



Guillaume Fournier

CentraleSupélec - Promo 2018
guillaume.fournier@supelec.fr



Paul de Kerdrel

CentraleSupélec - Promo 2018
paul.audrendekerdrel@supelec.fr



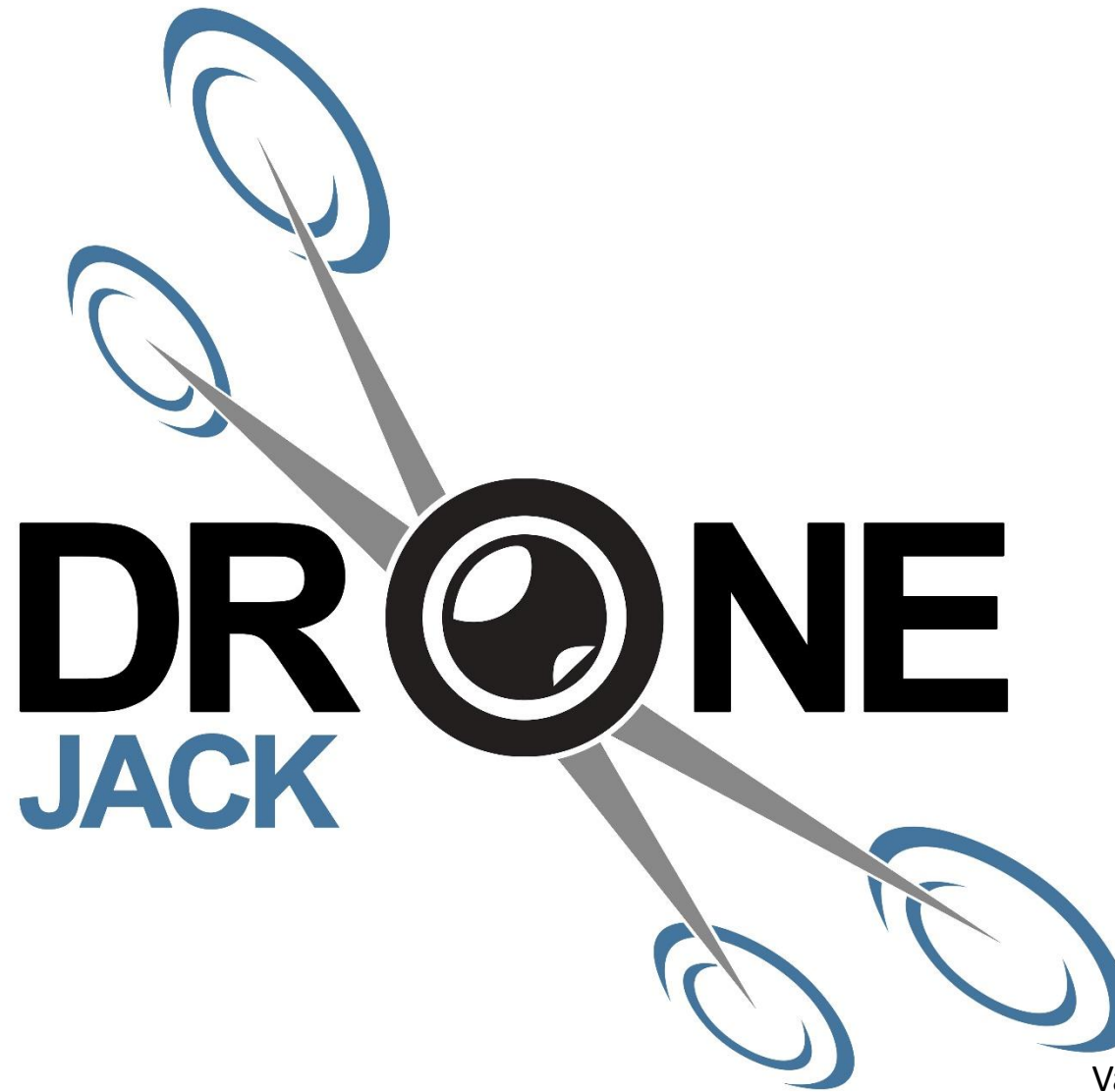
Pascal Cotret (@Pascal_r2)

