View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Xiamen University Institutional Repository

学校编码：10384　　分类号____密级_____
学　　号：23320091152801　　UDC_____

厦门大学

硕　士　学　位　论　文

基于频率响应的无线信道指纹研究

The Research of Wireless Channel Fingerprint Based on Frequency Response

林文彬

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：2012　年　　月
论文答辩时间：2012　年　　月
学位授予日期：2012　年　　月

答辩委员会主席：_____

评　　阅　　人：_____

2012 年 05 月

厦门大学博硕士论文摘要库

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

厦门大学博硕士论文摘要库

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。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

摘要

高层的安全机制虽然是保证无线通信安全的核心，但是无法解决直接针对无线物理层的攻击。尤其是在认知无线电网络中，因其网络的特殊性，通信过程还会受到模仿主用户（PUE）攻击。

为解决物理层攻击，本文通过射线跟踪算法从物理层提取出信道频率响应作为无线信道指纹。在此基础上，本文采用基于信道频率响应的信道指纹算法，并分析其性能，证明算法的可行性和可靠性。经过训练数据的实验结果表明，基于频率响应的信道指纹算法的识别精度与抽样的频点数量有关，抽样频点越多，不同信道的区分度越高，算法性能就越好。进一步，本文提出信道指纹算法-RSA 数字签名跨层协议，并通过 NS2 仿真软件搭建系统测试平台，对跨层协议的性能进行多方面分析。其中找出并分析影响协议性能的三大影响因子，分别是接收端信噪比、算法门限值、接收数据包比例。通过仿真分析，找到协议性能达到最佳时的影响因子取值。另外，对比 RSA 数字签名安全机制和跨层协议的性能，实验结果表明，使用信道指纹算法-RSA 数字签名跨层协议能很好地识别发射机，也能有效地减小高层安全机制的工作量，节省系统的开销。

本文的主要研究内容和创新点集中在两方面，一是利用射线跟踪算法获取信道频率响应值，二是研究基于频率响应的信道指纹算法，以及分析信道指纹算法-RSA 数字签名跨层安全协议的性能。

在未来的工作中，可以从线上仿真、增加仿真场景和寻求新的影响因子等方面对基于频率响应的无线信道指纹进行更加深入的研究。

关键词：无线信道指纹；频率响应；射线跟踪；RSA 数字签名；跨层协议

厦门大学博硕士论文摘要库

Abstract

Although high-layer security mechanisms are essential to secure wireless networks, these techniques do not directly leverage the unique properties of the wireless domain to address security threats. Especially in cognitive radio network, because of the particularity of its network, communication process will suffer Primary User Emulation (PUE) attacks.

For resisting the physical attacks, this paper uses the ray tracing algorithm to extract channel frequency response from physical layer as wireless channel fingerprint. Smoothly, a channel fingerprint algorithm based on channel frequency response is proposed. This paper analyses the performance of the algorithm, and proves the feasibility and reliability of the algorithm. The experimental results show that, the algorithm identification accuracy is related to the number of sampling frequency points. The more sampling frequency points are, the better the algorithm performance is. Further, the paper proposes cross-layer protocol include channel fingerprint algorithm and RSA digital signature. Based on NS2 simulation software, the paper analyses the cross-layer protocol performance from various aspects. We find and analyze three performance impact factors, the receiving signal-to-noise ratio, the threshold and the proportion of receiving packets. Through simulation analysis, we can get the most value of impact factors. Besides, comparing the performance between the RSA security mechanism and the cross-layer protocol, this paper gets conclusion that this cross-layer protocol can effectively identify transmitters and reduce the workload of high-layer security mechanism to save the cost of the system.

The main contents and innovative points of this paper concentrate in two aspects. The one aspect is using ray tracing algorithm to acquire channel frequency response, the other is researching channel fingerprint algorithm based on frequency response and the performance of the cross-layer protocol.

In the future work, we can research the algorithm deep from other aspects, such as online simulation, increasing the simulation scene and seeking new impact factors.

