无线通信前沿技术丛书
李少谦 周亮 主编

该书由国家自然科学基金（No.61032003和No.61071100）、新世纪优秀人才计划（NCET-09-0266）和东南大学移动通信国家重点实验室开放课题基金（2010D05）联合资助

“十二五”
国家重点
出版规划丛书

无线通信的可靠和安全编码

● 文 红◎著

Reliable and Security Coding for Wireless Communication

国防工业出版社
National Defense Industry Press

无线通信前沿技术丛书/李少谦　周亮　主编

该书由国家自然科学基金(No. 61032003 和 No. 61071100)、新世纪优秀人才
计划(NCET-09-0266)和东南大学移动通信国家重点实验室开放课
(2010D05)联合资助

无线通信的可靠和安全编码

Reliable and Security Coding for Wireless Communication

文红　著

国防工业出版社

·北京·

内容简介

本书介绍了无线通信系统的物理层可靠和安全通信的概念和框架。在详细介绍先进信道编码——Turbo 码和 LDPC 码的编、译码基本原理及各种译码算法基础上，分析了基于信道编码的无条件秘密通信系统的建立以及秘密安全编码设计标准；给出几类秘密编码的设计和安全性能。各章原理的叙述力求突出概念清晰，注重理论推导和仿真试验验证相结合。全书对材料的阐述循序渐进；在内容上既有必要的数学和信息论基础，又着重于物理概念的解释。本书在编写中充分考虑了不同层次读者的需求，读者可以通读，也可以根据需要选择相关章节阅读。本书适用对象为高等院校信息类各专业本科高年级、研究生、教师及科研院所从事无线通信可靠性和安全性等领域研究的科研和工程技术人员。

图书在版编目(CIP)数据

无线通信的可靠和安全编码 / 文红著. —北京：国防工业出版社，2011.5

（无线通信前沿技术丛书 / 李少谦，周亮主编）

ISBN 978-7-118-07469-7

Ⅰ. ①无… Ⅱ. ①文… Ⅲ. ①无线电通信－最佳编码 Ⅳ. ①TN92

中国版本图书馆 CIP 数据核字(2011)第 070375 号

※

国防工业出版社出版发行

（北京市海淀区紫竹院南路 23 号　邮政编码 100048）

腾飞印务有限公司印刷

新华书店经售

*

开本 787×1092　1/16　**印张** 10¼　**字数** 222 千字

2011 年 5 月第 1 版第 1 次印刷　**印数** 1—4000 册　**定价** 32.00 元

（本书如有印装错误，我社负责调换）

国防书店：(010)68428422　　发行邮购：(010)68414474

发行传真：(010)68411535　　发行业务：(010)68472764

序　言

在移动互联网和无线多媒体数据业务的巨大需求推动下，无线通信技术将持续快速发展，移动互联网用户不但要求无线移动通信能够传输大容量的信息，还希望信息传输能更加保密、更加安全。

为了实现这个目标，无线通信正在发展很多新技术，这些新技术将大大提高无线通信系统的数据传输速率和通信的可靠性，增强系统的安全性能。长期以来通信的可靠性和安全性都被认为是两个独立的领域，提高通信传输可靠性的重要手段是物理层的信道编码，传统的通信安全体制建立在信息加密的基础上，而信息加密处理在物理层之上。

1975 年，贝尔实验室的 Wyner 在其论文中首次提出在物理层统一实现通信的可靠性和安全性，提出了基于编码调制的安全新技术——物理层安全技术。物理层安全技术是利用信道特性、编码、调制等一系列通信传输方法来建立安全的通信模型，通信的双方不需要共享加密密钥，不需要复杂的加密解密算法。

随着 Turob 码的提出和 LDPC 码的“再发现”，Shannon 提出的可靠传输“Shannon 极限”得以实现，人们开始重新思考 Shannon 提出的“一次一密”绝对安全系统实现问题。2003 年，密歇根大学的 Hero 在其论文中重新提出物理层安全技术，使得 Wyner 的理论重新焕发光彩，并成为研究的热点，其被学者们认为是可以实现“一次一密”安全体制的新技术。

本书在系统介绍 LDPC 码和 Turbo 码的基本原理、分析方法和应用的基础上，介绍了无线通信中基于信道编码的物理层安全技术概念和框架，对无线移动通信信道模型下的物理层安全系统进行了剖析，对基于信道编码的“秘密编、译技术”进行了分析。

