网络协议的形式化分析与设计

古天龙　蔡国永　著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络协议的形式化分析与设计

古天龙　蔡国永　著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

计算机网络及数据通信是当今信息社会的基石,网络协议则是其中不可缺少的重要组成部分。形式化方法与技术已经渗透到网络协议开发的整个过程。本书就网络协议分析与设计中的形式化方法与技术展开讨论和介绍,主要内容包括:网络协议及开发概论;网络协议的形式化模型;网络协议的形式化描述语言;网络协议的形式化验证;网络协议的形式化综合;网络协议的测试;网络协议的分析和验证工具;电子商务协议的形式化分析等。本书可作为计算机、通信、自动化等专业高年级本科生或研究生的教学用书,也可作为相关领域的研究人员和工程技术人员的参考书。

图书在版编目(CIP)数据

网络协议的形式化分析与设计/古天龙等著. —北京:电子工业出版社,2003.6
ISBN 7-5053-8646-8

Ⅰ. 网… Ⅱ. 古… Ⅲ. 计算机网络—通信协议 Ⅳ. TN915.04

中国版本图书馆 CIP 数据核字(2003)第 026064 号

责任编辑:钟 金
印 刷:北京李史山胶印厂
出版发行:电子工业出版社 http://www.phei.com.cn
北京市海淀区万寿路 173 信箱 邮编 100036
经 销:各地新华书店
开 本:850×1 168 1/32 印张:11.875 字数:309 千字
版 次:2003 年 6 月第 1 版 2003 年 6 月第 1 次印刷
印 数:3 000 册 定价:25.00 元

凡购买电子工业出版社的图书,如有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系。联系电话:(010)68279077

前　言

计算机网络是计算机和通信密切结合的产物，近些年来得到了迅速发展和广泛应用，已逐渐成为当今信息社会的基石。网络协议是计算机网络中不可缺少的一个重要组成部分，它是计算机和计算机之间以及计算机和其他设备之间进行数据通信的必要条件。

协议最早就诞生于通信系统中，协议设计的历史与通信本身一样古老。从古至今，如何建立一个在远距离上快速传输信息的系统，一直是人们在不断探索和研究的问题。为了实现远距离的信息传递，一方面需要有发送和接收信号的装置，即硬件设备；同时还需要建立一套规则、标准或约定，用来规定信号的传送和接收方式以及所传送信号的意义，这就是协议。

从早期的烽火通信，到近代的电磁、电报通信，协议设计者凭借自己的经验和智慧，利用手工方法开发出了许多满足各自通信系统需要的协议。

20 世纪 60 年代以来，计算机和通信技术相结合，诞生了数据通信和计算机网络中的高度自动化数据交换，这些变化使得人们越来越强烈地意识到网络协议设计所面临的挑战和困难。为此，国际著名公司、国家机构和国际学术组织纷纷着手制订网络协议的标准，如：我们熟知的 TCP/IP, FTP, OSI 等。尽管如此，标准化并不能解决网络协议中的所有问题。首先，任何机构或组织制订的网络标准协议是否一定能够确保正确可靠的数据交换，需要一定的方法和技术来进行评判；其次，对于同一个网络协议标准，不同的工程和研究人员会有不同的实现方法，这种实现和标准之间的一致性又如何来保证？再次，在不同协议标准，甚至同一协议标准的不同版本下，

所实现系统的数据交换，对网络协议设计提出了新的问题。由于以上原因，建立网络协议分析和设计中的系统、科学的方法和技术成为必须重视的问题。因此，基于形式化方法和技术的网络协议分析与设计被推到了前台，诞生了计算机、通信等学科相互交叉的一个新分支——协议工程。

形式化方法是基于严密的、数学上的形式机制的系统研究方法。客观地讲，有了数学的应用，就有了形式化方法。但是，一般认为形式化方法是始于20世纪60年代末的Floyd, Hoare和Manna等在程序规格和验证方面的研究，当时由于“软件危机”，人们试图用数学方法证明程序的正确性而发展成为各种程序验证方法，但是受程序规模限制，这些方法并未达到预期的应用效果。从20世纪80年代末开始，在硬件设计领域，形式化方法在工业中的广泛应用，掀起了形式化方法和技术的学术研究和工业应用的热潮。迄今为止，形式化方法成功地应用于空中交通管制系统、铁路信号系统、核电站控制系统、通信系统、医疗监护系统、硬件电路等诸多领域。

