计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200300117

有适应力的分布式状态估计方法

高枫越[1]　王　琰[2]　朱铁兰[3]
1 陆军工程大学通信工程学院　南京 210007
2 军事科学院系统工程研究院　北京 100141
3 96125 部队　沈阳 110000

摘　要　为提高智能体系统对攻击的免疫力,研究了测量攻击下的适应力分布式状态估计方法。每个智能体对系统状态进行连续的本地线性测量。由于不同智能体的本地测量模型相互异构,对系统状态可能不具有本地可观测性,且攻击者能够操控部分智能体的测量数据,随意改变其测量结果。而智能体的目标是协同处理本地测量数据,并正确估计出未知的系统状态。因此,该问题的挑战在于在不对真实测量数据和恶意智能体的测量数据进行分辨时,如何设计算法估计得到真实的系统状态。为了解决这个问题,设计了适应性分布式最大后验概率估计算法。在该算法中,只要恶意智能体的数量小于某个特定值,所有智能体都能够收敛到系统状态。首先,根据卡尔曼滤波给出集中式最大后验概率(Maximum A Posteriori,MAP)估计方法,并与分布式一致性结合,进而得到分布式最大后验概率估计方法。然后,考虑到测量攻击,从估计一致性的角度,利用自适应饱和度增益设计了适应性分布式最大后验概率估计方法。最后,通过仿真实验验证算法的有效性。

关键词:适应性估计;分布式状态估计;卡尔曼滤波;最大后验概率;一致性滤波;多智能体系统
中图法分类号　TP13

Resilient Distributed State Estimation Algorithm

GAO Feng-yue[1],WANG Yan[2] and ZHU Tie-lan[3]
1 College of Communications Engineering,PLA University of Army Engineering,Nanjing 210007,China
2 System Engineering Research Institute,Academy of Military Sciences PLA,Beijing 100141,China
3 Unit 96125,Shenyang 110000,China

Abstract　In order to improve the immunity of multi-agent system against attack,resilient distributed state estimation under measurement attacks is studied. Each agent makes successive local linear measurements of the system state. The local measurement models are heterogeneous across agents and may be locally unobservable for the system state. An adversary compromises some of the measurement streams and changes their values arbitrarily. The agents' goal is to cooperate with their local measurements and estimate the value of the system state correctly. The challenge of this problem is how to design an algorithm to estimate the real system state without distinguishing the real measurements from the measurements of malicious agents. In order to solve this problem,an adaptive distributed maximum a posteriori probability estimation algorithm is designed. As long as the number of compromised measurement streams is lower than a particular bound,all of the agents' local estimates,including malicious agents' local estimates,can converge to the true system state. Firstly,a centralized maximum a posteriori (MAP) estimation method is proposed based on Kalman filter. Combining a centralized MAP estimation with distributed consensus protocol,a distributed MAP estimation method is derived. Then,considering the measurement attack and analyzing the consistency of distributed estimates,a resilient distributed MAP estimation method is designed by exploiting the saturating adaptive gain,which gives a small gain if the deviation from the practical measurement resulting from the attacks is too large. At last,Numerical simulations are provided to evaluate the effectiveness of the proposed algorithm against measurement attacks.

Keywords　Resilient estimation,Distributed state estimation,Kalman filter,Maximum a posteriori,Consensus filter,Multi-agent system

1　引言

在传感器网络中,分布式状态估计已经成为多智能体系统领域的研究热点[1-3]。为了保证估计的最优性,大多数方法是通过融合中心收集所有节点的测量数据来进行集中处理。这种处理方法在节点数目巨大、通信资源受限的复杂网络中显然是不适用的。与集中式的方案相比,分布式的机制可以通过与邻居节点进行信息交互以实现接近集中式的估计性能,从而大大减少通信资源的消耗,提高网络的鲁棒性[2]。

通过分布式的机制计算各节点测量数据的平均值来实现

到稿日期:2020-03-19　返修日期:2020-08-06　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
通信作者:高枫越(350471891@qq.com)

一致性滤波的方法已经成为了分布式状态估计中十分有效的方法[3]。文献[4]研究了提高多智能体系统的一致性收敛速度的问题，分析了不同复杂网络中影响一致性收敛速度的因素。但是，这种分布式一致性滤波方法容易受到外界的恶意攻击，加上传感器网络的节点规模庞大，网络资源受限，无法保证节点的安全性和可靠性。文献[5]设计了集中式和分布式的监测器来检测和鉴别攻击者。与检测攻击相比，具有攻击适应性的状态估计方法也是一个值得研究的方向。文献[6]研究了拜占庭将军的问题，指出如果 1/3 以上的将军叛国，那么任何分布式算法都不能做出正确的决定；反之，如果叛国将领的数量不到 1/3，那么就可以设计出算法使得忠诚将领能够做出正确决定。文献[7]将每个节点收到的邻居节点信息进行排序，通过舍弃部分奇异测量值，设计出一种迭代的分布式一致性算法。文献[8]从恶意节点的数目和网络的拓扑结构角度，分析得到了普通节点实现一致性的必要条件和充分条件。文献[9]设计了一种同时检测攻击和参数估计的算法，在正常节点具有全局可观测性的情况下，该算法或者能够检测出攻击的存在，或者能够正确估计出参数的真实值。文献[10]同时考虑了在间歇性观测、通信链路中断和网络丢包背景下的适应性分布式的状态估计算法，设计了可切换的线性观测器来处理时变测量模型以抵御恶意攻击行为。文献[11]考虑了基于分簇结构的信息物理系统的联合攻击检测和监测系统状态的问题，用混合伯努利随机集密度代表攻击信号和系统状态的联合信息，并结合递归贝叶斯和 Kullback-Leibler 平均，提出了分布式的混合伯努利随机集滤波算法并验证了其有效性。文献[12]研究了在物理和网络攻击下的联合分布式攻击监测和分布式安全估计问题，指出恶意攻击者在物理系统层发起虚假数据注入攻击，同时在网络层发起干扰攻击，阻断传感器与远程估计器之间的无线传输信道；为了提供局部可靠的状态估计和检测虚假数据攻击，设计了适应性的攻击检测估计器，并给出了估计性能分析。

