

基于孪生对抗训练的车联网 C-V2X 终端指纹识别^{*}杨 颢¹ 程杨晨^{2,3} 李 燕^{2,3} 胡爱群⁴

(1. 无锡学院网络空间安全学院 无锡 214105; 2. 无锡学院物联网工程学院 无锡 214105;

3. 南京信息工程大学计算机学院、网络空间安全学院 南京 210044; 4. 东南大学信息科学与工程学院 南京 210096)

摘 要: 蜂窝车联网(C-V2X)作为智能网联汽车的代表性通信技术,通过构建高可靠的通信链路,实现车与车、车与基础设施及车与人之间的数据交互。然而,车联网复杂多变的通信环境使得终端身份接入面临重大挑战。射频指纹(RFF)由于具备唯一性、稳定性和不可克隆的特点,可以为 C-V2X 终端身份接入提供物理层安全方案。基于此,提出了一种 C-V2X 终端射频指纹提取及认证方案:首先通过设计有效预处理算法分离物理侧链路共享信道(PSSCH)和控制信道(PSCCH)中的解调参考信号(DMRS);采用对数谱分离算法来抑制因 DMRS 序列随机化带来的噪声分量;设计了一种基于孪生对抗网络(SANet)的训练方法,使特征提取网络专注于提取硬件相关的设备指纹。实验结果表明:所设计的预处理和对数谱去噪算法在多场景中均可有效提升终端指纹的稳定性和识别准确率;SANet 在跨信道环境下测试显示出良好的泛化能力,其中静止场景的认证平均精确率和召回率可达 93.22%和 92.67%,移动场景下可达 82.85%和 82.21%。

关键词: C-V2X;DMRS;射频指纹;SANet**中图分类号:** TN929.5 **文献标识码:** A **国家标准学科分类代码:** 520.2040Siamese adversarial training-based C-V2X terminal fingerprint
identification in the internet of vehiclesYang Yang¹ Cheng Yangchen^{2,3} Li Yan^{2,3} Hu Aiqun⁴

(1. School of Cyber Science and Engineering, Wuxi University, Wuxi 214105, China;

2. School of Internet of Things Engineering, Wuxi University, Wuxi 214105, China; 3. School of Computer Science and

School of Cyberspace Security, Nanjing University of Information Science and Technology, Nanjing 210044, China;

4. School of Information Science and Engineering, Southeast University, Nanjing 210096, China)

Abstract: Cellular vehicle-to-everything (C-V2X), as a representative communication technology for intelligent connected vehicles, enables data interaction between vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-pedestrian by establishing highly reliable communication links. However, the complex and variable communication environment of the internet of vehicles poses significant challenges to terminal identity access. Due to its characteristics of uniqueness, stability, and unclonability, radio frequency fingerprint (RFF) can provide a physical layer security solution for C-V2X terminal identity access. Based on this, this paper proposes a C-V2X terminal radio frequency fingerprint extraction and authentication scheme: First, an effective preprocessing algorithm is designed to separate the demodulation reference signal (DMRS) in the physical sidelink shared channel (PSSCH) and the physical sidelink control channel (PSCCH); a logarithmic spectrum separation algorithm is adopted to suppress the noise components caused by the randomization of the DMRS sequence; a training method based on the siamese adversarial network (SANet) is designed to make the feature extraction network focus on extracting hardware-related device fingerprints. Experimental results show that the designed preprocessing and logarithmic spectrum denoising algorithms can effectively improve the stability and recognition accuracy of terminal fingerprints in multiple scenarios; the SANet exhibits excellent generalization ability in cross-channel environment tests; The average authentication precision and recall reach 93.22% and 92.67% in static scenarios, and 82.85% and 82.21% in mobile scenarios, respectively.

Keywords: C-V2X;DMRS;radio frequency fingerprint;SANet

0 引 言

车联网(vehicle-to-everything, V2X)技术已成为实现

车辆与车辆、车辆与基础设施、车辆与人之间高效互联的核心支撑^[1]。在车载网络通信领域,专用短程通信(dedicated short-range communications, DSRC)和蜂窝车联网(cellular

vehicle-to-everything, C-V2X) 形成两大主流技术标准。C-V2X 作为第 3 代合作伙伴 (3rd generation partnership project, 3GPP) 定义的蜂窝车联网解决方案, 以长期演进车联网 (long term evolution-vehicle-to-everything, LTE-V2X) 为当前主流技术, 逐步向 5G 新空口车联网 (5th generation new radio-vehicle-to-everything, 5G-V2X) 演进, 为未来交通系统智能化升级奠定基础^[2-3]。

然而, 无线网络天然具备的开放性, 使得 C-V2X 系统面临严峻的安全威胁。例如在 C-V2X 的直接模式通信 (proximity communication, PC5) 中, 虚假数据注入与伪装攻击风险始终存在^[4], 传统高级加密算法虽然能提供有效防护, 但会消耗大量计算资源且解密过程会增加数据包传输延迟^[5]。因此, 迫切需要探索多种适用于车联网通信环境的轻量级安全接入机制, 以精准识别信息广播者身份, 抵御恶意用户攻击, 保障车联网通信安全^[6]。

射频指纹 (radio frequency fingerprint, RFF) 源于无线发射机模拟电路内部电子元器件的微小差异^[7], 这些差异致使发射机无线信号中存在特有的硬件特征, 具有唯一性与长时稳定性, 可以为设备身份接入提供轻量级物理层安全认证方案^[8]。

在相关研究中^[9-18], 学者们针对 C-V2X 的 RFF 提取与识别提出了多种不同方法。Chen 等^[9]利用物理侧链路广播信道 (physical sidelink broadcast channel, PSBCH) 展开 RFF 提取的研究, 并基于最小二乘法 (least squares, LS) 加窗估计去除无线信道响应。PSBCH-LS 方案在 6 个 C-V2X 模块的分类平均准确率超过 90%。Qi 等^[10]则利用 PSBCH 中的主同步信号作为输入, 结合修正 Gramian 角场 (modified angular gramian field, MAGF) 和马尔可夫概率转移矩阵 (markov transition probability matrix, MTTD) 挖掘时间相关性特征。针对 C-V2X 系统, 作者进一步分析宽带系统中带外指纹的分布规律, 并设计了带外 RFF 的提取方法^[11]。虽然 PSBCH 格式帧结构相对固定, 但其较长的传输间隔 (160 ms) 导致 PSBCH 子帧数量无法大量被捕获, 从而限制了其在射频指纹识别 (radio frequency fingerprint identification, RFFI) 中的使用。相反, 用于承载数据和控制信息的物理侧链路共享信道/控制信道 (physical sidelink shared channel/physical sidelink control channel, PSSCH/PSCCH) 子帧在 C-V2X 通信中大量存在, 但在之前的 RFFI 研究中尚未被提出。

