Low-cost GPS simulator – GPS spoofing by SDR

Presentation · August 2015

CITATIONS
35

READS
24,882

2 authors, including:

Lin Huang

46 PUBLICATIONS **375** CITATIONS

SEE PROFILE

GPS SPOOFING

Low-cost GPS simulator

HUANG Lin, YANG Qing
Unicorn Team – Radio and Hardware Security Research
Qihoo 360 Technology Co. Ltd.

Who we are? Unicorn Team

- Qihoo360's UnicornTeam consists of a group of brilliant security researchers. We focus on the security of anything that uses radio technologies, from small things like RFID, NFC and WSN to big things like GPS, UAV, Smart Cars, Telecom and SATCOM.
- Our primary mission is to guarantee that Qihoo360 is not vulnerable to any wireless attack. In other words, Qihoo360 protects its users and we protect Qihoo360.
- During our research, we create and produce various devices and systems, for both attack and defense purposes.
- We are one of the DEF CON 23 vendors. https://defcon.org/html/defcon-23/dc-23-vendors.html

YANG Qing

- YANG Qing is the team leader of Unicorn Team.
- He has rich experiences in wireless and hardware security area, including WiFi penetration testing, cellular network interception, IC card cracking etc. His interests also cover embedded system hacking, firmware reversing, automotive security, and software radio.
- He is the first one who reported the vulnerabilities of WiFi system and RF IC card system used in Beijing subway.

HUANG Lin

- One of the early USRP users in China. Got the first USRP board in 2005 in Orange Labs
- Authored some tutorials about GNU Radio which were popular in China
- Made great effort on promoting Cloud-RAN technology in China from 2010 to 2013
- Join Qihoo 360 as a wireless security researcher in 2014

Beginning of the story …

Civilian-use GPS C/A Signal

GPS C/A signal is for civilian usage, and unencrypted.

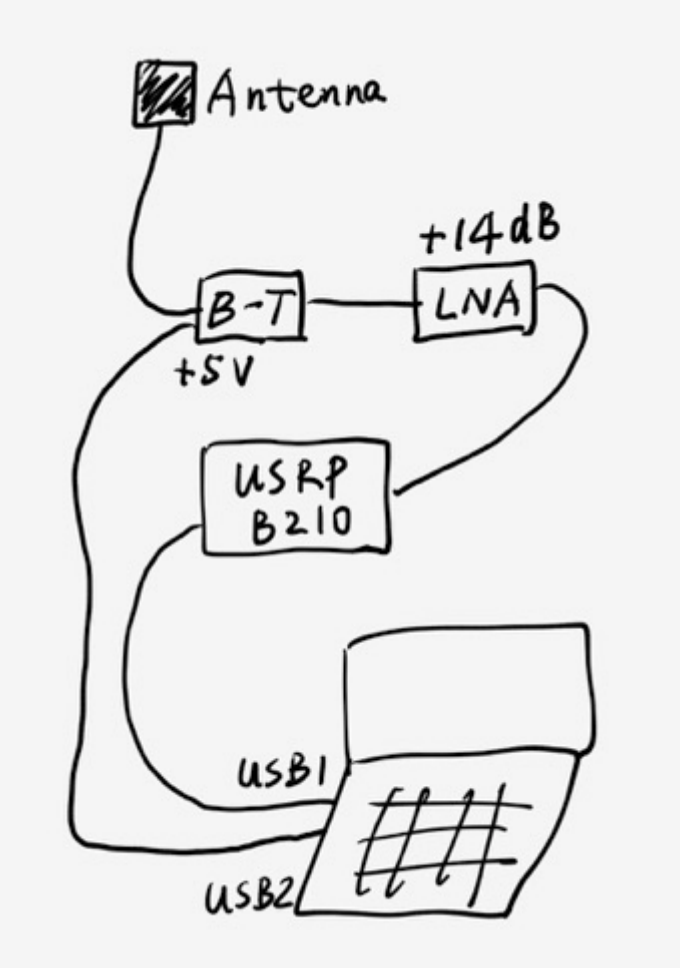
Replay attack is a typical GPS spoofing method.

