



信息科学技术专著丛书

# 多用户安全无线通信

王强 著

Secure Multi-user Wireless Communications



北京邮电大学出版社  
[www.buptpress.com](http://www.buptpress.com)



信息科学技术专著丛书

# 多用户安全无线通信

王 强 著



北京邮电大学出版社  
www.buptpress.com

## 内 容 简 介

无线通信技术的飞速发展带动了移动互联网和其应用的发展,无线通信的安全性、隐私性问题越来越受到重视。由于无线传输媒介的开放性和广播性,所以从信源到目的接收者的安全通信一直以来都是一个重要的挑战。对于这种天然存在的安全问题,自1948年香农创立信息论至今,学术界对其的研究从未停止。

本书根据作者近年来在多用户无线通信领域的研究成果所写。本书从基本的多天线传输技术和多用户传输模型引入,进而从安全自由度的角度对多用户无线传输系统的性能进行分析。本书针对有独立窃听者的Wire-tap类信道模型和无独立窃听者的机密消息传输信道模型分别进行了具体的模型分析和安全传输技术研究,还对多跳等其他场景的多用户无线传输及安全问题进行了分析。本书可作为从事无线通信安全相关方向工作的工程师的参考书,也可作为研究物理层安全方向的学生的工具书。

### 图书在版编目(CIP)数据

多用户安全无线通信 / 王强著. -- 北京: 北京邮电大学出版社, 2021. 7

ISBN 978-7-5635-6434-7

I. ①多… II. ①王… III. ①无线电通信—安全技术 IV. ①TN92

中国版本图书馆CIP数据核字(2021)第145614号

策划编辑: 马晓仟 责任编辑: 王小莹 封面设计: 七星博纳

出版发行: 北京邮电大学出版社

社 址: 北京市海淀区西土城路10号

邮政编码: 100876

发 行 部: 电话: 010-62282185 传真: 010-62283578

E-mail: publish@bupt.edu.cn

经 销: 各地新华书店

印 刷: 唐山玺诚印务有限公司

开 本: 787 mm×1 092 mm 1/16

印 张: 13.5

字 数: 350千字

版 次: 2021年7月第1版

印 次: 2021年7月第1次印刷

ISBN 978-7-5635-6434-7

定 价: 49.00元

· 如有印装质量问题, 请与北京邮电大学出版社发行部联系 ·

## 前 言

近年来,移动通信系统迅速发展,从 1G 到 5G 几乎每十年进行一代更新,已经深刻地改变了人们的生活和沟通方式,拉近了人与人之间的交流距离。移动通信技术的进步同时孕育了大量的新型信息服务业务,从基本的“衣食住行”、媒体文娱到金融商务等均可以及时而又方便地通过移动终端这种灵巧的载体呈现在面前,使人们获得不亚于线下的服务体验。新一代移动通信系统向更加高带宽、大容量、低延时的方向发展,其服务对象开始逐步从个人服务向工业生产和管理领域拓展,并逐步成为赋能各种行业发展的重要技术引擎。移动通信对各行各业的深度渗透带来安全隐患,特别是大数据应用的爆发增加了人们对隐私泄露的担心,这使得人们对移动通信系统的安全问题越来越重视。传统上,通信系统的安全通过签名认证、密码技术等实现,而随着系统结构越来越复杂,研究者们开始从网络内生安全角度出发,考虑基于网络内生结构的安全性能与保护技术。

由于无线传输媒介的开放性和广播性,所以从信源到目的接收者的安全通信一直以来都是一个重要的挑战。对于这种天然存在的安全问题,自 1948 年香农创立信息论至今,学术界对其的研究从未停止。在信息与通信理论的前驱研究者 Wyner 和 Maurer 等进行了单点至单点传输模型的基础理论研究之后,众多学者再次开展了对物理层安全的相关研究。物理层安全的基本前提是在窃听者在场的情况下,通过无线介质交换机密消息,而不依赖于更高层次的加密技术。信息的泄露可能发生在独立的外部窃听者或攻击者,也可能发生在不同的合法接入用户之间,这是近年来无线通信传输安全的基本研究点之一。

自移动通信系统引入多天线技术以来,空间资源得到有效利用,系统的传输容量大幅提升,天线空间资源的利用方法已经成为移动通信系统的重要基础技术之一。理论上,可以通过不断增加天线数目的方式来持续地增加系统的容量,当然实际系统还要考虑尺寸和功耗等各方面问题。在 4G 系统中,天线数目还比较少,但在 5G 系统中,天线数目可以达到百根以上。而目前面向下一代移动通信系统研究也涌现了智能反射面、多点对多点的非蜂窝传输方式,进一步利用发挥了空间资源的优势。其中,从信息理论基本模型来看,相比点对点的香农经典模型、点对多点广播信道模型,多点对多点的干扰信道传输是近年来的研究热点和难点之一,其基本结构的安全性和保护技术更加有挑战性。

