

比特率约束下的动态加密分布式估计算法

张志祥¹, 孙 颖², 丁德锐¹, 杜 雨³

(1. 上海理工大学 光电信息与计算机工程学院, 上海 200093; 2. 上海理工大学 管理学院, 上海 200093;
3. 上海理工大学 理学院, 上海 200093)

摘 要: 本文提出了一种面向无线传感器网络的比特率约束下带有动态加密机制的分布式估计算法。分布在不同位置上的传感器之间的通信是通过无线网络实现的, 不可避免地遭受隐私泄露和带宽受限的问题。因此, 针对该问题, 提出一种比特率约束下带有动态加密机制的分布式估计算法。为了防止敏感信息在传输过程中被窃听, 设计基于动态加密矩阵的数据加密方案, 并在带宽比特率约束下为每个信道分配带宽, 确保数据传输的隐私性并满足网络带宽限制。在此基础上, 提出一种新的分布式估计算法, 通过数学推导证明算法的误差有界性和误差方差的渐近有界性, 并确定迭代步长的取值范围。最后, 通过数值仿真验证算法的有效性, 并采用均方偏差作为衡量标准, 对算法的性能进行了全面验证, 结果表明所提出的算法在实际应用中表现卓越。

关键词: 无线传感器网络; 分布式估计; 扩散策略; 动态加密; 比特率约束; 隐私安全

中图分类号: TP309; TP393. 08

文献标志码: A

文章编号: 1003-7241(2026)10-0127-09

Distributed estimation algorithm with dynamic encryption mechanisms under bitrate constraints

Zhang Zhixiang¹, Sun Ying², Ding Derui¹, Du Yu³

(1. School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China; 2. Business School, University of Shanghai for Science and Technology, Shanghai 200093, China;
3. College of Science, University of Shanghai for Science and Technology, Shanghai 200093, China)

Abstract: This paper proposes a distributed estimation algorithm integrated with a dynamic encryption mechanism under bit rate constraints for wireless sensor networks (WSNs). Sensors deployed at disparate geographic locations communicate via wireless networks, which inevitably brings about two challenges: data privacy leakage and limited bandwidth resources. To tackle the above issues, a distributed estimation algorithm embedded with a dynamic encryption mechanism under bit rate constraints is developed in this work. To prevent sensitive information from being eavesdropped during transmission, a lightweight encryption scheme based on dynamic encryption matrices is devised. Meanwhile, fine-grained bandwidth allocation is performed for each communication channel subject to bit rate constraints, which simultaneously guarantees transmission privacy and complies with network bandwidth limitations. On this basis, a novel distributed estimation framework is constructed. Rigorous mathematical derivations are provided to prove the boundedness of estimation errors and the asymptotic boundedness of error variance, and the feasible interval of iterative step sizes is explicitly determined to stabilize algorithm convergence. Finally, numerical simulations are carried out to validate the efficacy of the proposed algorithm. The mean square deviation (MSD) is adopted as the performance metric for comprehensive evaluations. Simulation results verify that the proposed algorithm achieves outstanding performance in practical scenarios.

Keywords: wireless sensor networks; distributed estimation; diffusion strategy; dynamic encryption; bit rate constraints; privacy security

随着无线通信技术和传感器技术的发展, 具有传感、计算和通信能力的网络中的分布式估计已成为研究热点^[1-3]。在分布式估计中, 通过相邻节点的局部信息, 协同估计感兴趣的参数, 使得每个节点生成与感兴趣的参数相接近的估计值。其算法主要包括 3 种方式: 一致性策

略^[4]、增量策略^[5]、扩散策略^[6-7]。3 种方式中的扩散策略性能更好, 其具有更低的复杂性、更小的均方偏差和较好的稳定性^[8]。自适应扩散最小均方算法是一种流行的基于分布式扩散的优化问题自适应解决方案^[9]。本文对于算法的改进研究就是基于自适应-结合扩散最小均方算

收稿日期: 2025-06-20; 录用日期: 2025-08-23

基金项目: 国家自然科学基金(62203306, 62373251)

作者简介: 张志祥(2000—), 男, 硕士研究生, 研究方向为分布式状态估计等。

通信作者: 孙 颖(1991—), 女, 博士, 讲师, 硕士研究生导师, 研究方向为网络化系统的控制与滤波等。

引用本文: 张志祥, 孙颖, 丁德锐, 等. 比特率约束下的动态加密分布式估计算法[J]. 自动化技术与应用, 2026, 45(10): 127-134, 188. (Zhang Zhixiang, Sun Ying, Ding Derui, et al. Distributed estimation algorithm with dynamic encryption mechanisms under bitrate constraints[J]. Techniques of Automation and Applications, 2026, 45(10): 127-134, 188.)

法进行的。

然而,在一些场景中,个人隐私丢失和安全问题也逐渐显现^[10]。扩散策略需要与邻居之间进行信息交换,当目标参数向量包含敏感信息时,直接传输局部估计会导致严重的隐私泄露^[11]。为了避免敏感信息的泄露,一些文献^[12-14]将需要传输的数据添加一个扰动来保护隐私,这虽然保护了数据的安全,但是同样也导致数据的精度降低^[15],可能会有较大的均方误差,并且如何选择一个合适的扰动也是一个具有挑战性的任务。加密技术可以提供很高的隐私保护水平^[16-17],保证只有拥有解密密钥的人才能访问原始数据,还能防止数据在传输过程中被篡改,确保数据完整性^[18]。因此,本文使用加密机制对传输的数据进行加密。具体策略是,由于传输的是参数向量,通过对原始数据乘以一个加密矩阵,使其能较好的保护数据的隐私。

此外,在一些物联网和传感器网络中,每个传感器的节点都是由电池进行供电,它们的能量和通信带宽都是受限的^[19]。为了克服这个问题,一些文献提出减少需要合作的邻居节点数量^[20-22],还有一些提出降低邻居间传输信息的维度^[23-25]。但是这些方法都不可避免地影响了原本算法的性能。还有一些文献利用事件触发机制减少算法的通信量,在文献[26]提出的算法中,传感器的中间估计只有在满足触发准则时才会传递给相邻节点,从而减小通信负担。然而,事件触发机制要选择一个合适的阈值条件具有一定困难^[27]。在文献[28]中研究了无线传感器网络中总比特率约束下的分布式参数估计问题。文献[29]为了满足总的能量约束引入了等效单位能量均方误差函数来确定每个传感器的最佳量化比特率和传输能量。因此,结合节点能量和带宽有限的实际情况,本文在算法中加入了比特率约束,为每个节点分配合适的比特数,对数据进行量化,使得算法能够在总的比特率约束下正常进行。综上所述,本文的主要贡献如下。

1) 设计了一种基于动态加密矩阵的数据隐私保护策略。

2) 提出了一种比特率约束下的带有动态加密机制的分布式估计算法。

3) 得到了满足误差和误差方差渐近有界的步长的值范围。

1 问题描述

考虑一个由无向图 $G = (v, \varepsilon)$ 表示的网络,其中 $v = 1, 2, \dots, N$ 示节点集, ε 是边集。对任意的 $\forall i, j \in v$, 如果 $(i, j) \in \varepsilon$, 则节点 j 可视为节点 i 的邻居, N_i 为节点 i 邻居节点的集合。对于任意两个节点 $i, j \in v$, 如果存在一个序列 $(i, v_1), (v_1, v_2), \dots, (v_{p-1}, v_p), (v_p, j)$ 的边序列, 则称图 G 为连通图。在不失一般性, 本文假设采用的网络是连通的。

1.1 系统模型和扩散算法

设 N 个节点分别观测未知向量 $w_o \in \mathbb{R}^{L \times 1}$, 其观测的

线性标量值 $d_{k,i}$ 为

$$d_{k,i} = u_{k,i}^T w_o + v_{k,i} \quad (1)$$

其中, $k \in [1, N]$ 是传感器的索引, i 表示观测的时间, $u_{k,i} \in \mathbb{R}^{L \times 1}$ 是传感器 k 在 i 时刻已知的线性回归向量, $v_{k,i}$ 是一个零均值、方差为 $\sigma_{v,k}^2$ 的高斯白噪声。

