分类号：TN918　　密　级：公 开
UDC：　654.1　　学　号：079082

东　南　大　学

博　士　学　位　论　文

基于射频指纹的无线网络物理层认证关键技术研究

研究生姓名：　袁 红 林
导师姓名：　胡爱群 教授

申请学位专业　信息与通信工程　申请学位级别　工学博士
论文提交日期　2011 年 3 月　论文答辩日期　2011 年 5 月
答辩委员会主席　　评 阅 人

2011 年 5 月 8 日

东南大学博士学位论文

基于射频指纹的无线网络物理层认证关键技术研究

博士研究生：袁红林

专业：信息与通信工程（信息安全）

指导老师：胡爱群 教授

中国·南京·东南大学信息科学与工程学院

二零一一年五月

RESEARCH ON PHYSICAL-LAYER AUTHENTICATION OF WIRELESS NETWORK BASED ON RF FINGERPRINTS

A Dissertation Submitted to
Southeast University
For the Academic Degree of Doctor of Engineering

BY

Honglin Yuan

Supervised by

Professor HU Ai-qun

School of Information Science and Engineering

Southeast University

2011.5.

东 南 大 学 学 位 论 文 独 创 性 声 明

本人声明所呈交的学位论文是我个人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其它人已经发表或撰写过的研究成果，也不包含为获得东南大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

研究生签名：_____日 期：_____

东 南 大 学 学 位 论 文 使 用 授 权 声 明

东南大学、中国科学技术信息研究所、国家图书馆有权保留本人所送交学位论文的复印件和电子文档，可以采用影印、缩印或其它复制手段保存论文。本人电子文档的内容和纸质论文的内容相一致。除在保密期内的保密论文外，允许论文被查阅和借阅，可以公布（包括刊登）论文的全部或部分内容。论文的公布（包括刊登）授权东南大学研究生院办理。

研究生签名：_____导师签名：_____日 期：_____

摘要

随着无线网络的飞速发展与安全威胁的与日俱增，无线网络的物理层安全正在变得越来越重要。认证是无线网络业务的安全基础，它保证通信双方是其所声称的身份，防止非法用户的接入与访问。基于物理层之上的认证一般采用密码机制与安全协议实现。密码机制存在密钥泄露的风险，而安全协议通常存在安全缺陷。无线设备发射机的由于器件容差产生的射频指纹具有难以克隆的物理特性，可以用来进行无线设备的身份认证。这方面的相关文献较少，本文对基于射频指纹的无线网络物理层认证的若干关键性基础问题进行了一些探索研究，包括“射频指纹”的定义、“射频指纹识别”的过程划分与体系结构、射频指纹识别系统的基本模型、数字化射频指纹的可分离性、射频指纹的检测与变换方法等等。

本文的主要贡献如下：

1. 对“射频指纹”的概念进行了概括与提炼，尝试性提出一种“射频指纹”定义：射频指纹是携带无线设备发射机硬件信息的接收无线信号的变换结果，这种变换结果体现无线设备发射机的硬件特性并具备可比性。把“射频指纹识别”过程分为四个步骤：（1）接收无线信号的起始时刻检测与截取；（2）射频指纹变换；（3）特征提取；（4）无线设备的识别或确认。这种划分方法指出同一种射频指纹可以进行多种特征的提取。尝试性构建了包括信号层、射频指纹层、特征层及无线发射机层的射频指纹识别体系结构。本文的其它内容基于提出的这种“射频指纹”定义、“射频指纹识别”过程划分及体系结构展开。

2. 基于一种通用的无线数字发射机结构，对射频指纹的产生机理进行了分析与仿真，指出无线发射机的构件存在容差是产生射频指纹的主要内在机理。通过对无线设备发送的射频信号进行非线性与时变性分析，提出了射频指纹识别系统的一种基本模型，推导了该模型中接收无线信号的基带与带通理想等效形式。

3. 对数字化射频指纹的可分离性进行了理论分析，推导了其与主要影响因素之间关系的解析式。根据该解析式，得出如下结论：数字化射频指纹的可分离性由其识别系统分辨力、指纹维数与待识别无线设备发射机结构及构件容差性质的相对程度决定。另外，根据该解析式，可以推知：模拟射频指纹具有唯一性。

4. 针对 Wi-Fi 发射机，提出了一种基于前导的射频指纹检测方法。该方法根据 Wi-Fi 物理层帧前导的特征，运用“相关”技术进行检测。实验表明，由于该方法基于前导的稳态信号进行，因而得到的射频指纹的稳定性优于文献中基于瞬态信号检测得到的射频指纹的稳定性。

5. 对文献中已有的射频指纹变换方法进行了分析与分类，根据用于变换的接收无线

信号类型把“射频指纹”分为“基于瞬态信号”的 turn-on 射频指纹与“基于稳态信号”的 steady-state 射频指纹两类，在此基础上，提出了多种射频指纹变换与识别方法。

把待识别发射机建模为线性与非线性的混合系统，提出了“功率渐升前导射频指纹”变换及其产生方法。建模分析显示：该射频指纹的可分性比经典的 turn-on 与 steady-state 射频指纹的可分性优。

把待识别 Wi-Fi 发射机建模为非线性系统，提出了 Wi-Fi 信号的相空间差射频指纹识别方法，该方法利用了待识别发射机硬件的非线性信息，算法比同类方法简单。

当待识别无线发射机、无线信道及“射频指纹识别系统”可等效为线性系统时，提出了“BPSK 基带倒谱与频偏对数谱射频指纹”与“ARMA 模型系数射频指纹”变换方法。提出的“BPSK 基带倒谱与频偏对数谱射频指纹”主要由待识别发射机的硬件特性决定，因而具备独立性、时间平移不变性与稳健性；但是这两种射频指纹存在一些应用限制。提出的“ARMA 模型系数射频指纹”具有明确的物理意义，与直接采用 ARMA 系统模型的零点或极点构成的射频指纹相比，其可分离性有可能得到增强。

提出的这五种射频指纹中，“功率渐升前导射频指纹”属于 turn-on 射频指纹，其它四种射频指纹属于 steady-state 射频指纹。

关键词：无线安全，物理层认证，射频指纹识别，可分离性，倒谱分析，相空间重构

Abstract

As the rapid development of wireless networks and the increase of security threats, the physical-layer security of wireless networks is becoming important more and more. Authentication is the foundation of the security of wireless network services, authentication ensures that the communication entity is the entity he claims, and the goal of authentication is to prevent the access of illegal users. Authentication above the physical layer of wireless networks is normally based on cryptography mechanism and security protocol, while the key of cryptography mechanism is easy to be compromised and the defects of security protocol are common. The Radio Frequency (RF) fingerprints, which embodies the hardware property of the wireless transmitter to be identified, has the characteristics difficult to be cloned and can be used for non-cryptographic authentication of wireless transmitters. Relevant literatures are scarce, several basic issues on the physical layer authentication of wireless networks with RF fingerprints are studied in this dissertation, including the definition of RF fingerprints, the process partition and system structure of RF fingerprints identification, the basic models of RF fingerprints identification system, the discriminability of the digital RF fingerprints, the detecting and transform methods of RF fingerprints etc.

The main contributions of this dissertation are as follows:

1. A novel definition of RF fingerprints is tentatively put forward based on the analyses of the existing notions of RF fingerprints: RF fingerprints is the transform of a received wireless signal that carries the hardware information of the transmitter of the radio to be identified, and is comparable. Then, the process of RF fingerprints identification is partitioned into the following steps: the detection and truncation of the received signal, the transform of RF fingerprints, the feather extraction of RF fingerprints and the identification or verification of the wireless devices. This kind of partition method points out that multiple kinds of features can be extracted from one kind of RF fingerprints. A system structure of RF fingerprints identification is tentatively built, which includes signal layer, RF fingerprints layer, feature layer and wireless transmitter layer. This dissertation is unfolded based on the proposed definition of RF fingerprints, partition method of RF fingerprints identification process and the system structure of RF fingerprints identification.

2. Based on a general structure of wireless digital transmitter, the mechanism of RF fingerprints is analyzed and it is pointed out that component tolerances is the major foundation of RF fingerprints. The nonlinearity and time-variant of the transmitted RF signal from wireless devices are studied, a kind of basic model of RF fingerprints identification system is then proposed and the baseband and band-pass equivalence of the received wireless signal is derived.

3. The discriminability of digital RF fingerprints is analyzed theoretically, and an analytical formula on the discriminability of digital RF Fingerprints with their impact factors is derived.

Analyses demonstrates that the discriminability of digital RF Fingerprints is determined by the comparison between the distinguishing ability of the RF fingerprints identification system, the dimension numbers of fingerprints and the component tolerances property, the structure of the transmitter to be identified. The uniqueness of RF fingerprints is consequently predicted.

4. A novel method based on preamble is then proposed for the detection of Wi-Fi RF fingerprints. The novel method utilizes the characteristics of the steady-state Wi-Fi preamble and the technique of correlation. It is demonstrated by experiments that as the proposed detection method utilized the steady-state signals of preamble, the stability of the according transformed RF fingerprints is better than that utilizing transient signals whose stability is bad.

5. The RF fingerprints transform methods existing in literatures are analyzed and classified. The existing RF fingerprints are classified into two categories based on the signal used for transform: the RF fingerprints transformed from transient signals called “turn-on RF fingerprints” and the RF fingerprints transformed from steady-state signals called “steady-state RF fingerprints”. Several kinds of RF fingerprints and their identification methods are then proposed.

When the wireless transmitter to be identified is modeled as a linear and non-linear hybrid system, the “power ramp-up RF fingerprints” identification and generating methods are proposed. It is demonstrated by modeling analyses that the separability of the proposed RF fingerprints is better than that of classical turn-on and steady-state RF fingerprints.

When the Wi-Fi transmitter to be identified is modeled as a non-linear system, the phase space difference RF fingerprints identification method is proposed which utilized the non-linear hardware information of the transmitter to be identified. The algorithm of the proposed method is simple comparing to similar methods.

When the wireless transmitter to be identified, wireless channel, and the RF fingerprints identification system can be modeled as a linear system, the “BPSK baseband cepstrum and frequency difference logarithm spectrum RF fingerprints” and the “ARMA model coefficients RF fingerprints” transform methods are proposed. The proposed “BPSK RF fingerprints” are mainly determined by the hardware property of the transmitter to be identified, so are independent, time shift invariant and robust, while some limits exist in their applicaitons. The proposed “ARMA coefficients RF fingerprints” has clear physical meaning, its separability may be enhanced comparing to RF fingerprints used directly the zero and pole points of ARMA system models.

Among the proposed five kinds of RF fingerprints, the “power ramp-up RF fingerprints” belongs to turn-on RF fingerprints, and the other four kinds of RF fingerprints are steady-state RF fingerprints.

Key Words： wireless security, Physical-layer authentication, RF fingerprints identification, discriminability, cepstrum analysis, phase space reconstruction

目　录

第一章 绪论

1.1 论文的研究背景

随着无线通信与网络技术的快速发展，无线网络已渗透到国防军事、教学科研和医疗卫生等国民经济的各个部门，已与人们的日常生活紧密相关。无线网络技术的迅猛发展使人类的信息沟通摆脱了时间、地点和对象的束缚，极大地改善了人类的生活质量，加快了社会发展进程。当前，无线网络技术正朝着宽带、多媒体综合数据业务方向发展，最终实现在任何时间和任何地点都能与任何对象进行任何形式的通信。未来的无线网络必将与 Internet 实现全面的、深度的融合，甚至任何物体都可以在各种网络（广域网、城域网及局域网等）的协作下实现联接。

然而，无线网络的安全问题仍是阻碍其普及应用的因素之一，主要表现在以下几个方面：

（1）无线网络的开放性使其更容易受到恶意攻击。由于无线网络设备通过无线电波在空中传播信息，无线电波覆盖范围内的任何接收机都有可能接收到无线设备的发射信号，因而无线网络更容易受到从被动窃听到主动干扰的各种攻击。无线网络的这种开放性带来了非法信息截取、未授权信息服务等一系列的信息安全问题。

（2）无线网络的移动性使其安全管理难度大。无线网络节点终端不仅可在小范围内移动，而且还可以跨区域漫游，这意味着终端没有足够的物理保护，从而易于被窃听、破坏和劫持。另一方面，通过网络内部已经被入侵的节点终端实施攻击造成的破坏更大，也更难被检测。因此，无线网络移动终端的安全管理要困难得多。

（3）无线网络动态变化的拓扑结构使得安全方案的实施难度大。无线网络环境中，拓扑结构动态变化，缺乏集中管理机制，因此安全技术更复杂。另外，无线网络环境中许多决策是分散的，许多网络算法必须依赖所有节点的共同参与和协作。缺乏集中管理机制意味着攻击者可利用这一弱点进行攻击来破坏协作算法。

总之，无线网络的安全问题是由通信载体的开放性、节点终端的移动性、动态变化的网络拓扑结构等造成的。无线网络节点终端易受到的安全威胁主要有：

- 攻击者伪装成合法用户，非法访问网络资源；
- 截获无线链路上的传输数据；
- 实施拒绝服务攻击；
- 通过无线网络，连接到攻击对象网络上实施攻击；
- 通过无线网络，获得对攻击对象网络的管理控制权限。

在网络通信中，主要的安全防护措施称为安全业务，通用的安全业务主要有五种：认证业务、访问控制业务、保密业务、数据完整性业务和不可否认业务[1]。无线网络环

境下，具体的业务可分为：访问控制、实体认证、数据来源认证、数据完整性、机密性、不可否认、安全响应和安全性审计等。其中，认证是无线网络安全业务的基础。

认证保证通信双方是其所声称的身份，目的是防止非法用户的接入与访问。认证可进一步分为实体认证和数据源认证。实体认证的目的是证明一个用户、系统或应用是其所声称的身份。而数据源认证，也称为消息认证，是指验证通信数据的来源。认证有单向认证与双向认证之分，单向认证由验证者认证通信方的身份，而双向认证中通信双方都要进行认证。

认证一般通过安全协议进行[2]。安全协议是网络安全的一个重要组成部分，实际系统通过安全协议实现通信双方之间的认证、密钥及其它秘密的分配、发送和接收消息不可否认性的确认等。实现认证的主要安全协议是认证协议。

认证协议的实现基于密码机制，即如果通信一方声称知道某个秘密，则另一方据此验证其声称的身份。具体有以下几种方法：

- 声称者使用仅为声称者和验证者知道的密钥封装的一个消息，如果验证者能够成功地解密消息或验证封装是正确的，则声称者的身份得到证明；
- 声称者使用私钥对消息签名，验证者使用声称者的公钥验证签名，如果正确，则声称者的身份得到证明；
- 声称者通过可信第三方来证明自己。

通常，如果某通信方断定自己和对方正常运行了协议，而对方却有不同的结论，那么该协议存在缺陷。无线网络环境中，安全的接入网络并在通信双方之间安全地建立会话密钥是认证协议所要解决的核心问题，是安全通信的基础，也是无线网络安全与有线网络安全最大的区别之一。

实际中的无线网络认证机制经常存在缺陷。例如，IEEE 802.11 无线局域网（WLAN）的安全机制从最初的有线等效保密（WEP）经过 IEEE 802.1X 认证发展为 IEEE 802.11i，但仍不能保证没有安全问题。另外，如果密钥泄露，现有的认证机制则根本无法实现其声称的认证业务。

因此，当前的运行于无线网络链路层及其之上的认证机制需要进一步增强。

1.2 论文相关内容的国内外研究现状

近几年来，随着无线网络的飞速发展与安全威胁的与日俱增，无线网络安全正越来越依赖物理层技术。出现了一些非密码认证的新方法，主要可分为基于信道/位置、软件及硬件三类。其中，基于信道/位置的非密码认证可分为基于无线信道状态及基于接收信号强度的方法，基于软件的非密码认证可分为基于物理层 MAC 协议的实现行为、帧序号及通信模式等方法，而基于硬件的非密码认证可分为基于电路延时、时钟偏斜以及射频指纹的方法。各种非密码认证方法如图 1.1 所示[3, 4]。

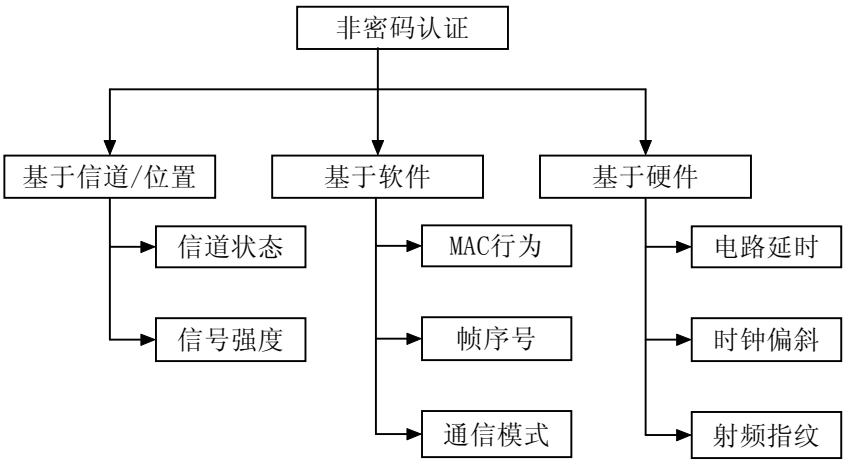

图 1.1 非密码认证方法

图 1.1 中的非密码认证方法简单介绍如下：

（1）基于信道/位置的方法[5-22]

无线信道状态与无线设备位置作为无线设备的外在特性被用于无线设备的非密码认证。无线网络中，通信接收方根据接收无线信号对无线信道的冲激响应进行估计，并与其登记的信息进行比较，从而对其是否合法用户进行判决。接收信号强度由发射机发射功率及无线信道状态共同决定，而无线信道状态与接收机与发射机之间的相对位置有关。这类非密码认证方法利用待识别无线设备的外特征，当无线设备的位置发生改变，或无线信道状态发生改变时，识别系统应做相应的改变，这是这类方法的缺点之一。

（2）基于软件的方法[23, 24]

尽管无线设备的相应标准对其功能进行了规范，但不同厂家的无线设备在实现标准细节上不一定完全相同。例如，IEEE 802.11 标准是无线局域网的事实上的物理层与媒介访问控制层的协议标准。由于其极其庞大并且复杂，不同厂家在生产 IEEE 802.11 设备及开发设备驱动软件时，可能都会有一些不同。基于软件的非密码认证利用各种无线设备实现物理层与媒介访问控制层协议的不同软件特征对无线设备进行识别，但该类方法不能区分同一厂家生产的同一批次的无线设备。

（3）基于硬件的方法

基于硬件的非密码认证方法是指根据无线发射机的硬件特征识别无线发射机硬件，从而实现无线设备的身份认证，包括基于电路延时、时钟偏斜以及射频指纹的方法。

基于电路延时的非密码认证方法属于基于物理不可克隆函数的研究范畴[25]。该方法利用不同集成电路内部的线延时及门延时的唯一性，根据不同激励产生具备唯一性的响应，对该集成电路进行认证。该方法的缺点是必须增加额外的定制硬件，并且必须改变协议行为。

基于时钟偏斜的非密码认证方法的基础是“不同发射机的时钟都具有一定的偏斜”，据此，文献[26]根据不同无线设备发送帧中的时间信息进行了相应无线设备的识别实验。该方法的缺点是攻击者同样可以通过记录无线设备的发送帧，从而获取该设备的时钟偏斜，然后通过修改帧中的时间信息进行攻击。

基于“射频指纹”[27-61]的非密码认证方法是指根据无线设备的“射频指纹”识别或确认无线设备，实现无线设备的身份认证，从而在无线网络物理层增强无线网络的接入控制安全性。这种方法的机理是任何无线设备的硬件都存在差异，并且难以克隆。文献[59]显示，基于“射频指纹”的非密码认证方法容易受到中间人攻击，但这种攻击的前提是攻击者必须配备高端的任意信号发生器，这种攻击的成本极高，因而不具有现实意义。无线设备的“射频指纹识别或确认”工作在物理层，能提供比传统无线网络认证方法更高的安全性能。

以上几种非密码认证方法各有优缺点，在特定应用场景下都具有应用价值。本文主要对基于“射频指纹识别”的无线网络物理层认证关键技术进行研究。

1.2.1 “射频指纹识别”概念的提出

“射频指纹”与“射频指纹识别”是2003左右加拿大的J. Hall等在蓝牙等无线网络设备识别研究中提出的新概念[29, 30]。自那之后，该概念主要出现在无线网络设备的识别研究中（下文中用“无线设备”简称“无线网络设备”）。相关文献总量不多，大部分在会议发表，SCI收录的期刊文献寥寥无几；并且，大部分文献主要介绍实验，理论性文献较少。与“射频指纹识别”相关的技术有“雷达辐射源识别”[62-72]及“通信电台个体识别”[73-96]等特定辐射源识别技术，可同属于基于物理不可克隆函数[97, 98]的研究范畴。

J. Hall在其2004年的文献中这样描述：射频指纹识别是一种基于发射机发射信号瞬态部分对发射机进行唯一识别的技术。该文献基于射频指纹构建IEEE 802.11b入侵检测系统来对抗MAC地址伪造等攻击[30]。

Ureten, O.在其2005年的文献中这样描述：唯一的开机（turn-on）特征被称为射频指纹，能用于诸如IEEE 802.11x无线发射机的识别。射频指纹识别需要三个阶段：瞬态检测、特征提取与指纹分类。该文献研究了IEEE 802.11b射频信号的一种基于Bayesian的检测方法[34]。

Barbeau, M.在其2006年的文献中这样描述：射频指纹识别是一种技术，该技术用于捕获基于射频的无线发射机射频能量的唯一特征。该文献介绍了采用射频指纹识别技术为未来的无线网络构建对抗中间人攻击的入侵检测系统[35]。

Ureten, O.在其2007年的文献中把射频指纹识别分为四个步骤：预处理、检测、特征提取与分类。该文献介绍了一个完整的Wi-Fi Ad-hoc网的射频指纹识别系统[43]。

Suski, W. C.在其2008年的文献中把射频指纹识别分为四个步骤：波形参数抽取、瞬态检测、特征提取与未知接收信号的分类。该文献基于OFDM信号的谱特征对三个IEEE 802.11a无线设备进行了概念性的实验研究[51]。

Danev, B.在其2009年的文献中这样描述：通过无线传感器节点发射的射频信号特征来识别该节点，这种技术一般称为射频指纹识别。该文献基于瞬态信号指纹对无线传感器节点进行了识别研究[54]。

Klein, R. W.在其2009年的文献中这样描述：射频指纹识别是物理层安全技术之一，该技术利用特定无线设备的内在的唯一射频特征，并且这种特征难以复制。该文献基于小波变换技术进行了IEEE 802.11a无线设备的识别研究[56]。

Danev, B.在其2010年的文献中这样描述：射频指纹识别，也称为无线设备的物理层识别，其目标是基于存在于无线设备内的物理层特征识别无线设备。该文献对基于射频指纹识别的物理层认证方法的攻击进行了研究[59]。

综合以上文献所述，现有的“射频指纹”及其识别过程的划分稍显混乱，没有揭示其本质，即：无线设备发送的射频信号中，不仅承载着无线设备发送的数字信息，而且承载着其发射机的硬件信息。为此，作者尝试性提出如下的一种“射频指纹”定义：射频指纹是携带无线设备发射机硬件信息的接收无线信号的变换结果，这种变换结果体现无线设备发射机的硬件特性并具备可比性。

基于该“射频指纹”定义，作者提出根据射频指纹识别无线设备（简称：射频指纹识别）的过程可分为四步，如图1.2所示。

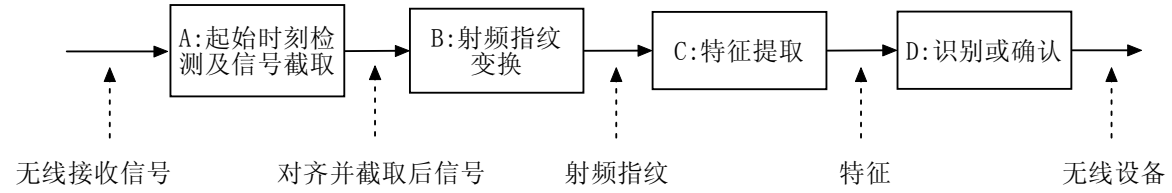

图 1.2 射频指纹识别过程

如图1.2所示，步骤A对接收无线信号进行起始时刻检测，根据检测的起始时刻对接收信号进行对齐与截取；步骤B把截取后的接收信号变换为射频指纹，例如把开机瞬态信号变换为其包络等；步骤C对射频指纹进行特征提取；步骤D根据提取的特征进行无线设备的识别或确认。提出的射频指纹识别四步骤中，对于同一个截取后接收无线信号，可能有多种射频指纹变换方法；而对于同一种射频指纹，可能有多种特征提取方法。与以往文献中的“射频指纹识别过程划分”相比，新的“射频指纹识别过程划分”具有更清晰的逻辑层次。本文即以尝试性提出的这种“射频指纹”定义与“射频指纹识别”过程划分方法展开。

1.2.2 主要的射频指纹识别技术

根据本文尝试性提出的“射频指纹”定义与“射频指纹识别”过程的4步骤划分法，射频指纹识别的体系结构可以总结为图1.3所示。

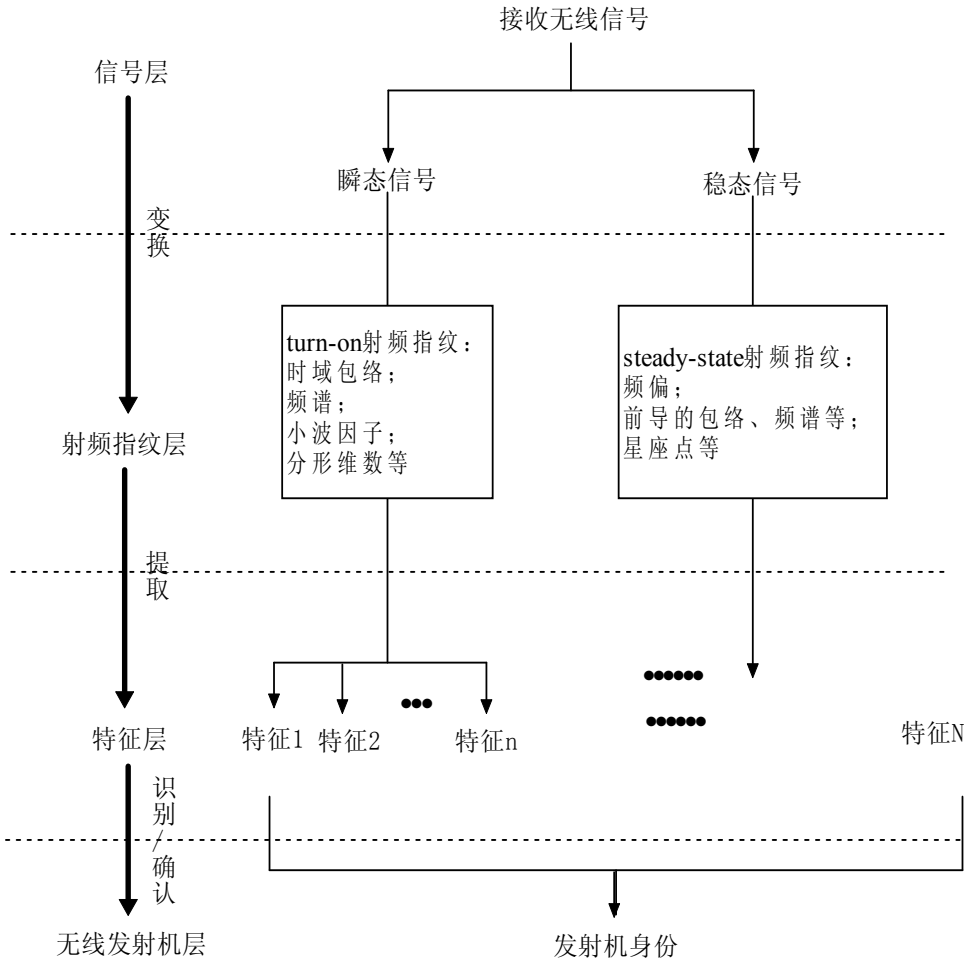

图 1.3 射频指纹识别的体系结构

如图1.3所示，可以把射频指纹识别的体系结构分为信号层、射频指纹层、特征层与待识别无线发射机层。同一个待识别无线发射机发送的无线信号，可以被从不同视角转换为多种射频指纹；而同一种射频指纹，可以从不同的视角抽取出不同的特征。射频指纹识别根据射频指纹的多个特征进行无线发射机的身份识别或确认，本文中称为“无线发射机的多射频指纹识别”。

如图1.3所示，当前文献中的射频指纹可以分为基于瞬态信号的turn-on射频指纹与基于稳态信号的steady-state射频指纹两类。射频指纹识别技术可以分为基于瞬态信号的射频指纹识别技术和基于稳态信号的射频指纹识别技术，分别介绍如下：

（1） 基于瞬态信号的射频指纹识别技术

基于瞬态信号的射频指纹识别是指截取后用于射频指纹变换的信号是接收无线信号的瞬态部分，即：无线设备处于发射机状态，其发射功率从0到达额定功率或从额定功率回到0过程时发射的信号部分。发射机发送瞬态信号的过程中，电容进行充放电，功率放大器渐升或渐降，频率综合器（如果存在）在稳定输出与无输出之间进行切换。

由于所有无线设备的发射信号都存在瞬态信号，因此，基于瞬态信号的射频指纹识别很早就受到了重视。瞬态信号被变换为时域包络、频谱、小波因子与分形维数等用于无线电发射机的识别[29, 30, 32-39, 41-43]。由于瞬态信号一般极其短暂，准确并且一致的瞬态

信号起始时刻检测对射频指纹识别的性能影响就极为关键。然而，这是极具挑战性的工作。已有的瞬态信号检测方法有门限检测、Bayesian阶跃改变检测与频域检测等。从已有文献看，当信噪比（Signal-to-noise ratio, SNR）较高并且起始时刻检测准确的情况下，小数量的无线设备测试集能获得较高的正确识别率。然而，大数量无线设备测试集，并且其中包含同一型号的多个无线设备时，低SNR条件下能否正确识别是一个不确定的问题。有文献称，基于瞬态信号的射频指纹识别基本无法正确识别同一厂家同一系列的无线设备[45]。

（2） 基于稳态信号的射频指纹识别技术

稳态信号是指接收无线信号的介于起始与结束瞬态信号之间的信号部分。近几年来，基于稳态信号的射频指纹识别得到了越来越多的重视，并且取得了较好的识别性能。

2008年，Kennedy, I. O.等首次进行了基于稳态信号的射频指纹识别研究。在该项研究中，通用移动通信系统(Universal Mobile Telecommunications System，UMTS) 的前导信号被变换为频谱并作为射频指纹用于UMTS用户设备的识别。实验室环境下，当SNR为15dB时，七个不同型号的UMTS用户设备能获得91%的正确识别率；而包含10个同一型号设备的共20个UMTS用户设备作为待识别对象时，识别率为85%[47]。

同年，Brik, V.等从IEEE 802.11b无线设备的稳态信号中抽取出频偏与星座点等调制域参数作为射频指纹。在一定的实验条件下，能以99%的高识别率对同一型号的130个无线网卡进行分类；并且声称对噪声、天线间距离改变及硬件老化具备稳健性。然而，该文献仅采用实验进行，未进行理论分析；并且，不能完全消除无线多径信道影响[45]。

同年，Suski, W. C.等变换前导OFDM信号为功率谱作为射频指纹用于Wi-Fi802.11a无线设备的识别研究，并展示了3个无线设备的概念性实验[51]。当SNR大于6dB时，可得到大于80%的正确识别率。

2009年及2010年，Klein, R. W. 采用双树复小波变换把IEEE 802.11a无线设备的前导信号变换为射频指纹用于其发射机识别。在低SNR下，识别率为80%时，能获得8dB的识别性能增益[56, 60]。

总之，由于基于稳态信号的射频指纹携带了更多的无线设备发射机的硬件信息，因而取得了更好的识别性能。然而，上述文献声称的识别性能是在一定的实验条件下获得的，这些实验条件离真正的应用条件还有距离，并且还有许多影响射频指纹稳定性的因素没有得到深入的研究。总之，根据射频指纹识别无线设备仍然是一个困难的问题。

尽管射频指纹识别的研究历史不长，并且相关文献较少，但最近的文献显示[3,4]：（1）无线网络的物理层安全方法得到了越来越多的重视；（2）基于射频指纹的非密码认证方法具有价值。文献[3]同时指出基于射频指纹的非密码认证方法具有以下缺点：（1）对“中间人”与“重放”攻击脆弱；（2）仅适用于静态的无线设备；（3）需要高端的射频指纹识别设备。然而，针对射频指纹的“中间人”与“重放”攻击仅在攻击者具备非常高端的任意信号发生器等设备时才能进行，这种攻击的成本极高，因而并不具备普遍的现实意义。在特定的应用场景下，基于射频指纹的物理层认证方法具有应用前景与研究价值。

1.2.3 相关技术及“射频指纹”特点

与“射频指纹识别”相关的技术有：雷达辐射源识别[62-72]与通信电台个体识别[73-96]等。国外从上世纪六十年代中期开始研究，取得了许多研究成果。近年来，国内多家单位开展了雷达与通信电台等辐射源的指纹识别研究，取得了许多进展。辐射源信号的个体特征被称为“辐射源指纹”，指附加在辐射源信号上的无意调制[68]。由于军事与商业秘密的原因，相关文献较少。根据公开文献，辐射源指纹识别研究主要有[72]：（1）基于信号参数特征的识别方法。此类方法采用的特征主要有传统的如载频、脉宽、重频、上升时间、下降时间及调制参数，以及分形维数特征等；（2）基于信号二维和高维变换域的识别方法。有关的变换主要有小波、时频分析核函数、双谱、模糊函数、余弦包变换、高阶谱及非线性动力学方法等；（3）基于信号中频波形或频谱；（4）基于发射机工作模式规律。研究射频指纹识别的国内其它单位基本没有。

与相关技术的待识别对象相比，射频指纹识别的待识别无线设备具有自身的特点，包括：（1）功率一般较小；（2）支持网络通信；（3）同一型号同一系列无线设备的数量一般较多等。这些特点决定了可以采用一些不同的方法进行射频指纹识别研究，例如：

（1）由于无线设备功率小，因而其非线性弱。当射频指纹识别系统滤除了发送信号的大部分非线性成分时，把剩下的带内非线性成分建模为噪声，则整个射频指纹识别系统可近似为线性系统。由于短时间内无线设备可近似为时不变，因而可以采用线性时不变系统理论对其进行研究。

（2）由于无线设备大都支持网络通信，其物理层帧格式一般由相关标准规定。所以，可以利用先验已知的物理层帧进行无线设备识别。例如，物理层帧的前导信号具备可比性，因而可变换为一种射频指纹用于无线设备的身份识别。

另外，待识别无线设备的自身特点也决定了射频指纹识别具有以下主要难点：

（1）射频指纹的可分离性及其影响因素。该概念与国防科大许丹博士提出的“可测性”概念类似[72]。由于同一无线网络内同一型号的无线设备众多，因而射频指纹的可分离性及其影响因素是一个重要问题。

（2）射频指纹的高精度检测方法。射频指纹的检测即接收无线信号的检测，这是射频指纹识别过程的重要一步[34]。利用无线网络中接收无线信号的特殊性，能否进一步提高检测性能，是一个值得研究的问题。

（3）具备独立性的射频指纹的变换方法。国防科大的许丹博士在雷达辐射源识别中提出了雷达指纹的“独立性”概念[72]，本文借用该概念，并强调具备独立性的射频指纹具有与射频信号中承载的数字信息无关的性质。

（4）射频指纹的稳健性。Danev B.在2009年的文献中的实验表明：两天线间距离、天线的方向角、电压等会对射频指纹产生影响[54]。射频指纹的稳定性指其对抗时变无线多径信道、天线间距离改变、天线方向改变、电压变化、温度变化、噪声及干扰等而保持的一致性性质。

（5）非线性问题。尽管线性是无线设备发射信号的主要性质，但非线性确实存在于无线设备的发送信号中。怎样从发送射频信号中提取出非线性信息，从而对无线设备进行识别是一个需要研究的问题。

（6）器件老化导致的射频指纹时变性问题。文献[45]显示，五个月期间内，射频指纹仍具有一致性，但元件的老化必然带来射频指纹的改变。与影响射频指纹稳定性的因素不同，老化引起的硬件性质改变是否可以作为一种射频指纹用于无线发射机的识别是一个值得探究的问题。另外，如何进行老化管理也是一个值得研究的问题。

（7）射频指纹的通用性。即射频指纹不随射频指纹识别系统中的接收机改变而变化的性质，也即射频指纹最大限度地仅与待识别无线发射机有关的性质。射频指纹具备通用性是射频指纹能够广泛应用的基础。

（8）天线极性对射频指纹识别性能的影响。天线极性的微小改变对射频指纹的影响是一个值得研究的问题。等等。

1.3 论文的研究内容与结构安排

本文针对“射频指纹识别”中存在的一些关键性基础问题进行了一些探索性研究。与大部分相关文献仅采用实验进行研究不同，本文力图以模型建立、理论分析与实验相结合的方法开展研究工作，研究内容与组织结构如下：

第二章建立了射频指纹识别系统的基本模型。首先给出一种通用的无线数字发射机结构；然后以此为基础对射频指纹的产生机理进行了分析，指出无线发射机的构件存在容差是射频指纹的主要产生机理，并采用实验进行了验证；接着建立了无线设备发送射频信号的模型，基于所建模型，对无线设备发送射频信号进行了非线性与时变性分析；然后提出射频指纹识别系统的一种基本模型，推导了该模型中接收无线信号的基带及带通理想等效形式。

第三章对数字化射频指纹的可分离性及其影响因素进行了研究。从两个角度对数字化射频指纹的可分离性进行了理论分析，推导了数字化射频指纹及其影响因素之间关系的解析式；该解析式也表明了模拟射频指纹的唯一性；接着构建了数字化射频指纹的可分离性与可分性度量；最后采用实验对本章得到的数字化射频指纹及其影响因素之间的关系结论进行了验证。

第四章对射频指纹识别中接收无线信号的检测方法进行了研究。首先介绍了基于Bayesian变点检测理论的Wi-Fi射频指纹Bayesian渐升变点检测方法；然后提出了基于Wi-Fi前导的Wi-Fi 射频指纹检测方法，并进行了实验验证。

第五章对射频指纹的变换方法进行了研究。首先对文献中已有的射频指纹变换方法进行了归类与分析，把射频指纹分为基于瞬态信号的 turn-on 射频指纹与基于稳态信号的 steady-state 射频指纹；接着提出了无线设备的“功率渐升前导射频指纹”的变换及其产生技术；然后提出了根据 Wi-Fi 前导射频信号重构的相空间识别 Wi-Fi 设备的方法；

再接着提出了BPSK信号的具备独立性、时间平移不变性与稳健性的射频指纹变换方法，包括“BPSK 基带倒谱射频指纹”与“BPSK 频偏对数谱射频指纹”变换方法；最后提出了基于 ARMA 系统模型系数的射频指纹变换方法，给出了理论推导与仿真实验。

第六章对本学位论文取得的研究成果进行了总结；根据取得的研究成果，得到了一定的结论，并指出进一步需要研究的问题。

第二章 射频指纹识别系统的基本模型

2.1 引言

严格来讲，任何电子元件都是非线性的，所以待识别无线设备发射机内部存在大量的非线性源。然而，由于人类目前认知能力的限制，在很多情况下把电子元件近似为线性也能得到精确解[99]。射频指纹识别系统的基本模型是后续研究的基础，没有文献对此进行过研究，把其建模为线性系统还是非线性系统，时变还是时不变系统，这些都是要考虑的问题。

