数据驱动安全

2015 中国互联网安全大会
China Internet Security Conference

全球GPS定位系统新威胁分析

黄琳，杨卿

UNICORNTEAM，奇虎360

Unicorn Team

- UnicornTeam是一群安全研究员组成的团队，主要关注无线安全和硬件安全。无线安全包括，例如RFID, NFC，还有GPS, UAV, 智能汽车相关的无线系统，还有蜂窝网络和卫星通信等等.
- 我们主要的职责是保护360公司和360产品的无线和硬件安全。我们不但研究防守方法，也研究攻击方法。
- 我们有自己的硬件研发团队，可以设计和制造我们攻防研究中的各种小工具。

杨卿

- 杨卿是UnicornTeam的负责人
- 他在无线和硬件攻防方面有比较丰富的经验。熟悉Wifi渗透，IC卡破解，对汽车安全和软件无线电也都很感兴趣。.
- 他是首个北京地铁Wifi系统的漏洞发现者，也是公交一卡通的首个漏洞发现者。

黄琳

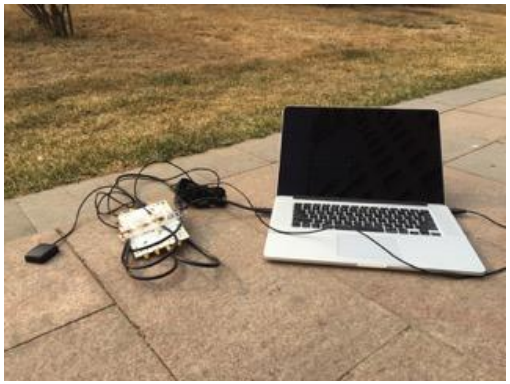
- 国内最早的USRP用户，从2005年开始使用USRP作为研究工具。
- 2009年编写了一本《GNU Radio入门 0.99》在国内GNU Radio用户中影响很大
- 2010至2013年，积极推动了Cloud-RAN技术在国内的发展
- 2014年，加入奇虎360，成为一名无线安全研究员

