面向车联网数据隐私保护的高效分布式模型共享策略

莫梓嘉，高志鹏，杨杨，林怡静，孙山，赵晨
（北京邮电大学网络与交换技术国家重点实验室，北京 100876）

摘 要：针对车联网隐私数据共享面临的效率问题，提出了基于区块链的高效分布式模型共享策略。针对车联网场景下多实体、多角色的数据共享需求，通过在车辆、路边单元和基站之间构建主从链架构，实现了分布式模型安全共享；提出了基于激励机制的异步联邦学习算法，以激励车辆及路边单元参与优化过程；构造了混合 PBFT 的改进 DPoS 共识算法来降低通信成本、提高共识效率。实验分析表明，所提机制能够提高数据共享效率，并具有一定的可扩展性。

关键词：区块链；车联网；联邦学习；边缘计算
中图分类号：TP393
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2022074

Efficient distributed model sharing strategy for data privacy protection in Internet of vehicles

MO Zijia, GAO Zhipeng, YANG Yang, LIN Yijing, SUN Shan, ZHAO Chen
State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: Aiming at the efficiency problem of privacy data sharing in the Internet of vehicles (IoV), an efficient distributed model sharing strategy based on blockchain was proposed. In response to the data sharing requirements among multiple entities and roles in the IoV, a master-slave chain architecture was built between vehicles, roadside units, and base stations to achieve secure sharing of distributed models. An asynchronous federated learning algorithm based on motivate mechanism was proposed to encourage vehicles and roadside units to participate in the optimization process. An improved DPoS consensus algorithm with hybrid PBFT was constructed to reduce communication costs and improve consensus efficiency. Experimental analysis shows that the proposed mechanism can improve the efficiency of data sharing and has certain scalability.

Keywords: blockchain, IoV, federated learning, edge computing

0 引言

在 5G 和人工智能等新一代信息和通信技术的支撑下，由车辆、路边单元（RSU, roadside unit）、基站（BS, base station）组成[1]的车联网（IoV, Internet of vehicles）[2]通过车与车、车与人、车与路边环境等多维交互方式实现智能化交通管理、动态信息服务以及车辆智能化控制。车联网场景中车辆与各节点之间的数据共享对于改善驾驶体验、增强车载服务起着至关重要的作用。海量的车载数据包含大量关于个人的敏感信息，例如轨迹、交通信息和多媒体数据等，泄露这些敏感信息对用户有着直接和明显负面的影响[3-5]。因此，如何在保护隐私的前提下高效地共享数据是一个关键的研究课题。

联邦学习[6-7]为车联网数据共享提供了一种去中心化的分布式安全解决方案。通过将本地数据保存在车辆节点上，中心服务器聚合多个节点模型参数的方式来训练模型，从而将数据共享问题转化为

收稿日期：2021−12−07；**修回日期**：2022−03−17
基金项目：国家自然科学基金资助项目（No.62072049）
Foundation Item: The National Natural Science Foundation of China (No.62072049)

模型共享问题，在很大程度上解决了隐私问题，同时降低了数据传输成本。但是，传统联邦学习方法缺少鼓励和吸引车辆节点参与学习的激励机制，为联邦学习引入激励机制可以有效地提高联邦学习获得信息的能力。而区块链[8]凭借着分布式存储特性天然地保证了联邦学习中多个节点的模型参数一致性，同时为模型共享提供激励，鼓励车辆节点参与系统学习以提升整体性能。

然而在车联网场景中，由于车辆的移动性和不可靠的车间通信，将区块链与联邦学习集成到车联网中面临新的问题。随着车联网中车辆数量的增加和网络带宽的限制，通信效率成为在车联网场景中进行大规模数据共享的瓶颈之一。在这种情况下，本文主要面对 3 个挑战：首先，区块链产生的额外计算和通信开销给予系统较大的通信压力；其次，联邦学习模型参数的同步聚合方式造成了难以忽视的计算效率问题；最后，由于车辆及路边单元等设备懈怠导致准确率降低，系统整体性能受限。因此，为解决上述挑战，本文为车联网设计了基于主从链体系的异步联邦学习架构，旨在保护数据隐私的同时，实现高效的分布式模型共享。本文的创新点如下。

1) 提出了基于主从链体系的异步联邦学习（AFL-MSC, asynchronous federated learning based on master-slave chain）机制，与传统基于区块链的方法相比，本文提出的分层架构可以有效降低通信成本，适用于动态多车辆场景。

2) 摒除了联邦学习同步聚合的等待时间限制，结合遗传算法（GA, genetic algorithm）构造了基于通信资源优化的异步联邦学习算法，提高了通信效率。

3) 弥补了联邦学习架构中参与节点积极性差的弱点，依靠联邦学习的参数更新方式，提出了基于共识交易的节点训练激励机制，将联邦学习的模型参数以交易格式进行存储和传输，从而降低了参数传输的通信成本以及共识时间。

4) 改进了拜占庭容错共识算法的不足，构造了轻量化的区块链共识机制——混合拜占庭容错的改进委托权益证明共识机制（DPoM, delegated protocol of model），实现了快速共识，减少了系统运行时间。

1 相关工作

车联网的重要特征在于协作环境数据传感、计算和处理[9]。分布式场景下的多方数据共享是缓解车联网中计算和存储资源受限问题的一种有效方法，联邦学习技术的出现为车联网数据共享提供了有力的技术基础支撑[10]。Mcmahan 等[7]提出了一种基于迭代模型平均的联邦学习方法，该方法在学习过程中将训练数据分布在移动设备上，通过聚合本地计算的更新来学习共享模型，大大降低了数据泄露的风险。进一步地，Zhao 等[11]将联邦学习框架引入车联网环境中，为了避免隐私威胁并降低车辆之间的通信成本，将联邦学习和本地差分隐私（LDP, local differential privacy）相结合，提出了一种 LDP-FedSGD 算法来协调云服务器和车辆协同训练模型。该模型提出了 4 种差分隐私机制来扰乱本地模型输出的梯度，同时提出了三输出机制，为隐私预算引入 3 种不同的输出可能性，并用两位编码以降低通信成本。类似地，为了减少节点和中央服务器之间的通信成本，Chen 等[12]提出一种基于深浅层异步参数更新的增强联邦学习（ASTW, temporally weighted asynchronous federated learning）技术，此外，在中央服务器上引入了时间加权聚合策略，以提高中心模型的准确性和收敛性。然而，这种方法存在一个集中式的管理服务器，显著增加了系统单点故障的风险。

