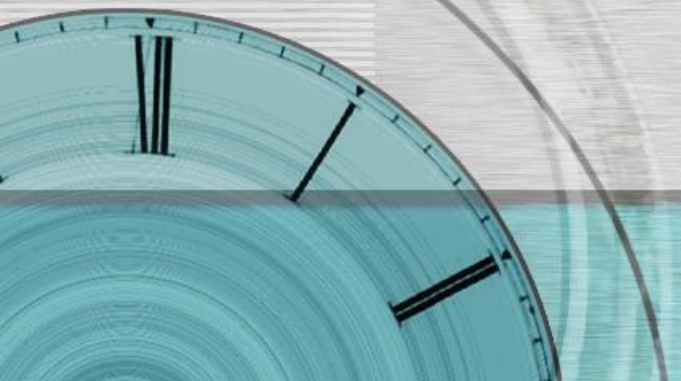
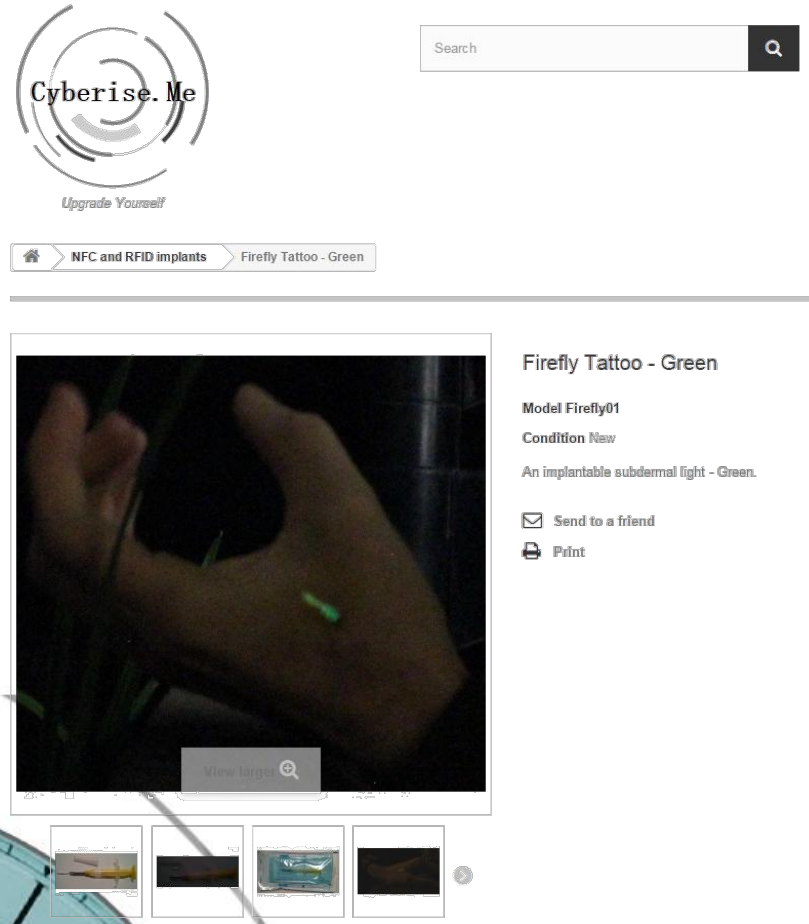
短距离无线系统与航空无线电系统攻击

UnicornTeam 无线电硬件实验室

演讲人：张婉桥

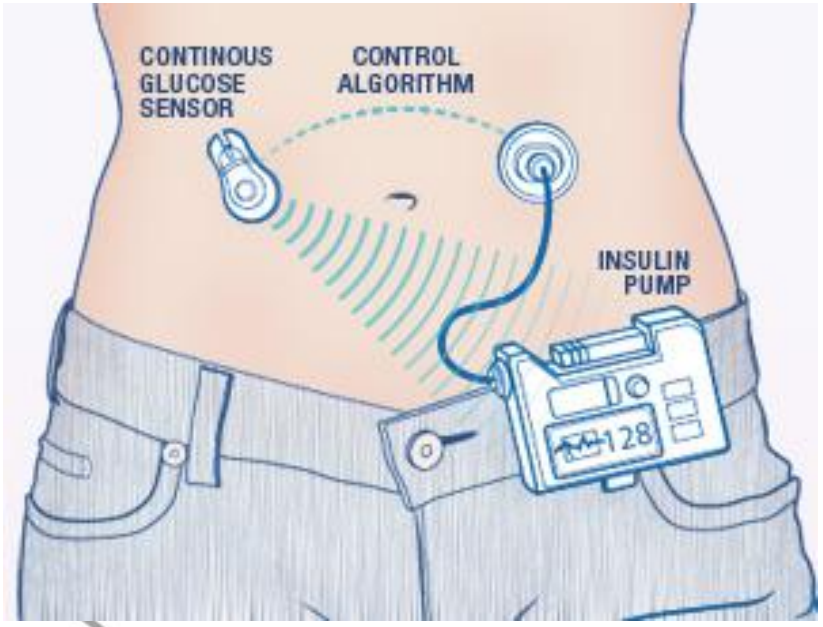


人体移植芯片

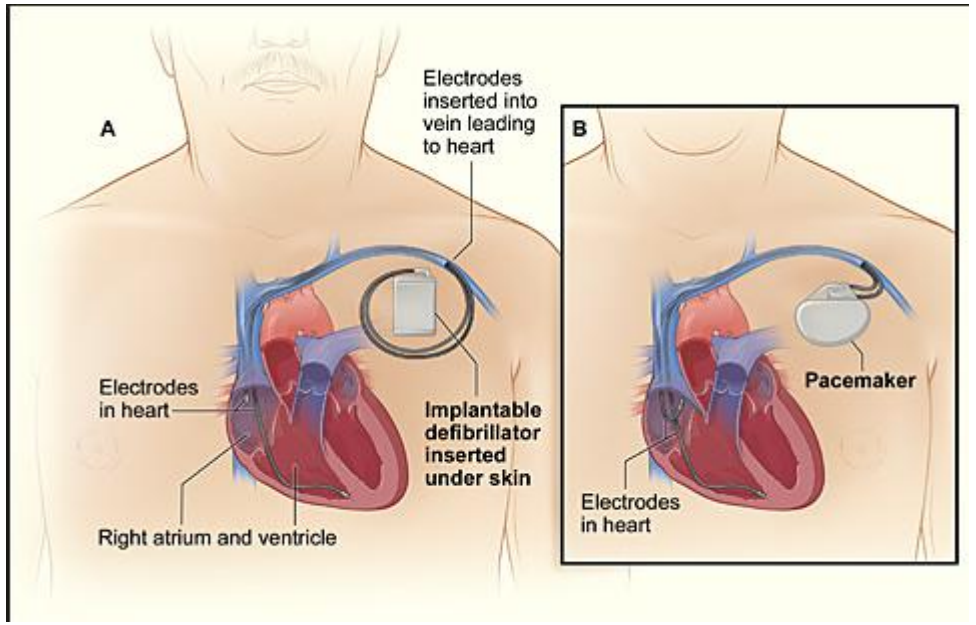

Cyberise.Me
Upgrade Yourself
Search
NFC and RFID implants
Firefly Tattoo - Green
View larger
Firefly Tattoo - Green
Model Firefly01
Condition New
An implantable subdermal light - Green.
Send to a friend
Print
US $119.00
US $119.00 per 1
Quantity
1
Add to cart