本书是作者从事无线通信可靠性和安全性跨领域交叉研究的重要成果，对于有志于从事无线通信可靠性和安全性理论及应用研究的人员来说，本书有助于引导其快速进入该研究领域，同时本书的出版将促进无线通信可靠性和安全性新技术的发展，并促进新技术在下一代移动通信中的应用。

李少谦

2011 年 4 月于成都

前　言

无线通信信道受干扰和噪声影响大，无线链路的不可靠性和物理层广播特性使得如何保证信息的安全无误接收成为关键，纠错编码是提高传输可靠性的重要手段。1948 年香农(Shannon)在他的开创性论文《通信的数学理论》中，首次阐明了在有噪信道实现可靠通信的方法，提出了著名的有噪信道编码定理，1993 年 Turbo 码的出现和 LDPC 码在 1996 年的“再发现”使得信道编码技术进入了一个崭新的时代，接近香农容量限的信道编码使得无线通信的可靠接收成为可能。

1949 年香农的另外一篇重要论文《保密系统的通信理论》奠定了现代通信安全的基础，在这篇文章中指出只有“一次一密”的安全体制才是绝对安全的。传统安全通信系统在上层通过现代密码学的理论为基础建立了一套安全体系，但这种体制依赖于数学的运算能力有限性，随着计算机运算能力的加强，现有的保密算法都将不再安全。物理层安全技术在通信双方不需要共享加密密钥，不需要复杂的加密解密算法，利用信道特性、编码、调制等一系列通信传输方法来建立安全的通信模型，而不依赖数学的计算能力有限性。而物理层安全技术的核心之一就是安全编码，安全编码在保证合法通信双方的可靠通信基础上，使得非法截获者只能收到完全淹没在噪声中的信号，其被认为是可能实现香农的“一次一密”安全体制的新技术。

本书介绍了 Turbo 码和 LDPC 码的编、译码基本原理及各种译码算法；详细分析了 LDPC 码的特点、分析方法；对无线移动通信信道模型下 LDPC 码的性能进行了剖析。在此基础上对物理层信息安全的概念和框架进行了介绍；分析了基于信道编码的无条件秘密通信的秘密编码设计标准；给出几类秘密编码的设计和性能。各章原理的叙述力求突出概念清晰，注重理论推导和仿真试验验证相结合。

全书共分为两部分。第一部分主要介绍 LDPC 码和 Turbo 码的编、译码基本原理、分析方法及应用，包括第 1 章到第 6 章；第二部分主要介绍物理层信息安全的框架和秘密编码的概念，包括第 7 章到第 9 章。

本书编写过程中参考了众多的国内、外参考文献，在本书最后均列出，在此对参考文献的作者表示感谢。

作者要感谢加拿大滑特卢大学的龚光教授，是她引领作者走入安全编码的研究新领域，还要感谢电子科技大学的吕世超、杨铃、宋时立、韩祺祎等的支持，在本书的编写中进行了认真的文本校对。

在这里，要特别感谢电子科技大学通信抗干扰试验室的李少谦教授为本书作序，正是通信抗干扰实验室的科研氛围和各方面的支持使作者能在短时间内完成本书的撰写。

由于作者水平有限，错误、遗漏之处在所难免，恳请专家和读者批评指正。

目　录

第1章 绪 论

1.1 无线通信系统的结构

无线通信网可以随时随地地进行数据通信，减少了对有线连接的要求，提高了网络的灵活性，并且因其可移动性、组网灵活性、应用范围的广泛性和传输速度快等优点，使得其在当前个人家庭和办公环境逐渐开始广泛应用。

无线通信（或称无线电通信）的类型很多，可以根据传输方法、频率范围、用途等分类。不同的无线通信系统，其设备组成和复杂度有较大差异，但它们的基本组成不变，图1-1是无线通信系统基本组成的方框图。

