北京林业大学
Beijing Forestry University

我的科研之路：从无线通信到人工智能

范新　信息学院




个人介绍及研究成果

北京林业大学 Beijing Forestry University

范新 信息学院讲师 计算机科学与技术学科/物联网与网络工程教研室

教育经历：获北京交通大学学士，硕士和博士学位，读博期间有两年九个月的海外联培经历。

项目经历：

- **主持**中央高校科研业务费项目1项和自然科学横向项目1项；
- 作为项目书**第二参与人**参与国家自然科学基金（NSFC）面上项目1项；
- 作为项目书**第二参与人**参与北京市自然科学基金面上项目1项；
- 作为项目书**第一参与人**参与自然科学横向项目1项；
- 作为主研人员之一参与NSFC面上项目1项，NSFC 重点项目1项，国家重点研发计划项目1项，基本科研业务费重大项目1项，美国自然科学基金（NSF）项目2项以及各类横向项目若干，**累计金额超8千万。**

研究方向：无线通信、机器学习、区块链、概率与统计、优化算法、安全与隐私等领域，主要科研方向为协作无线网络中的**物理层安全**和**边缘智能**技术研究。

学术成果：以**第一作者发表论文15篇**，其中**一区**SCI期刊**5篇**；发表论文谷歌学术**引用三百余次**，H指数10；**7篇**论文已投稿；授权发明**专利2项。**

学术兼职：IEEE MILCOM TPC member；**30多个**期刊会议审稿人，如J-SAC、TWC、TSP、TMC、TII等。

奖励荣誉：曾获**校级优秀博士学位论文(全校共18篇)**，校级硕士学位论文、校级三好研究生、优秀共产党员、研究生学业奖学金、国家公派奖学金、交控科技奖学金等荣誉。

目录

- 主要学术贡献
  - 无线通信
    - 物理层安全
  - 人工智能
    - 边缘智能

PART TWO

主要学术贡献一

学术贡献一

□物理层安全方面的研究

■针对第五代（5G）通信系统中的一些**特殊场景**，分别**创新性地提出了一系列基于协作干扰技术的物理层安全传输方案。重点解决**物理层安全领域中所涉及的**复杂网络场景协作干扰管理、多节点协作通信资源管理、窃听者共谋、窃听者信道状态未知**等关键性且未有实质性突破的问题。

■为物理层安全在特殊场景的应用**提供了方案设计、性能分析、优化算法等**多方面的理论支撑。

□研究成果

■以第一作者在多个学术期刊和国际会议上**发表5篇文章**，包括顶级期刊*IEEE Transactions on Wireless Communications（IEEE TWC）*，通信领域旗舰国际会议*IEEE International Conference on Communications (IEEE ICC)*和*IEEE Global Communications Conference (IEEE GLOBECOM)*等

物理层安全背景

物理层安全评价指标：

- 安全速率：$C_S = \begin{cases} C_B - C_E, & C_B > C_E \\ 0, & C_B \le C_E \end{cases}$

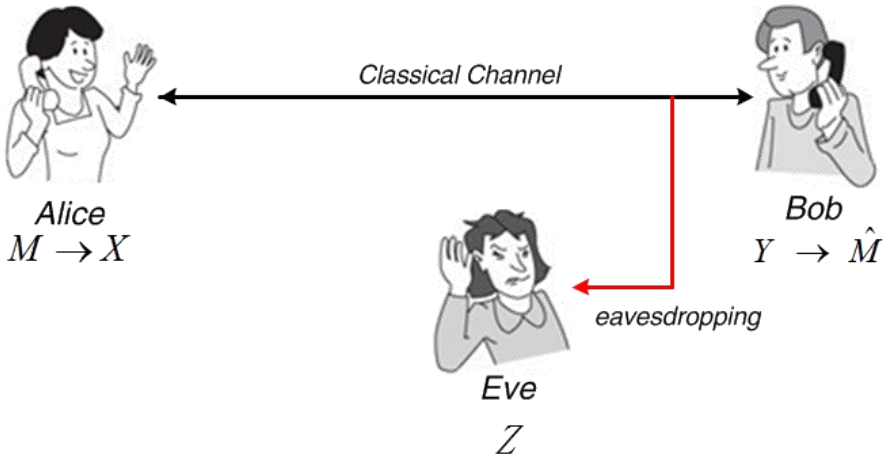
其中，$C_B = \log_2(1+\gamma_B)$，$C_E = \log_2(1+\gamma_E)$

■ 为什么研究物理层安全?

- ◆ 无线网络广播特性，用户隐私极易泄漏；
- ◆ 异构网络及IoT应用的普及，存在着大量的“低端”设备；
- ◆ 具有超级计算能力的窃听者使得传统基于密码学的安全策略未必有效。

■ 什么是物理层安全?

- ◆ **可靠性**：合法接收者能够无差错地接收信号，即$\mathbf{Pr}(\widehat{\boldsymbol{M}} = \boldsymbol{M}) \to \mathbf{1}$
- ◆ **安全性**：窃听者无法接收或正确解码信号（基于无线信道特征），即$\boldsymbol{I}(\boldsymbol{Z}, \boldsymbol{M}) \to \mathbf{0}$



物理层安全为传统基于密码学安全策略提供一种有益的补充

物理层安全背景

- **物理层安全研究现状**
  - 信道策略：基于物理信道特征生成的密钥实现安全传输；
  - 编码策略：使用扩频或安全编码技术实现抗干扰与防窃听；
  - 信号策略：在不影响合法接收者接收质量的前提下，降低窃听者的接收质量，如波束成形，人工噪声。
- **存在的问题及挑战**
  - 大多基于窃听者信道状态信息（CSI）已知的情况展开研究

不准确的信道估计 ⇒ **信道状态信息可能会有误差**

如果窃听者被动窃听 ⇒ **得不到任何窃听者的信道信息**

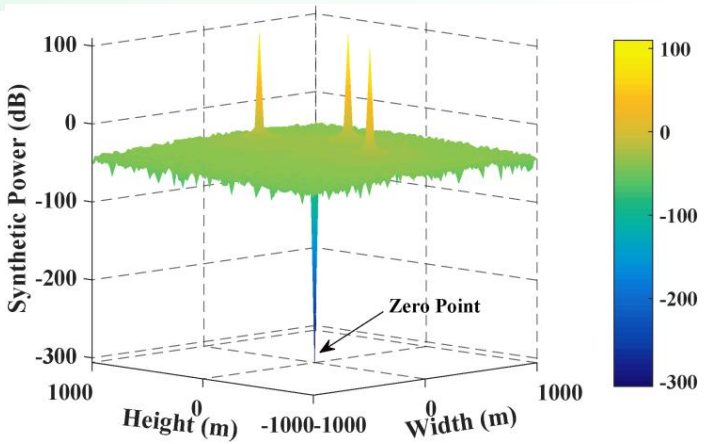
如何设计窃听者CSI未知的物理层安全策略?