为规避单点故障风险，Lu 等[13]将区块链技术扩展到车联网分布式数据共享架构中，设计了一种由许可区块链和本地有向无环图组成的混合区块链架构，以提高模型参数的安全性和可靠性。此外，Lu 等[13]还提出了一种异步联邦学习方案，通过深度强化学习进行节点选择以提高效率。遗憾的是，该方案并未采取有效方法来提高异步联邦学习参数传输中的通信效率。类似地，Chai 等[14]提出了适用于车联网数据共享的分层区块链和分层联邦学习（HBFL, hierarchical blockchain-enabled federated learning）算法。知识在联邦学习过程中以学习参数的形式共享，HBFL 算法将车辆和基础设施根据其区域特征分组并维护其专属区块链账本来记录联邦学习模型。同时，Chai 等[14]还提出了一种轻量级共识机制——知识证明（PoK, proof of knowledge），将知识共享过程建模为交易市场中的多领导者和多人非合作博弈。与传统区块链框架相比，该算法虽然充分考虑了计算成本问题，但忽略了联邦学习的参数共享造成的通信成本问题。针对通信效率问题，Pokhrel 等[15]依靠联邦学习的更新奖励方法，设计了一个包含区块链参数的数学框架（例如，重传限制、块大小、块到达率和帧大小），通过对端到端时延的严格分析量

表 1　　**已有研究方案对比**

方案	设计	优点	缺点
文献[8]	数据持有者各自在本地训练模型，基于中央服务器聚合用户训练参数更新全局模型，迭代更新	降低了数据泄露风险	对数据隐私保护力度较弱
文献[11]	将联邦学习与本地差分隐私相结合，为联邦学习本地输出梯度增加噪声扰动，并用两位编码降低通信成本	提高了数据共享过程中的安全性，同时降低了通信成本	存在单点故障问题
文献[12]	将神经网络分为浅层和深层，深层网络参数的更新频率低于浅层，引入时间加权聚合策略，提高中心模型的准确性和收敛性	提升了通信效率和收敛速度	存在单点故障问题
文献[13]	利用许可区块链和本地有向无环图组成的混合区块链架构以提高模型参数的安全性和可靠性	降低了数据泄露风险，同时避免了单点故障问题	忽略了参与训练的车辆用户存在懈怠问题，共享效率低
文献[14]	采用分层区块链和分层联邦学习框架，车辆和路旁单元通过维护专属区块链账本记录联邦学习模型	增强了数据共享过程中的安全性，并在一定程度上给予参与方激励	忽略了联邦学习参数共享造成的通信成本
文献[15]	依靠更新奖励方法，设计了一个包含区块链参数的数学框架，通过对端到端时延的严格分析量化来推导出最佳块到达率，从而最小化系统时延	提高了通信效率，压缩了系统运行时间	忽略了联邦学习同步聚合导致的时延问题

化来推导出最佳块到达率，从而最小化系统时延。该框架忽略了联邦学习中同步聚合导致的时延问题，从而影响了系统的整体运行时延。

已有研究方案对比如表 1 所示。通过以上调研发现，大多数面向车联网场景的数据共享方案忽略了用户激励以及共识算法对系统效率的影响。同时，联邦学习的聚合方法也是保障共享机制高效性与有效性的一个重要因素，为此，本文提出了面向车联网数据隐私保护的高效分布式模型共享策略。

2　系统模型

2.1　网络架构

车联网由车辆、路边单元、基站 3 个部分组成，如图 1 所示。其中，基站具有较高的计算和通信能力；路边单元配有移动边缘计算（MEC, mobile edge computing）服务器，具有一定的边缘侧计算和通信能力；车辆装有智能车载系统负责车辆数据实时处理和多传感器数据融合，保证车辆在各种复杂的情况下稳定、安全行驶。路边单元通过无线信道通信链路向上与基站相连接，向下与其覆盖范围内的车辆相连接。

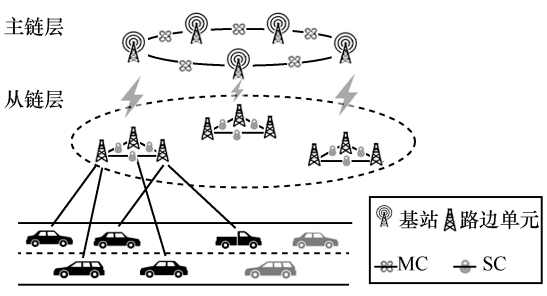


图 1　主从链架构

本文所提机制由基站组成的主链（MC, master chain）和多个由路边单元维护的从链（SC, slave chain）构成。本文假设参与学习的节点都是安全可信的，不存在恶意上传错误参数的可能性，但是，节点本身存在懈怠状态，有一定可能无法及时尽力地参与计算与共享过程。

本文所提主从链架构将全局计算与共享过程分为 3 个步骤，车辆层的本地计算过程、从链层的学习过程以及主链层的学习过程。系统参数如表 2 所示。

表 2　　**系统参数**

参数	含义
v_j^i	第 j 个路边单元范围内的第 i 个车辆
r_n^j	第 n 个基站范围内的第 j 个路边单元
b_n	主链中的第 n 个基站
$T_{v_j^i}^{\mathrm{cmp}}$	车辆 v_j^i 的本地计算时间
$w_j^i(t)$	第 t 次全局迭代中车辆 v_j^i 训练后模型参数
$F(w(t))$	在主链层全局聚合的损失函数
$\mathrm{rate}_{v_j^n}$	车辆 v_j^i 的通信传输速率
$T_{v_j^i}^{\mathrm{com}}$	车辆 v_j^i 的模型参数传输时间
T^{total}	单次迭代中系统总体运行时间

1) 车辆层的本地计算过程

车辆在本地执行基于机器学习的模型训练过程，一段时间后将训练结果向上发送给邻近的路边单元。在本地训练阶段，每个车辆基于其本地数据来训练模型，车辆 v_j^i 在训练数据集 d_j^i 上的损失函数为

$$F_j^i(w)=\frac{1}{\left|d_j^i\right|}\sum_{u\in\left|d_j^i\right|}f_u(w,x_u,y_u) \tag{1}$$

其中，$f_u(w,x_u,y_u)$ 是损失函数在数据样本 (x_u,y_u) 上的值，w 是所训练模型的参数，$\left|d_j^i\right|$ 是数据集所含有的样本数目。在不同的算法中，损失函数有不同的计算方式，本文采用梯度下降的算法来计算损失函数

$$w_j^i(t)=w_j^i(t-1)-\eta\nabla F_j^i(w_j^i(t-1)) \tag{2}$$

其中，$w_j^i(t)$ 是第 t 次迭代中的模型参数，η 是学习率，$\eta\nabla F_j^i(w_j^i(t-1))$ 是参数 $w_j^i(t-1)$ 的损失函数梯度。每轮训练完成后的模型参数通过无线网络上传至附近的路边单元。

2) 从链层的学习过程

路边单元收到所有参与训练的车辆发来的模型参数后执行全局聚合，其目标是通过全局聚合将损失函数值最小化。本文采用的加权聚合方式为

$$w_j(t)=\frac{1}{\sum_{i=1}^{I}\left|d_j^i\right|}\sum_{i=1}^{I}\left|d_j^i\right|w_j^i(t) \tag{3}$$

