控制与决策
Control and Decision

网络攻击下基于高斯混合分布式集员滤波的移动目标跟踪

朱洪波, 付源

引用本文:
朱洪波, 付源. 网络攻击下基于高斯混合分布式集员滤波的移动目标跟踪[J]. 控制与决策, 2025, 40(2): 572-580.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2023.1752

网络攻击下基于高斯混合分布式集员滤波的移动目标跟踪

朱洪波†, 付 源

(安徽理工大学 电气与信息工程学院，安徽 淮南 232001)

摘 要: 针对网络攻击下无线传感器网络中的目标跟踪,构建一种高斯混合分布式鲁棒集员滤波算法,旨在提高网络恶意攻击下移动目标跟踪的一致性和精确性. 该算法可分解为校正/测量更新、聚类融合和预测/时间更新3个步骤:校正/测量更新步是指根据传感器采集的测量值更新前一时刻的状态估计(先验估计);聚类融合步是指采用高斯混合模型聚类算法对传感器节点估计进行分类,分为信任节点估计和非信任节点估计,非信任节点估计会被忽略而信任节点估计将参与融合;预测/时间更新步是指预测目标状态的先验估计,将目标的当前时刻状态估计传递至下一时刻. 仿真结果表明:算法在抵御随机攻击、拒绝服务攻击、虚假数据注入攻击、重放攻击以及混合攻击这5种常见的网络攻击方式下具有较好的鲁棒性.

关键词: 无线传感器网络；目标跟踪；网络攻击；分布式集员滤波；高斯混合模型；聚类融合

中图分类号: TP13 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2023.1752

引用格式: 朱洪波,付源. 网络攻击下基于高斯混合分布式集员滤波的移动目标跟踪[J]. 控制与决策, 2025, 40(2): 572-580.

GMM-based distributed set-membership filtering for moving target tracking under cyber attacks

ZHU Hong-bo†, FU Yuan

(School of Electrical and Information Engineering，Anhui University of Science and Technology，Huainan 232001，China)

Abstract: For target tracking in wireless sensor networks under cyber attacks, this paper presents a Gaussian mixture distributed robust set-membership filtering algorithm, aiming to improve the consistency and accuracy of moving target tracking under malicious cyber attacks. The algorithm can be decomposed into three steps: the correction/measurement update step, the clustering fusion step, and the prediction/time update step. The correction/measurement update step is used to update the predicted state estimation (a priori estimation) based on the local measurement. In the clustering fusion step, the available local estimations of sensor nodes are clustered by the Gaussian mixture model clustering algorithm, which are classified into trusted nodes estimations and non-trusted nodes estimations. The non-trusted nodes estimations are ignored while the trusted nodes estimations are used to generate the fused estimation. The prediction/time update step is used for predicting the priori state estimate of the moving target and pass the current moment state estimate of the target to the next moment. Simulation results show that the proposed algorithm is robust against five common cyber attacks, namely random attacks, denial of service attacks, false data injection attacks, replay attacks and hybrid attacks.

Keywords: wireless sensor network; target tracking; cyber attacks; distributed set-membership filter; Gaussian mixture model; clustering fusion

0 引 言

无线传感器网络(wireless sensor network, WSN)由许多微型传感器节点构成,这些节点通过自组织与多跳组网的方式形成一个微型通信网络,用于感知、采集和处理网络信息[1]. 由于WSN具有网内协同感知与分布式处理的能力,广泛应用于智慧农业[2]、国防军事[3]、环境监测[4]和智能交通[5]等领域. 这些应用领域与目标跟踪紧密相关,例如,智慧农业中喷洒农药的无人机、军用无人驾驶战车和侦察机、水面环境监测无人船以及智能交通中车辆的定位和跟

收稿日期: 2023-12-17；**录用日期:** 2024-06-02.
基金项目: 国家自然科学基金项目(62003001)；安徽省高校自然科学研究项目重大项目(2023AH040157).
责任编委: 王燕舞.
†通讯作者. E-mail: hbzhu@aust.edu.cn.

踪. 因此,学术界一直关注WSN中目标跟踪综合性能的提高与改善[6]. 事实上,为了提高WSN中目标跟踪的综合性能,众多学者已经提出了多种不同的滤波方法,例如卡尔曼滤波[7] (Kalman filter, KF)、扩展卡尔曼滤波[8] (extended Kalman filter, EKF)、无迹卡尔曼滤波[9] (unscented Kalman filter, UKF)、容积卡尔曼滤波[10-11] (cubature Kalman filter, CKF)以及集员滤波[12] (set-membership filter, SMF)等. 然而, KF、EKF、UKF和CKF仅能在高斯白噪声的条件下才能发挥出良好的目标跟踪性能,所以当它们处理复杂且不确定的噪声时,目标跟踪性能会严重下降. SMF作为仅要求外界噪声有界而无需知晓其相关统计特性的滤波架构,可以实现在未知但有界的(unknown but bounded, UBB)噪声环境下的目标跟踪[13].

SMF可分为集中式和分布式两类. 集中式可以处理多传感器系统的目标状态估计,仅需将每个传感器接收的数据传输至同一中央估计单元,但是,众多传感器同时向中央估计单元发送传感数据会引起通信、计算与能耗成本过大[14]. 分布式集员滤波(distributed set-membership filter, DSMF)可以弥补集中式集员滤波的上述不足,其特点是每一个基于自身的传感器节点分别与相邻节点进行局部通信,从而实现由局部到全局的信息交换,并且不同传感器之间通过相互协作的方式达到目标状态估计的一致性[15]. 然而,由于WSN在数据传输过程中各传感器节点长期裸露在外,易遭受到恶意的网络攻击. 另外,对于DSMF而言,各个节点主要以局部通信方式处理数据,相较于集中式集员滤波对网络攻击更加敏感,一旦某个节点遭到攻击,其获得的错误估计会通过局部节点扩散至整个网络,进而显著降低目标跟踪的性能[16].

