研究与开发

基于轻量级 CNN 和信道特征辅助的多用户物理层认证机制

王延坤，郭登科，马东堂，熊俊，张晓瀛
（国防科技大学电子科学学院，湖南 长沙 410073）

摘　要：针对目前物理层的用户认证算法存在的鲁棒性差、复杂度高等问题，提出了一种轻量级卷积神经网络（CNN）信道特征提取算法，通过改变网络输入形式减少训练所需要的信道状态响应，同时基于该算法建立了一种多用户物理层信道特征辅助的认证机制，设计了从用户注册到认证的详细过程，并在线完成多用户认证及网络参数更新。仿真结果表明，所提算法能够完成多用户身份认证，在较小的训练轮次下获得良好的检测性能，且比现有的多用户认证算法需要的训练样本少。

关键词：物理层安全；多用户认证；轻量级；CIR；鲁棒性
中图分类号：TN92
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2023240

Multi-user physical layer authentication mechanism based on lightweight CNN and channel feature assistance

WANG Yankun, GUO Dengke, MA Dongtang, XIONG Jun, ZHANG Xiaoying
College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China

Abstract: To address the problems of poor robustness and high complexity of current physical layer user authentication algorithms, a lightweight convolutional neural network (CNN) channel feature extraction algorithm was proposed to reduce the channel state response required for training by changing the form of network input, and a multi-user physical layer channel feature-assisted authentication mechanism was established based on this algorithm to design a detailed process from user registration to authentication, and multi-user authentication and network parameter update online were completed. Simulation results show that the proposed algorithm can complete multi-user authentication, obtain good detection performance with smaller training rounds, and require fewer training samples than existing multi-user authentication algorithms.

Key words: physical layer security, multi-user authentication, lightweight, CIR, robustness

0　引言

5G 因其时延更低、网络带宽更大，在人类生活和工作中得以广泛普及和应用[1]。然而由于无线信道的开放特性，无线通信安全问题日益突出[2]，在低时延无线通信中，无线信道中密集

收稿日期：2023−07−26；**修回日期：**2023−11−10
基金项目：国家自然科学基金资助项目（No.61372099，No.61931020）
Foundation Items: The National Natural Science Foundation of China (No.61372099, No.61931020)

传输的数据让企图监听或窃取私人信息的恶意用户有了可乘之机，因此，迫切需要解决无线通信安全问题。

无线通信安全可以分为物理层安全和上层安全，上层安全主要依靠密码算法对传输数据进行加密，而物理层安全可以利用独特的物理层资源对上层安全传输协议进行增强[3]。认证作为无线网络中的第一道防线，能够有效区分接入设备的合法性，从而防止潜在的入侵者（Eve）访问网络。例如，在蜂窝小区中，恶意设备可以冒充合法设备通过上行链路对基站进行访问，因此基站必须具备识别恶意设备的能力，并且只授予合法用户安全接入权限。虽然基于上层的认证机制已经得到了广泛应用，但是这些方式仅在攻击者的计算能力有限的前提下是安全的[4]，忽略了物理层认证所能发挥的重要作用。

物理层的传输信号和信道特征信息可以用来辅助设计安全认证机制[5]，这在物理层认证中被称作射频指纹认证和信道指纹认证。发射机的射频滤波器、功率放大器中的电子元件容差所造成的发射信号独特的信号特征被称作射频指纹（radio frequency fingerprint，RFF）[6]。射频指纹通过提取发射设备固有特征对用户进行唯一标定，但都需要预先采集良好信道条件下的发射信号进行训练，在实际通信场景中并不容易部署实施。同时，更为严重的是无线信道带来的噪声、衰落特性对射频指纹的影响可能会造成识别准确度下降[7]。而无线信道具有短时互易性、空间唯一性、随机性等特征[8]，造成不同用户间信道的显著差异，可以用来对用户身份进行认证。但是如何有效提取信道特征来提高识别准确率，实现轻量级物理层认证仍是一个亟待解决的问题。

目前，国内外基于信道特征实现的物理层认证算法可以分为基于统计或瞬时信道特征的物理层认证算法和基于机器学习的信道特征物理层认证算法。在基于统计或瞬时信道特征的物理层认证算法中，文献[9]利用无线信道的接收信号强度（received signal strength，RSS）结合模糊提取器生成安全位置指纹，根据信道的短时互易性对用户的身份进行认证，实验结果表明，即使是两个相距很近的用户，RSS 在一定时间内也有着显著差异。文献[10-11]同样通过实验证明了 RSS 与用户位置唯一绑定。还有学者利用更加细粒度的信道特征完成物理层认证，文献[5]研究了一种利用信道时变特性增强物理层身份认证的技术，通过信道频率响应（channel frequency response，CFR）测量值结合假设检验来区分合法用户和 Eve；文献[12]基于信道冲激响应（channel impulse response，CIR）提出了一种物理层认证方案，通过对比两个连续 CIR 的变化认证发射设备的合法性；文献[13]通过时域信道状态信息（channel state information，CSI）完成合法设备检测，仿真结果表明了该算法在 0～20 dB 内具有较好的性能，能够有效检测合法设备。

在基于机器学习的信道特征物理层认证算法中，文献[14]利用深度卷积神经网络（deep convolutional neural network，DCNN）对无线信道进行特征提取，网络的输入为信道时频图，实验结果表明对无线信道的识别准确率可以达到 96.46%。还有学者利用其他信道特征作为神经网络的输入，文献[15-16]利用 CSI 增强 MIMO-OFDM 系统的物理层身份验证，首先每个接收机收集 200 个信道样本，然后将 CSI 进行降维处理后对神经网络进行训练，最终达到区分合法用户和 Eve 的目的；文献[10]设计了一种自适应神经网络（adaptive neural network，ANN），收集单个用户场景下的 4 000 个 RSS 样本进行训练，实验结果表明该方法在不同信噪比下能够完成对非法设备的检测。