本章首先介绍了一种通用无线数字发射机结构；接着分析了射频指纹的产生机理，并进行了软件仿真与实验验证；然后构建了无线设备的发送射频信号模型，对其非线性与时变性进行了分析；接着提出了射频指纹识别系统的一种基本模型、实验模型及等效模型；最后推导了接收无线射频信号的一种基带及带通理想等效形式。

2.2 一种通用无线数字发射机结构

一种采用正交调制技术的通用无线数字发射机结构如图2.1所示。

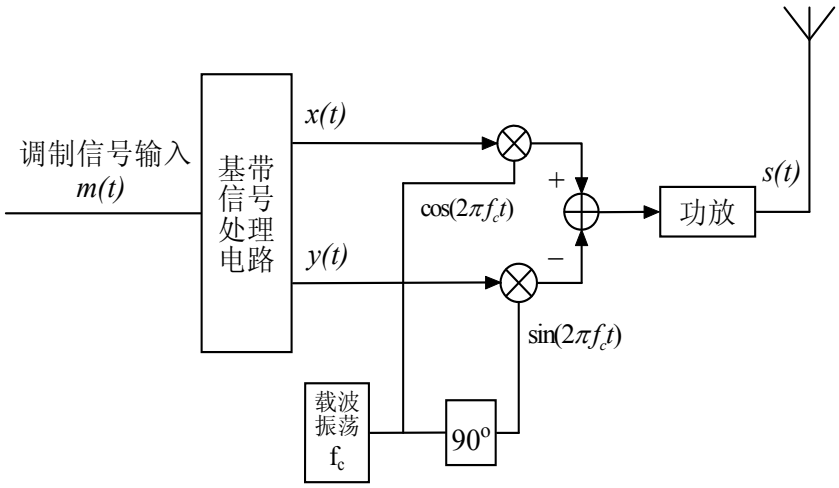

图 2.1 一种通用无线数字发射机结构

图 2.1 中 $m(t)$为待发送的调制信号，根据调制类型经基带信号处理电路产生两路基带信号 $x(t)$与 $y(t)$，再由正交调制电路生成射频已调信号经功放电路及天线发送到无线信道中。

2.3 射频指纹的产生机理

如图2.1所示通用无线数字发射机的内部元件都存在容差。文献[77]指出无线发射机

的电子元件容差效应是产生射频指纹的主要原因。电子元件容差可以分为制造容差与漂移容差。制造容差是指：元件制造过程中，由于生产精度不可能无限小，电子元件出厂时的实际值与标称值存在的差值。常用的百分比容差定义为：$\Delta X = \frac{|\text{实际值-标称值}|}{\text{标称值}} \times 100\%$，有±1%、±5%、±10%与±20%等。小于1%的容差也能获得，但这种器件的成本将显著增加。漂移容差是指：由于老化、温度、湿度、装配、压力、阳光、灰尘等因素导致的设备工作过程中元件值的变化。漂移容差一般等于甚至超过制造容差。元件总容差是制造容差与漂移容差之和。电子系统的器件总容差引起的同一设计的不同实现之间的性能差异称为容差效应。对于简单的电路，可以采用代数方法进行分析，即把电路中器件值用 $X' = X(1 \pm \Delta X)$ 代替，其中X表示了器件的标称值，器件容差ΔX度量了器件真实值与标称值之间的差异。例如一个简单的RC低通滤波器，截止频率是 $f_c = \frac{1}{2\pi RC}$。考虑了电阻R与电容C的容差后，滤波器的截止频率为 $f_c(1 \pm \Delta f_c) = \frac{1}{2\pi RC(1 \pm \Delta R)(1 \pm \Delta C)}$，也即 $1 \pm \Delta f_c = \frac{1}{(1 \pm \Delta R)(1 \pm \Delta C)}$。其中，$\Delta f_c$表示了由于电阻与电容参数容差引起的滤波器截止频率的漂移程度。从这个例子可以看出，对于同一个设计，即使使用同一精度的器件，系统输出也有可能不一样。

引起射频指纹的容差因素还包括印制电路板走线、集成电路内部元件与走线以及天线等无线发射机的所有构成成分。

无线发射机的容差效应导致即使同一型号同一系列的无线发射机的实际硬件参数也存在差异，包括：振荡器频偏、相位偏差、非线性失真等 —— 这是产生射频指纹的物质基础。

2.3.1 基于 ADS 的仿真实验

根据图2.1所示的通用无线数字发射机结构，基于Agilent公司的ADS（Advanced Design System）软件仿真环境，构建了射频指纹识别系统的仿真模型，包括待识别零中频发射机（图2.2）及射频指纹识别系统中的接收机（图2.3）。采用构建的该模型对射频指纹的产生机理进行了仿真验证。

图2.2是电路级的待识别零中频通信发射机，其中I路及Q路的数字速率分别为32Kbps，它们经过升余弦滤波器成形、功率放大器放大后进行QPSK调制，然后发射出去。图2.2中的IQ调制器（正交调制器）模块采用QPSK调制，其内部结构如图2.4所示，包括混频器（Gilbert）、功分器（Wilkinson）及移相器等；其中的Gilbert混频器电路如图2.5所示，其中的分立元件、走线等的参数值均设为随机变量。假设无线信道为高斯信道。对应的射频指纹识别系统中的接收机如图2.3所示。该接收机进行QPSK解调、低通滤波等。低通滤波后的基带信号送至Matlab进行射频指纹识别处理。

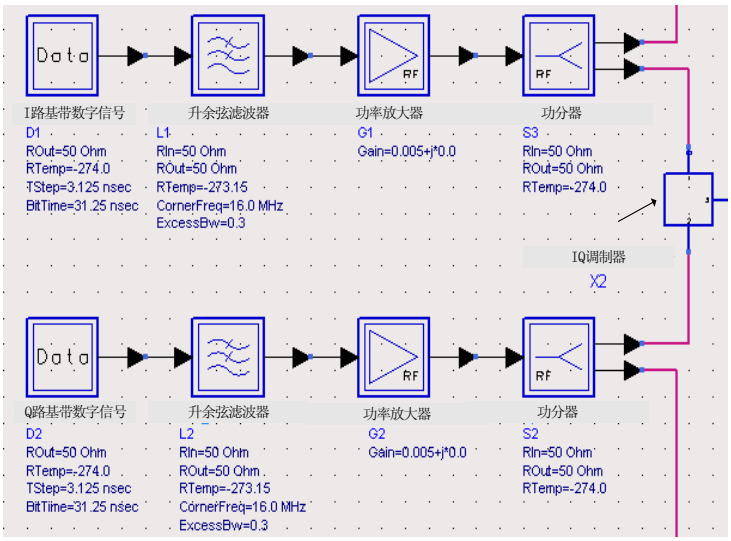

图 2.2 电路级零中频发射机

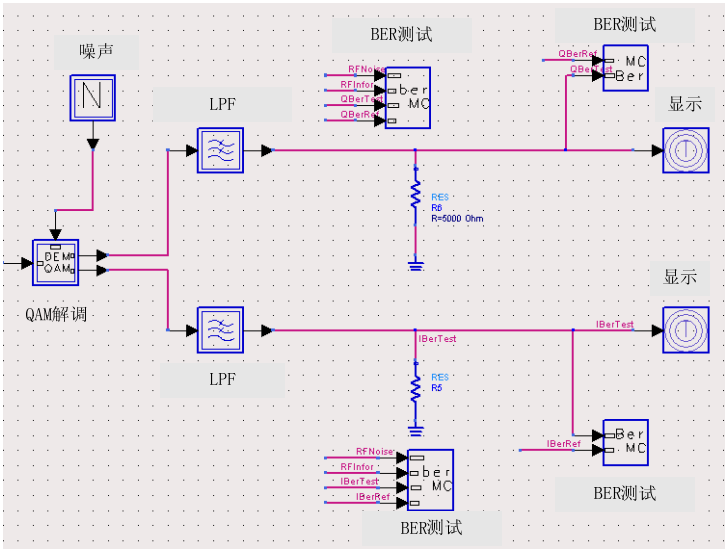

图 2.3 射频指纹识别系统中的接收机

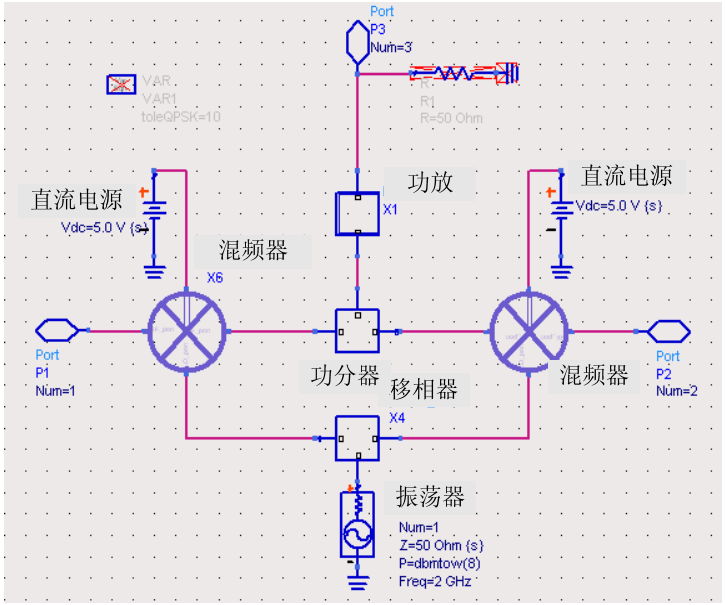

图 2.4 正交调制器内部结构

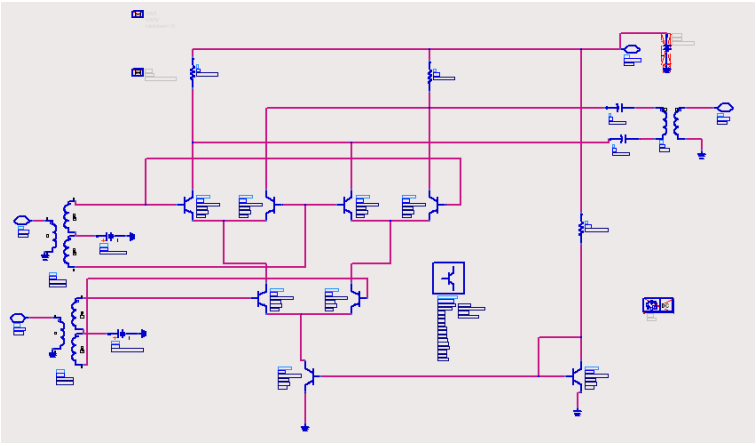

图 2.5 Gilbert 混频器电路图

把射频指纹识别系统仿真模型中待识别无线发射机的器件容差的概率性质设为高斯分布，R、L、C的容差级别设为±5%，进行Monte Carlo仿真。由于Monte Carlo仿真极其耗时，这里仅进行了10次仿真（相当于仿真了10个不同容差组合的待识别无线发射机），10次仿真的Q路基带信号如图2.6所示，其中子图（a）为人工延时了的Q路基带发送信号，而子图（b）为Q路接收基带信号。

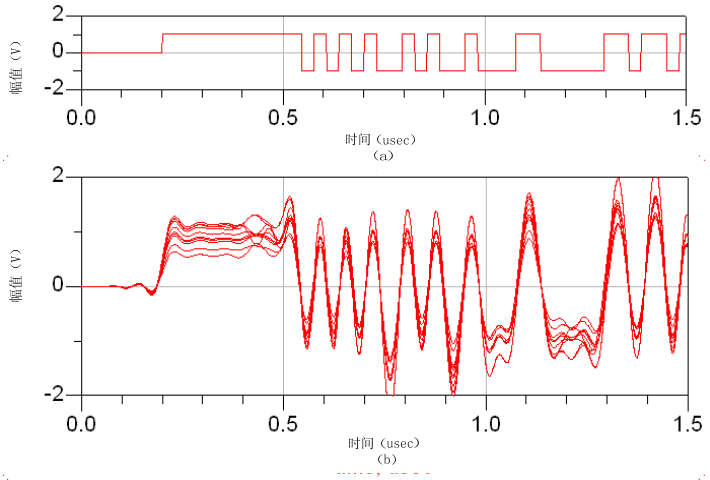

图 2.6 Q 路基带发送与接收信号

为防止元件容差导致待识别发射机的功能失效，同时进行了待识别发射机的误比特率（Bit Error Rate, BER）性能测试，结果如图2.7所示。图2.7中横轴Es/No为符号能量与噪声功率比，纵轴BER为误比特率。根据图2.7中可以看出，各次元件容差组合对应的BER没有大的变化。

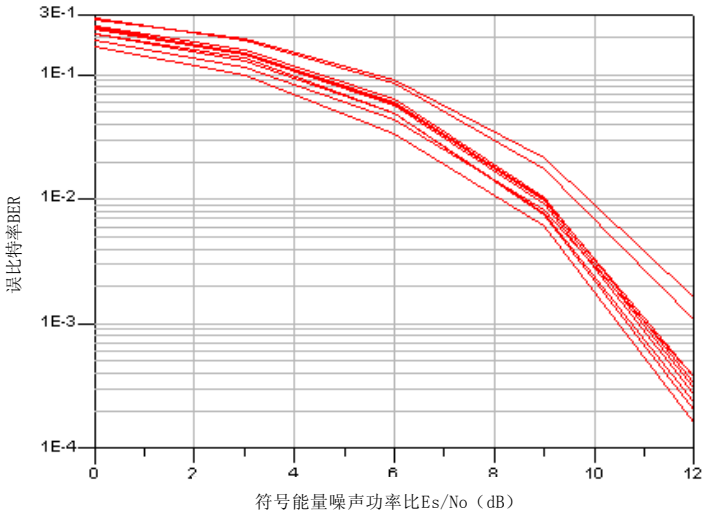

图 2.7 待识别发射机的 BER 性能

图2.6及图2.7中的每一条曲线对应所有电子器件容差的一个容差组合，相当于待识别无线发射机的一个实现。从图2.6与2.7中可以看出，即使是同一个型号同一系列的无线发射机，对于同样的基带发送信号，由于电子器件的容差效应，不同实现发射机的发送信号波形各不相同，因此，根据接收信号变换得到的射频指纹也有可能各不相同。该软件仿真实验验证了通信电子系统的电子器件容差是射频指纹主要产生机理的观点。

2.3.2 基于无线网卡的实验

基于无线网卡的射频指纹产生机理实验验证模型如图2.8所示。该模型由9只IEEE 802.11b无线网卡(三个型号，每个型号三只)、1个IEEE 802.11b无线接入点（AP）、2.4GHz天线、Agilent射频示波器（54854A）及计算机（PC）构成。2.4GHz天线安装在射频示波器上，实验时天线与IEEE 802.11b无线网卡位置固定，示波器采样率固定在20GSps，无插值处理，无线网卡的IEEE 802.11b的前导设定为“短”前导形式，无线信道设定为信道1（对应频率为2.412GHz），无线网卡端计算机PC通过无线网卡与无线AP通信，并通过有线网络Hub协调示波器端计算机PC进行射频信号的数据采集及处理。

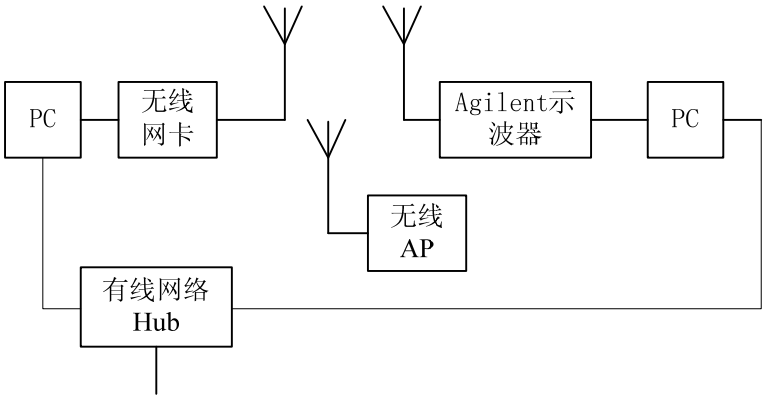

图 2.8 基于无线网卡的射频指纹产生机理实验验证模型

对9只无线网卡分别抓取IEEE 802.11b帧头，其中一个实例如图2.9所示。

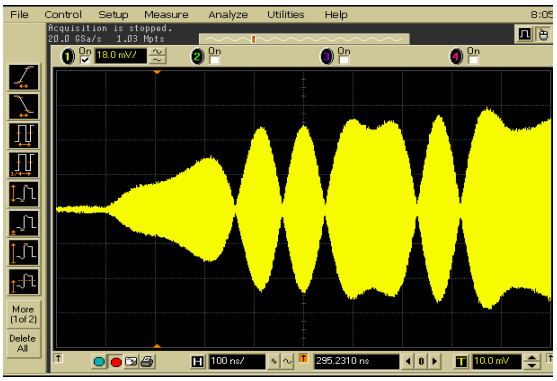

图 2.9 IEEE 802.11b 无线网卡的一个帧头实例

Hilbert 变换是一种生成实信号的复解析信号的技术，生成的复解析信号具有单边频谱，适合应用在射频指纹识别中。

用 $r(t)=A(t)\cos(2\pi f_c t+\varphi(t))$ 表示接收射频信号，对$r(t)$进行Hilbert变换，得到相应的复解析信号$y(t)$如式（2.1）所示。

$$\begin{aligned} y(t) &= r(t)+j\hat{r}(t) \\ &= A(t)\bullet e^{j(2\pi f_c t)}\bullet e^{j\varphi(t)} \end{aligned} \tag{2.1}$$

用f_o表示IEEE 802.11b规定的信道1频率（2.412GHz），对$y(t)$进行基于频率为f_o的复射频载波的软件下变频，得到中频复信号$R(t)$，如式（2.2）所示。

$$\begin{aligned} R(t) &= y(t)\bullet e^{-j2\pi f_o t} \\ &= A(t)\bullet e^{j2\pi f_c t}\bullet e^{j\varphi(t)}\bullet e^{-j2\pi f_o t} \\ &= A(t)\bullet e^{j2\pi\cdot\Delta f\cdot t}\bullet e^{j\varphi(t)} \end{aligned} \tag{2.2}$$

其中，$\Delta f=f_c-f_o$为实际发送射频信号频率与标准规定频率之间的频率偏差，从式（2.2）可知，Δf不影响中频复信号$R(t)$的包络$|R(t)|$，这里把$|R(t)|$作为一种IEEE 802.11b瞬态射频指纹。

9只无线网卡的IEEE 802.11b瞬态射频指纹各不相同，其中不同型号网卡瞬态射频指纹之间的差别较大，同一系列网卡瞬态射频指纹之间的差别相对较小。其中的三只同一系列IEEE 802.11b无线网卡的一个瞬态射频指纹样本如图2.10的3个子图（a）、（b）与（c）所示。

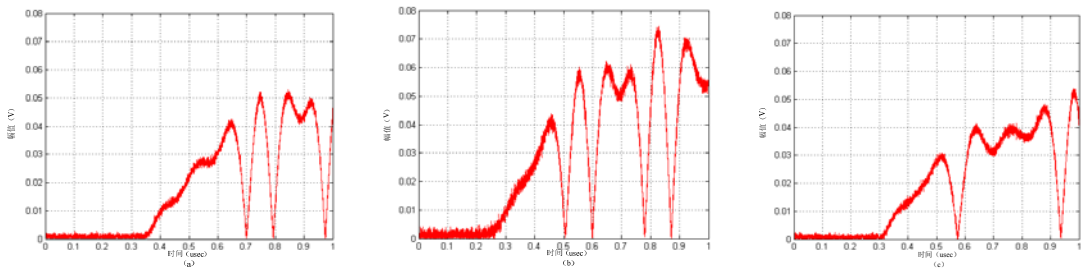

图 2.10 三只同一系列 IEEE 802.11b 无线网卡
的瞬态射频指纹样本

从图2.10可以看出，尽管无线设备的系统结构相同，元件标称值相同，发送数字信

号相同，无线信道条件相同，但由于元件容差的存在，不同无线设备的射频信号瞬态过程的包络却表现出明显的差异，从而验证了元件容差是产生射频指纹的主要原因的观点。

2.4 无线设备的射频信号模型

张贤达等在[100]中研究盲信道辨识与均衡时，把发射滤波器、传播信道与接收滤波器等效为“合成”信道，并假设为线性时不变系统进行研究。射频指纹识别中，能否进行类似的假设？本节对此进行研究。

IEEE 802.11b规定其发射机的频率偏差为标准频率的±25 ppm，则当无线信道为信道1（2.412GHz）时，最大频偏为60.3KHz。另外规定，当

$$f_c - 22MHz < f < f_c - 11MHz \tag{2.3}$$

与

$$f_c + 11MHz < f < f_c + 22MHz \tag{2.4}$$

时；发射功率谱应低于-30dBr（相对于sin(x)/x峰值的dB值）。当

$$f < f_c - 22MHz \tag{2.5}$$

与

$$f > f_c + 22MHz \tag{2.6}$$

时；发射功率谱应低于-50dBr；f_c为信道中心频率。

一个采用带宽为13GHz的射频示波器采集的IEEE 802.11b射频信号帧（信道1、采集时进行了最大限度的电磁屏蔽）如图2.11所示，采样率设为10GSps。其中上子图是一个完整Ad-hoc帧，下子图是其头部的局部放大图。

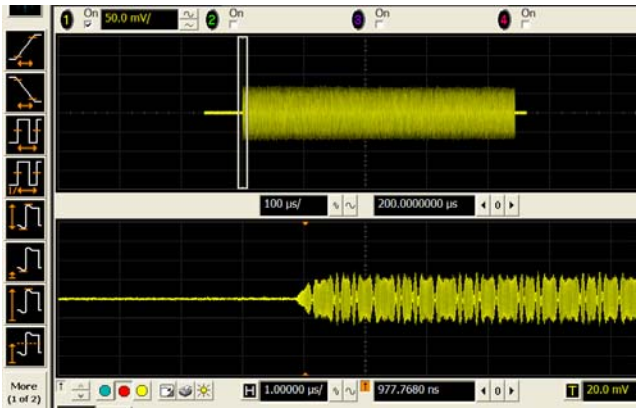

图 2.11 一个 IEEE 802.11b 射频信号帧

采用基于Welch的平均周期图法对图2.11所示IEEE 802.11b完整帧进行功率谱估计，结果如图2.12所示。图2.12中子图（b）是子图（a）的带内部分的局部放大图。该发射机的信道中心频率约为f_c=2.412GHz，并且带内功率主要集中在

$$f_c - 11MHz < f < f_c + 11MHz \tag{2.7}$$

内，这与IEEE 802.11b标准相符。

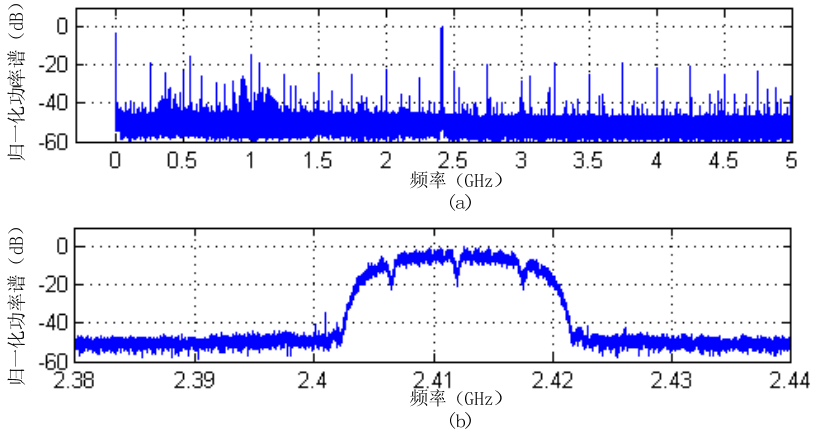

图 2.12 一个 IEEE 802.11b 射频信号帧的功率谱

但同时从图2.12的子图（a）可以看出，IEEE 802.11b射频信号含有除带内成分外的非线性等其它成分。假设射频指纹识别系统滤除了带内有效成分之外的其它成分，那么带内是否还含有非线性成分？如果有，带内的非线性成分有多少？下面对无线设备发送射频信号的非线性与时变性进行研究。

2.4.1 无线设备发送射频信号的非线性分析

尽管严格来讲，无线设备发射机的元件都具有非线性，但功率放大器（Power Amplifier，简称PA）是主要的非线性器件。这里，假设仅考虑PA的非线性，则无线设备发射机的等效模型如图2.13所示。

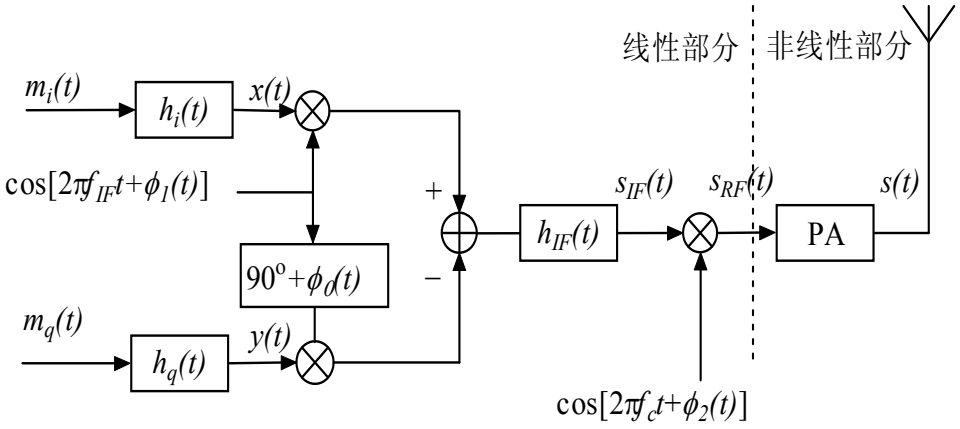

图 2.13 无线设备发射机的等效模型

图2.13中的中频信号 $s_{IF}(t)$ 的表达式为

$$\begin{aligned} s_{IF}(t) = BPF_{IF}\{&m_i(t)*h_i(t)\bullet\cos[2\pi f_{IF}t+\phi_1(t)] \\ &-m_q(t)*h_q(t)\bullet\sin[2\pi f_{IF}t+\phi_0(t)+\phi_1(t)]\} \end{aligned} \tag{2.8}$$

式（2.8）中的 $BPF_{IF}\{\bullet\}$ 表示单位冲激响应为 $h_{IF}(t)$ 的中频滤波器的滤波处理；* 表示卷积运算；$m_i(t)$和$m_q(t)$分别是无线设备发送基带数字序列的等效信号，表示为

$$m_i(t)=\sum_{k=0}^{\infty} i_k \delta(t-kT_b) \tag{2.9a}$$

与

$$m_q(t)=\sum_{k=0}^{\infty} q_k \delta(t-kT_b) \tag{2.9b}$$

其中i_k与q_k分别是I路与Q路发送的数字序列，取值为±1；T_b为数字比特周期；$h_i(t)$与$h_q(t)$分别是I路与Q路混频器之前及含混频器幅度偏差的电路等效系统冲激响应，包含发送基带数字序列的时间偏移、混频器的幅度偏差、I路与Q路的相位差等因素；f_{IF}为中频频率；$\phi_0(t)$是I路与Q路的相位偏差，$\phi_1(t)$是载波相位噪声。

图2.13中中频信号$s_{IF}(t)$经上变频后的射频信号

$$s_{RF}(t)=s_{IF}(t)\bullet\cos[2\pi f_c t+\phi_2(t)] \tag{2.10}$$

其中f_c为射频频率；$\phi_2(t)$是射频载波相位噪声。

图2.13中射频信号$s_{RF}(t)$经功率放大器PA后的射频发送信号

$$s(t)=g[S_{RF}(t)] \tag{2.11}$$

其中，$g[\bullet]$表示PA的输入-输出非线性关系，式(2.10)可以写成

$$\begin{aligned} s(t)&=g[S_{RF}(t)]\\ &=\sum_{n=1}^{\infty} s_{RF,n}(t) \end{aligned} \tag{2.12}$$

其中

$$s_{RF,n}(t)=a_n {s_{RF}}^n(t) \tag{2.13}$$

是各次幂级数，a_n是n次幂级数系数，a_1表示PA的线性增益，a_n（n>1）表示PA的非线性强度。如果$s(t)$是平稳的，则发送射频信号$s(t)$的自相关为

$$R_s(\tau)=E\{s(0)s(\tau)\}=\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} a_m a_n R_{s_{RF}}(\tau;m,n) \tag{2.14}$$

其中，$R_{s_{RF}}(\tau;m,n)=E\{s_{RF}^m(0)s_{RF}^n(\tau)\}$是输入信号$s_{RF}(t)$的 m+n 阶联合矩；而$R_s(\tau)$的傅立叶变换是输出信号$s(t)$的功率谱。由于傅立叶变换是线性变换，因此，$s(t)$功率谱的性质与其自相关性质相同。

由于无线设备功率小，所以呈现弱非线性，假设忽略三阶矩以上成分；由于二阶矩对带内无贡献，因此忽略二阶矩；则输出自相关函数为：

$$\begin{aligned} R_s(\tau)&=E\{[s_{RF,1}(0)+s_{RF,3}(0)][s_{RF,1}(\tau)+s_{RF,3}(\tau)]\}\\ &=E\{s_{RF,1}(0)s_{RF,1}(\tau)\}+E\{s_{RF,1}(0)s_{RF,3}(\tau)\}\\ &+E\{s_{RF,3}(0)s_{RF,1}(\tau)\}+E\{s_{RF,3}(0)s_{RF,3}(\tau)\} \end{aligned} \tag{2.15}$$

式（2.15）中第一项是线性成分$s_{RF,1}(t)$的自相关，对应带内线性成分；第二项与第三项是三次谐波与线性成分的互相关，对应带内失真；第四项是三次谐波的自相关，对应带外谱增长。

由式（2.15）可知，弱非线性的无线设备发送的射频信号带内存在非线性成分；这种带内非线性成分导致无线设备的发送波形失真。然而，相关标准规定波形失真必须在一定范围内，例如，IEEE 802.11b定义了误差向量幅度（Error Vector Magtitude，EVM）度量调制误差，并规定EVM最差不能超过35%。

所以，无线设备发送的射频信号是非线性的[101, 102]；通过带通滤波器滤除带外成分后，其带内仍存在一定的非线性成分。

2.4.2 无线设备发送射频信号的时变性分析

待识别无线设备发射机的构件存在漂移容差。然而，构件漂移容差引起的构件参数值改变是缓慢的；因此，短时间内，可把其建模为时不变量。

另外，无线通信的飞速发展对可用频谱资源提出了越来越高的要求，这种要求反过来对通信系统振荡器的频率稳定度提出了越来越高的要求。因此，振荡器的相位噪声正向越来越小的方向发展[103]。所以，无线设备的振荡器频率可近似为短时间内的时不变量。

文献[45]的实验显示，五个月内，无线设备的包括频偏等在内的射频指纹仍具有稳定性。无线设备的射频指纹是由无线设备发送的射频信号变换而来，因此，可把射频指纹识别中无线设备发送的射频信号建模为短时间内的时不变量。

2.5 射频指纹识别系统的基本模型

射频指纹识别系统的目的是根据接收的无线设备发送的射频信号，识别或确认该射频信号是由哪一个特定无线设备发射的。射频指纹识别系统的一种基本模型如图2.14所示。

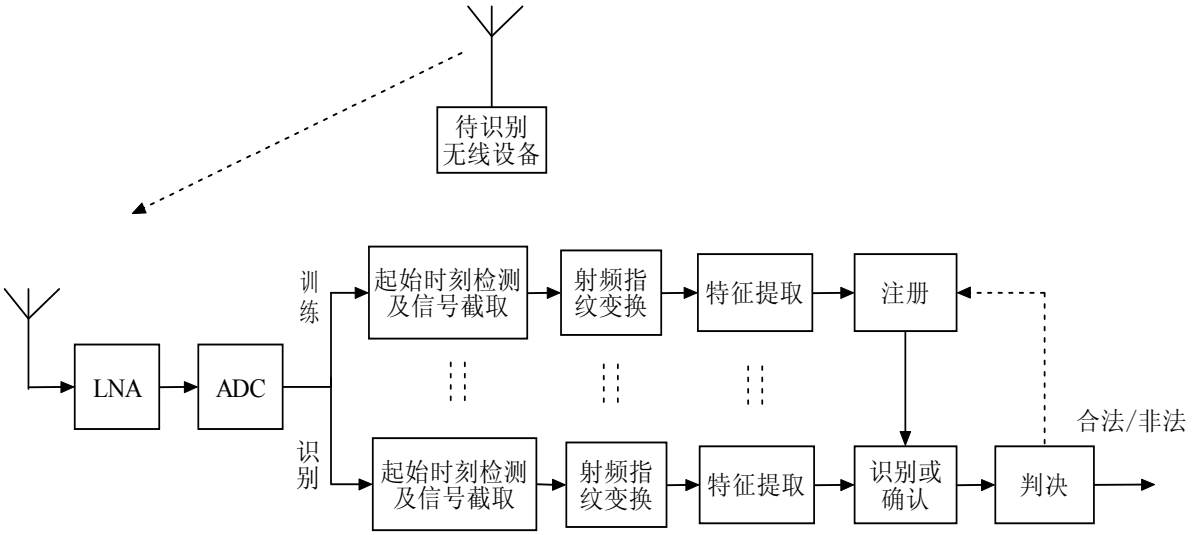

图 2.14 射频指纹识别系统的一种基本模型

如图2.14所示，接收天线接收待识别无线设备发送的微弱射频信号，经低噪声放大

器（Low Noise Amplifier，简称LNA）放大后进行模数转换（ADC），然后分别进入训练与识别阶段。在训练阶段，把射频指纹特征与无线设备进行注册，而识别阶段根据待识别无线设备的射频指纹特征与注册无线设备的射频指纹特征进行比对，从而对待识别无线设备是否合法进行判决。

本文采用的实验模型如图2.15所示。

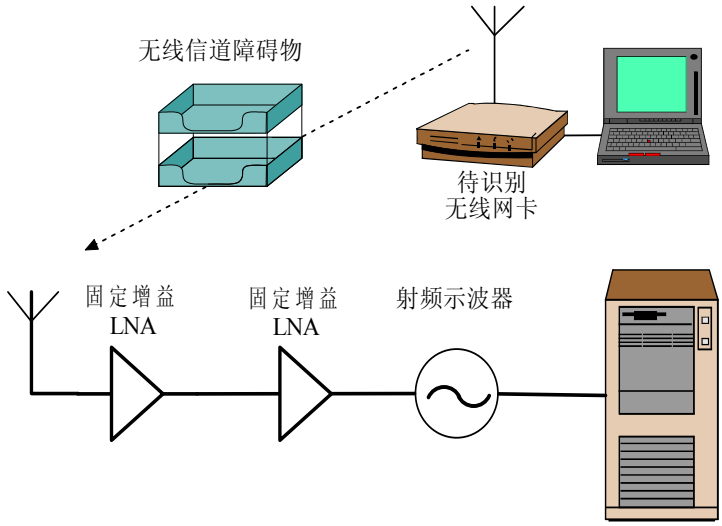

图 2.15 射频指纹识别系统的实验模型

如图2.15所示，外置式待识别无线网卡由笔记本电脑控制，不断发送射频信号帧；接收天线（定向或全向）接收的信号经固定增益LNA放大后送到射频示波器，示波器采集到无线射频信号后再经过网口送至计算机进行基于Matlab和Simulink的软件处理。图2.15中的无线信道障碍物用于改变无线信道的多径状态。

图2.15所示射频指纹识别系统实验模型的等效模型如图2.16所示。

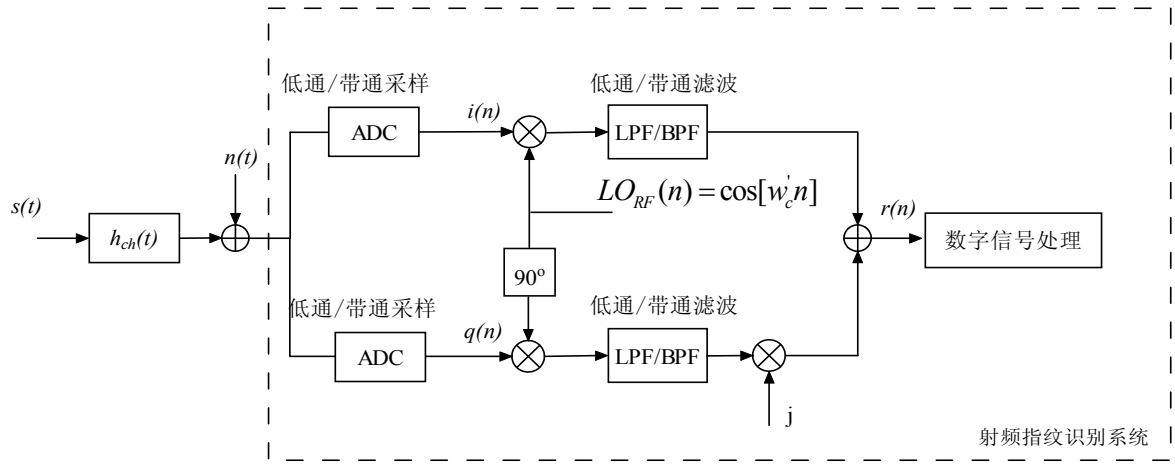

图 2.16 射频指纹识别系统的等效模型

图2.16中$h_{ch}(t)$为无线多径信道的单位冲激响应，$n(t)$是加性高斯白噪声（Additive White Gaussian Noise，简称AWGN），主要由LNA与射频示波器产生。如图2.16所示，待识别无线设备发送的射频信号$s(t)$经无线信道后由AWGN噪声叠加，然后进行低通或带通采样；接着进行基于正交下变频的处理：首先经频率为w_c'的数字载波的正交下变频，然后

根据感兴趣的频带进行低通滤波或带通滤波，把I路信号与Q路信号合并成复信号$r(n)$；最后对$r(n)$进行起始时刻与信号截取、射频指纹变换、特征提取与分类识别等数字信号处理。其中，滤波采用低通或者带通取决于感兴趣的频带及ADC形式。

2.6 接收无线信号的理想等效形式

假设图2.13中的中频滤波器为理想带通滤波器，并且忽略振荡器的相位噪声，则图2.13中的无线发射信号$s(t)$可表示为

$$s(t)=\mathrm{Re}\{s_l(t)e^{j2\pi(f_c+f_{IF})t}\} \tag{2.16}$$

其中$s_l(t)$为$s(t)$的低通等效

$$s_l(t)=g\{a(t)\}e^{j\{\varphi(t)+f[a(t)]\}} \tag{2.17}$$

式中，$g\{\bullet\}$与$f[\bullet]$表示PA的“幅度-幅度”与“幅度-相位”非线性性质；$a(t)$是已调中频信号的包络

$$a(t)=\sqrt{[x(t)-y(t)\sin(\phi_0)]^2+[y(t)\cos(\phi_0)]^2} \tag{2.18}$$

$\varphi(t)$是已调中频信号的相位

$$\varphi(t)=\arctan\{\frac{y(t)\cos(\phi_0)}{x(t)-y(t)\sin(\phi_0)}\} \tag{2.19}$$

式（2.18）与（2.19）中$x(t)$为

$$x(t)=m_i(t)*h_i(t) \tag{2.20}$$

而$y(t)$为

$$y(t)=m_q(t)*h_q(t) \tag{2.21}$$

无线多径信道的单位冲激响应可表示为[123]

$$h_{ch}(t)=2\,\mathrm{Re}\{c_l(t)e^{j2\pi(f_c+f_{IF})t}\} \tag{2.22}$$

其中，无线多径信道的低通等效

$$\begin{aligned}c_l(t)&=\sum_n\alpha_n e^{-j2\pi(f_c+f_{IF})\tau_n}\delta(t-\tau_n)\\&=\sum_n\alpha_n[\cos(2\pi(f_c+f_{IF})\tau_n)-j\sin(2\pi(f_c+f_{IF})\tau_n)]\delta(t-\tau_n)\\&=c_i(t)-jc_q(t)\end{aligned} \tag{2.23}$$

