面向天基信息网络的智能模型分布式训练技术

栗渊钧[1]，杨德伟[1]，李佳宁[1]，冯　笑[2]
（1.北京理工大学信息与电子学院，北京 100081；
2.中国电子科技集团公司第十五研究所，北京 100083）

摘　要：针对天基信息网络中智能模型的分布式训练存在数据分布异构、模型陈旧以及隐私安全等问题，提出基于区块链的智能模型联邦学习架构和安全高效训练方法，引入差分隐私噪声机制和参数评估方法，有效应对隐私泄露、中毒攻击和单点故障威胁；采用基于时延最小的模型聚合方法，通过轨道内外的模型广播及区块广播过程，加速模型训练。仿真结果表明，所提方法能使不同结构的智能模型快速收敛，缩短训练时间，并有效应对安全隐私威胁。

关键词：天基信息网络；联邦学习；智能模型；区块链技术
中图分类号：TP393
文献标识码：A
doi：10.11959/j.issn.2096−8930.2025004

Distributed Training Techniques for Intelligent Model in Space-Based Information Networks

LI Yuanjun[1], YANG Dewei[1], LI Jianing[1], FENG Xiao[2]
1. School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China
2. The 15th Institute of China Electronics Technology Group Corporation, Beijing 100083, China

Abstract: In addressing the issues of data distribution heterogeneity, outdated models, and data privacy and security in distributed training of intelligent models, a federated learning architecture of intelligent models was designed based on blockchain technology and applied to space-based information networks. A secure and efficient training method for intelligent models was proposed based on this architecture, where a differential privacy noise mechanism, the blockchain technology and a parameter evaluation method were introduced to effectively deal with privacy leakage, poisoning attacks and single-point failure threats. Meanwhile, using a model aggregation method based on the minimized delay, the model training was accelerated via the processes of intra-orbit and inter-orbit model broadcasting and block broadcasting. The simulation results indicated that the proposed method enables intelligent models of different structures to converge rapidly, shorten the model training time, and effectively deal with security and privacy threats.

Keywords: space-based information network, federated learning, intelligent model, blockchain technology

0　引言

人工智能（Artificial Intelligence，AI）技术在天基信息网络的应用得益于卫星星座朝着低轨道、大规模方向的发展，除了针对卫星通信网络性能的优化应用，还包含智慧城市、自然环境感知、军事战场决策以及灾害救援等方面[1-2]。这些场景中的应用需要大量设备采集环境数据、提取特征，然后利用AI模型决策出一个更接近目标或者获取更多长期奖励的行为。在数据准备阶段，单个设备感知到的数据往往会因为样本不够多而不足以充分训练模型，导致结果偏差，从而使智能模型丧失泛用性和精度。因此在理想情况下，所有设备收集到的数据会被汇聚到一个云端服务器上，并在其上训练模型。

然而，由于通信资源的限制，智能模型在天基信息

收稿日期：2024−11−15；**修回日期：**2025−02−10
基金项目：国家重点研发计划资助项目（No. 2022YFB2902703）
Foundation Item: National Key Research and Development Program of China(No. 2022YFB2902703)

网络上进行集中式训练面临很多问题和挑战。一方面，传统的中心化模型训练往往需要将数据传输到硬件性能较高的高轨卫星或者地面站进行处理。对于安全监控、战场侦察等场景中需要持续更新或快速响应的AI应用，传统方法的训练周期跟不上业务的数据更新速度，会造成智能模型过时、效能降低的问题；另外，从广泛分布的终端向云端传输庞大的数据量不仅会给通信网络带来重负，而且还会产生数据安全和隐私泄露问题。为了解决这些问题，联邦学习（Federated Learning，FL）成为了一个备受关注的研究方向[3-4]。

在传统联邦学习过程中，客户端负责模型训练，而中央服务器负责模型聚合，如图1所示。客户端会定期将本地模型更新并上传到中央服务器，以保持中央服务器中全局模型的时效性。不同于集中式训练方法，联邦学习将原始数据替换为模型参数进行数据传输，一定程度上保障了数据隐私安全性。

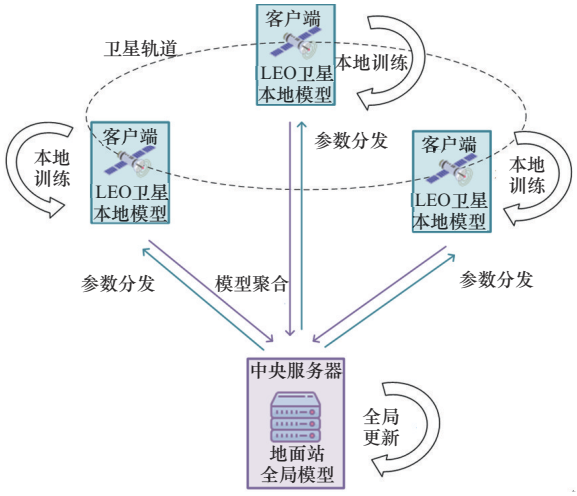

图1　天基信息网络的传统联邦学习架构

联邦学习可以在保护数据隐私的同时，实现多颗卫星之间的协同学习，从而提高数据处理的效率和准确度[5]。基于此，已经有许多学者研究了基于FL的卫星AI应用。例如，参考文献[6-8]针对天基信息网络中的安全隐患，如威胁检测、入侵探测等问题，设计并实现了一种基于FL的网络安全架构，该架构在恶意流量识别率、数据包丢失率与CPU资源占用情况等方面优于传统的深度学习入侵检测方法。

在天基信息网络场景中，尽管FL的引入使得卫星不再需要向地面云端服务器上传原始数据，但为了聚合和更新全局模型，处在边缘端的卫星仍需将本地更新的模型参数上传。随着网络模型规模的扩大以及卫星对地面站（Ground Station，GS）的非实时可见性，这种模型参数的传输依旧可能造成不可忽视的处理时延，另外，计算资源和数据的不均匀分布也会进一步影响训练效率和全局模型精度。为了应对以上挑战，许多学者针对天基信息网络的FL做了进一步优化[9-11]。首先，参考文献[9]假设了一种地面站位于北极的理想情况，根据可预测的卫星——地面站连接图案，将同步聚合算法调整修改为异步聚合的FedSat算法，从而减少聚合等待时间，进而在保证模型性能的同时加速了训练进程。其次，参考文献[10]又提出了FedISL方法，通过星间链路（Inter-Satellite Link，ISL）实现两阶段的模型聚合，包含轨道内的部分聚合和经由地面站的轨道间聚合，所提方法有效地降低了训练时延。在参考文献[10]基础上，FedSatSchedule[11]是一种通过评估每颗卫星的可见时间窗口来缓解模型陈旧问题的FL调度方法，当可见窗口不足以支撑本地更新上传时，就会让卫星在下一轮通信中再次上传本地模型的更新参数，并让卫星在不可见期间进行本地模型训练，确保资源的有效利用。此外，随着模型逆向攻击技术的发展，攻击者能够从模型梯度逆向推断出训练集特征属性、代表性数据乃至重构输入数据[12-14]。因此，在FL训练过程中客户端直接向云端服务器传输模型参数也存在一定的安全隐患。为此，区块链技术作为一种有望保障联邦学习过程中隐私安全的解决方案，正在被广泛研究[15-18]。

