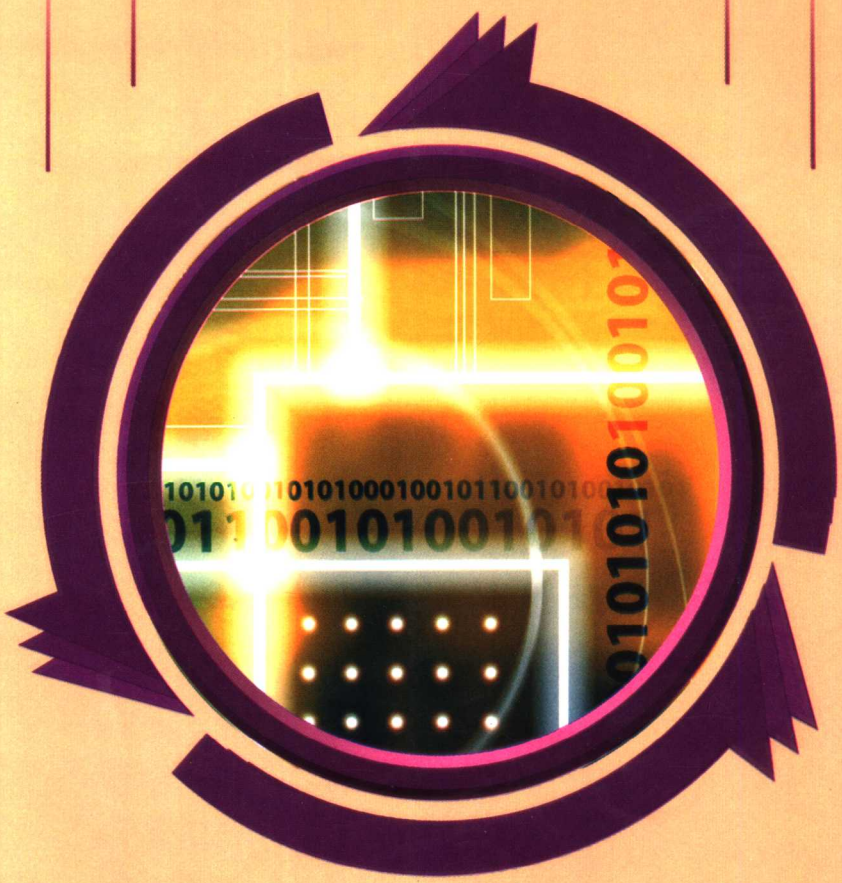
现代通信高技术丛书

差错控制编码与安全

周贤伟 主编
黄旗明 张丽静 姚恒艳 编著



国防工业出版社
National Defense Industry Press

现代通信高技术丛书

差错控制编码与安全

Chacuo Kongzhi Bianma Yu Anquan

周贤伟 主编

黄旗明 张丽静 姚恒艳 编著

国防工业出版社

http://www.ndip.cn

内 容 简 介

本书以差错控制编码和安全的知识性、综合性、实用性内容为主线，系统地介绍了差错控制编码理论的基本原理及其密码系统的安全性。主要内容包括：有限域代数基础；线性分组码、循环码、LDPC 码、卷积码、Turbo 码等纠错码的编/译码原理和方法；密码系统和密码体制的基本原理；利用纠错码构造密码体制、数字签名、身份认证码的方案以及方案的安全性分析；纠错码在数据网中的应用。

本书概念清晰、由浅入深、循序渐进，可作为通信工程、信息工程和计算机类各专业本科生和研究生的教材或参考书，也可供从事通信、电子、计算机、数学等专业工作的科技人员参考。

图书在版编目(CIP)数据

差错控制编码与安全／周贤伟主编；黄旗明，张丽静，姚恒艳编著. —北京：国防工业出版社，2006.9
（现代通信高技术丛书／周贤伟、邓忠礼，郑雪峰主编）
ISBN 7-118-04564-0