其中

$$c_i(t)=\sum_n\alpha_n\cos(2\pi(f_c+f_{IF})\tau_n)\delta(t-\tau_n) \tag{2.24}$$

$$c_q(t)=\sum_n\alpha_n\sin(2\pi(f_c+f_{IF})\tau_n)\delta(t-\tau_n) \tag{2.25}$$

假设接收端 AWGN 噪声表示为

$$n(t) = \mathrm{Re}\{n_l(t)e^{j2\pi(f_c+f_{IF})t}\} \tag{2.26}$$

其基带等效

$$n_l(t) = n_x(t) + jn_y(t) \tag{2.27}$$

假设射频指纹识别系统中用于正交下变频的载波频率 $f_c^{'} = f_c + f_{IF} + \Delta f$，其中 Δf 为正交下变频载波频率与实际接收无线射频信号频率之间的频率偏差，则接收无线信号的理想等效形式可表示为

$$r_l(t) = [s_l(t) * c_l(t) + n_l(t)] \bullet e^{j \bullet 2\pi \bullet \Delta f \bullet t} \tag{2.28}$$

设无线设备相关标准规定的最大频率偏差为f_m；例如，IEEE 802.11b/g规定其发射机的频率偏差为标准频率的±25 ppm，则当无线信道为信道1（2.412GHz）时，最大频偏为60.3KHz，即f_m=60.3KHz。本文把 $0 \le \Delta f < f_m$ 时的式（2.28）称为接收无线射频信号的理想基带等效形式，而把 $\Delta f \ge f_m$ 时的式（2.28）称为接收无线射频信号的理想带通等效形式。式（2.28）在第五章的“BPSK基带倒谱射频指纹变换”与“BPSK频偏对数谱射频指纹变换”中得到了应用。

2.7 本章小结

本章研究了通用无线数字发射机结构、射频指纹的产生机理、无线设备发送射频信号的模型、射频指纹识别系统的基本模型及其接收射频信号的理想等效形式等。

根据无线发射机硬件参数改变缓慢以及现代无线数字发射机的特征，可把待识别无线发射机、无线信道与射频指纹识别系统等效为含非线性PA的一定时间之内的时不变系统；当经处理后的接收无线信号非线性较弱时，可近似为线性系统；则该等效系统可建模为线性时不变系统。同时，该系统也可建模为非线性时不变系统等。

本章内容是后续研究的基础。

第三章 数字化射频指纹的可分离性及其影响因素

3.1 引言

正如“世界上没有两片相同的树叶”，从哲学上讲，任意两个不同无线设备发送的射频信号都是唯一的。所以，根据其接收信号变换得到的射频指纹也可能是唯一的。

然而，数字化接收信号过程中的采样与量化模糊了接收信号及其射频指纹的差异性，导致数字化射频指纹的可分离性存在不确定性。“数字化射频指纹的可分离性”指两数字化射频指纹存在类间距离的性质，国内工程领域对此尚存在争议[72]。文献[87]基于 28 个无线电设备，把接收机基带信号的瞬时幅度与相位作为射频指纹特征，研究了数字化射频指纹的唯一性（uniqueness，实际为可分离性），指出“许多无线发射机确实存在不同的特征，但是，识别同一型号同一系列的无线发射机很困难”。同一型号同一系列无线发射机的识别类似于生物特征识别中的孪生兄弟的识别。生物特征识别中，孪生兄弟的数量有限，而同一型号同一系列的无线发射机的数量却一般十分巨大，所以数字化射频指纹的可分离性研究必要且重要。然而，只有文献[87]对此进行过实验性研究。

另外，寻找新的数字化射频指纹时应依据何种准则对接收无线信号进行变换是一个需要解决的问题，同时，相关研究文献一般把相同型号无线设备的识别性能作为其数字化射频指纹质量的评价方法。当实际可得实验条件有限时，不同型号无线设备的识别性能是否能作为其数字化射频指纹的另一个质量评价方法也是一个需要回答的问题。

为了研究射频指纹的可分离性，本章基于第二章构建的射频指纹识别系统模型，首先构建了射频指纹的一种抽象模型；然后从两个角度研究了数字化射频指纹的可分离性及其影响因素之间的关系。其中，定义了数字化射频指纹的可分离性度量，据此推导出数字化射频指纹可分离性及其影响因素之间关系的解析式。

3.2 射频指纹的一种抽象模型

根据第二章无线设备发送射频信号模型的研究可知，无线设备发送的射频信号可表示为抽象形式

$$s(t) = F_1\{m_i(t), h_i(t), m_q(t), h_q(t), f_{IF}, \phi_1(t), \phi_0(t), h_{IF}(t), f_c, \phi_2(t), g[\bullet]\} \tag{3.1}$$

式（3.1）中，$F_1\{\bullet\}$表示某个确定的函数，$m_i(t)$与 $m_q(t)$是等效基带发送信号，$h_i(t)$与 $h_q(t)$是待识别无线设备发射机I路与Q路硬件的等效系统冲激响应，f_{IF}是调制载波频率，$h_{IF}(t)$是带通滤波器的的单位冲激响应，f_c与f_{IF}分别是射频载波频率与中频频率，$\phi_0(t)$是I路

与 Q 路的相位偏差，$\phi_1(t)$ 与 $\phi_2(t)$ 是载波的相位噪声，$g[\bullet]$ 是 PA 的输入-输出非线性关系。

假设 $T\{\bullet\}$ 为理想的射频指纹变换，即 $T\{\bullet\}$ 去除了待识别发射机的所有非硬件因素的影响，则 $s(t)$ 经 $T\{\bullet\}$ 变换后得到的射频指纹可表示为

$$\begin{aligned} &RFF(x) = T\{s(t)\} \\ &= F_2\{h_i(t), h_q(t), f_{IF}, \phi_1(t), \phi_0(t), h_{IF}(t), f_c, \phi_2(t), g[\bullet],\} \\ &= F_3\{V_k, k = 1,2,3,...\} \end{aligned} \tag{3.2}$$

其中，$F_2\{\bullet\}$ 与 $F_3\{\bullet\}$ 表示确定的函数，V_k, k=1,2,3,…表示待识别无线设备发射机硬件的等效构件值；$RFF(x)$ 表示某个射频指纹，x 表示射频指纹的自变量。

$F_2\{\bullet\}$ 的所有参量都是由待识别无线设备发射机的结构与其构件参数的等效值 V_k 确定。由于构件容差现象的存在，即使无线发射机的结构与构件标称值都相同，它们的各参量也各不相同，因此 V_k 是随机变量。从这个角度看，$RFF(x)$ 也各不相同。

例如，当 $RFF(x)$ 为待识别发射机的频偏时，此时 $RFF(x)$ 为一维射频指纹；当 $m_i(t)$ 与 $m_q(t)$ 为单位阶跃信号时，s(t)的瞬态信号包络即一种 turn-on 射频指纹[30]，此时 x 为连续时间变量，$RFF(x)$ 为无限维射频指纹；当 $m_i(t)$ 与 $m_q(t)$ 为物理层帧前导信号时，s(t)的功率谱即一种 steady-state 射频指纹[51]，此时 x 为连续频率变量，$RFF(x)$ 为无限维射频指纹。这些射频指纹实例同时也表明了：（1）射频指纹体现待识别发射机的硬件性质并具备可比性；（2）构件容差是射频指纹的产生机理。

3.3 数字化射频指纹的可分离性分析一

把射频指纹识别系统中的待识别无线发射机的所有电子元件等效为一个元件，元件值用 c 表示。c 是无线发射机的大量的相互独立的电子元件的等效参数值，由于构件容差的存在，不同待识别无线发射机的 c 可建模为随机变量。设随机变量 c 的概率密度函数近似服从正态分布，用 c_{nom} 表示元件标称值，用 Δc 表示电路等效元件的容差，则等效元件 c 为以 c_{nom} 为均值，在 $(c_{nom}-\Delta c, c_{nom}+\Delta c)$ 内近似服从正态分布的随机变量。假设其概率密度函数如图 3.1 所示，用 $pdf(c)$ 表示 c 的概率密度函数，$c_k, k = 0,2,...,M-1$ 表示元件离散值，其中 $c_0 = c_{nom} - \Delta c$，$c_M = c_{nom} + \Delta c$。

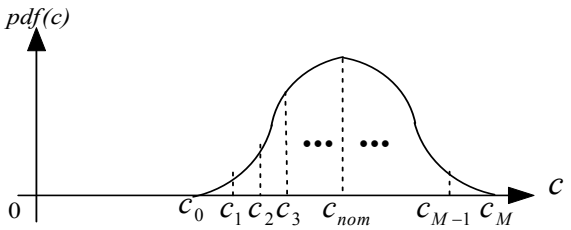

图 3.1 无线发射机等效元件的概率密度函数

假设射频指纹识别系统的简化等效模型如图 3.2 所示，系统模型由线性的“合成信道”部分与 ADC 采样量化部分组成。

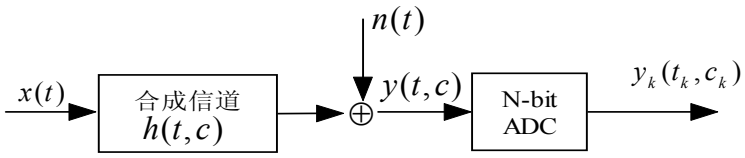

图 3.2 射频指纹识别系统的简化等效模型

图 3.2 中，$x(t)$ 表示发射机的基带发送信号，c 表示射频指纹识别系统的等效元件参数值，$h(t,c)$ 表示“合成信道”的冲激响应，$n(t)$ 表示 AWGN 噪声，$y(t,c)$ 表示射频指纹识别系统中接收机的接收信号。$y(t,c)$ 是发射机基带发送信号与“合成信道”系统冲激响应的卷积与噪声信号之和

$$y(t,c)=x(t)*h(t,c)+n(t) \tag{3.3}$$

$y(t,c)$ 经 N-bit 模数转换（采样量化）后的信号用 $y_k(t_k,c_k)$ 表示，$k=0,1,...$ 表示离散时间采样点，$t_k=kT_s$ 为采样时刻，T_s 为采样间隔，y_k 为“合成信道”系统输出的量化值，c_k 为 y_k 对应的元件量化值。

设有 N 个待识别无线发射机，用 $i,j(i,j=1,2,...,N;i\neq j)$ 表示 N 个无线发射机中的任意两个发射机序号，则任两台无线发射机接收信号的类间距离可定义为

$$Dist(i,j)=\sum_k (y_k(t_k,c_{ki})-y_k(t_k,c_{kj}))^2 \tag{3.4}$$

其中，c_{ki} 表示待识别发射机 i 的等效元件参数值，c_{kj} 表示待识别发射机 j 的等效元件参数值。则“射频指纹可分离”等效于

$$Dist(i,j)>DIST_{\min} \tag{3.5}$$

其中 $DIST_{\min}$ 为射频指纹的最小可分离距离。

用“任意两个射频指纹间存在类间距离的概率”度量“射频指纹的可分离性”，则“射频指纹不可分离的概率”为

$$P\{Dist(i,j)\le DIST_{\min}\} \tag{3.6}$$

假设理想的最小可分离距离 $DIST_{\min}$ 为零，根据式（3.4）类间距离的定义，$DIST_{\min}\ge 0$，则“RFF 不可分离的概率”为

$$P\{Dist(i,j)\le DIST_{\min}\}=P\{Dist(i,j)=0\} \tag{3.7}$$

由式（3.4）可知

$$P\{Dist(i,j)=0\}=\prod_k P\{y_k(t_k,c_{ki})=y_k(t_k,c_{kj})\} \tag{3.8}$$

即事情“任两射频指纹距离为 0”等价于事情“任两射频指纹的每个采样量化值都相等”。假设任意两射频指纹信号的激励 $x(t)$ 与噪声 $n(t)$ 相同；由于待识别发射机为同种型号，因而假设包含等效元件的“合成信道”系统的冲激响应满足

$$\begin{aligned}&P\{h(t_k,c_{ki})=h(t_k,c_{kj})\}\\&=P\{c_{ki}=c_{kj}\}\end{aligned} \tag{3.9}$$

则“任两射频指纹距离为 0 的概率”为

$$\begin{aligned}&\prod_k P\{y_k(t_k,c_{ki})=y_k(t_k,c_{kj})\}\\&=\prod_k P\{h(t_k,c_{ki})=h(t_k,c_{kj})]\}\\&=\prod_k P\{c_{ki}=c_{kj}\}\\&=P\{c_{ki}=c_{kj}\},k=0,1,2,...\end{aligned} \tag{3.10}$$

即命题“任意两射频指纹采样量化值相等”与命题“任意两系统冲激响应的每个采样量化值相等”等价；又与命题“任意两元件值的等效采样量化值相等”等价。

根据式（3.10），用 1LSB 表示 ADC 能够分辨的“合成信道”系统输出 $y(t,c)$ 的最小变化量，用 Δc_{lsb} 表示 1LSB 对应的元件值的最小变化量，简称为“元件等效量化间隔”。则元件参数值 c 的等效量化级数为 $M=\dfrac{2\Delta c}{\Delta c_{lsb}}$，由图 3.1 可知，元件等效量化值 c_k 的概率质量函数为

$$P\{c_k=c_m\}=\int_{c=c_m}^{c_{m+1}} pdf(c)dc, m=0,1,...,M-1 \tag{3.11}$$

其中 $c_m=m\Delta c_{lsb}, m=0,1,...,M-1$ 为元件离散值。由于不同待识别无线发射机的元件是独立同分布的随机变量，因此式（3.10）为

$$\begin{aligned}&\prod_k P\{y_k(t_k,c_{ki})=y_k(t_k,c_{kj})\}\\&=P\{c_{ki}=c_{kj}\}\\&=\sum_{m=0}^{M-1} P\{c_{ki}=c_m\}P\{c_{kj}=c_m\}\\&=\sum_{m=0}^{M-1}\left(\int_{c=c_m}^{c_{m+1}} pdf(c)dc\right)^2\end{aligned} \tag{3.12}$$

从式（3.12）不易看出其物理意义，假设把 c 的概率密度函数 $pdf(c)$ 近似为如图 3.3 所

示的三角形分布

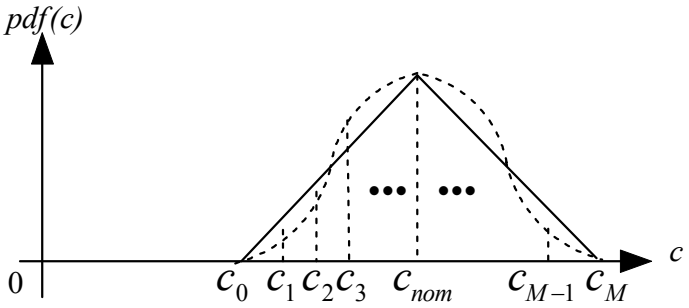

图 3.3 三角形概率密度函数分布

并假设 M 为偶数，则式（3.12）为式（3.13）（推导见附录 A）

$$\begin{aligned} &P\{Dist(i,j) \le DIST_{\min}\} \\ &= P\{y_k(t_k, c_{ki}) = y_k(t_k, c_{kj})\} \\ &= \sum_{m=0}^{M-1} \left(\int_{c=c_m}^{c_{m+1}} pdf(c)dc \right)^2 \\ &= \frac{1}{3}\left[\frac{1}{M} - \left(\frac{1}{M}\right)^3\right] \end{aligned} \tag{3.13}$$

则射频指纹的可分离性度量“任意两个射频指纹间存在类间距离的概率”为

$$\begin{aligned} &P\{Dist(i,j) > DIST_{\min}\} \\ &= 1 - P\{Dist(i,j) \le DIST_{\min}\} \\ &= 1 - \frac{1}{3M} + \frac{1}{3}\left(\frac{1}{M}\right)^3 \end{aligned} \tag{3.14}$$

从式（3.14）$P\{Dist(i,j) > DIST_{\min}\} \le 1$ 可知 $M^2 \ge 1$；又 $M = \dfrac{2\Delta c}{\Delta c_{lsb}} > 0$，所以 $M \ge 1$，即 $\Delta c_{lsb} \le 2\Delta c$ 是“任意两个射频指纹间存在类间距离”即“射频指纹可分离”的必要条件。

从式（3.14）可知，“射频指纹可分离”即“任意两个射频指纹间存在类间距离”的概率与元件参数值 c 的等效量化级数 $M = \dfrac{2\Delta c}{\Delta c_{lsb}}$ 成正比；也即与等效元件容差成正比，与元件等效量化间隔 Δc_{lsb} 成反比；由于 Δc_{lsb} 与 ADC 量化精度呈线性关系，也即与 ADC 量化精度成反比。

由于 Δc 是构成无线发射机的所有元件的等效元件的等效容差，而 Δc 与实际元件的容差成正比关系，所以，无线发射机的元件容差与 ADC 量化精度是射频指纹可分离性的两个主要影响因素。实际中，无线发射机的元件容差是确定的，只要 ADC 的量化精度足够高，任意两射频指纹存在类间距离的概率就足够大，从而保证射频指纹的可分离性。

3.4 数字化射频指纹的可分离性分析二

由于“数字化射频指纹的可分离性分析一”不够清晰，这里从另一个角度对这个问题进行进一步的研究。

设两个待识别无线设备发射机的结构相同、构件参数标称值相同，其某一种射频指纹用 $RFF_k(x)$与 $RFF_l(x)$表示，$k\neq l$，$xStart\leq x\leq xEnd$，$xStart$ 表示射频指纹自变量的起始值，$xEnd$ 表示射频指纹自变量的结束值。

定义“两射频指纹间欧氏距离为 0 的概率”为射频指纹的可分离性度量，记为 P_{disc}，则 $P_{disc}=P\{ RFF_k(x)= RFF_l(x),k\neq l\}$。$P_{disc}$ 越小表示两射频指纹间欧氏距离为 0 的概率越小，即两射频指纹间欧氏距离不为 0 的概率越大，也即该两射频指纹的可分离性越优。

实际的射频指纹识别中，采用离散量化后的接收无线信号进行射频指纹变换，等效于对射频指纹 $RFF(x)$进行采样，即把 x 离散化为 x_v，$v=1,...,M$，其中 $x_v=v*x_s$，x_s 为步长；把 $RFF(x)$值量化为 RFF_u，$u=1,...,N$，其中 $RFF_u=u*LSB$，LSB 为度量射频指纹识别系统分辨力的最小量化间隔。

设

$$LSB > \arg\max_{x_v}\{|RFF_{k,u}(x_v)-RFF_{l,u}(x_v)|\} \tag{3.15}$$

则 $P_{disc}=1$，即两射频指纹以概率 1 不可分离。当

$$LSB < \arg\max_{x_v}\{|RFF_{k,u}(x_v)-RFF_{l,u}(x_v)|\} \tag{3.16}$$

时

$$\begin{aligned} &P_{disc}=P\{RFF_k(x)=RFF_l(x)\}\\ &=P\{RFF_{k,u}(x_v)=RFF_{l,u}(x_v),u=1,...,N,v=1,...,M\}\end{aligned} \tag{3.17}$$

由于不同无线发射机的各离散点 x_v 处的 $RFF_u(x_v)$独立，因此

$$\begin{aligned} &P_{disc}=P\{RFF_{k,u}(x_v)=RFF_{l,u}(x_v),u=1,...,N;v=1,...,M\}\\ &=\prod_{v=1}^{M}P\{RFF_{k,u}(x_v)=RFF_{l,u}(x_v),u=1,...,N\}\end{aligned} \tag{3.18}$$

由式(3.2)可知，$RFF_u(x_v)$是 V_y 的某个确定的函数；由于构件容差的存在，V_y 可建模为具有确定概率分布的随机变量，则 $RFF_u(x_v)$也是某确定的随机变量，满足确定的概率分布，设其概率密度函数用 $pdf\{RFF_u(x_v)\}$表示，假设一个实例如图 3.4 所示

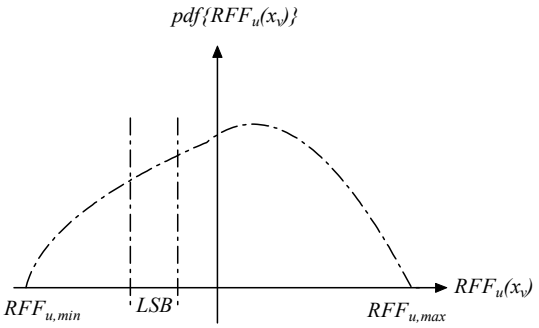

图 3.4 一个 $pdf\{RFF_u(x_v)\}$ 实例

图 3.4 中，$RFF_{u,min}$ 表示射频指纹识别系统能分辨的 $RFF_u(x_v)$ 最小值，$RFF_{u,\min} \subset [(N_{u,\min}-1)*LSB, N_{u,\min}*LSB]$，$N_{u,min}$ 为整数；$RFF_{u,max}$ 表示射频指纹识别系统能分辨的 $RFF_u(x_v)$ 最大值，$RFF_{u,\max} \subset [(N_{u,\max}-1)*LSB, N_{u,\max}*LSB]$，$N_{u,max}$ 为整数。则，式(3.18)为：

$$
\begin{aligned}
P_{disc} &= \prod_{v=1}^{M} P\{RFF_{k,u}(x_v) = RFF_{l,u}(x_v), u = 1,...,N\} \\
&= \prod_{v=1}^{M} [\sum_{N_u=N_{u,\min}}^{N_{u,\max}} P\{RFF_{k,u}(x_v) = LSB*N_u, RFF_{l,u}(x_v) = LSB*N_u\}] \\
&= \prod_{v=1}^{M} [\sum_{N_u=N_{u,\min}}^{N_{u,\max}} P^2\{RFF_u(x_v) = LSB*N_u\}] \\
&= \prod_{v=1}^{M} [\sum_{N_u=N_{u,\min}}^{N_{u,\max}} (\int_{\mathrm{RFF_u(x_v)}=LSB*(N_u-1)}^{LSB*N_u} pdf\{\mathrm{RFF_u(x_v)}\} d\mathrm{RFF_u(x_v)})^2]
\end{aligned}
\tag{3.19}
$$

式(3.19)中，随机变量 $RFF_{k,u}(x_v)$ 与 $RFF_{l,u}(x_v)$ 独立同分布于 $pdf\{RFF_u(x_v)\}$，则这两随机变量只要同时量化为同一值 $LSB*N_u, N_u = N_{u,\min},...,N_{u,\max}$ 即相等，因而事情 $RFF_{k,u}(x_v) = LSB*N_u$ 与事情 $RFF_{l,u}(x_v) = LSB*N_u$ 是“或”的关系。式（3.19）即射频指纹可分离性及其影响因素关系的解析式。

公式(3.19)显示：

（1） 两数字化射频指纹可分离性度量是离散后两射频指纹随机变量相等概率的累乘；

（2） 离散后两射频指纹随机变量相等概率是离散量化后射频指纹在各量化间隔内概率的平方和；

（3） 而离散量化后射频指纹在各量化间隔内概率由其概率密度函数及射频指纹识别系统的量化精度决定。

对公式(3.19)的进一步分析显示：

（1） 射频指纹随机变量的概率密度函数主要由待识别无线设备发射机的结构与构件的容差性质决定，因而数字化射频指纹可分离性与待识别无线设备发射

部分的结构与构件容差性质有关；

（2） 数字化射频指纹可分离性与射频指纹识别系统的量化间隔 *LSB* 有关。式(3.19)中的 *LSB* 减小为 i 分之一时，即射频指纹识别系统的分辨力增加为 i 倍时，可分离性度量 P_{disc} 下降（证明见附录 B），即 RFF 可分离性增强；当 *LSB* 大于两射频指纹离散量化值之差的最大值时，P_{disc} 为 1，即两数字化射频指纹依概率 1 不可分离；

（3） 把模拟射频指纹离散后的样点数称为“数字化射频指纹的维数”，则数字化射频指纹的可分离性与其维数有关。根据式(3.19)可知，在 *LSB* 小于两射频指纹离散量化值之差的最大值的条件下，离散化射频指纹的维数越多，则 P_{disc} 越小，即射频指纹的可分离性越好；当维数趋近无限多时，P_{disc} 趋近 0 ——— 两数字化射频指纹依概率 1 可分离。

根据以上对公式(3.19)的分析，可以得到数字化射频指纹可分离性及其影响因素之间的关系：

（1） 数字化射频指纹可分离性由射频指纹识别系统的分辨力、数字化射频指纹维数与待识别无线设备发射机结构及构件容差的性质的相对程度决定；

（2） 射频指纹识别系统的分辨力（即最小量化间隔）强于两数字化射频指纹之差的最大值是其可分离的必要条件；分辨力越高，则其可分离性越优；

（3） 对于给定的待识别无线设备，在射频指纹识别系统的分辨力一定的情况下，数字化射频指纹的维数越多，则其可分离性越优。

另外，上面分析中，“两数字化射频指纹依概率 1 可分离”即表明了模拟射频指纹具备唯一性。

本小节得到的结论包含了“数字化射频指纹的可分离性分析一”得到的结论。

3.5 射频指纹可分离性与可分性度量

设射频指纹模式的样本矢量记为 $\mathbf{x}_k^{(i)}$，$k=1,2,\bullet\bullet\bullet,N_i$ 表示样本序号，$i=1,2,\bullet\bullet\bullet,c$ 表示模式，N_i 表示 i 模式的样本数目，$N=\sum_{i=1}^{c}N_i$ 表示样本总数。则各模式的样本均值矢量为

$$\mathbf{m}^{(i)}=\frac{1}{N_i}\sum_{k=1}^{N_i}\mathbf{x}_k^{(i)} \tag{3.20}$$

所有模式样本的总体均值矢量为

$$\mathbf{m}=\sum_{i=1}^{c}P_i\mathbf{m}^{(i)} \tag{3.21}$$

式中 P_i 为相应类的先验概率。当用样本频率代替先验概率时，有

$$P_i = \frac{N_i}{N} \tag{3.22}$$

$$\mathbf{m} = \sum_{i=1}^{c} \frac{N_i}{N} \mathbf{m}^{(i)} = \frac{1}{N} \sum_{i=1}^{c} \sum_{k=1}^{N_i} \mathbf{x}_k^{(i)} = \frac{1}{N} \sum_{l=1}^{N} \mathbf{x}_l \tag{3.23}$$

则体现模式样本在本类的样本均值矢量周围的散布情况的类内离差矩阵为

$$S_{W_i} = \frac{1}{N_i} \sum_{k=1}^{N_i} (\mathbf{x}_k^{(i)} - \mathbf{m}^{(i)})(\mathbf{x}_k^{(i)} - \mathbf{m}^{(i)})^{'} \tag{3.24}$$

总的类内离差矩阵为

$$S_W = \sum_{i=1}^{c} P_i S_{W_i} = \sum_{i=1}^{c} P_i \frac{1}{N_i} \sum_{k=1}^{N_i} (\mathbf{x}_k^{(i)} - \mathbf{m}^{(i)})(\mathbf{x}_k^{(i)} - \mathbf{m}^{(i)})^{'} \tag{3.25}$$

总的类间离差矩阵为

$$S_B = \sum_{i=1}^{c} P_i (\mathbf{m}^{(i)} - \mathbf{m})(\mathbf{m}^{(i)} - \mathbf{m})^{'} \tag{3.26}$$

其中，S_W、S_B为对称阵，而任意对称阵均可经正交变换对角化，且对角线上阵元为特征值。由离差阵的定义可知，此时对角线上的阵元具有方差、均方距离等涵义，且各分量不相关。正交变换为相似变换，变换后矩阵迹不变、行列式值亦不变。因此构造如下的射频指纹可分性度量

$$J = \frac{Tr[S_B]}{Tr[S_W]} \tag{3.27}$$

由式(3.27)可知，当类内模式较密集，不同类模式相距较远时，J较大，此时分类较易。而式(3.26)的类间离差矩阵迹

$$D = Tr[S_B] \tag{3.28}$$

可以作为射频指纹可分离性的一种度量。

3.6 实验验证

通常，无线网络物理层包的前导是先验与确定的，可将其变换为射频指纹用于无线设备识别。本章把 IEEE 802.11 无线设备功率渐升期间发送的前导信号包络作为一种射频指纹（称为 ramp-up 射频指纹，详见第五章）用于实验。

采用射频示波器采集 5 只 IEEE 802.11b 同一系列无线网卡的短前导射频信号，并在计算机上采用基于 Matlab 与 Simulink 的软件无线电系统进行处理，得到其 ramp-up 射频指纹。按第一个完整 Barker 码包络起点对齐（详见第四章）后的 5 只无线网卡的 50 个 ramp-up 射频指纹样本如图 3.5 中子图（a）、（b）、（c）、（d）与（e）所示，其中子图（a）包含一个无线网卡的 ramp-up 射频指纹及其后的完整 barker 码包络。

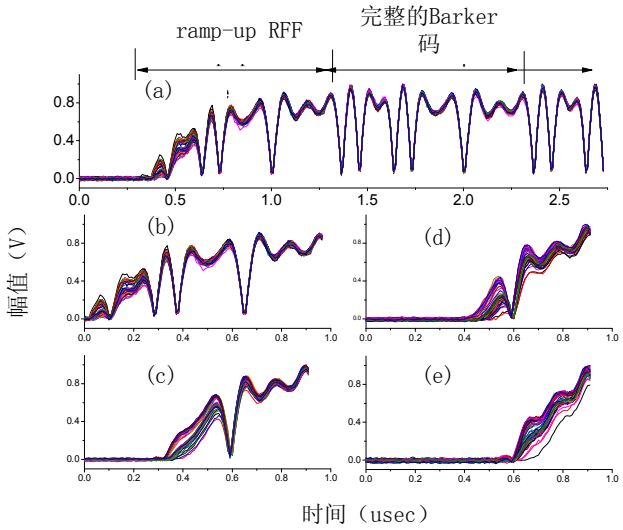

图 3.5 五只 IEEE 802.11b 同一系列
无线网卡的 ramp-up 射频指纹

由图 3.5 可知，该同一厂家同一型号 5 只无线网卡功率渐升期间的短前导信号及其 ramp-up 射频指纹存在很大差异。

无线网卡 ramp-up 射频指纹的维数由接收信号持续时间与识别系统的采样率决定。把图 3.5 所示 5 只无线网卡 ramp-up 射频指纹样本的类间离差矩阵迹 D 作为其可分离性度量[104]，则不同接收信号持续时间 dur 下，ramp-up 射频指纹可分离性度量 D 随不同采样率 f_s 的变化情况如图 3.6 所示。

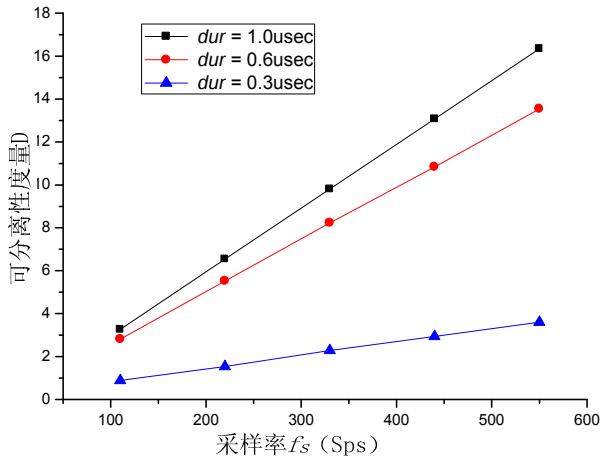

图 3.6 不同接收信号持续时间 dur 下，射频指纹
可分离性度量 D 随不同采样率 f_s 的变化

由图 3.6 可知，该 5 只无线网卡的 ramp-up 射频指纹可分离性随采样率提高而更优，随接收信号增长而更优，验证了式(3.19)的结果。

当接收信号持续时间为 1usec 时，不同量化精度 lsb(对应不同量化比特数 bits)下样

本可分离性度量 D 随不同采样率 f_s 的变化情况如表 3.1 所示。

表 3.1 接收信号持续时间为 1usec 时，不同采样率 f_s、不同量化精度 lsb 下的射频指纹可分性度量 D

f_s(Sps) \ lsb(bits)	0.0156(6)	0.002(9)	0.0002(12)
110	3.2691	3.2697	3.2699
220	6.5363	6.5371	6.5375
330	9.8008	9.8053	9.8056
440	13.0716	13.0736	13.0737
550	16.3395	16.3417	16.3419

由表 3.1 可知，尽管数据差别很小，但该 5 只无线网卡的 ramp-up 射频指纹可分离性仍随采样率提高而更优，随量化精度提高而更优。因此，实验结果与式(3.19)及其分析结论相符。

3.7 本章小结

本章基于第二章构建的射频指纹识别系统模型，从两个角度研究了数字化射频指纹的可分离性。其中，推导了数字化射频指纹可分离性及其影响因素之间的关系解析式，并采用基于 IEEE 802.11b 无线网卡的射频指纹识别系统进行了实验验证，结果显示：数字化射频指纹可分离性由射频指纹识别系统的分辨力、数字化射频指纹维数与待识别无线设备发射机结构及构件容差的性质的相对程度决定；射频指纹识别系统的分辨力强于两数字化射频指纹之差的最大值是其可分离的必要条件；分辨力越高，则其可分离性越优；对于给定的待识别无线设备，在射频指纹识别系统的分辨力一定的情况下，射频指纹的维数越多，则其可分离性越优。

因此，根据接收无线信号变换新的射频指纹时，当接收信号长度与采样率决定变换的射频指纹维数时，应取尽量长的无线接收信号并采用更高的采样率进行射频指纹变换。这与文献中“steady-state 射频指纹的识别性能一般优于 turn-on 射频指纹的识别性能”相吻合。由于射频指纹识别系统的分辨力主要由 ADC 的量化精度决定，因此，为提高数字化射频指纹的可分离性，可提高 ADC 的量化精度。

相关研究文献一般把同一型号无线设备的识别性能作为射频指纹质量的评价方法。当实际射频指纹识别系统不能分辨同一型号无线设备的数字化射频指纹时，这种情况即“射频指纹识别系统的分辨力与数字化射频指纹维数”不能分辨由“具有相同结构的无线设备发射机的构件容差”引起的接收信号差异。此时，采用结构与构件相异的不同型号无线设备的识别实验也具有价值，其识别率可作为提高射频指纹识别系统精度后该种射频指纹质量的参考。

另外，上文中“数字化射频指纹可分离性解析式的分析”中“两数字化射频指纹依概率 1 可分离”即相应的射频指纹是唯一的，也即表明了模拟射频指纹的唯一性。这与哲学上的“世界上没有两片完全相同的树叶”相一致。

本章结果对其它类似的无线电设备识别也具有参考价值。

第四章 射频指纹识别中接收无线信号的检测方法

4.1 引言

射频指纹识别中接收无线信号的检测直接影响着后续的信号截取，当射频指纹不具备时间平移不变性时，会进一步影响后续的射频指纹变换、特征提取与分类识别等，进而决定样本的类内距离，因而对整个射频指纹识别性能有着重要的作用。射频指纹识别中的“接收无线信号检测”等价于“射频指纹检测”。

虽然射频指纹检测很重要，但仅有几篇文献对此进行了研究。1997 年，Shaw 与 Kinsner 提出了基于信号幅度的门限检测方法[105]，门限方法有着对噪声敏感并且需要预先设定门限的缺点。同年，Ureten 提出了基于信号幅度变化的 Bayesian 阶跃变点检测方法[84]，与门限检测方法不同，Bayesian 阶跃变点检测方法不需要设定门限，仅利用信号的变化特征。然而，对于例如 IEEE 802.11 等信号，该方法却不能到达最优。原因是 IEEE 802.11 无线发射机一般采用渐升方法达到额定输出功率，并且功率渐升的同时进行前导信号的发送。因此，2005 年，Ureten 又提出了 Bayesian 渐升变点检测方法[34]。

本文作者在再现 Bayesian 变点检测方法的研究中，发现由于 Wi-Fi 信号的特殊性，Bayesian 渐升变点检测方法不能获得最优的无线设备射频指纹可分性。本章首先研究了 Bayesian 变点检测方法，然后提出了基于 Wi-Fi 前导的接收无线信号检测方法，并对两种方法得到的射频指纹可分性进行了比较。

4.2 Wi-Fi Bayesian 渐升变点检测

对信号观测数据进行概率推理的两个基本问题是：（1）选择最适合数据的信号模型；（2）根据观测数据对信号模型参数进行估计。

对于给定的 N 维观测数据 d_i，$i=1...N$，假定其由与系统有关的时间函数 $f(t_i,\theta)$ 及随机变量 e_i 构成

$$d_i = f(t_i,\theta) + e_i \tag{4.1}$$

其中，θ 是信号模型的参数矢量，t_i 为观测时刻。如果 e_i 为 0 均值的 Gaussian 噪声，则其概率密度函数为

$$p(e_i) = \frac{1}{\sqrt{2\pi\sigma^2}}\exp[-\frac{e_i^2}{2\sigma^2}] \tag{4.2}$$

其中，σ 为标准差。

定义似然函数是观测数据在给定参数值、系统模型及噪声统计量下的概率，用 I_k 表示特定的信号模型及噪声统计量，则似然函数可记为

$$p(\mathrm{d}\,|\,\Phi,\mathrm{I_k}) = L(\Phi,\mathrm{d}) \tag{4.3}$$

其中，Φ 包括信号模型及噪声的参数。

假设观测数据由信号与独立同分布（i.i.d）的随机变量构成，在此情况下，似然函数与随机变量的联合概率密度相同[106]

$$L(\Phi,\mathrm{d}) = p(\mathrm{e}) \tag{4.4}$$

如果式(4.1)中的 e_i 独立同分布，则观测数据 d_i 的似然函数

$$\begin{aligned} &L(\Phi,\mathrm{d}) = p(\mathrm{e}) \\ &= \prod_{i=1}^{N} p[d_i - f(t_i;\theta)] \end{aligned} \tag{4.5}$$

当 e_i 为 0 均值 Gaussian 噪声时，则式(4.5)为

$$\begin{aligned} &L(\Phi,\mathrm{d}) = p(\mathrm{e}) \\ &= \prod_{i=1}^{N} \frac{1}{\sqrt{2\pi\sigma^2}} \exp[-\frac{e_i^{\,2}}{2\sigma^2}] \\ &= (2\pi\sigma^2)^{-N/2} \exp[-\frac{\sum_{i=1}^{N} e_i^{\,2}}{2\sigma^2}] \end{aligned} \tag{4.6}$$

假设观测数据可用基函数 $g_k(t)$与噪声 $e(t)$的线性组合描述

$$d(i) = \sum_{k=1}^{M} b_k g_k(i) + e(i), 1 \le i \le N \tag{4.7}$$

其中，$g_k(i)$是基函数 $g_k(t)$在 t_i 时刻的值，b_k 是基因子；写成矩阵形式，即

$$\mathrm{d} = \mathrm{G\,b} + \mathrm{e} \tag{4.8}$$

其中，d 是 $Nx1$ 维观测数据样点矩阵；e 是 $Nx1$ 维 i.i.d.Gaussian 噪声样点；G 是 NxM 维基函数矩阵；b 是 $Mx1$ 维线性因子矩阵；则似然函数为

$$p(\mathrm{d}\,|\,\{w\},\delta,\mathrm{b},\mathrm{I}) = (2\pi\delta^2)^{-\frac{N}{2}} \exp[-\frac{\mathrm{e^T e}}{2\delta^2}] \tag{4.9}$$

其中 $\{w\}$ 表示基函数矩阵 G 的参数。

把式(4.8)代入式(4.9)，为：

$$p(\mathrm{d}\,|\,\{w\},\delta,\mathrm{b},\mathrm{I}) = (2\pi\delta^2)^{-\frac{N}{2}} \exp[-\frac{(\mathrm{d-G\,b})^{\mathrm{T}}(\mathrm{d-G\,b})}{2\delta^2}] \tag{4.10}$$

