创新技术学术专著

INNOVATIVE

IP 网络可生存性技术

The Enabling Technologies for Survivability of IP-based Networks

王滨 杨强 吴春明 著

人民邮电出版社
POSTS & TELECOM PRESS

创新技术学术专著

INNOVATIVE

IP网络可生存性技术

The Enabling Technologies for Survivability of IP-based Networks

王滨 杨强 吴春明 著

人民邮电出版社
北京

图书在版编目（CIP）数据

IP网络可生存性技术 / 王滨，杨强，吴春明著. --
北京 : 人民邮电出版社，2013.6
ISBN 978-7-115-31178-8

Ⅰ. ①I… Ⅱ. ①王… ②杨… ③吴… Ⅲ. ①计算机网络—通信协议 Ⅳ. ①TN915.04

中国版本图书馆CIP数据核字(2013)第049174号

内 容 提 要

本书从快速自愈路由、安全路由、多路径传输、快速故障检测、虚拟网构建及自愈 5 个方面介绍了 IP 网络可生存性技术。首先为读者介绍了 IP 网络可生存性研究技术的背景和发展现状；随后介绍了目前快速自愈路由中最为有效的多下一跳路由技术，以及支持多下一跳路由技术的并行传输技术和网络故障的快速检测技术；然后介绍了目前下一代网络技术中能够有效提高网络可生存性的虚拟网构建技术及其对应的自愈技术；最后介绍了安全路由技术，并详细介绍了距离矢量路由协议和域间路由协议的安全技术。

本书适合作为高等院校和研究机构从事网络、信息安全等相关技术人员的参考用书，也可以作为计算机、通信、网络、信息安全等相关专业学生学习网络可生存性技术的参考书和计算机网络课程的辅助教材。

IP 网络可生存性技术

◆ 著 王 滨 杨 强 吴春明
责任编辑 王建军
执行编辑 代晓丽
◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
三河市潮河印业有限公司印刷
◆ 开本：787×1092 1/16
印张：14 2013 年 6 月第 1 版
字数：331 千字 2013 年 6 月河北第 1 次印刷

ISBN 978-7-115-31178-8

定价：58.00 元

读者服务热线：(010)67119329 印装质量热线：(010)67129223
反盗版热线：(010)67171154

前　言

以因特网（Internet）为代表的计算机互联网络已成为现代信息社会最重要的基础设施，渗透到社会生活的各个方面，成为日常生活、军事、经济和政治活动不可或缺的工具。因此，保障网络持续提供服务的能力具有重要意义，它关乎经济稳定、国家安全以及个人活动的顺利进行。近年来，人们努力推动网络技术向前发展，但是自然发生的系统组件故障、不可预料的意外事件和针对网络设备的大规模恶意攻击及侵害事件都严重影响网络系统的正常运行。攻击、故障和意外事件的存在都降低了网络系统的可生存性，所以，目前对网络可生存性的研究成为了网络技术研究的一个热点。

网络生存性研究网络在各种故障、攻击或意外事件的情况下如何持续提供服务。关于网络生存性的研究已经有相当长的历史，随着网络的演进，生存性研究的重点也发生了变化，不同的应用场景对网络可生存性有不同层次的要求，具体可以概括为两个层次。第一个层次是要求保证网络业务的连通性，其含义为当网络发生故障时，网络业务节点对之间至少还有一条路径保持连通，如果要保证网络可生存性，首先必须要保证网络节点之间的连通，这是网络可生存性技术研究的第一个层次；第二个层次则是更进一步，从网络业务的服务质量要求着眼，提高网络在故障情况下的整体可用性和性能下降的可控性，其关注的服务质量具体参数包括系统通信时延、带宽利用率、系统吞吐量、系统整体可用性等。