从数据依赖性来看, RFFI 可分为数据有关和数据无关方法。前者从固定的稳态信号序列中提取指纹。例如, 在 IEEE 802.11 正交频分复用 (orthogonal frequency division multiplexing, OFDM) 协议中, 包括由短训练字段 (short training field, STF) 和长训练字段 (long training field, LTF) 组成的前导码。Xing 等^[12]利用 Wi-Fi 的 LTF 和 STF 提取对数频谱特征, 用于识别 7 个路由器。另一方面, Zhang 等^[13]从 LoRa 的固定前导信号中提取 RFF, 并使用数据增强技术

来增强认证模型的鲁棒性, 对 25 个 LoRa 设备实现了 99% 的识别准确率。相反, 后者从非固定符号序列 (如实际通信中的随机数据段) 中提取指纹。以基于 LTE 移动终端的 RFFI 方案为例, Peng 等^[14]通过从物理随机接入信道 (physical random access channel, PRACH) 信号的瞬态阶段和稳态部分提取小波系数来识别 LTE 手机。Li 等^[15]提出了一种频域倒谱相关性和 RFF 盲提取方法, 该方法不需要 Zadoff-Chu (ZC) 参数的任何先验知识, 即可使用 PRACH 信号来认证 LTE 上行链路设备。尽管实验表明混合信号特征可以增强识别能力, 但瞬态 RFF 严重依赖于接收器的采样分辨率, 从而限制了它们的实用性。因此, 如何在随机信号字段下, 实现数据无关 RFF 提取, 成为当前研究的难题。

此外, C-V2X 复杂多变的信道条件加剧了 RFF 的识别难度。一方面, 多径信道响应和硬件导致的信号失真相互叠加, 难以分离出射频指纹。Lu 等^[16]提出了一种基于深度学习的多维射频指纹增强物联网设备识别方法 MRFE, 该方法通过将原始的 IQ 信号解剖为多个维度, 并运用指纹增强技术结合注意力机制, 对信号特征进行提取并融合形成射频指纹, 在公共 ORACLE 数据集上达到 99.93% 识别准确率。Kong 等^[17]提出 Micro-CSI 方法, 利用信道状态信息 (channel state information, CSI) 提取 RFF, 通过时域分离出信道响应, 采用 K 近邻算法结合曼哈顿距离实现合法/非法设备区分; 在强视距场景下, 仅需 20 个 CSI 样本即可达成 99% 攻击检测率与 0% 误报率。后续进一步提出 DeepCRF^[18]方法, 该方法采用数据增强技术, 有效提升了模型对新的、未知信道条件的适应性和泛化能力, 同时结合监督对比学习策略, 显著增强了模型对噪声的鲁棒性, 在 19 个 COTS WiFi 网络接口卡中实现了 99.53% 的平均识别准确度。但上述研究^[16-18]的实验场景多局限于静态环境, 不能适应车联网复杂多变的信道环境。因此, 在 C-V2X 移动通信中, 如何从复杂信道中精准提取射频指纹特征, 仍是当前研究中极具挑战性的问题。

针对 C-V2X RFFI 中, PSBCH 子帧数量较少、随机信号字段下 RFF 提取难、认证模型泛化能力弱 3 大难题, 本文提出一种基于 PSSCH/PSCCH 帧的射频指纹提取及认证方案, 主要贡献包括:

1) 首次提出以 PSSCH/PSCCH 作为 C-V2X 中 RFF 提取的信号目标, 并设计完整的多符号精准同步-频偏补偿-定时偏移补偿预处理流程, 实现 PSSCH/PSCCH 帧内 DMRS 符号的精准分离, 有效提升 RFF 的稳定性。

2) 提出对数谱分离-离散小波变换 (discrete wavelet transform, DWT) 联合去噪算法; 通过对数域分析揭示 RFF 与随机数据引起的噪声的可分离性, 采用小波基分解, 解决随机 ZC 序列的 RFF 提取难题。

3) 设计孪生对抗网络 (siamese adversarial network, SANet) 实现指纹、信道解耦, 同时融合卷积块注意力模块 (convolutional block attention module, CBAM), 使特征提

取网络聚焦不易受信道扰动的特征空间区域,从而解决跨信道、移动场景下泛化能力弱的问题。

实验通过软件无线电平台(universal software radio peripheral, USRP)采集 10 台 C-V2X 终端信号,并构成多域数据集用于交叉验证测试。消融实验表明:预处理算法可使 F1-Score 平均提升 10% 以上,对数谱去噪算法可使 F1-Score 平均提升 10.05%;多域交叉测试结果表明:在跨信道环境下,静止场景认证的平均精确率、召回率分别达 93.22%、92.67%,移动场景分别为 82.85%、82.21%,在多种通信场景下认证性能良好。

1 系统流程与预处理

1.1 系统模型

图 1 为终端认证实施流程。首先通过 USRP 采集 C-V2X 终端设备发送的 PSSCH/PSCCH 信号。并将接收到的 PSSCH/PSCCH 子帧进行信号预处理,包括:OFDM 时频同步、频偏补偿、提取 DMRS 序列、定时偏移补偿。随后在对数谱域消除因随机序列带来的数据噪声。最后将处理后的信号加入认证模块,输入 SANet 得到认证结果。

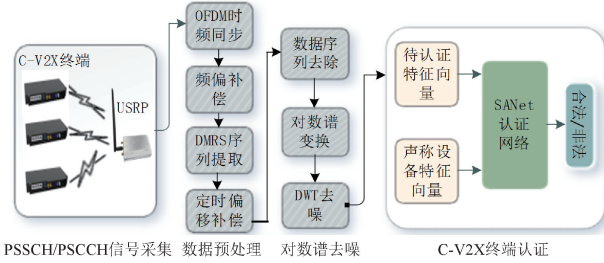


图 1 C-V2X 系统认证流程

Fig. 1 C-V2X system certification

1.2 帧结构

PSSCH 信号的主要功能是在车辆之间传输应用层数据, PSCCH 则包含诸如发射功率控制和调制编码方案选择等控制信息,两者在时频域捆绑发送。PSSCH/PSCCH 的具体帧结构如图 2 所示,由 14 个符号组成。第 1 个符号 AGC 用于自动增益控制调整,最后一个符号 GP 固定为发射-接收切换符号,即保护间隔符号。此外,索引为 2、5、8 和 11 的符号是 DMRS,用于接收端的正确解调和信道估计。其余符号是用于传输应用层信息的数据符号。