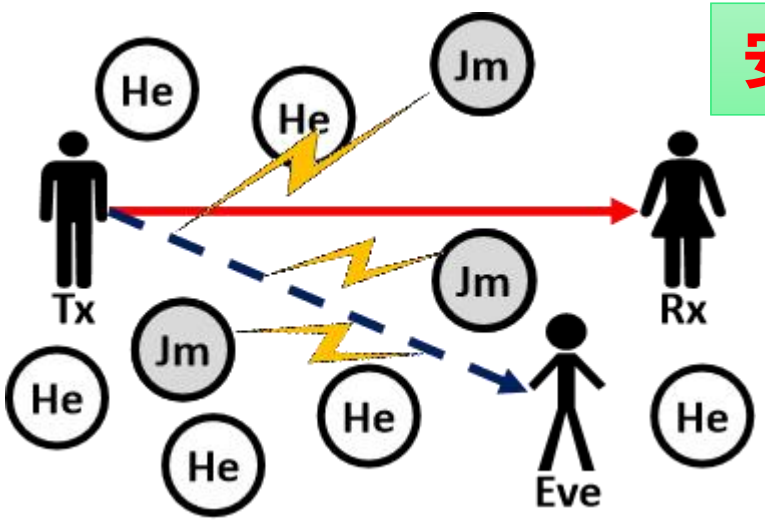
人生第一篇论文

北京林业大学 Beijing Forestry University

■不知道窃听者信道状态如何实现安全传输?

- ■**空间功率合成技术**实现网络内干扰信号的全覆盖
- ■电磁波在空间中的叠加原理
- ■合法用户处受到的干扰最小，而其它区域都有很强的干扰





安全目标：降低窃听者SINR，同时不影响合法接收者的 SINR

- **协作干扰策略** — 电磁信号空间功率合成 — **存在性**、**唯一性**
- **最优功率分配** — 最恶劣位置 — **优化问题建模**、**波浪之字搜索求解**

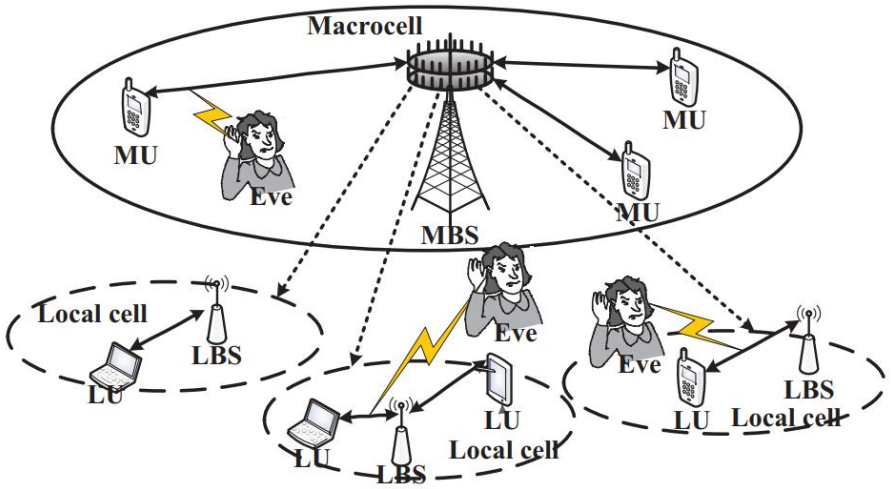
✓ **Xin Fan**, Liang Huang, Yan Huo, Chunqiang Hu, Yuqi Tian, Jin Qian. Space Power Synthesis-Based Cooperative Jamming for Unknown Channel State Information [C]// International Conference on Wireless Algorithms, Systems, and Applications (WASA 2017). Springer, Cham, 2017:483-495. **(EI 国际会议，CCF C 类)**

✓ Huang L, **Fan X**, Huo Y, et al. A Novel Cooperative Jamming Scheme for Wireless Social Networks Without Known CSI[J]. IEEE Access, 2017, PP(99):1-1. **(导师一本人二，SCI 2区)**

物理层安全代表作

■ 面向5G分层异构网络无线安全传输方法研究

- ◆双层异构网络、大规模天线阵列使能的宏蜂窝、NOMA使能的微蜂窝、信道估计误差
- ◆多层网络资源的管理、多节点发送信号的控制、干扰控制等
- ◆面向宏用户的安全传输方案、面向微用户的安全传输方案、宏-微用户联合安全传输方案
- ◆多种优化方案，并解决了一系列非凸的优化问题（酉矩阵、对角矩阵、泰勒展开、差分近似、欧拉界、松弛因子放缩、秩一约束、二阶锥、空间变换、连续凸逼近等等）



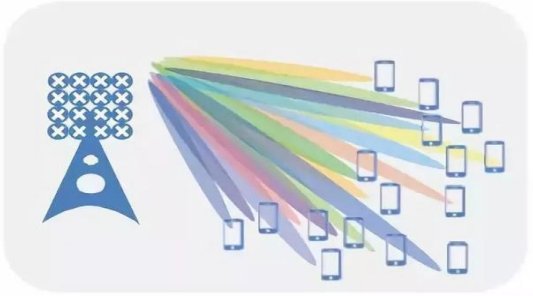
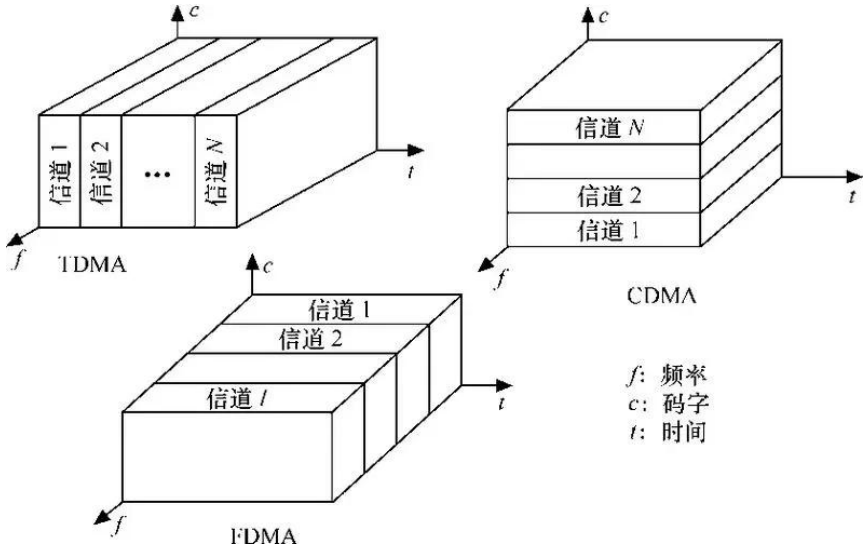


图1　3D-MIMO系统原理

物理层安全评价指标：

- 安全速率：$C_S = \begin{cases} C_B - C_E, & C_B > C_E \\ 0, & C_B \le C_E \end{cases}$

其中，$C_B = \log_2(1+\gamma_B)$，$C_E = \log_2(1+\gamma_E)$



✓ 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. **（导师一作本人二作，SCI期刊，中科院一区，JCR Q1区）**

物理层安全其它作品

- **Xin Fan**, Yan Huo. Security Analysis of Cooperative Jamming in Internet of Things with Multiple Eavesdroppers[C]//2019 IEEE Global Communications Conference (GLOBECOM). IEEE, 2019: 1-6.**（EI&ISTP 国际会议, 通信领域旗舰会议，CCF C 类）**
- **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; 中信所四区，中科院四区，JCR Q3 区）**
  - **多个窃听者共谋的问题**
  - 共谋的窃听者信号建模
  - 协作干扰技术对抗共谋的窃听者
  - 统计信号分析，推导了安全中断概率
  - 功率分配优化方案进一步提升安全性能
- **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), 1-6. IEEE, 2021: 1-6.**（EI&ISTP 国际会议, 通信领域旗舰会议， CCF C 类；）**
  - **基于NOMA的多节点多基站协作安全传输问题**
  - **协同多点传输（Coordinated Multi-Point Networks，CoMP）网络**
  - 混合上下行NOMA技术、网络编码技术、多点协作安全传输方案
  - 统计信号分析，推导了安全中断概率

