arXiv:2302.01772v1 [cs.LG] 3 Feb 2023

通过混合进行修复 异质性下的最优拜占庭机器学习：一种方法

Youssef Allouah[†*] **Sadegh Farhadkhani**[†] **Rachid Guerraoui**[†]
Nirupam Gupta[†] **Rafa¨el Pinot**[†] **John Stephan**[†]

摘要

拜占庭机器学习（ML）旨在确保分布式学习算法能够抵御行为异常（或拜占庭）机器的影响。尽管这一问题受到了广泛关注，但以往研究往往假设机器持有的数据是同质的，而这在实际场景中鲜少成立。数据异质性 使拜占庭机器学习更具挑战性，因为拜占庭机器很难与非拜占庭异常值区分开来。目前已有少数解决方案试图应对这一问题，但其概率保证并非最优，实际表现也不佳。

本文弥补了理论上的差距，实现了最优性，并取得了良好的实证结果。事实上，我们展示了如何通过一种强大的机制，自动将现有的（同质）拜占庭机器学习解决方案适配到异质设定中；我们将这一机制称为最近邻混合 （NNM）。该机制能够提升任何标准的鲁棒分布式梯度下降变体，使其在异质性条件下实现最优的拜占庭鲁棒性。将 NNM 应用于分布式随机 重球法（一种实用的分布式梯度下降替代方法），也能获得类似的保证（在期望意义下）。我们的实证结果显著优于当前最先进的拜占庭机器学习解决方案。

1 引言

分布式机器学习（ML），即将训练过程分散到多台机器（或工作节点）上，对开发具有高准确率保证的大型复杂模型至关重要 [1, 28, 24]。在如今的标准主从式架构中，分布式机器学习本质上是指工作节点在主机器（又称服务器）的协助下共享各自的本地操作，从而计算出准确的全局模型。尽管分布式机器学习日益普及，但可以说它十分脆弱，尚未做好现实世界部署的准备。尤其是，少数行为不端（又称拜占庭 [30]）的工作节点就可能严重损害标准分布式机器学习算法（如分布式梯度下降（D-GD） [6], ）的效能：它们会向服务器发送错误信息，例如参见 [5, 47]。这类行为可能由软件和硬件故障、投毒数据，或控制系统部分组件的恶意攻击者引起。此外，如果由此产生的机器学习模型被部署在医学等敏感数据应用领域，这种脆弱性可能导致严重的社会后果。

近年来，分布式机器学习（或拜占庭机器学习）中的拜占庭鲁棒性问题受到了广泛关注 [7, 11, 48, 3, 13, 25, 26, 17]。其核心是设计一种分布式算法，即使存在一部分拜占庭工作节点，也能输出准确的模型。在标准的主从式 架构中，常见做法是让服务器执行鲁棒聚合，合并工作节点发送的信息并剔除离群值。然而，大多数先前研究都依赖于同质性这一强假设同质性；也就是说，假设工作节点在训练过程中采样的数据服从相同的分布。尽管这一假设在集中式环境中或许合理 [8], ，但在分布式环境中并不切实际 [24]。事实上，由于每个工作节点仅持有整个训练数据集的一小部分，各工作节点上的数据样本通常具有异质性，未必能准确代表整体数据。因此，工作节点数据样本之间的差异可能掩盖拜占庭机器偏离既定算法的破坏性行为，使得异质性条件下的拜占庭机器学习问题远比同质条件下的对应问题更具挑战性 [13, 26]。

近期研究表明，在存在拜占庭工作节点的情况下，工作节点数据的异质性不可避免地会使任何分布式机器学习算法都无法输出任意精确的模型 [10, 34]。更具体地说，在光滑损失函数的情形下，拜占庭机器学习解决方案只能输出近似驻点，其误差下界为拜占庭工作节点所占比例乘以工作节点梯度的最大离散程度（源于

[†]洛桑联邦理工学院（EPFL），瑞士。作者姓名按字母顺序排列。 [*]通讯请联系：<youssef.allouah@epfl.ch>。

数据异质性） [26]。尽管已有少数尝试 [20, 13,26], , 但迄今为止，还没有任何解决方案能够确定性地达到上述下界，即实现最优拜占庭鲁棒性。目前最好的解决方案 [26] 都是随机化的，只能在期望 意义下达到该下界（见第 2 节）。

主要结果。 我们弥合了理论差距，实现了异质性下的最优拜占庭鲁棒性。具体而言，我们展示了如何将现有的同质拜占庭机器学习解决方案自动适配到异质设定，同时确保其达到最优。我们通过最近邻混合（NNM）实现这一点：这是一种预聚合方法，它将每个输入与其最近邻中的一部分取平均。我们证明，使用 NNM 与标准鲁棒聚合规则的复合来增强分布式梯度下降，可直接得到首个在异质性下实现最优鲁棒性的拜占庭机器学习解决方案。只要拜占庭工作节点不到一半，我们的保证就成立，而这一条件是最优的。

技术贡献。 为证明我们的保证，我们提出了一种名为（f，κ）-鲁棒性的新颖鲁棒性准则。该概念量化了聚合规则在f 个工作节点中有 n 个为拜占庭节点时，估计诚实工作者输入平均值的能力。至关重要的是，我们的准则刻画了一类聚合规则（其中$\kappa = \mathcal{O}(f/n)$），这类规则能够赋予分布式梯度下降在异质性下的最优拜占庭鲁棒性。尽管许多著名的聚合规则（例如几何中位数 [43], 逐坐标中位数 [48], 和*Krum* [7]）满足（f，κ）-鲁棒性，但它们的鲁棒性未达最优，因为其 κ 为 $\Theta(1)$。我们的主要技术贡献在于证明 NNM 克服了这一不足。具体而言，我们证明 NNM 能以确定性方式将诚实输入的方差降低 $\mathcal{O}(f/n)$ 倍，同时充分限制它们相对于真实均值的漂移。因此，我们证明，将（f，$\mathcal{O}(1)$）-鲁棒聚合规则与 NNM 复合，可使更大一类（f，$\mathcal{O}(1)$）-鲁棒聚合规则赋予分布式梯度下降最优的拜占庭鲁棒性。

实证评估。 尽管我们证明了经 NNM 增强的分布式梯度下降已达到最优，但工作节点仍需在每一步计算其本地损失函数的完整梯度，并且可能陷入鞍点 [12, 8]。我们进一步证明，将 NNM 应用于分布式梯度下降的一种随机变体，即分布式随机重球法（D-SHB） [39], , 在期望意义下达到了下界[1]。我们通过在 MNIST 和 CIFAR-10 等标准分类任务上进行测试，实证表明该方案显著优于当前最先进的方法。简言之，我们的方法为异质性环境下的拜占庭弹性机器学习提供了一种模块化实践路径：先用 NNM 改进现有方案，再将其与 D-SHB 配合使用。

[1]该期望是针对数据子采样所带来的随机性而言的，而 [26] 还包含其他随机性来源，这些来源会妨碍实际性能。详情请参见第5.2节。

论文结构。 第 2 节正式介绍拜占庭机器学习问题，并讨论相关工作。第 3 节介绍鲁棒分布式梯度下降变体的分析框架。第 4 节介绍 NNM，这是我们使现有方法达到最优的解决方案。第 5 节介绍我们方法的一种实用随机扩展。第 6 节介绍我们的实验结果。所有证明均放在附录8–13中。

2 背景与相关工作

我们考虑一种主从式分布式架构，其中包含 n个工作节点 $w_1, \ldots, w_n$ 和一台中心服务器。工作节点持有本地数据集 $\mathcal{D}_1, \ldots, \mathcal{D}_n$，每个数据集由输入空间 $\mathcal{Z}$中的 m 个数据点组成。具体而言，对于任意 $i \in [n]$，$\mathcal{D}_i := \{z_1^{(i)}, \ldots, z_m^{(i)}\} \subset \mathcal{Z}^m$。对于由向量 $\theta \in \mathbb{R}^d$ 参数化的给定模型，每个工作节点 w_i 都有一个损失函数

$$\mathcal{L}_i(\theta) := \frac{1}{m} \sum_{k=1}^{m} \ell(\theta, z_k^{(i)}),$$

其中 $\ell : \mathbb{R}^d \times \mathcal{Z} \to \mathbb{R}$ 是逐点损失函数，我们假设它关于 θ可微。此外，我们假设每个损失函数 $\mathcal{L}_i$ 都是 L-光滑的；也就是说，对于所有 $\theta, \theta' \in \mathbb{R}^d$，

$$\|\nabla \mathcal{L}_i(\theta) - \nabla \mathcal{L}_i(\theta')\| \leq L \|\theta - \theta'\| .$$

无拜占庭节点情形下的目标。 当所有工作节点都诚实时，即它们正确遵循规定的算法，服务器的目标是计算全局损失函数[2] $\mathcal{L}(\theta) := \frac{1}{n} \sum_{i=1}^{n} \mathcal{L}_i(\theta)$的一个驻点。具体而言，服务器试图计算一个驻点$\theta^*$，即 $\nabla \mathcal{L}(\theta^*) = \overline{0}$，其中 $\nabla \mathcal{L}$ 表示 $\mathcal{L}$的梯度 。假设 $\mathcal{L}$ 存在驻点，则可使用经典的分布式（随机）梯度下降（分布式梯度下降／随机梯度下降）方法 [6], , 以近似误差为代价实现这一目标。在该方法中，服务器维护一个模型，并通过对工作节点在各自损失函数上计算出的（随机）梯度取平均值来迭代更新该模型。

存在拜占庭工作节点时的目标。 我们考虑一种对抗情形，其中 f 个身份事先未知的工作节点是拜占庭节点 [30]。这些工作节点不必遵循规定的协议，并且可能向服务器发送任意消息。在此情形下，服务器的目标是找到诚实（即非拜占庭）工作节点的平均损失函数的一个驻点。我们正式将此情形下的拜占庭鲁棒性定义如下。

定义 1 ((f, ε)**-拜占庭鲁棒性**）。若学习算法(f, ε)-具有拜占庭弹性，则即使在

[2]理想情况下，服务器希望找到 $\mathcal{L}$ 的全局极小值点。然而，由于损失可能是非凸的（例如，对于神经网络而言），全局最小化通常是 NP难问题 [9]。因此，我们通常旨在寻找驻点。

ˆ存在 f 个拜占庭工作节点的情况下，它仍会输出 θ，使得

$$\left\|\nabla \mathcal{L}_{\mathcal{H}}(\hat{\theta})\right\|^2 \leq \varepsilon,$$

其中 $\mathcal{H}$ 表示诚实工作节点的索引集合，$\mathcal{L}_{\mathcal{H}}(\theta)$:
$= \frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}}\mathcal{L}_i(\theta)$。

换言之，即使存在 f 个拜占庭工作节点，(f,ε)-拜占庭弹性算法也能为诚实工作节点的经验损失找到一个ε-近似驻点。请注意，一般而言（对任意ε），当 $f \geq n/2$ 时，(f,ε)-拜占庭鲁棒性是不可能实现的，参见 [34]。因此，本文中我们始终假设 $f < n/2$。

标准拜占庭机器学习解决方案。实现(f,ε)-拜占庭鲁棒性的一种典型策略，是改进分布式梯度下降（或分布式随机梯度下降）方法：在服务器端用鲁棒聚合规则取代对工作节点梯度的简单平均。基本上，这类方案旨在通过准确估计诚实工作节点梯度的均值，减轻拜占庭梯度带来的负面影响。重要的聚合规则包括 Krum [7],几何中位数（GM） [43, 38, 2], 逐坐标中位数（CWMed） [48],坐标截尾均值（CWTM） [48], 以及最小直径平均（MDA） [40, 13]。近期研究还探索了利用工作节点梯度历史来增强这些方案容错保证的思路，例如使用分布式动量 [26, 17]或追踪工作节点梯度的历史 [3]。

然而，所有这些研究都高度依赖于这样一个假设：诚实工作节点拥有同质的数据，即存在一个真实分布 $\mathcal{D}$，使得 $D_i \sim \mathcal{D}^m$ 对所有 $i \in \mathcal{H}$均成立。关键在于，违反这一假设时，这些方法的鲁棒性会急剧下降 [26]。

拜占庭机器学习中的异质性**挑战**。在现实世界的分布式设置中，诚实工作节点之间的数据可以说是异质的。在非凸优化的背景下，数据异质性可按以下假设进行建模 [27, 26]。

假设 1（有界异质性）。存在一个实数 G，使得对于所有 $\theta \in \mathbb{R}^d$,

$$\frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}}\left\|\nabla \mathcal{L}_i(\theta) - \nabla \mathcal{L}_{\mathcal{H}}(\theta)\right\|^2 \leq G^2.$$

这种异质性使拜占庭机器学习问题更具挑战性，因为服务器可能会将错误的梯度（来自拜占庭工作节点）与持有离群数据点的诚实工作节点所提供的正确梯度混淆。事实上，近期研究表明，存在一个下界，限定了存在拜占庭工作节点时任何分布式算法的误差 [13, 26]。具体而言，根据 [26] 中的定理 III，我们得到以下结果。

命题 1。 如果学习算法 $\mathcal{A}$ 对于每一组光滑损失函数 $\mathcal{L}_1, \ldots, \mathcal{L}_n$ 满足假设 *1*，则 $\varepsilon = \Omega\left(f/n\, G^2\right)$。

现有异质性解决方案的脆弱性。此前只有少数研究探讨了异质性条件下的拜占庭机器学习。 [32]首次对这一问题进行了正式研究，提出了*RSA*，这是一种基于 ℓ_p 正则化的分布式随机梯度下降变体。然而，对*RSA* 的分析依赖于强凸性假设，而这一假设在现代机器学习中很少成立。随后的一项研究 [20] 提出了一种新颖的聚合规则，即比较梯度消除（CGE）。尽管这项研究为异质性拜占庭机器学习这一一般问题提供了一些有价值的见解（特别是指出了冗余的必要性），但即使在同质设置下，CGE 也无法保证收敛（见 [17]）。研究 [13] 考虑了异步通信和异质数据条件下的点对点设置。然而，所提出的算法仅进行了渐近分析，其概率鲁棒性并不理想。在这种点对点设置中，另一项研究采用了与我们类似的最近邻方案 [16], , 由诚实节点使用各自的诚实向量作为枢轴。然而，在我们的主从设置中，他们的技术无法使用，因为服务器无法访问任何可靠的向量。

与我们工作最相关的是 [26], , 它也提出了一种称为分桶的预聚合步骤，这让人联想到均值中的中位数估计量 [36, 23, 4, 44]。本质上，分桶是将输入随机划分为若干桶，然后将每个桶中输入的平均值传入鲁棒聚合规则。划分过程中的随机性会降低诚实输入的经验方差期望值，但会严重损害该方案的最坏情况鲁棒性（详细说明见附录 10）。此外，我们的实验揭示了这些方法无法抵御最先进的拜占庭攻击 [47, 5, 3, 26]。

3 鲁棒分布式梯度下降

本节将介绍一个通用框架，用于分析 D-GD 的鲁棒变体（或鲁棒 *D-GD*）的收敛性。我们将在第 4 节中运用这一框架，展示我们提出的预聚合步骤 NNM 的优势。首先，我们将在下文第 3.1 节介绍鲁棒 D-GD 的基本框架。随后，在引入 $(f,\ \kappa)$-鲁棒性的概念后，我们将在第 3.2 节分析鲁棒 D-GD 的收敛性。

3.1 RobustD-GD 的描述

如下方算法 1 所总结的，鲁棒分布式梯度下降是一种迭代算法，按 T 步进行。

本质上，服务器首先初始化参数向量 θ_0。在每一步 $t \in [T]$，服务器都会广播模型

聚合	GM	CWTM	CWMed	Krum	下界
κ	$\left(1+\frac{f}{n-2f}\right)^2$	$\frac{f}{n-2f}\left(1+\frac{f}{n-2f}\right)$	$\left(1+\frac{f}{n-2f}\right)^2$	$1+\frac{f}{n-2f}$	$\frac{f}{n-2f}$

表1：不同（f，κ）鲁棒聚合规则的鲁棒性系数 κ，忽略数值常数。精确的鲁棒性系数见附录 8.1。另请注意，我们的分析是紧的，且显著优于以往工作 [17, 26], ，例如消除了 CWMed 和 CWTM 对维度的依赖。

算法 1： 鲁棒 D-GD

输入： 初始模型 θ_0、鲁棒聚合 F、学习率 γ 和步数 T。

对 $t = 1 \dots T$ **执行**

  服务器 广播 θ_{t-1} 给所有工作节点；

  对每个 诚实工作节点，i **并行执行**

    计算并发送梯度 $g_t^{(i)} = \nabla \mathcal{L}_i(\theta_{t-1})$；

  服务器聚合梯度：

  $R_t = F\left(g_t^{(1)}, \dots, g_t^{(n)}\right)$；

  服务器更新模型：$\theta_t = \theta_{t-1} - \gamma R_t$；

服务器求 $\tau \in \operatorname{argmin}_{1 \le t \le T} \|R_t\|$ 并设置 $\hat{\theta} = \theta_{\tau-1}$。

返回 $\hat{\theta}$；

θ_{t-1} 发送给所有工作节点。收到 θ_{t-1}后，每个诚实工作节点都会返回梯度 $g_t^{(i)} = \nabla \mathcal{L}_i(\theta_{t-1})$，该梯度是通过在其本地数据集 $\mathcal{D}_i$上评估 θ_{t-1} 计算得到的。诚实工作节点会正确执行算法，而拜占庭工作节点 w_i 则可能为 $g_t^{(i)}$ 发送任意值。服务器收到所有工作节点发送的梯度后，会使用鲁棒聚合规则 F对其进行聚合：$\mathbb{R}^{d \times n} \to \mathbb{R}^d$。具体而言，服务器计算

$$R_t = F\left(g_t^{(1)}, \dots, g_t^{(n)}\right).$$

最后，服务器将模型更新为 $\theta_t = \theta_{t-1} - \gamma R_t$，其中 $\gamma > 0$ 称为学习率。经过 T步后，服务器输出模型 θ_t，该模型对应的聚合结果 R_t 的范数最小。也就是说，该算法的输出为 $\theta = \theta_{\tau-1}$，其中 $\tau \in \arg\min_{1 \le t \le T} \|R_t\|$.

3.2 RobustD-GD 的分析

鲁棒 D-GD 的核心是聚合规则 F。为了精确分析 F 的效用，我们引入 (f, κ)-鲁棒性的概念，该概念统一了以往的鲁棒性准则，且足够精细，能够获得紧确的收敛保证。也就是说，(f, κ)-鲁棒性确保聚合规则在估计诚实输入的平均值时，其误差始终不超过诚实输入方差的 κ 倍。形式化地说，其定义如下。

定义 2 （(f,κ)**-鲁棒性**）。设 $f < n/2$ 和 $\kappa \ge 0$。若聚合规则 F满足以下条件，则称其为(f,κ)-鲁棒的：对于任意向量 $x_1, \dots, x_n \in \mathbb{R}^d$以及任意大小为 $n-f$的集合 $S \subseteq [n]$，

$$\|F(x_1, \dots, x_n) - \bar{x}_S\|^2 \le \frac{\kappa}{|S|} \sum_{i \in S} \|x_i - \bar{x}_S\|^2$$

其中 $\bar{x}_S = \frac{1}{|S|}\sum_{i \in S} x_i$。我们将 κ 称为鲁棒性系数。

我们的准则统一了现有的鲁棒性定义，包括 (f, λ)-容错平均 [17] 和 (δ_{max}, c)-*ARAgg* [26]。具体而言，当 $\kappa = \mathcal{O}(f/n)$ 时，我们的定义同时蕴含 (f, λ)-容错平均和 (δ_{max}, c)- ARAgg[3]。我们在附录 8.3 中证明这一结论。此外，(f, κ)-鲁棒性使我们能够针对最多有 f 个工作节点遭受拜占庭故障的情况，在标准异质性假设下，为鲁棒 D-GD 设计通用的收敛分析。下面的定理 1 给出了鲁棒 D-GD 的通用收敛分析，并假设 F 满足 (f, κ)-鲁棒性。回顾一下，$\mathcal{H}$ 表示诚实工作节点的索引集合。

定理 1。设假设 *1* 成立，并注意到 $\mathcal{L}_{\mathcal{H}}$ 是L-光滑的。考虑算法 *1*，其中 $T \ge 1$ 且学习率为 $\gamma = 1/L$。若 F 是(f,κ)-鲁棒的，则

$$\left\|\nabla \mathcal{L}_{\mathcal{H}}(\hat{\theta})\right\|^2 \le 4\kappa G^2 + \frac{4L(\mathcal{L}_{\mathcal{H}}(\theta_0) - \mathcal{L}^*)}{T},$$

其中 $\mathcal{L}^* :=$ 下确界$_{\theta \in \mathbb{R}^d} \mathcal{L}_{\mathcal{H}}(\theta)$。

根据定理 1，鲁棒 D-GD 的渐近误差（当 $T \to \infty$ 时）是最优的；也就是说，当 F 是 (f, κ)-鲁棒且$\kappa = \mathcal{O}(f/n)$时，它与命题 1 给出的下界相匹配。在齐次情形下，即当 $G = 0$时，尽管存在f 个拜占庭工作节点，只要 F 是 (f, κ)-鲁棒且 κ有界，鲁棒 D-GD 仍可渐近地达到诚实方平均损失函数的一个驻点。请注意，在分析梯度下降等一阶方法时，$1/T$ 的收敛速率对于光滑非凸损失函数而言是标准的 [19]。

现有聚合方法的次优性。可以证明，若干现有聚合规则（如 CWTM、Krum、GM 和 CWMed）是 (f,κ)-鲁棒的。这些规则的鲁棒性系数 κ 列于表1，形式化推导见附录 8.1。另请注意，对于任意 $f < n/2$，聚合规则都不可能是 (f,κ)-鲁棒的

[3]尽管满足（f，λ）容错平均条件只需 $\kappa = \sqrt{\lambda}$，也就是说，它不必属于 $\mathcal{O}(f/n)$。

$\kappa < \frac{f}{n-2f}$（详情见附录 8.2）。这个下界意味着，一般而言，鲁棒聚合规则无法提供与诚实输入的平均值任意接近的估计。这也表明，表1中 Krum、GM 和 CWMed 的取值并非最优，因为它们没有达到该下界。我们将在下一节中证明，NNM 通过增强这些聚合规则的鲁棒性解决了这一问题，并为鲁棒 D-GD 提供最优收敛性。

4 通过最近邻混合进行修正

本节将介绍一种有原则的方法，以解决现有方案在拜占庭鲁棒性方面的次优问题。具体而言，我们提出一种名为最近邻混合（NNM）的预聚合算法，并证明将其嵌入分布式梯度下降（D-GD）后，可以实现最优的拜占庭鲁棒性。我们将在第 4.1 节介绍 NNM 过程，并在第 4.2 节证明，在聚合规则之前应用 NNM 可以增强鲁棒性。

4.1 NNM 描述

给定一组 n 输入向量 $x_1, \ldots, x_n \in \mathbb{R}^d$，NNM 会将每个向量替换为其 $n-f$ 最近邻（包括自身）的平均值。形式上，NNM 输出 $(y_1, \ldots, y_n) = \text{NNM}(x_1, \ldots, x_n)$，其中对每个 $i \in [n]$，

$$y_i = \frac{1}{n-f} \sum_{j=1}^{n-f} x_{i:j} \; ; \tag{1}$$

其中 $x_{i:j}$ 是 $(x_1, \ldots, x_n)$ 中距离 x_i 最近的向量。直观而言，在鲁棒 D-GD 的背景下，应用 NNM 会人为地混合梯度，从而使每个混合后的梯度 都能更好地表示 $\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})$。NNM 的完整过程见算法2。

算法2： 最近邻混合（NNM）

输入： 输入数量 n，拜占庭输入数量 $f < n/2$，向量 x_1、.....、$x_n \in \mathbb{R}^d$。

对于 $i = 1 \ldots n$，**执行**

对输入进行排序，得到 $(x_{i:1}$、.....、$x_{i:n})$，使得

$$\|x_{i:1} - x_i\| \leq \ldots \leq \|x_{i:n} - x_i\|;$$

对 x_i 的 $n-f$ 个最近邻取平均值，即:

$$y_i = \frac{1}{n-f} \sum_{j=1}^{n-f} x_{i:j} \; ;$$

返回 y_1、.....、y_n;

备注 1. *NNM* 的计算成本在最坏情况下为 $\mathcal{O}\big(dn^2\big)$，这是由于需要为每个输入搜索其 $n-f$ 个最近邻。用于近似的更快算法为了提高效率，可以使用最近邻搜索 *[21, 35]*。不过，我们认为，*NNM* 的成本与若干聚合规则相当（甚至更低），包括 *Krum [7]*, 、*Multi-Krum [7]*, 和 *MDA [40, 14]*。下面列出几种主要聚合规则的成本：*Krum* 和 *Multi-Krum*： $\mathcal{O}(dn^2)$，*CWMed [48]* 和 *MeaMed [46]*:$\mathcal{O}(dn)$，*CWTM [48]*: $\mathcal{O}(dn\log n)$，ϵ 近似几何中位数 *[2]*: $\mathcal{O}(dn + d\epsilon^{-2})$，*MDA*： $\mathcal{O}(dn^2 + \binom{n}{f} n^2)$。最后，与谱方法 *[42]*, 不同，我们强调，我们的算法保留了关于 d 的线性依赖关系，而在现代机器学习中，d 可能极大（即 $d \gg n$）。

4.2 NNM 的分析

我们现在在引理 1 中给出 NNM 为 (f, κ)-鲁棒聚合规则带来的鲁棒性增强。随后，我们在推论 1 中说明，这如何在异质性条件下带来最优的拜占庭韧性保证。

引理 1. 设 $f < n/2$ 和 F： $\mathbb{R}^{d \times n} \to \mathbb{R}^d$。若 F 是(f, κ)-鲁棒的，则 $F \circ \mathit{NNM}$ 是(f, κ')-鲁棒的，其中

$$\kappa' \leq \frac{8f}{n-f}(\kappa + 1).$$

本质上，引理 1 意味着，将 NNM 与任意 (f, κ)-鲁棒聚合规则复合，可将鲁棒性系数的渐近阶提升至 $\mathcal{O}(f/n(\kappa+1))$。具体而言，这意味着，如果 F 的鲁棒性系数为 $\kappa = \mathcal{O}(1)$，NNM 会使新的鲁棒性系数达到最优。我们认为，条件 $\kappa = \mathcal{O}(1)$ 足够一般，适用于任何标准的鲁棒聚合规则。事实上，假设存在 $\nu > 0$ 使得 $n \geq (2+\nu)f$，则所有上述聚合规则都是 (f, κ)-鲁棒的，且 $\kappa = \mathcal{O}(1)$。因此，从理论上说，表1中的任何聚合规则与 NNM 结合后，都是算法 1 的良好候选规则。接下来，如下文推论 1 所述，我们可以在异质性条件下获得最优的拜占庭韧性。

推论 1。 设假设 *1* 成立，并回顾 $\mathcal{L}_{\mathcal{H}}$ 是L-光滑的。考虑采用 $\gamma = 1/L$ 和聚合 $F \circ \mathit{NNM}$ 的算法 *1*。若 F 是 (f, κ)-鲁棒的，且满足 $\kappa = \mathcal{O}(1)$，则算法 *1* 具有 (f, ε)-拜占庭弹性，且

$$\varepsilon = \mathcal{O}\big(f/n G^2 + 1/T\big).$$

备注 2。 注意，在某个常数 $\nu > 0$ 满足 $n \geq (2+\nu)f$ 时，*CWTM* 无需使用 *NNM* 即可达到阶最优鲁棒性系数 $\kappa = \mathcal{O}(f/n)$。然而，在 *CWTM* 之前使用 *NNM* 能显著提升其经验性能（见第 *6* 节）。我们认为，相较于本文采用的最坏情形方法，平均情形分析或许能够在理论上刻画这种改进。

5 随机扩展

尽管具有最优性，我们的鲁棒 D-GD 解决方案在计算上开销较大，因为它要求诚实工作者

在整个数据集上计算每个梯度。实践中，更常见的做法是考虑 D-GD 的随机变体，其中工作节点在数据集的随机小批量上计算梯度。为此，我们证明，NNM 也可用于提升分布式随机重球法（D-SHB）鲁棒变体的性能；最近已有研究证明，该方法在同质设置下的拜占庭机器学习中表现良好 [15, 25, 17]。

5.1 鲁棒 D-SHB 的描述

与鲁棒 D-GD 类似，该算法按如下方式进行 T 次迭代。在每一步 $t \in [T]$，服务器持有一个模型 θ_{t-1}，每个诚实工作节点持有一个局部动量 $m_{t-1}^{(i)}$[4]。服务器将当前模型 θ_{t-1} 广播给所有工作节点，以便它们更新各自的局部动量。为此，每个诚实工作节点从 D_i 中随机抽取一个迷你批次数据 $S_t^{(i)}$，并计算其梯度 $\nabla \mathcal{L}_i(\theta_{t-1})$ 的随机估计值 $g_t^{(i)}$，定义如下：

$$g_t^{(i)} = \frac{1}{|S_t^{(i)}|} \sum_{z \in S_t^{(i)}} \nabla \ell(\theta_{t-1}, z). \tag{2}$$

随后，每个诚实工作节点更新其局部动量，并将其发送给服务器

$$m_t^{(i)} = \beta m_{t-1}^{(i)} + (1-\beta) g_t^{(i)}, \tag{3}$$

其中，$\beta \in (0,1)$ 是动量参数，并由所有诚实用户共享。与 D-SGD 类似，服务器将收到的动量聚合为 $R_t = F(m_t^{(1)}, \ldots, m_t^{(n)})$。最后，服务器将模型更新为 $\theta_t = \theta_{t-1} - \gamma R_t$，其中 $\gamma > 0$ 是学习率。经过 T 次迭代后，服务器从 $(\theta_0, \ldots, \theta_{T-1})$ 中均匀采样并输出 θ。鲁棒 D-SHB 的整体流程总结于算法 3。

5.2 使用 NNM 分析鲁棒 D-SHB

现在，我们给出使用 NNM 的鲁棒 D-SHB 的收敛保证。为此，我们对随机梯度的方差作出一个额外的（标准）假设。

假设2 (有界方差)。 对于每个诚实工作节点w_i，$i \in \mathcal{H}$，以及所有 $\theta \in \mathbb{R}^d$，均有

$$\frac{1}{m} \sum_{z \in \mathcal{D}_i} \left\| \nabla_\theta \ell(\theta, z) - \nabla \mathcal{L}_i(\theta) \right\|^2 \leq \sigma^2.$$

我们现在在定理 2 中将结果扩展到 D-SHB。基本上，我们在假设学习率为常数、假设 1 和 2 成立且 $\mathcal{L}_\mathcal{H}$ 是 L-光滑的条件下，分析算法 3。为方便起见，我们引入

算法 3： 鲁棒 D-SHB

输入：初始模型 θ_0、诚实工作节点的初始动量 $m_0^{(i)} = 0$、鲁棒聚合 F、学习率 γ、动量系数 β 和步数 T。对于 $t = 1 \ldots T$，执行：服务器向所有工作节点广播 θ_{t-1}；对于每个诚实工作节点 i，并行执行：根据 (2) 计算随机梯度 $g_t^{(i)}$；根据 (3) 更新局部动量 $m_t^{(i)}$；向服务器发送 $m_t^{(i)}$；服务器聚合各动量：$R_t = F(m_t^{(1)}, \ldots, m_t^{(n)})$；服务器更新模型：$\theta_t = \theta_{t-1} - \gamma R_t$；

ˆ从（θ_0、.....、θ_{T-1}）中均匀采样 θ；**ˆ返回** θ；

在陈述定理之前，先给出以下数值常数：

$$a_1 \coloneqq 36, a_2 \coloneqq 6\sqrt{\mathcal{L}_\mathcal{H}(\theta_0) - \mathcal{L}^*}, a_3 \coloneqq 1728L,$$
$$a_4 \coloneqq 288L, a_5 \coloneqq 6L\, a_2^2, \text{ and } \mathcal{L}^* = \inf_{\theta \in \mathbb{R}^d} \mathcal{L}_\mathcal{H}(\theta).$$

定理 2. 设假设 *1* 和 *2* 成立，并回顾一下，$\mathcal{L}_\mathcal{H}$ 是 L-光滑的。设 F 是一个(f, κ)-鲁棒聚合规则。考虑动量系数为 $\beta = \sqrt{1 - 24\gamma L}$、学习率为

$$\gamma = \min\left\{ \frac{1}{24L}, \frac{a_2}{2a_\kappa \sigma \sqrt{T}} \right\},$$

其中 $a_\kappa^2 \coloneqq a_3\kappa + \frac{a_4}{n-f}$ 对于所有 $T \geq 1$，我们有

$$\mathbb{E}\left[\left\| \nabla \mathcal{L}_\mathcal{H}(\hat{\theta}) \right\|^2 \right] \leq a_1 \kappa G^2 + \frac{a_2 a_\kappa \sigma}{\sqrt{T}} + \frac{a_5}{T} + \frac{a_2 a_4 \sigma}{n a_\kappa T^{3/2}},$$

其中期望是对算法的随机性取的。

紧概率保证。 定理 2 中的非消失误差为 $\mathcal{O}(\kappa G^2)$。因此，当$\kappa = \mathcal{O}(f/n)$时，此误差是紧的。然而，与鲁棒 D-GD（定理 1）的主要区别在于，该不等式仅在期望意义下成立，因此可能无法验证（f，ε）-拜占庭鲁棒性。尽管如此，这一结果与最先进的收敛保证 [26]（定理 II）一致。请注意，我们的结果与 [26] 中的结果之间仍有一个细微差别。我们在定理 2 中的结果，其随机性仅取决于数据的随机子采样和最终模型的选择。这些是研究随机梯度下降 [8]时通常会考虑的自然随机性来源。另一方面，[26] 中的结果还纳入了由 Bucketing 的打乱操作引入的额外（外生）随机性。即使

[4] θ_0 is set by the server and $m_0^{(i)} = 0$ for all honest workers.

