国防电子信息技术丛书

Modern Communications Jamming Principles and Techniques

Second Edition

现代通信干扰原理与技术（第2版）

[美] Richard A. Poisel 著

楼才义 王国宏 张春磊 等译

杨小牛 审校

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

国防电子信息技术丛书

现代通信干扰原理与技术

（第2版）

Modern Communications Jamming Principles and Techniques
（Second Edition）

[美] Richard A. Poisel 著

楼才义 王国宏 张春磊 等译

杨小牛 审校

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

本书是一本专门针对系统设计和分析实际问题提供有用、注重实效的解决方案的专业图书。其在第 1 版原有内容的基础上，增加了城市环境中的信号传播、信号检测、CDMA 盲估计、UWB 信号检测与干扰等新内容。全书系统介绍了现代通信，包括跳频、直接序列扩频、CDMA、UWB 等干扰技术，给出了详细的理论分析及其仿真结果。另外，书中有大量的数学公式，但推导很少，同时省略了定理证明。

本书对从事信息对抗尤其是通信对抗领域研究的院校师生和工程技术人员是一本难得的参考书，同时对从事现代军事通信研究的技术人员也有重要参考价值。

版权贸易合同登记号　图字：01-2012-7679

图书在版编目（CIP）数据

现代通信干扰原理与技术：第 2 版/（美）泊伊泽（Poisel,R.A.）著；楼才义等译. —北京：电子工业出版社，2014.9
（国防电子信息技术丛书）

书名原文: Modern Communications Jamming Principles and Techniques，Second Edition

ISBN 978-7-121-24145-1

Ⅰ. ①现…　Ⅱ. ①泊…　②楼…　Ⅲ. ①通信干扰　Ⅳ. ①TN975

中国版本图书馆 CIP 数据核字（2014）第 192703 号

责任编辑：竺南直　　特约编辑：郭　莉
印　　刷：涿州市京南印刷厂
装　　订：涿州市京南印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×1092　1/16　印张：33.75　字数：908 千字
版　　次：2005 年 6 月第 1 版
　　2014 年 9 月第 2 版
印　　次：2014 年 9 月第 1 次印刷
定　　价：79.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010)88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：(010)88258888。

第 2 版译者序

通信技术的发展是现代文明的重要标志。然而在军事领域，从通信技术诞生之日起，就产生了通信干扰与抗干扰、通信截获与抗截获、通信侦收与抗侦收的矛与盾的对抗，并由此产生了通信对抗也叫通信电子战这一崭新的专业技术领域。从 1905 年的日俄战争，日本联合舰队依靠无线电监听和通信干扰手段成功击败俄军，到 2013 年斯诺登暴露的美国监听门事件（到本书翻译出版时，这一事件的余波尚未平息），无论在战争年代，还是在和平时期，通信对抗（侦察、测向定位、干扰）就一直伴随时代变迁。随着通信与通信对抗的不断斗争较量，军事通信技术得到了长足发展，从常规定频通信发展到了跳频通信、扩频通信等各种现代通信抗干扰体制，通信对抗因此面临重大挑战。

如何对抗跳频、扩频等新型现代通信抗干扰体制是通信对抗领域最近一二十年研究的热点、重点，也是难点。值得高兴的是 2004 年国外 Arttech House Inc.公司出版了由著名通信电子战专家 Richard A. Poisel 博士的专著《Modern Communications Jamming Principles and Techniques》（第 1 版），该专著系统讨论了以跳频和扩频为代表的现代通信体制的干扰原理和技术，在电子工业出版社的大力支持下，我们于 2005 年及时组织人员进行了翻译出版，得到了通信对抗领域专家学者和院校师生的好评。然而，近十多年，现代战争形态已向以反恐为主的城市巷战转变，致使对个人移动通信系统的对抗成为反恐作战的重要方面。面对这一变化，Richard A. Poisel 博士又于 2011 年出版了《Modern Communications Jamming Principles and Techniques》（第 2 版），在第一版原有内容的基础上，又增加了城市环境中的信号传播、信号检测、CDMA 盲估计、UWB 信号检测与干扰等新内容。鉴于这些新增内容的新颖性、实用性，以及对现代反恐作战的重要意义，同时考虑到为了纠正我们在第 1 版翻译时存在的错误和不足，经与出版社沟通协商，我们又组织专业技术人员对第 2 版进行了认真翻译，并正式出版。

