

FL-IoV: 基于联邦学习的综合车联网入侵检测方法

蒋玉长, 蒋利兵, 黄凯

(北京银联金卡科技有限公司深圳分公司, 广东 深圳 518049)

摘要: 现有车联网入侵检测系统面临计算开销过大及数据隐私限制两大挑战, 难以高效部署与保障隐私。为此, 提出一种基于联邦学习架构的车联网入侵检测方法FL-IoV, 旨在于分布式边缘设备上协作完成检测任务, 同时降低数据隐私泄露风险。通过将车载通信流量转化为图像并利用定制轻量级模型 MobileNet-Tiny 提取特征, FL-IoV 在保证检测准确性的同时, 可部署于资源受限设备。经在公开数据集 Car-Hacking 上验证, FL-IoV 在本地环境和联邦环境下分别实现 99.17% 和 98.51% 的检测准确率, 且在 Raspberry Pi 4 低算力设备上保持每个样本预测时间低于 10 ms, 表现出比现有方法更优的准确率和实时性。FL-IoV 为车联网安全提供了一种既高效又保护隐私的入侵检测方案。

关键词: 车联网; 入侵检测; 联邦学习; 深度学习; 隐私保护

中图分类号: TN915

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025047

FL-IoV: comprehensive intrusion detection method for internet of vehicles based on federated learning

JIANG Yuchang, JIANG Libing, HUANG Kai

Beijing Unionpay Card Technology Co., Ltd., Shenzhen Branch, Shenzhen 518049, China

Abstract: Existing intrusion detection systems in the Internet of vehicles (IoV) were faced with two major challenges: excessive computational overhead and data privacy constraints, which had hindered efficient deployment and privacy protection. To address these issues, an IoV intrusion detection method based on a federated learning architecture, named FL-IoV, was proposed. It was designed to collaboratively accomplish detection tasks on distributed edge devices while the risk of data privacy breaches was reduced. Vehicular communication traffic within the IoV was converted into images, and a customized lightweight model, MobileNet-Tiny, was utilized to extract features, ensuring detection accuracy and enabling deployment on resource-constrained devices. When validated on the publicly available Car-Hacking dataset, FL-IoV achieved detection accuracies of 99.17% and 98.51% in local and federated IoV environments, respectively, and a per-sample prediction time of under 10 milliseconds was maintained on low-power devices such as the Raspberry Pi 4. These results demonstrate superior accuracy and real-time performance of FL-IoV compared to existing methods in IoV security. The successful application of FL-IoV provides an efficient and privacy-preserving new solution for IoV security.

Keywords: Internet of vehicles, intrusion detection, federated learning, deep learning, privacy protection

收稿日期: 2025-02-08; 修回日期: 2025-05-08

引用格式: 蒋玉长, 蒋利兵, 黄凯. FL-IoV: 基于联邦学习的综合车联网入侵检测方法[J]. 网络与信息安全学报, 2025, 11(4): 127-140.

Citation Format: JIANG Y C, JIANG L B, HUANG K. FL-IoV: comprehensive intrusion detection method for internet of vehicles based on federated learning[J]. Chinese Journal of Network and Information Security, 2025, 11(4): 127-140.

0 引言

随着智能汽车产业的蓬勃发展,车联网(Internet of vehicles, IoV)作为交通关键信息基础设施的重要组成部分,正逐渐成为黑客攻击的目标。车联网是由车辆、无线网络及其他单元相互连接构成的开放集成网络系统,是现代智能汽车的核心通信方式^[1]。随着针对车联网的网络攻击日益增多,人们对车联网安全性的担忧也日益加深。

近年来,深度学习技术在入侵检测领域获得了广泛应用^[2-7]。深度学习方法的核心流程如下:首先采集充足的网络流量数据包,继而通过对数据包的分析提取特征向量,将其作为分类模型的输入,最终通过训练深度学习模型构建出入侵检测分类器。与传统的基于签名匹配和机器学习的检测方法相比,深度学习方法的检测准确率得到了显著提升。

本文提出一种适用于车联网环境的综合入侵检测架构 FL-IoV。首先,针对当前基于深度学习的入侵检测方法在计算资源有限平台上难以部署及 IoV 数据隐私问题,本文采用联邦学习技术实现用户数据隐私保护。其次,在 FL-IoV 框架下,将车载通信流量数据转换为彩色图像表征,并通过优化剪枝设计轻量级 MobileNet-Tiny 神经网络模型,在保障检测准确率的同时有效缩减计算时延。最后,在树莓派设备上使用一个真实车载网络数据集开展实验验证,模拟了实际车载环境下的系统性能表现。

本文创新点与贡献如下。

1) 提出创新性预处理技术,将车载通信流量数据转换为图像表征,充分利用卷积神经网络(convolutional neural network, CNN)在图像处理领域的天然优势。基于该技术,设计了经优化剪枝的 MobileNet-Tiny 轻量级模型,在保证高检测准确率的同时实现实时响应能力,有效适配车载系统的计算资源约束条件。

2) 构建一种新型车联网入侵检测框架 FL-IoV。该框架基于联邦学习机制,通过多个独立同构的深度训练模型聚合形成综合检测模型。FL-IoV 支持客户端本地数据独立处理,从架构层面有效规避数据集中传输带来的隐私泄露风险。

3) 不仅完成模型的理论构建,还在低成本、计算资源受限设备上开展实验进行验证,采用真实车载网络数据集对 FL-IoV 架构的实际性能与可行性进行系统性测试。该验证过程充分彰显了 FL-IoV 的场景适配能力,为车联网真实应用环境提供了兼具技术可行性与成本效益的入侵检测解决方案。

1 相关工作

随着人工智能技术的蓬勃发展,尤其是深度学习领域的前沿进展,基于深度学习的车联网入侵检测方法已成为研究焦点。该类方法依托其卓越的数据特征提取与复杂模式识别能力,为车联网系统潜在安全威胁的检测与防御提供了强有力的技术方案。

在这一技术背景下,车联网环境中涌现的多种安全威胁,如恶意软件渗透、分布式拒绝服务(distributed denial of service, DDoS)攻击、伪造数据注入及隐私泄露等,已成为研究者借助深度学习技术探索解决方案的重点对象^[8]。Lo 等^[9]提出了一种基于 CNN 和 LSTM 构建的车载入侵检测系统 HyDL-IDS,该系统由 CAN 流量预处理器与 HyDL 检测器构成。CAN 流量预处理器先将捕获的 CAN 流量转换为统一尺度格式,再输入 HyDL 模块;HyDL 检测器通过提取流量中的空间与时间特征,结合深度学习方法实现流量分类。Javed 等^[10]将 CNN 与基于注意力的门控递归单元(attention-based gated recurrent unit, AGRU)相结合,提出了一种名为 CANintelliIDS 的入侵检测方法,其检测模型由 3 个 AGRU 层和 2 个 CNN 层组成,先将数据点转换为向量序列并输入 CNN 层进行特征提取,再通过 AGRU 学习序列依赖关系以动态调整权重,最终利用注意力机制分配数据点权重并生成上下文向量完成标签预测。

联邦学习作为一种解决孤立数据的有效技术,自 2016 年被提出以来^[11],引起了众多研究者的广泛关注。该技术支持多方机构在不共享数据的基础上实现模型协同,有效保障用户数据隐私安全。

如图 1 所示,经典分布式联邦学习架构以中央服务器为枢纽。各参与节点仅利用本地数据

集独立训练机器学习模型，生成模型参数更新（如权重调整值或梯度计算结果）。这些更新随后被安全地传输至中央服务器，由其作为汇总节点，采用特定策略（如加权平均算法）整合多个客户端的参数更新。整合完成后，服务器将全局模型参数更新广播至各参与节点，各参与节点据此进一步优化本地模型，实现模型的全局同步与性能提升。

