信息网络安全控制

Security Control for Info-Net

卢昱　王宇　吴忠望　编著

国防工业出版社
National Defense Industry Press

信息网络安全控制

Security Control for Info-Net

卢昱　王宇　吴忠望　编著

国防工业出版社

·北京·

前　言

以计算机通信网络为代表的各类信息网络，如 Internet、空间信息网络、院校网络、政府办公网络等，随着互联设备、应用服务、数据信息、使用人员等的不断增多，成为了越来越复杂的人机不确定系统。很多区域性的安全防护技术，如终端的访问控制技术、网络边界的防火墙技术、基于网络的入侵检测技术、链路的数据加密技术等，虽然从一定程度上增强了部分网络节点或链路的安全性，但是，在面对日益复杂多变的网络攻击技术和手段时，很难从整体上保护整个信息网络的安全，网络系统的安全可观性和可控性很差，进而导致安全管理的效率很低。

网络安全控制是运用控制论和系统论的思想，研究如何运用反馈控制的原理和方法，对复杂并且不确定的信息网络实施安全控制。采用这种方式，不论被控的网络系统内部组成结构及其相互关系多么复杂，均可运用黑箱或灰箱控制原理及其分析方法，从系统结构和系统行为两个方面进行观测、分析和调节，使被控网络的安全状态保持稳定，改变了“头痛医头、脚痛医脚”的传统安全防御思想。

本书以网络控制论为理论指导，以增强信息网络安全可控性为目标，重点研究信息网络安全控制的体系结构和分析方法。通过安全控制体系结构的研究，明确实施信息网络安全控制的结构、方法、手段、技术、模型和评价安全控制效能的指标，为设计信息网络安全控制系统、评价系统的安全可控性奠定基础。通过安全稳

定性分析方法和安全可控性分析方法的研究，为分析系统的安全控制性、增强系统的安全可观性和可控性提供科学手段。

本书对于充实和完善网络控制论的理论和方法体系，科学规划下一代安全、可控网络，改进现有网络的安全可控性和可观性，都具有重要的作用和意义。

作 者

2010 年 9 月

目 录

第1章 绪 论

1.1 控制论的发展历史与现状

控制论创始人维纳在他的《控制论》[1]一书的副标题上标明，控制论是“关于在动物和机器中控制和通讯的科学”。

控制论是多门科学综合的产物，也是许多科学家共同合作的结晶。控制论(Cybernetics)一词，来自希腊语，原意为掌舵术，包含了调节、操纵、管理、指挥、监督等多方面的涵义，维纳以它作为自己创立的一门新学科的名称，正是取它能够避免过分偏于哪一方面而“不能符合这个领域的未来发展”的意思，也是“纪念关于反馈机构的第一篇重要论文”。1948 年维纳的《控制论》出版，宣告了这门科学的诞生。

控制论诞生后，得到了广泛应用并迅猛发展，大致经历了三个发展时期。

第一个时期为 20 世纪 50 年代经典控制论时期。这个时期的代表著作为我国著名科学家钱学森 1954 年在美国发表的《工程控制论》。

第二个时期为 20 世纪 60 年代现代控制论时期。导弹系统、人造卫星、生物系统研究的发展，使控制论的重点从单变量控制向多变量控制，从自动调节向最优控制，从线性系统向非线性系统转变。美国卡尔曼提出的状态空间方法以及其他学者提出的极大值原理和动态规划等方法，形成了系统测辨、最优控制、自组织自适应系统等现代控制理论。

第三个时期为 20 世纪 70 年代后的大系统理论时期。控制论

由工程控制论、生物控制论向经济控制论、社会控制论发展:1975年国际控制论和系统论第三届会议,讨论的主题就是经济控制论的问题;1978年的第四届会议,主题又转向了社会控制论。电子计算机的广泛应用和人工智能研究的开展,使控制系统显现出规模庞大,结构复杂,因素众多,功能综合的特点,从而控制论也向大系统理论发展。

控制论是研究各类系统的调节和控制规律的科学,它是自动控制、通信技术、计算机科学、数理逻辑、神经生理学、统计力学、行为科学等多种科学技术相互渗透形成的一门横断性学科。它研究生物体和机器以及各种不同基质系统的通信和控制的过程,探讨它们共同具有的信息交换、反馈调节、自组织、自适应的原理和改善系统行为、使系统稳定运行的机制,从而形成了一套适用于各门科学的概念、模型、原理和方法。

