

Security in the open environment

IEEE 802.11 Availability Issues

海南大学2014级CS 3班 许若梦

THE BEGINNING

- 如果站在更高的角度来思考的话，很难不提到 1887 年的德国，赫兹在莱茵河边的卡尔斯鲁厄这座小城所做的一个实验。

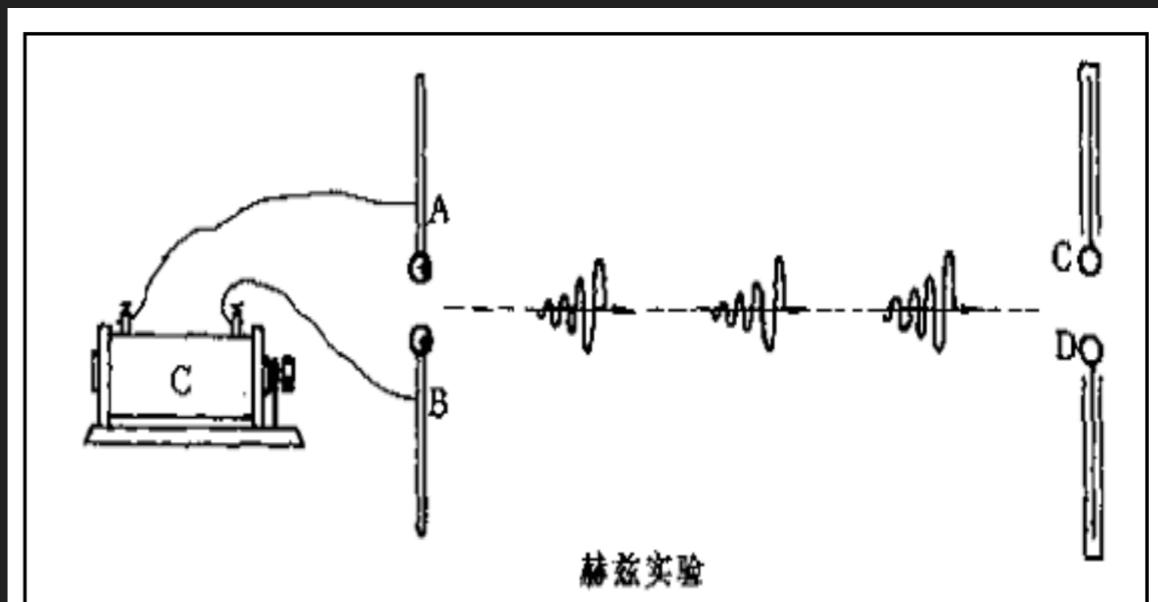


图 1.1(a) 赫兹实验原理图：A、B 是中间留有小空隙(约 0.1mm)的铜棒，分别接到高压感应圈的两电极上，感应圈上的周期性电压加到两棒间的空气隙上，当电压升高到空气被击穿时，电流就往复地通过空气隙而发生火花，这时就相当于一个振荡偶极子，发射间断性的作减幅振荡的电磁波.如果用一个不接感应圈的相同结构的偶极子 CD 来接收，适当调节接收偶极子的位置、取向和长度，可以使它发生共振，在气隙间产生放电火花，证实振荡偶极子能够发射电磁波.

THE GOLDEN AGE

▶ 赫兹注视了足足有一分钟之久，在他眼里，那些蓝色的火花显得如此地美丽。终于他揉了揉眼睛，直起腰来：现在不用再怀疑了，电磁波真真实实地存在于空间之中，正是它激发了接收器上的电火花。