综上所述，天基网络场景下的联邦学习仍存在数据分布异构、模型陈旧以及数据隐私安全等挑战，需要进一步研究。

1　系统模型

1.1　基本架构

为了在智能模型信息共享的同时保障数据隐私安全，本文将联邦学习技术与区块链技术相融合，并将其应用到卫星星座场景中，提出基于区块链的天基信息网络联邦学习架构，如图2所示。该架构包含卫星星座层、联邦学习层以及区块链层。处在底层的卫星星座层是整个架构的物理实体，具体指低轨卫星星座环境，主要包含LEO卫星和ISL；联邦学习层引入分布式的AI训练机制，其中主要包含训练节点，由LEO卫星上的AI计算硬件构成，完成智能模型的训练任务；最上层的区块链层用于加强整个架构的安全保障，主要包含区块链节点，通过共识过程对区块链中的区块进行同步验证，实现对联邦学习过程的安全隐私赋能。在整个架构中，每颗LEO卫

星既在卫星星座中充当通信节点，通过ISL与轨道内外的其他卫星进行数据通信，又充当联邦学习中的训练节点，运用星上的AI计算能力完成智能模型的本地训练，通过定期地上传和拉取全局模型实现多卫星协同训练；此外还充当区块链层中的区块链节点，通过共识机制产生区块，对区块进行同步验证，进而增强联邦学习的安全隐私保障。

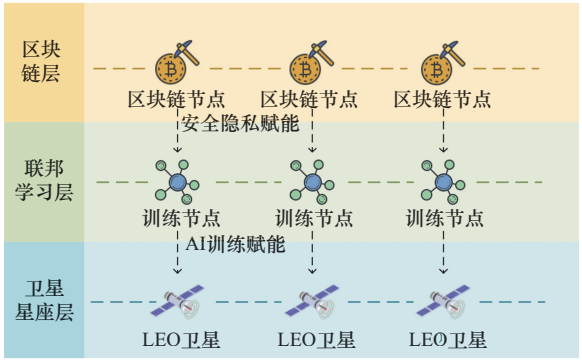

图2　基于区块链的天基信息网络联邦学习架构

1.2　时延模型

基于1.1节所述架构，卫星星座可以实现安全可信的分布式协同训练，时延是整个架构的重要评估指标，在本节中，时延模型主要建模为通信时延和计算时延之和。

通信时延包括传输时延和传播时延，如式（1）所示

$$t_{\mathrm{Comm}} = t_{\mathrm{Trans}} + t_{\mathrm{Prop}} \tag{1}$$

传输时延是指数据包从开始发送到结束发送所经历的耗时，在本节中定义为模型参数的数据量大小与系统容量的比值，如式（2）所示

$$t_{\mathrm{Trans}} = S(w)/r_{k_1,k_2} \tag{2}$$

其中，$S(w)$是模型参数w的数据量大小，单位为比特（bit），r_{k_1,k_2}为卫星k_1与卫星k_2之间ISL的信道容量，其计算表达式可以用香农公式表示为

$$r_{k_1,k_2} = B\log_2(1 + \mathrm{SNR}(k_1,k_2)) \tag{3}$$

其中，B为传输带宽，$\mathrm{SNR}(k_1,k_2)$为卫星k_1与卫星k_2之间ISL的信噪比（Signal to Noise Ratio，SNR）。

传播时延是指模型参数数据从发送卫星发出到接收卫星接收的耗时，定义为信号在自由空间中传播所需要的时延，如式(4)所示

$$t_{\mathrm{Prop}} = d(k_1,k_2)/c \tag{4}$$

其中，$d(k_1,k_2)$为卫星k_1与卫星k_2之间的直线距离，c为光速。

在所提架构中，计算时延包含智能模型的训练时延、模型参数的交易验证时延、区块的生成时延以及其验证时延等。在这些时延之中，智能模型的训练时延和通过共识机制区块的生成时延是主要部分，因此本节主要针对这两种时延进行建模，如式(5)所示

$$t_{\mathrm{Comp}} = t_{\mathrm{train}} + t_{\mathrm{block}} \tag{5}$$

其中，t_{block}为区块生成时延，其会随着共识算法、计算机的硬件设备性能变化而变化，例如在采用工作量证明（Proof of Work，PoW）共识方法时，区块生成时延会随着共识难度的提高而增加；t_{train}为智能模型的训练时延，主要与卫星计算能力以及智能模型训练的超参数配置有关，对于卫星k的训练时延，可以给出为

$$t_{\mathrm{train},k} = (I_{\mathrm{tr}}D_k c_{\mathrm{batch}} + I_{\mathrm{tr}}\left\lceil \frac{D_k}{S_{\mathrm{batch}}} \right\rceil n_w c_s + I_{\mathrm{tr}}\left\lceil \frac{D_k}{S_{\mathrm{batch}}} \right\rceil n_w c_g)/v_k \tag{6}$$

其中，$\lceil\ \rceil$表示向上取整操作，v_k为计算机的CPU频率，I_{tr}为训练轮次，D_k为数据集大小，S_{batch}为批大小，n_w为参数w的维度。每轮次训练包含3个过程：将数据打乱并拆分为$\left\lceil \frac{D_k}{S_{\mathrm{batch}}} \right\rceil$个批次，且每个样本需要经过$c_{\mathrm{batch}}$个CPU周期；对每个批次都进行一次网络前馈传播计算，此过程每批次每维度需要c_s个CPU周期；最后是计算梯度，每批次每维度需要c_g个CPU周期。

2　基于区块链的安全高效训练方法

2.1　总体流程

传统联邦学习方法面临来自各方面的威胁：其一为潜在的隐私泄露威胁，虽然联邦学习通过只传输模型参数的形式一定程度上保护了数据隐私，但是攻击者仍有办法通过模型参数信息推测出边缘卫星设备的隐私数据信息；其二为中毒攻击威胁，恶意参与方可以通过篡改原始数据或者提交错误的本地模型更新梯度来破坏联邦学习的收敛性；其三为单点故障威胁，在传统的联邦学习方法中，用于聚合本地更新的模型以及维护全局模型的中央服务器一旦被恶意方攻击导致瘫痪，整个联邦学习进程就会无法执行。

为了有效避免上述威胁，基于1.1节所述架构，本节提出一种基于区块链的安全高效分布式训练方法，如图3所示。

首先，在训练流程开始之前对系统进行初始化。系统中存在一个任务发布者，即发布智能模型训练任务的LEO卫星，其余所有参与分布式训练的LEO卫星向任务发布者申请注册为区块链网络中的区块链节点。任务发布者为其余LEO卫星分配私钥和公钥，并根据训练任务