工作节点计算真实梯度时，这种随机性来源也无法消除，而且可能会放大计算中的不确定性（详见第 6 节和附录 10）。因此，我们认为，定理 2 给出的概率收敛保证严格强于 [26] 中的结果。

再次利用引理 1，我们可以证明，定理 2 所隐含的紧致（概率）容错保证也适用于更广泛的 (f,κ)-鲁棒聚合规则类，且 $\kappa = \mathcal{O}(1)$。我们在下文的推论 2 中对这一点作出形式化表述。

推论 2。 设假设 *1* 成立，并回顾 $\mathcal{L}_{\mathcal{H}}$ 是*L*-光滑的。考虑在与定理 *2* 相同的设置下，使用聚合 $F \circ NNM$ 的算法 *3*。若 F 是(f,κ)-鲁棒的，且 $\kappa = \mathcal{O}(1)$，则有

$$\mathbb{E}\left[\left\|\nabla \mathcal{L}_{\mathcal{H}}(\hat{\theta})\right\|^2\right] = \mathcal{O}\big(f/n G^2 + 1/\sqrt{T}\big),$$

*wher*期望是对算法的随机性取的 性。

6 实验评估

在本节中，我们研究 NNM 的实际性能。我们报告了一系列全面的实验，在三个基准图像分类任务和五种不同的拜占庭攻击下，将我们的方法与当前最先进的方法进行比较。

6.1 实验设置

数据集、模型和超参数。 我们考虑三个图像分类数据集，即 MNIST [31],Fashion-MNIST [45], 和 CIFAR-10 [29]; 并在鲁棒 D-SHB 的基础上实现 NNM。受篇幅限制，我们仅展示 MNIST 和 CIFAR-10 上的结果，其余结果（包括使用 NNM 的分布式梯度下降实验）放在附录 15 中。

在 MNIST 上，我们使用批次大小为 $b = 25$ 的批次训练卷积神经网络（CNN）$T = 800$步，采用从 0.75 开始衰减的学习率，以及动量参数 $\beta = 0.9$。在 CIFAR-10 上，我们使用一个 CNN，其 $b = 50$、$T = 2000$、 $\gamma = 0.25$ 在第 1500 步衰减，且 $\beta = 0.9$。此外，我们使用四种聚合规则实现了该方法，即 Krum、CWTM、CWMed 和几何中位数[5], , 并将其性能与分桶 [26]方法以及原始聚合规则进行比较。作为基准，我们还在无故障（$f = 0$）的设置下实现了原始 D-SHB（即采用 F =平均值的鲁棒 D-SHB）。

异质性。 我们通过使用参数为 α 的狄利克雷分布从原始数据集中采样，来模拟诚实工作者数据中的异质性（做法同 [22]）。我们考虑三种异质性情形：极端（$\alpha = 0.1$），中等（$\alpha = 1$），以及低（$\alpha = 10$）。附录14中展示了由此产生的异质性随 α 变化的示意图。我们在上述定义的整个异质性范围内，将算法应用于MNIST和 Fashion-MNIST。不过，由于CIFAR-10的挑战性要大得多，我们将其异质性限制为 $\alpha \in \{1, 10\}$。

分布式系统与拜占庭攻击。 我们考虑一个包含 $n = 17$ 个工作节点的分布式系统，其中 $f < n/2$ 个工作节点可能是拜占庭工作节点。我们在 MNIST 数据集上改变 $f \in \{4, 6, 8\}$，在 CIFAR-10 数据集上改变 $f \in \{2, 3, 4\}$。拜占庭工作节点执行五种最先进的梯度攻击，分别为 Fall of Empires（FOE） [47], A Little is Enough（ALIE） [5], 符号翻转（SF） [3], 标签翻转 [3], 和 Mimic [26]。请注意，对于 ALIE 和 FOE，我们按照 [42] 中的做法设计了这些攻击的优化版本。我们将在附录14中进一步说明这一点。

可复现性与可复用性。 为确保可复现性，所有实验均使用五个随机种子运行，种子取值为 1 至 5。代码也将公开，以便复用。有关实验设置的更多细节，请参见附录14。

6.2 MNIST 上的实证结果

在表 2 中，我们仔细考察了 NNM 在极端异质性（$\alpha = 0.1$）下于 MNIST 上的表现，并将其与分桶和原始聚合规则进行比较。对于每个区块（即每种聚合规则）以及每种攻击，我们都用粗体标出相应场景中准确率最高的算法。

NNM 提升鲁棒性。我们清楚地看到，我们的算法增强了拜占庭场景下聚合规则的韧性，并使其在各种攻击下表现得最为稳定。事实上，对于 Krum、CWMed 和 CWTM（即表 2 中的第 1、3 和 4 个区块），NNM 在所有攻击下都能取得最高准确率。另两种技术（分桶和原始方法）的表现则弱得多，有时甚至与随机分类器相当（例如，原始 Krum 在 ALIE 和 FOE 攻击下的准确率分别为 10.19% 和 10.28%）。

GM 的情况不太明显，因为其他技术在某些设置下（例如 ALIE、SF）可能优于我们的方法。然而，一个关键观察是，始终至少存在一种攻击，会显著降低分桶+GM 和原始GM 的性能；而 NNM+GM 在所有攻击场景下都能稳定获得理想的准确率。事实上，NNM+GM 在各种攻击下取得的最低准确率为 75.27%，显著优于分桶+GM 和原始GM，后两者的最低准确率分别仅为 39.83% 和 57.86%。此外，尽管原始GM 在 ALIE 下的得分最高，但其在 FOE 和 SF 下的准确率较低，分别为 65.61% 和 57.86%。分桶+GM 在 ALIE 和 FOE 下也表现不佳，准确率远低于 50%。最后，尽管分桶+GM 的得分

[5]我们使用 [38] 中的近似方法实现几何中位数。

	聚合	ALIE	FOE	LF	SF	Mimic	最坏情况
①	Krum	10.19 ± 00.61	10.28 ± 00.57	12.76 ± 06.25	51.17 ± 06.14	86.78 ± 07.04	10.19 ± 00.61
	分桶 + Krum	44.78 ± 06.18	36.10 ± 15.70	56.21 ± 19.49	47.54 ± 11.74	94.92 ± 03.93	36.10 ± 15.70
	NNM + Krum	**78.30 ± 07.78**	**70.07 ± 04.39**	**93.07 ± 05.24**	**82.44 ± 02.86**	**97.69 ± 00.77**	70.07 ± 04.39
②	GM	**92.01 ± 04.35**	65.61 ± 12.17	93.94 ± 03.70	57.86 ± 10.42	96.85 ± 01.57	57.86 ± 10.42
	分桶 + 几何中位数	39.83 ± 11.35	44.73 ± 16.47	**96.22 ± 02.83**	**91.30 ± 03.91**	**97.68 ± 00.91**	39.83 ± 11.35
	NNM + 几何中位数	81.26 ± 08.91	**75.27 ± 02.69**	94.23 ± 03.20	86.33 ± 03.73	97.17 ± 01.09	75.27 ± 02.69
③	CWMed	68.74 ± 06.99	19.48 ± 10.97	33.34 ± 17.02	27.96 ± 09.97	64.01 ± 12.77	19.48 ± 10.97
	分桶 + CWMed	55.86 ± 10.00	42.80 ± 21.25	70.16 ± 11.65	50.96 ± 16.52	94.43 ± 03.48	42.80 ± 21.25
	NNM + CWMed	**80.52 ± 07.45**	**75.20 ± 08.80**	**93.42 ± 02.98**	**85.10 ± 06.05**	**97.38 ± 00.70**	75.20 ± 08.80
④	CWTM	76.16 ± 07.68	69.96 ± 16.57	36.87 ± 21.43	27.45 ± 08.83	89.83 ± 02.83	27.45 ± 08.83
	分桶 + CWTM	55.86 ± 10.00	42.80 ± 21.25	70.16 ± 11.65	50.96 ± 16.52	94.43 ± 03.48	42.80 ± 21.25
	NNM + CWTM	**79.04 ± 09.19**	**79.91 ± 03.94**	**94.75 ± 02.22**	**84.78 ± 05.78**	**96.02 ± 03.25**	79.04 ± 09.19

表 2：在极端异质性（%）条件下，MNIST 上跨 $T = 800$ 学习步数的最高测试准确率，其中（$\alpha = 0.1$）以及五种拜占庭攻击。共有 $f = 4$ 个拜占庭工作节点，占 $n = 17$。基线准确率（D-SHB）为$98.03 \pm 0.70\%$。在四个水平区块中的每个区块以及每种攻击下，我们用**粗体**标出最高准确率。对于每种方法，我们还展示其跨攻击的最差准确率，并在每个区块中标出最佳和最差结果。

在 LFandMimic 下表现最佳；NNM+GM 在这两种攻击下也表现出色，准确率均高于 96%。

最坏情况性能。我们在表 2 的最后一列中展示了每种聚合技术（即每一行）在所有攻击下的最坏情况 性能，并在每个区块内按性能从差（红色）到好（绿色）进行排名。我们认为，这是正确评估拜占庭鲁棒性的关键指标，因为同一种算法可能同时对某些攻击有很强的防御能力，却在面对其他攻击时表现不佳。因此，从最后一列可以看出，我们的方法始终呈现出“最佳”的最坏情况。事实上，NNM 在所有攻击和聚合规则下的最低准确率为 70.07%，对应 Krum。此外，其他技术的最坏情况性能远逊于我们，Krum 的准确率最低仅为 10.19%，而 Bucketing+GM 的准确率最低为 39.83%。

此外，对于所有聚合规则，分桶在最坏情况下的表现都几乎同样糟糕（36.1%、39.83% 和 42.80%）。然而，NNM 在最坏情况下的准确率都在 70%–79% 之间。这有力地表明，分桶并不可靠，因为无论采用何种聚合规则，其最坏情况表现都不尽如人意。

6.3 CIFAR-10 上的实证结果

在图 1 中，我们绘制了 NNM 和分桶在 CIFAR-10 上经过 $T = 2000$ 步学习后的表现，所使用的基础聚合规则为 GM、CWMed、CWTM 和 Krum[6]。我们考察了两种异质性水平（第 1 行为 $\alpha = 1$，第 2 行为 $\alpha = 10$），其中两名拜占庭工作节点分别执行 ALIE 和 LF 攻击。

异质性会阻碍学习。我们的第一个观察结果是，正如预期的那样，异质性情形越严重，学习越受阻。如图 1 所示，将 α 从 1 增加到 10，可显著改善所有 NNM 聚合（尤其是在 ALIE 下）的表现；而分桶+CWMed 的表现仍停滞在 10%，分桶+GM 的表现则勉强达到 30%。

NNM 的实证优势。在 ALIE 攻击下，我们清楚地看到，在两种异质性情形中，NNM 的表现都远胜于分桶。具体而言，当$\alpha = 1$时，使用结合几何中位数和 CWMed 的分桶会因 ALIE 而导致学习性能恶化，这两种方法的最终准确率都接近 10%。尽管分桶+Krum 的表现更好，但其准确率仍然较低，方差也远大于任何一种 NNM 聚合。另一方面，我们发现，标签翻转是一种弱得多的攻击。尽管所有聚合方法都能收敛到理想的准确率，但我们的算法仍表现出比分桶更好的收敛速率。在 $\alpha = 10$中，这一点尤其明显：所有 NNM 聚合的收敛速率几乎与 D-SHB 完全一致，而分桶的收敛速度较慢，尤其是在使用 Krum 时。其余三种攻击

[6]在所考虑的设置中，使用 CWMed 和 CWTM 的分桶完全等价。

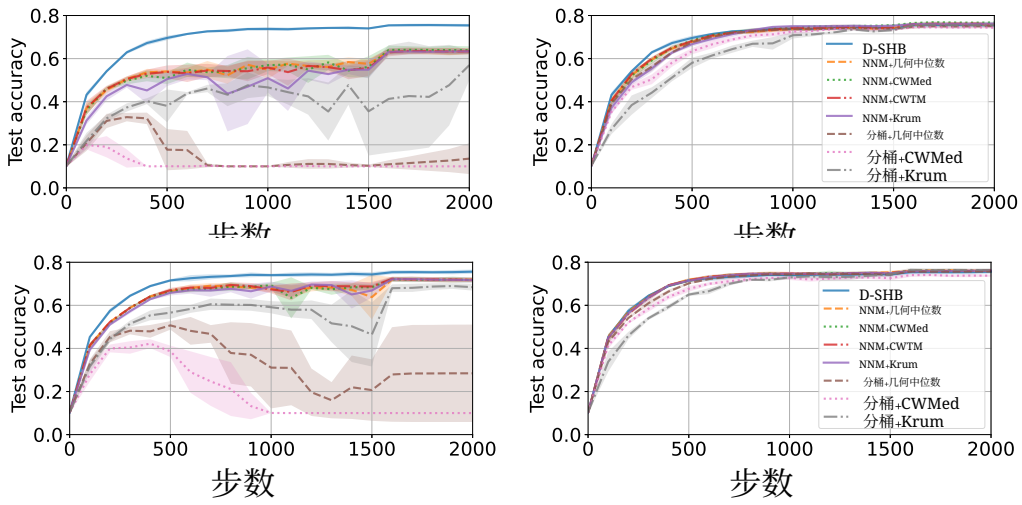

图 1：在 CIFAR-10 上进行的实验，其中 $f = 2$ 个拜占庭工作节点位于 $n = 17$ 个工作节点之中。拜占庭工作节点执行 ALIE（第 *1* 列）和 LF（第 *2* 列）攻击。 1st 行：中等异质性（$\alpha = 1$）。 2nd 行：低异质性（$\alpha = 10$）。

与标签翻转的表现相似，详见附录 15。

7 结论与未来工作

我们证明，经 NNM 增强的鲁棒 D-GD 是异质性条件下拜占庭机器学习的一种最优解。我们还推导了鲁棒 D-SHB（结合 NNM）的类似期望结果。我们认为，一个有趣的未来研究方向是，通过研究随机解的几乎必然收敛率来收紧这些保证。近期，拜占庭无攻击的情形下已针对随机重球法 SHB 引入了此类保证 [41, 33, 18]。然而，如何将其推广到我们的设定仍是一个开放问题。总的来说，我们认为，后续关于拜占庭机器学习的研究应力求获得几乎必然收敛保证（而非期望意义下的保证），避免使用不必要的随机性，并验证这些算法的鲁棒性。

致谢

本研究部分由瑞士国家科学基金会（SNSF）项目 200021 200477 和 200021 182542，以及 EPFL-Ecocloud 博士后项目资助。作者感谢匿名审稿人提出的建设性意见。

参考文献

[1] Mart´ınAbadi、Ashish Agarwal、Paul Barham、Eugene Brevdo、Zhifeng Chen、Craig Citro、Greg Corrado、Andy Davis、Jeffrey Dean、Matthieu Devin、Sanjay Ghemawat、Ian Goodfellow、Andrew Harp、Geoffrey Irving、Michael Isard、Yangqing Jia、Rafal Jozefow- icz、Lukasz Kaiser、Manjunath Kudlur、Josh Leven- berg、Dan Man´e、Rajat Monga、Sherry Moore、Derek Murray、Chris Olah、Mike Schuster、Jonathon Shlens、Benoit Steiner、Ilya Sutskever、Kunal Talwar、Paul Tucker、Vincent Vanhoucke、Vijay Vasudevan、Fernanda Vi´egas、Oriol Vinyals、Pete Warden、Martin Wattenberg、Martin Wicke、Yuan Yu 和 Xiaoqiang Zheng。《TensorFlow：异构分布式系统上的大规模机器学习》，2015 年。

[2] Anish Acharya、Abolfazl Hashemi、Prateek Jain、Sujay Sanghavi、Inderjit S. Dhillon 和 Ufuk Topcu。通过分块坐标几何中位数下降法实现高维鲁棒训练。载于 Gustau Camps-Valls、Francisco J. R. Ruiz 和 Isabel Valera（编），第 *25* 届人工智能与统计国际会议论文集，第 151 卷，机器学习研究论文集，第 11145–11168 页。PMLR，2022 年 3 月 28–30 日。

[3] Zeyuan Allen-Zhu、Faeze Ebrahimianghazani、Jerry Li 和 Dan Alistarh。拜占庭容错非凸随机梯度下降。载于国际学习表征会议，2020年。

[4] Noga Alon、Yossi Matias 和 Mario Szegedy。《频率矩近似的空间复杂度》。载于第二十八届 *ACM*计算理论研讨会论文集，第 20–29 页，1996 年。

[5] Moran Baruch、Gilad Baruch 和 Yoav Goldberg。《A Little is Enough：规避分布式学习防御》。载于《神经信息处理系统进展》第*32*卷：*2019*年神经信息处理系统年会，*2019*年*12*月*8*日至*14*日，美国加利福尼亚州长滩，2019年。

[6] Dimitri Bertsekas 和 John Tsitsiklis。《并行与分布式计算：数值方法》。Athena Scientific，2015年。[7] Peva Blanchard、El Mahdi El Mhamdi、Rachid Guer- raoui 和 Julien Stainer。《对抗者环境下的机器学习：拜占庭容错梯度下降》。载于 I. Guyon、U. V. Luxburg、S. Bengio、H. Wallach、R. Fergus、S. Vishwanathan 和 R. Garnett 编，《神经信息处理系统进展》第*30*卷，第119–129页。Curran Associates, Inc.，2017年。[8] L´eon Bottou、Frank E Curtis 和 Jorge Nocedal。《大规模机器学习的优化方法》。*Siam Review*，60(2)：223–311，2018年。

[9] Stephen Boyd 和 Lieven Vandenberghe。《凸优化》。剑桥大学出版社，2004 年。

[10]Moses Charikar、Jacob Steinhardt 和 Gregory Valiant。从不可信数据中学习。载于《第 49 届 ACM SIGACT 计算理论年会论文集》，第 47–60 页，2017 年。

[11] Yudong Chen、Lili Su 和 Jiaming Xu。对抗环境下的分布式统计机器学习：拜占庭梯度下降。《ACM测量、分析与计算系统》，1(2)，2017 年 12 月。

[12] Simon S Du、Chi Jin、Jason D Lee、Michael I Jordan、Aarti Singh 和 Barnabas Poczos。梯度下降可能需要指数时间才能逃离鞍点。《神经信息处理系统进展》，第 30 卷，2017 年。

[13] El Mahdi El Mhamdi、Sadegh Farhadkhani、Rachid Guerraoui、Arsany Guirguis、Lˆe Nguyˆen Hoang 和 S´ebastien Rouault。《丛林中的协作学习（去中心化、拜占庭、异质、异步和非凸学习）》。载于第三十五届神经信息处理系统大会，2021年。

[14]El Mahdi El Mhamdi、Rachid Guerraoui 和 S´ebastien Rouault。《拜占庭中的分布式学习隐藏的脆弱性》。载于 Jennifer Dy 和 Andreas Krause 编，《第*35*届国际机器学习会议论文集》，《机器学习研究论文集》第80卷，第3521–3530页。PMLR，2018年7月10日至15日。[15]El Mahdi El Mhamdi、Rachid Guerraoui 和 S´ebastien Louis Alexandre Rouault。《面向拜占庭弹性随机梯度下降的分布式动量》。载于《第*9*届国际学习表征会议（*ICLR*）》，编号 CONF，2021年。[16] Sadegh Farhadkhani、Rachid Guerraoui、Nirupam Gupta、Lˆe Nguyˆen Hoang、Rafael Pinot 和 John Stephan。《让拜占庭去中心化学习更高效》。*arXiv* 预印本 *arXiv:2209.10931*，2022年。[17] Sadegh Farhadkhani、Rachid Guerraoui、Nirupam Gupta、Rafael Pinot 和 John Stephan。《通过动量的弹性平均轻松实现拜占庭机器学习》。载于 Kamalika Chaudhuri、Stefanie Jegelka、Le Song、Csaba Szepesvari、Gang Niu 和 Sivan Sabato 编，《第*39*届国际机器学习会议论文集》，《机器学习研究论文集》第162卷，第6246–6283页。PMLR，2022年7月17日至23日。

[18] S´ebastien Gadat、FabienPanloup 和 Sofiane Saadane。随机重球法。《电子统计学期刊》，12(1):461–529，2018年。

[19] Saeed Ghadimi 和 Guanghui Lan。用于非凸非线性与随机规划的加速梯度方法。《数学规划》，156(1):59–99，2016年。

[20] Nirupam Gupta 和 Nitin H Vaidya。分布式优化中的容错：冗余问题。载于第*39*届分布式计算原理研讨会论文集，第365–374页，2020年。

[21] Kiana Hajebi、Yasin Abbasi-Yadkori、Hossein Shah- bazi 和 Hong Zhang。使用 k近邻图进行快速近似最近邻搜索。发表于第二十二届国际人工智能联合会议，2011年。

[22] Tzu-Ming Harry Hsu、Hang Qi 和 Matthew Brown。衡量非同一数据分布对联邦视觉分类的影响，2019年。

[23] Mark RJerrum、LeslieG Valiant 和 Vijay V Vazirani。从均匀分布中随机生成组合结构。《理论计算机科学》，43:169–188，1986年。

[24] Peter Kairouz、H. Brendan McMahan、Brendan Avent、Aur´elien Bellet、Mehdi Bennis、Arjun Nitin Bhagoji、Kallista Bonawitz、Zachary Charles、Graham Cor- mode、Rachel Cummings、Rafael G. L. D'Oliveira、Hubert Eichner、Salim El Rouayheb、David Evans、JoshGardner、ZacharyGarrett、Adri`aGasc´on、Badih Ghazi、Phillip B. Gibbons、Marco Gruteser、Zaid Har- chaoui、Chaoyang He、Lie He、Zhouyuan Huo、Ben Hutchinson、Justin Hsu、Martin Jaggi、Tara Javidi、Gauri Joshi、Mikhail Khodak、Jakub Konecn´y、Alek- sandra Korolova、Farinaz Koushanfar、Sanmi Koyejo、Tancr`ede Lepoint、Yang Liu、Prateek Mittal、Mehryar¨Mohri、Richard Nock、Ayfer Ozg¨ur、Rasmus Pagh、Hang Qi、Daniel Ramage、Ramesh Raskar、Mariana Raykova、Dawn Song、Weikang Song、Sebastian U. Stich、Ziteng Sun、Ananda Theertha Suresh、Florian

Tram`er, Praneeth Vepakomma, JianyuWang, Li Xiong, Zheng Xu, Qiang Yang, Felix X. Yu, Han Yu, and Sen Zhao. 联邦学习的进展与开放问题。*Foundations andTrends® in MachineLearning*，14(1–2):1–210，2021。

[25] Sai Praneeth Karimireddy、Lie He 和 Martin Jaggi。利用历史信息进行拜占庭鲁棒优化。国际机器学习大会，第 *139* 卷，139，2021年。

[26] Sai Praneeth Karimireddy、Lie He 和 Martin Jaggi。通过分桶在异构数据集上进行拜占庭鲁棒学习。载于国际学习表征会议，2022年。

[27] Sai Praneeth Karimireddy、Satyen Kale、Mehryar Mohri、Sashank Reddi、Sebastian Stich 和 Ananda Theertha Suresh。Scaffold：用于联邦学习的随机控制平均。在国际机器学习大会，第 5132–5143 页。PMLR，2020年。

[28]Jakub Koneˇcn`y、H Brendan McMahan、Felix X Yu、Peter Richt´arik、Ananda Theertha Suresh 和 Dave Bacon。联邦学习：提升通信效率的策略。*arXiv* 预印本 *arXiv:1610.05492*，2016年。

[29] Alex Krizhevsky、Vinod Nair 和 Geoffrey Hinton。CIFAR-10 数据集。在线地址：*http://www. cs. toronto. edu/kriz/cifar. html*，55(5)，2014年。

[30] Leslie Lamport、Robert Shostak 和 Marshall Pease。拜占庭将军问题。*ACMTrans.Program.Lang. Syst.*，4(3):382–401，1982年7月。

[31] Yann LeCun 和 Corinna Cortes。MNIST 手写数字数据库。2010年。

[32] Liping Li、Wei Xu、Tianyi Chen、Georgios B. Giannakis 和 Qing Ling。RSA：面向异构数据集分布式学习的拜占庭鲁棒随机聚合方法。载于第三十三届 *AAAI* 人工智能大会暨第三十一届创新人工智能应用大会和第九届 *AAAI* 人工智能教育进展研讨会论文集，AAAI'19/IAAI'19/EAAI'19。AAAI 出版社，2019年。

[33] Jun Liu 和 Ye Yuan。随机梯度方法的几乎必然收敛率。载于 Po-Ling Loh 和 Maxim Raginsky（编），第三十五届学习理论会议论文集，机器学习研究论文集第 178 卷，第 2963–2983 页。PMLR，2022年7月2日至5日。

[34] Shuo Liu、Nirupam Gupta 和 Nitin H. Vaidya。分布式优化中的近似拜占庭容错。载于*2021*年 *ACM* 分布式计算原理研讨会论文集，PODC'21，第 379–389 页，纽约，纽约州，美国，2021 年。计算机协会。[35] Marius Muja 和 David G Lowe。面向高维数据的可扩展近邻算法。*IEEE* 模式分析与机器智能汇刊，36(11):2227–2240，2014 年。[36] A.S. Nemirovsky、D.B. din 和 D.B. Yudin。优化中的问题复杂度与方法效率。Wiley-Interscience 出版物。Wiley，1983 年。[37] Yurii Nesterov 等。凸优化讲义，第 137 卷。Springer，2018年。

[38] Krishna Pillutla、Sham M. Kakade 和 Zaid Har- chaoui。联邦学习的鲁棒聚合。*IEEE*信号处理汇刊，第 70 卷：1142–1154，2022 年。

[39] Boris T Polyak。加速迭代方法收敛的一些方法。苏联计算数学与数学物理，第 4 卷（第 5 期）：1–17，1964 年。

[40] Peter J Rousseeuw。具有高崩溃点的多变量估计。数理统计与应用，第 8 卷（第 37 期）：283–297，1985 年。

[41] Othmane Sebbouh、Robert M Gower 和 Aaron De- fazio。随机梯度下降和随机重球法的几乎必然收敛率。载于学习理论会议，第 3935–3971 页。PMLR，2021 年。

[42] Virat Shejwalkar 和 Amir Houmansadr。《操纵拜占庭：优化联邦学习中的模型投毒攻击与防御》。发表于 *NDSS*，2021年。

[43] Christopher G Small。《多维中位数综述》。国际统计评论/*Revue Internationale de Statistique*，第263–277页，1990年。

[44] Jiyuan Tu、Weidong Liu、Xiaojun Mao 和 Xi Chen。《用于拜占庭鲁棒分布式推断的方差缩减中位数均值估计量》。发表于*J. Mach. Learn.Res.*，22:84–1，2021年。

[45]Han Xiao、Kashif Rasul 和 Roland Vollgraf。《Fashion-MNIST：用于机器学习算法基准测试的新型图像数据集》。*arXiv*预印本 *arXiv:1708.07747*，2017年。

[46] Cong Xie、Oluwasanmi Koyejo 和 Indranil Gupta。《广义拜占庭容错随机梯度下降》，2018年。

[47] Cong Xie、Oluwasanmi Koyejo 和 Indranil Gupta。《Fall of Empires：通过内积操纵攻破拜占庭容错随机梯度下降》。载于《会议论文集》

第三十五届人工智能不确定性会议，*UAI 2019*，以色列特拉维夫，*2019*年*7*月*22*日至*25*日，第83页，2019年。

[48] Dong Yin、Yudong Chen、Ramchandran Kannan 和 Peter Bartlett。拜占庭鲁棒分布式学习：迈向最优统计收敛速率。载于 Jennifer Dy 和 Andreas Krause 编，《第*35*届机器学习国际会议论文集》，第80卷，机器学习研究论文集，第5650–5659页。PMLR，2018年7月10日至15日。

补充材料：通过混合实现修正：异质性下最优拜占庭机器学习指南

附录结构

附录 8 包含与（f， κ）-鲁棒性相关的证明。附录 9 包含对 NNM 的分析（引理 1 的证明）。附录 10 包含关于分桶 [26] 的正式讨论。附录 11 包含对鲁棒 D-GD 的分析（定理 1 的证明）。附录 12 包含对采用 NNM 的鲁棒 D-GD 的分析（推论 1 的证明），以及拜占庭弹性下界（命题 1 ）。附录 13 包含对采用 NNM 的鲁棒 D-SHB 的分析（定理 2 和推论 2 的证明）。附录14介绍实验设置的详细信息。附录 15 包含所有实验结果。

8 鲁棒性分析

在本节中，我们将证明所有与 (f,κ)-鲁棒性相关的结论。在第 8.1 节中，我们将证明若干现有聚合规则是 (f,κ)-鲁棒的，并给出其精确的鲁棒性系数。接着，在第 8.2 节中，我们通过证明关于 κ 的普适下界以及特定聚合规则的下界，确立分析结果的紧致性。最后，我们将在第 8.3 节中证明 (f,κ)-鲁棒性统一了现有的鲁棒性定义。

我们首先回顾 (f,κ)-鲁棒性的定义：

定义 2. 设 $f < n/2$和 $\kappa \geq 0$。若对任意向量 $x_1, \ldots, x_n \in \mathbb{R}^d$，以及任意大小为 $n-f$ 的集合 $S \subseteq [n]$，聚合规则 F 满足(f,κ)-鲁棒，则称其为

$$\|F(x_1, \ldots, x_n) - \overline{x}_S\|^2 \leq \frac{\kappa}{|S|} \sum_{i \in S} \|x_i - \overline{x}_S\|^2$$

其中$x_{\underline{S}} = \frac{1}{|S|} \sum_{i \in S} x_i$。我们将 κ 称为鲁棒性系数。

8.1 $(f,\ \kappa)$-鲁棒聚合规则

本节证明，坐标截尾均值（CWTM） [48],Krum [7],几何中位数（GM） [43],和逐坐标中位数（CWMed） [48] 均满足（f， κ）-鲁棒性。

8.1.1 截尾均值

设 $x \in \mathbb{R}^d$，我们用 $[x]_k$表示 x的第 k个坐标。给定输入向量 x_1， ...， $x_n \in \mathbb{R}^d$，令 τ_k表示对 $[n]$ 的一个排列，该排列按照输入向量的第 k个坐标的非降序对其排序，即$[x_{\tau_k(1)}]_k \leq [x_{\tau_k(2)}]_k \leq .. \leq [x_{\tau_k(n)}]_k$。那么， x_1， ...， x_n的坐标截尾均值，记为 CWTM(x_1， ...， x_n)，是$\mathbb{R}^d$ 中的一个向量，其第 k个坐标定义如下：

$$[\text{CWTM}(x_1, \ldots, x_n)]_k \coloneqq \frac{1}{n-2f} \sum_{j=f+1}^{n-f} [x_{\tau_k(j)}]_k.$$

我们首先证明一个通用引理，以简化逐坐标聚合的 (f,κ)-鲁棒性分析：通过将分析简化为标量情形，无需损失一般性。具体来说，我们证明，如果 F 是逐坐标函数，也就是说， F 的每个 k 坐标（记为 F_k）仅取决于输入 $[x_1]_k, \ldots, [x_n]_k$ 中相应的 k 坐标，那么逐坐标鲁棒性就意味着整体鲁棒性。

引理 2. 假设 F： $\mathbb{R}^{d\times n} \to \mathbb{R}^d$ 是一个逐坐标聚合函数，即存在 d 实值函数F_1、.....、 F_d： $\mathbb{R}^n \to \mathbb{R}$，使得对于所有 x_1、.....、 $x_n \in \mathbb{R}^d$， $[F(x_1$、.....、 $x_n)]_k = F_k([x_1]_k$、.....、 $[x_n]_k)$。如果对于每个 $k \in [d]$， F_k都是$(f$， $\kappa)$-鲁棒的，那么 F就是$(f$， $\kappa)$-鲁棒的。

证明。 考虑 n 个属于 $\mathbb{R}^d$、 x_1、.....、 x_n的任意向量，以及满足 $|S| = n - f$的任意集合 $S \subseteq [n]$。假设对于每个 $k \in [d]$， F_k 都是（f， κ）-鲁棒的。由于假设 F是一个逐坐标聚合函数，因此我们有

$$\|F(x_1, \ldots, x_n) - \overline{x}_S\|^2 = \sum_{k=1}^{d} |F_k([x_1]_k, \ldots, [x_n]_k) - [\overline{x}_S]_k|^2 . \tag{4}$$

由于对于每个 $k \in [d]$, F_k 都是 (f, κ)-鲁棒的，因此我们有

$$\sum_{k=1}^{d} |F_k([x_1]_k, \ldots, [x_n]_k) - [\overline{x}_S]_k|^2 \leq \sum_{k=1}^{d} \frac{\kappa}{|S|} \sum_{i \in S} |[x_i]_k - [\overline{x}_S]_k|^2 = \frac{\kappa}{|S|} \sum_{i \in S} \sum_{k=1}^{d} |[x_i]_k - [\overline{x}_S]_k|^2 = \frac{\kappa}{|S|} \sum_{i \in S} \|x_i - \overline{x}_S\|^2 .$$

将上面的结果代入 (4)，即可完成证明。 □

接下来，我们将在下面的引理 3 中证明一个关于实数值排序的重要性质；该性质对于获得截尾均值的紧致 (f, κ)-鲁棒性保证至关重要。

引理 3. 设 n 个实数值 $x_1, \ldots, x_n$ 满足 $x_1 \leq \ldots \leq x_n$。令 $S \subseteq [n]$ 为大小为 $|S| = n - f$ 的集合，且 $I := \{f + 1, \ldots, n - f\}$。我们得到

$$\sum_{i \in I \setminus S} |x_i - \overline{x}_S|^2 \leq \sum_{i \in S \setminus I} |x_i - \overline{x}_S|^2 .$$

证明. 首先注意，由于 $|I| = n - 2f$ 和 $|S| = n - f$， $|I \setminus S| \leq f$ 和 $|S \setminus I| \geq f$。因此， $|I \setminus S| \leq |S \setminus I|$。为证明该引理，我们将证明存在一个单射 ϕ: $I \setminus S \to S \setminus I$，使得

$$\forall i \in I \setminus S, \ |x_i - \overline{x}_S| \leq \left|x_{\phi(i)} - \overline{x}_S\right| . \tag{5}$$

由于 $|I \setminus S| \leq |S \setminus I|$，我们有 $\sum_{i \in I \setminus S} \left|x_{\phi(i)} - \underline{x}_S\right|^2 \leq \sum_{i \in S \setminus I} |x_i - \underline{x}_S|^2$。因此，(5) 证明了该引理。

我们用 B 表示 $[n]$中 S 的补集，即 $B = [n] \setminus S$。因此， $|B| = f$ 和 $I \setminus S = I \cap B$。我们将 $I^+ := \{n - f + 1, \ldots, n\}$ 和 $I^- := \{1, \ldots, f\}$ 分别记为大于（或等于）和小于（或等于） I 中各值的数值所对应的索引。令 $|I \cap B| = q$。由于 $B = [n] \setminus S$，我们得到

$$\left|I^+ \cap S\right| = f - \left|I^+ \cap B\right| \geq f - |B \setminus (I \cap B)| = f - (f - q) = q. \tag{6}$$

类似地，我们得到

$$\left|I^- \cap S\right| \geq q. \tag{7}$$

回顾一下， $q = |I \cap B|$ 其中 $I \setminus S = I \cap B$。因此，由于 (6) 和 (7)，存在一个从 $I \setminus S$ 到 $(I^- \cap S) \times (I^+ \cap S)$ 的单射。令 ψ 为这样一个单射。对于每个 $i \in I \setminus S$， $\psi(i)$ 是一对，记作 $(\psi^-(i) \ \psi^+(i))$，属于 $(I^- \cap S) \times (I^+ \cap S)$。考虑任意一个 $i \in I \setminus S$。根据 I^- 和 I^+的定义，我们有

$$x_{\psi^-(i)} \leq x_i \leq x_{\psi^+(i)}.$$

因此，对于任意实数值 y,

$$|x_i - y| \leq \max\left\{\left|x_{\psi^+(i)} - y\right|, \left|x_{\psi^-(i)} - y\right|\right\}.$$

以上证明了 (5)， 其中，单射 ϕ 定义为 $\phi(i) = \arg\max_{j \in \{\psi^+(i) \ \psi^-(i)\}} |x_j - x_S|$，对所有$i \in I \setminus S$均成立 .

□

现在我们证明下述命题中截尾均值的 (f, κ)-鲁棒性。

命题 2. 设 $n \in \mathbb{N}^*$ 和 $f < n/2$。*CWTM* 是(f, κ)-鲁棒的，且满足 $\kappa = \frac{6f}{n-2f}\left(1 + \frac{f}{n-2f}\right)$。

证明。 首先，注意到截尾均值 Trimmed Mean 是一种逐坐标聚合，其定义见引理 2。因此，根据引理 2，只需证明截尾均值 Trimmed Mean 在标量域中是 (f,κ)-鲁棒的，即当 $d=1$ 时成立。

令 $x_1,\ldots,x_n\in\mathbb{R}$，不失一般性，假设 $x_1\leq\ldots\leq x_n$。记 $I:=\{f+1,\ldots,n-f\}$，并令 S 为 $[n]$ 的任意一个大小为 $n-f$ 的子集。回顾一下，TM $(x_1,\ldots,x_n)$ 所选取的索引集合为 $=\frac{1}{n-2f}\sum_{i\in I}x_i$。由此得到

$$\begin{aligned}
|\mathrm{CWTM}(x_1,\ldots,x_n)-\overline{x}_S|^2 &= \left|\frac{1}{n-2f}\sum_{i\in I}x_i-\overline{x}_S\right|^2=\left|\frac{1}{n-2f}\sum_{i\in I}(x_i-\overline{x}_S)\right|^2\\
&=\left|\frac{1}{n-2f}\sum_{i\in I}(x_i-\overline{x}_S)-\frac{1}{n-2f}\sum_{i\in S}(x_i-\overline{x}_S)\right|^2 \qquad \left(\text{as }\sum_{i\in S}(x_i-\overline{x}_S)=0\right)\\
&=\frac{1}{(n-2f)^2}\left|\sum_{i\in I\setminus S}(x_i-\overline{x}_S)-\sum_{i\in S\setminus I}(x_i-\overline{x}_S)\right|^2.
\end{aligned}$$

利用上面的詹森不等式，我们得到

$$|\mathrm{CWTM}(x_1,\ldots,x_n)-\overline{x}_S|^2\leq\frac{|I\setminus S|+|S\setminus I|}{(n-2f)^2}\left(\sum_{i\in I\setminus S}|x_i-\overline{x}_S|^2+\sum_{i\in S\setminus I}|x_i-\overline{x}_S|^2\right).$$

注意，$|I\setminus S|=|I\cup S|-|S|\leq n-(n-f)=f$。类似地，$|S\setminus I|=|I\cup S|-|I|\leq n-(n-2f)=2f$。因此，$|I\setminus S|+|S\setminus I|\leq 3f$。所以，我们有

$$|\mathrm{CWTM}(x_1,\ldots,x_n)-\overline{x}_S|^2\leq\frac{3f}{(n-2f)^2}\left(\sum_{i\in I\setminus S}|x_i-\overline{x}_S|^2+\sum_{i\in S\setminus I}|x_i-\overline{x}_S|^2\right).$$

回顾引理 3，$\sum_{i\in I\setminus S}|x_i-x_S|^2\leq\sum_{i\in S\setminus I}|x_i-x_S|^2$。利用上述事实，我们得到

$$|\mathrm{CWTM}(x_1,\ldots,x_n)-\overline{x}_S|^2\leq\frac{6f}{(n-2f)^2}\sum_{i\in S\setminus I}|x_i-\overline{x}_S|^2\leq\frac{6f}{(n-2f)^2}\sum_{i\in S}|x_i-\overline{x}_S|^2.$$

最后，由于 $\frac{f}{(n-2f)^2}=\frac{f}{(n-f)}\frac{1}{(n-2f)^2}\left(\frac{1}{n-f}\right)=\left(\frac{f}{n-2f}+\left(\frac{f}{n-2f}\right)^2\right)\frac{1}{n-f}$，我们得到

$$|\mathrm{CWTM}(x_1,\ldots,x_n)-\overline{x}_S|^2\leq 6\left(\frac{f}{n-2f}+\left(\frac{f}{n-2f}\right)^2\right)\frac{1}{|S|}\sum_{i\in S}|x_i-\overline{x}_S|^2. \tag{8}$$

以上完成了证明。 □

8.1.2 Krum

本节将研究一种对 Krum 算法的轻微改进，该算法最初在 [7] 中提出。基本上，给定输入向量$x_1,\ldots,x_n$，Krum 会丢弃 f（而非原始版本中的 $f+1$）个最远的向量，并输出与其最近邻最接近的向量。具体而言，我们将 $\mathcal{N}_j$ 记为 x_j 在 $\{x_1,\ldots,x_n\}$ 中的 $n-f$ 个最近邻的索引集合，遇到并列时任意打破平局。Krum 输出满足以下条件的向量 x_{k^*}

$$k^*\in\operatorname*{arg\,min}_{j\in[n]}\sum_{i\in\mathcal{N}_j}\|x_j-x_i\|^2,$$

如果上述最小化集合中包含多个元素，则可任意打破平局。

命题3. 设 $n\in\mathbb{N}^*$ 和 $f<n/2$。*Krum* 是(f,κ)-鲁棒的，其中 $\kappa=6(1+\frac{f}{n-2f})$。

证明。设 $n \in \mathbb{N}$、 $f < n/2$和 $x_1, \ldots, x_n \in \mathbb{R}^d$。考虑任意一个大小为 $|S| = n - f$ 的子集 $S \subseteq [n]$。下文中，对于每个 $j \in [n]$，我们将 $\mathcal{N}_j$ 记为 $\{x_1, \ldots, x_n\}$ 中 x_j 的 $n - f$ 个最近邻对应的索引集合，遇到并列时任意打破。注意，这意味着对于每个 $j \in [n]$，

$$\sum_{i \in \mathcal{N}_j} \|x_j - x_i\|^2 \leq \sum_{i \in S} \|x_j - x_i\|^2 . \tag{9}$$

令 $k^* \in [n]$ 表示 Krum 选出的索引。根据定义，有 $k^* \in \arg\min_{j \in [n]} \sum_{i \in \mathcal{N}_j} \|x_j - x_i\|^2$. 因此，利用（9）可得

$$\begin{aligned}
\sum_{i \in \mathcal{N}_{k^*}} \|x_{k^*} - x_i\|^2 &= \min_{j \in [n]} \sum_{i \in \mathcal{N}_j} \|x_j - x_i\|^2 \leq \min_{j \in S} \sum_{i \in \mathcal{N}_j} \|x_j - x_i\|^2 \leq \frac{1}{|S|} \sum_{j \in S} \sum_{i \in \mathcal{N}_j} \|x_j - x_i\|^2 \\
&\leq \frac{1}{|S|} \sum_{j \in S} \sum_{i \in S} \|x_j - x_i\|^2 = \frac{1}{|S|} \sum_{i,j \in S} \|x_j - \overline{x}_S - (x_i - \overline{x}_S)\|^2 \\
&= \frac{1}{|S|} \sum_{i,j \in S} \Big(\|x_j - \overline{x}_S\|^2 + \|x_i - \overline{x}_S\|^2 - 2 \langle x_j - \overline{x}_S, x_i - \overline{x}_S \rangle \Big) \\
&= \frac{1}{|S|} \Big[\sum_{i,j \in S} \|x_j - \overline{x}_S\|^2 + \sum_{i,j \in S} \|x_i - \overline{x}_S\|^2 - 2 \sum_{i,j \in S} \langle x_j - \overline{x}_S, x_i - \overline{x}_S \rangle \Big] \\
&= \frac{1}{|S|} \Big[2\,|S| \sum_{i \in S} \|x_i - \overline{x}_S\|^2 - 2 \sum_{i,j \in S} \langle x_j - \overline{x}_S, x_i - \overline{x}_S \rangle \Big] \\
&= \frac{1}{|S|} \Big[2\,|S| \sum_{i \in S} \|x_i - \overline{x}_S\|^2 - 2 \sum_{i \in S} \Big\langle \underbrace{\sum_{j \in S} (x_j - \overline{x}_S)}_{=0}, x_i - \overline{x}_S \Big\rangle \Big] = 2 \sum_{i \in S} \|x_i - \overline{x}_S\|^2 .
\end{aligned} \tag{10}$$

