times n_{y_{k,m}}} \\ (*)^T & (*)^T & \boldsymbol{\mathcal{S}}_m \end{bmatrix} \geq 0, \tag{8b}$$

$$\begin{bmatrix} \boldsymbol{I}_{N_x} & \boldsymbol{P}^d_\infty & \boldsymbol{Z} \\ \boldsymbol{P}^d_\infty & \frac{1}{\delta}\boldsymbol{I}_{N_x} & \mathbf{0}_{N_x \times N_x} \\ \boldsymbol{Z} & \mathbf{0}_{N_x \times N_x} & \delta \boldsymbol{I}_{N_x} \end{bmatrix} \geq 0, , \tag{8c}$$

$$0 \leq \boldsymbol{s}_m \leq \boldsymbol{s}_{max}, \ \mathbf{tr}\left[\boldsymbol{M}_x \boldsymbol{P}^d_\infty \boldsymbol{M}_x^T\right] \leq \gamma_d, \tag{8d}$$

$$\boldsymbol{M}_{11} := \boldsymbol{M}_x \left(\boldsymbol{P}^d_\infty - \boldsymbol{\mathcal{B}}_m \boldsymbol{\mathcal{Q}}_m \boldsymbol{\mathcal{B}}_m^T\right) \boldsymbol{M}_x^T, \ \boldsymbol{\mathcal{S}}_m := \mathbf{diag}\left(\boldsymbol{s}_m\right).$$

Outine of the Proof :

- Use DARE and guarantee monotonicity
- Introduce $\boldsymbol{Z}^{-1} \geq \boldsymbol{P}^d_\infty$ and rewrite the monotonicity condition in $\boldsymbol{Z}$
- Take the Schur complement and substitute $\boldsymbol{\mathcal{S}}_m := \boldsymbol{\mathcal{R}}_m^{-1}$ to get (8b).

$$\begin{bmatrix} \boldsymbol{M}_{11} & \boldsymbol{M}_x \boldsymbol{\mathcal{A}}_m (\boldsymbol{I}_{N_x} - \boldsymbol{\mathcal{K}}_\infty \boldsymbol{\mathcal{C}}_m) & \boldsymbol{M}_x \boldsymbol{\mathcal{A}}_m \boldsymbol{\mathcal{K}}_\infty \\ (*)^T & \boldsymbol{Z} & \boldsymbol{0}_{N_x \times n_{y_{k,m}}} \\ (*)^T & (*)^T & \boldsymbol{\mathcal{S}}_m \end{bmatrix} \geq 0$$

- Using Young's Relation on the non-convex relaxation $\boldsymbol{Z}^{-1} \geq \boldsymbol{P}^d_\infty$ to get (8c)

$$\begin{bmatrix} \boldsymbol{I}_{N_x} & \boldsymbol{P}^d_\infty & \boldsymbol{Z} \\ \boldsymbol{P}^d_\infty & \frac{1}{\delta}\boldsymbol{I}_{N_x} & \boldsymbol{0}_{N_x \times N_x} \\ \boldsymbol{Z} & \boldsymbol{0}_{N_x \times N_x} & \delta \boldsymbol{I}_{N_x} \end{bmatrix} \geq 0,$$

- The optimal precision is given by minimizing $\mathbf{tr}\left[\boldsymbol{W}\boldsymbol{\mathcal{S}}_m\right]$.

Improving Conservative Solution of Theorem 2 :

The optimal $\boldsymbol{\mathcal{S}}_m$ ($\boldsymbol{\mathcal{S}}_m^*$) can be conservative

$$\mathbf{tr}\left[\boldsymbol{M}_x \boldsymbol{P}_\infty^* \boldsymbol{M}_x^T\right] << \gamma_d.$$

What can we do about it:

Use a bisection algorithm to iteratively scale up the noise

$$\boldsymbol{\mathcal{R}}_m \to \xi \boldsymbol{\mathcal{R}}_m.$$

Satellite Tracking Problem

$$\ddot{r} = -\frac{\mu_E}{r^2} + \dot{\theta}^2 r + \frac{3J_2}{2r^4}\left(3\sin(\theta)^2 - 1\right), \tag{9a}$$

$$\ddot{\theta} = -\frac{2\dot{\theta}\dot{r}}{r} - \frac{3J_2}{r^4}\cos(\theta)\sin(\theta). \tag{9b}$$

Length and time in the dynamics are normalized.