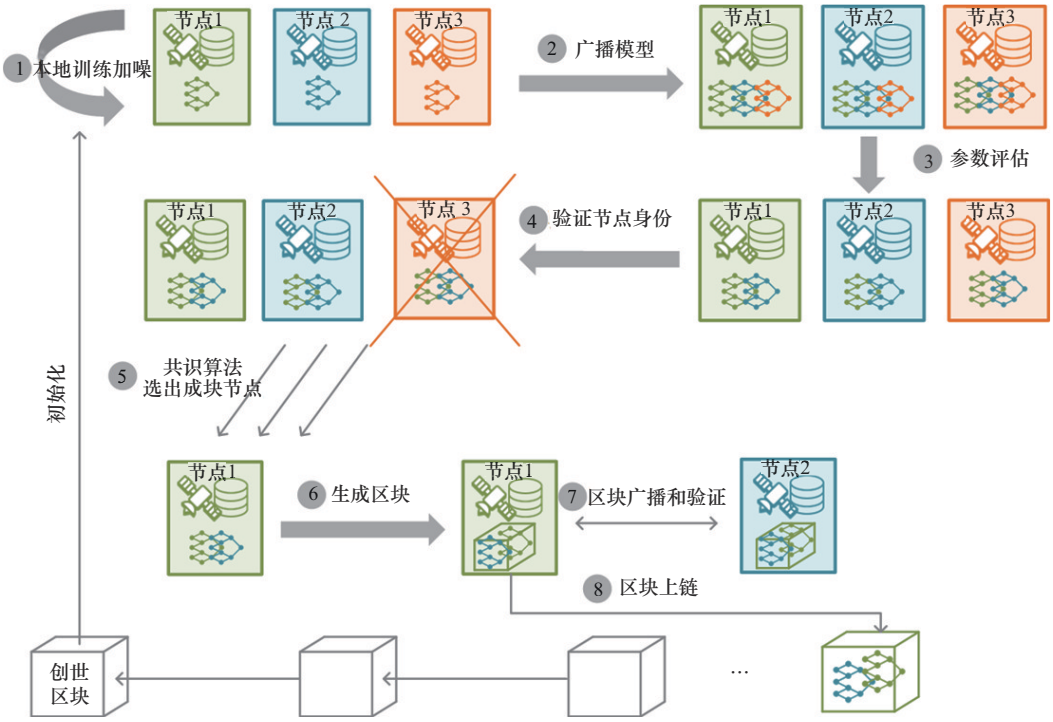

图 3　基于区块链的安全高效分布式训练方法

初始化创世区块（区块链中的第一个区块），通过安全链路分发给所有 LEO 卫星。创世区块主要包含如下信息：全局模型的初始化参数和总训练轮数、所有 LEO 卫星的公钥及所有本地训练数据集大小。另外，本节假设在系统初始化阶段，创世区块的分发同步是安全可靠的，并在后续模型训练过程中，任务发布者与其他 LEO 卫星节点不再进行区分。该方法的训练过程分为以下几个阶段，具体流程如下。

其一，本地训练并加噪。区块保存着每轮训练的全局模型，并且按照时间先后次序排列，在训练开始之前，每个 LEO 节点通过拉取区块链末尾的区块来获得最新的全局模型，并将其作为本轮本地训练的初始模型；接着利用预先存储的训练数据集进行本地模型训练，得到新的本地模型参数。为了应对隐私泄露威胁，引入差分隐私噪声，并通过训练过程自适应调整噪声容限，减少噪声对模型精度的负面影响。

其二，广播模型。每颗 LEO 卫星利用本节点的私钥对训练好并加噪的模型参数进行签名，并将模型参数与签名广播给其他 LEO 卫星。在收到其他 LEO 卫星的模型参数及签名后，本节点首先从创世区块中找到对应的公钥，并用公钥验证签名，将得到的结果与接收到的模型参数进行对比。如果一致，则说明传输过程没有遭受恶意攻击或篡改，可以有效避免中毒攻击威胁。

其三，参数评估。在分布式训练架构中，由于训练数据分布的异构性以及不同 LEO 卫星计算能力的差异性，同一训练轮次中不同 LEO 卫星得到的模型参数质量也不尽相同。另外，LEO 卫星存储的训练数据中可能包含用户的隐私信息，且训练模型需要消耗计算资源，因此存在部分节点不愿意参与协同训练，甚至出现部分恶意节点上传虚假参数误导全局模型训练趋势的现象。

为了保障分布式训练过程的真实有效，避免恶意节点上传虚假参数，本节利用基于 Multi-KRUM 参数的评估方法对模型参数进行筛选，从而有效抵御中毒攻击。该方法能够有效抵御部分参与分布式训练节点的恶意行为，其核心思想是“少数服从多数”，通过欧式距离测度来筛选出离群的模型参数，进而将其剔除。假设共有 N_{sat} 个 LEO 卫星节点，其中 N_{po} 个恶意节点，那么每个节点的模型质量表达式为

$$\text{mq}_i = \sum_{i \to j} \left\| \bar{w}_i - \bar{w}_j \right\| \tag{7}$$

其中，mq_i 为 LEO 卫星 i 经过模型参数质量评估的得分，$\bar{w}_i$ 为 LEO 卫星 i 经过模型训练并加噪后的模型参数，$i \to j$ 代表距离 $\bar{w}_i$ 最近的 $N_{\text{sat}} - N_{\text{po}} - 2$ 个模型参数之一。通过比较每颗卫星的模型参数质量得分，最终选出 $N_{\text{sat}} - N_{\text{po}}$ 个质量得分最低的模型参数作为本轮聚合的合法模型。

其四，验证节点身份。经过第三步的参数评估，一

些节点由于自身数据和计算能力的限制或者恶意行为，其产生的模型参数将不参与全局模型聚合，因此在本轮训练中将其认定为恶意节点，不参与后续的流程。

其五，通过共识算法选出成块节点。在本节中采用PoW共识算法，每个节点根据节点序号、时间戳、前一个区块的哈希值以及一个非重复的随机数值进行哈希计算，首先计算出哈希值前N_{zero}位为零的节点作为成块节点，N_{zero}也被称为PoW共识算法的难度系数。

其六，生成区块。通过共识机制选出的成块节点，对所有合法的本地模型进行聚合得到全局模型，并将其打包为区块，聚合表达式给出为

$$w_{\text{avg}} = \sum_{i-1}^{N_{\text{sat}} - N_{\text{po}}} \bar{w}_i / D_i \tag{8}$$

其中，w_{avg}为全局模型参数，D_i为LEO卫星i上训练数据集的大小。

其七，区块广播和验证。成块节点将打包好的区块在合法节点范围内广播，其他合法节点需要对区块进行验证：区块内的前驱区块哈希值与上一个区块内对应的哈希值相同，且区块的索引值等于上一个区块的索引值加一。经过这两个步骤，区块被验证为合法区块。

其八，区块上链。区块被验证合法后，接入区块链，结束本轮训练。为了应对单点故障威胁，利用区块链替代中央服务器进行模型聚合和全局模型维护，将联邦学习去中心化，有效地解决了单点故障问题。

