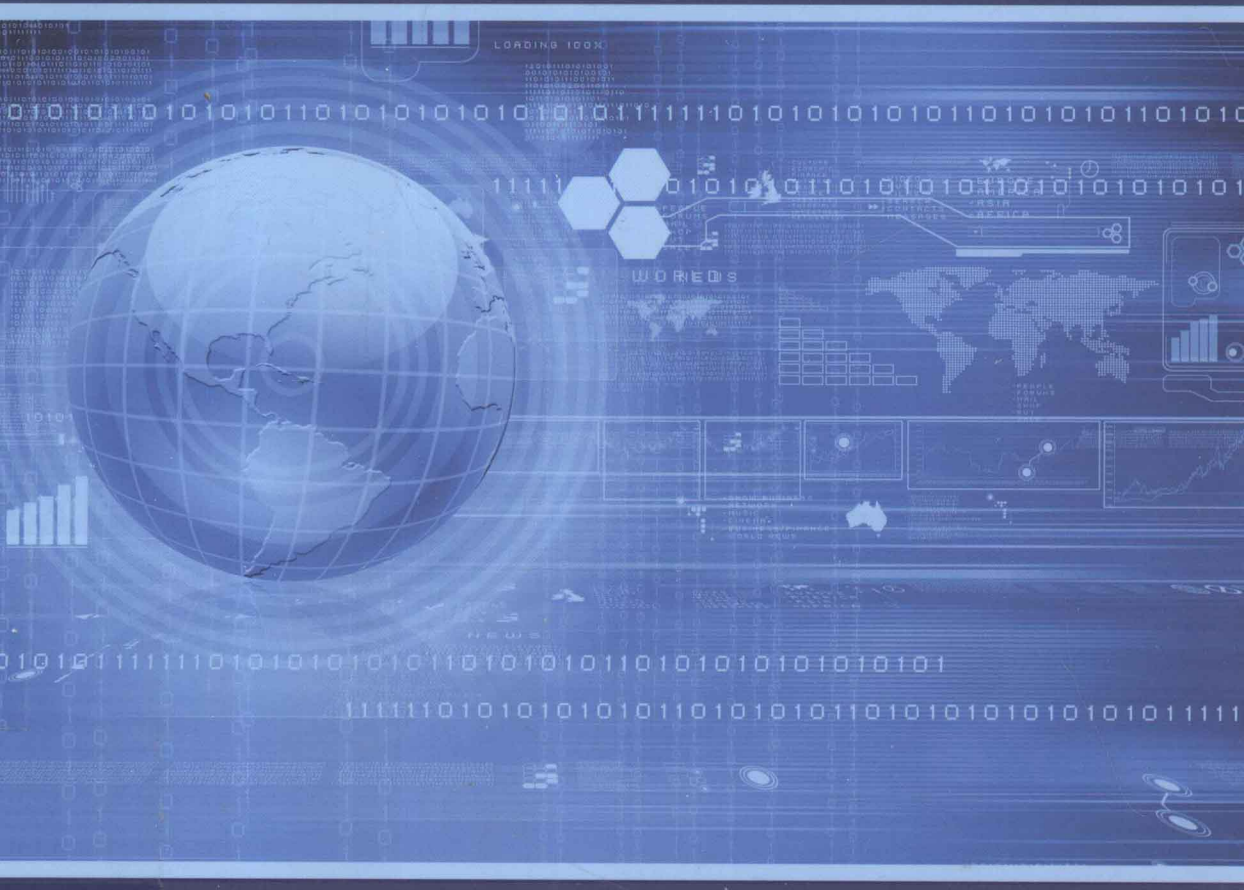
安全通信论

ANQUAN TONGXIN LUN

张焕炯 著



国防工业出版社
National Defense Industry Press

安全通信论

张焕炯　著

国防工业出版社

·北京·

内 容 简 介

本书是专门论述如何实现安全通信的论著。它以信息论与系统论等的观点和相应的研究方法为出发点，采用系统分析的方式，对不同模式下的通信安全问题进行了深入分析，在总结作者多年研究成果的同时，试图有机地结合通信理论与信息安全理论的相关理论，构建具有复合交叉性的新学科——“安全通信论”。