Record

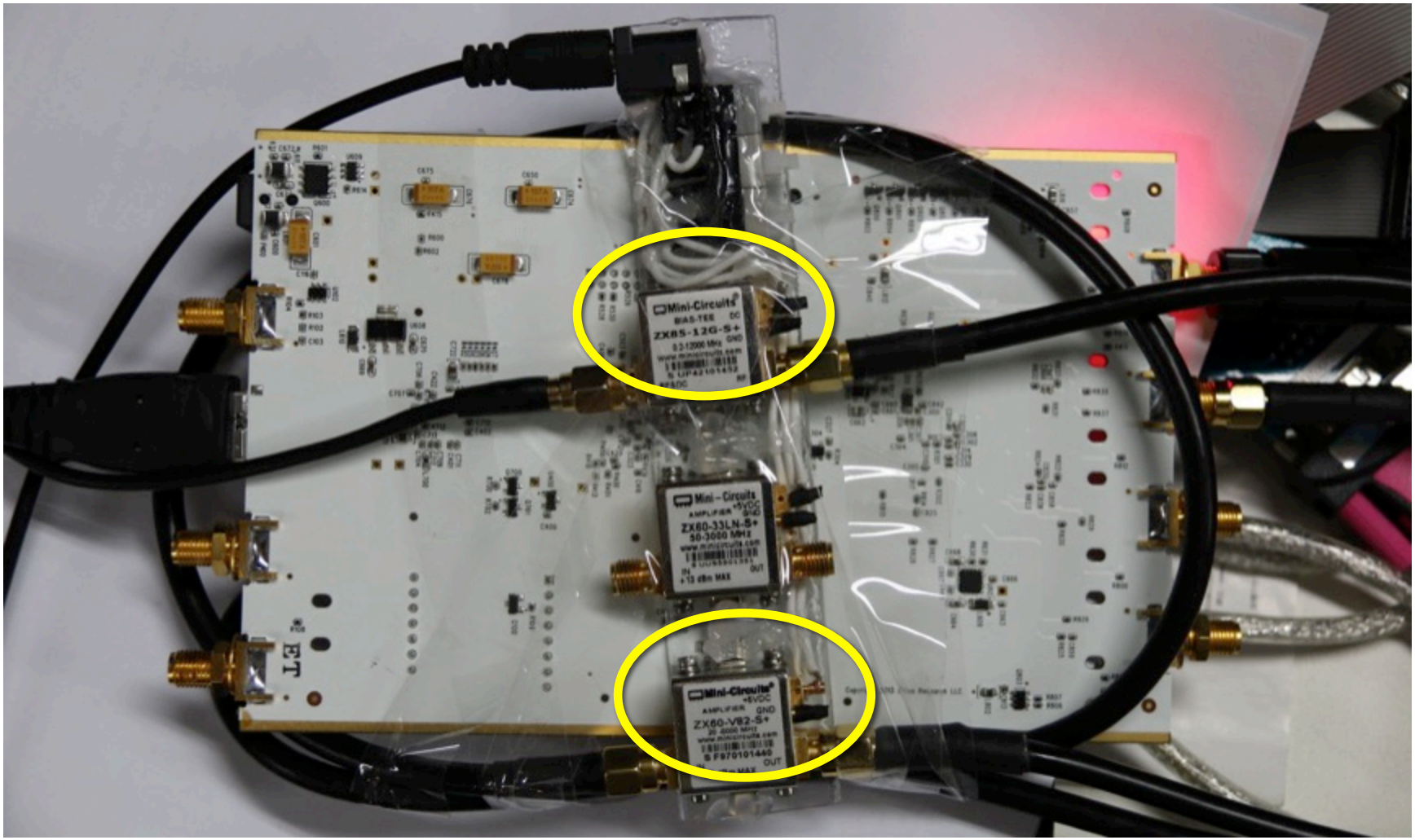
Replay

Firstly try replay attack

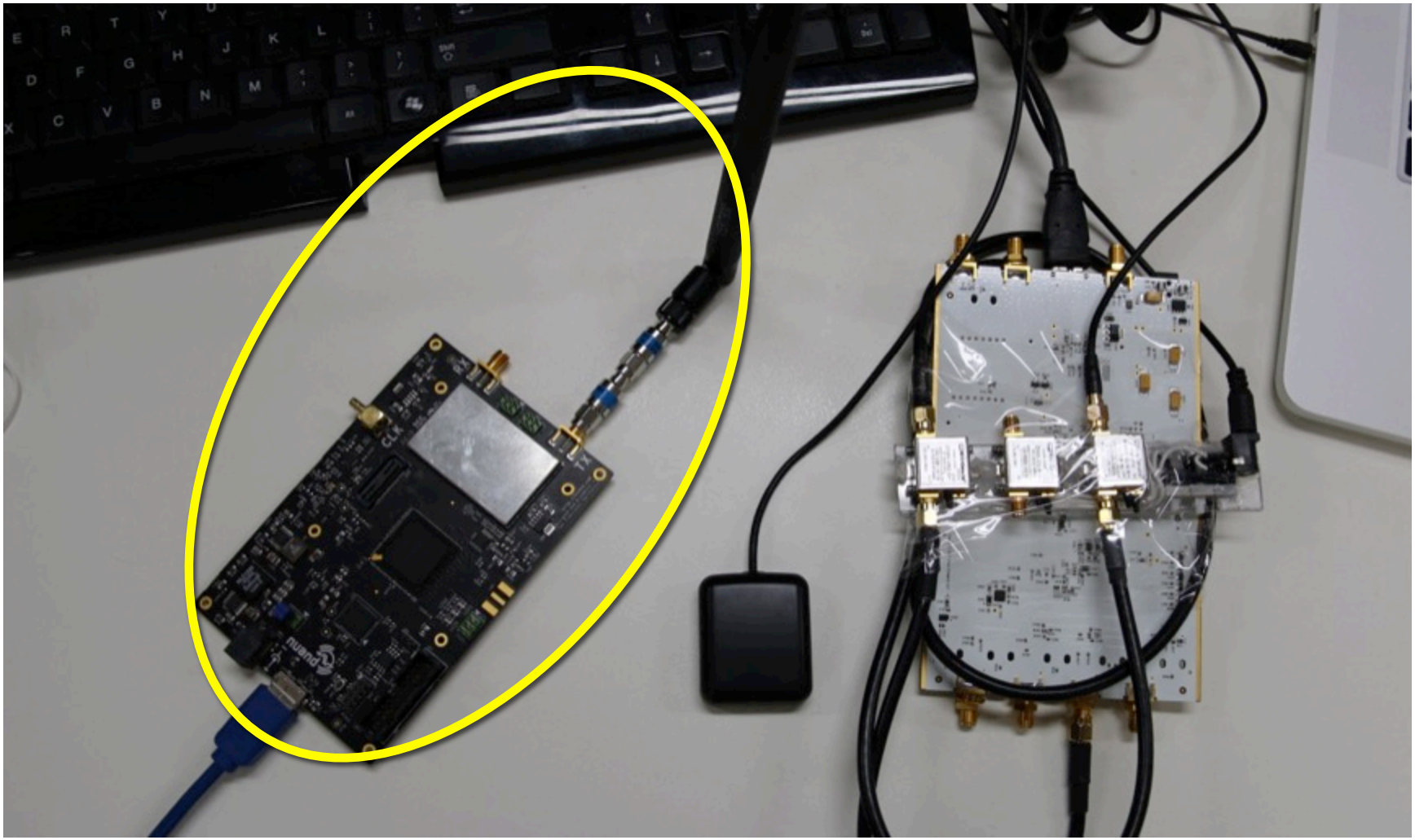
- Hardware
  - USRP B210
  - Active GPS antenna
  - Bias-tee circuit (Mini-Circuit ZX85-12G-S+)
  - LNA (Mini-Circuit ZX60-V82-S+)



Record GPS signal by a USRP B210



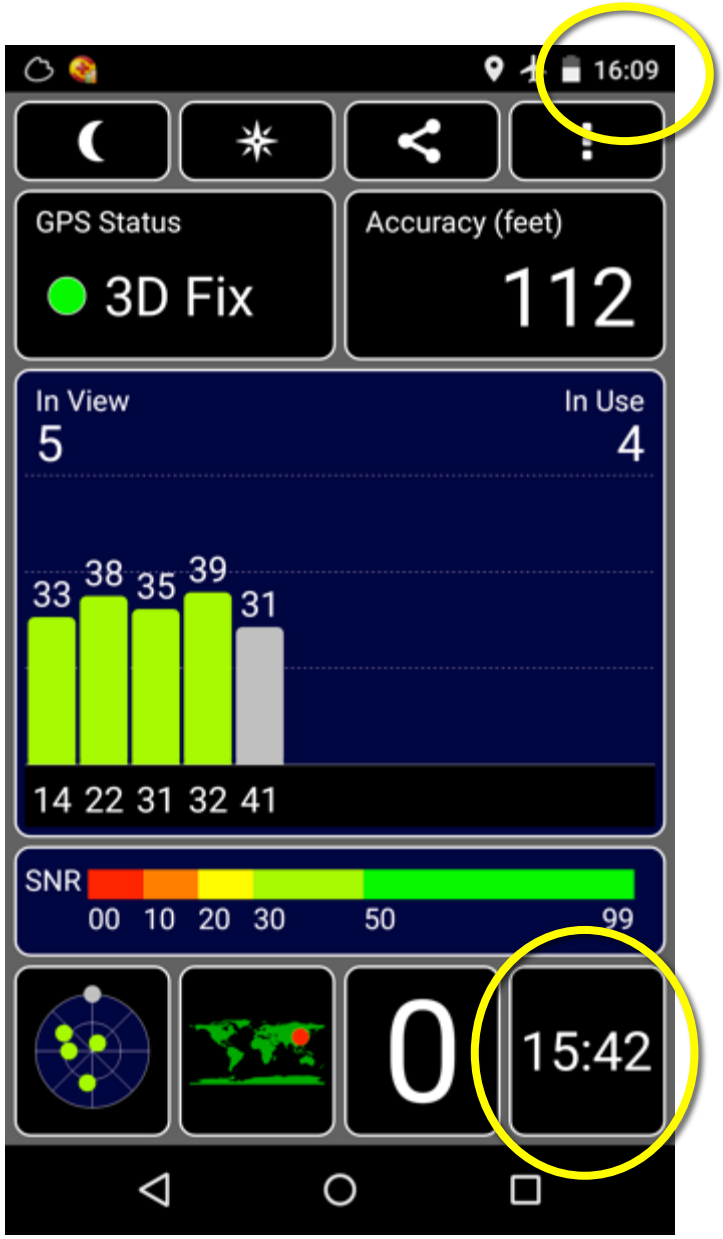
Replay the signal by a bladeRF



Success!

Record then replay the GPS signal. You can see the cellphone gets the position and timing information from the replayed GPS signal.

