光电技术及应用

DOI：10.16818/j.issn1001－5868.2020.04.027

基于星座图对射频指纹识别方法的研究

袁建国*，赵富强，覃陆祯玥，徐一为，熊首泽
（重庆邮电大学 光电信息感测与传输技术重庆市重点实验室，重庆 400065）

摘　要： 针对星座图的射频(RF)指纹识别方案中，低信噪比环境下识别准确率低的问题，提出一种基于欧式距离与幅度距离的二维识别算法来进行RF指纹识别。该方案通过对星座图进行优化处理，可从优化后的星座图中提取识别性能更好的RF指纹，再通过二维识别算法来提高识别准确率。仿真结果表明：与仅用欧式距离作为判断依据的方法相比，所提出的二维识别算法的识别准确率最高可提升8%，在设备容量为50组的情况下识别准确率为77.8%，并且从优化后的星座图中所提取的RF指纹具有更好的唯一性和稳定性。

关键词： 射频指纹；星座图；欧式距离；幅度距离
中图分类号： TN929.11　**文章编号：** 1001－5868(2020)04－0592－06

Research on the Radio Frequency Fingerprint Identification Method Based on the Constellation Diagram

YUAN Jianguo, ZHAO Fuqiang, QINLU Zhenyue, XU Yiwei, XIONG Shouze
(Chongqing Key Laboratory of Photoelectronic Information Sensing and Transmitting Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, CHN)

Abstract: In the RF fingerprint identification scheme for the constellation diagram, with respect to the problem of the low identification precision rate in low signal noise ratio (SNR) environment, a two-dimensional identification algorithm based on the Euclidean distance and amplitude distance is proposed. This solution optimizes the constellation diagram to extract RF fingerprints with better identification performance from the optimized constellation diagram, and then uses the two-dimensional identification algorithm to improve the identification precision rate. Simulation results show that compared with the method based on the Euclidean distance, the identification precision rate of the proposed two-dimensional identification algorithm can be improved by up to 8% and the identification precision rate is 77.8% when the equipment capacity is 50. The RF fingerprints characterized by the optimized constellation diagram present better uniqueness and robustness.

Key words: radio frequency fingerprint; constellation diagram; Euclidean distance; amplitude distance

0　引言

随着网络信息技术的飞速发展，无线通信设备的接入认证问题已成为当今无线网络安全面临的严峻挑战。在传统的无线通信系统中，设备访问时的认证主要取决于存储在设备中的身份认证信息或输入的认证指令，这种认证方式存在密码泄露等问题。由于射频(RF)指纹是设备本身的物理特征，建立在物理层上的RF指纹信息不易被修改，可从通信系

收稿日期：2020－04－04.
基金项目：国家自然科学基金项目(61671091)；重庆市基础与前沿研究计划项目(csts2017jcyjAX0427).
* 通信作者：袁建国　E-mail：yyyyjg@126.com

统的底层来保护系统。基于 RF 指纹的物理层安全技术可有效地解决无线设备的安全接入问题[1-2]。

射频指纹的特征提取过程是射频指纹识别中的重要环节。现有的射频指纹特征提取方法主要分为两种[1-3]：一种是基于瞬态信号响应射频指纹提取方法，另一种是基于稳态信号响应射频指纹提取方法。星座图中包含了稳态信号信息，其中包括滤波器响应、功率放大器的非线性效应和其他线性与非线性相干因素等。设备间的差异可体现在星座图中，反过来星座图也可以反映设备间的差异，所以可直接提取星座图中的特征作为射频指纹。

本文开展了基于星座图的射频指纹识别方法的研究，选用星座图中聚类中心点作为射频指纹，以欧式距离的和与幅度距离的和作为指纹特征。提出一种基于欧式距离与幅度距离的二维识别算法来进行指纹识别，并进行了相应的仿真分析。

1　系统描述与分析

实际的无线网络安全协议中常出现漏洞现象。比如，IEEE 820.11 无线局域网（Wireless Local Area Network，WLAN）最初的有线等效加密（Wired Equivalent Privacy，WEP）协议中很容易被攻击者通过抓包来实现统计攻击。尽管此后已将其升级到保护无线电脑网络安全系统（Wi-Fi Protected Access，WPA）和 WPA2，但其口令句可被恢复，仍然存在各种安全问题。针对 WLAN 中非法访问、密码泄露等问题，选取 IEEE 802.11n 正交频分复用（Orthogonal Frequency Division Multiplexing，OFDM）系统作为本次仿真系统模型，系统框图如图 1 所示。

