# Disorienta i cercatori di Pokemon (GPS Spoofing)

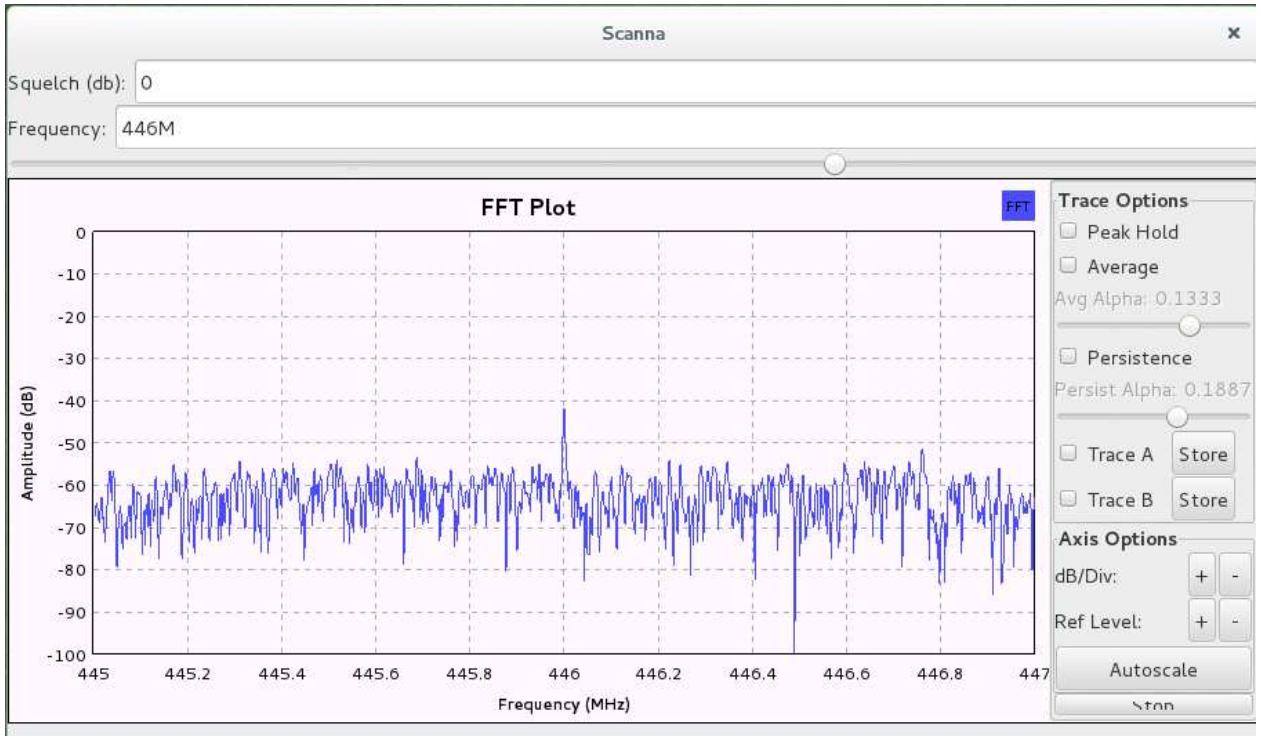
blackflag@paranoici.org

June 19, 2017

# Chi controlla i cacciatori di Pokemon?

# Scanna

http://git.lattuga.net/blackflag/Scanna




ovvero: come registrare uno (o piu') canali radio evitando di passare intere giornate aspettando il segnale!

# IL GPS
(Global Position System)

# Il GPS

Il GPS è un sistema per identificare una posizione sulla terra

- Sotto il controllo del dipartimento della difesa americano

# Il GPS

Il GPS è un sistema per identificare una posizione sulla terra

- Sotto il controllo del dipartimento della difesa americano
- 24 Satelliti a 20.200 km dalla terra

# Il GPS

Il GPS è un sistema per identificare una posizione sulla terra

- Sotto il controllo del dipartimento della difesa americano
- 24 Satelliti a 20.200 km dalla terra
- Precisione di 2-4 m osservata (2-8 m massima)

