République Algérienne Démocratique et Populaire
Ministère de L'enseignement Supérieur et de la Recherche Scientifique
**Université A/Mira de Béjaia**
Faculté des Sciences Exactes
**Département Informatique**


# Mémoire de Fin de cycle

**En vue de l'obtention du diplôme Master recherche en Informatique**
**Option : Réseaux et Systèmes Distribués**

THÈME

---

# Contrôle d'un groupe d'avions sans pilote (UAVs)

---

**Réalisé par**

*M^elle* ***BEN BOUDAOUD Lynda*** *&* *M^elle* ***ALBANE Saadia***

Devant le jury composé de

**Président** M. KABYL Kamel
**Examinateur** M. BAADACHE Abderrahmane
**Examinateur** M. AMAD Mourad
**Rapporteur** M. HAMOUMA Moumen

Année Universitaire 2012/2013

# Remerciement

*Au terme de ce travail,nous adressons nos vifs remerciements à notre promoteur Mr Hammouma Moumen pour son aide et son encouragement.*

*Nous tenons particulièrement à remercier vivement :*

- *Mr Omar Mawloud : Notre chef de département Informatique ;*
- *Mr Nadir Salhi : Enseignant dans le département d'informatique ;*
- *Mr Abdessamad Ait El Cadi : Enseignant à l'École Polytechnique de Montréal ;*
- *Mr Tomeu Serra : Professeur à l'université Balearic Islands University (UIB) ;*
- *Mr Ben Mansour Djaafar : Oncle de Lynda ; ingénieur en automatique ;*
- *Mr Ben Boudaoud Boualem : Ingénieur en Informatique à l'université de Montréal ;*

*Pour leurs directives, conseils et encouragement qu'ils nous ont prodigués.*

*Nous remercions les membres de jury pour avoir accepté d'évaluer notre travail.*

*Nous remercions également tout enseignant et enseignante du département d'informatique.*

*Enfin nous tenons à remercier sincèrement toutes les personnes ayant contribué de prés ou de loin à la réalisation de ce travail.*

# Dédicaces

*A l'Eternel Dieu pour sa protection continue dans notre vie.*

*A nos très chers parents, qui ont toujours été là pour nous, et nous ont donné un magnifique modèle de labeur et de persévérance.*

*Nous espérons qu'ils trouveront dans ce travail toutes nos reconnaissances. Nous dédions ce projet de fin d'étude en espérant la réussite et le succès.*

**Lynda et Saadia**

# Table des matières

# Liste des figures

# Liste des abréviations

**A**

**ADS-B** : Automated Dependent Sureveillance Broadcast.

**G**

**GPS** :Global Positioning System.

**H**

**HALE** :Haute Altitude Longue Endurance.

**K**

**KF** : Kalman Filter.

**M**

**MALE** : Moyenne Altitude Longue Endurance.
**MMSE** : Minimum Mean Square Error.

**T**

**TOA** : Time Of Arrival.
**TDOA** : Time Difference Of Arrival.

**U**

**UAS** : Unmanned Aerial System
**UAV** : Unmanned Aerial Vehicles.
**UAVNet** :Unmanned Aerial Vehicles Network.
**UCAV** :Unmanned Combat Aerial Vehicle.

# Liste des tableaux

# Introduction générale

Voler est et restera l'un des plus grands plaisirs de l'homme...
Toutefois, si celui-ci était à bord de la première machine volante, pour sa plus grande fierté, ses connaissances scientifiques et technologiques lui permettent aujourd'hui de rester au sol dans certaines circonstances et ce, pour son plus grand avantage.

Il étend ainsi de façon considérable le champ d'utilisation des aéronefs qui, prenant le nom de " drones " lorsqu'ils sont inhabités, semblent être légitimement appelés à une carrière prometteuse.
Ce nouveau palier aéronautique franchi par l'homme est le fruit des plus récents progrès accomplis dans des domaines clés, tels que l'informatique, l'automatique, la robotique, l'optronique, l'imagerie radar, la transmission de données, etc.

Les drones occupent ainsi à juste titre une place de plus en plus importante dans les milieux aéronautiques et de la défense. Et l'on assiste à une montée en puissance des expérimentations dans le monde entier, ouvrant la voie à des utilisations opérationnelles. Cependant, si le potentiel d'applications civiles et militaires semble effectivement très élevé, ce n'est pas sans soulever certains problèmes fondamentaux qui, à défaut d'être résolues, pénalisaient gravement une utilisation optimale des drones. Ces problèmes peuvent tous être aplanies. A condition d'en avoir la volonté et de s'en donner les moyens.

Les drones sont des automates et en tant que tels ne peuvent se passer de réseau et de systèmes informatiques, de liaisons de données, de stations sol et aéroportées avec la présence, encore pour longtemps, de l'homme dans la boucle. Ils pourraient représenter une extension dans la troisième dimension de l'Intranet terrestre avec l'avantage, jamais démenti dans les guerres, d'être capables de tenir " les points hauts " sans jamais être coupés du sol.

Malgré la haute technologie des drones, leur usage et leur contrôle ne sont pas toujours aisés, ils présentent certaines vulnérabilités qui fragilisent le réseau et la continuation correcte de mission, tels que des fautes, des erreurs de fonctionnement inattendues, des pannes matériels simples ou multiples, des attaques matérielles et logicielles telles qu'elles sont les nouvelles cibles

des forces ennemis et hackers-successivement.

C'est sur le thème " Contrôle d'un groupe d'avions sans pilote UAVs " que porte notre recherche de défi, afin de traiter différentes problématiques des drones.

Dans notre démarche, nous proposons le plan suivant : Chapitre 1 : présente des généralités sur les drones, son but est à la fois d'expliquer ce que sont les drones, de démontrer leur potentiel considérable ainsi d'exposer les notions les plus élémentaires.

Chapitre2 : " Sûreté et fiabilité dans la coopération des UAS" présente les notions informatiques des drones, tel que décris en premier lieu l'architecture des UAS, la communication, les défaillances et fautes des drones, leur coopération, -en suite- les notions de consensus et d'accord approximatif, et termine par une simple description du récepteur GPS, notions de sûreté et de fiabilité ainsi que l'attaque spoofing(usurpation) GPS.

Chapitre3 : " Etat de l'art" qui présente quatre problématiques qui n'ont été jamais traitées auparavant. Par la suite investigue les travaux déjà effectués et qui sont reliés ou proches à ces quatre problématiques.

En clôture, le chapitre 4 : "Proposition et validation" qui expose les solutions que nous avons proposées, et les démonstrations mathématiques afin de les valider.

# 1

# Généralités sur les drones

## 1.1 Introduction

Une nouvelle page de l'histoire de l'aérospatiale est incontestablement en train de s'écrire avec l'apparition de drones ou UAVs.

Dans le présent chapitre nous allons présenter les drones, leur historique, formes et classes, démontrer leur potentiel considérable. Nous définissons en clôture le système de positionnement GPS qui est une notion primordial dans notre mémoire.

## 1.2 Historique

Ce sont les lourdes pertes subies pendant la seconde guerre mondiale par les aviations d'observation de chacun des antagonistes qui suscitèrent l'idée d'un engin d'observation militaire sans équipage (ni pilote, ni observateur).

Les premiers drones apparurent en France dans les années 1960, tel le R20 de Nord-Aviation, dérivé de l'engin cible CT20.Mais les exemples significatifs d'une utilisation opérationnelle des drones sont encore peu nombreux.

Pendant la guerre de Vietnam, les Américains ont utilisés des drones (Firebee) pour localiser les rampes de lancement des missiles sol-air Soviétiques " SAM-2 " : 3500 missions furent recensées. Plus tard, en 1991, lors de la guerre du Golfe, ils ont fait appel aux drones (Pioneer) pour la surveillance jour/nuit, l'acquisition des objectifs, et les réglages de l'artillerie. Dans ce même conflit, les Britanniques et les Français commencèrent à se servir des drones.

