

# 控制与决策

Control and Decision

复杂协同攻击下一类非线性系统的分布式一致性滤波器设计

高霞, 吴怀宇, 郑秀娟

引用本文:

高霞, 吴怀宇, 郑秀娟. 复杂协同攻击下一类非线性系统的分布式一致性滤波器设计[J]. *控制与决策*, 2024, 39(1): 189–195.

在线阅读 View online: <https://doi.org/10.13195/j.kzyjc.2022.0534>

---

## 您可能感兴趣的其他文章

### Articles you may be interested in

[分布式最小二乘估计中隐匿FDI攻击策略的设计](#)

Hidden FDI attack strategy for distributed least square estimation

*控制与决策*. 2021, 36(8): 1963–1969 <https://doi.org/10.13195/j.kzyjc.2019.1688>

[基于转换量测容积卡尔曼滤波器带多普勒量测的目标跟踪算法](#)

Converted measurement cubature Kalman filter for Doppler-assisted target tracking

*控制与决策*. 2021, 36(6): 1425–1434 <https://doi.org/10.13195/j.kzyjc.2019.1070>

[一种反向递推正弦干扰观测器的设计方法](#)

Design method of reverse recursive sinusoidal disturbance observer

*控制与决策*. 2021, 36(2): 403–410 <https://doi.org/10.13195/j.kzyjc.2019.0769>

[含有分数阶有色关联噪声的分数阶系统的卡尔曼滤波器设计](#)

Design of Kalman filter for fractional-order systems with correlated fractional-order colored noises

*控制与决策*. 2021, 36(7): 1672–1678 <https://doi.org/10.13195/j.kzyjc.2019.1418>

[事件触发机制下分布时滞网络化控制系统 \$H\_\infty\$ 故障检测](#)

Event-triggered  $H_\infty$  fault detection for networked control systems with distributed delays

*控制与决策*. 2020, 35(12): 3059–3065 <https://doi.org/10.13195/j.kzyjc.2019.0456>

# 复杂协同攻击下一类非线性系统的分布式一致性滤波器设计

高霞<sup>1,2</sup>, 吴怀宇<sup>1,2</sup>, 郑秀娟<sup>1,2†</sup>

(1. 武汉科技大学机器人与智能系统研究院, 武汉 430081;  
2. 武汉科技大学冶金自动化与检测技术教育部工程研究中心, 武汉 430081)

**摘要:** 针对复杂协同攻击下一类非线性系统的状态估计问题, 提出一种分布式一致性递推滤波算法. 首先, 将拒绝服务攻击 (denial of service, DoS) 和虚假数据注入攻击 (false data injection, FDI) 现象描述为两个随机 Bernoulli 序列, 并利用统一的框架建立包含 DoS 和 FDI 的复杂协同攻击模型; 然后, 基于一致性理论设计具有分布式结构的递推滤波器, 计算最优滤波器增益, 并推导该滤波器估计误差满足均方有界的充分必要条件; 最后, 利用室内机器人的定位问题进行验证, 仿真结果验证了所提出滤波器算法的有效性.

**关键词:** 一致性滤波器; 状态估计; FDI 攻击; DoS 攻击; 室内机器人定位

中图分类号: TP273 文献标志码: A

DOI: 10.13195/j.kzyjc.2022.0534

引用格式: 高霞, 吴怀宇, 郑秀娟. 复杂协同攻击下一类非线性系统的分布式一致性滤波器设计 [J]. 控制与决策, 2024, 39(1): 189-195.

## Distributed consensus filter design for a class of nonlinear systems under complex cooperative attacks

GAO Xia<sup>1,2</sup>, WU Huai-yu<sup>1,2</sup>, ZHENG Xiu-juan<sup>1,2†</sup>

(1. Institute of Robotics and Intelligent Systems, Wuhan University of Science and Technology, Wuhan 430081, China;  
2. Engineering Research Center for Metallurgical Automation and Measurement Technology of Ministry of Education, Wuhan University of Science and Technology, Wuhan 430081, China)

**Abstract:** Aiming at the state estimation problem of a class of nonlinear systems under complex cooperative attack, a distributed consensus-based recursive filtering algorithm is proposed. Firstly, the phenomena of denial of service (DoS) and false data injection (FDI) are described as two random Bernoulli sequences, and a complex cooperative attack model including DoS and FDI is established by using a unified framework. Then, a recursive filter with distributed structure is designed based on the consensus theory, the optimal filter gain is calculated, and the necessary and sufficient conditions for the estimation error of the filter to meet the mean square boundedness are derived. Finally, the indoor robot positioning problem is used to verify the effectiveness of the proposed filter algorithm

**Keywords:** consensus-based filtering; state estimation; FDI attack; DoS attack; indoor robot positioning

## 0 引言

近年来, 随着无线通信、传感和嵌入式系统技术的快速发展, 无线传感器网络 (wireless sensor networks, WSN) 在军事监测、智能交通、目标定位和跟踪等领域得到了广泛应用<sup>[1-2]</sup>. 由于网络环境的开放性, 特别是传感器、估计器与执行器之间存在的无线连接漏洞, 使得 WSN 容易受到恶意的网络攻击. 目前, 被广大研究人员关注的攻击行为主要包括: 拒绝

服务攻击 (denial-of-service attack, DoS)<sup>[3-4]</sup> 和虚假数据注入攻击 (false data injection, FDI)<sup>[5]</sup>.

恶意的网络攻击会严重影响网络系统的安全和估计性能. 为了提高估计的准确性, 一些学者研究了基于一致性的状态估计问题<sup>[6-7]</sup>, 其基本思想是 WSN 中各个节点均可与其邻居节点进行信息共享, 从而能够根据邻居节点提供的数据信息不断进行更新和校正. 对于 DoS 攻击, 文献 [8-9] 研究了 DoS 攻击下

收稿日期: 2022-04-02; 录用日期: 2022-09-03.

基金项目: 国家自然科学基金面上项目 (62073250); 武汉科技大学冶金自动化与检测技术教育部工程研究中心开放基金项目 (MADTOF2020B03).

责任编辑: 张维海.

†通讯作者. E-mail: zhengxj@wust.edu.cn.

\*本文附带电子附录文件, 可登录本刊官网该文“资源附件”区自行下载阅览.