Key words: Wireless channel fingerprint; Frequency response; Ray tracing; RSA digital signature; Cross-layer protocol

厦门大学博硕士论文摘要库

目录

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

Contents

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

第一章 绪论

1.1 论文的研究背景及意义

当今社会，科技快速发展，人们的生活也随之发生着重大的变化。而通信技术的飞速发展，使得人们对通信的要求越来越高。为了适应社会的需求，无线通信技术已经渗透到了生活的各个角落，成为人们生活不可缺少的一部分。然而，在快速发展的同时，安全问题也日益突出，并且已经成为无线通信最重要的问题之一，保障无线通信的安全已刻不容缓。

尽管已有的上层安全机制日渐成熟，比如加密、摘要、认证、数字签名机制等，而且它们是保障无线网络安全的核心环节，但是这些技术并没有直接解决针对无线环境的网络攻击。在没有协作的情况下，攻击者可以通过模仿合法用户的物理层识别号、无线电信号等对通信过程实施攻击。

认知无线电是一种新型的无线通信技术，其分布式感知协作的特点对未来的无线通信具有重要的意义。已经越来越多的学者进入认知无线电的研究领域，并且取得了一系列进展。但是类似于传统的无线通信网络，在认知无线电网络中，物理层的安全问题仍然未能得到有效地解决，而且由于认知无线电本身的特点，在通信过程中还会受到自私行为攻击和模仿主用户攻击（PUE）等。攻击者在进行 PUE 攻击时，会发送一个模仿主用户的信号来欺骗认知用户，使认知用户退出信道以达到独占此信道的目的。

为了解决无线通信过程中出现的物理层攻击问题，研究人员从物理层的特性中寻求突破点。令人振奋的是，无线通信的一些物理层特性越来越多的被人们发掘出来，并能够用于证明其独特性。物理层特性包括信道特性和发射机本身的特性。发射机本身的特性主要有稳态特性和瞬态特性两种。稳态特性可包括发射机稳定工作时的相位、频率、调制参数等，而瞬态特性主要有发射机的开关过程或因工作模式改变而产生的瞬态信息。已有的研究对发射机本身的特性进行了相关的研究，如发射机的瞬态响应[1]和发射机发送信号的时钟抖动[2]等。

所谓的信道特性，主要是由于无线通信过程中的多径效应产生的。无线信道

厦门大学博硕士论文摘要库

的主要特征是多径传播。多径传播是由于无线传播环境的影响，在电波的传播路径上电波产生了反射、绕射和散射，当电波传输到接收设备的天线时，信号不是单一路径来的，而是许多路径来的多个信号的叠加。因为电波通过各个路径的距离不同，所以各个路径电波到达接收机的时间不同，相位也就不同。不同相位的多个信号在接收端叠加，有时是同相叠加而加强，有时是反相叠加而减弱。这样接收信号的幅度将急剧变化，即产生了所谓的多径衰落[3]。无线信道的多径效应会导致信号衰减、产生误码以及码间干扰等，对通信的准确性产生十分严重的影响。然而从另一方面来说，多径效应造成了不同信道间的非相关性增强，使得利用信道的特性来识别不同的通信过程成为可能。由多径衰落引起的信道特性主要包括信号幅度衰落和时延扩展。在实测过程中，我们可以根据接收端测量的数据反映多径信道的特性，测量数据可以包括接收端的功率、能量、场强、时延、信道响应等。因为信道的特性可以用来识别不同的信道，类似于生活中人的指纹识别个人身份，所以又把信道的特性称为信道指纹。

信道指纹的独特性可以用来识别不同的信道，这也就为无线发射机的识别提供了信道的方法。在无线通信过程中，接收机接收到从不同位置的发射机发送来的信号，接收机与每台发射机之间的信道都不同。根据信道的不同，接收机可以区别不同位置的发射机，从而实现发射机识别的目的。

1.2 信道指纹的研究现状

信道指纹可以包括信道的各类特性，包括功率、能量、场强、时延、信道响应。其中功率、能量、场强、时延这几个参量可以称为信道的一阶指纹特性，信道响应可以称为信道的二阶指纹特性。关于以上信道特性，或多或少有着相关的研究。

1.2.1 一阶指纹特性研究

任何研究都是由简单到复杂、由外在到内含的过程，信道指纹的研究也不例外。最初，为了识别不同的发射机，人们考虑能否利用上层的数据辅助识别。在已有的网络构造下，上层的数据处理起来相对容易一些。因此，人们也考虑利用一些辅助的信号或者序列，来间接的进行指纹识别。比如文献[4]，研究的是一

厦门大学博硕士论文摘要库

种使用嵌入伪随机序列的发射机识别系统。其中，码生成器用来研究 Kasami 序列的自相关和互相关特性。利用这一伪随机序列也能够达到识别发射机的作用。但是添加辅助的信号或者序列进行发射机识别的这一方法，淡化了信号本身的指纹信息。而本文的研究重点是，在不添加其它信息的情况，单纯的利用通信过程中的环境指纹进行发射机的识别。