De leur côté, les Israéliens ont pu saturer les défenses aériennes le long du canal de Suez lors de la guerre de Kippour (1973) grâce à un nombre élevé de drones bon marché. Plus tard, ils ont détecté et " leurré " par le même moyen les batteries Syriennes anti-aériennes. Aujourd'hui, ils utilisent couramment les drones dans la lutte anti-terroriste.
D'une façon générale, les spécialistes considèrent que les drones ont pu vraiment démontrer leur capacité opérationnelle d'observation aérienne (renseignement), sur les trois récents théâtres d'opérations qu'ont constitué les conflits en ex-Yougoslavie, en Irak, et en Afghanistan. La France a notamment acquis une expérience opérationnelle, en déployant des drones de reconnaissance tactique (CL289 et crécerelle).
C'est encore un drone(Hunter) qui a successivement assuré la surveillance des réunions du G8 à Evian en 2003, ainsi que celle de cérémonies de célébration du 60ème anniversaire du débarquement allié en Normandie en 2004.
Les drones ont été ensuite de tous les conflits et opérations de maintien de la paix. Ils ont notamment été utilisé au Kosovo ou au Tchad, lors des attaques aériennes américaines au Pakistan ou contre la piraterie maritime, par les Américains qui l'ont introduit en 2009. Les drones sont développés et déployés par de nombreux pays dans le monde[4].
L'Algérie est l'un des pays qui ont pu en 2011 construire le premier drone algérien qui s'appelle AL fajer L-10 de type HALE (Haute Altitude-Longue Endurance) pouvant voler jusqu'à 7 000 m d'altitude avec une autonomie de 36 heures.

## 1.3 Définition d'un drone (UAV)

Les drones sont des aéronefs capables de voler et d'effectuer une mission sans présence humaine à bord. Cette première caractéristique essentielle justifie leur désignation de Uninhabited (ou Unmanned) Aerial Vehicle (UAV). D'origine anglaise, le mot " drone ", qui signifie " bourdon ", ou " bourdonnement ",est communément employé en Français en référence au bruit que font certains d'entre eux en volant !
La désignation de drone ne recouvre qu'un véhicule aérien. Celui-ci n'est en fait que l'un des éléments d'un système, conçu et déployé pour assurer une ou plusieurs missions. C'est la raison pour laquelle les spécialistes parlent de " systèmes drones "[1].

FIGURE 1.1 – Avion sans pilote

## 1.4 Formes des drones

De quelques centimètres à une quarantaine de mètres, de quelque dizaines de grammes à une quinzaine de tonnes, les drones sont de taille et de masse essentiellement variable ; c'est, d'une part, les performances requises par la mission et, d'autre part, la nature et l'importance de la charge utile, qui sont déterminants.

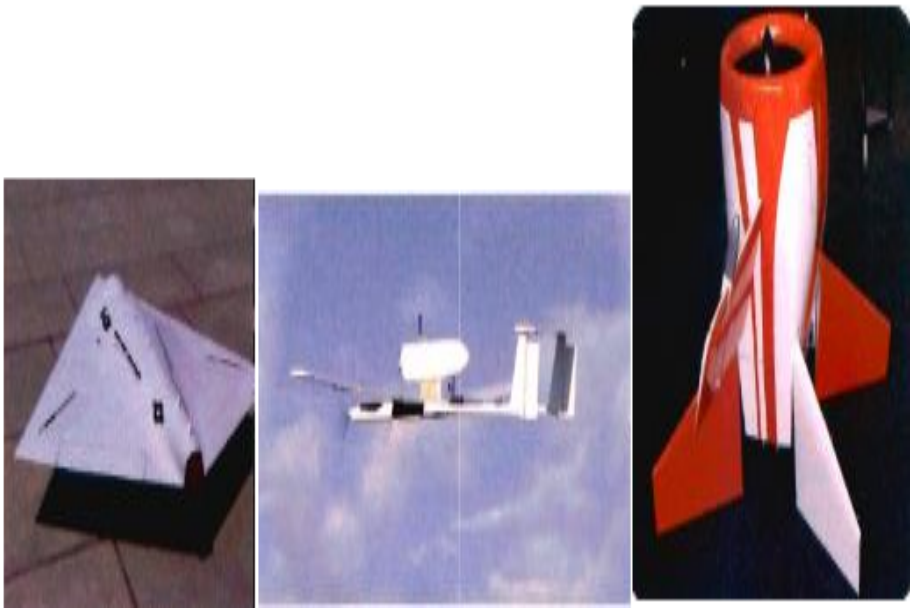

FIGURE 1.2 – Formes des drones

La plupart des drones sont comparable aux avions, sauf que leur forme n'est pas dictée par celle d'un fuselage devant abriter au moins un pilote (de façon confortable). Il existe de nombreuses configurations de drones, très différentes les unes des autres pratiquement une pour chaque machine et dont certaines sont novatrices[1].

## 1.5 Les composants des drones

Les éléments composant un drone répondent aux mêmes fonctions que sur un avion ou un hélicoptère[1]. On trouve généralement les composants suivants :

– La cellule : porte et abrite la charge utile, le moteur et les systèmes de bords ainsi que le carburant.

FIGURE 1.3 – Cellule d'un UAV

– La sustentation est en général assurée par une voilure fixe (comme un avion) ou tournante (comme un hélicoptère). Cette dernière est choisie pour certaines missions spécifiques, requérant le vol stationnaire, par exemple pour des relevés devant s'effectuer de façon immobile (inspection de gros ouvrages d'art, photogrammétrie...), ainsi qu'une grande souplesse de manœuvre (évolutions autour de l'objectif) ; ou encore nécessitant l'appontage sur un bateau (surveillance maritime ou mission de recherche et sauvetage...).

– La motorisation du drone : Dictée par la mission qui lui est attribuée ; elle est déterminée par les dimensions de la machine et sa masse, l'altitude et la durée de son vol. On retrouve sur les drones toute la palette de la motorisation possible pour les avions, auxquelles s'ajoutent pour les petits drones et ceux dotés d'une voilure tournantes les moteurs électriques.

– Systèmes de bord : Les systèmes de bord sont essentiels car ils assurent le pilotage et la navigation de façon automatique. Ils peuvent fonctionner en parfaite autonomie ou selon des ordres émis depuis le sol, par un opérateur chargé de conduire la mission.

– Le système de conduite de vol : asservit plusieurs équipements entre eux : les capteurs (mesurant les paramètres du vol) ; des calculateurs, respectivement dédiés au pilotage et à la navigation et d'où sont émis les ordres de pilotage ; une mémoire (contenant la programmation du vol et, éventuellement des critères de décision préalablement enregistrés), et les actionneurs (agissant sur les commandes de vol).

– charge utile : proprement dite constitue l'un des éléments fondamentaux du système drone car c'est elle qui permettra, en parfaite adéquation avec le vecteur aérien, de réaliser la mis-

sion. Souvent placé en dessous de la structure, elle consiste en un ensemble d'équipement pouvant assurer trois fonctions essentielles :

1. L'acquisition des données : par des capteurs, électro-optique (caméra visible ou infrarouge) ou électromagnétique (radars), capable de restituer des images, ou tout autre capteur spécifique (par exemple bio-senseur sorte de capteurs chimique/biologique capable de détecter la pollution et les radiations).

2. Un éventuel traitement à bord des données : par des calculateurs afin de les rendre directement et plus rapidement exploitables, en vol (mise à un format spécifique) ou au sol (restitution d'images ou interprétation par l'opérateur), et suivi si nécessaire, de leur fusion/compression.

3. Une possible sélection à bord des informations utiles qui seront transmises vers le sol, requérant une pré-analyse des données acquises effectuée par des processeurs, par comparaison aux critères entrés en mémoire. L'ensemble de ces données peut aussi être enregistré à bord, pour envoi différé ou pour dépouillement ultérieur après retour au sol.


FIGURE 1.4 – La charge utile

– Un système spécifique produit l'énergie électrique nécessaire au fonctionnement de l'ensemble des équipements embarqués. Comme sur un avion, cette énergie est obtenue par transformation de l'énergie mécanique prélevée sur la partie tournante du moteur.
Certaines charges utiles requièrent une grande quantité d'énergie, qui s'ajoute à celle consommée par les autres équipements. Ce paramètre peut devenir dimensionnant pour le drone et sa mission.

– Un système de transmission de données entre le drone et le sol : Achemine à la fois les informations venant du sol(en temps réel) et les informations envoyées par le drone (en temps réel ou différé). Cette transmission s'effectue par télécommunication, soit en porté

optique (ligne directe) sur de courte distance jusqu'a 150km ; soit en utilisant un relais, ce dernier pouvant être un satellite ou un autre vecteur aérien (avion ou drone).
Dans les deux cas, la densité des données transmises (malgré fusion et compression) peut nécessiter de grands débits. En outre, la haute définition, en matière d'imagerie n'est pas compatible avec une vitesse de transmission trop élevée.
La transmission par Laser constitue une perspective qui demandera, d'une part, une connaissance précise de la position du drone, d'autre part, une parfaite stabilité du dispositif émetteur et ce, de façon à assurer avec précision et de façon constante la projection des faisceaux.