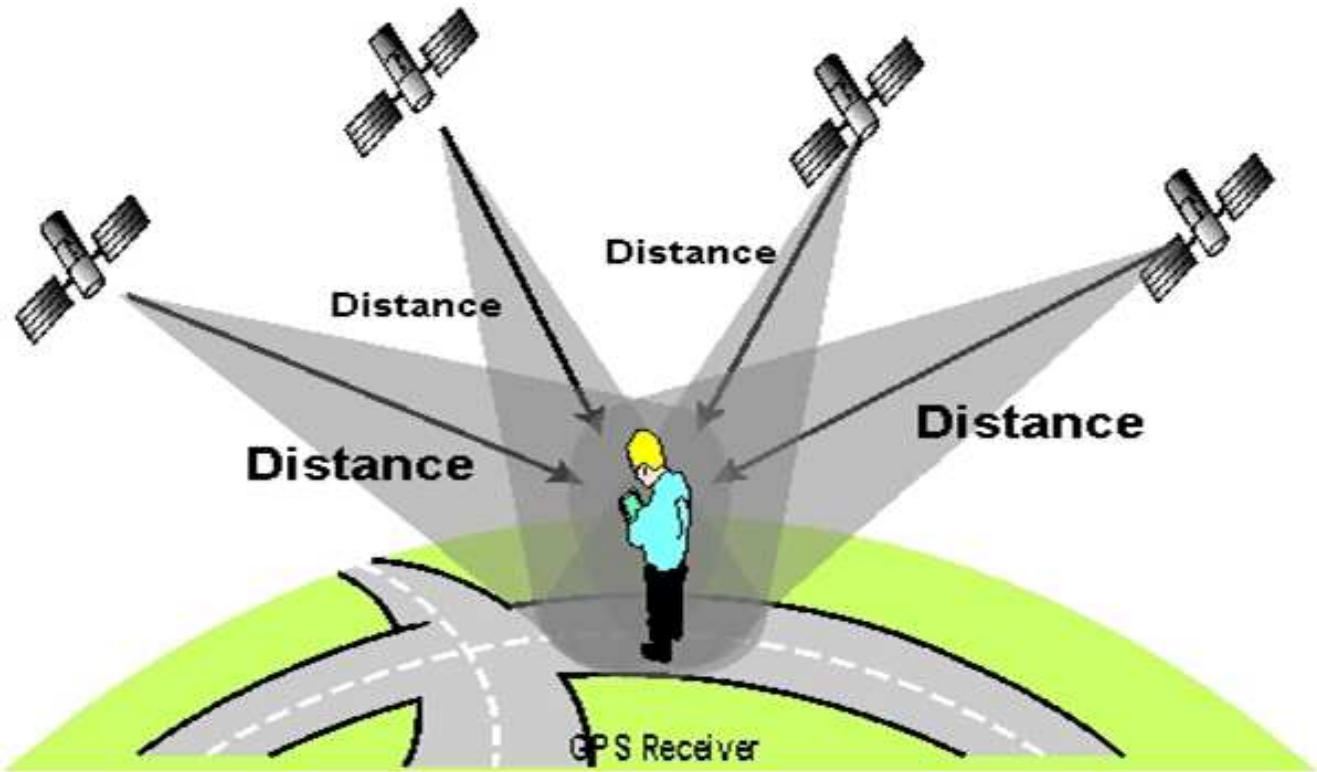
# Il GPS

Il GPS è un sistema per identificare una posizione sulla terra

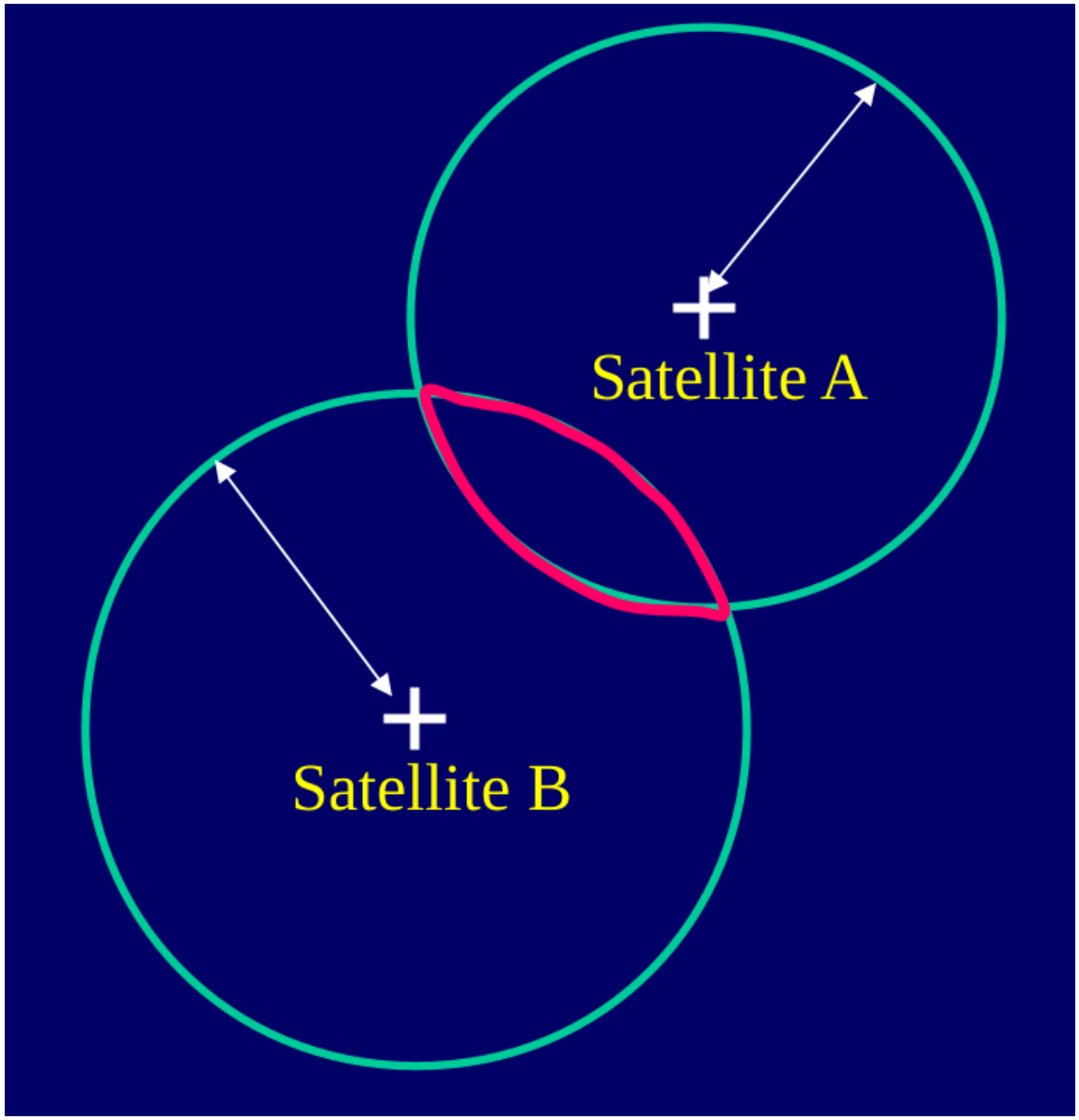
- Sotto il controllo del dipartimento della difesa americano
- 24 Satelliti a 20.200 km dalla terra
- Precisione di 2-4 m osservata (2-8 m massima)
- Ci sono sempre 12 satelliti visibili

