

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. 1... 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

(本书如有印装错误,我社负责调换)

国防书店:(010)68428422

发行邮购:(010)68414474

发行传真:(010)68411535

发行业务:(010)68472764

《现代通信高技术丛书》编委会

名誉主任 周炯槃(院士)

总 编 宋俊德

主 编 周贤伟 邓忠礼 郑雪峰

副主编 曾广平 景晓军 雷雪梅 王丽娜 杨裕亮 马伍新

王祖珮 班晓娟 刘蕴络 王昭顺 王建萍 黄旗明

李新宇 杨 军 覃伯平 薛 楠

编 委 (按姓名笔画排序)

马伍新 王 丹 王 华 王 培 王 强 王庆梅

王丽娜 王建萍 王祖珮 王昭顺 王淑伟 韦 炜

尹立芳 邓忠礼 申吉红 付娅丽 白浩瀚 冯 震

冯晓莹 吕 越 朱 刚 闫 波 安 然 刘 宁

刘 宾 刘 潇 刘志强 刘晓娟 刘蕴络 关靖远

孙 硕 孙亚军 孙辰宇 孙晓辉 李 杰 李宏明

李新宇 苏力萍 肖超恩 吴齐跃 宋俊德 张海波

张臻贤 陈建军 林 亮 杨 军 杨文星 杨裕亮

周 蓉 周贤伟 郑如鹏 郑雪峰 孟 潭 赵鹏(男)

赵鹏(女) 赵会敏 胡周杰 施德军 姜 美 姚恒艳

班晓娟 崔 旭 黄旗明 韩 旭 韩丽楠 覃伯平

景晓军 曾广平 雷雪梅 薛 楠 霍秀丽 戴昕昱

丛书策划 王祖珮

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。

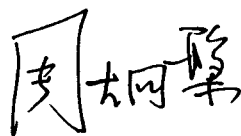
网络技术的飞速发展,通信技术在经济发展中的重要地位日趋重要,世界各国特别重视通信技术的理论研究和通信技术专业人才的培养,国外有关通信领域的文献资料和专著较多。就国内来讲,通信专业人才大量急需,为适应社会经济发展的需要,各高校和科研单位都在培养社会所需的通信专业人才。

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。

A handwritten signature in black ink, appearing to read '周炯明' (Zhou Jiongming), enclosed within a rectangular frame.

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 TCP/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	1
1.1 组播安全的动机	4
1.2 组播内容保护	6
1.2.1 问题区 1: 安全组播数据处理	6
1.2.2 问题区 2: 密钥素材管理	7
1.2.3 问题区 3: 组播安全策略	11
1.3 基础设施保护	12
1.4 安全组播的应用	12
1.5 本书导读	13
参考文献	13
第 2 章 IP 组播概述	16
2.1 IP 组播的概念和特点	16
2.1.1 单播、广播与组播	16
2.1.2 IP 组播的特点	17
2.2 IP 组播地址	17
2.2.1 IPv4 组播地址	17
2.2.2 IPv6 组播地址	19
2.3 IP 组播的相关协议	20
2.3.1 IP 组播组管理协议	20
2.3.2 IP 组播路由协议	21
2.4 可靠组播	26
2.5 拥塞控制	27
2.6 IP 组播面临的问题	27
2.6.1 组播通信所面临的安全风险	27
2.6.2 组播中的安全问题	28
2.7 小结	29
参考文献	29
第 3 章 组播安全体系结构	31
3.1 引言	31
3.2 组播安全参考框架	32
3.2.1 参考框架	32
3.2.2 集中式参考框架的组成部分	33

3.2.3 分布式参考框架的组成部分	33
3.3 功能区	34
3.3.1 组播数据处理	35
3.3.2 组密钥管理	35
3.3.3 组播安全策略	35
3.4 组安全关联	36
3.4.1 安全关联	36
3.4.2 组安全关联结构介绍	37
3.4.3 组安全关联结构论证	37
3.4.4 组安全关联的定义	38
3.4.5 典型的组安全关联组成部分	38
3.5 安全服务	39
3.5.1 组播数据保密性	39
3.5.2 组播源认证和数据完整性	39
3.5.3 组播组认证	40
3.5.4 组播组成员管理	40
3.5.5 组播密钥管理	40
3.5.6 组播策略管理	41
3.6 安全考虑	41
3.6.1 组播数据处理	41
3.6.2 组密钥管理	41
3.6.3 组播安全策略	41
3.7 小结	42
参考文献	42
第4章 组密钥管理的体系结构	44
4.1 组密钥管理体系结构问题和评估标准	44
4.2 IKAM	46
4.2.1 域、区域和密钥分发器	47
4.2.2 控制组播组和数据组播组	48
4.2.3 密钥:组播组和控制组播组	49
4.2.4 控制组播组:地址分发	50
4.2.5 域内密钥分发	50
4.3 Iolus	52
4.3.1 层次型子组	53
4.3.2 子组密钥管理	54
4.3.3 Iolus 的安全组通信	54
4.3.4 Iolus 的优缺点	55
4.4 Nortel	56
4.4.1 Nortel 体系结构	56

