车辆算力网络中异步鲁棒联邦学习方法研究

尹宏博[1]，王帅[1]，张科[1,2]，张引[1,3]
（1. 电子科技大学信息与通信工程学院，四川 成都 611731；2. 电子科技大学（深圳）高等研究院，广东 深圳 518110；
3. 广东省智能机器人研究院，广东 东莞 523830）

摘　要：传统联邦学习的同步训练机制并不适用于动态的车辆算力网络场景，且在恶意车辆攻击的威胁下，缺乏有效的攻击检测机制。为了解决以上问题，首先，提出一种异步鲁棒联邦学习方法，通过车辆之间异步地执行联邦学习过程，在实现车辆数据隐私保护的同时，提高模型协同训练的效率。其次，有针对性地设计了模型选择方法，并提出潜在恶意模型检测方法和车辆信誉评估方法，进一步增强系统鲁棒性。然后，从概率上详细分析了所提方法的安全性，为各项参数优化提供理论基础。最后，仿真结果表明该方法能够在实现高效异步联邦学习的同时具有较好的鲁棒性。

关键词：车辆算力网络；联邦学习；鲁棒性；异步学习
中图分类号：TN915.08
文献标志码：A
doi：10.11959/j.issn.2096−3750.2024.00452

Research on asynchronous robust federated learning method in vehicle computing power network

YIN Hongbo[1], WANG Shuai[1], ZHANG Ke[1,2], ZHANG Yin[1,3]
1. School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
2. Shenzhen Institute for Advanced Study, University of Electronic Science and Technology of China, Shenzhen 518110, China
3. Guangdong Intelligent Robot Research Institute, Dongguan 523830, China

Abstract: The synchronous training mechanism of traditional federated learning was not suitable for dynamic vehicle computing power network scenarios, and lacked effective detection mechanisms under the threat of malicious vehicle attacks. To address the above issues, an asynchronous robust federated learning method was proposed, which achieves vehicle data privacy protection while improving the efficiency of model collaborative training through asynchronous execution of federated learning processes between vehicles. Secondly, a model selection method was designed, and potential malicious model detection and vehicle reputation evaluation methods are proposed to further enhance the robustness of the system. Then, the safety of the proposed method was analyzed in detail from a probabilistic perspective, providing a theoretical basis for optimizing various parameters. Finally, the simulation results show that this method can achieve efficient asynchronous federated learning while having good robustness.

Key words: vehicle computing power network, federated learning, robustness, asynchronous learning

0　引言

随着“交通强国”等国家战略的不断提出，智能交通系统（ITS, intelligent transportation system）正在成为现代城市交通管理的关键领域。在第五代移动通信技术、边缘算力网络等新技术深度融合背

收稿日期：2024−11−18；**修回日期：**2024−12−10
通信作者：张引，zhangyin123@uestc.edu.cn
基金项目：广东省重点研发计划（No.2024B1111060001）
Foundation Item: The Key Research and Development Program of Guangdong Province (No.2024B1111060001)

景下，中国汽车网联化与智能化协同发展按下“加速键”，车联网产业已成为国内外新一轮科技创新和产业发展的必争之地[1-2]。

车辆用户和基础设施等交通参与方产生的实时数据将呈指数级增长[3-4]。在实际交通场景中，单个车辆每天可以产生高达30 TB的数据，包括雷达图像、交通信息、驾驶信息等多类数据。这些数据被应用于各类智能服务中，在车联网和自动驾驶技术中发挥着重要作用[5-7]。算力网络（CPN, computing power network）是一种根据业务需求灵活调度网络资源的新型信息基础设施[8]，其与车联网相结合逐渐发展为车辆算力网络[9]。在车辆算力网络场景中，车辆之间可以高效地利用感知数据，通过丰富的算力来提供更多样的智能驾驶服务[10-13]。

随着人工智能（AI, artificial intelligence）等技术的发展，各类智能驾驶服务可以通过机器学习（ML, machine learning）等技术实现[14-15]。ML技术是AI的核心，同时也是实现智能驾驶，如行人检测[16]、故障识别[17]、自动驾驶[18]等服务的关键技术。在车辆算力网络中，车辆之间可以共享本地数据，协同训练更强大的智能驾驶模型。然而，分布式数据的隐私问题带来数据“孤岛”现象，导致难以收集大量可用的车辆数据进行ML的模型训练。

联邦学习（FL, federated learning）[19]作为一种新兴的分布式ML框架，旨在通过利用分散在边缘设备上的数据进行模型训练，从而保护用户隐私。FL允许模型在车辆本地进行训练，将车辆的隐私数据保留在本地，从而保护车辆用户隐私。目前，FL已被广泛应用于车联网场景中，以实现车辆间智能驾驶模型的协同训练[20-22]。文献[5]在车联网中结合FL提出了去中心化的ML系统，保护车辆FL过程的安全和隐私。然而，在车辆算力网络中，传统FL的直接应用将带来许多挑战。