聚合后的新模型参数以交易的方式由主记账节点发起共识，从链层中多个路边单元共识后的结果被记录到区块链上由主记账节点向上发送给邻近的基站。

3) 主链层的学习过程

同从链层的学习过程相似，基站收到由路边单元发送的模型参数及计算结果后将其存储在本地，同时将所有收到的参数聚合，此处全局聚合的损失函数定义为

$$F(w(t))=\frac{1}{|R_J|}\frac{1}{|V_J^I|}\sum_{j\in J}\sum_{i\in I}\sum_{u\in\left|d_j^i\right|}\frac{f_j^i(w_j^i,x_i^u,y_i^u)}{\left|d_j^i\right|} \tag{4}$$

其中，$|R_J|$ 和 $|V_J^I|$ 分别代表该基站所属区域内的路边单元数量和车辆数目。联邦学习的训练是通过沿着负梯度方向最小化整体损失函数 $F(w)$，从而提升模型精度的迭代过程。获得记账权的基站发起共识并将共识通过后的结果作为全局模型参数下发到各个从链层的主节点，从链层主节点更新全局模型参数并将其发送至所属区域内的车辆节点。一直重复这个过程，直到式(4)定义的损失函数收敛或者达到本文预期的学习准确度 α $(0<\alpha\leqslant 1)$。

2.2 计算时延模型

本文所提机制的系统时延主要分为计算时延和通信时延，其中，计算时延包括节点本地计算的时间以及多节点参数聚合的时间。为了简化分析过程，本文以一次迭代过程为例进行分析，V_I 是所有参与学习的车辆集合，对于车辆 $v_j^i\in V_I$，其所持数据集用 d_j^i 表示，车辆的 CPU 主频用 $f(v_j^i)$ 表示；C_j^i 为训练单位数据的 CPU 周期个数。那么在本地计算中，每辆车每轮的训练时间为

$$T_{v_j^i}^{\mathrm{cmp}}=\frac{C_j^i\left|d_j^i\right|}{f(v_j^i)} \tag{5}$$

类似地，$f(r_n^j)$ 和 C_n^j 分别为路边单元 r_n^j 的 CPU 主频以及训练单位数据的 CPU 周期个数，$\sum_{i=1}^{I}\left|w_j^i\right|$ 为路边单元在一段时间内收到的来自所属区域内各车辆上传的参数值。在侧链层，路边单元用来聚合区域内车辆上传的模型参数所需的计算时间为

$$T_{r_n^j}^{\mathrm{cmp}}=\frac{C_n^j\sum_{i=1}^{I}\left|w_j^i\right|}{f(r_n^j)} \tag{6}$$

类似地，$f(b_n)$ 和 C_n 分别为基站 b_n 的 CPU 主频以及训练单位数据的 CPU 周期个数，$\sum_{j=1}^{J}\left|w_n^j\right|$ 为基站在一段时间内收到的来自所属区域内各路边单元上传的参数值。在主链层，基站用来聚合区域内路边单元上传的模型参数所需的计算时间为

$$T_{b_n}^{\mathrm{cmp}}=\frac{C_n\sum_{j=1}^{J}\left|w_n^j\right|}{f(b_n)} \tag{7}$$

在本文的系统模型中，相比于本地计算以及上传时间，模型聚合所需要的时间非常少，所以，本文不把聚合时间作为一个重要影响参数衡量。

2.3 通信时延模型

本文考虑使用时分多址（TDMA, time division multiple access）方法来实现数据的传输并用加性白高斯噪声信道（AGWN, additive white Gaussian noise）计算方式来表示 AFL-MSC 机制中的信道状态。本文所提 AFL-MSC 机制中的模型参数通过无线信道进行数据传输的过程主要分为 2 个部分，下载全局模型参数的时延和上传本地模型参数的时延。假设数据传输中总带宽为 B，可用的信道数为 c_0，对于车辆 v_j^i，其上行链路可达到的数据传输速率为

$$\mathrm{rate}_{v_j^i}=\frac{c_{v_j^i}(t)}{c_0}B\mathrm{lb}\left(1+\frac{\phi P_{v_j^i}(t)}{N_0}\right) \tag{8}$$

其中，$c_{v_j^i}(t)$ 是第 t 次迭代轮数被分配的子信道数，N_0 是噪声强度，$P_{v_j^i}(t)$ 是车辆的发射功率，ϕ 是车辆与上行路边单元之间的无线信道增益，$\Delta w_j^i(t)$ 是车辆客户端传输的模型参数量，为固定值。车辆 v_j^i 上传模型参数至路边单元的传输时间为

$$T_{v_j^i}^{\text{com}}=\frac{\left|\Delta w_j^i(t)\right|}{\text{rate}_{v_j^i}(t)} \tag{9}$$

其中，$\left|\Delta w_j^i(t)\right|$ 为模型更新的大小。同样地，对于路边单元 r_n^j，其上传模型参数至对应基站的传输时间为

$$T_{r_n^j}^{\text{com}}=\frac{\left|\Delta w_n^j(t)\right|}{\text{rate}_{r_n^j}(t)} \tag{10}$$

由于系统的下行带宽远大于上行带宽，因此本文不考虑下行时间。

3　算法设计

3.1　基于通信资源优化的异步联邦学习算法

本文设计了一种基于通信资源优化的异步联邦学习算法，通过降低联邦学习中单轮次所需通信资源来降低系统的整体通信开销，提升共享效率。

以从链层中车辆上传参数至路边单元的过程为例，传统的联邦学习通信过程如图 2 所示。由于车辆计算和通信资源的异构性，不同车辆的本地计算完成时间不同，路边单元等待所有参与学习的车辆完成本地计算并上传参数后才开始聚合，冗余的等待时间降低了系统的通信效率。

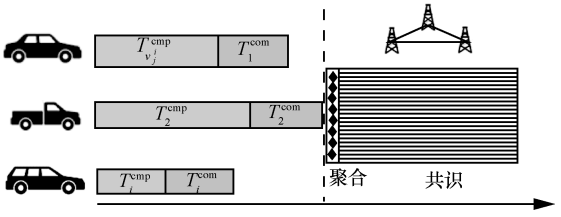


图 2　传统的联邦学习通信过程

本文提出的基于通信资源优化的异步联邦学习算法根据车辆当前的计算能力和信道状态信息，自适应地将通信资源分配给参与的车辆，以减轻通信性能的不平衡。如图 3 所示，计算能力较差的车辆被分配更多的通信资源，而计算能力较强的车辆被分配更少的通信资源。

