文章编号：1672-3961(2026)01-0014-12 DOI：10.6040/j.issn.1672-3961.0.2024.231

基于差分隐私机制和单点反馈的分布式在线优化算法

张波[1]，徐悦[1]，康乐[1]，张贵军[2]
（1.国网宁夏电力有限公司信息通信公司，宁夏 银川 750002；2.太原理工大学财经学院，山西 太原 030024）

摘要：针对有向网络上具有隐私保护特性的分布式在线优化问题，基于差分隐私机制提出一种分布式在线优化算法。通过符合拉普拉斯分布的随机噪声对节点的状态进行扰动，有效保护节点的隐私信息。针对梯度信息显式未知的问题，引入单点反馈估计真实的梯度，利用估计的梯度信息指导决策变量的更新，使算法能够适应梯度信息不可用的场景。理论结果表明，所提出的算法不仅能够保护节点的隐私信息同时能够实现次线性Regret，能够有效解决分布式在线优化问题。仿真结果验证了算法的有效性。

关键词：分布式优化；在线优化；多智能体系统；差分隐私机制；单点反馈
中图分类号：TP181 **文献标志码**：A
引用格式：张波，徐悦，康乐，等. 基于差分隐私机制和单点反馈的分布式在线优化算法[J]. 山东大学学报(工学版)，2026，56(1)：14-25.
ZHANG Bo，XU Yue，KANG Le，et al. Distributed online optimization algorithm based on differential privacy mechanism and one-point feedback[J]. Journal of Shandong University（Engineering Science），2026，56(1)：14-25.

Distributed online optimization algorithm based on differential privacy mechanism and one-point feedback

ZHANG Bo[1]，XU Yue[1]，KANG Le[1]，ZHANG Guijun[2]
（1. State Grid Ningxia Electric Power Co.，Ltd.，Information Communication Company，Yinchuan 750002，Ningxia，China；
2. College of Finance and Economics，Taiyuan University of Technology，Taiyuan 030024，Shanxi，China）

Abstract：For distributed online optimization problem with privacy protection on directed networks，this research proposed a distributed online optimization algorithm based on differential privacy mechanism. The state of the node was disturbed by random noise which conformed to the Laplacian distribution，and the privacy information of the node was effectively protected. To solve the problem of unknown gradient information explicitly，this research introduced an one-point feedback to estimate the real gradient，and used the estimated gradient information to guide the update of decision variables，so that the algorithm could adapt to the scenario where the gradient information was unavailable. The theoretical results showed that the proposed algorithm could not only protect the privacy information of nodes but also realize the sublinear regret，and the distributed online optimization problem could be effectively solved. The simulation results verified the effectiveness of the algorithm.

Keywords：distributed optimization；online optimization；multi-agent system；differential privacy mechanism；one-point feedback

0 引言

分布式优化问题作为多智能体系统的基本问题之一已经得到广泛研究。该问题在不同领域有着诸多应用，如隐私保护[1]、智能电网[2]、鲁棒控制[3]。这些应用促进了分布式优化算法的发展，其目的是通过设计分布式优化算法使所有智能体仅通过与邻居通信就能收敛到全局最优解[4-8]。文献[4]提出一种基于事件触发机制的分布式优化算法，解决无向网络下的分布式优化问题；文献[5]基于比例积分策略提出一种分布式优化算法，并证明算法能够实现指数收敛；在文献[6]中，分布式梯度下降算法用来解决有向网络下的

收稿日期：2024-09-07
第一作者简介：张波(1985—)，男，宁夏贺兰人，高级工程师，主要研究方向为信息系统的设计开发、建设、维护、管理，电力通信网的规划、运行、维护。E-mail：zhangbbo1@163.com

分布式优化问题;文献[7]进一步将分布式优化算法应用于微电网的经济调度问题中;文献[8]研究具有集合约束的分布式优化问题。

然而,上述算法要求成本函数是时不变的,但是在实际应用场景中,分布式优化问题,通常发生在动态变化的环境中,其中成本函数是时变的。这类问题促使人们将分布式优化算法推广到在线场景中[9-13]。文献[9]提出一种分布式在线优化算法解决无向网络上的分布式优化问题,并引入 Regret 衡量算法的性能;文献[11]研究有向网络上的分布式在线优化问题;文献[13]基于行随机矩阵和列随机矩阵提出一种分布式在线优化算法,释放对双随机权值矩阵的需求。

上述算法要求有精确的梯度信息,但是在某些情况下,成本函数可能是不可微的,梯度信息无法使用。Bandit 反馈作为一种梯度估计方案解决这种问题特别有效,Bandit 反馈主要分为单点反馈和两点反馈。文献[14]将两点反馈引入分布式优化算法中,有效提高算法的收敛速度。然而两点反馈在每次迭代查询两点函数值时造成较大的通信负担。单点反馈也可以实现同样的目的,而且它的计算成本更低,计算效率更高。在文献[15]中,单点反馈被扩展到分布式优化算法,在每次迭代中,通过查询一点的函数值估计梯度信息。目前,基于单点反馈的分布式在线优化算法的相关成果仍很有限。

此外,上述分布式算法在信息传递的过程中,节点的隐私信息可能泄露,设计节点的隐私保护机制是有必要的。经典的隐私保护机制主要包括同态加密技术和差分隐私机制。同态加密技术需要对节点的隐私信息加密和解密,会造成较大的通信负担;差分隐私机制由于其严格的数学基础而得到广泛研究。文献[16]首次提出差分隐私的概念;文献[17]将差分隐私机制应用于分布式优化算法,其基本原理是利用一定规则的噪声对节点的状态进行扰动;文献[18]将差分隐私机制扩展到分布式在线凸优化场景中。上述算法严重依赖于真实的梯度信息。文献[19]提出一种基于盈余变量的隐私保护在线算法,该类算法中关键参数的选取依赖于全局信息;文献[20]提出一种基于 Push-Sum 的隐私保护在线算法,该算法要求权值矩阵是列随机的,每个节点需要知道自身的出度信息。

基于上述分析,本研究基于差分隐私机制和单点残差反馈设计一种分布式在线优化算法解决分布式在线优化问题。

1　预备知识及问题描述

1.1　图论

多智能体系统之间的通信关系可以用一个有向图 G 建模,公式为

$$G=(V,E),$$

$$N_i^{\text{in}}=\{j\in V\mid(j,i)\in E\},$$

$$N_j^{\text{out}}=\{j\in V\mid(i,j)\in E\},$$

式中:V 为智能体的集合,$V=\{1,2,\cdots,n\}$;E 为边的集合,$E\in\{V\times V\}$;N_i^{in}、N_j^{out} 分别为内邻和外邻。

定义 $\boldsymbol{A}$ 为 G 的加权邻接矩阵,$\boldsymbol{A}=[a_{ij}]_{n\times n}$,$a_{ij}$为$(i,j)$的加权值,如果$(i,j)\in E$,则 $a_{ij}>0$,否则 $a_{ij}=0$。当 $\boldsymbol{A}\boldsymbol{1}_n=\boldsymbol{1}_n$ 时,矩阵 $\boldsymbol{A}$ 为行随机矩阵;当 $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{1}_n=\boldsymbol{1}_n$ 时,矩阵 $\boldsymbol{A}$ 为列随机矩阵。此外,每个智能体都考虑自环。

1.2　差分隐私

定义 1(邻接关系)　考虑数据集 $E=\{e_i\}_{i\in V}$和 $E'=\{e_i'\}_{i\in V}$,如果存在一个 i 使得 $e_i\neq e_i'$和 $e_j=e_j'$,其中 $\forall j\neq i$,则称 E 和 E'是相邻的。

接下来,引入差分隐私的定义,它可以在相邻的数据集上生成几乎相同的随机结果。

定义 2(差分隐私)　如果给定的数据集 E 和 E',以及 $\forall U\in R(H)$,则算法 H 可以保证 ϵ-差分隐私,公式为

$$P[H(E)=U]\leqslant e^{\epsilon}P[H(E')=U],\tag{1}$$

式中,P 为概率,$R(H)$为算法 H 输出的值的范围。方法结果不会受到单个数据点的微小变化的影响。网络对手无法获取到个人敏感信息。隐私参数 ϵ 表示隐私级别。在这种情况下,需要考虑为了实现 ϵ-差分隐私,每次迭代需要注入多少噪声。接下来,在这里介绍灵敏度的概念。

