研究与开发

无人机联邦学习场景下动态选择性同态加密隐私保护研究

仇建斌[1]，章祖葳[2]，郑宇辉[2]

（1. 南京工业大学信息管理中心，江苏 南京 211816；
2. 南京工业大学计算机与信息工程学院（人工智能学院），江苏 南京 211816）

摘　要：随着低空经济的快速发展，无人机（unmanned aerial vehicle，UAV）在环境监测、应急救援和物流配送等领域得到广泛应用，并在数据采集与处理过程中面临日益突出的隐私保护需求。为了应对这一挑战，联邦学习结合同态加密被引入以提升数据安全性，但在计算与通信资源受限的无人机场景下，其高昂的资源开销成为实际应用的主要瓶颈。为此，提出了一种面向无人机场景的选择性同态加密隐私保护方案。在每轮本地训练后，客户端基于梯度敏感度评估参数重要性，并结合通信与能耗预算，通过启发式贪心算法动态选择“隐私收益”最大的参数子集进行加密。该方案在联邦学习框架下实现，并采用CKKS同态加密库进行模拟实验。基于CIFAR-10数据集和SimpleCNN模型，对比了5种方案：无加密、全加密、MaskCrypt固定比例加密、DP-AvgFed方案及提出的动态预算方案。实验结果表明，所提方法在实现与MaskCrypt相当安全性的同时，资源开销降低约10%，在保障隐私的同时有效控制了资源消耗，验证了其在资源受限的无人机场景中的可行性和优越性。

关键词：无人机；联邦学习；同态加密；MaskCrypt方法

中图分类号：TP18；TN918

文献标志码：A

doi: 10.11959/j.issn.1000−0801.2025224

Research on privacy protection of dynamic selective homomorphic encryption in the context of UAV federated learning

QIU Jianbin[1], ZHANG Zuwei[2], ZHENG Yuhui[2]

1. Information Management Center, Nanjing Tech University, Nanjing 211816, China
2. College of Computer and Information Engineering (College of Artificial Intelligence), Nanjing Tech University, Nanjing 211816, China

Abstract: With the rapid development of the low-altitude economy, unmanned aerial vehicle (UAV) has been widely used in areas such as environmental monitoring, emergency rescue, and logistics delivery. As UAV increasingly engage in data collection and processing, the demand for privacy protection in such scenarios has become increasingly prominent. To address this issue, federated learning combined with homomorphic encryption has been adopted to en-

收稿日期：2025−06−16；修回日期：2025−07−05

通信作者：仇建斌，qiujia@njtech.edu.cn

hance data security. However, under the constraints of limited computational and communication resources on UAV, the high resource overhead of such approaches becomes a major bottleneck for practical deployment. To this end, a selective homomorphic encryption scheme for privacy protection tailored to UAV scenarios was proposed. After each round of local training, the client evaluates the importance of model parameters based on gradient sensitivity was evaluated by client, and within the given communication and energy budget, dynamically a subset of parameters was selected with the highest “privacy gain” for encryption via a heuristic greedy algorithm. The scheme was implemented within a federated learning framework and simulated using the CKKS homomorphic encryption library. Experiments were conducted on the CIFAR-10 dataset using the SimpleCNN model, comparing five schemes: no encryption, full encryption, fixed-ratio MaskCrypt, DP-AvgFed scheme and the proposed dynamic budget scheme. Results show that the proposed method achieves a balanced trade-off between resource consumption and security. Compared to MaskCrypt, it achieves comparable privacy protection with approximately 10% lower resource overhead, demonstrating its feasibility and effectiveness in resource-constrained UAV scenarios.

Key words: UAV, federated learning, homomorphic encryption, MaskCrypt method

0　引言

随着低空经济的快速发展，无人机（unmanned aerial vehicle，UAV）凭借其高灵活性、高机动性和低部署成本等优点，已广泛应用于环境监测、应急救灾、精准农业和物流配送等多个任务场景。每架无人机单次飞行会产生导航、避障、载荷状态以及与业务相关的数据，人工智能技术能够深度学习这些海量数据并提炼有价值的信息，现已成为处理海量数据需求的前沿解决方案[1-3]。

无人机采集数据通常具有实时性强、采集点分布广、隐私敏感、差异性大、数据量多等特性，且无人机低空场景对隐私保护、实时性、通信效率有严苛的要求，如果采用传统的机器学习（machine learning，ML）方法将数据传输到一个数据中心进行集中处理，通常面临着高时延和高风险等挑战[4]。联邦学习（federated learning，FL）作为一种新型的分布式机器学习方法，支持不直接共享本地数据，而是通过共享模型参数或梯度等更新值来训练模型，既避免了暴露本地数据，又能达到较好的训练效果[5]。无人机联邦学习通常采用感知采集完成后基于本地数据集进行联邦学习的模式，这样既可避免无人机有限的算力冲突也可保障数据集的质量。无人机设备经过标准化采集、智能标注与多维度增强等步骤，最终形成可支撑深度学习模型的高质量稳定数据集，基于该数据集参与联邦学习训练，达到在保护本地数据隐私的前提下提升全局模型泛化能力的目标。通过“数据不动模型动”的分布式训练模式，联邦学习为低空无人机的规模化应用提供了关键技术支撑。

但最近的一些研究工作[6-7]表明，即使仅共享模型参数或者梯度参数，攻击者仍然可以利用模型参数或者梯度参数来恢复目标数据，这会泄露用户隐私信息，因此隐私问题成为联邦学习的核心问题。

为了抵抗各类隐私攻击，密码学等技术被引入联邦学习中，同态加密（homomorphic encryption，HE）允许在密文状态下直接执行计算，服务器可聚合加密后的模型参数或梯度参数，无须解密客户端数据，凭借在保障隐私数据安全的同时提供密文计算的优势，同态加密被广泛应用于隐私保护联邦学习方案中[8]。李晓东等[9]针对联邦学习中模型参数泄露隐私的问题，提出基于模分量同态加密的FLFC方案，采用自研高效浮点运算支持的加密算法，保护用户梯度与聚合结果，实验显示准确率较FedAvg平均提升2.54%，且加密效率优于主流库；Liu等[10]提出了隐私增