现在，利用詹森不等式，对于所有 $i \in S$，我们可以写成

$$\|x_{k^*} - \overline{x}_S\|^2 \leq 2 \|x_{k^*} - x_i\|^2 + 2 \|x_i - \overline{x}_S\|^2 .$$

因此，通过重新排列各项，对于所有 $i \in S$，我们有

$$\|x_{k^*} - x_i\|^2 \geq \frac{1}{2} \|x_{k^*} - \overline{x}_S\|^2 - \|x_i - \overline{x}_S\|^2 .$$

结合 $|S \cap \mathcal{N}_{k^*}| = |S| + |\mathcal{N}_{k^*}| - |S \cup \mathcal{N}_{k^*}| \geq (n - f) + (n - f) - n = n - 2f$ 这一事实，前述不等式意味着

$$\begin{aligned}
\sum_{i \in \mathcal{N}_{k^*}} \|x_{k^*} - x_i\|^2 &\geq \sum_{i \in S \cap \mathcal{N}_{k^*}} \|x_{k^*} - x_i\|^2 \geq |S \cap \mathcal{N}_{k^*}| \, \frac{1}{2} \|x_{k^*} - \overline{x}_S\|^2 - \sum_{i \in S \cap \mathcal{N}_{k^*}} \|x_i - \overline{x}_S\|^2 \\
&\geq \frac{n - 2f}{2} \|x_{k^*} - \overline{x}_S\|^2 - \sum_{i \in S \cap \mathcal{N}_{k^*}} \|x_i - \overline{x}_S\|^2 .
\end{aligned}$$

通过重新排列各项，并利用 (10)，我们可以写成

$$\begin{aligned}
\|x_{k^*} - \overline{x}_S\|^2 &\leq \frac{2}{n - 2f} \left[\sum_{i \in \mathcal{N}_{k^*}} \|x_{k^*} - x_i\|^2 + \sum_{i \in S \cap \mathcal{N}_{k^*}} \|x_i - \overline{x}_S\|^2 \right] \\
&\leq \frac{2}{n - 2f} \left[\sum_{i \in \mathcal{N}_{k^*}} \|x_{k^*} - x_i\|^2 + \sum_{i \in S} \|x_i - \overline{x}_S\|^2 \right] \\
&\leq \frac{2}{n - 2f} \left[2 \sum_{i \in S} \|x_i - \overline{x}_S\|^2 + \sum_{i \in S} \|x_i - \overline{x}_S\|^2 \right] \\
&= \frac{6}{n - 2f} \sum_{i \in S} \|x_i - \overline{x}_S\|^2 = \frac{6(n - f)}{n - 2f} \frac{1}{|S|} \sum_{i \in S} \|x_i - \overline{x}_S\|^2 .
\end{aligned}$$

最后，我们指出 $\frac{n-f}{n-2f} = 1 + \frac{f}{n-2f}$。 —— □

8.1.3 几何中位数

x_1、……、 $x_n \in \mathbb{R}^d$ 的几何中位数，记作 GM(x_1、……、 x_n)，定义为使其到这些向量的 ℓ_2-距离之和最小的向量。具体而言，我们有

$$\mathrm{GM}(x_1, \ldots, x_n) \in \arg\min_{y \in \mathbb{R}^d} \sum_{i=1}^{n} \|y - x_i\| .$$

命题 4。 设 $n \in \mathbb{N}^*$ 和 $f < n/2$。*GM* 是(f， κ)-鲁棒的，其中 $\kappa = 4\left(1 + \frac{f}{n-2f}\right)^2$。

证明。 证明与 [26] 中对几何中位数的分析类似。为完整起见，我们给出根据（f， κ）-鲁棒性的定义改写后的完整证明。记 $x^* :=$ GM(x_1、 ……、 x_n) 为输入向量的几何中位数。考虑任意一个大小为 $|S| = n - f$ 的子集 $S \subseteq [n]$。根据反三角不等式，对于任意 $i \in S$，我们有

$$\|x^* - x_i\| \geq \|x^* - \overline{x}_S\| - \|x_i - \overline{x}_S\| . \tag{11}$$

同理，对于任意 $i \in [n] \setminus S$，我们得到

$$\|x^* - x_i\| \geq \|x_i - \overline{x}_S\| - \|x^* - \overline{x}_S\| . \tag{12}$$

对所有输入向量将 (11) 和 (12) 求和，我们得到

$$\sum_{i \in [n]} \|x^* - x_i\| \geq (n - 2f) \|x^* - \overline{x}_S\| + \sum_{i \in [n] \setminus S} \|x_i - \overline{x}_S\| - \sum_{i \in S} \|x_i - \overline{x}_S\| .$$

重新排列各项后，我们得到

$$\|x^* - \overline{x}_S\| \leq \frac{1}{n-2f} \left(\sum_{i \in [n]} \|x^* - x_i\| - \sum_{i \in [n] \setminus S} \|x_i - \overline{x}_S\| + \sum_{i \in S} \|x_i - \overline{x}_S\| \right)$$

注意，根据几何中位数的定义，我们有

$$\sum_{i \in [n]} \|x^* - x_i\| \leq \sum_{i \in [n]} \|\overline{x}_S - x_i\| .$$

因此，

$$\|x^* - \overline{x}_S\| \leq \frac{1}{n-2f} \left(\sum_{i \in [n]} \|x_i - \overline{x}_S\| - \sum_{i \in [n] \setminus S} \|x_i - \overline{x}_S\| + \sum_{i \in S} \|x_i - \overline{x}_S\| \right) \leq \frac{2}{n-2f} \sum_{i \in S} \|x_i - \overline{x}_S\| .$$

两边平方并应用詹森不等式后，我们得到

$$\begin{aligned} \|x^* - \overline{x}_S\|^2 &\leq \frac{4(n-f)}{(n-2f)^2} \sum_{i \in S} \|x_i - \overline{x}_S\|^2 = \frac{4(n-f)^2}{(n-2f)^2} \cdot \frac{1}{n-f} \sum_{i \in S} \|x_i - \overline{x}_S\|^2 \\ &= 4\left(1 + \frac{f}{n-2f}\right)^2 \frac{1}{|S|} \sum_{i \in S} \|x_i - \overline{x}_S\|^2 . \end{aligned}$$

这就是期望的结果。 □

8.1.4 中位数

对于输入向量 x_1、.....、 x_n，其逐坐标中位数记作 CWMed(x_1、.....、 x_n)，定义为一个向量；对于所有 $k \in [d]$，其 k 个坐标定义为

$$[\mathrm{CWMed}\,(x_1, \ldots, x_n)]_k \coloneqq \mathrm{Median}\,([x_1]_k, \ldots [x_n]_k)\,. \tag{13}$$

命题 5. 设 $n \in \mathbb{N}^*$ 和 $f < n/2$。*CWMed* 是（f， κ）-鲁棒的，且满足 $\kappa = 4\left(1 + \frac{f}{n-2f}\right)^2$。

证明。 鉴于对于一维输入，几何中位数与中位数一致，根据命题 4 可知，对于一维输入，中位数是 (f， κ)-鲁棒的，且满足 $\kappa = 4\left(1 + \frac{f}{n-2f}\right)^2$。由于中位数是逐坐标计算的，我们根据引理 2 推知，这一结论对任意 d维输入均成立，从而完成证明。

□

8.2 下界

本节将通过在命题 6 中证明关于 κ 的普适下界，并在命题 7 中证明特定聚合规则的下界，来确立我们分析的紧确性。

Pr命题 6. 设 $n \in \mathbb{N}^*$、 $f < n$和 $\kappa > 0$。若 F是 (f, κ)-鲁棒的，则 $n > 2f$和 $\kappa \geq \frac{f}{n-2f}$。

证明。 设 $n \in \mathbb{N}^*, f < n$和 $\kappa > 0$。假设 F是 (f, κ)-弹性平均聚合规则。考虑满足 $x_1 = \ldots = x_{n-f} = 0$和 $x_{n-f+1} = \ldots = x_n = 1$的 $x_1, \ldots, x_n$。首先考虑集合 $S_0 = \{1, \ldots, n-f\}$。由于$|S_0| = n - f$，根据定义，我们有

$$\left|F(x_1, \ldots, x_n) - \overline{x}_{S_0}\right|^2 \leq \kappa \frac{1}{n-f} \sum_{i \in S_0} \left|x_i - \overline{x}_{S_0}\right|^2 = 0.$$

因此， $F(x_1, \ldots, x_n) = \overline{x}_{S_0} = 0$。

现在，考虑另一个集合 $S_1 = \{f+1, \ldots, n\}$。注意，我们必然有 $n > 2f$。反设 $2f \geq n$，即 $f + 1 \geq n - f + 1$。这意味着，对于每个 $i \in S_1$，都有 $x_i = 1$。因此， $x_{S_1} = 1$。又由于 F是 (f, κ)-鲁棒的，我们必有

$$\left|F(x_1, \ldots, x_n) - \overline{x}_{S_1}\right|^2 \leq \kappa \frac{1}{n-f} \sum_{i \in S_1} \left|x_i - \overline{x}_{S_1}\right|^2.$$

因此， $0 = x_{S_0} = F(x_1, \ldots, x_n) = \overline{x}_{S_1} = 1$，这就产生了矛盾。

因此，我们必须有 $n > 2f$。这意味着 $x_{S_1} = \frac{f}{n-f}$。于是，

$$\left|F(x_1, \ldots, x_n) - \overline{x}_{S_1}\right|^2 = \left(\frac{f}{n-f}\right)^2. \tag{14}$$

由于 F 是 (f， κ)-抗故障平均规则，我们有

$$\begin{aligned}
\left|F(x_1, \ldots, x_n) - \overline{x}_{S_1}\right|^2 \leq \kappa \frac{1}{n-f} \sum_{i \in S_1} \left|x_i - \overline{x}_{S_1}\right|^2 &= \frac{\kappa}{n-f}\left((n-2f)\left|0 - \frac{f}{n-f}\right|^2 + f\left|1 - \frac{f}{n-f}\right|^2\right) \\
&= \frac{\kappa}{n-f}\left((n-2f)\frac{f^2}{(n-f)^2} + f\frac{(n-2f)^2}{(n-f)^2}\right) \\
&= \frac{\kappa f(n-2f)}{n-f}\left(\frac{f + n - 2f}{(n-f)^2}\right) = \kappa\frac{f(n-2f)}{(n-f)^2}.
\end{aligned}$$

将此不等式代回式 (14)，我们得出 $\kappa \geq \frac{f}{n-2f}$。 □

命题 7. 设 $n \in \mathbb{N}^*, f \geq 1$满足 $n > 2f$，且 $\kappa \geq 0$。对于任意 $F \in \{$几何中位数、*CWMed*、*Krum*$\}$，若 F是(f, κ)-鲁棒的，则 $\kappa \in \Omega(1)$。

证明。设 $n \in \mathbb{N}^*, f \geq 1$ 满足 $n > 2f$ 和 $\kappa \geq 0$。令 $F \in \{$几何中位数,CWMed,Krum$\}$。我们将证明，若 F 是(f, κ)-鲁棒的，则存在一个绝对常数 $c > 0$，使得 $\kappa \geq c$。

考虑 $x_1, \ldots, x_n \in \mathbb{R}$，使得 $x_1, \ldots, x_{\lfloor \frac{n-f}{2} \rfloor} = -1$，并且 $x_{\lfloor \frac{n-f}{2} \rfloor + 1}, \ldots, x_{n-f} = 1$。此外，我们设定 $x_{n-f+1}, \ldots, x_n = 1$。注意，由于 $f \geq 1$，取值为 1 的输入构成严格多数：此类输入的数量为 $\left(n - f - \left\lfloor \frac{n-f}{2} \right\rfloor\right) + f = \left\lceil \frac{n-f}{2} \right\rceil + f \geq \left\lfloor \frac{n-f}{2} \right\rfloor + f > \left\lfloor \frac{n-f}{2} \right\rfloor$。

此外，回想一下，通过设置 $S = \{1, \ldots, n-f\}$，任何 (f, κ)-鲁棒函数 F 都应满足

$$\left|F(x_1, \ldots, x_n) - \overline{x}_S\right|^2 \leq \kappa \, \frac{1}{n-f} \sum_{i \in S} \left|x_i - \overline{x}_S\right|^2 . \tag{15}$$

然而，平均值 x_S 等于

$$\begin{aligned} \overline{x}_S &= \frac{1}{n-f} \sum_{i \in S} x_i = \frac{1}{n-f} \left[\left\lfloor \frac{n-f}{2} \right\rfloor \times (-1) + \left(n - f - \left\lfloor \frac{n-f}{2} \right\rfloor \right) \times (+1) \right] \\ &= \frac{1}{n-f} \left(n - f - 2 \left\lfloor \frac{n-f}{2} \right\rfloor \right) = \begin{cases} 0 & \text{if } n-f \text{ is even,} \\ \frac{1}{n-f} & \text{if } n-f \text{ is odd.} \end{cases} \end{aligned} \tag{16}$$

此外，经验平均值 $\frac{1}{n-f} \sum_{i \in S} \left|x_i - x_S\right|^2$ 等于

$$\begin{aligned} \frac{1}{n-f} \sum_{i \in S} \left|x_i - \overline{x}_S\right|^2 &= \frac{1}{n-f} \sum_{i \in S} \left(x_i^2 + \overline{x}_S^2 - 2 x_i \overline{x}_S \right) = \frac{1}{n-f} \sum_{i \in S} x_i^2 - \overline{x}_S^2 \\ &= 1 - \overline{x}_S^2 = \begin{cases} 1 & \text{if } n-f \text{ is even,} \\ 1 - \left(\frac{1}{n-f} \right)^2 & \text{if } n-f \text{ is odd.} \end{cases} \end{aligned} \tag{17}$$

现在，注意到对于每个 $F \in \{$GM、CWMed、Krum$\}$，$F(x_1, \ldots, x_n)$ 的值都等于 1。事实上，由于 $f \geq 1$，严格多数的输入取值为 1，而其余输入取值为 -1。还要回想一下，一维时 GM 与 CWMed 完全相同。

将此代入 (15)，利用 (16) 和 (17)，并重新整理各项后，我们对每个 $F \in \{$GM、CWMed、Krum$\}$ 得到

$$\kappa \geq \frac{\left|F(x_1, \ldots, x_n) - \overline{x}_S\right|^2}{\frac{1}{n-f} \sum_{i \in S} \left|x_i - \overline{x}_S\right|^2} = \frac{\left|1 - \overline{x}_S\right|^2}{\frac{1}{n-f} \sum_{i \in S} \left|x_i - \overline{x}_S\right|^2} = \begin{cases} 1 & \text{if } n-f \text{ is even,} \\ \frac{\left|1 - \frac{1}{n-f}\right|^2}{1 - \left(\frac{1}{n-f}\right)^2} & \text{if } n-f \text{ is odd.} \end{cases} \tag{18}$$

但请注意，$\frac{\left|1 - \frac{1}{n-f}\right|^2}{1 - \left(\frac{1}{n-f}\right)^2} = \frac{1 - \frac{1}{n-f}}{1 + \frac{1}{n-f}} = \frac{n-f-1}{n-f+1} = 1 - \frac{2}{n-f+1}$。由于 $f \geq 1$，因此 $n \geq 2f + 1 \geq 3$，进而 $1 - \frac{2}{n-f+1} \geq \frac{1}{3}$。所以，对于 (18) 中的两种情况，我们对每个 $F \in \{$GM、CWMed、Krum$\}$ 都有 $\kappa \geq \frac{1}{3}$。证明至此完成。 □

现在可以看出，表1中给出的鲁棒性系数在数量级上是紧的。假设 $n \geq (2 + \nu)f$，其中 $\nu > 0$ 是某个绝对常数。CWTM 的系数为 $\mathcal{O}\left(\frac{f}{n-2f}\right)$ 量级，根据命题 6，这是最优的。CWMed、几何中位数和 Krum 的系数为 $\mathcal{O}(1)$ 量级，根据命题 7，这是最优的。

8.3 统一鲁棒性定义

在本节中，我们证明 $(f,\ \kappa)$-鲁棒性统一了文献中现有的鲁棒性定义 [17, 26]。具体而言，我们证明，验证我们的定义即可推出验证其他定义。这背后的原因是，在 $(f,\ \kappa)$-鲁棒性中，与现有研究相比，我们将估计平均值时的误差控制在一个更小的量上。

8.3.1 (f,λ)-容错平均

回顾下方给出的（f,λ）-容错平均的定义 [17] 。

定义 3（$(f,\ \lambda)$-容错平均）。对于 $f<n$ 和实数值 $\lambda\geq 0$，若聚合规则 F 满足：对于任意一组 n 个向量 x_1、.....、 x_n，以及任意大小为 $n-f$ 的集合 $S\subseteq\{1,\ldots,n\}$，

$$\|F(x_1,\ldots,\ x_n)-\overline{x}_S\|\leq\lambda\max_{i,j\in S}\|x_i-x_j\|\,,$$

其中 $x_S:=\frac{1}{|S|}\sum_{i\in S}x_i$，且 $|S|$ 是 S的基数。

下面的命题表明，(f,κ)-鲁棒性意味着 (f,λ)-弹性平均。

命题 8。 设 $n\in\mathbb{N}^*, f<n$ 和 $\kappa>0$。若 F 是 (f,κ)-鲁棒的，则 F 是 (f,λ)-弹性的，其中 $\lambda=\sqrt{\kappa/2}$.

证明。 设 $n\in\mathbb{N}^*, f<n$ 和 $\lambda,\kappa>0$。设 $x_1,\ldots,x_n\in\mathbb{R}^d$ 和 $S\subseteq\{1,\ldots,n\}$，使得 $|S|=n-f$。
若 F 是 (f,κ)-鲁棒的，则有

$$\|F(x_1,\ldots,x_n)-\overline{x}_S\|^2\leq\kappa\frac{1}{n-f}\sum_{i\in S}\|x_i-\overline{x}_S\|^2=\kappa\frac{1}{2(n-f)^2}\sum_{i,j\in S}\|x_i-x_j\|^2\leq\frac{\kappa}{2}\max_{i,j\in S}\|x_i-x_j\|^2\,. \tag{19}$$

上面的等式由以下事实得出

$$\begin{aligned}
\frac{1}{2(n-f)^2}\sum_{i,j\in S}\|x_i-x_j\|^2&=\frac{1}{2(n-f)^2}\sum_{i,j\in S}\|x_i-\overline{x}_S+\overline{x}_S-x_j\|^2\\
&=\frac{1}{2(n-f)^2}\sum_{i,j\in S}\Big(\|x_i-\overline{x}_S\|^2+\|\overline{x}_S-x_j\|^2-2(x_i-\overline{x}_S)(x_j-\overline{x}_S)\Big)\\
&=\frac{1}{2(n-f)^2}\left[(n-f)\sum_{i\in S}\|x_i-\overline{x}_S\|^2+(n-f)\sum_{j\in S}\|\overline{x}_S-x_j\|^2\right]\\
&\quad-\frac{1}{(n-f)^2}\sum_{i,j\in S}(x_i-\overline{x}_S)(x_j-\overline{x}_S)\\
&=\frac{1}{n-f}\sum_{i\in S}\|x_i-\overline{x}_S\|^2-\frac{1}{(n-f)^2}\sum_{i\in S}(x_i-\overline{x}_S)\underbrace{\sum_{j\in S}(x_j-\overline{x}_S)}_{=0}\\
&=\frac{1}{n-f}\sum_{i\in S}\|x_i-\overline{x}_S\|^2\,.
\end{aligned} \tag{20}$$

对式 (19) 两边开平方，证明即告完成。 □

作为命题 8 的推论，我们可以衡量相较于 [17] 中对聚合规则的分析所取得的显著改进。例如， [17] 中为 CWMed 证明的系数 λ 为 $2\sqrt{n}(n-f)\min\{2\sqrt{n-f},\sqrt{d}\}$，它要么随维度增长，要么为 $\sqrt{n}$。相比之下，命题 8 表明，我们的分析得出的系数为 $\lambda=\sqrt{\kappa}/2=\sqrt{2}\left(1+\frac{f}{n-2f}\right)$；只要存在某个 $\nu>0$ 使得 $n\geq(2+\nu)f$，该系数就是有界的。对 CWTM 也可以得出类似的结论。

8.3.2 $(\delta_{\max}, c)$-无先验鲁棒聚合

下面回顾无先验鲁棒聚合器（ARAgg）[26] 的定义。请注意，在原始定义中，所谓的"良好"子集（$\delta_{\max}$，c）-ARAgg [26] 只需满足其大小为 $|S| \geq (1-\delta)n$，其中 δ 是拜占庭工作节点所占比例的上界。在我们的形式化表述中，f 是拜占庭工作节点的实际数量，因此不失一般性，我们直接要求 $|S| = n - f$。

定义 4 ($(\delta_{\max}, c)$-**ARAgg**)。给定输入 $X_1, \ldots, X_n$，使得存在子集 S、$|S| = n - f$，且 $\frac{f}{n} \leq \delta_{max} < 0.5$ 满足：对于所有 i、$j \in S$，$\mathbb{E}\left[\|X_i - X_j\|^2\right] \leq \rho^2$。然后，$(\delta_{max}, c)$-*ARAgg* 的输出 $\hat{X}$ 满足 $\mathbb{E}\left[\left\|\hat{X} - \overline{X}_S\right\|^2\right] \leq c\,\frac{f}{n}\rho^2$。

下面的命题表明，(f, κ)-鲁棒性意味着 $(\delta_{\max}, c)$-无先验鲁棒聚合。我们还将证明，要在 $c = \mathcal{O}(1)$ 的条件下获得 $(\delta_{\max}, c)$-无先验鲁棒聚合，尽管 [26], 中没有这样的理论要求，但只需满足 $\kappa \in \mathcal{O}\left(\frac{f}{n-2f}\right)$ 即可。

命题 9. 令 $n \in \mathbb{N}^*$、$0 < f < n/2$、$\kappa > 0$ 和 $\frac{f}{n} \leq \delta_{max} < \frac{1}{2}$。若 F 是(f, κ)-鲁棒的，则 F 是(δ_{max}, c)-*ARAgg*，且$c = \kappa\,\frac{n}{2f}$。此外，若 $\kappa \in \mathcal{O}\left(\frac{f}{n-2f}\right)$，则 $c = \mathcal{O}(1)$。

证明。令 $n \in \mathbb{N}^*$、$0 < f < n/2$、$\kappa > 0$ 和 $0 < \delta_{\max} < \frac{1}{2}$。假设 F 是 (f, κ)-鲁棒的。考虑任意满足 $|S| = n - f$ 的 $x_1, \ldots, x_n \in \mathbb{R}^d$ 和 $S \subseteq [n]$。

由于 F 是 (f, κ)-鲁棒的，根据 (20)，我们有

$$\|F(x_1, \ldots, x_n) - \overline{x}_S\|^2 \leq \frac{\kappa}{n-f} \sum_{i \in S} \|x_i - \overline{x}_S\|^2 = \frac{\kappa}{2(n-f)^2} \sum_{i,j \in S} \|x_i - x_j\|^2 . \tag{21}$$

对于任意随机变量 $X_1, \ldots, X_n$，以这些变量的联合概率测度对 (21) 积分，得到

$$\begin{aligned}\mathbb{E}\left[\left\|F(X_1, \ldots, X_n) - \overline{X}_S\right\|^2\right] &\leq \frac{\kappa}{2}\,\mathbb{E}\left[\frac{1}{(n-f)^2} \sum_{i,j \in S} \|X_i - X_j\|^2\right] = \frac{\kappa}{2}\frac{1}{|S|^2} \sum_{i,j \in S} \mathbb{E}\left[\|X_i - X_j\|^2\right] \\ &\leq \frac{\kappa}{2} \max_{i,j \in S} \mathbb{E}\left[\|X_i - X_j\|^2\right] = c\,\frac{f}{n} \max_{i,j \in S} \mathbb{E}\left[\|X_i - X_j\|^2\right] . \end{aligned} \tag{22}$$

其中 $c := \kappa\,\frac{n}{2f}$。因此，如果 $X_1, \ldots, X_n$ 满足存在一个子集 $S \subseteq [n], |S| = n - f,$，使得对于所有 $i, j \in S$，都有 $\mathbb{E}\left[\|X_i - X_j\|^2\right] \leq \rho^2$。那么，有 $\rho^2 \geq \max_{i,j \in S} \mathbb{E}\left[\|X_i - X_j\|^2\right]$。结合 (22)，这一事实即可得出所需结果；即，

$$\mathbb{E}\left[\left\|F(X_1, \ldots, X_n) - \overline{X}_S\right\|^2\right] \leq c\,\frac{f}{n}\rho^2.$$

此外，如果 $\kappa = \mathcal{O}\left(\frac{f}{n-2f}\right)$，那么我们可以写成 $\kappa \leq 2m(1 - 2\delta_{\max})\,\frac{f}{n-2f}$，其中 $m > 0$ 是某个绝对常数，因为 $\delta_{\max} \in (0, 1/2)$。然而，由于 $\frac{f}{n} \leq \delta_{\max}$，且 $\delta \mapsto \frac{2\delta}{1-2\delta}$ 非递减，我们有 $\frac{f}{n-2f} = \frac{f}{n}(1 + \frac{2f}{n-2f}) \leq \frac{f}{n}(1 + \frac{2\delta_{\max}}{1-2\delta_{\max}})$，因此 $\kappa \leq 2m(1 - 2\delta_{\max})\,\frac{f}{n-2f} \leq 2m\,\frac{f}{n}$。由此可得 $c = \kappa\,\frac{n}{2f} \leq m = \mathcal{O}(1)$。证明至此完成。 □

与 [26] 对 CWMed 和 Krum 的分析相比，我们的分析有所改进。对于 CWMed，他们的收敛速率依赖于维度，而我们的不依赖。对于 Krum，他们仅在假设 $n > 4f$ 的情况下证明了鲁棒性，而我们的分析适用于 $n > 2f$。

9 引理1的证明：NNM分析

9.1 证明概述

引理 1 的证明基于这样一个观察：NNM 会使输入更接近真实均值。这一点在引理5中得到了形式化，我们证明经验方差按 f/n 的量级缩小了。请注意，尽管 NNM 的输出方差小于原始输入的方差，但其平均值可能偏离原始平均值。随后，在引理 1 的证明中，我们控制了 NNM 操作引入的这一偏差，并利用引理5中证明的缩减结果得出结论。

符号约定。 下文中，对于每个集合 $S \subseteq [n]$ 以及任意向量 $x_1, \ldots, x_n \in \mathbb{R}^d$，我们将 x_S 记作$\frac{1}{|S|}\sum_{i\in S} x_i$的平均值。令 $\mu \in \mathbb{R}^d$。我们将 y_μ 记作 μ 在 $\{x_1, \ldots, x_n\}$中的 $n-f$ 个最近邻的平均值：

$$y_\mu \coloneqq \frac{1}{|\mathcal{N}_\mu|} \sum_{i\in\mathcal{N}_\mu} x_i,$$

其中， $\mathcal{N}_\mu \subseteq \{1, \ldots, n\}, |\mathcal{N}_\mu| = n-f$ 是 μ的 $n-f$ 个最近邻的索引集合。

9.2 辅助引理的证明

我们首先证明一个一般性引理，以便利用围绕枢轴 μ 的 $(x_i)_{i\in S}$ 离散程度，控制最近邻均值 y_μ 与真实均值 x_S 之间的距离。

引理4。 设 $n \in \mathbb{N}^*$、 $f < n$ 和 $\mu \in \mathbb{R}^d$。对于任意集合 $S \subseteq \{1, \ldots, n\}$、 $|S| = n-f$，对任意向量 x_1、…、$x_n \in \mathbb{R}^d$，有

$$\|y_\mu - \overline{x}_S\|^2 \leq \frac{4f}{n-f}\frac{1}{|S|}\sum_{i\in S}\|x_i - \mu\|^2.$$

证明。 设 $n \in \mathbb{N}^*$、 $f < n$、 $\mu \in \mathbb{R}^d$、 x_1、…、 $x_n \in \mathbb{R}^d$，以及 $S \subseteq \{1, \ldots, n\}$、 $|S| = n-f$。回顾一下，根据定义，我们有 $y_\mu = \frac{1}{n-f}\sum_{i\in\mathcal{N}_\mu} x_i$，其中 $\mathcal{N}_\mu \subseteq \{1, \ldots, n\}$， $|\mathcal{N}_\mu| = n-f$，是 μ 的 $n-f$ 个最近邻对应的索引集合。于是有

$$\begin{aligned}\|y_\mu - \overline{x}_S\|^2 &= \left\|\frac{1}{n-f}\sum_{i\in\mathcal{N}_\mu} x_i - \frac{1}{n-f}\sum_{i\in S} x_i\right\|^2 = \frac{1}{(n-f)^2}\left\|\sum_{i\in\mathcal{N}_\mu} x_i - \sum_{i\in S} x_i\right\|^2 \\ &= \frac{1}{(n-f)^2}\left\|\sum_{i\in\mathcal{N}_\mu\setminus S} x_i - \sum_{i\in S\setminus\mathcal{N}_\mu} x_i\right\|^2.\end{aligned}$$

注意到，由于 $|S| = |\mathcal{N}_\mu| = n-f$，我们有 $|S\setminus\mathcal{N}_\mu| = |\mathcal{N}_\mu\setminus S| = |S\cup\mathcal{N}_\mu| - |S| \leq n-(n-f) \leq f$。因此，应用詹森不等式可得

$$\begin{aligned}\|y_\mu - \overline{x}_S\|^2 &= \frac{1}{(n-f)^2}\left\|\sum_{i\in\mathcal{N}_\mu\setminus S} x_i - \sum_{i\in S\setminus\mathcal{N}_\mu} x_i\right\|^2 = \frac{1}{(n-f)^2}\left\|\sum_{i\in\mathcal{N}_\mu\setminus S}(x_i-\mu) - \sum_{i\in S\setminus\mathcal{N}_\mu}(x_i-\mu)\right\|^2 \\ &\leq \frac{|S\setminus\mathcal{N}_\mu| + |\mathcal{N}_\mu\setminus S|}{(n-f)^2}\left[\sum_{i\in\mathcal{N}_\mu\setminus S}\|x_i-\mu\|^2 + \sum_{i\in S\setminus\mathcal{N}_\mu}\|x_i-\mu\|^2\right] \\ &\leq \frac{2f}{(n-f)^2}\left[\sum_{i\in\mathcal{N}_\mu\setminus S}\|x_i-\mu\|^2 + \sum_{i\in S\setminus\mathcal{N}_\mu}\|x_i-\mu\|^2\right].\end{aligned}$$

On 一方面，由于 $\mathcal{N}_\mu$ 是 μ的 $n-f$ 个最近邻的集合，第一项可以界定为 b y

$$\sum_{i\in\mathcal{N}_\mu\setminus S}\|x_i-\mu\|^2 \leq \sum_{i\in\mathcal{N}_\mu}\|x_i-\mu\|^2 \leq \sum_{i\in S}\|x_i-\mu\|^2.$$

另一方面，第二项可以界定为

$$\sum_{i\in S\setminus\mathcal{N}_\mu}\|x_i-\mu\|^2\leq\sum_{i\in S}\|x_i-\mu\|^2.$$

我们最终得出

$$\|y_\mu-\overline{x}_S\|^2\leq\frac{4f}{(n-f)^2}\sum_{i\in S}\|x_i-\mu\|^2.$$

□

第二个引理至关重要地表明，偏差与方差之和缩小了 $\frac{8f}{n-f}$ 倍。为此，我们令枢轴为元素 x_i，$i\in S$，从而对第一个引理作特化。

引理5。 设 $n\in\mathbb{N}^*, f<n$。对于任意集合 $S\subseteq\{1,\ldots,n\}, |S|=n-f$，对于任意向量 $x_1,\ldots,x_n\in\mathbb{R}^d$，向量$(y_1,\ldots,y_n)=NNM(x_1,\ldots,x_n)$ 验证

$$\underbrace{\frac{1}{|S|}\sum_{i\in S}\|y_i-\overline{y}_S\|^2}_{variance}+\underbrace{\|\overline{y}_S-\overline{x}_S\|^2}_{bias}\leq\frac{8f}{n-f}\frac{1}{|S|}\sum_{i\in S}\|x_i-\overline{x}_S\|^2.$$

证明。 设 $n\in\mathbb{N}^*, f<n, x_1,\ldots,x_n\in\mathbb{R}^d$，以及 $S\subseteq\{1,\ldots,n\}, |S|=n-f$。我们首先证明以下偏差-方差分解

$$\frac{1}{|S|}\sum_{i\in S}\|y_i-\overline{y}_S\|^2+\|\overline{y}_S-\overline{x}_S\|^2=\frac{1}{|S|}\sum_{i\in S}\|y_i-\overline{x}_S\|. \tag{23}$$

我们展开上述等式左侧的第一项，得到

$$\begin{aligned}\frac{1}{n-f}\sum_{i\in S}\|y_i-\overline{y}_S\|^2&=\frac{1}{n-f}\sum_{i\in S}\|y_i-\overline{x}_S+\overline{x}_S-\overline{y}_S\|^2\\&=\frac{1}{n-f}\sum_{i\in S}\|y_i-\overline{x}_S\|^2+\|\overline{x}_S-\overline{y}_S\|^2+2\frac{1}{n-f}\sum_{i\in S}\langle y_i-\overline{x}_S,\overline{x}_S-\overline{y}_S\rangle.\end{aligned}$$

然而，我们有

$$\frac{1}{n-f}\sum_{i\in S}\langle y_i-\overline{x}_S,\overline{x}_S-\overline{y}_S\rangle=\left\langle\underbrace{\frac{1}{n-f}\sum_{i\in S}y_i}_{=\overline{y}_S}-\overline{x}_S,\overline{x}_S-\overline{y}_S\right\rangle=-\|\overline{x}_S-\overline{y}_S\|^2.$$

因此，我们得到

$$\begin{aligned}\frac{1}{n-f}\sum_{i\in S}\|y_i-\overline{y}_S\|^2&=\frac{1}{n-f}\sum_{i\in S}\|y_i-\overline{x}_S\|^2+\|\overline{x}_S-\overline{y}_S\|^2-2\|\overline{x}_S-\overline{y}_S\|^2\\&=\frac{1}{n-f}\sum_{i\in S}\|y_i-\overline{x}_S\|^2-\|\overline{x}_S-\overline{y}_S\|^2.\end{aligned}$$

这就证明了（23）。此外，对于任意 $i\in S$，由引理4可知，在 $\mu=x_i$ 的条件下，

$$\|y_i-\overline{x}_S\|^2\leq\frac{4f}{n-f}\frac{1}{n-f}\sum_{j\in S}\|x_j-x_i\|^2.$$

因此，利用（23），我们得到

$$\begin{aligned}
\frac{1}{|S|}\sum_{i\in S}\|y_i-\overline{y}_S\|^2+\|\overline{y}_S-\overline{x}_S\|^2 &= \frac{1}{n-f}\sum_{i\in S}\|y_i-\overline{x}_S\|^2 \le \frac{4f}{n-f}\frac{1}{(n-f)^2}\sum_{i,j\in S}\|x_j-x_i\|^2\\
&= \frac{4f}{n-f}\frac{1}{(n-f)^2}\sum_{i,j\in S}\|x_j-\overline{x}_S-(x_i-\overline{x}_S)\|^2\\
&= \frac{4f}{n-f}\frac{1}{(n-f)^2}\sum_{i,j\in S}\Big(\|x_j-\overline{x}_S\|^2+\|x_i-\overline{x}_S\|^2-2\langle x_j-\overline{x}_S,\,x_i-\overline{x}_S\rangle\Big)\\
&= \frac{4f}{n-f}\frac{1}{(n-f)^2}\Big[\sum_{i,j\in S}\|x_j-\overline{x}_S\|^2+\sum_{i,j\in S}\|x_i-\overline{x}_S\|^2-2\sum_{i,j\in S}\langle x_j-\overline{x}_S,\,x_i-\overline{x}_S\rangle\Big]\\
&= \frac{4f}{n-f}\frac{1}{(n-f)^2}\Big[2(n-f)\sum_{i\in S}\|x_i-\overline{x}_S\|^2-2\sum_{i,j\in S}\langle x_j-\overline{x}_S,\,x_i-\overline{x}_S\rangle\Big]\\
&= \frac{4f}{n-f}\frac{1}{(n-f)^2}\Big[2(n-f)\sum_{i\in S}\|x_i-\overline{x}_S\|^2-2\sum_{i\in S}\Big\langle\underbrace{\sum_{j\in S}(x_j-\overline{x}_S)}_{=0},\,x_i-\overline{x}_S\Big\rangle\Big]\\
&= \frac{8f}{n-f}\frac{1}{n-f}\sum_{i\in S}\|x_i-\overline{x}_S\|^2.
\end{aligned}$$

证明到此结束。 □

9.3 引理 1 的证明

We 现在可以证明引理 1，这主要得益于引理所保证的偏差-方差权衡 5.

