控制与决策
Control and Decision

网络攻击下基于分布式意图识别的集群逃逸与汇聚控制

张祥银, 张曦梁, 张天

引用本文:
张祥银, 张曦梁, 张天. 网络攻击下基于分布式意图识别的集群逃逸与汇聚控制[J]. 控制与决策, 2024, 39(12): 4171-4180.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2023.1436

网络攻击下基于分布式意图识别的集群逃逸与汇聚控制

张祥银[1,2,3†], 张曦梁[1,2], 张 天[1,2]

(1. 北京工业大学 信息学部，北京 100124；2. 数字社区教育部工程研究中心，
北京 100124；3. 北京工业大学 北京人工智能研究院，北京 100124)

摘 要: 多机器人或无人机组成的集群在执行任务的过程中,当探测到未知外部个体时,需要识别其意图来决定如何应对. 然而,集群内部节点会受到针对测量信号的干扰攻击,导致对外部个体的测量存在误差,进而影响到对其意图的识别. 针对此问题,设计一种考虑网络攻击的基于分布式意图识别的集群控制算法. 在该算法中,集群内部执行集群控制律,当探测到未知外部个体时,集群内部各个节点采用攻击识别算法来识别其是否受到网络攻击;然后,利用基于攻击识别策略的分布式卡尔曼滤波算法,对外部个体的状态进行分布式状态估计,以最大程度上削弱网络攻击对测量值的影响;接着,利用Fréchet距离计算期望轨迹与测量轨迹的相似性,并采用基于分布式共识算法来判断该外部个体的意图,作出逃逸或汇聚控制. 仿真结果验证了所提方法的有效性.

关键词: 网络攻击；分布式估计；集群控制；卡尔曼滤波；攻击识别；状态估计

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2023.1436

引用格式: 张祥银,张曦梁,张天. 网络攻击下基于分布式意图识别的集群逃逸与汇聚控制[J]. 控制与决策, 2024, 39(12): 4171-4180.

Swarm escape and convergence control based on distributed intent recognition under network attack

ZHANG Xiang-yin[1,2,3†], *ZHANG Xi-liang*[1,2], *ZHANG Tian*[1,2]

(1. Faculty of Information Technology，Beijing University of Technology，Beijing 100124，China；2. Engineering Research Centre of Digital Community of Ministry of Education，Beijing 100124，China；3. Beijing Institute of Artificial Intelligence，Beijing University of Technology，Beijing 100124，China)

Abstract: When a swarm composed of multiple robots or drones detects an unknown external node during the execution of a task, it needs to identify its intention to decide how to respond. However, the internal nodes of the swarm will be attacked against the measurement signal, resulting in increased measurement error, and then the intention identification of the external nodes will fail, posing a threat to the swarm. To solve this problem, a distributed control algorithm for swarm which considers the network attack is designed. In this algorithm, the control law is the flocking algorithm. When an unknown external node is detected, firstly, the internal node determines whether it is under network attack based on the designed attack recognition algorithm. Then, according to the distributed Kalman filtering based on attack identification strategy, the state of external nodes is estimated to minimize the impact of network attacks. Next, the similarity between the expected trajectory and the measured trajectory is calculated according to the Fréchet distance, and the distributed consensus algorithm is used to judge the intention of the external node, control swarm escape or converge. Finally, the effectiveness of the proposed method is demonstrated by simulation results.

Keywords: network attack；distributed estimation；swarm control；Kalman filtering；attack identification；state estimation

0 引 言

当多机器人或者多无人机组成的集群探测到外界运动的不明个体时,需要集群各个节点对不明个体的运动轨迹进行观察与探测,并判断出其真实意图. 此过程中,集群节点依靠无线传感器网络(wireless sensor network, WSN)获取外界信息,但WSN会遭受到外部的恶意攻击,如各节点传感器会被干扰导致对目标个体的测量状态偏离、节点间的传输网络会受到恶意信号干扰而断联等. 因此,集群需要对未知外部个体的运动信息进行分布式的抗攻击测量与预测,以识别其意图,进而使集群作出准确的集体决策,从而保证集群的安全.

对于机器人等智能体的集群运动,已有大量相关研究. 最为人所熟知的是Reynolds提出的蜂拥控制

收稿日期: 2023-10-14；**录用日期:** 2024-03-14.
基金项目: 国家自然科学基金项目(62373015).
†通讯作者. E-mail: xy_zhang@bjut.edu.cn.

算法[1],可实现集群运动所遵从的聚集、分离和对齐3种基本行为准则. 当集群在网络攻击下对外部环境进行分布式的探测感知时,文献[2]最早将多智能体一致性理论与卡尔曼滤波相结合,用于解决集群的分布式状态估计问题;文献[3]针对量测信号攻击下的目标状态估计,结合势博弈理论与卡尔曼滤波,提出了一种基于分布式稀疏优化的安全状态估计方法,有效提升了集群的抗量测攻击目标跟踪能力;文献[4]对邻居节点的测量信息进行聚类,将与自身测量信息相似度高的节点作为信任节点进行信息融合,有效抑制了攻击信号的影响;文献[5]提出了基于一致性的分布式卡尔曼滤波算法,实现了部分节点故障下的一致性状态估计;文献[6]设计了一种基于事件触发机制的分布式扩展卡尔曼滤波器,在恶意攻击信号存在有限上界的情况下,保证系统能够达到一定的安全估计精度;文献[7]通过在卡尔曼滤波框架中融入卡方检测器对集群的虚假攻击信息进行检测,进而排除系统故障.

上述文献在对智能体集群运动控制和受到恶意攻击时的节点状态估计已进行了研究并取得了进展,但如何在恶意攻击下根据测量信息与集群运动规律,对未知外部个体的意图进行识别并作出相应的决策,尚未得到充分研究.

本文设计考虑网络攻击的基于分布式意图识别的集群决策控制算法,针对上述问题进行了研究. 首先,集群节点基于测量信息判断其是否受到网络攻击;然后,利用基于攻击识别策略的分布式卡尔曼滤波算法对外部个体的状态进行估计;集群各个节点对探测到的外界个体运动轨迹,与对其的预测轨迹相比对,利用Fréchet距离计算二者的相似度,进而利用集群多数表决方法来获得集群整体对外部个体意图的判定,并作出相应的逃逸或汇聚动作.

1 场景描述与建模

1.1 场景描述

考虑由多个智能节点形成的具有稳定队形的集群系统,当遇到在空间运动的“不明”智能个体向集群靠近时,需要通过集群各节点对该不明个体运动状态的观测与跟踪,经过分布式的决策,最终判定该个体的真实意图,并确定适当的规避或接纳动作. 本文中,节点指代形成稳定集群系统的内部各个智能体,个体指代外部空间中出现的智能体.

在二维空间中,分别令$\boldsymbol{q}_o = [x_o, y_o]^{\mathrm{T}}$、$\boldsymbol{p}_o = [v_{xo}, v_{yo}]^{\mathrm{T}}$和$\boldsymbol{a}_o = [a_{xo}, a_{yo}]^{\mathrm{T}}$为外部个体的位置、速度和加速度矢量,因此个体的运动方程可以表示为

$$[\dot{\boldsymbol{q}}_o \quad \dot{\boldsymbol{p}}_o]^{\mathrm{T}} = [\boldsymbol{p}_o \quad \boldsymbol{a}_o]^{\mathrm{T}}. \tag{1}$$

根据来源及其真实意图,外部个体分为如下3类:

1) 第1类个体(捕食者):该类个体来自敌对方,以一定的速度冲向并追击集群中心,对集群结构以及各个节点进行捕捉和攻击. 集群中的节点应该对其敌对意图进行准确识别,并快速躲避.

