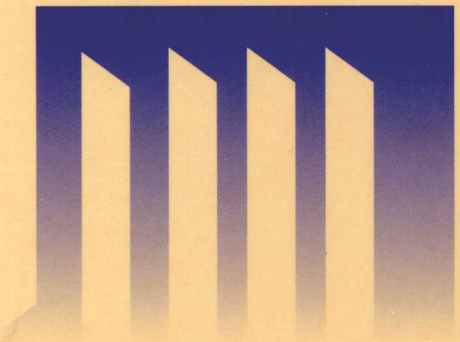
军队“2110工程”建设项目 信息安全技术

网络安全与控制技术

WANGLUO ANQUAN YU KONGZHI JISHU

王宇 卢昱 等编著



国防工业出版社
National Defense Industry Press

序

计算机技术、通信技术、网络技术的发展，给军队指挥自动化系统、综合电子信息系统的建设与发展带来了深刻的影响。未来以电子战、网络战和作战保密等为主要作战样式的信息化战争，离不开信息技术的支撑。武器装备的信息化、网络化加快了信息技术在装备的研制、试验、采购、指挥、管理、保障和使用全过程中的渗透与应用。因此，在军队深入开展军事信息技术学科的建设，加强军事人才信息化素质与能力的培养，是继往开来的一件大事，也是对军事装备学、作战指挥学等学科建设的有力支持。

为了总结梳理装备指挥技术学院军事信息技术学科的建设成果，提升学科建设水平和装备人才培养质量，在军队“2110 工程”专项经费支持下，在装备指挥技术学院“2110 工程”教材（著作）编审委员会统一组织指导下，军事信息技术学科领域的专家学者编著了一批适应装备人才培养需求，对我军装备信息化和装备信息安全工作具有主要指导作用的系列丛书。

编辑这套丛书是我院军事信息技术学科建设的重要内容，也是体现军事信息技术学科建设水平的重要标志。通过系统、全面地梳理，将军队开展信息化建设的实践经验进一步理论化、科学化，形成具有军事装备特色的军事信息技术知识体系。

本套丛书定位准确、内容创新、结构合理、针对性强，一方面总结了我院军事信息技术学科建设和装备信息化人才培养的理论研究与实践探索的重要成果和宝贵经验；另一方面紧紧围绕我军武器装备信息化建设的需要，以装备全寿命管理的信息化和装备信息保障为主要内容，着重基本概念、原理的论述和技术方法的应用，其编著出版对于推进军事信息技术学科的建设，提高装备人才的培养质量，加快装备信息化建设和军事斗争准备具有十分重要的现实意义和深远的历史意义。

装备指挥技术学院
信息安全技术教材（著作）编委会
2009 年 12 月

前　言

网络技术、通信技术的发展使得网络的时空范围不断扩大，各种具有联网功能的设备及终端越来越多，人们接入网络、使用网络的机会越来越多、频率越来越高，网上信息越来越丰富，网络正逐渐成为人们工作与生活中不可或缺的组成要素。然而，网络空间（Cyberspace）从来就不是风平浪静的！在现实社会空间中存在的各种利益冲突和斗争，同样反映在网络空间中：病毒、木马、后门、僵尸网络、伪装欺骗等各种形式的攻击方法与技术在黑客、间谍等手中不断推陈出新，而新的系统及应用的安全漏洞层出不穷，网络安全与控制将成为当今及今后很长时期内网络化、信息化不可回避的关键问题。

网络安全与控制技术是以网络控制论为指导，以密码学为基础，以网络安全保障体系和控制体系为框架，以各种安全基本技术、应用技术为基石，以网络安全控制为手段与方法，目的是尽可能降低与控制网络的安全风险，确保网络信息的机密性、完整性、可用性、可控性和不可否认性。实现计算机网络安全是一项系统工程，必须掌握全面、系统的技术方法，提高工程实践能力。

本书重点讲述了计算机网络领域中的安全技术问题，涵盖了网络安全保障与控制体系、网络安全基本技术、应用技术及网络攻击技术，在此基础上，着重介绍了网络安全基础设施 PKI 与 PMI，实施网络安全工程的方法，以及如何实现统一身份认证与授权，如何进行安全协议的设计，如何构造容侵与容灾系统等。本书第 1 章由吴忠望编写，第 2、第 5、第 8、第 10 章由王宇编写，第 3、第 4、第 11 章由韩伟杰编写，第 6、第 7 章由顾晓丹编写，第 9 章由姚宏林编写，卢昱负责全书的

