

基于物理层射频指纹的车联网设备 攻击检测

解男男^{1,2}, 刘妍利^{1,2}, 曹金辉^{1,2}, 祁 晖^{1,2}

(1. 吉林省网络与信息安全重点实验室; 2. 长春理工大学 计算机科学技术学院, 吉林 长春 130022)

摘要: 智能车辆通过Wi-Fi、蓝牙无线技术实现互联,但其开放信道易受设备伪装攻击。现有方法多依赖网络流量特征,难以识别射频层面高度相似的伪造设备,且单一模式方案常面临泛化性差与鲁棒性不足的问题。为此,提出一种基于射频指纹的自适应攻击检测方法,通过正交频分复用(OFDM)符号级信号分析去除冗余信息,降低计算复杂度。首先,对原始信号进行协议对齐与结构化预处理,提取时序化OFDM符号序列;其次,采用长短期记忆网络建模信号时域动态特性,捕捉设备特有细微波动;再次,通过多头注意力聚合正常原型,并经多层感知机非线性变换生成负原型,以构建更具区分性的特征参考,增强判别能力;最后,对于初步判定正常的样本,结合负原型、共轭训练与余弦距离,采用基于正负原型间的相对关系动态划定拒绝边界,实现无需人工设阈的攻击检测。在Oracle数据集上的实验表明,所提方法的准确率、精确率分别为94.75%、99.47%,误报率仅为0.51%,相较于较最优的基线方法精度提升5.35%,误报率显著降低,有效提升了攻击检测能力。

关键词: 智能车辆;设备欺骗攻击;射频指纹识别;负原型;共轭训练

DOI:10.11907/rjdk.251708

中图分类号:TP393

文献标识码:A

文章编号:1672-7800(2025)012-0033-09

扫描二维码阅读全文:



Device Attack Detection in Vehicular Networks Based on Physical-Layer RF Fingerprinting

XIE Nannan^{1,2}, LIU Yanli^{1,2}, CAO Jinhui^{1,2}, QI Hui^{1,2}

(1. Jilin Province Key Laboratory of Network and Information Security;

2. School of Computer Science and Technology, Changchun University of Science and Technology, Changchun 130022, China)

Abstract: Intelligent vehicles are interconnected through Wi-Fi and Bluetooth wireless technology, but their open channels are susceptible to device spoofing attacks. Existing methods mostly rely on network traffic characteristics, which makes it difficult to identify counterfeit devices that are highly similar at the radio frequency level, and single mode schemes often face the problems of poor generalization and insufficient robustness. To this end, an adaptive attack detection method based on radio frequency fingerprinting is proposed, which removes redundant information and reduces computational complexity through symbol level signal analysis using orthogonal frequency division multiplexing (OFDM). Firstly, perform protocol alignment and structured preprocessing on the original signal to extract a sequential OFDM symbol sequence; Secondly, a long short-term memory network is used to model the temporal dynamic characteristics of signals and capture subtle fluctuations unique to the device; Again, by aggregating normal prototypes with multi head attention and generating negative prototypes through non-linear transformations of multi-layer perceptrons, more discriminative feature references are constructed to enhance discriminative ability; Finally, for samples that are preliminarily judged to be normal, combining negative prototypes, conjugate training, and cosine distance, the rejection boundary is dynamically delineated based on the relative relationship between positive and negative prototypes, achieving attack detection without the need for manual threshold setting. Experiments on the Oracle dataset show that the accuracy and precision of the pro-

收稿日期:2025-10-17

基金项目:吉林省科技发展计划项目(20250102242JC)

作者简介: 解男男(1987-),女,博士,长春理工大学计算机科学技术学院副教授、硕士生导师,研究方向为车联网安全、人工智能等;刘妍利(1999-),女,长春理工大学计算机科学技术学院硕士研究生,研究方向为车联网攻击检测;曹金辉(1995-),男,博士,长春理工大学计算机科学技术学院讲师,研究方向为车联网异常检测、射频指纹识别;祁晖(1983-),男,长春理工大学计算机科学技术学院教授、博士生导师,研究方向为空间网络、网络安全等。本文通讯作者:解男男。

posed method are 94.75% and 99.47%, respectively, with a false positive rate of only 0.51%. Compared with the optimal baseline method, the accuracy is improved by 5.35%, and the false positive rate is significantly reduced, effectively enhancing the attack detection capability.

Key Words: intelligent vehicle; device spoofing attack; RF fingerprint recognition; negative prototypes; conjugate learning

0 引言

智能车辆的快速发展推动了 Wi-Fi、蓝牙、NFC 等无线通信技术在车载娱乐、高级驾驶辅助系统和车联网中的广泛应用,加速了汽车产业的数字化转型。然而,无线通信架构的开放性带来了严峻的安全挑战,攻击者可通过无线入侵或硬件篡改实施远程控制、指令注入或非法数据访问,严重威胁了行车安全与用户隐私。

尽管,已有基于密码和入侵检测系统的软件防护手段,但难以有效应对设备伪装、主从冒充和身份伪造等攻击。射频指纹识别作为一种硬件级安全技术,利用无线设备硬件固有的制造偏差所导致的细微信号差异,生成唯一且稳定的生物特征标识,可在协议层外提供细粒度的设备身份认证能力,有效抵御了传统方法难以防范的物理层欺骗攻击。然而,现有的射频指纹识别方法多依赖稳态信号特征或瞬态启动特性,特征表达能力有限。传统检测模型通常采用人工设定的判别阈值,在车载网络环境下泛化能力差、误报率高。此外,多数方法缺乏对正常行为的精细化建模,导致对高仿真伪装设备的识别能力不足。

为此,提出一种正交频分复用(Orthogonal Frequency Division Multiplexing, OFDM)符号级的射频指纹建模方法,设计基于多头注意力的负原型生成机制,构建基于共轭训练与负原型的动态拒绝边界生成方法。首先,为了提升模型对硬件设备间细微差异的敏感性,从原始同相/正交分量(In-phase/Quadrature, I/Q)信号中提取 OFDM 符号序列,以保留时序结构信息;其次,采用长短期记忆网络(Long Short-Term Memory, LSTM)获取时域动态特征;最后,引入负原型生成机制并与共轭训练策略协同设计,构建具有相对判别性的特征空间,以动态形成自适应拒绝边界,从而有效检测伪装成合法的恶意设备的攻击。

