KCon 2017 洞见未来

KCon

玩转无人机攻防

Kevin2600

- Twitter: @Kevin2600
- Github: https://github.com/kevin2600
- 狗汪汪系列: 玩转无线电-不安全的蓝牙锁; 玩转嵌入式-I2C 协议分析; 玩转嵌入式-WINKHUB 边信道;
  玩转无线电-GPS Hacking; 玩转无线电-温哥华天车 RFID 票务系统 ...

议程:

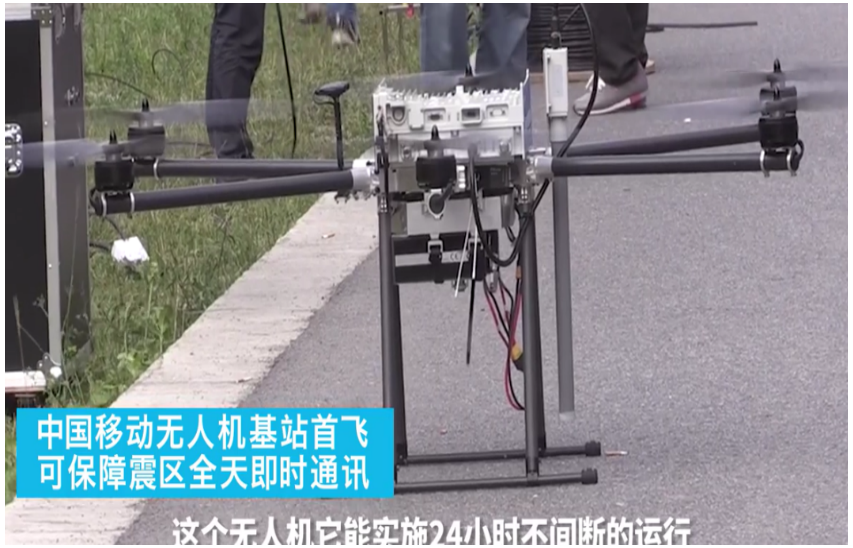
- 无人机攻防那点事
- 无人机攻防案例篇
- 无人机攻防实战篇
- 无人机攻防科幻篇

无人机攻防那点事

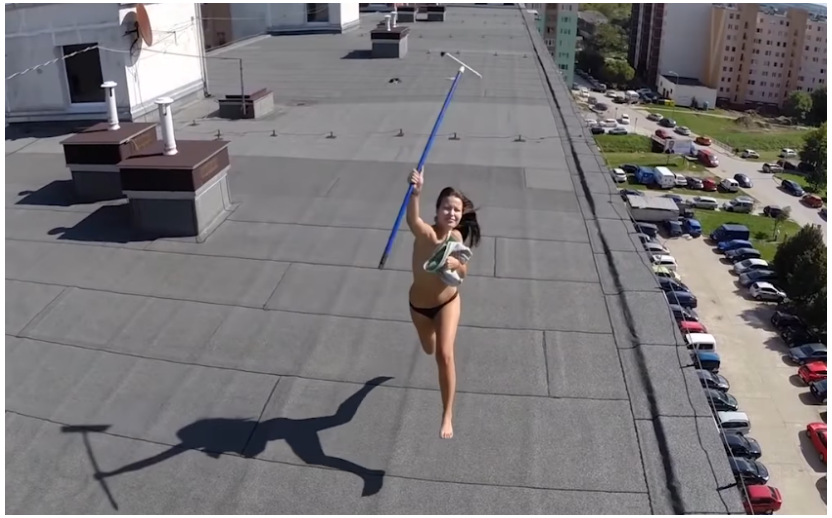
无人机世界百家齐放

- 无人机厂商众多 (DJI; Parrot; Xiaomi; DIYer...)
- 无人机运用场景广泛 (航拍; 运输; 求婚; 应急反应...)
- 无人机遥控种类繁多 (RF; WIFI; XBEE; 开源 & 私有协议...)





无人机侵犯隐私？



无人机扰航频发 昆明机场严禁 “黑飞”

2017-05-02 17:32:50　　来源：中国新闻网　　作者：　　字号：T T

　　核心提示：昆明机场呼吁，民众应自觉遵守国家及地区相关法律法规，主动避免出现在机场净空保护区范围内放飞无人机、风筝等影响飞行安全的升空物体，确保昆明机场的净空安全。民众如发现上述行为，积极向昆明机场反映

广州男子登山时用 “黑飞” 无人机拍军队营地 被拘7日

2017-05-05 09:00:57　　来源：大洋网　　作者：　　字号：T

　　核心提示：因黄某出于好玩好奇之心航拍部队营区，且航拍资料没有外传，未造成严重后果，根据《中华人民共和国治安管理处罚法》的规定，依法对黄某作出行政拘留七天处罚。

无人机走私犯罪？

无人机攻防现状？

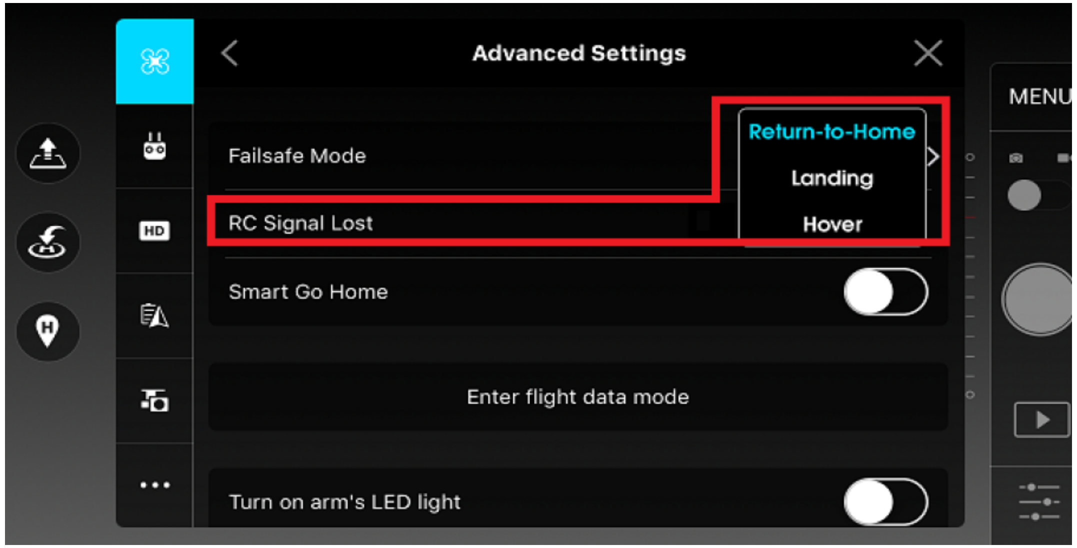
- DARPA 举行无人机攻防比赛 (禁止使用GPS-欺骗)

- 花样百出的防御方式: 视频; 音频; WIFI; 红外; 无线电 ...

- 千奇百怪的攻击方式: 老鹰; WI-FI 攻击; 超声波干扰; 电磁波干扰 ...

无人机攻防现状！

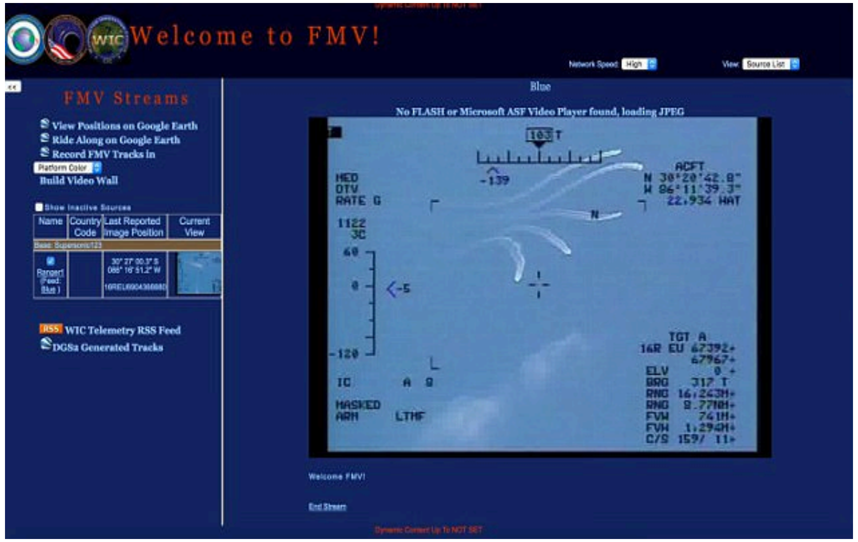
- GPS 欺骗攻击效果各异 (DJI 精灵3S 禁飞区 & 启始返航)
- 防御设备价格高昂, 不适合普通民众 (每只老鹰 1年开销 6922 $)
- 电磁波枪覆盖范围有限, 切断遥控信号后反应各异 (降落; 悬停; 返航)