4.4.2	Nortel 的优点和缺点	57
4.5	PSMA	58
4.5.1	对用户接入的控制	58
4.5.2	阻塞出现组播异常的用户端口	59
4.5.3	MAS 和 MuPS 的信息交互	59
4.5.4	基于策略的安全组播体系结构的特点	60
4.6	DSMA	60
4.6.1	DSMA 的初始化过程	61
4.6.2	DSMA 的数据传输过程	63
4.6.3	DSMA 解决单点故障	63
4.7	小结	64
	参考文献	64
第 5 章	组密钥管理协议	66
5.1	一种简单的组密钥管理协议	66
5.2	组密钥管理协议	67
5.2.1	GKMP 实体	67
5.2.2	发送方发起的组播	68
5.2.3	接收方发起的组播	68
5.3	GSAKMP	69
5.3.1	GSAKMP 信任模型	70
5.3.2	组生命周期	70
5.4	GDOI	74
5.4.1	GSA 模型	75
5.4.2	GSA 的定义	76
5.4.3	GDOI 和 IKE	78
5.4.4	GDOI 的新元素	78
5.4.5	新的 GDOI 阶段 2	80
5.4.6	更新 SA	81
5.4.7	GDOI 的功能模块图	81
5.5	小结	82
	参考文献	82
第 6 章	组密钥管理算法	84
6.1	批量密钥更新与周期密钥更新	84
6.2	MARKS	86
6.3	LKH	87
6.3.1	LKH 的初始化	88
6.3.2	向密钥树添加一个成员	88
6.3.3	LKH 的加入更新	88
6.3.4	LKH+ 的高效加入密钥更新	89

6.3.5	LKH 的离开密钥更新	90
6.3.6	利用 OFC 的高效的离开密钥更新	90
6.4	OFT	91
6.4.1	OFT 的初始化	93
6.4.2	OFT 的加入密钥更新	93
6.4.3	OFT 的离开密钥更新	94
6.5	一种高效的密钥管理算法	95
6.5.1	加入密钥更新	95
6.5.2	离开密钥更新	96
6.6	基于用户概率分组模型的密钥分发方法	96
6.6.1	用户概率分组模型	97
6.6.2	基于用户概率分组模型的密钥分发方法性能分析	98
6.7	基于成员行为的 LKH 方案	99
6.7.1	R-LKH 方案	99
6.7.2	R-LKH 的实现	102
6.8	密钥树中成员关系变化的批量处理	103
6.9	密钥更新消息的可靠传输	103
6.9.1	密钥更新消息的反复重传	103
6.9.2	FEC	104
6.9.3	加权密钥分配	104
6.10	无状态密钥撤销算法	104
6.10.1	STR	105
6.10.2	SDR	106
6.11	小结	107
	参考文献	108
第 7 章	组播数据认证	110
7.1	组播数据认证中的问题	111
7.1.1	提供组认证	112
7.1.2	提供源认证	112
7.2	用于源认证的数字签名	113
7.3	用于认证流式数据的散列链	116
7.3.1	散列链的示意图	116
7.3.2	高效的多重链流签名	117
7.3.3	扩张链	118
7.3.4	捎带确认	118
7.3.5	关于使用散列链进行认证的讨论	119
7.4	用于不可靠流的基于 MAC 的源认证	120
7.4.1	TESLA 的初始化	121
7.4.2	发送方基于 MAC 的数据包认证	121

