정보보호 Introduction

컴퓨터공학과 장대희

경희대학교
KYUNG HEE UNIVERSITY

PWNJAB
@KYUNGHEE UNIVERSITY

RF 통신 해킹과 SDR 목차

- ❖1. 필요 SW 설치
- ❖2. RF 해킹이란?
- ❖3. RF 기본 개념
- ❖4. Modulation
- ❖5. RF 신호 해석 그래프
- ❖6. SDR 사용법
  - HackRF One, 안테나
  - SDR 소프트웨어
- ❖7. 실습
  - Capture & Replay
  - Jamming
  - Hack-A-Sat

RF 해킹이란?

❖RF == Radio Frequency

- 무선상으로 통신하는 모든 것에 대한 해킹

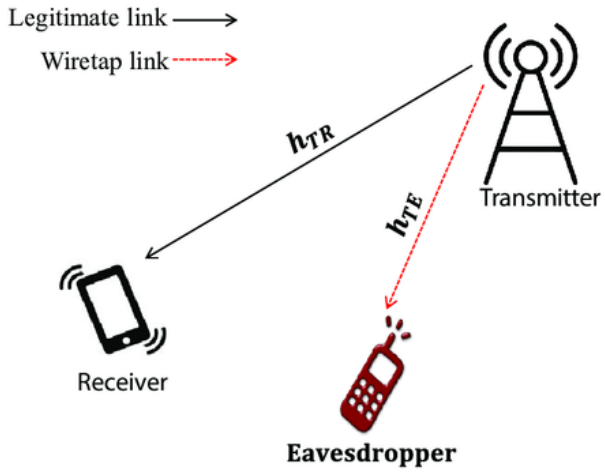
❖Physical Layer

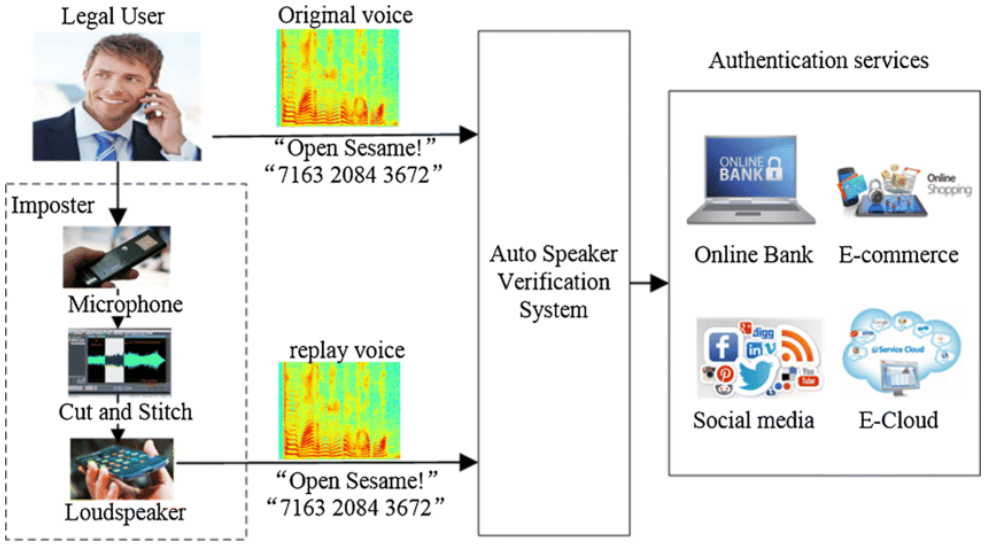
- Wi-fi, Bluetooth 등의 무선 통신 기술의 가장 아래 Layer에 대한 해킹

RF 해킹이란?

❖대표적인 공격 기법들

- Eavesdropping
- Replay Attack
- MITM
- Signal Manipulation & Spoofing





RF 해킹이란?