IETR/SCEE
pascal.cotret@centralesupelec.fr



Valérie Viet Triem Tong

Cidre CentraleSupélec / Inria
Valerie.viettriemtong@centralesupelec.fr



CentraleSupélec

SSTIC 2017

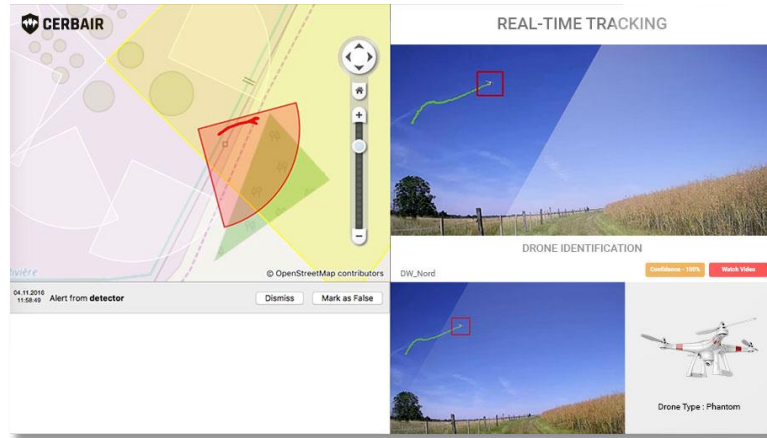
Guillaume Fournier

Paul de Kerdrel, Pascal Cotret, Valérie Viet Triem Tong

