扩展卡尔曼滤波在受到恶意攻击系统中的状态估计

周 雪 [1] 张 皓 [1] 王祝萍 [1]

摘 要 设计了一种分布式扩展卡尔曼滤波器 (Extended Kalman filter, EKF), 对非线性目标状态进行估计. 在设计过程中, 对滤波误差上界进行优化, 获得了最优滤波增益. 此外, 在通信过程中, 考虑恶意攻击信号的同时引入了分布式事件触发机制, 使得系统在保持一定的估计精度的情况下节省通信资源. 最后, 以室内的机器人定位问题为例, 验证了提出的滤波器的有效性.

关键词 分布式事件触发, 扩展卡尔曼滤波, 状态估计, 恶意攻击

引用格式 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. 自动化学报, 2020, **46**(1): 38−46

DOI 10.16383/j.aas.c170609

Extended Kalman Filtering in State Estimation Systems With Malicious Attacks

ZHOU Xue[1] ZHANG Hao[1] WANG Zhu-Ping[1]

Abstract A distributed extended Kalman filter (EKF) is designed to estimate the nonlinear target state. In the design process, the optimal filtering gain is obtained by optimizing the upper bound of error covariance. In the process of communication, the distributed event-trigger mechanism is introduced meanwhile the malicious attack signal is considered, so that the system can save the communication resources in the case of maintaining certain estimation accuracy. Finally, an indoor robot localization problem is used to verify the effectiveness of the proposed method.

Key words Distributed event-trigger, extended Kalman filtering (EKF), state estimation, malicious attacks

Citation Zhou Xue, Zhang Hao, Wang Zhu-Ping. Extended Kalman filtering in state estimation systems with malicious attacks. *Acta Automatica Sinica*, 2020, **46**(1): 38−46

近年来, 无线传感器网络的状态估计问题在军事监测、智能交通、目标定位等方面取得了极大的应用[1−5]. 受到多智能体领域研究的启发[6−7], 一致性理论在传感器网络中也取得了许多研究成果. Yu 研究了一种基于一致性的混合卡尔曼滤波, 将粒子滤波与传统卡尔曼滤波相结合通过分布式估计来获得条件线性系统的状态[4]. Liu 等提出了一种基于一致性的迭代的分布式卡尔曼滤波方法, 以抵御随机的非线性扰动[8]. 但是在以上提及的这些研究中, 都没有考虑到网络的安全问题. 然而, 近年来随着网络攻击事件不断上升, 无线传感器网络的安全研究已成为一个不可忽视的重要方面. 针对三种主流的恶意攻击方式, 即拒绝服务攻击 (DoS)[9]、欺骗攻击[10]和重放攻击[11], 已做出了许多具体的研究. Zhang 等[12] 从一个攻击者的角度研究了最优的 DoS 攻击策略, 使得攻击者能在有限能量的情况下对目标系统造成最大的伤害. 而 Ding 等[13] 则研究了受到拒绝服务攻击和欺骗攻击的系统的基于事件的安全控制, 提出了均方安全域的概念来量化安全程度.

此外, 由于传统卡尔曼滤波只能对线性系统进行滤波, 而实际中的系统多为非线性的, 所以其应用受到很大限制. 因此, Stanley Schmidt 提出了扩展卡尔曼滤波 (Extended Kalman filtering, EKF). 目前, 对于扩展卡尔曼滤波的研究, 已经存在相当多的文献. 但是在这些文献中鲜有考虑到网络的安全问题[14−15]. 针对这一点, 我们萌生了在网络受到欺骗攻击的情况下设计有效的扩展卡尔曼滤波器以抵御攻击信号, 实现目标定位这一想法.

此外, 由于传感器主要采用电池供电, 而其更换又十分不便, 所以, 节省传感器网络的能量消耗十分必要. 事件触发机制能够有效地解决这一问题. 基于事件的方法可以使得估计器在缺少测量信息的情况下, 仍然能够从已知数据中获得目标的状态信息, 所以能在减少通信能耗的情况下保持估计的准确性[16]. 目前, 基本的事件触发方式有基于状态的事件触发[17]、基于时间的事件触发[18] 以及绝对触发[19]. 而这些触发方式在无线传感器网络中也已经有相当多的应用与研究[20−21]. Zhang 等[21]

收稿日期 2017-11-03 录用日期 2018-06-09
Manuscript received November 3, 2017; accepted June 9, 2018
国家自然科学基金 (61922063, 61773289), 上海自然科学基金 (17ZR1445800, 19ZR1461400), 上海曙光计划 (18SG18) 资助
Support by National Natural Science Foundation of China (61922063, 61773289), Shanghai Natural Science Foundation (17ZR1445800, 19ZR1461400), and Shanghai Shuguang Project (18SG18)
本文责任编委 张军平
Recommended by Associate Editor ZHANG Jun-Ping
1. 同济大学控制科学与工程系 上海 200092
1. Department of Control Science and Engineering, Tongji University, Shanghai 200092

研究了一类基于 RSSI (Received signal strength indication) 测距的分布式移动目标跟踪问题, 在此基础上提出了一种适用于事件触发无线传感器网络的分布式随机目标跟踪方法, 可以使得在减少通信的情况下获得良好的跟踪效果. 而 Zhang 等[21] 则将事件触发机制应用于一类耗散控制系统中以降低通信资源. 通过上述文献的研究, 可知事件触发在节省传感器之间通信能量的同时, 能保持良好的估计性能, 因此在本文中我们考虑将其应用于估计非线性目标状态的滤波网络中, 以延长传感器的使用寿命.

在考虑了以上提及的所有情况后, 我们设计了一种基于事件触发的扩展卡尔曼滤波器, 其能够在受到网络攻击的情况下进行有效的滤波, 从而获得目标的状态. 本文的贡献主要有: 1) 在分布式扩展卡尔曼滤波中引入事件触发机制, 能够在保证估计效果的前提下有效地节省传感器的能量, 延长传感器的使用寿命. 2) 考虑了网络的欺骗攻击, 使得设计的滤波器能抵抗恶意攻击.

符号: $\otimes$ 代表克罗内克积, $\mathrm{col}_N\{\cdot\}$ 代表 N 列元素, $\mathrm{diag}_N\{\cdot\}$ 代表对角线有 N 个元素的方阵.

1　问题描述

无线传感器网络的通信拓扑图可以定义为有向图 $\mathcal{G}=\{\mathcal{V},\mathcal{E},\mathcal{A}\}$. 其由 $\mathcal{V}=\{1,2,\cdots,n\}$ 个节点以及 $\mathcal{E}\subseteq\mathcal{V}\times\mathcal{V}$ 条边组成, 边 (i,j) 的存在表示节点 i, j 之间可以互相通信, 节点 i 的邻居集合表示为 $\mathcal{N}_i=\{j;(i,j)\in\mathcal{V}\}$, 非负矩阵 $\mathcal{A}(k)=[a_{ij}(k)]$ 为邻接矩阵, 如果 $(i,j)\in\mathcal{E}$, $a_{ij}(k)=1$, 反之, $a_{ij}(k)=0$, 图 $\mathcal{G}$ 的度矩阵定义为 $\mathcal{D}(k)=\mathrm{diag}\{\mathcal{D}_1(k),\mathcal{D}_2(k),\cdots,\mathcal{D}_n(k)\}$, 则拉普拉斯矩阵 $\mathcal{L}(k)=\mathcal{D}(k)-\mathcal{A}(k)$.

首先给出滤波网络的事件触发与欺骗攻击示意图, 见图 1. 每个采样时刻, 测量值和时刻值合并成一个数据包通过信道传输给滤波器, 只有当达到事件触发条件时, 才能传输成功, 滤波器在接收到事件触发时刻的测量值后, 将最新一次的数据包保存在零阶保持器中, 等待其他邻居节点来获取. 而在传输过程中, 攻击者可能会通过修改测量值来破坏滤波网络的有效性.

注 1. 从图 1 可以看出基于事件触发的扩展 Kalman 滤波与传统扩展 Kalman 滤波的本质区别就在于, 传感器并不是在每个采样时刻都会将测量的数据传输给远程的滤波器, 只有当传感器的测量值与测量的估计值之间的差值超过某一可接受的值时, 传感器才会传输测量值. 而相对于传统扩展 Kalman 滤波来说, 基于事件触发的扩展 Kalman 滤波的主要优势为在保证了一定的估计精度的情况下降低了通信率, 节省了系统能耗.