2.2　基于时延最小的模型聚合方法

在传统的联邦学习架构中，模型的聚合过程通过一个中央服务器收集客户端的本地更新参数来完成，在卫星场景中，中央服务器通常部署在地面，卫星客户端通过星地链路向地面站传输本地模型更新，由于卫星与地面站的非实时可见性，这种学习架构通常需要较长的时间来完成模型训练任务。为此，本节采用时延最小的模型聚合方法，加速模型训练过程。

首先，建立系统模型。考虑一个包含N_{o}个轨道面的卫星星座，星座构型为Walker Delta，每个轨道的卫星数目为N_{spo}，且相邻轨道面的卫星运行方向相反。不同卫星之间通过ISL实现数据的传输，距离海平面80 km之内的大气层会阻挡ISL的传输[15]，因此可以进行数据交互的两颗卫星之间的最远距离为

$$d_{\max}(t; k_1, k_2) = \sqrt{\left\| r_{k_1}(t) \right\|^2 - r_{\text{T}}^2} + \sqrt{\left\| r_{k_2}(t) \right\|^2 - r_{\text{T}}^2} \tag{9}$$

其中，$\left\| r_{k_1}(t) \right\|$与$\left\| r_{k_2}(t) \right\|$分别是$t$时刻卫星$k_1$与卫星$k_2$到地心的距离，$r_{\text{T}} = r_{\text{E}} + 80$，$r_{\text{E}}$为地球半径。当卫星$k_1$与卫星$r_{k_2}$在$t$时刻的直线距离$d_t(t; k_1, k_2)$小于最大距离$d_{\max}(t; k_1, k_2)$时，认为两颗卫星之间存在ISL，能够传输数据。此外，假定每颗卫星具有4条链路，轨道内能够通过上下两条ISL与同一轨道的相邻卫星传输数据，左右两条轨道间ISL能够与其他轨道上的卫星建立连接关系。

其次，提出优化问题。基于2.1节所述方法的总体流程，为了加快模型训练速度，本节建立最小化一轮次模型训练时延的优化问题，如式（10）所示

$$\min T_{\text{round}} = t_{\text{train}} + t_{\text{mob}} + t_{\text{op}} + t_{\text{block}} + t_{\text{blb}} \tag{10}$$

其中，t_{train}为所有卫星完成本地模型训练的时间；t_{mob}为模型参数广播所需要的时延，包含轨道内广播时延和轨道间广播时延；t_{op}为中间处理时延，包含参数评估与验证节点身份所需要的处理时延；t_{block}为区块链点通过共识机制竞争产生区块所消耗的时间；t_{blb}为区块的广播时延。其中，t_{train}与t_{block}的计算方法已经在1.2节给出，t_{op}通常来说时延相对极短，可以忽略不计。

最后，本节重点关注模型广播时延与区块广播时延，提出基于时延最小的模型聚合方法，该方法共包含轨道内的模型广播、轨道间的模型广播及区块广播3个过程。

（1）轨道内的模型广播

当某颗卫星完成本地模型训练之后，需要先将本地模型更新广播给该卫星所在轨道面的其他卫星。鉴于轨道内卫星的环状拓扑，且相邻卫星间的传输时延相同，轨道内的模型广播时延可以表示为

$$t_{\text{mointra}} = \left\lfloor N_{\text{spo}}/2 \right\rfloor \times t_{\text{cointra}} \tag{11}$$

其中，t_{cointra}为轨道内一跳ISL所需要的通信时延，计算方法同式（1）。每个轨道有N_{spo}颗卫星，则将某颗卫星的本地参数广播到整个轨道面的ISL跳数最多为$\left\lfloor N_{\text{spo}}/2 \right\rfloor$（$\lfloor\ \rfloor$表示向下取整）。图4给出了一个$N_{\text{spo}} = 8$时的轨道内模型广播示意，各颗卫星同时开始广播本地模型，而两颗距离最远的卫星之间的通信时延为t_{mointra}，因此经过t_{mointra}，所有本地模型的广播完成。

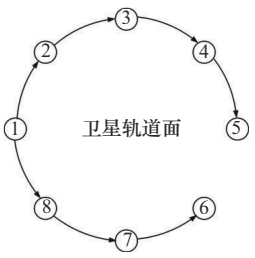

图4　N_{spo}=8时的轨道内模型广播示意

（2）轨道间的模型广播

对于相邻轨道运行方向相反的 Walker Delta 卫星来说，在任意时刻都会有 N_o 颗处在不同轨道上的卫星位于同一纬度，若将其分为一个卫星组，则整个卫星星座共有 N_{spo} 个卫星组。另外，当卫星组内的卫星之间相互不可见时，表示卫星组处于未激活状态；若组内卫星之间存在ISL，可以进行数据传输时，卫星组进入激活状态。鉴于卫星运动轨迹的可预测性，在得到轨道内模型广播结束时各卫星的地理位置后，从 N_{spo} 个卫星组中选择一个进行轨道间的模型广播，选择依据是：当有若干卫星组之间存在轨道间ISL时，选择相邻卫星距离最短的一组；若所有卫星组均处于未激活状态，则选择最快可以进入激活状态的一组卫星，如图5所示。当选择好某一个卫星组之后，首先在这组卫星间进行轨道间的模型广播，这样该组内的卫星获得了所有的模型参数，之后所有轨道再各自同时进行一次轨道内的模型广播过程。因而，整个星座内的模型广播时延可以给出为

$$t_{\text{mointer}} = t_{\text{wait}} + \left\lfloor N_o/2 \right\rfloor \times t_{\text{cointer}} + t_{\text{mointra}} \tag{12}$$

其中，t_{mointer} 为轨道间一跳ISL所需要的通信时延，计算方法同式（1）。

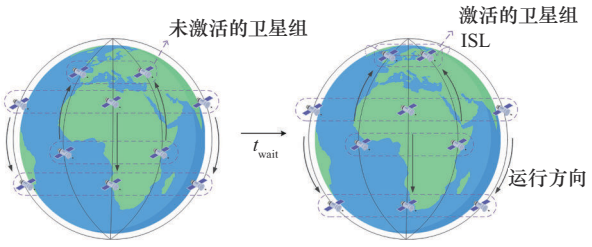

图5　模型参数的轨道间广播

（3）区块广播

在模型广播过程结束后，会先经过参数评估和节点身份认证将恶意节点剔除。为了加快区块生成之后的广播过程，按照前述卫星组选择依据，在合法节点中挑选卫星组作为区块链节点完成共识过程。需要注意的是，该组内不能存在被剔除的恶意节点。另外，由于共识过程需要的时延远小于卫星组的可见周期，该卫星组内通过共识竞争选出成块节点后，首先进行轨道间的区块广播，其次在各个轨道内进行轨道内的区块广播。因此，区块广播时延可以给出为

$$t_{\text{blinter}} = t_{\text{wait}} + t_{\text{block}} + \left\lfloor N_o/2 \right\rfloor \times t_{\text{cointer}} + \left\lfloor N_{spo}/2 \right\rfloor \times t_{\text{cointra}} \tag{13}$$

