Pure Mathematics 理论数学, 2025, 15(3), 273-287
Published Online March 2025 in Hans. https://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2025.153102

Hans汉斯

一类状态饱和非线性系统的隐私保护分布式最大相关熵滤波：基于状态分解的方法

杜　雨[1]，张志祥[2]，丁德锐[2]

[1]上海理工大学理学院，上海
[2]上海理工大学光电信息与计算机工程学院，上海

收稿日期：2025年2月17日；录用日期：2025年3月10日；发布日期：2025年3月31日

摘　要

本文研究了一类在非高斯噪声影响下的状态饱和系统的分布式隐私保护熵滤波问题。首先，引入变量分解策略结合系统状态饱和的特征设计了一个分布式滤波器，其中考虑的系统遭受的乘性噪声以及非高斯噪声。接下来，结合已有的符合约束条件的时变动态密钥以及分解规则，得到私有误差协方差矩阵与公共协方差矩阵之间的关系以及它们的上界。在此基础上，最小化基于S-t核函数的最大熵准则下的代价函数得到待设计的滤波器增益。最后，通过对比窃听者滤波误差协方差和正常滤波误差协方差，分析了所设计的滤波算法的隐私性。最后利用仿真算例验证了算法的有效性以及安全性。

关键词

分布式滤波，最大相关熵，状态分解，状态饱和，S-t核函数，隐私保护

Privacy-Preserving Distributed Maximum Correntropy Filtering for State-Saturation Nonlinear Systems: A State Decomposition Approach

Yu Du[1], Zhixiang Zhang[2], Derui Ding[2]

[1]College of Science, University of Shanghai for Science and Technology, Shanghai
[2]School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai

Received: Feb. 17th, 2025; accepted: Mar. 10th, 2025; published: Mar. 31st, 2025

文章引用: 杜雨, 张志祥, 丁德锐. 一类状态饱和非线性系统的隐私保护分布式最大相关熵滤波: 基于状态分解的方法[J]. 理论数学, 2025, 15(3): 273-287. DOI: 10.12677/pm.2025.153102

Abstract

This paper studies the distributed privacy-preserving entropy filtering problem for a class of state-saturated systems under the influence of non-Gaussian noise. Firstly, a distributed filter is designed by introducing a variable decomposition strategy and considering the characteristics of system state saturation, where the multiplicative noise and non-Gaussian noise suffered by the system are taken into account. Next, by combining the existing time-varying dynamic keys that meet the constraint conditions and the decomposition rules, the relationship between the private error covariance matrix and the public covariance matrix and their upper bounds are obtained. On this basis, the filter gain to be designed is obtained by minimizing the cost function under the maximum entropy criterion based on the S-t kernel function. Finally, the privacy of the designed filtering algorithm is analyzed by comparing the eavesdropper's filtering error covariance with the normal filtering error covariance. The effectiveness and security of the algorithm are verified by simulation examples.

Keywords

Distributed Filtering, Maximum Correntropy, State Decomposition, State Saturation, S-t Kernel Function, Privacy Protection

1. 引言

状态估计是导航[1]、目标追踪[2]、系统识别、最优控制等[3]研究领域的重要关注之一，是获取系统动态行为的重要理论与关键技术。对于线性系统，卡尔曼滤波器(KF)是利用最小二乘思想提供状态估计问题最优递归解的线性滤波器。但现实中大多数系统均为非线性系统，从而使得KF的应用具有较大的局限性。为了解决非线性条件下的状态估计问题，许多改进的卡尔曼滤波器相继涌现，例扩展卡尔曼滤波器(EKF) [4]、无迹卡尔曼滤波器(UKF) [5]、正交卡尔曼滤波器(QKF) [6]等。

上述滤波器大都依据最小均方误差(MMSE)原则所设计的，当系统遭受的噪声符合高斯分布时，它们的估计精度较高。然而，由于MMSE原则只捕捉到了噪声的二阶统计特征，当系统遭受的噪声为非高斯噪声时，此类算法对异常值表现较为敏感从而使得算法的估计性能大大降低[7]。为了解决这一问题，学者们提出了一些基于非MMSE原则的滤波器。例如，基于Huber的卡尔曼滤波器(HKF) [8]通过采用Huber函数将残差有界化从而抑制了异常值对于状态估计的影响。最大相关熵卡尔曼滤波器(MCKF) [9]是基于信息理论学习(ITL) [10]中的最大相关熵准则(MCC)提出的。实验结果表明，其在复杂非高斯噪声干扰下展示了良好的性能，优于传统的滤波方法。

需要指出的是基于ITL的滤波器性能在很大程度上依赖于核函数及其选择的参数。目前，大多数此类滤波器仍采用高斯核函数。然而，在一些实际应用场景例如敏捷目标跟踪[11]、多路径估计等，系统通常遭受到重尾非高斯噪声的干扰。对于重尾噪声，基于高斯核的滤波器难以选择适当的核带宽而往往无法充分捕捉其重尾特性；此外，在执行过程中奇异矩阵的出现通常会导致算法的崩溃，从而可能导致估计精度的显著下降。因此，高斯核函数作为代价函数并非最优选择，探索其他类型的核函数以克服高斯核函数固有的不足具有重要意义。文献[12]中提出了一种基于Cauchy核函数的最大相关熵卡尔曼滤波器(CKKF)。与使用

高斯核函数的MCKF相比，CKKF在处理多维非高斯噪声时表现更优。同时，当选择不同的Cauchy核带宽时，CKKF的性能始终保持稳定。最近，基于S-t分布提出了一种新的核函数：S-t核函数[13]。与高斯核函数不同，S-t核函数具有两个参数，可以分别控制核函数的形状和带宽，从而其更有效地捕捉噪声的重尾特性。在适当选择核函数参数的情况下，当噪声为重尾非高斯分布时，STKKF的状态估计精度优于传统算法。

另一方面，分布式滤波可以在多个节点上并行处理信息，其相较于集中式滤波具有显著的优点，包括提高系统的鲁棒性、降低通信负担、提升可扩展性等。但目前部署的网络通常是开放的。尽管已经采取了大量保护措施，但数据泄露和网络攻击等问题仍然无法避免[14]。这种情况往往会导致巨大的经济损失、负面的社会影响，甚至对国家安全构成威胁。近年来，研究者提出了几种隐私保护方法，如同态加密[15]、水印[16]和注入扰动策略等。状态饱和[17]是实际系统中普遍存在的一种现象，通常由系统状态的物理限制所引起。如果未能妥善处理状态饱和，滤波器的性能可能会迅速下降。综上所述，本文针对一类状态和非线性系统，旨在设计一种基于状态分解和S-t核函数的隐私保护分布式最大相关熵滤波算法，以增强其在非高斯环境下的鲁棒性以及数据分享的隐私性。研究面临的主要挑战包括：1) 如何选择适当的隐私保护策略设计状态饱和下的熵滤波器；2) 如何分析滤波算法的隐私性。本文系统地解决了上述挑战，给出了变量分解下的方差上界的迭代计算规则，并结合传统的定点迭代技术设计了一种新型的分布式熵滤波算法，主要贡献如下：

1) 基于分解的状态，设计了一种针对状态饱和非线性系统的分布式滤波器；

2) 基于S-t核函数的损失函数和定点迭代规则，给出了私有估计与公共估计的误差协方差矩阵的上界及其分布式最大相关熵滤波器增益。

2. 问题描述

本文考虑的传感器网络由n个传感器节点组成，节点之间的通信描述为有向图$\mathcal{G}=(\mathcal{N},\mathcal{E},\mathcal{H})$，其中$\mathcal{N}=\{1,2,\cdots,n\}$为节点集，$\mathcal{E}\subseteq\mathcal{N}\times\mathcal{N}$代表边连接集，$\mathcal{H}=\left[a_{ij}\right]_{n\times n}$表示传感器节点间的加权邻接矩阵。对于所有节点$i,j\in\mathcal{N}$，如果$(i,j)\in\mathcal{E}$，则有$a_{ij}>0$，即节点$i$可以接收到来自节点$j$的信息；否则$a_{ij}=0$，即节点$i$不能接收到来自节点$j$的信息。显而易见，矩阵元素$a_{ij}$反应了节点$i$与节点$j$之间连接的紧密程度。最后，记第$i$个传感器的邻居传感器集为$\mathcal{N}_i=\{j:(i,j)\in\mathcal{E}\}$，邻居的个数为$d_i$。

考虑一类带有状态饱和的离散随机线性系统，其动力学行为可描述为

$$\begin{cases}x_{k+1}=\sigma\left(Ax_k+\zeta_k Gx_k\right)+\omega_k\\ y_{i,k+1}=C_i x_{k+1}+v_{i,k+1}\end{cases}\tag{1}$$

式中$x_{k+1}\in\mathbb{R}^{n_x}$和$y_{i,k+1}\in\mathbb{R}^{n_y}$分别表示待估计的状态变量和传感器$i$的测量输出；$\omega_k\in\mathbb{R}^{n_\omega}$和$v_{i,k}\in\mathbb{R}^{n_v}$为互不相关的非高斯噪声，它们的均值均为0且对应的协方差矩阵分别为$\mathbb{E}\left[\omega_k\omega_k^{\mathrm{T}}\right]=W_k$和$\mathbb{E}\left[v_{i,k}v_{i,k}^{\mathrm{T}}\right]=V_{i,k}$；随机变量$\zeta_k$是均值为0方差为1的噪声序列，描述了系统遭受的乘性噪声。进而，考虑到实际工程系统通常运行在一个有限的范围内，即系统遭受状态保护，故引入非线性映射$\sigma(\cdot):\mathbb{R}^n\to\mathbb{R}^n$是一描述受状态饱和影响。具体地，对于向量$x\triangleq\left[x_1\ \ x_2\ \ \cdots\ \ x_n\right]^{\mathrm{T}}\in\mathbb{R}^n$，定义$\sigma(x)=\left[\sigma_1(x_1)\ \ \sigma_2(x_2)\ \ \cdots\ \ \sigma_n(x_n)\right]^{\mathrm{T}}$，其中$\sigma_i(x_i)=\mathrm{sign}(x_i)\min\{\gamma_i,|x_i|\}$。这里，$\gamma_i>0$代表饱和水平。$A$，$G$和$C_i$分别代表系统矩阵和测量矩阵。

