KCon 洞见未来 2017

KCon

如何DIY一套低成本反无人机系统

qingxp9

whoami

杨芸菲 @qingxp9

360 PegasusTeam 无线安全研究员

WLAN安全研究、WIPS等无线安全产品研发

东北大学无线安全课程客座讲师

C-SEC 《如今我们面临的无线威胁》

CCF YOCSEF沈阳《公共无线安全的现状与未来》

“绵羊墙”公共WiFi风险演示系统

Outline

① 无人机安全威胁背景

② 基于802.11的反无人机方案

③ 低成本反无人机系统的设计与实现

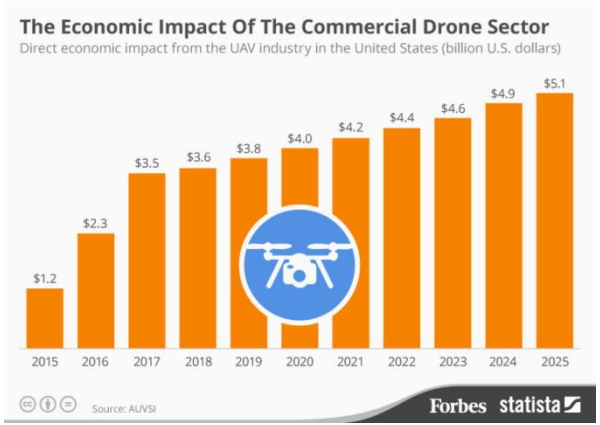
④ 承载在802.11上的无人机管控方案

无人机安全威胁

近年来，无人机应用范围越来越广泛（航拍、快递、灾后搜救、数据采集），无人机数量迅速增加，随之也产生了一系列安全管控问题。

未经许可闯入敏感区域、意外坠落、影响客机正常起降、碰撞高层建筑等事件不断发生。

向各国政府提出了新的监管命题。



无人机安全威胁

个人隐私

无人机安全威胁

军事安全

ISIS改装无人机用于投放炸弹

无人机安全威胁

民航安全

成都双流机场无人机事件:

从4月14日至4月27日，双流机场接连发生8件无人机扰航事件，总计造成114个航班备降、超过40个航班延误、4架飞机返航、超1万旅客出行受阻被滞留机场，严重威胁民航飞行安全。

Unauthorised drone causes delay at Queenstown Airport | Stuff.co.nz
www.stuff.co.nz/.../unauthorised-drone-causes-delay-at-queenstown-airport - 翻译此页
2016年8月17日 - An unauthorised drone flight caused delays at Queenstown Airport. ... According to civil aviation rules, UAVs must not be flown within four ...

英国反无人飞行器防御系统(AUDS)

Blighter Surveillance Systems

CHESS DYNAMICS

Enterprise Control Systems Ltd

AUDS system combines electronic-scanning radar target detection, electro-optical (EO) tracking/classification and directional RF inhibition capability.

三家公司各自的系统分别在雷达探测、影像/视频跟踪和射频干扰/数据通信方面达到了行业最佳水平。

核心技术：

1.Ku波段（12GHz到18GHz）电子扫描防空雷达技术

a. 支持检测距离：10KM
b. 支持检测0.01平方米大小设备
c. 结合多普勒检测

2.高精度水平和倾斜方位指示器

a. 动态方位定位器、热感摄像机进行目标识别
b. 视频追踪

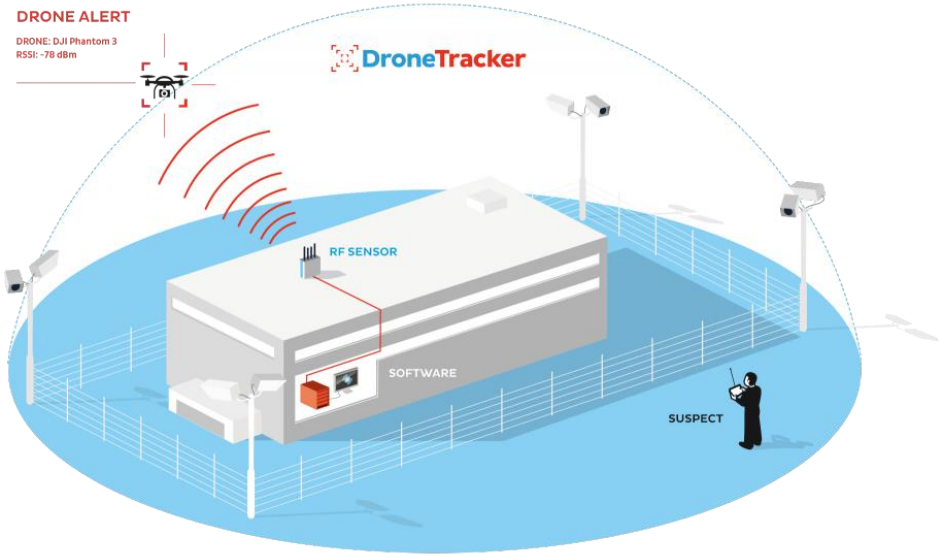
3.智能定向射频抑制干扰系统

a. 高增益四频五天线
b. 自定义抑制波形、支持GNSS频率
c. 软件定义智能射频抑制

可实现15秒内探测、跟踪和干扰无人机

DroneTracker

- 红外线
- 视图
- 音频
- 雷达
- Wi-Fi
- RF
- …



DroneTracker：
identification and counter-measures platform to defeat drone
http://www.dedrone.com/en/dronetracker/drone-protection-software