引理 1. 设 $f<n/2$ *and* $F\colon \mathbb{R}^{d\times n}\to\mathbb{R}^d$。若 F是(f,κ)-鲁棒的，则 $F\circ NNM$ 是(f,κ')-鲁棒的，其中 $\kappa'\le\frac{8f}{n-f}(\kappa+1)$。

证明。 设 $n\in\mathbb{N}^*, f<n, x_1,\dots,x_n\in\mathbb{R}^d$, $S\subseteq\{1,\dots,n\}, |S|=n-f$。假设 F是 (f,κ)-鲁棒的。首先，记 $(y_1,\dots,y_n)\coloneqq F\circ\mathrm{NNM}(x_1,\dots,x_n)$，并令 $\overline{y_S}\coloneqq\frac{1}{n-f}\sum_{i\in S}y_i$。由于 F 是 (f,κ)- 鲁棒的，向量 $y_1,\dots,y_n$ 满足

$$\|F\circ\mathrm{NNM}(x_1,\dots,x_n)-\overline{y}_S\|^2=\|F(y_1,\dots,y_n)-\overline{y}_S\|^2\le\kappa\frac{1}{|S|}\sum_{i\in S}\|y_i-\overline{y}_S\|^2. \tag{24}$$

现在，根据杨氏不等式，对于 $c=1/\kappa$，我们具有质量估计 $(a+b)^2\le(1+c)a^2+(1+1/c)b^2$。随后可以利用 (24) 写成

$$\begin{aligned}
\|F\circ\mathrm{NNM}(x_1,\dots,x_n)-\overline{x}_S\|^2 &= \|F\circ\mathrm{NNM}(x_1,\dots,x_n)-\overline{y}_S+\overline{y}_S-\overline{x}_S\|^2\\
&\le (1+\frac{1}{\kappa})\|F\circ\mathrm{NNM}(x_1,\dots,x_n)-\overline{y}_S\|^2+(1+\kappa)\|\overline{y}_S-\overline{x}_S\|^2\\
&\le (1+\frac{1}{\kappa})\kappa\frac{1}{|S|}\sum_{i\in S}\|y_i-\overline{y}_S\|^2+(1+\kappa)\|\overline{y}_S-\overline{x}_S\|^2\\
&= \frac{1+\kappa}{n-f}\sum_{i\in S}\|y_i-\overline{y}_S\|^2+(1+\kappa)\|\overline{y}_S-\overline{x}_S\|^2.
\end{aligned}\tag{25}$$

回顾一下，引理5表明，$\frac{1}{|S|}\sum_{\underline{i\in S}}\|y_i-y_S\|^2\pm\|y_S-\underline{x}_S\|^2\le\frac{8f}{n-f}\frac{1}{|S|}\sum_{\underline{i\in S}}\|x_i-x_S\|^2$。将其代入（25）即可得出结论

$$\|F\circ\mathrm{NNM}(x_1,\dots,x_n)-\overline{x}_S\|^2\le\frac{8f}{n-f}\frac{1+\kappa}{n-f}\sum_{i\in S}\|x_i-\overline{x}_S\|^2.$$

□

10 分桶分析

本节将比较分桶算法 [26] 与 NNM 的鲁棒性保证。分桶是一种预聚合步骤，它将输入向量 $\{x_1, \ldots, x_n\}$ 映射为输出向量 $\{y_1, \ldots, y_{\lceil n/s \rceil}\}$，其中 s 是一个称为桶大小的参数。分桶算法的工作方式如下。首先，它采样一个随机排列 π: $[n] \to [n]$。然后，对于每个 $i \in \{1, \ldots, \lceil n/s \rceil\}$，它将桶 i 的输出计算为[7]

$$y_i := \frac{1}{s} \sum_{k=s(i-1)+1}^{\min(s \cdot i, n)} x_{\pi(k)}.$$

回想一下，NNM 能够提高聚合鲁棒性的原因在于，输出向量 $\frac{1}{|S|} \sum_{i \in S} \|y_i - x_S\|^2$ 的异质性比输入向量 $\frac{1}{|S|} \sum_{i \in \overline{S}} \|x_i - x_S\|^2$ 的异质性低一个因子 $\mathcal{O}(f/n)$（见引理5）。但是，与 NNM 不同，分桶只会在对随机排列取期望时降低异质性（见 [26] 中的引理 1）。因此，在学习算法的某些迭代中，分桶可能不会降低异质性，而这些迭代正是拜占庭工作节点最有机会对学习造成最大损害的时候。

我们在下文的观察 1 中给出一个简单示例，说明一般而言，即使不存在恶意输入，也无法通过分桶确定性地降低输入的异质性。

观察 1。 使用分桶时，无论 s 的值是多少，都无法保证异质性在最坏情况下有所降低，即使不存在拜占庭输入。

证明。 令 π 为 $[n]$ 上的任意一个排列。我们将构造一个由 n 个输入组成的实例，使得使用排列 π 执行分桶时，异质性不会降低。考虑输入 $(x_1, \ldots\ldots, x_n)$，使得对于所有 $1 \le i \le \lceil n/s \rceil$ 和所有 $k, l \in \{s(i-1)+1, \ldots\ldots, s \cdot i\}$，均有 $x_{\pi(k)} = x_{\pi(l)} =: y_i$。因此，将排列 π 应用于这些输入后，得到 $\underbrace{\left(y_1, \ldots\ldots, y_1, \ldots\ldots, y_{n/s}, \ldots\ldots, y_{n/s}\right)}_{s\text{ 次 }s\text{ 次}}$，其中每个向量 y_i 都重复出现 s 次。总之，使用 π 执行分桶将产生 $(y_1, \ldots\ldots, y_{n/s})$，其方差与原始输入相同，因此异质性并未降低。 □

此外，鉴于桶是随机选取的，异质性的（预期）降低只是以拜占庭输入所占比例增加为代价实现的：

观察 2. 最坏情况下，分桶会使拜占庭工作节点的比例增加 s 倍。

证明。 在某些执行过程中，分桶可能会将每个拜占庭输入分配到不同的桶中。在这种情况下，由于每个“受污染”桶内的均值都可以被单个拜占庭输入任意操纵，因此拜占庭输出向量的数量与拜占庭输入向量的数量相同。然而，输出向量的总数比输入向量的总数少 s 倍，从而实际上提高了拜占庭工作节点所占的比例。 □

这一观察表明，为了获得最坏情况鲁棒性保证，桶大小 s 最多只能为 $\left\lfloor \frac{n}{2f} \right\rfloor$，如 [26]中所做的那样。这种降低异质性的不稳定性会导致某些迭代中的均值估计较差。如下文在 CIFAR-10 实验中所示，我们在实践中也观察到了这种不稳定性。

实验验证。 回顾鲁棒 D-SHB（算法 3）及其相应符号。在图 2 中，我们绘制了每一步的 $t \in [T]$ 量 $\hat{\kappa}_t$，其定义如下

$$\hat{\kappa}_t^2 := \|R_t - \overline{m}_t\|^2 / \frac{1}{|\mathcal{H}|} \sum_{i \in \mathcal{H}} \left\| m_t^{(i)} - \overline{m}_t \right\|^2, \tag{26}$$

其中 $\underline{m}_t := \frac{1}{|\mathcal{H}|} \sum_{i \in \mathcal{H}} m_t^{(i)}$ 是第 t步诚实动量的平均值。换言之，图 2 展示了在学习的不同步骤中，真实均值估计误差相对于诚实输入标准差的大小。公式 (26) 中的量是对 κ 的经验估计； κ 是我们理论中 (f, κ)-鲁棒性定义中的一个参数。该图验证了我们关于分桶的见解，并表明 NNM 无论在误差曲线的稳定性还是均值估计的质量方面都更优。事实上，NNM 曲线始终低于分桶曲线。

[7]在理论分析中，为简便起见，我们假设 n 可被 s整除。如果情况并非如此，则某些分桶将包含少于 s 个向量，这对分桶的理论保证较为不利，但不会改变其渐近行为。

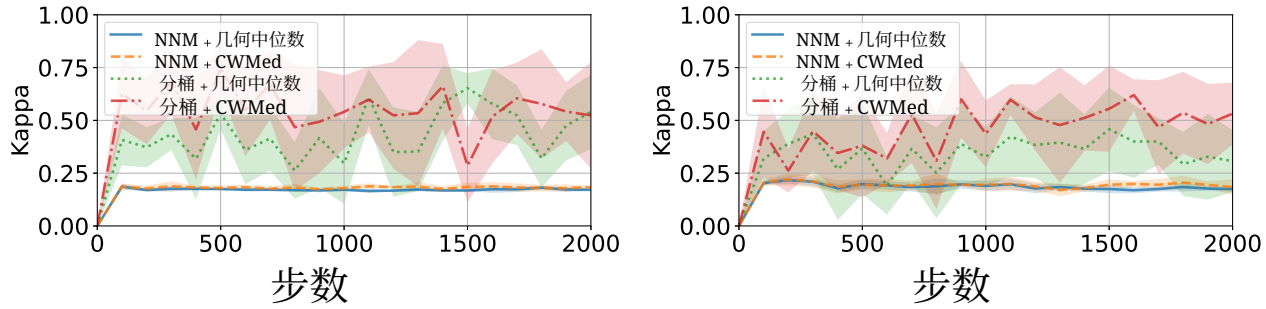

图 2：在 CIFAR-10 上绘制的$\hat{\kappa}_t$（定义见 (26)），其中 $n = 17$ 个工作节点正在执行 ALIE（第 *1* 列）和 FOE（第 *2* 列）攻击，$f = 2$ 个为拜占庭工作节点。异质性水平为 $\alpha = 1$。相应的准确率见图 24。

11 定理1 的证明：鲁棒 D-GD 的分析

定理 1。 设假设 *1*成立，并回顾 $\mathcal{L}_{\mathcal{H}}$ 是 L-光滑的。考虑采用学习率 $\gamma = \frac{1}{L}$ 的算法 *1*。如果 F是(f, κ)-鲁棒的，则对于所有 $T \geq 1$

$$\left\|\nabla \mathcal{L}_{\mathcal{H}}(\hat{\theta})\right\|^2 \leq 4\kappa G^2 + \frac{4L(\mathcal{L}_{\mathcal{H}}(\theta_0) - \mathcal{L}^*)}{T}.$$

证明。 设假设 1 成立。假设 $\mathcal{L}_{\mathcal{H}}$ 为 L-光滑，且 F 为 (f, κ)-鲁棒。考虑学习率为 $\gamma = \frac{1}{L}$ 的算法 1。对于每个 $t \geq 1$，更新步骤对应于 $\theta_t = \theta_{t-1} - \frac{1}{L} R_t$。
由于 $\mathcal{L}_{\mathcal{H}}$ 是 L-光滑的，根据 [8]，对于所有 $t \geq 1$，有

$$\begin{aligned}\mathcal{L}_{\mathcal{H}}(\theta_t) - \mathcal{L}_{\mathcal{H}}(\theta_{t-1}) &\leq \langle \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1}), \theta_t - \theta_{t-1} \rangle + \frac{L}{2} \|\theta_t - \theta_{t-1}\|^2 = -\gamma \langle \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1}), R_t \rangle + \frac{1}{2}\gamma^2 L \|R_t\|^2 \\ &= -\frac{1}{L} \langle \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1}), R_t \rangle + \frac{1}{2L} \|R_t\|^2 . \end{aligned} \tag{27}$$

我们将第二项展开如下

$$\begin{aligned}\|R_t\|^2 &= \|R_t - \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1}) + \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\|^2 \\ &= \|R_t - \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\|^2 + \|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\|^2 + 2 \langle \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1}), R_t - \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1}) \rangle .\end{aligned}$$

将其代回（27）并化简，可得

$$\begin{aligned}\mathcal{L}_{\mathcal{H}}(\theta_t) - \mathcal{L}_{\mathcal{H}}(\theta_{t-1}) &\leq -\frac{1}{L} \langle \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1}), R_t \rangle + \frac{1}{2L} \|R_t - \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\|^2 + \frac{1}{2L} \|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\|^2 \\ &\quad + \frac{1}{L} \langle \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1}), R_t - \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1}) \rangle \\ &= \frac{1}{2L} \|R_t - \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\|^2 - \frac{1}{2L} \|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\|^2 .\end{aligned}$$

重新整理各项并将两边乘以 $2L$，可得

$$\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\|^2 \leq \|R_t - \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\|^2 + 2L(\mathcal{L}_{\mathcal{H}}(\theta_{t-1}) - \mathcal{L}_{\mathcal{H}}(\theta_t)).$$

By 根据 F 和假设 1 的 (f, κ)-鲁棒性，我们可以将第一项界定如下

$$\begin{aligned}\|R_t - \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\|^2 &= \left\| F\left(g_t^{(1)}, \ldots, g_t^{(n)}\right) - \frac{1}{|\mathcal{H}|} \sum_{i \in \mathcal{H}} g_t^{(i)} \right\|^2 \leq \frac{\kappa}{|\mathcal{H}|} \sum_{i \in \mathcal{H}} \left\| g_t^{(i)} - \frac{1}{|\mathcal{H}|} \sum_{i \in \mathcal{H}} g_t^{(i)} \right\|^2 \\ &= \frac{\kappa}{|\mathcal{H}|} \sum_{i \in \mathcal{H}} \|\nabla \mathcal{L}_i(\theta_{t-1}) - \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\|^2 \leq \kappa G^2. \end{aligned} \tag{28}$$

因此，我们有

$$\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\|^2 \leq \kappa G^2 + 2L \left(\mathcal{L}_{\mathcal{H}}(\theta_{t-1}) - \mathcal{L}_{\mathcal{H}}(\theta_t)\right).$$

对从 1 到 T 的 t 求平均值，并且由于 $\mathcal{L}_{\mathcal{H}}(\theta_T) \geq \inf_{\theta \in \mathbb{R}^d} \mathcal{L}_{\mathcal{H}}(\theta) = \mathcal{L}^*$，我们有

$$\frac{1}{T}\sum_{t=0}^{T-1} \|\nabla \mathcal{L}_{\mathcal{H}}(\theta_t)\|^2 \leq \kappa G^2 + \frac{2L\left(\mathcal{L}_{\mathcal{H}}(\theta_0) - \mathcal{L}_{\mathcal{H}}(\theta_T)\right)}{T} \leq \kappa G^2 + \frac{2L\left(\mathcal{L}_{\mathcal{H}}(\theta_0) - \mathcal{L}^*\right)}{T}. \tag{29}$$

最后一步。回顾算法 1，$\theta = \theta_{\tau-1}$ 满足 $\tau \in \arg\min_{1\leq t\leq T} \|R_t\|$。因此，利用詹森不等式、式 (28)，再结合式 (29)，我们有

$$\begin{aligned}
\left\|\nabla \mathcal{L}_{\mathcal{H}}(\hat{\theta})\right\|^2 &= \min_{1\leq t\leq T} \|R_t\|^2 = \min_{1\leq t\leq T} \|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1}) + (R_t - \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1}))\|^2 \\
&\leq \min_{1\leq t\leq T} \left\{2\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\|^2 + 2\|R_t - \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\|^2\right\} \leq 2\min_{1\leq t\leq T} \|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\|^2 + 2\kappa G^2 \\
&\leq 2\frac{1}{T}\sum_{t=0}^{T-1} \|\nabla \mathcal{L}_{\mathcal{H}}(\theta_t)\|^2 + 2\kappa G^2 \leq 2\kappa G^2 + \frac{4L(\mathcal{L}_{\mathcal{H}}(\theta_0) - \mathcal{L}^*)}{T} + 2\kappa G^2 \\
&= 4\kappa G^2 + \frac{4L(\mathcal{L}_{\mathcal{H}}(\theta_0) - \mathcal{L}^*)}{T}.
\end{aligned}$$

证明至此完成。 □

12 推论 1 的证明：采用 NNM 的鲁棒分布式梯度下降分析

推论 1。设假设 *1* 成立，并回顾 $\mathcal{L}_{\mathcal{H}}$ 是 L-光滑的。考虑采用 $\gamma = 1/L$ 和聚合$F \circ$*NNM* 的算法 *1*。若 F是(f, κ)-鲁棒的，且满足 $\kappa = \mathcal{O}(1)$，则算法 *1* 具有(f, ε)-拜占庭弹性，且

$$\varepsilon = \mathcal{O}\big(f/n G^2 + 1/T\big).$$

证明。设假设 1 成立。假设 $\mathcal{L}_{\mathcal{H}}$是 L-光滑的，且 F是 (f, κ)-鲁棒的。首先回顾，根据引理 1，复合 $F \circ$ NNM 是 (f, κ')-鲁棒的，且满足 $\kappa' = \frac{8f}{n-f}(\kappa + 1)$。
考虑学习率为 $\gamma = 1/L$、聚合规则为 $F \circ$NNM 的算法 1。根据定理 1，对于每个$T \geq 1$，我们有

$$\left\|\nabla \mathcal{L}_{\mathcal{H}}\left(\hat{\theta}\right)\right\|^2 \leq 4\kappa' G^2 + \frac{4L(\mathcal{L}_{\mathcal{H}}(\theta_0) - \mathcal{L}^*)}{T} = \frac{32f}{n-f}(\kappa+1)G^2 + \frac{4L(\mathcal{L}_{\mathcal{H}}(\theta_0) - \mathcal{L}^*)}{T}.$$

回想一下，由于 $f < n/2$，我们有 $\frac{f}{n-f} \leq \frac{2f}{n}$。因此，如果 $\kappa = \mathcal{O}(1)$，我们可以写成

$$\left\|\nabla \mathcal{L}_{\mathcal{H}}\left(\hat{\theta}\right)\right\|^2 = \mathcal{O}\big(f/n G^2 + 1/T\big).$$

至此，证明完成。 □

我们给出 以下是异质性条件下拜占庭韧性下界的证明（命题 1） .

命题 1. 如果某个学习算法 $\mathcal{A}$ 对于满足假设 *1* 的每一组光滑损失函数$\mathcal{L}_1$、.....、 $\mathcal{L}_n$，都是(f, ε)-拜占庭弹性的，那么 $\varepsilon = \Omega\left(f/n\, G^2\right)$。

证明。证明过程与定理 III [26]类似。假设学习算法 $\mathcal{A}$ 对于满足假设 1 的每一组光滑损失函数 $\mathcal{L}_1, \ldots, \mathcal{L}_n$，都是（$f, \varepsilon$）-拜占庭弹性的。考虑以下二次损失函数 $\mathcal{L}_1 = \ldots = \mathcal{L}_{n-f} = \theta \mapsto \frac{1}{2}\|\theta\|^2$和
$\mathcal{L}_{n-f+1} = \ldots = \mathcal{L}_n = \theta \mapsto \frac{1}{2}\|\theta - z\|^2$，其中 $z \in \mathbb{R}^d$满足$\|z\|^2 = \frac{(n-f)^2}{f}\frac{()}{n-2f}G^2$。考虑两种情形 $\mathcal{H}_1 = \{1, \ldots, n-f\}$和 $\mathcal{H}_2 = \{f+1, \ldots, n\}$。
我们首先证明，在两种情形下，损失函数都满足假设 1。在情形 $\mathcal{H}_1$ 中，这显然成立，因为诚实损失完全相同。在情形 $\mathcal{H}_2$中，对于所有 $\theta \in \mathbb{R}^d$，我们有，

$$\nabla \mathcal{L}_{\mathcal{H}_2}(\theta) = \frac{1}{n-f}\sum_{i\in\mathcal{H}_2} \nabla \mathcal{L}_i(\theta) = \frac{n-2f}{n-f}\theta + \frac{f}{n-f}(\theta - z) = \theta - \frac{f}{n-f}z.$$

那里 因此，得益于对 z 的选择，我们现在证明假设 1 成立，因为对于所有 $\theta \in \mathbb{R}^d$，我们有 e

$$\frac{1}{|\mathcal{H}_2|}\sum_{i\in\mathcal{H}_2}\left\|\nabla\mathcal{L}_i(\theta)-\nabla\mathcal{L}_{\mathcal{H}_2}(\theta)\right\|^2=\frac{n-2f}{n-f}\left\|\frac{f}{n-f}z\right\|^2+\frac{f}{n-f}\left\|\frac{n-2f}{n-f}z\right\|^2=\frac{f(n-2f)}{(n-f)^2}\left\|z\right\|^2=G^2.$$

现在，由于学习算法 $\mathcal{A}$ 是 $(f,\ \varepsilon)$-拜占庭弹性的，因此它输出 $\hat{}\theta$，满足 $\left\|\nabla\mathcal{L}_{\mathcal{H}_1}(\hat{}\theta)\right\|^2\leq\varepsilon$ 和 $\left\|\nabla\mathcal{L}_{\mathcal{H}_2}(\hat{}\theta)\right\|^2\leq\varepsilon$。

注意，情形 $\mathcal{H}_1$ 和 $\mathcal{H}_2$ 对算法 $\mathcal{A}$ 来说无法区分，因为它忽略了拜占庭身份，因此 θ 在这两种情形下相同。因此，利用詹森不等式，我们有

$$\begin{aligned}\varepsilon&\geq\max\left\{\left\|\nabla\mathcal{L}_{\mathcal{H}_1}(\hat{\theta})\right\|^2,\left\|\nabla\mathcal{L}_{\mathcal{H}_2}(\hat{\theta})\right\|^2\right\}\geq\frac{1}{2}\left(\left\|\nabla\mathcal{L}_{\mathcal{H}_1}(\hat{\theta})\right\|^2+\left\|\nabla\mathcal{L}_{\mathcal{H}_2}(\hat{\theta})\right\|^2\right)\\&=\frac{1}{2}\left(\left\|\hat{\theta}\right\|^2+\left\|\hat{\theta}-\frac{f}{n-f}z\right\|^2\right)\geq\frac{1}{4}\left\|\frac{f}{n-f}z\right\|^2=\frac{1}{4}\left(\frac{f}{n-f}\right)^2\frac{(n-f)^2}{f(n-2f)}G^2=\frac{1}{4}\frac{f}{n-2f}G^2.\end{aligned}$$

由于 $n-2f\leq n$，我们得到 $\varepsilon\geq{}^1\!/_4\,f/n\,G^2$，证明得证。 □

13 定理 2 的证明：鲁棒 D-SHB 的分析

13.1 证明概要

我们对鲁棒 D-SHB（算法 3）的分析遵循 [17]，包含四个部分：(i) 动量漂移 （引理 6）、(ii)聚合误差（引理 7）、(iii) 动量偏差 （引理 8），以及 (iv) 下降界 （引理 9）。我们将这些部分结合起来，得到定理 2 中给出的最终收敛结果。与 [17], 相比，我们分析的新意在于：(i) 得益于 (f,κ)-鲁棒性，对聚合误差的分析更加紧密；(ii) 将动量漂移分析扩展到了异质设定。其他方面也存在一些细微差异，例如学习率的选择。

符号约定。回顾一下，对于每个步骤 t，以及每个诚实工作节点 w_i，

$$m_t^{(i)}=\beta m_{t-1}^{(i)}+(1-\beta)g_t^{(i)}\tag{30}$$

其中按照约定 $m_0^{(i)}=0$。由于我们分析的是采用聚合方法 F 的算法 3，记

$$R_t\coloneqq F\Big(m_t^{(1)},\ldots,m_t^{(n)}\Big),\tag{31}$$

and

$$\theta_t=\theta_{t-1}-\gamma R_t.\tag{32}$$

我们用 $\mathcal{P}_t$ 表示从步骤 1 到 t 的历史。具体而言，

$$\mathcal{P}_t\coloneqq\left\{\theta_0,\ldots,\,\theta_{t-1};\,m_1^{(i)},\ldots,\,m_{t-1}^{(i)};i=1,\ldots,\,n\right\}.$$

按照约定，$\mathcal{P}_1=\{\theta_0\}$。我们分别用 $\mathbb{E}_t[\cdot]$ 和 $\mathbb{E}[\cdot]$ 表示条件期望 $\mathbb{E}[\cdot\ \mathcal{P}_t]$ 和全期望。因此，$\mathbb{E}[\cdot]=\mathbb{E}_1[\cdots\mathbb{E}_T[\cdot]]$。

13.1.1 动量漂移

沿着轨迹 θ_0，.....，θ_{t-1}，诚实工作节点的局部动量可能会彼此偏离。这部分是由训练集之间的异质性造成的。这会导致诚实工作节点的局部梯度存在差异，而我们可以借助假设 1 对其进行控制。漂移也源于局部梯度的随机性。

我们在下文的引理 6 中证明，诚实工作者之间动量的漂移上界可以通过调节动量系数 β 来控制。事实上，$1-\beta$ 越小，漂移上界也越小。回想一下，我们用 $\mathcal{H}\subseteq[n]$ 表示 $n-f$ 诚实工作者的集合。我们定义

$$\overline{m}_t\coloneqq{}^1\!/_{(n-f)}\sum_{i\in\mathcal{H}}m_t^{(i)},\tag{33}$$

诚实工作者的局部动量的平均值。我们得到以下关于动量漂移的界限，即引理 6，其证明见附录 13.4.1。

引理 6。假设　设假设 *1* 和 *2* 成立。考虑算法 *3*。对于每个 $t \in [T]$，我们得到　　t

$$\mathbb{E}\left[\frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}}\left\|m_t^{(i)}-\overline{m}_t\right\|^2\right] \leq 3\left(\frac{1-\beta}{1+\beta}\right)\left(1+\frac{1}{n-f}\right)\sigma^2+3G^2.$$

13.1.2 聚合误差

基于这个初始引理和（f，κ）-鲁棒性，我们可以得到该情形下聚合结果 R_t 与 m_t 诚实工作者平均动量之间误差的上界。具体而言，将误差定义为

$$\xi_t \coloneqq R_t - \overline{m}_t, \tag{34}$$

由此可得引理 7 中误差的以下上界，其证明见附录 13.4.2。

引理 7。 假设假设 *1* 和 *2* 成立。设 F 满足（f，κ）-鲁棒。考虑采用聚合F的算法 *3*。对于每一步 $t \in [T]$，我们有

$$\mathbb{E}\left[\|\xi_t\|^2\right] \leq 6\kappa\frac{1-\beta}{1+\beta}\sigma^2+3\kappa G^2.$$

13.1.3 动量偏差

接下来，我们研究动量偏差，即任意步数 t中诚实动量平均值 m_t 与真实梯度$\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})$之间的距离。具体而言，我们将偏差 定义为

$$\delta_t \coloneqq \overline{m}_t - \nabla\mathcal{L}_{\mathcal{H}}\left(\theta_{t-1}\right), \tag{35}$$

并在下文的引理 8 中得到学习步数 $t \in [T]$内偏差增长的上界。（引理 8 的证明见附录 13.4.3。）

引理 8. 假设假设*2*成立。回顾一下，$\mathcal{L}_{\mathcal{H}}$ 是 L-光滑的。考虑满足 $T > 1$的算法 *3*。对于所有 $t \geq 2$，我们得到

$$\begin{aligned}\mathbb{E}\left[\|\delta_t\|^2\right] \leq& \beta^2 c\,\mathbb{E}\left[\|\delta_{t-1}\|^2\right] + 4\gamma L(1+\gamma L)\beta^2\,\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})\right\|^2\right] + (1-\beta)^2\frac{\sigma^2}{(n-f)}\\ &+ 2\gamma L(1+\gamma L)\beta^2\,\mathbb{E}\left[\|\xi_{t-1}\|^2\right],\end{aligned}$$

其中 $c \coloneqq (1+\gamma L)(1+4\gamma L)$。

13.1.4 下降界

最后，我们分析第四个要素，即沿着算法 3 的轨迹，成本函数 $\mathcal{L}_{\mathcal{H}}(\theta)$ 的增长。由 (32) 和 (31) 可得，对于每一步 t,

$$\theta_t = \theta_{t-1} - \gamma R_t = \theta_{t-1} - \gamma\,\overline{m}_t - \gamma\left(R_t - \overline{m}_t\right),$$

此外，由 (34) 可得，$R_t - m_t = \xi_t$。因此，对于所有 t,

$$\theta_t = \theta_{t-1} - \gamma\,\overline{m}_t - \gamma\xi_t. \tag{36}$$

这意味着，算法 3 实际上可以视为带有动量项的分布式随机梯度下降，只不过每一步 t 都会受到与 ξ_t 成比例的扰动。基于这一视角，我们得到引理 9，其证明见附录 13.4.4。

引理 9。 回想一下，$\mathcal{L}_{\mathcal{H}}$ 是 L-光滑的。考虑算法 *3*。对于所有 $t \in [T]$，可得

$$\begin{aligned}\mathbb{E}\left[2\mathcal{L}_{\mathcal{H}}(\theta_t) - 2\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right] \leq& -\gamma\left(1-4\gamma L\right)\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] + 2\gamma\left(1+2\gamma L\right)\mathbb{E}\left[\|\delta_t\|^2\right]\\ &+ 2\gamma\left(1+\gamma L\right)\mathbb{E}\left[\|\xi_t\|^2\right].\end{aligned}$$

综合前面所有引理，我们将在下文第 13.2 节证明定理 2。作为定理 2 和引理 1 的推论，我们将在第 13.3 节证明推论 2。

13.2 定理 2 的证明

为方便起见，我们在下文重述定理。请注意，

$$\mathcal{L}^* = \inf_{\theta\in\mathbb{R}^d} \mathcal{L}_{\mathcal{H}}(\theta),\ a_1 = 36, a_2 = 6\sqrt{\mathcal{L}_{\mathcal{H}}(\theta_0) - \mathcal{L}^*}, a_3 = 1728L, a_4 = 288L, \text{ and } a_5 = 6L\,a_2^2. \tag{37}$$

定理 2. 设假设 *1* 和假设 *2* 成立，并回顾 $\mathcal{L}_{\mathcal{H}}$ 是 L-光滑的。设 F 是一个 (f,κ)-鲁棒聚合规则。考虑动量系数为 $\beta = \sqrt{1-24\gamma L}$、学习率为

$$\gamma = \min\left\{\frac{1}{24L},\ \frac{a_2}{2a_\kappa\sigma\sqrt{T}}\right\},$$

其中 $a_\kappa^2 \coloneqq a_3\kappa + \frac{a_4}{n-f}$ 对于所有 $T \geq 1$

$$\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}(\hat{\theta})\right\|^2\right] \leq a_1\kappa G^2 + \frac{a_2a_\kappa\sigma}{\sqrt{T}} + \frac{a_5}{T} + \frac{a_2a_4\sigma}{na_\kappa T^{3/2}},$$

其中期望是对算法的随机性取的。

证明。定义

$$\gamma_o \coloneqq \frac{1}{18L}. \tag{38}$$

注意，按照定理陈述中的规定，根据 γ的定义，我们有

$$\gamma \leq \frac{1}{24L} \leq \gamma_o. \tag{39}$$

因此， $\beta = \sqrt{1-24\gamma L}$（按定义）是 (0，1) 中定义良好的实数值。

为得到收敛结果，我们将李雅普诺夫函数定义为

$$V_t \coloneqq \mathbb{E}\left[2\mathcal{L}_{\mathcal{H}}(\theta_{t-1}) + z\left\|\delta_t\right\|^2\right] \text{ and } z = \frac{1}{8L}. \tag{40}$$

我们考虑任意一个 $t \in [T]$。

应用引理 8。 代入引理 8 中的结果后，我们得到

$$\begin{aligned}\mathbb{E}\left[z\left\|\delta_{t+1}\right\|^2 - z\left\|\delta_t\right\|^2\right] \leq& z\beta^2c\,\mathbb{E}\left[\left\|\delta_t\right\|^2\right] + 4z\gamma L(1+\gamma L)\beta^2\,\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] + z(1-\beta)^2\frac{\sigma^2}{n-f}\\ &+ 2z\gamma L(1+\gamma L)\beta^2\,\mathbb{E}\left[\left\|\xi_t\right\|^2\right] - z\,\mathbb{E}\left[\left\|\delta_t\right\|^2\right].\end{aligned} \tag{41}$$

回想一下

$$c = (1+\gamma L)(1+4\gamma L) = 1 + 5\gamma L + 4\gamma^2L^2. \tag{42}$$

调用引理 9。 代入引理 9 可得

$$\begin{aligned}\mathbb{E}\left[2\mathcal{L}_{\mathcal{H}}(\theta_t) - 2\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right] \leq& -\gamma(1-4\gamma L)\,\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] + 2\gamma(1+2\gamma L)\,\mathbb{E}\left[\left\|\delta_t\right\|^2\right]\\ &+ 2\gamma(1+\gamma L)\,\mathbb{E}\left[\left\|\xi_t\right\|^2\right].\end{aligned} \tag{43}$$

将（41）和（43）代入（40），可得

$$\begin{aligned}V_{t+1} - V_t =& \mathbb{E}\left[2\mathcal{L}_{\mathcal{H}}(\theta_t) - 2\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right] + \mathbb{E}\left[z\left\|\delta_{t+1}\right\|^2 - z\left\|\delta_t\right\|^2\right]\\ \leq& -\gamma(1-4\gamma L)\,\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] + 2\gamma(1+2\gamma L)\,\mathbb{E}\left[\left\|\delta_t\right\|^2\right] + 2\gamma(1+\gamma L)\,\mathbb{E}\left[\left\|\xi_t\right\|^2\right]\\ &+ z\beta^2c\,\mathbb{E}\left[\left\|\delta_t\right\|^2\right] + 4z\gamma L(1+\gamma L)\beta^2\,\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] + z(1-\beta)^2\frac{\sigma^2}{n-f}\\ &+ 2z\gamma L(1+\gamma L)\beta^2\,\mathbb{E}\left[\left\|\xi_t\right\|^2\right] - z\,\mathbb{E}\left[\left\|\delta_t\right\|^2\right].\end{aligned} \tag{44}$$

重新整理（44）右侧的表达式，可得

$$V_{t+1} - V_t \leq -\gamma \left((1-4\gamma L) - 4zL(1+\gamma L)\beta^2\right) \mathbb{E}\left[\left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] + z(1-\beta)^2 \frac{\sigma^2}{n-f} + \left(2\gamma\left(1+2\gamma L\right) + z\beta^2 c - z\right) \mathbb{E}\left[\left\|\delta_t\right\|^2\right] + 2\gamma\left(1+\gamma L + zL(1+\gamma L)\beta^2\right) \mathbb{E}\left[\left\|\xi_t\right\|^2\right].$$

为简便起见，我们定义

$$A \coloneqq (1-4\gamma L) - 4zL(1+\gamma L)\beta^2, \tag{45}$$

$$B \coloneqq 2\gamma\left(1+2\gamma L\right) + z\beta^2 c - z, \tag{46}$$

and

$$C \coloneqq 2\gamma\left(1+\gamma L + zL(1+\gamma L)\beta^2\right), \tag{47}$$

因此，

$$V_{t+1} - V_t \leq -A\gamma\, \mathbb{E}\left[\left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] + B\, \mathbb{E}\left[\left\|\delta_t\right\|^2\right] + C\, \mathbb{E}\left[\left\|\xi_t\right\|^2\right] + z(1-\beta)^2 \frac{\sigma^2}{n-f}. \tag{48}$$

现在我们分析以下各项 A、 B 和 C。

项 A。 由（39）可知， $\gamma \leq \gamma_o = \frac{1}{18L}$，将其代入（45），并利用 $z = \frac{1}{8L}$ 和 $\beta^2 < 1$这一事实，我们得到

$$A \geq 1 - 4\gamma_o L - \frac{4L}{8L}(1+\gamma_o L) \geq \frac{1}{2} - \frac{9\gamma_o L}{2} \geq \frac{1}{4}. \tag{49}$$

项 B。 将（42）中的 c 代入（46），我们得到

$$\begin{aligned} B &= 2\gamma\left(1+2\gamma L\right) + z\beta^2\left(1+5\gamma L + 4\gamma^2 L^2\right) - z \\ &= -\left(1-\beta^2\right)z + \gamma\left(2 + 4\gamma L + 5z\beta^2 L + 4z\beta^2 L\gamma L\right). \end{aligned}$$

利用 $\beta^2 \leq 1$ 和 $\gamma \leq \gamma_o \leq \frac{1}{18L}$ 这两个事实，再代入 $z = \frac{1}{8L}$，我们得到

$$B \leq \frac{-(1-\beta^2)}{8L} + \gamma\left(2 + \frac{4}{18} + \frac{5}{8} + \frac{4}{18\times 8}\right) \leq \frac{-(1-\beta^2)}{8L} + 3\gamma \leq \frac{-(1-\beta^2) + 24\gamma L}{8L} = 0, \tag{50}$$

其中，最后一个等式由事实 $1-\beta^2 = 24\gamma L$ 得出。

项 C。 将 $z = \frac{1}{8L}$ 代入式(47)，再利用事实 $\beta^2 < 1$，我们得到

$$C = 2\gamma\left(1 + \gamma L + \frac{1}{8}(1+\gamma L)\right) \leq \frac{9\gamma}{4}\left(1+\gamma L\right).$$

由于 $\gamma \leq \gamma_o \leq \frac{1}{18L}$，由上文可得

$$C \leq \frac{9\gamma}{4}\left(1 + \frac{1}{18}\right) \leq 3\gamma. \tag{51}$$

合并各项 A， B**和** C。 最后，将 (49)、(50) 和 (51) 代入 (48)（并回想 $z = \frac{1}{8L}$），我们得到

$$V_{t+1} - V_t \leq -\frac{\gamma}{4}\, \mathbb{E}\left[\left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] + 3\gamma\, \mathbb{E}\left[\left\|\xi_t\right\|^2\right] + (1-\beta)^2 \frac{\sigma^2}{8L(n-f)}.$$

由于上述结论对　　对于任意的 $t \in [T]$，将两边从 $t=1$ 到 $t=T$ 求和，可得

$$V_{T+1} - V_1 \leq -\frac{\gamma}{4}\sum_{t=1}^{T}\mathbb{E}\left[\left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] + 3\gamma\sum_{t=1}^{T}\mathbb{E}\left[\left\|\xi_t\right\|^2\right] + (1-\beta)^2\frac{\sigma^2}{8L(n-f)}T.$$

因此，

$$\frac{\gamma}{4}\sum_{t=1}^{T}\mathbb{E}\left[\left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] \leq V_1 - V_{T+1} + 3\gamma\sum_{t=1}^{T}\mathbb{E}\left[\left\|\xi_t\right\|^2\right] + (1-\beta)^2\frac{\sigma^2}{8L(n-f)}T. \tag{52}$$

注意，由于 $\beta > 0$ 且 $1-\beta^2 = 24\gamma L$，我们有

$$(1-\beta)^2 = \frac{\left(1-\beta^2\right)^2}{(1+\beta)^2} \leq \left(1-\beta^2\right)^2 = 576\gamma^2L^2.$$

将上面的结果代入式（52），可得

$$\frac{\gamma}{4}\sum_{t=1}^{T}\mathbb{E}\left[\left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] \leq V_1 - V_{T+1} + 3\gamma\sum_{t=1}^{T}\mathbb{E}\left[\left\|\xi_t\right\|^2\right] + \frac{576\gamma^2L^2\sigma^2}{8L(n-f)}T.$$

两边乘以 $4/\gamma$，可得

$$\sum_{t=1}^{T}\mathbb{E}\left[\left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] \leq \frac{4\left(V_1 - V_{T+1}\right)}{\gamma} + 12\sum_{t=1}^{T}\mathbb{E}\left[\left\|\xi_t\right\|^2\right] + \frac{576\gamma L\sigma^2}{2(n-f)}T. \tag{53}$$

调用引理 7。接下来，我们使用引理 7 推导 $\sum_{t=1}^{T}\mathbb{E}\left[\left\|\xi_t\right\|^2\right]$ 的上界。由于 F 是 $(f,\ \kappa)$-鲁棒的，根据引理 7，对于所有 $t \in [T]$，我们有

$$\mathbb{E}\left[\left\|\xi_t\right\|^2\right] \leq 6\kappa\frac{1-\beta}{1+\beta}\sigma^2 + 3\kappa G^2.$$