本书共分为 8 章。第 1 章是概述。第 2、3 章分别介绍多天线技术和多用户通信的基础。第 4~8 章针对不同基本模型讲述安全无线通信技术:第 4 章针对存在独立窃听者的无线通信系统模型,分析了无线传输的安全性能以及介绍可靠的传输方式;第 5 章详细介绍了中继系统的物理层安全传输技术,并分别讨论了单中继、多中继、多窃听者的情况;第 6 章针对多用户中继网络,讨论在当前中继系统下干扰对齐的工作,分析无干扰传输的条件及安全性能;第 7 章针对非对称信道的安全无线传输,从基础的机密干扰信道模型出发,分析系统的安全自由度,

进而分析安全自由度的可达性;第8章针对非满秩信道的安全无线传输,分析机密信息广播信道和机密信息干扰信道的安全自由度,进而分析非满秩信道的干扰网络性能。

本书包含了作者近年来在无线安全传输领域的研究成果,在本书写作的过程中作者得到了近年来所指导相关方向的研究生的倾心支持,本书之所以能成文离不开他们的工作,特别是在本书资料的编辑和整理过程中,少不了陈镜伊、梁彬彬等同学提供的帮助。在此感谢国家自然科学基金委员会对作者工作及本书的支持。最后,感谢北京邮电大学出版社的大力支持和高效工作,使本书能尽早与读者见面。

本书基于作者对相关方向的研究和该领域的理解,并且撰写时间紧张,书中难免存在不周之处,敬请读者谅解,并希望读者批评指正,提出宝贵意见。

王 强

# 目 录

<b>第 1 章 多天线无线通信</b> .....	1
1.1 无线通信历史 .....	1
1.2 无线通信系统安全 .....	2
1.3 本书章节安排和内容梗概 .....	3
本章参考文献.....	4
<b>第 2 章 多天线技术</b> .....	5
2.1 分集技术 .....	5
2.1.1 接收分集 .....	5
2.1.2 发射分集 .....	7
2.2 空间复用技术 .....	9
2.2.1 发射机和接收机结构.....	10
2.2.2 贝尔实验室分层空时码.....	11
2.3 DMT 分集复用折中 .....	13
2.3.1 信道模型.....	14
2.3.2 分集和复用折中.....	15
2.3.3 最佳折中.....	16
2.4 波束赋形技术.....	18
本章参考文献 .....	20
<b>第 3 章 多用户无线通信</b> .....	23
3.1 广播传输.....	23
3.1.1 背景知识.....	23
3.1.2 MIMO 广播传输模型 .....	24
3.1.3 MIMO 系统容量 .....	25

3.2 多址 MIMO 系统接收机 .....	36
3.2.1 空时分组编码 .....	36
3.2.2 点对点和多址 MIMO 模型 .....	37
3.2.3 多址 MIMO 线性接收机 .....	39
3.3 多用户干扰信道 .....	41
3.3.1 自由度概念 .....	42
3.3.2 $K > 2$ 用户干扰信道 .....	46
3.3.3 一种渐近干扰对齐算法 .....	47
3.3.4 协同干扰网络 .....	52
本章参考文献 .....	54
<b>第 4 章 无线窃听信道安全传输 .....</b>	<b>58</b>
4.1 窃听信道 .....	58
4.2 MIMO 窃听信道 .....	64
4.2.1 单用户 MIMO 窃听信道 .....	64
4.2.2 多用户 MIMO 窃听信道 .....	68
4.3 带有协作干扰器的 MIMO 干扰信道 .....	74
本章参考文献 .....	80
<b>第 5 章 中继系统物理层安全 .....</b>	<b>84</b>
5.1 全双工单中继系统物理层安全的性能研究 .....	84
5.2 全双工多中继系统物理层安全的性能研究 .....	94
5.3 多窃听者全双工中继系统物理层安全的性能研究 .....	104
本章参考文献 .....	110
<b>第 6 章 多用户多跳网络 .....</b>	<b>113</b>
6.1 多用户多跳无线通信 .....	113
6.2 单中继多用户干扰传输 .....	115
6.2.1 多用户中继系统研究 .....	115
6.2.2 单中继干扰网络的性能研究 .....	119
6.3 多跳多用户分组传输 .....	126
6.3.1 系统模型 .....	127
6.3.2 瞬时安全容量 .....	127

