

可信网络中安全、可控可管及可生存技术研究

Security, Controllability, Manageability and Survivability in Trustworthy Networks

中图分类号: TP393 文献标识码: A 文章编号: 1009-6868 (2008) 01-0036-06

摘要: 互联网在日益成为人们日常生活中不可或缺的组成部分的同时,也日益暴露出其设计思路与当前人们对网络的需求不符合的弊端。虽然“未来网络应该是可信的”这一观点已成为业界共识,但可信网络这一概念应包含哪些内涵,应该从哪些方面努力才能保证网络是可信的,却仍然没有定论。文章认为网络的可信性,应该至少包括安全性、可控可管性和可生存性3个方面的内涵。文章对这3个方面的关键技术进行了分析和点评,在此基础上对可信网络的未来发展和面临的挑战作了评述。

关键词: 可信网络;网络安全;可控可管性;可生存性

Abstract: The Internet plays increasingly important roles in everyone's life, but the existence of a mismatch between the basic architectural idea beneath the Internet and the emerging requirements for it is also becoming more and more obvious. Although the Internet community came up with a consensus that the future network should be trustworthy, the concept of "trustworthy networks" and the ways leading us to a trustworthy network are not yet clear. This research insists that the security, controllability, manageability, and survivability should be basic properties of a trustworthy network. The key ideas and techniques involved in these properties are studied, and recent developments and progresses are surveyed. At the same time, the technical trends and challenges are briefly discussed.

Key words: trustworthy network; network security; controllability and manageability; survivability

王晟/WANG Sheng

虞红芳/YU Hong-fang

许都/XU Du

(电子科技大学 通信与信息工程学院, 四川 成都 610054)

(School of Communication and Information Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China)

性”,以及“应该从哪些方面努力才能使得网络可信”这些问题,尚没有明确的定义。不过,没有清晰的概念界定,并不妨碍人们对这个问题相关的范畴和相关技术的研究。事实上,目前已有与可信网络相关的研究成果和研究思路。

因此,本文试图总结和讨论的重点是这些成果和思路,而不打算给出明确的关于“可信网络”的定义。只是在进行这样的总结和讨论时,我们沿用部分学者的看法^[1],从网络安全、可控可管性,以及可生存性3个方面进行评述。达到更高的安全性往往需要网络的控制和管理能力提出更高的要求,而网络生存性所需要应对的威胁也从单纯的随机故障扩展到了包括人为攻击在内的各种异常。

1 网络安全

根据《CNCERT/CC2007年上半年网络安全工作报告》^[2],目前中国的互联网络安全实际状况不容乐观。各种网络安全事件与2006年同期相比都有明显增加。半年时间内,CNCERT/CC接收的网络仿冒事件和网页恶意代码事件,已分别超出2006

互联网无疑是人类可能建造的最伟大的奇迹之一。其巨大成功的根源来自于它简单、开放的设计理念。用户和终端数目的急剧增长、网络技术的飞速进步、商业模式的被吸引等等,都是这种巨大成功的具体表现。然而,正是随着这些因素的引入,互联网面临着越来越多的新的要求和挑战。其最初的成功之后逐渐暴露出来的问题也越来越引人注目。例如

安全性差,难以控制和管理,面对故障和攻击难以及时做出反应等等。

由于互联网的种种局限,人们普遍认识到,未来的网络应该具有新的特性,使得用户在使用它的时候更加方便的同时,也更加安全;也应该使得网络的运营者在面临各种异常状态时能及时地发现,并有效地做出反应。人们借鉴可信计算的名称,将这样的网络称为可信网络。

然而,虽然“未来的网络应该是可信的”已成为业界共识,对于“如何定义可信性”,“如何评估可信

基金项目: 国家重点基础研究发展规划项目 (“973”计划) (2007CB307104、2007CB307100)

年全年总数的14.6%和12.5%。中国大陆地区被植入木马的主机IP远远超过2006年全年,增幅达21倍。中国大陆被篡改网站数量比2006年同期增加了4倍。中国的公共互联网网络面临着更加严重的安全威胁。而以获益为目的的网络攻击事件将为广大用户带来更加直接的经济损失。