对 t 从 1 到 T 求和，我们得到

$$\sum_{t=1}^{T}\mathbb{E}\left[\left\|\xi_t\right\|^2\right] \leq 6\kappa\frac{1-\beta}{1+\beta}\sigma^2T + 3\kappa G^2T. \tag{54}$$

由于 $\beta > 0$，且根据 $1-\beta^2 = 24\gamma L$，我们有

$$\frac{1-\beta}{1+\beta} = \frac{1-\beta^2}{(1+\beta)^2} \leq 1-\beta^2 = 24\gamma L.$$

将上述结果代入（54），我们得到

$$\sum_{t=1}^{T}\mathbb{E}\left[\left\|\xi_t\right\|^2\right] \leq (24\times 6)\sigma^2\kappa\gamma LT + 3\kappa G^2T = 144\sigma^2\kappa\gamma LT + 3\kappa G^2T.$$

将上述结果代入（53），我们得到

$$\sum_{t=1}^{T}\mathbb{E}\left[\left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] \leq \frac{4\left(V_1 - V_{T+1}\right)}{\gamma} + (12\times 144)\sigma^2\kappa\gamma LT + (12\times 3)\kappa G^2T + \frac{288\gamma L\sigma^2}{(n-f)}.$$

回顾一下，

$$a_1 = (12\times 3) = 36, a_3 = (12\times 144)L = 1728L, \text{ and } a_4 = 288L$$

因此，根据上述内容可得，

$$\sum_{t=1}^{T}\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right]\leq\frac{4\left(V_1-V_{T+1}\right)}{\gamma}+a_3\kappa\sigma^2\gamma T+\frac{a_4\sigma^2}{(n-f)}\gamma T+a_1\kappa G^2T.$$

将两边除以 T，我们得到

$$\frac{1}{T}\sum_{t=1}^{T}\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right]\leq\frac{4\left(V_1-V_{T+1}\right)}{\gamma T}+a_3\kappa\sigma^2\gamma+\frac{a_4\sigma^2}{(n-f)}\gamma+a_1\kappa G^2. \tag{55}$$

分析 V_t。回想一下，$\mathcal{L}^*=\inf_{\theta\in\mathbb{R}^d}\mathcal{L}_{\mathcal{H}}(\theta)$。注意，对于任意 t，根据 (40) 中 V_t 的定义，

$$V_t-2\mathcal{L}^*=2\,\mathbb{E}\left[\mathcal{L}_{\mathcal{H}}(\theta_{t-1})-\mathcal{L}^*\right]+z\,\mathbb{E}\left[\left\|\delta_t\right\|^2\right]\geq0+z\,\mathbb{E}\left[\left\|\delta_t\right\|^2\right]\geq0.$$

因此，

$$V_1-V_{T+1}=V_1-2\mathcal{L}^*-(V_{T+1}-2\mathcal{L}^*)\leq V_1-2\mathcal{L}^*. \tag{56}$$

此外，

$$V_1=2\mathcal{L}_{\mathcal{H}}(\theta_0)+z\,\mathbb{E}\left[\left\|\delta_1\right\|^2\right]. \tag{57}$$

根据 (35) 中 δ_t 的定义、(33) 中 m_t 的定义，以及对所有 $i\in\mathcal{H}$ 都有 $m_0^{(i)}=0$ 这一事实，我们得到

$$\mathbb{E}\left[\left\|\delta_1\right\|^2\right]=\mathbb{E}\left[\left\|\overline{m}_1-\nabla\mathcal{L}_{\mathcal{H}}(\theta_0)\right\|^2\right]=\mathbb{E}\left[\left\|(1-\beta)\overline{g}_1-\nabla\mathcal{L}_{\mathcal{H}}(\theta_0)\right\|^2\right]$$

其中，$\bar{}g_1$（定义见（59））是第 1 步中 $n-f$ 诚实工作者的随机梯度平均值。展开上面的右侧可得

$$\mathbb{E}\left[\left\|\delta_1\right\|^2\right]=(1-\beta)^2\,\mathbb{E}\left[\left\|\overline{g}_1-\nabla\mathcal{L}_{\mathcal{H}}(\theta_0)\right\|^2\right]+\beta^2\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_0)\right\|^2-2\beta(1-\beta)\left\langle\mathbb{E}\left[\overline{g}_1\right]-\nabla\mathcal{L}_{\mathcal{H}}(\theta_0),\,\nabla\mathcal{L}_{\mathcal{H}}(\theta_0)\right\rangle.$$

回顾一下，$\underline{\mathbb{E}}\left[g_1\right]=\nabla\mathcal{L}_{\mathcal{H}}(\theta_0)$，并且（根据假设2）$\mathbb{E}\left[\left\|g_1-\underline{\nabla}\mathcal{L}_{\mathcal{H}}(\theta_0)\right\|^2\right]\leq\sigma^2/(n-f)$。因此，

$$\mathbb{E}\left[\left\|\delta_1\right\|^2\right]\leq\frac{(1-\beta)^2\sigma^2}{(n-f)}+\beta^2\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_0)\right\|^2.$$

回顾一下，$\mathcal{L}_{\mathcal{H}}$ 是 L-光滑的。因此，$\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_0)\right\|^2\leq2L(\mathcal{L}_{\mathcal{H}}(\theta_0)-\mathcal{L}^*)$（参见 [37], 定理2.1.5）。因此，

$$\mathbb{E}\left[\left\|\delta_1\right\|^2\right]\leq\frac{(1-\beta)^2\sigma^2}{(n-f)}+2\beta^2L(\mathcal{L}_{\mathcal{H}}(\theta_0)-\mathcal{L}^*).$$

将上面的结果代入（57），可得

$$V_1\leq2\mathcal{L}_{\mathcal{H}}(\theta_0)+z\left(\frac{(1-\beta)^2\sigma^2}{(n-f)}+2\beta^2L(\mathcal{L}_{\mathcal{H}}(\theta_0)-\mathcal{L}^*)\right).$$

回顾一下 $(1-\beta)^2\leq\left(1-\beta^2\right)^2=576\gamma^2L^2$。利用这一点以及 $\beta^2<1$ 和 $z=\frac{1}{8L}$，可得

$$V_1\leq2\mathcal{L}_{\mathcal{H}}(\theta_0)+\frac{1}{4}(\mathcal{L}_{\mathcal{H}}(\theta_0)-\mathcal{L}^*)+\frac{72\gamma^2L^2\sigma^2}{L(n-f)}.$$

回顾一下 $a_4=288L$。因此，

$$V_1\leq2\mathcal{L}_{\mathcal{H}}(\theta_0)+\frac{1}{4}(\mathcal{L}_{\mathcal{H}}(\theta_0)-\mathcal{L}^*)+\frac{a_4\sigma^2}{4(n-f)}\gamma^2.$$

将上述结果代入式（56），可得

$$V_1 - V_{T+1} \leq 2\mathcal{L}_{\mathcal{H}}(\theta_0) - 2\mathcal{L}^* + \frac{1}{4}(\mathcal{L}_{\mathcal{H}}(\theta_0) - \mathcal{L}^*) + \frac{a_4\sigma^2}{4(n-f)}\gamma^2 = \frac{9}{4}(\mathcal{L}_{\mathcal{H}}(\theta_0) - \mathcal{L}^*) + \frac{a_4\sigma^2}{4(n-f)}\gamma^2.$$

将上式代入（55），可得

$$\frac{1}{T}\sum_{t=1}^{T}\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] \leq \frac{(4\times\frac{9}{4})(\mathcal{L}_{\mathcal{H}}(\theta_0) - \mathcal{L}^*)}{\gamma T} + \left(\frac{a_4\sigma^2}{n-f}\right)\frac{\gamma}{T} + a_3\kappa\sigma^2\gamma + \frac{a_4\sigma^2}{(n-f)}\gamma + a_1\kappa G^2.$$

对上述右侧各项重新排列后，可得

$$\frac{1}{T}\sum_{t=1}^{T}\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] \leq a_1\kappa G^2 + \frac{9(\mathcal{L}_{\mathcal{H}}(\theta_0) - \mathcal{L}^*)}{\gamma T} + \left(a_3\kappa + \frac{a_4}{n-f}\right)\sigma^2\gamma + \left(\frac{a_4\sigma^2}{n-f}\right)\frac{\gamma}{T}.$$

回顾 $a_2^2 = 36(\mathcal{L}_{\mathcal{H}}(\theta_0) - \mathcal{L}^*)$ 和 $a_\kappa^2 := a_3\kappa + \frac{a_4}{n-f}$，可得

$$\frac{1}{T}\sum_{t=1}^{T}\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] \leq a_1\kappa G^2 + \frac{a_2^2}{4\gamma T} + a_\kappa^2\sigma^2\gamma + \left(\frac{a_4\sigma^2}{n-f}\right)\frac{\gamma}{T} \tag{58}$$

最后一步。回顾定义可知

$$\gamma = \min\left\{\frac{1}{24L}, \frac{a_2}{2a_\kappa\sigma\sqrt{T}}\right\},$$

因此 $\frac{1}{\gamma} = \max\left\{24L, \frac{2a_\kappa\sigma\sqrt{T}}{a_2}\right\} \leq 24L + \frac{2a_\kappa\sigma\sqrt{T}}{a_2}$。

将 γ 代入式 (58)，并回忆 $a_5 = 6La_2^2$，可得

$$\begin{aligned}\frac{1}{T}\sum_{t=1}^{T}\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] &\leq a_1\kappa G^2 + \frac{a_2a_\kappa\sigma}{\sqrt{T}} + \frac{24La_2^2}{4T} + \frac{a_2a_4\sigma^2}{2(n-f)a_\kappa T^{3/2}} \\ &\leq a_1\kappa G^2 + \frac{a_2a_\kappa\sigma}{\sqrt{T}} + \frac{a_5}{T} + \frac{a_2a_4\sigma}{na_\kappa T^{3/2}}. \qquad \text{（因为 } n \geq 2f\text{）}\end{aligned}$$

最后，回顾算法 3，$\hat{\theta}$ 是从计算得到的参数向量集合 $(\theta_0$、……、$\theta_{T-1})$ 中随机选取的。因此，$\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}\left(\hat{\theta}\right)\right\|^2\right] = \frac{1}{T}\sum_{t=1}^{T}\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right]$。将其代入上式即可证明该定理。 □

13.3 推论 2 的证明：带 NNM 的鲁棒 D-SHB 分析

推论 2。 设假设 *1* 成立，并回顾 $\mathcal{L}_{\mathcal{H}}$ 是 L-光滑的。在与定理 *2* 相同的设定下，考虑采用聚合 $F \circ NNM$ 的算法 *3*。如果 F 是(f, κ)-鲁棒的，且满足 $\kappa = \mathcal{O}(1)$，则有

$$\mathbb{E}\left[\left\|\nabla \mathcal{L}_{\mathcal{H}}(\hat{\theta})\right\|^2\right] = \mathcal{O}\big(f/n G^2 + 1/\sqrt{T}\big),$$

其中，期望是对算法的随机性取的。

证明。 设假设 1 成立。假设 $\mathcal{L}_{\mathcal{H}}$ 为 L-光滑，且 F 为 (f, κ)-鲁棒。首先回顾，根据引理 1，复合 $F \circ \mathrm{NNM}$ 是 (f, κ')-鲁棒的，且 $\kappa' = \frac{8f}{n-f}(\kappa + 1)$。
考虑采用聚合规则 $F \circ \mathrm{NNM}$ 的算法 1，并将学习率和动量系数设为定理 2 中的取值。根据定理 2，并回顾式 (37) 中定义的常数，对于每个 $T \geq 1$，我们有：

$$\begin{aligned}\mathbb{E}\left[\left\|\nabla \mathcal{L}_{\mathcal{H}}(\hat{\theta})\right\|^2\right] &\leq a_1 \kappa' G^2 + \frac{a_2 a_{\kappa'} \sigma}{\sqrt{T}} + \frac{a_5}{T} + \frac{a_2 a_4 \sigma}{n a_{\kappa'} T^{3/2}} \\ &= \frac{8 a_1 f}{n-f}(\kappa+1) G^2 + \frac{a_2 a_{\kappa'} \sigma}{\sqrt{T}} + \frac{a_5}{T} + \frac{a_2 a_4 \sigma}{n a_{\kappa'} T^{3/2}}.\end{aligned}$$

回顾 $a_{\kappa'}^2 = a_3 \kappa' + \frac{a_4}{n-f} = \frac{8 a_3 f}{n-f}(\kappa+1) + \frac{a_4}{n-f}$。由于根据假设，$\kappa \geq 0$ 且 $\kappa = \mathcal{O}(1)$，我们有 $a_{\kappa'} = \Theta(1)$。现在，忽略常数以及上文右侧的最后两项（因为它们被 $\frac{1}{\sqrt{T}}$ 支配），得到

$$\mathbb{E}\left[\left\|\nabla \mathcal{L}_{\mathcal{H}}(\hat{\theta})\right\|^2\right] = \mathcal{O}\left(\frac{f}{n-f}(\kappa+1) G^2 + \frac{1}{\sqrt{T}}\right).$$

回想一下，根据 $f < n/2$，我们有 $\frac{f}{n-f} \leq \frac{2f}{n}$。因此，如果 $\kappa = \mathcal{O}(1)$，我们可以写成

$$\mathbb{E}\left[\left\|\nabla \mathcal{L}_{\mathcal{H}}(\hat{\theta})\right\|^2\right] = \mathcal{O}\big(f/n G^2 + 1/\sqrt{T}\big).$$

证明到此结束。 □

13.4 支持性引理的证明

13.4.1 引理 6 的证明

下面回顾引理 6，并给出其证明。

引理 6. 假设假设 *2* 和假设 *1* 成立。考虑算法 *3*。对于每个 $t \in [T]$，我们有

$$\mathbb{E}\left[\frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}}\left\|m_t^{(i)}-\overline{m}_t\right\|^2\right] \le 3\left(\frac{1-\beta}{1+\beta}\right)\left(1+\frac{1}{n-f}\right)\sigma^2+3G^2.$$

证明。 回顾式 (33)，可得

$$\overline{m}_t \coloneqq {}^1\!/_{(n-f)}\sum_{i\in\mathcal{H}} m_t^{(i)}.$$

我们考虑任意一个 $i \in \mathcal{H}$。为简便起见，我们定义

$$\overline{g}_t \coloneqq {}^1\!/_{(n-f)}\sum_{j\in\mathcal{H}} g_t^{(j)}. \tag{59}$$

现在，我们考虑任意一个步骤 $t \in [T]$。展开式 (30) 中的求和可得

$$m_t^{(i)} = (1-\beta)\sum_{k=1}^{t}\beta^{t-k}g_k^{(i)}.$$

因此，应用詹森不等式，我们可以写出

$$\begin{aligned}
\mathbb{E}\left[\frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}}\left\|m_t^{(i)}-\overline{m}_t\right\|^2\right] &= (1-\beta)^2\,\mathbb{E}\left[\frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}}\left\|\sum_{k=1}^{t}\beta^{t-k}(g_k^{(i)}-\overline{g}_t)\right\|^2\right]\\
&\le 3(1-\beta)^2\,\mathbb{E}\left[\frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}}\left\|\sum_{k=1}^{t}\beta^{t-k}(g_k^{(i)}-\nabla\mathcal{L}_i(\theta_{k-1}))\right\|^2\right]\\
&\quad+3(1-\beta)^2\,\mathbb{E}\left[\frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}}\left\|\sum_{k=1}^{t}\beta^{t-k}(\overline{g}_k-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{k-1}))\right\|^2\right]\\
&\quad+3(1-\beta)^2\,\mathbb{E}\left[\frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}}\left\|\sum_{k=1}^{t}\beta^{t-k}(\nabla\mathcal{L}_i(\theta_{k-1})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{k-1}))\right\|^2\right].
\end{aligned} \tag{60}$$

下面给出式 (60) 右侧三个项各自的上界。

对于式 (60) 右侧的第一项，我们记为

$$A_t \coloneqq \mathbb{E}\left[\left\|\sum_{k=1}^{t}\beta^{t-k}(g_k^{(i)}-\nabla\mathcal{L}_i(\theta_{k-1}))\right\|^2\right].$$

我们得到

$$\begin{aligned}
A_t &= \mathbb{E}\left[\left\|\sum_{k=1}^{t-1}\beta^{t-k}(g_k^{(i)}-\nabla\mathcal{L}_i(\theta_{k-1}))+(g_t^{(i)}-\nabla\mathcal{L}_i(\theta_{t-1}))\right\|^2\right]\\
&= \mathbb{E}\left[\left\|\sum_{k=1}^{t-1}\beta^{t-k}(g_k^{(i)}-\nabla\mathcal{L}_i(\theta_{k-1}))\right\|^2\right]+\mathbb{E}\left[\left\|g_t^{(i)}-\nabla\mathcal{L}_i(\theta_{t-1})\right\|^2\right]\\
&\quad+2\,\mathbb{E}\left[\left\langle\sum_{k=1}^{t-1}\beta^{t-k}(g_k^{(i)}-\nabla\mathcal{L}_i(\theta_{k-1})),\, g_t^{(i)}-\nabla\mathcal{L}_i(\theta_{t-1})\right\rangle\right]
\end{aligned}$$

根据全期望公式以及随机梯度的无偏性（假设2），右侧最后一项为零:

$$\begin{aligned}\mathbb{E}\left[\left\langle\sum_{k=1}^{t-1}\beta^{t-k}(g_k^{(i)}-\nabla\mathcal{L}_i(\theta_{k-1})),\, g_t^{(i)}-\nabla\mathcal{L}_i(\theta_{t-1})\right\rangle\right] &= \mathbb{E}\left[\mathbb{E}_t\left[\left\langle\sum_{k=1}^{t-1}\beta^{t-k}(g_k^{(i)}-\nabla\mathcal{L}_i(\theta_{k-1})),\, g_t^{(i)}-\nabla\mathcal{L}_i(\theta_{t-1})\right\rangle\right]\right]\\ &= \mathbb{E}\left[\left\langle\sum_{k=1}^{t-1}\beta^{t-k}(g_k^{(i)}-\nabla\mathcal{L}_i(\theta_{k-1})),\, \underbrace{\mathbb{E}_t\left[g_t^{(i)}-\nabla\mathcal{L}_i(\theta_{t-1})\right]}_{=0}\right\rangle\right]\\ &= 0.\end{aligned}$$

根据假设2，我们有 $\mathbb{E}\left[\left\|g_t^{(i)}-\nabla\mathcal{L}_i(\theta_{t-1})\right\|^2\right]\leq\sigma^2$。因此，我们有

$$A_t\leq\mathbb{E}\left[\left\|\sum_{k=1}^{t-1}\beta^{t-k}(g_k^{(i)}-\nabla\mathcal{L}_i(\theta_{k-1}))\right\|^2\right]+\sigma^2=\beta^2A_{t-1}+\sigma^2.$$

通过递归，我们得到

$$A_t\leq\beta^{2(t-1)}A_1+\sigma^2\sum_{l=0}^{t-2}\beta^{2l}.$$

由于 $A_1=\mathbb{E}\left[\left\|g_1^{(i)}-\nabla\mathcal{L}_i(\theta_0)\right\|^2\right]\leq\sigma^2$，由上文可得

$$A_t\leq\sigma^2\sum_{l=0}^{t-1}\beta^{2l}\leq\frac{\sigma^2}{1-\beta^2}. \tag{61}$$

对于（60）右侧的第二项，我们记为

$$B_t\coloneqq\mathbb{E}\left[\left\|\sum_{k=1}^{t}\beta^{t-k}(\overline{g}_k-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{k-1}))\right\|^2\right].$$

根据假设2以及随机梯度的相互独立性，我们有

$$\mathbb{E}\left[\|\overline{g}_t-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\|^2\right]=\frac{1}{(n-f)^2}\sum_{i\in\mathcal{H}}\mathbb{E}\left[\left\|g_t^{(i)}-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right]\leq\frac{\sigma^2}{n-f}.$$

因此，与关于 A_t的界类似，我们得到

$$B_t\leq\frac{\sigma^2}{(1-\beta^2)(n-f)}. \tag{62}$$

对于式 (60) 右侧的第三项，我们记为

$$C_t\coloneqq\mathbb{E}\left[\frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}}\left\|\sum_{k=1}^{t}\beta^{t-k}(\nabla\mathcal{L}_i(\theta_{k-1})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{k-1}))\right\|^2\right].$$

应用詹森不等式，再结合假设 1，我们得到

$$\begin{aligned} C_t &\leq \left(\sum_{k=1}^{t}\beta^{t-k}\right)\mathbb{E}\left[\frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}}\sum_{k=1}^{t}\beta^{t-k}\left\|\nabla\mathcal{L}_i(\theta_{k-1})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{k-1})\right\|^2\right] \\ &= \left(\sum_{k=1}^{t}\beta^{t-k}\right)\mathbb{E}\left[\sum_{k=1}^{t}\beta^{t-k}\frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}}\left\|\nabla\mathcal{L}_i(\theta_{k-1})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{k-1})\right\|^2\right] \\ &\leq \left(\sum_{k=1}^{t}\beta^{t-k}\right)^2\cdot G^2 \leq \frac{G^2}{(1-\beta)^2}. \end{aligned} \tag{63}$$

最后，将 (61)、(62) 和 (63) 代入 (60)，可得

$$\begin{aligned} \mathbb{E}\left[\frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}}\left\|m_t^{(i)}-\overline{m}_t\right\|^2\right] &\leq 3(1-\beta)^2\frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}}(A_t+B_t+C_t) \\ &\leq 3(1-\beta)^2\frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}}\left(\frac{\sigma^2}{1-\beta^2}+\frac{\sigma^2}{(1-\beta^2)(n-f)}+\frac{G^2}{(1-\beta)^2}\right) \\ &= 3\,\frac{1-\beta}{1+\beta}\left(1+\frac{1}{n-f}\right)\sigma^2+3G^2. \end{aligned}$$

以上即证明了该引理。 □

13.4.2 引理 7 的证明

引理 7. 假设假设 *1* 和 *2* 成立。设 F 是(f,κ)-鲁棒的。考虑采用聚合F的算法 *3*。对于每一步 $t\in[T]$，可得

$$\mathbb{E}\left[\left\|\xi_t\right\|^2\right] \leq 6\kappa\frac{1-\beta}{1+\beta}\sigma^2+48\kappa G^2.$$

证明。 根据 (31) 和 (34)，分别可得

$$m_t \coloneqq F\left(m_t^{(1)},\ldots,m_t^{(n)}\right) \text{ and } \xi_t \coloneqq m_t-\overline{m}_t.$$

考虑任意步骤 t。由于 F 是 (f,κ)-鲁棒的，我们得到

$$\left\|\xi_t\right\|^2=\left\|m_t-\overline{m}_t\right\|^2 \leq \frac{\kappa}{n-f}\sum_{i\in\mathcal{H}}\left\|m_t^{(i)}-\overline{m}_t\right\|^2. \tag{64}$$

对两边取全期望后，我们得到

$$\mathbb{E}\left[\left\|\xi_t\right\|^2\right] \leq \frac{\kappa}{n-f}\sum_{i\in\mathcal{H}}\mathbb{E}\left[\left\|m_t^{(i)}-\overline{m}_t\right\|^2\right]. \tag{65}$$

根据引理 6，在假设2下，我们有

$$\begin{aligned} \mathbb{E}\left[\frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}}\left\|m_t^{(i)}-\overline{m}_t\right\|^2\right] &\leq 3\,\frac{1-\beta}{1+\beta}\left(1+\frac{1}{n-f}\right)\sigma^2+3G^2 \\ &\leq 6\,\frac{1-\beta}{1+\beta}\sigma^2+3G^2. \qquad (n-f\geq 1) \end{aligned}$$

将上述结果代入 (65) 即可证明该引理，也就是说，我们得出

$$\mathbb{E}\left[\left\|\xi_t\right\|^2\right] \leq 6\kappa\frac{1-\beta}{1+\beta}\sigma^2+3\kappa G^2.$$

证明至此结束。 □

13.4.3 引理 8 的证明

引理 8 的证明与 [17] 中引理 3 的证明类似。为完整起见，我们在下文回顾该引理及其证明。**引理 8.** 假设假设 *2*成立。回顾 $\mathcal{L}_{\mathcal{H}}$ 是 L-光滑的。考虑满足 $T>1$ 的算法 *3*。对于所有 $t\geq 2$，我们得到

$$\begin{aligned}\mathbb{E}\left[\left\|\delta_t\right\|^2\right] \leq & \beta^2 c\,\mathbb{E}\left[\left\|\delta_{t-1}\right\|^2\right]+4\gamma L(1+\gamma L)\beta^2\,\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})\right\|^2\right]+(1-\beta)^2\frac{\sigma^2}{(n-f)}\\ & +2\gamma L(1+\gamma L)\beta^2\,\mathbb{E}\left[\left\|\xi_{t-1}\right\|^2\right],\end{aligned}$$

其中 $c:=(1+\gamma L)\ (1+4\gamma L)$。

证明。 回顾式 (35)，有

$$\delta_t \coloneqq \overline{m}_t-\nabla\mathcal{L}_{\mathcal{H}}\left(\theta_{t-1}\right).$$

考虑任意一步 $t>1$。将式 (30) 和 (33) 代入可得

$$\delta_t=\beta\,\overline{m}_{t-1}+(1-\beta)\,\overline{g}_t-\nabla\mathcal{L}_{\mathcal{H}}\left(\theta_{t-1}\right).$$

Up在上式右侧加上并减去 $\beta\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})$ 和 $\beta\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})$ 后，可得

$$\begin{aligned}\delta_t &=\beta\,\overline{m}_{t-1}-\beta\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})+(1-\beta)\,\overline{g}_t-\nabla\mathcal{L}_{\mathcal{H}}\left(\theta_t\right)+\beta\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})+\beta\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\beta\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\\ &=\beta\left(\overline{m}_{t-1}-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})\right)+(1-\beta)\,\overline{g}_t-(1-\beta)\nabla\mathcal{L}_{\mathcal{H}}\left(\theta_{t-1}\right)+\beta\left(\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right).\end{aligned}$$

由于 $m_{t-1}-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})=\delta_{t-1}$（根据 (35)），由上文可得

$$\delta_t=\beta\delta_{t-1}+(1-\beta)\left(\overline{g}_t-\nabla\mathcal{L}_{\mathcal{H}}\left(\theta_{t-1}\right)\right)+\beta\left(\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right).$$

因此，

$$\begin{aligned}\left\|\delta_t\right\|^2 =&\beta^2\left\|\delta_{t-1}\right\|^2+(1-\beta)^2\left\|\overline{g}_t-\nabla\mathcal{L}_{\mathcal{H}}\left(\theta_{t-1}\right)\right\|^2+\beta^2\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2+2\beta(1-\beta)\left\langle\delta_{t-1},\,\overline{g}_t-\nabla\mathcal{L}_{\mathcal{H}}\left(\theta_{t-1}\right)\right\rangle\\ &+2\beta^2\left\langle\delta_{t-1},\,\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\rangle+2\beta(1-\beta)\left\langle\overline{g}_t-\nabla\mathcal{L}_{\mathcal{H}}\left(\theta_{t-1}\right),\,\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\rangle.\end{aligned}$$

对两边取条件期望 $\mathbb{E}_t\left[\cdot\right]$，并回想一下，给定历史 $\mathcal{P}_t$ 时，δ_{t-1}、θ_{t-1} 和 θ_{t-2} 都是确定值，由此可得

$$\begin{aligned}\mathbb{E}_t\left[\left\|\delta_t\right\|^2\right] =&\beta^2\left\|\delta_{t-1}\right\|^2+(1-\beta)^2\mathbb{E}_t\left[\left\|\overline{g}_t-\nabla\mathcal{L}_{\mathcal{H}}\left(\theta_{t-1}\right)\right\|^2\right]+\beta^2\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2+\\ &2\beta(1-\beta)\left\langle\delta_{t-1},\,\mathbb{E}_t\left[\overline{g}_t\right]-\nabla\mathcal{L}_{\mathcal{H}}\left(\theta_{t-1}\right)\right\rangle+2\beta^2\left\langle\delta_{t-1},\,\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\rangle\\ &+2\beta(1-\beta)\left\langle\mathbb{E}_t\left[\overline{g}_t\right]-\nabla\mathcal{L}_{\mathcal{H}}\left(\theta_{t-1}\right),\,\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\rangle.\end{aligned}$$

回想一下，$g_t:=1/(n-f)\sum_{j\in\mathcal{H}}g_t^{(i)}$。因此，我们有 $\mathbb{E}_t\left[g_t\right]=\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})$。利用上述结果可得

$$\begin{aligned}\mathbb{E}_t\left[\left\|\delta_t\right\|^2\right] =&\beta^2\left\|\delta_{t-1}\right\|^2+(1-\beta)^2\mathbb{E}_t\left[\left\|\overline{g}_t-\nabla\mathcal{L}_{\mathcal{H}}\left(\theta_{t-1}\right)\right\|^2\right]+\beta^2\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\\ &+2\beta^2\left\langle\delta_{t-1},\,\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\rangle.\end{aligned}$$

此外，根据假设2以及 $j\in\mathcal{H}$ 的 $g_t^{(j)}$ 彼此独立这一事实，我们得到 $\mathbb{E}_t\left[\left\|g_t-\nabla\mathcal{L}_{\mathcal{H}}\left(\theta_{t-1}\right)\right\|^2\right]\leq\frac{\sigma^2}{n-f()}$。

因此，

$$\mathbb{E}_t\left[\left\|\delta_t\right\|^2\right]\leq\beta^2\left\|\delta_{t-1}\right\|^2+(1-\beta)^2\frac{\sigma^2}{(n-f)}+\beta^2\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2+2\beta^2\left\langle\delta_{t-1},\,\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\rangle.$$

根据柯西-施瓦茨不等式，$\left\langle\delta_{t-1},\ \nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\rangle\leq\left\|\delta_{t-1}\right\|\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|$。由于$\mathcal{L}_{\mathcal{H}}$是 L-光滑的，我们有 $\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|\leq L\left\|\theta_{t-1}-\theta_{t-2}\right\|$。回顾式（32），可知 $\theta_t=\theta_{t-1}-\gamma m_t$。因此，$\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})-\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|\leq\gamma L\left\|m_{t-1}\right\|$。利用上述结果，我们得到

$$\mathbb{E}_t\left[\left\|\delta_t\right\|^2\right]\leq\beta^2\left\|\delta_{t-1}\right\|^2+(1-\beta)^2\frac{\sigma^2}{(n-f)}+\gamma^2\beta^2L^2\left\|m_{t-1}\right\|^2+2\gamma\beta^2L\left\|\delta_{t-1}\right\|\left\|m_{t-1}\right\|.$$

由于 $2ab \le a^2 + b^2$，由上文可得

$$\begin{aligned}\mathbb{E}_t\left[\|\delta_t\|^2\right] &\le \beta^2\|\delta_{t-1}\|^2 + (1-\beta)^2\frac{\sigma^2}{(n-f)} + \gamma^2\beta^2L^2\|m_{t-1}\|^2 + \gamma L\beta^2\left(\|\delta_{t-1}\|^2 + \|m_{t-1}\|^2\right)\\ &= (1+\gamma L)\beta^2\|\delta_{t-1}\|^2 + (1-\beta)^2\frac{\sigma^2}{(n-f)} + \gamma L(1+\gamma L)\beta^2\|m_{t-1}\|^2. \end{aligned} \tag{66}$$

根据式 (34) 中 ξ_t 的定义，我们有 $m_{t-1} = \xi_{t-1} + m_{t-1}$。因此，利用三角不等式以及 $2ab \le a^2 + b^2$ 这一事实，我们有 $\|m_{t-1}\|^2 \le 2\|\xi_{t-1}\|^2 + 2\|m_{t-1}\|^2$。类似地，根据式 (35) 中 δ_t 的定义，我们有 $\|m_{t-1}\|^2 \le 2\|\delta_{t-1}\|^2 + 2\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})\|^2$。因此，$\|m_{t-1}\|^2 \le 2\|\xi_{t-1}\|^2 + 4\|\delta_{t-1}\|^2 + 4\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})\right\|^2$。将其代入式 (66)，我们得到

$$\begin{aligned}\mathbb{E}_t\left[\|\delta_t\|^2\right] \le&(1+\gamma L)\beta^2\|\delta_{t-1}\|^2 + (1-\beta)^2\frac{\sigma^2}{(n-f)}\\ &+ 2\gamma L(1+\gamma L)\beta^2\left(\|\xi_{t-1}\|^2 + 2\|\delta_{t-1}\|^2 + 2\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})\right\|^2\right).\end{aligned}$$

对右侧的各项重新排列，可得

$$\begin{aligned}\mathbb{E}_t\left[\|\delta_t\|^2\right] \le&\beta^2(1+\gamma L)(1+4\gamma L)\|\delta_{t-1}\|^2 + 4\gamma L(1+\gamma L)\beta^2\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})\right\|^2 + (1-\beta)^2\frac{\sigma^2}{(n-f)}\\ &+ 2\gamma L(1+\gamma L)\beta^2\|\xi_{t-1}\|^2.\end{aligned}$$

将上面的 $c = (1+\gamma L)(1+4\gamma L)$ 代入，可得

$$\mathbb{E}_t\left[\|\delta_t\|^2\right] \le \beta^2 c\|\delta_{t-1}\|^2 + 4\gamma L(1+\gamma L)\beta^2\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-2})\right\|^2 + (1-\beta)^2\frac{\sigma^2}{(n-f)} + 2\gamma L(1+\gamma L)\beta^2\|\xi_{t-1}\|^2.$$

回想一下，上述 t 是 $[T]$ 中大于 1 的任意值。因此，对上式两边取全期望，即可证明该引理。

□

13.4.4 引理 9 的证明

引理 9 的证明与 [17] 中引理4的证明类似。为完整起见，我们在下面重述该引理及其证明。**引理 9.** 回想一下，$\mathcal{L}_{\mathcal{H}}$ 是 L-光滑的。考虑算法 3。对于所有 $t \in [T]$，可得

$$\begin{aligned}\mathbb{E}\left[2\mathcal{L}_{\mathcal{H}}(\theta_t) - 2\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right] \le&-\gamma(1-4\gamma L)\mathbb{E}\left[\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right] + 2\gamma(1+2\gamma L)\mathbb{E}\left[\|\delta_t\|^2\right]\\ &+ 2\gamma(1+\gamma L)\mathbb{E}\left[\|\xi_t\|^2\right].\end{aligned}$$

证明。考虑任意一步 t。由于 $\mathcal{L}_{\mathcal{H}}$ 是 L-光滑的，我们有（见 [8]）

$$\mathcal{L}_{\mathcal{H}}(\theta_t) - \mathcal{L}_{\mathcal{H}}(\theta_{t-1}) \le \left\langle\theta_t - \theta_{t-1}, \nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\rangle + \frac{L}{2}\left\|\theta_t - \theta_{t-1}\right\|^2.$$

代入公式（36），即 $\theta_t = \theta_{t-1} - \gamma m_t = \theta_{t-1} - \gamma\xi_t$，可得

$$\begin{aligned}\mathcal{L}_{\mathcal{H}}(\theta_t) - \mathcal{L}_{\mathcal{H}}(\theta_{t-1}) &\le -\gamma\left\langle\overline{m}_t, \nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\rangle - \gamma\left\langle\xi_t, \nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\rangle + \gamma^2\frac{L}{2}\|\overline{m}_t + \xi_t\|^2\\ &= -\gamma\left\langle\overline{m}_t - \nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1}) + \nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1}), \nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\rangle - \gamma\left\langle\xi_t, \nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\rangle + \gamma^2\frac{L}{2}\|\overline{m}_t + \xi_t\|^2.\end{aligned}$$

By D定义（35），$\overline{m}_t - \nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1}) = \delta_t$。因此，由上文可得（缩放因子为 2 ）

$$2\mathcal{L}_{\mathcal{H}}(\theta_t) - 2\mathcal{L}_{\mathcal{H}}(\theta_{t-1}) \le -2\gamma\left\|\nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2 - 2\gamma\left\langle\delta_t, \nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\rangle - 2\gamma\left\langle\xi_t, \nabla\mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\rangle + \gamma^2L\|\overline{m}_t + \xi_t\|^2. \tag{67}$$

现在，我们分别考虑右侧的最后三项。利用柯西-施瓦茨不等式以及对任意 $c > 0$ 都有 $2ab \leq \frac{1}{c}a^2 + cb^2$ 这一事实，可得（代入 $c = 2$）

$$2\left|\left\langle \delta_t,\, \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\rangle\right| \leq 2\left\|\delta_t\right\| \left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\| \leq \frac{2}{1}\left\|\delta_t\right\|^2 + \frac{1}{2}\left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2. \tag{68}$$

同理,

$$2\left|\left\langle \xi_t,\, \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\rangle\right| \leq 2\left\|\xi_t\right\| \left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\| \leq \frac{2}{1}\left\|\xi_t\right\|^2 + \frac{1}{2}\left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2. \tag{69}$$

最后，利用三角不等式以及 $2ab \leq a^2 + b^2$ 这一事实，我们得到

$$\begin{aligned}\left\|\,\overline{m}_t + \xi_t\right\|^2 &\leq 2\,\left\|\overline{m}_t\right\|^2 + 2\left\|\xi_t\right\|^2 = 2\,\left\|\overline{m}_t - \nabla \mathcal{L}_{\mathcal{H}}(\theta_t) + \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2 + 2\left\|\xi_t\right\|^2 \\ &\leq 4\,\left\|\delta_t\right\|^2 + 4\,\left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2 + 2\left\|\xi_t\right\|^2. \qquad [\text{since } \overline{m}_t - \nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1}) = \delta_t]\end{aligned} \tag{70}$$

将 (68)、(69) 和 (70) 代入 (67)，我们得到

$$\begin{aligned}2\mathcal{L}_{\mathcal{H}}(\theta_t) - 2\mathcal{L}_{\mathcal{H}}(\theta_{t-1}) \leq &-2\gamma\left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2 + \gamma\left(2\left\|\delta_t\right\|^2 + \frac{1}{2}\left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right) + \gamma\left(2\left\|\xi_t\right\|^2 + \frac{1}{2}\left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2\right) \\ &+ \gamma^2 L\left(4\,\left\|\delta_t\right\|^2 + 4\,\left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2 + 2\left\|\xi_t\right\|^2\right).\end{aligned}$$

重新整理右侧各项后，我们得到

$$2\mathcal{L}_{\mathcal{H}}(\theta_t) - 2\mathcal{L}_{\mathcal{H}}(\theta_{t-1}) \leq -\gamma\left(1 - 4\gamma L\right)\left\|\nabla \mathcal{L}_{\mathcal{H}}(\theta_{t-1})\right\|^2 + 2\gamma\left(1 + 2\gamma L\right)\left\|\delta_t\right\|^2 + 2\gamma\left(1 + \gamma L\right)\left\|\xi_t\right\|^2.$$

