北京交通大學
BEIJING JIAOTONG UNIVERSITY

面向高效鲁棒联邦学习的传算联合优化方法研究

答辩学生：范新

指导老师：霍炎教授、Zhi Tian教授（联培导师）

答辩日期：2022年12月5日

目录

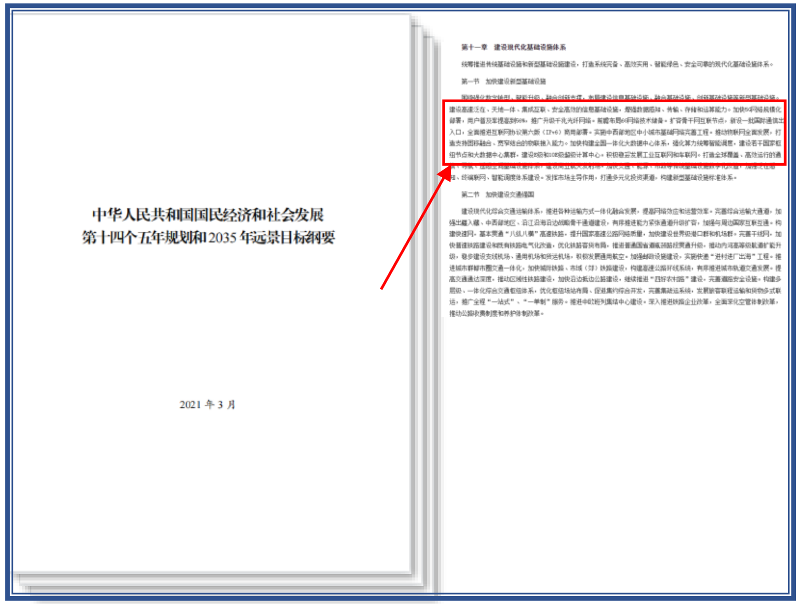
CONTENTS

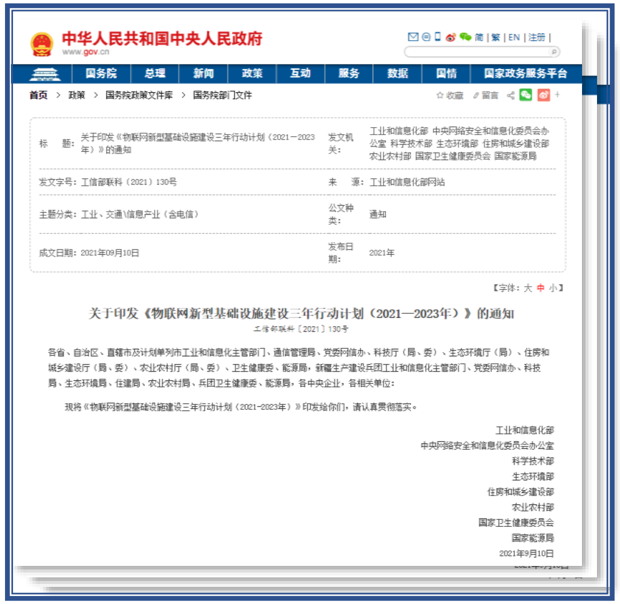
PART ONE

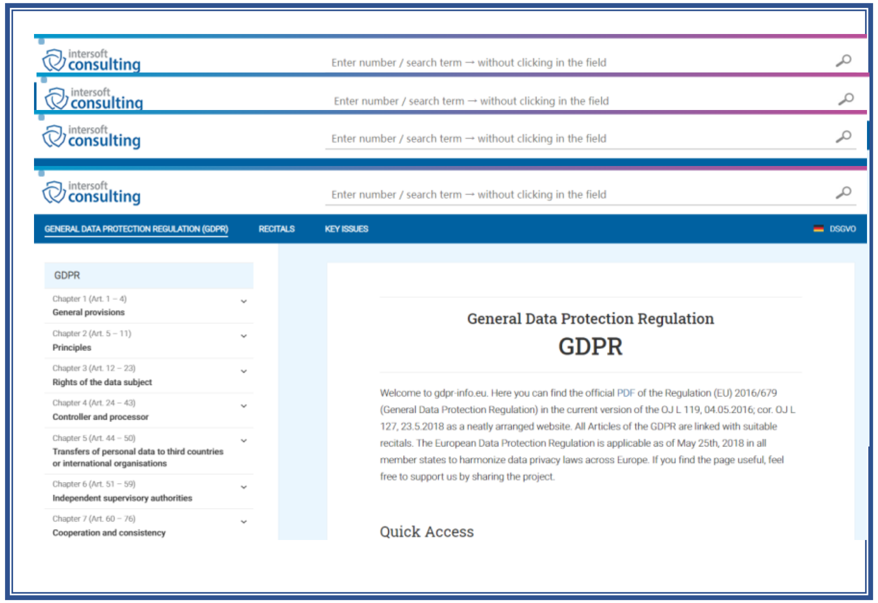
研究背景

研究背景

- 2021年3月国务院发布《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》，**我国要增强数据感知、传输、存储和运算能力，强化算力统筹智能调度**。
- 2021年9月国家工业和信息化部等部门联合发布《物联网新型基础设施建设三年行动计划（2021-2023年）》，提出要**聚焦感知、传输、处理、存储、等重点环节，加快关键核心技术攻关**。
- 2018年5月欧洲联盟出台《通用数据保护条例（General Data Protection Regulation，GDPR）》，提出针对**大数据合理应用与隐私保护的法案**。





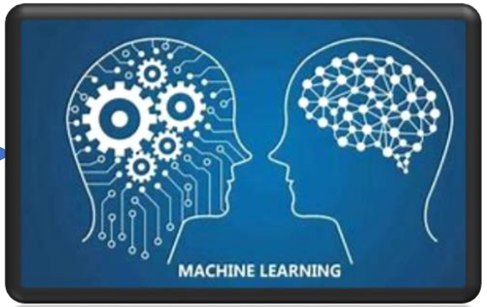


研究背景

大数据

大数据

机器学习



充分利用数据
精准做出决策

集中式机器学习

- 原始数据传输消耗巨大
- 收集数据暴露用户隐私
- 中心节点负担过重

联邦学习（Federated Learning，FL）

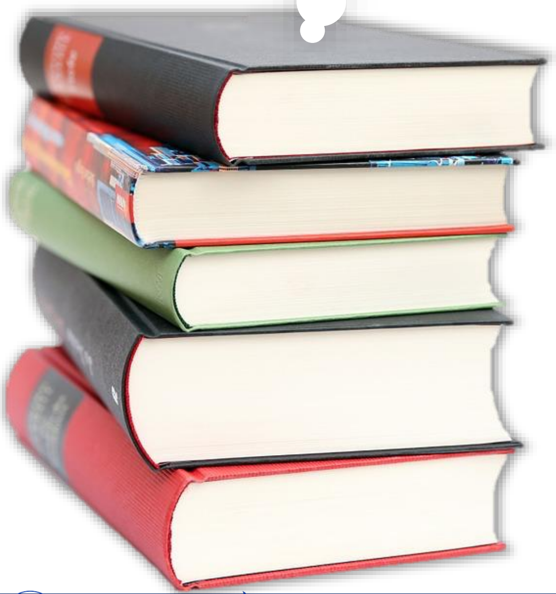
仅传输模型参数　　节省通信开销同时保护用户隐私
分布式协作计算　　充分利用计算资源，减轻中心节点负担

高维神经网络
海量设备
复杂场景

通信
新的瓶颈

本文主题：
FL中的通信问题

研究现状



传什么?