形式化方法在协议开发中的应用研究，始于20世纪60年代末。人们首先开展了协议的各种形式化技术的研究工作，如：Petri网、有限状态机、形式语言等。在此基础上，建立了协议的标准形式描述语言，如：ESTELLE, SDL, LOTOS等。目前，随着形式化方法和技术的日趋完善，网络协议的开发已逐步从非形式化描述、手工方法实现过渡到以形式化描述技术为基础，渗透到网络协议分析、综合、测试等各环节的软件工程方法。同时，已开发出了支持协议开发活动中形式化描述、正确性验证、性能分析、自动代码生成和一致性测试等各个方面的许多软件工具。网络协议的形式化分析和设计正在向完善化、系统化、自动化和标准化方向发展。

本书对网络协议的形式化分析和设计进行了介绍，可作为计算机、通信、自动化等专业高年级本科生或研究生的教学用书，也可作为相关领域的研究和工程技术人员的参考用书，以期对国内形式

化方法的教育以及工业界推广应用形式化技术有所帮助。

全书内容共有 8 章。第 1 章对网络协议及开发进行一般介绍，包括：早期的通信及协议的简要历史回顾、网络协议的定义及其基本要素、网络协议的分层结构和 OSI 模型、网络协议的开发过程等。第 2 章讨论了网络协议的形式化模型，主要包括有限状态机、Petri 网、时态逻辑和通信进程演算等。第 3 章对网络协议的典型形式描述语言 ESTELLE,LOTOS 和 SDL 等进行了介绍。第 4 章介绍网络协议的形式化验证，主要包括网络协议性质概述、系统断言语言、不变性分析、可达性分析和符号模型检验等。第 5 章对基于有限状态机规格的网络协议综合及相关问题进行了介绍。第 6 章介绍了网络协议的测试，包括：协议测试概述、协议测试语言 TTCN、控制流测试序列设计和数据流测试序列设计等。第 7 章 对网络协议的典型分析检验工具 SPIN 和 SMV 进行了介绍。第 8 章讨论了电子商务协议的形式化分析，包括：电子商务及其协议设计、典型电子商务协议、电子商务协议的 BAN 逻辑和 Kailar 逻辑分析、电子商务协议原子性和安全性的模型检验分析等。

在本书写作过程中，作者的同事董荣胜、李凤英以及研究生常亮、郭云川、赵新有等同学提出了许多宝贵的建议并参与了部分书稿的整理。钟金编辑为本书的出版做了大量具体细致的工作。在此，一并表示感谢。

由于作者水平有限，本书错漏和不妥之处在所难免，恳请广大读者批评指正。

作　者

2003.01

目　录

第 1 章　网络协议及开发概论

顾名思义，协议是某一种活动或者行为所遵守的准则或规则。协议在人类社会和日常生活中经常用到。在计算机世界中，协议是计算机之间或计算机与其他设备之间用来通信的规则或语言。本章回顾了早期的通信及协议所存在的问题，介绍了计算机网络及其不可缺少的组成部分——网络协议。同时，讨论了网络协议的分层结构，以及网络协议开发的一般过程。

1.1　早期的通信及协议

协议最早诞生于通信系统中，协议设计的历史与通信本身一样古老。如何建立一个在远距离上快速传输信息的系统，这是很久以来人们就在不断探索和研究的问题。为了实现远距离的信息传递，一方面需要有发送信号的装置，即硬件设备；同时还需要建立一套规则、标准或约定，用来规定传送信号的方式，以及所传送信号的意义。下面将对早期的通信系统及其所使用的协议进行简要回顾。

1.1.1　早期的通信系统

1．烽火通信

关于使用火信号来进行通信的最早记录，我们可在公元前 458 年的史诗“阿伽门农”（“阿伽门农”是特洛伊战争中希腊军队的统帅）中找到。在这里面，埃斯库罗斯（希腊悲剧诗人）详细地描述了火信号是如何用来传送消息的。即通过使用火光，将特洛伊败给

