过增加它的传输功率来降低接收到差错帧的概率。然而，注意到当该功率超过某个阈值时，如 BER 从 10^{-12} 降低到 10^{-13}，可证明几乎不会有实际增益。增加传输功率也会伴随着一些缺点：发送方必须消耗更多的能量（对于用电池供电的移动用户，这一点非常重要），并且发送方的传输更可能干扰另一个发送方的传输（参见图 7-4b）。

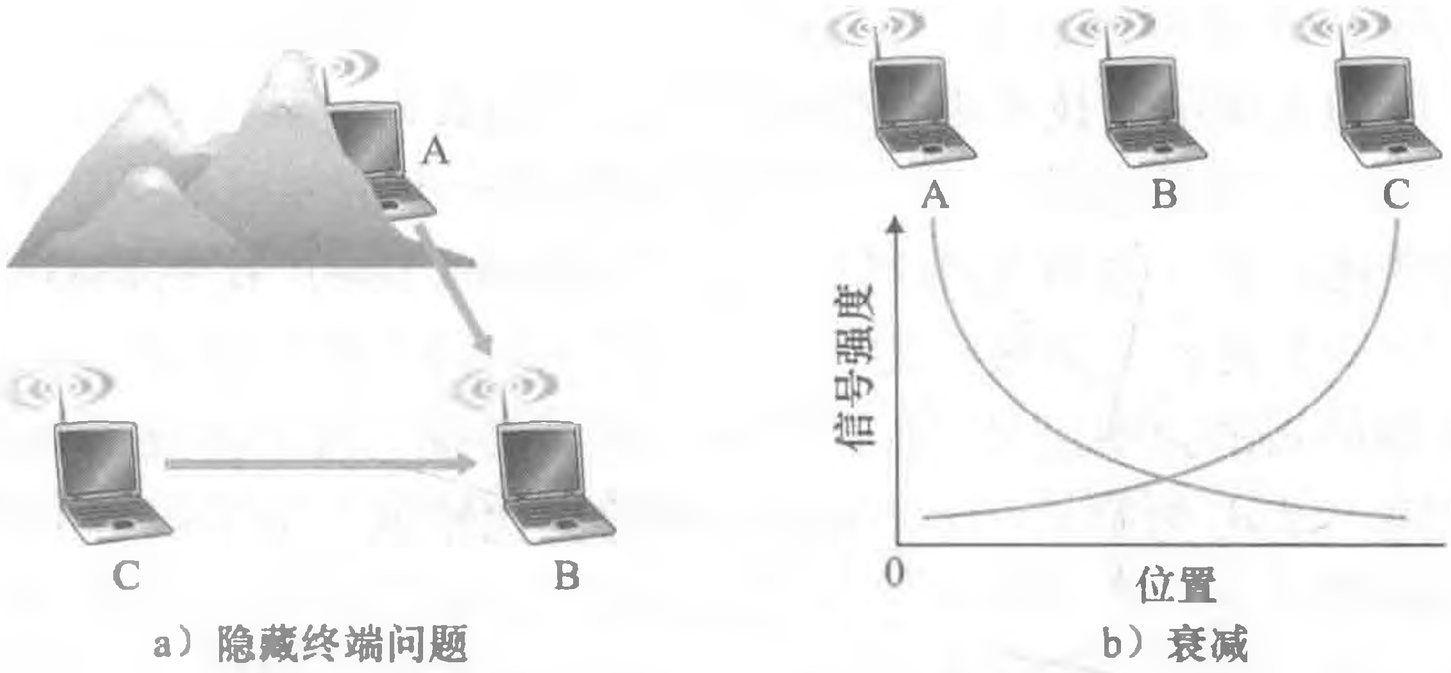


图 7-4　隐藏终端问题和衰减

- 对于给定的 SNR，具有较高比特传输率的调制技术（无论差错与否）将具有较高的 BER。例如在图 7-3 中，对于 10dB 的 SNR，具有 1Mbps 传输速率的 BPSK 调制具有小于 10^{-7} 的 BER，而具有 4Mbps 传输速率的 QAM 16 调制，BER 是 10^{-1}，该值太高而没有实际用处。然而，具有 20dB 的 SNR，QAM 16 调制具有 4Mbps 的传输速率和 10^{-7} 的 BER，而 BPSK 调制具有仅 1Mbps 的传输速率和一个低得“无法在图上表示”的 BER。如果人们能够容忍 10^{-7} 的 BER，在这种情况下由 QAM 16 提供的较高的传输速率将使它成为首选的调制技术。这些考虑引出了我们下面描述的最后一个特征。
- 物理层调制技术的动态选择能用于适配对信道条件的调制技术。SNR（因此 BER）可能因移动性或由于环境中的改变而变化。在蜂窝数据系统中以及在 802.11 WiFi 和 4G 蜂窝数据网络中（我们将在 7.3 节和 7.4 节中学习）使用了自适应调制和编码。例如，这使得对于给定的信道特征选择一种调制技术，在受制于 BER 约束的前提下提供最高的可能传输速率。

有线和无线链路之间的差异并非仅仅只有较高的、时变的误比特率这一项。前面讲过在有线广播链路中所有节点能够接收到所有其他节点的传输。而在无线链路中，情况并非如此简单。如图 7-4 所示，假设站点 A 正在向站点 B 发送，同时假定站点 C 也在向站点 B 传输。由于所谓的**隐藏终端问题**（hidden terminal problem），即使 A 和 C 的传输确实是在目的地 B 发生干扰，环境的物理阻挡（例如，一座大山或者一座建筑）也可能会妨碍 A 和 C 互相听到对方的传输。这种情况如图 7-4a 所示。第二种导致在接收方无法检测的碰撞情况是，当通过无线媒体传播时信号强度的**衰减**（fading）。图 7-4b 图示了这种情况，A 和 C 所处的位置使得它们的信号强度不足以使它们相互检测到对方的传输，然而它们的传输足以强到在站点 B 处相互干扰。正如我们将在 7.3 节看到的那样，隐藏终端问题和衰减使得多路访问在无线网络中的复杂性远高于在有线网络中的情况。

CDMA

在第6章讲过，当不同主机使用一个共享媒体通信时，需要有一个协议来保证多个发送方发送的信号不在接收方互相干扰。在第6章中，我们描述了3类媒体访问协议：信道划分、随机访问和轮流。码分多址（Code Division Multiple Access，CDMA）属于信道划分协议族。它在无线LAN和蜂窝技术中应用很广泛。由于CDMA对无线领域十分重要，在后面小节中对具体的无线接入技术进行探讨以前，我们首先对其快速地浏览一下。

在CDMA协议中，要发送的每个比特都通过乘以一个信号（编码）的比特来进行编码，这个信号的变化速率（通常称为**码片速率**，chipping rate）比初始数据比特序列的变化速率快得多。图7-5表示一个简单的、理想化的CDMA编码/解码情形。假设初始数据比特到达CDMA编码器的速率定义了时间单元；也就是说，每个要发送的初始数据比特需要1比特时隙时间。设 d_i 为第 i 个比特时隙中的数据比特值。为了数学上便利，我们把具有0值的数据比特表示为-1。每个比特时隙又进一步细分为 M 个微时隙；在图7-5中，$M=8$，不过在实际中 M 的值要大得多。发送方使用的CDMA编码由 M 个值的一个序列 c_m 组成，$m=1, \cdots, M$，每个取值为+1或者-1。在图7-5的例子中，被发送方使用的 M 比特的CDMA码是（1，1，1，-1，1，-1，-1，-1）。

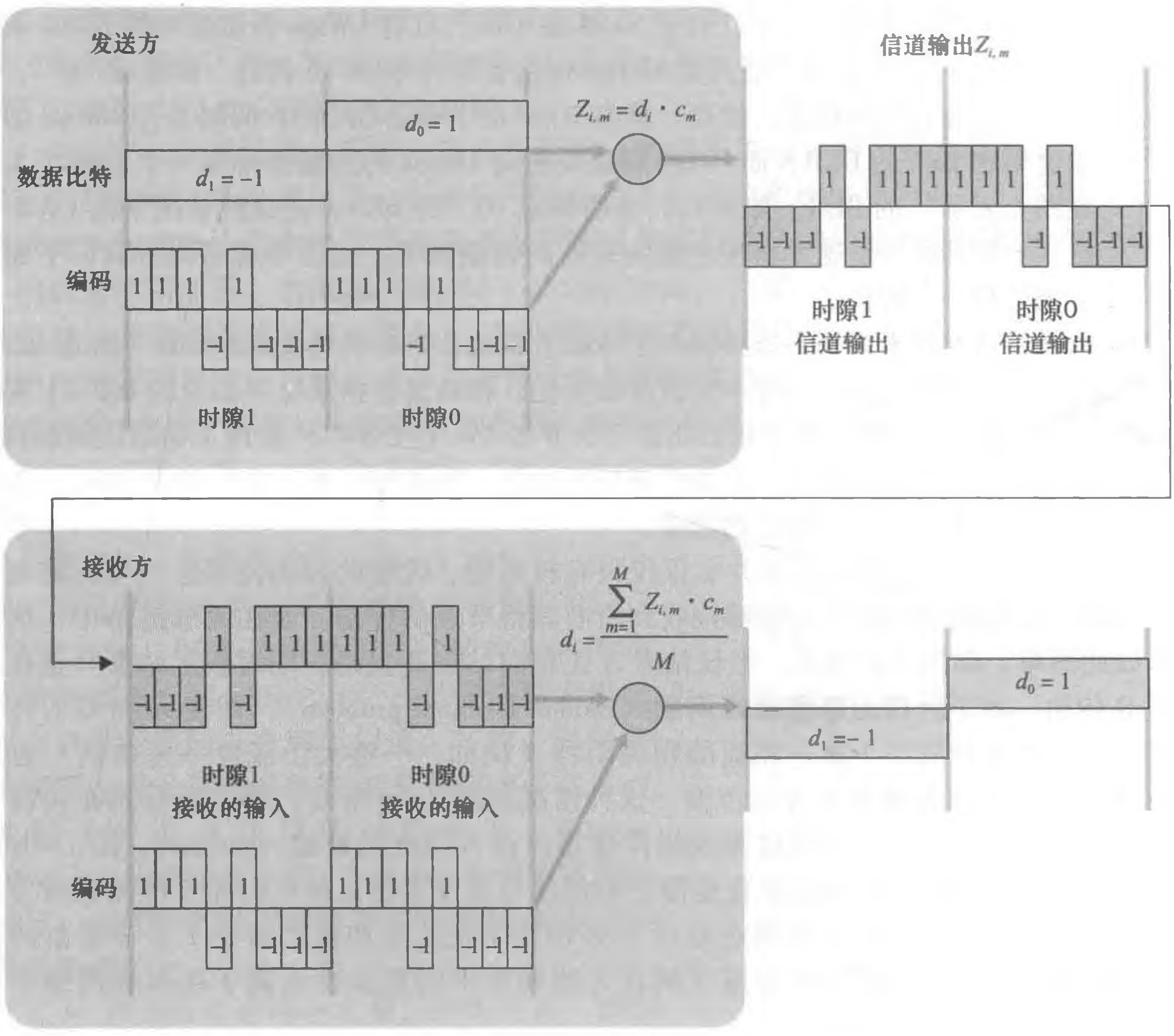


图7-5　一个简单的CDMA例子：发送方编码，接收方解码

为了说明 CDMA 的工作原理，我们关注第 i 个数据比特 d_i。对于 d_i 比特传输时间的第 m 个微时隙，CDMA 编码器的输出 $Z_{i,m}$ 是 d_i 乘以分配的 CDMA 编码的第 m 比特 c_m：