1 相关工作

1.1 车载无线系统安全挑战

随着无线通信技术在智能车辆中的广泛应用,开放的通信架构面临严重的安全威胁,例如拒绝服务攻击和 MAC 地址伪造等^[1]。近年来,多起真实攻击事件充分暴露了车载无线接口的脆弱性:2024 年大众集团信息娱乐系统漏洞及特斯拉车载系统遭攻破案例,均表明车载无线接口已成为攻击入口^[2,3]。

复杂的车内电磁环境具有高移动性、强干扰与显著多径效应,易引发信号衰落与低信噪比现象,严重影响入侵检测方法在动态场景下的稳定性与可靠性^[1]。车载设备

普遍受限于低功耗与有限算力,难以支持复杂模型的实时运行^[4]。同时,基于支持向量数据描述的报文特征分析、基于改进自编码的深层特征提取以及结合 LSTM 与注意力机制的时序数据流检测等现有方法,虽在静态数据集上取得一定的性能提升,但存在检测准确率低、误报率高、计算复杂度大等问题,难以适应实时高干扰环境^[5-7]。有研究指出,高移动性环境下的异常检测,面临着模型泛化能力不足与训练数据稀缺等问题,亟需发展对突发干扰具有鲁棒性的轻量化检测机制^[8]。因此,在资源受限条件下,研究仍具备高鲁棒性与自适应性的物理层安全机制,对维护智能汽车的安全具有重大意义。

1.2 射频指纹识别技术

射频指纹识别利用设备硬件制造偏差引起的细微信号特征,例如相位噪声、I/Q 不平衡,实现设备的唯一性认证,在协议层外抵御设备伪装与主从冒充攻击^[9]。早期,依赖启动瞬态信号进行识别,但对同步精度要求高,且在动态信道中性能下降明显^[10]。

近年来,深度学习显著提升了射频指纹识别的鲁棒性与精度。基于深度复数网络的随机傅里叶特征方法,可有效利用 IQ 信号的幅度与相位信息进行设备验证^[11]。结合残差结构与注意力机制,在 15 dB 信噪比下的识别精度能达到 91%^[12]。基于轻量级卷积神经网络(Convolutional Neural Network, CNN)的模型,在 ZigBee 设备上识别率达到 100%,使得模型轻量化成为可能^[13]。同时,还有研究将傅里叶同步压缩变换与对比学习相结合,在噪声环境下提升特征提取稳定性^[14];以及进一步探索对比学习在信道鲁棒性中的应用等^[15]。陈翔等^[16]系统梳理了基于原始 I/Q 信号的端到端深度学习方法,指出其在噪声抑制与特征鲁棒性方面具有显著优势,并强调在车载高干扰场景下,需进一步集成时序注意力机制以增强动态适应性。

针对高移动性场景下的射频指纹识别,王豪等^[17]认为现有深度学习方法在多径效应建模方面已有初步探索,但在车联网复杂动态环境中的泛化能力仍需提升。研究趋势表明,面向动态环境的特征建模正从静态识别向自适应演化。

在实际系统部署方面,黄河^[18]设计并实现了一套完整的无线局域网安全监测系统,集成了流量采集、异常检测与可视化告警功能,为射频安全机制的工程化落地提供了系统架构参考。该系统可实时监控非法接入点和异常通信行为,体现了从算法到系统的转化路径。王梦寒等^[19]提出随机森林-双向长短期记忆网络框架,通过双向长短期记忆网络建模网络流量的时序演化模式,在复杂电磁环境中实现了高效的异常流量检测,为射频信号的序列建模提供了新思路。Dai 等^[20]提出的 Transformer-XL 架构,突破

了上下文长度的限制,在语言建模任务中展现出了卓越性能,可用于长时间连续射频信号的建模。Zeng 等^[21]设计了一种双注意力 LSTM 自编码器,用于工业动态过程中的故障检测,结合通道注意力与时序注意力的机制有助于突出关键特征并抑制噪声干扰,对车载高动态场景下的指纹提取具有重要参考价值。Lu 等^[22]提出一种基于深度学习的多维射频指纹增强框架 MRFE 方法,融合时域、频域与统计特征,能显著提升物联网设备识别的精度与鲁棒性,为应对车载环境中信号畸变与低信噪比挑战提供了可行路径。虽然,这些方法在静态场景中表现良好,但在车载高动态环境下仍面临特征漂移与泛化能力不足的问题。

1.3 自适应与少样本检测机制

为了应对动态环境下的未知攻击,已有研究探索增量学习、开放集识别等机制在动态环境下的应用效果,但多数射频指纹方法仍依赖人工设定的固定判别阈值,在信道快速变化时易导致误报率上升、灵活性不够^[14,23,24]。例如, Sun 等^[24]提出的二阶段检测方法虽检测率超过 90%,但其性能严重依赖阈值调优。还有研究探讨了信道通用预训练大模型在数字孪生信道中的应用,实现了少样本条件下的射频异常自适应预测,展现出了模型先验知识迁移的潜力^[25]。

现有方法少有对正常设备行为进行建模,因此难以在少量正常样本的情况下识别高仿真伪装设备。尽管, CNN-LSTM 混合模型被用于时序 RFF 建模,但其判别边界仍为静态,无法实现动态调整^[26]。Xie 等^[27]提出频谱再生技术以增强特征一致性。Gong 等^[28]利用信息最大化生成对抗网络实现无监督 RFF 提取,但计算复杂或实时性不足,难以满足车载实时性需求。Reus-Muns 等^[29]提出的方法在第五代移动通信开放无线接入网中,基站认证的精度为 99.86%,但依赖大量标注数据与高算力平台,不适用于资源受限的车载环境。马俊光等^[30]通过支持集特征增强

的元学习框架,在小样本目标检测中有效建模了类别原型,表明增强支持集代表性可提升少样本的泛化能力,对射频指纹中正常设备原型构建具有重要的启发意义。

综上,现有射频指纹识别方法在车载场景下面临三大挑战:①特征建模对动态信道敏感;②判别机制依赖固定阈值,缺乏自适应能力;③在少样本条件下难以构建正常类表示。

为此,本文通过 OFDM 符号级时序建模增强特征稳定性,设计负原型生成机制与共轭训练策略,构建正负原型间的相对判别空间,实现无需人工阈值的自适应异常检测,在资源受限与动态变化的车载环境中仍具有较高的鲁棒性与泛化能力。