多智能体系统一致性问题. 文献[10]提出了一个新的抵抗周期性DoS攻击的弹性事件触发一致性设计方法. 对于FDI攻击, 恶意攻击者通过将虚假数据注入通信信道, 达到破坏系统性能的目的. 为此, 文献[11]研究了基于一致性的分布式滤波的攻击检测问题. 文献[12]针对FDI攻击下的工业信息物理系统安全问题展开研究, 分析了FDI攻击对该系统稳定性的影响. 文献[13]研究了线性系统同时在未知输入和FDI攻击下的基于事件的分布式状态估计问题. 文献[14-15]提出了一种抵御FDI攻击的分布式一致性状态估计器.

随着攻击者智能化水平的不断提高, 网络攻击越来越智能化和复杂化, 出现了多种攻击方式组合的协同攻击. 例如: 文献[16]研究了WSN系统在恶意通信环境中的安全分布式一致性估计问题, 攻击者以随机发起的DoS攻击或FDI攻击破坏系统的安全性; 文献[17]考虑了传感器到滤波器信道上的数据传输中同时存在拒绝服务攻击、欺骗攻击和重放攻击的 $H_\infty$ 滤波问题; 文献[18]建立了一种基于欺骗攻击和拒绝服务攻击的新型网络化控制系统模型; 文献[19]研究了在虚假数据注入攻击和拥塞攻击下, WSN系统的攻击检测与集中式状态估计问题. 值得注意的是, 现有的研究大多针对集中式状态估计, 且只考虑单一的网络攻击, 针对复杂攻击的分布式状态估计研究较少. 由于分布式网络节点之间存在信息交换过程, 恶意攻击者可以在相邻节点的通信信道上发起复杂网络攻击, 恶意修改系统状态, 阻断相邻节点之间的无线传输信道. 因此, 研究复杂协同攻击下非线性系统的分布式状态估计问题具有重要的理论意义和工程应用价值.

鉴于此, 本文设计一种分布式一致性滤波器, 即使在受到复杂协同攻击的情况下, 仍然能够有效地估计系统状态. 主要贡献如下: 1) 综合考虑DoS和FDI的协同攻击行为对系统性能的影响, 采用统一的框架模型进行描述; 2) 基于一致性理论构造具有分布式结构的递推滤波器, 设计最优滤波器增益, 实现复杂协同攻击下的系统状态估计, 并克服设计过程中的线性化误差问题; 3) 利用Lyapunov稳定性理论证明该滤波器估计误差的均方有界性.

## 1 问题描述

WSN的通信拓扑图可定义为无向图 $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ . 其中:  $\mathcal{V} = \{1, 2, \dots, N\}$ 表示传感器节点的集合,  $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$ 表示边缘. 相连的边 $(i, j)$ 表示节点 $i$ 与 $j$ 之间可以相互通信, 与节点 $i$ 相连的节点集合 $\mathcal{N}_i =$

$\{j | (i, j) \in \mathcal{E}\}$ 称为节点的邻居节点集. 节点 $i$ 的邻居节点个数表示为 $d_i = |\mathcal{N}_i|$ , 并称其为度.

考虑以下具有 $n$ 个传感器的离散时间非线性系统:

$$x_{k+1} = f(x_k) + \omega_k, \quad (1)$$

$$z_{i,k} = h_i(x_k) + v_{i,k}. \quad (2)$$

其中:  $x_k \in \mathbf{R}^{n_x}$ 为系统状态向量,  $z_{i,k} \in \mathbf{R}^{n_z}$ 为第 $i$ 个传感器在 $k$ 时刻的测量向量,  $\omega_k \in \mathbf{R}^{n_\omega}$ 为过程噪声,  $v_{i,k} \in \mathbf{R}^{n_\nu}$ 为第 $i$ 个传感器测量噪声. 假设 $\omega_k$ 和 $v_{i,k}$ 为互不相关的零均值高斯白噪声, 其协方差分别为 $Q_k$ 和 $R_{i,k}$ , 且不同时刻不同传感器之间的测量噪声互不相关,  $f(\cdot)$ 和 $h_i(\cdot)$ 为已知的连续两次可微的非线性函数.

WSN未受到网络攻击时, 基于一致性理论, 对于第 $i$ 个传感器节点, 构建具有如下结构的递推滤波器进行状态估计:

$$\hat{x}_{i,k+1|k} = f(\hat{x}_{i,k|k}), \quad (3)$$

$$\hat{x}_{i,k+1|k+1} =$$

$$\hat{x}_{i,k+1|k} + K_{i,k+1}[z_{i,k+1} - h_i(\hat{x}_{i,k+1|k})] +$$

$$C_{i,k+1} \sum_{j \in \mathcal{N}_i} (\hat{x}_{j,k+1|k} - \hat{x}_{i,k+1|k}). \quad (4)$$

其中:  $\hat{x}_{i,k+1|k}$ 为 $k$ 时刻状态的一步预测值,  $\hat{x}_{i,k+1|k+1}$ 为 $k+1$ 时刻状态的估计值,  $\hat{x}_{j,k+1|k}$  ( $j \in \mathcal{N}_i$ )为除节点 $i$ 外其他节点的一步状态预测值,  $K_{i,k+1}$ 为第 $i$ 个传感器在 $k+1$ 时刻的滤波器增益矩阵,  $C_{i,k+1}$ 为第 $i$ 个传感器在 $k+1$ 时刻的一致性增益矩阵.

考虑到攻击者可以在相邻节点之间的无线通信信道随机发起两种网络攻击, 即DoS攻击和FDI攻击, 当攻击者在无线通信信道发起FDI攻击时, 节点 $i$ 从其相邻节点 $j$ 接收的数据包描述为

$$D_{j,k} = \hat{x}_{j,k|k-1} + \gamma_{ij,k} \xi_k. \quad (5)$$

其中:  $\hat{x}_{j,k|k-1}$ 为邻居节点 $j$ 在 $k-1$ 时刻的状态预测值;  $\gamma_{ij,k}$ 为服从伯努利分布的二元随机变量, 用来描述FDI攻击,  $\gamma_{ij,k} = 1$ 表示攻击者成功在通信信道 $j \rightarrow i$ 发起FDI攻击, 且 $\Pr\{\gamma_{ij,k} = 1\} = \bar{\gamma}_{ij,k}$ ,  $\gamma_{ij,k} = 0$ 表示未发起攻击行为;  $\xi_k \in \mathbf{R}^n$ 为攻击者传递的虚假数据, 且满足 $\|\xi_k\| \leq \delta$ ,  $\delta$ 为已知的正标量<sup>[13]</sup>.