本译著由楼才义、王国宏、张春磊为主翻译，李新付、章军、郑仕链、华军、陈鼎鼎、陈良文、唐秀玲、金文敏等参与了部分章节的翻译工作，杨小牛院士负责全书审校。电子工业出版社竺南直博士为本书的出版付出了辛勤的劳动，在此表示诚挚的感谢。

由于译者水平有限，对书中的有些术语难免把握不准，翻译不到位，可能会给读者带来误导，敬请读者批评指正。

译者于嘉兴

2014 年 5 月

目　录

第1章　现代通信和电子对抗

1.1　引言

信息时代的到来使我们越来越依赖于无线电通信。虽然便携式电话系统和个人通信系统使无线电通信得到了广泛的应用，但无疑军事领域对于无线通信的依赖更大。多年来，军事部门一直都依赖无线通信来实施战术部队的指挥控制。

由于战术指挥员使用无线通信来实施对其部队的控制，因此敌人对其通信就特别感兴趣。其主要体现在两个方面：（1）截获他们发出的信息；（2）阻止信息在发送者和接收者之间成功交换。前者向截获者提供关于其敌对方的状态和意图信息，这些信息称作情报或战斗信息。情报与战斗信息两者之间的区别在于这些信息的用途不同，但这不是本书讨论的重点。后者是本书讨论的主题。

1.2　电子战

通信电子战（EW）是指为完成截获或阻止通信所采取的各种行动的总称。它主要包括三个部分：

- 电子攻击（EA）；
- 电子支援（ES）；
- 电子防护（EP）。

电子攻击是电子对抗（ECM）的新名称。它使用有源信号阻止通信系统有效交换信息。目前大家普遍认为（但不排除其他观点），电子攻击主要包括三种活动：（1）干扰；（2）欺骗；（3）定向能（DE）。

根据信息的三个主要原则：相关性、精确性和适时性[1]，干扰主要针对最后一个原则——适时性。如果信息成功交换，那么干扰就几乎不能直接影响信息的相关性和精确性。但是，干扰活动能够通过降低交换速度暂时影响信息交换的适时性。干扰还能够影响信息的相关性，因为如果信息到达期望目的地太迟而不能使用，那么这些信息就变得不相关了。

欺骗针对信息的第二个原则——精确性，其意图是通过设计陷阱误导对手。伪造通信信号是任何战术欺骗活动的重要组成部分。这里不对欺骗做详细介绍，因为欺骗本身就是一个范围非常广的主题。

定向能的应用类似于干扰，但它以永久损害或摧毁通信设备为目标。它需要比干扰大得多的能量和功率。

电子支援是对电子攻击的一种支撑功能。它用于测量无线电信号的参数，以确定信号是否出现（检测）或确定其特征。如果针对不存在的信号进行干扰，那就是浪费能量和时间。

电子防护是为阻止敌人对友军通信实施电子攻击和电子支援所采取的行动。电子防护的一个例子是掩蔽友军通信，挫败敌人对友军通信进行电子支援（侦察）的企图。通过向着敌人而远离友军通信网络发射信号，而且信号频率和频段都与友军使用的相同，能够阻止敌人有效地实现其电子支援（侦察）企图。电子防护的其他例子还有发射控制（Emission Control，EMCON）和加密。

关于电子防护的这种描述显然是针对通信的，还有其他形式的电子防护——飞机自卫设（Aircraft Self-protect Equipment，ASE）。比如，使用雷达检测或其他形式的传感器来确定飞机是否正被瞄准，就是一种形式的电子防护。本书不讨论这种应用。

问题自然就提出来了：当使用了抗干扰通信技术时，通信干扰如何才能很好地阻止信息传输？这就是本书讨论的主题。从20世纪80年代开始公开出版了一些关于通信抗干扰技术的文献。在此之前，美国国防部在该技术领域的绝大部分投资都是保密的和不公开的。

我们主要讨论可应用EW的RF层——即所谓的ISO数据链路模型的第0层，也被称为物理层。在该层上，EW通过把选定的信号注入到通信系统来阻止信号接收，以防止其精确地接收预期的信息。

1.3　抗干扰通信

无论是为了截获通信还是阻断通信，从敌对关系来看，其目的显然都是为了阻止成功通信。“抗干扰”通信技术是在敌人有意降低和中断通信机的通信能力时，为保证通信畅通而开发的。这种技术还有助于抗截获，但这不是本书讨论的主题。