强联邦学习方案PEFL，PEFL使用皮尔逊相关系数作为判断梯度是否恶意的指标，并且采用同态加密作为底层技术；Zhang等[11]提出了融合中国剩余定理（CRT）与Paillier同态加密的梯度保护方案，通过双线性聚合签名实现服务器聚合结果验证，但其依赖可信第三方机构（TPA）生成密钥，且未解决用户与服务器的合谋攻击问题；余晟兴等[12]开发了基于同态加密的梯度筛选方法，通过动态阈值过滤冗余参数，降低30%~50%通信负载，但密钥管理体系仍延续传统TPA集中化模式，难以适应去中心化场景需求；Ma等[13]设计了多密钥同态加密协议，允许多方独立加密模型更新并协作解密，但加密噪声导致CIFAR-10数据集分类使精度下降，揭示隐私与精度的固有矛盾；Xu等[14]将VerifyNet协议结合同态哈希与伪随机技术优化验证效率，但通信开销和计算成本随用户规模线性增长；郭显等[15]提出了一种基于同态加密的可验证隐私保护联邦学习方案，通过分布式密钥生成协议和双线性聚合签名技术，实现去中心化密钥管理、抗合谋攻击及用户独立验证聚合结果，并结合激励机制吸引高质量数据参与。

然而，无人机本身还存在计算能力弱、内存和电池容量小等局限，这些限制一方面影响数据的安全传输与模型的高效训练，另一方面也给同态加密等隐私保护手段带来巨大的计算和通信成本。随着数据安全要求的不断提升，这类成本开销也随之上涨，成为无人机隐私保护方案部署的主要障碍。Neveen等[16]针对物联网智能城市中联邦学习的数据隐私与通信安全问题，提出了4种结合全同态加密（FHE）的联邦学习方案（OUCM/OECM/MUCM/MECM），通过加密模型参数聚合与分簇通信，降低通信开销及时延，同时保持高分类准确率。但FHE计算开销仍较大，且未验证大规模设备场景下的扩展性。卢为党等[17]提出了一种基于无人机辅助联邦边缘学习的资源优化方案，通过联合优化终端设备传输带宽、中央处理器（central processing unit，CPU）频率、发射功率及无人机CPU频率，最大化安全隐私能效（安全传输速率与成本开销的比值），并采用改进的深度确定性策略梯度（DDPG）算法动态调配资源，该方案未充分解决DDPG算法在复杂动态环境中的训练效率问题，且依赖终端设备完全遵守协议的假设，实际场景中可能存在恶意节点未被有效防御的风险，加密传输的计算开销也可能增加系统时延。卢彦丰等[18]针对无人机辅助联邦学习中高能耗、通信时延、资源分配不均的问题，提出了3类优化方案，解决了传统基站覆盖不足、隐私泄露问题，但能源管理依赖外部充电、算法复杂度过高，且未验证万级设备扩展性。鉴于此，在资源有限的无人机场景下，利用联邦学习与同态加密进行机器学习时，如何权衡数据安全和成本开销的矛盾关系，合理分配有限的系统资源，在提高安全性能的同时降低成本开销，成为本文研究的重点。

为了应对无人机场景下同态加密联邦学习在数据加解密效率与通信开销方面的挑战，本文在MaskCrypt[19]方法基础上，提出了一种兼顾隐私保护与资源开销的联邦学习优化方案，主要贡献如下。（1）系统架构构建：设计并实现了一个面向多无人机协同的联邦学习系统架构，其中客户端资源受限的无人机设备参与本地训练，中心服务器负责模型聚合。系统引入动态掩码加密机制以实现安全高效的参数聚合，有效平衡模型性能与隐私保护需求，同时充分考虑了无人机设备在计算与通信资源上的约束。（2）算法设计与优化：针对掩码选择问题的NP-hard特性，提出一种基于梯度敏感度排序的启发式贪心近似算法。该算法以参数的“隐私收益–资源消耗比”为标准，在资源预算内优先选择加密性价比高的参数，从而在确保资源可控的前提下近似最大化整体加密安全性。

1　系统模型

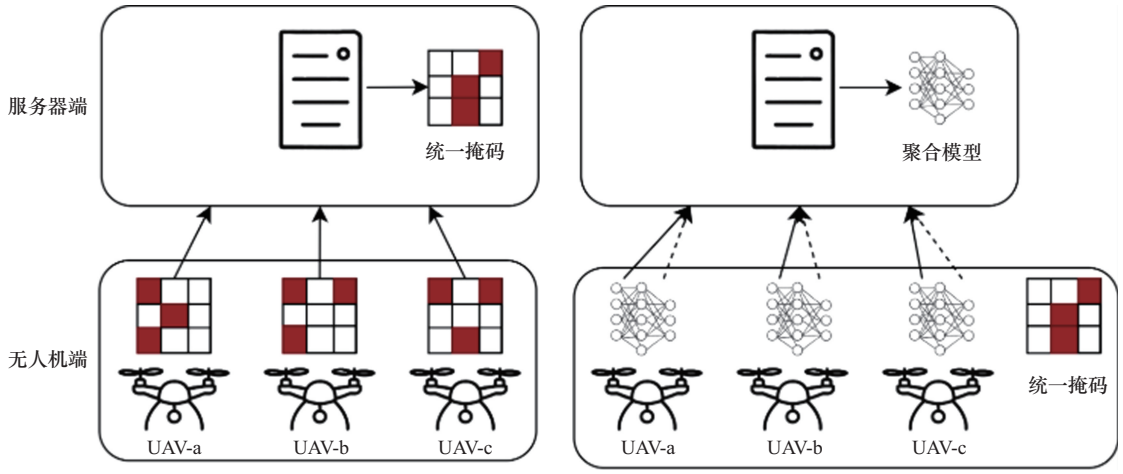
本文考虑由多个无人机客户端和一个集中式服务器构成的联邦学习系统。其中，每个无人机 k（$k=1,2,\cdots,K$）搭载传感器或摄像头等设备，可采集本地数据并利用其计算单元训练本地模型。系统运行时，首先，服务器初始化全局模型参数 w^0 并广播给所有无人机。然后，各无人机在第 t 轮迭代时基于本地数据集 $\boldsymbol{D_k}$ 和收到的全局模型 w^{t-1} 进行本地训练，得到更新的本地模型参数向量 $\boldsymbol{w_t^k}$。接着，无人机 k 将本地更新以一定形式上传至服务器，服务器据此计算聚合得到新的全局模型 $\boldsymbol{w^t}$（如通过加权平均 $\boldsymbol{w^t}=\sum_{k=1}^{K} p_k \boldsymbol{w_t^k}$）。如此循环进行多轮，直到全局模型收敛。为了在上述训练过程中保护无人机的模型更新不被泄露，系统引入了选择性同态加密的动态掩码机制。每轮本地训练结束后，无人机将当前更新与上一轮模型进行差分和梯度敏感度分析，确定本轮需要加密的“掩码”参数集 $\boldsymbol{m_k}$。为了减少各客户端独立选择掩码可能带来的不一致，服务器实施掩码共识机制：对所有无人机上报的本地掩码集合按重要性进行交替合并，去重后取前 ρN 个参数索引形成全局掩码 $\tilde{\boldsymbol{m}}$。这里 $\rho \in [0,1]$ 称为加密比例，N 为模型参数总数，ρN 表示每轮加密的参数数量上限。系统架构如图 1 所示。