综上所述，基于统计或瞬时信道特征的物理

层认证算法有效证明了不同无线信道之间存在差异性，通过提取或对比信道特征可以区分不同的发射设备，完成对合法设备的认证过程，但是对无线信道所携带的差异性信息利用不够充分，同时基于先验知识设计并提取特征依赖于特定的信道环境，存在鲁棒性较差的问题；基于机器学习的信道特征物理层认证算法实现了更好的性能，但在实际通信系统中，获取大量信道响应样本并对网络进行训练十分困难，即使在慢时变信道下，对于训练网络也需要及时更新以适应新的信道状态，因此对网络训练时间和训练所需要的信道响应样本数提出了很高的要求。针对上述问题，本文设计了一种轻量级卷积神经网络，通过改变网络输入特征的方式解决信道响应样本较少的问题，加快网络训练速度。

本文的主要创新点如下。

- 提出了一种基于轻量级卷积神经网络的无线信道提取识别算法，通过改变网络输入形式降低对信道样本数目的需求。
- 提出了多用户场景下基于上述算法的物理层认证机制，因为无线信道具有空间唯一性，因此用户只需要直接访问基站即可获得接入权限，进一步提高了认证效率。

1　系统模型

1.1　通信网络模型

蜂窝网技术贯穿 4G、5G 时代，是移动通信网络的基础[17]，而单个小区（cell）内基站与用户的无线通信过程具有代表性，因此本文聚焦蜂窝网中单个小区内的无线通信安全认证问题。考虑单个小区中一个基站为多个用户提供服务，而由于无线信道具有开放性，潜在的 Eve 可以冒充合法用户访问基站。而与基站相连接的服务器存储大量隐私信息，因此基站必须具备对合法用户的认证能力，蜂窝小区中多个散射路径的多用户环境如图 1 所示。

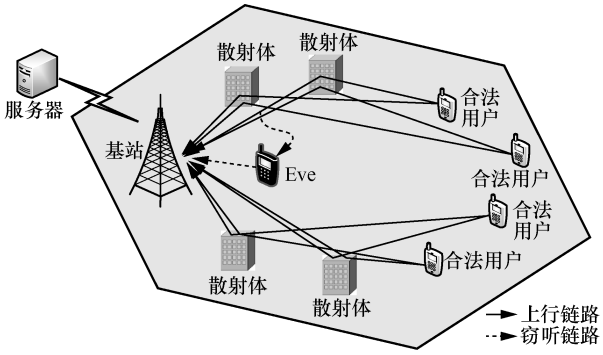


图 1　蜂窝小区中多个散射路径的多用户环境

1.2　基本假设

为方便说明，首先考虑基站对单个用户的认证过程。在建立基站和单个用户的通信链路之前，用户首先通过上行链路对基站进行访问，得到基站的授权后才能够建立合法的通信链路。在本文的模型中，假定初始认证在安全环境中完成，认为基站获得并存储了两者间的 CIR。当用户再次对基站进行访问时，基站只需要根据当前两者间的信道状态信息便能够判断用户是否合法。而在这个过程中，Eve 所具备的能力将直接影响整个网络的安全性，因此对 Eve 的能力做如下定义。

- 具备合法用户的所有硬件和软件条件，包括所有认证方案和通信协议。
- 具备监听和窃取上行链路通信过程的能力，能够无误差地窃取到完整的通信信息。
- 具备假冒和欺骗基站的能力，能够完全模仿合法用户并尝试欺骗基站为其提供服务。

在 Eve 存在的条件下，认证协议必须具备区分不同用户的能力，同时能够识别 Eve 的假冒或欺骗攻击。

1.3　信道模型

设计或提取 CSI 中的特征与信道建模过程息息相关，本文研究典型室外多径场景下的通信信道。假设有 N 个用户，则第 n 个用户的 CIR 可以表示为：

$$h_n(t,\tau)=\sum_{l=1}^{L(t)}h_{l,n}(t)\delta\left(\tau-\tau_l(t)\right) \tag{1}$$

其中，$L(t)$为时刻 t 的抽头（tap）总数；$h_{l,n}(t)$为时变 tap 增益，通常为复数；$\tau_l(t)$为时刻 t 的第 l 个抽头所对应时延；$\delta(\cdot)$为冲激函数，因此 $h_n(t,\tau)$包含了第 n 个用户的完整时变信道信息，时变信道冲激响应如图 2 所示。如果认证过程的持续时间比信道变化时间（相干时间）短，则认为认证过程设计合理。

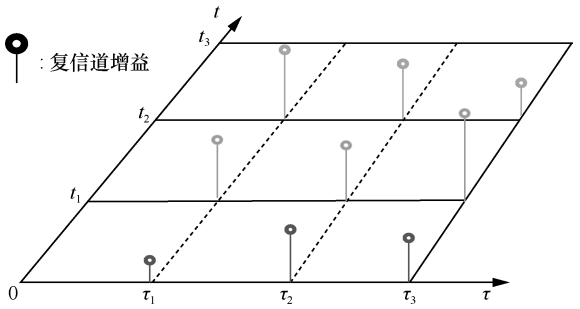


图 2　时变信道冲激响应

同时，认为发射信号经过散射体反射 3 次及以上到达接收端的信号可以忽略不计，即仅考虑单跳和双跳的情况，因此$h_{l,n}(t)$可以进一步表示为：

$$h_{l,n}(t)=h_{l,n}^{\mathrm{Los}}(t)+h_{l,n}^{\mathrm{SB}}(t)+h_{l,n}^{\mathrm{DB}}(t) \tag{2}$$