至今已经出版了多本关于抗干扰通信技术和系统的书籍。但这些文献的主题都是如何设计通信系统来挫败对抗技术，即存在有意干扰情况下如何进行通信。而本书的重点恰好相反，它讨论的是当所需要干扰目标采用了抗干扰技术时，如何对其实施有效干扰。这两种情况所遵循的基本物理原理是一样的，只是它们使用技术的目的不同而已。

为开发防止通信被中断的各种方法已付出了很大努力——特别是针对有意干扰。当目的完全是防止被截获或检测时，那么这些技术被称为低截获概率（Low Probability of Intercept，LPI）技术或类似的称呼。而当目的是存在有意扰乱（干扰）的情况下也要确保通信时，那么该技术称为抗干扰（Anti-jam，AJ）技术。

阻止敌方战术行动的方法之一是通过实施电子对抗来阻断网络通信，在这里就是使用通信干扰。这种干扰是通过在敌方网络工作的频率上向其通信接收机辐射能量来实现的。

本书的大多数例子和具体讨论都以地面移动通信为基础，其结果可广泛应用于美国陆军和海军陆战队的军事行动中。但是这里讨论的技术都是一些基本技术，可以应用于所有军种，准确地说，可以应用于使用无线通信的所有军种。当然，抗干扰电子对抗（AJ ECM）的讨论结果同样可以应用于商业通信场合。特别地，许多讨论都可以直接应用于前面提到的便携式电话和个人通信系统。显然，在军事作战中，我们的敌人经常会利用商业通信手段进行指挥控制[2,3]。

1.4　网络

军用战术指挥控制通常借助无线通信来实现。这些通信一般构成网络形式，称为通信网，这样许多节点就可以根据需要互相通信。这些网络一般都是预先配置好的，网络中的每个成员都知道网络中的其他成员。如果这些通信被有意干扰或被其他方法阻断，那么指挥控制过程就会中断，作战就会受到影响。

现在使用的有几种网络形式。一种是战术无线多对多网络，如图1.1所示。这是一种典型的战术一键通（PTT，*push-to-talk*）网络，网络中的所有人员都可以互相通信。还有一种是一对多/多对一网络，如图1.2所示，这种配置的典型示例就是甚小口径卫星（Very Small Aperturesatellite，VSAT）网络，其中一个节点作为网络中心。最后一种是一对一网络，如图1.3所示。这种网络的典型代表是便携式电话、个人通信系统（Personal Communication Systems，PCS）和老式的公用电话交换网（Public Switched Telephone Network，PSTN）。在这种网络中，所有节点都能互相通信，但一般每次只有两个节点进行通信。所有这些形式的网络都很容易受到干扰。

当用现代术语讨论网络时，显然必须包括众所周知的网络：互联网。它几乎存在于全世界的任何角落且正被数十亿人们应用着。互联网并不遵循上述模型，但像多对多通信（见图 1.4）一样，可在任何个人之间提供通信。本书将讨论互联网通信的几个方面。