首先，传统FL系统通常依赖同步训练机制，这要求所有参与车辆在相同时间内上传其本地训练得到的模型。在不稳定的网络环境中，某些节点可能因信号弱、网络拥堵或设备故障无法及时进行上传，因此，FL训练和聚合过程往往是不稳定的[23]，导致全局模型的收敛速度显著降低，训练缓慢。

其次，在车辆算力网络的动态场景中，车辆的移动性进一步加剧了同步机制所面临的问题。车辆的移动性导致网络拓扑的不稳定性，使得模型聚合和数据同步变得复杂，频繁的网络变化也增加了协议设计的复杂性，需要更灵活的架构来适应环境的动态变化。因此，应针对动态的车辆算力网络场景，设计异步FL方案，以实现车辆间更高效的FL。

最后，基础设施的离散部署和频繁的信息交互给模型的安全性带来了巨大挑战。传统FL通常未考虑有效的安全机制来识别和防范恶意车辆的攻击[24]，恶意车辆可能通过提交错误的模型更新，以干扰全局模型的训练过程，造成全局模型精度的降低[25-26]。因此，需要有针对性地设计恶意攻击检测方案，以增强FL的鲁棒性。

针对上述问题，目前已有许多研究人员提出相应的解决方案。文献[27]提出了一种异步FL框架，但传统区块链技术的引入使得系统面临较高的资源消耗问题。为此，文献[28]采用更轻量化的区块链，提出了一种面向设备端的异步FL机制，以提高FL的有效性和鲁棒性。然而，将区块链部署在车辆端使得在动态场景中很难维持区块链账本的同步，导致延迟增加。文献[29]提出了一种分层FL机制，车辆通过向边缘服务器共享FL模型，将FL应用于大规模动态车联网中，然而，其面对恶意攻击场景时，具有较低的鲁棒性。为此，文献[30]提出了一种用于车联网FL的分层架构，其通过深度强化学习方法进行节点选择，以提高FL模型训练的效率和鲁棒性，但由于其半异步机制和车辆的深度参与，在车辆移动的场景中FL效率较低。

为了解决以上问题，本文提出一种应用于车辆算力网络场景的异步鲁棒FL方法。车辆之间可以异步地执行FL过程，在实现车辆数据隐私保护的同时，进一步提高模型协同训练的效率。在此之上，本文有针对性地设计了模型选择方法，通过优化模型选择过程以增强所提异步FL方法的鲁棒性。进一步提出了潜在恶意模型检测方法和车辆信誉评估方法，实时甄别潜在的恶意模型，并基于此动态地更新车辆信誉值，以有效地识别恶意车辆，限制其参与FL过程，进一步增强系统鲁棒性。然后，从概率上详细分析了所提方案的安全性，为各项参数优化提供理论基础。最后，通过仿真实验验证了本文所提异步鲁棒FL方法的有效性。

本文所提方法能够充分利用车辆算力和本地数据，实现车辆算力网络中安全高效的异步FL，同

时确保车辆用户隐私和模型安全，为各类智能驾驶服务提供新的模型训练方法。

1　系统模型

本文车辆算力网络系统模型如图 1 所示，主要由一个基站（BS, base station）、多个路边单元（RSU, road side unit）和多个车辆组成。

1) 车辆。车辆可以通过车载传感器，如摄像头、雷达等，不断收集环境信息和驾驶数据，用于智能驾驶模型的训练，如行人检测、交通标志识别等。在本文场景中，车辆作为联邦学习的客户端参与模型本地训练，通过无线链路与 RSU 形成车对基础设施（V2I, vehicle-to-infrastructure）通信网络，以获取和上传 FL 模型。车辆集合表示为 N。

2) RSU。搭载小型服务器的 RSU 部署在更靠近车辆的道路两侧，为车辆提供通信与缓存服务。每个 RSU 都将通过 BS 实时同步模型池，为车辆 FL 提供最新模型。此外，车辆更新的模型也将通过 RSU 添加到模型池。

3) BS。BS 具有强大的通信、存储和计算能力。BS 有一个模型库，以保留系统中所有车辆训练的 FL 模型。同时，BS 在模型库中实时维护一个模型池，并将模型池实时同步给所有 RSU，用于异步的 FL 模型训练。

车辆将异步地执行模型训练，其通过 RSU 获取模型池中的模型，并选择部分模型进行聚合。然后使用隐私数据进行本地模型训练，最后通过 RSU 将更新后的模型添加到模型池中，模型池将通过 BS 在所有 RSU 中实现同步。

此外，在车辆算力网络场景中，可能存在恶意车辆发起中毒攻击等恶意攻击，意图降低全局模型质量。本文提出一种模型选择方法来规避低质量的模型，并加快收敛速度。基于此，BS 可以根据模型库中的历史记录，分析每个模型被聚合的次数，有效识别潜在的恶意模型。同时，进一步实现对车辆的信誉值评估与管理，可以识别和限制潜在的恶意车辆，增强 FL 的鲁棒性。