# Calcolo posizione

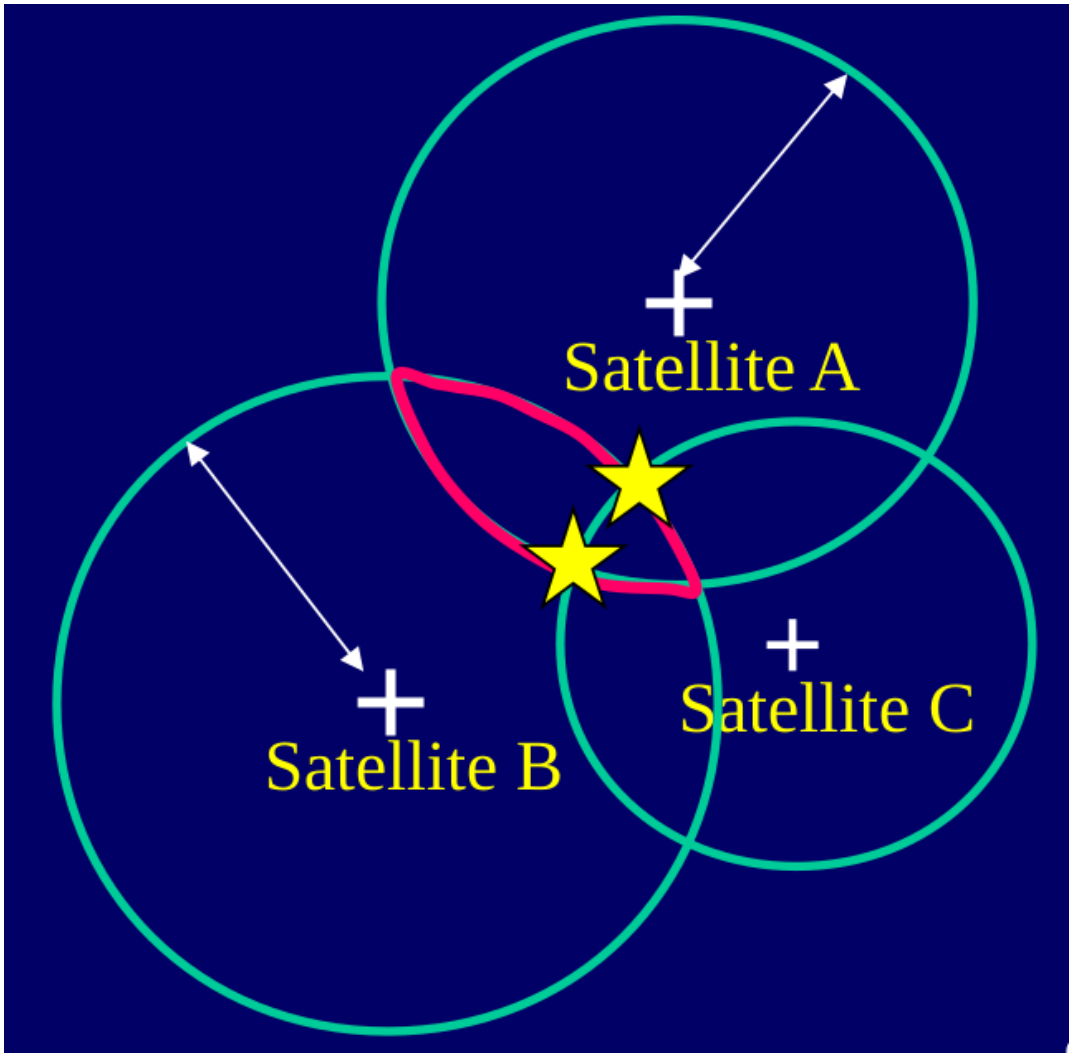
Distanza = tempo di ricezione del segnale X velocità della luce



# Calcolo posizione



# Calcolo posizione



# Precisione

Parametri che influenzano la precisione:

- Tempo di acquisizione

# Precisione

Parametri che influenzano la precisione:

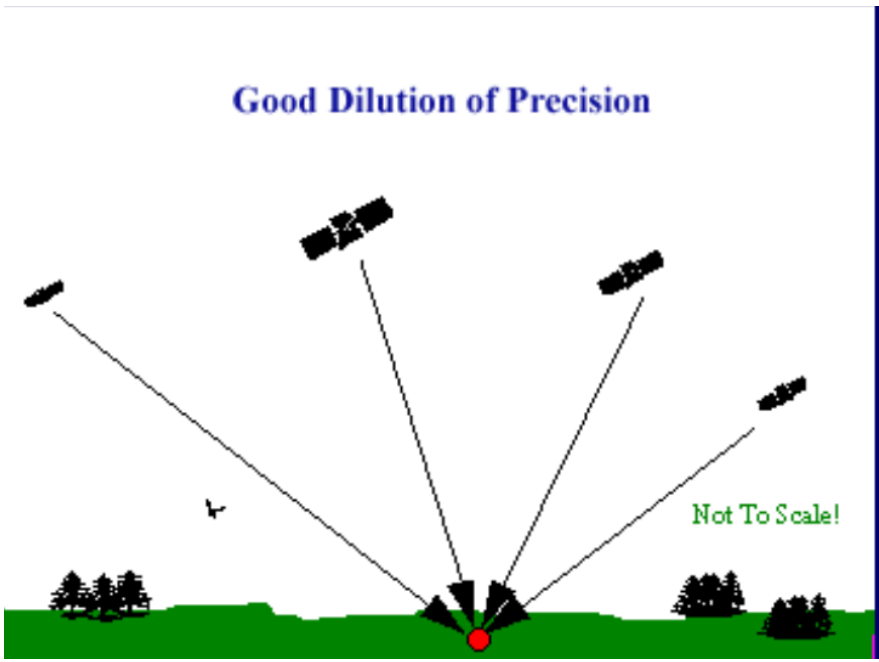
- Tempo di acquisizione
- Qualità del ricevitore