Ⅰ. 差… Ⅱ. ①周…②黄…③张…④姚… Ⅲ. ①误差控制码②密码术 Ⅳ. ①TN919.3②TN918.1

中国版本图书馆 CIP 数据核字(2006)第 059215 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 100044）
天利华印刷装订有限公司印刷
新华书店经售
*
开本 787×1092 1/16 印张 20¼ 字数 456 千字
2006 年 9 月第 1 版第 1 次印刷 印数 1—4000 册 定价 37.00 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

《现代通信高技术丛书》编委会

序

当今世界已经进入了信息时代，信息成为一种重要的战略资源，信息科学成为最为活跃的学科领域之一，信息技术改变着人们的生活和工作方式，信息产业已经成为国民经济的主导产业，作为信息传输基础的通信技术则成为信息产业中发展最为迅速，进步最快的行业。目前，个人通信系统和超高速通信网络迅猛发展，推动了信息科学的进一步发展，并成为21世纪国际社会和全球经济的强大动力。

随着通信技术日新月异，学习通信专业知识不但需要扎实的专业基础，而且需要学习和了解更多的现代通信技术和理论，特别是数字通信、卫星通信以及传感器网络的现代通信技术方面的知识。从有线通信到无线通信，从固定设备间的通信到移动通信，从无线通信到无线因特网，到传感器网络技术。未来的通信将为人们提供全方位以及无缝的移动性接入，最终实现任何人在任何地方、任何时间进行任何方式的通信，使得通信技术适应社会的发展需要呈现经久不衰的势头。

网络技术的飞速发展，通信技术在经济发展中的重要地位日趋重要，世界各国特别重视通信技术的理论研究和通信技术专业人才的培养，国外有关通信领域的文献资料和专著较多。就国内来讲，通信专业人才大量急需，为适应社会经济发展的需要，各高校和科研单位都在培养社会所需的通信专业人才。

为了增进通信及安全技术领域的学术交流，为了满足通信及信息安全专业领域的读者的需要，提供一套能系统、全面地介绍和讲解通信技术原理及新技术的系列丛书，北京科技大学等组织编写了这套《现代通信高技术丛书》。这套丛书内容涵盖了通信技术的主要专业领域，既可作为高等院校通信类、信息类、电子类、计算机类等专业高年级本科生或研究生的教材，又可作为有关通信技术和科研人员的技术参考书。

我觉得这套丛书的特点是内容全面、技术新颖、理论联系实际，针对目前

我国通信技术发展情况与目前已有的相关出版物之间已有一定距离这一情况，本丛书立足于现在，通过对基本的技术进行分析，由浅入深，努力反映通信技术领域的新成果、新技术和进展，是国内目前较为全面、技术领先、适用面广的一套丛书。在我国大量培养通信专业人才的今天，这套丛书的出版是非常及时和十分有益的。

我代表编委会对丛书的作者和广大读者表示感谢！欢迎广大读者提出宝贵意见，以使丛书进一步修改完善。

2005 年 3 月 20 日

前　言

随着科学技术特别是信息技术的发展，差错控制编码在数据通信领域中发挥着越来越重要的作用，它是解决数据通信领域中相关问题的有力工具。由于差错控制编码解决问题的思路和方法非常独特、新颖和有效，越来越广泛地应用到各个领域当中，并且显示出它的勃勃生机和不可估量的发展前景。

随着差错控制编码理论的发展，有关它的书籍也越来越多。然而，大部分书籍讲述的都是基于物理层和数据链路层涉及的差错控制编码问题，这些问题都是纠错码的传统应用问题。通常人们会认为：在数据通信网中，纠错码仅仅是提高数据在不同信道传输可靠性的一种方式，编码对于网络的其他层次造成的影响没有考虑在内。本书作者根据多年教学和科研经验，并参考大量相关文献，总结出：纠错码可以应用在网络中高于数据链路层的其他层，并且在该层编码之后，不但能够有效降低信息的传输延时，而且还可以提高信息本身的可靠性。特别地，对基于纠错码构造的密码系统，可以非常有效地解决数据通信网的安全保密问题。此外，对网络的某一层次进行编码，还会对其他层次的性能产生一定影响。由于纠错码理论和技术涉及的范围非常广泛，本书只能够提纲挈领地介绍纠错码的基本理论、编/译码方法以及相关的应用，目的是使读者对纠错码有一个全面的了解，以便为进一步深入研究打下扎实的基础。