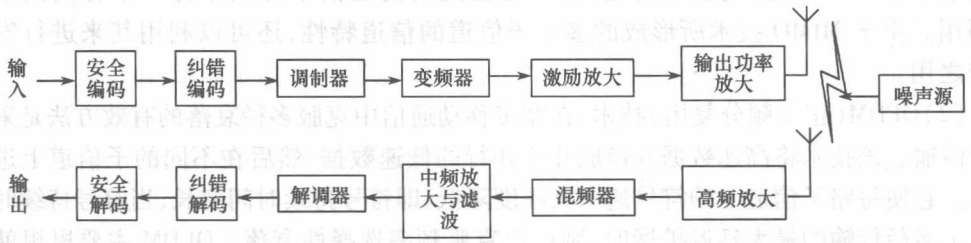


图1-1 无线通信系统基本组成

自1978年第一个蜂窝移动通信系统AMPS（先进移动电话系统）研制成功以来，无线通信大致经历了第一代、第二代、第三代移动通信系统的三个不同的发展阶段。第一代无线通信系统以蜂窝小区设计技术的应用为标志。第二代移动通信系统兴起于20世纪90年代。第二代移动通信系统在商业的应用中取得了巨大的成功，从而带动了全球范围内的移动通信用户数量急剧增加。欧洲的GSM、美国的DAMPS和CDMA（IS-95）以及日本的PDC是第二代移动通信系统的主要代表。

随着移动用户数目的快速增长，促使移动通信系统急于解决如何进一步提高系统的频谱利用率和增大系统容量的问题。同时，由于近几年互联网的快速发展以及普及，人们不再满足于单一的话音业务，而希望移动通信系统具有承载包括视频、图像等在内的多媒体业务能力，加之移动互联网概念的提出，这一切对第二代移动通信系统提出了严峻的挑战，其低的数据率以及单一的业务传输体制无法达到这些要求。为实现任何人在任何时间、地点以任何方式与任何人进行通信的目标，ITU提出了第三代移动通信系统（3G）的研究，并于1998年后确定了最终的无线传输技术（RTT）标准。第三代移动通信系统又称为IMT-2000，到目前为止，主要有三种主流的技术标准：欧洲标准WCDMA、美国标准CDMA2000和中国标准TD-SCDMA。一般认为CDMA通信技术与宽带业务是第三代移动通信系统的主要标志。

虽然3G的标准和规范已达成协议，并且已经开始商用，但是第三代移动通信系统还是面临着更高的无线通信需求的挑战。尤其是3G仍然采用第二代移动通信系统的电路交换方式，而非纯IP方式进行通信，这就使得第三代移动通信系统与Internet的融合、移动互联网络的建立和无线宽带多媒体系统的实现比较困难。同时，3G无线传输的速率依然无法满足使用的需求。因此，新一代移动通信系统（B3G/4G）的概念应运而生。有关4G的研究已经取得了丰硕的成果。相对于3G而言，第四代无线通信系统（4G）在技术和应用上将有质的飞跃。为了满足高速率的数据传输与灵活多样的通信业务，第四代移动通信系统采用了一系列新技术。在这些技术中，与信号传输有关的技术包括：

（1）MIMO（多输入多输出）技术：MIMO技术通过利用多发射、多接收天线进行空间分集的技术，将通信链路分解成为许多并行的空间子信道。利用MIMO信道提供的空间分集增益，可以提高信道的可靠性，降低误码率，同时利用MIMO信道提供的空间复用增益，可以提高信道的容量。通常，无线通信的多径要引起衰落，因而被视为有害因素。然而研究结果表明，对于MIMO系统来说，传输信息流多个天线发射出去，经空间多个子信道后由多个接收天线接收，多天线接收机利用先进的空时编码处理能够分开并解码这些数据子流，从而实现最佳的处理，多径在此时的通信中可以作为一个有利因素加以利用。由于MIMO技术所形成的多个子信道的信道特性，还可以利用其来进行安全加密之用。

（2）OFDM（正交频分复用）技术：在宽带移动通信中克服多径衰落的有效方法是采用并行传输。该技术将高速数据变换成几路并行的低速数据，然后在不同的子信道上进行传输。它使每路子信道上的符号速率大幅度降低，即符号持续时间变长，当符号持续时间远大于多径传输的最大延迟扩展时，则可以克服频率选择性衰落。OFDM主要思想就是在频域内将给定信道分成许多正交子信道，在每个子信道上使用一个子载波进行调制，各子载波并行传输。一般的多载波传输使用互不交叠的频分复用多载波，为减少各载波间相互干扰，通常各载波间要有一个保护频带，这就造成了系统带宽资源的浪费。而OFDM这种多载波调制技术就避免了这一浪费，它把高速数据流分散到多个正交的子载波上并行传输，各子载波之间允许交叠，但由于各子载波之间相互正交，载波间干扰可以为零，因此可以保证系统带宽资源充分利用。OFDM技术在第四代移动通信系统不仅会单独使用，同时也可以与其他多址接入方案（如TDMA/FDMA/CDMA等）相结合，以此提供无线链路资源利用方面的灵活性，同时支持用户传输速率的动态分配。