SPH5311
5.25"x 10"/ 13 x 25 cm
www.adelphi.com

人体移植设备



人造胰腺



植入型心率复除颤器

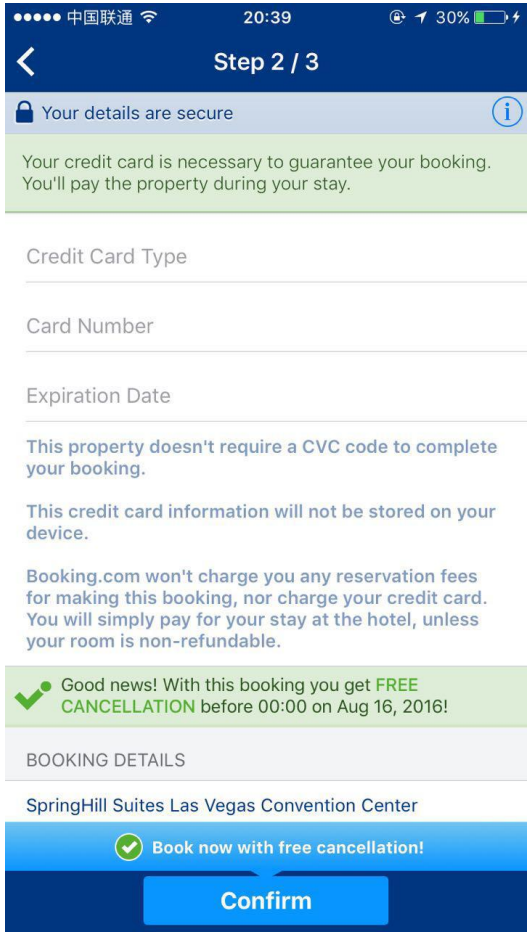
汽车无线控制

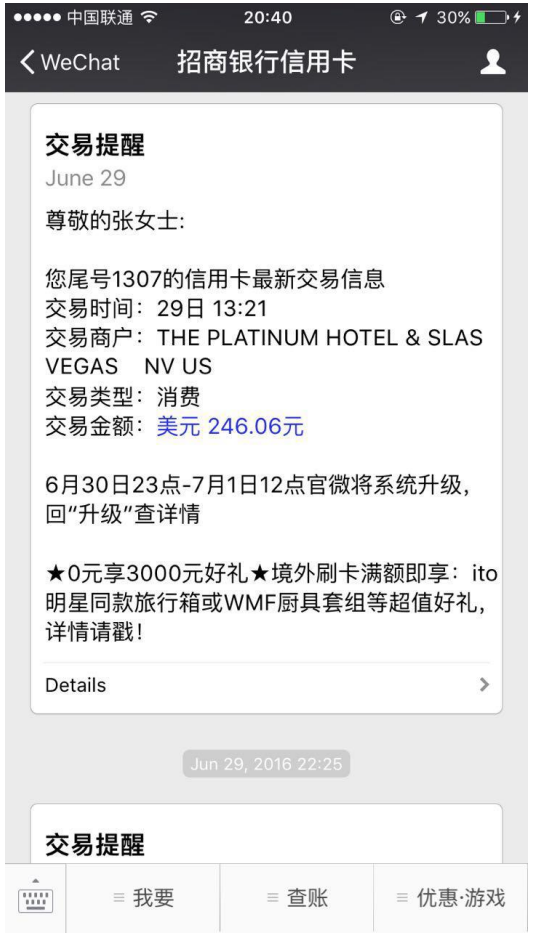
IC智能卡


ICBC
中国工商银行
白金卡
6222 0688 8888 8888
6222
月/年
有效期限 88/88
MU DAN KA
UnionPay
银联


优酷

IC智能卡


●●●●● 中国联通 20:39 30%
Step 2 / 3
Your details are secure
Your credit card is necessary to guarantee your booking.
You'll pay the property during your stay.
Credit Card Type
Card Number
Expiration Date
This property doesn't require a CVC code to complete your booking.
This credit card information will not be stored on your device.
Booking.com won't charge you any reservation fees for making this booking, nor charge your credit card. You will simply pay for your stay at the hotel, unless your room is non-refundable.
Good news! With this booking you get FREE CANCELLATION before 00:00 on Aug 16, 2016!
BOOKING DETAILS
SpringHill Suites Las Vegas Convention Center
Book now with free cancellation!
Confirm


●●●●● 中国联通 20:40 30%
WeChat
招商银行信用卡
交易提醒
June 29
尊敬的张女士:
您尾号1307的信用卡最新交易信息
交易时间：29日 13:21
交易商户：THE PLATINUM HOTEL & SLAS VEGAS NV US
交易类型：消费
交易金额：美元 246.06元
6月30日23点-7月1日12点官微将系统升级，回"升级"查详情
★0元享3000元好礼★境外刷卡满额即享：ito明星同款旅行箱或WMF厨具套组等超值好礼，详情请戳！
Details
Jun 29, 2016 22:25
交易提醒
我要
查账
优惠·游戏

