结合联邦学习和增强学习的车联网数据差分隐私保护*

邬忠萍[1] 郝宗波[2] 王文静[3] 刘冬[4]

（1.成都工业学院，成都 611730；2.电子科技大学，成都 610054；3.太原师范学院，晋中 030619；4.成都市笛卡科技有限公司，成都 610097）

【摘要】为保证车联网环境下用户数据的安全性和隐私性，提出了结合联邦学习和增强学习的分布式数据差分隐私保护方案。利用联邦学习架构将数据保留在车辆节点或边缘设备上进行学习，通过分布式存储实现数据隐私保护，并减少数据传输开销；基于拉普拉斯机制实现差分隐私，并通过逐层相关传播（LRP）技术管理数据扰动，确保模型参数传递的隐私性和高效率。试验结果表明，所提出的方案在10轮通信内实现了约80%的全局准确度，最高可达98%，能够在消耗较少通信轮数的情况下完成模型聚合，实现了隐私保护和全局数据准确度的较好平衡，且通过增强学习策略准确检测到虚假噪声的注入，能够提升车联网的智能化水平和安全等级。

主题词：车联网 联邦学习 增强学习 差分隐私 拉普拉斯机制 逐层相关传播

中图分类号：U461；TP391 **文献标识码：**A **DOI:** 10.19620/j.cnki.1000-3703.20230294

Differential Privacy Data Protection for Internet of Vehicle by Combining Federated Learning and Reinforced Learning

Wu Zhongping[1], Hao Zongbo[2], Wang Wenjing[3], Liu Dong[4]

（1. Chengdu Institute of Technology, Chengdu 611730; 2. University of Electronic Science and Technology of China, Chengdu 610054; 3. Taiyuan Normal University, Jinzhong 030619; 4. Chengdu Desca Technology Co., Ltd., Chengdu 610097）

【Abstract】To ensure the security and privacy of sensitive data in Internet of Vehicle (IoV) environments, this paper proposed a distributed differential privacy data protection scheme combining federated learning and reinforced learning mechanisms. In this scheme, a federated learning architecture was applied to keep data on vehicle nodes or edge devices for learning, enabling data privacy protection, reducing data transmission costs through distributed storage. The Laplace mechanism was employed to achieve differential privacy, the Layer-wise Relevance Propagation (LRP) was used to manage data perturbation, ensuring the privacy and efficiency of model parameter transmissions. Experimental results show that the proposed scheme can achieve approximately 80% global accuracy within 10 rounds of communication, with a maximum of 98%, can complete model aggregation within less communication rounds, achieving a good balance between privacy protection and global data accuracy, and accurately detecting the injection of false noise through the reinforced learning strategy, promoting the intelligence and security levels of IoV.

Key words: Internet of vehicle, Federated learning, Reinforced learning, Differential privacy, Laplace mechanism, Layer-wise relevance propagation

【引用格式】邬忠萍, 郝宗波, 王文静, 等. 结合联邦学习和增强学习的车联网数据差分隐私保护[J]. 汽车技术, 2023(11): 56-62.
WU Z P, HAO Z B, WANG W J, et al. Differential Privacy Data Protection for Internet of Vehicle by Combining Federated Learning and Reinforced Learning[J]. Automobile Technology, 2023(11): 56-62.

1 前言

近年来，随着物联网（Internet of Things，IoT）设备的普及，交通系统的自动化和智能化水平不断提高[1]。车联网（Internet of Vehicles，IoV）中的车辆通信可提高交通场景感知水平，缓解交通拥堵，减少交通事故[2]。云计

*基金项目：国家自然科学基金项目（61003032）；山西省教改项目（J20220943）。

算、移动边缘计算（Mobile Edge Computing，MEC）等新兴技术也促进了智能交通系统的发展[3]。

IoV中，海量终端节点设备的数据传输会增加网络负荷，延长响应时间。此外，在传统的集中式云解决方案中，由于数据必须发送到云端处理，导致其不能确保用户数据的隐私性[4]。为此，支持分布式架构的联邦学习范式成为研究热点。联邦学习是一种联合学习机制，利用驻留在边缘设备上的数据集对其学习模型进行本地训练，其后将模型参数发送回中央服务器进行聚合，以生成全局模型[5]。联邦学习在IoV中应用的优点包括：灵活处理每辆车不平衡的稀疏数据；满足车联网的扩展性和移动性需求；通过仅发送本地学习的模型参数提高数据隐私性[6]。文献[7]提出了用于车辆间通信的联邦学习架构，并通过极值理论和李雅普诺夫优化降低了资源消耗。文献[8]提出了车联网中联邦学习的数据聚合选择模型，以实现计算资源消耗和图像质量之间的权衡。