控制论的研究表明[2],无论自动机器,还是神经系统、生命系统,以至经济系统、社会系统,撇开各自的质态特点,都可以看作是一个自动控制系统。在这类系统中有专门的调节装置来控制系统的运转,维持自身的稳定和系统的目的功能。控制机构发出指令,作为控制信息传递到系统的各个部分(即控制对象)中去,它们按指令执行之后再把执行的情况作为反馈信息输送回来,并作为决定下一步调整控制的依据。这样就看到,整个控制过程就是一个信息流通的过程,控制就是通过信息的传输、变换、加工、处理来实现的。反馈对系统的控制和稳定起着决定性的作用,无论是生物体保持自身的动态平稳(如温度、血压的稳定),或是机器自动保持自身功能的稳定,都是通过反馈机制实现的,反馈是控制论的核心问题。控制论就是研究如何利用控制器,通过信息的变换和反馈作用,使系统能自动按照人们预定的程序运行,最终达到最优目标的学问,是具有方法论意义的科学理论。

自1948年维纳发表著名的《控制论》以来,控制论经过50多年的发展,与其他的学科互相结合,产生了许多新的边缘学科和综合学科。这些学科不断地"分化—结合",形成了以控制论为核心

的“学科树”和“学科林”。控制论发展到今天已经取得了辉煌成就，诞生了工程控制论、生物控制论、经济控制论、社会控制论和人口控制论等一系列现代控制论的分支学科。与此同时，控制论与其他学科的界线也越来越模糊，理论创新的难度也越来越大，理论和实际结合还存在不少问题。

计算机网络是复杂的网络系统，对该系统的研究是控制论的一个极富挑战性的领域。为了寻求网络系统中控制和管理的新方法和新途径，卢昱等[3]将控制论（包括大系统控制论）、系统论[4,5]、信息论的思想和方法引入到信息网络领域，形成了应用控制论的概念和方法来研究网络系统的一般理论，提出了网络控制论（Network Cybernetics，NC）的概念。网络是一个互联互通的结构，对于状态流的监测和控制流的传递都提供了良好的基础，在网络领域研究网络控制具有很强的适用性；而且，网络应用、网络安全和网络攻防等各个方面的问题都可以归结为网络状态控制、资源控制和行为控制的问题。可以预见，以网络控制论为核心的新的网络控制理论和技术能够为网络控制提供更为有效的方法和手段，能够为解决日益严峻的网络安全和管理问题提供新的途径。

随着人类社会进入信息时代，控制论的发展又面临新的巨大挑战和重大机遇。控制论应当而且可以在信息化和现代化的建设中发挥作用，应当而且能够为网络化、集成化、协调化和智能化的实现提供方法支持。可以预见，控制论发展前途光明，仍将是高新技术的前沿和推动新技术革命的核心力量之一。

1.2 网络控制的发展历史与现状

网络控制是随着计算机网络的出现与发展而逐步发展起来的。计算机网络是计算机科学和通信科学紧密结合的产物。在计算机网络的发展中，有从通信到计算机和从计算机到通信的说法，前者说明提供图形图像、音频和视频数据的通信系统对计算机系统的依赖正在不断增加，后者说明计算机间的互联和交互需要越

来越多的通信技术。网络的诞生正是计算机与通信技术相互融合的必然。

网络控制是控制论与计算机网络这两个学科交叉发展的一个产物，目前正面临着一个新的生长期。比较控制和网络的交叉发展，也存在从网络到控制和从控制到网络的说法。前者是指在计算机网络环境下，研究控制技术的变革，即利用计算机网络实现更广泛、更复杂、更迅捷的控制。目前已有不少学者开展了这个方面的研究工作，也有不少厂商开发出了相应的产品，如集散（分布）式控制系统 DCS（Distributed Control System）、现场总线控制系统 FCS（Field－bus Control System）等。后者是指用控制论、系统论的概念和方法去研究和解决计算机网络本身的控制问题，这一类的研究现在还很少。

计算机网络是复杂的大系统，对该系统的控制研究是控制理论的一个极富挑战性的领域。如前面所述，网络是计算机和通信技术结合的产物。对于网络中出现的问题，如路由控制、流量控制等，是从计算机和通信科学的角度出发来寻找解决办法的，这些研究已经取得了并将继续取得大量成果。但是随着网络技术及其应用的飞速发展，网络中出现的更加复杂的问题必须用大系统控制论[6]和系统科学的方法与技术来解决，这也是网络控制得到进一步发展的动力所在。