同样, 用一个服从伯努利分布的二元随机变量 $\phi_{ij,k} \in \{0, 1\}$ 表示DoS攻击过程<sup>[16]</sup>, 如果 $\phi_{ij,k} = 1$ , 则表示攻击者成功在信道 $j \rightarrow i$ 发起DoS攻击, 且 $\Pr\{\phi_{ij,k} = 1\} = \bar{\phi}_{ij,k}$ ; 否则认为攻击者未发起DoS攻击行为. 假设在同一时刻, 攻击者只能发起一种类型的攻击, 即 $\Pr\{\phi_{ij,k} \gamma_{ij,k} = 1\} = 0$ , 此外,  $\phi_{ij,k}$ 独立于

$\phi_{rs,t}, \gamma_{ij,k}$  独立于  $\gamma_{rs,t}$ . 其中:  $(i, j) \neq (r, s), k \neq t$ .

由式(5)和复杂的攻击行为分析可知,传感器  $i$  从传感器  $j(j \in \mathcal{N}_i)$  实际接收的数据包可以表示为

$$D_{j,k}^* = (1 - \phi_{ij,k})(\hat{x}_{j,k|k-1} + \gamma_{ij,k}\xi_k). \quad (6)$$

**注1** 根据文献[20],由于攻击者的能量有限,攻击者需要在能量耗尽之前停止攻击,并且在攻击结束后存储能量,为下一次攻击做好准备,存储能量的多少取决于下一次攻击的时间长度与发动攻击的规模大小.考虑到由于攻击者的一些攻击可以被防护设备截获,使用服从伯努利分布的二进制变量描述随机发生的攻击现象.

在实际系统中,通常采用检测器提高系统的安全性,本文考虑检测器能够正确检测到系统是否遭受攻击.基于上述分析,当WSN受到网络攻击时,构造递推滤波器

$$\begin{aligned} \hat{x}_{i,k+1|k+1} = & \hat{x}_{i,k+1|k} + K_{i,k+1}[z_{i,k+1} - h_i(\hat{x}_{i,k+1|k})] + \\ & C_{i,k+1} \sum_{j \in \mathcal{N}_i} (1 - \phi_{ij,k+1})(\hat{x}_{j,k+1|k} + \\ & \gamma_{ij,k+1}\xi_{k+1} - \hat{x}_{i,k+1|k}). \end{aligned} \quad (7)$$

为分析方便,定义第  $i$  个节点的一步预测误差、滤波误差及相应的协方差分别为

$$e_{i,k+1|k} = x_{k+1} - \hat{x}_{i,k+1|k}, \quad (8)$$

$$e_{i,k+1|k+1} = x_{k+1} - \hat{x}_{i,k+1|k+1}, \quad (9)$$

$$P_{i,k+1|k} = E\{e_{i,k+1|k}e_{i,k+1|k}^T\}, \quad (10)$$

$$P_{i,k+1|k+1} = E\{e_{i,k+1|k+1}e_{i,k+1|k+1}^T\}. \quad (11)$$

## 2 滤波器设计

为了方便分析,首先给出如下引理.

**引理1**<sup>[2]</sup> 给定适当维数的矩阵  $A, B, C, D$ , 有  $CC^T \leq I$ , 设  $G$  为对称正定矩阵,  $a > 0$  为任意正常数, 若  $a^{-1}I - DGD^T > 0$ , 则以下矩阵不等式成立:

$$\begin{aligned} (A + BCD)G(A + BCD)^T \leq \\ A(G^{-1} - aD^T D)^{-1}A^T + a^{-1}BB^T. \end{aligned} \quad (12)$$

**引理2**<sup>[16]</sup> 假设  $A = A^T > 0$ , 两个矩阵函数序列  $\psi_k(\cdot)$  和  $\Gamma_k(\cdot)$ , 对于任意  $0 \leq k \leq n$ , 使得

$$\psi_k(A) = \psi_k(A^T), \quad \Gamma_k(A) = \Gamma_k(A^T). \quad (13)$$

如果矩阵  $B = B^T > A$  成立, 则可得出如下结论:

$$\psi_k(B) \geq \psi_k(A), \quad \Gamma_k(B) \geq \Gamma_k(A). \quad (14)$$

如下差分方程的解  $X_k$  和  $Y_k$ :

$$X_k = \psi_k(X_{k-1}), \quad Y_k = \Gamma_k(Y_{k-1}), \quad X_0 = Y_0 \quad (15)$$

满足  $X_k \leq Y_k$ .

**引理3**<sup>[16]</sup> 对于任意给定的  $x, y \in \mathbf{R}^n$ , 以下不

等式成立:

$$x^T y + xy^T \leq xx^T + yy^T. \quad (16)$$

从式(1)中减去(3)可以得到第  $i$  个滤波器的一步预测误差为

$$\begin{aligned} e_{i,k+1|k} = x_{k+1} - \hat{x}_{i,k+1|k} = \\ f(x_k) + \omega_k - f(\hat{x}_{i,k|k}). \end{aligned} \quad (17)$$

将非线性函数  $f(x_k)$  在点  $\hat{x}_{i,k|k}$  处用泰勒级数展开, 可得

$$f(x_k) = f(\hat{x}_{i,k|k}) + F_{i,k}e_{i,k|k} + o(|e_{i,k|k}|), \quad (18)$$

其中  $F_{i,k} = \partial f(x)/\partial x|_{x=\hat{x}_{i,k|k}}$ . 高阶项可以表示为

$$o(|e_{i,k|k}|) = U_{i,k}\Omega_{i,k}e_{i,k|k}. \quad (19)$$

其中:  $U_{i,k}$  为一个已知的标度矩阵,  $\Omega_{i,k}$  为未知的时变矩阵, 满足  $\Omega_{i,k}\Omega_{i,k}^T \leq I$ , 矩阵  $U_{i,k}$ 、 $\Omega_{i,k}$  用来描述线性化误差. 由式(17)~(19)可以得到

$$e_{i,k+1|k} = (F_{i,k} + U_{i,k}\Omega_{i,k})e_{i,k|k} + \omega_k. \quad (20)$$

预测误差的协方差矩阵可以表示为

$$\begin{aligned} P_{i,k+1|k} = E\{e_{i,k+1|k}e_{i,k+1|k}^T\} = \\ (F_{i,k} + U_{i,k}\Omega_{i,k})P_{i,k|k}(F_{i,k} + U_{i,k}\Omega_{i,k})^T + Q_k. \end{aligned} \quad (21)$$