在无线通信过程中，接收设备能够直接测量出接收信号的能量和功率，即信号的一阶特性，因此研究者最早对接收的能量或者功率进行研究。在文献[5]中，为了防止同频干扰，作者通过 8VSB 信号来进行发射机信号的识别，估计出到达接收端的各个功率的大小，进而识别出来自不同的发射机的信号。

另外，一个室内研究成果体现在[6]中，即利用接收信号强度 RSS（Received Signal Strength）来进行发射机的识别。此文中，作者利用 USRP（Universal Software Radio Peripheral）/GNU Radio 软件无线电平台，设计了一套收发信机，实现了基于接收信号强度 RSS 的无线信道测试系统，并在幅频特性基础上研究无线信道指纹的时不变性以及不同多径环境下信道指纹差异性、空间分辨率、对环境变化的敏感性。测试的结果表明了不同位置信道指纹的差异性。最后，文章对无线信道指纹进行空间多维特性的分析，结果表明随着表征无线信道指纹特性参数 RSS 的增多，信道的识别效果越好，同时测试系统具有较低的误判概率，性能较好。

1.2.2 二阶指纹特性研究

与信道一阶指纹特性相比，二阶指纹特性的识别精度更高。信道的二阶指纹特性主要指信道的冲激响应，利用它能够准确的识别不同的信道，当然也有独特的限制条件。

如今，精确定位室内移动设备的能力在零售、健康服务和娱乐产业都有许多的应用。虽然 GPS 在室内的定位并不准确，但是移动设备的快速增长为室内定位系统的实现提供了机遇。基于环境指纹的方案在室内定位中被广泛的接受和采用。在典型的环境指纹系统中，一般选择若干个测试位置。在线下的测试过程中，独立的定位信号参数（经常使用接收信号强度 RSS）被接收位置的几个 AP 测量得到。测量到的 RSS 值组成一个向量，作为特定位置的环境指纹向量。在线上的测试过程中，只要线上 RSS 值是正确的，有很多方法能够用来估计目的设备

厦门大学博硕士论文摘要库

的位置。但是为了减小硬件开销和干扰，希望能在已经存在的室内无线体系的基础上构造出一个定位系统。在这个定位系统中，少量的 AP 就能提供通信覆盖给一个大的区域。由于每个 AP 仅仅能提供一维的环境指纹向量，那么得到的环境指纹向量可能无法识别位置。为了改善指纹识别的精度，研究人员从二阶指纹方面对发射机识别进行研究，并取得了一定的成果。

比如，在文献[7]中，作者提出一种基于环境指纹的定位方案，这种方案依靠信道脉冲响应（CIR）来定位。接收机进行信道估计，将信道估计值利用傅里叶逆变化估算出 CIR。CIR 的估计值向量的幅度进一步转变成对数模式，以确保估计的 CIR 向量的元素能够对位置估计有效。而位置估计完全是通过非参数核回归（Nonparametric Kernel Regression）的方法得到的。本文的仿真证明了当接入点的数量和训练位置的密度是相同的，该方案在定位精确性方面显示出很好的效果。而且，方案的定位精确度能够适应真实环境中的各种变化，接入点在随机的位置和方向都适用。

在文献[8]中，作者也是利用信道冲激响应来识别设备位置，记录的数据是估计的测量值和建模，它们是关于两个不同的办公大楼的冲激响应的函数。计算出来的数据由信道的12000个冲激响应估计值组成，这些数据是由信道传输函数的反傅里叶变换得到的。文章的仿真分析结果包括：（1）在每个冲激响应估计下的多径信道分量的数量是一个服从正态分布的随机变量，其均值随天线分离的增加而增长。（2）一个改进的泊松分布能够很好的表示多径信道分量的到达时间。（3）振幅在本地和全球区域都服从对数分布，且对数均值随多余延时的增加而线性降低。（4）接收天线进行小的移位不会影响取值，多径分量的幅度值仍是正确的；相关系数是关于天线位置偏移和额外延时的递减函数。（5）相同的冲激响应函数的邻近多径信道分量的幅度几乎是不相关的。（6）在大区域的均方根值（RMS）的时延扩展是正态分布的，且均值随天线分离的增加而增长。每个位置的平均的RMS的时延扩展和平均的路径损耗是线性相关的。