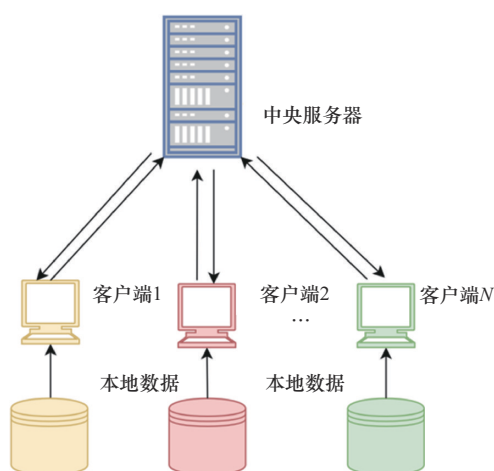


图1 联邦学习架构

Figure 1 Federated learning framework

表1为不同车联网入侵检测方法的优势和局限性对比。

综上，基于深度学习的入侵检测方法虽能提升检测准确率，但面临计算和存储资源需求高、集中式训练隐私泄露风险高等问题，难以满足车联网场景的隐私保护需求。当前尚未出现兼具高准确率、低时延、轻量级部署及隐私保护能力的综合性车联网入侵检测方案。尽管

联邦学习技术在物联网边缘计算与隐私保护领域已取得一定进展，但其在车联网入侵检测中的应用仍处于探索阶段，尤其考虑到车载设备的性能限制及用户隐私保护的迫切需求，联邦学习技术在车联网领域具备显著的研究价值与广阔的应用前景。

2 FL-IoV方法

2.1 整体架构

本文提出的基于联邦学习的车联网入侵检测方法FL-IoV的整体框架如图2所示，该框架主要由可信权威机构、云服务器和客户端3部分组成。

可信权威机构：负责提供公钥与私钥，该公私钥对用于客户端与云服务器在训练过程中的安全通信。因此，可以在客户端和服务端之间建立一个参数更新的安全通道，确保客户端私有数据在传输与交互过程中的安全性。

云服务器：作为模型聚合的核心节点，通过与各客户端进行模型参数交换，收集并整合多个客户端的局部模型更新，构建全局入侵检测模型。

客户端：每个客户端代表一个本地入侵检测模型，承担本地数据集收集、数据预处理、本地模型训练任务。客户端完成局部模型训练后，在加密条件下与云服务器交互更新模型参数。

联邦学习涵盖参数上传、下发、传输及模型聚合等多个阶段。联邦学习尽管不直接交换原始数据，相比传统的集中式机器学习训练具备更高的隐私保障，但联邦学习自身并未提供全面的隐

表1 不同车联网入侵检测方法对比

Table 1 Comparison of different intrusion detection methods in the internet of vehicles

方法类别	代表方法	优势	局限性
传统方法	基于签名、机器学习	计算开销小，对已知攻击模式检测效率高	依赖先验知识，无法识别新型攻击；特征工程复杂导致泛化能力受限
集中式深度学习	CNN、LSTM、ViT	自动特征提取能力突出，对复杂攻击模式具备高检测准确率	需集中数据训练，隐私泄露风险大；模型参数量庞大，难以部署至边缘设备
混合深度学习	HyDL-IDS	结合时空特征提取，提升对序列化攻击的检测能力	多模型融合带来计算复杂度的激增，导致实时检测性能显著下降
联邦学习框架	DeepFed	分布式训练保护数据隐私，适用于多机构协作场景	通信开销大，模型聚合过程中存在梯度信息泄露风险

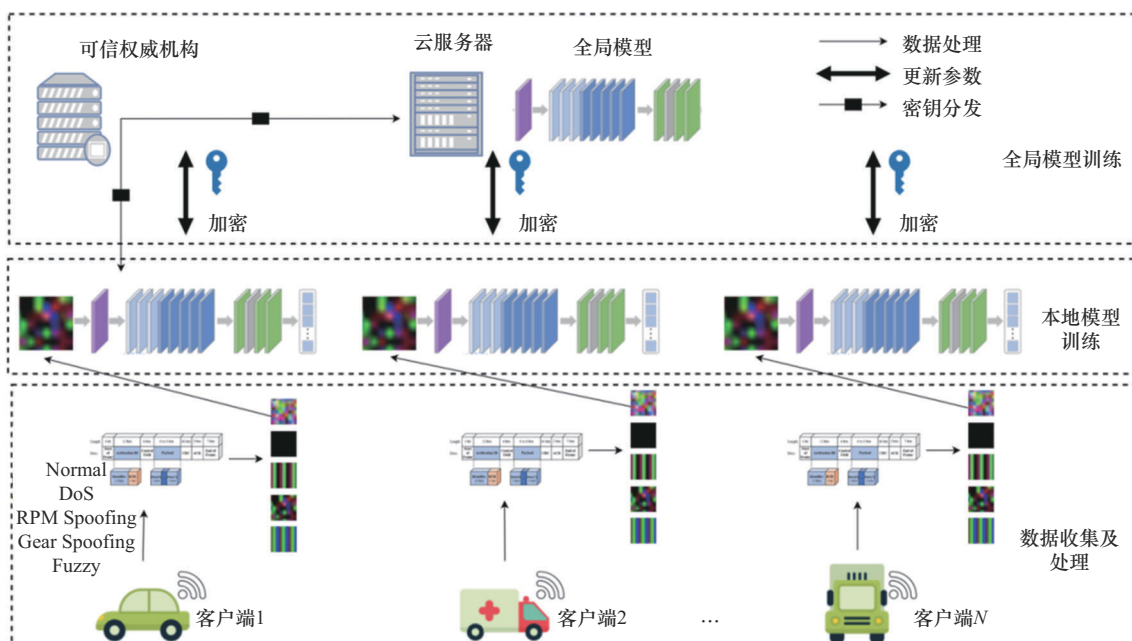


图2 FL-IoV 整体架构

Figure 2 Overall architecture of FL-IoV

私保护机制，仍面临信息泄露风险。这种风险源于模型训练过程中内在脆弱性与攻击者的技术能力。基于此，本文重点分析以下两类以窃取数据、破坏模型隐私性和机密性为目标的隐私攻击。

1) 客户端参数上传阶段的中央服务器攻击：当客户端完成本地模型训练向中央服务器上传参数时，中央服务器作为参数收集与聚合的核心节点，可利用其权限发起原始数据重建攻击以恢复目标终端的原始训练数据，或者发起敏感属性推断攻击以推断目标终端的训练数据是否包含敏感属性。

2) 全局参数下发阶段的不可信终端攻击：当中央服务器完成参数聚合向终端下发全局模型时，不可信终端可利用接收到的全局参数发起类别样本重建攻击，或发起个体敏感属性关联攻击以推断其他终端数据中的敏感属性。

针对上述两类典型的隐私泄露场景，其核心风险均源于上传与下发环节的中间参数泄露。为此，本文提出可信权威机构与同态加密 (homomorphic encryption, HE) 协同的增强型隐私保护架构。该方案通过密码学实现数据全生命周期的隐私保障：客户端可将本地训练参数进行同态加密后上传至云服务器，云服务器直接在加密的数