考虑一个具有 n 个传感器的网络, 观测目标及测量输出分别表示为

$$\boldsymbol{x}_{k+1}=f(\boldsymbol{x}_k)+\boldsymbol{\omega}_k \tag{1}$$

$$\boldsymbol{y}_{i,k}=h_i(\boldsymbol{x}_k)+\boldsymbol{v}_{i,k},\quad i=1,2,\cdots,n \tag{2}$$

其中, $\boldsymbol{x}_k\in\mathbf{R}^{n_x}$ 为目标状态, $\boldsymbol{y}_{i,k}\in\mathbf{R}^{n_y}$ 为不同传感器的测量值, $\boldsymbol{\omega}_k\in\mathbf{R}^{n_\omega}$ 为过程噪声, $\boldsymbol{v}_{i,k}\in\mathbf{R}^{n_v}$ 为量测噪声. $\boldsymbol{\omega}_k$ 和 $\boldsymbol{v}_{i,k}$ 均为零均值高斯白噪声. $\boldsymbol{\omega}_k$ 的协方差记为 Q_k, 不同时刻的 $\boldsymbol{\omega}$ 互不相关. $\boldsymbol{v}_{i,k}$ 的协方差记为 $R_{i,k}$, 不同时刻, 不同传感器之间的 $\boldsymbol{v}$ 互不相关. $f(\cdot)$ 和 $h_i(\cdot)$ 是二次连续可微的非线性函数. 此外, 定义新息序列

$$\boldsymbol{z}_{i,k}=\boldsymbol{y}_{i,k}-h_i(\hat{\boldsymbol{x}}_{i,k})$$

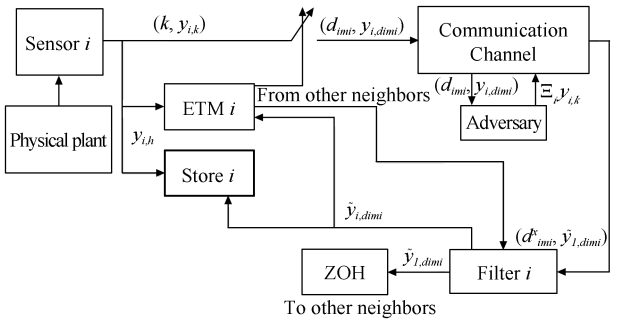

图 1　带有事件触发的滤波网络攻击示意图

Fig. 1　The diagram of attacks on an event-based filtering network

将欺骗攻击信号表示为

$$\vec{\boldsymbol{y}}_{i,k}=-\boldsymbol{y}_{i,k}+\boldsymbol{\vartheta}_{i,k} \tag{3}$$

其中, $\boldsymbol{\vartheta}_{i,k}$ 满足高斯分布, 这是为了与噪声信号混淆, 以起到欺骗效果. 此外, $\boldsymbol{\vartheta}_{i,k}$ 具有上界 $\bar{\boldsymbol{\vartheta}}_{i,k}$, 当此上界超过一定值时, 滤波器无法抵御攻击信号, 此上界可通过大量仿真来确定. 由于实际传输过程中受到信道衰退, 信号量化等限制[5], 所以实际的攻击信号可以表示为 $\Xi_{i,k}\vec{\boldsymbol{y}}_{i,k}$. 其中 $\Xi_{i,k}=\mathrm{diag}\{\xi_{i,1,k},\xi_{i,2,k},\cdots,\xi_{i,s,k}\}$, 而且 $\Xi_{i,k}$ 的每一个元素都有上下界

$$0\le\underline{\xi}_{i,s,k}\le\xi_{i,s,k}\le\bar{\xi}_{i,s,k}<\infty,\quad s=1,2,\cdots,n_y \tag{4}$$

由于攻击信号在信道中传输时会衰减或放大, 所以, $\xi_{i,s,k}$ 的上下界取值为 $0\le\underline{\xi}_{i,s,k}<1$, $\bar{\xi}_{i,s,k}>1$. $0\le\underline{\xi}_{i,s,k}<1$ 表示在 k 时刻, 攻击信号传输到第 i 个传感器的第 s 个分量通过信道时信号衰减. 而 $\bar{\xi}_{i,s,k}>1$ 表示信号放大.

注 2. 考虑到攻击者以修改测量信息为手段来发动欺骗攻击, 因此假设攻击者知道测量信号. 根据文献 [12], 由于攻击者具有有限的能量, 所以在发动一次攻击时, 其需要在能量耗尽之前停止, 在一次攻击结束之后, 攻击者需要储存能量, 为下一次攻击做准备, 而存储的能量大小取决于下一次攻击的时长. 具体的时间以及能量大小与发动攻击的规模大小以及其自身性能有关. 此外, 与文献 [13] 相比, 本文中的攻击信号是时变的, 这意味着并不是在每一个时刻, 攻击者都会发起进攻, 这更加符合实际情况.

考虑到如上讨论的欺骗攻击, 实际的测量输出可以表示为

$$\begin{aligned}\tilde{\boldsymbol{y}}_{i,k} =& \boldsymbol{y}_{i,k} + \Xi_{i,k}\vec{\boldsymbol{y}}_{i,k} = \\ & (I-\Xi_{i,k})\boldsymbol{y}_{i,k} + \Xi_{i,k}\boldsymbol{\vartheta}_{i,k}\end{aligned} \tag{5}$$

则实际的新息表示为

$$\tilde{\boldsymbol{z}}_{i,k} = \tilde{\boldsymbol{y}}_{i,k} - h_i(\hat{\boldsymbol{x}}_{i,k}) \tag{6}$$

为了对目标进行定位, 设计如下的分布式滤波器:

$$\begin{aligned}\hat{\boldsymbol{x}}_{i,k+1} =& f(\hat{\boldsymbol{x}}_{i,k}) + K_{i,k}[\tilde{\boldsymbol{y}}_{i,k} - h(\hat{\boldsymbol{x}}_{i,k})] + \\ & C_{i,k}\sum_{j\in\mathcal{N}_i}(\tilde{\boldsymbol{z}}_{j,k} - \tilde{\boldsymbol{z}}_{i,k})\end{aligned} \tag{7}$$

其中, $K_{i,k}$ 为滤波器增益矩阵, $C_{i,k}$ 为一致性增益矩阵. 它们都是待设计的矩阵.

传感器的能量消耗主要集中在通信部分, 所以如何节省通信能量显得尤为重要, 而事件触发机制已被广泛证明是一种节省通信消耗的有效方法. 为此, 本文引入事件触发机制, 其描述如下:

$$\begin{aligned}d^i_{m_i+1} \le& \min_{k>d^i_{m_i}}\{k|\boldsymbol{f}^{\mathrm{T}}_{i,k}\Phi_{i,k}\boldsymbol{f}_{i,k} > \\ & \sigma_i\boldsymbol{\Psi}^{\mathrm{T}}_{i,d^i_{m_i}}\tilde{\Phi}_{i,k}\boldsymbol{\Psi}_{i,d^i_{m_i}}\}\end{aligned} \tag{8}$$

其中, $d^i_{m_i}$ 代表上一次事件触发时刻, $\Phi_{i,k}$ 和 $\tilde{\Phi}_{i,k}$ 是两个待设计的对称矩阵, σ_i 是节点 i 的阈值, 用以调整事件触发允许的误差上限, 满足 $\sigma_i \in (0,1)$, $\boldsymbol{\Psi}_{i,d^i_{m_i}} = \sum_{j\in\mathcal{N}_i}(\tilde{\boldsymbol{z}}_{j,d^j_{m_j}} - \tilde{\boldsymbol{z}}_{i,d^i_{m_i}})$, $\boldsymbol{f}_{i,k} = \tilde{\boldsymbol{z}}_{i,k} - \tilde{\boldsymbol{z}}_{i,d^i_{m_i}}$. 在引入事件触发机制之后, 式 (7) 中的滤波器可以重新表示为

$$\begin{aligned}\hat{\boldsymbol{x}}_{i,k+1} =& f(\hat{\boldsymbol{x}}_{i,k}) + K_{i,k}[\tilde{\boldsymbol{y}}_{i,d^i_{m_i}} - h_i(\hat{\boldsymbol{x}}_{i,d^i_{m_i}})] + \\ & C_{i,k}\boldsymbol{\Psi}_{i,d^i_{m_i}}\end{aligned} \tag{9}$$

注 3. 与大部分现存的文献 [2, 8, 21] 不同, 本文设计的滤波器的一致性项中, 节点之间交换的是新息序列 $\tilde{\boldsymbol{z}}_{i,k}$ 而不是测量值 $\boldsymbol{y}_{i,k}$, 这使得我们的滤波器对不稳定的系统仍能够进行有效的滤波.

