GPS SPOOFING

By Low-cost SDR Tools

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 vendors in POC 2015. Welcome to visit our booth ☺

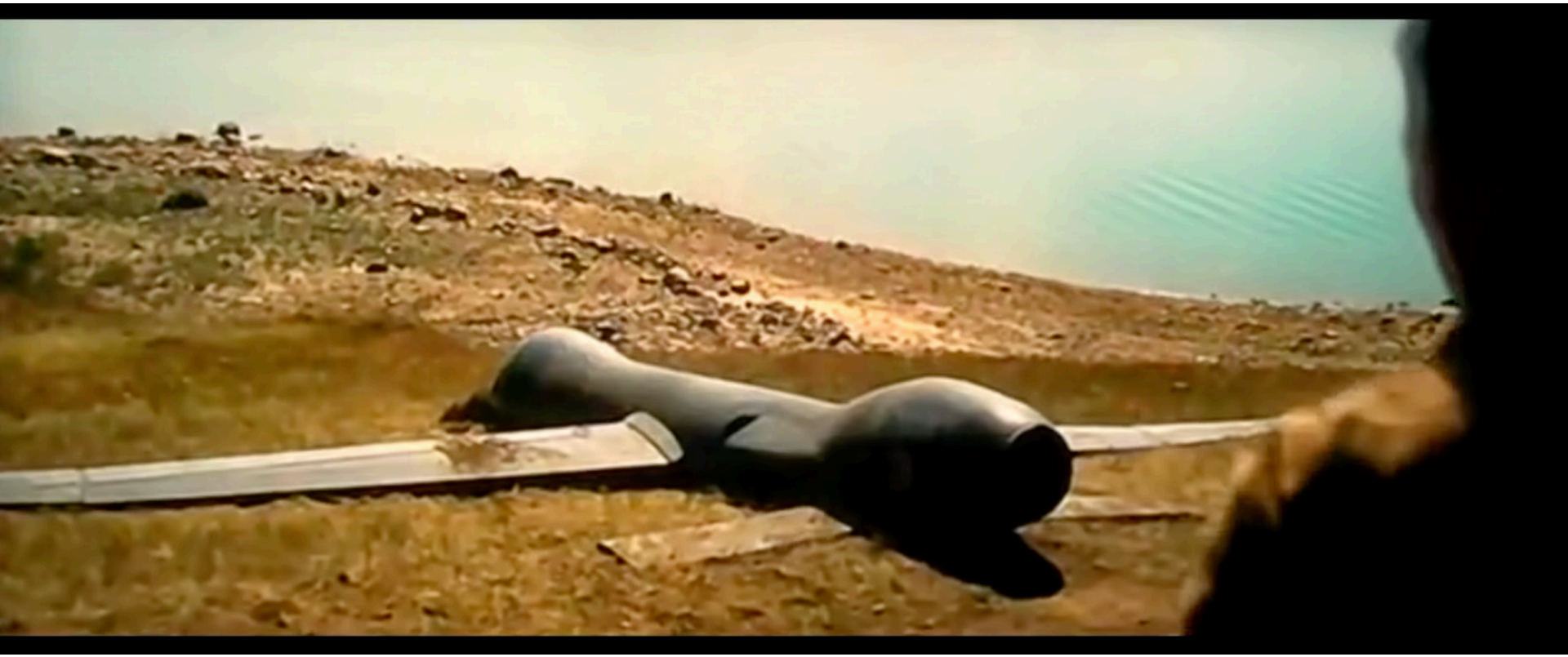
YANG Qing

- 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.
- Presenter of DEFCON 23

HUANG Lin – SDR expert

- One of the early USRP users in China. Authored some tutorials about GNU Radio which were popular in China
- 9-year research experience in telecom operator. Join Qihoo 360 as a wireless security researcher in 2014.
- Presenter of DEFCON 23

Beginning of the story … ‘Interstellar’

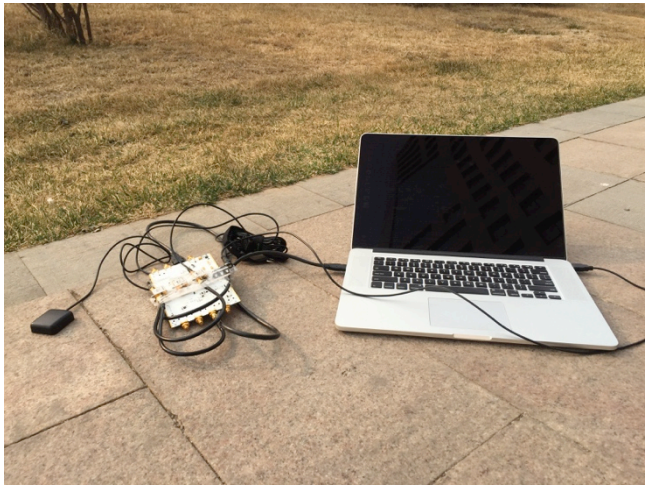


Civilian-use GPS C/A Signal

GPS 1575.42MHz C/A signal is for civilian usage, and unencrypted.

Replay attack is a typical GPS spoofing method.