根据文献[107]可得

$$p(\{\delta,w\}\,|\,\mathrm{d},\mathrm{I}) = \int p(\{\mathrm{b,w},\delta\}|\mathrm{d,I})\mathrm{db} \tag{4.11}$$

式（4.11）正比于

$$\frac{(2\pi\delta^2)^{-\frac{N-M}{2}}}{\sqrt{\det(G^T G)}} \exp[-(\frac{d^T d - f^T f}{2\delta^2})] \tag{4.12}$$

根据文献[107]把 δ 积去，可得

$$p(\{w\}\,|\,\mathrm{d},\mathrm{I}) \propto \frac{[\mathrm{d}^{\mathrm{T}}\mathrm{d}-\mathrm{d}^{\mathrm{T}}\mathrm{G}(\mathrm{G}^{\mathrm{T}}\mathrm{G})^{-1}\mathrm{G}^{\mathrm{T}}\mathrm{d}]^{-\frac{N-M}{2}}}{\sqrt{\det(\mathrm{G}^{\mathrm{T}}\mathrm{G})}} \tag{4.13}$$

式（4.13）仅为$\{w\}$的函数，也即后验概率密度，式（4.13）意味着仅通过观测数据与数据模型，即可对模型的参数进行最大似然估计。

IEEE 802.11b/g 规定，帧发送时的功率从 0 到达额定功率采用渐升方法，目的是避免对临近信道造成干扰，一个典型信号如图 2.11 所示。因此，其信号模型可表示为分段函数

$$d_i = \begin{cases} u+u_i, 1 \le i \le m \\ u+\alpha(i-m)+u_i, m \le i \le N \end{cases} \tag{4.14}$$

其中，d_i是分段信号 i 时刻样点，N 是样点总数，m 是变点，u 是变点之前的信号均值，α 是线性斜率，u_i是零均值高斯白噪声。则在观测数据与信号模型的情况下，变点的概率密度函数为

$$p(\{m\}\,|\,\mathrm{d},\mathrm{I}) \propto \frac{[\mathrm{d}^{\mathrm{T}}\mathrm{d}-\mathrm{d}^{\mathrm{T}}\mathrm{G}(\mathrm{G}^{\mathrm{T}}\mathrm{G})^{-1}\mathrm{G}^{\mathrm{T}}\mathrm{d}]^{-\frac{N-M}{2}}}{\sqrt{\det(\mathrm{G}^{\mathrm{T}}\mathrm{G})}} \tag{4.15}$$

其中矩阵 G 包含变点信息，为

$$G^T = \begin{bmatrix} 1,1,1,1,1,...,1,1,1,1,1,...,1 \\ 0,0,0,0,0,...,0,1,2,3,...,N-m \end{bmatrix} \tag{4.16}$$

则当噪声标准差、u 与α 未知的情况下，仅根据观测数据即可对变点进行最大后验估计，即变点是后验概率密度最大值的样点序号值。

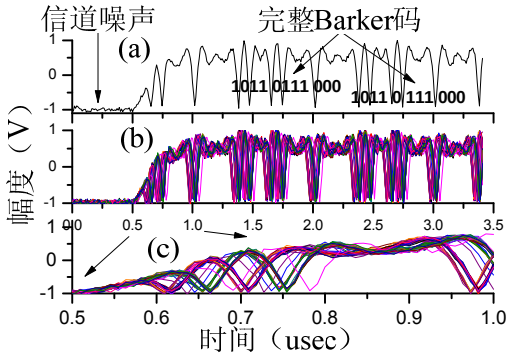

图 4.1 IEEE 802.11b 短前导包络头样本

一只 IEEE 802.11b 无线网卡发送的短前导包络头样本如图 4.1 的子图（a）至（c）所示。其中子图（a）是一个短前导包络样本，开始是信道噪声，接着是功率渐升部分不完整的 Barker 码（10110111000），跟着是完整的 Barker 码。由于同一无线网络中不同无线设备发送的前导具有可比性，因而其前导包络可以作为一种射频指纹用于无线设备识别。子图（b）是根据采用 Bayesian 渐升变点检测方法检测到的变点对齐后的 50 个前导包络射频指纹样本叠加图；子图（c）是子图（b）头部 0.5usec 至 1.0usec 部分的局部放大图。从子图（c）可知，尽管 Bayesian 渐升变点检测得到的变点很准确，但该 50

个前导包络射频指纹样本却显示出很大的类内距离，导致其可分性差[61]。究其原因，这种渐升功率控制方式导致发送的前导波形瞬态的稳定性差，进而导致基于 Bayesian 渐升变点检测方法得到的前导包络射频指纹的可分性差。

4.3 基于 Wi-Fi 前导的检测方法

4.3.1 IEEE 802.11 物理层帧格式

IEEE 802.11 协议定义了三种基本的物理层规范：2.4GHz ISM 频段的跳频扩展频谱（FHSS）物理层规范，直接序列扩展频谱（DSSS）物理层规范和红外（Infrared）物理层规范。其中 DSSS 物理层规范得到了广泛的应用，采用此方式时，要发送的数据采用伪随机码（PN 码）扩展到一个比原始信号频谱宽的频谱上实现扩频。接收端使用相同的伪随机码进行解扩，把接收数据还原为原始数据。该方式的优点是具有很强的抗噪声能力。DSSS 物理层汇聚过程（Physical Layer Convergence Procedure，简称 PLCP）子层把 PLCP 服务数据单元（PLCP Service Data Units，简称 PSDU）映射成物理层协议数据单元（Physical protocol data units，简称 PPDU），使之包含物理层发送与接收所需的信息，其 PLCP PPDU 格式分为“长”与“短”两种，“长”PLCP PPUD 格式如图 4.2 所示。

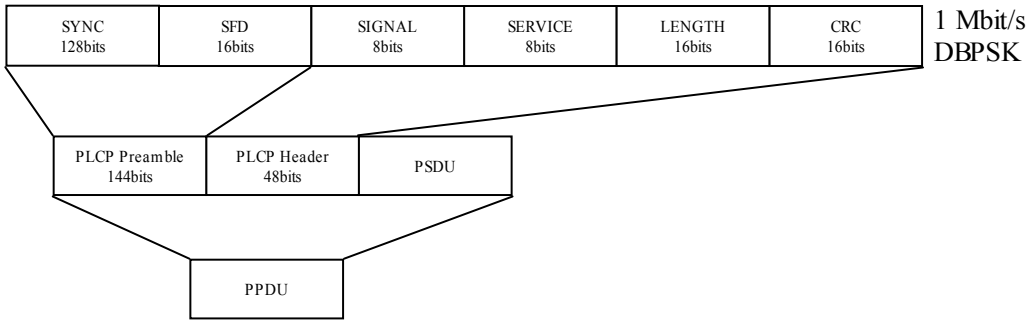

图 4.2 “长”PLCP PPDU 格式

如图 4.2 所示，“长”PLCP 分为 PLCP 前导与 PLCP 头两部分，其中 PLCP 前导又分为同步码 SNYC 与帧起始定界符 SFD 两部分。“长”PLCP 的同步码 SNYC 由 128bits 的 1 扰码后生成；而“短”PLCP 的同步码 shortSNYC 由 56bits 的 0 扰码后生成，“短”PLCP PPDU 格式如图 4.3 所示。

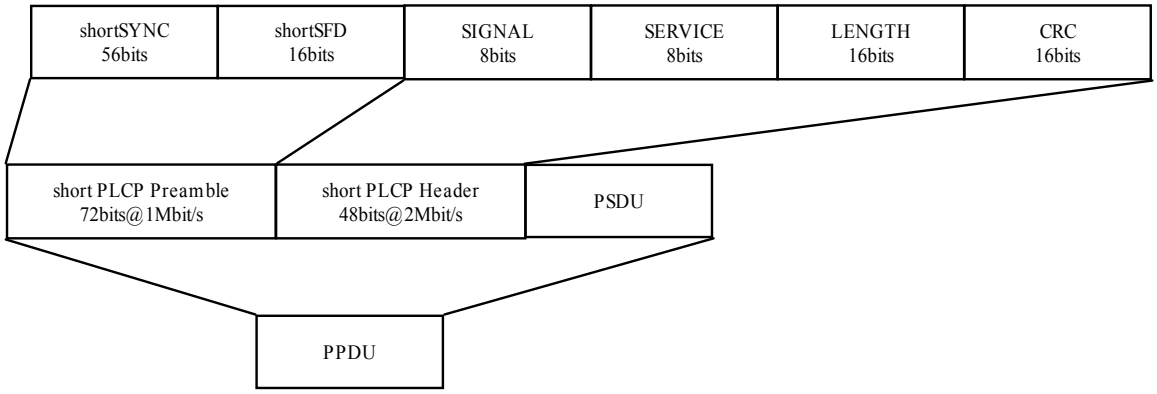

图 4.3 “短”PLCP PPDU 格式

“长”与“短”PLCP 前导采用 11chips Barker 码（1、0、1、1、0、1、1、1、0、0、0 对应+1、-1、+1、+1、-1、+1、+1、+1、-1、-1、-1）直接序列扩频的 1Mbit/s DBPSK 调制方式，如图 4.4 所示。

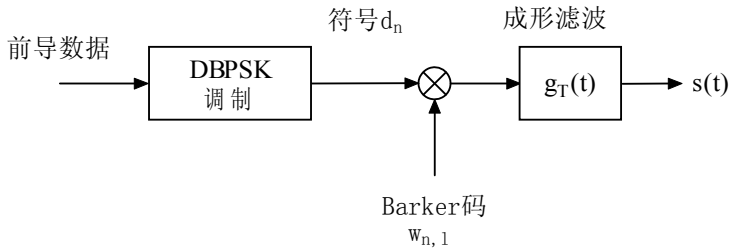

图 4.4 PLCP 前导信号的产生示意图

如图 4.4 所示，PLCP 前导数据经 DBPSK 调制后为符号 d_n，d_n 的符号率为 1Mbits/s；d_n 经 Barker 码 $W_{n,l}$ 直接序列扩频后为码片率为 11MChips/s 的码片；码片经单位脉冲响应为 $g_T(t)$的成形滤波器成形后为发送信号 $s(t)$，$s(t)$的低通等效可表示为

$$s_l(t)=\sum_{n=-\infty}^{\infty} d_n \bullet \sum_{l=0}^{L-1} w_{n,l} \bullet g_T(t-n \bullet T_s - l \bullet T_c) \tag{4.17}$$

式（4.17）中，$w_{n,l}$ 为 IEEE 802.11b/g 规定的 Barker 码，L 为 $w_{n,l}$ 的长度 11；T_s 与 T_c 分别为符号与码片周期，且有 $L=T_s/T_c$。

4.3.2 基于 Wi-Fi 前导的检测方法

Wi-Fi 标准规定其物理层前导具有周期性。假设其前导包络的基本周期长 T_p，并假设其功率渐升时间为 T_{ramp}；则功率渐升期间的前导包络基本周期数为

$$N_{ramp}=[\frac{T_{ramp}}{T_p}] \tag{4.18}$$

这里[]表示向上取整操作，则接收 Wi-Fi 前导包络为

$$e(t)=p(t) \bullet \sum_{m=0}^{N_{ramp}-1} e_{peri}(t-m \bullet T_p)+\sum_{n=N_{ramp}}^{N-1} e_{peri}(t-n \bullet T_p) \tag{4.19}$$

这里，$p(t)$是功率渐升导致的包络幅度函数，$0<t<N_{ramp} \bullet T_p$；$e_{peri}(t)$是前导基本周期的包

络幅度函数，$0<t<T_p$；N 是前导基本周期总数。

接收的 Wi-Fi 前导包络 $e(t)$与其基本周期 $e_{peri}(t)$的相关为：

$$c(t)=\int_{\tau=0}^{T_p} e_{peri}(\tau)\bullet e(t+\tau)d\tau \tag{4.20}$$

式(4.20)的相关 $c(t)$具有以下性质：

(1) $t=N_{ramp}\bullet T_p$ 时的 $c(t)$值是 $N_{ramp}\bullet T_p \le t<(N_{ramp}+1)\bullet T_p$ 内 $c(t)$的局部最大值；

(2) $t\ge N_{ramp}\bullet T_p$ 时的 $c(t)$具有周期为 T_p 的局部最大值。

根据 $c(t)$的以上性质可知：$t_0=N_{ramp}\bullet T_p$ 可看作发射机完成功率渐升并进入第一个完整前导周期的时刻，定义 t_0 为接收 Wi-Fi 信号的参考时刻，则提出的 Wi-Fi 射频指纹检测方法如下：

步骤 1：根据前导基本周期的包络形状设计相关模板，用 $e_{peri}(t)$表示；

布骤 2：计算接收 Wi-Fi 信号的包络，用 $e(t)$表示；

步骤 3：计算 $e(t)$与 $e_{peri}(t)$的相关，用 $c(t)$表示；

步骤 4：根据 $c(t)$性质搜索 $t=N_{ramp}\bullet T_p$ 时刻作为接收 Wi-Fi 信号的参考时刻。

根据检测到的参考时刻对接收 Wi-Fi 信号进行截取，然后把截取后的 Wi-Fi 信号变换为射频指纹。

4.3.3 基于 Wi-Fi DSSS 前导的实验验证

IEEE 802.11b/g 的 PLCP 前导采用 11chips Barker 码（10110111000）扩频的 1Mbit/s DBPSK 调制方式，因而其前导包络具有周期为 1usec 的周期性。采用 IEEE 802.11b 的 DSSS 前导对提出方法进行验证，用于采集并处理 IEEE 802.11b 射频信号的实验系统如图 4.5 所示。

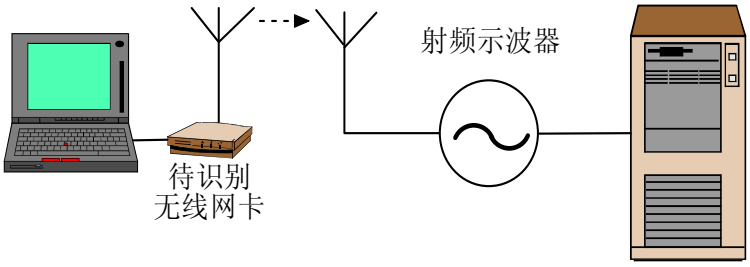

图 4.5 IEEE 802.11b 射频信号采集与处理系统

如图 4.5 所示，待识别外置式 IEEE 802.11b 无线网卡通过 USB 接口与笔记本电脑相连并由其控制，无线网卡设为 Ad-hoc 模式；则其不断发送射频信号帧。发送天线采用全向天线，而接收天线采用定向天线，两天线间距离约为 10cm；以保证接收天线接收到的信号能量主要由发送天线直接发送而来。接收天线直接与射频示波器 Agilent 54854A 的输入端口相连，以保证由待识别无线网卡发送的信号触发。采集时采用铁丝网对两天线部分进行了最大限度的电磁屏蔽。

射频示波器被触发后，数据保存到通过有线网络相连的台式计算机中。台式计算机

采用 Matlab 软件对接收射频帧前导信号进行 Hilbert 变换并求其绝对值得到其包络，并对其加 AWGN 噪声改变其 SNR。SNR 为 15dB 时的一个 IEEE 802.11b 前导包络如图 4.6 中的 $e(n)$所示。

图 4.6 中 $b(n)$为设计的与 IEEE 802.11b 前导包络基本周期形状相似的相关模板；而 $b(n)$与 $e(n)$的相关结果为 $c(n)$；$c(n)$上的 p 为局部最大值，而 P_{ref}为经过搜索得到的第一个完整 Barker 码包络的起始时刻。

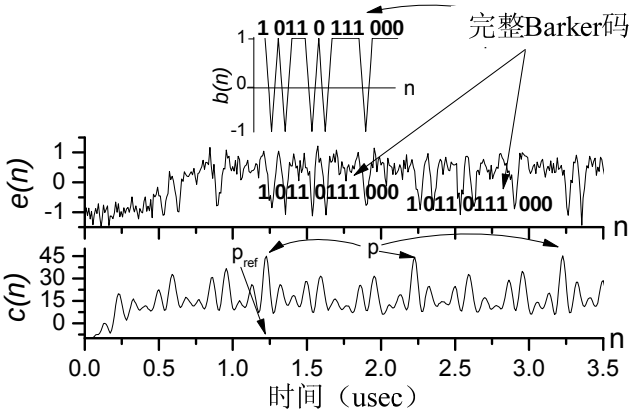

图 4.6 一个 IEEE 802.11b 前导包络及与模板的相关

把 P_{ref}作为接收 IEEE 802.11b 帧射频信号的参考时刻，截取从 P_{ref}开始向历史时间方向 T_{head}长的接收射频信号进行射频指纹变换。假设进行的射频指纹变换即求取包络运算，则 IEEE 802.11b 帧前导包络就是一种射频指纹，称为 IEEE 802.11b 前导包络射频指纹。

取 3 只待识别 IEEE 802.11b 无线设备，工作模式设为 Ad-hoc 模式，前导设为“短”型，功率设为“连续接入”模式；每只采集 50 个射频帧信号样本，根据各自的 P_{ref}进行对齐后得到的 SNR 为 15dB 的前导包络射频指纹叠加图如图 4.7 所示，图中子图（a）、（b）与（c）分别对应不同的待识别无线设备。

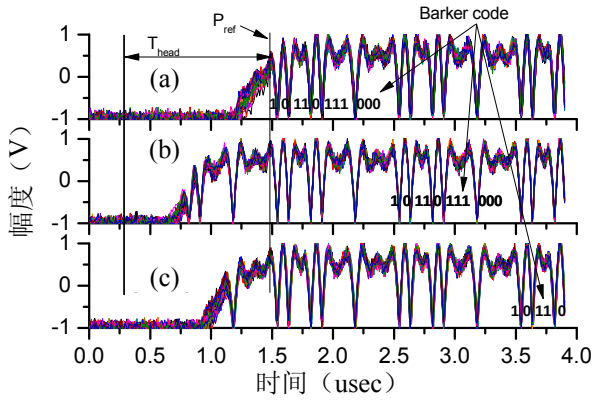

图 4.7 对齐后的前导包络射频指纹叠加图

与采用 Bayesian 渐升变点检测方法得到的图 4.1 显示的样本相比，图 4.7 的样本表现得更为整齐；为进行检测方法的对比，采用第三章定义的射频指纹可分性度量 J（见式 3.27）。图 4.7 所示三只无线设备的样本在不同检测方法下得到的射频指纹可分性度

量如表 4.1 所示。

表 4.1 三只无线设备的射频指纹可分性度量对比

可分性度量	基于 Wi-Fi 前导的检测方法	Bayesian 渐升变点检测
$Tr(S_B)$	15.225	2.0648
$Tr(S_W)$	6.8527	11.5682
J	**2.2218**	**0.1785**

其中 $T_r(S_B)$为射频指纹样本类间离差矩阵迹，是射频指纹样本可分离性的一种度量；而 $T_r(S_W)$为射频指纹样本类内离差矩阵迹，是射频指纹样本稳定性的一种度量。

由表 4.1 可知，相比采用 Bayesian 渐升变点检测方法而言，采用基于 Wi-Fi 前导的检测方法得到的射频指纹类内距小、类间距大，因而得到的射频指纹可分性优。这是由于基于 Wi-Fi 前导的检测方法根据稳态信号进行，而 Bayesian 渐升变点检测方法根据瞬态信号进行。由于 Wi-Fi 帧的瞬态信号稳定性一般差于稳态信号稳定性，因而提出方法得到的射频指纹可分性更优。

4.4 本章小结

鉴于接收无线信号的检测对后续的射频指纹变换等具有重要作用，本章首先研究了 Wi-Fi Bayesian 渐升变点检测方法，然后提出了基于 Wi-Fi 前导的射频指纹检测方法。提出方法利用 Wi-Fi 前导信号的固有特征与“相关”技术进行 Wi-Fi 信号的起始时刻检测，采用实验进行了验证，结果显示：就射频指纹的稳定性与可分性而言，基于稳态信号的提出方法优于基于瞬态信号的 Bayesian 渐升变点检测方法。

第五章 射频指纹的变换方法

5.1 引言

本文在第一章基于“无线设备发送的射频信号，不仅承载着无线设备发送的数字信息，而且承载着其发射机的硬件信息”的事实，尝试性提出了“射频指纹”的一种定义，即射频指纹是承载无线设备发射机硬件信息的接收无线信号的变换结果，这种变换结果体现无线设备发射机的硬件特性并具有可比性。基于该定义，作者进一步提出了“射频指纹识别”过程的4步骤划分法，即：接收无线信号的起始时刻检测与信号截取、射频指纹变换、特征提取与无线设备的识别或确认。并根据射频指纹识别过程的中间结果，尝试性构建了包括信号层、射频指纹层、特征层及无线发射机层的射频指纹识别体系结构。

本文在第二章构建了射频指纹识别系统的一种基本模型；第三章研究了数字化射频指纹的可分离性及其影响因素；这两章是射频指纹识别的基础。本文第四章研究了射频指纹识别过程的第一个步骤：接收无线信号的检测方法。

本章着重研究射频指纹识别过程的第二个步骤 —— 射频指纹的变换方法。首先对文献中已有的射频指纹变换方法进行了归类与分析，对进行本章研究的动机进行了解释；然后提出了以下几种射频指纹变换方法：基于渐升功率前导的Wi-Fi射频指纹变换方法、基于非线性动力学的射频指纹识别方法、基于BPSK信号的射频指纹变换方法及基于ARMA模型系数的射频指纹变换方法、。提出的有些射频指纹在特定的应用场景下性能优良，而有些射频指纹在某些应用场景下性能不佳。其中，介绍了相像系数特征提取方法与*k*-NN分类器，二者分别作为射频指纹识别过程第三、四步骤的基本方法，用于评估有关射频指纹的性能。

5.2 射频指纹变换方法的分类与分析

根据本文尝试性提出的“射频指纹”定义与“射频指纹识别”过程的4步骤划分法，文献中已有的射频指纹及本章将要提出的射频指纹可用图5.1表示，其中带*号的射频指纹表示本文将要提出的射频指纹。

如图5.1所示，射频指纹可以分为采用“瞬态信号”变换而来的turn-on射频指纹与采用“稳态信号”变换而来的steady-state射频指纹两种。“瞬态信号”指无线发射机功率从0到达额定功率时发送信号的瞬态部分，该部分不包含发送符号信息，因而具有可比性；并且体现发射机的硬件性质，因而很早就被变换为时域包络、频谱、小波因子及分形维数等基于瞬态信号的turn-on射频指纹用于无线发射机的识别[29, 30, 32-39, 41-43]。“稳态信号”

指无线发射机发射功率稳定下发送的信号，由于无线发射机的频偏、前导、星座点具有可比性，并且体现无线发射机的硬件性质，因而“稳态信号”被变换为频偏、前导包络、前导频谱、前导小波因子及星座点等steady-state射频指纹用于无线发射机的识别[45] [47] [51] [58] [56, 60]。

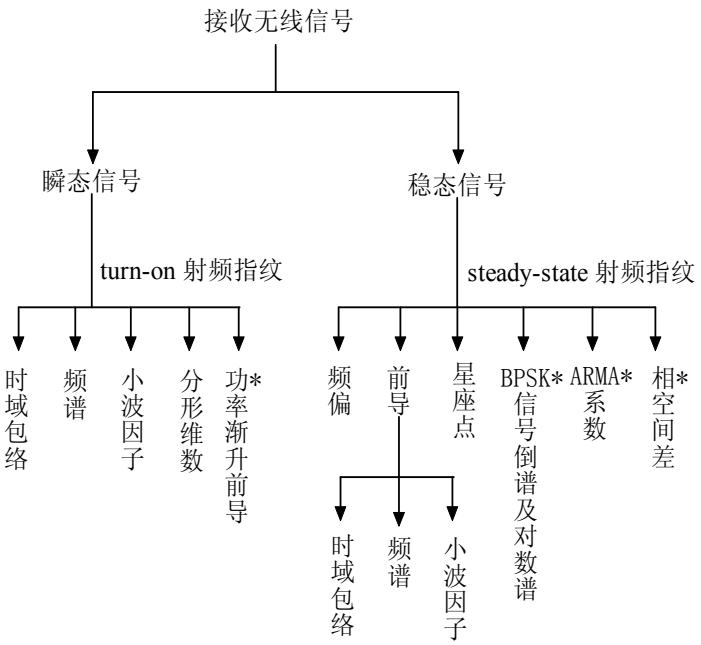

图 5.1 射频指纹分类

由于“瞬态信号”极其短暂，因而turn-on射频指纹实用价值有限。然而，steady-state射频指纹却表现了很好的应用前景。相关文献采用一般的通信接收机结构，在一定的条件下，能获得很好的识别性能[47, 51, 58]。例如，文献[58]采用IEEE 802.11b无线设备的频偏、帧前导相关值以及调制域星座点等作为射频指纹取得了很好的识别性能，条件是保持两天线间直达径没有障碍物并且天线角度不变。分析其原因：IEEE 802.11b规定其调制质量参数EVM误差范围为±35%，因而其设备的容限很大，等价于无线设备发射机构件的容差允许很大；同时，调制域星座点射频指纹采用无线信号调制域星座点的平均值作为射频指纹，对于QPSK调制，其维数为4；由于加取平均提高了其SNR，等价于提高了射频指纹识别系统的分辨力；所以文献[58]取得了很好的射频指纹识别性能。另外，星座点的加取平均消除了时变无线多径信道的部分影响，这也是其识别性能优的原因之一。该文献的实验结果与本文第三章建模分析得到的“数字化射频指纹可分离性及其影响因素之间关系”的结论部分吻合。

尽管不多的文献显示，根据steady-state射频指纹识别无线网络设备能够获得较好的识别性能，但这都是在一定的条件下获得的。我们的研究表明，根据同一种射频指纹，识别某些无线网卡的性能好，但识别另一些无线网卡的性能就可能较差。根据射频指纹识别无线设备离实际应用仍有很大距离。根据第一章尝试性建立的射频指纹识别体系结构（见图1.3）可知，同一个接收无线信号可以被变换为多种射频指纹。如果这些射频指纹具有独立性，即体现了待识别无线设备发射机的各种不同的硬件信息，那么，对于同

一个接收无线信号，变换得到的独立性射频指纹越多，体现的待识别无线发射机的硬件信息就越多，对后续的分类识别就越有利。所以，寻找同一个接收无线信号的多种射频指纹变换方法是“射频指纹识别”的关键性基础问题之一。本章根据此思路展开研究。

5.3 基于渐升功率前导的无线设备射频指纹

由开机瞬态信号变换而来的turn-on射频指纹是经典的射频指纹，包括包络turn-on射频指纹与相位turn-on射频指纹等。五只IEEE 802.11b/g无线网卡的包络turn-on射频指纹样本对齐图如图5.2的5个子图所示，其中每个子图对应一只无线网卡，每个子图中样本数为50。图5.2中子图（a）包含包络turn-on射频指纹及其后的barker码包络。由子图（a）可知，该型号无线网卡首先以阶跃方式到达额定功率，然后进行Barker码发送(未按IEEE 802.11b/g标准进行)。如子图（a）所示，这里截取其头部包含瞬态信号的1usec长包络作为该无线网卡的包络turn-on射频指纹(本节中简称为turn-on射频指纹)。图5.2中子图（b）、（c）、（d）及（e）分别为同一厂家相同型号的另外4只无线网卡的50个包络turn-on射频指纹样本的对齐图。由图5.2可知，该五只无线网卡的turn-on 射频指纹差异小。

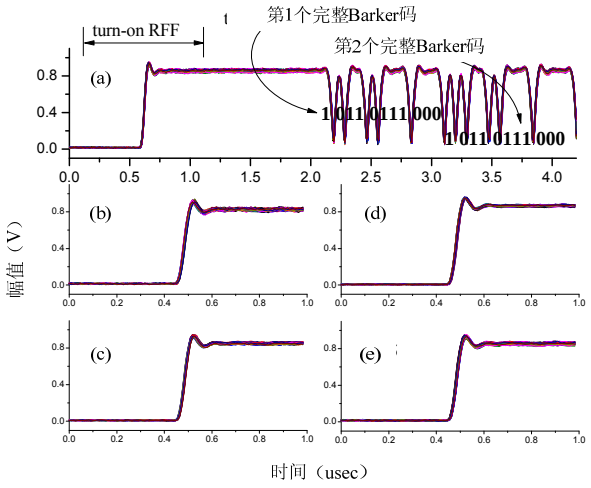

图 5.2 五只 IEEE 802.11b/g 无线网卡的
包络 turn-on 射频指纹样本对齐图

无线发射机功率放大器的功率渐升控制方式具有抑制带外频谱泄漏的性质，先验确定的前导序列常用于基于包的无线通信的同步等；据此，本节提出无线设备发送前导信号的同时进行功率渐升，变换功率渐升期间发送的前导信号为一种称为ramp-up射频指纹的新的射频指纹产生方法；理论分析与实验验证表明：ramp-up射频指纹的可分性优。

另外，从本质上看，本节提出的ramp-up 射频指纹是一种变异的turn-on射频指纹，因为尽管其是由功率渐升阶段的信号变换而来，但同时其包含了不完整的发送数字信息；而经典的turn-on射频指纹不包含发送信息。

5.3.1 理论分析

根据第二章无线设备发送射频信号模型的研究可知，无线设备发送的射频信号可表示为抽象形式

$$s(t)=F_1\{m_i(t),h_i(t),m_q(t),h_q(t),f_{IF},\phi_1(t),\phi_0(t),h_{IF}(t),f_c,\phi_2(t),g[\bullet]\} \tag{5.1}$$

式（5.1）中，$F_1\{\bullet\}$表示某个确定的函数，$m_i(t)$与$m_q(t)$是等效基带发送信号，$h_i(t)$与$h_q(t)$是待识别无线设备发射机 I 路与 Q 路的等效系统冲激响应，f_{IF}是调制载波频率，$h_{IF}(t)$是中频滤波器的的单位冲激响应，f_c与f_{IF}分别是射频载波频率与中频频率，$\phi_0(t)$是 I 路与 Q 路的相位偏差，$\phi_1(t)$与$\phi_2(t)$是载波的相位噪声，$g[\bullet]$是功率放大器 PA 的输入-输出非线性关系。

根据第二章的射频指纹识别系统的基本模型可知，接收无线信号可表示为

$$r(t)=F_2\{s(t),h_{ch}(t),n(t),h_{rcv}(t)\} \tag{5.2}$$

其中$F_2\{\bullet\}$表示某个确定的函数，$h_{ch}(t)$是无线多径信道的冲激响应，$n(t)$是接收机的 AWGN 噪声，$h_{rcv}(t)$是射频指纹识别系统接收机的等效冲激响应。假设射频指纹变换去除了无线多径信道与 AWGN 的影响，由于$h_{rcv}(t)$主要由射频指纹识别系统的软件无线电部分决定，因而可视为已知的，所以对式（5.2）进行射频指纹变换，为

$$\begin{aligned} RFF(x)&=T\{r(t)\}\\ &=F_3\{m_i(t),h_i(t),m_q(t),h_q(t),f_{IF},\phi_1(t),\phi_0(t),h_{IF}(t),f_c,\phi_2(t),g[\bullet]\}\end{aligned} \tag{5.3}$$

其中，$T\{\bullet\}$表示某个射频指纹变换。

当$m_i(t)$与$m_q(t)$为单位阶跃激励$u(t)$，等价于发射机功率以阶跃方式到达额定发射功率时，由于$u(t)$具备可比性，因而，$r(t)$瞬态部分的变换

$$RFF(x)=F_4\{h_i(t),h_q(t),f_{IF},\phi_1(t),\phi_0(t),h_{IF}(t),f_c,\phi_2(t),g[\bullet]\} \tag{5.4}$$

由待识别发射机的硬件性质决定，所以是一种 turn-on 射频指纹，例如 turn-on 包络射频指纹。

当$m_i(t)$与$m_q(t)$为确定的前导信号时，由于前导具备可比性，因而，$r(t)$稳态部分的变换

$$RFF(x)=F_5\{h_i(t),h_q(t),f_{IF},\phi_1(t),\phi_0(t),h_{IF}(t),f_c,\phi_2(t),g[\bullet]\} \tag{5.5}$$

由发射机的硬件性质决定，所以是一种稳态射频指纹，例如稳态前导频谱射频指纹。

当无线发射机采用渐升方式进行功率控制，并且功率渐升的同时进行前导序列发送时，功率渐升期间发送的前导信号$m_i(t)$与$m_q(t)$可等效为

$$m(t)=[u(t)-u(t-T_r)]\bullet ramp(t)\bullet prea(t) \tag{5.6}$$

其中T_r为功率渐升时间长度，$ramp(t)$为渐升函数，$prea(t)$为功率渐升期间发送的前导信号。由于前导具备可比性，因而，功率渐升期间发送的前导信号的变换

$$RFF(x)=F_6\{h_i(t),h_q(t),f_{IF},\phi_1(t),\phi_0(t),h_{IF}(t),f_c,\phi_2(t),g[\bullet],T_r,ramp(t)\} \tag{5.7}$$

可作为一种射频指纹，称为 ramp-up 射频指纹。式(5.6)中的T_r与 $ramp(t)$由发射机功率渐升部分的硬件性质决定。

对比式(5.7)与式(5.5)、(5.4)可知：影响 ramp-up 射频指纹的因素比影响 turn-on 射频指纹与 steady-state 射频指纹的因素增加了功率渐升控制参量T_r与 $ramp(t)$。在射频段，容差引起的构件微小差异会产生发送信号的较大差异。所以，在相同的接收信号采集条件及相同的射频指纹变换下，ramp-up 射频指纹的可分性比 turn-on 射频指纹及 steady-state 射频指纹的可分性优。

据此，基于功率渐升前导的无线发射机 ramp-up 射频指纹产生方法可总结为：功率渐升同时发送前导序列，变换功率渐升期间的接收前导信号为射频指纹用于无线发射机识别。

5.3.2 实验验证

由于 IEEE 802.11b/g 规定其物理层包的直序扩频前导（DSSS-preamble）采用产生 ramp-up 射频指纹的这种功率渐升同时发送前导序列方式，因而同一厂家同一型号的某型号 IEEE 802.11b 无线网卡被用于实验。

5.3.2.1 Ramp-up 射频指纹获取

采用第四章中图 4.5 所示的“IEEE 802.11b 射频信号采集及处理系统”进行 IEEE 802.11b 无线网卡的 DSSS-preamble 分析。无线网卡安装于计算机，设定为 ad-hoc 工作模式，工作频道为 2.412GHz，无线网卡不断发送包宣布其存在。一个外接高增益天线的 Agilent 射频示波器 54854A 用于 RF 信号采集，采样率为 10GSps。采集时，户内温度与湿度保持恒定。由于 2.45GHz 射频信号的无功近场区为 1.9cm，辐射远场区为 16.4cm 之外，两者之间为辐射近场区[108]，所以本实验把待识别无线网卡天线与接收天线距离设为 10cm。并且对两天线进行了最大限度的电磁屏蔽。

采集相同型号的三块 IEEE 802.11b 无线网卡的 DSSS-preamble 头部，每只无线网卡一个实例，如图 5.3 的子图(a)、(b)与(c)图所示。从图 5.3 可以看出，该 3 个 DSSS-preamble 头部功率渐升阶段的信号存在较明显的差异。

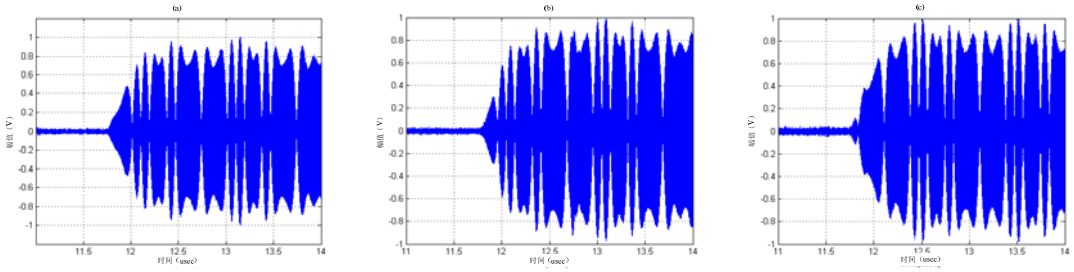

图 5.3 三只 IEEE 802.11b 无线设备的 DSSS-preamble 头部

18 只该型号 IEEE 802.11b 无线网卡被用于实验，功率设为“continuous access”模

式，前导设为“short”模式。采用“IEEE 802.11b 射频信号采集及处理系统”采集每只无线网卡的帧射频信号样本，并采用如图 5.4 所示的软件无线电系统对采集的射频信号样本进行处理。

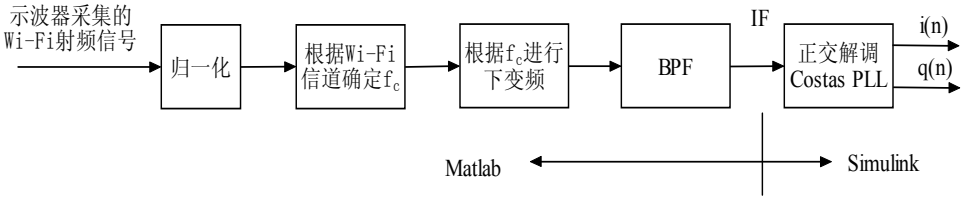

图 5.4 射频指纹识别的软件无线电系统

如图 5.4 所示，首先使用 Matlab 对接收 IEEE 802.11b DSSS-preamble 头部射频信号进行基于 Wi-Fi 信道频率 f_c、中频频率为 200MHz/带宽为 400MHz 的软件下变频；然后进行带通滤波，得到中频信号 IF；接着使用 Simulink 对得到的中频信号 IF 进行基于 Costas PLL 的正交解调，得到 I 路基带解调信号 $i(n)$与 Q 路基带解调信号 $q(n)$；最后计算包络 $a(n)=\sqrt{i(n)^2+q(n)^2}$ 。

图 5.4 中的正交解调 Costas PLL 如图 5.5 所示。

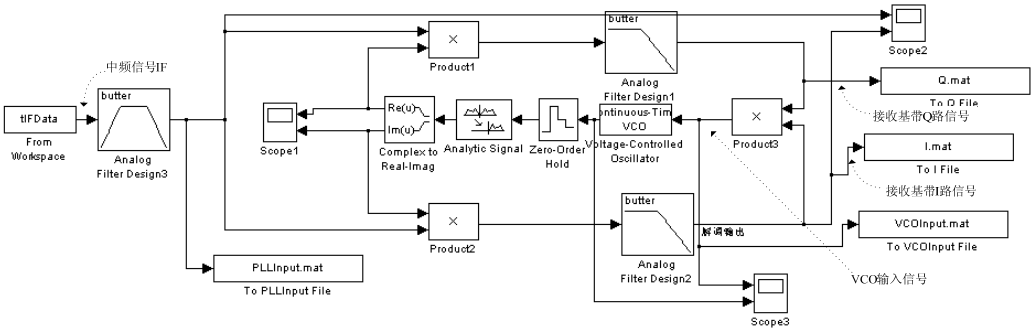

图 5.5 正交解调 Costas PLL

图 5.5 中，输入变量 tIFData 为中频信号，输出文件 I.mat 为 $i(n)$，输出文件 Q.mat 为 $q(n)$。

图 5.3 中的 IEEE 802.11b DSSS-preamble 射频信号经图 5.4 所示的软件无线电系统处理后的结果如图 5.6 所示。图 5.6 的子图（a）为 PLL 模块的 VCO 输入信号；子图（b）为中频信号 IF 及人工同步码后的 $i(n)$、$q(n)$与 $a(n)$；子图（c）为子图（b）的头部信号放大图。从图 5.6 可以看出，由 I 路与 Q 路基带解调信号得到的包络信号 $a(n)$与中频信号 IF 的包络吻合；VCO 锁定后，I 路基带解调信号 $i(n)$与中频信号 IF 的包络一致，Q 路基带解调信号 $q(n)$=0。