2 车联网设备自适应攻击检测方法

2.1 本文方法框架

本文在开放无线信道环境下,基于 OFDM 符号级射频指纹对伪装设备实现高精度、低误报的自适应攻击检测,提出一种两阶段融合的射频指纹攻击检测框架,具备自适应阈值调整能力,无需人工设定固定判别边界,可确保系统能动态响应不断变化的威胁环境,并保持高精度与低漏报率。首先,模型以协议对齐后的 OFDM 符号序列为输入,提取其时序化射频特征以构建正常设备的正原型表示;其次,引入可学习的负原型机制,在共轭训练框架下动态建模正负原型间的相对距离关系;最后,以基于余弦相似度的自适应拒绝边界为判据,对合法设备与高仿真伪装攻击进行鲁棒地区分。

本文方法的整体框架采用“粗筛+精检”的级联策略,实现了从高效过滤到细粒度辨别的逐层增强,在保障实时性的同时,显著提升了系统对未知欺骗攻击的鲁棒性与泛化能力,如图 1 所示。

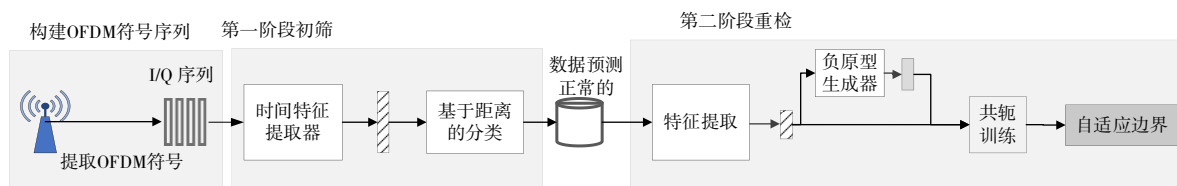


Fig. 1 Attack detection framework based on RF fingerprint

图 1 基于射频指纹的攻击检测框架

(1) OFDM 符号序列构建。对采集的原始 I/Q 信号进行协议解析与帧同步,提取 OFDM 符号序列,并通过符号对齐与归一化处理,构建成固定长度的时间序列,作为后续建模的输入。

(2) 第一阶段初筛检测。采用 LSTM 提取时间序列中的时域动态特征,并结合基于距离的分类器完成初步分类,筛选出疑似正常的设备。该阶段旨在高效区分合法设备与大多数攻击设备,显著降低后续计算负担,提升整体检测效率。

(3) 负原型生成机制。首先,针对第一阶段判定为正常的样本集,引入负原型表示学习;其次,通过多头注意力机制对多个潜在负类进行加权聚合,形成聚合原型;最后,将聚和原型输入多层感知机进行非线性变换,生成可学习的负原型表示。该机制确保了负原型在特征空间中与正常原型保持可区分性,增强了判别能力。

(4) 第二阶段自适应重检。将正负原型嵌入同一特征空间,利用共轭训练策略联合优化两者之间的相对距离关系,动态构建自适应拒绝边界。该阶段专注于识别在第一

阶段被误判为正常的高仿真伪装设备,以有效检测试图模仿合法行为的隐蔽攻击,确保仅有真实设备可通过认证。

2.2 OFDM 符号数据处理

本文以 IEEE 802.11a 协议为例开展数据预处理,这是智能车载 Wi-Fi 通信场景中常用的通信协议,数据帧结构

如图 2 所示。由此可见,前导码字段可用于信号的定时捕捉、同步和信道估计,包含短前导码(10 个重复序列,每序列 16 个 I/Q 样本,共 160 样本)和长前导码(两个 64 样本的长序列);Signal 字段用于指示传输参数;数据字段承载实际通信数据,是提取时间和空间关联特征的主要对象。

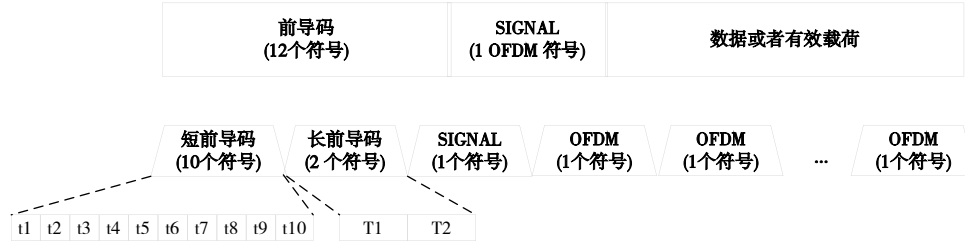


Fig. 2 IEEE 802.11a data frame structure

图2 IEEE 802.11a数据帧结构

为了提取可用于分析的 OFDM 符号序列,对原始 I/Q 采样信号进行标准解调处理。首先,依据 IEEE 802.11a 协议规范筛选有效帧;其次,利用前导码实现帧同步,通过短前导码序列的自相关特性粗略定位帧起始位置,结合长前导码序列互相关实现精确符号对齐;最后,对每个 OFDM 符号进行快速傅里叶变换,将时域信号转换至频域,如式(1)所示。

$$Y[k] = \sum_{n=0}^{N-1} x[n] e^{-j \frac{2\pi}{N} kn}, \quad k = 0, 1, \dots, N-1 \quad (1)$$

式中: $x[n]$ 为输入信号; $N=64$ 为快速傅里叶变换长度; $Y[k]$ 为第 k 个频域值; $e^{-j \frac{2\pi}{N} kn}$ 为复指数基函数。

进一步的,利用已知的长前导码序列进行信道增益估计,用于校正信号失真,如式(2)所示。

$$H[i] = \frac{1}{2} (LTS_1[i] + LTS_2[i]) \times L[i], \quad i \in [-26, 26] \quad (2)$$

式中: $LTS_1[i]$ 、 $LTS_2[i]$ 分别为两个长前导码; $L[i]$ 为极性,表示为以 0 为中心的极性集合,取值为 1 和 -1,例如 $L[i] = \{1, 1, \dots, 0, \dots, 1, 1\}$ 。