$$Z_{i,m} = d_i \cdot c_m \tag{7-1}$$

简单地说，对没有干扰的发送方，接收方将收到编码的比特 $Z_{i,m}$，并且恢复初始的数据比特 d_i，计算如下：

$$d_i = \frac{1}{M}\sum_{m=1}^{M} Z_{i,m} \cdot c_m \tag{7-2}$$

读者可能想通过推敲图 7-5 所示例子的细节，来明白使用式（7-2）在接收方确实正确恢复了初始数据比特。

然而，这个世界远不是理想化的，如上面所述，CDMA 必须在存在干扰发送方的情况下工作，这些发送方用分配的不同编码来编码和传输它们的数据。但是当一个发送方的数据比特和其他发送方发送的比特混在一起时，一个 CDMA 接收方怎样恢复该发送方的初始数据比特呢？CDMA 的工作有一种假设，即对干扰的传输比特信号是加性的，这意味着，例如在同一个微时隙中，如果 3 个发送端都发送 1，第 4 个发送端发送 -1，那么在那个微时隙中所有的接收方接收的信号都是 2（因为 1 +1 +1 -1 =2）。在存在多个发送方时，发送方 s 计算它编码后的传输 $Z^s_{i,m}$，计算方式与式（7-1）中的完全相同。然而在第 i 个比特时隙的第 m 个微时隙期间，接收方现在收到的值是在那个微时隙中从所有 N 个发送方传输的比特的总和：

$$Z^*_{i,m} = \sum_{s=1}^{N} Z^s_{i,m}$$

令人吃惊的是，如果仔细地选择发送方的编码，每个接收方只通过式（7-2）中的同样的方式使用发送方的编码，就能够从聚合的信号中恢复一个给定的发送方发送的数据：

$$d_i = \frac{1}{M}\sum_{m=1}^{M} Z^*_{i,m} \cdot c_m \tag{7-3}$$

如在图 7-6 中所示，描述了两个发送方的 CDMA 例子。上部的发送方使用的 M 比特 CDMA 编码是（1，1，1，-1，1，-1，-1，-1），而下部的发送方使用的 CDMA 编码是（1，-1，1，1，1，-1，1，1）。图 7-6 描述了一个接收方恢复从上部发送方发送的初始数据比特的情况。注意到这个接收方能够提取来自发送方 1 的数据，而不管来自发送方 2 的干扰传输。

再回到我们第 6 章中鸡尾酒会的类比，一个 CDMA 协议类似于让聚会客人使用多种语言来谈论；在这种情况下，人们实际上非常善于锁定他们能听懂的语言的谈话，而过滤了其余的谈话。我们这里看到 CDMA 是一个划分协议，因为它划分编码空间（与时间或频率相对），并且给每个节点分配一段专用的代码空间。

我们这里对 CDMA 的讨论是简要的；实践中还必须处理大量的困难问题。首先，为了使 CDMA 接收方能够提取一个特定的发送方的信号，必须仔细地选择 CDMA 编码。其次，我们的讨论假设在接收方接收到的来自从不同发送方的信号强度是相同的；这可能在实际中很难获得。有大量的文章讨论了有关 CDMA 的这些和其他问题；详细内容见［Pickholtz 1982；Viterbi 1995］。

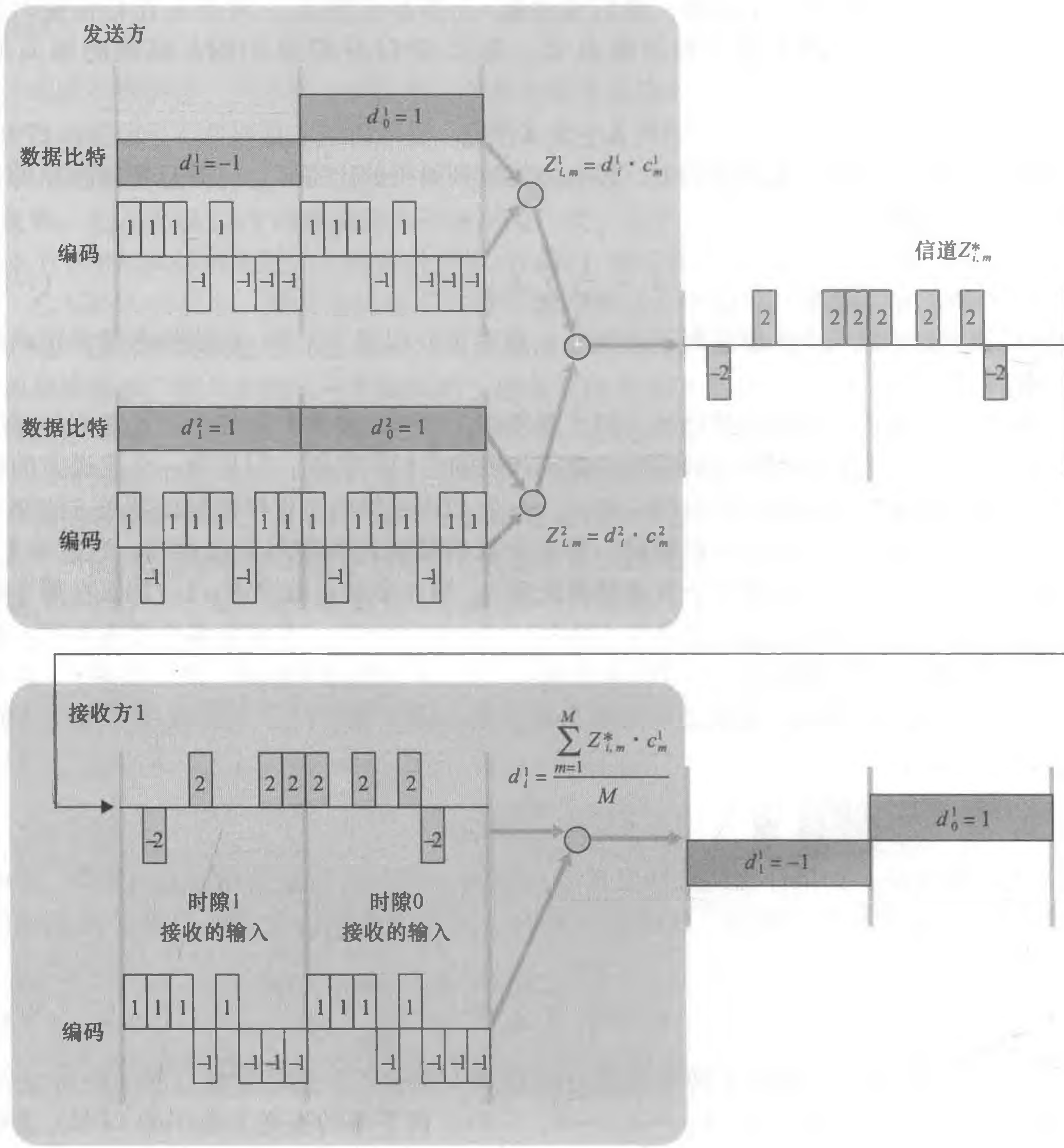


图 7-6　两个发送方的 CDMA 例子

7.3　WiFi：802.11 无线 LAN

当前，无线 LAN 在工作场所、家庭、教育机构、咖啡屋、机场以及街头无所不在，它已经成为因特网中的一种十分重要的接入网技术。尽管在 20 世纪 90 年代研发了许多有关无线 LAN 的标准和技术，但其中有一类标准已经明显成为赢家：IEEE 802.11 无线 LAN（也称为 WiFi）。在本节中，我们将详细研究 802.11 无线 LAN，分析它的帧结构、它的媒体访问协议以及 802.11 LAN 与有线以太网 LAN 的互联。

在 IEEE 802.11（“WiFi”）协议族中有几套有关无线 LAN 的 802.11 标准，表 7-1 中对它们进行了总结。不同的 802.11 标准都具有某些共同的特征。它们都使用相同的媒体访问协议 CSMA/CA，我们稍后将讨论该协议。这些标准对它们的链路层帧也都使用相同

的帧结构，而且它们都具有减少其传输速率的能力以伸展到更远的距离。并且重要的是，802.11 产品也都是向后兼容的，这意味着例如仅支持 802.11g 的移动站仍可以与较新的 802.11ac 基站交互。

然而，如表 7-1 所示，这些标准在物理层有一些重要的区别。802.11 设备工作在两个不同的频率段上：2.4～2.485GHz（称之为 2.4GHz 频段）和 5.1～5.8GHz（称之为 5GHz 频段）。2.4GHz 频段是一种无须执照的频段，在此频段上，使用 2.4GHz 的电话和微波炉等 802.11 设备可能会争用该频段的频谱。在 5GHz 频段，对于给定的功率等级 802.11 LAN 有更短的传输距离，并且受多径传播的影响更多。两种最新的标准 802.11n［IEEE 802.11n 2012］和 802.11ac［IEEE 802.11ac 2013；Cisco 802.11ac 2015］使用多输入多输出（MIMO）天线；也就是说在发送一侧的两根或更多的天线以及在接收一侧的两根或更多的天线发送/接收着不同的信号［Diggavi 2004］。802.11ac 基站可以同时向多个站点传输，并且使用“智能”天线在接收方的方向上用自适应成型波束向目标传输。这减少了干扰并增大了以给定数据率传输的可达距离。在表 7-1 中显示的数据率是针对理想环境的数据，例如一个离基站 1 米远的接收方没有干扰，而这种场景在实践中是不可能经历到的！因此正如谚语所说：你走过的路（或者此时是你的无线数据率）也许是变化的（YMMV）。