2　异步鲁棒 FL 方法

在车辆算力网络中，由于车辆的移动性带来网络拓扑的动态变化，传统 FL 的同步训练机制在不稳定环境中导致性能下降和训练缓慢，而在动态开放的网络中存在恶意车辆攻击，使得 FL 模型安全面临威胁。为解决以上问题，本文提出了一种用于车辆算力网络的异步鲁棒 FL 方法，异步鲁棒 FL 流程如图 2 所示，具体步骤如下。

步骤 1　异步模型下载：每个车辆将异步地通过 V2I 链路，从 RSU 的模型池中获取模型。为了避免传输所有模型带来的额外的通信开销，所关联的 RSU 将从模型池中随机选择 K 个模型发送给车辆。

步骤 2　车辆本地更新：车辆 n 接收到 K 个模型后，根据模型选择算法（详见第 2.1 节），选择 k 个

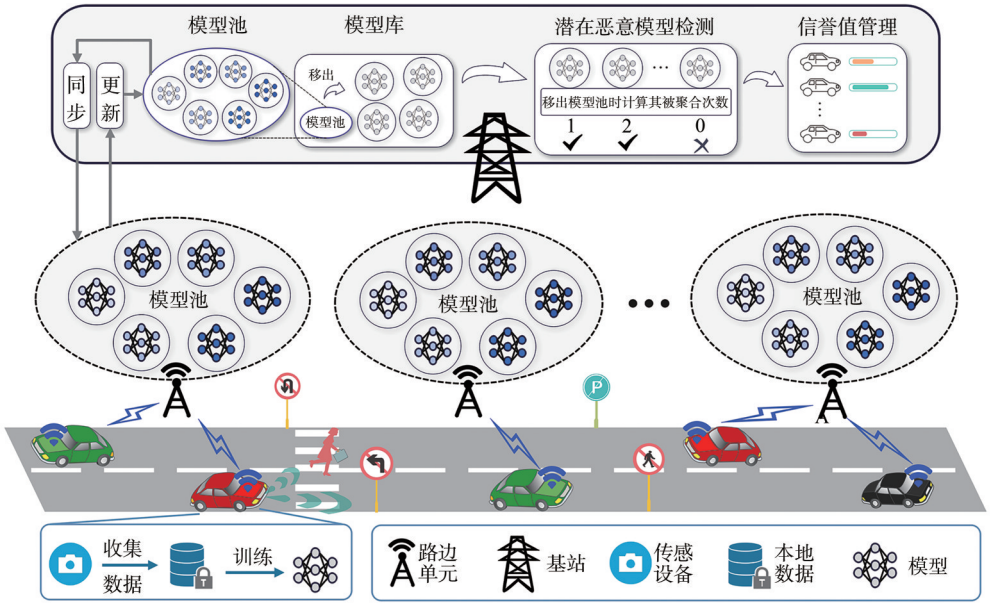

图 1　车辆算力网络系统模型

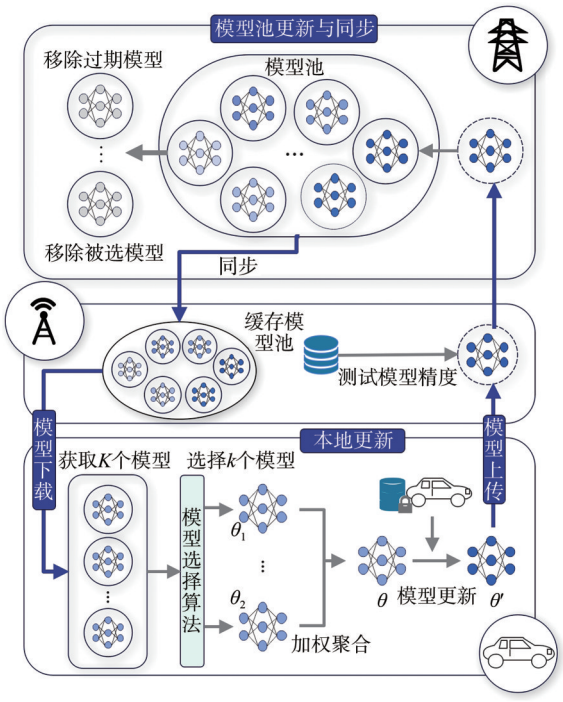

图2　异步鲁棒FL流程

模型，加权聚合作为初始模型θ，θ表示为

$$\theta=\frac{\sum_{i=1}^{k}W_i\theta_i}{\sum_{i=1}^{k}W_i} \tag{1}$$

其中，W_i为聚合的权重，θ_i为所选择模型的参数。然后，车辆n将使用本地隐私数据D_n训练该模型得到更新后的模型θ'。

步骤3　异步模型上传：每个车辆在完成本地更新后，将异步地上传更新后的模型。首先，车辆将模型上传至RSU。其次，所关联的RSU将使用一个由BS统筹下发的规模为l的小数据集$D_0=\{(x_i, y_i)|i\in\{1, 2, \cdots, l\}\}$来测试车辆所上传模型的精度Accuracy

$$\text{Accuracy}=\frac{\sum_{i=1}^{l}I(\hat{y}_i=y_i)}{l} \tag{2}$$

其中，$I(\cdot)$为指示函数，y_i为样本真实标签，$\hat{y}_i$为样本预测标签。测试数据集D_0决定了模型更新的大致方向，可用来快速评估上传模型的质量。该精度将作为步骤2中模型选择算法的重要依据。最后，RSU将模型及其相关信息打包发送给BS，以将其更新到模型池中。