注 4. 在滤波网络中, 不仅信息交换是分布式的, 事件触发也是分布式的, 即不同的节点可以具有不同的事件触发时刻.

针对提出的滤波器式 (9), 本文的设计目标之一是设计滤波参数 $\{K_{i,k}\}_{1\le k<N}$ 和 $\{C_{i,k}\}_{1\le k<N}$, 使得如下的不等式成立.

$$\mathrm{E}\{(\boldsymbol{x}_k - \hat{\boldsymbol{x}}_{i,k})(\boldsymbol{x}_k - \hat{\boldsymbol{x}}_{i,k})^{\mathrm{T}}\} \le \phi_{i,k} \tag{10}$$

其中, $\phi_{i,k}$ 表示滤波误差协方差的上界. 另一个目标是在满足 (10) 的条件下, 使得 $\phi_{i,k}$ 最小, 这可以通过解一个最优问题来获得, 具体的设计将在下一节描述.

2 分布式滤波器参数设计

首先, 介绍对接下来的推导有用的引理.

引理 1[22]**.** 令 $\kappa_0(\cdot), \kappa_1(\cdot), \cdots, \kappa_s(\cdot)$ 为变量 $\boldsymbol{\zeta} \in \mathbf{R}^n$ 的二次函数. $\boldsymbol{\zeta}$ 满足 $\kappa_j(\boldsymbol{\zeta}) = \boldsymbol{\zeta}^{\mathrm{T}}T_j\boldsymbol{\zeta}$ ($j = 0, 1, \cdots, s$), 其中, T_j 满足 $T_j = T_j^{\mathrm{T}}$. 如果存在 $\tau_1 \ge 0, \tau_2 \ge 0, \cdots, \tau_s \ge 0$ 使得 $T_0 - \sum_{j=1}^{s}\tau_j T_j \le 0$, 则如下的不等式成立.

$$\kappa_1(\boldsymbol{\zeta}) \le 0, \cdots, \kappa_s(\boldsymbol{\zeta}) \le 0 \Longrightarrow \kappa_0(\boldsymbol{\zeta}) \le 0 \tag{11}$$

引理 2[23]**.** 对于实矩阵 P, $M = M^{\mathrm{T}}$, $R = R^{\mathrm{T}}$, 下面的三个不等式互为等价,

$$\begin{aligned}& M + PR^{-1}P^{\mathrm{T}} \le 0 \\ & \begin{bmatrix} M & P \\ P^{\mathrm{T}} & -R \end{bmatrix} \le 0 \\ & -R - P^{\mathrm{T}}M^{-1}P \le 0\end{aligned}$$

为了方便推导, 将实际的攻击信号 $\Xi_{i,k}\vec{\boldsymbol{y}}_{i,k}$ 重新表示成

$$\Xi_{i,k}\vec{\boldsymbol{y}}_{i,k} = \Xi_{i,k}\vec{\boldsymbol{y}}_{i,k} + \varphi_i(\vec{\boldsymbol{y}}_{i,k}) \tag{12}$$

其中, $\Xi_{i,k} = \mathrm{diag}\{\underline{\xi}_{i,1,k}, \underline{\xi}_{i,2,k}, \cdots, \underline{\xi}_{i,s,k}\}$. 于是,

$$\varphi_i^{\mathrm{T}}(\vec{\boldsymbol{y}}_{i,k})(\varphi_i(\vec{\boldsymbol{y}}_{i,k}) - \tilde{\Xi}_{i,k}\vec{\boldsymbol{y}}_{i,k}) \le 0 \tag{13}$$

其中, $\tilde{\Xi}_{i,k} = \bar{\Xi}_{i,k} - \Xi_{i,k} > 0$ 为正定矩阵. $\varphi_i(\vec{\boldsymbol{y}}_{i,k})$ 为非线性函数, 其满足条件 $\varphi_i(\vec{\boldsymbol{y}}_{i,k}) \in [0, \tilde{\Xi}_{i,k}\vec{\boldsymbol{y}}_{i,k}]$.

注 5. 由前文的描述可知, 攻击信号在范围 $[\Xi_{i,k}\vec{\boldsymbol{y}}_{i,k}, \bar{\Xi}_{i,k}\vec{\boldsymbol{y}}_{i,k}]$ 内, 因此可表示成其下界与一个在 $[0, \tilde{\Xi}_{i,k}\vec{\boldsymbol{y}}_{i,k}]$ 之间的信号的叠加, 而实际攻击信号又是随机的, 可近似为非线性函数. 所以, 在推导过程中, 可将攻击信号表示成式 (12) 的形式.

每一个传感器的滤波误差可以表示为

$$\begin{aligned}\boldsymbol{e}_{i,k+1} = \boldsymbol{x}_{i,k+1} - \hat{\boldsymbol{x}}_{i,k+1} = \\ f(\boldsymbol{x}_k) + \boldsymbol{\omega}_k - f(\hat{\boldsymbol{x}}_{i,k}) - K_{i,k}[\tilde{\boldsymbol{z}}_{i,k} - \boldsymbol{f}_{i,k}] - \\ C_{i,k}\boldsymbol{\Psi}_{i,d^i_{m_i}}\end{aligned} \tag{14}$$

将 $f(\boldsymbol{x}_k)$ 在 $\hat{\boldsymbol{x}}_{i,k}$ 点用泰勒级数展开, 可得

$$f(\boldsymbol{x}_k) = f(\hat{\boldsymbol{x}}_{i,k}) + F_{i,k}\boldsymbol{e}_{i,k} + \mathrm{O}(|\boldsymbol{e}_{i,k}|) \tag{15}$$

其中, $F_{i,k} = \partial f(\boldsymbol{x})/\partial \boldsymbol{x}|_{\boldsymbol{x}=\hat{\boldsymbol{x}}_{i,k}}$. 根据文献 [24], 以上方程中的高阶项可以表示为

$$\mathrm{O}(|\boldsymbol{e}_{i,k}|) = (F_{i,k} + U_{i,k}\Omega_{i,k})\boldsymbol{e}_{i,k} \tag{16}$$

其中, $U_{i,k}$ 是一个已知的放缩矩阵, $\Omega_{i,k}$ 是未知的时变矩阵, 满足 $\Omega^{\mathrm{T}}_{i,k}\Omega_{i,k} \le I$. 由式 (16) 可得

$$f(\boldsymbol{x}_k) - f(\hat{\boldsymbol{x}}_{i,k}) = (F_{i,k} + U_{i,k}\Omega_{i,k})\boldsymbol{e}_{i,k} \tag{17}$$

同理, 有

$$h(\boldsymbol{x}_k) - h(\hat{\boldsymbol{x}}_{i,k}) = (H_{i,k} + V_{i,k}\Theta_{i,k})\boldsymbol{e}_{i,k} \tag{18}$$

其中, $H_{i,k} = \partial h(\boldsymbol{x})/\partial \boldsymbol{x}|_{\boldsymbol{x}=\hat{\boldsymbol{x}}_{i,k}}$, $V_{i,k}$ 是一个已知的放缩矩阵, $\Theta_{i,k}$ 是未知的时变矩阵, 满足 $\Theta^{\mathrm{T}}_{i,k}\Theta_{i,k} \le I$. 将式 (17), 式 (18) 代入式 (14) 得

$$\begin{aligned}\boldsymbol{e}_{i,k+1} = &(F_{i,k} + U_{i,k}\Omega_{i,k})\boldsymbol{e}_{i,k} + \boldsymbol{\omega}_k - \\ &K_{i,k}[\boldsymbol{y}_{i,k} + \Xi_{i,k} \times \vec{\boldsymbol{y}}_{i,k} + \varphi_i(\vec{\boldsymbol{y}}_{i,k}) - \\ &h_i(\hat{\boldsymbol{x}}_{i,k}) - \boldsymbol{f}_{i,k}] - C_{i,k}\boldsymbol{\Psi}_{i,d^i_{m_i}} = \\ &(F_{i,k} + U_{i,k}\Omega_{i,k})\boldsymbol{e}_{i,k} + \boldsymbol{\omega}_k - \\ &K_{i,k}[\boldsymbol{y}_{i,k} + \Xi_{i,k} \times \vec{\boldsymbol{y}}_{i,k} + \\ &\varphi_i(\vec{\boldsymbol{y}}_{i,k}) - h_i(\hat{\boldsymbol{x}}_{i,k}) - \boldsymbol{f}_{i,k}] - \\ &C_{i,k}\sum_{j\in\mathcal{N}_i}(\tilde{\boldsymbol{z}}_{j,k} - \tilde{\boldsymbol{z}}_{i,k} + \boldsymbol{f}_{i,k} - \boldsymbol{f}_{j,k})\end{aligned} \tag{19}$$