1.1 保证网络安全的主要技术手段

目前保证网络安全的机制主要有网络内容安全、网络认证授权、防火墙、虚拟专用网、网络入侵检测、网络脆弱性检测、安全接入、安全隔离与交换、安全网关、安全监控与管理、网络安全审计、恶意代码检测与防范、垃圾邮件处置、应急响应等^[3]。

公开密钥基础设施(PKI)技术是一种能够解决网络环境中信任与授权问题的重要技术,包括身份的真实性、数据的机密性、文件的完整性、行为的不可否认性等。但是该技术中存在一个最大的安全隐患,就是安全控制点,一旦攻击者攻破了安全控制点,那么所有采用的认证技术将形同虚设。

入侵检测系统(IDS)的目的是检测出系统中的入侵行为以及未被授权许可的行为。入侵检测系统通过定时检查审计信息、监督网络流量来查找系统中当前发生的可疑事件。目前,入侵检测系统和防火墙相结合形成的入侵防御系统(IPS),可以大大地扩展防御纵深,更好地保障网络的安全。但IDS面临的最大的问题是其误报率不能满足实际应用的要求^[4]。近年来,UC Davis、UC Berkeley、Carnegie Mellon和MIT等大学和实验室在入侵检测领域做了大量的工作,取得了许多重要成果。但是,面对日益复杂的网络环境和层出不穷的安全威胁,入侵检测技术尚处在发展阶段,许多重要的课题有待解决。

1.2 网络安全防护技术的发展趋势

各种孤立的网络安全应对措施

在面对大范围的网络安全事件时,都是无能为力的。针对互联网全网范围的攻击,需要互联网用户的广泛参与防御,才能达到最理想的效果。文献[5]中就提出了这样一种设想。UC Berkeley、Intel的相关研究机构正在进行该课题的研究。要达到“互联网用户的广泛参与”的目标,需要克服很多技术与非技术难题,如用户间信任关系的确立,用户隐私的保证,互联网范围的分布式数据处理技术等。

正如文献[1]指出的那样,脆弱性的来源是多方面的,存在于系统设计、实现、运行和管理的各个环节。分散孤立的应对方式不可取。因此,网络安全未来的一个重要的研究方向就是以网络的安全性作为重要的考虑,并以此指导未来网络体系结构的研究与设计^[6]。Carnegie Mellon、Stanford、UC Berkeley、MIT、Princeton等大学以及Microsoft、Cisco、Intel等企业的研究机构都有人员参与这个充满挑战的方向的研究。

2 可控可管性

我们认为,网络的可控可管性主要是指网络具有对用户行为、网络运行状态和网络资源的有效控制和管理的能力。这种能力不仅对于建设安全的网络是必不可少的,而且对于未来网络的健康发展和持续的技术革新,都是必不可少的。

2.1 用户行为的可控可管性

为了实现真正的可信和安全,网络必须具有对用户行为高度的控制和管理能力。

现有的网络安全研究主要关注的是“防御”(Defense)。正如许多学者普遍意识到的那样^[7],实际上要达到真正的安全,防御与“威慑”(Deterrence)应该同等重要。为了达到真正的威慑目的,最好的办法似乎是让网络中的业务流自己具有自我认证的能力,即给每个流,甚至每个分组都附上一个标签,该标签能够唯一地指

定发出该分组的计算机,并且这个标签是不可篡改的(或者篡改是可以被发现的),相应地也就是不可抵赖的。另一方面,在网络中对这种标签进行来源确认时,又不能过多地侵犯用户的隐私。一种称为“群签名”(Group Signature)的公钥签名机制^[8]可以达到这个目的。以这种工具为基础,就可以设想出新的对用户进行有效管理和控制的方法。Snoeren等人提出^[7],可以在网络边缘设置关联认证服务(利用群签名技术),对每个进入网络的分组的归属都进行认证,一旦发现无法认证的分组(不能归属于任何已知的群),就不准该分组进入网络。反之,如果发现了对网络有害的分组,也可以通过其群签名,确定分组的发送者。如果能克服计算量大的缺陷,这种思路无疑会对改善现有Internet难管、难控的现状具有重大的意义。

与上述系统类似,文献[9]提出的企业网安全结构(SANE)结构也希望在网络边缘,特别是企业网内设置一个集中式的控制中心,称为域控制器(Domain Controller)。所有与管辖范围内主机有关的通信都必须得到域控制器的允许。这种集中式的方式对于用户行为的控制和管理能力当然是令人满意的,而且可以方便地在企业网内部署相应的安全策略。但是如何将这一思想拓展到公用网领域,既保证监控的力度,又保证可伸缩性,是一个挑战。