全书共分 8 章：第 1 章为绪言，从通信系统的基本概念出发，阐述了安全通信这一学科的基本特征和研究方法；第 2 章主要分析通信系统的基本模式；第 3 章主要论述安全通信理论研究的理论基础；第 4 章着重分析以加密算法和认证技术为主要内容的安全通信的基本手段和方法；第 5 章论述安全通信协议；第 6 章论述管理安全下的安全措施；第 7 章主要论述非技术因素的安全保障；第 8 章是对本书的总结和展望。

图书在版编目(CIP)数据

安全通信论/张焕炯著. —北京：国防工业出版社，2013.10

ISBN 978-7-118-09069-7

Ⅰ. ①安… Ⅱ. ①张… Ⅲ. ①通信系统—安全管理 Ⅳ. ①TN914

中国版本图书馆 CIP 数据核字(2013)第 238215 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)

北京嘉恒彩色印刷责任有限公司

新华书店经售

*

开本 710×1000　1/16　**印张** 15¾　**字数** 296 千字

2013 年 10 月第 1 版第 1 次印刷　**印数** 1—2000 册　**定价** 68.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)88540777　发行邮购：(010)88540776

发行传真：(010)88540755　发行业务：(010)88540717

前　言

随着通信技术的不断发展及通信在人们生产生活中的普及，通信设备越来越成为重要的社会基础设施，随之而来的通信的安全问题也日益显现，而解决这个问题的理论、技术、手段和举措等就构成了一个新颖的学科方向，可用“安全通信论”来概括。

早在20世纪四五十年代，Shannon就关注通信中的安全问题，他在提出了基于统计意义上的信息理论之后，在通信系统的优化指标中首次提出了安全性指标，并就保密通信等通信安全问题展开了卓有成效的研究，得到了著名的Shannon保密定理等。虽然Shannon只是研究基于点对点通信模式的安全性能，所获得的主要成果也是基于这种通信模式的，但他的研究工作仍具有非常重要的意义：一是由此开创了定量分析通信安全的先河，并把原本仅是保密工程实践中的具体技巧和经验提升为具有严格理论支撑的密码学理论；二是由此延展开来，它成为安全通信学理论的重要组成部分，更由于点对点的通信模式是所有通信模式的基础，面向点对点模式的安全通信理论自然也成为安全通信论的基础；三是从方法论来讲，Shannon的研究方法具有很强的示范作用；等等。

现今，通信系统的模式逐渐向着以网络为基本支撑的模式转变，由此而来的通信安全也有了相应的改变，现在的一个共识是密码学和安全通信协议成为实现通信安全的基本支撑点，随着密码技术和安全通信协议研究的日益深入，相关的材料也已相当丰富，在此基础上，相应的理论体系也越来越趋于完善，作为通信系统安全这一交叉性的学科——安全通信论也已经基本形成。

本书以通信系统中的安全问题为研究对象，试着以信息论和系统论为研究问题的基本工具，对于包括下一代网络在内的各种通信模式的安全问题进行了深入的讨论，试图从中寻找到它们内在的共同规律，以期对各种通信模式下的通信安全有更深刻的认识。本书包含了作者多年来对信息论、网络的体系结构和通信安全问题等研究的相关成果，试图通过总结，使之构成安全通信学科的专门著作。本书共分8章，具体的结构为：第1章是绪言，从通信系统和信息安全等的基本概念出发，阐述了安全通信论这一学科的基本特征和研究方法；第2章具体分析通信模式，对包括下一代网络在内的通信模式的结构及特性进行分析，为研究不同通信模式下的安全做好准备；第3章重点讨论安全通信论中处理问题的基本观点和方法，分别从系统控制论和信息论的角度来分析安全通信的本质

特性；第4章着重分析加密算法和认证技术的相关理论；第5章论述具有很强规范性和标准性的安全通信协议，不仅分析了协议的结构和功能，同时也阐述了它们的设计思想；第6章分析了在网络模式下的管理安全的实现，分别就预防攻击和检测入侵的理论和方法展开论述；第7章重点分析通信安全中的非技术因素的保障作用，它通过对“人”的行为的规范，以及环境等的影响来促进通信安全水平的提高；第8章是总结与展望，尤其对作者在该领域中的相关研究的成果进行了总结，并提出了几点具有重要意义的展望和设想，这些也可看成是安全通信论的发展趋势。