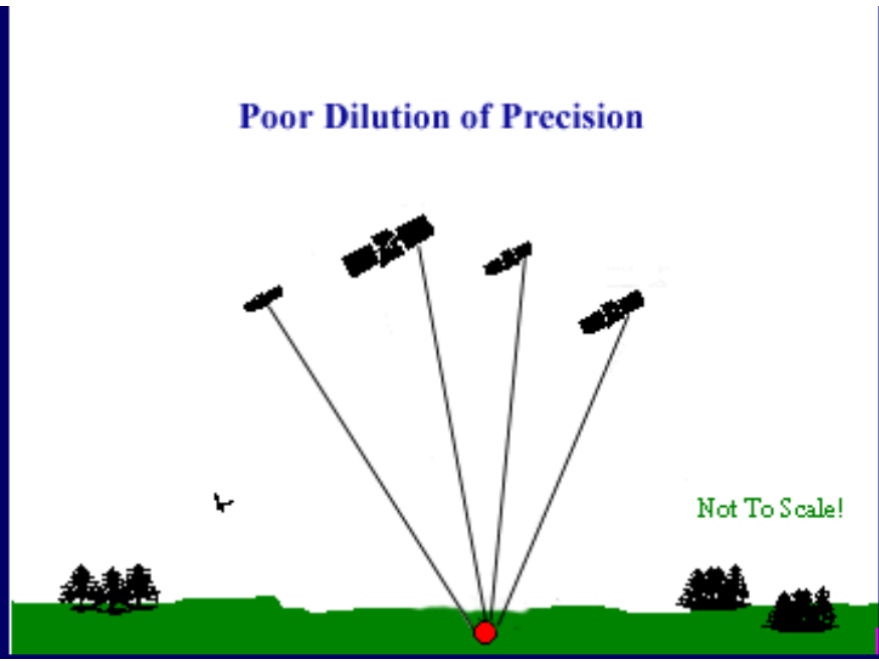
# Precisione

Parametri che influenzano la precisione:

- Tempo di acquisizione
- Qualità del ricevitore
- Posizione relativa dei satelliti (parametro DOP)

# DOP


Good Dilution of Precision
Not To Scale!


Poor Dilution of Precision
Not To Scale!

# SNR

Signal Noise Ratio - Differenza tra rumore e segnale

# GPS Spoofing
(Diventiamo satelliti...)

# Satellite-trasmettitore

Trasmettitore, satellite:

- invia il tempo di trasmissione (TOT)

# Satellite-trasmettitore

Trasmettitore, satellite:

- invia il tempo di trasmissione (TOT)
- invia la posizione del satellite rispetto al centro della terra

# Satellite-trasmettitore

Trasmettitore, satellite:

- invia il tempo di trasmissione (TOT)
- invia la posizione del satellite rispetto al centro della terra

# Satellite-trasmettitore

Trasmettitore, satellite:

- invia il tempo di trasmissione (TOT)
- invia la posizione del satellite rispetto al centro della terra

Ricevitore:

- misura il tempo di arrivo (TOA) secondo il suo clock

# Satellite-trasmettitore

Trasmettitore, satellite:

- invia il tempo di trasmissione (TOT)
- invia la posizione del satellite rispetto al centro della terra