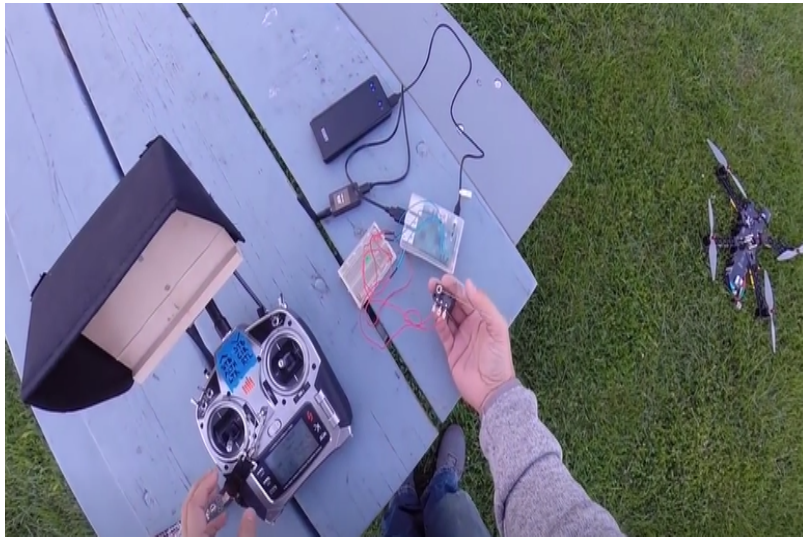


无人机攻防案例篇

无人机安全漏洞？

- 无人机安全漏洞 (捕食者; AR-Drone 2.0; 大疆精灵3S ...)
- 无人机攻击点 (WIFI; GPS 信号; 固件; 遥控器; 手机APP; 飞控协议; 摄像视频 ...)
- 无人机安全漏洞类型 (WIFI 空密码; GOT ROOT; 飞控指令无认证; 航拍视频无加密 ...)

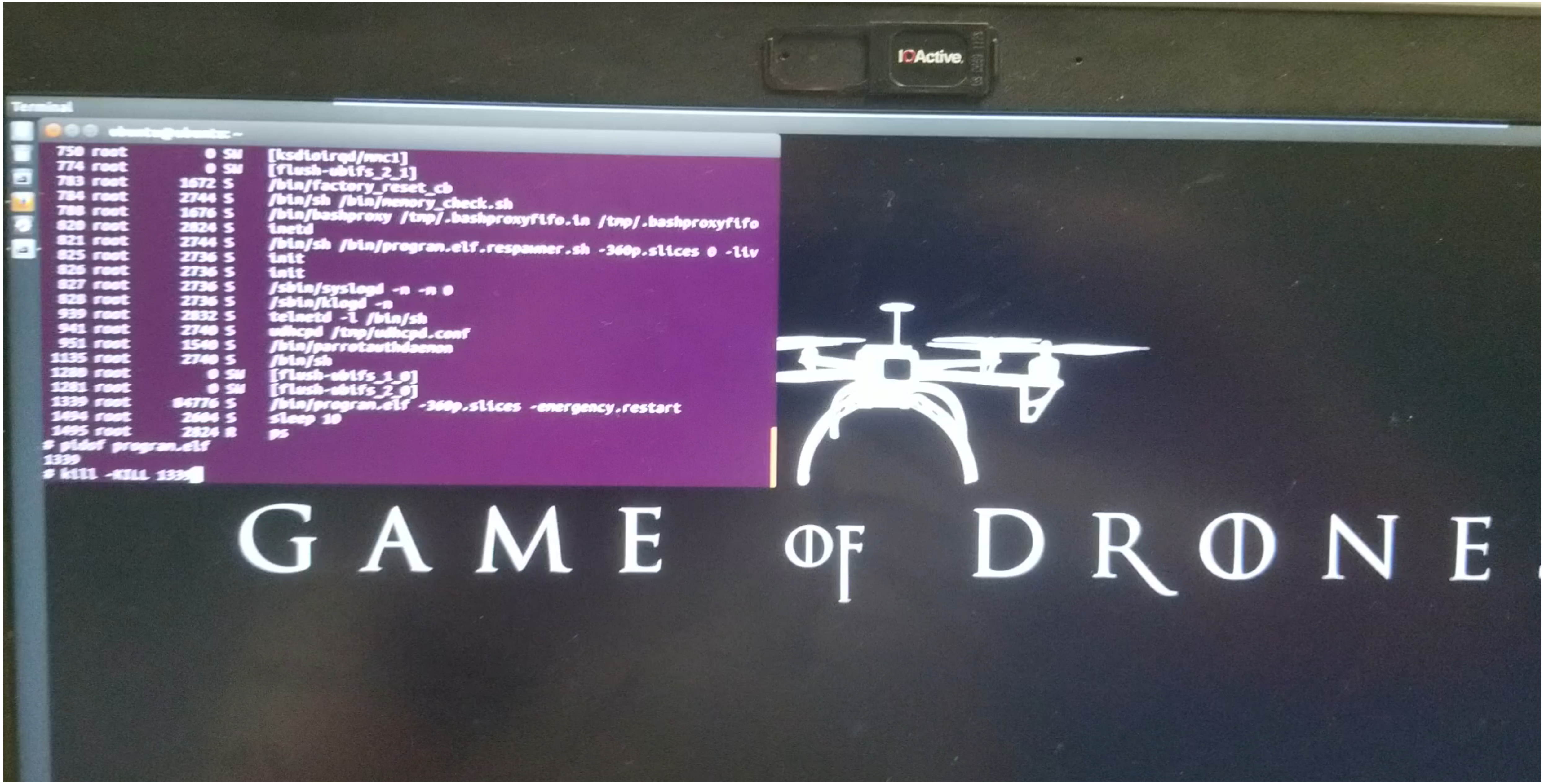




案例: Parrot AR Drone 2.0

- AR Drone 2.0 提供WIFI 热点 (无口令保护)
- 研究无人机安全必备 Linux on ARM (**SkyJack** 劫持; **Maldrone** 病毒..)
- 默认提供 **Telnet Root** 访问权限. 通过 Pairing 模式来保证安全 (MAC 地址)
- kill –KILL “pidof **program.elf**”

DEMO


IOActive
Terminal
750 root 0 SW [ksdioirqd/mmc1]
774 root 0 SW [flush-ubifs_2_1]
783 root 1672 S /bin/factory_reset_cb
784 root 2744 S /bin/sh /bin/memory_check.sh
788 root 1676 S /bin/bashproxy /tmp/.bashproxyfifo.in /tmp/.bashproxyfifo
820 root 2824 S inetd
821 root 2744 S /bin/sh /bin/program.elf.respawner.sh -360p.slices 0 -liv
825 root 2736 S init
826 root 2736 S init
827 root 2736 S /sbin/syslogd -n -m 0
828 root 2736 S /sbin/klogd -n
939 root 2832 S telnetd -l /bin/sh
941 root 2740 S udhcpd /tmp/udhcpd.conf
951 root 1540 S /bin/parrotauthdaemon
1135 root 2740 S /bin/sh
1280 root 0 SW [flush-ubifs_1_0]
1281 root 0 SW [flush-ubifs_2_0]
1339 root 84776 S /bin/program.elf -360p.slices -emergency.restart
1494 root 2604 S sleep 10
1495 root 2824 R ps
pidof program.elf
1339
kill -KILL 1339
GAME OF DRONE

案例: DBPOWER U818A-WIFI

- U818A 提供WIFI 热点 (无口令保护)
- U818A 基于 BusyBox 1.20.2 (潜在其它 BusyBox 隐患?)
- **CVE-2017-3209** (未知 FTP server 允许匿名账号任意文件访问, 照片视频等)
- “curl -T shadow ftp://192.168.0.1:21/etc/jffs2/shadow”

案例: Parrot Bebop2

- Bebop2 基于 Android 系统. 提供TELNET, FTP, UART Root 访问
- 当Bebop2 接收到大量WIFI连接请求，将无法处理请求包并坠机
- 当Bebop2 接收到超大数据包，Buffer将无法处理超额数据包并坠机

案例: Mavlink 开源协议

- 适用于接受遥控; GPS; 飞行时速等信息 (AR.Drone; ArduPilot ..)
- 各地面站(GCS) 可同时操控 255 架无人机 (Intel 的 500 架无人机 Show, 劫持攻击?)
- Fuzzing 环境配置: SCAPY or KITTY + Test cases (ERROR : Floating point exception)
- Fuzzing 环境配置: 架设虚拟无人机及虚拟地面站环境 (SITL Simulator; MAVProxy; Wireshark)