❖다양한 공격 대상들

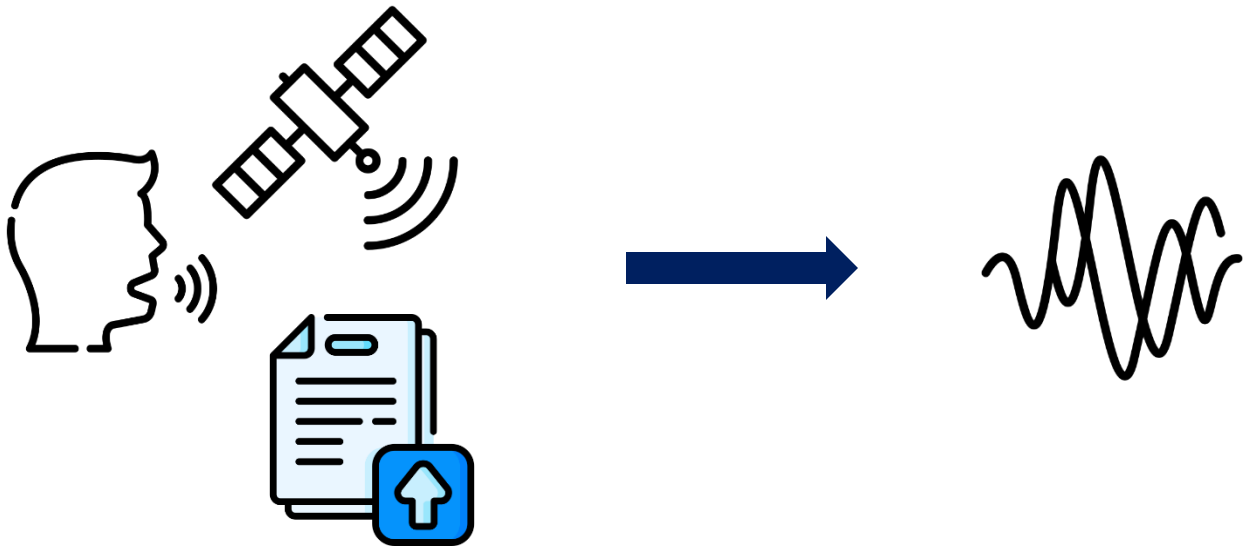
- 드론
- 인공위성
- 셀룰러 네트워크
- IoT 장비
- …

❖무선 신호를 사용하는 모든 기기가 공격 대상

RF 기본 개념

❖신호 송수신의 원리

- 음성을 먼 곳 까지 들리게 하려면 어떤 방법을 사용해야 할까?
- 데이터를 무선으로 송신하려면 어떤 방법을 사용해야 할까?



RF 기본 개념 - 송신

❖신호 송신의 원리

- **신호 세기**가 충분히 커야 함.
  - ✓ 신호 감쇠, noise
- 적당한 **주파수**를 이용해야 함.
  - ✓ 사용 환경, 거리
- 적당한 **대역폭**을 이용해야 함.
  - ✓ 데이터 전송 속도
- 적당한 **방법**으로 신호를 송신해야 함.
  - ✓ Modulation(변조)

RF 기본 개념 - 송신

❖신호 송신의 원리

- 1. 데이터를 신호로 변환
- 2. 변조(Modulation) 및 증폭
- 3. 안테나를 통한 송신

RF 기본 개념 - 수신

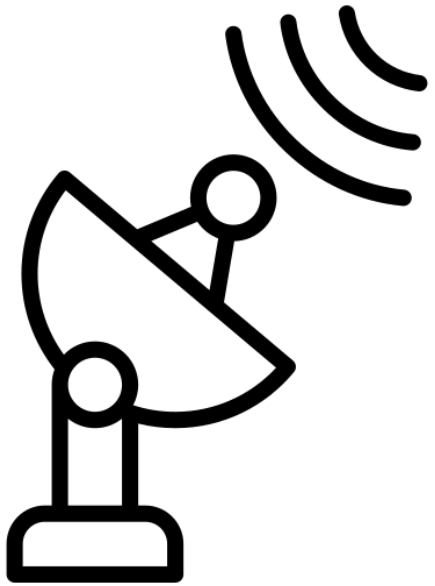
❖신호 수신의 원리

- 신호 감쇠, noise 를 적절히 처리해야 함.
- 원하는 주파수의 신호를 수신해야 함.
- 수신한 신호를 Demodulation(복조)해야 함.

RF 기본 개념 - 수신

❖신호 수신의 원리

- 1. 안테나를 통한 수신
- 2. 복조(Demodulation)
- 3. 신호를 데이터로 변환



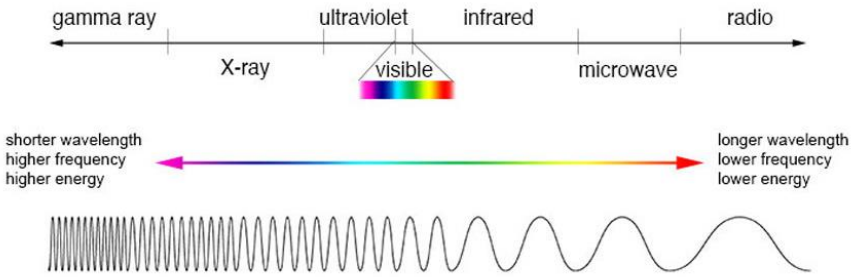
RF 기본 개념 - 용어

❖주파수(Frequency)

- 1초 동안 신호가 반복되는 횟수 (단위: Hz)
- 일반적으로 수 MHz ~ GHz 대역 사용.
- 낮을수록 멀리 전송 가능.
- 높을수록 넓은 대역폭을 가질 수 있음. (빠른 데이터 전송)

❖대역폭(Bandwidth)

- 사용할 수 있는 주파수 범위 (Hz 단위)
- 넓을수록 더 많은 데이터를 한번에 전송 가능.