- ◆减少分布式设备数目[20, 38]
- ◆稀疏[13,14]
- ◆量化[15-17]
- ◆通信审查[18-22]

如何传?

- （数字）通信、计算资源的分配和调度方法[40-44]
- **基于空中计算技术的联邦学习（Federated Learning Over the Air，FLOA）[31,32,59,61]**

空中计算技术

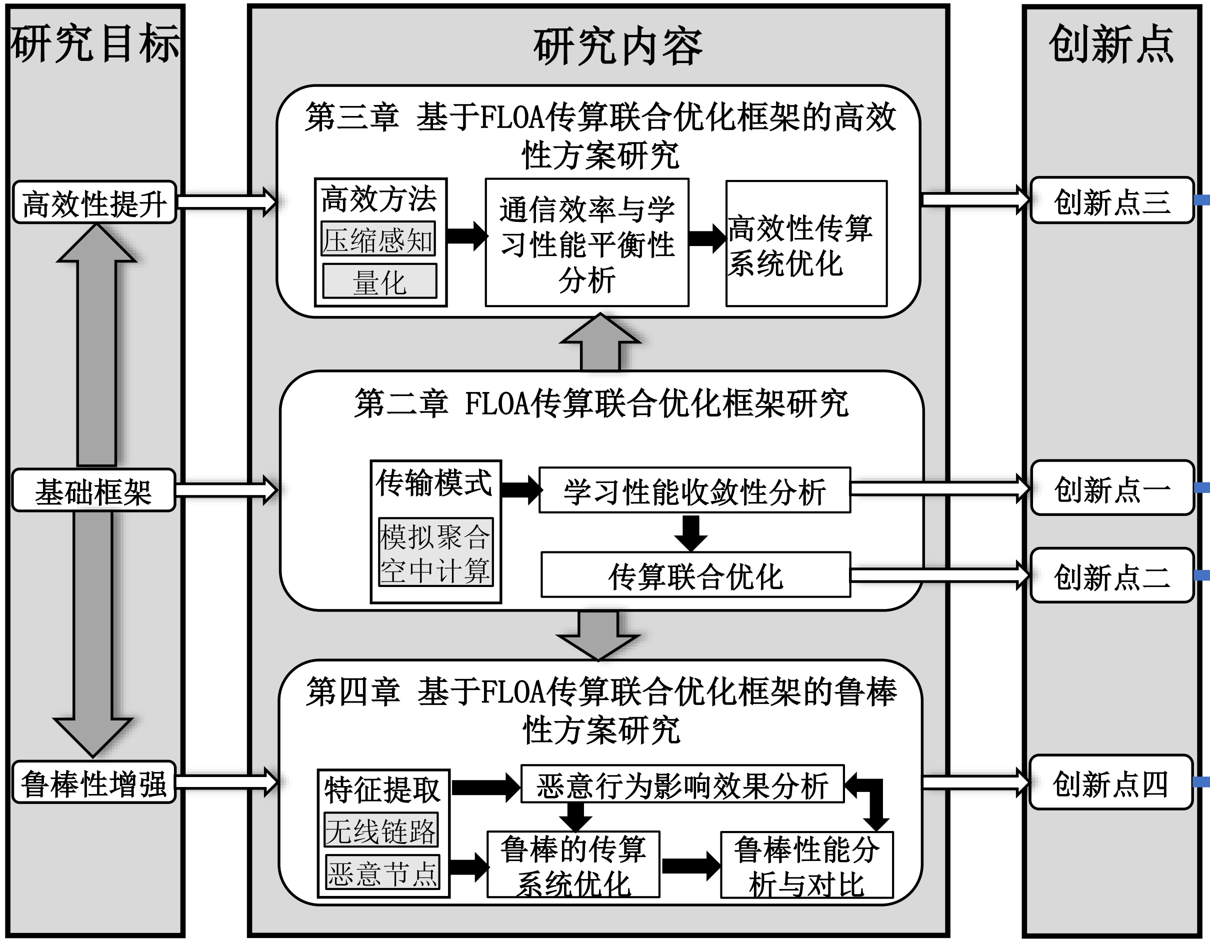
- ■ 非编码的线性模拟调制
- ■ 多设备同时同频同空间传输
- ■ 电磁波叠加，实现和函数功能
- ■ 在接收端直接得到聚合值

FLOA尚未解决问题

- ☐ 通信与学习关系定量化描述问题
- ☐ 传算联合优化问题
- ☐ 高效性提升问题
- ☐ 恶意节点对抗问题

PART TWO

论文结构



FLOA尚未解决的问题

- 高效性提升问题
- 通信与学习关系的定量化描述问题
- 传算联合优化问题
- 恶意节点对抗问题

PART THREE

研究内容

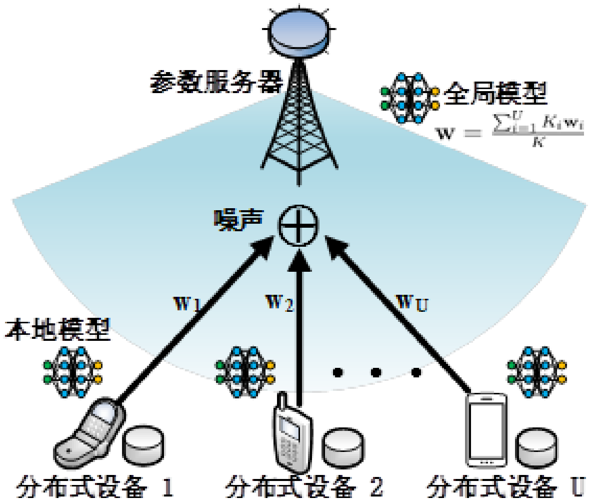
研究内容一

FLOA传算联合优化框架研究

FLOA传算联合优化框架研究

系统模型

- **联邦学习模型（不考虑通信误差）**
  - 分布式设备
    - 接收模型参数
      $$\mathbf{w} = [w^1, \ldots, w^D] \in \mathcal{R}^D$$
    - 更新模型参数 $\mathbf{w}_i$
    - 发送新的模型参数
  - 服务器
    - 接收所有模型参数 $\mathbf{w}_i$
    - 求模型的平均值 $\boxed{\mathbf{w} = \frac{\sum_{i=1}^{U} K_i \mathbf{w}_i}{K}}$
    - 广播 $\mathbf{w}$ 给所有分布式设备