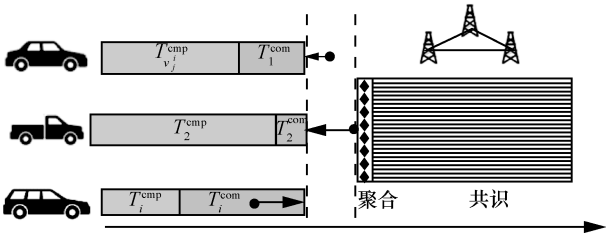


图 3　优化的联邦学习通信过程

车辆 v_j^i 的数据传输速率为

$$R_j^i=\sum_{j=1}^{c_0}\theta_i^k\,\text{rate}_{v_j^i} \tag{11}$$

其中，$\theta_i^k\in\{0,1\}$ 表示当前子信道是否分配给车辆 v_j^i，$\theta_i^k=1$ 表示当前子信道分配给车辆，$\theta_i^k=0$ 表示当前子信道不分配给车辆。对于车辆 v_j^i，本文算法在第 t 次迭代期望的平均执行时间为

$$T_{\text{exc}}(t)=\frac{1}{N}\sum_{i=1}^{N}\left(T_{v_j^i}^{\text{cmp}}(t)+T_{v_j^i}^{\text{com}}(t)\right) \tag{12}$$

基于以上内容，本文算法的优化问题可以表示为

$$\min_{\lambda,\theta}\sum_{i=1}^{N}\lambda_i\left(T_i^{\text{com}}(\theta,t)+T_i^{\text{cmp}}-T_{\text{exc}}\right)^2 \tag{13}$$

$$\text{s.t.}\lambda_i,\theta_i^k\in\{0,1\},\forall i\in N \tag{14}$$

$$\sum_{i\in N,k\in c_0}\theta_i^k\leqslant c_0 \tag{15}$$

其中，λ_i 表示车辆是否参与此次联邦学习，$\lambda_i=1$ 代表是，$\lambda_i=0$ 代表否。为了找到式(13)的最优解，本文引入遗传算法。遗传算法具有良好的全局搜索能力，利用它的内在并行性可以方便地进行分布式计算，加快求解速度。基于遗传算法的车辆选择和通信资源分配算法如算法 1 所示。

算法 1　基于遗传算法的车辆选择和通信资源分配算法

输入　候选车辆集合 $V=\{v_j^0,v_j^1,\cdots,v_j^i\}$，子信道集合 $\Theta=\{\theta_j^0,\theta_j^1,\cdots,\theta_i^k\}$

1) 从候选车辆集合中随机选择 i 个车辆为其分配子信道，其解集大小为 C_I^i

2) 设置二进制位数 l，满足 $2^l\geqslant C_I^i$

3) 设置选择率 P_i、杂交率 P_c、变异率 P_m 以及循环次数 T

4) 初始化原始解集种群 $P_0(V_0,\Theta_0)$

5) 循环：

6) 根据式(14)计算解集的适应度函数

7) 根据杂交率交叉二进制编码产生新的子集

8) 根据变异率变异部分二进制编码产生新的子集

9) 更新解集

10) 循环结束

3.2 基于主从链架构的 DPoM 共识机制

由于传统区块链共识机制的密集资源消耗以及高时延特性，将其应用于本文提出的主从链联邦学习框架中不利于系统的整体性能。因此，针对区块链共识效率及激励问题，本文提出了一种轻量级的共识方案来提高整体的通信效率。

3.2.1 交易格式及激励机制

本文所提机制的交易过程如图 4 所示。

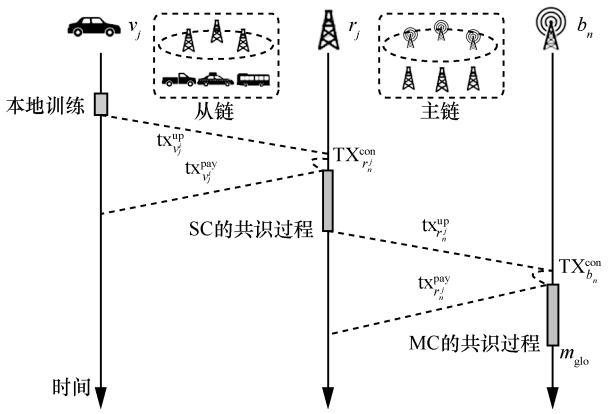


图 4　本文所提机制的交易过程

在从链层，所有参与学习的车辆 v_j^i 通过计算本地数据集 d_j^i 得到模型参数 w_j^i 以及训练结果的损失函数下降比例 ε_j^i，每个车辆将上述参数打包为交易的格式发送给邻近的路边单元

$$\mathrm{tx}_{v_j^i}^{\mathrm{up}}=\{\mathrm{Addr}_{v_j^i}\mid 0\mid w_j^i\mid \varepsilon_j^i\mid \mathrm{Addr}_{r_n^j}\mid \mathrm{SIG}_{v_j^i}\}\tag{16}$$

交易中的第二项为 0 意味着该交易为车辆上传训练好的模型参数，在收到该笔交易后，路边单元 r_n^j 先检查该笔交易的真实性，然后提取交易中的参数为后续的聚合过程做准备，并返回一个奖励给车辆。针对车辆的工作懈怠问题，本文提出了相应的激励机制：将收到的所有车辆上传的结果按照损失函数值减少的比例进行倒序排序，本文期望车辆能够将更多的计算资源贡献给学习过程，以达到系统的最快收敛。对于排序好的队列，假设 v_j^i 上传的交易排第 n 个位置，则其所获得的奖励为

$$p_j^i=\lambda\frac{p_n^j}{2In}\tag{17}$$

其中，I 为参与学习的所有车辆数；p_n^j 为路边单元的本地奖励，初始值设为 1。路边单元返回奖励给相应车辆的交易为

$$\mathrm{tx}_{v_j^i}^{\mathrm{pay}}=\{\mathrm{Addr}_{r_n^j}\mid p_j^i\mid 0\mid 0\mid \mathrm{Addr}_{v_j^i}\mid \mathrm{SIG}_{r_n^j}\}\tag{18}$$

在下一步的共识过程中，路边单元负责锻造新的区块。本文期望提升通信效率，因此在共识过程中用哈希来代替原有交易中的参数内容。因为联邦学习的模型参数量相比于一般区块交易中值来说是巨大的，常用的数据集如 MNIST 数据集每次更新的参数量大概在 1 MB 左右[16]，所以本文在区块交易中记录模型参数的方法是记录它的哈希值，当智能合约验证交易时，它需要查询星际文件系统（IPFS, inter planetary file system）以获得链下值。此时，路边单元在共识阶段发起的区块包含的交易格式为

$$\mathrm{TX}_{r_n^j}^{\mathrm{con}}=\{\mathrm{Addr}_{r_n^j}\mid \mathrm{TXID}\mid H(w_n^j)\mid \delta_n^j\mid p_n^j\mid \mathrm{SIG}_{r_n^j}\}\tag{19}$$

