文章编号： 1671-7449(2024)04-0345-09

基于声誉机制的区块链赋能多无人机系统联邦学习研究

郭禹江，张志才*

（山西大学 物理电子工程学院， 山西 太原 030006）

摘　要： 配置探测器的无人机可用于空气质量预测等应用。联邦学习赋能多无人机系统面临单点故障、恶意攻击、难实现公平激励等挑战。本文研究一种基于声誉机制的区块链赋能多无人机系统联邦学习方案，通过基于区块链的智能合约自动执行任务，以声誉值评估局部模型质量，以声誉阈值为基准识别并移除恶意无人机。根据声誉值将全局模型进行稀疏化，实现公平分配模型利润，综合考虑声誉值与数据量使诚实无人机获得与成本相对应的奖励。仿真通过MNIST数据集验证了本文提出的算法精度高于FedAVG算法，能在恶意无人机占比不同的情况下将其识别并驱逐，实现了模型利润与总预算的公平分配。

关键词： 声誉值；无人机；联邦学习；智能合约；区块链

中图分类号： TP393　　**文献标识码：** A　　**doi:** 10.3969/j.issn.1671-7449.2024045

引用格式： 郭禹江，张志才．基于声誉机制的区块链赋能多无人机系统联邦学习研究[J]．测试技术学报，2024，38(4)：345-353.

GUO Yujiang，ZHANG Zhicai．Research on federated learning of blockchain enabled multi UAV system based on reputation mechanism[J]．Journal of Test and Measurement Technology，2024，38(4)：345-353.

Research on Federated Learning of Blockchain Enabled Multi UAV System Based on Reputation Mechanism

GUO Yujiang，ZHANG Zhicai*

（College of Physical and Electronic Engineering，Shanxi University，Taiyuan 030006，China）

Abstract： Drones equipped with detectors can be used for applications such as air quality prediction. Federated learning empowers multi-drone systems to face challenges such as single point of failure，malicious attacks，and difficulty in achieving fair incentives. This article studies a reputation based blockchain enabled federated learning scheme for multi-drone systems. By automatically executing tasks through blockchain-based smart contracts，local model quality is evaluated based on reputation values，and malicious drones are identified and removed based on reputation thresholds. Sparse the global model based on reputation value to achieve fair distribution of model profits，and comprehensively consider reputation value and data volume to reward honest drones with corresponding costs. The simulation verified through the MNIST dataset that the algorithm proposed in this paper has higher accuracy than the FedAVG algo-

收稿日期： 2023-07-29

基金项目： 山西省基础研究计划自然科学研究面上资助项目(202103021224024)；山西省基础研究计划青年科学研究资助项目(20210302123021)；山西省重点研发计划资助项目(202202020101004)

作者简介： 郭禹江(1998－)，男，硕士生，主要从事联邦学习激励机制研究。E-mail:1370289349@qq.com。

***通信作者：** 张志才(1982－)，男，博士，讲师，硕士生导师，主要从事算网融合领域研究。E-mail:zzcai@sxu.edu.cn。

rithm, and can identify and expel malicious drones under different proportions, achieving a fair distribution of model profits and total budget.

Key words: reputation value; unmanned aerial vehicles; federated learning; smart contracts; blockchain

0 引 言

Liu 等[1]提出一种基于联邦学习的无人机群空气质量感知框架。Zhang 等[2]考提出一种增强的 actor-critic 算法，有效优化了频谱资源分配。Zhang 等[3]通过优化无人机轨迹提高能源效率。Fu 等[4]通过优化车辆调度以优化资源分配。武文涛等[5]提出一种基于联邦学习的智能网联车驾驶策略优化方案。文献[1—5]介绍了基于联邦学习的多无人机协同机制。

Yuan 等[6]介绍了区块链与物联网技术结合在智能设备领域的潜能。Upadhyay 等[7]介绍了区块链与智能合约技术结合的优势。Wang 等[8]设计了一种基于局部差分隐私的算法。Xu 等[9]提出一个基于区块链的联邦学习框架。Zheng 等[10]提出一种新的区块链安全协议。文献[6—10]介绍了区块链在隐私保护方面的有效性。

Kang 等[11]提出一种将声誉与契约理论结合的激励机制。Yi 等[12]提出一种基于 Stackelberg 博弈的激励机制。本文研究一种基于声誉机制的区块链赋能多无人机系统联邦学习框架，主要贡献在于：

1）通过区块链防止全局模型被破坏，使用智能合约，以透明、可追溯、不可篡改的方式来执行模型训练任务。

2）引入基于局部模型质量的声誉机制，以声誉值为权重聚合全局模型。以声誉阈值为基准驱逐恶意无人机，对贡献不同的无人机公平分配模型利润。

3）考虑无人机的采集，计算与通信成本，综合考虑数据量和声誉值分配奖励。

4）基于 MNIST 数据集进行仿真实验，结果表明，本文提出的基于声誉的联邦学习算法精度高于 FedAVG 算法，在恶意无人机占比不同的情况下能将其识别并驱逐，同时实现了模型利润与总预算的公平分配。

1 系统模型

1.1 网络模型

图 1 为基于声誉机制的区块链赋能多无人机系统联邦学习模型，由任务发布者、N 架配备传感器与处理器的无人机、M 台配备边缘计算设备（Edge Computer Device，ECD）的基站、区块链四部分组成。$N=\{1,2,\cdots,N\}$，$M=\{1,2,\cdots,M\}$。无人机配备传感器、全球定位系统（Global Position System，GPS）、处理器、通信模块。无人机通过 GPS 沿预定义轨迹移动感知采集数据，并使用处理器计算局部模型更新，将模型参数传输给邻近的基站。