2) 第2类个体(中立者):该类个体为在空间中自由移动的第三方个体,既不会主动对集群进行冲撞,也不会对集群进行躲避,即集群状态不会影响到该类节点的运动. 集群中的节点只需将其视为普通障碍物,避免与之发生碰撞.

3) 第3类个体(入队者):该类个体来自我方,为走散后归队,或者根据任务需求而补充进入集群,遵循的运动规律与集群内节点相同. 集群中的节点识别其意图后,将接纳该个体成为集群内部节点.

1.2 集群控制律

集群中各智能体节点遵循蜂拥控制算法,该分布式控制算法的灵感源于鸟类群体行为,能够保证集群各节点之间不发生碰撞、速度一致以及拓扑结构的稳定. 在二维空间中,考虑空间中由n个自由移动智能体组成的集群,其中第i个智能体运动方程描述为如下双积分器形式:

$$\dot{\boldsymbol{q}}_i = \boldsymbol{p}_i,\ \dot{\boldsymbol{p}}_i = \boldsymbol{u}_i,\ i = 1, 2, \ldots, n. \tag{2}$$

考虑离散二维空间下运动,令$\boldsymbol{s}_i(k) = [\boldsymbol{q}_i(k), \boldsymbol{p}_i(k)]^{\mathrm{T}}$表示第$i$个智能体的状态量,$\boldsymbol{u}_(k) = [u_{xi}(k), u_{yi}(k)]^{\mathrm{T}}$表示第$i$个智能体的输入量,则第$i$个智能体运动方程可写为如下状态转移方程:

$$\boldsymbol{s}_i(k+1) = F\boldsymbol{s}_i(k) + B\boldsymbol{u}_i(k). \tag{3}$$

其中:F为4×4的状态转移矩阵;B为4×2的输入矩阵,由智能体模型决定.

设置每个智能体节点只能与距离r以内的节点进行交互,因此定义第i个智能体的邻居集合为$\boldsymbol{N}_i = \{j : ||q_i - q_j|| \leqslant r, j = 1, 2, \ldots, n, j \neq i\}$,其中符号$||\cdot||$表示向量的欧氏距离. 对于集群内部的任意智能体节点,其控制输入的表达式如下:

$$\boldsymbol{u}_i = \boldsymbol{u}_i^{\alpha} + \boldsymbol{u}_i^{\beta} + \boldsymbol{u}_i^{\gamma},\ i = 1, 2, \ldots, n, \tag{4}$$

其中$\boldsymbol{u}_i^{\alpha}$、$\boldsymbol{u}_i^{\beta}$、$\boldsymbol{u}_i^{\gamma}$分别为集群的队形控制项、障碍规避项、目标引导项. 第1项$\boldsymbol{u}_i^{\alpha}$利用一致性算法结合人工势场来实现集群中所有节点的一致运动和队形稳定,其表达式如下:

$$\boldsymbol{u}_i^{\alpha} = -c_1 \sum_{j\in N_i} (\boldsymbol{p}_i - \boldsymbol{p}_j) - c_2 \sum_{j\in N_i} \nabla_{q_i} U^{\alpha}(||\boldsymbol{q}_i - \boldsymbol{q}_j||), \tag{5}$$

其中c_1、c_2为正的控制增益. 第1项通过一致性算法来实现集群各个节点的速度匹配,第2项则利用交互

势场函数的负梯度方向来驱动各个节点之间保持固定的距离并避免碰撞. 这里采用的交互势场表达式如下:

$$U^{\alpha}(||\boldsymbol{x}||)=\frac{d^2}{||\boldsymbol{x}||}+\ln||\boldsymbol{x}||^{\boldsymbol{2}},\tag{6}$$

其中d表示节点i与邻居j之间的期望距离,当$||\boldsymbol{q}_i-\boldsymbol{q}_j||=d$时,$U^{\alpha}$取最小值.

式(4)中的障碍规避项$\boldsymbol{u}_i^{\beta}$用来驱动集群中的各个节点对外部障碍或者威胁进行躲避,表达式如下:

$$\boldsymbol{u}_i^{\beta}=-c_3\sum_{k=1}^{n_{\rm obs}}\nabla_{q_i}U_k^{\beta}(\boldsymbol{q}_i).\tag{7}$$

其中:c_3为正的控制增益. $n_{\rm obs}$为障碍或者威胁的数量. $U_k^{\beta}(\boldsymbol{q})$为第$k$个障碍物在空间形成的斥力势场函数,其表达式如下:

$$U_k^{\beta}(\boldsymbol{q})=\begin{cases}\dfrac{1}{2}\eta\Big(\dfrac{1}{\rho(\boldsymbol{q},\boldsymbol{q}_k^{\rm obs})}-\dfrac{1}{\rho_0}\Big)^2,\ \rho(\boldsymbol{q},\boldsymbol{q}_k^{\rm obs})\leqslant\rho_0;\\ 0,\ \text{otherwise}.\end{cases}\tag{8}$$

η表示正的尺度因子,ρ_0表示障碍的斥力范围,$\boldsymbol{q}_k^{\rm obs}$表示第$k$个障碍物的位置,$\rho(\boldsymbol{q},\boldsymbol{q}_k^{\rm obs})$表示位置点$q$到第$k$个障碍点的最小距离.

式(4)中的目标引导项$\boldsymbol{u}_i^{\gamma}$用于驱动集群向目标点移动,如下所示:

$$\boldsymbol{u}_i^{\gamma}=-c_4(\boldsymbol{q}_i-\boldsymbol{q}_t)-c_5(\boldsymbol{p}_i-\boldsymbol{p}_t).\tag{9}$$

其中:c_4、c_5为正的控制增益,q_t、p_t分别为目标点位置和速度.

1.3　网络攻击的量测模型

集群中节点的WSN在对外部个体进行感知时,往往会受到恶意量测攻击信号的干扰,从而极大地削弱集群节点对外部个体运动状态的探测跟踪可靠性,进而影响对其真实意图的判断. 针对此问题,需要设计一个网络攻击识别算法.

考虑离散二维空间下的分布式估计问题,令$\boldsymbol{x}(k)=[\boldsymbol{p}_o(k),\boldsymbol{q}_o(k),\boldsymbol{a}_o(k)]^{\rm T}$表示所要探测的外部个体的状态量,则式(1)的个体运动方程可写为如下状态转移方程:

$$\boldsymbol{x}(k+1)=A\boldsymbol{x}(k),\tag{10}$$

其中A为6×6的状态转移矩阵.

集群中的每个节点都试图对探测范围内外部个体的状态进行测量. 恶意量测攻击信号则是在集群各节点对外部个体状态的测量值中注入固定或随机的攻击矢量. 在k时刻,集群中第i个节点对外部目标个体具有如下状态测量方程:

$$\boldsymbol{y}_i(k)=H\boldsymbol{x}_i(k)+\boldsymbol{v}_i(k)+\alpha_i(k)\boldsymbol{e}_i(k).\tag{11}$$

其中:$\boldsymbol{y}_i(k)=[x_{o,i}(k),y_{o,i}(k),v_{ox,i}(k),v_{oy,i}(k)]^{\rm T}$是节点$i$对目标个体状态的测量输出,$\boldsymbol{x}_i(k)=\boldsymbol{x}(k)$是节点$i$探测到的目标个体的状态;$H$是$4\times6$的测量矩阵;$v_i(k)$是协方差为$R_i$、均值为0的高斯测量白噪声;$e_i(k)$是与$v_i(k)$相互独立的攻击矢量;$\alpha_i(k)$是攻击因子,受到攻击时为1,未受到攻击时为0. 此攻击矢量的类型为干扰注入攻击,其特点为与原系统的测量噪声相互独立的高斯白噪声,它通过改变集群节点测量方程的总测量噪声,进而增大集群状态估计器的一致性估计误差.