伊朗捕获美国无人机
GPS欺骗开始受到关注

民用的GPS信号

C/A信号是民用的GPS信号，没有加密。

因此民用信号是可以被重放攻击的。

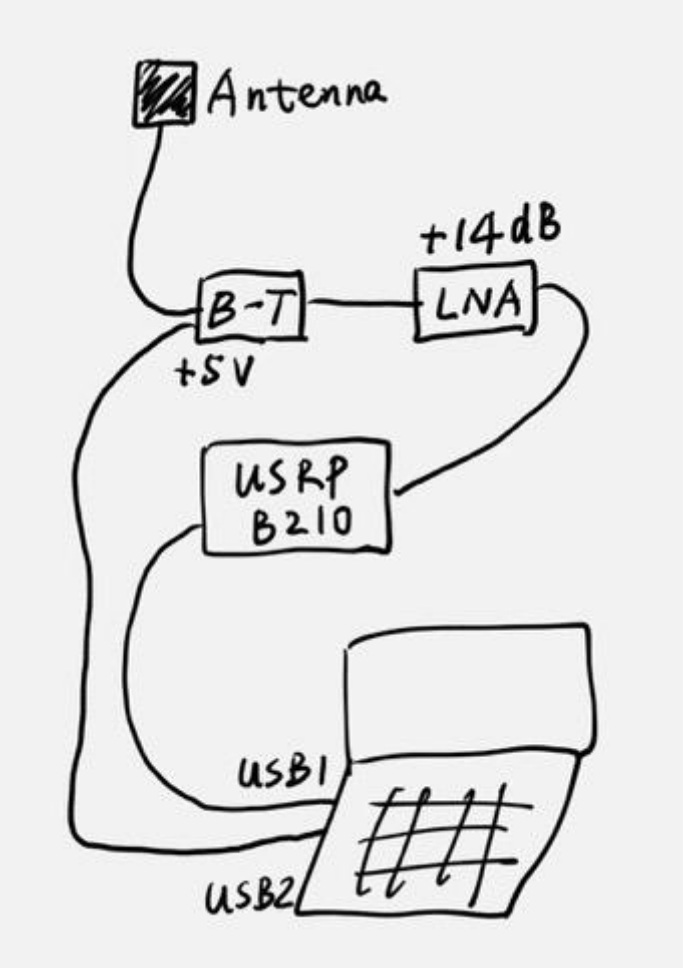


Record

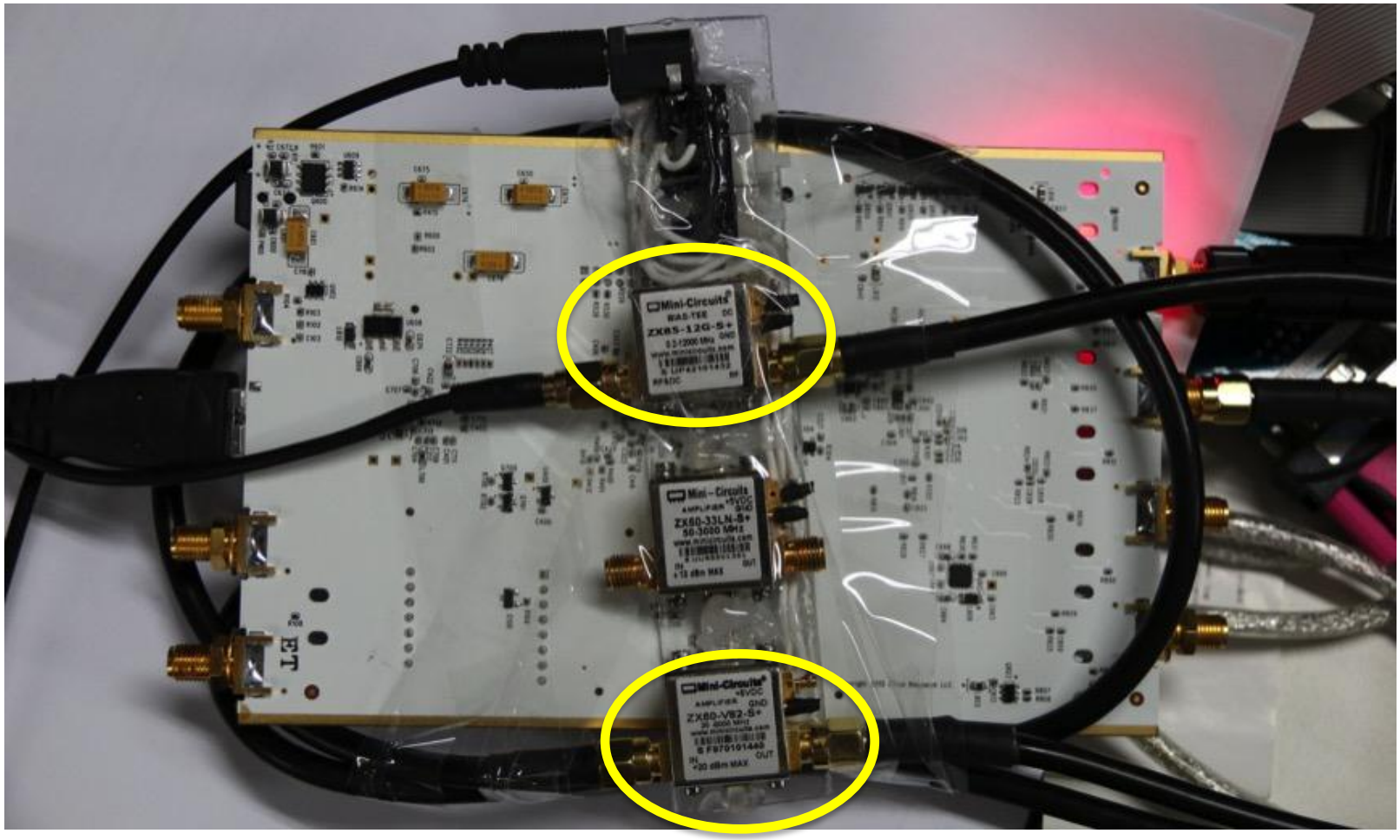
Replay

首先尝试GPS重放

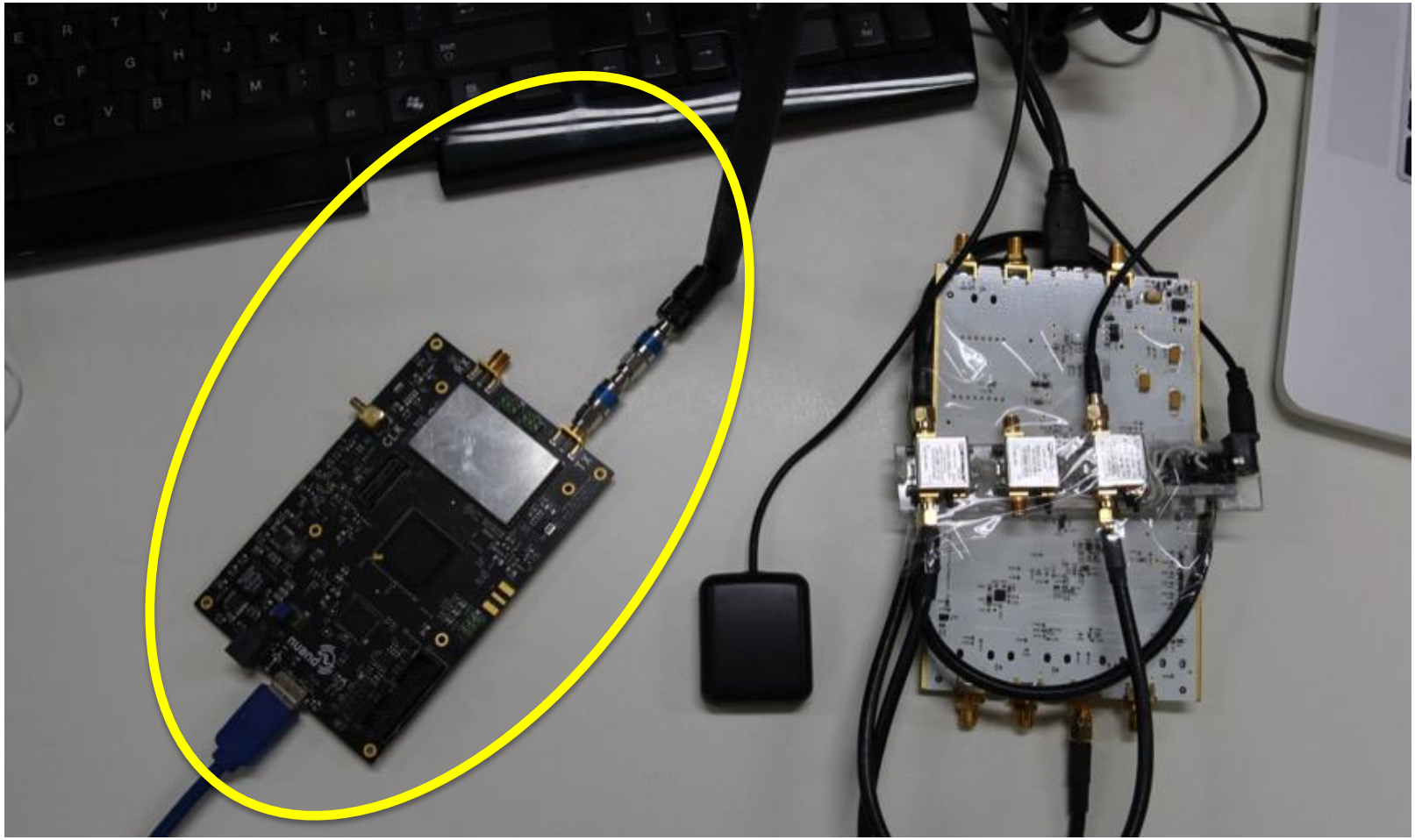
- 硬件
  - USRP B210
  - 有源GPS天线
  - 有源天线的bias-tee模块(Mini-Circuit ZX85-12G-S+)
  - 低噪声放大器(Mini-Circuit ZX60-V82-S+)



