课程 | 实验

教育部产学合作协同育人项目成果教材
西普教育研究院IT前沿技术方向高校系列教材

无线网络安全及实践

在线实验+在线测试

主　编　冯光升　林雪纲　吕宏武
副主编　林俊宇　刘春利　孙东岳
　　赵　倩　李冰洋　邹世辰

- 内容新颖，可操作性强，层层深入，简明易懂。
- 从实用角度出发，重点培养学生动手解决问题的能力。
- 提供体系完整的100学时在线实验，即学即练，书网结合。
- 108个案例实战（课程配套案例48个、扩展案例60个），附赠案例源代码、视频等资源。

实验吧
让实验更简单

开放实验云平台

HEUP 哈爾濱工程大學出版社

无线网络安全及实践

主　编　冯光升　林雪纲　吕宏武
副主编　林俊宇　刘春利　孙东岳
　　赵　倩　李冰洋　邹世辰

HEUP 哈尔滨工程大学出版社

内容简介

本书是针对目前信息安全专业及相关专业本科生而编写的无线网络安全理论及实验教材，内容涵盖了本书实验所需要的基础知识、实验工具和实践技能。基础知识方面涉及无线局域网、无线个域网、无线城域网、无线体域网等主流无线网络的核心协议及安全机制；实验方面注重从 Wi-Fi 破解及防护、入侵检测、移动终端安全等角度提高学生的实践能力。此外，本书专门安排一章内容对当前的研究热点即无线路由安全进行了讲解。

本书内容丰富，实用性强，可作为信息安全专业的本科生的理论及实验教材，也可以作为网络安全及保密培训的参考书和培训教材。

图书在版编目(CIP)数据

无线网络安全及实践 / 冯光升，林雪纲，吕宏武主编. —哈尔滨：哈尔滨工程大学出版社，2017.12
ISBN 978-7-5661-1775-5

Ⅰ. ①无… Ⅱ. ①冯… ②林… ③吕… 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(2017)第 313434 号

选题策划 张淑娜
责任编辑 王洪菲
封面设计 博鑫设计 秦延新

出版发行 哈尔滨工程大学出版社
社　　址 哈尔滨市南岗区东大直街 124 号
邮政编码 150001
发行电话 0451-82519328
传　　真 0451-82519699
经　　销 新华书店
印　　刷 北京中石油彩色印刷有限责任公司
开　　本 787 mm×1 092 mm 1/16
印　　张 24.5
字　　数 641 千字
版　　次 2017 年 12 月第 1 版
印　　次 2017 年 12 月第 1 次印刷
定　　价 75.80 元
http://www.hrbeupress.com
E-mail:heupress@hrbeu.edu.cn

前　言

随着无线网络服务的应用和普及，无线网络安全形势越发不容乐观，相关的安全事件层出不穷，已经成为安全领域的重灾区，培养无线网络安全领域的专业人才更是迫在眉睫。因此，编者结合多年从事无线网络安全理论与实验教学的经验，在与北京西普阳光教育科技股份有限公司的紧密合作下，通过研读现有资料和文献，最终整理和编写成本书。

在内容编排上，本书力求兼顾和满足信息安全专业、计算机科学与技术专业和其他相关专业对无线网络安全理论及实践能力的要求。本书理论部分（第 1 ~ 5 章）首先对无线网络基础知识进行概述，然后对与安全隐患和安全保护相关的技术环节进行了讲解；实验内容部分（第 6 ~ 12 章）实验难度逐步增加，由易到难，符合学生学习的基本规律，易于上手。随着实验的进行，学生在提高动手实践能力的同时，对无线网络安全的基本理论知识也达到融会贯通，从而形成较为完整的无线网络安全理论与实践体系。此外，由北京西普阳光教育科技股份有限公司开发的在线教育平台——实验吧（www. shiyanbar. com），提供了强大的集成实验环境及丰富的在线教学资源，把本书配套的实验搬到线上，读者可以更方便地结合本书动手实践。

