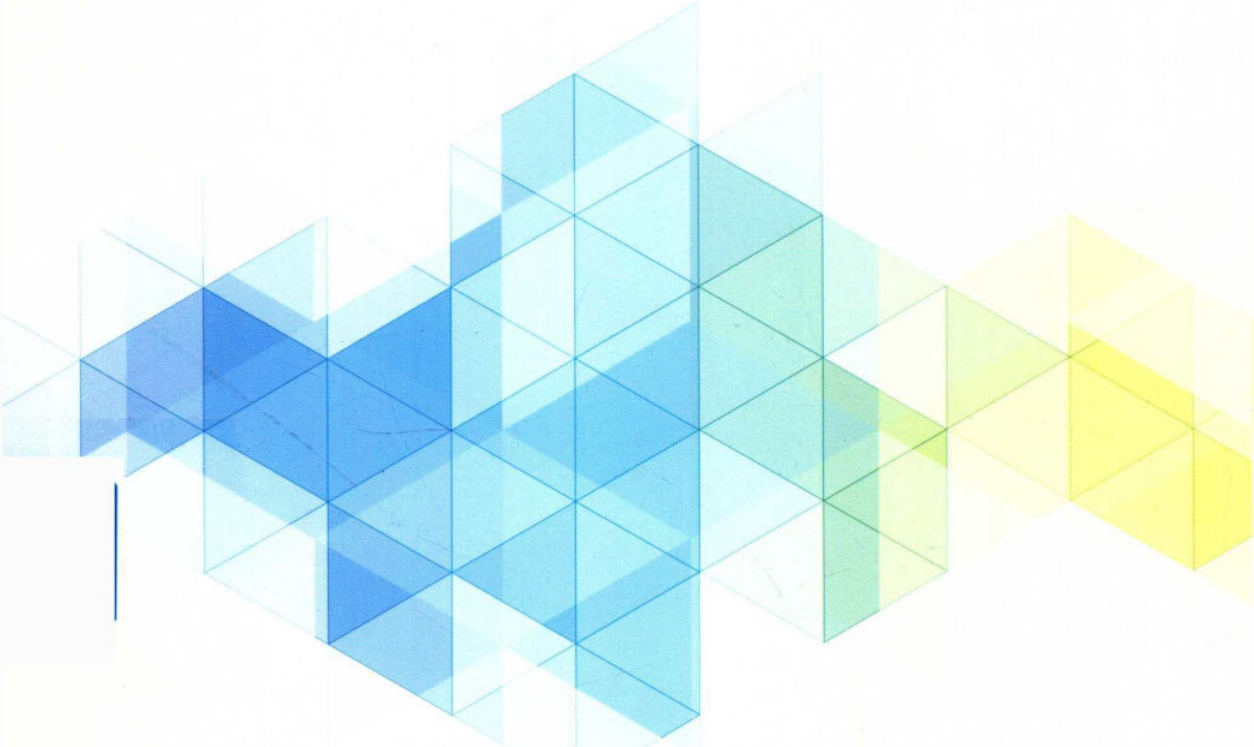
无线网络安全方法与技术研究

张 辉 著



科学出版社

无线网络安全方法与技术研究

张 辉 著

科学出版社
北京

内 容 简 介

本书从无线网络技术的安全机制出发，提出了无线网络安全优化的部分解决方案。全书研究总结了无线局域网、移动通信网络、蓝牙通信和其他新型无线网络的安全机制；从无线网络最佳中继选择方法出发，提出了异构无线网络自适应协作分集算法；通过设置粒子群中的每个粒子代表一个差异化节点定位的解，提出了不定攻击中网络最弱节点的定位技术；在综合分析网络入侵检测系统的基础上，提出了基于重复博弈的自体集网络入侵检测中的高效寻优算法；针对混合式网络中应用数据丢失、遗漏等情况，提出了粒子群优化的混合式网络丢失数据包恢复方法；针对网络控制系统的时延进行了分析，总结出网络控制系统中各种时延的影响因素。