无偏估计

- **FLOA模型（采用模拟聚合通信）**
  - 分布式设备
    - 信道反转功率控制策略
      $$\mathbf{p}_{i,t} = [p_{i,t}^1, \ldots, p_{i,t}^d, \ldots, p_{i,t}^D]$$
      发送 $\mathbf{w}_{i,t}$ ，其中
      $$p_{i,t}^d = \frac{\beta_{i,t}^d K_i b_t^d}{h_{i,t}^d}$$
  - 服务器
    - 接收信号为
      $$\mathbf{y}_t = \sum_{i=1}^{U} \mathbf{p}_{i,t} \odot \mathbf{w}_{i,t} \odot \mathbf{h}_{i,t} + \mathbf{z}_t$$
    - 使用后处理操作估计 $\mathbf{w}_t$
      $$\boxed{\begin{aligned}\mathbf{w}_t &= \left(\sum_{i=1}^{U} K_i \boldsymbol{\beta}_{i,t} \odot \mathbf{b}_t\right)^{\odot -1} \odot \mathbf{y}_t \\ &= \left(\sum_{i=1}^{U} K_i \boldsymbol{\beta}_{i,t}\right)^{\odot -1} \sum_{i=1}^{U} K_i \boldsymbol{\beta}_{i,t} \odot \mathbf{w}_{i,t} + \left(\sum_{i=1}^{U} K_i \boldsymbol{\beta}_{i,t} \odot \mathbf{b}_t\right)^{\odot -1} \odot \mathbf{z}_t,\end{aligned}}$$

通信如何影响学习的?

➢收敛性分析

✓**推导了**强凸损失函数假设下的收敛性（见**定理2.1**和**引理2.1**）

$$\mathbb{E}[F(\mathbf{w}_t)-F(\mathbf{w}^*)] \le \underbrace{\sum_{i=1}^{t-1}\left(\prod_{j=1}^{i} A_{t+1-j}\right)B_{t-i}+B_t}_{\Delta_t} + \prod_{j=1}^{t} A_j \mathbb{E}[F(\mathbf{w}_0)-F(\mathbf{w}^*)].$$

Δ_t → 性能误差 → 指导优化

推导了收敛条件（见**命题2.1**） → $0<\rho_2<\frac{\mu}{(\frac{K}{K_{min}}-1)DL}$

✓**推导了**非凸损失函数假设下的收敛性（见**定理2.2**）

$$\frac{1}{T}\sum_{t=1}^{T}\|\nabla F(\mathbf{w}_{t-1})\|^2 \le \frac{2L\sum_{t=1}^{T}B_t}{T(1-\rho_2 D(\frac{K}{K_{min}}-1))} + \frac{2L}{T(1-\rho_2 D(\frac{K}{K_{min}}-1))}\mathbb{E}[F(\mathbf{w}_0)]-F(\mathbf{w}^*)].$$

→ Δ_t^{NC} → 性能误差 → 指导优化

→ 收敛条件与强凸下相同

✓**推导了**随机梯度下降法场景的收敛性（见**定理2.3**）

$$\mathbb{E}[F(\mathbf{w}_t)-F(\mathbf{w}^*)] \le \underbrace{\sum_{i=1}^{t-1}\prod_{j=1}^{i} A_{t+1-j}^{SGD}B_{t-i}^{SGD}+B_t^{SGD}}_{\Delta_t^{SGD}} + \prod_{j=1}^{t} A_j^{SGD}\mathbb{E}[F(\mathbf{w}_0)-F(\mathbf{w}^*)],$$

Δ_t^{SGD} → 性能误差 → 指导优化

推导了收敛条件（见**命题2.2**） → $0<\rho_2<\frac{\mu}{(\frac{2UK_b}{K}+\frac{U^2K_b^2}{K^2}+DU-\frac{2DUK_b}{K}+\frac{DU^2K_b^2}{K^2})L}$

FLOA传算联合优化框架研究

➢优化问题建模

最小化性能误差

$$\begin{aligned}\triangle_t &= B_t + A_t\triangle_{t-1},\\ \triangle_t^{NC} &= B_t,\\ \triangle_t^{SGD} &= B_t^{SGD} + A_t^{SGD}\triangle_{t-1}^{SGD}.\end{aligned}$$

元素级优化

优化问题P2.2

$$\begin{aligned}\min_{\{b_t,\beta_{i,t}\}_{i=1}^U} \quad & R_t\\ \text{s.t.} \quad & \left|\frac{\beta_{i,t}K_i b_t}{h_{i,t}} w_{i,t}\right|^2 \le P_i^{\max},\\ & \beta_{i,t}\in\{0,1\}, i\in\{1,2,...,U\}\end{aligned}$$

假设2.4 (局部参数更新有界) $|w_{t-1}-w_{i,t}|\le\eta$

优化问题P2.3

$$\begin{aligned}\min_{\{b_t,\beta_{i,t}\}_{i=1}^U} \quad & R_t\\ \text{s.t.} \quad & \left|\frac{\beta_{i,t}K_i b_t}{h_{i,t}}\right|^2 (|w_{t-1}|+\eta)^2 \le P_i^{\max}\\ & \beta_{i,t}\in\{0,1\}, i\in\{1,2,...,U\},\end{aligned}$$

解决了“蛋鸡悖论”问题

➢优化问题求解

推导了一个紧密的解空间（见**定理2.4**）

$$\mathcal{S}=\left\{\left\{\left(b_t^{(k)},\beta_{i,t}^{(k)}\right)\right\}_{k=1}^U \middle| b_t^{(k)}=\left|\frac{\sqrt{P_k^{\max}}h_{k,t}}{K_k(|w_{t-1}|+\eta)}\right|, \boldsymbol{\beta}_t^{(k)}(b_t^{(k)})=\left[\beta_{1,t}^{(k)},\dots,\beta_{U,t}^{(k)}\right], k=1,\dots,U\right\},$$

提出了一种离散规划方法

$$\min_{(b_t,\boldsymbol{\beta}_t)\in\mathcal{S}} R_t = R_t(b_t,\boldsymbol{\beta}_t)$$ 优化问题**P2.4**