7.4.3	TESLA 中接收方处理数据包的过程	122
7.4.4	改进的 TESLA	123
7.4.5	TESLA 的应用性分析	123
7.5	有损信道下实时组播的高效源认证方案	124
7.5.1	攻击者模型及安全保证	124
7.5.2	用于分析强健的源认证方案的数据包信道模型	124
7.5.3	强健的链式流数据源认证方案	124
7.5.4	强健的链式流数据源认证方案的实施	125
7.5.5	混合方案的实施	126
7.5.6	自适应链式流数据源认证方案	128
7.5.7	延迟显密密钥的扩展方案	128
7.5.8	通信开销的增加	129
7.6	IPSec ESP 和 MESP	129
7.7	小结	130
	参考文献	130
第 8 章	组安全策略	132
8.1	组安全策略框架	132
8.2	组安全策略的分类	134
8.2.1	通告策略	134
8.2.2	成员关系策略	135
8.2.3	访问控制或授权策略	135
8.2.4	数据保护策略	135
8.2.5	组管理委派策略	136
8.2.6	密钥分发策略	136
8.2.7	泄露恢复策略	136
8.3	组安全策略规范	137
8.3.1	GSPT	137
8.3.2	Ismene 策略规范	138
8.3.3	CCNT	139
8.3.4	策略规范语言的讨论	140
8.4	策略协商和调和	140
8.4.1	Ismene 策略调和	140
8.4.2	DCCM 中的策略协商	141
8.5	组安全策略实施	141
8.5.1	GSAKMP 策略分发和实施	141
8.5.2	Antigone 策略框架	142
8.5.3	GDOI 中的策略分发和实施	142
8.6	策略令牌	143
8.6.1	令牌的创建和接收	143

8.6.2 策略令牌	144
8.6.3 安全考虑	145
8.7 小结	145
参考文献	146
第9章 安全组播路由协议	148
9.1 组播安全的3个组成部分	148
9.1.1 组播路由的一般攻击类型	149
9.1.2 组播路由及安全	150
9.2 组播路由概述	151
9.2.1 组播路由协议分类	152
9.2.2 DVMRP	152
9.2.3 PIM	153
9.2.4 IGMP	155
9.2.5 ASM 与 SSM	157
9.2.6 MOSPF	157
9.3 单播和组播路由的安全需要	158
9.4 PIM-SM 安全	160
9.4.1 背景	160
9.4.2 PIM 认证	160
9.4.3 适于 PIMv2 的 SKMP	161
9.4.4 PIM-SM 的修订版:安全问题	163
9.4.5 PIM-SM 的修订版:可能的解决方案	164
9.5 MSDP 安全	165
9.6 IGMP 安全	166
9.6.1 IGMP 攻击类型	166
9.6.2 防御 IGMP 攻击的策略	167
9.6.3 成员授权和认证问题	167
9.6.4 成员授权方法	168
9.6.5 消息认证方法	169
9.6.6 未解决的问题	170
9.7 其他路由协议的安全	170
9.7.1 安全 CBT 组播:SMKD	171
9.7.2 KHIP	171
9.8 Ad-hoc 网络及 WSN 的安全组播路由	172
9.8.1 Ad-hoc 及 WSN 的安全特性	172
9.8.2 基于 GPS 的安全组播协议	173
9.8.3 非 GPS 的安全组播协议	175
9.9 小结	177
参考文献	178

第 10 章 可靠与半可靠组播安全	182
10.1 预备知识	182
10.2 RM 协议的分类	183
10.2.1 好的吞吐策略	183
10.2.2 网络实体参与和支持	185
10.2.3 前馈式与反馈式	185
10.3 RM 协议通用安全需求	186
10.4 TRACK 协议的安全	187
10.4.1 TRACK 模型	188
10.4.2 RMTP - II	188
10.4.3 TRAM	191
10.5 NORM 协议的安全	191
10.5.1 NORM 模型	192
10.5.2 PGM	194
10.5.3 LARMP	196
10.6 基于 FEC 的协议的安全	198
10.7 可靠组播拥塞控制机制的安全	201
10.8 小结	202
参考文献	202
第 11 章 组播应用及其安全	204
11.1 股市数据分发	204
11.1.1 背景	204
11.1.2 网络拓扑	205
11.1.3 安全需求和可能的解决方法	206
11.2 组播的多媒体应用	207
11.2.1 背景	207
11.2.2 网络拓扑	207
11.2.3 安全需要和可能的的方法	209
11.3 软件更新	209
11.3.1 MFTP	210
11.3.2 MFTP 应用的安全需求	211
11.3.3 MFTP 的安全解决方案	211
11.4 军事应用	212
11.5 小结	213
参考文献	214
第 12 章 总结和展望	215
12.1 IETF 组播安全框架	215
12.2 安全组播数据传输	216
12.2.1 组认证	216

12.2.2 源认证	216
12.3 组密钥分发	217
12.3.1 密钥更新信息的可靠传送	217
12.3.2 安全组播组管理	218
12.3.3 分布式组密钥管理	219
12.3.4 在无线环境中移动成员之间安全组通信	219
12.4 策略	219
12.5 基础设施保护	219
12.6 未来的研究方向和结语	220
参考文献	224
缩略语	225

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