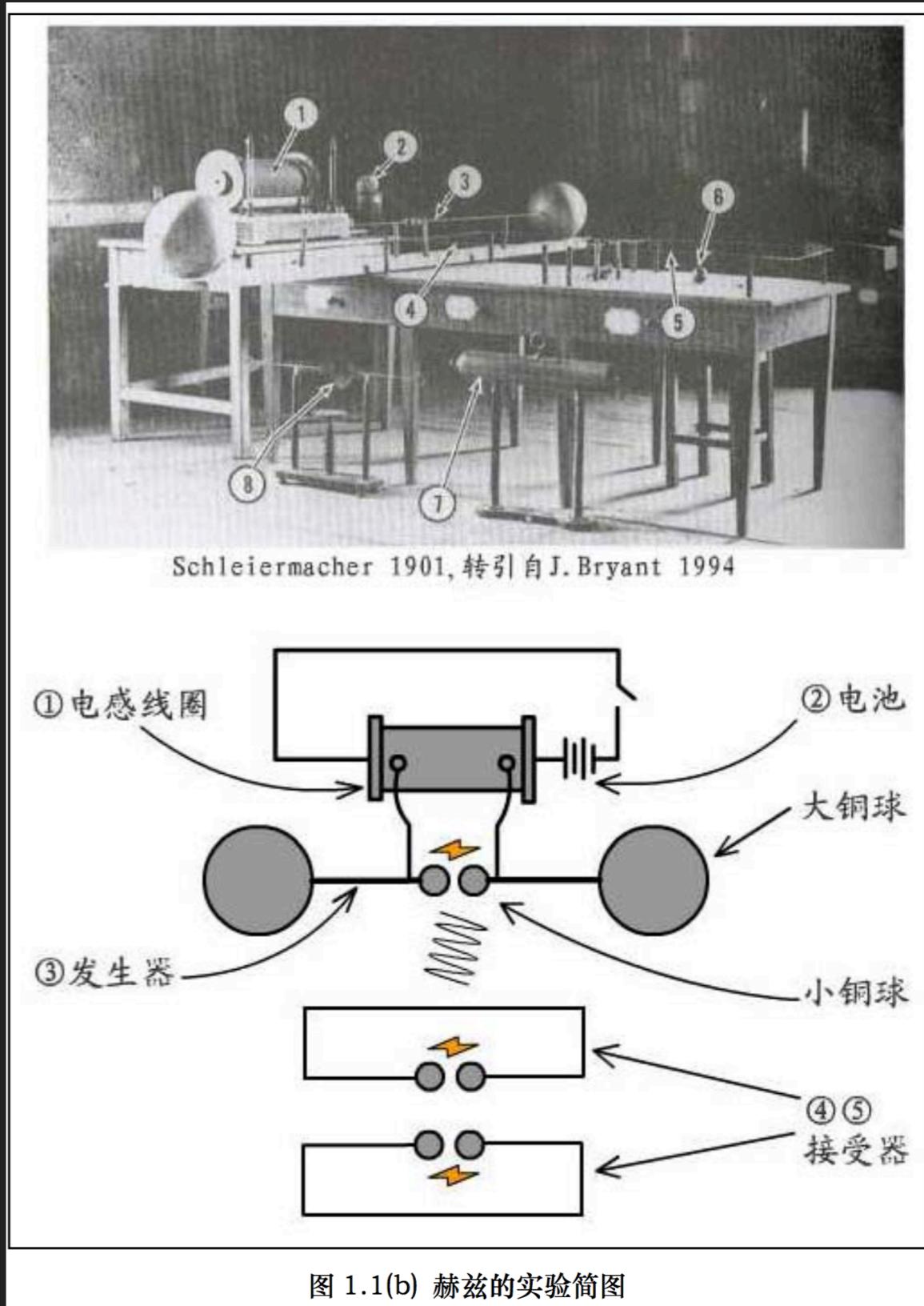


图 1.1(b) 赫兹的实验简图

SECURITY IN THE OPEN ENVIRONMENT

- ▶ Deauthentication Flood

SECURITY IN THE OPEN ENVIRONMENT

- ▶ Deauthentication Flood
- ▶ Fake Beacon

SECURITY IN THE OPEN ENVIRONMENT

- ▶ Deauthentication Flood
- ▶ Fake Beacon
- ▶ Authentication Flood

- ▶ Deauthentication Flood
- ▶ Fake Beacon
- ▶ Authentication Flood

这三种方法不涉及任何密码学的东西，仅仅需要靠近受害者的网络范围，然后嗅探到几个包就可以开始攻击，并且足以让被攻击的人完全用不了无线网络。

- ▶ Deauthentication Flood
- ▶ Fake Beacon
- ▶ Authentication Flood

这三种方法不涉及任何密码学的东西，仅仅需要靠近受害者的网络范围，然后嗅探到几个包就可以开始攻击，并且足以让被攻击的人完全用不了无线网络。

- ▶ One simple means to defend Wi-Fi availability

- ▶ Deauthentication Flood
- ▶ Fake Beacon
- ▶ Authentication Flood

这三种方法不涉及任何密码学的东西，仅仅需要靠近受害者的网络范围，然后嗅探到几个包就可以开始攻击，并且足以让被攻击的人完全用不了无线网络。

- ▶ One simple means to defend Wi-Fi availability
- ▶ Future Security—Can we depend on quantum mechanism instead of P vs. NP