在掩码共识阶段（图 1（a）），首先，各无人机客户端（UAV-A、UAV-B、UAV-C）根据本地梯度敏感性计算各自的掩码索引并生成初步掩码向量，随后将该向量上传至集中式服务器。服务器端将所有客户端掩码按轮询或交错方式合并，并通过“掩码共识”形成“统一掩码”，再下发回各 UAV。此时，所有客户端在相同索引位置对其模型参数进行同态加密，保证加密一致性并为后续聚合打下基础。

在本地模型上传阶段（图 1（b）），各 UAV 基于本地数据完成模型训练，得到明文模型参数后依照前述统一掩码对关键权重进行同态加密，再将明文与密文两部分参数一并上传。服务器端接收后即可对明文部分和密文部分分别聚合，最终得到新的全局模型并下发至各 UAV，实现全局模型的更新与同步。

1.1　加密掩码选择机制

梯度引导的掩码选择机制通过选择最关键权重进行加密，次关键权重直接以明文传输，达到降低通信和计算开销的同时保证加密的安全性。在每一轮本地训练结束后，无人机首先计算模型



（a）掩码共识　　（b）本地模型上传

图 1　系统架构

参数梯度：

$$\boldsymbol{g}=\mathrm{grad}\left(\boldsymbol{w}_t^k,\boldsymbol{D}^k\right) \tag{1}$$

其中，$\boldsymbol{w}_t^k$为无人机k在第t轮更新后的权重向量，$\boldsymbol{D}^k$为其本地数据集。计算$\boldsymbol{w}_{t-1}^k$与当前$\boldsymbol{w}_t^k$的差值绝对值：

$$\tilde{\boldsymbol{w}}_t^k=\left|\boldsymbol{w}_t^k-\boldsymbol{w}_{t-1}^k\right| \tag{2}$$

逐个元素计算重要性：

$$\boldsymbol{v}[i]=\boldsymbol{g}[i]\cdot\tilde{\boldsymbol{w}}_t^k[i] \tag{3}$$

该量能够体现每个维度对暴露后被恢复数据的贡献。将向量$\boldsymbol{v}$按照降序排序，取前ρN个元素的索引组成本地掩码集合$\boldsymbol{m}^k$。根据文献[19]此策略等价于在梯度方向上最大化预测模型损失，从而有效混淆攻击者对训练痕迹的推断。

为了保证所有客户端对加密维度的一致性，服务器对各客户端上报的本地掩码$\boldsymbol{m}^k$按优先级交替合并：依次取每个客户端的第$1,2,\cdots$优先级索引并追加至列表，去重后截取前ρN项，得到全局掩码$\tilde{\boldsymbol{m}}$。该机制不仅避免了对齐失败，还兼顾各客户端的隐私需求公平性。

1.2 加密和聚合流程

获得全局掩码$\tilde{\boldsymbol{m}}$后，无人机将其本地模型更新划分为明文部分和密文部分。

明文部分$\boldsymbol{w}_{\mathbf{plain},t}^k=\{\boldsymbol{w}_t^k[i]\,|\,i\notin\tilde{\boldsymbol{m}}\}$：即未被选中加密的参数，这部分按原始数值直接发送。

密文部分$\boldsymbol{w}_{\mathbf{enc},t}^k=\mathrm{Enc}\left(K_{\mathrm{pub}},\{\boldsymbol{w}_t^k[i]|i\in\tilde{\boldsymbol{m}}\}\right)$：即选中加密的参数集合，使用预先部署的同态加密公共密钥K_{pub}逐元素加密得到密文向量。这里加密算法可采用支持加法同态的方案（如Paillier加密），保证密文可在不解密的情况下进行聚合运算。

随后，每个无人机将明文和密文两部分$\left(\boldsymbol{w}_{\mathbf{plain},t}^k,\boldsymbol{w}_{\mathbf{enc},t}^k\right)$一并上传给服务器。首先，服务器对所有收到的明文部分逐元素求和得到全局明文聚合$\boldsymbol{w}_{\mathbf{plain},t}=\sum_{k=1}^{K}p_k\boldsymbol{w}_{\mathbf{plain},t}^k$。对于密文部分，由于同态加密的加法封闭性，服务器可以直接对对应密文进行逐元素求和得到全局密文聚合$\boldsymbol{w}_{\mathbf{enc},t}=\sum_{k=1}^{K}p_k\boldsymbol{w}_{\mathbf{enc},t}^k$，服务器无法解读或解密$\boldsymbol{w}_{\mathbf{enc},t}$的内容，其仅持有密文结果。最后，服务器将明文聚合结果和密文聚合结果分别下发给各无人机；无人机利用自身持有的同态加密私钥对收到的全局密文部分$\boldsymbol{w}_{\mathbf{enc},t}$执行解密，结合明文部分$\boldsymbol{w}_{\mathbf{plain},t}$还原得到完整的全局模型参数$\boldsymbol{w}^t$。此后进入下一轮训练。整个过程中，服务器始终无法获知被掩码加密参数的真实值，但又能完成全局模型的正确聚合更新，保证了模型性能和隐私安全的兼顾。