类似地, 将式(7)代入(8), 得到更新的估计误差为

$$\begin{aligned} e_{i,k+1|k+1} = x_{k+1} - \hat{x}_{i,k+1|k+1} = \\ e_{i,k+1|k} - K_{i,k+1}(H_{i,k+1} + V_{i,k+1} \times \\ \Theta_{i,k+1})e_{i,k+1|k} - K_{i,k+1}v_{i,k+1} - \\ C_{i,k+1} \sum_{j \in \mathcal{N}_i} (1 - \phi_{ij,k+1})(\hat{x}_{j,k+1|k} + \\ \gamma_{ij,k+1}\xi_{k+1} - \hat{x}_{i,k+1|k}) = \\ \mathcal{A}_{i,k+1}e_{i,k+1|k} - K_{i,k+1}v_{i,k+1} + \\ C_{i,k+1} \sum_{j \in \mathcal{N}_i} (1 - \phi_{ij,k+1})e_{j,k+1|k} - \\ C_{i,k+1} \sum_{j \in \mathcal{N}_i} \gamma_{ij,k+1}\xi_{k+1}. \end{aligned} \quad (22)$$

其中

$$\begin{aligned} H_{i,k+1} = \partial h(x)/\partial x|_{x=\hat{x}_{i,k+1|k}}, \\ \mathcal{A}_{i,k+1} = I - C_{i,k+1} \sum_{j \in \mathcal{N}_i} (1 - \phi_{ij,k+1}) - \\ K_{i,k+1}H_{i,k+1} - K_{i,k+1}V_{i,k+1}\Theta_{i,k+1}, \end{aligned} \quad (23)$$

$V_{i,k+1}$  为一个已知的标度矩阵,  $\Theta_{i,k+1}$  为一个未知时变矩阵, 满足  $\Theta_{i,k+1}\Theta_{i,k+1}^T \leq I$ . 则更新的估计误差协方差矩阵可以表示为

$$\begin{aligned} P_{i,k+1|k+1} = \\ \mathcal{A}_{i,k+1}P_{i,k+1|k}\mathcal{A}_{i,k+1}^T + \end{aligned}$$

$$\begin{aligned} & \sum_{j \in \mathcal{N}_i} E\{\mathcal{A}_{i,k+1} e_{i,k+1|k} e_{j,k+1|k}^T (1 - \phi_{ij,k+1})^T \times \\ & C_{i,k+1}^T + (1 - \phi_{ij,k+1}) C_{i,k+1} e_{j,k+1|k} e_{i,k+1|k}^T \times \\ & \mathcal{A}_{i,k+1}^T\} + \sum_{j \in \mathcal{N}_i} C_{i,k+1} (1 - \bar{\phi}_{ij,k+1}) P_{j,k+1|k} \times \\ & C_{i,k+1}^T - \sum_{j \in \mathcal{N}_i} E\{\mathcal{A}_{i,k+1} e_{i,k+1|k} \xi_{k+1}^T \gamma_{ij,k+1}^T \times \\ & C_{i,k+1}^T + \gamma_{ij,k+1} C_{i,k+1} \xi_{k+1} e_{i,k+1|k}^T \mathcal{A}_{i,k+1}^T\} + \\ & \sum_{j \in \mathcal{N}_i} \sum_{l \in \mathcal{N}_i} E\{C_{i,k+1} \gamma_{ij,k+1} \xi_{k+1} \xi_{k+1}^T \gamma_{il,k+1}^T C_{i,k+1}^T\} - \\ & \sum_{j \in \mathcal{N}_i} \sum_{l \in \mathcal{N}_i} E\{C_{i,k+1} (1 - \phi_{ij,k+1}) e_{j,k+1|k} \xi_{k+1}^T \times \\ & \gamma_{il,k+1}^T C_{i,k+1}^T + \gamma_{ij,k+1} C_{i,k+1} \xi_{k+1} e_{l,k+1|k}^T \times \\ & (1 - \phi_{il,k+1})^T C_{i,k+1}^T\} + K_{i,k+1} R_{i,k+1} K_{i,k+1}. \quad (24) \end{aligned}$$

**注2** 由式(21)和(24)可以看出,由于线性化误差引入未知矩阵  $\Omega_{i,k}$  和  $\Theta_{i,k+1}$ ,不能直接计算出协方差矩阵的值.一种方法是求出  $P_{i,k+1|k}$  和  $P_{i,k+1|k+1}$  的上界矩阵,然后确定滤波增益矩阵  $K_{i,k+1}$ .

本文的设计目标是求出滤波误差协方差矩阵的一个上界矩阵,即

$$P_{i,k+1|k+1} \leq \Phi_{i,k+1|k+1}. \quad (25)$$

并且通过设计合适的滤波增益矩阵  $K_{i,k+1}$ ,使得每个时刻上界矩阵  $\Phi_{i,k+1|k+1}$  的迹最小.

**定理1** 由式(1)和(2)描述的离散时间非线性系统,设  $\sigma_{i,k}$ 、 $\beta_{i,k}$  为正标量,  $\varepsilon$  为满足不等式  $0 < \varepsilon < 1/d_{\max}$  的正标量,其中  $d_{\max} = \max_{1 \leq i \leq N} \{d_i\}$ .如果如下两个类黎卡提差分方程:

$$\begin{aligned} \Phi_{i,k+1|k} &= F_{i,k} [\Phi_{i,k|k}^{-1} - (1 + \varepsilon) \sigma_{i,k} I]^{-1} F_{i,k}^T + \\ & \varepsilon^{-1} \sigma_{i,k}^{-1} U_{i,k} U_{i,k}^T + Q_k, \quad (26) \end{aligned}$$

$$\begin{aligned} \Phi_{i,k+1|k+1} &= \\ & (1 + 2d_i) \left[ I - C_{i,k+1} \sum_{j \in \mathcal{N}_i} (1 - \phi_{ij,k+1}) - \right. \\ & \left. K_{i,k+1} H_{i,k+1} \right] (\Phi_{i,k+1|k}^{-1} - \beta_{i,k} I)^{-1} \left[ I - C_{i,k+1} \times \right. \\ & \left. \sum_{j \in \mathcal{N}_i} (1 - \phi_{ij,k+1}) - K_{i,k+1} H_{i,k+1} \right]^T + \\ & \sum_{j \in \mathcal{N}_i} 3(1 - \bar{\phi}_{ij,k+1}) C_{i,k+1} \Phi_{j,k+1|k} C_{i,k+1}^T + \\ & \sum_{j \in \mathcal{N}_i} 3\delta^2 \bar{\gamma}_{ij,k+1} C_{i,k+1} C_{i,k+1}^T + K_{i,k+1} \times \\ & [(1 + 2d_i) \beta_{i,k}^{-1} V_{i,k+1} V_{i,k+1}^T + R_{i,k+1}] K_{i,k+1}^T \quad (27) \end{aligned}$$