本书虽以论述实现通信安全的理论和方法为重点，但信息和网络的理论也有较多论述，对于想较深入地了解信息理论和网络理论的读者来说，本书也不失为是一本能窥探门径的书籍。本书是作者在该领域中长期研究的一个总结，感谢该领域中提供卓越论述的各位作者，在学习他们资料的基础上，不仅学到了很多知识，而且也获得了研究成果。同时，非常感谢家人的理解和支持，他们温暖的支持和守望，让我在耐得寂寞中获得最可宝贵的慰藉，谨把该书作为初熟的果子，敬献给我的家人。

感谢“杭州电子科技大学专著出版基金”资助出版，最后，殷切地希望读者能提出宝贵意见，以便我能进一步改进和提高。

张焕炯

2013年9月于杭州

目　录

第1章 绪 言

1.1 安全通信论的概念

通信可理解为信息的传输、交换等相应的处理。通信系统则是实现信息传输、交换和处理的具体设备的集合，也可理解为用来实现通信的设备的总和，它以最基本的“输入-处理-输出”模式为基础，并处于不断的发展之中，已从单纯的“信源-信道-信宿”模式发展成为具有广泛互联的通信网络及相关的辅助网络，并进一步向着网格网络等下一代网络（NGN）等模式发展。通信业已成为整个信息社会的高级“神经中枢”，通信系统不仅成为具有举足轻重的影响力的基础设施，也成为人们日常生活中用于沟通交流的必备工具。它的技术水准在很大程度上是展现一个国家或地区的科技水平的重要指标，更成为一个国家和地区的科技创新的重要策动力量。

在设计和评价通信系统时，需要用到相应的性能指标，这些指标大致可归纳为有效性、可靠性、适应性、稳健性、经济性和安全性等特性。对通信系统中的信息传输来说，它主要涉及有效性和可靠性；对于通信系统的构造、维护等来说，它最终体现在稳健性和经济性指标上；而对于通信系统中传输的信息是否安全、完整和可用等角度来分析，就涉及相应的安全性分析。Shannon 通过对传统通信系统的分析，认为从技术层面上来评估或优化通信系统，它所涉及的主要性能指标可归纳为可靠性、为效性和安全性，早在 20 世纪 40 年代后期，他发表了著名的《保密系统的信息理论》论文，并采用概率统计的观点及信息论的手段定量地分析了明文源、密钥源、密文源，进而提出了唯一解距离等描述密码体制的物理量，并深入分析了理想保密、绝对保密等密码体制。他的工作为深入分析通信系统的安全性能及针对安全性能的优化建立了可靠的理论依据，开创了通信系统安全性能理论分析的先声。

随着通信系统的发展，尤其以网络互联为基础的通信模式的普及，通信系统的安全问题越来越突出，同时，以密码学为代表的信息安全技术也有了长足的进步，由此，人们越来越重视通信系统中安全问题的分析研究，但往往是以信息流的安全为主要研究对象，仅把通信系统作为信息安全的应用领域，这种观点虽作为主流观点影响了很长时间，但随着各种研究成果的大量涌现，人们的观点也发生了改变，提出了“安全通信论”的概念。何谓“安全通信论”，就是以通信为核心，把与通信相关的，能确保促使通信安全性能优化的一切理论、技术、操作、人

员、环境、法规等因素所组成的一个研究方向及学科门类。它突出了通信的主体地位，在更宽泛的意义下来讨论包括网络在内的所有通信系统的安全性能，它不仅包含了已有的关于通信系统安全的概念、理论、技术等内容，还极大地拓展了通信系统安全的范围。概括起来，安全通信论至少应该包括以下几个方面的安全概念：一是传统的通信系统中数据形式等的信息安全，也就是传统的以信息流为主体的安全；二是包括通信系统设备等在内的系统安全，它涉及系统的可用性、稳健性以及系统的正常运行、维护和维修等内容；其三，它还包括使用通信系统的用户的安全，这个层面的安全不仅仅指一个个具体直接使用系统者的安全，还包括所在的地区和相应的国家主权等方面的安全；等等。随着科技的发展，相应的安全的范围还将进一步拓展。