Ricevitore:

- misura il tempo di arrivo (TOA) secondo il suo clock
- dal TOT ricevuto calcola il "tempo di volo" (TOF = TOA - TOF)

# Satellite-trasmettitore

Trasmettitore, satellite:

- invia il tempo di trasmissione (TOT)
- invia la posizione del satellite rispetto al centro della terra

Ricevitore:

- misura il tempo di arrivo (TOA) secondo il suo clock
- dal TOT ricevuto calcola il "tempo di volo" (TOF = TOA - TOF)
- calcola la sua posizione rispetto al centro della terra

# Satellite-trasmettitore

Trasmettitore, satellite:

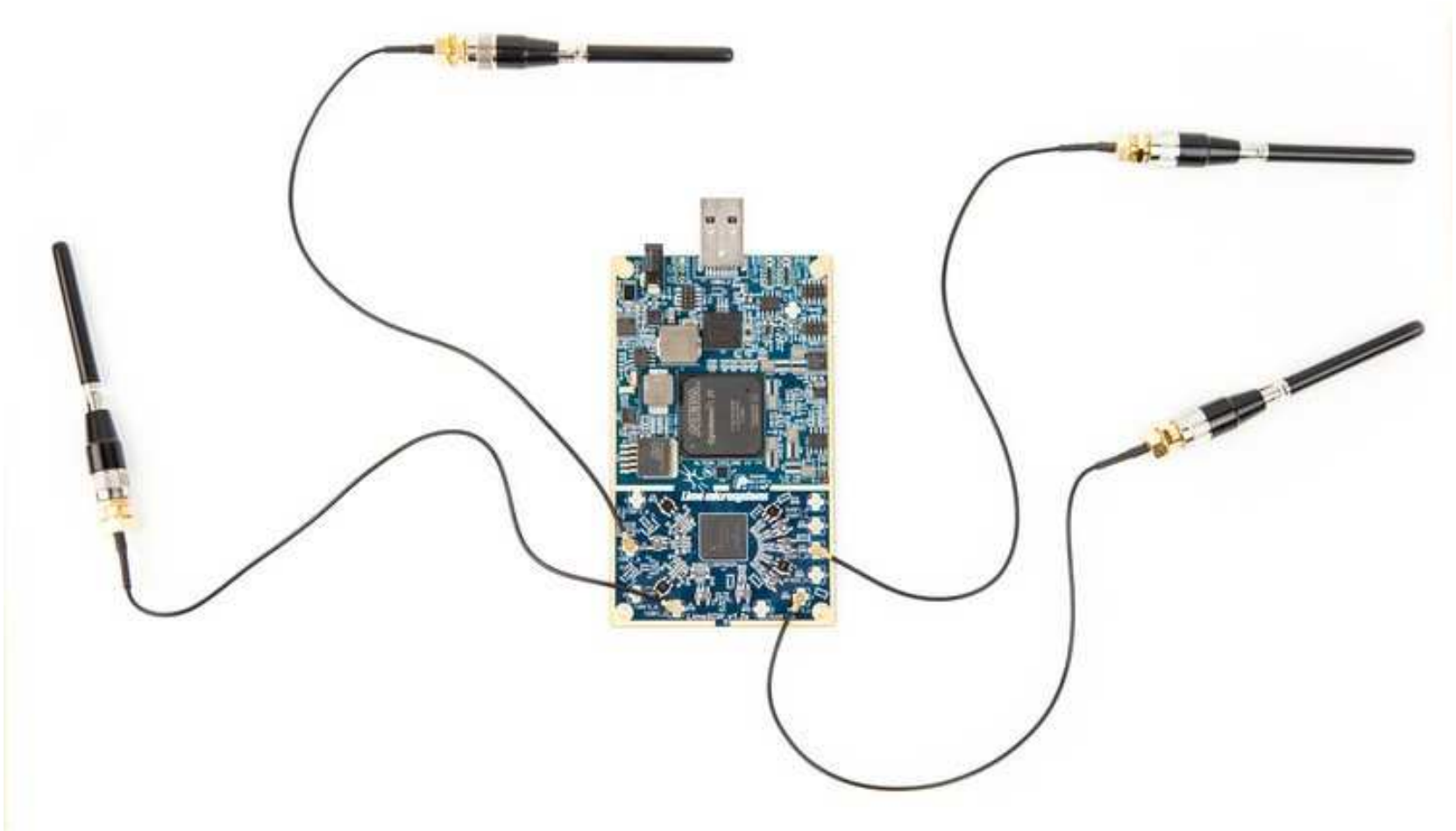
- invia il tempo di trasmissione (TOT)
- invia la posizione del satellite rispetto al centro della terra