除了网络安全之外,对未来网络中支持移动设备的需求也要求网络能够对用户/端设备的位置信息进行有效的监管。这可以看作是对另一种用户行为的可控可管要求。人们很早就认识到如果能够将地理位置信息结合进无线网络的路由设计中,将是非常有效的^[10]。近来有研究者提出在未来的网络体系结构中,应该在协议层次中充分考虑地理位置信息的作用^[11]。这样做的好处是明显的,但是在互联网范围内如何能提供对数量惊人(而且还在继续快速增长)的移动

设备提供高效的定位服务,无疑是一个挑战。文献[11]中提出的多分辨率定位服务方案,借鉴了固定电话号码的设置思想,充分利用了分级网络的特点,具有一定的可行性。

2.2 网络状态的可控可管性

除了对网络的配置之外,网络管理最主要的功能应该是对网络运行期间的各种状态的及时感知;而这种感知的目的是对包括故障、攻击和服务质量下降等各种异常现象的及时感知、定位、推理和诊断,最终做出适当的反应。但是,现有的互联网中,由于控制和管理功能依赖于数据平面,完全的、缺乏协调的分布式控制,以及大多数控制和管理功能都是后期定制(而不是在网络设计之初就统一考虑)等原因,呈现出难以有效收集网络状态、难以有效发现和定位网络异常,从而难以及时做出反应的特点。因此,越来越多的研究者从不同的侧面提出了对未来网络的管理控制系统的研究构想。例如,文献[12]强调了集中式控制的好处;知识平面^[13]的概念强调了推理和诊断能力的必要性;文献[14]和文献[15]试图回答哪些功能模块是必不可少的问题;CONMan^[16]在文献[12]的基础上进一步强调了控制管理功能与数据转发功能的分离;Maestro^[17]借鉴主动网和可编程网络^[18]的成果,试图给出针对网管功能的、统一的操作平台。

文献[12]提议将现今路由器中的主要功能重新划分为4个平面:数据(Data)、分发(Dissemination)、发现(Discovery)和决策(Decision),即4D。网络中的状态信息由发现平面来收集;然后由分发平面负责将这些信息发布到决策平面;决策平面根据这些信息计算合适的路由和网络配置,并把这些决策结果发到数据平面。其基本目标是,通过集中式管理和重新组织关键功能,有望达到简化网络管理的复杂度并使状态发现自动化的目的。

CONMan同样采用集中控制的思

路。其设计目标是简化对数据平面的配置操作。CONMan中,数据平面的协议被抽象化为一些功能组件,例如管道、交换、过滤等。这些抽象的组件都向网管平面开放其接口。这样,网管平面可以方便地将一个高层次的需求转化为对这些功能模块的一系列级联配置。CONMan的设计灵感部分来自于4D的决策平面的概念。通过借鉴7号信令系统中物理分离的管理通道的思路,拓展了4D中的管理通道的概念,使得CONMan中数据和管理通道虽然共用物理链路,但在逻辑上是分离的。CONMan的设计者们认为,这种分离是保证网络管理和控制真正有效监控网络行为的必要手段。

Maestro的设计思路是对网络管理和控制功能的模块化和通用化。该方案设计了一种通用的操作平台,各种类型的网络控制/管理功能模块都以该平台上的独立的应用程序的方式来实现,模块之间的交换和隔离由平台来完成。Maestro的目标是将网络中现有的各种功能(例如分组转发和路由维护)抽象为功能单一的模块,这些模块更容易维护,不易出错,并且也便于针对不同的应用进行定制和组装。

从上述这些最新的研究思路来看,网络的控制和管理系统的未来发展呈现出3个主要的趋势。一是控制管理平面与数据平面的分离化,如CONMan所倡导的那样;二是控制管理功能的集中化;三是便于组装的功能模块化。

2.3 网络资源的可控可管性

如果缺乏对资源的有效管理,无法以整体的、协调的方式来利用网络资源,就会导致技术和体系结构的发展出现障碍。近年来,各种网络虚拟化(Virtualization)的提案就是为了克服当前互联网难以支持新技术的缺陷而提出的。