其中，$h_{l,n}^{\mathrm{Los}}(t)$为直射路径的增益，$h_{l,n}^{\mathrm{SB}}(t)$为单跳路径的增益，$h_{l,n}^{\mathrm{DB}}(t)$为双跳路径的增益。

$$h_{l,n}^{\mathrm{SB}}(t)=\frac{1}{\sqrt{M}}\sum_{m=1}^{M}\mathrm{e}^{\mathrm{j}\left(2\pi f_{\mathrm{D}}t-\frac{2\pi D_{\mathrm{SB}}}{\lambda}+\phi_m\right)} \tag{3}$$

$$h_{l,n}^{\mathrm{DB}}(t)=\frac{1}{\sqrt{MK}}\sum_{m=1}^{M}\sum_{k=1}^{K}\mathrm{e}^{\mathrm{j}\left(2\pi f_{\mathrm{D}}t-\frac{2\pi D_{\mathrm{DB}}}{\lambda}+\phi_{mn}\right)} \tag{4}$$

其中，M 和 K 表示散射体个数，f_{D} 表示载波频率，D_{SB} 和 D_{DB} 分别表示单跳和双跳距离，ϕ_m 和 ϕ_{mn} 表示反射引入的随机相移。

信道冲激响应关于变量 τ 的傅里叶变换可以得到时变传输函数，即 CFR，表示为：

$$H_n(t,f)=\mathcal{F}\{h_n(t,\tau)\}=\int_{-\infty}^{+\infty}h_n(t,\tau)\mathrm{e}^{-\mathrm{j}2\pi f\tau}\mathrm{d}\tau \tag{5}$$

对于慢时变信道而言，可以认为系统是准静态的，那么信号 $x(t)$通过信道后的输出可以表示为：

$$y(t)=\int_{-\infty}^{+\infty}X(f)H_n(t,f)\mathrm{e}^{\mathrm{j}2\pi ft}\mathrm{d}f \tag{6}$$

当发射信号 $X(f)$是固定的导频信号时，接收信号就可以直接反映信道响应，输出可以近似为 $h_{l,n}(t)$，即获得了当前时刻用户和基站的 CSI。

2　多用户物理层认证机制描述

基于轻量级卷积神经网络的多用户认证流程如图 3 所示。当单个小区中的基站为多个用户服

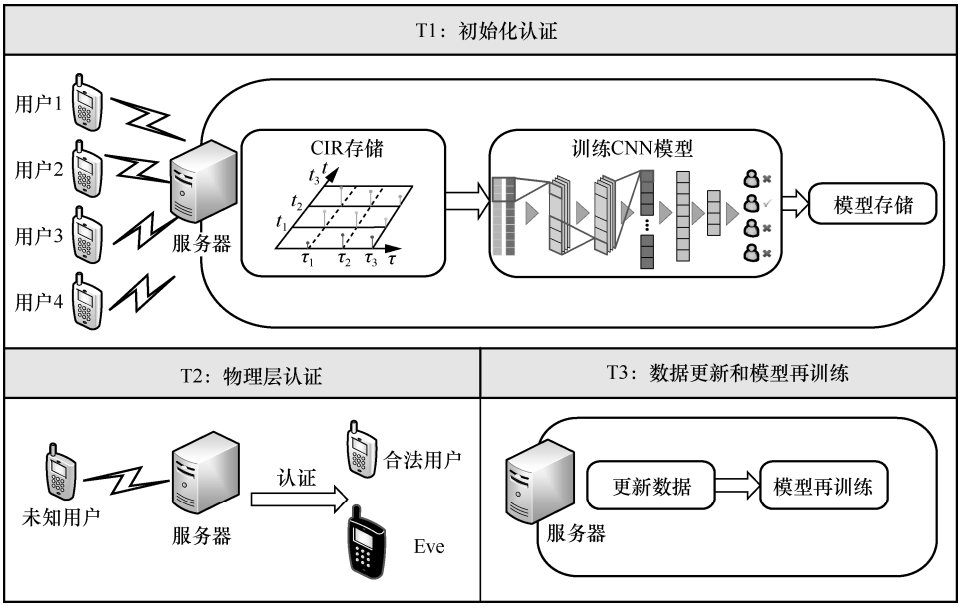


图 3　基于轻量级卷积神经网络的多用户认证流程

务时，基站通过该认证流程可以完成对合法用户的身份认证，避免 Eve 的入侵。

整个过程分 4 步进行，首先是初次认证，基站获取所有合法发射设备的无线信道初始特征，对网络进行训练，并将训练好的网络模型存储在服务器中，用户接入（初次认证）之后向基站发送消息时，基站可以直接判别该消息来源的合法性，最后完成服务器参数和网络模型的更新，详细的步骤描述如下。

步骤 1　初始化认证过程中由合法用户向基站服务器发出认证请求，发射信息包含用户的 ID，基站服务器接收用户 ID 后，对 ID 和 CIR 进行存储，用户信息注册如图 4 所示。

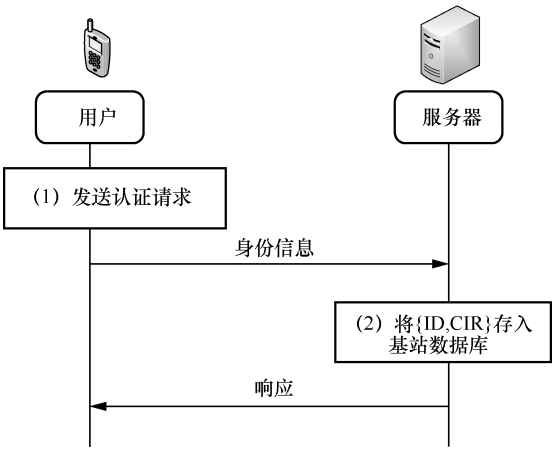


图 4　用户信息注册

步骤 2　在初始化认证阶段，基站服务器需要根据不同用户的 ID 和 CIR 对本文所提轻量级卷积神经网络进行训练（其中 ID 作为训练时的标签），完成初始化认证并将最终训练完成的模型存储在服务器上。

