基于信誉机制的分布式扩散最小均方算法

卢光跃* 陈文晓 黄庆东
(西安邮电大学无线网络安全技术国家工程实验室 西安 710121)

摘 要：非安全环境中的无线传感器网络(WSN)可能存在恶意攻击节点，恶意节点将会篡改其观测数据以影响参数估计的准确性。为此，该文提出基于信誉机制的分布式扩散最小均方(R-dLMS)算法和扩散归一化最小均方(R-dNLMS)算法。该算法能够根据各节点对整个网络参数估计的贡献来设置相应的信誉值，从而减小恶意节点对网络攻击的影响。仿真结果表明，与无信誉值的算法相比，该算法的性能得到大幅度提高，且 R-dNLMS 算法在 R-dLMS 算法的基础上，算法性能得到进一步提升。

关键词：无线传感器网络；恶意攻击；分布式；扩散最小均方；信誉值
中图分类号： TP393; TN911.7 **文献标识码**： A **文章编号**：1009-5896(2015)05-1234-07
DOI: 10.11999/JEIT140851

Distributed Diffusion Least Mean Square Algorithm Based on the Reputation Mechanism

Lu Guang-yue Chen Wen-xiao Huang Qing-dong
(*National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an* 710121, *China*)

Abstract: To deal with the problem of signal estimation for Wireless Sensor Networks (WSN) in a untrustworthy environment where malicious nodes tamper the measured data, two reputation-based algorithms, that are, Reputation-based diffusion Least Mean Square (R-dLMS) algorithm and Reputation-based diffusion Normalized Least Mean Square (R-dNLMS) algorithm, are proposed. The proposed algorithms could assign the appropriate reputation value to each node according to its contribution to the whole network, and minimize the reputation value of malicious nodes to lower the impact of malicious nodes in the network. Simulation results show that the proposed algorithms can greatly improve the performance compared with the one without reputation value, and the performance of R-dNLMS algorithm has been further improved based on R-dLMS algorithm.

Key words: Wireless Sensor Network (WSN); Malicious attack; Distributed; Diffusion Least Mean Square (dLMS); Reputation value

1 引言

由多节点组成的无线传感器网络(Wireless Sensor Network, WSN)能够利用传感器节点(简称节点)间的相互协作来实现对监测区域的监测，已广泛应用于精密农业、防火救灾、雷达跟踪、目标定位等[1]。

在利用WSN进行参数估计时，估计算法可分为集中式和分布式。集中式算法要求网络中所有节点将观测数据发送到中心节点，并由中心节点完成数据的处理，因此中心节点负荷较重，易造成网络拥塞，容错能力差；分布式算法没有中心节点，通过节点之间的相互协作实现对参数的估计，与集中式算法相比，分布式算法潜在地节约了能量和通信资源，并且提高了算法的鲁棒性[2−5]。

分布式算法是由不同的协作模式结合不同的自适应算法得到的。根据网络的拓扑结构，协作模式有增量(incremental)协作模式[3]、扩散(diffusion)协作模式[4]和一致协作模式[5]。在增量协作模式中，要求所有的节点组成一个环状循环结构，每个节点利用前一个邻居节点的信息来更新自身的估计值，然后把所得的估计值发送到下一个节点[3]，其中有学者分别针对各节点中的噪声不同[6]以及基于空间和网络的增量算法[7]进行了研究。这样的协作模式虽然需要的能量和通信量较小，易于实现，但对于由大量节点组成的网络来说，把所有节点设计成一个环状循环结构是不现实的。在扩散协作模式中，每个节点与其多个邻居节点进行实时通信，并利用自身和其邻居节点的数据来更新自身的估计值，然后把所得的估计值发送给其邻居节点，这样可以充分利用网络的联通性，且能够处理由大量节点组成的网

2014-06-26 收到，2014-11-18 改回
国家自然科学基金(61271276, 61301091)，陕西省国际合作项目(2013KW01-03)，工业和信息化部通信软科学项目(2014R33)和陕西省自然科学基金(2014JM8299)资助课题
*通信作者：卢光跃 tonylugy@163.com

络[8−10]。而一致协作模式也是通过节点间的协作来达到参数估计的，但需要所有的节点都达到一致的效果，即收敛到相同的值，如基于一致的分布式最小均方算法[5]和能量检测算法[11]以及应用于目标追踪的 Kalman 算法[12]。由于一致协作模式需要每个节点都要收敛到相同值，这也限制了该协作算法在一些实际场景中的应用[13]。而扩散协作模式由于其简单的分布结构和较好的稳健性，得到广泛的关注，例如在稀疏结构当中的应用[14]和一些其它的改进算法[15−17]等。

目前的分布式估计算法一般都是假定网络处于安全信任的环境中，即认为所有节点的观测数据都是安全可靠的，不存在恶意攻击节点。而实际 WSN 中可能存在恶意攻击节点，它通过篡改自身的观测数据，以达到干扰或攻击整个网络的目的[12]。而被恶意篡改的数据参与数据融合时，将会影响参数估计的准确性，甚至无法实现对监测区域内参数的估计或动态目标跟踪[18]。如果能根据恶意节点的篡改程度，对其设置相应的信誉值，就能够在一定程度上减小恶意节点对整个网络参数估计的影响[19,20]。

本文针对 WSN 中恶意节点对参数估计的影响，提出基于信誉机制的扩散最小均方(Reputation-based diffusion Least Mean Square, R-dLMS)和扩散归一化最小均方(Reputation-based diffusion Normalized Least Mean Square, R-dNLMS)算法，它们根据节点对网络的贡献来设置其信誉值，以减小恶意节点对网络的影响。

2　扩散LMS算法

假定由 N 个节点组成的 WSN(如图 1 所示)，要估计未知参数 $\boldsymbol{x}^0 \in R^{M\times 1}$。当节点 k 和节点 l 有通信链接时，它们互为邻居节点，设 N_k 为节点 k 的邻居节点集合(包括节点 k 本身)，记其邻居节点的个数(也称该节点的度)为 $|N_k|$，例如图 1 中节点 3 的 $N_3=\{2,3,k,k+1\}$，$|N_3|=4$。这里假设节点 k 在第 i 时刻的观测值 $y_k(i)$ 和观测向量 $\boldsymbol{h}_k(i)$ 都是相互独立的广义平稳随机过程。