射频指纹之所以能用来识别不同个体，是因为射频设备中的电子元器件存在容差效应，导致发射出的电磁波包含发射设备独有的射频指纹特征。图 1 中正交调制器和功率放大器两个器件对射频指纹的影响最大，正交调制器的原理框图如图 2 所示。

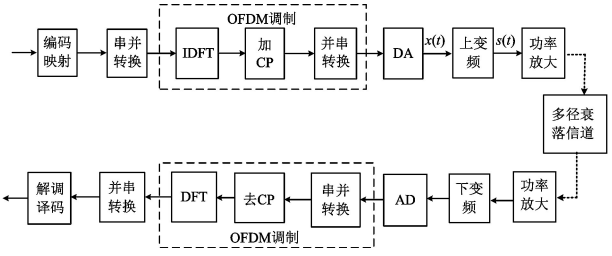


图 1　基于 802.11n OFDM 系统模型

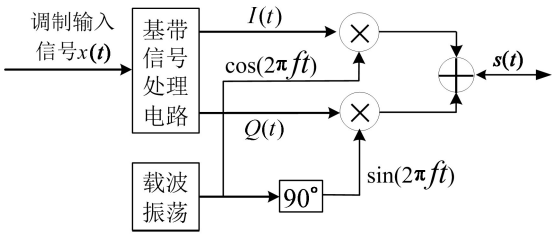


图 2　正交调制器原理框图

正交调制的一般表达式为[4]

$$s(t)=I(t)\times\cos(2\pi ft)-Q(t)\times\sin(2\pi ft) \tag{1}$$

其中，$I(t)$ 和 $Q(t)$ 分别为正交调制前输入信号 $x(t)$ 的实部和虚部；上变频时的载波频率为 f，其值为 2.4 GHz。在实际的通信过程中会产生线性误差，主要包括增益误差和偏移误差两种。

正交调制过程中的基带信号，考虑其线性增益误差，若 A_I 和 A_Q 分别为 I 路和 Q 路的增益误差，需将 $I(t)$ 和 $Q(t)$ 做如下替换：

$$I(t)=(I+A_I)I(t) \tag{2}$$

$$Q(t)=(I+A_Q)Q(t) \tag{3}$$

对于两路正交载波，除了考虑其线性偏移误差外，因载波不能准确相移 90°，故 I，Q 两路还存在初始相位。若 f_i 和 f_q 为载波频率偏移，I_i 和 I_q 为初始相位，则需将两路正交载波做如下变换：

$$\cos(2\pi ft)\rightarrow\cos[2\pi(f+f_i)+I_i] \tag{4}$$

$$\sin(2\pi ft)\rightarrow\sin[2\pi(f+f_q)+I_q] \tag{5}$$

将式(2)～(5)代入式(1)中，得到实际情况下的已调信号 $s(t)$，可用式(8)表示：

$$i(t)=(1+A_I)\times I(t)\times\cos[2\pi(f+f_i)t+I_i] \tag{6}$$

$$q(t)=(1+A_Q)\times Q(t)\times\sin[2\pi(f+f_q)t+I_q] \tag{7}$$

$$s(t)=i(t)-q(t) \tag{8}$$

由于存在容差效应，每个 RF 设备都有不同的调制误差。正因为这些调制误差，每个 RF 设备均拥有自身唯一的指纹特征。

功率放大器模型其实是一个非线性系统，可用沃尔泰拉级数模型和泰勒级数模型来表示。本文采用无记忆泰勒级数功率放大器模型进行研究，其系统模型如图 3 所示。

功率放大器的系统响应函数可用式(9)表示。

$$\psi(n)=\sum_{l=1}^{K}a_l[s(n)]^l \tag{9}$$

其中，输入信号是 $s(n)$，功率放大器的输出信号为 $\psi(n)$，K 是泰勒多项式的阶数，a_l 代表泰勒多项式的系数。对于无记忆泰勒级数功率放大器而言，l 一般取奇数项，K 取 5，即可得到输出 $\psi(n)$。通过式(9)可看出，对于不同的泰勒级数功率放大器，可通过改变泰勒多项式的系数来区别不同设备。