目前,为了解决网络攻击下WSN中目标跟踪性能严重退化的问题,文献[17]提出了一种受约束测量和重放攻击下时变系统的DSMF算法,采用递归线性矩阵不等式(recursive linear matrix inequalities, RLMI)方法在受约束测量和重放攻击的条件下保障目标跟踪的可靠性. 文献[18]提出了一种应对拒绝服务(denial-of-service, DoS)攻击和信号衰落测量的递归DSMF算法,利用区域拓扑方法解决DoS攻击和信号衰落测量问题,使得DSMF参数得到优化. 文献[19]提出了一种二进制编码下基于动态偏差和DoS攻击的时域DSMF算法,由于采用二进制编码方案进行数据传输,其过程容易遭受信道噪声引起的随机误码和DoS攻击,可以在网络系统受到此类攻击的情况下,利用RLMI方法估计每个网络节点的动态偏差和状态性能. 但是,以上算法仅针对特定的网络攻击方式,可能无法应对其他非特定方式. 为了抵御各种网络攻击方式,文献[20]提出了一种基于信任分布式KF算法,利用分布式KF与K-means聚类算法相结合的方式抵御各种网络攻击并验证了其有效性,但是K-means聚类算法存在着不可忽视的问题,例如聚类时集群数量和聚类中心难以确定、非凸面形状或者大小差异大的集群聚类精度差以及样本均值受异常值影响会导致聚类中心偏移[21]. 高斯混合模型(Gaussian mixture model, GMM)聚类算法对集群规模和形状不再有局限性,所以相较于传统K-means聚类算法更加灵活.

受上述讨论启发,本文借助无监督空间聚类改进DSMF,将权重自适应扩散融合框架引入DSMF,提出一种基于高斯混合分布式集员融合滤波的移动目标跟踪方法,以增强对各种恶意网络攻击的抵御能力. 该方法的主要思想是,各传感节点独自执行局部SMF利用局部测量更新移动目标运动状态的局部估计,并仅与相邻节点交换局部估计,然后利用GMM聚类算法将获得的局部节点估计分为信任节点估计与非信任节点估计,信任节点估计参与权重自适应扩散融合,最后利用融合估计及时更新局部预测估计,从而实现网络攻击下各节点仅利用局部测量与局部信息交互对移动目标的精确鲁棒跟踪. 与现有方法相比,所提出方法具有以下优势:

1) 在非持续时间内受到大规模节点网络攻击下,提供了一种在各种网络攻击(非单一特定网络攻击)下移动目标跟踪的统一应对框架;

2) 将GMM聚类引入到DSMF中,设计的权重自适应GMM聚类扩散融合机制不仅实现了信任节点局部估计筛选与融合,而且分离出非信任节点与其局部估计,额外完成了受攻击节点的检测与定位;

3) 该方法仅要求邻近节点间交互数据,虽增加了GMM聚类扩散融合步,但在该步中仅信任节点估计参与融合计算,在保证与DSMF具有近似通讯负担、电能消耗与计算复杂度的基础上,提升了网络攻击下移动目标跟踪的精确性与鲁棒性.

1　问题描述

对于目标跟踪,将系统模型简化为如下线性系统[13]:

$$x_k = A_k x_{k-1} + w_k, \tag{1}$$

$$z_k = H_k x_k + v_k. \tag{2}$$

其中: $x_k \in \mathbb{R}^n$ 为 k 时刻移动目标的状态向量, $z_k \in \mathbb{R}^m$ 为 k 时刻传感器的观测向量; $w_k \in \mathbb{R}^n$ 和 $v_k \in \mathbb{R}^m$ 分别为系统的过程噪声和测量噪声; $A_k \in \mathbb{R}^{n\times n}$ 为 $k-1$ 时刻到 k 时刻移动目标的状态转移矩阵; $H_k \in \mathbb{R}^{m\times n}$ 为 k 时刻的测量矩阵. 当有 $N \in \mathbb{Z}^+$ 个传感器节点时, 其观测模型[20]为

$$z_k^i = H_k^i x_k + v_k^i,\ i = 1, 2, \ldots, N, \tag{3}$$

其中 $H_k^i \in \mathbb{R}^{m\times n}$ 和 $v_k^i \in \mathbb{R}^m$ 分别为传感器节点 i 的测量矩阵和测量噪声.

假设噪声类型是UBB, 并分别属于以下椭球体集合:

$$W_k = \{w_k : w_k^{\mathrm{T}} Q_k^{-1} w_k \leqslant 1\}, \tag{4}$$

$$V_k^i = \{v_k^i : (v_k^i)^{\mathrm{T}} (R_k^i)^{-1} v_k^i \leqslant 1\}. \tag{5}$$

其中: $Q_k \in \mathbb{R}^{n\times n}$ 和 $R_k^i \in \mathbb{R}^{m\times m}$ 为已知正定矩阵且已知初始状态 x_0 属于以下椭球体集合:

$$U_0^i = \{x_0 : (x_0 - \hat{x}_0^i)^{\mathrm{T}} (\hat{P}_0^i)^{-1} (x_0 - \hat{x}_0^i) \leqslant 1\}. \tag{6}$$

这里: $\hat{x}_0^i \in \mathbb{R}^n$ 为初始设置的椭球体中心, $P_0^i \in \mathbb{R}^{n\times n}$ 为描述初始椭球体形状大小和方向的正定矩阵. 已知在 $k-1$ 时刻移动目标的状态属于以下椭球体集合:

$$\begin{aligned} &U_{k-1}^i = \\ &\{x_{k-1} : (x_{k-1} - \hat{x}_{k-1}^i)^{\mathrm{T}} (\hat{P}_{k-1}^i)^{-1} \times \\ &(x_{k-1} - \hat{x}_{k-1}^i) \leqslant 1\}. \end{aligned} \tag{7}$$

由式(1)可知, 移动目标的状态属于如下预测椭球体集合 $U_{k|k-1}^i$:

$$\begin{aligned} &U_{k|k-1}^i = \\ &\{x_k : x_k = A_k x_{k-1} + w_k, x_{k-1} \in U_{k-1}^i, w_k \in W_k\}. \end{aligned} \tag{8}$$

由式(3)可知, 移动目标的状态属于如下测量椭球体集合 Y_k^i:

$$\begin{aligned} &Y_k^i = \\ &\{x_k : (z_k^i - H_k^i x_k)^{\mathrm{T}} (R_k^i)^{-1} \times (z_k^i - H_k^i x_k) \leqslant 1\}. \end{aligned} \tag{9}$$

局部SMF的测量更新步骤是求出预测椭球体集合 $U_{k|k-1}^i$ 和测量椭球体集合 Y_k^i 的交集[22], 即

$$U_k^i = U_{k|k-1}^i \bigcap Y_k^i. \tag{10}$$

如图1所示, 网络攻击下使得移动目标的真实状态脱离式(10)给出的交集, 为了处理无线传感器网络下的该问题, 重点考虑以下5种常见的网络攻击方式:

1) 随机攻击. 攻击者将随机生成的错误数据添加至某个节点, 并通过该受损节点将错误数据传输至其他相邻节点, 此类攻击可以在任意时间发起并且每次攻击时长是不确定的.

