Air Kiss(飞吻)技术实现方案

一、Air Kiss 技术原理简介

802.11 是 IEEE 制定的无线局域网协议，802.11 以 802.2 的逻辑链路控制封装来携带 IP 封包，因此能够以 802.2 SNAP 格式接收无线网络数据。如果开启 wifi 芯片的混杂模式监听空间中的无线信号，并以 802.2 SNAP 格式从数据链路层截取数据，就会得到如下图所示的数据包：

38-1492bytes

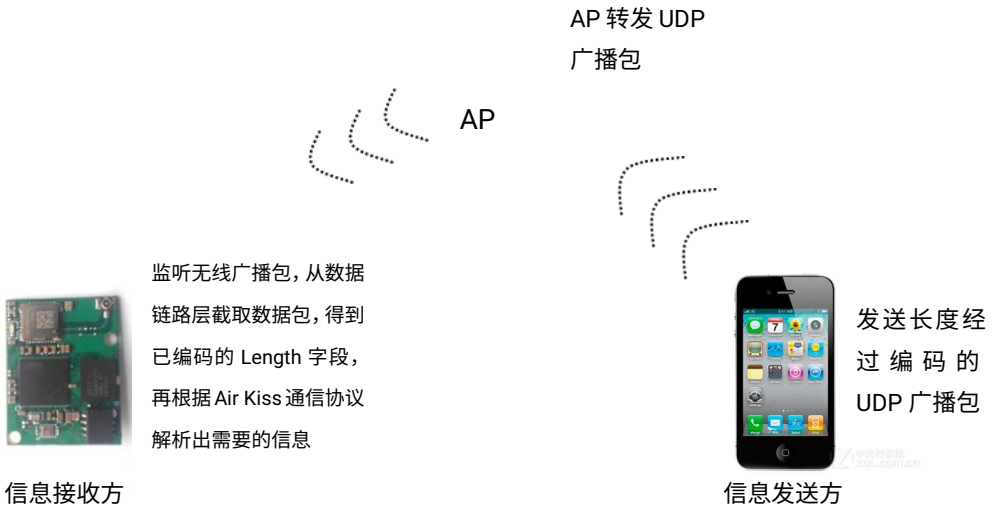
DA	SA	Lengt	LLC	SNA	DAT	FCS
6bytes	6bytes	2bytes	3bytes	5bytes		4bytes

802.2 SNAP 格式数据包

DA 字段表示目标 mac 地址，SA 字段表示源 mac 地址，Length 字段表示后面数据的长度，LLC 字段表示 LLC 头，SNAP 字段包括 3bytes 的厂商代码和 2bytes 的协议类型标识，DATA 字段为负载，对于加密信道来说是密文的，FCS 字段表示帧检验序列。

从无线信号监听方的角度来说，不管无线信道有没有加密，DA、SA、Length、LLC、SNAP、FCS 字段总是暴露的，因此信号监听方便有了从这 6 个字段获取信息的可能。但从发送方的角度来说，由于操作系统的限制(比如 ISO 或者 Android)，DA、SA、LLC、SNAP、FCS 五个字段的控制需要很高的控制权限，发送方一般是很难拿到的。因此只剩下 Length 这一字段，发送方可以通过改变其所需要发送数据包的长度进行很方便的控制。所以，只要制定出一套利用长度编码的通信协议，就可利用 802.2 SNAP 数据包中的 Length 字段进行信息传递。

在实际应用中，我们采用 UDP 广播包作为信息的载体。信息发送方向空间中发送一系列的 UDP 广播包，其中每一包的长度(即 Length 字段)都按照 Air Kiss 通信协议进行编码，信息接收方利用混杂模式监听空间中的无线信号，并从数据链路层截取 802.2 SNAP 格式数据包，便可得到已编码的 Length 字段，随后接收方便可根据 Air Kiss 通信协议解析出需要的信息。整个过程如下图所示：



Air Kiss 技术信息传输过程

二、Air Kiss 通信协议

2.1. 物理层协议

在信号载体方面，采用 wifi 无线信号进行信息传递，1-14 全信道支持。

在信号编码方面，802.2 SNAP 数据包中的 Length 字段为数据发送方唯一可控字段，因此 Air Kiss 通信协议利用发送数据包的长度进行编码。由于受到 MTU 的限制，Length 字段最大可编码位数为 10bit。但实际测试过程中发现，UDP 包长度与丢包率、乱序率成正比。因此本协议中，我们把 Length 字段编码位数限制在 9bit，即 UDP 广播包的发送长度不大于 512 字节。