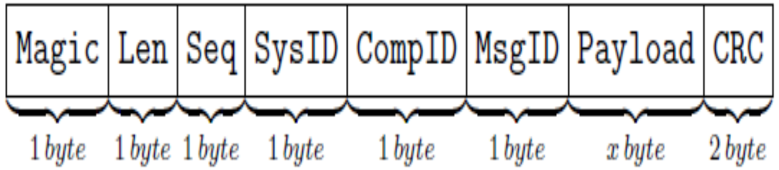
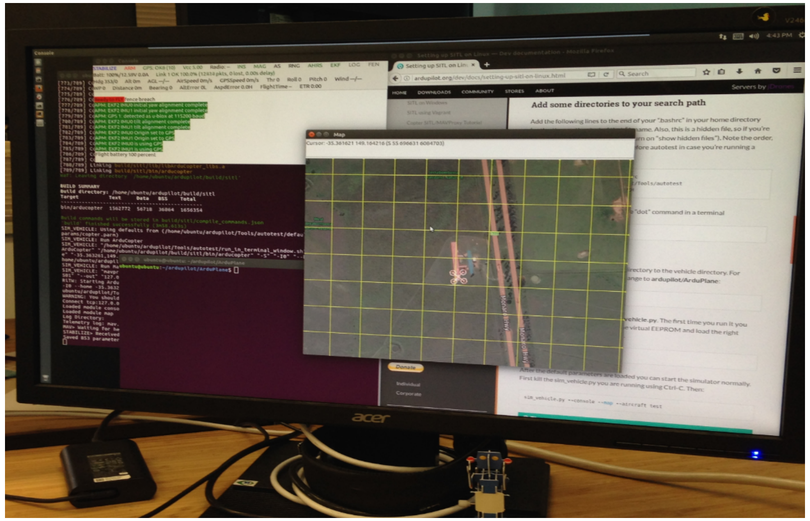


Figure 1: MAVLink packet structure



案例: DJI 大疆无人机系列

- 大疆精灵3 无人机易被 GPS 欺骗 (flyforbid.json)
- 大疆精灵3 遥控器 & 无人机 WIFI Probing (MAC: 60:60:1F)
- 大疆精灵3 Sniffer: github.com/a232319779/PHANTOM-3-STANDARD
- 大疆精灵3 RF 劫持 Geekpwn 2015 (315晚会报道的无人机是怎么被劫持的?)

ENTER VENDOR NAME

dji [lookup vendor]

SELECT LOOKUP TYPE: ○ LOOKUP MAC ◉ LOOKUP VENDOR

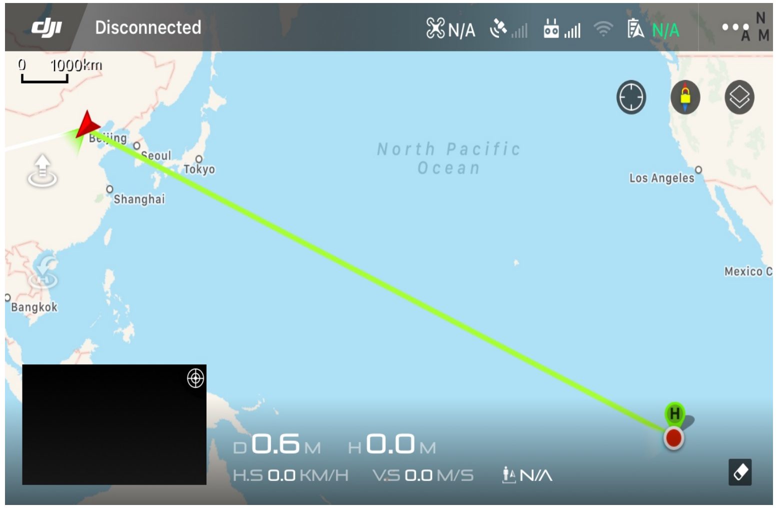
example: 00:0B:14

This database was last updated on 3 March 2017

Results for Vendor search dji

Found 1 results.

MAC Address/OUI	Vendor {Company}
60:60:1F	SZ DJI TECHNOLOGY CO.,LTD



案例: DJI 大疆无人机系列

Security Analysis of DJI Phantom 3 Standard

Fernando Trujano, Benjamin Chan, Greg Beams, Reece Rivera

May 11, 2016


```
{
    "groupName": "SkyWifi",
    "weight": 20,
    "isCameraGroup": false,
    "isSingleFile": true,
    "upgradeMode": 0,
    "devices": ["0700"],
    "ftpDstFileName": "HG310.bin",
    "ftpPwd": "Big~9China",
    "ftpUrl": "192.168.1.2",
    "ftpUsername": "root",
    "pushDevice": 7
},
```


```java
public static String a(String arg2) {
    String v0_1;
    Class v1 = b.class;
    __monitor_enter(v1);
    try {
        v0_1 = b.a(arg2, "你破解，我加固，求别互相伤害");
    }
    catch(Throwable v0) {
        __monitor_exit(v1);
        throw v0;
    }

    __monitor_exit(v1);
    return v0_1;
}
```

dji_rev	This repository contains tools for reverse engineering DJI product firmware images.
deejayeye-modder	APK "tweaks" for settings & "mods" for additional / altered functionality
pyduml	PyDUML allows you to send firmware to your DJI aircraft without using DJI assistant, or get root access using fireworks.tar
RedHerring	RedHerring was the initial July 4th Independence Day exploit to get root access to DJI aircraft
dji_system.bin	Archive of bin files for to allow you to upgrade/downgrade using other tools provided here
firm_cache	Individual module components from within bin files for analysis, or to allow creating custom packages using individual components
DUMLrub	Ruby port of PyDUML, and firmware cherry picking tool. Make your own custom firmware images.
DUMLdore	Windows version of the DUML firmware tools. Archive, and flash bin from windows
DJI_ftpd_aes_unscramble	DJI has modified the GPL Busybox ftpd on Mavic, Spark, & Inspire 2 to include AES scrambling of downloaded files... this tool will reverse the scrambling

```
channel : 78,   preamble : AA,   address : B1D30F431F,   payload length : 32,    pid : 2,       no_ack : 0,     payload : 1F430FD302000420150
108400002108000080800000000000000000000000032,   crc : C817
! : 10000000.000000ms may be the period.
channel number : 79       channel frequency : 5804000000
channel number : 80       channel frequency : 5805000000
```

```
channel : 13,   pk_count : 2,   preamble : AA,   address : F2EEE12220,   payload length : 32,    pid : 3,       no_ack : 0,   payload :
 2022E1EE03CB0D64F7AFEDCEBBA28466E30FEDCFB7E28464F38FEDCFB3E2848D,       crc : B728
channel : 13,   pk_count : 3,   preamble : AA,   address : F2EEE12220,   payload length : 32,    pid : 3,       no_ack : 0,   payload :
 2022E1EE03D00D47F98497C4D9A80245ED2497C5D5E80247FDA497C5D1E80284,       crc : D77C
end.
```

DEMO

无人机攻防实战篇

目标: CX-10WD

- 适宜无人机逆向入门 CX-10 系列 (WIFI; RF; 视频图传)
- 遥控操作分为 4 个频道, 工作在频率 2.4Ghz 范围
- 遥控最远距离为 WIFI 可达 40 米, RF 可达 15 米 (室内飞行)

CX-10WD 情报收集

- 无人机工作频率 (900mhz ? 2.4ghz ? 5.8ghz ?)
- 无人机采用何种无线模块 (芯片? GFSK ? 数率 ?)
- 无人机工作模式 (有无跳频 ? 有无加密 ? 数据包结构 ?)