6.3.3 遍历安全容量 .....	129
6.3.4 节点位置对系统安全容量的影响 .....	133
6.3.5 仿真分析 .....	134
本章参考文献 .....	138
<b>第 7 章 非对称信道的安全无线传输</b> .....	<b>143</b>
7.1 多用户隐私传播信道 .....	143
7.1.1 机密消息广播信道 .....	143
7.1.2 机密消息干扰信道 .....	150
7.2 非对称安全传输 .....	156
7.2.1 干扰信道的安全自由度 .....	157
7.2.2 非对称多用户 MIMO 干扰信道模型 .....	157
7.2.3 非对称干扰信道的安全自由度 .....	158
本章参考文献 .....	169
<b>第 8 章 非满秩信道的安全无线传输</b> .....	<b>173</b>
8.1 非满秩 BCCM 安全自由度 .....	173
8.2 非满秩 ICCM 安全自由度 .....	176
8.3 非满秩信道的干扰网络性能 .....	184
8.3.1 模型 .....	185
8.3.2 结论 .....	186
8.3.3 模型上界证明 .....	186
8.3.4 模型可达证明 .....	187
8.3.5 实验结果分析 .....	199
本章参考文献 .....	200
<b>附录</b> .....	<b>201</b>

# 第 1 章 多天线无线通信

## 1.1 无线通信历史

移动通信从 20 世纪 70 年代贝尔实验室提出蜂窝小区开始,成为向公众的生产生活提供通信服务的重要技术。数十年来,移动通信系统每隔十年左右进行一代技术更迭和演进。20 世纪 80 年代第 1 代移动通信系统(1G)商用,如今全球已经进入第 5 代移动通信系统(5G)大规模商用部署阶段,新技术和标准化研究开始向第 6 代移动通信系统(6G)迈进。

### (1) 第一代移动通信技术(1G)

1G 是指第一代移动通信技术,于 20 世纪 80 年代系统商用,基于频分多址(Frequency Division Multiple Access, FDMA)和模拟调频多址技术,如高级移动电话系统(Advanced Mobile Phone System, AMPS)。其中 AMPS 最初在美国推出。在 1G 中,语音呼叫被叠加在更高的频率上,以便在塔之间传输。该行为可通过频分复用技术来完成。1G 作为较早的移动通信技术,具有较多的缺点,如传输慢,存在较多的干扰问题,没有安全性,语音连接差,交接不可靠和设备不轻便等。

### (2) 第二代移动通信技术(2G、2.5G、2.75G)

2G 主要基于全球移动通信系统(Global System for Mobile Communications, GSM)。2G 系统所使用的基本技术包括有数字时分多址技术(Time Division Multiple Access, TDMA)和码分多址技术(Code Division Multiple Access, CDMA)。CDMA 是多路复用的一种类型。它允许各种信号使用同一个的传输信道,以提高可用带宽的使用率。2G 主要于 20 世纪 90 年代系统商用,与 1G 相比,2G 的频谱效率提高了 2 倍或更多。电路交换技术的使用能够支持互联网浏览,如文本信息、图片信息和多媒体信息服务(Multimedia Message Service, MMS)等。2G 利用编译器对数字数据进行压缩和复用,不仅能够使语音更清晰,同时也可以减少噪音。由于 2G 使用的是数字信号,所以其消耗的电池电量较少,且有助于手机寿命的延长。使用 2G 时需满足一定的要求,如发送者和接收者都需要有足够的安全性。其原因是 2G 使用数字信号进行数据传输,数据将被发送到预定的接收方。2G 以较低的成本提供更好的服务质量(Quality of Service, QoS)和更高的容量。

### (3) 第三代移动通信技术(3G)

3G 也被国际电信联盟(ITU)规范称为 IMT-2000。具体的系统标准主要包括 W-CDMA、CDMA2000、TD-SCDMA、WiMAX。3G 中的通信是通过使用网络语音协议(Voice over Internet Protocol, VoIP)来完成的。该技术于 2000 年引入,以提供更高的数据速率。其数据传输率要求从车速移动下的 144 kbit/s,提高至室内状态的 2 Mbit/s。此外,3G 采用了更高的

频率,且频谱效率得到提高。3G 系统有更高的数据速率,支持了视频会议等无线服务,网页浏览速度更高,单位区域的网络容量也更高。

#### (4) 第四代移动通信技术(4G)

4G 又被称为无处不在的移动宽带,且常被称为 MAGIC(Mobile Multimedia Anywhere Global Mobility over Customized Services)。4G 所使用的技术是 LTE/WiMAX,其下载速度为 100 Mbit/s。4G 移动数据的传输速率高达 20 Mbit/s,且在静止状态下的传输速率为 1 Gbit/s。而在移动状态下,传输速率约为 100 Mbit/s。OFDM 的传输数据速率为 54~70 bit/s,这比 CDMA 系统高得多。此外,4G 使用的技术还有正交频分复用(Orthogonal Frequency-Division Multiplexing, OFDM)、功率预测和自适应调制等。

4G 具有以下优势:使用软件定义无线电,具有更高的效率,速度在 20 Mbit/s 到 100 Mbit/s 之间和安全度高等。同时,4G 也具有以下劣势,即昂贵、难以实施以及硬件复杂。因此,4G 存在以下几点有待解决的问题,如切换、位置协调、QoS 支持、网络认证和网络故障等。