I. Les solutions existantes

II. Dronejack

- Détection & tracking
- Prise de contrôle
- Attaque



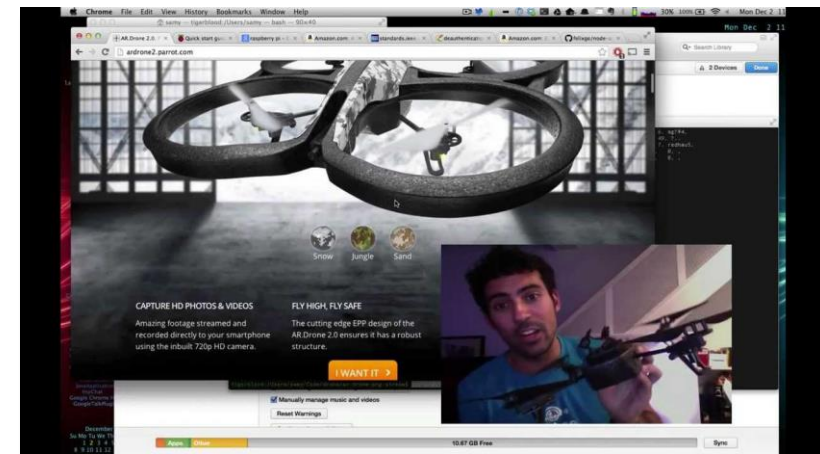
DroneWatch



Drones VS Eagles

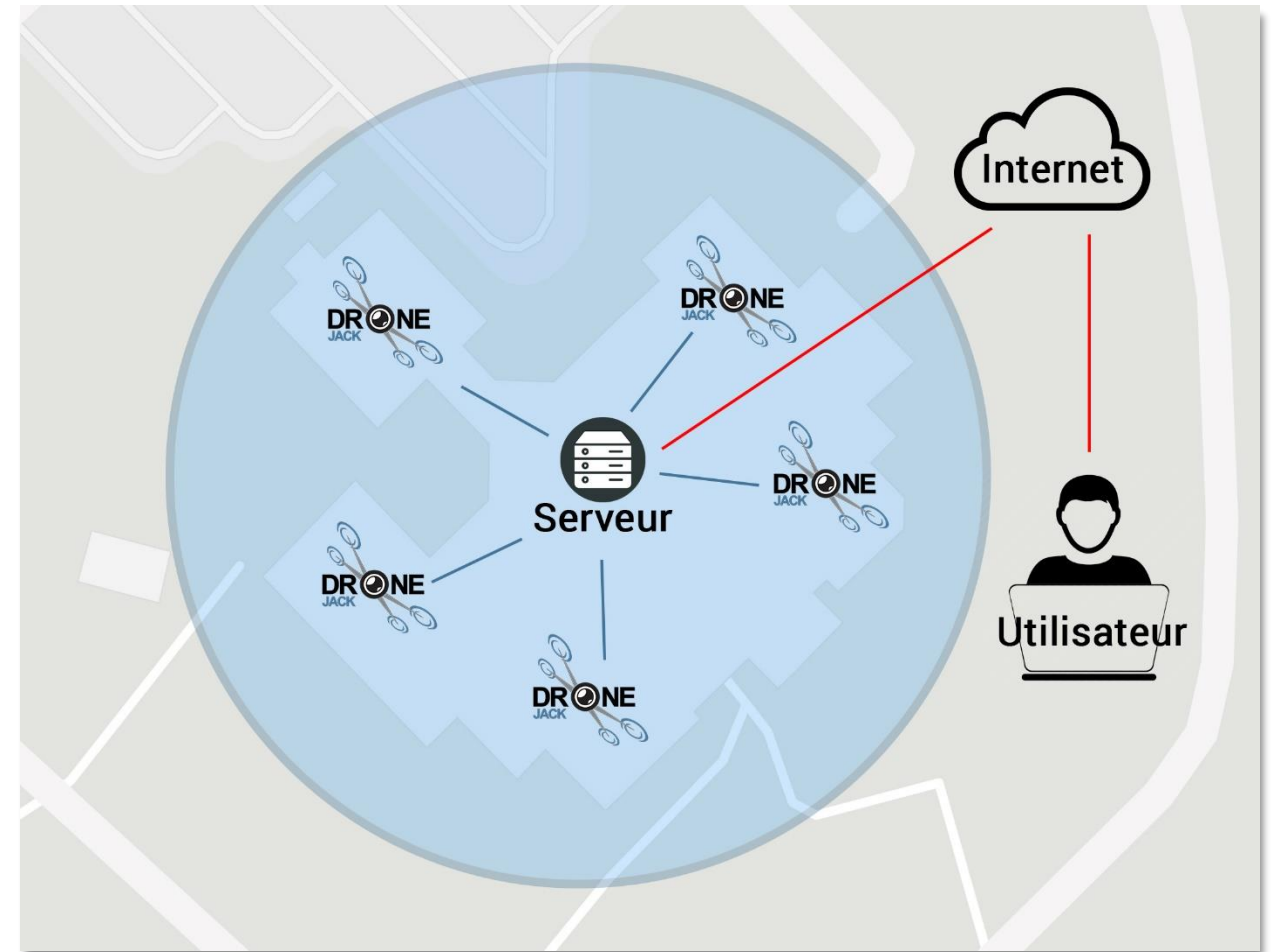


DroneDefender



SkyJack