CX-10WD 工作频率

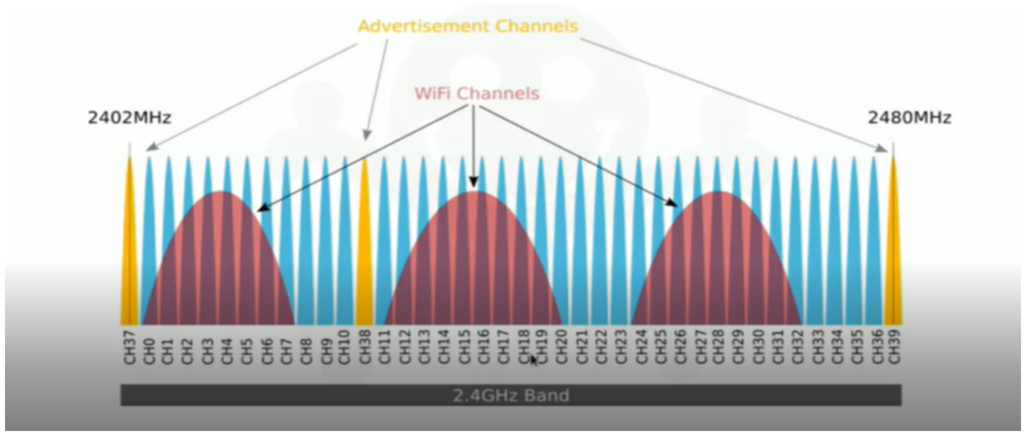
- FCCID 数据查询
- 芯片类型文档阅读
- SDR 软件无线电侦测

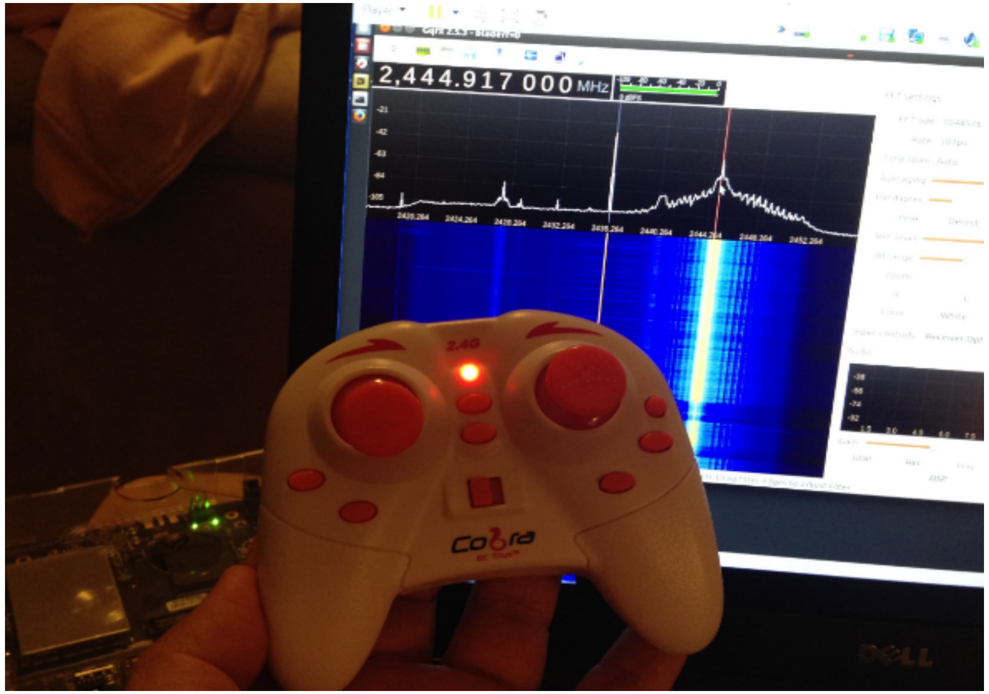
XN297L 系列产品说明书

2.4GHz 单片高速无线收发芯片

概 述

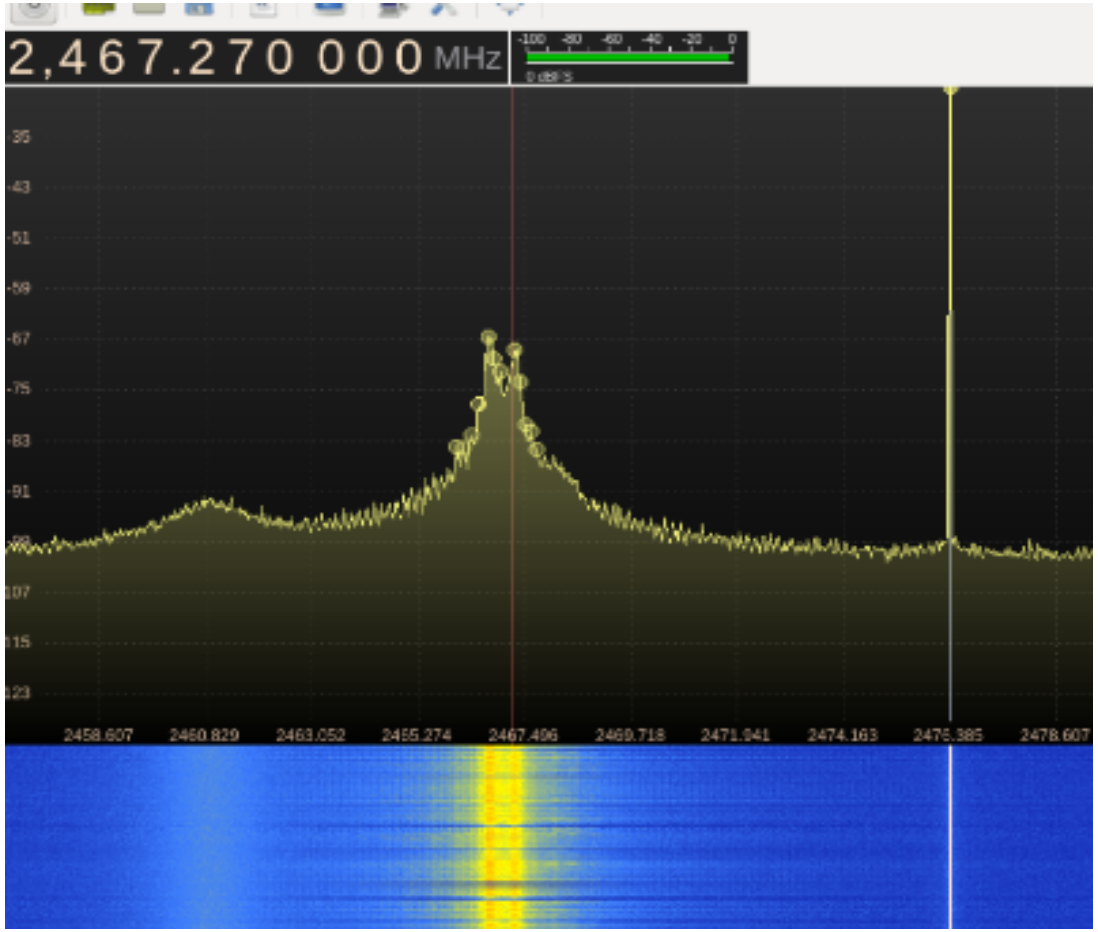
XN297L系列芯片是工作在2.400~2.483GHz世界通用ISM频段的单片无线收
该芯片集成射频收发机、频率发生器、晶体振荡器、调制解调器等功能模块，并且
多组网和带ACK的通信模式。发射输出功率、工作频道以及通信数据率均可配置。