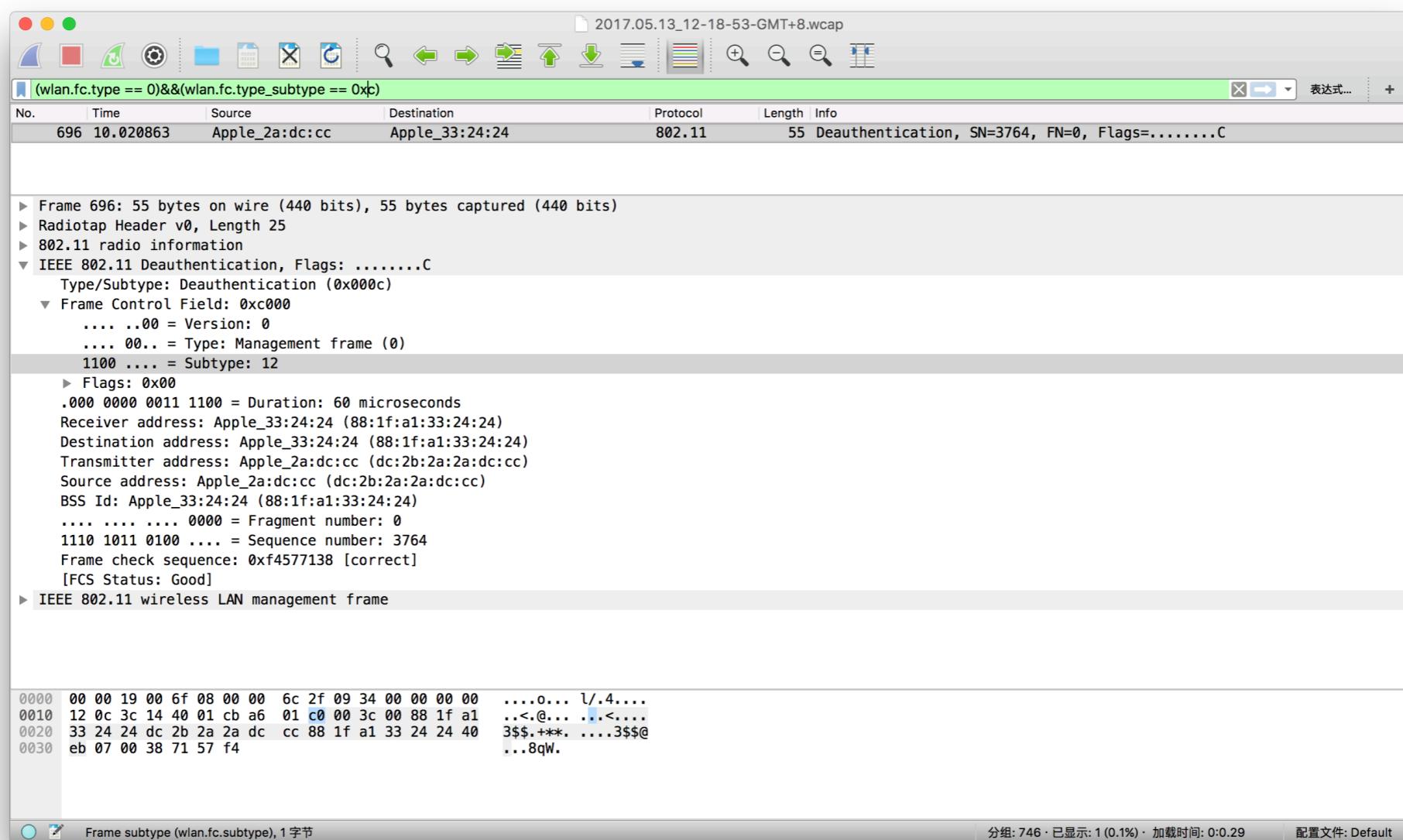
DEAUTHENTICATION FLOOD

1

不管你使用什么加密方式、密码强度有多高，甚至隐藏你的 SSID（毕竟隐藏 SSID 正如字面意义上的，它只是藏了 SSID，并不是隐藏了你和 AP 之间的数据包）都不行。

在 802.11 – 2012 标准 8.2.4.1.3 Type and Subtype fields 下面，列举了所有有效的 MAC 帧的 type 与 subtype 的组合，这里我们关注的 deauthentication 是 type 为 management 的帧。

在无线网络中，MAC 子层的通信是不加密的，于是我们可以利用 pcap 抓包，确定这个 AP 有哪些 STA。拿到 STA 的 MAC 之后，我们只需要伪造 MAC 管理子层的 deauthentication 类别的包就可以了。



在无线网络中，MAC 子层的通信是不加密的，于是我们可以利用 pcap 抓包，确定这个 AP 有哪些 STA。拿到 STA 的 MAC 之后，我们只需要伪造 MAC 管理子层的

```
de ▼ IEEE 802.11 Deauthentication, Flags: .......c
      Type/Subtype: Deauthentication (0x000c)
      ▼ Frame Control Field: 0xc000
          .... ..00 = Version: 0
          .... 00.. = Type: Management frame (0)
          1100 .... = Subtype: 12
      ► Flags: 0x00
```

```
► Flags: 0x00
  .000 0000 0011 1100 = Duration: 60 microseconds
  Receiver address: Apple_33:24:24 (88:1f:a1:33:24:24)
  Destination address: Apple_33:24:24 (88:1f:a1:33:24:24)
  Transmitter address: Apple_2a:dc:cc (dc:2b:2a:2a:dc:cc)
  Source address: Apple_2a:dc:cc (dc:2b:2a:2a:dc:cc)
  BSS Id: Apple_33:24:24 (88:1f:a1:33:24:24)
  .... .... 0000 = Fragment number: 0
  1110 1011 0100 .... = Sequence number: 3764
  Frame check sequence: 0xf4577138 [correct]
  [FCS Status: Good]
  ► IEEE 802.11 wireless LAN management frame
```



```
0000 00 00 19 00 6f 08 00 00 6c 2f 09 34 00 00 00 00 ...o... l/.4...
0010 12 0c 3c 14 40 01 cb a6 01 c0 00 3c 00 88 1f a1 ..<.@... .a<....
0020 33 24 24 dc 2b 2a 2a dc cc 88 1f a1 33 24 24 40 3$$.+**. ....3$@.
0030 eb 07 00 38 71 57 f4 ...8qW.
```

SECURITY IN THE OPEN ENVIRONMENT—DEAUTHENTICATION FLOOD

▼ IEEE 802.11 Deauthentication, Flags:C

Type/Subtype: Deauthentication (0x000c)

▼ Frame Control Field: 0xc000

... .00 = Version: 0

.... 00.. = Type: Management frame (0)

1100 = Subtype: 12

► Flags: 0x00

SECURITY IN THE OPEN ENVIRONMENT—DEAUTHENTICATION FLOOD

SECURITY IN THE OPEN ENVIRONMENT—DEAUTHENTICATION FLOOD

DEAUTHENTICATION FLOOD

1

Live Demonstration

FAKE BEACON

2

这是另一种 802.11 攻击，或者说扰乱更合适。攻击者发出无数个 Beacon 帧，这些 Beacon 帧既可以是和你的 AP 拥有相同的 SSID，也可以是攻击者自定的 SSID，或者就是一些随机字符串，取决于攻击的目的和实际环境。

这样的攻击在公共场合比较实用，拥有多个具有相同 SSID 的 AP 的地方不外乎是公司、学校、公园、餐厅等等。因为即使你以前连接过合法的 AP，你也难以分辨目前的列表里哪个是合法的（即使你同时能看到 BSSID）。在家庭环境中的话，绝大多数人也不会记自家 AP 的 BSSID，毕竟不是每个人都是计算机爱好者。