定义 3(灵敏度) 在 t 时刻,将随机算法 H 的灵敏度定义为

$$\Delta_t = \sup_{\mathrm{Adj}(E_t,E_t')} \| H(E_t) - H(E_t') \|_1, \tag{2}$$

式中 $\mathrm{Adj}(E_t,E_t')$ 表示相邻数据集 E 和 E'之间的邻接关系。

1.3 单点反馈

在本节中,引入单点反馈避免精确的梯度计算。单点反馈定义为

$$\tilde{g}_t^i(x_t^i) = \frac{d}{\delta} f_t^i(x_t^i + \delta u_t^i)\, u_t^i, \tag{3}$$

式中:d 为维度,假设维度等于 1;δ 为勘探参数;u_t^i 是从标准正态分布元素中采样均值为 0 的单位随机变量,$u_t^i \in \boldsymbol{S}^d$。单点反馈具有一些重要性质,本节将其组织在下列的引理中。

引理 1[15]

(1)对于 $\delta>0$ 和均值为 0 的单位随机变量$u_i(t+1)$,有

$$E_{u_t^i \in S}[\tilde{g}_t^i(x_t^i)] = \nabla \hat{f}_t^i(x_t^i), \tag{4}$$
$$\hat{f}_t^i(x_t^i) = E[f_t^i(x_t^i + \delta u_t^i)],$$

式中 $\hat{f}_t^i$ 为 f_t^i 的光滑版本。

(2)对于梯度估计器$\tilde{\nabla} f_t^i(x_t^i)$,有

$$\| \tilde{g}_t^i(x_t^i) \| \leqslant \frac{dQ}{\delta}, \tag{5}$$

式中 Q 为 f_t^i 的上界。

(3)对于函数 $f_t^i(x)$ 和 $\hat{f}_t^i(x)$,有

$$|\hat{f}_t^i(x) - f_t^i(x)| \leqslant \delta L, \ \forall x \in \mathbf{R}^d。 \tag{6}$$

1.4 问题描述

在本节中,提出一个考虑隐私保护以及梯度信息未知的分布式在线问题。每个智能体 i 都和一个局部代价函数 $f_t^i:\mathbf{R}^d \to \mathbf{R}$ 相匹配。在 t 时刻,智能体 i 在约束集 Ω 中做出一个决策 x_t^i,并生成一个相应的代价函数 $f_t^i(x_t^i)$。所有智能体目标是协同解决下列优化问题,即

$$\min_{x_t \in \Omega} \sum_{t=0}^{T} f_t(x_t), \quad f_t(x_t) \triangleq \sum_{i=1}^{n} f_t^i(x_t^i), \tag{7}$$

式中 $\Omega \subset \mathbf{R}^d$ 为一个约束集。为了评估在线算法的性能,引入个体 Regret 的概念。用 F 表示算法从 0 到 t 时刻所生成的 σ-域。个体 Regret $\mathscr{R}_T^j$ 定义为所做决策总成本和最佳决策总成本之间的差值,公式为

$$E[\mathscr{R}_T^j | F_T] = \sum_{t=1}^{T}\sum_{i=1}^{n} E[f_t^i(x_t^j)] - \sum_{t=1}^{T}\sum_{i=1}^{n} f_t^i(x^*), \tag{8}$$

式中 x^* 为全局最优值。直观地说,如果分布式在线优化算法能够实现次线性 Regret,即$\lim\limits_{T\to\infty} \mathscr{R}_T^j / T = 0$,则称算法的性能好。

本研究的目的是提出一种基于差分隐私机制和单点反馈的分布式在线优化算法,使所有智能体实现次线性 Regret,同时保证期望的隐私程度。在提出该算法之前,做了如下假设。

假设 1 有向图 G 是强连通的,加权矩阵 $\boldsymbol{A}$ 是行随机的。Ω 是一个闭凸集,$\Omega \subseteq \mathbf{R}^d$。此外,集合 Ω 的直径是有界的, $R<\infty$ 。

假设 2 函数 $f_t^i:\mathbf{R}^d \to \mathbf{R}$ 是 L-Lipschitz 连续的,即对于所有 x, $y \in \mathbf{R}^d$, $|f(x)-f(y)| \leqslant L\|x-y\|$,其中 L 是正常数。

假设 3 每个代价函数 f_t^i 在 Ω 上都是 μ-强凸的,也就是说,对于所有的 x, $y \in \mathbf{R}^d$,有 $f(y) \geqslant f(x) + \boldsymbol{g}^{\mathrm{T}}(x)(y-x) + \frac{\mu}{2}\|y-x\|^2$,其中 $\mu>0$。

假设 4 对于任何 $x \in \Omega$,次梯度 $g_t^i(x)$ 满足 $\| g_t^i(x) \| \leqslant G$,其中 G 为正常数。

假设 5 成本函数 f_t^i 是有界的,即$|f_t^i(x)| \leqslant Q$,其中 Q 为正常数。

2　算法设计及主要结果

2.1　分布式在线优化算法

本节基于单点反馈和差分隐私机制设计一种分布式在线优化算法,具体公式为

$$y_t^i=x_t^i+\eta_t^i, \tag{9}$$

$$x_{t+1}^i=\mathscr{P}_{\Omega}\left(\sum_{j=1}^{n}a_{ij}y_t^j-\alpha_t\frac{\tilde{g}_t^i(x_t^i)}{z_t^{ii}}\right), \tag{10}$$

$$z_{t+1}^i=\sum_{j=1}^{n}a_{ij}z_t^j, \tag{11}$$

式中 $\mathscr{P}_{\Omega}$ 指在集合 Ω 上的投影。具体来说,每个智能体都有 2 种状态,即 $x_t^i\in\mathbf{R}^d$ 和 $z_t^i\in\mathbf{R}^n$。x_t^i 是智能体的主状态,初始化为 $x_0^i\in\Omega$,每个状态对应一个成本函数 $f_t^i(x_t^i)$;z_t^i 是辅助变量,其初始化为 $z_0^i=e^i$,其中 e^i 第 i 项等于 1,其余项等于 0。在 t 时刻,每个智能体 j 生成一个符合拉普拉斯分布 $\mathrm{Lap}(\sigma_t)$ 的随机噪声 η_t^j,并用噪声 η_t^j 扰动变量 x_t^j,然后将扰动量 y_t^j 和辅助变量 z_t^j 传输到它的外邻 i。智能体 i 用收到的信息更新 x_{t+1}^i 和 z_{t+1}^i。

2.2　主要结果

在本节中,给出所提出算法的隐私保护证明以及收敛性分析。在陈述主要结果之前,给出一些有用的引理。首先在下面的引理中揭示矩阵 $\boldsymbol{A}$ 的一些重要性质。

引理 2[18]　令假设 1~5 成立。

对于 $\forall t\geqslant 0$,存在一个 Perron 特征向量 $\boldsymbol{\pi}=[\pi_1,\pi_2,\cdots,\pi_n]^{\mathrm{T}}$,满足

(1) 存在 $C>0$ 和 $\xi\in(0,1)$,使得 $|[\boldsymbol{A}^t]_{ij}-\pi_j|\leqslant C\xi$ 和 $|z_t^{ii}-\pi_i|\leqslant C\xi^t$;

(2) $\boldsymbol{\pi}^{\mathrm{T}}\boldsymbol{A}=\boldsymbol{\pi}^{\mathrm{T}}$, $\boldsymbol{\pi}^{\mathrm{T}}\boldsymbol{I}_n=1$。

