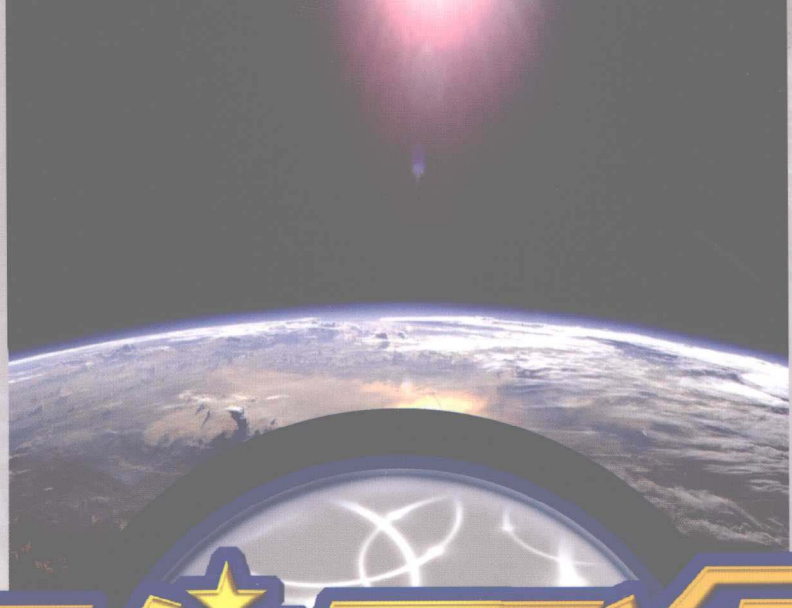

可信互联网

若干问题研究

杜秀娟 著

西安交通大学出版社
XI'AN JIAOTONG UNIVERSITY PRESS

青海省科技厅应用基础研究项目（项目编号：2010-J-728）资助研究

973计划前期研究专项（2011CB31189）资助研究

青海师范大学博士立项计算机学科建设专项经费资助出版

杜秀娟 著

西安交通大学出版社
XI'AN JIAOTONG UNIVERSITY PRESS

内容简介

大量移动设备的接入，使互联网呈现出大规模、复杂性和异构性的发展趋势。本书分别从用户终端、中间节点和互联网骨干等三个层面对互联网系统进行了加固，主要包括 MPLS 骨干网络的可信接入、无线网络的匿名通信、用户隐私保护以及违反协议的不良行为的检测等。

对于学习和理解计算机网络安全的本科生和研究生，本书可作为他们的参考书；而对于那些从事网络工程、网络安全的工程技术及研究人员，本书则是一本很好的参考读物。

图书在版编目(CIP)数据

可信互联网若干问题研究/杜秀娟著. —西安：西安交通大学出版社，2011.6

ISBN 978-7-5605-3966-9

Ⅰ.①可… Ⅱ.①杜… Ⅲ.①计算机网络-研究 Ⅳ.①TP393

中国版本图书馆 CIP 数据核字(2011)第 139675 号

书　　名	可信互联网若干问题研究
著　　者	杜秀娟
责任编辑	杨　璠
出版发行	西安交通大学出版社 (西安市兴庆南路 10 号　邮政编码 710049)
网　　址	http://www.xjtupress.com
电　　话	(029)82668357　82667874(发行中心) (029)82668315　82669096(总编办)
传　　真	(029)82668280
印　　刷	西安交通大学印刷厂
开　　本	727mm×960mm　1/16　**印张**　7.5　**字数**　135 千字
版次印次	2011 年 6 月第 1 版　2011 年 6 月第 1 次印刷
书　　号	ISBN 978-7-5605-3966-9/TP·551
定　　价	21.00 元

读者购书、书店添货如发现印装质量问题，请与本社发行中心联系、调换。

订购热线：(029)82665248　(029)82665249

投稿热线：(029)82664954

读者信箱：jdlgy@yahoo.cn

前　言

TCP/IP是目前互联网广为使用的协议。最初的互联网仅作为一种研究工具在科研人员之间使用，使用者之间能够建立良好的信任关系。因此，TCP/IP协议在设计之初以追求高效为目标，忽略了安全因素。近年来，随着互联网在业务种类、用户数量以及复杂度上的急剧膨胀，病毒、木马以及间谍软件的数量和种类也正快速增长，而当前分散、孤立、单一防御、外在附加的网络安全系统已经无法应对具有多样、随机、隐蔽和传播等特点的攻击和破坏行为，互联网正面临着严峻的安全挑战。