步骤4　模型池更新与同步：BS将不断接收RSU发来的模型。首先，BS为接收到的模型添加时间戳，并将其添加到模型池中。其次，BS将对模型池进行更新，分别移除过期模型和被选模型。其中过期模型是指在模型池中存在时间大于阈值t'的模型，其在存在时间内未被任何模型选择和聚合。被选模型指BS所接收的模型在步骤2中所选择的k个模型，其已经被聚合到新的模型中并得到了进一步的训练。值得注意的是，由于该过程是异步的，同一个模型可能会被不同的车辆所选择，直至第一个选择该模型的车辆所上传的模型被添加至模型池中，该模型才会被移除。因此，模型池中的模型数量将维持稳定。最后，更新后的模型池将同步给所有的RSU。

基于以上步骤，模型池中的模型将不断地被更新，其中的模型精度将不断升高直至收敛。

2.1　模型选择算法

基于所提出的异步FL方法，在步骤2中，当车辆收到RSU发送来的K个模型后，将选择k个模型进行聚合和训练。为了避免恶意车辆所发出的恶意模型的影响，同时提高系统效率，本节提出一种基于测试精度的模型选择算法。具体地，在K个模型中，模型i被选中的概率p_i为

$$p_i=\frac{\exp\{\gamma A_i\}}{\sum_{j\in K}\exp\{\gamma A_j\}} \tag{3}$$

其中，A_i、A_i分别为模型i、j的测试精度，该精度在步骤3中由RSU使用规模为l的小数据集D_0测试得到。γ为放大参数，其决定了精度差异对选择结果影响的大小。当γ较大时，精度越高的模型被选概率越大，其可以更大程度地避免选择到恶意模型，但可能会导致模型池中仅有少数当前精度较高的模型被选择，使模型泛化性降低。当γ较小时，大多数模型都将被选择，由此可以聚合多个模型当中的知识，增强模型泛化性，但可能会受到恶意模型的影响。具体细节将在第2.3节进一步讨论。

2.2　潜在恶意模型检测与信誉值评估

基于所提出的异步FL方法，在步骤4中，当模型被成功上传后，BS将更新模型池。当模型已被其他模型选择或过期时，该模型被移出模型池。根据所提出的模型选择算法，精度较低的模型（潜在的恶意模型）几乎不被选择，导致其过期而被移出模型池。

基于此，在模型i被移出时，BS可以根据其被选择的次数C_i来识别潜在的恶意模型。当C_i为0时，表示没有任何模型选择模型i，其可能为恶意模型，

由于精度较低而不被选择。因此将C_i为0的模型判定为潜在的恶意模型，以进一步评估车辆信誉值，限制恶意车辆的参与。

车辆n的信誉值R_n为

$$R_n = \frac{\sum_{i \in M_n} C_i}{|M_n|} \tag{4}$$

其中，M_n为车辆n所上传的所有模型的集合。当R_n小于给定阈值R'，即$R_n<R'$时，车辆n被认为是恶意车辆。车辆的信誉值将随着模型上传实时更新，并同步给所有RSU，恶意车辆将被限制参与异步FL过程，以确保系统的鲁棒性。

2.3　安全性分析

所提出的异步鲁棒FL方法涉及两阶段的模型选择过程。第一阶段为RSU随机选择K个模型发送给车辆。第二阶段为车辆根据所提出的模型选择算法选择k个模型进行聚合，用于后续的本地模型训练和更新。

假设模型池中模型数量为M，恶意车辆比例设定为p^m。可以估算当前模型池中恶意模型数量H为

$$H = Mp^m \tag{5}$$

对于模型选择的第一阶段，RSU将从模型池M个模型中随机选择K个发送给车辆。在这种情况下，RSU所选择的K个模型中恶意模型的数量服从如下超几何分布

$$X \sim H(M, H, K) \tag{6}$$

基于此，在该阶段，RSU选择了x个恶意模型的概率为

$$P^1(X = x) = \frac{\mathrm{C}_H^x \mathrm{C}_{M-H}^{K-x}}{\mathrm{C}_M^K} \tag{7}$$