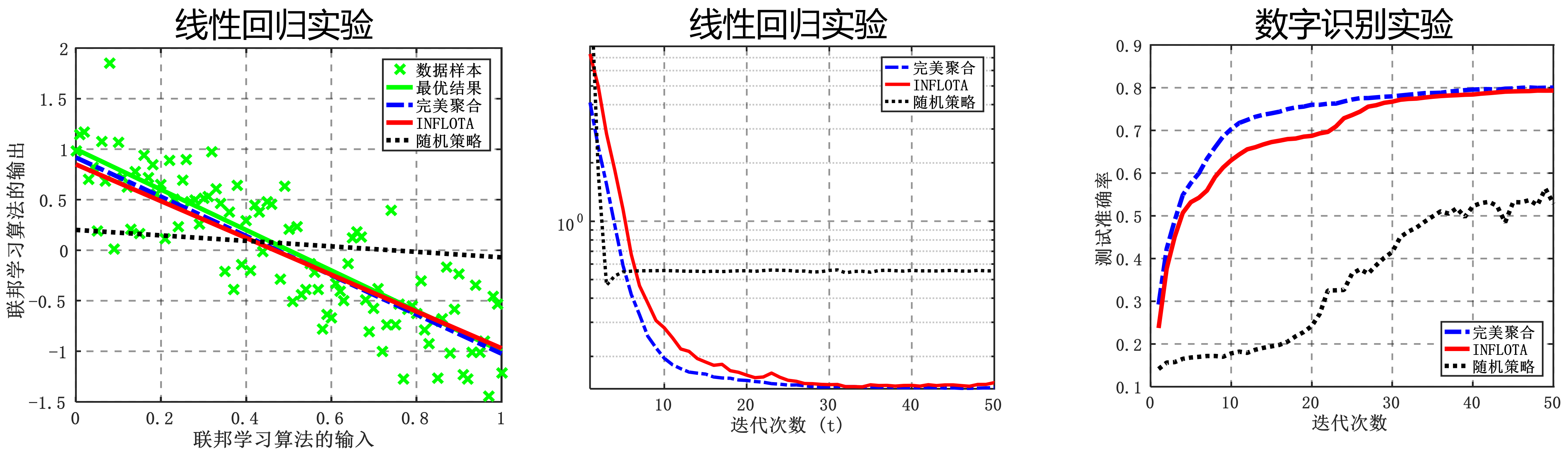
分析了算法复杂度

复杂度**降低**为$\mathcal{O}(U)$ 与设备数成正比

➢实验设定

- 学习任务：线性回归任务（生成数据集）、数字识别任务（MNIST数据集）
- 对比方案：完美聚合（通信无误差、所有设备成功参与）、随机策略（随机选择设备、固定功率分配策略）

➢主要实验结果



结果分析：所提出的INFLOTA方案**逼近**理想完美聚合方案、**优于**随机策略方案

FLOA传算联合优化框架研究

➢小结

- 在GD或SGD实现的凸和非凸损失函数情况下，本章**全面推导了**FLOA算法的收敛速率闭式表达式，**量化了**通信与学习间关系，**奠定了**传算联合优化理论基础
- **提出了**考虑分布式设备选择和功率控制的通信和学习联合优化框架，**降低了**通信对学习的负面影响，**提升了**学习准确率

➢相关研究成果

- ✓ **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. Joint Optimization for Federated Learning Over the Air [C] //*2022 IEEE International Conference on Communications* (IEEE ICC 2022). **（EI/ISTP检索；通信领域旗舰国际会议； CCF C类；北交大A类；对应学位论文第二章)**
- ✓ **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. Joint Optimization of Communications and Federated Learning Over the Air[J]. *IEEE Transactions on Wireless Communications*, vol. 21, no. 6, pp. 4434-4449, June 2022.**（SCI检索； 2022年影响因子8.346；中科院一区；JCR一区；北交大A+；对应学位论文第二章)**

研究内容二

基于FLOA传算联合优化框架的高效性方案研究

➢系统模型

□分布式设备

■接收到模型后计算梯度 $\mathbf{g}_i$

■稀疏化

- Top-k： $\tilde{\mathbf{g}}_{i,t} = \mathtt{sparse}_{\kappa}(\mathbf{g}_{i,t}),$

■降维

- 高斯矩阵 $\mathbf{\Phi} \in \mathbb{R}^{S\times D}\ (S \ll D)$

■一比特量化

- 全部压缩操作

$$\mathcal{C}(\mathbf{g}_{i,t}) = \mathtt{sign}(\mathbf{\Phi}\mathtt{sparse}_{\kappa}(\mathbf{g}_{i,t}))$$

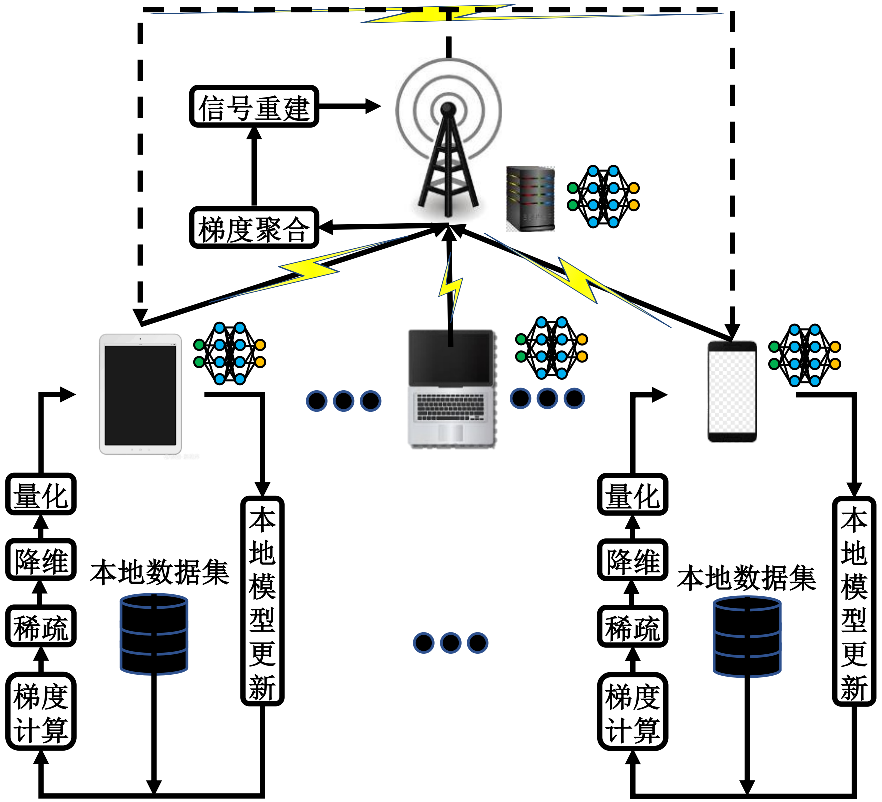
■模拟聚合传输

- 功率控制 $p_{i,t} = \dfrac{\beta_{i,t}K_i b_t}{h_{i,t}},$

□服务器

■信号重建

$$\hat{\mathbf{y}}_t^{desired} = (\sum_{i=1}^{U} K_i\beta_{i,t}b_t)^{-1}\mathbf{y}_t \longrightarrow \hat{\mathbf{g}}_t = \mathcal{C}^{-1}(\hat{\mathbf{y}}_t^{desired})$$



➢收敛性分析

□**推导了**非凸假设下的收敛性（见**定理3.1**）

$$\frac{1}{T}\sum_{t=1}^{T}\|\nabla F(\mathbf{w}_{t-1})\|^2 \le \frac{2L}{T(1-2\rho_2(U+K))}\mathbb{E}[F(\mathbf{w}_0)-F(\mathbf{w}^*)] + \frac{2L}{T(1-2\rho_2(U+K))}\sum_{t=1}^{T}B_t,$$

□ T 趋于无穷时

$$\frac{1}{T}\sum_{t=1}^{T}\|\nabla F(\mathbf{w}_{t-1})\|^2 \le \frac{2L}{T(1-\rho_2)}\mathbb{E}[F(\mathbf{w}_0)-F(\mathbf{w}^*)] + \frac{2L}{T(1-\rho_2)}\sum_{t=1}^{T}B_t$$

$$\xrightarrow{T\to\infty} \frac{2L}{T(1-\rho_2)}\sum_{t=1}^{T}B_t.$$

→ 性能误差 → 指导优化 →

如何求解?