本书共 12 章内容。第 1 章对无线网络的入门知识进行了阐述，包括无线局域网、无线个域网、无线城域网和无线体域网，进而对无线网络安全的相关概念和发展趋势做概要性阐述，激发学生对无线网络及安全防护的学习兴趣。第 2 章到第 4 章，通过对各种无线网络核心协议及安全机制的详细阐述，使学生初步掌握无线网络基础知识和安全防护基本技术，形成无线网络安全防护的知识体系。无线网络路由安全问题是近年来的研究热点和难点，第 5 章对这一领域的安全隐患和防护机制进行了专门探讨，作为入门书籍，希望能够启发学生开展更为深入的研究。第 6 章到第 8 章从实践角度对 Wi-Fi 破解及防护问题进行了由浅入深地分类阐述，涵盖目前主流工具、主流方法的应用。第 9 章讲述了无线网络中主要的入侵检测实验方法，培养学生具备应用入侵检测工具的能力，并能够洞悉入侵检测原理，为深入研究入侵检测方法奠定基础。第 10 章到第 12 章阐述了移动终端侧的安全问题及实验方法，从 ADT 及反编译工具的使用到数据存储，再到 App 安全加固，对于学生形成较为全面的移动终端侧安全分析及防护能力具有重要的作用。

本书适合大中专院校信息安全专业及相关专业的本科生作为教材或者参考书使用，同时对从事无线网络安全技术和管理等相关领域工作的人员具有一定的参考价值。

特别感谢黑龙江省新一代网络技术与信息保障重点实验室中的邹世辰、谭静、吕海滨、夏富民、李腾、赵雅欣、孙嘉钰、王伟平、赵世昭、刘凯等同学在本书的整理工作及实验验证工作中给予的极大支持；特别感谢哈尔滨商业大学的赵倩副教授负责了本书理论部分约 10 万字书稿的撰写和校对工作；特别感谢哈尔滨商业大学的李云负责了本书理论和实践部分

6万字的撰写和校对工作;更特别感谢王慧强教授在本书编写过程中给予的重要指导。同时,本书的编写受到中央高校基本科研业务费(HEUCF170602)、黑龙江省自然科学基金(F2016028,F2016009,F2015029)、国家自然科学基金(61502118,61402127)等项目的支持。

限于编者的学术水平,错误与不妥之处在所难免,敬请读者批评指正。

编　者

2017年8月

目　　录

第 1 章　无线网络概述

相比有线网络，无线网络结构灵活，应用丰富，但安全性问题也更加突出。按照覆盖范围分类，无线网络结构可划分为：无线个域网（小于 10 m）、无线局域网（10 m 至几千米）和无线城域网（1 km 至 50 km）。当然，由于分类标准的差别，较小的无线个域网（例如小于 2 m）也被称为无线体域网，而大于 50 km 的无线城域网也被称为无线广域网。这几种常见无线网络的通信范围如图 1.1 所示。

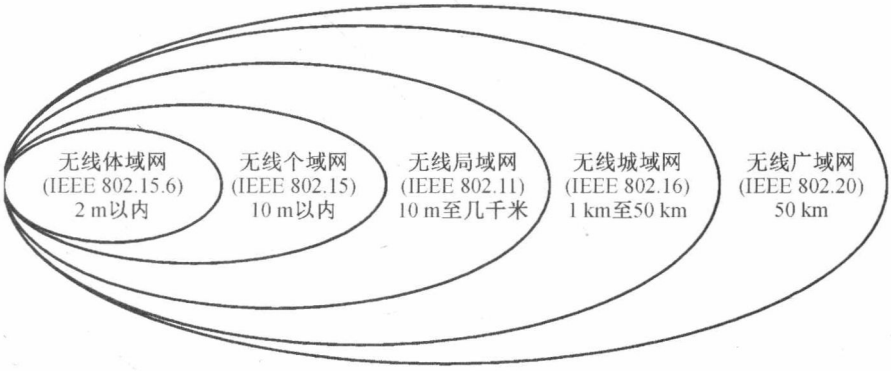

图 1.1　常见无线网络的通信范围

本书的内容采用无线个域网、无线局域网和无线城域网这种分类方式。为了便于了解无线个域网的最新应用，在本章也对无线体域网这一应用形态进行了阐述。通过对各种无线网络的基本概念、特点、应用形态及发展趋势进行论述分析，以及对无线网络所面临的安全威胁和所采用的防御技术进行介绍，使读者在学习无线网络知识之后能对其安全问题有初步的了解。