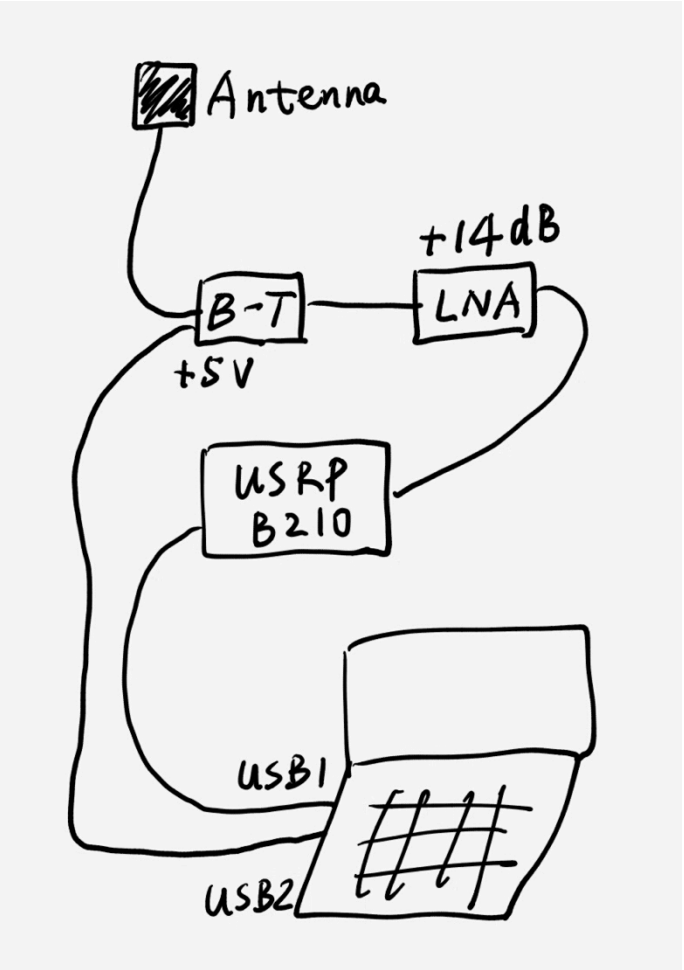
Record



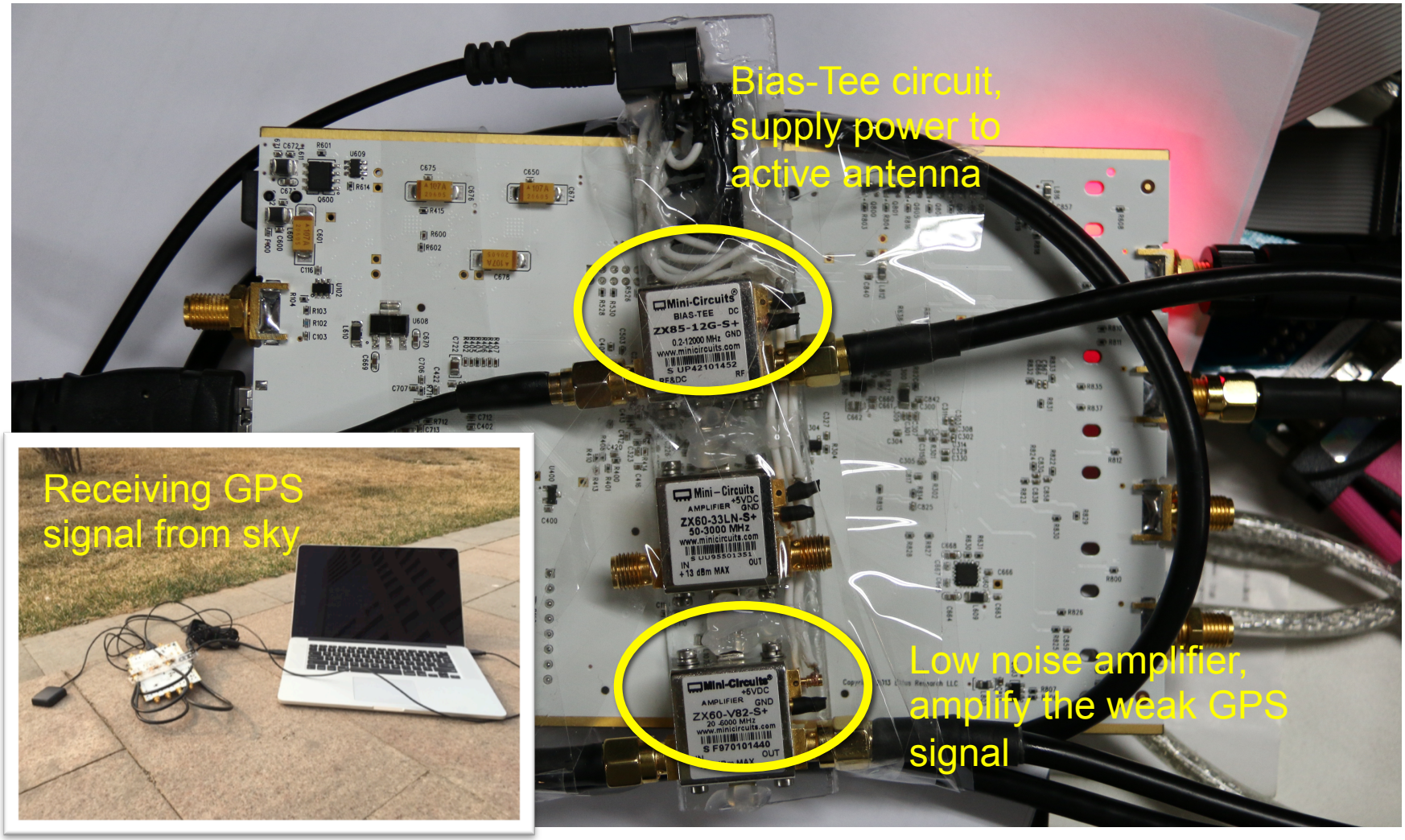
Replay

Firstly try replay attack

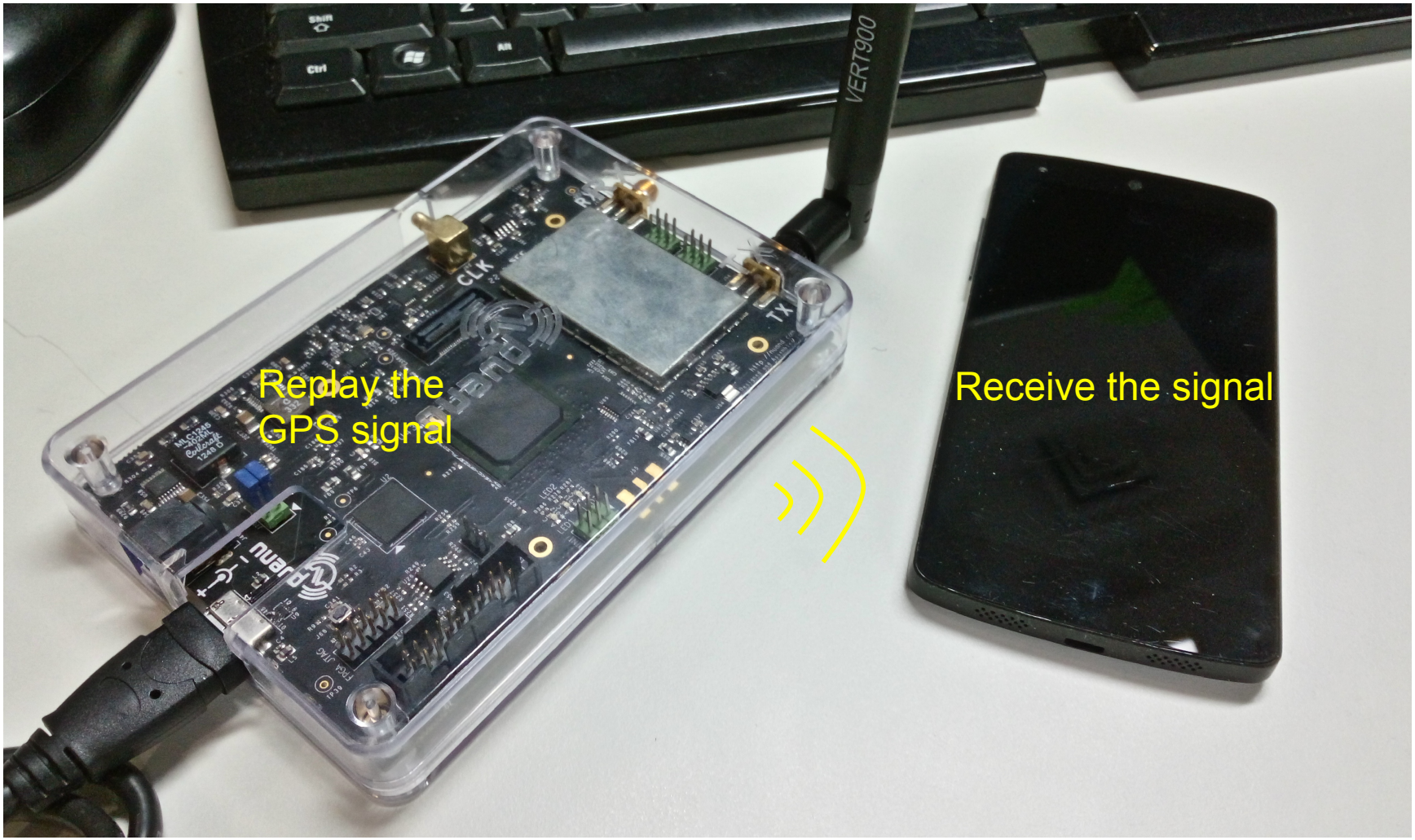
- Hardware
  - USRP B210
  - Active GPS antenna
  - Bias-tee circuit (Mini-Circuit ZX85-12G-S+)
  - LNA (Mini-Circuit ZX60-V82-S+)



Record GPS signal by a USRP B210



Replay the signal by a bladeRF

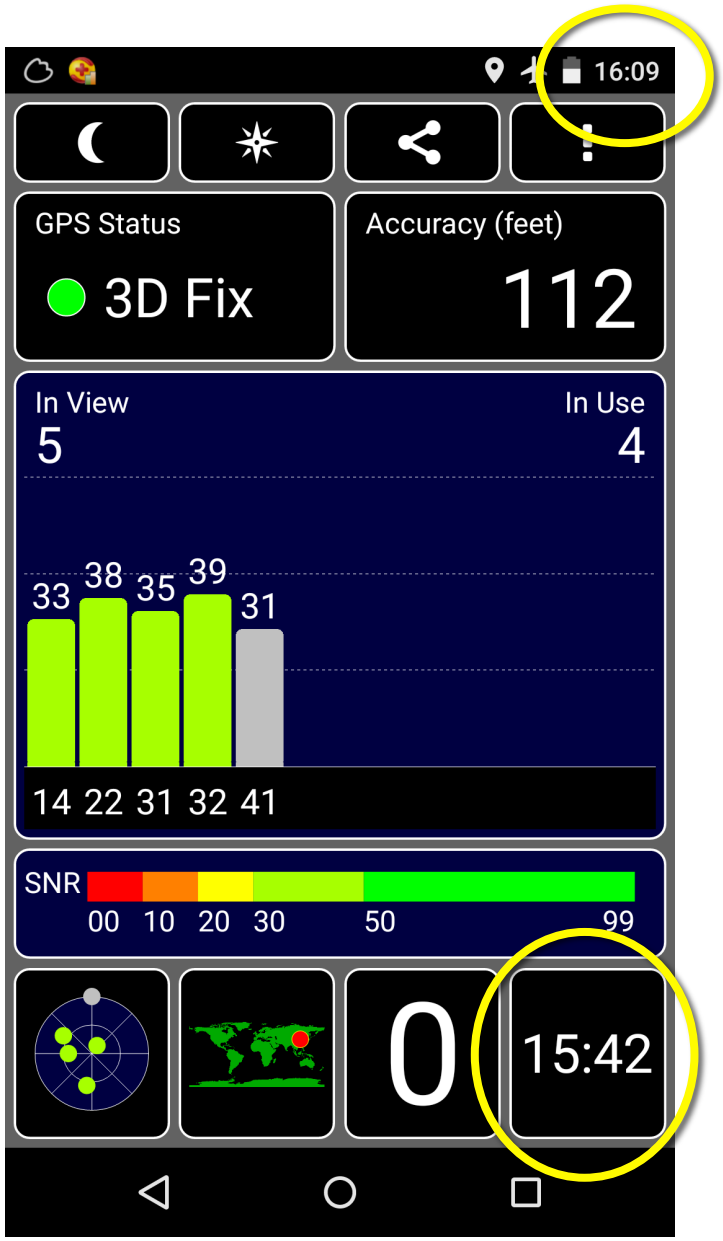


Replay Success!