虽然安全通信论可被简单地描述为研究通信的安全性能的理论、技术和方法等的总和，但在科技突飞猛进的当今，不仅纯粹的信息安全的研究业已非常深入，同样地，有关通信的研究的进展也异常迅猛，安全通信论作为通信理论与信息安全等理论有机融合的交叉学科，既可以看成已经建立起来的通信与信息安全各自部门之间的共同地带，当然也是曾经的“无人区”，这正如维纳所说：“在科学发展上可以得到最大收获的领域是各种已经建立起来的部门之间的无人区。”我们相信，安全通信论具有深厚理论支撑的同时，必将展现蓬勃发展的态势，它更将成为具有鲜明特色的综合性的学科新方向。

1.2 安全通信论中的基本问题

安全通信论涉及通信中关于安全的一切问题，它不仅是信息流的传输与交换等处理的安全实现，还包括通信系统的安全、通信环境的安全、通信人员的安全等内容。安全通信论中的基本问题，从通信技术发展的角度来归纳，可总结为面向经典通信系统模式的通信安全和面向网络模式的通信安全。

在经典的通信模式中，通信系统实现信息的传输和存储等处理功能时，面临着一个非常重要的安全问题，如何有效提升通信系统的安全性能，是传统通信模式的重要内容之一。突出安全性能的经典通信系统的结构模型如图 1-1 所示。

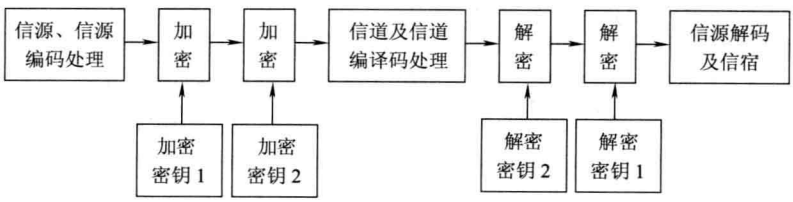


图 1-1 突出安全性能的经典通信系统的结构模型

从模型中不难看出，经典通信系统中最基本的要素为信源、信道和新宿，这三要素能实现通信系统中的信息发送、传输、存储及接收等功能。但是，因为环境的复杂性以及技术的局限性等因素，如何实现“好”的通信是一个十分现实的大问题，它至少涉及如下三个方面：首先，需确定用来描述系统好坏的具体指标；其次，给出所确定的具体指标的定量表述；其三，在不能达到技术指标要求的前提下，如何进行行之有效的技术手段来优化相应的具体指标。Shannon 根据自己的长期研究，提出了“好”的通信系统的具体指标应该包括有效性、可靠性和安全性等指标。有效性表现为可用的信息量占总的传输信息量的比例多少的问题，它需要尽可能地减少冗余来提高系统的有效性，可以借助于压缩处理等的信源编码等方法加以优化；可靠性则是体现在所传输的信息的正确率的问题，它往往用误码率或误比特率的大小来具体衡量，在很多时候，人们看到，要提高系统的有效性，则很可能需牺牲系统的可靠性，它们构成了互相对立的一对矛盾体，类同于通常所谓的精度与速度之间的矛盾。但是，我们必须看到，在某种条件下，它们事实上也是相辅相成的，在传输总量确定的前提下，若通信系统在信息传输过程中出现错误越多，这不仅表现在系统的可靠性越差，同时也表现在系统的有效性也是越差，因此提高系统的有效性与提高系统的可靠性可得到内在的统一。

不难理解，一个通信过程的完成，需要有特定的发送方和接收方，它们具有很强的相对专属性，如何保障在语义透明的信道中所传输的信息流不被非接收方截获，以及从接收方的角度来说，如何实现所接收的信息流就是由对应的发送方所发送，及接收到的信息具有完整性、可用性等特征，等等，这些相关问题就构成了经典通信中主要的安全问题。