我们身处的无线网络环境有可能及其复杂，很有可能在同一个空间中存在多个 AP，而这些 AP 又分布在相同或者不同的信道上，这样接收者一开始是不知道发送方在 1-14 哪个信道上发送信息，而且同一个信道上也可能会有很多设备在发送 UDP 广播包。在这种情况下，接收方监听到的数据包是海量的。必须从海量的数据信息中定位出发送方所在的信道和发送方的 mac 地址。另外，由于在 UDP 广播包发送过程中，一个 UDP 层的数据包，要经过 IP 层、数据链路层的封装，并且通过加密(加密方式包括 WPA2、WPA、WEP 三种)后才会被发送出去，所以发送方发送 UDP 广播包的长度与接收方监听 SNAP 包中的 Length 字段值存在差异，这就需要进行转义。然而，由于底层加密方式的不确定性，使得这个差异值也具有不确定性。

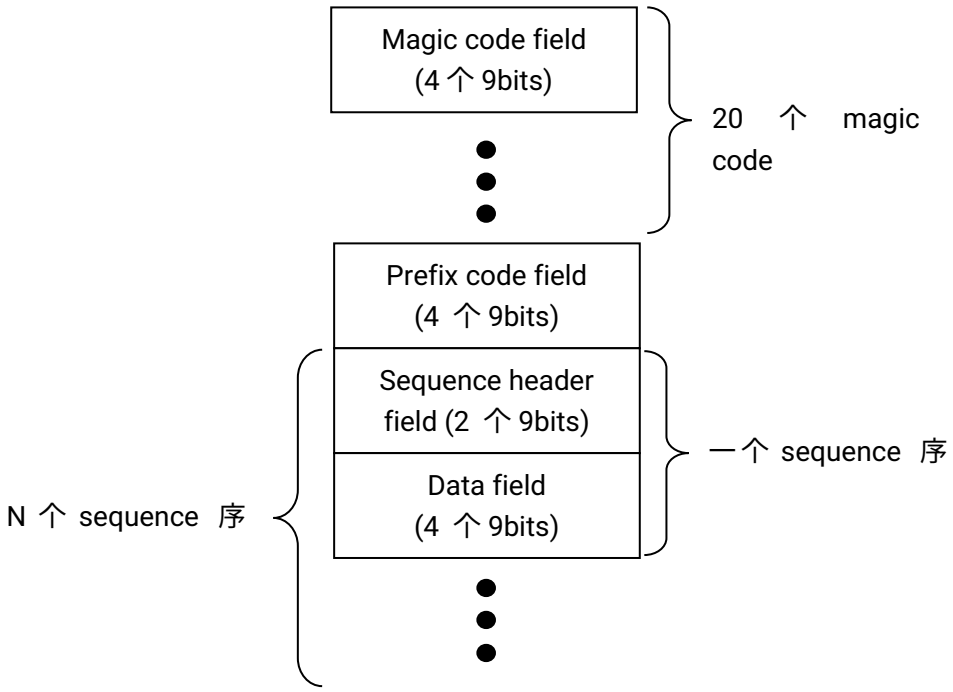
为解决这两个问题，在发送链路层数据（见下节）之前，需要先发送 400ms

的前导域（400ms = 8*50ms，即如果设备端以 50ms 的频率切换信道，则可以覆盖 8 个信道,因为一般用户环境不用监听 14 个信道,所以覆盖 8 个信道足已)。前导域由 4 个字节组成，其值固定为 {1,2,3,4}。接收方在接收到这些前导域数据包后，利用 SNAP 包中的 Length 字段与之相减，从而获取到这个差异值。

举个例子，接受方通过监听，在链路层截获 802.2 SNAP 格式的前导数据包，其 Length 字段的值分别为 53，54，55，56，那差异值就能确定为 53-1=52。之后接收方接收到数据之后都用 SNAP 包的 Length 字段值减去 52，即能得到实际的信息数据。

