学校编码：10384　　分类号____密级____
学号：23320061152615　　UDC_____

厦门大学

硕　士　学　位　论　文

认知无线电感知技术的研究

The Study on Sensing Technology for Cognitive Radio

王五妹

指导教师姓名：姚　彦教授
专　业　名　称：通信与信息系统
论文提交日期：2009 年　月
论文答辩时间：2009 年　月
学位授予日期：2009 年　月

答辩委员会主席：_____

评阅人：_____

2009 年 04 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）》。

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

随着软件无线电技术的发展和认知无线电概念的提出，人们已经认识到认知无线电技术是当前技术条件下解决无线频谱利用率低的最佳方案之一。频谱感知技术是认知无线电中最基本和最关键的技术，因此实现快速而准确地搜索可用频谱，为认知无线电其他关键技术的研究奠定坚实的基础。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，比如冒充主用户信号的攻击（PUE攻击）等，一个网络能否得到广泛应用，它的安全性成为一个重要的因素，因此研究认知无线电的安全问题对认知无线电的应用有着重要的意义。

当前存在的几种频谱感知技术，都不能同时兼顾到感知的准确性和有效性。本文的研究内容之一就是对现有频谱感知方法进行改进，将 Wiener 滤波器应用于能量检测算法中，仿真结果表明，在同一个信噪比下，其检测率比原来增加了两倍多，误检率降低了两倍多；另外，将戈泽尔算法应用于循环周期特征检测中，仿真结果表明，在降低算法复杂度的同时，能保证较高的感知精确度，在信噪比接近 3 时就能达到零漏检率，实现了频谱的快搜索和准搜索。

检测 PUE 攻击的常用方法大多数是通过对合法主用户发射机的位置验证来实现的，本文采用将多普勒频差定位和时差定位二者相结合进行定位，使用时差定位估计出目标的运动方向，然后再使用多普勒频差定位技术修正时差定位中估计出的目标位置，进一步提高定位精度。此方法仅适用于发射机位置固定的网络，如 TV 塔网络，且如果一个恶意用户位置非常靠近 TV 塔时，它就可能躲过这样的位置认证，导致漏检。

本文另一个创新点就是将发射机的“指纹”引入认知无线电中，利用发射机的特性参数如相位噪声的普遍性、唯一性和短期永久性，对合法主用户的发射机进行识别，从而抵御 PUE 攻击问题，本文对用户的调制信号进行高次方运算去调制，提取带相位噪声的载波，大量实验结果表明，相位噪声能够作为识别发射机的依据，当相位噪声的特征极细微时，仍然能通过小波分析和高阶统计分析进行识别。此方法不仅可以抵御移动用户的 PUE 攻击，而且对于高级攻击者，如调制方式、信号带宽和信息传输速率等参数跟合法主用户一致的攻击者，有很好的抵御能力，对认知无线电有重要的应用意义。

关键词：频谱感知；位置确认；指纹识别

Abstract

With the development of software radio and the proposed concept of cognitive radio (CR), it is recognized that CR technology is one of the best options for solving the problem of low spectrum utilization. Spectrum sensing is the most basic and critical technology for CR, thus fast and accurate sensing technology lays a solid foundation for other key technologies for cognitive radio. CR network, compared with traditional wireless network, would suffer additional security problems, such as the Primary User Emulation (PUE) attacks. The safety of a network decides whether it can be widely used, therefore, the research on the security of CR network has an important significance for CR application.

The traditional spectrum sensing algorithms are very difficult to have a good tradeoff between accuracy and simplicity. One of the elements of this paper is to improve the existing spectrum sensing technologies. Wiener filter is utilized in the energy detect, the result of simulation shows that for the same Signal to Noise Ratio (SNR), the percentage of detecting (Pd) is increased approximately as twice and the percentage of missed detecting (PMD) decreased more than twice. In additional, we apply the Goertzel algorithm to the cyclostationary feature detector, the result of simulation indicates that it can reduce the complexity as well as guarantying the high sensing accuracy and it is feasible to get nearly zero PMD when the SNR is 3, which makes fast-searching and precise-searching of spectrum come true.

