基于星座轨迹图的射频指纹提取方法

彭林宁[1], 胡爱群[1], 朱长明[2], 姜 禹[1]

[1] 东南大学信息科学与工程学院 南京 中国 210096
[2] 中国运载火箭技术研究院研究发展中心 北京 中国 100076

摘要 无线设备的接入安全是当今无线网络安全的一个严重挑战。基于射频指纹的物理层安全技术是解决无线设备接入安全的一个有效途径。在不同于已有的基于瞬态响应和稳态响应的射频指纹特征提取方法上，本文提出了一种使用星座轨迹图(CTF, Constellation Trace Figure)的射频指纹提取方法。在获得的星座轨迹图上，进一步通过 K 均值聚类提取射频指纹特征并进行设备身份识别。在理论阐述的基础上，本文通过在实际无线通信系统中提取射频指纹特征并进行无线设备身份识别，验证了提出方法的可靠性与实用性。使用基于星座轨迹图的射频指纹特征提取方法不需要获得设备发送信号的先验信息就可以快速获得无线设备唯一的射频指纹特征，可以被用于物理层安全以及无线接入设备的身份识别及认证。

关键词 物理层安全；接入安全；射频指纹；设备特征；星座轨迹图；软件无线电；K 均值；模式识别
中图法分类号 TP309.1

Radio Fingerprint Extraction based on Constellation Trace Figure

PENG Linning[1], HU Aiqun[1], ZHU Changming[2], JIANG Yu[1]

[1] Institute of Information Science and Engineering, Southeast University, Nanjing 210096, China
[2] Research Center of China Academy of Launch Vehicle Technology, Beijing 100076, China

Abstract Wireless device accessing security is a great challenge in wireless communication networks. Radio fingerprint based physical layer security technique is an effective approach to solve this problem. In this paper, a novel radio fingerprint extraction based on constellation trace figure (CTF) method is proposed, which distinguishes from classical transient based and modulation based radio fingerprint extraction methods. Furthermore, a K-mean clustering algorithms is adopted for wireless device identification from CTF. From theoretical analysis, a software defined radio experimental system for wireless device identification is built. Experimental verifications show that the proposed CTF based method can successfully extract radio fingerprint without prior information, which could be a suitable solution for wireless device identification and authorization in physical layer security.

Key words physical layer security; accessing security; radio fingerprint; device features; constellation trace figure; software defined radio; K-mean; pattern recognition

1 引言

在当今的通信系统中，对接入设备的身份进行认证是保障通信系统安全的重要步骤。在传统的无线通信系统中，设备接入时的认证主要是依靠存储在设备里的身份认证信息或输入的身份验证指令。例如在移动通信系统里身份认证使用的全球用户识别卡(Universal Subscriber Identity Module, USIM)[1]，蓝牙通信系统的身份认证时双方输入的 PIN 码[2]。

近些年来，越来越多的研究表明，可以通过无线通信系统发射的电磁波，提取其设备的射频特征[3,4]。由于射频设备电子元器件的差异，导致了其发射出的电磁波包含有设备独特的射频特征。如图 1 所示的是一个简要的无线通信系统射频前端框图。由于无线通信系统射频前端的放大器、混频器、滤波器、功率放大器和天线的射频响应及参数都不尽相同，导致最终发射的射频信号不可避免的寄生了发射机系统独特的射频特征，从而可以成为进行设备身份认证的参数，也被称为“射频指纹”。文献[5]的研究表明，射频指纹特征在不同的无线设备发射机中是唯一的。此外，由于射频指纹是设备本身所具有的物理特征，基于射频指纹的特征提取建立在通信

通讯作者：彭林宁，博士，副研究院, E-mail: pengln@seu.edu.cn。本课题得到江苏省“六大人才高峰”项目资助；国家自然科学基金项目(61571110)资助; CALT 基金项目资助。收稿日期：2015-11-17；修改日期：2015-12-10；定稿日期：2016-01-03

系统的物理层上。在物理层上的射频指纹信息不易受到修改，可以很好的从通信系统的底层保护系统的安全。由于射频指纹这些优异的特性，在世界范围内的众多研究机构开始了对射频指纹特征提取的研究[3-8]。现有的射频指纹特征提取方法主要分为两类，一类是基于瞬态响应的射频指纹提取方法，一类是基于稳态响应的射频指纹提取方法[3]。这两类方法都可以获得唯一的射频指纹信息，也是现在普遍使用的方法。

在本篇文章中，我们将简要的介绍射频指纹特征提取的方法并评价其在实际系统中的可靠性和实用性。不同于现有的射频指纹特征提取方法，在本文中我们提出了一种基于星座轨迹图的射频指纹特征提取方法。该方法可以很好的获得射频指纹特征并可以被用于射频设备的身份识别及认证。最后，我们通过实际测量结果展现了使用星座轨迹图进行射频指纹特征提取的方法，并针对实验结果给出了进一步可以研究的工作。

本文的结构如下：第2章将介绍基于瞬态响应的射频指纹提取方法；第3章将介绍基于稳态响应的射频指纹提取方法；第4章将简要的介绍星座轨迹图的概念；第5章将介绍星座轨迹图的获取方法；第6章将分析星座轨迹图特征，给出基于可视化处理后的特征提取方法；第7章将展现通过基于星座轨迹图的射频指纹特征提取方法对实际的无线设备进行身份识别，通过加入人工噪声的方式验证系统在实际环境下的可靠性与实用性；第8章将讨论基于星座轨迹图的射频指纹特征提取可能受到的影响因素；最后，在第9章对全文进行总结与展望。