步骤 3　当未知用户访问基站时，基站通过存储的网络模型对用户身份进行认证，判断该用户是否为合法用户，物理层认证过程如图 5 所示。首先由用户向基站服务器发出接入请求，发射信息包含用户的 ID；基站服务器接收用户 ID 和 CIR 后，从数据库中加载 CNN 模型，计算出 softmax(z_{ID}) 作为检验统计量，并和阈值 γ 做比较。

$$H_0:\mathrm{softmax}(z_{\mathrm{ID}})>\gamma \tag{7}$$

$$H_1:\mathrm{softmax}(z_{\mathrm{ID}})<\gamma \tag{8}$$

其中，阈值 γ 的选择将会影响检测概率 P_{D} 和误警概率 P_{F}，其中 $P_{\mathrm{F}}=P(H_1\mid H_0)$，$P_{\mathrm{D}}=1-P(H_0\mid H_1)$。当检验统计量大于阈值时，认证成功，否则认证失败。

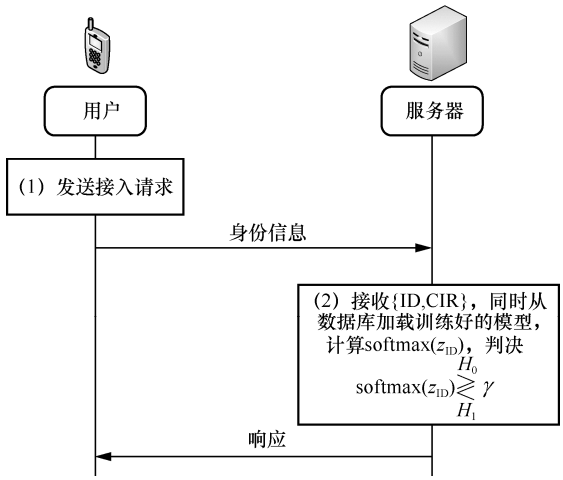


图 5　物理层认证过程

步骤 4　当用户初始化认证成功后，可以通过上层链路与基站建立一个安全的连接，定期对 CIR 进行更新，重新训练网络模型，并将训练好的模型存储在服务器上。

3　基于轻量级卷积神经网络的信道特征提取识别算法

在合法用户认证阶段，不同用户的信道特征提取识别是重要一环，因此本节设计了一种信道特征提取识别算法。

传统信道特征提取识别算法主要依赖专家知识，普适性不强。而卷积神经网络中的卷积操作通过不同大小的卷积核对输入进行卷积运算，其本质是提取特征。因此，本文设计了一种基于轻量级卷积神经网络的信道特征提取识别算法，算法流程如图 6 所示。

首先获得 CIR，例如，在 OFDM 通信系统中，通常会在特定的子载波上插入导频序列，导频序

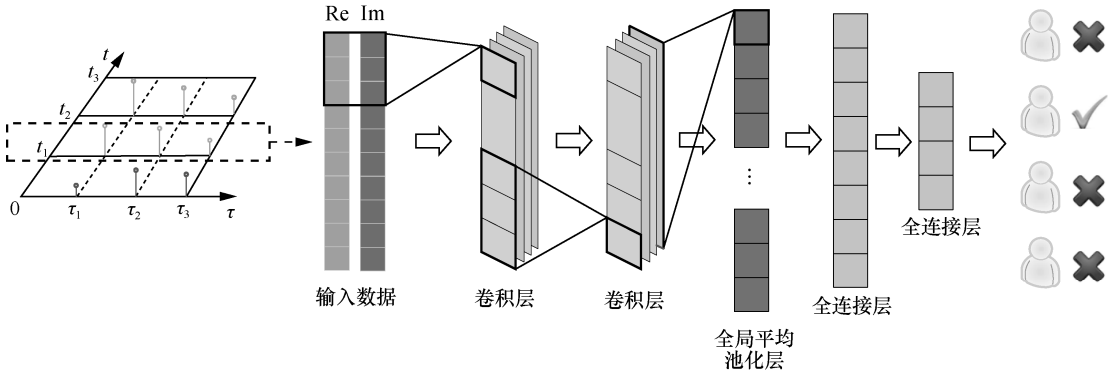


图 6　基于轻量级卷积神经网络的信道特征提取识别算法流程

列经过信道后可以由接收信号和导频得到信道估计。然后，将信道冲激响应中每一时刻下的复信道增益看作一个单独的样本，分为 Re、Im 两路并作为卷积神经网络的输入，对网络进行训练。

为了使在线训练成为可能，采用轻量级卷积神经网络，该网络仅由两层卷积层、一层全局平均池化层（global average pooling，GAP）和两层全连接层构成。

卷积层是卷积神经网络的核心。在一维卷积神经网络中，卷积核只在一个方向上移动，每个卷积层的输出维度由卷积核大小、步长决定。共有 F 个卷积核 G_n（$1<n<F$），卷积核的深度为 D、宽度为 W，输入特征向量为 $\boldsymbol{X}\in\mathbf{R}^{D\times L}$，$L$ 为特征向量的宽度，每个卷积核单步长的输出特征向量为 $\boldsymbol{Y}^n\in\mathbf{R}^{L-W+1}$，则它们之间的关系可以表示为：

$$Y_l^n=\sum_{i=1}^{D}\sum_{j=1}^{W}G_n^{i,j}X_{l-1+i,j} \tag{9}$$

其中，Y_l^n 表示第 n 个滤波器计算得到的输出特征向量的第 l 个元素，$0<l\leqslant L-W+1$。

全局平均池化层可以对卷积神经网络的特征向量进行降维，进一步缩减网络参数，提升网络效率。全局平均池化层对输入通道的每个特征图计算出一个均值，可以极大地缩减网络中的参数数量，对网络训练效率的提高有一定帮助。

