DOI:10.13878/j.cnki.jnuist.2018.04.007

胡传昊[1,2]　杜丽双[1,2]　张亚[1,2]

带网络攻击识别机制的传感器网络分布式滤波算法

摘要

研究了面向网络攻击的无线传感器网络的分布式目标估计问题.由于测量范围有限,网络中只有部分传感器能测量到目标,而且节点受到随机的攻击从而使得测量值被注入虚假信息.在此背景下,本文提出了基于攻击检测识别策略的改进分布式卡尔曼滤波算法.在该算法中,节点首先基于设计给出的攻击识别阈值来判断其是否受到攻击,生成识别因子;然后以估计误差协方差的迹最小为信息融合原则来设计一致性卡尔曼滤波算法,对处于监测域内的运动目标进行分布式状态估计.同时,分析了算法的收敛性,明确给出了网络估计误差均方有界的随机攻击概率的充分条件.最后用数值仿真验证了算法的有效性和优越性.

关键词

网络安全;一致性卡尔曼滤波;网络攻击;最小迹原则;无线传感器网络

中图分类号 TP393

文献标志码 A

收稿日期 2018-06-04

资助项目 国家自然科学基金(61473081);江苏省六大人才高峰项目(XYDXX-005)

作者简介

胡传昊,女,硕士生,研究方向为网络安全.15895821990@163.com.

张亚(通信作者),女,博士,副教授,博士生导师,研究方向为多智能体系统及网络安全.yazhang@seu.edu.cn

1 东南大学 自动化学院,南京 210096

2 复杂工程系统测量与控制教育部重点实验室,南京,210096

0 引言

最近,无线传感器网络(Wireless Sensor Networks,WSNs)受到无线通信、微电子、感知和嵌入式系统技术的发展推动,广泛应用于军事、工业和消费等领域,如战场监视、工业过程等.与集中式和分散式状态估计相比,分布式状态估计由于其高估计精度、低通信资源利用率以及高鲁棒性而得到更广泛的研究和关注.然而,在实际应用中,无线传感器网络容易遭受欺骗攻击、拒接服务攻击、虚假信息注入攻击等网络攻击,使得状态估计性能受到毁灭性的破坏.因此,研究面向网络攻击的无线传感器网络的分布式估计问题,具有重大的现实意义.

近年来,许多研究人员从不同角度研究网络的安全问题.例如,文献[1]定义了网络化控制系统的欺骗攻击和 DOS 攻击,提出了基于半定规划的对策.Liu 等[2]于 2009 年首次提出针对电网系统状态估计的数据注入攻击问题.自此,该问题受到了广泛关注.2010 年 Teixeira 等[3]定义了两个安全指标用以衡量针对某些特定测量值注入数据攻击的难度,研究了监控与数据采集系统中的偷袭攻击.Smith[4]研究了隐蔽攻击对控制系统的影响.Pasqualetti 等[5]借助系统论和图论工具分别研究了出现误导行为个体时的一致性问题和 CPSs 的检测和辨识问题.Mo 等[6]研究了针对线性时不变系统存在完美隐蔽攻击时的状态估计和控制问题,将该问题建模为约束控制问题,并利用椭圆积分给出其最大扰动.文献[7]对存在虚假信息注入的攻击网络提出了基于事件触发的攻击判定机制,设计优化的状态估计器并进行估计误差收敛性分析.Guo 等[8]对远程状态估计设计线性的攻击策略从而使得攻击者能够成功地注入虚假信息而且不被检测到.Shoukry 等[9]提出了两种面向测量攻击的事件驱动状态观测器.Mo 等[10]分析了攻击对随机线性时不变系统的影响,从而设计攻击策略.Yang 等[11]研究了传感器网络中存在攻击时的分布式估计问题,提出了事件驱动机制来抗击攻击的影响,但没有考虑随机的攻击策略和传感器有限的测量范围,给出的收敛性条件形式比较复杂.目前关于网络攻击的安全控制和估计的文献主要集中于讨论单个网络化系统,还没有广泛研究传感器网络、多智能体系统等复杂的分布式系统.

分布式估计是传感器网络广泛应用的重要基础.自 Olfati-Saber 等[12-13]提出一致性卡尔曼滤波算法以来,已有不少文献研究该算法.按通信和测量的机制,算法可以分成两类.一类中通信间隔小于测量

间隔,在一步测量内执行多次通信从而实现一致性信息融合[14-15].这种算法只要求网络协同可观和强连通,但通信代价大,节点能耗很高.另一类中通信间隔等于测量间隔,节点获取测量值后进行一次一致性迭代[16-17].该算法相比前一种通信能耗低,但对网络的可观性和权重设计要求高.目前的工作还没有给出一种完全分布式的设计方法.

本文针对网络节点测量能力有限并且测量信息受到随机攻击的传感器网络,提出一种攻击检测机制和完全分布式的滤波算法.首先给出了攻击识别阈值的计算公式;其次提出了以误差协方差的迹最小为准则的信息融合方法;接着将识别攻击触发因子和最小迹融合准则融入一致性卡尔曼滤波算法中设计出了面向网络攻击的安全状态估计器;最后用理论严格推导和分析了保证估计误差有界的随机攻击概率条件.

1 问题描述

本文研究的是在传感器网络遭到随机攻击时,对动态目标的状态估计算法的设计.考虑的攻击类别为虚假信息注入攻击,其攻击策略为向传感器网络中的各传感器节点的测量值随机注入攻击矢量.