将新息式 (6) 代入式 (19) 得

$$\begin{aligned}\boldsymbol{e}_{i,k+1} = &(F_{i,k} + U_{i,k}\Omega_{i,k})\boldsymbol{e}_{i,k} + \boldsymbol{\omega}_k - \\ &K_{i,k}[(I - \Xi_{i,k}) \times (H_{i,k} + V_{i,k}\Theta_{i,k})\boldsymbol{e}_{i,k} + \\ &(I - \Xi_{i,k})\boldsymbol{v}_{i,k} + \Xi_{i,k}\boldsymbol{\vartheta}_{i,k} + \varphi_i(\vec{\boldsymbol{y}}_{i,k}) - \\ &\Xi_{i,k}h_i(\hat{\boldsymbol{x}}_{i,k}) - \boldsymbol{f}_{i,k}] - C_{i,k}\sum_{j\in\mathcal{N}_i}(\tilde{\boldsymbol{y}}_{j,k} - \\ &h_j(\hat{\boldsymbol{x}}_{j,k}) - \tilde{\boldsymbol{y}}_{i,k} + h_i(\hat{\boldsymbol{x}}_{i,k}) + \boldsymbol{f}_{i,k} - \boldsymbol{f}_{j,k})\end{aligned} \tag{20}$$

将式 (20) 写成紧凑形式,

$$\begin{aligned}\boldsymbol{e}_{k+1} = &[\tilde{F}_k + \Omega_k - K_k(I - \Xi_k)(H_k + \Theta_k)]\boldsymbol{e}_k + \\ &\tilde{\boldsymbol{\omega}}_k - K_k[(I - \Xi_k)\tilde{\boldsymbol{v}}_k + \Xi_k\boldsymbol{\vartheta}_k + \boldsymbol{\varphi}_k - \boldsymbol{f}_k] - \\ &\Xi_k h(\hat{\boldsymbol{x}}_k)] - C_k\bar{L}_k[\tilde{\boldsymbol{y}}_k - h(\hat{\boldsymbol{x}}_k) - \boldsymbol{f}_k]\end{aligned} \tag{21}$$

其中

$$\begin{aligned}\tilde{\boldsymbol{y}}_k - h(\hat{\boldsymbol{x}}_k) = &(I - \Xi_k)(H_k + \Theta_k)\boldsymbol{e}_k + (I - \Xi_k)\tilde{\boldsymbol{v}}_k + \\ &\Xi_k\boldsymbol{\vartheta}_k + \boldsymbol{\varphi}_k - \Xi_k h(\hat{\boldsymbol{x}}_k)\end{aligned} \tag{22}$$

将其代入式 (21) 得到

$$\begin{aligned}\boldsymbol{e}_{k+1} = &[\tilde{F}_k + \Omega_k - K_k(I - \Xi_k)(H_k + \Theta_k)]\boldsymbol{e}_k + \\ &\tilde{\boldsymbol{\omega}}_k - K_k[(I - \Xi_k)\tilde{\boldsymbol{v}}_k + \Xi_k\boldsymbol{\vartheta}_k + \boldsymbol{\varphi}_k - \boldsymbol{f}_k - \\ &\Xi_k h(\hat{\boldsymbol{x}}_k)] - C_k\bar{L}_k[(I - \Xi_k)(H_k + \Theta_k)\boldsymbol{e}_k + \\ &(I - \Xi_k)\tilde{\boldsymbol{v}}_k + \Xi_k\boldsymbol{\vartheta}_k + \boldsymbol{\varphi}_k - \Xi_k h(\hat{\boldsymbol{x}}_k) - \boldsymbol{f}_k]\end{aligned} \tag{23}$$

其中

$$\begin{aligned}&\boldsymbol{f}_k = \mathrm{col}_N\{\boldsymbol{f}_{i,k}\}, \boldsymbol{e}_k = \mathrm{col}_N\{\boldsymbol{e}_{i,k}\}, \tilde{\boldsymbol{\omega}}_k = \mathrm{col}_N\{\boldsymbol{\omega}_k\} \\ &\tilde{\boldsymbol{v}}_k = \mathrm{col}_N\{\boldsymbol{v}_{i,k}\}, \boldsymbol{\vartheta}_k = \mathrm{col}_N\{\boldsymbol{\vartheta}_{i,k}\}, \hat{\boldsymbol{x}}_k = \mathrm{col}_N\{\hat{\boldsymbol{x}}_{i,k}\} \\ &\boldsymbol{\varphi}_k = \mathrm{col}_N\{\varphi_i(\vec{\boldsymbol{y}}_{i,k})\}, \quad h(\hat{\boldsymbol{x}}_k) = \mathrm{col}_N\{h_i(\hat{\boldsymbol{x}}_{i,k})\} \\ &\tilde{F}_k = \mathrm{diag}_N\{F_{i,k}\}, \quad \Omega_k = \mathrm{diag}_N\{U_{i,k}\Omega_{i,k}\} \\ &K_k = \mathrm{diag}_N\{K_{i,k}\}, \quad \Xi_k = \mathrm{diag}_N\{\Xi_{i,k}\} \\ &H_k = \mathrm{diag}_N\{H_{i,k}\}, \quad \Theta_k = \mathrm{diag}_N\{V_{i,k}\Theta_{i,k}\} \\ &C_k = \mathrm{diag}_N\{C_{i,k}\}, \quad \bar{L}_k = \mathcal{L}(k) \otimes I_{ny}\end{aligned}$$

接下来, 将给出主要结论.

定理 1. 给定滤波误差协方差上界 $\{\phi_k\}_{1\le k<N}$, 受欺骗攻击的分布式扩展卡尔曼滤波问题可解, 如果存在实矩阵 $\{K_k\}_{1\le k<N}$ 和 $\{C_k\}_{1\le k<N}$, 正定矩阵 $\{\Omega_k\}_{1\le k<N}$, $\{\Theta_k\}_{1\le k<N}$, $\{\Phi_k\}_{1\le k<N}$, $\{\tilde{\Phi}_k\}_{1\le k<N}$, 以及非负系数 $\{\tau_{1,k}\}_{1\le k<N}$ 和 $\{\tau_{2,k}\}_{1\le k<N}$, 使得以下矩阵不等式 (24) 成立.

$$\begin{bmatrix} -\phi_{k+1} & \Lambda_k \\ \Lambda_k^T & -\Delta_k \end{bmatrix} \le 0 \tag{24}$$

其中

$$\begin{aligned}&\Delta_k = \mathrm{diag}\{1,0,0,0,0,0\} - \tau_{1,k}\boldsymbol{\xi}_k^{\mathrm{T}}\Pi_k\boldsymbol{\xi}_k - \\ &\quad \tau_{2,k}\boldsymbol{\xi}_k^{\mathrm{T}}M_k\boldsymbol{\xi}_k \\ &\boldsymbol{\xi}_k^{\mathrm{T}} = [\mathbf{1} \quad \boldsymbol{e}_k^{\mathrm{T}} \quad \tilde{\boldsymbol{v}}_k^{\mathrm{T}} \quad \boldsymbol{\vartheta}_k^{\mathrm{T}} \quad \boldsymbol{f}_k^{\mathrm{T}} \quad \boldsymbol{\varphi}_k^{\mathrm{T}}] \\ &\Pi_k = [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad \Pi_1] \\ &\Lambda_k = (25), \quad \Pi_1^{\mathrm{T}} = (26), \quad M_k = (27) \\ &\Phi_l = \bar{L}_k^{\mathrm{T}}\tilde{\Phi}_k\bar{L}_k, \quad \Theta_l = (I - \Xi_k)(H_k + \Theta_k) \\ &\Phi_k = \mathrm{diag}_N\{\Phi_{i,k}\}, \quad \tilde{\Phi}_k = \mathrm{diag}_N\{\tilde{\Phi}_{i,k}\} \\ &\underline{\sigma} = \mathrm{diag}_N\{\sigma_i\}\end{aligned}$$