在初始条件  $P_{0|0} \leq \Phi_{0|0}$  下,有正定的解  $\Phi_{i,k+1|k}$  和  $\Phi_{i,k+1|k+1}$ ,并且使得如下不等式:

$$\Phi_{i,k|k}^{-1} > (1 + \varepsilon) \sigma_{i,k} I, \quad (28)$$

$$\Phi_{i,k+1|k}^{-1} > \beta_{i,k} I \quad (29)$$

对于所有的  $k \geq 0$  均成立,则矩阵  $\Phi_{i,k+1|k+1}$  是  $P_{i,k+1|k+1}$  的上界,且最优滤波增益矩阵为

$$\begin{aligned} K_{i,k+1} &= \\ & \left[ I - C_{i,k+1} \sum_{j \in \mathcal{N}_i} (1 - \phi_{ij,k+1}) \right] (\Phi_{i,k+1|k}^{-1} - \beta_{i,k} I)^{-1} \times \\ & H_{i,k+1}^T \left[ H_{i,k+1} (\Phi_{i,k+1|k}^{-1} - \beta_{i,k} I)^{-1} H_{i,k+1}^T + \right. \\ & \left. \beta_{i,k}^{-1} V_{i,k+1} V_{i,k+1}^T + \frac{1}{1 + 2d_i} R_{i,k+1} \right]^{-1}. \quad (30) \end{aligned}$$

**证明** 由引理1和式(21),如下不等式成立:

$$\begin{aligned} P_{i,k+1|k} &= \\ & (F_{i,k} + U_{i,k} \Omega_{i,k}) P_{i,k|k} (F_{i,k} + U_{i,k} \Omega_{i,k})^T + Q_k \leq \\ & F_{i,k} [P_{i,k|k}^{-1} - (1 + \varepsilon) \sigma_{i,k} I]^{-1} F_{i,k}^T + \\ & (1 + \varepsilon)^{-1} \sigma_{i,k}^{-1} U_{i,k} U_{i,k}^T + Q_k \leq \\ & F_{i,k} [P_{i,k|k}^{-1} - (1 + \varepsilon) \sigma_{i,k} I]^{-1} F_{i,k}^T + \\ & \varepsilon^{-1} \sigma_{i,k}^{-1} U_{i,k} U_{i,k}^T + Q_k. \quad (31) \end{aligned}$$

同理,将引理1运用于式(24)右侧的第1项,有

$$\begin{aligned} \mathcal{A}_{i,k+1} P_{i,k+1|k} \mathcal{A}_{i,k+1}^T &\leq \\ & \left[ I - C_{i,k+1} \sum_{j \in \mathcal{N}_i} (1 - \phi_{ij,k+1}) - K_{i,k+1} H_{i,k+1} \right] \times \\ & (P_{i,k+1|k}^{-1} - \beta_{i,k} I)^{-1} \left[ I - C_{i,k+1} \times \right. \\ & \left. \sum_{j \in \mathcal{N}_i} (1 - \phi_{ij,k+1}) - K_{i,k+1} H_{i,k+1} \right]^T + \\ & \beta_{i,k}^{-1} K_{i,k+1} V_{i,k+1} V_{i,k+1}^T K_{i,k+1}^T. \quad (32) \end{aligned}$$

利用引理3可以得到式(24)右侧第2、4、6项满足如下不等式:

$$\begin{aligned} & \sum_{j \in \mathcal{N}_i} E\{\mathcal{A}_{i,k+1} e_{i,k+1|k} e_{j,k+1|k}^T (1 - \phi_{ij,k+1})^T C_{i,k+1}^T + \\ & C_{i,k+1} (1 - \phi_{ij,k+1}) e_{j,k+1|k} e_{i,k+1|k+1}^T \mathcal{A}_{i,k+1}^T\} \leq \\ & \sum_{j \in \mathcal{N}_i} E\{\mathcal{A}_{i,k+1} e_{i,k+1|k} e_{i,k+1|k}^T \mathcal{A}_{i,k+1}^T + \\ & C_{i,k+1} (1 - \phi_{ij,k+1}) e_{j,k+1|k} e_{j,k+1|k}^T \times \\ & (1 - \phi_{ij,k+1})^T C_{i,k+1}^T\} = \\ & \sum_{j \in \mathcal{N}_i} (1 - \bar{\phi}_{ij,k+1}) C_{i,k+1} P_{j,k+1|k} C_{i,k+1}^T + \\ & d_i \mathcal{A}_{i,k+1} P_{i,k+1|k} \mathcal{A}_{i,k+1}^T, \quad (33) \end{aligned}$$

$$\begin{aligned} & \sum_{j \in \mathcal{N}_i} E\{-\mathcal{A}_{i,k+1} e_{i,k+1|k} \xi_{k+1}^T \gamma_{ij,k+1}^T C_{i,k+1}^T - \\ & C_{i,k+1} \gamma_{ij,k+1} \xi_{k+1} e_{i,k+1|k}^T \mathcal{A}_{i,k+1}^T\} \leq \\ & \sum_{j \in \mathcal{N}_i} E\{\mathcal{A}_{i,k+1} e_{i,k+1|k} e_{i,k+1|k}^T \mathcal{A}_{i,k+1}^T + \\ & C_{i,k+1} \gamma_{ij,k+1} \xi_{k+1} \xi_{k+1}^T \gamma_{ij,k+1}^T C_{i,k+1}^T\} = \end{aligned}$$