2) 拒绝服务攻击. 攻击者可以在任意时刻攻击传感器的观测值, 从而引起WSN数据包缺失, 进一步使其数据传输系统不能正常工作.

3) 虚假数据注入攻击. 攻击者向WSN系统的原始数据中恶意注入虚假数据, 从而破坏其数据的完整性. 由于攻击者得知系统的模型和参数, 错误估计能够有效地绕过现有的不良数据检测技术.

4) 重放攻击. 攻击者将当前时刻的状态估计篡改为曾经某一时刻的数值, 注入的信号经过伪装不易被系统检测到, 所以此攻击类型隐蔽性和欺骗性较强.

5) 混合攻击. 攻击者将上述4种网络攻击叠加在一起对WSN系统发起攻击.

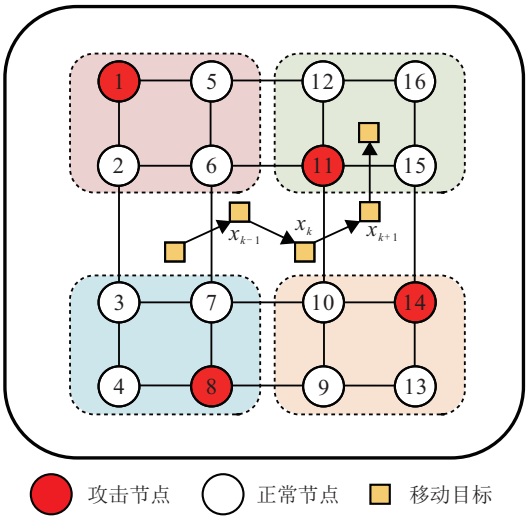

图 1 网络攻击下无线传感器网络的目标跟踪

2 高斯混合分布式鲁棒集员滤波

2.1 测量更新

对于节点 i, 根据测量更新后的椭球体 U_k^i 可以求出椭球体 U_k^i 的中心[23]为

$$\hat{x}_k^i = \hat{x}_{k|k-1}^i + K_k^i (z_k^i - H_k^i \hat{x}_{k|k-1}^i). \tag{11}$$

计算局部SMF增益 K_k^i 为

$$K_k^i = \hat{P}_{k|k-1}^i (H_k^i)^{\mathrm{T}} \left(\frac{H_k^i \hat{P}_{k|k-1}^i (H_k^i)^{\mathrm{T}}}{1-\varphi_k^i} + \frac{R_k^i}{\varphi_k^i} \right)^{-1}. \tag{12}$$

由局部SMF增益更新 k 时刻椭球体 U_k^i 的形状矩阵为

$$\hat{P}_k^i = \frac{\hat{P}_{k|k-1}^i}{1-\varphi_k^i} \left(I - \frac{K_k^i H_k^i}{1-\varphi_k^i} \right). \tag{13}$$

根据椭球体的最小迹原则, φ_k^i 的最优取值如下:

$$\varphi_k^i = \frac{\sqrt{r_{\max}}}{\sqrt{\beta_{\max}} + \sqrt{r_{\max}}}, \tag{14}$$

其中 $r_{\max}$ 和 $\beta_{\max}$ 分别为矩阵 $H_k^i \hat{P}_{k|k-1}^i (H_k^i)^{\mathrm{T}}$ 和 R_k^i 的最大奇异值.

令B^i表示节点i和其相邻节点的集群,$|B^i|$表示集群B^i中节点的个数,在B^i中的各节点交换其椭球体中心$\hat{x}_k^i$和形状矩阵$\hat{P}_k^i$.

2.2　高斯混合聚类融合

本文采用高斯混合模型(GMM)聚类算法识别信任节点和非信任节点,信任节点参与下一阶段的状态更新,非信任节点被忽略. 该算法假设传感器节点数据由多个高斯分布生成,并采用期望最大化(expectation maximum, EM)算法[24]估计每个高斯分布的参数. 假设不超过半数的传感器节点受到攻击,$\hat{x}_k^b$为k时刻节点b的椭球体中心,根据最大概率密度将$|B^i|$个局部估计$\{b \in B^i,\ b = 1,2,\ldots,|B^i|\}$分为信任和非信任集群,则$|B^i|$个局部估计的高斯混合联合概率密度函数为

$$f(\hat{x}_k^b;\pi_j,\mu_j,\Sigma_j)=\sum_{j=1}^{J}\pi_j G(\hat{x}_k^b;\mu_j,\Sigma_j). \tag{15}$$

其中:J为高斯子模型的数量;$G(\hat{x}_k^b;\mu_j,\Sigma_j)$为第$j$个子模型的高斯概率密度函数,且该函数可以看作状态估计$\hat{x}_k^b$属于该子模型的概率;π_j为第j个子模型所占的权重且所有π_j的总和为1;μ_j和Σ_j分别为第j个子模型的样本均值和协方差矩阵.

为了求解GMM中的模型参数,采用EM算法对参数π_j、μ_j和Σ_j进行迭代直至收敛,具体步骤如下.

step 1: 设高斯子模型数量为$J=2$,输入数据为$\hat{x}_k^b$,给定π_j、μ_j和Σ_j的初始值,开始迭代.

step 2 (E步): 计算第j个子模型中节点b的后验概率λ_j^b为

$$\lambda_j^b=\frac{\pi_j G(\hat{x}_k^b;\mu_j,\Sigma_j)}{\sum\limits_{h=1}^{J}\pi_h G(\hat{x}_k^b;\mu_h,\Sigma_h)}. \tag{16}$$

step 3(M步): 根据E步的后验概率值,通过迭代方法更新模型各参数的最大似然函数值为

$$\mu_j=\sum_{b=1}^{|B^i|}\lambda_j^b\hat{x}_k^b\Big/\sum_{b=1}^{|B^i|}\lambda_j^b, \tag{17}$$

$$\Sigma_j=\sum_{b=1}^{|B^i|}\lambda_j^b(\hat{x}_k^b-\mu_j)(\hat{x}_k^b-\mu_j)^{\mathrm{T}}\Big/\sum_{b=1}^{|B^i|}\lambda_j^b, \tag{18}$$

$$\pi_j=\sum_{b=1}^{|B^i|}\lambda_j^b\Big/|B^i|, \tag{19}$$

其中$\sum\limits_{b=1}^{|B_j^i|}\lambda_j^b$为第$j$个子模型中$|B^i|$个节点的后验概率之和.

step 4: 检查更新后模型各参数的似然函数值是否收敛,若不收敛则重新执行E步和M步,直至收敛为止.

