现代通信高技术丛书

IP组播与安全

周贤伟 主编
杨军 薛楠 戴昕昱 编著

国防工业出版社
National Defense Industry Press

现代通信高技术丛书

IP组播与安全

IP Zubo Yu Anquan

周贤伟 主编

杨 军 薛 楠 戴昕昱 编著

国防工业出版社
http://www.ndip.cn

内 容 简 介

本书从实用和科研的角度出发，比较全面、系统地介绍了 IP 组播及相关安全技术的最新发展。

全书共分 12 章，系统地全面地介绍了 IP 组播技术，组播安全体系结构，组密钥管理技术，组播数据认证技术，组安全策略，安全组播路由技术，可靠组播的安全，组播应用安全及展望。

本书内容翔实，深入浅出，覆盖面广，具有先进性、科学性和一定的实用价值，适合高等院校计算机、通信、信息安全等专业师生和对组播安全感兴趣的科研人员和工程技术人员选作参考用书。

图书在版编目(CIP)数据

IP 组播与安全／周贤伟主编；杨军，薛楠，戴昕昱编著. —北京：国防工业出版社，2006.5

（现代通信高技术丛书／周贤伟，邓忠礼，郑雪峰主编）

ISBN 7-118-04466-0

Ⅰ. I... Ⅱ. ①周...②杨...③薛...④戴...

Ⅲ. 互连网络－通信协议 Ⅳ. TN915.05

中国版本图书馆 CIP 数据核字(2006)第 021609 号

※

国防工业出版社出版发行

（北京市海淀区紫竹院南路 23 号 邮政编码 100044）

腾飞胶印厂印刷

新华书店经售

*

开本 787×1092 1/16 印张 15½ 字数 342 千字

2006 年 5 月第 1 版第 1 次印刷 印数 1—4000 册 定价 29.00 元

《现代通信高技术丛书》编委会

序

当今世界已经进入了信息时代，信息成为一种重要的战略资源，信息科学成为最为活跃的学科领域之一，信息技术改变着人们的生活和工作方式，信息产业已经成为国民经济的主导产业，作为信息传输基础的通信技术则成为信息产业中发展最为迅速，进步最快的行业。目前，个人通信系统和超高速通信网络迅猛发展，推动了信息科学的进一步发展，并成为21世纪国际社会和全球经济的强大动力。

随着通信技术日新月异，学习通信专业知识不但需要扎实的专业基础，而且需要学习和了解更多的现代通信技术和理论，特别是数字通信、卫星通信以及传感器网络的现代通信技术方面的知识。从有线通信到无线通信，从固定设备间的通信到移动通信，从无线通信到无线因特网，到传感器网络技术。未来的通信将为人们提供全方位以及无缝的移动性接入，最终实现任何人在任何地方、任何时间进行任何方式的通信，使得通信技术适应社会的发展需要呈现经久不衰的势头。

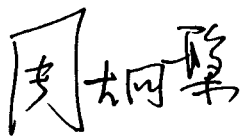
网络技术的飞速发展，通信技术在经济发展中的重要地位日趋重要，世界各国特别重视通信技术的理论研究和通信技术专业人才的培养，国外有关通信领域的文献资料和专著较多。就国内来讲，通信专业人才大量急需，为适应社会经济发展的需要，各高校和科研单位都在培养社会所需的通信专业人才。

为了增进通信及安全技术领域的学术交流，为了满足通信及信息安全专业领域的读者的需要，提供一套能系统、全面地介绍和讲解通信技术原理及新技术的系列丛书，北京科技大学等组织编写了这套《现代通信高技术丛书》。这套丛书内容涵盖了通信技术的主要专业领域，既可作为高等院校通信类、信息类、电子类、计算机类等专业高年级本科生或研究生的教材，又可作为有关通信技术和科研人员的技术参考书。

我觉得这套丛书的特点是内容全面、技术新颖、理论联系实际，针对目前

我国通信技术发展情况与目前已有的相关出版物之间已有一定距离这一情况，本丛书立足于现在，通过对基本的技术进行分析，由浅入深，努力反映通信技术领域的新成果、新技术和进展，是国内目前较为全面、技术领先、适用面广的一套丛书。在我国大量培养通信专业人才的今天，这套丛书的出版是非常及时和十分有益的。

我代表编委会对丛书的作者和广大读者表示感谢！欢迎广大读者提出宝贵意见，以使丛书进一步修改完善。



2005 年 3 月 20 日

前　言

研究者和工程人员一直在研究怎样更有效地利用 IP 网络的潜在优势作为多方通信方案的基础。有多种可能的方式可以提供多方或组通信，而且有不同的通信方法和协议可用于建立一个组内的通信。IP 组播就是其中的一种方法——它发生在 TPC/IP 模型中的 IP 网络层。

1989 年，IETF(Internet Engineering Task Force，Internet 工程任务组)通过 RFC1112 定义了 Internet 上的组播方式。组播是一种针对多点传输和多方协作应用的组通信模型，发送方仅传输 1 份数据，通过让网络元素(如组播路由器和交换机)给接收方复制所需份数的数据，然后把数据包适当地转发到所有用户。组播的优势在于既能降低发送方的计算负荷，也能降低网上数据的份数，从而高效地利用网络资源。组播是用于广域网特别是 Internet 上组通信的一种高效解决方案，是下一代 Internet 应用的重要支撑技术。

通过为 1 到多及多到多通信提供一个高效传送机制，组播使高效的大规模内容分发成为可能。近年来，它已成为许多学术研究和工程实施努力追求的目标。这些努力结果已把组播转化成许多应用都依赖的一门技术。已经开展了可靠性、可管理性、可扩展性、服务质量及部署的便利性等方面的工作。