了雅典的消息送给 300 多英里（1 英里=1.609 3 km）外的希腊神亚古尔。显然，单单一个火把所能传送的不同消息的数量是有限的。公元前二世纪的希腊历史学家 Polybius 对这个情况也进行了详细的评论，这可能是第一个对数据传输方法的准确描述。Polybius 首先解释了使用火信号能有效传送信息的原因，即“通过这些方法，就算是相距三四天或更多天的行程距离，人们也能在很短的时间内及时获得远方的信息”。然后，Polybius 提出了单个火信号所存在的问题，即当出现未预料到的事件（该事件未在协议所规定的内容之中），而又急需通知时，使用单个火信号就无能为力了。

紧接着，Polybius 描述了一种新的发送信号的方案，他认为该方案能解决在上述通信中出现的问题。该方案使用了一个由两组火炬构成的系统，每一组火炬又由五支组成。通过点燃每一组中按次序排放的第一至第五支火炬，总共就可得到对 5^2 个符号的编码，从而能够通过一串编码字符来传输任意的消息。如图 1-1 所示，该火炬可用来发出一个二进制的火炬代码。通过将火炬升高以超过屏障，远方的接收者便可以看到，相当于“1”；相反，也可以将火炬降低从而被屏蔽起来，从而得到“0”。Polybius 对使用该系统进行通信的具体方法也进行了描述。首先将字母表分成五个部分，每个部分由五个字母组成（5×5=25）。因此 26 个英文字母中有一个字母将不能被表示（26–25=1），但这并不存在实际的影响。通信双方事先准备好五张表，并将对字母表的划分填在表上；对这五张表进行编号（分别为 1～5），同时对各张表中的五个字母也分别进行编号。在通信之前，信息发送方先举起两支火炬，等待对方以同样的方式（举起两支火炬）作出响应，从而建立连接。在得到对方的回答后，发送方将火炬降下，然后开始正式的数据传送。首先，发送方将左边的一组火炬中的一部分举起，火炬的数量代表目前发送的是那一张表中的字母。例如，一支火炬代表第 1 张表，两支火炬代表第 2 张表等。然后发送方将右边的一组火炬中的一部分举起，火炬的数量

代表所传送的是当前表中的第几个字母。例如，一支火炬代表所传送的是当前表中的第一个字母，两支火炬代表所传送的是当前表中的第一个字母等。如此循环下去，直到传送完所有字母。接收端将所收到的字母排列起来，便可得到信息。不难看出，该方案实施起来非常复杂，并且也只是部分地解决了前面所提到的问题。

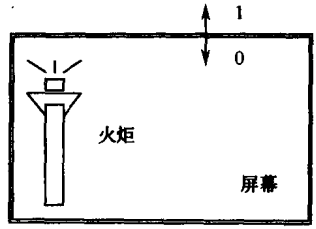

图 1-1　火炬电报

2. 光通信

在电报系统发明并推广之前，第一个得到成功应用的通信系统是由法国工程师 Claude Chappe 于 1793 年发明的。他的系统由建立在高山顶或教堂的塔尖上的一些巨大的木制建筑物组成，并由配有望远镜的公务员进行操作。该信号系统包括三个可移动的部分：一个调节器和两个指示器（如图 1-2 所示）。

图 1-2　Chappe 的信号系统

系统的臂部可以按 45° 的角度增量移动，故从理论上来说，三个可移动部分组合起来后，系统可被设置为 256（8×8×4）个不同的位置。其中，对于容易混淆的组合则可以不用，比如指示器与调节

器的角度相同或相似的位置。此外，有效位置中的一半用来对数字、标点符号、大写及小写字母进行编码，另外一半则用于特殊的控制码。当公务员从邻近的站点读到信号后，便将其复制到自己的系统，从而将信息继续传下去。

在电报系统流行之前，对 Chappe 的信号系统的使用曾一度达到了高峰。建立了至少 556 个站点，其网络覆盖了 3000 多英里，几乎遍及了法国的每一个地方。当然，该系统也存在协议上的问题，比如当前、后两个站点同时向中间站传送同样的消息时，中间站点的操作员该怎么办？

在这个时期，几乎每个国家都有一套或多套与 Chappe 的系统相类似的反射光的信号系统。比如，英国舰队使用了一套由六扇百叶窗组成的系统，该系统如图 1-3 所示。在传送消息时，每扇百叶窗可打开或关闭，从而相当于一个 6 比特的二进制编码。六扇百叶窗都关闭时代表“未准备好”，六扇都打开时则代表“准备发送”。与之相似，瑞典也发明了一套使用十扇百叶窗传送消息的系统。在这类系统中，已经包括了一系列对通信进行控制的功能，如会话控制（开始、结束）、差错控制、流量控制（重传）、速率控制（减慢、加快），甚至否定确认（如“看不见”）等。