该系统特别考虑了资源约束的因素，即每个无人机都存在电池能量及与服务器通信带宽的上限，模型训练、本地加解密和无线传输都会消耗宝贵的能量，同时，无人机与服务器的链路容量也会限制每轮上传的参数数据量。如果隐私保护方案过于消耗能量或带宽，可能导致无人机中途掉线或系统时延过高，因此，设计掩码选择策略时必须权衡隐私增益与资源开销，在满足能耗和通信约束的前提下尽可能提升安全性能。

2 隐私威胁模型

本文假定服务器为“诚实但好奇”的潜在对手，即按协议正常执行全局聚合，但会尝试从收集到的模型更新中推断各无人机的隐私信息，此外本文还考虑存在服务器可能与部分恶意客户端合谋攻击、共同分析其他诚实客户端的更新以挖掘敏感数据的情况。攻击者的能力包括：拦截并分析每轮从无人机上传到服务器的明文模型更新部分，以及利用历史全局模型参数的变化趋势。攻击者无法破解同态加密的密文部分（假设加密算法足够安全），但可以利用未加密暴露的参数和模型信息实施以下两类已知威胁。

（1）梯度反演攻击（数据重建攻击）：攻击者试图根据客户端上传的模型梯度或参数更新重建该客户端的原始训练数据。由于无人机可能在某轮仅用极少量本地数据（甚至单个样本）完成训练，其上传的模型更新中包含有关该数据的丰富信息，当模型参数完全暴露时，已有研究表明攻击者可以近乎完美地重构出原始输入，如重建出高清晰度的图片，这对隐私保护造成重大威胁。

（2）成员推断攻击：攻击者利用获得的全局模型或各轮更新，判断某特定数据是否被某客户端用来训练过，如果模型对某些样本输出过高置信度，则表明这些样本可能出现在训练集中。由于在FL中服务器能够白盒访问每轮客户端模型，且本地训练容易发生过拟合，成员推断攻击在联邦场景成功率更高。换言之，如果没有防护措施，参与训练的客户端很容易成为成员推断攻击的受害者。

为了应对上述威胁，本文从攻击者视角出发构建防御策略，即通过选择性加密隐藏梯度更新中最敏感的信息，削弱攻击者的推断能力。攻击者能够获取的仅是每轮未加密部分的参数更新，而这些更新缺少关键敏感维度，难以被利用进而重构原始数据或进行成员识别。本文在安全性指标建模部分将详细定义攻击成功率与掩码选择的关系，并以此为依据优化掩码策略，达到攻击成功的概率最低、重建误差最大化的目标，从而实现对攻击的有效防御。

3　掩码选择优化建模

问题定义：在资源受限的无人机联邦学习中，在满足每轮能耗和通信约束的前提下，动态选择加密掩码以达到最大化隐私安全性的目的。形式化地针对每一轮t定义决策变量如下。

（1）加密比例$\rho_t \in [0,1]$：表示第t轮选择加密的模型参数所占比例，即全局掩码大小占总参数N的比率。由$\rho_t N = |\tilde{\boldsymbol{m}}_t|$得到加密参数数量。

（2）掩码向量$\boldsymbol{x_t} = (x_{t,1}, x_{t,2}, \cdots, x_{t,N}) \in \{0,1\}^N$：长度为$N$的0-1向量，其中$x_{t,i}=1$表示第$t$轮中第$i$个模型权重被选中加密，否则$x_{t,i}=0$。显然，$\sum_{i=1}^{N} x_{t,i} = \rho_t N$。

本文引入安全性指标$S(x_t)$用于量化在选择掩码x_t时系统抵御攻击的能力大小，直观上，S应随加密的“重要”参数越多而越高。通过梯度导向的掩码选择可以最大程度混淆攻击者对训练痕迹的推断，因此可以将每个参数的重要性度量s_i（本文使用的是梯度与权重变化的乘积，即第1.1节中论述的参数重要性$\boldsymbol{v}[i]$）作为权重，定义$S(x_t) = \sum_{i=1}^{N} s_i x_{t,i}$即被加密参数的重要性之和作为安全性指标。$S$值越大，意味着本轮加密掩盖了越多敏感信息，攻击者能够利用的剩余明文信息越有限，系统隐私安全性越高。为了确保基本的安全要求，S通常应不低于某个下限$S_{\min}$，系统不至于出现隐私泄露漏洞。

本文问题的约束条件包括如下3点。

（1）能量约束：无人机的剩余能量E_{remain}有限。每轮本地训练以及通信会消耗能量E_{consume}，不得使其超过E_{remain}。能耗包括两部分：一是计算能耗（本地训练过程及对$\rho_t N$个参数的加密和对全局模型密文部分的解密所耗能量）；二是通信能耗（上传明文和密文参数时无线发送所耗能量）。如果单个参数明文传输消耗能量为e_0，单个参数加密及密文传输消耗能量为e_1（包含加密计算和更大的数据发送成本），则本轮总能耗可近似表示为：

$$E_{\text{consume}}(\boldsymbol{x}_t) = E_{\text{train}} + \sum_{i=1}^{N} \left(x_{t,i} e_1 + (1 - x_{t,i}) e_0 \right) \quad (4)$$

其中，E_{train}为本地训练计算能耗常量项，要求$E_{\text{consume}}(\boldsymbol{x}_t) \leqslant E_{\text{remain}}$。

（2）通信约束：无人机与服务器间每轮上行

通信量受限于最大带宽容量$C_{\max}$密文参数的数据大小远高于明文，需要保证上传数据总量不超过带宽限制。例如，若每个明文参数大小为d_0（如32位=4 byte），每个密文参数大小为d_1，则上传数据量为$\left(N-\sum_i x_{t,i}\right)d_0+\sum_i x_{t,i}d_1$，需满足：

$$D(\boldsymbol{x}_t)=\sum_{i=1}^{N}\left(x_{t,i}d_1+\left(1-x_{t,i}\right)d_0\right)\leqslant C_{\max} \quad (5)$$

（3）安全性约束：为了达到基本隐私要求，要求安全指标$S(x_t)$不低于系统设定的阈值$S_{\min}$束，确保每轮至少加密一定关键信息使攻击成功率降至可接受范围。该阈值设定遵循MaskCrypt原则[19]，即通过实验证实，当攻击成功率低于40%时系统仍能保持模型性能稳定，隐私泄露风险可控。