捕获方案

1. 肩扛式反无人机装置

厂商：俄罗斯 SkyWall100

干扰方式：发射捕捉导弹

2. 日本用无人机捕捉无人机

厂商：日本a

干扰方式：发现无人机通过捕捉网进行捕获

3. 老鹰捉小“机”

厂商：荷兰 Guard from Above

干扰方式：发现后直接捕捉

4. 声波干扰

厂商：韩国先进科学技术研究院(KAIST)

干扰方式：利用声波使无人机陀螺仪发生共振，输出错误信息

检测与干扰 总结

1. 检测识别

a. 无线频段监测：2.4GHz、5.8GHz、1.5GHz（不同国家频段不同）
b. GPS监测
c. 图像识别：相机、红外相机
d. 音频识别
e. 超声波+雷达

2. 干扰拦截：包括毁伤技术、干扰技术、伪装欺骗技术

a. 干扰GPS系统
b. 中断控制器和无人机之间通信：命令控制隧道
c. 激光炮（暴力手段）
d. 劫持：GPS欺骗、无线控制链路劫持

无线电干扰攻击面

无人机使用无线电技术来实现定位、遥控、图像传输等功能。

Up-link

- 遥控信号。如果上行信号被干扰，无人机将失去即时控制，通常会降落或者悬停

Down-link

- 图传信号。事实上大多数民用无人机的遥控、图传需要双向通信才能正常工作，干扰其上行也可能使其下行无法正常工作。

GPS Signal

- 伪造禁飞区域的GPS信号，无人机会降落。

不建议使用GPS欺骗技术打击无人机

会严重干扰其他设备

- 干扰范围内有可能存在的移动通信基站、电网基础设施，军事设施等，都会受到影响
- 影响周围所有的手机、汽车导航定位等
- 若在机场附近，则会干扰飞机的导航系统

需要很大的干扰功率

- 当无人机距离较远时，需要很大的发射功率
- 无人机的GPS天线通常是朝向天空方向，从地面发射的GPS干扰信号对无人机的GPS接收天线影响较弱。导致需要更大的干扰功率

无线电干扰缺点

- 会影响其他无线电信号的正常通信

  无人机普遍采用跳频、扩频技术，具有一定的抗干扰能力。容易出现干死一大片，无人机照样飞的窘境

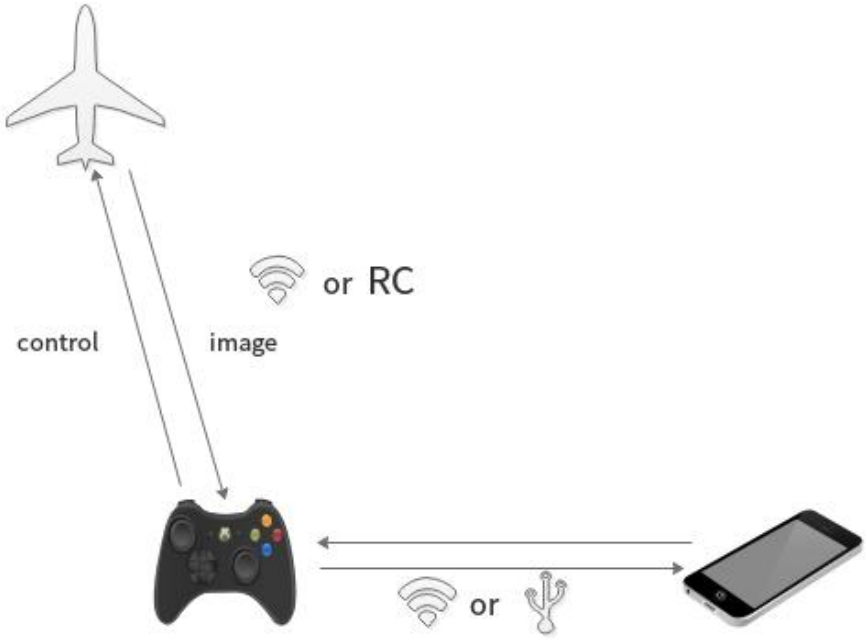
- 无线电信号干扰设备存在法律风险

《中华人民共和国刑法修正案（九）》第288条

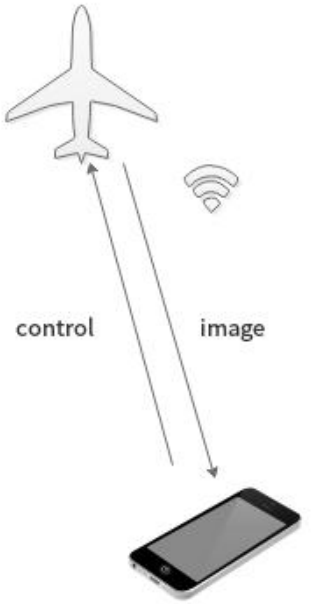
“违反国家规定，擅自设置、使用无线电台（站），或者擅自使用无线电频率，干扰无线电通讯秩序，情节严重的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。”