本书可供通信类、网络类、控制类专业的博士研究生和硕士研究生使用，也可供无线网络安全相关领域的科研人员参考。

图书在版编目(CIP)数据

无线网络安全方法与技术研究 / 张辉著. —北京：科学出版社，2019.11
ISBN 978-7-03-058280-5

Ⅰ. ①无… Ⅱ. ①张… 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（2018）第 160494 号

责任编辑：王会明 / 责任校对：王 颖
责任印制：吕春珉 / 封面设计：东方人华平面设计部

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

三河市骏杰印刷有限公司印刷
科学出版社发行 各地新华书店经销

*

2019 年 11 月第 一 版 开本：B5（720×1000）
2019 年 11 月第一次印刷 印张：8
字数：160 000

定价：59.00 元

（如有印装质量问题，我社负责调换〈骏杰〉）
销售部电话 010-62136230 编辑部电话 010-62135397-2008

前　言

随着科技和经济的日益发展，网络已经成为人们生活中不可或缺的一部分。由于我国无线网络应用日益广泛，特别是智能手机的普及，传统的有线网络技术已不能满足人们对更灵活的网络的需求。与此同时，计算机网络与无线通信技术相结合的无线局域网技术凭借其架设便捷、接入灵活、经济节约、扩展性强等特点迅速发展起来。随着无线技术的不断成熟和广泛应用，如今的无线网络俨然成了大到公司、小到家庭都离不开的新的网络主角。

无线网络在给人们带来便利的同时，其安全问题也日益凸显。由于无线传输介质的开放性，无线网络面临网络、终端、信息等多个层面的安全威胁。如何基于无线通信设备计算能力受限、存储能力受限和用户移动等特点，实现无线网络及其应用的安全，是当前无线通信系统快速发展的基础和关键。无线网络技术虽更替频繁，但其演进路线日渐清晰，系统梳理无线网络体系结构，分析各种无线网络技术安全防护的特点，从网络安全优化角度研究无线网络安全技术及其发展趋势，已成为掌握无线网络安全内涵的重要途径。

本书内容是作者对其从事无线网络安全研究成果的梳理与总结，较为深入地阐述了无线网络安全优化在无线网络技术发展中的应用及性能分析。

本书由 8 章组成。第 1 章为本书的绪论，通过对无线网络的发展现状、原理及规范的介绍，阐述了无线网络的技术特点，在此基础上介绍了无线网络面临的主要安全问题；第 2 章从无线网络技术的安全机制出发，总结了无线局域网、移动网络、蓝牙通信和其他新型无线网络的安全机制；第 3 章介绍了异构无线网络研究现状，分析了无线网络最佳中继选择方法，给出了基于功率控制的信道增益模型，最后提出了一种中继选择机制；第 4 章利用粒子群优化方法，实现无线网络最弱节点定位，计算网络节点之间的特征差值，在不定攻击中提取网络节点特征的残差参数，进行极小化处理，通过设置粒子群中的每个粒子代表一个差异化节点定位的解，最大限度地减小随机性带来的关联特征弱化问题；第 5 章在综合分析网络入侵检测系统的基础上，提出基于重复博弈的自体集网络入侵检测中的高效寻优算法，采用这种算法对网络数据进行分类，能够过滤掉数据中的多余信息，增强网络的检测效率和准确率；第 6 章针对混合式网络中的应用数据丢失、遗漏等情况，提出了粒子群优化的混合式网络丢失数据包恢复的方法；第 7 章首先对网络控制系统的时延进行了分析，进而得出网络控制系统中的时延与网络协

议、网络负载、信息优先级、信息长度、网络速率、节点间距离、采样技术和信息调度算法等诸多因素的关系；第 8 章给出了本书的主要研究成果及有待进一步研究的问题。

由于作者水平有限，加之成书时间仓促，书中难免存在不足之处，恳请业界专家及广大读者批评指正。

目　录

第1章 绪 论

近年来，计算机技术及通信技术发展突飞猛进，无线网络在一定程度上也得到了快速发展，其技术越来越成熟，应用越来越便捷，在信息化变革中扮演了相当重要的角色。传统的计算机网络在由有线向无线、由固定向移动、由单一业务向多媒体业务演进过程中得到了快速的发展。无线网络作为有线网络的补充和延伸，其安全问题不仅影响到用户自身，而且影响到与之相关的有线网络用户。因此，怎样有效而又安全地使用无线网络成为人们关注的又一热点问题，无线网络的安全问题必须引起足够的重视。