证明. 首先根据式 (23), 可以得到

$$\boldsymbol{e}_{k+1} = \Lambda_k\boldsymbol{\xi}_k \tag{28}$$

$$\Lambda_k = \Big[(K_k + C_k\bar{L}_k)\Xi_k h(\hat{\boldsymbol{x}}_k) + \tilde{\boldsymbol{\omega}}_k \quad \Lambda_{11} \quad -K_k(I-\Xi_k) - C_k\bar{L}_k(I-\Xi_k) \quad -K_k\Xi_k - C_k\bar{L}_k\Xi_k \quad K_k - C_k\bar{L}_k \quad -K_k - C_k\bar{L}_k\Big] \tag{25}$$

其中, $\Lambda_{11} = \tilde{F}_k + \Omega_k - (K_k - C_k\bar{L}_k)(I-\Xi)(H_k + \Theta_k)$

$$\Pi_1^{\mathrm{T}} = \Big[(\boldsymbol{y}_k^{\mathrm{T}}\mathrm{diag}_N\{\tilde{\Xi}_i\}\mathrm{col}_{n_xN}\{1\})^{\mathrm{T}} \quad 0 \quad 0 \quad -\mathrm{diag}_N\{\tilde{\Xi}_i\} \quad 0 \quad I_{n_xN,n_xN}\Big] \tag{26}$$

$$M_k = \begin{bmatrix} -h^{\mathrm{T}}(\hat{\boldsymbol{x}}_k)\Xi_k^{\mathrm{T}}\Phi_l\Xi_k h(\hat{\boldsymbol{x}}_k) & h^{\mathrm{T}}(\hat{\boldsymbol{x}}_k)\Xi_k^{\mathrm{T}}\Phi_l\Theta_l & h^{\mathrm{T}}(\hat{\boldsymbol{x}}_k)\Xi_k^{\mathrm{T}}\Phi_l(I-\Xi) & h^{\mathrm{T}}(\hat{\boldsymbol{x}}_k)\Xi_k^{\mathrm{T}}\Phi_l\Xi_k & -h^{\mathrm{T}}(\hat{\boldsymbol{x}}_k)\Xi_k^{\mathrm{T}}\Phi_l & h^{\mathrm{T}}(\hat{\boldsymbol{x}}_k)\Xi_k^{\mathrm{T}}\Phi_l \\ * & -\Theta_l^{\mathrm{T}}\Phi_l\Theta_l & -\Theta_l^{\mathrm{T}}\Phi_l(I-\Xi_k) & \Theta_l^{\mathrm{T}}\Phi_l\Xi_k & \Theta_l^{\mathrm{T}}\Phi_l & -\Theta_l^{\mathrm{T}}\Phi_l \\ * & * & -(I-\Xi_k)^{\mathrm{T}}\Phi_l(I-\Xi_k) & -(I-\Xi_k)^{\mathrm{T}}\Phi_l\Xi_k & (I-\Xi_k)^{\mathrm{T}}\Phi_l & -(I-\Xi_k)^{\mathrm{T}}\Phi_l \\ * & * & * & \Xi_k^{\mathrm{T}}\Phi_l\Xi_k & \Xi_k^{\mathrm{T}}\Phi_l & -\Xi_k^{\mathrm{T}}\Phi_l \\ * & * & * & * & \frac{1}{\underline{\sigma}}\Phi_k - \Phi_l & \Phi_l \\ * & * & * & * & * & -\Phi_l \end{bmatrix} \tag{27}$$

根据事件触发条件 (8) 有

$$\sum_{i=1}^{N}\boldsymbol{f}_{i,k}^{\mathrm{T}}\Phi_{i,k}\boldsymbol{f}_{i,k} \le \sum_{i=1}^{N}\sigma_i\boldsymbol{\Psi}_{i,k}^{\mathrm{T}}\tilde{\Phi}_{i,k}\boldsymbol{\Psi}_{i,k}$$

将其写成紧凑形式可得

$$\boldsymbol{f}_k^{\mathrm{T}}\Phi_k\boldsymbol{f}_k \le \underline{\sigma}(\tilde{\boldsymbol{z}}_k - \boldsymbol{f}_k)^{\mathrm{T}}\bar{L}_k^{\mathrm{T}}\tilde{\Phi}_k\bar{L}_k(\tilde{\boldsymbol{z}}_k - \boldsymbol{f}_k) \tag{29}$$

将式 (22) 代入式 (29), 可得

$$\begin{aligned}\boldsymbol{f}_k^{\mathrm{T}}\Phi_k\boldsymbol{f}_k - \underline{\sigma}[&(I-\Xi_k)(H_k+\Theta_k)\boldsymbol{e}_k + (I-\Xi_k)\times\\ &\tilde{\boldsymbol{v}}_k + \Xi_k\boldsymbol{\vartheta}_k + \boldsymbol{\varphi}_k - \Xi_k h(\hat{\boldsymbol{x}}_k) - \boldsymbol{f}_k]^{\mathrm{T}}\bar{L}_k^{\mathrm{T}}\tilde{\Phi}_k\bar{L}_k\times\\ &[(I-\Xi_k)(H_k+\Theta_k)\boldsymbol{e}_k + (I-\Xi_k)\tilde{\boldsymbol{v}}_k +\\ &\Xi_k\boldsymbol{\vartheta}_k + \boldsymbol{\varphi}_k - \Xi_k h(\hat{\boldsymbol{x}}_k) - \boldsymbol{f}_k] \le 0\end{aligned}$$

整理得

$$\boldsymbol{\xi}_k^{\mathrm{T}}M_k\boldsymbol{\xi}_k \le 0 \tag{30}$$

现在考虑欺骗攻击信号, 根据式 (2)、(3) 和式 (13) 有

$$\begin{aligned}\varphi_i^{\mathrm{T}}(\vec{\boldsymbol{y}}_{i,k})(&\varphi_i(\vec{\boldsymbol{y}}_{i,k}) + \tilde{\Xi}_{i,k}h_i(\boldsymbol{x}_{i,k}) +\\ &\tilde{\Xi}_{i,k}\boldsymbol{v}_{i,k} - \tilde{\Xi}_{i,k}\boldsymbol{\vartheta}_{i,k}) \le 0\end{aligned}$$

上式表示为紧凑形式为

$$\boldsymbol{\varphi}_k^{\mathrm{T}}(\boldsymbol{\varphi}_k + \tilde{\Xi}_k h(\boldsymbol{x}_k) + \tilde{\Xi}_k\tilde{\boldsymbol{v}}_k - \tilde{\Xi}_k\boldsymbol{\vartheta}_k) \le 0 \tag{31}$$

式 (31) 等价于

$$\boldsymbol{\xi}_k^{\mathrm{T}}\Pi_k\boldsymbol{\xi}_k \le 0 \tag{32}$$

根据引理 1 可知, 如果存在系数 $\tau_{1,k} \ge 0$ 和 $\tau_{2,k} \ge 0$ 使得 $\Lambda_k^{\mathrm{T}}\phi_{k+1}^{-1}\Lambda_k - \mathrm{diag}\{1,0,0,0,0,0\} - \tau_{1,k}\boldsymbol{\xi}_k^{\mathrm{T}}\Pi_k\boldsymbol{\xi}_k - \tau_{2,k}\boldsymbol{\xi}_k^{\mathrm{T}}M_k\boldsymbol{\xi}_k \le 0$ 成立, 则有

$$\boldsymbol{\xi}_k^{\mathrm{T}}(\Lambda_k^{\mathrm{T}}\phi_{k+1}^{-1}\Lambda_k - \mathrm{diag}\{1,0,0,0,0,0\})\boldsymbol{\xi}_k \le 0$$

所以

$$\boldsymbol{\xi}_k^{\mathrm{T}}\Lambda_k^{\mathrm{T}}\phi_{k+1}^{-1}\Lambda_k\boldsymbol{\xi}_k - 1 \le 0 \tag{33}$$

将式 (28) 代入式 (33) 得

$$\boldsymbol{e}_{k+1}^{\mathrm{T}}\phi_{k+1}^{-1}\boldsymbol{e}_{k+1} - 1 \le 0$$

根据 Schur 补引理[23] 有

$$\begin{bmatrix} -1 & \boldsymbol{e}_{k+1}^{\mathrm{T}} \\ \boldsymbol{e}_{k+1} & -\phi_{k+1} \end{bmatrix} \le 0.$$

由此可得

$$\mathrm{E}\{\boldsymbol{e}_{k+1}^{\mathrm{T}}\boldsymbol{e}_{k+1}\} \le \phi_{k+1} \tag{34}$$

于是, 设计的滤波器的误差具有一个上界. □

接下来, 为了在每一个时刻都能确定预先设定的滤波误差协方差的上界, 以获得最好的目标定位效果, 形成了如下的最优问题.