SECURITY IN THE OPEN ENVIRONMENT—— FAKE BEACON

Screenshot of Wireshark showing captured wireless traffic. The main pane displays a list of frames, with frame 1 selected. Frame 1 is a Beacon frame (Type/Subtype: 0x0008). The detailed pane shows the frame structure:

- Type/Subtype: Beacon frame (0x0008)**
- Frame Control Field: 0x8000**
 - .000 0000 0000 0000 = Duration: 0 microseconds
 - Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
 - Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
 - Transmitter address: bc:bc:bc:bc:bc:01 (bc:bc:bc:bc:bc:01)
 - Source address: bc:bc:bc:bc:bc:01 (bc:bc:bc:bc:bc:01)
 - BSS Id: bc:bc:bc:bc:bc:01 (bc:bc:bc:bc:bc:01)
 - 0000 = Fragment number: 0
 - 1011 0010 0011 = Sequence number: 2851
 - Frame check sequence: 0x95da693b [correct]
 - [FCS Status: Good]
- IEEE 802.11 wireless LAN management frame**
 - Fixed parameters (12 bytes)**
 - Timestamp: 0x00000000591d0cc5
 - Beacon Interval: 0.102400 [Seconds]
 - Capabilities Information: 0x1011**
 -1 = ESS capabilities: Transmitter is an AP
 -0. = IBSS status: Transmitter belongs to a BSS
 -0. 00.. = CFP participation capabilities: No point coordinator at AP (0x00)
 - 1 = Privacy: AP/STA can support WEP
 - 0. = Short Preamble: Not Allowed
 - 0. = PBCC: Not Allowed
 - 0.... = Channel Agility: Not in use
 - 0.... = Spectrum Management: Not Implemented
 -0.... = Short Slot Time: Not in use
 - 0.... = Automatic Power Save Delivery: Not Implemented
 - 1.... = Radio Measurement: Implemented
 - 0.... = DSSS-OFDM: Not Allowed
 - 0.... = Delayed Block Ack: Not Implemented
 - 0.... = Immediate Block Ack: Not Implemented
 - Tagged parameters (252 bytes)**
 - Tag: SSID parameter set: \357\277\275\357\277\275**
 - Tag Number: SSID parameter set (0)
 - Tag length: 6

The bottom status bar indicates: Indicates the identity of an ESS or IBSS (wlan_mgt.ssid), 6 bytes.

SECURITY IN THE OPEN ENVIRONMENT—— FAKE BEACON

► Frame Control Field: 0x8000
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: bc:bc:bc:bc:bc:01 (bc:bc:bc:bc:bc:01)
Source address: bc:bc:bc:bc:bc:01 (bc:bc:bc:bc:bc:01)
BSS Id: bc:bc:bc:bc:bc:01 (bc:bc:bc:bc:bc:01)
.... 0000 = Fragment number: 0
1011 0010 0011 = Sequence number: 2851

.... 0 = Spectrum Management: Not Implemented
.... 0.... = Short Slot Time: Not in use
.... 0.... = Automatic Power Save Delivery: Not Implemented
.... 1 = Radio Measurement: Implemented
.... 0.... = DSSS-OFDM: Not Allowed
.... 0.... = Delayed Block Ack: Not Implemented
.... 0.... = Immediate Block Ack: Not Implemented

▼ Tagged parameters (252 bytes)
▼ Tag: SSID parameter set: \357\277\275\357\277\275
Tag Number: SSID parameter set (0)
Tag length: 6
SSID: \357\277\275\357\277\275\357\277\275\357\277\275\357\277\275

0030	b2	c5	0c	1d	59	00	00	00	00	64	00	11	10	00	06	e5Y.... .d.....
0040	a5	b3	e8	a3	85	01	08	82	84	8b	96	0c	12	18	24	03\$. *.2.0H`
0050	01	01	05	04	00	01	00	00	2a	01	06	32	04	30	48	60	

Indicates the identity of an ESS or IBSS (wlan_mgt.ssid), 6 bytes

分组: 573 · 已显示: 573 (100.0%) · 加载时间: 0:0.26

配置文件: Default

FAKE BEACON

2

Live Demonstration

3

AUTHENTICATION FLOOD

与第一个 Deauthentication Flood 相对应。Deauthentication Flood 是强制让一个 AP 上、已经建立 association 的 STA 断开，从而达到目的。而Authentication Flood 则是通过伪造一大堆请求认证的包（其实还有 Association Flood），来塞满 AP 中的 Authentication / Association table，这样，真正的用户只能等到这个表有空 entry 的时候才能和 AP 建立连接了。