#### (5) 第五代移动通信技术(5G)

5G 高度支持无线万维网。它具有大容量和高速度。5G 速度高于 1 Gbit/s。5G 有效地解决了使用 4G 时所面临的问题。5G 不仅能够提供更准确可靠的数据传输,支持虚拟专用网络,还具有更高的下载和上传速率。移动中,5G 可达 1 Gbit/s 左右的数据速率。此外,5G 还具有更广的覆盖面、更高的软件定义的无线电(Software Definition Radio, SDR)安全性、更便宜的流量费、更高的频谱效率、更低的电池消耗等特点。5G 中所使用的技术有大区域同步码分多址接入技术、正交频分复用、多载波码分多址、超宽带、本地多点分布服务等。表 1-1 展示了 1G~5G 技术的相似性和差异性。

表 1-1 1G~5G 技术的相似性和差异性

参数	1G	2G	3G	4G	5G
数据带宽	2 kbit/s	64 kbit/s	2 Mbit/s	1 Gbit/s	>1 Gbit/s
技术	模拟蜂窝技术	数字蜂窝技术	CDMA 2000	WiMAX LTE WiFi	WWW
服务项目	移动电话(声音)	数字语音、短信	视频和数据	可穿戴设备	AI 功能
复用	FDMA	TDMA/CDMA	CDMA	CDMA	CDMA
交换	电路	电路和分组	分组	全分组	全分组
核心网络	公共交换电话网络	公共交换电话网络	分组网络	互联网	互联网

## 1.2 无线通信系统安全

无线介质具有两个基本特性,即广播和叠加。在具有对抗用户时,上述两个基本特性对确保可靠和/或安全的无线通信提出了不同的挑战。无线通信的广播特性使得发送信号很难不被非预期的接收者接收,而叠加会导致多个信号在接收者重叠。因此,对抗用户通常被建模为:①在未被检测到的情况下,试图从正在进行的传输中提取信息的未授权接收者;②试图减少目标接收者信号的恶意发送者(干扰者)<sup>[2]</sup>。无线通信系统安全一直是学术界关注的焦点。

在 Wyner 和 Maurer 进行了一些初步的理论研究之后<sup>[3]</sup>,众多学者再次开展了对物理层安全的相关研究。物理层安全的基本前提是允许在未经授权的窃听者在场的情况下,通过无

线介质交换机密消息,而不依赖于更高层次的加密。这主要可以通过以下两种方式实现:第一种方式是通过智能设计传输编码策略,不需要密钥;第二种方式是在公共信道上利用无线通信介质开发密钥。物理层安全的基本原理是利用噪声和通信信道的固有随机性,来限制未经授权的接收者可以提取的信息量。更重要的是,在不考虑窃听者在计算资源和网络参数知识方面的限制的情况下,可以精确量化所获得的安全性。通过设计编码和传输预编码方案,以及利用任何可用的信道状态信息,物理层安全方案可以在无线介质上实现秘密通信,而无须加密密钥的帮助<sup>[4]</sup>。即物理层安全解决方案利用无线信道的随机特性来生成用于加密机密信息的密钥,以及利用一系列其他复杂的技术来降低窃听者和其他恶意用户接收到的信号质量。在复杂的信号设计和信号处理技术的帮助下,它们也能够支持不需要密钥的安全传输<sup>[5-6]</sup>。

物理层安全有望在 6G 网络中提供除上层加密技术之外的另一层防御<sup>[7-9]</sup>。物理层安全技术利用先进的信道编码、大规模 MIMO、太赫兹等技术,可以实现无线信号的安全传输。此外,物理层密钥和物理层认证可以为空中接口提供轻量级的安全保护。

### 1.3 本书章节安排和内容梗概

针对前文所述的无线通信历史和无线通信系统的安全问题,本书将从技术背景、理论分析和多用户安全无线通信技术三部分,针对多天线安全无线通信展开阐述与探讨。各部分和章节安排如下。

技术背景部分:以本书第 2 章为主,介绍多天线技术,其中包括分集技术、空间复用技术、DMT 分集复用折中以及波束赋形技术。

理论分析部分:以本书第 3 章为主,介绍多用户无线通信。首先介绍广播信道模型,然后介绍多址 MIMO 系统,并分析多址 MIMO 接收机如何消除多址干扰、自干扰和噪声。最后考虑多用户干扰信道,包括重要指标如自由度(DoF)以及干扰对齐算法。

多用户安全无线通信技术部分:包括本书第 4 章至第 8 章,具体章节安排如下。

第 4 章针对存在独立窃听者的无线通信系统模型,分析了无线传输的安全性能以及介绍了可靠的传输方式。在此基础上,进而介绍了多用户 MIMO 窃听信道的模型和性能分析,对 MIMO Wire-tap 信道的安全传输技术做了详细描述。