随着网络技术和应用的飞速发展，互联网日益呈现出复杂、异构等特点，当前的网络体系已经暴露出严重的不足，网络正面临着严峻的安全和服务质量(QoS)保证等重大挑战，以往那种将安全完全建立在对用户绝对信任的网络模式已经不符合互联网发展的现状，新一代计算机网络必须提供可信性机制以解决安全问题来消除网络脆弱性，国内外研究表明网络安全也正向着可信方向发展。如今，“高可信网络”已被正式写进中国国务院公布的《国家中长期科学和技术发展规划纲要(2006—2020年)》。《纲要》明确指出：“以发展高可信网络为重点，开发网络信息安全技术及相关产品，建立信息安全技术保障体系，防范各种信息安全突发事件。”

随着无线通信技术的发展，大量的移动设备通过WLAN、无线Ad Hoc、无线Mesh等网络接入到互联网。无线网络正以无可比拟的优势成

为下一代互联网的重要组成部分，公共的、灵活的、无缝的异构网络成为未来网络的发展目标。因此，互联网可信性除了包含传统有线网络的可信性之外，还应该包括对用户身份、信息内容的可认证性、无线网络中用户身份位置等隐私的匿名性、存在攻击时的网络可用性、违反网络协议的不良行为的检测以及可控性等。事实上，可信网络架构就是一个通过对现有网络安全产品和网络安全子系统的有效整合和管理，并结合可信网络的接入控制机制、网络内部信息的保护和信息加密传输机制，实现全面提高网络整体安全防护能力的可信网络安全技术体系。

连续两年对可信网络的理论研究和一年的技术实践经验总结构成了本书全部的内容，核心技术部分涉及基于数字短签名的MPLS网络可信访问机制、无线Ad Hoc网络MAC层攻击综合检测方法、基于数字短签名的安全匿名源路由协议等若干可信网络技术研究。

在本书的撰写过程中，天津大学的金志刚教授提出了许多宝贵的意见，在此表示衷心感谢。我还要感谢我的家人和朋友，特别感谢爱人的陪伴和父亲的鼓励，谨以此书献给他们。

由于水平有限，加之时间仓促，本书一定存在缺点，希望得到广大读者的指正，我将在吸取大家意见和建议的基础上，不断修改和完善书中有关内容，为推动该领域的进步尽绵薄之力。

杜秀娟

青海师范大学教授

2011年4月23日

目　录

第一章

绪　论

1.1　研究背景

随着计算机网络技术及应用的飞速发展，人们对信息网络的应用需求与依赖性不断提升，随之而来的信息安全威胁也在不断增加。互联网广为使用的协议是TCP/IP协议簇。最初的互联网仅作为一种研究工具在科研人员之间使用，用户相对单一，使用者之间能够建立良好的信任关系。由于，TCP/IP在设计之初只考虑了执行效率，没有考虑安全因素，又由于TCP/IP是公布于世的，几乎所有应用协议都架设在TCP/IP之上，因此建立在TCP/IP协议之上的互联网存在较大的安全隐患。

以往的互联网将安全完全建立在对用户绝对信任的基础上，这已经不符合互联网发展的现状，新一代计算机网络必须提供可信性机制以解决安全问题来消除网络脆弱性，国内外研究表明网络安全也正向着可信方向发展[1~3]。国际可信计算组织TCG(Trusted Computing Group)TNC(Trusted Network Connect)分组于2004年提出了可信网络连接TNC技术，定义并发布了一种开放的TNC体系架构和一系列标准，为端点准入强制策略开发一个对所有开发商开放的架构规范。目前国内已有不少学者从事可信网络的相关研究，其中包括清华大学林闯、北京交通大学张宏科、解放军信息工程大学郭云飞、中科院软件所吴志美以及电