本书主要从 IP 网络快速故障恢复和安全两个方面对网络可生存性进行了介绍。首先介绍了网络可生存性技术的背景及其发展现状，然后介绍了 IP 网络路由的快速故障恢复方法和多下一跳并行传输的知识，接着介绍了多播路由的故障恢复方法和新一代网络中虚拟网构建技术、可生存性技术。由于这些可生存性技术有效工作的前提是网络故障的快速感知，所以，本书也介绍了网络故障快速感知的相关知识。安全路由作为 IP 网络可生存性另外的一个主要研究内容，本书也分别介绍了安全路由的研究现状、距离矢量路由的安全模型和域间安全路由技术。这些内容作为网络生存性研究的一个子集，其研究开展的较晚，到目前为止还有许多问题亟待解决，并且随着新一代网络研究的日趋丰富很完善，下一代网络的可生存性研究也提上了日程，希望通过本书能够引起更多研究人员和技术人员的兴趣，并且能够将相关的研究内容扩展到下一代网络技术中去。

这本书是我在攻读博士、博士后 6 年时间内科研工作的系统表述，包含了本人和合作作者们共同完成的相关研究，有理论方面的探索和技术方面的创新，也是我在 6 年的研究过程中主持和参与的所有项目的成果汇总。这些项目分别是：国家“863”计划目标导向类

课题“快速自愈路由协议与试验系统”（编号：2007AA01Z2a1）、国家科技支撑计划重大课题“新一代可信任互联网真实地址寻址关键技术”（编号：2008BAH37B02）、国家“863”重大课题“可重构柔性试验网综合管理平台”（编号：2008AA01A323）、国家“973”课题“一体化可信网络与普适服务体系基础研究”（编号：2007CB307102）、国家“973”课题“可重构信息通信基础网络体系研究”（编号：2012CB315903）、国家自然科学基金面上项目“服务适配的虚拟网资源配置与管理机制研究”(编号：61070157)、国家自然科学基金青年基金项目“面向突发毁击事件的 IP 网络路由自愈方法研究”（编号：61103200）。所以，也希望读者能够通过阅读本书了解到目前国内该方向研究的一些进展，从而吸引更多的研究工作者从事该领域的研究，那么将是对本书作者及其推动本书问世的朋友们的最大肯定。

下面将感谢所有为本书研究成果有过贡献和帮助的老师、朋友和学生，没有他们的指导与支持，就没有本书的出版。

本书的研究内容除作者之外，还包括了很多人的心血，他们包括：指导我研究的 3 位导师，国家数字交换工程技术研究中心（NDSC）常务副所长、两项国家科技进步一等奖获得者、一等功臣郭云飞教授，国家数字交换工程技术研究中心（NDSC）总工、“973”首席科学家兰巨龙教授，浙江大学新一代网络实验室主任、“863”信息领域专家吴春明教授；还有我在国家数字交换工程技术研究中心（NDSC）工作学习期间一起帮助和指导过我的刘文芬教授、张建辉博士、郭虹博士、王苏南博士，以及跟我合作过的国家数字交换工程技术研究中心课题组成员陈文平、王超、曹敏、杨琴、周佳、王肖楠、王伟、朱建章等；浙江大学的姜明教授、杨强博士、张旻博士、缪宇庭博士、吴晓春博士、钱亚冠博士、陈飞博士等，本书的很多研究成果与他们的聪明才智和无私的帮助是分不开的；最后向代晓丽女士表示衷心的感谢，正是她的积极推动才有了本书的出版，并且在本书的出版过程中由于我工作的原因屡次推迟交稿，在此致以深深的歉意。

最后感谢我的家人和朋友，特别是我的妻子，6 年来她在生活中对我无微不至的关怀，给予我学业上的支持、精神上的鼓励和生活上的关心，她承担了大量照顾家和孩子的重担，让我有更多的时间和精力从事与本书相关的研究。

由于科研水平有限，加之著书的经验不足，本书一定有不少的缺点和错误，希望得到广大读者的指正。随着网络在当今社会的地位的逐步增强，人们必然会对网络的可生存性提出更高的要求，它也会受到越来越多人的关注和重视，我们将在吸取大家的意见和建议的基础上，不断修改和完善书中的内容，为推动网络可生存性理论与技术的进步尽绵薄之力。