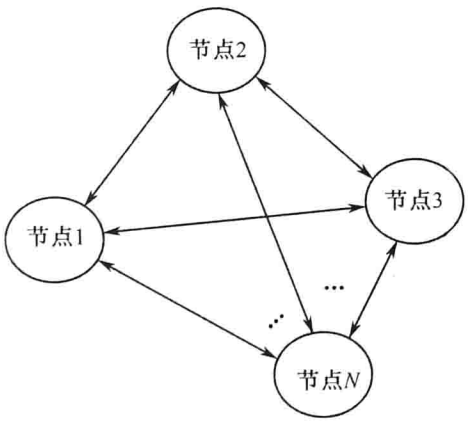

图 1.1　多对多配置的战术无线通信网络

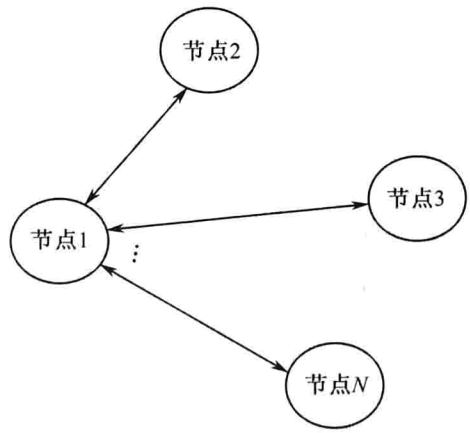

图 1.2　一对多和多对一网络，如VSAT网络

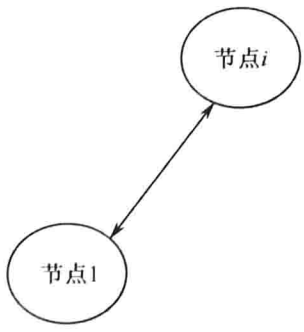

图 1.3　一对一网络

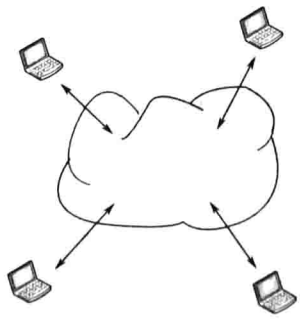

图 1.4　互联网连通性

1.5 扩频技术

扩频通信技术最初是由美国国防部开发的，用来防止敌方的检测、利用和对抗。这些通信技术迅速从纯粹的军事领域应用扩展到商业通信应用中。扩频通信技术应用的一个例子是码分多址（CDMA）扩频（SS）。另一个例子是使用频率跳变来达到频率分集（diversity）。扩频技术在商业通信中的应用将使这些能力在未来很长时间内得到普及。

扩频通信是为通信机提供一定程度的反电子对抗(Electronic Counter-Countermeasures，ECCM)能力（假定干扰是一种电子对抗技术）而开发的一种通信技术。它是一种低截获概率、低利用概率（Low Probability of Exploitation，LPE）和抗干扰技术。传统的单音干扰机对这些系统的性能几乎不会产生任何影响，迫使干扰方采用不同的攻击策略。至少必须关注干扰机需要具备更宽的干扰带宽。

直接序列扩频技术的优点之一是能够重复使用频谱，对商业无线通信同样如此。这种通信技术在频域上互相重叠，允许多个用户共用同样的频率。在 CDMA 中每个用户都可方便地使用不同编码来扩展其波形。

对干扰技术和策略的分析与成功通信技术的分析在一些细微方面存在差别。最大的不同是误比特率（BER）的分析方式不同。通信策略专家强调的是使通信的误比特率低于 10^{-3}（平均每 1000 比特出现 1 比特错误），并且开发误比特率低于 10^{-3} 的各种通信技术。电子对抗技术则试图将误比特率提高到 10^{-1} 甚至更高，研究提高误比特率的通信对抗有效策略。本书的第 3 章将证明，如果能将误比特率提高到 10^{-1}，那么干扰机就能够成功对抗抗干扰目标（AJ）。

严格地说，抗干扰通信技术指的是通信系统抗击通信干扰的能力。在无线通信环境中完全不受射频干扰的影响是不切实际的。只要具备合适的前提条件，所有射频系统都可能被干扰。实现抗干扰的通用技术包括隐藏信号的技术、在频谱上快速移动信号的技术和数字信号冗余编码技术。隐藏信号使截获者或无意闯入者不知道该信号的存在，信号在频谱上快速移动，使传统窄带截获接收机收不到该信号。数字信号冗余编码技术最初不是用于反干扰的，而是用于对付噪声对数字信号影响的。如果干扰信号与热噪声相类似，那么这类技术也可以有效地抗干扰。

扩展频谱技术是我们将要讨论的所有现代通信技术的基础。这里只对频谱扩展方法和技术做简要介绍，详细内容将在后面几章讨论。

1.5.1 低检测概率

低检测概率（Low Probability of Detection，LPD）系统的目标是以某种方式隐藏信号，以便非预期的接收机难以发现该信号的存在。有许多潜在的理由要求这样做。在军用环境中，可能是期望能够与一个没有任何人知道驻守着部队的特定城市进行通信。直接序列扩频就是一种低检测概率技术。

1.5.2 低截获概率

顾名思义，如果信号不能做到低检测概率，那么非预期的接收机就能检测到该信号的存在。但即使这样，也仍然能够为该信号提供一些保护。可以使信号很难被截获，这种情况下，信号就被认为是低截获概率的。后面要介绍的跳频就是一种低截获概率技术。