当GMM的参数确定后,将$|B^i|$个局部估计进行分类,其具体步骤如下.

step 1: 计算各子模型估计状态$\hat{x}_k^b$的概率密度,并将其估计状态$\hat{x}_k^b$分配给集群ζ,有

$$\zeta=\arg\max_j\{G(\hat{x}_k^b;\mu_j,\Sigma_j)\},\ j=1,2,\ldots,J. \tag{20}$$

step 2: 令D_ζ^i表示集群ζ中所有的节点集合,$|D_\zeta^i|$表示集群ζ中所有节点的个数,由于假设不超过半数的传感器节点受到网络攻击,k时刻具有节点数量大的集群被认为是信任节点的集群,用D_k^i表示,有

$$D_k^i=\arg\max_j(|D_j^i|),\ j=1,2,\ldots,J. \tag{21}$$

step 3: D_k^i中节点被认为是信任节点,$|D_k^i|$表示D_k^i中节点的个数,节点d表示D_k^i中的某个节点,则节点i的椭球体中心为

$$\hat{x}_k^i=\sum_{d\in D_k^i}\frac{1}{|D_k^i|}\hat{x}_k^d,\ d=1,2,\ldots,|D_k^i|. \tag{22}$$

节点i的椭球体形状矩阵为

$$\hat{P}_k^i=\sum_{d\in D_k^i}\frac{1}{|D_k^i|}\hat{P}_k^d,\ d=1,2,\ldots,|D_k^i|. \tag{23}$$

注1　集群D_k^i为信任节点的集群,B^i/D_k^i为非信任节点的集群. 在GMM聚类融合步骤中,正常节点的状态估计会与受攻击节点的状态估计差别较大,GMM聚类算法恰好可以根据各节点状态估计的空间分布差异,将各节点分为信任节点和非信任节点. 所以正常节点会被划分到信任节点的集群,受攻击节点会被划分到非信任节点的集群.

2.3　时间更新

对于节点i,根据测量椭球体集合求出$k+1$时刻的椭球体的参数[25],即由式(9)可得椭球体中心为

$$\hat{x}_{k+1|k}^i=A_k\hat{x}_k^i. \tag{24}$$

椭球体形状矩阵为

$$\hat{P}_{k+1|k}^i=A_k\frac{\hat{P}_k^i}{1-s_{k+1}}A_k^{\mathrm{T}}+\frac{Q_{k+1}}{s_{k+1}}. \tag{25}$$

根据椭球体的最小迹原则,通过优化参数s_{k+1}得到预测后的最小迹状态椭球体如下:

$$s_{k+1}=\arg\min_{s_{k+1}\in(0,1)}\mathrm{tr}(\hat{P}_{k+1|k}^i), \tag{26}$$

椭球体的迹用运算符$\mathrm{tr}(\cdot)$表示,从而得到s_{k+1}最优取值如下:

$$s_{k+1}=\frac{\sqrt{\mathrm{tr}(Q_{k+1})}}{\sqrt{\mathrm{tr}(A_k\hat{P}_k^iA_k^{\mathrm{T}})}+\sqrt{\mathrm{tr}(Q_{k+1})}}. \tag{27}$$

本文提出的高斯混合分布式鲁棒集员滤波算法详细过程见算法1.

算法1 高斯混合分布式鲁棒集员滤波算法.

输入: 椭球体初始化中心 $\hat{x}^i_{k|k-1}$ 和形状矩阵 $\hat{P}^i_{k|k-1}$, 正定矩阵参数 Q_k 和 R^i_k;

输出: 椭球体中心 $\hat{x}^i_{k+1|k}$ 和形状矩阵 $\hat{P}^i_{k+1|k}$.

step 1: 测量更新. 根据式(11)和(13)计算椭球体 U^i_k 的中心 $\hat{x}^i_k$ 和形状矩阵 $\hat{P}^i_k$.

step 2: 聚类融合.

step 2.1: 根据式(20)和(21)求出信任节点的集群 D^i_k;

step 2.2: 根据式(22)和(23)计算聚类融合后节点 i 的椭球体中心 $\hat{x}^i_k$ 和形状矩阵 $\hat{P}^i_k$.

step 3: 时间更新.

step 3.1: 根据式(24)和(25)计算更新后的椭球体中心 $\hat{x}^i_{k+1|k}$ 和形状矩阵 $\hat{P}^i_{k+1|k}$;

step 3.2: 判断 k 是否小于等于 $k_{\max}$, 若是则令 $k = k+1$, 并转至step 1, 否则结束.

2.4 计算复杂度分析

为了进一步分析基于高斯混合DSMF算法在实际应用中的可行性, 分别对DSMF和GMM聚类融合机制进行详细的计算复杂度分析, 并用 O 表示计算复杂度[21]. DSMF的计算复杂度分析如表1所示.

表1 DSMF的计算复杂度

公式	复杂度成本
(11)	$4nm$
(12)	$m^3+2n^2m+2nm^2+4m^2-2nm+m+1$
(13)	$2n^3+2n^2m+n^2$
(14)	$2n^2m+2nm^2-m^2-nm+4$
(24)	$2n^2-n$
(25)	$3n^2+1$
(26)	$n-1$
(27)	$4n^3-2n^2+2n+2$

由表1可知DSMF中每个公式的复杂度成本. 其中: n 和 m 表示各运算向量的维数. 通过表1可以求出DSMF的复杂度成本总和, 有

$$\begin{aligned}\text{Sum(DSMF)} = {}& 6n^3+m^3+6n^2m+4nm^2+\\ & 4n^2+3m^2+nm+\\ & 2n+m+7.\end{aligned} \tag{28}$$

由式(28)可知, DSMF的复杂度成本主要随着 n^3、m^3、n^2m 以及 nm^2 的增大而增大, 故DSMF的计算复杂度可以描述为 $O(n^3+m^3+n^2m+nm^2)$. 当 $n>m$ 时, n 的取值是影响DSMF计算复杂度的主要因素; 反之, 则 m 的取值是影响其计算复杂度的主要因素.

GMM聚类融合机制的计算复杂度如表2所示.

