文章编号：2095-4980(2021)04-0596-07

基于功率谱密度的通信辐射源个体识别方法

李靖超[1]，应雨龙[2]

(1.上海电机学院 电子信息学院，上海 201306；2.上海电力大学 能源与机械工程学院，上海 201303)

摘　要：为阻止设备克隆、重放攻击和用户身份假冒等问题的发生，准确识别和认证物联对象，提出一种基于功率谱密度指纹特征与智能分类器的通信辐射源个体识别方法。利用接收机采集 I 路射频基带信号；通过方差轨迹检测截取稳态信号片段，并对稳态信号片段进行数据标准化处理；计算数据标准化处理后的稳态信号片段的功率谱密度得到特征向量，将所述特征向量作为发射机的射频指纹；最后利用智能分类器识别所述射频指纹，完成通信辐射源个体识别。通过对同厂家、同型号、同批次的 8 个无线数传电台 E90-DTU 设备和 100 个 WiFi 网卡设备的实验测试表明，本文所提方法在视距(LOS)场景、视距场景与非视距(NOS)场景的混合场景、低信噪比场景、大数量物联设备场景都具有良好的识别准确率。

关键词：物联网；射频指纹；功率谱密度；灰关联分类器；支持向量机

中图分类号：TN92　　**文献标志码：**A　　**doi：**10.11805/TKYDA2021140

Individual identification method of communication radiation source based on power spectral density

LI Jingchao[1]，YING Yulong[2]

(1.School of Electronic and Information，Shanghai Dianji University，Shanghai 201306，China；
2.School of Energy and Mechanical Engineering，Shanghai University of Electric Power，Shanghai 201303，China)

Abstract：An individual identification method of communication radiation sources based on Power Spectral Density(PSD) fingerprint characteristics and intelligent classifier is proposed in order to prevent the occurrence of problems such as device cloning, replay attacks and user identity impersonation, and to accurately identify and authenticate Internet of Things(IoT) objects. First, the radio frequency baseband signal is collected by receiver, and the in-phase signal is collected. Then the steady-state signal segment is intercepted through variance trajectory detection, and data normalization processing on the steady-state signal segment is performed; the PSD of the steady-state signal segment is calculated after data normalization processing to obtain a feature vector, and the feature vector is used as the radio frequency fingerprint of the transmitter. Finally, an intelligent classifier is adopted to identify the radio frequency fingerprint to complete the individual identification of the communication radiation source. The experimental test to identify eight wireless data transmission radio E90-DTU devices and 100 WiFi network card devices of the same manufacturer, the same type and the same batch shows that the proposed method can obtain good recognition accuracy when applied in Line-Of-Sight(LOS) scenarios, mixed scenes of LOS and Non-line-Of-Sight(NOS) scenarios, low signal-to-noise ratio scenes, and scenarios with a large number of IoT devices, etc.

Keywords：Internet of Things；RF fingerprint；Power Spectral Density；gray relation classifier；Support Vector Machine

信息安全是构建可靠、稳健的物联网(IoT)的关键。由于无线电传输的开放性，无线通信网络带来的信息安全问题不断涌现，尤其是用户身份假冒、重放攻击和设备克隆等问题。可信的识别认证对于保障物联网设备信

收稿日期：2021-04-06；**修回日期：**2021-05-19
基金项目：国家自然科学基金资助项目(62076160；51806135；61603239)；上海市自然科学基金资助项目(21ZR1424700)

息安全至关重要。每个物联网设备都应具有自己的身份，以形成一个可信的物联生态网络系统。为阻止设备克隆、重放攻击和用户身份假冒等问题的发生，如何准确地识别和认证物联对象是物联网面临的首要问题，也是物联网应用的基础[1]。

传统的认证机制在应用层利用密码算法生成第三方难以仿冒的数值结果来实现，但这种应用层认证机制通常存在密钥泄露和协议安全漏洞等风险。现今，物联网感知层的终端设备具有智能化、多样化、复杂化等特点，传统的认证机制已难以满足物联网的信息安全需求[2]。物理层认证是保障无线通信安全的核心技术之一，相比于应用层认证机制，它能够有效抵御模仿攻击，具有兼容性好，复杂度低，认证速度快，不需要考虑各种协议执行的特点；其基本原理是联合传输信号与收发信道的空时特异性，对通信双方的物理特性进行认证，从而在物理层实现身份认证与识别。目前丰富的物理层资源还未得到充分利用，对物理层认证方法的研究尚处于初级阶段，仍有较大的研究空间。