1.1　无线局域网概述

在无线局域网发明之前，人们通常采用有线网络进行通信，这种有线网络可以由双绞线或光纤相互连接构成。然而网络规模增加之后，这种有线网络无论是组建、拆装还是重新布局和改建都极其困难，代价高昂。在此背景下，无线局域网的组网方式应运而生。

1.1.1　无线局域网基本概念

无线局域网（Wireless Local Area Network，WLAN）是计算机网络与无线通信技术相结合的产物，通常指采用无线传输介质的计算机局域网。从连通角度，WLAN 通过射频技术来实现计算机之间的对等或点对点连通性的数据通信。从技术角度，WLAN 利用无线多址信

道和宽带调制技术来提供统一的物理层平台，以此来支持节点间的数据通信，其为通信的移动化、个性化和多媒体应用提供可能。

WLAN 技术具有传统有线局域网无法比拟的灵活性。WLAN 的通信范围受环境制约较小，但覆盖范围有限。距离的差异使数据传输的性能不同，导致网络具体设计和实现有所区别。WLAN 能在几十到几千米范围内支持较高数据率，可采用微蜂窝（Microcell）、微微蜂窝（Picocell）或非蜂窝（Ad Hoc）结构。图 1.2 是典型 WLAN 集成部署示意图。

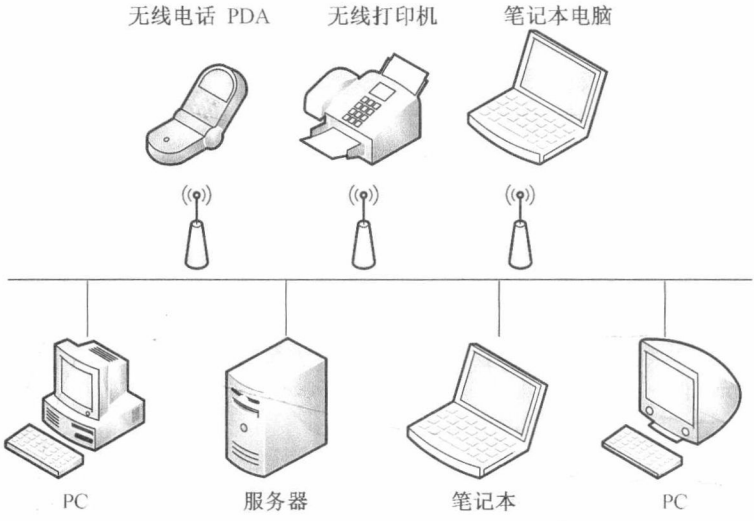

图 1.2　典型 WLAN 集成部署示意图

1.1.2　无线局域网的特点

1. 无线局域网的优点

WLAN 是在有线局域网的基础上发展而来的，主要特点如下：

（1）移动性。网络和主机迁移方便。通信范围不再受线路环境的限制，扩大了覆盖范围，为便携式设备提供有效的网络接入功能，可随时随地连接到网络。

（2）灵活性。简单方便，组网灵活，可将网络延伸到线缆无法连接的地方。

（3）可伸缩性。无线局域网有多种配置方式，可以很快从只有几个用户的小型局域网扩展到上千用户的大型网络，放置或添加接入点（Access Point，AP）或扩展点（Extend Point，EP），可扩展组网。

（4）经济性。可用于难以物理布线的环境，节省线缆、附件和人工费用，同时省去布线工序，能快速组网、快速投入使用，其成本效益显著。可低成本快速组建临时性网络。对需频繁布线或更换地点的场合，费用节约更明显。

（5）故障定位容易。有线网络一旦出现物理故障，尤其是由于线路连接不良而造成的网络中断，往往很难查明，而且检修线路成本较高。无线网络则很容易定位故障，只需更换故障设备即可恢复网络连接。

2. 无线局域网的局限性

WLAN 尽管有很多优点，但也有一些不足，具体如下：

(1)可靠性。传统局域网的信道误码率小于 10^{-9},可靠性和稳定性极高。而 WLAN 的无线信道并不十分可靠,各种干扰和噪音会引起信号衰落和误码,进而导致吞吐性能下降和不稳定。此外,无线传输的特殊性还会产生“隐藏节点”“暴露节点”等现象。