Ricevitore:

- misura il tempo di arrivo (TOA) secondo il suo clock
- dal TOT ricevuto calcola il "tempo di volo" (TOF = TOA - TOF)
- calcola la sua posizione rispetto al centro della terra
- converte la distanza dal centro della terra in Latitudine, Longitudine e altezza

# Trasmettitore

LimeSDR / USRP



# Ricevitore

# Tutorial
(https://wiki.myriadrf.org/GPS_Simulation)

# Tutorial

- Scaricare e installare https://github.com/osqzss/gps-sdr-sim
- Scaricare una traccia delle traiettorie dei satelliti da "cddis.gsfc.nasa.gov"

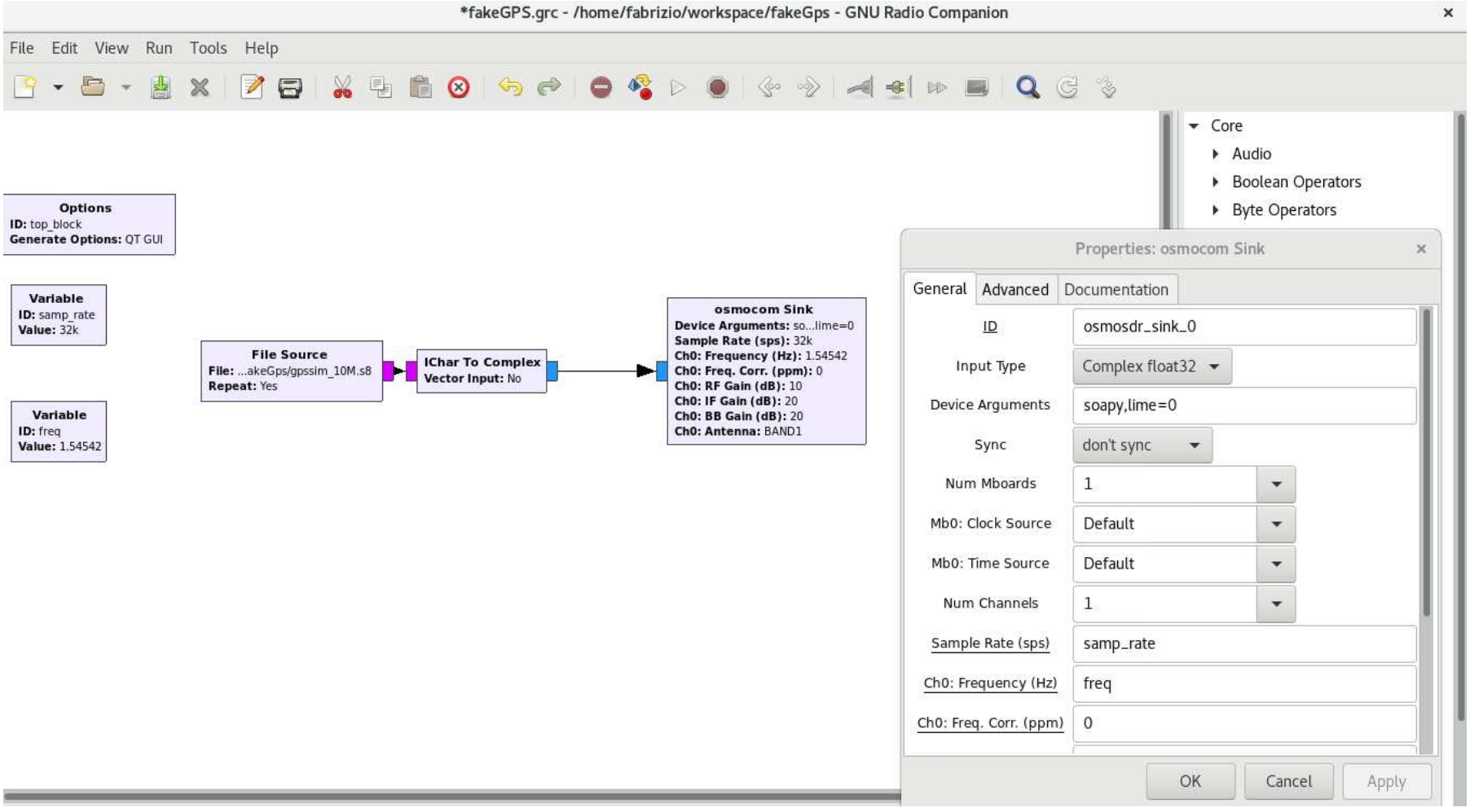
# ?????????

```
Connected to ftp.cddis.eosdis.nasa.gov.
220-********************************************************************
220-                  Welcome to the CDDIS Anonymous FTP Archive
220-
220-
220-This U.S. Government resource is for authorized use only.
220-
220-If not authorized to access this resource, disconnect now.
220-Unauthorized use of, or access to this resource may subject you to
220-disciplinary action or criminal prosecution.
220-
220-By accessing and using this resource, you are consenting to
220-monitoring, keystroke recording or auditing.
220-
220-Please consult the /pub/00readme file for a list of the main
220-directories and their contents.
220-
220-Contact Carey Noll (Carey.Noll@nasa.gov) for further information.
220-********************************************************************
220
```