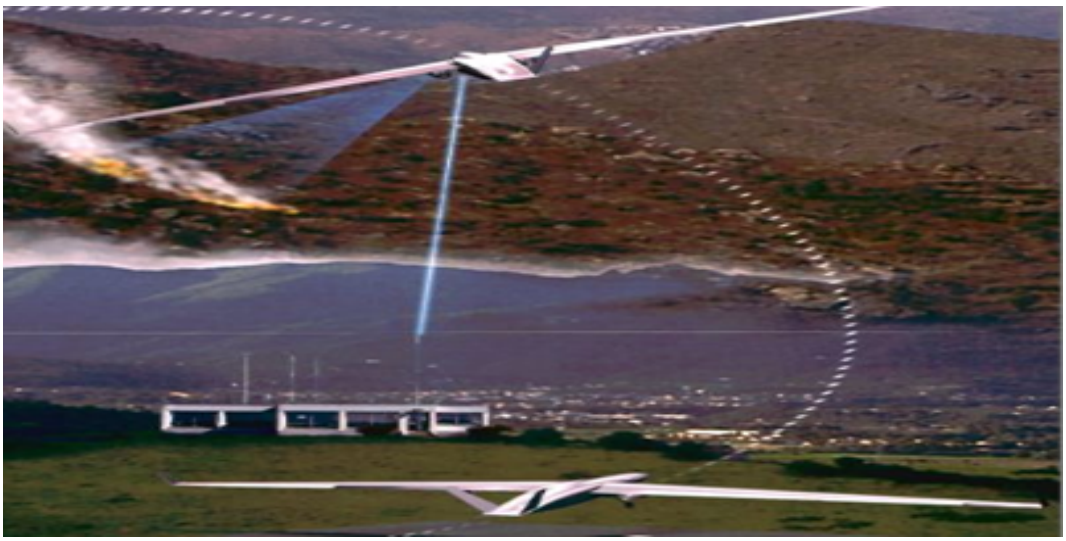

FIGURE 1.5 – Transmission par Laser

– Une intelligence embarquée : donne au drone ses différents degrés d'autonomie, en matière de pilotage et pour la réalisation de sa mission.
Cette intelligence est implantée au moyen de calculateurs de bord dédiés, et permet de gérer le système de conduite de vol, d'une part, et la charge utile d'autre part, ainsi que les bases de données spécifiques auxquelles sont comparées les informations acquises par le drone.
– Les logiciels : mis en œuvre revêtent une importance capitale, notamment dans la rapidité et la stabilité de leurs algorithmes.

– Un système de gestion spécifique à l'armement embarqué : sont nécessaires dans certains drones militaires qui peuvent être armés afin de remplir des missions d'attaques au sol.

## 1.6 Le système drone

La mise en œuvre d'un ou plusieurs drones fait appel à différents éléments, constituant un système de drones. Ce système a deux composantes qu'on détaillera dans le prochain chapitre :

- **Un segment air** : lui-même composé du drone, de sa charge utile et de son système de transmission (Composants du drone).

- **Un segment sol** : constitué d'un ensemble de matériels, mis en œuvre par un ou plusieurs opérateurs humains, ayant un degré d'intervention plus ou moins élevé [3].


FIGURE 1.6 – Station au sol

On distingue encore dans la composante sol deux catégories de matériels [3] :

- Ceux ayant trait au lancement et la récupération des drones (catapulte, filets, etc.), et auxquels s'ajoutent les moyens techniques nécessaire à la maintenance et reconditionnement des drones, exactement de la même façon pour l'exploitation des avions.
- Ceux ayant trait à la conduite de la mission : ils permettent d'assurer au sein d'une station sol les fonctions suivantes :

1. La gestion de vol et de navigation(en temps réel si le drone est piloté de sol, ou en simple surveillance s'il est autonome).
2. La réception des données envoyées depuis le drone et éventuellement le décryptage.

3. L'analyse et l'interprétation des données leur éventuelle retransmission à un centre de décision ou d'intervention, ainsi que leur enregistrement.

FIGURE 1.7 – Station de réception de données Speewer.

La station de contrôle et de réception des données peut s'envisager dans l'avenir, étant elle même aéroportée (avions gros porteurs ou de combat).
L'ensemble de ces composantes interviennent évidemment dans l'évaluation des coûts d'un " système drones ".

## 1.7 Comment utilise t-on un drone ?

Le départ d'un drone peut s'effectuer depuis une plateforme terrestre ou maritime, ou encore depuis un autre véhicule aérien, il peut être lancé à la main (c'est le cas des drones de petites dimensions) il peut être catapulté ; enfin, il peut décoller depuis une piste, soit en mode télécommandé par un pilote au sol, soit de façon entièrement automatique.

C'est une fois arrivés sur la zone de mission (après une navigation automatique) que les drones se distinguent par leur degré d'autonomie. Certains nécessiteront des interventions humaines, notamment face à des situations imprévues (dues à la mission ou au vol), d'autres seront dotés d'une intelligence embarquée leur donnant une autonomie de décision et donc, d'action ou de réaction[3].

Pour la récupération du drone, plusieurs solutions sont possibles : faire revenir celui-ci à l'endroit d'où il est parti et le faire atterrir(en mode automatique ou télécommandé), ou le faire " se poser " à un endroit spécifié à l'avance. En général, cette dernière pratique s'applique à ceux qui sont partis d'une catapulte et qui ne sont pas dotés de terrain d'atterrissage. La séquence

consiste après réduction de l'altitude et de la vitesse, à ouvrir un ou plusieurs parachutes, puis à déployer des ballons gonflables (" airbags ") sous la structure. On peut également récupérer le drone dans un filet, ce qui élimine tout système embarqué pour atterrissage [2].

FIGURE 1.8 – Lancement et récupération d'un drone.

## 1.8 L'utilité des drones

Les principales qualités des drones découlent du fait qu'ils sont "sans pilote ". Cette caractéristique essentielle, supprime toute notion de risque pour l'équipage, notamment dans le domaine militaire(dangerosité des missions), mais également pour toute les missions considérées comme physiologiquement difficiles ou pénibles pour l'homme(accès à haute altitude, long temps passé sur site...).En outre, là ou il faut 2 à 3 hommes pour réaliser des tâches multiples à bord d'un avion (pilotage, mise en œuvre de la charge utile, analyse et décision, transmission radio...) de même que là ou il faut compter plusieurs équipages techniques pour qu'un avion d'observation soit parfaitement opérationnel (compte-tenu des repos et congés réglementaire, des maladies, etc.), le drone est économique en personnel navigant. Néanmoins, les premières " expériences " ont montré que l'exploitation d'un drone mobilisait beaucoup de monde au sol[2].

FIGURE 1.9 – Utilisation militaire des drones

Enfin, l'entraînement et les qualifications des opérateurs au sol sont moins complexes et moins coûteux.
La deuxième qualité essentielle d'un drone est sa souplesse d'opération (envoi, récupération, réutilisation), et son efficacité. On citera par exemple : l'accessibilité des sites à survoler ; la qualité de l'observation (logiquement meilleur à 5000 m d'altitude qu'a 800km par satellite...) ; le temps élevé passé sur zone ; la transmission des données en temps réel ou peu différé. Cette dernière qualité permet l'exploitation des informations dans un délai très court.
Enfin, des drones de même modèle peuvent constituer un vecteur commun à plusieurs missions différentes mais faisant appel aux mêmes équipements de base (observation et surveillance aériennes) et, surtout au même sous- système sol.
De même des drones de différents types peuvent utiliser la même station sol. Ils peuvent par exemple être rentabilisés sur plusieurs saisons pour différentes missions civiles (surveillance des feux de forêts, du trafic routier, du trafic maritime côtier...) c'est un facteur important d'amortissement et donc de rentabilité de ces moyens aériens.