1.1 无线网络技术概述

无线网络技术涵盖的范围很广，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，也包括为近距离无线连接进行优化的红外线技术及射频技术（王继红等，2015）。通常使用无线网络的设备包括便携式计算机、台式计算机、手持电脑、个人数字助理（personal digital assistant，PDA）、移动电话、笔式计算机等。无线技术用于多种实际用途。例如，手机用户可以使用移动电话查看电子邮件；使用便携式计算机的旅客可以通过安装在机场、火车站和其他公共场所的基站连接到 Internet；使用台式机的用户可以通过连接桌面设备同步数据和发送文件。

无线网络的初步应用可以追溯到第二次世界大战期间，当时美国陆军研发了一套无线电传输设备，使用无线电信号传输资料，并且融合了高强度的加密技术，在当时这种资料传输方式得到美军和盟军的广泛使用（Nilsson，1998）。后来，这项技术让许多学者受到了启发，在 1971 年，夏威夷大学的研究员创造了第一个基于封包式技术的无线电通信网络，被称为 ALOHNET 网络，这个网络可以算是早期的无线局域网络（wireless local area networks，WLAN），它包括 7 台计算机，采用双向星型拓扑横跨四座夏威夷的岛屿，中心计算机放置在瓦胡岛上（Alamouti，1998）。

如今的无线网络技术无论是在难以布线或是频繁变化的环境中，还是在移动办公区域的网络接入方面都有很强的优势。在学术界、医疗界、制造行业、仓储行业等领域，无线网络扮演着越来越重要的角色。目前，全球在建和规划中的无线网络覆盖城市已超过 1000 个（Jetcheva et al.，2017）。从总体上看，全球无线热点、无线热区、无线城市的建设已是大势所趋，成为当今世界发展的潮流。

我国最具有代表性的无线城市有北京、天津、青岛、武汉、上海、南京、杭

州、厦门、广州、深圳、苏州等。与其他无线网络发展迅速的国家一样，我国无线热点、无线热区和无线城市的发展势头也十分强劲，而且正从沿海地区向内地发展（魏传佳等，2016）。基于 Wi-Fi、Mesh 技术的无线宽带网络具有高带宽、低成本、灵活方便的优势，成功应用于无线数字小区、无线监控、无线分机等社会公共领域。

1.2　无线网络原理、标准与类型

1.2.1　无线网络原理

1. 无线网络的传输原理

无线网络的传输原理和普通有线网络一样，也是采用了 OSI/RM（open system interconnection/reference model，开放系统互联参考模型）七层网络类型，只是在模型的最低两层“物理层”和“数据链路层”中，使用了无线的传输方式（何明等，2009）。尽管目前各类无线网络的标准和规范并不统一，但是按传输方式不同，可分为无线电波传输方式和红外线传输方式两种（肖景等，2011）。

1）无线电波传输方式，不仅覆盖范围大、发射功率强，而且还具有隐蔽性、保密性等特点，不会干扰同频的系统，具有很高的可用性，因此，现在的无线网络基本都是采用此种方式（徐程等，2016）。

2）红外线传输方式是目前使用非常广泛的无线网络技术，例如，家用电器的遥控器几乎都采用红外线传输技术。作为一种无线局域网的传输方式，红外线传输的最大优点是不受无线电波的干扰，而且红外线的使用也不会被国家无线电管理委员会加以限制。但是，红外线传输方式的传输质量受距离的影响非常大，并且红外线对非透明物体的穿透性也较差，直接导致了红外线传输技术与无线网络的“主角地位”无缘（史雪松等，2016）。

相比之下，无线电波传输方式的应用更广泛。无线网络是通过发射和接收装置（无线设备）连接交换机的，工作站就通过无线网卡和无线设备进行通信，无线设备接收到信号后传送给交换机，再由交换机连接到路由器，路由器接入 Internet，实现上网。