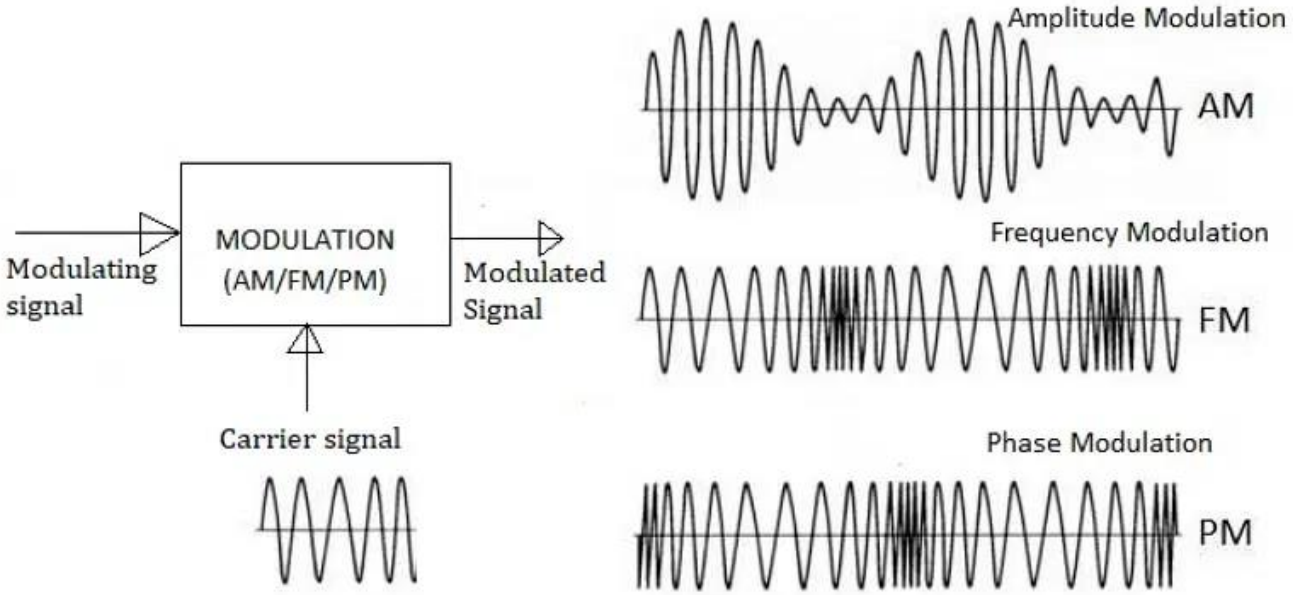
RF 기본 개념 - 용어

❖변조(Modulation)

- 데이터를 RF 신호에 실어서 보내는 과정.
- 널리 알려진 AM, FM을 비롯한 여러가지 방법이 있음.

❖복조(Demodulation)

- 변조된 신호를 받아서 원래 데이터로 복구하는 과정.

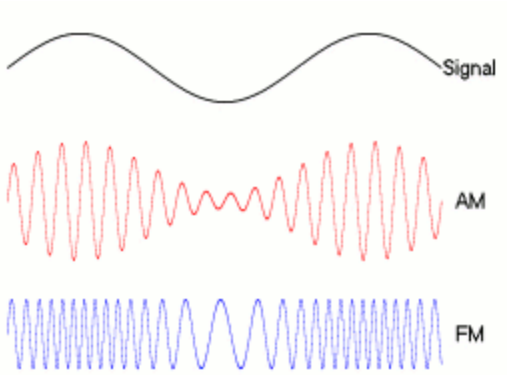


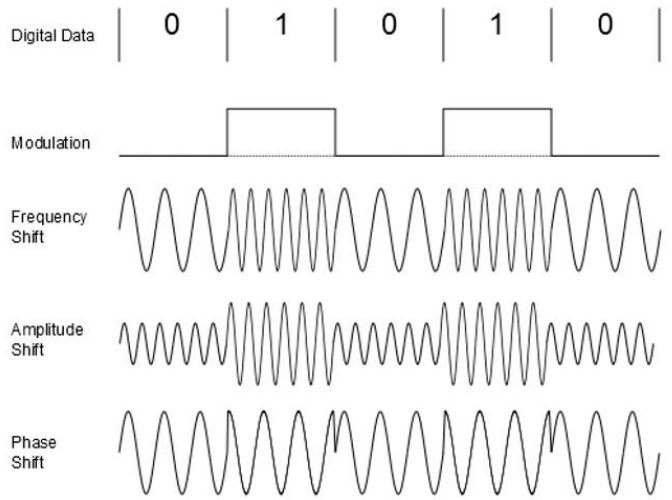
Modulation

❖Baseband
- 변조하기 전의 신호 (Raw Signal)

❖Analog Modulation
- 음성과 같은 연속적인 신호 변조
- AM, FM, PM

❖Digital Modulation
- 0,1의 bit 데이터를 변조
- ASK, FSK, PSK, QAM …





Modulation

❖AM, ASK (Amplitude Shift Keying)