据上执行特定运算，全程无须接触任何明文数据。当计算任务完成后，客户端通过可信权威机构颁发的密钥解密得到的结果与明文环境下的运算结果完全一致。

云服务器和客户端属于半诚实的一方且严格遵守规定。

2.2 数据预处理

2.2.1 数据描述

控制器局域网 (controller area network, CAN) 总线是当前汽车领域应用最广泛的车内通信协议，其采用总线拓扑结构实现电子控制单元 (electronic control unit, ECU) 间的信息交互，支持转向控制、转速调节等关键信号的实时传输。该协议通过预先定义的帧格式实现节点间的广播通信，CAN 帧格式如图 3 所示，各字段从左往右依次为：帧起始 (Start of Frame)、仲裁 ID (Arbitration ID)、控制字段 (Control Field)、数据字段 (Payload)、循环冗余校验 (CRC)、确认字段 (ACK) 和帧结束字段 (End of Frame)。其中，CAN 标识符 (ID) 和 8 字节数据字段承载的是通信流量的关键特征。

2.2.2 数据转换

受 CAN 工作原理及 CNN 在图像分类任务中优越性能的启发，本文提出了一种全新的数据转

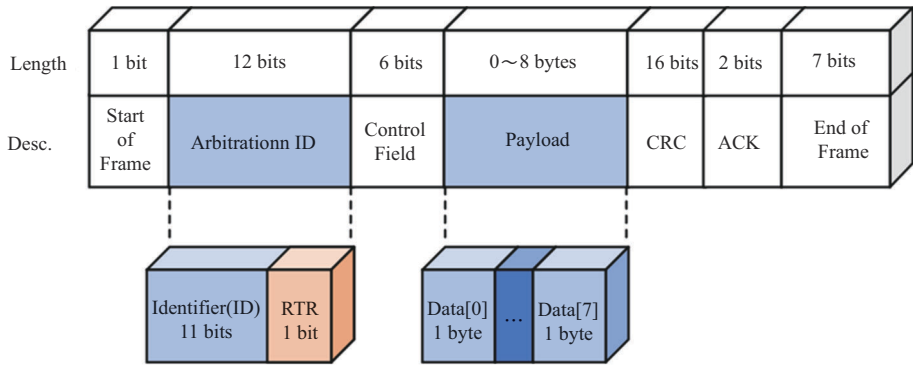


图3 CAN帧格式

Figure 3 CAN frame format

换方法。该方法通过解析CAN报文中数据字段的特征模式，将数据字段映射为灰度图像矩阵，一旦攻击者注入消息，数据字段中的模式就会被破坏，因此，通过数据字段，模型能够捕获不同类别数据包的特征并进行精准分类。此外，将CAN报文转为灰度图像后，原数据字段的明文内容不再以结构化形式传输。与传统基于原始字段训练的方法相比，此方法使攻击者仅能获取图像像素值，而无法直接通过字段解析关联车辆实时状态。

具体而言，本方法以表2中的原始数据为基

础，通过精细化拆分与重组，构建出如表3所示的包含9个特征维度的新型数据集。在此过程中，CAN ID保持不变，而原数据包中8字节数据字段（Data）被拆分为8个独立子字段（D0~D7），每个子字段对应数据帧中的一个字节，且每个字节以两个十六进制数值表示。为了后续处理的便利性与高效性，本文将这些十六进制数值逐一转换为十进制数值，随后对整个数据集实施归一化处理，以确保所有特征值均处于同一量级，便于模型学习。

本文通过上述转换策略，不仅将原本复杂的

表2 原始数据
Table 2 Original data

数据集	时间戳	ID	DLC	数据字段	标签
Car-Hacking	1479121434.85022	0350	8	05 28 84 66 6d 00 00 a2	0
	1478191110.35041	0316	8	45 29 24 ff 29 24 00 ff	1
	1478193258.15421	043f	8	01 45 60 ff 29 00 00 00	2
	1478198408.90276	0000	8	00 00 00 00 00 00 00 00	3
	1478195880.83481	062e	8	95 5f 01 e7 19 47 2e 12	4

表3 拆分后数据
Table 3 Split data

ID	数据字段								标签
	D0	D1	D2	D3	D4	D5	D6	D7	
0.013	0.019	0.110	0.518	0.400	0.427	0	0	0.635	0
0.012	0.267	0.161	0.141	1	0.161	0.141	0	1	1
0.017	0.004	0.270	0.376	1	0.420	0	0	0	2
0	0	0	0	0	0	0	0	0	3
0.024	0.0584	0.373	0.004	0.900	0.980	0.278	0.18	0.071	4

网络流量数据以更直观、更容易被 CNN 模型捕捉的形式呈现出来,还为车载网络入侵检测提供了一种全新的视角与解决方案。

经过数据归一化处理后,本方法将网络流量数据集中的时间戳 (Timestamp) 与特征维度重构为数据块。数据集包含 9 个核心特征 (CAN ID 与 D0~D7 字节)。选取 27 个连续样本,将每个样本的 9 维特征转换为形状为 $9 \times 9 \times 3$ 的三通道彩色图像 (即每个图像由 27 个样本按时间序列堆叠形成 3 个 9×9 特征平面,共包含 243 个特征值)。这种转换方法保留了原始网络数据的时间序列相关性。根据数据块中的攻击模式对图像进行标记,正常样本图像标记为“正常”,包含攻击样本的图像标记为该数据块中占比最高的攻击类型。例如,若某图像对应的 27 个样本中 DoS 攻击占比最高,则该图像标记为 DoS 攻击。

此外,考虑到原始 $9 \times 9 \times 3$ 图像维度较小,为避免模型在训练过程中出现过拟合,本方法采用双线性插值法将图像尺寸扩大至 $224 \times 224 \times 3$ 。双线性插值通过二维空间内的 4 次线性插值实现像素值估计,其数学原理如下。假设 $f(x, y_1)$ 为待求 (x, y) 数据点的像素值,已知 $f(Q_{11})$ 、 $f(Q_{12})$ 、 $f(Q_{21})$ 、 $f(Q_{22})$ 分别为 (x_1, y_1) 、 (x_1, y_2) 、 (x_2, y_1) 、 (x_2, y_2) 坐标所对应数据点的像素值。双线性插值分两步计算:首先,使用关于 x 的单线性插值从 x 轴方向计算 $f(x, y_1)$ 与 $f(x, y_2)$ 的像素值。

$$\begin{aligned} f(x, y_1) &= \frac{x_2 - x}{x_2 - x_1} f(Q_{11}) + \frac{x - x_1}{x_2 - x_1} f(Q_{21}) \\ f(x, y_2) &= \frac{x_2 - x}{x_2 - x_1} f(Q_{12}) + \frac{x - x_1}{x_2 - x_1} f(Q_{22}) \end{aligned} \quad (1)$$

然后,使用关于 y 的单线性插值从 y 轴方向计算 (x, y) 数据点的像素值 $f(x, y)$ 。

$$f(x, y) = \frac{y_2 - y}{y_2 - y_1} f(x, y_1) + \frac{y - y_1}{y_2 - y_1} f(x, y_2) \quad (2)$$

经过上述数据预处理,最终生成的图像数据集作为检测模型的输入。

如图 4 所示, Car-Hacking 数据集^[12]中各类攻击样本在视觉表征上呈现显著差异。正常 (Normal) 样本的图像呈现规则的纹理分布特征。模糊 (Fuzzy) 攻击样本的图像因随机噪声注入

