LAB 3–WLAN 协议的测试和分析

张煌昭，1400017707，元培学院

摘要—本次 Lab 使用 Wireshark 软件对已经抓取好的 WLAN 数据（Wireshark_802_11.pcap）的信标帧，数据传输过程及关联和去关联过程等进行分析，并使用 Wireless-Mon 软件对 Wifi 信号强度进行分析。本次报告使用 Overleaf L^AT_EX 在线平台编写[1]。

I. 802.11 帧结构

802.11 帧的结构固定，如表 I所示，一个完整的 802.11 帧包括**帧控制**（Frame control，I-A节），**持续期**（Duration ID，I-B节），**地址 1**（Addr 1，I-C节），**地址 2**（Addr 2，I-C节），**地址 3**（Addr 3，I-C节），**序号控制**（Seq control，I-D节），**地址 4**（Addr 4，I-C节），**有效载荷**（Payload，I-E节）和**循环冗余校验码**（CRC，I-E节）几个字段。下面对 802.11 帧各个字段和子字段进行详细的介绍。[2]

A. 帧控制字段

帧控制字段被用来确定帧的各类属性，以及确定帧的类型等，各个子字段即其含义和功能如表 II所示。

一般而言，802.11 帧按功能可以分作数据帧，管理帧和控制帧，帧的类型由**类型**和**子类型**子字段确定。802.11 帧的 MAC 地址版本由**协议版本**子字段确定。**到 AP** 和**从 AP** 子字段确定该帧来自还是送往 AP。**重试**子字段指示该帧是否需要重传。**功率管理**用来指出发送端在完成当前的原子帧交换之后是否进入省电（power-save）模式。如果帧受到链路层安全协议的保护，设置 **WEP** 子字段。如果要求帧严格地依次传送，则设置 **Rsvd** 子字段。

B. 持续期字段

802.11 协议允许传输节点预约信道，并保留一段时间用于传输帧以及等待传输确认。这一持续时间值被放置于持续期字段中，不论数据帧还是控制帧或管理帧，这一字段均存在。

C. 地址 1∼4 字段

802.11 协议需要使用 4 个地址字段，而非以太网中的两个（源 MAC 和目的 MAC），是因为将网络层数据报从无线站点通过 AP 送至一个路由器接口时，需要 3 个地址字段。对此的解释如下。

AP 是链路层设备，它并不支持 IP 地址，因此考虑将数据报从路由器移至无线站点的情况。路由器并不知道 AP 的存在，因此其按照以太网协议进行处理，通过获取 H1 的 MAC 地址后，将数据报封装在以太网帧之中，该帧具有两个地址字段，一个是路由器的源 MAC 地址，一个是无线站点的目的 MAC 地址。以太网帧顺着链路到达 AP，AP 需要其转换为 802.11 帧后再由无线信道发出，为了能够标记链路，必须将 AP 的 MAC 地址也记录在帧中，因此需要使用 3 个地址字段，分别为路由器源 MAC，无线站点目的 MAC，和 AP 的 MAC 地址。通过 AP 的 MAC，无线站点可以确定将数据报发回路由器的 MAC 地址。

地址 1 和**地址 2** 字段，对应以太网帧中的源 MAC 地址和目的 MAC 地址两个地址字段。在上文中对**地址 3** 字段的作用进行解释，在有线局域网互联和 BSS 中其作用十分重要。802.11 帧中的**地址 4** 字段，是 Ad Hoc 模式下，相互转发时标记 MAC 所使用的，基础设

表 I
802.11 帧结构

字段	长度/Byte	功能
帧控制	2	802.11 协议控制字段，包括多个子字段
持续期	2	传输节点预约信道的保持时间
地址 1	6	目的端地址，即负责将帧交付上层处理站点
地址 2	6	源端地址，即帧传送的来源站点
地址 3	6	接收端地址，负责处理该帧的站点
序号控制	2	区分重传帧和新帧，以及丢弃重复帧
地址 4	6	发送端地址，将帧传送至无线媒介的站点
有效载荷	0∼2312	IP 数据报/ARP 分组，802.11 帧的核心
CRC	4	循环冗余校验码，检验和纠正错误 bit

[1]本报告源码可通过以下 git 命令获得，
git clone https://git.overleaf.com/15239115cwnhdmxtwshf

[2]Kurose, J. F., Ross, K. W., and Chen Ming. 计算机网络：自顶向下方法（第六版）. 2008. 356-358

表 II
802.11 帧控制字段结构

子字段	长度/bit	功能
协议版本	2	标明该帧所使用的 MAC 版本
类型	2	标明使用的帧的类型
子类型	4	标明使用的帧的类型
到 AP	1	标明帧送往 AP
从 AP	1	标明帧来自 AP
更多标识	1	
重试	1	标明该帧是否需要重传
功率管理	1	标明完成当前的原子帧发送进入省电模式
贡多数据	1	标明至少有一个帧待传经过休眠中的工作站
WEP	1	标明帧受到链路层安全协议的保护
Rsvd	1	标明帧严格依次传送