- The system is linearized about a nominal trajectory — normalized time interval of $[0, 1]$ is discretized with $dt = 0.1$ resulting in a temporal grid of 10 laser sensors around the orbit.
- We use modified Theorem 1 with $\gamma_d = 0.1 \times \mathbf{tr}\left[\mathbf{\Sigma}^-(t_k = 1)\right]$ as the utility requirement.

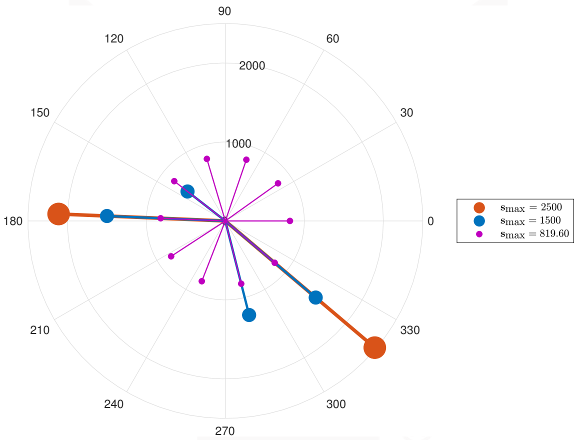
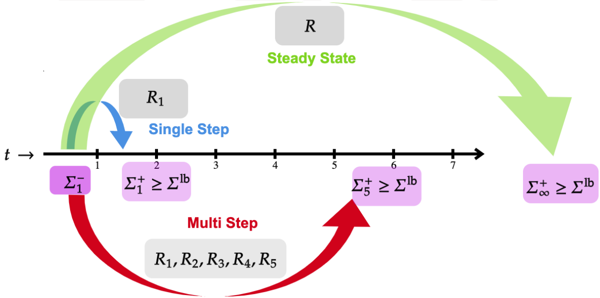


Figure 9: Optimal precisions for $s_{\text{max}} = 2500, 1500, 819.60$.

We solved the **utility problem** for the Kalman Filter

Next: We solve the **privacy problem** for the Kalman Filter

Privacy Problem :



- We present an Eigen-value analysis based result to solve the steady state problem $\to$ Optimize $c_2(\boldsymbol{R}_k)$ such that $\boldsymbol{\Sigma}_{lb} \preceq \boldsymbol{\Sigma}_\infty$.

Steady State Privacy Theorem:

Theorem 3

For a given scalar cost function c($\boldsymbol{R}$) and an lower bound $(1/\lambda_u^f)$ on the spectrum of $\boldsymbol{R}$ ($\lambda(\boldsymbol{R}^*) := \{\lambda_1 \geq \cdots \geq \lambda_{ny}\}$, where $\lambda_{ny} \geq (1/\lambda_u^f)$,), the solution $\boldsymbol{R}^*$,that satisfies a given lower bound $\boldsymbol{P}_l^f$ on the steady state prior covariance matrix $\boldsymbol{P}^{(p)} := \boldsymbol{M}^{(p)}\boldsymbol{P}{\boldsymbol{M}^{(p)}}^T$ of Kalman filter, is given by the following optimization problem.

$$\left.\begin{array}{l} \underset{\boldsymbol{R}}{\operatorname{argmin}}\; c(\boldsymbol{R}), \;\; \textit{subject to} \\ \boldsymbol{R} \succeq \dfrac{1}{\lambda_u^f}\boldsymbol{I}, \quad \begin{bmatrix} \boldsymbol{T}_1 & \boldsymbol{T}_2 \\ \boldsymbol{T}_2^T & \boldsymbol{T}_4 \end{bmatrix} \succeq 0, \end{array}\right\} \tag{10}$$