本文考虑了线性动态系统的适应性分布式状态估计问题，即恶意的攻击者能够劫持部分节点并且任意修改节点的测量值。针对此问题，本文通过融合本地节点的观测值和邻居节点的先验估计值，并利用一致性协议和自适应类饱和度增益，设计了适应性分布式最大后验概率估计器，实现了对动态参数的正确估计，并通过仿真实验验证了所提算法的有效性和优越性。

首先，在无线传感器网络安全系统中建立了系统未知参数的动态更新模型和智能体的观测数据模型。然后，在此基础之上，在测量攻击情况下，引入恶意智能体的观测数据模型和一些假设。接着，根据卡尔曼滤波的思想，从集中式最大后验概率估计入手，将每个智能体都作为融合中心，融合节点和邻居的观测数据和先验估计值，并利用一致性协议，进而得到了分布式最大后验概率估计方法。最后，从估计一致性的角度展开分析，利用类饱和度增益限制数据攻击对估计算法的影响，推导得出适应性分布式最大后验概率估计方法，并结合概率论的相关知识，推导算法的收敛性。

2 系统模型

2.1 符号说明

$\mathbb{Z}$ 表示自然数集合。$\mathbb{R}^k$ 定义为 k 维的欧氏空间。矩阵 $\boldsymbol{A}$，$\boldsymbol{A}^{-1}$ 和 $\boldsymbol{A}^{\mathrm{T}}$ 分别表示矩阵 $\boldsymbol{A}$ 的逆矩阵和转置矩阵。$\boldsymbol{B}\leqslant\boldsymbol{A}$ 表示 $\boldsymbol{A}-\boldsymbol{B}$ 为正定矩阵。$\mathrm{diag}(\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_n)$ 表示主对角线由矩阵 $(\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_n)$ 构成的块对角阵。$\|\cdot\|$ 表示向量的 2 范数和矩阵的诱导 2 范数。$|\cdot|$ 表示集合的基数。$\mathbb{P}\{\cdot\}$ 和 $\mathbb{E}\{\cdot\}$ 分别表示随机向量的概率和数学期望。

2.2 图谱论的基础

假设有 N 个传感器节点独立分布在一个矩形区域内，节点间的通信可以用一个无向的简单图 $G=(v,\varepsilon)$ 表示。其中，v 表示 N 个传感器节点的集合，ε 表示节点之间的链路集合。Ω_n 代表节点 n 的邻居节点集合，节点 n 只能与自己的邻居节点进行通信。图 G 的度矩阵 $\boldsymbol{D}$ 定义为 $\boldsymbol{D}=\mathrm{diag}(d_1,\cdots,d_N)$，其中，$d_n$ 表示节点 n 的度，即 $d_n=|\Omega_n|$。图 G 的结构矩阵 $\boldsymbol{A}$ 是一个对称的邻接矩阵，其中，$a_{nl}=1$ 表示节点 n 与节点 l 之间有链路，否则，$a_{nl}=0$。定义半正定矩阵 $\boldsymbol{L}=\boldsymbol{D}-\boldsymbol{A}$，将 $\boldsymbol{L}$ 的特征值从小到大排列为 $0=\lambda_1(\boldsymbol{L})\leqslant\cdots\leqslant\lambda_n(\boldsymbol{L})$。根据文献[13]，如果图 G 是连通的，那么 $\lambda_2(\boldsymbol{L})>0$。

2.3 状态转移和节点测量方程

考虑一个时间离散的线性动态系统，其状态更新方程的表达式为：

$$\boldsymbol{\theta}^*(t+1)=\boldsymbol{F}\boldsymbol{\theta}^*(t)+\boldsymbol{v}_n(t) \tag{1}$$

其中，$\boldsymbol{\theta}^*(t)\in\mathbb{R}^M$ 表示 $t\in\mathbb{Z}$ 时刻的状态向量，$\boldsymbol{F}$ 是状态转移矩阵，$\boldsymbol{v}_n(t)$ 是均值为 0、协方差矩阵为 $\boldsymbol{Q}$ 的高斯白噪声过程。