子科技大学王晟教授等。进入 21 世纪以来，国内相继启动了一系列可信网络研究项目，国家自然科学基金委员会于 2001 年启动并实施了“网络与信息安全重大研究计划”，于 2007 年启动了“可信软件重大研究计划”，《国家高技术研究发展计划(863 计划)“十一五”发展纲要》设立了“新一代高可信网络”重大项目，国家科技部于 2007 年 5 月启动了国家 973 项目“一体化可信网络与普适服务体系基础研究”。

随着无线通信技术的发展，大量的移动设备通过 WLAN、无线 Ad Hoc、无线 Mesh 等网络接入到互联网。互联网呈现出大规模、复杂性和异构性的发展趋势，无线网络正以无可比拟的优势成为下一代互联网的重要组成部分，公共的、灵活的、无缝的异构网络成为未来网络的发展目标[4]。因此，互联网可信性除了包含传统有线网络的可信性之外，还应该包括对用户身份、信息内容的可认证性、无线网络中用户身份位置等隐私的匿名性、存在攻击时的网络可用性、违反网络协议的不良行为的检测以及可控性等。事实上，可信网络架构就是一个通过对现有网络安全产品和网络安全子系统的有效整合和管理，并结合可信网络的接入控制机制、网络内部信息的保护和信息加密传输机制，实现全面提高网络整体安全防护能力的可信网络安全技术体系。

本书在现有研究基础上，提出了基于数字短签名的 MPLS 网络可信访问机制、无线 Ad Hoc 网络 MAC 层攻击综合检测方法、基于数字短签名的安全匿名源路由协议等若干可信网络技术，以期为复杂异构的可信网络研究做出进一步的探索。

1.2 网络安全脆弱性分析与可信网络模型

1.2.1 有线网络脆弱性分析

随着互联网技术的发展，以往那些对单台主机的威胁已经发展为对网络基础设施的攻击，多数网络安全事件都是由脆弱的用户终端和“失控”的网络使用行为引起的[5~6]。病毒的入侵，木马的植入，拒绝服务攻击，地址盗用，DHCP 欺骗以

及 ARP 攻击等之所以对网络产生较大的破坏，是因为它们利用了脆弱的终端节点的连接作为入侵网络的通路。在传统有线网中，用户终端不及时升级系统补丁和病毒库的现象普遍存在。私设 DHCP 服务器、盗用 IP 地址、忽视主机安全管理、滥用企业禁用软件等行为比比皆是。“失控”的用户终端一旦接入网络，就等于给潜在的安全威胁敞开了大门，使安全威胁在更大范围内快速扩散。因此，保证用户终端的安全、阻止威胁入侵网络，对用户的网络访问行为进行有效的控制，是保证网络安全运行的前提，也是目前网络安全管理亟需解决的问题[7~8]。

传统的网络安全问题的解决，通常是被动防御，事后补救。目前，针对病毒与攻击的防御体系还是以孤立的单点防御为主，如在个人计算机上安装防病毒软件、防火墙软件等。当发现新的病毒或网络攻击时，一般是由网络管理员发布告警或补丁升级公告，要求网络中的所有计算机安装相关防御软件。从目前企业病毒泛滥、攻击频繁、损失严重的结果来看，当前的防御方式主要存在以下三方面不足[9~14]。

1. 被动防御，缺乏主动抵抗能力

通常情况下，当终端被发现受到感染时，病毒早已散布于整个网络了。企业用户需要在安全威胁尚未发生时就对网络进行监控和修补，使其能够自己抵御来自外部的侵害。但对网络管理员来说，目前无法有效监控每一个终端安全状态，缺乏隔离、修复不合格终端的手段，因此网络的主动防御能力低下。

2. 单点防御，对病毒的重复、交叉感染缺乏控制

目前解决安全威胁的方式主要采用单点防范。因此，只要网络中有一台机器没有清除病毒仍能够顺利上网，整个网络就会始终处于被感染、被攻击状态。

3. 分散管理，安全策略不统一，缺乏全局防御能力

在传统网络中，任何一台终端的安全状态（终端的防病毒能力、补丁级别、系统安全设置、地址使用和服务的授权运行等），都直接影响整个网络的安全。不符合企业安全策略的终端（如防病毒库版本低，补丁未升级）感染了病毒，它将不断在网络中试图寻找下一个受害者，这在一个没有安全防护的网络中的最终结果可能是全网瘫痪。因此只有从用户的接入终端进行安全控制，才能够从源头上防御威胁。但是，分散管理的终端难以保证其安全状态符合企业安全策略，无法有效