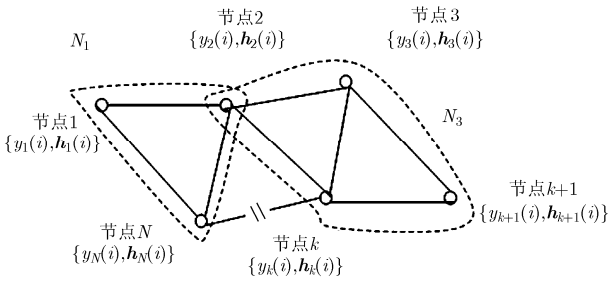


图 1 由 N 个节点组成的 WSN

观测数据的信号模型为

$$y_k(i)=\boldsymbol{h}_k(i)\boldsymbol{x}^0+v_k(i),\quad i=0,1,\cdots \tag{1}$$

其中 $v_k(i)$ 在时间和空间上都相互独立的背景噪声，其方差为 $\sigma_{v,k}^2$。根据分布式扩散协作模式，网络中每个节点只与其邻居节点通信，节点 k 先利用其邻居节点的局部估计值 $\{\boldsymbol{x}_l(i-1)\}_{l\in N_k}$ 进行融合，然后利用融合估计值 $\boldsymbol{\phi}_k(i-1)$ 和节点 k 上的 LMS 自适应滤波算法来更新自身的局部估计值 $\boldsymbol{x}_k(i)$ [4](如图 2 所示)。

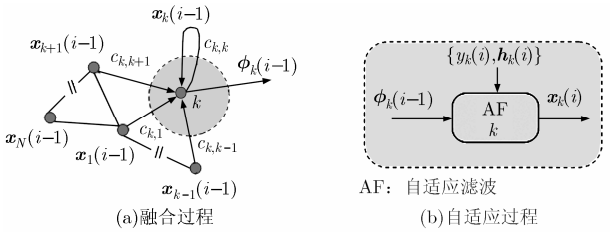


图 2 扩散协作模式的网络结构

对应的扩散LMS(dLMS)算法可总结为

$$\boldsymbol{\phi}_k(i-1)=f_k(\boldsymbol{x}_l(i-1)),\quad l\in N_k \tag{2}$$

$$\boldsymbol{x}_k(i)=\boldsymbol{\phi}_k(i-1)+\boldsymbol{U}_k\boldsymbol{h}_k^{\mathrm{T}}(i)(y_k(i)-\boldsymbol{h}_k(i)\boldsymbol{\phi}_k(i-1)) \tag{3}$$

其中 $\boldsymbol{U}_k=\mu_k\boldsymbol{I}_M$ 是各节点的收敛步长 $\mu_k>0$ 组成的对角矩阵；局部融合函数 f_k 可以是线性或非线性，可以是时变或非时变的，常用的是线性融合函数，即各节点权重的线性组合 $\boldsymbol{\phi}_k(i-1)=\sum_{l\in N_k}c_{kl}\boldsymbol{x}_k(i-1)$，且满足 $\sum_{l\in N_k}c_{kl}=1,\ \forall k$，其中计算融合参数 $c_{kl}(k=1,2,\cdots,N)$ 的融合准则有梅特波利斯(Metropolis)、拉普拉斯和邻近准则[21−23]。

这些融合准则只适用于安全信任环境下的网络，若存在恶意节点，算法性能就会急剧恶化。为此，可根据节点对网络参数估计的贡献来动态地对其设置相应的信誉值，以减小恶意节点对整个网络性能的影响。

3　基于信誉机制的扩散算法

3.1 信誉值的确定

当 WSN 中存在恶意攻击节点时，恶意节点将根据其自身的攻击目的篡改其测量数据。假设恶意攻击节点相对总节点的个数较小，其数据篡改信号模型为

$$y_k(i)=\lambda\cdot\boldsymbol{h}_k(i)\boldsymbol{x}^0+v_k(i) \tag{4}$$

其中 λ 表示恶意节点对信号的篡改程度。λ=1 该节点无攻击行为，而 λ 值偏离 1 越大，其攻击程度越强。

为了反映各节点对整个网络的贡献，利用节点

估计值与其邻居节点估计值的均值之差(这里的差值表示差值的绝对值)，根据其差值大小来对其设置相应的信誉值。

首先，信誉值的初始值设为 $r_{kl}(0)=1/|N_k|$，表示各节点对整个网络的贡献都相等。然后，节点 k 在第 i 时刻将其本身和接收到的邻居节点的估计值集合 $\boldsymbol{X}_{k1}(i)=(x_l(i),\cdots,x_{k-1}(i),x_k(i),x_{k+1}(i),\cdots,x_m(i))$ 做升序排列得到 $\boldsymbol{X}_{k2}(i)$，其中 $l,\ k-1, k+1, m$ 是节点 k 的邻居节点。由于被篡改的信号数据偏离了正常估计值范围，所以如果节点 k 及其邻居节点中存在恶意节点，被恶意篡改的估计值在 $\boldsymbol{X}_{k2}(i)$ 两端的可能性最大。故利用序列 $\boldsymbol{X}_{k2}(i)$ 中间数据的均值 $\theta_k(i)$ 作为当前时刻的估计值。均值 $\theta_k(i)$ 的计算方法为

若 $|N_k|$ 为偶数时，

$$\boldsymbol{X}_{k2}(i)=(x_1(i)\cdots\underbrace{x_l(i)\cdots x_m(i)}_{\text{中间}|N_k|/2\text{个数据}}\cdots x_{|N_k|}(i)) \tag{5}$$

若 $|N_k|$ 为奇数时，

$$\boldsymbol{X}_{k2}(i)=(x_1(i)\cdots\underbrace{x_l(i)\cdots x_m(i)}_{\text{中间}(|N_k|+1)/2\text{个数据}}\cdots x_{|N_k|}(i)) \tag{6}$$

记集合 $\boldsymbol{X}_{k2}(i)$ 中间的 $|N_k|/2$ ($|N_k|$ 为偶数)或 $(|N_k|+1)/2$ ($|N_k|$ 为奇数)个数据集合为 $\boldsymbol{X}_{k3}(i)$。因此节点 k 在第 i 时刻的均值为

$$\theta_k(i)=\begin{cases}\sum\limits_{l\in\boldsymbol{X}_{k3}} x_{kl}(i)/(|N_k|/2), & N_k\text{为偶数}\\ \sum\limits_{l\in\boldsymbol{X}_{k3}} x_{kl}(i)/((|N_k|+1)/2), & N_k\text{为奇数}\end{cases} \tag{7}$$