用USRP B210录制GPS信号



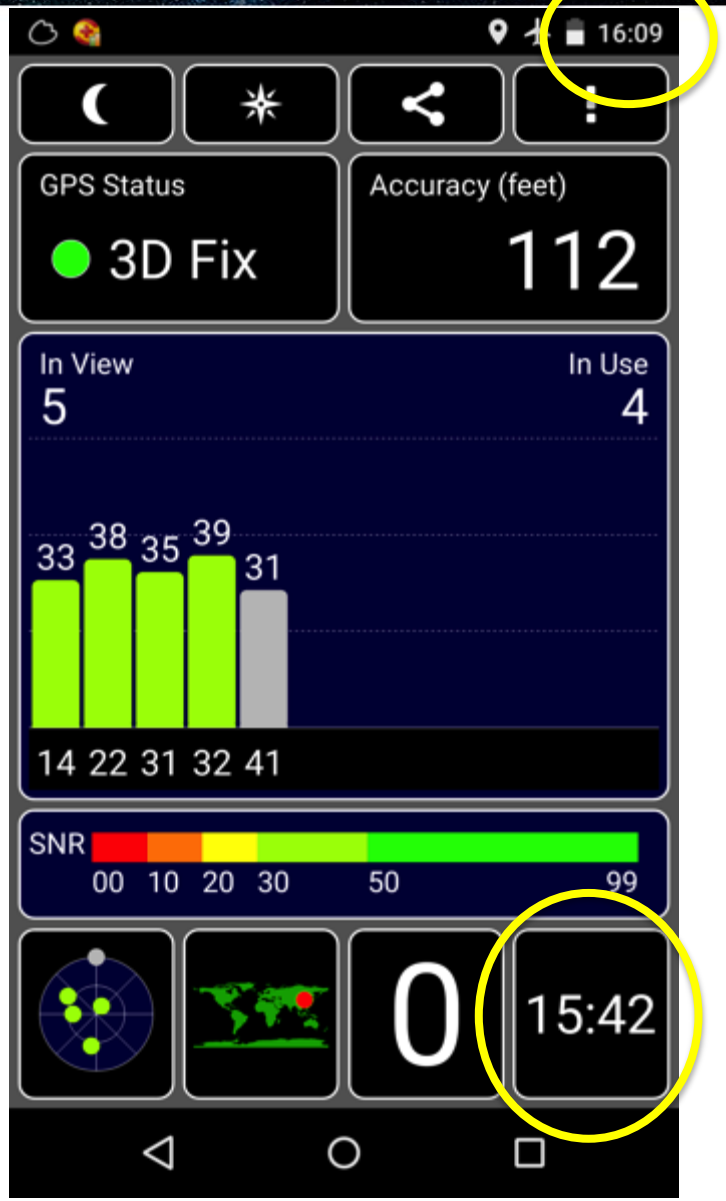
用bladeRF重放信号



成功！

重放录制的信号，你会发现手机锁定在错误的时间和位置。GPS时间和手机的系统时间，不一致了。

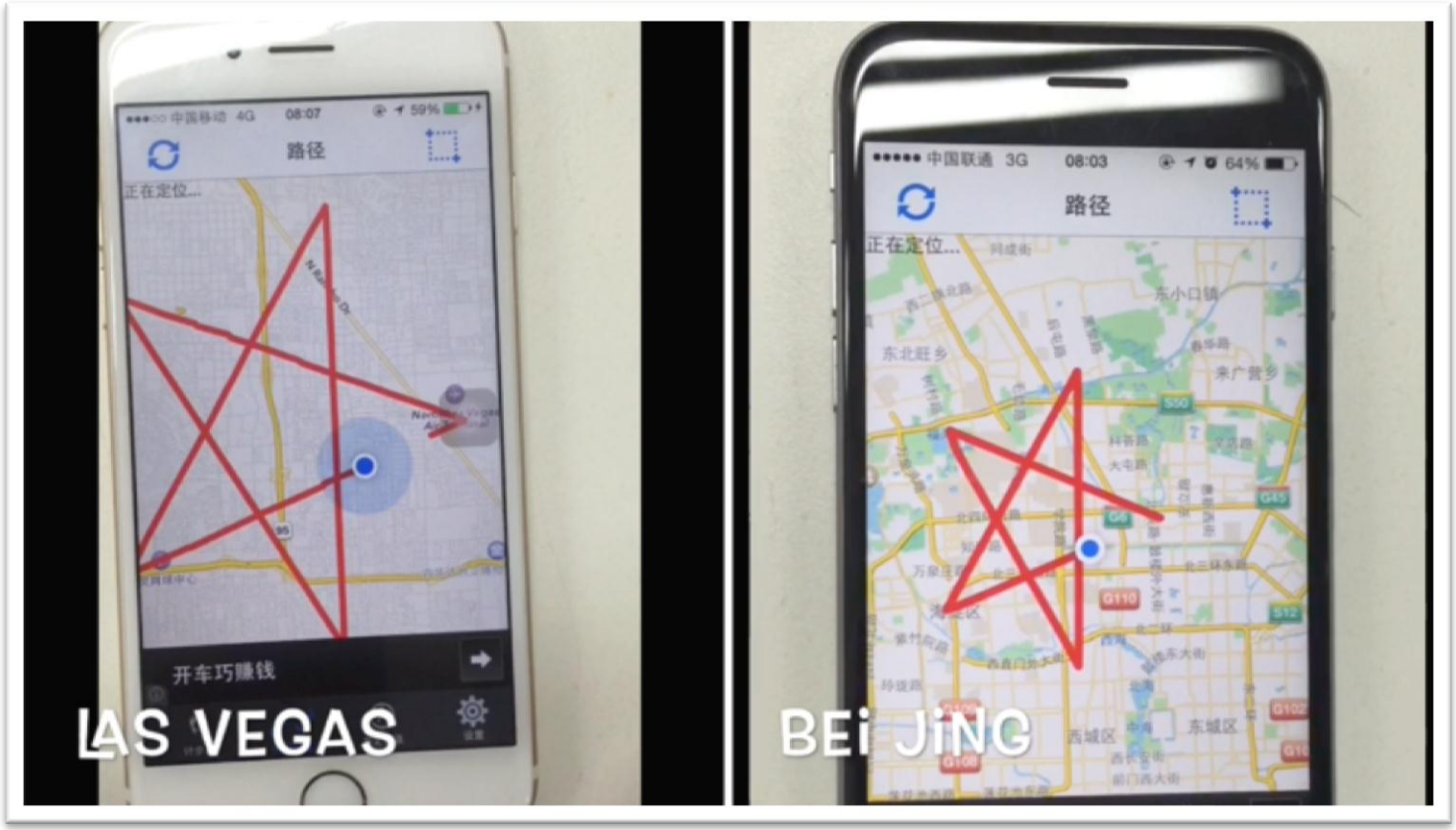
Nexus 5



重放必须要先录制信号，太麻烦！

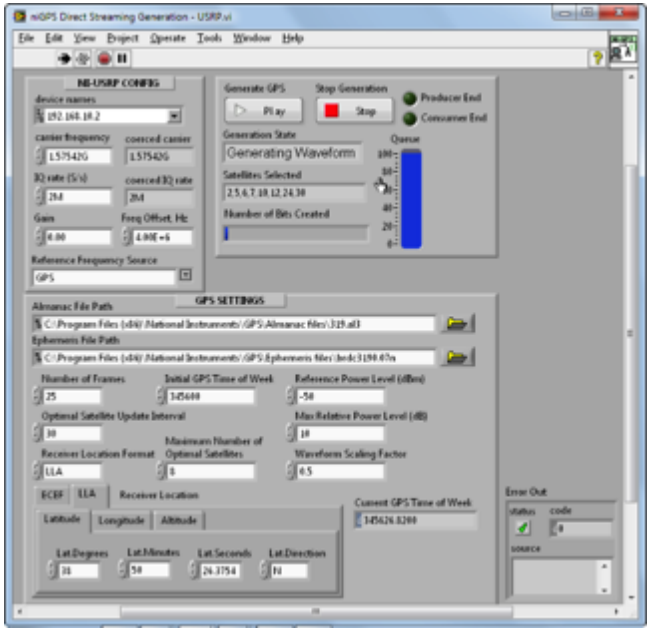
这显然不是一次重放

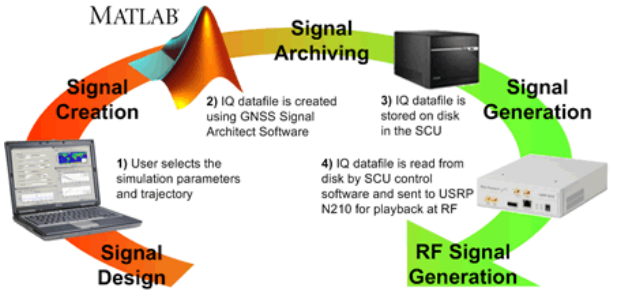
- Demo video



看看网络上有没有现成的方案

- 好像都有点贵，至少不是免费的
- NI LabVIEW ~$6000
- NAVSYS ~$5000





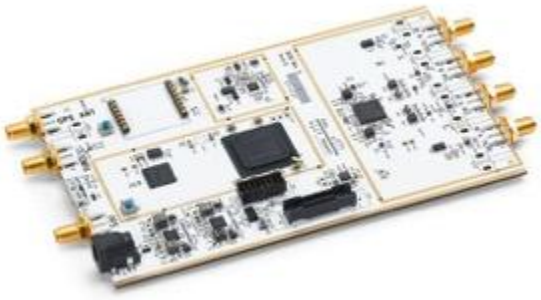
其他的GPS欺骗都是怎么做的？

- 一个牛逼的实验室：RadioNavigation Lab from Univ. of Texas at Austin (https://radionavlab.ae.utexas.edu/)
- Todd E. Humphrey 教授带领这个团队
  - 2012年TED演讲: how to fool GPS
  - 2013年欺骗了一辆昂贵的游艇
  - 2014年欺骗了一架无人机

我们可不是导航专家
GPS小白该怎么办呢？

作为SDR玩家，有这些工具

USRP



bladeRF

HackRF

网上还是能够找到一些开源代码的

- 这个网址搜集了很多GPS有关的开源项目
- http://www.ngs.noaa.gov/gps-toolbox/index.html

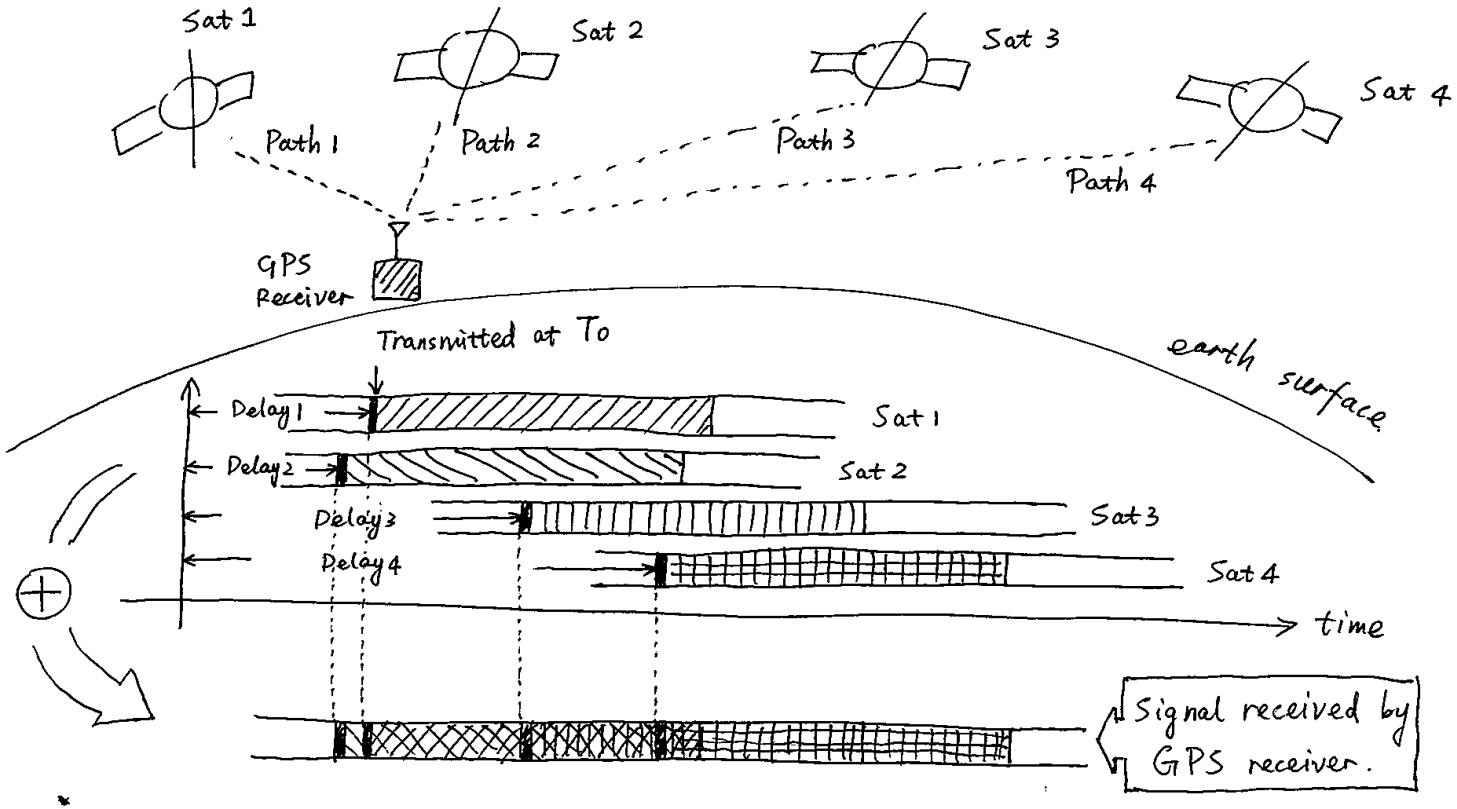
- 这是个非常好的GPS接收机程序 http://gnss-sdr.org/

- 大部分的项目都是接收机，发射机非常少. 这里是一个发射机的例子: https://code.csdn.net/sywcxx/gps-sim-hackrf
- 可惜这个程序没有写完☹

DIY一个GPS发射器吧！

从GPS基本原理讲起

GPS系统原理


Sat 1
Sat 2
Sat 3
Sat 4
Path 1
Path 2
Path 3
Path 4
GPS Receiver
Transmitted at To
earth surface
Delay 1
Delay 2
Delay 3
Delay 4
Sat 1
Sat 2
Sat 3
Sat 4
time
Signal received by GPS receiver.

数学...伪距方程 ...

$$Delay1 \cdot C = Path\ 1$$

$$\Downarrow \qquad \Downarrow$$

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

$$\Downarrow \qquad \Downarrow$$

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

4 equations

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

伪距方程里的已知数

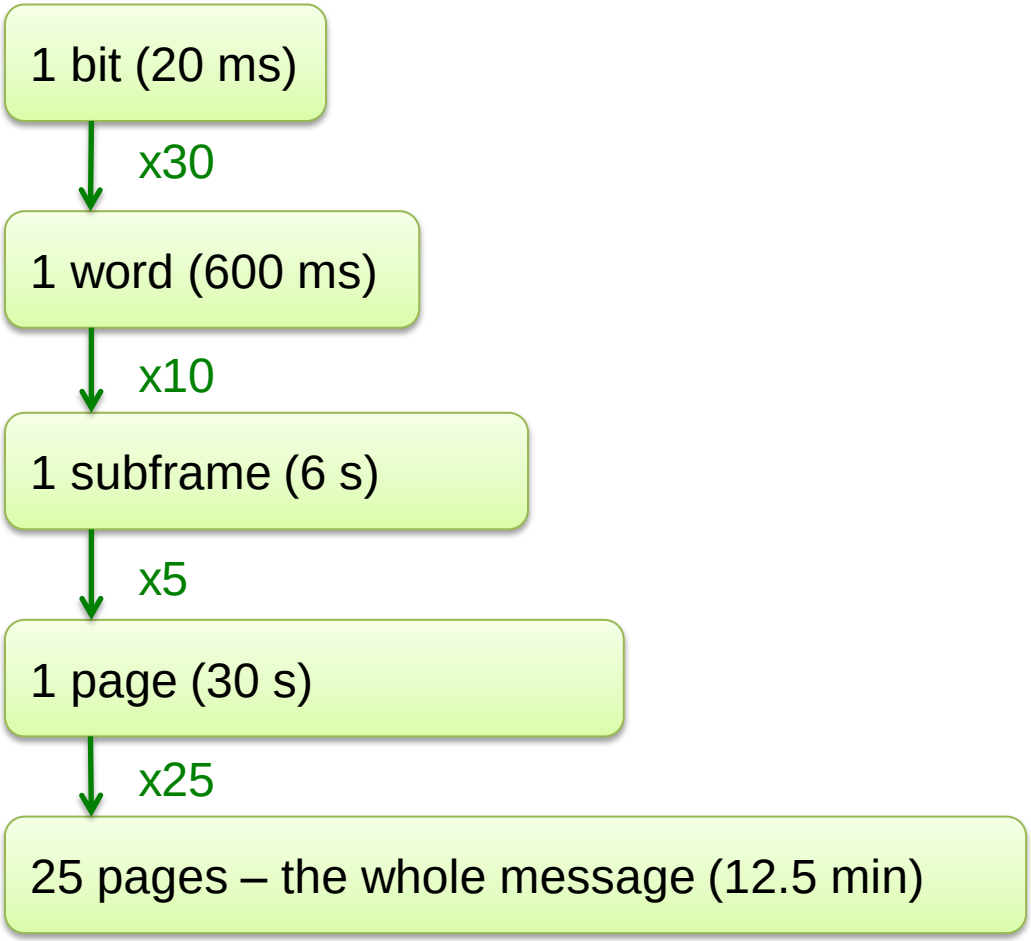
$$\begin{cases} (T + D_1 - T_0) \cdot C = Pos(x_1, y_1, z_1) - Pos(x, y, z) \\ (T + D_2 - T_0) \cdot C = Pos(x_2, y_2, z_2) - Pos(x, y, z) \\ (T + D_3 - T_0) \cdot C = Pos(x_3, y_3, z_3) - Pos(x, y, z) \\ (T + D_4 - T_0) \cdot C = Pos(x_4, y_4, z_4) - Pos(x, y, z) \end{cases}$$