第 5 章在第 4 章的基础上引入中继传输技术。中继传输技术作为无线通信网络的关键技术之一,具有显著提高无线通信的吞吐量和扩大网络覆盖范围的特点。该章详细介绍了全双工中继系统的物理层安全传输技术,并分别讨论了单中继、多中继、多窃听者的情况。

第 6 章介绍多用户多跳网络。首先讨论在已有的中继系统下干扰对齐的研究,接下来根据中继干扰网络场景,给出无干扰传输的条件,并分析干扰中和技术的可行性。最后,从不同角度分析多用户多跳网络的安全性能,和衡量系统性能的容量指标。

第 7 章介绍非对称信道的安全无线传输。针对非对称信道,从基础的机密干扰信道模型出发,理论推导系统的安全自由度,进而分析安全自由度的可达性。

第 8 章介绍非满秩信道的安全无线传输。针对非满秩信道,理论推导机密信息广播信道(Broadcast Channel with Confidential Messages, BCCM)和机密信息干扰信道(Interference Channel with Confidential Messages, ICCM)的安全自由度,进而分析非满秩信道的干扰网络

性能。

## 本章参考文献

- [1] Stark W E, McEliece R J. On the capacity of channels with block memory[J]. IEEE Transactions on Information Theory, 1988, 34(2):322-324.
- [2] Kashyap A, Tamer Başar, Srikant R. Correlated jamming on MIMO Gaussian fading channels[J]. IEEE Transactions on Information Theory, 2004, 50(9):2119-2123.
- [3] Wyner A D. The wire-tap channel[J]. Bell Labs Technical Journal, 1975, 54(8).
- [4] Mukherjee A, Fakoorian S A A, Huang J, et al. Principles of physical layer security in multiuser wireless networks: A Survey[J]. IEEE Communications Surveys & Tutorials, 2014, 16(3):1550-1573.
- [5] Sun L, Du Q. Physical layer security with its applications in 5G networks: a review[J]. China Communications, 2017.
- [6] Wu Y, Khisti A, Xiao C, et al. A survey of physical layer security techniques for 5G wireless networks and challenges ahead [J]. IEEE Journal on Selected Areas in Communications, 2018, 36(4):679-695.
- [7] Yang P, Xiao Y, Xiao M, et al. 6G wireless communications: vision and potential techniques[J]. IEEE Network, 2019, 33(4):70-75.
- [8] Mahmood N H, Alves H, Lopez O A, et al. Six key enablers for machine type communication in 6G[EB/OL]. <https://arxiv.org/pdf/1903.05406.pdf>.
- [9] Tariq F, Khandaker M R A, Wong K K, et al. A speculative study on 6G[J]. IEEE Wireless Communications, 2020, 27(4):118-125.

## 第2章 多天线技术

### 2.1 分集技术

在通信系统中,我们需在保持较高频谱效率的前提下,提高发射机和接收机之间通信工作的可靠性。对分集技术的应用是一种有效的解决方案。可以应用于通信系统的分集技术有很多,本节主要从接收分集和发射分集两个方面展开讨论。此外,分集技术还可以划分为时间分集、频率分集和空间分集或这三种分集的任意组合。在时间分集中,同一信息承载信号在不同的时隙中传输。当传输同一符号的两个时隙之间的持续时间大于信道的相干时间时,可以获得良好的增益。在频率分集中,同一信息承载信号在不同的子载波上传输。当子载波之间的分离度大于相干带宽时,就可以获得良好的分集增益。在空间分集中,相同的信息承载信号通过不同的天线进行传输或接收。当信道中发生的衰落是独立的或低相关的时,可以获得最大的增益。在接收机中,可以通过合并独立或低相关信道来实现分集增益。

#### 2.1.1 接收分集

我们首先考虑接收分集的情况,即指额外的接收天线对系统性能的影响。为了隔离接收分集的影响,我们考虑一个发射机有单根天线、接收机有多根天线的传输系统。这种系统也被称为单输入多输出系统(SIMO)。需注意的是,此处的“输入”和“输出”指的是信道,而不是设备。即在该系统中,一个信号进入信道, $N$ 个信号出信道。

在SIMO中,每个接收天线都会接收到一个独立的信号副本。在接收机上,所有这些信号可以合并成一个更强的信号。因此,SIMO系统的信道容量为

$$C = \log_2(1 + \rho(\|h_1\|^2 + \dots + \|h_{N_{RX}}\|^2)) \quad (2-1)$$

由于可以将不相关信号的功率相加以求出总功率,所以接收端的平均信噪比是各个路径的信噪比之和。假设所有路径的信噪比衰减大致相同,则多天线接收机的平均信噪比将近似于 $N_{RX}$ 。其中,SNR为单信道的信噪比。因此可得一个使用接收分集的信道容量近似值:

$$C = \log_2(1 + N_{RX}\rho \|h_{avg}\|^2) \quad (2-2)$$

由实验可知,接收分集在容量上有很大的提升。 $1 \times 1$ 系统在10 dB SNR下提供的理论容量为2.92 bit/(s · Hz),而 $1 \times 2$ 系统的可提高到4.05 bit/(s · Hz)。 $1 \times 3$ 系统的为4.73 bit/(s · Hz), $1 \times 4$ 系统的为5.19 bit/(s · Hz)。这种改进是在不增加功率或带宽的情况下实现的,该改进完全依靠MIMO信道中的额外自由度。该结果体现了MIMO系统的惊人潜力。为了在 $1 \times 1$ 系统中获得类似从2.92 bit/(s · Hz)到5.19 bit/(s · Hz)的改进,需要