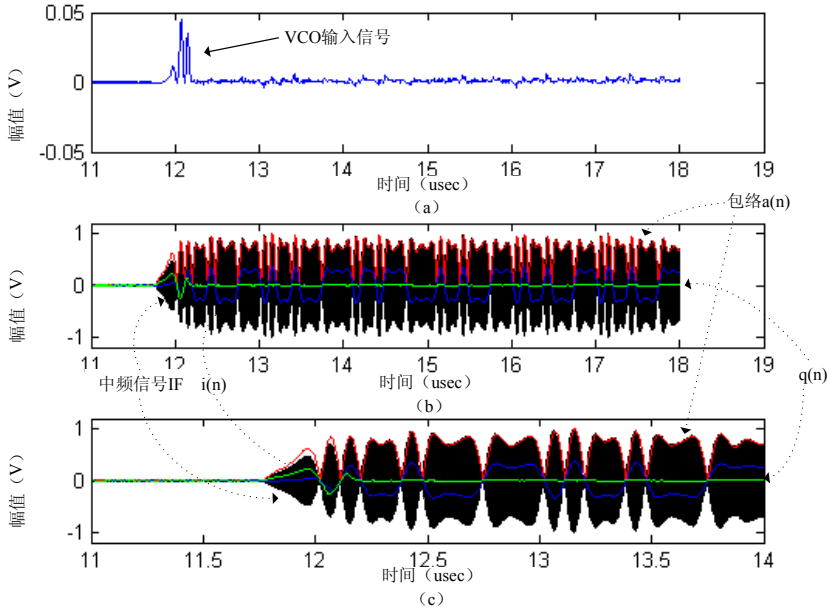

图 5.6 中频信号、正交解调基带信号及其包络等

对人工同步后的 $i(n)$信号进行抽取，得到一个码片一个样点的码片信号 $c(n)$，如图 5.7 所示。其中，子图（b）是子图（a）的头部放大图，而子图（a）包括中频信号 IF 及人工同步后的 $i(n)$与 $c(n)$。

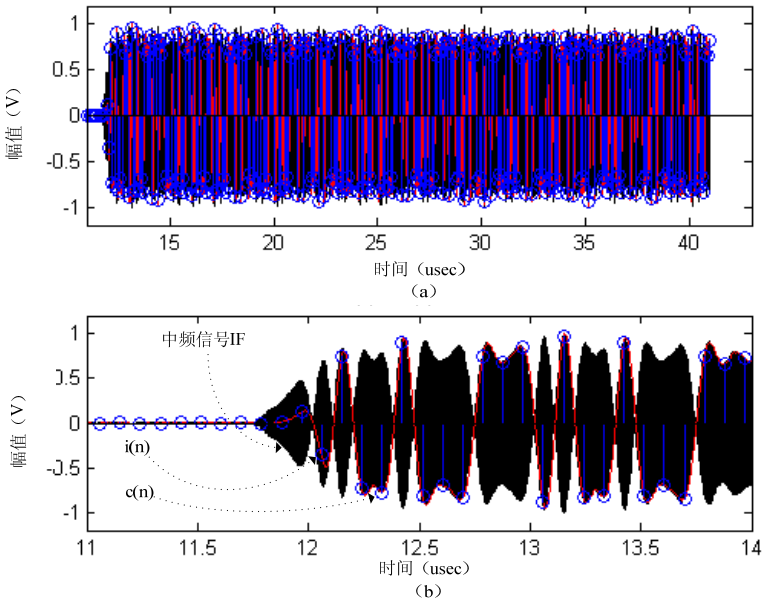

图 5.7 IF、i(n)及 c(n)对比图

接着对 $c(n)$进行 Barker 码解码，11 个码片对应一个符号，得到 Barker 码信号 $b(n)$；然后对 $b(n)$进行 DBPSK 解码，得到接收基带数字信号 $d(n)$；最后把 $d(n)$与 IEEE 802.11b 标准规定的同步码信号 $I(n)$进行比较，如图 5.8 的子图（a）、（b）与（c）所示。从图 5.8 中可以看出，该 IEEE 802.11b 无线网卡帧的第一个完整 Barker 码符号之前的 2 个符号在功率渐升阶段被“吃掉”了，后续码与标准相合。

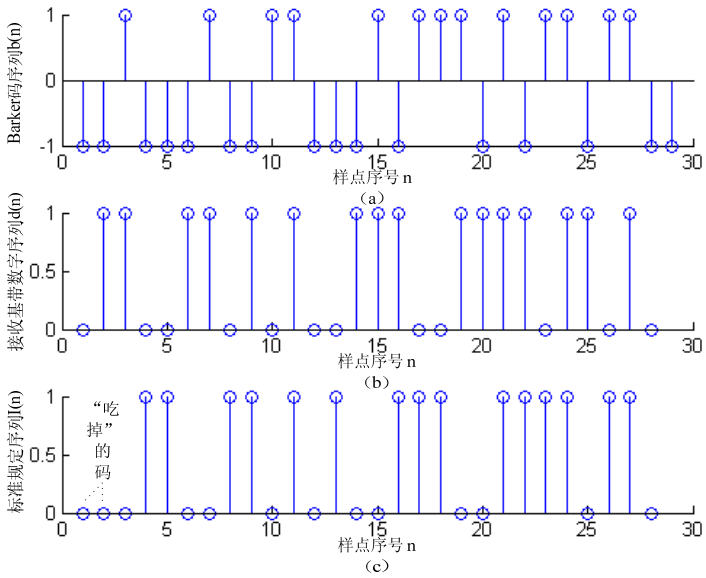

图 5.8 Barker 码解码对比

由于 IEEE 802.11b/g 规定其 DSSS-preamble 采用 11chips 的 Barker 码（10110111000）扩频的 DBPSK 调制方式，因而其包络 $a(n)$是周期为 1usec 的周期信号，其完整基本周期波形是确定的。把 $a(n)$的第一个完整基本周期波形起始点作为参考时刻，记为 P_{ref}；采用第四章提出的基于前导的射频指纹检测方法对包络 $a(n)$进行 P_{ref}检测；从 P_{ref}向历史时间方向截取 1usec 作为 ramp-up 射频指纹用于实验；并把所有 ramp-up 射频指纹按 P_{ref}对齐。根据人工观察，18 只无线网卡的 ramp-up 射频指纹可分为 5 个子类，表示为 A、B、C、D 与 E；从各子类无线网卡的样本中随机选择 50 个样本，根据 P_{ref}对齐后如图 5.9 所示，其中子图（a）、（b）、（c）、（d）与（e）分别是各 ramp-up 射频指纹子类样本的对齐图。

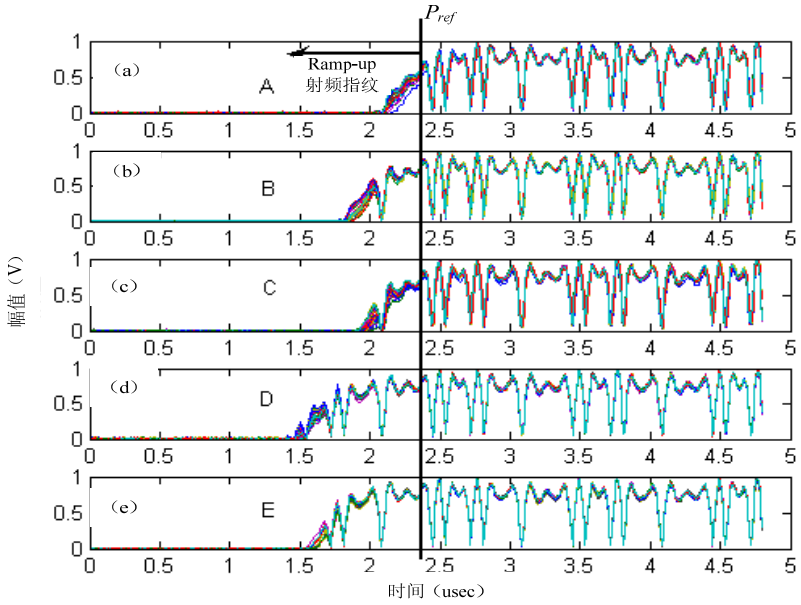

图 5.9 类的样本对齐图

从图 5.9 可知，5 子类 ramp-up 射频指纹之间存在一些大的差异。根据 IEEE 802.11b 标准对 DSSS-preamble 的接收基带信号进行解码分析，结果显示：

- 每个网卡的 DSSS-preamble 头部都损失了 2 或 3 个完整 DBPSK 符号；
- 其它的 DBPSK 符号与标准相符。

因此，ramp-up 射频指纹是功率渐升期间的残留 Barker 码信号包络。各 ramp-up 射频指纹子类的无线网卡数目如表 5.1 所示。

表 5.1 各 ramp-up 射频指纹子类无线网卡数目

ramp-up 射频指纹子类	A	B	C	D	E
无线网卡数目	3	5	4	2	4

5.3.2.2 Ramp-up 射频指纹分类实验

5. 3. 2. 2. 1 相像系数特征提取方法

尽管文献中有许多种特征提取方法，文献[67, 109]提出的相像系数特征提取方法很适合在这里使用，该特征提取方法简介如下。

定义 设有两个一维连续正值实函数$f(x)$和$g(x)$，即$f(x)\geq 0$，$g(x)\geq 0$，定义系数

$$c_{rc}=\frac{\int f(x)g(x)dx}{\sqrt{\int f^2(x)dx}\sqrt{\int g^2(x)dx}} \tag{5.8}$$

为函数$f(x)$与$g(x)$的相像系数。公式(5.8)中积分的范围为函数的定义域，且函数$f(x)$与$g(x)$在其定义域内不恒为0。由于公式(5.8)中的系数能表征两函数形状的差异，即两函数的形状是否相像，因而称为相像系数。

式（5.8）的实质是$g(x)$对$f(x)$投影的归一化处理。如果将函数$g(x)$投影到不同的两函数$f_1(x)$与$f_2(x)$上，则可以得到两个不同的投影值，若$f_1(x)$与$f_2(x)$正交，则所得的投影为函数$g(x)$在两正交坐标上的投影，若$f_1(x)$与$f_2(x)$不正交，则为一种斜投影。

性质 相像系数C_{rc}的取值范围为

$$0\leq C_{rc}\leq 1 \tag{5.9}$$

由于相像系数定义中的函数为正值实函数，由著名的Cauchy Schwartz不等式可得：

$$0\leq \int f(x)g(x)dx\leq \sqrt{\int f^2(x)dx}\bullet\sqrt{\int g^2(x)dx} \tag{5.10}$$

$$0\leq \frac{\int f(x)g(x)dx}{\sqrt{\int f^2(x)dx}\bullet\sqrt{\int g^2(x)dx}}\leq 1 \tag{5.11}$$

由于Cauchy Schwartz不等式右边取等号的条件是$f(x)$与$g(x)$相等，所以可得函数$f(x)$与函数$g(x)$相等时相像系数取的最大值1；实际上，当$f(x)$是$g(x)$的某个固定常数倍时，相像系数就为1。不等式左边取等号的条件是$f(x)$与$g(x)$的乘积的积分为0，即函数$f(x)$与$g(x)$正交。

若将式（5.8）中的函数*f*(*x*)与*g*(*x*)进行分解，分解后信号分别用$\{S_1(i)\}$与$\{S_2(i)\}$表示，则有

$$f(x)=\sum[S_1(i)\cdot \sin c(x-i\cdot T)] \tag{5.12}$$

及

$$g(x)=\sum[S_2(i)\cdot \sin c(x-i\cdot T)] \tag{5.13}$$

式(5.12)与式(5.13)中，*T*为采样周期，函数*sinc*()为采样函数，即

$$\sin c(t)=\begin{cases}1, t=0\\ \dfrac{\sin(\pi t)}{\pi t}, t\neq 0\end{cases} \tag{5.14}$$

则离散化的相像系数

定义 设有两个一维离散正值信号序列$\{s_1(i), i=1,2,...,N\}$和$\{s_2(j), j=1,2,...,N\}$，即$s_1(i)\geq 0$，$s_2(j)\geq 0$，定义系数

$$c_{rc}=\frac{\sum s_1(i)s_2(j)}{\sqrt{\sum {s_1}^2(i)}\sqrt{\sum {s_2}^2(j)}} \tag{5.15}$$

为信号序列$s_1(i)$与$s_2(j)$的相像系数。公式(5.15)中$s_1(i)$与$s_2(j)$不恒为0。C_r的取值范围在0与1之间，当两信号序列成固定比例时，C_r取最大值1，当两信号正交时，C_r取值为0。

假设数字化射频指纹序列为*RFF*(*k*)，假设两用于投影的信号序列为矩形信号序列*U*(*k*)与三角形信号序列*T*(*k*)

$$U(k)=\begin{cases}mx, 1\leq k\leq N\\ 0, other\end{cases} \tag{5.16}$$

$$T(k)=\begin{cases}2k\cdot mx/N, 1\leq k\leq N/2\\ 2mx-2k\cdot mx/N, N/2\leq k\leq N\end{cases} \tag{5.17}$$

式(5.16)与式(5.17)中，*mx*可以设为*RFF*(*k*)的最大值；*N*为偶数。由于矩形信号的能量分布均匀，而三角形信号的能量分布较集中，将射频指纹序列*RFF*(*k*)向这两种信号序列投影，可反映出射频指纹序列*RFF*(*k*)的能量分布情况。

因此，基于相像系数的数字化射频指纹特征提取方法的步骤如下：

步骤1：计算射频指纹序列*RFF*(*k*)与矩形序列*U*(*k*)的相像系数

$$c_{r1}=\frac{\sum RFF(i)U(j)}{\sqrt{\sum RFF^2(i)}\sqrt{\sum U^2(j)}} \tag{5.18}$$

步骤2：计算射频指纹序列*RFF*(*k*)与三角形序列*T*(*k*)的相像系数

$$c_{r2}=\frac{\sum RFF(i)T(j)}{\sqrt{\sum RFF^2(i)}\sqrt{\sum T^2(j)}} \tag{5.19}$$

步骤3：把c_{r1}与c_{r2}构成特征矢量CR=<c_{r1},c_{r2}>。

文献[67]对相像系数特征提取方法进行了抗噪性能分析，结果表明：当信噪比大于

5dB时，相像系数特征值趋于稳定。

由以上分析可知，相像系数特征提取方法用二维量刻画了射频指纹序列的形状特征，同时实现了降维，适合用作射频指纹的一种基本特征提取方法。

5.3.2.2.2 K-近邻分类方法

最近邻模式分类方法是Cover. T与1967年提出的[110]；*k*-近邻分类是将一个测试样本分类为与它最接近的*k*个训练样本中出现最多的那个类[111]。

对于c类问题，设类$w_i(i=1,2,...,c)$有N_i个样本$x_j^{(i)}(j=1,2,...,N_i)$。分类思想是，对于一个待识别模式x，分别计算它与$N=\sum_{i=1}^{c}N_i$个已知类别的样本$x_j^{(i)}$的距离，将它判为距离最近的那个样本所属的类。在这样的分类思想下，w_i的判决函数为

$$d_i(x)=\min_{j=1,2,...,N_i}\| x-x_j^{(i)} \|, i=1,2,...,c \tag{5.20}$$

判决规则为：如果$d_m(x)=\min_{i=1,2,...,c} d_i(x)$，则判为$x\in w_m$ 。

当上述方法只根据离待识别模式最近的一个样本的类别而决定其类别，通常称为1-NN方法。当考察待识别模式的*k*个最近邻样本，这*k*个最近邻元中哪一类的样本最多，就将*x*判属哪一类。设$k_1,k_2,...,k_c$分别为待识别模式*x*的*k*个最近邻样本实属$w_1,w_2,...,w_c$类的样本数，定义w_i的判决函数为

$$d_i(x)=k_i, i=1,2,...,c \tag{5.21}$$

判决规则为：如果$d_m(x)=\max_{i=1,2,...,c} d_i(x)$，则判为$x\in w_m$。称为*k*-NN近邻分类方法。

5.3.2.2.3 Ramp-up 射频指纹分类实验

对图5.9所示的ramp-up 射频指纹子类样本进行相像系数特征提取与*k*-NN分类实验。首先对ramp-up射频指纹子类样本信号进行抽取，使其采样率降为普通的100MSps；然后采用软件对样本信号进行加AWGN噪声处理，使其SNR为18dB；接着进行相像系数特征提取，采用式（5.16）与式（5.17）所示的矩形与三角形基函数进行投影，得到的5子类ramp-up射频指纹样本的特征分布如图5.10所示。

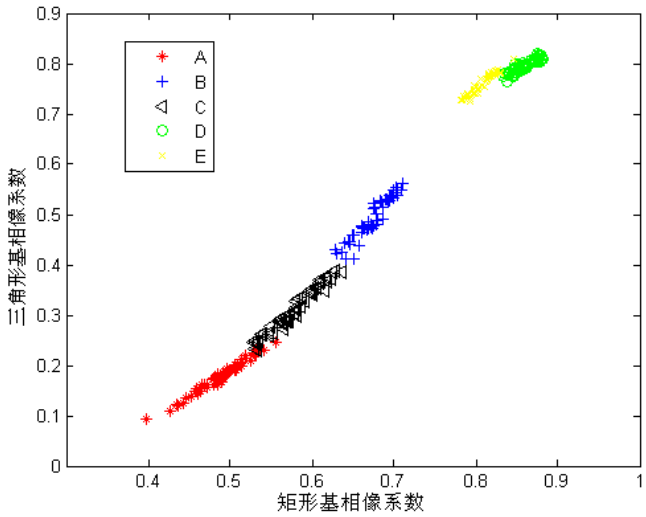

图 5.10 五子类 ramp-up 射频指纹样本的特征分布

接着从各50个ramp-up射频指纹子类样本特征中随机选择k个作为训练集，从各剩余的50-k个样本中随机选择10-k个样本作为测试集，进行各子类的k-NN分类实验。得到的ramp-up射频指纹子类的正确识别率如表5.2所示。

表 5.2 两种射频指纹的 k-NN 识别率

射频指纹	1-NN(%)	2-NN(%)	3-NN(%)	4-NN(%)
ramp-up 射频指纹子类	88.89	90.00	94.29	100.00
turn-on 射频指纹	15.56	22.50	28.57	26.67

表5.2中turn-on射频指纹识别率是根据图5.2所示5只IEEE 802.11b/g无线网卡样本获得；该5只无线网卡的功率控制方式为阶跃方式（未按标准执行）；其样本采集条件、采样率、SNR及k-NN分类器与ramp-up 射频指纹采用的各项相同。

从表5.2可知，根据ramp-up射频指纹可把同一厂家同一型号的基于前导的无线设备以较高的正确识别率分为多个子类；而根据turn-on射频指纹识别无线网卡的正确识别率低。

本节提出的ramp-up射频指纹的产生技术，即无线发射机功率开始渐升的同时发起前导序列发送，可应用于无线设备的设计、制造并规定到相关标准中。

本节中的ramp-up射频指纹是前导信号包络，前导信号相位等也可作为其它种类的ramp-up射频指纹。

5.3.3 小结

本节提出了变换无线设备功率渐升期间发送的前导信号为一种称为“ramp-up射频指纹”的射频指纹产生方法，理论分析与实验表明：ramp-up射频指纹的可分性优。

但是，根据本节提出的ramp-up射频指纹并不能把所有相应的无线网卡都以较高正确识别率区分开。例如，本节中，对于18个待识别IEEE 802.11b/g无线网卡，根据ramp-up

射频指纹仅能以较高正确识别率分为5个子类。

本节提出的 ramp-up 射频指纹可应用于相关无线设备的多射频指纹识别中。

5.4 Wi-Fi 信号的相空间差射频指纹识别方法

由第二章的“无线设备的射频信号模型”可知：当采用BPF滤除无线设备发送射频信号的带外成分后，其带内仍存在一定的非线性成分，当带内非线性成分相对于线性成分较小时，无线设备的发射机可建模为线性系统；当不对接收无线信号进行BPF滤波时，无线设备的发射机可建模为非线性系统。

线性系统中，系统状态变化与该系统的先前状态成比例、相差常量或是两者组合。非线性系统指系统的状态变化以复杂方式依赖于系统的先前状态，这里的“复杂方式”指除按比例、相差常量及这两者组合之外的任何其它方式。非线性系统常用非线性微分方程组或非线性差分方程组描述。与线性系统相比，非线性系统具有更复杂的性质。首先，线性系统经常采用的叠加原理对非线性系统不再适用。其次，非线性系统运动的周期不像线性系统那样仅由系统性质确定，一般还与初始条件相关。第三，非线性系统可能具有多个平衡位置和稳态运动，系统的动力学行为既取决于这些平衡位置和稳态运动的稳定性，也与初始条件有关。第四，对工程中的非线性机械、结构和机电系统，系统的响应与激励频率存在复杂的依赖关系，而线性系统响应与激励的频率是相同的。最后，线性系统仅存在周期运动和准周期运动两种有限运动，非线性系统存在其它复杂运动现象[112] [113]。

非线性动力学研究非线性系统的状态变量随时间变化规律的学科，尤其是系统的长时间演化行为中的复杂性。对于有限维系统，主要内容是混沌、分岔和分形等。混沌是由确定性动力学系统产生，服从确定性规律，对初值极为敏感并具有内在随机性的运动。分岔指非线性系统的定性行为随系统参数改变而发生质的变化的性质。分形是没有特征尺度而又具有自相似性的几何结构，用于描述破碎、不规则的复杂几何形体。

本节基于非线性动力学理论，把无线设备发送的射频信号建模为非线性时间序列，对待识别无线设备的发射机等效系统进行相空间重构。在再现文献[102]提出的根据功率放大器的相空间差识别功率放大器硬件的基础上，提出Wi-Fi信号的相空间差射频指纹变换方法，并采用实验进行了验证。

5.4.1 时间序列的相空间重构

5.4.1.1 基本概念

非线性系统通常使用非线性常微分方程组描述，而常见的非线性微分方程都可以化为自治的一阶常微分方程组。因此，非线性系统可以用一阶自治方程组

$$\begin{bmatrix} x_1^{'} \\ x_2^{'} \\ . \\ . \\ . \\ x_n^{'} \end{bmatrix} = \begin{bmatrix} f_1(x_1, x_2, \cdots, x_n) \\ f_2(x_1, x_2, \cdots, x_n) \\ . \\ . \\ . \\ f_n(x_1, x_2, \cdots, x_n) \end{bmatrix} \tag{5.22}$$

描述。其中 $x_i, i = 1,2,...,n$ 为非线性系统的状态变量， $x_i^{'}, i = 1,2,...,n$ 为状态变量的一阶导数，写成矢量形式

$$\mathbf{x}^{'} = \mathbf{f}(\mathbf{x}) \tag{5.23}$$

式中

$$\mathbf{x} = (x_1, x_2, ..., x_n)^T \in \mathbf{R}^n \tag{5.24}$$

$$\mathbf{f} = (f_1, f_2, ..., f_n)^T \in \mathbf{R}^n \tag{5.25}$$

其中，*T*表示矩阵的转置，$\mathbf{R}^n$ 为状态变量 x_i 所张的*n*维欧几里得空间，称为相空间（phase space）或状态空间(state space)，而 $\mathbf{x}$ 是其中的矢量，其第*i*方向的分量就是 x_i 。显然，用相空间分析非线性系统的运动规律具有几何学直观的优势。方程组（5.22）或方程（5.23）称为动力学方程的标准形式，代表所要分析的动力学系统状态变化的规律，被称为动力学方程、运动方程或状态方程。动力学方程中只含有状态变量及其导数的一次项时，称系统为线性的；动力学方程中含有状态变量及其导数的高次项时，称系统为非线性的。

在相空间中，每一时刻的状态用相空间的一点或矢量 $\mathbf{x}$ 表示，状态随时间的变化则是相空间中的轨迹，也就是方程（5.23）的解曲线或积分曲线，轨迹形成的一个不变集合，称为吸引子(attractor)。相空间中状态变量的轨迹具有时间平移不变性，体现了系统动力学的规律[113]。

Henon吸引子[114]是最著名的简单动力学系统之一，是由Henon M.在研究天体问题时提出的吸引子模型，其映射方程为

$$\begin{cases} x(n+1) = 1 - ax^2(n) + y(n) \\ y(n+1) = bx(n) \end{cases} \tag{5.26}$$

当系统系数*a*=1.2、*b*=0.3，初始状态[*x*(0),*y*(0)]分别为(0.4, 0.6)与(0.35, 0.55)时，其相空间轨迹[*x*(*n*),*y*(*n*)]为图5.11所示，其中子图（a）中轨迹的初始状态为（0.4,0.6），子图（b）中轨迹的初始状态为(0.35,0.55)。

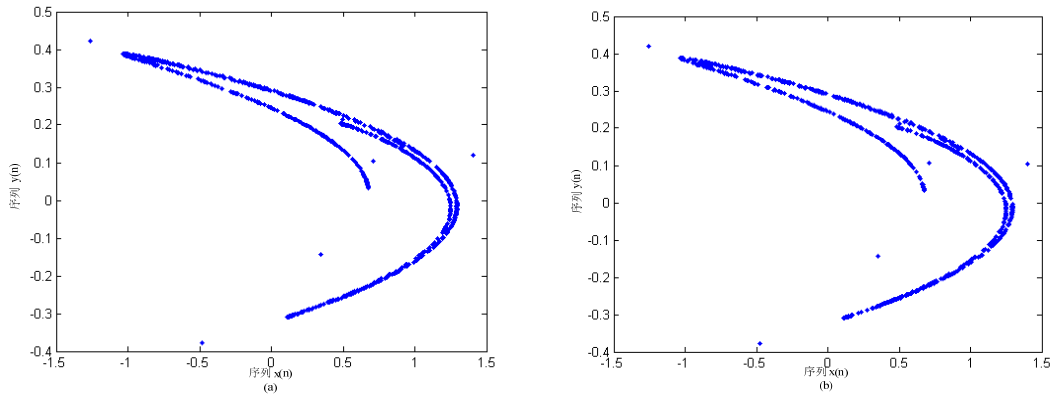

图 5.11 初始状态不同、系统系数
相同时的 Henon 吸引子相空间轨迹

由图5.11可知，系统系数不变的两系统的相空间轨迹基本相同。

当初始状态为(0.3,0.5)，系统系数分别为a=1.2、b=0.3与a=1.2、b=0.4时，其相空间轨迹如图5.12所示，其中子图（a）中轨迹的b=0.3，子图（b）中轨迹的b=0.4。

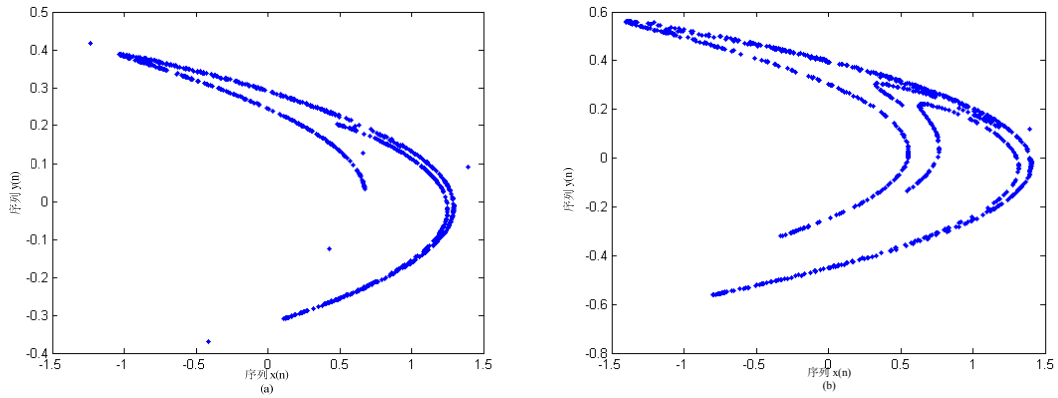

图 5.12 初始状态相同、系统系数
不同时的 Henon 吸引子相空间轨迹

由图5.12可知，系统系数的微小变化会产生相空间轨迹的较大变化。

5.4.1.2 相空间重构方法

由于非线性系统的动力学方程一般没有解析解，因而其全部状态变量一般无法获得。而且，通常来讲，非线性系统的相空间维数可能很高，甚至是无穷大，并且大部分情况下维数不能直接获得。实际问题中，大部分情况下观测到的只是一个状态变量的时间序列。但是，一个状态变量的变化是由整个系统的运动规律决定的，所以一个状态变量的时间序列隐含着整个动力学系统的运动规律。所以，有可能根据一个观测到的状态变量序列重构系统的相空间。

一种方法是求出状态变量$y(t)$的各阶导数，然后用$y(t)$及其各阶导数组成相空间。但是，由于时间序列计算出的导数一般误差较大，在有噪声情况下更甚，因此这种方法构造的相空间质量大大降低。

Takens与Packerd等[115, 116]提出了用单变量时间序列构造相空间的方法 —— 延迟坐

标状态空间重构法，即采用原始系统中的某状态变量的延迟来重构相空间。其中，Takens证明了可以找到一个合适的嵌入维，即如果延迟坐标的维数大于等于动力学系统维数的2倍加1，在这个嵌入维空间里可以把有规律的吸引子恢复出来。也即在重构的相空间中的轨迹上原动力学系统保持微分同胚，从而为时间序列的相空间重构奠定了坚实的理论基础。

定义 设(N,ρ)、(N_1,ρ_1)是两个度量空间，如果存在映射$\varphi:N\to N_1$满足：（1）φ满射；（2） $\rho(x,y)=\rho_1(\varphi(x),\varphi(y))(\forall x,y\in N)$，则称$(N,\rho)$、$(N_1,\rho_1)$是等距同构的。

定义 如果(N_1,ρ_1)与另一度量空间(N_2,ρ_2)的子空间(N_0,ρ_2)是等距同构的，则称(N_1,ρ_1)可以嵌入(N_2,ρ_2)。

Takens 定理 M是d维流形，$\varphi:M\to M$，φ是一个光滑的微分同胚，$y:M\to R$，y有二阶连续导数，$\phi(\varphi,y):M\to R^{2d+1}$，其中

$$\phi(\varphi,y)=(y(x),y(\varphi(x)),y(\varphi^2(x)),...,y(\varphi^{2d}(x))) \tag{5.27}$$

则$\phi(\varphi,y)$是M到R^{2d+1}的一个嵌入。

证明详见文献[116]。

延迟坐标状态空间重构法的具体步骤为：设动力学系统的某个状态变量为$y(t)$，适当选取一个时间延迟量τ，取$y(t)$、$y(t+\tau)$、$y(t+2\tau)$、…、$y[t+(m-1)\tau]$为坐标，构造一个m维空间。这样重构的相空间中的轨迹分布或结构（吸引子）便可反映系统的运动特征。当重构相空间中的轨迹趋于一点时，即对应原相空间的吸引子，这表示系统处于稳定定态；当轨迹构成一个闭曲线，表明系统在作周期运动；当轨迹最后是杂乱无章地密集在一有限范围内，表示系统在作随机运动；当轨迹分布有一些特殊的结构，则系统可能存在混沌。

由延迟坐标状态空间重构法的具体步骤可知，时间延迟τ与嵌入维数m参数的选取具有十分重要的意义。如果参数选取合适，则重构的相空间与原相空间相同或近似，反之重构的相空间与原相空间差异大，自然不能反映系统运动的特征。同时，延迟坐标状态空间重构法中时间延迟τ与嵌入维数m的选取也是十分困难的。比较常用的参数选取方法是“互信息量估计延迟时间法”与“Cao氏嵌入维数确定法”。

5.4.1.2.1 互信息估计延迟时间法

“互信息量估计延迟时间法”是根据系统状态变量某一时刻(t)的信息量与另一时刻$(t+\tau)$的信息量之间关系估计相空间重构的时间延迟参数。设一个时间序列及其时间延迟用A与B表示，测量结果为a_i与b_k的概率分别是$P_A(a_i)$和$P_B(b_k)$；令$P_{AB}(a_i,b_k)$表示同时对A和B进行观测、结果分别为a_i和b_k的概率，于是互信息量为

$$
\begin{aligned}
I_{AB}(a_i,b_k) &= \log_2[\frac{P_{AB}(a_i,b_k)}{P_A(a_i)P_B(b_k)}] \\
&= -\log_2[P_A(a_i)] - \log_2[P_B(b_k)] - \{-\log_2[P_{AB}(a_i,b_k)]\} \\
&= H_A(a_i) + H_B(b_k) - H_{AB}(a_i,b_k)
\end{aligned} \tag{5.28}
$$

其中，$H_A(a_i)$与$H_B(b_k)$分别为A与B的熵，$H_{AB}(a_i,b_k)$为A与B的联合熵。对所有观测结果的平均互信息量为

$$
I_{AB} = \sum_{a_i,b_k} P_{AB}(a_i,b_k) I_{AB}(a_i,b_k) \tag{5.29}
$$

I_{AB}统计地度量了A与B的相互关联程度，当A与B相互完全无关时，即

$$
P_{AB}(a_i,b_k) = P_A(a_i)P_B(b_k) \tag{5.30}
$$

则

$$
I_{AB}(a_i,b_k) = 0 \tag{5.31}
$$

当A为观测到的动力学系统的某个状态变量$y(k)$，B为$y(k+\tau)$，则平均互信息量为

$$
I(\tau) = \sum_k P[y(k), y(k+\tau)] \log_2 \{\frac{P[y(k), y(k+\tau)]}{P[y(k)]P[y(k+\tau)]}\} \tag{5.32}
$$

可以取$I(\tau)$第一次到达最小值时的τ作为延迟量的适当值。

5.4.1.2.2 Cao 氏嵌入维数确定法

文献[117]介绍的“Cao氏嵌入维数确定法”是一种实用的根据时间序列确定最小嵌入维数的方法，具有以下优点：（1）除了延迟时间必须先验给出外，不含任何主观参数；（2）不过分依赖时间序列的长短；（3）能够清晰地区分确定性信号与随机噪声；（4）对于具有高维吸引子的时间序列工作良好。

设一个时间序列为$x_1, x_2, ..., x_N$，第i个重建的d维时间延迟矢量为

$$
y_i(d) = (x_i, x_{i+\tau}, ..., x_{i+(d-1)\tau}), i = 1, 2, ..., N - (d-1)\tau \tag{5.33}
$$

其中d为嵌入维数，τ为时间延迟，定义

$$
\begin{aligned}
a(i,d) &= \frac{\| y_i(d+1) - y_{n(i,d)}(d+1) \|}{\| y_i(d) - y_{n(i,d)}(d) \|}, \\
i &= 1, 2, ..., N - d\tau
\end{aligned} \tag{5.34}
$$

其中$\|\bullet\|$表示某种欧氏距离度量，这里为

$$
\| y_k(m) - y_l(m) \| = \max_{0 \le j \le m-1} | x_{k+j\tau} - x_{l+j\tau} | \tag{5.35}
$$

$y_i(d+1)$表示第i个重建的$d+1$维矢量，例如，$y_i(d+1) = (x_i, x_{i+\tau}, ..., x_{i+d\tau})$；$n(i,d)(1 \le n(i,d) \le N - d\tau)$是在$d$维重建相空间中，在定义的$\|\bullet\|$含义下，使$y_{n(i,d)}(d)$是$y_i(d)$的最近邻的整数。

如果d是相空间的嵌入维，根据嵌入定理[116, 118]，在d维重建相空间内临近的任何两点在$d+1$维重建相空间中仍是临近的。这样的邻居称为真邻居，否则称为假邻居。完美

的嵌入意味着没有假邻居存在。

定义$a(i,d)$的平均值

$$E(d)=\frac{1}{N-d\tau}\sum_{i=1}^{N-d\tau}a(i,d) \tag{5.36}$$

$E(d)$仅依赖于维数d与延迟τ，为了研究维数由d增加到维数$d+1$后的变化，定义

$$E_1(d)=\frac{E(d+1)}{E(d)} \tag{5.37}$$

则，如果时间序列来源于某个吸引子，当d大于某个值d_0后，$E_1(d)$不再增加，而d_0+1就是寻找的最小嵌入维数。

5.4.1.2.3 相空间重构例子

为验证根据时间序列进行相空间重构时的“互信息量估计延迟时间法”与“Cao氏嵌入维数确定法”的正确性，采用两个例子进行实验，其中一个是离散映射得到的时间序列，另一个是连续系统采样后得到的时间序列。

例子1：Henon映射序列的相空间重构。取初始状态为(0.3,0.5)，a=1.2,b=0.4时Henon映射的一个状态变量$y(n)$作为时间序列，如图5.13所示。

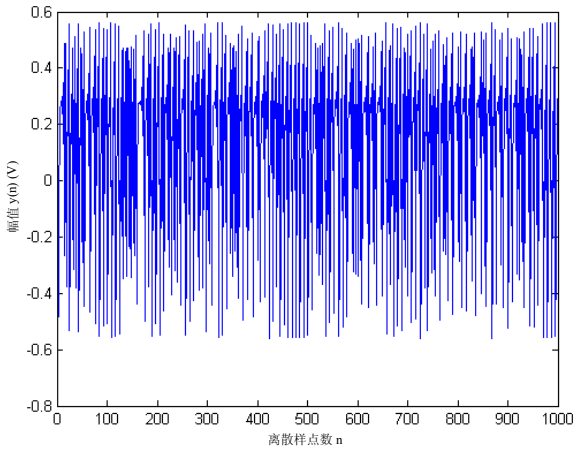

图 5.13 Henon 映射的一个状态变量时间序列

由于是离散映射，因而延迟时间τ为1，对其进行“Cao氏嵌入维数确定”，其$E_1(d)$随维数d的变化如图5.14所示。

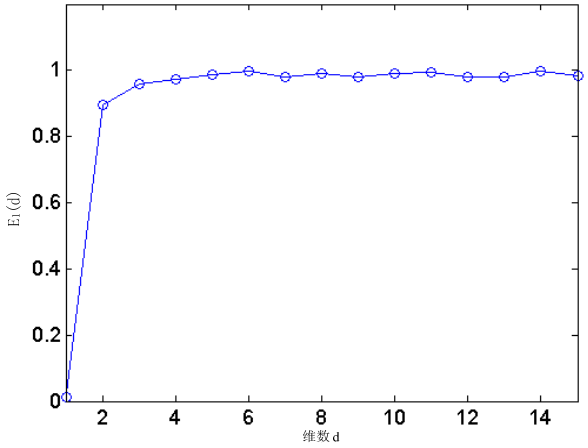

图 5.14 $E_1(d)$随维数 d 的变化图

由图5.14可知，当d大于2后，其E_1值不再增加，因此其维数为2。根据τ=1，d=2进行相空间重构，结果如图5.15所示。

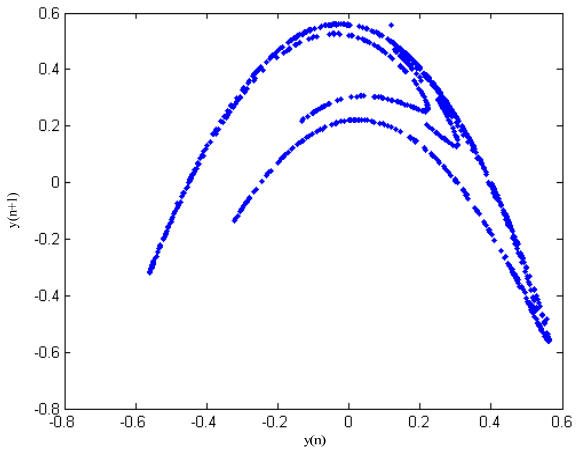

图 5.15 τ=1，d=2 的相空间重构

由图5.15可知，重建后Henon轨迹与图5.12形状相同，只是发生了旋转而已。

例子2：阻尼单摆实验。假设时刻t的单摆位置为$x(t)$，满足

$$x(t) = e^{-at}\sin(wt) \tag{5.38}$$

当a=0.3、w=2π弧度/秒时，t在0到400秒之内的波形如图5.16所示。

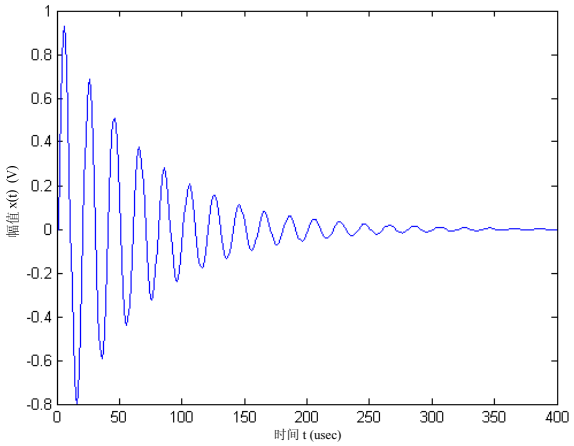

图 5.16 阻尼单摆位置波形

其中的采样率为20Sps，$x(t)$的导函数为

$$x'(t) = we^{-at}\cos(wt) - ae^{-at}\sin(wt) \tag{5.39}$$

表示t时的速率，把$x(t)$与$x'(t)$作为系统的状态变量，系统的相空间轨迹如图5.17所示。

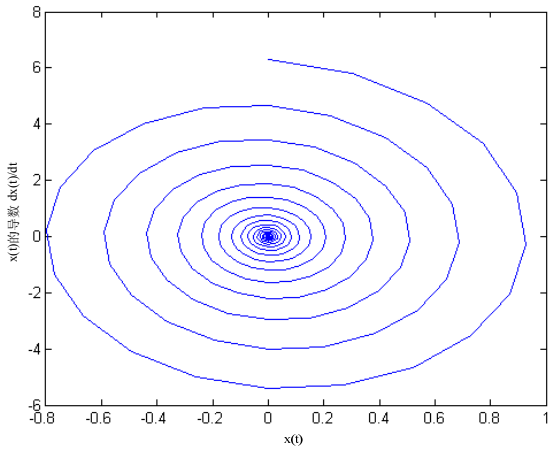

图 5.17 阻尼单摆系统的相空间轨迹

根据$x(t)$重构相空间，采用“互信息量估计延迟时间法”对重构采用的延迟时间进行估计，τ为0.25秒（对应于互信息量第一次到达局部最小值时的延迟样点数5），如图5.18所示。