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

Nexus 5

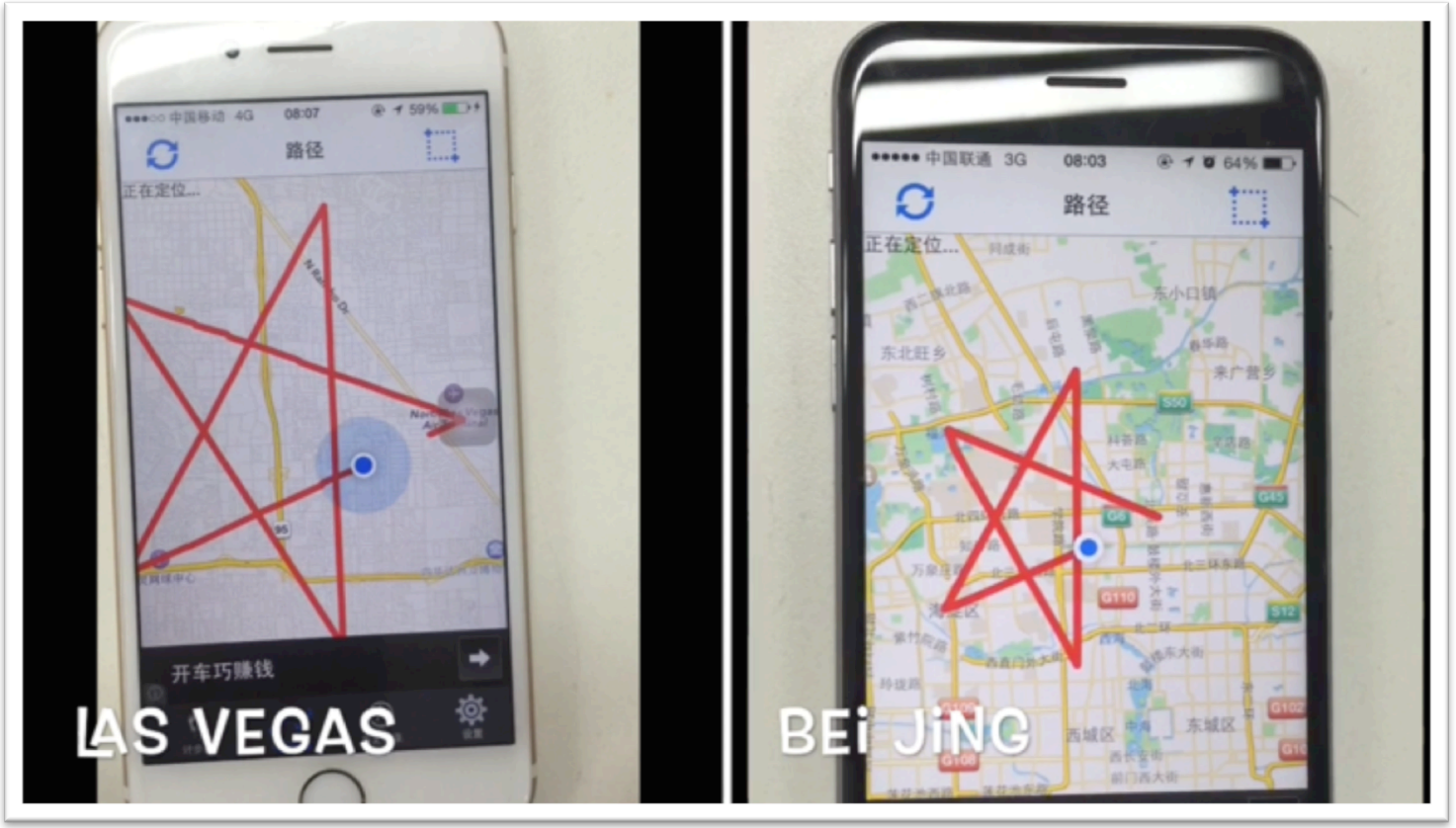
GPS Test Plus



If Create any GPS signal
rather than Record & Replay…

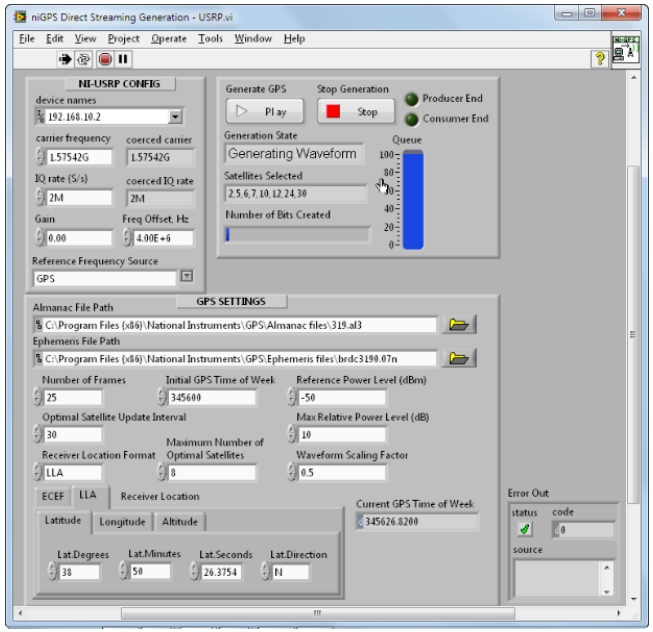
This is not a replay

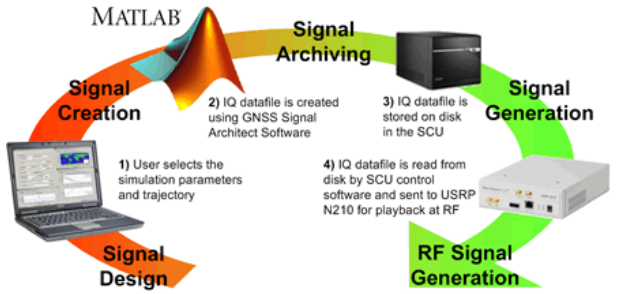
- Demo video



Search existing solutions on Internet

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





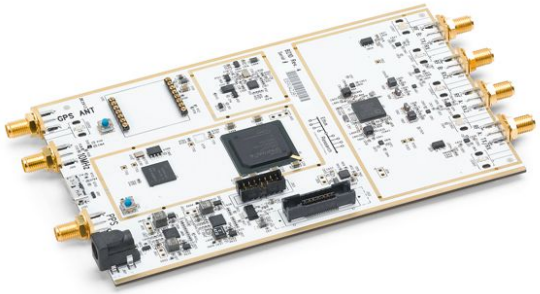
Some famous cases of GPS spoofing

- 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

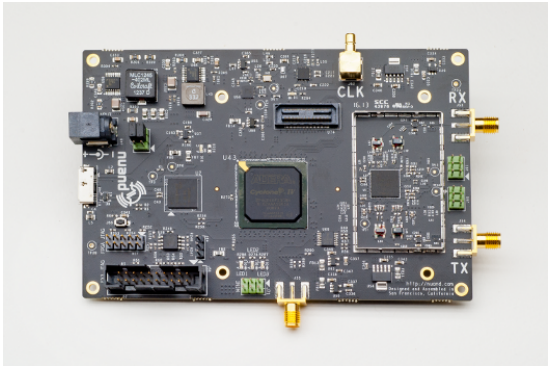
We are not navigation experts.
How can we do GPS spoofing?

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

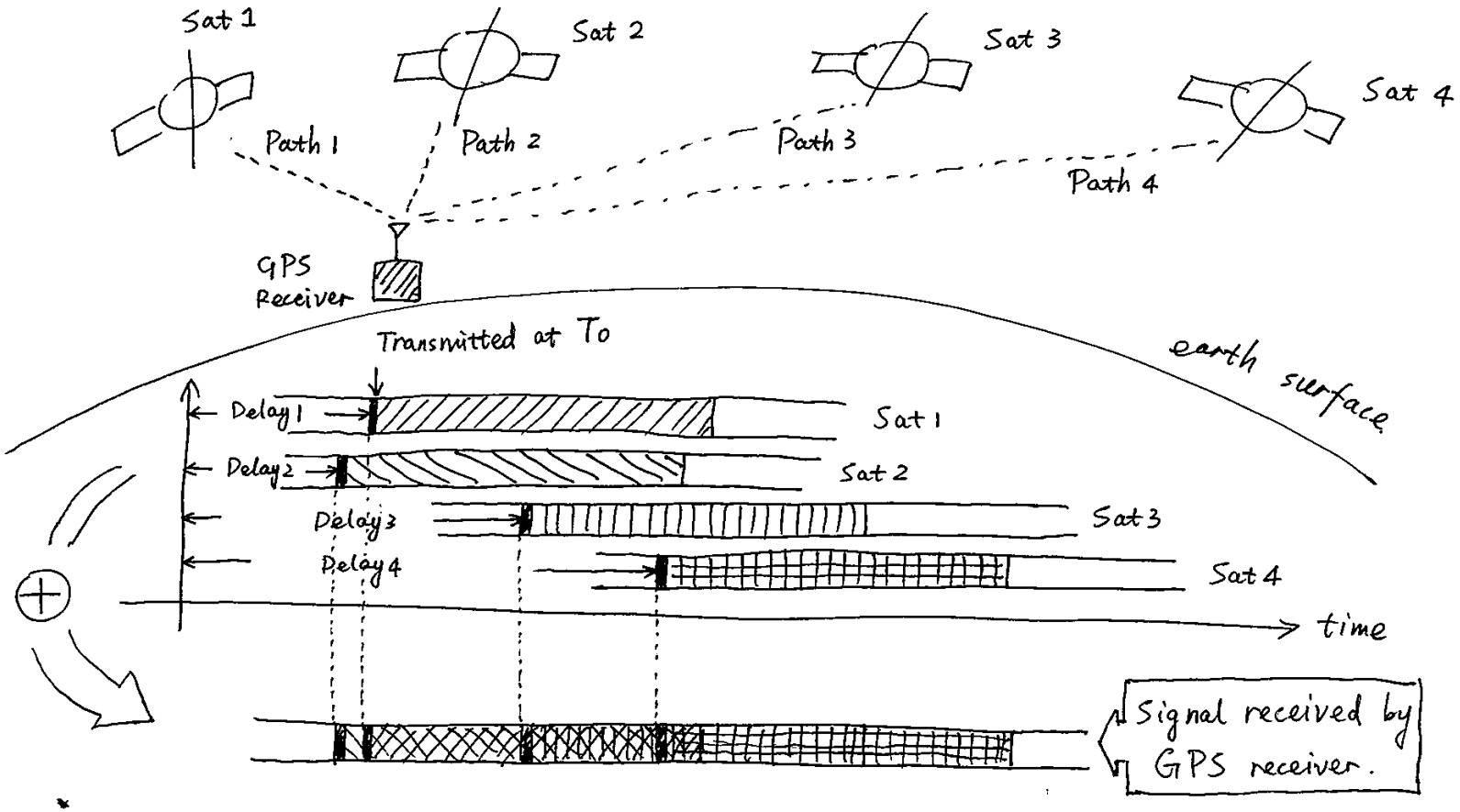
- This is a very good GPS receiver software based on GNU Radio
- http://gnss-sdr.org/

- Most of projects are GPS receivers and few are transmitters.