(2)兼容性与共存性。WLAN 要兼容有线局域网、现有网络操作系统和网络软件;同时,多种 WLAN 标准须互相兼容,不同厂家的无线设备也需兼容。共存性包括:同一频段的不同制式或标准共存,如 2.4 GHz 的 IEEE 802.11 和蓝牙系统共存;不同频段、不同制式或不同标准共存,如 2.4 GHz 和 5 GHz 的 WLAN 共存。

(3)带宽与系统容量。由于频率资源匮乏,WLAN 的信道带宽远小于有线网络带宽。即使进行复用,其系统容量通常也小于有线网络。

(4)安全性。包括两方面:一是信息安全,即信息传输的可靠性、保密性、合法性和不可篡改性等;二是人员安全,即电磁波辐射对人体的影响。不同于有线封闭信道,WLAN 中无线电波可能遭受窃听和恶意干扰。此外,WLAN 系统也会存在一些安全漏洞。

1.1.3　无线局域网的应用

1. 在医疗中的应用

目前,在医疗中无线局域网主要应用于对医疗垃圾的处理和对药物的跟踪等方面。因为医疗垃圾具有较大的危害性,处理上有更严格的要求。通过无线局域网可以实现实时监控,保证医疗垃圾的合法合规处理。对于药物的来源以及去向也可以通过无线局域网实现实时监控。此外,通过无线局域网还可以实现远程医疗、远程患者数据管理,为患者提供更优质的医疗服务,为社会提供全面的医疗救助。

2. 在军事上的应用

在现代作战信息通信技术上,通过无线局域网可实现作战实时通信,现代无线局域网通信技术的优势特征明显,其通信宽带大、架设简单且适用范围广,这些优势被应用到军事中将给军事作战带来更便捷、更先进的技术支持。

3. 在铁路通信中的应用

一般情况下,借助车地无线通信技术以及电视监视系统,在控制中心可随时调取在线列车车载摄像头拍摄的实时监控图像、视频,也可以通过信息系统向列车传发高清的视频节目或者特定信息。

4. 在其他服务行业中的应用

餐饮服务业使用无线局域网络产品,可以直接从餐桌输入并传送客人点菜单的内容。在大型会议和展览等临时场合,无线局域网可使工作人员在极短时间内,便捷地得到网络服务,以获得所需信息。酒店采用无线局域网,可以随时随地为顾客提供及时周到的服务。在办公环境中使用无线局域网,可以使办公用计算机具有移动办公能力,方便快捷。

1.2　无线个域网概述

人们在享受使用一系列电子产品带来方便的过程中,也逐渐感觉到电子产品功能的局限性。例如,随着外围设备的逐渐增多,用户不仅在自己的计算机上连接打印机、扫描仪、调制解调器等外围设备,还会使用 USB 接口传输数据,频繁地插拔某一接口,在计算机上缠

绕各种无序的接线，杂乱的布线影响用户体验。因此，人们希望能有一种短距离、低成本、小功耗的无线通信方式以实现不同设备的互联，于是产生了无线个域网（Wireless Personal Area Network，WPAN）。

1.2.1 无线个域网基本概念

无线个域网是指在个人工作的地方，把属于个人使用的电子设备通过无线技术连接起来的自组网络，无须接入点 AP，其覆盖范围在 10 m 左右。这些电子设备可以包括便携式电脑、打印机和蜂窝电话等，它们可以很方便地进行通信，就像使用普通电缆连接一样。

WPAN 设备具有价格低、体积小、易操作和功耗低等优点，将取代线缆成为连接移动电话、笔记本电脑和掌上设备等各类便携设备的工具。WPAN 可以实现随时随地为用户提供设备间的无缝通信，并使用户能够通过移动电话、局域网或广域网的接入点接入互联网。这种专用网络最重要的特征是采用动态拓扑结构以适应网络节点的移动性，其优点有按需建网、容错性高、连接不受限制等。因此，WPAN 有巨大的市场潜力，既可以与大范围快速移动情况下的通信应用相辅相成，又可在小范围内实现各种移动通信设备、固定通信设备，甚至各种家用电器之间的互联，而且其价格更为低廉，市场潜力巨大。

1.2.2 无线个域网的分类

无线个域网的应用范围广泛，WPAN 被定位于短距离无线通信技术，但根据不同的应用场合又分为低速 WPAN（LR-WPAN）、高速 WPAN（HR-WPAN）和超高速 WPAN 技术。