综合上述要素，本文建立掩码选择优化模型如下，其本质是一个0-1整数规划问题：

$$\begin{aligned}&\max_{\boldsymbol{x}_t\in\{0,1\}^N} S(\boldsymbol{x}_t)=\sum_{i=1}^{N}s_i x_{t,i},\\&\text{s.t. } E_{\text{consume}}(\boldsymbol{x}_t)\leqslant E_{\text{remain}},\\&D(\boldsymbol{x}_t)\leqslant C_{\max}\\&S(\boldsymbol{x}_t)\geqslant S_{\min}\\&x_{t,i}\in\{0,1\},i=1,2,\cdots,N\end{aligned} \quad (6)$$

上述目标函数旨在在资源许可范围内最大化被掩码加密的重要梯度信息总量，从而最大化隐私保护效力。这是一个背包类型问题：每个参数i若被选择加密（$x_{t,i}=1$），可获得隐私“收益”s_i，但要占用一定的能量和通信“成本”。通过求解该优化，可以得到当前资源条件下最优的掩码选择方案$\boldsymbol{x}_t^*$及相应的加密比例$\rho_t^*=\frac{1}{N}\sum_i x_{t,i}^*$。由于该问题在一般情况下为NP难，以传统精确算法求解在模型参数维度很高时并不现实，本文在第4节通过设计近似算法来高效求解这一掩码选择问题。

4 算法设计

为了求解上述0-1优化模型，本文设计了一种高效的贪心近似算法。该算法根据参数重要性排序并结合资源代价评估，优先选择在单位资源代价下对安全性提升贡献最大的参数进行加密，从而在保证攻击成功率受限的前提下，最大化安全指标并兼顾通信与能耗开销。其基本思路是通过引入每个参数的隐私收益密度来优先选择“性价比”最高的参数进行加密，隐私收益密度定义为$\theta_i=\frac{s_i}{c_i}$，其中s_i为参数重要性（加密所获安全增益），c_i为加密该参数所需消耗的资源代价。资源代价c_i可以综合能耗和通信成本来衡量，在简单情况下，可令每个参数加密代价相同，即$c_i=1$，则贪心策略退化为按s_i从大到小排序择优加密顶端ρN个参数。但本文考虑非均匀代价的情况，定义$c_i=0.5\cdot e_i+0.5\cdot t_i$，其中$e_i$和$t_i$分别是该参数加密和上传产生的能量消耗和通信开销，按θ_i排序以最大化单位代价的安全收益，算法在遍历排序列表时累计资源消耗，当预计加入某参数会违反约束时则跳过该参数。该近似方法计算复杂度为$\mathcal{O}(N\log N)$（主要来自排序），适用于模型参数规模较大的情形。本文提出的贪心掩码选择算法在服务器端集中执行，由服务器在每轮聚合前根据客户端上传的模型更新信息（如敏感度指标）统一计算加密掩码向量$\boldsymbol{x}$，并将其下发给各客户端。因此，该算法不会在资源受限的无人机客户端上运行，完全避免了对其计算资源和能量的直接消耗。其次，从算法复杂度角度来看，掩码选择算法的核心过程包括：按照每个参数的“加密收益密度”$\theta_i=s_i/c_i$计算排序指标，对所有参数索引进行一次排序操作（复杂度为$\mathcal{O}(N\log N)$），从排序后的序列中进行一次线性扫描选取满足约束的最大掩码集（复杂度为$\mathcal{O}(N)$）。因此，该算法的总计算复杂度为$\mathcal{O}(N\log N)$，其中N为模型参数规模。

以本文实验中使用的SimpleCNN模型为例，其总参数量约为50 000，即使在普通CPU上执行也仅需7.3 ms左右，对服务器计算资源和训练时延影响可忽略不计。为了进一步验证该点，本文在本地Intel i7-14700KF处理器上测试了不同参数规模下该算法的执行耗时，贪心算法时间开销随参数规模N变化关系如图2所示。

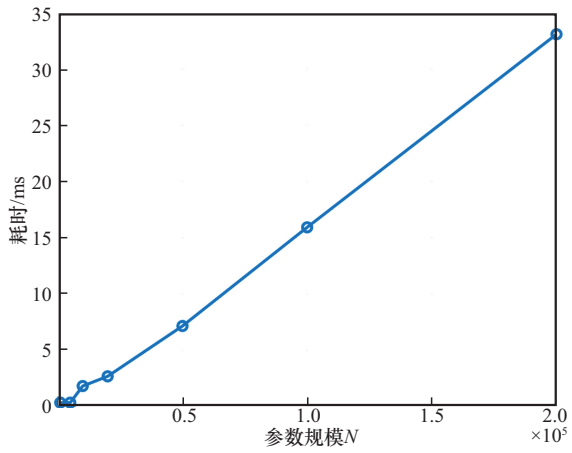


图2　贪心算法时间开销随参数规模N变化关系

可见即使在中大型模型中，该算法也能在100 ms内完成执行，远低于一轮本地训练（通常为数秒）的时间消耗。在无人机端能耗影响方面，由于加密掩码的选择结果x是由服务器直接生成并发送的，客户端仅需按照x对对应参数进行掩码加密。该过程只涉及基本的向量点乘与索引筛选操作，不会引入额外的梯度计算或训练迭代过程，不会造成客户端额外训练负担。

贪心算法的伪代码描述如算法1所示。

算法1　贪心算法

输入　参数重要性列表$\{s_i\}_{i=1}^{N}$；对应加密代价$\{c_i\}_{i=1}^{N}$；能量预算E_b；带宽预算C_b

输出　掩码选择向量$\boldsymbol{x}\in\{0,1\}^N$

初始化：$\boldsymbol{x}\leftarrow 0$; $E_{\text{sum}}\leftarrow 0$; $D_{\text{sum}}\leftarrow 0$;

for $i\leftarrow 1$ to N do

计算收益密度：$\theta_i\leftarrow s_i/c_i$;

end

将索引集合$\{1,2,\cdots,N\}$按照θ降序排列，得到索引$\pi=[\pi_1,\pi_2,\cdots,\pi_N]$;

for $j\leftarrow 1$ to N do

$i\leftarrow\pi_j$; // 获取当前第j大密度参数

设ΔE_t为参数i加密增加的能量消耗;