由 N 个节点构成的传感器网络对系统状态进行测量，t 时刻节点 n 的测量方程为：

$$\boldsymbol{y}_n(t)=\boldsymbol{H}_n\boldsymbol{\theta}^*(t)+\boldsymbol{w}_n(t) \tag{2}$$

其中，$\boldsymbol{w}_n(t)$ 是独立同分布的测量噪声，其均值为 0，协方差矩阵为 $\boldsymbol{R}_n$，且不同传感器节点处的测量噪声相互独立。$\boldsymbol{H}_n$ 是节点 n 的测量矩阵，$\boldsymbol{y}_n(t)$ 表示实际的测量数据。

2.4 攻击模型

攻击者企图控制部分节点，使得节点不能够对系统状态进行正确的估计。攻击者可以对其控制的部分节点的测量数据进行任意的篡改，如果被篡改的测量数据被当作真实的测量数据用于状态估计算法中，那么这两个测量数据的差可以被建模成一个加性的扰动 $\boldsymbol{a}_n(t)$。因此，处于攻击环境下，节点 n 的测量值可以表示为：

$$\boldsymbol{y}_n(t)=\boldsymbol{H}_n\boldsymbol{\theta}^*(t)+\boldsymbol{w}_n(t)+\boldsymbol{a}_n(t) \tag{3}$$

对于任意时刻 $t\in\mathbb{Z}$，如果 $\boldsymbol{a}_n(t)\neq\boldsymbol{0}$，就表明智能体受到攻击成为恶意智能体。但是，这并不意味着恶意智能体包含的所有数据流都是不可靠的，并且智能体 n 也不清楚其中的哪些数据流受到了篡改。

假设 1　攻击者只能操控部分智能体，即 $|\mathcal{A}|/N\in[0,1)$。其中，$\mathcal{A}$ 表示恶意智能体构成的集合。

假设 2　攻击者只能操控智能体的测量值，不能改变未知参数的真实值，即 $\boldsymbol{\theta}^*(t)$ 的值不会被攻击者修改。

3 分布式最大后验概率估计

3.1 集中式最大后验概率估计

在网络没有被攻击的情况下，所有节点的数据都是没有被篡改的实测数据。网络的融合中心可以将所有节点的测量数据集中起来，写成向量形式为：

$$\boldsymbol{y}_t=\mathcal{H}\boldsymbol{\theta}^*(t)+\boldsymbol{w}_t \tag{4}$$

其中，

$$\boldsymbol{y}_t=[\boldsymbol{y}_1^{\mathrm{T}}(t)\cdots\boldsymbol{y}_n^{\mathrm{T}}(t)]^{\mathrm{T}} \tag{5}$$

$$\mathcal{H}=[\boldsymbol{H}_1^{\mathrm{T}}\cdots\boldsymbol{H}_N^{\mathrm{T}}]^{\mathrm{T}} \tag{6}$$

$$\boldsymbol{w}_t=[\boldsymbol{w}_1^{\mathrm{T}}(t)\cdots\boldsymbol{w}_N^{\mathrm{T}}(t)]^{\mathrm{T}} \tag{7}$$

噪声向量 $\boldsymbol{w}_t$ 的协方差矩阵可以表示为 $\boldsymbol{R}=\mathrm{diag}(\boldsymbol{R}_1,\cdots,\boldsymbol{R}_N)$。假设 $\boldsymbol{Y}_t=\{\boldsymbol{y}_0,\boldsymbol{y}_1,\cdots,\boldsymbol{y}_t\}$，系统状态 $\boldsymbol{\theta}^*(t)$ 的先验估计和后验估计分别定义为：

$$\begin{aligned}\bar{\boldsymbol{x}}_t&=\arg\max_{\boldsymbol{\theta}^*(t)}\mathbb{P}\{\boldsymbol{\theta}^*(t)|\boldsymbol{Y}_{t-1}\}\\ \hat{\boldsymbol{x}}_t&=\arg\max_{\boldsymbol{\theta}^*(t)}\mathbb{P}\{\boldsymbol{\theta}^*(t)|\boldsymbol{Y}_t\}\end{aligned} \tag{8}$$

相应的先验估计误差和后验估计误差分别为：

$$\begin{aligned}\bar{\boldsymbol{e}}_t&=\bar{\boldsymbol{x}}_t-\boldsymbol{\theta}^*(t)\\ \hat{\boldsymbol{e}}_t&=\hat{\boldsymbol{x}}_t-\boldsymbol{\theta}^*(t)\end{aligned} \tag{9}$$

误差的协方差矩阵分别为：

$$\begin{aligned}\bar{\boldsymbol{P}}_t&=\mathbb{E}\{\bar{\boldsymbol{e}}_t\bar{\boldsymbol{e}}_t^{\mathrm{T}}\}\\ \hat{\boldsymbol{P}}_t&=\mathbb{E}\{\hat{\boldsymbol{e}}_t\hat{\boldsymbol{e}}_t^{\mathrm{T}}\}\end{aligned} \tag{10}$$