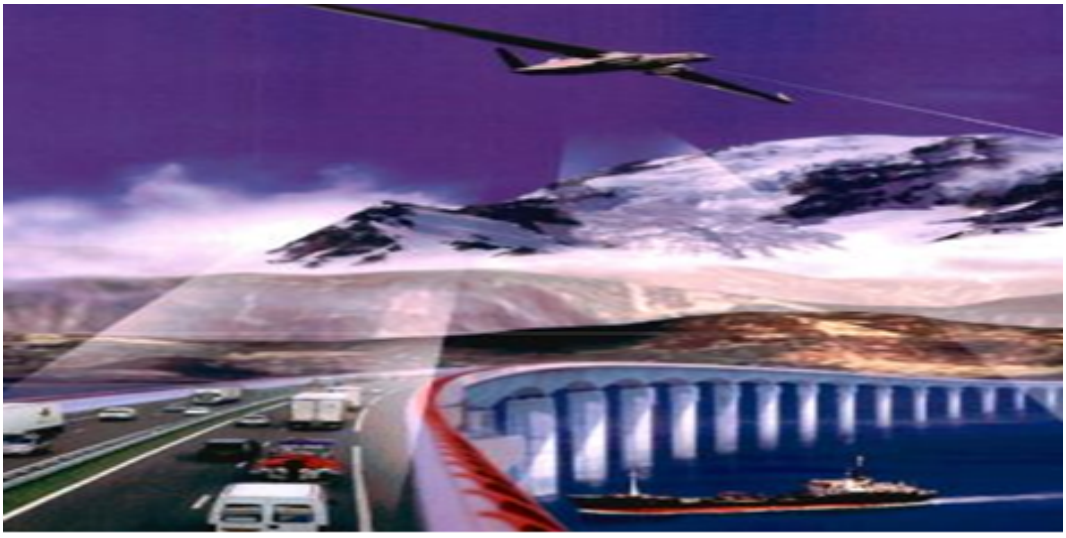

FIGURE 1.10 – Observation et surveillance aérienne.

## 1.9 Classes de drones

La classification la plus logique des drones adopte pour critères principaux la taille ou les performances (essentiellement la porté et l'altitude d'opérations) ; éventuellement le type de mission si celui-ci implique une spécificité particulière (utilisation maritime par exemple)[3]. On distingue :

### 1.9.1 Les drones miniatures

Cette catégorie recouvre globalement tout les drones dont l'envergure est inférieur à 50 centimètres, cette dernière pouvant descendre jusqu'à quelque cm seulement. Elle se divise elle-même en deux familles :

- Les mini drones : de taille comprise entre 15et 50cm, ils sont dédiés au recueil et à la transmission d'images, de jour comme de nuit, ils sont ainsi très prometteurs.
- Les micro drones : leurs tailles est en dessous de 15cm, ils pèsent environ 50grammes, pour une vitesse de croisière de l'ordre de 50km/h, une autonomie d'une vingtaine de minutes et un rayon d'action d'une dizaine de kilomètres.

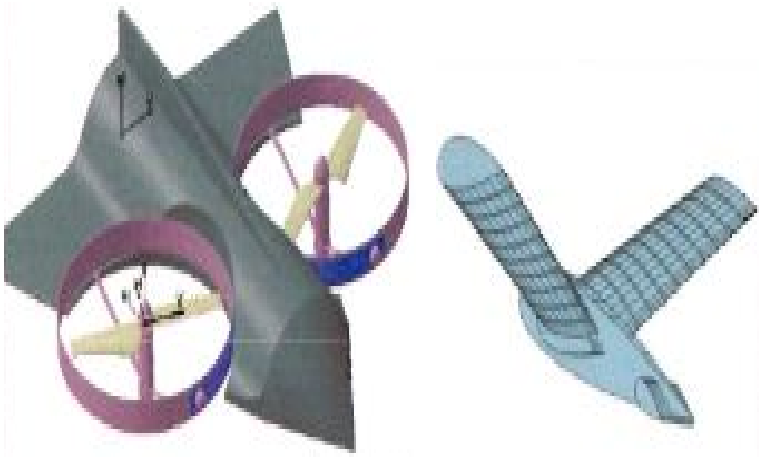

FIGURE 1.11 – Drones miniatures.

### 1.9.2 Les drones de court rayon d'action

Dits encore drones TCP (Très Courte Portée), ou dans le jargon militaire "drone du capitaine", ces drones sont destinés à " voir de l'autre côté de la colline", soit à quelque kilomètres. D'envergure de 0.5 à 2 mètres, et généralement à voilure fixe, ils ont une faible vitesse (quelque dizaine de km/h).

### 1.9.3 Les drones tactiques à moyen rayon d'action

Pouvant être doté de vitesse lente (150km/h) ou rapide (700km/h), ces drones représentent la catégorie intermédiaire, avec des performances variées. Avec une masse au décollage qui reste inférieure à une tonne, leur rayon d'action s'étend de 30 à 500 km, leur altitude de vol de 2000 à 5000mètres, et leur endurance, de 2 à 8 heures.

### 1.9.4 Les drones à voilure tournante

Cette catégorie se distingue par son mode de sustentation mais recouvre des tailles et des performances de drones très variées.


FIGURE 1.12 – Drones à voilure tournante.

### 1.9.5 Les drones de longue endurance

Avec des durées de vol comprises entre 12 et 48 heures, on entre ici dans la catégorie des "grands" drones, dont la taille est essentiellement dictée par une charge utile lourde et une quantité élevée de carburant nécessaire à la mission. Cette catégorie se divise elle-même en deux parties, en fonction de l'altitude de vol des machines : comme pour les avions, plus on vole haut plus on va vite, plus on parcourt de la distance .On distingue ainsi deux types :

#### 1.9.5.1 Les drones "MALE"

L'altitude de vol est, pour cette catégorie compris entre 5000 et 12000mètres, ce qui permet de parcourir jusqu'à 1000km. Les MALE opérationnelles les plus connus sont le Hunter et le Heron d'Israel Aircraft Industries ainsi que le Predator Américain.

#### 1.9.5.2 Les drones "HALE"

On atteint dans cette catégorie les dimensions d'un avion de transport de la classe de l'Airbus A320,pour des autonomies de plusieurs milliers de km(10000km et plus) parcourus en volant largement au dessus des trafics aériens courants, tant civils que militaires(jusqu'à 20 000m d'altitude).
Les capacités de ces drones HALE sont à rapprocher et à comparer à celle des avions pilotés de type de l'avion espion U2 ou des avions de renseignement électronique Sigint, ainsi qu'à celle des satellites d'observation ou d'alerte.

### 1.9.6 Les drones de combat (UCAV)

Les UCAVs sont conçu comme des véritables avions de combat non pilotés. Il s'agit bien sûr de drones à vocation offensive, dotés de missiles ou de bombes guidés et chargés d'effectuer des missions d'attaques au sol très précises voire, à plus long terme, de défense aérienne et de police du ciel.


FIGURE 1.13 – Drone de combat UCAV.

## 1.10 Système de positionnement GPS

Le système GPS permet de calculer la position tridimensionnelle (latitude, longitude, et altitude) d'un utilisateur, qui est dans notre cas un UAV, de manière continue et instantanée en tout endroit sur terre. Lorsqu'un récepteur GPS est mobile, sa vitesse et la direction de son mouvement peuvent être déterminées. De plus, le système GPS fournit une information temporelle, ainsi, un utilisateur peut associer un indicateur de temps à toutes les informations qui sont recueillies.
Conçu à l'origine pour des fins de navigations militaires, le système GPS a vite été utilisé pour des fins de localisation et de positionnement tant pour les civils que les militaires. Le Système GPS est une solution potentielle à presque toutes les applications nécessitant une référence spatiale (coordonnées géo référencées) telle que la circulation spatiale[5].

### 1.10.1 Description du système

Les 24 satellites NAVSTAR sont répartis sur 6 plans orbitaux (4 par plan) dont l'inclinaison est de 55° par rapport à l'équateur terrestre (figure I.14). Ils orbitent à une altitude de 20180 Km au-dessus de la surface terrestre (soit 3 fois le rayon de la Terre), ce qui leur confère une période de révolution d'environ 12 heures (ces satellites voyagent aux vitesses approximatives de 11600 Km à l'heure). Cette altitude élevée permet à des utilisateurs très éloignés

(plusieurs centaines de kilomètres) de capter simultanément les signaux des mêmes satellites. Au minimum, 4 satellites (parfois même 12) sont toujours disponibles en tous points du globe, 24 heures par jour, indépendamment des conditions météorologiques. Chaque satellite possède un oscillateur qui fournit une fréquence fondamentale de 10,23 MHz calibrée sur des horloges atomiques. L'émetteur génère deux ondes (L1 et L2) de fréquences respectives 1575,42 MHz et 1227,60 MHz. Il transmet régulièrement des signaux horaires, la description de l'orbite suivie (éphéméride) et diverses autres informations.

FIGURE 1.14 – Les 24 satellites NAVSTAR.