DIY a GPS Emulator!

Basic principle of GPS system

GPS principle



Mathematics time

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

$$\Downarrow \qquad\qquad \Downarrow$$

$$(T_1 - T_0)\cdot C \qquad \text{Position(Sat 1)} - \text{Position(RX)}$$

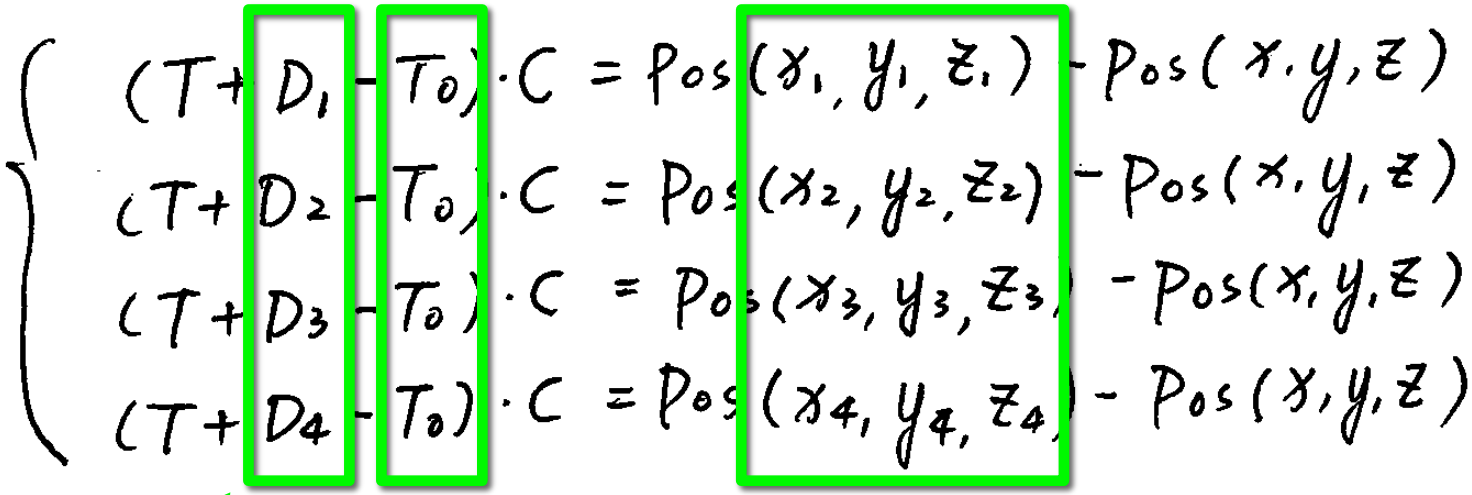
$$\Downarrow \qquad\qquad \Downarrow$$

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

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



Calculate the delays at receiver

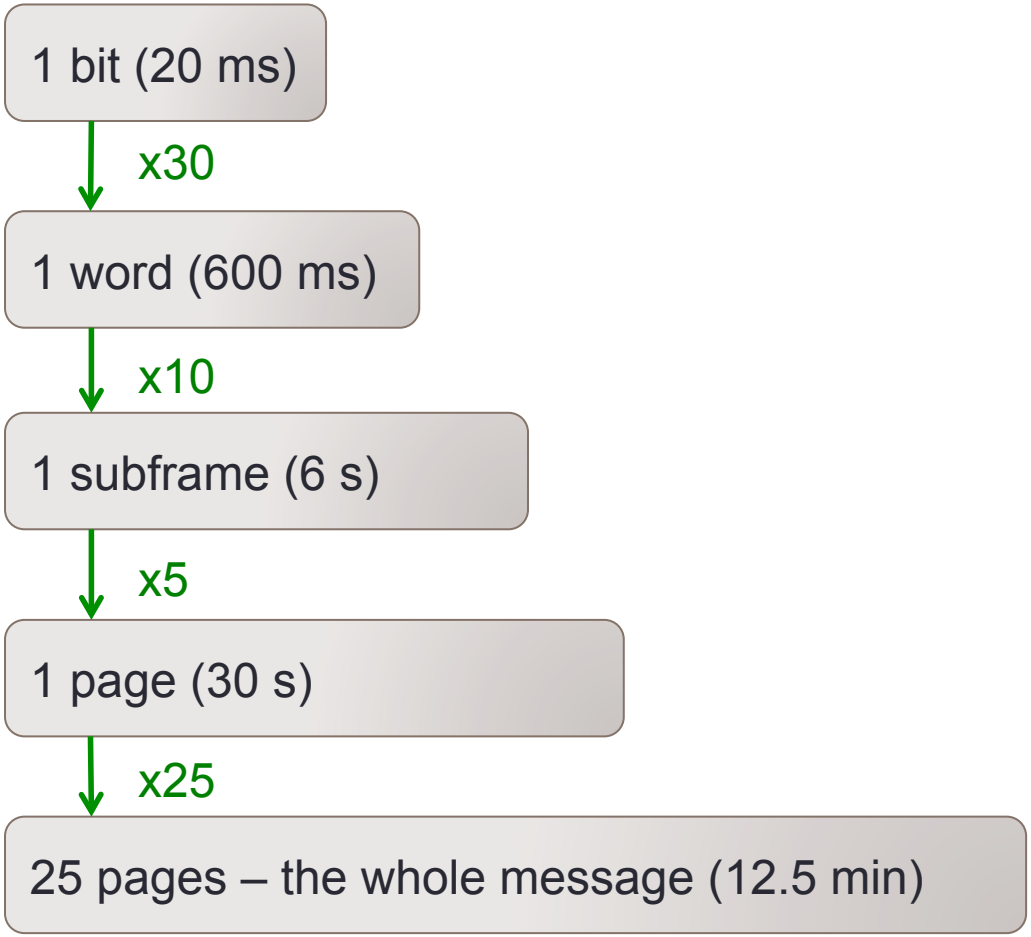
Position spoofing: give fake delays

WHEN

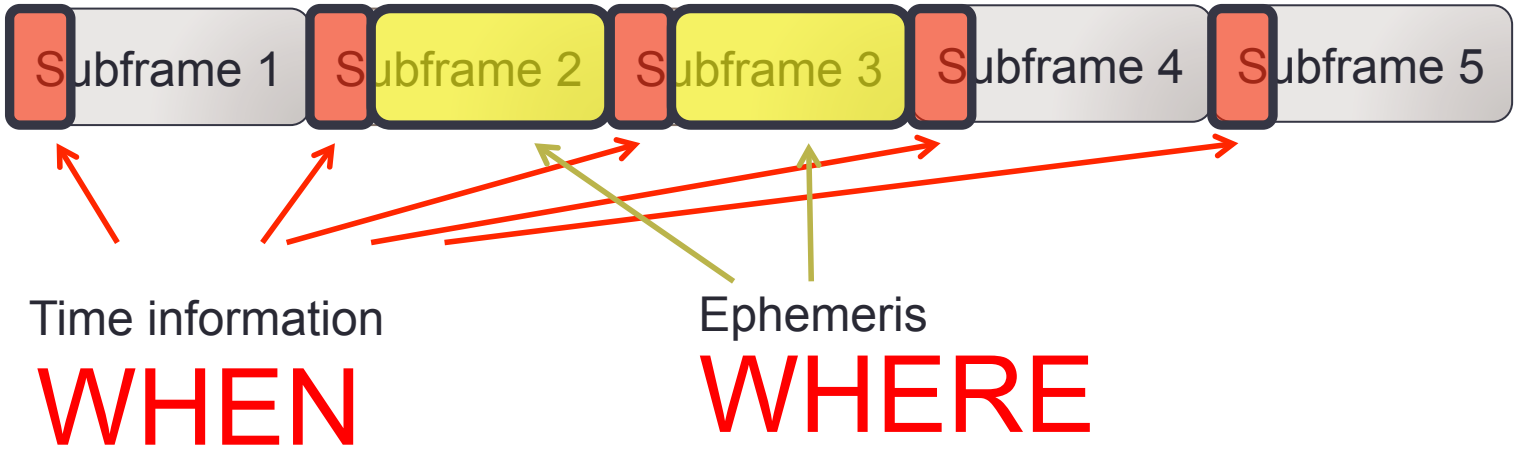
Time spoofing: give wrong time info

WHERE

Structure of message



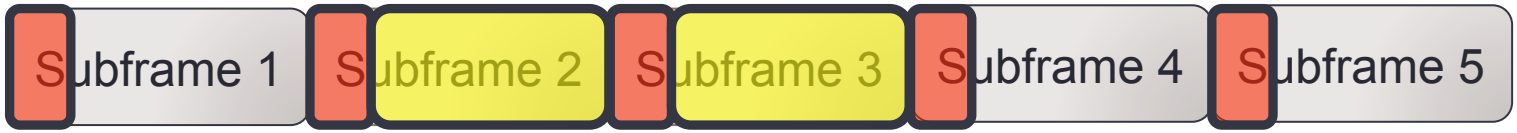
Info of WHEN & WHERE



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.