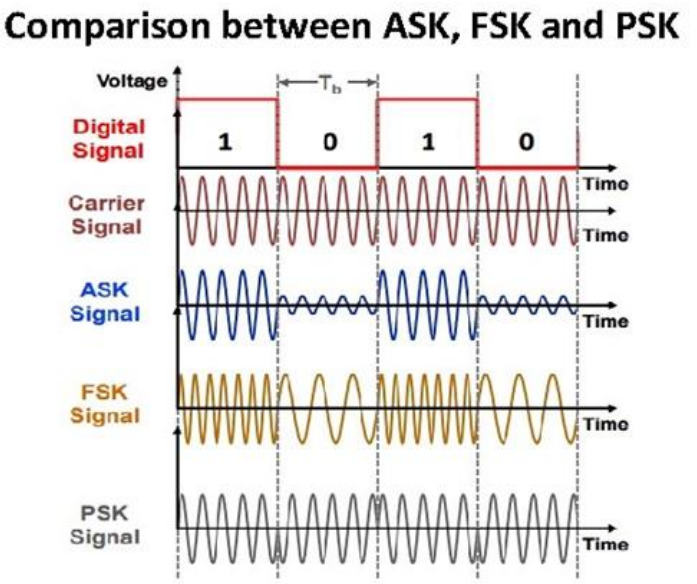
- 진폭(Amplitude)를 변화하여 정보를 표현.
- AM: 아날로그 신호의 변화에 따라 진폭 변화.
- ASK: 0, 1을 특정 진폭에 매핑.

❖FM, FSK (Frequency Shift Keying)

- 진폭(Frequency)를 변화하여 정보를 표현.
- FM: 아날로그 신호의 변화에 따라 주파수 변화.
- FSK: 0, 1을 특정 주파수에 매핑.

❖PM, PSK (Phase Shift Keying)

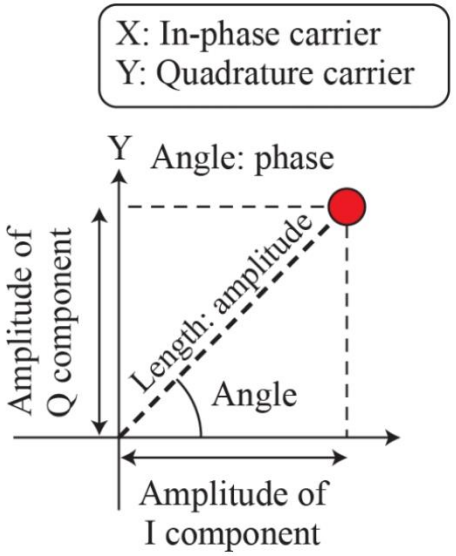
- 위상(Phase)를 변화하여 정보를 표현.
- FM: 아날로그 신호의 변화에 따라 위상 변화.
- PSK: 0, 1을 특정 위상에 매핑.

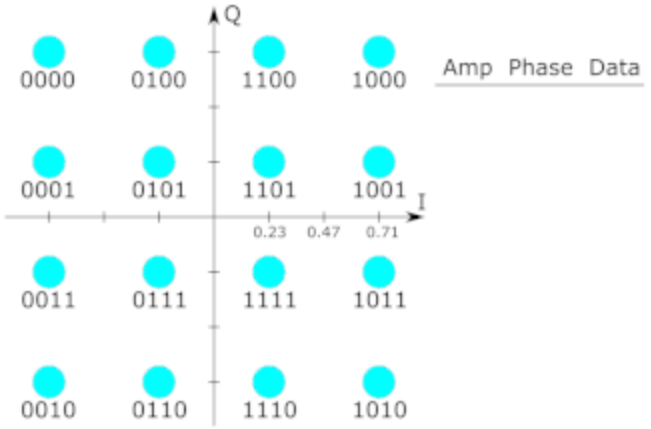


Modulation

❖QAM

- 진폭(Amplitude)과 위상(Phase)을 동시에 이용하여 데이터 전송.
- 위상 변조를 쉽게 표현하기 위해 보통 Constellation Diagram으로 표현함.
  - ✓ (0, 0) 으로부터의 거리 == 진폭
  - ✓ X축 양의 방향을 기준으로 한 각도 == 위상