PART TWO

主要学术贡献二

学术贡献二

北京林业大学 Beijing Forestry University

口边缘智能方面的研究

■在边缘智能场景中，分布式设备海量存在的情况下，针对联邦学习系统通信效率低下、隐私泄露、拜占庭攻击等问题，**创新性地提出一种面向联邦学习的传算联合优化框架**。

■**解决了**无线通信和联邦学习之间的关系**无法定量化描述的问题**，**突破了**无线通信和联邦学习**无法联合优化的瓶颈**。为**通信高效的**、**鲁棒性增强的**、**隐私保护的**联邦学习提供了基础理论与方法支撑。

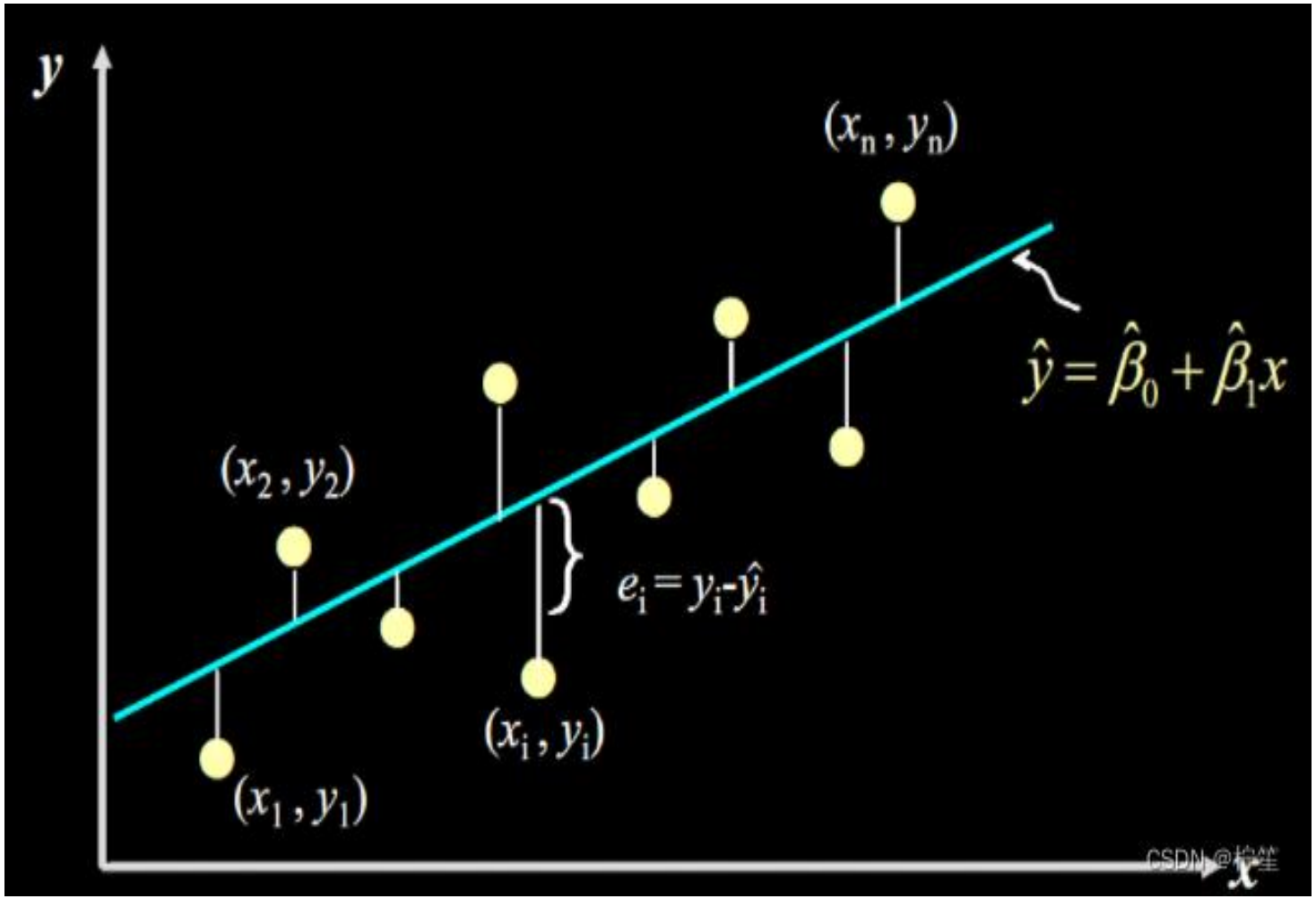
口研究成果

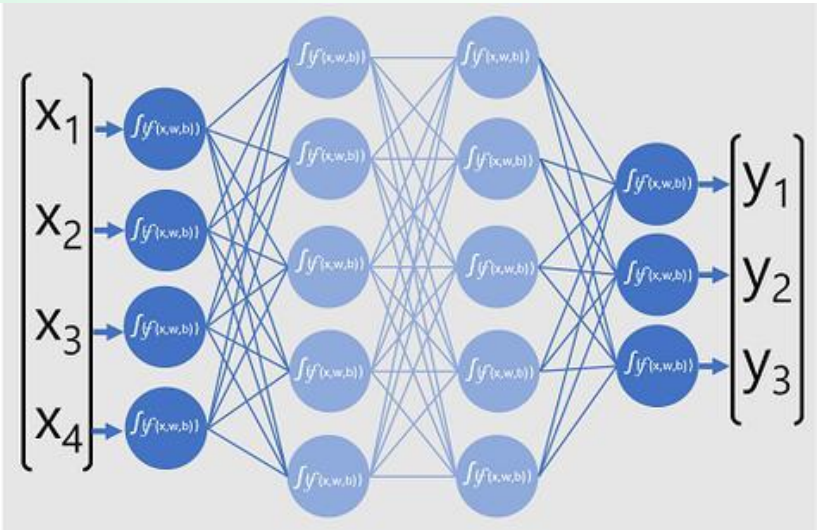
■以第一作者在多个学术期刊和国际会议上**发表6篇文章**，包括顶级期刊*IEEE Transactions on Wireless Communications*（*IEEE TWC*）***2篇***，*IEEE Internet of Things Journal*（*IEEE IoT-J*）***1篇***，和通信领域旗舰国际会议*IEEE International Conference on Communications (IEEE ICC)****3篇***。