2. 无线网络的传输方式

（1）扩展频谱方式

在扩展频谱方式下，数据信号的频谱被扩展成几倍甚至几十倍后再被发射出去。这一做法虽然牺牲了频带带宽，但却提高了通信系统的抗干扰能力和安全性。采用扩展频谱方式的无线局域网一般选择的是 ISM（industrial、scientific、

medical，工业、科学、医学）频段。许多工业、科研和医疗设备的发射频率均集中于该频段。例如，美国的 ISM 频段由 902～928MHz、2.4～2.48GHz、5.725～5.850GHz 三个频段组成，如果发射功率及带宽辐射满足美国联邦通信委员会（Federal Communications Commission，FCC）的要求，则无须向 FCC 提出专门申请即可使用该 ISM 频段（Giacomini et al.，2013）。

（2）窄带调制方式

与扩展频谱方式相比，窄带调制方式占用频带少，频带利用率高。但采用窄带调制方式的无线局域网要占用专用频段，因此，需经过国家无线电管理部门的批准才能使用。当然，用户也可以直接选用 ISM 频段免去频段申请，但当邻近的仪器设备或通信设备也在使用这一频段时，会严重影响通信质量，通信的可靠性无法得到保障（Giacomini et al.，2013）。

目前，基于 IEEE 802.11 标准的 WLAN 均使用扩展频谱方式。

1.2.2 无线网络协议标准

无线技术包括无线局域网技术和以 GPRS/3G/4G/5G 为代表的无线上网技术，这些标准和技术发展到今天，已经出现了包括 IEEE 802.11、蓝牙技术和 HomeRF 等多项标准和规范。以 IEEE（Institute of Electrical and Electronics Engineers，电气和电子工程师协会）为代表的多个研究机构针对不同的应用场合，制定了一系列协议标准，推动了无线局域网的实用化（Tarnoi et al.，2014）。这些协议由 Wi-Fi（Wi-Fi 联盟是一家世界性组织，成立的目标是确保符合 IEEE 802.11 标准的 WLAN 产品之间的相互协作性）组织制定和进行认证。我国早在 2004 年 7 月 26 日已向国际标准化组织提交了无线局域网中国国家标准 WAPI（Wireless LAN Authentication and Privacy Infrastructure，无线局域网鉴别与保密基础结构）提案，这是中国拥有自主知识产权的无线局域网标准，该标准较好地解决了无线局域网的安全问题（邓海良，2015）。下面列出了一些主要的无线局域网标准。

1. IEEE 802.11 系列协议

作为全球公认的研究局域网的权威，在过去的 20 多年内，IEEE 802 工作组建立的标准在局域网领域独领风骚。这些协议包括 IEEE 802.3 Ethernet 协议、IEEE 802.5 Token Ring 协议、IEEE 802.3z 100BASE-T 快速以太网协议。1997 年，IEEE 发布了 802.11 协议，这也是无线局域网领域内第一个国际上认可的协议。1999 年 9 月，IEEE 又提出了 802.11b“High Rate”协议，对 IEEE 802.11 协议进行补充，IEEE 802.11b 在 IEEE 802.11 的 1Mb/s 和 2Mb/s 速率的基础上又增加了 5.5Mb/s 和 11Mb/s 两个新的网络吞吐速率。通过 IEEE 802.11b，用户能够获得与 Ethernet 一样的性能、网络吞吐率与可用性。这个基于标准的技术，使管理员可以根据环境选择合适的局域网技术构造自己的网络，满足商业用户和其他用户的需求。

IEEE 802.11 协议主要工作在 ISO 协议的最低两层上，并在物理层上进行了一些改动，加入了高速数字传输的特性和连接的稳定性（Tarnoi et al.，2014）。

2. 蓝牙技术

蓝牙（bluetooth）是一种可实现固定设备、移动设备和楼宇个人域网之间的短距离数据交换的无线技术，它工作在 2.4～2.485GHz 波段，采用跳频展频（frequency hopping spread spectrum，FHSS）技术，数据速率为 1Mb/s，距离可达 10m。任意一个蓝牙技术设备一旦搜寻到另一个蓝牙技术设备，马上就可以建立联系，而无须用户进行任何设置。在无线电环境非常嘈杂的情况下，其优势更加明显。蓝牙技术的主要优点是成本低、耗电量低、支持数据/语音传输等（Tarnoi et al.，2014）。