其中，C表示排列数公式。

对于模型选择的第二阶段，根据所提出的模型选择算法，当第一阶段的K个模型中存在x个恶意模型时，第二阶段所选择的k个模型中不存在恶意模型的概率为

$$P^2(x) = \prod_{i=1}^{k} \frac{(K-x-i+1)\cdot\exp\{\gamma A^+\}}{(K-x-i+1)\cdot\exp\{\gamma A^+\} + x\cdot\exp\{\gamma A^-\}} \tag{8}$$

其中，A^+、A^-（$A^+>A^-$）分别为正常模型和恶意模型的平均精度。在该阶段，需要先前所选择的K个模型中恶意模型数量$x \leqslant K-k$，否则，第二阶段必将选择恶意模型。

模型选择过程在两个阶段是独立的，因此，在模型选择时能够成功避免选择到恶意模型的概率为

$$p^+ = \sum_{x=0}^{K-k} (P^1(X=x) P^2(x)) =$$

$$\sum_{x=0}^{K-k} \left(\frac{\mathrm{C}_H^x \mathrm{C}_{M-H}^{K-x}}{\mathrm{C}_M^K} \prod_{i=1}^{k} \frac{(K-x-i+1)\cdot\exp\{\gamma A^+\}}{(K-x-i+1)\cdot\exp\{\gamma A^+\} + x\cdot\exp\{\gamma A^-\}} \right) \tag{9}$$

根据式(3)，增大参数γ可以使得选择恶意模型的概率减小，当$\gamma \to +\infty$时，由于$A^+>A^-$，此时

$$\prod_{i=1}^{k} \frac{(K-x-i+1)\cdot\exp\{\gamma A^+\}}{(K-x-i+1)\cdot\exp\{\gamma A^+\} + x\cdot\exp\{\gamma A^-\}} \to 1 \tag{10}$$

第二阶段的模型选择过程可近似为直接选择精度最高的k个模型。进一步可得

$$p^+ \to \sum_{x=0}^{K-k} \frac{\mathrm{C}_H^x \mathrm{C}_{M-H}^{K-x}}{\mathrm{C}_M^K} \tag{11}$$

此时p^+将仅受K的影响，即第一阶段选择的模型数量的影响。在这种情况下，由于k固定，增大K可以有效地增大p^+以规避选择到恶意模型。

γ过大时，模型池中只有少量高精度模型被选择，进而影响模型泛化性。此外，K增大也将增大在模型下载阶段传输的数据量，导致额外的通信开销。同时，车辆可以增大k以聚合更多的模型，进而增强模型泛化性。然而，在恶意车辆存在的场景中，增大k也将增大恶意模型被选中的概率，进而影响模型质量。因此，在实际场景中，应当权衡安全性、模型泛化性和通信时延，以设置合适的参数γ、K和k。

3　仿真测试

3.1　仿真设置

3.1.1　数据集

采用基于德国交通标志识别基准数据集[31]的预处理数据集来测试本文所提异步鲁棒FL方法的有效性。该数据集包含86 989个训练集、4 410个验证集和12 630个测试集的43类交通标志图像。为了模拟更加真实的车辆算力网络场景，将数据集划分为多个非独立同分布（Non-IID, non independent and identically distributed）的子数据集以将其分配给所有车辆，使每个车辆中数据集的数据标签服从参数为$\alpha(\alpha>0)$的狄利克雷分布。当参数$\alpha \to \infty$时，所有车辆的数据为独立同分布（IID, independent and identically distributed）；当参数$\alpha \to 0$时，每个车辆本地仅有一类数据，车辆之间的数据差异程度达到最大。在本次仿真中考虑3种数据分布场景：

数据IID分布（$\alpha\to\infty$）、数据小程度Non-IID分布（α=1）和数据大程度Non-IID分布（α=0.2）。

3.1.2　模型

采用基于卷积神经网络（CNN, convolutional neural network）的LeNet5作为FL训练的模型。其包含一个输入为32×32×3的输入层，两个卷积核为5×5的卷积层，其激活函数为ReLU，两个2×2的池化层和3个全连接层。

3.1.3　对比算法

将本文方案与传统FL[19]以及目前先进的相关算法——基于有向无环图的FL（DFL, directed acyclic graph FL）[28]、基于许可有向无环图的FL（PermiDAG, permissioned directed acyclic graph FL）[30]和加权更新FL（WUFL, weighted update FL）[29]进行对比。对于传统FL，每一轮选取10%的空闲车辆参与模型训练；DFL将区块链与FL技术相结合实现面向设备端的鲁棒异步FL；PermiDAG为用于车联网的半异步FL机制；WUFL通过分层机制实现面向车联网的高效FL。此外，将一次迭代定义为一个车辆进行一次模型的训练和上传。仿真详细参数设置见表1。