本书的内容安排如下。

第 1 章介绍网络的不同层次面临的差错控制编码问题。第 2 章介绍编码理论中用到的代数基础。第 3 章讲述研究得最多的一种码：线性分组码，并且附带介绍线性码的不同译码方法和一些新的结论。第 4 章讲述应用广泛的码：汉明码、BCH 码和 RS 码，这些码的译码方法有助于阐述编码理论的一些重要结论。第 5 章介绍 LDPC 码的译码问题。第 6 章讲述另一种应用得非常广泛的码——卷积码及其迭代译码方法。第 7 章介绍 Turbo 码和它的应用。第 8 章介绍应用在密码学中的编码方法。第 9 章讲述基于纠错码的数字签名和消息认证码。第 10 章介绍纠错码应用的新领域：传输编码以及如何协调网络不同层次之间的编码问题。

数据通信网的差错控制编码问题涉及的范围是非常广泛的，甚至到了今天我们还不能给出这些问题的一个完整定义。虽然本书作者没有给出解决这些问题的一个完美方案，但仍旧希望这本书能够给在这个领域深入研究的人们提供一些帮助。

在此，对本书在编著过程中所有给予热情帮助过的同志表示真诚的感谢，同时，对本

书中引用的参考文献的所有作者表示衷心的感谢。

由于时间紧迫，加上作者水平有限，书中难免会有许多不足之处，敬请同行专家和各位读者批评指正。

编著者

2006 年 1 月于北京

目　录

第 1 章　数据网面临的差错控制编码问题

本章主要讲述目前数据网各层面临的差错控制编码问题，提出在不同网络层次中进行联合编码的建议，该建议可以提供最佳的算法冗余分布。

1.1　基于不同网络层次的差错控制编码

数据网的目标是给用户提供可靠、有效（即快速）的信息传输：通过在传输的数据中增加冗余信息去检测和纠正差错，保证信息传输的可靠性；同时，通过开发有效的信息处理程序，如重传、初始化、连接和断开连接等来提高信息传输的速度。但是数据包越大，就意味着传输速率越低，所以数据传输的可靠性和有效性是矛盾的。国际标准的目标是要解决这两个相互冲突的问题。致力于解决编码问题的信息理论建立在这样的事实基础之上：在网络的某一层进行数据的某种操作时，可以将该层看成是一个信道。

目前，国际标准组织制定的开放性系统互联参考模型（OSI）包括了如下 7 层。

（1）物理层：它通过在网络实体之间建立物理连接，从而提供比特流的透明传输。这一层采用了不同的调制技术。

（2）数据链路层：它的主要功能是代表网络层通过物理层建立一个可靠的协议端口，这意味着数据链路层执行检测差错和纠错的工作，这是编码应用得最普遍的领域。

（3）网络层：它的主要功能是在传输层实体之间提供协议数据的传输。在网络的每一个节点和每一个站点存在着一个网络层处理程序。这些程序都是端到端的，负责为网络层执行路由和流控制。

（4）传输层：它的主要功能是将报文进行分片并重新组成数据包，并在单个 L3 接口上采用多路技术。如果说网络层是不可靠的，那么可以说传输层可以达到端到端的可靠通信。端到端的流控制通常也在传输层进行。