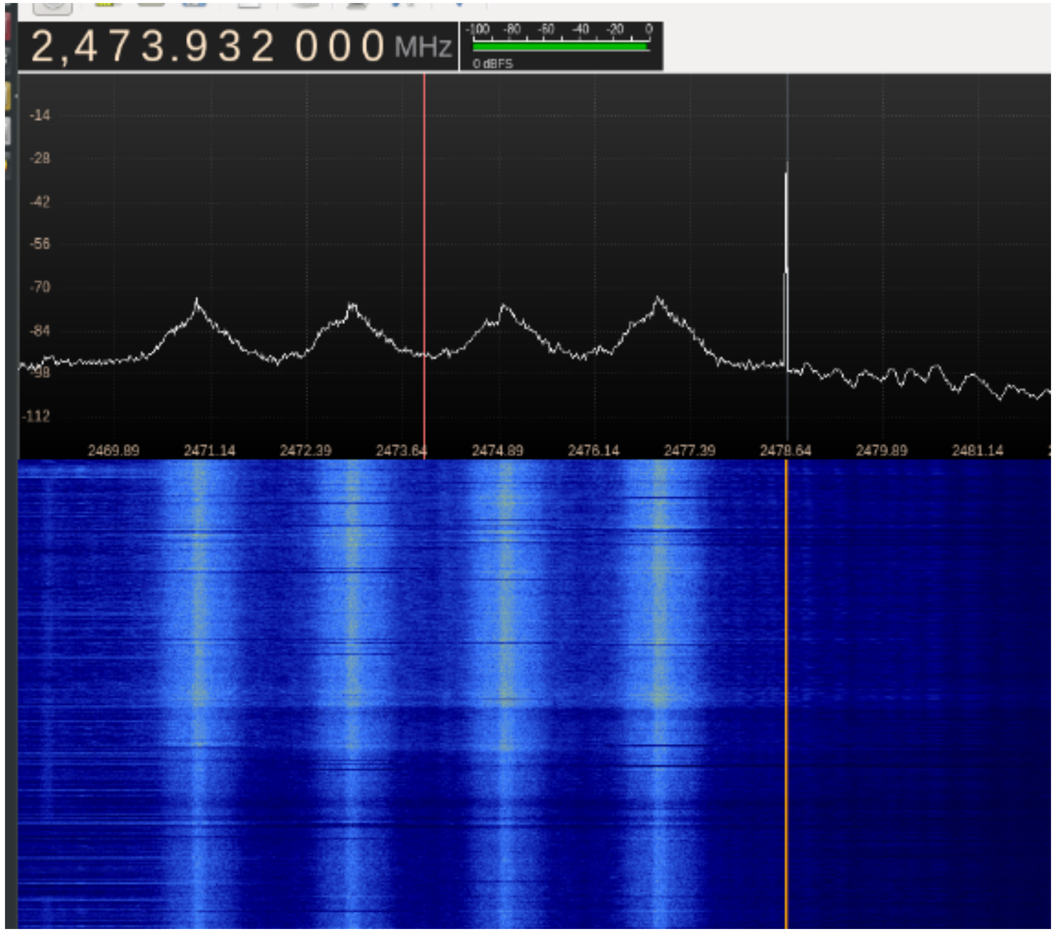


CX-10WD 工作频率

绑定信号

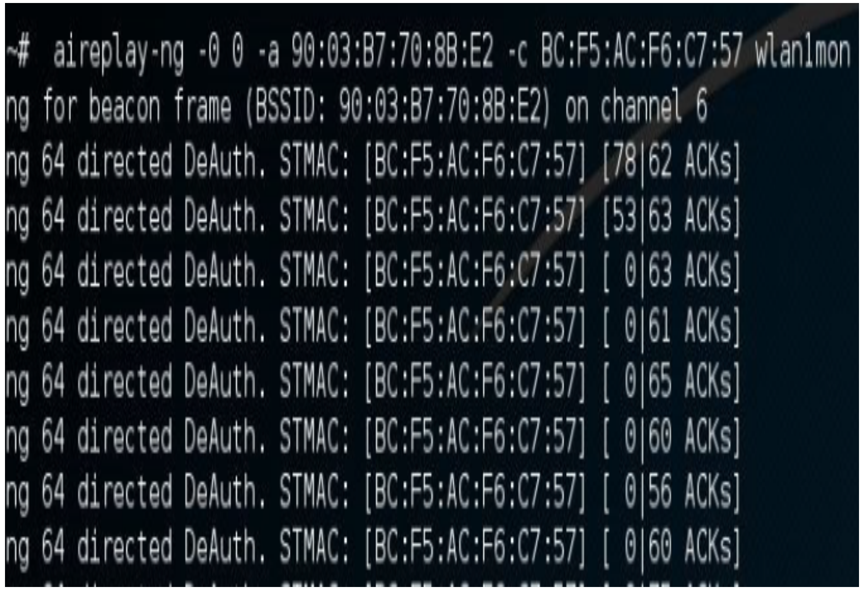


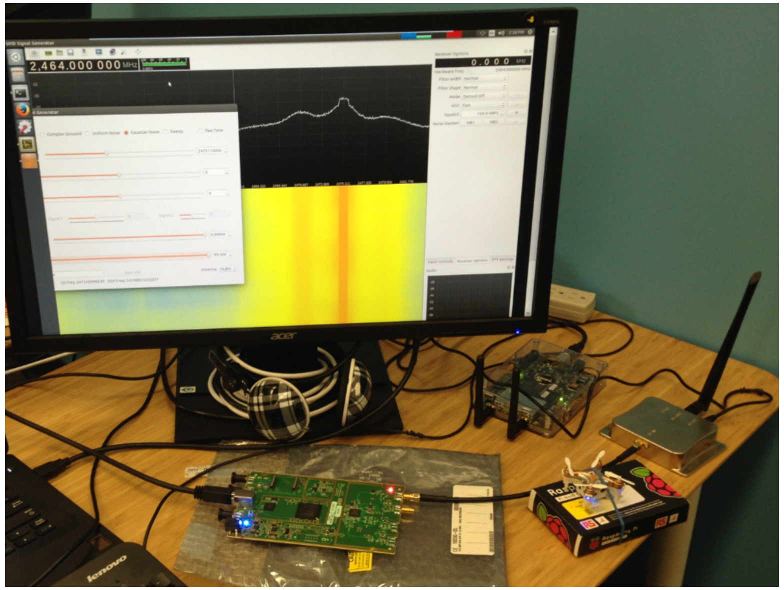
遥控信号



CX-10WD – 干扰攻击

- 最暴力的攻击方式: WIFI Deauth 攻击 (AirCrack-ng 依旧王道)
- 最暴力的攻击方式: 高功率信号放大器 + 2.4ghz 高斯噪音 (SDR 无线 Hacking 必备)