组播提供了一种发送方同时发送信息到多个接收方的高效通信机制，但是组播的安全问题却阻碍了组播技术的广泛使用。IP 组播的可扩展性得益于其开放性模型。然而，正是组播的这同一性质也就造成了安全问题，因为对已获授权的主机集合限制其通信是不可能的。尽管在过去 10 年里对组播协议有大量的研究和开发，组播应用的部署迄今仍然进展缓慢。主要的原因是组播服务对流量管理、记账与票据、可靠性、路由选择和安全性缺乏有力支持。

卫星电视转播、软件在线分发与升级、股市行情流、Web 超高速缓冲存储、MFTP、IP 电视、远程及视频会议、多媒体会议、视频点播、PPV(Pay-per-view，付费 1 次收看 1 次)、PPU(Pay-per-use，付费 1 次使用 1 次)、多方网络游戏、计算机协同工作等都是需要 1 到多(单源)或多到多(多源)的组通信(实时与非实时、有线与无线、固定与移动)的应用例子。

全书分为 12 章。第 1 章从组播内容保护和基础设施保护这两方面给出组播安全研究的框架和概貌。第 2 章简要介绍 IP 组播的基本原理、技术特点及面临的安全问题。第 3 章描述由 IRTF 安全组播研究组和 IETF 组播安全工作组发展起来的组播安全架构。第 4 章引入组密钥管理的体系结构，第 5 章描述组密钥管理的协议，而第 6 章讨论组密钥管理的算法。这 3 章的主要目标是保障组通信的机密性。安全组播数据处理是第 7 章的主题。安全组策略是第 8 章的主题。基础设施保护是第 9 章(路由协议的安全)和第 10 章(可靠与半可靠组播协议的安全)讨论的内容。第 11 章给出安全组播的几个应用案例。

第 12 章对未来的研究课题进行展望。

本书是作者在多年网络安全教学和科研工作体会、研究成果和吸收国内外相关著作精华的基础上编写而成的。在编写过程中得到了国防工业出版社和北京科技大学的大力支持和帮助。为编著本书，我们参考和吸收了国内外许多同行学者的研究成果，许多朋友都为此付出了辛勤的劳动，在此一并表示衷心感谢。

IP 组播及安全组通信是一门发展迅速的新兴技术，由于作者的学识与水平有限，书中难免出现不妥甚至失误之处，诚望大家批评指正。

编著者

2005 年 11 月于北京

目　录

第1章 概 述

1989年，IETF(Internet Engineering Task Force，Internet工程任务组)通过RFC(Request For Comments，请求评论)1112，定义了Internet上的组播方式[1]。组播是一种针对多点传输和多方协作应用的组通信模型，发送方仅传输1份数据，通过让网络元素(如组播路由器和交换机)给接收方复制所需份数的数据，然后把数据包适当地转发到所有用户。组播的优势在于既能降低发送方的计算负荷，也能降低网上数据的份数，从而高效地利用网络资源。组播是用于广域网特别是Internet上组通信的一种高效解决方案，是下一代Internet应用的重要支撑技术[2~5]。

卫星电视转播、软件在线分发与升级、股市行情流、Web超高速缓冲存储、MFTP、IP电视、远程及视频会议、多媒体会议、视频点播、PPV(Pay-per-view，Internet电视公司在Internet上用组播发送的电视节目，付费1次收看1次)、PPU(Pay-per-use，付费1次使用1次)、多方网络游戏、计算机协同工作等都是需要1到多(单源)或多到多(多源)的组通信(实时与非实时、有线与无线、固定与移动)的应用例子。

组播提供了一种发送方同时发送信息到多个接收方的高效通信机制，但是组播的安全问题却阻碍了组播技术的广泛使用[6~18]。尽管在过去10年里对组播协议有大量的研究和开发，组播应用的部署迄今仍然进展缓慢。尽管有些人把这归因于没有“杀手级应用”，事实上，主要的原因是组播服务对流量管理、记账与票据、可靠性、路由选择和安全性缺乏支持。为了组通信应用的成功部署，我们认为组播安全性是有待解决的重要问题之一。例如，投资者希望得到这样的保证：通过组播方式正在传送的股票报价的确是真实的。类似地，提供商也希望对服务已付费的订阅者的内容分发加以限制。最后，作为安全性的另一方面，机密性是诸如通过Internet的会议、公司通信及军事通信此类应用的一个要求。总之，组播的普通应用要求数据完整性、访问控制及保密性。

研究者和工程人员一直在研究怎样更有效地利用IP网络的潜在优势作为多方通信方案的基础。有多种可能的方式可以提供多方或组通信，而且有不同的通信方法和协议可用于建立一个组内的通信。IP组播就是其中的一种方法——它发生在TCP/IP(Transmission Control Protocol/Internet Protocol，传输控制协议/Internet协议)模型中的IP网络层。

通过为1到多及多到多通信提供一个高效传送机制，组播使高效的大规模内容分发成为可能[12~14,18]。近年来，它已是许多学术研究和工程实施努力追求的目标。这些努力结果已把组播转化成许多应用都依赖的一门技术。已经开展可靠性、可管理性、可扩展性、服务质量及部署的便利性等方面的工作。

IP组播的扩展性好是得益于其开放性模型[12]。不需要与一个集中式实体进行任何交互，接收方能够加入组播组且发送方能够向组播组发送数据。这种开放的组模型在许多环境中是有益的，因为它提供了一种轻量级的加入操作，不要求源保持所有组成员的状