Ephemeris data

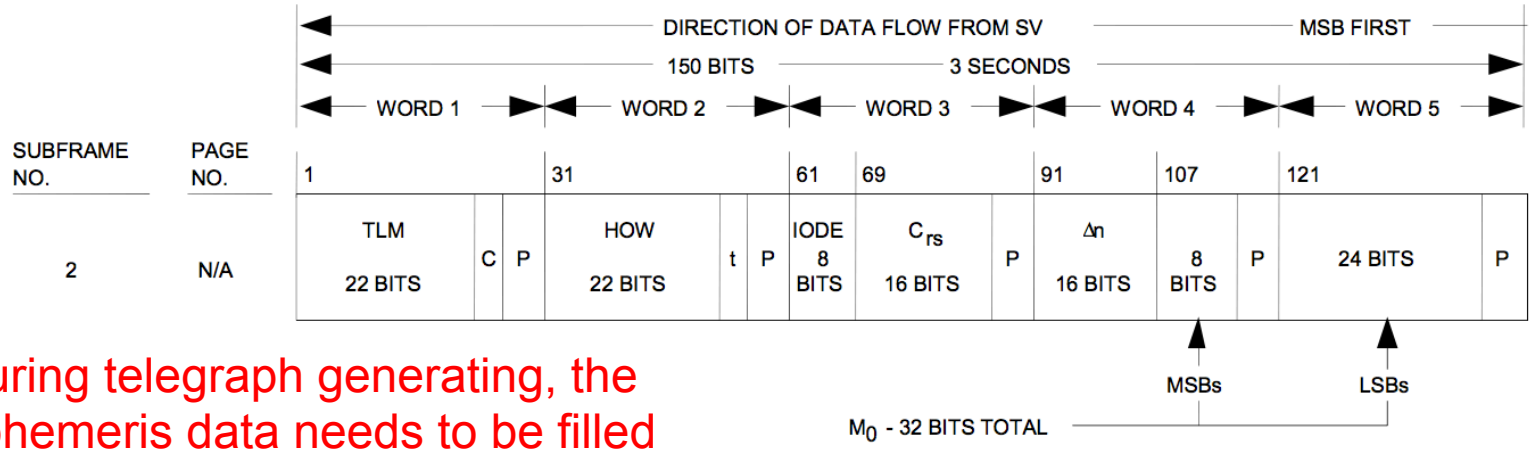
Matlab code of GPS simulator

main.m

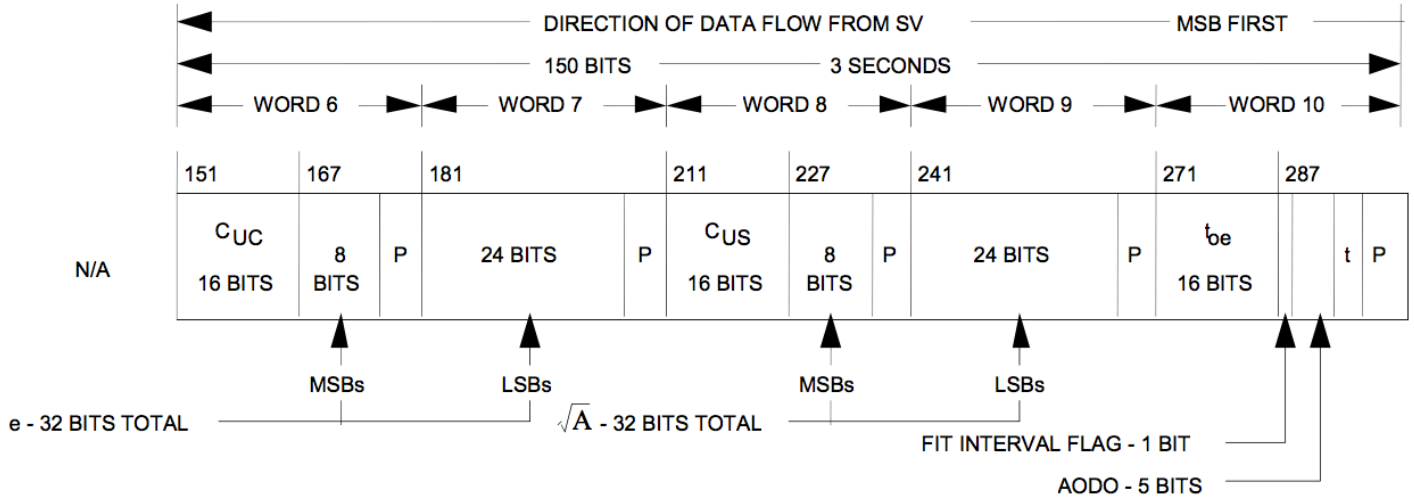
```
clear global;
clc;
global SimGlobal;
global CI;
disp('-----------------');
init;
disp('-----------------');

% % set datafile name
datafilename = 'test.dat';
ephameris_file = 'brdc0450.15n';

[SimGlobal.noeph,SimGlobal.aEphData]=readrinex(ephameris_file);% read ephemeris data
SimGlobal.aSatData=selecteph;% select ephemeris data
satvisible;% decide which satellite is visible
genmessage_wo_almanac;% generate telegraph
%genmessage;
channel_data = genchannel;
gensignal(channel_data,datafilename);
```

1. Read ephemeris data
2. Decide which satellite is visible
3. Generate the telegraph

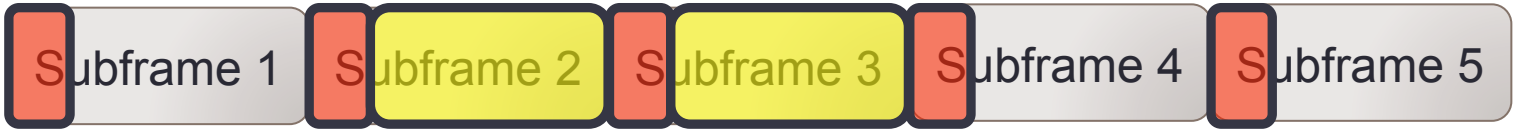
Example: structure of Subframe 2



During telegraph generating, the ephemeris data needs to be filled according to the frame structure



Almanac data in Subframe 4 & 5



Time information

Ephemeris

Almanac

Almanac data is not necessary for most GPS receiver. Only several key fields must be filled. And you may use ephemeris data to fill the almanac field.

Generate navigation message

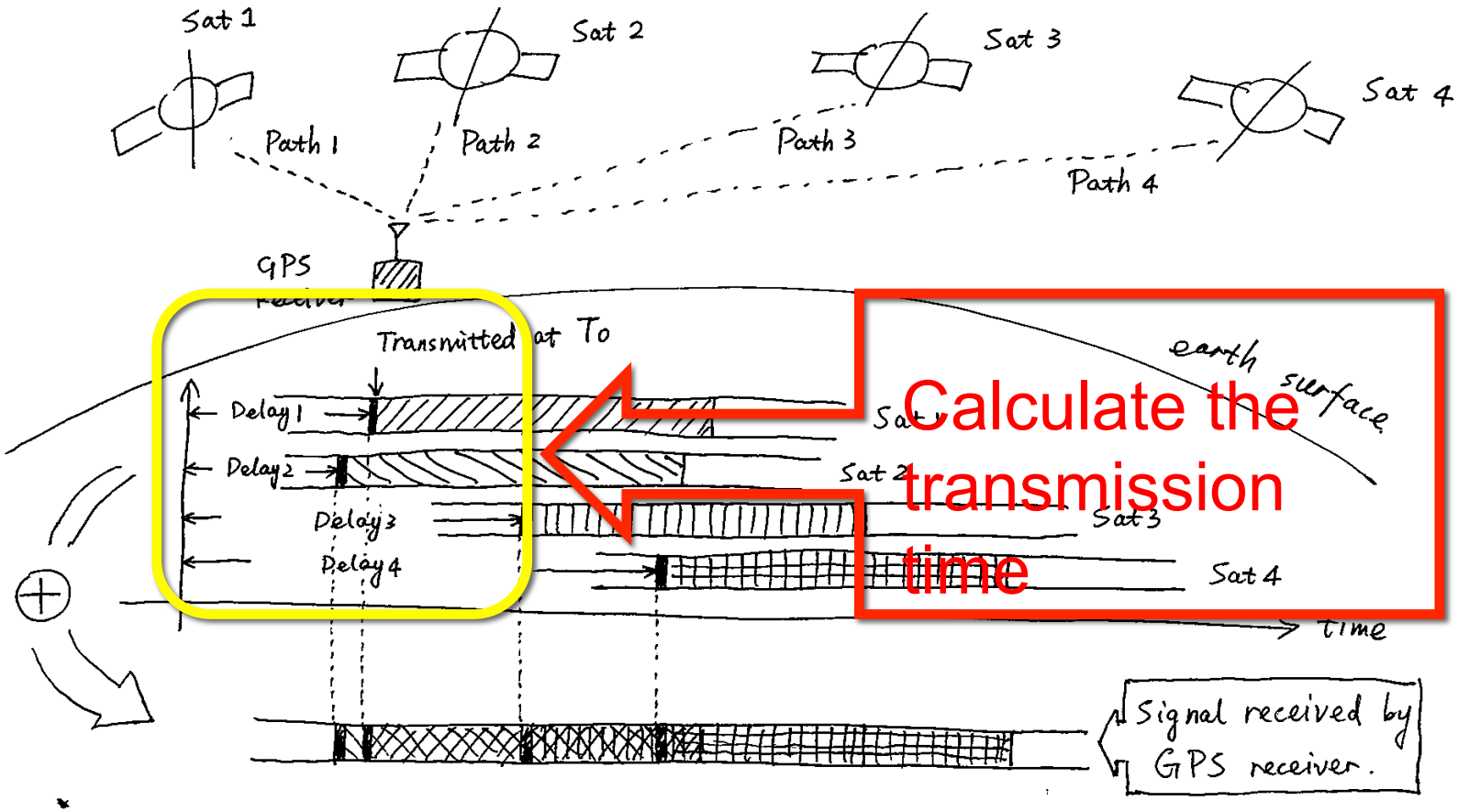
```
23 –      pA=SimGlobal.aSatData(i).sOrbitData.sAlmData;
24 –      if(p0.visflag==1)
25 –          visual_counter = visual_counter+1;
26 –          disp(['Satalite ' num2str(i) ' telegraph for ' num2str(visual_counter) 'th channel generating...']);
27 –          for idx_page = 1:25
28 –              for idx_subfrm = 1:5
29 –                  switch idx_subfrm
30 –                      case 1 % subframe 1...
84 –                      case 2 % subframe 2...
141 –                     case 3 % subframe 3...
195 –                     case 4 % subframe 4...
510 –                     case 5 % subframe 5...
618
619 –                 end % end of switch idx_subfrm
620 –             end % end of loop idx_subfrm
621 –         end % end of loop idx_page
622 –     end % end of visible
623 – end % end of loop satelite
```

Generating the telegraph, from Subframe 1 to 5.