网络的虚拟化的目标是:通过全新的网络构建方式,使得未来的In-

ternet具有容纳各种新技术、新服务,尤其是新的组网联网技术的能力,使得这些不同的端到端网络都能在一个公共的平台上共存。比较典型的方案包括文献[19]和文献[20]。其中文献[19]所提出的模型是在二、三层之间插入一个新的层次,称为底盘层(substrate)。该层提供对底层各种资源的管理和抽象,并向上层的各种不同类型的三层网络提供服务。文献[20]中提出的CABO模型的思路是类似的,同样希望通过构建一个虚拟的基础设施,向各种ISP提供组网必需的资源管理和隔离功能,从而允许各个不同的ISP组建各自的网络,这些网络的协议、服务、转发、信令、路由都可以不相同。

网络虚拟化的思考方向可以这样归纳:与其为所有的服务和应用(包括现在还未知的,将来出现的)设计一种通用的组网/转发方式(像ATM那样),不如干脆承认这样是不可能的,转而设计更为基本的管理各种组网方式都不可或缺的资源平台,使得任何协议、转发技术都可在这个平台上共存。

从网络的可控可管角度看,网络的虚拟化的概念在解决了一部分困难的同时,也引入了新的困难。如果substrate层对资源的抽象和管理做得足够好,那么的确可以达到隔离上层网络的目的,便于各个网络独自发展。但另一方面,这种可管方面的好处必须依赖于substrate层完备的资源管理能力,而这恰恰是最大的挑战。

正是从这个意义上说,虚拟化不一定是达到有效管理和控制网络资源,以应对未来的技术发展的唯一途径。事实上,FIND计划资助的另一个项目,eFIT^[21],以及中国“973”计划资助的课题^[22]都采用了不同的途径。这两个项目的基本思想中都包含了这样一种思路,即将服务的提供与保证递交的连通性两个任务分离开来,将网络边缘对用户的管理和控制与网络核心对资源的管理和使用分离

开来,通过定义合适的映射服务来实现二者的无缝连接。正如文献[21]中所说的那样,这种分离和控制同样可以有效地保证未来的新技术进展,只是与虚拟化的思路不同罢了;同时,这种思路对于加强网络的可控可管性也是具有积极意义的。

3 可生存性

可生存性(Survivability)是指网络在遭受攻击、失效或者意外后能够及时地完成的能力^[23]。网络可生存性的实现是靠具体的保护和恢复措施来保证的。保护和恢复均是在网络故障条件下,使受损的业务得以重新运行的具体措施。

目前,网络的安全性日益被纳入到可生存性的范畴。2004年国际实时系统研讨会上召开了基础设施生存性工作组会议,讨论了今天的网络系统面临的生存性挑战,需要综合考虑网络负荷、攻击和故障情况。文献[24]提出了包含了安全的可生存性(SoS)的概念,认为传统安全技术是保护系统部件的技术,而可生存性技术包含了整个系统的功能。可生存性的目标比安全性更高。

这里为了描述方便,我们将传统的针对随机故障的网络生存性称为“狭义可生存性”;而将扩展到包含了人为攻击的、内涵更广的可生存性概念称为“广义可生存性”。

3.1 狭义可生存性

网络可生存性研究最早集中在传送网;随着网络业务的发展,对IP网络的可生存性问题也日益关注。

传送网(如SDH网络、WDM网络)由于其链路的传输容量较大,其网络部件因故障失效时可能遭受比其他网络更大的损失。因此,20世纪70年代就开始研究SDH传送网的可生存性问题。目前已有大量文献对传送网可生存性问题进行了深入研究^[25]。根据具体应用情况的不同,这些研究可以分为以下几个方面:

(1)从网络拓扑结构的角度看,可以分为对环状、网状网的研究。

(2)从业务模型的角度看,有静态的和动态的生存性算法。

(3)从使用机制的角度看,又分为自愈环、1+1、共享保护、通路保护/恢复、链路保护/恢复、子通路保护/恢复和圈覆盖等。

(4)按照恢复故障场景的不同,又可以分为对单链路失效、多链路失效、节点失效、区域失效的研究。总的来说,这些研究的目的是如何提高网络的资源利用率(或者提高网络的吞吐率)以及在资源利用率和恢复时间之间找到较好的折衷。