考虑动态目标在一个传感器网络覆盖的地域上运动,该地域由 xOy 平面坐标系表示.这个运动目标的状态方程描述为

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

其中,$\boldsymbol{x}(k)$ 代表 k 时刻目标系统的状态向量,$\boldsymbol{A}$ 表示目标的系统矩阵,并且 $\boldsymbol{A}$ 不是Schur稳定的,$\boldsymbol{w}(k)$ 为协方差为 $\boldsymbol{Q}$ 的系统输入白噪声.

现有由 n 个传感器节点组成的一个传感器网络用于监测该运动目标.每个时刻,每个传感器节点都试图测量目标,第 k 步第 i 个传感器的测量方程由下式给出:

$$\boldsymbol{y}_i(k)=\boldsymbol{H}_i(k)\boldsymbol{x}(k)+\boldsymbol{v}_i(k)+\alpha_i(k)\boldsymbol{e}_i(k), \tag{2}$$

其中,$\boldsymbol{y}_i(k)$ 表示输出测量值,$\boldsymbol{H}_i$ 是测量矩阵且是满秩的,$(\boldsymbol{A},\boldsymbol{H}_i)$ 完全能观,$\boldsymbol{x}(k)$ 是目标状态,$\boldsymbol{v}_i(k)$ 是协方差为 $\boldsymbol{R}_i$ 的零均值高斯测量白噪声,$\boldsymbol{e}_i(k)$ 是与 $\boldsymbol{w}(k)$ 和 $\boldsymbol{v}_i(k)$ 都相互独立的外部攻击矢量,$\alpha_i(k)$ 表示是第 i 个传感器节点在 k 时刻是否受到攻击:

$$\alpha_i(k)=\begin{cases}1, & \text{受到真实攻击},\\ 0, & \text{未受到攻击}.\end{cases} \tag{3}$$

每个节点随机受到攻击,所以 $\alpha_i(k)$ 是随机变化的.假设 $\alpha_i(k)$ 服从独立同分布的变化,节点受攻击的概率为 p,即 $\Pr(\alpha_i(k)=1)=p$.

值得注意的是,由于传感器节点的测量范围有限以及障碍物遮挡、测量策略等因素,网络中的传感器节点尽管都试图测量目标,但只有部分节点可以成功测量到目标.用 λ_i 表示目标是否在传感器节点 i 的测量范围内,即目标可测因子,其表达式为

$$\lambda_i=\begin{cases}1, & \text{节点 } i \text{ 能测到目标},\\ 0, & \text{节点 } i \text{ 测不到目标}.\end{cases} \tag{4}$$

尽管传感器节点的测量模型是可观的,但由于部分节点无法获得目标的测量信息,节点之间必须协同从而估计目标的状态.本文的主要工作就是在传感范围受限以及存在网络攻击的情况下,设计分布式状态估计算法使得估计具有较高的准确性和较强的鲁棒性.

2 基于攻击识别检测和最小迹原则的分布式滤波算法

这一部分主要设计分布式滤波算法,然后分析估计误差有界的条件.算法设计集中于两个关键问题:一是如何建立传感器节点受到网络攻击的识别判断机制;二是如何设计面向网络攻击的分布式目标跟踪算法.

2.1 攻击识别检测方案

本文研究的是虚假注入信息攻击,其隶属于欺骗攻击.具体的攻击策略为:在传感器网络所覆盖的场区中,某一攻击信号以一定概率攻击传感器节点.传感器节点受到攻击后的具体表现形式为:受到攻击的传感器节点注入了一定大小的白噪声,进而引入了一个虚假的噪声信息.面对此类虚假信息注入的攻击,本文采用基于事件触发的攻击识别判断机制,以进行攻击检测.

由攻击策略可知,此攻击矢量的性质为与原系统的测量噪声相互独立的高斯白噪声,它通过改变传感器节点测量方程的测量总噪声,进而影响该传感器节点的估计准确性,最后使状态估计器的一致性估计产生较大的偏差.我们的目的是设计一个阈值来检测节点是否受到攻击.为使受到攻击后的状态估计器的性能不受太大的影响,由文献[7]知,可以设计以下攻击识别方案.如果传感器节点 i 能够测量到目标,则

$$\mathrm{Attack}(i)=\begin{cases}1, & \|\boldsymbol{e}_i\|>D^{e_i},\\ 0, & \text{其他},\end{cases} \tag{5}$$

其中,Attack(i) = 1 表示节点 i 受到攻击,Attack(i) = 0 表示节点没有受到攻击;D^{e_i} 表示受到真实攻击的节点 i 的攻击矢量的下边界.

在式(5)的攻击识别方案中,传感器节点 i 的攻击误差 $\boldsymbol{e}_i$ 和攻击矢量边界 D^{e_i} 的表达式如下:

$$\boldsymbol{e}_i = \boldsymbol{y}_i - \boldsymbol{H}_i\bar{\boldsymbol{x}}_i - \tilde{\boldsymbol{v}}_i\ , \tag{6}$$

$$D^{e_i} = 2\|\boldsymbol{H}_i\|\|\boldsymbol{H}_i^+\|\max_{\tilde{v}_i\in\Omega_i}\|\tilde{\boldsymbol{v}}_i\| + 2\max_{\tilde{v}_i\in\Omega_i}\|\tilde{\boldsymbol{v}}_i\|, \tag{7}$$

$\bar{\boldsymbol{x}}_i$ 表示传感器节点 i 对目标状态的预测值,$\boldsymbol{H}_i^+$ 表示 $\boldsymbol{H}_i$ 的伪逆,即:$\boldsymbol{H}_i^+ = \boldsymbol{H}_i^{\mathrm{T}}(\boldsymbol{H}_i\boldsymbol{H}_i^{\mathrm{T}})^{-1}$,$\Omega_i$ 表示第 i 个传感器的测量噪声矢量集,$\tilde{\boldsymbol{v}}_i$ 表示噪声集合里的任意矢量.