# Generazione pacchetto

```
$ ./gps-sdr-sim -e brdc0590.17n -l 1.8605853,73.5213033,5 -t 2017/02/28,22:00:00 -o gpssim_10M.s8 -s 10e6 -b 8
Using static location mode.
     9.313e-09    0.000e+00   -5.960e-08    0.000e+00
     9.011e+04    0.000e+00   -1.966e+05    0.000e+00
     1.86264514923e-09   1.77635683940e-15     319488      1938
    18
Start time = 2017/02/28,22:00:00 (1938:252000)
Duration = 600.0 [sec]
02   78.1   5.0  25142702.4   4.5
04  305.9  10.6  24630434.2   4.0
10  244.0  20.9  23656748.6   3.2
12  174.6  31.9  22801339.9   2.6
13   59.8  27.2  23001942.1   2.8
15   80.1  60.3  20615340.0   1.7
18  273.8  42.7  21969027.9   2.1
20    3.4  36.7  22141445.5   2.3
21  322.3  14.4  24860118.2   3.7
24  152.1  21.2  23574508.7   3.2
25  227.1  49.6  21537006.8   1.9
26  310.2   0.2  25799081.3   5.1
29    2.7  52.0  21259731.6   1.8
32  211.7   0.4  25733242.7   5.0
Time into run =  1.6
```

# Gnuradio


*fakeGPS.grc - /home/fabrizio/workspace/fakeGps - GNU Radio Companion
File Edit View Run Tools Help
Options
ID: top_block
Generate Options: QT GUI
Variable
ID: samp_rate
Value: 32k
Variable
ID: freq
Value: 1.54542
File Source
File: ...akeGps/gpssim_10M.s8
Repeat: Yes
IChar To Complex
Vector Input: No
osmocom Sink
Device Arguments: so...lime=0
Sample Rate (sps): 32k
Ch0: Frequency (Hz): 1.54542
Ch0: Freq. Corr. (ppm): 0
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20
Ch0: Antenna: BAND1
Core
Audio
Boolean Operators
Byte Operators
Properties: osmocom Sink
General
Advanced
Documentation
ID
osmosdr_sink_0
Input Type
Complex float32
Device Arguments
soapy,lime=0
Sync
don't sync
Num Mboards
1
Mb0: Clock Source
Default
Mb0: Time Source
Default
Num Channels
1
Sample Rate (sps)
samp_rate
Ch0: Frequency (Hz)
freq
Ch0: Freq. Corr. (ppm)
0
OK
Cancel
Apply

# Conclusioni

Grazie dell'attenzione

# Conclusioni

## Grazie dell'attenzione


... e grazie ai "radiopresibene"