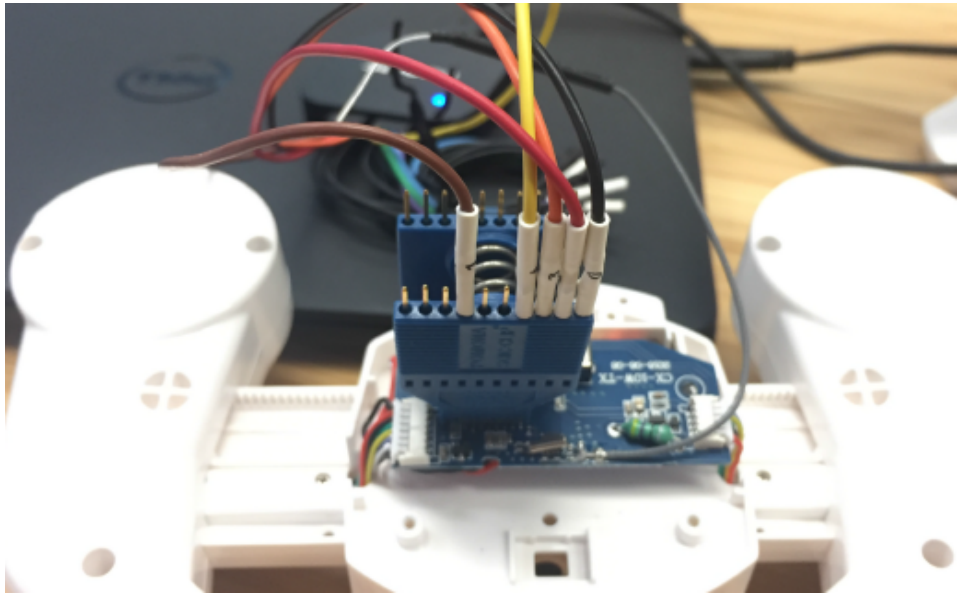


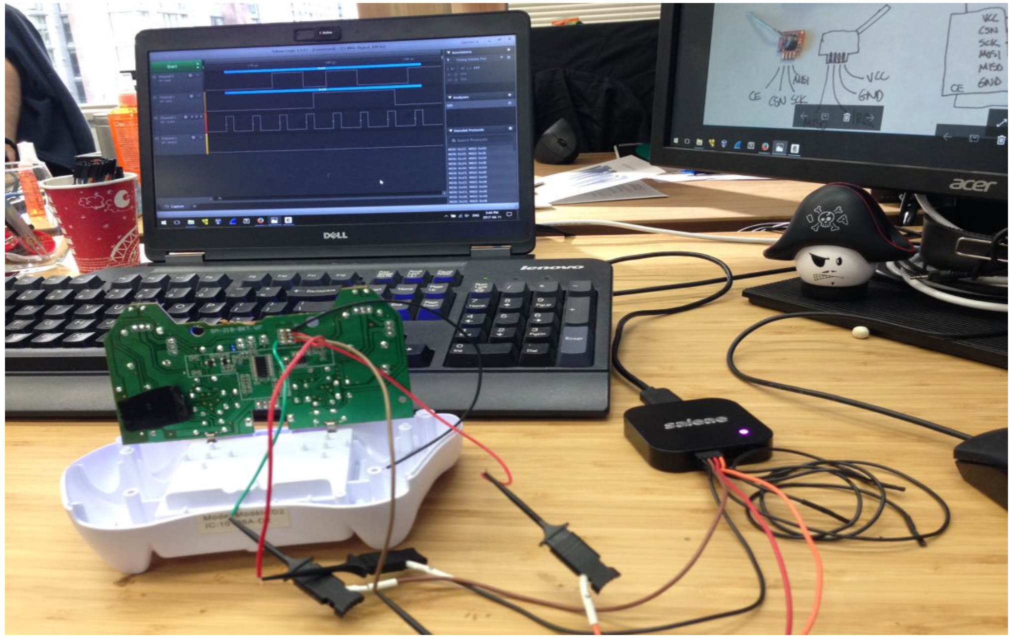
CX-10WD – 协议逆向

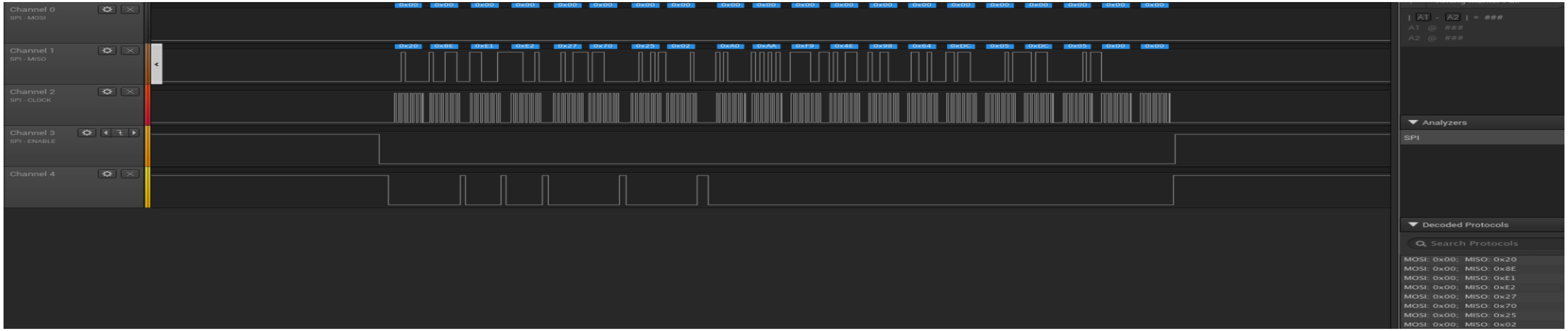
其它特性

四线 SPI 接口通信	SPI 接口速率最高支持4Mbps
支持最大数据长度为32字节（两级FIFO） 或者 64字节（单级FIFO）	QFN20L0303 / SOP16 / SOP8封装
1M / 2Mbps模式，需要晶振精度 ±40ppm 250kbps模式，需要晶振精度 ±20ppm	工作电压支持2.2~3.3V 工作温度支持-40~+85℃
GFSK通信方式	支持自动应答及自动重传
支持RSSI检测功能	带自动扰码和CRC校验功能

CX-10WD – 协议逆向






Channel 0
SPI - MOSI
Channel 1
SPI - MISO
Channel 2
SPI - CLOCK
Channel 3
SPI - ENABLE
Channel 4
Analyzers
SPI
Decoded Protocols
Search Protocols
MOSI: 0x00; MISO: 0x20
MOSI: 0x00; MISO: 0x8E
MOSI: 0x00; MISO: 0xE1
MOSI: 0x00; MISO: 0xE2
MOSI: 0x00; MISO: 0x27
MOSI: 0x00; MISO: 0x70
MOSI: 0x00; MISO: 0x25
MOSI: 0x00; MISO: 0x02

CX-10WD – 协议逆向

XX: YY:ZZ:....:AA:....

Command name (1 byte)

Payload (0-64bytes)

R_REGISTER	000A AAAA	1 to 5 低字节在前	读状态寄存器 AAAAA=5bit 寄存器地址

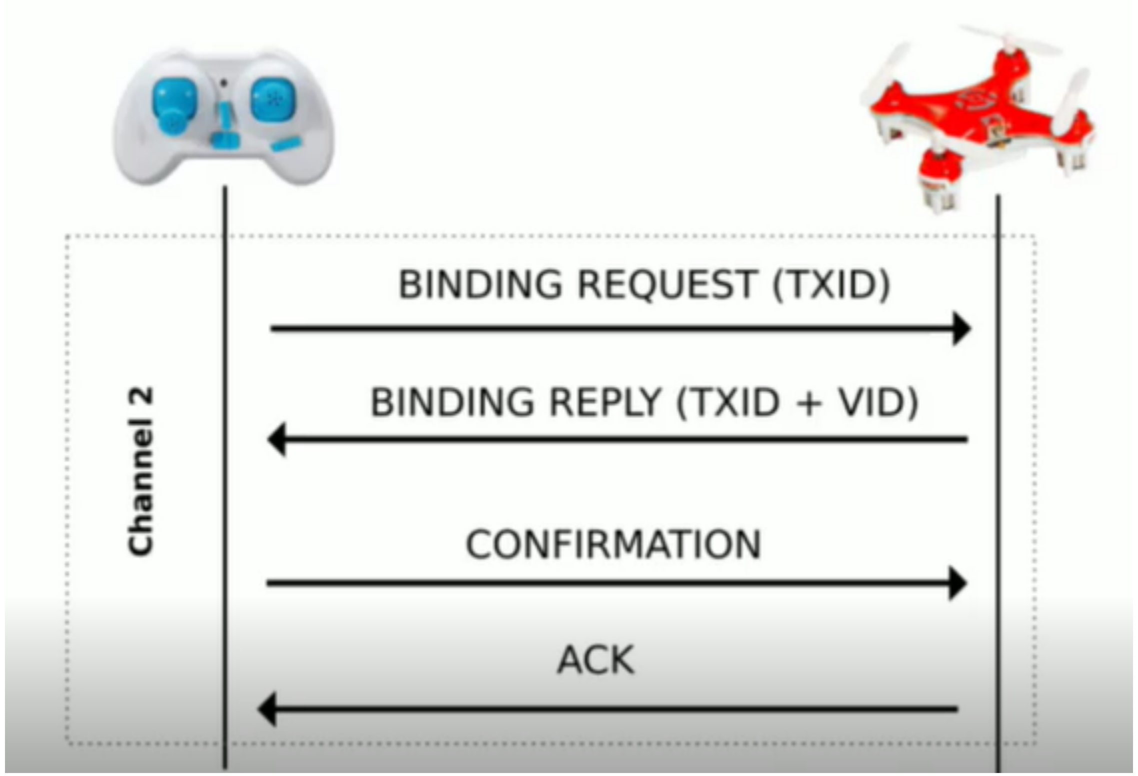
Register address (5 LSBits)

W_TX_PAYLOAD	1010 0000	1 to 32/64 低字节在前	写发射数据，写操作通常由 0 字节开始。

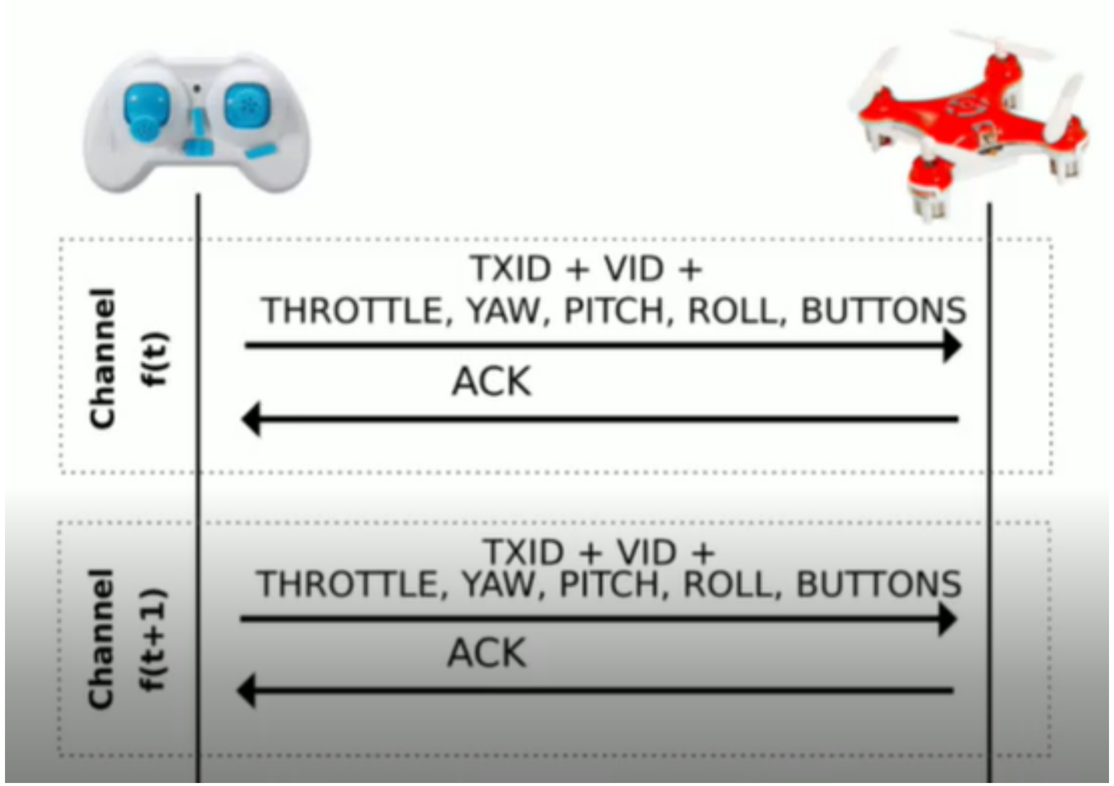
Payload (up to 64 bytes)

