DOI:10.19651/j.cnki.emt.2212228

一种去信道指纹的 IEEE802.11a 信号辐射源识别方法*

曾浩南 谢跃雷
(桂林电子科技大学信息与通信学院 桂林 541004)

摘 要：针对现有射频指纹识别技术中，使用卷积神经网络提取射频指纹容易受到信道指纹干扰，而导致识别精度急剧下降的问题，提出了一种去信道指纹的 IEEE802.11a 信号辐射源识别方法。首先提取出待识别信号帧头的时域训练序列，然后利用标准 IEEE802.11a 时域训练序列作为参考信号，结合 LMS 自适应滤波器对待识别信号进行信道均衡与补偿；最后采用 IQCNet 模型从时域信号中提取射频指纹特征进行设备身份识别。实验结果表明，在不同的无线信道环境下，对 6 台基于 IEEE802.11a 协议的无线路由器的识别正确率最高达到了 96%，能有效去除信道指纹对射频指纹识别带来的不良影响。

关键词：射频指纹识别；深度学习；信道均衡；LMS 自适应滤波
中图分类号：TN911.7；TP183 **文献标识码**：A **国家标准学科分类代码**：510.4

An IEEE802.11a signal radiation source identification method with channel fingerprint removal

Zeng Haonan Xie Yuelei
(School of Information and Communication, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: Aiming at the problem that the radio frequency fingerprint(RFF) extracted by convolutional neural network (CNN) is easily interfered by the channel fingerprint, resulting in a sharp decrease in recognition accuracy. An IEEE802.11a signal radiation source identification method with channel fingerprint removal was proposed. Firstly, extract the time-domain training sequence of the frame head of the signal to be recognized, and the time-domain training sequence is used as the reference signal. Then use the LMS adaptive filter and time-domain training sequence for channel equalization and compensation. Finally, IQCNet model is used to extract the RFF from the time domain signal for device identification. The experimental results show that the recognition rate of 6 wireless routers based on IEEE802.11a protocol reaches up to 96% in different wireless channel environments. The proposed method can effectively remove the negative influence of channel fingerprint on RFF identification.

Keywords: radio frequency fingerprint identification; deep learning; channel equalization; LMS adaptive filtering

0 引 言

近年来，随着物联网、民用小型无人机、第五代移动通信技术的发展，无线设备的数量呈现爆炸式增长[1-2]，这些设备的无线信号传输大都基于 IEEE802.11 系列协议。由于电磁波的开放性，传统的基于密钥安全协议的无线网络安全存在隐患，基于物理层的射频指纹识别，具有特征难以伪造的优点，能有效正确识别信号辐射源身份，是无线网络安全领域的研究热点之一。

目前射频指纹识别方法主要使用有监督学习方法，从接收的无线信号中提取射频指纹特征并分类识别[3-4]。Wang 等[5]对基带信号进行差分处理以消除载频偏差和相位偏差对特征提取的影响，并映射为差分星座图，使用卷积神经网络提取星座图内指纹特征，对 6 部手机进行实验测试，在 25 dB 信噪比的情况下识别正确率达到 93%；徐雄[6]利用改进的 AlexNet 模型识别广播式自动相关监视信号，综合识别率达到 98.32%；曹阳等[7-8]从时域射频信号中提取二维双谱特征，并构建基于卷积神经网络的变种模型实现了辐射源识别；吴子龙等[9]直接使用基带同向正交(inphase and quardrature，IQ)信号序列训练长短时记忆网络，实现了对短波电台个体的高效识别。尽管以上研究实现了射频指纹识别技术在信号辐射源识别方面的应用，但

