21世纪高等院校计算机网络工程专业规划教材

无线网络安全技术（第2版）

姚琳 林驰 王雷 编著

清华大学出版社

21世纪高等院校计算机网络工程专业规划教材

无线网络安全技术（第2版）

姚琳 林驰 王雷 编著

清华大学出版社
北京

内 容 简 介

本书对无线信息安全涉及的各个层面知识进行了梳理和论证，并讨论了与安全技术和产品相关的内容，介绍了信息安全领域的最新研究进展和发展趋势。结构上每章先进行安全协议的分析，然后是实践案例的设计，最后是情景分析运用。本书共分为9章，从不同层面介绍无线网络安全相关内容。第1章概要介绍了无线网络及无线网络安全方面的知识；第2章介绍无线局域网的安全内容；第3章主要介绍移动通信安全；第4章介绍移动用户的隐私与安全；第5章介绍无线传感器网络安全问题；第6章介绍移动Ad Hoc网络设计的安全问题；第7章介绍车载网络中面临的安全问题与保护机制；第8章介绍社交网络中面临的安全威胁与社交网络安全机制；第9章介绍容迟网络设计的安全问题。

本书适合作为高等院校计算机、软件工程、网络工程专业高年级本科生、研究生的教材，同时可供对无线网络安全感兴趣的开发人员、广大科技工作者和研究人员参考。

图书在版编目(CIP)数据

无线网络安全技术/姚琳，林驰，王雷编著. —2版. —北京：清华大学出版社，2018
(21世纪高等院校计算机网络工程专业规划教材)
ISBN 978-7-302-47824-9

Ⅰ. ①无… Ⅱ. ①姚… ②林… ③王… Ⅲ. ①无线网－安全技术－高等学校－教材 Ⅳ. ①TN92

中国版本图书馆CIP数据核字(2017)第170457号

责任编辑：刘向威　薛　阳
封面设计：何凤霞
责任校对：焦丽丽
责任印制：王静怡

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：三河市君旺印务有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：19.5　　**字　　数**：476千字
版　　次：2013年10月第1版　2018年1月第2版　　**印　　次**：2018年1月第1次印刷
印　　数：1～1500
定　　价：59.00元

产品编号：074699-01

前言

在网络信息技术高速发展的今天，信息安全已变得至关重要，信息安全已成为信息科学的热点课题。“无线信息安全”是信息安全专业、软件工程专业及物联网工程专业的一门重要的专业课。本课程讲解各种无线网络中的安全问题及其基本对策，内容全面，包括局域网、无线城域网、无线广域网、无线个域网、无线车载网等。本课程对培养和提高学生无线安全协议方面的分析和设计能力、综合知识运用能力和创新能力有重要作用。

第1章概述无线网络的历史、分类、未来发展和挑战，对无线网络的安全也进行了概要介绍。第2章主要介绍无线局域网安全的内容。其中主要分析了无线局域网中常见的WEP与WAPI协议，以及这两种协议存在的一些安全问题；另外也介绍IEEE 802.1x的协议原理以及其中的一些安全问题。第3章主要介绍了移动通信安全。本章开篇详细列举出了移动通信网络所面临的各种安全威胁，让读者对当前的通信网络安全情况有很好的了解；而后详细介绍了UMTS系统的安全情况、第3代移动通信系统概况以及现在移动通信网络的发展热点，即第4代、第5代移动通信系统的安全机制。第4章主要介绍了移动用户的隐私与安全。本章开篇概括了移动用户目前面临的安全问题，让读者对当前移动用户的安全情况有所了解；然后详细介绍移动用户间的实体认证机制、信任管理机制以及移动用户的位置隐私保护。第5章主要介绍了无线传感器网络安全问题，详细介绍了无线传感网络中的几个主要安全问题，包括密钥管理、认证机制、安全路由以及隐私问题等，最后介绍了节点俘获攻击的主要机制。第6章主要介绍了移动Ad Hoc网络设计的安全问题，并介绍了该网络的特点、安全问题和安全目标。然后分别从安全路由协议、密钥管理、认证机制和入侵检测等几个方面对移动Ad Hoc网络涉及的安全问题进行了详细的分析和说明。第7章主要介绍了车载网络中面临的安全问题与保护机制，对车载网络的特点、面临的安全威胁以及安全目标进行了介绍。然后分别从路由安全与隐私保护两个方面对车载网络涉及的安全问题以及相应的安全策略进行了详细介绍。第8章主要介绍了社交网络中面临的安全威胁与社交网络安全机制，介绍了社交网络的发展历史、特点、面临的安全威胁以及安全目标。然后分别从路由安全与隐私保护两个方面介绍了社交网络安全方面的研究进展。第9章主要介绍了容迟网络设计的安全问题，介绍容迟网络的特点、面临的安全威胁以及安全目标，并分别从路由安全、密钥管理机制、网络认证机制、数据隐私保护、位置隐私方面介绍了容迟网络安全的最新研究进展，最后介绍了容迟网络中一种较好的路由方式——机会网络的路由安全与隐私保护机制。