分布式估计是借助于相邻节点的信息交换以及已知的测量标量 $d_{k,i}$ 和回归向量 $u_{k,i}$ 协同自适应地估计未知向量 w_o 。为了准确地估计该未知向量, 通常采用基于扩散的分布式估计算法。扩散算法采用两种策略, 分别称为“先组合后适应”(combine-then-adapt, CTA) 和“先适应后组合”(adapt-then-combine, ATC)。由于已有文献证明 ATC 策略的性能优于 CTA 策略, 因此本文采用 ATC 策略:

$$\begin{cases} \varphi_{k,i} = w_{k,i-1} + \mu_k u_{k,i} (d_{k,i} - u_{k,i}^T w_{k,i-1}) \\ w_{k,i} = \sum_{l \in N_k} b_{lk} \varphi_{l,i} \end{cases} \quad (2)$$

式中, μ_k 是适当的迭代步长, $\varphi_{k,i}$ 是中间向量, 系数 $b_{lk} (l \in N_k)$ 表示邻居信息的权重, 满足如下假设。

假设 1 权重系数 b_{lk} 是非负实数且满足: 当 $l \notin N_k$ 时, $b_{lk} = 0$ 以及 $\sum_{l \in N_k} b_{lk} = 1$ 。

1.2 动态加密机制

上述 ATC 策略依赖于邻居节点之间的信息交换, 在信息传输过程中可能会遭到攻击使得某些重要的信息泄露。因此本文考虑利用一个动态加密机制对传输的中间向量 $\varphi_{k,i}$ 进行加密, 使得算法具有一定的安全性。为此, 本文采用基于时变的线性变换对待传输的中间向量 $\varphi_{k,i}$ 实施动态加密, 该加密机制可建模为

$$\vec{\varphi}_{k,i} = S_{k,i} \varphi_{k,i} \quad (3)$$

式中, $\vec{\varphi}_{k,i}$ 表示加密后的中间向量, $S_{k,i}$ 是有界的动态密钥, 满足 $S_{k,i}^T S_{k,i} \geq \bar{S}_k > 0$ 。动态加密机制使用的密钥的设计遵循如下特定的规则:

$$S_{k,i} = \begin{bmatrix} \varepsilon_h & F_h \\ x_h & y_{k,i} \end{bmatrix} \quad (4)$$

式中, $\varepsilon_h \in \mathbb{R}^{(L-P) \times (L-P)}$ 是可逆矩阵, $F_h \in \mathbb{R}^{(L-P) \times P}$ 和 $X_h \in \mathbb{R}^{P \times (L-P)}$ 是任意矩阵, 它们都是事先储存在每个传感器节点中的私钥, 并且可以根据整个网络所处的通信环境的评估结果进行更改。 $y_{k,i} \in \mathbb{R}^{P \times P}$ 是一个时变矩阵, 可产生如下公钥:

$$S_{k,i} = Y_{k,i} - X_h \varepsilon_h^{-1} F_h \quad (5)$$

可知 $S_{k,i}$ 是一个可逆的方阵。

为了使邻居节点可靠地获得它需要的信息, 时变的公钥 $S_{k,i}$ 和加密的中间向量 $\vec{\varphi}_{k,i}$ 一起传输给邻居节点。因此, 加密信息的解密机制可表示为

$$\hat{\varphi}_{k,i} = S_{k,i}^{-1} \vec{\varphi}_{k,i} \quad (6)$$

式中, $\hat{\varphi}_{k,i}$ 为 $\vec{\varphi}_{k,i}$ 解密后的中间估计值。在后续内容中,

$R_{\text{total}} \geq \sum_{k=1}^N R_k$ 可以表示为以下形式:

$$R_{\text{total}} \geq \sum_{k=1}^N R_k \quad (7)$$

1.3 比特率约束

在实际的传感器网络中,每个传感器节点的资源都是有限的,整个网络的带宽也是有限。因此,本文考虑了网络的比特率约束:

$$R_{\text{total}} \geq \sum_{k=1}^N R_k \quad (8)$$

式中, R_{total} 是由整个网络决定的总可用比特率, R_k 表示节点 k 所分配到的比特率。

为了信息在比特率约束下能够正常进行传输,加密后的中间向量 $\vec{\varphi}_{k,i}$ 需要通过一个设计好的量化器 k 编码为字符串。对于节点 k , 假设其加密后的数据包处于下面的量化区域中,即

$$Q_k \triangleq \{\vec{\varphi}_{k,i} \in \mathbb{R}^L: |\vec{\varphi}_{k,i}^{(f)}| \leq b_k, f \in \mathbb{Z}_m\} \quad (9)$$

式中, b_k 是一个尺度参数且 $b_k > 0$, $\vec{\varphi}_{k,i}^{(f)}$ 是向量 $\vec{\varphi}_{k,i}$ 的第 f 个元素。通过选择整数 q_k , 将超矩形 Q_k 划分为 q_k^L 个子超矩形。它们可以由下面的乘积形式描述:

$$I_{kf}(s_f^k) = \prod_{k=1}^L I_k^f(s_f^k) = I_k^1(s_1^k) \times \cdots \times I_k^L(s_L^k)$$

其中, $s_f^k \in \{1, 2, \dots, q_k\}$, $I_k^f(s_f^k)$ 表示与第 k 个传感器的第 f 个元素相关的第 s_f^k 个子超矩形。另外,该子超矩形可描述为

$$I_{kf}(s_f^k) = \left\{ \vec{\varphi}_{k,i}^{(f)} \left| -b_k + \frac{2(s_f^k - 1)b_k}{q_k} \leq \vec{\varphi}_{k,i}^{(f)} < -b_k + \frac{2s_f^k b_k}{q_k} \right. \right\}$$

这里,最佳量化水平值 $q_k^{[30]}$ 为

$$q_k = \text{Bit}_k = \lfloor \sqrt{2^{R_k}} - \lceil \log_2 N \rceil \rfloor$$

得益于该划分,记为

$$-b_k + \frac{2(s_{t,i}^{(i)}(\vec{\varphi}_{k,i}^{(i)})) - 1)b_k}{q_k} \leq \vec{\varphi}_{k,i}^{(i)} < -b_k + \frac{2s_{t,i}^{(i)}(\vec{\varphi}_{k,i}^{(i)})b_k}{q_k}。加$$

密后的中间向量 $\vec{\varphi}_{k,i}$ 可编码为序列:

$$S_{k,i}(\vec{\varphi}_{k,i}) = [s_0^k \ s_{1,i}^k(\vec{\varphi}_{k,i}^{(1)}) \ \cdots \ s_{L,i}^k(\vec{\varphi}_{k,i}^{(L)})] \quad (10)$$

式中, s_0^k 表示传感器标签(类似 IP 地址), 序列 $\{s_{1,i}^k, s_{2,i}^k, \dots, s_{L,i}^k\}$ 封装着来自传感器节点 k 的加密数据。该编码序列 $S_{k,i}$ 将传输给邻居。

接下来讨论解密操作。通过可识别的标签 s_0^k , 编码后的数据可通过以下操作进行解码,即

$$\begin{cases} \mathbf{n}_t = S_{t,i} \times [1 \ 0_L]^T \\ \vec{\varphi}_{n_t,i} = \mathbf{h}_{n_t}(s_{1,i}^{n_t}, s_{2,i}^{n_t}, \dots, s_{L,i}^{n_t}) \\ \mathbf{h}_{n_t} \triangleq [c_{1,i}^{n_t} \ c_{2,i}^{n_t} \ \cdots \ c_{L,i}^{n_t}]^T \end{cases} \quad (11)$$

式中, $c_{f,i}^{n_t}$ 可通过下式计算得到,有

$$c_{f,i}^{n_t} = -b_{n_t} + \frac{(2s_{f,i}^{n_t} - 1)b_{n_t}}{\text{Bit}_{n_t}} \quad (12)$$

显然, $c_{f,i}^{n_t}$ 代表区间 $I_{n_t}^f(s_{f,i}^{n_t})$ 的中点值。因此,对于任

意的 $\vec{\varphi}_{k,i} \in Q_k$, 有一组唯一的整数 $\{s_{1,i}^k, s_{2,i}^k, \dots, s_{L,i}^k\}$ 可以确保 $\vec{\varphi}_{k,i}$ 位于满足以下条件的指定子超矩形内,即

$$\|\vec{\varphi}_{k,i} - \vec{\varphi}_{k,i}^{\sim}\|_2 \leq \frac{\sqrt{L}b_k}{\text{Bit}_k} \quad (13)$$