表2 GMM聚类融合机制的计算复杂度

公式	复杂度成本	公式	复杂度成本
(16)	$2J^2+J$	(20)	J
(17)	$2n\lvert B^i\rvert$	(21)	J
(18)	$(3n^2+n)\lvert B^i\rvert$	(22)	$n\lvert D^i_k\rvert$
(19)	$\lvert B^i\rvert$	(23)	$n^2\lvert D^i_k\rvert$

根据表2可以求出迭代一次的EM算法复杂度成本总和为

$$\begin{aligned}&\text{Sum}(\text{EM}_1)=\\ &(3n^2+3n+1)|B^i|+2J^2+J.\end{aligned} \tag{29}$$

由于EM算法是通过对所求的参数变量进行迭代直至收敛的过程, 本文假设迭代次数为 η 时所求参数变量收敛, 则迭代 η 次EM算法复杂度成本总和为

$$\begin{aligned}&\text{Sum}(\text{EM}_\eta)=\text{Sum}(\text{EM}_1)\eta=\\ &(3n^2+3n+1)|B^i|\eta+2J^2\eta+J\eta.\end{aligned} \tag{30}$$

整体GMM聚类融合的复杂度成本总和为

$$\begin{aligned}&\text{Sum(GMM)}=\\ &(3n^2+3n+1)|B^i|\eta+(n^2+n)|D^i_k|+\\ &2J^2\eta+J\eta+2J.\end{aligned} \tag{31}$$

由式(30)可知, EM算法的复杂度成本随着 $n^2|B^i|\eta$ 的增大而增大, 故EM算法的计算复杂度可以描述为 $O(n^2|B^i|\eta)$. 由式(31)可知, 整体GMM聚类融合机制的复杂度成本主要取决于EM算法的复杂度成本, 故GMM聚类融合的计算复杂度也同样可以描述为 $O(n^2|B^i|\eta)$. 因此, GMM聚类融合机制的计算复杂度主要受状态向量维数 n、局部估计节点数量 $|B^i|$ 和迭代次数 η 的影响.

根据DSMF和GMM聚类融合机制的计算复杂度可知, 基于高斯混合DSMF算法的计算复杂度可以描述为 $O(n^3+m^3+n^2m+nm^2+n^2|B^i|\eta)$. 若 $\eta \gg n$, m 或 $|B^i| \gg n, m$, 则GMM聚类融合机制是影响该算法的计算复杂度的主要因素; 反之, 则DSMF是影响其计算复杂度的主要因素.

3 仿真实验结果

本文采用Matlab软件进行仿真实验, 实验中将16个不同的传感器节点按照图2所示分布在100 cm × 100 cm的平面区域内, 假设5、7、8、11以及14号节点受到恶意的网络攻击. 设置椭球体初始化中心 $\hat{x}^i_{0|-1}=[15\quad 15\quad 2\quad -1]^{\mathrm{T}}$, 椭球体形状矩阵 $\hat{P}^i_{0|-1}=30I^4$ 以及正定矩阵参数 $Q_k=2I^4$ 和 $R^i_k=0.8I^2$, 其中 I^a 为 a 阶的单位矩阵. 状态转移矩阵 A_k 和测量矩阵 H_k 的参数设置如下:

$$A_k=\begin{bmatrix}1&0&1&0\\0&1&0&1\\0&0&1&0\\0&0&0&1\end{bmatrix},\ H_k=\begin{bmatrix}1&0&0&0\\0&1&0&0\end{bmatrix}.$$

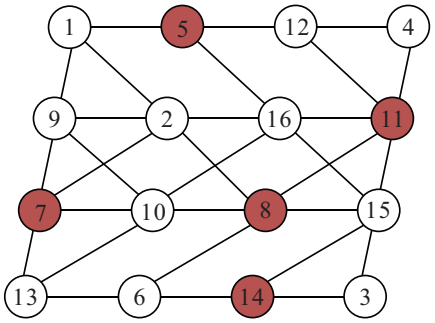

图 2　部分连接的无线传感器网络节点图

为了验证所提出基于高斯混合DSMF算法在网络攻击下目标跟踪中的有效性,采用DSMF+GMM聚类融合方案分别与不引入任何聚类的DSMF方案[18]、KF+GMM聚类融合方案[26]以及DSMF+K-means聚类融合方案[20]做对比实验. 根据上述参数设置,进行100次WSN运动目标跟踪的数值仿真. 为了比较各方案的目标跟踪综合性能,采用均方根误差(root mean squared error, RMSE)和平均均方根误差(sverage root mean squared error, ARMSE)衡量其综合性能,计算公式[25]如下:

$$\mathrm{RMSE}(k)=\sqrt{\frac{1}{C}\sum_{g=0}^{C}\|\hat{x}_{g,k}-x_{g,k}\|^2},\tag{32}$$

$$\mathrm{ARMSE}=\frac{1}{L_t}\sum_{k=0}^{L_t}\sqrt{\frac{1}{C}\sum_{g=0}^{C}\|\hat{x}_{g,k}-x_{g,k}\|^2}.\tag{33}$$

其中:$\hat{x}_{g,k}$和$x_{g,k}$分别为第g次实验中k时刻的目标运动状态估计值和目标运动状态真实值,L_t为仿真步长,C为仿真实验次数. 设置仿真时间为20 s,在此时间内,针对5种常见的网络攻击方式对传感器节点的目标运动过程进行观测和记录,仿真结果如图3～图10所示.