360UNICORNTEAM

Bits ➔ Waveform

GPS principle again

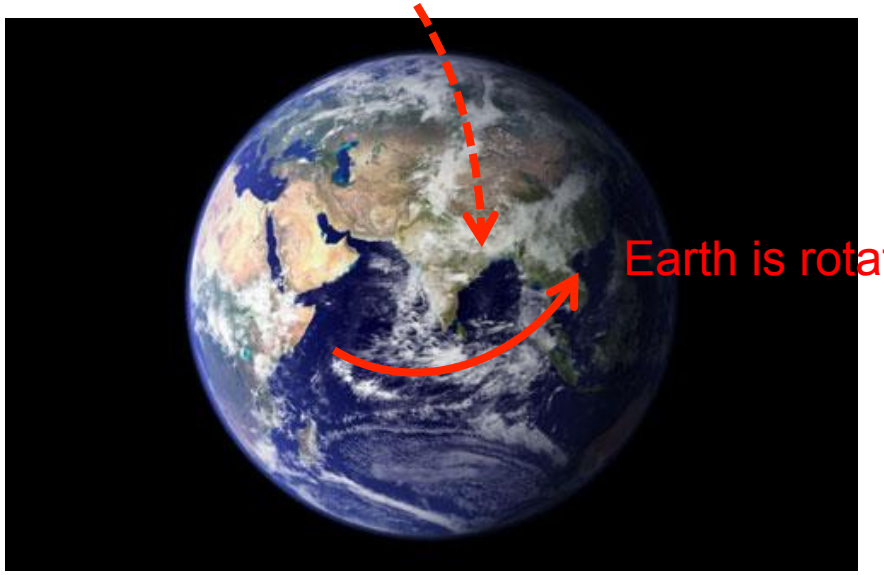


How to calculate transmission time

Satellite is moving

Calculate the length of signal path

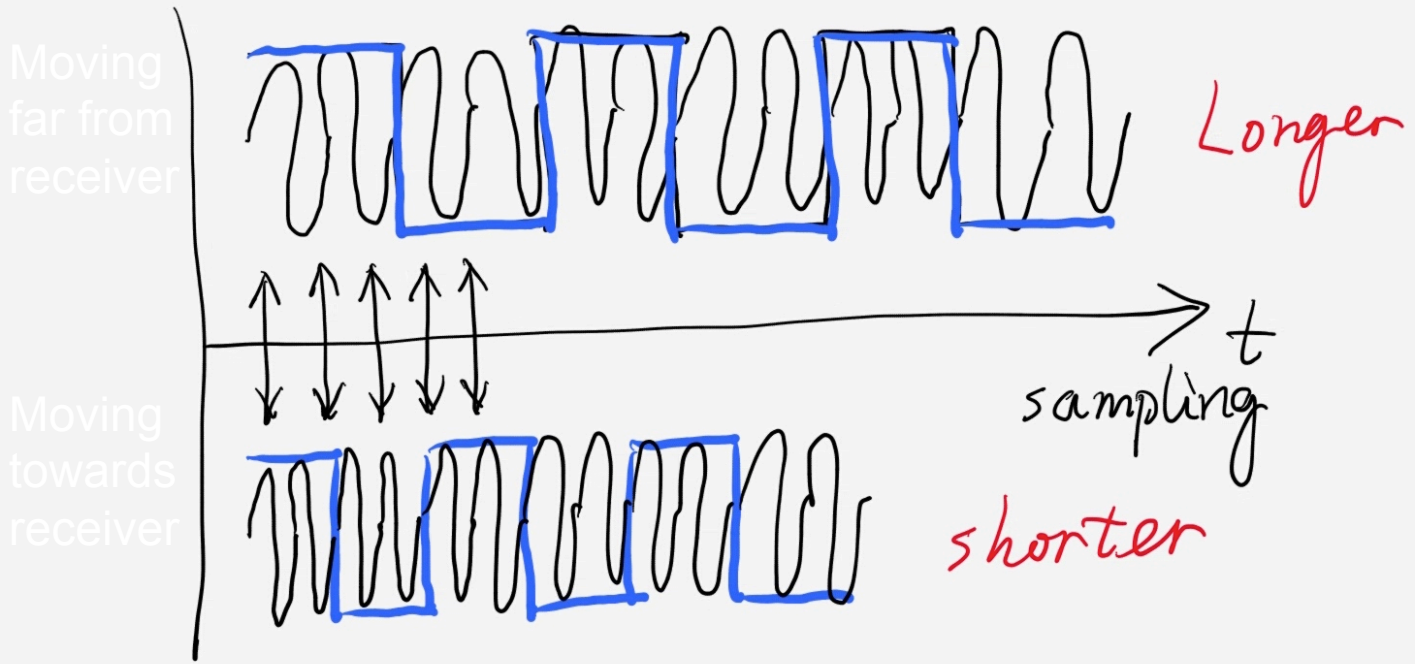
Calculate the coordinate according to ephemeris data



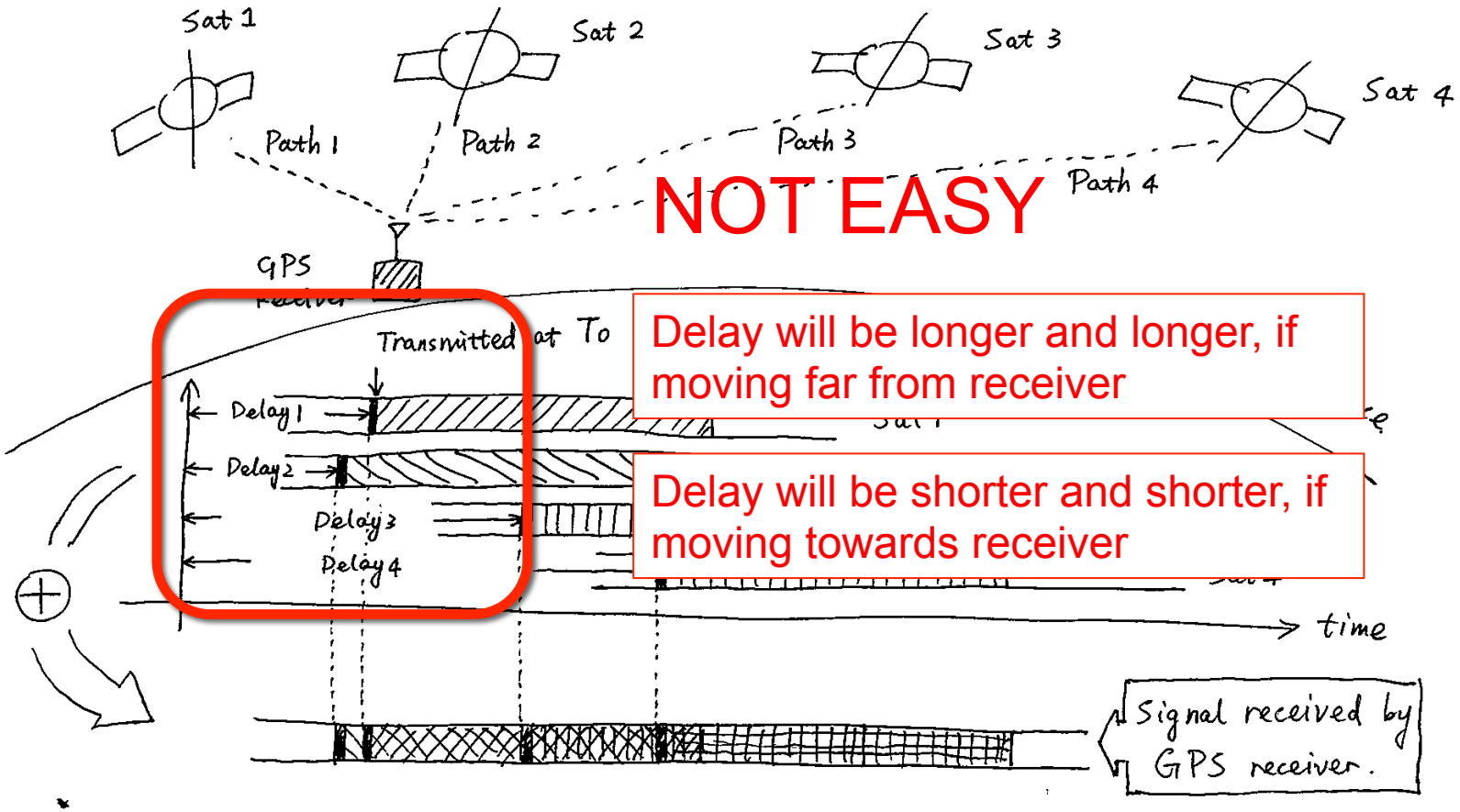
Earth is rotating

NOT EASY

Another challenge: Doppler effect



GPS principle again



Matlab code of generating waveform

main.m

```
clear global;
clc;
global SimGlobal;
global CI;
disp('------------------');
init;
disp('------------------');

% % set datafile name
datafilename = 'test.dat';
ephameris_file = 'brdc0450.15n';

[SimGlobal.noeph,SimGlobal.aEphData]=readrinex(ephameris_file);% read ephemeris data
SimGlobal.aSatData=selecteph;% select ephemeris data
satvisible;% decide which satellite is visible
genmessage_wo_almanac;% generate telegraph
%genmessage;
channel_data = genchannel;
gensignal(channel_data,datafilename);
```