联邦学习背景

北京林业大学 Beijing Forestry University

➢ 机器学习





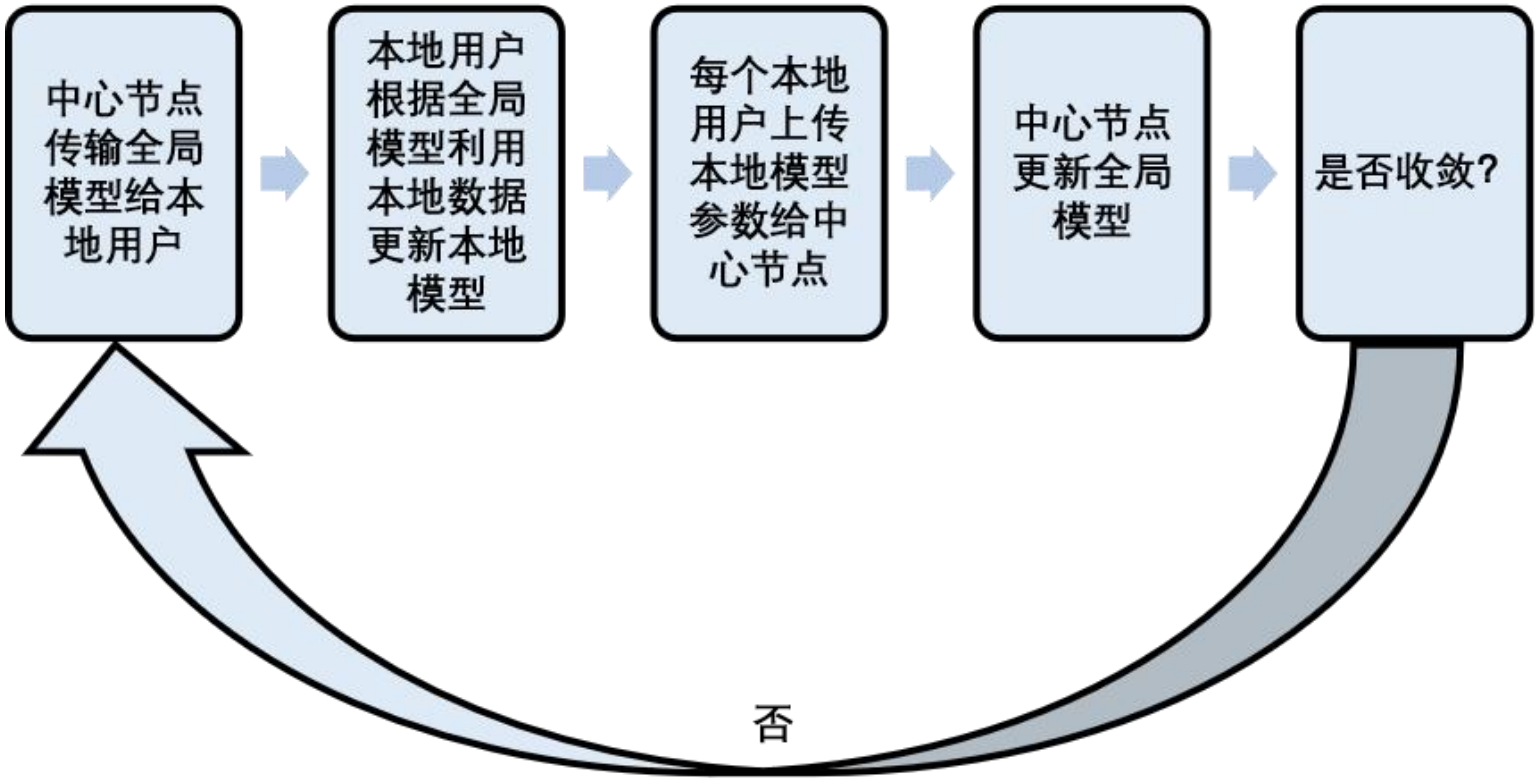
输入数据 → 模型 → 输出结果

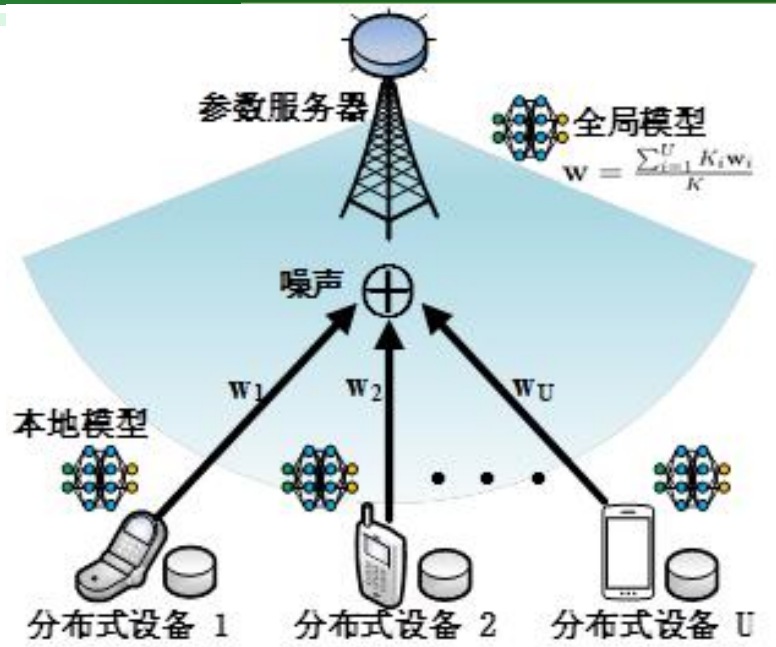
↓

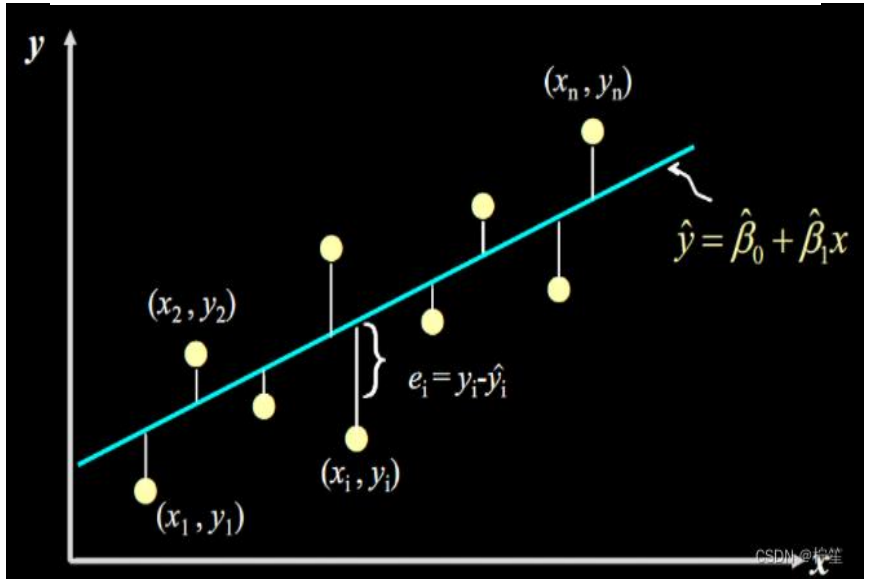
模型是用参数表征

联邦学习背景

➢ 联邦学习执行过程

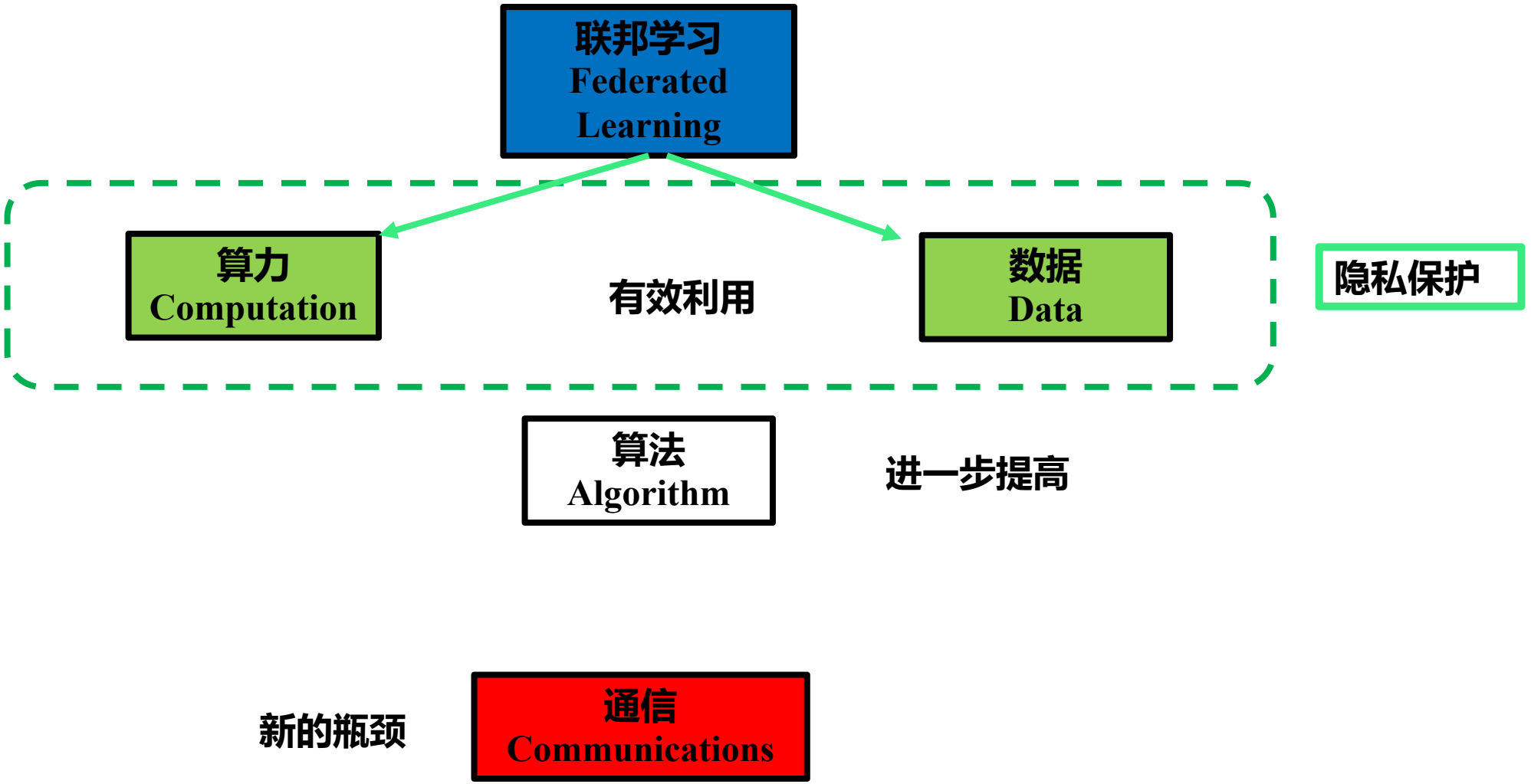






联邦学习背景

机器学习三大核心要素



联邦学习背景

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