施网络一般只使用前三个地址字段，而不使用地址 4 字段。

D. 序号控制字段

由于 802.11 网络中，无论站点在何时收到一个来自其他站点的帧，都会回发一个确认，同时由于传送过程中无线传输丢失的概率较大，因此发送站点会发送同一个帧的多个副本。序号控制字段，使得接收方可以区分新传输的帧和以前的重传的帧，从而接收新帧丢弃旧帧。

E. 有效载荷字段和 CRC 字段

有效载荷为一个 IP 数据报或一个 ARP 分组组成，这一字段是帧的核心。尽管其允许的最大长度为 2312 字节，但实际使用时，通常就是一个 IP 数据报或 ARP 分组的长度，远远达不到最大长度。

CRC 字段使用 32 位的循环冗余码进行校验和纠错。由于无线传输发生错误的概率相比有线传输会大得多，因此需要使用一种可靠的纠错机制，该 CRC 校验码可以检查并纠正 32 位突发错以下的错误，因此非常有用。

II. 802.11 帧类型

一般地，按照功能将 802.11 帧分作 3 类——数据帧，控制帧，和管理帧。其中数据帧（II-A节）包含需要传输的数据，控制帧（II-B节）用于协助和控制数据帧的传输，管理帧（II-C节）用于建立网络连接等设备管理。

表 III
802.11 帧地址字段在数据帧中的使用

功能	Addr1	Addr2	Addr3	Addr4
IBSS	目的地址	源地址	BSSID	未使用
To AP	BSSID	源地址	目的地址	未使用
From AP	目的地址	BSSID	源地址	未使用
WDS	接收端地址	发送端地址	目的地址	源地址

A. 数据帧

数据帧的类型子字段固定为 11。对于不同类型的数据帧，地址字段的用法也不同，如表 III所示。To AP 和 From AP 为 802.11 帧的基础结构，不进行赘述。

WDS（无线分布式系统），是一种 Ad Hoc 网络，其使用多台 AP 进行桥接，通过 AP 的中继连接，扩大信号覆盖。IBSS（独立基本服务集），又称特设模式，是一种专用的点对点连接。IBSS 没有无线基础设施骨干，但至少需要 2 台无线站点才能建立连接。在 IBSS 模式之下，无线站点之间点对点直接建立连接。

B. 控制帧

控制帧的类型子字段固定为 01，根据不同的控制帧，设置子类型子字段。控制帧具有四个子类型，分别介绍如下：

RTS 帧子类型为 1011，用于获取无线信道控制权。其具有帧控制，持续期，地址 1，地址 2，和 CRC 字段，长度固定为 20 字节。

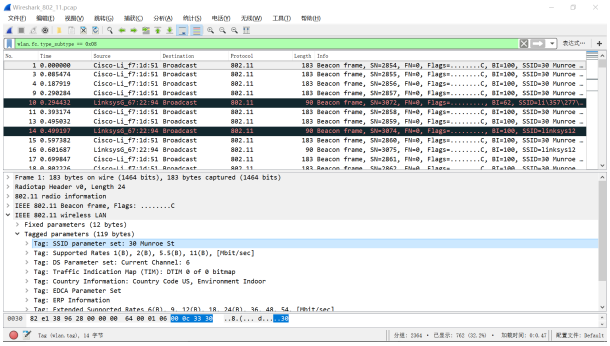
CTS 帧子类型为 1100，用于回复 RTS 帧，802.11 协议规定没有 RTS 帧就没有 CTS 帧。CTS 帧具有镇控制，持续期，地址 2，和 CRC 字段，长度为 14 字节，其中地址 3 字段为接收端字段，对应应答的 RTS 的发送端字段（地址 1）。

ACK 帧子类型为 1101，用于 MAC 及任何数据传输所需要的肯定确认。和 CTS 具有相同的字段。

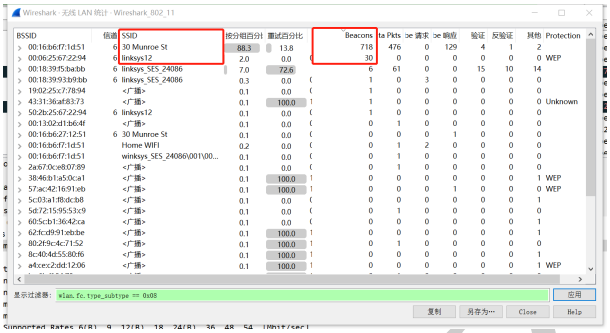
PS-Poll 帧子类型为 1010，用于无线站点从省电模式苏醒后，从 AP 获取缓存帧。具有帧控制，持续期，地址 2，地址 3，和 CRC 字段，长度固定为 20 字节。

