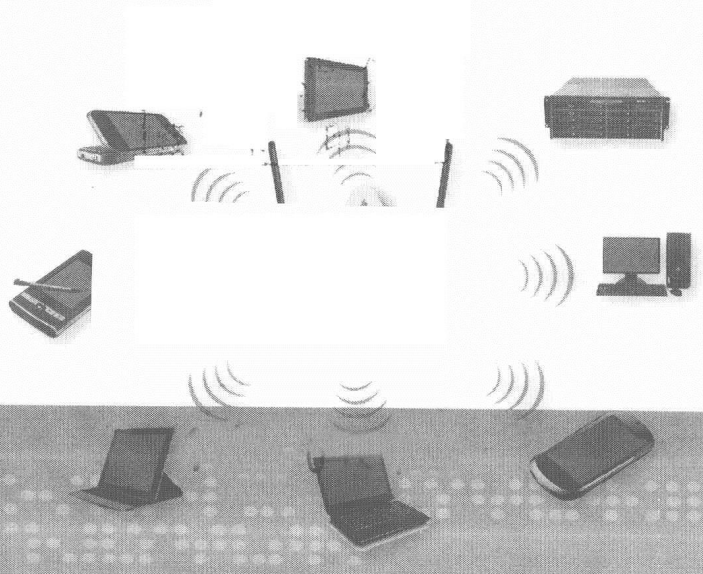
无线网络安全现状及对策研究

徐振华◎著

知识产权出版社
全国百佳图书出版单位

无线网络安全现状及对策研究

徐振华◎著



知识产权出版社
全国百佳图书出版单位

图书在版编目（CIP）数据

无线网络安全现状及对策研究/徐振华著. —北京：知识产权出版社，2016.1
ISBN 978-7-5130-3895-9

Ⅰ.①无… Ⅱ.①徐… Ⅲ.①无线网—安全技术—研究 Ⅳ.①TN92

中国版本图书馆 CIP 数据核字（2015）第 271073 号

内容提要

全书共分六章，分别为无线介质安全特性研究、无线协议安全标准现状研究、无线网络安全需求分析、基于 IEEE 802.1x 的无线局域网安全威胁对策、智能家居网络安全威胁对策、手机移动网络安全威胁对策。本书为读者系统地介绍了无线网络的技术特点，对其面临的安全威胁及安全对策进行了深入探讨，进而为读者深入了解无线网络运行机制提供有效参考。

责任编辑：甄晓玲　　**责任出版：**孙婷婷

封面设计：刘　伟

无线网络安全现状及对策研究

徐振华　著

出版发行：	知识产权出版社有限责任公司	**网　　址：**	http://www.ipph.cn
社　　址：	北京市海淀区马甸南村 1 号	**天猫旗舰店：**	http://zscqcbs.tmall.com
责编电话：	010-82000860 转 8393	**责 编 邮 箱：**	flywinda@163.com
发行电话：	010-82000860 转 8101/8102	**发 行 传 真：**	010-82000893/82005070/82000270
印　　刷：	北京中献拓方科技发展有限公司	**经　　销：**	各大网上书店、新华书店及相关专业书店
开　　本：	787mm×1092mm　1/16	**印　　张：**	11
版　　次：	2016 年 1 月第 1 版	**印　　次：**	2016 年 1 月第 1 次印刷
字　　数：	143 千字	**定　　价：**	32.00 元

ISBN 978-7-5130-3895-9

目　录

1

无线介质安全特性研究

随着社会和经济的发展，网络已经成了人们生活中必不可少的部分，而且人们对网络的依赖程度也越来越高了。近些年随着个人智能终端的迅速普及，人们需要随时随地能够接入信号稳定、传输速度快的网络。无线网络由于其接入的便捷性、工程实施相对简单而越来越受用户喜欢。大到空间通信、无线城市，小到无线社区、智慧家庭网络等都离不开无线网络。

无线网络（wireless network）是采用无线通信技术实现的网络。无线网络既包括允许用户建立远距离无线连接的全球语音和数据网络，也包括近距离无线连接的红外线技术及射频技术。无线网络功能与有线网络十分类似，两者最大的不同在于传输媒介的不同，无线网络利用无线电技术取代了传统的网线或光纤。