where,

$$
\begin{aligned}
\boldsymbol{T}_1 &= \boldsymbol{M}^{(p)}\boldsymbol{A}\boldsymbol{P}'_{l0}\boldsymbol{A}^T{\boldsymbol{M}^{(p)}}^T - \boldsymbol{P}_l^f + \boldsymbol{M}^{(p)}\boldsymbol{Q}{\boldsymbol{M}^{(p)}}^T \\
\boldsymbol{T}_2 &= \boldsymbol{M}^{(p)}\boldsymbol{A}\boldsymbol{P}'_{l0}\boldsymbol{C}^T, \boldsymbol{T}_4 = \boldsymbol{R} + \boldsymbol{C}\boldsymbol{P}'_{l0}\boldsymbol{C}^T \\
\boldsymbol{P}'_{l0} &\equiv \boldsymbol{A}(\varphi'^{-1}\boldsymbol{I} + \lambda_u^f\boldsymbol{C}^T\boldsymbol{C})^{-1}\boldsymbol{A}^T + \boldsymbol{Q}. \\
\varphi' &\equiv f(-[\lambda_{min}(\boldsymbol{A}\boldsymbol{A}^T - \boldsymbol{I}) + \lambda_{min}(\boldsymbol{Q})\lambda_u^f\lambda_{max}(\boldsymbol{C}^T\boldsymbol{C})] \\
&\quad , 2\lambda_u^f\lambda_{max}(\boldsymbol{C}^T\boldsymbol{C}), 2\lambda_{min}(\boldsymbol{Q})), \\
f(a,b,c) &\equiv \frac{-a + \sqrt{a^2 + bc}}{b}
\end{aligned}
$$

- The concept of private states and utility states are introduced will also be used in the UKF and EnKF optimal sensing problem.

Outline of the Proof:

- Use Theorem 1 & 2 from [1].
- Re-derive the theorems for $\boldsymbol{R}$ in place of $\boldsymbol{I}$ in the Unified Algebraic Riccati Equation.
- Apply approximation based on minimum and maximum eigen-value of a matrix.
- Extract the private states using masking matrix $\boldsymbol{M}^{(p)}$
- Use Matrix Inversion Lemma
- Apply Schur Complement to construct the LMI

[1] Chien-Hua Lee. Matrix bounds of the solutions of the continuous and discrete riccati equations–a unified approach. International Journal of Control, 76(6):635–642, 2003

We solved the **utility and privacy problem** for the **Kalman Filter**

Next:

We solve the **utility and privacy problem** for the **UKF and EnKF**

Motivation:

Data sharing for Space situational awareness (SSA)

- low-accuracy SSA data increases risk of collision but reduces risk from counter-space operations and protects details of operations, i.e. it improves privacy but degrades utility.
- high-accuracy SSA data improves utility but degrades privacy/security.

Current Scenario:

- The US military adds synthetic noise to the public domain SSA data conservatively for privacy or national-security, which impacts how accurately the space objects can be tracked.
- This conservative approach will not work and will impede accurate space traffic management, for mega-constellations in low earth orbits

Questions:

- What should be the accuracy in the SSA data that satisfies given utility and privacy objectives?
- Space object state estimation being non-linear problem motivated us to develop the privacy/utility preserving algorithms in the EnKF and UKF framework.

The variance update equation for EnKF and UKF are identical, which is

$$\boldsymbol{\Sigma}^{+}_{\boldsymbol{xx},k+1} = \boldsymbol{\Sigma}^{-}_{\boldsymbol{xx},k+1} - \boldsymbol{\Sigma}^{-}_{\boldsymbol{xy},k+1} \left(\boldsymbol{\Sigma}^{-}_{\boldsymbol{yy},k+1} + \boldsymbol{\mathcal{R}}_{k+1}\right)^{-1} \boldsymbol{\Sigma}^{-T}_{\boldsymbol{xy},k+1}.$$

- This allows us to formulate a common data privacy-utility policy for both the filtering frameworks.

- **Partitioning** : Privacy , Utility variables, & $\boldsymbol{\mathcal{R}}_{k+1}$.
- Utility constraints — **Theorem 4** — Calculate maximum noise
- Privacy constraints — **Theorem 5** : Calculate minimum noise
- **Privacy-Utility trade-off**
- **Numerical example** : International Space Station Tracking

TEXAS A&M UNIVERSITY

Partitioning Privacy and Utility Variables:

- We can achieve privacy-utility tradeoffs in space and time.

$$\boldsymbol{\Sigma}^{+}_{\boldsymbol{x}_u\boldsymbol{x}_u,k+1} := \boldsymbol{M}_u \boldsymbol{\Sigma}^{+}_{\boldsymbol{x}\boldsymbol{x},k+1} \boldsymbol{M}_u^T, \quad (11a)$$

$$\boldsymbol{\Sigma}^{+}_{\boldsymbol{x}_p\boldsymbol{x}_p,k+1} := \boldsymbol{M}_p \boldsymbol{\Sigma}^{+}_{\boldsymbol{x}\boldsymbol{x},k+1} \boldsymbol{M}_p^T, \quad (11b)$$

Partitioning $\mathcal{R}_{k+1}$:

$$\mathcal{R}_{k+1} := \mathcal{R}^{\text{sensor}}_{k+1} + \mathcal{R}^{\text{data}}_{k+1},$$

- $\mathcal{R}^{\text{sensor}}_{k+1}$ is the known sensor noise variance & $\mathcal{R}^{\text{data}}_{k+1}$ defines the additional synthetic noise.