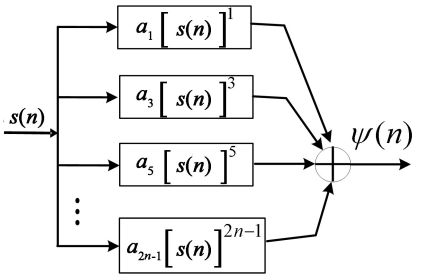


图 3 无记忆泰勒级数功率放大器的系统模型

2 射频指纹特征的获取与优化

基于星座图的射频指纹识别是一种基于稳态信号响应的射频指纹提取方法。在 802.11n 协议中有 16QAM，64QAM，BPSK 和 QPSK 四种调制方式，本文选择 QPSK 调制方式。以聚类中心点作为指纹，如果选取 16QAM 或 64QAM 会增加计算复杂度，还会占用更多的存储空间；BPSK 则过于简单，不利于提取射频指纹，故选择 QPSK 调制可获得更为清晰的星座图。

2.1 星座图的获取与优化处理

OFDM 系统是一种特殊的多载波传输技术，被广泛应用在 WLAN 领域。射频指纹识别技术也可应用在 WLAN 中以识别非法访问接入点(Access Point，AP)。所以本文选用 IEEE 802.11n OFDM 系统模型。然而，在 OFDM 系统中由于发送端和接收端的载波频率不相等、信道衰落、发送端硬件差异等问题会造成相位噪声，相位噪声会影响星座图的分布，因而通过数字信号处理(Digital Signal Processing，DSP)方法降低相位噪声对系统的干扰。将处理后的数字信号在复平面上绘制出来即为星座图。星座图提供了一种方便的方法来研究数字通信系统接收机的性能以及 I/Q 信号之间的关系。从式(10)[4]中可看到，当接收机和发射机的载波频率不相等时，星座图中的数据会有一个随时间 t 变化的相位旋转因子 $e^{j2\pi\theta t+\gamma}$。

$$Y(t)=X(t)e^{j2\pi\theta t+\gamma} \tag{10}$$

其中，$X(t)$为发射机基带信号，$Y(t)$为接收机下变频后的基带信号，γ 为接收机接收信号时的相位误差，θ 为接收机与发射机载波频率之差。可先利用差分处理得到较为稳定的星座图。具体操作如下[5]：

$$D(t)=Y(t)\cdot Y^{*}(t+n)$$

$$D(t)=X(t)e^{j2\pi\theta t+\gamma}\cdot X(t+n)e^{-j2\pi\theta(t+n)-\gamma}$$

$$D(t)=X(t)\cdot X(t+n)e^{-j2\pi\theta n} \tag{11}$$

其中，$Y^{*}(t)$为共轭取值，n 为差分间隔。虽然有一个选择因子 $e^{-j2\pi\theta n}$，但是其为一个恒定的数值。后续将运用 OFDM 系统中的信道估计技术进一步对星座图进行优化。

除此之外，星座图中难免会出现偏离较大的点，这些点在星座图中并不多，但会影响整体的聚类效果，导致得到的聚类中心点缺失稳定性。考虑到这一点，可将星座图中离散程度较大的点适当地进行拉回处理，而不是一味地进行滤除处理：首先设置四个阈值，分别为 ±1.5 和 ±0.2，再将星座图中点的实部和虚部的值分别定义为 i 和 q。当实部 i 的值满足 $i>1.5$ 或 $i<-1.5$ 条件时，将 i 分别赋值为 1.5 和 -1.5；若实部 i 的值满足 $0<i<0.2$ 或 $-0.2<i<0$ 条件时，将 i 分别赋值为 0.2 和 -0.2。同理，虚部的值 q 也按上述过程处理。这样处理的好处是既保留了星座图的离散性，又可得到较为稳定的聚类中心点。