CX-10WD 攻击模式

正常模式



攻击模式

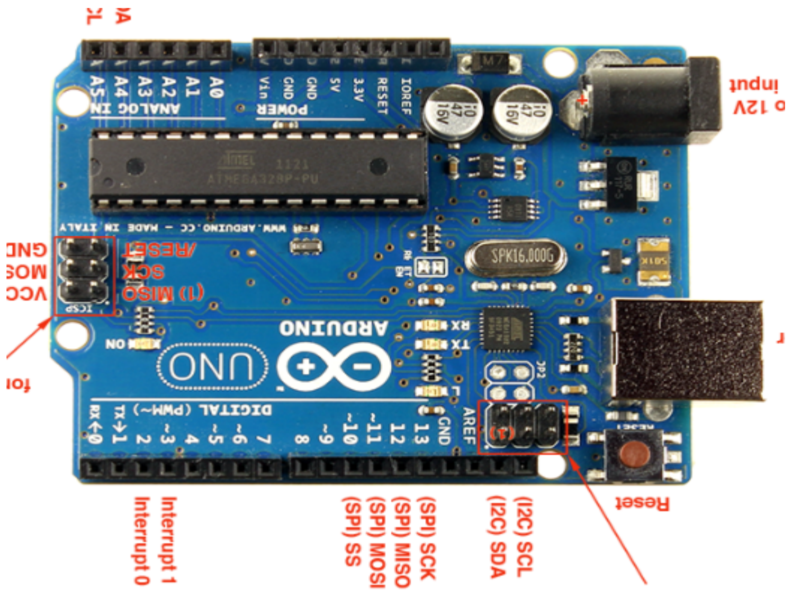


CX-10WD 攻击设备

NRF 24L01 无线模块

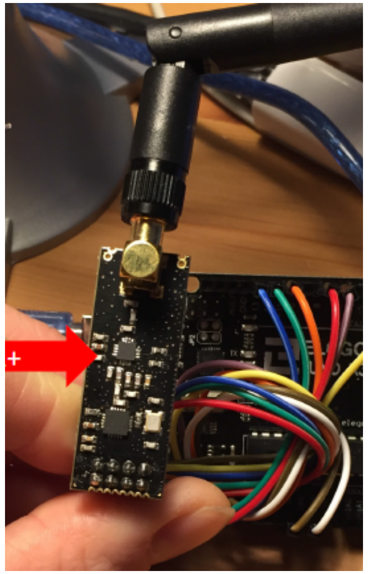
Arduino UNO 支持 SPI 传输

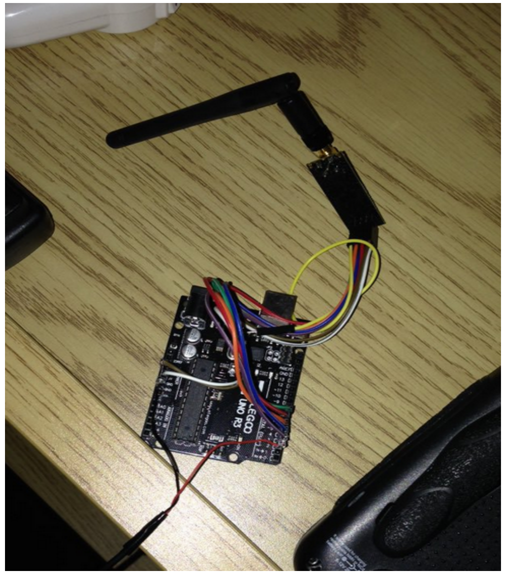
更快的发包率 + 以知的跳频算法



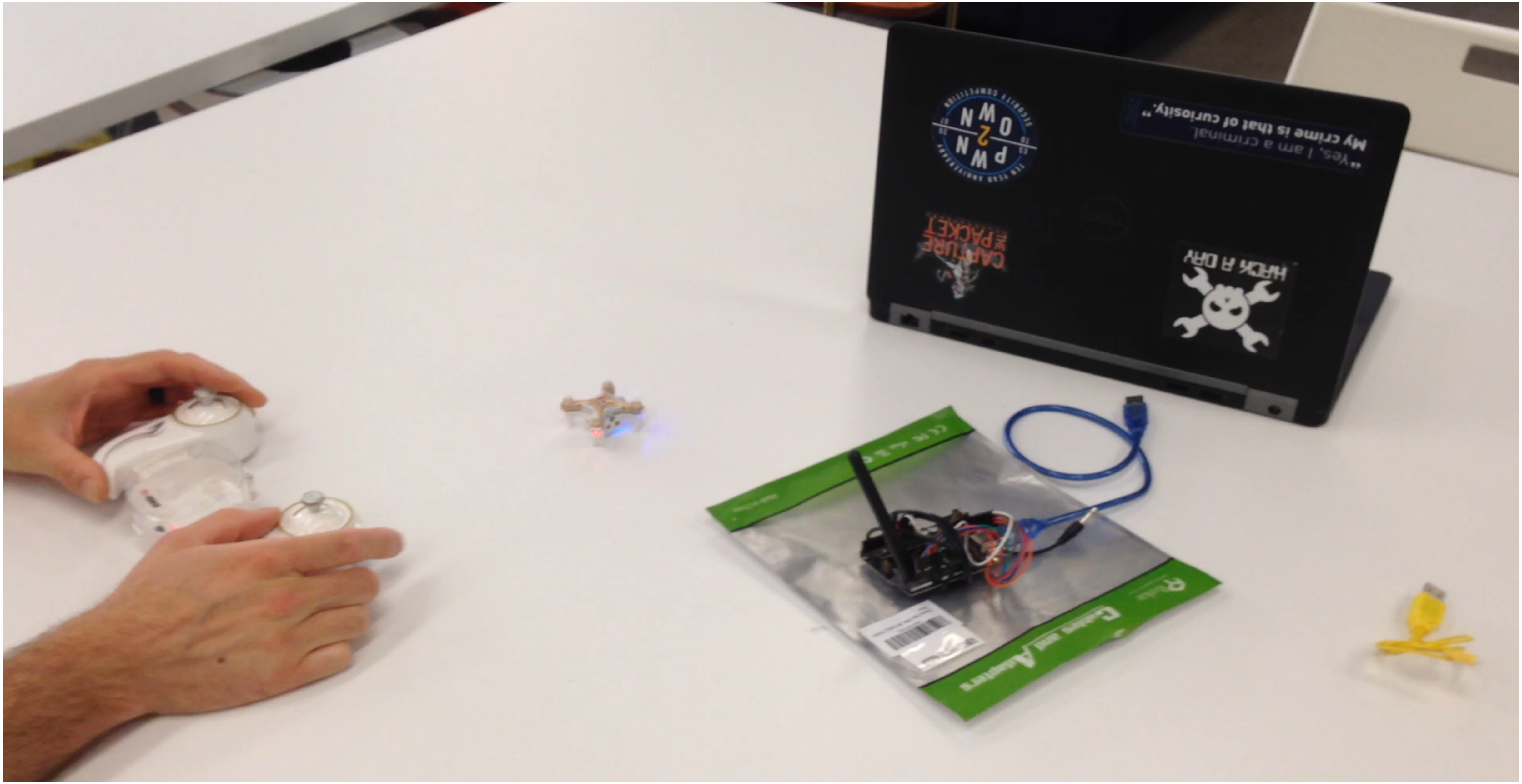
```
//########## Variables #################
static uint8_t aid[4]={0xFF,0xFF,0xFF,0xFF}; // aircraft ID
static uint8_t txid[4]; // transmitter ID
static uint8_t freq[4]; // frequency hopping table
static uint8_t packet[PACKET_LENGTH];
volatile uint16_t Servo_data[CHANNELS] = {0,};
int ledPin = 13;

void setup() {
    randomSeed((analogRead(A0) & 0x1F) | (analogRead(A1) << 5));
    for(uint8_t i=0;i<4;i++) {
        txid[i] = random();
    }
    txid[1] %= 0x30;
```



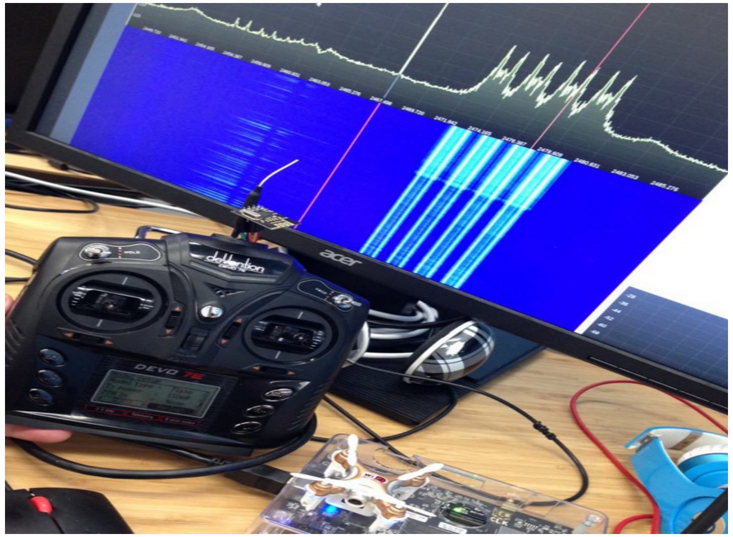


DEMO


PWN2OWN
"Yes, I am a criminal.
My crime is that of curiosity."
CAPTURE THE PACKET
HACK A DAY