SECURITY IN THE OPEN ENVIRONMENT—— AUTHENTICATION FLOOD

2017.05.18_22-30-15-GMT+8.wcap

wlan.da == 23:23:23:23:23:23

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	54:11:0e:82:74:41	23:23:23:23:23:23	802.11	70	Authentication, SN=197, FN=0, Flags=.....C
4	0.101376	21:3d:dc:87:70:e9	23:23:23:23:23:23	802.11	70	Authentication, SN=198, FN=0, Flags=.....C
6	0.202032	3e:a1:41:e1:fc:67	23:23:23:23:23:23	802.11	70	Authentication, SN=199, FN=0, Flags=.....C
9	0.300424	3e:01:7e:97:ea:dc	23:23:23:23:23:23	802.11	70	Authentication, SN=200, FN=0, Flags=.....C
11	0.400757	6b:96:8f:38:5c:2a	23:23:23:23:23:23	802.11	70	Authentication, SN=201, FN=0, Flags=.....C
13	0.501036	ec:b0:3b:fb:32:af	23:23:23:23:23:23	802.11	70	Authentication, SN=202, FN=0, Flags=.....C
18	0.601153	3c:54:ec:18:db:5c	23:23:23:23:23:23	802.11	70	Authentication, SN=203, FN=0, Flags=.....C
20	0.701189	MS-NLB-PhysServer-...	23:23:23:23:23:23	802.11	70	Authentication, SN=204, FN=0, Flags=.....C
22	0.798066	aa:3a:fb:29:d1:e6	23:23:23:23:23:23	802.11	70	Authentication, SN=205, FN=0, Flags=.....C
24	0.898217	05:3c:7c:94:75:d8	23:23:23:23:23:23	802.11	70	Authentication, SN=206, FN=0, Flags=.....C
26	0.998451	be:61:89:f9:5c:bb	23:23:23:23:23:23	802.11	70	Authentication, SN=207, FN=0, Flags=.....C
30	1.098469	a8:99:0f:95:b1:eb	23:23:23:23:23:23	802.11	70	Authentication, SN=208, FN=0, Flags=.....C
32	1.198562	f1:b3:05:ef:f7:00	23:23:23:23:23:23	802.11	70	Authentication, SN=209, FN=0, Flags=.....C
34	1.299637	e9:a1:3a:e5:ca:0b	23:23:23:23:23:23	802.11	70	Authentication, SN=210, FN=0, Flags=.....C
36	1.403691	cb:d0:48:47:64:bd	23:23:23:23:23:23	802.11	70	Authentication, SN=211, FN=0, Flags=.....C

IEEE 802.11 Authentication, Flags:

Type/Subtype: Authentication (0x000b)

Frame Control Field: 0xb000

.... .00 = Version: 0

.... 00.. = Type: Management frame (0)

1011 = Subtype: 11

Flags: 0x00

.000 0001 0011 1010 = Duration: 314 microseconds

Receiver address: 23:23:23:23:23:23 (23:23:23:23:23:23)

Destination address: 23:23:23:23:23:23 (23:23:23:23:23:23)

Transmitter address: 54:11:0e:82:74:41 (54:11:0e:82:74:41)

Source address: 54:11:0e:82:74:41 (54:11:0e:82:74:41)

BSS Id: 23:23:23:23:23:23 (23:23:23:23:23:23)

.... 0000 = Fragment number: 0

0000 1100 0101 = Sequence number: 197

Frame check sequence: 0x1cda906b [correct]

[FCS Status: Good]

IEEE 802.11 wireless LAN management frame

0000	00 00 19 00 6f 08 00 00 d0 03 51 40 00 00 00 000.... Q@....
0010	10 02 6c 09 80 04 d3 a6 00 b0 00 3a 01 23 23 23	..l..... .#:##
0020	23 23 23 54 11 0e 82 74 41 23 23 23 23 23 50	##T...t A#####P
0030	0c 00 00 01 00 00 00 dd 09 00 10 18 02 00 00 00
0040	00 00 6b 90 da 1c	..k...

Frame subtype (wlan.fc.subtype), 1 字节

分组: 347 · 已显示: 84 (24.2%) · 加载时间: 0:0.36 · 配置文件: Default

SECURITY IN THE OPEN ENVIRONMENT—— AUTHENTICATION FLOOD

The screenshot shows a Wireshark capture of a wireless interface named "wlan.da". The packet list pane displays a series of IEEE 802.11 frames, all of which are Authentication frames (SN=197 to SN=204). The details pane shows the raw hex and ASCII data for one of the frames, and the bytes pane shows the raw hex data for the selected frame. The bottom status bar indicates the current file is "2017.05.18_22-30-15-GMT+8.wcap".

Packet details for the selected frame:

- .000 0001 0011 1010 = Duration: 314 microseconds
- Receiver address: 23:23:23:23:23:23 (23:23:23:23:23:23)
- Destination address: 23:23:23:23:23:23 (23:23:23:23:23:23)
- Transmitter address: 54:11:0e:82:74:41 (54:11:0e:82:74:41)
- Source address: 54:11:0e:82:74:41 (54:11:0e:82:74:41)
- BSS Id: 23:23:23:23:23:23 (23:23:23:23:23:23)
- 0000 = Fragment number: 0
- 0000 1100 0101 = Sequence number: 197
- Frame check sequence: 0x1cda906b [correct]
- [FCS Status: Good]

IEEE 802.11 wireless LAN management frame

Frame subtype (wlan.fc.subtype), 1 字节

分组: 347 · 已显示: 84 (24.2%) · 加载时间: 0:0.36 · 配置文件: Default

3

AUTHENTICATION FLOOD

Live Demonstration

4

DEFEND WI-FI AVAILABILITY

现实生活中的情况总是复杂的，不过个人认为下面这个思路在理论上来看是成立的（也或许实践中早有公司应用），没有过多的问题，当然这也有它自身的局限性，似乎还没有一个足够完美的方案（如果有的话，业界应该早就推广开了）。

我们已经提到过三种攻击，分别是 Deauthentication Flood, Beacon Flood 和 Authentication Flood，这三种攻击都需要攻击者发送数量非常多的包才行。于是我们也可以反过来利用这一点。