首先，在经典通信中，根据是否是目的接收者，可把接收者分为合法用户（接收者）和非法用户（接收者）或期望用户和非期望用户。信息的发送方总是希望安全地把信息发送给合法用户，且不被非法接收者所窃听，这就需要提供如何防窃听的技术和手段，一种可行的办法就是选定专门的信道，以确保从发送到接收整个过程的安全性；显然这种方法仅适用于专线等特殊的信道，不适用于一般性的语义透明的公共信道，在普通的信道中，实现防窃听的安全目标，需要采用相应的处理技术，这就构成通信系统中防泄漏的安全问题，一般采用加密等信息处理技术来防泄漏问题。同样地，以接收方为参考对象，它需要接收到期望发送者的完整信息，它所面临的一个主要问题是如何防止非期望发送者伪造身份进行虚假信息的发送，这构成通信系统中防伪造的问题，同样需要专门的技术处理来克服这个难题，通常所采用的是认证技术，认证是一个过程，通过一系列的推演等步骤的处理，能够验证发送者的身份。所以对于通信系统来说，它的安全问题既涉及具体的防窃听问题，也涉及具体的防伪造问题，以及这些问题的交错混合

所构成的复杂安全问题。安全通信为解决相应的安全问题，同时提升或优化系统的安全性能，所采用的技术不仅需要有防窃听的加、解密技术，还需要防伪造的认证技术，以及包含它们的综合性的技术措施。

随着通信技术的发展，从传统的通信模式向现代化的网络方向演进和发展，随之，针对网络的安全成为了通信安全的重要组成部分，而且它的重要性更可谓是与日俱增。人们发现，网络中的安全问题层出不穷，不仅有针对不同网络种类的安全问题，也有针对网络分层中不同层的安全问题，如数据链路层、网络层、传送层以及应用层中的各种安全问题，进一步，还存在通信网络的辅助网络的安全问题及下一代网络的安全等问题，如何更加有效地解决通信网络中的安全问题，业已成为安全通信中重中之重的问题，除了采用传统的加密和认证技术外，需要有更加针对性的综合技术来解决这些安全问题，设计安全通信协议就是一种有效的综合方法。安全通信协议的实质就是为实现信息安全交换等目标，各通信方之间需要遵循的约定和采取的步骤，它可以兼顾通信体制及通信方，具有很好的协调性，除此之外，它还具有很好的构造性，能强有力地贯彻设计意图，还有，安全通信协议还具有很好的开放性，根据实际环境的变化，可以灵活地做出相应的调整，甚至可以进行升级。现在，人们越来越认识到实现通信网络安全的核心是“密码和安全协议”。所以对网络安全协议的研究和应用成为通信网络安全的主要组成部分，通信安全协议及相关的理论和技术构成了安全通信的重要内容。

通信系统是由人设计和制造的系统，“人”的因素在通信的每一个环节中都起着重要的作用。对于安全通信来说，同样需要“人”遵循相应的原则和规范，这些规范既有面向技术的，也有面向非技术的，如操作规范、道德守则和法律法规等，遵循这些规范同样能有效地规避相关的风险，对安全通信具有很好的保障和促进作用。

1.3 安全通信的发展与通信及信息安全的理论和实践的关系

通信系统的安全性能是表征通信系统优劣的重要指标之一，安全通信问题以及解决这些问题的所有技术和策略构成了安全通信的核心内容。如何理解安全通信与通信理论和信息安全之间的关系，是了解安全通信这个学科方向的重要前提条件，安全通信既有别于一般的通信理论，也有别于一般的信息安全理论，但它又与这两者有着非常紧密的联系。

一般的通信理论，重点探讨通信模式中的有效性与可靠性等相关问题，而安全通信则重点讨论通信的安全性问题，它随着通信技术的发展而发展，这可从考察通信技术的发展过程得到结论，通信模式已从单纯的点到点的模式发展到了

到网络化的模式，从单纯的话音业务到了以数据业务为主的综合业务，从面向单机和数据到了面向数据共享，所对应的对通信系统的安全的要求同样有了很大提高，通信安全已经不仅仅是解决某一个具体问题或漏洞那么简单，而是对面向数据和用户的安全属性赋予新的内涵的同时，更强调了面向系统的安全属性，构成了综合的面向数据、面向系统和面向用户的立体型的信息安全新概念。从面向数据的角度来看安全的概念，它最直接的体现就是信息的保密性、完整性和可用性，也就是信息安全的 C. I. A 准则；而面向系统的安全概念所涉及的是实现系统的可用性、可控性、稳健性和可再生、恢复等特性；面向用户的安全概念是以用户为主体，实现该主体的可操作性和自然法人等的特性，具体包括对实体的认证、访问控制、授权和服务性等实践等的相应功能。进一步，更随着通信系统和技术的发展，新的安全问题更是层出不穷，这为密码学和信息安全的理论和技术提出了全新的挑战，它促使人们对信息安全作更精深的研究，同时为信息安全的理论创新和技术创新提供良好的契机和应用领域，从这种意义上来看，通信系统的发展是促进安全技术创新的重要因素，也是展示安全新技术的重要领域，更是检验具体的安全技术和方法的先进行的重要场所。