提高约 8dB 的功率或增加 70% 的带宽。在功率受限和带宽受限的系统中,我们不能自由地提高功率或增加带宽,因此 MIMO 是增加吞吐量的唯一可用途径。

在接收侧的空间分集中,接收机中使用了多根天线。各天线之间有足够的时间,因此降低了天线之间的相互关联性,从而使分集增益增加<sup>[1]</sup>。为了得到接收机的分集增益,需将来自不同天线的接收信号进行组合。组合方法有四种,即选择合并(Select Combining, SC)、最大比合并(Maximal-ratio Combining, MRC)以及等增益合并(Equalgain Combining, EGC)、平方律合并(Square Law Combining, SLC)。表 2-1 为各组合方法的比较。从性能的角度来看, MRC 是最优的,即是性能最好的。前三种组合方法都是线性的,而最后一个需要非线性的接收机。线性合并方案的简单框图如图 2-1 所示。在 SC 中,SNR 最大分支处的信号被选择,而其他接收信号被丢弃。加权向量是大小为  $M$  的特征矩阵的第  $N$  列,其中第  $N$  个分支的 SNR 最大。

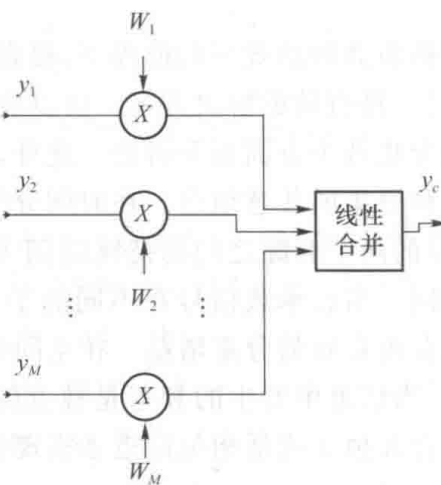


图 2-1 线性合并方案的简单框图

表 2-1 四种组合方法之间的比较

方法	是否需要 CSI	中断概率 $F(x)$	应用
SC	不需要	$F(x) [1 - e^{-\frac{x}{y_c}}]^M$	无约束
MRC	需要	$1 - e^{-\frac{x}{y_c}} \sum_{k=0}^{M-1} \frac{1}{k!} \left(\frac{x}{y_c}\right)^k$	无约束
EGC	需要	时无闭式解 $M > 2$	无约束
SLC	不需要		FSK 或 DS-CDMA

SC 方案不需要除了 SNR 之外的任何信道信息。而 MRC 和 EGC 方案需要信道状态信息(the Channel State Information, CSI)或其中的一部分信息(如信道包络、相位或延迟等)。MRC 方案根据接收信号的可靠性对其进行加权。可靠性较高的信号权重重大,可靠性较低的信号权重小。同时,该方案对信道相位失真进行补偿,随后在将信号对齐后进行合并。EGC 方案可以看成是 MRC 的简化版。在 MRC 中,信号的权重相等。随后 MRC 会先进行对齐,再进行相干合并。在实际工作中,不同分支处的相位常常是不能估计的。所以,EGC 和 MRC

方案不能被采用。在这种情况下,我们可以采用平方律合并来获得空间分集,从而不需要相位估计。与线性合并方案不同,SLC 方案只能应用于保留某种正交性的调制方案,包括频移键控或直接序列 CDMA<sup>[2-3]</sup>。

### 2.1.2 发射分集

发射分集的主要思想是通过在多个发射天线上发送冗余信号来提供分集和/或编码增益。而空间多路复用是在其中发送独立的比特序列。为了允许在接收机处进行相干检测,通常在发射机没有信道知识的情况下,在传输之前对信号进行适当的预处理。对于发射分集,仅在发射机侧需要多个天线,而多个接收天线是可选的。但是它们可以用来进一步提高性能。例如,在蜂窝网络中,总数据流量的主要部分通常发生在下行链路中。因此,为了增强关键下行链路,采用传输分集技术非常有吸引力。其原因在于那时仅在基站需要多个天线。