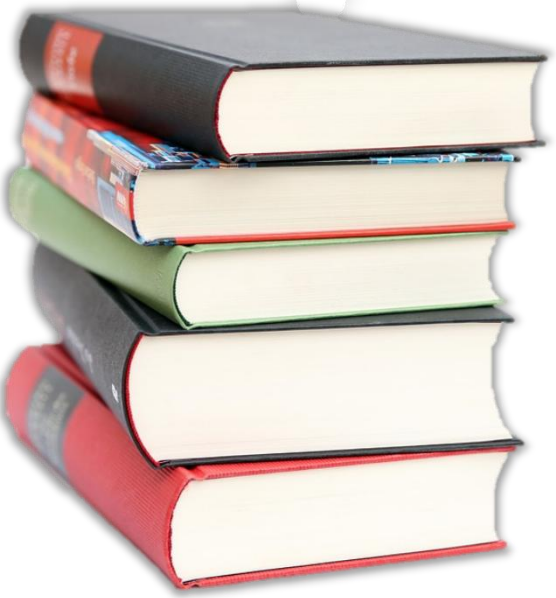
复杂场景

通信

新的瓶颈

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

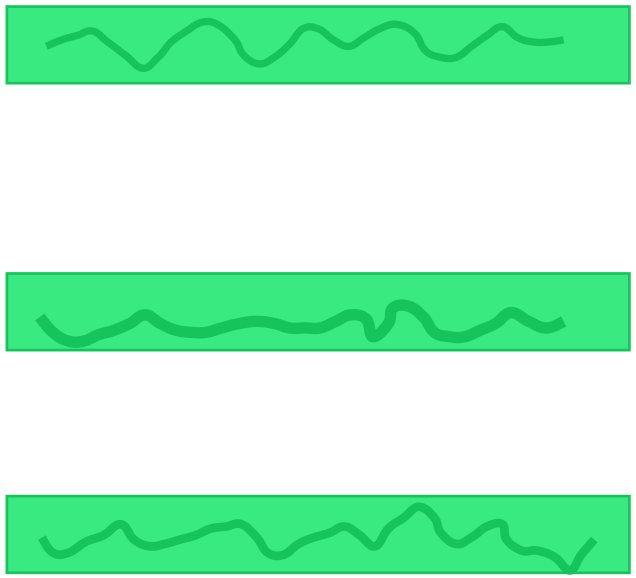
- 非编码的线性模拟调制
- 多设备同时同频同空间传输
- 电磁波叠加，实现和函数功能
- 在接收端直接得到聚合值

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

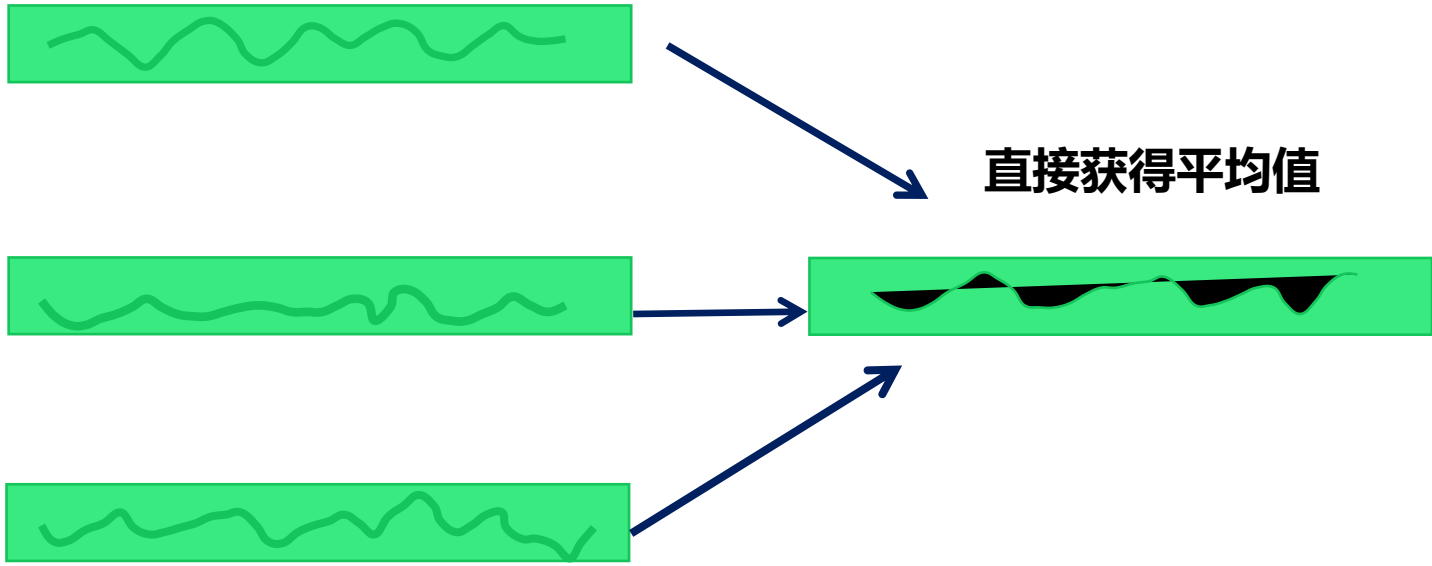
如何传?