芯片银行卡防护

无线电逆向分析

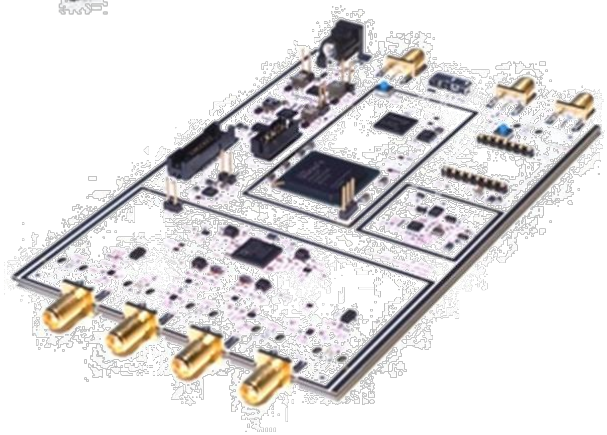
- 短距离无线遥控系统
- 无线传感器
- 航空无线电ADS-B

分析工具——SDR


DVB-T+DAB+FM


HackRF One
GREAT SCOTT GADGETS

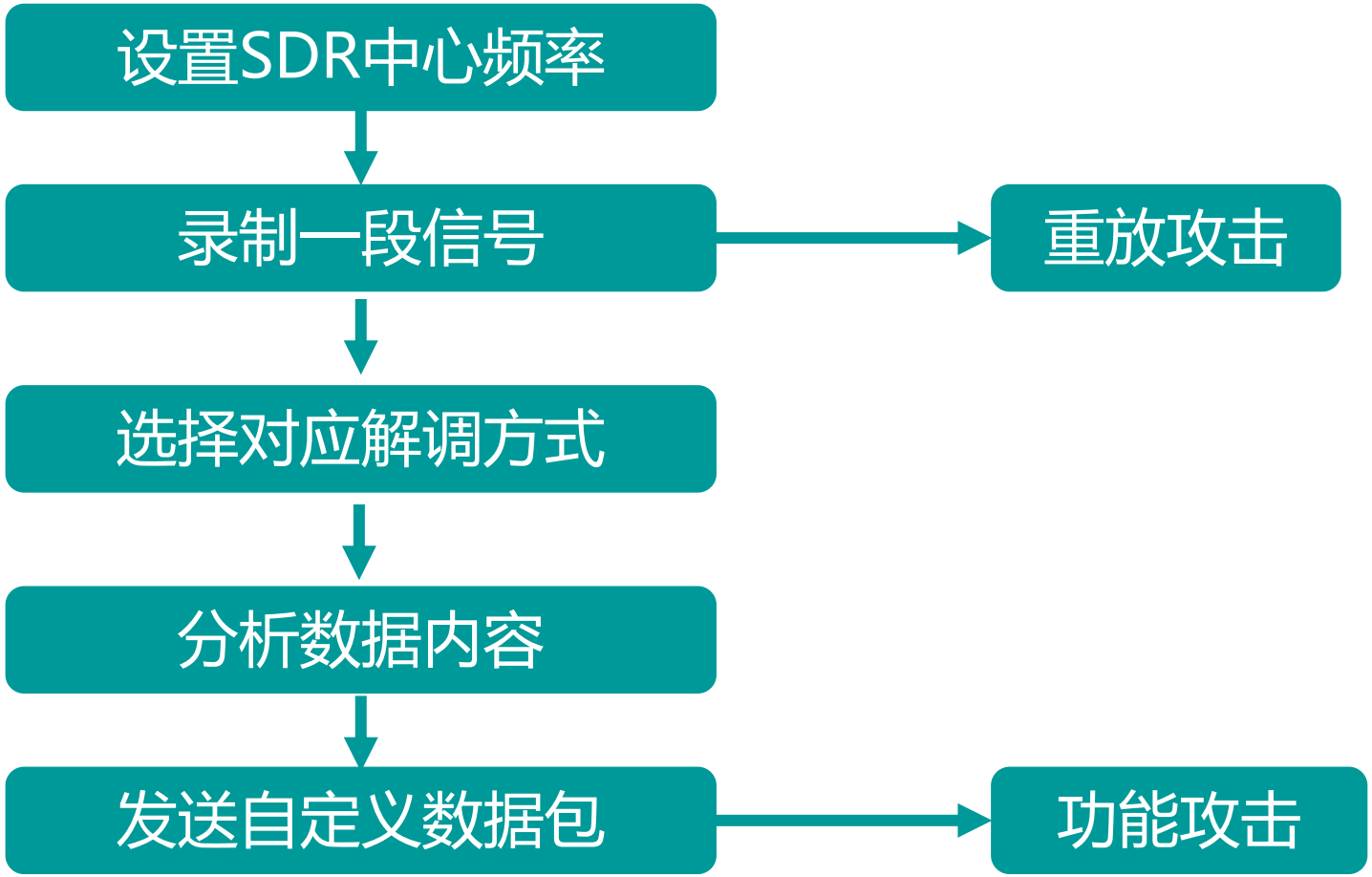

HackRF Jawbreaker



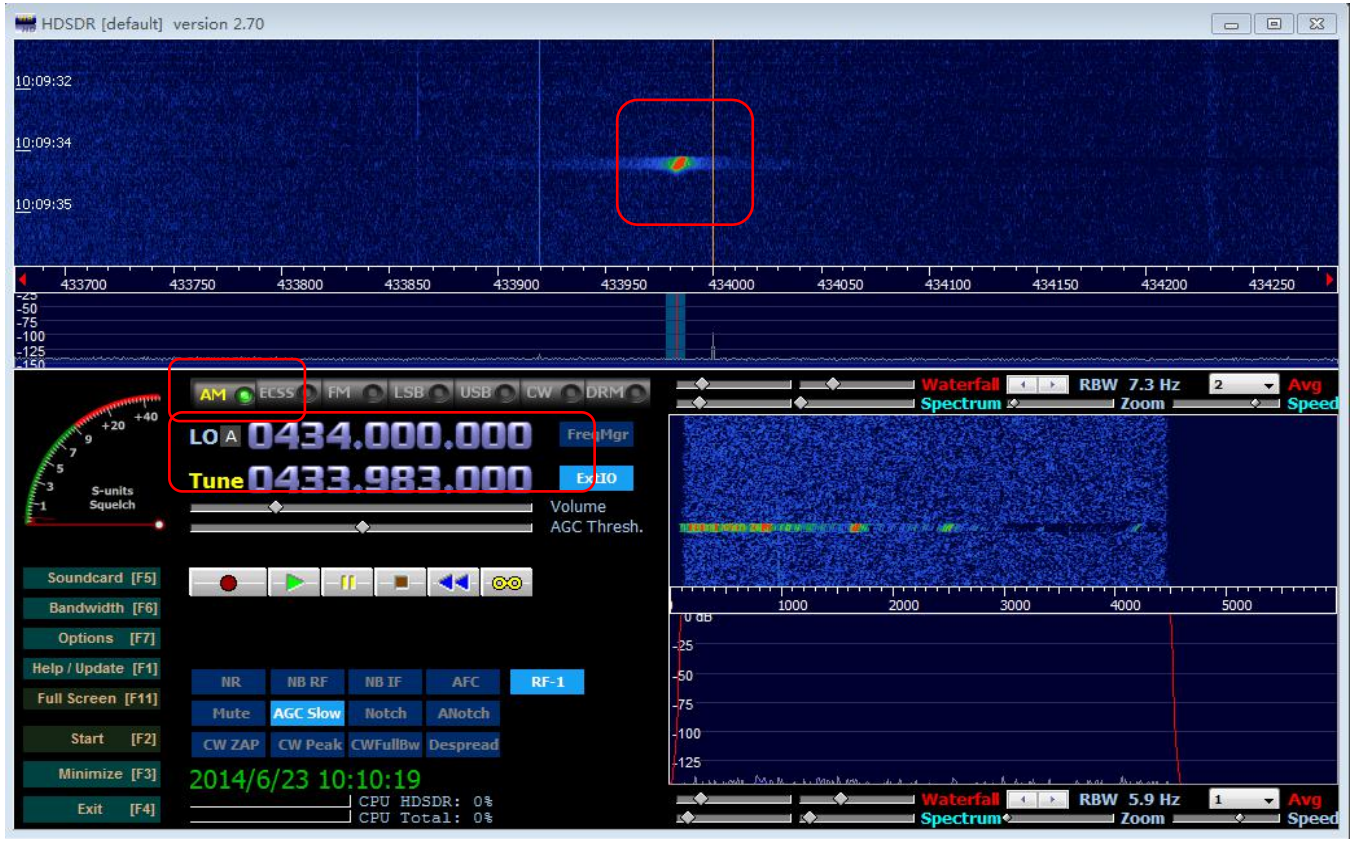
分析工具——SDR

	RTL-SDR	HackRF One	bladeRF x40	USRP B200mini
频段	52M – 2.2 GHz	1M – 6GHz	300M –3.8GHz	70M – 6GHz
带宽	2.56MS/s	20 MS/s	40MS/s	56MS/s
双工类型	只能接收	半双工	全双工	全双工
位宽	8-bit	8-bit	12-bit	12-bit
价格	$20	$300	$420	$675