编审。书中参考借鉴了大量学者的资料和最新研究成果，在此表示衷心的感谢。书中难免存在错误和不当之处，望广大读者批评指正，以便进一步修订完善。

编著者

2009年12月

目　录

第1章 绪 论

本章从控制与网络两个学科领域交叉发展的角度，引出网络控制、网络控制系统和网络安全控制等概念，对网络控制系统的体系结构、控制功能和网络安全控制技术做了初步介绍。

1.1 网络安全与控制的提出

控制论创始人维纳(Wiener N.)在他的《控制论》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信的科学”，意味着控制与人、计算机、通信是密切相关的。计算机网络的出现正是通信技术和计算机技术交互发展的产物，也是由人、计算机、通信和控制等要素集成的复杂巨系统。近半个世纪以来，控制和网络两个学科领域交叉发展，一方面，在计算机网络环境下，控制技术取得很大变革，出现了集散(分布)控制系统和现场总线控制系统等；另一方面，在控制理论、系统理论和网络系统的结合过程中，网络控制论和网络控制技术也取得了较大突破。运用控制论的观点和方法来审视和分析当前的网络问题，不仅在理论根源上是必需的，而且在实践应用中也是可行的。网络安全问题是随着网络技术及其应用的飞速发展而出现的一个非常复杂的问题，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。数据加密、防火墙、访问控制和入侵检测等都只是解决了网络的某一局部或某个环节的安全问题。网络安全问题需要运用控制论、系统论的方法和技术进行理论创新，在网络控制论的指导下研究网络的安全控制。

网络的开放性和不确定性带来的网络安全问题，一直备受关注而没有有效的解决方案。目前的信息安全技术大都缺乏统一的理论指导，都是针对某一方面或某个层次的安全问题提出的解决方案，很难从整体上和根本上解决网络信息安全问题。各种信息系统尤其是网络，因其自身的可控性、封闭性、专用性特点和在国家安全中的特殊作用，对系统的安全提出了更高需求。针对网络安全性的要求，可以从控制的角度考虑其安全问题，通过将系统的设备、人员、应用和环境纳入受控的体系，将系统中的各种进程、行为、状态都控制起来，减少整个系统的不确定性，而达到增强系统安全性的效果。网络安全控制就是要在尽量不改变现有信息基础设施的基础上，在系统的各个层次分

别安装控制器，各种控制器协同工作，构成一体化的安全控制系统，从而解决网络的安全问题。

1.1.1 网络控制与网络控制系统

网络控制是指施控网络主体对受控网络客体的一种能动作用，这种能动作用能够使得受控网络客体根据施控网络主体的预定目标而动作，并最终达到这一目标。网络控制作为一种作用，至少需要作用者（即施控主体）与被作用者（即受控客体），同时还需要有将作用传递到受作用者以及将受作用者的状态传递到作用者的两种传递者。

网络控制系统是由各种有序的相互联系的网络元素有机结合而成的集合。该集合可以包含许多子集合，它们之间具有各种联系而形成较复杂的结构；它们在某种网络控制和管理的目标下，以整体方式执行整个系统的某种网络功能。这里复杂结构的含义是：网络控制系统可以由各种子系统组成，它们体现为网络上不同的方面、不同的层次，各自相应有不同的子目标，执行不同的子功能。

在网络控制系统中，至少需要有施控部分、被控部分、控制环节和反馈环节四个组成部分。有了这四个组成部分，网络控制系统作为一个整体才能具有控制的功能和行为，而这些又总是相对于某种环境而言的。由于网络系统是由一些相互制约、相互作用的网络元素构成的，并具有整体的功能和行为的统一体。所以，上述四种元素构成了相对于某种环境的具有控制功能与行为的网络控制系统。网络控制系统的基本结构如图 1－1 所示。