3. HomeRF

HomeRF 是专门为家庭用户设计的无线技术，它工作在 2.4GHz 波段，采用 50 跳/s 的跳频扩谱方式，通过家庭中的一台主机实现移动设备之间的通信，既可以通过时分复用支持语音通信，又可以通过 CSMA/CA（carrier sense multiple access with collision avoidance，载波监听多重访问/冲突避免）协议提供数据通信的服务。同时，HomeRF 提供了与 TCP/IP 良好的集成，支持广播、多播和 48 位 IP 地址。HomeRF 最显著的优点是支持高质量的语音及数据通信，它把共享无线连接协议（share wireless access protocol，SWAP）作为未来家庭内联网的几项技术指标，使用 IEEE 802.11 标准作为数据传输标准（Ertürk et al.，2013）。

4. HyperLAN/HyperLAN2

HyperLAN 是 ETSI（European Telecommunications Standards Institute，欧洲电信标准化协会）制定的标准，分别应用在 2.4GHz 和 5GHz 两个波段中。与 IEEE 802.11 最大的不同之处是 HyperLAN 不使用调制技术，而使用载波侦听多路访问（carrier sense multiple access，CSMA）技术。HyperLAN2 采用 Wireless ATM 的技术（因此也可以将 HyperLAN2 视为无线网络的 ATM），采用 5GHz 射频频率，传输速率为 54Mb/s（Ertürk et al.，2013）。

5. WiMAX

作为宽带无线通信的推动者，IEEE 于 1999 年设立 IEEE 802.16 工作组，该工作组主要开发固定宽带无线接入系统标准，包括空中接口及其相关功能，标准涵盖 2～66GHz 的许可频段和免许可频段，解决最后 1km 的宽带无线城域网的接入问题。随着研究的深入，IEEE 相继推出了 IEEE 802.16、IEEE 802.16a、IEEE 802.16d、IEEE 802.16e 等一系列标准，该系列标准引起业界广泛关注，被认为是

宽带无线城域网（wireless MAN，WMAN）的理想解决方案。为了推广遵循 IEEE 802.16 和 ETSI HyperMAN 的宽带无线接入设备，并确保其兼容性及互用性，一些主要的通信部件及设备制造商结成了一个工业贸易联盟组织，即 WiMAX（Worldwide Interoperability for Microwave Access），IEEE 802.16 标准又被称为 WiMAX 技术。其最大传输速率可达 75Mb/s，最大传输距离可达 50km（Ahuja et al.，2014）。

6. GPRS 技术

GPRS（general packet radio service）即通用分组无线服务技术，它是利用“包交换”（packet-switched）的概念发展出的一套无线传输方式。包交换就是将数据封装成许多独立的封包，再将这些封包一个一个传送出去，形式上有点类似寄包裹。采用包交换的好处是只有在有资料需要传送时才会占用频宽，而且可以以传输的资料量计价，这对用户来说是比较合理的计费方式。GPRS 是一种新的 GSM 数据业务，它在移动用户和数据网络之间提供一种连接，给移动用户提供高速无线 IP 和 X.25 分组数据接入服务。GPRS 采用分组交换技术，它可以让多个用户共享某些固定的信道资源。如果把空中接口上的 TDMA 帧中的 8 个时隙都用来传送数据，那么数据传输速率最高可达 164Kb/s。GSM 空中接口的信道资源既可以被话音占用，也可以被 GPRS 数据业务占用（Ahuja et al.，2014）。

7. 3G 技术

3G（3rd-generation）是指第三代移动通信技术。相对于第一代模拟制式手机（1G）和第二代 GSM、TDMA 等数字手机（2G），第三代手机是指将无线通信与国际互联网等多媒体通信结合起来的新一代移动通信系统，它能够处理图像、音乐、视频流等多种媒体形式，提供包括网页浏览、电话会议、电子商务等多种信息服务。为了提供这种服务，无线网络必须能够支持不同的数据传输速率，也就是说在室内、室外和行车的环境中能够分别支持至少 2Mb/s、384Kb/s 及 144Kb/s 的传输速率（魏传佳等，2016）。