地从网络接入点进行安全防范，无法彻底解决病毒、操作系统漏洞及其他由网络协议脆弱性[15~18]带来的网络安全威胁。

由于 TCP/IP 协议栈最初的设计缺陷，对于接入网络的终端没有信息源验证，而现在的互联网应用环境已发生了巨大变化，用户数量急剧增加且用户素质与技术水平参差不齐，因此有必要在网络的核心部分增加认证、授权等控制机制，从信息安全的源头着手，从根本上遏制网络不安全因素的出现，内外共防来构造可信、可控的网络环境，为用户提供可信任的网络服务。

1.2.2 无线 Ad Hoc 网络概述及其脆弱性分析

现实的互联网涵盖了不同类型的传输技术，可信网络研究必须充分认识到网络的复杂异构性。随着技术的进步，信息社会从个人计算机时代步入到为用户提供随时随地接入和所需信息的普适计算时代[19]，无线网络成为普适计算设备互联的首选技术。WLAN 通过无线接入点等固定基础设施为无线用户提供网络接入和数据传输服务。由于基础设施部署耗时较长、代价较大，在某些地方无法实施等因素，作为下一代网络重要组成部分的无线 Ad Hoc 网络应运而生。移动设备通过无线 Ad Hoc 网络接入到因特网网关，从而有效地将因特网服务扩展到了无基础设施区域。

无线 Ad Hoc 网络起源于 20 世纪 70 年代，是一种多跳、对等的网络，远程节点通过逐跳转发的方式建立连接，任何节点既是分组业务的生成者，也是分组业务的中继者，传统的网络节点与终端系统的划分被模糊淡化。由于无基础设施和中心管理机构，该网络通常被称为移动自组织网络。由于无线信道开放性、完全的分布式组网、资源有限性以及无基础设施等特点，使得无线 Ad Hoc 网络在 TCP/IP 参考模型中除了具有传统有线网络在应用层与传输层的安全威胁外，还面临着更多的网络层、MAC 层与物理层的安全挑战[20~25]。与传统有线网络相比，无线 Ad Hoc 网络具有许多不同之处，如表 1－1 所示。

表 1-1 有线网络与无线 Ad Hoc 网络比较

有线网络	无线 Ad Hoc 网络
存在基础网络硬件设施	无基础网络硬件设施，可以随时随地、快速搭建，适合军事应用、灾难救助、偏远地区通信等应用
集中控制	所有节点地位平等，节点之间以对等方式进行通信，无需集中的管理控制中心，任何节点可以自由地加入和离开网络
拓扑相对稳定	节点可以随意移动，导致节点之间的链路增加或消失，加上无线发送功率的变化、环境的影响以及信号之间的相互干扰、节点的加入离开、节点故障等因素，造成网络拓扑结构动态变化
高带宽	Ad Hoc 网络中节点通信通过无线传输完成。由于无线信道本身的物理特性，它提供的网络带宽相对有线信道要低得多。此外由于无线共享信道的竞争而产生的碰撞、衰减、干扰等多种因素，使无线信道的实际带宽远远小于理论中的最大带宽值
外接电源	移动节点的能源主要由电池提供。节点能量损耗越多，网络功能越差。因此 Ad Hoc 网络具有能量有限的特性
存在单点故障	在 Ad Hoc 网络缺乏中心控制，节点通过分布式协议互联，某个或某些节点发生故障通常不会影响整个网络的正常工作
生存时间长	Ad Hoc 网络主要用于临时通信，其生存时间一般比较短

无线 Ad Hoc 网络需要节点的协同工作来弥补网络中没有基础设施的不足。然而由于网络缺乏集中的管理控制，近年来无线网络节点为了自身利益而不遵循协议约定的现象日趋严重。有些节点为了达到恶意攻击或是抢占信道、节约自身能量等目的，违背协议规则，对其他节点产生的分组或不参与路由、或不转发数据；在发送自身产生的分组时，通过 MAC 层协议作弊达到非法抢占信道目的；在物理层以较大功率持续发送干扰信号，造成网络的不可信，破坏网络的正常运行，或不考虑自身行为对其他节点带来的影响，肆意调整传输能量，以获得更好的信噪比。这都是由于节点的不合作行为所致，我们把这些不合作节点统称为不良行为节点，其中 MAC 层不良行为尤为典型。传统的授权与认证解决了用户的身份信任问题，但没有解决用户的行为信任问题。可信网络必须在传统用户身份信任研究的基础上研究用户的行为信任。网络节点间的协议交互以及用户之间的合