- Une protection continue contre un nuage de drones WiFi
- Une architecture flexible
gérée à distance
peu coûteuse
- Dronejack se décompose en 3 phases:
 - 1) détection & *tracking*
 - 2) prise de contrôle
 - 3) attaque



Architecture physique



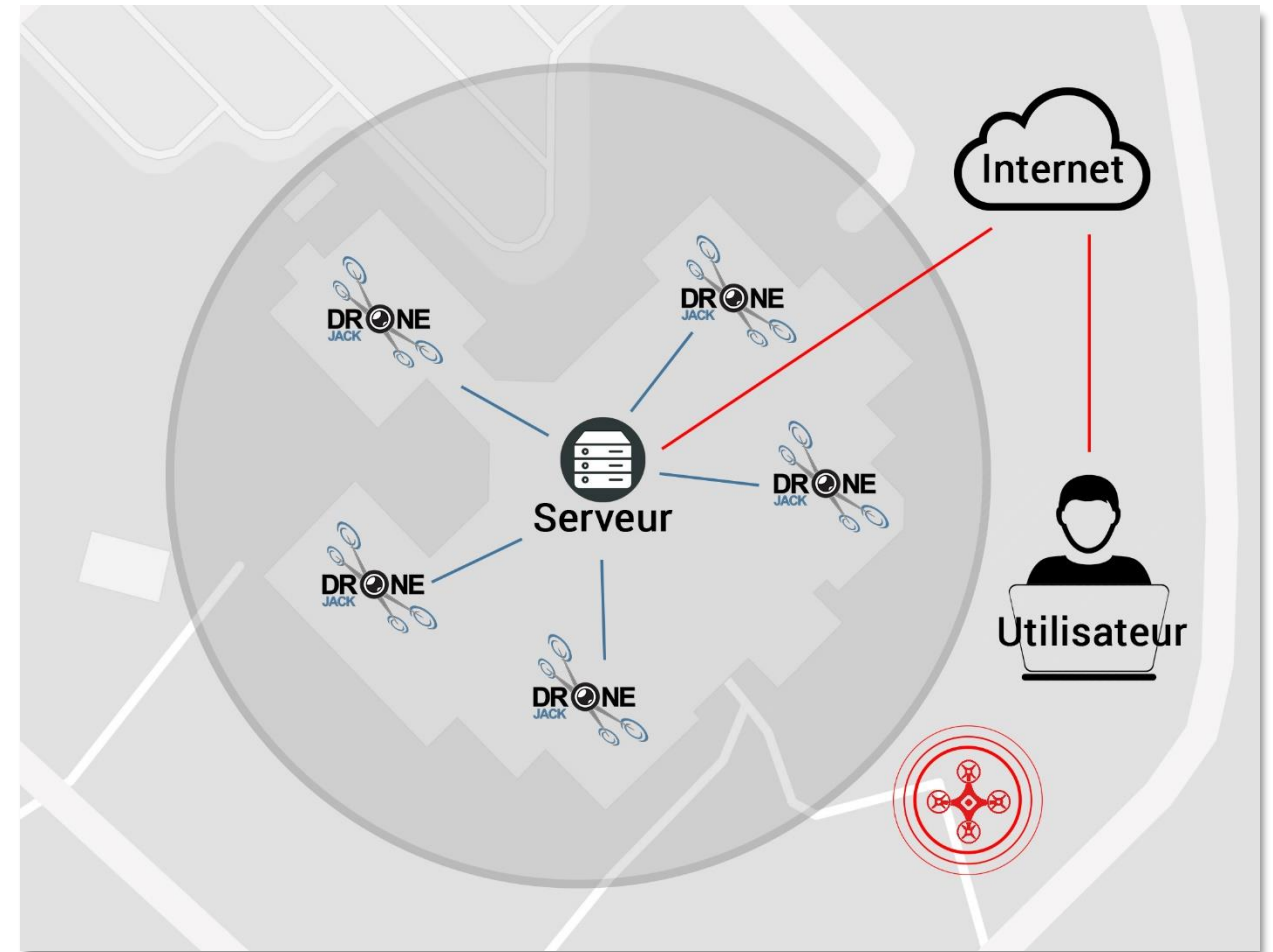
Un drone WiFi:

