

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 8.8 节看到,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。

6.3.2 802.11 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。然而因为许多站点可能希望同时经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。这里,站点(station)可以是一个无线站点,或者是一个 AP。正如在第 5 章和 6.2.1 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鼓舞,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 5.3.2 节和 5.4.2 节曾讲过,使用以太网的碰撞检测算法,以太网结点在发送过程中监听信道。在发送过程中如果检测到另一结点也在发送,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,802.11 MAC 协议并未实现碰撞检测。这主要由两个原因所致:

- 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 6.2 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。6.2 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 6-10 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。