其中 l 表示节点 k 的邻居节点。

最后，计算节点 k 及邻居节点的估计值和均值 $\theta_k(i)$ 之差，设 $\Delta\boldsymbol{X}_{k1}(i)$ 为 $\boldsymbol{X}_{k1}$ 和该节点均值 $\theta_k(i)$ 的差值集合，即

$$\begin{aligned}\Delta\boldsymbol{X}_{k1}(i)&=(\boldsymbol{X}_{k1}(i)-\boldsymbol{\theta}_k(i))^{\gamma}=((x_l(i)-\theta_k(i))^{\gamma},\cdots,\\&\quad(x_k(i)-\theta_k(i))^{\gamma},\cdots,(x_m(i)-\theta_k(i))^{\gamma})\\&\triangleq(\Delta x_l(i),\cdots,\Delta x_k(i),\cdots,\Delta x_m(i))\end{aligned} \tag{8}$$

其中 $\Delta x_l(i)$ 表示节点 l 与 k 的均值之差的 γ 次方。依据差值的大小可判别恶意节点，该差值越大，是恶意攻击节点的可能性越大，对该节点设置的信誉值也应越小。同时，节点 k 和其邻居节点的信誉值满足 $\sum_{l\in N_k} r_{kl}=1,\forall k$，那么，节点 k 为其邻居节点 l 设置的信誉值可以表示为

$$r_{kl}(i)=\frac{1}{|\Delta x_l(i)|}\Bigg/\left(\sum_{l\in N_k}\frac{1}{|\Delta x_l(i)|}\right) \tag{9}$$

3.2 R-dLMS 算法

当 $\boldsymbol{U}_k=\mu_k\boldsymbol{I}_M$ 时，式(3)的算法为标准的 dLMS 算法[4]，若 WSN 中存在恶意节点，利用所提出的信誉值计算方法来判别恶意节点并对其设置相应的信誉值，那么基于信誉机制的 R-dLMS 算法可总结为表 1。

表 1 基于信誉机制的 R-dLMS 算法

初始化：$r_{kl}(0)=1/|N_k|$, $\boldsymbol{\phi}_k(0)=\boldsymbol{0}$

for i (time)

for k (sensor number)

$$\boldsymbol{\phi}_k(i-1)=\sum_{l\in N_k} r_{kl}(i-1)\boldsymbol{x}_l(i-1)$$

$$e_k(i)=y_k(i)-\boldsymbol{h}_k(i)\boldsymbol{\phi}_k(i-1)$$

$$\boldsymbol{x}_k(i)=\boldsymbol{\phi}_k(i-1)+\mu_k\boldsymbol{h}_k^{\mathrm{T}}(i)e_k(i)$$

$$r_{kl}(i)=\frac{1}{|\Delta x_l(i)|}\Bigg/\sum_{l\in N_k}\frac{1}{|\Delta x_l(i)|}$$

end k

end i

3.3 R-dNLMS算法

由于 R-dLMS 算法的梯度噪声较大，为了降低梯度噪声的干扰，在 R-dLMS 算法的基础上，提出了基于信誉机制的 R-dNLMS 算法，即节点的步长矩阵为 $\boldsymbol{U}_k=\dfrac{\mu_k}{\boldsymbol{h}_k(i)\boldsymbol{h}_k^{\mathrm{T}}(i)+\varepsilon}\boldsymbol{I}_M$，其中 ε 为数值很小的常数，避免分母为 0。那么该算法可总结为表 2 所示。

与 R-dLMS 算法相比，该算法能够有效避免梯度噪声放大的干扰, 因而具有更好的收敛性能。

3.4 算法收敛分析

本节借助范数理论来分析所提出算法的收敛性，首先给出分块矩阵最大范数的定义和一个引理。

分块矩阵最大范数：由 N 个子块 $\boldsymbol{x}_k\in\mathbb{C}^M$, $k\in\{1,2,\cdots,N\}$ 以列 (columns) 形式组成的矩阵 $\boldsymbol{x}=\mathrm{col}\{\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_N\}\in\mathbb{C}^{MN}$，定义其在 $\mathbb{C}^{MN}$ 上的最大范数 $\|\cdot\|_{\mathrm{b}_\infty}$ 为

表 2 基于信誉机制的 R-dNLMS 算法

初始化：$r_{kl}(0)=1/|N_k|$, $\boldsymbol{\phi}_k(0)=\boldsymbol{0}$

for i (time)

for k (sensor number)

$$\boldsymbol{\phi}_k(i-1)=\sum_{l\in N_k} r_{kl}(i-1)\boldsymbol{x}_l(i-1)$$

$$e_k(i)=y_k(i)-\boldsymbol{h}_k(i)\boldsymbol{\phi}_k(i-1)$$

$$\boldsymbol{x}_k(i)=\boldsymbol{\phi}_k(i-1)+\mu_k\frac{\boldsymbol{h}_k^{\mathrm{T}}(i)e_k(i)}{\boldsymbol{h}_k(i)\boldsymbol{h}_k^{\mathrm{T}}(i)+\varepsilon}$$

$$r_{kl}(i)=\frac{1}{|\Delta x_l(i)|}\Bigg/\sum_{l\in N_k}\frac{1}{|\Delta x_l(i)|}$$

end k

end i

$$\|\boldsymbol{x}\|_{\mathrm{b}_\infty}=\max_{1\le k\le N}\|\boldsymbol{x}_k\|$$

其中$\|\cdot\|$表示在$\mathbb{C}^M$上的欧几里得范数。由向量范数可以诱导出分块矩阵最大范数，即一个$MN\times MN$的矩阵$\boldsymbol{A}$，其分块矩阵最大范数定义为

$$\|\boldsymbol{A}\|_{\mathrm{b}_\infty}=\max_{\substack{\boldsymbol{x}\in\mathbb{C}^{MN}\\ \boldsymbol{x}\neq 0}}\frac{\|\boldsymbol{A}\boldsymbol{x}\|_{\mathrm{b}_\infty}}{\|\boldsymbol{x}\|_{\mathrm{b}_\infty}}$$