- est un point d'accès WiFi
- émet des beacons
- a une adresse MAC identifiable

MAC	Company	Address
90:3A:E6	Parrot SA	174 Quai de Jemmapes Paris
90:03:B7	Parrot SA	174 Quai de Jemmapes Paris
A0:14:3D	Parrot SA	174 Quai de Jemmapes Paris
00:26:7E	Parrot SA	174 Quai de Jemmapes Paris
00:12:1C	Parrot SA	174 Quai de Jemmapes Paris

Détection:

- Les sondes écoutent le trafic sur la zone (airodump-ng)
- identification du modèle de drone

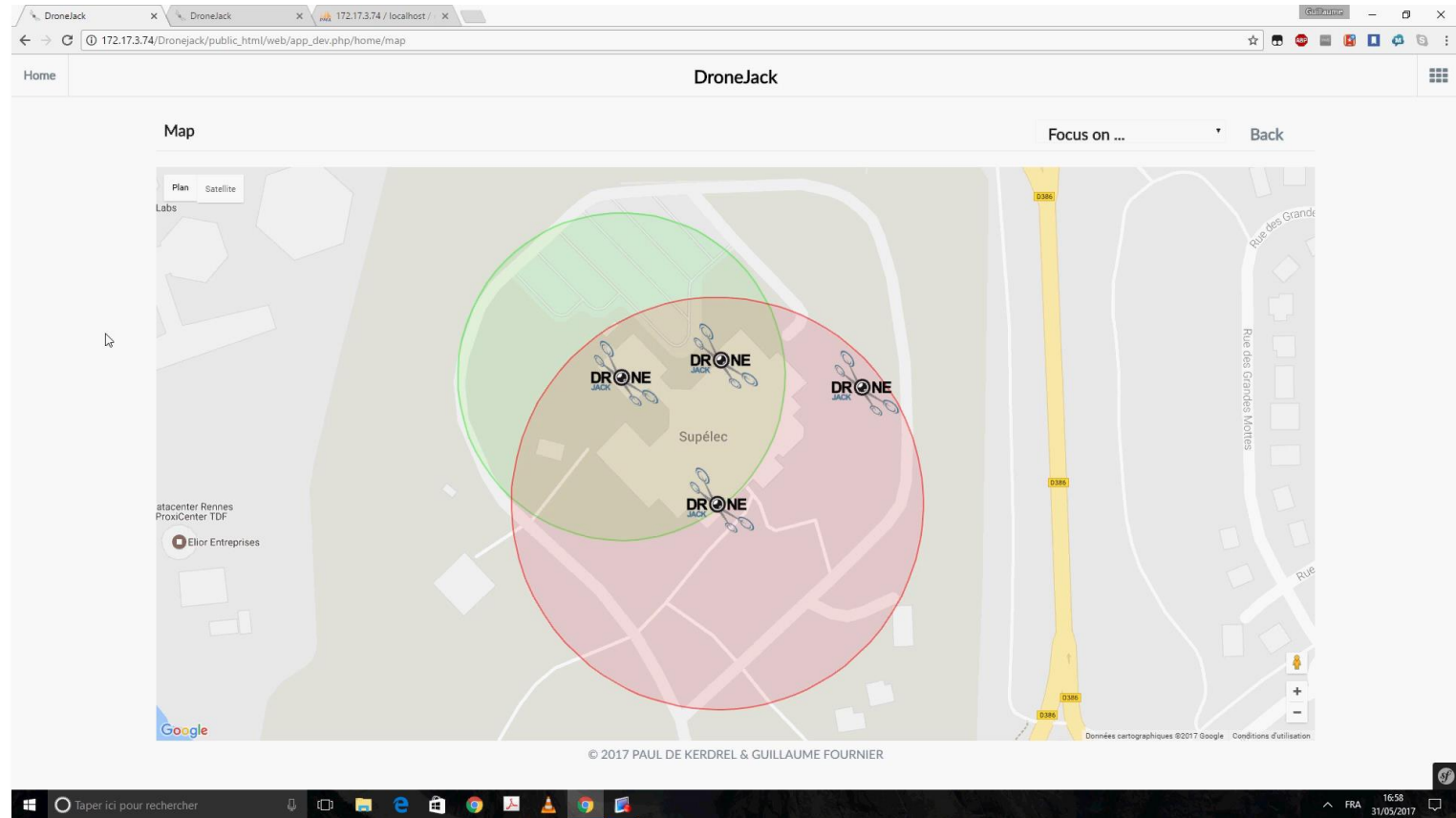


Architecture physique



Tracking:

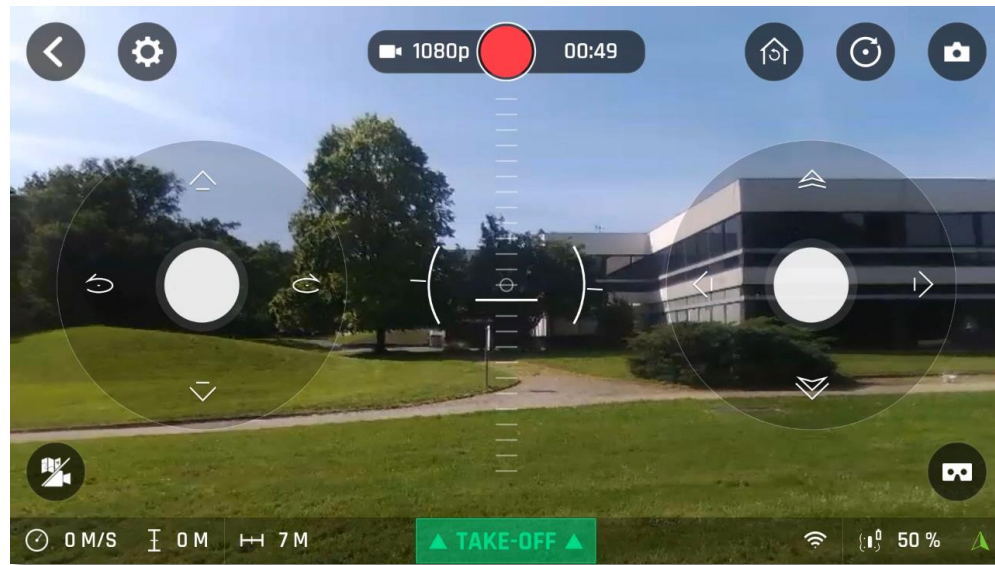
- Chaque sonde calcule la distance au drone détecté à l'aide de la puissance du signal reçu