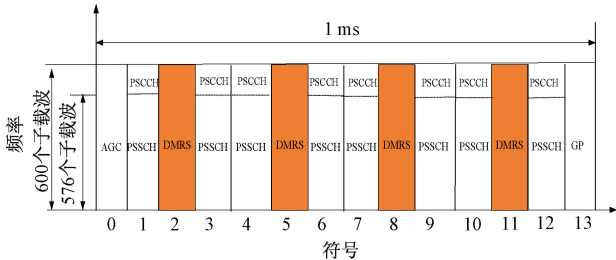


图 2 C-V2X PSSCH/PSCCH 帧结构

Fig. 2 Frame structure of C-V2X PSSCH/PSCCH

在 PSSCH/PSCCH 信号中,DMRS 是基于 ZC 序列生成,其优异的自相关特性可以减少噪声对信道估计的响应,并提升解调的精度;而在车联网通信中,终端移动会导致多普勒频偏,多径会导致时延扩展,而 ZC 序列对信道损伤具有较强的抗干扰能力。因此,本研究选用 PSSCH/PSCCH 子帧中 4 个 DMRS 符号进行 RFF 提取。

1.3 信号预处理

1) 基于循环前缀(cyclic prefix, CP)的多符号精准同步

PSSCH/PSCCH 子帧中 DMRS 符号精确定位是 RFF 提取的前提,同步错位会使其混入相邻数据符号,导致 RFF 受数据序列干扰;因此在 USRP 采集 PSCCH/PSSCH 信号后,需要获得每个子帧精准的起点。PSCCH/PSSCH 每个符号的 CP 是一个 OFDM 符号尾部数据序列的拷贝,因此 CP 和符号的尾部之间的相关性远大于其他区域,可以利用该特性进行同步运算。

首先,对接收到的信号 $r(n)$ 偏移一个符号长度 $Nfft$,从位置 n 开始取第 1 个符号 CP 段的长度 N_g 进行自相关,得到相关函数 $cor(n)$:

$$cor(n) = \sum_{m=0}^{N_g-1} r(n+m)r^*(n+m+Nfft) \quad (1)$$

其中, r^* 右上角 * 为共轭运算,计算 $cor(n)$ 第 1 个波峰对应位置得到子帧的大致起始位置 p ,完成粗同步,即:

$$p = \arg \max_{n \in [0, N_g+Nfft]} cor(n) \quad (2)$$

仅依赖首个符号 CP 相关性定位子帧起点在低信噪比或移动场景会存在误判,因此需要联合后续 13 个符号进行联合估计。将 n 作为子帧起始点时 $n \in (p-15, p+15)$, 14 个符号 CP 与相应符号尾部的相关值之和 $cor'(n)$ 为:

$$cor'(n) = \sum_{i=1}^{14} cor[\sum_{j=1}^i N_g(j) + i \cdot Nfft + n] \quad (3)$$

计算 $cor'(n)$ 峰值对应位置,对应使得子帧内所有循环前缀与对应符号尾部相关度总和最高的位置,即为子帧起点 syn ,即:

$$syn = \arg \max_{n \in [p-15, p+15]} cor'(n) \quad (4)$$

2) 频偏补偿

由于接收机和发射机之间存在频偏,在得到同步后的信号为 $r_{syn}(n)$,需要对同步后信号进行频偏估计。记每个符号对应的时域信号为 $r_{syn,i}(n)$, $i \in \{1, 2, \dots, 14\}$,对其 CP 段的信号位与符号尾部信号位进行共轭相乘,得到 CP 与符号尾部相位平均差值 $\Delta\psi_i$:

$$\Delta\psi_i = \text{angle}[\sum_{k=0}^{N_g(i)} r_{syn,i}(n) \cdot r_{syn,i}^*(n+Nfft)], i \in \{1, 2, \dots, 14\} \quad (5)$$

其中, $r_{syn,i}^*$ 右上角 * 为共轭运算。通过 CP 段与符号尾部的相位平均差值 $\Delta\psi_i$ 进行频偏运算得到每个符号的频偏 Δf_i , 其中 f_s 为信号采样率。

$$\Delta f_i = \frac{\Delta \psi_i}{2\pi \cdot Nfft} \cdot f_s \quad (6)$$

最后,根据估计出的频偏 Δf_i 对同步的信号逐点做相位旋转进行频偏补偿,得到校正后的序列:

$$r_{c,i}(n) = r_i(n) e^{-j \cdot 2\pi \cdot \Delta f_i \cdot n / f_s}, i \in \{1, 2, \dots, 14\} \quad (7)$$

3) DMRS 序列提取

PSSCH/PSCCH 帧结构中,每个 PSCCH 子帧包含 4 个 DMRS 符号,每个 DMRS 符号对应频域子载波集合。对第 i 个 DMRS 符号的频域子载波记为 $DMRS_i$,将第 k 种基序列记为 $PSCCH_DMRS_k, k \in \{1, 2, 3, 4\}$ 。计算首个子载波相位作为整体偏移量,进行相位矫正,矫正后子载波经标准化与归一化处理,得到 sub_DMRS 。将 sub_DMRS 与基序列 $PSCCH_DMRS$ 做比较,判断 DMRS 所属序列类型 $type$, 即:

$$type = \begin{cases} k, & sub_DMRS = PSCCH_DMRS_k \\ 0, & \text{其他} \end{cases} \quad (8)$$

对 PSCCH 的 4 个 DMRS 分别判断序列类型,将得出的第 i 个 DMRS 的判别序列类型记为 $type_i$ 。记 $num(l), l \in \{1, 2, 3, 4\}$ 为 $type_i = l$ 的 DMRS 个数。得到 PSCCH DMRS 本地序列 $R_{i,local}^{PSCCH} = PSCCH_DMRS_{type_i}$ 。

从 PSCCH 数据部分提取侧行控制信息 (sidelink control information, SCI), 计算循环冗余校验 (cyclic redundancy check, CRC) 值作为参数 n_{ID} 。由于 n_{ss}^{PSCCH} 无法直接获取,遍历其可能取值 ($0 < n_{ss}^{PSCCH} < 3$),生成候选序列,计算生成序列与接收 PSSCH DMRS 的相关值,选择相关值最大的 n_{ss}^{PSCCH} 作为有效参数,确定本地序列: R_{local}^{PSCCH} 。

4) 定时偏移补偿

在无线通信信号处理中,由于收发端时钟不一致导致接收信号发生采样定时偏移,为消除此类相位失真,需进行线性偏移补偿,具体计算为:

对每个 DMRS 符号的实际序列 R_{DMRS} 与本地序列 R_{local} , 计算逐点相位偏移,即:

$$A(k) = \{\angle[R_{DMRS}(k) \cdot R_{local}^*(k)]\}_{k=0}^{M-1} \quad (9)$$

其中, R_{local}^* 右上角 * 为共轭运算。对相位偏移 A 进行一阶多项式拟合,得到线性相位偏移函数 $A'(k) = a \cdot k + b$, 补偿后的序列为:

$$R(k) = R_{DMRS}(k) \cdot \exp(-j \cdot A'(k)) \quad (10)$$

频偏补偿与定时偏移补偿均针对 C-V2X 终端射频指纹提取中的关键相位干扰设计,前者消除收发端频偏偏差影响,后者剥离收发端时钟偏差干扰。如图 3 所示,频偏及定时偏移补偿前后 DMRS 序列与理想序列的相关值大幅提升,可以有效消除影响 RFF 稳定的相位偏移量。

2 基于信道对抗的 C-V2X 射频指纹识别

2.1 对数谱分离数据噪声

经过信号预处理过后,DMRS 的频域模型可以表示为:

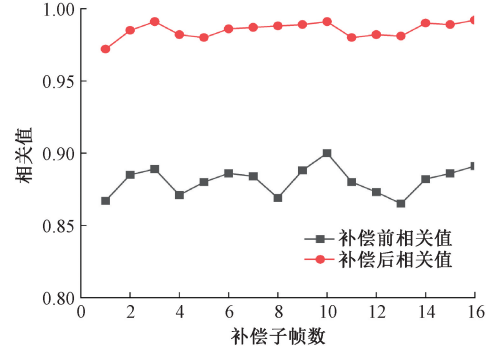


图 3 补偿前后相关值对比

Fig. 3 Comparison of correlation values before and after compensation

$$R(k) = S(k)G(k)H(k) + Z(k) \quad (11)$$

其中, $G(k)$ 为射频指纹分量, $S(k)$ 为 ZC 理想序列, $H(k)$ 为多径响应分量, $Z(k)$ 为加性噪声。其中 ZC 序列可建模为:

$$S_u(m) = e^{-j \frac{\pi u m^2}{N}}, m = 0, 1, \dots, N-1 \quad (12)$$

其中, u 为根索引, N 为序列长度。ZC 序列的根索引、循环移位等生成参数需适配多用户复用、时隙动态分配机制,导致序列参数动态变化,造成 ZC 序列随机化,无法利用固定的序列进行 RFF 提取。为了获取数据无关性指纹,首先对 $R(k)$ 进行去除数据序列 $S(k)$ 处理,可获得以下表达:

$$\tilde{R}(k) = G(k)H(k) \left(1 + \frac{Z(k)}{S(k)G(k)H(k)}\right) \quad (13)$$

其中, $(1 + \frac{Z(k)}{S(k)G(k)H(k)})$ 可建模为由随机序列和信道及高斯噪声共同产生的分量。为了去除该分量,对式 (13) 取对数得到对数谱信号:

$$\hat{R}(k) = \ln G(k) + \ln H(k) + \ln \left(1 + \frac{Z(k)}{S(k)G(k)H(k)}\right) \quad (14)$$

其中, $\ln G(k), \ln H(k)$ 可建模为慢变分量,而 $\ln(1 + \frac{Z(k)}{S(k)G(k)H(k)})$ 建模为快变分量。为了去除主要由 ZC 序列随机化产生的快变分量,对上式获取的结果可采用 DWT 实现变量分离:将处理后的信号 $\hat{R}(k)$ 采用 DB3 小波基进行 3 层分解,对各层细节系数施加软阈值处理,最终重构出去噪后的射频特征。

图 4(a) 为通过射频电缆直连采集的 DMRS 信号,即使在最大 20 dBm 的发射功率下,采集的信号因随机序列导致较大的抖动噪声。在 DWT 去噪后,如图 4(b) 所示,噪声分量被显著抑制,DMRS 子载波稳定性大幅提升。最终,将去噪后的四路子载波进行叠加求平均得到 $\mathbf{X}(k)$, 并送

入到设计的孪生认证网络进一步的特征提取及识别。

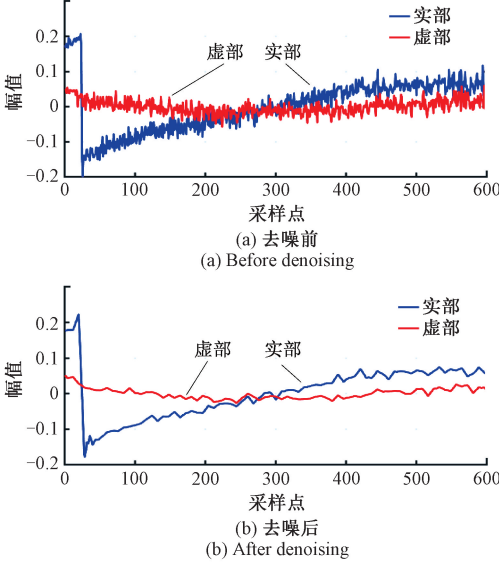


图 4 对数谱去噪前后信号对比图

Fig. 4 Signal comparison before and after DWT denoising

2.2 基于对抗训练的信道解耦方法

图 5 为直连(direct link, DL)、视距(line of sight, LOS)、非视距(non-line of sight, NLOS)及移动(movement, MOV)场景下短时采集的 DMRS 子载波幅度热力图。其中,图 5(a)中不同场景下子载波幅度存在显著的差异性,而同一场景下相同子载波又存在一致性;图 5(b)中,设备处于移动状态下,信道具有随机性,因此子载波幅度呈现一定的

随机性。

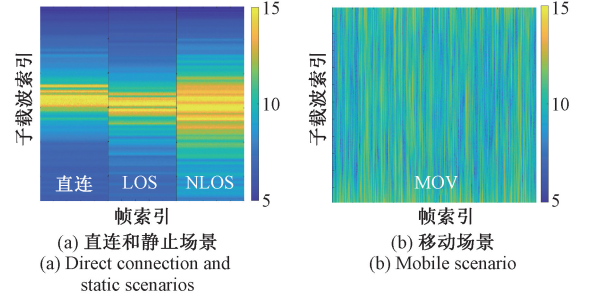


图 5 不同信道场景下子载波幅度热力图

Fig. 5 Subcarrier amplitude heatmap in different channel scenarios

综上,图 5 体现了不同信道场景下,子载波具有显著的差异性;而在同一场景下短时距采集的信号中,子载波又具有很好的一致性。因此可利用上述规律来构建基于 SANet 的信道与 RFF 解耦方法。