### 1.10.2 Les erreurs de positionnement GPS

Bien que la position soit donnée avec une grande précision, il faut tenir compte des erreurs du système GPS qui principalement à l'origine de :

- Freinage des ondes électromagnétiques dans l'ionosphère (5 à 100 Km d'altitude) ;
- Freinage des ondes électromagnétiques dans la troposphère (0 à 50 Km d'altitude) ;
- Erreur de synchronisation des horloges des satellites et du récepteur GPS ;
- Plus diverses raisons comme l'effet relativiste, réflexion des ondes etc.
- Le relief ainsi que la végétation perturbent la réception du signal ;
- Le nombre de satellites en visibilité et leurs répartitions dans le ciel ont une influence sur la précision de la position comme le montre les figures suivantes ;

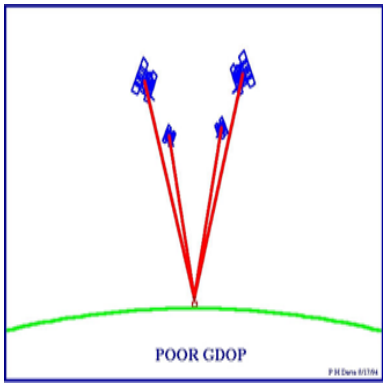


FIGURE 1.15 – "Mauvaise géométrie" ; incertitude plus grande.

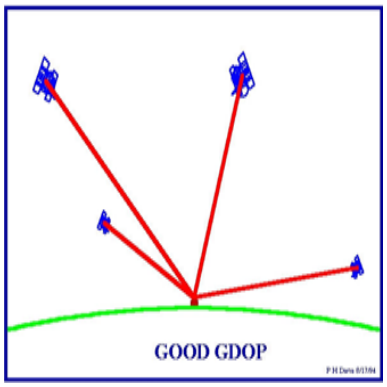


FIGURE 1.16 – "Bonne géométrie" ; incertitude réduite.

## 1.11 Conclusion

Dans ce chapitre on a pu donner quelques généralités sur les drones, leurs formes et classes, leurs domaines d'application ainsi que la façon de les utiliser.

# 2

# Sûreté et fiabilité dans la coopération des UAS

## 2.1 Introduction

Au cours de ces dernière années, il ya eu un intérêt significatif dans la conception des systèmes qui utilisent plusieurs agents autonomes coopératifs pour exécuter une mission. Dans des conditions défavorables, les capacités des véhicules individuels peuvent être réduite, ce qui compromet le succès des missions et risque la sécurité à proximité des populations civiles. Le présent chapitre s'articule comme suit : nous décrivons en premier lieu l'architecture des UAS, la communication, les défaillances et fautes des drones, leur coopération, en suite nous présentons les notions de consensus et d'accord approximatif, et nous clôturons le chapitre par une simple description du récepteur GPS, notions de sûreté et de fiabilité ainsi que l'attaque spoofing GPS.

## 2.2 Architecture des UAS

La démarche de conception de l'architecture du système a été " diviser pour Reigner ". L'architecture du système est désignée dans la figure 2.1

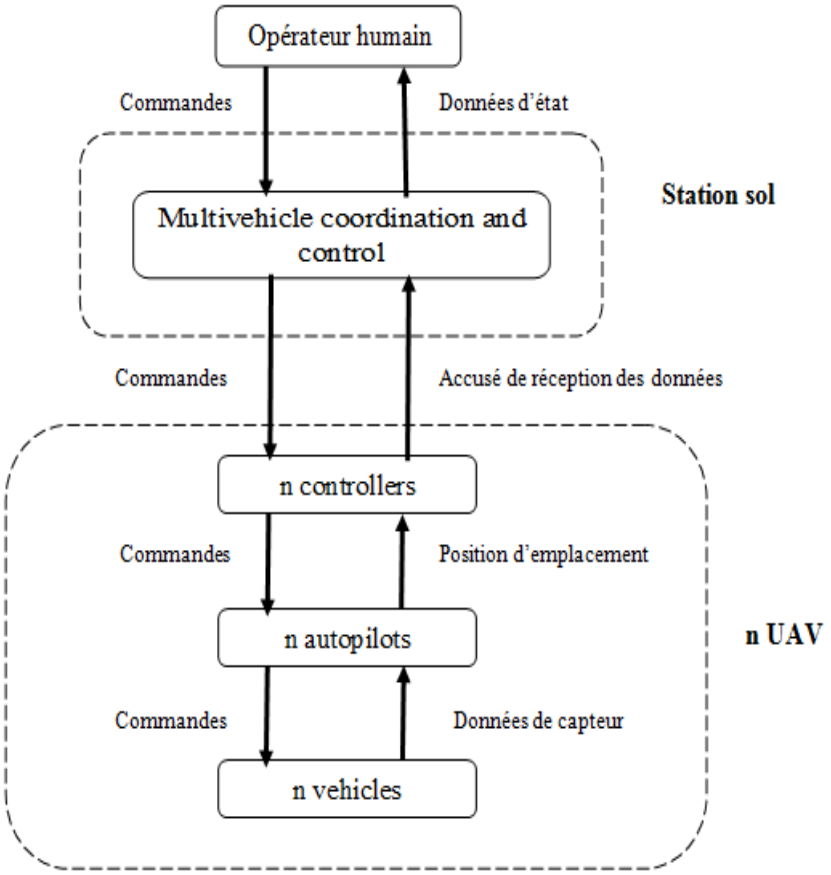


FIGURE 2.1 – Architecture du système.

L'opérateur humain fournira des commandes et des informations depuis le sol. Le bloc appelé n UAV représente les robots que le système est en mesure de contrôler. Toutes les séquences de vol et pilotage de l'UAV sont exécutées par un programme informatique qui est un "auto-pilote". Ce programme est stocké dans un ordinateur de bord qui est le "Cerveau" de toute l'avionique puisqu'il gère tout le système. La station au sol est un ordinateur personnel, où une grande partie de la coordination et du contrôle de groupe d'UAV sera effectuée [6]. L'architecture de la station sol a été divisée en tâches Figure2.2.

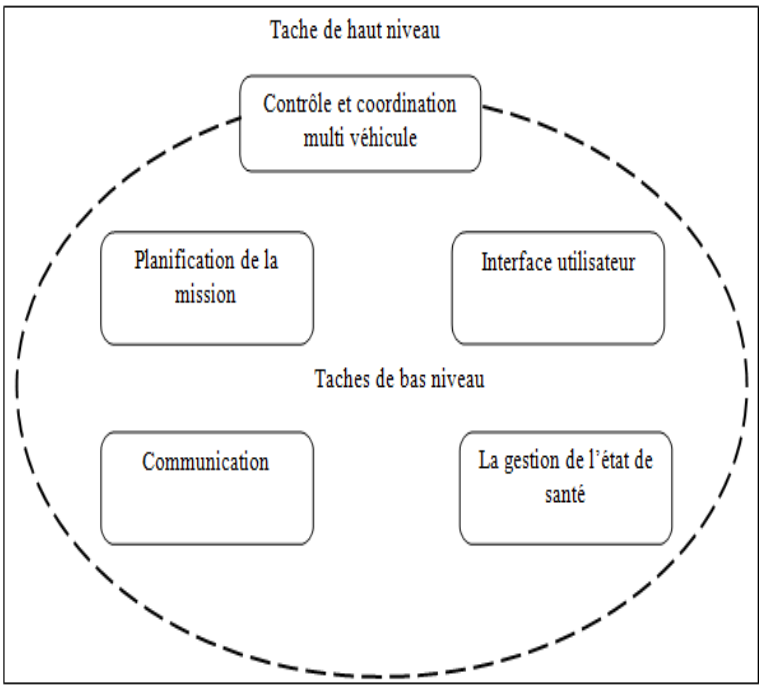


FIGURE 2.2 – Architecture de la station sol.

Le contrôle et la coordination du groupe d'avion sont des tâches de haut niveau sur le système. Selon l'algorithme mis en œuvre il peut être exécuté sur la station sol ou sur les UAVs. Si l'algorithme est exécuté sur une station sol, il sera considéré comme contrôle centralisé, et s'il est exécuté sur les UAVs il sera considère comme contrôle distribué [7].

## 2.3 Communication

La communication est un élément essentiel dans le système. Sans elle nous serions incapables de coordonner toute les tâches. Le système doit maintenir la communication entre la station sol et les UAVs. Les informations reçues de l'UAV seront distribuées entre des blocs de tâches différentes du système. D'autre part le drone recevra l'affectation des tâches à partir de la station sol. Enfin, en fonction de l'algorithme de contrôle du groupe d'avion, les UAVs seront en mesure de coordonner leur mouvements, soit en recevant des informations depuis le sol ou bien depuis d'autres UAVs. La figure suivante illustre la communication dans l'UAS[9].