Calculate the delays at receiver

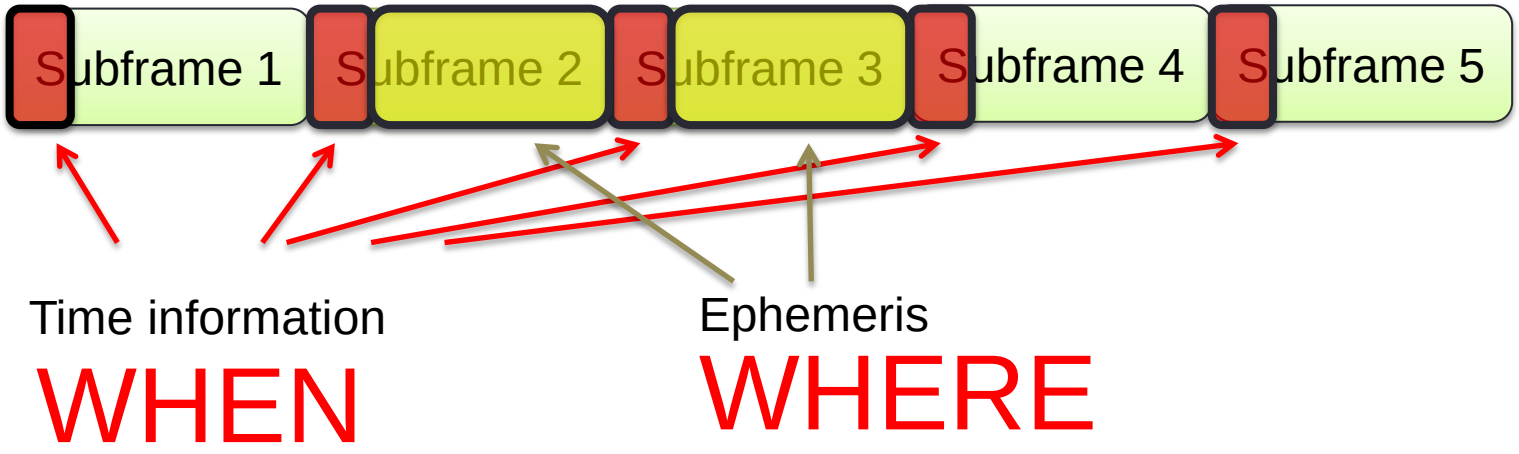
WHEN

WHERE

导航电文的结构


1 bit (20 ms)
x30
1 word (600 ms)
x10
1 subframe (6 s)
x5
1 page (30 s)
x25
25 pages – the whole message (12.5 min)

WHEN & WHERE 信息的位置



开始构造假信号……

找一份星历数据

- 方法一
  - 从CDDIS下载一份星历数据
  - ftp://cddis.gsfc.nasa.gov/gnss/data/daily/
  - 这里只提供前一天的星历
- 方法二
  - 使用gnss-sdr软件接收当前的GPS信号，并把解出来的星历提取出来
  - 其中的GSDR开头的文件就是星历数据，是标准的RINAX格式.

GNSS-SDR解调示例

- Software
  - 运行‘gnss-sdr’
  - 打开GSDR* 文件

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

数据驱动安全

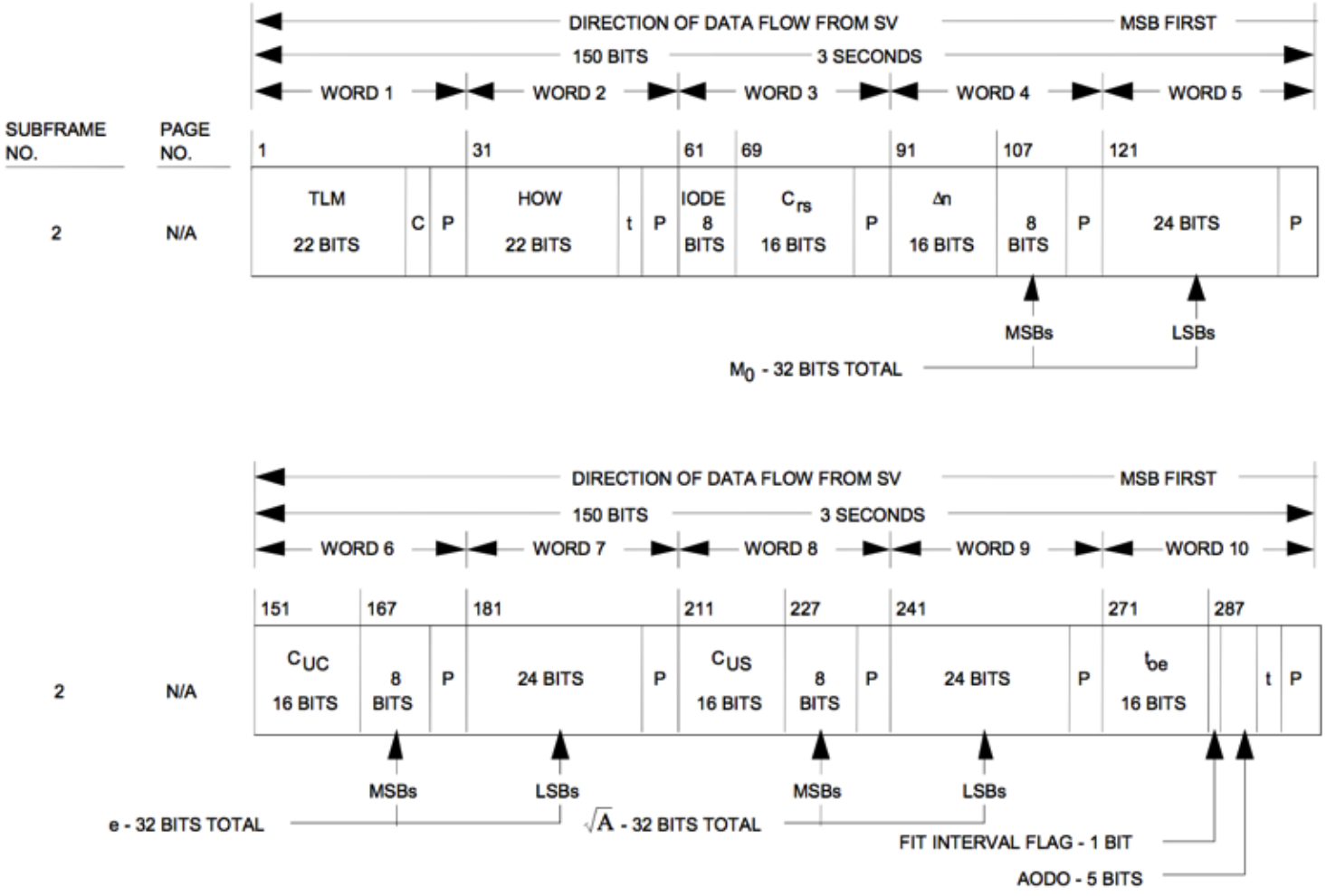
2015 中国互联网安全大会 China Internet Security Conference

GPS模拟器的Matlab代码

main.m

```
8 -     clear global;
9 -     clc;
10 -    global SimGlobal;
11 -    global CI;
12 -    disp('------------------');
13 -    init;
14 -    disp('------------------');
15
16      % % set datafile name
17 -    datafilename = 'test.dat';
18 -    ephameris_file = 'brdc0450.15n';
19
20 -    [SimGlobal.noeph,SimGlobal.aEphData]=readrinex(ephameris_file);% read ephemeris data
21 -    SimGlobal.aSatData=selecteph;% select ephemeris data
22 -    satvisible;% decide which satellite is visible
23 -    genmessage_wo_almanac;% generate telegraph
24      %genmessage;
25 -    channel_data = genchannel;
26 -    gensignal(channel_data,datafilename);
27
28
```