作与竞争，使网络行为呈现出相当的复杂性、非线性，而且攻击和破坏行为也呈现出多样、随机、隐蔽和传播等特点，从而较难预测、分析和研究。

此外，Ad Hoc 网络中，由于无线信道的开放共享和有限的节点资源等特性，使无线通信容易受到窃听、堵塞和恶意的干扰破坏等系列攻击；无线自组织网络缺乏集中的管理控制以及高度动态的本质给那些具有各种安全要求的协议设计带来很大的挑战。虽然固定网络中的安全路由问题有很多研究成果，但是往往依赖于基础设施的支持，因此不适用于移动自组网这种无基础设施、资源有限的网络。Ad Hoc 网络中安全可信的路由协议的设计关键是保证信息的私密性、完整性与不可抵赖性，节点身份的匿名性与可验证性，网络拓扑的隐蔽性等。许多网络攻击者在发起主动攻击前，往往通过实施被动攻击以获取有用信息，以此提高主动攻击的成功率。网络中的协议数据单元 PDU 包含着丰富的网络信息，如节点的身份、网络拓扑信息、节点的地址等，这为被动攻击的实施提供了可能性，而开放的无线信道和缺少集中的管理控制中心进一步增加了被动攻击的检测难度。因此，Ad Hoc 网络中如何抵抗被动攻击是一个重要的研究课题。一般认为安全可信的匿名路由协议[26~27]是用于抵抗被动攻击的有效方案。

1.2.3 可信网络连接模型

终端节点的安全状态关系到整个网络的安全运行。为了减少遭受攻击的风险和之后的恢复重建花销，企业和公用网络的管理者们更加关注如何通过技术手段实现主动式网络安全管理。在这种情况下，准入控制技术顺势而生。

准入控制的核心是从网络接入端点的安全控制入手，结合认证服务器，安全策略服务器和网络设备，以及第三方软件系统(病毒和系统补丁服务器)，完成对接入终端用户的强制认证和安全策略应用，从而保障网络安全。

准入控制发展很快，各种方案呈整合趋势。各厂商在突出自己方案的同时，加大了相互之间的合作力度。与此同时，准入控制的标准化过程也加快了步伐，不管是基于 802.1x，还是 DHCP、网关的方案，都需要标准化工作支持互操作的要求。鉴于此，可信计算组织 TCG TNC 分组于 2004 年提出了可信网络连接 TNC 技术，定义并发行了一种开放的 TNC 体系架构和一系列标准，为端点准入

强制策略开发一个对所有开发商开放的架构规范，从而保证各个开发商端点准入产品的互操作性[28~32]。

TNC将TCG的视野延伸到了网络的安全性和完整性，设计了防止不安全设备接入和破坏网络的机制。TNC规范的主要思想是，当终端访问网络之前，首先对终端的身份进行识别，并对其完整性状态进行检测并与系统的安全策略进行比较。如果满足安全策略要求，则允许终端接入网络，否则拒绝或是对该终端进行隔离。当终端处于隔离状态时，可以对该终端进行修复，从而大大提高整个网络系统的安全性及可信性。

TNC架构规范从2006年5月发布的V1.1至2009年5月已发展到V1.4版本[33]，增加了IF-T：捆绑TLS[34]、联合TNC[35]和无TNC客户端场景[36]支持规范。我们以V1.4为例介绍TNC体系架构，如图1-1所示，图中虚线表示标准接口(协议和APIs)。