利用无线电波在自由空间的传播可以实现多种无线通信。在自由空间传输的电磁波根据频谱可将其分为无线电波、微波、红外线、激光等。数据信息通过编码被加载在电磁波上进行传输，从而实现数据

信息的远距离传输。由于无线电波是在公共空间传播，因此无线传输效率受到环境、频段等多种因素的影响，而且存在无线信号被第三方截获的威胁，其安全性和可靠性有待提升。因此，关注无线网络安全，首先应该关注无线传输介质的特性及其安全性。

1.1 无线电

1.1.1 无线电技术

1. 无线电发展历史

无线电技术是利用无线电波传播信号的技术，早在100多年前，“嘀、嘀、嘀”三声微弱而短促的讯号，通过电波传到2500公里以外的大西洋彼岸，从此向世界宣告了无线电的诞生。在随后的无线电发展中，人们对无线电的研究逐渐深入，无线电被广泛用于通信、导航、雷达、加热、动力、遥距操控、天文学等多个领域。其中无线电在通信领域的应用最为人们熟知，广播、电话、电视、紧急服务（定位）、数据传输等在人们生活中的应用已经非常普遍。随着计算机技术和信息技术的不断发展，各自基于无线传输技术的无线网络也越来越成为人们生活中重要的一部分。

无线电的发展史，在很大程度上就是人们对各波段进行研究、运用的历史。人们对无线电的开发应用大概经历了两个阶段：软件无线电、认知无线电。

（1）软件无线电

软件定义的无线电（Software Defined Radio，SDR）是一种无线电

广播通信技术，它于20世纪90年代初被科学家正式提出，是基于软件定义的无线通信协议而非通过硬连线实现。频带、空中接口协议和功能可通过软件下载和更新来升级，而不用完全更换硬件。

经过几十年的推广和全世界范围的深入研究，软件无线电概念不仅得到了普遍认可，而且已获得广泛应用。近些年，软件无线电的发展已触动无线电工程的每一个角落：从3G到4G，从美军的MBMMR（多频段多模式电台）到JTRS（联合战术无线电系统）都是以软件无线电概念进行设计、开发的，甚至连完成单一功能的GPS也要进行软件化设计，以适应未来导航技术的发展需要。可以这样说，软件无线电的思想已对现代无线电工程的设计和开发产生了重大影响。

（2）认知无线电

认知无线电（Cognitive Radio，CR）是指包含一个智能收发器的一种无线通信技术，它于21世纪初被科学家提出，旨在提升空闲频谱的利用率。认知无线电中的智能收发器能检测出哪些波段未被占用以及哪些波段正在被使用，当检测出某些波段空闲时，CR系统就可以暂时使用该波段进行通信。

认知无线电可以感知周围电磁环境，通过无线电知识描述语言（RKRL）与通信网络进行智能交流，并实时调整传输参数（通信频率、发射功率、调制方式、编码体制等），使通信系统的无线电参数不仅与规则相适应，而且能与环境相匹配，以达到无论何时何地都能实现通信系统的高可靠性和频谱利用的高效性。

软件无线电和认知无线电两者相比，前者关注的是采用软件方式实现无线电系统信号的处理；而后者强调的是无线系统能够感知传播环境的变化，并据此调整系统工作参数，实现最佳适配。从这个意义上讲，认知无线电是更高层次的概念，不仅包括信号处理，还包括根据相应的任务、政策、规则和目标进行推理和规划的高层活动。所以，认知

无线电是智能化的软件无线电。

2. 无线电应用场景

（1）通信领域

无线电最早的应用就是在通信领域，人们可以借助无线电首次远距离传递信息。现代无线通信技术更为发达，空间通信技术日趋成熟。在日常生活中，移动通信已经必不可少。移动通信经历了1G（模拟）、2G（数字）、3G（高速）时代，目前正处于发展4G、探讨5G的时期。从3G时代开始，移动通信真正将人们带入多媒体通信时代，网页、音乐、图片、视频等都可以在智能手机上实现很好的客户体验。