由于状态噪声 $\boldsymbol{v}_n(t)$ 和测量噪声 $\boldsymbol{w}_n(t)$ 都服从高斯分布，条件概率 $\mathbb{P}\{\boldsymbol{y}_t|\boldsymbol{\theta}^*(t)\}\mathbb{P}\{\boldsymbol{\theta}^*(t)|\boldsymbol{Y}_{t-1}\}$ 也服从高斯分布，即：

$$\begin{aligned}&\mathbb{P}\{\boldsymbol{y}_t|\boldsymbol{\theta}^*(t)\}\propto\exp\left(-\frac{1}{2}(\boldsymbol{y}_t-\mathcal{H}\boldsymbol{\theta}^*(t))^{\mathrm{T}}\boldsymbol{R}^{-1}(\boldsymbol{y}_t-\mathcal{H}\boldsymbol{\theta}^*(t))\right)\\ &\mathbb{P}\{\boldsymbol{\theta}^*(t)|\boldsymbol{Y}_{t-1}\}\propto\exp\left(-\frac{1}{2}(\bar{\boldsymbol{x}}_t-\boldsymbol{\theta}^*(t))^{\mathrm{T}}\bar{\boldsymbol{P}}^{-1}(\bar{\boldsymbol{x}}_t-\boldsymbol{\theta}^*(t))\right)\end{aligned} \tag{11}$$

进而得到：

$$\begin{aligned}\hat{\boldsymbol{x}}_t&=\arg\max_{\boldsymbol{\theta}^*(t)}\mathbb{P}\{\boldsymbol{\theta}^*(t)|\boldsymbol{Y}_t\}\\ &=\arg\max_{\boldsymbol{\theta}^*(t)}\mathbb{P}\{\boldsymbol{y}_t|\boldsymbol{\theta}^*(t)\}\mathbb{P}\{\boldsymbol{\theta}^*(t)|\boldsymbol{Y}_{t-1}\}\\ &=\arg\min_{\boldsymbol{\theta}^*(t)}[(\boldsymbol{y}_t-\mathcal{H}\boldsymbol{\theta}^*(t))^{\mathrm{T}}\boldsymbol{R}^{-1}(\boldsymbol{y}_t-\mathcal{H}\boldsymbol{\theta}^*(t))+\\ &\quad(\bar{\boldsymbol{x}}_t-\boldsymbol{\theta}^*(t))^{\mathrm{T}}\bar{\boldsymbol{P}}_t^{-1}(\bar{x}_t-\boldsymbol{\theta}^*(t))]\end{aligned} \tag{12}$$

于是

$$\hat{\boldsymbol{x}}=((\bar{\boldsymbol{P}}_t)^{-1}+\mathcal{H}^{\mathrm{T}}\boldsymbol{R}^{-1}\mathcal{H})^{-1}((\bar{\boldsymbol{P}}_t)^{-1}\bar{x}_t+\mathcal{H}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{y}_t) \tag{13}$$

可以写成如下形式：

$$\hat{\boldsymbol{u}}_t=(\bar{\boldsymbol{P}}_t)^{-1}\bar{x}_t+\mathcal{H}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{y}_t \tag{14}$$

$$\hat{\boldsymbol{U}}_t=(\bar{\boldsymbol{P}}_t)^{-1}+\mathcal{H}^{\mathrm{T}}\boldsymbol{R}^{-1}\mathcal{H} \tag{15}$$

其中，$\hat{\boldsymbol{u}}_t$ 和 $\hat{\boldsymbol{U}}_t$ 分别表示后验信息向量和后验信息矩阵。

3.2 分布式最大后验概率估计

分布式最大后验概率估计是基于一致性协议和先验估计值的联合估计方法。一致性协议可以通过邻居节点之间进行信息交互实现，是一种有效的分布式状态估计方法。假设在 t 时刻，节点 n 将其前一状态 α_n^{k-1} 发送给邻居节点 $l\in\Omega_n$，同时收到邻居节点 $l\in\Omega_n$ 的状态 α_l^{k-1}。然后对节点 n 的当前状态进行更新，表达式为：

$$\alpha_n^k=\alpha_n^{k-1}+\sum_{l\in\Omega_n}\pi_{nl}(\alpha_l^{k-1}-\alpha_n^{k-1}) \tag{16}$$

当节点之间交互次数 k 趋于无穷时，每个节点的最终状态 α_n^K 都会收敛为所有连通节点初始状态的平均值[14]，而收敛速率的快慢与一致性权重 π_{nl} 的取值有关。在保证一定收敛速率的同时考虑到分布式网络的特点，一致性权重可由本地节点 n 和邻居节点 $l\in\Omega_n$ 的度数共同确定。节点的权重表达式为[15]：

$$\pi_{nl}=(1+\max\{d_n,d_l\})^{-1},\text{if } a_{nl}=1 \tag{17}$$

若已知 t 时刻的先验信息矩阵 $\bar{\boldsymbol{U}}_n(t)$ 和 $\bar{\boldsymbol{u}}_n(t)$ 信息向量 $\bar{\boldsymbol{u}}_n(t)$，则 t 时刻的后验信息矩阵和信息向量的初始状态分别为 $\hat{\boldsymbol{U}}_n^0(t)$ 和 $\hat{\boldsymbol{u}}_n^0(t)$，它们的表达式为：

$$\hat{\boldsymbol{U}}_n^0(t)=\bar{\boldsymbol{U}}_n(t)+\boldsymbol{H}_n^{\mathrm{T}}\boldsymbol{R}_n^{-1}\boldsymbol{H}_n \tag{18}$$

$$\hat{\boldsymbol{u}}_n^0(t)=\bar{\boldsymbol{u}}_n(t)+\boldsymbol{H}_n^{\mathrm{T}}\boldsymbol{R}_n^{-1}\boldsymbol{y}_n(t) \tag{19}$$