所定义的分块矩阵最大范数也具有欧几里得范数的性质。

引理 1[24]　由$M\times M$的子块酉阵$\boldsymbol{Y}_k,k\in\{1,2,\cdots,N\}$组成$MN\times MN$的对角酉阵$\boldsymbol{Y}=\mathrm{diag}\{\boldsymbol{Y}_1,\boldsymbol{Y}_2,\cdots,\boldsymbol{Y}_N\}$，具有下面的性质：

(1) $\|\boldsymbol{Y}\boldsymbol{x}\|_{\mathrm{b}_\infty}=\|\boldsymbol{x}\|_{\mathrm{b}_\infty}$，　$\boldsymbol{x}\in\mathbb{C}^{MN}$；

(2) $\left\|\boldsymbol{Y}\boldsymbol{A}\,\boldsymbol{Y}^*\right\|_{\mathrm{b}_\infty}=\|\boldsymbol{A}\|_{\mathrm{b}_\infty}$，$\boldsymbol{A}\in\mathbb{C}^{MN\times MN}$。

前面的随机变量(如$\boldsymbol{h}_k(i)$等)都用下面矩阵的形式来表示：

$$\boldsymbol{X}^0=\mathrm{col}\{\boldsymbol{x}^0,\boldsymbol{x}^0,\cdots,\boldsymbol{x}^0\}$$
$$\boldsymbol{y}_i=\mathrm{col}\{y_1(i),y_2(i),\cdots,y_N(i)\}$$
$$\boldsymbol{v}_i=\mathrm{col}\{v_1(i),v_2(i),\cdots,v_N(i)\}$$
$$\boldsymbol{H}_i=\mathrm{diag}\{\boldsymbol{h}_1(i),\boldsymbol{h}_2(i),\cdots,\boldsymbol{h}_N(i)\}$$

$\boldsymbol{H}_i$是由子块$\{\boldsymbol{h}_k(i):k=1,2,\cdots,N\}$组成的$N\times NM$的对角分块矩阵。那么式(1)的信号模型可表示为

$$\boldsymbol{y}_i=\boldsymbol{H}_i\boldsymbol{X}^0+\boldsymbol{v}_i,\quad i=0,1,\cdots \tag{10}$$

而$\{r_{lk}(i)\}_{l=1}^N$是节点k及其邻居节点l在i时刻的信誉值，且满足$r_{lk}=0,l\notin N_k$和$\sum_{l\in N_k}r_{lk}(i)=1$。各节点的信誉值组成$N\times N$矩阵$\boldsymbol{r}_i$，并定义$MN\times MN$的矩阵$\boldsymbol{G}_i$，

$$\boldsymbol{r}_i=\begin{bmatrix}r_{11}(i)&\cdots&r_{1N}(i)\\ \vdots&\ddots&\vdots\\ r_{N1}(i)&\cdots&r_{NN}(i)\end{bmatrix},\quad \boldsymbol{G}_i=\boldsymbol{r}_i^{\mathrm{T}}\otimes\boldsymbol{I}_M$$

其中$\otimes$表示克罗内克积。收敛步长和信号估计值的矩阵形式分别为

$$\boldsymbol{D}=\mathrm{diag}\{\mu_1\boldsymbol{I}_M,\mu_2\boldsymbol{I}_M,\cdots,\mu_N\boldsymbol{I}_M\}$$
$$\boldsymbol{X}_{i-1}=\mathrm{col}\{\boldsymbol{x}_1(i-1),\boldsymbol{x}_2(i-1),\cdots,\boldsymbol{x}_N(i-1)\}$$
$$\boldsymbol{\phi}_{i-1}=\mathrm{col}\{\boldsymbol{\phi}_1(i-1),\boldsymbol{\phi}_2(i-1),\cdots,\boldsymbol{\phi}_N(i-1)\}$$

那么基于信誉值的 R-dLMS 算法的状态空间模型为

$$\boldsymbol{\phi}_{i-1}=\boldsymbol{G}_i\boldsymbol{X}_{i-1} \tag{11a}$$
$$\boldsymbol{X}_i=\boldsymbol{\phi}_{i-1}+\boldsymbol{D}\boldsymbol{H}_i^*(\boldsymbol{y}_i-\boldsymbol{H}_i\boldsymbol{\phi}_{i-1}) \tag{11b}$$

定义信号估计误差为$\tilde{\boldsymbol{x}}_k(i)=\boldsymbol{x}^0-\boldsymbol{x}_k(i)$，$k=1,2,\cdots,N$，则

$$\widetilde{\boldsymbol{X}}_i=\mathrm{col}\{\tilde{\boldsymbol{x}}_1(i),\tilde{\boldsymbol{x}}_2(i),\cdots,\tilde{\boldsymbol{x}}_N(i)\}=\boldsymbol{X}^0-\boldsymbol{X}_i \tag{12}$$

由于$\sum_{l=1}^N r_{lk}(i)=1$，所以$\boldsymbol{G}_i\boldsymbol{X}^0=\boldsymbol{X}^0$，将式(11b)两边减去$\boldsymbol{X}^0$，则得出全局信号估计误差$\widetilde{\boldsymbol{X}}_i$的递推公式：

$$\widetilde{\boldsymbol{X}}_i=(\boldsymbol{I}_{MN}-\boldsymbol{D}\boldsymbol{H}_i^*\boldsymbol{H}_i)\boldsymbol{G}_i\widetilde{\boldsymbol{X}}_{i-1}+\boldsymbol{D}\boldsymbol{H}_i^*\boldsymbol{v}_i \tag{13}$$

对式(13)两边进行期望运算，由于矩阵$\boldsymbol{G}_i$的分析比较困难，因此，假设当$i\ge 0$时，信誉值矩阵$\boldsymbol{G}_i$与$\boldsymbol{H}_i$和$\boldsymbol{X}_{i-1}$是相互独立的，则推导得

$$E[\widetilde{\boldsymbol{X}}_i]=(\boldsymbol{I}_{MN}-\boldsymbol{D}\boldsymbol{R}_h)\boldsymbol{G}_iE[\widetilde{\boldsymbol{X}}_{i-1}] \tag{14}$$