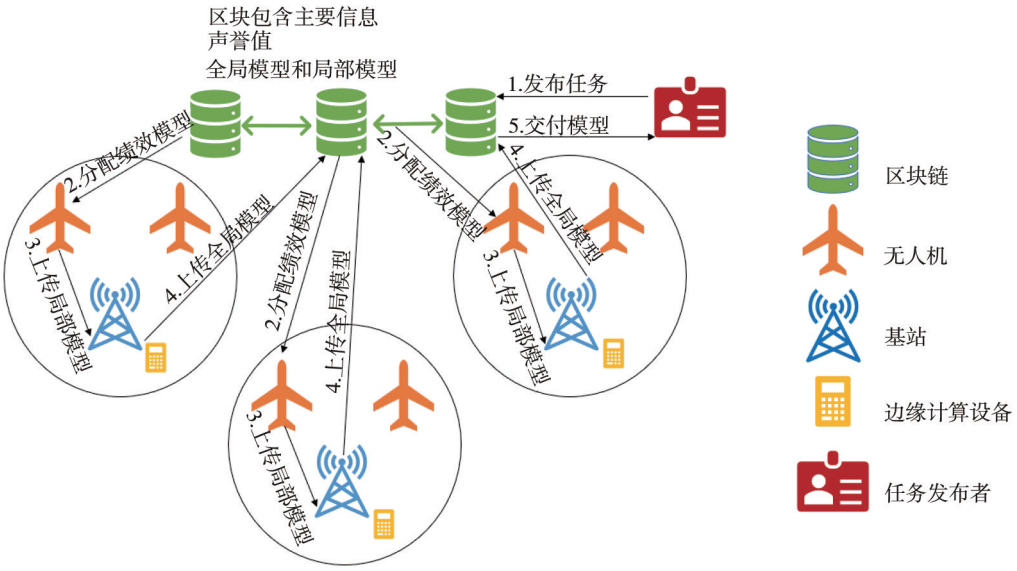


图 1 基于声誉机制的区块链赋能多无人机系统联邦学习

Fig. 1 Reputation based blockchain empowered multi uav system federated learning

联邦学习任务通过基于区块链的智能合约承担。N架无人机将局部更新传输给基站。M台基站收集局部模型参数，并评估局部模型质量计算声誉值聚合全局模型。

1.2　基于声誉机制的联邦学习模型

区域监测任务需要大量的新鲜数据，因此调用一组无人机应用联邦学习协同训练全局卷积神经网络（CNN）模型。

$$minF(W)=\sum_{i=1}^{N}p_nF_n(w), \tag{1a}$$

$$p_n\geqslant 0,\ \sum_{n=1}^{N}p_n=1, \tag{1b}$$

$$\Delta w_n^{(t)}:=\nabla F_n(w_n^{(t-1)}), \tag{2}$$

$$\Delta w^{(t)}=\sum_{n=1}^{N}p_n\Delta w_n^{(t)}。 \tag{3}$$

联邦学习任务目标是最小化全局损失函数$F(W)$。N架无人机合作训练全局模型$\Delta w^{(t)}$，优化局部参数$\Delta w_n^{(t)}$，目标最小化局部损失函数$F_n(w)$。p_n代表各无人机的权重。任务分为以下几阶段：

1）初始化全局模型：任务发布者将初始全局模型与任务奖励提交给区块链，通过智能合约分发给N架无人机。

2）无人机端局部更新：无人机收集数据并计算局部模型梯度更新。

3）上传局部更新：无人机将局部更新传输到基站，基站聚合全局模型。

4）全局模型聚合：M台基站测试模型质量并更新声誉值，将全局模型和所有局部模型参数以及声誉值发布到区块链。

1.3　基于区块链的智能合约模型

1）任务初始化合约：初始化全局模型参数。

2）成员选择合约：选择声誉良好的无人机参与任务，移除低于声誉阈值的无人机。

3）联邦学习合约：

a）局部模型上传，无人机训练模型后将模型参数和贡献的数据量上传到邻近基站。

b）局部模型下载，基站收集并共享局部模型。

c）模型质量测试，基站进行局部模型质量测试计算声誉值。

d）全局模型聚合，基站以声誉值为权重聚合全局模型。

e）信息上传区块链，基站将全局模型、所有局部模型和声誉值打包到新的区块中。

f）分配绩效模型，无人机通过区块链接收绩效模型。

4）声誉更新合约，基站计算无人机的声誉值。

5）奖励分配合约，衡量无人机贡献的数据量与声誉值通过区块链分配奖励。

6）成员查询合约，通过区块记录查询无人机的历史声誉。

1.4　无人机成本模型

C_n表示贡献单位数据量的成本。能量成本分为传感成本，计算成本与通信成本，时间成本分为传感时间，计算时间与通信时间。无人机n在目标区域按预定义轨迹移动采集数据，区域中均匀部署若干节点，目标是覆盖节点收集数据。

无人机n在目标区域通过传感器收集数据，历经的总距离为L_n，平均速度为v_n，传感总持续时间

$$\tau_n^s=\frac{L_n}{v_n}。 \tag{4}$$

无人机n推进功率为P_n，覆盖传感距离所消耗的传感能量E_n^s为

$$E_n^s=\frac{L_n}{v_n}P_n, \tag{5a}$$

$$P_n=c_{n1}v_n^3+\frac{c_{n2}}{v_n}, \tag{5b}$$

$$\alpha_n=\frac{P_nl_n}{v_n}, \tag{5c}$$

式中：c_{n1}为平衡寄生阻力的功率；c_{n2}为平衡空气阻力所需功率；l_n为历经单位距离；α_n为覆盖节点感知的单位数据成本。

无人机用采集的数据训练局部模型。无人机n的局部计算时间

$$\tau_n^c=\frac{Z_nD_n\log_2(1/A*)}{f_n}。 \tag{6}$$

无人机n的计算能量消耗

$$E_n^c=KZ_nD_nV\log_2(1/A*)f_n^2, \tag{7a}$$

$$\beta_n=KZ_nd_nV\log_2(1/A*)f_n^2, \tag{7b}$$

式中：K为有效开关电容；Z_n为计算样本数据的每比特周期数；D_n为样本的数量；d_n为单位数据样本；$A*$为局部最佳模型精度；$\log_2(1/A*)$为达到局部精度所需迭代次数的下限；f_n为n每秒CPU