全连接层将每个输入神经元和输出神经元相连，通过训练调配每个神经元连接的权重输出最终的特征向量。因此，全连接层在卷积神经网络中可被看作分类器。

最终输出通过函数产生，可以表示为：

$$\mathrm{softmax}(z_i)=\frac{\mathrm{e}^{z_i}}{\sum_{c=1}^{C}\mathrm{e}^{z_c}} \tag{10}$$

其中，z_i 为第 i 个神经元的输出值；C 为最后一层神经元个数，对应合法用户的个数。显然，经过 softmax 函数后输出值介于 0 和 1 之间，代表属于每个合法用户的概率值。

4　实验与分析

4.1　算法性能评估

为了验证提取识别算法的性能，基于文献[18]的数据集进行了测试。该数据集中提供了 3 种不同信道状态下的 CIR 真实测量结果，每种信道状态有 5 个 CIR 数据，每个 CIR 对应测试时间为 1 s，绝对时间采样点数为 1 500 个，时延域采样点数为 100 个。取其中 1 个样本的 CIR 进行插值，1 s 测试样本的信道冲激响应如图 7 所示。

应用所提算法对 3 种信道进行特征提取识别，轻量级卷积神经网络的具体参数配置见表 1。

网络的整体参数量为 3 459 个，待训练参数量为 3 363 个。将每种信道对应的样本划分为训练集和验证集（训练集为 4 个 CIR，验证集为 1 个 CIR），采取交叉训练验证的方式对网络进行训练，损失

函数选择随机梯度下降法，学习率为 0.001。训练轮次为 5 时，轻量级卷积神经网络性能结果如图 8 所示。轻量级卷积神经网络经过 5 个轮次的训练，在验证集上的准确率达到 97.8%，随机梯度损失值下降至 0.356。

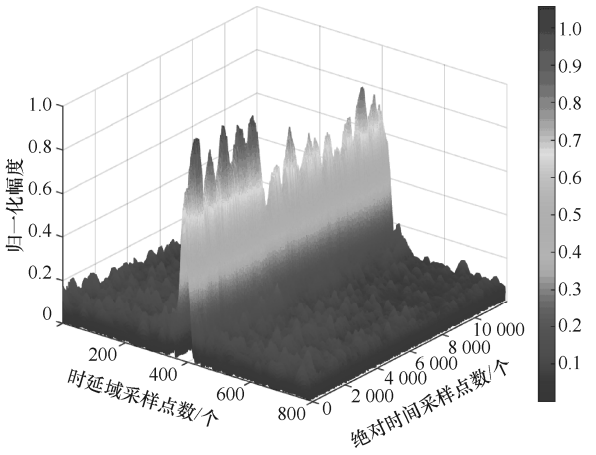


图 7　1 s 测试样本的信道冲激响应

表 1　轻量级卷积神经网络的具体参数配置

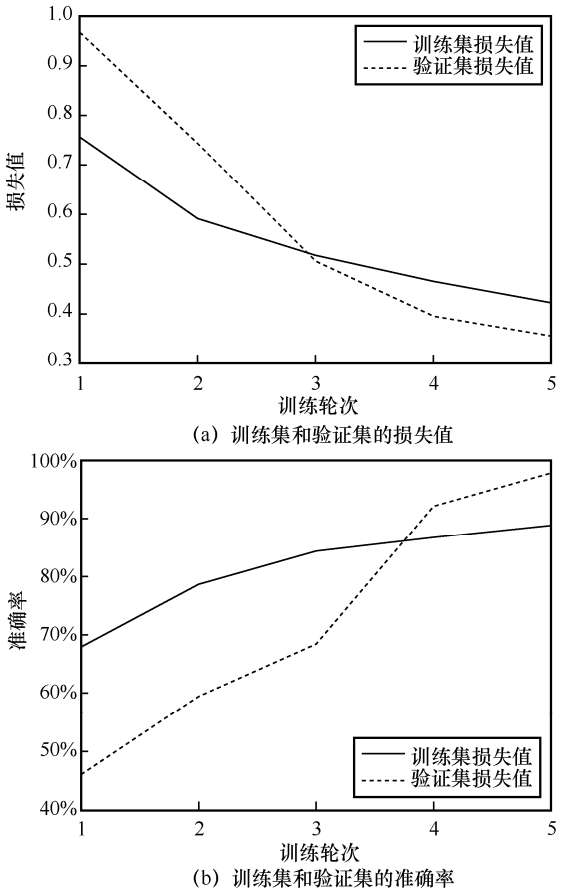
层	维度	参数量	激活函数
输入层	2×100×1	—	—
卷积层	1×41×16	640	ReLU
卷积层	1×19×32	2 048	ReLU
全局平均池化层	32	—	—
全连接层	16	528	—
全连接层	3	51	softmax

为了更好地衡量训练完成的网络模型在测试样本上的效果，首先对测试类别置信度做如下定义。

$$\mathrm{Con}=\frac{N_{\mathrm{correct}}}{N_{\mathrm{all}}}\times 100\% \tag{11}$$

其中，N_{correct} 代表一个 CIR 中判断正确的绝对时间采样点数，N_{all} 代表单个样本中绝对时间的采样点数，这里 N_{all}=1 500。测试类别置信度衡量了样本判别为某一对应信道的可信度，值越接近 100%，可信度越高。单个样本中判断正确的采样点数服从二项分布，因此测试类别置信度高于 x 的概率可以表示为：

$$P\left(\mathrm{Con}>x\right)=\sum_{i=N_{\mathrm{all}}\cdot x}^{N_{\mathrm{all}}}\binom{i}{N_{\mathrm{all}}}p^{i}(1-p)^{N_{\mathrm{all}}-i} \tag{12}$$