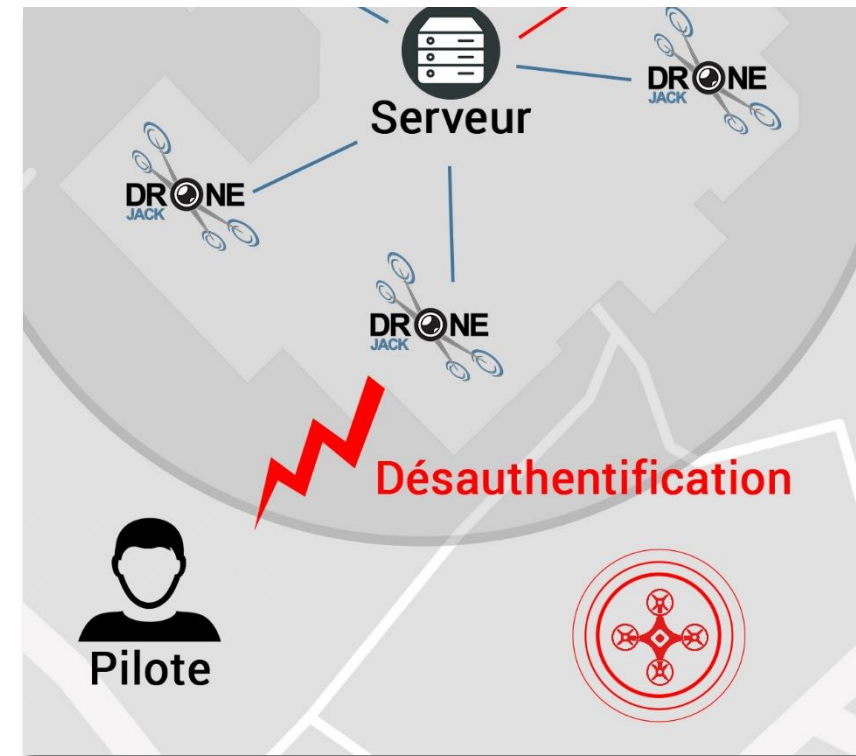
Déconnexion du pilote:

- les sondes envoient des paquets de désauthentification au pilote (aireplay-ng)

Le drone est alors en vol stationnaire en attente de reconnexion



Vue pilote



Désauthentification du pilote

Cas 1: réseau WiFi sécurisé (WPA/WPA2)

- Le drone reste stable puis finit par retourner à ses coordonnées GPS de décollage



Cas 2: réseau WiFi ouvert

- La sonde la plus proche se connecte au drone
- Phase 3

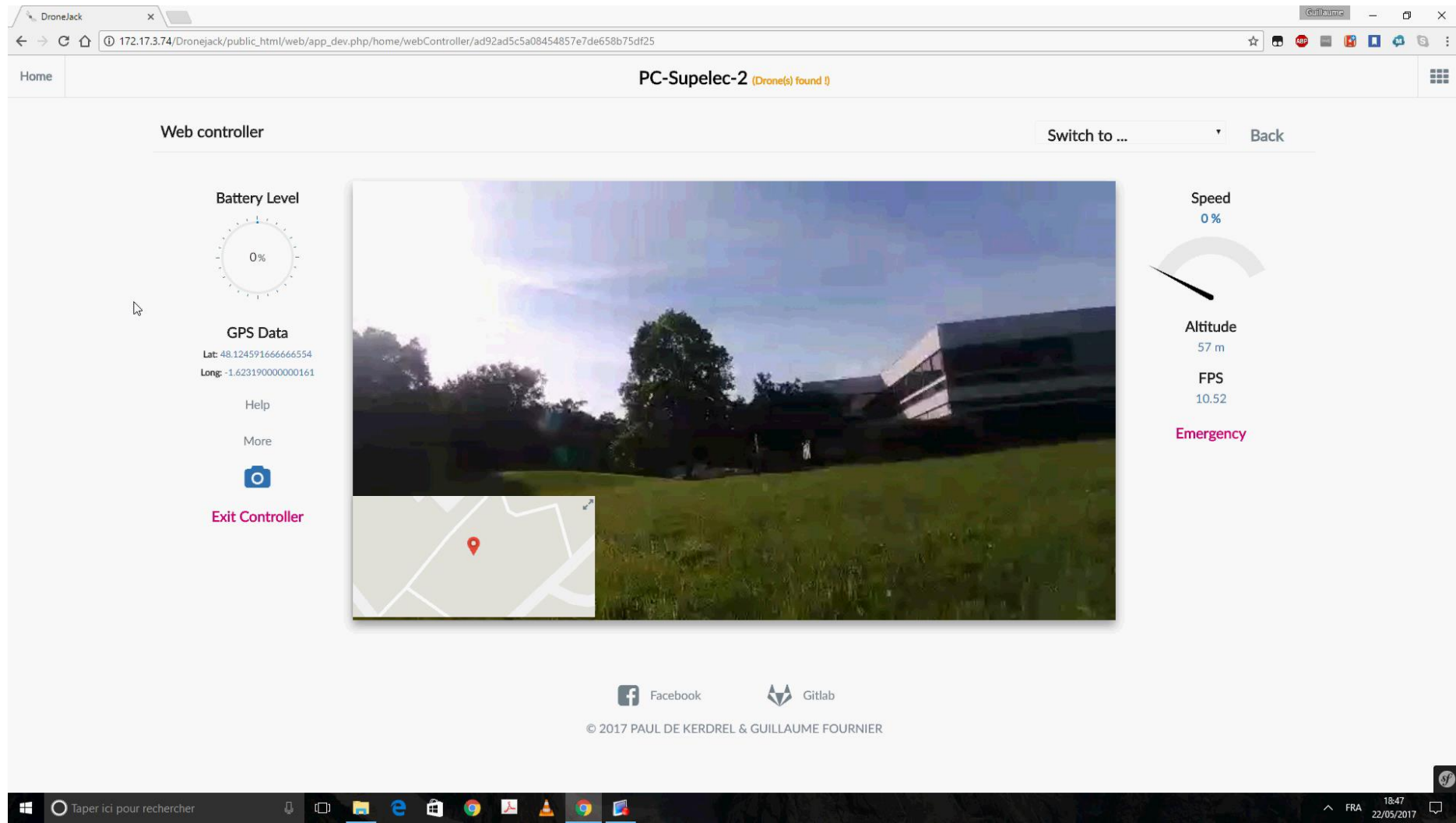
Attaques sur le contrôle du drone (avec API)