同时也必须看到，信息安全是一个相对宽泛的、具有鲜明特色的学科，通信安全不是信息安全的全部，但又是它的重要组成部分，安全通信的理论与技术发展离不开信息安全理论的创新与相应的实践。密码学等信息安全的理论和技术的发展，为顺利解决通信系统的安全问题提供理论的准备和实际的实现方法。信息安全作为一门严谨的学科，它具有自己内在发展脉络和轨迹，具有相对完整的自我完善的特性。新的加密算法的出现，新的加密技术标准的颁布，新颖的认证算法等的出现，或已有的加密算法的破译等，不仅能推动信息安全理论和技术自身的巨大发展，更能有力地推动安全通信的发展，尤其对通信系统的安全性能指标的优化产生巨大的促进作用，如 RSA 公钥制理论的提出、DES 和 AES 标准的颁布、基于椭圆曲线难解问题的数字认证方案的公布、用于电子邮件安全的 PGP 协议的公开，针对 TCP/IP 网络协议模型的安全通信协议的设计等，这些信息安全的理论和技术都能有力地提升通信系统的相应的安全能力。因此，密码学等信息安全的理论和技术的发展能极大地促使通信系统的安全性能的长足提升，是通信系统发展的重要推进力量。

此外，还必须看到，在很多时候，相关的通信技术本身能有效提高通信系统的安全性能，这方面最典型的莫过于扩频技术，在通信中，采用扩频技术能有效降低对信噪比的要求，同时由于信噪比的降低，能很好地起到信息的隐藏等效果，这就实现了安全理论和技术与通信系统的理论和技术的内在统一，它从一个方面也说明了两者之间内在的可融合性。

1.4 安全通信论应遵循的基本研究方法

在过去，研究密码学等信息安全理论的人们不大关注通信理论的研究，同样地，专注于通信理论等方面的研究者也不大关注信息安全等的问题，如他们设计通信系统及其各种规制时往往对安全问题的考虑不是非常充分，等系统在实际使用时，碰到了具体的安全挑战后，再来补强相关的安全举措，这似乎已经形成了一个传统，但随着人们对信息安全的重要性的认识越来越深入，人们认识到通信系统安全是一门综合的交叉于通信理论和安全理论的学科，并着手寻找最佳的深入研究的途径，总结和归纳合乎通信系统安全学科本身内在规律的研究方法。

Shannon 是创立信息论的伟大先贤，他关于通信系统中的安全问题的研究成果业已成为信息论的重要组成部分，他的关于通信系统的安全问题的研究方法也堪称经典，其中最有特色的是一方面能抓住问题的本质的前提下，对安全问题进行有效的简约；另一方面，他引进了描述不确定性的信息熵的概念，通过对通信系统处理前后不同状态下的信息熵的定量表述，引进了诸如唯一解距离等新概念的同时，堪称完美地给出并证明了保密定理，为密码学和信息安全的学科的确立奠定了重要的基础。分析他的研究方法，不难发现，他自觉地把通信系统安全问题纳入了信息处理的具体范畴，把加密、解密等安全处理看作信息处理器模块的功能实现，因此它也遵循信息处理的基本原理和准则。而迄今，所采用的信息处理的方法和手段都不外乎来自如 Weiner 等所创立的控制论和 Shannon 等所创立的信息论等的相关理论，控制论和信息论是信息与信号处理的所有方法的理论基础，当然它们也是信息安全处理的理论基础，所以通信系统安全的基本处理方法应该是以系统论和信息论为指引的能有效提升安全性能的方法，也就是说，通信系统安全的研究方法不能背离系统论和信息论的基本原则和要求。通信系统安全处理方法示意图如图 1-2 所示。