本书的内容是国家自然科学基金项目(61672129,61402078)部分研究成果的体现。在项目研究和本书撰写的过程中，得到了大连理工大学软件学院、辽宁省泛在网络与服务软件

重点实验室相关领导和同事的关心和支持。特别要感谢徐遣、宋奇、张天宇、张家宁、何丹阳、傅曼青、万柳夥等为本书撰写和收集资料、编写程序、文字校对等方面的贡献。

在本书撰写过程中,参考了大量国内外文献资料,并在书中尽量注明和列出,再次向相关作者表示衷心感谢!

由于作者水平有限,时间仓促,书中存在不足之处在所难免,恳请专家及读者批评指正!

姚琳　林驰　王雷

2017年4月于大连理工大学

目 录

第1章 无线网络导论

1.1 无线网络概述

在过去的十多年中，整个世界逐渐走向移动化，连接世界的传统方式已经无法应对日益加快的生活节奏和全球化的步伐所带来的挑战。因此，一个新的概念“无线网络”便应运而生。

无线网络代表了任何一种使用无线连接（但不包括无线电波）的计算机网络。目前，家庭、企业（商业机构）和电信网络都大量地采用无线网络连接，目的是避免在楼房内安装光纤电缆，或者是在不同地区的设备之间建立连接而产生巨大的开销。无线通信网络通常是通过无线电通信来实现和管理的，这是在 OSI 网络模型结构的物理层实现的。如果必须通过实体电缆才能够连接到网络，用户的活动范围势必大幅缩小。无线网络却无此限制，用户可以享有较宽广的活动空间。因此，无线技术正逐渐侵占传统的“固定式”或“有线式”网络所占有的领域。

1.1.1 无线网络的历史背景

无线网络的历史背景可以追溯到无线电波的发明。1888 年，海因里希·赫兹发现并率先提出了无线电波的概念。1896 年，古列尔默·马可尼实现了通过电报光纤传送信息。他在 1901 年把长波无线电信号从康沃尔（位于英国的西南部）跨过大西洋传送到 3200km 之外的圣约翰（位于加拿大）的纽芬兰岛。他的发明使双方可以通过彼此发送用模拟信号编码的字母数字符号来进行通信。

第二次世界大战期间，美国军队率先在数据传输中使用无线电信号。这给之后的科学研究提供了灵感：1971 年，夏威夷大学的研究小组基于无线电通信网络 ALOHNET 设计了第一个报文。ALOHNET 是第一个无线局域网（Wireless LAN，WLAN）。第一个 WLAN 包含 7 台计算机，它们构成了一个双流向的星状拓扑以实现相互通信。

第一代的 WLAN 技术采用了未经许可的频带（902～928MHz ISM），这一频带随后被小型的应用和工业机械的通信干扰所阻塞。一种扩频技术随后被用来减小这种干扰，它每秒可以传输 50 万比特。第二代的 WLAN 技术的传输速率达到了 2Mb/s，是第一代的 4 倍。第三代的 WLAN 技术和第二代 WLAN 运行在同样的频带上，这也是人们今天仍然用到的 WLAN 技术。

1990 年，IEEE 802.11 执行委员会建立了 820.11 工作小组来设计无线局域网（WLAN）标准。这一标准规定了在 2.45GHz ISM 频带下的工作频率。1997 年，工作小组批准 IEEE 802.11 成为世界上第一个 WLAN 标准，规定的数据传输速率是 1Mb/s 和 2Mb/s。

除 WLAN 之外,无线网络还衍生出了多种应用:无线网络技术使商业企业能够发展广域网(WAN)、城域网(MAN)和个域网(PAN)而无须电缆设备;IEEE 开发了作为无线局域网标准的 802.11;蓝牙(Bluetooth)工业联盟也在致力于能提供一个无缝的无线网络技术。