为了监控上述目标的动态行为，理想的滤波器可设计为：

$$\begin{cases}\hat{x}_{i,k+1}^{-}=\sigma\left(A\hat{x}_{i,k}^{+}+\varepsilon\sum\limits_{j\in\mathcal{N}_i}a_{ij}\left(A\hat{x}_{i,k}^{+}-A\hat{x}_{j,k}^{+}\right)\right)\\ \hat{x}_{i,k+1}^{+}=\hat{x}_{i,k+1}^{-}+K_{i,k+1}\left(y_{i,k+1}-C_i\hat{x}_{i,k+1}^{-}\right)\end{cases}\tag{2}$$

其中 $\hat{x}_{i,k+1}^{-}$ 和 $\hat{x}_{i,k+1}^{+}$ 分别代表 $k+1$ 时刻第 i 个传感器的一步状态预测和一步估计，$\hat{x}_{j,k}^{+}$ 代表来自于邻居的理想一步估计。正标量 $\varepsilon\in\left(0,1/\beta\right)$ 代表一致性增益，其中 $\beta=\max\left\{\lambda_i\right\}$，$\lambda_i$ 是通信拓扑图的拉普拉斯矩阵的特征值。矩阵 $K_{i,k+1}$ 为待设计的滤波器增益。不失一般性，初始状态假设满足 $\hat{x}_{i,k+1}^{-}=\hat{x}_{i,0}^{+}=\mathbb{E}\left\{x_0\right\}=\mu_0\left(i\in\mathcal{N}\right)$。

由(2)不难发现，分布式滤波器的实现依赖于邻居信息的交互。然而，开放的网络可能导致信息的泄露，从而被外部恶意攻击者利用，造成不必要的损失。为了保证数据传输的隐私性，对传输的估计值 $\hat{x}_{i,k}^{+}$ 进行状态分解：

$$\hat{x}_{i,k}^{+}=\alpha_{i,k}\hat{x}_{i,k}^{+}+\beta_{i,k}\hat{x}_{i,k}^{+}=\hat{x}_{i,k}^{\alpha+}+\hat{x}_{i,k}^{\beta+} \tag{3}$$

其中 $\alpha_{i,k}=1-\beta_{i,k}$，$\beta_{i,k}$ 是滤波器 i 的动态私钥，满足提前确定的变化规则，该规则与其邻居共享，并不被窃听所获取。需要指出的是，滤波器 i 的邻居 j 将根据该动态私钥传输信息对应的估计值 $\hat{x}_{ij,k}^{\beta+}=\beta_{ik}\hat{x}_{j,k}^{+}$。根据这一规则，滤波器 i 仅能够收到邻居分解后的信息。为此，实际设计的滤波器为

$$\begin{cases}\hat{x}_{i,k+1}^{-}=\sigma\left(A\hat{x}_{i,k}^{+}+\varepsilon\sum\limits_{j\in\mathcal{N}_i}a_{ij}\left(\beta_{ik}A\hat{x}_{i,k}^{+}-A\hat{x}_{ij,k}^{\beta+}\right)\right)\\ \hat{x}_{i,k+1}^{+}=\hat{x}_{i,k+1}^{-}+K_{i,k+1}\left(y_{i,k+1}-C_i\hat{x}_{i,k+1}^{-}\right)\end{cases} \tag{4}$$

其中 $\hat{x}_{ij,k}^{\beta+}$ 为外部窃听者可以听到的、邻居之间实际交换的数据。

对于外部窃听者来说，它可以使用网络中传输的部分数据来构建自己的状态估计，其迭代规则如下所示：

$$\begin{cases}\hat{x}_{i,k+1,e}^{-}=\sigma\left(A\hat{x}_{i,k,e}^{+}+\varepsilon\sum\limits_{j\in\mathcal{N}_i}a_{ij}\left(A\hat{x}_{i,k,e}^{+}-A\hat{x}_{ij,k}^{\beta+}\right)\right)\\ \hat{x}_{i,k+1,e}^{+}=\hat{x}_{i,k+1,e}^{-}+K_{i,k+1}\left(y_{i,k+1}-C_i\hat{x}_{i,k+1,e}^{-}\right)\end{cases} \tag{5}$$

其中 $\hat{x}_{i,k+1,e}^{+}$ 代表外部窃听者的估计值。

注 1：在上式中，$\varepsilon\sum\limits_{j\in\mathcal{N}_i}a_{ij}\left(A\hat{x}_{i,k,e}^{+}-A\hat{x}_{ij,k}^{\beta+}\right)$ 表明了窃听者是利用从其他节点获取的信息来调整其预测值。

针对系统的饱和约束，有如下引理。

引理 1 [13]：假设函数 $\sigma_i\left(\cdot\right)$ 如下式所定义，则有：

$$\sigma_i\left(u\right)-\sigma_i\left(v\right)=\lambda_i\left(u-v\right),\quad\forall u,v\in\mathbb{R}$$

其中 $\lambda_i\in\left[0,1\right]$。

记 $e_{i,k}^{+}=x_k-\hat{x}_{i,k}^{+}$，$e_{i,k}^{-}=x_k-\hat{x}_{i,k}^{-}$。考虑到系统的饱和特性，由引理 1 一定存在一个满足 $0\le\Lambda_k\le I$ 矩阵 Λ_k 使得

$$\begin{aligned}e_{i,k+1}^{-}&=x_{k+1}-\hat{x}_{i,k+1}^{-}\\&=\sigma\left(Ax_k+\zeta_kGx_k\right)+\omega_k-\sigma\left(A\hat{x}_{i,k}^{+}+\varepsilon\sum_{j\in\mathcal{N}_i}a_{ij}\left(\beta_{ik}A\hat{x}_{i,k}^{+}-A\hat{x}_{ij,k}^{\beta+}\right)\right)\\&=\Lambda_k\left(Ae_{i,k}^{+}-\varepsilon\sum_{j\in\mathcal{N}_i}a_{ij}\beta_{ik}A\left(e_{j,k}^{+}-e_{i,k}^{+}\right)\right)+\gamma_k\Lambda_kGx_k+\omega_k\end{aligned}$$

和

$$\begin{aligned}e_{i,k+1}^{+}&=x_{k+1}-\hat{x}_{i,k+1}^{+}\\&=x_{k+1}-\hat{x}_{i,k+1}^{-}-K_{i,k+1}\left(y_{i,k+1}-C_i\hat{x}_{i,k+1}^{-}\right)\\&=\left(I_n-K_{i,k+1}C_i\right)e_{i,k+1}^{-}-K_{i,k+1}v_{i,k+1}.\end{aligned}$$

在高斯噪声下，卡尔曼滤波算法实现了最小均方误差准下的最优估计。然而，当系统中的 $\omega_{i,k}$ 和 $\nu_{i,k}$ 均为服从非高斯分布时，传统的卡尔曼滤波算法并不能得到最优估计。特别地，当噪声呈现重尾分布式或存在野值的时候，可能造成滤波性能的衰减。针对这一问题，本文采用了基于高斯核函数的最大熵准则提高滤波器的滤波性能。为此，系统(1)中的测量可写为

$$\begin{bmatrix} \hat{x}_{i,k}^{-} \\ y_{i,k} \end{bmatrix} = \begin{bmatrix} I_{n_x} \\ C_i \end{bmatrix} x_k + \xi_{i,k} \tag{6}$$

其中

$$\xi_{i,k} = \begin{bmatrix} \hat{x}_{i,k}^{-} - x_k \\ \nu_{i,k} \end{bmatrix}$$

对该向量求方差，可得

$$\mathbb{E}\left[\xi_{i,k}\xi_{i,k}^{\mathrm{T}}\right] = \begin{bmatrix} P_{i,k}^{-} & 0 \\ 0 & V_{i,k} \end{bmatrix} = \begin{bmatrix} \Omega_{P_{i,k}}\Omega_{P_{i,k}}^{\mathrm{T}} & 0 \\ 0 & \Omega_{V_{i,k}}\Omega_{V_{i,k}}^{\mathrm{T}} \end{bmatrix} = \Omega_{i,k}\Omega_{i,k}^{\mathrm{T}} \tag{7}$$

其中 $P_{i,k}^{-}$ 代表一步预测协方差矩阵；$\Omega_{i,k}$ 为 $\mathbb{E}\left[\xi_{i,k}\xi_{i,k}^{\mathrm{T}}\right]$ 的 Cholesky 分解矩阵。为了对向量 $\xi_{i,k}$ 进行归一化处理，将式(6)两端同时乘以 $\Omega_{i,k}^{-1}$，得到

$$\bar{y}_{i,k} = \mathfrak{M}_{i,k}x_k + \eta_{i,k} \tag{8}$$

其中 $\eta_{i,k} = \Omega_{i,k}^{-1}\xi_{i,k}$，以及

$$\mathfrak{M}_{i,k} = \Omega_{i,k}^{-1}\begin{bmatrix} I_{n_x} \\ C_i \end{bmatrix}.$$

对于这一分解，不难发现 $\mathbb{E}\left[\eta_{i,k}\eta_{i,k}^{\mathrm{T}}\right] = I$，即将 $\eta_{i,k}$ 化为白噪声。此外，由于系统的分布式特性，精确的方差矩阵 $P_{i,k}^{-}$ 是难以获得的。一个可行的方法是寻找一个较小的上界加以替代。根据最大熵原则，同时为了更好地捕获噪声中的重尾特征，本文使用 S-t 核函数来代替高斯核函数[13]，采用的损失函数如下：

$$J_{n_x+n_y}\left(\hat{x}_{i,k}^{+}\right) = \frac{1}{n_x+n_y}\left(\sum_{\ell=1}^{n_x}\mathrm{Y}_{v,\lambda_k}\left[\eta_{x_{i,k}}\right]_{\ell} + \sum_{\ell=1}^{n_y}\mathrm{Y}_{v,\lambda_k}\left[\eta_{y_{i,k}}\right]_{\ell}\right)$$