目前，网络控制已经得到了比较广泛的认同和应用。以美军的全球信息栅格（Global Information Grid，GIG）为例，为了增强信息战和网络中心战能力，2001 年，美军在规划 GIG 的重要组成部分：全球指挥与控制系统（Global Command and Control System，GCCS）的体系结构时，提出了增强系统生存能力的解决方案[7]，具体包括：

（1）采用高级中间件技术，将 GCCS 的功能分布到所有可用的服务器上（有利于资源或服务的分配、查找和调度）。

（2）加固每个客户和服务器平台，通过代理服务器，以及运行在不同平台上的，支持冗余备份的服务器，实现关键服务的备份

恢复。

(3) 升级当前的局域网,提供备份信息路径,增强入侵检测和响应能力。

(4) 通过网络控制组件收集来自客户端、服务器、网络和应用程序的入侵检测数据,诊断系统范围的攻击状态,调度系统范围的控制组件做出响应,以最小化攻击造成的影响。

GCCS 可生存客户端系统的概念模型如图 1.1 所示。

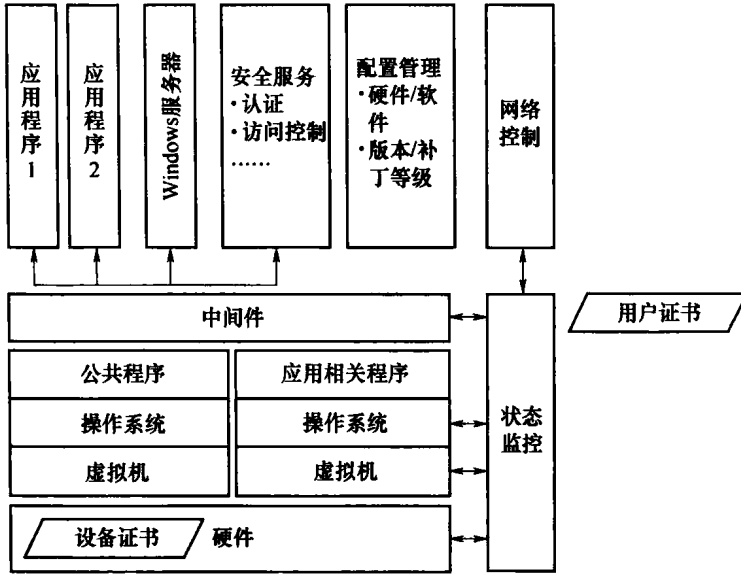

图 1.1 GCCS 可生存客户端系统概念模型

从这个模型可以看出,网络控制和中间件技术是实现可生存 GCCS 的关键。网络控制能将系统中所有的传感器、分析器和激励器集成起来,构成若干反馈控制回路,使之不但能观测来自系统或网络不同层次的状态信息,还能收集、整理、融合这些信息,并针对可疑的入侵和攻击行为调整系统的配置。

从 2005 年开始,国内外安全企业,如微软、启明星辰、天融信、瑞星、趋势科技等公司逐步认识到,单纯采用防火墙、入侵检测系

统等网络安全产品，从网络边界或局部网络区域保护网络的安全，是无法应对日益复杂的网络应用和层出不穷的网络攻击事件的。面向应用的网络攻击事件，如基于 Web 服务漏洞的攻击、垃圾邮件攻击、以网络钓鱼为代表的社会工程攻击以及各种恶意代码攻击等，对开放网络的安全带来了新的巨大的挑战。构建一体化的安全控制系统，把网络终端设备、服务器、安全基础设施等统一管理起来，实施全方位、整体性的监控调度，建立全网范围内的检测、分析、显示、响应和恢复控制体系，已经成为提高网络可观性、可控性和安全性的必然途径[8]。

1.3 网络安全的发展历史与现状

计算机网络安全的发展大致经历了三个重要阶段。

1. 通信保密阶段(1940 至 20 世纪 70 年代，COMSEC)

通信保密阶段以密码学研究为主，重在数据安全层面。这一阶段的主要安全威胁是搭线窃听、密码学分析，主要保护措施是通过加密解决通信保密问题，保证数据的机密性与完整性。通信保密阶段的重要标志有：

(1) 1949 年 Shannon 发表的《保密通信的信息理论》。

(2) 1977 年美国国家标准局公布的数据加密标准(Data Encryption Standard，DES)。

(3) 1976 年由 Diffie 与 Hellman 在“New Directions in Cryptography”一文中提出了公钥密码体制。

2. 计算机系统安全阶段(1970 至 20 世纪 80 年代，INFOSEC)