C. 管理帧

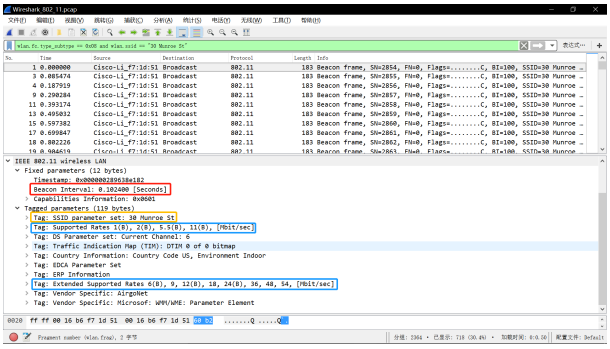
802.11 协议的网络设备管理过程大致可以分作 3 步，首先无线站点找到周围可访问的无线网络，其次网络系统对无线站点进行验证，最后无线站点与 AP 建立关联开始网络传输。管理帧的类型固定为 00。Association Request（子类型 0000），Probe Request



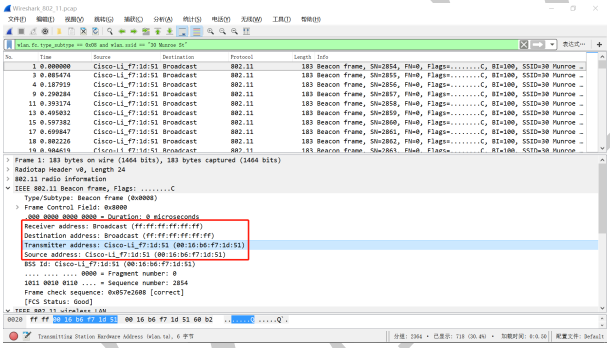
(a) Beacon 帧



(b) SSID 统计



(c) Beacon 间隔



(d) 地址字段

图 1. 使用 Wireshark 对抓取的 Wireshark_802_11.pcap 数据进行分析。图 1(a)为过滤出 Beacon 帧的结果。图 1(b)为对 Beacon 帧的 SSID 的统计结果，用红框圈出出现最多的两个 SSID。图 1(c)中红框圈出帧中标明的该 AP 的 Beacon 间隔时间，黄框圈出该帧的 SSID，蓝框圈出其支持的数据率和可拓展的数据率。图 1(d)为 Beacon 帧中 MAC 地址字段，用红框圈出。

(子类型 0100)，以及 Beacon（子类型 1000）等帧均属于管理帧。

III. 对 Beacon 帧的分析

使用 Wireshark_802_11.pcap 抓取的 802.11 帧进行分析。首先设置过滤器为 “wlan.fc.type_subtype == 0x08”，使其只显示 Beacon 帧[3]，得到所有的 Beacon 帧如图 1(a)所示。其中 IEEE 802.11 Wireless LAN / Tagged Parameters 内容下可以获得该 Beacon 帧的 SSID，图中编号为 1 的 Beacon 帧的 SSID 为 “30 Munroe St”。

对 Beacon 帧的 SSID 使用频率进行统计，使用 “无线/WLAN 流量” 工具进行统计，设置过滤器，并制定按照 Beacon 数目排序，得到的结果如图 1(b)所示。根据图可以发现，Beacon 帧中最常用的 SSID 为 “30 Munroe St” 和 “linksys12”，其中 “30 Munroe St 占绝大多数”。

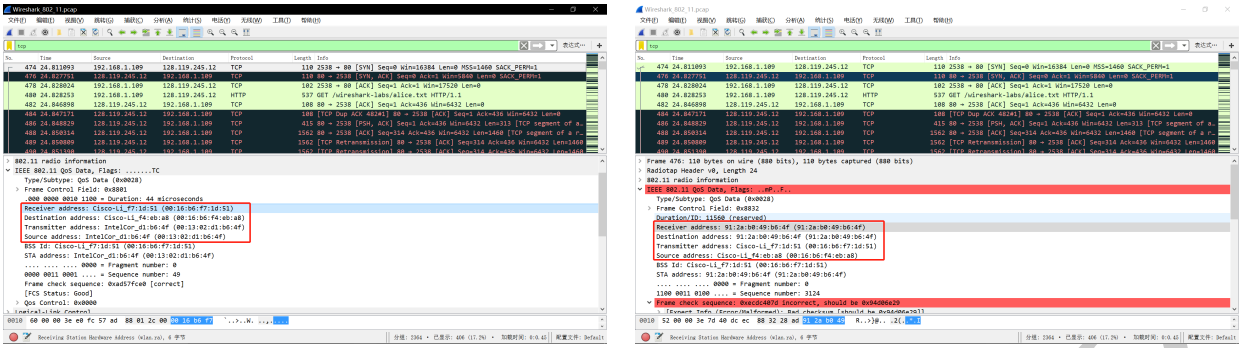
接下来将过滤器中再设置为 “wlan.fc.type_subtype == 0x08 and wlan.ssid == “30 Munroe St””，过滤出 SSID 最多的 Beacon 帧，如图 1(c)所示。选择其中一帧查看 Beacon 帧 IEEE 802.11 Wireless LAN / Fixed Parameters 下 Beacon Interval，发现该 SSID 的 Beacon 帧间隔为 0.1024 sec（图 1(c)中黄框圈出），检查各帧捕获时间的间隔，基本符合。在 IEEE 802.11 Wireless LAN / Tagged Parameters 下发现 Supported Rates 和 Extended Supported Rates，该帧支持的数据率和扩展数据率（图 1(c)中蓝框圈出）分别为 1.0，2.0，5.5，11.0Mbps 和 6.0，9.0，12.0，18.0，24.0，36.0，48.0，54.0Mbps。