下面的引理表明变量 z_t^{ii} 是有界的。

引理 3[18]　令假设 1 成立。

序列 $\{z_t^i\}_{t\geqslant 0}$ 由所提出的算法生成。则对 $\forall i\in\mathscr{V}$,存在 $\theta>0$,有

$$\theta^{-1}\leqslant z_t^{ii}\leqslant 1。 \tag{12}$$

此外,从定义 3 可以看出,灵敏度描述节点数据集 E 的轻微变化对整个算法的最大影响。因此,应该推导一个灵敏度界的上限,以确定保证差分隐私的噪声条件。

引理 4　令假设 1~5 成立。则

$$\Delta_t\leqslant 2\theta\alpha_t\frac{d^{\frac{3}{2}}Q}{\delta}。 \tag{13}$$

证明　E 和 E' 是满足定义 1 的两个数据集。设 $\{x_t^i\}$ 和 $\{x_t'^i\}$ 分别为 $H(E_t)$ 和 $H(E_t')$ 的执行结果。在这种情况下,对手获得的观测序列是相同的,即 $y_t^j=y_t'^j$。因此,可以得到

$$\|x_{t+1}^i-x_{t+1}'^i\|_1\leqslant\left\|\alpha_t\frac{\tilde{g}_t^i(x_t^i)}{z_t^{ii}}-\alpha_t\frac{\tilde{g}_t'^i(x_t^i)}{z_t^{ii}}\right\|_1\leqslant$$

$$\frac{\alpha_t}{z_t^{ii}}(\|\tilde{g}_t^i(x_t^i)\|_1+\|\tilde{g}_t'^i(x_t^i)\|_1)\leqslant 2\theta\alpha_t\frac{d^{\frac{3}{2}}Q}{\delta}, \tag{14}$$

式(14)中使用了投影的非扩张性质,即对于任意 x 和 y 在集合 Ω 上的投影满足 $\|\mathscr{P}_{\Omega}(x)-\mathscr{P}_{\Omega}(x)\|_1\leqslant\|x-y\|$,且应用了引理 1 和引理 2。引理 4 证明完毕。

从引理 4 可以看出,灵敏度随着算法的执行而减小。当灵敏度有限时,可以推导出一个差分隐私定理。基于引理 4,给出了差分隐私定理。

定理 1(ϵ-差分隐私)。令假设 1~5 成立,通过引入 Laplace 噪声 $\eta_t^i\sim\mathrm{Lap}(\sigma_t)$, $i\in V$, $t\in\{1,2,\cdots,T\}$ 对节点的状态进行扰动,且 $\sigma_t=\Delta_t/\epsilon$,其中 $\epsilon>0$。则所提出的算法可以保证 ϵ-差分隐私。

证明 对于两个相邻的数据集 E 和 E',在两个数据集上执行的观测序列是相同的,即 $y_{t,h}^i = y'^i_{t,h}$。定义 $\boldsymbol{x}_t = [x_t^1, x_t^2, \cdots, x_t^n]^{\mathrm{T}}$ 和 $\boldsymbol{x}'_t = [x'^1_t, x'^2_t, \cdots, x'^n_t]^{\mathrm{T}}$。则可以得到

$$\prod_{i=1}^{n}\prod_{h=1}^{d}\frac{P[y_{t,h}^i - x_{t,h}^i]}{P[y'^i_{t,h} - x'^i_{t,h}]} \leqslant \prod_{i=1}^{n}\prod_{h=1}^{d}\exp\left(\frac{|y_{t,h}^i - x_{t,h}^i - y'^i_{t,h} + x'^i_{t,h}|}{\sigma_t}\right) = \exp\left(\frac{\| x_t^i - x'^i_t \|}{\sigma_t}\right) \leqslant \exp\left(\frac{\Delta_t}{\sigma_t}\right) = e^{\epsilon}, \tag{15}$$

式中,$x_{t,h}^i$ 和 $x'^i_{t,h}$ 分别为 x_t 和 x'_t 的第 h 个分量。上述证明中分别使用三角形不等式和定义 3。证明完毕。

敏感度的有界性依赖中间变量的界 θ、单点梯度的界以及算法步长 α_t。因为更小的敏感度意味着隐私保护所需摄动的噪声更小,而通过将算法步长 α_t 设置成随时间衰减的量可以减小敏感度。由于 $\sigma_t = \Delta_t/\epsilon$,当隐私保护程度 ϵ 固定时,注入状态变量的噪声值大小 $\eta_t^i \sim \mathrm{Lap}(\sigma_t)$ 与算法的灵敏度成正比。灵敏度随着时间推移减小,噪声的注入也相应减小,当灵敏度有界时,定理 1 表明所提出的算法能够保证 ϵ 差分隐私。

本研究主要针对如何使用所提出的算法构建个体 Regret。为方便起见,定义网络 Regret 公式为

$$E[\mathscr{R}_T^{\mathrm{net}} \mid F_T] = \sum_{t=1}^{T}\sum_{i=1}^{n} E[f_t^i(x_t^i)] - \sum_{t=1}^{T}\sum_{i=1}^{n} f_t^i(x^*)。 \tag{16}$$

网络 Regret 衡量随着时间的推移,集体累计成本和最佳决策成本之间的差异。下面的主要思想是:首先,根据网络 $f_t^i(x_t^i)$ 与 $f_t^i(x_t^j)$ 之间的关系,得到网络 Regret 的界限;其次,给出个体 Regret 的界限。在给出该定理之前,给出一些引理支持主要的收敛结果。

由于不平衡有向图权矩阵是行随机的,$\boldsymbol{\pi}$ 中分量的不均匀性导致不能像大多数分布式算法直接研究 $\frac{1}{n}\sum_{i=1}^{n} x_t^i$。因此,为了验证所提出的算法的收敛性,定义一个辅助变量

$$\bar{x}_t \triangleq \sum_{i=1}^{n} \pi_i x_t^i, \tag{17}$$

式中 $\boldsymbol{\pi} = [\pi_1, \pi_2, \cdots, \pi_n]$。接下来,建立 $E[\| \bar{x}_{t+1} - x_{t+1}^i \| \mid F_t]$ 的上界。

引理 5 令假设 1~5 成立,步长为 α_t,序列 $\{x_t^i\}_{t\geqslant 0}$ 由所提出的算法生成。则

$$E[\| \bar{x}_{t+1} - x_{t+1}^i \| \mid F_t] \leqslant 4\sum_{j=1}^{n} E[\| \eta_t^j \|] + C\xi^{t+1}\sum_{j=1}^{n}\| x_0^j \| + 2nC\sum_{h=1}^{t}\xi^{t-h+1}\sum_{j=1}^{n} E[\| \eta_{h-1}^j \|] +$$

$$\frac{n\theta C d Q}{\delta}\sum_{h=1}^{t}\xi^{t-h+1}\alpha_{h-1} + C\sum_{h=0}^{t}\xi^{t-h+1}\sum_{j=1}^{n} E[\| \eta_h^j \|] + 2\frac{\theta d^{\frac{3}{2}} Q}{\delta}\alpha_t。 \tag{18}$$

证明 为了便于分析,定义一些变量,$q_t^i = \sum_{j=1}^{n} a_{ij} y_t^j$,$w_t^i = \sum_{j=1}^{n} a_{ij} x_t^j$ 和 $p_{t+1}^i = x_{t+1}^i - q_t^i$。接下来,开始建立 $\| p_{t+1}^i \|$ 的上界,公式为

$$\| p_{t+1}^i \| = \| x_{t+1}^i - q_t^i \| \leqslant \| x_{t+1}^i - w_t^i \| + \| w_t^i - q_t^i \| \leqslant \left\| q_t^i - \frac{\alpha_t \tilde{g}_t^i(x_t^i)}{z_t^{ii}} - w_t^i \right\| + \| w_t^i - q_t^i \| \leqslant$$

$$2\| q_t^i - w_t^i \| + \alpha_t \left\| \frac{\tilde{g}_t^i(x_t^i)}{z_t^{ii}} \right\| \leqslant 2\sum_{j=1}^{n} \| \eta_t^j \| + \frac{\theta d Q}{\delta}\alpha_t, \tag{19}$$