基于802.11的反无人机方案

拓扑



Aircraft--Controller--Phone



Aircraft--Phone

消费级无人机设备基本都使用了Wi-Fi在飞行器和手机间传输遥控、图传等信号。

Wi-Fi 特征

802.11 Beacon Frame

30	5.455065	SzDjiTec_25:95:bd	SzDjiTec_10:d7:46	802.11	141	QoS Da
31	5.455140		SzDjiTec_25:95:bd (…	802.11	40	Acknow
32	5.939464	SzDjiTec_25:95:bd	Broadcast	802.11	221	Beacon
33	6.042087	SzDjiTec_25:95:bd	Broadcast	802.11	221	Beacon
34	8.807052	SzDjiTec_25:95:bd	Broadcast	802.11	221	Beacon
35	8.909764	SzDjiTec_25:95:bd	Broadcast	802.11	221	Beacon
36	9.729072	SzDjiTec_25:95:bd	Broadcast	802.11	221	Beacon
37	9.751478	SzDjiTec_10:d7:46	SzDjiTec_25:95:bd	802.11	204	QoS Da
38	9.751553		SzDjiTec_10:d7:46 (…	802.11	40	Acknow
39	9.752352	SzDjiTec_25:95:bd	SzDjiTec_10:d7:46	802.11	141	QoS Da

```
+ Frame 32: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits) on interface 0
+ Radiotap Header v0, Length 30
- 802.11 radio information
    PHY type: 802.11b (4)
    Short preamble: False
    Data rate: 1.0 Mb/s
    Channel: 3
    Frequency: 2422 MHz
    Signal strength (dBm): -64 dBm
  + [Duration: 1720 us]
+ IEEE 802.11 Beacon frame, Flags: ........
- IEEE 802.11 wireless LAN management frame
  + Fixed parameters (12 bytes)
  - Tagged parameters (155 bytes)
    + Tag: SSID parameter set: PHANTOM3_2595bd
    + Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
```

Wi-Fi 特征

802.11 Probe Response Frame

26	7.382288	SzDjiTec_10:d7:46	Broadcast	802.11
27	7.383944	SzDjiTec_25:95:bd	SzDjiTec_10:d7:46	802.11
28	7.384125		SzDjiTec_25:95:bd (…	802.11
29	7.385867	SzDjiTec_25:95:bd	SzDjiTec_10:d7:46	802.11

```
me 27: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interfac
iotap Header v0, Length 30
.11 radio information
HY type: 802.11b (4)
hort preamble: False
ata rate: 1.0 Mb/s
hannel: 2
requency: 2417 MHz
ignal strength (dBm): -67 dBm
Duration: 1672 us]
802.11 Probe Response, Flags: ........
802.11 wireless LAN management frame
ixed parameters (12 bytes)
agged parameters (149 bytes)
Tag: SSID parameter set: PHANTOM3_2595bd
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
```

无人机型号

OUI	SSID	Drone Model
60:60:1f	PHANTOM3_xxxxxx	PHANTOM3
60:60:1f	Mavic-xxxxxx	MAVIC
e4:12:18	XPLORER_xxxxxx	XPLORER
	KONGYING-xxxxxx	KONGYING
	MiRC-xxxxxx	XiaoMi

OUI、SSID及型号对应关系

用于图像显示的操控者手机终端

操控者识别

No.	Time	Source	Destination	Protocol	Length	Info
52	20.448503	SzDjiTec_32:39:a1 (60…	QikuInte_9c:0c:39 (…	802.11	58	802.11 Block Ack, Flags=.....
53	20.451912		SzDjiTec_32:39:a1 (…	802.11	40	Clear-to-send, Flags=.....
54	20.452894	SzDjiTec_32:39:a1	QikuInte_9c:0c:39	802.11	1287	QoS Data, SN=49, FN=0, Flags=.p....F.
55	20.453006		SzDjiTec_32:39:a1 (…	802.11	40	Acknowledgement, Flags=.....
56	20.453242		SzDjiTec_32:39:a1 (…	802.11	40	Clear-to-send, Flags=.....
57	20.453481	SzDjiTec_32:39:a1	QikuInte_9c:0c:39	802.11	1287	QoS Data, SN=50, FN=0, Flags=.p....F.
58	20.453673	SzDjiTec_32:39:a1	QikuInte_9c:0c:39	802.11	1287	QoS Data, SN=51, FN=0, Flags=.p....F.
59	20.454239	SzDjiTec_32:39:a1	QikuInte_9c:0c:39	802.11	1287	QoS Data, SN=52, FN=0, Flags=.p....F.
60	20.454285	SzDjiTec_32:39:a1	QikuInte_9c:0c:39	802.11	1287	QoS Data, SN=53, FN=0, Flags=.p....F.
61	20.454323	QikuInte_9c:0c:39 (74…	SzDjiTec_32:39:a1 (…	802.11	58	802.11 Block Ack, Flags=.....
62	20.454494		SzDjiTec_32:39:a1 (…	802.11	40	Clear-to-send, Flags=.....

```
⊞ Frame 59: 1287 bytes on wire (10296 bits), 1287 bytes captured (10296 bits) on interface 0
⊞ Radiotap Header v0, Length 33
⊞ 802.11 radio information
⊟ IEEE 802.11 QoS Data, Flags: .p....F.
    Type/Subtype: QoS Data (0x0028)
  ⊞ Frame Control Field: 0x8842
    .000 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: QikuInte_9c:0c:39 (74:ac:5f:9c:0c:39)
    Destination address: QikuInte_9c:0c:39 (74:ac:5f:9c:0c:39)
    Transmitter address: SzDjiTec_32:39:a1 (60:60:1f:32:39:a1)
    Source address: SzDjiTec_32:39:a1 (60:60:1f:32:39:a1)
    BSS Id: SzDjiTec_32:39:a1 (60:60:1f:32:39:a1)
    STA address: QikuInte_9c:0c:39 (74:ac:5f:9c:0c:39)
    .... .... .... 0000 = Fragment number: 0
    0000 0011 0100 .... = Sequence number: 52
  ⊞ Qos Control: 0x0000
  ⊞ CCMP parameters
⊞ Data (1220 bytes)
```