□ **优化问题：**

优化功率缩放因子和设备选择向量

$$\min_{b_t,\boldsymbol{\beta}_t} \quad B_t$$

$$\text{s.t.} \quad \frac{\beta_{i,t}^2 K_i^2 b_t^2}{h_{i,t}^2} \le P_i^{\mathrm{Max}},$$

$$\beta_{i,t} \in \{0,1\}, i \in \{1,2,...,U\}$$

→ 非凸的混合整数规划

➢求解算法

□提出了基于离散规划的最优解

- ■ 遍历
  - ● 给定设备选择向量，优化问题为凸优化
  - ● 遍历所有设备选择情况可得最优解
- ■ 最优解
- ■ **分析了算法**复杂度 $\mathcal{O}(2^U)$
- ■ 适用于少量设备场景，e.g., U ≤ 10

□提出了基于交替方向乘子法的次优解

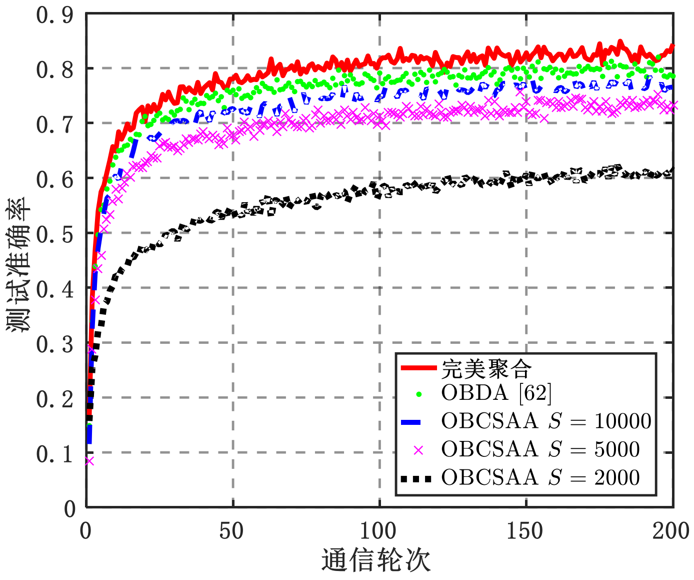
- ■分解
  - ●将优化变量进行解耦合操作
  - ●迭代求解
- ■次优解
- ■**分析了**算法复杂度 $\mathcal{O}(U)$
- ■适用于大规模场景，e.g., U ≥ 10

➢实验设定

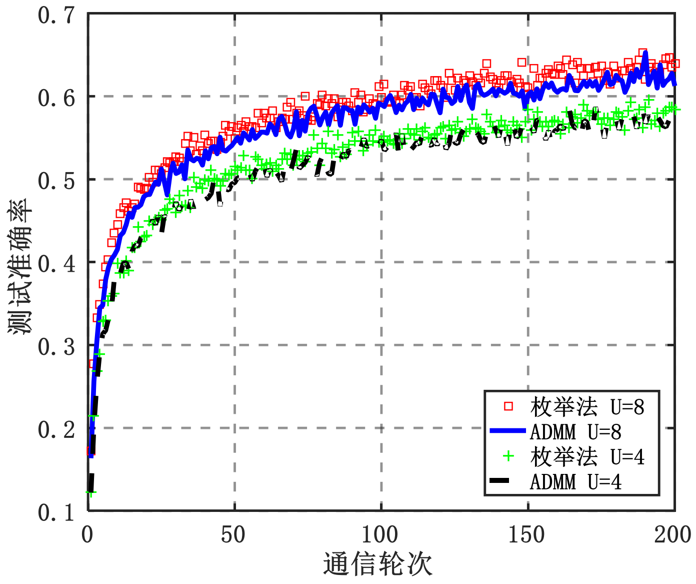
- ☐数字识别任务（MNIST数据集）
- ☐对比方案：OBDA（量化）[62]、CA-DSGD（稀疏、降维）[29]

➢主要实验结果

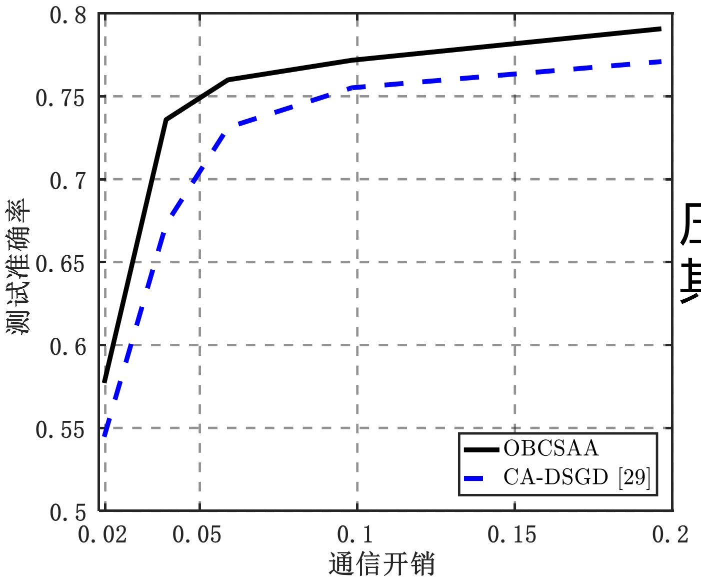
①



②



③



压缩比：S/D，其中D=50896

① 大压缩比下也可以趋近理想情况　② ADMM算法趋近枚举法性能　③ 相同压缩比下本方案有更高的学习性能

➢小结

- **提出了**一种基于1比特压缩感知技术和模拟聚合传输的高效通信联邦学习方案
- **推导了**收敛速率闭式表达式，**量化了**由稀疏化、降维压缩、量化、信号重构和信道噪声引起的聚合误差
- **提出了**通信和学习的联合优化方法，**减轻了**聚合误差对联邦学习的影响

➢相关研究成果

✓ **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. Communication-efficient Federated Learning Through 1-Bit Compressive Sensing and Analog Aggregation[C] //*2021 IEEE International Conference on Communications (IEEE ICC 2021)*. **(EI/ISTP国际会议；CCF C类；北交大A类; 对应学位论文第三章)**