蜂窝或移动电话是马可尼无线电报的现代对等技术,它提供了双方的、双向的通信。第一代无线电话使用的是模拟技术,这种设备笨重且覆盖范围是不规则的,然而它们成功地向人们展示了移动通信的固有便捷性。现在的无线设备已经采用了数字技术。与模拟网络相比,数字网络可以承载更高的信息量并提供更好的接收和安全性。此外,数字技术带来可能的附加的服务,诸如呼叫者标识。更新的无线设备使用能支持更高信息速率的频率范围连接到 Internet 上。

无线技术为人类社会带来了深刻的影响,而且这种影响还会继续。没有几个发明能够用这样的方式使整个世界"变小"。定义无线通信设备如何相互作用的标准很快就会有一致的结果,人们不久就可以构建全球无线网络,并使之提供广泛的服务。

1.1.2 无线网络的分类

无线网络可根据数据传输的距离分为下面几种不同类型。

1. 无线个域网

个域网(Personal Area Network,PAN)是计算设备之间通信所使用的网络,这些计算设备包括电话、个人数据助手(PDA)等。PAN 可以使用在私人设备之间的通信,或者与更高级别的网络或者 Internet(向上连接)取得连接。无线个域网(WPAN)是采用了多种无线网络技术的个域网,这些网络技术包括:IrDA,无线 USB,蓝牙,Z-Wave,ZigBee,甚至是人体域网。WPAN 的覆盖范围从几厘米到几米不等。IEEE 802.15 工作组为 WPAN 制定了相关的物理层和 MAC 层标准,这类网络包括 HomeRF 和 Bluetooth 等,也包括与 IEEE 802.11 局域网共同存在的问题。

HomeRF 是关于 PC 与各类电器之间语音和数字通信的技术标准。它可以连接 PC、打印机、电话、互联网等,如图 1.1 所示。Bluetooth 是小范围语音和数据通信的技术标准。

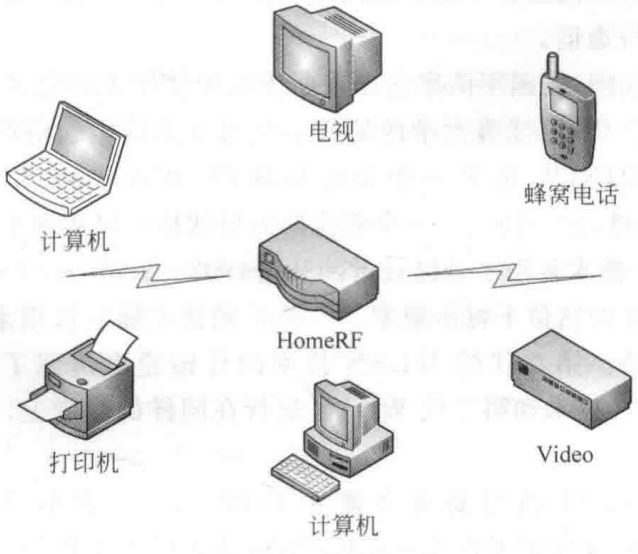

图 1.1 无线个人网

Bluetooth 的应用包括 PC 使用的无线连接键盘和鼠标等设备、小范围的无线局域网、蜂窝网络、有线网络和卫星网络的 AP 等。Bluetooth 制定了协议栈以支持各种传输介质和各种各样的应用。Bluetooth 物理层采用 FHSS 和 GFSK，工作频率为 2.402～2.480GHz，数据传送速率是 1Mb/s。Bluetooth 的 MAC 层采用 FH-CDMA/TDD 机制。

2. 无线局域网

无线局域网(Wireless LAN，WLAN)采用一些分布式无线措施(通常是扩频或 OFDM 无线电技术)来连接两个或更多的设备，并且在一个接入点向更大的互联网范围提供连接。像广域网一样，局域网是一种由各种设备相互连接，并在这些设备间提供交换信息手段的通信网络。这给用户提供了更多的移动性，使得他们可以在局域性的覆盖区域内移动的同时接入网络。而相对于广域网，局域网的范围较小，通常是一栋楼或一片楼群，但是局域网内的数据传输率通常要比广域网的高得多，大多数的现代 WLAN 技术都是基于 IEEE 802.11 标准，以 Wi-Fi 提供商的品牌名字命名并运营。WLAN 曾经被美国国防部称为 LAWN(在本地区提供无线网络)。