表 7-1　IEEE 802.11 标准小结

标准	频率范围	数据率
802.11b	2.4GHz	最高为 11Mbps
802.11a	5GHz	最高为 54Mbps
802.11g	2.4GHz	最高为 54Mbps
802.11n	2.5～5GHz	最高为 450Mbps
802.11ac	5GHz	最高为 1300Mbps

7.3.1　802.11 体系结构

图 7-7 显示了 802.11 无线 LAN 体系结构的基本构件。802.11 体系结构的基本构件模块是**基本服务集**（Basic Service Set，BSS）。一个 BSS 包含一个或多个无线站点和一个在 802.11 术语中称为**接入点**（Access Point，AP）的中央**基站**（base station）。图 7-7 展示了两个 BSS 中的 AP，它们连接到一个互联设备上（如交换机或者路由器），互联设备又连接到因特网中。在一个典型的家庭网络中，有一个 AP 和一台将该 BSS 连接到因特网中的路由器（通常综合成为一个单元）。

与以太网设备类似，每个 802.11 无线站点都具有一个 6 字节的 MAC 地址，该地址存储在该站适配器（即 802.11 网络接口卡）的固件中。每个 AP 的无线接口也具有一个 MAC 地址。与以太网类似，这些 MAC 地址由 IEEE 管理，理论上是全球唯一的。

如 7.1 节所述，配置 AP 的无线 LAN 经常被称作**基础设施无线** LAN（infrastructure wireless LAN），其中的“基础设施”是指 AP 连同互联 AP 和一台路由器的有线以太网。图 7-8 显示了 IEEE 802.11 站点也能将它们自己组合在一起形成一个自组织网络，即一个无中心控制和与“外部世界”无连接的网络。这里，该网络是由彼此已经发现相互接近且有通信需求的移动设备“动态”形成，并且在它们所处环境中没有预先存在的网络基础设施。当携带便携机的人们聚集在一起时（例如，在一个会议室、一列火车或者一辆汽车中），并且要在没有中央化的 AP 的情况下交换数据，一个自组织网络就可能形成了。随着要通信的便携设备的继续激增，人们对自组织网络产生巨大的兴趣。然而在本节中，我们只关注基础设施无线 LAN。

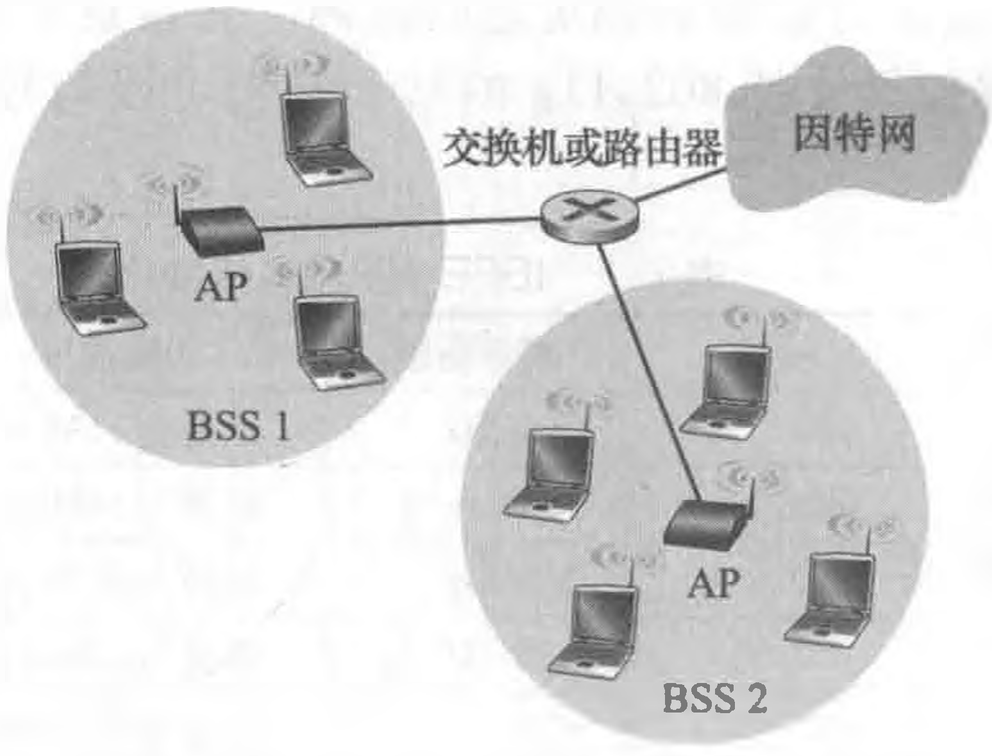


图 7-7　IEEE 802.11 LAN 体系结构

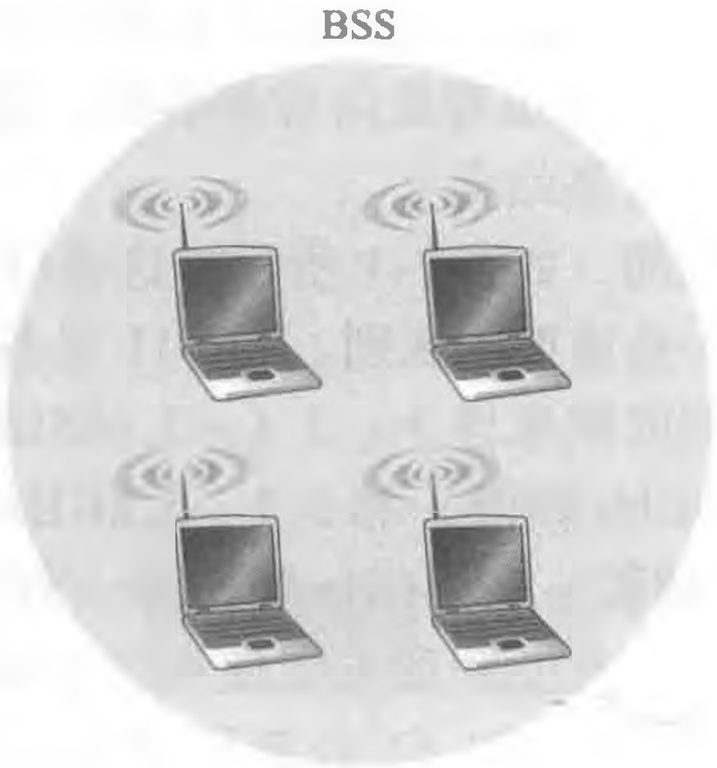


图 7-8　IEEE 802.11 自组织网络

信道与关联

在 802.11 中，每个无线站点在能够发送或者接收网络层数据之前，必须与一个 AP 相关联。尽管所有 802.11 标准都使用了关联，但我们将专门在 IEEE 802.11b/g 环境中讨论这一主题。

当网络管理员安装一个 AP 时，管理员为该接入点分配一个单字或双字的**服务集标识符**（Service Set Identifier，SSID）。（例如，当你在 iPhone 上选择设置 WiFi 时，将显示某范围内每个 AP 的 SSID。）管理员还必须为该 AP 分配一个信道号。为了理解信道号，回想前面讲过的 802.11 运行在 2.4～2.4835GHz 的频段中。在这个 85MHz 的频段内，802.11 定义了 11 个部分重叠的信道。当且仅当两个信道由 4 个或更多信道隔开时它们才无重叠。特别是信道 1、6 和 11 的集合是唯一的 3 个非重叠信道的集合。这意味着管理员可以在同一个物理网络中安装 3 个 802.11b AP，为这些 AP 分配信道 1、6 和 11，然后将每个 AP 都连接到一台交换机上。

既然已经对 802.11 信道有了基本了解，我们则可以描述一个有趣（且并非完全不寻常）的情况，即有关 WiFi 丛林。**WiFi 丛林**（WiFi jungle）是一个任意物理位置，在这里无线站点能从两个或多个 AP 中收到很强的信号。例如，在纽约城的许多咖啡馆中，无线站点可以从附近许多 AP 中选取一个信号。其中一个 AP 可能由该咖啡馆管理，而其他 AP 可能位于咖啡馆附近的住宅区内。这些 AP 中的每一个都可能位于不同的子网中，并被独立分配一个信道。

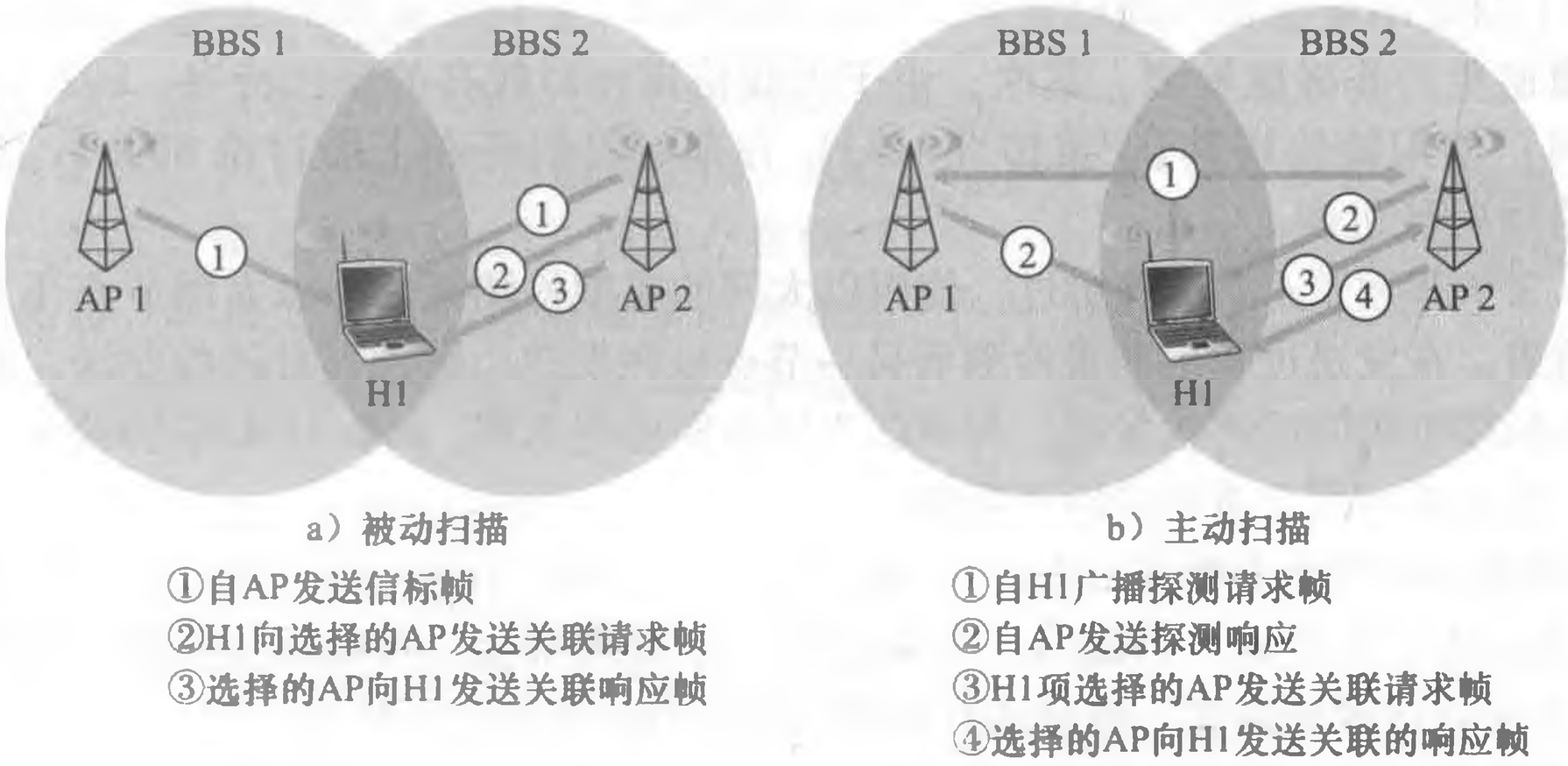
现在假定你带着自己的手机、平板电脑或便携机进入这样一个 WiFi 丛林，寻求无线因特网接入和一个蓝莓松饼。设在这个丛林中有 5 个 AP。为了获得因特网接入，你的无线站点需要加入其中一个子网并因此需要与其中的一个 AP 相**关联**（associate）。关联意味着这一无线站点在自身和该 AP 之间创建一个虚拟线路。特别是，仅有关联的 AP 才向你的无线站点发送数据帧，并且你的无线站点也仅仅通过该关联 AP 向因特网发送数据帧。然而，你的无线站点是如何与某个特定的 AP 相关联的？更为根本的问题是，你的无线站点是如何知道哪个 AP 位于该丛林呢？