式(19)中分别使用投影的非扩张性质以及引理 1 和引理 2。通过对 p_t^i 数学归纳,可以得到

$$x_{t+1}^i = p_{t+1}^i + \sum_{h=0}^{t}\sum_{j=1}^{n}[\boldsymbol{A}^{t-h+1}]_{ij}\eta_h^j \sum_{j=1}^{n}[\boldsymbol{A}^{t+1}]_{ij} x_0^j + \sum_{h=1}^{t}\sum_{j=1}^{n}[\boldsymbol{A}^{t-h+1}]_{ij} p_h^j。 \tag{20}$$

根据 $\bar{x}_t$ 和 p_t^i 的定义,有

$$\bar{x}_{t+1} = \bar{x}_t + \sum_{i=1}^{n}\pi_i \eta_t^i + \sum_{i=1}^{n}\pi_i p_{t+1}^i, \tag{21}$$

进一步可以得到

$$\bar{x}_{t+1} = \bar{x}_0 + \sum_{h=1}^{t+1}\sum_{i=1}^{n}\pi_i p_h^i + \sum_{h=0}^{t}\sum_{i=1}^{n}\pi_i \eta_h^i。 \tag{22}$$

根据式(19)、(21)可以得到

$$\| \bar{x}_{t+1} - x_{t+1}^i \| \leqslant 4\sum_{j=1}^{n}\| \eta_t^j \| + 2\alpha_t\frac{\theta d Q}{\delta} + C\xi^{t+1}\sum_{j=1}^{n}\| x_0^j \| +$$

$$C\sum_{h=0}^{t}\xi^{t-h+1}\sum_{j=1}^{n}\|\eta_h^j\|+n\theta CF\sum_{h=1}^{t}\xi^{t-h+1}\alpha_{h-1}+2nC\sum_{h=1}^{t}\xi^{t-h+1}\sum_{j=1}^{n}\|\eta_{h-1}^j\|,\tag{23}$$

式(23)应用引理 2、3 和不等式(19)。对式(23)取 F_t 的条件期望,则证明完毕。

引理 6　令假设 1~5 成立。序列$\{x_t^i\}_{t\geqslant 0}$由所提出的算法生成,步长为 α_t,则

$$\sum_{i=1}^{n}\pi_i E[\|x_{t+1}^i-x\|^2|F_t]\leqslant 2\alpha_t\sum_{i=1}^{n}E[\hat{f}_t^i(x)-\hat{f}_t^i(x_t^i)]+2\frac{\theta dQ}{\delta}\alpha_t\sum_{i=1}^{n}\pi_i E[\|\eta_t^i\|]+$$

$$4\frac{\theta dQ}{\delta}\alpha_t\sum_{i=1}^{n}\pi_i E[\|x_t^i-\bar{x}_t\|]+\frac{\theta^2d^2Q^2}{\delta^2}\alpha_t^2+\sum_{i=1}^{n}\pi_i E[\|\eta_t^i\|^2]+(1-\mu\theta\alpha_t)\sum_{i=1}^{n}\pi_i E[\|x_t^i-x\|^2]+$$

$$2\theta CL\alpha_t\xi^t\sum_{i=1}^{n}E[\|x-x_t^i\|]。\tag{24}$$

证明　根据式(10),对于$\forall x\in\Omega$,可以得到

$$\|x_{t+1}^i-x\|^2\leqslant\left\|q_t^i-\frac{\alpha_t\tilde{g}_t^i(x_t^i)}{z_t^{ii}}-x\right\|^2=\|q_t^i-x\|^2-2\frac{\alpha_t}{z_t^{ii}}\tilde{g}_t^i(x_t^i)(q_t^i-x)+\frac{\alpha_t^2}{z_t^{ii2}}\|\tilde{g}_t^i(x_t^i)\|^2。\tag{25}$$

对于式(25)中的$\|q_t^i-x\|$,基于行随机矩阵和凸函数$\|\cdot\|^2$的 Jensens 不等式,有

$$\|q_t^i-x\|^2=\|\sum_{j=1}^{n}a_{ij}x_t^j-x+\sum_{j=1}^{n}a_{ij}\eta_t^j\|^2\leqslant 2\sum_{j=1}^{n}a_{ij}\eta_t^j\Big(\sum_{j=1}^{n}a_{ij}x_t^j-x\Big)+\sum_{j=1}^{n}a_{ij}\|x_t^j-x\|^2+\sum_{j=1}^{n}a_{ij}\|\eta_t^j\|^2,\tag{26}$$

进一步取期望可以得到

$$E[\|q_t^i-x\|^2|F_{t-1}]\leqslant\sum_{j=1}^{n}a_{ij}E[\|\eta_t^j\|^2]+\sum_{j=1}^{n}a_{ij}E[\|x_t^j-x\|^2],\tag{27}$$

式(25)中使用 $E[\eta_t^j|F_{t-1}]=0$。对于式(25)中的$2\frac{\alpha_t}{z_t^{ii}}\tilde{g}_t^i(x_t^i)(q_t^i-x)$,有

$$-\tilde{g}_t^i(x_t^i)(q_t^i-x)\leqslant\|\tilde{g}_t^i(x_t^j)\|\,\|q_t^i-\bar{x}_t\|-\tilde{g}_t^i(x_t^i)(\bar{x}_t-x)\leqslant$$

$$\|\tilde{g}_t^i(x_t^i)\|\sum_{j=1}^{n}a_{ij}\|\eta_t^j\|+\|\tilde{g}_t^i(x_t^i)\|\sum_{j=1}^{n}a_{ij}\|x_t^j-\bar{x}_t\|+$$

$$\|\tilde{g}_t^i(x_t^i)\|\,\|\bar{x}_t-x_t^i\|+\tilde{g}_t^i(x_t^i)(x-x_t^i),\tag{28}$$

因此,可以得到

$$E[-\tilde{g}_t^i(x_t^i)(q_t^i-x)^2|F_t]\leqslant\frac{dQ}{\delta}\sum_{j=1}^{n}a_{ij}E[\|\eta_t^j\|]-\frac{\mu}{2}E[\|x-x_t^i\|^2]+$$

$$\frac{dQ}{\delta}E[\|\bar{x}_t-x_t^i\|]+E[\hat{f}_t^i(x)-\hat{f}_t^i(x_t^i)]+\frac{dQ}{\delta}\sum_{j=1}^{n}a_{ij}E[\|x_t^j-\bar{x}_t\|],\tag{29}$$

式(29)中使用假设 3。此外,对于式(25)中的$\frac{\alpha_t^2}{z_t^{ii2}}\|\tilde{g}_t^i(x_t^i)\|^2$,有

$$\frac{\alpha_t^2}{z_t^{ii2}}\|\tilde{g}_t^i(x_t^i)\|^2\leqslant\frac{\theta^2d^2Q^2}{\delta^2}\alpha_t^2。\tag{30}$$

根据式(27)、(29)、(30),并对式(25)取期望,并乘以 π_i,可以得到

$$\sum_{i=1}^{n}\pi_i E[\|x_{t+1}^i-x\|^2|F_t]\leqslant\sum_{i=1}^{n}\pi_i E[\|\eta_t^i\|^2]+(1-\mu\theta\alpha_t)\sum_{i=1}^{n}\pi_i E[\|x_t^i-x\|^2]+$$

$$2\frac{\theta dQ}{\delta}\alpha_t\sum_{i=1}^{n}\pi_i E[\|\eta_t^i\|]+2\alpha_t\sum_{i=1}^{n}\frac{\pi_i}{z_t^{ii}}E[\hat{f}_t^i(x)-\hat{f}_t^i(x_t^i)]+$$

$$4\frac{\theta dQ}{\delta}\alpha_t\sum_{i=1}^{n}\pi_i E[\|x_t^i-\bar{x}_t\|]+\frac{\theta^2d^2Q^2}{\delta^2}\alpha_t^2,\tag{31}$$