1. 低速 WPAN

低速 WPAN 是按照 IEEE 802.15.4 协议标准，为近距离联网而设计的，包括工业监控和组网、办公和家庭自动化与控制、库存管理、人机接口装置，以及无线传感器网络等。LR-WPAN 的出现完全是由于市场需要，与 WLAN 和其他 WPAN 相比，LR-WPAN 具有结构简单、数据率较低、通信距离近、功耗低和成本低等优点。

在家庭、工厂与仓库自动化控制中，安全监视、保健监视、环境监视、军事行动、消防队员操作指挥、货单自动更新、库存实时跟踪，以及在游戏和互动式玩具等方面都可以开展应用。

2. 高速 WLAN

高速 WLAN 是按照 IEEE 802.15.3 标准建立的，其数据传输速率高达 55 Mb/s。高速 WLAN 适用于多媒体文件、视频流和 MP3 等音、视频文件的传送，并在提供的带宽内确保一定的服务质量（Quality of Service，QoS）。例如，传送一幅图片，高速 WLAN 只需 1 s。

3. 超高速 WPAN

在日常生活中，对内容传送的更高速率的需求与日俱增。为此，IEEE 802.15.3a 工作组提出了更高速率的物理层标准，用以替代高速物理层，从而构成超高速 WPAN 或超宽带（Ultra Wide Band，UWB）WPAN，可支持 110 ~ 480 Mb/s 的数据率。

1.2.3 无线个域网的应用

WPAN 是随着短距离无线移动网络技术的发展而产生的，能够近距离为设备建立连接，而且 WPAN 设备是运动的，这意味着 WPAN 的技术标准应该具有良好的操作性，无论是

在汽车、轮船或飞机中，都能在传送语音和数据时不受干扰。最初的时候，这个领域主要涉及三个标准技术：红外技术（IrDA）、家庭射频（HomeRF）和蓝牙（Bluetooth）。

1. IrDA 技术

IrDA 技术是一种利用红外线进行点对点通信的技术。目前，全世界约有 5 000 万台设备采用 IrDA 技术，在成本上，红外线 LED 及接收器等组件比一般 RF（Radio Frequency）组件便宜，只是蓝牙产品的 1/10，因而 IrDA 技术得以普及应用。对于传输速率高、使用次数少、移动范围小、价格比较低的设备（如打印机、扫描仪、数码相机等），IrDA 技术是首选。

2. HomeRF 技术

HomeRF 技术是无绳电话技术（Digital Enhanced Cordless Telecommunications，DECT）与无线局域网技术融合发展的产物。HomeRF 无线家庭网络可以支持家庭娱乐、家居控制等，由于无线家庭网络通过与公用电话交换网（Public Switched Telephone Network，PSTN）和以太网进行无缝通信，是家庭范围内数据交换网络的重要组成部分。

3. 蓝牙技术

蓝牙技术能够提供低成本、低功耗的短距离无线通信，具有广阔的应用前景。蓝牙的可靠性和安全性标准，在一定程度上既可以保证通信双方身份的可靠性，又能保证通信数据的安全性，在电子商务领域拥有巨大的应用前景。

4. 超带宽技术

超带宽是一种基于 IEEE 802. 15. 3 标准的超高速、短距离无线接入技术。它在较宽的频谱上传送极低功率的信号，在约 10 m 范围内实现数百兆比特每秒的数据传输速率，此外，还具有抗干扰性能强、传输速率高、带宽极宽、能耗低、保密性好、发送功率小等诸多优势。

5. ZigBee 技术

ZigBee 是一种基于 IEEE 802. 15. 4 标准的新兴短距离、低功耗、低速率的无线接入技术，是一种关于组网、安全和应用软件等方面的技术标准。ZigBee 工作在 2. 4 GHz 频段，共有 27 个无线信道，数据传输速率为 20 ~ 250 kb/s，传输距离为 10 ~ 75 m。

6. 射频识别技术（Radio Frequency Identification，RFID）

RFID 俗称电子标签，是一种非接触式的自动化识别技术，通过射频信号自动识别目标对象并获得相关数据。RFID 由标签、读写器和数据管理系统 3 个基本要素组成，可广泛地用于物流业、交通运输和医药等领域。随着物联网技术的发展，RFID 已成为通信网络不可或缺的部分。