无线局域网因其易于安装的优势，在家用网络中得到了非常广泛的应用，并且在很多商业场所都向客户提供免费的接入服务。

IEEE 802.11 是关于无线局域网(WLAN)的标准，它主要涉及物理层和介质访问子层(MAC 层)。通过 IEEE 802.11 标准，无线用户可通过接入点(AP)连接到网络，每个用户终端使用无线网卡与 AP 连接。无线网卡和 AP 支持 IEEE 802.11 物理层和 MAC 层标准，同样 AP 也负责连接这些用户到像 IEEE 802.3 那样的网络。图 1.2 显示了 WLAN 和 LAN 连接。

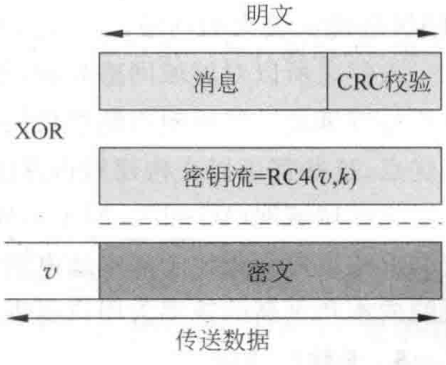

图 1.2　WLAN 和 LAN 连接

3. 无线 Mesh 网

无线 Mesh 网(Wireless Mesh Network，WMN)是由无线 Mesh 节点设备动态地、自动组成的通信网络。无线 Mesh 网络通常是由 Mesh 客户端、网格路由器和网关组成。网络的客户端往往是笔记本电脑、手机和其他无线设备，而 Mesh 路由向网关转发流量可能不需要连接到互联网。为一个单一的网络而工作的无线节点的覆盖区域有时也被称为 Mesh 云。访问此 Mesh 云是依赖于彼此和谐工作的节点所建立的无线网络。Mesh 网络是可靠的，并提供冗余。当一个节点不能工作的时候，其余的节点仍然可以直接或通过一个或多个中间节点互相通信。无线 Mesh 网络可以通过各种无线技术，包括 IEEE 802.11、IEEE 802.15、IEEE 802.16、蜂窝技术或多种类型的组合来实现。

无线 Mesh 网络可以被看作是一种特殊类型的无线 Ad Hoc 网络，如图 1.3 所示。一个无线 Mesh 网络通常有多个计划好的配置，可以将其部署到超过特定的地理区域中来提供动态的和划算的连接。无线 Ad Hoc 网络是临时的无线设备在彼此通信范围内形成的。Mesh 路由器是可以移动的，并且可以根据具体的要求在网络中移动。Mesh 路由器通常不受节点的资源限制，因此可以用来执行更多资源密集型的功能。由于 Ad Hoc 网络中的节点通常受资源约束，所以无线 Mesh 网络与 Ad Hoc 网络有所不同。

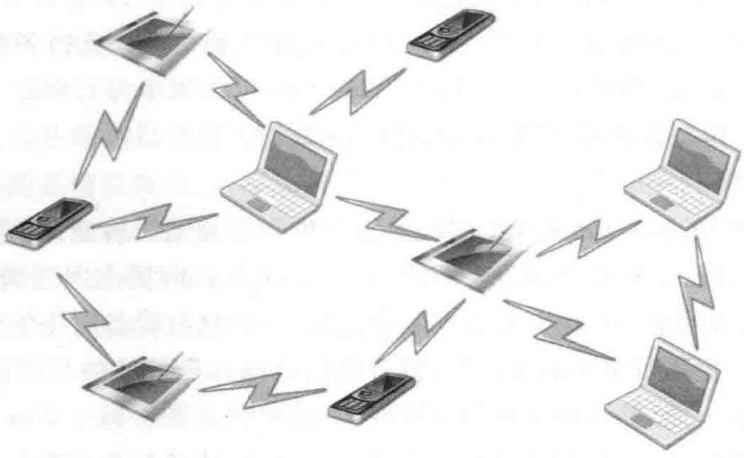

图 1.3　Ad Hoc 网

4. 无线城域网

城域网(MAN)是连接多个局域网的计算机网络。MAN 经常覆盖一个城市或者是大型的校园。MAN 通常采用大容量骨干技术,例如光纤链路来连接多个局域网。此外,MAN 还能向更大的网络(如广域网)提供向上连接服务。