周期数；β_n为局部模型训练的单位数据成本。

无人机n的上传速率为其发射功率ρ_n和比例因子χ_n的乘积，χ_n包括带宽分配和信道增益。无人机n上传大小为H的参数更新时间

$$\tau_n^T=\frac{H}{\chi_n\rho_n}。\tag{8}$$

给定模型更新固定维度，无论全局迭代次数或收集的数据量如何，局部模型更新上传大小恒定，无人机n传输能量消耗

$$E_n^T=\tau_n^T\rho_n=\gamma。\tag{9}$$

由于无人机更新的局部模型参数大小恒定，因此通信成本可视为固定值，γ为无人机传输局部模型的通信成本。

2 基于声誉机制的公平可靠联邦学习框架

2.1 基于模型质量的声誉评估机制

基站之间通过有线链路链接共享局部模型。基站进行模型质量测试并将声誉值上传到区块链。通过衡量局部模型参数与全局模型参数的余弦相似性来评估局部模型的质量。余弦相似性越高，证明该局部模型质量越高，则声誉值越高。为减轻随机模型初始化产生的噪声影响，综合当前和前一轮的声誉，使声誉值较为平滑地更新。

$$\tilde{\lambda}_n^{(t)}=\cos(\Delta w_g^{(t)},\Delta w_n^{(t)}),\tag{10a}$$

$$\hat{\lambda}_n^{(t)}=\xi\tilde{\lambda}_n^{(t-1)}+(1-\xi)\tilde{\lambda}_n^{(t)},\tag{10b}$$

$$\lambda_n^{(t)}=\frac{\hat{\lambda}_n^{(t)}}{\sum_{i=1}^{N}\hat{\lambda}_i^{(t)}},\tag{10c}$$

$$\cos(x,y)=\frac{\langle x,y\rangle}{\|x\|\times\|y\|},\tag{10d}$$

式中：$\tilde{\lambda}_n^{(t)}$为无人机n本轮的声誉值，通过全局模型梯度$\Delta w_g^{(t)}$与n本轮局部梯度$\Delta w_n^{(t)}$的余弦相似性评估。ξ是可调节权重系数，用来调节前一轮声誉值$\tilde{\lambda}_n^{(t-1)}$与本轮声誉值$\tilde{\lambda}_n^{(t)}$的权重，$\hat{\lambda}_{(n)}^{(t)}$代表本轮综合声誉值。为保证模型利润分配的公平性，需要将所有无人机声誉值进行归一化，将无人机n的综合声誉值除以综合声誉值的总和，确保声誉值的总和为1，$\lambda_n^{(t)}$为本轮最终声誉值。

使用声誉阈值σ衡量恶意无人机。每轮全局迭代中，将声誉小于σ的无人机驱逐，本文将声誉阈值设置为$\sigma=1/(2N)$，N为参与训练的无人机总数。

2.2 基于声誉加权的模型聚合机制

基站持有测试数据集，将收集到的局部模型进行质量测试，将声誉值作为全局模型聚合的权重。由于恶意无人机的声誉值较低，在聚合时权重较低，避免了恶意无人机对全局模型的破坏。

$$\Delta w_g^{(t)}=\frac{\mu\sum_{n\in R}\lambda_n^{(t-1)}\Delta w_n^{(t)}}{\|\Delta w_n^{(t)}\|},\tag{11a}$$

$$\Delta w_n^{(t)}=\nabla F_n(w_n^{(t-1)})。\tag{11b}$$

在第t轮全局迭代中，$\Delta w_g^{(t)}$为全局模型更新，$w_n^{(t-1)}$为无人机n前一轮局部模型，$\Delta w_n^{(t)}$为无人机n上传的局部更新，$\lambda_n^{(t-1)}$为无人机n前一轮的最终声誉值，R为声誉高于阈值的无人机集合，μ为防止梯度爆炸归一化系数。恶意无人机类型包括靶向投毒，非靶向投毒与搭便车攻击。靶向投毒指修改标签攻击。非靶向投毒包括篡改梯度符号攻击、放缩梯度攻击、反转梯度值攻击。本文考虑了5种恶意攻击评估所提方案的有效性。

1）修改标签攻击：将特定标签值转换为另一个标签值，以改变模型的训练结果。本文将标签2转换为4，实现修改标签攻击。

2）篡改梯度符号攻击：通过随机选择[－1，1]中的元素，将其与梯度的对应元素逐元素相乘，实现篡改梯度符号攻击。

3）放缩梯度攻击：通过生成与梯度形状相同的随机张量，经放大因子放缩，然后减去偏移量生成扰动项。将扰动项与梯度的对应元素相乘，实现放缩梯度攻击。

4）反转梯度值攻击：通过生成与梯度形状相同的随机张量，随机选择位置，将对应位置上的梯度元素加一个微小值，然后取倒数实现反转梯度值攻击。

5）搭便车攻击：通过随机生成与梯度形状相同的随机张量，其中每个元素的取值范围在[－1，1]之间，实现搭便车攻击。

为应对以上恶意攻击引入声誉值，由于恶意攻击者局部梯度更新与真实值相差较大，则余弦相似性较低，聚合时的权重较低，使诚实无人机的局部更新占主导地位。应对搭便车攻击，则通过将全局模型利用绩效值稀疏化，使搭便车无人机无法免费获利。