✓ **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. 1-Bit Compressive Sensing for Efficient Federated Learning Over the Air[J]. *IEEE Transactions on Wireless Communications*, oct, 2022, early access. **(SCI期刊；2022年影响因子8.346；中科院一区；JCR一区；北交大A+；对应学位论文第三章)**

研究内容三

基于FLOA传算联合优化框架的鲁棒性方案研究

➢系统模型

□共U个设备，N个攻击者，M=U-N个正常设备

性能如何?

$$\mathbf{y}_t = \sum_{m=1}^{M} p_{m,t}|h_{m,t}|\tilde{\mathbf{g}}_{m,t} + \sum_{n=1}^{N} \hat{p}_{n,t}|h_{n,t}|\hat{\mathbf{g}}_{n,t} + \mathbf{z}_t.$$

□现存的信道反转（Channel Inversion，CI）功率控制

□功率缩放

$$p_{i,t} = \frac{b_0}{|h_{i,t}|}, \quad \forall i$$

□当N=0时，

$$\mathbf{y}_t = \sum_{m=1}^{U} b_0 \tilde{\mathbf{g}}_{m,t} + \mathbf{z}_t \longrightarrow \hat{\mathbf{g}} = \frac{\mathbf{y}_t}{Ub_0} = \frac{\sum_{m=1}^{U} \tilde{\mathbf{g}}_{m,t}}{U} + \frac{\mathbf{z}_t}{Ub_0} \xleftrightarrow{\text{无偏估计}} \boxed{\mathbf{g} = \frac{\sum_{i=1}^{U} \mathbf{g}_{i,t}}{U}}$$

无通信误差的理想情况

□**提出了**最大努力投票（Best Effort Voting, BEV）功率控制

□最大功率发送

$$p_{i,t}^2 \leq p_i^{\max}, \quad \forall i$$

Voting: [3 2 1 4 -5]→5 ← **Voting: [1 1 1 1 -5]→-1**

性能分析

- **推导了**最强拜占庭攻击方式（见**定理4.1**）
  - 使用本地数据算出梯度
  - 以最大功率发送反向梯度
- **推导了**信道反转（CI）功率控制下的收敛性（见**定理4.2**）
  - **推导了**收敛性条件
  - **推导了**能对抗的最大拜占庭设备数 $\frac{U}{1+\sqrt{\pi U}}$
- **推导了**最大努力投票（BEV）功率控制下的收敛性（见**定理4.3**）
  - **推导了**收敛性条件
  - **推导了**能对抗的最大拜占庭设备数 $\frac{U}{2}$

U为设备总数

$$\boxed{\frac{U}{2} \geq \frac{U}{1+\sqrt{\pi U}}}$$

➢ 性能分析（续）

□大学习速率

- 收敛速度为 $O(\frac{1}{\Omega\sqrt{T}})$　　$\Omega_{BEV} > \Omega_{CI}$

<u>最大努力投票</u>优于<u>信道反转</u>

□小学习速率

- 收敛速度为 $O(\frac{\Omega}{\omega^2\sqrt{T}})$

取决于具体参数

□无攻击小学习速率

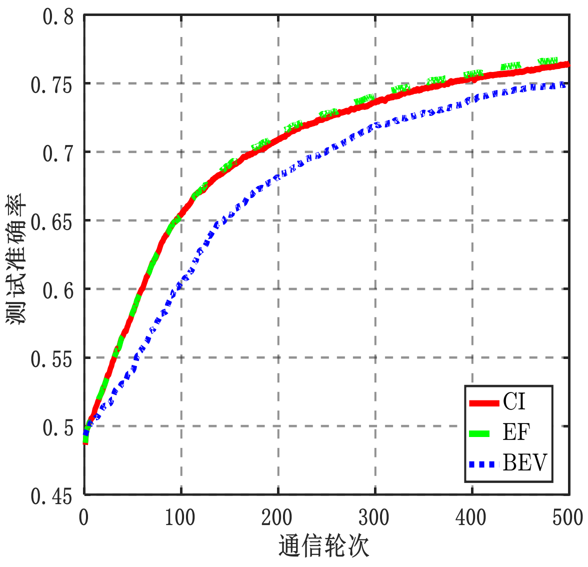
- CI 有 $\omega_{CI}^2 = \Omega_{CI}$
  - 收敛速度为 $O(\frac{1}{\sqrt{T}})$ → **无误差传输的理想情况**
- BEV 有 $\omega_{BEV}^2 \leq \Omega_{BEV}$
  - 收敛速度 $O(\frac{\Omega_{BEV}}{\omega_{BEV}^2\sqrt{T}})$