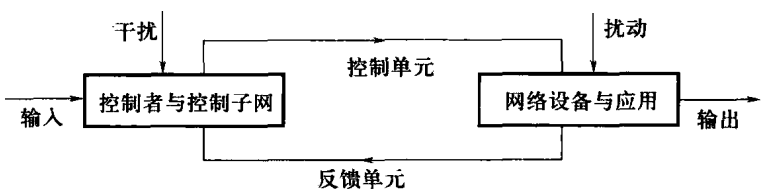


图 1－1　网络控制系统结构参考模型

网络设备和应用属于被控部分，包括各种网络的组成设备和网络中运行的各种信息系统。

控制者和控制子网属于施控部分，其中控制者包括各种网络管理人员和网络应用系统的使用人员，控制子网包含各种网络控制系统和网管中心。

控制单元包括各种控制作用和控制通道。网络控制系统在控制作用的影响下，能够改变自己的运动而进入某种状态。控制作用在某种意义上可以说是按一定目标对受控系统在状态空间中的各种可能状态进行选择，使系统的运动达到或趋近这些被选择的状态。因此，没有选择的目标就没有控制。控制通道是

控制信息得以流通的各种控制结构、控制方式和传输介质的组合，它可以是物理的组合，也可以是逻辑的组合。在控制通道上，控制信息从施控部分传递到被控部分，属于前向通道。

反馈单元包括反馈作用和反馈通道。网络控制系统在反馈作用的影响下，能够监视系统处于何种状态。反馈作用在某种意义上可以说是针对一定目标对受控系统的状态进行监测、分析和报告，使施控系统能及时做出响应，反馈作用的存在是控制论系统的典型特征。反馈通道由各种信息采集和分析设备、信息反馈和决策系统等组成。在反馈通道上，反馈信息从被控部分传递到施控部分，属于反向通道。

整个网络控制系统对外界而言，并不是一个封闭系统，它和外界环境之间存在物质、能量和信息交换。它的施控部分可能还有外界的输入和干扰，被控部分还可能受到外界的扰动或对外界有输出。这样，网络控制系统既是自成一体、构成闭环的完整体系，又是和外界互相作用、互相联系的开放系统。

1.1.2 网络控制系统的体系结构

网络控制系统的体系结构就是关于如何建造网络控制系统的技术。它给出了网络控制系统基本组成与功能，描述了网络控制系统各组成部分的关系以及它们集成的方式或方法，刻画了支持网络控制系统有效运转的机制。

目前，明确地对网络控制系统的体系结构进行论述的文献很少，我们将网络控制系统的体系结构定义为划分网络控制系统的基本部件，指定系统部件的目的与功能，说明部件之间如何相互作用、如何集成为一个整体以及通过何种机制实现整体功能的技术。

网络控制系统的体系结构贯穿“分解”与“集成”两条主线。网络控制系统的体系结构在一定程度上就是对网络控制系统进行剖解，必须标识出网络控制系统的基本组成成分，能够清楚地说明网络控制系统是由哪些关键部分结合在一起形成的。同时，网络控制系统的体系结构还必须能够对各部分的功能、目的、特点等进行清晰的描述，使人们能够了解各个组成部分的作用。这些都是“分解”的作用，在“分解”的基础上，网络控制系统的体系结构还需要进一步描述“集成”起来的功能，即在充分了解网络控制系统的各个组成部分的作用机理、作用方式等的基础上，将这些部分按照一定的方式进行组织和集成，形成一个具有特定功能的整体对外提供服务。

为了实现网络控制就必须有相互遵守的控制协议。这里的控制协议是指为了实现特定的控制而定义的网络系统元素之间控制与被控制的方式以及控制过程中交换的信息结构，如图 1－2 所示。它侧重于外部的、相互之间的行为而不是内部的特征，这对定义网络控制系统体系结构很有使用价值。

控制服务是由它使用的控制协议和实现的网络行为定义的，如图 1 - 3 所示。标准的协议还使得定义标准服务更加容易。标准服务的定义，如对计算资源的访问，存取数据，数据加密、数据传输控制等，可以进一步提供增强网络控制的能力，使用户得到更多的控制及安全服务。由于这些服务抽象掉了与资源相关的细节，所以，非常有利于应用的开发。

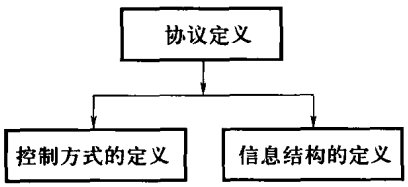


图 1 - 2　控制协议定义的两个方面

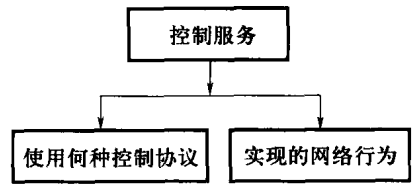


图 1 - 3　控制服务定义的两个方面

1.1.3　网络控制系统的控制功能

网络控制的对象是网络的各种资源，这些资源的抽象就是信息。因此，在建立网络控制系统的功能参考模型的过程中，可以从资源和信息的角度来考虑网络控制系统的控制作用与功能。另外，随着网络应用日益发展，网络控制与许多专业领域紧密结合，出现许多专有的网络控制功能。所以，可以从资源维、信息维和专业维三个角度建立网络控制系统的多层多视点功能参考模型，如图 1 - 4 所示。