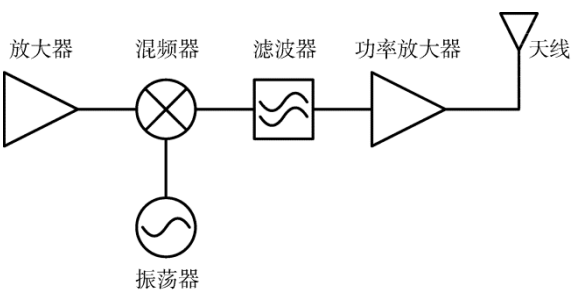

图 1　无线通信系统射频前端的框图

2　基于瞬态响应的射频指纹提取方法

基于射频设备瞬态响应的射频指纹提取方法的原理主要是当无线通信设备在发送数据时，其打开和关闭的瞬时状态下发射出的电磁波幅度起伏的包络以及相位信息各不相同。基于其信号包络的起伏及相位信息可以获得设备瞬态响应的射频指纹。此外，基于瞬态信号的频谱特征也可以提取出射频指纹信息并进行识别。在现有的论文中，针对不同的调制信号都有采取基于瞬态响应的射频指纹特征提取研究。例如文献[9]的研究是基于 FM 调频信号提取其瞬态响应特征。文献[10,11]的研究是针对 IEEE 802.11 标准的设备提取其瞬态响应特征。文献[11,12]的研究是针对蓝牙及 IEEE 802.15.4 标准的设备提取其瞬态响应特征。文献[13]的研究是针对 RFID 信号的瞬态响应提取其射频指纹特征。

值得注意的是，基于瞬态响应的射频指纹特征提取大多是直接在射频端采集设备发射出的信号。因此该射频指纹特征提取方法需要能够工作在射频端采集信号的较为精密的仪器设备。此外，由于采集无线设备的瞬态响应特征需要捕获无线信号在打开和关闭瞬间的信号起伏变化，这样的要求也加大了采集信号时的难度。当接收信号的信噪比不高时，基于信号瞬态响应的采集将会变得非常困难。

3　基于稳态响应的射频指纹提取方法

在获取无线设备射频指纹的方法中，还可以基于获取的无线设备基带的稳态响应进行特征提取。无线设备的基带稳态响应主要有载波频率偏移、同步信号相关值、基带 I/Q 两路信号偏移、解调信号的幅度和相位误差等。如文献[4]估计了 IEEE802.11 导频信号中的正交相移键控(Quadrature Phase Shift Keying, QPSK)信号的基带特征并进行了稳态射频指纹特征的提取。文献[14]估计了 IEEE 802.15.4(Zigbee)中的 QPSK 信号的基带特征并提取其相关的稳态射频指纹特征。文献[7]测量了不同位置的 4G LTE 基站并进行了稳态射频指纹特征的提取。

基于稳态响应的射频指纹提取方法一般需要对接收的信号进行准确的频率同步。估计出载波频率偏移后对接收的信号进行补偿。再基于补偿后的信号估计出其他稳态特征。例如文献[4]提取的稳态射频指纹特征就需要先估计出载波频率偏移才可以估计出基带的 I/Q 两路信号偏移以及解调信号的幅度和相位误差。然而，由于文献[4]提出的射频指纹提取方法中的解调信号的幅度和相位误差是针对 QPSK 信号进行的，当处理其他一些调制如最小频移键控(Minimum Shift Keying, MSK)调制信号时，接收机很难获得清晰散布的星座图，从而难以获得幅度和相位误差信息。此外，文献[4]中所采用的同步信号相关值和解调信号的幅度和相位误差特征还会受到发射机和接收机传播信道的影响，在有些情况下难以成为稳定的特征。

值得注意的是，基于稳态响应的射频指纹提取方法可以在基带完成对无线设备射频指纹特征的获取，因此比在射频端获取瞬态响应的射频指纹特征提取方法要更为实用。近些年来的研究表明，基于稳态响应的射频指纹特征提取可以使用较为低廉的软件无线电接收设备在基带采集无线信号来实现[15,16]。例如文献[15]的实验系统使用了通用软件无线电外设(Universal Software Radio Peripheral, USRP)平台就可以获得无线设备的射频指纹特征。

从现有的研究进展来看，现阶段针对射频指纹特征研究的主要技术为上述介绍的两种方法。对于这两种方法的一个总结框图如图 2 所示。然而，在射频指纹的研究中，为了使系统能够准确的对无线设备进行身份识别，需要研究如何获得更多维度的射频指纹特征。下面，我们将介绍一种新式的信号射频指纹特征获取方法，即基于星座轨迹图的射频指纹特征提取。