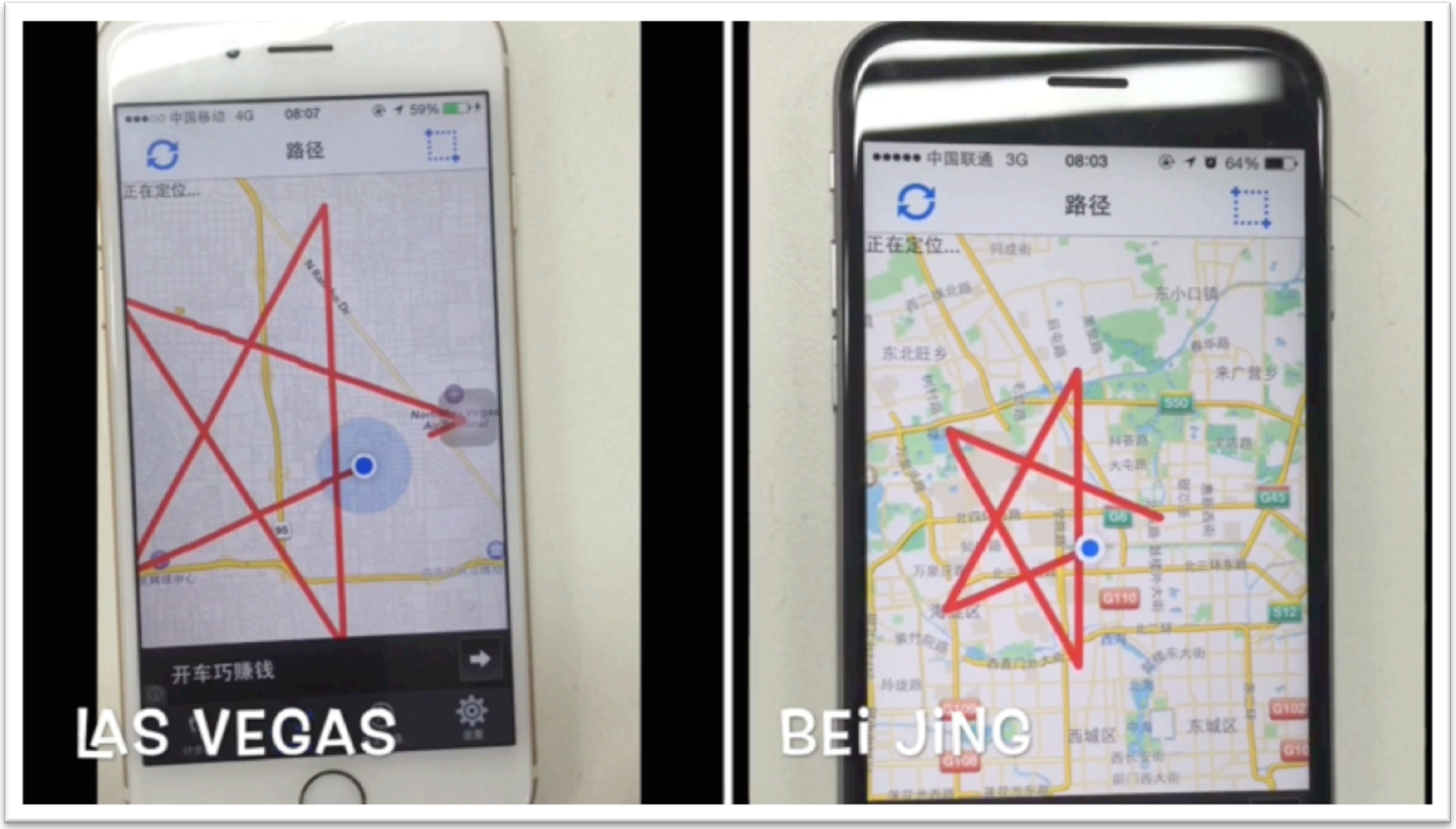
Nexus 5



If Create any GPS signal
rather than Record & Replay…

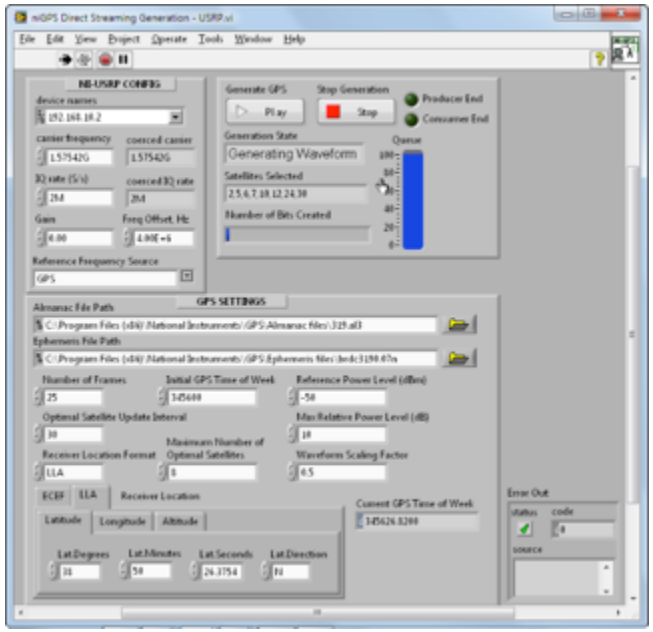
This is not a replay

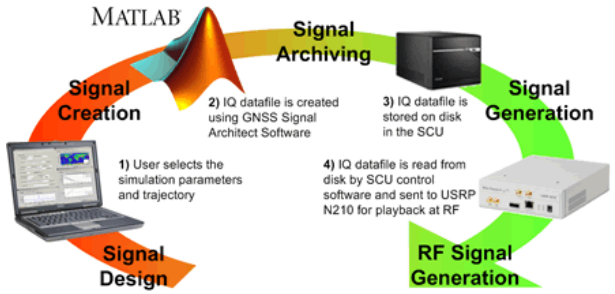
- Demo video



Search existing solutions on Internet

- Expensive or at least not free
  - NI LabVIEW ~$6000
  - NAVSYS ~$5000





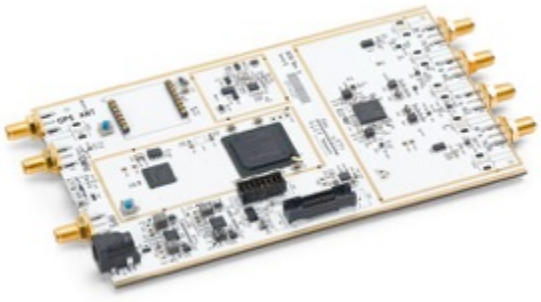
Some famous cases of GPS spoofing

- Leading lab: RadioNavigation Lab from Univ. of Texas at Austin (https://radionavlab.ae.utexas.edu/)
- Prof. Todd E. Humphrey and his team
  - 2012 TED talk: how to fool GPS
  - 2013: spoof an US$80M yacht at sea
  - 2014: unmanned aircraft capture via GPS spoofing

We are not navigation experts.
How can we do GPS spoofing?

As SDR guys, we have

USRP



bladeRF

HackRF

And we found some source codes on Internet

- This website collects many open source projects about GPS
- http://www.ngs.noaa.gov/gps-toolbox/index.html

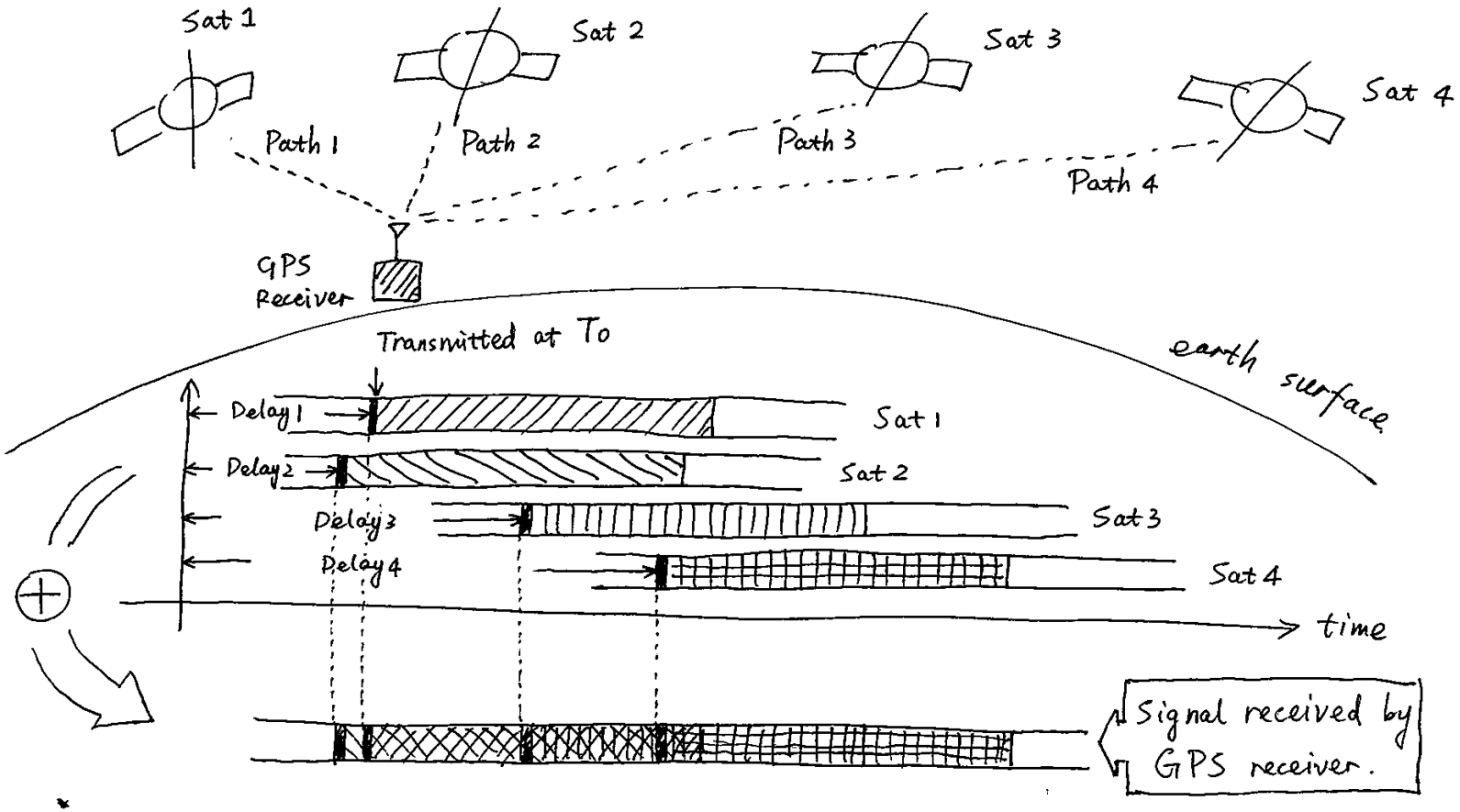
- This is a very good GPS receiver software based on GNU Radio
- http://gnss-sdr.org/

- Most of projects are GPS receivers and few are transmitters. This is a transmitter example: https://code.csdn.net/sywcxx/gps-sim-hackrf
- It's not finalized ☹

DIY a GPS Simulator!

Basic principle of GPS system

GPS principle



Mathematics time

$$\text{Delay}_1 \cdot C = \text{Path}_1$$

$$(T_1 - T_0) \cdot C$$

$$\text{Position}(\text{Sat}_1) - \text{Position}(RX)$$

$$(T + D_1 - T_0) \cdot C = \text{Pos}(x_1, y_1, z_1) - \text{Pos}(x, y, z)$$

4 equations

$$\begin{cases} (T + D_1 - T_0) \cdot C = \text{Pos}(x_1, y_1, z_1) - \text{Pos}(x, y, z) \\ (T + D_2 - T_0) \cdot C = \text{Pos}(x_2, y_2, z_2) - \text{Pos}(x, y, z) \\ (T + D_3 - T_0) \cdot C = \text{Pos}(x_3, y_3, z_3) - \text{Pos}(x, y, z) \\ (T + D_4 - T_0) \cdot C = \text{Pos}(x_4, y_4, z_4) - \text{Pos}(x, y, z) \end{cases}$$

Key information in Pseudo-range equations

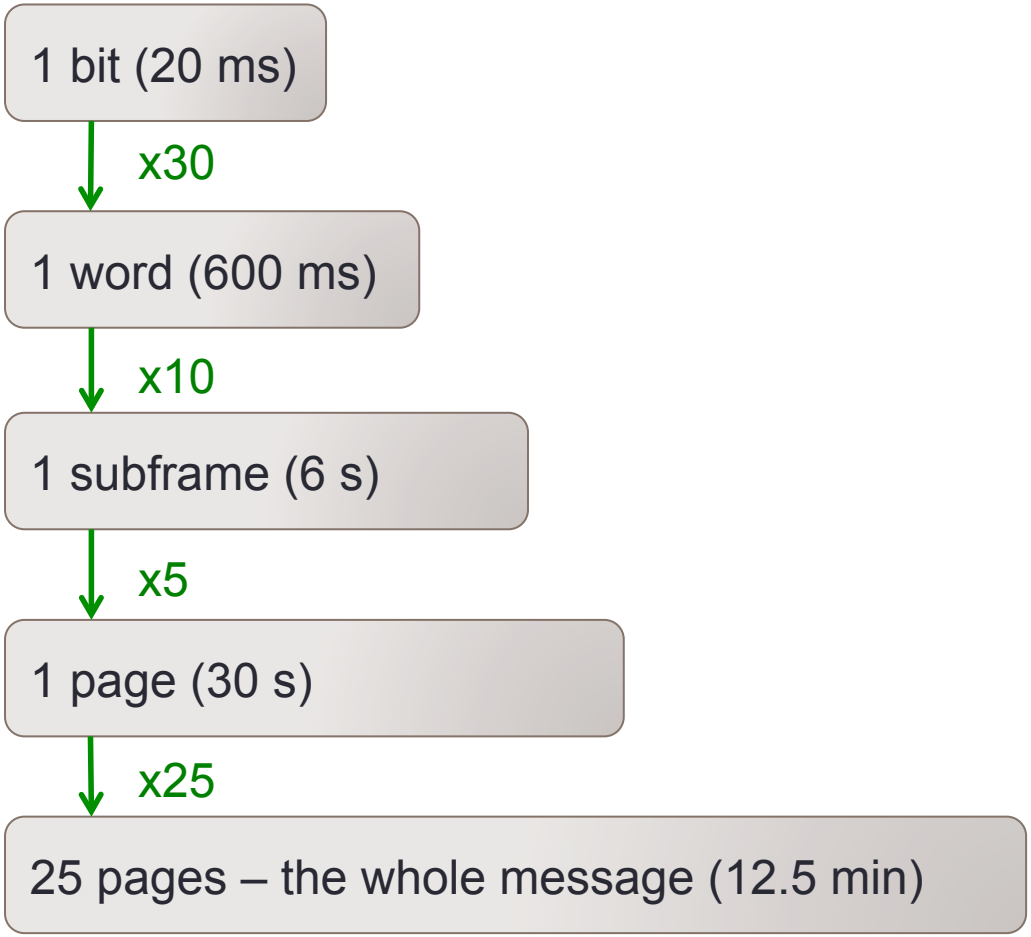
$$\begin{cases} (T + D_1 - T_0) \cdot C = Pos(x_1, y_1, z_1) - Pos(x, y, z) \\ (T + D_2 - T_0) \cdot C = Pos(x_2, y_2, z_2) - Pos(x, y, z) \\ (T + D_3 - T_0) \cdot C = Pos(x_3, y_3, z_3) - Pos(x, y, z) \\ (T + D_4 - T_0) \cdot C = Pos(x_4, y_4, z_4) - Pos(x, y, z) \end{cases}$$