观察上式可以知道 $\frac{\sqrt{L}b_k}{\text{Bit}_k}$ 反映了数据编码和解码的误差界限。定义解码误差为 $\gamma_{k,i} \triangleq \vec{\varphi}_{k,i} - \vec{\varphi}_{k,i}^{\sim}$, 它的上界

为 $\left(\frac{\sqrt{L}b_k}{\text{Bit}_k}\right)^2$ 。

2 本文提出的算法

在这一节中将提出的动态加密机制和比特率约束整合到扩散算法中,下面对算法进行详细的阐述。

首先,网络中每个节点还是利用其自身的信息和邻居的信息对参数向量 $\mathbf{w}_0$ 进行估计。对算法的改进是在中间向量 $\varphi_{k,i}$ 的传输部分,即局部节点计算得到的中间估计值先经过动态加密机制进行加密,然后考虑到比特率的限制,利用量化器进行二进制编码,进而将编码后的信息传递给邻居。结合式(13),邻居节点最终收到并用于计算的解密信息为

$$\hat{\varphi}_{k,i} = S_{k,i}^{-1} \vec{\varphi}_{k,i} = \varphi_{k,i} - S_{k,i}^{-1} \gamma_{k,i} \quad (14)$$

值得注意的是,在组合步骤中每个节点总是组合自身的中间估计值。因此,算法的组合步骤可写为

$$\mathbf{w}_{k,i} = b_{kk} \varphi_{k,i} + \sum_{l \in N_k/k} b_{lk} \hat{\varphi}_{l,i} \quad (15)$$

因此改进后的分布式估计算法可写为

$$\begin{cases} \varphi_{k,i} = \mathbf{w}_{k,i-1} + \mu_k \mathbf{u}_{k,i} (d_{k,i} - \mathbf{u}_{k,i}^T \mathbf{w}_{k,i-1}) \\ \mathbf{w}_{k,i} = b_{kk} \varphi_{k,i} + \sum_{l \in N_k/k} b_{lk} \hat{\varphi}_{l,i} \end{cases} \quad (16)$$

综上所述,将改进后的分布式估计总结为算法 1,并详细说明了算法的运行过程。算法 1 的详细步骤如下。

步骤 1 参数初始化。对每个节点 k 的每一时刻 k 进行更新。

步骤 2 局部更新。

$$\varphi_{k,i} = \mathbf{w}_{k,i-1} + \mu_k \mathbf{u}_{k,i} (d_{k,i} - \mathbf{u}_{k,i}^T \mathbf{w}_{k,i-1})$$

步骤 3 动态加密。设计密钥 $S_{k,i}$, 对中间估计 $\varphi_{k,i}$

进行加密,有 $\vec{\varphi}_{k,i} = S_{k,i} \varphi_{k,i}$

步骤 4 编码。计算编码序列 $S_{k,i}(\vec{\varphi}_{k,i})$

步骤 5 解码。根据标签 S_0^k 和(11)进行解码,有

$$\vec{\varphi}_{n_t,i} \triangleq [c_{1,i}^{n_t} \ c_{2,i}^{n_t} \ \cdots \ c_{L,i}^{n_t}]^T$$

步骤 6 数据解密。

$$\hat{\varphi}_{k,i} = \varphi_{k,i} - S_{k,i}^{-1} \gamma_{k,i}$$

步骤 7 扩散组合。

$$\mathbf{w}_{k,i} = b_{kk} \varphi_{k,i} + \sum_{l \in N_k/k} b_{lk} \hat{\varphi}_{l,i}$$

3 性能分析

在本节中,将通过理论推导对算法的误差有界性和误差方差有界性进行分析。

3.1 估计误差的递归形式

为了方便后面的性能分析,记每个节点 k 在 i 时刻的估计误差为

$$\bar{\varphi}_{k,i} = \mathbf{w}_o - \varphi_{k,i} \quad (17)$$

$$\bar{\mathbf{w}}_{k,i} = \mathbf{w}_o - \mathbf{w}_{k,i} \quad (18)$$

根据系统模型(1)和式(16)~(18)可以得到

$$\bar{\varphi}_{k,i} = (\mathbf{I}_L - \mu_k \mathbf{u}_{k,i} \mathbf{u}_{k,i}^T) \bar{\mathbf{w}}_{k,i} - \mu_k \mathbf{u}_{k,i} \mathbf{v}_{k,i} \quad (19)$$

由 $\gamma_{k,i}$ 的定义、式(14)和式(16),计算可得

$$\mathbf{w}_{k,i} = b_{kk} \varphi_{k,i} + \sum_{l \in N_k/k} b_{lk} (\varphi_{l,i} - \mathbf{S}_{l,i}^{-1} \gamma_{l,i}) \quad (20)$$

然后,对上面式子两边同时减去 $\mathbf{w}_o$ 得到

$$\bar{\mathbf{w}}_{k,i} = \sum_{l \in N_k} b_{lk} \bar{\varphi}_{l,i} + \sum_{l \in N_k/k} b_{lk} \mathbf{S}_{l,i}^{-1} \gamma_{l,i} \quad (21)$$

引入矩阵 $\mathbf{B}_o$, 它的第 (l,k) 个元素是组合权重系数 b_{lk} 。进而,记矩阵 $\mathbf{A}_o = \mathbf{B}_o - \text{diag}\{(b_{kk})_{k=1}^N\}$ 。此外,为了方便后续描述,定义了下面一些符号,有

$$\mathbf{W}_i = \text{col}\{(\bar{\mathbf{w}}_{k,i})_{k=1}^N\}, \quad (22)$$

$$\boldsymbol{\varepsilon}_i = \text{col}\{(\mathbf{S}_k^{-1}, i) \gamma_{k,i}\}_{k=1}^N$$

然后,综合考虑式(19)、(21)、(22)得到如下递归公式:

$$\mathbf{W}_i = \tilde{\mathbf{P}}_i \mathbf{W}_i - \mathbf{B}^T \mathbf{M} \mathbf{u}_i + \mathbf{A}^T \boldsymbol{\varepsilon}_i \quad (23)$$

其中,

$$\mathbf{B} = \mathbf{B}_o \otimes \mathbf{I}_L, \mathbf{A} = \mathbf{A}_o \otimes \mathbf{I}_L$$

$$\tilde{\mathbf{P}}_i = \mathbf{B}^T (\mathbf{I}_{LN} - \mathbf{M} \tilde{\mathbf{R}}_i^u)$$

$$\tilde{\mathbf{R}}_i^u = \text{diag}\{(\mathbf{u}_{k,i} \mathbf{u}_{k,i}^T)_{k=1}^N\}$$

$$\mathbf{M} = \text{diag}\{(\mu_k \mathbf{I}_L)_{k=1}^N\}$$

$$\mathbf{u}_i = \mathbf{B}^T \text{col}\{(\mathbf{u}_{k,j} \mathbf{v}_{k,i})_{k=1}^N\}$$

3.2 误差有界性

在给出主要结果之前,先给出一些假设,作为后续证明的基础。

假设2 噪声 $\mathbf{v}_{k,i}$ 是与所有的输入向量 $\mathbf{u}_{k,i}$ 不相关的。

假设3 输入的回归向量 $\{\mathbf{u}_{k,i}\}$ 是零均值、空间独立、时间白化的。回归向量 $\mathbf{u}_{k,i}$ 的协方差矩阵 $\mathbf{R}_k^u$ 是正定的,也就是 $\mathbf{R}_k^u = \mathbf{E}[\mathbf{u}_{k,i} \mathbf{u}_{k,i}^T]$ 。

假设4 每个节点 k 采用的回归协方差矩阵 $\mathbf{R}_k^u$, 其特征值满足:

$$\lambda_{\max}(\mathbf{R}_k^u) < \left(\frac{2 + \sqrt{2}}{2 - \sqrt{2}} \right) \lambda_{\min}(\mathbf{R}_k^u)$$

考虑假设2和假设3,对式(21)的两边同时取期望可以得到如下估计误差的递归形式,有

$$\mathbf{E}[\mathbf{W}_i] = \mathbf{P} \mathbf{E}[\mathbf{W}_{i-1}] + \mathbf{A}^T \mathbf{E}[\boldsymbol{\varepsilon}_i] \quad (24)$$