其中$\boldsymbol{R}_h=\mathrm{diag}\{\boldsymbol{R}_{h,1},\boldsymbol{R}_{h,2},\cdots,\boldsymbol{R}_{h,N}\}$,$\boldsymbol{R}_{h,k}=E[\boldsymbol{h}_k^*(i)\cdot\boldsymbol{h}_k(i)]$, $\boldsymbol{G}_i=E[\boldsymbol{G}_i]$。

由于所有的范数在有限维的向量空间中都是等价的，利用分块矩阵最大范数的性质，可以得到

$$\left\|E[\widetilde{\boldsymbol{X}}_i]\right\|_{\mathrm{b}_\infty}\le\|\boldsymbol{B}\|_{\mathrm{b}_\infty}\cdot\|\boldsymbol{G}_i\|_{\mathrm{b}_\infty}\cdot\left\|E[\widetilde{\boldsymbol{X}}_{i-1}]\right\|_{\mathrm{b}_\infty} \tag{15}$$

其中$\boldsymbol{B}=\boldsymbol{I}_{MN}-\boldsymbol{D}\boldsymbol{R}_h$，如果

$$\sup_{i\ge 0}\left\{\|\boldsymbol{B}\|_{\mathrm{b}_\infty}\cdot\|\boldsymbol{G}_i\|_{\mathrm{b}_\infty}\right\}<1 \tag{16}$$

则$E[\widetilde{\boldsymbol{X}}_i]\to 0$，所以算法收敛的一个充分条件就是$\|\boldsymbol{B}\|_{\mathrm{b}_\infty}<1$和$\|\boldsymbol{G}_i\|_{\mathrm{b}_\infty}<1$。

为了证明$\|\boldsymbol{B}\|_{\mathrm{b}_\infty}<1$，假设$\boldsymbol{R}_{h,k}$的特征值分解为：$\boldsymbol{R}_{h,k}=\boldsymbol{T}_k\boldsymbol{\Lambda}_k\boldsymbol{T}_k^*$，则$\boldsymbol{R}_h$特征值分解为$\boldsymbol{R}_h=\boldsymbol{T}\boldsymbol{\Lambda}\boldsymbol{T}^*$，其中$\boldsymbol{T}=\mathrm{diag}\{\boldsymbol{T}_1,\boldsymbol{T}_2,\cdots,\boldsymbol{T}_N\}$, $\boldsymbol{\Lambda}=\mathrm{diag}\{\boldsymbol{\Lambda}_1,\boldsymbol{\Lambda}_2,\cdots,\boldsymbol{\Lambda}_N\}$。

由于$\boldsymbol{T}^*\boldsymbol{D}\boldsymbol{T}=\boldsymbol{D}$，则$\boldsymbol{B}$特征值分解为：$\boldsymbol{B}=\boldsymbol{T}(\boldsymbol{I}_{MN}-\boldsymbol{D}\boldsymbol{\Lambda})\boldsymbol{T}^*$。

又因为$\boldsymbol{T}$是分块对角酉阵，所以由引理 1 性质(2)得到

$$\begin{aligned}\|\boldsymbol{B}\|_{\mathrm{b}_\infty}&=\|\boldsymbol{I}_{MN}-\boldsymbol{D}\boldsymbol{\Lambda}\|_{\mathrm{b}_\infty}=\max_{1\le k\le N}\|\boldsymbol{I}_{MN}-\mu_k\boldsymbol{\Lambda}_k\|\\&=\max_{1\le k\le N}\max_{1\le m\le M}|1-\mu_k\lambda_{m,k}|\end{aligned} \tag{17}$$

其中$\lambda_{m,k}$是第m个对角子块$\boldsymbol{\Lambda}_k$的特征值。所以，当且仅当

$$0<\mu_k<\frac{2}{\lambda_{\max}(\boldsymbol{R}_{h,k})},\quad k=1,2,\cdots,N \tag{18}$$

时可得$\|\boldsymbol{B}\|_{\mathrm{b}_\infty}<1$。其中$\lambda_{\max}(\boldsymbol{R}_{h,k})$为$\boldsymbol{R}_{h,k}$的最大特征值。而式(18)是 LMS 算法收敛的一个必要条件。

为了证明$\|\boldsymbol{G}_i\|_{\mathrm{b}_\infty}\le 1$，利用分块最大范数的定义和三角不等式，可得

$$\begin{aligned}\|\boldsymbol{G}_i\|_{\mathrm{b}_\infty}&=\max_{\substack{\boldsymbol{x}\in\mathbb{C}^{MN}\\ \boldsymbol{x}\neq 0}}\frac{\|\boldsymbol{G}_i\boldsymbol{x}\|_{\mathrm{b}_\infty}}{\|\boldsymbol{x}_i\|_{\mathrm{b}_\infty}}\\&=\max_{\substack{\boldsymbol{x}\in\mathbb{C}^{MN}\\ \boldsymbol{x}\neq 0}}\max_{1\le k\le N}\left\|\sum_{l\in N_k}E[r_{lk}(i)]\boldsymbol{x}_l\right\|\cdot\frac{1}{\|\boldsymbol{x}\|_{\mathrm{b}_\infty}}\\&\le\max_{\substack{\boldsymbol{x}\in\mathbb{C}^{MN}\\ \boldsymbol{x}\neq 0}}\max_{1\le k\le N}\sum_{l\in N_k}\left|E[r_{lk}(i)]\right|\cdot\frac{\|\boldsymbol{x}_l\|}{\|\boldsymbol{x}\|_{\mathrm{b}_\infty}}\\&\le\max_{1\le k\le N}\sum_{l\in N_k}\left|E[r_{lk}(i)]\right|\end{aligned} \tag{19}$$

由于$r_{lk}(i)\ge 0$且$\sum_{l\in N_k}r_{lk}(i)=1$，所以$\sum_{l\in N_k}|E[r_{lk}(i)]|\le 1$，也即$\|\boldsymbol{G}_i\|_{\mathrm{b}_\infty}\le 1$。

综上所述，如果各节点的步长 μ_k 满足 $0<\mu_k<2/\lambda_{\max}(\boldsymbol{R}_{h,k})$，且随机变量都相互独立时，所提出的 R-dLMS 算法的局部估计值 $\boldsymbol{x}_k(i)$ 能够收敛到未知参数 $\boldsymbol{x}^0$，也即 $E[\boldsymbol{x}_k(i)]\to\boldsymbol{x}^0, i\to\infty, k\in\{1,2,\cdots,N\}$。