- Retour maison
- Envoi du drone à des coordonnées GPS
- Arrêt d'urgence
- Pilotage via interface Web

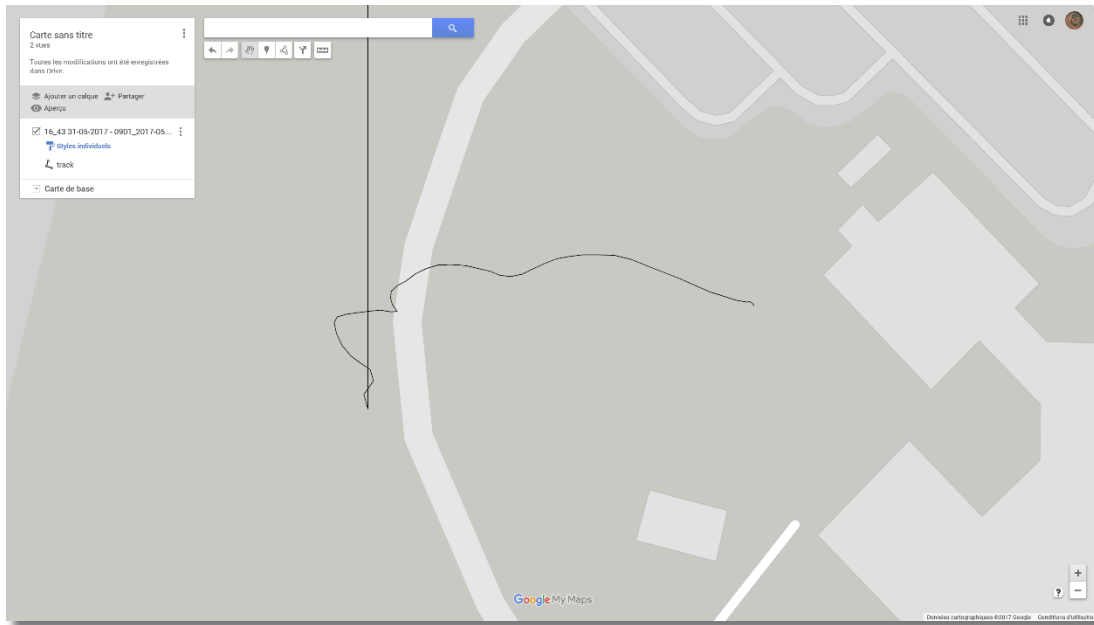
Attaques sur l'OS du drone

- Scan NMAP du drone
- Récupération des données vidéo / images
- Récupération des données de vol (tracé GPS du vol du drone)
- Suppression des données (vidéo / images / données de vol)