设ΔD_t为参数i加密增加的能量消耗;

if $E_{\text{sum}}+\Delta E_t\leqslant E_b \,||\, D_{\text{sum}}+\Delta D_t\leqslant D_b$ then

$x_i\leftarrow 1$; // 选择参数i加密

$E_{\text{sum}}=E_{\text{sum}}+\Delta E_t$

$D_{\text{sum}}=D_{\text{sum}}+\Delta D_t$

end

end

return x

在上述算法中，ΔE_i和ΔD_i分别表示选择加密参数i相较于不加密时新增的能量和数据开销。例如，ΔE_i可包括加密该参数的计算能耗和传输该参数密文的能耗增量；$\Delta D_i=d_1-d_0$则是参数i密文大小比明文大小增加的字节数。算法通过贪心选择高收益密度的参数并实时检查约束，确保输出的掩码集合既尽可能提升安全性又不超出资源限制。该贪心策略本质类似于背包问题的启发式解，对大规模问题能在短时间内给出近似可行解。在原始的MaskCrypt方法中，每轮联邦训练采用固定的加密比例，即对一定比例的参数梯度进行同态加密，该比例在训练前人为设定。然而，在实际系统中，参与方的资源约束（如通信带宽与电池电量）往往是动态变化的，且模型各参数的重要性也随训练轮次不断调整。因而，静态设定的固定加密比例难以在资源受限条件下兼顾隐私保护与系统性能之间的最优权衡。本文提出基于资源约束的动态掩码选择算法（Algorithm 1），通过计算每一参数单位资源代价下的加密收益密度$\theta_i=s_i/c_i$并进行排序，在资源预算范围内优先选择加密收益更高的参数。该算法无须预设固定加密比例，而是由当前轮次的安全需

求 $S_{\min}$ 源预算 E_b、C_b 共同决定最终的掩码选择结果 $\boldsymbol{x}_t$。在实际情况中，例如，一组22个随机生成的 s_i 和 c_i，利用本文的贪心算法和暴力求解最优解最终得到的总价值（即 $\sum_{i=1}^{N} s_i x_{t,i}$）分别是824和828，而时间开销分别是7 μs和2.11 s。尽管它不保证全局最优，但在实际场景中表现出接近最优的效果，贪心解通常与最优解差距很小，并且能够在相对极少的时间内得到近似最优解。

5 实验结果与分析

5.1 实验设置与平台实现

本文采用MNIST数据集和一个简单的卷积神经网络（SimpleCNN）作为基础实验环境。在联邦学习设置中，选取了10个客户端参与训练，每个客户端在本地进行5个epoch训练，批量大小为32。全局模型优化器为学习率0.1的随机梯度下降（SGD），损失函数为交叉熵，采用FedAvg算法对客户端模型更新取算术平均。所有实验均进行了20轮联邦训练，并以联邦轮次为横轴，考查不同方案的模型性能和资源消耗在每个轮次中的情况。实验衡量指标分别为通信开销、能量消耗、加密覆盖率、攻击成功率和模型准确率。为了支持上述实验流程的完整实现与评估，本文搭建了模拟实验平台，实现了包括客户端训练、攻击模拟、加密模拟和指标记录在内的核心功能模块。具体实现方式如下：采用Python编程语言实现，并基于PyTorch框架完成联邦学习与加密机制的建模与模拟。实验环境配置如下：处理器为Intel Core i7-14700KF，内存为32 GB，操作系统为Windows 11，Python版本为3.9，所有实验均在单机本地环境下完成模拟运行。在平台实现方面，系统功能模块包括联邦学习主控逻辑、客户端本地训练模块、攻击模拟器、掩码选择器、加密模拟器与指标评估模块等。其中，主程序main.py控制整体训练流程与轮次管理，client.py模拟各个客户端的本地模型更新过程，attack_simulator.py模拟潜在的模型窃取攻击者对未加密梯度的恢复，mask_selector.py实现基于贪心近似的加密选择算法，encryption_simulator.py则用于模拟梯度加密对通信与能耗的影响。实验所用的MNIST数据集通过torchvision库中的公共接口进行自动下载与加载，属于开放获取的标准手写数字识别数据集。所有实验运行中产生的指标数据（包括准确率、攻击成功率、能耗与通信开销等）均通过程序自动记录为结构化文件，并以Excel表格的形式输出用于后续可视化与分析。

实验比较了5种方案：方案1为未加密方案，方案2为全加密方案，方案3为MaskCrypt方法，方案4为本文提出的优化掩码选择方案，方案5为DP-FedAvg方法[20]。

5.2 结果与分析

通信开销如图3所示，能量消耗如图4所示，加密覆盖率如图5所示，攻击成功率如图6所示，模型准确率如图7所示。

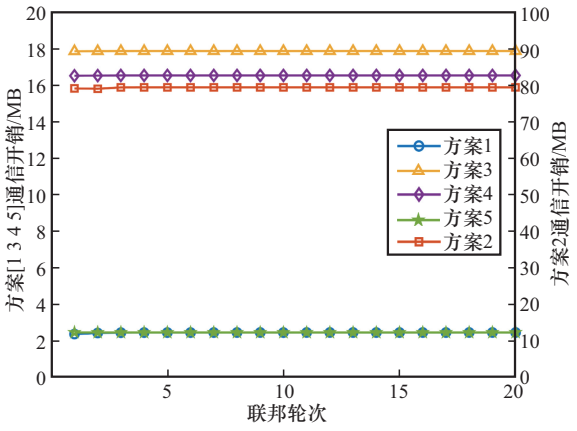


图3 通信开销

由于方案2与其他方案的资源开销差距过大，图3与图4使用了双 Y 轴记录，左轴用于表示方案[1,3,4,5]的结果，右轴用于表示方案2的结果。图3和图4中的通信开销和能量消耗分别记录每一轮次下无人机使用的通信和能量的总开销。图5和图6中加密覆盖率记录在统一掩码下被同态加密的参数个数占全模型参数总数的比例，而攻击成功率则记录

每一轮次中通过成员推理攻击和梯度反演攻击成功的次数比上攻击的总次数。图 7 中的模型准确率则用于记录通过同态加密方法进行联邦学习训练后每轮的模型训练精度是否会受到影响。

