Privacy-preserving Tobit filtering for nonlinear systems: when multi-rate sampling meets censored measurements

Shuo Yang[a,b], Raquel Caballero-Águila[b], Jun Hu[a] and Antonia Oya-Lechuga[b]

a: Department of Applied Mathematics, Harbin University of Science and Technology; b: Departamento de Estadística e Investigación Operativa, Universidad de Jaén

Abstract

- The filtering problem has long been recognized as an active research topic in signal processing.
- The differing physical features among system components usually cause the state updates and the measurement sampling to occur at different rates.
- Due to the intrinsic limitations of sensing devices, the acquired measurement data are frequently subject to censoring effects.
- In view of the openness of communication networks, the measurement signals are vulnerable to eavesdropping attacks during transmission.
- The Paillier encryption-decryption mechanism (PEDM) is integrated in our study, upon which a privacy-preserving Tobit filtering algorithm is presented for multi-rate nonlinear systems.
- An upper bound of the filtering error second moment is derived, and then minimized through the design of a proper filter parameter.
- The uniform boundedness of the filtering error in the mean-square sense is investigated.
- The effectiveness and feasibility of the proposed Tobit filtering algorithm are demonstrated through a simulation experiment.

Problem formulation

System model:

$$x_{t+1} = f(x_t) + C_t \omega_t,$$
$$y^*_{kt} = \hbar(x_{kt}) + v_{kt}.$$

Measurement censoring:

- Tobit Type I observation model:

$$\check{y}_{s,kt} = \begin{cases} y^*_{s,kt}, & \text{if } y^*_{s,kt} > \mathfrak{g}_s, \\ \mathfrak{g}_s, & \text{otherwise.} \end{cases}$$

- We denote:

$$\gamma^s_{kt} = \mathbb{1}_{[y^*_{s,kt} > \mathfrak{g}_s]} = \begin{cases} 1, & \text{if } y^*_{s,kt} > \mathfrak{g}_s, \\ 0, & \text{otherwise.} \end{cases}$$

- Approximation of the uncensored probability:

$$\bar{\gamma}^s_{kt} \approx \Phi\left(\frac{\hbar_s\left(\hat{x}_{kt|k(t-1)}\right) - \mathfrak{g}_s}{\sqrt{R^{s,s}_{kt}}}\right).$$

- Augmented form of censored measurements:

$$\check{y}_{kt} = \mathfrak{L}_{kt} y^*_{kt} + (I - \mathfrak{L}_{kt})\mathfrak{g}.$$

Multi-node random access protocol:

- The probability distribution of τ^s_{kt}:

$$\mathbb{P}\{\tau^s_{kt} = 1\} = \frac{\varrho}{m} \triangleq \bar{\vartheta}, \quad \mathbb{P}\{\tau^s_{kt} = 0\} = 1 - \bar{\vartheta}.$$

- Let $\vec{y}_{kt} = \mathrm{col}^m_{s=1}\{\vec{y}_{s,kt}\}$ and $\Omega_{kt} = \mathrm{diag}^m_{s=1}\{\tau^s_{kt}\}$. Then, we have $\vec{y}_{kt} = \Omega_{kt}\check{y}_{kt}$.

PEDM:

Key generation:

- Generate the public key $N = q_1 q_2$.
- Compute the private key $\kappa = \mathrm{lcm}\,(q_1 - 1, q_2 - 1)$ and $\mu = \kappa^{-1} \bmod N$.

Mapping:

- $\zeta_{s,kt} = \lceil \varpi_s \vec{y}_{s,kt} + \pi\left(\varpi_s \vec{y}_{s,kt}\right) \rfloor$, where

$$\pi\left(\varpi_s \vec{y}_{s,kt}\right) = \begin{cases} \rho_1, & \text{if } \varpi_s \vec{y}_{s,kt} < 0, \\ 0, & \text{otherwise.} \end{cases}$$

Encryption:

- $\delta_{s,kt} = (N+1)^{\zeta_{s,kt}} \alpha^N \bmod N^2$.

Decryption:

- $\zeta_{s,kt} = L\left((\delta_{s,kt})^\kappa \bmod N^2\right)\mu \bmod N$.

Inverse mapping:

- $\bar{y}_{s,kt} = \frac{\zeta_{s,kt} - \theta(\zeta_{s,kt})}{\varpi_s}$, where

$$\theta(\zeta_{s,kt}) = \begin{cases} \rho_1, & \text{if } \zeta_{s,kt} > \rho_2, \\ 0, & \text{otherwise.} \end{cases}$$

- The mapping error satisfies $|\iota_{s,kt}| \leq \frac{1}{2\varpi_s}$. Next, it is clear that $\bar{y}_{kt} = \vec{y}_{kt} + \iota_{kt}$.

Compensation strategy:

$$\tilde{y}_{s,kt} = \begin{cases} \bar{y}_{s,kt}, & \text{if } \tau^s_{kt} = 1, \\ \hat{\bar{y}}_{s,kt|k(t-1)}, & \text{otherwise.} \end{cases}$$

Then, we have $\tilde{y}_{kt} = \Omega_{kt}\bar{y}_{kt} + (I - \Omega_{kt})\hat{\bar{y}}_{kt|k(t-1)}$.