2.3 SANet 模型架构

SANet 模型结构如图 6 所示,以孪生网络^[19]为基础,利用权重共享分支实现设备特征对比,并借鉴领域自适应网络(domain-adversarial neural network, DANN)中特征提取-领域分类双模块对抗博弈思想^[20-21],新增信道域标签预测分支并插入梯度反转层(gradient reversal layer, GRL),通过“最小化设备认证损失+最大化信道域识别损失”的对抗目标,剥离信道干扰对指纹的叠加影响;同时结合 CBAM 的注意力增强特性,提升指纹的提取精度与抗干扰能力,提升设备指纹的跨信道鲁棒性,主要由 3 部分组成:

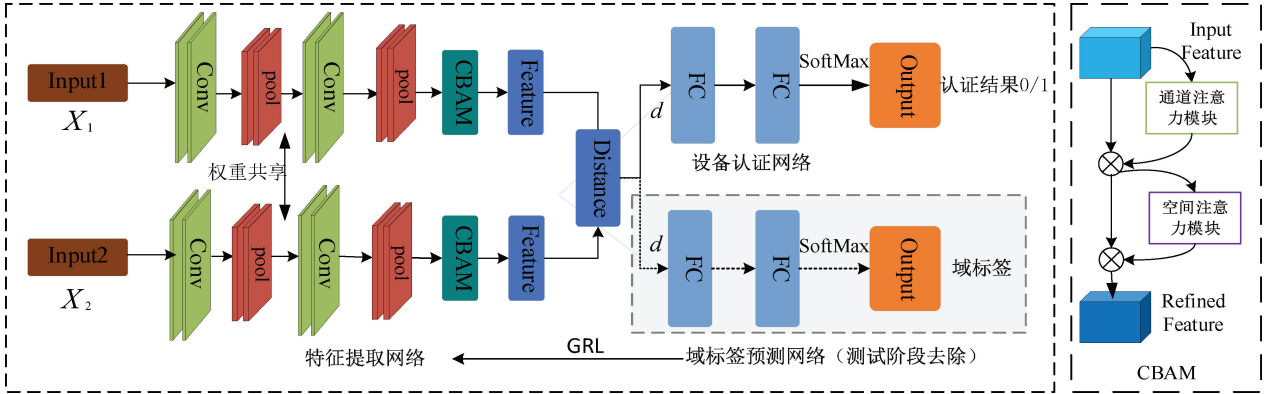


图 6 SANet 模型结构

Fig. 6 SANet model structure

1) 权重共享的特征提取网络

输入为经预处理、对数谱去噪后的特征向量对 (X_1, X_2) , 其中 X_1 为待认证设备的特征向量, X_2 则为待认证设备所声称合法设备的预存特征向量。两者输入权重共享的特征提取网络 $G_f(X, \theta_f)$ 。特征提取网络被设计为卷积层、池化层及融合 CBAM。CBAM 模块利用通道注意力自适应强化设备指纹主导的特征通道,抑制信道噪声干扰的

冗余通道;通过空间注意力聚焦信号中设备固有畸变的局部区域,精确特征提取;最终产生一个 400 维的特征输出,得到一个 D 维特征向量 $f \in \mathbf{R}^D$, 表示为 $f = G_f(X, \theta_f)$ 。 θ_f 表示特征提取网络中的参数。

对于输入样本对得到的两个特征向量 $f_1 = G_f(X_1, \theta_f)$ 、 $f_2 = G_f(X_2, \theta_f)$, 两个特征向量的距离向量计算为:

$$D(f_1, f_2) = \|f_1 - f_2\|_2^2 \quad (15)$$

2) 双标签预测网络

在获得距离向量 $\mathbf{d}$ 之后,模型分为两个分支:设备认证网络和信道标签预测网络。对于设备样本对,距离向量通过 $G_y(\mathbf{d}, \theta_y)$ 映射以获得设备样本对输出结果 0/1,即当前设备预测为非法/合法的认证结果。 θ_y 表示设备认证网络中的参数。设备认证网络由两个全连接层组成,输出一个一维向量经阈值判断得到认证结果,使用交叉熵损失函数,表达式为:

$$L_y(\theta_f, \theta_y) = \sum_{i=1, \dots, N_d} L_y(G_y(D(G_f(x_{i,1}^d; \theta_f), G_f(x_{i,2}^d; \theta_f)); \theta_y), y_i) \quad (16)$$

类似地,对于信道样本对, $G_c(\mathbf{d}, \theta_c)$ 将距离向量进行映射以得到信道样本对标签 c_i , 其交叉熵损失函数为:

$$L_c(\theta_f, \theta_y) = \sum_{j=1, \dots, N_c} L_c(G_c(D(G_f(x_{j,1}^c; \theta_f), G_f(x_{j,2}^c; \theta_f)); \theta_y), c_j) \quad (17)$$

在训练过程中,由于两个特征提取网络是共享权重的,因此训练过程中有两个目标:

(1) 迭代找出最优的 θ_f 和 θ_y , 使 L_y 最小化,从而实现设备标签的准确预测,减少认证错误。

(2) 确定合适的 θ_f 和 θ_c , 使 L_c 最大化,这可以混淆信道标签的预测结果,使信道识别错误最大化,便于网络模型提取跨信道的设备特征。

网络的总体损失函数定义为:

$$E(\theta_f, \theta_y, \theta_c) = \sum_{i=1, \dots, N_d} L_y^i(\theta_f, \theta_y) - \lambda \sum_{j=1, \dots, N_c} L_c^j(\theta_f, \theta_c) \quad (18)$$

3) 梯度反转层

GRL 在前向传播期间执行恒等变换 $R_\lambda(x) = x$; 在

反向传播期间,它反转梯度即 $\frac{dR_\lambda}{dx} = -\lambda \mathbf{I}$ 。通过在特征提

取网络和信道标签预测网络之间插入 GRL,将在信道标签预测网络的损失梯度反向传播到特征提取器之前将其反转。因此,特征提取网络的参数更新规则变为:

$$\theta \leftarrow \theta - \mu \left(\frac{\partial L_y}{\partial \theta} - \lambda \frac{\partial L_c}{\partial \theta} \right) \quad (19)$$