而表现出无序的像素模式。DoS 攻击样本的图像因高频无效消息的注入,而出现大面积黑色区域 (对应三通道像素低值) 并伴随少量红色异常点 (对应单通道像素高值), 形成鲜明的空间分布特征。对于 Gear Spoofing 与 RPM Spoofing 样本, 攻击者通过伪造特定 CAN 标识符的消息包模拟合法通信, 其数据模式在图像中映射为局部高密度区域, 具体表现为由红、蓝等高对比度色彩构成的垂直条纹或块状结构。此类样本的图像特征与正常样本图像均匀分布的特征形成鲜明对比, 为攻击检测模型提供了关键区分依据。此外, 三通道彩色图像设计通过多维度特征融合增强了分类鲁棒性: 当某一通道因硬件故障或噪声干扰而出现信息失真时, 其余通道仍能通过互补机制维持特征完整性。以 DoS 攻击为例, 其大面积黑色区域在 RGB 三通道中均呈现低值特征, 单通道灰度图可能因信息压缩而丢失此类全局特征。这种冗余设计显著提升了模型在复杂车载环境下的容错能力。

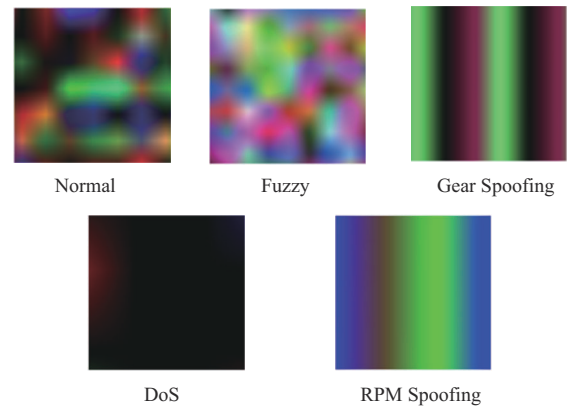


图 4 代表性样本的图像
Figure 4 Images of representative samples

2.3 模型设计

在计算机视觉领域,面对传统深度学习模型复杂度高、参数量大、部署环境要求严苛等挑战,轻量化模型应运而生,其中最具代表性的是 MobileNet 系列模型^[13]。该系列模型包括 MobileNet V1、MobileNet V2、MobileNet V3。

考虑到单个流量数据样本的特征维度比较有限,直接应用原始 MobileNet 网络时,其过深的架构可能导致模型在训练过程中容易陷入过拟合的困境。为优化训练过程,确保模型学习的稳定

性和预测结果的可靠性, 本文采取模型精简策略, 在 MobileNet V3 基础架构上进行定制化裁剪, 即删除了部分 Bottleneck 层 (具体为表 4 中列出的第 8、10、12 层), 保留了其余 13 层, 从而构建了一个更为紧凑且高效的模型。

MobileNet V3 采用的压缩-激励 (squeeze-and-excitation, SE) 注意力机制仅通过编码通道间信息来评估各通道的重要性, 忽略了对对象关键结构特征的捕捉。这种设计导致流量数据转换图像在关键像素坐标和视觉纹理上与原始图像存在明显差异。例如, Gear/RPM 欺骗攻击样本的流量图像表现为绿色竖纹, 而 Normal 和 Fuzzy 样本的流量图像呈现同色块状分布。为提高模型对攻击样本空间特征的捕捉能力, 本文提出以坐标注意力 (coordinate attention, CA) 机制替代 SE 机制。CA 机制不仅捕捉跨通道信息, 还捕捉空间敏感信息, 从而精准定位关键像素区域^[14]。该设计在满足轻量化 (计算量减少) 需求的同时, 提高了模型性能、节省了计算资源。

综上所述, 本文基于 MobileNet V3 框架进行轻量化适配, 针对车联网流量图像数据集的特性, 通过简化模型层级, 从而减少参数量。同

时, 采用 CA 机制增强模型对攻击特征的空间感知能力, 提升模型性能。最终形成的车联网入侵检测模型 MobileNet-Tiny 的架构如图 5 所示。

2.4 FL-IoV 的功能实现

FL-IoV 的完整工作流程涵盖系统初始化、本地模型训练、参数加密、参数聚合和参数更新 5 个核心阶段。下面将详细描述各阶段的实现方式。

2.4.1 系统初始化

为确保联邦学习过程中数据传输的安全性与隐私性, 可信权威机构采用混合加密体系构建安全基础设施。

1) 生成密钥: 选取两个大素数 p 和 q , 计算模数 $N = p \cdot q$; 设公钥 $PK = (N, g)$; 构造私钥 $SK = (\lambda, \mu)$, 其中 λ 为 $(p-1)$ 和 $(q-1)$ 的最小公倍数, μ 为模数 N 的乘法逆元。

2) 密钥分发机制: 初始化时, 将私钥 SK 分发给各客户端, 用于参数解密。同时, 可信权威机构为每对客户端-服务器分配唯一的对称密钥 S_i 和端口号, 实现通信链路隔离。

2.4.2 本地模型训练

每个客户端在其本地车载边缘设备上独立训

表4 MobileNet V3结构
Table 4 MobileNet V3 structure

序号	输入	操作	扩展尺寸	输出	SE	NL	步长
1	2 242×3	Conv2d, 3×3	—	16	—	HS	2
2	1 122×16	Bneck, 3×3	16	16	√	RE	2
3	562×16	Bneck, 3×3	72	24	—	RE	2
4	282×24	Bneck, 3×3	88	24	—	RE	1
5	282×24	Bneck, 5×5	96	40	√	HS	2
6	142×40	Bneck, 5×5	240	40	√	HS	1
7	142×40	Bneck, 5×5	240	40	√	HS	1
8	142×40	Bneck, 5×5	120	48	√	HS	1
9	142×48	Bneck, 5×5	144	48	√	HS	1
10	142×48	Bneck, 5×5	288	96	√	HS	2
11	72×96	Bneck, 5×5	576	96	√	HS	1
12	72×96	Bneck, 5×5	576	96	√	HS	1
13	72×96	Conv2d, 1×1	—	576	√	—	1
14	72×576	Pool, 7×7	—	—	—	HS	1
15	12×576	Conv2d, 1×1, NBN	—	1 280	—	—	1
16	12×1 280	Conv2d, 1×1, NBN	—	1 000	—	—	1

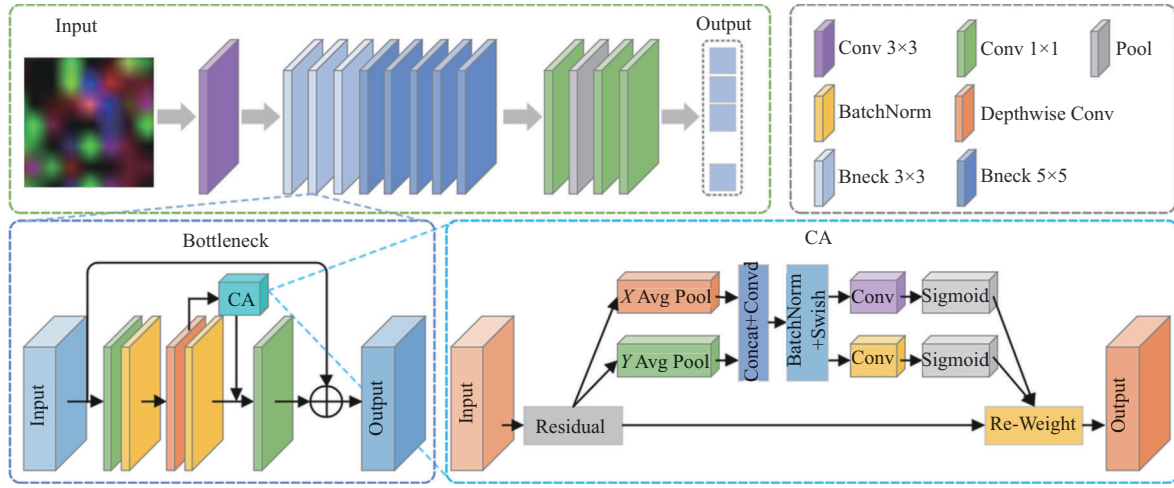


图5 MobileNet-Tiny 模型架构

Figure 5 MobileNet-Tiny model architecture

练面向车联网入侵检测的深度学习模型。采用第 2.2.2 节所述的数据转换方法将车载流量数据转换为彩色图像, 采用 MobileNet-Tiny 模型训练图像数据集, 直至收敛。