随后,基于信道估计结果和频域值对数据子载波进行频域均衡,如式(3)所示。

$$equalize[k] = \frac{Y[k]}{H[k]} \quad (3)$$

式中: $Y[k]$ 为数据在子载波 k 上的快速傅里叶变换输出的频域值; $H[k]$ 为信道增益, k 为子载波索引。

最后,按时间顺序提取所有均衡后的数据子载波,构成连续的 OFDM 符号序列,即 $D = \{d_1, d_2, \dots, d_n\}$, 其中每个 d_i 表示第 i 个 OFDM 符号中所有数据子载波组成的复数向量。

2.3 第一阶段攻击检测

2.3.1 特征提取

本文针对 I/Q 序列的显著时序特性,采用 LSTM 进行特征提取,利用门控机制捕捉信号序列中的长期依赖关系,克服梯度消失问题。同时,通过交叉熵损失优化学习到具有判别性的特征表示,以有效提升攻击检测中对信号动态

变化的识别能力。

本文设计的 LSTM 层包含一个隐藏层,每层 288 个单元,并基于自定义的 LSTM 单元构建,通过门控机制有效提取这些数据中的长期依赖关系。模型通过对 I/Q 数据中隐藏的复杂规律进行挖掘,能为攻击检测提供丰富的时间域特征表达。

假设输入的 I/Q 序列为 $D = \{d_1, d_2, \dots, d_n\}$, 其中 d_i 表示第 i 个时刻的 I/Q 向量。首先,初始化隐藏状态和细胞状态,即 $h_0 = 0, c_0 = 0$; 其次,对每个时间步 t , 依次计算细胞状态更新 c_t 和隐藏状态输出 h_t , 如式(4)、式(5)所示。

$$c_t = f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \quad (4)$$

$$h_t = o_t \odot \tanh(c_t) \quad (5)$$

式中: f_t 、 i_t 、 o_t 分别为遗忘门、输入门和输出门的输出; $\tilde{c}_t$ 为候选细胞状态; $\odot$ 表示逐元素乘法。

最后,输出最后一个时间步的隐藏状态 h_n , 将其作为整个 I/Q 序列的高维时序特征表示,如式(6)所示。

$$L_{class} = \frac{1}{N} \sum_{i=1}^N [y_i \log(\hat{y}_i) + (1 + y_i) \log(1 - \hat{y}_i)] \quad (6)$$

式中: $loss$ 为交叉熵损失; y_i 为真实标签; $\hat{y}_i$ 为预测概率。

2.3.2 基于余弦距离的检测

首先,计算正常样本的特征原型;其次,计算特征与特征原型之间的余弦距离,取值范围为 $[0, 2]$, 如式(7)所示。

$$\text{distance}(A, B) = 1 - \frac{A \cdot B}{\|A\| \|B\|} \quad (7)$$

为了最大化正常样本与攻击样本的区分度,设计余弦距离损失函数 L_1 , 使正常样本与特征原型的余弦距离趋近 0, 与攻击样本的余弦距离趋近 2, 如式(8)所示。

$$L_1 = \frac{1}{N_{normal}} \sum_{x \in normal} (\text{distance}(x, p) - 0)^2 + \frac{1}{N_{attack}} \sum_{x \in attack} (\text{distance}(x, p) - 2)^2 \quad (8)$$

式中: p 为正常样本的特征原型; N_{normal} 为正常样本的个数; N_{attack} 为异常样本的个数。

为了扩大正常样本与攻击数据的距离,引入三元组损失函数,同时缩小正常样本之间的距离,以提升模型对正常和异常样本的区分能力。在三元组损失函数中所用到的距离是余弦距离,目的是为了地衡量样本之间的相似性或差异性,如式(9)所示。

$$L_{\text{triplet}} = \max(0, \cos(a, p) - \cos(n, p) + \text{margin}) \quad (9)$$

式中: a 为攻击样本的特征; n 为正常样本的特征; $\text{margin}=0.3$ 。

第一阶段的损失函数为余弦距离损失和三元组损失之和,如式(10)所示。通过最小化损失,模型便能学习正常与攻击样本的本质差异,增强分类鲁棒性。

$$\text{loss}_1 = L_1 + L_{\text{triplet}} \quad (10)$$

2.4 第二阶段自适应攻击重检

2.4.1 基于注意力机制的负原型生成器

在实现过程中,引入可训练的权重矩阵分别对不同原型进行独立的线性变换,利用 Softmax 函数对注意力矩阵进行归一化处理,实现有效的权重分配。多层感知则通过非线性变换对加权后的原型均值进行建模,生成具有较强区分能力的负原型。实验发现,基于注意力机制的负原型生成方法能有效捕捉类别间的复杂关系,使负原型在特征空间中与正常原型形成显著差异,从而为动态拒绝边界的构建提供可靠依据。

本文使用预训练模型计算正常样本的原型向量 P_{normal} ,用来表示正常类别的中心,生成已知类别原型集合 P^f ,如式(11)所示。

$$P_{\text{normal}} = \frac{1}{N_{\text{normal}}} \sum_{x \in \text{normal}} f(x) \quad (11)$$

负原型生成基于正常类别原型集 $P_f = \{p_1^f, p_2^f, \dots, p_N^f\}$ 。首先,利用多头注意力机制计算原型之间的注意力权重矩阵 $A(P^f, P^f) \in \mathbf{R}^{N \times N}$,通过 Softmax 函数归一化得到加权原型集合 $P' = \{p_1', p_2', \dots, p_N'\}$;其次,计算加权原型集合的均值 p'_{avg} ,通过多层感知机对其进行非线性变换,生成负原型 p^- ,如式(13)所示。

$$P' = P^f + \sigma(A(P^f, P^f))(P^f W_V) \quad (12)$$

$$p'_{\text{avg}} = \frac{1}{N} \sum_{i=1}^N P'_i, \quad p^- = f_n(p'_{\text{avg}}) \quad (13)$$

式中: W_V 为可训练的权重矩阵,对原型向量进行线性变换; $A(P^f, P^f)$ 表示原型集合之间的注意力权重矩阵; $\sigma(\cdot)$ 为 Softmax 函数,用于归一化注意力权重,确保每行权重之和为 1; $f_n(\cdot)$ 为多层感知机函数,用于对加权后的原型均值进行非线性映射。