2.2 基于星座轨迹图的射频指纹特征提取

对星座图进行优化后，提取星座图中的指纹特征是最为重要的一个环节。可采用 K 均值(K-means)聚类算法来获取星座图中的 4 个聚类中心点。文献[4]选取的是 5 个聚类中心点，因为未做子载波解映射处理，保留了{$-21,-7,0,21,7$}子载波上的数据，这样会在聚类边缘出现聚类错误。如图 4 所示，数据点的归纳错误将影响聚类中心点的位置。

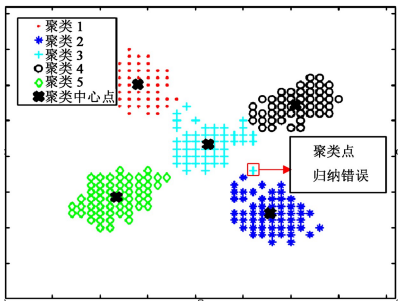


图 4 未做子载波解映射处理的 K-means 聚类

通过计算不同设备间聚类中心点的欧式距离的

和与幅度差值的和，可获得设备的匹配程度，从而可识别每个设备。如图 5 所示，设备 1 到达自身参考聚类中心点的欧式距离的和明显小于其他设备，说明欧式距离的和可用来计算匹配程度。

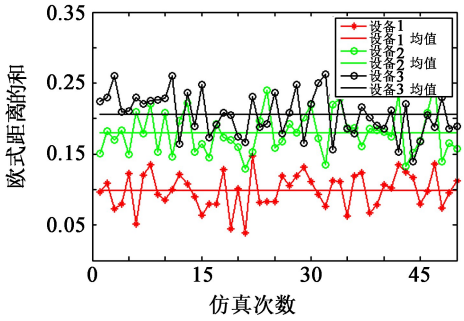


图 5　欧氏距离差异图

由于信道和噪声的影响，即使同一设备在调制前发送相同的数据，所得到的聚类中心点也有微小的差异。如图 6 所示，设备到达自身参考聚类中心点的欧式距离也是变化的。为尽可能地减少误差，在确定参考聚类中心点前必须进行优化操作。具体训练操作如下：

首先将设备通过如图 1 所示系统循环仿真 100 次，得到 100 组聚类中心点，将前 50 次聚类中心点作为训练数据，后 50 次聚类中心点进行识别操作。然后取前 50 次聚类中心点的平均值作为参考聚类中心点，再计算前 50 次聚类中心点到参考聚类中心点间的欧式距离，滤除掉离参考聚类中心点最近和最远的数据点。最后重新计算剩下 48 次聚类中心点的平均值，以这个平均值作为最后的参考聚类中心点，即为射频指纹。

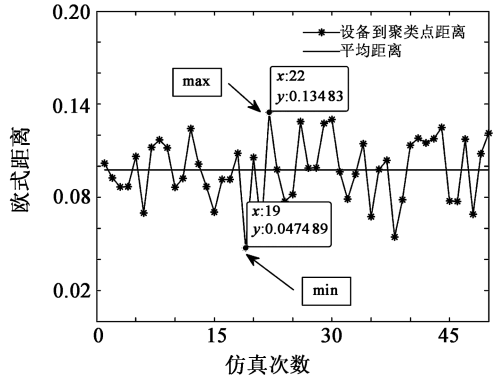


图 6　设备参考聚类中心点的确定

3　一种新颖的二维识别算法

射频指纹识别是一个模型分类问题，由训练和识别阶段组成。其中，将设备优化后的参考聚类中心点作为射频指纹，提取到每个设备的指纹后，再登记入库并完成训练过程。在识别阶段，首先采集待识别设备的射频指纹，然后将其与指纹数据库中的已有指纹进行比较，以确定身份是否合法。如果待识别设备身份合法，再进行身份匹配。