其中 λ_k 为带宽或者核宽度，v 用于控制 Student's t 核函数的形状，其他向量为

$$\eta_{x_{i,k}} = \Omega_{P_{i,k}}^{-1}\left(\hat{x}_{i,k}^{+} - \hat{x}_{i,k}^{-}\right),\ \eta_{y_{i,k}} = \Omega_{V_{i,k}}^{-1}\left(y_{i,k} - C_i\hat{x}_{i,k}^{+}\right),\ \mathrm{Y}_{v,\lambda_k}\left(\zeta\right) = \left(1 + \frac{\zeta}{v\lambda_k^2}\right)^{-\frac{v+2}{2}}$$

在该指标中，$\Omega_{P_{i,k}}$ 和 $\Omega_{V_{i,k}}$ 是一组权重矩阵，在实现白化处理的同时，实现了状态估计稳定和状态估计准确的权衡。

综述所述，本文的设计目标如下

1) 借助于估计误差方差，获得理想的权重矩阵 $\Omega_{i,k}$；

2) 设计合适的滤波增益矩阵 $K_{i,k+1}$ 获得最优估计值 $\hat{x}_{i,k}^{+}$，使得

$$\hat{x}_{i,k}^{+} = \arg\max_{\hat{x}_{i,k}^{+}} J_{n_x+n_y}\left(\hat{x}_{i,k}^{+}\right). \tag{9}$$

基于 MCC 下的滤波器增益计算

本节致力于设计基于 MCC 原则的分布式隐私保护滤波器。为此，记

$$P_{ii,k}^{-}=\mathbb{E}\left\{\hat{e}_{i,k}^{-}\left(\hat{e}_{i,k}^{-}\right)^{\mathrm{T}}\right\},\quad P_{ii,k}^{+}=\mathbb{E}\left\{\hat{e}_{i,k}^{+}\left(\hat{e}_{i,k}^{+}\right)^{\mathrm{T}}\right\}$$

代表先验协方差矩阵和后验协方差矩阵。进而，$\hat{e}_{i,k}^{-}$ 和 $\hat{e}_{i,k}^{+}$ 相应的分解可以表示为：

$$\hat{e}_{i,k}^{-}=\alpha_{i,k}\hat{e}_{i,k}^{-}+\beta_{i,k}\hat{e}_{i,k}^{-}=\hat{e}_{i,k}^{\alpha-}+\hat{e}_{i,k}^{\beta-},\ \ \hat{e}_{i,k}^{+}=\alpha_{i,k}\hat{e}_{i,k}^{+}+\beta_{i,k}\hat{e}_{i,k}^{+}=\hat{e}_{i,k}^{\alpha+}+\hat{e}_{i,k}^{\beta+}.$$

结合引入的状态分解规则和引理 1，两组误差动态可表示为：

$$\begin{cases}\hat{e}_{i,k+1}^{\alpha-}=\Lambda_k A\hat{e}_{i,k}^{\alpha+}+\gamma_k\alpha_{ik}\Lambda_k Gx_k+\alpha_{ik}w_k\\ \hat{e}_{i,k+1}^{\alpha+}=\left(I_n-K_{i,k+1}C_i\right)\hat{e}_{i,k+1}^{\alpha-}-\alpha_{ik}K_{i,k+1}v_{i,k+1}\end{cases}\tag{10}$$

和

$$\begin{cases}\hat{e}_{i,k+1}^{\beta-}=\Lambda_k\left(Ae_{i,k}^{\beta+}-\varepsilon\sum\limits_{j\in\mathcal{N}_i}a_{ij}A\left(e_{j,k}^{\beta+}-e_{i,k}^{\beta+}\right)\right)+\gamma_k\beta_{ik}\Lambda_k Gx_k+\beta_{ik}\omega_k\\ \hat{e}_{i,k+1}^{\beta+}=\left(I_n-K_{i,k+1}C_i\right)\hat{e}_{i,k+1}^{\beta-}-\beta_{ik}\,K_{i,k+1}v_{i,k+1}\end{cases}\tag{11}$$

明显地，误差动态(10)是由私钥分解部分驱动产生的，可称之为私有误差动态；误差动态(11)是由公钥分解部分驱动生成的，可称之为公共误差动态。对比窃听者的估计策略，不难发现其窃听不准确的原因正是由于私钥分解部分的缺失。

对于状态分解后的一步预测协方差矩阵和误差协方差矩阵满足如下关系：

$$P_{i,k}^{+}=P_{i,k}^{\alpha+}+P_{i,k}^{\beta+}+2\alpha_{i,k}\beta_{i,k}P_{i,k}^{+}=\left(1-2\alpha_{i,k}\beta_{i,k}\right)^{-1}\left(P_{i,k}^{\alpha+}+P_{i,k}^{\beta+}\right)\tag{12}$$

和

$$P_{i,k}^{-}=P_{i,k}^{\alpha-}+P_{i,k}^{\beta-}+2\alpha_{i,k}\beta_{i,k}P_{i,k}^{-}=\left(1-2\alpha_{i,k}\beta_{i,k}\right)^{-1}\left(P_{i,k}^{\alpha-}+P_{i,k}^{\beta-}\right)\tag{13}$$

定理 1 假设分解误差动态(即私有误差动态(10)和公共误差动态(11))的私有和公共估计误差协方差 $P_{i,k}^{\alpha+}$ 和 $P_{i,k}^{\beta+}$ 的初值满足 $P_{i,0}^{\alpha+}=\Xi_{i,0}^{\alpha+}$ 和 $P_{i,0}^{\beta+}=\Xi_{i,0}^{\beta+}$，先验误差协方差 $P_{i,k}^{\alpha-}$ 和 $P_{i,k}^{\beta-}$ 的初值满足 $P_{i,0}^{\alpha-}=\Xi_{i,0}^{\alpha-}$ 和 $P_{i,0}^{\beta-}=\Xi_{i,0}^{\beta-}$。分布式隐私保护滤波器(4)的先验协方差矩阵和后验协方差矩阵的上界分别为

$$\begin{cases}P_{ii,k}^{+}\le\Xi_{i,k}^{+}=\left(1-2\alpha_{i,k}\beta_{i,k}\right)^{-1}\left(\Xi_{i,k}^{\alpha+}+\Xi_{i,k}^{\beta+}\right),\\ P_{ii,k}^{-}\le\Xi_{i,k}^{-}=\left(1-2\alpha_{i,k}\beta_{i,k}\right)^{-1}\left(\Xi_{i,k}^{\alpha-}+\Xi_{i,k}^{\beta-}\right),\end{cases}\tag{14}$$

其中 $\Xi_{i,k}^{\alpha+}$、$\Xi_{i,k}^{\beta+}$、$\Xi_{i,k}^{\alpha-}$ 和 $\Xi_{i,k}^{\beta-}$ 满足如下递推矩阵约束

$$\begin{cases}\Xi_{ii,k+1}^{\alpha+}=\left(I-K_{i,k+1}C_{i,k+1}\right)\Xi_{ii,k+1}^{\alpha-}\left(I-K_{i,k+1}C_{i,k+1}\right)^{\mathrm{T}}+\alpha_{i,k+1}^2K_{i,k+1}V_{i,k+1}K_{i,k+1}^{\mathrm{T}}\\ \Xi_{ii,k+1}^{\alpha-}=\mathrm{tr}\left\{A\Xi_{ii,k}^{\alpha+}A^{\mathrm{T}}\right\}I+\mathrm{tr}\left\{\alpha_{ik}^2G\Psi_kG^{\mathrm{T}}\right\}I+\alpha_{ik}^2W_k\end{cases}\tag{15}$$

和

$$\begin{cases}\Xi_{ii,k+1}^{\beta+}=\left(I-K_{i,k+1}C_{i,k+1}\right)\Xi_{ii,k+1}^{\beta-}\left(I-K_{i,k+1}C_{i,k+1}\right)^{\mathrm{T}}+\beta_{i,k+1}^2K_{i,k+1}V_{i,k+1}K_{i,k+1}^{\mathrm{T}}\\ \Xi_{ii,k+1}^{\beta-}=\beta_{ik}^2W_k+\mathrm{tr}\left\{\left(1+\pi\right)A\Xi_{ii,k}^{\beta+}A^{\mathrm{T}}+2\varepsilon^2d_i\left(1+\pi^{-1}\right)\sum\limits_{j\in\mathcal{N}_i}a_{ij}^2A\left(\Xi_{ii,k}^{\beta+}+\Xi_{jj,k}^{\beta+}\right)A^{\mathrm{T}}\right\}I+\mathrm{tr}\left\{\beta_{ik}^2G\Psi_kG^{\mathrm{T}}\right\}I\end{cases}\tag{16}$$

这里，$\Psi_k = \min\left\{\mathrm{tr}\left\{(1+\rho)\Xi_{jj,k}^{\beta+} + \left(1+\rho^{-1}\right)\hat{x}_{j,k}^{\beta+}\hat{x}_{j,k}^{\beta+\mathrm{T}}\right\}, \mathrm{tr}\left\{\sum_{i=1}^{n_Y}\gamma_i^2 I + W_k\right\}\right\}$。