Pilotage via interface Web



Données GPS de vol

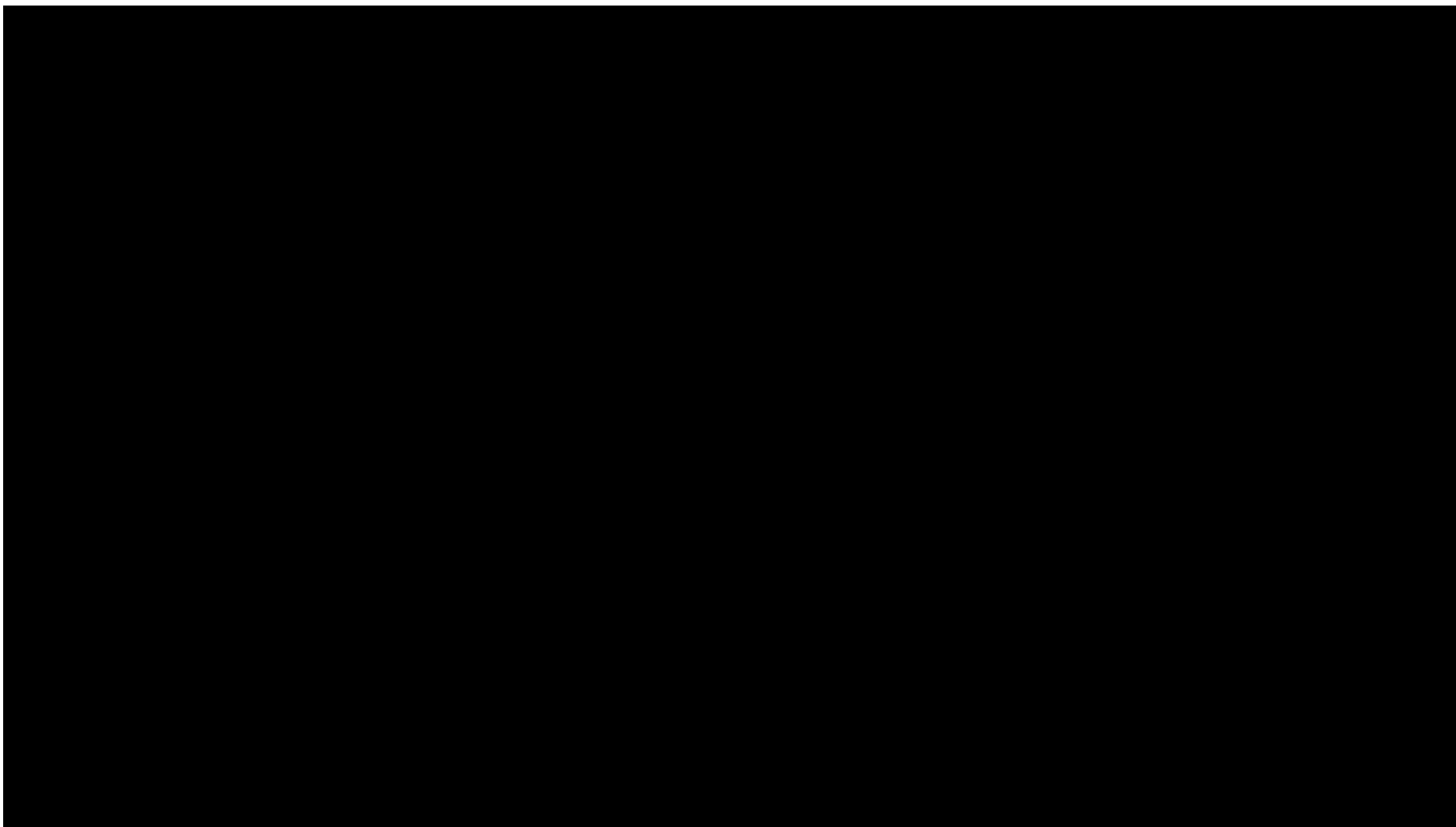


Vidéo prise par le drone piraté



Merci !

www.dronejack.fr



Attaque par rejeu

Objectif: Prendre le contrôle des drones sans API ?

- API « node-bebop » de Parrot sur [NodeJs](#)
- Même protocole ? (application Android / iOS)
- 1 paquet toutes les 25ms → 255 paquets en 6s

Conclusion: automatisation en cours !

```
66     type = type || constants.ARNETWORKAL_FRAME_TYPE_DATA;
67     id = id || constants.BD_NET_CD_NONACK_ID;
68
69     if (!seq[id]) {
70         seq[id] = 0;
71     }
72
73     seq[id]++;
74
75     if (seq[id] > 255) {
76         seq[id] = 0;
77     }
```

Protection Anti-replay

```
249     setInterval(function() {
250         this._writePacket(this._generatePCMD(this._pcmd));
251     }.bind(this), 25);
```

Une usine à paquets