由于 t 是从 $[T]$ 中任意选取的，对上述等式两边取期望即可证明该引理。 □

14 实验设置

14.1 详细实验设置

模型的架构以及实验设置的其他细节见表3。请注意，CNN 表示卷积神经网络，NLL 表示负对数似然损失。为了展示所用模型的架构，我们引入以下简洁的符号约定。

L（#outputs）表示一个**全连接线性层**，R 表示**ReLU激活函数**，S 表示**对数Softmax**，
C（#channels）表示一个全连接二维卷积层（卷积核大小为 5，填充为 0，步幅为 1），M 表示
二维最大池化（卷积核大小为 2），B 表示**批归一化**，D 表示**随机失活**（固定概率为 0.25）。

数据集	MNIST 和 Fashion-MNIST	CIFAR-10
模型类型	CNN	CNN
模型架构	C(20)-R-M-C(20)-R-M-L(500)-R-L(10)-S	(3,32×32)-C(64)-R-B-C(64)-R-B-M-D-C(128)-R-B-C(128)-R-B-M-D-L(128)-R-D-L(10)-S
Loss	NLL	NLL
梯度裁剪	2	5
ℓ_2-正则化	10^{-4}	10^{-2}
步数	$T = 800$	$T = 2000$
学习率	$\gamma_t = \frac{0.75}{1 + \lfloor \frac{t}{50} \rfloor}$	$\gamma_t = \begin{cases} 0.25 & t \leq 1500 \\ 0.025 & 1500 < t \leq 2000 \end{cases}$
动量参数	$\beta = 0.9$	$\beta = 0.9$，0。99
批次大小	$b = 25$	$b = 50$
工作节点总数	$n = 17$	$n = 17$
拜占庭工作节点数量	$f = 4$, 6,8	$f = 2$,3, 4

表3：模型架构、超参数和分布式设置

在所有数据集上，我们采用四种聚合规则实现 NNM 和分桶：几何中位数（GM）、坐标中位数（CWMed）、坐标截尾均值（CWTM）和 Krum。在每种设置中，我们都使用桶大小为 $s = \lfloor \frac{n}{2f} \rfloor$ [26] 的分桶算法。我们还实现了原始聚合规则。

请注意，当 $f = 4$（共 $n = 17$ 个）时，分桶+CWMed 和分桶+CWTM 完全等价。事实上，当$f = 4$时，每个桶的大小为 $s = 2$。因此，应用分桶后总共有 $n' = 9$ 个桶，其中可能有 $f' = 4$ 个桶包含拜占庭工作节点（即至少被一个拜占庭工作节点污染）。由此显然可见，使用 $n' = 9$ 和 $f' = 4$（即分桶后）执行 CWMed 和 CWTM 会输出相同的向量。因此，当 $f = 4$时，我们仅在附录 15 的图表中展示使用分桶+CWMed 的学习效果。最后请注意，我们采用了深度学习中的常用技巧来提高准确率，例如梯度裁剪。事实上，后者可能会对我们设置中的鲁棒聚合产生额外的积极影响，我们也正在对此进行研究。

14.2 数据集预处理

MNIST 的输入图像归一化采用均值 0.1307 和标准差 0.3081；Fashion-MNIST 则通过添加水平翻转图像进行扩充。此外，CIFAR-10 的图像也进行了水平翻转，并且还应用了逐通道归一化，均值为 0.4914、0.4822、0.4465，标准差为 0.2023、0.1994、0.2010。

14.3 拜占庭攻击

在我们的实验中，拜占庭工作节点执行五种最先进的梯度攻击，分别是 A Little is Enough（ALIE） [5],Fall of Empires（FOE） [47], 符号翻转（SF） [3], 标签翻转（LF） [3], 和 Mimic [26]。前三种攻击依赖于下文解释的同一种基本方法。

令 a_t 为第 t 步中的攻击向量，$\eta \geq 0$ 为一个固定实数。在每一步 t，拜占庭工作节点都会向服务器发送拜占庭向量 $B_t = s_t + \eta a_t$，其中 s_t 是对第 t 步真实梯度（或动量）的估计。

在实验中，运行梯度下降（GD）算法时，我们设定 $s_t = \frac{1}{|\mathcal{H}|} \sum_{i \in \mathcal{H}} g_t^{(i)}$，其中 $g_t^{(i)}$ 是诚实工作节点 w_i 在第 t步计算出的梯度。然而，执行随机重球法（SHB）时，我们设定 $s_t = \frac{1}{|\mathcal{H}|} \sum_{i \in \mathcal{H}} m_t^{(i)}$，其中 $m_t^{(i)}$ 是诚实工作节点 w_i 在第 t步发送的动量向量。

- **ALIE：** 在这种攻击中，$a_t = \sigma_t$，其中 σ_t 是 s_t逐坐标的标准差。
- **FOE：** 在这种攻击中，$a_t = -s_t$。因此，所有拜占庭工作节点在步骤 t中都会发送 $(1-\eta)s_t$。
- **SF：** 在这种攻击中，$a_t = -s_t$，并且 $\eta = 2$。因此，所有拜占庭工作节点在步骤 t中都会发送 $B_t = a_t = -s_t$。

在我们的实验中，与 [42], 中的做法相同，我们实现了 ALIE 和 FOE 的优化版本，其中最优的 η 通过在预先设定的取值范围内进行线性搜索来贪心确定。在每一步 t中，我们选择 η 的取值，使服务器端聚合规则 R_t 的输出与诚实梯度或动量的平均值之间的 L2 距离最大，即 s_t。换句话说，我们选择 η 的取值，使拜占庭工作节点造成的损害最大（以其与诚实输入平均值之间的 L2 距离衡量）。

另一方面，LF 和 Mimic 的执行方式如下：

- **LF：** 每个拜占庭工作节点都使用翻转标签计算其梯度。由于 l MNIST、Fashion-MNIST 和 CIFAR-10 的标签处于 $\{0, 1, ..., 9\}$中，拜占庭工作节点通过在批次上计算 $l' = 9 - l$ 来翻转标签，其中 l'是翻转后的／修改后的标签。

- **Mimic：** 所有拜占庭工作节点只需将某个诚实工作节点的梯度或动量发送给服务器，即可“模仿”该诚实工作节点。为了在学习过程中选择要模仿的诚实工作节点，我们采用了 [26]提出的启发式方法。

14.4 数据异质性

为了在实验中模拟异质性，我们使用参数为 α 的 **Dirichlet** 分布从原始数据集（即 MNIST、Fashion-MNIST 和 CIFAR-10 ）中进行采样，该参数表示工作节点数据集所引入的异质性程度。α 越小，设置的异质性越强（即工作节点越可能只拥有来自某一类别的样本）。在实验中，我们考虑了三种异质性情形，分别是 $\alpha = 0.1$ 时的 极端情形、 $\alpha = 1$ 时的 中等情形，以及 $\alpha = 10$ 时的 低异质性情形。不同工作节点之间样本数量和类别标签的相应分布（取决于 α）如图 3 所示。

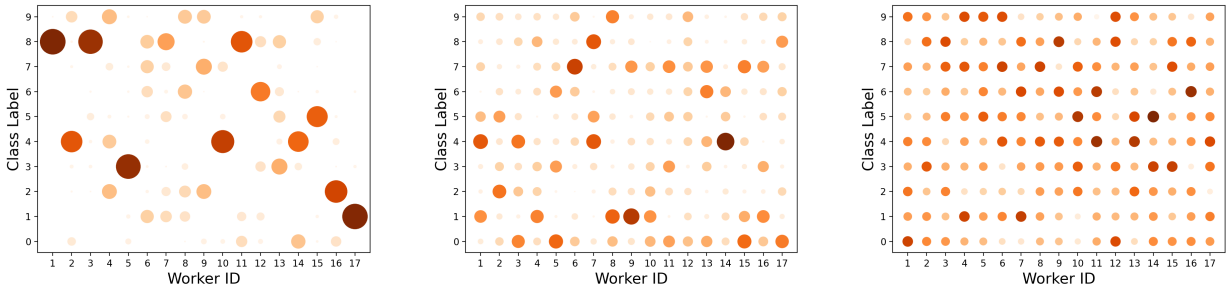

图 3：从参数为 α 的狄利克雷分布中进行采样时，MNIST/CIFAR-10 上各工作节点与类别标签之间的数据样本分布。左：$\alpha = 0.1$，中：$\alpha = 1$，右：$\alpha = 10$。

15 完整实验结果

第 15.1 节介绍了我们在 MNIST 数据集上的结果。第 15.2 节介绍了我们在 Fashion-MNIST 上的结果。第 15.3 节展示了我们的算法在 CIFAR-10 上的性能。

15.1 MNIST 上的综合结果

本节将展示我们在 MNIST 数据集上的全部实验结果。

15.1.1 D-SHB 的实验结果

我们考虑三种拜占庭设置：总计 $n = 17$ 个工作节点中有 $f = 4$、$f = 6$ 和 $f = 8$（可能的最大值）。我们还考虑三种异质性情形：$\alpha = 0.1$（极端）、$\alpha = 1$（中等）和 $\alpha = 10$（低）。我们比较 NNM 和分桶在采用四种聚合规则时的性能，分别为 Krum [7], 几何中位数 [43], CWMed [48],和 CWTM [48]。下方给出了图表，这些结果补充了正文第 6 节第 6.2 节中表 2 的（部分）结果。需要注意的是，在最强的两种拜占庭设置下，即当 $f > 4$ 时，分桶只能在桶大小为 $s = 1$ [26] 的情况下应用。这意味着，当 $f = 6$ 时，8 时，执行分桶就等同于运行原始聚合规则。

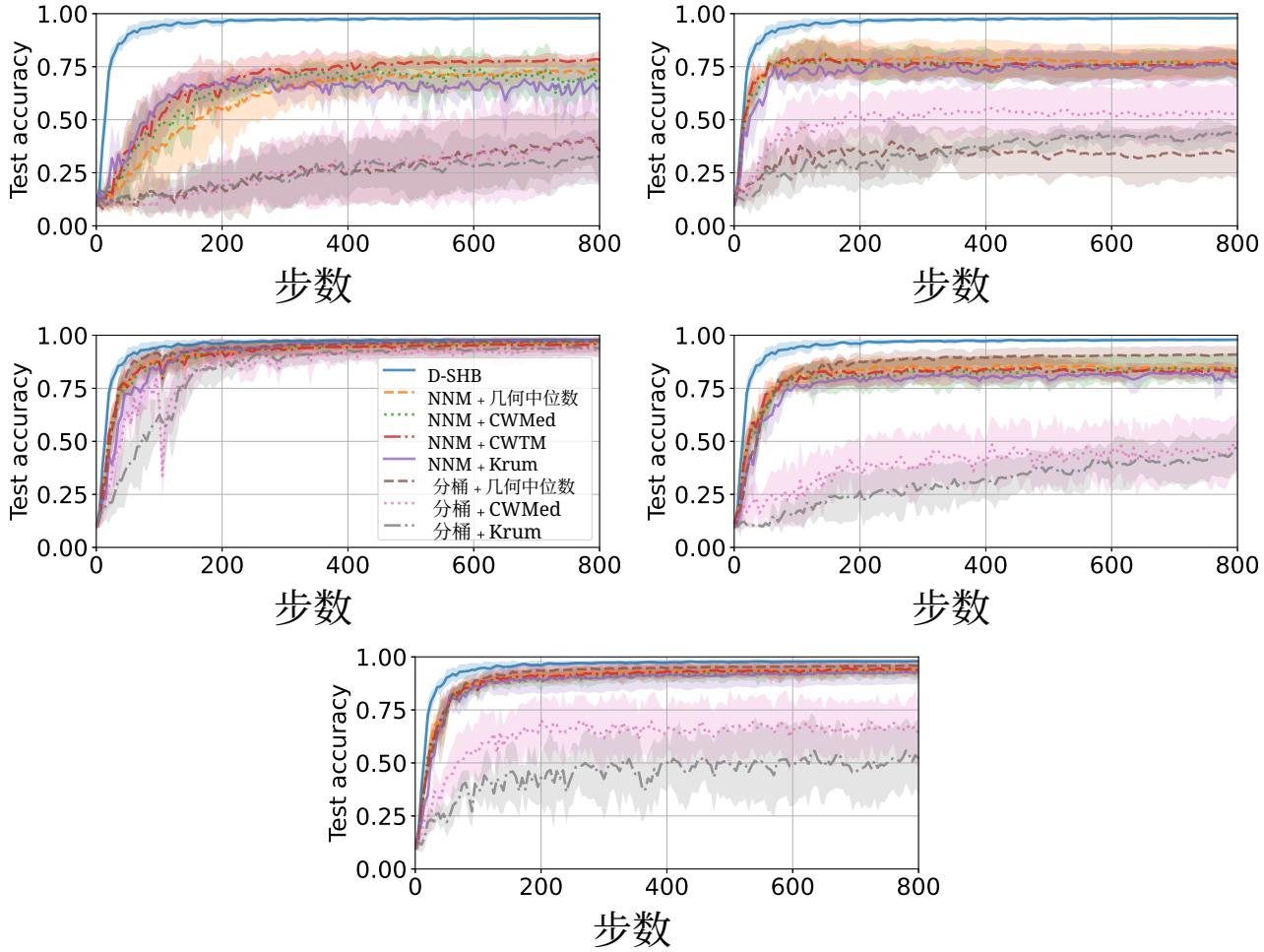

图 4：使用鲁棒 D-SHB 在 MNIST 上进行的实验，其中 $n = 17$ 个工作节点中有 $f = 4$ 个为拜占庭工作节点，$\beta = 0.9$ 和 $\alpha = 0.1$。拜占庭工作节点分别执行 FOE（第 *1* 行，左）、ALIE（第 *1* 行，右）、Mimic（第 *2* 行，左）、SF（第 *2* 行，右）和 LF（第 *3* 行）。

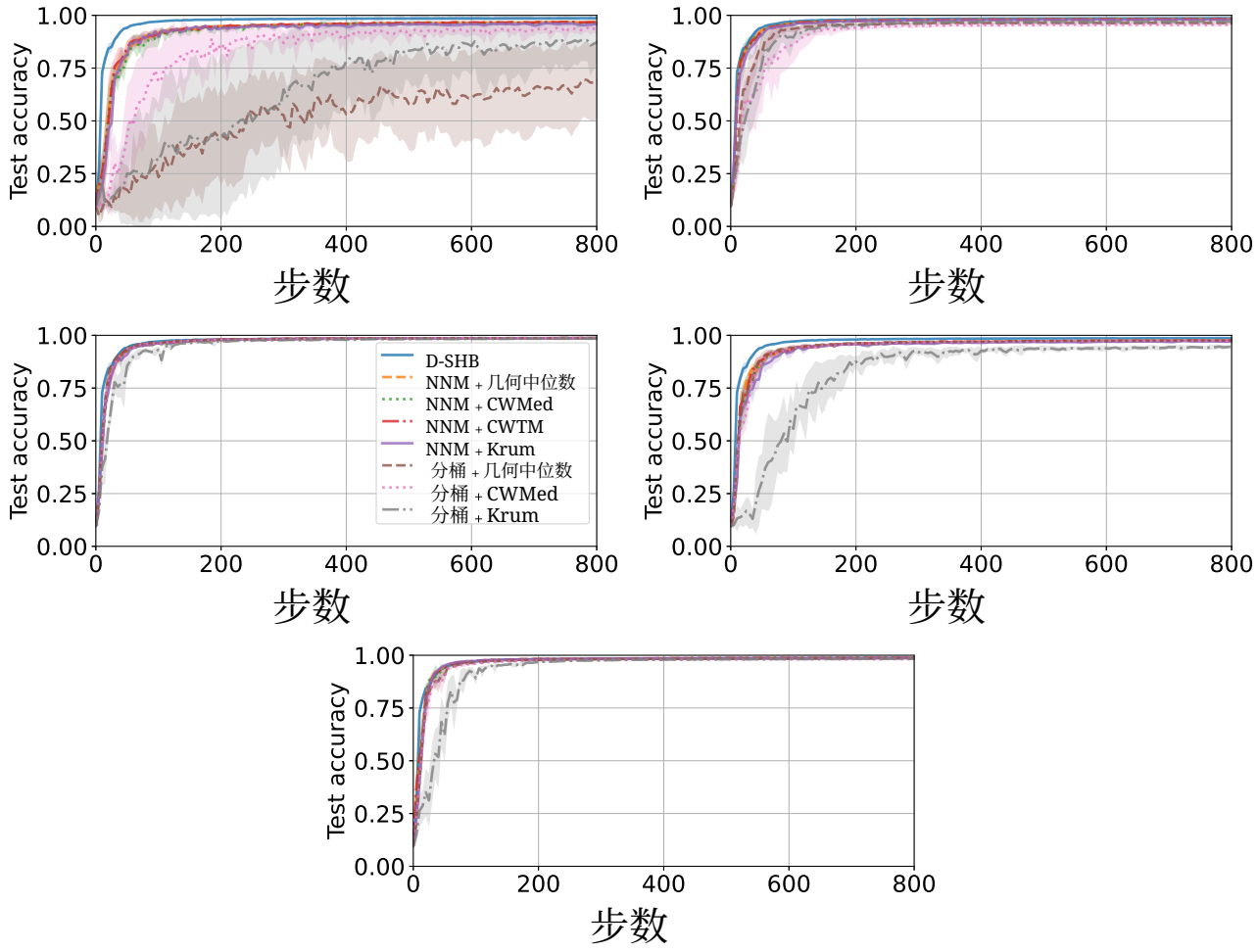

图5：使用鲁棒 D-SHB 在 MNIST 上进行的实验，其中 $f = 4$ 位于 $n = 17$ 个工作节点中，并采用 $\beta = 0.9$ 和 $\alpha = 1$。拜占庭工作节点执行 FOE（第 *1* 行，左侧）、ALIE（第 *1* 行，右侧）、Mimic（第 *2* 行，左侧）、SF（第 *2* 行，右侧）和标签翻转（第 *3* 行）。

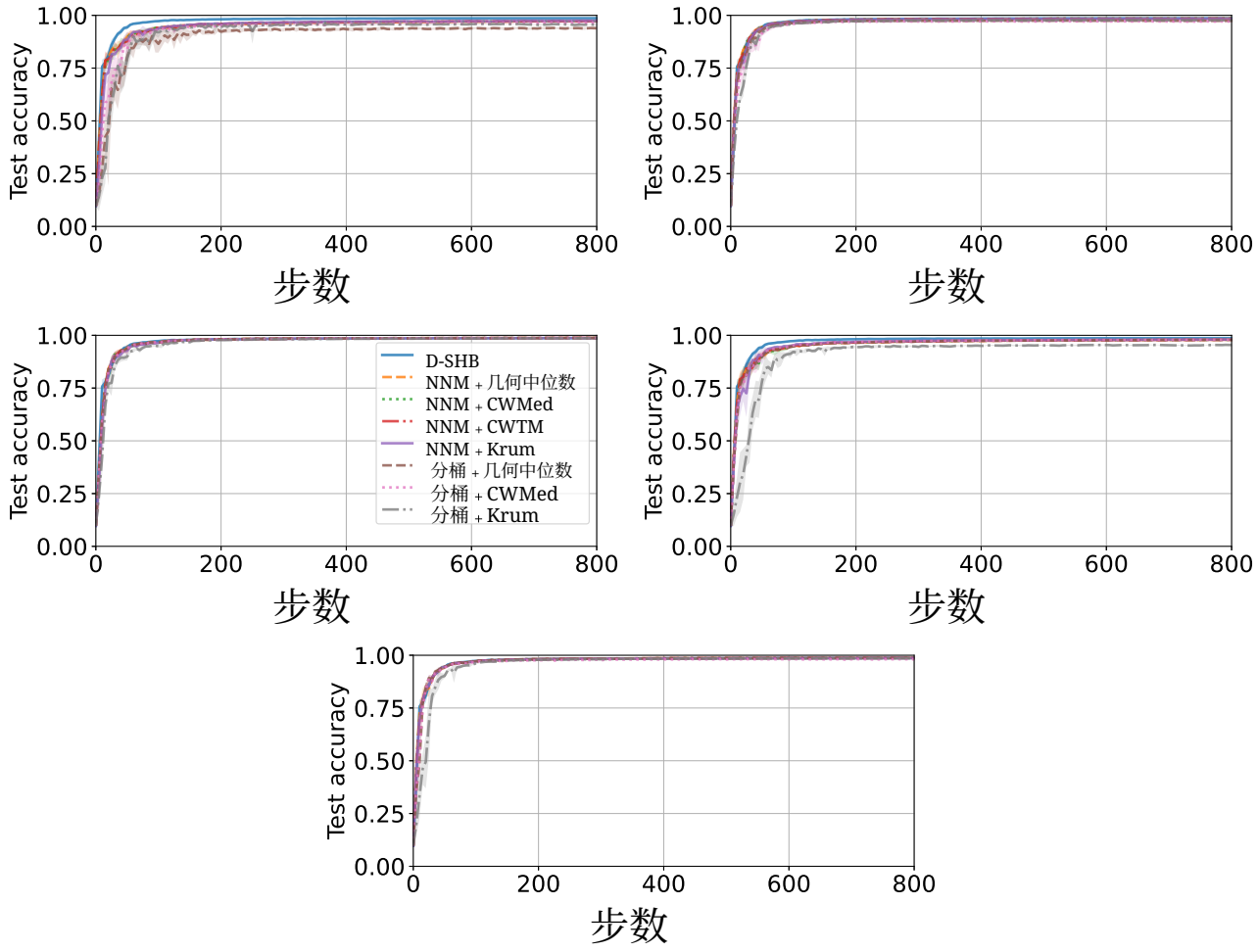

图6：使用 $f = 4$ 在 $n = 17$ 个工作节点中，采用 $\beta = 0.9$ 和 $\alpha = 10$ 的鲁棒 D-SHB 在 MNIST 上进行的实验。拜占庭工作节点执行 FOE（第*1*行，左）、ALIE（第*1*行，右）、Mimic（第*2*行，左）、SF（第*2*行，右）和 LF（第*3*行）。

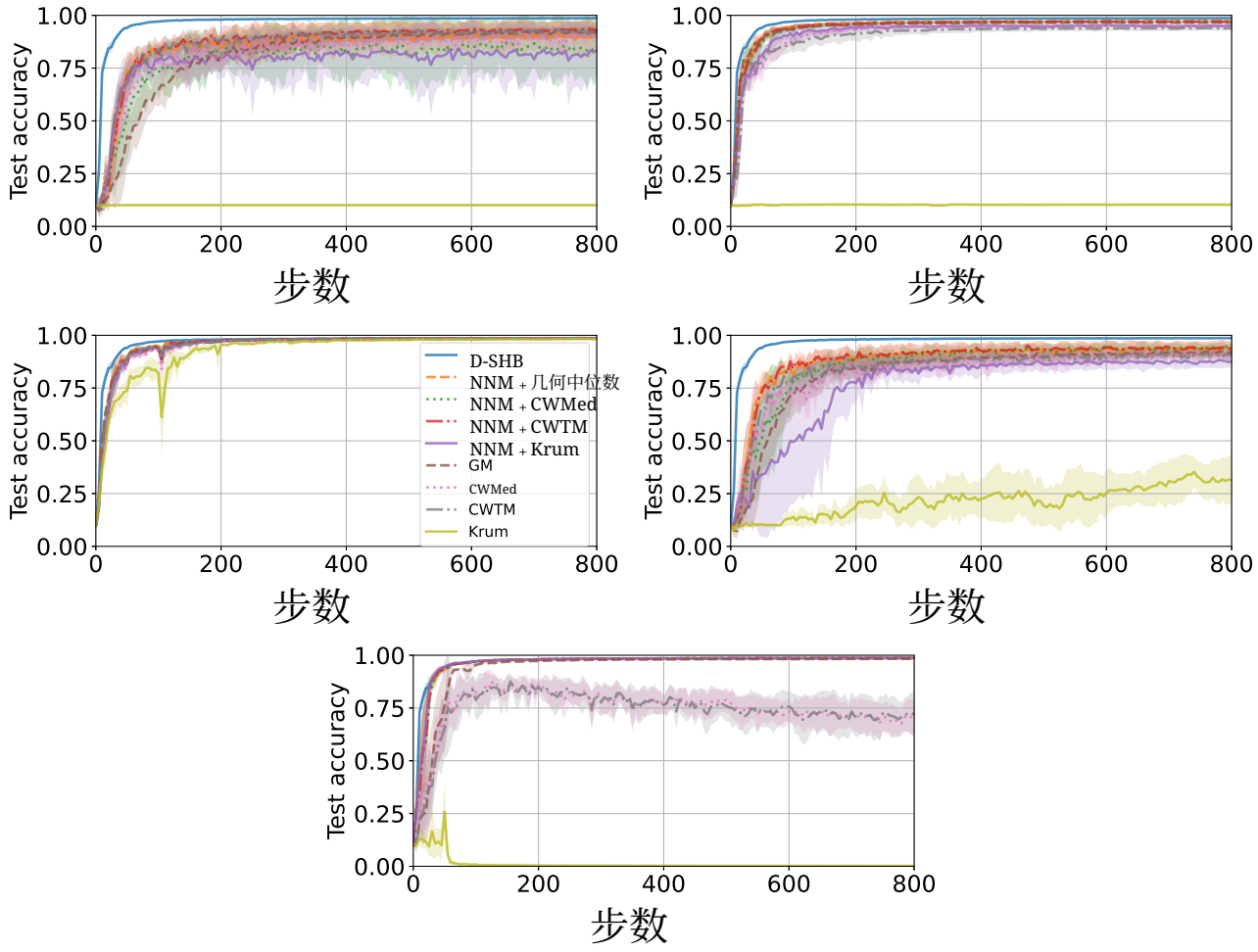

图 7：在 MNIST 上使用鲁棒 D-SHB 的实验，其中 $n = 17$ 个工作节点中有 $f = 6$，使用 $\beta = 0.9$ 和 $\alpha = 1$。拜占庭工作节点执行 FOE（第 *1* 行，左侧）、ALIE（第 *1* 行，右侧）、Mimic（第 *2* 行，左侧）、SF（第 *2* 行，右侧）和标签翻转（第 *3* 行）。

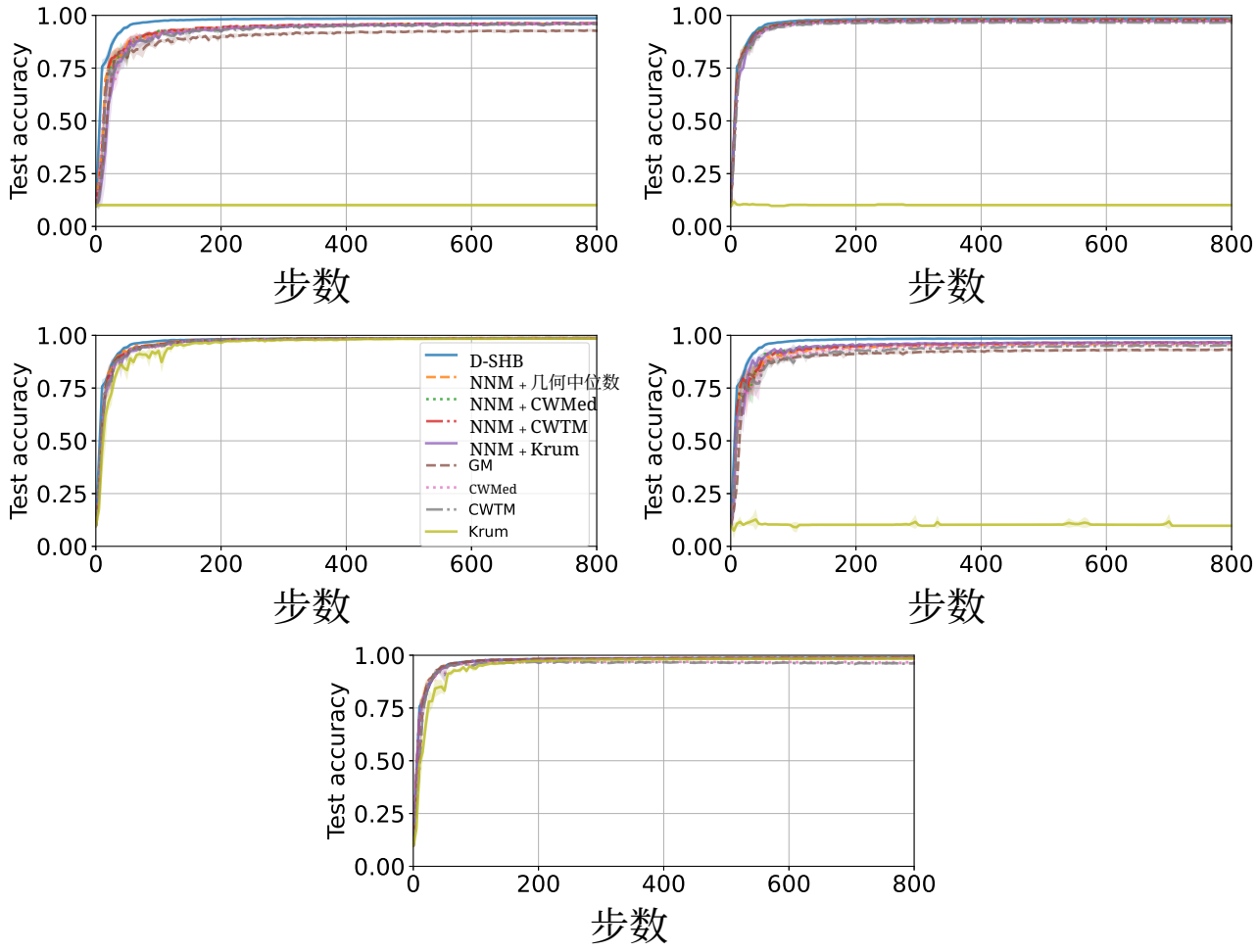

图 8：使用鲁棒 D-SHB 在 $f = 6$ 个工作节点中进行 $n = 17$，并使用 $\beta = 0.9$ 和 $\alpha = 10$ 在 MNIST 上开展的实验。拜占庭工作节点执行 FOE（第 *1* 行，左）、ALIE（第 *1* 行，右）、Mimic（第 *2* 行，左）、SF（第 *2* 行，右）和 LF（第 *3* 行）。

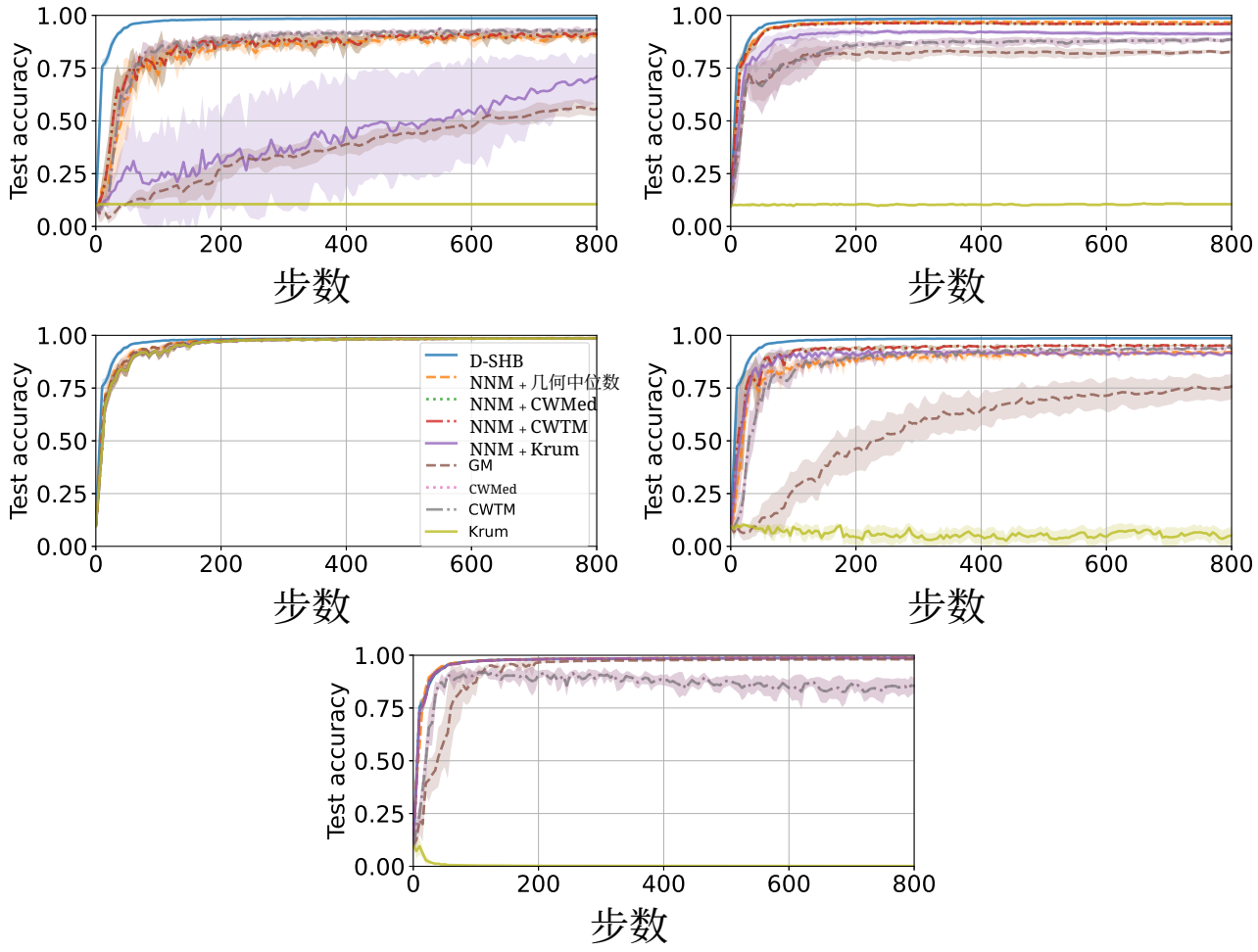

图 9：使用鲁棒 D-SHB 在 MNIST 上进行的实验，其中 $f = 8$ 个工作节点中有 $n = 17$，并采用 $\beta = 0.9$ 和 $\alpha = 10$。拜占庭工作节点执行 FOE（第 *1* 行，左侧）、ALIE（第 *1* 行，右侧）、Mimic（第 *2* 行，左侧）、SF（第 *2* 行，右侧）和 LF（第 *3* 行）。

15.1.2 分布式梯度下降的结果

我们还在一种拜占庭设置下，使用鲁棒 D-GD 在 MNIST 上测试了我们的算法：总共 $n = 17$ 个工作节点中有 $f = 4$ 个拜占庭工作节点。我们还考虑了三种异质性设置： $\alpha = 0.1$、 $\alpha = 1$ 和 $\alpha = 10$。结果如下所示，呈现出与附录 15.1 中相同的观察结果。

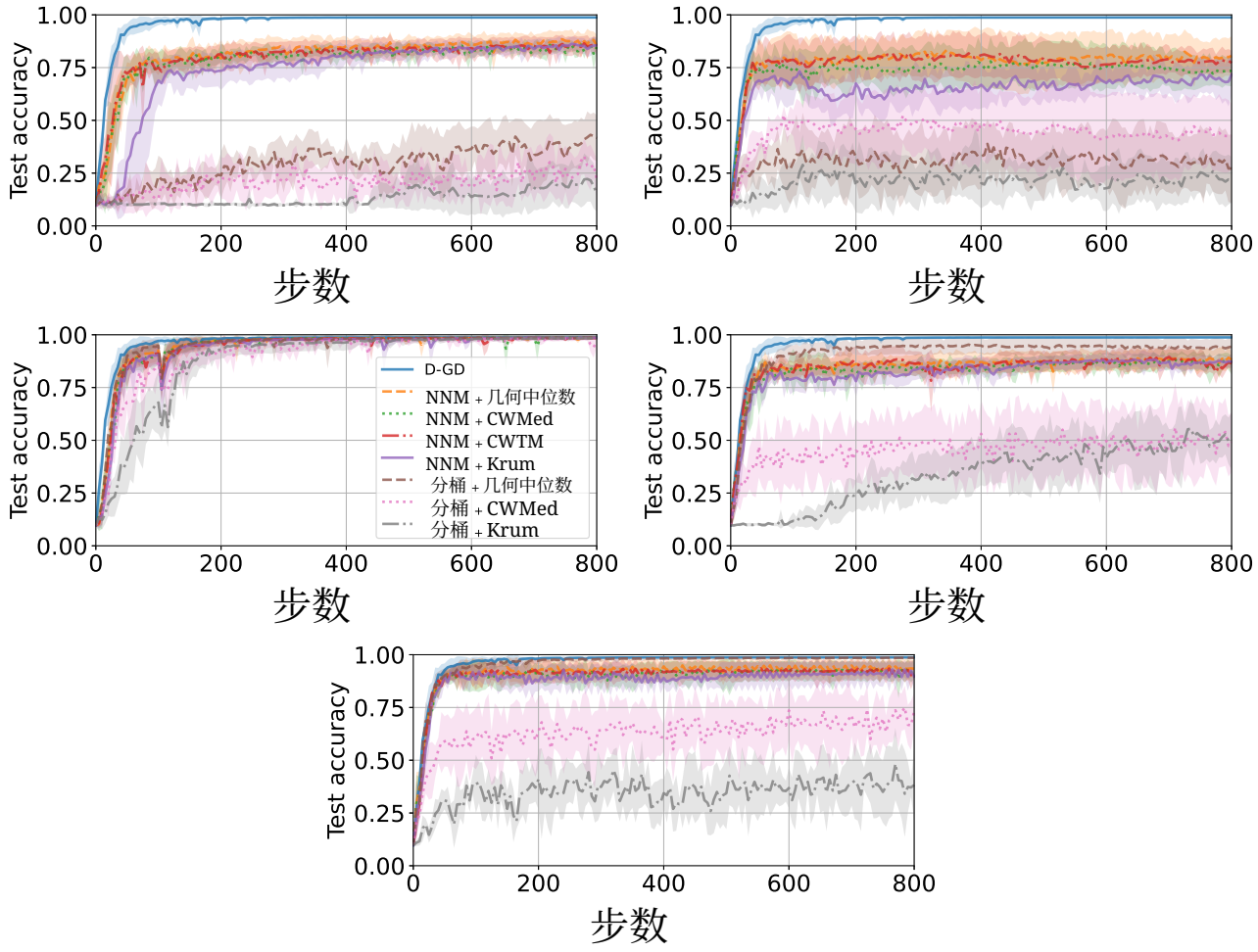

图 10：在 MNIST 上使用鲁棒 D-GD 进行的实验，其中 $n = 17$ 个工作节点中有 $f = 4$ 个，且 $\alpha = 0.1$。拜占庭工作节点执行 FOE（第 *1* 行，左侧）、ALIE（第 *1* 行，右侧）、Mimic（第 *2* 行，左侧）、SF（第 *2* 行，右侧）和 LF（第 *3* 行）攻击。