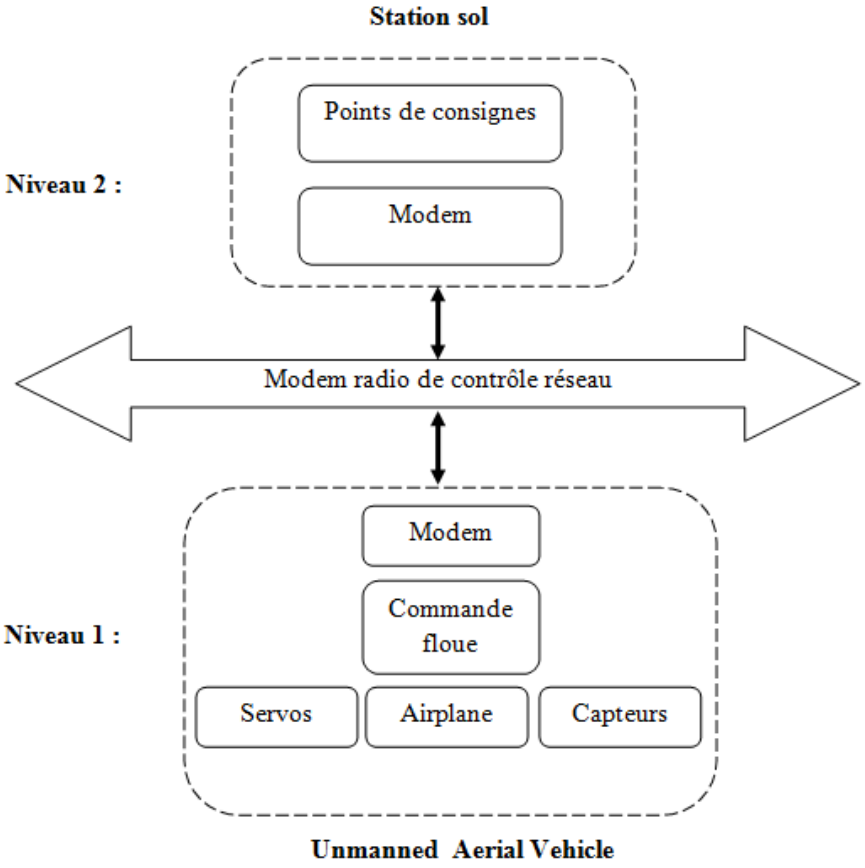


FIGURE 2.3 – Communication dans l'UAS.

### 2.3.1 Exemple de messages échangés dans l'UAS

Les tableaux 1 et 2 décrivent un exemple de type de messages utilisés par la station au sol et le drone pour échanger des informations.

| Message envoyé par la station sol | Description |
|---|---|
| <a1 : do cmd= ‘‘reqGPS’’/> [*checksum*] ~ | Demande d’information sur la position courante de l’UAV |
| <a1 : do cmd= ‘‘reqIMU’’/> [*checksum*] ~ | Demande d’information sur l’attitude courante de l’UAV |
| <a1 : do cmd= ‘‘GPSdes’’ lat= ‘‘xx.xxxxxxxx’’ lon= ‘‘xx.xxxxxxxx’’ alt= ‘‘xxx.xx’’/> [checksum]~ | télécharger l’information des points de passages que l’UAV doit visiter |

TABLE 2.1 – Les messages envoyés par la station sol à l’UAV.

| Message envoyé par l’UAV | Description |
|---|---|
| <a1 : info cmd = ‘‘reqGPS’’/> lat = ‘‘xx.xxxxx’’ lon = ‘‘xx.xxxxx’’ alt = ‘‘xxx’’ bat = ‘‘xxx’’/>[*checksum*] ~ /> [*checksum*] ~ | Informer la position du drone courante et l’état de la batterie |
| <a1 : info cmd= ‘‘reqIMU’’ pit = ‘‘xx.xxxxx’’ rol = ‘‘xx.xxxxx’’ yaw= ‘‘xx.xxxxx’’ bat = ‘‘xxx’’/> [Checksum]~ | Informer l’attitude du drone et l’état de la batterie |
| <a1 : info cmd = ‘‘GPS_IN/>’’ [*Checksum*] ~ | Informer la réception correct des points de passage téléchargés |
| <a1 : info cmd = ‘‘error/>’’ [*checksum*] ~ | Informer la mauvaise réception |

TABLE 2.2 – Les messages envoyés par l’UAV à la station sol.

### 2.3.2 Type de communication de drone

La modélisation du réseau de communication UAV est plus difficile et différente des autres réseaux (réseaux de capteurs et réseaux mobile ad-hoc) en raison de la complexité accrue et énorme disparité des différentes propriétés. Les canaux de type différents, la portée de communication (courtes/longue), différentes exigences de puissance pour différents appareils, différent types de flux de données (commandes/vidéo/audio/image), exigences d’intégrité et de confidentialité, sont quelques une des caractéristiques qui font des exigences de la sécurité d’un UAVNet

différentes des réseaux existants [10],[11].
La figure 2.4 ci-dessous montre un scénario de communication typique d'UAV, qui se compose de plusieurs éléments et différents types de liaisons de communication. Chacun de ces liens transporte différents types d'informations et de données. En règle générale, ce type de réseau dispose de trois types de liens basés sur le type d'informations transmises, à savoir, la communication radio, UAV-UAV, et le lien satellite.
Les liens de communication radio transportent des données de télémétrie, audio, vidéo et des informations de contrôle. En plus de ce que les liens de communication transportent, les liaisons satellites transportent GPS, la météo et les informations météorologiques.

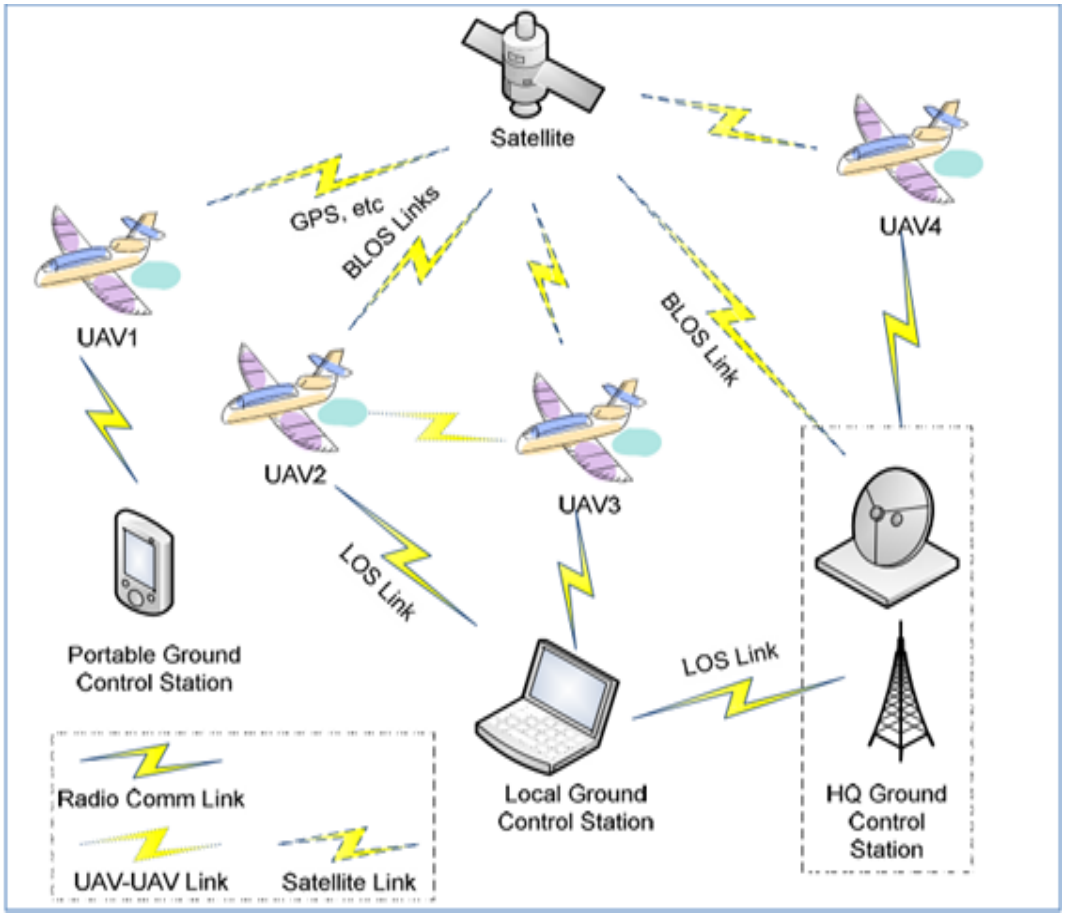


FIGURE 2.4 – Types de communication des drones.