定理 1 若满足 Attack(i) = 1,则传感器 i 一定受到了攻击.

证明 令传感器节点受到真实的攻击矢量为 $\boldsymbol{e}_i^*$,其在传感器节点未受攻击时为零,受到攻击时非零.由第 i 个传感器节点的测量方程(2)有:$\boldsymbol{e}_i^* = \boldsymbol{y} - \boldsymbol{H}_i\boldsymbol{x} - \boldsymbol{v}_i$,这里的 $\boldsymbol{v}_i$ 为系统的测量噪声.

令 $\Delta\boldsymbol{e}_i = \boldsymbol{e}_i - \boldsymbol{e}_i^*$,$\Delta\tilde{\boldsymbol{v}}_i = \tilde{\boldsymbol{v}}_i - \boldsymbol{v}_i$,$\Delta\boldsymbol{x}_i = \bar{\boldsymbol{x}}_i - \boldsymbol{x}$,则有:$\Delta\boldsymbol{e}_i = -\boldsymbol{H}_i\Delta\boldsymbol{x}_i - \Delta\boldsymbol{v}_i$.由 $\Delta\boldsymbol{e}_i = \boldsymbol{e}_i - \boldsymbol{e}_i^*$ 可知,若传感器未受到攻击,则 $\boldsymbol{e}_i^* = 0$,$\Delta\boldsymbol{e}_i = \boldsymbol{e}_i$.因此,若传感器的攻击矢量的估计误差 $\boldsymbol{e}_i$ 有上界,那可以确保所有超过界限的攻击矢量 $\boldsymbol{e}_i$ 对应于传感器受到攻击的情况.由上式得到

$$\|\Delta\boldsymbol{e}_i\| \leqslant \|\boldsymbol{H}_i\| \cdot \|\Delta\boldsymbol{x}_i\| + 2\max_{\tilde{v}_i\in\Omega_i}\|\tilde{\boldsymbol{v}}_i\|\ .$$

令 $\|\Delta\boldsymbol{x}_i\|$ 的边界为 D^{x_i},当使用抗攻击状态估计器时,状态观测器的最大误差边界 D^{x_i} 始终与噪声的大小成线性关系[7],可以得到误差边界的计算公式为

$$D^{x_i} = 2\|\boldsymbol{H}_i^+\|\max_{\tilde{v}_i\in\Omega_i}\|\tilde{\boldsymbol{v}}_i\|,$$

从而有:

$$\|\Delta\boldsymbol{e}_i\| \leqslant 2\|\boldsymbol{H}_i\|\|\boldsymbol{H}_i^+\|\max_{\tilde{v}_i\in\Omega_i}\|\tilde{\boldsymbol{v}}_i\| + 2\max_{\tilde{v}_i\in\Omega_i}\|\tilde{\boldsymbol{v}}_i\|\ ,$$

所以令 $\|\Delta\boldsymbol{e}_i\|$ 的边界为 D^{e_i},由上式可知,状态观测器的最大攻击误差边界 D^{e_i} 为

$$D^{e_i} = 2\|\boldsymbol{H}_i\|\|\boldsymbol{H}_i^+\|\max_{\tilde{v}_i\in\Omega_i}\|\tilde{\boldsymbol{v}}_i\| + 2\max_{\tilde{v}_i\in\Omega_i}\|\tilde{\boldsymbol{v}}_i\|\ .$$

由攻击识别方案知,当 Attack(i) = 1 时,有 $\|\boldsymbol{e}_i\| > D^{e_i}$,又 $\Delta\boldsymbol{e}_i = \boldsymbol{e}_i - \boldsymbol{e}_i^*$,则有

$$D^{e_i} < \|\boldsymbol{e}_i\| = \|\Delta\boldsymbol{e}_i + \boldsymbol{e}_i^*\| \leqslant \|\Delta\boldsymbol{e}_i\| + \|\boldsymbol{e}_i^*\| \leqslant D^{e_i} + \|\boldsymbol{e}_i^*\|\ ,$$

即 $\|\boldsymbol{e}_i^*\| > 0$ 恒成立.故传感器 i 的实际攻击矢量非零,意味着该传感器受到攻击.定理得证.

由式(5)的检测识别攻击方案可知,此方案是引入了一个判断无线传感器网络中的任意传感器节点是否受到攻击的二进制变量.

由上述分析可以看出,若某传感器节点 i 的攻击矢量误差大于攻击矢量下边界 D^{e_i},则判断该节点受到真实攻击,否则判断该传感器节点未受到攻击.因此,可以将该攻击矢量的下边界视为攻击识别阈值.在实际仿真中,利用该识别阈值来判断任意传感器节点是否受到攻击.