1　射频指纹识别技术

射频指纹识别是基于设备物理层硬件的非密码认证方法，无需消耗额外的计算资源，也无需嵌入额外的硬件，是构建低成本、更简洁、更安全的识别认证系统的非常有潜力的技术[3]。基于射频信号细微特征的设备识别，最早起源于特定辐射源识别(Specific Emitter Identification，SEI)，即将辐射源独特的电磁特性与辐射源个体关联起来的能力[4]。

如图 1 所示，现有的射频指纹识别技术利用物理层资源的不同，可分为基于信道的指纹识别技术[5-6]和基于传输信号的指纹识别技术。基于信道特征的指纹识别技术旨在利用设备的唯一位置信息来作为不同用户在不同场景下的身份检测指标，通常用于物联网设备的室内定位。基于传输信号的射频指纹识别技术可分为基于瞬态信号[7-8]和基于稳态信号的射频指纹识别技术[9-10]。瞬态信号不包含任何数据信息，只体现发射机的硬件特征，具有独立性，射频指纹最初就是从瞬态信号中提取的。但由于瞬态信号的持续时间较短，对突变点检测与定位较为敏感，难以捕获，限制了其在实际环境中的应用。稳态信号是发射机处于稳定工作状态时的信号，其持续时间长，更容易获得，通过廉价的接收机即可完成，但稳态信号中存在的射频指纹不容易提取。随着射频指纹识别技术的发展，学者们逐渐从利用瞬态信号到利用稳态信号的前导序列，再到利用稳态信号的传输数据段，逐步减少了对待识别信号检测和提取的要求。此外，基于特征提取方法的不同，基于传输信号的射频指纹识别技术还可分为基于波形域[11]和基于调制域的射频指纹识别方法[12]。现今，在通信信号中正交调制获得了广泛应用，调制域方法通过调制方案强制赋予的信号结构，以 I/Q 基带信号为处理单元，令发射机的特定物理属性更加容易识别，其调制域特征包括 I/Q 偏移、调制偏移、载频偏移、星座轨迹图[13]、差分星座轨迹图[14]、差分等势星球图[15]等特征。在识别认证阶段，根据分类器的不同，可分为基于传统机器学习的指纹识别技术[16]和基于深度学习的指纹识别技术[17]。深度学习方法给射频指纹特征提取与识别提供了新的思路，但由于其“黑箱”的特点，最好与特征工程方法相结合进行研究。

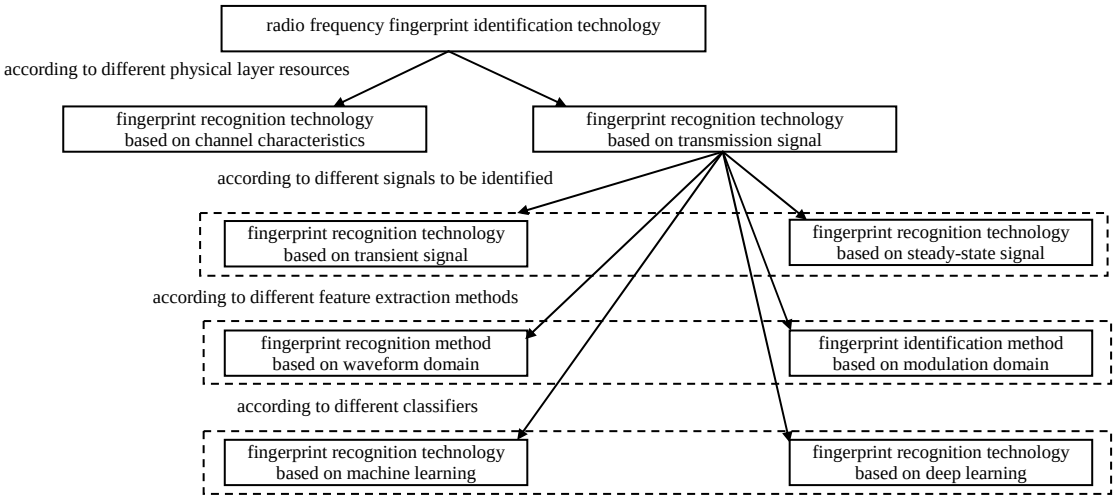


Fig.1 Characteristics and types of radio frequency fingerprint identification technology