### 2.3.3 Réseau de communication d'UAV

Du point de vue de l'analyse de sécurité et de la menace, il est nécessaire de comprendre qu'un réseau typique UAV n'est pas similaire au réseau informatique traditionnel.
Certain chercheurs l'ont comparé au réseau de capteur sans fil (WSN) et les réseaux ad-hoc (MANET) mobile. Bien que ce réseau porte une ressemblance étroite aux WSNs, comme les deux utilisent des protocoles de communication sans fil, il y a d'autres aspect dans lesquels ils

différent. Par exemple, les besoin en énergie, la quantité d'information menée par les canaux, et le nombre de nœuds dans WSN sont beaucoup plus faibles que dans le UAVNet [11],[12].
En outre, la zone de couverture d'un UAVNet est presque 1000fois plus grande que celle des WSN. De plus, alors que dans les réseaux de capteurs, tous les nœuds transmettent généralement leurs données de capteurs à un nœud central qui communique avec les systèmes externes, dans l'UAVNet, les drones communiquent avec la station de contrôle au sol(GCS) de manière indépendante. Certain chercheurs ont combiné l'application des drones dans les réseaux de capteurs afin d'utiliser la zone de couverture plus grande des drones.

## 2.4 Défaillances des composants d'UAVs

Les défaillances des composants critiques du vol de l'UAV incluent ceux affectant les capteurs, les actionneurs, ordinateurs de bord, le moteur et les surfaces de contrôle. Ces défaillances peuvent compromettre le vol du drone.

## 2.5 Dommages de véhicules

Un environnement dangereux peut endommager un UAV, l'impact des dommages sur l'exécution d'UAV dépend de la sévérité des dommages et de l'efficacité du système de gestion de santé qui surveille l'état de santé des systèmes et s'il ya détection d'un défaut, diagnostique la nature de la condition (recherche et analyse).
Le système de la gestion de la santé est intégré avec le système de contrôle et peut être conçu, pour détecter des pannes, identifier leur origine et permettre le rétablissement, de ce fait en fournissant un certain niveau de la robustesse aux pannes et aux échecs, il vise à maintenir le vol stable et un certain niveau d'exécution malgré les défauts à bord [13].
La plate-forme elle-même peut être endommagée aussi bien que les composants et les systèmes vol-critiques.

## 2.6 Défauts de circulation de l'information

Des communications inter-véhicule sont nécessaires dans n'importe quel effort de collaboration. Les réseaux ad hoc mobiles permettent la transmission sans fil des données dans les environnements dynamiques au-dessus des ondes radio. La topologie de ces réseaux informatiques peut varier avec du temps, avec des nœuds joignant et laissant le réseau selon leurs distances les uns des autres. Chaque UAV peut être vu comme nœud équipé de Tx/Rx sans fil capable de transmettre et de recevoir des paquets de données à et de ses voisins [13]. Le medium sans fil est, cependant, incertain. Les communications sans fil sont sujettes à des intrusions environnementales qui interfèrent les signaux et bloquent leurs chemins, en introduisant du bruit, et brouillage. Un défaut de circulation de l'information est une perte temporaire ou permanente de

l'information entre deux UAVs ou plus, ou entre les UAVs et l'équipe de conduite. Le défaut de circulation de l'information peut provenir d'une panne de communication en raison d'obstacles, de brouillage, une perte d'un nœud, le crash d'un drone, ou en raison de pannes Tx/Rx ou d'ordinateur de bord, par exemple. Si la perte d'informations est permanente et affecte toutes les formes de communications inter-véhicules simultanément, la coopération ne peut être rétablie entre les véhicules [13].

## 2.7 Fautes byzantines

On dit qu'un processus p commet une erreur byzantine s'il se ne comporte pas selon le protocole. Un tel processus est appelé processus byzantin. En particulier les fautes byzantines sont utilisées pour modéliser des comportements malicieux à partir desquels un processus va tenter de faire échouer un calcul.
Nous définissons une faute byzantine comme suit : une faute est dite byzantine si elle présente un comportement arbitraire et imprévisible. En d'autres termes, une faute est dite byzantine si on ne peut connaitre d'avance sa nature ni prédire son occurrence.

## 2.8 La coopération des systèmes d'UAV

Une collection lâche de véhicules qui ont des objectifs en commun est une équipe de collaboration. Si les véhicules travaillent ensemble pour atteindre un objectif commun, ils sont une équipé coopérative. La motivation principale de la coopération d'équipe provient de la synergie possible, comme la performance du groupe attendu dépasse la somme de performance de drone individuel. Cette coopération possible seulement si les drones ont un niveau élevé d'autonomie, devrait tirer parti des capacités suivantes à la disposition du groupe[8].

- **Information globale**
  Chaque drone porte une charge utile lui permettant de détecter l'environnement. En partageant ses informations de détection avec le reste du groupe, via un réseau de communication, toute l'équipe peut agir en fonction de cette situation globale de sensibilisation à la place de l'information locale disponible individuellement. Cette coopération de détection est souvent appelé réseau-centrique.
- **La gestion des ressources**
  Chaque drone peut prendre des décisions concernant son chemin et actions dans un environnement incertain. Fonctionnant indépendamment peut causer que certaines cibles peuvent être sur desservi par quelques uns des drones, alors que d'autres cibles peuvent être mal desservie. Avoir un algorithme de décision coopératif permet une allocation efficace de ressource du groupe sur les cibles multiples.
- **Robustesse**
  Si les drones sont dispersés de façon indépendante sur le terrain, puis une défaillance de

l'un des véhicules peut laisser un sous ensemble de la zone cible non couvert. Grâce à la coopération ; l'équipe peut reconfigurer son architecture de distribution ou essaie de trouver un autre moyen afin de réduire la dégradation des performances à ces défaillances attendues.

## 2.9 Le consensus

Le problème de consensus est défini comme suit : tous les processeurs doivent consentir sur une valeur (binaire ou réelle) représentant la majorité de leurs votes. Le consensus en présence de fautes est difficile, surtout lorsque des hypothèses sont posées sur la nature du système ou sur la nature des fautes à tolérer.

Ce problème de consensus en présence de fautes a été posé, nommé et résolu pour la première fois en 1980 et il a été appelé consistance interactive. En 1982, visant à établir un consensus avec des processeurs fautifs envoyant des messages erronés, les mêmes auteurs ont améliorés, reformulé leur analyse en introduisant le paradigme des généraux byzantins[14].

L'algorithme de consensus en présence de fautes s'est vu attribuer le nom " Byzantine Agreement " et le type de faute avec envoi de messages différents aux différents processeurs s'est connu sous le nom de "Byzantine failure", où un processeur fautif peut envoyer de faux messages pouvant contrecarrer la performance des processeurs non fautifs.

Selon Wei, Beard et Atkins dans [15],"les algorithmes de consensus sont conçus pour être distribués, en supposant seulement les interactions voisin à voisin entre les véhicules. Les véhicules mettent à jour la valeur de leurs états d'informations sur la base des états d'informations de leur voisins." En utilisant une loi de consensus, l'objectif est de faire converger, à une valeur commune, les états de tous les agents dans le réseau. Les algorithmes de consensus ont été étudiés pour résoudre des problèmes de rendez-vous, des problèmes de contrôle de la formation, les réseaux de capteurs.

## 2.10 L'accord approximatif

Le sujet d'accord approximatif n'est pas strictement lié au problème de consensus, mais il a été souvent mentionné. On peut modifier le problème des généraux byzantins de façon chaque processeur émet une valeur réelle plutôt qu'une valeur binaire, et tous les processeurs doivent consentir sur une seule valeur (approchée).
Un algorithme décris par Dolev et al [16] fonctionne par approximations successives : A chaque

tour on s'approche de plus en plus au but avec un taux de convergence garanti.
Les conditions sont similaires au problème de consensus : chaque processeur loyal s'arrête tout en ayant les valeurs de chacun des autres processeurs loyaux.

Pour les systèmes synchrones **le taux de convergence** dépend du pourcentage du nombre de processeurs fautifs : la convergence est garanti lorsque **n>3t**. Pour les systèmes asynchrones la convergence est garantie lorsque **n>5t**.
Les grandes lignes de l'algorithme traitant les systèmes synchrones sont les suivantes : **Chaque processeur envoie sa valeur à tous les autres processeurs, si un processeur fautif n'envoie pas de messages, une valeur, disons '0', est choisie par défaut. Par la suite, chaque processeur exécute une fonction $f_{t,t}$ sur les n valeurs réelles. En général, la fonction f est choisie pour éliminer la plus grande et la plus faible valeur t de la liste et calculer la moyenne du reste. Les processeurs fautifs sont ceux qui ne peuvent converger pour ces valeurs.**

## 2.11 Récepteur GPS d'UAV

Les récepteurs captent les signaux des satellites et calculent d'eux-mêmes la position à partir des données reçues. Le GPS calcule la position par triangulation[4].