综上所述,由式(7)可得攻击识别阈值(threshold)的计算公式如下:

$$y_{\text{threshold}} = 2\|\boldsymbol{H}_i\|\|\boldsymbol{H}_i^+\|\max_{\tilde{v}_i\in\Omega_i}\|\tilde{\boldsymbol{v}}_i\| + 2\max_{\tilde{v}_i\in\Omega_i}\|\tilde{\boldsymbol{v}}_i\|\ , \tag{8}$$

从式(8)可以看出,攻击识别阈值与系统的测量噪声和测量矩阵有关.

2.2 基于攻击识别和最小迹原则的一致性卡尔曼滤波算法

本文在经典一致性卡尔曼滤波的基础上,设计面向网络攻击的改进一致性卡尔曼滤波算法.

根据一致性卡尔曼滤波理论,各传感器节点基于测量信息更新的状态估计为

$$\hat{\boldsymbol{x}}_i(k) = \boldsymbol{A}\bar{\boldsymbol{x}}_i(k) + \lambda_i\gamma_i\boldsymbol{K}_i^*(k)(\boldsymbol{y}_i - \boldsymbol{H}_i\boldsymbol{x}(k))\ , \tag{9}$$

其中,$\boldsymbol{K}_i^*$ 为卡尔曼滤波增益,λ_i 表示目标是否在传感器节点 i 的测量范围内,即目标可测因子,γ_i 判断节点 i 是否收到攻击,若未受到攻击则为 1,受到攻击则为 0.由于节点受到随机的攻击,这里 γ_i 是二进制随机变量.

在式(9)中,卡尔曼滤波增益的计算公式为

$$\boldsymbol{K}_i^*(k) = \boldsymbol{A}\boldsymbol{P}_i(k)\boldsymbol{H}_i^{\mathrm{T}}(\boldsymbol{R}_i + \boldsymbol{H}_i\boldsymbol{P}_i(k)\boldsymbol{H}_i^{\mathrm{T}})^{-1}. \tag{10}$$

计算估计误差协方差 $\hat{\boldsymbol{P}}_i(k)$ 为

$$\hat{\boldsymbol{P}}_i(k) = \boldsymbol{F}_i(k)\boldsymbol{P}_i(k)\boldsymbol{F}_i(k)^{\mathrm{T}} + \lambda_i\gamma_i\boldsymbol{K}_i^*\boldsymbol{R}_i\boldsymbol{K}_i^{*\mathrm{T}} + \boldsymbol{Q}, \tag{11}$$

其中,$\boldsymbol{F}_i(k) = \boldsymbol{A} - \lambda_i\gamma_i\boldsymbol{K}_i^*\boldsymbol{H}_i$.

上述滤波已经完成了单个传感器对目标的最优估计.接下来进行邻近传感器之间交换信息的一致化处理,即进行信息融合.信息融合的公式如下:

$$\boldsymbol{x}_i(k+1) = \sum^{j\in S_i} w_{ij}(k)\hat{\boldsymbol{x}}_j(k)\ , \tag{12}$$

$$\boldsymbol{P}_i(k+1) = \sum^{j\in S_i} w_{ij}(k)\hat{\boldsymbol{P}}_j(k)\ , \tag{13}$$

其中,$\boldsymbol{x}_i(k+1)$ 和 $\boldsymbol{P}_i(k+1)$ 分别表示传感器 i 对 k+1 时刻的估计状态及其协方差矩阵;$S_i = \{i, N_i\}$,为传感器 i 包括自身和邻居传感器的集合;$\hat{\boldsymbol{x}}_j(k)$ 和

$\hat{\boldsymbol{P}}_j(k)$ 分别表示传感器在第 k 时刻接收到的来自传感器 j 传递的状态估计值和预测误差协方差矩阵;w_{ij} 表示传感器 i 划分的包括自身和邻居传感器的 S_i 集合中的每个传感器的信息融合权重,且对任意 $j \in S_i$,应满足:$\sum_{j\in S_i} w_{ij} = 1$.

设计信息融合方法是多传感器进行一致性估计好坏的一个关键.因为在实际应用中,由于各传感器节点自身的系统噪声和感知周边环境的差异,不同节点对系统的局部估计产生的影响和不确定度通常是不同的.因此,设计一个较优的信息融合准则可以更好地实现对目标的全局估计和跟踪.

本文设计采用以预测误差协方差的迹最小为信息融合准则来对目标进行一致性估计.由目标跟踪的目的可知,为了实现较为准确的目标跟踪,需要减小系统状态估计误差.而预测误差的大小可以间接地采用预测误差协方差的迹作为判断标准.基于此,可以将预测误差协方差的迹作为衡量状态估计误差的指示因子.即对于任意一个传感器节点来说,在对比包括自身在内的所有相邻传感的集合中的各节点的预测误差协方差矩阵的迹之后,选择预测误差协方差矩阵的迹最小的传感器节点的预测误差协方差和先验估计值作为该时刻整个传感器网络的一致性估计的结果,显然此时的误差是最小的.令更新误差协方差迹最小的传感器节点为主导传感器节点 i^*,满足:

$$\mathrm{tr}(\hat{\boldsymbol{P}}_{i^*}(k)) = \min\{\mathrm{tr}(\hat{\boldsymbol{P}}_j(k)),j \in S_i\}. \tag{14}$$