第 1 章　现代通信和电子对抗

1.1　引言

信息时代的到来使我们越来越依赖于无线电通信。虽然便携式电话系统和个人通信系统使无线电通信得到了广泛的应用，但无疑军事领域对于无线通信的依赖更大。多年来，军事部门一直都依赖无线通信来实施战术部队的指挥控制。

由于战术指挥员使用无线通信来实施对其部队的控制，因此敌人对其通信就特别感兴趣。其主要体现在两个方面：（1）截获他们发出的信息；（2）阻止信息在发送者和接收者之间成功交换。前者向截获者提供关于其敌对方的状态和意图信息，这些信息称作情报或战斗信息。情报与战斗信息两者之间的区别在于这些信息的用途不同，但这不是本书讨论的重点。后者是本书讨论的主题。

1.2　电子战

通信电子战（EW）是指为完成截获或阻止通信所采取的各种行动的总称。它主要包括三个部分：

- 电子攻击（EA）；
- 电子支援（ES）；
- 电子防护（EP）。

电子攻击是电子对抗（ECM）的新名称。它使用有源信号阻止通信系统有效交换信息。目前大家普遍认为（但不排除其他观点），电子攻击主要包括三种活动：（1）干扰；（2）欺骗；（3）定向能（DE）。

根据信息的三个主要原则：相关性、精确性和适时性[1]，干扰主要针对最后一个原则——适时性。如果信息成功交换，那么干扰就几乎不能直接影响信息的相关性和精确性。但是，干扰活动能够通过降低交换速度暂时影响信息交换的适时性。干扰还能够影响信息的相关性，因为如果信息到达期望目的地太迟而不能使用，那么这些信息就变得不相关了。

欺骗针对信息的第二个原则——精确性，其意图是通过设计陷阱误导对手。伪造通信信号是任何战术欺骗活动的重要组成部分。这里不对欺骗做详细介绍，因为欺骗本身就是一个范围非常广的主题。

定向能的应用类似于干扰，但它以永久损害或摧毁通信设备为目标。它需要比干扰大得多的能量和功率。

而如果每个数据比特需要多跳，它就叫做快跳频。在慢跳频系统中，每跳发送的数据比特数用L_S表示，快跳频系统中每发送一个数据比特跳频的次数用L_F表示。SFHSS和FFHSS的划分界线是每跳比特数，或等价地，每比特跳数。

跳频扩频具有频率分集的优点。由于信号从发射机到接收机的多条可能传播路径会造成衰减，在不同频率上传输同样的信息提高了信息到达接收机的正确概率。这种衰减与频率相关，如果发射机或接收机正在移动，那么衰减将会随运动而发生变化。

数字跳频通信系统一般使用频移键控（FSK）调制方式，特别地，在接收机端采用非相干检测时则采用二进制频移键控（BFSK）调制。在二进制频移键控中，一个数据比特以发射两个单音中的某一个来表示。这些单音通常比载频高或低一定的量，换句话说，频谱位置不断变化[5]。第3章讨论FSK和其他调制技术。

1.6.3 跳时

在条件比较宽泛时，检测扩频信号的最佳方法是采用辐射计。该装置在一段时间内测量辐射计覆盖带宽内的能量，这段时间叫做积分时间。在该时间段结束时，辐射计会确定发送的是一个传号还是发送一个空号。跳时技术将随机改变传输的时间，从而使辐射计在大部分时间上测量到的都是噪声。

从简化原理上说，军事上多年来使用的常规一键通（PTT）通信就是一种跳时形式，因为网络上各次传输之间的时间是随机的。试图收听这些通信的接收机调谐到该网络的频率时，在大部分时间上收听到的都是噪声。

现代通信系统设计的一种形式——超宽带（ultrawideband， UWB）通信，就是利用跳时技术来实现抗干扰保护的。它与直接序列扩频和跳频扩频一样，也允许多个用户共享同样的频谱。虽然这种技术的应用并不限于短距离网络通信，但在写作本书时，该技术的主要应用领域为短距离网络通信。要适用于足够的距离，则需要相当大的辐射功率。超宽带技术将信号扩展到更宽的带宽上，这可能会与同一频谱中的其他类型通信互相干扰。