无线电逆向分析流程

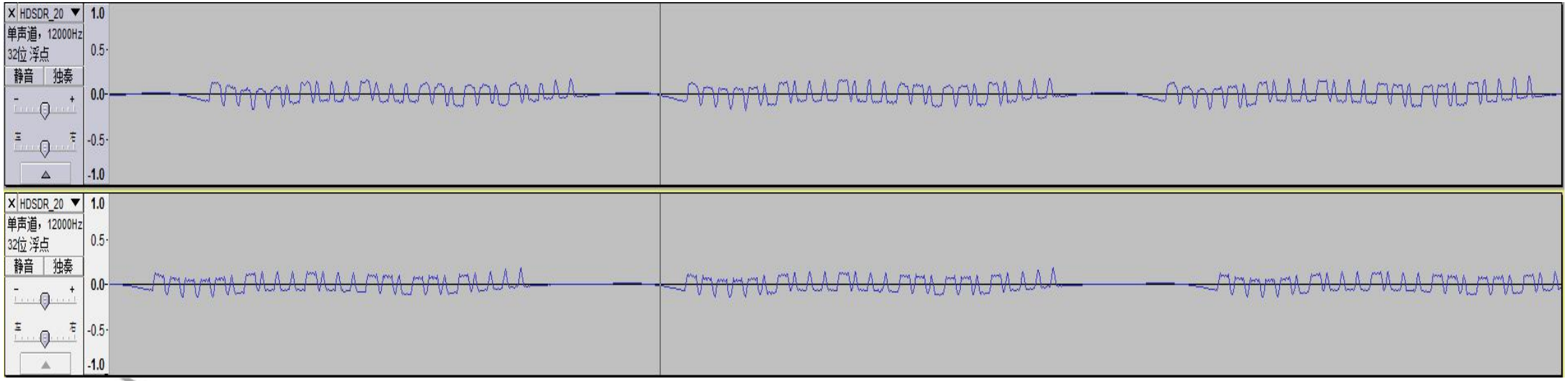


无线遥控信号



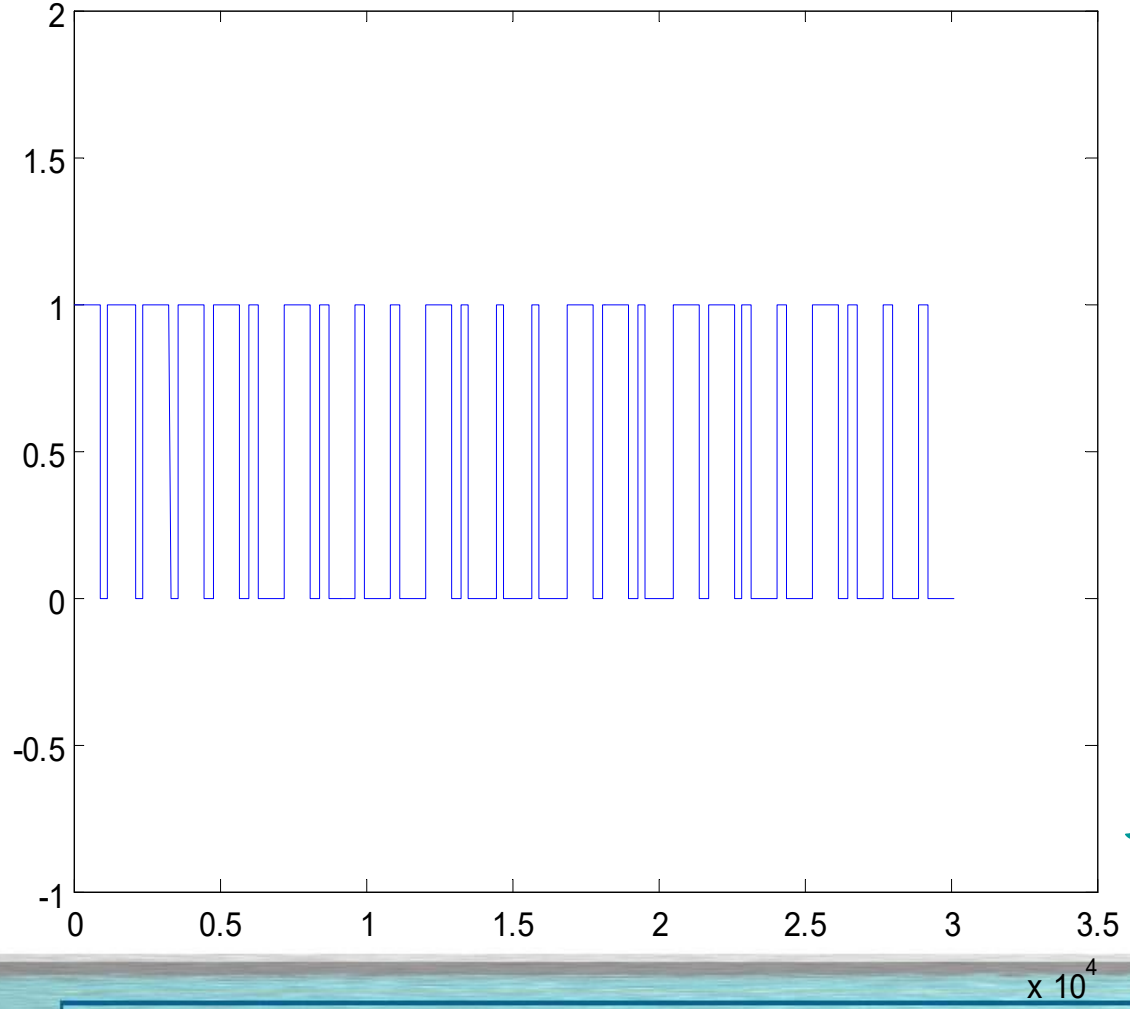
工具： 电视棒
软件： HDSDR

无线遥控信号解调后波形图



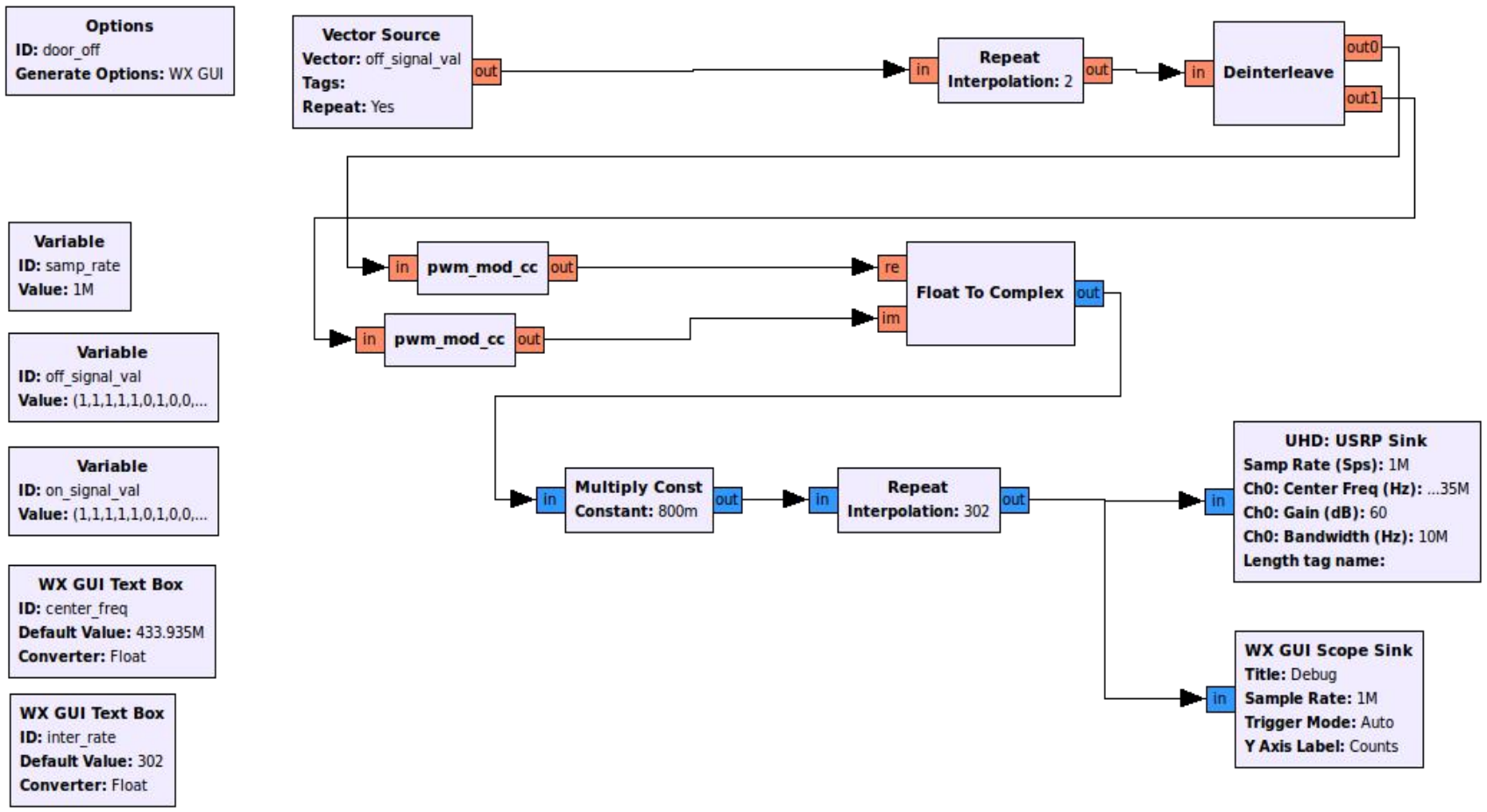
软件：Audacity

分析有效数据内容



软件：MATLAB

流图

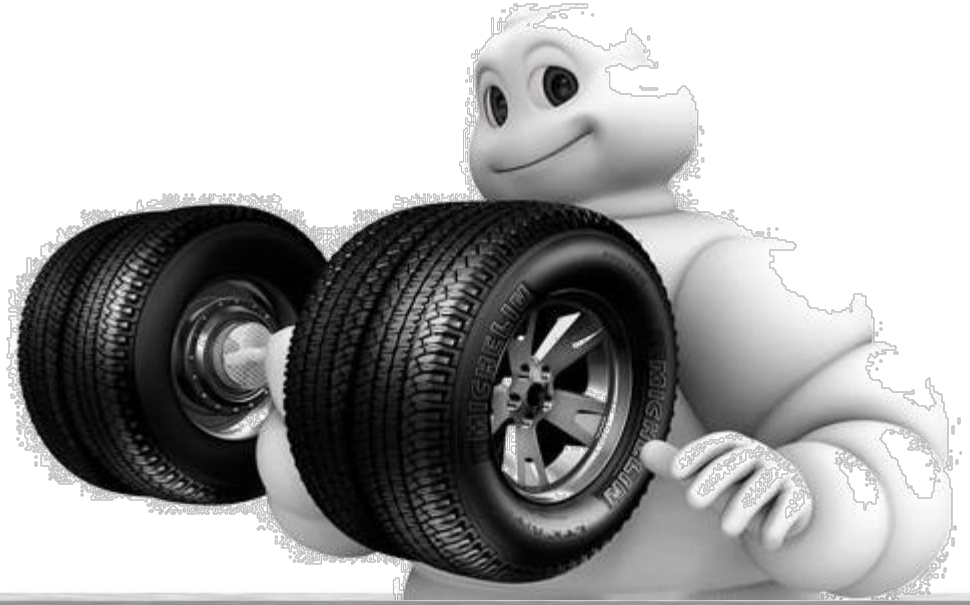


软件：Gnuradio