在身份匹配判断过程中，本文主要依照设备间聚类中心的欧式距离的和与幅度差值的和来获取设备相似度的匹配程度。本次实验中，利用 QPSK 调制得到 4 个聚类中心点，将其记为 k_p^i，$0<p\leqslant 4$。当获得设备 i 的聚类中心点后，针对新输入的设备 j，通过式(12)计算聚类中心的欧式距离的和：

$$S_{i,j}=\sum_{p=1}^{p}[d(k_p^i-k_p^j)] \tag{12}$$

其中，$S_{i,j}$ 表示设备 i 与设备 j 聚类中心的欧式距离的和，p 表示 QPSK 中的第 p 个点，d 表示两点间的欧式距离，k_p^i 和 k_p^j 分别表示 i 设备和 j 设备的第 p 个点的坐标。除了利用欧式距离的和来获得匹配程度外，幅度差的和同样也可计算匹配程度，式(13)为幅度差的计算公式。

$$A_{i,j}=\sum_{p=1}^{p}[a(k_p^i-k_p^j)] \tag{13}$$

其中，$A_{i,j}$ 表示设备 i 与设备 j 聚类中心的幅度距离的和，a 表示幅度差值。得到新输入设备 j 的聚类中心点后，如果 $A_{x,j}(x=1,2,3,\cdots,n)$ 最小，则判决 j 设备属于库中所存的第 x 个设备。最后，通过分析 $S_{i,j}$ 和 $A_{i,j}$ 的大小可对输入设备进行准确判断，具体判决流程如图 7 所示。

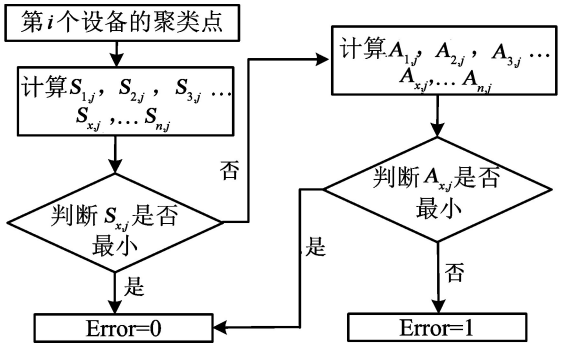


图 7　识别判决流程

在识别前，通过训练过程将每个设备的射频指纹记录到指纹数据库中。在识别阶段，以欧式距离的和作为第一判决特征，当获得设备 i 的 4 个聚类中心点后，计算设备 i 的聚类中心点与射频指纹库中每个设备聚类中心点的欧式距离总和，先判断是否与指纹数据库中设备 i 的欧式距离的和最小。如

果是，则判决正确；如果不是，再看幅度差值的和是否与设备 i 的幅度差值的和最小。

4 仿真结果分析

4.1 SNR 变化下射频指纹识别准确率的变化

在设备量为 10 组、信噪比(Signal Noise Ratio，SNR)在 0～40 dB 的情况下，依照上文中的二维识别过程，得到如图 8 所示的结果。仿真结果显示，在 SNR 为 20 dB 时，识别准确率为 91.4%。相比文献[1]对 4 个无线电设备的识别过程，二维识别算法在确保识别准确率大于 90%的情况下，提升了识别设备容量。此外，文献[1]还采用多特征的机器学习分类算法，不仅占用大量的存储空间，还会增加算法的计算复杂度。

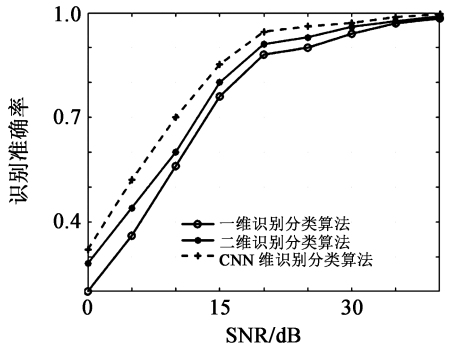


图 8 各算法在不同信噪比下的识别准确率

文献[6]仅根据欧式距离作为判断依据，虽然在高 SNR 环境下有良好的识别性能，但在低 SNR 环境下，识别性能明显降低。本文所提出的欧式距离与幅度距离的二维识别算法与一维识别算法相比，识别准确率提升显著，在 SNR 较低环境下作用更为明显，当 SNR 为 5 dB 时，识别准确率最高可提升 8%。

在分类识别过程中，机器学习算法可以提供出色的分类识别效果，例如卷积神经网络(Convolutional Neural Networks，CNN)算法、决策树算法等。但是这些算法需要长时间的训练过程，且算法复杂度较高[1-3,7]。本文提出的二维识别算法可同时满足低计算复杂度和高识别准确率的要求。