（2）无线局域网

无线局域网络（Wireless Local Area Networks，WLAN）在医疗、企业网络覆盖、仓储管理、餐饮零售、视频监控等方面都有广泛的应用，在日常生活中WiFi（Wireless Fidelity）热点网络的标识更是随处可见。图1-1为WLAN的发展历程。事实上WiFi是WLANA（无线局域网联盟）的一个商标，WiFi是WLAN技术标准中的一个；WiFi的覆盖半径可达300英尺左右（约合90m），WLAN（加天线）则可达到5km。

（3）物联网（智慧家庭）

在信息技术飞速发展的时代，物联网（Internet of things，IoT）呼之欲出，从字面上可以理解为物物相连的网络，通俗地讲就是将所有物体通过网络连接起来，显然如果通过有线网络连接，此情景是不可想象的。物联网用途广泛，遍及智能交通、环境保护、政府工作、公共安全、平安家居、智能消防、工业监测、环境监测、老人护理、个人健康、花卉栽培、水系监测、食品溯源、敌情侦查和情报搜集等多个领域。在当前日常生活中，智慧家庭就是典型的物联网应用之一，其应用前景非常广阔。

图 1－1　WLAN 的发展历程

根据日前由工业和信息化部电信研究院主办的“智慧家庭无线多媒体应用研讨会”公布的数据显示，到 2016 年全球智慧家庭收入将达到 2358 亿美元，中国市场将占 1200 亿元。从业务角度来看，智慧家庭应用可以划分为以下 4 个领域：多媒体娱乐、安全监控、智能家电和医疗照护。

近两年，国家在宏观层面上出台了一系列与智慧城市有关的政策措施，许多政策直接或间接地推动了智慧家庭的进一步发展。如国务院 2013 年 8 月出台的《“宽带中国”战略及实施方案》中明确提出了到 2015 年和 2020 年家庭宽带网络的发展目标，推动了智慧家庭的网络升级。《关于促进信息消费扩大内需的若干意见》中，明确提出“支持数字家庭智能终端研发及产业化，大力推进数字家庭示范应用和数字家庭产业基地建设”。此外，工信部也出台了《数字电视与数字家庭产业“十二五”规划》专项，以推动我国数字家庭产业发展。从上述政策可以看出，我国正从国家层面推动数字家庭/智慧家庭的建设，并将

数字家庭建设作为提高人民群众生活水平、改善人民生活环境、享受优质生活服务的一项重要举措。

1.1.2 无线电频段

无线电波含有迅速振动的磁场。振动的速度就是波的频率，以赫兹（Hz）为单位。1Hz 即每秒振动一下，不同频率的波段用来发射各种不同的信息。无线电的上限频率为 300GHz，不过商业上重要的无线电频段只占其中的一小部分，其他频率超过无线电频率的电磁波有红外线、可见光、紫外线、X 光及伽马射线。光谱分布如图 1－2 所示。

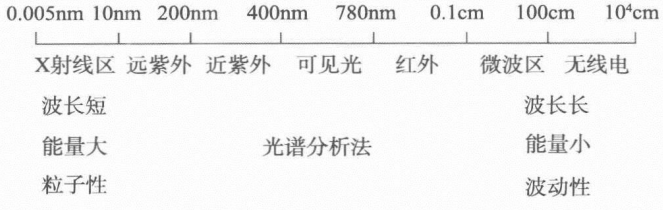


图 1－2 光谱分布

可用无线电波段分布如表 1－1 所示。

表 1－1 可用无线电波段分布

类 别	波 长	频 率
长波	>1000m	30～300kHz
中波	100～1000m	300～3000kHz
短波	10～100m	3～30MHz
超短波	1～10m	30～300MHz
微波	1mm～1m	300MHz～300GHz