在 IEEE 802.11 Beacon Frame 下查看各个地址字段，如图 1(d)所示。发现接收端 MAC 和目的 MAC 地址均为 Broadcast（ff:ff:ff:ff:ff:ff），发射端 MAC 和源 MAC 地址均为 Cisco-Li_f7:1d:51（00:16:b6:f7:1d:51）。

IV. 对 TCP 传输过程的分析

首先设置过滤器为 “tcp” 过滤包含 TCP 协议层的帧。发现第 480 帧为包含下载 alice.txt 的 HTTP 请求的帧（如图 2），向前寻找相应的 TCP SYN 帧，位于第 474 帧，与该帧对应的 TCP SYN ACK 帧位于第 476 帧。

[3]参考 https://blog.csdn.net/chaehom/article/details/22435953



(a) TCP SYN (b) TCP SYNACK

图 2. TCP SYN 发送和 TCP SYNACK 接收。图 2(a)为第 474 帧，主机发送 TCP SYN 的 802.11 数据帧内容，其中地址字段内容用红框圈出。图 2(b)为第 476 帧，主机接收 TCP SYNACK 的 802.11 数据帧内容，其中地址字段内容用红框圈出。

查看第 474 帧，该帧为 802.11 数据帧，其上具有 IPv4 层和 TCP 层，TCP 层内容为发送 TCP SYN。查看其 802.11 帧结构，如图 2(a)所示，其源 MAC 地址字段为 IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)，接收端 MAC 地址字段为 Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)，目的 MAC 地址字段为 Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)。由于 TCP SYN 是客户端向服务器端发送的握手信号，因此无线主机的 MAC 地址为 IntelCor_d1:b6:4f，第一跳路由器的 MAC 地址为 Cisco-Li_f4:eb:a8；又由于在第I-C节介绍的三地址机制，AP 的 MAC 地址为接收端地址，为 Cisco-Li_f7:1d:51。

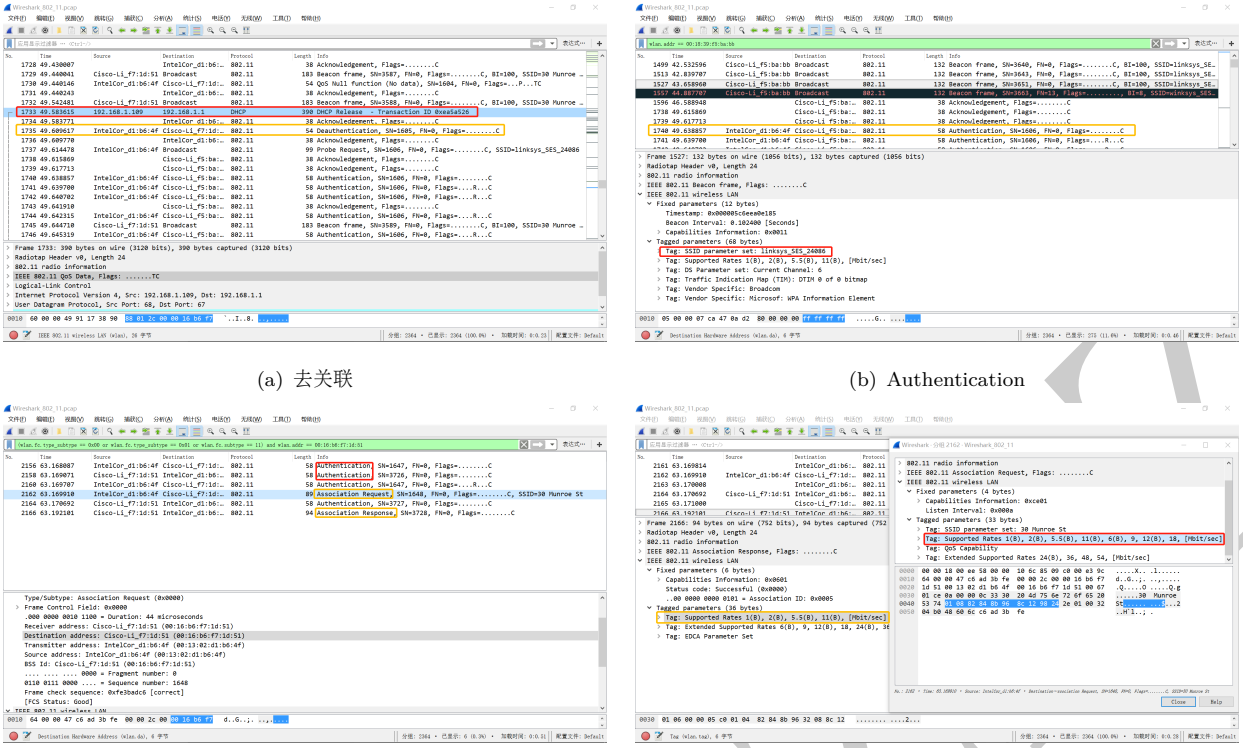
考虑这一 TCP SYN 请求的主机 IP 和目的 IP。通过图 2(a)发现 TCP SYN 请求的主机 IP 为 192.168.1.109，目的 IP 为 128.119.245.12。显然主机 IP 对应了无线主机的 IP，目的 IP 对应了服务器 IP。由于 IP 是网络层上的概念，因此这一对 IP 地址对应客户端和服务器端的 IP 地址，而和 AP 和第一跳路由器等无关。在 cmd 使用 nslookup 查看 128.119.245.12 对应的域名位 gaia.cs.umass.edu。使用浏览器访问该网址寻找 alice.txt，并未直接找到，猜测其可能位于 wireshark-labs 目录之下，访问以下网址 http://gaia.cs.umass.edu/wireshark-labs/alice.txt，找到 <ALICE'S ADVENTURES IN WONDERLAND> 的文本文件。

```
$> nslookup 128.119.245.12
服务器:  UnKnown
Address:  115.27.254.4
名称:    gaia.cs.umass.edu
Address:  128.119.245.12
```