证明：根据方差的定义，计算可得

$$\begin{aligned}
P_{ii,k+1}^{\alpha-} &= \mathbb{E}\left\{\hat{e}_{i,k+1}^{\alpha-}\left(\hat{e}_{i,k+1}^{\alpha-}\right)^{\mathrm{T}}\right\} = \Lambda_k A P_{ii,k}^{\alpha+} A^{\mathrm{T}}\Lambda_k^{\mathrm{T}} + \alpha_{ik}^2\Lambda_k G X_k G^{\mathrm{T}}\Lambda_k^{\mathrm{T}} + \alpha_{ik}^2 W_k,\\
P_{ii,k+1}^{\beta-} &= \mathbb{E}\left\{\hat{e}_{i,k+1}^{\beta-}\left(\hat{e}_{i,k+1}^{\beta-}\right)^{\mathrm{T}}\right\}\\
&= \Lambda_k A P_{ii,k}^{\beta+} A^{\mathrm{T}}\Lambda_k^{\mathrm{T}} - 2\varepsilon\sum_{j\in\mathcal{N}_i} a_{ij}\Lambda_k A\mathbb{E}\left\{e_{i,k}^{\beta+}\left(e_{j,k}^{\beta+} - e_{i,k}^{\beta+}\right)^{\mathrm{T}}\right\}A^{\mathrm{T}}\Lambda_k^{\mathrm{T}}\\
&\quad + \varepsilon^2\sum_{j\in\mathcal{N}_i}\sum_{s\in\mathcal{N}_i} a_{ij}a_{is}\Lambda_k A\mathbb{E}\left\{\left(e_{j,k}^{\beta+} - e_{i,k}^{\beta+}\right)\left(e_{s,k}^{\beta+} - e_{i,k}^{\beta+}\right)^{\mathrm{T}}\right\}A^{\mathrm{T}}\Lambda_k^{\mathrm{T}}\\
&\quad + \beta_{ik}^2\Lambda_k G X_k G^{\mathrm{T}}\Lambda_k^{\mathrm{T}} + \beta_{ik}^2 W_k.
\end{aligned} \tag{17}$$

同理可得

$$\begin{aligned}
P_{ii,k+1}^{\alpha+} &= \mathbb{E}\left\{\hat{e}_{i,k+1}^{\alpha+}\left(\hat{e}_{i,k+1}^{\alpha+}\right)^{\mathrm{T}}\right\}\\
&= \left(I_n - K_{i,k+1}C_i\right)P_{ii,k+1}^{\alpha-}\left(I_n - K_{i,k+1}C_i\right)^{\mathrm{T}} + \alpha_{ik}^2 K_{i,k+1}V_{i,k+1}K_{i,k+1}^{\mathrm{T}}\\
P_{ii,k+1}^{\beta+} &= \mathbb{E}\left\{e_{i,k+1}^{\beta+}\left(e_{i,k+1}^{\beta+}\right)^{\mathrm{T}}\right\}\\
&= \left(I_n - K_{i,k+1}C_i\right)P_{ii,k+1}^{\beta-}\left(I_n - K_{i,k+1}C_i\right)^{\mathrm{T}} + \beta_{ik}^2 K_{i,k+1}V_{i,k+1}K_{i,k+1}^{\mathrm{T}}
\end{aligned} \tag{18}$$

另一方面，让我们分析系统的二阶矩，可知

$$\begin{aligned}
X_k &= \mathbb{E}\left\{x_k x_k^{\mathrm{T}}\right\}\\
&= \mathbb{E}\left\{\left(\sigma\left(Ax_k + \zeta_k Gx_k\right) + \omega_k\right)\left(\sigma\left(Ax_k + \zeta_k Gx_k\right) + \omega_k\right)^{\mathrm{T}}\right\}\\
&= \mathbb{E}\left\{\sigma\left(Ax_k + \zeta_k Gx_k\right)\sigma^{\mathrm{T}}\left(Ax_k + \zeta_k Gx_k\right)\right\} + W_k\\
&\le \mathrm{tr}\mathbb{E}\left\{\sigma\left(Ax_k + \zeta_k Gx_k\right)\sigma^{\mathrm{T}}\left(Ax_k + \zeta_k Gx_k\right)\right\} I + W_k\\
&\le \sum_{i=1}^{n_Y}\gamma_i^2 I + W_k
\end{aligned}$$

又根据[18]得

$$\begin{aligned}
X_k &= \mathbb{E}\left\{x_k x_k^{\mathrm{T}}\right\}\\
&= \mathbb{E}\left\{\hat{x}_{j,k}^{\beta+}\hat{x}_{j,k}^{\beta+\mathrm{T}} + \hat{x}_{j,k}^{\beta+\mathrm{T}}e_{j,k}^{\beta+\mathrm{T}} + e_{j,k}^{\beta+\mathrm{T}}\hat{x}_{j,k}^{\beta+\mathrm{T}} + e_{j,k}^{\beta+}e_{j,k}^{\beta+\mathrm{T}}\right\}\\
&\le (1+\rho)P_{jj,k}^{\beta+} + \left(1+\rho^{-1}\right)\hat{x}_{j,k}^{\beta+}\hat{x}_{j,k}^{\beta+\mathrm{T}}
\end{aligned}$$

因此通过结合两式我们得到：

$$tr\left(X_k\right) \le \min\left\{\mathrm{tr}\left\{(1+\rho)P_{jj,k}^{\beta+} + \left(1+\rho^{-1}\right)\hat{x}_{j,k}^{\beta+}\hat{x}_{j,k}^{\beta+\mathrm{T}}\right\}, \mathrm{tr}\left\{\sum_{i=1}^{n_Y}\gamma_i^2 I + W_k\right\}\right\} \triangleq \Psi_k$$

接下来，让我们处理(17)中的交叉项，不难有

$$\begin{aligned}
P_{ii,k+1}^{\beta-} &\le (1+\pi)\Lambda_k A P_{ii,k}^{\beta+} A^{\mathrm{T}}\Lambda_k^{\mathrm{T}} + \beta_{ik}^2\Lambda_k G X_k G^{\mathrm{T}}\Lambda_k^{\mathrm{T}} + \beta_{ik}^2 W_k \\
&\quad + \varepsilon^2\left(1+\pi^{-1}\right)\sum_{j\in\mathcal{N}_i}\sum_{s\in\mathcal{N}_i} a_{ij}a_{is}\Lambda_k A\mathbb{E}\left\{\left(e_{j,k}^{\beta+}-e_{i,k}^{\beta+}\right)\left(e_{s,k}^{\beta+}-e_{i,k}^{\beta+}\right)\right\}A^{\mathrm{T}}\Lambda_k^{\mathrm{T}} \\
&\le (1+\pi)\Lambda_k A P_{ii,k}^{\beta+} A^{\mathrm{T}}\Lambda_k^{\mathrm{T}} + \beta_{ik}^2\Lambda_k G X_k G^{\mathrm{T}}\Lambda_k^{\mathrm{T}} + \beta_{ik}^2 W_k \\
&\quad + 2\varepsilon^2 d_i\left(1+\pi^{-1}\right)\sum_{j\in\mathcal{N}_i} a_{ij}^2\Lambda_k A\left(P_{ii,k}^{\beta+}+P_{jj,k}^{\beta+}\right)A^{\mathrm{T}}\Lambda_k^{\mathrm{T}} \\
&\le \beta_{ik}^2 W_k + \mathrm{tr}\left\{(1+\pi)\Lambda_k A P_{ii,k}^{\beta+} A^{\mathrm{T}}\Lambda_k^{\mathrm{T}} + \beta_{ik}^2\Lambda_k G X_k G^{\mathrm{T}}\Lambda_k^{\mathrm{T}}\right. \\
&\quad \left. + 2\varepsilon^2 d_i\left(1+\pi^{-1}\right)\sum_{j\in\mathcal{N}_i} a_{ij}^2\Lambda_k A\left(P_{ii,k}^{\beta+}+P_{jj,k}^{\beta+}\right)A^{\mathrm{T}}\Lambda_k^{\mathrm{T}}\right\} I \\
&= \beta_{ik}^2 W_k + \mathrm{tr}\left\{(1+\pi) A P_{ii,k}^{\beta+} A^{\mathrm{T}} + \beta_{ik}^2 G X_k G^{\mathrm{T}}\right. \\
&\quad \left. + 2\varepsilon^2 d_i\left(1+\pi^{-1}\right)\sum_{j\in\mathcal{N}_i} a_{ij}^2 A\left(P_{ii,k}^{\beta+}+P_{jj,k}^{\beta+}\right)A^{\mathrm{T}}\right\} I
\end{aligned} \tag{19}$$

综上，可得 $D_{ii,k+1}^{\beta-}$ 的上界为：

$$\begin{aligned}
P_{ii,k+1}^{\beta-} &\le \beta_{ik}^2 W_k + \mathrm{tr}\left\{(1+\pi) A P_{ii,k}^{\beta+} A^{\mathrm{T}} + 2\varepsilon^2 d_i\left(1+\pi^{-1}\right)\sum_{j\in\mathcal{N}_i} a_{ij}^2 A\left(P_{ii,k}^{\beta+}+P_{jj,k}^{\beta+}\right)A^{\mathrm{T}}\right\} I \\
&\quad + \mathrm{tr}\left\{\beta_{ik}^2 G\Psi_k G^{\mathrm{T}}\right\} I
\end{aligned} \tag{20}$$

最后根据[19]可得到分解后的一步预测协方差矩阵和误差协方差矩阵。 证毕■

定理2 假设分解误差动态(即私有误差动态(10)和公共误差动态(11))的私有和公共估计误差协方差 $P_{i,k}^{\alpha+}$ 和 $P_{i,k}^{\beta+}$ 的初值满足 $P_{i,0}^{\alpha+}=\Xi_{i,0}^{\alpha+}$ 和 $P_{i,0}^{\beta+}=\Xi_{i,0}^{\beta+}$，先验误差协方差 $P_{i,k}^{\alpha-}$ 和 $P_{i,k}^{\beta-}$ 的初值满足 $P_{i,0}^{\alpha-}=\Xi_{i,0}^{\alpha-}$ 和 $P_{i,0}^{\beta-}=\Xi_{i,0}^{\beta-}$。如果滤波增益取

$$K_{i,k}=\left(\Omega_{\Xi_{i,k}}\kappa_{x_{i,k}}^{-1}\Omega_{\Xi_{i,k}}^{\mathrm{T}}+C_i^{\mathrm{T}}\Omega_{V_{i,k}}C_{P_{i,k}}\kappa_{y_{i,k}}^{-1}\Omega_{V_{i,k}}^{\mathrm{T}}C_i\right)^{-1}C_i^{\mathrm{T}}\left(\Omega_{V_{i,k}}\kappa_{y_{i,k}}^{-1}\Omega_{V_{i,k}}^{\mathrm{T}}\right)^{-1}$$