收稿日期：2022-11-28
* 基金项目：广西科技重大专项(桂科 AA21077008)资助

均忽视了一个重要的问题，即在射频指纹识别过程中，无线信号容易受到信道干扰而导致识别精度急速下降[10]。Restuccia 等[11]利用同一天采集到的信号训练和测试卷积神经网络，识别准确率接近 100%，然而测试集换成另一天采集的信号时，识别准确度下降到 5%，这是因为卷积神经网络在学习信号样本的特征时，没有考虑到无线信道的时变特性对识别效果的影响，神经网络学习到的不仅是设备的射频指纹特征，还包括时变的信道指纹特征。

针对现有射频指纹识别技术在不同信道环境下识别率低的问题，提出了一种去信道指纹的 IEEE802.11a 信号辐射源识别方法，该方法使用时域训练序列结合最小均方(least mean square algorithm，LMS)自适应滤波器，对传输信号进行信道均衡与补偿，降低时变信道对射频指纹识别带来的不利影响，并使用 IQ 相关特征卷积神经网络(convolutional neural network structure based on IQ correlation features，IQCNet)从时域信号中提取射频指纹，极大的提高了不同信道环境下的识别率。

1　信号模型

射频指纹识别技术的核心思想是利用无线电磁信号中的独特特征来识别发射机。假设通信系统是理想的，IEEE802.11a 使用标准正交频分复用技术(orthogonal frequency division multiplexing，OFDM)技术，对于 OFDM 信号模型，其时域信号序列如下：

$$\boldsymbol{x}(n)=\frac{1}{N}\sum_{k=0}^{N-1}X(k)\exp\left(j\frac{2\pi nk}{N}\right) \tag{1}$$

其中，$X(k)$ 为 OFDM 中第 k 个子载波上的频域数据，N 表示 OFDM 信号中一共有 N 个子载波。

然而，在射频设备的射频电路中，器件存在非理想性的制造误差，电路的走线不同，会使不同射频设备的电路参数存在细微差异，这种细微差异会以无意调制的形式附加在发送信号上，导致射频设备实际发射的基带信号模型为：

$$\boldsymbol{s}(n)=[1+\Delta\boldsymbol{a}(n)]\boldsymbol{x}(n)\exp[j(2\pi\Delta f)n+\Delta\boldsymbol{\varphi}(n)] \tag{2}$$

$\Delta\boldsymbol{a}(n)$ 表示信号包络的无意调制函数，$\Delta\boldsymbol{\varphi}(n)$ 表示信号相位误差，Δf 表示信号的频率偏移。对于射频设备而言，发送的实际信号与理想调制信号之间总会存在偏差，导致 $\Delta\boldsymbol{a}(n)$、$\Delta\boldsymbol{\varphi}(n)$ 和 Δf 总是存在，这三者可以反应射频设备的个体差异[12]。

并且，无线信道也会对发射信号产生影响，导致在接收信号中出现信道信息：

$$\boldsymbol{r}(n)=\boldsymbol{h}(n)*\boldsymbol{s}(n)+\boldsymbol{n}_0(n) \tag{3}$$

式中：$*$ 表示卷积运算，$\boldsymbol{r}(n)$ 是接收机采集信号，$\boldsymbol{h}(n)$ 是信道冲击响应，$\boldsymbol{h}(n)$ 具有随时间变化的特性，$\boldsymbol{n}_0(n)$ 为加性噪声，$\boldsymbol{h}(n)$ 与 $\boldsymbol{n}_0(n)$ 共同构成了信道指纹特征。

由于无线信道的时变性，射频信号在经过实际信道传输后，其射频指纹的唯一性、稳健性和短时不变性遭到破坏，为后续设备认证带来了极大的困难。

2　基于 IQCNet 的射频指纹识别方法

本文采用 IQCNet 模型从 IEEE802.11a 设备的时域信号提取射频指纹，总体识别算法流程如图 1 所示，信号采集装置采集待识别设备的射频信号，经过前端处理为基带 IQ 信号，然后使用 LMS 自适应滤波器将基带信号进行信道均衡处理；最后将处理好的信号制作成数据集，标注出设备身份识别号，训练 IQCNet 模型，输出检测结果。