查看第 476 帧，该帧也为 802.11 数据帧，其上具有 IPv4 和 TCP 层，TCP 层内容为接收 TCP SYNACK。查看其 802.11 帧结构，如图 2(b)所示，其源 MAC 地址字段为 Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)，发送端 MAC 地址字段为 Cisco-Li_f7:1d:51(00:16:b6:f7:1d:51)，目的 MAC 地址为 91:2a:b0:49:b6:4f。由于 TCP SYNACK 是服务器端向客户端回发的确认信号，因此无线主机的 MAC 地址为 91:2a:b0:49:b6:4f，AP 的 MAP 地址为 Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)，第一跳路由器的 MAC 地址为 Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)。与前文相反，源 IP 地址为 128.119.245.12，对应服务器端 IP 地址，目的 IP 地址为 192.168.1.109，对应无线主机 IP 地址。

发现 TCP SYN 和 TCP SYNACK 的两帧 802.11 帧的无线主机的 MAC 地址不同，发送时 MAC 地址为 00:13:02:d1:b6:4f，而接收时 MAC 地址为 91:2a:b0:49:b6:4f。猜测可能是由于捕获产生 Wireshark_802_11.pcap 的计算机中具有两块无线网卡，一块为 Intel 主板上的集成网卡（因此 Wireshark 可以识别其 MAC 地址为 IntelCor），另一块为主板外的独立网卡。下面通过实验进行验证和说明。

设置过滤器为 "wlan.addr == 91:2a:b0:49:b6:4f"，过滤包含 "独立网卡" 的 MAC 地址字段的帧，发现只有 476 一帧。因此基本可以认定两张网卡的猜测不成立，91:2a:b0:49:b6:4f 并不对应一张网卡，而是由于传输错误引起的，第 476 帧为错帧 (如图 2(b))，该 802.11 帧的 CRC 校验出错。设置过滤器为 "wlan.addr == 00:13:02:d1:b6:4f and wlan.addr == 00:16:b6:f7:1d:51"，过滤包含 IntelCor_d1:b6:4f 网卡 MAC 地址字段的帧，发现第 466 帧为 ARP 帧，发送广播询问 IP 对应的



(a) 去关联 (b) Authentication

(c) 重新关联 (d) 速率协商

图 3. 关联与去关联的分析。图 3(a)为去关联过程捕获的帧，其中红框圈出 IP 层 DHCP Release 注销 IP，黄框圈出 802.11 层 Deauthencation 帧断开 WLAN 连接。图 3(b)为发现主机向 AP: linksys_ses_24086 发送 Authentication 帧的过程，红框圈出确认 AP 的 SSID，黄框圈出 Authentication 帧。图 3(c)为重新和 AP: 30 Munroe St 连接的过程，红框圈出认证的 Authentication 帧，黄框圈出正式建立连接的 Association 帧。图 3(d)为主机和 AP 协商传输速率的过程，红框圈出主机支持的速率，黄框圈出 AP 支持的速率。