2.4.2 共轭训练

共轭训练通过任务间的互监督机制优化模型对伪装攻击的识别能力,特别适用于少样本场景下的动态边界调整。本文定义共轭任务对 (Z_1, Z_2) , $Z_1 = (S_1, Q_1^n, Q_1^a | C_1^n)$ 和 $Z_2 = (S_2, Q_2^n, Q_2^a | C_2^n)$ 。其中, $S_1, Q_1^n, Q_1^a | C_1^n$ 分别表示正常样本的支持集、正常样本的查询集、异常样本的查询集及正

常样本的类别集合; $S_2, Q_2^n, Q_2^a | C_2^n$ 分别对应异常样本的支持集、异常样本的查询集、正常样本的查询集和异常样本的类别集合。如果满足 $Q_1^n = Q_2^n$ 且 $Q_2^a = Q_1^a$,即一个任务中的正样本被用作另一个任务中的负样本,从而模拟真实的未知攻击场景。

在智能车内网络中,共轭任务结构能有效利用少量攻击样本模拟攻击数据,充分利用有限的攻击样本与正常样本的关系,增强模型对伪装攻击的敏感性与泛化能力。共轭训练的实现过程分为以下 3 个步骤。

步骤 1:从训练数据集中采样两组互斥的类别集合 C_1^n, C_2^n ,分别构造任务 Z_1, Z_2 。

步骤 2:为每个任务生成负原型 p^- ,采用余弦相似度作为距离度量,计算查询样本与原型及负原型的相似度。对于任务 Z_1 ,正常样本 $q \in Q_1^n$ 的目标是最大化其与对应类别原型的相似度,异常样本 $q \in Q_1^a$ 的目标是最大化其与负原型的相似度,损失函数定义为交叉熵损失 L_{CE} ,如式(14)所示。

$$L_{\text{neg}}(c) = \frac{1}{|Q_{c,1}^n|} \sum_{q \in Q_{c,1}^n} L_{\text{BCE}}(0, f_s(f(q), P_c')) + \frac{1}{|Q_1^a|} \sum_{q \in Q_1^a} L_{\text{BCE}}(1, f_s(f(q), P_c')) \quad (14)$$

步骤 3:为进一步优化负原型,引入类特定负原型正则化项。对于每个加权原型 $p_i' \in P'$,最小化其与正样本的相似度,同时最大化与负样本的相似度,采用二元交叉熵损失 L_{BCE} 进行建模。该阶段的总损失函数如式(15)所示。

$$\text{loss}_2 = L_{\text{CE}}(Q_1^n \cup Q_1^a) + \frac{1}{|C_1^n|} \sum_{c \in C_1^n} L_{\text{neg}}(c) + L_{\text{CE}}(Q_2^n \cup Q_2^a) + \frac{1}{|C_2^n|} \sum_{c \in C_2^n} L_{\text{neg}}(c) \quad (15)$$

式中: $L_{\text{neg}}(c)$ 为负原型损失;共轭训练损失为 loss_2 。

负原型生成机制与共轭训练策略的结合,在智能车辆内部网络场景中展现出了显著优势。负原型通过注意力机制捕捉类别间的潜在关系,构建出与正常原型具有显著差异的特征表示,为动态拒绝边界的形成奠定了基础。同时,共轭训练利用任务间的互监督机制,借助正负样本之间的对偶关系,进一步优化了负原型及其对应的分类边界,可有效提升模型对伪装攻击的辨识能力。

相较于传统依赖人工设定阈值的方法而言,所提方法具备更强的自适应性。通过少样本训练即可实现对拒绝边界的自动调节,无需频繁的人工参数调优,显著提升了模型鲁棒性与泛化能力。

两阶段的检测算法的伪代码如算法 1 所示。

算法 1 两阶段自适应检测方法

输入:原始 I/Q 信号数据集(包含正常与攻击样本),训练轮次 E ,批次大小 B 。

输出:设备检测结果(正常/攻击)。

1. function TwoStageDetection

```

2. FOR 每个 I/Q 帧 DO // 信号预处理
3. 帧同步与信道估计
4. FFT → 频域均衡 → 提取数据子载波
5. 构建归一化 OFDM 符号序列 X
6. END FOR
7. 初始化 LSTM 与分类器 // 阶段 1: 初筛检测
8. FOR epoch = 1 TO E DO
9.  $h \leftarrow \text{LSTM}(X)$ ;  $h_{\text{norm}} \leftarrow \text{归一化}(h)$ 
10.  $P_{\text{normal}} \leftarrow \text{正常样本特征均值}$ 
11.  $L_{\text{total}} \leftarrow \text{余弦损失}(h, P_{\text{normal}}) + \text{三元组损失}(h, \text{标签})$ 
12. 反向传播, 更新模型
13. END FOR
14.  $M_{\text{error}} \leftarrow \text{收集误检样本}$ 
// 阶段 2: 自适应重检
15. 生成负原型  $p_{\text{neg}}$ 
16. 构建共轭任务对  $(Z1, Z2)$ 
17.  $L_{\text{conj}} \leftarrow \text{交叉熵损失} + \lambda \cdot \text{负原型损失}$ 
18. 微调模型并输出最终结果: "正常" 或 "攻击"
19. END function

```

3 实验结果与分析

3.1 数据集与评价指标

本文采用 ORACLE 开源数据集进行 Wi-Fi 环境下的物理层指纹识别, 数据集由 16 台 USRP X310 设备生成, 遵循 IEEE802.11 协议。本文以 2.45 GHz 中心频率和 5 MHz 采样率采集约 3.2 亿个 I/Q 样本来模拟真实 Wi-Fi 场景, 支持设备认证与检测^[31]。同时, 选取 2 ft 距离数据以匹配车内网络场景, 以减少环境干扰, 提升信号质量和训练效率。数据集包含 8 个正常设备和 8 个攻击设备, 训练集 70%、验证集 10% 和测试集 20%, 以确保类别平衡和模型泛化能力。

为了全面评估模型的性能, 实验采用准确率、精确率、召回率、F1 分数、误报率进行评价, TP 表示正确预测的阳性样本, TN 表示正确预测的阴性样本, FP 表示错误预测的阳性样本, FN 表示错误预测的阴性样本, 如式 (16)~式 (20) 所示。