2.3 基于声誉的绩效模型分配机制

基站根据声誉值确定无人机的绩效模型。首

先计算无人机n的声誉值相对于最大声誉值的比例，即绩效值p_n。将绩效值为1的无人机分配完整的全局模型，其他按照绩效值p_n进行相应稀疏化。

$$\Delta w_{*n}^{(t)}=\text{sparsify}(\Delta w_g^{(t)},p_n)-\lambda_n^{(t-1)}\Delta w_n^{(t)},\tag{12a}$$

$$p_n=\frac{\lambda_n^{(t)}\phi}{\max\limits_{i\in R}\lambda_i^{(t)}},\tag{12b}$$

$$w_n^{(t+1)}=w_n^{(t)}+\Delta w_n^{(t)}+\Delta w_{*n}^{(t)},\tag{12c}$$

式中：$w_n^{(t+1)}$为无人机n的下一轮的局部模型；$w_n^{(t)}$为n本轮局部模型；$\Delta w_{*n}^{(t)}$为n的绩效模型；$\Delta w_n^{(t)}$为n的局部更新；p_n是n的绩效值，代表n下载的参数的数量；ϕ为全局模型参数的总数量；$\lambda_n^{(t-1)}$为n前一轮的最终声誉值；$\tilde{\lambda}_n^{(t)}$为n本轮的最终声誉值；$\max\limits_{i\in R}\lambda_i^{(t)}$为本轮最高的最终声誉值。计算出$p_n$后，基站首先根据$p_n$值只保留梯度的最大值逐渐稀疏梯度向量，生成稀疏化后的全局模型，然后从中删除n自身的梯度。通过稀疏梯度向量逐渐减少全局模型的信息，使N架无人机根据自身局部模型质量获得相应的绩效模型。

2.4　基于声誉加权的预算分配机制

由于对全局模型真正有贡献的数据量由诚实的无人机提供，恶意无人机的数据对全局模型有破坏性，使用声誉值作为分配奖励的权重。基于此n的效用函数表示为

$$u_n^{(t)}=\frac{\lambda_n^{(t)}k_n}{\sum\limits_{i=1}^{N}\lambda_i^{(t)}k_i}R-S_n,\tag{13}$$

式中：R为学习任务的总预算；$\lambda_n^{(t)}$为无人机n本轮的最终声誉值；k_n为无人机n贡献的数据量；S_n为无人机n数据总成本，包括传感成本，计算成本与通信成本。由于给定模型更新的固定维度，因此通信成本固定。

$$S_n=k_nC_n+\gamma,\tag{14a}$$

$$C_n=\alpha_n+\beta_n,\tag{14b}$$

式中：C_n为训练模型时n的单位成本；k_n为n贡献的数据量；α_n为n收集数据的单位感知成本；β_n为n局部训练的单位计算成本；γ为n的通信成本。

2.5　基于声誉的可靠联邦学习算法

1）输入：N架无人机；初始全局模型参数$w_g^{(t)}$，可调节权重系数ξ；声誉阈值σ；梯度归一化常数μ;任务初始化合约；成员选择合约；联邦学习合约；声誉更新合约；奖励分配合约；成员查询合约；

2）输出：无人机n第t轮最终声誉值$\lambda_n^{(t)}$,绩效值p_n；局部更新$\Delta w_n^{(t)}$；绩效模型$\Delta w_{*n}^{(t)}$；效用函数$u_n^{(t)}$；无人机n的下一轮的局部模型$w_n^{(t+1)}$；