设计一种节点对攻击矢量的自主识别方案

$$\eta_i=\begin{cases}0,\ ||e_i||>D_{e_i};\\ 1,\ \text{otherwise}.\end{cases}\tag{12}$$

其中:$||e_i||$为测量值与估计值的误差,D_{e_i}为设定阈值,η_i为攻击识别因子.

命题1　若$\eta_i=0$,则节点i一定受到攻击.

证明　令$\boldsymbol{e}_i^{\star}$为节点i受到的真实攻击矢量,表示如下:

$$\boldsymbol{e}_i^{\star}=\boldsymbol{y}_i-H\boldsymbol{x}_i-\boldsymbol{v}_i.\tag{13}$$

由于在真实情况下,内部节点对新个体真实状态的测量存在一定误差,且噪声的真实值是未知的,节点i无法测量到真实的攻击矢量大小. 故设节点i测量到的攻击矢量为

$$\boldsymbol{e}_i=\boldsymbol{y}_i-H\bar{\boldsymbol{x}}_i-\bar{\boldsymbol{v}}_i.\tag{14}$$

其中:$\bar{\boldsymbol{x}}_i$为对新个体真实状态的假设值,$\bar{\boldsymbol{v}}_i$为对新个体真实测量噪声的假设值.

令$\Delta\boldsymbol{e}_i=\boldsymbol{e}_i-\boldsymbol{e}_i^{\star}$、$\Delta\boldsymbol{x}_i=\boldsymbol{x}_i-\boldsymbol{x}_i^{\star}$、$\Delta\boldsymbol{v}_i=\boldsymbol{v}_i-\boldsymbol{v}_i^{\star}$分别表示测量攻击矢量与真实攻击矢量的误差、假设状态与真实状态的误差、假设噪声与真实噪声的误差. 由式(13)与(14)相减可得

$$||\Delta\boldsymbol{e}_i||=-H\boldsymbol{x}_i-\Delta\boldsymbol{v}_i.\tag{15}$$

由三角不等式可得

$$\begin{aligned}||\Delta\boldsymbol{e}_i||&\leqslant||H\boldsymbol{x}_i||+||\Delta\boldsymbol{v}_i||\leqslant\\&||H||\max||\Delta\boldsymbol{x}_i||+\max||\Delta\boldsymbol{v}_i||,\end{aligned}\tag{16}$$

其中$\max||\Delta\boldsymbol{x}_i||$与$\max||\Delta\boldsymbol{v}_i||$分别为状态量与噪声量的误差上限. 设定检测阈值

$$D_{e_i}=||H||\max||\Delta\boldsymbol{x}_i||+\max||\Delta\boldsymbol{v}_i||.$$

由攻击方案可知,当$\eta_i=0$时,有$||\boldsymbol{e}_i||>D_{e_i}$,又因$\Delta\boldsymbol{e}_i=\boldsymbol{e}_i-\boldsymbol{e}_i^{\star}$,有

$$\begin{aligned}D_{e_i}<||\Delta\boldsymbol{e}_i||&=||\Delta\boldsymbol{e}_i+\boldsymbol{e}_i^{\star}||\leqslant\\&||\Delta\boldsymbol{e}_i||+||\boldsymbol{e}_i^{\star}||\leqslant D_{e_i}+||\boldsymbol{e}_i^{\star}||.\end{aligned}\tag{17}$$

即$||\boldsymbol{e}_i^{\star}||>0$恒成立,故节点$i$测量信号受到的攻击矢量非零,该节点受到外部攻击. □

2 分布式估计与决策方法

2.1 基于分布式卡尔曼滤波的信息融合算法

分布式卡尔曼滤波是一种用于多个传感器协同工作的滤波算法,每个传感器在本地进行卡尔曼滤波估计,并通过数据交换机制将本地估计结果与其他传感器进行共享,可以有效处理分布式传感器网络的估计问题. 本文在经典分布式卡尔曼滤波的基础上,设计带有测量信号攻击识别机制的分布式卡尔曼滤波算法. 根据分布式卡尔曼滤波理论,各传感器节点基于测量信息更新的状态估计为

$$\hat{\boldsymbol{x}}_i(k)=A\boldsymbol{x}_i(k)+\eta_iK_i^{\star}(\boldsymbol{y}_i-H\boldsymbol{x}_i(k)). \tag{18}$$

其中$K_i^{\star}$为卡尔曼滤波的最优增益. 上式中,卡尔曼滤波的最优增益被计算如下:

$$K_i^{\star}=AP_i(k)H^{\mathrm{T}}(R_i+HP_i(k)H^{\mathrm{T}})^{-1}. \tag{19}$$

估计误差的协方差计算为

$$\hat{P}_i(k)=F_i(k)P_i(k)F_i(k)^{\mathrm{T}}+\eta_iK_i^{\star}R_iK_i^{\star\mathrm{T}}+Q_i, \tag{20}$$

其中$F_i=A-\eta_iK_i^{\star}H$.

上述滤波已经完成了单个内部节点对外部个体的最优估计. 接下来邻近节点之间进行信息交换和融合. 信息融合的公式如下:

$$\boldsymbol{x}_i(k+1)=\begin{cases}\hat{\boldsymbol{x}}_i(k),\ \eta_i=1;\\ \displaystyle\sum_{j\in N_i}\frac{w_{ij}\hat{\boldsymbol{x}}_j(k)}{N_i},\ \eta_i=0;\end{cases} \tag{21}$$

$$P_i(k+1)=\begin{cases}\hat{P}_i(k),\ \eta_i=1;\\ \displaystyle\sum_{j\in N_i}\frac{w_{ij}\hat{P}_j(k)}{N_i},\ \eta_i=0.\end{cases} \tag{22}$$

其中:$\boldsymbol{x}_i(k+1)$和$P_i(k+1)$分别表示节点i对$k+1$时刻新个体的估计状态及其协方差矩阵;N_i表示判断出未受到攻击的节点个数;$\hat{\boldsymbol{x}}_j(k)$和$\hat{P}_j(k)$分别表示在$k$时刻接收到邻居节点$j$的状态估计值与预测误差协方差矩阵;$w_{ij}$表示节点$i$对自身和邻居节点的信息融合权重的划分,对任意的$j\in N_i$,$\displaystyle\sum_{j\in N_i}w_{ij}=1$.

2.2 基于Fréchet距离的轨迹相似度识别

当集群中节点i探测到未知外部个体时,会对个体状态进行测量并生成一条测量轨迹. 为了识别未知个体意图,节点i还需要根据集群运动规律计算出一条符合集群控制律的期望轨迹,根据两条轨迹相似度判断个体意图.

本节选用Fréchet距离来判断未知个体测量轨迹与期望轨迹的相似度. Fréchet距离考量的是图形特征点的整体特性,同时还考虑了路径空间距离的因素,是一种精度较高的路径相似度判别算法. Fréchet距离的定义为:两条有方向的曲线,不能回溯,这两条曲线之间最短的最大距离为Fréchet距离. 示意图如图1所示.