2.4.3 参数加密

在本地模型训练完成后, 客户端对模型参数进行加密。对于任意参数 $w_k^r \in \mathbb{Z}_N$ (模 N 的整数集合), $r \in \mathbb{Z}_N^*$ (模 N 的乘法群, $r < N$ 且与 N 互质), 如式(3)所示, 使用公钥 PK 对每个模型的参数进行加密, 生成密文 $\widetilde{w}_k^r$, 并将其发送给云服务器。

$$\widetilde{w}_k^r = E_{PK}(w_k^r) = g^{w_k^r r^N} \bmod N^2 \quad (3)$$

其中, $\widetilde{w}_k^r$ 为密文, r 为随机数, k 为客户端索引, E_{PK} 为公钥加密, w_k^r 为客户端本地模型参数, g 为加密参数, N 为大素数 $p \cdot q$ 的值。

2.4.4 参数聚合

云服务器在接收到所有参与客户端的模型参数后, 根据式(4)对模型参数进行聚合。

$$S = \prod_{i=1}^K \widetilde{w}_k^r = E_{PK}(\widetilde{w}_k^r) = g^{\widetilde{w}_k^r r_1^N} \cdot g^{\widetilde{w}_k^r r_2^N} \cdot \dots \cdot g^{\widetilde{w}_k^r r_K^N} \bmod N^2 = g^{\sum_{i=1}^K \widetilde{w}_k^r \cdot \prod_{i=1}^K r_i^N} \bmod N^2 \quad (4)$$

其中, $g^{\sum_{i=1}^K \widetilde{w}_k^r}$ 是核心运算项, 表示所有客户端加密参数的累加。 K 为参与联邦学习过程的客户端数量, i 表示遍历客户端的索引, 范围为 $1 \sim K$ 。

接下来, 在加密的情况下计算模型参数, 计算公式如下。

$$w_{\text{avg}}^r = \frac{1}{K} \prod_{i=1}^K E_{PK}(\widetilde{w}_k^r) \quad (5)$$

其中, w_{avg}^r 表示加密模型参数。

2.4.5 参数更新

云服务器在完成加密模型参数的聚合后, 将更新后的参数分发给客户端, 客户端按照式(6)对参数进行解密并更新模型。

$$w_{\text{sum}}^r = L\left(\widetilde{w}_{\text{avg}}^r \bmod N^2\right) \cdot \mu \bmod N = \frac{L\left(g^{\sum_{i=1}^K \widetilde{w}_{\text{avg}}^r} \cdot \prod_{i=1}^K r_i^N \bmod N^2\right)}{L\left(g^{\lambda} \bmod N^2\right)} \bmod N \quad (6)$$

其中, w_{sum}^r 表示所有客户端解密模型参数之和, $\widetilde{w}_{\text{avg}}^r$ 表示所有客户端加密模型参数的平均值。

上述是客户端和服务端之间更新模型参数的交互过程, 经过 R 轮, 最终得到全局最优的车联网入侵检测模型。

3 实验与分析

3.1 实验环境

本文实验使用 Python 3.7 编程语言, Pytorch 开发深度学习模型。在硬件方面, 模型训练在配置为 64 位 Windows 10、Intel(R) Xeon(R) Silver 4210 CPU @ 2.20 GHz、GPU NVIDIA GeForce RTX 2080ti (11G)、256 GB 内存的工作站上进

行。测试部署在 Raspberry Pi 4 (8 GB) 上, 分别模拟车联网云服务器和车载级本地机器。

3.2 数据集

本文在 Car-Hacking 和 Can-Train-And-Test (CTAT) [15] 数据集上开展实验评估。其中, Car-Hacking 数据集于 2018 年通过 OBD-II 端口注入 CAN 总线攻击完成采集, 目前已成为车联网入侵检测研究的基准数据集, 被广泛用于模拟攻击场景下的模型验证。CTAT 数据集是 2024 年发布的首个多厂商真实场景数据集, 其数据由两家车企生产的 4 款量产车型在真实车联网环境中采集得到。该数据集包含大量正常流量及 5 类不同的攻击流量, 详见表 5。

表 5 攻击类型及数量
Table 5 Attack types and quantities

数据集	攻击类别	总数	标签
Car-Hacking	Normal	988 872	0
	RPM Spoofing	654 897	1
	Gear Spoofing	597 252	2
	DoS	587 521	3
	Fuzzy	491 847	4
CTAT	Normal	91 827 504	0
	DoS	20 933 681	1
	Fuzzy	13 492 648	2
	Systematic	21 256 417	3
	StandStill	10 941 682	4
	Interval	7 559 143	5

此外, 为模拟现实联邦学习场景中各客户端数据的异构性, 本文实验采用基于 Dirichlet 分布 ($\alpha=0.1$) 的非独立同分布 (Non-IID) 数据划分策略。首先将原始数据集按 8:2 比例划分为训练集 (80%) 和测试集 (20%), 随后将训练集按攻击类型标签通过 Dirichlet 分布分配至 K 个客户端。其中, $\alpha=0.1$ 表示各客户端数据分布差异显著 (即每个客户端仅包含少数类别的样本)。例如, 当 $K=3$ 时, 客户端 1 主要包含 Normal (60%) 和 RPM Spoofing (40%) 样本, 客户端 2 包含 Gear Spoofing (55%) 和 DoS (45%) 样本, 客户端 3 包含 Fuzzy (70%) 和混合攻击 (30%) 样本。该策略确保各客户端的本地数据集在类别

分布上具有显著差异, 符合车载设备数据采集的真实场景。

3.3 评价指标

为全面多维度评估 FL-IoV 的分类效能, 本文构建了涵盖准确率 (accuracy)、精确度 (precision) 和召回率 (recall) 的多样化评估指标体系。这些指标基于的标准化定义与计算公式如下。

1) TP (true positive): 实际为恶意攻击且被模型正确识别的样本数量。

2) FP (false positive): 实际为良性但被误判为恶意攻击的样本数量。

3) TN (true negative): 实际为良性且被正确分类的样本数量。

4) FN (false negative): 实际为恶意攻击但被误判为良性的样本数量。

$$\text{accuracy} = \frac{TP + TN}{TP + FP + TN + FN} \quad (7)$$

$$\text{precision} = \frac{TP}{TP + PF} \quad (8)$$

$$\text{recall} = \frac{TP}{TP + FN} \quad (9)$$

此外, 考虑到车载设备通常性能有限, 为评估所提方法的效率及更直观地进行性能对比, 本文记录并对比了在服务器级机器上的训练时间 (train time)、在车载级机器上的测试时间 (test time) 和模型参数量 (params)。训练时间反映了方法的收敛速度, 测试时间展现了方法的检测实时性, 而模型参数量揭示了所使用的深度学习模型的规模。

3.4 实验结果

3.4.1 模型改进消融实验对比

为系统评估 MobileNet V3 架构改进的有效性, 本文设计了渐进式结构消融实验。以原始 MobileNet V3 为基线, 从第 4 个 Bottleneck 层 (Bneck, 5×5 , 对应表 4 第 5 行) 开始, 依次删除 1~5 层 Bottleneck, 生成对比模型系列 MobileNet ($-n$) ($n \in [1, 5]$)。在删除 3 层 Bottleneck 的基础上, 将 SE 机制替换为 CA 机制, 得到最终的本地模型 MobileNet-Tiny。