(1) 准确率。该指标衡量模型整体预测正确样本占总样本的比例。

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \quad (16)$$

(2) 精确率。该指标反映模型预测为正类的样本中实际为正类的比例。

$$Precision = \frac{TP}{(TP + FP)} \quad (17)$$

(3) 召回率。该指标表示所有真实正类样本中被模型正确识别出的比例。

$$Recall = \frac{TP}{(TP + FN)} \quad (18)$$

(4) F1 分数。该指标为精确率与召回率的调和平均, 用于综合评估二者平衡下的模型性能。

$$F1 = \frac{2 * (Precision * Recall)}{(Precision + Recall)} \quad (19)$$

(5) 误报率。该指标指所有真实负类样本中被错误判为正类的比例。

$$FPR = \frac{FP}{(FP + TN)} \quad (20)$$

此外, 本文还采用了 AUROC、FPR95、FNR95、Min (FPR+FNR) 作为补充评估标准, 以便从不同维度衡量模型性能。其中, AUROC 用于衡量模型在所有可能分类阈值下区分正负样本的能力, 数值越接近于 1 表示模型判别性能越好; FPR95 代表在真正例率达到 95% 时对应的假正例率, 反映了模型在高召回场景下的误报水平; FNR95 代表在假正例率控制在 5% 时对应的假负例率, 体现了模型在低误报约束下的漏检程度; Min (FPR + FNR) 是在所有可能阈值下 FPR 与 FNR 之和的最小值, 该值对应使两类错误总和最低的最佳操作点, 常用于衡量模型整体的平衡性能。

3.2 实验结果

3.2.1 LSTM 在数据维度压缩方面的效果

本文所设计的基于深度学习的特征重构机制, 不仅降低了数据维度, 还为后续基于原型匹配的异常检测提供了稳定可靠的输入基础, 如图 3 所示。

由图 3 可见, 降维前的 OFDM 数据在高维空间中呈现出复杂的螺旋状分布 (见图 3(a)), 表明原始信号包含大量冗余和其他信息, 计算复杂度高。图 3(b) 为经过 LSTM 特征提取与压缩后的结果, LSTM 通过其门控机制学习并保留输入序列中最具判别性的时序模式, 将其映射为低维隐藏状态表示, 使得冗余信息被有效抑制, 设备特有的射频指纹特征被提炼为一个低维、紧凑且具有一致性的新特征表示。

3.2.2 共轭训练机制在提升检测性能中的关键作用

本文设计了消融实验, 包含共轭训练的完整模型与移除该机制的模型, 实验结果如图 4 所示。由此可知, 完整的模型在精确率、误报率上显著优于无共轭训练版本, 尽管其召回率略有下降, 但整体 F1 分数仍保持在较高水平, 尤其在误报率方面表现显著, 表明共轭训练有效增强了模型对正常样本的判别能力, 降低了误报, 提升了模型在复杂环境下的安全性与可靠性。

3.2.3 所提方法在两个阶段的性能

本文根据各阶段目标采用差异化的评价指标体系。其中, 表 1 侧重初筛阶段的整体分类能力, 采用 Accuracy、Precision、Recall、F1 和 FPR 等通用指标; 表 2 聚焦重检机制的细粒度判别性能, 采用 Auroc、Fpr95、Fn95 和 Min (fpr+fnr) 等高精度场景专用指标; 表 3 则在统一标准下与主流

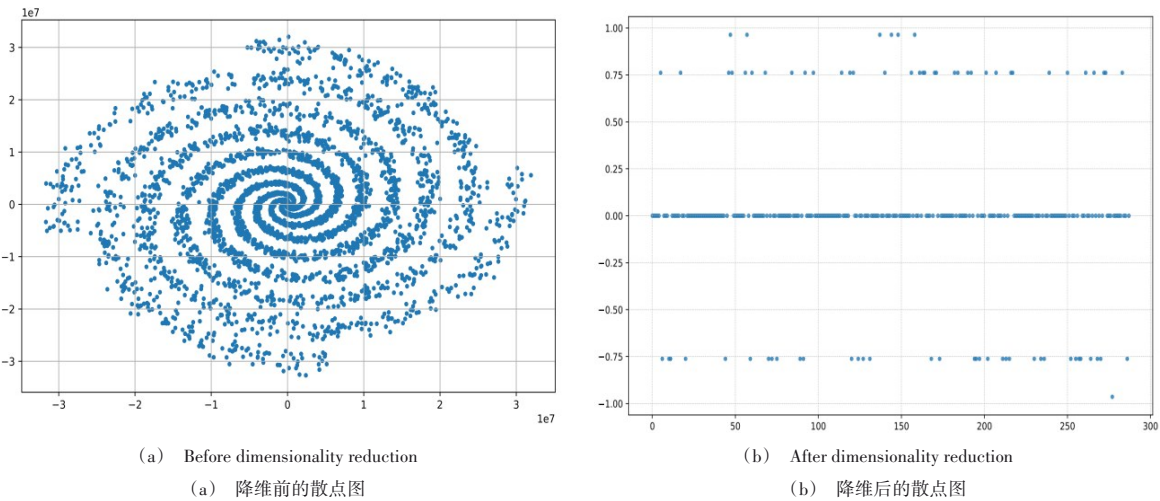


Fig. 3 Scatter plot of OFDM symbols before and after dimensionality reduction

图 3 OFDM 符号降维前后的散点图

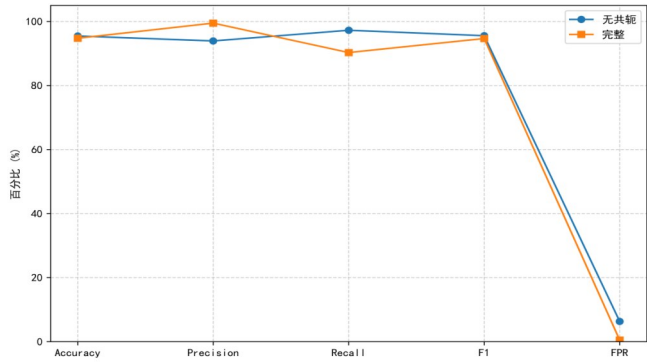


Fig. 4 Ablation experiment

图 4 消融实验

基线模型进行横向对比,沿用 Accuracy、Precision、Recall、F1 和 FPR 以确保比较一致性。

表 1 为第一阶段基于距离的检测策略在初步筛选中的性能表现,主要关注整体分类检测能力。由此可知,该方法在 Accuracy、Recall 和 F1 分数等关键指标上均超过 95%,表明其能有效识别大多数攻击样本,虽然存在一定的误报,但可通过后续阶段进行有效校正,整体仍具备较强的鲁棒性,为第二阶段的复检提供了高质量输入。