Objectives:

Calculating $\mathcal{R}_{k+1}^{\text{data}}$:

$$\text{Privacy: } \mathbf{tr}\left[\boldsymbol{\Sigma}^{+}_{\boldsymbol{x}_p\boldsymbol{x}_p,k+1}\right] \geq \gamma_p, \tag{12a}$$

$$\text{Utility: } \mathbf{tr}\left[\boldsymbol{\Sigma}^{+}_{\boldsymbol{x}_u\boldsymbol{x}_u,k+1}\right] \leq \gamma_u, \tag{12b}$$

where γ_p and γ_u are user defined.

Maximum Noise Satisfying Utility Constraints

Theorem 4

The maximum noise that satisfies $\mathbf{tr}\left[\boldsymbol{\Sigma}^{+}_{\boldsymbol{x}_u\boldsymbol{x}_u,k+1}\right] \leq \gamma_u$, *is given by the solution of the following optimization problem*

$$\min_{\boldsymbol{\mathcal{S}}^{\mathsf{data}}_{k+1}\geq 0,\boldsymbol{Q}_u\geq 0} \mathbf{tr}\left[\boldsymbol{\mathcal{S}}^{\mathsf{data}}_{k+1}\right], \textit{ subject to} \tag{13a}$$

$$\begin{bmatrix} \boldsymbol{T}_1 & \boldsymbol{M}_u\boldsymbol{\Sigma}^{-}_{\boldsymbol{xy},k+1} \\ \boldsymbol{\Sigma}^{-T}_{\boldsymbol{xy},k+1}\boldsymbol{M}_u^T & \boldsymbol{Z}+\boldsymbol{Z}\boldsymbol{\mathcal{S}}^{\mathsf{data}}_{k+1}\boldsymbol{Z} \end{bmatrix} \geq 0, \; \mathbf{tr}\left[\boldsymbol{Q}_u\right] \leq \gamma_u, \tag{13b}$$

$$\boldsymbol{T}_1 := \boldsymbol{Q}_u - \boldsymbol{M}_u\boldsymbol{\Sigma}^{-}_{\boldsymbol{xx},k+1}\boldsymbol{M}_u^T + \boldsymbol{M}_u\boldsymbol{\Sigma}^{-}_{\boldsymbol{xy},k+1}\boxed{\boldsymbol{Z}^{-1}}\boldsymbol{\Sigma}^{-T}_{\boldsymbol{xy},k+1}\boldsymbol{M}_u^T$$

where $\boldsymbol{Z} := \boldsymbol{\Sigma}^{-}_{\boldsymbol{yy},k+1} + \boldsymbol{\mathcal{R}}^{\mathsf{sensor}}_{k+1}$. *The maximum noise in the data for which the utility constraint is satisfied is then given by* $\boldsymbol{\mathcal{R}}^{\mathsf{data}}_{k+1} := \left(\boldsymbol{\mathcal{S}}^{\mathsf{data}}_{k+1}\right)^{-1}$.

Minimum Noise Satisfying Privacy Constraints

Theorem 5

The minimum noise that satisfies $\mathbf{tr}\left[\boldsymbol{\Sigma}^{+}_{\boldsymbol{x}_p\boldsymbol{x}_p,k+1}\right] \geq \gamma_p$*, is given by the solution of the following optimization problem*

$$\min_{\boldsymbol{\mathcal{R}}^{\mathit{data}}_{k+1}\geq 0,\, \boldsymbol{Q}_p\geq 0} \mathbf{tr}\left[\boldsymbol{\mathcal{R}}^{\mathit{data}}_{k+1}\right], \tag{14a}$$

such that,

$$\begin{bmatrix} \boldsymbol{M}_p\boldsymbol{\Sigma}^{-}_{\boldsymbol{xx},k+1}\boldsymbol{M}_p^T - \boldsymbol{Q}_p & \boldsymbol{M}_p\boldsymbol{\Sigma}^{-}_{\boldsymbol{xy},k+1} \\ \boldsymbol{\Sigma}^{-T}_{\boldsymbol{xy},k+1}\boldsymbol{M}_p^T & \left(\boldsymbol{\Sigma}^{-}_{\boldsymbol{yy},k+1} + \boldsymbol{\mathcal{R}}^{\mathit{sensor}}_{k+1} + \boldsymbol{\mathcal{R}}^{\mathit{data}}_{k+1}\right) \end{bmatrix} \geq 0, \tag{14b}$$