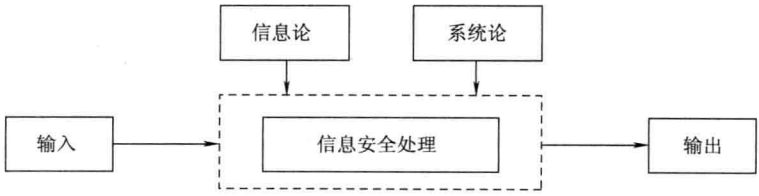


图 1-2 通信系统安全处理方法示意图

随着通信网络的发展，针对网络的安全问题的研究方法也呈现出新的特点，虽然人们越来越认识到“密码和安全协议是网络安全的核心”，比较专注于从密码学和通信安全协议的设计等方面着手进行通信系统的安全的处理，但是本质上还是没有跳过以信息论和系统论为基本理论依据的信息处理的方法。

另外，因为通信与普通的人们的生活息息相关，通信系统的安全实际上就是普通人的安全的重要组成部分，关于通信系统安全的研究要把具体的理论与大众的具体实践相结合，更要有很好的推广，这方面，Philip Zimmermann 的研究方法可以看成是一种榜样，他致力于把公钥制的 RSA 算法带到普通人的生活中，尤其把它应用到网络用户都要使用的电子邮件的安全防范中，起到了很好的作用。

当然，关于“安全通信”的研究方法是多姿多彩的，这些各有特色的方法和相应的研究成果都成为这门学科日益完善的重要资料。

1.5 安全通信论的基本框架结构

有别于通常的通信理论和信息安全的安全通信，它有相对独立而又完善的体系结构，梳理和总结它的知识框架，有助于深入理解它的本质特性，更有助于把握该学科的发展方向。图 1-3 是对安全通信论结构框架的示意图，从图中不难看出，安全通信论的主要来源是通信与信息安全，它又是一个开放的体系，体现在不但包含其他相关的内容，还随着其他相关理论和技术的发展，以及它本身的新问题等的解决，将进一步拓展它的内容。

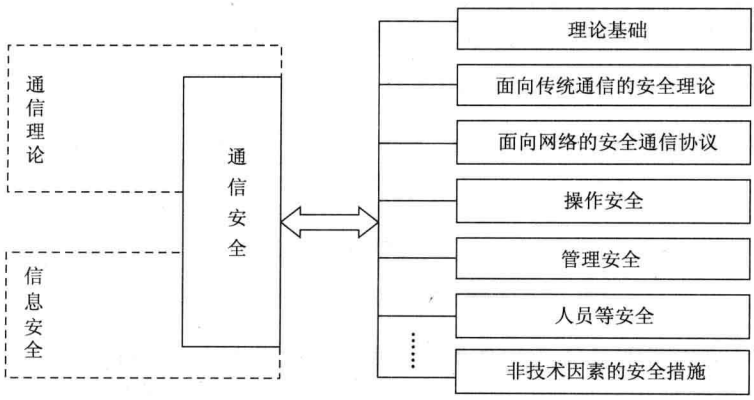


图 1-3 安全通信论的体系结构图示

1.6 小结

全方位、立体式地概述了“安全通信论”的基本特征，分别从安全通信论的问题提出、所包含的基本内容、与其他相关学科尤其与一般的通信理论和信息安全等的关系，及基本的框架结构和特征等方面进行论述和总结，勾勒出安全通信论的基本框架及特性，并为后续的深入讨论做好准备。

第 2 章　通 信 模 型

2.1　引言

在给定具体的通信模式的前提下讨论安全问题是一条行之有效的研究分析的路子，通信模式则是实现有效、可靠和安全通信的具体手段和工具。本章对通信模式进行具体梳理，介绍传统的点对点通信模式和重要的网络模式。

2.2　点对点通信模式

可以说，点对点通信模式是所有通信系统的基础，就其本身来说，可以独立构成通信系统，实现具体的信息发送、传输和接收，同时它更是构成通信网络的组成部分，无论网络如何发展，最终总可以分解成点对点的通信模式。