802.11 标准要求每个 AP 周期性地发送**信标帧**（beacon frame），每个信标帧包括该 AP 的 SSID 和 MAC 地址。你的无线站点为了得知正在发送信标帧的 AP，扫描 11 个信道，找出来自可能位于该区域的 AP 所发出的信标帧（其中一些 AP 可能在相同的信道中传输，即这里有一个丛林！）。通过信标帧了解到可用 AP 后，你（或者你的无线主机）选择一个

AP 用于关联。

802.11 标准没有指定选择哪个可用的 AP 进行关联的算法；该算法被遗留给 802.11 固件和无线主机的软件设计者。通常，主机选择接收到的具有最高信号强度的信标帧。虽然高信号强度好（例如可参见图 7-3），信号强度将不是唯一决定主机接收性能的 AP 特性。特别是，所选择的 AP 可能具有强信号，但可能被其他附属的主机（将需要共享该 AP 的无线带宽）所过载，而某未过载的 AP 由于稍弱的信号而未被选择。选择 AP 的一些可替代的方法近来已被提出［Vasudevan 2005；Nicholson 2006；Sudaresan 2006］。有关信号强度如何测量的有趣而朴实的讨论参见［Bardwell 2004］。

扫描信道和监听信标帧的过程被称为**被动扫描**（passive scanning）（参见图 7-9a）。无线主机也能够执行**主动扫描**（active scanning），这是通过向位于无线主机范围内的所有 AP 广播探测帧完成的，如图 7-9b 所示。AP 用一个探测响应帧应答探测请求帧。无线主机则能够在响应的 AP 中选择某 AP 与之相关联。



a）被动扫描　　b）主动扫描

图 7-9　对接入点的主动和被动扫描

选定与之关联的 AP 后，无线主机向 AP 发送一个关联请求帧，并且该 AP 以一个关联响应帧进行响应。注意到对于主动扫描需要这种第二次请求/响应握手，因为一个对初始探测请求帧进行响应的 AP 并不知道主机选择哪个（可能多个）响应的 AP 进行关联，这与 DHCP 客户能够从多个 DHCP 服务器进行选择有诸多相同之处（参见图 4-24）。一旦与一个 AP 关联，该主机希望加入该 AP 所属的子网中（以 4.3.3 节中的 IP 寻址的意义）。因此。该主机通常将通过关联的 AP 向该子网发送一个 DHCP 发现报文（参见图 4-24），以获取在该 AP 子网中的一个 IP 地址。一旦获得地址，网络的其他部分将直接视你的主机为该子网中的另一台主机。

为了与特定的 AP 创建一个关联，某无线站点可能要向该 AP 鉴别它自身。802.11 无线 LAN 提供了几种不同的鉴别和接入方法。一种被许多公司采用的方法是，基于一个站点的 MAC 地址允许其接入一个无线网络。第二种被许多因特网咖啡屋采用的方法是，应用用户名和口令。在两种情况下，AP 通常与一个鉴别服务器进行通信，使用一种诸如 RADIUS［RFC 2865］或 DIAMETER［RFC 3588］的协议，在无线终端站和鉴别服务器之间中继信息。分离鉴别服务器和 AP，使得一个鉴别服务器可以服务于多个 AP，将（经常是敏感的）鉴别和接入的决定集中到单一服务器中，使 AP 费用和复杂性较低。我们将在第 8 章看到，定义 802.11 协议族安全性的新 IEEE 802.11i 协议就恰好

采用了这一方法。

7.3.2　802.11 MAC 协议

一旦某无线站点与一个 AP 相关联，它就可以经该接入点开始发送和接收数据帧。然而因为许多无线设备或 AP 自身可能希望同时经过相同信道传输数据帧，因此需要一个多路访问协议来协调传输。下面，我们将无线设备或 AP 称为**站点**（station），它们共享多个接入信道。正如在第 6 章和 7.2.1 节中讨论的那样，宽泛地讲有三类多路访问协议：信道划分（包括 CDMA）、随机访问和轮流。受以太网及其随机访问协议巨大成功的激励，802.11 的设计者为 802.11 无线 LAN 选择了一种随机访问协议。这个随机访问协议称作**带碰撞避免的 CSMA**（CSMA with collision avoidance），或简称为 CSMA/CA。与以太网的 CSMA/CD 相似，CSMA/CA 中的“CSMA”代表“载波侦听多路访问”，意味着每个站点在传输之前侦听信道，并且一旦侦听到该信道忙则抑制传输。尽管以太网和 802.11 都使用载波侦听随机接入，但这两种 MAC 协议有重要的区别。首先，802.11 使用碰撞避免而非碰撞检测。其次，由于无线信道相对较高的误比特率，802.11（不同于以太网）使用链路层确认/重传（ARQ）方案。我们将在下面讨论 802.11 的碰撞避免和链路层确认机制。

在 6.3.2 节和 6.4.2 节曾讲过，使用以太网的碰撞检测算法，以太网节点在发送过程中监听信道。在发送过程中如果检测到另一节点也在发送，则放弃自己的发送，并且在等待一个小的随机时间后再次发送。与 802.3 以太网协议不同，802.11MAC 协议并未实现碰撞检测。这主要由两个重要的原因所致：

- 检测碰撞的能力要求站点具有同时发送（站点自己的信号）和接收（检测其他站点是否也在发送）的能力。因为在 802.11 适配器上，接收信号的强度通常远远小于发送信号的强度，制造具有检测碰撞能力的硬件代价较大。
- 更重要的是，即使适配器可以同时发送和监听信号（并且假设它一旦侦听到信道忙就放弃发送），适配器也会由于隐藏终端问题和衰减问题而无法检测到所有的碰撞，参见 7.2 节的讨论。

由于 802.11 无线局域网不使用碰撞检测，一旦站点开始发送一个帧，它就完全地发送该帧；也就是说，一旦站点开始发送，就不会返回。正如人们可能猜想的那样，碰撞存在时仍发送整个数据帧（尤其是长数据帧）将严重降低多路访问协议的性能。为了降低碰撞的可能性，802.11 采用几种碰撞避免技术，我们稍后讨论它们。

然而，在考虑碰撞避免之前，我们首先需要分析 802.11 的**链路层确认**（link-layer acknowledgment）方案。7.2 节讲过，当无线 LAN 中某站点发送一个帧时，该帧会由于多种原因不能无损地到达目的站点。为了处理这种不可忽视的故障情况，802.11 MAC 使用链路层确认。如图 7-10 所示，目的站点收到一个通过 CRC 校验的帧后，它等待一个被称作**短帧间间隔**（Short Inter-Frame Spacing，SIFS）的一小段时间，然后发回一个确认帧。如果发送站点在给定的时间内未收到确认帧，它假定出现了错误并重传该帧，使用 CSMA/CA 协议访问该信道。如果在若干固定次重传后仍未收到确认，发送站点将放弃发送并丢弃该帧。

讨论过 802.11 如何使用链路层确认后，我们可以描述 802.11 的 CSMA/CA 协议了。假设一个站点（无线站点或者 AP）有一个帧要发送。

1）如果某站点最初监听到信道空闲，它将在一个被称作**分布式帧间间隔**（Distributed

Inter-Frame Space，DIFS）的短时间段后发送该帧，如图 7-10 所示。

2）否则，该站点选取一个随机回退值（如我们在 6.3.2 节中遇到的那样）并且在侦听信道空闲时递减该值。当侦听到信道忙时，计数值保持不变。

3）当计数值减为 0 时（注意到这只可能发生在信道被侦听为空闲时），该站点发送整个数据帧并等待确认。

4）如果收到确认，发送站点知道它的帧已被目的站正确接收了。如果该站点要发送另一帧，它将从第二步开始 CSMA/CA 协议。如果未收到确认，发送站点将重新进入第二步中的回退阶段，并从一个更大的范围内选取随机值。