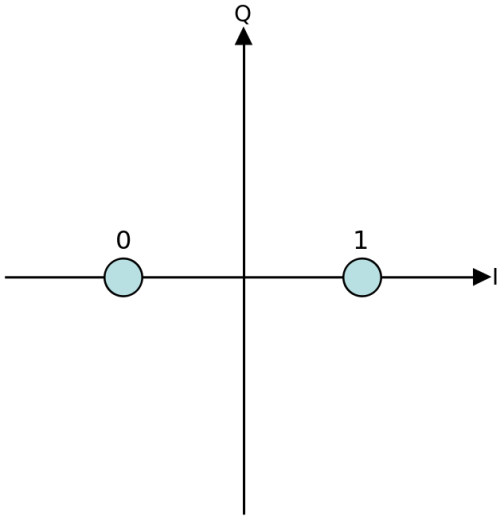


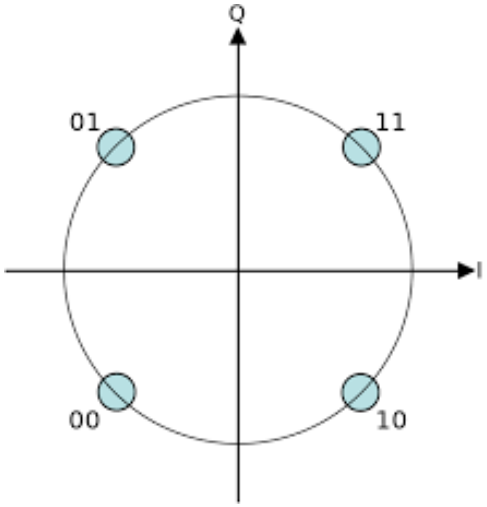


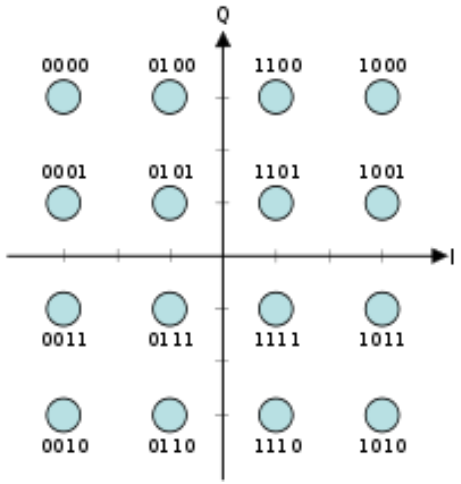
Modulation

❖QAM

- 매핑 개수에 따라 2-QAM, 4-QAM, 8-QAM 등 여러 종류가 존재.
- 매핑 개수가 증가함에 따라 하나의 "Symbol"에 더 많은 정보를 담을 수 있음.
  - ✓ 그러나 개수가 늘어나면 Symbol 간의 간격이 좁아져 오류가 증가할 수 있음.





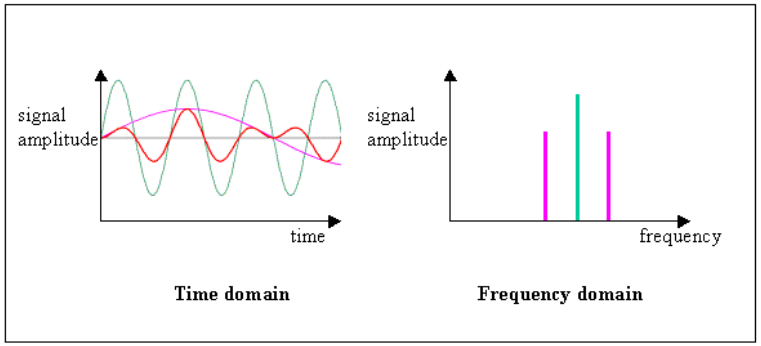


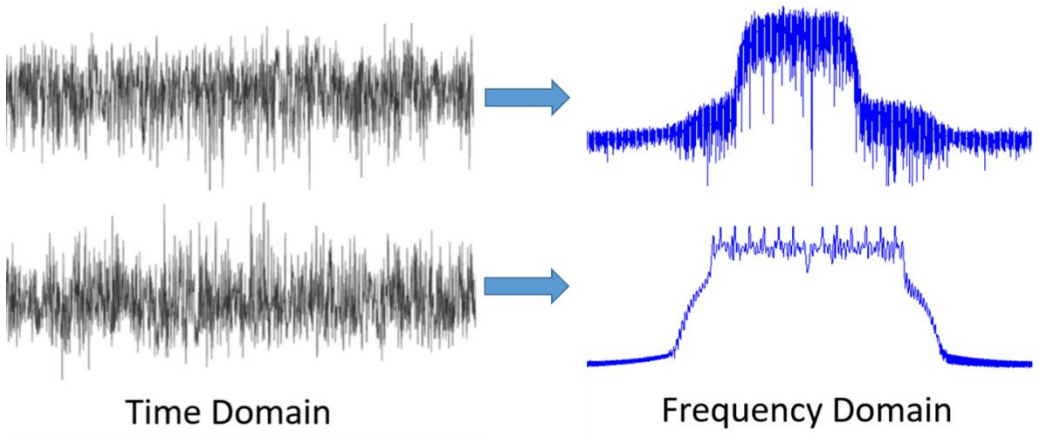
RF 신호 해석 그래프

❖사용자의 필요에 맞춰 여러 종류의 RF 신호 표현 방법이 있음.

❖Frequency Domain
- 주파수에 따른 진폭의 변화를 표현.
- FSK 종류의 신호 해석에 주로 사용.

❖Time Domain
- 시간에 따른 진폭의 변화를 표현.
- 펄스 형태 확인을 위해 사용.