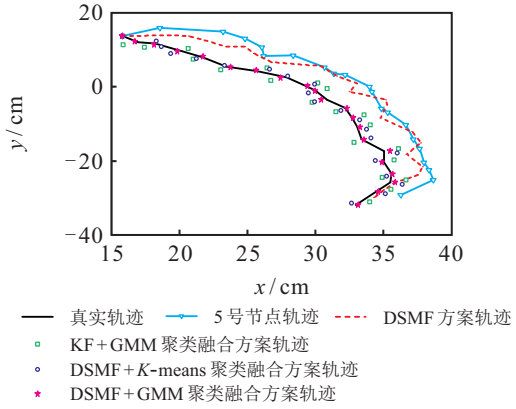

图 3　随机攻击下真实轨迹与不同方案下的轨迹比较

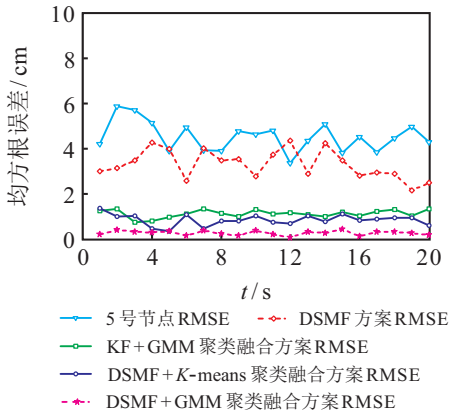

图 4　比较不同方案在随机攻击下的均方根误差

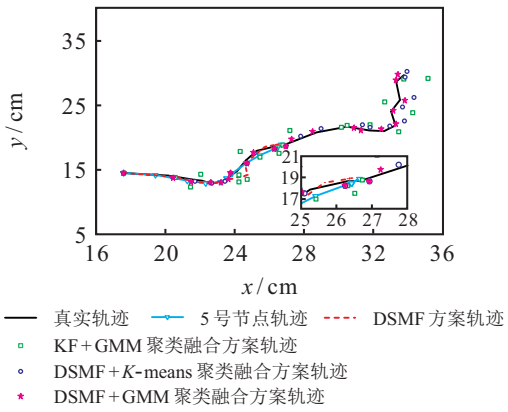

图 5　DoS攻击下真实轨迹与不同方案下的轨迹比较

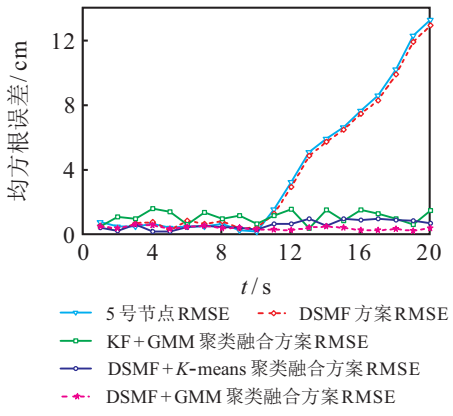

图 6　比较不同方案在DoS攻击下的均方根误差

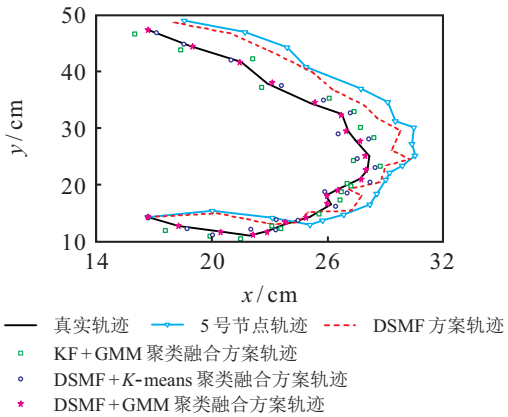

图 7　FDI攻击下真实轨迹与不同方案下的轨迹比较

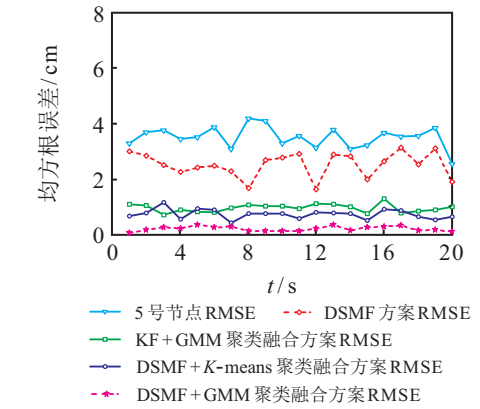

图 8 比较不同方案在 FDI 攻击下的均方根误差

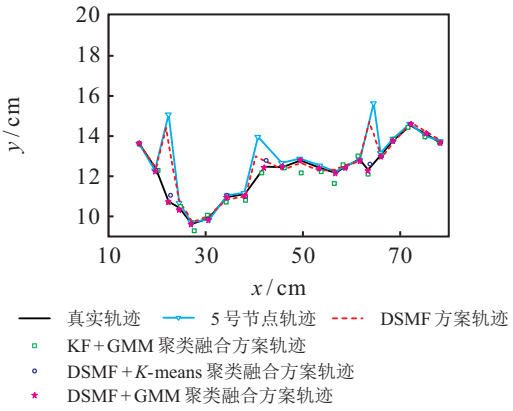

图 9 重放攻击下真实轨迹与不同方案下的轨迹比较

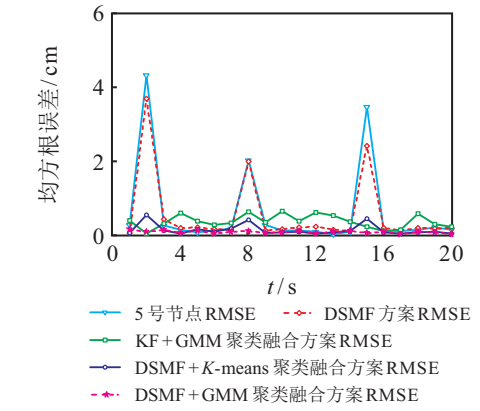

图 10 比较不同方案在重放攻击下的均方根误差

图 3 为 WSN 节点在随机攻击下, 仿真实验中移动目标运动真实轨迹、DSMF 方案所估计轨迹和 3 种不同组合聚类融合方案所估计轨迹, 图 4 为图 3 各方案相应的 RMSE.

图 5 为 WSN 节点在 DoS 攻击下, 仿真实验中移动目标运动真实轨迹、DSMF 方案所估计轨迹和 3 种不同组合聚类融合方案所估计轨迹. 图 6 为图 5 各方案相应的 RMSE. 其中攻击者在时间 $T = 10$ s 时对 WSN 系统发出攻击.

图 7 为 WSN 节点在虚假数据注入 (false data injection, FDI) 攻击下, 仿真实验中移动目标运动真实轨迹、DSMF 方案所估计轨迹和 3 种不同组合聚类融合方案所估计轨迹. 图 8 为图 7 各方案相应的 RMSE.

图 9 为 WSN 节点在重放攻击下, 仿真实验中移动目标运动的真实轨迹、DSMF 方案所估计轨迹和 3 种不同组合聚类融合方案所估计轨迹. 图 10 为图 9 各方案相应的 RMSE. 其中攻击者分别在时间 $T = 2$ s, 8 s, 15 s 这 3 个时刻对 WSN 系统发出攻击.

上述 4 种常见的网络攻击方式下各方案的 ARMSE 如表 3 所示.