To detect the PUE attackers, the location verification methods for incumbent transmitter have been most commonly used. This paper combines the Time Difference of Arrival (TDOA) and the Frequency Difference of Arrival (FDOA) to position, that is TDOA to estimate the moving direction of the target and the FDOA to amend the position of the target, which improve the positioning accuracy. This method can only be applied in the centralized scenario where the location of incumbent transmitter is static (e.g. TV tower), but not it the distributed networks (e.g. Ad hoc). Moreover, if a malicious user’s location is very near the TV tower, it may avoid such location verification, resulting in a missed detecting.

Another contribution of this paper is to introduce the “fingerprints” of transmitter

to the cognitive radio. We utilize the characteristic parameters of transmitter such as the universality, uniqueness and short-term permanent of the phase noise to do identification for the legitimate transmitters and then resist the PUE attack. In this paper, we use high-power computing to erase the modulation from the received signal and then extract the noisy carrier. A large number of experimental results show that phase noise can be used as the basis for transmitter identification. Moreover, even if the difference of the phase noise is subtle, it still can be identified with wavelet and high-order statistical analysis. This method can not only resist the PUE attack of mobile users, but also for high-level attacks, such as those attacks whose modulation, signal bandwidth and transmitting rate are the same as legitimate user. It has an important significance for CR application.

Key words: Spectrum Sensing; Location Verification; Fingerprint Identification.

目录

第 1 章　绪论 1

1.1 论文的研究背景 1

1.1.1 认知无线电的背景 1

1.1.2 认知无线电安全问题的研究背景 1

1.2 认知无线电的定义和标准化进展 2

1.2.1 什么是认知无线电 2

1.2.2 频谱政策和标准化工作进展 3

1.3 认知无线电关键技术及特点 3

1.3.1 频谱检测 3

1.3.1.1 能量检测 4

1.3.1.2 匹配滤波器检测 4

1.3.1.3 循环周期特征检测 4

1.3.1.4 干扰温度检测 5

1.3.1.5 合作式检测 5

1.3.2 频谱管理 6

1.3.3 功率控制 6

1.3.4 认知无线电安全技术 7

1.4 认知无线电的研究现状和应用前景 8

1.4.1 研究现状 8

1.4.2 认知无线电在 WRAN 中的应用 8

1.4.3 在 ad hoc 网中的应用 9

1.4.5 在 UWB 系统中的应用 10

1.5 本文的研究内容 10

1.6 论文的章节安排 11

第 2 章 认知无线电的频谱感知 12

2.1 频谱感知技术的综述 12

2.1.1 能量检测 13

2.1.2 匹配滤波 16
2.1.3 循环周期特征检测 17
2.2 频谱感知技术中存在的问题及改进方法 21
2.2.1 各种频谱感知技术中存在的问题 21
2.2.2 利用戈泽尔算法改进循环周期特征检测 22
2.2.2.1 戈泽尔算法（Goertzel）的原理 22
2.2.2.2 戈泽尔算法改进循环周期特征检测 25
2.2.3 利用 wiener 滤波器改进能量检测算法 29
2.2.3.1 能量检测模型 29
2.2.3.2 wiener 滤波器算法 30
2.2.3.3 改进的算法流程及仿真结果 30
第 3 章 认知无线电的位置感知 33
3.1 认知无线电的安全问题 33
3.1.1 认知无线电中可能存在的安全问题 33
3.1.1.1 模仿主用户攻击（PUE 攻击） 33
3.1.1.2 干扰主用户 34
3.1.1.3 攻击频谱管理者 34
3.1.1.4 公共控制信道干扰 34
3.1.1.5 自私行为攻击 34
3.1.1.6 拒绝服务攻击 35
3.1.1.7 窃听 35
3.1.1.8 GPS 信息干扰 35
3.1.1.9 路由安全 35
3.1.2 现有的感知方法对 PUE 攻击的脆弱性 35
3.2 位置确认技术 36
3.2.1 DRT 技术 38
3.2.2 DDT 技术 39
3.3 多站时差（TDOA）和多普勒频差（FDOA）的联合定位 42
3.3.1 多站时差定位（TDOA） 42