(a) 训练集和验证集的损失值

(b) 训练集和验证集的准确率

图 8　轻量级卷积神经网络性能结果

当 p=90.8%时，P(Con>83%)≈100%。此结果表明，即使验证集准确率只有 90.8%，测试类别置信度大于 83%的概率也接近 100%。而当测试类别置信度大于 50%时，可以认为该 CIR 判断正确。因此，当验证集准确率大于 90%时，则每个 CIR 被判断为正确类别的概率接近 100%。

同时，文献[18]所用数据中提供了两个测试 CIR（分别对应两种不同的信道状态），对上述训练后的网络模型进行测试，均能够完成有效识别，且置信度高于 95.0%。

实验证明了所提算法的有效性，该算法训练 5 个轮次后趋于收敛，在验证集上的准确率达到 90%以上，能够较好地提取识别信道特征，完成对不同信道特征的分类识别。

4.2　多用户认证系统性能评估

为了进一步验证所提多用户认证系统的检测

性能，在第 1 节所提系统模型的约束下，设计仿真实验场景，考虑在单个小区中一个基站服务器为多个用户提供服务，同时在距离用户很近的位置存在窃听方。

基于几何随机模型（geometry-based stochastic model，GBSM）仿真生成 6 个用户和 1 个 Eve 在不同信噪比（signal to noise ratio，SNR）下（SNR 分别为 1 dB、3 dB、5 dB、7 dB）的 CIR，并将其作为初始化认证时所需要的信道样本，每种信噪比下每个用户生成 5 个 CIR，共计 140 个 CIR。

多用户仿真场景如图 9 所示，散射体个数为 50，载波频率为 2.4 GHz，基站位于原点处，用户在距离基站 2 000 m 处以半径为 200 m 的距离随机散布，并保持静止。仿真时基站接收每个用户和 Eve 共 5 s 的 CIR，每个 CIR 持续时长为 1 s，绝对时间采样点数为 1 500 个，时延域采样点数为 534 个。

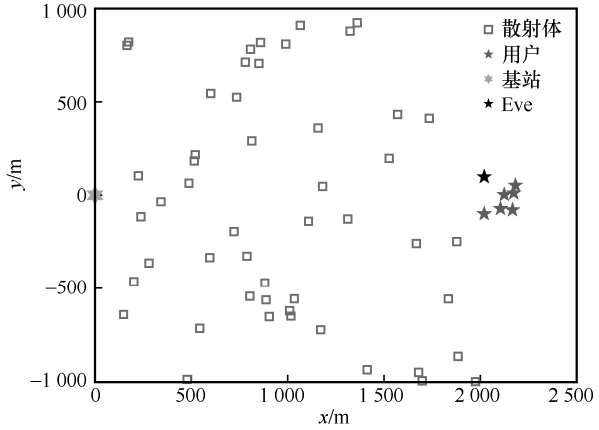


图 9　多用户仿真场景

在仿真中，引入受试者操作特征（receiver operating characteristic，ROC）曲线验证系统性能，曲线下面积（area under the curve，AUC）反映了认证性能，AUC 越大表明系统认证性能越好。