在联邦学习架构中，隐私数据始终驻留在边缘节点，但该架构也会面临差分攻击的威胁[9]。为此，近期部分研究尝试在联邦学习架构中开发安全多方计算[10]、可信执行环境[11]，以及基于差分隐私的隐私保护技术。其中，差分隐私技术能够很好地抵御成员推理攻击（Membership Inference Attack，MIA），得到了广泛关注。文献[12]利用差分隐私技术，在基于联邦学习的车联网资源共享过程中提供模型更新参数的隐私保护。文献[13]提出了基于联邦学习和差分隐私的车联网数据个性化隐私保护方案。

尽管差分隐私能够在一定程度上保护数据隐私性，但攻击者可利用差分隐私噪声发起数据投毒攻击或模型投毒攻击，并通过将虚假数据隐藏到差分隐私噪声中来绕过传统的异常检测机制[14]。为此，本文提出增强学习辅助的联邦学习（Reinforced Learning-assisted Federated Learning，RLaFL）方案，将联邦学习架构与差分隐私机制相结合，利用逐层相关传播（Layer-wise Relevance Propagation，LRP）方法增强拉普拉斯机制中的数据扰乱，并提出基于增强学习的防御方法，对边缘节点模型更新过程中的差分隐私等级进行智能化选择。

2 车联网场景模型

2.1 场景建模

图1所示为基于联邦学习的典型系统模型。通过移动设备、边缘设备和中央服务器3个层面的操作来支持智能化交通管理，其中，路侧单元（Round Side Unit，RSU）为边缘节点，通过光纤链路连接并集成了无线终端（WiFi、5G、C-V2X等）和NVIDIA Jetson等计算资源，以支持车辆与其他设备的通信。系统中的车辆节点均配置了车载单元（On-Board Unit，OBU）、全球定位系统（Global Positioning System，GPS）接收器、相机和速度传感器，并可通过图片或视频记录发生的交通事件（如交通拥堵或事故）。OBU通过第五代移动通信技术（5th Generation mobile communication technology，5G）与RSU和其他OBU建立连接，并将移动数据和环境数据发送至数据处理中心（云端）。

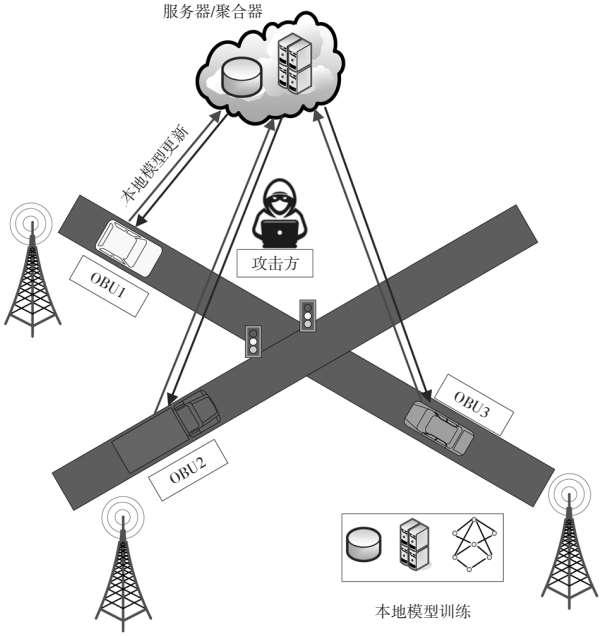

图1 基于联邦学习的车联网场景模型

2.2 联邦学习

联邦学习是一种分布式机器学习范式，由数据持有者和模型持有者（服务器）组成。多个节点和重要服务器利用分布式梯度下降技术进行协作，通过使训练数据集的损失函数最小化实现参数优化。

令D为训练数据集、w为模型训练参数、$L(w,D)$为训练数据集上的损失函数，在N个不同节点上，对个体数据集D_i进行本地训练，每个节点的模型训练参数为w_i，每个节点的损失函数为$L(w_i,D_i)$。则中央服务器的损失函数为[15]：

$$L(w,D)=\frac{\sum_{i=1}^{N}L(w_i,D_i)}{N} \tag{1}$$

联邦学习通常采用基于梯度下降的分布式学习算法，系统训练过程可分为本地更新（训练）、模型聚合、参数广播和模型更新4个步骤。在本地更新阶段，每个边缘节点利用梯度下降算法调整模型参数以实现损失最小化。模型聚合在云端或边缘节点上执行。其后，将更