3.3.2 多普勒频差定位（FDOA）.....43
3.3.3 TDOA 和 FDOA 的联合定位及仿真结果.....44
第四章 认知无线电的指纹感知.....51
4.1 位置确认抵制 PUE 攻击的缺点.....51
4.2 识别发射机的信号“指纹”.....51
4.3 本振相位噪声识别发射机.....52
4.3.1 实验系统.....53
4.3.2 前期实验过程及结果（内本振）.....54
4.3.2.1 载波输入和频谱仪分析.....54
4.3.2.2 载波输入和 PC 机分析.....57
4.3.2.3 调制信号输入和 PC 机分析.....61
4.3.3 中期实验过程及结果（外本振）.....63
4.3.3.1 单频信号输入.....66
4.3.3.2 单频+调频信号输入.....66
4.3.3.3 调制信号输入.....71
4.3.3.4 调制+调频信号输入.....72
第 5 章 结论及展望.....79
5.1 研究工作总结.....79
5.2 未来的研究方向.....79
攻读硕士学位期间的学术论文及参与项目.....81
致谢语.....82
参考文献.....84

Contents

Charpter1 Introduction.....1

1.1 Background 1

1.1.1 Background of Cognitive Radio 1

1.1.2 Background of Security of Cognitive Radio.....1

1.2 Definition and Standardized Progress of Cognitive Radio.....2

1.2.1 Whit is the Cognitive Radio.....2

1.2.2 Spectrum Policy and Standardized Progress.....3

1.3 Key Technologies of Cognitive Radio and its Characteristics 3

1.3.1 Spectrum Sensing.....3

1.3.1.1 Energy Detection 4

1.3.1.2 Matched Filter Detection 4

1.3.1.3 Cyclstationary Feature Detection.....4

1.3.1.4 Interference Temperature Detection.....5

1.3.1.5 Co-operative Detection 5

1.3.2 Spectrum Management 6

1.3.3 Power Control 6

1.3.4 The Security technologies of Cognitive Radio 7

1.4 Research Status and Application Prospects of Cognitive Radio.....8

1.4.1 Research Status 8

1.4.2 Application in WRAN.....8

1.4.3 Application in Ad Hoc 9

1.4.5 Application in UWB System.....10

1.5 Main Contents of Paper.....10

1.6 Framework of Paper.....11

Chapter2 Spectrum Sensing of Cognitive Radio 12

2.1 Summary of Spectrum Sensing Technologies.....12

2.1.1 Energy Detection.....13

2.1.2 Matched Filter Detection 16

2.1.3 Cyclstationary Feature Detection.....17

2.2 Problems of the Current Spectrum Sensing Technologies and the Improving methods.....21

2.2.1 Some Problems of Spectrum Sensing Technologies.....21

2.2.2 Improving Cyclstationary Feature Detection Based on Goertzel Algorithm.....22

2.2.2.1 Principle of Goertzel Algorithm.....22

2.2.2.2 Cyclstationary Feature Detection Based on Goertzel Algorithm 25

2.2.3 Using Wiener Filter to Improve the Energy Detection.....29

2.2.3.1 Model of Energy Detection.....29

2.2.3.2 Principle of Wiener Filter.....30

2.2.3.3 Procedure of the Improving Algorithm and Simulation Results. 30

Charper3 The Location Sensing of Cognitive Radio.....33

3.1 Security Issues of Cognitive Radio.....33

3.1.1 Main Security Issues Exisiting in Cognitive Radio.....33

3.1.1.1 Primary User Emulating（PUE Attack）.....33

3.1.1.2 Interfering the Primary User.....34

3.1.1.3 Attacking the Spectrum Manager.....34

3.1.1.4 Com-controlling Channel Interfered.....34

3.1.1.5 Selfish Behavior Attack.....34

3.1.1.6 Denial Service Attack.....35

3.1.1.7 Eavesdropping.....35

3.1.1.8 GPS Infromation Interfered.....35