首先我们需要一个预警，比如当收到以上三种类型的包超过每秒 χ 个之后，我们就触发针对攻击者的追踪。这个追踪过程也是很常见的三(多)点定位法，我们的目的是找到攻击者的大致位置。不过这个方法对于家庭用户来说不太现实，在公司的环境中还是可以做到的（而且考虑到，相比攻击个人用户，攻击公司的网络似乎会更有价值）。

那么这里在 Wi-Fi 中的三(多)点定位法也需要探知距离。显然，攻击者在发送这些伪造的包的时候，会有多个 AP 收到（这里我们再次简化模型，必然是有办法只让 1 / 2 个 AP 收到，但是被攻击的用户大可加入另一个 AP，所以这里的影响相对较小，本文不考虑）。在这些 AP 收到包的时候，我们可以根据 RSSI (Received Signal Strength Indicator)，配合 FSPL (Free-Space Path Loss) 估算出信号源到该 AP 的大概的距离。

FSPL, Free-Space Path Loss, 或者翻译为自由空间路径损耗。官方的定义在 Standard Definitions of Terms for Antennas 里。简单来说，它是描述了无线信号在一个开放空间中（即没有障碍物，因此也不会有该无线信号的反射和衍射）经过一个确定的距离之后，信号强度的衰减的函数。

FSPL, Free-Space Path Loss, 或者翻译为自由空间路径损耗。官方的定义在 Standard Definitions of Terms for Antennas 里。简单来说，它是描述了无线信号在一个开放空间中（即没有障碍物，因此也不会有该无线信号的反射和衍射）经过一个确定的距离之后，信号强度的衰减的函数。

$$\begin{aligned} \text{FSPL} &= \left(\frac{4\pi d}{\lambda} \right)^2 \\ &= \left(\frac{4\pi df}{c} \right)^2 \end{aligned}$$

SECURITY IN THE OPEN ENVIRONMENT—— DEFEND WI-FI AVAILABILITY

$$\begin{aligned}\text{FSPL} &= \left(\frac{4\pi d}{\lambda}\right)^2 \\ &= \left(\frac{4\pi df}{c}\right)^2\end{aligned}$$

SECURITY IN THE OPEN ENVIRONMENT—— DEFEND WI-FI AVAILABILITY

$$\begin{aligned}\text{FSPL} &= \left(\frac{4\pi d}{\lambda}\right)^2 \\ &= \left(\frac{4\pi df}{c}\right)^2\end{aligned}$$

- ▶ d 是到信号源的距离

$$\begin{aligned}\text{FSPL} &= \left(\frac{4\pi d}{\lambda}\right)^2 \\ &= \left(\frac{4\pi df}{c}\right)^2\end{aligned}$$

- ▶ d 是到信号源的距离
- ▶ λ 是信号的波长，单位是米

$$\begin{aligned} \text{FSPL} &= \left(\frac{4\pi d}{\lambda} \right)^2 \\ &= \left(\frac{4\pi df}{c} \right)^2 \end{aligned}$$

- ▶ d 是到信号源的距离
- ▶ λ 是信号的波长，单位是米
- ▶ f 是信号的频率，单位使用赫兹

$$\begin{aligned} \text{FSPL} &= \left(\frac{4\pi d}{\lambda} \right)^2 \\ &= \left(\frac{4\pi df}{c} \right)^2 \end{aligned}$$

- ▶ d 是到信号源的距离
- ▶ λ 是信号的波长，单位是米
- ▶ f 是信号的频率，单位使用赫兹
- ▶ c 则是真空中的光速，也就是 $2.99792458 \times 10^8 \text{ m/s}$

不过在我们抓的包中，信号强度的单位是 dB，因此需要变形一下，取原式以 10 为底的对数，然后乘以 10，得到 dB 为单位的度量

$$\begin{aligned}\text{FSPL(dB)} &= 10 \log_{10} \left(\frac{4\pi df}{c} \right)^2 \\ &= 20 \log_{10} \frac{4\pi df}{c} \\ &= 20 \log_{10} d + 20 \log_{10} f + 20 \log_{10} \frac{4\pi}{c} \\ &\approx 20 \log_{10} d + 20 \log_{10} f - 147.552216778\end{aligned}$$