（5）会话层：它的主要功能是提供用户到网络的接口，也常常提供用户和主机之间的连接。会话层的其他功能还包括流控制和数据传输方向的控制。

（6）表示层：它的主要功能是决定数据如何表示给用户，包括数据加密、数据变换和编码转换等。

（7）应用层：负责处理特定的应用程序细节。

在这个模型当中，数据从源终端系统的应用层传到物理层，再到达物理介质，如光纤、同轴电缆等。通过这些物理介质，数据传到了目的终端的物理层，最后再上传到应用层，如图 1 - 1 所示。值得注意的是：高于数据链路层的那些层存在着非二进制的、有着各种特殊类型的差错，如重复、丢失和溢出等，而差错控制编码是一种既能够提高数据传输可靠性、又能够降低数据传输延迟的通用方法。

差错控制编码主要应用在数据链路层，而编码技术涉及的领域非常广泛，包括从最简

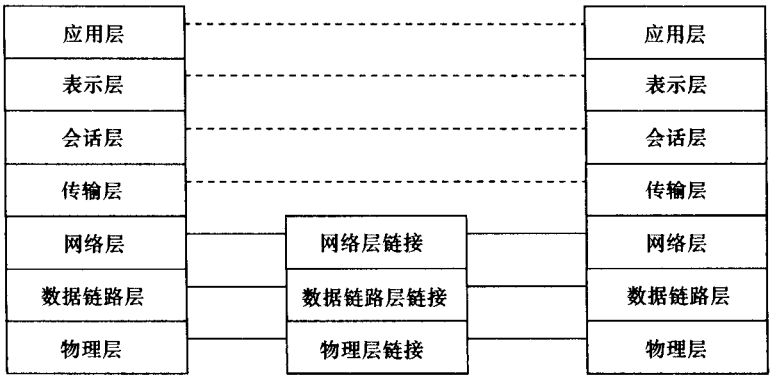


图 1-1 开放性系统互联参考模型

单的奇、偶校验到比较复杂的编码,这些特点在数据链路层的不同协议中都有陈述。

几乎所有的协议都用到了二进制循环分组码,这种码可以用来进行 16bit、24bit 或 32bit 的循环冗余校验(CRC)计算。例如,数字数据通信报文协议(DDCMP)和高级数据链路控制(HDLC)采用了 16bit CRC。链接访问程序(LAP)协议也采用了 16bit CRC,LAP 可以看成是 HDLC 的子集。特别地,LAPB 协议用在了著名的 X.25 标准当中。在 IEEE802.3 带有冲突检测的载波侦听多路存取(CSMA/CD)或者以太网协议的帧中采用了 32bit CRC,用以保护数据。IEEE802.4 令牌总线、IEEE802.5 令牌环网和光纤分布式数据接口(FDDI,Fiber Distributed Data Interface)协议也采用了相同的 32bit CRC[1]。10bit CRC 和 8bit CRC 分别提供了 ATM 的整个数据保护和 ATM 报头的数据保护。这个 8bit CRC 的主要特征是:它常常用于纠错而不是检错[2]。更为复杂的编码技术广泛地应用在无线网络中。在 GSM 标准中,除了 8bit CRC 之外,还采用了长度为 5、码率为 1/3 的卷积码。在改进的电路交换数据网(GSM 的一部分)中,采用了 $GF(2^8)$ 上缩短的(255,243)系统 RS 码[3](简称 RS 码)。在 UMTS 中,除了采用 24bit CRC,还采用了长度为 9、码率为 1/3 和 1/2 的卷积码[4];IEEE802.16 宽带无线接入(BWA,Broadband Wireless Access)采用了缩短的(255,239,17) RS 码;蓝牙标准中采用了缩短的(15,10)汉明码。

除了数据链路层,网络的其他层次也常常采用编码技术。传输控制协议(TCP,Transmission Control Protocol)经常采用 16bit CRC 去检测 TCP 帧的差错,同时,在必要的条件下还采用 CRC 计算和重传程序初始化来保护数据。