图 1 射频指纹识别技术的特点与种类

2 基于功率谱密度的射频指纹识别

从目前射频指纹识别的研究现状看，提取具有独特原生属性的射频指纹仍是一件极具挑战性的任务。提取的射频指纹仍受大量因素的制约，在射频指纹产生机理、特征提取和特征选择以及在射频指纹的鲁棒性和抗信道环境干扰等方面，还有大量问题有待研究。

为追求更高的数据速率和频谱效率，通信系统普遍采用线性调制方式，如 QPSK 和 16QAM。多载波系统中峰均比大，信号包络变化，系统应保持线性放大。非线性放大会导致带内信号失真，系统性能下降，导致带外互调分量，发射机载频的邻近信道产生干扰。放大器的非线性主要体现在信号的功率谱上，因此从能量域出发，使用功率谱估计方法对其进行特征提取。基于功率谱密度射频指纹特征的识别过程如图 2 所示。

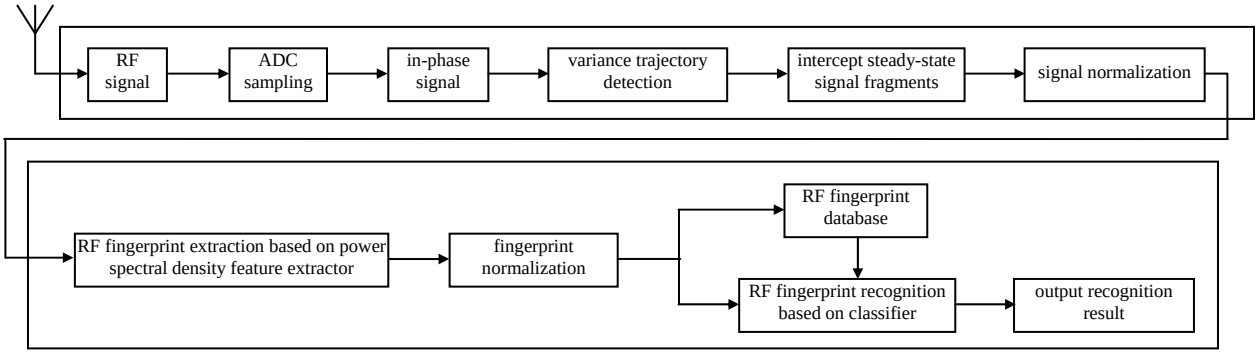


Fig.2 Individual identification method of communication radiation source based on power spectral density fingerprint feature and intelligent classifier

图 2 基于功率谱密度指纹特征与智能分类器的通信辐射源个体识别方法

1) 利用接收机采集 I/Q 两路射频基带信号；

2) 选取 I 路信号(根据大量测试结果，选取 I 路信号比选取 Q 路信号的效果更优)进行方差轨迹检测，截取稳态信号片段，对稳态信号片段进行数据标准化处理。数据标准化处理是指对截取的稳态信号数据或功率谱密度特征向量进行标准化处理，数据标准化处理包括中心化—压缩处理，如式(1)所示：

$$\boldsymbol{Y}=\boldsymbol{X}-\mathrm{mean}(\boldsymbol{X})/\max(\boldsymbol{X}) \tag{1}$$

式中：$\boldsymbol{X}$ 为截取的稳态信号数据或功率谱密度特征向量；$\boldsymbol{Y}$ 为标准化处理后的输出向量。

3) 计算数据标准化处理后的稳态信号片段的功率谱密度，得到特征向量，将得到的特征向量作为发射机的射频指纹，并生成射频指纹库；

4) 利用智能分类器识别射频基因库的射频指纹特征，输出识别结果，完成通信辐射源个体识别。

智能分类器包括支持向量机和灰关联分类器等，本文以灰关联分类器进行分类识别为例：

定义从待识别射频信号提取的表征通信辐射源个体特征的功率谱密度特征向量包括：

$$\boldsymbol{B}_1=\begin{bmatrix} b_1(1)\\ b_1(2)\\ \vdots\\ b_1(K)\end{bmatrix},\boldsymbol{B}_2=\begin{bmatrix} b_2(1)\\ b_2(2)\\ \vdots\\ b_2(K)\end{bmatrix},\cdots,\boldsymbol{B}_i=\begin{bmatrix} b_i(1)\\ b_i(2)\\ \vdots\\ b_i(K)\end{bmatrix},\cdots \tag{2}$$