$$\begin{aligned}
& \sum_{j \in \mathcal{N}_i} \bar{\gamma}_{ij,k+1} \delta^2 C_{i,k+1} C_{i,k+1}^T + \\
& d_i \mathcal{A}_{i,k+1} P_{i,k+1|k} \mathcal{A}_{i,k+1}^T, \quad (34) \\
& \sum_{j \in \mathcal{N}_i} \sum_{l \in \mathcal{N}_i} E \{ -C_{i,k+1} (1 - \phi_{ij,k+1}) e_{j,k+1|k} \xi_{k+1}^T \times \\
& \gamma_{il,k+1} C_{i,k+1}^T - C_{i,k+1} \gamma_{ij,k+1} \xi_{k+1} e_{l,k+1|k}^T \times \\
& (1 - \phi_{il,k+1})^T C_{i,k+1}^T \} \leq \\
& \sum_{j \in \mathcal{N}_i} \sum_{l \in \mathcal{N}_i} E \{ C_{i,k+1} (1 - \phi_{ij,k+1}) e_{j,k+1|k} e_{l,k+1|k}^T \times \\
& (1 - \phi_{il,k+1})^T C_{i,k+1}^T + C_{i,k+1} \gamma_{il,k+1} \xi_{k+1} \xi_{k+1}^T \times \\
& \gamma_{ij,k+1} C_{i,k+1}^T \} = \\
& \sum_{j \in \mathcal{N}_i} (1 - \bar{\phi}_{ij,k+1}) C_{i,k+1} P_{j,k+1|k} C_{i,k+1}^T + \\
& \sum_{j \in \mathcal{N}_i} \bar{\gamma}_{ij,k+1} \delta^2 C_{i,k+1} C_{i,k+1}^T. \quad (35)
\end{aligned}$$

对于式(24)右侧的第5项,有

$$\begin{aligned}
& \sum_{j \in \mathcal{N}_i} \sum_{l \in \mathcal{N}_i} E \{ C_{i,k+1} \gamma_{ij,k+1} \xi_{k+1} \xi_{k+1}^T \gamma_{il,k+1}^T C_{i,k+1}^T \} \leq \\
& \sum_{j \in \mathcal{N}_i} \bar{\gamma}_{ij,k+1} \delta^2 C_{i,k+1} C_{i,k+1}^T. \quad (36)
\end{aligned}$$

将式(32)~(36)代入(24),得到

$$\begin{aligned}
& P_{i,k+1|k+1} \leq \\
& (1+2d_i) \left[ I - C_{i,k+1} \sum_{j \in \mathcal{N}_i} (1 - \phi_{ij,k+1}) - K_{i,k+1} \times \right. \\
& \left. H_{i,k+1} \right] (P_{i,k+1|k}^{-1} - \beta_{i,k} I)^{-1} \times \\
& \left[ I - C_{i,k+1} \sum_{j \in \mathcal{N}_i} (1 - \phi_{ij,k+1}) - K_{i,k+1} H_{i,k+1} \right]^T + \\
& \sum_{j \in \mathcal{N}_i} 3(1 - \bar{\phi}_{ij,k+1}) C_{i,k+1} P_{j,k+1|k} C_{i,k+1}^T + \\
& \sum_{j \in \mathcal{N}_i} 3\bar{\gamma}_{ij,k+1} \delta^2 C_{i,k+1} C_{i,k+1}^T + K_{i,k+1} [(1+2d_i) \times \\
& \beta_{i,k}^{-1} V_{i,k+1} V_{i,k+1}^T + R_{i,k+1}] K_{i,k+1}^T. \quad (37)
\end{aligned}$$

将引理2应用于(26)、(27)、(31)和(37),可以得出结论

$$P_{i,k+1|k+1} \leq \Phi_{i,k+1|k+1}. \quad (38)$$

下面计算上界矩阵  $\Phi_{i,k+1|k+1}$  的迹相对于滤波增益矩阵  $K_{i,k+1}$  的偏导数,得到

$$\begin{aligned}
& \frac{\partial \text{tr}(\Phi_{i,k+1|k+1})}{\partial K_{i,k+1}} = \\
& (1+2d_i) \left[ -2(\Phi_{i,k+1|k}^{-1} - \beta_{i,k} I)^{-1} H_{i,k+1}^T + 2C_{i,k+1} \times \right. \\
& \left. \sum_{j \in \mathcal{N}_i} (1 - \phi_{ij,k+1}) \right] (\Phi_{i,k+1|k}^{-1} - \beta_{i,k} I)^{-1} H_{i,k+1}^T +
\end{aligned}$$

$$\begin{aligned}
& 2K_{i,k+1} H_{i,k+1} (\Phi_{i,k+1|k}^{-1} - \beta_{i,k} I)^{-1} H_{i,k+1}^T + \\
& 2K_{i,k+1} [(1+2d_i) \beta_{i,k}^{-1} V_{i,k+1} V_{i,k+1}^T + R_{i,k+1}]. \quad (39)
\end{aligned}$$

滤波增益矩阵  $K_{i,k+1}$  可以通过求解  $\partial \text{tr}(\Phi_{i,k+1|k+1}) / \partial K_{i,k+1} = 0$  确定,得到如式(30)的解.  $\square$

### 3 滤波器性能分析

**引理4**<sup>[21]</sup> 假设存在随机过程  $\mathcal{M}_k(\zeta_k)$  和实数  $\bar{\delta}, \underline{\delta}, \mu > 0$  以及  $0 < \alpha < 1$ , 使得

$$\underline{\delta} \|\zeta_k\|^2 \leq \mathcal{M}_k(\zeta_k) \leq \bar{\delta} \|\zeta_k\|^2 \quad (40)$$

成立,且有

$$E\{\mathcal{M}_k(\zeta_k) | \zeta_{k-1}\} \leq (1-\alpha)\mathcal{M}_{k-1}(\zeta_{k-1}) + \mu, \quad (41)$$

那么随机过程在均方上是指数有界的,即

$$\begin{aligned}
& E\{\|\zeta_k\|^2\} \leq \\
& \frac{\bar{\delta}}{\underline{\delta}} E\{\|\zeta_0\|^2\} (1-\alpha)^k + \frac{\mu}{\underline{\delta}} \sum_{i=1}^k (1-\alpha)^i. \quad (42)
\end{aligned}$$

**定理2** 假设上界矩阵  $\Phi_{i,k|k}$  满足

$$\Phi_{i,k|k}^{-1} \leq \frac{1+d_{\max}}{\theta} \sigma_{i,k} I, \quad d_{\max} < \theta < \frac{1+d_{\max}}{1+\varepsilon},$$

同时存在正标量  $\lambda, \ell$  使得对于任意的  $i$  和  $k$ , 有  $\lambda I \leq \sigma_{i,k} \leq \ell I$ . 考虑由式(1)和(2)描述的离散时间非线性系统,若初始估计误差  $e_{i,0|0}$  是有界的,则估计误差  $e_{i,k|k}$  满足均方有界.