其中,

$$\mathbf{P} = [\tilde{\mathbf{P}}_i] = \mathbf{B}^T (\mathbf{I}_{LN} - \mathbf{M} \mathbf{R}^u),$$

$$\mathbf{R}^u = \mathbf{E}[\tilde{\mathbf{R}}_i^u] = \text{diag}\{(\mathbf{R}_k^u)_{k=1}^N\}$$

接下来,将对所提算法的误差进行分析,揭示了误差期望的稳定性。

定理1 误差有界性。当假设1~3成立时,对于设计的分布式估计算法(16),如果步长 μ_k 的选择满足:

$$\mu_k < \frac{2}{\lambda_{\max}(\mathbf{R}_k^u)} \quad (25)$$

那么,估计误差向量 $\mathbf{W}_i$ 是渐近有界的,且上界为

$$\frac{\alpha}{1 - \beta} \max_{1 \leq k \leq N} \|\lambda(\bar{\mathbf{S}}_k^{-1})\| \frac{\sqrt{L} b_k}{\text{Bit}_k} \quad (26)$$

其中,

$$\alpha = \max_{1 \leq k \leq N} (1 - b_{kk}), \beta = \|\mathbf{I}_{LN} - \mathbf{M} \mathbf{R}^u\|_{\infty} < 1.$$

证明 根据可逆矩阵的性质,式(13)和式(22),计算可得

$$\begin{aligned} \|\boldsymbol{\varepsilon}_i\|_{\infty} &= \|\text{col}\{(\mathbf{S}_{k,i}^{-1}) \gamma_{k,i}\}\|_{\infty} \leq \\ &\max_{1 \leq k \leq N} \|\mathbf{S}_{k,i}^{-1} \gamma_{k,i}\|_{\infty} \leq \\ &\max_{1 \leq k \leq N} \|\mathbf{S}_{k,i}^{-1}\|_2 \frac{\sqrt{L} b_k}{\text{Bit}_k} \leq \\ &\max_{1 \leq k \leq N} \|\lambda(\mathbf{S}_{k,i}^{-1})\| \frac{\sqrt{L} b_k}{\text{Bit}_k} \end{aligned} \quad (27)$$

为了便于后续分析,记 $\Gamma \triangleq \frac{\sqrt{L} b_k}{\text{Bit}_k}$ 。根据范数的性质

可以得到

$$\|\boldsymbol{\varepsilon}_i\|_{\infty} \leq \max_{1 \leq k \leq N} \|\lambda(\mathbf{S}_{k,i}^{-1})\| \Gamma \quad (28)$$

另一方面, $\mathbf{B}$ 满足条件 $\mathbf{B}^T \mathbf{1} = \mathbf{1}$, 所以它是一个左随机矩阵。接下来,利用左随机矩阵的性质,有

$$\begin{aligned} \rho(\mathbf{P}) &= \rho(\mathbf{B}^T (\mathbf{I}_{LN} - \mathbf{M} \mathbf{R}^u)) \leq \rho(\mathbf{I}_{LN} - \mathbf{M} \mathbf{R}^u) = \\ &\|\mathbf{I}_{LN} - \mathbf{M} \mathbf{R}^u\|_{\infty} \end{aligned} \quad (29)$$

当条件(25)成立时,有

$$\|\mathbf{I}_{LN} - \mathbf{M} \mathbf{R}^u\|_{\infty} < 1 \quad (30)$$

由式(24)可得均方误差的上界为

$$\mathbf{E}[\mathbf{W}_i] = \mathbf{P}^i \mathbf{E}[\mathbf{W}_0] + \sum_{j=0}^{i-1} \mathbf{P}^{i-1-j} \mathbf{A}^T \mathbf{E}[\boldsymbol{\varepsilon}_{j+1}] \quad (31)$$

对式(31)两端取范数,并利用矩阵范数的一些基本特性,有

$$\begin{aligned} \|\mathbf{E}[\boldsymbol{\varepsilon}_i]\|_{\infty} &\leq \|\mathbf{P}\|_{\infty}^i \|\mathbf{E}[\mathbf{W}_0]\|_{\infty} + \\ &\sum_{j=0}^{i-1} \|\mathbf{P}\|_{\infty}^{i-1-j} \|\mathbf{A}\|_{\infty}^T \|\mathbf{E}[\boldsymbol{\varepsilon}_{j+1}]\|_{\infty} \leq \\ &\|\mathbf{B}\|_{\infty}^i \|\mathbf{I}_{LN} - \mathbf{M} \mathbf{R}^u\|_{\infty}^i \|\mathbf{E}[\mathbf{W}_0]\|_{\infty} + \\ &\sum_{j=0}^{i-1} \|\mathbf{B}\|_{\infty}^{i-1-j} \|\mathbf{I}_{LN} - \mathbf{M} \mathbf{R}^u\|_{\infty}^{i-1-j} \times \\ &\|\mathbf{A}\|_{\infty} \|\mathbf{E}[\boldsymbol{\varepsilon}_{j+1}]\|_{\infty} \end{aligned}$$

令 $\alpha = \|\mathbf{A}\|_{\infty}$, 根据文献[7]中的引理D.3,有

$$\alpha = \|\mathbf{A}\|_{\infty} = \max_{1 \leq k \leq N} (1 - b_{kk}) \quad (32)$$

然后,根据左随机矩阵的性质有 $\|\mathbf{B}\|_{\infty} = 1$ 。记 $\beta = \|\mathbf{I}_{LN} - \mathbf{M} \mathbf{R}^u\|_{\infty}$, 由式(32)可得:

$$\|\mathbf{E}[\mathbf{W}_i]\|_{\infty} \leq \beta^i \|\mathbf{E}[\mathbf{W}_0]\|_{\infty} + \alpha \max_{1 \leq k \leq N} \|\lambda(\bar{\mathbf{S}}_k^{-1})\| \Gamma \sum_{j=0}^{i-1} \beta^j$$

当 μ_k 满足式(25)时, β 满足 $0 \leq \beta < 1$ 。进而,由上式不难有

$$\lim_{i \rightarrow \infty} \|E[\mathbf{W}_i]\|_{\infty} \leq \frac{\alpha}{1 - \beta} \max_{1 \leq k \leq N} |\lambda(\bar{\mathbf{S}}_k^{-1})| \Gamma$$

即估计误差向量 $\mathbf{W}_i$ 是渐近有界的。

证毕。

3.3 误差方差的收敛性分析

由于引入动态加密机制和比特率约束,邻居接收到的信息与适应步得到中间估计存在一个间隙,精确地分析均方误差是难以实现的。代替地,本节将给出该误差方差的上界。

首先,给出权重误差方差的一个递归公式。具体地,给定一个具有合适维度的非负定矩阵 $\Xi = \mathbf{I}_{LN}/N$, 由递归式(23)推导可得

$$\begin{aligned} \|\mathbf{W}_i\|_{\Xi}^2 &= \mathbf{W}_{i-1}^T \tilde{\mathbf{P}}_i^T \Xi \tilde{\mathbf{P}}_i \mathbf{W}_{i-1} + \\ &\quad \mathbf{u}_i^T \mathbf{M}^T \mathbf{B} \Xi \mathbf{B}^T \mathbf{M} \mathbf{u}_i + \boldsymbol{\varepsilon}_i^T \mathbf{A} \Xi \mathbf{A}^T \boldsymbol{\varepsilon}_i + \\ &\quad 2\mathbf{W}_{i-1}^T \tilde{\mathbf{P}}_i \Xi \mathbf{A}^T \boldsymbol{\varepsilon}_i - 2\mathbf{u}_i^T \mathbf{M}^T \mathbf{B} \Xi \mathbf{A}^T \boldsymbol{\varepsilon}_i - \\ &\quad 2\mathbf{W}_{i-1}^T \tilde{\mathbf{P}}_i^T \Xi \mathbf{B}^T \mathbf{M} \mathbf{u}_i \end{aligned} \quad (33)$$

式中, $\|\mathbf{W}_i\|_{\Xi}^2 = \mathbf{W}_i^T \Xi \mathbf{W}_i$ 。

然后,对该式两边取数学期望有

$$E[\|\mathbf{W}_i\|_{\Xi}^2] = E[\|\mathbf{W}_{i-1}\|_{\Xi}^2] + z_2 + z_3 + 2z_4 - 2z_5 - 2z_6 \quad (34)$$