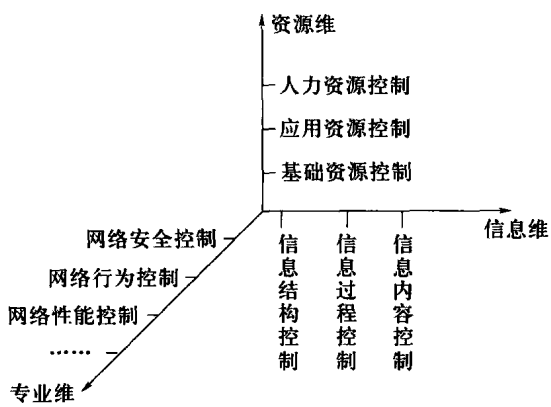


图 1 - 4　网络控制系统的控制功能参考模型

1.1.3.1　资源维网络控制

资源维网络控制是指按照网络资源的组成方式实施的网络控制，又可以成为网络资源控制或简称为资源控制。

网络控制系统是利用信息技术实现的信息自动化系统，它包括了物理上众多的人员和信息设备，以及逻辑上的信息资源、使用方法和信息流逻辑，是一个现实世界中用信息技术实现的系统。为了研究网络控制系统，我们需要有一个

合理的资源分类方法。这里，我们将网络控制系统中的资源分为三种。

（1）人力资源：网络系统的决策者、使用者和管理者。

（2）应用资源：是指面向业务的技术资源，由一些业务逻辑组件及界面组件组成。应用资源虽然也表现为软件或硬件组件，但通常更体现在它能为人解决什么样的问题。应用资源用技术的形式实现了一部分人执行业务的逻辑或智能。

（3）基础资源：为开发应用组件而提供技术上支撑的资源，包括网络设施、操作系统软件等。基础资源更多的是一些具体的技术，它们通常逻辑较简单，为应用类资源的实现提供服务。这类资源往往种类繁多，一般包括一系列的物理设施、电子设施、网络技术、操作系统等。

根据网络系统的资源类型，资源控制可以分为人力资源控制（人员控制）、应用资源控制（应用控制）和基础资源控制。其中，人员控制包括角色控制、权限控制等，应用资源控制包括计算控制、共享控制等，基础资源控制包括平台控制、通信控制等，如图 1－5 所示。

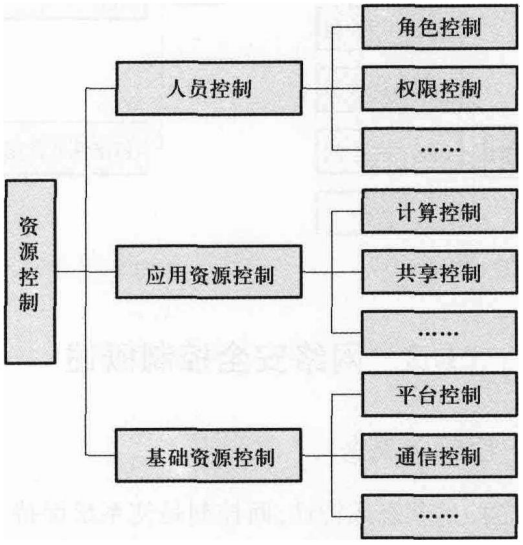


图 1－5　资源控制的组成

1.1.3.2　信息维网络控制

信息作为网络系统各种资源的逻辑抽象，既是网络控制的重要对象，又是控制得以实现的重要条件。网络控制系统所有控制功能，可以通过对信息进行有效控制而实现。没有信息，就谈不上网络控制。信息维网络控制（简称信息控制）包括信息结构控制、信息过程控制和信息内容控制，如图 1－6 所示。

1.1.3.3　专业维网络控制

在许多与网络技术相关的专业领域里，控制理论得到了广泛运用，形成了专