新后的参数返回每个参与节点，为下一轮迭代作准备。

2.3 攻击模型

基于联邦学习的车联网环境中，车辆节点持有自身与环境的敏感数据，并通过内容缓存减少通信约束和延迟。联邦学习通过本地训练避免将原始数据发送至云端，但模型参数依然会在OBU、RSU与云服务器之间交换，必须确保车辆信息交换的隐私性，防止数据共享和内容缓存过程中的数据泄露。

攻击者可能在车辆节点、边缘节点和服务器端进行伪装。在数据投毒攻击中，攻击者可篡改本地训练数据并伪装为诚实车辆节点。而在模型投毒攻击中，攻击者可能伪装成RSU或服务器，通过入侵通信路径获取模型参数，并向参数中注入假噪声，实现对联邦学习模型的篡改[16]。

本文假定攻击者能够在任何情况下通过中间人攻击或服务器端攻击获取模型更新参数，但无法直接更改服务器上的已有模型。攻击者拥有全局和本地模型参数的全部知识，并可能获取训练和测试数据的数据分布知识。此外，假定攻击者知晓要实施的差分隐私机制和隐私预算。

3 基于联邦学习和增强学习的差分隐私保护

图2给出了本文提出的RLaFL框架流程，主要包括边缘服务和云服务。边缘服务在RSU上执行，使用本地数据对模型进行连续训练，以便满足RSU覆盖区域内的车辆节点的各种预测需求。边缘聚合器是边缘服务的重要组件，向云端发送要聚合的本地模型参数。云服务负责管理边缘模型的聚合过程，接受边缘设备上的模型参数，管理全局模型中的参数聚合过程，直至达到所需的数据准确度。利用该框架，RSU基于采集到的本地数据训练基础模型，并通过预测接口提供预测服务。满足聚合规则时，云服务通知边缘服务进行参数发送，在接收到所有边缘模型后运行聚合算法，并将聚合后的模型发送至边缘服务模块。数据聚合过程不断循环，直至本地模型的数据准确度达到预设阈值。

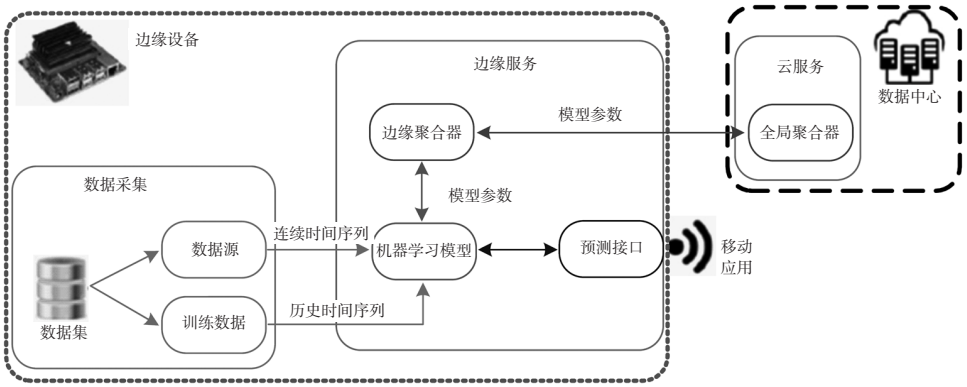

图2 本文框架流程

3.1 联邦平均算法

本文提出的框架使用联邦平均（Federated Average，FedAvg）算法进行模型聚合：

算法1 FedAvg算法

输入：本地批大小B、每次迭代参与节点数量m、本地训练代数E、学习率η

输出：全局模型

For 参与节点i

LT(i,w)　　//LT表示本地训练

将本地数据集D_i分割为大小为B的小批B_i

For 每代本地训练$j\in[1,E]$ **do**

For $b\in B_i$ do

$$w\leftarrow w-\eta\Delta L(w;b)$$

End for

End for

For 云服务器

初始化模型的全局训练参数 w_G^0

For 每次迭代$t\in[1,T]$ **do**

随机选择m个参与节点的子集S_t

For 每个参与节点$i\in S_t$并行执行：

$w_i^{t+1}\leftarrow \mathrm{LT}(i,w_G^t)$ //更新节点i的训练参数

End for

$$w_G^t=\frac{1}{\sum_{i\in N}D_i}\sum_{i=1}^{N}D_i w_i^t$$ //迭代后的全局训练参数

End for

模型训练开始时，云服务器向参与节点发送初始全局模型，并确定客户端数量、批大小、代数、学习率和衰减率。聚合器确定参与节点，并将最新模型广播至参与节点。在接收到全局模型后，参与节点将本地模型修改为共享模型，将数据分为不同批大小，并使用随机梯度下降（Stochastic Gradient Descent，SGD）法执行一定代数的模型训练，其后将新生成的本地模型发送至服务器。