然后对 $\hat{\boldsymbol{U}}_n^0(t)$ 和 $\hat{\boldsymbol{u}}_n^0(t)$ 进行 K 次递归的状态更新，更新的方程式为：

$$\hat{\boldsymbol{U}}_n^k(t)=\hat{\boldsymbol{U}}_n^{k-1}(t)+\sum_{l\in\Omega_n}\pi_{nl}(\hat{\boldsymbol{U}}_l^{k-1}(t)-\hat{\boldsymbol{U}}_n^{k-1}(t)) \tag{20}$$

$$\hat{\boldsymbol{u}}_n^k(t)=\hat{\boldsymbol{u}}_n^{k-1}(t)+\sum_{l\in\Omega_n}\pi_{nl}(\hat{\boldsymbol{u}}_l^{k-1}(t)-\hat{\boldsymbol{u}}_n^{k-1}(t)) \tag{21}$$

得到 t 时刻的最大后验概率估计和信息矩阵：

$$\hat{\boldsymbol{x}}_n(t)=\hat{\boldsymbol{U}}_n^K(t))^{-1}\hat{\boldsymbol{u}}_n^K(t),\hat{\boldsymbol{U}}_n(t)=\hat{\boldsymbol{U}}_n^K(t) \tag{22}$$

根据传感器节点 n 在 t 时刻的最大后验概率估计和信息矩阵 $\hat{\boldsymbol{U}}_n(t)$ 计算得到 $t+1$ 时刻的先验概率估计和信息矩阵分别为：

$$\bar{\boldsymbol{x}}_n(t+1)\boldsymbol{F}\bar{\boldsymbol{x}}_n(t) \tag{23}$$

$$\bar{\boldsymbol{U}}_n(t+1)=(\boldsymbol{F}\hat{\boldsymbol{U}}_n^{-1}(t)\boldsymbol{F}^{\mathrm{T}}+\boldsymbol{Q})^{-1} \tag{24}$$

相应的先验信息向量为：

$$\bar{\boldsymbol{u}}_n(t+1)=\bar{\boldsymbol{U}}_n(t+1)\bar{\boldsymbol{x}}_n(t+1) \tag{25}$$

4 适应性分布式最大后验概率估计

在网络受到测量攻击的情况下，部分传感器节点被攻击者控制，这些节点的数据可能被攻击者任意地篡改，导致分布式算法的估计值偏离真实值。因此，需要设计一种改进的算法来适应部分节点数据被篡改的情况，保证节点仍能有效估计出正确的系统状态。通过分析给出适应性分布式最大后验概率估计方法，具体内容如下。

假设所有节点的初始估计值都相同，初始估计误差的协方差矩阵已知，那么根据一致性可以得到[16]：

$$\mathbb{E}\{(\hat{\boldsymbol{x}}_n(0)-\boldsymbol{\theta}^*(0))(\hat{\boldsymbol{x}}_n(0)-\boldsymbol{\theta}^*(0))^T\}\leq\hat{\boldsymbol{P}}_n(0) \tag{26}$$

由于 $\hat{\boldsymbol{U}}_n(t)=\hat{\boldsymbol{P}}_n^{-1}(t)$，在式(27)中用 $\hat{\boldsymbol{U}}_n(t)$ 来表示，则推导得到表达式：

$$\hat{\boldsymbol{U}}_n(0)\leq(\mathbb{E}\{(\hat{\boldsymbol{x}}_n(0)-\boldsymbol{\theta}^*(0))(\hat{\boldsymbol{x}}_n(0)-\boldsymbol{\theta}^*(0))^{\mathrm{T}}\})^{-1}\} \tag{27}$$

假设式(28)在 t 时刻成立，即：

$$\hat{\boldsymbol{U}}_n(t)\leq(\mathbb{E}\{(\hat{\boldsymbol{x}}_n(t)-\boldsymbol{\theta}^*(t))(\hat{\boldsymbol{x}}_n(t)-\boldsymbol{\theta}^*(t))^{\mathrm{T}}\})^{-1} \tag{28}$$

同时对关系表达式式(18)和式(19)加入类饱和度自适应增益 $\beta_n(t)$，即：

$$\hat{\boldsymbol{U}}_n^0(t)=\bar{\boldsymbol{U}}_n(t)+\beta_n(t)\boldsymbol{H}_n^{\mathrm{T}}\boldsymbol{R}_n^{-1}\boldsymbol{H}_n \tag{29}$$

$$\hat{\boldsymbol{u}}_n^0(t)=\bar{\boldsymbol{u}}_n(t)+\beta_n(t)\boldsymbol{H}_n^{\mathrm{T}}\boldsymbol{R}_n^{-1}\boldsymbol{y}_n(t) \tag{30}$$