3）全局模型聚合：

① for无人机$n\in R$ do；

② 根据式(2)无人机n上传自身更新的局部模型到基站；

③ 各基站收集无人机n的局部模型进行质量测试；

④ 执行声誉更新合约，根据式(10a)～(10d)计算无人机n本轮的最终声誉值；

⑤ if $\lambda_n^{(t)}<\sigma$ then；

⑥ 执行成员选择合约，根据$R=\{\lambda_n^{(t)}\geqslant\sigma\}$移除低于声誉阈值的无人机；

⑦ end if；

⑧ 根据式(11a)使用声誉值加权聚合全局模型；

⑨ 基站将全局模型，各无人机的声誉值，局部模型均上传到区块链；

⑩ end for。

4）公平奖励分配

for 无人机$n\in R$ do；

5）绩效模型分配

① 根据式(12b)利用无人机的声誉比例值计算无人机n的绩效值；

② 根据式(12a)计算无人机n的绩效梯度值；

③ 无人机n通过区块链下载绩效梯度值$\Delta w_{*n}^{(t)}$，根据式(12c)与局部梯度整合；

6）总预算分配

① 根据式(14b)计算无人机n训练的数据单位成本；

② 根据式(14a)计算无人机n训练的数据总成本；

③ 根据式(13)由无人机n贡献的数据量与声誉值乘积所占比重计算无人机n的效用函数$u_n^{(t)}$；

④ 执行奖励分配合约，通过区块链将奖励$u_n^{(t)}$分配给无人机n；

⑤end for。

3　仿真结果与分析

3.1　仿真实验设置

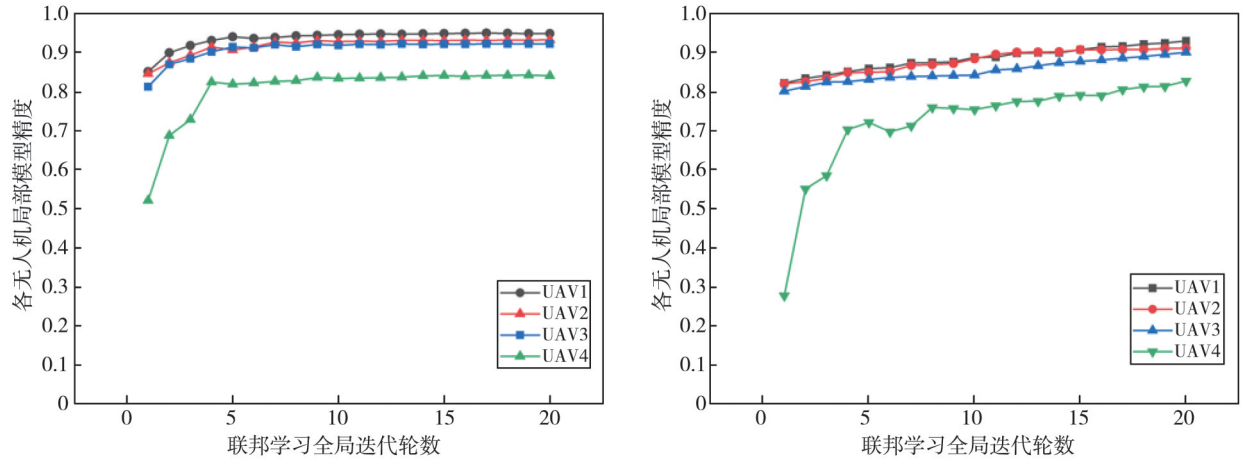
在仿真实验中，目标区域为圆形网络区域，

半径 r=500 m，区域内基站数量 M=3，无人机的数量 N=6。每台基站通信范围内包括 2 架无人机，无人机协同使用 MNIST 数据集进行手写数字分类。为体现各无人机的异质性，数据集按数据量大小不均匀地分成 6 份给无人机。4 架诚实无人机分别为 u_1，u_2，u_3，u_4，数据量分别设置为 2 400，1 400，800，200。2 架恶意无人机为 u_5，u_6，数据量均设置为 1 200，攻击类型相同，可分别设置为搭便车，靶向投毒与非靶向投毒。采用具有 2 个卷积层和 1 个全连接层的 CNN 模型对无人机收集的数据局部训练。声誉阈值 σ=1/(2N)=1/12，可调节权重系数 ξ=0.8，梯度归一化常数 μ=0.5，批次大小 B=64，学习率 η=0.12，折扣因子 γ=0.95、全局迭代轮数 T=20，局部迭代次数 E=100。仿真考虑了 4 种类型的无人机：诚实型、搭便车型、靶向投毒型、非靶向投毒型。靶向投毒指修改标签攻击；非靶向投毒包括篡改梯度符号攻击、放缩梯度攻击、反转梯度值攻击。

3.2 实验结果分析

3.2.1 基于声誉的可靠联邦学习精度分析

实验评估了本文基于声誉的联邦学习算法与 FedAVG 算法在存在恶意节点的情况下诚实无人机所能达到的精度性能，以搭便车攻击为例。由于搭便车无人机并未真正计算梯度更新，因此精度忽略。图 3 显示了两种算法在受到搭便车攻击时，使用 MNIST 数据集的精度性能。



(a) 基于声誉的可靠联邦学习算法精度图　(b) FedAVG算法精度图

图 2 算法精度性能比较

Fig. 2 Comparison of algorithm accuracy performance

图 2(a)中 u_1，u_2，u_3，u_4 精度分别达到 95%，93%，92%，84%，平均测试精度为 91.00%，图 2(b)中 u_1，u_2，u_3，u_4 的精度分别达到了 91%，90%，87%，75%，平均测试精度为 85.75%，图 2 说明本文基于声誉的可靠联邦学习算法存在恶意无人机参与的情况下比 FedAVG 算法精度更高。

3.2.2 驱逐恶意无人机的有效性分析

实验评估了基于声誉的可靠联邦学习算法在识别和驱逐 5 种恶意无人机方面的有效性，如图 3 所示。

在图 3(a) 中，u_1，u_2，u_3，u_4 的声誉基本保持稳定，而搭便车无人机 u_5，u_6 的声誉值迅速下降到声誉阈值 σ 以下第 5 轮被移除。在图 3(b) 中，u_1，u_2，u_3，u_4 的声誉值缓慢上升，在第 15 轮时基本稳定，修改标签无人机 u_5，u_6 的声誉值在前 10 轮内下降缓慢，在第 13 轮低于 σ 后被移除。在图 3(c) 中，u_1，u_2，u_3，u_4 的声誉值基本保持稳定，放缩梯度攻击无人机 u_5，u_6 的声誉值迅速下降到 σ 以下，在第 5 轮被移除。在图 3(d)中，u_1，u_2，u_3，u_4 的声誉基本保持稳定，篡改梯度符号攻击无人机 u_5，u_6 的声誉值迅速下降到 σ 以下，在第 5 轮被移除。在图 3(e) 中，u_1，u_2，u_3，u_4 的声誉基本保持稳定，反转梯度值攻击无人机 u_5，u_6 的声誉值迅速下降到 σ 以下，在第 5 轮被移除。图 3 说明本文提出的方案能有效识别并清除恶意攻击无人机。

3.2.3 绩效模型与总预算分配公平性分析

实验评估了基于声誉的可靠联邦学习算法在奖励分配方面的公平性，如图 4 所示。以搭便车攻击为例。

在图 4(a) 中，绩效值为 1 的无人机 u_1 获得完整的全局模型，u_2，u_3，u_4 按绩效值进行梯度稀疏化得到相应的绩效模型，而 2 架搭便车无人机 u_5，u_6 前 5 轮得到稀疏比例低于 20% 的绩效模型，

第5轮相对声誉迅速降低至0。图4(a)说明本文提出的方案实现了模型利润的公平分配。在图4(b)中，无人机u_1获得最多奖励，无人机u_2，u_3，u_4奖励依次减少，这是由于贡献的数据量越多，声誉值也越高，因此，在预算分配中获得的奖励就越多。而2架搭便车无人机并未真正进行数据采集与局部计算，因此，它的成本只限于通讯成本，远小于数据采集与计算成本。搭便车无人机u_5，u_6前5轮获得的奖励迅速降低并在第5轮被移除，图4(b)说明本文提出的方案实现了总预算的公平分配。

