廣東工業大學

QG 中期考核项目详细报告书

题　　目	《差分隐私平均共识》学习报告
学　　院	计算机学院
专　　业	计算机类
年级班别	大一 7 班
学　　号	3124004298
学生姓名	吴嘉健

2025 年 4 月 2 日

目 录

1.研究背景与意义

随着社交网络、智能电网和智能交通等网络化物理系统的广泛应用，个体信息的隐私保护成为技术社会采纳的关键因素。在这些场景中，网络系统需要融合信息、计算未知量的公共估计并就"共同世界观"达成一致。平均共识问题在此背景下尤为重要，它要求一组智能体仅通过与邻居交换信息来就个体值的平均数达成一致。

差分隐私(DP)近年来因其严谨的数学表述和经证明的安全属性而广受欢迎，这些属性包括对后处理和辅助信息的弹性，以及对对抗模型的独立性。简而言之，如果一个策略是差分隐私的，那么单个代理的信息对算法聚合输出的影响微乎其微，因此对抗者无法从其执行中推断出原始数据。

2.主要贡献与研究成果

论文研究的是在**一组智能体试图计算并同意其局部变量的平均值**的同时，**保护这些变量免受具有潜在访问所有组通信能力的对抗者的差分隐私攻击**的问题。这种隐私要求也适用于每个智能体希望对其初始状态保持私密性，不受组内其他成员（例如由于通信泄漏可能性）获取的情况。研究发现，在差分隐私约束下无法保证智能体状态收敛到其初始值的精确平均值，并提出了最优的线性一致性算法设计。

该研究的主要贡献包括：

1) 一般不可能性结果的表述和证明：研究表明，只要协调算法是差分隐私的，就不可能保证代理状态收敛到其初始值的平均值(即使在分布中)。这一结果自动暗示了更强收敛概念的相同不可能性。

2) 线性 Laplacian-based 共识算法设计：设计了一种在期望中达到平均共识的算法(这是可以期望的最多结果)，证明了该算法的几乎必然收敛性和差分隐私性，并表征了其准确性和收敛速度。

3) 最优设计参数计算：在智能体固定(局部)所需隐私要求值的情况下，将算法收敛点的方差最小化为噪声状态增益以及噪声振幅和衰减率的函数。结果显示，通过拉普拉斯噪声对初始状态的单次扰动可实现最小方差。

3.关键技术与理论框架

3.1 障碍分析

作者证明了即使采用最弱的收敛性定义，也无法实现完全精确的差分隐私平均共识（即(0,0)-精度的不可能性）。这源于隐私保护要求与算法准确性之间的根本矛盾。

矛盾构造：通过 Borel 集和概率分析，作者构造了一个反例场景（R’(2)_k），证明随着参数调整，某些事件的概率可被无限缩小，导致隐私保护与准确性无法同时满足。

关键不等式：通过选择参数 υ ＜ δ/2n，推导出两个集合 N(1)_k 与 N(2)_k 不相交，从而验证隐私约束下必然存在精度损失。

算法的收敛性需放宽至渐近形式（如第 5 节分析的算法(12)-(14)所示），而严格的精确收敛会破坏差分隐私条件。第 5.3 节进一步说明，最优噪声设计是平衡隐私与精度的关键[未直接引用但逻辑关联]。

3.2 算法设计与分析

研究提出的线性一致性算法具有以下特征：

1)几乎必然收敛性

2)差分隐私保证

3)期望中的平均共识

4)最优噪声参数设计

5)量化了隐私保护与精度之间的权衡

在理论分析方面，研究首先确立了即使考虑最弱的收敛概念，也无法用(0,0)-精度解决问题。随后通过数学推导表明，概率 P(R’(2)k)可以通过某种方式变得任意小。

4.实验结果与验证

实验通过多种场景（不同噪声参数、拓扑结构、初始状态）验证了微分隐私平均共识算法的**收敛性**、**无偏性**和**最优性**，同时量化了隐私保护与精度之间的权衡。这些结果与理论分析（如命题 5.2、5.10 等）高度一致，并通过大量重复实验和统计方法确保了结论的可靠性。

4.1 实验设置与网络拓扑

网络结构：实验中使用的网络由 50 个智能体（n=50） 构成，其通信拓扑为随机生成的无向图。

边权重的生成方式：每条边的权重是独立同分布的随机变量，由两个参数为 p=0.1 的伯努利随机变量相加得到。这种设计旨在模拟稀疏连接的网络场景。

初始状态：智能体初始状态服从正态分布 N(50,100)，且与网络拓扑无关。值得注意的是，算法的隐私性和准确性理论上与初始值和通信拓扑无关，但收敛速度会受拓扑影响。

噪声设计与隐私参数：噪声机制采用 拉普拉斯分布（Lap($b_i(k)$)），其中噪声参数 $b_i(k)$ 按 $c_iq_i^k$ 动态衰减。隐私预算 ε 和邻接敏感度 δ 固定为 δ=1，拉普拉斯噪声被证明在差分隐私保护下能最小化信息熵，是理论最优选择。

4.2 仿真结果与关键发现

通过多种仿真验证了研究结果[19]，表明:

1)所设计的差分隐私共识算法确实能在期望中实现平均共识

2)单次 Laplace 噪声扰动是最优噪声策略

3)算法的收敛性、隐私性和准确性达到了理论分析预测的性能

4)当参数 s（噪声增益）接近 1 时，算法表现出最优的收敛精度（最小方差）和最快的收敛速度（"settling time"最短）

5)精度与隐私的为反比关系

5.研究启示与意义

本文研究表明,在差分隐私约束下,多智能体系统无法精确实现传统意义上的平均共识,但通过精心设计的噪声机制可以在期望意义上达到最优近似。这一发现为隐私保护协同控制提供了理论基础和实用算法，对构建既安全又高效的大型分布式系统具有重要价值。

该研究对网络化系统中隐私保护与控制算法的协同设计具有重要意义。未来的研究方向包括：

1)多智能体系统中差分隐私限制与优势的进一步研究

2)结果扩展到动态平均共识、分布式优化、滤波和估计

3)设计用于保护网络结构隐私和其他参数(如边权重和顶点度数)的算法

4)差分隐私与多智能体系统的结合,为隐私保护算法设计提供了新思路

5)非理想场景的鲁棒性:如通信延迟或恶意节点存在时，如何保持隐私-性能权衡（参考输入扰动分析）仍需深入。

6)动态拓扑与时变隐私需求:当前分析基于固定通信图，未来可探索动态网络下的自适应隐私算法。

6.参考文献

[1]Erfan Nozari ,Pavankumar Tallapragada , Jorge Cortés ,《Automatica》81,221-231, 3 February 2017,“Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design”[J]