帧结构示例 - 子帧2

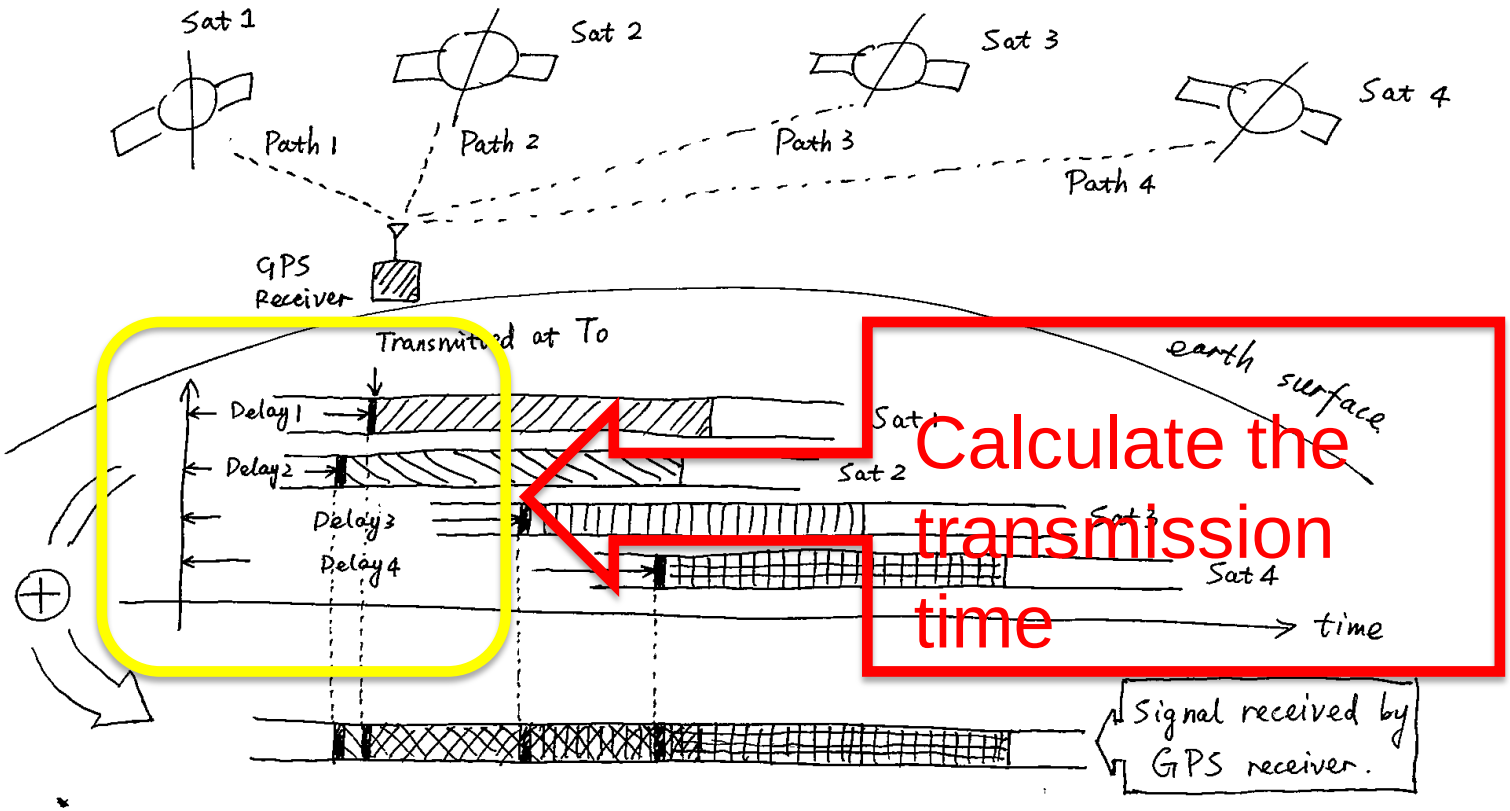

DIRECTION OF DATA FLOW FROM SV
MSB FIRST
150 BITS
3 SECONDS
WORD 1
WORD 2
WORD 3
WORD 4
WORD 5
SUBFRAME NO.
PAGE NO.
1
31
61
69
91
107
121
2
N/A
TLM 22 BITS
C
P
HOW 22 BITS
t
P
IODE 8 BITS
C_{rs} 16 BITS
P
Δn 16 BITS
8 BITS
P
24 BITS
P
MSBs
LSBs
M_0 - 32 BITS TOTAL
DIRECTION OF DATA FLOW FROM SV
MSB FIRST
150 BITS
3 SECONDS
WORD 6
WORD 7
WORD 8
WORD 9
WORD 10
151
167
181
211
227
241
271
287
2
N/A
C_{UC} 16 BITS
8 BITS
P
24 BITS
P
C_{US} 16 BITS
8 BITS
P
24 BITS
P
t_{oe} 16 BITS
t
P
MSBs
LSBs
MSBs
LSBs
e - 32 BITS TOTAL
$\sqrt{A}$ - 32 BITS TOTAL
FIT INTERVAL FLAG - 1 BIT
AODO - 5 BITS

产生5个子帧的导航电文

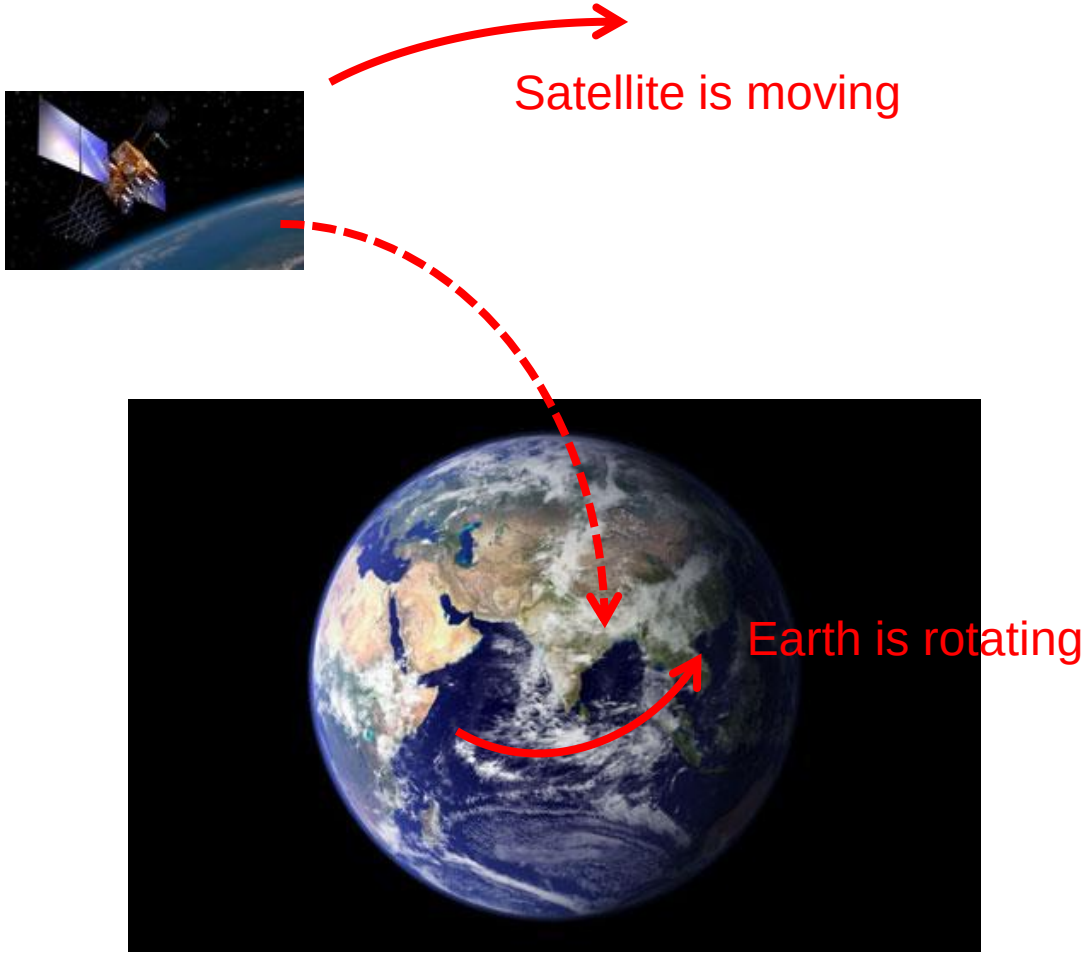
```
for i=1:CT.MaxSatNum
    pO=SimGlobal.aSatData(i).sOrbitData;
    pN=SimGlobal.aSatData(i).sNavData;
    pE=SimGlobal.aSatData(i).sOrbitData.sEphData;
    pA=SimGlobal.aSatData(i).sOrbitData.sAlmData;
    if(pO.visflag==1)
        visual_counter = visual_counter+1;
        disp(['Satalite ' num2str(i) ' 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
```

比特 ——→ 波形

再回顾一下基本原理


Sat 1
Sat 2
Sat 3
Sat 4
Path 1
Path 2
Path 3
Path 4
GPS Receiver
Transmitted at To
earth surface
Delay 1
Delay 2
Delay 3
Delay 4
Sat 1
Sat 2
Sat 3
Sat 4
time
Signal received by GPS receiver.
Calculate the transmission time