表1　　仿真详细参数设置

参数	设置
样本抽样规模	100
学习率	0.005
K	5
k	2
恶意车辆比例	0%~50%
车辆节点数	100

3.2　仿真结果及分析

在不同数据分布情况下，不同算法的模型精度见表2，不同算法的模型收敛迭代次数见表3。

表2　　不同算法的模型精度

算法	精度		
	$\alpha\to\infty$	α=1	α=0.2
FL	0.937 8	0.932 5	0.931 4
DFL	0.928 7	0.926 1	0.912 2
PermiDAG	0.935 0	0.929 5	0.921 9
WUFL	0.925 1	0.924 1	0.919 1
本文方法	0.935 1	0.930 2	0.930 1

表3　　不同算法的收敛迭代次数

算法	迭代次数		
	$\alpha\to\infty$	α=1	α=0.2
FL	764	1 106	1 535
DFL	1 159	1 535	1 955
PermiDAG	1 857	2 140	2 479
WUFL	1 900	2 600	3 100
本文方法	827	1 199	1 349

首先，在车辆数据IID（$\alpha\to\infty$）场景下，得益于其同步机制，理想情况下传统的FL算法具有更高的精度和更快的收敛速度。然而，传统FL算法并不适用于动态的车辆算力网络场景。与传统FL相比，本文算法在实现了异步训练和聚合的同时，精度和收敛速度仅有轻微下降。此外，本文算法所提出的模型选择法，通过优化模型的选择，与其他异步或半异步算法相比表现出更高的精度和更快的收敛速度。而PermiDAG和WUFL算法由于其特殊的模型聚合方式，收敛速度较慢，且WUFL的模型泛化性较差。

其次，在车辆数据Non-IID分布（α=1, α=0.2）场景下，不同算法的模型精度和收敛速度均受到影响。尽管传统FL仍有较高的模型精度，但其收敛速度慢于本文算法。由于采用同步和半异步机制，FL、PermiDAG和WUFL可以减轻Non-IID数据对精度的影响，而DFL由于其特殊的模型聚合机制对Non-IID数据更加敏感。本文算法可以有效地缓解Non-IID数据引起的模型精度下降，相较其他对比算法具有更好的收敛速度和更高的模型精度。

在3种不同数据分布场景中，存在10%的恶意车辆（发起中毒攻击）时的模型精度见表4。其中，DFL采用的聚合算法可在一定程度上规避恶意模型的影响，对中毒攻击表现出一定程度的免疫力，但其模型精度有明显降低。PerimiDAG对恶意车辆具有一定的检测能力，但其模型精度也有显著下降。而FL和WUFL由于缺乏对恶意车辆的防御机制，不具备识别和筛除恶意车辆的能力，最终导致模型无法收敛。本文所提算法中，低精度的模型几乎不会被选择，因此在不同数据分布场景下均对恶意车辆有较好的鲁棒性，本文算法与其他对比算法相比具有更高的模型精度。

在3种数据分布场景中，存在不同比例（0%~50%）恶意车辆时本文算法的模型精度见表5。可以看出，本文算法对恶意车辆存在的场景具有较好

的鲁棒性。在数据IID场景中，本文算法对恶意车辆比例的容错率约为40%。当恶意车辆的比例大于40%时，模型精度将显著降低。在数据Non-IID场景中，容错率降低为30%。这表明本文算法能够很好地应对更复杂的网络场景，实现更安全的异步鲁棒FL。

表4　存在10%的恶意车辆（发起中毒攻击）时的模型精度

算法	精度		
	$\alpha\to\infty$	α=1	α=0.2
FL	不收敛	不收敛	不收敛
DFL	0.925 5	0.911 3	0.901 9
PermiDAG	0.926 6	0.921 2	0.897 9
WUFL	不收敛	不收敛	不收敛
本文方法	0.934 7	0.930 1	0.927 4

表5　存在不同比例（0%~50%）恶意车辆时本文算法的模型精度

比例	精度		
	$\alpha\to\infty$	α=1	α=0.2
0%	0.935 1	0.930 2	0.930 1
10%	0.934 7	0.930 1	0.927 4
20%	0.926 2	0.924 9	0.922 9
30%	0.920 7	0.916 1	0.915 2
40%	0.912 1	0.894 8	0.885 9
50%	0.886 8	0.883 5	0.876 1

图3展示了不同K值下p^+与参数γ的关系，即在不同的K值（RSU随机选择模型的数量）下，车辆执行模型选择时能够成功避免选择到恶意模型的概率p^+与参数γ的关系，其中γ为式(3)中的放大参数。假设当前模型池的模型数量M=20，其中恶意模型数量H=5；车辆选择模型的数量k=2；模型池中正常模型平均精度A^+=0.8；恶意模型平均精度A^-=0.6。如图5所示，当K固定时，γ越大，p^+越大，这意味着增大参数γ可以提高系统安全性。但是γ过大，如式(10)和式(11)，会使得模型池中只有少量高精度模型被选择，进而影响模型泛化性。此外，增大K可以显著提高系统的安全性，当K足够大时，如图5中K=5和K=6时，安全性增益将降低，过大的K将导致车辆模型下载量增大，带来更多的通信开销。因此，在实际部署时，应当首先根据车辆信誉值的变化，估计模型池中的恶意模型数量，然后设定合适的γ和K值以权衡系统安全性、模型泛化性和通信开销。

