学校编码：10384　　分类号_____密级_____
学号：X2006224003　　UDC_____

硕　士　学　位　论　文

基于载波功率谱特征的无线发射机指纹识别研究

The Study on Wireless Transmitter Fingerprint Identification Based on Carrier Power Spectral Features

龙振弘

指导教师姓名：黄联芬副教授
专　业　名　称：通信与信息系统
论文提交日期：2011 年 12 月
论文答辩时间：2012 年　5 月
学位授予日期：2011 年　6 月

答辩委员会主席：

评阅人：_____

2012 年　6 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容）

声明人（签名）：

年　　月　　日

摘 要

随着无线电的迅速发展，认知无线电是目前解决无线频谱利用率低的最佳方案之一。认知无线电网络，相对于传统无线网络，会面临一些新的安全隐患，比如冒充主用户（PUE）信号的攻击等，能否得到广泛应用，它的安全性成为一个重要的因素。无线发射机本振相位噪声具有普遍性、唯一性和短期不变性的特点，可以作为识别发射机的特征，因此基于载波功率谱特征的无线发射机身份识别，在认知无线电应用中具有重要的意义。

本文首先在研究相位噪声基本概念及特征的基础上，对无线发射机的 QPSK 调制信号进行四次方运算去调制，提取带相位噪声的载波。为后续研究提供了大量研究数据。而后在研究信号的功率谱估计和主要成分（PCA）法理论的基础上，对带噪载波的功率谱分别从特征提取和分类识别两个方面进行深入的研究。

一方面，用多项式拟合的方法对带噪载波的单边平滑谱线进行拟合，提取拟合的多项式系数作为带噪载波的功率谱特征，由于平滑后的谱线丢失了许多噪声的细节信息，该方法提取的特征区分度较差。因此本文提出了一种基于主成分分析法的载波功率谱值累积比例特征提取方法，先求出每个频点对应的功率谱值在带噪载波整个功率谱值序列中的比例，所有频点的比例值经累积处理后进行主成分分析，提取出主成分作为带噪载波的功率谱特征。实验结果表明，该方法提取的特征区分度得到了进一步提高。

另一方面，本文设计了 BP 神经网络分类器和 RBF 神经网络分类器，分别输入多项式特征参数和累积比例参数对无线发射机进行分类识别。实验结果表明，BP 神经网络适用于多项式单边谱线拟合法提取的特征数据，平均识别率为 86.67%；RBF 神经网络适用于功率谱值累积比例法提取的特征数据，平均识别率为 99.33%。

由于宽带无线通信迅速发展，今后可针对具有突发数据包的信号发射机进行身份识别，如对各种无线网卡进行识别研究，具有重要创新和理论意义。

关键字： 相位噪声 功率谱估计 主成分分析法 神经网络

Abstract

With the rapid development of radio, Cognitive Radio (CR) is one of the best options for improving the low utilization ratio of spectrum. Compared with the traditional wireless network, CR network is threatened by some new incipient fault, such as PUE (Primary User Emulation) attack, the CR security is the key whether CR could be widely applied. The characteristics of phase noise in local oscillators of the wireless transmitter are universal, uniqueness and short-term invariability. The wireless transmitter fingerprint identification based on carrier power spectral features has an important significance for the application of CR.

In this paper, we use the fourth power computing to erase the modulation from the QPSK modulated signals and intercept the noisy carrier based on deep studies of the concept and characteristics of phase noise, provide large amounts of data for the further study. The further study is on the extraction and identification of the noisy carrier power spectral features based on studies of the main theories of power spectrum estimation and Principal Component Analysis (PCA).

Firstly, this paper adopts a polynomial function to fit the smooth noisy carrier single-sideband power spectral line, and extracts polynomial coefficients as the noisy carrier power spectral features. The features extracted by polynomial fitting method are only small distinction because much noisy detail information has been lost after smoothing the power spectral line. A new method of the noisy carrier power spectral features extracted using cumulative proportion of the noisy carrier power spectral amplitude value based on principal component analysis is proposed. The proportion of every frequency bin in the sequence of the noisy carrier power spectral amplitude values is computed and cumulated. The principal components extracted from the cumulated proportions of all frequency bins using principal component analysis are the noisy carrier power spectral features. Experimental results show that the distinction of features extracted by this method is improved.

Finally, this paper designs a BP neural network classifier and a RBF neural network classifier，and input the polynomial features and the cumulated proportional features into the classifiers to identify the wireless transmitters. Experimental results

show that the BP neural network is applied to the polynomial features，the average identification of different wireless transmitters could achieve 86.67%. The RBF neural network is applied to the cumulated proportional features， the average identification of different wireless transmitters could achieve 99.33%.

Since the rapid development of wide bandwidth radio, the future study on identifying the signal transmitter with burst data, especially the Wireless Local Area Network (WLAN) card. The study has very innovative and theoretical significance.

Key word： phase noise; spectral estimation; PCA; neural network.