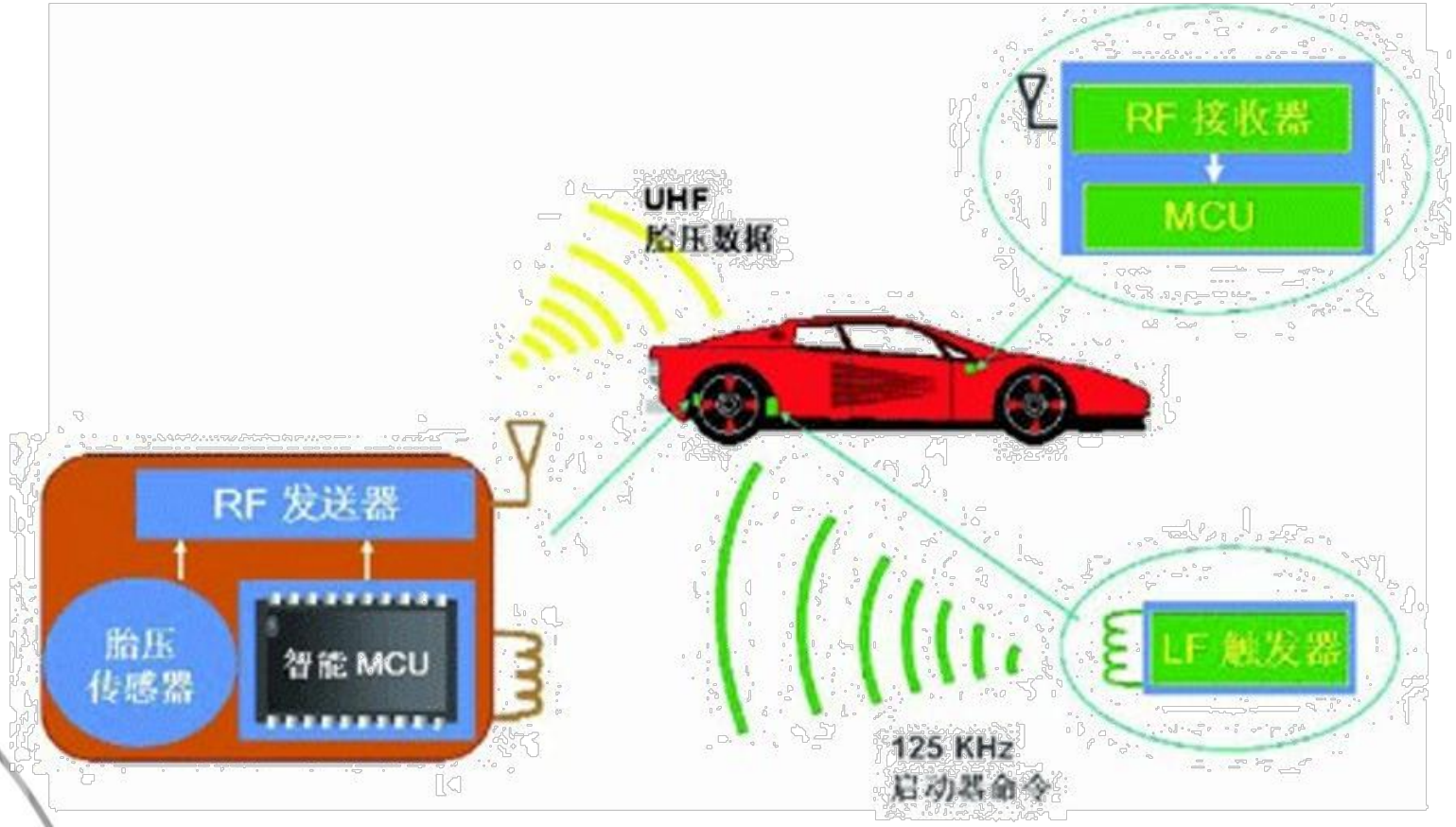
手表抬杆

硬件：Chronos手表

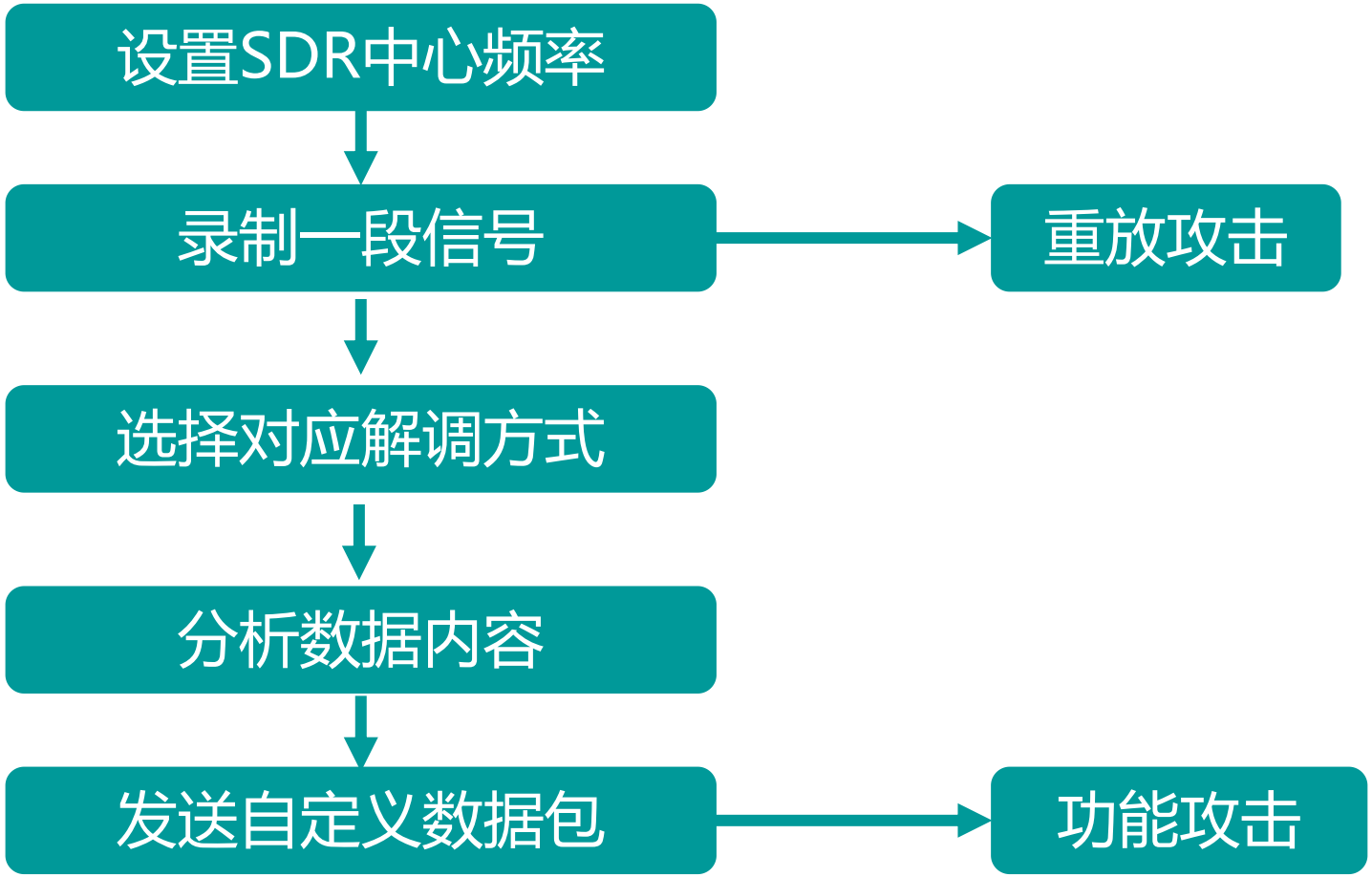
胎压报警器破解



胎压报警器工作原理

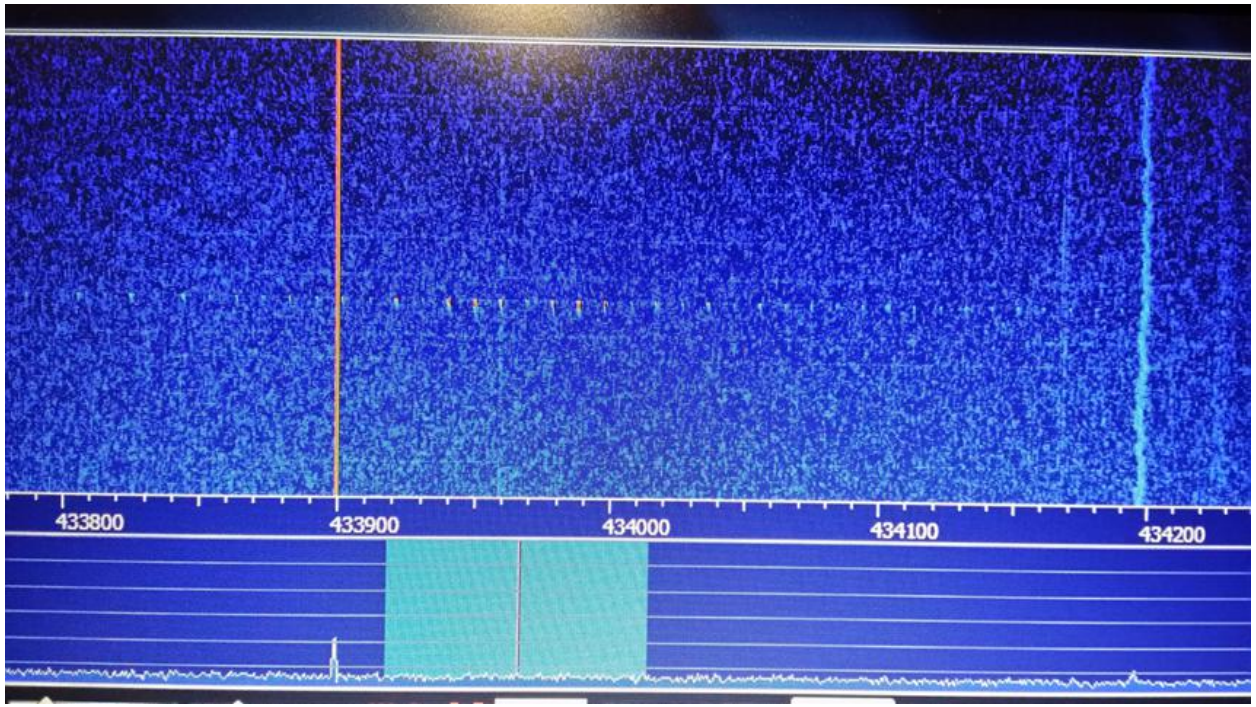


无线电逆向分析流程



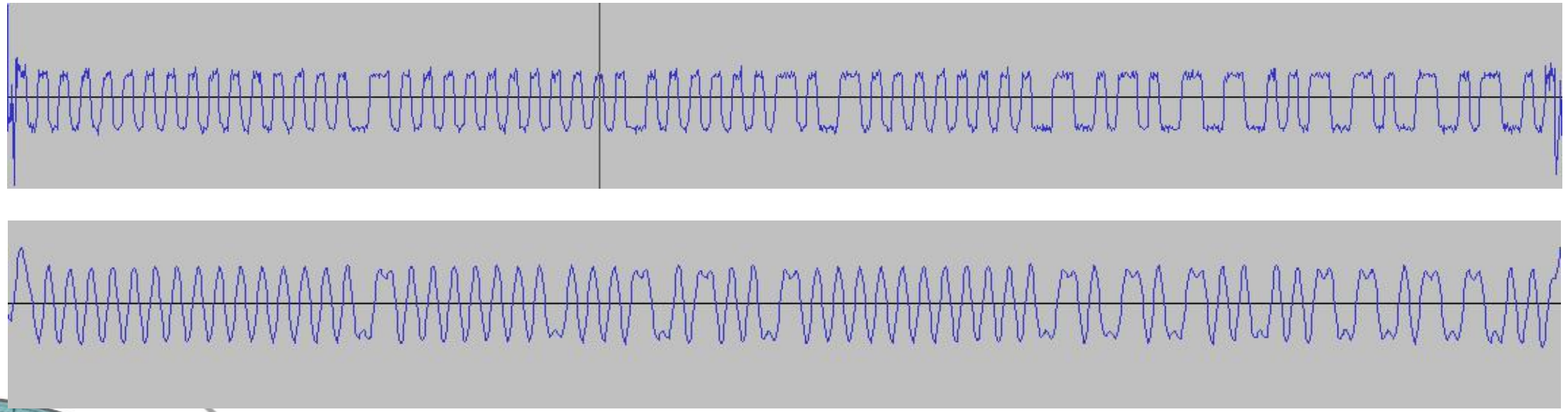
录制信号

- 中心频率 433.92MHz
- 解调： FM
- 比特率9.6Kbps

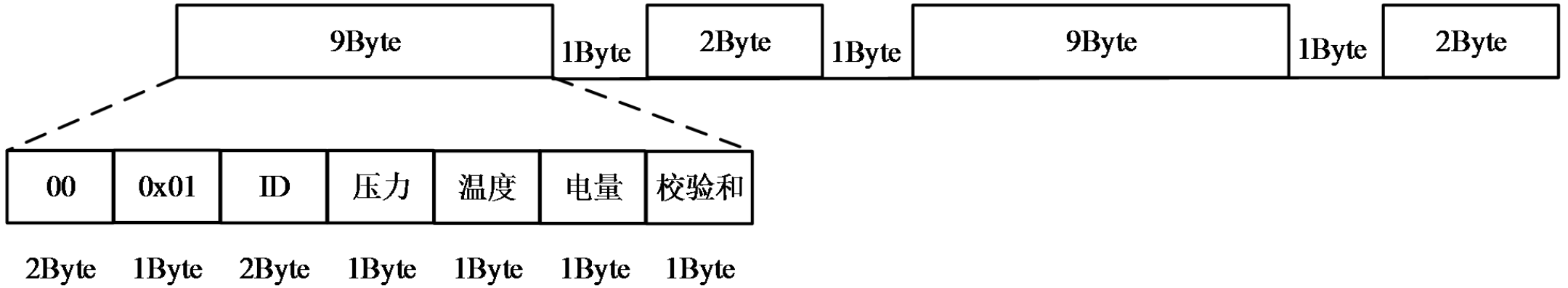