传输分集方案是在早期的两篇论文中提出的。这两篇论文独立地提出了一种称为延迟分集的简单技术<sup>[4-5]</sup>。但发射分集的价值直到 1998 年才得到认可。当时 Alamouti 提出了一种用于两个发射天线的简单技术<sup>[6]</sup>。同年, Tarokh、Seshadri 和 Calderbank 提出了他们的空时网格码<sup>[7]</sup>,这是具有多个发射天线的系统的二维编码方案。尽管延迟分集和 Alamouti 的发射分集方案仅提供了分集增益,但空时网格码既产生了分集增益又产生了额外的编码增益。对于发射分集也可以做类似 2.1.1 节中的分析。为了隔离发射分集的影响,我们考虑一个带有天线的发射机和一个带有单天线的接收机的情况。这样的系统也被称为 MISO 系统。目前假设发射机没有信道的知识。对于这种情况,最佳的功率分配方案是在天线之间平均分配功率。此外,在该情况下,各种信号的功率可以在接收机上再次相加。这些信号只携带  $1/N_{TX}$  的功率,其中  $N_{TX}$  为传输天线的数量。因此,容量为

$$C = \log_2 \left( 1 + \rho \left( \frac{\|h_1\|^2}{N_{TX}} + \dots + \frac{\|h_{N_{TX}}\|^2}{N_{TX}} \right) \right) \quad (2-3)$$

式(2-3)可近似为式(2-4):

$$C = \log_2 (1 + \rho \|h_{avg}\|^2) \quad (2-4)$$

这意味着发射分集不提供从接收分集中获得的增益,至少在没有发射机上的信道信息时不提供。即使近似表达式(2-4)没有显示出改进,但发射分集确实提供了增益效果,尽管比接收分集的阶数小。相同的数据现通过多条独立路径到达接收机,因此衰减的影响在一定程度上被平均化。丢失信号的概率随不相关传输路径数量的增多呈指数级下降。因此,接收到的信号在一定程度上会降低。与单输入单输出(Single-Input Single-Output, SISO)系统相比,在任何一条多路径上都容易受到衰落的影响。

接下来,本节讲介绍两种空时编码及循环延迟分集,如表 2-2 所示。

表 2-2 Alamouti 和广义复时空码的比较

空时编码	T <sub>x</sub> 天线数量	传输符号数量 $l$	使用时隙的数量 $m$	T <sub>x</sub> 矩阵的正交性	Rate= $l/m$
<b>S</b>	2	2	2	空间+时间	1
<b>G<sub>3</sub></b>	3	4	8	时间	1/2

(1) 复杂正交空时编码

对于这种类型的空时编码,必须满足以下三个条件,即正方形传输矩阵、统一码率和传输矩阵在时空域的正交性。其中,正方形传输矩阵是指发射天线数量等于已使用的时隙数,统一码率是指使用的时隙数等于传输符号数,传输矩阵在时空域的正交性是指  $\mathbf{S}\mathbf{S}^H = \mathbf{S}^H\mathbf{S}$ , 其中  $\mathbf{S}^H$  为  $\mathbf{S}$  的共轭转置。Alamouti 码是最简单的复杂正交时空码。它使用两个发射天线和一个接收天线。此外,Alamouti 方案要求在两个时隙内,衰落信道包络线保持不变。

图 2-2 为采用 QPSK 调制的 Alamouti 方案的编码过程实例<sup>[6,8]</sup>。图 2-3 显示了用于解码接收的组合符号的接收机结构。