4.2.1　不同信噪比和不同用户数量的认证性能对比

在不同信噪比和不同用户数量下进行测试，网络模型训练轮次为 8 轮。

多用户认证系统在不同用户数量、不同信噪比下的 ROC 曲线如图 10 所示。

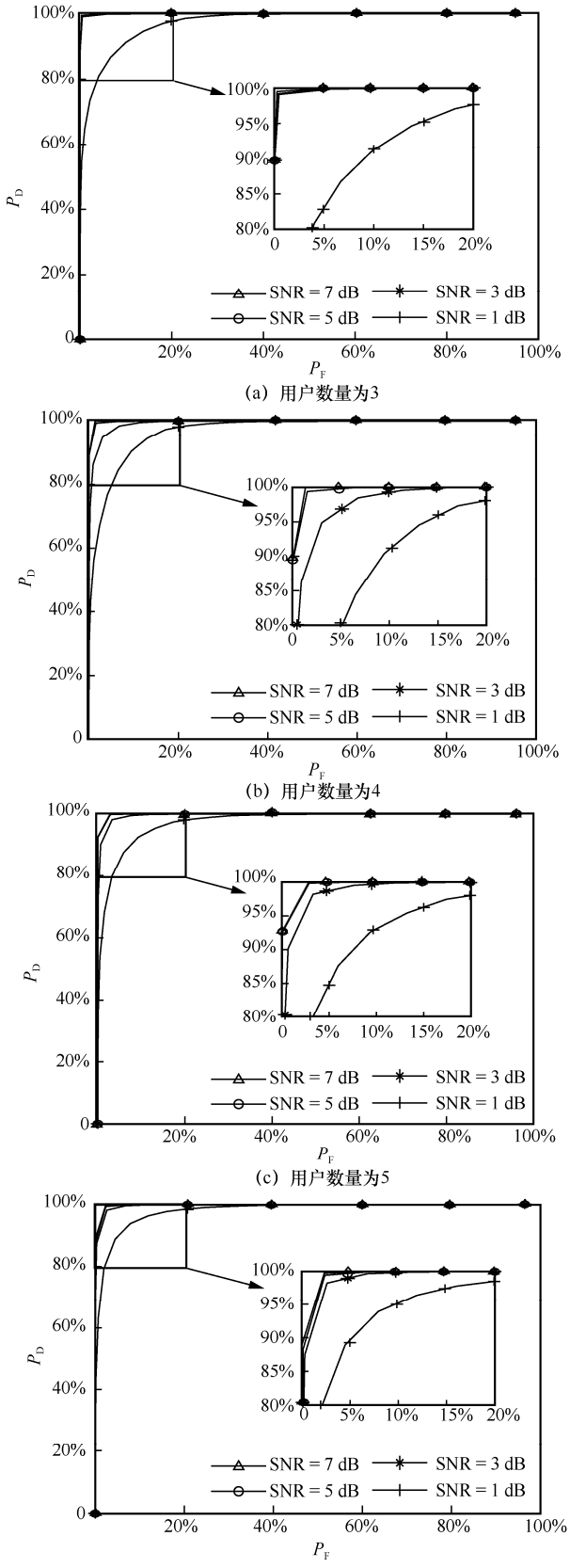


图 10　多用户认证系统在不同用户数量、不同信噪比下的 ROC 曲线

从图 10 可以看出，在相同的虚警概率下，随着信噪比不断降低，检测概率也降低。从图 10（a）可以看出，在 SNR 不低于 3 dB 的条件下，P_F 大于 5.6%时，P_D 不低于 99.8%；从图 10（b）可以看出，在 SNR 不低于 3 dB 的条件下，P_F 大于 6.7%时，P_D 不低于 98.4%；从图 10（c）可以看出，在 SNR 不低于 3 dB 的条件下，P_F 大于 7.6%时，P_D 不低于 99.5%；从图 10（d）可以看出，在 SNR 不低于 3 dB 的条件下，P_F 大于 6.7%时，P_D 不低于 99.6%。而且随着用户数量不断上升，多用户认证系统的检测性能仍然较好，在用户数为 6、SNR=1 dB 的条件下，P_F=7.9%时，P_D=93.9%。

4.2.2　不同训练轮次的认证性能对比

本文还探索了所提多用户认证系统的检测性能与训练轮次（epoch）之间的关系。多用户认证系统在不同训练轮次下的 ROC 曲线如图 11 所示。从图 11 可以看出，在相同的 P_F 下，随着训练轮次增加，P_D 不断提高，但在训练轮次超过 10 以后多用户认证系统趋近收敛，当 epoch=10、P_F 大于 7.3%时，P_D 不低于 97.1%；当 epoch=12 时，训练模型对数据的拟合程度最好，P_D 最高；当 epoch=14 时，P_D 有所下降，但值得注意的是，P_F=5%时，P_D 达到 95%以上，相比于 epoch=8 时仍然有较大的提升。

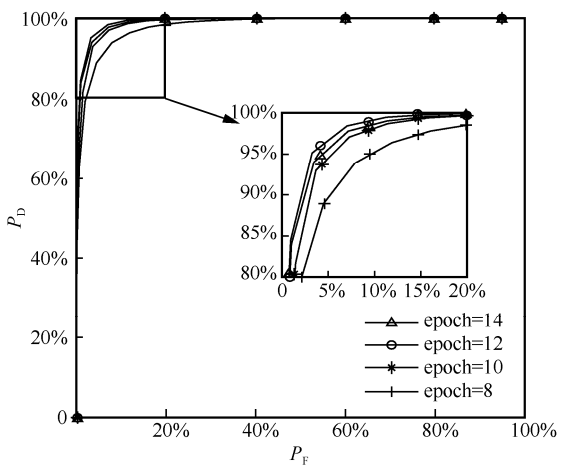


图 11　多用户认证系统在不同训练轮次下的 ROC 曲线

4.2.3　不同认证方式的性能对比

为了进一步体现所提算法的性能优势，与文献[16]的认证算法进行对比。文献[16]采用深度神经网络（deep neural network，DNN）对不同用户的 CSI 进行识别认证，并结合 3 种不同的加速梯度下降算法设计了多用户认证方案，其中 Adam-based 多用户认证算法具备最快的收敛速度和较好的认证准确率，因此将它作为本文算法的对比基准。仿真时 DNN 层数为 5 层，每一层的神经元个数分别为 120、50、25、12、4，其余参数配置为 $\alpha=1\times10^{-3}$、$\beta_1^{\perp}=0.9$、$\beta_2^{\perp}=0.999$、$\phi_0=1$，其中 α 代表 DNN 的学习率，$\beta_1^{\perp}$ 和 $\beta_2^{\perp}$ 代表 Adam-based 算法的梯度下降系数，ϕ_0 代表小批量数量。

用户数量为 4、SNR=4 dB 时，不同认证方法的 ROC 曲线如图 12 所示，文献[16]中的方法在总样本数为 20 时模型无法收敛，因此对比本文所提 CNN 方法在样本数为 20 时与 DNN 方法在样本数为 80 和 100 时的性能。可以看出，所提方法仅需要 20 个 CIR 即可得到较好的效果，在 P_F 大于 2.4%时，P_D 不低于 99.5%，而对比方法在训练样本数为 80、P_F 大于 2.4%时，P_D 不低于 75.0%，比本文所提方法低 24.5%，而当对比方法训练 CIR 数量增加到 100 时，效果才略优于本文所提方法。上述结果表明，本文所提多用户认证系统能在保证较高认证准确率的同时，显著降低对 CIR 的需求数量。

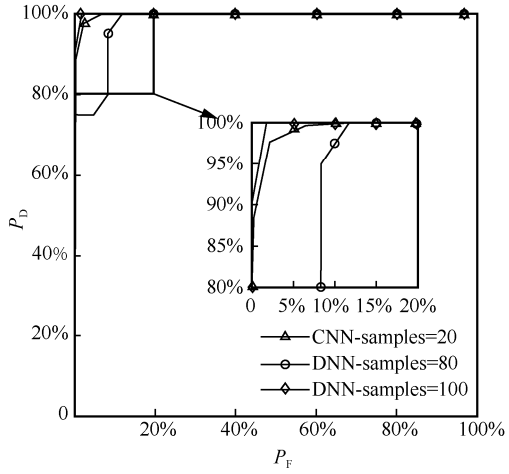


图 12　不同认证方法的 ROC 曲线

5 结束语

本文提出了一种基于轻量级卷积神经网络和信道特征辅助的多用户物理层认证机制，通过改变输入的形式减少对 CIR 的需求，同时仅利用两层卷积层对 CIR 进行特征提取，然后利用一层全局平均池化层和两层全连接层对特征进行分类识别。同时，分析了算法的检测性能和多用户认证系统的性能，结果表明，本文提出的多用户物理层认证机制能够很好地对不同用户的身份进行认证，而且网络收敛所需要的 CIR 数量少，训练时间短，相比现有方法更加适合在物理层实际部署。

参考文献：

[1] ALHILAL A Y, FINLEY B, BRAUD T, et al. Street smart in 5G: vehicular applications, communication, and computing[J]. IEEE Access, 2022(10): 105631-105656.