1.6.4 混合体制

组合抗干扰技术可以并且已经在使用，以利用各种技术的优点。最常用的混合体制是将直接序列扩频与跳频扩频结合起来。在这种组合中，直接序列扩频的隐蔽特性和跳频扩频的频率分集特性都能够被利用。基带数字信号首先利用直接序列扩频技术形成一个（相对）宽带的信号，然后该信号使用跳频频率集中的频率进行跳频。这样的信号很难检测，比单独采用任何一种调制技术进行通信都更可靠。

1.7 同步

根据战术军事通信的特征，适应无线电台动态入网和脱网非常必要。即使网络的标准组成部分已经提前建立网络，也必须使新节点能够加入网络。这对自组织或所谓的“ad hoc”网络特别重要，这些网络的设计要方便网络参与者动态加入或离开。另外，战术网络上的通信是断

断续续的。没有交互时，振荡器会发生偏差。因此，同步是这些网络中需要解决的一个重要问题。对于非扩频网络来说，这并不困难。当没有其他发射机使用某信道时，一个发射机每次只在指定的频率上传输。但是，对于跳频扩频网络来说，新加入的发射机一般不知道网络在该时刻正在使用的频率；对于直接序列扩频网络来说，新加入的发射机不知道网络所处的扩频序列的相位。这就给此类网络提出了一些特殊要求，而这些要求在非扩频通信中是不存在的。

1.8　通信系统模型

这里所用的带干扰机的通信系统模型如图 1.5 所示。来自发射机的信号通过大气传播至期望的接收机，同样也到达了干扰机的 ES 系统接收机（如果有的话）。信号被热噪声或其他干扰所扰乱，这对两条传播路径而言其结果可能不一样（事实上，绝大多数情况下是不一样的）。在期望接收机处，信号通过处理以获取由发射机发送的信息。在干扰机处，接收的信号通过几种途径进行处理，然后干扰机向通信接收机方向发射信号，试图阻止接收机精确地获取信息。

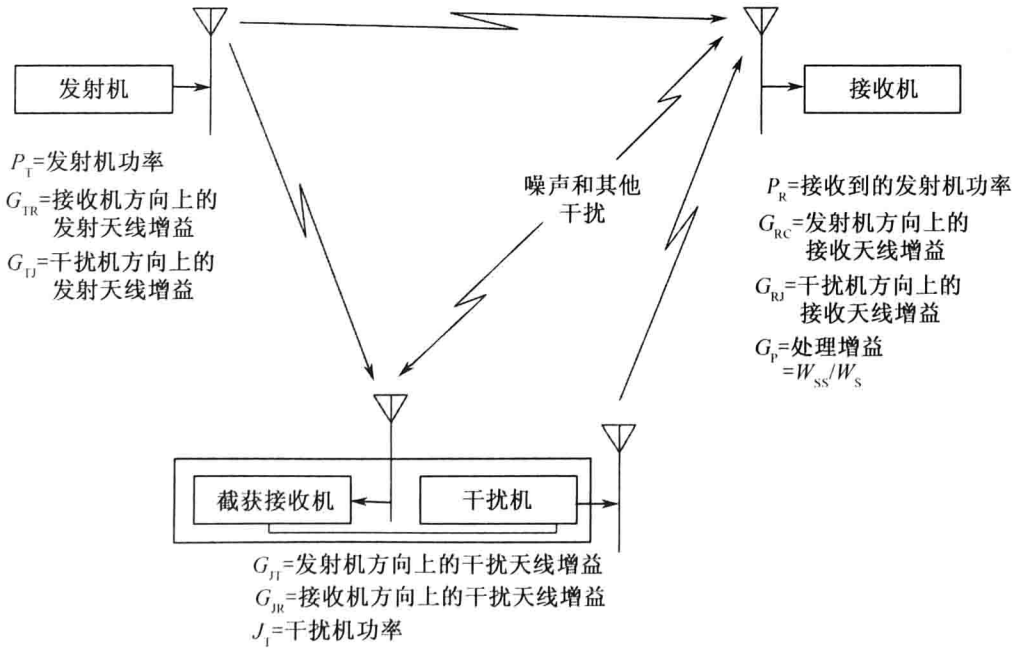

图 1.5　通信系统模型

干扰机希望扰乱接收机，而不是发射机。这样，干扰机必须掌握接收机的部署位置。在以网络为主要通信手段的战术通信环境中，一般每个节点要在某个时间段内至少发射一次，这些发射信号被截获和定位后就提供了接收机的位置信息。