孪生对抗网络使特征提取网络能够专注于提取硬件指纹相关特征,并最小化信道的影响,从而提高跨信道域识别的准确性。

在认证阶段,将移除信道标签预测网络。样本对由特征提取器进行处理以得到距离向量,随后将这个距离向量直接输入到设备认证网络中进行认证。

3 实验结果

3.1 实验设备与采集环境

实验搭建了包含硬件平台、软件环境与通信连接的测试系统:硬件平台采用 Ettus USRP 设备(型号为 B205mini),并搭配 Ubuntu22.04 系统的计算机作为上位机,以 10 块宸

芯(型号: CX7100)C-V2X 开发板作为测试设备。

在本实验中,实验设置与数据采集方案如表 1 所示。其中 DL 状态下,开发板通过射频电缆串联 30 dB 信号衰减器后与 USRP 直接连接采集。此外,为保证同一场景下子载波信道近似不变,LOS/NLOS 数据集均为短时间内采集。

表 1 实验数据说明

Table 1 Description of experimental data

采集状态	样本数量	数据集名称	采集时间
直连	200 帧/台	DL	2024-11
静态	500 帧/台	LOS1, LOS2, NLOS1, NLOS2	2024-10
移动	500 帧/台	MOV1, MOV2	2025-01

图 7 为信号采集环境模型,其中图 7(a)为静止场景 LOS/NLOS 采集环境,图 7(b) MOV 场景为 C-V2X 终端挂车以 30~50 km/h 速度移动采集。其中 Rx 为 USRP 所放置位置,LOS、NLOS、MOV 中 Tx 为 C-V2X 开发板摆放的位置。图 8 为信号采集实际场景图。

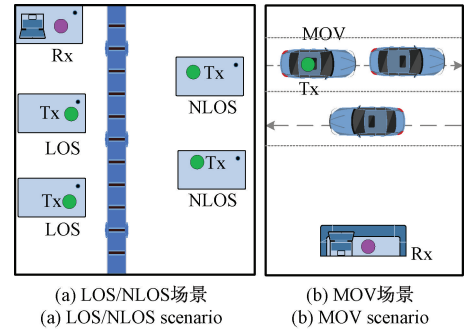


图 7 3 种信号采集场景

Fig. 7 Three signal acquisition scenarios



图 8 C-V2X 终端及实验实景

Fig. 8 C-V2X terminals and experimental real-world scenarios

3.2 实验结果和讨论

1) 评估指标与数据集设置

本实验主要选用精确率(precision, P)、召回率(recall, R)以及 F1-Score 对实验结果进行评估,其中:

$$Precision = \frac{TP}{TP + FP}$$

(20)

$$Recall = \frac{TP}{TP + FN}$$

(21)

$$F1-Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

(22)

其中, TP (true positive) 为合法类预测为合法类的个数, FN (false negative) 为非法类预测为非法类的个数, FP (false positive) 是将非法类预测为合法类的个数, TN (true

negative) 是将非法类预测为非法类的个数。 P 表征模型对合法类的预测精准度, R 刻画真实合法类的覆盖能力, 而 $F1$ 能综合反映两者的平均水平, 其值越接近 1, 模型认证性能越优越。

实验数据集按源域、跨域两类场景划分, 源域数据集用于验证模型在已知信道环境下的性能, 跨域数据集用于验证模型跨场景泛化能力。具体实验场景训练测试组合如表 2 所示。

表 2 实验场景定义

Table 2 Definitions of experimental scenarios

场景	训练集	测试集	备注
源域 LOS	DL+LOS	LOS	LOS1, LOS2 混合
跨域 LOS	DL+LOS1/LOS2	LOS2/LOS1	LOS1, LOS2 交叉测试
源域 MOV	DL+MOV	MOV	MOV1, MOV2 混合
跨域 MOV	DL+MOV1/MOV2	MOV2/MOV1	MOV1, MOV2 交叉测试

2) 预处理算法验证

此外, 为了评估多符号精准同步、逐符号频偏补偿、定时偏移补偿等预处理流程的必要性与有效性, 进行消融实验。通过逐步移除预处理核心步骤, 验证每个步骤对认证性能的贡献度, 实验设置 4 组对比方案, 如表 3 所示。

表 3 消融实验方案

Table 3 Ablation experiment schemes

组别	实验方案
G1	移除多符号精确同步
G2	移除频偏补偿
G3	移除定时偏移补偿
G4	完整预处理

验证结果如图 9 所示, $G4$ 较 $G1$ 的 $F1-Score$ 平均提升 16.79%, 在移动场景性能提升更明显达到 26%, 验证了多符号精准同步可以准确定位子帧起始点位置。 $G4$ 较 $G2$ 的 $F1-Score$ 平均提升 7.94%, 说明逐符号频偏补偿通过 CP 相位差逐符号估计频偏, 避免了频偏导致的 DMRS 子载波相位偏移, 提高了指纹提取的稳定性。 $G4$ 较 $G3$ 的 $F1-Score$ 平均提升 7.11%, 定时偏移补偿消除收发端时钟偏差导致的线性相位失真, 进一步提高了指纹的可靠性。

3) 对数谱去噪验证

实验首先验证对数谱去噪算法的有效性, 通过对比去噪前后在源域及跨域中准确率进行验证。

如图 10 所示, 从对数谱去噪前后的模型认证的 $F1-Score$ 对比来看: 使用对数谱去噪的 $F1-Score$ 在源域及跨域场景下均高于未去噪的结果, 且认证结果表明去噪后 $F1-Score$ 数值平均提升 10.05%。这表明设计的对数域数据剥离及去噪能有效抑制因随机 ZC 序列带来的 RFF 抖动。

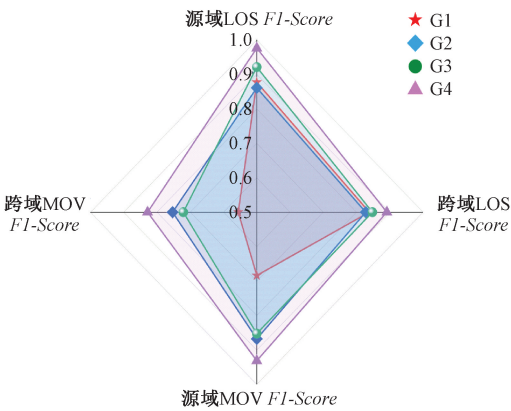


图 9 4 组方案认证准确率

Fig. 9 Authentication accuracy rates of the four schemes

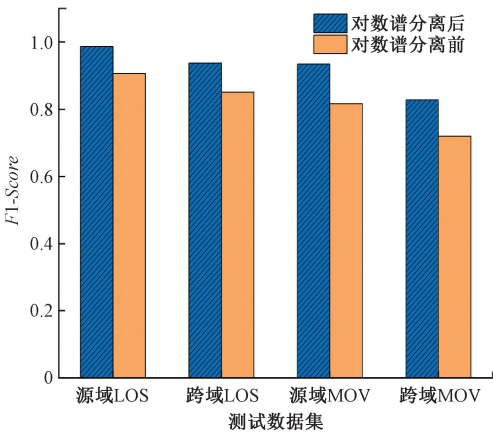


图 10 对数谱分离前后认证准确率

Fig. 10 Authentication accuracy before and after logarithmic spectrum separation

4)SANet 模型验证

为了验证基于对抗训练的多径响应与 RFF 的解耦的效果,以及融合 CBAM 模块的特征提取的性能表现。实验在源域 LOS、跨域 LOS、源域 MOV、跨域 MOV 4 个不同的测试集上测试,比较了使用完整 SANet、去除对抗模块、去除 CBAM 模块的准确性性能。