王　滨

2013 年 1 月 11 日　于浙大求是园

目　录

第1章 绪 论

本章首先介绍网络可生存性的由来，对目前网络生存性面临的威胁以及现有提高网络生存性技术进行了全面的介绍，最后给出了本书的章节安排。

1.1 网络生存性

互联网是20世纪发展最为迅速的技术，以Internet为代表的计算机互联网络已成为现代信息社会最重要的基础设施，它已渗透到社会生活的各个方面，成为日常生活、军事、经济和政治活动不可或缺的工具。因此，保障网络持续提供服务的能力具有重要意义，它关乎经济稳定、国家安全以及个人日常活动的顺利进行。尽管在新技术如无线自组织网络（ad-hoc）、传感器网络（sensor networks）、容迟网络（delay-tolerant networks，DTN）以及新需求如多播、服务质量、移动性的驱动下网络互联的范围日渐扩大，但是数据连接服务仍然是网络所提供的主要服务[1~3]。

多年来，人们努力推动网络技术向前发展，但是由于网络系统组件故障和不可预料的意外事件总会影响网络系统的正常运行[4]。另外由于网络的开放性和攻击技术的进步，恶意的攻击者总是有机可乘，使得构建绝对安全的网络系统成为不可能完成的任务。故障、意外事件和恶意攻击的存在都降低了网络系统的服务质量。

可生存性的概念最早出现在武器系统[5]和通信系统[6]中，都被定义成系统被破坏或发生故障后服务可用的概率。Newmann等人于1993年最先定义了网络系统可生存性[7]：在任意不利条件下，计算机通信系统的应用所具有的持续满足用户需求的能力。其中，用户需求包括安全性、可靠性、实时响应和正确性等需求。与之相似，1997年Ellison等人更正式地定义了网络系统的可生存性[8,9]：网络系统在遭受攻击、故障和意外事故的情况下及时完成任务的能力。目前，Ellison等人的定义已经成为普遍认可的定义[10]。网络系统的可生存性是指在出现攻击、故障和意外事件的情况下，网络系统所具有的及时完成任务的能力。其研究与已有的相关研究，如安全性、可信性容错、可依赖性研究等，关系密切。下面具体说明这些概念的差异。

1．可生存性与传统的安全性

网络安全性研究经历了3个阶段：“保护”→“检测”→“容忍”。

在“保护”阶段[11,12]，网络系统的所有者或者管理员通过划分明确的网络边界，利用各种保护和隔离技术手段，如用户鉴别和认证、存取控制、权限管理以及信息加解密等技术，试图在网络边界上阻止非法入侵，达到保护信息安全的目的。第一代网络安全技术解决了很多安全问题，但是由于无法清晰地划分和控制网络边界，第一代

网络安全技术对一些攻击行为如计算机病毒、用户身份冒用、系统漏洞攻击等就显得无能为力。

在“检测”阶段[13~16]，第二代网络安全性研究以检测技术为核心。众所周知，脆弱性+攻击 =入侵。第二代安全性研究也正是从防止脆弱性和抗攻击两个方面展开的：

（1）防止脆弱性的方法主要是在组件使用之前进行严格测试，试图找出并修正系统组件中存在的脆弱点；或者根据系统配置之后发现的针对系统的成功入侵，对系统加补丁。尽管这种方法在处理许多攻击时都很有效，然而现实经验表明，大多数应用系统中仍然存在着相当数量的脆弱点，特别是对于分布式的网络系统，由于其组件之间可能存在的复杂交互，脆弱点的预防变得尤其困难。

（2）防火墙可以很有效地抵御来自外部的入侵攻击，但对于来自网络内部的攻击却显得无能为力。对于信息系统而言，一个存在缺陷的安全措施在运行中不可能非常有效和可靠地提供安全保护。更危险的是，由此造成的“安全”错觉对于安全关键的应用，会造成十分严重的后果。

（3）在处理安全威胁方面，入侵检测系统（IDS）起到了非常重要的作用，然而也存在缺陷，例如通常只关注一些已知的和定义好的攻击、高误报率、高漏报率、时间延迟等问题。攻击者在入侵以后都会试图抹去其入侵的痕迹，因此，即使恶意攻击能够被检测出来，系统管理员仍要面临如何确定其影响以及如何恢复的难题。