Model transformation:

$$\xi_t = \begin{cases} 1, & \text{if } t \text{ is a multiple of } k, \\ 0, & \text{otherwise.} \end{cases}$$

Then, the output signal is rewritten as $y_t = \xi_t \tilde{y}_t$.

Tobit recursive filter:

The Tobit recursive filter is designed as

$$\begin{aligned} \hat{x}_{t+1|t} &= f(\hat{x}_{t|t}), \\ \hat{x}_{t+1|t+1} &= \hat{x}_{t+1|t} + \mathscr{K}_{t+1}\{y_{t+1} - \xi_{t+1}\bar{\vartheta}\left(2 - \bar{\vartheta}\right) \\ &\quad \times \big[\bar{\mathfrak{L}}_{t+1}\left(\hbar(\hat{x}_{t+1|t}) + \mathcal{X}_{t+1}\mathfrak{R}_{t+1}\right) \\ &\quad + (I - \bar{\mathfrak{L}}_{t+1})\mathfrak{g}\big]\}. \end{aligned}$$

Main results

- Upper bound of prediction error second moment:

$$\begin{aligned} \mathscr{P}_{t+1|t} &= 2(1 + \mathfrak{h}_t)\left(\lambda^2_{1,t}\mathrm{tr}\left(\mathscr{P}_{t|t}\right) + \lambda^2_{2,t}\right) I \\ &\quad + (1 + \mathfrak{h}_t^{-1})\mathscr{A}_t\mathscr{P}_{t|t}\mathscr{A}_t^T + C_t Q_t C_t^T. \end{aligned}$$

- Upper bound of filtering error second moment:

$$\begin{aligned} &\mathscr{P}_{t+1|t+1} \\ &= (1 - \xi_{t+1})\mathscr{P}_{t+1|t} + \xi_{t+1}\Big\{\mathfrak{k}_{1,t+1}\mathscr{O}_{t+1}\mathscr{P}_{t+1|t}\mathscr{O}^T_{t+1} \\ &\quad + 2\mathfrak{k}_{2,t+1}\left(\eta^2_{1,t+1}\mathrm{tr}\left(\mathscr{P}_{t+1|t}\right) + \eta^2_{2,t+1}\right)\bar{\vartheta}^2\mathscr{K}_{t+1}\bar{\mathfrak{L}}_{t+1} \\ &\quad \times \bar{\mathfrak{L}}^T_{t+1}\mathscr{K}^T_{t+1} + \mathfrak{k}_{3,t+1}\mathscr{K}_{t+1}\left(\mathfrak{B}_{t+1} \circ \bar{\mathscr{H}}_{t+1}\right)\mathscr{K}^T_{t+1} \\ &\quad + \mathfrak{k}_{4,t+1}\bar{\vartheta}^2\mathscr{K}_{t+1}\big[\mathfrak{C} \circ \big(\bar{\mathfrak{L}}_{t+1}\hbar(\hat{x}_{t+1|t})\hbar^T(\hat{x}_{t+1|t}) \\ &\quad \times \bar{\mathfrak{L}}^T_{t+1}\big)\big]\mathscr{K}^T_{t+1} + \mathfrak{k}_{5,t+1}\mathscr{K}_{t+1}\left(\mathfrak{D} \circ \mathscr{G}_{t+1}\right)\mathscr{K}^T_{t+1} \\ &\quad + \mathfrak{k}_{6,t+1}\mathscr{K}_{t+1}\left[\mathfrak{F}_{t+1} \circ \left(\mathcal{X}_{t+1}\mathfrak{R}_{t+1}\mathfrak{R}^T_{t+1}\mathcal{X}^T_{t+1}\right)\right]\mathscr{K}^T_{t+1} \\ &\quad + \mathfrak{k}_{7,t+1}\mathscr{K}_{t+1}\left[\mathfrak{G}_{t+1} \circ \left(\mathfrak{g}\mathfrak{g}^T\right)\right]\mathscr{K}^T_{t+1} + \mathfrak{k}_{8,t+1}\bar{\vartheta}^2 \\ &\quad \times \mathscr{K}_{t+1}\left\{\mathfrak{C} \circ \left[(I - \bar{\mathfrak{L}}_{t+1})\mathfrak{g}\mathfrak{g}^T(I - \bar{\mathfrak{L}}_{t+1})^T\right]\right\}\mathscr{K}^T_{t+1} \\ &\quad + \mathfrak{k}_{9,t+1}\mathscr{K}_{t+1}\left(\mathfrak{D} \circ \mathfrak{H}\right)\mathscr{K}^T_{t+1}\Big\}. \end{aligned}$$