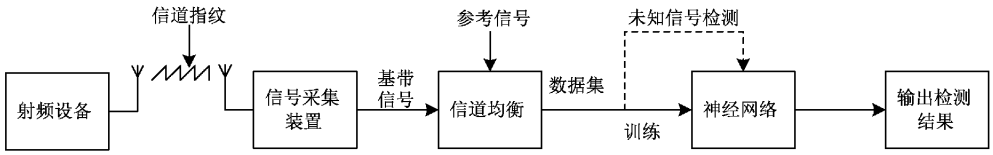

图 1　总体识别流程

2.1　基于时域训练序列的自适应信道均衡算法

射频指纹识别技术是利用射频信号中独一无二的特征来识别不同的设备，由于无线信道的影响，信号采集装置采集到的射频信号中包含了信道指纹信息[13]，信道均衡是一种消除信道指纹的有效技术。

为了对采集信号做信道均衡，首先分析 IEEE802.11a 信号的时域帧结构[14]，如图 2 所示 t1～t10 是 10 个周期的短训练序列，主要用来做帧同步计算、频偏粗估计；T1 和 T2 是两个长训练序列，主要用来进行信道估计和频偏细估计；接下来是 SIGNAL 字段和 DATA 字段，从 SIGNAL 字段开始后，每个符号中都包含 4 个导频，导频可以用来定时跟踪、频偏跟踪以及信道估计。

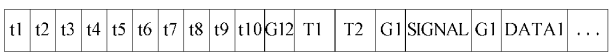

图 2　IEEE802.11a 时域信号帧结构

从上述帧结构分析中可以看出，基于 IEEE802.11a 协议的 OFDM 系统信道估计既可以用时域训练序列估计也可以用导频估计。由于 IEEE802.11a 无线局域网主要应用在室内，在发送数据帧不长的情况下可以假设一帧内信道保持不变。因此，本文用 IEEE802.11a 信号中的时域训练序列，即帧头长训练字段 T1 和 T2 完成信道估计。

本文使用 LMS 自适应滤波器对采集信号做信道均衡处理，使用 LMS 自适应滤波器做信道均衡中，有以下式成立：

$$\hat{\boldsymbol{s}}(n)=\boldsymbol{W}(n)*\boldsymbol{r}(n)=\boldsymbol{W}(n)*\boldsymbol{h}(n)*\boldsymbol{s}(n) \tag{4}$$

$\boldsymbol{s}(n)$ 为发射信号序列，$\boldsymbol{h}(n)$ 为传输信道的离散时间

冲激响应,$\boldsymbol{r}(n)$ 为经过信道传输后的接收序列,$\boldsymbol{W}(n)$ 为 LMS 自适应滤波器的冲击响应,$\hat{\boldsymbol{s}}(n)$ 为滤波器输出信号即经过均衡恢复后的信号。

由式(4)可知,$\boldsymbol{r}(n)$ 是由 $\boldsymbol{s}(n)$ 与 $\boldsymbol{h}(n)$ 卷积而得到,由于 $\boldsymbol{W}(n)$ 是对 $\boldsymbol{h}(n)$ 的逆系统的逼近,故 $\boldsymbol{r}(n)$ 经过 $\boldsymbol{W}(n)$ 滤波后,可从 $\boldsymbol{r}(n)$ 中恢复出 $\boldsymbol{s}(n)$ 的近似信号 $\hat{\boldsymbol{s}}(n)$。

LMS 自适应滤波器的迭代流程如下:

1)初始化滤波器系数:

$$\boldsymbol{W}(n)=0 \tag{5}$$

2)更新抽头权值:

$$y(n)=\boldsymbol{W}^{\mathrm{T}}(n)\boldsymbol{X}_0(n) \tag{6}$$

$$e(n)=d(n)-y(n)=d(n)-\boldsymbol{W}^{\mathrm{T}}(n)\boldsymbol{X}_0(n) \tag{7}$$

$$\boldsymbol{W}(n+1)=\boldsymbol{W}(n)+2\mu e(n)\boldsymbol{X}_0(n) \tag{8}$$

3)重复步骤 2)直到达到迭代次数。

其中,$\boldsymbol{W}(n)=[w_0(n),w_1(n),\cdots,w_{N-1}(n)]^{\mathrm{T}}$,$\boldsymbol{W}(n)$ 是自适应滤波器的抽头权值向量,N 代表滤波器的阶数;$\boldsymbol{X}_0(n)$ 是滤波器训练输入信号;$\boldsymbol{d}(n)$ 是参考信号;$e(n)$ 是误差信号,μ 为迭代步长。在 LMS 自适应滤波器训练过程中,将待识别的 IEEE802.11a 信号中的长训练字段作为输入信号 $\boldsymbol{X}_0(n)$,采用标准 IEEE802.11a 长训练字段作为参考信号 $\boldsymbol{d}(n)$,完成 LMS 自适应滤波器的迭代。

2.2　基于 IQCNet 的射频指纹识别方法

卷积神经网络是一种普遍使用在图像处理领域的有监督学习方法,近年来也被逐渐运用于数字信号处理领域。卷积神经网络具有较高的泛化能力,能够有效从电磁信号的时域或变换域中提取射频指纹特征[15]。

在射频指纹识别领域,常用的卷积神经网络对 IQ 信号的处理都是将其简单视为图像进行的,原始 IQ 采集数据格式为 $N\times2$,其中 N 对应信号的时间长度,2 对应 IQ 两路正交分量,两个维度不具备相同性质,无法进行图像处理一样的二维对称处理,所以目前卷积神经网络对 IQ 信号的处理都是采用一维卷积核提取时间维度特征,然而,这种一维卷积操作忽略了 IQ 两路信号间的相关特征,降低了识别率。

针对以上问题,崔天舒等[16]提出了一种 IQCNet 模型。IQCNet 模型通过 1×2 卷积核提取了 IQ 相关特征及时域特征,后续层再使用一维卷积核提取射频指纹特征,在提取 IQ 信号的射频指纹信息中,保留了 IQ 两路信号间的相关特征,并通过自适应平均池化获得了各通道特征均值,用单个全连接层进行分类。较传统卷积网络结构,IQCNet 在多种场景下的识别准确率更高,并且计算量更小,IQCNet 模型结构如图 3 所示。