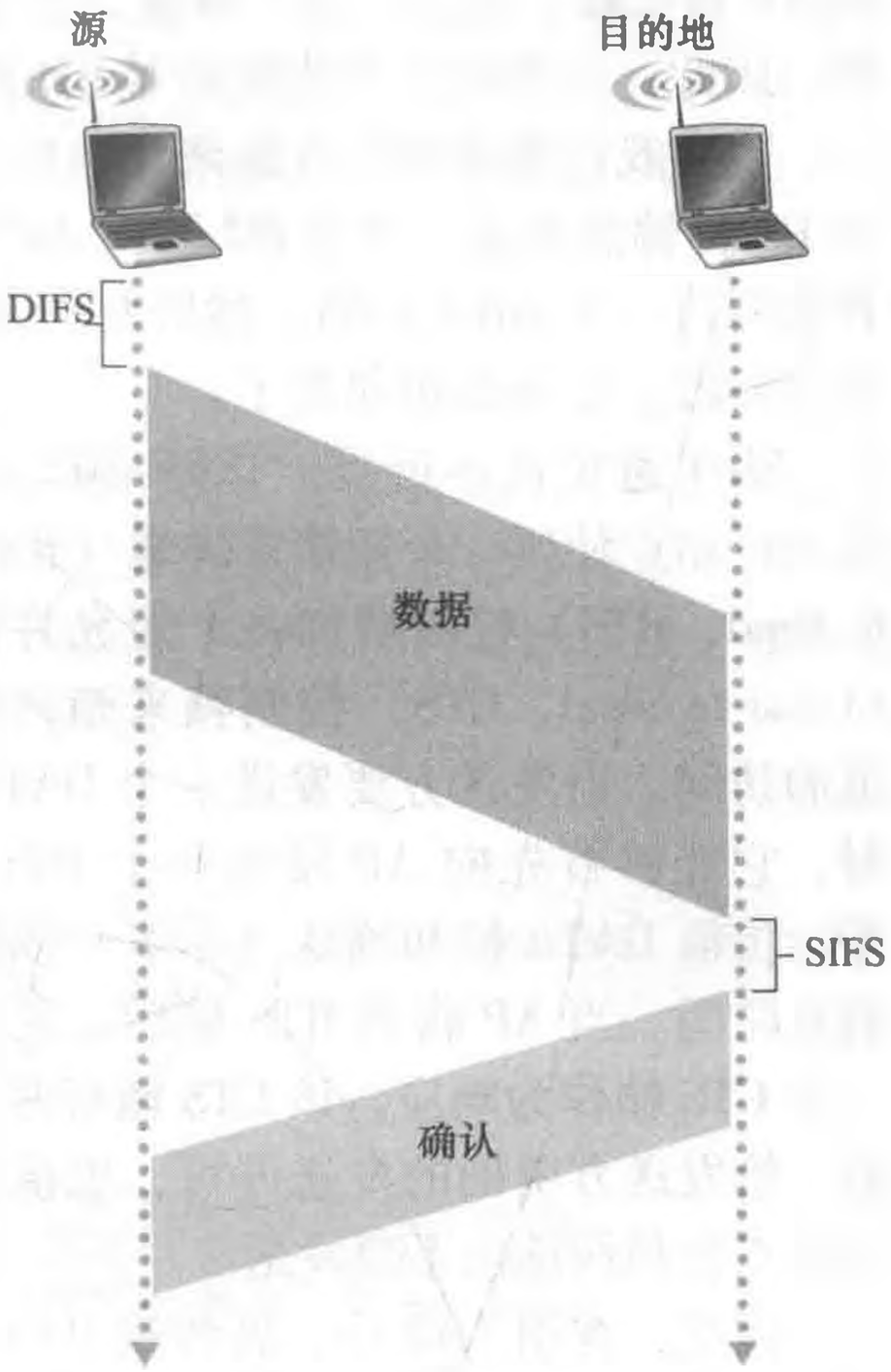


图 7-10　802.11 使用链路层确认

前面讲过，在以太网的 CSMA/CD 的多路访问协议（6.3.2 节）下，一旦侦听到信道空闲，站点开始发送。然而，使用 CSMA/CA，该站点在倒计数时抑制传输，即使它侦听到该信道空闲也是如此。为什么 CSMA/CD 和 CSMA/CA 采用了不同的方法呢？

为了回答这一问题，我们首先考虑这样一种情形：两个站点分别有一个数据帧要发送，但是，由于侦听到第三个站点已经在传输，双方都未立即发送。使用以太网的 CSMA/CD 协议中，两个站点将会在检测到第三方发送完毕后立即开始发送。这将导致一个碰撞，在 CSMA/CD 协议中碰撞并非是一个严重的问题，因为两个站点检测到碰撞后都会放弃它们的发送，从而避免了由于碰撞而造成的该帧剩余部分的无用发送。而在 802.11 中情况却十分不同，因为 802.11 并不检测碰撞和放弃发送，遭受碰撞的帧仍将被完全传输。因此 802.11 的目标是无论如何尽可能避免碰撞。在 802.11 中，如果两个站点侦听到信道忙，它们都将立即进入随机回退，希望选择一个不同的回退值。如果这些值的确不同，一旦信道空闲，其中的一个站点将在另一个之前发送，并且（如果两个站点均未对对方隐藏）“失败站点”将会听到“胜利站点”的信号，冻结它的计数器，并在胜利站点完成传输之前一直抑制传输。通过这种方式，避免了高代价的碰撞。当然，在以下情况下使用 802.11 仍可能出现碰撞：两个站点可能互相是隐藏的，或者两者可能选择了非常靠近的随机回退值，使来自先开始站点的传输也必须到达第二个站点。回想前面我们在图 6-12 的环境中讨论随机访问算法时遇到过这个问题。

1. 处理隐藏终端：RTS 和 CTS

802.11 MAC 协议也包括了一个极好（但为可选项）的预约方案，以帮助在出现隐藏终端的情况下避免碰撞。我们在图 7-11 的环境下研究这种方案，其中显示了两个无线站点和一个接入点。

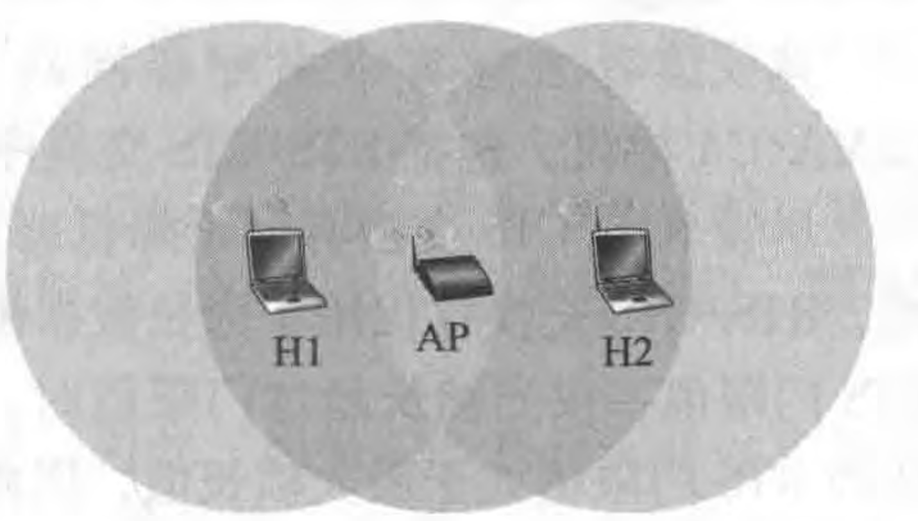


图 7-11　隐藏终端的例子：H1 和 H2 彼此互相隐藏

这两个无线站点都在该 AP 的覆盖范围内（其覆盖范围显示为阴影圆环），并且两者都与该 AP 相关联。然而，由于衰减，无线节点的信号范围局限在图 7-11 所示的阴影圆环内部。因此，尽管每个无线站点对 AP 都不隐藏，两者彼此却是隐藏的。

现在我们考虑为什么隐藏终端会导致出现问题。假设站点 H1 正在传输一个帧，并且在 H1 传输的中途，站点 H2 要向 AP 发送一个帧。由于 H2 未听到来自 H1 的传输，它将首先等待一个 DIFS 间隔，然后发送该帧，导致产生了一个碰撞。从而在 H1 和 H2 的整个发送阶段，信道都被浪费了。

为了避免这一问题，IEEE 802.11 协议允许站点使用一个短**请求发送**（Request to Send，RTS）控制帧和一个短**允许发送**（Clear to Send，CTS）控制帧来预约对信道的访问。当发送方要发送一个 DATA 帧时，它能够首先向 AP 发送一个 RTS 帧，指示传输 DATA 帧和确认（ACK）帧需要的总时间。当 AP 收到 RTS 帧后，它广播一个 CTS 帧作为响应。该 CTS 帧有两个目的：给发送方明确的发送许可，也指示其他站点在预约期内不要发送。