式中 $\boldsymbol{B}_i(i=1,2,\cdots)$表示某一待识别的通信辐射源个体特征。

定义已建立的通信辐射源个体特征与个体标签之间的射频指纹库包括：

$$\boldsymbol{C}_1=\begin{bmatrix} c_1(1)\\ c_1(2)\\ \vdots\\ c_1(K)\end{bmatrix},\boldsymbol{C}_2=\begin{bmatrix} c_2(1)\\ c_2(2)\\ \vdots\\ c_2(K)\end{bmatrix},\cdots,\boldsymbol{C}_j=\begin{bmatrix} c_j(1)\\ c_j(2)\\ \vdots\\ c_j(K)\end{bmatrix},\cdots,\boldsymbol{C}_m=\begin{bmatrix} c_m(1)\\ c_m(2)\\ \vdots\\ c_m(K)\end{bmatrix} \tag{3}$$

式中：$\boldsymbol{C}_j(j=1,2,\cdots)$表示已知合法的通信辐射源个体标签；$c_j(j=1,2,\cdots)$表示某一特征参数。

定义：

$$\xi\left[b_i(k),c_j(k)\right]=\frac{\min\limits_j\min\limits_k\left|b_i(k)-c_j(k)\right|+\rho\cdot\max\limits_j\max\limits_k\left|b_1(k)-c_j(k)\right|}{\left|b_1(k)-c_j(k)\right|+\rho\cdot\max\limits_j\max\limits_k\left|b_1(k)-c_j(k)\right|} \tag{4}$$

$$\xi(\boldsymbol{B}_i,\boldsymbol{C}_j)=\frac{1}{K}\sum_{k=1}^{K}\xi\left[b_i(k),c_j(k)\right] \tag{5}$$

式中：ρ 表示分辨系数，$\rho\in(0,1)$，通常取值 0.5；$\xi\left[b_i(k),c_j(k)\right]$表示 $\boldsymbol{B}_i$ 与 $\boldsymbol{C}_j$ 之间第 k 个特征参数的关联系数；$\xi(\boldsymbol{B}_i,\boldsymbol{C}_j)$ 表示 $\boldsymbol{B}_i$ 与 $\boldsymbol{C}_j$ 之间的灰色关联度。

当求得 $\boldsymbol{B}_i$ 与已知射频指纹库中的每一个 $\boldsymbol{C}_j(j=1,2,\cdots,m)$的关联度 $\xi(\boldsymbol{B}_i,\boldsymbol{C}_j)$ $(j=1,2,\cdots,m)$后，为了识别 $\boldsymbol{B}_i$ 所属的通信辐射源个体是否为合法接入无线通信设备，加入如下判断准则：

$$test=\frac{\text{最大关联度}-\dfrac{1}{m}}{\dfrac{1}{m}\displaystyle\sum_{j=1}^{m}\xi(\boldsymbol{B}_i,\boldsymbol{C}_j)} \tag{6}$$

若 $test$<某一阈值(定义阈值为 0.004 2)，则 $\boldsymbol{B}_i$ 所属的通信辐射源个体为非法接入无线通信设备；否则，$\boldsymbol{B}_i$ 所属的通信辐射源个体为合法接入无线通信设备，就可以将 $\boldsymbol{B}_i$ 分类至射频指纹库中最大关联度所属的通信辐射源个体标签。

3　应用与分析

3.1 案例 1

以识别同厂家、同型号、同批次的 8 个 EBYTE 生产的无线数传电台 E90-DTU 设备(图 3)为例，基带信号采集设备：Signal Hound 公司生产的 SM200B 实时频谱分析仪，如图 4 所示。

Fig.3 Wireless data transmission radio station E90-DTU produced by EBYTE
图 3 EBYTE 生产的无线数传电台 E90-DTU

Fig.4 SM200B real-time spectrum analyzer produced by Signal Hound
图 4 Signal Hound 公司生产的 SM200B 实时频谱分析仪