Convert bits to waveform in this function

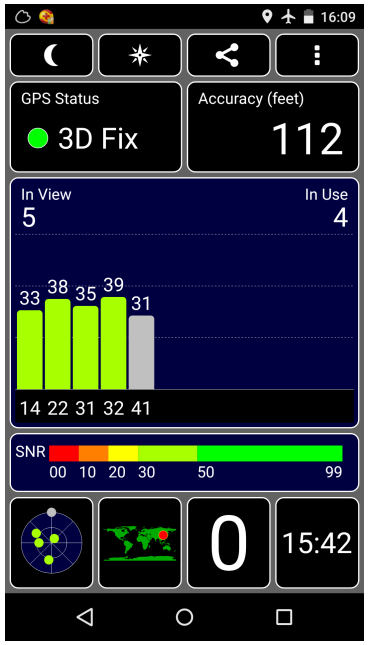
GPS emulator is done

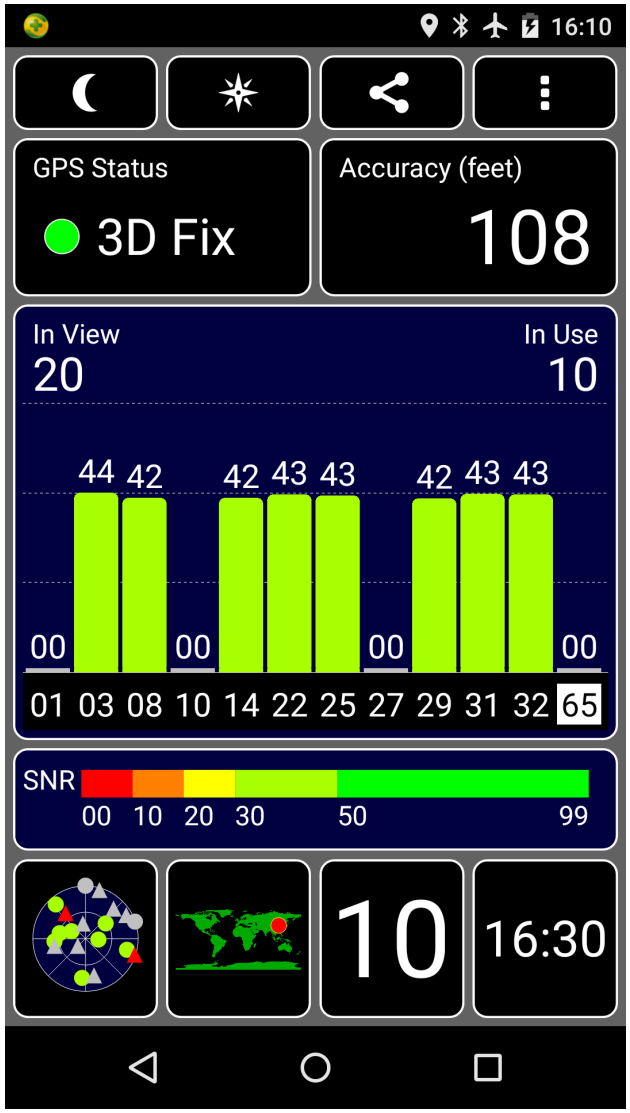
Test spoofing

Try to spoof cellphone's GPS …

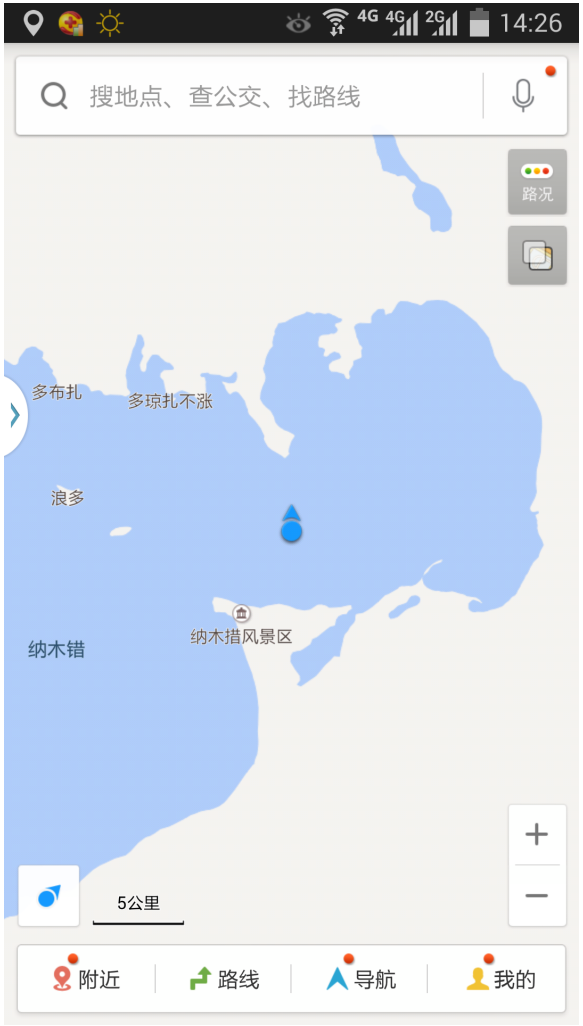
Bingo! Nexus 5

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

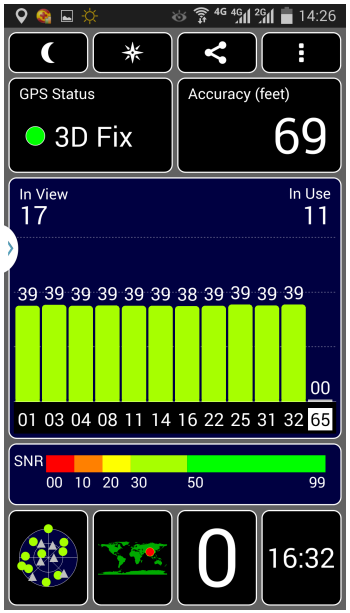


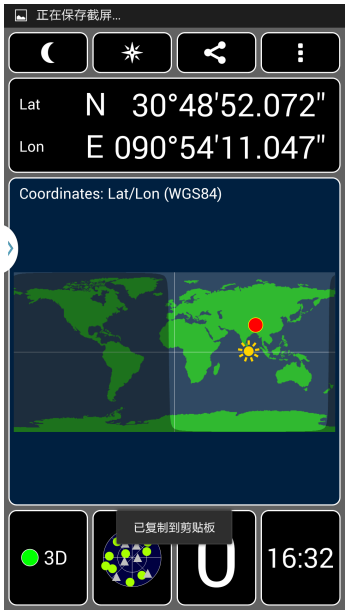


Bingo! Samsung Note 3

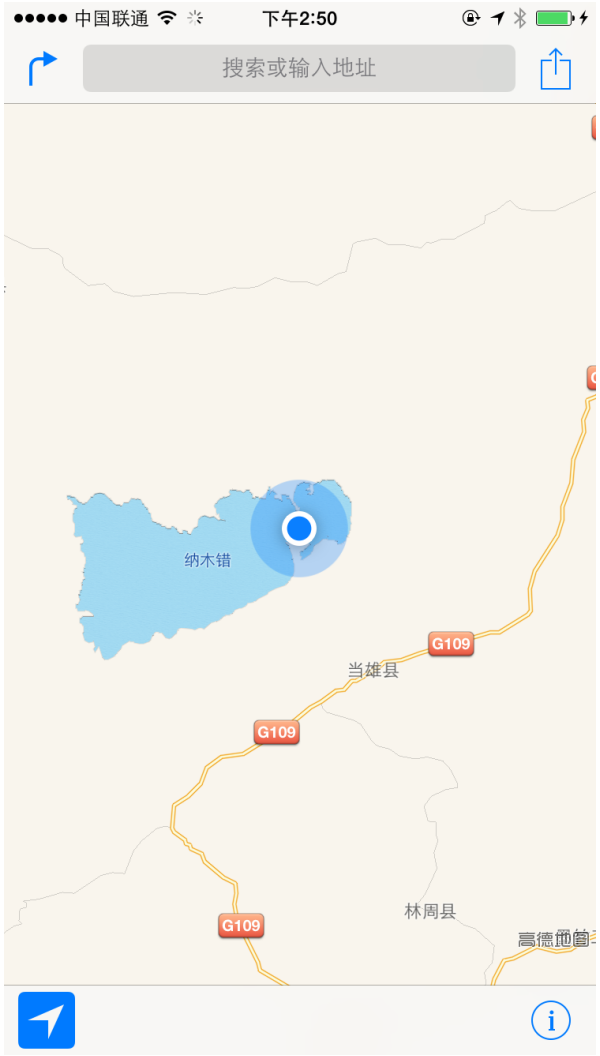


- Located at Namco Lake in Tibet but the cellphone is actually in Beijing.