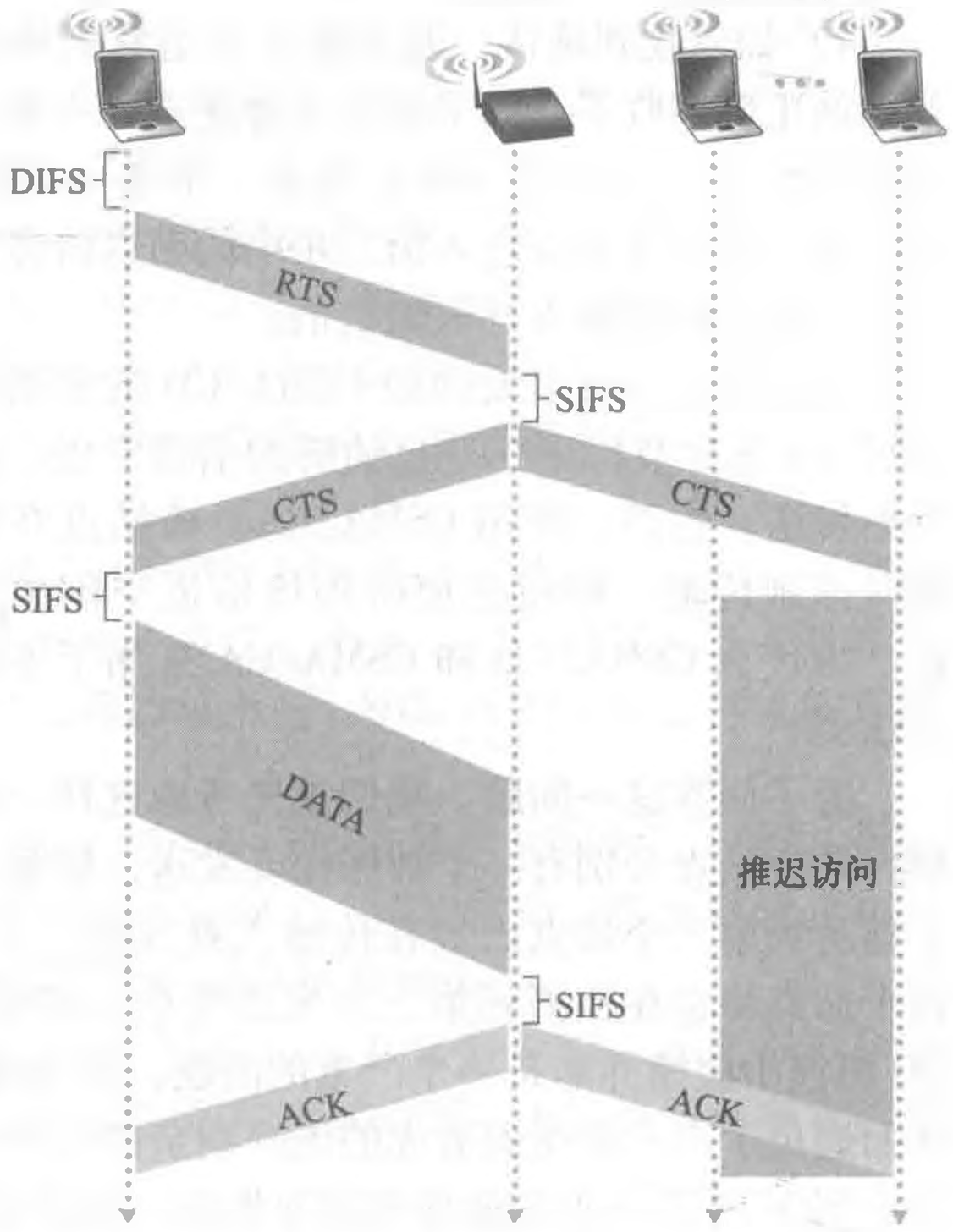


图 7-12　使用 RTS 和 CTS 帧的碰撞避免

因此，在图 7-12 中，在传输 DATA 帧前，H1 首先广播一个 RTS 帧，该帧能被其范围内包括 AP 在内的所有站点听到。AP 然后用一个 CTS 帧响应，该帧也被其范围内包括 H1 和 H2 在内的所有站点听到。站点 H2 听到 CTS 后，在 CTS 帧中指明的时间内将抑制发送。RTS、CTS、DATA和 ACK 帧如图 7-12 所示。

RTS 和 CTS 帧的使用能够在两个重要方面提高性能：

- 隐藏终端问题被缓解了，因为长 DATA 帧只有在信道预约后才被传输。
- 因为 RTS 和 CTS 帧较短，涉及 RTS 和 CTS 帧的碰撞将仅持续短 RTS 和 CTS 帧的持续期。一旦 RTS 和 CTS 帧被正确传输，后续的 DATA 和 ACK 帧应当能无碰撞地发送。

建议读者去查看本书配套网站上的 802.11 Java 程序。这个交互式程序演示了 CSMA/CA 协议，包括 RTS/CTS 交换序列。

尽管 RTS/CTS 交换有助于降低碰撞，但它同样引入了时延以及消耗了信道资源。因此，RTS/CTS 交换仅仅用于为长数据帧预约信道。在实际中，每个无线站点可以设置一个 RTS 门限值，仅当帧长超过门限值时，才使用 RTS/CTS 序列。对许多无线站点而言，默认的 RTS 门限值大于最大帧长值，因此对所有发送的 DATA 帧，RTS/CTS 序列都被跳过。

2. 使用 802.11 作为一个点对点链路

到目前为止我们的讨论关注在多路访问环境中使用 802.11。应该指出，如果两个节点

每个都具有一个定向天线，它们可以将其定向天线指向对方，并基本上是在一个点对点的链路上运行 802.11 协议。如果商用 802.11 硬件产品价格低廉，那么使用定向天线以及增加传输功率使得 802.11 成为一个在数十公里距离中提供无线点对点连接的廉价手段。[Raman 2007] 描述了这样一个运行于印度恒河郊区平原上的多跳无线网络，其中包含了点对点 802.11 链路。

7.3.3　IEEE 802.11 帧

尽管 802.11 帧与以太网帧有许多共同特点，但它也包括了许多特定用于无线链路的字段。8021.11 帧如图 7-13 所示，在该帧上的每个字段上面的数字代表该字段以字节计的长度；在该帧控制字段中，每个子字段上面的数字代表该子字段以比特计的长度。现在我们查看该帧中各字段以及帧控制字段中一些重要的子字段。

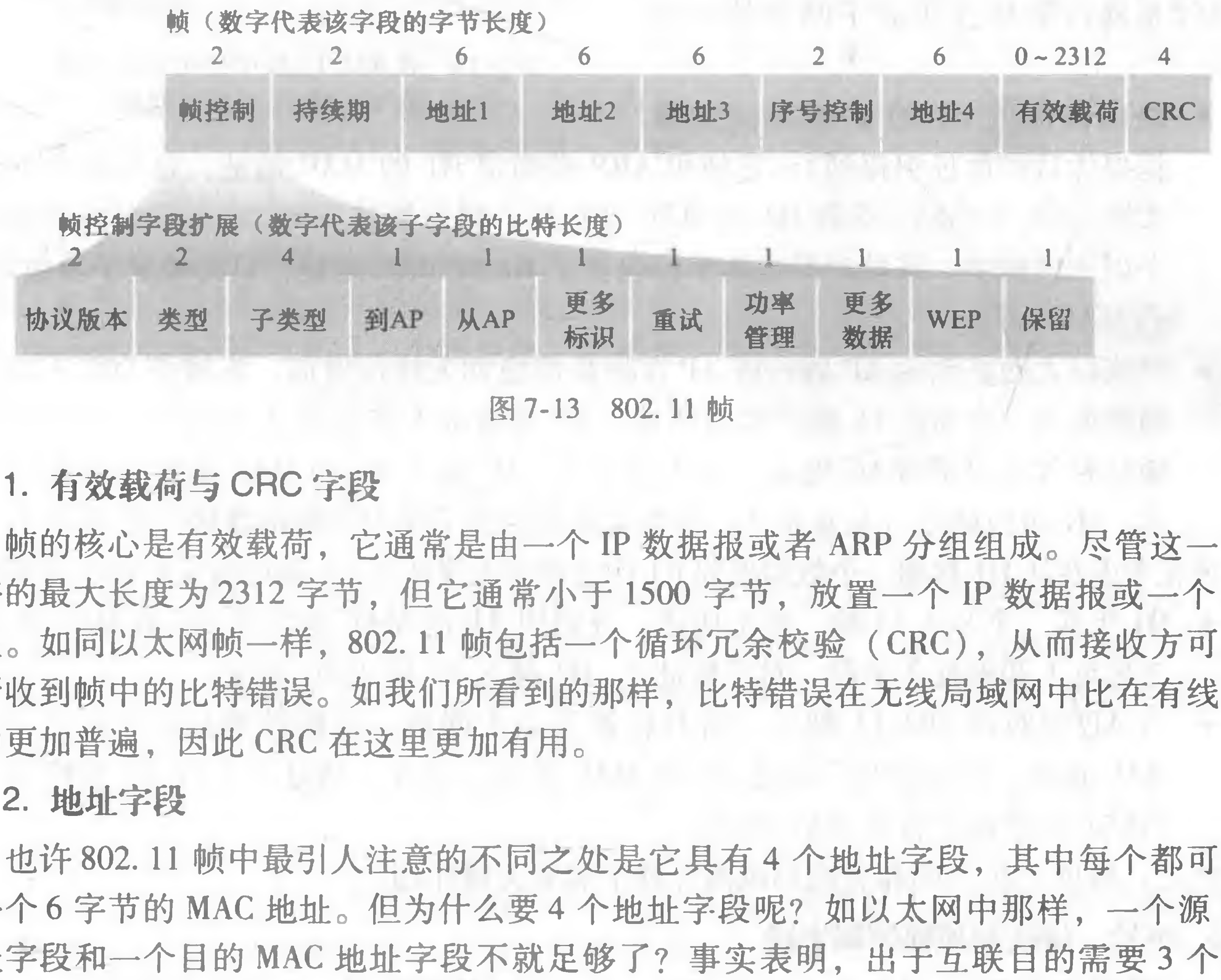


图 7-13　802.11 帧

1. 有效载荷与 CRC 字段

帧的核心是有效载荷，它通常是由一个 IP 数据报或者 ARP 分组组成。尽管这一字段允许的最大长度为 2312 字节，但它通常小于 1500 字节，放置一个 IP 数据报或一个 ARP 分组。如同以太网帧一样，802.11 帧包括一个循环冗余校验（CRC），从而接收方可以检测所收到帧中的比特错误。如我们所看到的那样，比特错误在无线局域网中比在有线局域网中更加普遍，因此 CRC 在这里更加有用。

2. 地址字段

也许 802.11 帧中最引人注意的不同之处是它具有 4 个地址字段，其中每个都可以包含一个 6 字节的 MAC 地址。但为什么要 4 个地址字段呢？如以太网中那样，一个源 MAC 地址字段和一个目的 MAC 地址字段不就足够了？事实表明，出于互联目的需要 3 个地址字段，特别是将网络层数据报从一个无线站点通过一个 AP 送到一台路由器接口。当 AP 在自组织模式中互相转发时使用第四个地址。由于我们这里仅仅考虑基础设施网络，所以只关注前 3 个地址字段。802.11 标准定义这些字段如下：

- 地址 2 是传输该帧的站点的 MAC 地址。因此，如果一个无线站点传输该帧，该站点的 MAC 地址就被插入在地址 2 字段中。类似地，如果一个 AP 传输该帧，该 AP 的 MAC 地址也被插入在地址 2 字段中。
- 地址 1 是要接收该帧的无线站点的 MAC 地址。因此，如果一个移动无线站点传输该帧，地址 1 包含了该目的 AP 的 MAC 地址。类似地，如果一个 AP 传输该帧，地址 1 包含该目的无线站点的 MAC 地址。
- 为了理解地址 3，回想 BSS（由 AP 和无线站点组成）是一个子网的一部分，并且这个

子网经一些路由器接口与其他子网相连。地址 3 包含这个路由器接口的 MAC 地址。

为了对地址 3 的目的有更深入的理解，我们观察在图 7-14 环境中的网络互联的例子。在这幅图中，有两个 AP，每个 AP 负责一些无线站点。每个 AP 到路由器有一个直接连接，路由器依次又连接到全球因特网。我们应当记住 AP 是链路层设备，它既不能“说”IP 又不理解 IP 地址。现在考虑将一个数据报从路由器接口 R1 移到无线站点 H1。路由器并不清楚在它和 H1 之间有一个 AP；从路由器的观点来说，H1 仅仅是路由器所连接的子网中的一台主机。