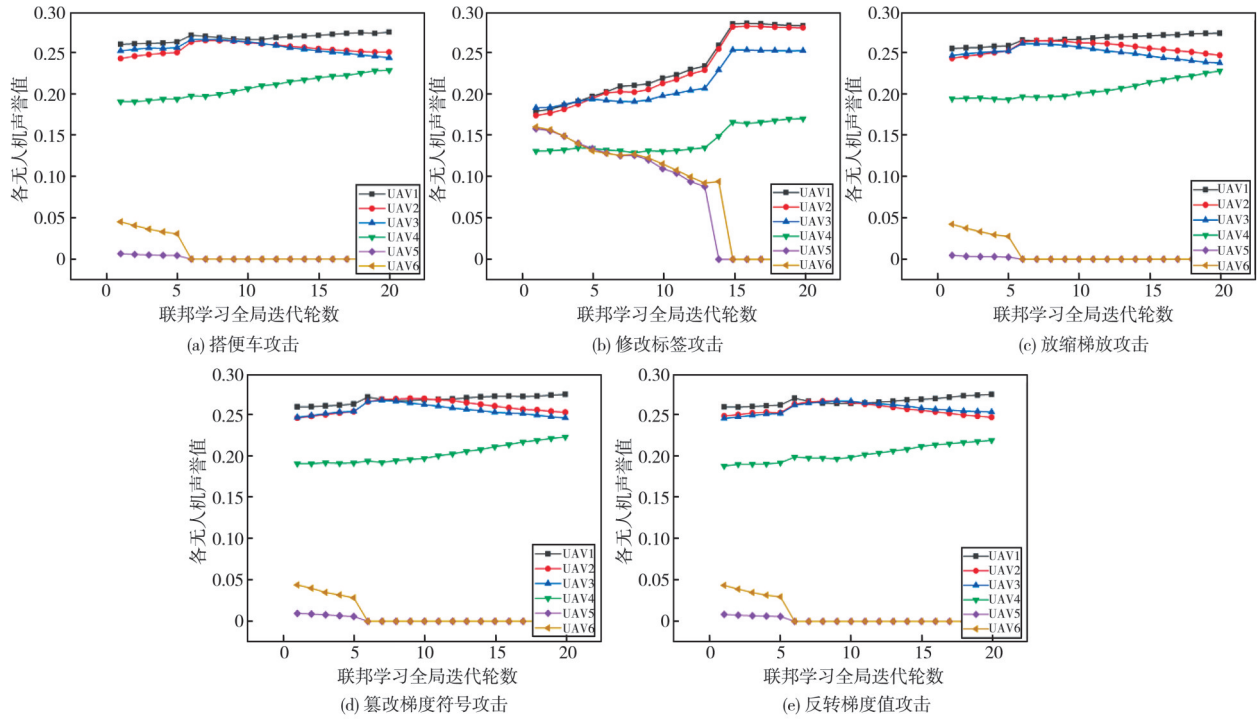


图3　受到5种恶意攻击的各无人机声誉值

Fig. 3　Reputation values of each drone under 5 types of malicious attacks

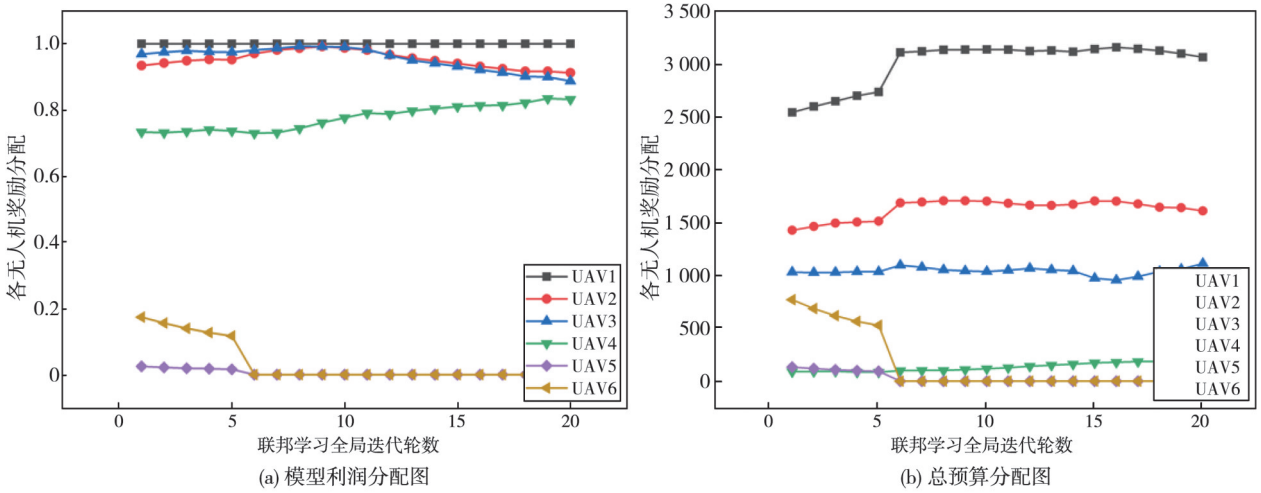
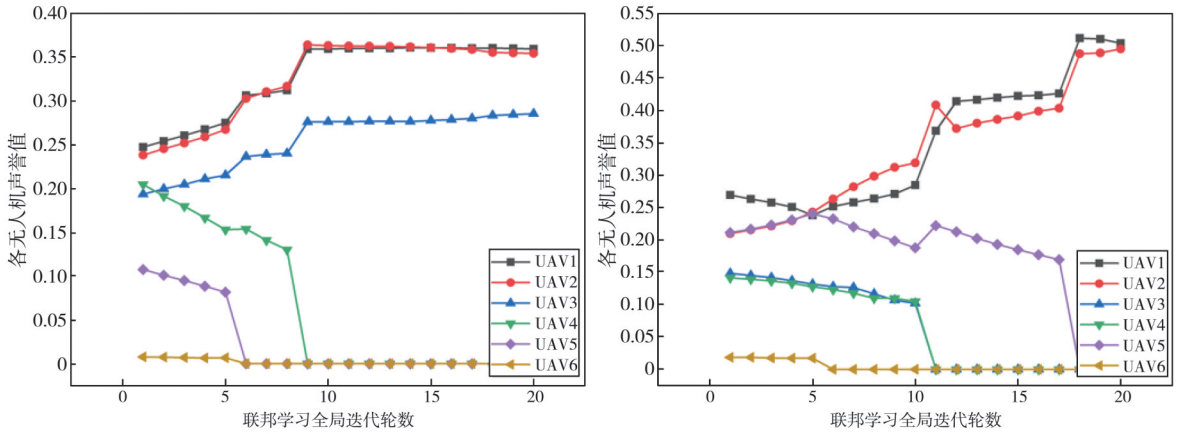