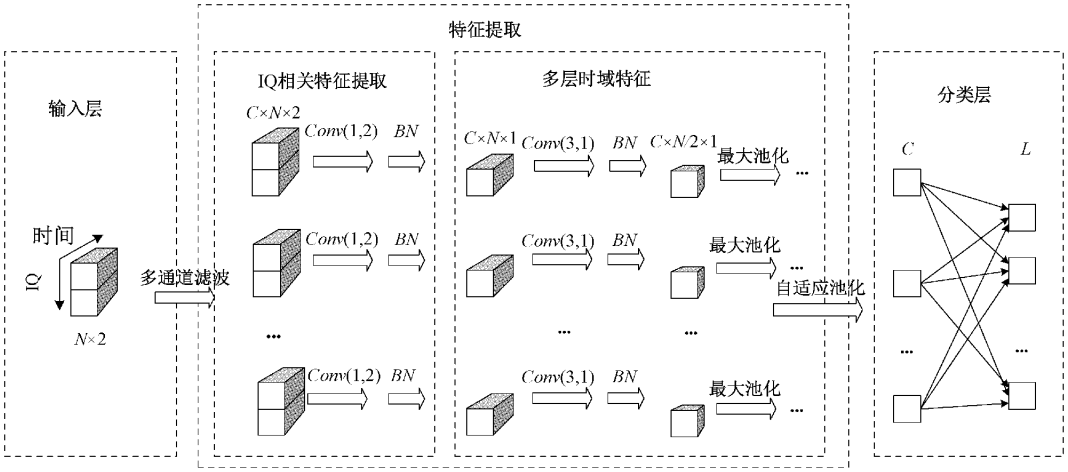

图 3　IQCNet 模型结构

本文采用的 IQCNet 模型由输入层,特征提取层和分类层组成。特征提取层中包含两个部分:首先是 IQ 相关特征提取,采用 1×2 卷积核提取 IQ 相关特征;然后借鉴 AlexNet 模型,采用 5 层 3×1 小卷积核提取时域特征。在保证感受野的条件下提取不同的维度上的特征,能充分利用 IQ 信号的 IQ 相关特征和时域特征,相较于传统的神经网络模型,对 IQ 信号的信息利用率更高。由于第一个卷积层采用了 1×2 卷积核提取 IQ 相关特征,输出数据维度由 $N\times2$ 变为了 $N\times1$,后续处理的计算量降低了一半,接着每 2 个卷积层后采用一个最大池化降低数据维度,减小了模型计算量。

在分类层中借鉴了残差神经网络(residual neural network,ResNet)模型,采用自适应池化层代替代压平层,并采用一个全连接层进行分类。自适应池化操作将每个特征通道的特征平均值作为新的特征值,能提高网络的泛化性能,且进一步减小模型的参数量和计算量。

3　实验与分析

为了验证本文算法的性能,搭建了实验平台。实验的信号样本来自 6 台华为 ws5106 无线路由器。路由器的工作模式统一设置为发送 IEEE802.11a 协议的 WiFi 信号,使用 40 号信道,中心频率为 5.2 GHz,信道带宽为 20 MHz。

信号采集装置使用 NI 公司的软件无线电设备，型号为 USRP2954。在实验室实际电磁环境下分别采集每台路由器的发射信号，将 USRP2954 载频设置为 5.2 GHz，采样频率设置为 20 MHz，经过采集后得到基带 IQ 信号序列。

实验的神经网络模型运行在一台显卡为 Nvidia RTX3070、内存 32 GB 的 Windows10 系统的电脑上，实验平台使用基于 Python 语言的开源深度学习框架 Tensorflow。

3.1　实验流程

1)信号采集：

信号采集在一个封闭房间中进行，如图 4 所示，采集位置表示信号采集装置的位置，辐射位置 1、辐射位置 2、辐射位置 3 表示无线路由器的 3 个不同固定位置。其中，采集位置与辐射位置的间隔距离为 4～6 m，辐射位置之间的间隔距离为 1 m 左右。信号采集装置与无线路由器之间有实验器材、桌椅等杂物对射频信号造成反射和阻隔等影响，但信号收发路径中存在没有被完全阻隔的信号直射分量，加之封闭房间中墙壁对信号的反射，导致传输信道是一个莱斯衰落信道。

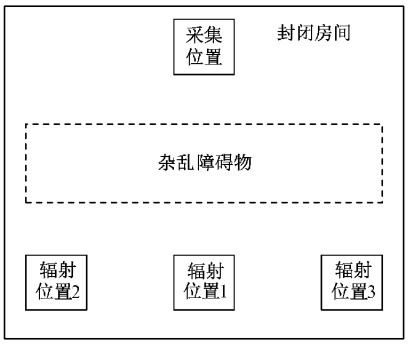

图 4　实验环境

信号采集装置固定在采集位置不变，将 6 个无线路由器分别固定在辐射位置 1 位置时的信道命名为信道一，相同的，固定在辐射位置 2 和辐射位置 3 位置时的信道分别命名为信道二和信道三。

2)信道均衡处理：

提取出每个采集信号的长训练序列，然后结合 IEEE802.11a 标准长训练序列训练 LMS 自适应滤波器。LMS 滤波器训练中，设置滤波器阶数为 64，迭代步长为 0.001，迭代次数为 100。采集信号通过 LMS 自适应滤波器做自适应信道均衡，均衡前后信号对比如图 5、6 所示。从信号频谱图中可以观察到，经过信道均衡的 OFDM 信号的子信道间隔相对于原始接收信号更清晰。