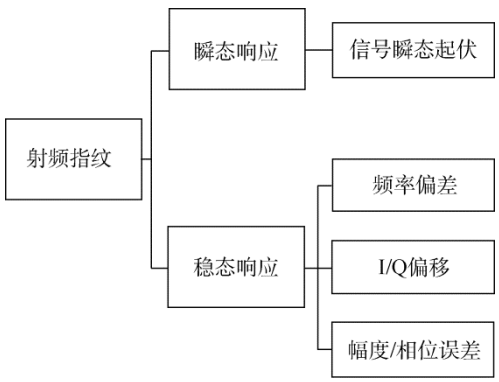

图 2　现有的射频指纹提取方法总结

4　星座轨迹图

在数字通信中，当接收机经过预处理得到了和发射机同频率同相位的基带信号后，再通过时间同步获得用于判决的采样点。将上述处理后的数字信号在复平面上绘制出来即为星座图。星座图可以直观的表示信号之间的关系，从而为研究数字通信系统接收机的性能以及 I/Q 两路信号的关系提供了一种便捷的途径。如图 3 所示的为二元相移键控(Binary Phase Shift Keying, BPSK)和正交相移键控 QPSK 信号的星座图。

然而，在数字通信中，获取星座图是为了研究解调信号的性能，因此一般绘制用于判决的采样点。为了能够更好的研究接收信号所包含的射频指纹特征，可以在接收端以高于发射端采样率的方式获得过采样的信号。将过采样的信号直接绘制在复平面上，就可以得到信号的星座轨迹图(Constellation Trace Figure, CTF)。

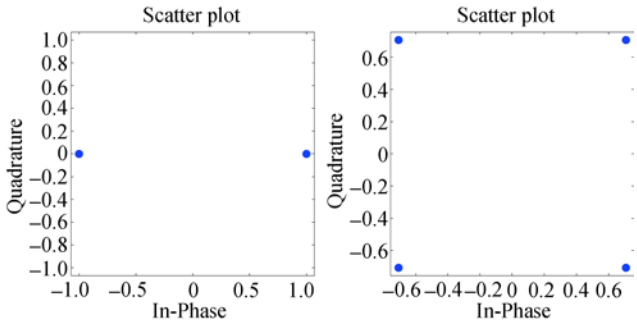

图 3　BPSK 和 QPSK 信号的星座图

由于是采用了过采样，不仅是原先星座图中每一个判决的采样点，甚至是判决采样点之间的变化过程都可以在星座轨迹图上表现出来。星座轨迹图是一种可以度量发射信号本身以及其信号变化规律的手段。由于发射机的放大器非线性响应、滤波器的响应以及其他的线性和非线性干扰因素都会在星座轨迹图的变化轨迹中体现出来。星座轨迹图可以更全面的衡量接收信号的特征。

在获得星座轨迹图的过程中，有一点值得注意的是，由于接收机和发射机的载频会有一定的频率偏差。如果直接将过采样的信号绘制在复平面上，会因为频偏而使得绘制的信号产生旋转。具体的过程如下:

首先，发射机发射的信号如公式(1)所示:

$$S(t) = X(t)e^{-j2\pi f_{c_{Tx}}t} \tag{1}$$

其中，$X(t)$是发射机基带的信号，$f_{c_{Tx}}$是发射机的载波频率，$S(t)$是发射的信号。假设发射机的射频电路是理想的，信道也是理想的，接收机接收到的信号$R(t) = S(t)$。接收机将信号进行下变频获得基带信号:

$$Y(t) = R(t)e^{j2\pi f_{c_{Rx}}t+\varphi} \tag{2}$$

其中，$f_{c_{Rx}}$为接收机的载波频率，φ为接收机接收信号时的相位误差。当$f_{c_{Rx}} \neq f_{c_{Tx}}$时，接收机下变频获得的基带信号即为:

$$Y(t) = X(t)e^{j2\pi\theta t+\varphi} \tag{3}$$

其中$\theta = f_{c_{Rx}} - f_{c_{Tx}}$

如公式(3)所示，由于解调的信号含有残余的频率偏差θ，导致基带信号的每一个采样点都有一个相位旋转因子$e^{j2\pi\theta t}$。该相位旋转因子随着采样点位置t的不同而变化。因此会造成星座轨迹图整体的旋转。

在大部分相干解调的通信系统里，将频率偏差及相位偏差进行估计可以得到估计的频率偏差$\tilde{\theta}$和相位偏差$\tilde{\varphi}$。接收机利用估计的结果对接收的信号进行频率偏差和相位偏差补偿，从而获得稳定的星座

图。而在本文基于星座轨迹图的射频指纹提取方法中，由于接收机的目的不是正确的解调出每一个接收的信号符号。因此可以将接收的信号按照一定的间隔进行差分处理后得到稳定的星座轨迹图。进行差分处理的方法如公式(4)所示:

$$D(t) = Y(t) \cdot Y^*(t+n)$$
$$= X(t)e^{j2\pi\theta t+\varphi} \cdot X(t+n)e^{-j2\pi\theta(t+n)-\varphi}$$
$$= X(t) \cdot X(t+n)e^{-j2\pi\theta n} \quad (4)$$

其中，Y^*为取共轭值，n为差分的间隔。可以看到，在进行了公式(4)所示的差分处理后，获得的差分处理后的信号$D(t)$虽然还是含有一个相位旋转因子$e^{-j2\pi\theta n}$，但是该相位旋转因子是一个恒定的数值，不会随着采样点位置的变化而改变。因此进过差分处理后，即使不对接收机的载波频率偏差和相位偏差进行估计和补偿，也可以获得稳定的星座轨迹图，从而可以进行后续的基于星座轨迹图的特征提取。