经过“保护”和“检测”阶段之后，研究者意识到成功的入侵不可避免，依靠入侵防御技术和检测技术难以保证网络系统的安全性，因此，研究的重点转移到了对入侵的“容忍”[17~19]。与传统的思路不同，容忍入侵的概念承认系统中脆弱点的存在，并假定随着时间的发展，其中某些脆弱点可能会被入侵者利用。其设计目标就是使得系统在受到攻击时，即使系统的某些部分或组件已经被破坏，或者被恶意攻击者操控，系统仍能够触发一些防护机制，使得系统能够继续运行，提供核心的或系统的基本服务，保证系统的基本功能。由于这种方法在一定程度上消除了入侵的影响，因此被称作安全防护的最后防线。

网络系统的可生存性研究以安全性研究为基础，是安全性研究的延续和发展。安全性“保护”技术是抵御恶意攻击的有效手段，安全性“检测”技术可以识别故障和入侵及其影响，与“容忍”技术相结合，为系统从故障和入侵的影响中恢复提供了可能。目前，各种安全技术，尤其是容忍入侵技术，仍然是增强可生存性的有效手段。但是，可生存性与安全性之间存在明显的区别：安全性研究，包括容忍入侵，都侧重于保护网络系统的安全性，一旦系统的安全机制被破坏，则其服务也不再具有所需的属性；而可生存性研究侧重于安全机制被破坏以后，系统及时地做出响应与恢复，使得系统所提供的服务仍然保持所需的属性。

2．可生存性与可信性

网络系统可信性的概念很多[20~26]，但是还没有形成多数人普遍认可的定义。对于可信性要实现的目标，研究者的观点也不尽相同，例如：TCG[27~30]认为可信性的目标包括：①鉴别（authentication）：系统用户可以确定与他们通信的对象身份；②完整性（integrity）：用户确保信息能被正确传输；③私密性（privacy）：用户相信系

统能保证信息的私有性。而 Microsoft 认为要实现的目标是：①安全性（security）：即客户希望系统对攻击具有恢复能力，而且系统及其数据的机密性、完整性和可用性得到保护；②私密性（privacy）：即客户能够控制与自己相关的数据；并按照信息平等原则使用数据；③可靠性（reliability）：即客户可在任何需要服务的时刻能够得到服务；④业务完整性（business integrity）：强调服务提供者以快速响应的方式提供负责任的服务。

然而，可以肯定的是，可信性与安全性紧密相关，如果网络系统是安全的，则其提供的服务一定是可信的。因此，我们认为可以把可信性作为安全性的一个衍生属性，甚至可以细化成综合了机密性、完整性、不可否认性（服务的提供者和接收者双方的不可否认）的一个复合属性。因此，可信性和可生存性之间也存在密切的关系，也是可生存性的研究基础之一。

3．可生存性与容错

对于系统的可生存性而言，除了恶意入侵以外，还需要考虑组件故障的影响，组件故障同样会导致系统服务失败，两者之间也存在明显的区别，如：

（1）并不是所有的破坏都是由故障导致的，例如攻击者的恶意攻击。而容错理论并不是针对攻击专门设计的。

（2）并不是所有攻击都表现为信息和系统的破坏，例如篡改数据等，只要这种攻击本身不构成一种显式的错误，容错就无法解决这些问题。

（3）故障错误是随机发生的，而攻击却是有预谋地利用了系统的弱点和漏洞，这比随机错误更难预防。

（4）容错中常用的备份技术使得攻击者的攻击点从一台主机变成多台主机，这不仅不能增强系统中敏感数据的安全性，相反倒增加了攻击成功的机会。

入侵和故障之间存在的区别使得不能直接套用容错技术解决入侵的问题。然而，从恶意入侵和组件故障对系统服务的影响来看，入侵可以看作一种由外部操作引起的恶意逻辑故障，这种故障将引起系统组件的错误，使得系统进入错误状态，从而引起系统的安全性失败。因此从本质上讲，容忍入侵也可看成是一个容忍和避免故障的问题，其对入侵的检测和响应类似于容错系统中对于系统故障的诊断与处理。

对于可生存性研究，在系统进入异常状态以后，首要的问题不是确定引起系统状态变化的原因，而是评估入侵和故障的影响，使得系统可以及时恢复其服务。因此，重要的容错理念、原理和方法，如冗余、多样性等，也是解决入侵问题的主要组成部分。

4．可生存性与可依赖性

从本质上说，可生存性和可依赖性都是网络系统的可量化的属性。定量研究这些属性可以发现网络系统的弱点、确定存在的风险、有针对性地改善其服务质量（QoS），也有助于保持系统所需的属性。