表 3 各种网络攻击下不同方案的 ARMSE

ARMSE/cm	攻击方式			
	随机攻击	DoS 攻击	FDI 攻击	重放攻击
5 号节点	4.541 8	3.954 6	3.487 7	0.613 1
DSMF 方案	3.325 1	3.855 8	2.494 7	0.553 5
KF+GMM 聚类融合方案	1.143 3	1.060 4	0.923 7	0.363 8
DSMF+ K-means 聚类融合方案	0.861 9	0.570 1	0.698 5	0.135 9
DSMF+GMM 聚类融合方案	0.286 8	0.370 9	0.169 9	0.077 3

由图 3、 图 5、 图 7 和图 9 可知, 仿真实验中 DSMF+GMM 聚类融合方案所估计的目标运动轨迹更接近于实验中目标运动的真实轨迹. 由图 4、图 6、图 8、 图 10 以及表 3 可知, 在同等噪声环境下, 随着时间的增加, 不引入任何聚类的 DSMF 方案表现出的 RMSE 精度较差, 所以此方案无法抵御网络攻击. 虽然 KF+GMM 聚类融合方案和 DSMF+K-means 聚类融合方案表现出的 RMSE 精度相较于 DSMF 方案有所提高, 但所提出的 DSMF+GMM 聚类融合方案表现出的 RMSE 精度更加优秀. 因此, 根据仿真实验结果可以得出: 当聚类方式同为 GMM 时, DSMF 目标跟踪性能优于 KF; 同样地, 当滤波方式同为 DSMF 时, GMM 聚类效果优于 K-means 聚类, 所以本文提出的 DSMF+GMM 聚类融合方案在抵御随机攻击、DoS 攻击、FDI 攻击和重放攻击下, 具有较强的鲁棒性. 仿真实验中, 5 号节点分别受到上述 4 种不同的网络攻击方式, 其估计的目标运动轨迹均严重偏离真实轨迹, 均表现出较大的 RMSE. 由图 2 给定的网络拓扑结构可知, 每个传感器节点至少与周围两个以上节点进行局部通信. 例如, 对 1 号节点而言, 1 号节点分别与 2 号、 5 号和 9 号节点进行局部信息交互, 其中 5 号节点受到网络攻击, 未受到攻击的 1 号、2 号和 9 号节点局部测量更新的目标运动轨迹均靠近真实的目标运动轨迹, 而 5 号节点局部测量更新的目标运动轨迹严重偏离目标运动的真实轨迹. 从空间分布上看, 5 号节点局部测量更新的状态会严重偏离 1 号、2 号和 9 号节点局部测量更新的状态, GMM 聚类算法恰好可以有效地从状态空间分布上将 5 号节点的局

部估计分离出来. 因此,根据受攻击节点的局部状态估计与正常节点的局部状态估计的空间分布差异,利用GMM聚类算法可以将1号、2号和9号识别为信任节点,而5号节点被识别为非信任节点(即受攻击节点). 同理,可以有效地识别与定位其他受攻击节点.

由于传感器节点长期处在复杂的网络环境中,可能会面临多种网络攻击叠加的情况. 针对混合攻击这一网络攻击方式,根据上述初始参数设置进行仿真实验. 图11为WSN节点在混合网络攻击实验下移动目标运动的真实轨迹、DSMF+GMM聚类融合方案所估计轨迹以及不同节点受到不同网络攻击时所估计的运动轨迹. 图12为图11各估计轨迹相应的RMSE. 具体而言,假设5号节点遭受随机攻击、7号节点在$T = 12$ s时遭受DoS攻击、8号节点遭受FDI攻击以及11号节点分别在$T = 3$ s、14 s时遭受重放攻击. 由图11和图12可知,当WSN系统遭受混合攻击时,DSMF+GMM聚类融合方案估计的轨迹仍然与目标运动真实轨迹相近,并且表现出较高精度的RMSE,该算法对于多种叠加的混合网络攻击方式具有较好的鲁棒性.

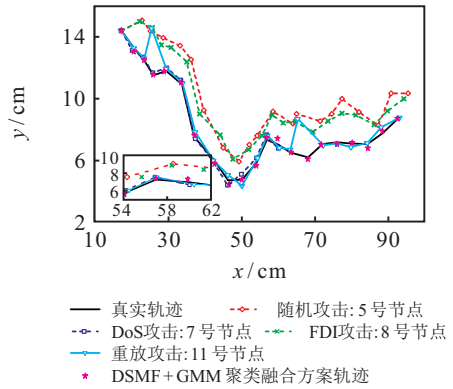

图11　混合攻击下DSMF+GMM聚类融合的轨迹比较

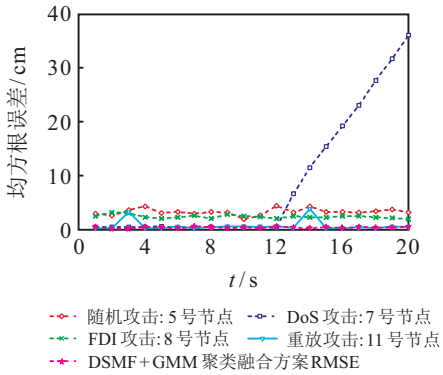

图12　混合攻击下各轨迹相应的均方根误差

4　结　论

为了提高在各种恶意的网络攻击下WSN中目标跟踪的综合性能,本文提出了一种基于高斯混合DSMF移动目标跟踪算法. 针对5种常见的网络攻击方式,对DSMF+GMM聚类融合方案进行仿真实验,并加入不引入任何聚类算法的DSMF方案、KF+GMM聚类融合方案和DSMF+K-means聚类融合方案作为对比方案. 仿真结果表明,相比另外3种方案,该方案在抵御各种网络攻击下具有显著效果.

本文所提出算法能够有效提高WSN受网络攻击下的移动目标跟踪性能,尤其是在稀疏与显著异常网络攻击下效果更加显著. 目前,该算法能有效应对同一时刻不超过半数的传感器节点受到网络攻击的情形,未来将进一步加强算法的适用性,考虑应对大面积传感器节点受到持续不间断网络攻击的情形,并将其扩展至高机动移动目标和强非线性测量系统.

参考文献(References)

[1] 陈作汉, 曹洁, 赵付青. 基于NSGA-II的无线传感网络簇首选择算法[J]. 控制与决策, 2019, 34(11): 2358-2365.
(Chen Z H, Cao J, Zhao F Q. A NSGA-II-based algorithm for WSN cluster head selection[J]. Control and Decision, 2019, 34(11): 2358-2365.)

[2] Haseeb K, Din I U, Almogren A, et al. An energy efficient and secure IoT-based WSN framework: An application to smart agriculture[J]. Sensors, 2020, 20(7): 2081.

[3] Ali A, Jadoon Y K, Ali Changazi S, et al. Military operations: Wireless sensor networks based applications to reinforce future battlefield command system[C]. IEEE 23rd International Multitopic Conference. Bahawalpur, 2020: 1-6.

[4] Behera T M, Mohapatra S K, Samal U C, et al. I-SEP: An improved routing protocol for heterogeneous WSN for IoT-based environmental monitoring[J]. IEEE Internet of Things Journal, 2020, 7(1): 710-717.