将无线电按用途进行分类，主要可分为：民用无线电、商用无线

电、军用无线电。

民用无线电：一般指我们生活中听的无线广播。

商用无线电：机场、通信运营商使用的无线电。

军用无线电：用作军事用途的无线电。

1.1.3　无线局域网

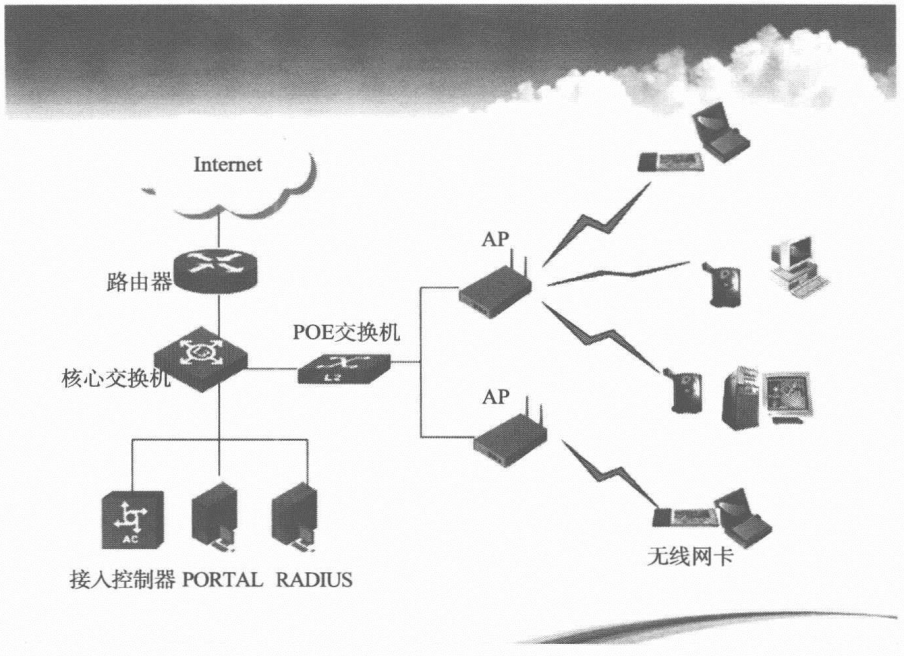


图 1-3　WLAN 组网架构图

1. 前端术语

（1）无线热点（Hotpoint）

无线热点指通过无线接入点为移动用户提供联网或互联网服务的区域。公共热点一般建立在图书馆、机场、酒店、咖啡厅和餐馆等室

内环境中。

（2）无线接入点

无线接入点（AccessPoint，AP），一般有胖 AP 与瘦 AP 两种形式。

（3）服务集合标识符

服务集合标识符（Service Set Identifier，SSID）又称网络名称，是 AP 独一无二的标识字符，每个 AP 必须配置一个 SSID。

（4）信道与频段

信道是对无线通信中发送端和接收端之间的通路的一种形象比喻，对于无线电波而言，它从发送端传送到接收端，其间并没有一个有形的连接，它的传播路径也可能不只一条，但是为了形象地描述发送端与接收端之间的工作，可以想象两者之间存在一个看不见的道路衔接，我们把这条衔接通路称为信道。信道具有一定的频率带宽，正如公路有一定的宽度一样，该频率我们称之为频段。

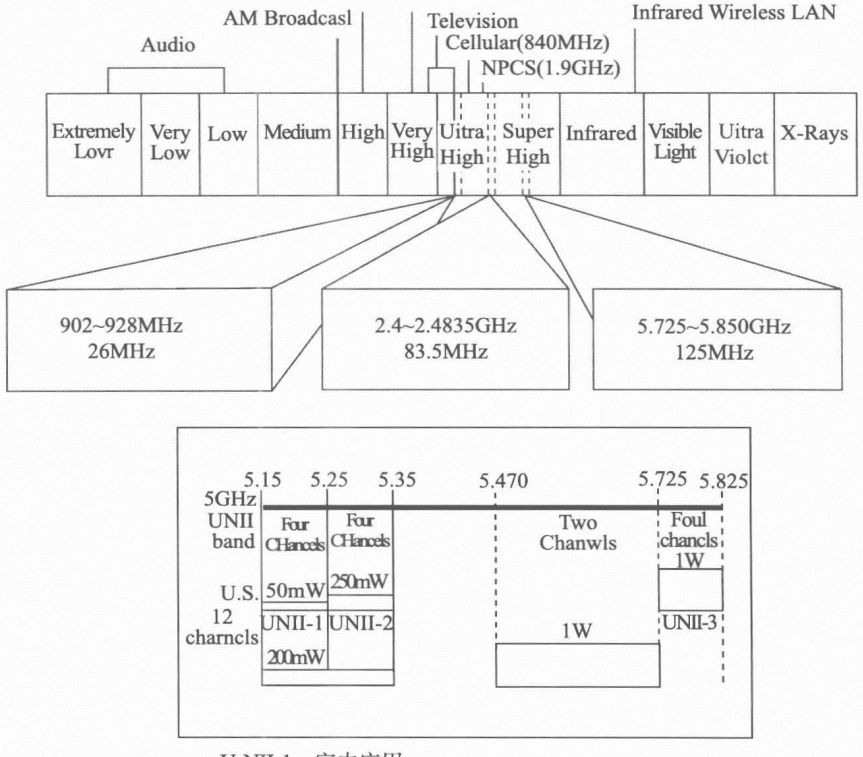
ISM（Industrial Scientific Medical）频段（其分布如图 1－4 所示）是一个免许可证的可用于消费电子产品的频段，由美国联邦通信委员会（FCC）分配，设备功率不超过 1W。ISM 频段主要是开放给工业（902～928MHz）、科学研究（2.42～2.4835GHz）和医疗（5.725～5.850GHz）三类机构使用。目前，主流的无线局域网标准由 IEEE（美国电气和电子工程师协会）所制定，在 IEEE 802.11 协议组中，主要采取后两种 ISM 频段。无线局域网的信道特点如表 1－2 所示。