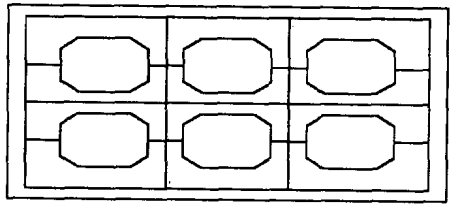

图 1-3　六扇百叶窗信号系统

3. 电磁通信

电报的基本原理最早出现在 1753 年一个署名“C.M”的神秘人

物给 Scots 杂志的一封信中。该信中描述了一个使用一些平行电线来通信的电子电报。1830 年后不久，英国的 Michael Faraday 和美国的 Joseph Henry 发现了电磁感应。1837 年，英国的 William Cooke 根据电磁感应的原理构造了第一套电报。William Cooke 利用电流来使处在接收端磁场中的罗盘指针发生偏转，从而得到信号。这种“针示电报机”的思想在 William Cooke 与 Charles Wheatstone 于 1837 年合作发表的文章中进行了详细的阐述。电报系统的第一个专利便是诞生于 1837 年 6 月 12 日的五磁针信号系统。如图 1-4 所示，五颗磁针中的任意两颗可以向右或向左偏转，从而足够表示 20 个不同的字母。其后不久，William Cooke 与 Charles Wheatstone 相继开发了单针电报的传输代码，其中还包括了等待、重传等控制代码。例如，磁针连续 10 次向右击打表示“重传”码。

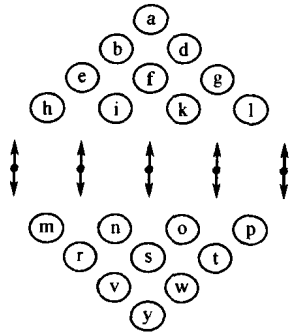

图 1-4　五磁针信号系统

William Cooke 花了很大的精力来向英国的铁路公司推销他的系统，将其作为一种交通控制工具。1842 年，William Cooke 发表了一本小册子，在其中对该系统将带来的好处进行了过于乐观的估计：“火车可以无所畏惧地行驶，而无论其时间是否正确，也不管其是否在正确的轨道上，因为在使用该系统后，其速度总可以及时地降下来，从而避免了碰撞。”不久以后，该系统在英国铁路系统的一些

线路上被采用，其操作成本仅为光通信系统的十分之一，并且传输速度要比未采用此系统前快得多。

William Cooke 的电报系统最初主要用于铁路收发信号，但不久后就在各行业推广开来。1851 年，伦敦与巴黎的证券交易所使用电报系统进行了连接，同时也诞生了第一个公众电报公司。这个时候广泛使用的信号码是改进的莫尔斯电码，即使用两个常见的信号元素：点和线。后来，对该手工操作系统的第一个改进是“纸带读出穿孔器”。1858 年，惠斯登（Wheatstone）设计实现了惠斯登自动电报机，其传输速率可达到 30 bps。同时，在 1850~1950 年间，另外两个我们现在所熟知的通信方法——电话和无线电，也相继诞生并且不断得到发展。

1.1.2 协议缺陷的教训

William Cooke 的电报系统从通信技术上来说是无可非议的，但在使用了该系统后，却引起了一连串的火车事故。下面我们来看发生在 1861 年 8 月的英国克莱顿隧道的事故。

英国的克莱顿隧道应该是当时英国的铁路中保护得最好的一段。在该 1.5 英里长的隧道的两端，一天 24 小时都有信号员值班，并且在 1841 年的时候，该隧道还配备了一套新的“空间空闲/阻塞信号系统”。在隧道的两端都有信号发射器，并且“空闲/阻塞信号系统”能够保证任何一辆火车通过绿色信号时会自动将该信号设为红色，之后再由信号员将信号重设为绿色。当然，在重设信号之前，要确信从该端进入隧道的火车已经在另一端出现。穿过隧道的轨道有两条，每个方向各一条。在任意时刻，隧道中的每一条轨道上只允许有一列火车经过。此外，作为更加安全的措施，隧道还装配了单针电报，用来在隧道两端的信号员之间交换预先已定义的少量消息。

一般情况下，在允许火车进入隧道的一端（A）之后，该端的