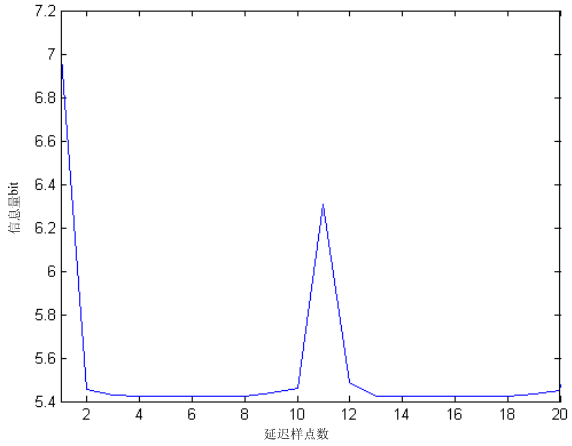

图 5.18 互信息量估计延迟时间

对其进行“Cao氏嵌入维数确定”，维数d与$E_1(d)$之间的关系如图5.19所示。

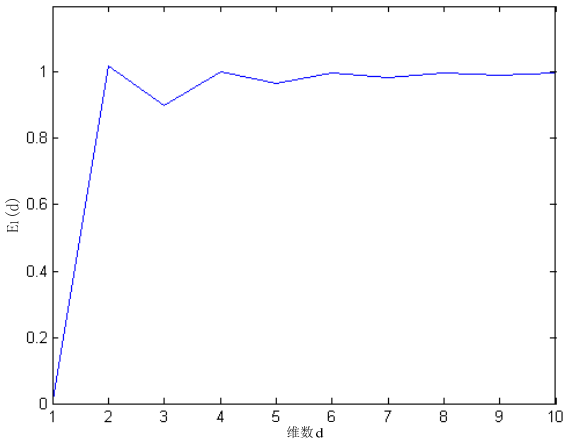

图 5.19 Cao 氏嵌入维数确定

由图5.19可知，最小维数为2，采用$\tau = 0.5$，d=2根据$x(t)$进行相空间重构，重构的相空间如图5.20所示。

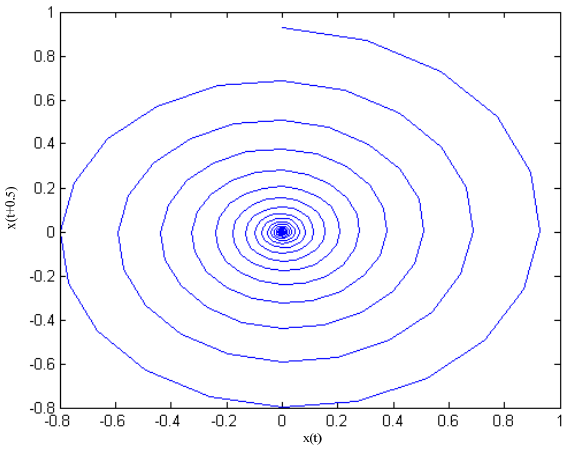

图 5.20 重构的阻尼单摆系统相空间

对比图5.17与图5.20可知，根据观测序列重构的相空间与原相空间相似，保持了原相空

间的吸引子、轨迹不相交等主要性质。

5.4.2 Wi-Fi 信号的相空间差射频指纹识别方法

根据非线性识别无线设备的文献几乎没有。文献[102]把功率放大器视为非线性系统，基于相空间重构方法，从功率放大器输出中抽取出非线性“签名”，用于非线性系统识别，该文献把提出方法称为“相空间差算法”。该方法基于以下两点：（1）任何放大器都具有非线性，因而可建模为动力学系统；（2）由同一信号驱动的同一种确定性动力学系统的相空间中的同一点应具有相同的导数。该文献针对同一调频信号驱动下的三个同种型号功率放大器进行了实验，有线连接下取得了良好的识别率。但是，由于该方法要考虑信号之间的相位相干问题，因而算法复杂。

本文把待识别Wi-Fi无线设备的发射机建模为非线性系统，根据Wi-Fi信号的特点，采用第四章提出的“射频指纹信号检测方法”实现了接收Wi-Fi信号的相位同步，从而提出比原“相空间差算法”更简单的识别方法，本文把该方法称为“Wi-Fi信号的相空间差射频指纹”识别方法。另外，本文在无线连接场景下对提出方法进行了实验验证。

假设待识别Wi-Fi无线设备的发射机用A、B、C等表示，则提出方法简述如下：

步骤1：对已知来源的Wi-Fi接收信号进行幅值归一化，并采用第四章提出的“基于Wi-Fi前导的射频指纹检测方法”获得相位同步，分别用$v_A(t)$、$v_B(t)$与$v_C(t)$等表示，作为参考信号；

步骤2：对未知信号采用“基于Wi-Fi前导的射频指纹检测方法”获得相位同步后并进行幅值归一化，用$u(t)$表示；

步骤3：把$u(t)$与$v_A(t)$、$v_B(t)$及$v_C(t)$等嵌入相同的相空间（相空间重构的参数采用相应方法估计获得）。假设$u(t)$嵌入相空间中的点用U_i表示，$v_A(t)$、$v_B(t)$及$v_C(t)$等嵌入相空间中的点分别用$V_{A,j}$、$V_{B,j}$及$V_{C,j}$等表示，i,j=1,2,…,N，N为相空间中点数；

步骤4：对于未知信号相空间中的任一点对(U_i，U_{i+1})，i=1,2,…,N-1，在一参考信号相空间中找到其最近邻，用（$V_{X,j}$，$V_{X,j+1}$）表示，计算两个点对之间的导数差（各导数差元素平方和的平方根）

$$D1(i,X)=|(V_{X,j+1}-V_{X,j})-(U_{i+1}-U_i)|, i=1,2,...,N \tag{5.40}$$

步骤5：计算未知信号相空间中的$D1(i,X)$的平均值

$$D2(X)=\frac{1}{N-1}\sum_{i=1}^{N-1}D1(i,X), X=A,B,C,... \tag{5.41}$$

步骤6：根据$D2(X)$，对未知信号进行判决。如果$D2_m=\min_{X=A,B,C,...}D2(X)$，则$u(t)$来源与$m$。即：未知信号与$D2(X)$最小的参考信号来自于同一个待识别Wi-Fi无线设备。

5.4.2.1 数值仿真例子

设Wi-Fi无线设备发射信号的中频信号为

$$s(t) = s_1(t) + \rho_3 s_1^3(t) \tag{5.42}$$

其中

$$s_1(t) = [m(t) * h_{tx}(t)] \bullet \cos(2\pi f_{IF} t) \tag{5.43}$$

为BPSK中频调制信号，ρ_3为3次非线性项系数，$m(t)$为基带发送数字信号，$h_{tx}(t)$为待识别发射机的等效低通滤波器脉冲响应，*为卷积运算，f_{IF}为中频频率。$m(t)$的数字序列的chip率为11Mbps，$h_{tx}(t)$为滚降因子k=0.5的升余弦21阶低通滤波器，f_{IF}为176MHz，采样率f_s为1.76GSps，$\rho_3 = 0.2$。比特数为110的一帧BPSK中频调制信号的时域波形如图5.21的子图（a）所示，而其功率谱如图5.21的子图（b）所示。

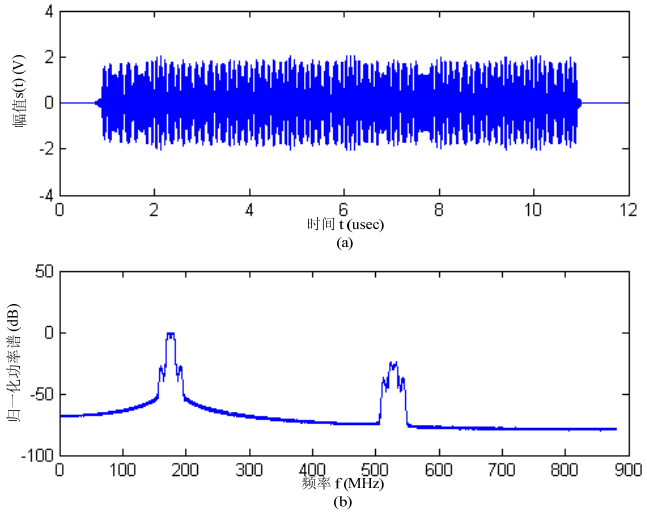

图 5.21 一帧 BPSK 中频调制信号的时域波形及其功率谱

把$s(t)$的离散序列视为时间序列，采用“互信息量估计延迟时间法”对相空间重构采用的延迟时间进行估计，延迟样点数为4时互信息量达到局部最小，如图5.22所示。

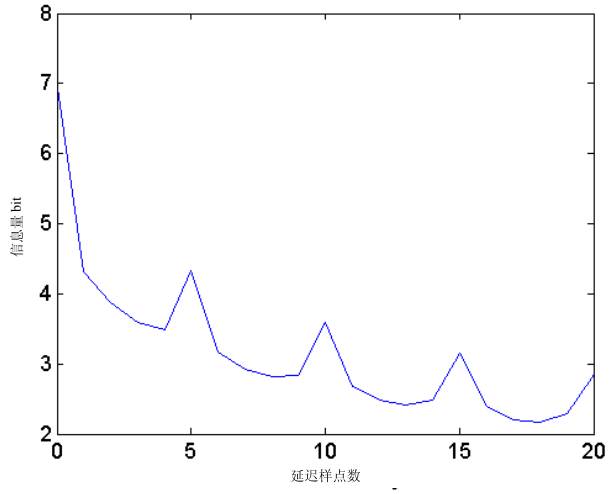

图 5.22 互信息量估计延迟时间

接着对时间序列$s(t)$进行“Cao氏嵌入维数确定”，当延迟样点数为4时，维数d与$E_1(d)$之间的关系如图5.23所示。

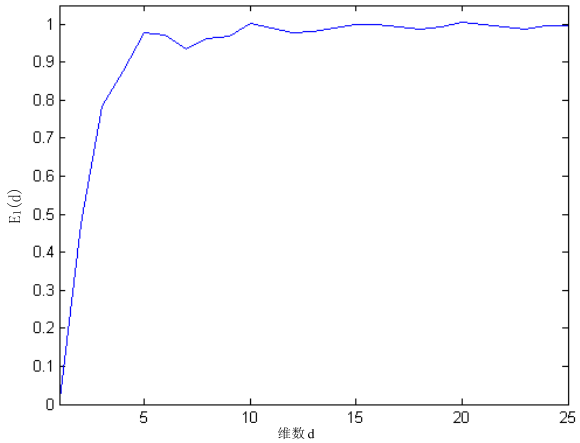

图 5.23 Cao 氏嵌入维数确定

由图5.23可知，最小维数为5。采用延迟样点数为4，d为5，根据$s(t)$进行相空间重构。

设式（5.42）的两个版本为$s_A(t)$与$s_B(t)$，其中$s_A(t)$为参考信号，$s_B(t)$为未知信号。设$\rho_3=0$，即$s_A(t)$与$s_B(t)$皆为线性的；设$s_A(t)$的$h_{tx}(t)$的滚降因子k=0.5，$s_B(t)$的$h_{tx}(t)$的滚降因子k分别为0.3、0.5与0.8。采用提出的“相空间差射频指纹变换方法”得到的$D2$与k之间关系如图5.24中实线所示。当$s_A(t)$与$s_B(t)$皆为非线性的，设$\rho_3=0.2$，采用提出的“相空间差射频指纹变换方法”得到的$D2$与k之间关系如图5.24中虚线所示。

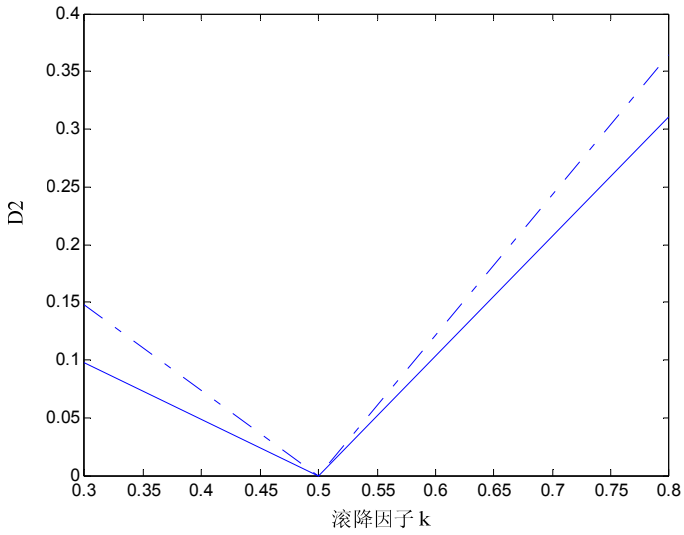

图 5.24 D2 与 k 之间的关系

由图5.24可知，$D2$对非线性系统中的线性参数差异更敏感。

当$s_A(t)$与$s_B(t)$的$h_{tx}(t)$的滚降因子k=0.5，即线性参数相同；设$s_A(t)$的非线性因子$\rho_3=0.1$，$s_A(t)$的非线性因子在0.0至0.2之间进行改变；采用提出的“相空间差射频指纹变换方法”得到的$D2$与ρ_3之间关系如图5.25所示。

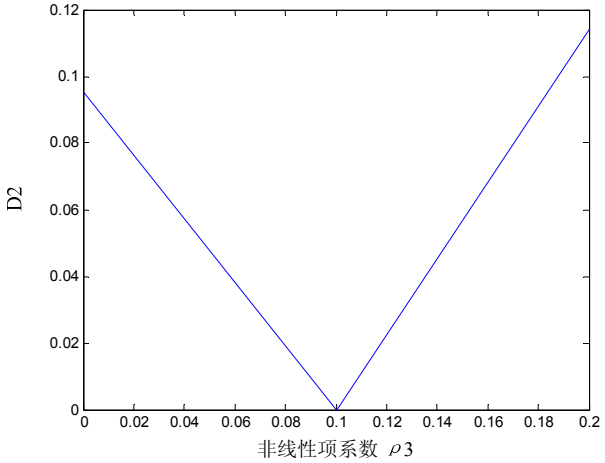

图 5.25 D2 与 ρ_3 之间关系

如图5.25所示，当系统线性参数相同时，*D2*对非线性参数敏感。

把式（5.42）中生成基带信号$m(t)$的随机数种子设为3、$h_{tx}(t)$ 的滚降因子k=0.5、非线性因子 $\rho_3=0.2$、其它参数不变，产生的$s(t)$作为参考信号$A(t)$；

把式（5.42）中生成基带信号$m(t)$的随机数种子设为3、$h_{tx}(t)$ 的滚降因子k=0.3、非线性因子 $\rho_3=0.4$、其它参数不变，产生的$s(t)$作为参考信号$B(t)$；

把式（5.42）中生成基带信号$m(t)$的随机数种子设为300、$h_{tx}(t)$ 的滚降因子k=0.8、非线性因子 $\rho_3=0.6$、其它参数不变，产生的$s(t)$作为参考信号$C(t)$；

把产生“参考信号$A(t)$”的参数中的生成基带信号$m(t)$的随机数种子设为300~399，其它参数与产生“参考信号$A(t)$”的参数相同，产生的100个$s(t)$作为未知信号$U(t)$；

采用提出的“Wi-Fi信号的相空间差射频指纹”变换方法进行实验，得到的*D2*(*X*)直方图如图5.26所示。

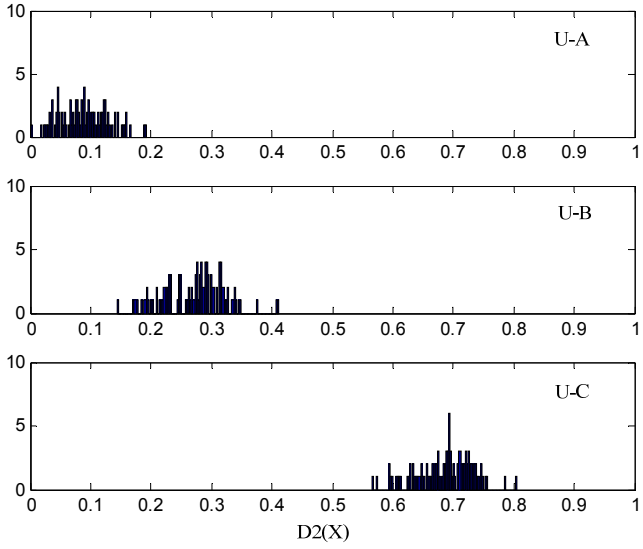

图 5.26 D2(X)直方图

图5.26中，U-A、U-B与U-C分别表示未知信号$U(t)$与参考信号$A(t)$、$B(t)$与$C(t)$的$D2(X)$的直方图，由图5.26可知，未知信号与参考信号$A(t)$来源相同，但存在一定的判为与$B(t)$来源相同的误判概率。

5.4.2.2 实验验证

采用图4.5所示的“IEEE 802.11b射频信号采集及处理系统”采集某型号同一系列3只IEEE 802.11b USB无线设备的射频信号用于实验，3只无线设备用NIC-A、NIC-B、NIC-C表示。

如图4.5所示，IEEE 802.11b USB无线设备外接在计算机上，频率设为2.412GHz，工作模式设置为Ad-hoc状态（不断发送帧宣布其存在）；射频示波器外接的接收天线为高增益天线，与待识别无线设备天线间距离仅为10厘米；射频示波器为带宽13GHz带宽、采样率40GSps的Agilent DSO91304A；示波器采样率设为500MSps，进行2.412GHz射频信号的带通采样；采集时采用铁丝网对两天线进行了最大限度的电磁屏蔽。NIC-A的1个射频信号样本如图5.27的子图（a）所示，而其功率谱如图5.27的子图（b）所示。

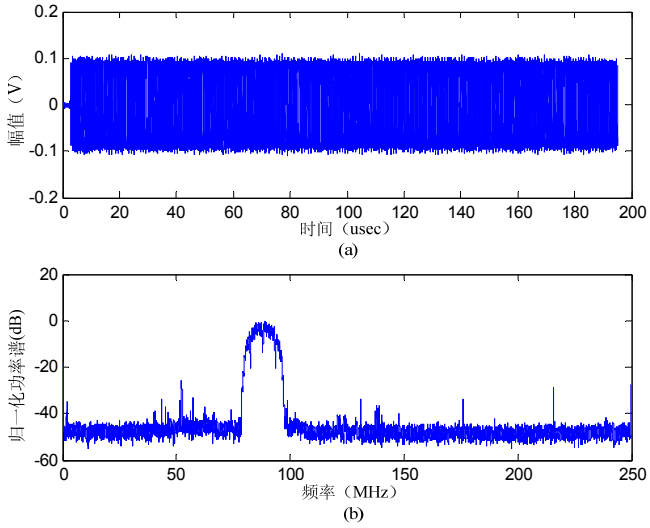

图 5.27 NIC-A 的 1 个射频信号样本及其功率谱

由图5.27可知，射频信号存在许多带外成分。

分别取NIC-A、NIC-B与NIC-C的一个样本作为参考信号，取NIC-A的100个样本作为未知测试信号，采用提出的“Wi-Fi信号的相空间差射频指纹”变换方法进行实验；相空间重构的最小维数为8、延迟样点数为3，得到的$D2(X)$直方图如图5.28所示。

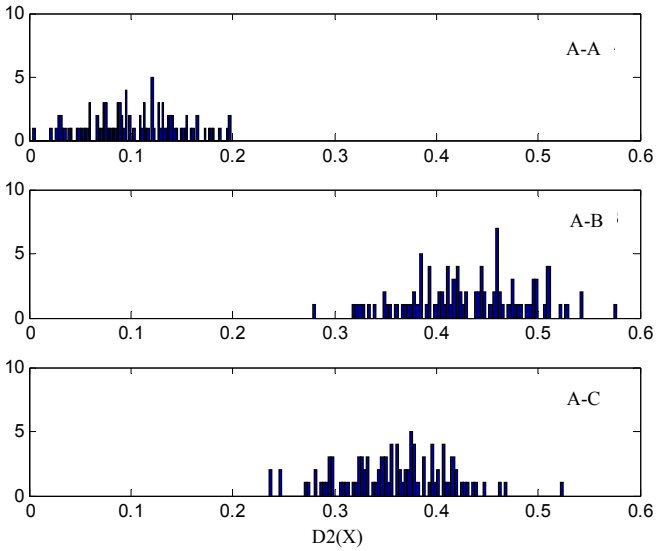

图 5.28 D2(X)直方图

图5.28中，A-A、A-B与A-C分别表示NIC-A的测试信号分别与NIC-A、NIC-B与NIC-C参考信号的*D2*(*X*)的直方图。

由图5.28可知，当测试信号与参考信号来源于同一个无线设备时，*D2*(*X*)最小，并且与测试信号与参考信号不同源时的*D2*值之间有一定的可分距离。从而验证了该方法的可行性。

5.4.3 小结

本节提出了根据“Wi-Fi信号的相空间差射频指纹”对Wi-Fi设备进行识别的方法，即把Wi-Fi设备发送的射频信号建模为非线性动力学系统的输出，根据输出序列对非线性动力学系统进行相空间重构，进而根据重构的相空间对发射机进行识别。对提出方法进行了数值仿真与实验验证。

本节提出方法利用了发射机的非线性信息，并且具有算法相对简单的优点。但本节提出方法并不是对所有Wi-Fi设备都有效，本节中用于实验验证的Wi-Fi设备是经过挑选后获得的，目的是验证提出方法的可行性。

本节提出的相空间差射频指纹可应用于相关无线设备的多射频指纹识别中。

5.5 基于 BPSK 信号的射频指纹

射频指纹具备稳健性是根据射频指纹进行后续的特征提取与分类识别的前提条件。研究表明，时变的无线多径信道以及无线接收信号参考时刻的检测精度对无线设备射频指纹稳健性的影响较大。

国防科大的许丹博士在雷达辐射源识别中提出了雷达指纹的“独立性”概念[72]，本文借用该概念，并强调具备独立性的射频指纹具有与射频信号中承载的数字信息无关的

性质。

由第二章的射频指纹识别系统可知，无线多径信道影响无线接收信号，因而也影响射频指纹的稳健性；现有有关文献大多没有考虑如何消除无线多径信道对射频指纹的影响，仅认为其是使正确识别率降低的一个不利因素。

当射频指纹不具备时间平移不变性，即射频指纹与其无线接收信号的参考时刻有关的情况下，参考时刻的检测精度将影响变换后射频指纹的稳健性。

由于BPSK调制的符号间距离大，因而常被用于无线通信物理层帧前导的调制方式。本节根据BPSK射频信号的特殊性，并假设其带内主要是线性成分时，提出了基于BPSK无线接收基带信号及带通信号的两种射频指纹变换方法。

5.5.1 BPSK 信号的基带倒谱射频指纹

5.5.1.1 系统模型

对第二章的通用无线数字发射机系统模型及射频指纹识别系统的基本模型进行简化，得到如图5.29所示的一种射频指纹识别系统简化等效图。

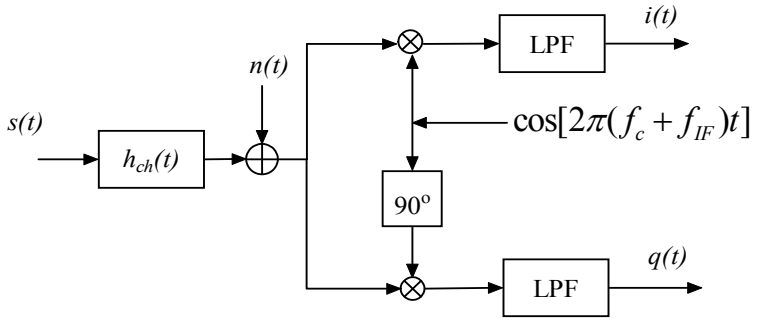

图 5.29 一种射频指纹识别系统的简化等效图

由本文第二章研究可知，假设待识别无线设备的发送信号经处理后可近似为线性，则待识别BPSK无线设备发送信号$s(t)$的基带等效为

$$s_l(t)=x(t)+jy(t) \tag{5.44}$$

而由第二章可知，射频指纹识别系统接收信号的理想基带等效形式为

$$r_l(t)=[s_l(t)*c_l(t)+n_l(t)]\bullet e^{j\cdot 2\pi\cdot\Delta f\cdot t} \tag{5.45}$$

式(5.45)中的$\Delta f<f_m$，f_m为无线设备相关标准规定的最大频偏值。当Δf很小时，把Δf近似为0（Δf很大的情况见下节）。则式(5.45)为

$$\begin{aligned} r_l(t)&=s_l(t)*c_l(t)+n_l(t)\\ &=[x(t)*c_i(t)+y(t)*c_q(t)+n_x(t)]+j[y(t)*c_i(t)-x(t)*c_q(t)+n_y(t)] \end{aligned} \tag{5.46}$$

则图5.29中的I路基带信号$i(t)$为

$$\begin{aligned} i(t) &= \mathrm{Re}\{r_l(t)\} \\ &= x(t)*c_i(t)+y(t)*c_q(t)+n_x(t) \\ &= m_i(t)*h_i(t)*c_i(t)+m_q(t)*h_q(t)*c_q(t)+n_x(t) \end{aligned} \tag{5.47}$$

而Q路基带信号$q(t)$为

$$\begin{aligned} q(t) &= \mathrm{Im}\{r_l(t)\} \\ &= y(t)*c_i(t)-x(t)*c_q(t)+n_y(t) \\ &= m_q(t)*h_q(t)*c_i(t)-m_i(t)*h_i(t)*c_q(t)+n_y(t) \end{aligned} \tag{5.48}$$

假设待识别 BPSK 发射机仅采用单路进行发送，即星座点为(1,0)与(-1,0)或(0,1)与(0,-1)，则 I 路或 Q 路接收基带信号可用

$$r(t)=m(t)*h_{tx}(t)*h_{ch}(t)+w(t) \tag{5.49}$$

表示，其中，* 表示卷积运算，$m(t)$表示$m_i(t)$或$m_q(t)$，$h_{tx}(t)$表示$h_i(t)$或$h_q(t)$，$h_{ch}(t)$表示$c_i(t)$，$w(t)$表示AWGN噪声。（有关符号详见本文第二章的2.4.1节与2.6节，在此不再重复描述）

5.5.1.2 “BPSK 基带倒谱射频指纹”的变换方法

式(5.49)中，$w(t)$主要为接收机的AWGN噪声。假设对接收基带信号进行了去噪处理后式(5.49)可近似为

$$r(t)=m(t)*h_{tx}(t)*h_{ch}(t) \tag{5.50}$$

式(5.50)中，基带发送BPSK信号可表示为

$$m(t)=\sum_k b(k)\delta(t-kT) \tag{5.51}$$

其中，$b(k)$是速率为$1/T$ bits/s 的二进制序列$\{\pm 1\}$，$\delta(t)$为单位脉冲信号。

式(5.50)中，无线多径信道的脉冲响应

$$\begin{aligned} h_{ch}(t) &= c_i(t) \\ &= \sum_k \alpha_k \cos[2\pi(f_c+f_{IF})\tau_k]\delta(t-\tau_k) \end{aligned} \tag{5.52}$$

其中，τ_k为第k径延时，α_k为第k径衰减系数。

式(5.50)的数字表示形式为

$$r(n)=m(n)*h_{tx}(n)*h_{ch}(n) \tag{5.53}$$

其中$r(n)$、$m(n)$、$h_{tx}(n)$及$h_{ch}(n)$分别是$r(t)$,$m(t)$,$h_{tx}(t)$及$h_{ch}(t)$的采样序列。

设数字信号$x(n)$的实倒谱定义为

$$\hat{x}(n)=F^{-1}\{\ln[|X(e^{jw})|]\} \tag{5.54}$$

其中，F^{-1}表示逆傅立叶变换，ln表示对数运算，$|X(e^{jw})|$是$x(n)$的离散傅立叶变换的幅度谱；式(5.53)的实倒谱表达式为

$$\hat{r}(n)=\hat{m}(n)+\hat{h}_{tx}(n)+\hat{h}_{ch}(n) \tag{5.55}$$

从式(5.55)可知，式(5.53)所示的“卷积”关系变成了式(5.55)所示的“加”关系。根据通信系统的一般硬件结构可知，式(5.55)中$\hat{h}_{tx}(n)$能量集中在“低时”部分并且缓慢变化。进一步分析式(5.55)中其它两项的性质。

从式(5.51)可知，数字化基带发送BPSK信号$m(n)$是等间隔脉冲序列，所以其实倒谱$\hat{m}(n)$也是等间隔脉冲序列[119]；从式(5.52)可知，数字化无线多径信道的脉冲响应序列$h_{ch}(n)$是脉冲串序列，因而其实倒谱序列$\hat{h}_{ch}(n)$是仅在原始多径延时的复杂函数处有值的脉冲序列[120]。所以，接收BPSK序列的实倒谱是缓慢变化的“低时”部分$\hat{h}_{tx}(t)$与快速变化的脉冲序列$\hat{m}(n)$与$\hat{h}_{ch}(n)$之和。根据这个性质，可以把式（5.55）中的$\hat{h}_{tx}(n)$分离出来，作为发射机射频指纹。

由于指数加权后的序列具有以下性质[119]：（1）保持序列的卷积关系；（2）使序列最小相位化；（3）加权后序列的实倒谱具有因果性。因此，提出BPSK倒谱射频指纹的变换方法为

步骤1：对接收的BPSK信号进行解调与归一化，得到其基带信号；

步骤2：对接收基带信号进行起始时刻检测，并截取一定长度的信号；

步骤3：对截取后信号进行去噪声处理，以提高其SNR；

步骤4：对提高SNR后的截取后信号进行衰减指数加权；

步骤5：对加权后信号进行如式（5.54）所示的实倒谱处理；

步骤6：对实倒谱进行低通滤波与加“低时”窗处理，结果即“BPSK基带倒谱射频指纹”，用$LPF\{\hat{r}(n)\}$表示。

其中步骤6的“低通滤波”滤除接收BPSK序列实倒谱中的快速变化的脉冲序列成分$\hat{m}(n)$与$\hat{h}_{ch}(n)$，保留缓慢变化的“低时”部分$\hat{h}_{tx}(t)$，因而$LPF\{\hat{r}(n)\}$主要由待识别无线发射机的硬件性质决定，所以具备独立性与时间平移不变性。由于其削弱了无线信道影响，因而是一种具备稳健性的射频指纹。

当待识别无线设备发射机采用I-Q调制结构时，设I路发送BPSK信号得到的“BPSK基带倒谱射频指纹”为$LPF\{\hat{r}_i(n)\}$，Q路发送BPSK信号得到的“BPSK基带倒谱射频指纹”为$LPF\{\hat{r}_q(n)\}$，则

$$\hat{f}(n)=LPF\{\hat{r}_i(n)\}-LPF\{\hat{r}_q(n)\} \tag{5.56}$$

体现了I路与Q路的硬件差异，可作为另一种射频指纹用于BPSK发射机的识别。

5.5.1.3 实验验证

采用如图5.30所示的“射频信号采集与射频指纹变换系统”进行“BPSK基带倒谱射

频指纹”的实验验证。图5.30中的“待识别发射机”为BPSK无线发射机，参数与IEEE 802.11b前导的物理层参数类似：（1）基带采用单路发送符号、符号序列可随机生成、符号速率为1MSymbol/s、采用11chips的Barker码（10110111000）进行直序扩频；（2）射频频率为2.412GHz；（3）帧长为800usec。图5.30中的LNA为定制的固定增益低噪声放大器。

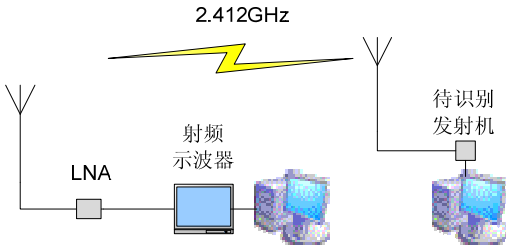

图 5. 30 射频信号采集与射频指纹变换系统

图5.30中的无线信道直达径上放置了多个纸盒组成的障碍物，采集每一帧时，人工改变纸盒状态，从而改变两天线间直达径无线信道状态。接收天线采用高增益定向天线，与待识别发射机天线间距离约为3米。接收天线连接LNA。LNA连接射频示波器，射频示波器为13GHz带宽、采样率40GSps的Agilent DSO91304A；示波器采样率设为500MSps，进行2.412GHz射频信号的带通采样。

采集的一个帧射频信号如图5.31所示，其中子图（a）为帧头部，而子图（b）是子图（a）的局部放大图。

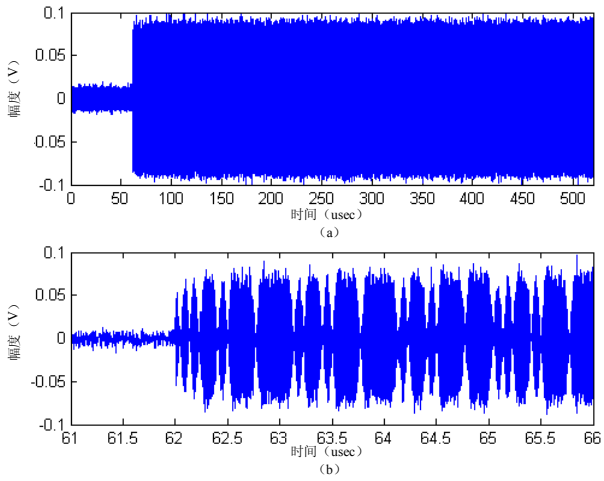

图 5. 31 一个 BPSK 帧射频信号及其头部放大图

图5.31所示帧射频信号的功率谱如图5.32所示。

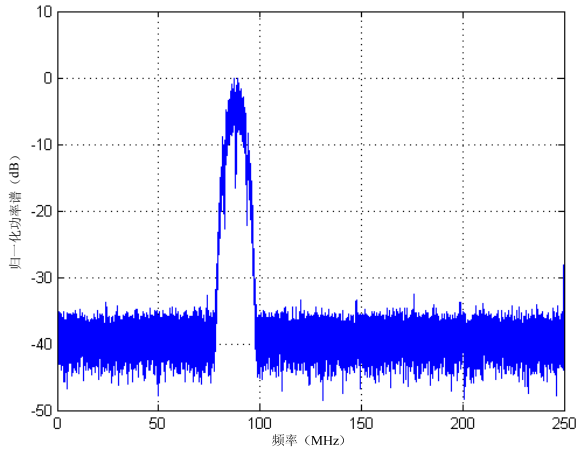

图 5.32 图 5.31 所示帧射频信号的功率谱

由图5.32可知，2.412GHz的BPSK射频信号经500MSps带通采样后带内中心频率为88MHz左右。

首先对采样序列进行幅值归一化；接着采用中心频率为88MHz、带宽为22MHz、阶数为48的FIR带通数字滤波器，对归一化后序列进行带通滤波，以滤除带外非线性成分；然后进行基于Costas PLL（Simulink）的正交解调，得到基带信号的采样序列$r_i(n)$与其正交分量$r_q(n)$（PLL锁定后，$r_q(n)$近似为0）。

根据$r_i(n)$与$r_q(n)$计算其包络$a(n)$，并对$a(n)$进行归一化；然后对归一化后$a(n)$按能量门限为0.5进行起始时刻P_{ref}检测，并人工加上1-500样点内均匀分布的检测误差，以验证射频指纹的时间平移不变性；从P'_{ref}向前截取189usec长、向后取3usec长的序列$r_i(n)$用于后续的“BPSK基带倒谱射频指纹”变换；采用以上方法得到的一个待识别无线发射机的50个$a(n)$样本头部如图5.33所示。

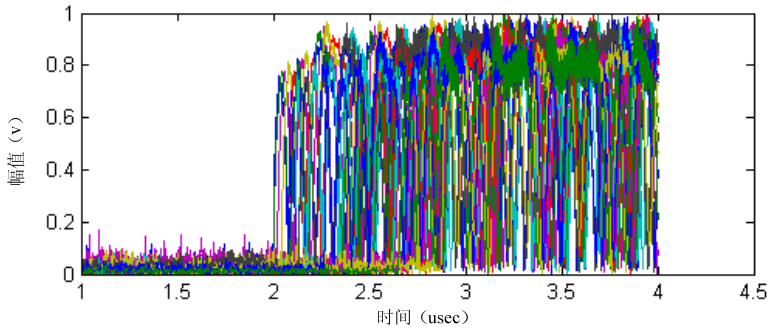

图 5.33 五十个 a(n)样本头部

基于Stanford大学的WaveLab小波包，采用小波收缩去噪法对截取后$r_i(n)$进行去噪处理，使用具有8阶消失矩的近似对称小波（Nearly Symmetric wavelet），采用软阈值法对小波系数进行处理，再对处理后系数做逆变换；接着对去噪后$r_i(n)$ 进行底数为0.99999的衰减指数加窗；然后再对加窗后$r_i(n)$进行式（5.54）所示的实倒谱处理；接着对得到的实倒谱序列进行截止频率为11MHz、阶数为48的FIR低通滤波；最后对低通滤波后的实倒谱加长度为0.7usec的“低时”窗，结果即“BPSK基带倒谱射频指纹”。

从待识别BPSK无线发射机中挑选3只（记为：发射机1、发射机2与发射机3）进行实验，每只发射机采集50个射频信号样本。由提出方法变换得到的“BPSK基带倒谱射频指纹”样本如图5.34所示，图中分开的3条线分别是每个发射机的50个“BPSK基带倒谱射频指纹”样本。