正常车辆与恶意车辆的信誉值随全局训练迭代次数的变化如图4所示。设定每间隔50轮迭代观察一次，在全局第200轮迭代时，恶意车辆开始发起中毒攻击。可以观察到，正常车辆的信誉值将维持在较高的水平并保持稳定。恶意车辆的信誉值在第200轮迭代后开始迅速下降，直至在400轮迭代时低于设定阈值，其被成功识别为恶意车辆。BS将在模型池更新时，同时更新参与车辆的信誉值表，以有效地识别网络中的恶意车辆，增强系统鲁棒性。

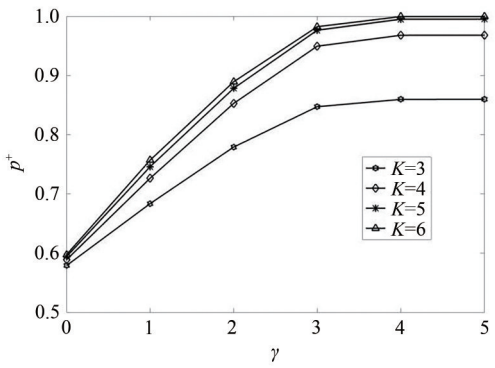

图3　不同K值下p^+与参数γ的关系

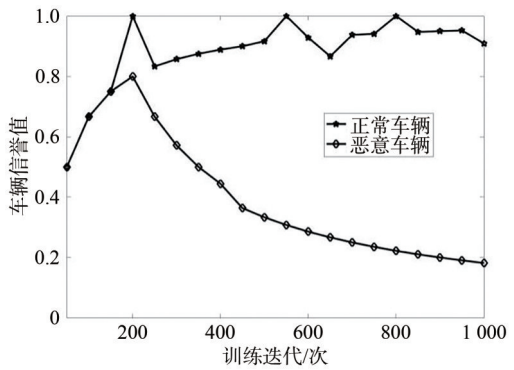

图4　正常车辆与恶意车辆的信誉值随全局训练迭代次数的变化

4　结束语

传统FL受限于同步机制和较低的鲁棒性，难以被直接应用于车辆算力网络场景，因此本文提出一种异步鲁棒FL方法，以实现车辆的异步模型训练，并确保系统的安全性。首先，本文介绍了所提方法的工作流程；其次，有针对性地设计了模型选择方法，通过优化模型选择过程以增强所提异步FL方法的鲁棒性；并进一步提出了潜在恶意模型检测方法和车辆信誉评估方法，实时检测潜在的恶意模型，基于此动态地更新车辆信誉值，以识别恶意车辆，增强系统鲁棒性；然后，从概率上详细分析了所提方案的安全性，为各项参数优化提供理论

基础；最后，通过仿真实验验证了本文所提异步鲁棒联邦FL的有效性。未来可针对模型池的缓存优化展开深入研究。

参考文献：

[1] 陈山枝, 胡金玲, 时岩, 等. LTE-V2X车联网技术、标准与应用[J]. 电信科学, 2018, 34(4): 1-11.
CHEN S Z, HU J L, SHI Y, et al. Technologies, standards and applications of LTE-V2X for vehicular networks[J]. Telecommunications Science, 2018, 34(4): 1-11.

[2] 中国信息通信研究院. 车联网白皮书（2023年）[R]. 2023.
China Academy of Information and Communications Technology. Internet of vehicles white paper（2023）[R]. 2023.

[3] HÄFNER B, BAJPAI V, OTT J, et al. A survey on cooperative architectures and maneuvers for connected and automated vehicles[J]. IEEE Communications Surveys & Tutorials, 2022, 24(1): 380-403.

[4] AGBAJE P, ANJUM A, MITRA A, et al. Survey of interoperability challenges in the Internet of vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(12): 22838-22861.

[5] HE Y, HUANG K, ZHANG G Z, et al. Bift: a blockchain-based federated learning system for connected and autonomous vehicles[J]. IEEE Internet of Things Journal, 2022, 9(14): 12311-12322.

[6] QIU C, YAO H P, WANG X F, et al. AI-chain: blockchain energized edge intelligence for beyond 5G networks[J]. IEEE Network, 2020, 34(6): 62-69.

[7] YAO H P, LIU C, ZHANG P Y, et al. Identification of encrypted traffic through attention mechanism based long short term memory[J]. IEEE Transactions on Big Data, 2022, 8(1): 241-252.

[8] 雷波, 刘增义, 王旭亮, 等. 基于云、网、边融合的边缘计算新方案: 算力网络[J]. 电信科学, 2019, 35(9): 44-51.
LEI B, LIU Z Y, WANG X L, et al. Computing network: a new multi-access edge computing[J]. Telecommunications Science, 2019, 35(9): 44-51.