3)训练并测试神经网络：

提取每个信号帧头序列的前 256 个点，再把每个信号段做能量归一化，由于采集信号分为 IQ 两通道，所以将 IQ 两通道信号按上述步骤处理后拼接成 256×2 大小的二维

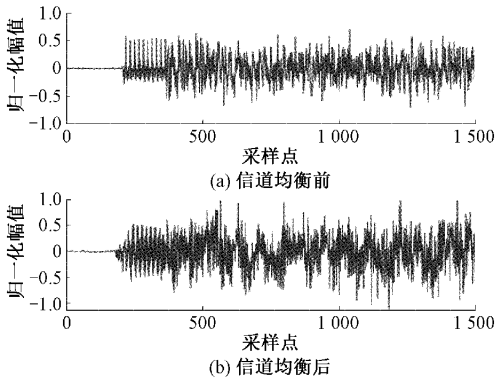

图 5　信道均衡前后信号时域图

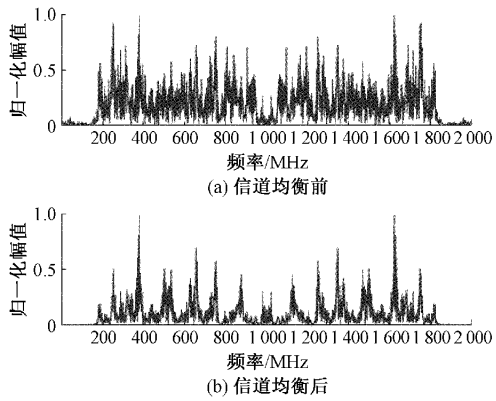

图 6　信道均衡前后信号频谱图

信号段。将信号段按照对应的无线路由器分类打包制成数据集，其中，训练集一共 4 800 个信号段，每个路由器对应 800 个信号段；测试集一共 1 200 个信号段，每个路由器对应 200 个信号段。

本文采用 IQCNet 模型提取信号的射频指纹并分类识别，在神经网络训练过程中，设置批处理大小为 64，损失函数为交叉熵损失函数，学习率为 0.001，训练迭代次数为 60 次。

3.2　实验结果与分析

首先对未做信道均衡的原始信号进行测试，将信道一、信道二、信道三环境下采集的信号分别制作成训练集，并分别训练 IQCNet 模型，再用同样信道环境下采集的信号作为 IQCNet 模型的测试集，分类准确率如图 7 所示。

从实验结果中可知，对于在相同信道环境下采集的信号，分类正确率达到 99%以上，能准确识别信号辐射源。

为了验证不同信道对射频指纹识别结果的影响，将信道一信道环境下采集的信号作为 IQCNet 模型的训练集，将其它两种信道环境下采集的信号作为 IQCNet 模型的测试集，模型识别正确率如图 8 所示。