在实验过程中, 根据第 2.2.2 节所述的数据转换方法, 将 Car-Hacking 数据集样本转换为图像, 并输入深度学习模型进行本地训练。本地模型的参数设置见表 6。

表6 本地模型的参数设置

Table 6 Parameters setting of the local model

参数	值
Epoch	50
Batch Size	64
Optimizer	Adam
Momentum	0.9
Learning Rate	0.001

各模型实验结果见表7, 在 Car-Hacking 数据集上开展的对比实验充分验证了模型结构优化的有效性。具体分析如下: 当删除 1~3 层 Bottleneck 时, 模型的各项评估指标呈现正向提升趋势, 且在删除 3 层时达到最佳效果, 模型的检测准确率达到最高, 即 MobileNet-Tiny 的检测准确率比 MobileNet V3 高出 0.05%。尽管检测准确率提升幅度较小, 但表明简化后的模型相比复杂模型对车联网数据集具有更好的拟合能力。此外, 由于删除了 3 层结构, 模型的参数量减少至 2.22×10^6 , 比原始模型减少了 0.57×10^6 , 仅为原来的 79.57%, 有利于轻量化部署。然而, 当删除 4 层和 5 层 Bottleneck 时, 尽管模型的参数量进一步减少, 但检测的准确率和精确度均下降。具体而言, MobileNet(-4)相比 MobileNet(-3)的检测准确率和精确度分别降低 0.72% 和 0.75%, 表明模型结构过于简单, 难以有效拟合车联网数据集; MobileNet(-4)相比 MobileNet(-3)参数仅减少了 0.19×10^6 , 收益较小。由此说明, 当 MobileNet V3 删除 3 层 Bottleneck 时, 在准确率和参数量之间实现了最佳平衡。

从表4展示的原始 MobileNet V3 结构来看, 第 5~12 层均为重复堆叠的同构 Bottleneck 层, 这意味着删除任意一层的效果理论上是等效的。

在操作时, 只需对扩展尺寸和步长进行调整, 即可确保删除层后特征矩阵的输出尺寸保持不变。以删除第 7 层为例, 可将其替换为删除第 8 层, 同时将第 8 层的扩展尺寸调整为 120, 这样能保证特征矩阵的输出尺寸维持在 142×48 。同理, 删除第 11 层与删除第 12 层所获得的效果完全一致。基于简化操作的考量, 本文最终选择删除原 MobileNet V3 的第 8、10、12 层。

在 MobileNet V3 模型基础上, 通过删除 3 层 Bottleneck 层构建 MobileNet (-3) 模型, 进一步采用 CA 机制替换 SE 机制, 最终形成轻量化本地模型 MobileNet-Tiny。实验结果显示, 改进后的 MobileNet-Tiny 在 Car-Hacking 数据集上的各项关键性能指标均实现提升。具体而言, 该模型在 Car-Hacking 数据集上的检测准确率达到 99.17%, 比 MobileNet V3 提高了 0.92%; 同时, 模型参数量降至 2.24×10^6 , 相比原始模型减少 0.57×10^6 , 仅为原始模型的 80.29%。与 MobileNet(-3)相比, MobileNet-Tiny 虽仅增加 0.02×10^6 的参数量, 但显著提升了检测准确率。这些成果证明, 第 2.3 节提出的模型剪枝方法成功去除了多余的参数结构, 显著减少了资源消耗; CA 机制的应用很好地适应了车联网入侵检测图像数据集的特点, 通过增强对像素位置差异的关注, 在仅增加少数参数的情况下, 有效提升了模型的检测准确率。

3.4.2 各本地模型实验对比

为验证所提出的数据转换方法与 MobileNet-

表7 各模型实验结果

Table 7 Experimental results of each model

模型	准确率	精确度	召回率	参数量
MobileNet V3	98.25%	98.21%	98.19%	2.79×10^6
MobileNet (-1)	98.25%	98.24%	98.21%	2.60×10^6
MobileNet (-2)	98.28%	98.25%	98.29%	2.41×10^6
MobileNet (-3)	98.30%	98.27%	98.32%	2.22×10^6
MobileNet (-4)	97.58%	97.52%	96.22%	2.03×10^6
MobileNet (-5)	96.12%	96.05%	95.59%	1.84×10^6
MobileNet-Tiny	99.17%	99.10%	99.21%	2.24×10^6

Tiny 模型的优越性, 本文实验遵循第 2.2 节所述的数据预处理流程, 将 Car-Hacking 数据集样本转换为图像, 随后将图像输入深度学习模型进行本地训练直至收敛。实验选取两类主流模型作为对比: 一类是 ResNet54、Vision Transformer (ViT) 等复杂化深度学习模型; 另一类是 EfficientNet-B0、ShuffleNet V2、MobileNet V3 等轻量化模型。

本地模型实验结果见表 8, 其中准确率、精确度、召回率和测试时间 (单样本) 均是在树莓派设备上对测试集进行实验得到的; 训练时间是在有 GPU 加持的服务器上进行训练直至收敛所需要的时间; 参数量是模型中可训练的参数的总数, 与计算复杂度和内存占用大小直接相关。从表 8 可以看出, Car-Hacking 数据集上所有分类模型的检测准确率均超过 96%, 验证了数据转换方法的有效性。当流量数据转换为三通道图像后, 其特征和结构特征被转换成图像的纹理和视觉特征, 使得深度学习模型既能有效区分不同类别的图像特征, 又能通过时间戳挖掘字节序列的深层特征。三通道特征互补机制进一步增强了模型对检测结果的修正能力。

在 Car-Hacking 数据集上, 改进后的 MobileNet-Tiny 在所有关键指标上均有提升。该模型的检测准确率达到 99.17%, 较 MobileNet V3 提升 0.92%, 参数量降至 2.24×10^6 , 降幅达 19.71%。这一进步印证了模型剪枝策略成功剔除冗余参数, 在轻量化的同时减少了资源消耗。此外, CA 机制通过聚焦像素位置差异的特性, 完美适配车联网图像数据集, 进一步推动准确率的提升。

ResNet54 虽检测准确率仅比 MobileNet-Tiny

高 0.03%, 但在服务器上的训练时间是 MobileNet-Tiny 的 3.36 倍, 在树莓派上的测试时间是 MobileNet-Tiny 的 16.33 倍, 参数量是 MobileNet-Tiny 的 11.69 倍。ViT 的检测准确率达 99.08%, 但将其部署到树莓派会导致内存不足。ResNet54 与 ViT 虽具备更强的模型拟合能力, 但其训练/测试时间过长且硬件资源需求极高, 难以适配车联网边缘设备。

根据实时性检测标准, 每个数据包的测试时间应少于 10 ms^[16]。实验结果表明, 仅 ShuffleNet V2 (8 ms) 与 MobileNet-Tiny (6 ms) 满足要求。其中, MobileNet-Tiny 在检测准确率上比 ShuffleNet V2 高出 3.13%, 参数量仅为 84.5%。

从综合性能来看, MobileNet-Tiny 在保证轻量化部署的前提下, 实现了检测准确率与运算效率的双重突破。相比其他模型, MobileNet-Tiny 在车联网入侵检测场景中具备更佳的综合性能适配性。

3.4.3 各联邦学习框架实验对比

为验证 FL-IoV 的检测性能, 本文选取 DeepFed (CNN-GRU)^[17]、FedCV (MobileNet V3)^[18] 和 ViT-FL (Vision Transform)^[19] 3 种联邦学习检测方法, 与 FL-IoV 在 Car-Hacking 数据集上开展对比实验。为确保数据的可靠性, 实验设置不同客户端数量 ($K=3, 5, 7$), 并将各模型训练至收敛状态。