同时,随着网络业务的进一步发展,对IP网络在可靠性、可用性方面提出了更高的要求,传统的“尽力而为”服务已远远不能满足业务需要。传统的IP网在故障发生后通过动态路由收敛来恢复,恢复时间较慢,一般在几秒至几分钟;这对高速骨干网络是不可接受的。因此,在本世纪提出了多种快速自愈机制以提高IP网络的可用性和可靠性^[26],大概可分为3类。一类是全网反应式的路由重构自愈机制;第二类是本地预配置的快速重路由机制;第三类是基于多协议标记交换(MPLS)的保护倒换方案。反应式的路由重构自愈机制是利用IP路由协议天然的自愈能力,发生失效后,在新的网络状态下重新计算路由来达到自愈的目的。另一类方法是预先计算多个路由,本地发现失效后,通过本地倒换到备份路由的方式实现路由的本地修复。本地修复的研究工作集中在快速重路由(FRR)^[27]和多拓扑路由(MTR)^[28]。而保护切换是预先建立备份通路,为每条工作预留空闲资源,因此恢复速度快。保护切换是MPLS网络中达到快速自愈的合适方法。保护切换根据所保护的粒度不同分为端到端方式和本地方式。

3.2 广义可生存性

广义可生存性的研究主要有两

大问题:一是定量评估问题,涉及建立包括网络的脆弱性分析、用户攻击行为描述在内的合理故障模型理论和定量评估的方法。二是保证广义可生存性的机制和策略问题,从单纯容错到容错、容侵同时考虑;从同构网络环境下的单种技术到异构网络下的层次化、协同可生存性技术。

(1)可生存性定量评估研究

建造一个完美的可生存性网络是不可能的,定量评估网络的可生存性就显得非常有价值。定量研究可生存性可以发现网络的脆弱点、确定存在的风险、有针对性地改善。

可生存性的量化才刚刚起步,尚处于探索阶段,已经出现的研究工作大多借鉴了可依赖性研究的成功经验。与此相比,可依赖性研究经历了多年的发展,已经形成了多种模型方法分别适用于不同的应用场景,如Petri net^[29]状态空间的模型方法等。因此,可依赖性研究为可生存性量化研究奠定了基础。但是,可依赖性分析中通常假设故障是由硬件或软件的随机事件引起。而在广义可生存性分析中,除了考虑由随机事件引起的故障外,还有人为故意引起的故障。尽管人为故障从外部观察者来看这些事件似乎是随机的、没有关联,但实际上它们之间是精心设计、彼此相关的。使得它们很难用经典随机模型来正确描述。

目前,在随机故障场景下网络的可生存性量化分析方面和入侵容忍、入侵检测、安全模型等理论和技术等安全方面进行了大量研究。但恶意攻击对网络可生存性的影响的研究还不够深入,主要的研究机构有Virginia大学、Arizona大学、Carnegie Mellon大学和CERT组织等,其研究各有侧重点:Virginia大学和Arizona大学的研究侧重于系统可生存性的量化^[30]和体系结构^[31];文献[32]基于问题空间转换的思路,把网络系统的可生存性评估转换为某种经典问题求解的方法框架等等。这些研究都处于摸索阶

段,还没有形成完整的理论体系和实用技术。

为量化评估网络的可生存性,建立包括网络的脆弱性分析、用户攻击行为描述在内的故障模型理论是非常重要的,也是量化评估的最大挑战。网络故障的特点对可生存性方案的设计是至关重要的,只有准确地建立故障失效特点和模型,才可以有针对性地设计解决方案。2004年,UC-DAVIS大学研究了IP骨干网络的故障特点^[33]。但这些研究尚不足以导出合适的评估模型。

(2)广义可生存性技术和策略研究

当前关于可生存性机制和算法的研究大都集中于给定网络的故障情况(比如单故障、双故障等)或假设网络的故障是随机发生的情况。对恶意攻击下的网络保护恢复技术研究得很少。错误是随机发生的,而攻击却是有预谋地利用了系统的弱点和漏洞,导致网络中的故障数和故障场景不确定。显然,二者之间存在的区别使得不能直接用现有针对随机故障的保护恢复技术解决恶意攻击的问题。以前提出的生存性机制或者生存性路由算法就不再适用。因此,针对可信网络的容错、容侵问题的解决方案仍有待研究。