[9] MOU F Y, LOU J, TANG Z Q, et al. Adaptive digital twin migration in vehicular edge computing and networks[J]. IEEE Transactions on Vehicular Technology, 2024, PP(99): 1-16.

[10] 柴浩野. 基于区块链的安全高效车联网数据共享策略研究[D]. 成都: 电子科技大学, 2022.
CHAI H Y. Research on safe and efficient data sharing strategy of Internet of vehicles based on blockchain[D]. Chengdu: University of Electronic Science and Technology of China, 2022.

[11] LIU Y M, YU F R, LI X, et al. Blockchain and machine learning for communications and networking systems[J]. IEEE Communications Surveys & Tutorials, 2020, 22(2): 1392-1431.

[12] XU D H, DING Z Z, HE X, et al. Learning from naturalistic driving data for human-like autonomous highway driving[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(12): 7341-7354.

[13] HE Y, ZHANG Z, YU F R, et al. Deep-reinforcement-learning-based optimization for cache-enabled opportunistic interference alignment wireless networks[J]. IEEE Transactions on Vehicular Technology, 2017, 66(11): 10433-10445.

[14] WANG J D, LIU J J, KATO N. Networking and communications in autonomous driving: a survey[J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1243-1274.

[15] BETZ J, ZHENG H R, LINIGER A, et al. Autonomous vehicles on the edge: a survey on autonomous vehicle racing[J]. IEEE Open Journal of Intelligent Transportation Systems, 2022, 3: 458-488.

[16] XUE T, ZHANG Z Q, MA W N, et al. Nighttime pedestrian and vehicle detection based on a fast saliency and multifeature fusion algorithm for infrared images[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(9): 16741-16751.

[17] FANG Y K, MIN H G, WANG W Q, et al. A fault detection and diagnosis system for autonomous vehicles based on hybrid approaches[J]. IEEE Sensors Journal, 2020, 20(16): 9359-9371.

[18] WU Y Q, LIAO S Q, LIU X, et al. Deep reinforcement learning on autonomous driving policy with auxiliary critic network[J]. IEEE Transactions on Neural Networks and Learning Systems, 2023, 34(7): 3680-3690.

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

[20] NGUYEN D C, DING M, PATHIRANA P N, et al. Federated learning for Internet of Things: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2021, 23(3): 1622-1658.

[21] CHELLAPANDI V P, YUAN L Q, BRINTON C G, et al. Federated learning for connected and automated vehicles: a survey of existing approaches and challenges[J]. IEEE Transactions on Intelligent Vehicles, 2024, 9(1): 119-137.

[22] XING L, ZHAO P C, GAO J P, et al. A survey of the social Internet of vehicles: secure data issues, solutions, and federated learning[J]. IEEE Intelligent Transportation Systems Magazine, 2023, 15(2): 70-84.

[23] MOLLAH M B, ZHAO J, NIYATO D, et al. Blockchain for the Internet of vehicles towards intelligent transportation systems: a survey[J]. IEEE Internet of Things Journal, 2021, 8(6): 4157-4185.

[24] ALAZAB M, RM S P, PARIMALA M, et al. Federated learning for cybersecurity: concepts, challenges, and future directions[J]. IEEE Transactions on Industrial Informatics, 2022, 18(5): 3501-3509.

[25] WANG H, SREENIVASAN K, RAJPUT S, et al. Attack of the tails: yes, you really can backdoor federated learning[J]. arXiv preprint, 2020, arXiv: 2007.05084.

[26] SHAFAHI A, HUANG W R, NAJIBI M, et al. Poison frogs! targeted clean-label poisoning attacks on neural networks[J]. arXiv preprint, 2018, arXiv: 1804.00792.

[27] XU C H, QU Y Y, EKLUND P W, et al. BAFL: an efficient blockchain-based asynchronous federated learning framework[C]// Proceedings of the 2021 IEEE Symposium on Computers and Communications (ISCC). Piscataway: IEEE Press, 2021: 1-6.

[28] CAO M R, ZHANG L, CAO B. Toward on-device federated learning: a direct acyclic graph-based blockchain approach[J]. IEEE Transactions on Neural Networks and Learning Systems, 2023, 34(4): 2028-2042.

[29] 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.

[30] 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.

[31] STALLKAMP J, SCHLIPSING M, SALMEN J, et al. Man vs. computer: Benchmarking machine learning algorithms for traffic sign recognition[J]. Neural Networks, 2012, 32: 323-332.

[作者简介]

尹宏博（1998– ），男，电子科技大学信息与通信工程学院博士生，主要研究方向为算力网络、联邦学习、边缘计算等。

王帅（2001– ），男，电子科技大学信息与通信工程学院硕士生，主要研究方向为算力网络、边缘智能等。

张科（1978– ），男，博士，电子科技大学信息与通信工程学院副教授，主要研究方向为边缘智能网络、智慧车联网、边缘计算等。

张引（1986– ），男，博士，电子科技大学信息与通信工程学院研究员，主要研究方向为移动计算、算力网络、边缘智能等。