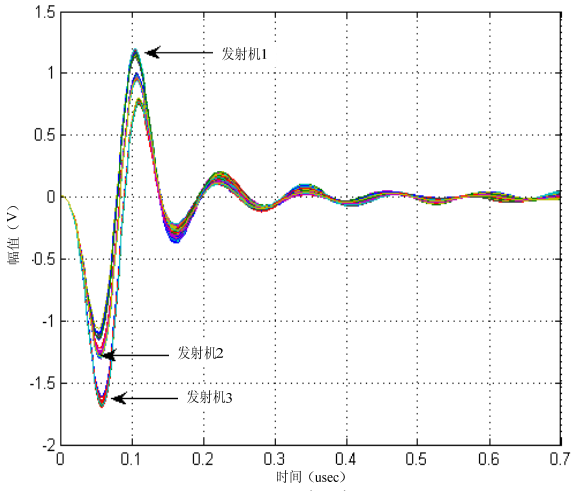

图 5.34 三只 BPSK 发射机的“基带倒谱射频指纹”样本

由图5.34可知，3只BPSK发射机的“基带倒谱射频指纹”样本存在明显的类间距离，并且其形状与低通滤波器的脉冲响应类似，这是由于其实倒谱的“类冲激信号”性质决定的。“发射机1”的50个实倒谱样本的“低时”区如图5.35所示。

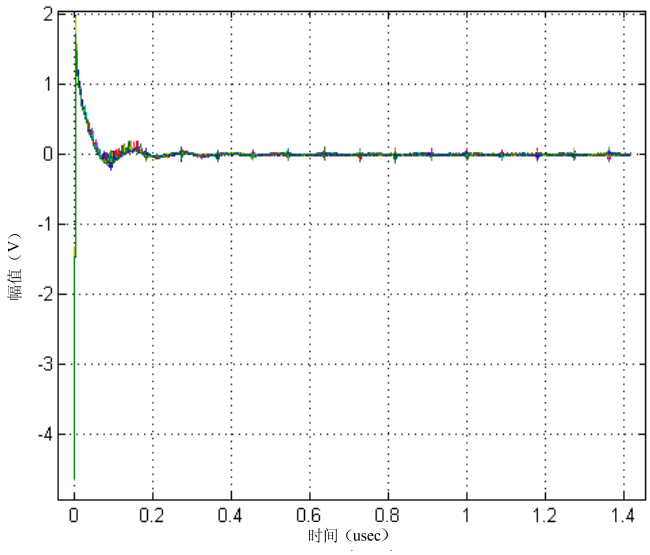

图 5.35 “发射机 1”的 50 个实倒谱样本的“低时”区

下面来分析“BPSK基带倒谱射频指纹”稳健性优的主要原因。首先，根据理论分析可知，“BPSK基带倒谱射频指纹”主要由待识别无线发射机的系统脉冲响应决定，而无线发射机的系统脉冲响应由其结构与构成元件的硬件性质确定，因而具备独立性；其次，根据理论分析可知，“BPSK基带倒谱射频指纹”减弱了无线多径信道影响，而“前导包络射频指纹”包含了无线多径信道影响，这从其变换

$$a(n)=\sqrt{r_i(n)^2+r_q(n)^2} \tag{5.57}$$

可知。最后，由理论分析可知，“BPSK基带倒谱射频指纹”对起始点检测精度不敏感，具有时间平移不变性，但从式(5.57)可知，“前导包络射频指纹”对起始点检测精度敏感。所以，“BPSK基带倒谱射频指纹”的稳健性优。

5.5.2 BPSK 信号的频偏对数谱射频指纹

5.5.2.1 系统模型

对第二章的通用无线数字发射机系统模型及射频指纹识别系统的基本模型进行简化，得到如图5.36所示的一种基于正交下变频的射频指纹识别系统的简化等效模型。

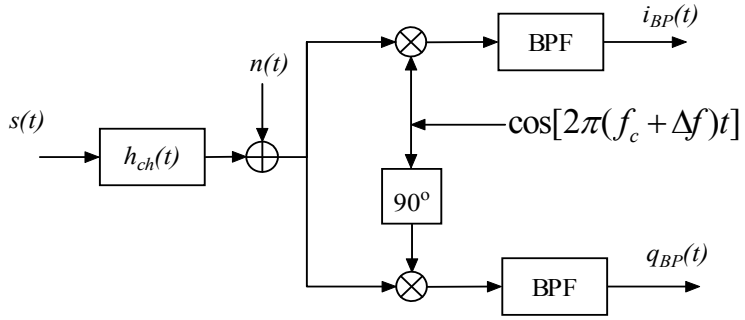

图 5.36 基于正交下变频的射频指纹识别系统简化等效模型

由本文第二章研究可知，假设待识别无线设备的发送信号经处理后可近似为线性，则图5.36 中待识别无线设备发送的单载波窄带信号 $s(t)$可表示为

$$s(t)=\mathrm{Re}\{s_l(t)e^{j\cdot 2\pi\cdot f_c\cdot t}\} \tag{5.58}$$

其中，$s_l(t)=x(t)+jy(t)$ 为 $s(t)$的基带等效复信号，f_c 为载波频率，$x(t)$与 $y(t)$分别为 I 路与 Q 路的基带等效发送信号，表示为

$$x(t)=m_x(t)*h_x(t) \tag{5.59}$$

与

$$y(t)=m_y(t)*h_y(t) \tag{5.60}$$

其中，$m_x(t)$、$m_y(t)$为基带发送数字序列信号；$h_x(t)$与 $h_y(t)$分别为 I 路与 Q 路电路的等效单位冲激响应，分别由待识别无线设备发射机的 I 路与 Q 路的硬件性质决定。

图 5.36 中，无线多径信道的单位冲激响应

$$h_{ch}(t)=2\,\mathrm{Re}\{c_l(t)e^{j2\pi f_c t}\} \tag{5.61}$$

其中

$$c_l(t)=\sum_n \alpha_n \cos(2\pi f_c \tau_n)\delta(t-\tau_n)-j\bullet\sum_n \alpha_n \sin(2\pi f_c \tau_n)\delta(t-\tau_n) \tag{5.62}$$

其中，$c_l(t)$为$h_{ch}(t)$的基带复等效；式（5.62）中，α_n与τ_n分别为第 n 径无线信道的衰减系数与延时。

图 5.36 中，接收端 AWGN 噪声

$$n(t)=\mathrm{Re}\{n_l(t)e^{j2\pi f_c t}\} \tag{5.63}$$

其中

$$n_l(t)=n_x(t)+jn_y(t) \tag{5.64}$$

式（5.64）中，$n_l(t)$为$n(t)$的基带等效复信号，$n_x(t)$与$n_y(t)$分别为 I 路与 Q 路的基带等效。

图 5.36 中的Δf为正交下变频载波频率与发送信号载波频率之间的频差，$\Delta f > f_m$，f_m为无线设备相关标准规定的最大频偏值。$i_{BP}(t)$与 $q_{BP}(t)$ 分别为 I 路与 Q 路的接收带通信号。

假设图 5.36 中的 BPF 为理想的带通滤波器，采用基带等效进行推导，则接收信号的基带等效复信号为

$$r_l(t)=[s_l(t)*c_l(t)+n_l(t)] \tag{5.65}$$

而 I 路接收带通信号

$$\begin{aligned} &i_{BP}(t)=\mathrm{Re}\{r_l(t)\bullet e^{j\bullet 2\pi\bullet\Delta f\bullet t}\}\\ &=[x(t)*c_i(t)+y(t)*c_q(t)+n_x(t)]\bullet\cos(2\pi\bullet\Delta f\bullet t)-\\ &[y(t)*c_i(t)-x(t)*c_q(t)+n_y(t)]\bullet\sin(2\pi\bullet\Delta f\bullet t) \end{aligned} \tag{5.66}$$

Q 路接收带通信号

$$\begin{aligned} &q_{BP}(t)=\mathrm{Im}\{r_l(t)\bullet e^{j\bullet 2\pi\bullet\Delta f\bullet t}\}\\ &=[y(t)*c_i(t)-x(t)*c_q(t)+n_y(t)]\bullet\cos(2\pi\bullet\Delta f\bullet t)+\\ &[x(t)*c_i(t)+y(t)*c_q(t)+n_x(t)]\bullet\sin(2\pi\bullet\Delta f\bullet t) \end{aligned} \tag{5.67}$$

5.5.2.2 “BPSK 频偏对数谱射频指纹”的变换方法

假设对接收带通信号进行去噪处理后，式（5.66）与（5.67）中的噪声项$n_x(t)$与$n_y(t)$可忽略，则式（5.66）可近似为

$$\begin{aligned} &i_{IF}^{'}(t)=[x(t)*c_i(t)+y(t)*c_q(t)]\bullet\cos(2\pi\bullet\Delta f\bullet t)-\\ &[y(t)*c_i(t)-x(t)*c_q(t)]\bullet\sin(2\pi\bullet\Delta f\bullet t)\} \end{aligned} \tag{5.68}$$

式（5.67）可近似为

$$\begin{aligned} q'_{IF}(t) &= [y(t)*c_i(t) - x(t)*c_q(t)]\bullet\cos(2\pi\bullet\Delta f\bullet t) + \\ &[x(t)*c_i(t) + y(t)*c_q(t)]\bullet\sin(2\pi\bullet\Delta f\bullet t) \end{aligned} \tag{5.69}$$

假设单路 BPSK 信号的 $y(t)=0$，$i'_{IF}(t)$ 与 $q'_{IF}(t)$ 的傅立叶变换分别为 $I_{IF}(f)$ 与 $Q_{IF}(f)$，则

$$\begin{aligned} &I_{IF}(f) - j\bullet Q_{IF}(f) = X(f+\Delta f)\bullet C_i(f+\Delta f) \\ &= M_x(f)\bullet H_x(f+\Delta f)\bullet C_i(f+\Delta f) \end{aligned} \tag{5.70}$$

其中，$M_x(f)$是基带发送数字序列信号 $m_x(t)$的傅立叶变换，$H_x(f)$是发射机 I 路硬件的等效脉冲响应 $h_x(t)$的傅立叶变换，$C_i(f)$是无线多径信道 I 路低通等效的傅立叶变换。对式(5.70)进行取模与 log 运算，为

$$\begin{aligned} &\log[|I_{IF}(f) - j\bullet Q_{IF}(f)|] = \log[|M_x(f)|] + \\ &\log[|H_x(f+\Delta f)|] + \log[|C_i(f+\Delta f)|] \end{aligned} \tag{5.71}$$

式(5.71)中的 $\log[|M_x(f)|]$ 与 $\log[|C_i(f+\Delta f)|]$ 是由脉冲串序列构成的快速变化分量，根据通信发射机的一般结构可知，式(5.71)中的 $\log[|H_x(f+\Delta f)|]$ 是能量集中在带通区的缓慢变化分量。对式（5.71）进行低通滤波，假设式（5.71）中的带通频率 Δf 在低通滤波器的通带内，则

$$\begin{aligned} &LPF\{\log[|I_{IF}(f) - j\bullet Q_{IF}(f)|]\} = LPF\{\log[|H_x(f+\Delta f)|]\} \\ &+LPF\{\log[|M_x(f)|] + \log[|C_i(f+\Delta f)|]\} \\ &\approx LPF\{\log[|H_x(f+\Delta f)|]\} \end{aligned} \tag{5.72}$$

即 $LPF\{\log[|I_{IF}(f) - j\bullet Q_{IF}(f)|]\}$ 主要由待识别发射机的等效脉冲响应与带通频率 Δf 决定。

带通频率 Δf 是射频指纹识别系统的“正交下变频频率”与待识别发射机的实际振荡器频率之差，射频指纹识别系统的“正交下变频频率”一般依据无线设备的相关标准人为设定，因此带通频率 Δf 体现了待识别无线设备发射机的振荡器硬件性质。所以，式（5.72）可称为“BPSK 频偏对数谱射频指纹”。

5.5.2.3 实验验证

采用如图 5.30 所示的“射频信号采集与射频指纹变换系统”对“BPSK 频偏对数谱射频指纹”进行验证，包括待识别 BPSK 发射机、射频示波器、固定增益低噪声放大器(LNA)、计算机及天线等。如图 30 所示，待识别 BPSK 发射机外接在计算机上；射频示波器为 13GHz 带宽、40GSps 采样率的 Agilent DSO91304A，外接高增益天线及 LNA 的 DSO91304A 用于射频信号采集，DSO91304A 的采样率设为 500MSps，进行射频信号的带通采样。实验时室内温度及湿度保持恒定。

人为改变无线信道直达径上的障碍物的同时进行 BPSK 射频信号样本的采集，然后进行基于 Matlab 的处理：采集信号幅值的归一化，载波频率为 77MHz 的正交下变频（2.412GHz 的射频信号经 500MSps 带通采样后能量集中在 88MHz 处），中心频率为 11MHz、带宽为 22MHz 的带通滤波，得到 I 路与 Q 路带通信号 $i_{BP}(t)$与 $q_{BP}(t)$，并构成带通复信号；对带通复信号进行基于双树复小波变换的去噪处理[60]，去噪后的 I 路与 Q 路带通信号仍用 $i_{BP}(t)$与 $q_{BP}(t)$表示。

根据去噪后的 I 路与 Q 路带通信号计算其包络

$$e(t)=\sqrt{i_{BP}^2(t)+q_{BP}^2(t)} \tag{5.73}$$

根据 $e(t)$进行基于能量门限的带通信号起始点检测，并且人为增大起始点检测误差（为了检验射频指纹的时间平移不变性），得到的同一个待识别发射机的 100 个带通信号样本的前导包络头部如图 5.37 所示。由图 5.37 可知，起始点存在较大的人为误差。

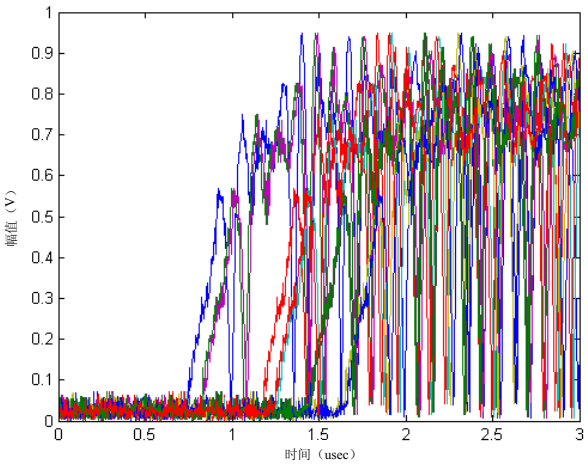

图 5.37 同一个待识别无线发射机的
100 个带通信号样本的前导包络头部

从图 5.37 所示同一个待识别无线发射机的 100 个样本信号的 0 时刻开始，分别截取 192usec 长对应的 BPSK 带通信号 $i_{BP}(t)$与 $q_{BP}(t)$，构成复信号 $i_{BP}(t)-j\bullet q_{BP}(t)$，进行本文提出的“频偏对数谱射频指纹”变换，得到的 100 个“频偏对数谱射频指纹” $LPF\{\log[I_{BP}(f)-j\bullet Q_{BP}(f)]\}$ 样本如图 5.38 所示，其中 LPF 采用了带宽为 22MHz 的 96 阶 FIR 低通滤波器。由图 5.38 可知，尽管用于变换的信号样本存在较大的起始点检测误差，同一个待识别发射机的 100 个“BPSK 频偏对数谱射频指纹”样本表现出很小的类内距，因而具备时间平移不变性与稳健性。

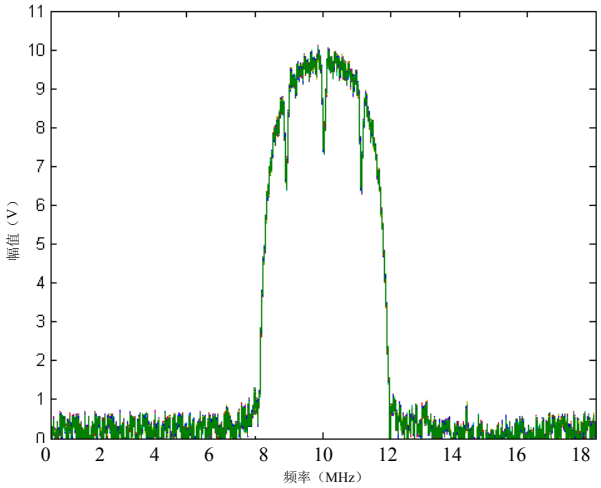

图 5.38 同一个 NIC 的 100 个频偏对数谱射频指纹样本

挑选三只待识别 BPSK 发射机（记为：发射机 1、发射机 2 与发射机 3）进行实验，每个发射机采集 100 个射频信号样本进行“BPSK 频偏对数谱射频指纹”变换；并且对“BPSK 频偏对数谱射频指纹”进行基于矩形与三角形的相似因子特征提取[109]，得到的 300 个“BPSK 频偏对数谱射频指纹”样本的相似因子特征散布图如图 5.39 所示。

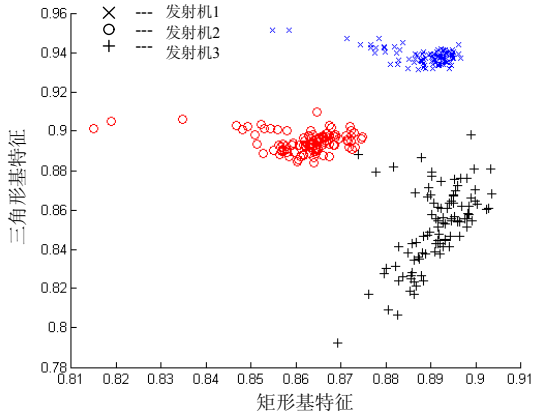

图 5.39 三只待识别发射机的“BPSK 频偏对数谱
射频指纹”的相似因子特征散布图

由图 5.39 可知，该三只待识别发射机的“BPSK 频偏对数谱射频指纹”的相似因子特征具备以下性质：不同待识别发射机的相似因子特征集的中心间具有一定的距离，因而根据相似因子特征可以把该三只待识别发射机以一定的识别率进行分类。

5.5.3 小结

本节提出了用于 BPSK 无线发射机识别的“BPSK 基带倒谱射频指纹”与“BPSK 频偏对数谱射频指纹”变换方法，提出的这两种射频指纹主要由待识别发射机的硬件性质决定，因而具备独立性、时间平移不变性与稳健性。然而，尽管本节提出的射频指纹具有一些优良性质，但其应用仍存在如下要求：（1）经处理后的 BPSK 信号的性质主要

为线性；（2）用于变换的 BPSK 信号必须经过去噪处理。

当待识别无线设备发射机采用 I-Q 正交调制结构时，如果能分别得到 I 路与 Q 路“BPSK 基带倒谱射频指纹”与“BPSK 频偏对数谱射频指纹”，则 I 路与 Q 路的这两种射频指纹之差分别体现各自的 I 路与 Q 路的硬件差异，可作为其他种类的射频指纹用于 BPSK 无线发射机识别。

另外，本节提出的这两种 BPSK 射频指纹并不能把所有 BPSK 无线发射机都区分开，本节实验中采用的无线网卡是经过挑选后获得的。

如果把“单路发送 BPSK 信号”规定到无线设备的相关标准中，则提出的这两种“BPSK 射频指纹”可以应用到相关无线设备的多射频指纹识别中。

5.6 基于 ARMA 模型系数的射频指纹

无线设备的识别研究中，当待识别发射机发送的射频信号带内非线性较弱时，可把发射机基带到接收机基带部分近似等效为一个线性时不变系统(Linear Time Invariant简称LTI)[100]，则接收基带信号的离散序列可建模为ARMA（Automatic Regressive Moving Average ，自回归移动平均）过程，对应的LTI系统可称为ARMA系统。其中由相同标称值元件构成的同一型号同一系列无线发射机的分类条件最紧，相应ARMA系统的系统函数结构相同、零点与极点有细微差别，这种系统的分类较为困难。

本节研究ARMA系统模型的系统函数间的多项式系数差别与零点或极点差别之间的关系，提出了把系统函数多项式的第二个系数作为射频指纹的新方法。该方法对于增大微小差别ARMA系统间的类间距离具有一定意义。本节首先介绍了等效ARMA系统模型及提出方法的理论推导，然后给出了基于两个相同标称值元件构成的无线发射机的该方法的仿真实例。

5.6.1 系统模型

根据第二章所述的无线发射机系统模型及射频指纹识别系统的基本模型，对其进行简化，得到如图5.40所示的一种射频指纹识别系统简化模型。

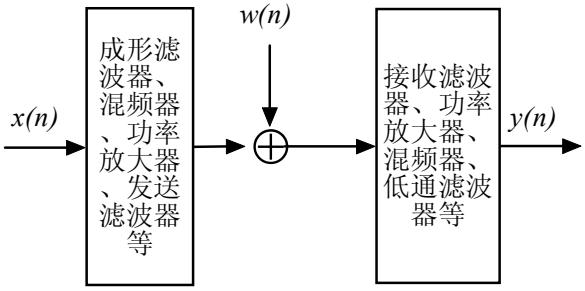

图 5.40 一种简化的射频指纹识别系统模型

其中 $x(n)$ 为等效基带发送序列信号， $w(n)$ 为AWGN噪声， $y(n)$ 为接收基带序列信号。

由第二章的分析可知，当对接收无线信号进行处理后，可把从 $x(n)$ 到 $y(n)$ 之间部分建模为一个线性时不变的 ARMA 系统。设 ARMA（p,q）系统的传递函数为 $H(z)=\dfrac{B(z)}{A(z)}$，其中 $A(z)=\prod_{i=1}^{p}(1-\alpha_i z^{-i})$，$p\geq 1$；$B(z)=\prod_{j=1}^{q}(1-\beta_j z^{-j})$，$q\geq 1$；$\alpha_i$ 为系统极点，β_j 为系统零点。

由于构成无线发射机的电路相同、元件标称值相同，所以对应的ARMA系统的系统函数 $H(z)$ 的结构相同。根据系统理论，系统函数的零点或极点值由构成系统的元件值决定，由于仅存在元件容差，所以各发射机对应的ARMA系统的系统函数的零点 β_j 或极点 α_i 存在细微差别。

5.6.2 “ARMA 模型系数射频指纹”的变换方法

引理1：多项式等式 $\sum_{i=0}^{p}a_i z^{-i}=\prod_{i=1}^{p}(1-\alpha_i z^{-1})$，$a_0=1, p\geq 1$，则：$a_1=-\sum_{i=1}^{p}\alpha_i$，即左边的累加形式的多项式的第二个系数是右边的连乘形式各项的 z^{-1} 系数（不含 α_0）之和。

证明：数学归纳法。

(1) 当 $p=1$ 时，等式为 $\sum_{i=0}^{1}a_i z^{-i}=\prod_{i=1}^{1}(1-\alpha_i z^{-1})$，即 $1+a_1 z^{-1}=1-\alpha_1 z^{-1}$，$a_1=-\alpha_1=-\sum_{i=1}^{1}\alpha_i$；

(2) 假设当 $p=m\geq 1$ 时等式成立，即

$\sum_{i=0}^{m}a_i z^{-i}=\prod_{i=1}^{m}(1-\alpha_i z^{-1})=1-\sum_{i=1}^{m}\alpha_i z^{-1}+f(\bullet)z^{-2}+\ldots$，则 $a_1=-\sum_{i=1}^{m}\alpha_i$；

(3) 当 $p=m+1$ 时，原多项式等式为

$\sum_{i=0}^{m}a_i z^{-i}+a_{m+1}z^{-(m+1)}=(1-\alpha_{m+1}z^{-1})*\prod_{i=1}^{m}(1-\alpha_i z^{-1})$，由该式可知：等式左边增加的项不改变 z^{-1} 的系数 a_1，而等式右边为 $(1-\alpha_{m+1}z^{-1})*\prod_{i=1}^{m}(1-\alpha_i z^{-1})=1-\sum_{i=1}^{m+1}\alpha_i z^{-1}+g(\bullet)z^{-2}+\ldots$，则 $a_1=-\sum_{i=1}^{m+1}\alpha_i=-\sum_{i=1}^{p}\alpha_i$；

综上所述，得证。

定理 1：设 ARMA 系统的传递函数为 $H_k(z)=\dfrac{B_k(z)}{A_k(z)}$，$k=1,2,\ldots$ 其中 $A_k(z)=\sum_{i=0}^{p}a_{ki}z^{-i}=\prod_{i=1}^{p}(1-\alpha_{ki}z^{-i})$，$a_{k0}=1, p\geq 1$；$B_k(z)=\sum_{j=0}^{q}b_{kj}z^{-j}=\prod_{j=1}^{q}(1-\beta_{kj}z^{-j})$，

$b_{k0}=1, q\geq 1$；则任意两系统 $H_m(z)$ 与 $H_n(z)$（$m\neq n$）的极点之间距离为 $\Delta\alpha_i=\alpha_{mi}-\alpha_{ni}$，$i=1,...,p$，零点之间距离为 $\Delta\beta_j=\beta_{mj}-\beta_{nj}$，$j=1,...,q$。以 $(a_{k1},b_{k1}),k=m,n$ 构成射频指纹，则

$$\begin{aligned} &dist((a_{m1},b_{m1}),(a_{n1},b_{n1})) \\ &=\sqrt{(a_{m1}-a_{n1})^2+(b_{m1}-b_{n1})^2} \\ &=\sqrt{(\sum_{i=1}^{p}\Delta\alpha_i)^2+(\sum_{j=1}^{q}\Delta\beta_j)^2} \end{aligned} \tag{5.74}$$

即以 $(a_{k1},b_{k1}),k=m,n$ 构成射频指纹的两个ARMA系统间的类间距离是两系统的零点之间距离和平方与极点之间距离和平方和的平方根。

证明：由引理1，$a_{m1}=-\sum_{i=1}^{p}\alpha_{mi}$，$a_{n1}=-\sum_{i=1}^{p}\alpha_{ni}$，$b_{m1}=-\sum_{i=1}^{q}\beta_{mi}$，$b_{n1}=-\sum_{i=1}^{q}\beta_{ni}$；则

$$\begin{aligned} &dist((a_{m1},b_{m1}),(a_{n1},b_{n1}))=\sqrt{(a_{m1}-a_{n1})^2+(b_{m1}-b_{n1})^2} \\ &=\sqrt{(\sum_{i=1}^{p}\alpha_{ni}-\sum_{i=1}^{p}\alpha_{mi}{}_{n1})^2+(\sum_{i=1}^{q}\beta_{ni}-\sum_{i=1}^{q}\beta_{mi})^2} \\ &=\sqrt{(\sum_{i=1}^{p}\Delta\alpha_i)^2+(\sum_{j=1}^{q}\Delta\beta_j)^2} \end{aligned} \tag{5.75}$$

证毕。

ARMA系统模型的系数仅由硬件性质决定，具有可比性，因而可构成射频指纹。虽然由相同元件标称值构成的无线发射机对应的ARMA系统模型的零点之间的距离 $\Delta\beta_j$、极点之间的距离 $\Delta\alpha_j$ 很微小，但采用ARMA系统模型分子多项式的第二个系数 a_{k1} 与分母多项式的第二个系数 b_{k1} 构成的射频指纹之间的距离是各阶零点之间距离和与各阶极点之间距离和构成的两直角边的直角三角形的斜边边长。因而，提出的射频指纹具有明确的物理意义，对于增大微小差别ARMA系统间的距离具有一定作用。

5.6.3 仿真实验

构建了如第二章2.3.1节所述的基于ADS软件仿真环境的射频指纹识别系统模型，模型包括两个待识别无线发射机、相同的无线信道、相同的接收机。两个待识别无线发射机的电路相同、元件（电阻、电感、电容等）的标称值相同，存在±20%的元件容差；元件值设为随机变量，概率密度函数设为均匀分布。两无线发射机的发送基带数字信号及接收基带信号头部如图5.41所示，其中子图（a）为I路信号，子图（b）为Q路信号。从图5.41可见，尽管两发射机的发送基带数字信号相同，两发射机的相应接收基带信号存在细微差异。图中的接收信号与发送信号经过了人工同步。

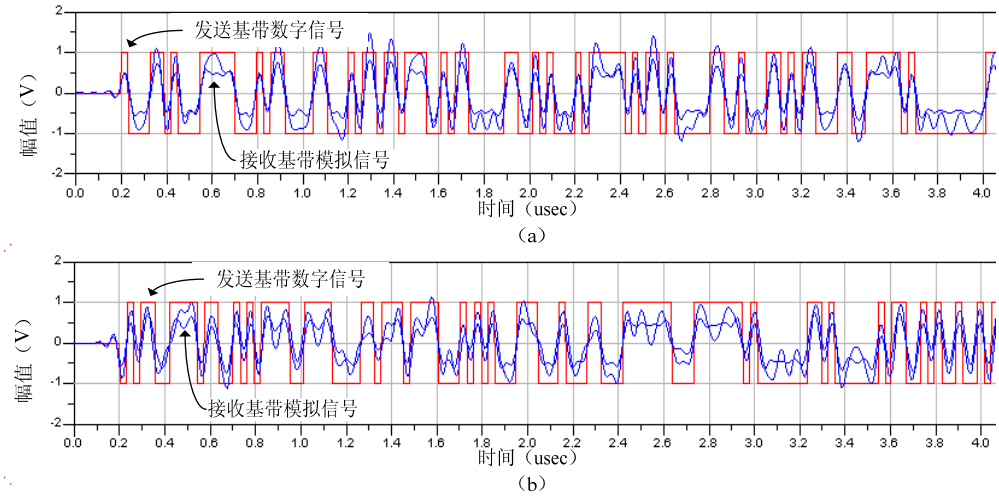

图 5.41 两无线发射机的发送与接收基带信号

对接收基带信号进行Baud率采样，并人为加入AWGN噪声，使接收基带信号的SNR为20dB；采用Ananthram Swami等编写的高阶谱分析工具箱进行基于高阶统计量的系统函数参数的盲辨识[121, 122]。当把系统建模为仅有零点的MA系统时，盲辨识得到的两待识别发射机的阶数都为11，两发射机的零点分布如图5.42所示。

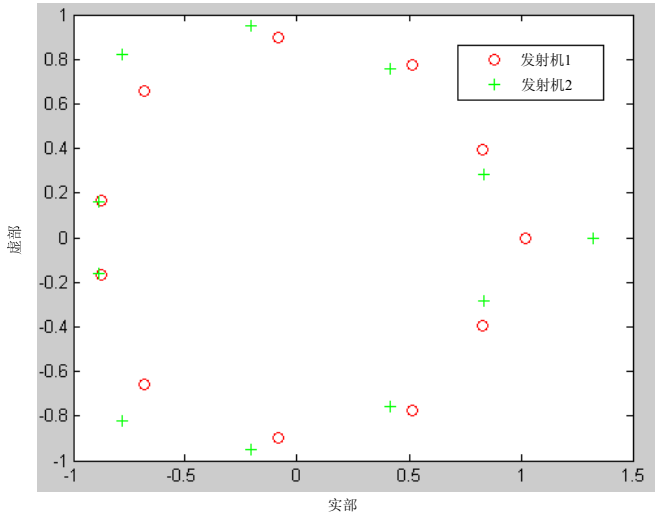

图 5.42 两发射机对应的 MA 系统的零点分布图

由图5.42可见，两MA系统的零点之间存在细微差别，其数值如表5.3所示。

表 5.3 两发射机的零点

序号 序号	零点		零点之差 （发射机 1 - 发射机 2）
	发射机 1	发射机 2	
1	-0.87893 + 0.16918i	-0.77749 + 0.82046i	-0.10144 - 0.65128i
2	-0.87893 - 0.16918i	-0.77749 - 0.82046i	-0.10144 +0.65128i
3	-0.68147 + 0.6606i	-0.89052 + 0.15893i	0.20905 + 0.50167i
4	-0.68147 - 0.6606i	-0.89052 - 0.15893i	0.20905 - 0.50167i
5	-0.082343 + 0.89929i	-0.20828 + 0.95005i	0.12594 - 0.050761i
6	-0.082343 - 0.89929i	-0.20828 – 0.95005i	0.12594 + 0.050761i
7	0.51027 + 0.77357i	1.3234	-0.81309 + 0.77357i
8	0.51027 - 0.77357i	0.41327 + 0.75786i	0.097008 - 1.5314i

9	1.0194	0.41327 - 0.75786i	0.60617 + 0.75786i
10	0.83178 + 0.39366i	0.83274 + 0.28588i	-0.0009593 + 0.10777i
11	0.83178 - 0.39366i	0.83274 - 0.28588i	-0.0009593 - 0.10777i
汇总			**0.35524**

相应的两发射机系统函数系数数值如表5.4所示。

表 5.4 两发射机的系统函数系数

序号	系统函数系数		系统函数系数之差（发射机 1－发射机 2）
	发射机 1	发射机 2	
1	-0.41805	-0.062811	**-0.35524**
2	-0.60106	-0.92171	0.32065
3	0.20449	-1.2133	1.4178
4	0.12449	0.044844	0.07965
5	-0.13182	0.27776	-0.40957
6	-0.052547	-0.0094499	-0.043097
7	0.034922	0.26723	-0.23231
8	-0.21101	-0.35718	0.14617
9	0.32024	0.53297	-0.21273
10	0.097992	0.13562	-0.037627
11	-0.43631	-0.75599	0.31968

表5.3与5.4的数值结果表明：两MA系统间的多项式的第二个系数间距离是两系统的各零点间距离和，即当系统为MA系统时，定理1为 $dist((a_{m1},b_{m1}),(a_{n1},b_{n1}))=|\sum_{j=1}^{q}\Delta\beta_j|$。

同理，当把系统建模为AR系统或ARMA系统时，结果类似。

因此，理论推导与数值仿真实验证明了本节提出的把发射机基带到接收机基带部分近似为一个ARMA系统，采用ARMA系统模型分子或分母多项式的第二个系数构造射频指纹方法的正确性。

5.6.4 小结

本节的理论推导与数值仿真显示：采用ARMA系统模型分子多项式的第二个系数 a_{k1} 与分母多项式的第二个系数 b_{k1} 构成的射频指纹之间的距离是各阶零点之间距离和与各阶极点之间距离和构成的两直角边的直角三角形的斜边边长。因此，本节提出的采用ARMA系统模型分子多项式的第二个系数 a_{k1} 与分母多项式的第二个系数 b_{k1} 构成的射频指纹具有明确的物理意义。

由相同元件标称值构成的无线发射机对应的ARMA系统模型的零点之间的距离 $\Delta\beta_j$ 、极点之间的距离 $\Delta\alpha_j$ 很微小。与直接采用ARMA系统模型的零点与极点构成射频指纹相比，本节提出的射频指纹的可分离性却有可能得到增强。

本节提出的 ARMA 模型射频指纹可应用于相关无线设备的多射频指纹识别中。

5.7 本章小结

本章研究了“射频指纹识别”的第二个步骤，即：射频指纹的变换方法。首先对文献中已有的射频指纹变换方法进行了分析，把射频指纹分为基于“瞬态信号”与“稳态信号”两种；接着介绍本文提出的多种射频指纹变换方法。包括：（1）基于渐升功率前导的无线设备射频指纹变换方法。其中，提出基于渐升功率前导的无线设备射频指纹时，运用了第四章中提出的“基于前导的Wi-Fi射频指纹检测方法”，介绍了相像系数特征提取方法与*k*-NN分类器，并根据提出射频指纹对待识别无线设备进行了特征提取与分类实验；（2）基于非线性动力学中相空间重构方法的Wi-Fi发射机相空间差射频指纹识别方法；（3）基于BPSK信号的具备独立性、时间平移不变性与稳健性的射频指纹变换方法，分别为“BPSK基带倒谱射频指纹”与“BPSK频偏对数谱射频指纹”变换方法，这两种射频指纹也是对本文在第一章中尝试性提出的一种“射频指纹”定义的实例解释；（4）基于ARMA模型系数的射频指纹变换方法。

由本章提出的多种射频指纹识别研究可知，根据同一种射频指纹，有可能把某几个无线设备以较高正确识别率区分开，但对于其它无线设备，却可能得不到类似的性能。因此，基于射频指纹的无线设备识别仍是一个困难问题。

但从图1.3所示的射频指纹识别体系结构可知，从多种视角变换接收无线信号为多种独立的射频指纹时，这些独立的射频指纹体现了待识别无线发射机的各种硬件信息。因此，根据这些独立的射频指纹的多个特征对无线发射机进行识别仍具有可行性。所以，本章研究的射频指纹变换是射频指纹识别中的一个重要步骤。

第六章 总结与展望

本论文以增强无线网络物理层认证的安全性为目标，研究了根据无线设备发射机的硬件性质识别无线设备（即射频指纹识别）的关键性基础问题，包括：“射频指纹”的定义、“射频指纹识别”的过程划分与体系结构、射频指纹识别系统的基本模型、数字化射频指纹的可分离性及其影响因素、射频指纹识别中接收无线信号的起始时刻检测及各种射频指纹变换与识别方法。提出的射频指纹变换与识别方法包括：（1）基于线性与非线性混合系统的“功率渐升前导射频指纹”变换方法；（2）基于非线性系统假设的 Wi-Fi 设备相空间差射频指纹识别方法；（3）基于线性系统假设的“BPSK 射频指纹”与“ARMA 模型系数射频指纹”变换方法。其中介绍了用于评估射频指纹性能的相像系数特征提取方法与 *k*-NN 最近邻分类方法。本章对本学术论文进行总结，并指出可以进一步开展的相关研究工作。

6.1 本论文已取得的研究成果总结

本学术论文的研究取得了以下成果：

（1）针对已有文献对“射频指纹”定义及“射频指纹识别”过程划分未能揭示其本质的问题，尝试性提出了“射频指纹”的一种定义，并提出了“射频指纹识别”的一种四步骤划分法。尝试性提出的“射频指纹”定义是：射频指纹是携带无线设备发射机硬件信息的接收无线信号的变换结果，这种变换结果体现无线设备发射机的硬件性质并具有可比性；提出的“射频指纹识别”过程包括：接收无线信号的起始时刻检测、接收无线信号的对齐与截取、截取后接收无线信号的射频指纹变换、射频指纹的特征提取与特征的分类识别。提出的这种“射频指纹”定义及“射频指纹识别”过程划分方法隐含了把“射频指纹识别”体系结构分为四个层，即：接收无线信号层、射频指纹层、特征层与待识别无线发射机层。

（2）基于现代无线数字发射机的一种通用结构，分析了射频指纹的产生机理，并采用软件仿真与实验进行了验证，指出构件容差是射频指纹的主要产生机理。对待识别无线设备发送的射频信号进行了非线性与时变性分析，指出：短期内射频指纹及其识别系统可建模为时不变的，待识别发射机可建模为线性、非线性或线性/非线性的；在此基础上，构建了射频指纹识别系统的软件仿真模型、实验模型及接收无线信号的等效形式。

（3）基于构建的射频指纹识别系统模型，定义了数字化射频指纹的可分离性度量，据此推导了数字化射频指纹可分离性及其影响因素之间关系的解析式。根据该解析式，得到了以下结论：数字化射频指纹可分离性由射频指纹识别系统的分辨力、指纹维数与待识别无线设备发射机结构及构件容差性质的相对程度决定；射频指纹识别系统的分辨

力强于两数字化射频指纹之差的最大值是其可分离的必要条件；分辨力越高，则其可分离性越优；对于给定的待识别无线设备，在射频指纹识别系统的分辨力一定的情况下，射频指纹的维数越多，则其可分离性越优。“极限情况下数字化射频指纹可分离”等价于“模拟射频指纹是唯一的”。

（4）提出了利用无线设备物理层帧前导的确定性及“相关”技术进行接收无线信号起始时刻检测的新方法；根据提出方法确定的起始时刻进行接收无线信号的对齐与截取，采用截取后信号变换得到的射频指纹的可分性优于基于Wi-Fi Bayesian渐升变点检测得到的射频指纹的可分性。

（5）提出了无线设备的“功率渐升前导射频指纹”的变换及其产生技术。建模理论分析显示：在相同的接收信号采集条件下，“功率渐升前导射频指纹”的可分性比经典的 turn-on 射频指纹与 steady-state 射频指纹的可分性优。“功率渐升前导射频指纹”的产生方法（功率渐升同时发送前导序列）可应用到相关标准中。

（6）提出了根据 Wi-Fi 前导射频信号重构的非线性相空间识别 Wi-Fi 设备的方法。该方法把待识别 Wi-Fi 无线设备的发射机建模为非线性动力学系统，对 Wi-Fi 射频信号进行带通采样，把带通采样信号嵌入相同的非线性相空间，计算相空间中连续两点的导数，通过对训练样本与测试样本的相空间导数差进行比对从而实现 Wi-Fi 发射机的识别。数值仿真实验与实验表明了该方法的正确性与有效性。

（7）提出了基于接收 BPSK 信号的两种射频指纹变换技术，分别为基于接收基带信号的“基带倒谱射频指纹”变换技术与基于接收带通信号的“频偏对数谱射频指纹”变换技术。建模理论分析与实验显示：提出的这两种 BPSK 射频指纹减弱了时变无线多径信道及发送基带数字信号影响，主要由待识别发射机的硬件性质决定，因而具备独立性、时间平移不变性与稳健性。

（8）提出了在把射频指纹识别系统建模为ARMA系统的假设下，把ARMA系统函数多项式的第二个系数作为射频指纹的方法。理论推导与数值仿真显示：与直接采用ARMA系统的零点与极点相比，该方法有可能增大微小差别ARMA系统间的类间距离。

6.2 可以进一步研究的问题

基于射频指纹的无线网络物理层安全增强方法在信息技术日益重要的当今社会中具有广阔的应用前景。国外在这方面已经做了一些研究工作，近年来取得了一些研究成果。然而，国内的研究工作才刚刚开始。本文仅对一些关键性基础问题进行了一些探索研究，仍有许多问题有待同行们来一起研究，我们认为如下的问题值得考虑：

（1） 克服无线多径信道对射频指纹的不利影响问题。无线多径信道的时变性导致射频指纹缺乏稳定性，如何消除或减弱基于各种通信信号的射频指纹中无线多径信道的影响仍是一个需要研究的问题。

（2） 射频指纹的特征提取问题。同一种射频指纹可以采用不同的特征提取方法，

采用何种特征提取方法进行射频指纹的特征提取也是需要进一步研究的问题。

（3） 其它种类的射频指纹变换方法问题。从不同的视角，变换更多种类的射频指纹，从而提取尽量多的待识别发射机硬件信息的问题。

（4） 射频指纹的时变性问题。由于老化等原因导致的射频指纹长期稳定性是影响射频指纹识别的一个不利因素；同时也是由该硬件所处外界环境决定的。因此，待识别发射机的时变性质是否可以作为一种射频指纹用来识别该发射机问题。另外，如何对射频指纹的老化进行管理也是一个需要研究的问题。

（5） 无线发射机天线极性对射频指纹的影响问题。天线极性对于射频指纹各种性质的影响问题。

（6） 射频指纹的跨层融合识别问题。如何融合射频指纹识别体系中各层之间及之内信息，提高射频指纹识别性能的问题。

（7） 多天线无线设备的识别问题。

（8） 采用多天线接收机进行射频指纹识别的问题。等等。

本学位论文的研究表明：基于射频指纹的无线网络物理层认证方法在未来的无线通信中具备应用价值。不同待识别无线发射机的构件容差差别一般较小，加上时变无线多径信道与噪声等的不利影响，根据射频指纹识别无线发射机仍是一个困难的问题。从不同角度变换接收无线信号为多种射频指纹，进而进行无线发射机的多射频指纹、多层次识别值得进一步的深入研究。

本文仅对“射频指纹识别”中的一些关键性基础问题进行了一些初步的探索研究。基于待识别无线设备相对于“雷达”与“电台”等其他辐射源的一些特殊性，本文取得了一些结果，但仍需同行专家给予评价或指正。

致谢

首先，我要感谢我的博士生导师胡爱群教授。胡老师在我博士生入学之前早就认识到该题目的研究价值，事实证明，本论文的选题具有重要的实际意义，已显示出成为无线安全领域研究热点的趋势。攻读期间，胡老师与我关于研究题目的讨论不仅改变了我许多根深蒂固的“工程”观念，而且使我的研究不断向前推进。射频指纹的产生机理、唯一性、可分性与可分离性；无线发射机的线性与非线性；接收射频信号的分离与倒谱变换；如此等等，不胜枚举。与胡老师的每一次讨论，都使我的研究向前迈进一点。可以说，这篇博士大论文的所有内容，都是在与胡老师的讨论中诞生的。胡老师的指导令我终生收益，毕生难忘。同时，我要感谢东南大学的毕光国与张在琛老师，他们在我的研究初期提供了帮助。

其次，我要感谢南通大学电子信息学院及“通信与信息系统”学科的领导与同事，没有他们，我的在职攻读博士学位工作无法完成。其中，徐晨与章国安教授带领我在入学之前参加了毕光国与张在琛老师的科研项目，使我有机会参加高水平的科研活动；章国安与包志华教授对我的科研活动与项目申请给予了大力支持；丁伟红与杨永杰主任对我的日常教学工作提供了支持。另外，我要感谢包志华教授领导的“通信与信息系统”学科，该学科配置的高性能仪器为我的研究提供了有力支撑，该学科的张士兵、谢正光、周晖与陈建新等教授/博士为我与他们的讨论营造了宽松的学术氛围。如此等等，不胜枚举。

再次，我要感谢东南大学信息安全学科的其他老师与同学，是他们让我的博士生活如此丰富多彩并且如此难忘。

最后，我要感谢我的家人。我的爱人独自操持家庭，解除了我的后顾之忧，给我节省了大量的科研时间；我的四年级的儿子一直在等着看我的博士帽；我的农民父母赋予了我勤劳肯干与百折不挠的习惯。

参考文献

[1] 王育民, 刘建伟. 通信网的安全 --- 理论与技术 [M]. 西安: 电子科技大学出版社, 1999.