TNC架构包括网络访问、完整性测量和完整性实施三个层次，每个层次都包括若干个接口组件。TNC在传统的网络访问基础上，通过各接口组件实现对接入终端的完整性测量，并进一步基于访问策略和端点的完整性实现对接入平台的认证、接入控制和隔离修复等。TNC架构包括五个实体，这五个实体分别是访问请求者AR(Access Requestor)、策略执行点PEP(Policy Enforcement Point)、策略决定点PDP(Policy Decision Point)、元数据访问点MAP(Metadata Access Point)及元数据访问点客户端MAPC(Metadata Access Point Client)。AR主要通过发送网络访问请求申请建立网络连接，并收集其所在平台的完整性信息，将该信息提交给PDP进行认证；PDP作为是否允许AR访问网络的决策实体，其决策依据来源于AR附送的身份信息与其完整性状态信息，若AR的身份与完整性状态信息符合预配的本地安全策略，则PDP指令PEP授权AR的访问请求，否则指令PEP禁止AR的访问或对AR实施隔离；PEP作为策略执行实体，其主要功能是接收PDP的指令，并根据该指令控制AR对被保护网络的访问；MAP用来存储TNC组件状态信息帮助策略的判别与实施；MAPC中的传感器、流控等设备通过向MAP发布或提取信息完成各自功能。

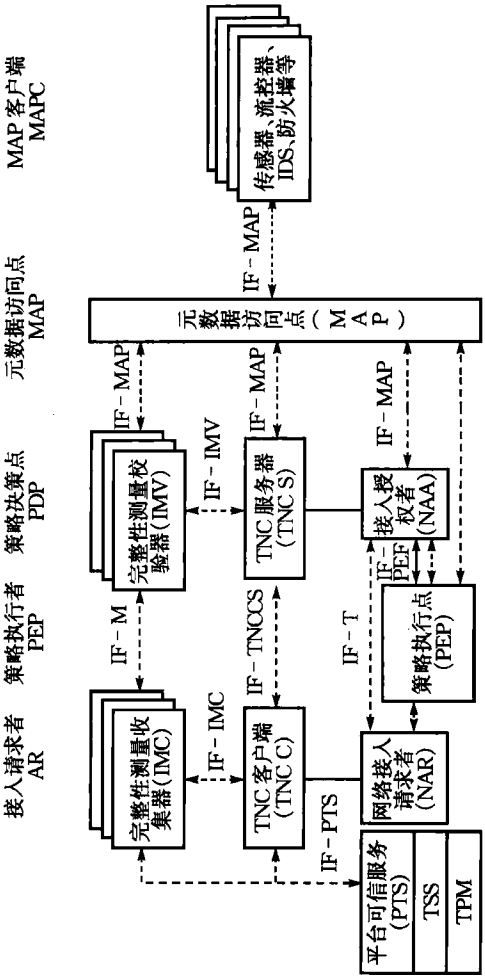
接入请求者
AR
策略执行者
PEP
策略决策点
PDP
元数据访问点
MAP
MAP 客户端
MAPC
完整性测量收集器(IMC)
完整性测量校验器(IMV)
TNC 客户端(TNC C)
TNC 服务器(TNC S)
网络接入请求者(NAR)
策略执行点(PEP)
接入授权者(NAA)
元数据访问点(MAP)
传感器、流控器、IDS、防火墙等
平台可信服务(PTS)
TSS
TPM
IF-M
IF-IMC
IF-TNCCS
IF-T
IF-PTS
IF-IMV
IF-MAP
IF-PEP
恳请者 VPN 客户端等
边缘交换机
网络防火墙
VPN 网关
AAA 服务器
完整性测量层
完整性实施层
网络访问层

图 1-1　TNC 体系架构

目前，国内的可信网络连接相关研究也取得了一定进展。2005 年 1 月国家信息安全技术标准化委员会成立了我国的可信计算工作小组。2007 年北京工业大学开始组织包括芯片、主板、软件和网络的可信计算关键标准的研究并着手建立可信网络连接架构模型[37]，如图 1-2 所示。该模型分完整性测量、可信平台评估、网络访问控制三个层次，包括访问请求者、访问控制器和策略管理器三个实体。访问请求者和访问控制器作为对等实体，策略服务器作为可信第三方对前二者实施集中管理，通过采用国家自主知识产权的鉴别协议，实现访问请求者和访问控制器的双向身份认证、平台可信评估与访问控制。