其中，$\mathrm{Addr}_{r_n^j}$ 是确认区块发起者的身份，p_n^j 是这笔交易在达到共识后的奖励，$H(w_n^j)$ 是模型的哈希值，δ_n^j 是该模型的准确率。共识通过后，主记账节点将新交易上传至邻近基站

$$\mathrm{tx}_{r_n^j}^{\mathrm{up}}=\{\mathrm{Addr}_{r_n^j}\mid 0\mid w_n^j\mid \mathrm{Addr}_{b_n}\mid \mathrm{SIG}_{r_n^j}\}\tag{20}$$

与从链层类似，基站收到后提取交易中的参数值，在本文的设定中，路边单元和基站都不会产生懈怠，所以此时基站返回的奖励为

$$p_n^j(t)=p_n^j(t-s)+\frac{p_n}{|J|}\tag{21}$$

其中，$p_n^j(t-s)$ 为上一个迭代过程中 p_n^j 的值，p_n 为 b_n 的本地奖励，$|J|$ 为 b_n 区域内所有参与学习的路边单元总数。与上一过程相似，基站将返回奖励至路边单元

$$\mathrm{tx}_{r_n^j}^{\mathrm{pay}}=\{\mathrm{Addr}_{b_n}\mid p_n^j\mid 0\mid 0\mid \mathrm{Addr}_{r_n^j}\mid \mathrm{SIG}_{b_n}\}\tag{22}$$

基站聚合所有参数后开始锻造区块并发起共识，此时的交易为

$$\mathrm{TX}_{b_n}^{\mathrm{con}}=\{\mathrm{Addr}_{b_n}\,|\,\mathrm{TXID}\,|\,H(w_n)\,|\,\delta_n\,|\,p_n\,|\,\mathrm{SIG}_{b_n}\}\quad(23)$$

所有基站通过共识后得到新的全局模型 w_{glo} 并将全局模型下发。本文提出的框架结合区块链和联邦学习技术来解决隐私问题。分层联邦学习方法利用参数上传机制取代传统的数据上传方法，有效地保护参与者的隐私，此外，区块链技术利用非对称加密技术和数字签名技术将参数本身替换为哈希值，进一步保护用户的隐私。

3.2.2 DPoM 共识机制

在本文提出的区块链框架中，模型聚合后的参数共享过程通过共识来达到。本文使用多个路边单元来聚合车辆在其覆盖范围内生成的本地模型，并利用区块链来同步这些模型，在不同的路边单元和基站之间达成共识。由于全局模型需要确认为区块链交易，因此区块链的运行效率对整个学习过程至关重要。由于本文提出的框架分为两层，而在从链和主链这两层的共识内容是相似的，为了方便分析，本文只给出了从链层的共识过程。

传统共识机制比如工作量证明（PoW, proof of work）机制采用哈希难题来确定候选区块的发布者，其中能够最快解出难题的获得记账权，但是该方法拥有较低的吞吐量和较高的确认时延；代理权益证明（DPoS, delegated proof of stake）机制作为主流共识算法中最平衡的算法，采用选举部分特殊节点代理网络中其余节点的方式，减少了参与区块生产和验证的节点数量，既能满足公有链对吞吐量的需求，又可以在一定程度上降低确认时延。基于此，本文提出了代理模型证明（DPoM, delegated proof of model）机制，将实用拜占庭容错（PBFT, practical Byzantine fault tolerance）算法引入 DPoS 的节点验证部分，能够进一步降低验证时延，同时引入惩罚机制，对节点生产区块的质量进行评估，以提高系统整体性能。

1) 节点类型

本文见证人选举模型涉及 4 种角色节点：普通节点、候选节点、见证人节点、备选见证人节点。

普通节点是系统中占比最大的节点类型，具有投票权和被选举权。被普通节点选举出来的节点称为候选节点。候选节点通过排序分为见证人节点和备选见证人节点 2 个集合。见证人节点具有区块打包的权力。备选见证人节点则负责对见证人节点生产的区块进行验证以及替换效率低的见证人节点。

2) 选举机制

在本文的方案中，所有参与的路边单元都充当区块链用户。它们持有的股份代表它们对训练模型的贡献，本文将其设为模型的质量。区块链用户根据路边单元计算和通信能力投票选择首选的路边单元作为验证者。持股节点在投票选举阶段会将手中的股份作为票数通过赞成投票的方式给支持的节点进行投票，每个节点允许给其他节点投一票。当投票结束后，系统计算所有节点的有效得票数，选择有效得票数排名前 $2TN$ 个节点作为候选见证人节点（TN 是系统通过至少 50%投票的持股节点认为足够去中心化的见证人节点数目），并将其分为两组，得票数排名前 TN 个节点作为本轮的见证人节点集合 $A_1=\{x_0,x_1,\cdots,x_{TN-1}\}$，另一组作为备选见证人节点集合 $A_2=\{x_{TN},x_{TN+1},\cdots,x_{2TN-1}\}$。

3) 见证人节点出块

DPoS 算法通过选择一部分称作“见证人”的节点，代为行使区块链系统中区块生成和区块验证的工作。每个见证人节点排好序后在规定的时间间隔内按序生产区块，如果没有生产成功则跳过该见证人，由下一见证人继续锻造区块。这样可以有效避免见证人出块错误导致的系统时延问题。

4) 区块验证

针对 DPoS 算法目前存在的节点生成区块后验证时延过长的问题，引入 PBFT 算法，将见证人节点生成的区块立即通过 PBFT 算法进行验证，新的机制可以在更短的时间内完成区块的验证，从而大大降低交易的确认时延。

在原始 DPoS 算法中，选举出的见证人节点会被随机打乱序列，然后在规定的时间内按照序列生产区块，新生成的区块随着见证人节点的序列交由后续的见证人节点进行区块验证。当一个区块生成后需要得到的验证确认数为总见证人节点数目的 $\frac{2}{3}$ 时，才能被加入区块链中，这样大大延长了验证时间。为了提升区块验证时延并更好地利用选举出的备选见证人节点集合 A_2，本文通过 A_2 集合中的节点对 A_1 生成的区块进行立即验证。

基于 DPoS 的见证人选举模型选举产生了 2 个节点集合：见证人节点集合 A_1 和备选见证人节点集合 A_2。A_1 节点的主要作用是对网络中产生的交易进行打包，生产区块，A_2 节点则作为备选节点用户运行 PBFT 算法，A_1 生产的区块立即广播给 A_2 集合中

的节点进行验证工作，从而更快地完成区块的验证工作，降低区块内交易的时延。

除此之外，在区块验证过程中，以主链层为例，每个基站将其聚合模型发送给其他验证节点进行验证。除了常规的验证外，验证者还根据模型是否对最后一个全局模型进行更新做出了积极贡献来验证接收到的模型。主验证节点从所有验证节点收集验证结果并确认事务。审核后的区块被添加到区块链中，并广播到其他基站进行存储。

见证人节点将产生的区块向备选见证人集合中广播。备选见证人集合中的主节点接收到该区块信息后，会封装信息并签名，主节点的选取遵循

$$P = v \bmod \left| A_2 \right| \tag{24}$$

其中，v 为 PBFT 的视图编号，$\left|A_2\right|$ 为备选见证人节点个数。主节点将封装并签名的消息向 A_2 中的其余节点广播，当其余备选见证人接收到区块消息时需要验证，验证的规则如下。