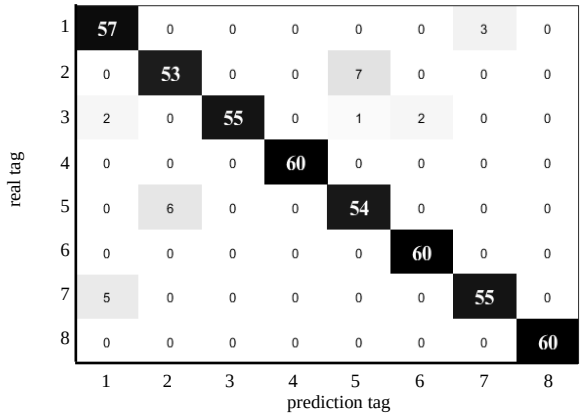
采集环境：视距(LOS)场景、视距(LOS)场景+非视距(NOS)场景的混合场景、变化信噪比场景。采集 8 个 EBYTE 生产的无线数传电台 E90-DTU 信号，信号采集频点为 433 MHz，经过方差轨迹检测截取的稳态信号片段长度为 15 000 点。其中，功率谱密度算法中，设置快速傅里叶变换点数为 2 048，降采样率为 2(根据大量测试结果，当采样频率为 40 MHz 时，降采样率为 2 时识别效果最佳)。

1) LOS 场景

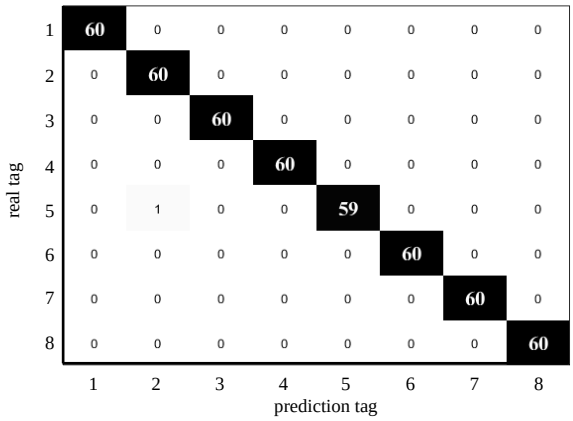
每个设备采集 200 个样本(其中随机选取 140 个样本作为训练样本，剩余 60 个样本作为测试样本)，得到的识别结果如图 5 所示。从图 5 可知，在 20 dB 信噪比下，本文所提方法基于灰关联分类器的准确识别率为 94.58%；基于支持向量机分类器的准确识别率为 99.79%。作为对比，本文测试了基于熵特征[18]、Holder 系数特征[9]与支持向量机分类器的识别效果，得到的准确识别率仅为 19.17%和 12.92%。

2) LOS+NOS 的混合场景

采集 8 个 EBYTE 生产的无线数传电台 E90-DTU 信号，每个设备在 LOS 下采集 200 个样本，在 NOS 下采集 50 个样本，共采集 250 个样本。随机选取 200 个样本作为训练样本，剩余 50 个样本作为测试样本，得到的识别结果如图 6 所示。由图 6 可知，在 20 dB 信噪比下，本文所提方法基于灰关联分类器得到的准确识别率为 93.50%；基于支持向量机分类器的准确识别率为 98.75%。

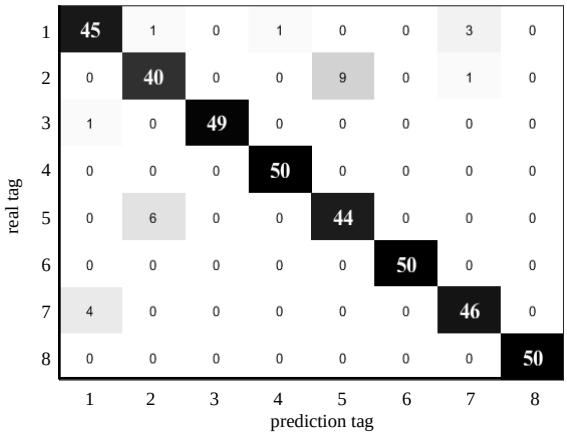


(a) confusion matrix of recognition results based on gray relation classifier under 20 dB signal−to−noise ratio