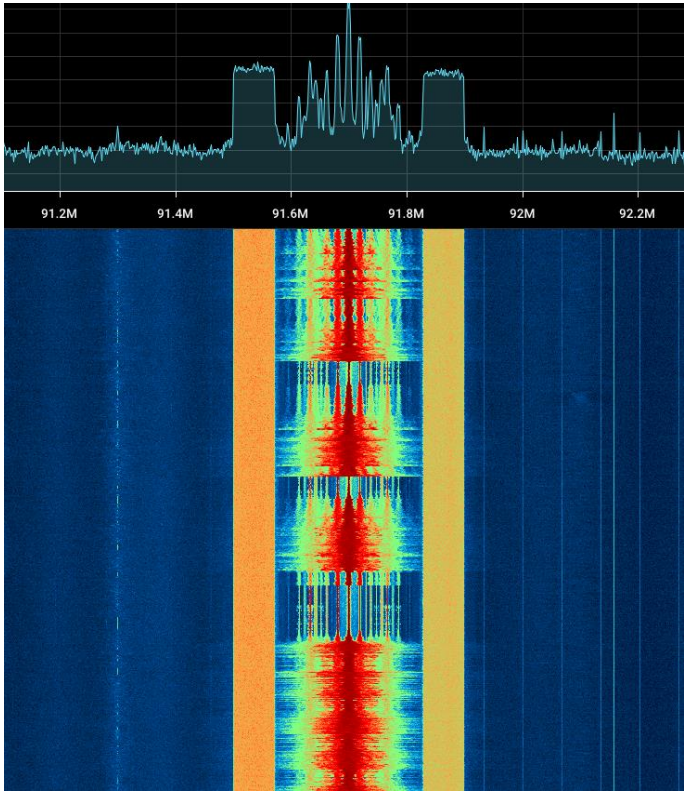


RF 신호 해석 그래프

❖사용자의 필요에 맞춰 여러 종류의 RF 신호 표현 방법이 있음.

❖Waterfall Plot (Spectogram)

- 시간에 따른 주파수, 진폭(색상 표현)를 표현.
- 신호의 존재 유무 확인에 주로 사용.

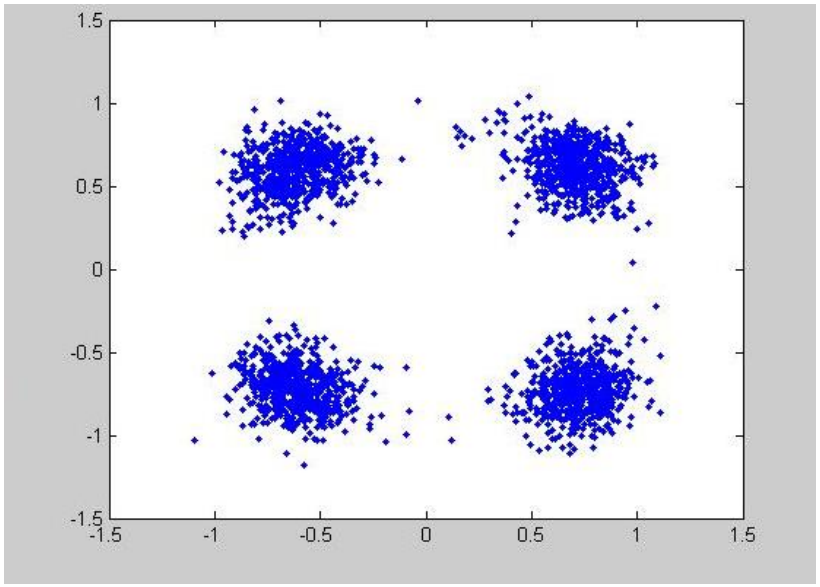


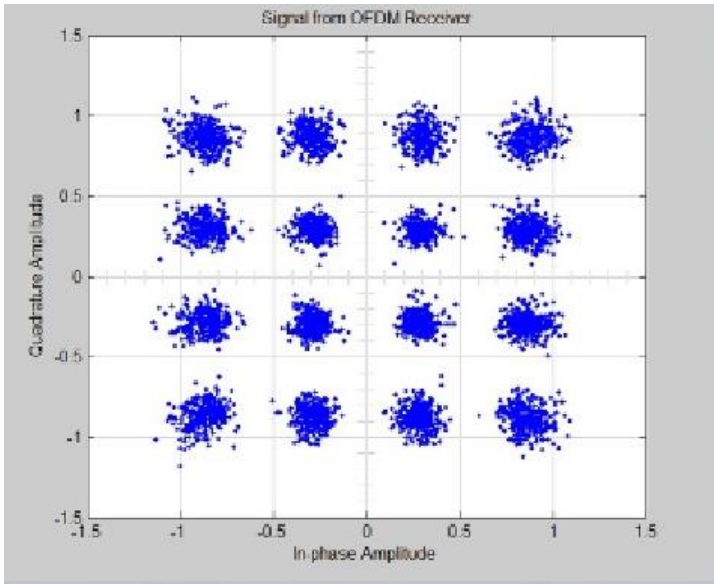
RF 신호 해석 그래프

❖사용자의 필요에 맞춰 여러 종류의 RF 신호 표현 방법이 있음.

❖Constellation Diagram

- 위상, 진폭을 점의 형태로 표현.
- QAM 종류의 신호 해석을 위해 주로 사용.