其中,

$$\Xi'_1 = E[\tilde{\mathbf{P}}_i^T \Xi \tilde{\mathbf{P}}_i]$$

$$z_2 = E[\mathbf{u}_i^T \mathbf{M}^T \mathbf{B} \Xi \mathbf{B}^T \mathbf{M} \mathbf{u}_i]$$

$$z_3 = E[\boldsymbol{\varepsilon}_i^T \mathbf{A} \Xi \mathbf{A}^T \boldsymbol{\varepsilon}_i]$$

$$z_4 = E[\mathbf{W}_{i-1}^T \tilde{\mathbf{P}}_i \Xi \mathbf{A}^T \boldsymbol{\varepsilon}_i]$$

$$z_5 = E[\mathbf{u}_i^T \mathbf{M}^T \mathbf{B} \Xi \mathbf{A}^T \boldsymbol{\varepsilon}_i]$$

$$z_6 = E[\mathbf{W}_{i-1}^T \tilde{\mathbf{P}}_i^T \Xi \mathbf{B}^T \mathbf{M} \mathbf{u}_i]$$

在假设 2 和假设 3 下, z_6 的期望值为零。进而,令

$$\begin{aligned} \mathbf{D} &= E[\tilde{\mathbf{P}}_i^T \Xi \tilde{\mathbf{P}}_i] = (\mathbf{I}_{L^2N^2} - \mathbf{I}_{LN} \otimes \mathbf{M} \mathbf{R}^u - \mathbf{M} \mathbf{R}^u \otimes \mathbf{I}_{LN} + \\ &\quad (\mathbf{M} \otimes \mathbf{M}) E[\tilde{\mathbf{R}}_i^u \otimes \tilde{\mathbf{R}}_i^u]) \mathbf{B} \otimes \mathbf{B} \end{aligned} \quad (35)$$

式中, $E[\tilde{\mathbf{R}}_i^u \otimes \tilde{\mathbf{R}}_i^u] = \text{diag}\{(\mathbf{R}_k^u \otimes \mathbf{R}_k^u)_{k=1}^N\}$ 。

定义 $\mathbf{J} = \text{vec}(\Xi)$ 和 $\mathbf{J}' = \text{vec}(\Xi')$, 可得 $\mathbf{J}' = \mathbf{D}\mathbf{J}$ 。基于此,式(34)可以表示为

$$E[\|\mathbf{W}_i\|_{\mathbf{J}}^2] = E[\|\mathbf{W}_{i-1}\|_{\mathbf{D}\mathbf{J}}^2] + z_2 + z_3 + 2z_4 - 2z_5 \quad (36)$$

为了计算得到权重误差方差的渐近上界,接下来将讨论式(36)中的后三项 $z_2 - z_5$ 。

1) 项 z_2 的上界

根据矩阵内积的迹等于两个矩阵的向量化向量的内积,即 $\text{Tr}(\mathbf{A}\mathbf{B}) = (\text{vec}(\mathbf{A}))^T \text{vec}(\mathbf{B})$ 的性质,有

$$\begin{aligned} z_2 &= E[\text{Tr}(\mathbf{B}^T \mathbf{M} \mathbf{u}_i \mathbf{u}_i^T \mathbf{M} \mathbf{B} \Xi)] = \text{Tr}[\mathbf{B}^T \mathbf{M} E[\mathbf{u}_i \mathbf{u}_i^T] \mathbf{M} \mathbf{B} \Xi] = \\ &\quad \text{Tr}(\mathbf{B}^T \mathbf{M} \mathbf{H} \mathbf{M} \mathbf{B} \Xi) = \text{vec}(\mathbf{B}^T \mathbf{M} \mathbf{H} \mathbf{M} \mathbf{A})^T \mathbf{J} \end{aligned} \quad (37)$$

式中, $\mathbf{H} = \text{diag}\{(\sigma_{v,k}^2 \mathbf{R}_k^u)_{k=1}^N\}$ 。

2) 项 z_3 的上界

与 z_2 项类似,对项 z_3 计算可得

$$\begin{aligned} z_3 &= \text{Tr}[\mathbf{A}^T E[\boldsymbol{\varepsilon}_i \boldsymbol{\varepsilon}_i^T] \Xi] = \\ &\quad \text{vec}(\mathbf{A})^T [\Xi \otimes E[\boldsymbol{\varepsilon}_i \boldsymbol{\varepsilon}_i^T]] \text{vec}(\mathbf{A}) \end{aligned} \quad (38)$$

进一步地,不难有

$$E[\boldsymbol{\varepsilon}_i \boldsymbol{\varepsilon}_i^T] \leq E[\boldsymbol{\varepsilon}_i^T \boldsymbol{\varepsilon}_i] \mathbf{I}_{LN} \leq N \max_{1 \leq k \leq N} |\lambda(\bar{\mathbf{S}}_k^{-1})| \Gamma \mathbf{I}_{LN} \quad (39)$$

记 $\Lambda = N \max_{1 \leq k \leq N} |\lambda(\bar{\mathbf{S}}_k^{-1})| \Gamma$ 。由于 Ξ 中的每个元素均大于 0, 有如下不等式

$$\Xi \otimes [E[\boldsymbol{\varepsilon}_i \boldsymbol{\varepsilon}_i^T] - \Lambda \mathbf{I}_{LN}] \leq 0 \quad (40)$$

所以有

$$\text{vec}(\mathbf{A})^T \{\Xi \otimes [E[\boldsymbol{\varepsilon}_i \boldsymbol{\varepsilon}_i^T] - \Lambda \mathbf{I}_{LN}]\} \text{vec}(\mathbf{A}) \leq 0 \quad (41)$$

为了获得 z_3 项的上界,经过一些移项操作得到一个与式(41)等价的不等式,有

$$\begin{aligned} \text{vec}(\mathbf{A})^T \{\Xi \otimes E[\boldsymbol{\varepsilon}_i \boldsymbol{\varepsilon}_i^T]\} \text{vec}(\mathbf{A}) &\leq \\ \Lambda \text{vec}(\mathbf{A})^T (\Lambda \otimes \mathbf{I}_{LN}) \text{vec}(\mathbf{A}) &= \\ \Lambda \text{Tr}(\mathbf{A}^T \mathbf{A} \Xi) \end{aligned} \quad (42)$$

最后,回顾 z_3 的表达式(38),通过式(42)的对比可得到其上界为

$$z_3 \leq \Lambda \cdot \text{vec}(\mathbf{A}^T \mathbf{A}) \mathbf{D} \quad (43)$$

3) 项 z_4 的上界

根据正半定矩阵的性质,矩阵 Ξ 可分解为 $\Xi = \mathbf{U}\mathbf{U}^T$ 。

然后,令

$$\mathbf{Y} = \mathbf{W}_{i-1}^T \tilde{\mathbf{P}}_i^T \mathbf{U}, \mathbf{K} = \boldsymbol{\varepsilon}_i^T \mathbf{A} \mathbf{U} \quad (44)$$

鉴于事实 $(\mathbf{Y} - \mathbf{K})(\mathbf{Y} - \mathbf{K})^T \geq 0$, 可以得到:

$$\mathbf{Y}\mathbf{K}^T + \mathbf{K}\mathbf{Y}^T \leq \mathbf{Y}\mathbf{Y}^T + \mathbf{K}\mathbf{K}^T \quad (45)$$

将 $\mathbf{Y}$ 和 $\mathbf{K}$ 的表达式代入到式(45)中,对不等式两边同时取数学期望,可以得到:

$$\begin{aligned} 2z_4 &\leq E[\mathbf{w}_{i-1}^T \tilde{\mathbf{P}}_i^T \Xi \tilde{\mathbf{P}}_i \mathbf{w}_{i-1}] + E[\boldsymbol{\varepsilon}_i^T \Xi^T \boldsymbol{\varepsilon}_i] = \\ &\quad E\|\mathbf{w}_{i-1}\|_{\Xi'_1}^2 + z_3 \end{aligned} \quad (46)$$

4) 项 z_5 的下界

采用类似的方法,不难有

$$\begin{aligned} z_5 &= \text{Tr}[\mathbf{A}^T E[\boldsymbol{\varepsilon}_i \mathbf{u}_i^T] \mathbf{M} \mathbf{B} \Xi] = \\ &\quad \text{vec}(\mathbf{A}^T E[\boldsymbol{\varepsilon}_i \mathbf{u}_i^T] \mathbf{M} \mathbf{B} \Xi)^T \mathbf{J} \end{aligned} \quad (47)$$