目录

Contents

第一章 绪论

1.1 论文的研究背景及意义

1.1.1 认知无线电的背景

目前随着无线通信业务需求的快速增长，可用频谱资源变得越来越稀缺，人们通过采用链路自适应技术、多天线技术等先进的无线通信理论和技术，努力提高频谱利用率。但在同时却发现全球授权频段，尤其是信号传播特性比较好的低频段的频谱利用率极低。据研究表明，在任一时刻，人们所用到的频谱只占所有可用频谱的 2%-6%[1]，因此，频谱并不是真正地匮乏，而是我们需要一种在满足现行授权频谱用户要求的同时，对频谱访问进行智能管理技术，以提高频谱资源的利用率。 为此，MITRE 公司的顾问、瑞典皇家技术学院 Joseph Mitola 博士和 GERALD Q MAGUIRE，JR 教授于 1999 年 8 月在 IEEE Personal Communications 杂志上明确提出了认知无线电的概念 [2]。他认为认知无线电是一种智能无线通信系统，通过实时感知周围的电磁环境，智能地调整通信参数，实现在不影响主用户正常通信的基础上伺机接入空闲频段，动态地利用频谱，从而有效缓解了频谱资源的短缺的问题，解决了目前因固定的频谱分配政策导致的对频谱资源的不合理应用，从而极大地提高了频谱使用率。

近年来，认知无线电已成为无线通信领域研究的热点，国内外的许多研究机构都对认知无线电的理论、实现方式和实际应用展开了广泛的研究，启动了很多重要的研究项目，国外的主要有德国 Karlsruhe 大学的 F. K. Jondral 教授等提出的频谱池系统[3]、美国国防先期研究计划局(Defense Advanced Research Projects Agency， DARPA) 的 XG（NeXt Generation Networks）项目[4]、欧盟的 E2R(End-to-end Reconfigurability)项目等[5]。国内主要的相关项目有厦门大学的厦大-清华-美国高通的国际技术合作项目“认知无线电关键技术”[6]，西安电子科技大学的 863 项目“认知无线电技术研究”[7]，浙江大学的 863 项目“基于认知无线电的多模式自适应调制解调技术研究”和“基于认知无线电的混合波形调制解调技术研究”[8]，以及中国科学技术大学和国防科学技术大学等的相关研究。

1.1.2 认知无线电安全问题的研究背景

由于认知无线电是无线通信的一种，因此它具有传统无线通信的所有安全问题，如无线信号的被截获和篡改、拒绝服务攻击(DOS)、GPS 信息干扰以及路由安全等。此外，由于认知无线电采用开放式的频谱和动态的接入方式，它还将面临一些新的安全隐患，如物理层的模仿主用户信号(Primary User Emulation, PUE)攻击、攻击集中式频谱策略数据库、公共控制信道干扰、自私行为攻击等。因此，随着认知无线电技术的发展，信息安全就成为决定认知无线电是否具有广泛应用前景，特别是在军事无线电和紧急网络中应用的关键。从 2008 年开始出现了研究认知无线电网络安全性的论文[9]，并且认识到安全性的考虑应该贯穿整个协议栈，因为安全性的缺失会破坏技术上的潜在优势[10]。但现阶段对认知无线网络新出现的安全方面的相关研究还比较少，而且大多数无线网络的安全技术都是针对高层的，因此研究认知无线电物理层的安全技术具有重要的学术意义和应用前景。

在认知无线电的通信过程中，认知用户感知到主用户存在时，立即退出该信道防止对主用户干扰。由于现有的频谱知方案是基于能量检测来区分主用户信号和认知用户号,认知用户检测到一个它不能识别的信号时将认为该号来自主用户[11]。这种过于简单的信任模型容易遭 PUE 攻击者的利用，当它检测到一个空闲的频段时，通过在授权频段上发送次用户无法识别的信号来对物理层的频谱感知过程实施干扰，达到冒充主用户的目的，阻止其它认知用户竞争此频段，从而显著减少了合法感知用户的可用信道资源。PUE 攻击根据目的不同可以分为自私 PUE 攻击和恶意 PUE 攻击两种。（1）自私 PUE 攻击。在这种攻击中，攻击者的目标是使自身拥有的频谱资源最大化。当攻击者检测到一个空闲频段时，就会模仿主用户的信号特征发送信号，从而阻止其他的感知用户竞争此频段。（2）恶意 PUE 攻击，攻击者阻止合法认知用户检测和利用授权频段，引起拒绝服务攻击。

对于 PUE 攻击，无论是自私的还是恶意的，对认知无线电网络都有着严重的影响。因此，如何识别主用户的信号和恶意认知用户信号的差别是防范 PUE 攻击的关键所在。基站可以通过授权证书来验证主用户，但是一旦证书丢失，就很难鉴别。

为了对抗 PUE 攻击，RuiLiang Chen 和 Jun-Min Park[12,13]等提出了 LocDef