[2] WANG D, BAI B, ZHAO W B, et al. A survey of optimization approaches for wireless physical layer security[J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1878-1911.

[3] SHAWKY M A, BOTTARELLI M, EPIPHANIOU G, et al. An efficient cross-layer authentication scheme for secure communication in vehicular ad-hoc networks[J]. IEEE Transactions on Vehicular Technology, 2023, 72(7): 8738-8754.

[4] XIE N, ZHANG J H, ZHANG Q H. Security provided by the physical layer in wireless communications[J]. IEEE Network, 2022(99): 1-7.

[5] XIAO L, GREENSTEIN L J, MANDAYAM N B, et al. Using the physical layer for wireless authentication in time-variant channels[J]. IEEE Transactions on Wireless Communications, 2008, 7(7): 2571-2579.

[6] BRIK V, BANERJEE S, GRUTESER M, et al. Wireless device identification with radiometric signatures[C]//Proceedings of the 14th ACM international conference on Mobile computing and networking. New York: ACM Press, 2008: 116-127.

[7] AL-SHAWABKA A, RESTUCCIA F, D'ORO S, et al. Exposing the fingerprint: dissecting the impact of the wireless channel on radio fingerprinting[C]//Proceedings of IEEE INFOCOM 2020-IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2020: 646-655.

[8] AZIMI-SADJADI B, KIAYIAS A, MERCADO A, et al. Robust key generation from signal envelopes in wireless networks[C]//Proceedings of the 14th ACM conference on Computer and communications security. New York: ACM Press, 2007: 401-410.

[9] JAVALI C, REVADIGAR G, PLETEA D, et al. Demo abstract: location fingerprint evidence and authorisation using WiFi channel characteristics[C]//Proceedings of 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops). Piscataway: IEEE Press, 2016: 1-3.

[10] QIU X Y, DAI J M, HAYES M. A learning approach for physical layer authentication using adaptive neural network[J]. IEEE Access, 2020(8): 26139-26149.

[11] SHENG Y, TAN K, CHEN G, et al. Detecting 802.11 MAC layer spoofing using received signal strength[C]//Proceedings of IEEE INFOCOM 2008 - The 27th Conference on Computer Communications. Piscataway: IEEE Press, 2008: 1768-1776.

[12] LIU F J, WANG X B, TANG H. Robust physical layer authentication using inherent properties of channel impulse response[C]//Proceedings of 2011 - MILCOM 2011 Military Communications Conference. Piscataway: IEEE Press, 2012: 538-542.

[13] TUGNAIT J K, KIM H. A channel-based hypothesis testing approach to enhance user authentication in wireless networks[C]//Proceedings of 2010 Second International Conference on COMmunication Systems and NETworks (COMSNETS 2010). Piscataway: IEEE Press, 2010: 1-9.

[14] YU Y L, LIU F X, MAO S. Fingerprint extraction and classification of wireless channels based on deep convolutional neural networks[J]. Neural Processing Letters, 2018, 48(3): 1767-1775.

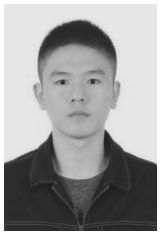
[15] LIAO R F, WEN H, PAN F, et al. A novel physical layer authentication method with convolutional neural network[C]//Proceedings of 2019 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA). Piscataway: IEEE Press, 2019: 231-235.

[16] LIAO R F, WEN H, WU J S, et al. Security enhancement for mobile edge computing through physical layer authentication[J]. IEEE Access, 2019(7): 116390-116401.

[17] RAPPAPORT T S. 无线通信原理与应用（第二版）[M]. 周文安, 付秀花, 王志辉, 等, 译. 北京: 电子工业出版社, 2018.
RAPPAPORT T S. Wireless communications: principles and practice (second edition)[M]. Translated by ZHOU W A, FU X H, WANG Z H, et al. Beijing: Publishing House of Electronics Industry, 2018.

[18] 王瑞星, 刘斌, 杜健鹏, 等. 基于两种算法的无线信道“指纹”特征识别[J]. 通信技术, 2016, 49(10): 1271-1279.
WANG R X, LIU B, DU J P, et al. Recognition of wireless channel “fingerprint” feature based on two algorithms[J]. Communications Technology, 2016, 49(10): 1271-1279.

[作者简介]



王延坤（2000−），男，国防科技大学电子科学学院硕士生，主要研究方向为物理层安全、信道探测与建模等。

郭登科（1996− ），男，国防科技大学电子科学学院博士生，主要研究方向为无线物理层安全、智能超表面技术等。

马东堂（1969− ），男，博士，国防科技大学电子科学学院教授、博士生导师，主要研究方向为智能无线通信与网络、物理层安全、无人机通信与网络优化等。

熊俊（1987− ），男，博士，国防科技大学电子科学学院副研究员、硕士生导师，主要研究方向为智能无线通信、物理层安全、分布式协同等。

张晓瀛（1980− ），女，博士，国防科技大学电子科学学院副教授、硕士生导师，主要研究方向为宽带移动通信接收、信道探测与建模等。