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，如非状态空间的模型方法和状态空间的模型方法等。可依赖性研究为其他可量化属性的研究奠定了基础。与之相比，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可依赖性研究的成功经验。

1.2 网络生存性的重要性及面临的挑战

1.2.1 网络生存性的重要性

近年来 Internet 得到了迅速的发展，根据互联网系统协会 ISC[31]调查 Internet 主机数量从 1985 年的 213 台主机到 2009 年的 7 亿多（如图 1-1 所示），一直保持着指数级的增长速度。另外，中国互联网网络信息中心 CNNIC[32] 2010 年 1 月公布的域名和网民规模统计数据也同样以指数级速度快速增长，如图 1-2 所示。截至 2009 年 12 月 31 日，我国网民数达到 3.84 亿人。互联网普及率高达 28.9%。无论世界还是中国网络都在飞速的发展，这也导致了网络结构日益复杂，同时底层拓扑结构也要发生巨大的变化。

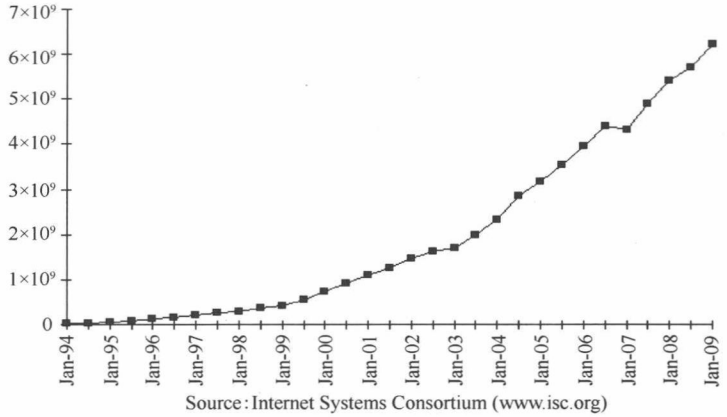

图 1-1 ISC 2009 年 Internet 主机数量统计分析

图 1-2 CNNIC 2010 年中国互联网网民规模统计数据数据统计

随着互联网规模的不断扩大，互联网不仅需要承载传统的传输非实时业务，如收发电子邮件，浏览网页等，过去许多在电信网和有线电视网中传输的业务也开始在互联网上传输，例如 VoIP、在线聊天、视频点播、多用户在线游戏等，并且这些新的数据业务呈现不断增加的趋势，如图 1-3 所示。

图 1-3 基于 IP 实时性应用的增加趋势

表 1-1 列出了几种典型的应用及其需求，其中时延的敏感和对恢复的需求被标记为 1（不敏感）、2（一般敏感）、3（敏感）、4（比较敏感）、5（最敏感）5 个等级。

表 1-1　　新兴的应用服务及其需求

应用	比特率	比特率变化	时延敏感	需要恢复
普通电话服务	32～64kbit/s	不变	5	5
IP 语音	8～32kbit/s	不变	5	5
视频电话	256～1920kbit/s	高	5	5
视频会议	＞256kbit/s	高	5	5
远程办公	64 kbit/s～2Mbit/s	很高	5	4
电视广播	2～8Mbit/s	高	4	4
远程教育	64kbit/s～2Mbit/s	很高	5	5
电影点播	750kbit/s～4Mbit/s	高	4	3
新闻点播	64kbit/s	很高	2	2
网络接入	64kbit/s～2Mbit/s	很高	1	2
电视购物	64kbit/s～2Mbit/s	很高	2	2

综上所述，人们对网络服务的质量和网络在各种异常事件下的服务提供能力要求越来越高，所以迫切的需要提高网络在各种异常环境下的可生存能力。

1.2.2 网络生存性面临的挑战

从表 1-1 可以看出很多应用对网络的服务质量有很高的要求，要求网络尽量的稳定，且当出现故障后要求很快恢复。故障处理时间过长会严重影响时延敏感应用甚至使之完全瘫痪，例如 ITU 标准要求高质量话音的单向时延小于 150ms[33]，VOIP 的话音端到端的单向时延也必须小于 200ms[34]。