人们之所以对城域网感兴趣,是因为用于广域网中的传统的点到点连接和交换网络技术不足以满足一些组织不断增长的通信需求。局域网标准中的高度共享媒体技术具有很多的优点,这些都可以在构建城市范围的网络中实现。

无线城域网(Wireless MAN,WMAN)的主要市场是那些在城市范围内对高容量通信有需求的用户。相比于从本地电话公司那里获得的同样服务,一个无线城域网就是要以更低的成本和更高的效率为用户提供所需容量的通信服务。

5. 无线广域网

无线广域网(Wireless WAN,WWAN)是无线网络的一种。相比于局域网,广域网覆盖了更大的地理范围。它可能需要通过公共信道,或者至少有一部分依靠的是公共载波电路进行传输的网络。一个典型的无线广域网包括多个相互连接的交换节点。所有的传输过程都是从一个设备出发,途经这些网络节点,最后到达所规定的目的设备。所有规模的无线网络都为电话通信、网页浏览和串流视频影像等应用提供数据传输服务。

WWAN 采用了无线通信蜂窝网络技术来传输数据,例如 LTE、WiMAX(通常也称为无线城域网,WMAN)、UMTS、CDMA2000、GSM 等。GSM 数字蜂窝系统是由欧洲电信公司提出的标准,CDMA 接入技术采用 TDMA 和 FDMA,调制采用 GMSK 技术。WLAN 也可以采用局域多点分布式接入服务(LMDS)或者 Wi-Fi 来提供网络连接。这些技术是区域性、全国性甚至是全球性的,并且是由无线服务提供商负责提供。WWAN 的联通性使得持有便携式计算机和 WWAN 上网卡的用户可以浏览网页、收发邮件,或者接入虚拟私人网络(VPN)。只要用户处在蜂窝网络服务的区域范围之内,就都能够享受到 WWAN 带来的服务。不同的计算机有着统一的 WWAN 性能。

目前,中国可供选择的无线广域通信服务,有联通 CDMA1X 服务、移动公司的 GPRS 服务、中国卫星通信公司的专线服务等。

6. 蜂窝网络

蜂窝网络(或移动网络)是一个分布在陆地区域的无线电网络,称为"细胞",每一个"细胞"都由一个固定的无线电收发机提供服务,这也被称为行动通信基地台或者基站。在蜂窝网络中,每一个"细胞"都典型地采用与其他邻居"细胞"相同的无线电频率来避免干扰。

当共同加入网络后,这些"细胞"在广阔的地理区域内提供无线电覆盖。这使得大多数便携的无线电收发机(例如:移动电话,寻呼机等)可以相互之间或者是与网络中任意固定的电话和收发机通过基站进行通信。即使一些收发机在多个"细胞"之间移动,通信也不会受到影响。

尽管蜂窝网络最初是为移动电话设计的,但随着智能手机的发展,蜂窝电话网络在电话对讲之外还照常携带数据进行传输。

(1) 全球移动通信系统(GSM)。全球移动通信系统网络可以分为三个主要系统:交换系统,基站系统和运营支持系统。连接到基站的移动电话可以再连接入运营支持系统站点;再接入交换系统站点,在这里,通话可以被转发到它需要去的地方。GSM 是目前最常用的标准,并且它在绝大多数的移动电话中得到了使用。

(2) 个人通信服务(PCS)。PCS 是一种无线电波段,它在北美和南亚地区的移动电话中得到使用。Sprint 成为第一个创立 PCS 的服务提供商。

(3) 数字高级移动电话服务(D-AMPS)。D-AMPS 是 AMPS 的一种升级版本,由于技术的更新,AMPS 正逐渐被淘汰。

1.1.3 无线网络未来的发展和挑战

1. 无线局域网的应用前景

作为无线网络中应用最广的技术,无线局域网技术(WLAN)经过不断的发展,目前正逐渐趋于成熟,但仍在产生着意义重大的革新,目的是在与有线网络和蜂窝网络的竞争中处于优势。此外,WLAN 也在不断产生分化,尽管其核心特征正逐渐商品化并且服务提供商正逐渐趋于统一。例如,WLAN 的传输速度正呈指数增长。所有的无线网络服务提供商正逐渐走在一起,致力于提升所部属服务的可信赖性和安全性,这在之前几乎是纸上谈兵的事,而现在即将变成现实。