对于期望 $E[\boldsymbol{\varepsilon}_i \mathbf{u}_i^T]$, 它的第 (k, l) 元素的值为

$$\begin{aligned} E[\boldsymbol{\varphi}_{k,l} \mathbf{u}_{l,i} \mathbf{v}_{l,i}] &= E[\mathbf{w}_{k,i-1} \mathbf{u}_{l,i} \mathbf{v}_{l,i}] + \\ &\quad \mu_k E[\mathbf{u}_{k,i} \mathbf{u}_{k,i}^T \mathbf{W}_{i-1} \mathbf{u}_{l,i} \mathbf{v}_{l,i}] + \mu_k E[\mathbf{u}_{k,i} \mathbf{v}_{k,i} \mathbf{u}_{l,i} \mathbf{v}_{l,i}] \end{aligned} \quad (48)$$

值得注意的是,当 $l \neq k$ 时,式(48)的值是等于零的。但是,当 $l = k$ 时,式(48)中的前两项值为零,而最后一项的值为 $\mu_k \sigma_{v,k}^2 \mathbf{R}_k^u$ 。所以,对于项 z_5 的取值情况仅有以下两种

$$z_5 = \begin{cases} 0, & l \neq k \\ \text{vec}(\mathbf{A}^T \mathbf{M} \mathbf{H} \mathbf{M} \mathbf{B})^T \mathbf{J}, & l = k \end{cases} \quad (49)$$

根据式(36)可知,需使用 z_5 的最小值进行计算,即取 $z_5 = 0$ 。因此,将上述的界代入式(36),可以得到权重误差方差上界为

$$E\|\mathbf{W}_i\|_{\mathbf{J}}^2 \leq E\|\mathbf{W}_{i-1}\|_{\mathbf{F}\mathbf{J}}^2 + [\mathbf{o}_1 + \mathbf{o}_2]^T \quad (50)$$

其中,

$$\mathbf{o}_1 = \text{vec}(\mathbf{B}^T \mathbf{M} \mathbf{H} \mathbf{M} \mathbf{B}),$$

$$\mathbf{o}_2 = 2\Lambda \cdot \text{vec}(\mathbf{A}^T \mathbf{A}), \mathbf{F} = 2\mathbf{J}$$

定理 2 误差方差的渐近有界性。当假设 1~4 成立时,对于设计的分布式估计算法 (16),如果步长 μ_k 的选择满足:

$$\frac{1 - \frac{\sqrt{2}}{2}}{\lambda_{\min}(\mathbf{R}_k^u)} < \mu_k < \frac{1 + \frac{\sqrt{2}}{2}}{\lambda_{\max}(\mathbf{R}_k^u)}$$

那么,估计误差向量 $\mathbf{W}_i$ 的方差是渐近有界的,且上界近似为

$$(\mathbf{o}_1 + \mathbf{o}_2)^T (\mathbf{I}_{L^2 N^2} - \mathbf{f})^{-1} \text{vec}(\mathbf{I}_{LN}) / N,$$

其中,

$$\mathbf{f} = 2\mathbf{P}^T \otimes \mathbf{P}^T = [\mathbf{I}_{L^2 N^2} - \mathbf{I}_{LN} \otimes \mathbf{M}\mathbf{R}^u - \mathbf{M}\mathbf{R}^u \otimes \mathbf{I}_{LN} + (\mathbf{M} \otimes \mathbf{M})(\mathbf{R}^u \otimes \mathbf{R}^u)] \mathbf{B} \otimes \mathbf{B} \quad (51)$$

证明 为了分析算法误差方差的渐近有界性,由式(50)迭代计算可得

$$\mathbb{E} \|\mathbf{W}_i\|_J^2 \leq \mathbb{E} \|\mathbf{W}_0\|_{F^i J}^2 + (\mathbf{o}_1 + \mathbf{o}_2)^T \left(\sum_{j=0}^{i-1} \mathbf{F}^j \right) \mathbf{J} \quad (52)$$

将式(35)代入 $\mathbf{F} = 2\mathbf{D}$, 并与式(51)进行比较,可得

$$\mathbf{F} = \mathbf{f} + \mathbf{O}(\mathbf{M}^2) \quad (53)$$

其中,

$$\mathbf{O}(\mathbf{M}^2) = (\mathbf{M} \otimes \mathbf{M})(\mathbb{E}[\tilde{\mathbf{R}}_i^u \otimes \tilde{\mathbf{R}}_i^u] - \mathbf{R}^u \otimes \mathbf{R}^u)$$

进而 $\mathbf{F}$ 的 i 次幂可展开为

$$\mathbf{F}^i = (\mathbf{f} + \mathbf{O}(\mathbf{M}^2))^i = \mathbf{f}^i + i\mathbf{f}^{i-1}\mathbf{O}(\mathbf{M}^2) + \mathbf{C}$$

其中, $\mathbf{C}$ 为包含 $\mathbf{O}(\mathbf{M}^2)$ 的更高阶项。因此,对于足够小的步长 μ_k , 不难有

$$\mathbf{F}^i \approx \mathbf{f}^i + i\mathbf{f}^{i-1}\mathbf{O}(\mathbf{M}^2)$$

接下来,将式(53)代入到式(52)中,可得 $\mathbb{E} \|\mathbf{W}_i\|_J^2$ 的近似上界为

$$\begin{aligned} \mathbb{E} \|\mathbf{W}_i\|_J^2 &\leq \mathbb{E} \|\mathbf{W}_0\|_{\mathbf{f}^i J + i\mathbf{f}^{i-1}\mathbf{O}(\mathbf{M}^2)J}^2 + \\ &\mathbf{h}^T \sum_{j=0}^{i-1} \mathbf{f}^j + j\mathbf{f}^{j-1}\mathbf{O}(\mathbf{M}^2) \mathbf{J} \leq \\ &\mathbb{E} \|\mathbf{W}_0\|_{\mathbf{f}^i J}^2 + \mathbb{E} \|\mathbf{W}_0\|_{\mathbf{f}^{i-1}\mathbf{O}(\mathbf{M}^2)J}^2 + \\ &\mathbf{h}^T \sum_{j=0}^{i-1} \mathbf{f}^j J + \mathbf{h}^T \sum_{j=0}^{i-1} j\mathbf{f}^{j-1}\mathbf{O}(\mathbf{M}^2) \mathbf{J} \end{aligned} \quad (54)$$

其中, $\mathbf{h} = \mathbf{o}_1 + \mathbf{o}_2$ 。

另一方面,矩阵 $\mathbf{f}$ 可分解为 $\mathbf{f} = \mathbf{V}\mathbf{\Theta}\mathbf{V}^{-1}$, 其中 $\mathbf{V}$ 是一个正交矩阵, $\mathbf{\Theta}$ 表示由 $\mathbf{f}$ 的特征值构成的对角矩阵。当 $\rho(\mathbf{f}) < 1$ 时, $\mathbf{f}$ 是指数衰减的,使得

$$\begin{cases} \lim_{i \rightarrow \infty} \mathbf{f}^i = 0, \\ \lim_{i \rightarrow \infty} \sum_{j=0}^i j\mathbf{f}^{j-1}\mathbf{O}(\mathbf{M}^2) = \frac{\mathbf{O}(\mathbf{M}^2)}{(\mathbf{I}_{L^2 N^2} - \|\mathbf{f}\|)^2} \end{cases}$$

将其代入(54)并取极限,有

$$\begin{aligned} \lim_{i \rightarrow \infty} \mathbb{E} \|\mathbf{W}_i\|_J^2 &\leq \lim_{i \rightarrow \infty} (\mathbb{E} \|\mathbf{W}_0\|_{\mathbf{f}^i J}^2 + \\ &\mathbf{h}^T \sum_{j=0}^{i-1} \mathbf{f}^j J + \mathbf{h}^T \sum_{j=0}^{i-1} j\mathbf{f}^{j-1}\mathbf{O}(\mathbf{M}^2) \mathbf{J}) = \\ &\lim_{i \rightarrow \infty} \mathbf{h}^T \sum_{j=0}^{i-1} \mathbf{f}^j J + \frac{\mathbf{O}(\mathbf{M}^2)}{(\mathbf{I}_{L^2 N^2} - \|\mathbf{f}\|)^2} \end{aligned} \quad (55)$$