式(31)中使用了引理 2。

值得注意的是,式(31)中的项目 $E[\hat{f}_t^i(x)-\hat{f}_t^i(x_t^i)]$是按 π_i 进行缩放的,因此,需要进一步分析该项以获得所需的结果。对于式(31)中的最后一项,可以推导为

$$\frac{\pi_i}{z_t^{ii}}E[\hat{f}_t^i(x)-\hat{f}_t^i(x_t^i)]\leqslant\left|\frac{\pi_i-z_t^{ii}}{z_t^{ii}}\right|E[|\hat{f}_t^i(x)-\hat{f}_t^i(x_t^i)|]+E[\hat{f}_t^i(x)-\hat{f}_t^i(x_t^i)]\leqslant$$

$$\theta CL\xi^t E[\|x-x_t^i\|]+E[\hat{f}_t^i(x)-\hat{f}_t^i(x_t^i)], \tag{32}$$

式(32)中使用假设 2 和引理 2。合并式(31)、(32),引理 6 证明完毕。

定理 2(网络 Regret) 令假设 1~5 成立,序列$\{x_t^i\}_{t\geqslant 0}$是由所提出的算法生成,且 $\alpha_t=\frac{1}{\mu\theta t}$。则

$$E[\mathscr{R}_T^{\text{net}}|F_T]\leqslant 2\delta LT+\mathscr{C}_1+\mathscr{C}_2(1+\log T), \tag{33}$$

$$\mathscr{C}_1=\frac{\xi C}{1-\xi}\left(2\frac{\theta dQ}{\delta}\sum_{i=1}^n\|x_0^i\|+n\theta LR\right),$$

$$\mathscr{C}_2=\frac{1}{\mu}\left(\frac{2\sqrt{2}(8n+1)\theta md^2Q^2}{\delta^2}+\frac{4m^2\theta d^2Q^2}{\epsilon^2\delta^2}+\frac{2n\theta Cd^2Q^2}{(1-\xi)\delta^2}+\frac{9}{2}\frac{\theta d^2Q^2}{\delta^2}+\frac{4\sqrt{2}mn(2n+1)\theta Cd^2Q^2}{(1-\xi)\epsilon\delta^2}\right)。$$

证明 调用引理 6,并设置 $x=x^*$。不等式(24)两边除 $2\alpha_t$,有

$$\sum_{i=1}^n E[\hat{f}_t^i(x_t^i)-\hat{f}_t^i(x^*)|F_{t-1}]\leqslant\frac{1}{2\alpha_t}\left((1-\mu\theta\alpha_t)\sum_{i=1}^n\pi_iE[\|x_t^i-x^*\|^2]-\sum_{i=1}^n\pi_iE[\|x_{t+1}^i-x^*\|^2]\right)+$$

$$\frac{1}{2}\frac{\theta^2d^2Q^2}{\delta^2}\alpha_t+\frac{1}{2\alpha_t}\sum_{i=1}^n\pi_iE[\|\eta_t^i\|^2]+\theta CL\xi^t\sum_{i=1}^nE[\|x_t^i-x^*\|]+$$

$$\frac{\theta dQ}{\delta}\sum_{i=1}^n\pi_iE[\|\eta_t^i\|]+2\frac{\theta dQ}{\delta}\sum_{i=1}^n\pi_iE[\|x_t^i-\bar{x}_t\|]。 \tag{34}$$

此外,根据引理 1,可以得到

$$f_t^i(x_t^i)-\delta L\leqslant\hat{f}_t^i(x_t^i)\leqslant f_t^i(x_t^i)+\delta L, \tag{35}$$

结合不等式(34)、(35),可以得到

$$\sum_{i=1}^n E[f_t^i(x_t^i)-f_t^i(x^*)|F_{t-1}]\leqslant\frac{1}{2\alpha_t}\left((1-\mu\theta\alpha_t)\sum_{i=1}^n\pi_iE[\|x_t^i-x^*\|^2]-\sum_{i=1}^n\pi_iE[\|x_{t+1}^i-x^*\|^2]\right)+$$

$$\frac{1}{2\alpha_t}\sum_{i=1}^n\pi_iE[\|\eta_t^i\|^2]+\theta CL_2\xi^t\sum_{i=1}^nE[\|x_t^i-x^*\|]+\frac{1}{2}\frac{\theta^2d^2Q^2}{\delta^2}\alpha_t+\frac{\theta dQ}{\delta}\sum_{i=1}^n\pi_iE[\|\eta_t^i\|]+$$

$$2\delta L+2\frac{\theta dQ}{\delta}\sum_{i=1}^n\pi_iE[\|x_t^i-\bar{x}_t\|]。 \tag{36}$$

应用引理 5 以及引理 2,并对时刻进行累加求和,可以得到

$$E[\mathscr{R}_T^{\text{net}}|F_T]\leqslant\sum_{\nu=1}^6 H_\nu, \tag{37}$$

其中

$$H_1=\sum_{t=1}^T\frac{1}{2\alpha_t}\left((1-\mu\theta\alpha_t)\sum_{i=1}^n\pi_iE[\|x_t^i-x^*\|^2]-\sum_{i=1}^n\pi_iE[\|x_{t+1}^i-x^*\|^2]\right),$$

$$H_2=\sum_{t=1}^T\left(4n\theta C\frac{dQ}{\delta}\sum_{h=1}^{t-1}\xi^{t-h}\sum_{i=1}^nE[\|\eta_{h-1}^i\|]+2\theta C\frac{dQ}{\delta}\sum_{h=0}^{t-1}\xi^{t-h}\sum_{i=1}^nE[\|\eta_h^i\|]\right),$$

$$H_3=\sum_{t=1}^T\left(\frac{\theta dQ}{\delta}\sum_{i=1}^n\pi_iE[\|\eta_t^i\|]+\frac{1}{2\alpha_t}\sum_{i=1}^n\pi_iE[\|\eta_t^i\|^2]+8\frac{\theta dQ}{\delta}\sum_{i=1}^nE[\|\eta_{t-1}^i\|]\right),$$

$$H_4=\sum_{t=1}^T\left(4\frac{\theta^2d^2Q^2}{\delta^2}\alpha_{t-1}+\frac{1}{2}\frac{\theta^2d^2Q^2}{\delta^2}\alpha_t\right)+2\delta LT,$$

$$H_5=\sum_{t=1}^T 2nC\frac{\theta^2d^2Q^2}{\delta^2}\sum_{h=0}^t\xi^{t-h}\alpha_h,$$

$$H_6=\sum_{t=1}^T\theta CL\xi^t\sum_{i=1}^nE[\|x_t^i-x^*\|]+\sum_{t=1}^T 2\theta C\frac{dQ}{\delta}\xi^t\sum_{i=1}^n\|x_0^i\|。$$

因此,只需要分别推导出 H_ν 的边界,$\nu\in[6]$。首先,H_1 可以推导为

$$H_1=\left(\frac{1}{2\alpha_1}-\frac{\mu\theta}{2}\right)\sum_{i=1}^{n}\pi_i E[\ \|x_1^i-x^*\|^2]-\frac{1}{2\alpha_T}\sum_{i=1}^{n}\pi_i E[\ \|x_{T+1}^i-x^*\|^2]+$$

$$\sum_{t=2}^{T}\left(\frac{1}{2\alpha_t}-\frac{1}{2\alpha_{t-1}}-\frac{\mu\theta}{2}\right)\sum_{i=1}^{n}\pi_i E[\ \|x_t^i-x^*\|^2]\leqslant\left(\frac{1}{2\alpha_1}-\frac{\mu\theta}{2}\right)R^2+R^2\sum_{t=2}^{T}\left(\frac{1}{2\alpha_t}-\frac{1}{2\alpha_{t-1}}-\frac{\mu\theta}{2}\right)=\frac{1}{2\alpha_T}R^2-\frac{\mu\theta}{2}TR^2,\tag{38}$$

式中使用假设 1 和引理 2。

对于 H_2,有

$$\sum_{t=1}^{T}\sum_{h=1}^{t-h}\xi^{t-l}\sum_{i=1}^{n}E[\ \|\eta_{h-1}^i\|\ ]\leqslant\frac{1}{1-\xi}\sum_{h=0}^{T-1}\sum_{i=1}^{n}E[\ \|\eta_h^i\|\ ]。\tag{39}$$