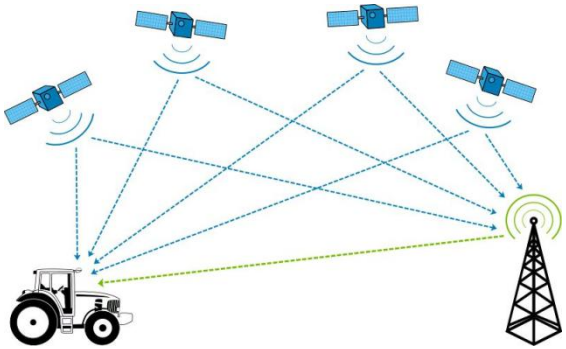
Station Hardware Address (wlan.staa), 6 字节　　分组: 11406 · 已显示: 11406 (100.0%) · 加载时间: 0:0.35　　配置文件: Default

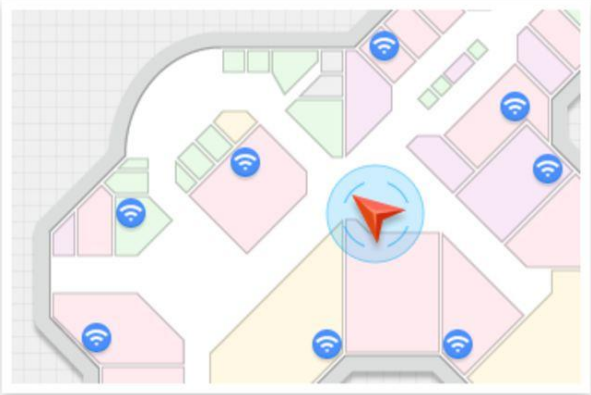
干扰无人机

Deauthentication Attack

类型	热点位置	中断图像？
Dji PHANTOM3	遥控器	Yes
Dji MAVIC(Wi-Fi)	飞行器	Yes
XPLORER	遥控器	Yes

定位与追踪





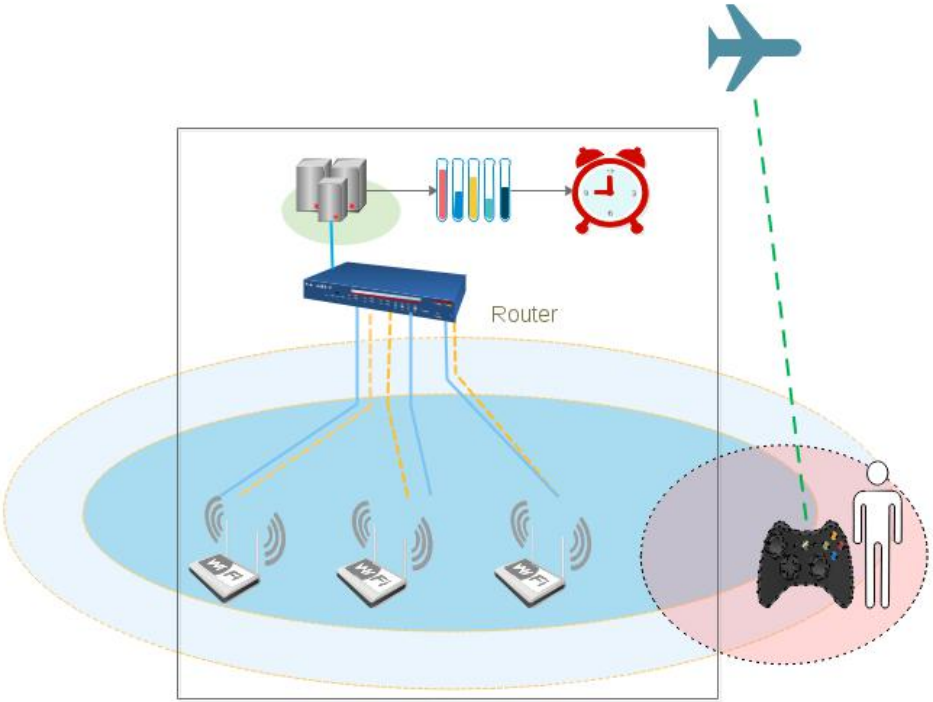
通过多个WiFi senior进行三角定位，判断目标的大致方位。

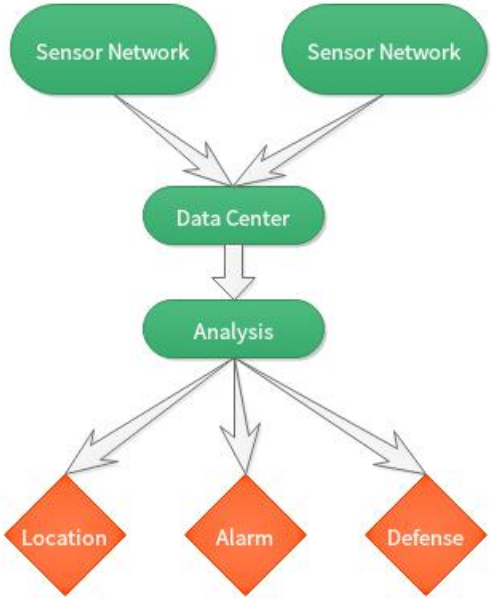
功能总结

- 无人机发现与识别
- 控制/图传干扰
- 飞行器、操控者定位跟踪
- 黑白名单管理
- 电子证据

反无人机系统的设计与实现

系统架构


Router


Sensor Network
Sensor Network
Data Center
Analysis
Location
Alarm
Defense

Requiremnts

Hardware:

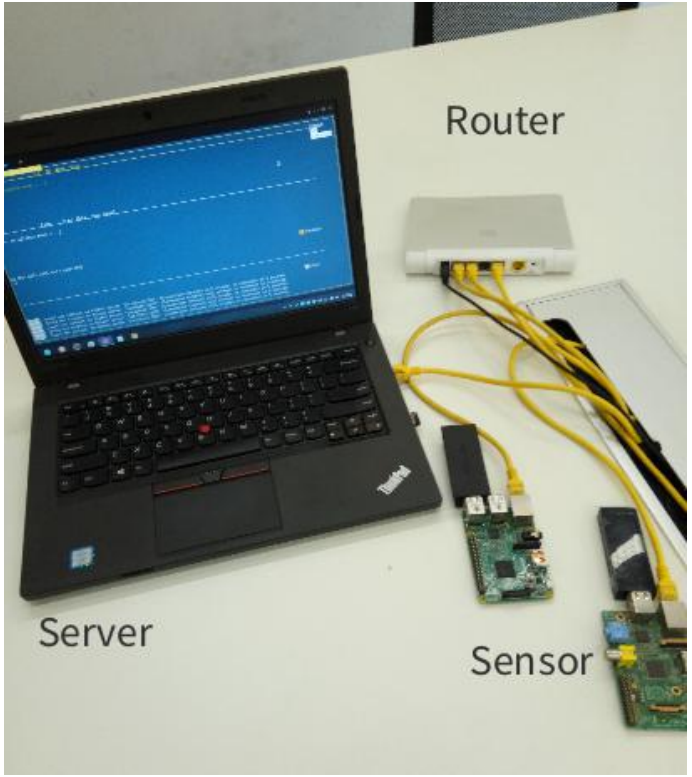
- Linux host
- 5G&2.4G Dual Band WiFi module
- GPS module

Software:

- Kismet
- Analysis scripts

Test UAV:

- DJI Phantom 3



Kismet Drone

#kismet_drone.conf

servername=Kismet-Drone

dronelisten=tcp://<LocalIP>:2502

droneallowedhosts=<ServerIP>

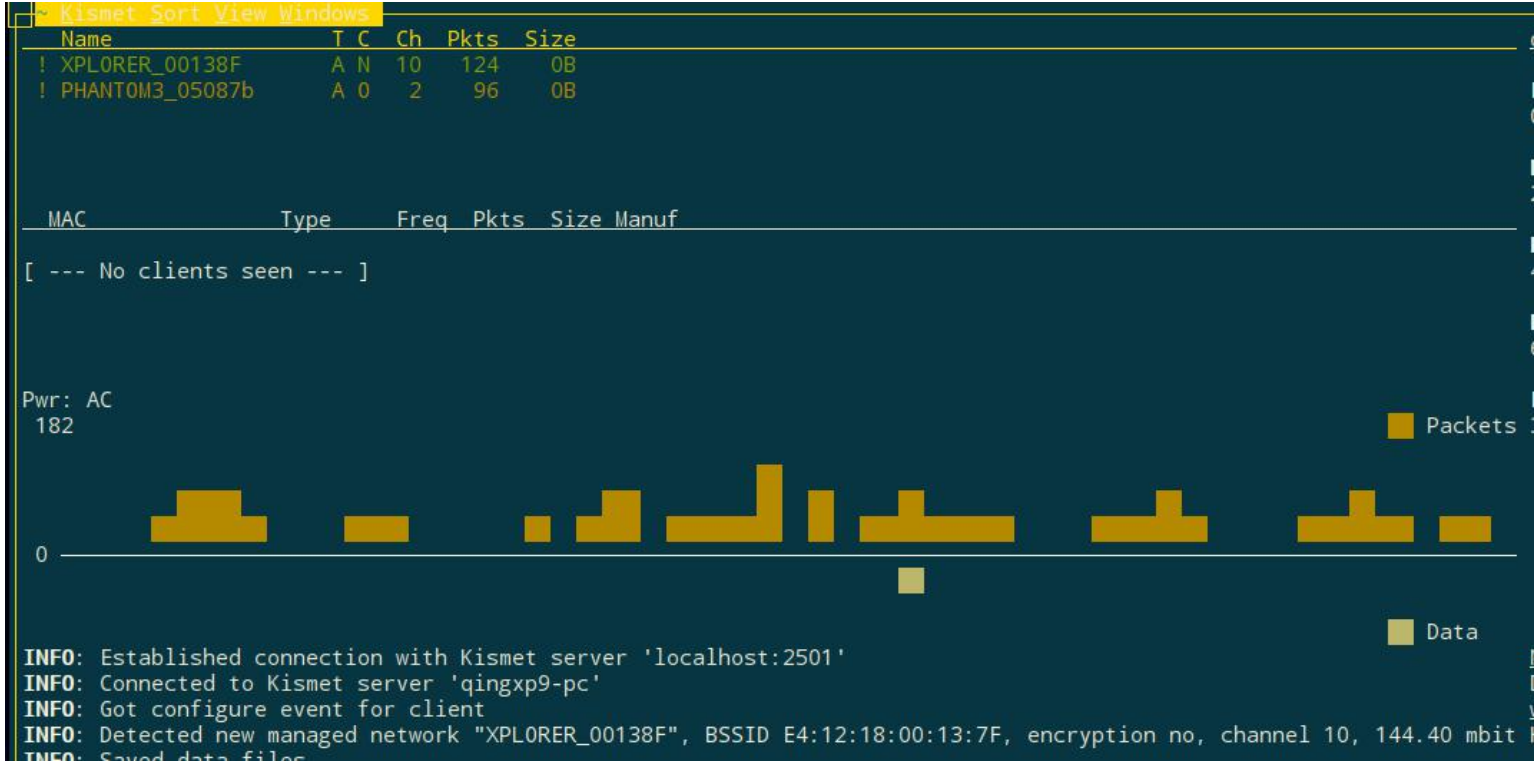
ncsource=<Interface>:channellist:IEEE80211b