数字通信

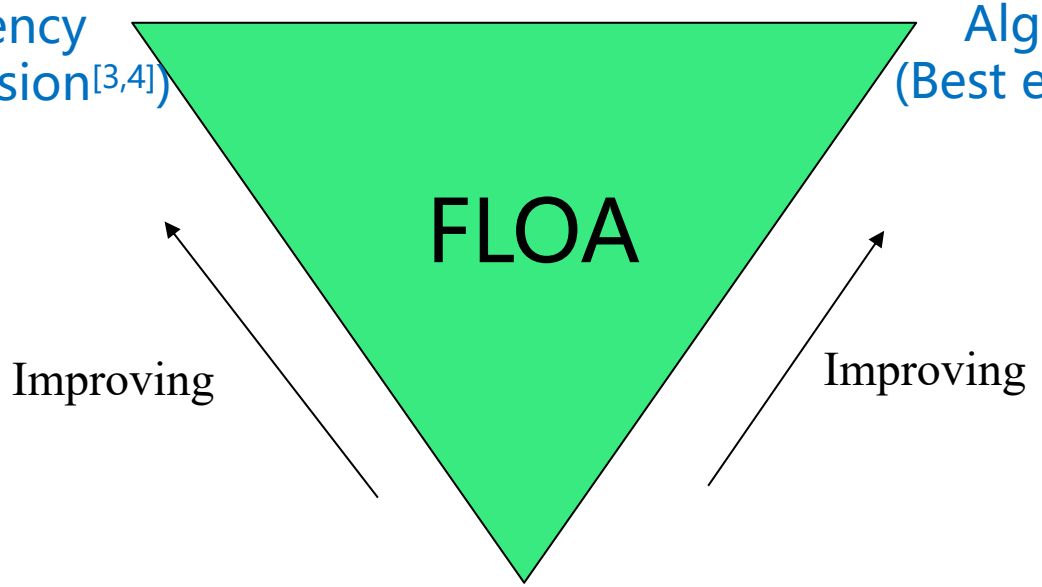


单独解调

模拟聚合通信



学术贡献二

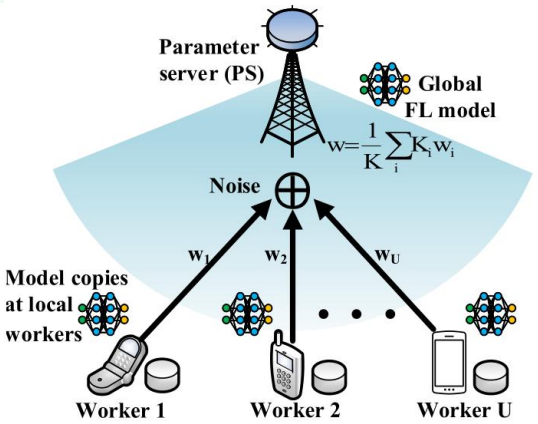


1. **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. Joint Optimization for Federated Learning Over the Air [C] //2022 IEEE International Conference on Communications (IEEE ICC 2022).
2. **Xin Fan**, Yue Wang, Yan Huo, Zhi Tian. Joint Optimization of Communications and Federated Learning Over the Air[J]. IEEE Transactions on Wireless Communications, vol. 21, no. 6, pp. 4434-4449, June 2022.
3. **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).
4. **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.
5. **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).
6. **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.

FLOA联合优化框架研究

❑ Federated learning (FL)

- Local devices (workers)
  - Receive $\mathbf{w} = [w^1, \ldots, w^D] \in \mathcal{R}^D$ from a parameter server (PS)
  - Train to get the updates (local parameters, $\mathbf{w}_i$)
  - Send $\mathbf{w}_i$ to the PS
- PS
  - Receive $\mathbf{w}_i$ and average them to obtain the sharing model $\mathbf{w} = \frac{\sum_{i=1}^{U} K_i \mathbf{w}_i}{K}$
  - Broadcast $\mathbf{w}$ to local workers



Unbiased estimation

❑ Federated learning over the air (FLOA)

- Local workers
  - Send $\mathbf{w}_{i,t}$ with the power control policy $\mathbf{p}_{i,t} = [p_{i,t}^1, \ldots, p_{i,t}^d, \ldots, p_{i,t}^D]$ where $p_{i,t}^d = \frac{\beta_{i,t}^d K_i b_t^d}{h_{i,t}^d}$
- PS
  - Receive $\mathbf{y}_t = \sum_{i=1}^{U} \mathbf{p}_{i,t} \odot \mathbf{w}_{i,t} \odot \mathbf{h}_{i,t} + \mathbf{z}_t$
  - Estimate $\mathbf{w}_t$ via a post-processing operation as

$$\begin{aligned}\mathbf{w}_t &= \left(\sum_{i=1}^{U} K_i \boldsymbol{\beta}_{i,t} \odot \mathbf{b}_t\right)^{\odot -1} \odot \mathbf{y}_t \\ &= \left(\sum_{i=1}^{U} K_i \boldsymbol{\beta}_{i,t}\right)^{\odot -1} \sum_{i=1}^{U} K_i \boldsymbol{\beta}_{i,t} \odot \mathbf{w}_{i,t} + \left(\sum_{i=1}^{U} K_i \boldsymbol{\beta}_{i,t} \odot \boldsymbol{b}_t\right)^{\odot -1} \odot \mathbf{z}_t\end{aligned}$$

FLOA联合优化框架研究

Convergence analysis

- Convergence with assumption of strongly convex

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

Guideline for optimization ← Performance gap ← Imposes a convergence condition

- Convergence with assumption of non-convex

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

$\triangle_t^{NC}$ → Performance gap → Guideline for optimization

- Convergence with SGD

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

Guideline for optimization ← Performance gap ← Imposes a convergence condition

FLOA联合优化框架研究

❑ Optimization problem

Minimizing performance gap

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

Entry-wise optimization

Problem P1

$$\min_{\{b_t, \beta_{i,t}\}_{i=1}^U} R_t$$

Layer paradox

$$\text{s.t.} \left| \frac{\beta_{i,t} K_i b_t}{h_{i,t}} w_{i,t} \right|^2 \leq P_i^{\max},$$
$$\beta_{i,t} \in \{0,1\}, i \in \{1,2,...,U\}$$