8. 4G 技术

4G（4th-generation）是指第四代移动通信技术，它集 3G 与 WLAN 于一体，并能够传输高质量的视频图像，它的图像传输质量与高清晰度电视不相上下。4G 系统能够以 100Mb/s 的速度下载，比拨号上网快 2000 倍，上传的速度也能达到 20Mb/s，并能够满足几乎所有用户对于无线服务的要求。而在用户最为关注的价格方面，4G 与固定宽带网络不相上下，而且计费方式更加灵活、机动，用户完全可以根据自身的需求选择所需的服务（魏传佳等，2016）。此外，4G 可以在 DSL（digital subscriber line，数字用户线路）和有线电视调制解调器没有覆盖的地方部署，然后扩展到整个地区。

9. 5G 技术

5G（5th-generation）是指第五代移动通信技术，与 4G、3G、2G 不同的是，5G 并不是独立的、全新的无线接入技术，而是对现有无线接入技术（包括 2G、3G、4G 和 Wi-Fi）的演进，及对一些新增的补充性无线接入技术集成后解决方案的总称（Hu et al.，2014）。从某种程度上讲，5G 将是一个真正意义上的融合网络，以融合和统一的标准，提供人与人、人与物及物与物之间高速、安全和自由的联通。目前，3GPP（Third generation partnership project，第三代合作伙伴计划）全会（TSG＃80）批准了第五代移动通信技术标准（5G NR）独立组网功能冻结。加之 2017 年 12 月完成的非独立组网 NR 标准，5G 已经完成第一阶段全功能标准化工作，进入了产业全面冲刺新阶段。

1.2.3 无线网络类型

无线网络是采用无线通信技术实现的网络，根据网络覆盖范围、传输速率和用途的差异，大体可分为无线广域网、无线局域网、无线个域网和无线城域网。

1. 无线广域网

无线广域网（wireless wide area network，WWAN）技术可使用户通过远程公用网络或专用网络建立无线网络连接。通过使用由无线服务提供商负责维护的若干天线基站或卫星系统，这些连接可以覆盖广大的地理区域，如若干城市或者国家（地区）。

2. 无线局域网

无线局域网（wireless local area network，WLAN）具有可移动性、安装简单、高灵活性和扩展能力，作为对传统有线网络的延伸，在许多特殊环境中得到了广泛的应用。随着无线数据网络解决方案的不断推出，“不论你在任何时间、任何地点都可以轻松上网”这一目标被轻松实现了。无线网络的应用扩展了用户的自由度，还具有安装时间短，增加用户或更改网络结构方便、灵活、经济，可以提供无线覆盖范围内的全功能漫游服务等优势。然而，无线网络技术为人们带来极大方便的同时，安全问题已经成为阻碍无线网络技术应用普及的一个主要障碍（Bhattarai et al.，2015）。

无线局域网采用公共电磁波作为载体，任何人都有条件窃听或干扰信息，因此，在一开始应用无线网络时，就应该充分考虑其安全性。

无线局域网由无线网卡、无线接入点（access point，AP）、计算机和有关设备组成，采用单元结构，将整个系统分成多个单元，每个单元称为一个基本服务集（basic service set，BSS），BSS 的组成有无中心的分布对等方式、有中心的集

中控制方式及这两种方式的混合方式。在无中心的分布对等方式下，无线网络中的任意两站之间可以直接通信，无须设置中心转接站，这时，介质访问控制（medium access control，MAC）功能由各站分布管理。在有中心的集中控制方式下，要在无线网络中设置一个中心控制站，主要完成 MAC 及信道的分配等功能，网内的其他各站在该中心的协调下与其他各站通信。第三种方式是前两种方式的组合，在这种方式下，网络中的任意两站均可以直接通信，而中心控制站完成部分无线信道资源的控制（Mohammadizadeh et al.，2013）。