（3）高性能调制与编码技术：新一代移动通信系统对服务质量提出了高的要求，因此其将采用更高级的信道编码方案，如Turbo码、级联码和LDPC等，同时配合自动重发差错控制技术和分集接收技术，从而保证在高速率传输条件下能获取良好的系统服务性能。同时也采用新的调制技术，如多载波正交频分复用调制技术以及高阶调制技术，并和纠错编码结合成为根据通信环境自适应选择的自适应编码调制方式，以保证无线频谱资源能有效利用，同时提高单位带宽上的传输速率。

1.2 信道编码技术概述

伴随着通信技术的飞速发展以及各种传输方式对可靠性要求的不断提高，差错控制

编码技术成为抗干扰技术的一种重要手段，在数字通信领域和数字传输系统中显示出越来越重要的作用。由于通信信道固有的噪声和衰落特性，信号在经过信道传输到达通信接收端的过程中不可避免地会受到干扰而出现信号失真。通常需要采用差错控制码来检测和纠正有信道失真引起的信息传输错误。最早的纠错码主要是用于深空通信和卫星通信，随着数字蜂窝电话、数字电视以及高分辨率数字存储设备的出现，编码技术的应用已经不仅仅局限于科研和军事领域，而是逐渐在各种实现信息交流和存储的设备中得到成功应用。

1948 年香农发表的著名的《通信的数学理论》一文，为信道编码技术的发展指明了方向。香农在著名的有噪信道编码定理中，给出了在数字通信系统中实现可靠通信的方法以及在特定信道上实现可靠通信的信息传输速率上限。香农在他的证明中引用了三个基本条件：

(1)采用随机的编译码方法。

(2)构造码长的渐进好码或香农码。

(3)译码采用最佳的最大似然译码算法。

50 多年来构造好码的思想基本上是按照香农所引用的基本条件的后两条为主线进行研究的。经过 50 年的不懈努力，各种差错控制编码方案不断涌现。

在 20 世纪 40 年代，R. Hamming 和 M. Golay 提出了第一个实用的差错控制编码方案，使编码理论这个应用数学分支的发展得到了极大的推动。Hamming 所采用的方法就是将输入数据每 4 个比特分为一组，然后通过计算这些信息比特的线性组合来得到 3 个校验比特。然后将得到的 7 个比特送入计算机。计算机按照一定的原则来读取这些码字，通过采用一定的算法，不仅能够检测到是否有错误发生，同时还可以找到发生单个比特错误的比特位置，该码可以纠正 7 个比特中所发生的单个比特错误。这个编码方法就是分组码的基本思想，Hamming 提出的编码方案后来被命名为汉明码。

虽然汉明码的思想是比较先进的，但是它也存在许多难以接受的缺点。首先，汉明码的编码效率比较低，它每 4 个比特编码就需要 3 个比特的冗余校验比特。另外，在一个码组中只能纠正单个的比特错误。M. Golay 研究了汉明码的这些缺点，并提出了两个以他自己的名字命名的高性能码字：一个是二元 Golay 码，在这个码字中 Golay 码将信息比特每 12 个分为一组，编码生成 11 个冗余校验比特。相应的译码算法可以纠正 3 个错误。另外一个是三元 Golay 码，它的操作对象是三元而非二元数字。三元 Golay 码将每 6 个三元符号分为一组，编码生成 5 个冗余校验三元符号。这样由 11 个三元符号组成的三元 Golay 码码字可以纠正 2 个错误。

1954 年 Reed 在 Muller 提出的分组码的基础上得到了一种新的分组码，称为 Reed-Muller 码(简记为 RM 码)。RM 码在汉明码和 Golay 码的基础上前进了一大步，在码字长度和纠错能力方面具有更强的适应性，RM 码是一类参数选择范围很广的分组码。1969 年到 1977 年之间，RM 码在火星探测方面得到了极为广泛的应用。即使在今天，RM 码也具有很大的研究价值，其快速的译码算法非常适合于光纤通信系统。

在 RM 码提出之后人们又提出了循环码的概念。循环码实际上也是一类分组码，但它的码字具有循环移位特性，即码字比特经过循环移位后仍然是码字集合中的码字。这种循环结构使码字的设计范围大大增加，同时大大简化了编译码结构。循环码是线性码