广义可生存性的目标在于网络的整体可生存性能,更强调层次化的多域多层联合设计。文献[34]研究了多层网络的可生存性问题。通过层间信息交互,灵活决定在何时、何层实施合适的恢复动作,从而建立起有效的层间调整策略,实现不同层故障恢复机制之间的协调,以避免不同层恢复机制间的竞争,提高网络的整体可生存性。文献[35]研究了多域环境中的网络可生存性问题,指出了现有多域网络中存在的问题和挑战。

4 结束语

本文从网络的安全性、可控可管性和可生存性3个方面讨论了现有的关于可信网络关键技术的研究现状,

并分析和评述了技术发展的趋势和方向。从中不难看出,可信网络的研究尚处于起步阶段,仍有众多的问题有待解决。例如,如何整合现有的孤立和分散的安全策略和技术手段;如何从体系结构的角度设计和实现具有内在安全防护和威慑能力的网络;如何在保证对用户行为的高度控制和管理能力的同时,兼顾用户的隐私;如何在集中式控制与可扩展性之间找到合适的平衡;如何定量评估网络的容错、容侵和容忍故障的能力等等。随着技术的进步和业界的共同努力,我们相信,这些困难的问题终将解决,这些困难的折中和平衡终将被找到,而“使网络可信”这一目标也终将被达到。

5 参考文献

- [1] 林闯,彭雪海.可信网络研究[J].计算机学报,2005,28(5):751-758.
- [2] CNCERT/CC 2007年上半年网络安全工作报告[EB/OL]. <http://www.cert.org.cn/>.
- [3] 沈昌祥,张焕国,冯登国,等.信息安全综述[J].中国科学:E辑(信息科学),2007,37(2):129-150.
- [4] PAXSON V. Considerations and pitfalls for conducting intrusion detection research [C]//Proceedings of the Fourth GI International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA2007), Jul 12-13, 2007, Lucerne, Switzerland. 2007.
- [5] Belovin S M, Clark D D, Perrig A, et al. Report of NSF workshop on a clean-slate design for the next-generation secure Internet [R]. GENI Design Document 05-05, 2005.
- [6] HELLERSTEIN J, CONDIE T, GAROFALAKIS M, et al. Public health for the Internet: Towards a new grand challenge for information management [C]//Proceedings of the 3rd Biennial Conference on Innovative Data Systems Research (CIDR'07), Jan 7-10, 2007, Asilomar, CA, USA. 2007:332-340.
- [7] SNOEREN A, KOHNO T, SAVAGE S, et al. Privacy-preserving attribution and provenance [EB/OL]. NSF FIND' 2006 project. <http://www.nets-find.net/Funded/Privacy.php>.
- [8] CHAUM D, HEYST E. Group Signatures [C]//Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Apr 8-11, 1991, Brighton, UK, Berlin, Germany: Springer-Verlag, 1991:257-265.
- [9] CASADO M, GARFINKEL T, AKELLA A, et al. SANE: A protection architecture for enterprise networks [C]//Proceedings of 15th USENIX Security Symposium, Jul 31-Aug 4, 2006, Vancouver, Canada. 2006:137-151.
- [10] BASAGNI S, CHLAMTAC I, SYROTIUK V, et al. A distance routing effect algorithm for mobility (DREAM) [C]//Proceedings of the 4th annual ACM/IEEE International Conference on Mobile Computing and Networking, Oct 25-30, 1998, Dallas, TX, USA. New York, NY, USA:ACM. 1998:76-84.
- [11] GRUTESER M. A geometric stack for location-aware networking [EB/OL]. NSF FIND' 2006 project. <http://www.nets-find.net/Funded/GeometricStack.php>.
- [12] GREENBERG A, HJALMTYSSON G, MALTZ D, et al. A clean slate 4D approach to network control and management [J]. ACM Computer Communication Review, 2005,35(5):41-54.
- [13] CLARK D, PARTRIDGE C, RAMMING J, et al. A knowledge plane for the Internet [C]//Proceedings of Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (SIGCOMM 2003), Aug 25-29,2003, Karlsruhe, Germany. New York, NY,USA:ACM, 2003:3-10.
- [14] SHENKER S, ALLMAN M, PAXSON V. Architectural support for network trouble-shooting [EB/OL]. NSF FIND' 2006. <http://www.nets-find.net/Funded/ArchSupportNet.php>.
- [15] BARFORD P, BANERJEE S, ESTAN C. Design for manageability in the next generation Internet [EB/OL]. NSF FIND' 2006. <http://www.nets-find.net/Funded/Manageability.php>.
- [16] FRANCIS P, LEPREAU J. Towards complexity-oblivious network management [EB/OL]. NSF FIND' 2006. <http://www.nets-find.net/Funded/TowardsComplexity.php>.
- [17] EUGENE NG T S, YAN H. Towards a framework for network control composition [C]//Proceedings of ACM SIGCOMM Workshop on Internet Network Management (INM' 06), Sep 11,2006, Pisa, Italy.2006.
- [18] CAMPBELL A, MEER H, KOUNAVIS M, et al. A survey of programmable networks [J]. ACM Computer Communications Review, 1999,29(2):7-23.
- [19] TURNER J, CROWLEY P, GORINSKY S, et al. An architecture for a diversified Internet [EB/OL]. NSF FIND' 2006 project. <http://www.nets-find.net/Funded/DiversifiedInternet.php>.
- [20] FEAMSTER N, GAO L, REXFORD J. CABO: Concurrent architectures are better than one [EB/OL]. NSF FIND' 2006 project. <http://www.nets-find.net/Funded/Cabo.php>.
- [21] MASSEY D, WANG L, ZHANG B, et al. Enabling future Internet innovations through transit wire (eFIT) [EB/OL]. NSF FIND' 2006 project. <http://www.nets-find.net/Funded/eFIT.php>.
- [22] 张宏科,苏伟.新网络体系基础研究——一体化网络与普适服务[J].电子学报,2007,35(4):593-598.
- [23] ELLISON R, FISCHER D, LINGER R, et al. Survivable network systems: An emerging discipline[R]. CMU/SEI-2001-TN-001. Pittsburgh, PA, USA: Software Engineering Institute, Carnegie Mellon University, 2001.
- [24] YURCIK W, DOSS D, KRUSE H. Survivability-over-security: Providing whole system assurance [C]//Proceedings of IEEE/SEI/CERT 3rd Information Survivability