图4　在搭便车攻击下的各无人机奖励分配

Fig. 4　Reward allocation for each drone under free riding attack

3.2.4　恶意无人机占比不同时的算法分析

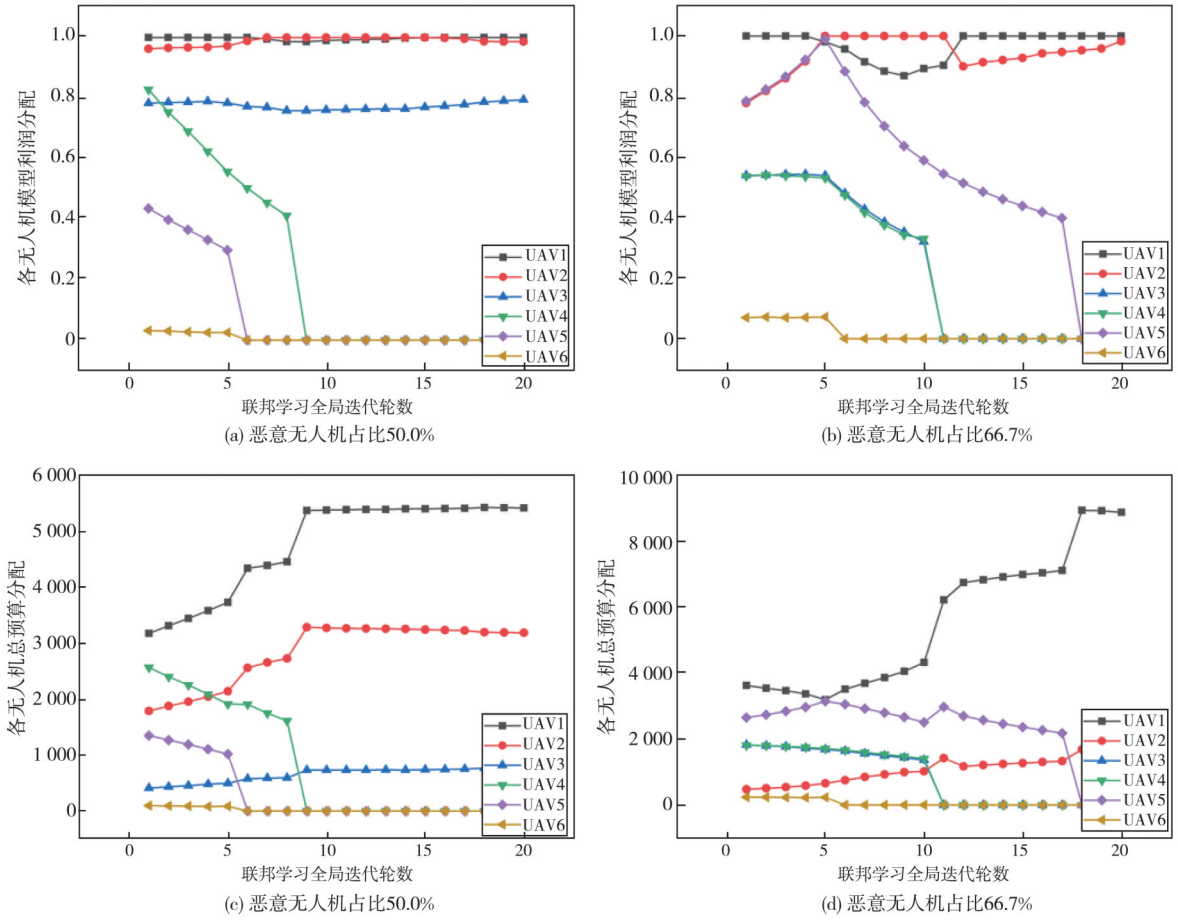
实验评估了基于声誉的联邦学习算法在恶意无人机占比50%与66.7%两种情况。第1种是3架诚实无人机u_1，u_2，u_3数据量分别为1 800，1 200，600；3架恶意无人机u_4，u_5，u_6数据量均为1 200，攻击类型相同。第2种是2架诚实无人机u_1，u_2数据量分别为1 800，600；4架恶意无人机u_3，u_4，u_5，u_6数据量均为1 200，攻击类型相同。以搭便车攻击为例，如图5与图6所示。



(a) 恶意无人机占比50.0% (b) 恶意无人机占比66.7%

图 5 恶意无人机不同占比时的各无人机声誉值

Fig. 5 Reputation values of malicious drones at different proportions



(a) 恶意无人机占比50.0% (b) 恶意无人机占比66.7%

(c) 恶意无人机占比50.0% (d) 恶意无人机占比66.7%

图 6 恶意无人机不同占比时的各无人机奖励分配

Fig. 6 Reward allocation for malicious drones with different proportions

在图5(a)中，u_1，u_2，u_3的声誉稳定增长在第10轮达到稳定。而搭便车无人机u_4，u_5，u_6的声誉值迅速下降到声誉阈值σ以下，u_4在第8轮被移除，u_5，u_6在第5轮被移除。在图5(b)中，u_1，u_2的声誉值均稳定增长，在第18轮达到稳定。搭便车无人机u_3，u_4，u_5，u_6的声誉值迅速下降到声誉阈值σ以下。u_3，u_4在第10轮被移除，u_5在第17轮被移除，u_6在第5轮被移除。图5说明，在恶意无人机占比与诚实无人机持平以及超过诚实无人机的情况下，本文提出方案能有效识别并清除恶意攻击无人机。