各方法在不同客户端数量下的检测精确度见表 9。在 Non-IID 数据分布场景中, FL-IoV 展现出显著优势: 平均精确度达 98.51%, 较 DeepFed (91.65%)、FedCV (96.64%) 和 ViT-FL (94.28%) 分别高出 6.86%、1.87% 和 4.23%。

表 8 本地模型实验结果

Table 8 Experimental results of the local model

模型	准确率	精确度	召回率	训练时间/s	测试时间/ms	参数量
ResNet54	99.20%	99.15%	99.21%	10 462	98	26.18×10^6
ViT	99.08%	99.02%	99.10%	32 834	内存不足	85.76×10^6
EfficientNet-B0	97.46%	97.47%	97.46%	3 865	15	5.41×10^6
ShuffleNet V2	96.04%	96.10%	96.02%	3 663	8	2.65×10^6
MobileNet V3	98.25%	98.21%	98.19%	3 491	11	2.79×10^6
MobileNet-Tiny	99.17%	99.10%	99.21%	3 137	6	2.24×10^6

表 9 各方法在不同客户端数量下的检测精确度
Table 9 Detection accuracy of each method under different numbers of clients

轮次 K	DeepFed	FedCV	ViT-FL	FL-IoV
3	91.84%	96.64%	94.34%	98.55%
5	92.46%	97.28%	95.51%	99.07%
7	90.66%	96.01%	92.99%	97.92%
平均精确度	91.65%	96.64%	94.28%	98.51%

客户端与云服务器间的通信开销（以参数交换量衡量）如图 6 所示。FL-IoV 的通信开销仅为 165 MB，显著低于 DeepFed（1 250 MB）、FedCV（778 MB）和 ViT-FL（2 483 MB）。

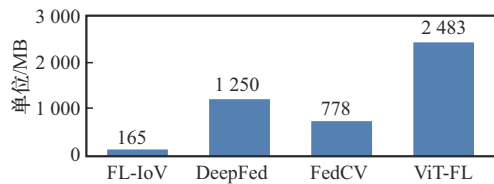


图 6 通信开销
Figure 6 Communication overhead

实验结果表明，在不同联邦客户端数量（ $K=3,5,7$ ）的测试场景下，FL-IoV 方法在检测精确度与通信开销两方面均显著优于 DeepFed、FedCV、ViT-FL 等现有联邦学习检测技术。这得益于 FL-IoV 中的 MobileNet-Tiny 的轻量化设计和高效的通信加解密策略。综上，FL-IoV 为车联网入侵检测的联邦学习部署提供了兼顾精确度、效率与隐私的一体化解决方案。

3.4.4 与现有权威车联网入侵检测方法对比

FL-IoV 凭借高检测准确率、低算力设备适配性及实时检测能力，在车联网入侵检测场景中

展现显著优势。其核心特性源于联邦学习框架（各客户端数据本地训练、隐私数据零共享，结合加密参数更新机制，构建起高隐私保护体系）。下面从检测准确率、实时性、隐私保护和训练时间 4 个维度，对 4 种权威车联网入侵检测方法在 Car-Hacking 数据集上展开对比。

如表 10 所示，MTH-IDS 方法在 Car-Hacking 数据集上实现了 99.99% 的检测准确率，但其依赖人工特征工程和复杂的双层检测架构，导致训练时间长达 12.4 h。由于计算需求较高，该方法难以部署在车载低性能设备上，且未解决隐私保护问题，存在数据泄露风险。Rec-CNN^[20]通过组合循环网络与多模块融合等深度学习模型，将检测准确率提升至 99.90%，但计算复杂使其训练时间激增至 19.5 h。此外，该方法的检测时延超过 10 ms，无法满足车载场景的实时性要求，其中心化训练模式也限制了分布式部署的可行性。SSL-Autoencoders^[21]借助轻量化集成学习，仅用 1.8 h 就完成了训练，检测准确率达 96.29%，并满足实时性要求。不过，其中心化训练模式和隐私保护机制的缺失，限制了实际应用范围，尤其在分布式车联网场景中，难以保障数据隐私安全。

本文提出的轻量化本地检测方法 MobileNet-Tiny，在 Car-Hacking 数据集上实现了 99.17% 的高检测准确率，训练时间仅需 0.9 h，较传统深度学习方法 Rec-CNN 的效率提升 21.7 倍。凭借模型规模优势，该方法成功部署于树莓派等算力受限设备，同时保持少于 10 ms 的实时检测能力。为解决隐私保护问题，本文进一步提出联邦学习架构 FL-IoV。通过分布式训练模式，该架构将检测准确率维持在 98.51%（仅比本地模型下降

表 10 4 种权威车联网入侵检测方法对比
Table 10 Comparison of four authoritative methods for intrusion detection in internet of vehicles

检测方法	数据集	准确率	实时性	隐私保护	训练时间/h
FL-IoV	Car-Hacking	98.51%	满足	有	1.2
MobileNet-Tiny		99.17%	满足	无	0.9
MTH-IDS ^[1]		99.99%	不满足	无	12.4
Rec-CNN ^[20]		99.90%	不满足	无	19.5
SSL-Autoencoders ^[21]		96.29%	满足	无	1.8

0.66%), 同时实现隐私数据的本地化处理。尽管联邦学习引入的多轮加密通信使训练时间增至 1.2 h, 但较同类联邦方案仍有显著优化, 且可通过客户端并行训练进一步提升效率。实验结果表明, FL-IoV 在隐私保护与检测性能间取得良好平衡, 综合表现优于现有方法: 避免了 MTH-IDS 的高计算开销与部署限制; 解决了 SSL-Autoencoders 的中心化隐私缺陷问题; 通过轻量化设计突破了 Rec-CNN 等复杂深度模型的实时性瓶颈。

3.4.5 在 CTAT 数据集上的表现

为评估 FL-IoV 模型的鲁棒性与泛化能力, 本文在 2024 年发布的公共车联网入侵检测数据集 CTAT 上开展了实验。该数据集总计包含 166 011 075 条流量数据, 覆盖 1 类正常流量与 5 类攻击流量, 类别体系丰富, 但存在显著的类别不平衡问题 (最大类别样本量约为最小类别样本量的 13.12 倍), 对模型泛化能力构成考验。

根据图 7 的混淆矩阵结果, FL-IoV 在 CTAT 数据集不同类别样本上展现出优异的整体识别性能, 尤其在 Normal 和 DoS 类别中表现突出。

1) Normal 类别: 识别准确率达 99.1%, 这得益于该类别样本量丰富 (最大类别), 模型得以充分学习正常流量的特征分布。

2) DoS 类别: 准确率高达 99.9%, 其关键原因在于流量数据转换为图像会呈现大面积全黑的显著视觉特征, 便于模型识别。

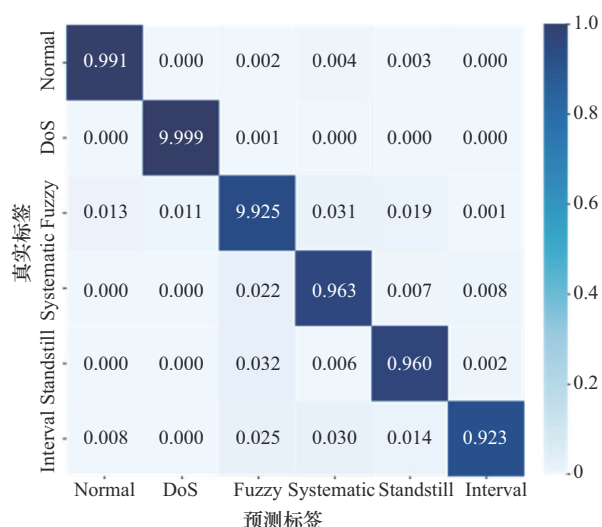


图7 在 CATA 数据集上的混淆矩阵

Figure 7 Confusion matrix on the CATA dataset

在 CTAT 数据集的类别识别中, FL-IoV 对 Fuzzy、Standstill 和 Interval 等复杂类别的检测表现体现了模型在特征随机性与样本稀缺场景下的适应性。对于 Fuzzy 类别, 模型识别的准确率为 92.5%, 尽管展现了较强的分类能力, 但该类别的误判率相对其他类别略高。这种误判主要归因于 Fuzzy 流量字段特征具有高度随机性, 转换为图像会呈现无序的复杂纹理模式, 导致特征提取难度增加。Standstill 和 Interval 类别的样本量相对较少, 这两类的识别准确率虽低于优势类别, 但仍达到了较高水平。