4.2 设备容量变化下射频指纹识别准确率的变化

在现有的研究中，有的算法准确率高达 95%，但只是针对几个设备进行识别，不符合实际的应用场景。考虑到设备容量问题，本文仿真了设备量在 3～50 组时的识别准确率，结果如图 9 所示。

由图 9 可知，在 SNR 为 20 dB 时，对 3 组设备的识别准确率高达 100%。但随着设备量的增加，识别准确率明显下降：当设备容量提升至 50 组时，二维识别算法的识别准确率为 77.8%。由上述仿真结果可知，二维识别算法与一维识别算法相比，不仅可以提高识别准确率，还可以增加系统的设备容量。

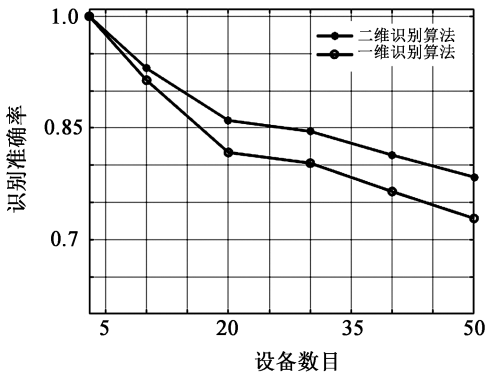


图 9 不同设备容量下的识别准确率

4.3 基于星座图提取的射频指纹特点

无线通信设备的射频指纹是可识别信号的一个或多个特征的集合，用来识别信号发射源。在实际应用时，射频指纹应具备唯一性、稳定性、时不变性等特点。文献[4]已指出，WLAN 网卡提取的射频指纹在 5 个月内保持一致，设备识别分类性能保持稳定。然而，发射机和接收机之间的距离、电压、电流等的变化会影响射频指纹的稳定性[8]。本文将对基于星座图提取的射频指纹进行唯一性和稳定性性能分析。

设备的参考聚类中心点因受信道和噪声的影响，会随着 SNR 的变化而变化，参考聚类中心点也就丢失了射频指纹应具备的唯一性。为解决这个问题，可选取 SNR 为 10 dB 以下的参考聚类中心点作为唯一的射频指纹，在不同 SNR 下仿真得到如图 10 所示的识别情况。如果识别准确率和图 8 所示的识别准确率相似，则可论证基于星座图提取的射频指纹具有唯一性。虽然随着 SNR 的变化，设备的射频指纹会改变，但是本文只选取 SNR 为 10 dB 时的聚类中心点作为射频指纹的固定参考聚类中心点，确保了射频指纹的唯一性。仿真实验表明，射频指纹的参考聚类中心点保持不变，在 SNR 为 20 dB 时，识别准确率可达 90.4%。

通过对射频指纹唯一性特点的分析可知 SNR 对聚类中心点的影响不是特别大。表 1 与表 2 是

50 组中某一设备的 4 个聚类中心点受到 SNR 影响的变化情况。

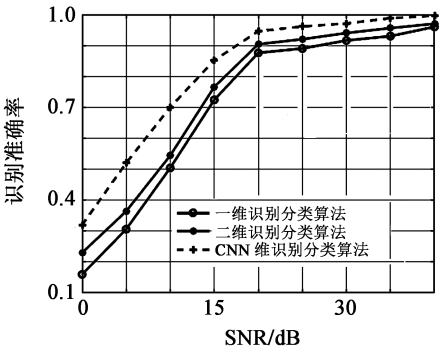


图 10　各算法在参考聚类中心点固定时不同 SNR 下的识别准确率

表 1　各象限聚类中心点实部的变化

参数	实部一	实部二	实部三	实部四
标准值	−0.708 0	0.700 0	0.714 9	−0.710 4
最大值	−0.702 2	0.700 0	0.716 3	−0.709 9
最小值	−0.708 0	0.694 2	0.710 3	−0.715 5
波动范围/%	±0.82	±0.83	±0.64	±0.72

表 2　各象限聚类中心点虚部的变化

参数	虚部一	虚部二	虚部三	虚部四
标准值	0.698 8	0.699 4	−0.713 2	−0.706 3
最大值	0.698 8	0.699 6	−0.710 1	−0.705 2
最小值	0.694 5	0.695 2	−0.713 5	−0.709 1
波动范围/%	±0.62	±0.60	±0.43	±0.40