- Workshop (ISW '00), Oct 24–26, 2000, Boston, MA, USA. Los Alamitos, CA, USA: IEEE Computer Society, 2000:201–204.
- [25] GROVER W. Mesh-based survivable transport networks: Options and strategies for optical, MPLS, SONET and ATM networking [M]. New York, NY, USA: Prentice-Hall, 2003.
- [26] RAI S, MUKHERJEE B, DESHPANDE O. IP resilience within an autonomous system: Current approaches, challenges, and future directions [J]. IEEE Communications Magazine, 2005, 43(10): 142–149.
- [27] SHAND M. IP fast-reroute framework [EB/OL].
draft-ietf-rtgwg-ipfrr-framework-06.
- [28] Kvalbein A., Hansen, A f, Cicic T, et al. Fast IP network recovery using multiple Routing Configurations [C]// Proceedings 25th IEEE International Conference on Computer Communications (INFOCOM 2006), Apr 23–29, 2006, Barcelona, Spain. Piscataway, NJ, USA: IEEE, 2006:1–11.
- [29] NICOL D, SANDERS W, TRIVEDI K. Model-based evaluation: From dependability to security [J]. IEEE Transactions on Dependable and Secure Computing, 2004, 1(1): 48–65.
- [30] ORTALO R, DESWARTE Y, KANICHE M. Experimenting with quantitative evaluation tools for monitoring operational security [J]. IEEE Transactions on Software Engineering, 1999, 25(5): 633–650.
- [31] CHU C, CHU M. An integrated framework

- for the assessment of network operations, reliability, and security [J]. Bell Labs Technical Journal, 2004, 8(4): 133–152.
- [32] JHA S, SHEYNER O, WING J. Minimization and reliability analyses of attack graphs [R]. CMU-CS-02-109. Pittsburgh, PA, USA: School of Computer Science, Carnegie Mellon University, 2002.
- [33] MARKOPULU A, IANNACCONE G, BHATTACHARYA S, et al. Characterization of failures in an IP backbone [C]// Proceedings of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2004): Vol 4, Mar 7–11, 2004, Hong Kong, China. Piscataway, NJ, USA: IEEE: 2307–2317.
- [34] PUYE B, YAN Q, DE MAESSCHALCK S. et al. Multi-layer resilience in data-centric optical networks [C]// Proceedings of SPIE Conference on Optical Transmission Systems and Equipment for WDM Networking III, Oct 25–28, 2004, Philadelphia, PA, USA. Bellingham, WA, USA: SPIE, 2004: 255–267.
- [35] HUANG C, MESSIER D. A fast and scalable inter-domain MPLS protection mechanism [J]. Journal of Communications and Networks, 2004, 6(1): 60–67.