推论 1. 给定滤波误差协方差上界 $\{\phi_k\}_{1\le k<N}$, 受欺骗攻击的分布式扩展卡尔曼滤波问题可解, 如果存在实矩阵 $\{K_k\}_{1\le k<N}$ 和 $\{C_k\}_{1\le k<N}$, 正定矩阵 $\{\Omega_k\}_{1\le k<N}$, $\{\Theta_k\}_{1\le k<N}$, $\{\Phi_k\}_{1\le k<N}$, $\{\tilde{\Phi}_k\}_{1\le k<N}$, 以及非负系数 $\{\tau_{1,k}\}_{1\le k<N}$ 和 $\{\tau_{2,k}\}_{1\le k<N}$, 使得以下最优问题 (35) 成立.

$$\min_{\phi_{k+1},K_k,\tau_{1,k},\tau_{2,k},\Phi_k,\tilde{\Phi}_k,\Omega_k,\Theta_k,C_k} \mathrm{tr}(\phi_{k+1}) \tag{35}$$

$$\text{满足} \begin{bmatrix} -\phi_{k+1} & \Lambda_k \\ \Lambda_k^{\mathrm{T}} & -\Delta_k \end{bmatrix} \le 0$$

注 6. 在本文中, 滤波器增益 $K_{i,k}$ 采用在线计算方式, 虽然会降低定位的实时性, 但是由于攻击信号是时变的, 所以这种在线计算方式能有效抵御攻击, 以获得最好的滤波效果. 不过如果恶意攻击不是时变的话, 也可以将本文中对 $K_{i,k}$ 的计算推广到离线方式, 以提高实时性.

为了使滤波方法阐述更明确, 给出如下的滤波算法伪代码.

算法 1. 滤波算法

1: 初始化: 随机给定状态初始值 $\boldsymbol{x}_0$ 与估计初始值 $\boldsymbol{x}_{i,0}$;
2: for $k = 1 : M$
3: 根据式 (3) 和 (4), 利用传感器的测量值以及随机生成的满足高斯分布的 $\boldsymbol{\vartheta}_{i,k}$ 产生欺骗信号, 并且设定信号限制系数 $\underline{\xi}_{i,s,k}$ 和 $\bar{\xi}_{i,s,k}$, 设定未知数 $K_k, \tau_{1,k}, \tau_{2,k}, \Phi_k, \tilde{\Phi}_k, \Omega_k, \Theta_k, C_k$;
4: 根据式 (1) 和 (9) 产生 $\boldsymbol{x}_k$ 及其估计值 $\boldsymbol{x}_{i,k}$, 并计算 $\boldsymbol{e}_k$;
5: 根据迭代式 (19), 计算得到误差协方差 $\phi_{k+1} = \boldsymbol{e}_{k+1}\boldsymbol{e}_{k+1}^{\mathrm{T}}$;
6: 根据推论 1 的最优问题, 计算出最优解 ϕ_{k+1}, K_k, $\tau_{1,k}$, $\tau_{2,k}$, Φ_k, $\tilde{\Phi}_k$, Ω_k, Θ_k, C_k, 将其重新代入 (7), 得到状态的估计值, 再根据事件触发公式 (8) 计算出触发时刻;
7: end

3　仿真

采用 8 个摄像头对移动机器人进行室内定位以验证本文所提出的目标定位算法的有效性. 机器人的运动学模型表示如下[25]:

$$x_{k+1} = x_k + \frac{s_k^R + s_k^L}{2}\cos\theta_k + \omega_k^x \tag{36}$$

$$y_{k+1} = y_k + \frac{s_k^R + s_k^L}{2}\sin\theta_k + \omega_k^y \tag{37}$$

$$\theta_{k+1} = \theta_k + \frac{s_k^R - s_k^L}{b} + \omega_k^\theta \tag{38}$$

其中, (x_k, y_k) 代表机器人的位置信息, θ_k 代表机器人的转向. (s_k^R, s_k^L) 代表在时间段 $(k, k+1)$ 内, 机器人的左右轮驶过的距离. b 表示左右轮之间的距离, 在本文中, 取 $b = 1.5$. $\boldsymbol{\omega}_k = (\omega_k^x, \omega_k^y, \omega_k^\theta)$ 为零均值高斯白噪声, 其协方差为 Q_k.

在对机器人定位的过程中, 采用 8 个摄像头, 其拓扑结构如图 2 所示. 每个摄像头的测量方程表示如下,

$$p_{i,k} = \frac{\gamma_u}{z_f^c}[-(x_{i,k} - x_k)\sin\theta_k + (y_{i,k} - y_k)\cos\theta_k - d_2] + p_0 + v_{i,k}^p \tag{39}$$

$$q_{i,k} = \frac{\gamma_v}{z_f^c}[-(x_{i,k} - x_k)\cos\theta_k - (y_{i,k} - y_k)\sin\theta_k - d_1] + q_0 + v_{i,k}^q \tag{40}$$

其中, $(p_{i,k}, q_{i,k})$ 代表像平面上的目标的坐标, (d_1, d_2) 为机器人在自身坐标系下的坐标. z_f^c 表示摄像头的视觉中心到目标的距离. γ_u 和 γ_v 代表像素放大系数. (p_0, q_0) 是摄像头主点的图像坐标. $(x_{i,k}, y_{i,k})$ 代表每一个摄像头的位置坐标. $\boldsymbol{v}_{i,k} = (v_{i,k}^p, v_{i,k}^q)$ 为零均值高斯白噪声, 具有协方差 $R_{i,k}$. 仿真过程中, 以上参数取值为: $d_1 = -0.0668$, $d_2 = 0.0536$, $z_f^c = 2.1050$, $\gamma_u = 9.0213283$, $\gamma_v = 9.0250141$, $p_0 = 347.20436$, $q_0 = 284.34750$, $Q_k = \mathrm{diag}\{1, 1, 1\}$, $R_{i,k} = \mathrm{diag}\{1, 1\}$ $(i = 1, 2, \cdots, 8)$. 摄像头的位置分别为: $(0.6, 0.6)$, $(0.6, 1.8)$, $(1.2, 1.8)$, $(1.8, 1.8)$, $(2.4, 1.8)$, $(2.4, 0.6)$, $(1.8, 1.2)$, $(1.2, 1.2)$.

欺骗攻击如图 3 所示. 攻击信号由于信道限制而附加的系数的上下界取值为 $\underline{\xi}_{i,s,k} = 0.1$, $\bar{\xi}_{i,s,k} = 1.5$. 每个信道的欺骗攻击信号的 $\boldsymbol{\vartheta}_{i,k}$ 部分都是通过 MATLAB 的 normrnd() 函数随机产生的高斯信号, 其均值为 0, 方差为 2, 并且限定其上界为 7. 产生的随机数的数值大小表明了攻击信号的强弱. 从图 3 中可以看出, 攻击者每攻击一段时间之后就会停下来储存能量, 为下一次攻击做准备. 每一个信道的攻击信号强度都不相同, 这里假设每个信道的攻击时刻都是相同的, 在本文的示例中, 信道 3 的攻击信号最弱.

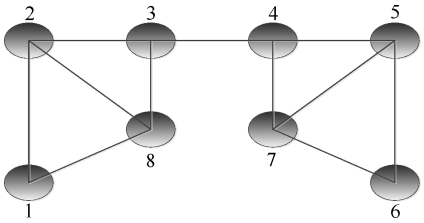

图 2　摄像头分布拓扑图

Fig. 2　The topology of the camera

图 4 和图 5 分别描绘了对 $p_{i,k}$ (状态分量 x_1) 和 $q_{i,k}$ (状态分量 x_2) 的估计效果, 从图中可以看出, 虽然在受到攻击的时刻, 对目标位置的估计略有偏差, 但是仍然能够追踪到目标. 这表明我们设计的滤波器是能够有效抵御网络攻击以完成目标定位的. 同时, 由于信道 3 受到的攻击信号最小, 其滤波轨迹最接近目标轨迹.

为了更准确地描述滤波误差, 图 6 画出了 8 个滤波器的估计误差协方差的迹. 从图 6 中可以看出, 在经过大约 10 个时间步长之后, 所有滤波器的误差都变得非常小, 且趋于稳定.