Kismet Server

#kismet.conf

```
ncsource=drone:host=<DroneIP>,port=2502
#(无人机过滤规则)
filter_tracker=BSSID(60:60:1F:00:00:00/FF:FF:FF:00:00:00)
...
filter_tracker=BSSID(e4:12:18:00:00:00/FF:FF:FF:00:00:00)
logtypes=netxml,pcapdump
```

Monitoring


Kismet Sort View Windows
Name T C Ch Pkts Size
! XPLORER_00138F A N 10 124 0B
! PHANTOM3_05087b A 0 2 96 0B
MAC Type Freq Pkts Size Manuf
[--- No clients seen ---]
Pwr: AC
182
Packets
0
Data
INFO: Established connection with Kismet server 'localhost:2501'
INFO: Connected to Kismet server 'qingxp9-pc'
INFO: Got configure event for client
INFO: Detected new managed network "XPLORER_00138F", BSSID E4:12:18:00:13:7F, encryption no, channel 10, 144.40 mbit

Log Analysis


```
<wireless-network number="1" type="infrastructure" firs
  <SSID first-time="Fri Mar 10 16:33:06 2017" last-time
      <type>Probe Response</type>
      <max-rate>144.400000</max-rate>
      <packets>166</packets>
      <wps>No</wps>
      <encryption>WPA+PSK</encryption>
      <encryption>WPA+AES-CCM</encryption>
      <wpa-version>WPA2</wpa-version>
      <essid cloaked="false">PHANTOM3_05087b</essid>
  </SSID>
  <BSSID>60:60:1F:05:08:7B</BSSID>
  <manuf>SzDjiTec</manuf>
  <channel>10</channel>
```


无人机热点信息：

- ESSID
- BSSID
- 频道
- 厂商
- 发现时间

Log Analysis

```
</wireless-client>
<wireless-client number="2" type="established" firs
6:41:35 2017" last-time="Fri Mar 10 16:41:58 2017">
  <client-mac>74:AC:5F:9C:0C:39</client-mac>
  <client-manuf>QikuInte</client-manuf>
  <channel>0</channel>
  <freqmhz>2442 2</freqmhz>
  <freqmhz>2447 3</freqmhz>
  <freqmhz>2452 3</freqmhz>
  <freqmhz>2457 4</freqmhz>
  <freqmhz>2462 5</freqmhz>
  <maxseenrate>1000</maxseenrate>
```

客户端信息：

- MAC
- OUI

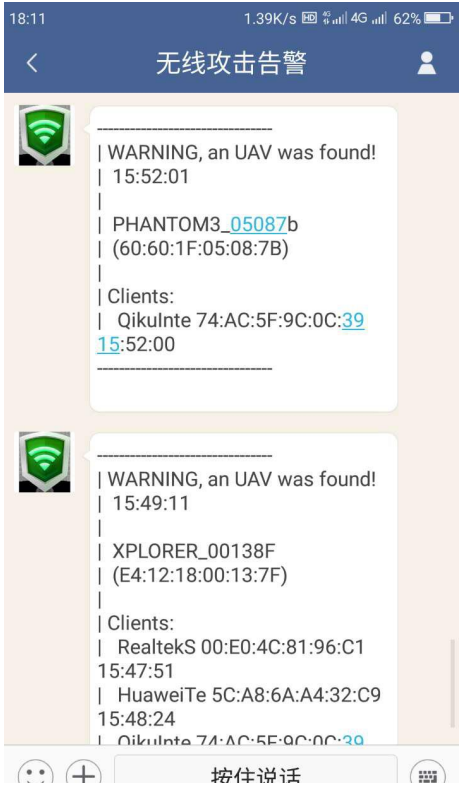
告警

```ruby
xml = File.open("/tmp/uav_logs/uav-#{date}.netxml")
uavs = Hash.from_xml(xml)["detection_run"]["wireless_network"]
uavs = (uavs.class == Hash)?  Array.new.push(uavs) : uavs
uavs.each do |item|
    time = DateTime.parse(item['last_time']).strftime("%T")
    meg = []
    meg.push "-------------------------------"
    meg.push "| WARNING, an UAV was found! "
    meg.push "|  #{time}"
    meg.push "| "
    meg.push "|  #{item['SSID']['essid']}"
    meg.push "|  (#{item['BSSID']})"
    meg.push "| "
    meg.push "| Clients:"

    clients = item["wireless_client"]
    clients = (clients.class == Hash)?  Array.new.push(clients) : clients
    clients.each do |client|
```

```
➜ ~ ruby detectuav.rb
-----------------------------------------
| WARNING, an UAV was found!
|  15:52:01
|
|  PHANTOM3_05087b
|  (60:60:1F:05:08:7B)
|
| Clients:
|   QikuInte 74:AC:5F:9C:0C:39 15:52:00
-----------------------------------------
-----------------------------------------
| WARNING, an UAV was found!
|  15:49:11
|
|  XPLORER_00138F
|  (E4:12:18:00:13:7F)
|
| Clients:
|   RealtekS 00:E0:4C:81:96:C1 15:47:51
|   HuaweiTe 5C:A8:6A:A4:32:C9 15:48:24
|   QikuInte 74:AC:5F:9C:0C:39 15:49:11
-----------------------------------------
```