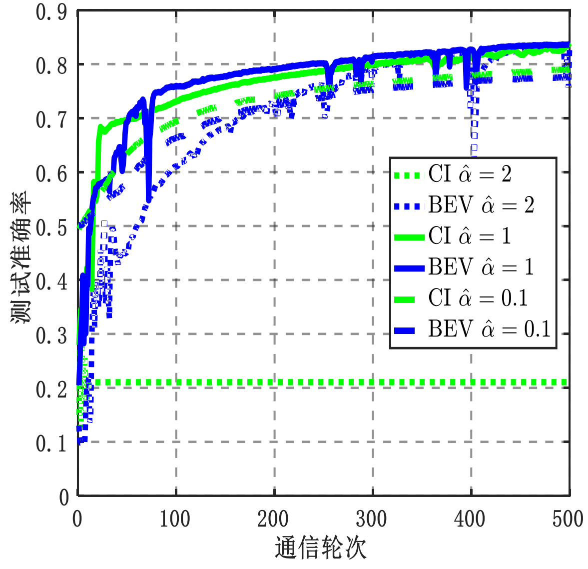
<u>信道反转</u>优于<u>最大努力投票</u>

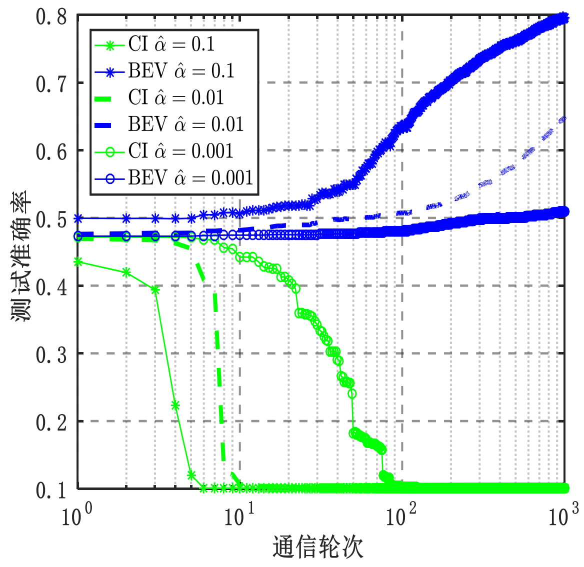
➢实验设定

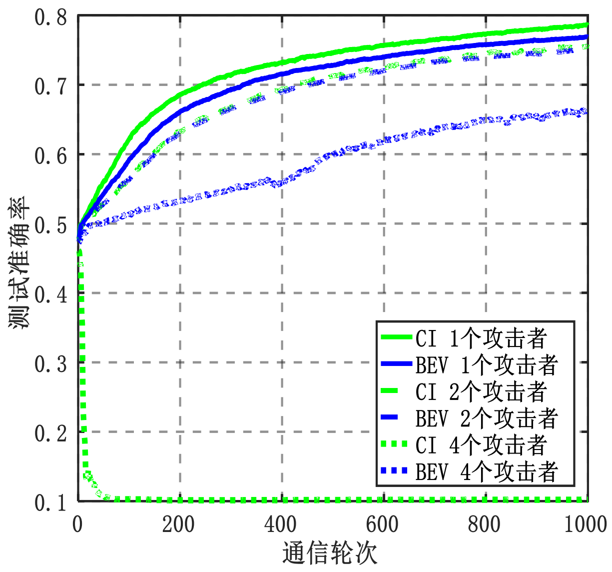
➢强攻击：最高信道增益的单个攻击者；弱攻击：最低信道增益的单个攻击者

➢主要实验结果









① 无攻击，CI优于BEV

② 弱攻击，大学习速率BEV优于CI

③ 强攻击，BEV优于CI

④ BEV可对抗更多攻击者

➢小结

□**提出了**一种基于传输功率控制的拜占庭对抗方案，**增强了**FLOA的鲁棒性

□**推导了**拜占庭攻击者可以施加的最强攻击模式，**阐明了**FLOA对抗攻击的水平

□**推导了**不同功率控制下的收敛速率闭式表达式，**分析了**各方案的性能优势

➢相关研究成果

✓ **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. Best Effort Voting Power Control for Byzantine-resilient Federated Learning Over the Air[C] //*2022 IEEE International Conference on Communications (IEEE ICC 2022).* **(EI/ISTP国际会议；CCF C类；北交大A类; 对应学位论文第四章)**

✓ **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. BEV-SGD: Best Effort Voting SGD Against Byzantine Attacks for Analog-Aggregation-Based Federated Learning Over the Air[J]. *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 18946-18959, Oct, 2022. **(SCI期刊；2022年影响因子10.238；中科院一区；JCR一区；北交大A+；对应学位论文第四章)**

PART FOUR

总结与展望

总结与展望

➢主要工作与创新点

- **全面推导了**模拟聚合通信对FLOA影响的定量化描述表达式，**量化了**无线通信对联邦学习的影响，**奠定了**传算联合优化基础
- **提出了**一个基于收敛性分析的FLOA的传算联合优化基础框架，**节省了**通信带宽，**降低了**通信时延，**保护了**用户数据隐私，**缓解了**通信链路对联邦学习性能的负面影响，**提高了**学习准确率
- **提出了**基于1比特压缩感知的高效性FLOA方案，**进一步降低了**通信负载与通信时延，**实现了**快速高效的联邦学习
- **提出了**基于功率控制的FLOA的鲁棒性方案，从理论上**证明了**拜占庭攻击下学习算法的性能边界，**证明了**所提算法**提高了**FLOA的鲁棒性

➢研究展望

- ➢针对复杂场景的边缘智能研究（设备的异构性、数据的异质性、无中心拓扑、动态环境）
- ➢针对半实物实验平台的边缘智能研究

PART FIVE

研究成果

研究成果

序号	论文题目	本人排序	刊物名称/出版单位	论文等级	对应学位论文章节
1	Joint Optimization of Communications and Federated Learning Over the Air	1	IEEE Transactions on Wireless Communications	SCI检索；中科院一区；JCR一区；北交大A+	第2章
2	1-Bit Compressive Sensing for Efficient Federated Learning Over the Air	1	IEEE Transactions on Wireless Communications	SCI检索；中科院一区；JCR一区；北交大A+	第3章
3	BEV-SGD: Best Effort Voting SGD Against Byzantine Attacks for Analog-Aggregation-Based Federated Learning Over the Air	1	IEEE Internet of Things Journal	SCI检索；中科院一区；JCR一区；北交大A+	第4章
4	Joint Optimization for Federated Learning Over the Air	1	IEEE International Conference on Communications (ICC2022)	EI/ISTP检索；通信领域旗舰国际会议；CCF C类；北交大A类	第2章
5	Communication-efficient Federated Learning Through 1-Bit Compressive Sensing and Analog Aggregation	1	IEEE International Conference on Communications (ICC2021)	EI/ISTP检索；通信领域旗舰国际会议；CCF C类；北交大A类	第3章
6	Best Effort Voting Power Control for Byzantine-resilient Federated Learning Over the Air	1	IEEE International Conference on Communications (ICC2022)	EI/ISTP检索；通信领域旗舰国际会议；CCF C类；北交大A类	第4章

➢ 博士在读期间第一作者已发表论文

1. **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. Joint Optimization of Communications and Federated Learning Over the Air[J]. IEEE Transactions on Wireless Communications, vol. 21, no. 6, pp. 4434-4449, June 2022. **（SCI期刊；2022年影响因子8.346；中科院一区；JCR一区；北交大A+；对应学位论文第二章）**

2. **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. 1-Bit Compressive Sensing for Efficient Federated Learning Over the Air[J]. IEEE Transactions on Wireless Communications, oct, 2022, early access. **（SCI期刊；2022年影响因子8.346；中科院一区；JCR一区；北交大A+；对应学位论文第三章）**

3. **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. BEV-SGD: Best Effort Voting SGD Against Byzantine Attacks for Analog-Aggregation-Based Federated Learning Over the Air[J]. IEEE Internet of Things Journal, vol. 9, no. 19, pp. 18946-18959, Oct, 2022. **（SCI期刊；2022年影响因子10.238；中科院一区；JCR一区；北交大A+；对应学位论文第四章）**

4. Yan Huo, **Xin Fan**, Liran Ma, Xiuzhen Cheng, Zhi Tian, Dechang Chen. Secure communications in tiered 5G wireless networks with cooperative jamming[J]. IEEE Transactions on Wireless Communications, 2019, 18(6): 3265-3280. **（SCI期刊；2022年影响因子8.346；中科院一区；JCR一区；北交大A+）**

5. **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. Joint Optimization for Federated Learning Over the Air [C] //2022 IEEE International Conference on Communications (IEEE ICC 2022). **（EI/ISTP国际会议；CCF C类；北交大A类；对应学位论文第二章）**

6. **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. Communication-efficient Federated Learning Through 1-Bit Compressive Sensing and Analog Aggregation[C] //2021 IEEE International Conference on Communications (IEEE ICC 2021). **（EI/ISTP国际会议；CCF C类；北交大A类；对应学位论文第三章）**

7. **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. Best Effort Voting Power Control for Byzantine-resilient Federated Learning Over the Air[C] //2022 IEEE International Conference on Communications (IEEE ICC 2022). **（EI/ ISTP国际会议；CCF C类；北交大A类；对应学位论文第四章）**