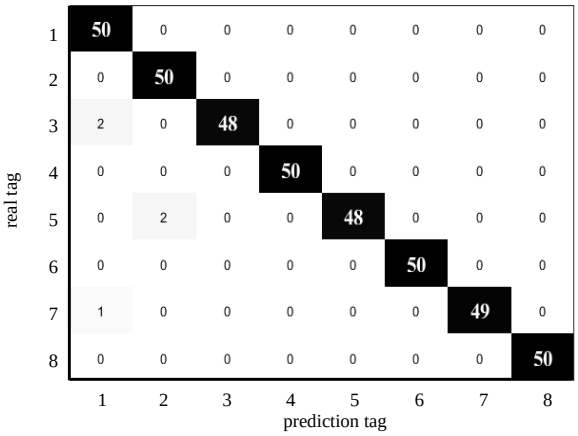


(b) confusion matrix of recognition results based on support vector machine classifier under 20 dB signal−to−noise ratio

Fig.5 Confusion matrix of recognition results in LOS scene
图 5 在 LOS 场景下识别结果混肴矩阵



(a) confusion matrix of recognition results based on gray relation classifier under 20 dB signal−to−noise ratio



(b) confusion matrix of recognition results based on support vector machine classifier under 20 dB signal−to−noise ratio

Fig.6 Confusion matrix of recognition results in LOS scene and NOS scene
图 6 在 LOS 场景与 NOS 场景的混合场景下识别结果混肴矩阵

3) 变化信噪比场景

采集 8 个无线数传电台 E90-DTU 设备，每个设备在 LOS 下采集 200 个样本，在 NOS 下采集 50 个样本，即每个设备采集 250 个样本，其中随机选取 200 个样本作为训练样本，剩余 50 个样本作为测试样本，得到不同信噪比下的识别结果，如图 7 所示。由图 7 可知，在 5 dB 信噪比下，本文所提方法基于灰关联分类器仍得到 89.75%识别准确率；基于支持向量机分类器仍得到 96.25%识别准确率。上述 3 个实施案例平均每个测试样本的识别计算耗时不超过 0.034 8 s(基于灰关联分类器)和 $2.055\ 2\times10^{-4}$ s(基于支持向量机分类器)，说明本文所提方法在保证识别计算实时性的同时，具有优异的识别准确率。

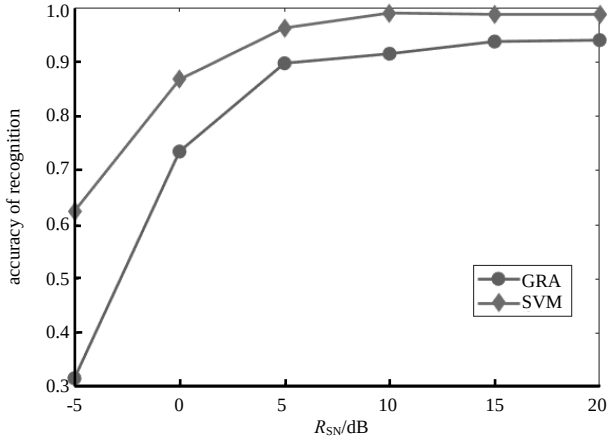
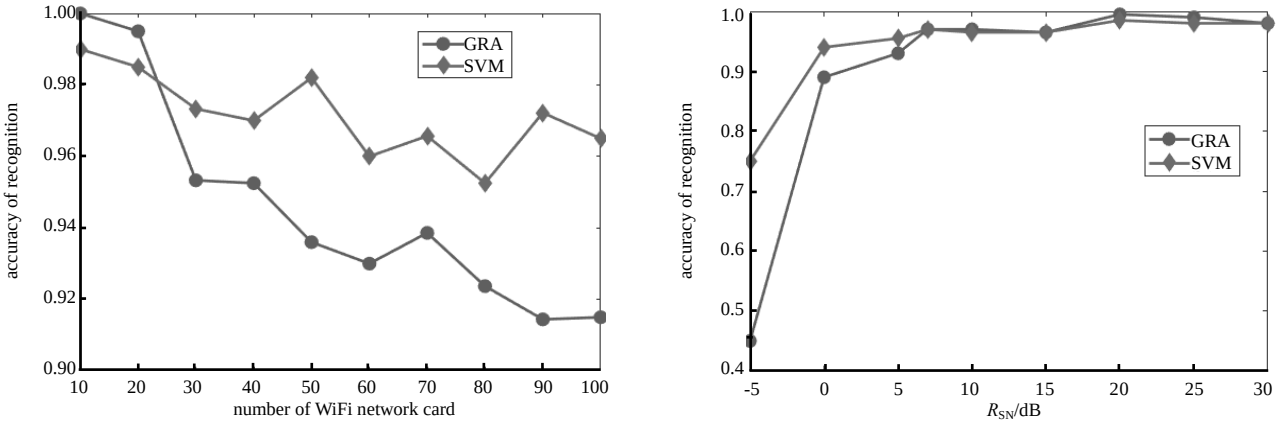