结果如图 11 所示,在源域环境下去除对抗模块测试结果相差较小,但在跨域环境下使用对抗模型 $F1-Score$ 平均提升 22.49%;说明对抗训练可显著提高了跨域环境下 RFF 识别准确性,证明了该方法可减轻多径信道影响。同时融合 CBAM 模块也能辅助 RFF 特征提取,提升复杂场景下特征提取能力。

如表 4 所示,进一步通过尝试不同场景数据进行对抗训练,并进行多场景数据来交叉测试模型的认证性能。实验结果表明:当训练集为 DL+其他场景时,认证性能总体更优。以 DL+LOS1 训练,LOS1 测试为例, P 值达 98.15%、 R 值 97.85% 高于“LOS1+LOS2”等跨场景组

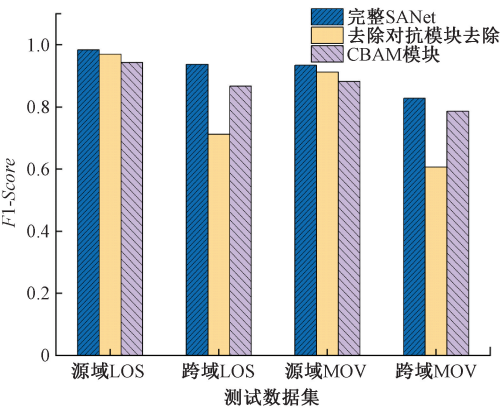


图 11 不同模块配置的认证准确率

Fig. 11 Authentication accuracy of different module configurations

合;这一规律在 LOS、NLOS、MOV 场景中也普遍成立,证实了 DL+其他信道的对抗方式在跨信道领域效果最为明显。

表 4 不同场景下认证准确率

Table 4 Authentication accuracy rates in different scenarios												%
训练集	LOS1		LOS2		NLOS1		NLOS2		MOV1		MOV2	
	P	R	P	R	P	R	P	R	P	R	P	R
DL+LOS1	98.15	97.85	92.23	91.50	90.12	89.30	93.34	92.50	81.64	80.80	79.88	79.10
DL+LOS2	94.23	93.50	99.12	98.50	90.98	90.20	91.24	90.50	82.56	81.80	80.14	79.40
DL+NLOS1	94.12	93.40	90.74	90.00	97.82	97.00	93.13	93.51	87.94	87.20	90.28	89.60
DL+NLOS2	89.96	89.20	93.21	92.50	93.21	92.50	98.98	97.76	89.36	88.60	91.97	91.30
DL+MOV1	83.69	83.00	84.54	83.80	89.31	88.60	90.23	89.50	93.56	92.90	82.34	81.74
DL+MOV2	87.69	87.00	83.24	82.50	91.68	91.00	90.97	90.30	83.36	82.70	93.32	92.94
LOS1+LOS2	94.21	93.50	93.39	92.70	84.21	83.50	83.91	83.20	79.69	79.00	80.24	79.50
LOS1+NLOS1	92.69	92.00	90.13	89.40	89.67	89.00	84.21	83.50	81.94	81.20	82.17	81.50
LOS1+MOV1	91.17	90.50	82.64	82.00	84.78	84.10	85.21	84.50	89.97	89.30	81.22	80.50
NLOS1+NLOS2	90.31	89.60	89.98	89.30	93.97	93.30	92.89	92.20	79.12	78.50	80.65	80.00
NLOS1+MOV1	78.21	77.50	79.33	78.60	90.37	89.70	87.14	86.50	89.64	89.00	82.17	81.50

进一步对“直连+其他场景”训练的模型做细分,统计得出 SANet 在源域静止(LOS+NLOS)场景平均精确率、召回率为 98.48%和 98.02%,源域移动(MOV)场景则为 93.44%和 92.92%展现对静态信道合法类的精准识别能力;跨域场景中,静止场景的认证平均精确率和召回率为 93.22%和 92.67%,移动场景为 82.85%和 82.21%,平均精确率召回率仍稳定在 82%以上,有效抑制信道时变与终端移动引发的认证性能衰减。该结果证实了模型在源域的分类精度优势,及跨域时变环境下的鲁棒性适配能力。

可见,孪生对抗训练在源域信道场景下对 LOS/NLOS 的识别精度接近 98%,即便在跨域信道或移动场景,仍能维持较高准确率,可有效缓解信道时变、终端移动带来的认证波动。

实验将 SANet 模型与文献中 3 种现有 RFF 认证方法进行对比,分别为基于 Chen 等 PSBCH-LS、Kong 等 Micro-CSI 及 DeepCRF 方案。

该实验评估了 4 种模型在静止和移动的场景下的识别准确性。实验构建源域与跨域测试集,涵盖 LOS 和 MOV 两类场景,从 P 和 R 综合评估各方法性能,实验结果如表 5 所示。结果表明,源域场景下 SANet 与 PSBCH-LS、Micro-CSI 性能趋近,显著优于 DeepCRF;跨域场景中,SANet 泛化优势凸显,LOS 场景下精确率与召回率较 DeepCRF 提升约 12%,MOV 场景下较 Micro-CSI 领先超 29%。此外,SANet 在所有场景下认证性能均高于其他 3 种方法,能有效应对车联网信道不确定性挑战。

表 5 4 种方法在不同场景下认证准确率

Table 5 Authentication accuracy of four methods in different scenarios

%

测试集方法	SANet		PSBCH-LS		Micro-CSI		DeepCRF	
	P	R	P	R	P	R	P	R
源域 LOS	98.64	98.18	98.32	97.13	98.12	96.64	81.34	80.44
跨域 LOS	93.23	92.50	86.66	85.18	87.87	86.68	77.56	77.24
源域 MOV	93.44	92.92	83.71	82.76	70.32	70.91	78.74	77.98
跨域 MOV	82.85	82.21	66.65	65.71	54.16	53.69	69.63	68.25