此外，针对恒包络调制信号如最小频移键控MSK，由于接收的信号和差分后的信号都是分布在圆周上的，不易进行特征提取。通过在 I/Q 两路加入不同的延迟可以在星座轨迹图上获得更明显的特征。

综上所述，基于 I/Q 两路延迟和差分处理的信号处理框图如图 4 所示。

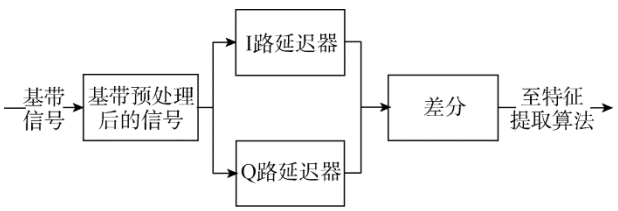

图 4　基于 I/Q 两路延迟和差分处理的信号处理框图

如图所示，接收端在收到过采样的基带信号后可以先对信号进行简单的预处理。预处理主要是对信号的能量进行归一化。对接收的信号进行预处理后将信号送入 I/Q 两路延迟器。延迟器可以选择 I/Q 两路相同的延迟以及不同的延迟。延迟器对 I/Q 两路信号延迟的选择主要取决于对信号调制方式的判断。之后，系统对信号进行差分处理，就可以在复平面上绘制出稳定而又清晰的星座轨迹图。

5　获得星座轨迹图

本文将结合实验系统，介绍基于星座轨迹图的射频指纹特征提取方法。实验系统选择 USRP 通用软件无线电外设平台和电脑主机。其中，软件无线电平台由 Ettus 公司生产的 USRP N210 主机和 CBX 射频子板构成[17]。该软件无线电平台可以工作在 1.2GHZ-6.0GHz 频段，其中接收和发射部分的带宽为 20MHz。最大采样率为 25MSamples/s。 USRP 主机通过千兆网线和电脑主机连接。电脑主机采用 Intel Core i7-4790 处理器。主机使用的操作系统为 Linux Ubuntu14.04。装有开源的软件无线电平台软件 GUN Radio 和 Matlab。实验系统用的软件无线电平台及实验系统框图如图 5 所示。

图 5　实验系统用的软件无线电平台及实验系统框图

如图 5 所示，2 个 USRP 软件无线电平台和 1 台主机构成了一个测试系统。主机端使用 Matlab 生成不同的调制信号，如 BPSK、QPSK 和 MSK。主机端可以选择不同的成型滤波器，如升余弦滤波器或高斯低通滤波器，并选择不同的滤波器参数。主机端最终生成可供发送的数据序列。主机端将数据序列发送至软件无线电平台 1，软件无线电平台 1 选取合适的发射频率将数据发送出去。主机同时通过软件无线电平台 2 进行无线数据的接收。将接收的数据按照如图 4 所示的算法流程进行处理，得到软件无线电平台 1 的射频特征。主机端再将数据序列发送至软件无线电平台 2，并通过软件无线电平台 1 进行接

收。将接收的数据按照相同的算法流程进行处理，得到软件无线电平台 2 的射频特征。

通过实际的通信系统，在没有频率偏差和相位偏差的情况下(自发自收)，设备发送的 BPSK、QPSK 和 MSK 信号过采用后的星座轨迹图如图 6 所示:

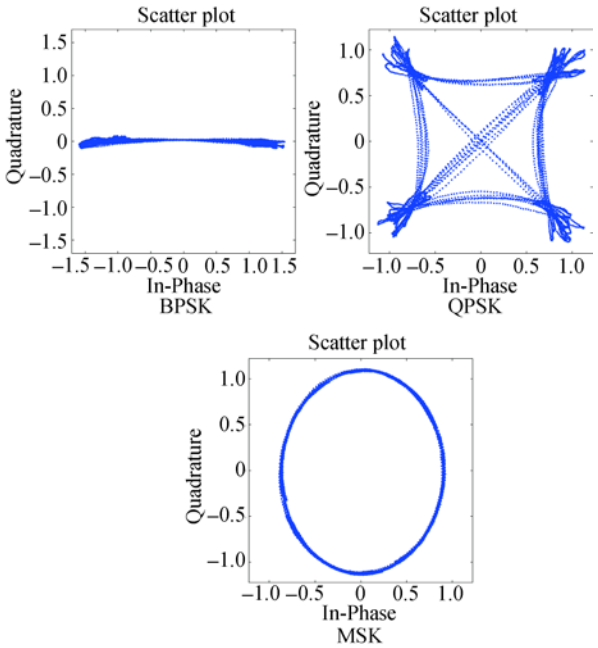

图 6　在没有频率偏差和相位偏差情况下接收到的星座轨迹图

如图 6 所示，不同的调制方式在经过预处理和过采样后，可以得到不同形态的星座轨迹图。但是在实际通信系统中，由于接收到的信号存在频率偏差。在没有完全消除频率偏差和相位偏差的情况下，2 台通信系统是无法获得如图 6 所示的星座轨迹图。

因此，在实际的系统中，按照如图 4 所示的方式进行差分处理。将接收到的 BPSK、QPSK 和 MSK 信号通过如图 4 所示的差分处理后，可以得到如图 7 所示的差分星座轨迹图(Differential CTF, DCTF):