[5] Lin C, Han G J, Qi X Y, et al. Energy-optimal data collection for unmanned aerial vehicle-aided industrial wireless sensor network-based agricultural monitoring system: A clustering compressed sampling approach[J]. IEEE Transactions on Industrial Informatics, 2021, 17(6): 4411-4420.

[6] 郭戈, 王兴凯, 徐慧朴. 基于递归工具变量卡尔曼滤波算法的纯方位水下目标跟踪[J]. 控制与决策, 2020, 35(1): 107-114.
(Guo G, Wang X K, Xu H P. Recursive instrumental variable Kalman filtering algorithm for underwater bearing-only target tracking[J]. Control and Decision, 2020, 35(1): 107-114.)

[7] Jondhale S R, Deshpande R S. Kalman filtering framework-based real time target tracking in wireless sensor networks using generalized regression neural networks[J]. IEEE Sensors Journal, 2019, 19(1): 224-233.

[8] Dai Y, Yu S, Yan Y, et al. An EKF-based fast tube MPC scheme for moving target tracking of a redundant underwater vehicle-manipulator system[J]. IEEE/ASME

Transactions on Mechatronics, 2019, 24(6): 2803-2814.

[9] Kulikov G Y, Kulikova M V. Hyperbolic-SVD-based square-root unscented Kalman filters in continuous-discrete target tracking scenarios[J]. IEEE Transactions on Automatic Control, 2022, 67(1): 366-373.

[10] Zhu H B, Luo M Z. Hybrid robust sequential fusion estimation for WSN-assisted moving-target localization with sensor-node-position uncertainty[J]. IEEE Transactions on Instrumentation and Measurement, 2020, 69(9): 6499-6508.

[11] Zhu H B, Wu H B, Luo M Z. Environmentally adaptive event-driven robust cubature Kalman filter for RSS-based targets tracking in mobile wireless sensor network[J]. IEEE Internet of Things Journal, 2023, 10(6): 5530-5542.

[12] 王子赟, 李旭, 王艳, 等. 基于超平行空间集员滤波的非线性系统状态估计方法[J]. 控制与决策, 2022, 37(9): 2287-2295.
(Wang Z Y, Li X, Wang Y, et al. Hyperparallel space set-membership filtering based state estimation algorithm for nonlinear system[J]. Control and Decision, 2022, 37(9): 2287-2295.)

[13] Zhu H B, Chen H, Luo M Z. Adaptive event-driven robust set-membership estimation for received-signal-strength-based moving targets localization[J]. IEEE Internet of Things Journal, 2022, 9(14): 12825-12835.

[14] 林志赟, 吴金泽, 陈亮名. 分布式多智能体网络定位的线性理论与算法综述[J]. 控制与决策, 2024, 39(2): 353-370.
(Lin Z Y, Wu J Z, Chen L M. Survey of distributed multi-agent network localization: Linear theory and algorithms[J]. Control and Decision, 2024, 39(2): 353-370.)

[15] 戴凌飞, 陈昕, 过榴晓, 等. 分布式网络系统的任意预设时间分组一致[J]. 控制与决策, 2023, 38(12): 3482-3489.
(Dai L F, Chen X, Guo L X, et al. Prescribed-time group consensus of multiagent systems[J]. Control and Decision, 2023, 38(12): 3482-3489.)

[16] 叶丹, 靳凯净, 张天予. 网络攻击下的信息物理系统安全性研究综述[J]. 控制与决策, 2023, 38(8): 2243-2252.
(Ye D, Jin K J, Zhang T Y. A survey on security of cyber-physical systems under network attacks[J]. Control and Decision, 2023, 38(8): 2243-2252.)

[17] Liu L, Ma L F, Wang Y W, et al. Distributed set-membership filtering for time-varying systems under constrained measurements and replay attacks[J]. Journal of the Franklin Institute, 2020, 357(8): 4983-5003.

[18] Li X, Wei G L, Wang L C. Distributed set-membership filtering for discrete-time systems subject to denial-of-service attacks and fading measurements: A zonotopic approach[J]. Information Sciences, 2021, 547: 49-67.

[19] Li X, Song J, Hou N, et al. Finite-horizon distributed set-membership filtering with dynamical bias and DoS attacks under binary encoding schemes[J]. Information Sciences, 2023, 641: 119084.

[20] Liang C, Wen F X, Wang Z M. Trust-based distributed Kalman filtering for target tracking under malicious cyber attacks[J]. Information Fusion, 2019, 46: 44-50.

[21] 廖纪勇, 吴晟, 刘爱莲. 基于相异性度量选取初始聚类中心改进的K-means聚类算法[J]. 控制与决策, 2021, 36(12): 3083-3090.
(Liao J Y, Wu S, Liu A L. Improved K-means clustering algorithm for selecting initial clustering centers based on dissimilarity measure[J]. Control and Decision, 2021, 36(12): 3083-3090.)

[22] 林爽, 张依恋, 丁宗贺, 等. 基于改进集员滤波的港口自动跨运车状态估计方法[J]. 控制与决策, 2024, 39(1): 129-136.
(Lin S, Zhang Y L, Ding Z H, et al. State estimation of automated straddle carriers via improved setmembership filtering approach[J]. Control and Decision, 2024, 39(1): 129-136.)

[23] Cong Y, Wang X, Zhou X. Rethinking the mathematical framework and optimality of set-membership filtering[J]. IEEE Transactions on Automatic Control, 2021, 67(5): 2544-2551.

[24] 王宏伟, 柴秀俊. 基于高斯混合模型聚类的非均匀采样系统的多模型切换辨识[J]. 控制与决策, 2021, 36(12): 2946-2954.
(Wang H W, Chai X J. Multi-model switching identification for non-uniformly sampled systems based on Gaussian mixture model clustering[J]. Control and Decision, 2021, 36(12): 2946-2954.)

[25] Zhu H B, Luo J X, Luo M Z, et al. A recursive robust set-membership estimator for WSN-assisted moving targets tracking with UBB anchor location uncertainty[J]. IEEE Transactions on Vehicular Technology, 2023, 72(5): 6547-6557.

[26] Luo J, Zhu H. GMM-based distributed Kalman filtering for target tracking under cyber attacks[J]. IEEE Sensors Letters, 2024, 8(1): 1-4.

作者简介

朱洪波(1988−), 男, 副教授, 博士, 硕士生导师, 主要研究方向为网络化感知估计、控制与优化及其应用, E-mail: hbzhu@aust.edu.cn;

付源(1999−), 男, 硕士生, 主要研究方向为无线传感器网络下的移动目标安全鲁棒跟踪方法, E-mail: 55826443@qq.com.