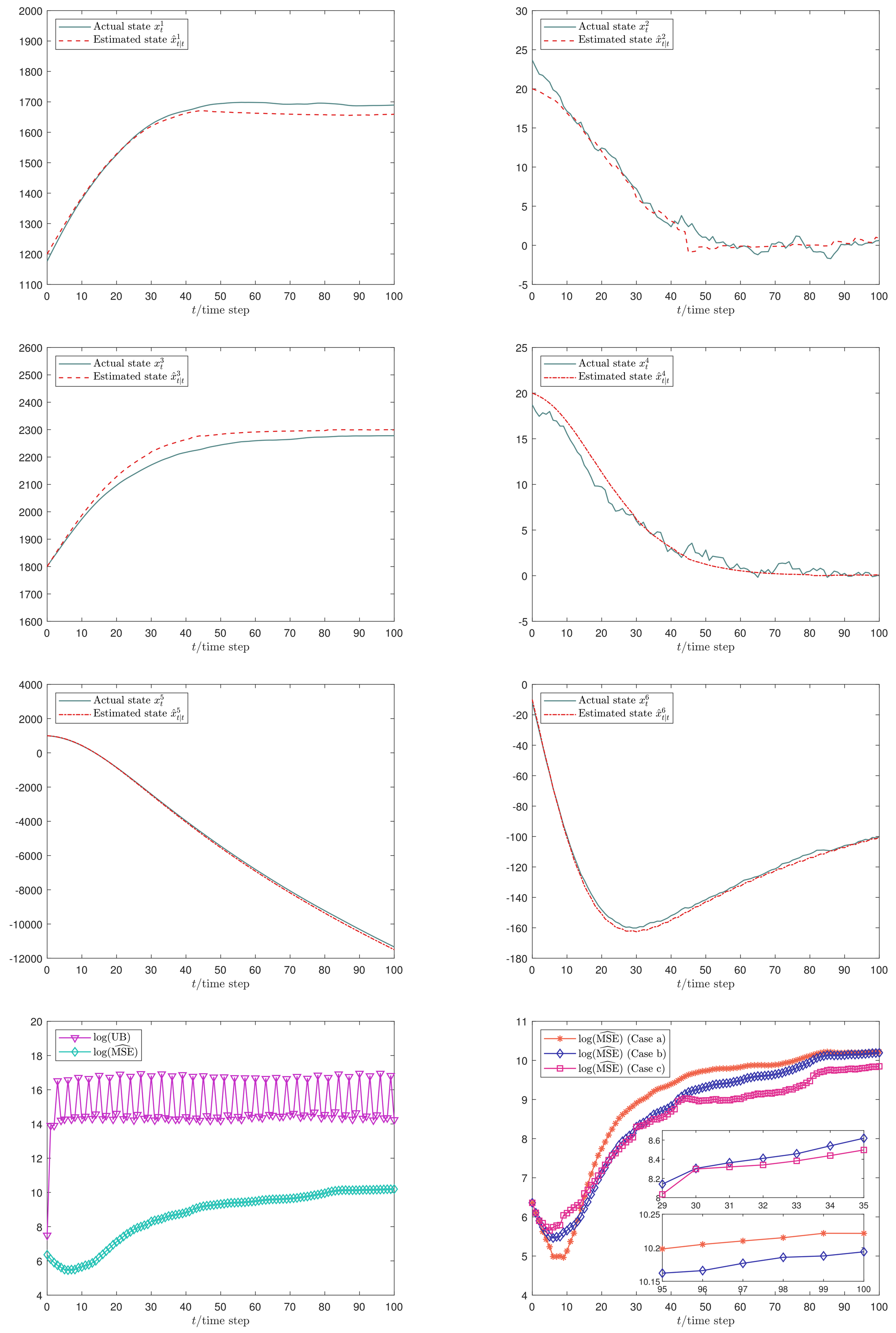
- The filter gain: $\mathscr{K}_{t+1} = \mathfrak{k}_{1,t+1}\bar{\vartheta}\mathscr{P}_{t+1|t}\mathscr{B}^T_{t+1}\bar{\mathfrak{L}}^T_{t+1}\mathfrak{I}^{-1}_{t+1}$.
- We give some parameter constraints and symbol definitions. It is obtained that $\mathbb{E}\{\tilde{x}_{t|t}\tilde{x}^T_{t|t}\} \leq \mathscr{P}_{t|t} \leq \bar{\mathfrak{p}}I$. Hence, using the linearity of expectation, one has

$$\mathbb{E}\{\|\tilde{x}_{t|t}\|^2\} \leq \mathrm{tr}(\mathscr{P}_{t|t}) \leq n_x\bar{\mathfrak{p}},$$

which indicates that the filtering error is uniformly bounded in the mean-square sense.

Target tracking simulation

$x_t = \mathrm{col}^6_{i=1}\{x^i_t\}$, where (x^1_t, x^3_t, x^5_t) and (x^2_t, x^4_t, x^6_t) denote 3D position and velocity.



Conclusions

- An innovative Tobit filtering strategy has been developed to mitigate the effects of measurement censoring and eavesdropping attacks under a multi-node random access protocol.
- An upper bound of the filtering error 2nd moment has been derived, enabling the filter computation.
- The uniform boundedness of the filtering error has been examined in the mean-square sense.
- A target tracking example has shown the efficacy of the proposed Tobit filtering scheme.