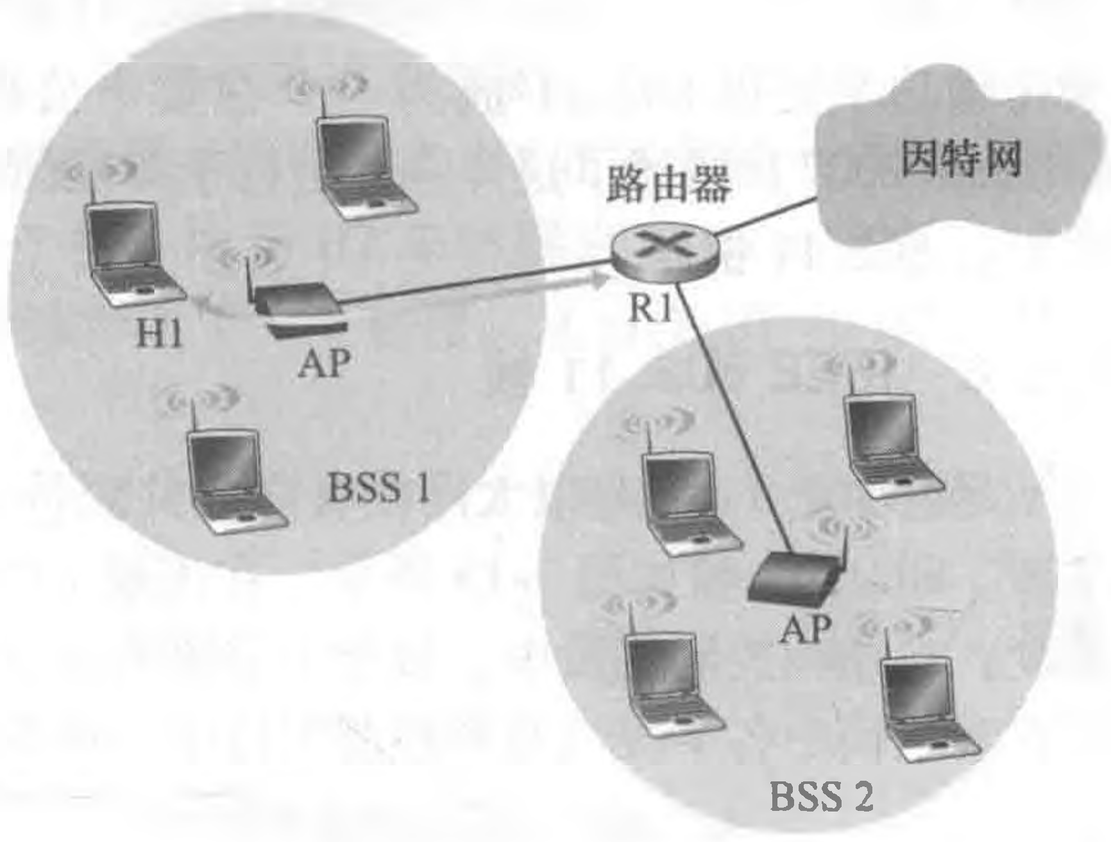


图 7-14　在 802.11 帧中使用地址字段：在 H1 和 R1 之间发送帧

- 路由器知道 H1 的 IP 地址（从数据报的目的地址中得到），它使用 ARP 来确定 H1 的 MAC 地址，这与在普通的以太网 LAN 中相同。获取 H1 的 MAC 地址后，路由器接口 R1 将该数据报封装在一个以太网帧中。该帧的源地址字段包含了 R1 的 MAC 地址，目的地址字段包含 H1 的 MAC 地址。
- 当该以太网帧到达 AP 后，该 AP 在将其传输到无线信道前，先将该 802.3 以太网帧转换为一个 802.11 帧。如前所述，AP 将地址 1 和地址 2 分别填上 H1 的 MAC 地址和其自身的 MAC 地址。对于地址 3，AP 插入 R1 的 MAC 地址。通过这种方式，H1 可以确定（从地址 3）将数据报发送到子网中的路由器接口的 MAC 地址。

现在考虑在从 H1 移动一个数据报到 R1 的过程中无线站点 H1 进行响应时发生的情况。

- H1 生成一个 802.11 帧，如上所述，分别用 AP 的 MAC 地址和 H1 的 MAC 地址填充地址 1 和地址 2 字段。对于地址 3，H1 插入 R1 的 MAC 地址。
- 当 AP 接收该 802.11 帧后，将其转换为以太网帧。该帧的源地址字段是 H1 的 MAC 地址，目的地址字段是 R1 的 MAC 地址。因此，地址 3 允许 AP 在构建以太网帧时能够确定目的 MAC 地址。

总之，地址 3 在 BSS 和有线局域网互联中起着关键作用。

3. 序号、持续期和帧控制字段

前面讲过在 802.11 网络中，无论何时一个站点正确地收到一个来自于其他站点的帧，它就回发一个确认。因为确认可能会丢失，发送站点可能会发送一个给定帧的多个副本。正如我们在 rdt2.1 协议讨论中所见（3.4.1 节），使用序号可以使接收方区分新传输的帧和以前帧的重传。因此在 802.11 帧中的序号字段在链路层与在第 3 章中运输层中的该字段有着完全相同的目的。

前面讲过 802.11 协议允许传输节点预约信道一段时间，包括传输其数据帧的时间和传输确认的时间。这个持续期值被包括在该帧的持续期字段中（在数据帧和 RTS 及 CTS 帧中均存在）。

如图 7-13 所示，帧控制字段包括许多子字段，我们将提一下其中比较重要的子字段，更加完整的讨论请参见 802.11 规范［Held 2001；Crow 1997；IEEE 802.11 1999］。类型和

子类型字段用于区分关联、RTS、CTS、ACK 和数据帧。To（到）和 From（从）字段用于定义不同地址字段的含义。（这些含义随着使用自组织模式或者基础设施模式而改变，而且在使用基础设施模式时，也随着是无线站点还是 AP 在发送帧而变化。）最后，WEP 字段指示了是否使用加密（WEP 将在第 8 章中讨论。）

7.3.4　在相同的 IP 子网中的移动性

为了增加无线 LAN 的物理范围，公司或大学经常会在同一个 IP 子网中部署多个 BSS。这自然就引出了在多个 BSS 之间的移动性问题，即无线站点如何在维持进行中的 TCP 会话的情况下，无缝地从一个 BSS 移动到另一个 BSS？正如我们将在本小节中所见，当这些 BSS 属于同一子网时，移动性可以用一种相对直接的方式解决。当站点在不同子网间移动时，就需要更为复杂的移动性管理协议了，我们将在 7.5 节和 7.6 节中学习这些协议。

我们现在看一个同一子网中的不同 BSS 之间的移动性的特定例子。图 7-15 显示了具有一台主机 H1 的两个互联的 BSS，该主机从 BSS1 移动到 BSS2。因为在这个例子中连接两个 BSS 的互联设备不是一台路由器，故在两个 BSS 中的所有站点（包括 AP）都属于同一个 IP 子网。因此，当 H1 从 BSS1 移动到 BSS2 时，它可以保持自己的 IP 地址和所有正在进行的 TCP 连接。如果互联设备是一台路由器，则 H1 必须在它移动进入的子网中获得一个新地址。这种地址的变化将打断（并且最终终止）在 H1 的任何进行中的 TCP 连接。在 7.6 节中，我们将能看到一种网络层移动性协议如移动 IP 能被用于避免该问题。

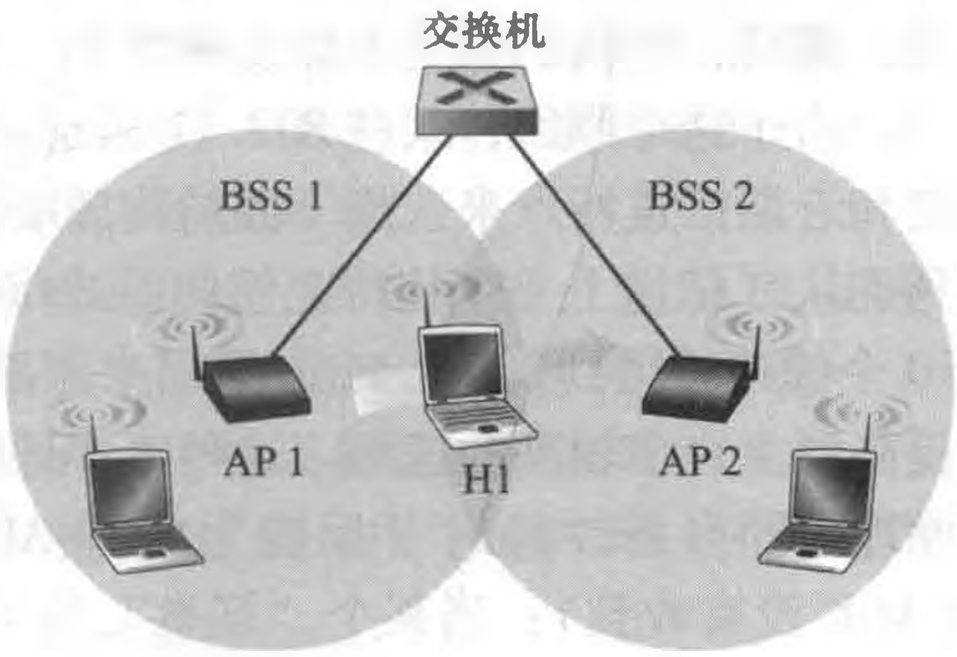


图 7-15　同一子网中的移动性

但是 H1 从 BSS1 移动到 BSS2 时具体会发生哪些事呢？随着 H1 逐步远离 AP1，H1 检测到来自 AP1 的信号逐渐减弱并开始扫描一个更强的信号。H1 收到来自 AP2 的信标帧（在许多公司和大学的设置中它与 AP1 有相同的 SSID）。H1 然后与 AP1 解除关联，并与 AP2 关联起来，同时保持其 IP 地址和维持正在进行的 TCP 会话。

从主机和 AP 的角度，这就处理了切换问题。但对图 7-15 中的交换机又会发生什么样的情况呢？交换机如何知道主机已经从一个 AP 移动到另一个 AP 呢？回想第 6 章所述，交换机是“自学习”的，并且自动构建它们的转发表。这种自学习的特征很好地处理了偶尔的移动（例如，一个雇员从一个部门调转到另一个部门）。然而，交换机没有被设计用来支持用户在不同 BSS 间高度移动，同时又希望保持 TCP 连接。为理解这一问题，回想在移动之前，交换机在其转发表中有一个表项，对应 H1 的 MAC 地址与到达 H1 所通过的出交换机端口。如果 H1 初始在 BSS1 中，则发往 H1 的数据报将经 AP1 导向 H1。然而，一旦 H1 与 BSS2 关联，它的帧应当被导向 AP2。一种解决方法（真有点不规范）是在新的关联形成后，让 AP2 以 H1 的源地址向交换机发送一以太网广播帧。当交换机收到该帧后，更新其转发表，使得 H1 可以通过 AP2 到达。802.11f 标准小组正在开发一个 AP 间的协议来处理这些以及相关的问题。