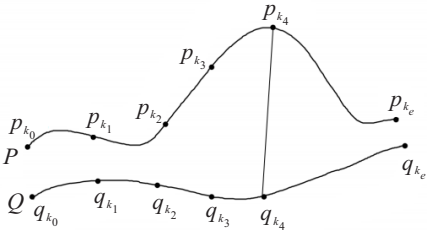


图 1 Fréchet距离

离散Fréchet距离[8]的定义为:设2条由离散位置点表示的曲线P和Q,即$P=\{\boldsymbol{p}_{k_0},\boldsymbol{p}_{k_1},\dots,\boldsymbol{p}_{k_e}\}$和$Q=\{\boldsymbol{q}_{k_0},\boldsymbol{q}_{k_1},\dots,\boldsymbol{q}_{k_e}\}$,则它们的组合序列$L=\{(\boldsymbol{p}_{k_0},\boldsymbol{q}_{k_0}),\dots,(\boldsymbol{p}_{k_e},\boldsymbol{q}_{k_e})\}$,并且组合序列对必须遵循曲线$P$和$Q$所有点的顺序,定义$L$的长度为所有序列对的最大距离,即$||L||=\max\limits_{k=k_0,\dots,k_e}d(\boldsymbol{p}_k,\boldsymbol{q}_k)$,那么曲线$P$与$Q$之间的Fréchet距离$F(P,Q)$为

$$F(P,Q)=\min\{||L||\}. \tag{23}$$

假设集群从时刻k_0探测到未知外部个体,持续至新个体到集群中任意节点的距离达到距离阈值dt为止,记录此时的时刻为k_e. 在$k_1\sim k_e$时刻,集群中的每个节点i根据基于攻击识别策略的分布式卡尔曼滤波,即式(18)~(22),对个体状态进行估计,得到$\boldsymbol{x}_i(k)=[x_i(k),y_i(k),v_{x,i}(k),v_{y,i}(k),a_{x,i}(k),a_{y,i}(k)]^{\mathrm{T}}$. 令

$$\boldsymbol{p}_{ik}=[x_i(k),y_i(k)]^{\mathrm{T}},\ k\in(k_0,k_e),$$

表示节点i在k时刻对未知节点位置的测量,并将$\boldsymbol{p}_{ik}$存入测量轨迹序列P,最终可得到$k_0\sim k_e$时刻节点i对未知节点的测量轨迹

$$P=\{\boldsymbol{p}_{ik_0},\boldsymbol{p}_{ik_1},\dots,\boldsymbol{p}_{ik_e}\}.$$

若未知个体为友方节点,其每个时刻的期望输出应符合集群控制律. 同时,个体状态应符合集群内部节点状态转移方程. 为作判断,在$k_0\sim k_e$时刻每个节点i根据集群控制律,即式(4)~(9)计算出未知个体符合集群运动规律的期望输出$u_i(k)$,然后根据内部状态转移方程,即式(3)计算出未知个体的期望轨迹Q,并与测量轨迹P进行比对. 令$\boldsymbol{x}_{ip}(k_0)=[x_i(k_0),y_i(k_0),v_{x,i}(k_0),v_{y,i}(k_0)]^{\mathrm{T}}$为时刻$k_0$节点$i$探测到外部个体时其位置和速度矢量,根据式(3),可计算出$\boldsymbol{x}_{ip}(k)=[x_{ip}(k),y_{ip}(k),v_{x,ip}(k),v_{y,ip}(k)]^{\mathrm{T}},k\in(k_1,k_e)$,令

$$\boldsymbol{q}_{ik}=[x_{ip}(k),y_{ip}(k)],\ k\in(k_0,k_e),$$

表示节点i在k时刻对未知节点作出符合集群控制律位置的期望,并将$\boldsymbol{q}_{ik}$存入期望轨迹序列Q,最终可得到$k_0\sim k_e$时刻节点i对未知节点的期望轨迹

$$Q=\{\boldsymbol{q}_{ik_0},\boldsymbol{q}_{ik_1},\cdots,\boldsymbol{q}_{ik_e}\}.$$

将测量轨迹P和期望轨迹Q代入Fréche距离定义可得$F(P,Q)$. 节点i通过该偏差是否小于设定阈值e_t判断新个体意图.

2.3　基于多数表决的集群共识决策

在单个节点完成意图识别后,集群采用多数表决的方式达成共识,即根据大多数节点的识别结果决定最终结果. 对于集群中节点i,若$F(P,Q)<e_t$,则节点i判断新个体为入侵个体;若集群中超过2/3的节点判定新个体为入侵个体,则达成共识新个体为第1、第2类个体,需要躲避;否则视新个体为第3类个体,允许其加入集群,不予躲避.

集群对外部个体意图识别具体流程如下:

step 1: 在k_0时刻初始化未知外部个体的状态;

step 2: 每个节点i根据式(12)判断测量信号是否受到攻击;

step 3: 每个节点i根据式(18)～(22)更新估计状态与协方差矩阵信息,并将测量状态存入测量轨迹序列P;

step 4: 每个节点i根据集群控制律计算新个体的期望状态并存入期望轨迹序列Q;

step 5: 每个节点i根据式(3)～(9)更新状态;

step 6: 更新迭代次数$k=k+1$,重复step 1～step 6,直到新个体到集群中任一节点的距离达到距离阈值dt,记录此时的时刻k_e;

step 7: 每个节点i根据式(23)计算$k_0\sim k_e$时刻内P与Q的Fréchet距离$F(P,Q)$,结合阈值e_t对新个体进行分布式意图识别;

step 8: 若2/3内部节点决策出新个体为第1、第2类个体,则进行躲避,否则允许新个体加入.

3　仿真结果与分析

设集群中节点个数$n=36$,设定位置量的最大测量误差$\max||\Delta\boldsymbol{x}_i||=1$;速度量的最大测量误差$\max||\Delta\boldsymbol{v}_i||=0.3$. 集群控制算法参数设置为$d=3,\rho_0=4,Q=0.04E(6),R=0.01E(4)$;目标点初始位置和速度为$q(0)=[0,0]^{\mathrm{T}},p(0)=[0.5,0]^{\mathrm{T}}$. 定义攻击识别率如下:

$$E_{\text{attack}}=n_{\text{identify}}/n_{\text{real}}. \tag{24}$$

其中:n_{real}表示真实受到攻击的节点总数,n_{identify}表示识别出受到攻击的节点总数.

内部节点对新个体状态测量的均方误差定义为

$$\text{MES}(k)=\frac{1}{n}\sum_{i=1}^{n}(\boldsymbol{x}_i(k)-\boldsymbol{x}(k))^2. \tag{25}$$

仿真1　外部个体为第1类个体,向集群中心冲撞. 设定新个体的初始位置为$q(0)=[30,15]^{\mathrm{T}}$,速度恒定为$[-5,2]^{\mathrm{T}}$,攻击矢量的大小为恒定值12. 仿真结果如图2～图7所示.