7. 近距离无线通信技术（Near-Field Communication，NFC）

由飞利浦公司和索尼公司共同开发的 NFC 是一种非接触式识别和互联技术，可以在移动设备、消费类电子产品、PC 和智能控件工具之间进行近距离无线通信。使用双方只需互相接近就可以完成信息交换、访问和获得服务。NFC 提供了一种简单、触控式的解决方案，可以让消费者简单直观地交换信息、访问内容与获得服务。目前，NFC 已广泛地应用于电子商务快捷支付、短距离数据传输等领域。

1.2.4　无线个域网发展趋势

过去，WPAN 技术得到了飞速的发展，蓝牙、UWB、ZigBee、RFID 等各种技术先后出现，在功耗、成本、传输速率、传输距离、组网能力等方面各有所长，但还未实现大规模的商业应用。在当前标准林立的短距离无线通信市场，还有许多的诸如标准化等问题亟待解决。

到目前为止,各种无线个域网技术虽然已经取得了长足进步,但是要获得商业上的成功,还应从技术和应用两方面改进。在技术方面:要进一步提高系统的传输速率和吞吐量;在保证 QoS 的前提下提高频谱利用率和系统容量;改善功率控制功能,延长个人设备的电池使用寿命;进一步增强系统的安全性;采用智能的无线资源管理技术满足不同的服务请求。在应用方面:要进一步降低市场价格,使设备更加容易安装、使用和维护。

总之,随着无线个域网技术的不断发展,以及不断地和其他类型无线网络融合与互补,无线个域网将在全球范围内获得极为广泛的应用,取代线缆连接各种个人用户设备,给人们的生活带来便利。

1.3 无线城域网概述

无线城域网(Wireless Metropolitan Area Network,WMAN)能够提供更大的传输范围和更快的传输速率,是城市无线接入的一种新型手段。随着互联网的不断普及和发展,人们对于网络带宽、通信距离和覆盖范围的要求越来越高。目前,众多无线通信技术存在接入速率太低、覆盖范围太小和移动速度慢等缺陷,无线城域网的出现打破了这种局面。

1.3.1 无线城域网基本概念

无线城域网是以电磁波作为传输介质的一种网络传输形式,在数据传输速度方面与有线网络相比有着明显的优势。现阶段,城域网无线网络传输速度已经能够达到 300 Mb/s,个别网络数据通信速度要求较高的区域,其传输速度甚至达到 450 Mb/s,能够实现 2 km 以内的高效传输,是城际网络通信的关键技术,改善了有线网络数据传输速率有限、线路维护工作量大的情况。而未来采用 5G 通信技术的无线传输峰值速率甚至能够达到数十吉比特,将极大改变通信网络的数据传输条件,并促进现有的网络应用形态的变革。

1.3.2 无线城域网的特点

1. 无线城域网传输速度快,传播距离远

典型无线城域网关键技术包含 OFDM 技术、自适应编码技术等,它们的作用是提高系统发射功率和信道利用率,其网络覆盖范围广可达 50 km,而数据传输速率最高可达 70 Mb/s,比无线局域网具有更大的覆盖范围优势。

2. 优良的最后一千米接入性能

无线城域网接入方式广,不仅是有线接入方式的无线拓展,还可以将 Wi-Fi 热点接入互联网中,只是热点必须在网络覆盖范围内。也就是说,无线城域网解决了最后一千米的宽带接入问题,能够通过网络直接进行通信和信息传递,无须有线通信线路,提高了运行效率。

3. 多媒体服务广泛多样

相比于传统的服务,城域网通过无线连接的方式与电信级别的服务相结合,而电信的 QoS 系统完善,加之先进的技术基础及服务,其安全性高,服务范围广,形式类别多样,从而达到对不同层次客户的多样的多媒体服务需求。

4. 性价比较高

与传统的无线通信服务比较，无论是安全性还是灵活性都有较大程度的提高，同时兼容性也有一定程度的提升。

1.3.3　无线城域网应用

全球互通微波存取（Worldwide Interoperability for Microwave Access，WiMax）被定义为无线城域网解决方案。WiMax 技术应用广泛，大致可以分为固定接入应用、游离式接入应用、全移动接入应用和便携式接入应用四个方面。特别是在政府公共事业中的应用非常突出，并且将成为 IPTV 无线到户的另一种选择。