主要针对计算机信息系统的安全性进行研究，重在研究物理安全与运行安全，兼顾数据安全。这一阶段的主要安全威胁扩展到非法访问、恶意代码、脆弱口令等，主要保护措施是安全操作系统设计技术，确保计算机系统中硬件、软件及正在处理、存储、传输信息的机密性、完整性和可控性。计算机系统安全阶段的主要标志是 1983 年美国国防部公布的可信计算机系统评估准则(TC-

SEC),它将操作系统的安全级别分为四类七个级别(D、C1、C2、B1、B2、B3、A1),以便于安全测评[9]。

3. 信息网络系统安全阶段(20 世纪 90 年代以后,NETSEC)

开始针对信息安全体系进行研究,重在运行安全与数据安全,兼顾内容安全。这一阶段的主要安全威胁发展到网络入侵、病毒破坏、信息对抗的攻击等,主要保护措施包括防火墙、防病毒软件、漏洞扫描、入侵检测、公钥基础设施(Public Key Infrastructure,PKI)和虚拟专用网(Virtual Privacy Network,VPN)等,通过这些措施重点保护需要保护的信息,确保信息在存储、处理、传输过程中不被破坏,确保合法用户能够获得服务,限制非授权用户访问信息系统或相关服务,并提供必要的防御反击措施,并强调保护信息的机密性、完整性、可控性与可用性。信息网络系统安全阶段的主要标志是提出了新的安全评估准则 CC(ISO 15408 标准)[10,11] 和 IPv6 的安全性设计。

目前网络安全研究发展面临的现状是:安全技术与产品的研发始终无法跟上与满足网络安全保障的客观需要。其根本原因是:目前的网络安全解决方案都缺乏整体的安全策略,不能从系统和控制的观点来分析、研究和构建网络安全体系,网络的安全可控性、可观性和稳定性较差,当然这和互联网开放、复杂及不确定因素众多的特点有关。数据加密、防火墙、访问控制和入侵检测等安全技术与产品只是解决了网络的某一局部或某个环节的安全问题。中国工程院何德全院士也指出:"从现实来讲,将各组件作为黑箱,用控制论的方法达到对各组件的动态安全控制是一个可行的途径。"[12] 因此,要提高整个网络系统的安全,需要运用控制论、系统论的方法和技术进行理论创新,在网络控制论[3] 的指导下研究网络的安全控制。

1.4 安全控制是网络控制研究的重点方向

信息网络安全本身和解决信息网络安全问题都是一个过程。

这个过程既包括了安全利益关系和目标的变动不定，也包括了安全威胁与保护的技术手段的此消彼涨，还包括“技术工程平台”的结构变化，更包括了人和社会组织关于信息的行为规则的不断调整。这是一个复杂系统的控制论过程，也是一个不断反馈从而不断优化安全能力的过程。无论从社会还是从技术上，无论从目的还是从手段上，都没有一成不变的安全、一劳永逸的安全和一蹴而就的安全。因此，信息网络的安全控制问题随之涌现[13]。

信息网络的安全控制是伴随着通信、计算机和网络安全发展的历史逐步凸显出来的、亟需解决的现实问题。从历史发展的角度来看，20 世纪 40 年代左右，为了提高数据通信的安全，出现了通信的保密控制和电磁频谱控制等控制手段；20 世纪 60 年代至 70 年代，为了确保计算机系统的安全，出现了以访问控制为代表的安全控制手段；20 世纪 80 年代以后，随着计算机网络的发展，才出现了诸如完整性检测与保护、内容过滤等针对信息可用性、完整性的安全控制措施，安全控制的重要性和必要性日显突出。在控制的体系结构方面，信息网络的安全控制主要经历了以下几个发展阶段。

（1）以计算机为中心的访问控制阶段。典型的访问控制模型包括可信计算基（Trusted Computing Base，TCB）、参考监视器（Reference Monitor，RM）等。

（2）以边界防护为主的“洋葱”控制。即运用分层防御的思想，实施深度边界防御，边界防护的代表是防火墙、虚拟专用网和入侵检测系统，但是这些系统各自为主，缺乏联动。

（3）以统一威胁模型（Uniform Threat Model，UTM）为代表的内网安全监控。在认识到分散控制的不足后，采用了集中控制的方式，将各种安全技术和手段综合集成起来，重点保护关键网络、应用或服务的安全，如目前出现的各种内网安全控制系统、入侵防护系统以及集中式的安全网关等。

从上述发展历史可以看出，目前信息网络的安全控制还存在