最后,服务器对不同参与节点的本地模型进行加权平均,从而得到新的全局模型。

3.2 基于逐层相关传播的差分隐私

差分隐私通过添加噪声保护统计数据和实时数据。原则上,差分隐私机制旨在使大规模数据集内某条记录或个体的识别概率尽量接近0。通过随机化算法消除数据集中特定数值的统计显著性。由此,即使攻击者获取了某条查询的输出信息,也无法将该信息与特定个体相关联。

本文利用拉普拉斯机制实施基于差分隐私的数据扰动。令2个相邻数据集D和D'之间仅有单个成员差异,则差分隐私的形式化定义如下:

对于任意2个相邻数据集D和D',令输出的任意子集$S\subseteq Range(\boldsymbol{R})$,其中,$Range(\ )$为区间集合函数,$\boldsymbol{R}$为随机化算法。若以下条件成立[17]:

$$P_r[\boldsymbol{R}(D)\in S]\leqslant e^{\varepsilon}\times P_r[\boldsymbol{R}(D')\in S] \tag{2}$$

则$\boldsymbol{R}$满足隐私预算损失ε-差分隐私条件P_r。其中,ε决定隐私预算水平,其数值越小,则隐私性越强。

在差分隐私中,灵敏度指添加随机噪声后引起的结果不确定性与数据原始形式相比的信息损失,其大小由单个记录对该函数输出的最大更改确定。敏感度决定了应对数据施加的扰动量。全局敏感度表示2个相邻数据集(D和D')的查询输出之间的最大可能差异。对于随机查询$f:D\rightarrow\boldsymbol{R}$,$f$的$L_1$全局敏感度计算为:

$$\Delta f=\max_{D,D'}\left\|f(D)-f(D')\right\| \tag{3}$$

本文提出的方案在差分隐私中使用的LRP算法为:

算法2 分层相关传播LRP

输入:预测得分

输出:相关得分

Procedure 计算相关得分

For 每个网络层l **do**

$\boldsymbol{R}^{l}=l\rightarrow LRP(\boldsymbol{R}^{l-1})$

End for

End Procedure

LRP旨在估计不同特征对机器学习模型的输出层的影响,即分析每层的每个神经元对整个神经网络模型输出的作用。前向传播的最终输出可视为数据聚合的总相关度,用于估计网络每层神经元与输入层的相关度。LRP利用预设的传播规则在神经网络中进行反向预测传播[18]。本文方案中,差分隐私通过扰乱训练数据提高数据隐私性,LRP则用于确定在神经网络中执行扰动处理的数据点。

3.3 基于增强学习的防御策略

本文提出的框架通过加入基于LRP的差分隐私机制提高了用户数据隐私性,但差分隐私机制并不能抵御虚假数据注入或投毒攻击。为了在隐私性、效用和安全性之间实现平衡,本文开发了基于增强学习的辅助防御策略,帮助联邦学习模型选择最优隐私预算水平。

增强学习是一种自适应的机器学习算法,基于最优动作集搜索和延迟奖励机制实现反馈回路,可在无需任何监督的情况下提供智能支持[19]。令A={increase, decrease, static}为动作空间,假定智能体受事件驱动进行决策制定。通过观察联邦环境的当前状态,智能体执行动作集A中的某个决策。为促进智能体决策过程,假定智能体能够在多个步骤中增加或减少隐私预算损失ε。

增强学习通过设计奖励函数使智能体基于学习目标进行决策制定。为防御投毒攻击,智能体必须将攻击成功率最小化,同时最大限度增加模型整体预测准确度。智能体的奖励函数定义为:

$$\beta=\delta_1\frac{L_p^{\max}}{L_p}+\delta_2\frac{L_{FL}^{\max}}{L_{FL}}+\delta_3\frac{1}{\varepsilon} \tag{4}$$