解调后的信号

- 前导码 + 有效码字



逆向分析数据包格式

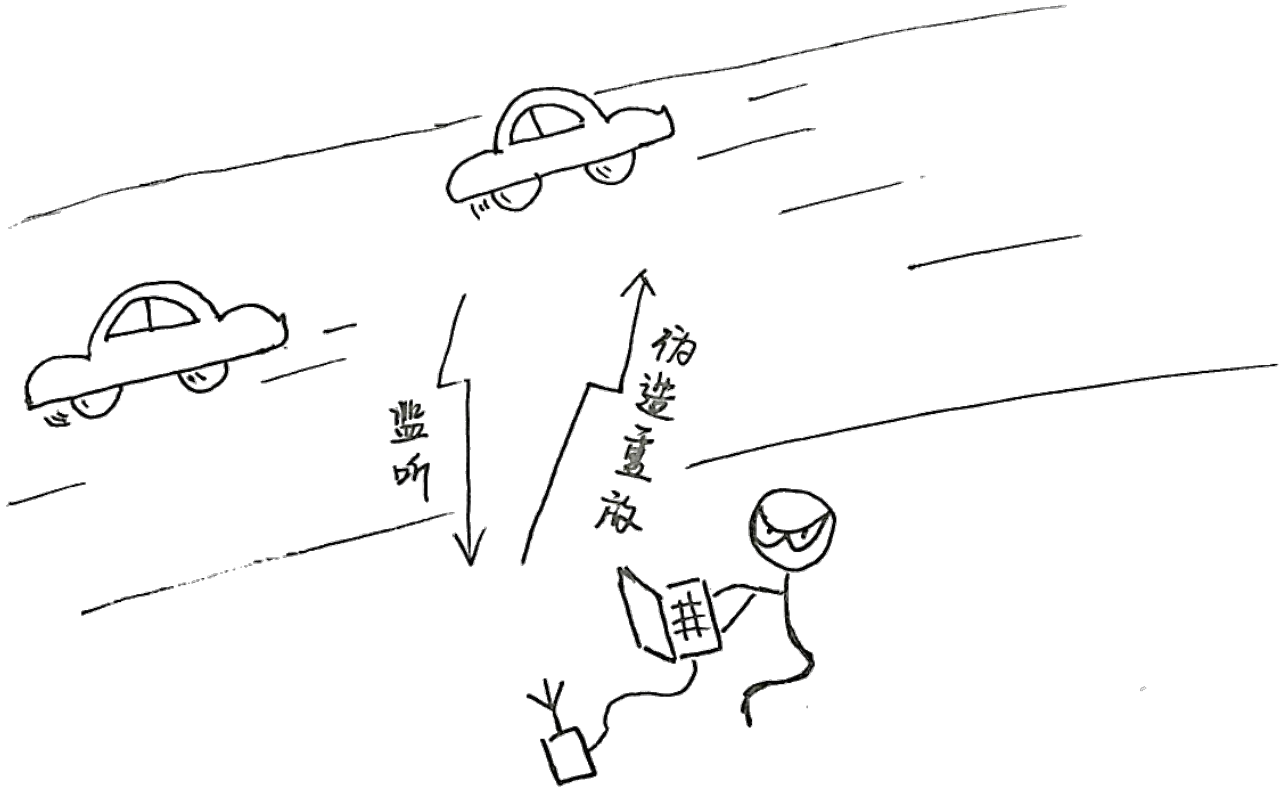


- 11位有效比特
- LSB模式
- CRC校验 = 前6字节相叠加取低8位

功能攻击效果

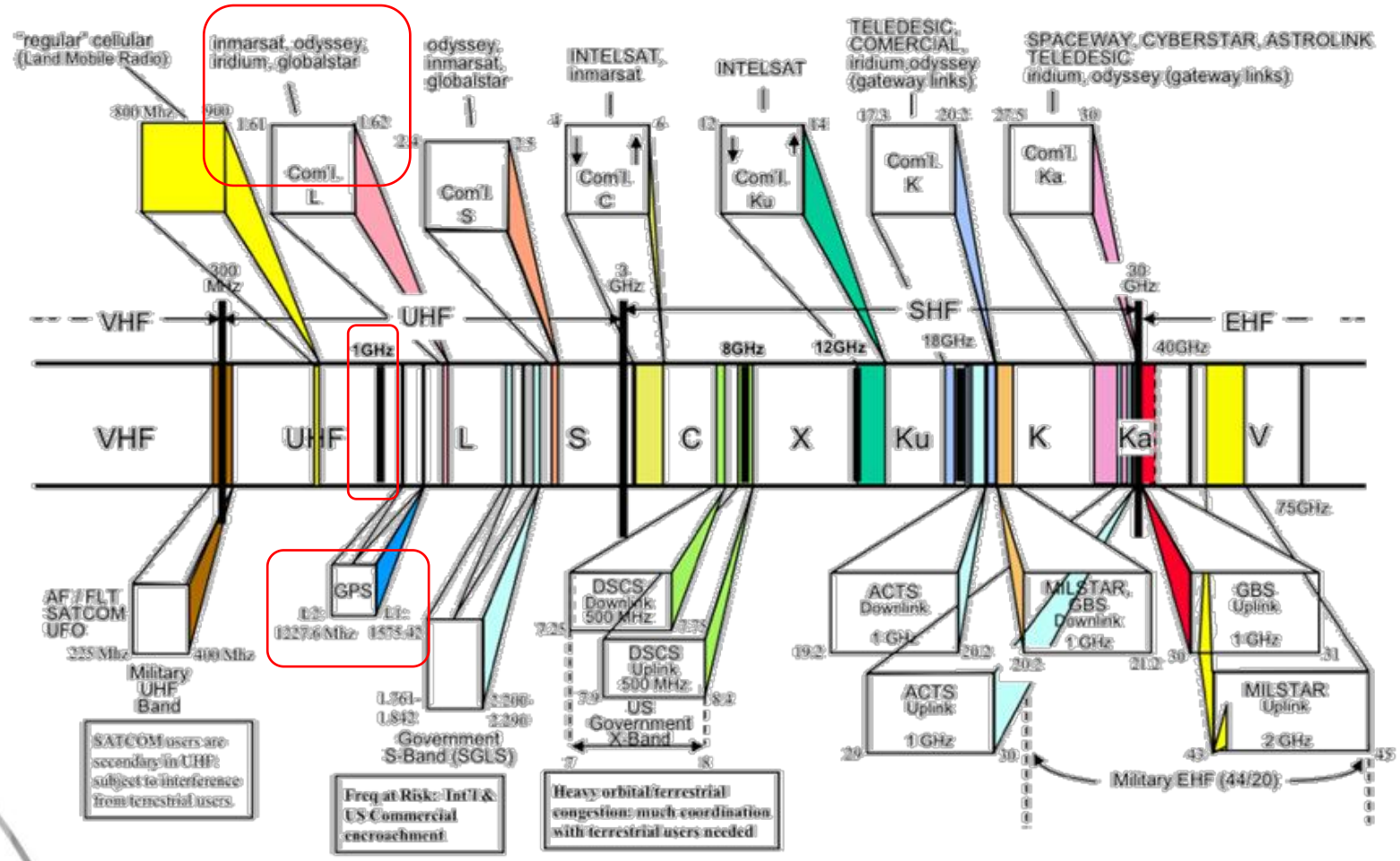
高压与低压攻击效果

现实中的攻击情况



远距离无线电导航攻击

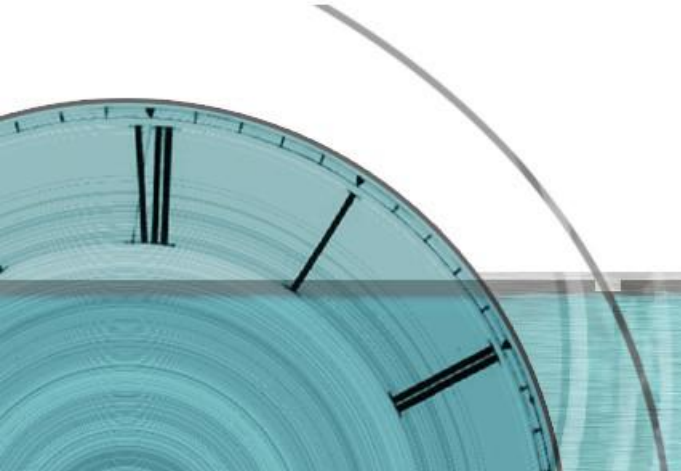
航空无线电导航攻击



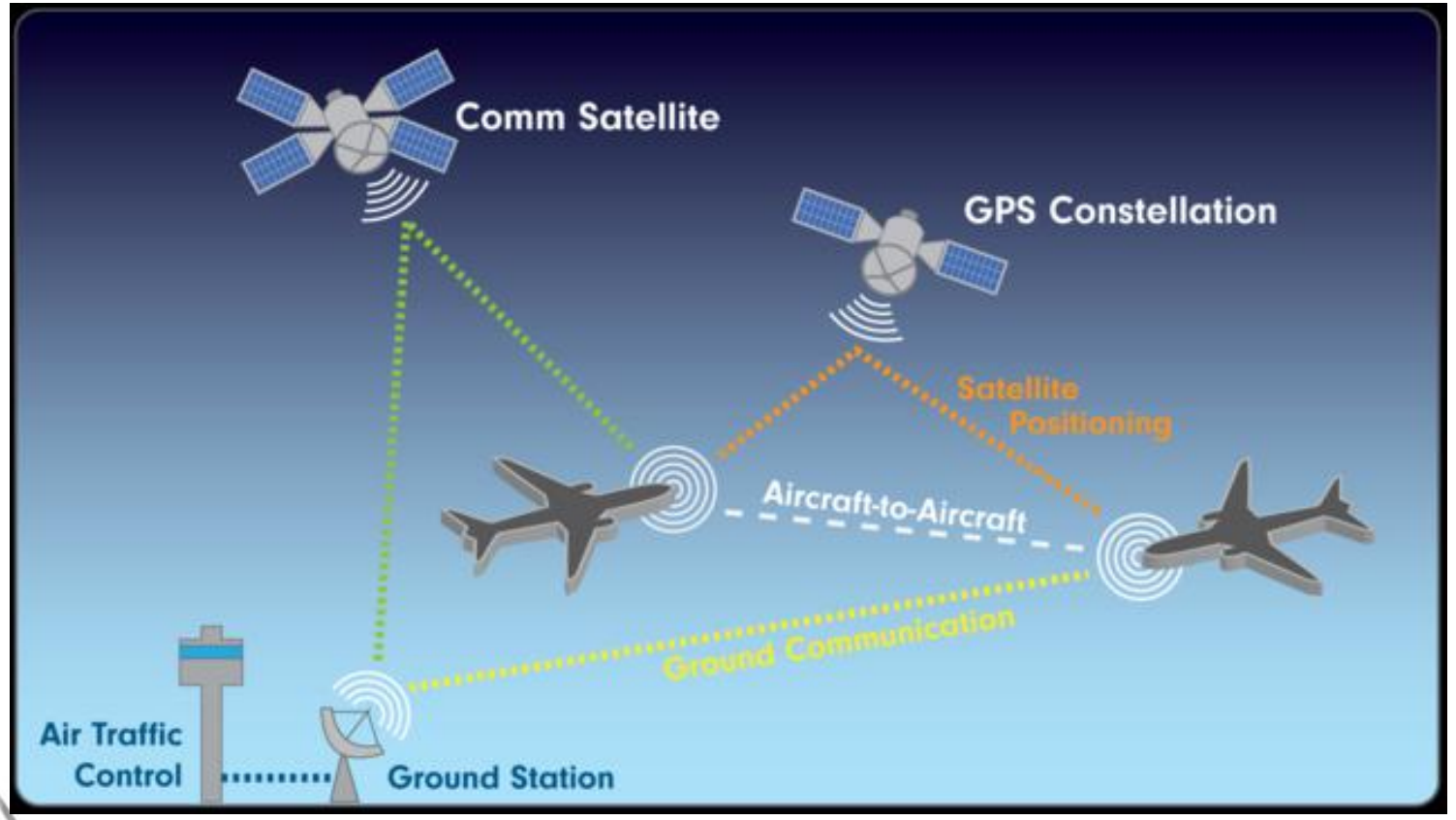