Calculate the delays at receiver

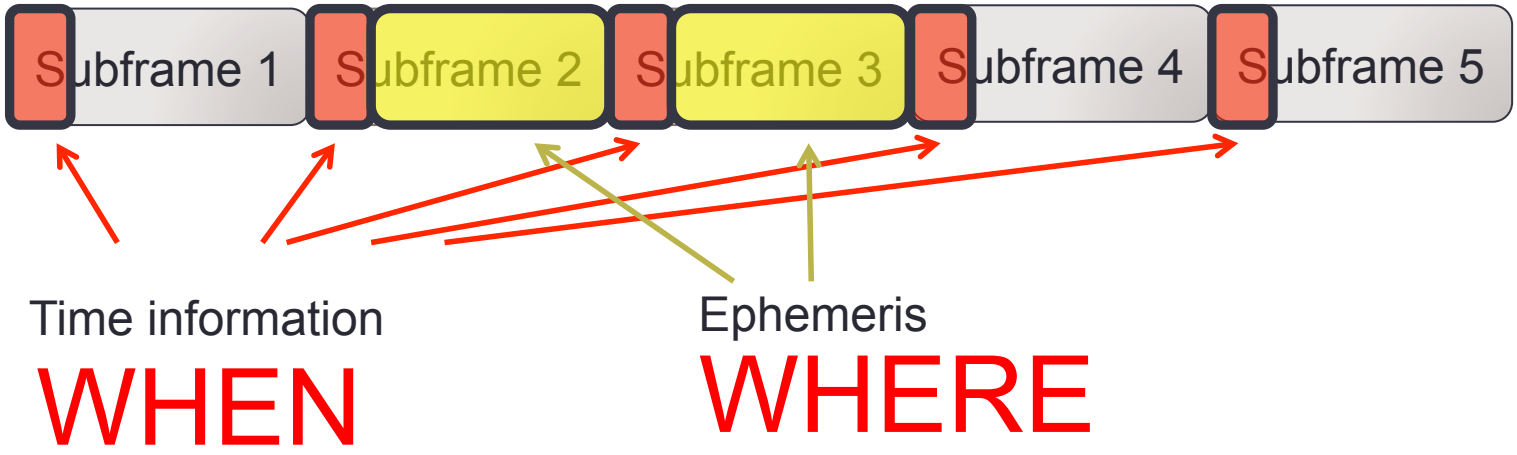
WHEN

WHERE

Structure of message



Info of WHEN & WHERE



Start building the signal

Get Ephemeris data

- Method 1
  - Download ephemeris data file from CDDIS website
  - ftp://cddis.gsfc.nasa.gov/gnss/data/daily/
  - Here we can only get yesterday's ephemeris data
- Method 2
  - Use 'gnss-sdr' program to receive the real-time GPS signal and get the fresh ephemeris data
  - The 'GSDR*' files are the decoded ephemeris data, in standard RINAX format.

Decode the fresh ephemeris data

- Software
  - Run ‘gnss-sdr’
  - Get the GSDR* file

GSDR076o52.15O (~/gnss-sdr/install) - gedit

Open Save Undo

GSDR076o52.15O

```
     3.02           OBSERVATION DATA    G                   RINEX VERSION / TYPE
G = GPS  R = GLONASS  E = GALILEO  S = GEO  M = MIXED       COMMENT
GNSS-SDR            test                20150317 065317 UTC PGM / RUN BY / DATE
GPS OBSERVATION DATA FILE GENERATED BY GNSS-SDR             COMMENT
GNSS-SDR VERSION 0.0.5                                      COMMENT
See http://gnss-sdr.org                                     COMMENT
DEFAULT MARKER NAME                                         MARKER NAME
test                CTTC                                    OBSERVER / AGENCY
GNSS-SDR            Software Receiver   0.0.5               REC # / TYPE / VERS
Antenna number      Antenna type                            ANT # / TYPE
        0.0000        0.0000        0.0000                  APPROX POSITION XYZ
        0.0000        0.0000        0.0000                  ANTENNA: DELTA H/E/N
G    4 C1C L1C D1C S1C                                      SYS / # / OBS TYPES
DBHZ                                                        SIGNAL STRENGTH UNIT
  2015    02    18    03    11   18.9888020     GPS         TIME OF FIRST OBS
                                                            END OF HEADER

> 2015 02 18 03 11 18.9888020  0  4
G15  20626320.695     -26816.471      -800.296        39.051
G18  22239572.066    -133214.378     -4288.659        46.460
G21  21383921.751     -82740.741     -2525.623        43.862
G24  21475647.374     147039.064      4495.737        48.170
> 2015 02 18 03 11 19.0888020  0  4
G15  20626320.695     -26898.093      -835.858        39.383
G18  22239508.275    -133643.231     -4284.667        48.544
G21  21383895.373     -82993.548     -2529.366        47.246
G24  21475579.942     147489.612      4507.612        47.516
> 2015 02 18 03 11 19.1888020  0  4
G15  20626320.695     -26979.672      -859.714        41.132
G18  22239443.669    -134071.995     -4272.785        45.715
G21  21383862.854     -83246.301     -2514.986        44.122
G24  21475512.816     147940.110      4497.862        46.267
> 2015 02 18 03 11 19.2888020  0  4
G15  20626320.695     -27061.162      -819.067        40.970
G18  22239376.106    -134500.738     -4297.145        47.513
```