3. 无线个域网

无线个域网（wireless personal area network，WPAN）技术使用户能够为个人操作空间（personal operation space，POS）设备（如 PDA、移动电话和笔记本电脑等）创建临时无线通信。POS 指的是以个人为中心，最大距离为 10m 的一个空间范围。目前，两个主要的为 POS 创建临时无线通信的技术是蓝牙和红外线。蓝牙是一种电缆替代技术，蓝牙数据可以穿过墙壁、口袋和公文包进行传输。蓝牙专门利益组（Special Interest Group，SIG）推动着蓝牙技术的发展，于 1999 年发布了蓝牙版本 1.0 规范。作为替代方案，要近距离（1m 以内）连接设备，用户还可以创建红外连接（Maltz et al.，2016）。

为了规范无线个域网技术的发展，IEEE 已经为无线个域网成立了 802.15 工作组。该工作组正在发展基于蓝牙版本 1.0 规范的 WPAN 标准，该标准草案的主要目标是低复杂性、低能耗、交互性强并且能与 IEEE 802.11 网络共存（Maltz et al.，2016）。无线个域网和无线局域网并不一样。无线个域网是以个人为中心使用的无线个人区域网，它实际上就是一个低功率、小范围、低速度和低价格的电缆替代技术。但无线局域网却是同时为许多用户服务的无线网络，它是一个大功率、中等范围、高速率的局域网。

最早使用的 WPAN 是 1994 年爱立信公司推出的蓝牙系统，其标准是 IEEE 802.15.1。蓝牙的数据传输速率为 1Mb/s，通信范围在 10m 左右。为了适应不同用户的需求，无线个域网还定义了另外两种低速 WPAN 和高速 WPAN（Bellofiore et al.，2015）。其中，低速 WPAN 的标准是 IEEE 802.15.4，其传输速率一般在 2～250Kb/s；高速 WPAN 的标准是 IEEE 802.15.3，目前应用超宽带技术的高速 WPAN 传输速率可达 100～400Mb/s。

4. 无线城域网

无线城域网（wireless metropolitan area network，WMAN）技术使用户可以在城区的多个场所之间创建无线连接（如在一个城市或大学校园的多个办公楼之间），而不必花费高昂的费用铺设光缆、铜质电缆和租用线路。此外，当有线网络的主要租赁线路不能使用时，无线城域网还可以作为备用网络使用。无线城域网

使用无线电波或红外光波传送数据。为用户提供高速 Internet 接入的宽带无线接入网络的需求量日益增长。尽管目前正在使用各种不同技术，如多路多点分布服务（multichannel multipoint distribution service，MMDS）和本地多点分布服务（local multipoint distribution service，LMDS），但负责制定宽带无线访问标准的 IEEE 802.16 工作组仍在开发规范，以便实现这些技术的标准化（Seppanen et al.，2015）。

无线城域网服务范围可覆盖整个城市或城市的部分区域，通信的距离变化较大（远的可达 50km），接收到的信号功率和信噪比等也会有很大的差别。这就要求有多种调制方法，因此工作在毫米波段的 IEEE 802.16 必须有不同的物理层。IEEE 802.16 的基站可能需要多个定向天线，各指向对应的接收点。由于天气条件（雨、雪、雹、雾等）对毫米波的传输影响较大，与室内工作的无线局域网相比较时，IEEE 802.16 对差错的处理更为重要（Seppanen et al.，2015）。

1.3　无线网络安全现状

随着无线网络在各行各业的应用不断深入，无线网络出现的安全问题也越来越多。通过对无线网络面临的安全问题进行分析，可将常见的无线网络安全技术分为服务集标识符、物理地址过滤、有线等效保密、Wi-Fi 保护接入、无线局域网鉴别与保密基础结构、端口访问控制技术等。