商业领域产生的对于 WLAN 性能的新要求正逐渐提高,特别是在移动设备变得更流行和多样化的今天。这种发展趋势的关键驱动在于商业用户对所用设备的可用性和功能性提出了严苛的要求。这意味着对于智能手机、便携式计算机和多媒体应用设备在商务环境下的要求更高,并且对于企业级的 WLAN 也有着不同的严格要求。

技术的发展同样也在支持着 WLAN 的进步:便携式计算机和平板电脑都依赖于 Wi-Fi 的发展。此外,随着无线热点、酒店接入点和其他形式的公共无线接入点等更广泛的应用,商务人士和其他职场雇员会越来越多地利用 Wi-Fi,并在他们的办公场所对 Wi-Fi 的服务质量有同样高的期待。这将会使得相关 WLAN 服务提供组织的建立,它们具备更快适应新的无线网络技术的能力,以更好地服务于移动用户。这与商务人士开始严格要求无线网络下的无打扰的连接、高速传播的多媒体应用和所有形式的基于云的功能等需求密切相关。

与此同时,不断进步的工业化标准以及服务提供商的技术革新使得 WLAN 速率显著

提高,并且更加可信也更加安全。现行的IEEE 802.11n标准相比于之前的IEEE 802.11g版本在数据吞吐量方面有着10倍的提升,从54Mb/s提高到将近GBE。这有助于弥合有线和无线环境的性能差距。事实上,企业应该考虑的是IEEE 802.11n而不是工作站的电缆分支,如果该标准能够有效部署,这将创建一个真正的无线办公室,而伴随着这些优点的同时也满足了带宽的要求。

2. 无线传感网的发展

无线传感网(Wireless Sensor Networks,WSN)在过去几年已经成为最受关注的研究领域之一。WSN是由若干无线传感器节点形成的一个传感器区域和一个接收器。这些有能力感知周围环境的大量节点,执行有限的计算和无线通信进而形成了WSN。最近无线和电子技术的进步已经使无线传感网在军事、交通监视、目标跟踪、环境监测和医疗保健监控等方面有了很广阔的应用。随之而来有许多新的挑战已经浮出水面,无线传感网要满足各种应用的要求,如检测到的传感器数量、节点大小、节点的自主权等。因此需要改进当前的技术,更好地迎接这些挑战。未来传感器必须功能强大并节约成本,让应用程序使用它们,如水下声学传感器系统、基于传感器的信息物理系统、对时间有严格要求的应用、认知传感和频谱管理、安全和隐私管理等。无线传感器在如下几个典型领域得到了广泛应用。

1) 认知感应

认知传感器网络通过部署大量智能的和自治的传感器来获取本地的和周围环境的信息。管理大量的无线传感器是一项复杂的任务。认知感应两个众所周知的例子是群智能和群体感应:群智能是从人工智能发展而来的,用来研究分散的自组织系统中的集体行为;群体感应是仿生传感网络的一个例子。群体感应是细菌沟通协调、通过信号分子合作的能力。

2) 频谱管理

低功耗无线应用协议越来越多,人们可以设想未来的无线设备,如无线键盘、投影片演示器、手机耳机和健康监测传感器等将无处不在。但是这些设备的普及会导致网络内的干扰和拥塞的增加,因为这些设备的物理频率会重叠。认知无线电和多频MAC的一些方法已经发展到利用多个并行的通信频率。一个通用的解决方案是由周(2009年)提出的称作SAS:WSNs下的一个自适应无线传感网络中间件,它可以很容易地通过现存的单频率集成得到。

3) 水下声学传感器系统

Akyildiz在2005年提出了一个完整的水下传感器网络调查。水下传感器网络的设计使得应用程序可以对海洋数据进行收集,实现污染监测、海上勘探、灾害预防、辅助导航和战术监控等应用。水下传感器也被应用于勘探天然海底资源和科学数据的收集。因此,需要水下设备之间产生通信。水下传感器节点和车辆应协调运作,交换它们的位置和运动信息,最终将监测到的数据转播到陆上的基站。新的水下无线传感器网络(UWSN)相比于陆基无线传感器网络也带来了其他挑战,如传播延迟大、节点的移动性问题和水下声音信道的错误率高。Domingo在2008年提出一种叫做DUCS(分布式水下聚类计划)的协议,这是一个GPS的免费路由协议。它最大限度地减少了主动路由信息交换并且不会导致洪泛问题。它还使用了数据的聚合,从而消除冗余信息。