$$\mathbf{tr}\left[\boldsymbol{Q}_p\right] \geq \gamma_p. \tag{14c}$$

Optimal Privacy-Utility Tradeoff

Utility-aware privacy:

$$\max\ \gamma_p,\ \text{subject to } \mathbf{tr}\left[\boldsymbol{\Sigma}^{+}_{\boldsymbol{x}_p\boldsymbol{x}_p,k+1}\right] \geq \gamma_p,\ \text{and } \mathbf{tr}\left[\boldsymbol{\Sigma}^{+}_{\boldsymbol{x}_u\boldsymbol{x}_u,k+1}\right] \leq \gamma_u.$$

Privacy-aware utility:

$$\min\ \gamma_u,\ \text{subject to } \mathbf{tr}\left[\boldsymbol{\Sigma}^{+}_{\boldsymbol{x}_p\boldsymbol{x}_p,k+1}\right] \geq \gamma_p,\ \text{and } \mathbf{tr}\left[\boldsymbol{\Sigma}^{+}_{\boldsymbol{x}_u\boldsymbol{x}_u,k+1}\right] \leq \gamma_u.$$

- Solved by introducing $\boldsymbol{\mathcal{S}}^{\text{data}}_{k+1}$ and $\boldsymbol{\mathcal{R}}^{\text{data}}_{k+1}$ as separate variables and linearizing the non-convex constraint $\boldsymbol{\mathcal{S}}^{\text{data}}_{k+1}\boldsymbol{\mathcal{R}}^{\text{data}}_{k+1} = \boldsymbol{I}_{n_y}$.

Numerical Simulation

The proposed algorithms are used for tracking the International Space Station (ISS), with its orbit defined by the following TLE set:

Figure 10: International Space Station, Courtesy of nasa.gov

TEXAS A&M UNIVERSITY

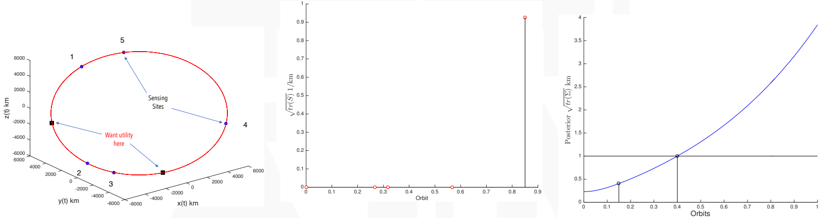
ISS tracking objectives:

With 5 sensing sites at at 0, 0.27 T_{orb}, 0.32 T_{orb}, 0.57 T_{orb}, 0.85 T_{orb}, ($T_{orb} := 6000$ secs), the objective of this example is to calculate:

- minimum sensor precision — satisfy given utility
- minimum synthetic noise — achieves the prescribed privacy
- optimal sensor precision — achieve utility-aware privacy

- We assume — Only initial condition uncertainty in the semi-major axis — we can measure (x, y, z) location.

UKF and EnKF

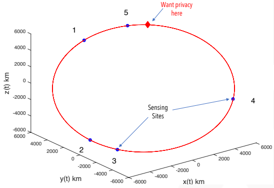


(a) Sensing sites **(b)** Optimal sensor precisions: $0, 0, 0, 0, 0.94$. **(c)** Posterior variance.

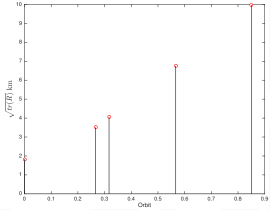
Figure 11: Optimal sensing precision satisfying utility constraints only.

Utility constraint is imposed on $0.15\,T_{\text{orb}}$, and $0.4\,T_{\text{orb}}$. We impose the utility constraints : $\textbf{tr}\left[\boldsymbol{M}_{u_i}\boldsymbol{\Sigma}^{+}\boldsymbol{M}_{u_i}^{T}\right] \leq 1$.

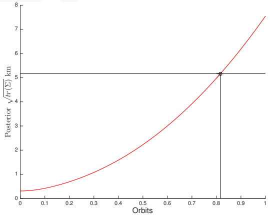
UKF and EnKF



(a) Privacy location.