航空飞行涉及的无线电种类

- 通信类：用于飞机与飞机之间，飞机与地面之间的通信

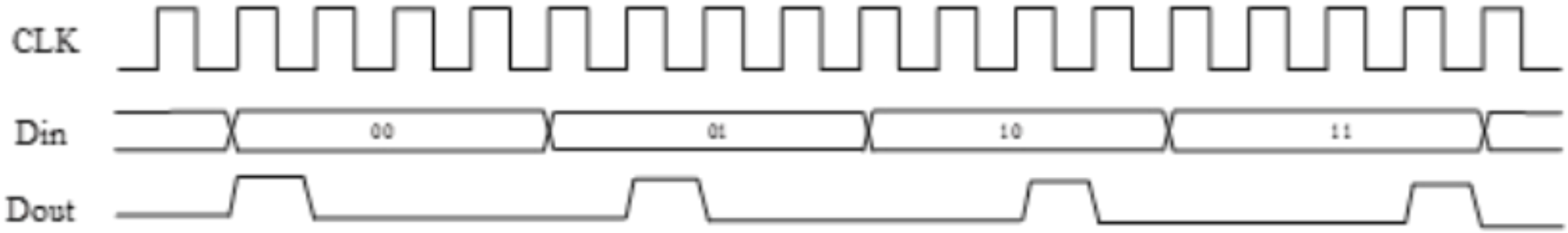
- 导航类：主要是卫星导航和地面信标导航



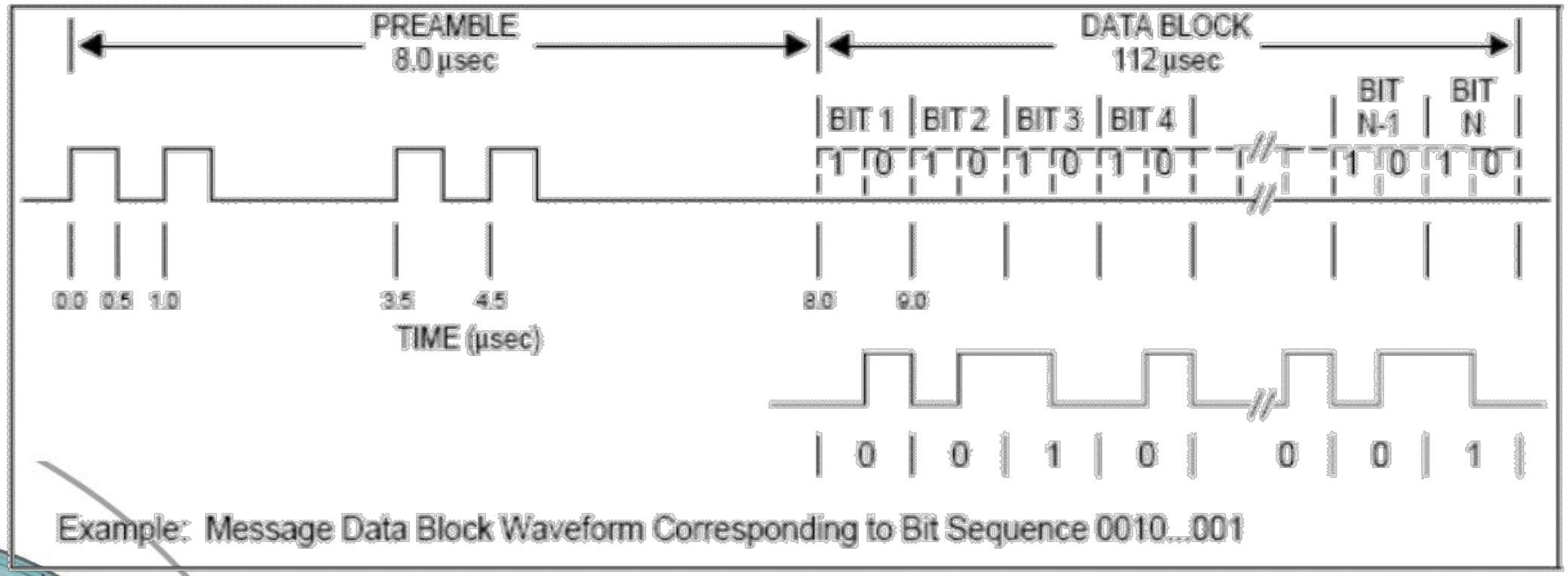
ADS-B自动相关监视广播



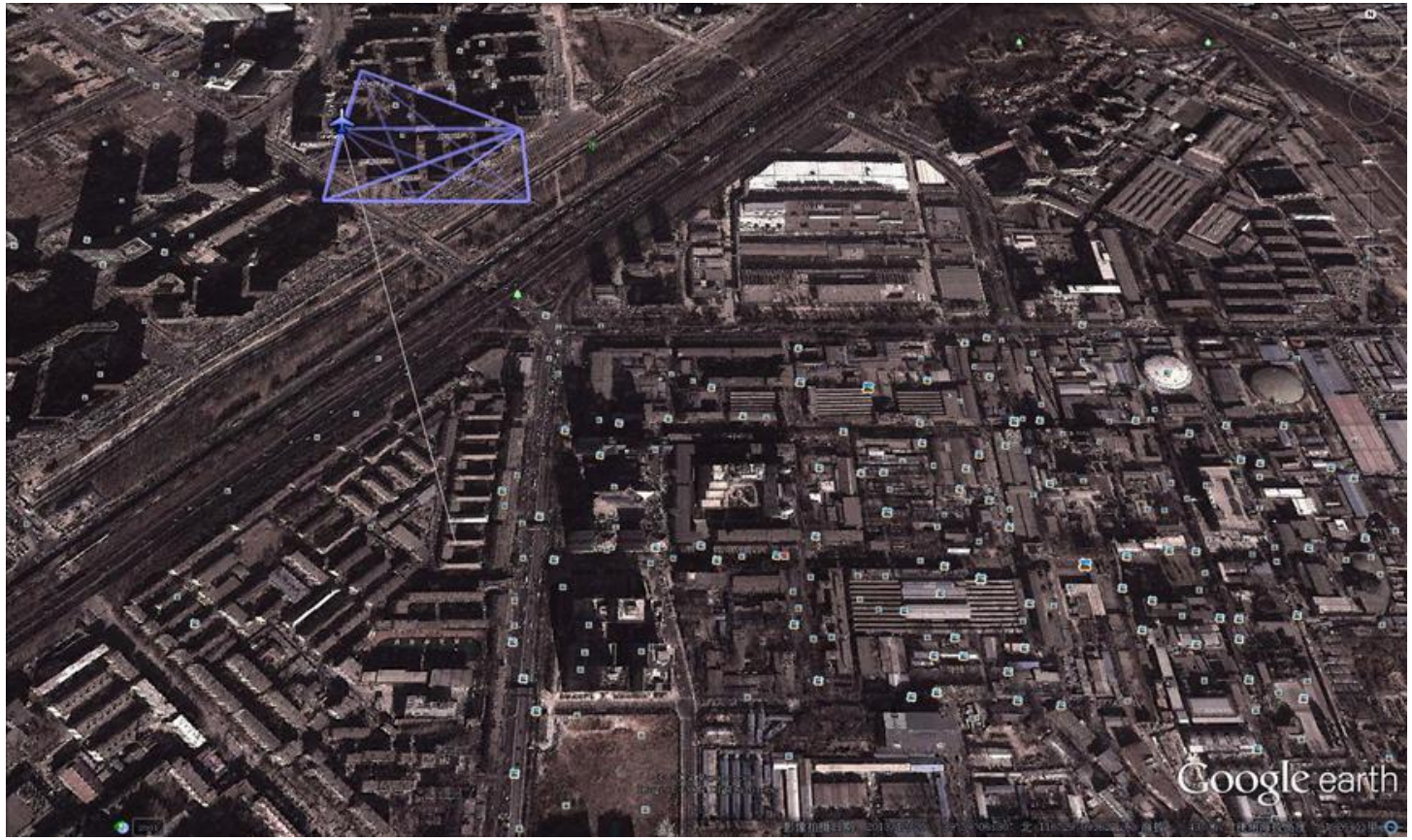
调制方式PPM



ADS-B报文格式


PREAMBLE
8.0 µsec
DATA BLOCK
112 µsec
BIT 1
BIT 2
BIT 3
BIT 4
BIT N-1
BIT N
1 0 1 0 1 0 1 0 1 0 1 0
0.0 0.5 1.0 3.5 4.5 8.0 9.0
TIME (µsec)
0 0 1 0 0 0 1
Example: Message Data Block Waveform Corresponding to Bit Sequence 0010...001

通过虚假的ADS-B信号构造出的飞机



攻防分析

http://www.flightradar24.com

更多无线电攻防案例请参考……

视频资料：www.ichunqiu.com

Thanks & Join us

360UNICORNTEAM