可以观察到，使用不同信道下采集的信号来分别训练和测试 IQCNet 模型，模型的识别性能大幅下降，这是因为神经网络不仅提取了信号中的射频指纹，还提取了信道指

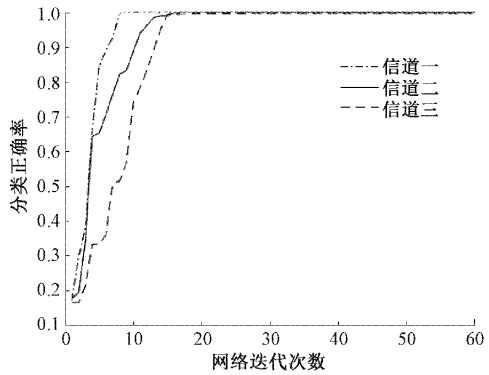

图 7　同一信道识别精度

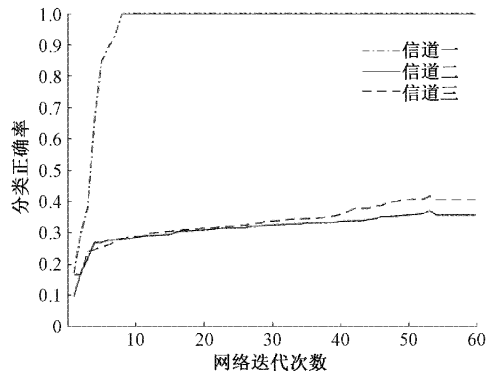

图 8　不同信道识别精度

纹,不同信道下采集的某一无线路由器信号的射频指纹信息相同,但信道指纹信息不相同,导致了识别率降低到 40%以下。

为了验证本文的方法能有效降低信道环境对射频指纹识别的影响,将信道一采集的信号使用本文方法做信道均衡处理,处理后的信号训练 IQCNet 模型;将其它两种信道环境下采集的信号也进行信道均衡处理,并作为模型的测试集,实验结果如图 9、10 所示。

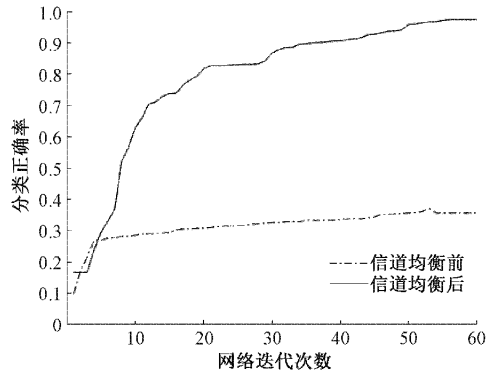

图 9　信道二采集信号识别正确率对比

由实验结果图可知,不同信道环境下采集的信号经过本文算法处理后,相比于没有经过处理的信号识别率有了大幅提升,信道二采集信号识别正确率达到 96%以上,信道三采集信号识别正确率达到 86%以上,证明了本文方法可以有效消除射频信号中的信道指纹信息,在不同的信道环境下,可以准确识别出 IEEE802.11a 信号辐射源的身份信息。

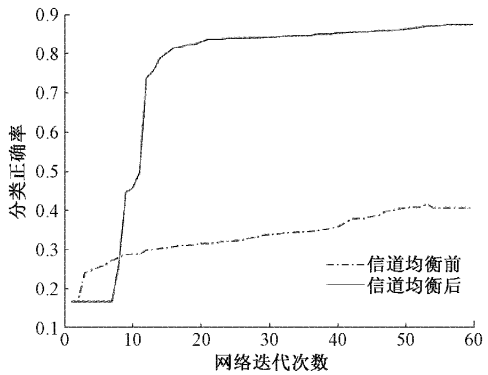

图 10　信道三采集信号识别正确率对比

3.3　不同方法对比

为了进一步体现本文方法的优越性,将本文方法与文献[6]和[8]方法进行对比。使用经本文算法处理后,信道一采集信号作为神经网络的训练集,信道二采集信号作为神经网络的测试集,实验结果对比如表 1 所示。

表 1　不同方法对比

识别方法	分类结果/%	模型参数量
ResNet+信号双谱[8]	85.5	11 195 014
AlexNet+IQ 序列[6]	80.1	1 716 774
IQCNet+帧头 IQ 序列	96.7	482 694

由实验结果可知,相较于其他两种算法,本文使用 IQCNet 模型加 IQ 时域信号序列的方法识别率更高,且神经网络模型的参数量更小;文献[6]使用的 AlexNet 模型不能有效地从时域信号中提取 IQ 相关信息从而影响了其识别能力;文献[8]中,为了减小模型训练难度将信号双谱图压缩而损失了部分射频指纹信息,导致了识别率偏低;本文使用的模型能有效地从时域信号提取射频指纹信息,且抛弃了参数较多的全连接层,减小了模型参数量,更适合应用于射频指纹识别领域。