8. **Xin Fan**, Yan Huo. Cooperative secure transmission against collusive eavesdroppers in Internet of Things[J]. International Journal of Distributed Sensor Networks, 2020, 16(6). **（SCI期刊；2022年影响因子1.938，中科院四区；JCR三区）**

9. **Xin Fan**, Yue Wang, Guangkai Li, Yan Huo, Zhi Tian. Hybrid Uplink-Downlink NOMA for Secure Coordinated Multi-Point Networks[C] //2021 IEEE International Conference on Communications (IEEE ICC 2021). **（EI/ISTP国际会议；CCF C类；北交大A类）**

10. **Xin Fan,** Yan Huo. Security Analysis of Cooperative Jamming in Internet of Things with Multiple Eavesdroppers[C]//2019 IEEE Global Communications Conference (GLOBECOM 2019). IEEE, 2019: 1-6. **（EI/ISTP国际会议；CCF C类；北交大A类）**

11. **Xin Fan,** Yan Huo. Blockchain Based Dynamic Spectrum Access of Non-Real-Time Data in Cyber-Physical-Social Systems[J]. IEEE Access, 2020, 8: 64486-64498. **（SCI期刊；2022年影响因子3.476；中科院三区；JCR二区）**

➢ 博士在读期间第一作者已投稿论文

1. **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. Robust Distributed Swarm Learning for Intelligent IoT [C], submitted to IEEE ICC 2023.
2. **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. Efficient Distributed Swarm Learning for Edge Computing [C], submitted to IEEE ICC 2023.
3. **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. CB-DSL: Communication-efficient and Byzantine-robust Distributed Swarm Learning on Non-i.i.d. Data[J]. arXiv preprint arXiv:2208.05578， 2022. Submitted to IEEE Transactions on Cognitive Communications and Networking, under review.
4. **Xin Fan**, Yan Huo. An Overview of Low latency for Wireless Communications: An Evolutionary Perspective[J] arXiv preprint arXiv:2107.03484, 2021.
5. **Xin Fan**, Yue Wang, Weishan Zhang, Yan Huo, Zhi Tian. GANFed: GAN-based Federated Learning with Non-IID Datasets[J]. Submitted to IEEE wireless communication letters, under review.

➢ 博士在读期间第一作者授权发明专利

1. **范新**, 霍炎, 荆涛. 基于区块链的频谱接入和管理方法, ZL 2019 1 0197190.3

PART SIX

参考文献

- [13] Y. Lin, S. Han, H. Mao, Y. Wang, and B. Dally, Deep gradient compression: Reducing the communication bandwidth for distributed training[C], International Conference on Learning Representations, 2018.
- [14] A. F. Aji and K. Heafield, Sparse communication for distributed gradient descent[J], arXiv preprint arXiv:1704.05021, 2017.
- [15] Y. Liu, K. Yuan, G. Wu, Z. Tian, and Q. Ling, Decentralized dynamic ADMM with quantized and censored communications[C], 2019 53rd Asilomar Conference on Signals, Systems, and Computers. IEEE, 2019, pp. 1496–1500.
- [16] F. Seide, H. Fu, J. Droppo, G. Li, and D. Yu, 1-bit stochastic gradient descent and its application to data-parallel distributed training of speech DNNs[C], Fifteenth Annual Conference of the International Speech Communication Association, 2014.
- [17] D. Alistarh, D. Grubic, J. Li, R. Tomioka, and M. Vojnovic, QSGD: Communication-efficient SGD via gradient quantization and encoding[J], Advances in Neural Information Processing Systems, 2017, pp. 1709–1720.
- [18] Y. Liu, W. Xu, G. Wu, Z. Tian, and Q. Ling, Communication-censored ADMM for decentralized consensus optimization[J], IEEE Transactions on Signal Processing, vol. 67, no. 10, pp. 2565–2579, 2019.
- [19] P. Xu, Z. Tian, Z. Zhang, and Y. Wang, Coke: Communication-censored kernel learning via random features[C], 2019 IEEE Data Science Workshop (DSW), 2019, pp. 32–36.
- [20] T. Chen, G. Giannakis, T. Sun, and W. Yin, LAG: Lazily aggregated gradient for communication-efficient distributed learning[J], Advances in Neural Information Processing Systems, 2018, pp. 5050–5060.
- [21] P. Xu, Z. Tian, and Y. Wang, An energy-efficient distributed average consensus scheme via infrequent communication[C], 2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP), 2018, pp. 648–652.
- [22] P. Xu, Y. Wang, X. Chen, and T. Zhi, Coke: Communication-censored kernel learning for decentralized non-parametric learning[J], arXiv preprint arXiv:2001.10133, 2020.
- [31] Y. Sun, S. Zhou, and D. Gündüz, Energy-aware analog aggregation for federated learning with redundant data[J], arXiv preprint arXiv:1911.00188, 2019.
- [32] K. Yang, T. Jiang, Y. Shi, and Z. Ding, Federated learning via over-the-air computation[J], IEEE Transactions on Wireless Communications, vol. 19, no. 3, pp. 2022–2035, 2020.
- [38] M. Kamp, L. Adilova, J. Sicking, F. Hüger, P. Schlicht, T. Wirtz, and S. Wrobel, Efficient decentralized deep learning by dynamic model averaging[C], Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Springer, 2018, pp. 393–409.
- [40] H. H. Yang, Z. Liu, T. Q. S. Quek and H. V. Poor, Scheduling Policies for Federated Learning in Wireless Networks[J], IEEE Transactions on Communications, vol. 68, no. 1, pp. 317-333, Jan. 2020.
- [41] Q. Zeng, Y. Du, K. K. Leung, and K. Huang, Energy-efficient radio resource allocation for federated edge learning[J], arXiv preprint arXiv:1907.06040, 2019.
- [42] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, and K. Chan, Adaptive federated learning in resource constrained edge computing systems[J], IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, pp. 1205–1221, 2019.
- [43] N. H. Tran, W. Bao, A. Zomaya, N. M. NH, and C. S. Hong, Federated learning over wireless networks: Optimization model design and analysis[C], IEEE INFOCOM 2019-IEEE Conference on Computer Communications. IEEE, 2019, pp. 1387–1395.
- [44] M. Chen, Z. Yang, W. Saad, C. Yin, H. V. Poor, and S. Cui, A joint learning and communications framework for federated learning over wireless networks[J], arXiv preprint arXiv:1909.07972, 2019.
- [59] X. Cao, G. Zhu, J. Xu and K. Huang, Optimal Power Control for Over-the-Air Computation[C], 2019 IEEE Global Communications Conference (GLOBECOM), 2019, pp. 1-6.
- [61] G. Zhu, Y. Wang and K. Huang, Broadband Analog Aggregation for Low-Latency Federated Edge Learning[J], IEEE Transactions on Wireless Communications, vol. 19, no. 1, pp. 491-506, Jan. 2020.

谢谢！

天道酬勤

◆**范新** Tel:15652955761 Email: fanxin@bjtu.edu.cn