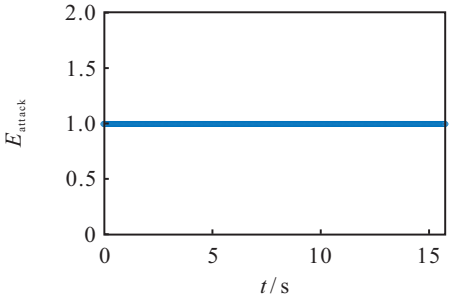


图 2　场景1下的攻击识别率

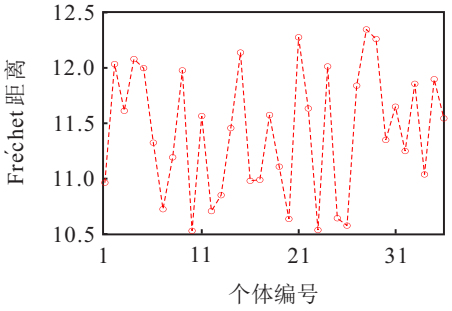


图 3　场景1下测量轨迹与预测轨迹的Fréchet距离

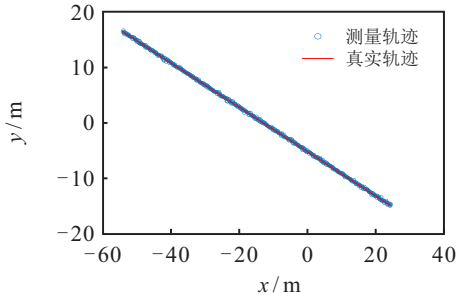


图 4　场景1下新个体的轨迹测量曲线

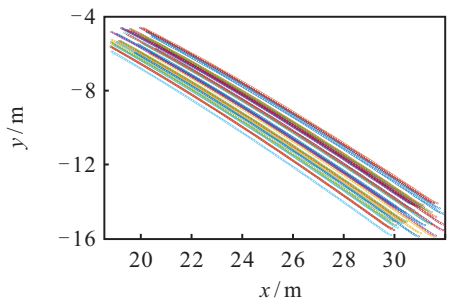


图 5　场景1下新个体期望轨迹预测值

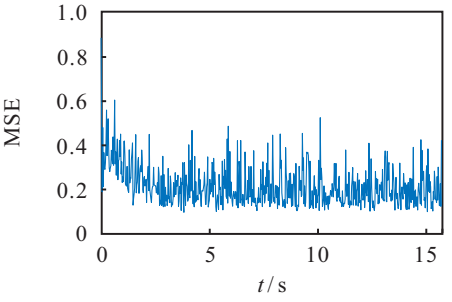


图 6　场景1下新个体轨迹测量的均方误差

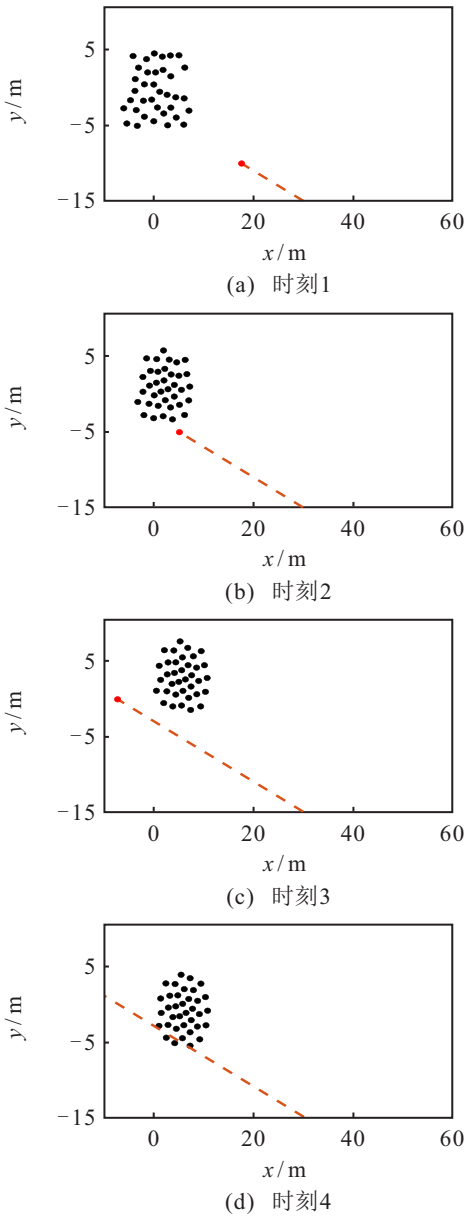


图 7 场景1下节点的中间状态

由图2可知,在攻击矢量固定时,集群的攻击识别率可达到100%. 由图3可知,每个内部节点计算出的Fréchet距离均大于2.8. 由图4和图6可以看出,所提出的方法可以有效跟踪新个体的真实状态,并在存在定值攻击矢量和测量噪声的情况下保证较小的均方误差. 由图5可知,集群对新个体的期望轨迹预测由于初始估计值的不同而存在差异,但均满足集群运动规律. 图7展示了不同时刻的新个体与集群内部节点的状态. 其中,红色点为新个体,黑色点为内部节点,虚线为新个体的运动轨迹. 可以看出,集群在形成后决策出了新个体为威胁节点,并顺利躲避了新个体,保证了集群自身的安全.

仿真2 外部个体为第2类个体,运动轨迹与集群轨迹有交叉. 设定新个体的初始位置为$q(0)=[15,0]^{\mathrm{T}}$,其运动轨迹满足以下方程:

$$\begin{cases} x=15+10\cos 0.4t, \\ y=10\sin 0.4t. \end{cases} \tag{26}$$

仿真结果如图8～图13所示.

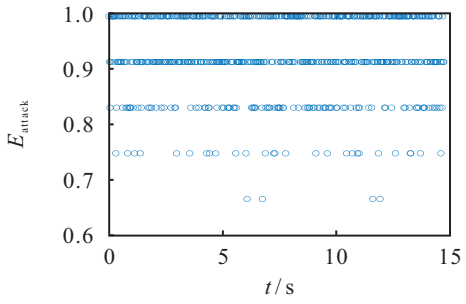


图 8 场景2下的攻击识别率

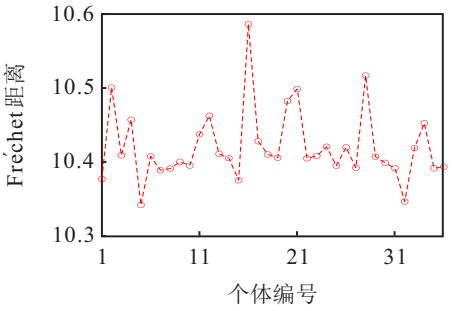


图 9 场景2下测量轨迹与预测轨迹的Fréchet距离

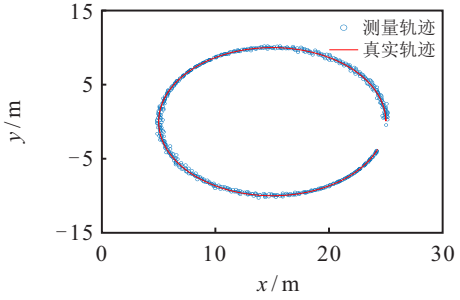


图 10 场景2下新个体的轨迹测量曲线

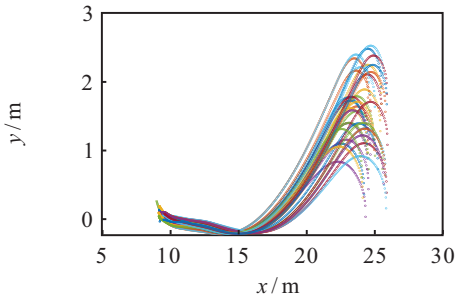


图 11 场景2下新个体期望轨迹预测值

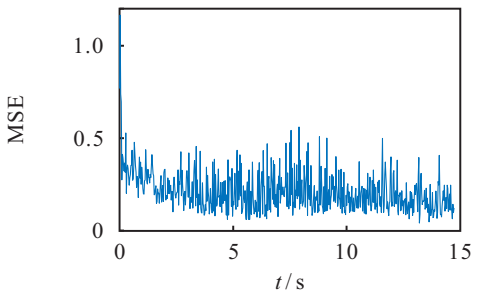
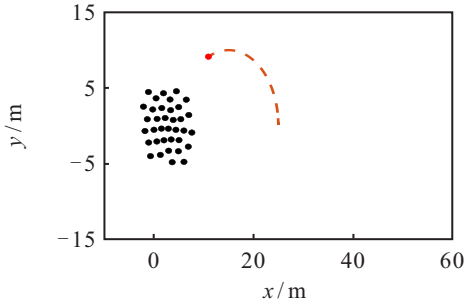
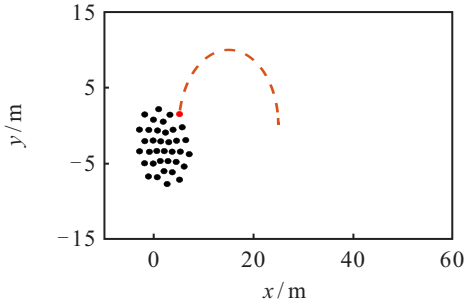