收稿日期: 2007-11-23

作者简介



王晟, 电子科技大学通信与信息工程学院教授、博士生导师。2005年入选教育部“新世纪优秀人才资助计划”。主要研究领域为宽带通信网络。已发表论文80余篇, 其中被SCI/EI检索40余篇; 申请国家发明专利10余项, 已获授权3项。



虞红芳, 电子科技大学通信与信息工程学院副教授、博士。主要研究方向为网络可生存性、宽带网络优化设计和路由协议设计等。已在国内外主要学术刊物上发表学术论文50余篇, 国际会议交流论文20余篇, 其中被SCI/EI检索30余篇; 申请国家发明专利6项。



许都, 电子科技大学通信与信息工程学院副教授、博士。主要研究方向为网络性能分析与优化、大容量交换与路由系统、网络安全体系结构等。已在国内外主要学术刊物上发表学术论文30余篇, 其中被SCI/EI检索20余篇; 申请国家发明专利10项。

←上接第16页

续监测、并优化配置网络设备运行参数的过程, 包含网络扫描和优化决策两个重要方面, 如图3所示。

对网络可管理性的研究就是通过改进网络体系中导致可管理性不足的设计原则, 实现网络的充分可管理性, 从而实现网络行为的可信, 并进一步为解决一系列现实的网络本质属性问题如安全性、鲁棒性、普适性、QoS保障等提供支撑, 以及为网络的进一步发展提供自适应的能力。

5 结束语

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, 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, 然而系统的脆弱性又不可避免, 网络正面临着严峻的安全挑战。可信网络是当前网络发展的重要研究方向, 本文对可信网络的概念、发

展、以及需要解决的关键问题进行了分析和论述, 为进一步研究的开展提供了方向。

6 参考文献

- [1] Trusted Computing Group [EB/OL]. <https://www.trustedcomputinggroup.org/home>, 2005.
- [2] Trusted Computing Group [R]. IWG Reference Architecture for Interoperability: Part 1 Specification Version 1.0, Revision 0.86. 2005.
- [3] Trusted Computing Group. IF-IMC Interface Specification, v.1.0 [R]. 2005.
- [4] Program Solicitation [EB/OL]. 2006-02-06. <http://www.nsf.gov/pubs/2005/nsf05518/nsf05518.htm>.
- [5] Cyber Trust [EB/OL]. <http://www.nap.edu/catalog/6161.html>, 2006.
- [6] 林闯, 任丰原. 可控可信可扩展的新一代互联网 [J]. 软件学报, 2004, 15(12): 1815–1821.
- [7] LIN Chuang, PENG Xuehai. Research on network architecture with trustworthiness and controllability [J]. Journal of Computer Science and Technology, 2006, 21(5): 732–739.
- [8] 林闯, 彭雪海. 可信网络研究 [J]. 计算机学报, 2005, 28(5): 751–758.
- [9] 林闯, 汪洋, 李泉林. 网络安全的随机模型方法与评价技术 [J]. 计算机学报, 2005, 28(12): 1943–1956.

收稿日期: 2007-11-09

作者简介



林闯, 清华大学计算机科学与技术系教授、博士生导师。现任 ACM 理事, IFIP TC6 (Communication Systems) 中国代表, IEEE 高级会员, 主要研究方向为计算机网络, 系统性能评价, 安全分析, 随机 Petri 网。2 发表学术论文 290 多篇, 并已出版 3 本专著。



王元卓, 清华大学助理研究员。北京科技大学博士毕业。现任中国计算机学会高级会员。主要研究方向为可信网络、网格计算、网络服务质量、安全性评价等, 已发表学术论文 20 多篇。



田立勤, 华北科技学院计算机系副教授, 硕士生、硕士生导师。现任计算机学会 Petri 网专业委员会委员。主要研究方向是计算机网络、工作流模型和可信网络等, 已发表学术论文 32 篇。