此外, 为了确定滤波器抵御攻击的能力上限, 我们修改了 $\bar{\boldsymbol{\vartheta}}_{i,k}$, 并计算了 8 个滤波器稳定后的 RMSE (均方根误差), 确定了当 $\bar{\boldsymbol{\vartheta}}_{i,k} \geq 15$ 时, 我们设计的滤波器在给定的仿真时间内将不再能够追踪到目标. 表 1 给出了不同的 $\bar{\boldsymbol{\vartheta}}_{i,k}$ 所对应的 RMSE , 其中, "–" 表示在仿真时间内滤波误差相当大且没有达到稳定. 此外, 应当指出, $\bar{\boldsymbol{\vartheta}}_{i,k}$ 的取值还与具体的目标对象有关, 滤波器针对不同的受到恶意攻击的对象, 具有不同的抵御攻击能力的上限.

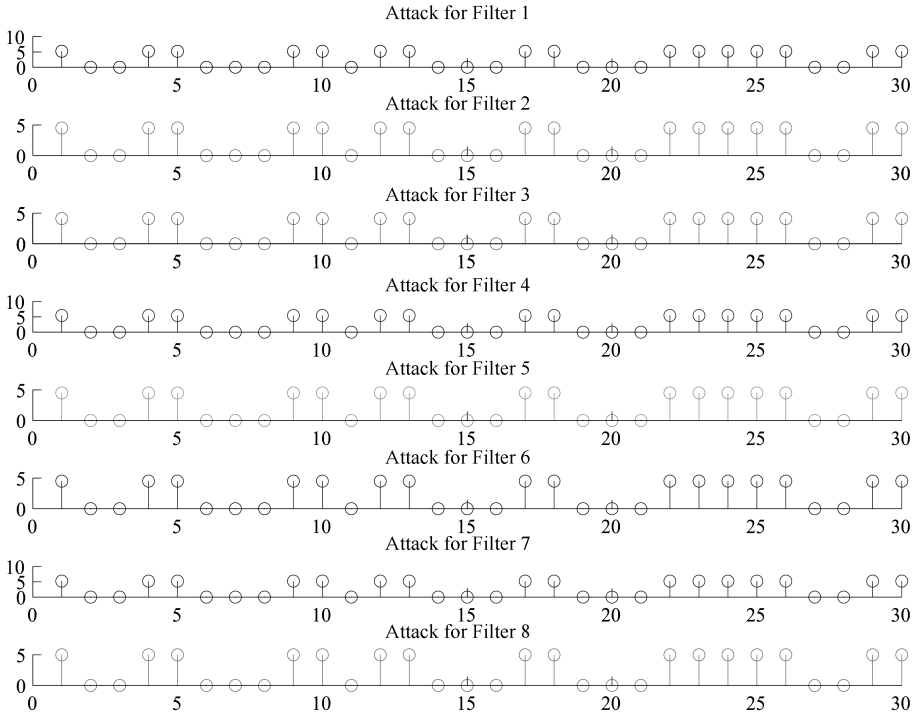

图 3 欺骗攻击示意图

Fig. 3 The diagram of deception attacks

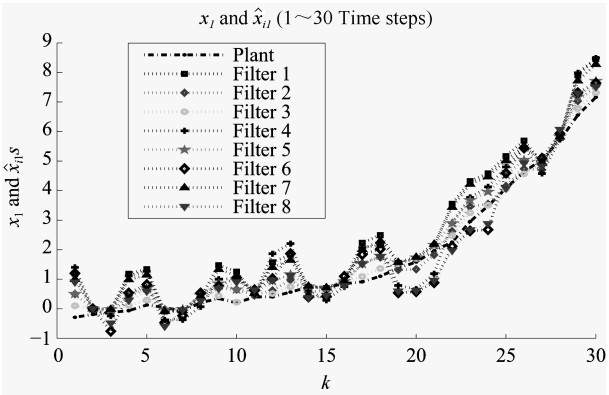

图 4 对 $p_{i,k}$ 的估计效果

Fig. 4 The estimation performance of $p_{i,k}$

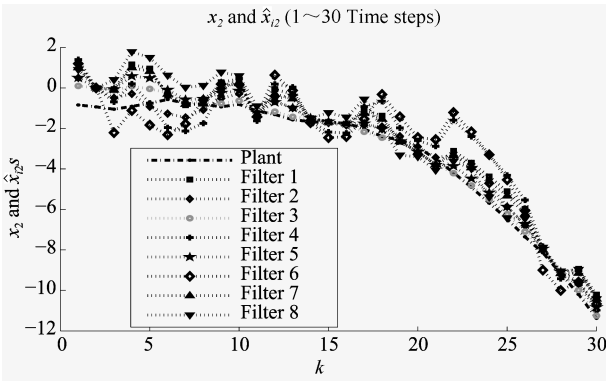

图 5 对 $q_{i,k}$ 的估计效果

Fig. 5 The estimation performance of $q_{i,k}$

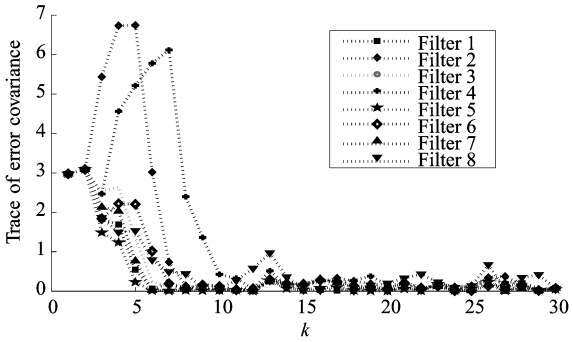

图 6 8 个传感器的滤波误差

Fig. 6 The estimation error of 8 sensors

接下来, 为了描述事件触发情况, 给出其触发时刻图形. 从图 7 可以看出, 当攻击信号比较大, 造成滤波误差比较大的时候, 就会发生事件触发. 此外, 不同的滤波器的事件触发时刻也不相同, 这与我们的期望相符合. 为了量化事件触发降低通信率的效果, 定义如下的平均通信率[16].

$$\varpi = \frac{\sum\limits_{i=1}^{N}\sum\limits_{k=0}^{M-1}\gamma_{i,k}}{NM}$$

其中, M 表示总的仿真步数, $\gamma_{i,k}=1$ 表示采样数据被传输, $\gamma_{i,k}=0$ 表示采样数据未被传输. 根据事件触发图形, 可以计算得到仿真中的平均通信率为 36 %, 可见加入事件触发之后大大降低了通信率.

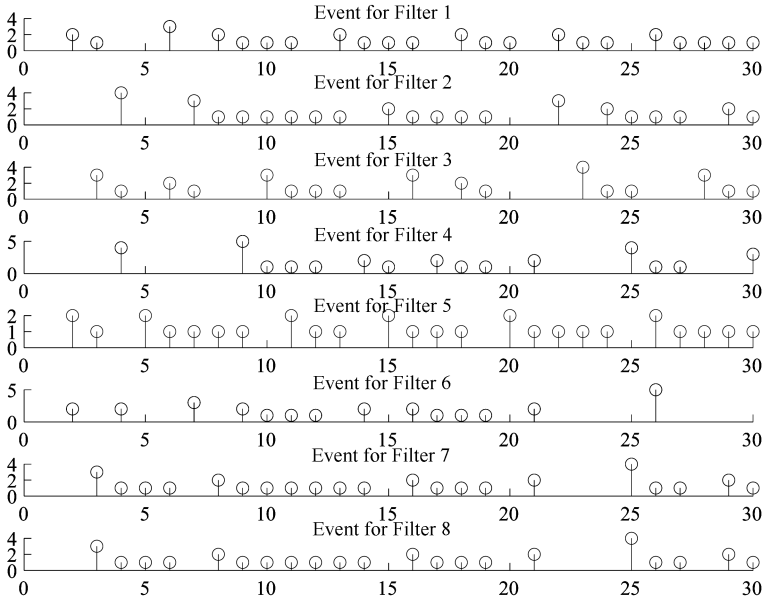

图 7　事件触发示意图

Fig. 7　The diagram of event-trigger

表 1　不同 $\bar{\boldsymbol{\vartheta}}_{i,k}$ 对应的 RMSE

Table 1　RMSE corresponding to different $\bar{\boldsymbol{\vartheta}}_{i,k}$

$\bar{\boldsymbol{\vartheta}}_{i,k}$	5	7	9	11	13	15
RMSE	0.2	0.25	1.38	8.75	15.59	–

4　结论

在充分考虑了网络欺骗攻击的情况下, 提出了一种分布式的基于事件触发的扩展卡尔曼滤波器. 设计的滤波器最主要特点是采用协方差受限的方式, 通过将误差协方差的上界最小化来获得最优的滤波增益. 通过仿真例子可以看到, 该滤波器能够有效地抵抗网络攻击, 对非线性目标进行定位. 但是由于采用线性矩阵不等式方法来解最优的滤波器增益, 因此计算量比较大, 实时性不够好. 所以, 怎样采用更好的算法来提高滤波的实时性, 成为今后要解决的一个方面.