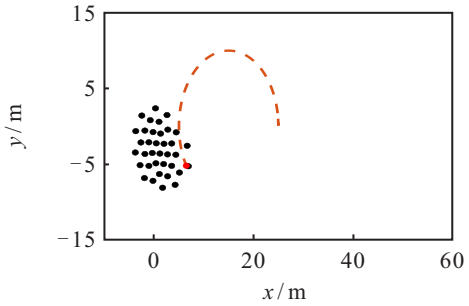
图 12 场景2下新个体轨迹测量的均方误差



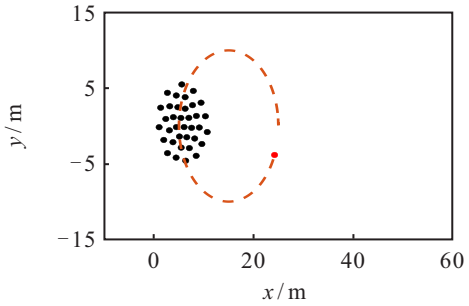
(a) 时刻1



(b) 时刻2



(c) 时刻3



(d) 时刻4

图 13　场景 2 下节点的中间状态

由图 8 可知, 在攻击矢量时变时, 集群仍然在多数时间内有着较高的攻击识别率. 由图 9 可知, 每个内部节点计算出的 Fréchet 距离均大于 10.25. 由图 10 和图 12 可知, 在攻击矢量时变且存在测量噪声的情况下, 所提出的方法仍然可以有效跟踪新个体的真实状态, 保证较小的均方误差. 由图 11 可知, 集群对新个体的期望轨迹预测由于初始估计值的不同而存在差异, 但均满足集群运动规律, 并且最终趋于一致. 图 13 展示了不同时刻的新个体与集群内部节点的状态, 可以看出, 形成集群后, 集群决策出了新个体为威胁节点, 并顺利躲避了新个体, 保证了集群自身的安全.

仿真 3　外部个体为第 3 类个体, 意图加入集群. 设新个体满足集群运动规律, 攻击矢量的大小为随机值 $12 \times \mathrm{rand}(4, 1)$. 仿真结果如图 14 ~ 图 19 所示.

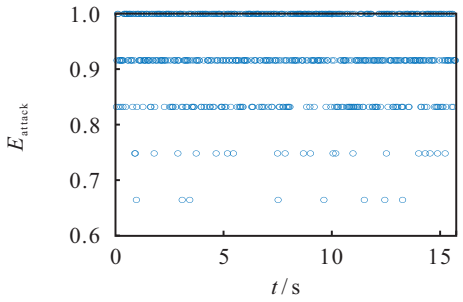


图 14　场景 3 下的攻击识别率

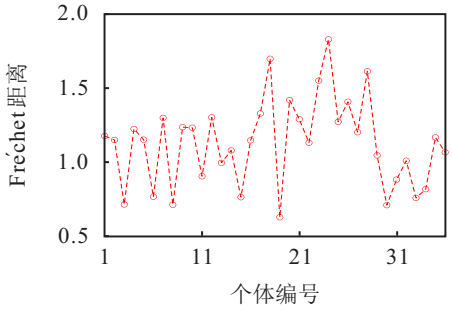


图 15　场景 3 下测量轨迹与预测轨迹的 Fréchet 距离

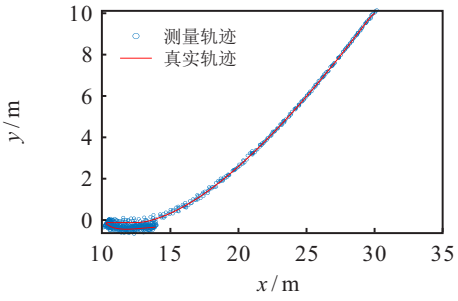


图 16　场景 3 下新个体的轨迹测量曲线

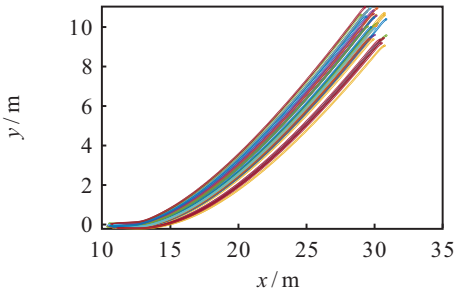


图 17　场景 3 下新个体期望轨迹预测值

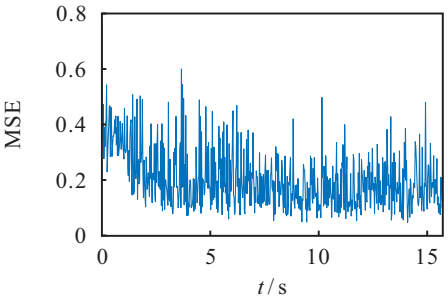
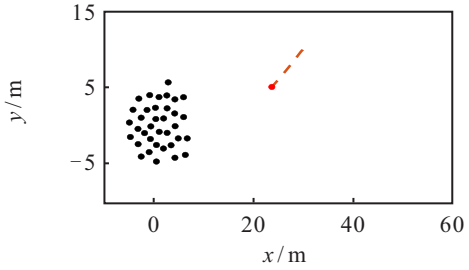
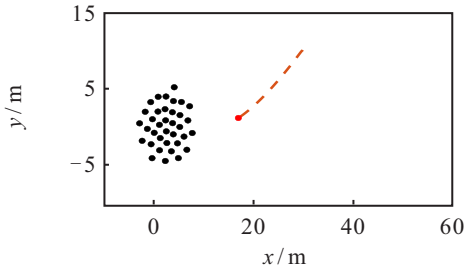