由于 $\mathbf{\Xi} = \mathbf{I}_{LN}/N$,

不难有 $\mathbf{J} = \frac{1}{N} \text{vec}(\mathbf{I}_{LN})$ 。当 $\rho(\mathbf{f}) < 1$ 成立时,可得

$$\lim_{i \rightarrow \infty} \mathbf{h}^T \sum_{j=0}^{i-1} \mathbf{f}^j \mathbf{J} = \frac{1}{N} \mathbf{h}^T (\mathbf{I}_{L^2 N^2} - \mathbf{f})^{-1} \text{vec}(\mathbf{I}_{LN}) \quad (56)$$

因此,误差方差是渐近有界的。

最后,回顾:

$$\rho(\mathbf{f}) = \rho(2\mathbf{P}^T \otimes \mathbf{P}^T) = 2\rho(\mathbf{P})^2,$$

其约束 $\rho(\mathbf{f}) < 1$ 成立的充分条件是 $\rho(\mathbf{P}) < \frac{\sqrt{2}}{2}$ 。根

据文献[7]中的引理 D.5,可得

$$\rho(\mathbf{P}) \leq \rho(\mathbf{I}_{LN} - \mathbf{M}\mathbf{R}^u) = \max_{1 \leq k \leq N} \rho(\mathbf{I}_L - \mu_k \mathbf{R}_k^u)$$

进一步地,为了确保 $\rho(\mathbf{P}) < \frac{\sqrt{2}}{2}$, 需有

$$\max_{1 \leq k \leq N} \rho(\mathbf{I}_L - \mu_k \mathbf{R}_k^u) < \frac{\sqrt{2}}{2}$$

这就意味着每个节点 k 都要满足

$$\max_{1 \leq l \leq L} |1 - \mu_k \lambda_l(\mathbf{R}_k^u)| < \frac{\sqrt{2}}{2}$$

该式等价于

$$|1 - \mu_k \lambda_l(\mathbf{R}_{u,k})| < \frac{\sqrt{2}}{2}$$

因此,对于任意的 $\{\lambda_l(\mathbf{R}_k^u) | 1 \leq l \leq L\}$, 由上式可以得出 μ_k 需满足条件

$$\frac{1 - \frac{\sqrt{2}}{2}}{\lambda_l(\mathbf{R}_k^u)} < \mu_k < \frac{1 + \frac{\sqrt{2}}{2}}{\lambda_l(\mathbf{R}_k^u)}$$

最后,注意到假设 4, 不难得到

$$\frac{1 - \frac{\sqrt{2}}{2}}{\lambda_{\min}(\mathbf{R}_k^u)} < \mu_k < \frac{1 + \frac{\sqrt{2}}{2}}{\lambda_{\max}(\mathbf{R}_k^u)}$$

证毕。

4 数值仿真

本节将借助于一个数值例子来验证提出的分布式算法的有效性。具体地,一方面在比特率约束下,检验了动态加密机制对数据的隐私保护能力;另一方面,通过与非合作的分布式估计算法、经典的扩散最小均方算法^[9]和变步长的最小均方算法^[31]的比较,检验所提算法的优越性。实验设备采用 Windows 11 操作系统且配置了一个运行在 2.30 GHz 和 16.00 GB RAM 的 Intel (R) Core (TM) i7-11800H 处理器,应用程序在 Matlab R2021b 环境中运行。实验结果是网络经过 $i = 10\ 000$ 次迭代运行获得的。

设待估计的未知参数向量 $\mathbf{w}_0$ 的维度 $L = 10$, 其理论值的 10 个元素依次为 1.455 7, 8.532 6, 1.969 6, 7.673 5, 4.723 8, -2.081 1, -2.317 8, 4.754 6, 5.450 0, -2.116 2。传感器网络由 20 个节点组成,其拓扑结构如图 1 所示。

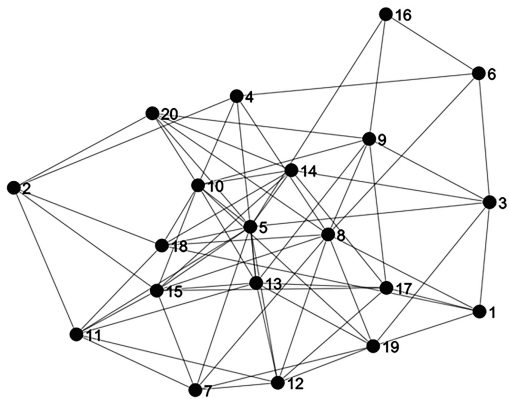


图 1 网络拓扑图
Fig. 1 Network topology diagram

为了获得测量数据,实现该未知向量的估计,本文具有高斯分布的输入 $u_{k,i}$ 是通过 Matlab 随机生成的,且满足假设 3,其中 $R_k^u = \sigma_{u,k}^2 I_L$, $\sigma_{u,k}$ 是在区间 $[10, 12]$ 之间均匀选取的。测量噪声的方差 $\sigma_{v,k}^2 = 0.0001$ 。在仿真中,我们为每个节点都分配了相同的比特数 $R_k = 29 \times L + 2$, 其中额外的 2 比特用于传输传感器的 IP 地址。此外,动态密钥取 ϵ_h 为一个 5×5 的矩阵:

$$\epsilon_h = \begin{bmatrix} 4 & -3 & -1 & 4 & 8 \\ 5 & 8 & 9 & 7 & 9 \\ 1 & 10 & -4 & 10 & 6 \\ 7 & 8 & -4 & 5 & 2 \\ 7 & 8 & 0 & 9 & -3 \end{bmatrix}$$

对于任意矩阵 ϵ_h 和 X_h 其中的元素都为 1,即

$$\epsilon_h = X_h = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

对于动态矩阵 $Y_{k,i}$ 是通过 MATLAB 生成的,其中的元素是均匀分布在 w_o 中元素的最大值和最小值的范围中的。最终的加密矩阵满足条件 $S_{k,i} S_{k,i}^T \geq \bar{S}_k > 0$, 其中,

$$\bar{S}_k = \begin{bmatrix} 111 & 92 & 71 & 49 & 21 & 26 & 26 & 26 & 26 \\ 92 & 305 & 178 & 121 & 140 & 52 & 52 & 52 & 52 \\ 71 & 178 & 258 & 170 & 164 & 37 & 37 & 37 & 37 \\ 49 & 121 & 170 & 163 & 157 & 32 & 32 & 32 & 32 \\ 21 & 140 & 164 & 157 & 208 & 35 & 35 & 35 & 35 \\ 26 & 52 & 37 & 32 & 35 & 130 & 48 & 49 & 48 \\ 26 & 52 & 37 & 32 & 35 & 48 & 130 & 49 & 49 \\ 26 & 52 & 37 & 32 & 35 & 49 & 49 & 130 & 49 \\ 26 & 52 & 37 & 32 & 35 & 49 & 49 & 49 & 130 \\ 26 & 52 & 37 & 32 & 35 & 48 & 49 & 49 & 48 & 130 \end{bmatrix}$$

最后,根据定理 2 可得迭代步长取 $\mu_k = 0.03$ 。算法性能是根据均方偏差(dB) 来进行评估的,计算方式为

$$MSD = 10 \log_{10} (E \| w_k - w_o \|^2 / N)$$

1) 算法的收敛性实验。

图 2 的结果展示了所提算法的估计结果,观察整体和局部放大图可以很轻松看出,在稳态时,算法所得到的估计值 w_k 处于最优值 w_o 附近。这表明算法经过一定的迭代次数后能够收敛到最优值,展示了本文所提算法的收敛性能。

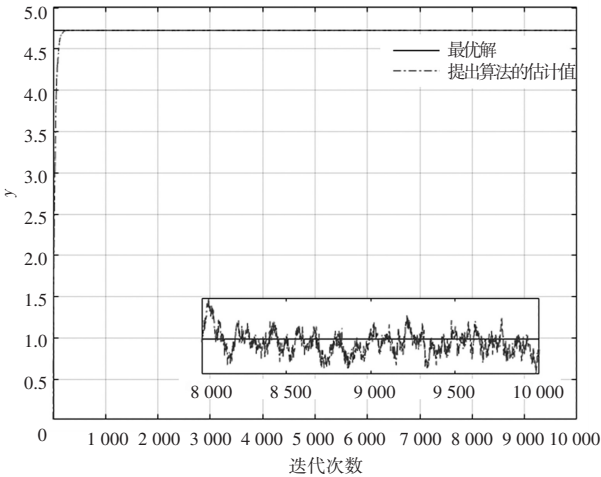


图 2 算法估计值与最优值

Fig. 2 Estimated values of the algorithm versus optimal values

2) 算法的隐私性实验及结果。

另外,进行了算法的隐私性实验,节点自身的动态密钥为 $S_{k,i}$,假设窃听者收到加密信息后用来解密信息的密钥为 $0.9 \times S_{k,i}^{-1}$ 。然后,选取了第二十个节点,展示了窃听者和节点自身的估计结果,如图 3 所示。