类似于式(39)中的过程,有

$$\sum_{t=1}^{T}\sum_{h=0}^{t-1}\xi^{t-h}\sum_{i=1}^{n}E[\ \|\eta_h^i\|\ ]\leqslant\frac{1}{1-\xi}\sum_{h=0}^{T-1}\sum_{i=1}^{n}E[\ \|\eta_h^i\|\ ]。\tag{40}$$

由于 $E[\ \|\eta_t^i\|\ ]$是符合拉普拉斯分布的独立噪声,因此,有 $E[\ |\eta_{t,k}^i|^2]=2\sigma_t^2$,其中 $\eta_{t,k}^i$是 η_t^i 的第 k 个元素。可以得到

$$\sum_{i=1}^{n}E[\ \|\eta_{i,t}\|\ ]=n\sqrt{2d}\sigma_t\leqslant\frac{2\sqrt{2}\theta d^2nQ\alpha_t}{\epsilon\delta},\tag{41}$$

式(41)中使用引理 4。结合式(39)、(41),可以得到

$$H_2\leqslant\frac{4\sqrt{2}d^3n\theta^2(2n+1)CQ^2}{(1-\xi)\epsilon\delta^2}\sum_{t=1}^{T}\alpha_t。\tag{42}$$

根据式(41),有

$$H_3\leqslant\left(\frac{2\sqrt{2}(8n+1)d^3\theta^2Q^2}{\epsilon\delta^2}+\frac{4d^2\theta^2G^2}{\epsilon^2}\right)\sum_{t=1}^{T}\alpha_t。\tag{43}$$

与式(39)中使用的分析类似,有

$$H_5\leqslant\frac{2n\theta^2Cd^2Q^2}{(1-\xi)\delta^2}\sum_{t=1}^{T}\alpha_t。\tag{44}$$

很明显可以得到 H_6,即

$$H_6\leqslant\frac{\xi C}{1-\xi}\left(2\theta\frac{dQ}{\delta}\sum_{i=1}^{n}\|x_0^i\|+\theta nLR\right)。\tag{45}$$

由于 $H_1\leqslant\frac{1}{2\alpha_T}R^2-\frac{\mu\theta}{2}TR^2$,当 H_1 结果中存在 T 时算法无法实现次线性收敛,因此通过选取步长 $\alpha_t=\frac{1}{\theta\mu t}$从而消除 H_1 项,使算法能够实现次线性收敛。注意到 $\sum_{t=1}^{T}\alpha_t=\frac{1}{\theta\mu}\sum_{t=1}^{T}\frac{1}{t}\leqslant\frac{1}{\theta\mu}(1+\log T)$,将其代入上述不等式,证明完毕。然后,给出本研究的主要定理。

定理 3(个体 Regret)　令假设 1~5 成立,序列$\{x_t^i\}_{t\geqslant0}$是由所提出的算法生成,$\alpha_t=\frac{1}{\mu\theta t}$,则

$$E[\mathscr{R}_T^j|F_T]\leqslant2\delta LT+\mathscr{D}_1+\mathscr{D}_2(1+\log T),\tag{46}$$

其中

$$\mathscr{D}_1=\frac{\xi C}{1-\xi}\left(2(\theta\frac{dQ}{\delta}+nG)\sum_{i=1}^{n}\|x_0^i\|+n\theta LR\right),$$

$$\mathscr{D}_2=\frac{1}{\mu}\left(\frac{2\sqrt{2}mdQ\left((8n+1)\theta\frac{dQ}{\delta}+8n^2G\right)}{\delta\epsilon}+\frac{4\sqrt{2}mn\left((2n+1)\theta\frac{dQ}{\delta}+nG+2n^2\theta G\right)CdQ}{(1-\xi)\epsilon\delta}+\right.$$

$$\left.4nG\frac{dQ}{\delta}+\frac{4m^2\theta d^2Q^2}{\epsilon^2\delta^2}+\frac{2n(nG+\theta^2)CdQ}{(1-\xi)\delta}+\frac{9}{2}\theta\frac{d^2Q^2}{\delta^2}\right)。$$

证明　回顾网络 Regret 和个体 Regret 的定义,可以得到

$$E[\mathscr{R}_T^j \mid F_T]-E[\mathscr{R}_T^{\text{net}} \mid F_T] \leqslant E\left[\sum_{t=1}^{T}\sum_{i=1}^{n} \| g_t^i(x_t^j) \| \, \| x_t^j-x_t^i \|\right] \leqslant$$

$$E\left[\sum_{t=1}^{T}\sum_{i=1}^{n} G(\| x_t^j-\bar{x}_t \| + \| x_t^i-\bar{x}_t \|)\right], \tag{47}$$

其中使用假设 4 和函数的凸性。使用引理 5,可以得到

$$E[\mathscr{R}_T^j \mid F_T]-E[\mathscr{R}_T^{\text{net}} \mid F_T] \leqslant \sum_{t=1}^{T} 4n^2CG\sum_{h=1}^{t-1}\xi^{t-h}\sum_{i=1}^{n} E[\| \eta_{h-1}^i \|] + \sum_{t=1}^{T} 4n\theta G\frac{dQ}{\delta}\alpha_{t-1} +$$

$$\sum_{t=1}^{T} 8nG\sum_{i=1}^{n} E[\| \eta_{t-1}^i \|] + \sum_{t=1}^{T} 2nCG\sum_{h=0}^{t-1}\xi^{t-h}\sum_{i=1}^{n} E[\| \eta_h^i \|] +$$

$$\sum_{t=1}^{T} 2n^2\theta CG\frac{dQ}{\delta}\sum_{h=1}^{t-1}\xi^{t-h}\alpha_{h-1} + \sum_{t=1}^{T} 2nCG\xi^t\sum_{i=1}^{n} \| x_0^i \| 。 \tag{48}$$

此外,应用式(39)~(41),可以得到

$$E[\mathscr{R}_T^j \mid F_T]-E[\mathscr{R}_T^{\text{net}} \mid F_T] \leqslant \frac{2n\xi CG}{1-\xi}\sum_{i=1}^{n} \| x_{i,0} \| + \frac{2n^2\theta CGdQ}{(1-\xi)\delta}\sum_{t=1}^{T}\alpha_t +$$

$$\frac{8\sqrt{2}mn^3\theta CGdQ}{(1-\xi)\delta\epsilon}\sum_{t=1}^{T}\alpha_t + 4n\theta G\frac{dQ}{\delta}\sum_{t=1}^{T}\alpha_{t-1} + \frac{4\sqrt{2}mn^2\theta(\theta+n)CGdQ}{(1-\xi)\delta\epsilon}\sum_{t=1}^{T}\alpha_t + \frac{16\sqrt{2}n^2d\theta GdQ}{\delta\epsilon}\sum_{t=1}^{T}\alpha_t 。 \tag{49}$$

基于 $\alpha_t=\dfrac{1}{\theta\mu t}$、不等式(33)和(49)得到期望的结果。

下面的推论表明,通过选择合适的勘探参数本研究所提出的算法能够实现次线性收敛。

推论 1 在定理 3 的条件下,令 $\delta=\log T/T$,则对于所有的 $j\in V$,有

$$E[\mathscr{R}_T^j \mid F_T]=\mathscr{O}(T^{2/3}\log^{1/3}T)。 \tag{50}$$

定理 3 给出每个智能体 Regret 的收敛结果,表明算法能够实现次线性收敛。通过定理 3 中个体 Regret 的形式可以发现,第一部分是使用单点反馈的惩罚项,该项可以通过选取合适的勘探参数进行调整。在 $\mathscr{D}_1$ 和 $\mathscr{D}_2$ 中可以发现,单点反馈仍然影响算法的收敛性能,且维度越高影响越大,但在一个可接受的范围内,算法仍能够实现次线性收敛。单点反馈和两点反馈相比具有较大的估计方差,两点反馈面对高维系统适应性更强,但是两点反馈需要在同一时刻查询两点函数值。这在某些场景中是无法实现的,如非平稳在线优化问题中。单点反馈在每次迭代查询一个函数值更现实。