至此，完成一轮模型训练，所提的模型聚合方法实现了几乎实时的模型聚合过程，有效缩短了卫星的等待时延，进而加快了模型训练过程。

3　实验与仿真分析

3.1　实验设置

首先，为了分析天基信息网络中基于区块链的分布式训练技术，需要构建卫星星座的仿真环境，获取每颗卫星的运行轨迹。因此，如图6所示，构建了一个包含5个轨道共40颗LEO卫星的Walker Delta卫星星座，具体的卫星星座参数见表1。

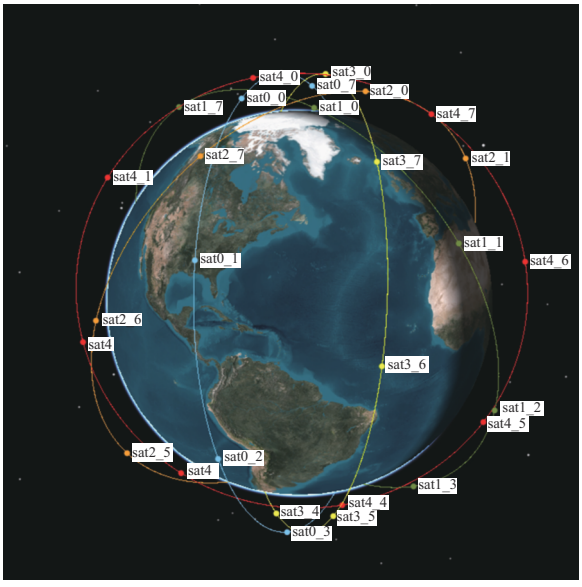

图6　Walker Delta卫星星座

表1　卫星星座参数

参数	取值
轨道个数	5个
每个轨道上的卫星数	8颗
轨道倾角	80°
轨道高度	1 200 km
频率	20 GHz
带宽	250 MHz
EIRP	34.6 dBW
调制与编码方式	16 APSK
滚降系数	0.1
最大仰角	55°

其次，本节以经典的手写数字图像分类任务为例，测试算法性能。模型训练集为MINIST数据集[19]，

MINIST 数据集一共有 7 万张图片，其中 6 万张是训练集，1 万张是测试集。另外，为了测试不同模型结构在所提学习架构中的收敛性，考虑 4 种不同的网络结构：多层感知机（Multilayer Perceptron，MLP）、卷积神经网络（Convolutional Neural Network，CNN）[4]、LeNet[20] 以及 AlexNet[21]，这 4 种网络结构的网络层参数见表 2。

表 2　网络层参数

网络结构	卷积层个数/个	全连接层个数/个	总层数/层
MLP	0	2	2
CNN	2	2	4
LeNet	2	3	5
AlexNet	5	3	8

最后，为了测试不同类型的数据分布对于模型性能的影响，考虑两种不同的数据分布情况：独立同分布（Independent Identically Distributed，IID）与非独立同分布（Non-Independent Identically Distributed，Non-IID）。对于数据分布为 IID 的情况，每个客户端所持有的手写数字图片的类型分布是一样的，即不同手写数字的样本数目相等；对于数据分布为 Non-IID 的情况，每个客户端将随机持有两种数字的样本，并且它们的数目相等。

3.2　仿真分析

（1）收敛性仿真

首先，依据基于区块链的联邦学习架构，对不同网络模型进行收敛性仿真，表 3 为不同网络模型在 50 轮次训练后的分类准确度对比结果，图 7、图 8 为不同网络模型的训练准确度曲线。受初始参数的影响，训练初期的模型准确度较低，且模型结构越复杂，训练难度越大，准确度性能表现越差。随着训练轮次逐步增多，最终的准确度排行如下：AlexNet 最优，LeNet 次之，CNN 和 MLP 最差。同时相比于数据分布为 Non-IID 的情况，在数据分布为 IID 的情况下，模型收敛更快更稳定，且准确度更好。

表 3　不同网络模型在不同数据分布情况下的准确度对比

模型	数据分布为 IID 时的准确度	数据分布为 Non-IID 时的准确度
MLP	97.22%	92.57%
CNN	98.39%	93.34%
LeNet	98.84%	95.85%
AlexNet	98.94%	96.72%

图 9、图 10 给出了不同数据分布情况下不同网络模型的训练损失曲线。从不同模型的角度看，LeNet 与 AlexNet 相比其他模型有着更低的训练损失，对应着更好的预测精度；从不同数据分布的角度看，图 9 中所有模型均在 10 个训练轮次之后逐渐收敛，且收敛平稳，图 10 中 AlexNet 在 10 个训练轮次附近仍然有一定波动，且曲线的整体波动幅度相较 IID 情况更大，对应模型预测性能的不平稳。