目前最新的指纹研究由文献[9]提出，将信道频率响应值作为指纹特征，利用信道指纹算法识别不同的传输信道，进而识别出不同的发射机。此外，作者还提出将信道指纹算法与高层安全机制结合的协作检测机制，并且分析了这种跨层协作的可行性。

厦门大学博硕士论文摘要库

基于以上指纹特征识别的研究现状，我们确定了本文的研究目标，那就是在无线通信网络尤其是在认知网络中，文献[9]利用指纹特征有效地识别发射机的身份，同时还能够很好地减小高层安全机制的工作量，减小系统的开销。

1.3 章节安排

本文的题目是基于频率响应的无线信道指纹研究，其中主要的研究内容集中在两方面，一是利用射线跟踪算法获取信道频率响应值，二是研究基于频率响应的信道指纹算法，以及分析信道指纹算法-RSA 数字签名跨层安全协议的性能。

第一章介绍了本文的研究背景及意义，分析了国内外无线信道指纹的研究现状和应用前景。

第二章介绍了基于频率响应的无线信道指纹的基本原理，简述了无线通信存在的安全问题以及相应的安全机制，介绍了信道指纹的特征量，阐述了信道指纹算法的原理及其实现过程。

第三章从框架上对基于 NS2 的频率响应信道指纹系统进行设计，分析了无线信道指纹的特性，介绍了系统测试平台以及系统的流程，并对本文使用的射线跟踪算法进行了说明和分析，利用射线跟踪算法求出仿真需要的信道频率响应值。

第四章对基于频率响应的无线信道指纹算法进行了详细的研究，分析了该算法的流程，提出了信道指纹算法-RSA 数字签名跨层安全协议，对算法和跨层协议的性能进行了理论和仿真实验结果的分析，并验证了跨层协议的有效性和准确性。

第五章对全文的工作进行了总结，并对未来的研究工作进行展望。

厦门大学博硕士论文摘要库

第二章 基于频率响应的无线信道指纹基本原理

2.1 无线通信存在的安全问题

无线通信具有灵活多变的优点，与有线通信相比，无线通信的信道不需要硬件连接，且通信双方的位置变化可以更加灵活，成为未来通信的主要形式。无线通信和有线通信就本身和应用而言面临许多相同的信息安全问题，如入侵、病毒攻击等。然而，由于无线通信本身固有的一些特点，使其在信息安全方面有着与有线通信不同的特点[10]。

（1）无线通信没有固定的传输媒质，具有很大的开放性。例如无线局域网中，无线接入点的信号通过定向或者全向天线发向空中，在有效的覆盖范围内，若没有接入控制措施，具有相同接收频率的用户可能同时收到接入点发送的信息，或者通过接入点访问上级网络。因此，无线通信的开放性带来了非法信息截取、未授权信息服务等安全问题。（2）与有线通信相比，无线通信具有移动性。无线终端可在较大范围内移动，还可跨区域漫游，因此，无线通信的移动性带来了新的安全管理问题。（3）无线传输信道是不稳定和随时变化的，无线通信过程中会受到干扰、衰落、多普勒频移、多径等多方面的影响，造成信号质量出现较大的波动，甚至无法进行正常的通信。因此，无线通信的传输信道的不稳定性带来了通信过程的鲁棒性问题。

总的来说，无线通信的安全问题主要包括几个方面。（1）监听攻击：攻击者截取空中的信号，进行分析并获取相关信息。（2）插入攻击：攻击者通过监听获取相关信息，假冒合法用户，再通过无线信道接入信息系统，获得系统的控制权。（3）未授权信息服务：在未经授权的情况下，用户能够享用系统的信息资源。（4）网络鲁棒性：也就是网络的生存能力。它是衡量网络本身对局部破坏或个别设备损坏的容忍能力，或者对信道干扰的抵御能力。（5）移动 IP 安全：它反映了用户终端在某个区域内移动或者跨区域漫游的情况下，管理信息以及用户信息的安全问题。（6）无线干扰：攻击设备通过发射较大功率的同频信号干扰无线信道的正常工作[11]。

厦门大学博硕士论文摘要库

Degree papers are in the “Xiamen University Electronic Theses and Dissertations Database”. Full texts are available in the following ways:
1. If your library is a CALIS member libraries, please log on http://etd.calis.edu.cn/ and submit requests online, or consult the interlibrary loan department in your library.
2. For users of non-CALIS member libraries, please mail to etd@xmu.edu.cn for delivery details.

厦门大学博硕士论文摘要库