1. 城市安全

在“911 事件”以后，城市安全已经成为国际上的首要问题。在美国，很多的城市与州政府、防恐单位开始进行密切合作，不同政府职能部门的信息可以互通互联，以保证市民的公共安全。通过 WiMax 无缝漫游技术，建立高安全性的警察专用网，警察局可以及时有效地查找违法犯罪人员并监控其活动情况。同时，WiMax 无线宽带技术可以提升城市对紧急事件的处理能力，有效地提升城市整体安全防范水平。

2. 森林防火

无线联网甚至可以应用在森林防火方面。目前 IBM 已经帮助消防部门开发了一套森林防火系统。当前，该系统是通过卫星链路保证火场中的数据通信，传输时延较高；可以想象未来通过 WiMax 新型系统，城市安全方面的信息，其沟通和传达将以更有效、更快速和覆盖更广的方式进行。

3. 监控交通状况

城市中的交通拥堵以及衍生的环境污染问题已经是世界性问题。通过基于 RFID 和 WiMax 技术的智能交通综合管理方案，就可以事先预防这类问题的发生，如 IBM 和新加坡政府合作的全程跟踪车辆与管理系统，利用 RFID 技术监控进入特殊路段的车辆，通过 WiMax 技术全程跟踪车辆情况。

4. 物流企业

在未来的智能城市中，无线网络将无处不在，其他类似 WiMax 的技术可能将全面覆盖城市区域，提供比 Wi-Fi 热点范围更广的高速无线连接。在无线城域网、传感网等技术支持下，可以对大型物流企业的车队和运送的包裹、货物进行有效的跟踪和管理，可随时了解包裹、货物的运送状态。

1.3.4　无线城域网的射频干扰

射频干扰是影响城域网稳定和性能的常见因素，在日常生活中，会产生射频干扰的物体主要是手机和微波炉。由于手机进行通信时会产生微波，微波炉的加热原理也是通过微波进行加热，若是城域网接受地靠近这两类物体，其信号就会受到影响，导致数据传输不稳定甚至传输失败。所以，在构建城域网的过程中，如果出现了此类情况，就需要对射频干扰进行考虑，及时展开射频源的排查。从基本诱因上说，如果没有任何的射频干扰源，可以考虑是外界干扰源使用了相同的波段，导致网络传输受到干扰。从另一个角度说来，不同用

户在使用无线网络时,必然会出现射频段重复的情况,这也可能导致不同用户之间相互干扰,影响彼此的正常使用。所以,若是出现了网络不稳定的问题,可以通过更换信号发射频的方法避开干扰源形成的干扰,确保其正常工作。

1.4 无线体域网概述

随着无线通信、电子器件、射频识别、传感及信息处理等技术的发展,信息网络更加全面深入地融合人与人、人与物、物与物之间的现实物理空间与抽象信息空间。无线体域网(Wireless Boay Area Network,WBAN)正广泛地应用于远程医疗诊断、疾病监控和预防、家庭看护等方面。

1.4.1 无线体域网基本概念

无线体域网是以人体为中心,以采集人体各种生理参数为目的,由分布在人体表面或植入人体内部的传感器及个人数据采集处理终端组成的通信网络。通过 WBAN,人可以和其身上携带的个人电子设备(如 PDA、手机等)进行通信、数据同步等。WBAN 和其他数据通信网络(如其他人的 WBAN、无线/有线接入网络、移动通信网络等)成为整个通信网络的一部分,可以和网络上的任何终端(如 PC、手机、电话机、媒体播放设备、数码相机、游戏机等)进行通信。

通常个域网包含的若干节点共同采集数据,通过无线网络汇集至个人数据采集处理终端,并在必要时与外部网络进行通信。目前,该无线传感网多采用先分布式采集或感知、再集中式处理的工作模式,大致可分为三层。第一层包含一组具有检测功能的传感器节点或设备,这些节点通常比较简单,主要用于采集人体生理数据或者采集该节点所在环境(如人体内部)的状况。第二层是个人佩戴或家庭自有的个人数据终端,节点采集的数据将被传送至个人数据终端,并进行简单的分析整合。这一层还与路由器和外部网络连接。这一层的设备可以是专门的移动个人服务器,也可以是手机、MP3 等通用设备。第三层是提供各种应用服务的远程服务器及外部网络,通常由医院等医疗机构所有,负责监控辖区内的个人数据终端,对它们所传递的信息进行分析、判断、储存,并提醒医护人员做出及时、正确的医疗救助。