式中,L_p、L_{FL}分别为当前状态中投毒攻击损失和联邦学习模型损失;$L_p^{\max}$、$L_{FL}^{\max}$分别为投毒攻击损失和联邦学习模型损失的最大值;δ_1、δ_2、δ_3为平衡参数。

本文利用Epsilon贪婪策略[20]确定探索和利用之间的权衡。Epsilon贪婪策略是一种基于价值估计的权重调整策略。在每个时间步,Epsilon贪婪策略以概率φ选择一个随机动作,以探索新的状态和动作,而以概率$(1-\varphi)$选择当前状态下估计价值最高的动作,以利用已有的知识。本文将初始探索概率设置为1.0,并逐渐降低探索概率,直至最小探索概率0.05。

4 试验验证

本文通过试验分析所提出的RLaFL方案的通信效率、隐私保护和安全性能,并通过测试台开展仿真分析。

4.1 数据集

使用MNIST数据集[21]分析本文提出的方案在图像分类任务中的性能。MNIST是模式识别领域广泛使用的基准数据集,数据集样本为28×28灰度图像的手写数字,训练样本和测试样本数量分别为60 000个和10 000个。将该数据集分割为10份,代表10个客户端节点。在应用联邦学习后,在10个客户端上进行本地训练,并在聚合器中完成全局聚合。

此外,基于ATCLL数据集[22]搭建测试台,评估所提出的方法在现实场景中的表现。ATCLL包含智能城市

中大量用于通信、感知和计算的IoT设备。其中包含44个集成了通信终端和嵌入式计算平台的边缘节点。

4.2 硬件平台

本文试验中，服务器配置了Intel Core i5-12400F@2.5 GHz CPU、12 GB显存的NVIDIA Geforce RTX 3060 GPU、16 GB RAM、Windows 10的64位操作系统，使用Python 3.8.8和PyTorch 1.5.1作为实现本文算法的编程语言和深度学习框架。

此外，在测试台仿真中，使用20个小型计算机Jetson Nano，通过局域网连接到服务器作为边缘设备，Jetson Nano的处理器为4核心的Arm Cortex A57，配置2 GB RAM，操作系统为Ubuntu 18.04.5 LTS。

4.3 试验结果

图3所示为RLaFL方法在MNIST数据集上的全局准确度随通信轮数的变化情况。在数据类型方面，MNIST数据集为手写数字图像数据集，在IoV隐私保护试验中，也使用图像数据进行隐私保护，因此数据类型一致。在数据分布方面，MNIST数据集中的手写数字图像是由多人手写而成，具有一定的数据分布特征，数据集中不同数字的出现频率相对平均，且图像的背景和噪声也相对均衡，符合IoV场景下来自不同车辆的图像数据的数据分布特征。由于车辆节点存在计算资源限制，隐私保护方案必须在较少通信轮数下实现较好的准确度，以促进现实车联网应用。由图3可知：本文方法在10轮通信内实现了约80%的全局准确度；随着通信轮数的增加，全局准确度不断上升，最高达到98%。该试验中将通信轮数限制在100轮以内，因为在车联网场景下，过高的通信轮次会显著增加计算负担，影响系统整体性能。

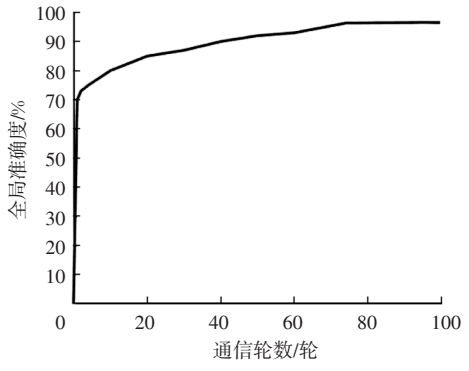

图3 不同通信轮数下的模型预测准确度

图4所示为本文方法与文献[8]和文献[12]的方法的性能比较结果。其中，文献[8]的联邦学习方法未应用任何差分隐私机制，文献[12]的方法在本地完成差分隐私损失ε的选择，RLaFL方案利用LRP在差分隐私环境中选择ε。应用差分隐私机制能够显著提升用户敏感信息的安全性，但需要尽量减少全局准确度的下降。由图4可知：文献[8]的全局准确度保持不变，但不能抵御MIA攻击；文献[12]的全局准确度随ε的减小而显著下降；RLaFL方法使用LRP技术，在不同ε（即不同的隐私保护等级）下均取得了较为合理的全局准确度。