表 1－2　无线局域网信道特点

频率	频段	特　点
2.4G	2.4～2.4835GHz	每个信道宽度为 22MHz； 相邻信道的中心频点间隔 5MHz； 相邻的多个信道存在频率重叠（如 1 信道与 2、3、4、5 信道有频率重叠）； 整个频段内只有 3 个（1、6、11）互不干扰信道

续表

频率	频段	特　点
5.8G	5.725～5.850MHz	5.8G 频段的频率范围为 5.725～5.850GHz，共 125M 带宽；该频段划分为 5 个信道，每个信道为 20MHz 带宽。各信道互不交叠。中心频率 = 5000 + n * 5（MHz）n = 149、153、157、161、165； IEEE 802.11a/n 标准均可在 5.8GHz 工作



U-NII-1：室内应用

U-NII-2：室内或短距离室外应用，如校园网

U-NII-3：长距离室外应用，点对链路

图 1－4　ISM 频段分布

2. 传输术语——IEEE 802.11 无线协议组

IEEE 802.11 协议组是 IEEE 为无线局域网络制定的标准。IEEE 802.11 协议是 IEEE 最初制定的一个无线局域网标准，主要用于小型局域网中用户与用户终端的无线接入，业务主要限于数据存取，速率最高只能达到2Mbit/s。由于它在速率和传输距离安全性上都不能满足人们的需要，因此，IEEE 小组又相继推出其他若干项标准，如表 1－3 所示。

表 1－3　IEEE 802.11 协议组主要协议

协议	发布日期	频带	最大传输速率
IEEE 802.11	1997 年	2.4～2.5GHz	2Mbit/s
IEEE 802.11a	1999 年	5.15～5.35GHz/5.47～5.725GHz/5.725～5.875GHz	54Mbit/s
IEEE 802.11b	1999 年	2.4～2.5GHz	11Mbit/s
IEEE 802.11g	2003 年	2.4～2.5GHz	54Mbit/s
IEEE 802.11n	2009 年	2.4GHz 或者 5GHz	600Mbit/s（40MHz＊4MIMO）
IEEE 802.11ac	2011 年 11 月（草案）	2.4GHz 或者 5Hz	867Mbit/s，173Gbit/s，3.47Gbit/s，6.93Gbit/s（8MIMO，160MHz）
IEEE 802.11ad	2012 年 12 月（草案）	60GHz	高达 7000Mbit/s

3. 硬件设备

（1）无线网卡

无线网卡（如图 1－5 所示）按照接口的不同可以分为多种：

① 一种是台式机专用的 PCI 接口无线网卡。

② 一种是笔记本电脑专用的 PCMCIA 接口网卡。

③ 一种是 USB 无线网卡，这种网卡不管是台式机用户还是笔记本用户，只要安装了驱动程序，都可以使用。