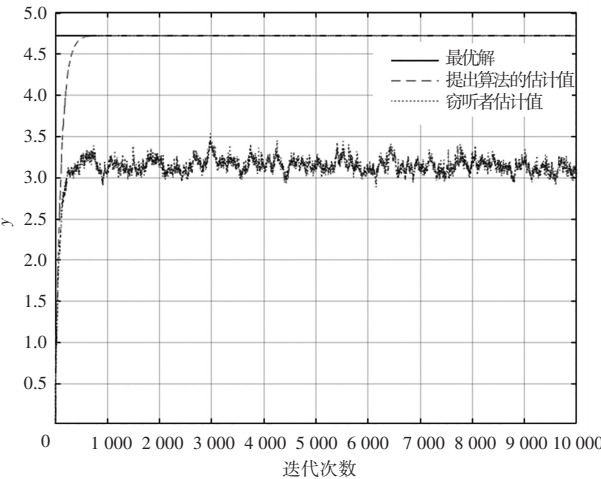


图 3 估计值比较

Fig. 3 Comparison of estimated values

从图 3 中可以知道,只要设计的加密矩阵没有被破解,即使使用相近的密钥,窃听器端也会出现明显的偏差,从而无法准确获取参数的真实值。这说明所设计的动态加密技术达到了保护数据隐私的效果。

3) 数据编码和解码实验及结果。

同样的选取了第二十个节点展示了加密后数据进行

编码解码后的结果,如图4所示。从图4中可以得到,当对需要传输的数据施加比特率约束后,得到的结果在解码误差允许范围内。

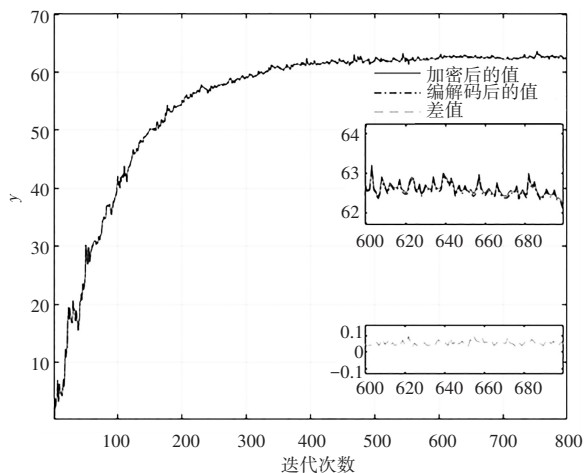


图4 编解码误差

Fig. 4 Encoding and decoding errors

4) 对比实验结果及结果分析。

本文提出的算法与其他几种具有相同测量噪声功率干扰的算法的对比结果如图5所示。观察图5可以看到非合作的算法具有比其他3种算法更大稳态均方偏差值,所提出的算法在加入比特率约束和动态加密机制的条件下,虽然存在编解码误差,但是仍能获得与标准扩散最小均方算法相当的稳态均方偏差值,继续观察局部放大图可以更清楚发现算法迭代时也只有偶尔略高于标准扩散均方算法的均方偏差值。而变步长的扩散最小均方算法由于迭代步长的变化,虽然得到了最低稳态均方偏差值,但是其收敛速度相比其他算法较慢。

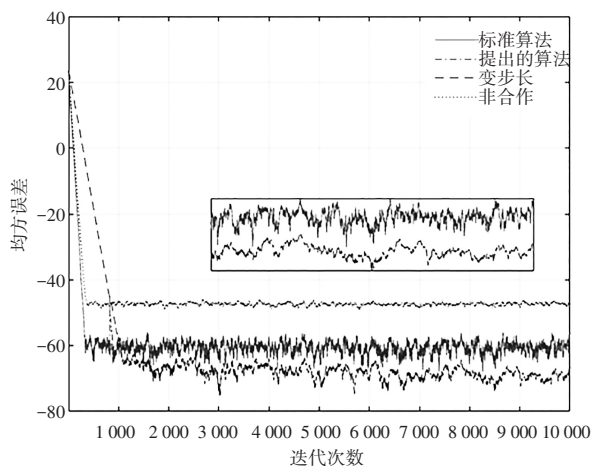


图5 均方偏差随迭代次数的变化

Fig. 5 Variation of mean square deviation with the number of iterations

5 结论

本文研究了比特率约束下带有动态加密机制和噪声观测值的分布式估计算法。通过考虑一个带宽分配协议,引入了一个比特率约束条件来反映网络带宽的限制。为

了防止敏感信息在传输过程中被窃听,加入了一个动态加密机制。通过理论分析,本文证明了所提算法在误差有界性和误差方差的渐近有界性的优越性。最终,采用均方偏差作为衡量标准,对算法的性能进行了全面验证,结果表明所提出的算法在实际应用中表现卓越。

参考文献

- [1] Moradi A, Venkatesh N K D, Talebi S P, et al. Distributed Kalman filtering with privacy against honest-but-curious adversaries [C]//2021 55th Asilomar Conference on Signals, Systems, and Computers. Pacific Grove, CA, USA; IEEE, 2021; 790-794.
- [2] Aristov M, Noack B, Hanebeck U D, et al. Encrypted multisensor information filtering [C]//2018 21st International Conference on Information Fusion (FUSION). Cambridge, UK; IEEE, 2018; 1631-1637.
- [3] Zhou Y, Chen G. Linear Convergence of distributed estimation with constraints and communication delays [J]. Journal of the Franklin Institute, 2024, 361(2): 834-851.
- [4] Li Z, Wang J, Su H, et al. Distributed consensus filtering in sensor networks considering correlated estimation errors [J]. Signal Processing, 2024, 222: 109516.
- [5] Wang Y, Tay W P, Hu W. An event-based diffusion LMS strategy [C]//2018 IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM). Sheffield, UK; IEEE, 2018; 154-158.
- [6] Shi Q, Feng M, Li X, et al. A secure distributed information sharing algorithm based on attack detection in multi-task networks [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2020, 67(12): 5125-5138.
- [7] Ni J, Zhu Y, Chen J. Multitask diffusion affine projection sign algorithm and its sparse variant for distributed estimation [J]. Signal processing, 2020, 172: 107561.
- [8] Liu J, Suo W, Zha L, et al. Security distributed state estimation for nonlinear networked systems against DoS attacks [J]. International Journal of Robust and Nonlinear Control, 2020, 30(3): 1156-1180.
- [9] Wang Y, Nedić A. Tailoring gradient methods for differentially private distributed optimization [J]. IEEE Transactions on Automatic Control, 2024, 69(2): 872-887.
- [10] Dai X, Yang H, Gu H, et al. Privacy-preserving distributed state estimation in smart grid [J]. Electric Power Systems Research, 2024, 229: 110203.
- [11] Wang S, Guay M. Distributed state estimation for jointly observable linear systems over time-varying networks [J]. Automatica, 2024, 163: 111564.
- [12] Yi X, Xu T. Distributed event-triggered estimation for dynamic average consensus: A perturbation-injected privacy-preservation scheme [J]. Information Fusion, 2024, 108: 102396.
- [13] Moradi A, Venkatesh N K D, Talebi S P, et al. Privacy-preserving distributed Kalman filtering [J]. IEEE Transactions on Signal Processing, 2022, 70: 3074-3089.
- [14] Liang Y, Sun H, Li Y, et al. Event-triggered differential private distributed fusion estimation for sensor networks with unknown cross-correlations [J]. International Journal of Robust and Nonlinear Control, 2024, 34(11): 7064-7081.
- [15] Wang J, Tan J, Zhang J F. Differentially private distributed parameter estimation [J]. Journal of Systems Science and Complexity, 2023, 36(1): 187-204.
- [16] 张昕, 荀宇欣, 徐雁翎, 等. 无线体域网数据隐私保护中的对抗扰动嵌入遗忘 [J]. 小型微型计算机系统, 2026, 47(8): 2014-2022.

(下转第188页)