如何计算信号的传播时间？



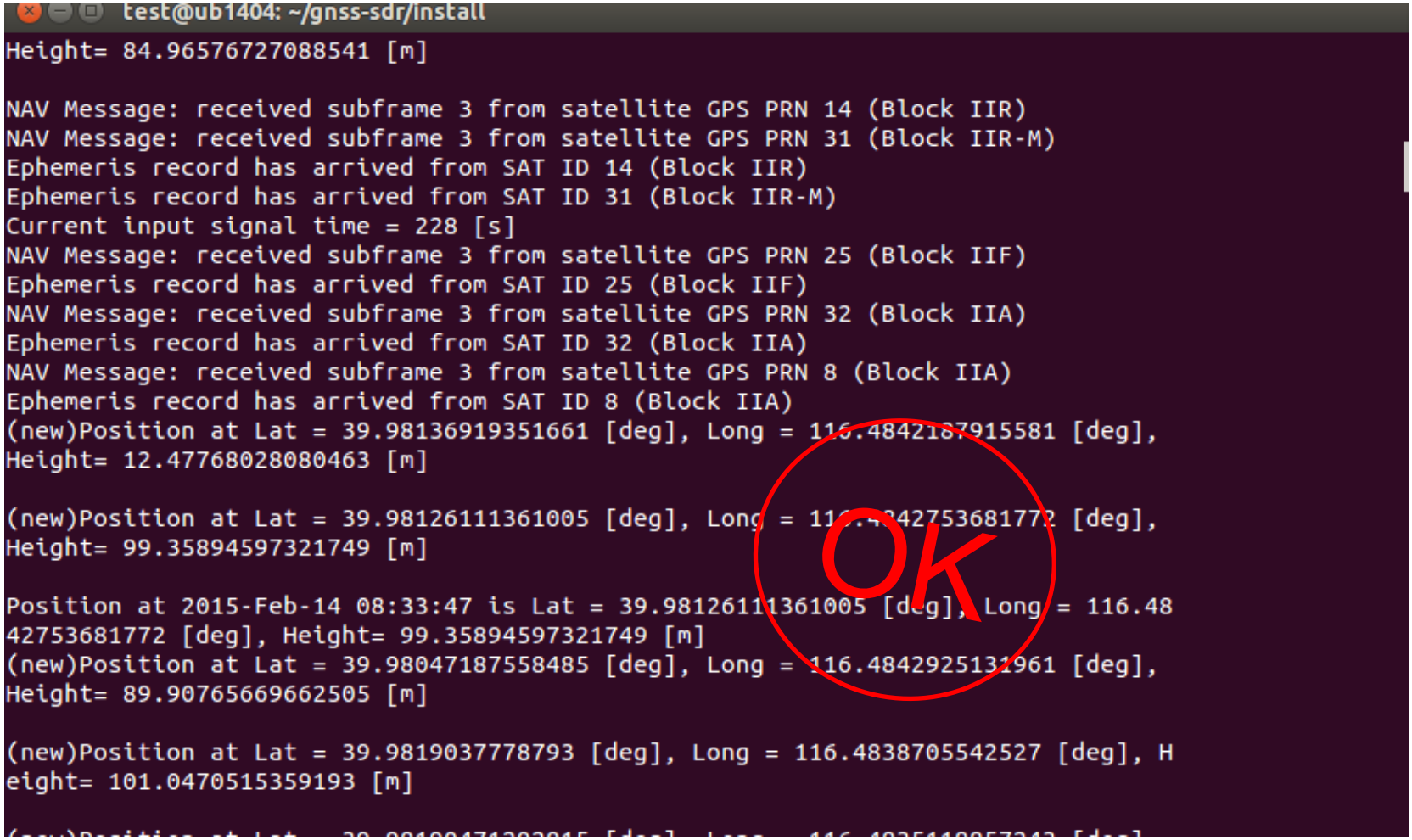
NOT
EASY

产生波形的Matlab代码

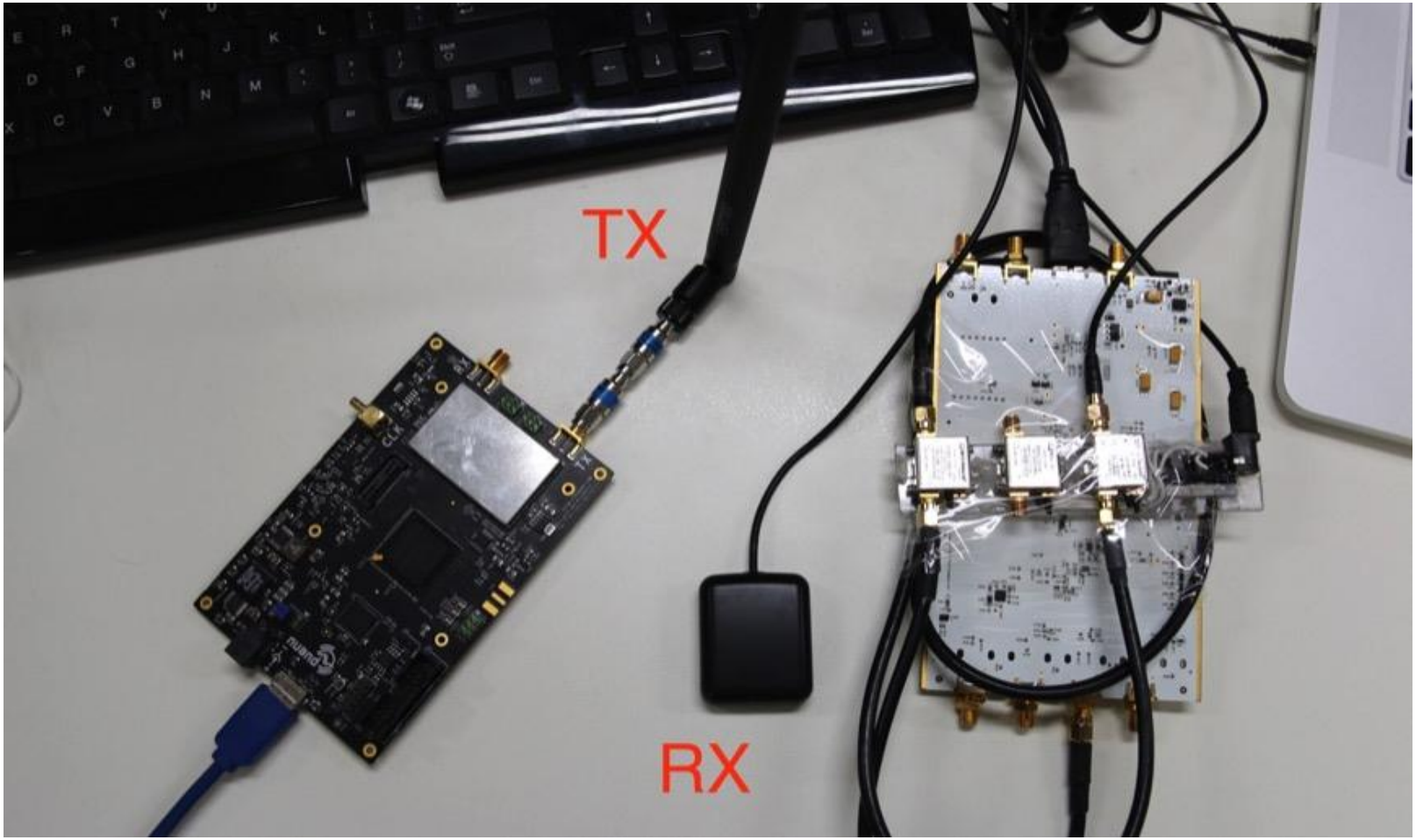
main.m

```
8 -     clear global;
9 -     clc;
10 -    global SimGlobal;
11 -    global CI;
12 -    disp('------------------');
13 -    init;
14 -    disp('------------------');
15
16      %% set datafile name
17 -    datafilename = 'test.dat';
18 -    ephameris_file = 'brdc0450.15n';
19
20 -    [SimGlobal.noeph,SimGlobal.aEphData]=readrinex(ephameris_file);% read ephemeris data
21 -    SimGlobal.aSatData=selecteph;% select ephemeris data
22 -    satvisible;% decide which satellite is visible
23 -    genmessage_wo_almanac;% generate telegraph
24      %genmessage;
25 -    channel_data = genchannel;
26 -    gensignal(channel_data,datafilename);
27
28
```