3.1.1.9 Routing Security.....35

3.1.2 The Vulnerability of the Existing Spectrum Sensing Technologies to PUE.....35

3.2 Location-Comfirmed Technologies.....36

3.2.1 DRT Technology.....38

3.2.2 DDT Technology.....39

3.3 Joint Position of Time Difference of Arrival (TDOA) and Frequency Difference of Arrival (FDOA) 42

3.3.1 Multi-Station TDOA Position（TDOA） 42

3.3.2 Dopple Frequency Difference Position（FDOA） 43

3.3.3 Joint of TDOA and FDOA and Simulation Results 44

Chapter4 Fingerprint Sensing of Cognitive Radio 51

4.1 The Shortcomings of Location-Comfirmed Technologies Resisting PUE Attack 51

4.2"Fingerprint" for Transmitter Identification 51

4.3 Transmitter Identification Based on Phase Noise 52

4.3.1 Experimental System 53

4.3.2 Pre-term Experimental Procedures and Results (Internal Oscillator） 54

4.3.2.1 Carrier Input and Analysis on Spectrum Analyzer 54

4.3.2.2 Carrier Input and Analysis on PC 57

4.3.2.3 Modulated Signal Input and Analysis on PC 61

4.3.3 Mid-term Experimental Procedures and Rusults (External Oscillator) 63

4.3.3.1 Single-Frequency Signal Input 66

4.3.3.2 Single-Frequency + FM Signal Input 66

4.3.3.3 Modulated Signal Input 71

4.3.3.4 Modulated Signal + FM Input 72

Chapter5 Conclusions and Future Work 79

5.1 Conclusion 79

5.2 Future Work 79

Research Works and Achievements Durint Pursing Master Degree .81

Acknowledgements 82

References 84

第 1 章　绪论

1.1 论文的研究背景

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。随着软件无线电技术的发展和认知无线电概念的提出，人们已经认识到认知无线电技术是当前技术条件下解决无线频谱利用率低的最佳方案之一。认知无线电技术通过无线频谱感知，来有效地利用时间和空间上的空闲频谱资源提供无线通信服务，从而提高无线频谱的利用率，因此频谱感知技术是认知无线电中最基础、最重要的关键技术。

1.1.2 认知无线电安全问题的研究背景

认知无线电作为一种无线通信技术，它也面临传统无线通信的所有安全问题，如无线信号的被截获或篡改等，而认知用户是基于软件无线电架构，具有感知环境变化及调整自身参数的能力。因此认知无线电网络将会面临一些新的安全隐患，比如冒充主用户信号的攻击（PUE）等。随着认知无线电技术的发展，信息安全就成为决定其是否具有广泛应用前景的关键因素，而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。由于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。

当前检测冒充主用户的攻击的方法大多是通过对合法主用户发射机的位置验证来实现。但此方法仅适用于有发射机位置固定的网络，如 TV 塔等；而对于

分布式网络，如 Ad Hoc 网络等，就无法进行准确的位置验证。因此，在各种无线网络场景中，对冒充主用户信号的攻击必须提出新的防御方法。

1.2 认知无线电的定义和标准化进展

1.2.1 什么是认知无线电

认知无线电的概念是由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杂志上明确提出的[2]。他认为认知无线电是一种智能无线通信系统，它可以感知周围通信环境，通过对周围环境变化的学习，自适应地调整内部通信机理，来适应外部环境变化，提高通信的稳定性，提高频谱利用率。认知无线电通过“无线电知识表示语言（RKRL）”提高个人无线业务的灵活性，随后在2000年瑞典皇家科学院举行的博士论文答辩中详细探讨了这一理论[3]。

自从Mitola博士首次提出CR的概念并系统的阐述CR的原理后，不同的机构和学者从不同的角度给出了CR的定义，其中比较有代表性的有FCC（Federal Communications Commission）和Simon Haykin教授的定义。FCC认为“CR是能够基于对工作环境的交互改变发射机参数的无线电[4]”。Simon Haykin教授则认为：“CR是一个智能无线通信系统，它能够感知外界环境，并使用人工智能技术从环境中学习，通过实时改变某些操作参数（比如传输功率、载波频率和调制技术等），使其内部状态适应接收到的无线信号的统计性变化，以达到以下目的：任何时间任何地点的高度可靠通信；对频谱资源的有效利用[5]”

总结上述的定义，认知无线电（Cognitive Radio，CR）作为一种智能的频谱共享技术，能够依靠人工智能的支持，感知无线通信环境，根据一定的学习和决策算法，实时自适应地改变系统工作参数，动态地检测和有效地利用空闲频谱，理论上允许在时间、频率以及空间上进行多维的频谱复用，这将大大降低频谱和宽带限制对无线技术发展的束缚，因此，这一技术被预言为未来最热门的无线技术。