那么，分布式隐私保护滤波器(4)的先验协方差矩阵和后验协方差矩阵的上界满足(14)，其中

$$\kappa_{x_{i,k}}=\mathrm{diag}\left\{\frac{v\lambda_k^2\mathrm{Y}_{v,\lambda_k}\left(\left[\eta_{x_{i,k}}\right]_1\right)}{v\lambda_k^2+\left[\eta_{x_{i,k}}\right]_1^2},\cdots,\frac{v\lambda_k^2\mathrm{Y}_{v,\lambda_k}\left(\left[\eta_{x_{i,k}}\right]_{n_x}\right)}{v\lambda_k^2+\left[\eta_{x_{i,k}}\right]_{n_x}^2}\right\},$$

$$\kappa_{y_{i,k}}=\mathrm{diag}\left\{\frac{v\lambda_k^2\mathrm{Y}_{v,\lambda_k}\left(\left[\eta_{y_{i,k}}\right]_1\right)}{v\lambda_k^2+\left[\eta_{y_{i,k}}\right]_1^2},\cdots,\frac{v\lambda_k^2\mathrm{Y}_{v,\lambda_k}\left(\left[\eta_{y_{i,k}}\right]_{n_y}\right)}{v\lambda_k^2+\left[\eta_{y_{i,k}}\right]_{n_y}^2}\right\},$$

证明： 令

$$\frac{\partial\mathcal{J}_{n_x+n_y}\left(\hat{x}_{i,k}^{+}\right)}{\partial\hat{x}_{i,k}^{+}}=0$$

可得

$$\begin{aligned}\frac{\partial \mathcal{J}_{n_x+n_y}\left(\hat{x}_{i,k}^{+}\right)}{\partial \hat{x}_{i,k}^{+}} &= \sum_{l=1}^{n_x} \frac{v\lambda_k^2}{v\lambda_k^2+\eta_{x_{i,k}}^2} \mathrm{Y}_{v,\sigma}\left(\left[\eta_{x_{i,k}}\right]_l\right)\left[\Omega_{P_{i,k}}^{-1}\right]_l^{\mathrm{T}}\left[\Omega_{P_{i,k}}^{-1}\right]_l\left(\hat{x}_{i,k}^{+}-\hat{x}_{i,k}^{-}\right) \\ &\quad -\sum_{l=1}^{n_y} \frac{v\lambda_k^2}{v\lambda_k^2+\eta_{y_{i,k}}^2} \mathrm{Y}_{v,\sigma}\left(\left[\eta_{y_{i,k}}\right]_l\right)\left[\Omega_{V_{i,k}}^{-1}\right]_l^{\mathrm{T}}\left[\Omega_{V_{i,k}}^{-1}\right]_l\left(y_{i,k}-C_i\hat{x}_{i,k}^{+}\right) \\ &= 0.\end{aligned}$$

上式可以化简为：

$$\Omega_{P_{i,k}}^{-\mathrm{T}}\kappa_{x_{i,k}}\Omega_{P_{i,k}}^{-1}\left(\hat{x}_{i,k}^{+}-\hat{x}_{i,k}^{-}\right)-\Omega_{V_{i,k}}^{-\mathrm{T}}\kappa_{y_{i,k}}\Omega_{V_{i,k}}^{-}\left(y_{i,k}-C_i\hat{x}_{i,k}^{+}\right)=0$$

移项可得 $\hat{x}_{i,k}^{+}=\hat{x}_{i,k}^{-}+K_{i,k}\left(y_{i,k}-C_i\hat{x}_{i,k}^{+}\right)$，其中

$$K_{i,k}=\left(\Omega_{P_{i,k}}\kappa_{x_{i,k}}^{-1}\Omega_{P_{i,k}}^{\mathrm{T}}+C_i^{\mathrm{T}}\Omega_{V_{i,k}}C_{P_{i,k}}\kappa_{y_{i,k}}^{-1}\Omega_{V_{i,k}}^{\mathrm{T}}C_i\right)^{-1}C_i^{\mathrm{T}}\left(\Omega_{V_{i,k}}\kappa_{y_{i,k}}^{-1}\Omega_{V_{i,k}}^{\mathrm{T}}\right)^{-1}$$

即对应的权重矩阵取作 $\Omega_{Pi,k}=\Omega_{\Xi i,k}$。因此，最优估计值 $\hat{x}_{i,k}^{+}$ 可以直接由下式得到

$$\hat{x}_{i,k}^{+}=\hat{x}_{i,k}^{-}+K_{i,k}\left(y_{i,k}-B_i\hat{x}_{i,k}^{-}\right).$$

由此可得该定理成立。

最后，本文设计的算法的具体实现步骤如下表 1 所示。

Table 1. Algorithm pseudocode
表 1. 算法伪代码

步骤 1	参数初始化。给定初始值 $x_0=\hat{x}_{i,0}^{+},\Xi_{i,0}^{+}=\Xi_{i,0}^{-}$ 令 $k=1$
步骤 2	收集 $y_{i,k}$；通过(5)和(14)计算 $\hat{x}_{i,k}^{-}$ 和 $\Xi_{ii,k}^{\alpha-}$，$\Xi_{ii,k}^{\beta-}$，$\Xi_{ii,k}^{-}$；通过对 $\Xi_{ii,k}^{-}$ 和 $V_{ii,k}$ 的 Cholesky 分解计算 $C_{\Xi_{ii,k}}$ 和 $C_{V_{i,k}}$；
步骤 3	记 $\left(\hat{x}_{i,k}^{+}\right)_t$ 为固定点迭代步骤 t 处的估计值，并令 $\left(\hat{x}_{i,k}^{+}\right)_0=\hat{x}_{i,k}^{-}$ 作为初始迭代值；
步骤 4	令 $t=0$；当 $\varpi>\varsigma^{*}$ 或 $t<t^{*}$ 时；更新迭代步骤 $t=t+1$； 1) 计算向量 $\left(\tilde{\eta}_{x_{i,k}}\right)_t=\Omega_{\Xi_{ii,k}}^{-1}\left(\left(\hat{x}_{i,k}^{+}\right)_{t-1}-\hat{x}_{i,k}^{-}\right)$，以及 $\left(\tilde{\eta}_{y_{i,k}}\right)_t=\Omega_{V_{i,k}}\left(y_{i,k}-C_i\left(\hat{x}_{i,k}^{+}\right)_{t-1}\right)$； 2) 计算矩阵 $\left(\tilde{\kappa}_{x_{i,k}}\right)_t$ 和 $\left(\tilde{\kappa}_{y_{i,k}}\right)_t$； 3) 计算矩阵 $\left(\tilde{\Xi}_{ii,k}^{-}\right)_t=\Omega_{\Xi_{i,k}}\left(\tilde{\kappa}_{x_{i,k}}\right)_t^{-1}\Omega_{\Xi_{i,k}}^{\mathrm{T}}$，$\left(\tilde{V}_{ii,k}\right)_t=\Omega_{V_{i,k}}\left(\tilde{\kappa}_{y_{i,k}}\right)_t^{-1}\Omega_{V_{i,k}}^{\mathrm{T}}$； 4) 计算滤波增益 $K_{i,k}$； 5) 使用以下公式更新估计值 $\left(\hat{x}_{i,k}^{+}\right)_t=\hat{x}_{i,k}^{-}+K_{i,k}\left(y_{i,k}-B_i\hat{x}_{i,k}^{-}\right)$； 6) 计算迭代精度 $\varpi=\dfrac{\left\|\left(\hat{x}_{i,k}^{+}\right)_t-\left(\hat{x}_{i,k}^{+}\right)_{t-1}\right\|}{\left\|\left(\hat{x}_{i,k}^{+}\right)_{t-1}\right\|}$；
步骤 5	记 $\hat{x}_{i,k}^{+}=\left(\hat{x}_{i,k}^{+}\right)_t$；通过(15)更新 $\Xi_{ii,k}^{\alpha+}$，$\Xi_{ii,k}^{\beta+}$ 和 $\Xi_{ii,k}^{+}$，结束算法。

3. 隐私性分析

由于状态分解策略对于外部窃听者来说是未知的，因此利用类似于定理 1 的方法，可得窃听端的先验误差协方差矩阵和后验协方差矩阵为：

$$\begin{cases} P_{ii,k+1,e}^{-} = \Lambda_k A P_{ii,k,e}^{+} A^{\mathrm{T}} \Lambda_k^{\mathrm{T}} + \Lambda_k G X_k G^{\mathrm{T}} \Lambda_k^{\mathrm{T}} + W_k - 2\varepsilon \sum_{j\in\mathcal{N}_i} a_{ij} \Lambda_k A \mathbb{E}\left\{ e_{i,k,e}^{+} \left(e_{j,k,e}^{+} - e_{i,k,e}^{+} \right)^{\mathrm{T}} \right\} A^{\mathrm{T}} \Lambda_k^{\mathrm{T}} \\ \qquad + \varepsilon^2 \sum_{j\in\mathcal{N}_i} \sum_{s\in\mathcal{N}_i} a_{ij} a_{is} \Lambda_k A \mathbb{E}\left\{ \left(e_{j,k,e}^{+} - e_{i,k,e}^{+} \right) \left(e_{s,k,e}^{+} - e_{i,k,e}^{+} \right)^{\mathrm{T}} \right\} A^{\mathrm{T}} \Lambda_k^{\mathrm{T}} \\ \qquad \le W_k + \mathrm{tr}\left\{ (1+\pi) A P_{ii,k,e}^{+} A^{\mathrm{T}} + 2\varepsilon^2 d_i \left(1+\pi^{-1} \right) \sum_{j\in\mathcal{N}_i} a_{ij}^2 A \left(P_{ii,k,e}^{+} + P_{jj,k,e}^{+} \right) A^{\mathrm{T}} \right\} I + \mathrm{tr}\left\{ G \Psi_{k,e} G^{\mathrm{T}} \right\} I, \\ P_{ii,k+1,e}^{+} = \left(I_n - K_{i,k+1} C_i \right) P_{ii,k+1,e}^{-} \left(I_n - K_{i,k+1} C_i \right)^{\mathrm{T}} + K_{i,k+1} V_{i,k+1} K_{i,k+1}^{\mathrm{T}} \end{cases} \tag{21}$$