可以递推得到 $t+1$ 时刻先验信息矩阵的表达式为：

$$\begin{aligned}\bar{\boldsymbol{U}}_n(t+1)&=(\boldsymbol{F}\hat{\boldsymbol{U}}_n^{-1}(t)\boldsymbol{F}^{\mathrm{T}}+\boldsymbol{Q})^{-1}\\ &\leq(\boldsymbol{F}(\mathbb{E}\{(\hat{\boldsymbol{x}}_n(t)-\boldsymbol{\theta}^*(t))(\hat{\boldsymbol{x}}_n(t)-\boldsymbol{\theta}^*(t))^{\mathrm{T}}\})\boldsymbol{F}^{\mathrm{T}}+\\ &\quad\boldsymbol{Q})^{-1}\end{aligned}$$

$$=(\mathbb{E}\{(\bar{\boldsymbol{x}}_n(t+1)-\boldsymbol{\theta}^*(t+1))(\bar{\boldsymbol{x}}_n(t+1)-\boldsymbol{\theta}^*(t+1))^{\mathrm{T}}\})^{-1} \tag{31}$$

得到最大后验概率估计误差为：

$$\begin{aligned}&\hat{\boldsymbol{x}}_n(t+1)-\boldsymbol{\theta}^*(t+1)\\&=\hat{\boldsymbol{U}}_n^{-1}(t+1)\hat{\boldsymbol{u}}_n(t+1)\hat{\boldsymbol{U}}_n^{-1}(t+1)\hat{\boldsymbol{U}}_n(t+1)\boldsymbol{\theta}^*(t+1)\\&=\hat{\boldsymbol{U}}_n^{-1}(t+1)(\bar{\boldsymbol{U}}_n(t+1)(\bar{\boldsymbol{x}}_n(t+1)-\boldsymbol{\theta}^*(t+1))+\beta_n(t+1)\boldsymbol{H}_n^{\mathrm{T}}\boldsymbol{R}_n^{-1}(\boldsymbol{y}_n(t+1)-\boldsymbol{H}_n\boldsymbol{\theta}^*(t+1)))\end{aligned} \tag{32}$$

得到协方差矩阵为：

$$\begin{aligned}&\mathbb{E}\{(\hat{\boldsymbol{x}}_n(t+1)-\boldsymbol{\theta}^*(t+1))(\hat{\boldsymbol{x}}_n(t+1)-\boldsymbol{\theta}^*(t+1))^{\mathrm{T}}\}\\&\leq\hat{\boldsymbol{U}}_n^{-1}(t+1)(\bar{\boldsymbol{U}}_n(t+1)\beta_n^2(t+1)\boldsymbol{H}_n^{\mathrm{T}}\boldsymbol{R}_n^{-1}\boldsymbol{\Sigma}_n\boldsymbol{R}_n^{-1}\boldsymbol{H}_n)\hat{\boldsymbol{U}}_n^{-1}(t+1)\end{aligned} \tag{33}$$

因为

$$\boldsymbol{\Sigma}_n=\mathbb{E}\{(\boldsymbol{y}_n(t+1)-\boldsymbol{H}_n\boldsymbol{\theta}^*(t+1))(\boldsymbol{y}_n(t+1)-\boldsymbol{H}_n\boldsymbol{\theta}^*(t+1))^{\mathrm{T}}\} \tag{34}$$

所以，若

$$\bar{\boldsymbol{U}}_n(t+1)=\beta_n^2(t+1)\boldsymbol{H}_n^{\mathrm{T}}\boldsymbol{R}_n^{-1}\boldsymbol{\Sigma}_n\boldsymbol{R}_n^{-1}\boldsymbol{H}_n\leq\hat{\boldsymbol{U}}_n(t+1) \tag{35}$$

成立，则

$$\hat{\boldsymbol{U}}_n(t+1)\leq(\mathbb{E}\{(\hat{\boldsymbol{x}}_n(t+1)-\boldsymbol{\theta}^*(t+1))(\hat{\boldsymbol{x}}_n(t+1)-\boldsymbol{\theta}^*(t+1))^{\mathrm{T}}\})^{-1} \tag{36}$$

进而得到：

$$\beta_n^2(t+1)\boldsymbol{H}_n^{\mathrm{T}}\boldsymbol{R}_n^{-1}\boldsymbol{\Sigma}_n\boldsymbol{R}_n^{-1}\boldsymbol{H}_n\leq\beta_n(t+1)\boldsymbol{H}_n^{\mathrm{T}}\boldsymbol{R}_n^{-1}\boldsymbol{H}_n \tag{37}$$

进一步得到：

$$\beta_n(t+1)\boldsymbol{\Sigma}_n\leq\boldsymbol{R}_n \tag{38}$$

因此令自适应增益为：

$$\beta_n(t+1)=\min\left\{1,\frac{1}{\|\boldsymbol{R}_n^{-1/2}(\boldsymbol{y}_n(t+1)-\boldsymbol{H}_n\bar{\boldsymbol{x}}_n(t+1))\|^2}\right\} \tag{39}$$