当传感器节点为主导传感器节点,则权重为 1,否则为 0.即:

$$w_{ij} = \begin{cases} 1, & j = i^*, \\ 0, & \text{其他}. \end{cases} \tag{15}$$

2.3 算法收敛性分析

本节将分析算法的收敛性与攻击概率之间的关系.在对状态估计的收敛性进行分析之前,首先做出如下假设和定义:

1)假设无线传感器网络各传感器节点之间的通信拓扑是连通的;

2)假设传感器网络中,能测量到目标的传感器节点是恒定的;

3)假设传感器网络是一个有限空间,整个拓扑图的直径是 m;

4)定义函数 $\boldsymbol{\Phi}_i(k)$,此函数代表第 i 个传感器节点的误差协方差迹的大小,即:

$$\boldsymbol{\Phi}_i(k) = \mathrm{tr}(\boldsymbol{P}_i(k)).$$

定理 2 如果网络随机攻击概率满足:

$$p < \frac{1}{\prod |\lambda_i^u(\boldsymbol{A})|^2},$$

其中,$\lambda_i^u(\boldsymbol{A})$ 表示系统矩阵的不稳定特征值,那么在基于攻击识别机制和最小迹原则的一致性卡尔曼滤波算法下,传感器网络所有节点的期望协方差 $\mathrm{E}(\boldsymbol{\Phi}_i(k))$ 是有界的.

证明 首先证明只要网络中存在一个节点的误差协方差有界,那么其他所有节点的误差协方差都是有界的.

设网络中节点 i_0 的协方差有界,即 $\boldsymbol{\Phi}_{i_0}(k)$ 有界.根据最小迹原则传感器节点 i_0 在第 k+1 时刻的误差协方差迹为

$$\boldsymbol{\Phi}_{i_0}(k+1) = \min_{j\in S_{i_0}}\{\mathrm{tr}(\hat{\boldsymbol{P}}_j(k))\} \leqslant \mathrm{tr}(\hat{\boldsymbol{P}}_{i_0}(k)).$$

由于传感器网络通信拓扑是连通的,在第 k+1 时刻,至少有一个传感器节点 i_1 与第 i_0 个传感器连通,即可以进行信息交互.与第 i_0 的分析类似,在 k+2 时刻,传感器节点 i_1 的误差协方差迹为

$$\boldsymbol{\Phi}_{i_1}(k+2) = \min_{j\in S_{i_1}}\{\mathrm{tr}(\hat{\boldsymbol{P}}_j(k+1))\} \leqslant$$
$$\mathrm{tr}(\hat{\boldsymbol{P}}_{i_0}(k+1)) \leqslant \mathrm{tr}(\boldsymbol{A}\boldsymbol{P}_{i_0}(k+1)\boldsymbol{A}^{\mathrm{T}} + \boldsymbol{Q}) \leqslant$$
$$\|\boldsymbol{A}\|_2^2\boldsymbol{\Phi}_{i_0}(k+1) + \mathrm{tr}(\boldsymbol{Q}).$$

依此类推,由于网络拓扑是连通的并且直径为 m,对距离节点 i_0 路径长度为 m 的节点 i_m:

$$\boldsymbol{\Phi}_{i_m}(k+m+1) \leqslant \|\boldsymbol{A}\|_2^{2m}\boldsymbol{\Phi}_{i_0}(k+1) +$$
$$(\|\boldsymbol{A}\|_2^{2(m-1)} + \|\boldsymbol{A}\|_2^{2(m-2)} + \cdots + \|\boldsymbol{A}\|_2^2 + 1)\mathrm{tr}(\boldsymbol{Q}).$$

显然网络中任意节点 $\boldsymbol{\Phi}_i(k)$ 都是有界的.

接下来证明当 $p < \frac{1}{\prod |\lambda_i^u(\boldsymbol{A})|^2}$ 时,节点的协方差是有界的.设能测到目标的一个传感器节点为 i_0,由假设知能测量到目标的传感器节点是恒定的,故 $\lambda_{i_0} = 1$.结合可测因子和攻击识别机制得到:

$$\hat{\boldsymbol{P}}_{i_0}(k) = \boldsymbol{A}\boldsymbol{P}_{i_0}(k)\boldsymbol{A}^{\mathrm{T}} + \boldsymbol{Q} - \gamma_{i_0}(k)\boldsymbol{A}\boldsymbol{P}_{i_0}(k)\boldsymbol{H}_{i_0}^{\mathrm{T}}(\boldsymbol{R}_{i_0} + \boldsymbol{H}_{i_0}\boldsymbol{P}_{i_0}(k)\boldsymbol{H}_{i_0}^{\mathrm{T}})^{-1}\boldsymbol{H}_{i_0}\boldsymbol{P}_{i_0}(k)\boldsymbol{A}^{\mathrm{T}}.$$

根据定理 1 得到:

$$\hat{\boldsymbol{P}}_{i_0}(k) \leqslant f(\boldsymbol{P}_{i_0}(k),\alpha_{i_0}(k)) = \boldsymbol{A}\boldsymbol{P}_{i_0}(k)\boldsymbol{A}^{\mathrm{T}} + \boldsymbol{Q} - (1-\alpha_{i_0}(k))\boldsymbol{A}\boldsymbol{P}_{i_0}(k)\boldsymbol{H}_{i_0}^{\mathrm{T}}(\boldsymbol{R}_{i_0} + \boldsymbol{H}_{i_0}\boldsymbol{P}_{i_0}(k)\boldsymbol{H}_{i_0}^{\mathrm{T}})^{-1}\boldsymbol{H}_{i_0}\boldsymbol{P}_{i_0}(k)\boldsymbol{A}^{\mathrm{T}}.$$