Fig.7 Recognition results in changing signal−to−noise ratio scenarios
图 7 在变化信噪比场景下识别结果

3.2 案例 2

为准确地识别和认证物联对象，阻止用户身份假冒和设备克隆等问题的发生，以识别同厂家、同型号、同批次的 100 个 WiFi 网卡设备为例，测试过程如下：

基带信号采集设备为 FSW26 型频谱仪，采集环境为实验室室内场景。共采 100 个 WiFi 网卡设备，每个设备采集 50 个样本，信号采样频率为 40 MHz，经过方差轨迹检测截取的稳态信号片段长度为 15 000 点。对于每个无线设备，训练样本个数为 40，测试样本个数为 10，得到的识别结果如图 8 所示。其中，功率谱密度算法中，设置 FFT 点数为 2 048，降采样率为 2(根据大量测试结果，当采样频率为 40 MHz，降采样率为 2 时识别效果最佳)。



(a) recognition results with different number of WiFi network card devices under 20 dB signal−to−noise ratio

(b) recognition results of 20 WiFi network card devices in changing signal−to−noise ratio scenarios

Fig.8 Recognition results with different number of WiFi network card devices and changing signal-to-noise ratio scenarios

图 8 在不同 WiFi 网卡设备数目和变化信噪比场景下的识别结果

如图 8(a)所示，在 20 dB 的信噪比下，随着 WiFi 网卡设备数目增多，本文所提方法的识别准确率都有一定程度的降低，但基于支持向量机分类器的识别准确率降低幅度较小，当 WiFi 网卡设备数目增加到 100 个时，识别准确率仍大于 96%，说明了本文所提方法适用于处理物联网感知层终端设备数量庞大的场景。如图 8(b)所示，在变化信噪比场景下，20 个 WiFi 网卡设备数目的识别准确率保持了良好的稳定性，在 5 dB 的信噪比下，本文所提方法的识别准确率仍大于 90%，直到低于 0 dB 的信噪比时，本文所提方法的识别准确率才出现明显的降幅，说明了本文所提方法提取的射频指纹特征具有优异的鲁棒性和抗信道环境干扰能力。

4　结论

为准确地识别和认证物联对象，阻止用户身份假冒和设备克隆等问题的发生，提出了一种基于功率谱密度指纹特征与智能分类器的通信辐射源个体识别方法。通过对识别同厂家、同型号、同批次的 8 个无线数传电台 E90-DTU 设备和 100 个 WiFi 网卡设备的实验测试，可以得到如下结论：

1) 在识别同厂家、同型号、同批次的 8 个无线数传电台 E90-DTU 设备的实验测试中，在 LOS+NOS 的混合场景下，在 5 dB 信噪比下，本文所提方法基于支持向量机分类器仍得到 96.25%识别准确率。

2) 平均每个测试样本的识别计算耗时不超过 0.0348 s(基于灰关联分类器)和 0.000 205 52 s(基于支持向量机分类器)，说明了本文所提方法既能有效保证识别准确性，又能有效保证计算实时性。

3) 在识别同厂家、同型号、同批次的 100 个 WiFi 网卡设备的实验测试中，在 20 dB 的信噪比下，本文所提方法基于支持向量机分类器的识别准确率仍大于 96%，说明了本文所提方法适用于处理物联网感知层终端设备数量庞大的场景。

4) 在变化信噪比场景下，20 个 WiFi 网卡设备数目的识别准确率在 5 dB 的信噪比下仍大于 90%，说明了本文所提方法提取的射频指纹特征具有优异的鲁棒性和抗信道环境干扰能力。

参考文献：

[1] LI Jingchao,YING Yulong,JI Chunlei. Study on radio frequency signal gene characteristics from the perspective of fractal theory[J]. IEEE Access, 2019(7):124268–124282.