2.2. 链路层协议

链路层数据结构如下图所示：



链路层数据结构示意图

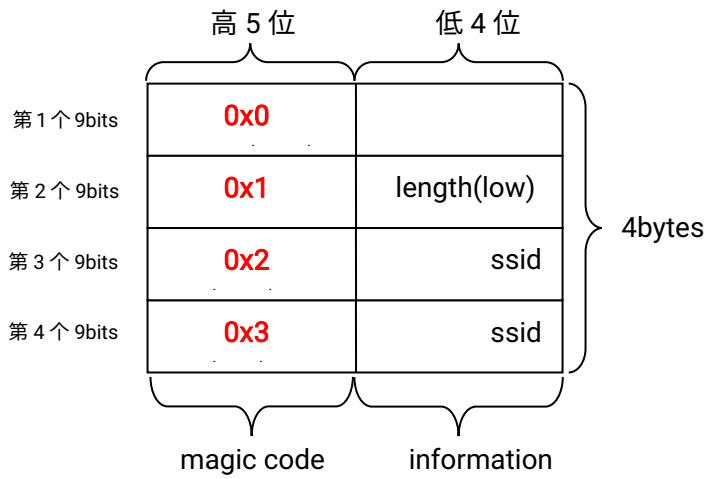
链路层数据结构可分为两类，control 字段与 data 字段，magic code、prefix code、sequence header field 属于 control 字段,data field 属于 data 字段。control 字段与 data 字段以第 8bit 位（最高位）加以区别，该位为 1 表示 data field 字段，为 0 表示 control 字段。在 control 字段中，magic code 字段与 prefix code 字段完全相同，magic code 字段与 sequence header 字段通过第 7bit 位加以区分，

该位为 1 表示 sequence header 字段，为 0 表示 magic code 字段。

以下分别对各个字段进行详细介绍。

⑴magic code 字段

magic code 字段的数据结构如下图所示：



magic code 字段的数据结构

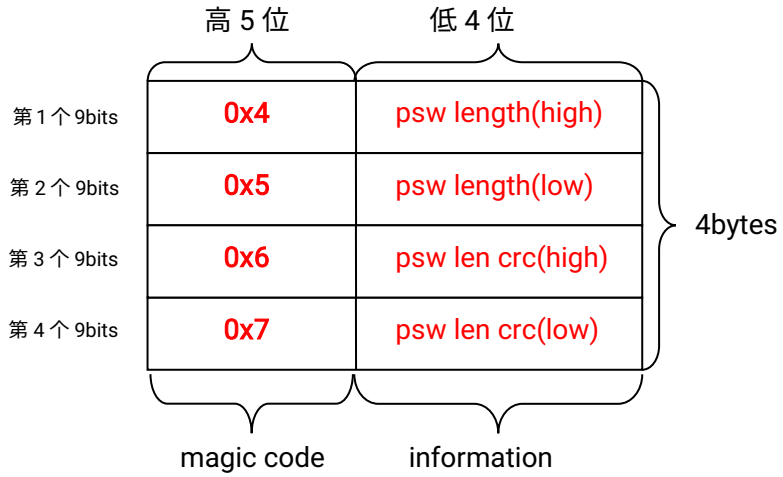
magic code 由 4 个 9bits 组成，每个 9bits 的高 5 位为 magic code 字段，低 4 位为 information 字段。前两个 9bits 的 information 字段分别装载要发送数据长度的高 4 位和低 4 位，后面两个 9bits 的 information 字段分别装载要发送 ssid 的 crc8 值的高 4 位和低 4 位。

这里单独传输 ssid 的 crc8 字段是对整个传输过程所做的优化。在研究中我们发现，在信息传输之前先对 AP 进行扫描，通过获取的 beacon 可以得知无线环境中所有非隐藏 AP 的 ssid、rssi 以及信道。在传输过程中，接收方先从 magic code field 中获取目标 AP ssid 的 crc8 值，然后再和事先扫描所得到的 ssid 的 crc8 值进行比对，如果发现相同值，那么在接下来的接收过程中接收方就不用再接收 ssid 信息，这就大大加快了传输的时间。

在传输过程中，需要发送 5 个 magic code 字段。这里重复发送的原因是 magic code 中的字段很重要，接收端可以通过对比多次接收的结果来保证正确性。

⑵prefix code 字段

prefix code 字段的数据结构如下图所示：



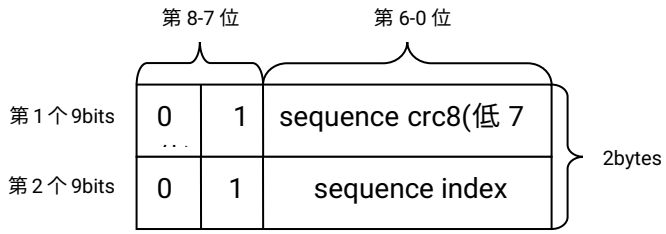
magic code 字段的数据结构

prefix code 由 4 个 9bits 组成，每个 9bits 的高 5 位为 magic code 字段，低 4 位为 information 字段。前两个 9bits 的 information 字段分别装载要发送密码的长度的高 4 位和低 4 位，后面两个 9bits 的 information 字段分别装载发送密码长度的 crc8 值的高 4 位和低 4 位。