对应的上界为：

$$\begin{cases} \Xi_{ii,k+1,e}^{-} = W_k + \mathrm{tr}\left\{ (1+\pi) A \Xi_{ii,k,e}^{+} A^{\mathrm{T}} + 2\varepsilon^2 d_i \left(1+\pi^{-1} \right) \sum_{j\in\mathcal{N}_i} a_{ij}^2 A \left(\Xi_{ii,k,e}^{+} + \Xi_{jj,k,e}^{+} \right) A^{\mathrm{T}} \right\} I + \mathrm{tr}\left\{ G \Psi_{k,e} G^{\mathrm{T}} \right\} I \\ \Xi_{ii,k+1,e}^{+} = \left(I - K_{i,k+1,e} C_{i,k+1} \right) \Xi_{ii,k+1,e}^{-} \left(I - K_{i,k+1} C_{i,k+1} \right)^{\mathrm{T}} + K_{i,k+1} V_{i,k+1} K_{i,k+1}^{\mathrm{T}}. \end{cases} \tag{22}$$

接下来，让我们比较窃听者的估计误差协方差与正常滤波器的误差协方差之间的关系。具体地，由(14)、(15)和(16)可得

$$\begin{aligned} \frac{\Xi_{i,k+1}^{\alpha+} + \Xi_{i,k+1}^{\beta+}}{1-2\alpha_{i,k+1}\beta_{i,k+1}} &= \frac{1-2\alpha_{i,k}\beta_{i,k}}{1-2\alpha_{i,k+1}\beta_{i,k+1}} \left(I - K_{i,k+1} C_{i,k+1} \right) \frac{\Xi_{ii,k+1}^{\alpha-} + \Xi_{ii,k+1}^{\beta-}}{1-2\alpha_{i,k}\beta_{i,k}} \left(I - K_{i,k+1} C_{i,k+1} \right)^{\mathrm{T}} \\ &\quad + \frac{\alpha_{ik}^2 + \beta_{ik}^2}{1-2\alpha_{i,k+1}\beta_{i,k+1}} K_{i,k+1} V_{i,k+1} K_{i,k+1}^{\mathrm{T}}, \end{aligned}$$

以及

$$\begin{aligned} \frac{\Xi_{i,k+1}^{\alpha-} + \Xi_{i,k+1}^{\beta-}}{1-2\alpha_{i,k+1}\beta_{i,k+1}} &= \frac{\alpha_{ik}^2 + \beta_{ik}^2}{1-2\alpha_{i,k+1}\beta_{i,k+1}} W_k + \frac{\alpha_{ik}^2 + \beta_{ik}^2}{1-2\alpha_{i,k+1}\beta_{i,k+1}} \mathrm{tr}\left\{ G \Psi_k G^{\mathrm{T}} \right\} I \\ &\quad + \frac{1-2\alpha_{i,k}\beta_{i,k}}{1-2\alpha_{i,k+1}\beta_{i,k+1}} \mathrm{tr}\left\{ (1+\pi) A \frac{\Xi_{ii,k}^{\alpha+} + \Xi_{ii,k}^{\beta+}}{1-2\alpha_{i,k}\beta_{i,k}} A^{\mathrm{T}} \right. \\ &\quad \left. + 2\varepsilon^2 d_i \left(1+\pi^{-1} \right) \sum_{j\in\mathcal{N}_i} a_{ij}^2 A \frac{\Xi_{ii,k}^{\alpha+} + \Xi_{jj,k}^{\alpha+} + \Xi_{ii,k}^{\beta+} + \Xi_{jj,k}^{\beta+}}{1-2\alpha_{i,k}\beta_{i,k}} A^{\mathrm{T}} \right\} I \\ &\quad - \frac{1-2\alpha_{i,k}\beta_{i,k}}{1-2\alpha_{i,k+1}\beta_{i,k+1}} \mathrm{tr}\left\{ \frac{\pi A \Xi_{ii,k}^{\alpha+} A^{\mathrm{T}}}{1-2\alpha_{i,k}\beta_{i,k}} + 2\varepsilon^2 d_i \pi^{-1} \sum_{j\in\mathcal{N}_i} a_{ij}^2 A \frac{\Xi_{ii,k}^{\alpha+} + \Xi_{jj,k}^{\alpha+}}{1-2\alpha_{i,k}\beta_{i,k}} A^{\mathrm{T}} \right\} I. \end{aligned}$$

鉴于状态分解的复杂性，文本只讨论一类特殊的分解规则的隐私性，即 $\alpha_{i,k+1} = \alpha_{ik}$ 且取 $\Psi_k = \Psi_{k,e} = \mathrm{tr}\left\{ \sum_{i=1}^{n_X} \gamma_i^2 I + W_k \right\}$。在这种情况下，我们不难有

$$\begin{cases}\Xi_{i,k+1}^{-}=W_k+\mathrm{tr}\left\{G\Psi_k G^{\mathrm{T}}\right\}I+\mathrm{tr}\left\{\left(1+\pi\right)A\Xi_{ii,k}^{+}A^{\mathrm{T}}+2\varepsilon^2 d_i\left(1+\pi^{-1}\right)\sum_{j\in\mathcal{N}_i}a_{ij}^2 A\left(\Xi_{ii,k}^{+}+\Xi_{jj,k}^{+}\right)A^{\mathrm{T}}\right\}I\\ \qquad -\mathrm{tr}\left\{\frac{\pi A\Xi_{ii,k}^{\alpha+}A^{\mathrm{T}}}{1-2\alpha_{i,k}\beta_{i,k}}+2\varepsilon^2 d_i\pi^{-1}\sum_{j\in\mathcal{N}_i}a_{ij}^2 A\frac{\Xi_{ii,k}^{\alpha+}+\Xi_{jj,k}^{\alpha+}}{1-2\alpha_{i,k}\beta_{i,k}}A^{T}\right\}I,\\ \Xi_{i,k+1}^{+}=\left(I-K_{i,k+1}C_{i,k+1}\right)\Xi_{ii,k+1}^{-}\left(I-K_{i,k+1}C_{i,k+1}\right)^{\mathrm{T}}+K_{i,k+1}V_{i,k+1}K_{i,k+1}^{\mathrm{T}}.\end{cases}\tag{23}$$

如果 $\Xi_{ii,0}^{+}=\Xi_{ii,0,e}^{+}$，对比(22)和(23)，不难有 $\Xi_{i,k+1}^{-}<\Xi_{ii,k+1,e}^{-}$。因此，窃听者估计的状态的有效性低于正常的滤波器。因此，系统的隐私性是可以满足的。对于更一般的状态分解情形，即 $\alpha_{i,k+1}\neq\alpha_{ik}$ 且取 $\Psi_k=\Psi_{k,e}=\mathrm{tr}\left\{\sum_{i=1}^{n_X}\gamma_i^2 I+W_k\right\}$ 时，如果分解策略使得

$$\theta_{ik}=\frac{\alpha_{ik}^2+\beta_{ik}^2}{1-2\alpha_{i,k+1}\beta_{i,k+1}}=\frac{1-2\alpha_{i,k}\beta_{i,k}}{1-2\alpha_{i,k+1}\beta_{i,k+1}}\geq 1,$$

那么

$$\begin{aligned}&\frac{\alpha_{ik}^2+\beta_{ik}^2}{1-2\alpha_{i,k+1}\beta_{i,k+1}}W_k+\frac{\alpha_{ik}^2+\beta_{ik}^2}{1-2\alpha_{i,k+1}\beta_{i,k+1}}\mathrm{tr}\left\{G\Psi_k G^{\mathrm{T}}\right\}I\\ &=W_k+\mathrm{tr}\left\{G\Psi_k G^{\mathrm{T}}\right\}I+\left(\theta_{ik}-1\right)\left(W_k+\mathrm{tr}\left\{G\Psi_k G^{\mathrm{T}}\right\}I\right)\end{aligned}$$

所采用的状态分解算法可能会降低系统的隐私性。反之，系统的隐私性的隐私性将被增强。因此，理想的分解策略应当满足 $\alpha_{i,k}\beta_{i,k}$ 是不增的。最后，不难发现矩阵 $\Xi_{ii,k+1}^{+}$ 反映了系统的估计性能，矩阵 $\Xi_{ii,k+1,e}^{+}$ 反映了系统的安全性能。因此，可以引入调节参数 $\varepsilon\in(0,1)$ 构建了一个综合估计和安全性能的复合指标 $\Xi_{ii,k+1}^{+}+\varepsilon\Xi_{ii,k+1,e}^{+}$。这时，$\varepsilon$ 可以被称作是风险水平。当 ε 接近于零时表明系统对隐私性的关注较小，这将会造成较大的安全风险。

4. 仿真实验

在本节中，通过仿真算例来验证所提出的具有状态分解的安全分布式估计算法的有效性。所采用的微电网包含两个分布式发电机组，其物理参数与文献[19]中的一致。此外，系统中部署了 4 个互联传感器，其中加权邻接矩阵为

$$\mathcal{H}=\begin{bmatrix}0 & 0.2 & 0 & 0.8\\ 0.2 & 0 & 0 & 0.3\\ 0 & 0 & 0 & 0.5\\ 0.8 & 0.3 & 0.5 & 0\end{bmatrix}$$