又由最小迹原则知:

$$\boldsymbol{\Phi}_{i_0}(k+1) \leqslant \mathrm{tr}(\hat{\boldsymbol{P}}_{i_0}(k)) \leqslant \mathrm{tr}(f(\boldsymbol{P}_{i_0}(k),\alpha_{i_0}(k))).$$

因为攻击是随机的,设攻击概率为 $\Pr(\alpha_{i_0}(k)=1)=p$,下面分析 $\mathrm{E}(\boldsymbol{\Phi}_{i_0}(k+1))$ 的有界性.由上式可得:

$$\mathrm{E}(\boldsymbol{\Phi}_{i_0}(k+1)) \leqslant \mathrm{tr}(\boldsymbol{A}\boldsymbol{P}_{i_0}(k)\boldsymbol{A}^{\mathrm{T}}+\boldsymbol{Q}-(1-p)\boldsymbol{A}\boldsymbol{P}_{i_0}(k)\boldsymbol{H}_{i_0}^{\mathrm{T}}(\boldsymbol{R}_{i_0}+\boldsymbol{H}_{i_0}\boldsymbol{P}_{i_0}(k)\boldsymbol{H}_{i_0}^{\mathrm{T}})^{-1}\boldsymbol{H}_{i_0}\boldsymbol{P}_{i_0}(k)\boldsymbol{A}^{\mathrm{T}}).$$

根据文献[18],代数 Riccati 迭代方程:

$$\boldsymbol{P}(k+1)=\boldsymbol{A}\boldsymbol{P}(k)\boldsymbol{A}^{\mathrm{T}}+\boldsymbol{Q}-(1-p)\boldsymbol{A}\boldsymbol{P}(k)\boldsymbol{H}^{\mathrm{T}}(\boldsymbol{R}+\boldsymbol{H}\boldsymbol{P}(k)\boldsymbol{H}^{\mathrm{T}})^{-1}\boldsymbol{H}\boldsymbol{P}(k)\boldsymbol{A}^{\mathrm{T}}$$

收敛的充分条件是 $p<\dfrac{1}{\prod|\lambda_i^u(\boldsymbol{A})|^2}$. 所以当定理 2 中的条件满足时,$\mathrm{E}(\boldsymbol{\Phi}_{i_0}(k+1))$ 必然是有界的,从而网络中所有节点的期望协方差都是有界的.定理得证.

3 数值仿真

无线传感器网络的构建如图 1 所示,设置传感器节点的监测范围为 2 km×2 km 的正方形区域,初始化 200 个传感器节点,通信距离和可测范围均为 300 m. $\boldsymbol{H}_i=\begin{bmatrix}1&0&0&0\\0&0&1&0\end{bmatrix}$.考虑一个变加速曲线运动的目标,其系统的状态矩阵 $\boldsymbol{A}=\begin{bmatrix}0&0&1&0\\0&0&0&1\\16&0&0&0\\0&0&0&0\end{bmatrix}$.

由上式,可以求出 $\boldsymbol{A}$ 的特征值为:1.264 9,-1.264 9,0,0.

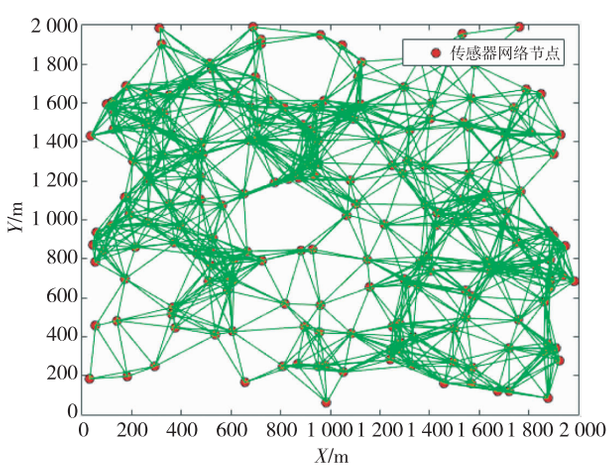


图 1 传感器网络

Fig. 1 Wireless sensor network

首先仿真分析攻击识别的误差率.设置攻击概率为 0.1,攻击矢量大小为 11,原系统的测量噪声为 2.由式(8)的攻击识别阈值的计算公式,可以得到 $y_{\mathrm{threshold}}\approx 8$.受攻击的传感器节点的识别误差如图 2 所示.此图横坐标为采样时间步长,纵坐标为识别误差百分比 $E_{\mathrm{attack}}=\dfrac{|n_{\mathrm{real}}-n_{\mathrm{identify}}|}{n_{\mathrm{real}}}$,其中,$n_{\mathrm{identify}}$ 表示识别受攻击传感器节点总数,n_{real} 表示真实受攻击传感器节点总数.由图 2 可知,识别误差最大约为 10%,在误差允许的范围内,故可知本文设计的攻击检测识别方案是可行的.