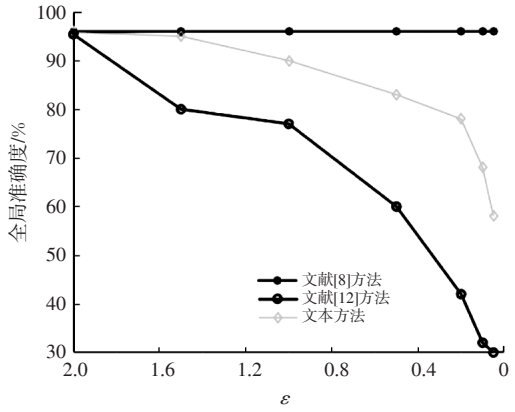

图4 不同隐私保护等级下的全局准确度

为分析本文提出的增强学习策略对模型安全性能的影响，在差分隐私机制中加入恶意噪声，即为模拟攻击者行为，将差分隐私机制中的高斯分布噪声替换为攻击分布噪声，以模拟模型投毒攻击。图5所示为本文方法在MNIST数据集上的防御智能体的累计奖励。从图5中可以看出，随代数增加，智能体能够学习到最优策略，并在一定的执行代数后实现收敛。本文增强学习策略中，奖励函数的定义考虑到了联邦学习模型损失、攻击者损失和隐私损失，因此模型收敛意味着所提出的方案寻找到了隐私性、安全性和效用之间的最优权衡。智能体会为每个状态输出一个动作（或ε），由此可计算该状态下的联邦学习损失的标准值。基于该标准值，若观察到的实际联邦学习损失值出现较大偏差，意味着检测到可能的模型投毒攻击。由此证明，增强学习策略显著提高了模型对主动攻击的安全防护能力。

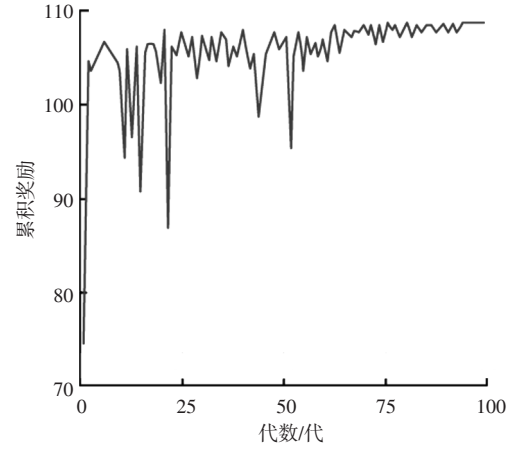

图5 不同代数下的累积奖励值

4.4 测试台实施

使用Jetson Nano作为边缘设备,在实验室内搭建测试台,基于ATCLL数据集,评估本文方案在现实车联网场景中的应用性能。ATCLL数据集是基于真实场景的车联网数据集,由多个传感器在真实交通环境中采集而成,包含了大量的车辆行驶数据、交通信号数据、道路信息数据等,使用该数据集可以更好地模拟真实交通环境,从而验证算法的有效性和性能。Jetson Nano通过1 Gbit/s的无线局域网连接到服务器,服务器负责聚合分布在边缘设备上的机器学习模型。表1给出了不同边缘节点和客户端数量条件下,本文模型达到最优准确度时,所有客户端连接到服务器的平均时长、每轮运行平均时长,以及服务器完成10轮聚合后得到全局模型的平均时长,所有测试均取10次测试均值。由表1可知,本文方法的扩展性较好,当客户端数量达到200台时,系统每轮的平均运行耗时仅为15.28 s,能够满足现实车联网应用需求。每个边缘设备服务的客户端达到14个时,系统耗时会大幅增加。但在现实车联网场景中,以将智能路灯作为RSU为例,每个边缘设备所服务的车辆通常不超过10辆,表明所提出的方法的效率符合现实车辆网应用需求。

表1 不同边缘设备和客户端数量条件下的系统耗时

Jetson Nano数量/台	客户端总数量/台	连接时间/s	每轮运行耗时/s	总时长/s
1	1	13.57	1.35	26.74
5	5	39.28	1.51	55.83
5	25	61.35	4.88	121.05
5	50	177.39	11.01	272.16
5	70	422.33	24.14	680.96
10	100	195.72	14.48	305.77
10	140	580.19	34.62	765.33
20	200	231.22	15.28	324.51
20	280	701.33	39.44	875.20