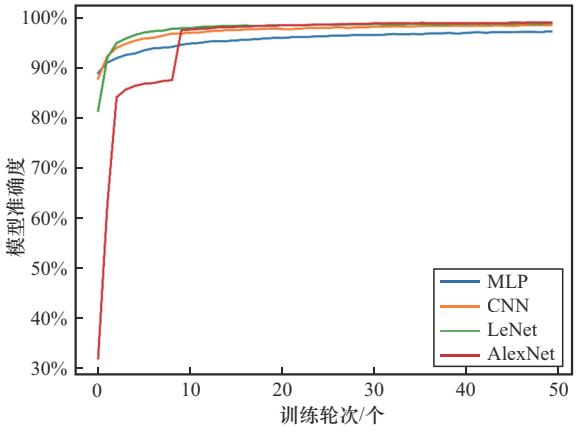

图 7　数据分布为 IID 时不同网络模型的训练准确度

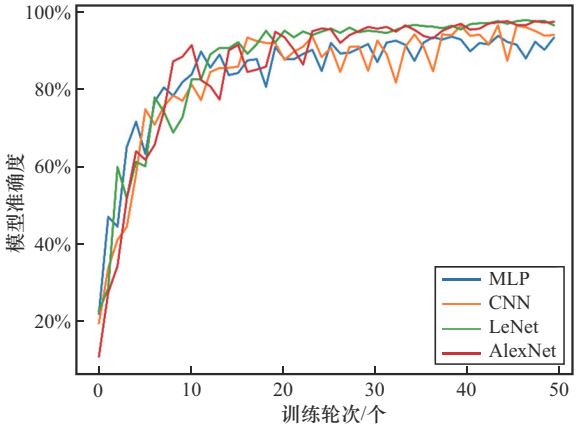

图 8　数据分布为 Non-IID 时不同网络模型的训练准确度

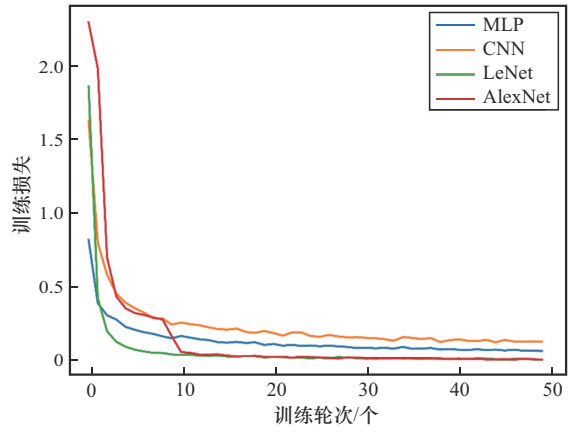

图 9　数据分布为 IID 时不同网络模型的训练损失

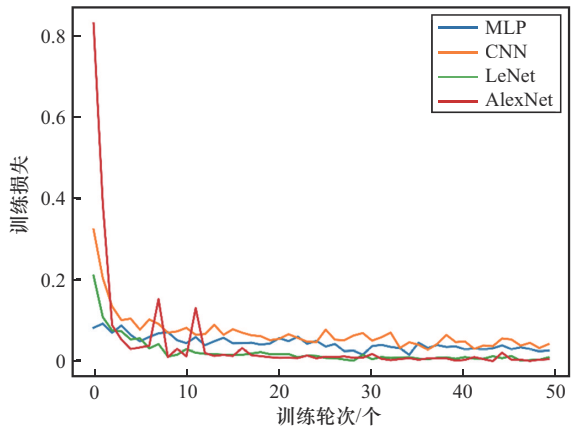

图 10　数据分布为 Non-IID 时不同网络模型的训练损失

另外，训练损失的大小并不严格对应模型准确度的高低。这是由于训练损失是测试样本的预测值与真实值之间的距离平均，因此一些距离较远的样本（离群点）会影响最终的损失大小。如图 9 所示，CNN 的训练损失要比 MLP 高，但是不论是 IID 还是 Non-IID 的情况，CNN 的测试准确度都要比 MLP 的准确度要高。

（2）训练时延仿真

为了验证 3.2 节所述方法能够加速模型聚合，进而缩短模型训练时间，本节将其与传统的中心化联邦学习架构进行对比，并采用同步聚合算法 FedAvg[12]。为此，构建两个地面站位置不同的卫星星座场景，如图 11、图 12 所示，图 11 中地面站位于北极点，图 12 中地面站位于北京。

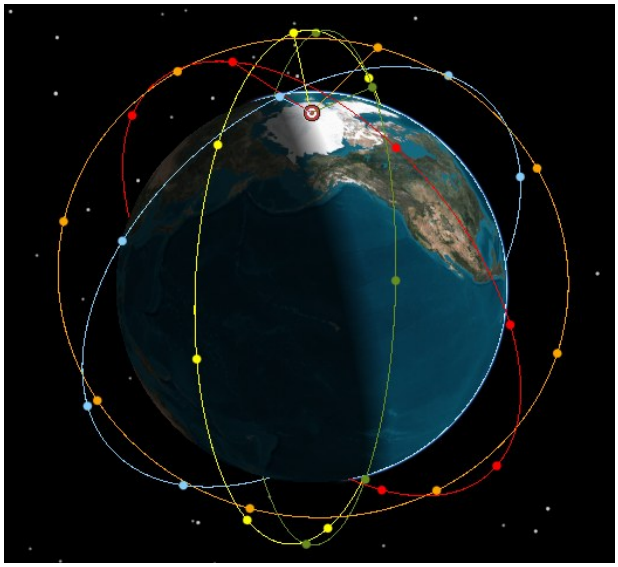

图 11　地面站在北极点的星座场景

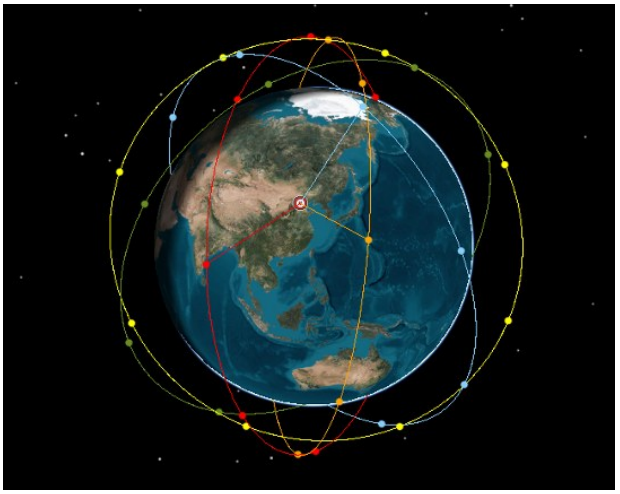

图 12　地面站在北京的星座场景

为了得到每颗卫星对地面站的访问时间段，下面从地面站角度对卫星星座进行可见性分析，如图 13、图 14 所示。地面站地理位置的不同会带来卫星星座访问时间图案的巨大差异。当地面站处于北极点时，由于每个轨道中的卫星是均匀分布的，且不受地球自转的影响，因此它们的访问周期完全一致。但由于初始位置不同，访问时间有所偏差。当地面站位于北京时，受地球自转的影响，每颗卫星连接地面站的访问时间图案就会各不相同。一方面，在同一轨道内，地面站会经历远离、靠近以及再远离卫星轨道的过程，因此同一轨道内的卫星之间存在访问差异；另一方面，对于处在不同轨道上的卫星，由于卫星轨道位置与运行方向的差异性，不同轨道上的卫星访问时间图案也存在差异。

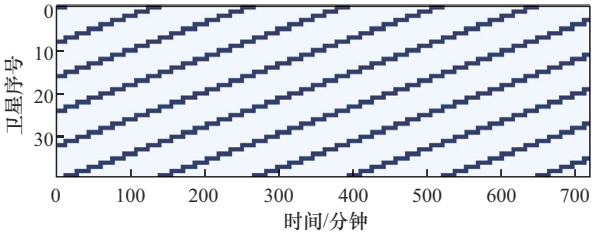

图 13　地面站在北极点的星座可见性分析

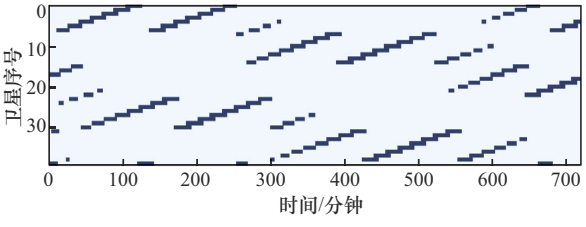

图 14　地面站在北京的星座可见性分析

在以上两种场景下对传统的联邦学习方法进行仿真，卫星与地面站建立连接期间，接收到全局模型后会在本地训练 5 次[15]，由于本地训练时间小于卫星的地面可见时间，训练结束后会立即将更新后的模型参数上传。图 15、图 16 为不同数据分布情况下 MLP 模型采用不同训练方法的模型准确度收敛曲线。由图 15、图 16 可知，不管在何种数据分布情况下，地面站的位置都会影响卫星与地面站之间的可见频次，进而大幅影响模型收敛速度，因此地面站在北京时的模型收敛速度要小于地面站在北极点时的收敛速度。然而，基于区块链的安全高效训练方法能够脱离地面站的约束，有效缩短模型收敛时延，相比其他两种模型聚合方式能实现更快的模型训练。另外，对于同一种模型训练方法，Non-IID 的数据分布会延缓智能模型的训练收敛过程。