$\mathscr{D}_2$ 中的参数 ϵ 是添加噪声保护节点隐私信息所导致的惩罚项。噪声的存在在一定程度上影响算法的收敛结果。隐私保护水平越高,所注入的噪声越大,算法的收敛性能越差,因此在隐私保护水平和收敛性能之间存在一个折中。

3 仿真结果

本研究在多智能体系统中的分布式估计问题中验证所提出算法的有效性,其中智能体之间的通信结构由 10 个智能体的非平衡有向图建模。通信拓扑如图 1 所示。

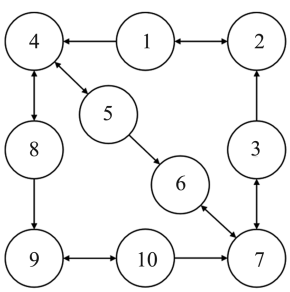

图 1 通信拓扑图

Fig.1 Communication topology

分布式估计问题的目标是最小化函数,公式为

$$\min f(x)=\sum_{i=1}^{n}\left(\|\varphi_i-\boldsymbol{H}_i x\|^2+\sigma_i\|x\|^2\right),\ x\in\Omega, \tag{51}$$

式中:φ_i 为观测数据,$\varphi_i=\boldsymbol{H}_i x+\omega_i$; σ_i 为正则化参数;$\boldsymbol{H}_i$ 为测量矩阵,$\boldsymbol{H}_i\in\mathbf{R}^{m\times d}$;$\omega_i$ 为高斯噪声;多智能体系统中每个智能体用来测量未知参数 x, $x\in\Omega$。在整个仿真过程中,设置 $\theta=20$, $\mu=1$,步长 $\alpha_t=0.05/t$, $\delta=0.4$。仿真结果如图 2~7 所示。

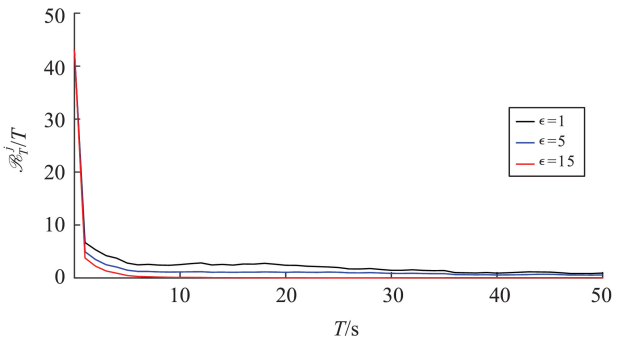

图 2　隐私水平对算法收敛性能的影响

Fig.2　The influence of privacy level on the convergence performance of the algorithm

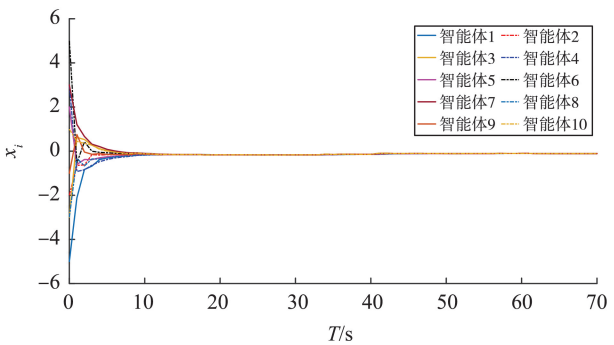

图 3　x 的收敛过程

Fig.3　The convergence process of x

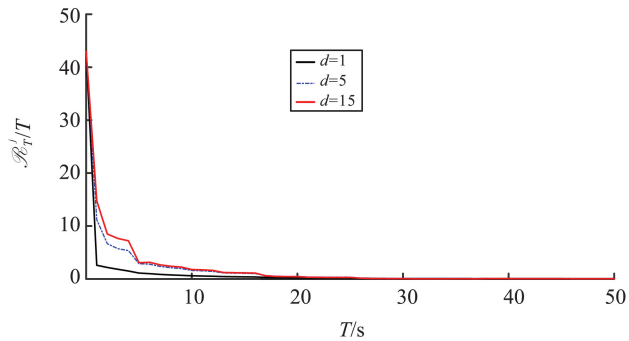

图 4　维度对算法收敛性能的影响

Fig.4　The influence of dimension on the convergence performance of the algorithm

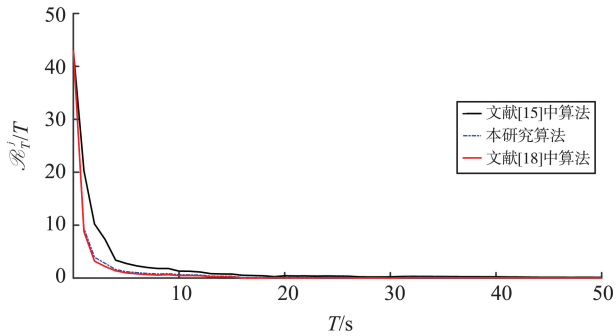

图 5　算法性能比较

Fig.5　Performance comparison of algorithms

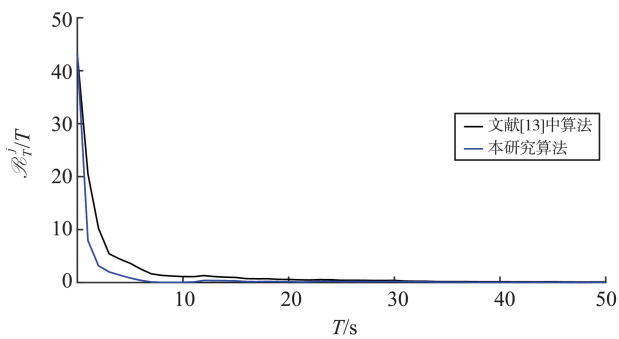

图 6　梯度已知下本研究算法和梯度下降算法性能比较

Fig.6　Comparison of performance between the algorithm proposed and the gradient descent algorithm under known gradients

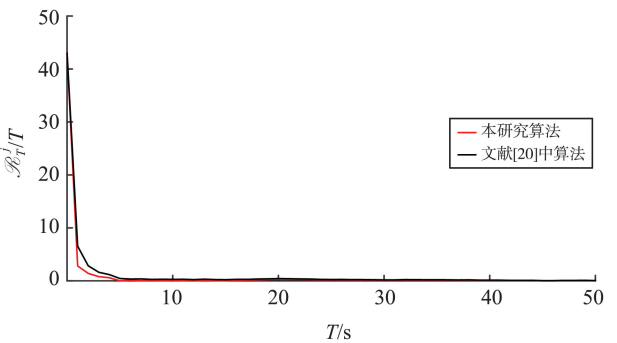

图 7　本研究算法和单点反馈算法性能比较

Fig.7　Comparison of performance between the algorithm proposed and the One-Point feedback algorithm

本文研究在不同隐私保护水平下算法的收敛性能,隐私水平对算法收敛性能的影响如图 2 所示。由图 2 可知,隐私保护程度越高,算法收敛性能越差,在节点状态中注入噪声对收敛精度造成一定的影响,隐私保护水平和收敛精度之间存在一个折中。

x 的收敛过程如图 3 所示。在图 3 中,通过设置 ϵ 为 15,研究每个智能体的状态演化轨迹。结果表明,每个智能体的状态收敛到全局最优解,能够有效解决分布式在线优化问题。

维度对算法收敛性能的影响如图 4 所示。由图 4 可知,维度越低,个体 Regret 的收敛性能越好。

在相同的设置下,对本研究提出的算法、传统的单点反馈算法[15]、基于真实梯度信息的算法[18]的收敛性能进行比较。结果如图 5 所示。

和传统的单点反馈算法相比,本研究的单点反馈算法收敛速率更快。和基于真实梯度信息的算法相比,本研究提出的算法收敛性能略差,但本研究所提出的算法不需要精确的梯度计算,适应于梯度信息不可用的场景。