① 签名是否正确。

② 消息中的视图编号和该节点的视图编号是否一致。

③ 该区块消息是否已经接收过。

④ 消息中的区块高度是否和该节点的区块高度一致。

⑤ 模型是否对最后一个全局模型做了积极贡献。

满足上述条件的区块消息才会被备选见证人节点承认。当备选见证人节点承认接收的区块消息有效时，该节点状态就会进入准备状态，之后会继续封装准备消息并进行签名，准备消息会继续向其余节点广播，当检验通过累积达到 $\frac{TN}{3}+1$ 后，节点会进入提交状态，然后封装并签名确认消息，同样地，当确认消息个数达到 $\frac{2TN}{3}+1$ 时，该消息得到验证，该轮验证区块完成，验证结果会被返回给生产区块的见证人节点，意味着该区块可加入区块链中。基于改进 PBFT 的优化区块验证算法如算法 2 所示。

算法 2 基于改进 PBFT 的优化区块验证算法

输入 见证人节点集合 $A_1=\{x_0,x_1,\cdots,x_{TN-1}\}$，本轮见证人主节点 $N_i^{R_1}$，备选见证人节点集合 $A_2=\{x_{TN},x_{TN+1},\cdots,x_{2TN-1}\}$

输出 区块确认消息 $\text{block}_{\text{confirm}}$ 或区块错误消息 $\text{block}_{\text{error}}$

1) 封装区块消息
2) $N_i^{R_1}$ 广播消息 (block, blockMessage)
3) 选择验证主节点： $N_P^{R_2} \leftarrow v \bmod \left| N^{R_2} \right|$
4) 更新区块准备消息为 $<v,$ blockHeight, tx, Hash(tx), blockMessage $>$
5) if 节点验证准备消息为真
6) 节点 $N_P^{R_2}$ 广播准备消息
7) if 节点验证准备消息为真且验证累计到 $\frac{TN}{3}+1$
8) 节点 $N_i^{R_2}$ 广播确认消息
9) if 节点验证确认消息为真且验证累计达到 $\frac{2TN}{3}+1$
10) 节点 $N_P^{R_2}$ 广播消息 ($\text{block}_{\text{true}}$) 并且将该区块加入区块链上
11) else
12) 节点 $N_P^{R_2}$ 广播消息 ($\text{block}_{\text{error}}$) 并且记录该错误信息 (error, $N_i^{R_1}$)
13) end if
14) else
15) 节点 $N_P^{R_2}$ 广播消息 ($\text{block}_{\text{error}}$) 并且记录该错误信息 (error, $N_i^{R_1}$)
16) end if
17) end if

4 仿真与性能分析

4.1 仿真设置

4.1.1 参数设置

为了验证本文所提机制的有效性，分别在 MNIST[17]数据集和 SVHN[18]数据集上对其进行了评估。二者均为来自真实世界的数据集，可代表本地设备所收集的复杂度中等的数据，也被大量基于车联网场景的联邦学习算法作为测试数据使用。其中，MNIST 作为一个大型手写数字数据库广泛应用于图像分类任务，由 60 000 个训练示例和 10 000 个测试示例组成。SVHN 摘自 Google 街景图像中的门牌号，适用于车联网中车载传感器读取车辆周围图像数据场景，SVHN 中包含了超过 60 万张数字图像，其中训练集有 73 257 张图像，测试集有 26 032 张图像，以及额外 531 131 张图像作为训练使用。

为了更好地评估本文所提机制，数据集被平均分为 100 个子集分配给 100 个节点。实验使用卷积神经网络（CNN, convolutional neural network）作为训练模型，该网络由 2 个 5×5 的卷积层、一个全连接层和一个 softmax 输出层组成。在每个迭代周期中，包含一次全局聚合和 10 次本地训练时隙。基于上述设置，本节将对本文所提机制进行性能验证。

4.1.2　对比方案

在本文所提机制的仿真过程中，有以下 3 种对比方案。

1) 激励机制评价。通过对比本文所提机制 AFL-MSC 与 FedAVG 和 ASTW-FedAVG，可以看出本文所提激励机制对提升系统通信效率的有效性。

2) 共识机制评价。通过对比本文所提 DPoM 共识机制与 PBFT 和 DPoS 在区块确认时间上的差异，可以看出本文所提共识机制对提升系统通信效率的有效性。

3) 综合性能评价。通过改变参与训练的节点数量，可以清晰地看出本文所提机制的可扩展性；通过与 ASTW-FedAVG 以及本地 CNN 算法的对比，可以看出本文所提机制的准确率以及对不同数据集的通用性。

4.2　仿真结果分析

4.2.1　激励机制评价

为了验证本文所提激励机制的效果，本节采用 2 个指标来衡量比较算法的性能。一个是中心模型在 200 轮内的最佳准确率，另一个是在中心模型的准确率达到 95%（SVHN 数据集为 90%）。相同的计算轮次意味着相同的通信成本。MNIST 数据集和 SVHN 数据集均被分为 100 个子集并部署于 100 个节点上，由于数据集切分的随机性，本文采用 3 次随机分配结果，例如，第一次数据集的随机分配被称为 1@MNIST，比较本文所提机制 AFL-MSC 与 FedAVG 和 ASTW-FedAVG 在 MNIST 和 SVHN 数据集上的结果，如表 3 所示。

从表 3 可以看出，ASTW-FedAVG 和 AFL-MSC 在所有数据集上的通信轮数、准确率都优于 FedAVG，这是由于 FedAVG 未采用任何激励机制或其他优化算法对联邦学习中的通信效率进行优化。以 1@MNIST 为例，AFL-MSC 需要 31 轮通信即可达到 95%的准确率，优于需要 61 轮才能达到相应准确率的 ASTW-FedAVG 以及需要 75 轮才能达到相应准确率的 FedAVG。实验说明，AFL-MSC 在大多数数据集上的通信轮数和准确率方面都取得了最优结果，证明本文所提激励机制加速了学习的收敛速度并提高了学习性能，显著降低了联邦学习的通信成本。

4.2.2　共识机制评价

时延是衡量共识算法效率的指标，本文所指区块确认时延是区块从见证人节点生成后到最终被备选见证人节点验证可添加到区块链的时间间隔。作为比较，对比分析相同环境下本文所提 DPoM 与 DPoS 和 PBFT 的确认时延，如图 5 所示。