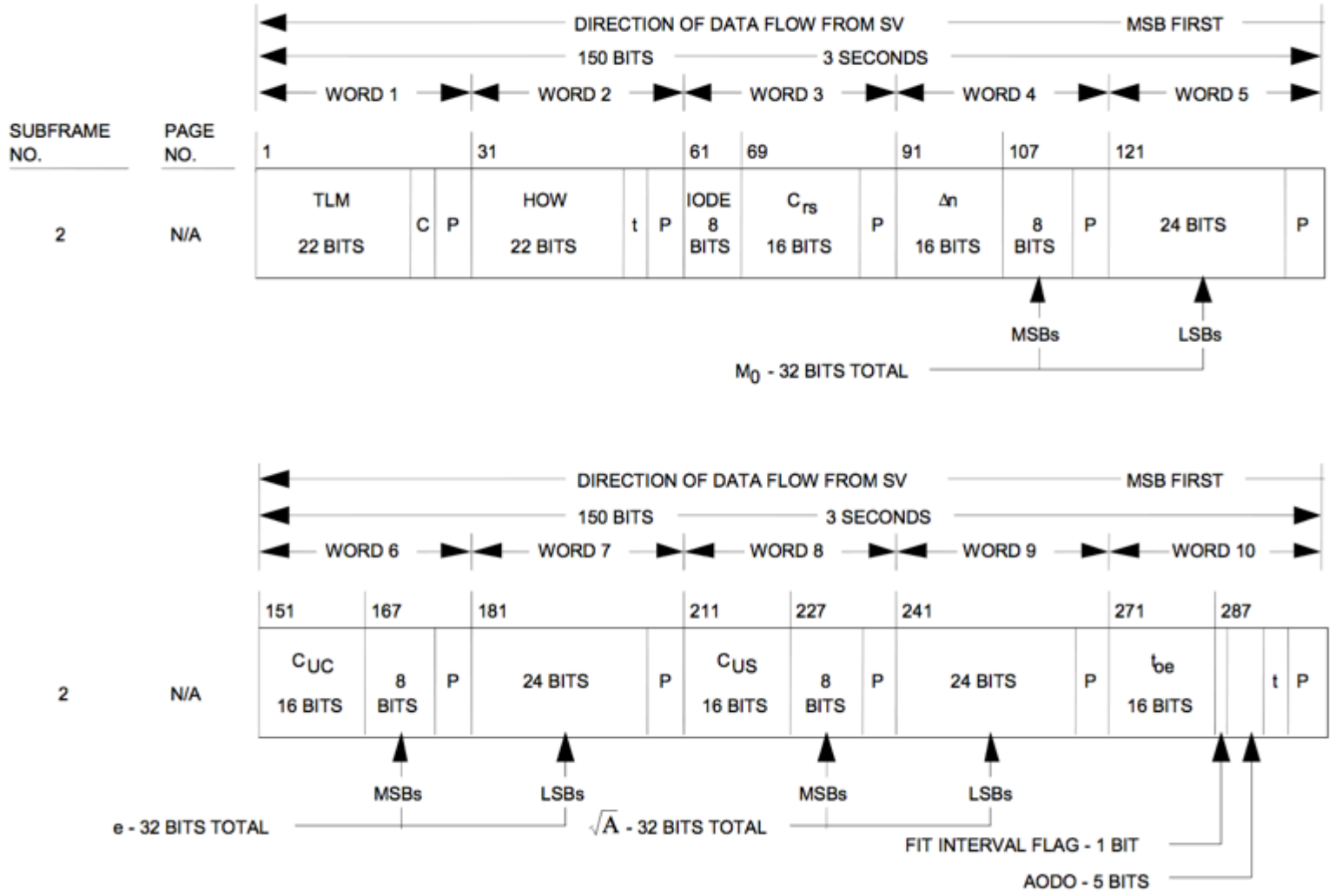
Plain Text Tab Width: 8 Ln 1, Col 1 INS

360UNICORNTEAM

Matlab code of GPS simulator

```
ear global;
:;
bal SimGlobal;
bal CI;
p('-----------------');
.t;
p('-----------------');

 set datafile name
afilename = 'test.dat';
ameris_file = 'brdc0450.15n';

mGlobal.noeph,SimGlobal.aEphData]=readrinex(ephameris_file);% read ephemeris data
Global.aSatData=selecteph;% select ephemeris data
visible;% decide which satellite is visible
message_wo_almanac;% generate telegraph
rmessage;
nnel_data = genchannel;
signal(channel_data,datafilename);
```

Example: structure of Subframe 2

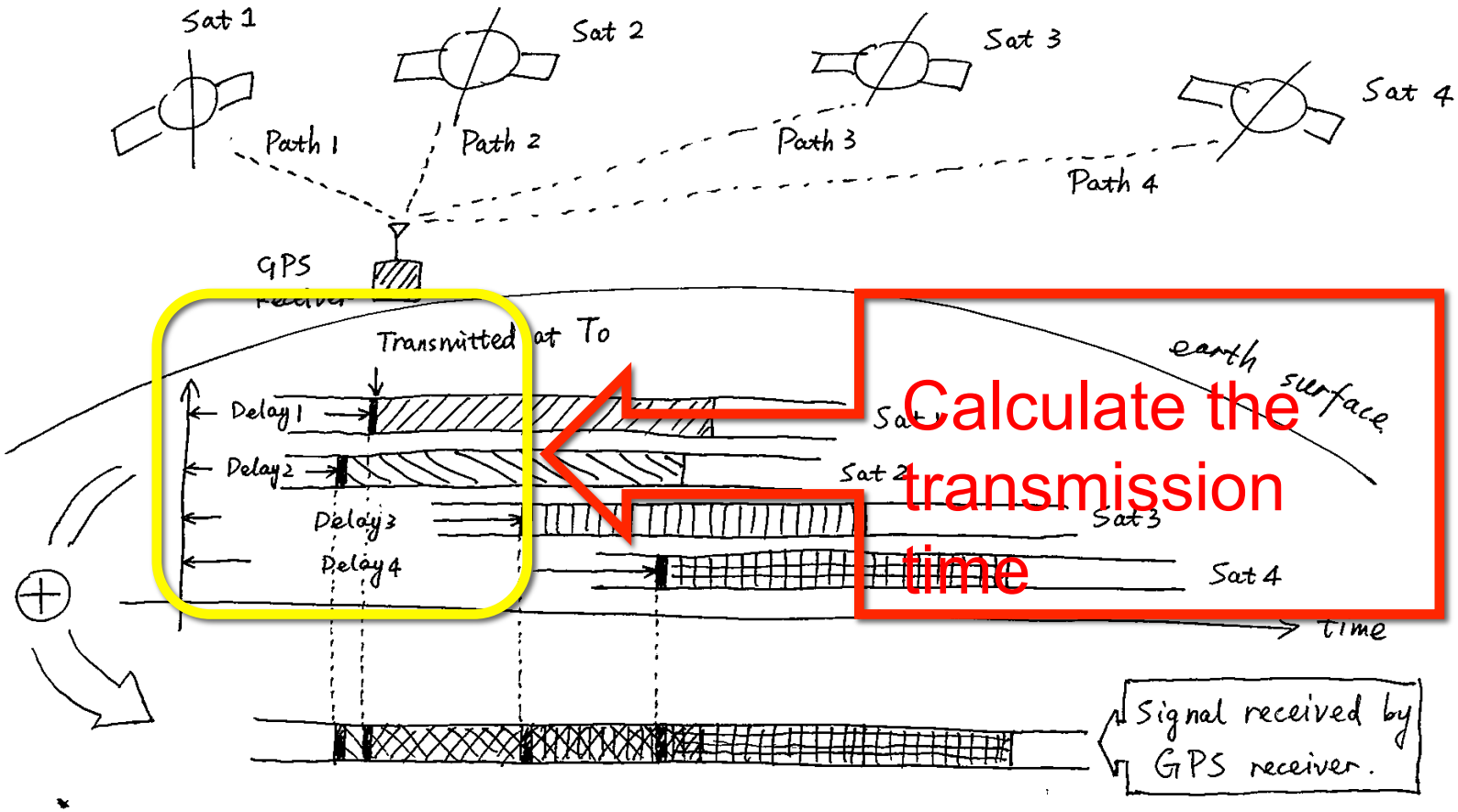


Generate navigation message

```
for i=1:CT.MaxSatNum
    pO=SimGlobal.aSatData(i).sOrbitData;
    pN=SimGlobal.aSatData(i).sNavData;
    pE=SimGlobal.aSatData(i).sOrbitData.sEphData;
    pA=SimGlobal.aSatData(i).sOrbitData.sAlmData;
    if(pO.visflag==1)
        visual_counter = visual_counter+1;
        disp(['Satalite ' num2str(i) ' telegraph for ' num2str(visual_counter) 'th channel generating...']);
        for idx_page = 1:25
            for idx_subfrm = 1:5
                switch idx_subfrm
                    case 1 % subframe 1...
                    case 2 % subframe 2...
                    case 3 % subframe 3...
                    case 4 % subframe 4...
                    case 5 % subframe 5...

                end % end of switch idx_subfrm
            end % end of loop idx_subfrm
        end % end of loop idx_page
    end % end of visible
end % end of loop satelite
disp(['Total ' num2str(visual_counter) ' satelite telegraphs are generated' ]);
end
```