以上是对 R-dLMS 算法的收敛分析，而 R-dNLMS 算法是在 R-dLMS 算法的基础上进行了归一化处理[20]，其收敛性能分析与归一化 LMS(NLMS)算法一致，此处不再赘述。

4 仿真分析

本文采用全局均方偏差(Mean Square Deviation, MSD)作为评价算法性能的指标，即 $\mathrm{MSD}=E\left\|\boldsymbol{x}(i)-\boldsymbol{x}^{(0)}\right\|^2\Big/N$，其中 $\boldsymbol{x}(i)=[\boldsymbol{x}_1(i),\boldsymbol{x}_2(i),\cdots,\boldsymbol{x}_N(i)]$ 和 $\boldsymbol{x}^{(0)}=[\boldsymbol{x}^0,\boldsymbol{x}^0,\cdots,\boldsymbol{x}^0]$ 是各节点估计信号和初始信号的矩阵形式。由20个节点组成的WSN网络拓扑结构如图3所示；假设未知参数 $\boldsymbol{x}^0=[1\ 1\ 1\ 1]^{\mathrm{T}}$，每个节点的背景噪声 $v_k(i)$ 的方差分别为 $\sigma_v^2=$ [0.014, 0.034, 0.006, 0.006, 0.0201, 0.0235, 0.006, 0.0251, 0.0345, 0.032, 0.0101, 0.0125, 0.007, 0.018, 0.0127, 0.012, 0.0358, 0.017, 0.016, 0.0225][25]，收敛步长 $\mu_k=0.05, k=1,2,\cdots,N$, γ=0.5, ε=0.01。利用Matlab (R2010a)软件进行1000次独立仿真实验，在下面的仿真中，如无特殊说明，假设节点11(其度为 $|N_{11}|=5$)为恶意攻击节点。

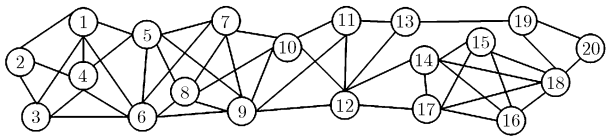


图 3 网络拓扑结构

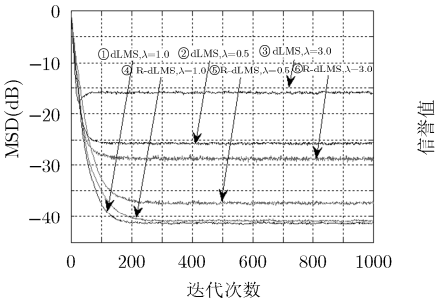
图 4 给出了攻击程度不同时 dLMS 算法与所提出的 R-dLMS 算法仿真对比结果。由图 4 可知，当 $\lambda=1.0$ 时，即网络中没有恶意攻击节点时，R-dLMS 算法的偏差曲线几乎和 dLMS 算法重合，都是在迭代 200 次时达到−41 dB 左右的平稳状态，说明了所提出的 R-dLMS 算法的有效性；当 $\lambda=0.5$ 时，R-dLMS 算法的偏差达到了−37 dB，比 dLMS 算法降低了 11 dB；当 $\lambda=3.0$ 时，R-dLMS 算法偏差达到−29 dB 左右，比 dLMS 算法降低了 14 dB。而此时 R-dLMS 算法对节点 11 和其邻居节点设置的信誉值如图 5 所示，当 R-dLMS 算法达到平稳状态时，给恶意节点 11 设置的信誉值为 0.06 左右，而其邻居节点的信誉值在 0.23 上下波动，是恶意节点的信誉值的 4 倍左右。由对比分析可知，当存在恶意攻击节点时，R-dLMS 算法能够判别出恶意节点并对其设置相应小的信誉值，从而减小恶意节点对参数估计的影响，提高算法的性能。

图 6 给出了在随迭代次数增加的过程中，出现不同攻击程度时 dLMS 与 R-dLMS 算法的对比仿真结果。由图 6 可知，当迭代 200 次左右时 dLMS 和 R-dLMS 算法的偏差都达到了−41 dB 的平稳状态；当迭代 300 次时，出现了恶意攻击且 $\lambda=2.0$，dLMS 算法性能急剧恶化，而 R-dLMS 算法的偏差水平达到了−35 dB，比 dLMS 算法小了 12 dB 左右；当迭代 500 次时，恶意节点攻击程度增加至 $\lambda=3.0$，dLMS 算法性能进一步恶化，而 R-dLMS 算法的偏差达到了−30 dB，比 dLMS 算法小了 13 dB；当迭代 800 次时，恶意攻击消失，dLMS 和 R-dLMS 算法都开始好转，dLMS 算法经过迭代 100 次左右达到平稳，而 R-dLMS 经过迭代近 50 次就达到了平稳状态。

同时，R-dLMS 算法对节点 11 及其邻居节点设置的信誉值如图 7 所示，当迭代 100 次左右时，各节点的信誉值都在 0.200 左右的稳定状态，说明各节点对整个网络参数估计的贡献基本相等；当迭代 300 次时，节点 11 的信誉值由 0.215 变为 0.075 左右，而其邻居节点的信誉值在不同程度上有所增加；当迭代 500 次时，节点 11 的信誉值减小至 0.062 左右，说明节点 11 又实施了进一步的攻击；当迭代 800 次时，所有节点的信誉值又回到了 0.200 左右，说明恶意攻击消失。由此可知，当迭代过程中出现恶意节点时，R-dLMS 算法也能够判别出恶意节点并对其设置相应小的信誉值，从而减小对整个网络的攻击影响。

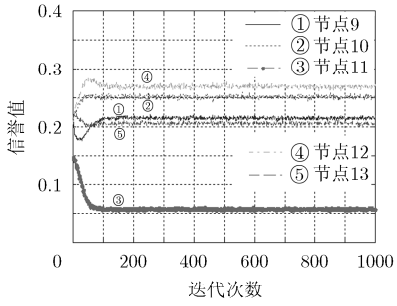
根据攻击节点的度不同时来分析其对整个网络偏差性能的影响，分别假设节点 6, 11, 20(其度分别为 $|N_6|=8, |N_{11}|=5, |N_{20}|=3$)为恶意节点，且 $\lambda=3.0$ 时，dLMS 和 R-dLMS 算法的对比仿真结果如图 8 所示。由图 8 可知，dLMS 算法对应的偏差曲线①, ②, ③，其偏差分别达到−13 dB, −16 dB, −19 dB；而 R-dLMS 算法所对应曲线的偏差分别达到了−26 dB, −28 dB, −31 dB，与 dLMS 算法相比，R-dLMS 算法性能有很大的提升。同时也可以看出，恶意节点的度越大，对整个网络的估计性能影响越大，因此，网络中那些度较大的节点，也应该是网络中保护的重点。