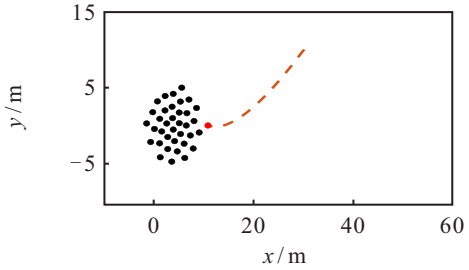
图 18　场景 3 下新个体轨迹测量的均方误差



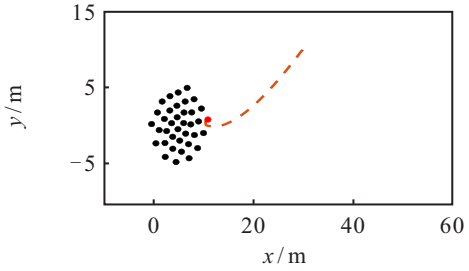
(a) 时刻1



(b) 时刻2



(c) 时刻3



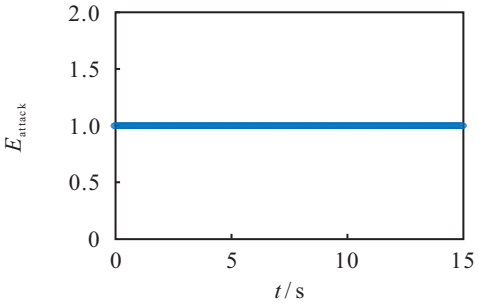
(d) 时刻4

图 19 场景3下节点的中间状态

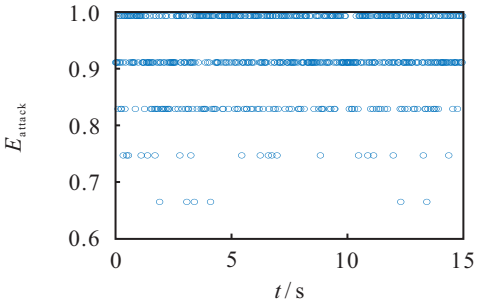
由图14可知,在攻击矢量时变时,集群仍然在多数时间内有着较高的攻击识别率. 由图15可知,Fréchet距离均小于2.4. 由图16和图18可知,在攻击矢量时变且存在测量噪声的情况下,所提出的方法仍然可以有效跟踪新个体的真实状态,保证较小的均方误差. 由图17可知,集群对新个体的期望轨迹预测由于初始估计值的不同而存在差异,但均满足集群运动规律,并且最终趋于一致. 图19展示了不同时刻的新个体与集群内部节点的状态,可以看出,集群经过决策,识别出新个体为友方,允许其加入. 更进一步地,结合图3、图9和图15可以看出,基于Fréchet距离的轨迹相似度判定方法可以较好地表征出预测轨迹与测量轨迹的差异性,通过设定合理的阈值(本文设定为2.5),可以使得集群获得精准的识别结果.

仿真4 外界同时存在多个不同类型的个体. 设定红色个体a为第1类个体,初始位置为$x(0) = [30, -15]^{\mathrm{T}}$,速度恒定为$[-5, 2]^{\mathrm{T}}$,攻击矢量大小恒定为12;设定蓝色个体b为第3类个体,攻击矢量的大小为随机值$12 \times \mathrm{rand}(4, 1)$. 仿真结果如图20～图25所示.

由图20～图24可知,在有多个节点且攻击矢量时变时,所提出的方法仍然可保证较高的识别率和较小的均方误差. 图25展示了不同时刻的两个新个体与集群内部节点的状态,可以看出:集群在形成后,决策出了新个体a为威胁节点,顺利躲避了新个体;决策出了新个体b为第3类个体节点,并允许其加入.