1.4.2 无线体域网特点

1. 规模小、可扩展、近距离、以人体为中心

由于人体几何结构的限制,无线体域网的网络规模很小,根据采集的人体特征信息将传感器节点部署在身体的相应位置,相对位置固定。因此,根据不同的数据业务需求,无线体域网的规模可以很小,甚至可以由几个节点组成一个小型的数据采集网络。在无线体域网中也会出现各种微型的便携式设备,根据需求部署这些设备,按照相关协议可将其组建成一个应用型的网络。由此可见,无线体域网应该是一个可扩展的网络,并能够提供各种服务的空中接口。另外,由于人体本身的几何特性,导致传感器节点之间的通信范围有限,

无线体域网的有效通信距离通常小于等于 2 m。对于这样近距离的网络来说,用于无线传感器网络、无线自组织网络等网络中的一些基于簇拓扑的网络协议和算法就不再适用。无线体域网的网络拓扑结构和路由算法相对简单,普通传感器节点最多通过三次路由就可以将采集的数据传送到网关节点。

与其他传统网络最大的不同是:无线体域网是以人为中心的网络。必须考虑人体的安全性,这就要求传感器节点的发射功率必须足够低。另外,各传感器节点或便携式设备以人为载体,分布于人体的不同部位,人体不仅可以影响传感器节点之间的通信,而且也可以作为传感器节点之间的通信信道。这就使得无线体域网的信道特征相对比较复杂,在网络结构设计中也必须考虑这一点。

2. 业务数据的多样性与相关性

随着无线便携式技术、网络技术等技术的飞速发展,无线体域网的业务模式呈现出多样性的特点。无线体域网的数据业务多样性包括以下两方面的含义:一方面是该网络可以提供多种业务服务,如数据业务、音频、视频、Internet 服务等,这些业务可以由网络同时提供;另一方面,对于同一种应用场景,如医疗应用,无线体域网中所处理的数据会因为传感器节点所采集的人体生理数据不同而呈现多样性的特点。因此,无线体域网是一种与应用相关的网络,应根据不同的应用需求,构建不同的网络模型。

在无线体域网的医疗应用中,采集的各种生理信息在一定程度上具有相关性。例如,当一个病人发烧时,他的体温、血压、心率、呼吸率等生理参数会相应升高。因此,在传输数据时必须保证多种生理数据的传输在时间上达到同步,使得传输到远程控制中心的数据是同一时间域内采集的数据,便于准确地掌握病人的身体状况。

3. 高度动态性

无线体域网的拓扑结构可能会因为下列因素而改变:身体四肢的随机移动导致节点之间的通信中断;电能耗尽造成节点出现故障或失效;新节点的加入。这就要求无线体域网必须能够适应这些变化,其网络拓扑应具有可重构性。另外,在不同的频率范围内,节点之间的通信机制不同。如果不同传感器工作在不同的频率范围内,那么整个网络将对应混合型的信道特征。

4. 以数据为中心

无线体域网中的节点采用节点编号标识,节点编号和节点位置没有关系。远程控制中心如果需要某方面的数据信息时,只需要把指令信息直接告诉网络的汇聚节点,然后由汇聚节点向全网广播该指令信息,不需要给确定编号的节点发送信息。因此,该网络以数据本身作为查询或传输的索引。

1.4.3　无线体域网的发展趋势

WBAN 目前仍处在早期发展阶段,国际上对 WBAN 已经开展了广泛研究,但在毫瓦级网络能耗、互操作性、系统设备、安全性、传感器验证、数据一致性等方面还面临一系列挑战。为了让 WBAN 成为医疗保健领域长期监控和记录人体健康信号的基本技术,医疗技术提供商、医院、保险公司以及工业界的各方人士正在展开战略性合作,WBAN 将有着广阔的应用前景。

体域网最初应用于医疗保健、身体康复领域,近年来已逐步向其他领域发展,在娱乐、