循环码的另外一个特点，就是一个给定的(N,K)码可以用一个幂次为$N-K=R$的生成多项式来表示，循环码也称为循环冗余校验(Cyclic Redundancy Check，CRC)码，并且可以用Meggitt译码器来实现译码。

Hocquenghem在1959年，Bose和Ray-Chaudhuri研究组在1960年几乎同时提出了BCH码(Bose Chaudhuri Hocquenghem，BCH)，BCH码是循环码的一个非常重要的子集，BCH码是汉明码的延伸，属于线性循环分组码，根据不同的码长与码率，这种码字可以纠正任意t个错误。对于任意正整数$m\geqslant 3$，$t<2^{m-1}$，存在(n,k)BCH码，码长$n=2^m-1$，每个码字纠正t个错误，校验位数$n-k\leqslant mt$，最小汉明距离$d_{\min}\geqslant 2t+1$。1960年Reed和Solomon将BCH码扩展到了非二元的情况，得到了RS(Reed-Solomon)码。RS码的最大优点是其非二元特性可以纠正突发错误。但直到1967年Berlekamp给出了一个非常有效的译码算法之后，RS码才得到了广泛的应用。此后，RS码在CD播放器、DVD播放器以及CDPD(Cellular Digital Packet Dara)标准中都得到了很好的应用。

1955年Elias等人提出了卷积码，卷积码与分组码的不同在于分组码在编码之前先将信息序列按照一定的数据块长度分组，然后对每一组信息进行独立编码，即对于分组码来说，码字中的$n-k$个检验元仅与本码字的k个信息元有关，而与其他码字的信息元无关。

Forney在1966年提出两个短码构造长的串行级联的思想。其基本思想是将编制长码的过程分级完成，从而通过用短码级联构造长码的方法来提高纠错码的纠错能力。级联码的目标是构造具有较大等效分组长度的纠错码，并且允许将最大似然译码分为几个较简单的译码步骤，这样便得到一个次最优但实际可行的译码策略。其纠错能力强，译码也不复杂，展现了构造香农码的美好前景。

20世纪70年代期间，在构造香农码中一个重要成果是1972年由Justeson用级联构造的Justeson码，另一个重要成果是苏联学者Goppa用有理分式表示码字基础上所构造的Goppa码，其渐进性很好，但n很长时，真正构造出这种好码仍然很困难。构造香农码的一个重要突破是20世纪80年代初由Goppa提出的代数几何码。他将代数几何的理论和方法系统地应用于编码理论中，使得原来线性码中的重要参数如码长、距离、维数等具有全新的几何意义，代数几何码的研究成为80年代和90年代编码领域中研究热点之一。

传统通信系统的最佳接收机中解调器和译码器是独立的两个部分。在处理接收信号的过程中，解调器首先对调制器输入符号做最佳判决，然后将硬判决结果送给译码器；译码器再对编码器输入消息做最佳判决，纠正解调器可能发生的错误判决，这是硬判决译码的思想。事实上，经过解调器对符号的硬判决，丢失了很多有利于译码的信息。为了提高编码通信系统的性能，人们从信息论的角度对接收机中解调器与信道译码器的功能划分和接口重新审视，提出了软判决译码方法，即解调器对输出不进行判决，送到译码器的是判决符号可能的概率值或未量化输出，而非硬判决值，则译码器就可以利用这些信息与编码信息综合做出判决，从而提高系统性能，这就是软判决译码的基本思想。研究表明，在接收机中解调器采用软输出可以得到比硬输出高2dB左右的附加编码增益。

软判决译码算法主要分为两大类：一类是使符号错误概率最小的逐位软判决译码算法，如1974年有Bahl、Cocke、Jelinek和Raviv共同提出的前向后向最大后验概率(MAP)

译码算法(也称为 BCJR 算法)和 Lee 提出的前向 MAP 算法,1976 年 Hartman 和 Rudolph 提出的逐位译码算法(HR 算法)以及 1971 年 Weldon 提出的重量删除译码算法(WED 算法)等。另一类是使码字错误概率最小的逐组软判决译码方法,如 1966 年 Forney 提出的广义最小距离译码(GMD)算法、1972 年 Chase 提出的 Chase 算法以及 1967 年 Viterbi 提出的 Viterbi 译码算法等。