显然我们这里是已知接收到的信号的强度 RSSI，它的绝对值则是 FSPL(dB)，信号的频率f，需要求的是 d，那么再次简单变形

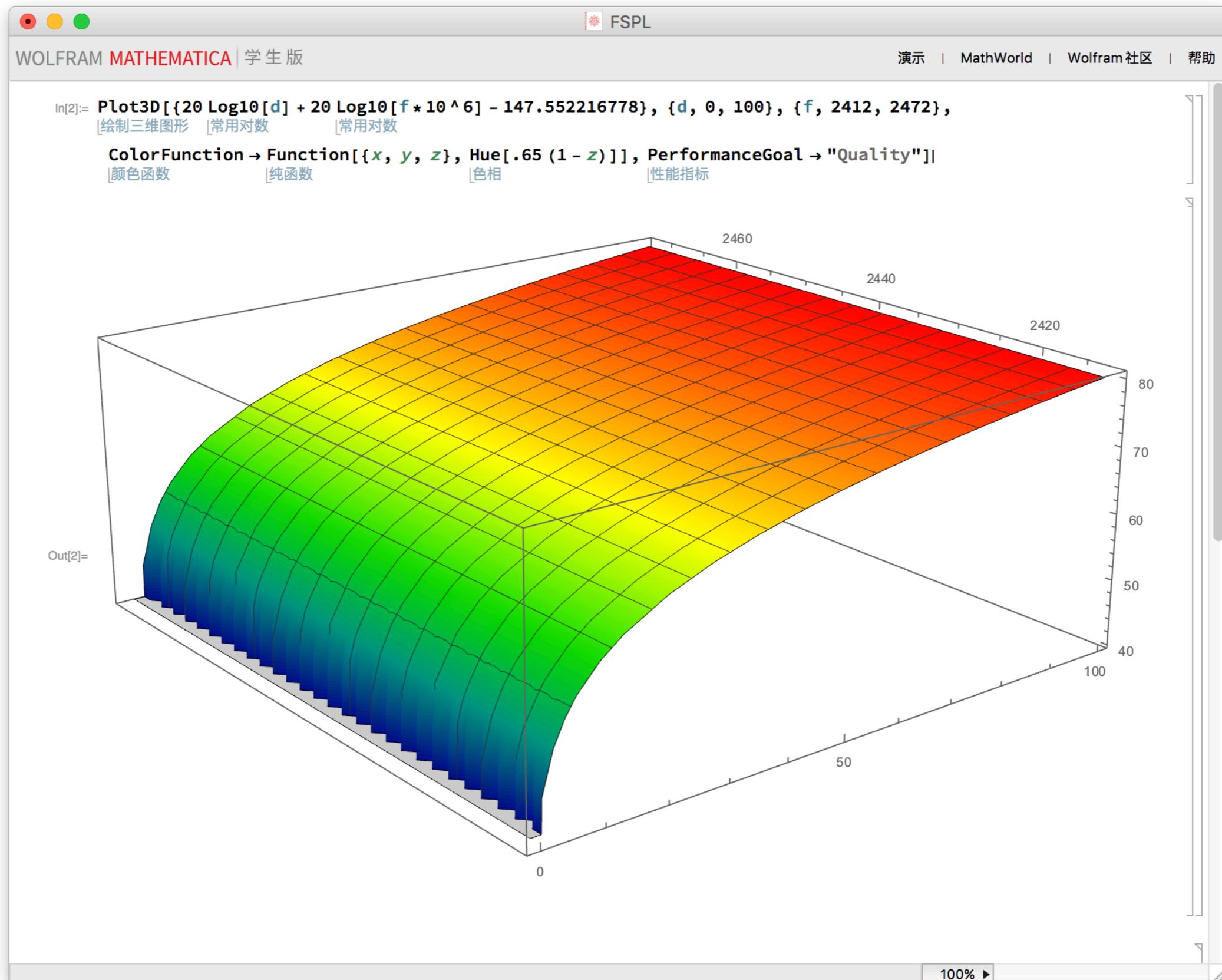
$$\text{FSPL(dB)} = 20 \log_{10} d + 20 \log_{10} f - 147.552216778$$

$$20 \log_{10} d = \text{FSPL(dB)} - 20 \log_{10} f + 147.552216778$$

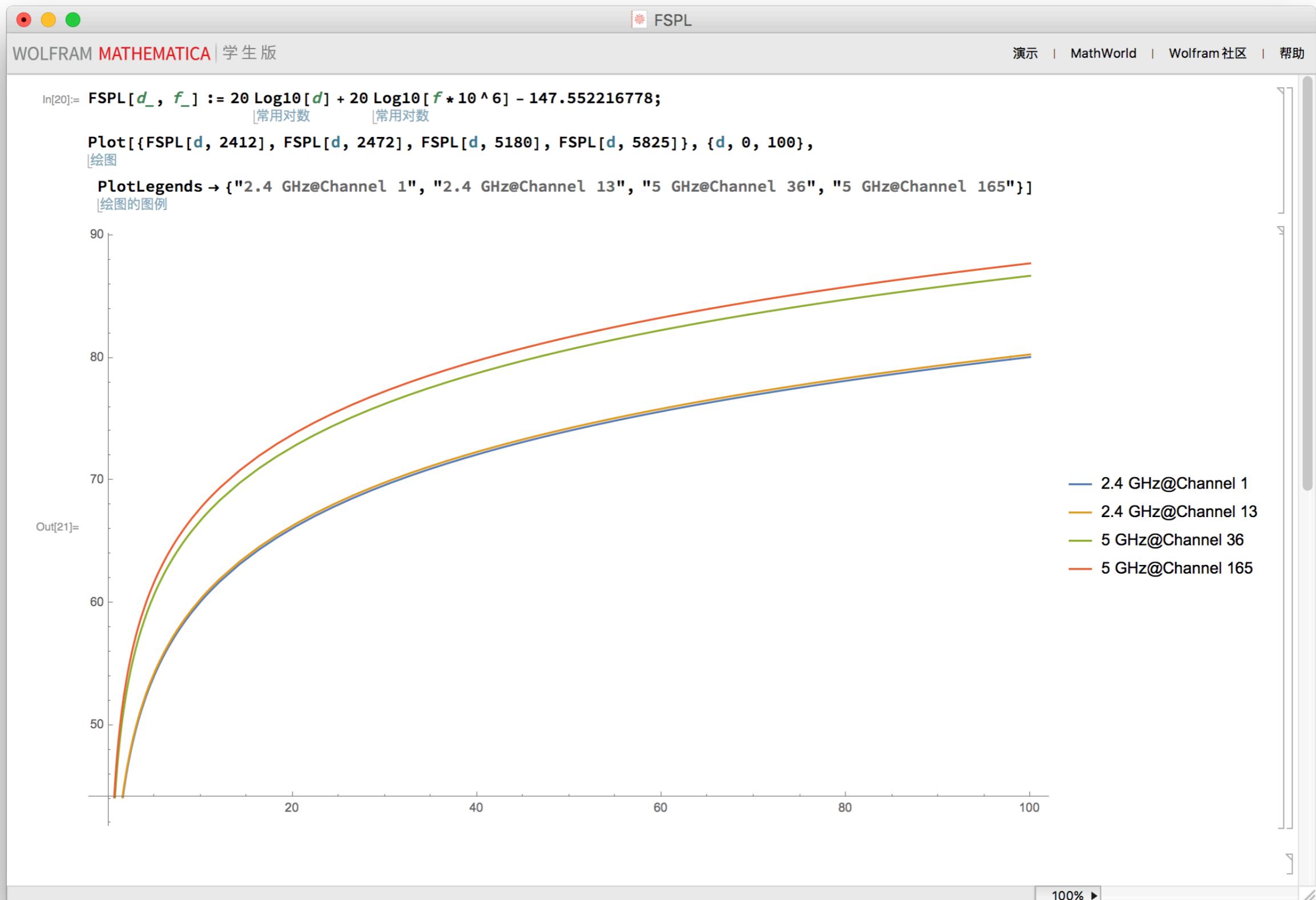
$$\log_{10} d = \frac{\text{FSPL(dB)} - 20 \log_{10} f + 147.552216778}{20}$$