References

1 Wu L G, Shi P, Gao H J. State estimation and sliding-mode control of Markovian jump singular systems. *IEEE Transactions on Automatic Control*, 2010, **55**(5): 1213−1219

2 Wang Chang-Cheng, Qi Guo-Qing, Li Yin-Ya, Sheng An-Dong. Consensus-based distributed filtering algorithm in sensor networks. *Control Theory & Applications*, 2012, **29**(12): 1645−1650
(王长城, 戚国庆, 李银伢, 盛安东. 传感器网络一致性分布式滤波算法. 控制理论与应用, 2012, **29**(12): 1645−1650)

3 Niu Jian-Jun, Deng Zhi-Dong. Markov chain-based distributed scheduling approach for wireless sensor network. *Acta Automatica Sinica*, 2010, **36**(5): 685−695
(牛建军, 邓志东. 基于马尔可夫链的无线传感器网络分布式调度方法. 自动化学报, 2010, **36**(5): 685−695)

4 Yu Y H. Consensus-based distributed mixture Kalman filter for maneuvering target tracking in wireless sensor networks. *IEEE Transactions on Vehicular Technology*, 2016, **65**(10): 8669−8681

5 Dong H L, Wang Z D, Lam J, Gao H J. Distributed filtering in sensor networks with randomly occurring saturations and successive packet dropouts. *International Journal of Robust and Nonlinear Control*, 2014, **24**(12): 1743−1759

6 Wu Miao-Miao, Zhang Hao, Yan Huai-Cheng, Chen Shi-Ming. Cooperative output regulation for asynchronously switched multi-agent systems. *Acta Automatica Sinica*, 2017, **43**(5): 735−742
(吴苗苗, 张皓, 严怀成, 陈世明. 异步切换多智能体系统的协同输出调节. 自动化学报, 2017, **43**(5): 735−742)

7 Yang Ruo-Han, Zhang Hao, Yan Huai-Cheng. Event-triggered cooperative output regulation of heterogeneous multi-agent systems with switching topology. *Acta Automatica Sinica*, 2017, **43**(3): 472−477
(杨若涵, 张皓, 严怀成. 基于事件触发的拓扑切换异构多智能体协同输出调节. 自动化学报, 2017, **43**(3): 472−477)

8 Liu Q Y, Wang Z D, He X, Zhou D H. Consensus-based recursive distributed filtering with stochastic nonlinearities over sensor networks. In: Proceedings of the 33rd Chinese Control Conference. Nanjing, China: IEEE, 2014. 310−315

9 Foroush H S, Martínez S. On event-triggered control of linear systems under periodic Denial-of-Service jamming attacks. In: Proceedings of the 2012 IEEE 51st IEEE Conference on Decision and Control. Maui, HI, USA: IEEE, 2012. 2551−2256

10 Pang Z H, Liu G P. Design and implementation of secure networked predictive control systems under deception attacks. *IEEE Transactions on Control Systems Technology*, 2012, **20**(5): 1334−1342

11 Mo Y L, Sinopoli B. Secure control against replay attacks. In: Proceedings of the 47th Annual Allerton Conference on Communication, Control, and Computing. Monticello, IL, USA: IEEE, 2009. 911−918

12 Zhang H, Cheng P, Shi L, Chen J M. Optimal DoS attack scheduling in wireless networked control system. *IEEE Transactions on Control Systems Technology*, 2016, **24**(3): 843−852

13 Ding D R, Wang Z D, Wei G L, Alsaadi F E. Event-based security control for discrete-time stochastic systems. *IET Control Theory & Applications*, 2016, **10**(15): 1808−1815

14 Wang J B, Luo X L. Research on airborne passive location based on extend Kalman filter with control inputs. In: Proceedings of the 3rd International Conference on Information Science and Control Engineering. Beijing, China: IEEE, 2016. 1389−1392

15 She Zhi-Ting, Zou Wei, Dong Wang-Hua, Qin Ya-Sheng. Extended Kalman filters combined with feed-forward compensation for permanent magnet synchronous moter position estimation. *Control Theory & Applications*, 2016, **33**(10): 1312−1318
(佘致廷, 邹薇, 董旺华, 秦亚胜. 扩展卡尔曼滤波结合前馈补偿永磁同步电机位置估计. 控制理论与应用, 2016, **33**(10): 1312−1318)

16 Wu J F, Jia Q S, Johansson K H, Shi L. Event-based sensor data scheduling: trade-off between communication rate and estimation quality. *IEEE Transactions on Automatic Control*, 2013, **58**(4): 1041−1046

17 Yu H, Hao F. Periodic event-triggered state-feedback control for discrete-time linear systems. *Journal of the Franklin Institute*, 2016, **353**(8): 1809−1828

18 Liu S L, Quevedo D E, Xie L H. Event-triggered distributed constrained consensus. *International Journal of Robust and Nonlinear Control*, 2017, **27**(16): 3043−3060

19 Cong Y R, Zhou X Y. Event-trigger based robust-optimal control for energy harvesting transmitter. *IEEE Transactions on Wireless Communications*, 2017, **16**(2): 744−756

20 Yang Xu-Sheng, Zhang Wen-An, Yu Li. Distributed tracking method for maneuvering targets with event-triggered mechanism. *Acta Automatica Sinica*, 2017, **43**(8): 1393−1401
(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. 自动化学报, 2017, **43**(8): 1393−1401)

21 Zhang X M, Han Q L. A decentralized event-triggered dissipative control scheme for systems with multiple sensors to sample the system outputs. *IEEE Transactions on Cybernetics*, 2016, **46**(12): 2745−2757

22 Boyd S, El Ghaoui L, Feron E, Balakrishnan V. *Linear Matrix Inequalities in System and Control Theory*. Philadelphia, USA: SIAM, 1994.

23 Horn R A, Zhang F Z. Basic properties of the Schur complement. *The Schur Complement and Its Applications*. Boston, MA: Springer, 2005. 17−46

24 Ma L F, Wang Z D, Han Q L, Lam H K. Variance-constrained distributed filtering for time-varying systems with multiplicative noises and deception attacks over sensor networks. *IEEE Sensors Journal*, 2017, **17**(7): 2279−2288

25 Li W L, Jia Y M, Du J P. Distributed consensus extended Kalman filter: a variance-constrained approach. *IET Control Theory & Applications*, 2017, **11**(3): 382−389

周 雪 同济大学控制科学与工程系研究生. 2016 年获得合肥工业大学自动化专业学士学位. 主要研究方向为无线传感器网络.
E-mail: 1631560@tongji.edu.cn
(**ZHOU Xue** Master student in the Department of Control Science and Engineering, Tongji University. She received her bachelor degree in automation from Hefei University of Technology in 2016. Her research interest covers wireless sensor networks.)

张 皓 同济大学电子与信息工程学院教授. 2007 年获得华中科技大学控制科学与工程博士学位. 2001 年获得武汉科技大学学士学位. 主要研究方向为网络控制系统, 多智能体系统, 复杂系统. 本文通信作者.
E-mail: 07102@tongji.edu.cn
(**ZHANG Hao** Professor at the School of Electronics and Information Engineering, Tongji University. She received her Ph. D. degree in control theory and control engineering from Huazhong University of Science and Technology in 2007 and received her bachelor degree in automatic control from Wuhan University of Technology in 2001. Her research interest covers network based control systems, multi-agent systems, and complex networks. Corresponding author of this paper.)

王祝萍 同济大学电子与信息工程学院教授. 1994 年和 1997 年获得西北工业大学自动控制学院学士学位与硕士学位. 2003 年获得新加坡国立大学博士学位. 主要研究方向为机器人智能控制, 自动驾驶, 非完整性控制系统.
E-mail: elewzp@tongji.edu.cn
(**WANG Zhu-Ping** Professor at the School of Electronics and Information Engineering, Tongji University. She received her Ph. D. degree in National University of Singapore in 2003, and received her bachelor and master degree from the Department of Automatic Control Northwestern Polytechnic University in 1994 and 1997, respectively. Her research interest covers intelligent control of robotic systems, selfdriving vehicles, and nonholonomic control systems.)