4　结　　论

提出了一种去信道指纹的 IEEE802.11a 信号辐射源识别方法,首先提取出待识别信号帧头的时域训练序列,然后利用标准 IEEE802.11a 时域训练序列作为参考信号,结合 LMS 自适应滤波器进行信道指纹消除,最后采用 IQCNet 模型提取经过信道均衡的时域信号的射频指纹并分类识别。该方法将基于卷积神经网络的射频指纹识别方法与自适应信道均衡技术相结合,解决了现有的射频指纹识别方法容易受信道指纹干扰的问题。实验过程中,对

6 个 IEEE802.11a 无线路由器进行分类测试，分别使用不同信道环境下采集的信号训练和测试神经网络，对设备的识别正确率最高能达到 96%以上。

参考文献

[1] 顾林轩. 5G 无线通信技术及对物联网产业链发展的价值分析[J]. 网络安全技术与应用，2022(7)：64-65.

[2] 王睿. 大数据时代物联网技术的应用与发展[J]. 网络安全技术与应用，2021(4)：67-68.

[3] 李昆，朱卫纲. 基于机器学习的雷达辐射源识别综述[J]. 电子测量技术，2019，42(18)：69-75.

[4] 汤春阳. 基于深度学习的射频指纹识别研究[D]. 兰州：兰州交通大学，2022.

[5] WANG S，PENG L. A convolutional neural network-based RF fingerprinting identification scheme for mobile phones [C]. Proceedings of 2020 IEEE INFOCOM，2020：115-120.

[6] 徐雄. 采用改进型 AlexNet 的辐射源目标个体识别方法[J]. 电讯技术，2018，58(6)：625-630.

[7] 曹阳，徐程骥，狄恩彪，等. 基于局部双谱和深度卷积神经网络的通信电台识别研究[J]. 通信技术，2020，53(7)：1652-1657.

[8] 谢跃雷，邓涵方. 基于改进 ResNet 的射频指纹识别方法[J]. 电讯技术，2022，62(4)：416-423.

[9] 吴子龙，陈红，雷迎科，等. 基于堆栈式 LSTM 网络的通信辐射源个体识别[J]. 系统工程与电子技术，2020，42(12)：2915-2923.

[10] RESTUCCIA F，D′ ORO S，et al. DeepRadioID：Real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms [C]. Proceedings of the Twentieth ACM International Symposium on Mobile Ad Hoc Networking and Computing(Mobihoc′19)，2019：51-60.

[11] Al-SHAWABKA A，RESTUCCIA F. Exposing the fingerprint：Dissecting the impact of the wireless channel on radio fingerprinting [C]. Proc of IEEE INFOCOM 2020—IEEE Conference on Computer Communications，2020：646-655.

[12] 俞佳宝，胡爱群，朱长明，等. 无线通信设备的射频指纹提取与识别方法[J]. 密码学报，2016，3(5)：433-446.

[13] 朱丰超，曾盛，周雅彬. 基于信道均衡的无线信道指纹滤除方法[J]. 华中科技大学学报(自然科学版)，2022，50(3)：29-35.

[14] 韩翔，周钦山，王峰. IEEE802.11a 信号解调算法研究[J]. 国外电子测量技术，2021，40(3)：103-107.

[15] 张晔. 基于深度学习的射频指纹识别系统设计与实现[D]. 北京：中国科学院大学(中国科学院国家空间科学中心)，2021.

[16] 崔天舒，黄永辉，沈明，等. 面向射频指纹识别的高效 IQ 卷积网络结构[J]. 国防科技大学学报，2022，44(4)：180-189.

作者简介

曾浩南，硕士研究生，主要研究方向为射频指纹识别。

谢跃雷，副教授，主要研究方向为通信信号处理、信号处理的 ASIC 设计实现、FPGA 数字系统设计等。

E-mail：ylxie_guet@126.com