从图 7 可以看到，在差分处理后的星座轨迹图上，可以较直接的分辨出设备 1 和设备 2 发送的 BPSK、QPSK 和 MSK 调制信号在接收端星座轨迹图上的特征，该特征将被用于无线目标的识别。此外，由于发射机和接收机存在着载波频率偏差，由公式(4)可知，得到的星座轨迹图在形态上具有一定程度的旋转。由于在本实验中使用了 USRP 设备 1 和 USRP 设备 2 互相作为发射机和接收机进行了实验，设备 1 和设备 2 实验结果的频率偏差的绝对数值一样，仅为在符号上相反。因此在图 7 上得到的设备 1 和设备 2 的差分星座轨迹图在旋转角度上是互为对称的。

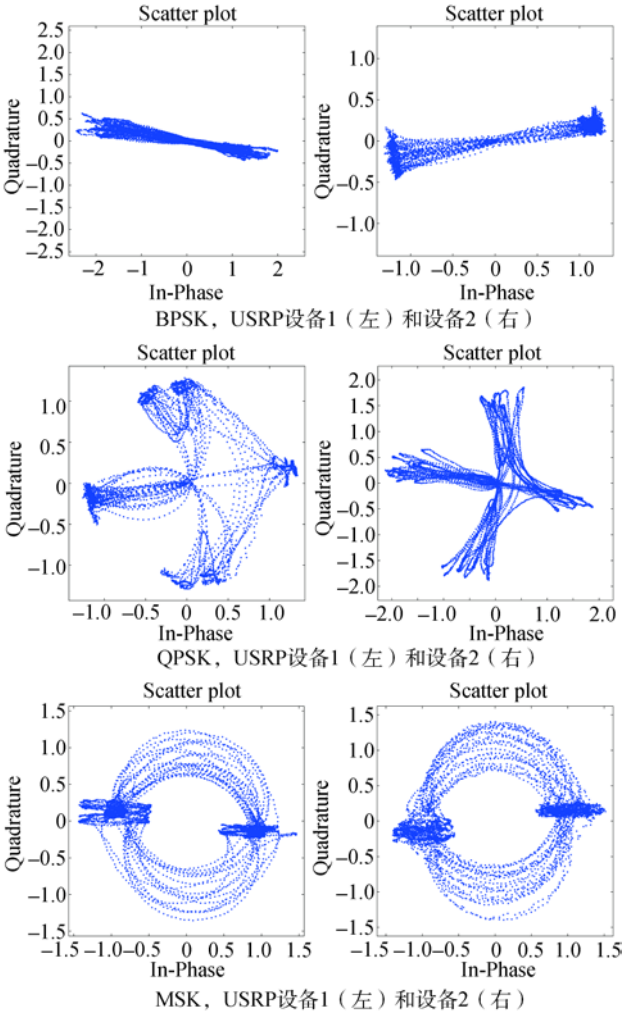

图 7　差分星座轨迹图(Differential CTF)

6　基于星座轨迹图的射频指纹特征提取

基于获得的星座轨迹图，可以获取其射频指纹特征。获取射频指纹特征可以直接从星座轨迹图上通过相关计算获得，也可以通过图像处理的方式获得。下面我们将简要介绍一下使用图像处理的方法进行星座轨迹图的射频指纹特征的提取。

基于图 7 中的差分星座轨迹图，可以进行可视化处理。通过可视化处理后的差分星座轨迹图如图 8 所示:

在图 8 所示的经过可视化处理后的差分星座轨迹图中，不仅可以表示出星座轨迹图的运行轨迹，还可以通过颜色的变化表示出星座轨迹点的密集程度。其中颜色越深的区域星座轨迹点的分布越密集。从图 8 可以看出，不同的无线设备经过可视化处理后的差分星座轨迹图有着明显的差异，这种差异可以被看作是设备独特的“射频指纹”特征。基于该图像上的差异，可以应用图像处理以及模式识别中的方

法进行特征提取。本文将介绍一种基于模式识别的用于差分星座轨迹图的无线设备身份识别方法。

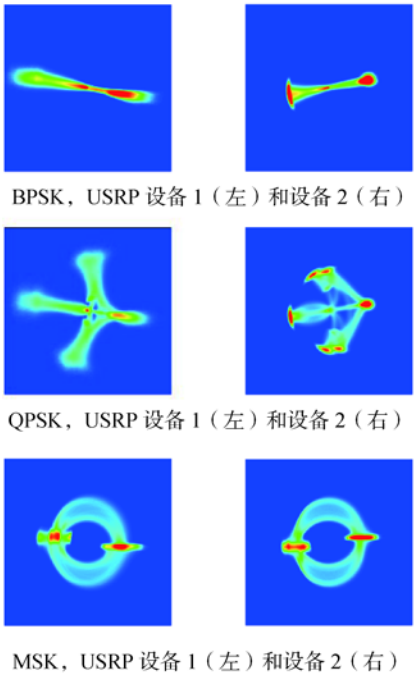

图 8　经过可视化处理后的差分星座轨迹图

基于图 8 所示的差分星座轨迹图，可以选择分布密集的点进行聚类。聚类算法选择 K 均值算法[18]。通过K均值算法得到分布密集的点不同的聚类中心。由于每一个设备射频指纹的差异，得到的聚类中心会有一定的差异。通过计算不同设备间聚类中心的欧式距离的和就可以得到设备相似度的匹配程度，从而可以对设备进行身份识别。

具体的基于差分星座轨迹图的特征提取与身份识别的实现方法如下:

首先将第i个设备的差分星座轨迹图分为$M \times N$的区域，生成一个$M \times N$的矩阵 Q。然后选择一个门限 α。将差分星座轨迹图中每个区域$Z^i[m,n]$, $0<m\leqslant M$, $0<n\leqslant N$的密集程度进行计算:当密集程度大于α，设置矩阵$Q^i[m,n]=1$。对处理后的矩阵Q中为1的点按照一共为P类进行K均值聚类，得到P个聚类中心$K_p^i, 0<p\leqslant P$。当获得设备i的聚类中心信息后，针对新输入的设备j，计算其聚类中心的欧式距离和:

$$S_{i,j}=\sum_{p=1}^{P}\left(d\left(K_p^i-K_p^j\right)\right) \tag{5}$$

其中d为计算欧式距离。

最后，系统通过分析$S_{i,j}$的大小可以对输入的设备j是否是设备i进行判断。在实际系统中具体的判决门限将根据系统训练后的结果确定。

7　实验结果及分析

在前面的章节中，我们介绍了如何通过星座轨迹图进行射频指纹特征的提取并通过图像处理和模式识别的方法对无线设备进行身份识别。在本章中，我们将展现通过 USRP 软件无线电平台对实际的无线设备进行射频指纹特征的提取与身份识别。

实验使用的无线设备发射装置为 Ti 公司的 CC2530 (Zigbee)模块[19]。实验通过 USRP 软件无线电平台对 12 个 CC2530 模块进行射频指纹特征提取与身份识别。实验用的 CC2530 模块及实验的框图如图 9 所示。

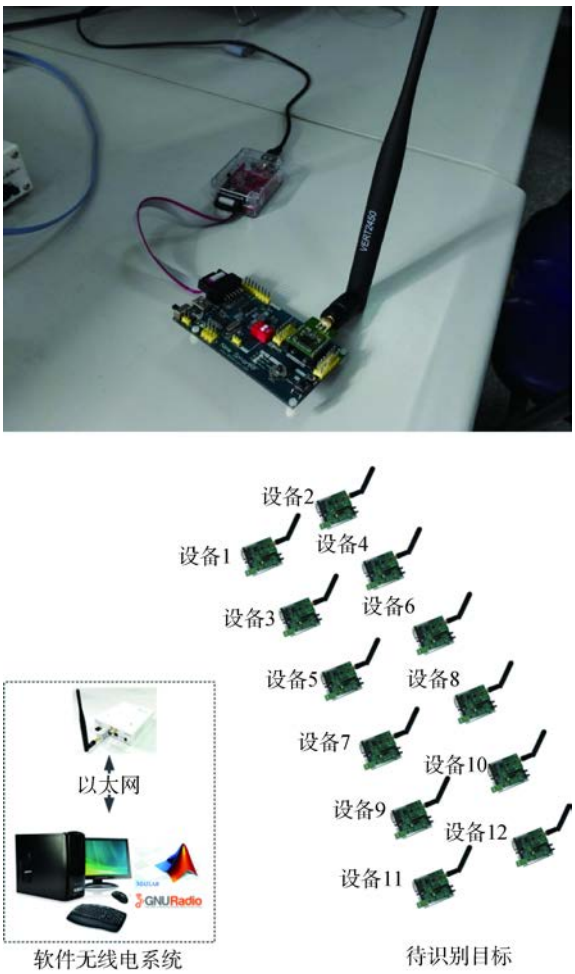

图 9　CC2530 无线设备模块及实验系统框图

CC2530 调制的信号为 OQPSK(偏移四相相移键控, Offset-QPSK)，类似于 MSK 调制信号。软件无线电平台将接收到的信号进行如图 4 所示的处理后可以得到如图 10(a)所示差分星座轨迹图。系统按照 4 个类对获得的差分星座轨迹图进行聚类，可以得到聚类中心如图 10(b)所示。

如图所示，CC2530 设备 1 的星座轨迹图密集点被成功分为了 4 类。我们首先对 12 个 CC2530 设备进行训练，得到 12 个 CC2530 设备的射频指纹特征。