Bits ➔ Waveform

GPS principle again

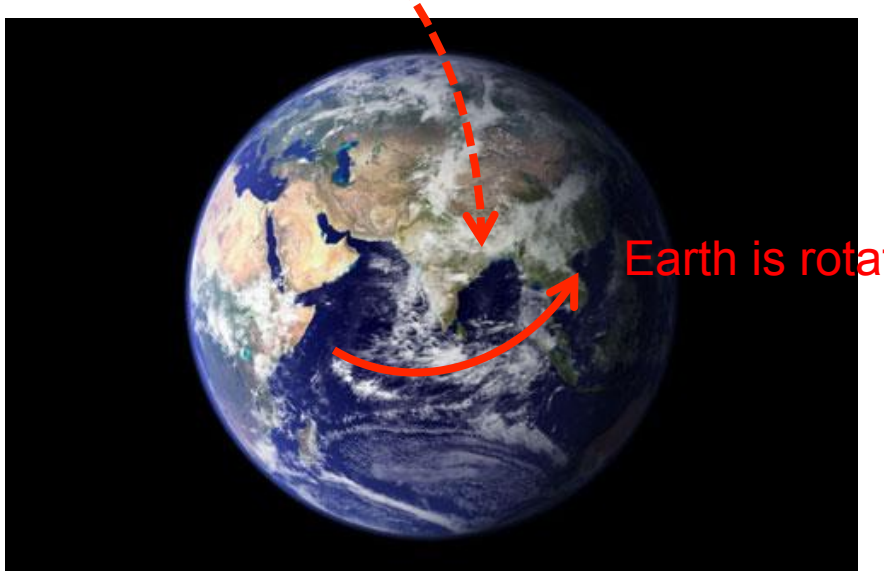


How to calculate transmission time

Satellite is moving

Calculate the length of signal path

Calculate the coordinate according to ephemeris data



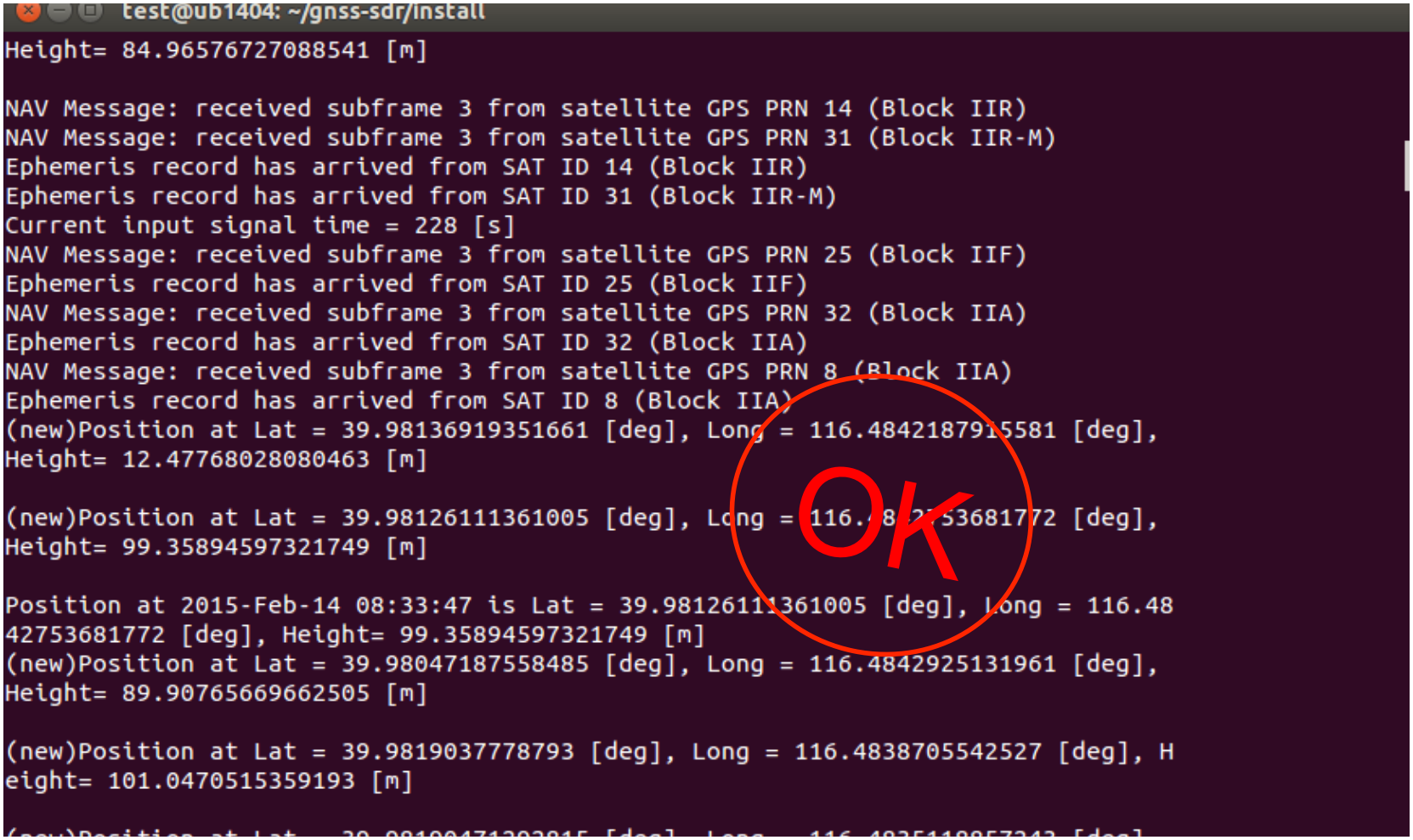
Earth is rotating

NOT EASY

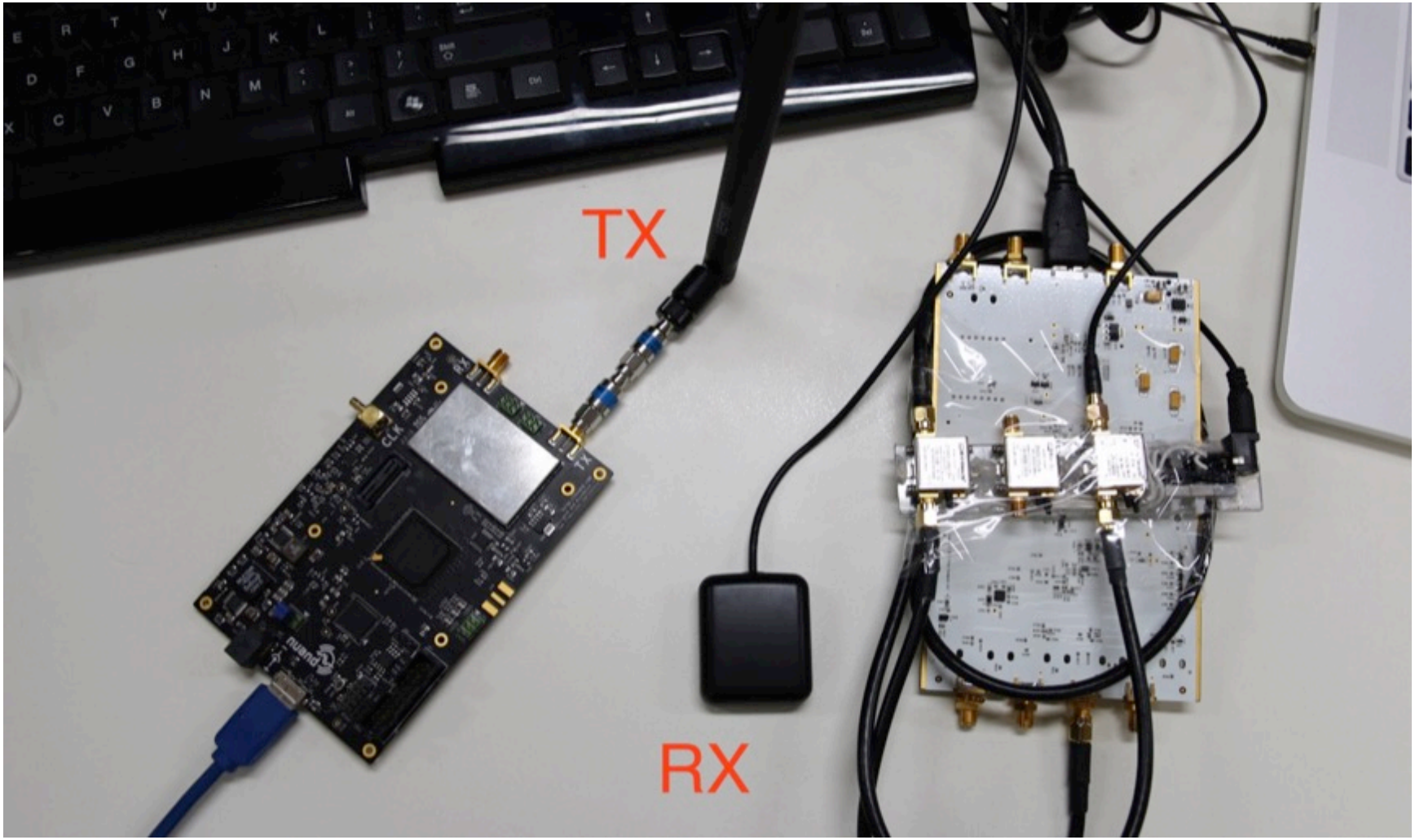
Matlab code of generating waveform

```
ear global;
:;
bal SimGlobal;
bal CI;
p('-----------------');
.t;
p('-----------------');

 set datafile name
afilename = 'test.dat';
ameris_file = 'brdc0450.15n';

mGlobal.noeph,SimGlobal.aEphData]=readrinex(ephameris_file);% read ephemeris data
Global.aSatData=selecteph;% select ephemeris data
visible;% decide which satellite is visible
message_wo_almanac;% generate telegraph
rmessage;
nnel_data = genchannel;
signal(channel_data,datafilename);
```

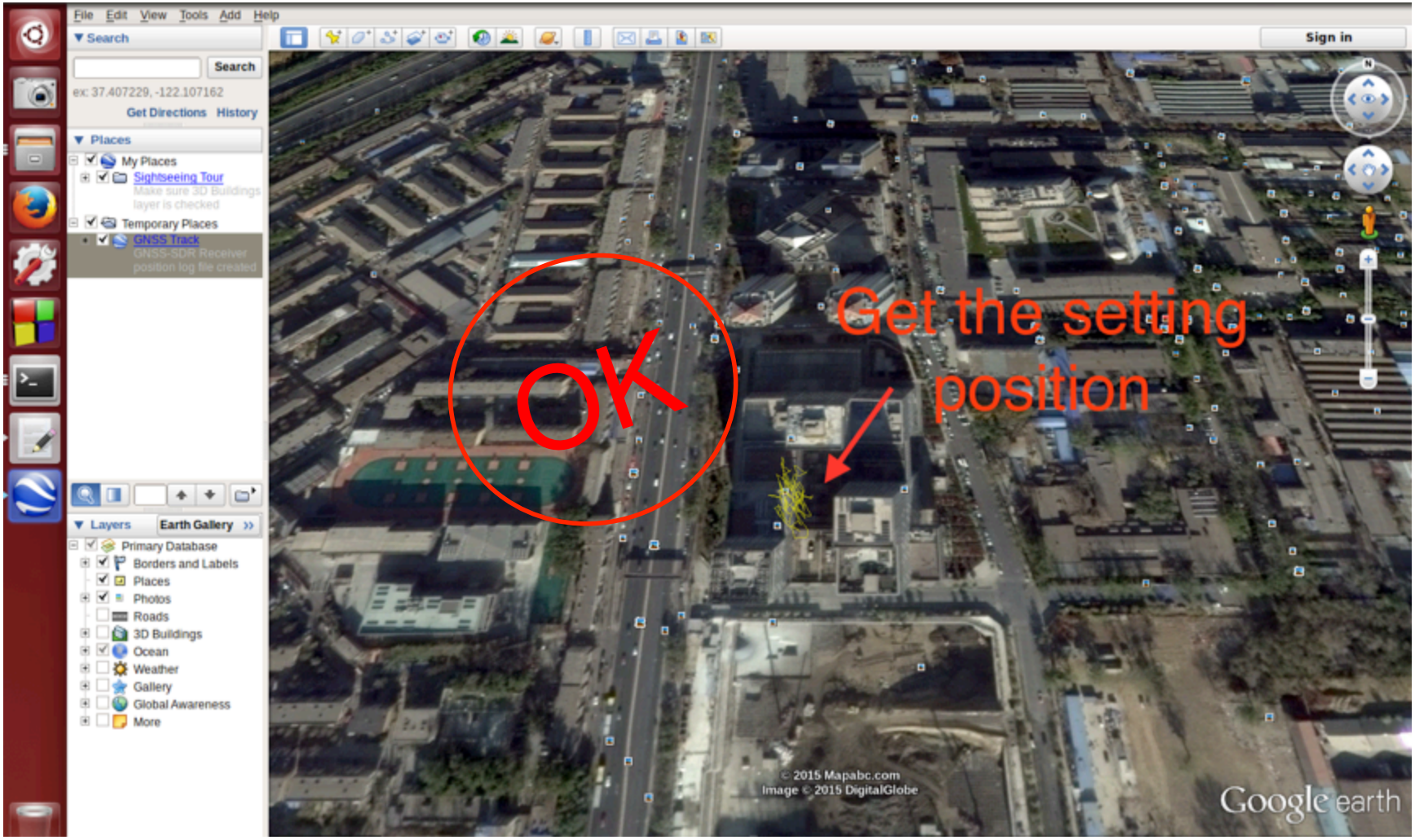
Firstly offline verify the signal by ‘gnss-sdr’