4 结束语

本文提出了一种名为 FL-IoV 的综合车联网入侵检测方法。针对车载流量中 CAN 数据的独特性, 首先通过数据转换技术, 将其按时间戳顺序转换为三通道彩色图像, 这种转换方式能够有效保留数据中的时序特征与潜在模式。考虑到车载设备在计算资源和存储能力上的限制, 本文定制开发了轻量化模型 MobileNet V3-Tiny, 专门用于训练和学习上述图像数据集, 在保证检测精度的同时, 大幅缩减了模型对硬件资源的消耗。在此基础上进一步构建了基于联邦学习架构的车联网入侵检测框架。该框架实现了客户端模型在本地进行数据训练, 无须共享原始数据, 同时采用加密技术对参数传递过程进行保护, 从根本上保障了用户的隐私安全。实验结果表明, 在公开数据集上, MobileNet V3-Tiny 模型的检测准确率、实时性和参数量等关键指标均显著优于其他主流深度学习模型。这一结果充分证明 FL-IoV 作为一款高效、实时且具备隐私保护能力的综合检测方案, 能够满足实际车联网场景中对入侵检测的严苛需求。

在当前框架中, 模型参数聚合基于客户端诚实且服务器无恶意修改的假设, 这使得其在面对数据投毒攻击时存在防御短板。为提升框架的安全性与可靠性, 未来计划从增强联邦学习鲁棒性方面展开探索, 如引入拜占庭容错算法等。

参考文献:

[1] YANG L, MOUBAYED A, SHAMI A. MTH-IDS: a multitiered hy-

- brid intrusion detection system for internet of vehicles[J]. IEEE Internet of Things Journal, 2022, 9(1): 616-632.
- [2] 潘桐, 陈伟, 吴礼发. 面向不平衡样本的物联网入侵检测方法[J]. 网络与信息安全学报, 2023, 9(1): 130-139.
PAN T, CHEN W, WU L F. IoT intrusion detection method for unbalanced samples[J]. Chinese Journal of Network and Information Security, 2023, 9(1): 130-139.
- [3] 罗文华, 张晓龙. 基于联邦学习与卷积神经网络的入侵检测模型[J]. 信息安全研究, 2024, 10(7): 642-648.
LUO W H, ZHANG X L. Model of intrusion detection based on federated learning and convolutional neural network[J]. Journal of Information Security Research, 2024, 10(7): 642-648.
- [4] SINGH N B, SINGH M M, SARKAR A, et al. A novel wide & deep transfer learning stacked GRU framework for network intrusion detection[J]. Journal of Information Security and Applications, 2021, 61: 102899.
- [5] NGUYEN M T, KIM K. Genetic convolutional neural network for intrusion detection systems[J]. Future Generation Computer Systems, 2020, 113: 418-427.
- [6] 杨晓文, 张健, 况立群, 等. 融合 CNN-BiGRU 和注意力机制的网络入侵检测模型[J]. 信息安全研究, 2024, 10(3): 202-208.
YANG X W, ZHANG J, KUANG L Q, et al. A network intrusion detection model integrating CNN-BiGRU and attention mechanism[J]. Journal of Information Security Research, 2024, 10(3): 202-208.
- [7] 郑诚波, 闫皓楠, 傅彩利, 等. 面向智能物联网的双层级联邦安全学习架构[J]. 网络与信息安全学报, 2024, 10(6): 71-80.
ZHENG C B, YAN H N, FU C L, et al. Double layer federated security learning architecture for artificial intelligence of things[J]. Chinese Journal of Network and Information Security, 2024, 10(6): 71-80.
- [8] XIE G Q, YANG L T, YANG Y D, et al. Threat analysis for automotive CAN networks: a GAN model-based intrusion detection technique[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(7): 4467-4477.
- [9] LO W, ALQAHTANI H, THAKUR K, et al. A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic[J]. Vehicular Communications, 2022, 35: 100471.
- [10] JAVED A R, REHMAN S U, KHAN M U, et al. CANintelliIDS: detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU[J]. IEEE Transactions on Network Science and Engineering, 2021, 8(2): 1456-1466.
- [11] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[EB]. 2016.
- [12] SONG H M, WOO J, KIM H K. In-vehicle network intrusion detection using deep convolutional neural network[J]. Vehicular Communications, 2020, 21: 100198.
- [13] HOWARD A, SANDLER M, CHEN B, et al. Searching for MobileNet V3[C]//Proceedings of the 2019 IEEE/CVF International Conference on Computer Vision (ICCV). Piscataway: IEEE Press, 2019: 1314-1324.
- [14] TSAI T H, YU W T. BiSeNet V3: bilateral segmentation network with coordinate attention for real-time semantic segmentation[J]. Neurocomputing, 2023, 532: 33-42.
- [15] LAMPE B, MENG W Z. Can-train-and-test: a curated CAN dataset for automotive intrusion detection[J]. Computers & Security, 2024, 140: 103777.
- [16] TSAI T H, TSENG Y W. BiSeNet V3: bilateral segmentation network with coordinate attention for real-time semantic segmentation[J]. Neurocomputing, 2023, 532: 33-42.
- [17] LI B B, WU Y H, SONG J R, et al. DeepFed: federated deep learning for intrusion detection in industrial cyber-physical systems[J]. IEEE Transactions on Industrial Informatics, 2021, 17(8): 5615-5624.
- [18] HE C Y, SHAH A D, TANG Z H, et al. FedCV: a federated learning framework for diverse computer vision tasks[EB]. 2021.
- [19] QU L Q, ZHOU Y Y, LIANG P P, et al. Rethinking architecture design for tackling data heterogeneity in federated learning[C]//Proceedings of the 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE Press, 2022: 10051-10061.
- [20] DESTA A K, OHIRA S, ARAI I, et al. Rec-CNN: in-vehicle networks intrusion detection using convolutional neural networks trained on recurrence plots[J]. Vehicular Communications, 2022, 35: 100470.
- [21] HOANG T N, KIM D. Detecting in-vehicle intrusion via semi-supervised learning-based convolutional adversarial autoencoders[J]. Vehicular Communications, 2022, 38: 100520.

[作者简介]



蒋玉长 (1998-), 男, 广东广州人, 北京银联金卡科技有限公司深圳分公司助理工程师、技术支持工程师, 主要研究方向为数据安全、车联网安全、金融科技。



蒋利兵 (1986-), 男, 湖南永州人, 主要研究方向为终端机具产品安全、信息系统安全、网络通信安全、数据安全。



黄凯 (1995-), 男, 广东潮州人, 主要研究方向为数据安全、金融科技。