图 9 给出了扩散归一化 LMS(dNLMS)算法和基于信誉值的 R-dNLMS 算法对比仿真结果。由图 9



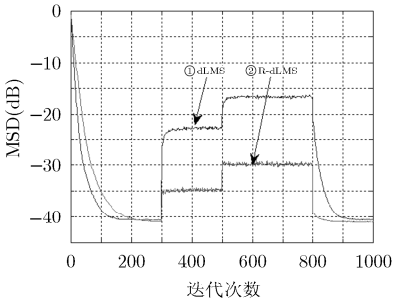
①②③分别为λ不同时dLMS算法的偏差曲线
④⑤⑥分别为λ不同时R-dLMS算法的偏差曲线

图 4　λ值不同时，R-dLMS 算法与 dLMS 算法对比



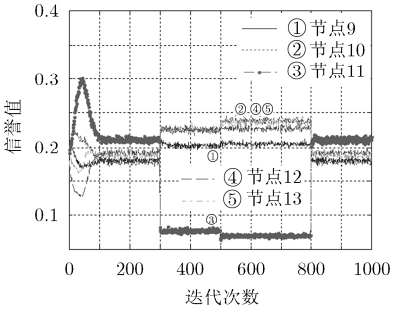
①②④⑤分别为节点9,10,12,13的信誉值曲线
③为恶意节点11的信誉值曲线

图 5　当 $\lambda = 3.0$ 时，恶意节点 11 和其邻居节点的信誉值



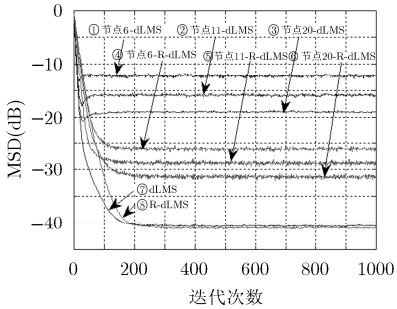
①dLMS算法的偏差曲线
②R-dLMS算法的偏差曲线

图 6　迭代过程中出现恶意攻击时算法对比



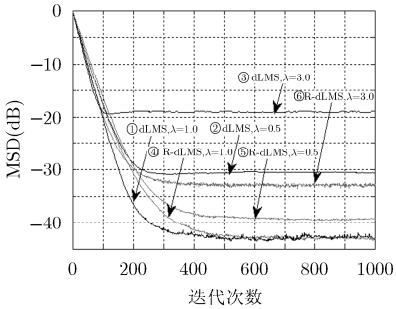
①②④⑤分别为节点9,10,12,13的信誉值曲线
③为恶意节点11的信誉值曲线

图 7 R-dLMS 对节点 11 及其邻居节点设置的信誉值



①②③为节点6,11,20分别是恶意节点时dLMS算法的偏差曲线
④⑤⑥为节点6,11,20分别是恶意节点时R-dLMS算法的偏差曲线
⑦⑧分别为没有恶意节点时dLMS算法和R-dLMS算法的偏差曲线

图 8　节点 6, 11, 20 分别为恶意节点时算法对比



①②③分别为λ不同时dNLMS算法的偏差曲线
④⑤⑥分别为λ不同时R dNLMS算法的偏差曲线

图 9　λ值不同时，R-dNLMS 算法与 dNLMS 算法对比

可知，当 $\lambda = 1.0$ 时，即没有恶意攻击节点时，R-dNLMS 算法能够达到 dNLMS 算法的性能水平，偏差都能达到−43 dB，也进一步说明了所提出算法的有效性；当 $\lambda = 0.5$ 时，R-dNLMS 算法偏差达到了−39 dB，比 dNLMS 算法的偏差降低了 9 dB 左右；当 $\lambda = 3.0$ 时，R-dNLMS 算法的偏差达到了−33 dB，比 dNLMS 算法降低了 14 dB 左右。同时，R-dNLMS 算法给节点 11 及其邻居节点设置的信誉值和图 5 的结果非常相近，并且 R-dNLMS 算法也有与图 6～图 8 相似的仿真结果，此处不再赘述。这也说明了所提出的基于信誉机制的扩散算法能够有效地分辨出恶意节点，并给其设置相应小的信誉值，从而减小恶意节点对整个网络的影响。

从图 4 和图 9 的对比中，可以看出，当 $\lambda = 1.0$ 时，即网络处于安全的环境中，R-dLMS 算法和 R-dNLMS 算法都能分别达到 dLMS 算法和 dNLMS 算法的性能水平；当存在恶意节点且 $\lambda = 3.0$ 时，R-dLMS 算法和 R-dNLMS 算法偏差分别达到−29 dB 和−33 dB，与 dLMS 和 dNLMS 算法相比，所提出的算法都能够大幅度地提升算法的性能。同时，R-dNLMS 算法比 R-dLMS 算法有更好的稳定性，偏差也更小，算法性能更优。

5　结束语

本文主要对处于非安全环境中的无线传感器网络进行研究，当网络中存在恶意攻击节点时，恶意节点篡改其观测数据，并参与数据融合，影响参数估计的准确性，甚至无法实现对监测区域的参数估计。本文利用节点估计值与其邻居节点估计值的均值之差，根据其差值大小来反映节点对整个网络的贡献，并对其设置相应的信誉值，提出基于信誉机制的 R-dLMS 算法和 R-dNLMS 算法，该算法能够使恶意节点的信誉值最小，非恶意节点的信誉值相对较大，从而减小恶意节点对网络攻击的影响。仿真结果验证了算法的正确性和有效性，并且 R-dNLMS 算法在 R-dLMS 算法的基础上，算法性能在一定程度上又得到了进一步的提升。而该算法与信道环境相关的研究将是下一步的重点工作。

参 考 文 献

[1]　Estrin D, Girod L, Pottie G, *et al*.. Instrumenting the world

with wireless sensor networks[C]. Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'01), Salt Lake City, USA, 2001, 4: 2033–2036.