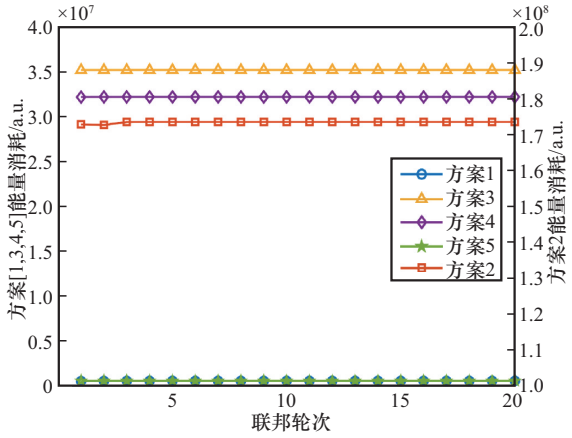


图 4　能量消耗

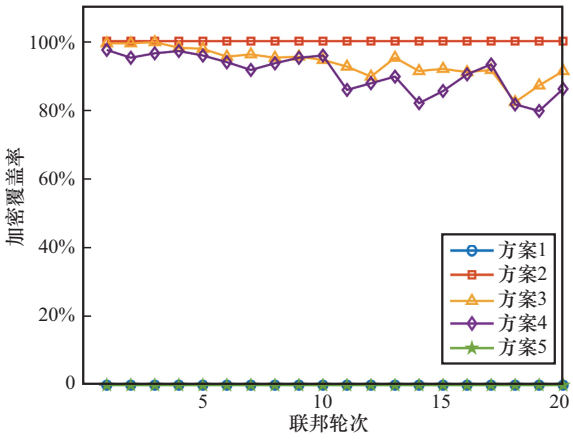


图 5　加密覆盖率

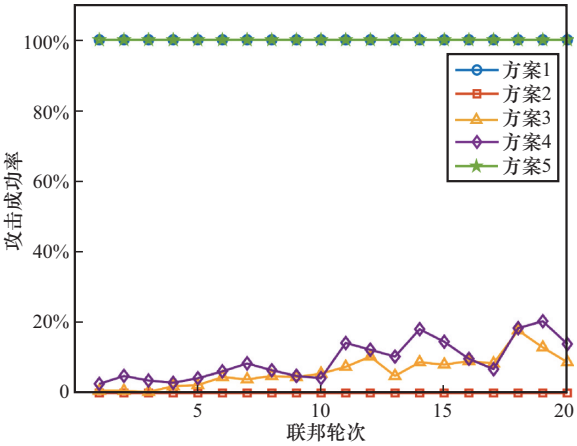


图 6　攻击成功率

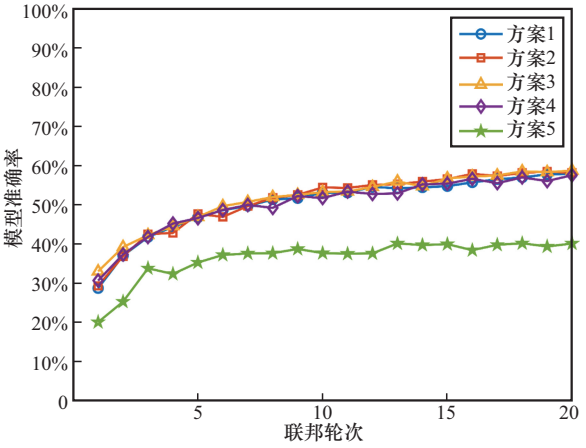


图 7　模型准确率

如图 3 和图 4 所示，方案 1 未进行同态加密而方案 2 对全部参数都进行了同态加密，因此分别使用了最少和最多的通信和能量资源，此外方案 4 的两种资源开销均低于方案 3，方案 5 由于无须进行同态加密，其通信与能量开销与方案 1 相近，开销极低，适合对资源敏感的场景。如图 5 和图 6 所示，由于方案 1 和方案 2 的加密方式，方案 1 拥有 0 的加密覆盖率和 100% 的攻击成功率，方案 2 拥有 100% 的加密覆盖率和 0 的攻击成功率，而方案 3 和方案 4 分别拥有 90.22% 和 91.33% 的加密覆盖率，以及 9.77% 和 8.66% 的攻击成功率，方案 5 未使用同态加密，加密覆盖率为 0，因此即使添加了差分隐私扰动，其对成员推断和梯度反演的防御能力仍然有限。如图 7 所示，方案[1,2,3,4]每轮次的训练精度相差不超过 1%，可以视为误差。而方案 5 是差分隐私机制注入噪声所致，对模型训练稳定性造成干扰，显著低于前 4 种方案。

综上所述，方案 3 与方案 4 相对方案[1,2,5]有显著优势，而方案 4 相对于方案 3 拥有更小的资源开销和更好的安全性。具体表现在方案[1,5]无法保护任何敏感参数而方案 2 的资源开销巨大，方案 3 和方案 4 可以显著降低资源开销（约为方案 2 的 20%），却可以同时保证 10% 以下的攻击成功率（显著低于 MaskCrypt 文章中提到的安全线

49.2%）。此外，与方案3相比，方案4通过掩码选择优化和资源限制模型，在通信开销为前者92.6%、能量消耗为前者91.5%的背景下，实现了比方案3略高的加密覆盖率和略低的攻击成功率（幅度在1%左右，可以视为安全性相当），从实验角度也验证了本文设计方案的优越性。

6 结束语

本文针对无人机场景下联邦学习与同态加密应用中存在的高开销与隐私保护矛盾，提出了一种基于MaskCrypt掩码选择的资源受限优化方案。首先，该方案通过梯度敏感度分析，识别最关键的参数维度；接着，优化模型建模，在能耗与通信预算约束内最大化安全收益；最后，通过贪心近似算法，快速求解模型得到较优解。

实验结果表明，与传统全加密方案相比，利用本文方案在将通信开销与能量消耗分别降低至20%以下的情况下，可以保持较高的加密覆盖率与较低的攻击成功率；与MaskCrypt基线相比，仅以其90%左右的资源开销，实现了与之相当的安全性保护和模型准确率。由此可知，本文所提方案能够在无人机等资源受限设备上高效平衡隐私保护与开销约束，为实际部署提供了可行的解决思路。

未来可进一步结合飞行路径规划与通信拓扑演化，优化加密资源分配策略，使其更适应动态变化的网络结构；同时也可考虑引入更强隐私保护机制如差分隐私与同态加密的协同融合，在保证加密效果的同时降低资源消耗。与此同时，还需评估本文所提方案在更复杂多任务协同、异构数据分布环境下的适应性与泛化能力，拓展其在实际低空智能网络中的应用边界。

参考文献：

[1] BASHIR A K, VICTOR N, BHATTACHARYA S, et al. Federated learning for the healthcare metaverse: concepts, applications, challenges, and future directions[J]. IEEE Internet of Things Journal, 2023, 10(24): 21873-21891.