5 仿真分析

为了验证提出的弹性分布式最大后验概率估计算法的有效性，本文设计了一个目标跟踪的场景。在这个场景中，有 8 个传感器节点随机地均匀分布在监测区域内，节点之间的通信链路拓扑关系如图 1 所示。

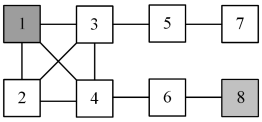

图 1 传感器网络拓扑

Fig. 1 Sensor network topology

在监测区域内，有一个正在移动的目标，目标的移动轨迹服从离散时间的线性模型。在 t 时刻，目标的状态向量表示为 $\boldsymbol{\theta}^*(t)=[\chi(t),\eta(t),\dot{\chi}(t),\dot{\eta}(t)]^{\mathrm{T}}$。其中，$(\chi(t),\eta(t))$ 和 $(\dot{\chi}(t),\dot{\eta}(t))$ 分别表示二维笛卡尔坐标系 $\mathcal{YOX}$ 中的位置和速率。状态向量的转移矩阵 $\boldsymbol{F}$ 和转移噪声的协方差矩阵 $\boldsymbol{Q}$ 分别为：

$$\boldsymbol{F}=\begin{bmatrix}1&0&1&0\\0&1&0&1\\0&0&1&0\\0&0&0&1\end{bmatrix},\boldsymbol{Q}=\begin{bmatrix}10&0&0&0\\0&10&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} \tag{40}$$

在 500×500 的矩形区域内随机选择一点作为目标的初始位置，设初始速率为 2，方向角随机，误差的协方差矩阵为 $\boldsymbol{P}_0=\mathrm{diag}(100,100,10,10)$，各节点的初始先验估计为真实初始值与均值为 0、协方差矩阵为 $\boldsymbol{P}_0$ 的白噪声之和，总的测量时间为 $T=100$。假设节点 n 具有本地可观测性，则其测量矩阵和相应的测量噪声协方差矩阵设计为：

$$\boldsymbol{H}_n=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix},\boldsymbol{R}_n=\begin{bmatrix}100&0&0&0\\0&100&0&0\\0&0&1&0\\0&0&0&10\end{bmatrix} \tag{41}$$

如果节点 l 不具有本地可观测性，其只能测量第一维和第四维的系统状态，则其测量矩阵和相应的测量噪声协方差矩阵为：

$$\boldsymbol{H}_l=\begin{bmatrix}1&0&0&0\\0&0&0&1\end{bmatrix},\boldsymbol{R}_l=\begin{bmatrix}100&0\\0&10\end{bmatrix} \tag{42}$$

即每个节点的测量方程为 $\boldsymbol{y}_n(t)=\boldsymbol{H}_n\boldsymbol{\theta}^*(t)+\boldsymbol{w}_n(t)$。假设攻击者控制了节点 1 和节点 8 这 2 个节点(2/8=25%)，令这 2 个节点的测量方程为 $\boldsymbol{y}_n^a(t)=-\boldsymbol{H}_n\boldsymbol{\theta}^*(t)+\boldsymbol{w}_n(t)$。

图 2 给出了目标真实运动轨迹 $(\chi(t),\eta(t))$，并对比了提出的适应性分布式 MAP 估计与安全分布式一致滤波(Secure Distributed Consensus Filter，SDCF)[17] 的节点预测轨迹性能。在仿真实验中，随机选择节点 1 和节点 8 作为受损节点。如图 2 所示，横纵坐标分别表示移动目标在区域内的 x 和 y 的坐标。图 2 给出了正常节点 7 在这 2 种算法下的估计结果，提出的算法可以有效地适应测量攻击，能够有效跟踪目标，而 SDCF 算法在受到测量攻击时不能有效地跟踪目标。

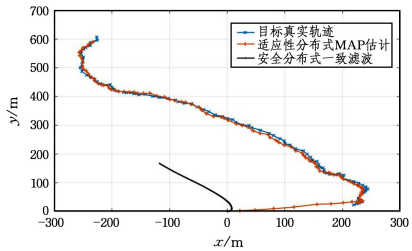

图 2 适应性分布式 MAP 估计与安全分布式一致滤波轨迹跟踪性能对比

Fig. 2 Trajectory tracking performance comparison between resilient distributed MAP estimation and secure distributed consensus filter

图 3 给出了目标真实运动轨迹 $(\chi(t),\eta(t))$ 与节点预测轨迹的仿真结果。在仿真实验中，随机选择节点 1 和节点 8 作为受损节点。

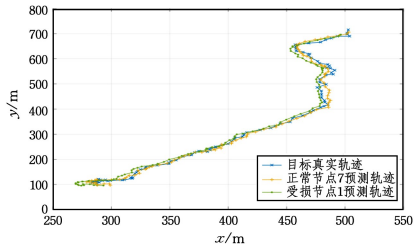

图 3 状态估计结果

Fig. 3 State estimation results

图 3 给出了正常节点 7 和受损节点 1 的估计结果。由图可知，无论是正常节点还是受损节点，均采用了弹性分布式最大后验概率估计方法且能够有效抵御攻击，估计结果接近目标的真实运动轨迹。