Secondly verify it by transmitting GPS signal file over air by bladeRF



Soft-receiver ‘gnss-sdr’ demod the signal

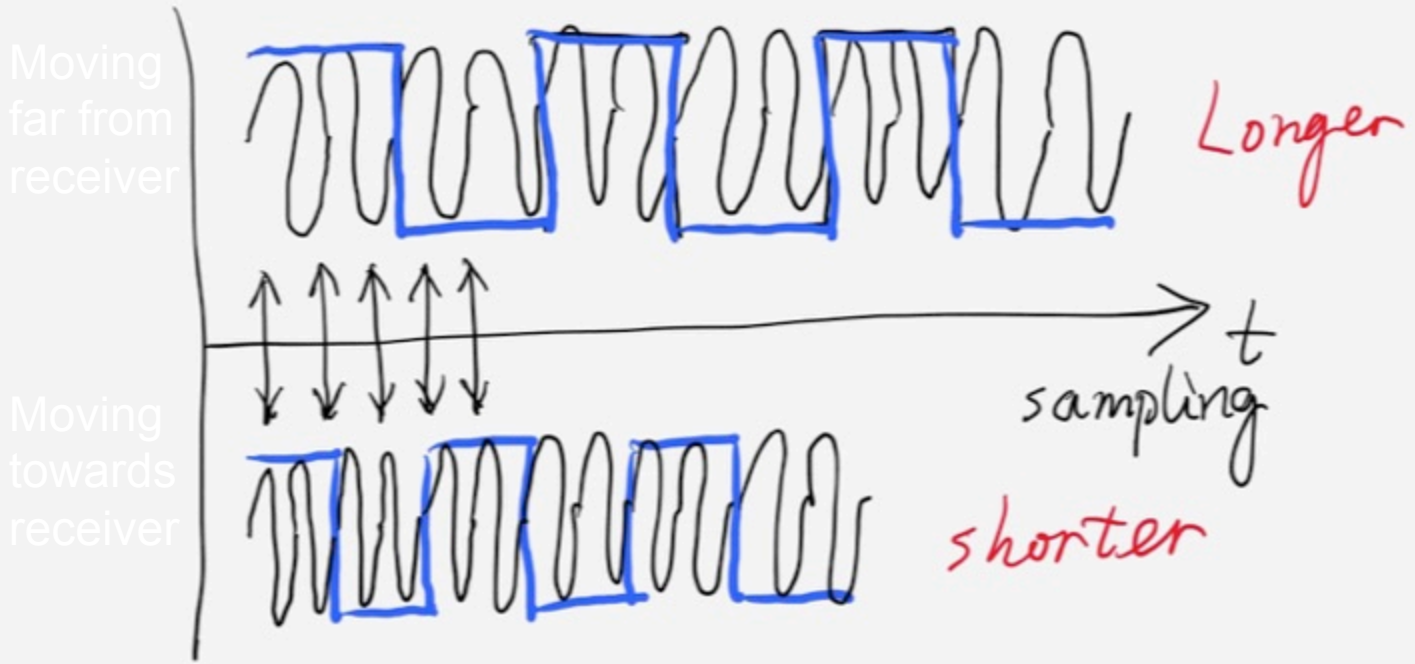


Try to spoof cellphone's GPS …

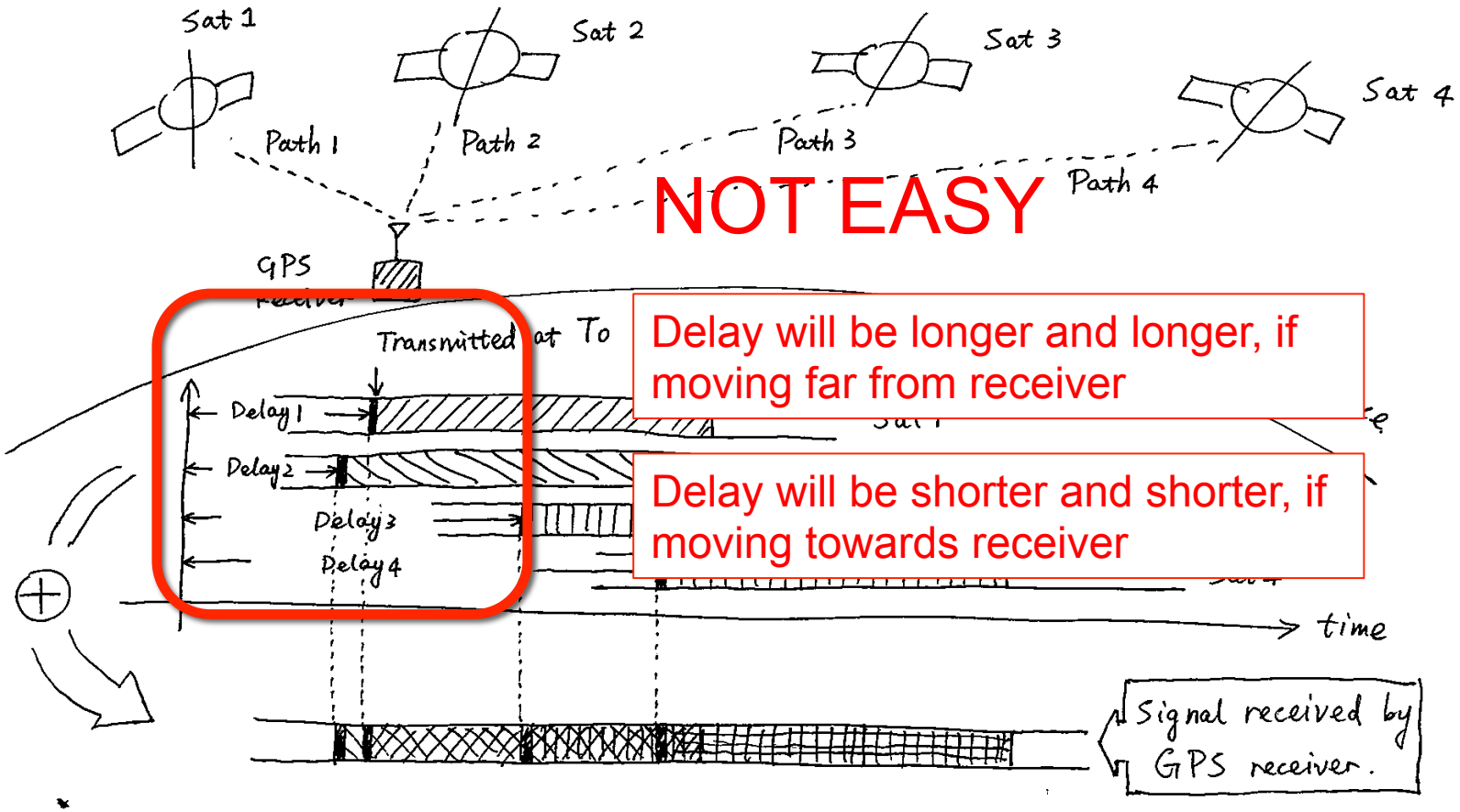
Which part is not perfect?