告警


18:11
1.39K/s
4G
62%
无线攻击告警

| WARNING, an UAV was found!
| 15:52:01
|
| PHANTOM3_05087b
| (60:60:1F:05:08:7B)
|
| Clients:
| QikuInte 74:AC:5F:9C:0C:39
15:52:00

| WARNING, an UAV was found!
| 15:49:11
|
| XPLORER_00138F
| (E4:12:18:00:13:7F)
|
| Clients:
| RealtekS 00:E0:4C:81:96:C1
15:47:51
| HuaweiTe 5C:A8:6A:A4:32:C9
15:48:24
按住说话

干扰

DEAUTH ATTACKING

DISCONNECTING

Demo

https://drive.google.com/file/d/0B5LLwBgKenflbGZnVE9VU19jN3M/view

优势

- 可进行黑白名单管理
- 适应城市等复杂环境，不影响其它无线电通信
- 可定位追踪到操控者的手机设备
- 已部署有WIPS产品的场所，利用现有Wi-Fi传感器网络便可快速升级支持

Monitoring Analysis

Location Ranking（2/9/2017）

Ranking	Location	Count	Duration
1	机场高速滑行东桥	10	00:40:51
2	北京首都机场国际酒店	8	00:33:00
3	货运北路	6	00:30:11
4	哨马营	5	00:35:24
5	机场航站楼东侧	5	00:22:30
6	中国民用航空飞行校验中心	3	00:10:55
7	航港二路	3	00:05:03


Prison
Details
Location: 看守所外围墙东侧
Time: 2/9/2017 22:55:00
Duration: 17 minutes
Type: Mavic
MAC: 60:60:1f:32:39:a1
Monitoring Analysis
Count
02-04
无人机为近飞行次数：7
Date
Location Ranking（2/9/2017）
Ranking Location Count Duration
1 看守所外围墙东侧 10 00:40:51
2 看守所外围墙西侧 8 00:33:00
3 正门南侧 6 00:30:11
4 监一区北 5 00:35:24
Image © 2016 DigitalGlobe
1/31 2/1 2/2 2/3 2/4 2/5 2/5 2/6 2/7 2/8 2/9 (十三) 2/10 2/11 2/12 2/13 2/14 2/15 2/16 2/17 2/18

缺点

- 检测及类型识别依赖于指纹库
- 无法覆盖所有类型的无人机设备，部分无人机不使用Wi-Fi

不同型号无人机具有不同的通信频段、不同的私有协议，加上现实世界比较复杂的无线电环境，只靠无线电的角度去做无人机检测是比较困难的

承载在802.11上的无人机管控方案

无人机管控方案

鉴于无人机厂家相互独立，行业缺乏统一管控标准的现状，提出一套承载在802.11上的无人机管控方案。

优点：便于现有大部分无人机通过固件升级的方式予以支持，不需额外添加硬件模块

- 无人机身份识别机制

  无人机不断发送广播信号，报告自身身份及位置

- 无人机围栏

  围栏发送信息广播，以示无人机避让

802.11管理帧信息元素由三部分组成：Type-Length-Value

Type值从0~255，不同标号代表管理帧的不同作用，

tag= 0 表示SSID;

tag= 1表示所支持的速率;

Try It! *SSID: SmellOfWifiTalk*

Signature: Information Elements

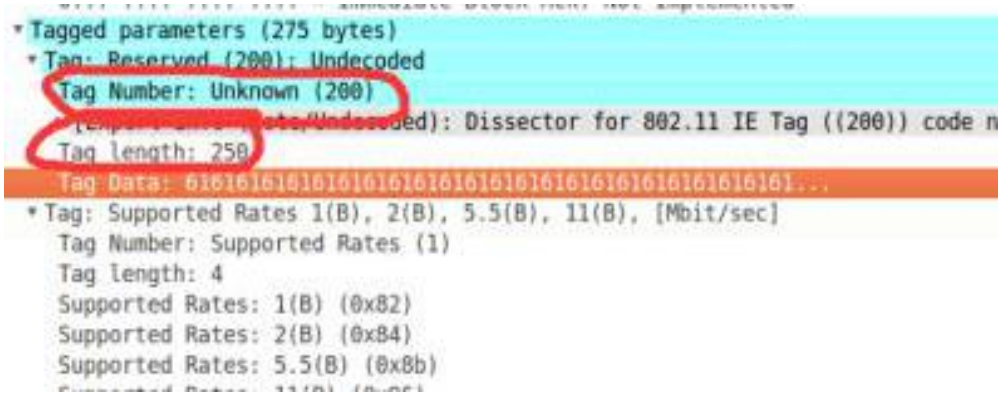
```
▶ Frame 9: 199 bytes on wire (1592 bits), 199 bytes ca
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▶ IEEE 802.11 Association Request, Flags: .........
▼ IEEE 802.11 wireless LAN management frame
  ▶ Fixed parameters (4 bytes)
  ▼ Tagged parameters (142 bytes)
    ▶ Tag: SSID parameter set: XXXXXXXXXX
    ▶ Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B),
    ▶ Tag: Power Capability Min: 249, Max :19
    ▶ Tag: Supported Channels
    ▶ Tag: RSN Information
    ▶ Tag: RM Enabled Capabilities (5 octets)
    ▶ Tag: HT Capabilities (802.11n D1.10)
    ▶ Tag: VHT Capabilities (IEEE Std 802.11ac/D3.1)
    ▶ Tag: Vendor Specific: Apple
    ▶ Tag: Vendor Specific: Broadcom
    ▶ Tag: Vendor Specific: Microsof: WMM/WME: Inform
```

