8.8.1 有线等效保密

IEEE 802.11 的 WEP 协议设计于 1999 年，为在主机和无线接入点（即基站）之间提供鉴别和数据的加密。WEP 并没有指定密钥管理算法，因此它假定主机和无线接入点之间通过带外方式就密钥达成了某种一致。鉴别以下列方式进行：

1）无线主机通过接入点请求鉴别。

2）接入点以一个 128 字节的不重数值响应该鉴别请求。

3）无线主机用它与这个接入点共享的密钥加密这个不重数值。

4）接入点解密主机加密的不重数值。

如果解密所得不重数值与初始发给主机的值相同，则这个接入点鉴别了该主机。

图 8-30 阐述了 WEP 数据加密算法。假定主机和接入点都知道一个秘密的 40 比特对称密钥 K_S。此外，一个 24 比特的初始向量（IV）附加到这个 40 比特的密钥后面，产生用于加密单个帧的一个 64 比特密钥。每一个帧所使用的 IV 都不同，所以每一帧都由不同的 64 比特密钥加密。加密以如下方式进行。首先为每个数据载荷计算一个 4 字节的 CRC 值（见 5.2 节）。然后用 RC4 流密码加密该载荷和该 4 字节 CRC。我们这里不涉及 RC4 的细节（细节参见［Schneier 1995］和［Edney 2003］）。就我们的目的而言，知道下列事实即可：对于密钥值（此时为 64 比特（K_S、IV）密钥），RC4 算法产生一个密钥值的流为 k_1^{IV}，k_2^{IV}，k_3^{IV}，…，这些密码值用于加密一帧中的数据和 CRC 值。出于实用的目的，我们可以认为每次对一个字节执行这些操作。通过把数据的第 i 字节 d_i 和由（K_S、IV）对生成的密钥值流中的第 i 个密钥 k_i^{IV} 执行异或操作进行加密，以产生密文的第 i 字节 c_i：

$$c_i = d_i \oplus k_i^{IV}$$

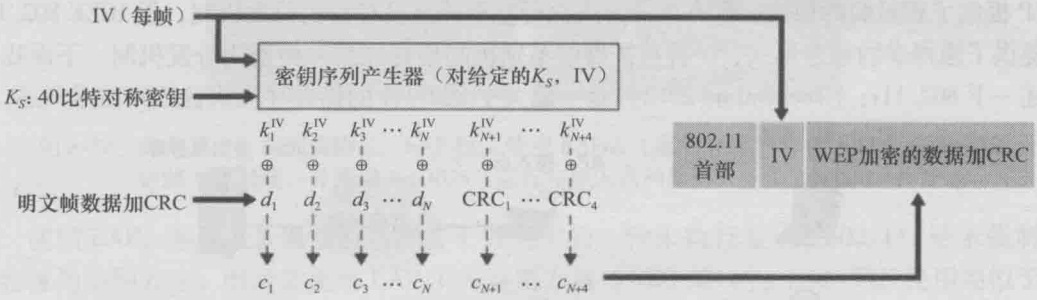

图 8-30 802.11 WEP 协议

如图 8-30 中所示，该 IV 值逐帧而变化，以明文形式出现在每一个 WEP 加密的 802.11 帧的首部中。接收方取它与发送方共享的秘密 40 比特对称密钥，添加上该 IV，并使用形成的 64 比特的密钥（它与发送方执行加密所用的密钥相同）来解密这个帧。

$$d_i = c_i \oplus k_i^{IV}$$

正确使用 RC4 算法要求同一个 64 比特密钥决不能使用超过 1 次。前面讲过 WEP 密钥是每一帧变换一次。对于某给定的 K_S（如果它有变化的话也是很少的），这意味着只有 2^{24} 个不同的密钥可用。如果随机选择这些密钥的话，我们能够看到［Walker 2000；Edney 2003］，则仅在处理 12 000 帧之后就选中相同的 IV 值（从而使用相同的 64 比特密钥）的概率超过 99%。在 1KB 帧长和 11Mbps 数据传输率的情况下，传输 12 000 帧仅需几秒的时间。