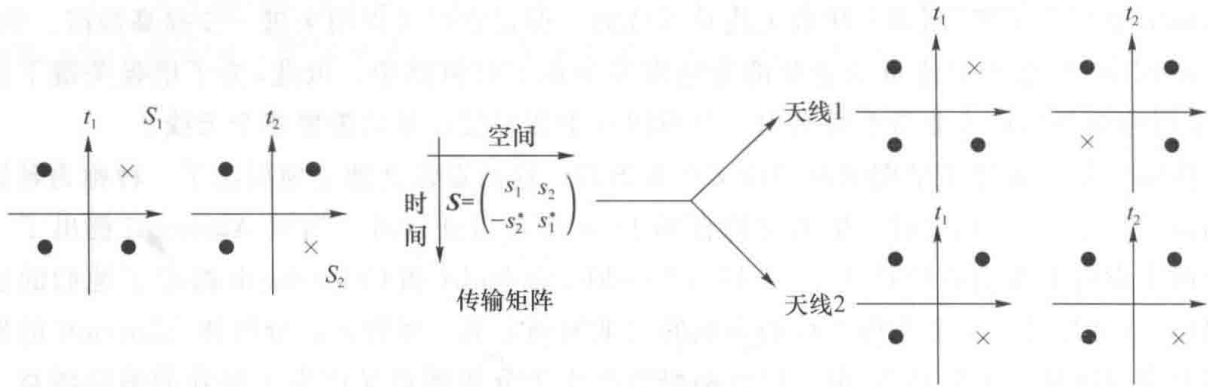


图 2-2 采用 QPSK 调制的 Alamouti 方案的编码过程实例

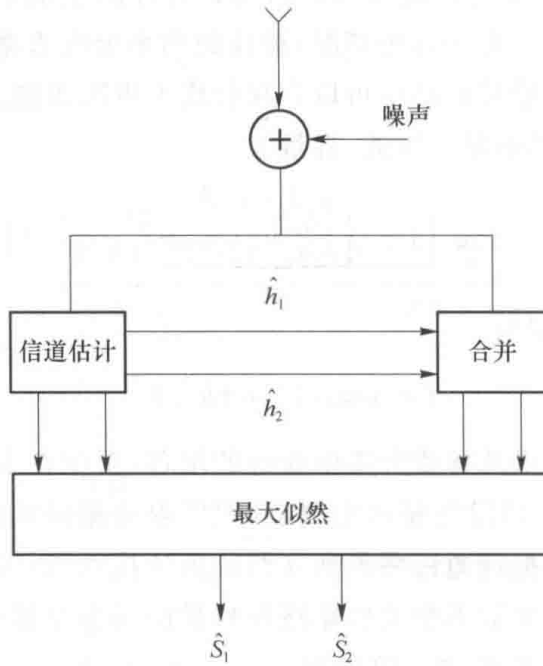


图 2-3 Alamouti 码的接收机

式(2-5)表示在接收机上所接收到的信号。

$$\begin{pmatrix} y_1 \\ y_2^* \end{pmatrix} = \begin{pmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2^* \end{pmatrix} \quad (2-5)$$

线性组合器将接收到的符号乘以信道矩阵的 Hermitian 转置。为了简单,此处认为信道是完全估计的。则线性组合器的输出如下:

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = (h_1^2 + h_2^2) \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} + \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \quad (2-6)$$

随后,最大似然解码器被应用以得到传输的符号。可以看出,接收机的简单性是由于传输矩阵的时空正交性。Tarokh 等人在文献[9]中提出了一种使用 4 或 8 根天线的复杂正交时空码。

### (2) 广义复正交空时编码

对于超过两根天线的空时编码的寻找工作是由 Tarokh、Jafarkhani 和 Calderbank 开始的。他们建立了广义复正交设计理论的基础。广义复正交空时编码与 Alamouti 码的区别主要有三点。首先,广义复正交空时编码为非正方形传输矩阵。也就是说,第一,使用的时隙数不等于 Tx 天线数;第二,其为小码率,即传输符号数小于使用的时隙数;第三,传输矩阵的正交性仅在时间意义上得到保证。这些特点降低了频谱效率,增加了信道应恒定的时隙数。

具有 3 根天线、4 个传输符号和 8 个使用时隙的广义复正交空时编码的传输矩阵如 A 式(2-7)所示。

$$\mathbf{G}_3 = \begin{pmatrix} s_1 & s_2 & s_3 \\ -s_2 & s_1 & -s_4 \\ -s_3 & s_4 & s_1 \\ -s_4 & -s_3 & s_2 \\ s_1^* & s_2^* & s_3^* \\ -s_2^* & s_1^* & -s_4^* \\ -s_3^* & s_4^* & s_1^* \\ -s_4^* & -s_3^* & s_2^* \end{pmatrix} \quad (2-7)$$

### (3) 循环延迟分集(Cyclic Delay Diversity, CDD)

CDD 是一种非常简单的发射分集方案。CDD 可以通过选择适当的发射延迟来实现发射人工频率分集。在这种方法中,通过基于频域信道响应的调度得到的多用户分集,可以通过调整时延传播来改善。其中,时延传播是通过控制依赖于信道条件的时延值来实现的<sup>[10-11]</sup>。

## 2.2 空间复用技术

在无线通信系统中,使用多天线可以获得三种类型的基本增益:复用增益、分集增益和天线增益。在本节中,我们将主要关注复用增益。

具有  $M$  个发射天线和  $N$  个接收天线的 MIMO 系统的容量随着  $M$  和  $N$  的最小值线性增长<sup>[12-13]</sup>,这是一个有趣的结果。对于单天线系统,给定固定带宽,通过增加发射功率,容量只能与 SNR 呈对数关系增加。在文献[14]中,MIMO 系统的理论容量结果得到了贝尔实验室分层空时(Bell Labs Layered Space-Time, BLAST)方案的建议补充,该方案被证明可以实现接近中断容量为 90% 的比特率。与理论容量结果类似,当增加天线元件的数量时,BLAST 方案的比特率也随之线性增长。第一个实时 BLAST 演示器配备了 8 个发射天线和 12 个接收天线<sup>[15]</sup>。在富散射的室内环境中,它达到了每赫兹带宽高达每秒 40 bit 的比特率。这种规模的无线频谱效率是前所未有的,任何单天线系统都无法实现。