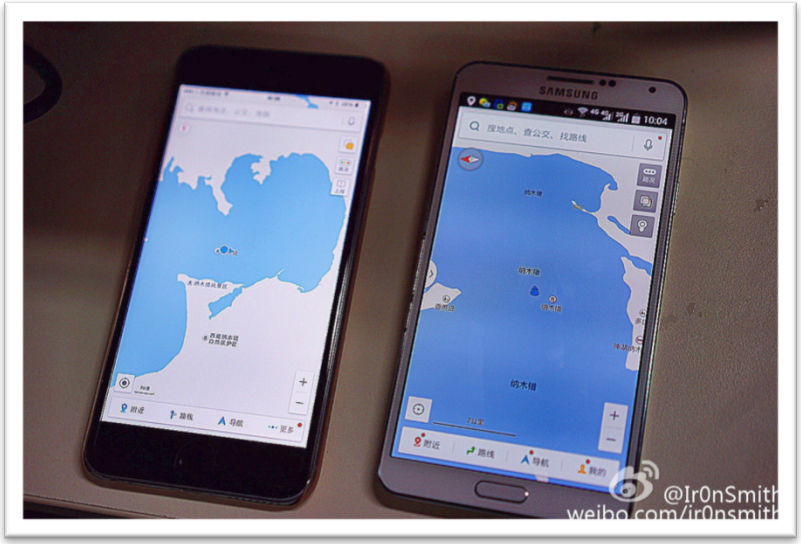




Bingo! iPhone 6



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



Time spoofing

- You may find the date we set is always Feb. 14 2015. This is because the ephemeris data file we use is gotten at that day.
- Actually not only space, but also time, can be spoofed.
- Use the same orbit data from the same ephemeris file, but only change the time parameters.

Time spoofing - A cellphone in future time

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

Spoofing cars

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

Spoofing drones - Forbidden area policy

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

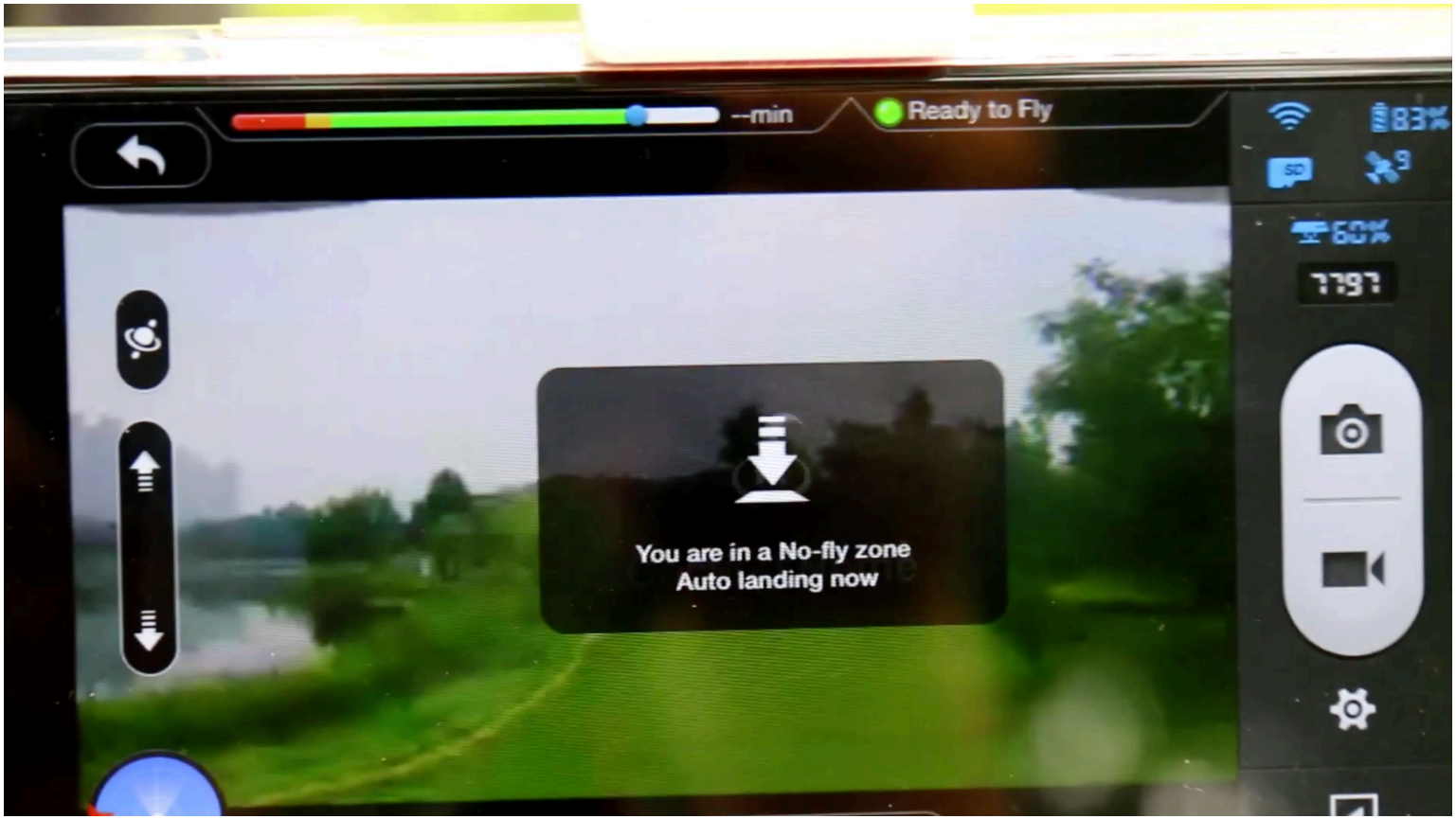
360UNICORNTEAM

Spoofing drones - Bypass drones' no-fly zone

- Demo: 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.

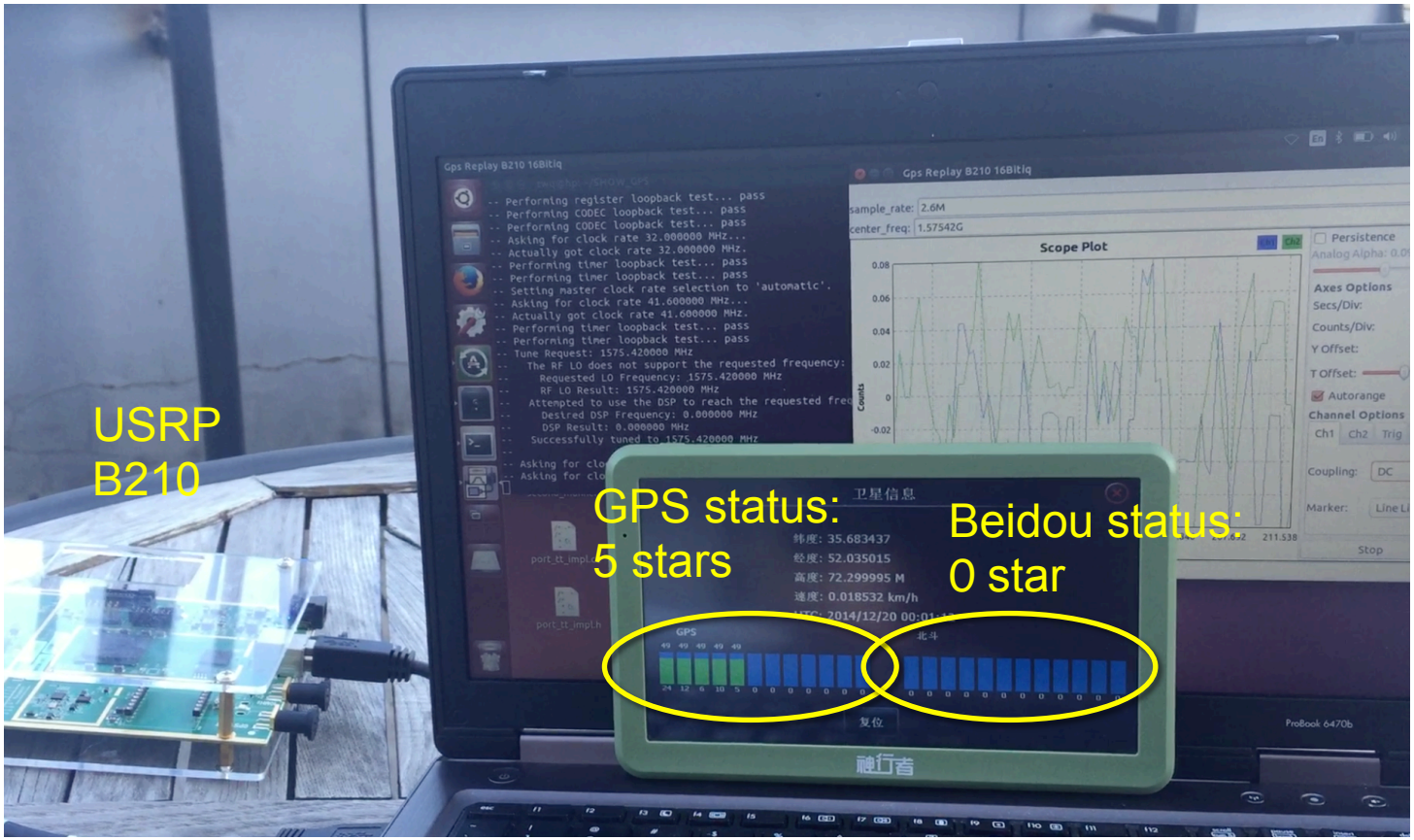
Spoofing drones – Hijack flying drone

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



Spoofing dual-mode positioning

This car navigation module has GPS and Beidou dual-mode positioning, but it was spoofed either.
Beidou uses the neighbor band very closed to GPS band, so it is interfered by the strong fake GPS signal then it cannot fix the positioning.



Summary – the risks

- Very simple and low-cost
  - Open source software
  - SDR hardware

- Influence
  - Portable devices: Cellphone, path tracer
  - Conveyance: car, yacht, even plane
  - Timing system: in cellular base station, financial trading system

How to anti-spoof

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

Thank you!