在不失一般性的情况下，所考虑的电力系统的初始状态平均值和设计的估计器分别选为 $x_0=\hat{x}_{i,0}^{+}=\left[1;3;1.5;1.6;2.2;1.3;1;1;1;1;1;1\right]^{\mathrm{T}}$，并且取 $P_{i,0}^{\alpha+}=P_{i,0}^{\beta+}=P_{i,0}^{+}=0.1I_{12}$，$G=0.1*randn(48,12)$ 为 Matlab 随机生成的矩阵，另外共识系数 $\varepsilon=0.1$，S-t 核函数中两个参数分别取做 $\lambda_k=0.5$，$\nu=4$，高斯核函数的参数取为 $\lambda_k=0.5$，其它参数设置为 $\pi=1.2$，$\rho=0.35$，$\varsigma^{*}=10^{-5}$，$\gamma_i=0.4$ 和 $t^{*}=10^{3}$。通过使用 Matlab 软件生成变量分解参数 α_{ik} 服从均匀分布 $U(0.35,0.55)$，四对随机序列 (α_{ik},β_{ik}) $(i=1,2,3,4)$ 的变化见图1，并且该序列无法被窃听者识别。

本文涉及的过程噪声和测量噪声是与[20]类似的高斯混合噪声：

$$\omega_k = p_1\mathrm{Rand}_{1\omega,k} + (1-p_1)\mathrm{Rand}_{2\omega,k},$$
$$\nu_{1,k} = p_1\mathrm{Rand}_{1\nu,1k} + (1-p_1)\mathrm{Rand}_{2\nu,1k},\ \nu_{2,k} = p_2\mathrm{Rand}_{1\nu,2k} + (1-p_2)\mathrm{Rand}_{2\nu,2k},$$
$$\nu_{3,k} = p_3\mathrm{Rand}_{1\nu,3k} + (1-p_3)\mathrm{Rand}_{2\nu,3k},\ \nu_{4,k} = p_4\mathrm{Rand}_{1\nu,4k} + (1-p_4)\mathrm{Rand}_{2\nu,4k}.$$

其中 $p_1 = 0.3, p_2 = 0.1, p_3 = 0.8, p_3 = 0.2$，并且上述随机变量满足以下分布：

$$\mathrm{Rand}_{1\omega,k} \sim \mathcal{N}(0.1, 0.05),\ \mathrm{Rand}_{2\omega,k} \sim \mathcal{N}(0.4, 0.09),$$
$$\mathrm{Rand}_{1\nu,ik} \sim \mathcal{N}(0.9, 0.03),\ \mathrm{Rand}_{1\nu,ik} \sim \mathcal{N}(0.6, 0.01).$$

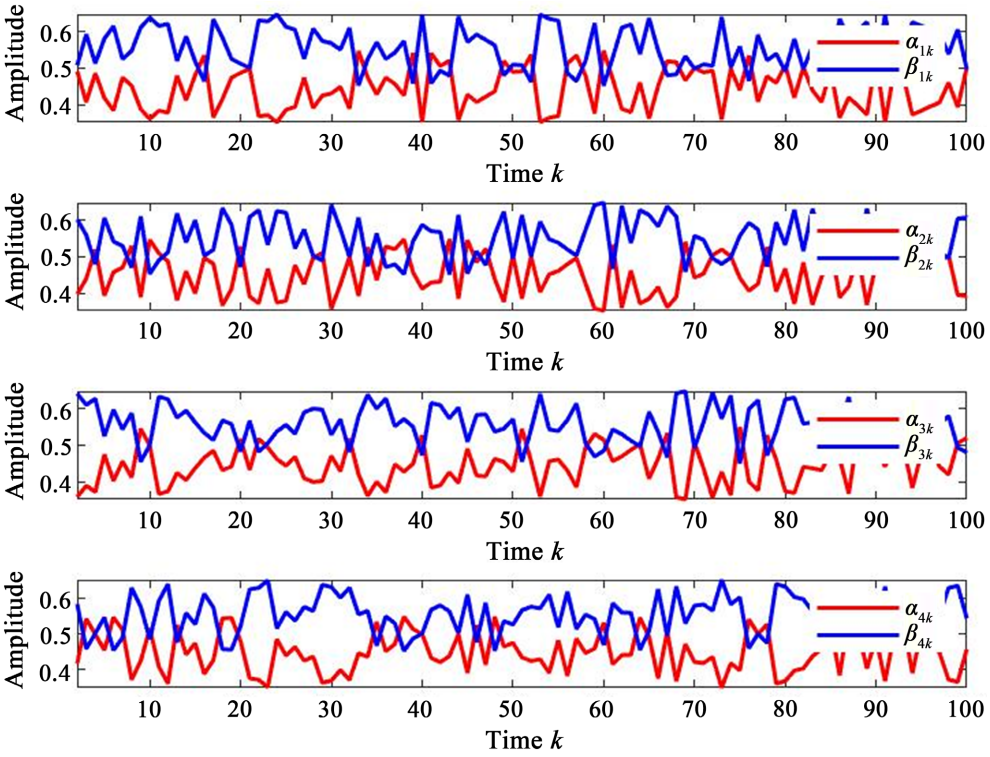


Figure 1. Decomposition coefficient
图 1. 分解系数

图 2 展示了系统在状态饱和时算法使用高斯核函数(红线)和 S-t 核函数(蓝线)估计系统状态的仿真结果，其中上标 i ($i \in 1,2,3,4$)表示状态向量的第 i 个分量。图 3 展示了基于两种核函数下的系统状态估计的均方误差(MSE)。在该图中，MSE 的定义为[21]：

$$MSE_k = \frac{1}{T}\sum_{t=1}^{T}\sum_{i=1}^{4}\left(x_k^i - \hat{x}_{k|k}^i\right)^2$$

其中，该式中 $T = 100$ 代表独立实验的数量。

图 2 和图 3 展示了使用 S-t 核函数的算法的估计精度要高于使用高斯核函数的算法的估计精度。另外，除了算法的估计精度外，我们还要对系统的安全性进行分析。为此，假设外部窃听者使用估计方案(5)，并且假设窃听者除了无法获得时变参数的分解参数外，其他所有参数(包括设计增益)都能够轻易获得。实验结果如图 4 所示，该图展示了窃听者在估计器 1 和 4 的状态估计过程中，与真实系统状态之间的差异。

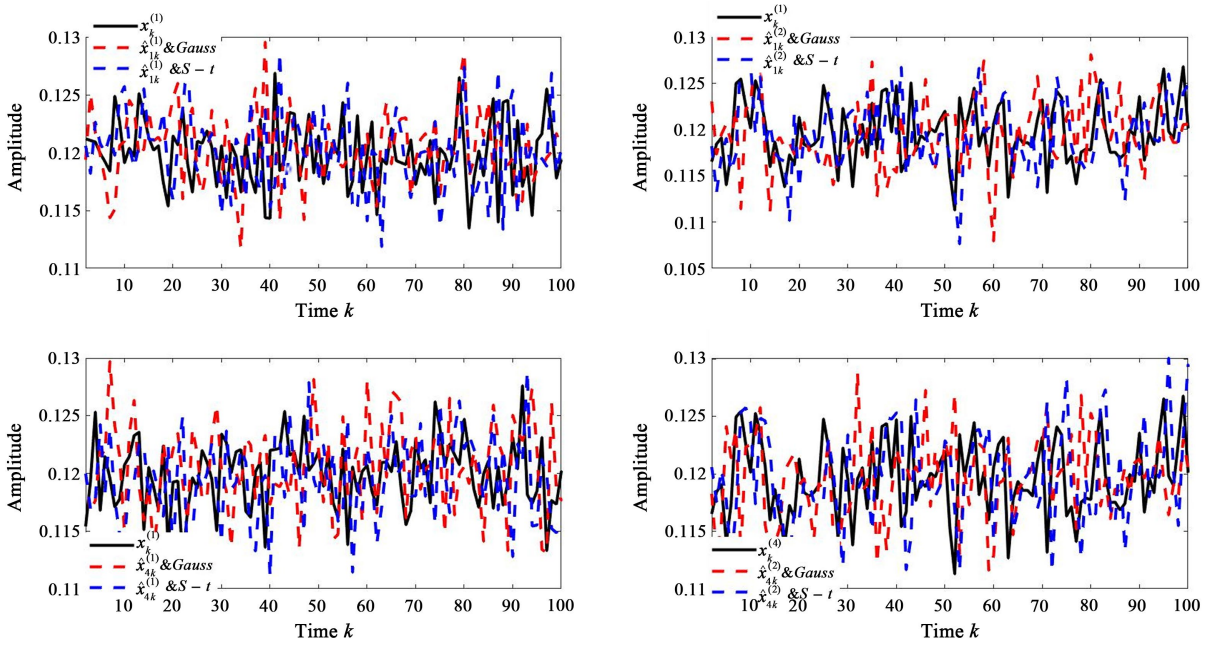


Figure 2. The estimation of the 1st and 4th components of the state variable by estimators 1 and 4
图 2. 估计器 1、4 对状态变量的第 1 个和第 4 个分量的估计