### 4 仿真分析

本节通过移动机器人室内定位问题验证所提出算法的有效性.机器人的运动模型表示为

$$x_{k+1} = x_k + \frac{s_k^R + s_k^L}{2} \cos \theta_k + \omega_k^x, \quad (43)$$

$$y_{k+1} = y_k + \frac{s_k^R + s_k^L}{2} \sin \theta_k + \omega_k^y, \quad (44)$$

$$\theta_{k+1} = \theta_k + \frac{s_k^R - s_k^L}{b} + \omega_k^\theta. \quad (45)$$

其中:  $(x_k, y_k)$  为机器人位置,  $\theta_k$  为机器人转向,  $s_k^R, s_k^L$  分别为在时间间隔  $[k, k+1)$  内机器人左右轮驶过的距离,  $b$  为左右轮之间的距离,  $\omega_k = (\omega_k^x, \omega_k^y, \omega_k^\theta)$  是协方差为  $Q_k$  的零均值高斯白噪声.

采用8个摄像头对机器人的位置进行测量,传感器节点的通信拓扑图如图1所示<sup>[2]</sup>. 每个摄像头的测量方程表示为

$$\begin{aligned}
p_{i,k} = & \frac{\gamma_u}{z_f^c} [-(x_{i,k} - x_k) \sin \theta_k + (y_{i,k} - y_k) \cos \theta_k - \\
& d_2] + p_0 + v_{i,k}^p, \quad (46)
\end{aligned}$$

$$\begin{aligned}
q_{i,k} = & \frac{\gamma_v}{z_f^c} [-(x_{i,k} - x_k) \cos \theta_k - (y_{i,k} - y_k) \sin \theta_k - \\
& d_1] + q_0 + v_{i,k}^q. \quad (47)
\end{aligned}$$

其中:  $(p_{i,k}, q_{i,k})$  为像平面上目标的坐标,  $(d_1, d_2)$  为机器人在自身坐标系下的坐标,  $z_f^c$  为摄像头的视觉中心到目标的距离,  $\gamma_v$  和  $\gamma_u$  为像素放大系数,  $(p_0, q_0)$  为摄像头主点的图像坐标,  $(x_{i,k}, y_{i,k})$  为每一个摄像头的位置坐标,  $v_{i,k} = (v_{i,k}^p, v_{i,k}^q)$  是协方差为  $R_{i,k}$  的零均值高斯白噪声.

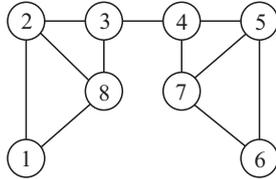


图1 摄像头分布拓扑图

仿真过程中, 参数取值如下:  $d_1 = -0.0668, d_2 = 0.0536, z_f^c = 2.1050, \gamma_u = 9.0213283, \gamma_v = 9.0250141, p_0 = 347.20436, q_0 = 284.34750, R_{i,k} = \text{diag}\{1, 1\}, Q_k = \text{diag}\{1, 1, 1\}, i = 1, 2, \dots, 8$ . 摄像头位置分别为:  $(0.6, 0.6), (0.6, 1.8), (1.2, 1.8), (1.8, 1.8), (2.4, 1.8), (2.4, 1.6), (1.8, 1.2), (1.2, 1.2)$ . 攻击信号  $\xi_k$  选择为  $[1.5 \ 1.5]^T \sin(s_{i,k})$ , 其中  $s_{i,k}$  是服从高斯分布  $\mathcal{N}(0, 1)$  的随机变量. 注意到, 攻击信号的界满足  $\delta = 2.12. \sigma_{i,k} = \beta_{i,k} = 0.1$ . 设置一致性增益矩阵  $C_{i,k+1} = \tau \Phi_{i,k+1|k}, \tau = 0.01$ .

以节点2、5为例, 给出节点与其邻居节点之间的通信信道受到恶意复杂攻击时的示意图如图2和图3所示. 图中位于横坐标轴上的点表示未发生攻击行为, 每个信道的复杂攻击信号均是通过 Matlab 的  $\text{randn}()$  函数随机产生的高斯信号, 均值为0, 方差为9. 产生的随机数的数值大小表明了攻击信号的强弱.

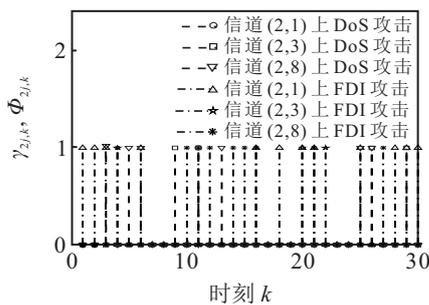


图2 节点2通信信道受攻击情况

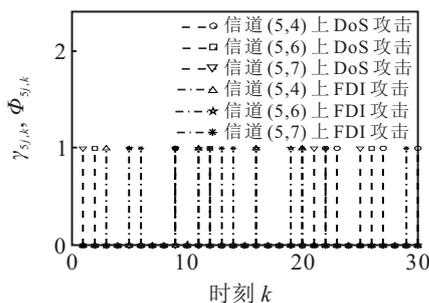


图3 节点5通信信道受攻击情况

图4为1~30时间步机器人运动轨迹的跟踪效果. 由图4可见, 虽然在受到攻击时估计器对目标位置的估计略有偏差, 但是依然能够有效追踪到目标位置, 这表明所设计的滤波器是能够有效抵御网络攻击, 完成目标定位的.

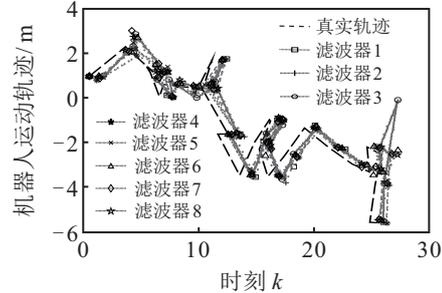


图4 机器人运动轨迹的估计效果

为了进一步分析8个滤波器在每一时刻的估计误差, 图5给出了1~30时间步每个滤波器的均方根误差(RMSE). 由图5可见, 8个滤波器大致实现一致性估计, 且趋于稳定.