1974 年 J. Massey 提出了将编码与调制作为一个整体看待可能会提高系统性能的设想。此后,许多学者研究了将此设想付诸于实践的途径。其中,1982 年 Ungerboeck 提出的 TCM 概念是解决带宽和纠错这对矛盾的一个理想方案,它将纠错编码技术与调制技术有机结合,在不增加系统带宽要求的条件下通过扩展符号映射空间来达到提高编码增益的目的。TCM 技术奠定了限带信道上编码调制技术的研究基础,被认为是信道编码发展中的一个里程碑。另外,几乎在同一时期日本学者 Imai 提出了一种采用分组码的编码调制技术,称为 BCM(Block Coding Modulation)技术。它在衰落信道中的性能比较突出。

虽然软判决译码、级联码和编码调制技术都对信道码的设计和发展产生了重大影响,但是其增益与香农限始终都存在 2dB ~ 3dB 的差距。因此,在 Turbo 码提出以前,信道截止速率一直被认为是差错控制码性能的实际极限,香农限仅仅是理论上的极限,在实际中是不可能达到的。

直到 1993 年 Turbo 码的提出,1996 年再发现的低密度校验(Low Density Parity Check,LDPC)码,让人们看到了逼近香农限的可能。

1.3 无线通信安全

随着互联网的出现和成功,结合大规模无线网络的发展,网络通信已经无处不在。然而,无处不在的在线服务则带来了更大的安全问题。例如,无线通信的广播特性使得通信更易受到窃听的威胁。数据的拦截和恶意使用将是一个很大的社会问题,因此安全通信的需求极大地增加了。

在无线通信发展中,由于第一代、第二代移动通信系统或者没有采取相应的安全措施或者安全措施并不完善,使得通信安全得不到保证,这样一来就给网络运营商带来了巨大损失。尽管在后来出现的两代无线通信网络中,信息安全机制在某种程度上得到了加强,但不可否认的是:通信的安全问题一直是无线通信一个不容忽视的问题。相比较而言,移动通信网络与传统的有线电话网络的显著区别就是移动通信网络的信息传输通道是无线信道。

除了标准的安全特性之外,无线系统还面临着由无线通信本身的开放特性引起的特定的安全弱点。首先,无线通信信道容易受到信道阻塞的攻击。攻击者能够很容易地阻塞物理通信信道,由此阻止合法用户访问网络。第二,没有适当的认证机制,攻击者可以使非授权的用户绕过像防火墙之类的安全基础设施而直接访问网络资源。最后,由于无线媒体先天的开放特性,在没有采用先进的技术设备的情况下,窃听很容易实现。在原理上,即使是网络中的合法用户也被认为是一个潜在的窃听者。

目前的无线通信网络大多数是采用传统的密码体系,利用传统的密码学的理论对数

据进行加密，可分为对称加密体系与非对称加密体系。对称加密体系通过一条绝对安全的信道首先在通信双方之间共享密钥，通过各种加密算法对数据进行加密处理，现在常用的 AES 就属于这种加密机制，这种机制可以实现很高的加密速率；非对称加密体制即公钥密钥体制，通信中公钥被所有人可见，但密钥只有接收方所有，发送方使用公钥对数据加密，接收方使用只有自己知道的密钥对数据解密，著名的 RSA 就是这种机理，很显然，公钥密钥体系相对于对称密钥体系更安全，但运算缓慢。这两种体制都很大程度上依赖于计算机的运算能力，并且没有任何一种是绝对安全的，随着计算机运算能力的加强，现有的保密算法都将不再安全，保密算法也必须升级。

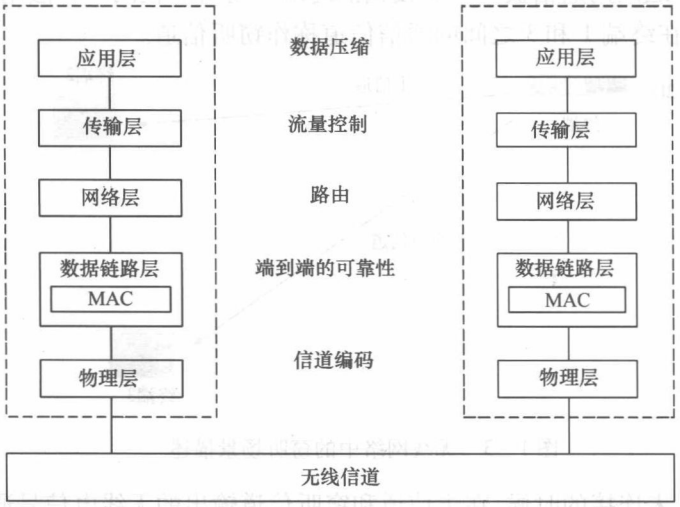
基于传统密码学的无线系统安全理论在安全性设计方面，都是与物理层独立分开并在物理层之上来应用这些密码体系的。然而传统的密码体制在无线通信中依然面临着巨大挑战，这就需要从另外一个角度来研究无线通信的安全性问题，即允许合法通信双方在不依赖密钥的条件下获得所需要的安全性条件。