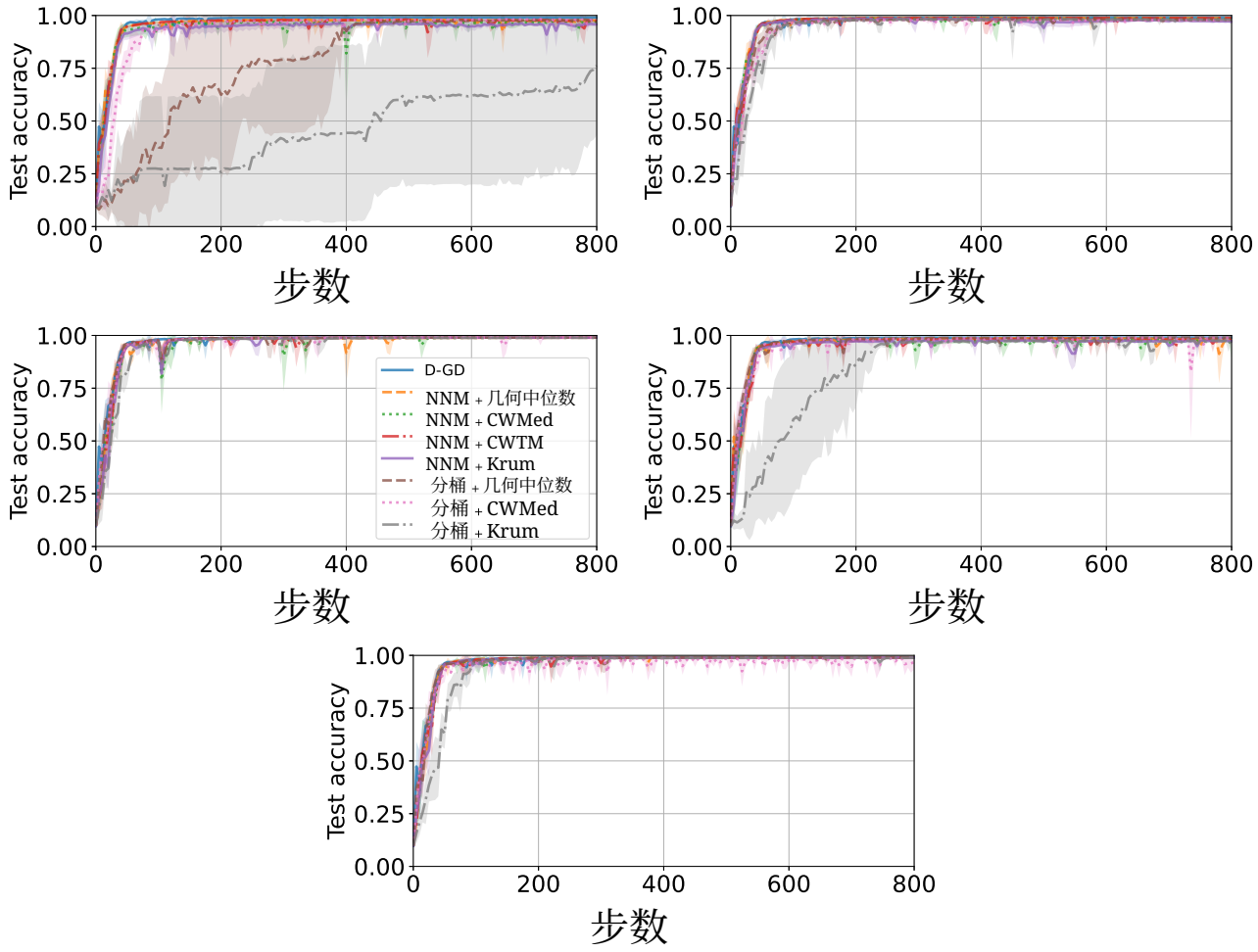

图 11：在 MNIST 上使用鲁棒 D-GD 进行的实验，$f = 4$ 个工作节点中有 $n = 17$ 个采用 $\alpha = 1$。拜占庭工作节点执行 FOE（第 *1* 行，左）、ALIE（第 *1* 行，右）、Mimic（第 *2* 行，左）、SF（第 *2* 行，右）和 LF（第 *3* 行）攻击。

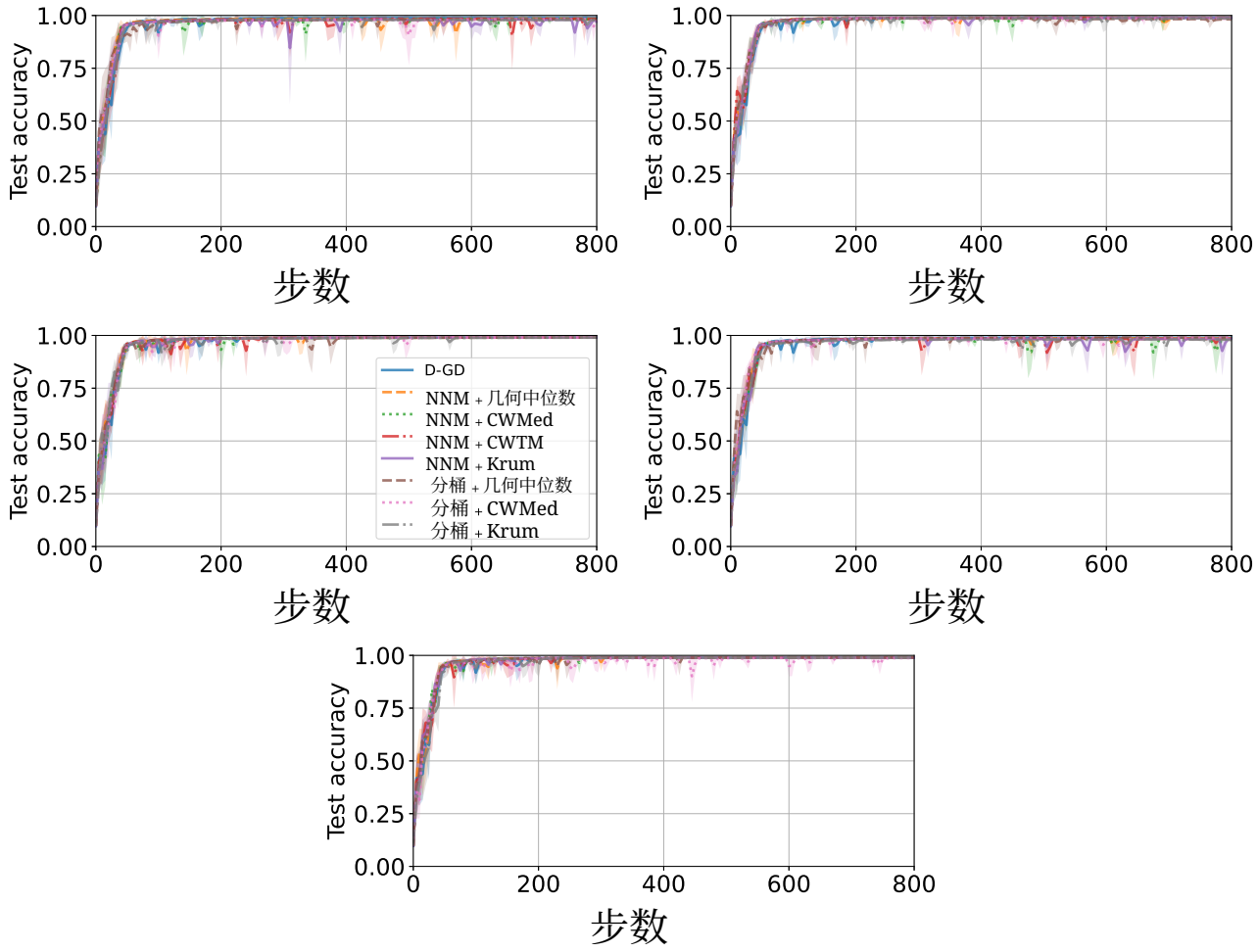

图 12：使用鲁棒 D-GD 在 MNIST 上进行的实验，其中 $f = 4$ 个工作节点中有 $n = 17$， $\alpha = 10$。拜占庭工作节点执行 FOE（第 *1* 行，左侧）、ALIE（第 *1* 行，右侧）、Mimic（第 *2* 行，左侧）、SF（第 *2* 行，右侧）和 LF（第 *3* 行）攻击。

15.1.3 其他聚合规则的结果：MDA、MultiKrum 和 MeaMed

我们还使用三种额外的聚合规则运行 NNM，即 MDA [40, 13], MeaMed [46], 和 Multi-Krum [7]。实验设置如下。我们考虑三种拜占庭设置：总计 $n = 17$ 个工作节点中有 $f = 4$、$f = 6$ 和 $f = 8$ 个（可能的最大数量）是拜占庭节点。我们还考虑三种异质性情形：$\alpha = 0.1$（极端）、$\alpha = 1$（中等）和$\alpha = 10$（低）。我们比较 NNM 和分桶在使用 MDA、MultiKrum 和 MeaMed 时的表现。结果（如下所示）与附录 15.1 中的结果非常相似，并得出了与第 6 节完全相同的观察结果。事实上，NNM 与这些方法结合，在三种数据异质性情形下以及面对五种最先进的拜占庭攻击时，均能在 MNIST 上持续取得良好表现。鉴于目前尚未为这些聚合技术推导出任何保证，一个有趣的未来方向是证明 MDA、MultiKrum 和 MeaMed 是 (f, κ)-鲁棒的，且 $\kappa \in \mathcal{O}(1)$，从而确认我们的方法具有模块化特性，可作为异质拜占庭学习的可靠框架。

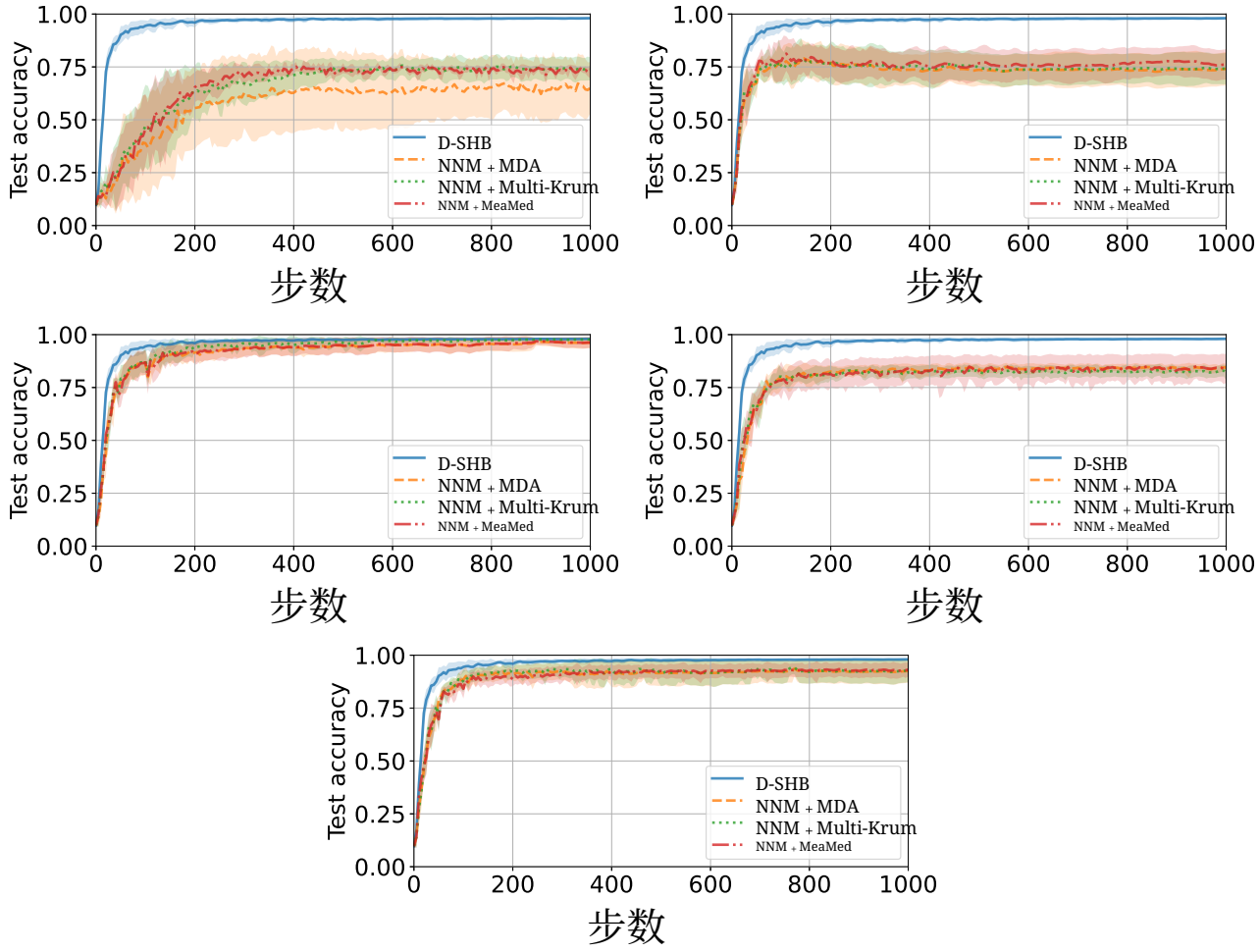

图 13：使用鲁棒 D-SHB 在 MNIST 上进行实验，其中 $n = 17$ 个工作节点中有 $f = 4$ 个拜占庭工作节点，且 $\beta = 0.9$ 和 $\alpha = 0.1$。拜占庭工作节点执行 FOE（第 *1* 行，左）、ALIE（第 *1* 行，右）、Mimic（第 *2* 行，左）、SF（第 *2* 行，右）和 LF（第 *3* 行）攻击。

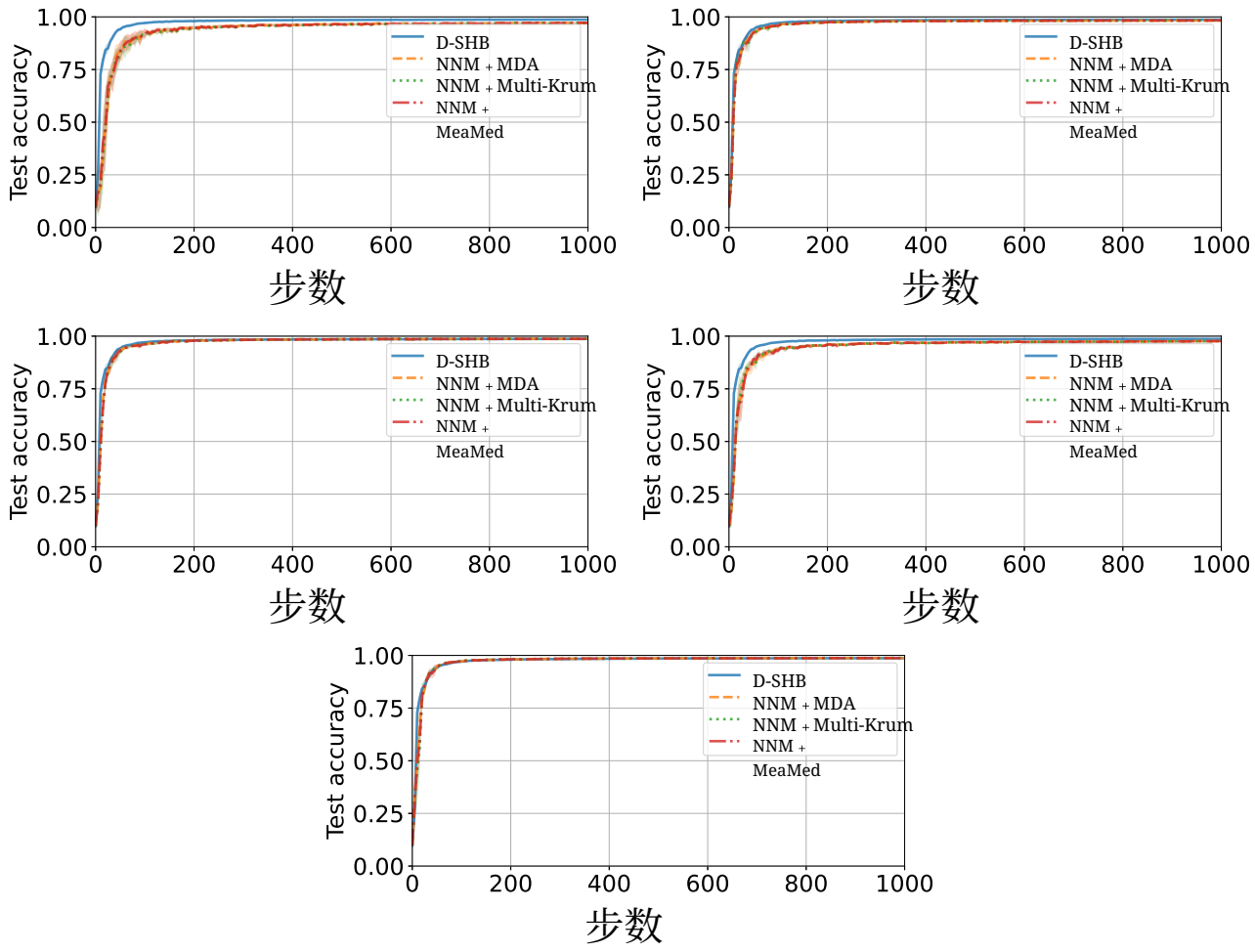

图14：使用鲁棒 D-SHB 在 MNIST 上进行的实验，其中 $n = 17$ 个工作节点中有 $f = 4$ 个拜占庭工作节点，且 $\beta = 0.9$ 和 $\alpha = 1$。拜占庭工作节点执行 FOE（第 *1* 行，左侧）、ALIE（第 *1* 行，右侧）、Mimic（第 *2* 行，左侧）、SF（第 *2* 行，右侧）和 LF（第 *3* 行）攻击。

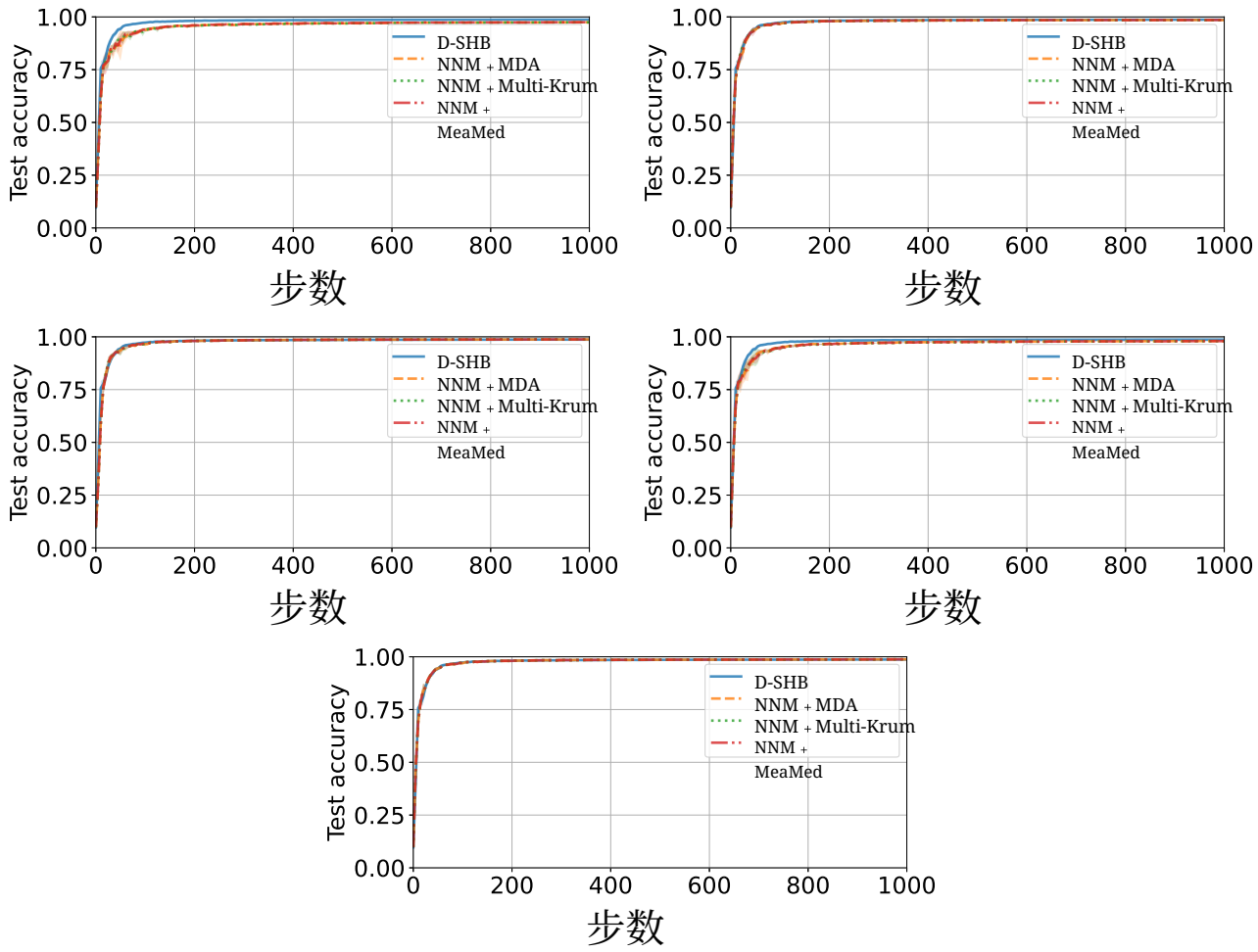

图 15：使用鲁棒 D-SHB 在 MNIST 上进行的实验，其中 $n = 17$ 个工作节点中有 $f = 4$ 个拜占庭工作节点，采用 $\beta = 0.9$ 和 $\alpha = 10$。拜占庭工作节点执行 FOE（第 *1* 行，左）、ALIE（第 *1* 行，右）、Mimic（第 *2* 行，左）、SF（第 *2* 行，右）和 LF（第 *3* 行）攻击。

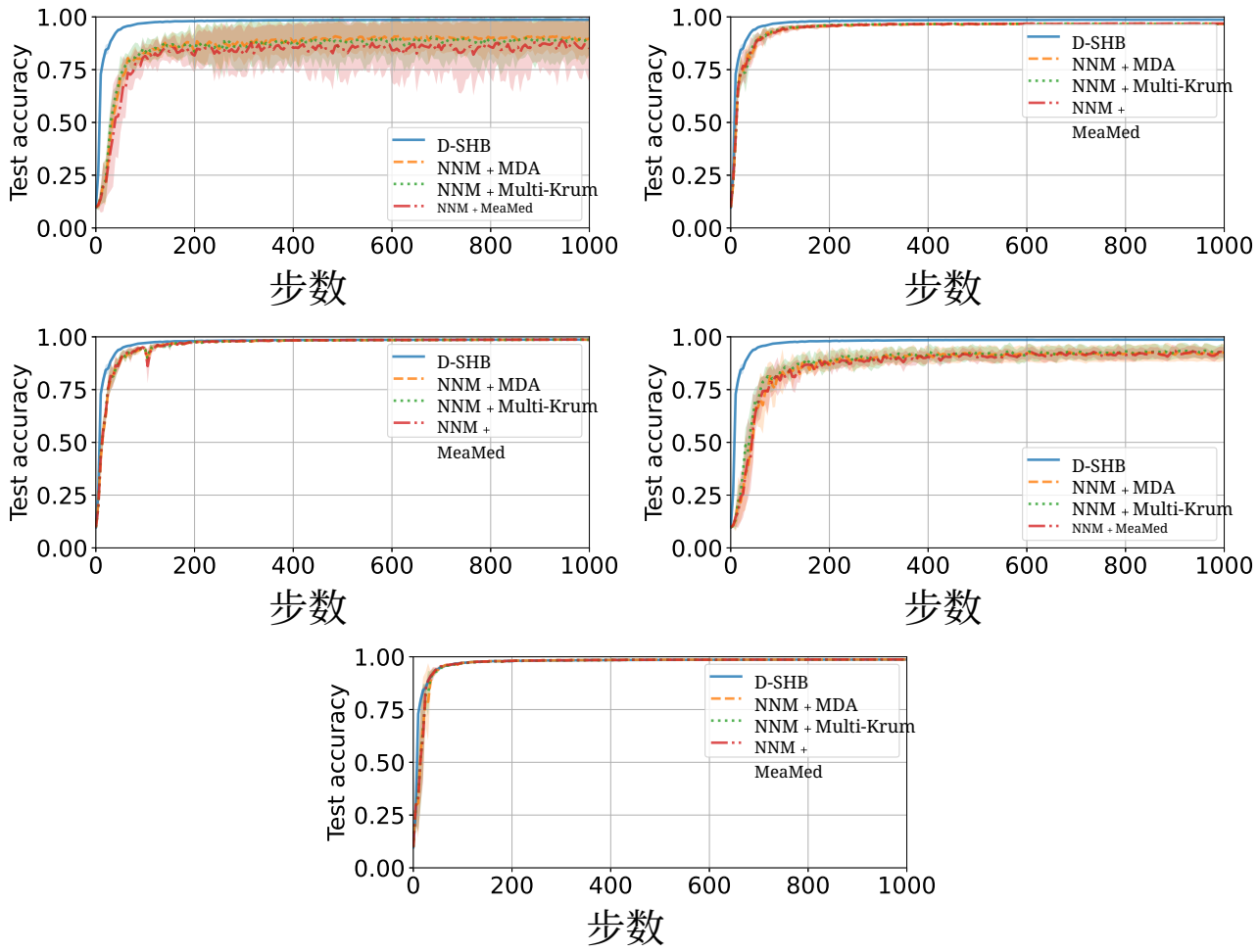

图16：使用鲁棒 D-SHB 在 MNIST 上进行的实验，其中 $n = 17$ 个工作节点中有 $f = 6$ 个拜占庭工作节点，$\beta = 0.9$ 和 $\alpha = 1$。拜占庭工作节点执行 FOE（第 *1* 行，左侧）、ALIE（第 *1* 行，右侧）、Mimic（第 *2* 行，左侧）、SF（第 *2* 行，右侧）和 LF（第 *3* 行）攻击。

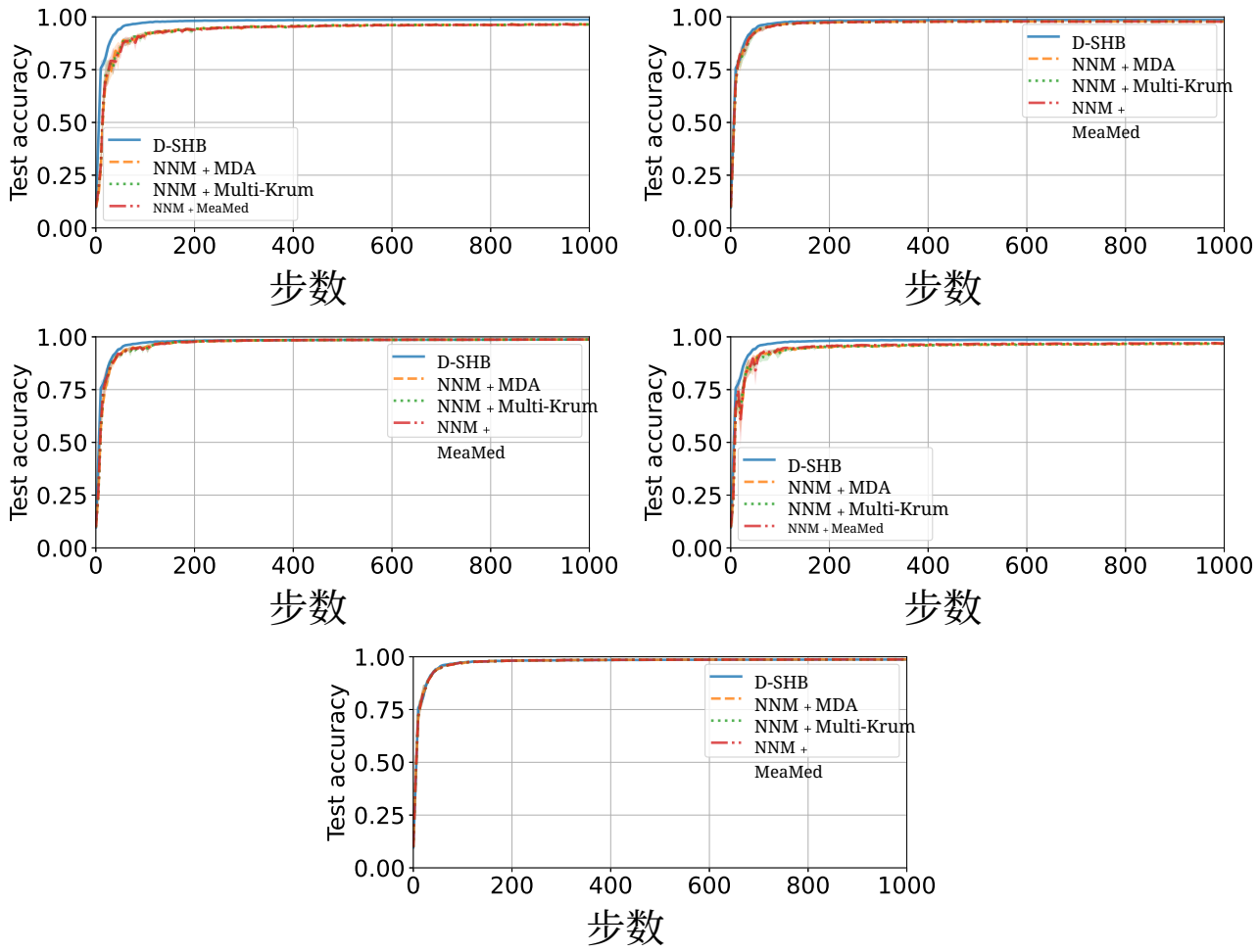

图 17：使用鲁棒 D-SHB 在 MNIST 上进行的实验，其中 $n = 17$ 个工作节点中有 $f = 6$ 个拜占庭工作节点，且 $\beta = 0.9$ 和 $\alpha = 10$。拜占庭工作节点执行 FOE（第 *1* 行，左侧）、ALIE（第 *1* 行，右侧）、Mimic（第 *2* 行，左侧）、SF（第 *2* 行，右侧）和标签翻转（第 *3* 行）攻击。

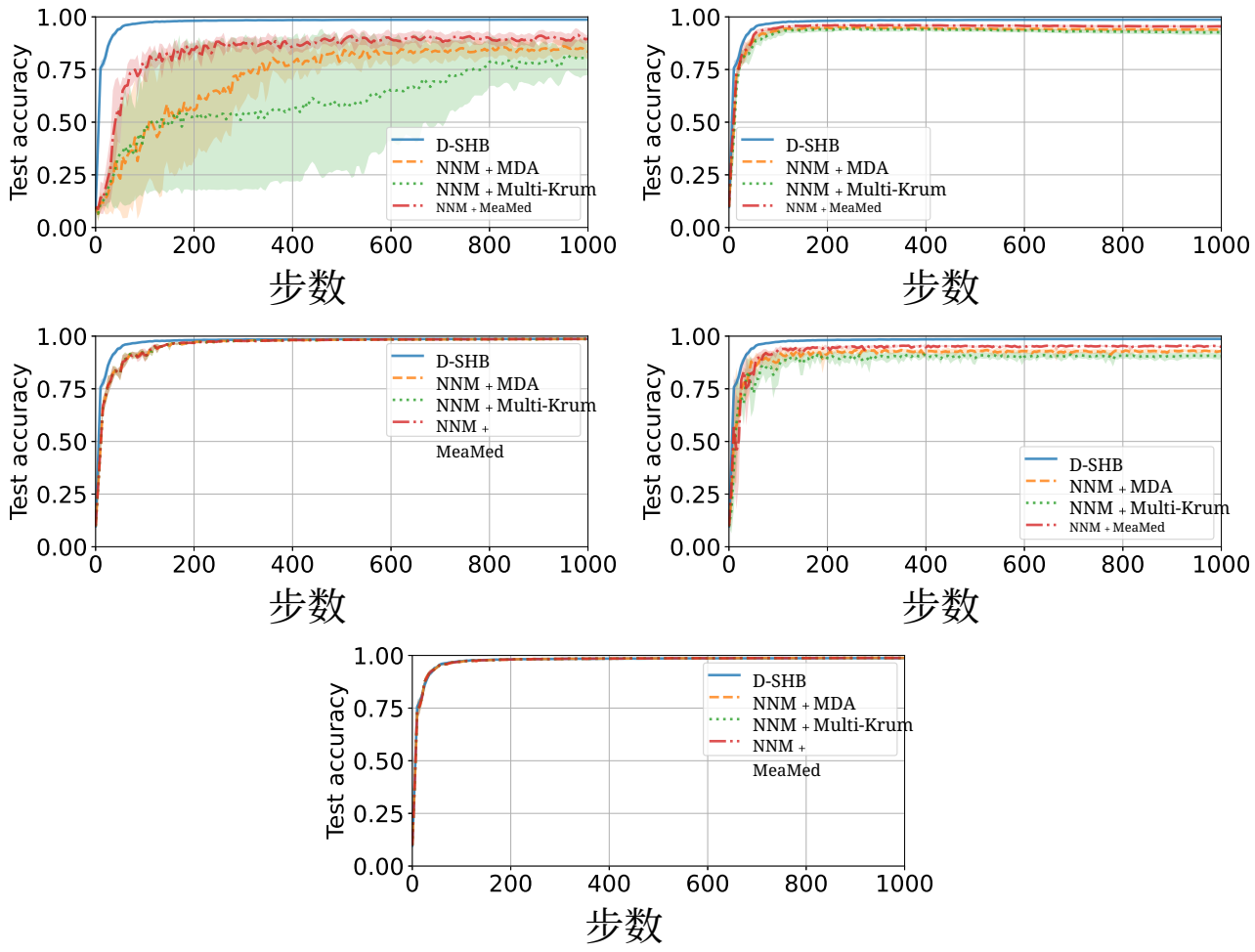

图18：使用鲁棒 D-SHB 在 MNIST 上进行的实验，其中 $n = 17$ 个工作节点中有 $f = 8$ 个拜占庭工作节点，并采用 $\beta = 0.9$ 和 $\alpha = 10$。拜占庭工作节点执行 FOE（第 *1* 行，左）、ALIE（第 *1* 行，右）、Mimic（第 *2* 行，左）、SF（第 *2* 行，右）和 LF（第 *3* 行）攻击。

15.2 Fashion-MNIST 上的综合结果

本节展示我们在 Fashion-MNIST 数据集上的结果。我们考虑两种拜占庭设置： $f = 4$ 和$f = 6$，总共 $n = 17$ 个工作节点。我们还考虑三种异质性情形： $\alpha = 0.1$ （极端）、 $\alpha = 1$ （中等）和 $\alpha = 10$ （低）。图中比较了使用四种聚合规则（即 Krum、几何中位数、CWMed 和 CWTM）时 NNM 和分桶的性能。图表如下所示。值得注意的是，在最强的拜占庭设置下，也就是当 $f > 4$时，分桶只能在桶大小为 $s = 1$ [26]的情况下应用。这意味着当 $f = 6$时，执行分桶实际上等同于运行原始聚合规则。

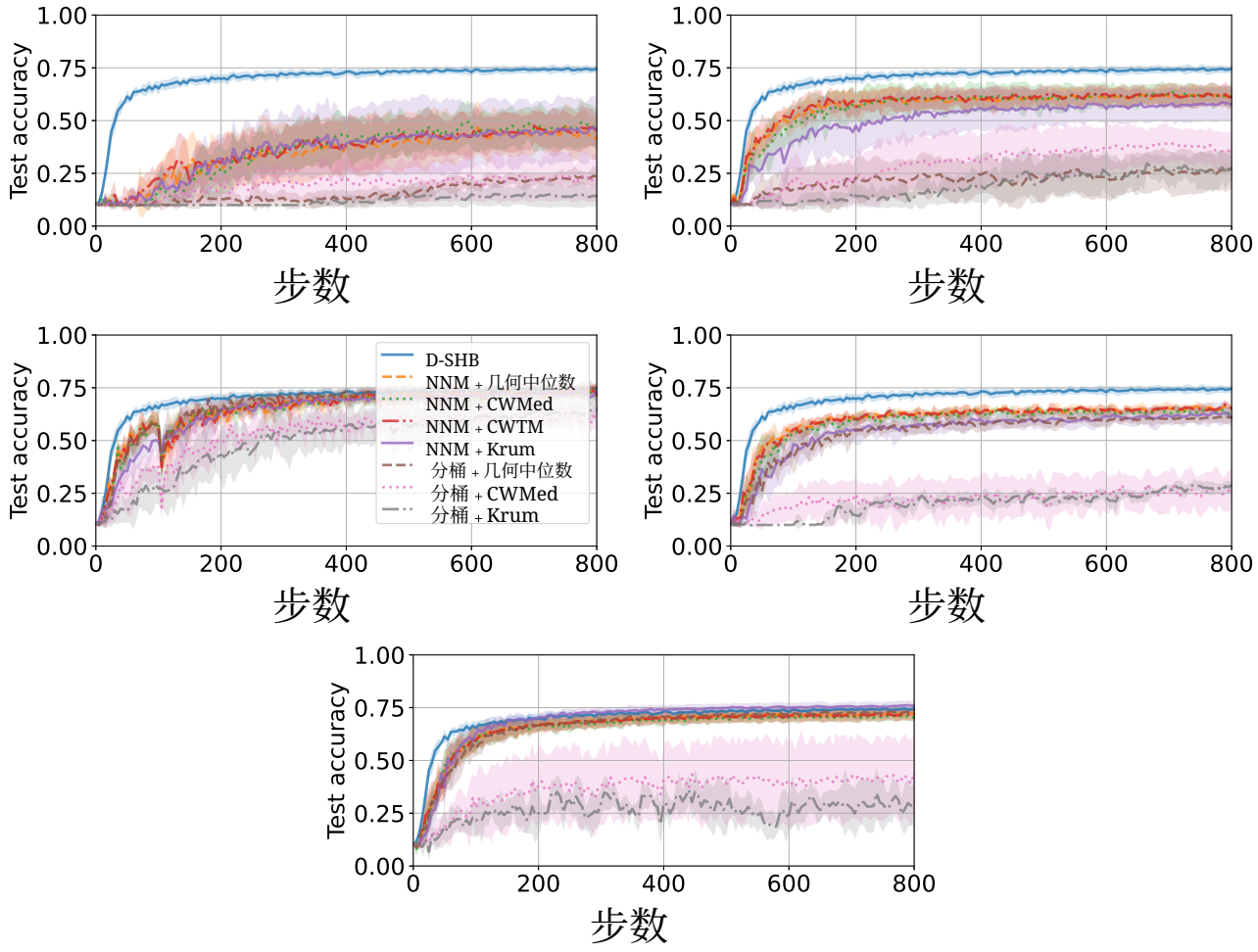

图 19：使用鲁棒 D-SHB 在 Fashion-MNIST 上进行的实验，其中 $f = 4$ 个拜占庭工作节点（共 $n = 17$ 个工作节点），且 $\beta = 0.9$ 和 $\alpha = 0.1$。拜占庭工作节点执行 FOE（第 *1* 行，左侧）、ALIE（第 *1* 行，右侧）、Mimic（第 *2* 行，左侧）、SF（第 *2* 行，右侧）和 LF（第 *3* 行）攻击。