Table 1 Performance based on distance detection in the first stage

表 1 第一阶段基于距离检测性能 (%)

指标	Acc	Precision	Recall	F1	FPR
本文方法	95.45	93.90	97.24	95.54	6.33

Table 3 Overall performance comparison

表 3 总性能比较 (%)

指标	Acc	Precision	Recall	F1	FPR
GRU	94.96	94.12	96.34	95.22	6.53
Bilstm	93.20	93.74	92.81	93.27	6.40
Transformer-xl	79.83	83.58	76.18	79.71	16.21
Dual-Attention LSTM-Autoencoder	92.25	93.67	91.00	92.32	6.44
MRFE	87.18	86.89	87.57	86.79	13.21
本文方法	94.75	99.47	90.28	94.66	0.51

表 2 为第二阶段基于负原型与共轭训练策略的自适应复检机制在关键检测指标上的性能表现,重点考察模型在高置信度条件下的判别稳定性,评估指标聚焦于 Auroc、Fpr95、Fn95 和 Min(fpr+fnr)。由此可知,所提方法在 Auroc 上达到 0.97,表明其整体判别能力较强;Fpr95 指标低至 0.050 6,显著优于传统方法;Fn95 为 0.029 6,在高置信度下仍能有效识别异常设备。特别的,Min(fpr+fnr)指标仅为 0.085 1,表明模型在最优阈值下实现了误报与漏报之和的最小化,充分体现了其在“安全—可用”权衡中的优化能力。此外,系统基于负原型与共轭训练的动态拒绝边界机制,能在无需人工设定阈值的前提下,显著提升检测的鲁棒性与实用性。

Table 2 Adaptive re-detection performance in the second stage

表 2 第二阶段自适应复检性能

指标	Acc	F1	Recall	Auroc	Fpr95	Fn95	Min(fpr+fnr)
本文方法	0.92	0.92	0.92	0.97	0.050 6	0.029 6	0.085 1

表 3 进一步展示了本文方法与 GRU、BiLSTM、Transformer-xl、Dual-Attention LSTM-Autoencoder^[19,20,32,33]、MRFE 等主流模型的综合性能^[19,20,32,33]。在准确率方面,本文方法达到了 94.75%,仅次于 GRU,但在误报率上优势明显;精确率为 99.47% 高于表 1 中的 95.54%,误报率远低于表 1 的 6.33%,表明第二阶段有效抑制了初筛阶段的误报,充分验证了两阶段递进式优化机制的有效性。

综上,实验表明所提方法不仅能高效识别恶意设备,还能有效减少对正常通信行为的误判,降低了因频繁误警带来的安全风险和运维负担。尽管本文方法的召回率略低于GRU,但在精确率与召回率之间的平衡方面仍展现出优异的表现。

4 结语

由于智能网联汽车设备的伪装接入可能会导致严重的安全威胁,而传统检测方法难以应对硬件级仿真攻击,且普遍依赖固定阈值,缺乏环境适应性。为此,本文提出一种基于OFDM符号级射频指纹的自适应恶意设备检测方法。

首先,通过协议对齐与结构化预处理提取的时序I/Q序列,结合LSTM建模设备特有的瞬态响应;其次,引入多头注意力的负原型生成机制,构建高判别性特征空间;最后,设计融合共轭训练与余弦距离的自适应判别策略,利用正负原型间的相对相似度动态判定,实现无需人工阈值的鲁棒检测。

在Oracle数据集上的实验表明,所提方法的准确率、精确率、误报率分别为94.75%、99.47%和0.51%,在少样本场景下仍具有良好的泛化能力。

参考文献:

- [1] HOSSAIN S M M, BANIK S, BANIK T, et al. Survey on security attacks in connected and autonomous vehicular systems[C]// 2023 IEEE International Conference on Computing, 2023: 295-300.
- [2] Security Affairs. Hacking Volkswagen group infotainment unit flaws could allow attackers to compromise vehicles[EB/OL]. <https://securityaffairs.com/172024/hacking/volkswagen-group-infotainment-unit-flaws.html>.
- [3] SANDERS C, WANG Y. Localizing spoofing attacks on vehicular GPS using vehicle-to-vehicle communications[J]. IEEE Transactions on Vehicular Technology, 2020, 69(12): 15656-15667.
- [4] BAJRACHARYA C. Performance evaluation for secure communications in mobile internet of vehicles with joint reactive jamming and eavesdropping attacks[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 23(11): 22563-22570.
- [5] LI Q J, HOU W X, WANG Z Y, et al. Vehicle CAN bus intrusion detection method based on SVDD[J]. Electronic Design Engineering, 2025, 33(19): 55-59, 64.
李泰君, 侯文昕, 王之雨, 等. 基于SVDD的车载CAN总线入侵检测方法[J]. 电子设计工程, 2025, 33(19): 55-59, 64.
- [6] SHEN Z B, LIAO G Z. Vehicle mounted CAN bus anomaly detection based on improved sparse autoencoder[J]. Computer and Digital Engineering, 2025, 53(7): 1928-1933, 1953.
申子彬, 廖光忠. 基于改进稀疏自编码的车载CAN总线异常检测[J]. 计算机与数字工程, 2025, 53(7): 1928-1933, 1953.
- [7] ZHANG Z, ZHANG J F, LIU S X, et al. Anomaly detection of vehicle data flow based on heterogeneous LSTM and AM[J]. Computer Simulation, 2025, 42(7): 6-14, 579.
张震, 张金锋, 刘少勋, 等. 基于异构LSTM和AM的车载数据流异常检测[J]. 计算机仿真, 2025, 42(7): 6-14, 579.
- [8] DONG M Y, FU Y C, NIU X J. Integration of sensing and computing in 6g connected vehicles: current status and challenges[J]. Radio Communication Technology, 2023, 49(1): 37-45.
董梦圆, 付宇钊, 牛晓健. 6G车联网中的通感算融合:现状与挑战[J]. 无线电通信技术, 2023, 49(1): 37-45.
- [9] JAGANNATH A, JAGANNATH J, KUMAR P S P V. A comprehensive survey on radio frequency (RF) fingerprinting: traditional approaches, deep learning, and open challenges[J]. Computer Networks, 2022, 219: 109455.
- [10] BRIK V, BANERJEE S, GRUTESER M, et al. Wireless device identification with radiometric signatures[C]// 14th ACM International Conference on Mobile Computing and Networking, 2008: 116-127.
- [11] WANG S, JIANG H, FANG X, et al. Radio frequency fingerprint identification based on deep complex residual network[J]. IEEE Access, 2020, 8: 204417-204424.
- [12] LIN Y, WANG H, ZHA H. The technology of radio frequency fingerprint identification based on deep learning for 5G application[J]. Security and Safety, 2024, 3: 2023026.
- [13] QING G, WANG H, ZHANG T. Radio frequency fingerprinting identification for Zigbee via lightweight CNN[J]. Physical Communication, 2021, 44: 101250.
- [14] HUANG R, PENG X, CHAI Z, et al. Radio frequency fingerprint extraction and authentication towards open set in noisy channels[J]. Digital Signal Processing, 2024, 146: 104363.
- [15] MA J, ZHANG J, SHEN G, et al. Towards channel-robust radio frequency fingerprint identification using contrastive learning[C]// 2025 IEEE Wireless Communications and Networking Conference, 2025: 1-6.
- [16] CHEN X, WANG L D, XU X, et al. A review of RF fingerprint recognition methods based on Raw I/Q and deep learning[J]. Journal of Radar, 2023, 12(1): 214-234.
陈翔, 汪连栋, 许雄, 等. 基于Raw I/Q和深度学习的射频指纹识别方法综述[J]. 雷达学报, 2023, 12(1): 214-234.
- [17] WANG H, LUO J S, WANG H M, et al. Overview of radio frequency fingerprint recognition methods for drones[J]. Radio Engineering, 2024, 54(11): 2672-2684.
王豪, 罗俊松, 王惠明, 等. 无人机射频指纹识别方法综述[J]. 无线电工程, 2024, 54(11): 2672-2684.
- [18] HUANG H. Design and Implementation of wireless LAN security monitoring system[D]. Beijing: Beijing University of Posts and Telecommunications, 2021.
黄河. 无线局域网安全监测系统的设计与实现[D]. 北京: 北京邮电大学, 2021.
- [19] WANG M H, DENG Y H, WEI B. Network anomaly traffic detection method based on RF-BiLSTM[J]. Communication Technology, 2024, 57(12): 1297-1304.
王梦寒, 邓永晖, 魏波. 基于RF-BiLSTM的网络异常流量检测方法[J]. 通信技术, 2024, 57(12): 1297-1304.

- [20] DAI Z, YANG Z, YANG Y, et al. Transformer-xl: attentive language models beyond a fixed-length context[C]// Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics, 2019: 2978–2988.
- [21] ZENG L, JIN Q, LIN Z, et al. Dual-attention LSTM autoencoder for fault detection in industrial complex dynamic processes[J]. Process Safety and Environmental Protection, 2024, 185: 1145–1159.
- [22] LU Q, YANG Z, ZHANG H, et al. MRFE: a deep-learning-based multidimensional radio frequency fingerprinting enhancement approach for IoT device identification[J]. IEEE Internet of Things Journal, 2024, 11(18): 30442–30454.
- [23] LIU Y, WANG J, LI J, et al. Class-incremental learning for wireless device identification in IoT[J]. IEEE Internet of Things Journal, 2021, 8(23): 17227–17235.
- [24] SUN Q, MIAO X, GUAN Z, et al. Spoofing attack detection using machine learning in cross-technology communication[J]. Security and Communication Networks, 2021(1): 3314595.
- [25] ZHANG J H, SHI L Z, YU L, et al. Channel universal pre trained large model empowering digital twin channels: principles and practices[J]. Radio Engineering, 2025, 55(4): 679–686.
张建华, 史廉正, 于力, 等. 信道通用预训练大模型赋能数字孪生信道: 原理与实践[J]. 无线电工程, 2025, 55(4): 679–686.
- [26] HALBOUNI A, GUNAWAN T S, HABAEBI M H, et al. CNN-LSTM: hybrid deep neural network for network intrusion detection system[J]. IEEE Access, 2022, 10: 99837–99849.
- [27] XIE L, PENG L, ZHANG J. Towards robust RF fingerprint identification using spectral regrowth and carrier frequency offset[C]// IEEE Infocom, 2025: 1–10.
- [28] GONG J, XU X, LEI Y. Unsupervised specific emitter identification method using radio-frequency fingerprint embedded InfoGAN[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 2898–2913.
- [29] REUS-MUNS G, JAISINGHANI D, SANKHE K, et al. Trust in 5G open RANs through machine learning: RF fingerprinting on the POWDER PAWR platform[C]// 2020 IEEE Global Communications Conference, 2020: 1–6.
- [30] MA J G, WEN F, YIN X Y. Meta faster R-CNN small sample object detection based on support set feature enhancement [J]. Journal of Shenyang University of Technology, 2025, 44(2): 48–54.
马俊光, 文峰, 殷向阳. 基于支持集特征增强的 Meta Faster R-CNN 小样本目标检测[J]. 沈阳理工大学学报, 2025, 44(2): 48–54.
- [31] SANKHE K, BELGIOVINE M, ZHOU F, et al. ORACLE: optimized radio classification through convolutional neural networks[C]// IEEE INFOCOM 2019–IEEE Conference on Computer Communications, 2019: 370–378.
- [32] ABDULLAH H S, ALI N H, ABDULLAH N A Z. Evaluating the performance and behavior of CNN, LSTM, and GRU for classification and prediction tasks[J]. Iraqi Journal of Science, 2024, 65(3): 1741–1751.
- [33] ZENG L, JIN Q, LIN Z, et al. Dual-attention LSTM autoencoder for fault detection in industrial complex dynamic processes[J]. Process Safety and Environmental Protection, 2024, 185: 1145–1159.
- [34] SHI J, PENG L, FU H, et al. Robust RF fingerprint extraction based on cyclic shift characteristic[J]. IEEE Internet of Things Journal, 2023, 10(21): 19218–19233.

(责任编辑:刘嘉文)