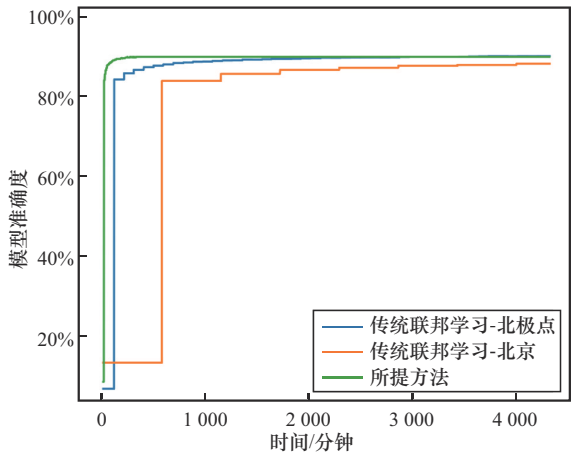

图 15　数据分布为 IID 时不同训练方法的模型准确度

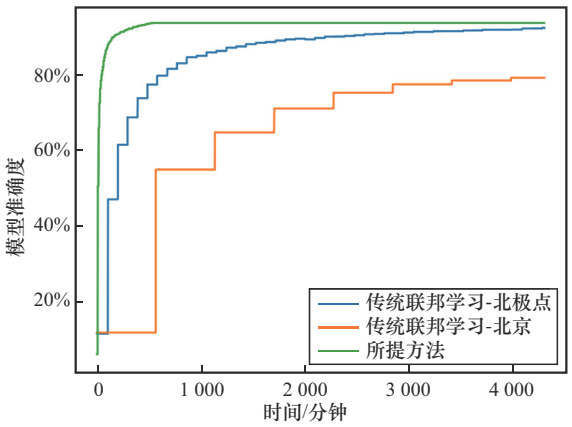

图 16　数据分布为 Non-IID 时不同训练方法的模型准确度

图 17 展示了在不同训练方法下，达到不同模型准确度阈值所需的训练时间。由图 17 可知，在相同训练方法、相同准确度下，训练在数据分布 IID 时的耗时比 Non-IID 更短；在 IID 和 Non-IID 数据分布下，所提方法比两种传统联邦学习方法的训练效率更高。这是因为虽然区块链带来了更复杂的通信和计算过程，但相比于传统联邦学习中地面站不稳定可见性所需的额外等待时间，引入区块链技术的时间开销非常小。

（3）安全隐私仿真

差分隐私通过引入扰动或者噪声对模型参数进行加密，使得攻击者无法在模型传播时截取到参数信息，或者从模型参数反推出样本信息。图 18 针对高斯噪声和拉普拉斯噪声两种差分隐私机制，考虑不同的隐私预算 ε，得到 MLP 在 IID 数据分布下进行联邦学习训练的准确度仿真结果。由图 18 可知，差分隐私的引入会带来性能的

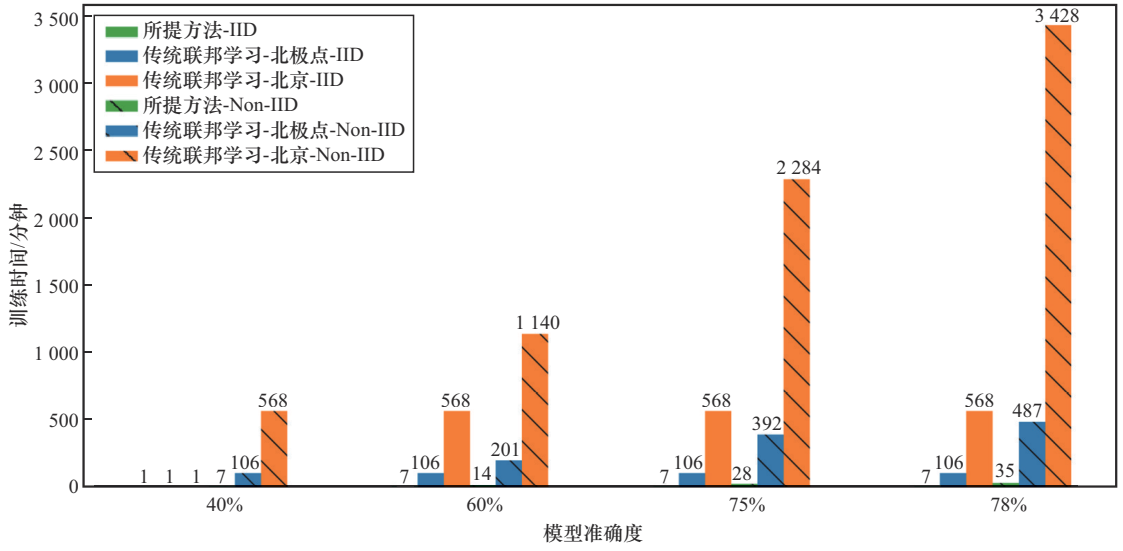

图 17　不同训练方法达到不同模型准确度阈值所需的训练时间

损失，隐私预算和差分噪声类型不同，性能损失的大小也会变化。一方面，隐私预算ε越大，即对模型数据变化的容忍度越高，所加噪声的方差就会越小，对模型准确度的影响就会越低，反之隐私预算ε较小时，如图中$\varepsilon=1$的情况，模型准确度严重降低；另一方面，在相同隐私预算的情况下，高斯噪声对模型精度的影响要更小一些。

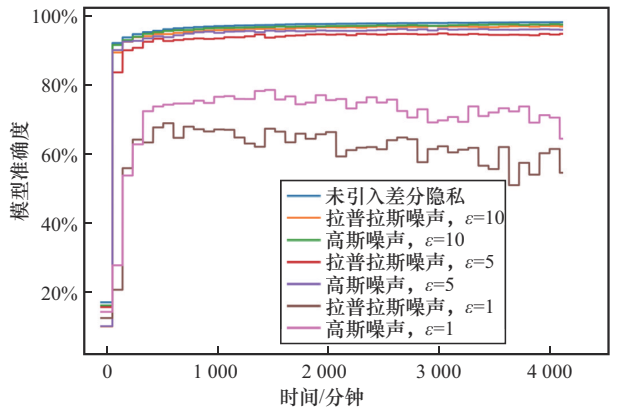

图 18　差分隐私机制对联邦学习模型准确度的影响

图 19 为不同恶意节点占比下有无参数评估的模型准确度对比。图 19 中虚线为不同恶意节点占比下无参数评估的模型准确度，实线为不同恶意节点占比下有参数评估的模型准确度。一方面，在没有参数评估的情况下，恶意节点的占比越大，模型准确度性能损失越严重；另一方面，参数评估机制能够有效减弱恶意节点带来的影响，在恶意节点占比为 10% 和 20% 的情况下，参数评估能够有效消除恶意节点带来的性能损失，但是当恶意节点占比达到 30% 时，参数评估机制只能带来有限的性能提升。