在梯度信息可用的情况下,将本研究算法与文献[13]中的梯度下降算法进行比较,比较结果如图 6 所示。

由图 6 可知,本研究所提出的算法性能明显优于文献[13]中的梯度下降算法,且本研究的算法能够保护节点的隐私信息。

将本研究的算法和同样基于单点反馈的分布式在线优化算法相比,结果如图 7 所示。

由图 7 可知,本研究的算法能够实现与之相当的性能,但本研究的算法仅要求权值矩阵是行随机的,适用于更一般的网络拓扑结构。

4 结论

本研究针对具有隐私保护特性和梯度信息不可用的分布式在线优化问题,提出一种分布式在线优化算法,引入性能评估指标个体 Regret 的概念。经过严格分析表明,算法个体 Regret 能够实现次线性收敛,能够有效解决分布式在线优化问题。通过差分隐私机制对节点的状态进行扰动,有效保护了节点的隐私信息,并揭示了优化精度和隐私保护水平之间的平衡,隐私水平越高,算法收敛性能越差。引入单点反馈估计真实的梯度信息,以估计的梯度信息指导节点状态的更新,避免精确的梯度计算。仿真结果验证了算法的有效性。在未来的工作中,将进一步考虑优化算法的 Regret 界,并将所提出的算法扩展到时变拓扑场景中。

参考文献:

[1] ZHAO Z Y, XIA L C, JIANG L Y, et al. Zeroth-order gradient tracking for decentralized learning with privacy guarantees[J]. ISA Transactions, 2024, 152: 1-14.

[2] 王程, 刘念. 基于交替方向乘子法的互联微电网系统分布式优化调度[J]. 电网技术, 2016, 40(9): 2675-2681.
WANG Cheng, LIU Nian. Distributed optimal dispatching of interconnected microgrid system based on alternating direction method of multipliers[J]. Power System Technology, 2016, 40(9): 2675-2681.

[3] WANG S N, LI C G. Distributed robust optimization in networked system[J]. IEEE Transactions on Cybernetics, 2016, 47(8): 2321-2333.

[4] ZHAO Z Y. Sample-based dynamic event triggered algorithm for optimization problem of multi-agent systems[J]. International Journal of Control, Automation and Systems, 2022, 20(8): 2492-2502.

[5] 杨涛, 徐磊, 易新蕾, 等. 基于事件触发的分布式优化算法[J]. 自动化学报, 2022, 48(1): 133-143.
YANG Tao, XU Lei, YI Xinlei, et al. Event-triggered distributed optimization algorithms[J]. Acta Automatica Sinica, 2022, 48(1): 133-143.

[6] XI C G, KHAN U A. Distributed subgradient projection algorithm over directed graphs[J]. IEEE Transactions on Automatic Control, 2017, 62(8): 3986-3992.

[7] LI H Q, WANG Z, CHEN G, et al. Distributed robust algorithm for economic dispatch in smart grids over general unbalanced directed networks[J]. IEEE Transactions on Industrial Informatics, 2020, 16(7): 4322-4332.

[8] 陈刚, 李志勇. 集合约束下多智能体系统分布式固定时间优化控制[J]. 自动化学报, 2022, 48(9): 2254-2264.
CHEN Gang, LI Zhiyong. Distributed fixed-time optimization control for multi-agent systems with set constraints[J]. Acta Automatica Sinica, 2022, 48(9): 2254-2264.

[9] YAN F, SUNDARAM S, VISHWANATHAN S V N, et al. Distributed autonomous online learning: regrets and intrinsic privacy-preserving properties[J]. IEEE Transactions on Knowledge and Data Engineering, 2012, 25(11): 2483-2493.

[10] 刘洋. 时变非平衡图下多智能体分布式优化算法设计[D]. 大连：大连理工大学，2021：35-43.
LIU Yang. Design of distributed optimization algorithm for multi-agent systems over time-varying unbalanced graphs[D]. Dalian:Dalian University of Technology, 2021: 35-43.

[11] MATEOSN ÚÑEZ D, CORTÉS J. Distributed online convex optimization over jointly connected digraphs[J]. IEEE Transactions on Network Science and Engineering, 2014, 1(1): 23-37.

[12] 吴庆涛，朱军龙，葛泉波，等. 一种基于条件梯度的加速分布式在线学习算法[J]. 自动化学报，2024，50(2)：386-402.
WU Qingtao, ZHU Junlong, GE Quanbo, et al. An accelerated distributed online learning algorithm based on conditional gradient[J]. Acta Automatica Sinica, 2024, 50(2): 386-402.

[13] PANG Y P, HU G Q. Randomized gradient-free distributed online optimization with time-varying cost functions[C]//2019 IEEE 58th Conference on Decision and Control (CDC). Nice, France:IEEE, 2019: 4910-4915.

[14] PANG Y P, HU G Q. Randomized gradient-free distributed optimization methods for a multiagent system with unknown cost function[J]. IEEE Transactions on Automatic Control, 2020, 65(1): 333-340.

[15] WANG C, XU S Y, YUAN D M, et al. Push-sum distributed online optimization with bandit feedback[J]. IEEE Transactions on Cybernetics, 2022, 52(4): 2263-2273.

[16] DWORK C. Differential privacy[C]// International Colloquium on Automata, Languages, and Programming. Berlin, Germany: Springer, 2006: 1-12.

[17] DING T, ZHU S Y, HE J P, et al. Differentially private distributed optimization *via* state and direction perturbation in multiagent systems[J]. IEEE Transactions on Automatic Control, 2022, 67(2): 722-737.

[18] XIONG Y Y, XU J M, YOU K Y, et al. Privacy-preserving distributed online optimization over unbalanced digraphs *via* subgradient rescaling[J]. IEEE Transactions on Control of Network Systems, 2020, 7(3): 1366-1378.

[19] WEI M L, YANG Z Q, JI Q T, et al. Privacy-preserving distributed projected one-point bandit online optimization over directed graphs[J]. Asian Journal of Control, 2023, 25(6): 4705-4720.

[20] ZHAO Z Y, YANG J, GAO W, et al. Differentially private distributed online optimization *via* push-sum one-point bandit dual averaging[J]. Neurocomputing, 2024, 572: 127184.

(编辑:郭少华)

(上接第 13 页)

[64] CAO Y M, CUI L Z, ZHANG L, et al. MMTN: multi-modal memory Transformer network for image-report consistent medical report generation[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2023, 37(1): 277-285.

[65] CAO Y M, CUI L Z, ZHANG L, et al. CMT: cross-modal memory Transformer for medical image report generation[C]// Database Systems for Advanced Applications. Cham, Switzerland: Springer, 2023: 415-424.

[66] CAO Y M, LI Z, CUI L Z, et al. Adaptive human-LLMs interaction collaboration: reinforcement learning driven vision-language models for medical report generation[C]//Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems. Yokohama, Japan: ACM, 2025: 1-6.

[67] QU Z, CUI L Z, XU Y H. Disease risk prediction via heterogeneous graph attention networks[C]//2022 IEEE International Conference on Bioinformatics and Biomedicine (BIBM). Las Vegas, USA: IEEE, 2023: 3385-3390.

[68] GE W, GUO W, CUI L Z, et al. Detection of wrong disease information using knowledge-based embedding and attention[C]// Database Systems for Advanced Applications. Cham, Switzerland: Springer, 2020: 459-473.

[69] CAO Y M, CUI L Z, ZHANG L, et al. KdINet: knowledge-driven interpretable network for medical imaging diagnosis[C]//2022 IEEE International Conference on Bioinformatics and Biomedicine (BIBM). Las Vegas, USA: IEEE, 2023: 1457-1460.

[70] GUO W, GE W, CUI L Z, et al. An interpretable disease onset predictive model using crossover attention mechanism from electronic health records[J]. IEEE Access, 2019, 7: 134236-134244.

[71] YU F Q, CUI L Z, CAO Y M, et al. Feature-guided logical perception network for health risk prediction [C]//2022 IEEE International Conference on Bioinformatics and Biomedicine (BIBM). Las Vegas, USA: IEEE, 2023: 1787-1790.

(编辑:孙亚彤)