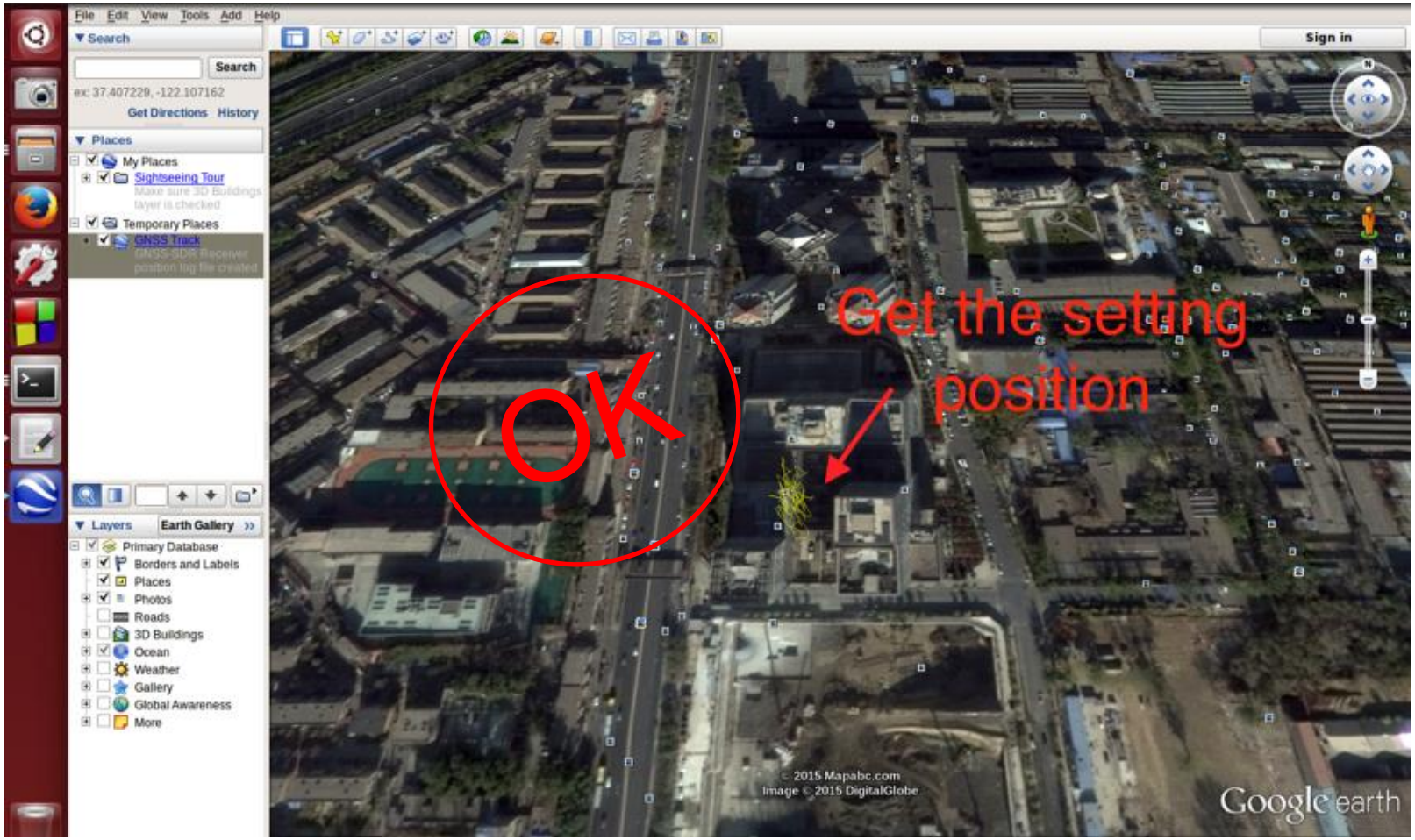
先用GNSS-SDR验证一下



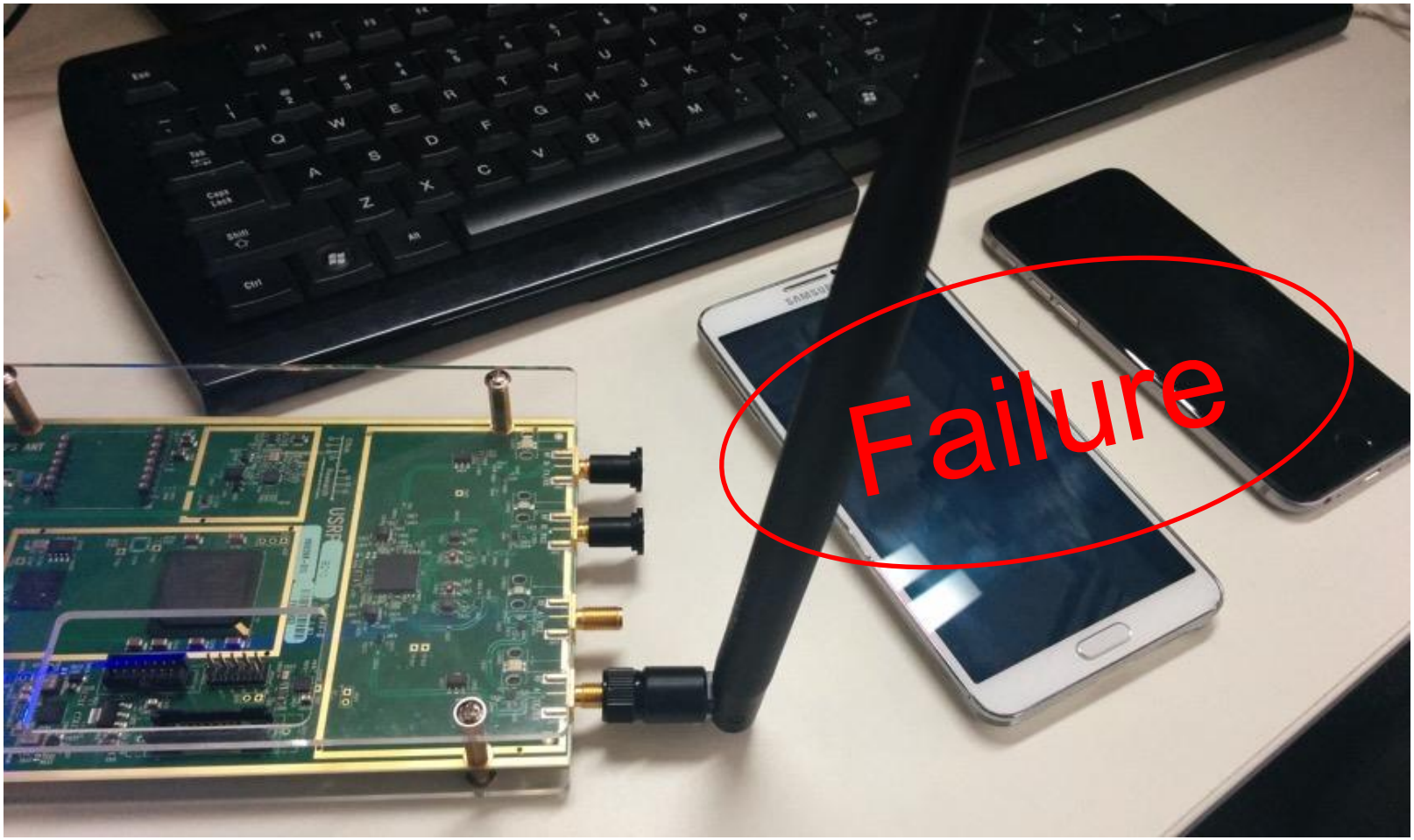
然后经过空中传播，验证一下



GNSS-SDR软接收机正确解调！

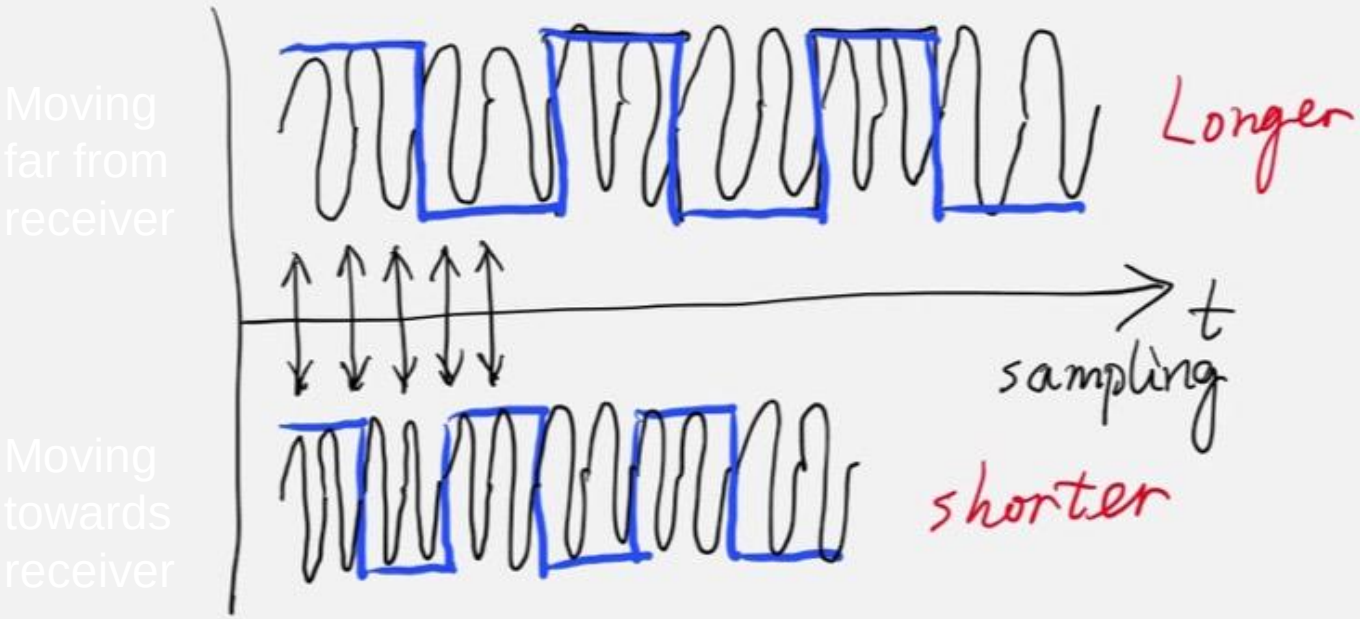


试试手机的反应...