然而根据文献[35, 36]观测了运营商 ISP 骨干网络链路状态后得到的统计数据，如图 1-4 所示，运营网络的故障每星期、每天、每小时、每分钟都在发生着。

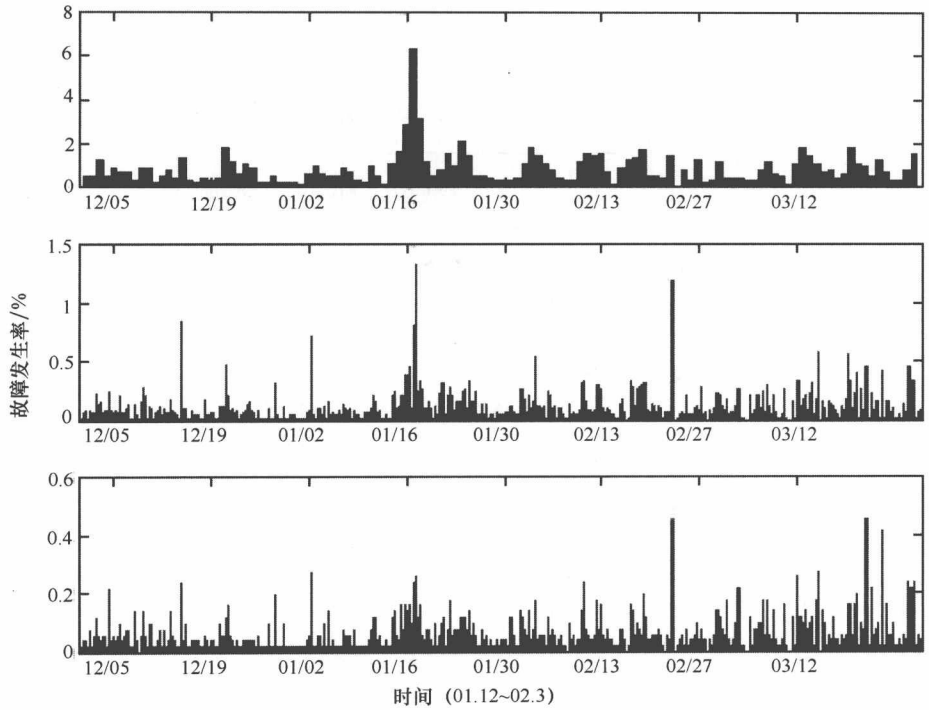

图 1-4　链路故障在各个时间尺度上的发生概率

特别是新的历史形势下，军事打击、自然灾害等导致的突发毁击事件给网络的可生存性造成了严峻挑战。目前尚没有对突发毁击事件的正式定义，一般指能对网络可用性造成严重影响的事件，本文定义的突发毁击事件是会导致网络同时发生多链路或多节点故障的事件[37]，比如 2002 年发生的太平洋海底光缆故障，2006 年年底，台湾附近海域地震，均可定义为突发毁击事件。在突发毁击事件发生时的网络故障同一般运营故障相比，具有以下新的特点：①不具备长期或短期的统计规律性，突发性强，难以预测；②多点并发，在时间与空间分布上表现出完全不同的特性；③破坏作用更加强烈、持续时间长及故障点可能无法恢复。突发毁击事件下的网络故障的上述特点，需要从新的思路出发研究提高网络的可生存性。

另外，当前对网络设备的恶意攻击也越来越频繁，例如 2007 年 5 月 3 日～15 日，爱沙尼亚因为搬迁苏军解放塔林纪念碑而导致与俄罗斯关系紧张后，重要网站因遭到大规模的网络攻击而瘫痪 3 周等事件；如何应对日益严峻的针对网络设备的大规模恶意攻击和侵害突发事件也成为网络可生存性技术研究的挑战之一。

所以，研究定位如何在极端网络环境下提高网络的可生存性：首先是如何在军事打击、恐怖袭击以及自然灾害等突发毁击事件下提高网络的可生存性；其次，如何应对针对网络设备的大规模恶意攻击和侵害事件，提高网络的可生存性。

1.3　网络可生存性技术的研究现状

网络可生存性技术的研究随着网络规模的扩大不断深入，不同的应用场景对网络可