然而,不幸的是,网络某一层次的数据保护程序常常不与另外一层的数据保护程序协同作用,即数据保护在网络的不同层次是独立进行的,或者同一层次的数据保护程序也常常不与相同层次的其他保护程序相协调。解决这个问题的方法一般是将第 1 层和第 2 层相互协同作用。然而,第 1 层的主要技术是调制而不是编码。在 HDLC(或者是 LAP)中,最重要的问题是帧同步如何与借助 CRC 进行的差错检测相互作用(图 1-2)。在 HDLC 和 LAP 中,传输的报文边界是由形式为"0111110"的标记来界定的,这个标记在比特填充的程序中完成,即在报文传输期间,若数据帧里出现了 5 个连续的"1"bit,则在这些比特后面填入"0"bit。因此,在比特填充之后,数据帧里不会再出现多于 5 个连续的"1"bit,同时数据帧的结尾标记是唯一可辨别的。在接收端,将会删除 5 个连续的"1"bit 之后出现

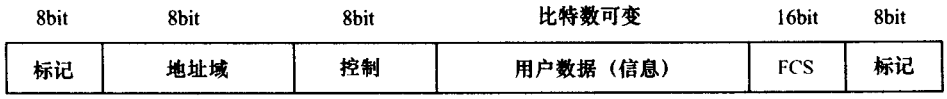


图 1－2　HDLC 帧结构图

的“0”bit。假如 5 个连续的“1”bit 之后跟着的比特是“1”，那么这个数据帧将宣告结束，之后进行的是 CRC 校验。

因此，可以假设，循环码应该在某个扩展的离散信道（EDC）中检测差错，这是离散信道（DC）、比特填充以及附加标记程序的一个组合（图 1－3）。由于在 DC 中存在差错，分组同步可能会失败（即错误地检测到数据帧结束了）。失败有 2 种情形：第 1 种情形是，由于删除了标记位置上的某些比特，导致标记出现错误，就有可能将整个数据帧分成了 2 个；第 2 种情形是，由于破坏了结束标记，致使 2 个或者更多的数据帧粘到一起。因此，这些差错由于插入或者删除了某些比特而导致数据帧边界发生了改变。不幸的是，二进制循环码的检错能力是非常弱的，但是在加性信道中，它们却可以检测出任何 $d-1$ 个差错，这里 d 是该码的最小汉明距离。

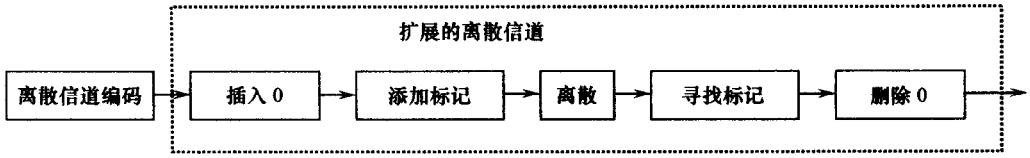


图 1－3　HDLC 帧异步处理程序中的扩展离散信道

本书的一个目标是：如何使编码在网络的不同层次中更好的相互作用。

1.2　网络编码问题分类

在设计数据网的过程中，如何减小系统的噪声是必定要涉及的一个中心问题。为了解决这个问题，有必要考虑到：数据在网络中丢失，除了可能是由通信信道产生的失真引起的外，作为信息传输服务方式的数据网的拓扑结构，其特征的特殊化也常常是差错产生的原因之一。

通常，在通信信道中，编码只用来提供信息传输的可靠性。同时，数据网的每一层可以看成是一个数据信道，这个信道拥有自己的数量级别（如比特、帧、数据包、消息）传输方式和特定的失真。从这个观点来看，编码问题是一个全局问题，这个问题是相对于将数据网看成是一个整体而言的，因为它不仅要分析物理差错的来源，也要分析提供给数据网的协议。解决这个全局问题涉及开发非传统的编码方法，这个方法还应该能够提供网络不同层次编码的相互协调。

然而，在网络的较高层次中进行编码时，增加冗余通常认为是增加了网络的负载，从而无条件导致了信息传输的延迟。

在文献[5～9]中，编码的主要用途不仅是增加网络的可靠性，而且也用于增加网络功能参数的可靠性，并减少信息传输的延时。本书的后半部分将谈到编码在物理层和数