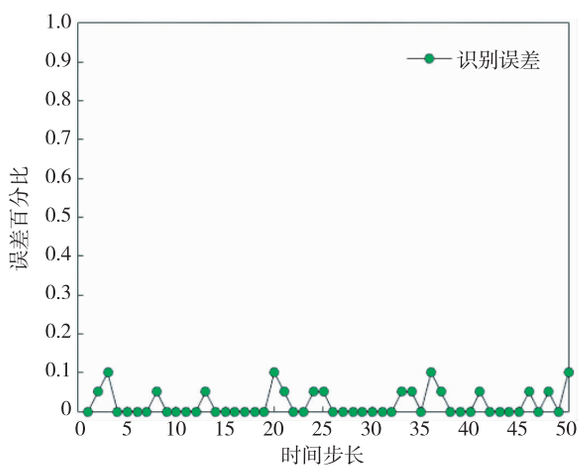


图 2 攻击识别误差率

Fig. 2 Error rates of attack recognition

为了更好地验证本文所设计的以最小迹为信息融合原则算法的优越性,本文将其与常用的平均原则和加权原则算法进行对比.平均加权中权重为 $w_{ij}=\dfrac{1}{1+d_i}, j\in N_i$,其中 d_i 为传感器第 i 个传感器的度. 加权原则算法的权重分配为 $w_{ij}=\dfrac{\dfrac{1}{\mathrm{tr}(\boldsymbol{P}_j(k))}}{\sum_{j\in S_i}\dfrac{1}{\mathrm{tr}(\boldsymbol{P}_j(k))}}, j\in S_i$.三种一致性协议下的目标跟踪轨迹如图 3 所示.显然,最小迹原则下的跟踪性能最好.

接下来展示攻击概率对状态估计器的影响.由定理 2 得到误差协方差有界的充分条件是 $p<0.625$.这里将丢包网络(丢包概率为 0.5)和未丢包网络一起考虑,得到攻击概率分别为 0.1,0.4,0.6,0.7 时,最小迹原则下的误差和协方差迹如图 4 所示.

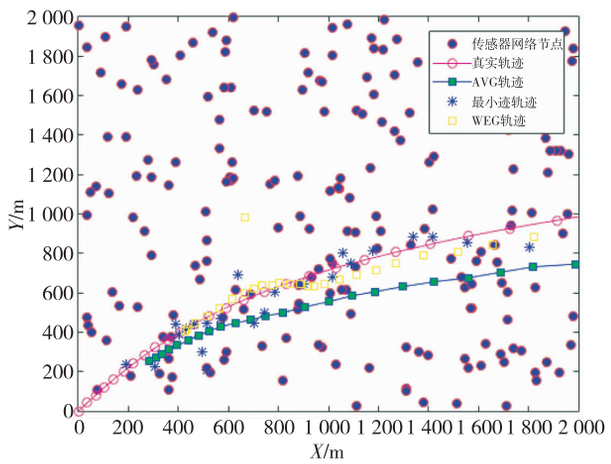


图 3　三种一致性协议下的目标跟踪

Fig. 3　Target tracking under three types of consensus strategies

由图 4 可以看出,随着攻击概率的增加,跟踪误差增加.在攻击概率大于 0.7 时,估计误差发散.

4　结论

针对网络节点测量能力有限并且测量信息受到随机攻击的传感器网络,提出一种攻击识别检测机制和基于最小迹原则的完全分布式的一致性卡尔曼滤波算法,并给出了保证估计误差有界的随机攻击概率条件.仿真验证了算法的有效性.本文在收敛性分析时假设传感器对目标的能否测量是固定的,后续将研究时变的网络.