MAC 地址，之后 470 和 472 帧为 DNS 解析的请求和回应，474 和 478 帧对应 TCP 请求的第一次 SYN 握手和第三次 ACK 握手，缺少第二次 SYNACK 握手。而错误的 476 帧对应了 TCP 请求的第二次 SYNACK 握手，一般而言，错误帧会丢弃重传，而在本实验中，主机可能对错误帧进行了纠错，从而恢复了第 476 帧的 TCP SYNACK 第二次握手。

V. 对关联与去关联的分析

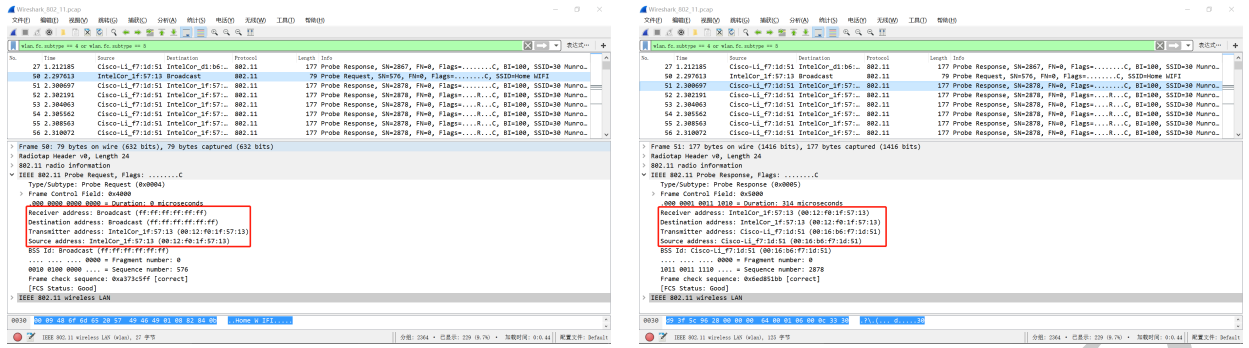
A. *802.11 协议关联和去关联的过程*

主机接入一无线网络的关联过程通过 802.11 管理帧完成，具体的过程如下：1. AP 定期发送 Beacon 帧广播，表明自身的 MAC 地址等，假设某一时刻无线主机网卡接收到 Beacon 帧，之后该 AP 所对应的网络显示在该主机的“可用的无线网络连接列表”；2. 另一种情况下，主机主动扫描周围 AP，广播发送 Probe Request 帧，接收到的 AP 回复 Probe Response 帧，从而使得主机发现该 AP；3. 主机发现 AP 后，发送 Authentication 帧要求进行身份验证，即进行 WiFi 密码验证等，主机接收后进行验证并回发 Authentication 帧作为身份验证的响应；4. 若身份验证成功，则主机发送 Association 帧正式请求建立连接，接入 WLAN 中，AP 回发 Association Response 对其进行回应，并正式建立 WLAN 连接，之后进行正常的数据传输。

去关联的过程相对简单，因为去关联基本不需要进行验证等操作，分作两种情况——主动断开和被动断开。当用户选择“断开连接”后，无线主机向 AP 发送 Disassociation 帧，AP 接收后直接断开连接，不再回发任何管理帧；而当用户远离 AP 信号覆盖范围后，一段时间阈值后 AP 检测不到该无线主机，则自动断开，不需要主机发送 Disassociation 帧。

B. *实验分析*

对 49s 后的去关联过程进行分析。首先分析 802.11 层的去关联动作，设置过滤器为 “wlan.fc.type == 0 and wlan.fc.type_subtype != 8”，滤出所有非 Beacon 帧的 802.11 管理帧，方便寻找和去关联相关的帧。发现第 1735 帧为 Deauthentication 帧，该帧之后的 1737 帧为另一 SSID 的 Probe Request 帧，说明第 1735 帧后主机断开了与 Cisco-Li_f7:1d:51（00:16:b6:f7:1d:51）AP



(a) Probe Request 帧 (b) Probe Response 帧

图 4. Probe 帧。图 4(a)为捕获到的第一个 Probe Request 帧，红框圈出该帧的 MAC 地址字段内容。图 4(b)为 AP 回复的 Probe Response 帧，红框圈出该帧的 MAC 地址字段内容。

的连接。接下来对 IP 层进行的去关联动作进行分析，设置过滤器为“ip”，只选择 IP 层协议相关的帧。发现 1733 帧 IP 层为 DHCP Release 数据报，该数据报的作用是释放 IP。综上所述，49s 后选择了断开网络连接，之后主机先发送 DHCP Release 数据报释放分配的 IP，断开网络层连接之后发送 Deauthencation 帧断开 802.11 层连接，如图 3(a)所示。