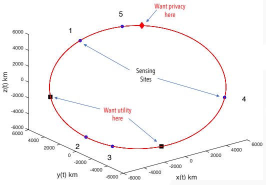
(b) Optimal sensor noise with l_1 minimization.



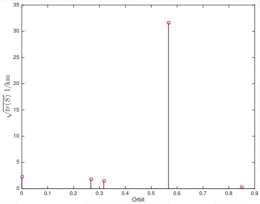
(c) Posterior variance.

Figure 12: Optimal sensor noise for only privacy.

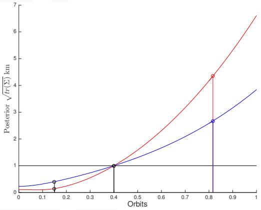
The location where privacy is required is shown in fig.(12a), which corresponds to time $0.82\,T_{\text{orb}}$. The privacy constraint is $\gamma_p := 5.17^2$ calculated from $\mathbf{tr}\left[\boldsymbol{M}_p\boldsymbol{\Sigma}^{+}\boldsymbol{M}_p^T\right] \geq 10^{-4}\mathbf{tr}\left[\boldsymbol{M}_p\boldsymbol{\Sigma}^{-}\boldsymbol{M}_p^T\right]$



(a) Privacy & Utility locations.



(b) Sensor $\underline{\text{precisions}}$: $2.30, 1.82, 1.51, 31.62, 0.29.$



(c) Red: Posterior variance. Blue: fig.(11c) shown again.

Figure 13: Optimal sensor precision for utility-aware privacy over one orbit of the ISS.

1. Showed how to solve the **Utility Problem** and **Privacy Problem** for
   1.1 **Kalman Filter**
   1.2 **Ensemble Kalman Filter** and **Unscented Kalman Filter**
2. A framework for **joint optimization** problem for utility-aware privacy and privacy-aware utility is shown.
3. This privacy-utility trade-off problem can be addressed for other filters such as particle filters.

Resulting Publications:

1. **Optimal Sensor Precision and Sensor Selection for Kalman Filtering with Bounded Errors** — Niladri Das & Raktim Bhattacharya — Signal Processing, Elsevier [under review, 2020]
2. **Privacy and Utility Aware Data Sharing for Space Situational Awareness from Ensemble and Unscented Kalman Filtering Perspective** — * — IEEE Transactions on Aerospace and Electronic Systems [minor revisions, 2020]
3. **Eigen Value Analysis in Lower Bounding Uncertainty of Kalman Filter Estimates** — * — IFAC World Congress 2020
4. **Optimal Transport Based Filtering with Nonlinear State Equality Constraints** — * — IFAC World Congress 2020
5. **Optimal Sensing Precision in Ensemble and Unscented Kalman Filtering** — * — IFAC World Congress 2020
6. **Sparse Sensing Architecture For Kalman Filtering With Guaranteed Error Bound** — * — IAA Conference on Space Situational Awareness 2017

Other Publications:

1. **Optimal Transport Based Tracking of Space Objects in Cylindrical Manifolds** — Niladri Das, R. P. Ghosh, N. Guha, Raktim Bhattacharya & B. Mallick — Journal of Astronautical Sciences, Springer [2019]
2. **Optimal Transport based Tracking of Space Objects using Range Data from a Single Ranging Station** — Niladri Das, V. Deshpande & Raktim Bhattacharya —Journal of Guidance, Control, and Dynamics [2019]
3. **Utility and Privacy in Object Tracking from Video Stream using Kalman Filter** — * — International Conference on Information Fusion 2020
4. **Modeling and Optimal Control of Hybrid UAVs with Wind Disturbance** — Sunsoo Kim, * — International Conference on Systems and Control 2020
5. **On Neural Network Training from Noisy Data using a Novel Filtering Framework** — V. Deshpande, Niladri Das, V. Tadiparthi & Raktim Bhattacharya — AIAA SciTech Forum and Exposition 2020

Acknowledgment:

- My Family (back in India) & Dr. Raktim Bhattacharya
- Dr. Srinivas Rao Vadali — Dr. Suman Chakravorty — Dr. P. R. Kumar — Dr. Kyle DeMars — Dr. Robert Skelton
- Friends, Co-workers, & Staff of Aerospace Engineering.
- Air Force Office of Scientific Research, Intelligent Fusion Technology, Inc., & National Science Foundation.

Thank You