在图6(a)中，第1到第6轮u_1获得完整的全局模型，u_2，u_3得到相应的绩效模型，第7轮到第15轮u_2获得完整模型，u_1，u_3得到相应绩效模型，第16轮到第20轮u_1获得完整模型，u_2，u_3得到相应的绩效模型，

3架搭便车无人机获得的利润迅速降低，u_4在第8轮被移除，u_5，u_6第5轮被移除，之后模型利润均为0。在图6(b)中，第1轮到第4轮u_1获得完整的全局模型，u_2得到相应绩效模型，第5轮到第11轮u_2绩效值为1获得完整的全局模型，u_1得到绩效模型，第12轮到第20轮u_1获得完整模型，u_2得到相应绩效模型，4架搭便车无人机获得的利润迅速降低，u_3，u_4在第10轮被移除，u_5第17轮被移除，u_6第5轮被移除。图6(a)与图6(b)说明本文提出的方案在恶意无人机占比与诚实无人机持平以及超过诚实无人机的情况下实现了模型利润的公平分配。

在图6(c)中，诚实无人机u_1获得的奖励最多，u_2，u_3按贡献数据量排序奖励依次减少，这是由于贡献的数据量越多，声誉值也相对较高，因此在预算分配中获得的奖励就越多。3架搭便车无人机获得奖励迅速降低，u_4在第8轮被移除，u_5，u_6第5轮被移除，之后轮次奖励均为0。在图6(d)中，无人机u_1获得奖励最大，u_2奖励次之，4架搭便车无人机获得的奖励迅速降低，u_3，u_4在第10轮被移除，u_5第17轮被移除，u_6第5轮被移除，之后轮次奖励均为0。图6(c)与图6(d)说明本文提出的方案在恶意无人机占比与诚实无人机持平以及超过诚实无人机的情况下实现了总预算的公平分配。

4　结束语

提出了一种基于声誉机制的区块链赋能多无人机系统联邦学习方案，通过基于区块链的智能合约执行任务，评估各无人机的局部模型质量，得出声誉值，以声誉阈值为基准识别并驱逐恶意无人机，按声誉值稀疏化全局模型，以公平分配模型利润，并综合考虑声誉值与数据量，使诚实无人机获得与成本相符的奖励。仿真通过MNIST数据集表明，本文提出的算法精度高于FedAVG算法，能在恶意无人机占比不同的情况下将其识别并驱逐，实现了奖励的公平分配。未来计划研究新型模型压缩技术。

参考文献：

[1] LIU Y, NIE J, LI X, et al. Federated learning in the sky: Aerial-ground air quality sensing framework with UAV swarms[J]. IEEE Internet of Things Journal, 2021, 8(12): 9827-9837.

[2] ZHANG Z, WANG R, YU F R, et al. QoS aware transcoding for live streaming in edge-clouds aided HetNets: an enhanced actor-critic approach[J]. IEEE Transactions on Vehicular Technology, 2019, 68(11): 11295-11308.

[3] ZHANG Z, ZHANG Q, MIAO J, et al. Energy-efficient secure video streaming in UAV-enabled wireless networks: a safe-DQN approach[J]. IEEE Transactions on Green Communications and Networking, 2021, 5(4): 1892-1905.

[4] FU F, KANG Y, ZHANG Z, et al. Soft actor-critic drl for live transcoding and streaming in vehicular fog-computing-enabled IoV[J]. IEEE Internet of Things Journal, 2021, 8(3): 1308-1321.

[5] 武文涛，张志才，付芳. 基于联邦学习的智能网联车驾驶策略优化研究[J]. 测试技术学报，2023，37(5)：420-427.
WU Wentao, ZHANG Zhicai, FU Fang. Federated learning-based driving strategies optimization for intelligent connected vehicles[J]. Journal of Test and Measurement Technology, 2023, 37(5): 420-427. (in Chinese)

[6] YUAN Y, WANG F Y. Blockchain and cryptocurrencies: model, techniques, and applications[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018, 48(9): 1421-1428.

[7] UPADHYAY K, DANTU R, ZACCAGNI Z, et al. Is your legal contract ambiguous? convert to a smart legal contract[C]//2020 IEEE International Conference on Blockchain (Blockchain), 2020: 273-280.

[8] WANG Y, SU Z, ZHANG N, et al. Learning in the air: secure federated learning for UAV-assisted crowdsensing[J]. IEEE Transactions on Network Science and Engineering, 2021, 8(2): 1055-1069.

[9] XU G, LI H, LIU S, et al. VerifyNet: secure and verifiable federated learning[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 911-926.

[10] ZHENG Y, DUAN H, YUAN X, et al. Privacy-aware and efficient mobile crowdsensing with truth discovery[J]. IEEE Transactions on Dependable and Secure Computing, 2020, 17(1): 121-133.

[11] KANG J, XIONG Z, NIYATO D, et al. Incentive mechanism for reliable federated learning: a joint optimization approach to combining reputation and contract theory[J]. IEEE Internet of Things Journal, 2019, 6(6): 10700-10714.

[12] YI Z, JIAO Y, DAI W, et al. A stackelberg incentive mechanism for wireless federat-ed learning with differential privacy[J]. IEEE Wireless Communications Letters, 2022, 11(9): 1805-1809.