1.3.1　无线网络与有线网络的区别

由于无线网络通过无线电波在空中传输数据，在数据发射机覆盖区域内几乎所有的无线网络用户都能接触到这些数据（王甜甜等，2016）。只要具有相同接收频率就可能获取所传递的信息。要将无线网络环境中传递的数据仅仅传送给一个目标接收者是不可能的。另外，无线移动设备在存储能力、计算能力和电源供电时间方面的局限性，使得原来在有线环境下的许多安全方案和安全技术不能直接应用于无线环境。例如，防火墙对通过无线电波进行的网络通信起不了作用，任何人在区域范围之内都可以截获和插入数据（Sharma et al.，2016）；计算量大的加密解密算法不适用于移动设备等。因此，需要研究新的适合于无线网络环境的安全理论、安全方法和安全技术。与有线网络相比，无线网络所面临的安全威胁更加严重。所有常规有线网络中存在的安全威胁和隐患都存在于无线网络中；外部人员可以通过无线网络绕过防火墙，对专用网络进行非授权访问；无线网络传输的信息容易被窃取、篡改和插入；无线网络容易受到拒绝服务攻击（denial of service，DoS）和干扰；内部员工可以设置无线网卡以端对端的模式与外部员工直接连接。此外，无线网络的安全技术相对比较新，安全产品还比较少。以无线局域网为例，移动节点、AP 等每一个实体都有可能是攻击对象或攻击者。由于无线网络在移动设备和传输媒介方面的特殊性，一些攻击更容易实施，对无线网络

安全技术的研究比有线网络的限制更多，难度更大。无线网络在信息安全方面与有线网络有不同之处，具体表现在以下4个方面。

1）无线网络的开放性使其更容易受到恶意攻击。无线链路使网络更容易受到从被动窃听到主动干扰的各种攻击。有线网络的网络连接是相对固定的，具有确定的边界，攻击者必须物理接入网络或经过几道防线，如防火墙和网关，才能进入有线网络。在有线网络中，通过对接入端口的管理可以有效地控制非法用户的接入，而无线网络则没有一个明确的防御边界，攻击者可能来自四面八方和任意节点，每个节点必须面对攻击者直接或间接的攻击。无线网络的这种开放性带来了非法信息截取、未授权信息服务等一系列信息安全问题。

2）无线网络的移动性使安全管理难度加大。有线网络的用户终端与接入设备之间通过线缆连接，终端不能在大范围内移动，对用户的管理比较容易。而无线网络终端不仅可以在较大范围内移动，还可以跨区域漫游，这意味着移动节点没有足够的物理防护，从而易被窃听、破坏和劫持。一方面，攻击者可能在任何位置通过移动设备实施攻击，而在全球范围内跟踪一个特定的移动节点是很难做到的；另一方面，通过网络内部已经被入侵的节点实施攻击而造成更大的破坏，从而更难被检测到。因此，对无线网络移动终端的管理困难得多，无线网络的移动性带来了新的安全管理问题，移动节点及其体系结构的安全性更加脆弱。

3）无线网络动态变化的拓扑结构使安全方案的实施难度加大。有线网络具有固定的拓扑结构，安全技术和方案较容易实现。而在无线网络环境中，一方面，动态变化的拓扑结构缺乏集中管理机制，使安全技术更加复杂；另一方面，无线网络环境中做出的许多决策是分散的，而许多网络算法必须依赖所有节点的共同参与和协作，缺乏集中管理机制，意味着攻击者可能利用这一弱点实施新的攻击破坏协作算法。

4）无线网络传输信号的不稳定性带来无线通信网络的健壮性问题。有线网络的传输环境是确定的，信号质量稳定，而无线网络随着用户的移动，其信道特性是变化的，会受到干扰、衰落、多径、多普勒频谱等多方面的影响，造成信号质量波动较大，甚至无法进行通信（Sharma et al.，2016）。此外，移动计算引入了新的计算和通信行为，这些行为在固定或有线网络中很少出现。例如，移动用户通信能力不足，其原因是链路速度慢、带宽有限、成本较高、电池能量有限等。而无线连接操作和依靠地址运行的情况只出现在移动无线环境中。因此，有线网络中的安全措施不能应付基于这些新的应用而产生的攻击。无线网络的脆弱性是由其媒体的开放性、终端的移动性、动态变化的网络拓扑结构、协作算法、缺乏集中监视和管理点及没有明确的防线造成的。因此，在无线网络环境中，设计实现一个完善的无线网络系统时，除了要考虑在无线传输信道上提供完善的移动环境下的多业务服务平台外，还必须考虑其安全方案的设计，这包括用户接入控制设计、用户身份认证方案设计、用户证书管理系统设计、密钥协商及密钥管理