Doppler effect

Another challenge: Doppler effect

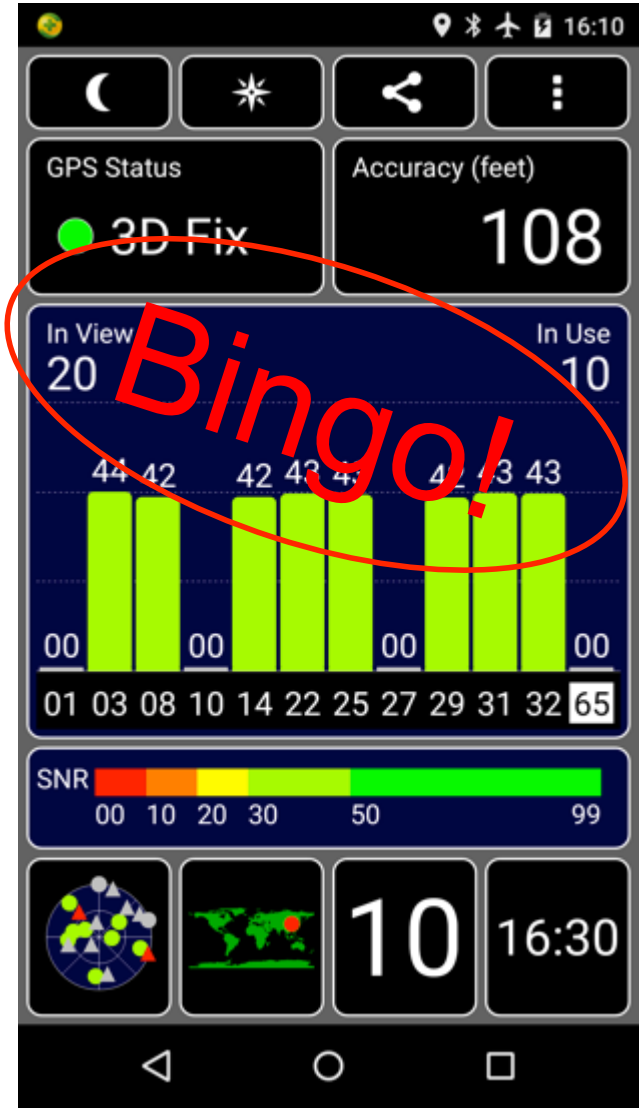


GPS principle again

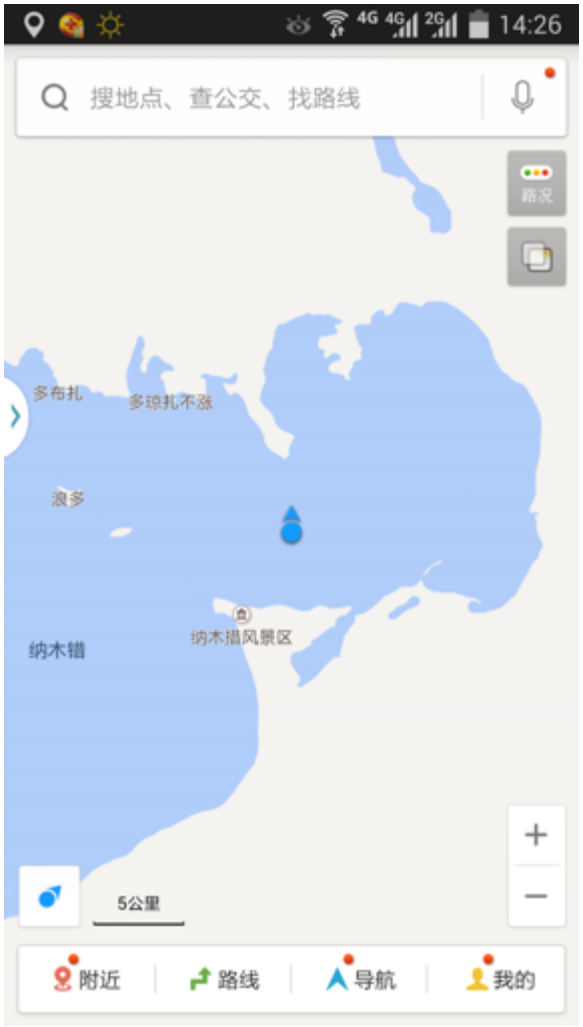


Try cellphone again

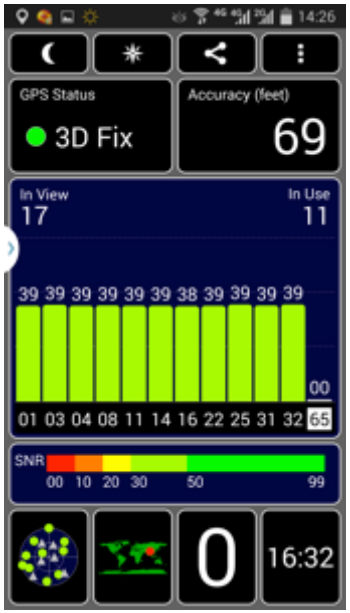
- Nexus 5 GPS chipset
  - Satellites are detected as pre-setting.
  - Satellite signal strengths are same as we defined.
  - 3D fixed by simulated signal

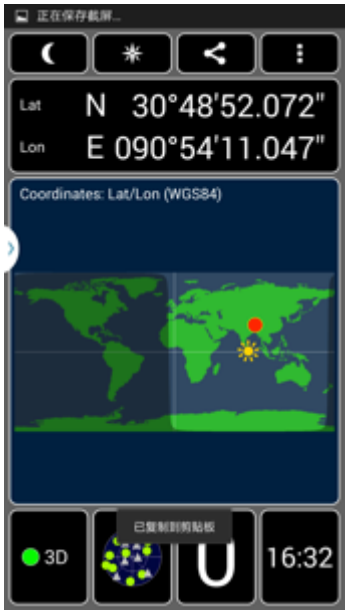


Bingo! Samsung Note 3

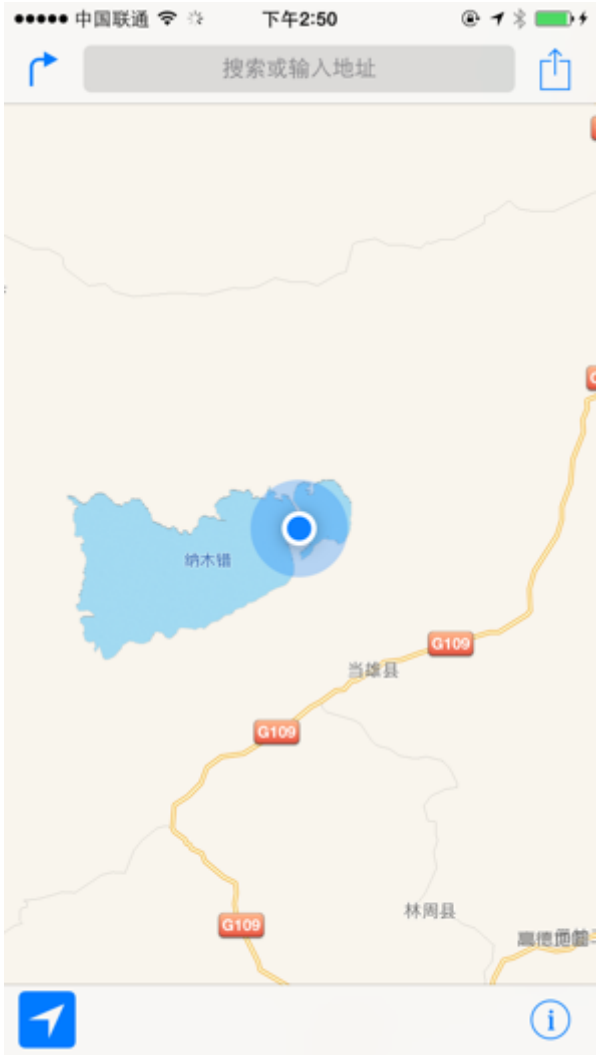


- Located at Namco Lake in Tibet but the cellphone is actually in Beijing.

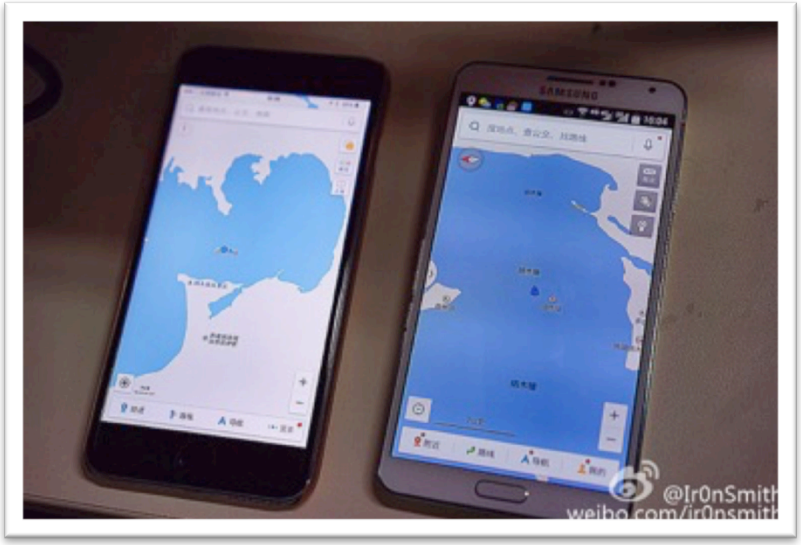




Bingo! iPhone 6



- Namco Lake in Tibet
- iPhone positioning is much slower.
- The cellphone clock was also reset to wrong time if auto-calibration is enabled.



Set any time

- You may find the date we set is always Feb. 14 2015. This is because the ephemeris data file we use is at that day.

- Actually not only space, but also time, can be spoofed.

A cellphone in future time

We set the time as Aug. 6, 2015 (today is Jul. 14) and position as Las Vegas.

Try to spoof cars

- Demo video: The car, BYD Qin,was located in a lake center.

DJI drone - forbidden area policy

- To avoid the risk from drone,to people and to critical facilities, drone flying are forbidden in many cities.

- For example, DJI drone's engine will keep off when it finds the position is in forbidden area.

A drone that crashed on the grounds of the White House had evaded radar detection.

Try to spoof DJI drone

- Demo video: Disable forbidden area
- The drone is actually at a forbidden location in Beijing. We gave it a fake position in Hawaii, then it was unlocked and can fly up.

Try to spoof DJ drone

- Demo video: Hijack flying drone
- We gave a forbidden position to a flying drone, then it would automatically land.

Lessons – how to anti-spoof

- Application layer
  - Now usually GPS has highest priority. Cellphone is spoofed even if it has cellular network connection.
  - Use multi-mode positioning, GLONASS, Beidou
  - Jointly consider cellular network and wifi positioning
- Civil GPS receiver chipset
  - Use some algorithms to detect spoofing
- Civil GPS transmitter
  - Add digital signatures into the extensible GPS civil navigation message

GPS is still a great system

- First global positioning system
- Usable for all of the world
- Very low cost, small size…

- It keeps updating,so we believe the security issue will be improved in future.

Acknowledgment

- JIA Liwei
  - Graduate student of BUAA,majoring radio navigation
  - https://code.csdn.net/sywcxx/gps-sim-hackrf

- JIAO Xianjun
  - Senior iOS RFSW engineer at Apple, SDR amateur
  - http://sdr-x.github.io/

360UNICORNTEAM

Thank you!