图6所示为不同轮数和不同客户端数量条件下测试台仿真中服务器的模型聚合耗时情况。由图6可知,随着客户端数量的增加,服务器的模型聚合时长出现了小幅度增加。当客户端数量达到70个时,平均聚合时间低于0.15 s,即使客户端数量达到280个,系统的平均聚合时间仍低于0.25 s,表现出良好的可扩展性,证明了本文提出的方案具有较好的可扩展性。

图7所示为使用1台Jetson Nano作为边缘设备,在服务器和客户端之间进行10次模型传输的平均时间评估结果。由图7可知,本文方法可实现毫秒级的模型参数上传和下载,能够满足现实车联网的通信延迟要求。

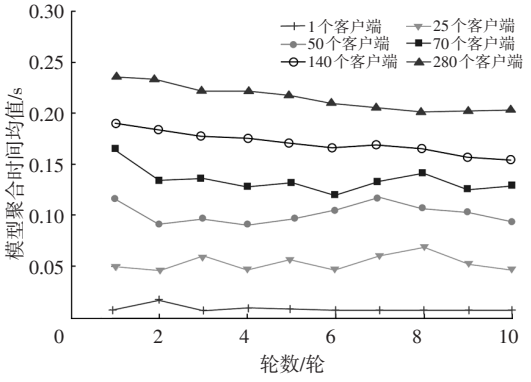

图6 服务器的模型聚合平均耗时

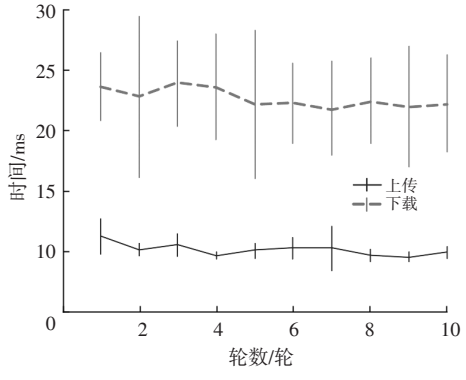

图7 模型上传和下载耗时

5 结束语

本文提出了结合联邦学习和增强学习的车联网数据差分隐私保护方案,通过联邦学习范式实现分布式架构,利用结合LRP的差分隐私机制提高敏感数据的隐私性,并通过增强学习辅助的安全策略实现对模型投毒攻击的检测和防御。试验结果表明,所提出的方法在隐私性、安全性和效率之间实现了较好平衡,处理速度和通信延迟能够满足现实车联网应用需求。未来,将尝试进一步优化模型,并将所提出的方案部署在嵌入式车载单元上,在真实车载网络环境中测试方案的信息安全鲁棒性。

参 考 文 献

[1] 程翔, 张浩天, 杨宗辉, 等. 车联网通信感知一体化研究: 现状与发展趋势[J]. 通信学报, 2022, 43(8): 188-202.
CHENG X, ZHANG H T, YANG Z H, et al. Integrated Sensing and Communications for Internet of Vehicles: Current Status and Development Trend[J]. Journal on Communications, 2022, 43(8): 188-202.

[2] 王晶晶, 郭文博, 张友松, 等. 基于车联网的行人主动避撞策略及仿真验证[J]. 汽车技术, 2022(5): 41-49.
WANG J J, GUO W B, ZHANG Y S, et al. Simulation and Verification of the Control Strategies for Pedestrian Active

Collision Avoidance System Based on V2XP[J]. Automobile Technology, 2022(5): 41-49.

[3] 莫瑞超, 许小龙, 何强, 等. 面向车联网边缘计算的智能计算迁移研究[J]. 应用科学学报, 2020, 38(5): 779-791.
MO R C, XU X L, HE Q, et al. Intelligent Computing Offloading for Internet of Vehicles in Edge Computing[J]. Journal of Applied Sciences, 2020, 38(5): 779-791.

[4] AL-SHAREEDA M A, ANBAR M, MANICKAM S, et al. Towards Identity- Based Conditional Privacy- Preserving Authentication Scheme for Vehicular Ad Hoc Networks[J]. IEEE Access, 2021, 9(1): 113226-113238.

[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] LI Y F, GUO Y J, ALAZAB M, et al. Joint Optimal Quantization and Aggregation of Federated Learning Scheme in VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(10): 19852-19863.

[7] SAMARAKOON S, BENNIS M, SAAD W, et al. Federated Learning for Ultra- Reliable Low- Latency V2V Communications[C]// 2018 IEEE Global Communications Conference (GLOBECOM). Abu Dhabi, United Arab Emirates: IEEE, 2018: 1-7.