Tag #0
Tag #1
Tag #33
Tag #36
Tag #48
Tag #70
Tag #45
Tag #191
Tag #221, Vendor OUI `00:17:f2`, #10
Tag #221, Vendor OUI `00:10:18`, #2
Tag #221, Vendor OUI `00:50:f2`, #2

0,1,33,36,48,70,45,191,221(0017f2,10),221(001018,2),221(0050f2,2)

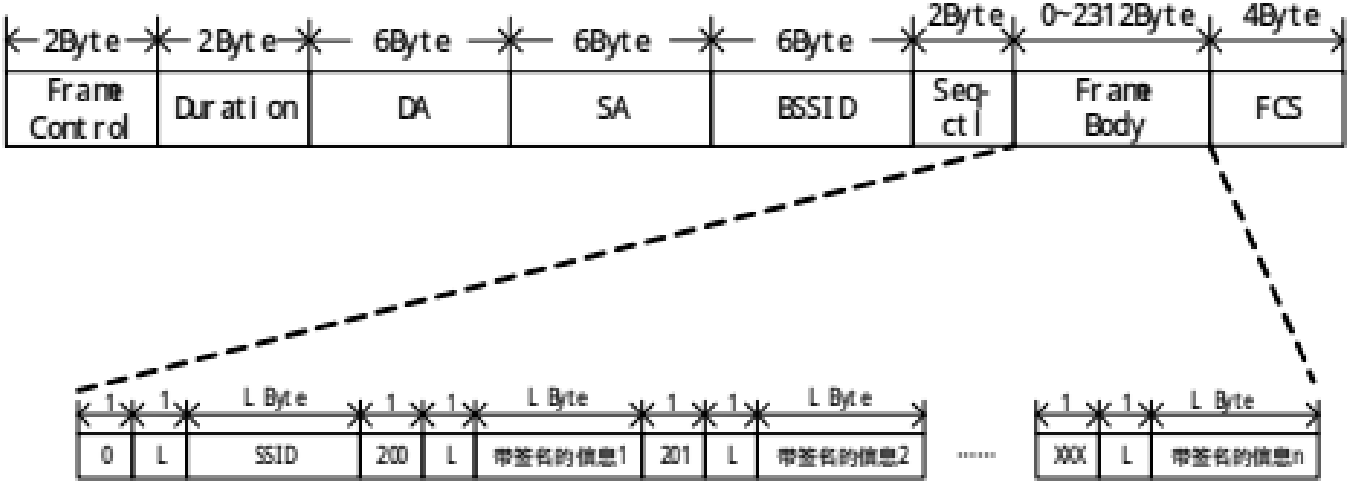
身份识别机制

通过未定义的tag值携带签名信息



数字签名部分可采用椭圆曲线加密（ECC :Elliptic Curve Cipher）算法，也可采用其他签名算法。ECC算法是一种成熟的公钥密码系统，密钥的长度要远小于RSA加密技术。

整个Framebody最长为2312，信息拼接起来。若采用ECC算法384*3bit加密技术，一帧就可以发送完整签名信息帧。



拼接的管理帧

身份识别机制

```
Timestamp: 0x0000000000000000
Beacon Interval: 0.102400 [Seconds]
▸ Capabilities Information: 0x0001
Tagged parameters (813 bytes)
▸ Tag: SSID parameter set: 00123456789abcdef123456789abcdef
▸ Tag: Reserved (200): Undecoded
▾ Tag: Reserved (201): Undecoded
  ▸ Tag Number: Unknown (201)
    Tag length: 250
    Tag Data: 626262626262626262626262626262626262626262626262...
▸ Tag: Reserved (202): Undecoded
▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
▸ Tag: DS Parameter set: Current Channel: 6
▸ Tag: CF Parameter set: CFP count 1: CFP Period 2: CFP Max Duration 0: CFP Dur Remaining 0
▸ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
```

证书签发

根证书由政府管理部门或国际机构管理，根证书之下可以签发二级证书、三级证书……

- 例如民航管理部门持有根证书，分别给不同无人机厂商签发二级证书。无人机厂商为每一台出售的无人机配置证书。
- 民航管理部门也可以给例如电网、遥测遥感、公安武警等单位签发二级证书。这些单位负责给自己的专用无人机配置证书。

每个证书对应的私钥存储在无人机上，公钥存放在网络服务器上。无人机监控设备可通过公钥服务器获取对应的公钥，检验签名合法性。

无人机围栏

无人机围栏通过信息广播以示无人机避让。广播内容以时间戳（防止重放攻击）与特定警告信息为主。

带数字签名：

重要限飞区域所使用，无人机收到该信息后需立即返航或降落。

不带数字签名：

无人机的控制端发出警告，自行避让。

无人机围栏配合无人机监测系统同时使用，当发现无人机时发出报警，当闯入围栏内时进行干扰。

Thank you!