设置过滤器为“wlan.fc.type_subtype == 11”过滤 Authentication 帧，寻找主机建立的新的 WLAN 连接。发现 49s 断开连接之后，无线主机又在 1740 帧发送 Authentication 帧，查看该帧发现目的地址字段为 Cisco-Li_f5:ba:bb（00:18:39:f5:ba:bb），该 MAC 地址与之前的 AP 的 MAC 地址不同。接下来设置过滤器为“wlan.addr == 00:18:39:f5:ba:bb and wlan.fc.type_subtype == 0x08”，寻找该 MAC 的 AP 的 Beacon 帧，从 Beacon 帧中便可以获知其 SSID。发现第 1527 帧，为来自该 MAC 地址的 Beacon 帧，查看 SSID 正是所寻找的 AP: linksys_ses_24086。综上，主机在第 1740 帧向 AP: linksys_ses_24086 发送 Authentication 帧请求身份验证，整个过程如图 3(b)所示。

查看第 1740 帧的 Authentication 帧的 IEEE 802.11 Wireless LAN / Fixed Parameters 下内容，发现“Authentication Algorithm: Open System (0)”，即主机不需要提供密码，认证过程是开放的。由于是开放认证，所有认证都会直接通过，因此可能可以允许 AP 不作回复，无线主机直接默认认证成功，事实上该 Authentication 帧未收到 AP 的回复 Authentication 帧，而且该帧的状态直接被主机设置为“Successful”而非待验证。

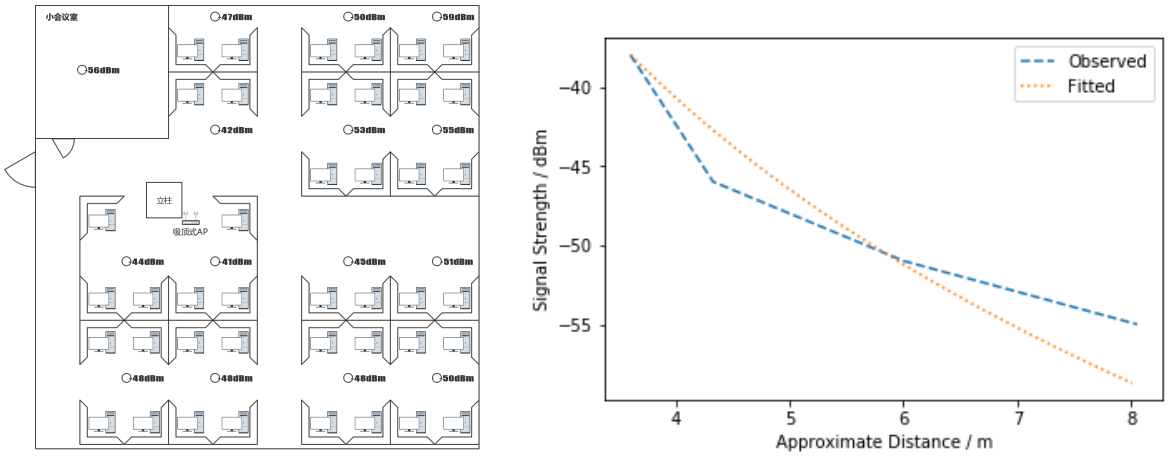
第 2142 帧，主机向 linksys_ses_24086（00:16:b6:f7:1d:51）AP 发送 Deauthentication 断开 WLAN 连接。设置过滤器为“(wlan.fc.type_subtype == 0x00 or wlan.fc.type_subtype == 0x01 or wlan.fc.type_subtype == 11) and wlan.addr == 00:16:b6:f7:1d:511”，过滤主机重新连接 AP: 30 Munroe St 时的 Authentication 帧，Association Request 帧和 Association Response 帧，发现第 2156 和第 2158 帧分别为无线主机向 AP 发送和 AP 回复的 Authentication 帧，第 2162 帧为主机发送的请求关联的 Association Request 帧，第 2166 帧为 AP 回复的 Association Response 帧，过程如图所示。

再对第 2162 帧和 2166 帧进行深入分析，对其传输速率的沟通过程进行分析。查看 IEEE 802.11 Wireless LAN / Tagged Parameters，发现有主机和 AP 支持的速率，如图 3(d)所示。主机在 Association Request 帧中说明其支持的速率为 1,2,5.5,11,6,9,12,18Mbps，AP 在 Association Response 帧中说明其支持的数据率为 1,2,5.5,11Mbps。之后在传输时，二者会选择共有的可支持的速率进行数据传输。

VI. 对 PROBE 帧的分析

A. *Probe* 帧的作用

在第V-A中已经介绍过建立 WLAN 连接的过程，其中的一步就是需要主机知道周围 AP 的存在，有两种方法对此进行实现：1. 被动扫描，即 AP 广播发送 Beacon 帧，主机在接收 Beacon 帧后才知道 AP 的存在；2. 主动扫描，主机广播发送 Probe Request 帧，扫描周围 AP，周围 AP 接收到后回复 Probe Response 帧说明自己的存在。二者各有优势，主动扫描下主机更