prefix code 有两个作用，首先是表示数据序列的正式开始，其次告诉接收端发送密码的长度，以便接收方在接收完数据后，对数据进行分割解密。

⑶sequence header 字段：

sequence header 字段的数据结构如下图所示：



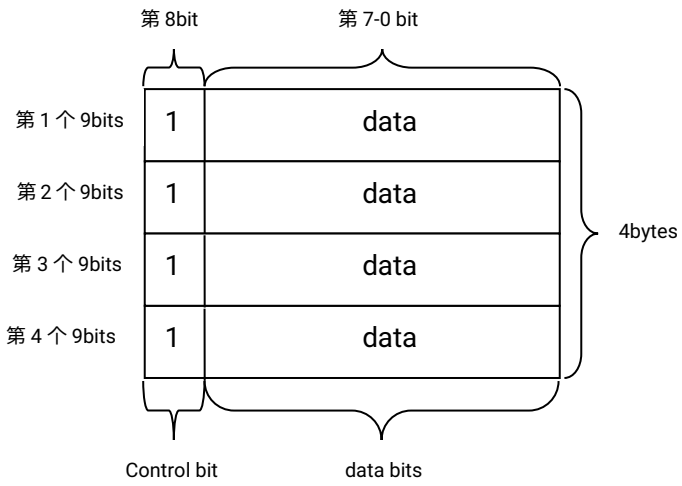
sequence header 字段的数据结构

我们把待发送的数据以 4 为粒度进行划分，每 4 个数据组成一个 sequence，以 sequence 为单位进行数据的发送。每个 sequence 都由 sequence header 字段和 data 字段组成。最后一个 sequence 如果不够 4 个数据，不用补全。

sequence header 字段由两个 9bits 组成，第一个的低 7 位装载的是从本 sequence index 开始到本 sequence 结束发送的所有数据的 crc8 的低 7 位值（计算过程中不计入字段标识位，因此 sequence index 最高位需补 0），在接收完一个 sequence 的数据之后，需进行 crc8 值的效验，如果不相同，证明该 sequence 的数据接收出错，应该丢弃。

⑷data 字段：

data 字段的数据结构如下图所示：



data 字段的数据结构

data 字段由 4 个 9bits 组成，每个 9bits 的第 8 位为控制位，固定为 1，其余的 8 位装载需要传输的数据。

2.3. 应用层协议

送方所要发送的数据由三部分组成：密码、随机数、ssid。其中随机数的作用是，当数据接收方连上 AP 之后，立即发送以该随机数为内容的 UDP 广播包，当发送方收到该广播包后就能确认接收方已经准确接收到所有数据。密码和 ssid 都'\0'结尾，并且分别用 AES 进行加密，再发送。这三部分数据的发送顺序为先发送密码，再发送随机数，最后发送 ssid，如下图所示：

应用层协议示意图

三、Air Kiss 通信协议性能分析

3.1. 纠错能力分析

Air Kiss 技术中的通信模型可以抽象为错误率为 0-5%的单向的信道,所需要传递信息的最大长度为 68bytes。在这种情况下，如果不采用纠错算法，就很难保证在有限次数内完成信息的发送。

Air Kiss 采用了累积纠错算法来保证在有限次内完成传输过程。累积纠错算法的理论基础为：多轮数据发送过程中，在同一位数据上发生错误的概率是很低的。因此可以累积多轮的数据传递结果进行分析，其中一轮中某一位错误数据有很大的概率能其它轮中找到其对应的正确值，这样就能保证在有限次内完成信息的发送。

假定需要传递信息的长度为 68bytes，我们计算了在最坏的情况下，使用累积纠错算法与不使用累积纠错算法信息发送成功的概率与发送次数的关系，结果如下表所示：

Air Kiss 纠错能力分析表

发送次数	使用累积纠错成功率	不使用累积纠错的成功率
1	3%	3%

2	81%	3%
3	98%	3%
4	99.9%	3%
5	99.999%	3%

3.2. 基本性能分析

Air Kiss 技术的传输速率取决于信息发送方 UDP 广播包的发送速率，目前广播包的发送频率为 5ms 发送一个，因此其传输速率为 200bytes/s。在不计算 magic code field 的情况下，负载效率为 66.7%。

从纠错能力的分析可能，如果发送信息长度为最长的 68bytes，那么在最坏情况下，最多需要 5 次就可以完成信息发送，最大的传输时间需要 2.039s。