图 4 给出了所有节点的根均方误差(Root Mean Square Error，RMSE)随时间变化的仿真结果。假设所有节点没有初始先验估计值，即当受损节点数为 2 时，经过 15 次迭代后，RMSE 从初始的 200 下降到 20 左右，这说明本文提出的算法可以有效消除攻击的影响，能够估计出正确的结果。随着受损节点数的增加，当节点数为 4 时，即受损节点数达到 50% 时，RMSE 呈上升态势，这说明此时所提算法已经失效，不能估计出正确的结果。因为此时正常的测量数据在数量上已经没有优势，所以不能主导估计结果。

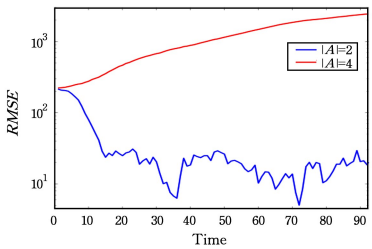

图 4 RMSE 随时间变化曲线

Fig. 4 RMSE versus Time

结束语 本文针对无线传感器网络中线性动态系统在测量攻击下的适应性分布式状态估计问题，即恶意的攻击者能够劫持部分传感器节点并且能够任意修改传感器节点的观测值，提出了适应性分布式最大后验概率估计方法。首先，本文根据卡尔曼滤波设计了集中式最大后验概率估计器。然后，通过融合节点的观测值和邻居节点的先验估计值，利用一致性协议和集中式最大后验概率估计器，进一步设计了分布式最大后验概率估计器。接着，从估计一致性的角度，利用类饱和度的方法，设计出适应性分布式最大后验概率估计器以对抗攻击者。最后，通过仿真实验验证了该算法的有效性。该算法的主要问题在于收敛平台的波动较大，因此可以针对此问题进行进一步的改进。下一步的研究可以与一些非线性模型的卡尔曼滤波方法结合(如扩展卡尔曼滤波、无迹卡尔曼滤波和容积卡尔曼滤波)，考虑非线性测量模型下的适应性状态估计问题。

参 考 文 献

[1] RASTGAR F, RAHMANI M. Consensus-based distributed robust filtering for multisensory systems with stochastic uncertainties [J]. IEEE Sensors Journal, 2018, 18: 7611-7618.

[2] DESHMUKH R, KWON C, HWANG I. Optimal Discrete-Time Kalman Consensus Filter [C]// Proceedings of the 2017 American Control Conference (ACC). Seattle, WA, USA, 2017: 5801-5806.

[3] AMINIOMAM M, TORKAMANI-AZAR F, GHORASHI S A. Generalised Kalman-consensus filter[J]. IET Signal Processing, 2017, 11(5): 495-502.

[4] ZHANG S, LIU W Q, ZHAO N. Research of Consensus in Multi-agent Systems on Complex Network [J]. Computer Science, 2019, 46(4): 95-99.

[5] PASQUALETTI F, DÖRFLER F, BULLO F. Attack detection and identification in cyber-physical systems[J]. IEEE transactions on automatic control, 2013, 58(11): 2715-2729.

[6] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine Generals Problem[J]. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382-401.

[7] DOLEV D, LYNCH N A, PINTER S S, et al. Reaching approximate agreement in the presence of faults [J]. Journal of the ACM (JACM), 1986, 33(3): 499-516.

[8] LEBLANC H J, ZHANG H, KOUTSOUKOS X, et al. Resilient asymptotic consensus in robust networks[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(4): 766-781.

[9] CHEN Y, KAR S, MOURA J M F. Resilient distributed estimation: Sensor attacks[J]. IEEE Transactions on Automatic Control, 2018, 64(9): 3772-3779.

[10] MITRA A, RICHARDS J A, BAGCHI S, et al. Resilient distributed state estimation with mobile agents: overcoming Byzantine adversaries, communication losses, and intermittent measurements[J]. Autonomous Robots, 2019, 43(3): 743-768.

[11] FORTI N, BATTISTELLI G, CHISCI L, et al. Distributed joint attack detection and secure state estimation[J]. IEEE Transactions on Signal and Information Processing over Networks, 2017, 4(1): 96-110.

[12] GUAN Y, GE X. Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks[J]. IEEE Transactions on Signal and Information Processing over Networks, 2017, 4(1): 48-59.

[13] BOLLOBÁS B. Modern graph theory[M]. Springer Science & Business Media, 2013.

[14] OLFATI-SABER R, FAX J A, MURRAY R M. Consensus and cooperation in networked multi-agent systems[J]. Proceedings of the IEEE, 2007, 95(1): 215-233.

[15] WANG S, REN W. On the convergence conditions of distributed dynamic state estimation using sensor networks: A unified framework[J]. IEEE Transactions on Control Systems Technology, 2017, 26(4): 1300-1316.

[16] BATTISTELLI G, CHISCI L. Kullback-Leibler average, consensus on probability densities, and distributed state estimation with guaranteed stability[J]. Automatica, 2014, 50(3): 707-718.

[17] HE X, REN X, SANDBERG H, et al. Secure distributed filtering for unstable dynamics under compromised observations[J]. arXiv: 1903.07345, 2019.

GAO Feng-yue, born in 1987, Ph.D candidate. His main research interests include cooperative communications, network coding and channel coding.