(a) 各工位 WLAN 信号强度　　(b) WiFi 信号强度-距 AP 距离曲线

图 5. WiFi 信号强度。图 5(a)为对理科一号楼 1726 实验室内各工位处 Wireless PKU 信号强度的测量，图中小圈为测量位置。图 5(b)为距 AP 距离对 WiFi 信号强度的影响曲线，横轴为距离，单位米（m），纵轴为信号强度，单位 dBm。其中蓝色长虚线为根据测量值绘制的曲线，黄色短虚线为拟合的曲线。

为主动，并且不需要主机频繁接收 Beacon 帧，AP 安全性高，因为其可以选择对危险 Probe 不进行回复，但主动扫描下，AP 可以通过 Probe 收集用户的信息；相对的，被动扫描下 AP 可以通过增大 Beacon 间隔达到节点的目的，用户可以选择只响应安全的 Beacon，隐藏性和安全性较好，但无法发现隐藏的 AP。

Probe 帧，使得主机可以主动扫描周遭 AP，从而连接一些隐藏的 AP（不广播 Beacon 的 AP），从而建立一些较为安全和高效的网络连接。

B. 实验分析

将过滤器设置为 “wlan.fc.subtype == 4 or wlan.fc.subtype == 5”，过滤出所有的 Probe Request 帧和 Probe Response 帧。发现第 50 帧为第一个 Probe Request 帧，第 51 帧为对其的 Probe Response 回复帧，如图 4所示。

Probe Request 帧的源 MAC 地址为 IntelCor_1f:57:13（00:12:f0:1f:57:13），由于 Probe Request 帧为广播发送，因此其目的 MAC 地址和接收端 MAC 地址都是 Broadcast（ff:ff:ff:ff:ff:ff），如图 4(a)所示。Probe Request 帧广播发送，主动扫描周围 AP。Probe Response 帧的源 MAC 地址和发送端 MAC 地址都为 Cisco-Li_f7:1d:51 （00:16:b6:f7:1d:51），目的 MAC 地址为 IntelCor_1f:57:13（00:12:f0:1f:57:13）。Probe Response 帧为 AP 对主动扫描的响应，表明其存在。

VII. 对 WiFi 信号强度的分析

使用 WirelessMon 软件测量 WiFi 信号强度，进行实验的无线网络环境为理科一号楼 1726 实验室，测试 WLAN 网络为 Wireless PKU 网络，无线设备通过位于房间中部的吸顶式 AP 接入 WLAN 网络。实验室房间结构及各个工位信号强度示意图如图 5(a)所示。

测量 WiFi 信号强度与距 AP 距离的关系，测量曲线如图 5(b)中蓝色曲线所示。由于没有精确测量距离，导致导致会有较大的误差，但总体上而言，随着 WiFi 信号强度与距 AP 距离呈现近似对数衰减的关系。使用路径损失模型[4]（path loss model），信号衰减如 1式所示，其中 d 为待测位置，d_0 为参考位置，$\bar{PL}(d)$ 为待测位置的信号强度，单位为 $[dB]$，$\bar{PL}(d_0)$ 为参考位置的信号强度，n 为衰减系数。根据该模型进行拟合，得到的曲线如图 5(b)中黄色曲线所示

$$\bar{PL}(d) = \bar{PL}(d_0) + 10 \cdot n \cdot \log \frac{d}{d_0} \tag{1}$$

使用不同材质的障碍物进行遮挡，测量信号强度的衰减，得到的结果如表 IV所示。由于并不能保证遮挡前后直线距离保持不变（比如使用墙壁遮挡），因而这一实验误差很大，仅能作为定性实验，而不能作为定量实验。

[4]Seidel S Y, Rappaport T S. 914 MHz path loss prediction models for indoor wireless communications in multifloored buildings[J]. IEEE transactions on Antennas and Propagation, 1992, 40(2): 207-217.

表 IV
不同的障碍物引起的 WiFi 信号强度的衰减

障碍物	遮挡前信号强度	遮挡后信号强度
立柱	-45dBm	-54dBm
玻璃幕墙	-43dBm	-53dBm
墙壁	-52dBm	-64dBm
防盗门	-53dBm	-60dBm

VIII. 参考文献和资料

[1] James F. Kurose, and Keith W. Ross. 计算机网络: 自顶向下方法（原书第六版）. 机械工业出版社, 2008.

[2] wireshark 中无线帧的类型、子类型对照表. https://blog.csdn.net/chaehom/article/details/22435953

[3] Seidel S Y, Rappaport T S. 914 MHz path loss prediction models for indoor wireless communications in multifloored buildings[J]. IEEE transactions on Antennas and Propagation, 1992.