点对点通信模式的基本组成部分包括信息源、发送设备、信道、接收设备和接收者，具体如图 2-1 所示，它的共性可概括为发送方、传输方和接收方。

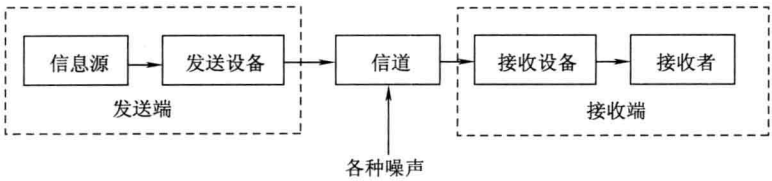


图 2-1　点对点通信系统的共性化结构模型

其中，发送方指具体的信息源和用来把该信息源进行具体发送的设备，还应包括在发送前需要对信息源进行处理的设备；传输方就是具体的信道，信道可简单地理解为信息传输的通道，在信道中会有一些干扰和噪声。比较起来，干扰可根据它的产生原因，进行具体的处理，易于遏制或消除，但噪声总是与系统和环境等相伴随的，一般有加性噪声和乘性噪声，往往把它们建模成白噪声，难以通过相关的信息处理而消除，而很多时候，相关的信息处理后，白噪声有可能转化成了有色噪声；接收方就是接收具体信息这一方，它包括接收设备和信息接收者。

根据被传输的信息源的形式不同，点对点的通信模式可分为模拟通信系统(图 2-2)和数字通信系统，它们的实质区别主要体现在发送设备处理信息源的

能力上，当发送设备对源信息处理后，信息源还是连续形式的，那么它就是一个模拟系统；而不论原始信息源是连续形式还是离散形式，经过发送设备的处理，待发送的信息就变成数字形式，这样的系统就是数字通信系统，这时，发送设备中一定包含具体的模数转换设备。在不同的通信模式中，发送设备中往往包含调制器，对应地，接收设备中需要包含解调器，但有一种情况是例外的，那就是在基带数字通信模式中，发送端只需要基带信号形成器，而在接收端只需要接收滤波器就可以形成一个完整的基带传输通信模式。虽然这两种数字通信方式结构不尽相同，但它们之间存在内在的规律，理论上业已证明，一个采用线性调制的频带传输系统，总可以用一个等效的基带数字通信系统来代替，也就是，任一个线性调制下的频带系统总等价于某一个基带数字通信系统。基带数字通信系统结构如图 2-3(a)所示。

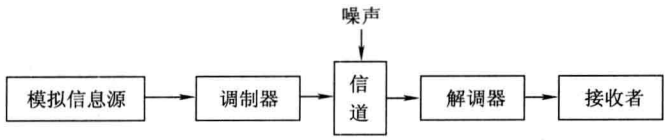


图 2-2　模拟通信系统结构

频带数字通信系统结构如图 2-3(b)所示。

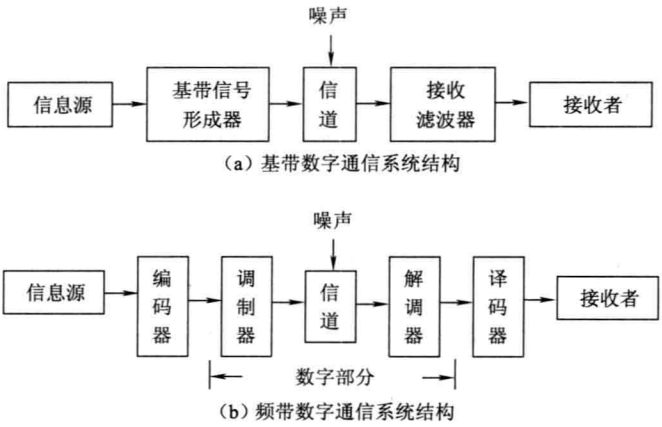


图 2-3　基带与频带数字通信系统结构

根据不同的分类标准，点对点通信模式可分成不同的种类，如按照传输介质的不同，通信模式可分为有线、无线及复合形式等种类；根据传送信号复用方式的不同，通信模式可分为时分复用(TDMA)、频分复用(FDMA)和码分复用(CDMA)，一般的模拟通信系统大多采用频分复用，数字通信系统大多采用时分复用，而扩频通信等系统大多采用码分复用。