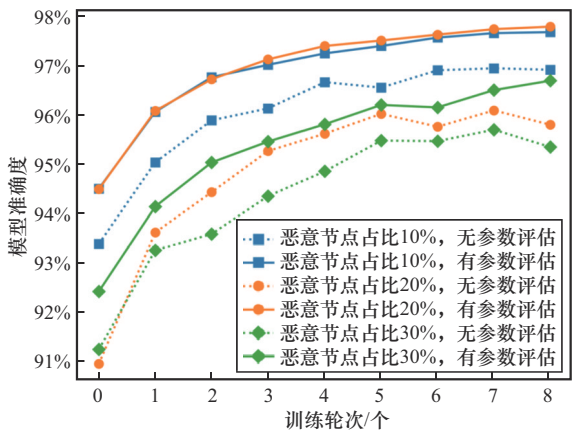

图 19　不同恶意节点占比下有无参数评估的模型准确度对比

4　结束语

本文研究了天基信息网络的智能模型分布式训练技术。首先建立了系统模型，设计了天基信息网络基于区块链的联邦学习架构，包含卫星星座层、联邦学习层以及区块链层，并给出了时延模型，包含通信时延和计算时延；其次提出了基于区块链的智能模型安全高效训练方法，详细介绍了方法的总体流程，通过差分隐私机制、参数评估方法以及区块链的去中心化特性有效应对隐私泄露、中毒攻击以及单点故障威胁，并采用基于时延最小的模型聚合方法，有效加速了模型训练过程；最后以手写数字图像分类任务为例，在 Walker Delta 星座场景中进行了仿真实验，从模型收敛性、模型训练时延以及安全隐私角度对所提方法进行性能分析。结果表明，所提方法能够让不同结构的智能模型有效收敛，相对于传统的联邦学习聚合方法能够有效缩短模型训练时间，并且在保障模型性能的情况下通过差分隐私和参数评估有效应对隐私泄露威胁与中毒攻击威胁。

参考文献：

[1] CENTENARO M, COSTA C E, GRANELLI F, et al. A survey on technologies, standards and open challenges in satellite IoT[J]. IEEE Communications Surveys & Tutorials, 2021, 23(3): 1693-1720.

[2] ZHANG J X, ZHANG X, WANG P, et al. Double-edge intelligent integrated satellite terrestrial networks[J]. China Communications, 2020, 17(9): 128-146.

[3] KONE VCNÝ J, BRENDAN MCMAHAN H, YU F X, et al. Federated learning: strategies for improving communication efficiency [J]. ArXiv e-Prints, 2016: arXiv: 1610.05492.

[4] MCMAHAN B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[C]// Proceedings of the 20th International Conference on Artificial Intelligence and Statistics. [S.l.:s.n.], 2017: 1273-1282.

[5] CHEN H, XIAO M, PANG Z B. Satellite-based computing networks with federated learning[J]. IEEE Wireless Communications, 2022, 29(1): 78-84.

[6] SALIM S, MOUSTAFA N, HASSANIAN M, et al. Deep-federated-learning-based threat detection model for extreme satellite communications[J]. IEEE Internet of Things Journal, 2024, 11 (3): 3853-3867.

[7] MOUSTAFA N, KHAN I A, HASSANIN M, et al. DFSat: deep federated learning for identifying cyber threats in IoT-based satellite networks[J]. IEEE Transactions on Industrial Informatics, 2022 (99): 1-8.

[8] LI K, ZHOU H C, TU Z, et al. Distributed network intrusion detection system in satellite-terrestrial integrated networks using federated learning[J]. IEEE Access, 2020, 8: 214852-214865.

[9] RAZMI N, MATTHIESEN B, DEKORSY A, et al. Ground-assisted federated learning in LEO satellite constellations[J]. IEEE Wireless Communications Letters, 2022, 11(4): 717-721.

[10] RAZMI N, MATTHIESEN B, DEKORSY A, et al. On-board federated learning for dense LEO constellations[C]//Proceedings of the ICC 2022 - IEEE International Conference on Communications. Piscataway: IEEE Press, 2022: 4715-4720.

[11] RAZMI N, MATTHIESEN B, DEKORSY A, et al. Scheduling for ground-assisted federated learning in LEO satellite constellations [C]//Proceedings of the 2022 30th European Signal Processing Conference (EUSIPCO). Piscataway: IEEE Press, 2022: 1102-1106.

[12] FREDRIKSON M, JHA S, RISTENPART T. Model inversion attacks that exploit confidence information and basic countermeasures[C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2015: 1322-1333.

[13] YANG Z Q, ZHANG J Y, CHANG E C, et al. Neural network inversion in adversarial setting *via* background knowledge alignment [C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2019: 225-240.

[14] FREDRIKSON M, LANTZ E, JHA S, et al. Privacy in pharmacogenetics: an end-to-end case study of personalized warfarin dosing [J]. Proceedings of the USENIX Security Symposium UNIX Security Symposium, 2014: 17-32.

[15] LU Y L, HUANG X H, ZHANG K, et al. Blockchain and federated learning for 5G beyond[J]. IEEE Network, 2021, 35(1): 219-225.

[16] POKHREL S R. Blockchain brings trust to collaborative drones and LEO satellites: an intelligent decentralized learning in the space[J]. IEEE Sensors Journal, 2021, 21(22): 25331-25339.

[17] QU Y Y, UDDIN M P, GAN C Q, et al. Blockchain-enabled federated learning: a survey[J]. ACM Computing Surveys, 2022, 55(4): 1-35.

[18] NGUYEN D C, DING M, PHAM Q V, et al. Federated learning meets blockchain in edge computing: opportunities and challenges [J]. IEEE Internet of Things Journal, 2021, 8(16): 12806-12825.

[19] DENG L. The MNIST database of handwritten digit images for machine learning research best of the web[J]. IEEE Signal Processing Magazine, 2012, 29(6): 141-142.

[20] LECUN Y, BOTTOU L, BENGIO Y, et al. Gradient-based learning applied to document recognition[J]. Proceedings of the IEEE, 1998, 86(11): 2278-2324.

[21] KRIZHEVSKY A, SUTSKEVER I, HINTON G E. ImageNet classification with deep convolutional neural networks[J]. Communications of the ACM, 2017, 60(6): 84-90.

[作者简介]

栗渊钧（1999– ），男，北京理工大学信息与电子学院硕士生，主要研究方向为边缘智能计算。

杨德伟（1979– ），男，博士，北京理工大学信息与电子学院副教授，主要研究方向为卫星通信、边缘智能计算。

李佳宁（2000– ），女，北京理工大学信息与电子学院硕士生，主要研究方向为边缘智能计算。

冯笑（1989– ），男，硕士，中国电子科技集团公司第十五研究所高级工程师，主要研究方向为计算机体系架构、边缘智能计算。