然后再开启不同编号的 CC2530 设备，系统通过射频指纹库中的信息对接收到的 CC2530 设备的信号进行匹配，完成对接入设备的身份识别。

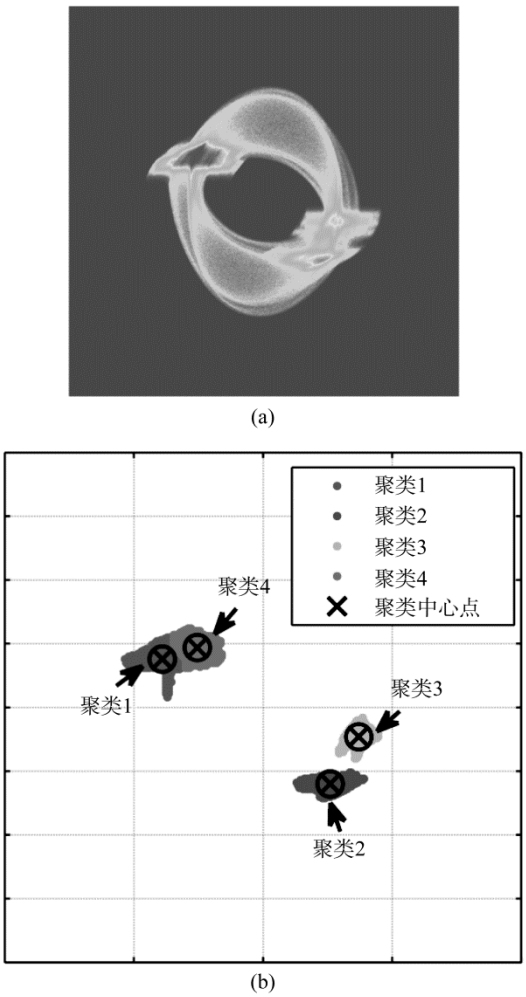

图 10　得到的 CC2530 无线设备模块差分星座轨迹图与 K 均值聚类后的结果

在实验室环境的测试系统中，接收的信号包含有发射设备的射频指纹特征以及室内环境下的传输信道特征。由于发射设备的射频指纹特征明显强于室内环境下的传输信道特征，我们认为接收端的信号主要包含了发射端的射频指纹特征，因而不考虑传输信道特征。然而，在实验室环境中，接收的信号拥有较高的信噪比。因此我们可以通过对接收到的信号加入人工白噪声的方式，以检测射频指纹特征提取算法和身份识别算法的可靠性。加入人工白噪声的流程框图如图 11 所示:

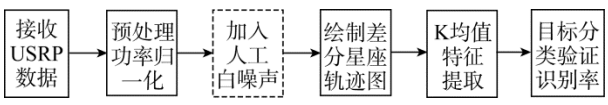

图 11　加入人工白噪声的系统处理框图

经过添加不同大小的人工白噪声，可以对射频指纹特征提取算法和身份识别算法的性能进行评估，加入人工白噪声后的实验结果如图 12 所示:

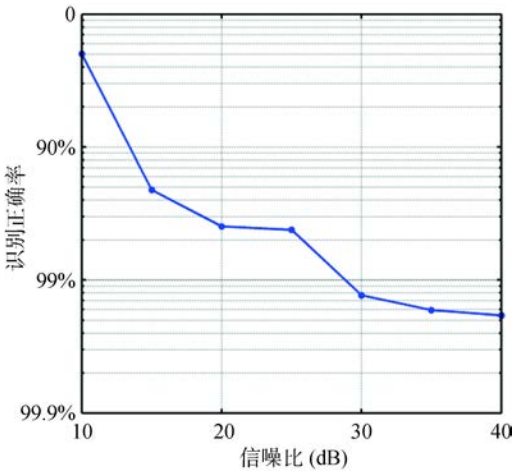

图 12　加入人工白噪声的基于星座轨迹图

射频指纹特征提取及身份识别算法的识别正确率通过对实际测量的结果加入不同大小的人工白噪声后可以看出，当系统的信噪比高于 15dB 时，系统可以达到高于 95%的正确识别率。当系统的信噪比高于 30dB 时，系统的正确识别率可以达到 99%。因此，在实际的环境中，该基于星座轨迹图的射频指纹特征提取及身份识别算法可以较好的工作在信噪比高于 15dB 的情况下。

8　影响星座轨迹图特征的因素

在前面的章节中，我们通过实验系统展示了如何通过星座轨迹图进行射频指纹特征的提取。从实验结果可以看到，基于星座轨迹图的射频指纹特征提取方法可以很好的对无线设备进行身份识别。然而，在实际的通信系统中，可能会有比实验室环境更为复杂的影响因素。本章节将分析在实际信道下影响基于星座轨迹图的射频指纹特征提取的因素。

首先，在实际系统中，最容易影响星座轨迹图特征的是接收信号功率的变化。这个问题可以通过如图 4 所示的对接收信号进行功率归一化的预处理解决。此外，由于接收信号功率的变化还会导致接收信号信噪比的变化。在不同噪声环境下对基于星座轨迹图的射频指纹特征提取将是一个挑战。本文提出的射频指纹特征提取及身份识别算法可以较好的工作在 15dB 信噪比以上的环境中。对于低信噪比环境下基于星座轨迹图的射频指纹特征提取方法及身份识别算法的研究是后续需要解决的问题。

除了噪声的影响因素，信道的参数变化也是影

响基于星座轨迹图的射频指纹特征提取的一个因素。在实际通信系统中，信道的变化在一定的时间和空间范围内有统计特性。因此通过增加采样的时间，在获得一定长度的接收信号后，可以在星座轨迹图上将信道的统计特性模糊在射频指纹特征中。但是，信道统计特性中残留的慢变参数还是会影响星座轨迹图的变化。针对这一影响因素还需要进一步的通过使用信号处理的方法来分离信道和设备的特征参数。此外，根据我们所获得的研究资料表明，在现有的针对射频指纹特征的论文中，并没有研究信道变化对射频指纹特征提取的影响。在一些研究结果中，选取的特征参数很容易受到信道变化的影响[4,7]。虽然这样的考虑在实际系统的应用中需要进一步的改进，但是在实验系统设备的位置是固定不移动的情况下，不考虑信道参数对射频指纹特征的影响还是可以被接受的。

9 总结与展望

本文介绍了一种基于星座轨迹图的射频指纹特征提取方法。不同于现有的用于射频指纹特征提取的瞬态响应和稳态响应方法，本方法不需要获得设备发送信号的先验信息，可以在基带快速的获得无线设备的射频指纹。本文详细介绍了星座轨迹图的生成方法以及通过可视化处理得到清晰的星座轨迹图的方法。基于得到的差分星座轨迹图，本文介绍了一种通过 K 均值聚类进行特征提取和设备身份识别的方法。通过对实际无线设备进行特征提取和身份识别的实验，验证了本文提出的基于星座轨迹图的射频指纹特征提取方法的可靠性与实用性。后续的工作将主要围绕着如何基于图像处理的方法设计用于无线设备特征提取及身份识别的分类器。此外，如何克服噪声和信道对星座轨迹图特征提取的影响也将是需要重点研究的内容。

参考文献

[1] 3GPP TS 31.102 Characteristics of the USIM Application.