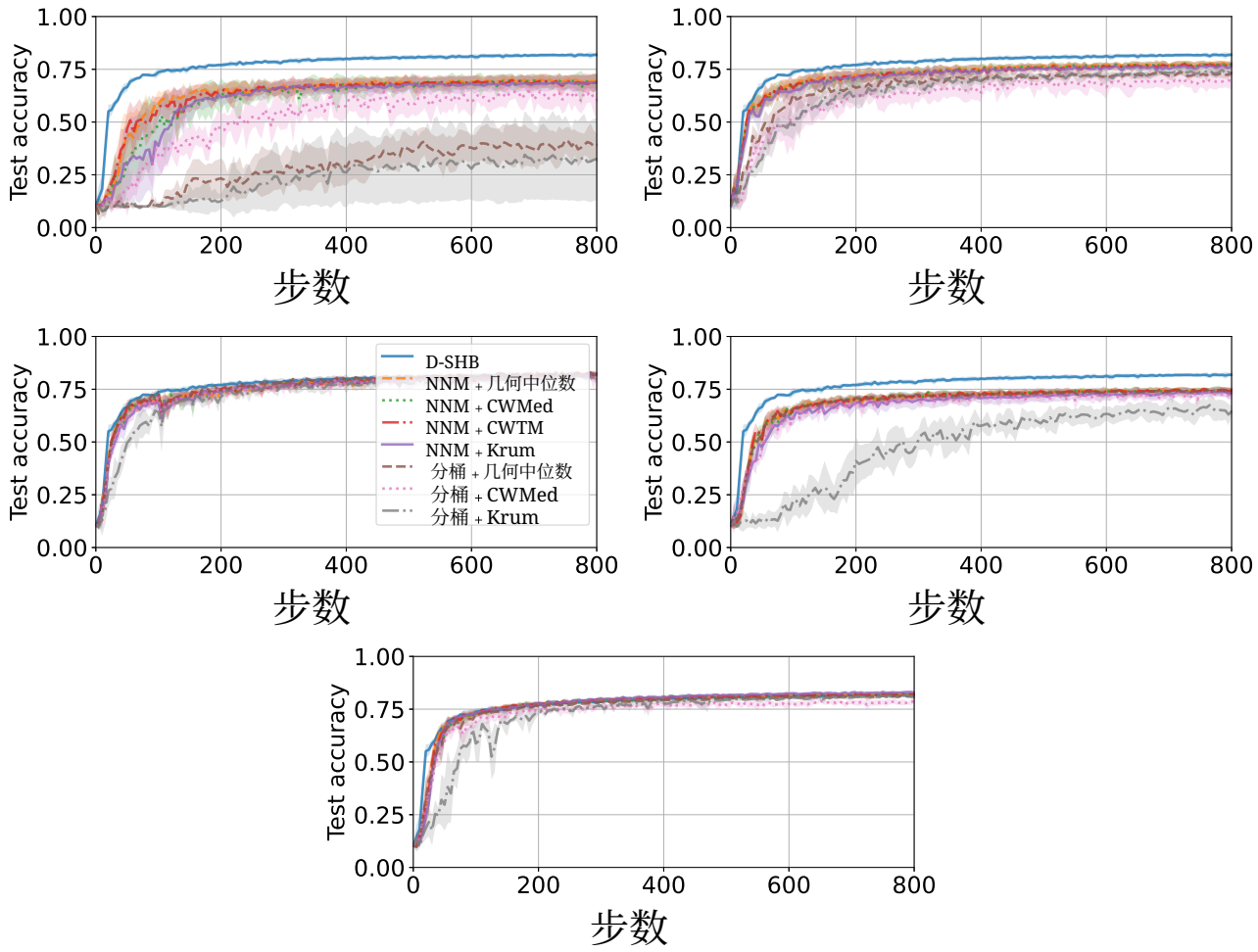

图 20：使用鲁棒 D-SHB 在 Fashion-MNIST 上进行的实验，其中 $f = 4$ 个工作节点中有 $n = 17$ 个拜占庭工作节点，$\beta = 0.9$ 和 $\alpha = 1$。拜占庭工作节点执行 FOE（第 *1* 行，左侧）、ALIE（第 *1* 行，右侧）、Mimic（第 *2* 行，左侧）、SF（第 *2* 行，右侧）和 LF（第 *3* 行）攻击。

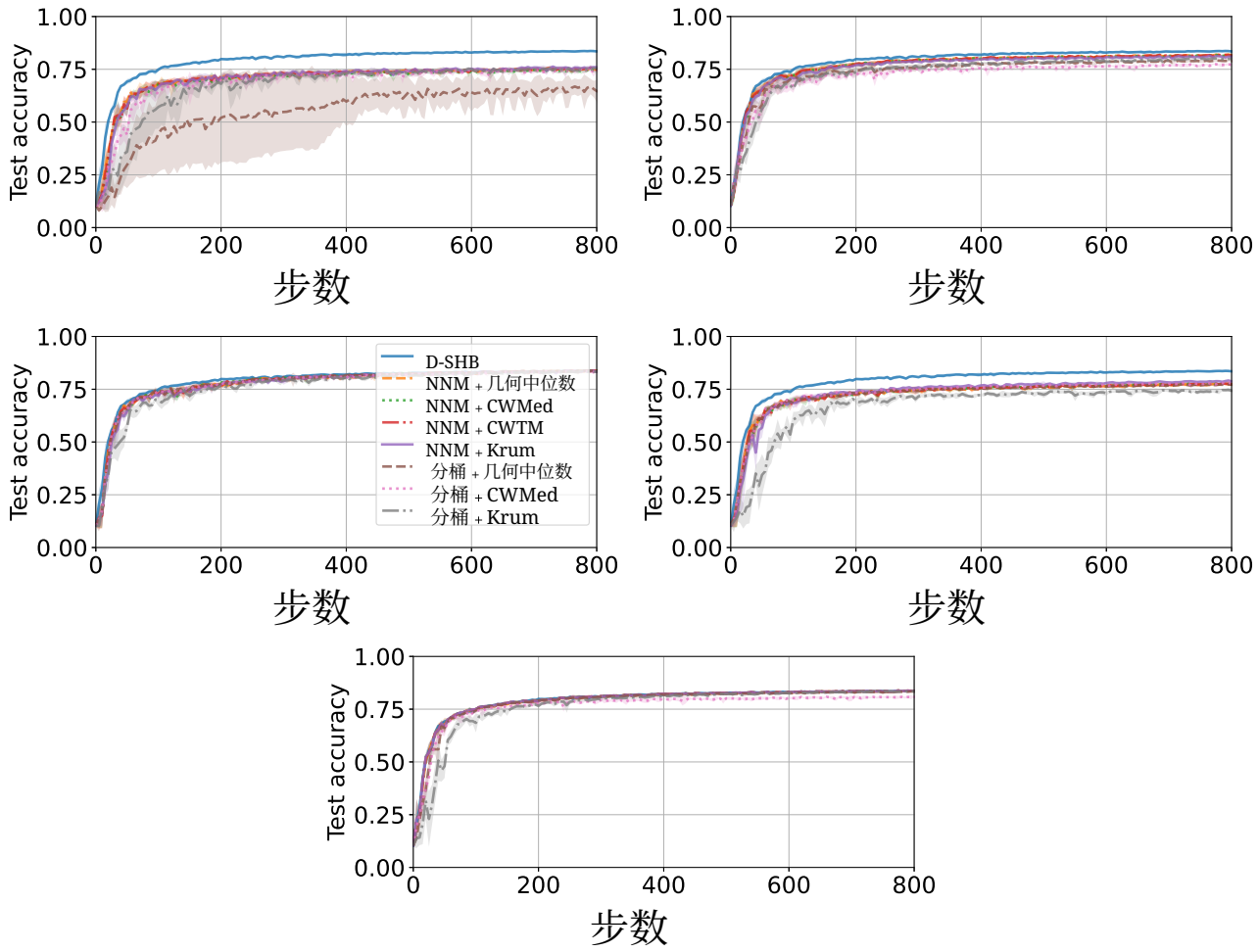

图 21：使用鲁棒 D-SHB 在 Fashion-MNIST 上进行的实验，其中 $f = 4$ 个拜占庭工作节点来自 $n = 17$ 个工作节点，并采用 $\beta = 0.9$ 和 $\alpha = 10$。拜占庭工作节点执行 FOE（第 *1* 行，左侧）、ALIE（第 *1* 行，右侧）、Mimic（第 *2* 行，左侧）、SF（第 *2* 行，右侧）和标签翻转（第 *3* 行）攻击。

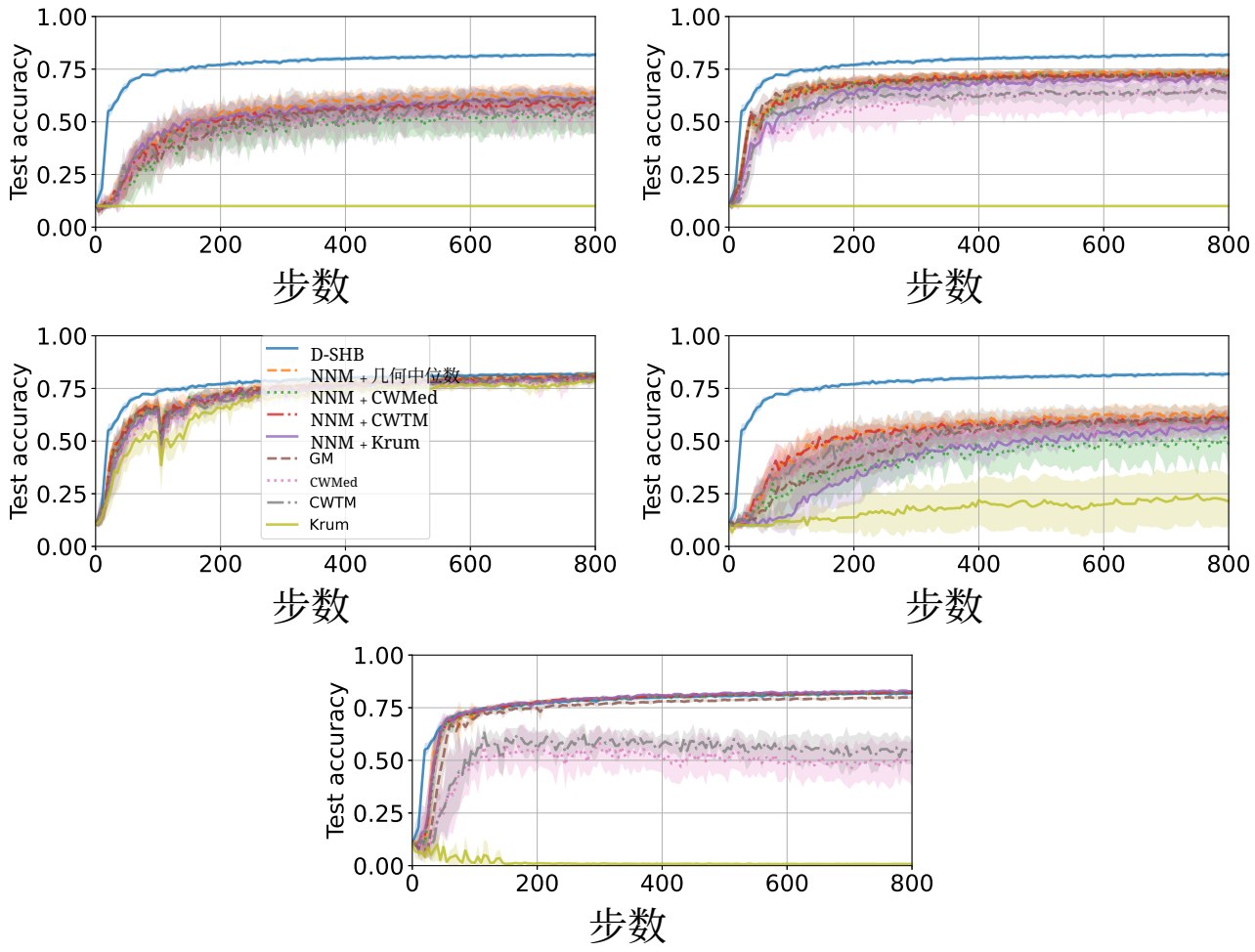

图 22：使用鲁棒 D-SHB 在 Fashion-MNIST 上进行的实验，其中 $n = 17$ 个工作节点中有 $f = 6$ 个拜占庭工作节点，$\beta = 0.9$ 和 $\alpha = 1$。拜占庭工作节点执行 FOE（第 *1* 行，左）、ALIE（第 *1* 行，右）、Mimic（第 *2* 行，左）、SF（第 *2* 行，右）和 LF（第 *3* 行）攻击。

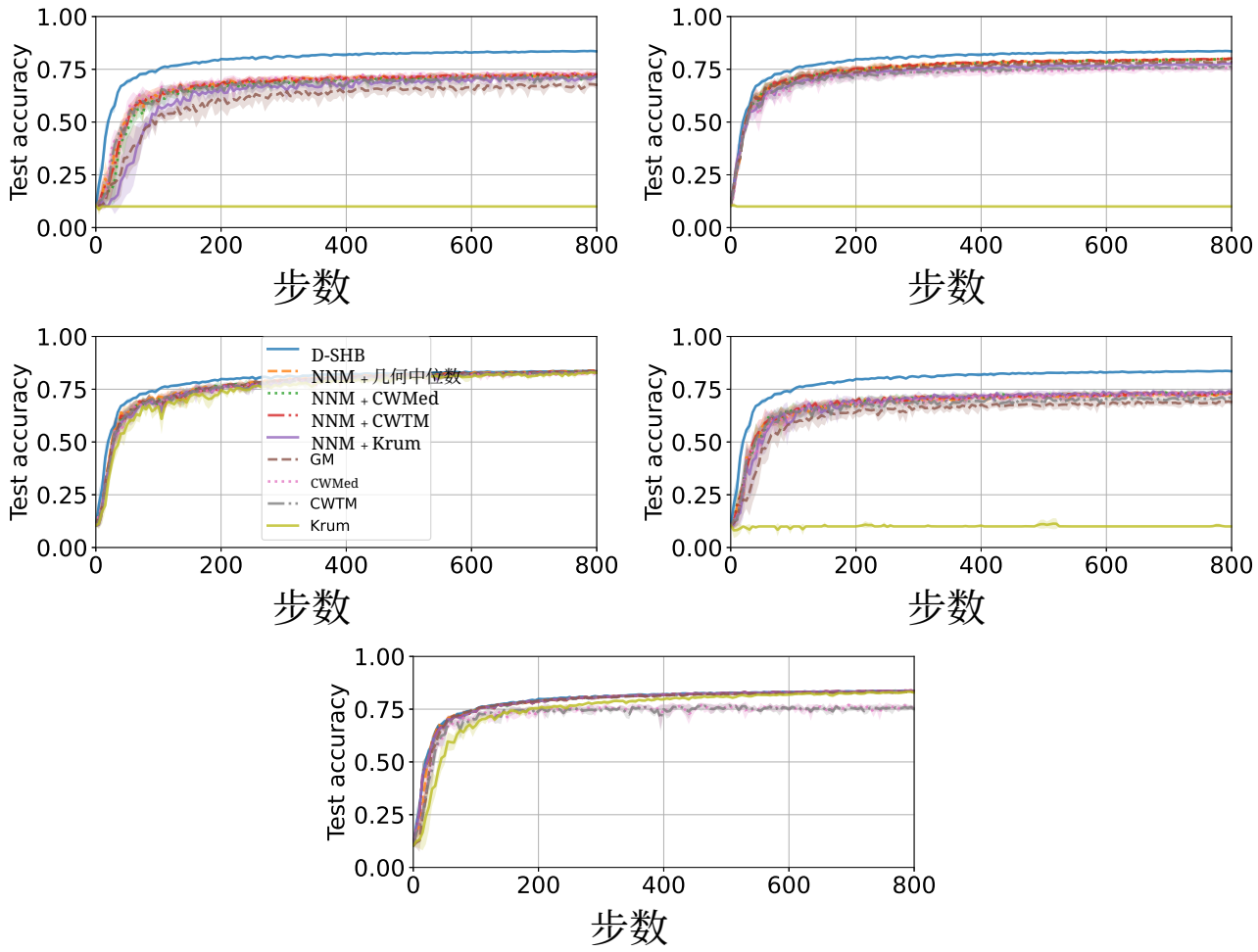

图 23：在 Fashion-MNIST 上使用鲁棒 D-SHB 进行的实验，其中 $f = 6$ 个拜占庭工作节点占 $n = 17$ 个工作节点，且 $\beta = 0.9$ 和 $\alpha = 10$。拜占庭工作节点执行 FOE（第 *1* 行，左）、ALIE（第 *1* 行，右）、Mimic（第 *2* 行，左）、SF（第 *2* 行，右）和 LF（第 *3* 行）攻击。

15.3 CIFAR-10 上的综合结果

本节将全面展示我们在 CIFAR-10 上的实验结果。我们考虑三种拜占庭设置：总共 $n = 17$ 个工作节点中有 $f = 2$、$f = 3$ 和 $f = 4$ 个。我们还考虑两种异质性情形：$\alpha = 1$（中等）和 $\alpha = 10$（低）。我们比较 NNM 和分桶在采用四种聚合规则（即 Krum、几何中位数、CWMed 和 CWTM）时的性能。下方给出了图表，它们补充了主论文第6.3节图 1 中的（部分）结果。

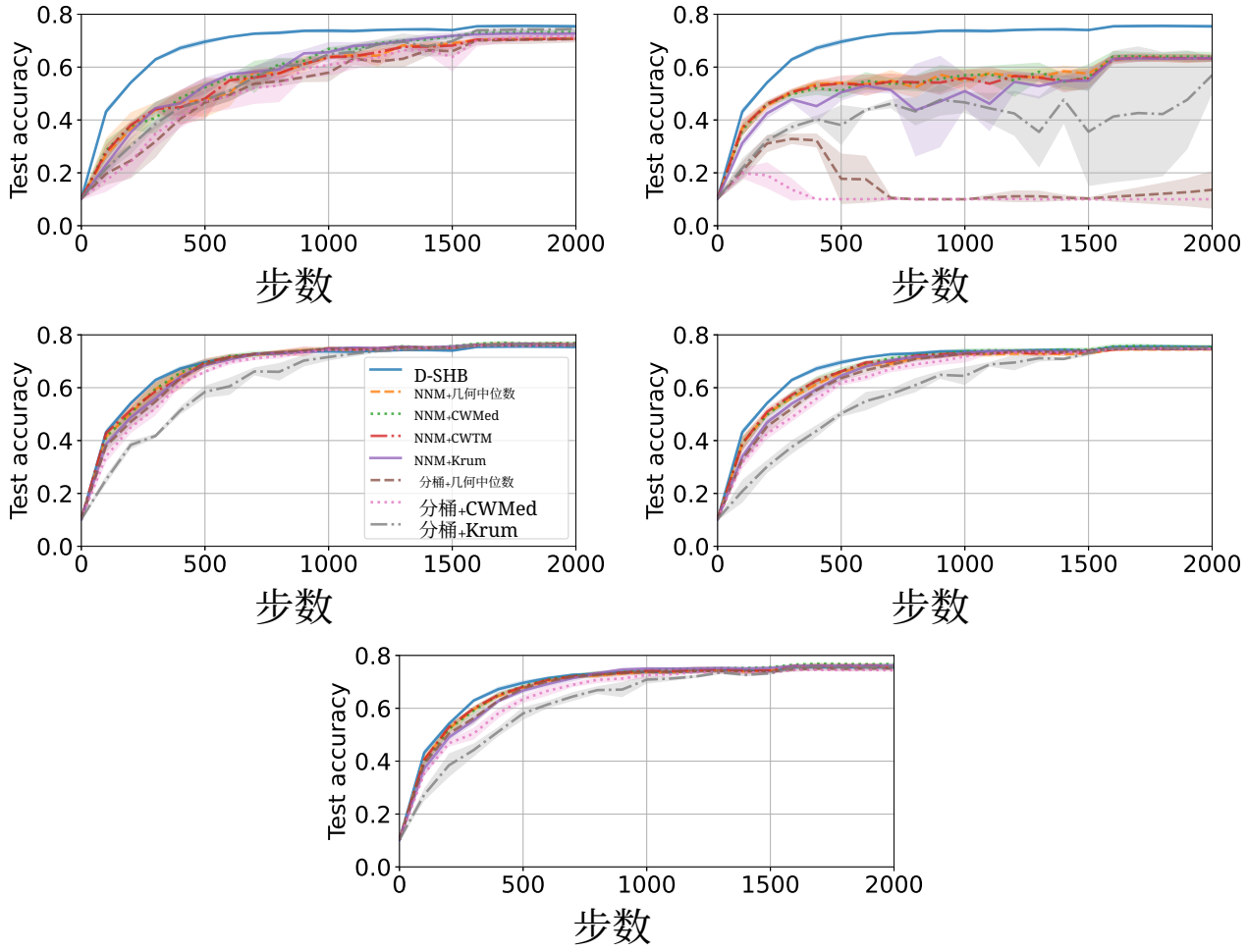

图 24：使用鲁棒 D-SHB 在 CIFAR-10 上进行的实验，其中 $n = 17$ 个工作节点中有 $f = 2$ 个为拜占庭节点，且 $\beta = 0.9$ 和 $\alpha = 1$。拜占庭工作节点执行 FOE（第 *1* 行，左）、ALIE（第 *1* 行，右）、Mimic（第 *2* 行，左）、SF（第 *2* 行，右）和 LF（第 *3* 行）攻击。

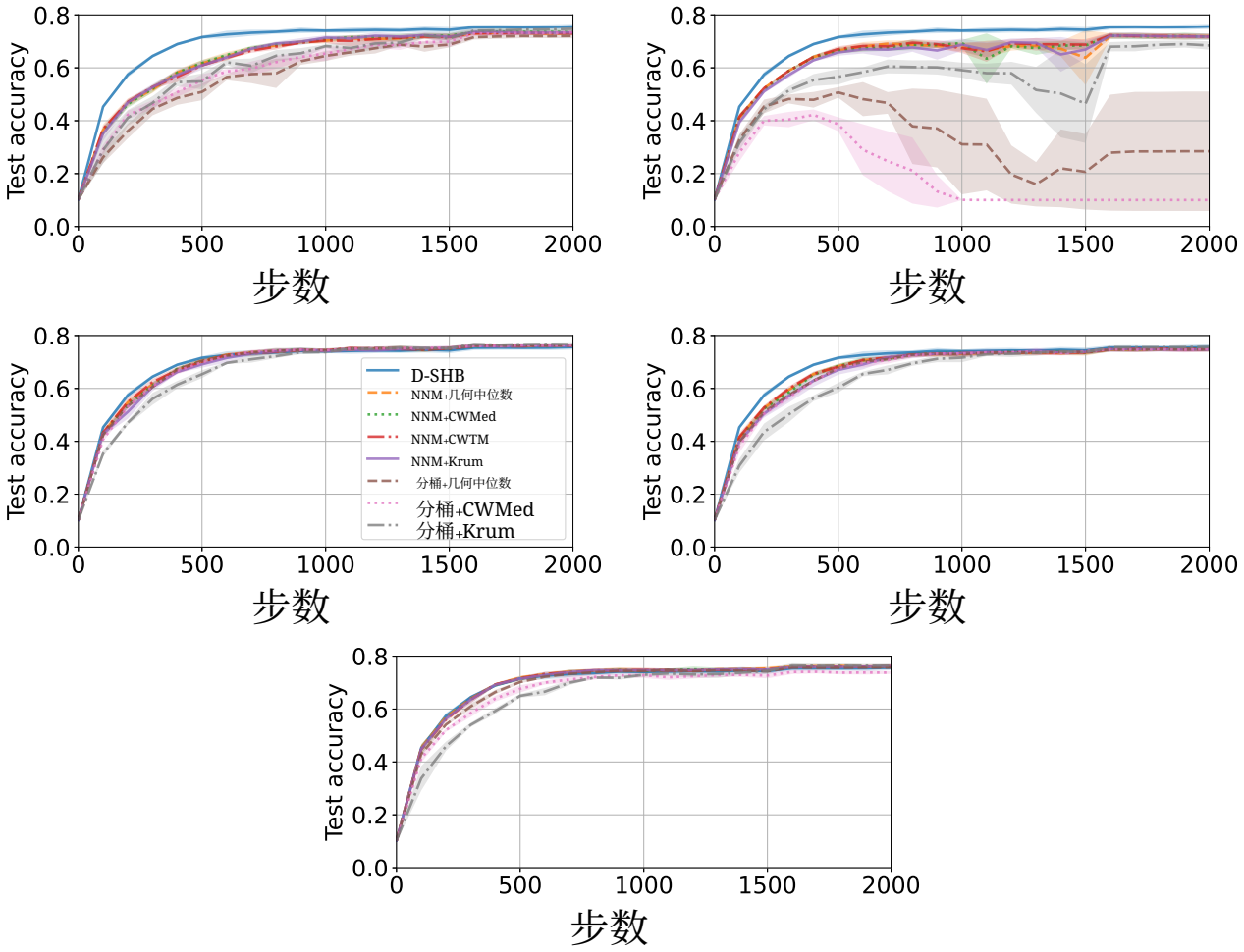

图 25：使用鲁棒 D-SHB 在 CIFAR-10 上进行的实验，其中 $n = 17$ 个工作节点中有 $f = 2$ 个拜占庭工作节点，使用 $\beta = 0.9$ 和 $\alpha = 10$。拜占庭工作节点执行 FOE（第 *1* 行，左侧）、ALIE（第 *1* 行，右侧）、Mimic（第 *2* 行，左侧）、SF（第*2*行，右侧）和标签翻转（第 *3* 行）攻击。

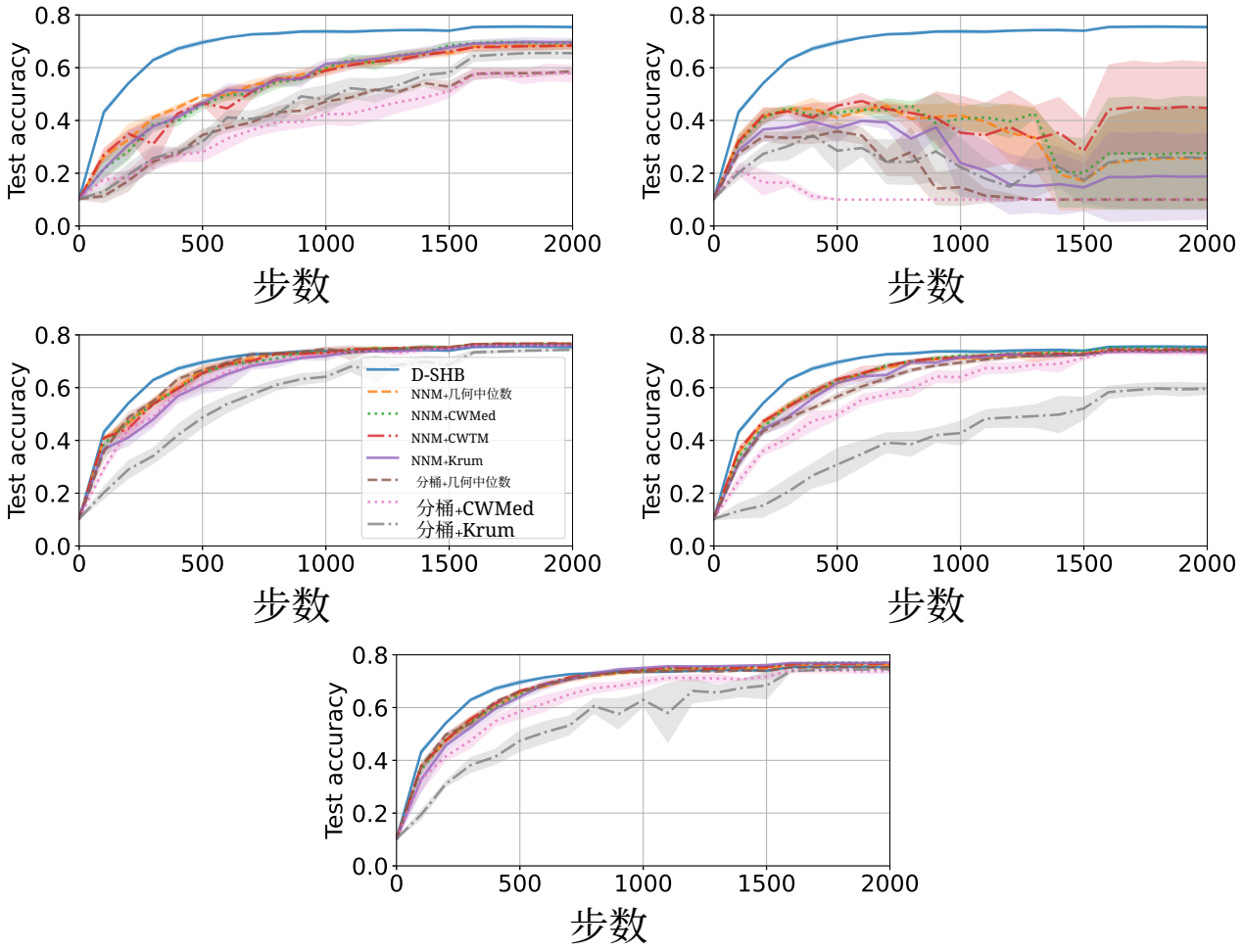

图 26：使用鲁棒 D-SHB 在 CIFAR-10 上进行的实验，其中 $n = 17$ 个工作节点中有 $f = 3$ 个拜占庭节点，且满足 $\beta = 0.9$ 和 $\alpha = 1$。拜占庭工作节点执行 FOE（第 *1* 行，左侧）、ALIE（第 *1* 行，右侧）、Mimic（第 *2* 行，左侧）、SF（第 *2* 行，右侧）和 LF （第 *3* 行）攻击。

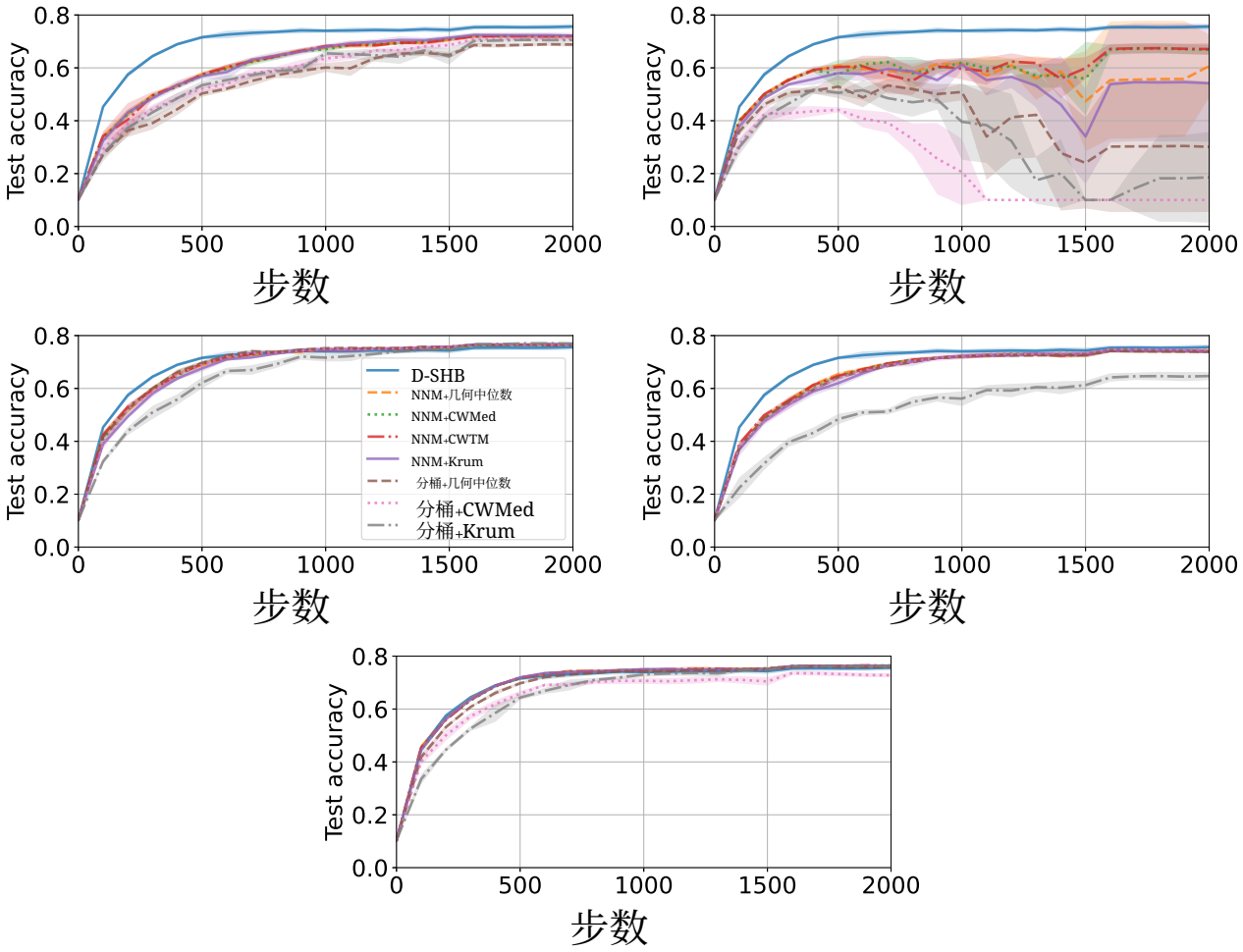

图 27：使用鲁棒 D-SHB 在 CIFAR-10 上进行的实验，其中 $n = 17$ 个工作节点中有 $f = 3$ 个拜占庭工作节点，且包含 $\beta = 0.9$ 和 $\alpha = 10$。拜占庭工作节点执行 FOE（第 *1* 行，左侧）、ALIE（第 *1* 行，右侧）、Mimic（第 *2* 行，左侧）、SF（第 *2* 行，右侧）和标签翻转（第 *3* 行）攻击。

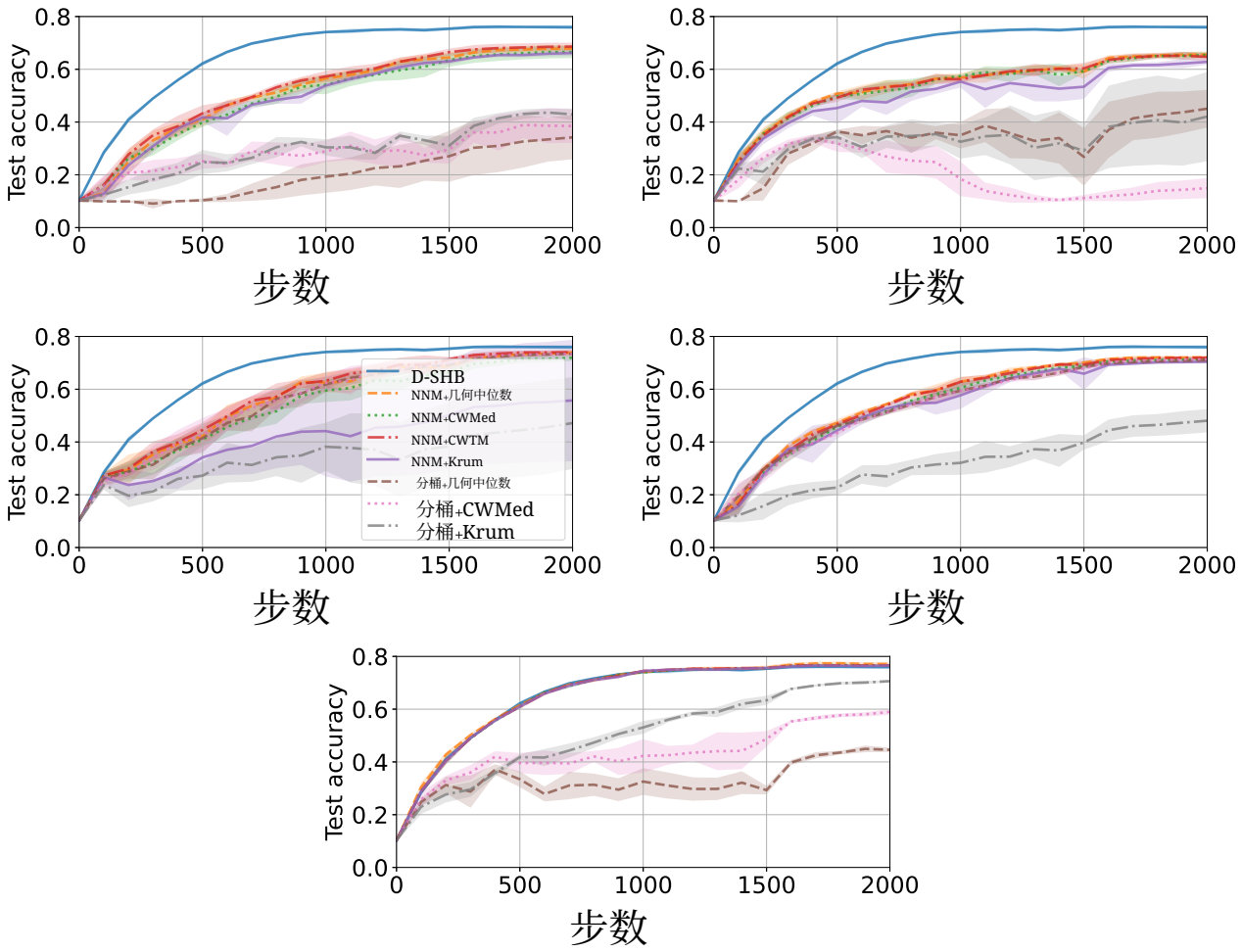

图 28：使用鲁棒 D-SHB 在 CIFAR-10 上进行的实验，其中 $n = 17$ 个工作节点中有 $f = 4$ 个拜占庭工作节点，采用 $\beta = 0.99$ 和 $\alpha = 10$。拜占庭工作节点执行 FOE（第 *1* 行，左）、ALIE（第 *1* 行，右）、Mimic（第 *2* 行，左）、SF（第 *2* 行，右）和 LF（第 *3* 行）攻击。