[2] Sayed A H and Lopes C G. Distributed processing over adaptive networks[C]. Proceedings of the 9th International Symposium on Signal Processing and Its Applications (ISSPA), Sharjah, UAE, 2007: 1–3.

[3] Lopes C G and Sayed A H. Incremental adaptive strategies over distributed networks[J]. *IEEE Transactions on Signal Processing*, 2007, 55(8): 4064–4077.

[4] Lopes C G and Sayed A H. Diffusion least-mean squares over adaptive networks: formulation and performance analysis[J]. *IEEE Transactions on Signal Processing*, 2008, 56(7): 3122–3136.

[5] Schizas I D, Mateos G, and Giannakis G B. Distributed LMS for consensus-based in-network adaptive processing[J]. *IEEE Transactions on Signal Processing*, 2009, 57(6): 2365–2382.

[6] Khalili A, Tinati M A, and Rastegarnia A. Steady-state analysis of incremental LMS adaptive networks with noisy links[J]. *IEEE Transactions on Signal Processing*, 2011, 59(5): 2416–2421.

[7] Cattivelli F S and Sayed A H. Analysis of spatial and incremental LMS processing for distributed estimation[J]. *IEEE Transactions on Signal Processing*, 2011, 59(4): 1465–1480.

[8] Khalili A, Tinati M A, Rastegarnia A, *et al*.. Steady-state analysis of diffusion LMS adaptive networks with noisy links[J]. *IEEE Transactions on Signal Processing*, 2012, 60(2): 974–979.

[9] Zhao X and Sayed A H. Combination weights for diffusion strategies with imperfect information exchange[C]. Proceedings of the IEEE International Conference on Communications (ICC), Ottawa, Canada, 2012: 398–402.

[10] Li C, Shen P, Liu Y, *et al*.. Diffusion information theoretic learning for distributed estimation over network[J]. *IEEE Transactions on Signal Processing*, 2013, 61(16): 4011–4024.

[11] 王晓侃, 卢光跃, 包志强, 等. 一种新的分布式协作能量检测算法[J]. 电讯技术, 2012, 52(9): 1480–1485.
Wang Xiao-kan, Lu Guang-yue, Bao Zhi-qiang, *et al*.. A novel distributed cooperative energy detection algorithm[J]. *Telecommunication Engineering*, 2012, 52(9): 1480–1485.

[12] 白辉, 卢光跃, 王晓侃. 非信任环境中一致卡尔曼滤波的数据融合算法[J]. 西安邮电学院学报, 2012, 17(5): 10–14.
Bai Hui, Lu Guang-yue, and Wang Xiao-kan. Data fusion algorithm based on consensus Kalman filter in untrustworthy environment[J]. *Journal of Xi'an University of Posts and Telecommunications*, 2012, 17(5): 10–14.

[13] Cattivelli F S and Sayed A H. Distributed detection over adaptive networks using diffusion adaptation[J]. *IEEE Transactions on Signal Processing*, 2011, 59(5): 1917–1932.

[14] Di Lorenzo P and Sayed A H. Sparse distributed learning based on diffusion adaptation[J]. *IEEE Transactions on Signal Processing*, 2013, 61(6): 1419–1433.

[15] 聂文梅, 卢光跃. 无线传感器网络中丢包扩散卡尔曼算法的改进[J]. 西安邮电学院学报, 2013, 18(4): 9–12.
Nie Wen-mei and Lu Guang-yue. Improved diffusion Kalman algorithm with packet-dropping in wireless sensor networks[J]. *Journal of Xi'an University of Posts and Telecommunications*, 2013, 18(4): 9–12.

[16] 陈文晓, 卢光跃, 黄庆东. 改进的分布式扩散符号 LMS 算法[J]. 电讯技术, 2013, 53(12): 1580–1585.
Chen Wen-xiao, Lu Guang-yue, and Huang Qing-dong. An improved distributed diffusion sign-LMS algorithm[J]. *Telecommunication Engineering*, 2013, 53(12): 1580–1585.

[17] Li J, Chen W, Kang S, *et al*.. A diffusion-based distributed collaborative energy detection algorithm for spectrum sensing in cognitive radio[J]. *Communications and Network*, 2013, 5(3): 276–279.

[18] 冯景瑜, 卢光跃, 包志强. 认知无线电安全研究综述[J]. 西安邮电学院学报, 2012, 17(2): 47–52.
Feng Jing-yu, Lu Guang-yue, and Bao Zhi-qiang. A survey on cognitive radio security[J]. *Journal of Xi'an University of Posts and Telecommunications*, 2012, 17(2): 47–52.

[19] de Paula A and Panazio C. Analysis of distributed parameter estimation in WSN with unreliable nodes[C]. Proceedings of the International Symposium on Wireless Communication Systems, Paris, France, 2012: 116–120.

[20] Lopes C G. Diffusion adaptive networks with changing topologies[C]. Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, Las Vegas, USA, 2008: 3285–3288.

[21] Xiao L and Boyd S. Fast linear iterations for distributed averaging[J]. *Systems & Control Letters*, 2004, 53(1): 65–78.

[22] Olfati-Saber R and Murray R M. Consensus problems in networks of agents with switching topology and time-delays[J]. *IEEE Transactions on Automatic Control*, 2004, 49(9): 1520–1533.

[23] Jadbabaie A, Lin J, and Morse A S. Coordination of groups of mobile autonomous agents using nearest neighbor rules[J]. *IEEE Transactions on Automatic Control*, 2003, 48(6): 988–1001.

[24] Takahashi N, Yamada I, and Sayed A H. Diffusion least-mean squares with adaptive combiners: formulation and performance analysis[J]. *IEEE Transactions on Signal Processing*, 2010, 58(9): 4795–4810.

[25] Xie S L and Li H R. Distributed LMS with limited data rate[J]. *Electronics Letters*, 2011, 47(9): 541–542.

卢光跃： 男，1971 年生，博士，教授，博士生导师，研究方向为现代移动通信中信号处理.

陈文晓： 男，1985 年生，硕士生，研究方向为无线传感器网络中的数据融合.

黄庆东： 男，1977 年生，博士，副教授，研究方向为自适应信号处理及分布式算法.