Assumption (bounded local gradient) $|w_{t-1} - w_{i,t}| \leq \eta$

Problem P2

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

❑ Solution

Tight search space

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

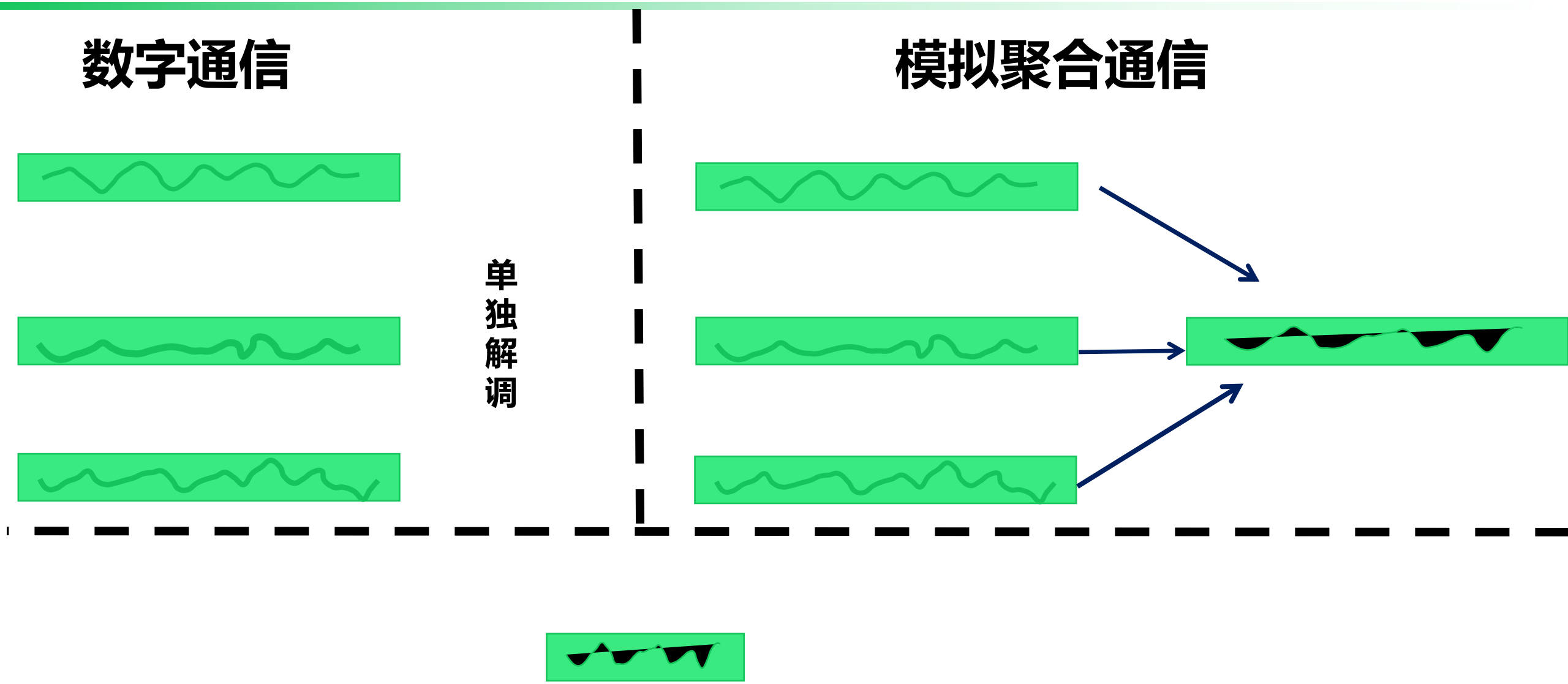
Discrete Programming

Problem P3 $\min_{(b_t, \boldsymbol{\beta}_t) \in \mathcal{S}} R_t = R_t(b_t, \boldsymbol{\beta}_t)$

Computation Complexity

Reduced to $\mathcal{O}(U)$ proportional to the number of local devices

高效性FLOA



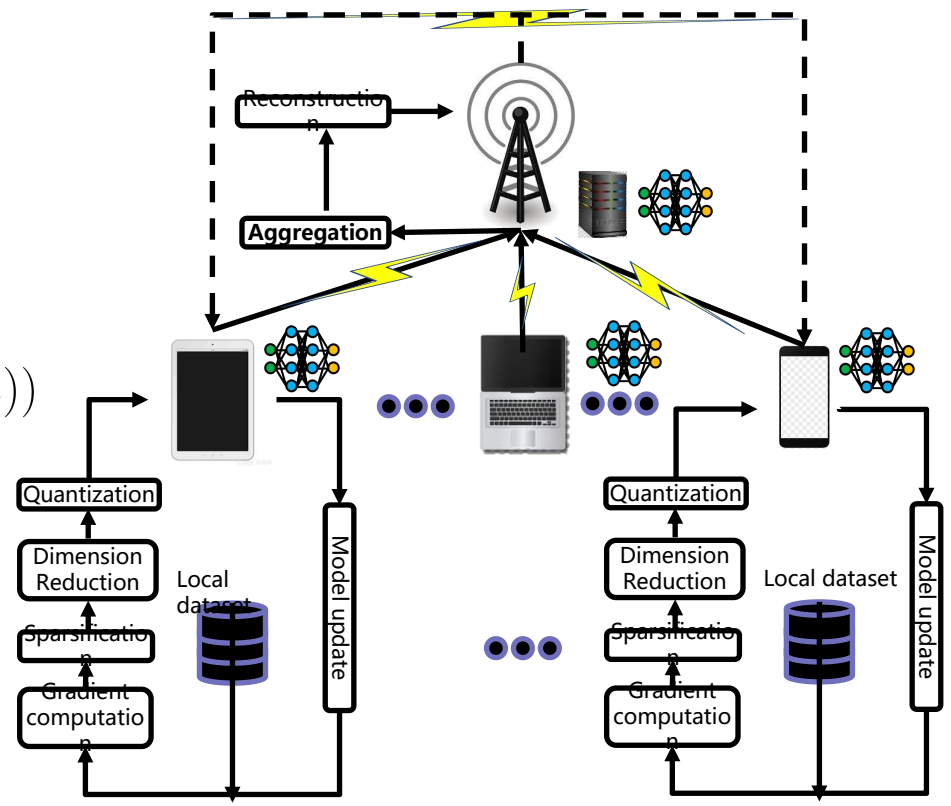
高效性FLOA

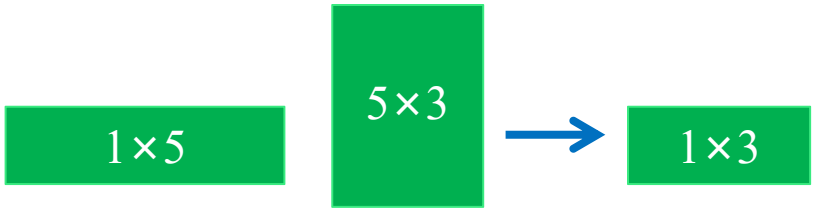
❑ One-bit compressive sensing and analog aggregation transmission（OBCSAA）