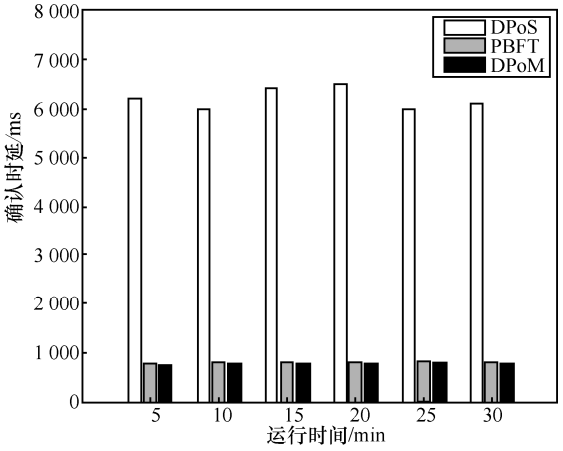


图 5　区块确认时延对比

表 3　　激励机制性能测试

数据集	FedAVG		ASTW-FedAVG		AFL-MSC	
	通信轮数	准确率	通信轮数	准确率	通信轮数	准确率
1@MNIST	75	97.2%	61	97.7%	31	97.9%
2@MNIST	85	97.2%	70	98.1%	32	98.5%
3@MNIST	73	97.3%	70	97.9%	31	98.7%
1@SVHN	126	92.3%	98	94.6%	66	94.0%
2@SVHN	156	90.2%	107	94.1%	81	95.1%
3@SVHN	137	92.6%	105	93.1%	75	93.6%

从图 5 可以看出，本文所提 DPoM 在区块的验证上做到了及时确认，所以时间上只需要 800 ms 左右，而原本 DPoS 算法因为需要得到至少 $\frac{2}{3}$ 个总验证人节点的验证确认，所以验证时间至少需要 6 s。同时，因为采用了 PBFT 算法的核心思想，所以 DPoM 与 PBFT 的验证时延基本一致。由于本文所提 DPoM 是通过选举部分见证人节点的方式代为生产区块，且见证人的数量在很长一段时间内是固定的，因此区块的吞吐量和验证时延都不会随着全网节点的增加而有很大的变化，这一特性较好地保证了区块链网络的稳定性。

4.2.3 综合性能评价

图 6 和图 7 给出了在不同训练节点数量的情况下本文所提机制在 MNIST 和 SVHN 数据集上的准确率。为了更加符合车联网中真实场景，实验将随机选取 3 个节点设置为低质量的参与者，这 3 个节点的通信和计算能力较差，通过随机噪声干扰原始参数为模型聚合过程提供较差的模型参数质量。实验结果表明，本文所提机制具有良好的精确度，由于数据集本身结构更加复杂，本文所提算法在 SVHN 上的全局准确率结果略低于 MNIST，但是同样能够达到较高的精度，证明了本文所提算法对不同数据集的通用性。

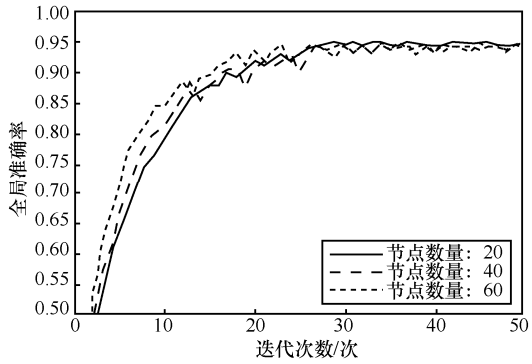


图 6 MNIST 数据集上不同数量节点的全局准确率

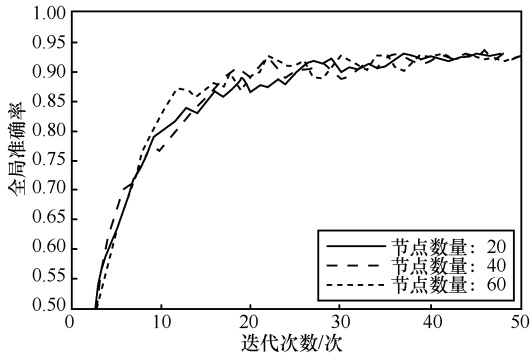


图 7 SVHN 数据集上不同数量节点的全局准确率

当参与训练的节点数量分别从 20、40 变为 60 时，随着迭代次数的增加，全局准确率结果有小幅的降低但整体差异不大。实验结果变化的幅度较小，说明了本文所提机制具有良好的可扩展性并且能够有效减少低质量节点对整体学习结果的影响。

在综合性能评价的算法对比实验中，本节将本文所提机制与本地 CNN 和 ASTW-FedAVG 进行比较。数据集被随机分为 100 个子集以分配给 100 个训练节点，本地 CNN 中节点使用被分配的子集进行模型训练，ASTW-FedAVG 在节点的子数据集上进行局部模型训练，并在中央服务器采用加权平均聚合算法更新全局模型。图 8 和图 9 表明，本文所提机制的准确率略优于 ASTW-FedAVG。本地 CNN 的准确率远低于其他 2 种机制，原因是在本地 CNN 训练算法中，本地训练的目标是最小化本地数据集的损失，这样导致其可以得到局部最优解，但可能离全局最优解仍有一定距离，因此准确率较低。实验证明，本文所提机制在保障数据安全和隐私保护的情况下仍可以达到较高的准确率。

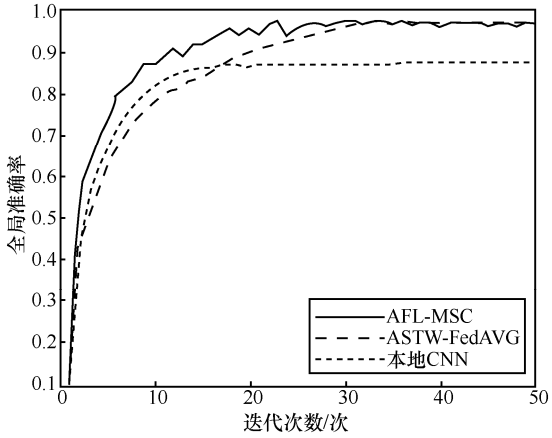


图 8 MNIST 数据集上 3 种算法的全局准确率

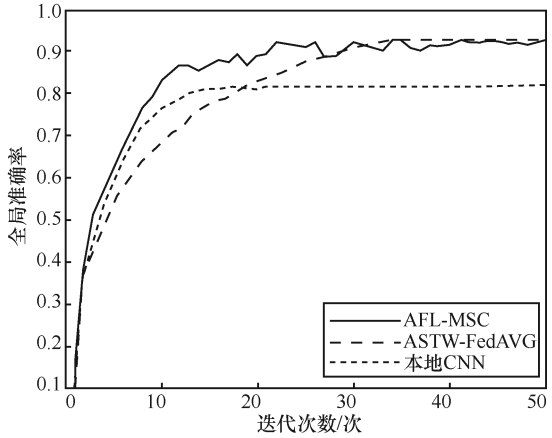


图 9 SVHN 数据集上 3 种算法的全局准确率

图 10 评估了系统总体运行时间。对于相同数量的用户，系统的运行时间随着数据集大小的增加而增加，最终趋于平稳，这是由于本文所提机制在一定程度上优化了联邦学习的计算效率以及区块链的共识效率，从而提高了系统的运行效率。对于不同数量的用户，系统的运行时间随着用户数量的增加而增加，原因是用户越多，实现协同工作所需的时间就越多。