从历史的观点看，图 1 -2(a)所描述的传统无线通信协议中的分层方法是针对简化通信协议而设计的，这些方法对安全性的考虑是很少的。以上提到的安全问题必须在这种分层的方式中得到解决。首先来看一下图 1 -2 所描述的各层的用途。信道编码被应用在物理层以确保所有上层无差错的信息传输，以及保证 MAC 层的控制处理。尽管现在的通信协议并不严格地按照这种分层方式而通常是跨层方式，为了表达的方便，在本文的以后各部分仍然使用传统的分层概念。

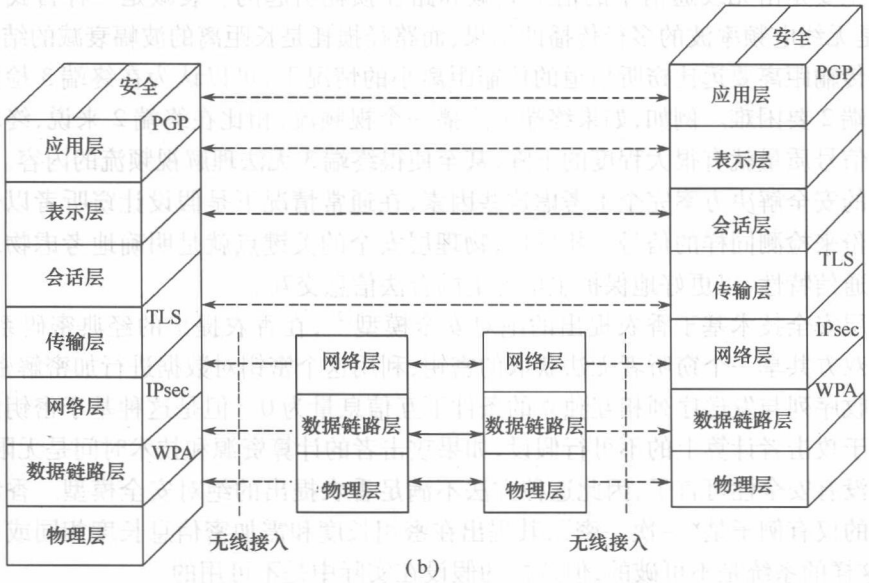
图 1 -2(b)列举了在不同协议层的几种安全性实现的机制：WPA(Wi-Fi Protected Access，Wi-Fi 保护接入)、IPsec(Iternet Protocol security，互联网 IP 协议安全)、TLS(Transport Layer Security，传输层安全)以及 PGP 加密机制，并显示出了它们实现时所处在的网络层次。明显可以看出，Wi-Fi 保护接入设计的层次是离物理层最近的，其次是 IP 协议安全，所有的这些安全机制都是运用在物理层之上的。

这些传统的安全机制几乎都存在着安全方面的漏洞，以 Wi-Fi 保护接入为例来说明其安全性方面存在的问题。在 Wi-Fi 保护接入的无线局域网中，其安全威胁主要来自于下面两个方面。(1)会话劫持(Session Hijack)攻击的威胁。当“公众热点(public-hotspot)”仅使用 802.1x 认证时，无线网络特别易受攻击。(2)在传统有线网络环境下，单向认证不存在问题，但在无线网络中，信息传输时就可能会遭到“非法窃听者”的攻击。如黑客对服务器伪装成客户端，而将无线客户端伪装成 AP(Access Point)，即无线访问接入点，这样黑客在经过单向认证之后，这个“非法窃听者”便充当中间人角色，来完全窃取无线信道中的任何数据。此外，在这些密码体制实现都有一个共同的假设：信息在物理层的传输是完美无差错的。然而对于无线信道而言，到目前为止，还没有足够的证据来表明这样的假设是完全成立的。

再比如，扩频调制技术是一个分层安全解决方案的例子，扩频调制用在物理层来减轻信道阻塞，认证机制用在链路层来阻止非授权的接入，信息加密应用在应用层阻止窃听。可以注意到，信道干扰和非授权接入分别是物理层和链路层的弱点，它们在各层中得到了很好的安全解决方案；然而，窃听仍然是物理层的一个弱点，但目前却是在应用层中解决的。人们自然地会问到：在物理层忽略这个物理现象是否是恰当的呢？以及是否存在在物理层解决这种窃听的方法呢？