[8] YE D D, YU R, PAN M, et al. Federated Learning in Vehicular Edge Computing: A Selective Model Aggregation Approach[J]. IEEE Access, 2020, 8(1): 23920-23935.

[9] 陈兵, 成翔, 张佳乐, 等. 联邦学习安全与隐私保护综述[J]. 南京航空航天大学学报, 2020, 52(5): 675-684.
CHEN B, CHENG X, ZHANG J L, et al. Survey of Security and Privacy in Federated Learning[J]. Journal of Nanjing University of Aeronautics & Astronautics, 2020, 52(5): 675-684.

[10] LI Y, ZHOU Y P, JOLFAEI A, et al. Privacy-Preserving Federated Learning Framework Based on Chained Secure Multiparty Computing[J]. IEEE Internet of Things Journal, 2020, 8(8): 6178-6186.

[11] CHEN Y, LUO F, LI T, et al. A Training-Integrity Privacy-Preserving Federated Learning Scheme with Trusted Execution Environment[J]. Information Sciences, 2020, 522(1): 69-79.

[12] LU Y L, HUANG X H, DAI Y Y, et al. Differentially Private Asynchronous Federated Learning for Mobile Edge Computing in Urban Informatics[J]. IEEE Transactions on Industrial Informatics, 2019, 16(3): 2134-2143.

[13] 徐川, 丁颖祎, 罗丽, 等. 车联网中基于位置服务的个性化位置隐私保护[J]. 软件学报, 2022, 33(2): 699-716.
XU C, DING Y Y, LUO L, et al. Personalized Location Privacy Protection for Location- Based Services in Vehicular Networks[J]. Journal of Software, 2022, 33(2): 699-716.

[14] LECUYER M, ATLIDAKIS V, GEAMBASU R, et al. Certified Robustness to Adversarial Examples with Differential Privacy[C]// 2019 IEEE Symposium on Security and Privacy (SP). San Francisco, CA, USA: IEEE, 2019: 656-672.

[15] 莫慧凌, 郑海峰, 高敏, 等. 基于联邦学习的多源异构数据融合算法[J]. 计算机研究与发展, 2022, 59(2): 478-487.
MO H L, ZHENG H F, GAO M, et al. Multi- Source Heterogeneous Data Fusion Based on Federated Learning [J]. Journal of Computer Research and Development, 2022, 59(2): 478-487.

[16] TOLPEGIN V, TRUEX S, GURSOY M E, et al. Data Poisoning Attacks Against Federated Learning Systems[C]// Computer Security - ESORICS 2020: 25th European Symposium on Research in Computer Security. Guildford, UK: IEEE, 2020: 480-501.

[17] WEI K, LI J, DING M, et al. Federated Learning with Differential Privacy: Algorithms and Performance Analysis [J]. IEEE Transactions on Information Forensics and Security, 2020, 15(1): 3454-3469.

[18] GREZMAK J, ZHANG J J, WANG P, et al. Interpretable Convolutional Neural Network through Layer- Wise Relevance Propagation for Machine Fault Diagnosis[J]. IEEE Sensors Journal, 2019, 20(6): 3172-3181.

[19] 章航嘉, 谢志军. 基于强化学习的车联网隐私保护和资源优化策略[J]. 传感技术学报, 2022, 35(8): 1073-1079.
ZHANG H J, XIE Z J. Privacy Protection and Resource Optimization Strategies for Internet of Vehicles Based on Reinforcement Learning[J]. Chinese Journal of Sensors and Actuators, 2022, 35(8): 1073-1079.

[20] MOWLA N I, TRAN N H, DOH I, et al. AFRL: Adaptive Federated Reinforcement Learning for Intelligent Jamming Defense in FANET[J]. Journal of Communications and Networks, 2020, 22(3): 244-258.

[21] LI B B, JIANG Y K, SUN W B, et al. FedVANET: Efficient Federated Learning with Non- IID Data for Vehicular Ad Hoc Networks[C]// 2021 IEEE Global Communications Conference (GLOBECOM). Madrid, Spain: IEEE, 2021.

[22] VÍTOR G, RITO P, SARGENTO S. Smart City Data Platform for Real-Time Processing and Data Sharing[C]// 2021 IEEE Symposium on Computers and Communications (ISCC). Athens, Greece: IEEE, 2021.

（责任编辑　斛　畔）
修改稿收到日期为2023年6月9日。