[2] ZHANG S Y, LI J, SHI L, et al. Federated learning in intelligent transportation systems: recent applications and open problems[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(5): 3259-3285.

[3] ZHAO Y, ZHAO J, JIANG L S, et al. Privacy-preserving blockchain-based federated learning for IoT devices[J]. IEEE Internet of Things Journal, 2021, 8(3): 1817-1829.

[4] KURUNATHAN H, HUANG H L, LI K, et al. Machine learning-aided operations and communications of unmanned aerial vehicles: a contemporary survey[J]. IEEE Communications Surveys & Tutorials, 2024, 26(1): 496-533.

[5] 汤凌韬, 陈左宁, 张鲁飞, 等. 联邦学习中的隐私问题研究进展[J]. 软件学报, 2023, 34(1): 197-229.
TANG L T, CHEN Z N, ZHANG L F, et al. Research progress of privacy issues in federated learning[J]. Journal of Software, 2023, 34(1): 197-229.

[6] HITAJ B, ATENIESE G, PEREZ-CRUZ F. Deep models under the GAN: information leakage from collaborative deep learning [C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 603-618.

[7] PHONG L T, AONO Y, HAYASHI T, et al. Privacy-preserving deep learning via additively homomorphic encryption[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(5): 1333-1345.

[8] JIANG Z F, WANG W, LIU Y. FLASHE: additively symmetric homomorphic encryption for cross-silo federated learning[EB]. 2021.

[9] 李晓东, 李慧, 赵炽野, 等. 基于模分量同态加密的隐私数据联邦学习研究[J]. 信息安全研究, 2025, 11(3): 198-204.
LI X D, LI H, ZHAO C Y, et al. Privacy-preserving federated learning research based on confused modulo projection homomorphic encryption[J]. Journal of Information Security Research, 2025, 11(3): 198-204.

[10] LIU X Y, LI H W, XU G W, et al. Privacy-enhanced federated learning against poisoning adversaries[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 4574-4588.

[11] ZHANG X L, FU A M, WANG H Q, et al. A privacy-preserving and verifiable federated learning scheme[C]//Proceedings of the 2020 IEEE International Conference on Communications (ICC). Piscataway: IEEE Press, 2020: 1-6.

[12] 余晟兴, 陈钟. 基于同态加密的高效安全联邦学习聚合框架[J]. 通信学报, 2023, 44(1): 14-28.
YU S X, CHEN Z. Efficient secure federated learning aggrega-

tion framework based on homomorphic encryption[J]. Journal on Communications, 2023, 44(1): 14-28.

[13] MA J, NAAS S A, SIGG S, et al. Privacy-preserving federated learning based on multi-key homomorphic encryption[J]. International Journal of Intelligent Systems, 2022, 37(9): 5880-5901.

[14] XU G W, LI H W, LIU S, et al. VerifyNet: secure and verifiable federated learning[J]. IEEE Transactions on Information Forensics and Security, 2019, 15: 911-926.

[15] 郭显, 王典冬, 冯涛, 等. 基于同态加密的可验证隐私保护联邦学习方案[J]. 电子与信息学报, 2025, 47(4): 1113-1125.
GUO X, WANG D D, FENG T, et al. A verifiable privacy protection federated learning scheme based on homomorphic encryption[J]. Journal of Electronics & Information Technology, 2025, 47(4): 1113-1125.

[16] HIJAZI N M, ALOQAILY M, GUIZANI M, et al. Secure federated learning with fully homomorphic encryption for IoT communications[J]. IEEE Internet of Things Journal, 2024, 11(3): 4289-4300.

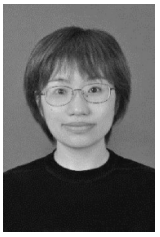
[17] 卢为党, 冯凯, 丁雨, 等. 基于无人机辅助联邦边缘学习通信系统的安全隐私能效研究[J]. 电子与信息学报, 2025, 47(5): 1322-1331.
LU W D, FENG K, DING Y, et al. Research on security, privacy, and energy efficiency in unmanned aerial vehicle-assisted federal edge learning communication systems[J]. Journal of Electronics & Information Technology, 2025, 47(5): 1322-1331.

[18] 卢彦丰, 吴韬, 刘春生, 等. 无人机辅助的高能效边缘联邦学习综述[J]. 计算机科学, 2024, 51(4): 270-279.
LU Y F, WU T, LIU C S, et al. Survey of UAV-assisted energy-efficient edge federated learning[J]. Computer Science, 2024, 51(4): 270-279.

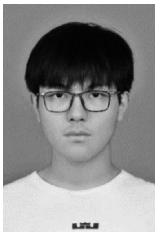
[19] HU C H, LI B C. MaskCrypt: federated learning with selective homomorphic encryption[J]. IEEE Transactions on Dependable and Secure Computing, 2025, 22(1): 221-233.

[20] MCMAHAN H B, RAMAGE D, TALWAR K, et al. Learning differentially private recurrent language models[C]//Proceedings of the 6th International Conference on Learning Representations (ICLR). Vancouver: ICLR, 2018.

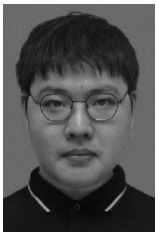
[作者简介]



仇建斌（1988– ），女，南京工业大学信息管理中心工程师，主要研究方向为数据安全、高校信息化。



章祖葳（2002– ），男，南京工业大学计算机与信息工程学院（人工智能学院）硕士生，主要研究方向为网络调度、密码学。



郑宇辉（2002– ），男，南京工业大学计算机与信息工程学院（人工智能学院）在读，主要研究方向为计算机网络、网络安全。