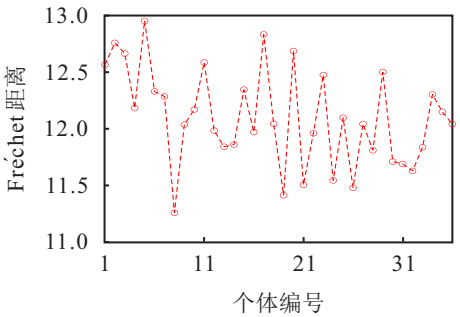


(a) 个体a

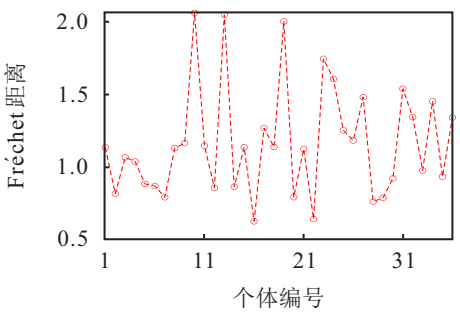


(b) 个体b

图 20 场景4下两个新个体的攻击识别率

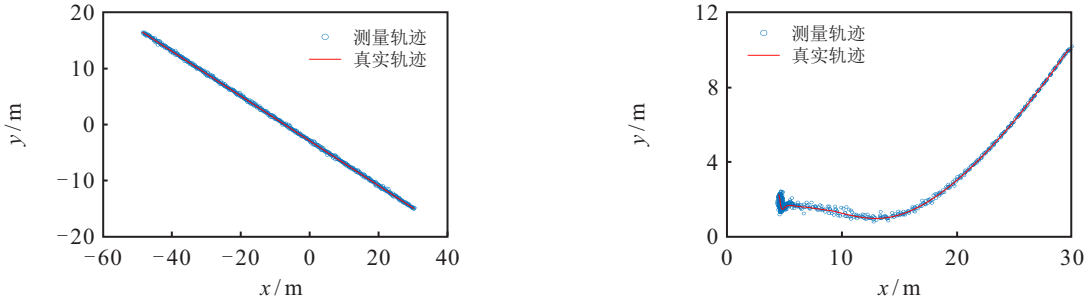


(a) 个体a



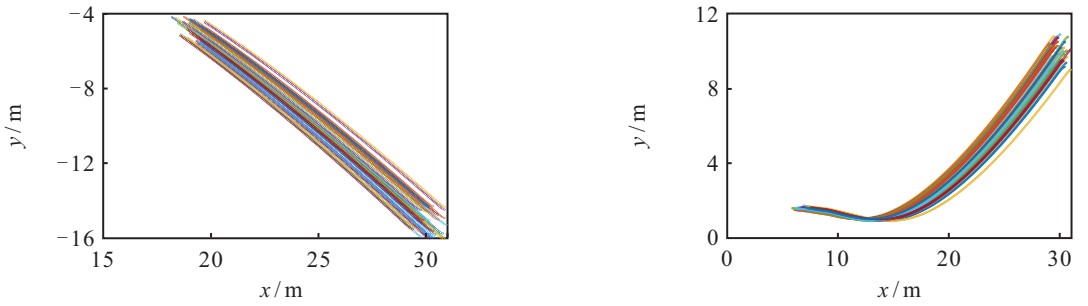
(b) 个体b

图 21 场景4下两个新个体的测量轨迹与预测轨迹的Fréchet距离



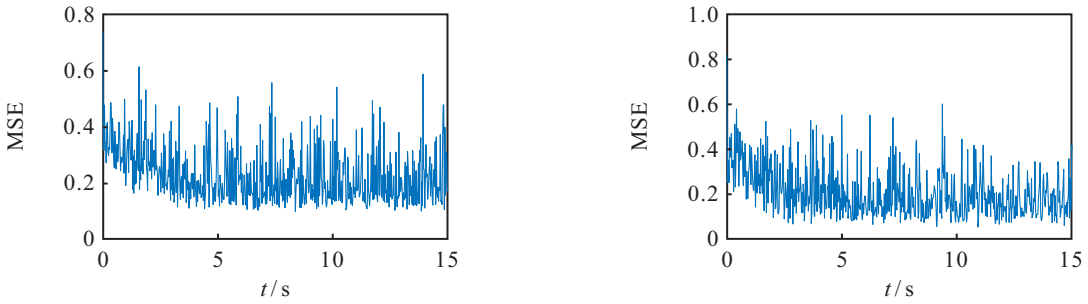
(a) 个体a　　(b) 个体b

图 22　场景4下两个新个体的轨迹测量曲线



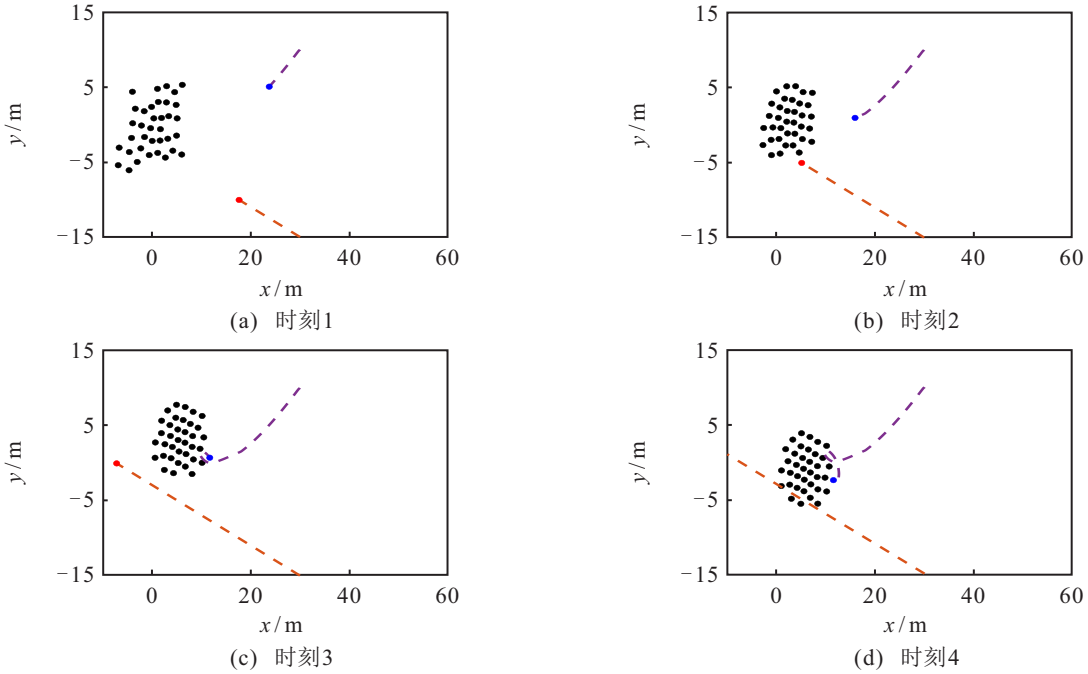
(a) 个体a　　(b) 个体b

图 23　场景4下两个新个体期望轨迹预测值



(a) 个体a　　(b) 个体b

图 24　场景4下两个新个体轨迹测量的均方误差



(a) 时刻1　　(b) 时刻2

(c) 时刻3　　(d) 时刻4

图 25　场景4下两个节点的中间状态

4 结 论

针对在恶意攻击下根据测量信息与集群运动规律对未知外部个体进行分布式的意图识别问题,本文设计了考虑网络攻击的基于分布式意图识别的集群控制算法. 该算法中,集群内部节点满足集群运动规律的情况下,探测到未知外部个体时,首先内部节点根据设计的攻击识别阈值来判断其是否受到网络攻击,并生成识别因子. 然后,根据设计的基于攻击识别策略的改进分布式卡尔曼滤波算法对外部个体的状态进行分布式状态估计,以最大程度上削弱网络攻击对测量值的影响. 接着,基于Fréchet距离计算期望轨迹与量测轨迹的相似性,利用多数表决的方法进行新个体的意图识别. 最后,通过仿真实验验证了所提出方法可以准确识别未知节点的意图,保证集群安全.

参考文献(References)

[1] Reynolds C W. Flocks, herds and schools: A distributed behavioral model[J]. ACM SIGGRAPH Computer Graphics, 1987, 21(4): 25-34.

[2] Olfati-Saber R. Distributed Kalman filtering for sensor networks[C]. 2007 46th IEEE Conference on Decision and Control. New Orleans, 2007: 5492-5498.

[3] 张岱峰, 段海滨. 恶意攻击下基于分布式稀疏优化的安全状态估计[J]. 自动化学报, 2021, 47(4): 813-824.
(Zhang D F, Duan H B. Secure state estimation based on distributed sparse optimization under malicious attacks[J]. Acta Automatica Sinica, 2021, 47(4): 813-824.)

[4] 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(C): 44-50.

[5] Xin D J, Shi L F, Yu X K. Distributed Kalman filter with faulty/reliable sensors based on Wasserstein average consensus[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2022, 69(4): 2371-2375.

[6] 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.

[7] Ma L F, Wang Z D, Han Q L, et al. Variance-constrained distributed filtering for time-varying systems with multiplicative noises and deception attacks over sensor networks[J]. IEEE Sensors Journal, 2017, 17(7): 2279-2288.

[8] Zhang X L, Yang W J. Trajectory privacy protection method based on Fréchet distance function[J]. Journal of Beijing University of Technology, 2021, 47(2): 127-134.

[9] 徐博, 王朝阳, 王潇雨, 等. 通信随机时滞条件下基于分布式模型预测的AUV编队控制[J]. 控制与决策, 2023, 38(5): 1363-1372.
(Xu B, Wang Z Y, Wang X Y, et al. AUV formation control with communication stochastic delay based on distributed model prediction[J]. Control and Decision, 2023, 38(5): 1363-1372.)

[10] 王祥科, 陈浩, 赵述龙. 大规模固定翼无人机集群编队控制方法[J]. 控制与决策, 2021, 36(9): 2063-2073.
(Wang X K, Chen H, Zhao S L. Formation control of large-scale fixed-wing unmanned aerial vehicle swarms[J]. Control and Decision, 2021, 36(9): 2063-2073.)

[11] Poornima I A, Paramasivan B. Anomaly detection in wireless sensor network using machine learning algorithm[J]. Computer Communications, 2020, 151(C): 331-337.

[12] 齐小刚, 吴相远, 刘立芳. 无人机集群编队自组网可靠性评估[J]. 控制与决策, 2024, 39(2): 689-696.
(Qi X G, Wu X Y, Liu L F. Reliability evaluation of ad hoc network for UAV swarm formation[J]. Control and Decision, 2024, 39(2): 689-696.)

[13] Muruganandam S, Joshi R, Suresh P, et al. A deep learning based feed forward artificial neural network to predict the K-barriers for intrusion detection using a wireless sensor network[J]. Measurement: Sensors, 2023, 25: 100613.

[14] 敖伟, 宋永端, 温长云. 受攻击信息物理系统的分布式安全状态估计与控制——一种有限时间方法[J]. 自动化学报, 2019, 45(1): 174-184.
(Ao W, Song Y D, Wen C Y. Distributed secure state estimation and control for CPSs under sensor attacks — A finite time approach[J]. Acta Automatica Sinica, 2019, 45(1): 174-184.)

[15] Manandhar K, Cao X J, Hu F, et al. Combating false data injection attacks in smart grid using Kalman filter[C]. 2014 International Conference on Computing, Networking and Communications. Honolulu, 2014: 16-20.

[16] Li Y Z, Shi L, Cheng P, et al. Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach[J]. IEEE Transactions on Automatic Control, 2015, 60(10): 2831-2836.

[17] 夏国清, 孙显信, 任哲达. 基于状态反馈控制器的多无人水面船集群控制[J]. 控制与决策, 2023, 38(7): 2028-2034.
(Xia G Q, Sun X X, Ren Z D. Swarm control for multiple unmanned surface vehicles system based on state feedback controller[J]. Control and Decision, 2023, 38(7): 2028-2034.)

[18] 张祥银, 夏爽, 张天. 基于自适应遗传学习粒子群算法的多无人机协同任务分配[J]. 控制与决策, 2023, 38(11): 3103-3111.
(Zhang X Y, Xia S, Zhang T. Adaptive genetic learning particle swarm optimization based cooperative task allocation for multi-UAVs[J]. Control and Decision, 2023, 38(11): 3103-3111.)

作者简介

张祥银(1986−), 男, 副教授, 博士, 博士生导师, 主要研究方向为无人系统自主控制与决策优化、群智能优化、机器人控制, E-mail: xy_zhang@bjut.edu.cn;

张曦梁(2000−), 男, 硕士生, 主要研究方向为群智能优化, E-mail: S202373087@emails.bjut.edu.cn;

张天(1997−), 男, 硕士生, 主要研究方向为多机器人编队控制, E-mail: tian_zhang@emails.bjut.edu.cn.