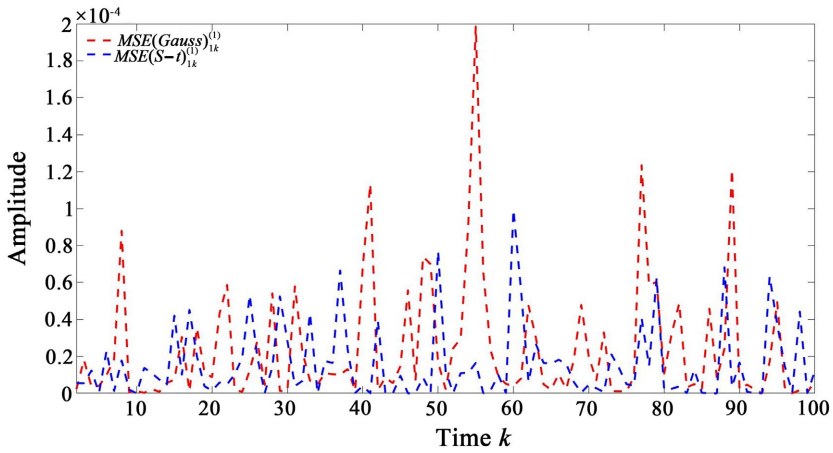
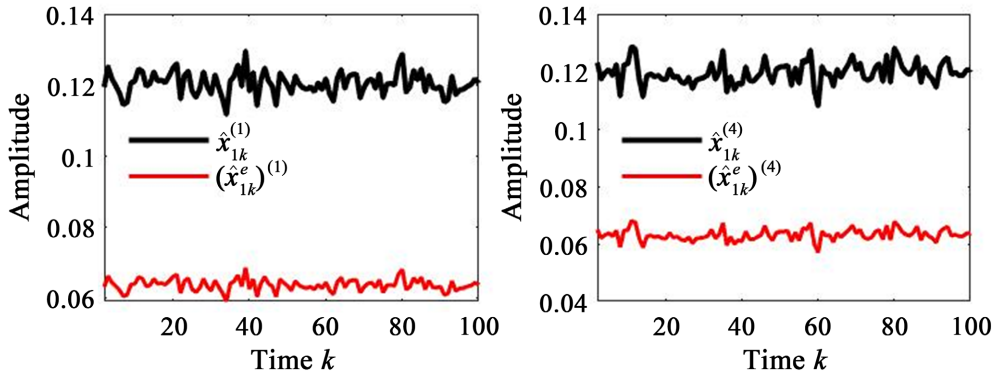


Figure 3. The MSE of the estimator 1 for the first component of the state variable using the Gaussian kernel function and the S-t kernel function
图 3. 估计器 1 对状态变量的第 1 个分量分别使用高斯核函数与 S-t 核函数的 MSE



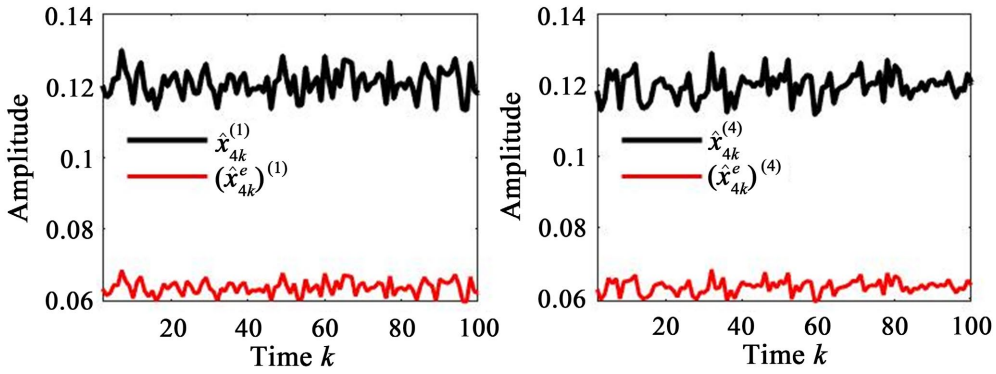


Figure 4. The estimation of the 1st and 4th components of the state variable by an external eavesdropper
图 4. 外部窃听者对状态变量的第 1 个和第 4 个分量的估计

5. 结语

基于状态饱和与状态变量分解，本文提出了一种新的以 S-t 核函数的分布式安全状态估计算法。本文根据状态分解规则系统地分析了私有估计误差协方差矩阵与公共估计误差协方差矩阵之间的关系。同时，利用新的 S-t 核函数构造区别于高斯核函数的代价函数进而构建了估计器的增益，以优化整个估计过程。状态变量分解的引入有效保障了数据传输的安全性，防止外部窃听者从中提取敏感信息。最终，结合系统状态饱和的特征利用 Matlab 进行仿真实验，验证了所提出算法在安全性和有效性方面的优越性能。

基金项目

国家自然科学基金(No. 62303322)；上海市教委创新基金(No. XJ2024111)资助。

参考文献

[1] Dunik, J., Biswas, S.K., Dempster, A.G., Pany, T. and Closas, P. (2020) State Estimation Methods in Navigation: Overview and Application. *IEEE Aerospace and Electronic Systems Magazine*, **35**, 16-31. https://doi.org/10.1109/maes.2020.3002001

[2] Huang, Y., Zhang, Y., Shi, P., Wu, Z., Qian, J. and Chambers, J.A. (2019) Robust Kalman Filters Based on Gaussian Scale Mixture Distributions with Application to Target Tracking. *IEEE Transactions on Systems*, *Man*, *and Cybernetics*: *Systems*, **49**, 2082-2096. https://doi.org/10.1109/tsmc.2017.2778269

[3] Deng, R., Xiao, G., Lu, R., Liang, H. and Vasilakos, A.V. (2017) False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: A Survey. *IEEE Transactions on Industrial Informatics*, **13**, 411-423. https://doi.org/10.1109/tii.2016.2614396

[4] 张云涵, 邓涛, 龚琦皓. 基于 LSTM-EKF 的无人机航迹追踪算法[J]. 导航定位学报, 2024, 12(6): 62-69.

[5] Liu, N., Zhang, K., Xie, X. and Yue, D. (2024) UKF-Based Optimal Tracking Control for Uncertain Dynamic Systems with Asymmetric Input Constraints. *IEEE Transactions on Cybernetics*, **54**, 7224-7235. https://doi.org/10.1109/tcyb.2024.3471987

[6] Arasaratnam, I., Haykin, S. and Elliott, R.J. (2007) Discrete-Time Nonlinear Filtering Algorithms Using Gauss-Hermite Quadrature. *Proceedings of the IEEE*, **95**, 953-977. https://doi.org/10.1109/jproc.2007.894705

[7] Chen, B., Liu, X., Zhao, H. and Principe, J.C. (2017) Maximum Correntropy Kalman Filter. *Automatica*, **76**, 70-77. https://doi.org/10.1016/j.automatica.2016.10.004

[8] Chang, L., Hu, B., Chang, G. and Li, A. (2012) Huber-Based Novel Robust Unscented Kalman Filter. *IET Science*, *Measurement & Technology*, **6**, 502-509. https://doi.org/10.1049/iet-smt.2011.0169

[9] Song, H., Ding, D., Dong, H. and Han, Q. (2022) Distributed Maximum Correntropy Filtering for Stochastic Nonlinear Systems under Deception Attacks. *IEEE Transactions on Cybernetics*, **52**, 3733-3744. https://doi.org/10.1109/tcyb.2020.3016093

[10] Chen, B., Zhu, Y., Hu, J. and Principe, J.C. (2013) System Parameter Identification: Information Criteria and Algorithms. Newnes, 51-55.

[11] Huang, Y., Zhang, Y., Li, N. and Chambers, J. (2016) Robust Student's T Based Nonlinear Filter and Smoother. *IEEE Transactions on Aerospace and Electronic Systems*, **52**, 2586-2596. https://doi.org/10.1109/taes.2016.150722

[12] Song, H., Ding, D., Dong, H. and Yi, X. (2022) Distributed Filtering Based on Cauchy-Kernel-Based Maximum Correntropy Subject to Randomly Occurring Cyber-Attacks. *Automatica*, **135**, Article ID: 110004. https://doi.org/10.1016/j.automatica.2021.110004

[13] Wang, H., Li, X., Bi, D., Xie, X. and Xie, Y. (2021) A Robust Student's *t*-Based Kernel Adaptive Filter. *IEEE Transactions on Circuits and Systems II*: *Express Briefs*, **68**, 3371-3375. https://doi.org/10.1109/tcsii.2021.3074643

[14] 罗贞. 基于卡尔曼滤波器的系统状态估计和故障检测[D]: [博士学位论文]. 武汉: 华中科技大学, 2013.

[15] Tran, H., Hu, J. and Pota, H.R. (2023) A Privacy-Preserving State Estimation Scheme for Smart Grids. *IEEE Transactions on Dependable and Secure Computing*, **20**, 3940-3956. https://doi.org/10.1109/tdsc.2022.3210017

[16] Zhou, J., Yang, W., Ding, W., Zheng, W.X. and Xu, Y. (2023) Watermarking-Based Protection Strategy against Stealthy Integrity Attack on Distributed State Estimation. *IEEE Transactions on Automatic Control*, **68**, 628-635. https://doi.org/10.1109/tac.2022.3171422

[17] Wen, C., Wang, Z., Liu, Q. and Alsaadi, F.E. (2018) Recursive Distributed Filtering for a Class of State-Saturated Systems with Fading Measurements and Quantization Effects. *IEEE Transactions on Systems*, *Man*, *and Cybernetics*: *Systems*, **48**, 930-941. https://doi.org/10.1109/tsmc.2016.2629464

[18] Shen, B., Wang, X. and Zou, L. (2023) Maximum Correntropy Kalman Filtering for Non-Gaussian Systems with State Saturations and Stochastic Nonlinearities. *IEEE*/*CAA Journal of Automatica Sinica*, **10**, 1223-1233. https://doi.org/10.1109/jas.2023.123195

[19] Zhao, P., Ding, D., Dong, H., Liu, H. and Yi, X. (2024) Secure Distributed State Estimation for Microgrids with Eavesdroppers Based on Variable Decomposition. *IEEE Transactions on Circuits and Systems I*: *Regular Papers*, **71**, 3307-3316. https://doi.org/10.1109/tcsi.2024.3357523

[20] Izanloo, R., Fakoorian, S.A., Yazdi, H.S. and Simon, D. (2016). Kalman Filtering Based on the Maximum Correntropy Criterion in the Presence of Non-Gaussian Noise. 2016 *Annual Conference on Information Science and Systems* (*CISS*), Princeton, 16-18 March 2016, 500-505. https://doi.org/10.1109/ciss.2016.7460553

[21] Theodor, Y. and Shaked, U. (1996) Robust Discrete-Time Minimum-Variance Filtering. *IEEE Transactions on Signal Processing*, **44**, 181-189. https://doi.org/10.1109/78.485915