[2] IEEE Standard 802.15.1–2005 – IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks. Ieeexplore.ieee.org. doi:10.1109/IEEESTD.2005.96290. Retrieved 4 September 2010.

[3] B. Danev, D. Zanetti, and S. Capkun, “On Physical-Layer Identification of Wireless Devices”, *Computing Surveys (CSUR)*, Volume 45 Issue 1,November 2012.

[4] V.Brik, S.Banerjee, M.Gruteser, and S. Oh, “Wireless Device Identification with Radiometric Signatures”, [C] In *Proceedings of the 14th ACM international conference on Mobile computing and networking (MobiCom2008)*.

[5] H. L. Yuan and A. Q. Hu, “Fountainhead and uniqueness of RF fingerprint”, *Journal of Southeast University (Natural Science Edition)*, vol. 39, no.2, pp.230-233, Mar. 2009.
(袁红林, 胡爱群, “射频指纹的产生机理与唯一性”, *东南大学学报(自然科学版)*, 第 39 卷第 2 期, 第 230-233 页, 2009 年 3 月)

[6] D.R. Reising, M.A. Temple, and J.A. Jackson, “Authorized and Rogue Device Discrimination Using Dimensionally Reduced RF-DNA Fingerprints”, *IEEE Transactions on Information Forensics and Security*, vol.10, no.6, pp.1180-1192, Jun. 2015.

[7] F. Demers and M.S. Hilaire, “Radiometric Identification of LTE Transmitters”, *2013 IEEE Global Communications Conference (GLOBECOM)*.

[8] S.U.Rehman, K.W. Sowerby, and C.Coghill, “Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios”, *IET Communications*, vol.8, no.8, pp.1274-1284, 2014.

[9] J. Toonstra and W. Andkinsner, “Transient analysis and genetic algorithms for classification”, In *Proceedings of the IEEE Conference on Communications, Power, and Computing (WESCANEX 1995)*. vol.2, pp.432–437, 1995.

[10] K.A. Remley, C.A. Grosvenor, R.T.Johnk, D.R. Novotny, P.D. Hale, and M.D. McKinley, “Electromagnetic Signatures of WLAN Cards and Network Security”, *2005 IEEE International Symposium on Signal Processing and Information Technology*.

[11] J.Hall, “Detection of rogue devices in Wireless Networks [Ph.D.dissertation]”, *Carleton University*, 2006.

[12] B.Danev and S.Capkun, “Transient-based Identification of Wireless Sensor Nodes”, In *Proceedings of International Conference on Information Processing in Sensor Networks (IPSN 2009)*.

[13] H.P. Romero, K.A. Remley, D.F. Williams, and C.M. Wang, “Electromagnetic Measurements for Counterfeit Detection of Radio Frequency Identification Cards”, *IEEE Transactions on Microwave Theory and Techniques*, vol.57, no.5, pp.1383-1387, May 2009.

[14] N.T. Nguyen, G. Zheng, Z.Han, and R. Zheng, “Device fingerprinting to enhance wireless security using nonparametric Bayesian method”, In *Proceedings of IEEEINFOCOM*, pp.1404- 1412, 2011.

[15] M. Pospisil, R. Marsalek, and J. Pomenkova, “Wireless device authentication through transmitter imperfections - measurement and classification”, *IEEE 24th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2013)*.

[16] Candore, O. Kocabas, and F. Koushanfar, “Robust Stable Radiometric Fingerprinting forWireless Devices”, I*EEE International Workshop onHardware-Oriented Security and Trust (HOST 2009)*.

[17] USRP, http://www.ettus.com/, online available 2015-11-4.

[18] S. Theodoridis and K.Koutroumbas, 模式识别(第四版) Pattern Recognition (Fourth Edition), 电子工业出版社, 2010.

[19] CC2530, http://www.ti.com/product/cc2530, online available 2015-11-4.

彭林宁 于 2014 年在法国雷恩国立应用科学学院, 电子与通信专业获得博士学位。现为东南大学信息科学与工程学院副研究院。主要研究领域为物理层安全。
E-mail: pengln@seu.edu.cn

胡爱群 于 1992 年在东南大学, 信号与信息处理专业获得博士学位。现为东南大学信息科学与工程学院教授/博导。主要研究领域为通信安全、无线网络安全。
E-mail: aqhu@seu.edu.cn

朱长明 河南焦作人, 博士, 高工. 主要研究领域信息安全.
E-mail:zhuchangming2003@126.com

姜禹 于 2009 年在东南大学, 信号与信息处理专业获得博士学位。现为东南大学信息科学与工程学院讲师。 主要研究领域无线网络安全.
E-mail: jiangyu@seu.edu.cn