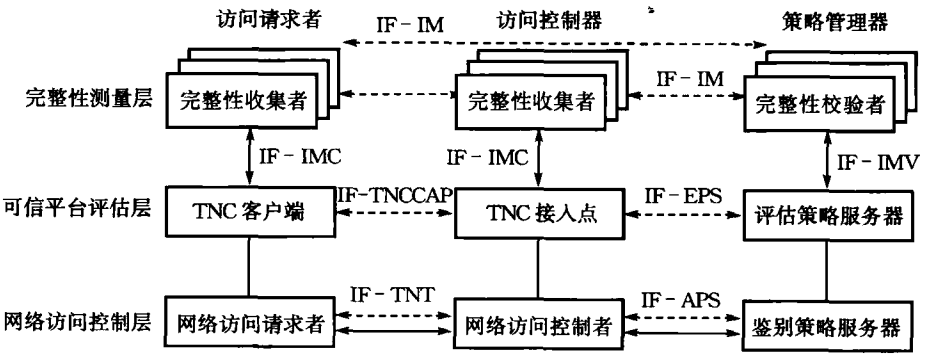

图 1-2 中国可信网络连接架构模型

1.3 本书工作

1. 选题动机

通过上述分析可知：企业网、政务网、校园网等传统有线网络以及目前正在兴起的各种无线网络存在众多安全隐患，导致了互联网中普遍存在的脆弱性问题。互联网“尽力而为”的存储转发设计思想使路由节点对传输的数据包来源不执行任何验证和审计功能，导致了大量的地址假冒，病毒与垃圾信息肆意泛滥，各种入侵与攻击行为随处可见且难以跟踪；主机软硬件系统的脆弱性、网络运行与维护中各种安全漏洞以及安全机制与管理政策之间的不一致性进一步加重了互联网的脆弱性，导致了网络的不可信，路由系统无法验证数据源的可信性，用户敏感信息或个人隐私面临泄露风险，互联网因暴露在各种攻击的威胁之下，其服务质量

与可用性在某些关键应用中难以保证。

随着光和无线通信技术以及网格计算等应用的研究发展，新一代互联网正向着可信、可控与可扩展方向发展。本书在 1.2 节可信网络连接架构模型下，基于 MPLS 骨干网络，提出一种基于“源目 IP 地址对”数字短签名技术的网络可信访问机制，对接入源节点执行审核认证，对终端用户的网络行为进行完整性测量，从源头实施安全防御，提高互联网的可信性。

多种类型的传输技术使互联网呈现出复杂异构的特性，互联网骨干连接了有线和无线多种用户。无线网络的完全分布性、信道的开放共享性以及资源有限性等使无线网络附加了更多的安全隐患，网络层、MAC 层的安全攻击检测与无线网络中通信的匿名要求、个人隐私保护等不能单纯依赖于互联网设备的认证审核完成，无线 Ad Hoc 网络迫切需要建立一种可信机制用来实现对各种攻击的检测防御，为各类用户提供隐私保护和可信匿名通信。本书提出一种基于人工免疫的 MAC 层攻击检测机制和基于改进的数字短签名技术的安全的匿名源路由协议 S^2ASR。

2. 主要贡献

本书的创新点包括以下几个方面。

(1)通过分析 TNC 模型，面向 MPLS 骨干网络提出了基于“源目 IP 地址对”的短签名算法。基于该算法设计了可信接入控制方案，并在网络处理器上通过微码实现了相关算法，实现了互联网骨干的可信接入。实验结果表明，本方案在有效提高网络可信性前提下，稳定工作且具有良好的兼容性。

(2)针对无线 Ad Hoc 网络 MAC 层攻击行为，建立了攻击检测人工免疫模型，设计了基于人工免疫的综合攻击检测技术方案 AIIDM。对恶意攻击，以 Δt 时间内饱和状态下的传帧计数为特征序列，基于 SW－DCUSUM 算法执行检测，仿真表明，该算法对恶意攻击的误检率和漏检率分别为 0.4%和 0.2%；根据检测节点的状态不同，自私型攻击检测分别采用两种不同方式：饱和状态的节点基于滑动窗口的残差阈值判别法 SW－RET 对邻居节点的攻击行为执行快速检测，非饱和状态节点基于相对位置的子串相关基因匹配法执行检测，并在可接受的假阳性概率下给出了节点判别公式。仿真表明，饱和状态下节点的检测准确率大于