[2] CHEN Xiang,LI Jingchao,HAN Hui,et al. Improving the signal subtle feature extraction performance based on dual improved fractal box dimension eigenvectors[J]. Royal Society Open Science, 2018,5(5):180087.

[3] ZHENG Tianhang,SUN Zhi,REN Kui. FID:function modeling-based data-independent and channel-robust physical-layer identification[C]// IEEE Conference on Computer Communications. Paris,France:IEEE, 2019:199–207.
[4] LI Jingchao,LI Yibing,SHOUHEI Kidera,et al. A robust signal recognition method for communication system under time-varying SNR environment[J]. IEICE Transactions on Information and Systems, 2013,E96–D(12):2814–2819.
[5] SHU Yuanchao,HUANG Yinghua,ZHANG Jiaqi,et al. Gradient-based fingerprinting for indoor localization and tracking[J]. IEEE Transactions on Industrial Electronics, 2016,63(4):2424–2433.
[6] LIN Kai,CHEN Min,DENG Jing,et al. Enhanced fingerprinting and trajectory prediction for IoT localization in smart buildings[J]. IEEE Transactions on Automation Science and Engineering, 2016,13(3):1294–1307.
[7] LI Jingchao,BI Dongyuan,YING Yulong,et al. An improved algorithm for extracting subtle features of radiation source individual signals[J]. Electronics, 2019,8(2):1–11.
[8] HAN Hui,LI Jingchao,CHEN Xiang. The individual identification method of wireless device based on a robust dimensionality reduction model of hybrid feature information[J]. Mobile Networks & Applications, 2018,23(4):709–716.
[9] LI Jingchao. A novel recognition algorithm based on holder coefficient theory and interval gray relation classifier[J]. KSII Transactions on Internet and Information Systems, 2015,9(11):4573–4584.
[10] LI Jingchao. A new robust signal recognition approach based on holder cloud features under varying SNR environment[J]. KSII Transactions on Internet and Information Systems, 2015,9(12):4934–4949.
[11] YUAN Yingjun,HUANG Zhitao,WU Hao,et al. Specific emitter identification based on Hilbert–Huang transform-based time–frequency–energy distribution features[J]. IET Communications, 2014,8(13):2404–2412.
[12] WANG Shenhua,JIANG Hongliang,FANG Xiaofang,et al. Radio frequency fingerprint identification based on deep complex residual network[J]. IEEE Access, 2020(8):204417–204424.
[13] PENG L,ZHANG J,LIU M,et al. Deep learning based RF fingerprint identification using differential constellation trace figure[J]. IEEE Transactions on Vehicular Technology, 2020,69(1):1091–1095.
[14] JIANG Yu,PENG Linning,HU Aiqun,et al. Physical layer identification of LoRa devices using constellation trace figure[J]. EURASIP Journal on Wireless Communications and Networking, 2019(1):223.
[15] YING Yulong,LI Jingchao,JI Chunlei,et al. Differential contour stellar based radio frequency fingerprint identification for Internet of Things[J]. IEEE Access, 2021(9):53745–53753.
[16] DING L,WANG S,WANG F,et al. Specific emitter identification via Convolutional Neural Networks[J]. IEEE Communications Letters, 2018,22(12):2591–2594.
[17] TU Y,LIN Y,WANG J,et al. Semi-supervised learning with Generative Adversarial Networks on digital modulation classification[J]. Computers Materials & Continua, 2018,55(2):243–254.
[18] LI Jingchao,YING Yulong,JI Chunlei. Study on gas turbine gas-path fault diagnosis method based on quadratic entropy feature extraction[J]. IEEE Access, 2019(7):89118–89127.

作者简介：

李靖超(1986–)，女，博士，副教授/硕导，主要研究方向为信号特征提取与模式识别.email:lijc@sdju.edu.cn.

应雨龙(1987–)，男，博士，副教授/硕导，主要研究方向为信号特征提取与识别、机器学习与深度学习算法、综合能源系统规划、物联网物理层认证等.