[2] 胡爱群, 宋宇波, 蒋睿. 信息安全 [M]. 武汉: 华中科技大学出版社, 2010.

[3] K. Zeng, K. Govindan, and P. Mohapatra. Non-Cryptographic Authentication and Identification in Wireless Networks [J]. IEEE Wireless Communications, vol. 17, pp. 56-62, Oct 2010.

[4] S. Mathur, A. Reznik, C. X. Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe, and N. Mandayam. Exploiting the Physical Layer for Enhanced Security [J]. IEEE Wireless Communications, vol. 17, pp. 63-70, Oct 2010.

[5] J. Kwon, B. Dundar, and P. Varaiya. Hybrid algorithm for indoor positioning using wireless LAN [C]. In Vehicular Technology Conference, IEEE 60th, 2004, pp. 4625-4629 Vol. 7.

[6] K. Raman Kumar, V. Apte, and Y. A. Powar. Improving the accuracy of wireless lan based location determination systems using kalman filter and multiple observers [C]. In Wireless Communications and Networking Conference, IEEE, 2006, pp. 463-468.

[7] H. Liu, H. Darabi, P. Banerjee, and J. Liu. Survey of wireless indoor positioning techniques and systems [J]. IEEE Transactions on Systems Man and Cybernetics Part C-Applications and Reviews, vol. 37, pp. 1067-1080, Nov 2007.

[8] Y. Qingming, W. Fei-Yue, G. Hui, W. Kunfeng, and Z. Hongxia. Location estimation in ZigBee Network based on fingerprinting [C]. In Vehicular Electronics and Safety, IEEE International Conference on, 2007, pp. 1-6.

[9] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe. Fingerprints in the ether: Using the physical layer for wireless authentication [C]. In IEEE International Conference on Communications (ICC 2007), Glasgow, SCOTLAND, 2007, pp. 4646-4651.

[10] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe. Fingerprints in the Ether-ppt [R]. 2007.

[11] M. F. Catedra, J. M. Gomez, L. Lozano, and I. Gonzalez. Application of GTD for location systems [J]. Radio Science, vol. 43, p. 10, Dec 2008.

[12] A. Malekpour, T. C. Ling, and W. C. Lim. Location Determination Using Radio Frequency RSSI and Deterministic Algorithm [C]. In Communication Networks and Services Research Conference, 6th Annual, 2008, pp. 488-495.

[13] M. S. Obaidat and T. Guelzim. A new security access scheme for WLANs and its performance simulation analysis [J]. Simulation-Transactions of the Society for Modeling and Simulation International, vol. 84, pp. 311-321, Jun 2008.

[14] A. Sayeed and A. Perrig. Secure wireless communications: Secret keys through multipath [C]. In 33rd IEEE International Conference on Acoustics, Speech and Signal Processing, Las Vegas, NV, 2008, pp. 3013-3016.

[15] E. Velasco, W. F. Chen, P. Ji, and R. Hsieh. Wireless forensic: A new radio frequency based locating system [C]. In Pacific Asian Workshop on Intelligence and Security Informatics, Taipei, TAIWAN, 2008, pp. 272-277.

[16] E. Velasco, C. Weifeng, J. Ping, and R. Hsieh. Challenges of Location Tracking Techniques in Wireless Forensics [C]. In Intelligent Information Hiding and Multimedia Signal Processing, International Conference on, 2008, pp. 3-6.

[17] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe. A physical-layer technique to

enhance authentication for mobile terminals [C]. In IEEE International Conference on Communications (ICC 2008), Beijing, PEOPLES R CHINA, 2008, pp. 1520-1524.
[18] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe. Using the physical layer for wireless authentication in time-variant channels [J]. IEEE Transactions on Wireless Communications, vol. 7, pp. 2571-2579, Jul 2008.
[19] J. Yang and Y. Chen. A theoretical analysis of wireless localization using RF-based fingerprint matching [C]. In 22nd IEEE International Parallel and Distributed Processing Symposium (IPDPS 2008), Miami, FL, 2008, pp. 3566-3571.
[20] A. Peres and R. F. Weber. Network Security Through Wireless Location [C]. In 2009 Latin American Network Operations and Management Symposium, J. Baliosian, L. Z. Granville, and P. RodriguezBocca, Eds., 2009, pp. 33-40.
[21] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe. Channel-Based Detection of Sybil Attacks in Wireless Networks [J]. IEEE Transactions on Information Forensics and Security, vol. 4, pp. 492-503, Sep 2009.
[22] H. Wen, P. H. Ho, and G. Gong. A framework of physical layer technique assisted authentication for vehicular communication networks [J]. Science China-Information Sciences, vol. 53, pp. 1996-2004, Oct 2010.
[23] F. guo and T. Chiueh. Sequence Number-based MAC Address spoof detection [C]. In Proc. 8th int'l. Symp. Recent Advnces in intrusion detection, 2005.
[24] J. Pang. 802.11 User Fingerprinting [C]. In Proc. 13th ACM MobiCom'07, 2007.
[25] L. Bolotnyy and G. Robins. Physically Unclonable Function-Based Security and Privacy in RFID Systems [C]. In Pervasive Computing and Communications, Fifth Annual IEEE International Conference on, 2007, pp. 211-220.
[26] S. Jana and S. K. Kasera. On fast and accurate detection of unauthorized wireless access points using clock skews [C]. In Proc. 14th ACM MobiCom'08 2008.
[27] G. Kambourakis and S. Gritzalis. On device authentication in wireless networks: Present issues and future challenges [C]. In 4th International Conference on Trust, Privacy, and Security in Digital Business, Regensburg, GERMANY, 2007, pp. 135-144.
[28] C. Yu-Tso, A. Studer, and A. Perrig. Combining TLS and TPMs to Achieve Device and User Authentication for Wi-Fi and WiMAX Citywide Networks [C]. In Wireless Communications and Networking Conference, IEEE, 2008, pp. 2804-2809.
[29] J. Hall, M. Barbeau, and E. Kranakis. Detection of Transient in Radio Frequency Fingerprinting using Signal Phase [C]. Wireless and Optical Communications, 2003.
[30] J. Hall, M. Barbeau, and E. Kranakis. Enhancing Intrusion Detection in Wicreless Networks Using Radio Frequency Fingerprinting (Extended Abstract) [C]. In Communications,Internet and Information Technology(CIIT), St. Thomas, US Virgin Islands, 2004.
[31] H. Y. Chen and T. Sivakumar. Access control for future mobile devices [C]. In IEEE Wireless Communications and Networking Conference, New Orleans, LA, 2005, pp. 1527-1532.
[32] T. Daniels, M. Mina, and S. F. Russell. Short paper: A signal fingerprinting paradigm for general physical layer and sensor network security and assurance [C]. In 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, Athens, GREECE, 2005, pp. 219-221.
[33] K. A. Remley, C. A. Grosvenor, R. T. Johnk, D. R. Novotny, P. D. Hale, M. D. McKinley, A. Karygiannis, and E. Antonakakis. Electromagnetic signatures of WLAN cards and network security [C]. In Signal Processing and Information Technology, Proceedings of the Fifth IEEE International Symposium on, 2005, pp. 484-488.
[34] O. Ureten and N. Serinken. Bayesian detection of Wi-Fi transmitter RF fingerprints [J].

Electronics Letters, vol. 41, pp. 373-374, 2005.
[35] M. Barbeau, J. Hall, and E. Kranakis. Detecting impersonation attacks in future wireless and mobile networks [C]. In Secure Mobile Ad-Hoc Networks and Sensors. vol. 4074, M. Burmester and A. Yasinsac, Eds., 2006, pp. 80-95.
[36] C. L. Corbett, R. A. Beyah, and J. A. Copeland. Using active scanning to identify wireless NICs [C]. In 2006 IEEE Information Assurance Workshop, 2006, pp. 239-246.
[37] B. Sieka. Using radio device fingerprinting for the detection of impersonation and Sybil attacks in wireless networks [C]. In 3rd European Workshop on Security and Privacy in Ad Hoc and Sensor Network, Hamburg, GERMANY, 2006, pp. 179-192.
[38] A. A. Tomko, C. J. Rieser, and L. H. Buell. Physical-Layer Intrusion Detection in Wireless Networks [C]. In Military Communications Conference, IEEE, 2006, pp. 1-7.
[39] J. Heider and J. Schutte. Security made easy: Achieving user-friendly communication protection in ad-hoc situations [C]. In Emerging Security Information, Systems, and Technologies, The International Conference on, 2007, pp. 139-144.
[40] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall. 802.11 User Fingerprinting [C]. In 13th ACM International Conference on Mobile Computing and Networking, Montreal, CANADA, 2007, pp. 99-110.
[41] K. B. Rasmussen and S. Capkun. Implications of radio fingerprinting on the security of sensor networks [C]. In 3rd International Conference o Security and Privacy in Communication Networks and Workshops, Nice, FRANCE, 2007, pp. 331-340.
[42] K. Tao, J. Li, and S. Sampalli. Detection of Spoofed MAC Addresses in 802.11 Wireless Networks [C]. In 4th International Conference on E-Business and Telecommunication Networks, Barcelona, SPAIN, 2007, pp. 201-213.
[43] O. Ureten and N. Serinken. Wireless security through RF fingerprinting [J]. Electrical and Computer Engineering, Canadian Journal of, vol. 32, pp. 27-33, 2007.
[44] S. Bratus, C. Cornelius, D. Kotz, and D. Peebles. Active Behavioral Fingerprinting of Wireless Devices [C]. In 1st ACM Conference on Wireless Network Security, Alexandria, VA, 2008, pp. 56-61.
[45] V. Brik, S. Banerjee, M. Gruteser, and S. Oh. Wireless Device Identification with Radiometric Signatures [C]. In 14th ACM International Conference on Mobile Computing and Networking, San Francisco, CA, 2008, pp. 116-127.
[46] C. L. Corbett, R. A. Beyah, and J. A. Copeland. Passive classification of wireless NICs during active scanning [J]. International Journal of Information Security, vol. 7, pp. 335-348, Oct 2008.
[47] I. O. Kennedy, P. Scanlon, and M. M. Buddhikot. Passive Steady State RF Fingerprinting: A Cognitive Technique for Scalable Deployment of Co-Channel Femto Cell Underlays [C]. In New Frontiers in Dynamic Spectrum Access Networks, 3rd IEEE Symposium on, 2008, pp. 1-12.
[48] I. O. Kennedy, P. Scanlon, F. J. Mullany, M. M. Buddhikot, K. E. Nolan, and T. W. Rondeau. Radio Transmitter Fingerprinting: A Steady State Frequency Domain Approach [C] In Vehicular Technology Conference, IEEE 68th, 2008, pp. 1-5.
[49] D. A. Knox and T. Kunz. Secure Authentication in Wireless Sensor Networks Using RF Fingerprints [C]. In Embedded and Ubiquitous Computing, IEEE/IFIP International Conference on, 2008, pp. 230-237.
[50] D. A. Knox and T. Kunz. RF Fingerprints for Secure Authentication in Single-Hop WSN [C]. In Networking and Communications, IEEE International Conference on Wireless and Mobile Computing, 2008, pp. 567-573.
[51] W. C. Suski, M. A. Temple, M. J. Mendenhall, and R. F. Mills. Using Spectral Fingerprints to Improve Wireless Network Security [C]. In Global

Telecommunications Conference, IEEE, 2008, pp. 1-5.
[52] 胡云波等. 基于无线局域网的认证方法研究 [J]. 计算机工程与应用, vol. 44, p. 4, 2008.
[53] A. Chouchane, S. Rekhis, and N. Boudriga. Defending against Rogue Base Station Attacks using Wavelet Based Fingerprinting [C]. In 7th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA-09), Rabat, MOROCCO, 2009, pp. 523-530.
[54] B. Danev and S. Capkun. Transient-based Identification of Wireless Sensor Nodes[C]. In 2009 International Conference on Information Processing in Sensor Networks, 2009, pp. 25-36.
[55] M. Hamdi, A. Meddeb-Makhlouf, and N. Boudriga. Multilayer Statistical Intrusion Detection in Wireless Networks [J]. Eurasip Journal on Advances in Signal Processing, 2009.
[56] R. W. Klein, M. A. Temple, and M. J. Mendenhall. Application of Wavelet-Based RF Fingerprinting to Enhance Wireless Network Security [J]. Journal of Communications and Networks, vol. 11, pp. 544-555, Dec 2009.
[57] R. W. Klein, M. A. Temple, M. J. Mendenhall, and D. R. Reising. Sensitivity Analysis of Burst Detection and RF Fingerprinting Classification Performance [C]. In Ieee International Conference on Communications, Vols 1-8, 2009, pp. 641-645.
[58] A. Candore, O. Kocabas, and F. Koushanfar. Robust stable radiometric fingerprinting for wireless devices[C]. In Hardware-Oriented Security and Trust, IEEE International Workshop on, 2009, pp. 43-49.
[59] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy. Attacks on Physical-layer Identification[C]. In Wisec 10: Proceedings on the Third Acm Conference on Wireless Network Security, 2010, pp. 89-98.
[60] R. W. Klein, M. A. Temple, and M. J. Mendenhall. Application of wavelet denoising to improve OFDM-based signal detection and classification[J]. Security and Communication Networks, vol. 3, pp. 71-82, Jan-Feb 2010.
[61] H. L. Yuan and A. Q. Hu. Preamble-based detection of Wi-Fi transmitter RF fingerprints [J]. Electronics Letters, vol. 46, pp. 1165-1167, 2010.
[62] Most secret war [M]. Hamilton, 1978.
[63] L. L. E. Specific emitter identification(SEI) and classical parameter fusion technology [M], 1993.
[64] B. W. Gillespie and L. E. Atlas. Optimization of time and frequency resolution for radar transmitter identification[C]. In Acoustics, Speech, and Signal Processing, IEEE International Conference on, 1999, pp. 1341-1344 vol.3.
[65] B. W. Gillespie and L. E. Atlas. Optimizing time-frequency kernels for classification[C]. Signal Processing, IEEE Transactions on, vol. 49, pp. 485-496, 2001.
[66] T. K. I and D. P. R. Specific Emitter Identification and Verification [M], 2003.
[67] 张葛祥. 雷达辐射源信号智能识别方法研究 [D]. 博士: 西南交通大学, 2005.
[68] 张国柱. 雷达辐射源识别技术研究 [D]. 博士: 国防科学技术大学, 2005.
[69] L. Du, H. W. Liu, and Z. Bao. Radar HRRP statistical recognition: Parametric model and model selection [J]. IEEE Transactions on Signal Processing, vol. 56, pp. 1931-1944, May 2008.
[70] L. Hoi-Shun and N. V. Z. Shuley. Sampling Procedures for Resonance Based Radar Target Identification [J]. Antennas and Propagation, IEEE Transactions on, vol. 56, pp. 1487-1491, 2008.
[71] J. Matuszewski. Specific emitter identification [C]. In Radar Symposium, International, 2008, pp. 1-4.

[72] 许丹. 辐射源指纹机理及识别方法研究 [D]. 博士: 国防科学技术大学, 2008.
[73] C. A. Rypinski. Equipment for an automatic transmitter identification system (ATIS) [C]. In Vehicular Technology Conference, 26th IEEE, 1976, pp. 111-117.
[74] K. G. Johannsen. Automatic transmitter identification system [J]. Broadcasting, IEEE Transactions on, vol. 38, pp. 127-132, 1992.
[75] H. C. Choe, C. E. Poole, A. M. Yu, and H. H. Szu. Novel identification of intercepted signals from unknown radio transmitters [J]. SPIE, vol. 2491, p. 14, 1995.
[76] M. B. Frederick. Cellular telephone anti-fraud system [P]. U.S. Patent No.5448760, 1995.
[77] J. Toonstra and W. Kinsner. Transient analysis and genetic algorithms for classification [C]. In Communication, Power, and Computing, Winnipeg, Man., 1995, pp. 432-437.
[78] R. D. Hippenstiel and Y. Payal. Wavelet Based Transmitter Identification [C]. In Signal Processing and Its Applications, Fourth International Symposium on, 1996, pp. 740-742.
[79] J. Toonstra and W. Kinsner. A radio transmitter fingerprinting system ODO-1 [C]. In Electrical and Computer Engineering, Canadian Conference on, 1996, pp. 60-63 vol.1.
[80] D. Shaw and W. Kinsner. Multifractal modelling of radio transmitter transients for classification [C]. In WESCANEX 97: Communications, Power and Computing, IEEE, 1997, pp. 306-312.
[81] K.D.Hawkes. Transient analysis system for characterizing RF transmitters by analyzing transmitted RF signals [P]. U.S. Patent No. 5758277, 1998.
[82] L. Sun and W. Kinsner. Fractal segmentation of signal from noise for radio transmitter fingerprinting [C]. In Electrical and Computer Engineering, IEEE Canadian Conference on, 1998, pp. 561-564 vol.2.
[83] L. Sun, W. Kinsner, and N. Serinken. Characterization and feature extraction of transient signals using multifractal measures [C]. In Electrical and Computer Engineering, IEEE Canadian Conference on, 1999, pp. 781-785 vol.2.
[84] O. Ureten and N. Serinken. Detection of radio transmitter turn-on transients [J]. Electronics Letters, vol. 35, pp. 1996-1997, 1999.
[85] M. J. Riezenman. Cellular security: better, but foes still lurk [J]. Spectrum, IEEE, vol. 37, pp. 39-42, 2000.
[86] N. Serinken and O. Ureten. Generalised dimension characterisation of radio transmitter turn-on transients [J]. Electronics Letters, vol. 36, pp. 1064-1066, 2000.
[87] K. J. Ellis and N. Serinken. Characteristics of radio transmitter fingerprints [J]. Radio Science, vol. 36, pp. 585-597, 2001.
[88] I. KEN, S. MASAAKI, and S. TSUTOMU. Adaptive Array Algorithms for Radio Transmitter Identification Based on the Transient Response [J]. IEICE Transactions on Communications, vol. J84-B, pp. 1233-1238, 2001.
[89] E. Carlos and J. Takada. ICA based blind source separation applied to radio surveillance [J]. IEICE Transactions on Communications, vol. E86B, pp. 3491-3497, Dec 2003.
[90] O. H. Tekbas, N. Serinken, and O. Ureten. An experimental performance evaluation of a novel radio-transmitter identification system under diverse environmental conditions [J]. Electrical and Computer Engineering, Canadian Journal of, vol. 29, pp. 203-209, 2004.
[91] O. H. Tekbas, O. Ureten, and N. Serinken. Improvement of transmitter identification system for low SNR transients [J]. Electronics Letters, vol. 40, pp. 182-183, 2004.
[92] O. H. Tekbas, O. Ureten, and N. Serinken. Classification of low SNR transient signals using training with noise technique [C]. In Signal Processing and Communications Applications Conference, Proceedings of the IEEE 12th, 2004, pp. 91-94.

[93] 任春辉. 通信电台个体特征分析 [D].博士: 电子科技大学, 2006.
[94] X. Shuhua, H. Benxiong, H. Yuchun, and X. Zhengguang. Identification of Individual Radio Transmitters Based on Selected Surrounding-line Integral Bispectra [C]. In Advanced Communication Technology, The 9th International Conference on, 2007, pp. 1147-1150.
[95] S. H. Xu, B. X. Huang, L. Xu, and Z. G. Xu. Radio transmitter classification using a new method of stray features analysis combined with PCA [C]. In IEEE Military Communications Conference (MILCOM 2007), Orlando, FL, 2007, pp. 1803-1807.
[96] S. Xu, L. Xu, Z. Xu, and B. Huang. Individual radio transmitter identification based on spurious modulation characteristics of signal envelop [C]. In Military Communications Conference, IEEE, 2008, pp. 1-5.
[97] P. S. Ravikanth. Physical One-Way Functions [D]. Doctor of Philosophy in Media Arts and Sciences: Massachusetts Institute of Technology, 2001.
[98] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld. physical one-way functions [J]. Science, vol. 297, p. 5, 2002.
[99] L. W. Couch, 罗新民, 任品毅, 田琛. 数字与模拟通信系统 [M]. 北京: 电子工业出版社, 2002.
[100] 张贤达, 保铮. 通信信号处理 [M]. 北京: 国防工业出版社, 2000.
[101] D. Wisell. Identification and Measurement of Transmitter Non-Linearities [C]. In ARFTG Conference Digest-Fall, 56th, 2000, pp. 1-6.
[102] T. L. Carroll. A nonlinear dynamics method for signal identification [J]. Chaoe, vol. 17, 2007.
[103] A. Hajimiri and T. H. Lee. A general Theory of Phase Noise in Electronical Oscillators [J]. IEEE Journal of Solid-State Circuits, vol. 33, pp. 179-194, 1998.
[104] S. Theodoridis and K. Koutroumbas. Pattern Recognition [M]. Academic Press, fourth Edition, 2008.
[105] D. Shaw and W. Kinsner. Multifractal modelling of radio transmitter transient for classification [C]. In Communications Power and Computing, Winnipeg Manitoba, 1997, pp. 306-312.
[106] J. J. Rajan. Time Series Classification [D]. Doctor of Philosophy: Cambridge University, England, 1994.
[107] J. K. Joseph and J. F. William. Numerical Bayesian Methods Applied to signal Processing [M]. New York: Springer, 1996.
[108] 周晓光, 王晓华. 射频识别(RFID)技术原理与应用实例 [M]. 北京: 人民邮电出版社, 2006.
[109] Z. Gexiang, J. Weidong, and H. Laizhao. Resemblance Coefficient Based Intrapulse Feature Extraction Approach for Radar Emitter Signals [J]. Chinese Journal of Electronics, vol. 14, pp. 337-340, 2005.
[110] T. Cover and P. Hart. Nearest neighbor pattern classification [J]. Information Theory, IEEE Transactions on, vol. 13, pp. 21-27, 1967.
[111] 孙即祥. 现代模式识别 [M]. 长沙: 国防科技大学出版社, 2001.
[112] 刘延柱, 陈立群. 非线性动力学 [M]. 上海: 上海交通大学出版社, 2000.
[113] 刘秉正. 非线性动力学 [M]. 北京: 高等教育出版社, 2004.
[114] M. Henon. A Two-dimonsional Mapping with a Strange Attractor [J]. Commun. math. Phys., vol. 50, pp. 69-77, 1976.
[115] N. H. Packard, J. P. Crutchfield, and J. D. Farmer. Geometry from a time series [J]. Phys Rev Lett, vol. 45, p. 712~715, 1980.
[116] F. Takens. Detecting strange attractors in turbulence [J]. Lecture Notes in Mathematica, vol. 898, 1981.

[117] L. Cao. Practical method for determining the minimum embedding dimension of a scalar tiem series [J]. Phys. D, vol. 110, pp. 43-50, 1997.
[118] S. T., Y. J. A., and C. M. J. Stat. [J]. Phys., vol. 65, p. 579, 1991.
[119] R. W. Schafer. Echo Removal By Discrete Generalized Linear Filtering [D]. Doctor of Philosophy: Massachusefts Institute of Technology, 1969.
[120] 皇甫堪, 陈建文, 楼生强. 现代数字信号处理 [M]. 北京: 电子工业出版社, 2004.
[121] C. L. Nikias and J. M. Mendel. Signal processing with higher-order spectra [J]. IEEE Signal Processing Magzine, vol. 10, pp. 10-37, 1993.
[122] B. Friedlander and B. Porat. Asymptotically optimal estimation of MA and ARMA parameters of non-Gaussian process from high-order moments [J]. IEEE Trans. On Automatic Control, vol. 35, pp. 27-37, 1990.
[123] Proakis, 张力军（译）. 数字通信（第四版） [M]. 北京: 电子工业出版社, 2006.

附录 A：式（3.13）的推导

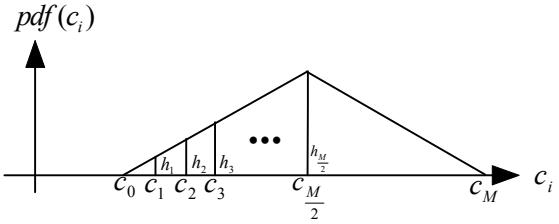

图 A.1 三角形概率密度函数分布

已知：$c_i, i = 0,1,...,M$ 为元件值，M 为偶数，$\Delta c_{lsb} = c_{m+1} - c_m, m = 0,1,2,...,M-1$，$M * \Delta c_{lsb} = 2\Delta c$，$\int_0^{2\Delta c} pdf(c)dc = 1$。求：$\sum_{m=0}^{M-1}(\int_{c=c_m}^{c_{m+1}} pdf(c)dc)^2$。

解：假设 $S_m = \int_{c=c_m}^{c_{m+1}} pdf(c)dc, m = 0,1,...,M-1$；

由 $\int_0^{2\Delta c} pdf(c)dc = 1$ 得，$h_{\frac{M}{2}} = \frac{1}{\Delta c}$；

由相似三角形关系，得 $h_1 = \frac{2}{M * \Delta c}$，$S_0 = \frac{2}{M^2}$；

则：

$$\frac{1}{2}\sum_{m=0}^{M-1}(\int_{c=c_m}^{c_{m+1}} pdf(c)dc)^2 = \sum_{m=0}^{\frac{M}{2}-1}(S_m)^2$$

$$= \sum_{m=0}^{\frac{M}{2}-1}(S_0 + \Delta c_{lsb} h_o m)^2$$

$$= \frac{4}{M^4}\sum_{m=0}^{\frac{M}{2}-1}(1+2m)^2$$

$$= \frac{4}{M^4}[\frac{M}{2} + 4\sum_{m=0}^{\frac{M}{2}-1} m + 4\sum_{m=0}^{\frac{M}{2}-1} m^2]$$

$$= \frac{2}{3}[\frac{1}{M} - (\frac{1}{M})^3]$$

即：

$$\sum_{m=0}^{M-1}\left(\int_{c=c_m}^{c_{m+1}} pdf(c)dc\right)^2$$

$$=\frac{1}{3}\left[\frac{1}{M}-\left(\frac{1}{M}\right)^3\right]$$

附录 B：3.4 节中的证明

“当 *LSB* 减小为 i 分之一时，即射频指纹识别系统的分辨力增加为 i 倍时，可分离性度量 P_{disc} 下降”的证明。

证明：文中

$$P_{disc}=\prod_{v=1}^{M}[\sum_{N_u=N_{u,\min}}^{N_{u,\max}}(\int_{\mathrm{RFF_u(x_v)}=LSB*(N_u-1)}^{LSB*N_u} pdf\{\mathrm{RFF_u(x_v)}\}d\mathrm{RFF_u(x_v)})^2] \\ =\prod_{v=1}^{M}P_v \tag{B.1}$$

其中

$$P_v=\sum_{N_u=N_{u,\min}}^{N_{u,\max}}(\int_{\mathrm{RFF_u(x_v)}=LSB*(N_u-1)}^{LSB*N_u} pdf\{\mathrm{RFF_u(x_v)}\}d\mathrm{RFF_u(x_v)})^2] \tag{B.2}$$

为简单起见，*LSB* 用 Δx 代替，表示为 $LSB\rightarrow\Delta x$，下同。$\mathrm{RFF_u(x_v)}\rightarrow$X，$pdf\{\mathrm{RFF_u(x_v)}\}\rightarrow$f(X)，$RFF_{u,\min}\rightarrow x_{\min}$，$RFF_{u,\max}\rightarrow x_{\max}$。则第三章中图 3.4 为图 B.1 所示。

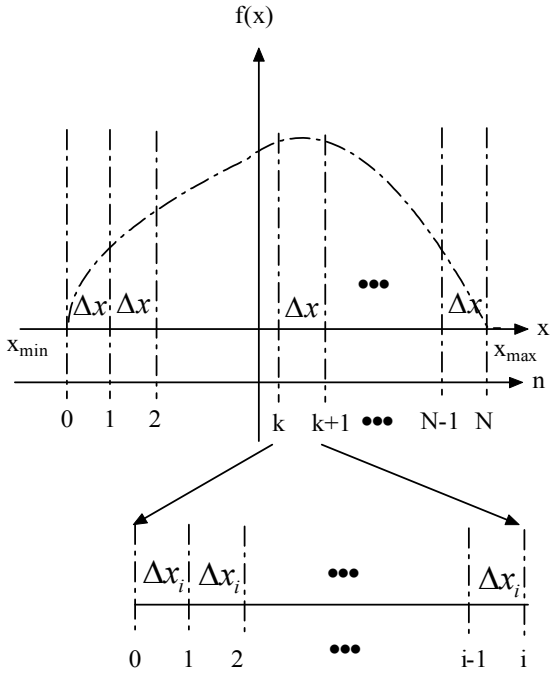

图 B. 1 一个 $pdf\{RFF_u(x_v)\}$ 实例

假设 $\frac{x_{\max}-x_{\min}}{\Delta x}=N$，N 为整数；则如图 B.1 所示，把 X 在 $(x_{\min},x_{\max})$ 部分分为 N 等份。假设再把每个 Δx 分为 i 等份，即：$i\bullet\Delta x_i=\Delta x$，第 k 个 Δx 分为 i 等份的示意图如图 B.1 所示；则 X 在第 k 个 Δx 内的概率为

$$
\begin{aligned}
P_k &= \int_{X=k\bullet\Delta x}^{(k+1)\bullet\Delta x} f(X)dX \\
&= \int_{X=k\bullet\Delta x}^{k\bullet\Delta x+i\bullet\Delta x_i} f(X)dX \\
&= \int_{X=k\bullet\Delta x}^{k\bullet\Delta x+\Delta x_i} f(X)dX + \int_{X=k\bullet\Delta x+\Delta x_i}^{k\bullet\Delta x+2\bullet\Delta x_i} f(X)dX + \bullet\bullet\bullet + \int_{X=k\bullet\Delta x+(i-1)\bullet\Delta x_i}^{k\bullet\Delta x+i\bullet\Delta x_i} f(X)dX
\end{aligned}
\tag{B.3}
$$

则 X 在其各 Δx 内的概率平方和

$$
\begin{aligned}
P_v &= \sum_{n=0}^{N-1} P_n^2 \\
&= \sum_{n=0}^{N-1} [\int_{X=n\bullet\Delta x}^{n\bullet\Delta x+\Delta x_i} f(X)dX + \int_{X=n\bullet\Delta x+\Delta x_i}^{n\bullet\Delta x+2\bullet\Delta x_i} f(X)dX + \bullet\bullet\bullet + \int_{X=n\bullet\Delta x+(i-1)\bullet\Delta x_i}^{n\bullet\Delta x+i\bullet\Delta x_i} f(X)dX]^2 \\
&= P_v^{'} + r
\end{aligned}
\tag{B.4}
$$

其中

$$
\begin{aligned}
P_v^{'} &= \sum_{n=0}^{N-1} \{[\int_{X=n\bullet\Delta x}^{n\bullet\Delta x+\Delta x_i} f(X)dX]^2 + [\int_{X=n\bullet\Delta x+\Delta x_i}^{n\bullet\Delta x+2\bullet\Delta x_i} f(X)dX]^2 + \bullet\bullet\bullet \\
&+ [\int_{X=n\bullet\Delta x+(i-1)\bullet\Delta x_i}^{n\bullet\Delta x+i\bullet\Delta x_i} f(X)dX]^2\} \\
&= \sum_{m=0}^{i\bullet N-1} [\int_{X=m\bullet\Delta x_i}^{(m+1)\bullet\Delta x_i} f(X)dX]^2
\end{aligned}
\tag{B.5}
$$

而

$$
\begin{aligned}
r = \sum_{n=0}^{N-1} \{ & 2\bullet\int_{X=n\bullet\Delta x}^{n\bullet\Delta x+\Delta x_i} f(X)dX \bullet \int_{X=n\bullet\Delta x+\Delta x_i}^{n\bullet\Delta x+2\bullet\Delta x_i} f(X)dX \\
& + 2\bullet\int_{X=n\bullet\Delta x++\Delta x_i}^{n\bullet\Delta x+2\bullet\Delta x_i} f(X)dX \bullet \int_{X=n\bullet\Delta x+2\bullet\Delta x_i}^{n\bullet\Delta x+3\bullet\Delta x_i} f(X)dX + \bullet\bullet\bullet]\} > 0
\end{aligned}
\tag{B.6}
$$

式（B.4）中 $P_v^{'}$ 表示 X 在各 Δx_i 内的概率平方和，由于 r>0，所以，由式（B.4）可知，$P_v^{'} = P_v - r < P_v$，即 Δx 减小为 i 分之一后，X 在各小份内概率的平方和下降；即式（B.1）中的 LSB 减小为 $\frac{LSB}{i}$（i 为大于 1 的整数）时，式（B.4）表示的 P_v 下降。

由式（B.1）可知，可分离性度量 P_{disc} 随 P_v 的下降而下降。

攻读博士学位期间的主要研究成果

（一）以第一作者发表和完成的论文

1. Honglin Yuan, Aiqun Hu. Preamble-based detection of Wi-Fi transmitter RF fingerprints. Electronics letters, 2010,46(16):1165-1167. (检索情况：SCI)
2. 袁红林, 胡爱群. 射频指纹的唯一性研究. 应用科学学报, 2009,27(1):1-5.
3. 袁红林,胡爱群. 射频指纹的产生机理与惟一性. 东南大学学报（自然科学版）,2009,39(2):230-233. （检索情况：EI）
4. 袁红林, 胡爱群, 陈开志. 无线网络中独立性射频指纹提取方法. 高技术通讯（投稿）.
5. 袁红林, 胡爱群, 等. 数字化射频指纹的可分离性及其影响因素. 电子学报（投稿号：C100814）.
6. 袁红林,胡爱群, 等. 稳健的Wi-Fi 802.11b/g倒谱射频指纹. 应用科学学报（投稿）.
7. Honglin Yuan, Aiqun Hu, etc. Robust intermediate frequency logarithmic spectrum RF fingerprints of BPSK wireless devices. Chinese Journal of Electronics (Submitted No. E110278).

（二）参加的科研项目

1. 江苏省自然科学基金“网络信息安全协议的形式化分析与设计”，BK2006108，2006.8～2008.8，第五，安全协议分析.