$$d = 10^{\frac{\text{FSPL(dB)} - 20 \log_{10} f + 147.552216778}{20}}$$

SECURITY IN THE OPEN ENVIRONMENT—— DEFEND WI-FI AVAILABILITY



SECURITY IN THE OPEN ENVIRONMENT—— DEFEND WI-FI AVAILABILITY



我们以 2.4 GHz 下的信道 1 (2412 MHz) 为例子，假如 RSSI 是 -63dB ，那么带入计算距离 d 的式子，我们有

我们以 2.4 GHz 下的信道 1 (2412 MHz) 为例子，假如 RSSI 是 -63dB ，那么带入计算距离 d 的式子，我们有

$$\begin{aligned} d &= 10^{\frac{\text{FSPL(dB)} - 20 \log_{10} f + 147.552216778}{20}} \\ &\approx 10^{\frac{63 - 187.647546069 + 147.552216778}{20}} \\ &= 10^{\frac{22.904670709}{20}} \\ &= 10^{1.14523353545} \\ &\approx 13.971194395m \\ &\approx 13.97m \end{aligned}$$

我们以 2.4 GHz 下的信道 1 (2412 MHz) 为例子，假如 RSSI 是 -63dB ，那么带入计算距离 d 的式子，我们有

$$\begin{aligned} d &= 10^{\frac{\text{FSPL(dB)} - 20 \log_{10} f + 147.552216778}{20}} \\ &\approx 10^{\frac{63 - 187.647546069 + 147.552216778}{20}} \\ &= 10^{\frac{22.904670709}{20}} \\ &= 10^{1.14523353545} \\ &\approx 13.971194395m \\ &\approx 13.97m \end{aligned}$$

于是可以估算出信号源距离我们大约是 13.97 米，即以该 AP 为圆心，半径约 13.97 米这个范围的圆内。当然，严格来讲，我们还应该考虑信号源的发射功率、发射端的 cable loss、发射端和接收端的天线增益、接收端的灵敏度、信号穿墙的衰减等等。实际中是非常复杂的，这里做了许多的简化

FUTURE SECURITY

5

Can we depend on quantum mechanisms instead of P vs. NP

在量子计算机上存在整数分解问题的多项式时间算法。而在我们目前的图灵机上，还没有找到这一问题的多项式时间算法。

RSA等密码方案的安全性构建在大整数质因数分解的困难性基础之上。若有的确存在经典高效算法，则目前基于此猜想的密码算法都会变得没有意义。

目前理论上在量子计算机上进行整数质因数分解的算法——
肖尔算法。

P.W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput., 26(5): 1484–1509, 1997

Can we depend on quantum mechanisms instead of P vs. NP

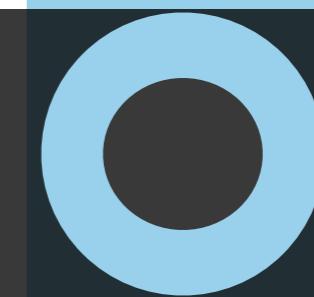
我们已经有证明，运用量子力学和EPR佯谬 / 贝尔“悖论”背后的思想可以构造出具有无条件安全性的公钥密码系统，也就是量子密钥分发，或者更一般的称为量子密码学。

这些密码系统在抵御计算能力无限的敌方时仍是安全的。

C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, 175, 1984

SECURITY IN THE OPEN ENVIRONMENT—

ENDING



在肖发明了他的算法之后，1996 年贝尔实验室的另一位科学家 洛弗·格鲁弗(Lov Grover)很快发现了另一种算法，可以有效地搜索未排序的数据库。如果我想从一个有 n 个记录但未排序的数据库中找出一个特定的记录的话，大概只好靠随机地碰运气，平均试 $n/2$ 次才会得到结果，但如果用格鲁弗的算法，复杂性则下降到根号 n 次。这使得另一种著名的非公钥系统加密算法，DES 面临崩溃。

Security in the open environment

$$\Delta p \times \Delta q \geq \frac{h}{2\pi}$$

Security in the open environment

$$\Delta p \times \Delta q \geq \frac{h}{2\pi}$$

理论不但决定我们能够观察到的东西，它还决定哪些是我们观察不到的东西！

Security in the open environment



Security in the open environment

Demo:

<https://github.com/BlueCocoa/WirelessKit>

Security in the open environment