- Sparsification
  - Top-k or other methods
- Dimension reduction
  - Random Gaussian matrix $\mathbf{\Phi} \in \mathbb{R}^{S\times D}(S \ll D)$
- Quantization
  - The overall operation $\mathcal{C}(\mathbf{g}_{i,t}) = \mathtt{sign}(\mathbf{\Phi}\mathtt{sparse}_{\kappa}(\mathbf{g}_{i,t}))$
- Analog aggregation transmission
  - Power control $p_{i,t} = \dfrac{\beta_{i,t}K_i b_t}{h_{i,t}}$
- The received signal at PS

$$\mathbf{y}_t = \sum_{i=1}^{U} K_i b_t \beta_{i,t} \mathcal{C}(\mathbf{g}_{i,t}) + \mathbf{z}_t$$

- Reconstruction
  - Reconstruct the sparse averaged gradient





高效性FLOA

- Aggregation errors
  - Sparsification, Quantization, Reconstruction and Channel noise
- Convergence analysis
  - The convergence in the non-convex case

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

$T \to \infty$ → Performance gap → Guideline for optimization

  - **To mitigate aggregation errors, minimize B_t**
  - Optimization problem

$$\min_{b_t,\boldsymbol{\beta}_t} \quad B_t$$
$$\text{s.t.} \quad \frac{\beta_{i,t}^2 K_i^2 b_t^2}{h_{i,t}^2} \leq P_i^{\text{Max}},$$
$$\beta_{i,t} \in \{0,1\}, i \in \{1,2,...,U\}$$

→ Mixed integer programming that is non-convex

高效性FLOA

- Mixed integer programming (MIP)
  - The coupling of b_t and $\boldsymbol{\beta}_t$
  - Nonlinear and Non-convex

$$\min_{b_t,\boldsymbol{\beta}_t} \quad B_t$$
$$\text{s.t.} \quad \frac{\beta_{i,t}^2 K_i^2 b_t^2}{h_{i,t}^2} \leq P_i^{\text{Max}},$$
$$\beta_{i,t} \in \{0,1\}, i \in \{1,2,...,U\}$$

- Optimal Solution via Discrete Programming
  - Given $\boldsymbol{\beta}_t = [\beta_{1,t}, \beta_{2,t}, ..., \beta_{U,t}]$, the problem is convex.
  - Applicable for a small number of local workers, e.g., U ≤ 10
  - The complexity is $\mathcal{O}(2^U)$
- ADMM-based Suboptimal Solution
  - Decomposition
    - Decompose the hard combinatorial problem into U parallel smaller convex problems.
    - Iteratively solve them.
  - The complexity is $\mathcal{O}(U)$
  - Applicable for large-scale scenarios

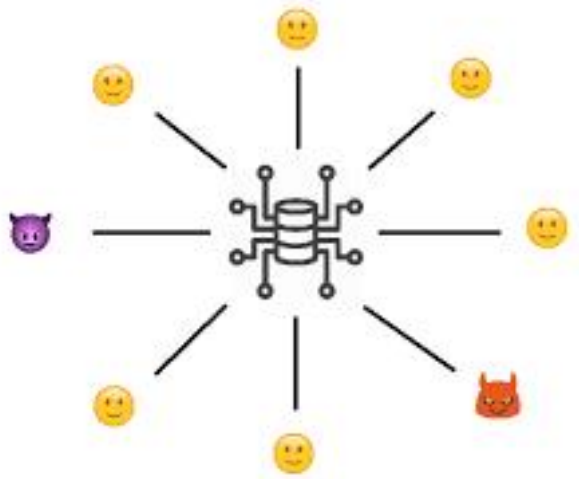
鲁棒性FLOA

❑ Challenges

- The individual local updates are unavailable
- Existing screening methods (such as geometric median, coordinate-wise median/trimmed mean) cannot work

❑ Contributions

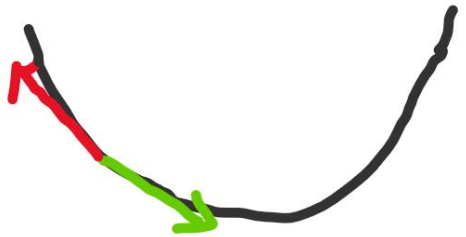
- Power control policy
  - Best effort voting (BEV)
- Convergence analysis
  - Strongest attack
  - Existing power control policy
  - Our BEV



鲁棒性FLOA

- FL over the air
  - N out of U workers are Byzantine attackers and $M = U\text{-}N$ normal workers

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



Voting: [1 1 1 1 -5]→-1

- The existing channel inversion (CI) power control
  - The power allocation factor

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

  - When N=0, then $\mathbf{y}_t = \sum_{m=1}^{U} b_0\tilde{\mathbf{g}}_{m,t} + \mathbf{z}_t \longrightarrow \hat{\mathbf{g}} = \frac{\mathbf{y}_t}{Ub_0} = \frac{\sum_{m=1}^{U}\tilde{\mathbf{g}}_{m,t}}{U} + \frac{\mathbf{z}_t}{Ub_0} \Longleftrightarrow \mathbf{g} = \frac{\sum_{m=1}^{U}\mathbf{g}_{m,t}}{U}$

Unbiased estimation **Error-free case**

- Our best effort voting SGD (BEV- SGD)
  - Transmission with the maximum power.
  - Byzantine attackers can send anything under the power constraints.

Voting: [3 2 1 4 -5]→5

鲁棒性FLOA

Beijing Forestry University

Tolerable maximum number of attackers

- The convergence of SGD with CI transmission

$$\mathbb{E}[\sum_{t=1}^{T}\frac{1}{T}\|\mathbf{g}_t\|^2)] \leq \frac{1}{\sqrt{T}}\left(\frac{2L\Omega_{CI}}{\omega_{CI}^2\bar{\alpha}}(F(\mathbf{w}_0)-F(\mathbf{w}^*))+\bar{\alpha}\left(\delta^2+\frac{1}{\Omega_{CI}}\epsilon^2 z^2\right)\right)$$

$\frac{U}{1+\sqrt{\pi U}}$

- The convergence of SGD with BEV transmission

$$\mathbb{E}[\sum_{t=1}^{T}\frac{1}{T}\|\mathbf{g}_t\|^2)] \leq \frac{1}{\sqrt{T}}\left(\frac{2L\Omega_{BEV}}{\bar{\alpha}\omega_{BEV}^2}(F(\mathbf{w}_0)-F(\mathbf{w}^*))+\bar{\alpha}\left(\delta^2+\frac{1}{\Omega_{BEV}}\epsilon^2 z^2\right)\right)$$

$\frac{U}{2}$

- For large learning rate
  - Dominated by $O(\frac{1}{\Omega\sqrt{T}})$ $\quad \Omega_{BEV} > \Omega_{CI}$ **BEV is better than CI**
- For small learning rate
  - Dominated by $O(\frac{\Omega}{\omega^2\sqrt{T}})$ **Depends on the specific parameters**
- No attackers for small learning rate
  - CI has $\omega_{CI}^2 = \Omega_{CI}$
    - Dominated by $O(\frac{1}{\sqrt{T}})$ → **Error-free case** **CI is better than BEV**
  - BEV has $\omega_{BEV}^2 \leq \Omega_{BEV}$
    - Dominated by $O(\frac{\Omega_{BEV}}{\omega_{BEV}^2\sqrt{T}})$

学术贡献二总结

➢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

及时当勉励

人类文明的进程是由伟人推动的，
还是由人民推动的？

谢谢！

天道酬勤

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