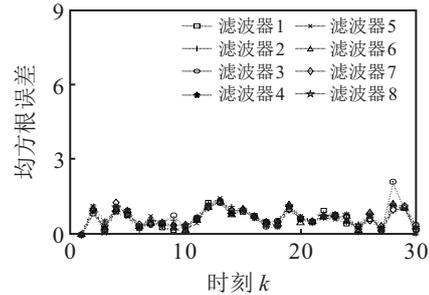


图5 8个滤波器的RMSE

### 5 结论

本文在同时包含 DoS 和 FDI 的复杂攻击情况下, 研究了一类非线性系统的分布式一致性滤波器设计问题. 通过求解两个类黎卡提差分方程得到估计误差协方差矩阵的一个上界矩阵, 并推导出最优滤波器增益矩阵, 同时证明了估计误差的均方有界性. 最后, 通过仿真实验验证了所提出算法能够降低复杂攻击行为对系统的不利影响, 实现对目标的定位.

### 参考文献(References)

[1] 杨旭升, 张文安, 俞立. 适用于事件触发的分布式随机目标跟踪方法[J]. 自动化学报, 2017, 43(8): 1393-1401.  
(Yang X S, Zhang W A, Yu L. Distributed tracking method for maneuvering targets with event-triggered mechanism[J]. Acta Automatica Sinica, 2017, 43(8): 1393-1401.)  
[2] Li W L, Jia Y M, Du J P. Distributed consensus extended Kalman filter: A variance-constrained approach[J]. IET Control Theory & Applications, 2017, 11(3): 382-389.  
[3] He H F, Chen Y, Qi W H, et al. Observer-based resilient

- control of positive systems with heterogeneous DoS attacks: A Markov model approach[J]. *Journal of the Franklin Institute*, 2022, 359(1): 272-293.
- [4] 孙洪涛, 彭晨, 王志文. DoS攻击下的信息物理系统事件触发预测控制设计[J]. *控制与决策*, 2019, 34(11): 2303-2309.  
(Sun H T, Peng C, Wang Z W. Event-triggered predictive control of cyber-physical systems under DoS attacks[J]. *Control and Decision*, 2019, 34(11): 2303-2309.)
- [5] 孙子文, 张炎棋. 工业信息物理系统的攻击建模研究[J]. *控制与决策*, 2019, 34(11): 2323-2329.  
(Sun Z W, Zhang Y Q. Research on attack modeling of industrial cyber physical systems[J]. *Control and Decision*, 2019, 34(11): 2323-2329.)
- [6] Li W L, Jia Y M, Du J P. Distributed extended Kalman filter with nonlinear consensus estimate[J]. *Journal of the Franklin Institute*, 2017, 354(17): 7983-7995.
- [7] Rezaei H, Ghorbani M. Event-triggered resilient distributed extended Kalman filter with consensus on estimation[J]. *International Journal of Robust and Nonlinear Control*, 2022, 32(3): 1303-1315.
- [8] Liu H. Event-triggering-based leader-following bounded consensus of multi-agent systems under DoS attacks[J]. *Communications in Nonlinear Science and Numerical Simulation*, 2020, 89: 105342.
- [9] 李丽, 王夕娟. 拒绝服务攻击下领导-跟随多智能体系统的均方一致性研究[J]. *控制与决策*, 2019, 34(11): 2317-2322.  
(Li L, Wang X J. Mean square consensus for leader-following multi-agent systems under denial-of-service attacks[J]. *Control and Decision*, 2019, 34(11): 2317-2322.)
- [10] Cheng Z H, Yue D, Hu S L, et al. Distributed event-triggered consensus of multi-agent systems under periodic DoS jamming attacks[J]. *Neurocomputing*, 2020, 400: 458-466.
- [11] Xia Y Y, Yang W, Zhao Z Y. Consensus-based filtering under false data injection attacks[J]. *European Journal of Control*, 2019, 48: 3-8.
- [12] 彭大天, 董建敏, 蔡忠闽, 等. 假数据注入攻击下信息物理融合系统的稳定性研究[J]. *自动化学报*, 2019, 45(1): 196-205.  
(Peng D T, Dong J M, Cai Z M, et al. On the stability of cyber-physical systems under false data injection attacks[J]. *Acta Automatica Sinica*, 2019, 45(1): 196-205.)
- [13] Li L, Yang H, Xia Y Q, et al. Event-based distributed state estimation for linear systems under unknown input and false data injection attack[J]. *Signal Processing*, 2020, 170: 107423.
- [14] 周雪, 张皓, 王祝萍. 扩展卡尔曼滤波在受到恶意攻击系统中的状态估计[J]. *自动化学报*, 2020, 46(1): 38-46.  
(Zhou X, Zhang H, Wang Z P. Extended Kalman filtering in state estimation systems with malicious attacks[J]. *Acta Automatica Sinica*, 2020, 46(1): 38-46.)
- [15] Lei L, Yang W, Yang C, et al. False data injection attack on consensus-based distributed estimation[J]. *International Journal of Robust and Nonlinear Control*, 2017, 27(9): 1419-1432.
- [16] Yang W, Zhang X T, Luo W J, et al. Detection against randomly occurring complex attacks on distributed state estimation[J]. *Information Sciences*, 2021, 547: 539-552.
- [17] Liu J L, Yang M, Xie X P, et al. Finite-time  $H_\infty$  filtering for state-dependent uncertain systems with event-triggered mechanism and multiple attacks[J]. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2020, 67(3): 1021-1034.
- [18] Cao J, Da Ding, Liu J L, et al. Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks[J]. *Information Sciences*, 2021, 548: 69-84.
- [19] Guan Y P, Ge X H. Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks[J]. *IEEE Transactions on Signal and Information Processing Over Networks*, 2018, 4(1): 48-59.
- [20] Zhang H, Cheng P, Shi L, et al. Optimal DoS attack scheduling in wireless networked control system[J]. *IEEE Transactions on Control Systems Technology*, 2016, 24(3): 843-852.
- [21] Reif K, Gunther S, Yaz E, et al. Stochastic stability of the discrete-time extended Kalman filter[J]. *IEEE Transactions on Automatic Control*, 1999, 44(4): 714-728.

## 作者简介

高霞(1998—), 女, 硕士生, 从事分布式系统滤波的研究, E-mail: gaoxia980224@163.com;

吴怀宇(1961—), 男, 教授, 博士生导师, 从事机器人技术及其应用领域研究, E-mail: wuhy@wust.edu.cn;

郑秀娟(1986—), 女, 讲师, 博士, 从事信息物理系统状态估计和故障诊断等研究, E-mail: zhengxj@wust.edu.cn.