(a)



(b)

图 1-2　无线通信安全与 ISO 的网络分层协议结构

(a)分层协议结构；(b)无线通信安全与 ISO 网络结构模型。

1.4　无线通信的物理层安全概述

物理层安全技术在通信双方不需要共享加密密钥，不需要复杂的加密解密算法，利用信道特性、编码、调制等一系列通信传输方法来建立安全的通信模型。在整个通信过程中，系统不需要绝对安全的信道进行密钥分发、密钥管理，即该系统是一个无条件安全通信系统。

为了描述物理层安全方案的一般概念，考虑使用如图 1-3 所示无线网络的例子，在

该图中终端1和2之间的通信被一个未授权的终端3窃听。在两个合法用户之间的通信信道称作主信道，在终端1和3之间的通信信道称作窃听信道。

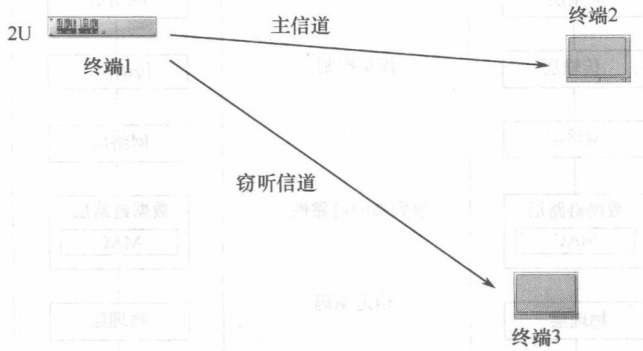


图1-3　无线网络中的窃听场景描述

当终端2和3未连接的时候，在主信道和窃听信道输出的无线电信号通常是不同的。这些差异主要是由无线通信中的信道衰减和路径损耗引起的。衰减是一种自我干扰现象，主要是无线电频率波的多径传播的结果，而路径损耗是长距离的波幅衰减的结果。在主信道的传输距离要远比窃听信道的传输距离小的情况下，可以认为在终端3检测信号要远比终端2要困难。例如，如果终端1广播一个视频流，相比在终端2来说，终端3处接收到的信号质量就有很大程度的下降，甚至使得终端3无法理解视频流的内容。目前，针对窃听的安全解决方案完全不考虑这些因素，在通常情况下是假设让窃听者以合法接收者的身份来检测同样的信号。相反地，物理层安全的关键点就是明确地考虑物理层的不同物理通信特性，以更好地保护主信道上的合法信息交互。

物理层安全技术基于香农提出的绝对安全模型[2]，在香农提出的经典密码系统中，合法通信双方共享一个窃听者无法获取的密钥，利用这个密钥对数据进行加密解密处理，窃听者接收序列与发送序列相互独立的条件下互信息量为0。但是这种基于密钥的秘密技术依赖于攻击者计算上的不可行假设，如果攻击者的计算资源和技术时间是无限的，则此时就是没有安全性可言了，因此这种方法不满足香农提出的绝对安全模型。香农绝对安全模型的仅有例子是“一次一密”，其提出在密钥长度和需加密信息长度相同或更长的情况下，这样的系统是不可破的，但这样的假设在实际中是不可用的。

Wyner在1973年提出了绝对安全模型的新解决思路——第一类窃听信道模型[3]，之后Csiszar与Korner对模型进行了改进[4]。在窃听信道模型中，发送方发送出的数据，合法接收者与窃听者同时收到了数据，假设窃听信道的信道质量劣于主信道，在这个条件下，证明了不依赖分享密钥即可实现绝对安全通信。但在实际中，很难保证窃听信道的信道质量劣于合法主信道，比如窃听者利用高功率的接收天线，轻易地就可以保证接收误码率低于合法接受者。上述模型中只是证明了可实现性，但并未提出合理的秘密编码方案以及窃听信道模型如何建立。

文献[5-7]提出了利用多天线系统的优势来构建完美秘密系统，文献[8]提出协同的方式有利于秘密消息的传输，文献[9]考虑了多点接入的双向窃听信道，文献[10]提出了利用LDPC码来构建窃听信道模型的方法，文献[11]提出了利用反馈信道的方式构建窃听信道模型。