我们以上的讨论关注了在相同 LAN 子网中的移动性。前面我们在 6.4.4 节学习过 VLAN，它能够用来将若干 LAN 孤岛连接成为一个大虚拟 LAN，该虚拟 LAN 能够跨越很大的地理范围。在这种 VALN 中的基站之间的移动性能够以上述完全相同的方式来处理［Yu 2011］。

7.3.5　802.11 中的高级特色

我们将简要地讨论 802.11 网络中具有的两种高级能力，以此来完成我们学习 802.11 的内容。如我们所见，这些能力并不是完全特定于 802.11 标准的，而是在该标准中可能由特定机制产生的。这使得不同的厂商可使用他们自己（专用）的方法来实现这些能力，这也许能让他们增强竞争能力。

1. 802.11 速率适应

我们在前面图 7-3 中看到，不同的调制技术（提供了不同的传输速率）适合于不同的 SNR 情况。考虑这样一个例子，一个 802.11 用户最初离基站 20 米远，这里信噪比高。在此高信噪比的情况下，该用户能够与基站使用可提供高传输速率的物理层调制技术进行通信，同时维持低 BER。这个用户多么幸福啊！假定该用户开始移动，向离开基站的方向走去，随着与基站距离的增加，SNR 一直在下降。在这种情况下，如果在用户和基站之间运行的 802.11 协议所使用的调制技术没有改变的话，随着 SNR 减小，BER 将高得不可接受，最终，传输的帧将不能正确收到。

由于这个原因，某些 802.11 实现具有一种速率自适应能力，该能力自适应地根据当前和近期信道特点来选择下面的物理层调制技术。如果一个节点连续发送两个帧而没有收到确认（信道上一个比特差错的隐式指示），该传输速率降低到前一个较低的速率。如果 10 个帧连续得到确认，或如果用来跟踪自上次降速以来时间的定时器超时，该传输速率提高到上一个较高的速率。这种速率适应机制与 TCP 的拥塞控制机制具有相同的“探测”原理，即当条件好时（反映为收到 ACK），增加传输速率，除非某个“坏事”发生了（ACK 没有收到）；当某个“坏事”发生了，减小传输速率。因此，802.11 的速率适应和 TCP 的拥塞控制类似于年幼的孩子，他们不断地向父母要求越来越多（如幼儿要糖果，青少年要求推迟睡觉），直到父母亲最后说“够了!”，孩子们不再要求了（仅当以后情况已经变好了才会再次尝试）。已经提出了一些其他方案以改善这个基本的自动速率调整方案[Kamerman 1997；Holland 2001；Lacage 2004]。

2. 功率管理

功率是移动设备的宝贵资源，因此 802.11 标准提供了功率管理能力，以使 802.11 节点的侦听、传输和接收功能以及其他需要“打开”电路的时间量最小化。802.11 功率管理按下列方式运行。一个节点能够明显地在睡眠和唤醒状态之间交替（像在课堂上睡觉的学生!）。通过将 802.11 帧首部的功率管理比特设置为 1，某节点向接入点指示它将打算睡眠。设置节点中的一个定时器，使得正好在 AP 计划发送它的信标帧前唤醒节点（前面讲过 AP 通常每 100ms 发送一个信标帧）。因为 AP 从设置的功率传输比特知道哪个节点打算睡眠，所以该 AP 知道它不应当向这个节点发送任何帧，先缓存目的地为睡眠主机的任何帧，待以后再传输。

在 AP 发送信标帧前，恰好唤醒节点，并迅速进入全面活动状态（与睡觉的学生不同，这种唤醒仅需要 250μs[Kamerman 1997]）。由 AP 发送的信标帧包含了帧被缓存在 AP 中的节点的列表。如果某节点没有缓存的帧，它能够返回睡眠状态。否则，该节点能够通过向 AP 发送一个探询报文明确地请求发送缓存的帧。对于信标之间的 100ms 时间来说，250μs 的唤醒时间以及类似的接收信标帧及检查以确保不存在缓存帧的短小时间，没有帧要发送和接收的节点能够睡眠 99% 的时间，从而大大节省了能源。

7.3.6　个人域网络：蓝牙和 ZigBee

如图 7-2 所示，IEEE 802.11 WiFi 标准主要针对相距多达 100m 的设备间的通信（当使用 802.11 具有定向天线的点对点配置时除外）。两个其他的 IEEE 802 无线协议是蓝牙和 ZigBee（定义在 IEEE 802.15.1 和 IEEE 802.15.4 标准中［IEEE 802.15 2012］）。

1. 蓝牙

IEEE 802.15.1 网络以低功率和低成本在小范围内运行。它本质上是一个低功率、小范围、低速率的“电缆替代”技术，用于计算机与其无线键盘、鼠标或其他外部设备如蜂窝电话、扬声器、头戴式耳机及其他设备的互联，而 802.11 是一个较高功率、中等范围、较高速率的“接入”技术。为此，802.15.1 网络有时被称为**无线个人域网络**（Wireless Personal Area Network，WPAN）。802.15.1 的链路层和物理层基于早期用于个人域网络的**蓝牙**（Bluetooth）规范［Held 2001，Bisdikian 2001］。802.15.1 网络以 TDM 方式工作于无须许可证的 2.4GHz 无线电波段，每个时隙长度为 625μs。在每个时隙内，发送方利用 79 个信道中的一个进行传输，同时从时隙到时隙以一个已知的伪随机方式变更信道。这种被称作**跳频扩展频谱**（Frequency-Hopping Spread Spectrum，FHSS）的信道跳动的形式将传输及时扩展到整个频谱。802.15.1 能够提供高达 4Mbps 的数据率。

802.15.1 网络是自组织网络：不需要网络基础设施（如一个接入点）来互连 802.15.1 设备。因此，802.15.1 设备必须自己进行组织。802.15.1 设备首先组织成一个多达 8 个活动设备的**皮可网**（piconet），如图 7-16 所示。这些设备之一被指定为主设备，其余充当从设备。主节点真正控制皮可网，即它的时钟确定了皮可网中的时间，它可以在每个奇数时隙中发送，而从设备仅当主设备在前一时隙与其通信后才可以发送，并且只能发送给主设备。除了从设备，网络中还可以有多达 255 个的寄放（parked）设备。这些设备仅当其状态被主节点从寄放转换为活动之后才可以进行通信。

希望了解更多有关 802.15.1WPAN 信息的读者可以查阅蓝牙参考资料［Held 2001，Bisdikian 2001］，或者 IEEE 802.15 官方 Web 网站［IEEE 802.15 2012］。

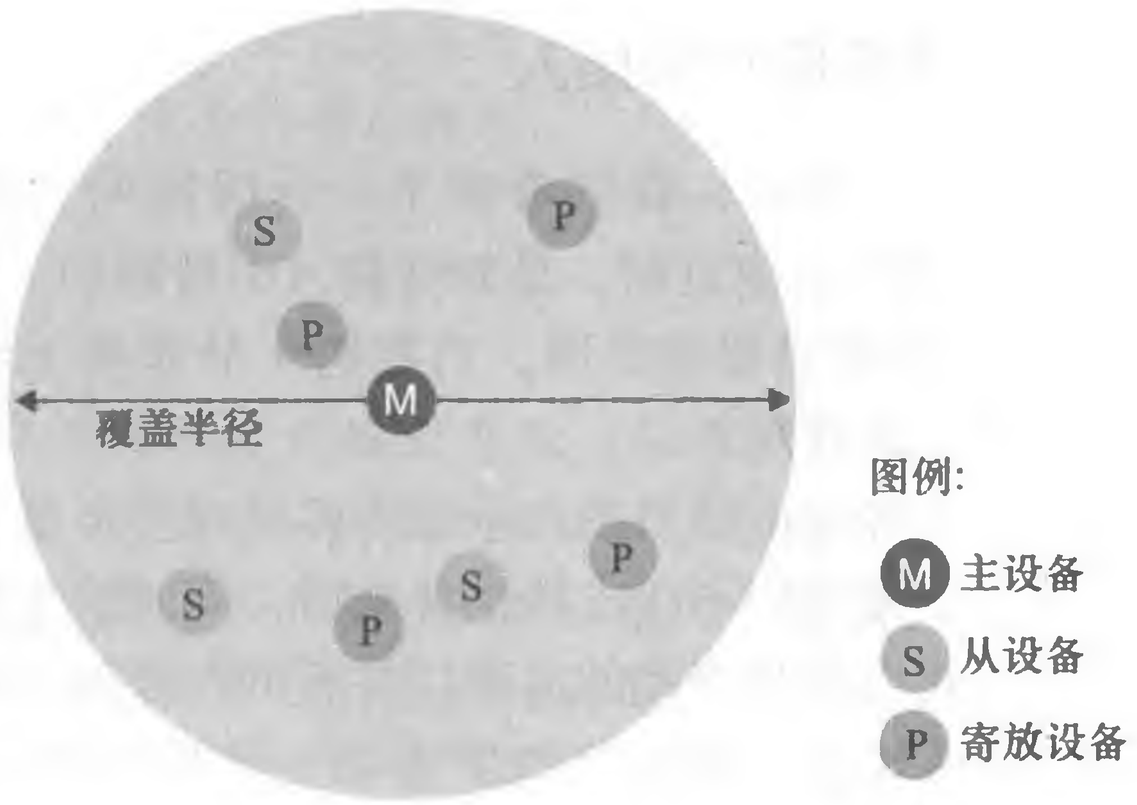


图 7-16　蓝牙皮可网

2. ZigBee

IEEE 标准化的第二个个人域网络是 802.14.5［IEEE 802.15 2012］，它被称为 ZigBee。虽然蓝牙网络提供了一种“电缆替代”的超过每秒兆比特的数据率，但 ZigBee 较之蓝牙其服务目标是低功率、低数据率、低工作周期的应用。尽管我们可能倾向于认为“更大和更快就更好”，但是并非所有的网络应用都需要高带宽和随之而来的高成本（经济和功率成本）。例如，家庭温度和光线传感器、安全设备和墙上安装的开关都是非常简单、低功率、低工作周期、低成本设备。ZigBee 因此是非常适合于这些设备的。ZigBee 定义了 20kbps、40kbps、100kbps 和 250kbps 的信道速率，这取决于信道的频率。

ZigBee 网络中的节点具有两个特色。多个所谓“简化功能设备”在单个“全功能设