
Drone predator,
one drone tu rule them all

Rapport de projet long TLS-SEC

Florent Fayollas et Antoine Vacher, promotion 2018 – 2019

DRONE PREDATOR



ONE DRONE TO RULE THEM ALL

Table des matières

1	Introduction	2
1.1	Introduction généraliste sur les drones	2
1.2	Motivations de ce travail	2
1.3	Définition des objectifs	2
2	Prise de contrôle d'un drone Parrot AR.Drone 2.0	3
2.1	Présentation technique de l'attaque	3
2.2	Réalisation	3
2.2.1	Utilisation d'une unique puce WiFi	3
2.2.2	Problème de pilote de puce WiFi	3
2.3	Détection et prévention de l'attaque	3
3	Prise de contrôle d'un drone Syma X5C-1	4
4	Embarquement de l'outil de prise de contrôle sur un drone prédateur	5
4.1	Installation de l'outil sur une Raspberry Pi Zero W	5
4.1.1	Utilisation du cockpit <code>ardrone-webflight</code>	5
4.1.2	Compilation de la bibliothèque <code>pyRF24</code>	5
4.1.3	Utilisation distante d'une manette	5
4.1.4	Contrôle distant de l'outil	5
4.2	Tests finaux de l'outil embarqué	5
5	Conclusion	6

1 Introduction

1.1 Introduction généraliste sur les drones

Les UAVs (*Unmanned Aerial Vehicles*), communément appelés drones, sont des aéronefs sans pilote humain à bord. Un drone est un composant d'un UAS (*Unmanned Aircraft System*), qui comprend un UAV, une station de contrôle au sol et un système de communication entre les deux.

Les UAVs étaient, à l'origine, développés par les militaires et utilisés pour des missions trop dangereuses pour les humains. Cependant, ces dernières années, leur utilisation s'est généralisée à beaucoup de secteurs, tels que l'industrie ou les loisirs. Des exemples concrets d'utilisations sont la surveillance de réseaux électriques EDF ou des voies ferrées ou la photographie aérienne.

Leur champ d'utilisation est en croissance continue. En effet, les drones pourraient nous aider lors de scénarios de secours, par exemple, en étant utilisés par les pompiers pour un suivi en temps réel par images thermiques d'un feu. En outre, certaines entreprises, telles qu'Amazon, envisagent d'effectuer des livraisons par drone.

1.2 Motivations de ce travail

Bien que les précédents cas d'usage civils soient bénéfiques, d'autres usages peuvent exister... En effet, un cas concret concernant tout le monde est celui d'une personne qui utiliserait un drone pour vous espionner, en survolant votre maison et passant proche de vos fenêtres. Une autre utilisation, plus grave, est l'utilisation, par Daesh, de drones civils pour larguer des bombes sur le front en Syrie. Enfin, plus récemment, l'aéroport de Londres Gatwick a été fermé pour cause de survols répétés par un drone non identifié.

Ainsi, il devient nécessaire de pouvoir se protéger des drones. Du côté militaire, des solutions existent déjà, telles que le brouillage de la liaison de commandes, par exemple grâce à des sortes de fusils, comme le DroneGun développé par DroneShield¹. Cependant, très peu de solutions sont présentes côté civil.

On pourrait penser à importer les solutions militaires dans le civil. Or, celles-ci mettent souvent hors d'état de nuire le drone, peu importe l'état final (un *crash* par exemple). Ceci n'étant pas acceptable dans un cadre civil.

1.3 Définition des objectifs

L'objectif de notre projet est donc de développer un outil capable de prendre le contrôle de plusieurs drones. Cette prise de contrôle ne doit pas impliquer une chute du drone piraté. Cet outil pourrait ensuite être utilisé, par exemple, pour sécuriser la médiatisation d'un match sportif : il sera en mesure de "capturer" les drones détectés et de les récupérer. Après capture, il sera aussi possible d'analyser le contenu des drones et éventuellement de remonter au propriétaire.

Pour réaliser cet outil, nous nous sommes focalisés sur la prise de contrôle de drones civils : le Parrot AR.Drone 2.0 et le Syma X5C-1. C'est ce que nous détaillons dans les deux premières parties de ce rapport. Lorsque ces prises de contrôle furent terminées, nous avons cherché à embarquer l'outil sur un autre drone. Ceci est discuté dans la troisième partie de ce rapport.

1. <https://www.droneshield.com/>

2 Prise de contrôle d'un drone Parrot AR.Drone 2.0

présentation vulgarisée

2.1 Présentation technique de l'attaque

TODO

2.2 Réalisation

TODO

2.2.1 Utilisation d'une unique puce WiFi

TODO

2.2.2 Problème de pilote de puce WiFi

TODO

2.3 Détection et prévention de l'attaque

TODO : capture ENAC

3 Prise de contrôle d'un drone Syma X5C-1

TODO

4 Embarquement de l'outil de prise de contrôle sur un drone prédateur

4.1 Installation de l'outil sur une Raspberry Pi Zero W

présentation vulgarisée

4.1.1 Utilisation du cockpit ardrone-webflight

déport par iptables

4.1.2 Compilation de la bibliothèque pyRF24

compilation pyrf24

4.1.3 Utilisation distante d'une manette

usbip

4.1.4 Contrôle distant de l'outil

Bluetooth PAN

4.2 Tests finaux de l'outil embarqué

volière ENAC avec paparazzi + utilisation moyens volière (vidéo, etc.) + portée bluetooth

5 Conclusion

TODO