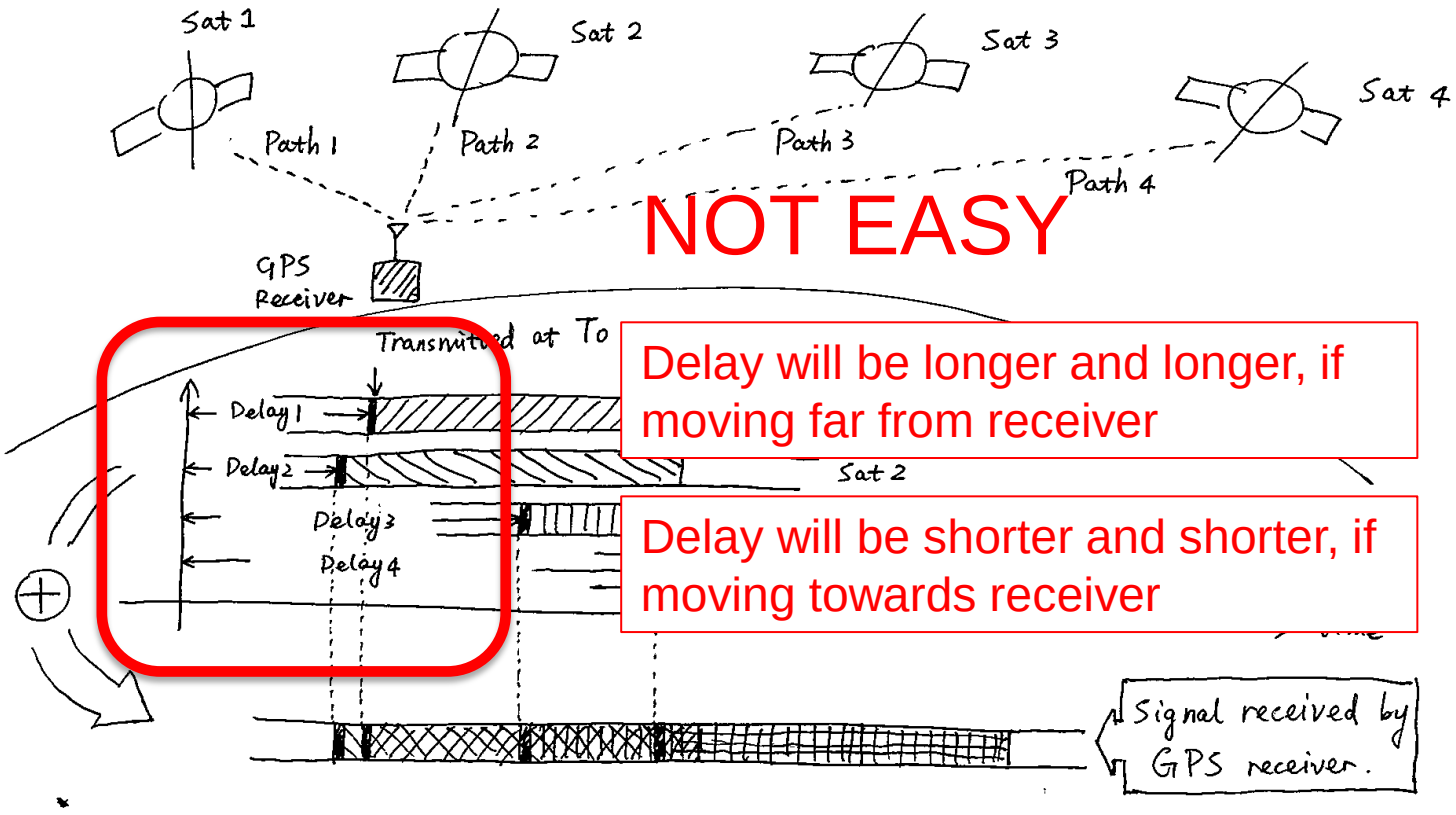


哪里不对？？

多普勒频移需要模拟出来



再次回顾这张图

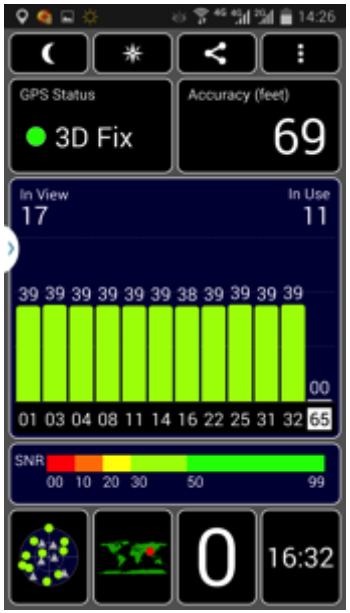

Sat 1
Sat 2
Sat 3
Sat 4
Path 1
Path 2
Path 3
Path 4
NOT EASY
GPS Receiver
Transmitted at To
Delay 1
Delay 2
Delay 3
Delay 4
Sat 2
Delay will be longer and longer, if moving far from receiver
Delay will be shorter and shorter, if moving towards receiver
Signal received by GPS receiver.

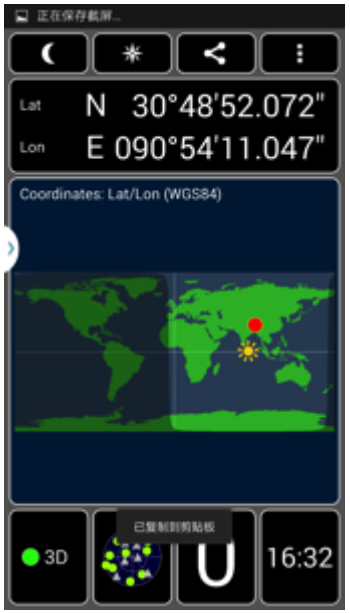
加上多普勒频移了，再试试手机？

- Nexus 5手机
  - 卫星的位置跟设定的一样.
  - 卫星的信号强度几乎一样.
  - 3D定位成功！

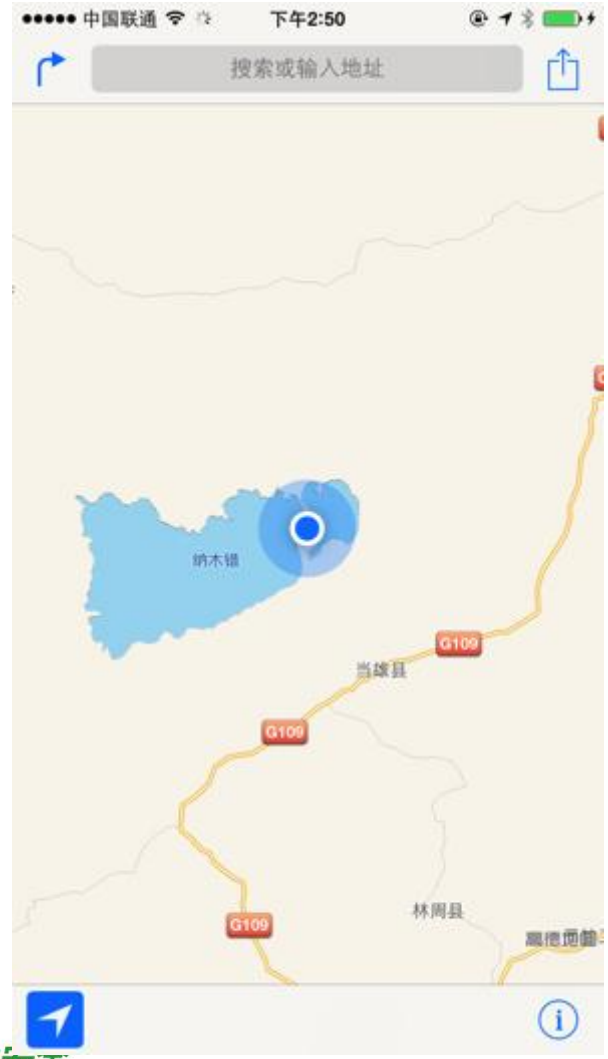
Bingo! Samsung Note 3

- 定位到美丽的纳木错，湖中央……

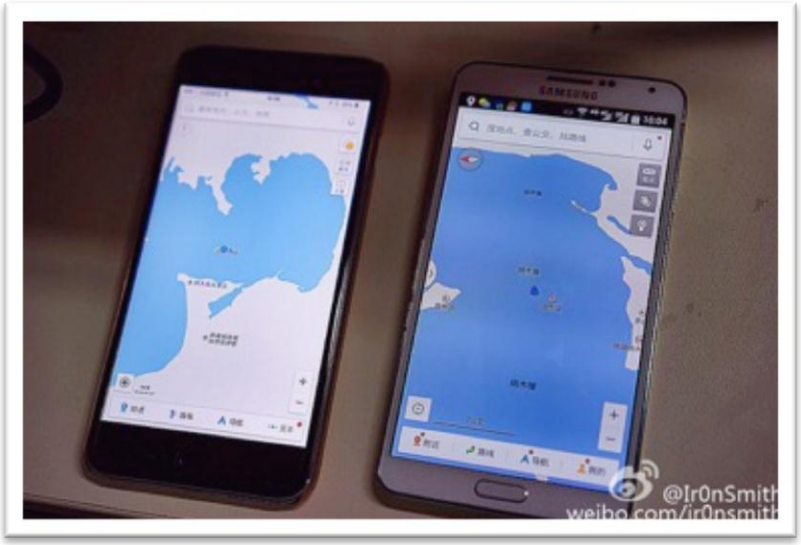




Bingo! iPhone 6



- 也跑到纳木错去了.
- 还发现：如果开启了自动设置时间，系统时间就会被假GPS信号自动改掉。.



可是任意设置时间吗？设到未来？

- 你可能发现我们之前的实验中，时间都是设定为2015年2月14号. 这是因为我们一直在用那一天的星历.

- 实际上除了空间坐标以外，时间坐标也是可以随意设置的.

看一个手机的时空穿梭

我们把时间设置为2015年8月6日，DEF CON 23的开幕时间。实际上这一天是2015年7月14日。

骗完手机，试试骗汽车吧

- 但是重放攻击是可以成功的。

哪里不对？！

子帧4&5没有填数据

子帧结构图

Time information

Ephemeris

Almanac
（历书）

再次测试汽车

- Demo video: 车也泡在纳木错的湖水里了.

欺骗无人机呢？

- 我们都知道，为了避免无人机威胁到人和一些重要设施，无人机是有禁飞区设置的.
- 例如大疆无人机，在禁飞区里飞机是不能起飞的.

欺骗无人机

- Demo video: 绕过禁飞区功能
- 给无人机发送一个夏威夷的坐标，于是它就可以起飞了，即使它正处于北京的禁飞区范围内.

欺骗无人机

- Demo video: 劫持正在飞行的无人机
- 对一架正在自动导航飞行的无人机，给它一个禁飞区的坐标，它会怎样呢？

如何防御GPS欺骗

- 从应用层着手
  - 目前的很多定位系统，把GPS作为最高优先级。因此即使其他定位结果与GPS不一致，也会以GPS坐标为准。
  - 因此，要修改为，综合考虑多个系统的定位结果，从逻辑上把假GPS坐标鉴别出来。
  - 使用多模芯片，例如GPS北斗双模，提高攻击的门槛
- 从接收机芯片着手
  - 在接收机芯片中使用一些算法，检测出GPS欺骗。
- 从GPS卫星的发射信号着手
  - 修改GPS卫星的发射信号，添加带有数字签名的内容

GPS依然不愧为一个伟大的系统

- 它是第一个全球定位系统
- 供全世界使用
- GPS芯片很便宜，可供各种产品使用

- 而且，它实际上一直在更新，也一直有新的卫星发射。
- 因此，我们有信心，未来的GPS系统能够解决这个问题

致谢

- 贾立伟
  - 北航研究生，GPS模拟器项目的创立者，给予我专业的指导
  - https://code.csdn.net/sywcxx/gps-sim-hackrf
- 焦现军
  - 目前是苹果的工程师，SDR爱好者，给予我重要的指导
  - http://sdr-x.github.io/

谢谢！