SDR 사용법 - 하드웨어

❖SDR 이란?

- Software Defined Radio
- 기존의 RF 장비는 필요한 기능들을 하드웨어로 구현됨.
- SDR은 해당 기능들을 소프트웨어로 처리하여 다양한 RF 신호 구현 가능.

❖SDR 셋업

- 안테나 – SDR 장비 – 컴퓨터

SDR 사용법 - 하드웨어

❖RTL-SDR

- 수신 가능 주파수: 24 MHz ~ 1.7 GHz
- Sampling rate: 최대 3.2 MSPS
- 수신만 가능
- 지원 SW: GNU Radio, Gqrx, SDR# …
- Antenna connector: SMA female

SDR 사용법 - 하드웨어

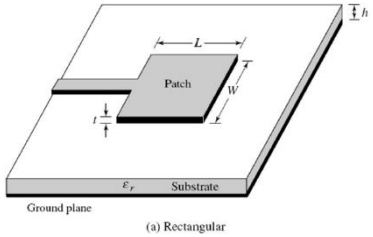
❖HackRF One

- 수신 가능 주파수: 1 MHz ~ 6 GHz
- Sampling rate: 최대 20 MSPS
- 송수신 모두 가능 (half-duplex transceiver)
- 지원 SW: GNU Radio, Gqrx, SDR# …
- Antenna connector: SMA female

SDR 사용법 - 하드웨어

❖안테나

- 특정 주파수 수신을 위해서 해당 주파수를 지원하는 안테나를 사용해야 함.
- 용도에 따라 형태도 달라짐.
  - ✓ 파라볼라(접시), 야기, 로드, 패치, 헬리칼 …



(a) Rectangular

SDR 사용법 - 소프트웨어

❖SDR을 목적에 맞게 정의하기 위해 다양한 소프트웨어를 사용함.

❖GNU Radio

- SDR 개발.
- 자유도가 높아 다양한 변조/복조와 필터링이 가능함.
- 그러나 자유도가 높은 만큼 사용하기 어려움.

❖Gqrx

- 실시간 RF 신호 수신 및 분석.
- Waterfall Diagram 분석에 용이.

❖Universal Radio Hacker

- 신호 분석 및 리버스 엔지니어링(해킹/보안 연구)용.

❖SDR++

- 신호 스펙트럼 분석 (Waterfall Diagram)
- 안드로이드 앱으로도 지원.

실습 – 시작하기 전에...

❖전파법

- 수신은 허가 받지 않고 가능.
- 그러나 송신은 일부 주파수 외에는 허가 받고 사용해야함.

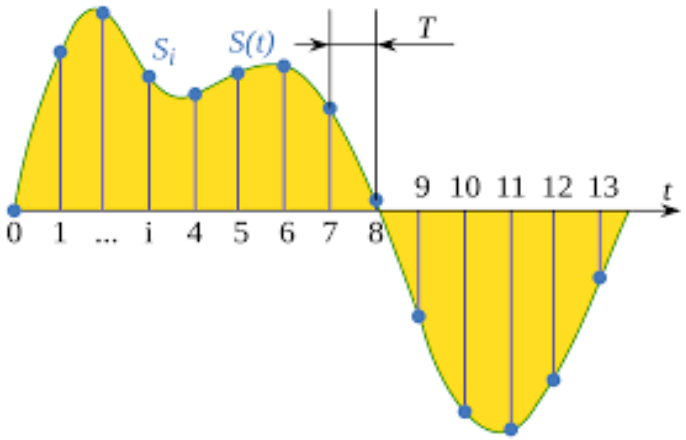
❖허가 없이 사용 가능한 주파수

- 13.56MHz 대역
- 433 MHz 대역 (433.05 MHz ~ 434.79 MHz)
- 2.4 GHz 대역 (2.4 GHz ~ 2.4835 GHz)
- 5.8 GHz 대역 (5.725 GHz ~ 5.875 GHz)

실습 - 시작하기 전에...

❖Sampling 이란?

- RF 신호를 일정한 시간 간격으로 측정하여 디지털 값으로 변환하는 과정.
- 연속적인 신호를 순간순간 캡처한다고 생각하면 됨.



실습 - 시작하기 전에...

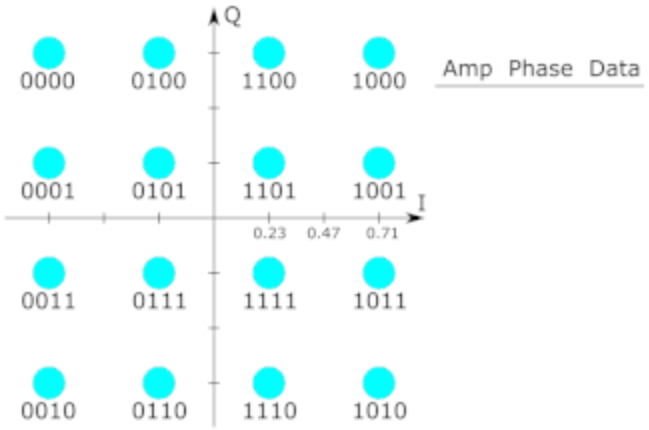
❖Sample Rate

- Sampling 하는 속도.
- Rate가 높으면 보다 정확히 수신 가능하다.
  - ✓ 특히 bandwidth와 Sample Rate는 같이 움직인다.
  - ✓ e.g. Sample Rate: 20 MHz → Bandwidth: 20 MHz
- 그러나 무작정 Rate를 높이면 안됨!
  - ✓ 수신기 내부에서 여러 주파수 성분이 섞이는 상호 변조 왜곡(IMD)가 생김.
  - ✓ SDR 소프트웨어에서 가짜 신호(Ghost Signal)가 검출될 수 있음.