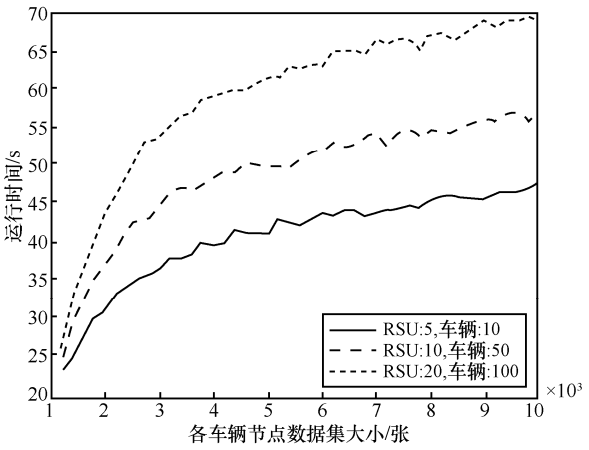


图 10　系统总体运行时间

通过以上实验可以发现，用户数量的增加对本文所提机制的准确性影响不大，但运行时间则会明显增加。稳定的准确率是因为所提方案中的主从链模式保证了稳定的学习精度，然而用户的增加使更多的本地模型需要被更新和计算，同时更多的路边单元需要执行共识，这增加了训练和更新传输的时间开销。尽管运行时间略有增加，但多个用户的参与扩大了用于计算的数据规模，从而使数据共享的内容更加准确。

5　结束语

为解决车联网场景中隐私数据共享的效率问题，本文提出了基于主从链体系的异步联邦学习架构 AFL-MSC，为分布式边缘计算在数据隐私方面提供了一个安全高效的解决方案。进一步地，为提高系统效率，本文提出基于 PBFT 的改进 DPoS 共识算法 DPoM，将激励机制引入异步联邦学习主从链架构中。仿真实验证明，相较于 ASTW-FedAVG，本文所提机制拥有更高的准确率和更低的运行时间，最终实现了安全可靠、智能高效的数据共享。

在未来工作中，将进一步对本文所提机制进行改进和完善。一方面，针对异步联邦学习时间决策问题对用户节点的选择进行优化，考虑多个因素对节点选择的影响，如能耗、通信开销、计算成本等；另一方面，改进共识算法，增强其对动态环境的适用性，以进一步提高算法的可扩展性及稳健性。

参考文献：

[1] YANG F C, WANG S G, LI J L, et al. An overview of Internet of vehicles[J]. China Communications, 2014, 11(10): 1-15.

[2] CONTRERAS-CASTILLO J, ZEADALLY S, GUERRERO-IBAÑEZ J A. Internet of vehicles: architecture, protocols, and security[J]. IEEE Internet of Things Journal, 2018, 5(5): 3701-3709.

[3] BILOGREVIC I, JADLIWALA M, KALKAN K, et al. Privacy in mobile computing for location-sharing-based services[C]// International Symposium on Privacy Enhancing Technologies Symposium. Berlin: Springer, 2011: 77-96.

[4] LIANG X H, LI X, LUAN T H, et al. Morality-driven data forwarding with privacy preservation in mobile social networks[J]. IEEE Transactions on Vehicular Technology, 2012, 61(7): 3209-3222.

[5] YING B D, MAKRAKIS D, HOU Z Z. Motivation for protecting selfish vehicles' location privacy in vehicular networks[J]. IEEE Transactions on Vehicular Technology, 2015, 64(12): 5631-5641.

[6] WANG X F, HAN Y W, WANG C Y, et al. In-edge AI: intelligentizing mobile edge computing, caching and communication by federated learning[J]. IEEE Network, 2019, 33(5): 156-165.

[7] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[J]. arXiv Preprint, arXiv: 1602.05629, 2016.

[8] DAI H N, ZHENG Z B, ZHANG Y. Blockchain for Internet of things: a survey[J]. IEEE Internet of Things Journal, 2019, 6(5): 8076-8094.

[9] CHEN M, TIAN Y W, FORTINO G, et al. Cognitive Internet of vehicles[J]. Computer Communications, 2018, 120: 58-70.

[10] ELBIR A M, SONER B, COLERI S. Federated learning in vehicular networks[J]. arXiv Preprint, arXiv: 2006.01412, 2020.

[11] ZHAO Y, ZHAO J, YANG M M, et al. Local differential privacy-based federated learning for Internet of things[J]. IEEE Internet of Things Journal, 2021, 8(11): 8836-8853.

[12] CHEN Y, SUN X Y, JIN Y C. Communication-efficient federated deep learning with layerwise asynchronous model update and temporally weighted aggregation[J]. IEEE Transactions on Neural Networks and Learning Systems, 2020, 31(10): 4229-4238.

[13] LU Y L, HUANG X H, ZHANG K, et al. Blockchain empowered asynchronous federated learning for secure data sharing in Internet of vehicles[J]. IEEE Transactions on Vehicular Technology, 2020, 69(4): 4298-4311.

[14] CHAI H Y, LENG S P, CHEN Y J, et al. A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in Internet of vehicles[J]. IEEE Transactions on Intelligent Transportation

Systems, 2021, 22(7): 3975-3986.

[15] POKHREL S R, CHOI J. Federated learning with blockchain for autonomous vehicles: analysis and design challenges[J]. IEEE Transactions on Communications, 2020, 68(8): 4734-4746.

[16] 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.

[17] 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.

[18] NETZER Y, WANG T, COATES A, et al. Reading digits in natural images with unsupervised feature learning[C]// NIPS Workshop on Deep Learning and Unsupervised Feature Learning. [S.l.:s.n.], 2011: 1-9.

[作者简介]

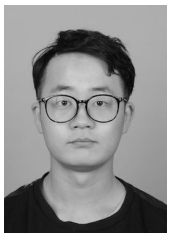
莫梓嘉（1996− ），女，河北保定人，北京邮电大学博士生，主要研究方向为边缘智能、模型轻量化等。

高志鹏（1980− ），男，山东滨州人，博士，北京邮电大学教授、博士生导师，主要研究方向为云计算、网络服务与管理、边缘计算等。

杨杨（1981− ），女，山东淄博人，博士，北京邮电大学副教授、博士生导师，主要研究方向为数据挖掘、人工智能等。

林怡静（1997– ），女，福建莆田人，北京邮电大学博士生，主要研究方向为边缘计算、区块链等。

孙山（1998– ），男，山东济宁人，北京邮电大学硕士生，主要研究方向为边缘智能、云边协同等。



赵晨（1992– ），男，河南南阳人，北京邮电大学博士生，主要研究方向为边缘计算、联邦学习等。