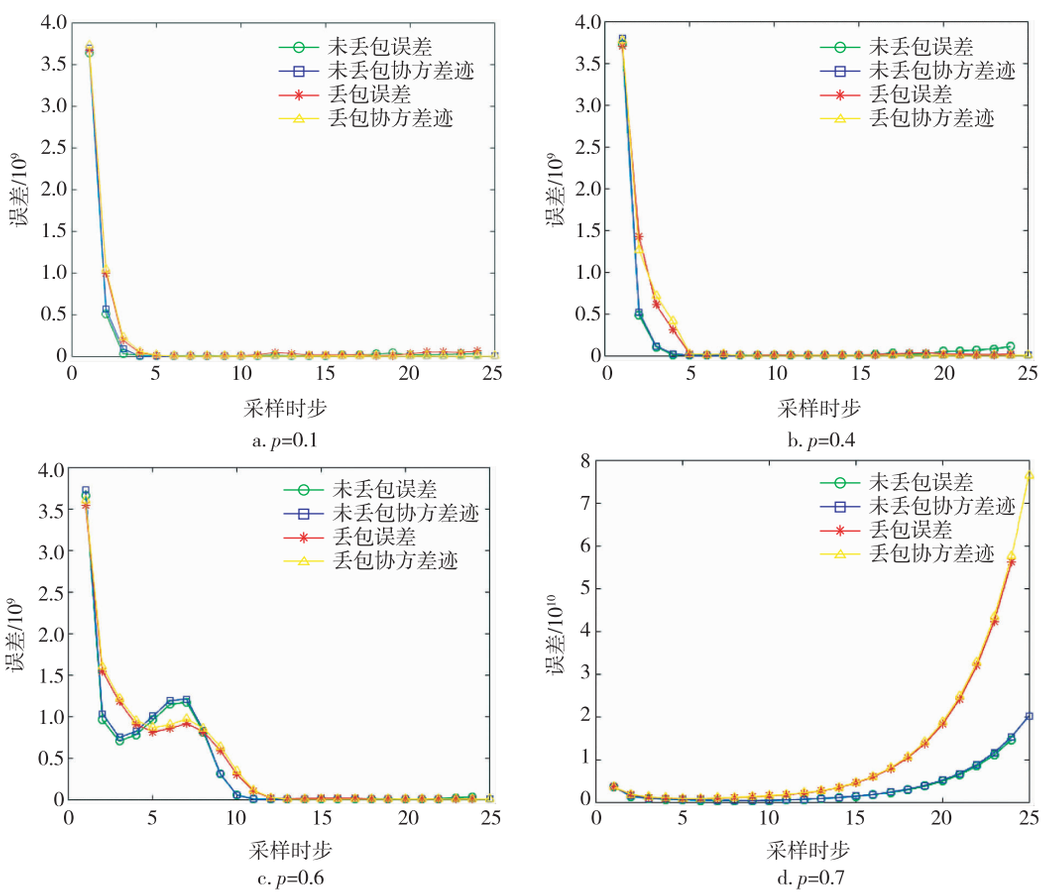


图 4　不同攻击概率下的网络估计误差

Fig. 4　Estimation errors under different attack probabilities

参考文献

References

[1] Nikiforov I V. Detection of abrupt changes: theory and application [M]. Upper Saddle River, NJ: Prentice Hall, 1993

[2] Liu Y, Ning P, Reiter M K. False data injection attacks against state estimation in electric power grids[J]. ACM Transactions on Information and System Security, 2009, 14(1): 21-32

[3] Teixeira A, Amin S, Sandberg H, et al. Cyber security

analysis of state estimators in electric power systems[C]// IEEE Conference on Decision and Control, 2010: 5991-5998
[4] Smith R S. A decoupled feedback structure for covertly appropriating network control systems[M]. IFAC Proceedings Volumes, 2011, 44(1): 90-95
[5] Pasqualetti F, Dorfler F, Bullo F. Attack detection and identification in cyber-physical systems[J]. IEEE Transactions on Automatic Control, 2013, 58(11): 2715-2729
[6] Mo Y L, Sinopoli B. Secure control against replay attacks[C]//47th Annual Allerton Conference on Communication, Control, and Computing, 2009: 911-918
[7] Pajic M, Lee I, George G J. Attack-resilient state estimation for noisy dynamical systems[J]. IEEE Transactions on Control of Network Systems, 2016, DOI: 10.1109/TCNS.2016.2607420
[8] Guo Z Y, Shi D W, Johansson K H, et al. Optimal linear cyber-attack on remote state estimation[J]. IEEE Transactions on Control of Network Systems, 2017, 4(1): 4-13
[9] Shoukry Y, Tabuada P. Event-triggered state observers for sparse sensor noise/attacks[J]. IEEE Transactions on Automatic Control, 2016, 61(8): 2079-2091
[10] Mo Y, Sinopoli B. On the performance degradation of cyber-physical systems under stealthy integrity attacks[J]. IEEE Transactions on Automatic Control, 2016, 61(9): 2618-2624
[11] Yang W, Lei L, Yang C. Event-based distributed state estimation under deception attack[J]. Neurocomputing, 2017, 270: 145-151
[12] Olfati-Saber R. Distributed Kalman filter with embedded consensus filters[C]//IEEE Conference on Decision and Control, 2006: 8179-8184
[13] Olfati-Saber R, Shamma J S. Consensus filters for sensor networks and distributed sensor fusion[C]//IEEE Conference on Decision and Control, 2006: 6698-6703
[14] Battistelli G, Chisci L, Mugnai G, et al. Consensus-based linear and nonlinear filtering[J]. IEEE Transactions on Automatic Control, 2015, 60(5): 1410-1415
[15] Battistelli G, Chisci L. Stability of consensus extended Kalman filter for distributed state estimation[J]. Automatica, 2016, 68(C): 169-178
[16] Matei I, Baras J S. Consensus-based linear distributed filtering[J]. Automatica, 2012, 48(8): 1776-1782
[17] Yang W, Yang C, Shi H B, et al. Stochastic link activation for distributed filtering under sensor power constraint[J]. Automatica, 2017, 75: 109-118
[18] Sinopoli B, Schenato L, Franceschetti M, et al. Kalman filtering with intermittent observations[J]. IEEE Transactions on Automatic Control, 2004, 49(9): 1453-1463

Distributed filtering algorithm based on attack recognition scheme for sensor networks

HU Chuanhao[1,2] DU Lishuang[1,2] ZHANG Ya[1,2]
1 School of Automation, Southeast University, Nanjing 210096
2 Key Laboratory of Measurement and Control of Complex Systems of Engineering, Ministry of Education, Nanjing 210096

Abstract The distributed target estimation problem in a wireless sensor network (WSN) which is under network attack is studied in this paper. Due to the limited measurement range, only some sensors in WSN can measure the target, and at the same time, the nodes are randomly attacked so that the measurement value is injected into false information. An improved consensus Kalman filter algorithm based on the attack detection and recognition strategy is proposed. In this algorithm, firstly, the node judges whether it is attacked based on the attack recognition threshold given in this paper. Secondly, a consensus Kalman filtering algorithm is designed based on the minimum trace fusion principle. Finally, the convergence of the algorithm is analyzed, and a sufficient condition of the attack probability for the boundedness of the mean-square estimation error in WSN is given. Besides, numerical simulations are given to verify the effectiveness and superiority of the algorithm.

Key words network security; consensus Kalman filtering; network attack; minimum trace principle; wireless sensor networks