실습 - 시작하기 전에...

❖I/Q 파일

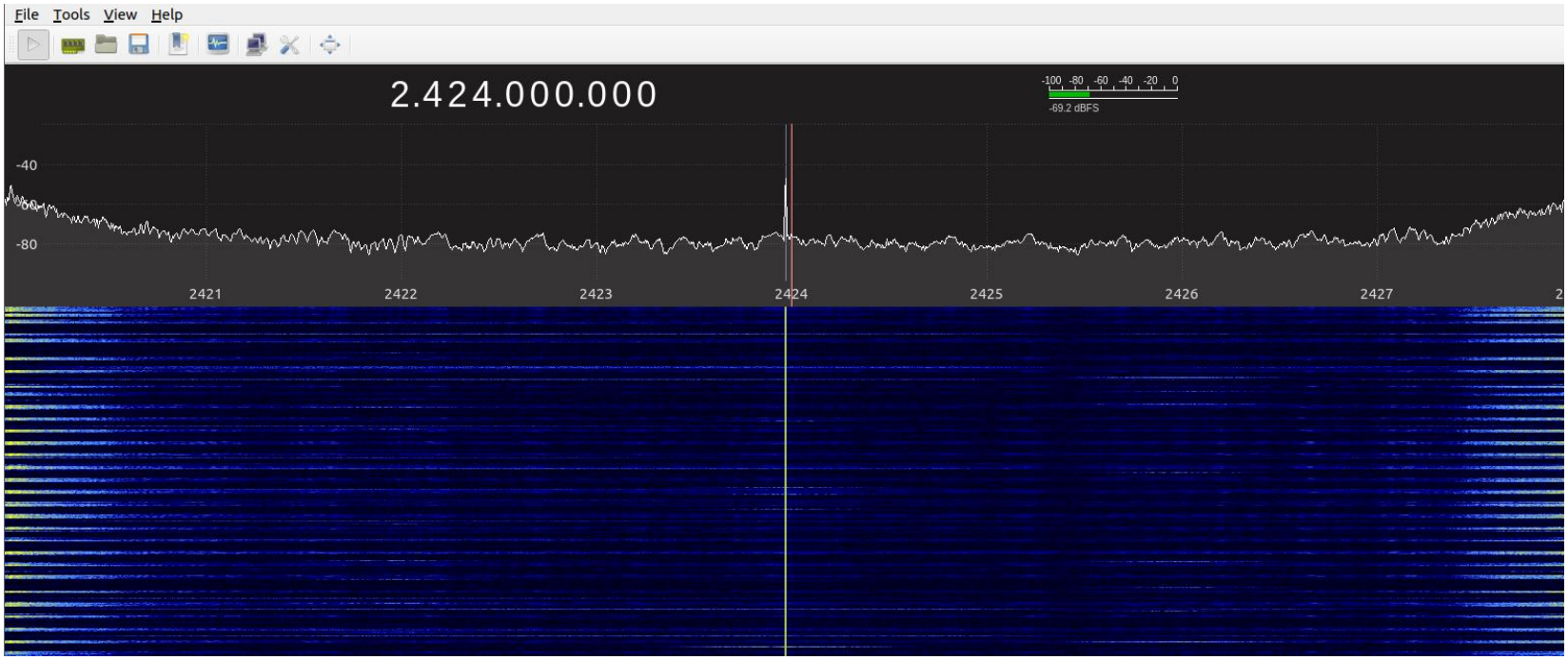
- SDR에서 수신한 복소수 신호(I: In-phase, Q: Quadrature) 데이터를 저장한 파일.
- 복소수??
  - ✓ 신호 sample 값을 표현하기 위해 사용.
  - ✓ I와 Q는 Constellation Diagram 에서 각각 x축 값, y축 값을 의미함.
- 정확한 신호 정보를 저장하기 위해 wav 파일보다는 I/Q 파일로 신호 캡처함.
  - ✓ wav 파일은 실수 부분만 저장.



실습 - 시작하기 전에...

❖Mirror Signal

- 일반적으로 SDR은 Mixer를 사용해서 신호를 IF로 변환.
- 이 과정에서 불필요한 Mirror Signal이 함께 생성될 수 있음.
- Ghost Signal과 다르게 실제 신호와 대칭적인 위치에서 나타남.




Q
A