4 结 论

本研究提出一种基于孪生对抗训练的 C-V2X 终端 RFF 认证方法。通过设计有效的预处理方法,从 PSSCH/PSCCH 子帧中精准分离出 4 个 DMRS 符号,并融合对数谱去噪与孪生对抗训练方法,实现了 C-V2X 设备指纹的鲁棒性提取及认证识别。为验证方法性能,实验在直连模式、静态场景(含 LOS/NLOS)及移动(MOV)场景下,对 10 台 C-V2X 终端设备进行大量交叉验证。结果表明:跨域场景下,在静止信道场景,认证的平均精确率和召回率可分别达到 93.22%和 92.67%;在移动场景下,认证的平均精确率和召回率分别为 82.85%和 82.21%。所提方法有效解决了车联网终端因 PSSCH/PSCCH DMRS 序列不固定导致的特征干扰、信道场景时变导致的泛化性能下降等核心问题,为车联网终端身份认证提供可靠解决方案。

参考文献

[1] ZHOU H B, XU W CH, CHEN J CH, et al. Evolutionary V2X technologies toward the internet of vehicles: Challenges and opportunities[J]. IEEE, 2020, 108(2): 308-323,DOI:10.1109/JPROC.2019.2961937.

[2] 朱振东,姚强强,石艺恒,等. 基于改进 JPS 的智能车路径规划策略研究[J]. 仪器仪表学报, 2025, 46(6): 194-204.

 ZHU ZH D, YAO Q Q, SHI Y H, et al. Research on path planning strategy for intelligent vehicles based on improved JPS [J]. Chinese Journal of Scientific Instrument, 2025, 46(6): 194-204.

[3] 王晓昌,朱文星,孙彦赞,等. 基于图卷积网络的车联网资源管理[J]. 电子测量技术, 2021, 44(3): 114-119.

 WANG X CH, ZHU W X, SUN Y Z, et al. Study on resource management in internet of vehicles based on graph convolutional network [J]. Electronic Measurement Technology, 2021, 44(3): 114-119.

[4] XIE L N, PENG L N, ZHANG J Q, et al. Radio frequency fingerprint identification for internet of things: A survey[J]. Security and Safety, 2024, 3: 2023022.

[5] HASSIJA V, CHAMOLA V, SAXENA V, et al. A survey on IoT security: Application areas, security threats, and solution architectures[J]. IEEE Access, 2019, 7: 82721-82743.

[6] 陈静,张晓龙. 基于 MVO-SVR 的室内指纹定位算法[J]. 电子测量与仪器学报, 2024, 38(9): 45-53.

 CHEN J, ZHANG X L. Indoor fingerprint positioning algorithm based on MVO-SVR [J]. Journal of Electronic Measurement and Instrumentation, 2024, 38(9): 45-53.

[7] ZHANG J Q, LI G Y, MARSHALL A, et al. A new frontier for IoT security emerging from three decades of key generation relying on wireless channels [J]. IEEE Access, 2020, 8: 138406-138446.

[8] 张振,贾济铖,康健,等. 射频指纹识别技术方法综述[J]. 无线电通信技术, 2021, 47(3): 249-258.

 ZHANG ZH, JIA J CH, KANG J, et al. Overview of radio frequency fingerprint identification technology methods [J]. Radio Communications Technology, 2021, 47(3): 249-258.

[9] CHEN T SH, SHEN H, HU AI Q, et al. Radio frequency fingerprints extraction for LTE-V2X: A channel estimation based methodology[C]. 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall), London, United Kingdom, 2022: 1-6.

[10] QI X Y, HU AI Q, CHEN T SH. Lightweight radio frequency fingerprint identification scheme for V2X based on temporal correlation[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 1056-1070.

[11] QI X Y, HU AI Q, ZHANG ZH. Data-and-channel-independent radio frequency fingerprint extraction for LTE-V2X [J]. IEEE Transactions on Cognitive Communications and Networking, 2024, 10(3): 905-919.

[12] XING Y X, HU AI Q, ZHANG J Q, et al. Design of a channel robust radio frequency fingerprint identification scheme[J]. IEEE Internet of Things Journal, 2022, 10(8): 6946-6959.

[13] ZHANG J Q, SHEN G X, SAAD W, et al. Radio frequency fingerprint identification for device authentication in the internet of things [J]. IEEE Communications Magazine, 2023, 61(10): 110-115.

[14] PENG L N, WU ZH N, ZHANG J Q, et al. Hybrid RFF identification for LTE using wavelet coefficient graph and differential spectrum [J]. IEEE Transactions on Vehicular Technology, 2024, 73(8): 11621-11636.

[15] LI D M, YANG X, HU AI Q, et al. LTE device radio frequency fingerprints blind extraction based on temporal-frequency domain PRACH signals[J]. IEEE Transactions on Vehicular Technology, 2023, 72(10): 13229-13242.

[16] LU Q, YANG Z K, XIAN H Q. 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.

[17] KONG R Q, CHEN H. CSI-RFF: Leveraging micro-signals on CSI for RF fingerprinting of commodity WiFi[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 5301-5315.

[18] KONG R Q, CHEN H. DeepCRF: Deep learning-enhanced CSI-based RF fingerprinting for channel-resilient WiFi device identification [J]. IEEE Transactions on Information Forensics and Security, 2025, 20: 264-278.

[19] LI L Y, MUM Q. Visual tracking based on siamese neural network with non-local attention network[C]. 2022 IEEE 8th International Conference on Computer and Communications(ICC), 2022: 1905-1909.

[20] GANIN Y, USTINOVA E, AJAKAN H, et al. Domain-adversarial training of neural networks [J]. The Journal of Machine Learning Research, 2016, 17(1): 2030-2096.

[21] HE J L, XIE Y L, LIU X G. Channel-robust specific emitter identification based on domain-adversarial training of neural networks and multi-feature fusion[J]. IEEE Access, 2025, 13: 153093-153104.

作者简介

杨颢,博士,讲师,主要研究方向为无线网络安全方向,射频指纹识别技术。
E-mail: yangyang@cw Xu. edu. cn

程杨晨,硕士研究生,主要研究方向为射频指纹识别技术,车联网安全。
E-mail: cych@nuist. edu. cn

李燕(通信作者),博士,教授,主要研究方向为机器学习、智能预测与控制。
E-mail: 002200@nuist. edu. cn

胡爱群,博士,教授,主要研究方向为网络安全与通信系统安全。
E-mail: aqhu@seu. edu. cn