CX-10WD – 刷新固件

- 比 Arduino + NRF24 模块更好的劫持方案？
- 无人机世界的瑞士军刀 DeviationTX 固件项目
- 改造加载多款无线硬件模块, 同时支持多款无线协议 (遥控器 DEVO 7E)



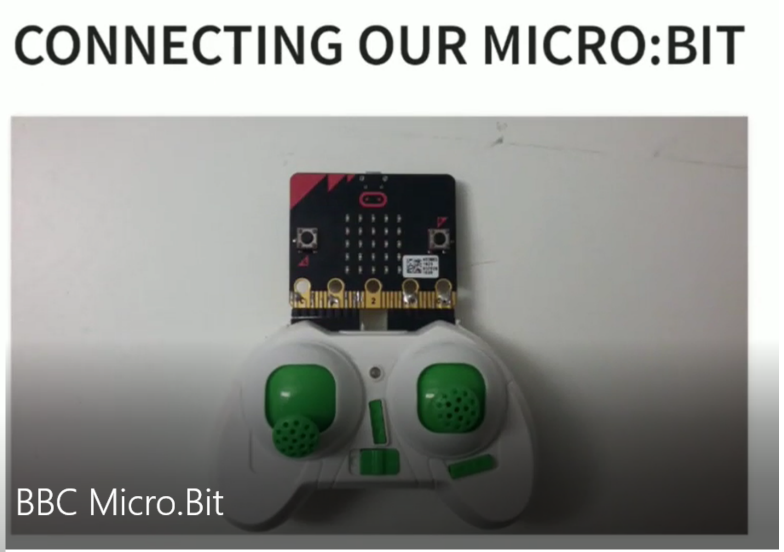
CX-10WD – 刷新固件

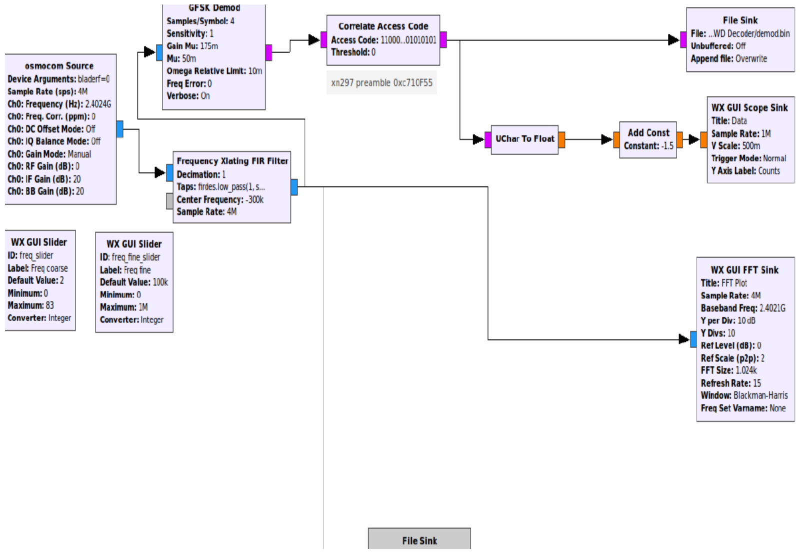

CYRF 6936
CC2500
A7105
nRF24L01
protocols
• Specktrum : DSM2/DSMX
• Walkera
protocols
• FrSky (D8/D16)
protocols
• FlySky
• Hubsan
protocols
• V2x2
• YD717
• SYMA
• HiSky
• Cheerson

DEMO

其它玩法

- 玩法众多: MicroBIT; Devo7E; 树莓派; 软件无线电 ...
- 还有更高大上的么? 😌

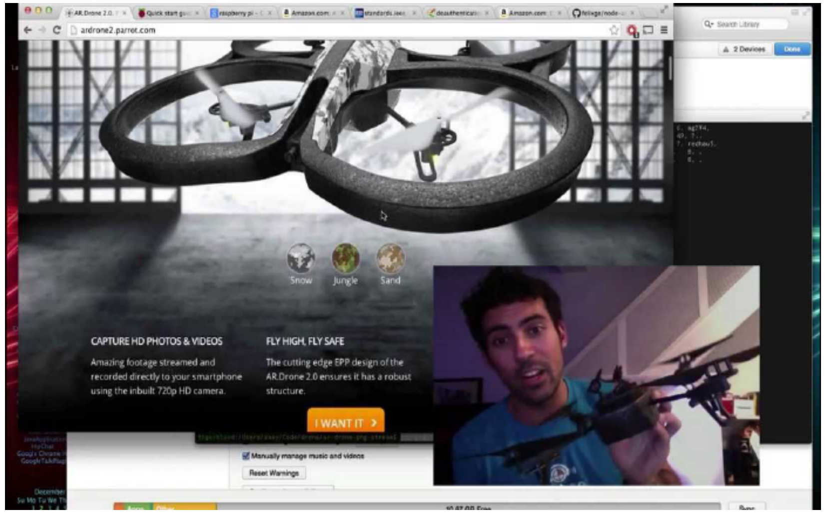




无人机攻防科幻篇

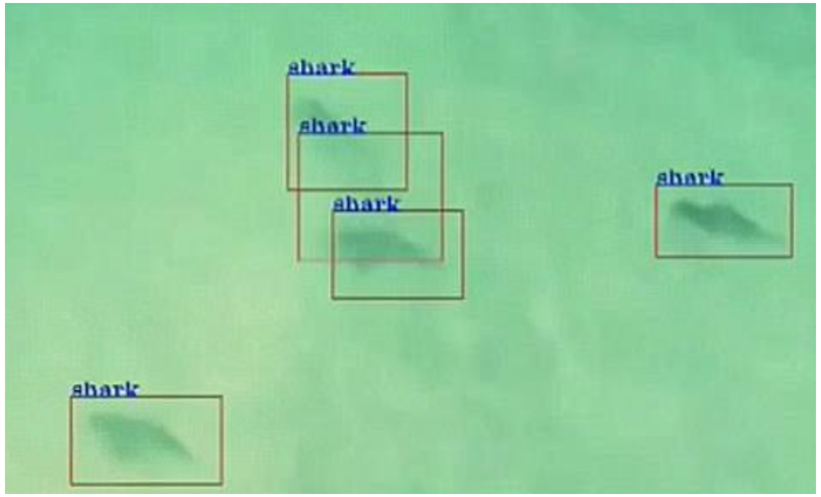
无人机 vs 无人机

- 无人机攻防, 最佳的防守是否就是攻击？
- 东京警方采用无人机&渔网的方式对违规无人机进行围捕
- Skyjack 项目 (AR.Drone + 树莓派) && Hack5 项目 (DJI3S + WIFI大菠萝)



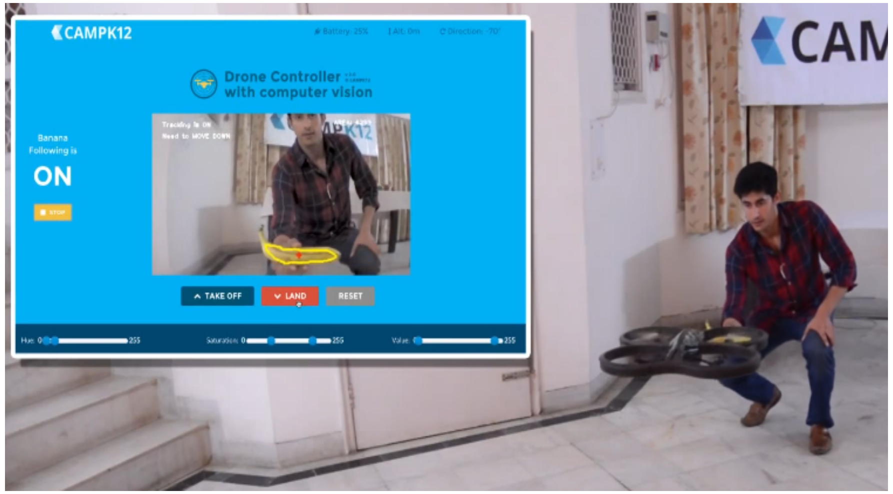
无人机 vs 人工智能

- 微软研究通过机器学习与无人机自动驾驶结合 (无人机安保系统)
- 澳洲采用无人机与图像识别技术监控鲨鱼攻击事件 (海岸救生员)
- 卡耐基大学AI 实验室通过机器学习研究无人机自动规避技术 (空中巴士)



无人机 Skynet 雏形？

- AR.Drone 物体追踪 (ardronelabviewtoolkit.wordpress.com)
- NVIDIA Jetson TX 系列: 无人机自动分类识别的大脑
- 未来人工智能无人机攻防系统: 自动巡逻 + 敌我识别 + 主动攻击



DEMO

总结:

- Kein System Ist Sicher: 100% 安全的系统并不存在
- 无人机安全研究与其他嵌入式无线产品大同小异
- 无人设备与人工智能相结合是未来趋势 (安全性能如何?)