从表 1 与表 2 中可知，聚类点的波动范围在 ±0.1%以内，且设备的聚类点一般在小数点后第三位开始变化。通过大量实验发现，设备与设备之间聚类点的差异往往出现在小数点后第二位，说明允许设备的聚类点有较小的变化。通过以上分析可知 SNR 对射频指纹的影响小于设备自身硬件对射频指纹的影响，正是因为这种关系，才可利用聚类点作为射频指纹。

5　结束语

本文首先建立了 IEEE 802.11n OFDM 系统模型，对正交调制器和功率放大器的硬件差异建立了相应的数学模型。选用星座图中聚类中心点作为射频指纹进行研究，对星座图进行适当的拉回处理后，既保留了一定的离散性，又可得到较为稳定的聚类点。将优化后的星座图按 4 类进行 K 均值聚类，避免了聚类错误现象。仿真发现，设备到达自身参考聚类点的欧式距离的和明显小于其他设备，验证了欧式距离的和可用来计算匹配程度的方案。通过对设备 50 组聚类点的训练，得到了设备最终的参考聚类中心点，并以此作为射频指纹。实验结果表明，所提出的二维识别算法可获得较高的识别准确率，还可降低算法的计算复杂度和训练时间。当 SNR 为 20 dB 且设备容量为 10 组时，识别准确率为 91.4%，在 SNR 为 5 dB 时所提出的二维识别算法的识别准确率最高可提升 8%，设备容量为 50 组情况下识别准确率为 77.8%，并且基于星座图提取的 RF 指纹具有唯一性与稳定性等优点。

参考文献：

[1] Wang X L, Zhang Y F, Zhang H X, et al. Identification and authentication for wireless transmission security based on RF-DNA fingerprint[J]. Eurasip J. on Wireless Communications and Networking, 2019, 12(1): 120-131.

[2] Yu J, Hu A, Li G, et al. A robust RF fingerprinting approach using multisampling convolutional neural network[J]. IEEE Internet of Things J., 2019, 6(4): 6786-6799.

[3] 吴皓威，赵俊波，徐浩然，等. 全双工终端的收发 I/Q 不平衡估计与补偿算法[J]. 通信学报，2017，38(1)：141-148.
Wu Haowei, Zhao Junbo, Xu Haoran, et al. Estimation and compensation for transmitter and receiver I/Q imbalance of full-duplex terminals[J]. J. on Communications, 2017, 38(1): 141-148.

[4] 陈　强. 基于差分星座图的射频指纹提取方法研究[D]. 西安：西安电子科技大学，2018.
Chen Qiang. Research on authentication technology based on radio frequency fingerprint[D]. Xi'an: Xidian University, 2018.

[5] 彭林宁，胡爱群，朱长明. 基于星座轨迹图的射频指纹提取方法[J]. 信息安全学报，2015，1(1)：50-58.
Peng Linning, Hu Aiqun, Zhu Changming. Radio fingerprint extraction based on constellation trace figure[J]. J. of Cyber Security, 2015, 1(1): 50-58.

[6] Peng Linning, Hu Aiqun, Jiang Yu, et al. A differential constellation trace figure based device identification method for ZigBee nodes [C]// 2016 8th Inter. Conf. on Wireless Communications & Signal Processing (WCSP), 2016: 1-6.

[7] 袁红林，陆小丹，徐　晨. 基于 B-Spline 神经网络的宽带通信发射机指纹估计[J]. 应用科学学报，2019，37(1)：16-27.
Yuan Honglin, Lu Xiaodan, Xu Chen. Fingerprints based on B-Spline neural network[J]. J. of Appl. Sciences-Electronics and Information Engineering, 2019, 37(1): 16-27.

[8] Wang W, Sun Z, Piao S. Wireless physical-layer identification: Modeling and validation[J]. IEEE Trans. on Information Forensics and Security, 2016, 11(9): 2091-2106.

作者简介：

袁建国(1968－)，男，重庆人，博士，教授，硕士生导师，主要研究方向为电子与通信工程技术，尤其是通信系统中 FEC 编译码技术与 OFDM 技术。