### 2.11.1 Principe de la triangulation

En 2 dimensions, le principe de détermination de la position d'un récepteur GPS se présente ainsi :
Le récepteur GPS connait, grâce aux ondes émises par les satellites, leur position précise ainsi que l'heure d'émission des ondes. Il peut donc calculer sa distance, nommée "pseudo-distance", à chacun des satellites grâce à la formule :
(Distance = temps x vitesse).
D = distance
V = vitesse de la lumière
t = temps du signal
Ces distances correspondent aux rayons des cercles S1, S2 et S3. Il se forme un unique point P, point d'intersection des 3 cercles, où se trouve le récepteur GPS comme le montre la figure ci-dessous :

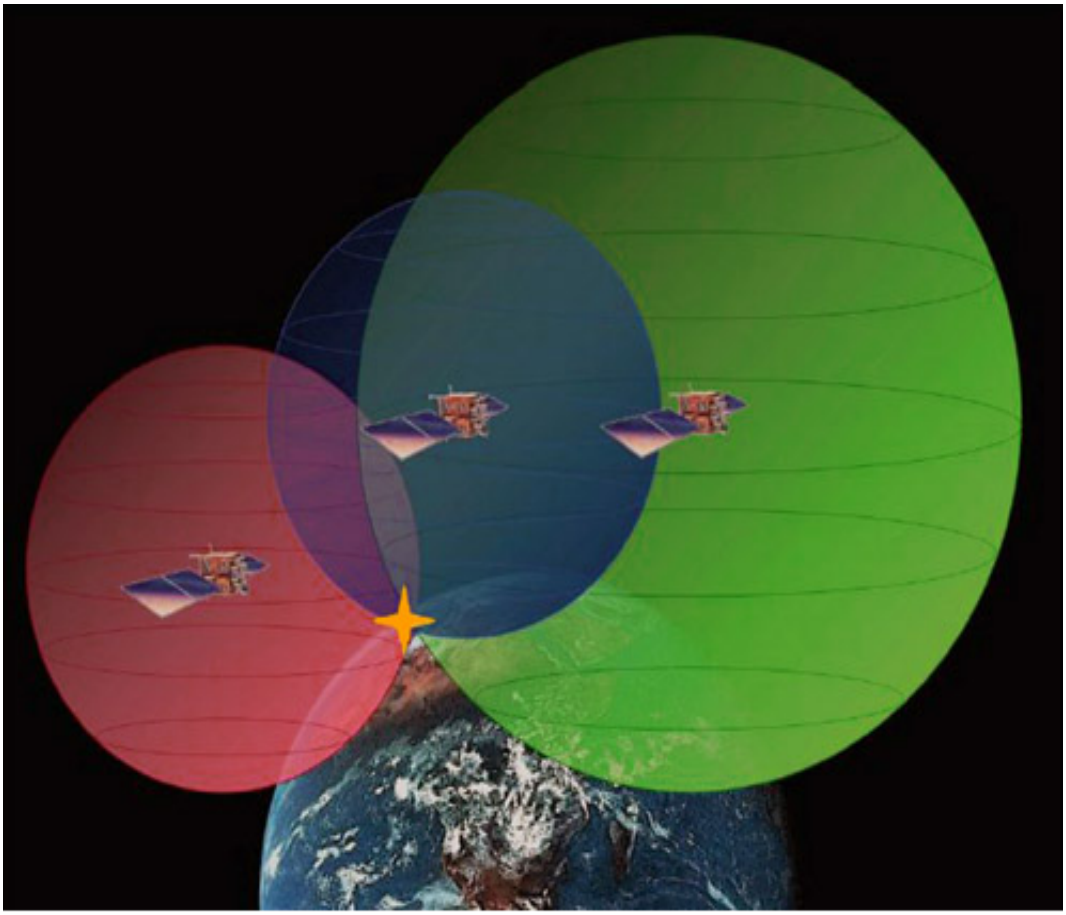

FIGURE 2.5 – Triangulation.

## 2.12 Notions de sûreté et fiabilité

La sûreté dans ce contexte est définie en tant que réduction de l'exposition humaine aux risques.
La fiabilité en tant que l'accomplissement réussie d'une mission coopérative en dépit des événements inattendus[17].

## 2.13 Le spoofing GPS

Le spoofing GPS est l'acte de produire une version falsifiée du signal GPS dans le but de prendre le contrôle de la solution position-vitesse-temps (PVT) d'un récepteur GPS. Ceci est plus efficacement accompli lorsque le spoofer a connaissance du signal GPS tel que vu par le récepteur de la cible de la sorte que le spoofer peut produire une version adaptée du signal falsifié. Dans le cas des signaux militaire, ce type d'attaque est presque impossible par ce que le signal est crypté et donc imprévisible à un soi-disant usurpateur. Le signal GPS, d'un autre côté, est connu publiquement et facilement prévisible[18].

### 2.13.1 Incident d'un drone en Iran

En Décembre 2011, l'Iran a capturé un drone de surveillance de Central Intelligence Agency américaine (CIA) avec des dommages mineurs à l'atterrissage du drone, probablement en raison d'un atterrissage brutal lorsqu'il a été capturé.
Un ingénieur iranien revendiqué dans une interview que "l'Iran a réussi de bloquer les liens de communication du drone aux opérateurs américains" provoquant le drone de passer dans un mode pilote automatique qui se fonde uniquement sur le GPS pour se guider vers son port d'attache en Afghanistan. Avec le drone dans cet état, l'ingénieur iranien a affirmé que "l'Iran a usurpé le système GPS du drone avec de fausses coordonnées, en le trompant , et en lui faisant croire qu'il était proche de la maison et l'atterrir dans les griffes de l'Iran"[18],[19].
Bien que les allégations iraniennes soient très discutables, cet incident a laissé de nombreuses questions sans réponse quant à la sécurité des systèmes GPS dans les véhicules aériens sans pilote (UAV).
Le drone CIA aurait dû se guidant d'après les signaux GPS militaires cryptées, ce qui serait extrêmement difficile d'usurper. Cependant, certains experts ont supposé que le brouillage simultané des signaux militaires et usurpation des signaux civils auraient travaillé si le drone avait été programmé pour se rabattre sur les signaux GPS civils dans le cas où les signaux militaires ont été bloqués[18],[19],[20].

## 2.14 Conclusion

Dans ce chapitre on a décrit l'architecture et la communication des UAS, les différentes défaillances et les fautes que peuvent subir ces systèmes. On a défini en clôture les concepts de coopération, consensus, ainsi que les notions de fiabilité et sûreté des systèmes UAS.

# 3

# Etat de l'art

## 3.1 Introduction

La problématique des UAVs est très vaste, elle touche à plusieurs disciplines, dans ce chapitre nous allons commencer par expliquer l'origine et la motivation derrière ce projet suivi d'une présentation de quatre problématiques, et afin de répondre à ces dernières nous allons investiguer en suite les travaux déjà effectués dans ce domaine.

## 3.2 Motivation

Récemment le contrôle et la coordination d'un ensemble de robots mobiles aérien autonomes UAVs a été accordé une grande attention, par ce que la coopération d'UAVs simple offre plusieurs avantages, tels que la redondance et la flexibilité, et permet d'effectuer des tâches difficiles qui pourraient être impossible pour un seul drone. Il ya beaucoup d'applications intéressantes d'UAV multiples, telle que des missions de surveillance. Les caractéristiques de la simplicité de robots mobiles apportent des applications potentielles ; larges, mais cette caractéristique conduit aussi à des crashs avec une probabilité élevée au cours de la coopération, en particulier dans les environnements difficiles. Etonnamment, seulement quelque recherche considère la tolérance aux pannes d'UAVs, ce qui nous a motivé à faire une étude particulière.

## 3.3 Présentation des problématiques

### 3.3.1 Contexte

Les militaires utilisent les UAVs pour ces types d'opérations soit : la reconnaissance d'un territoire hostile où il est risqué d'envoyer des soldats,soit pour la surveillance d'une zone dont on a le contrôle pour des opérations de maintien de la paix ou bien pour réaliser des missions d'attaques. Dans tous ces cas les UAVs doivent se déplacer dans un milieu hostile pour visiter des cibles prédéterminées.

La figure suivante illustre le cas de la reconnaissance de terrain ennemi par un seul UAV guidé par GPS. Dans ce cas on n'a pas le contrôle de la zone ennemi à visiter et on dispose de peu d'information sur cette dernière.

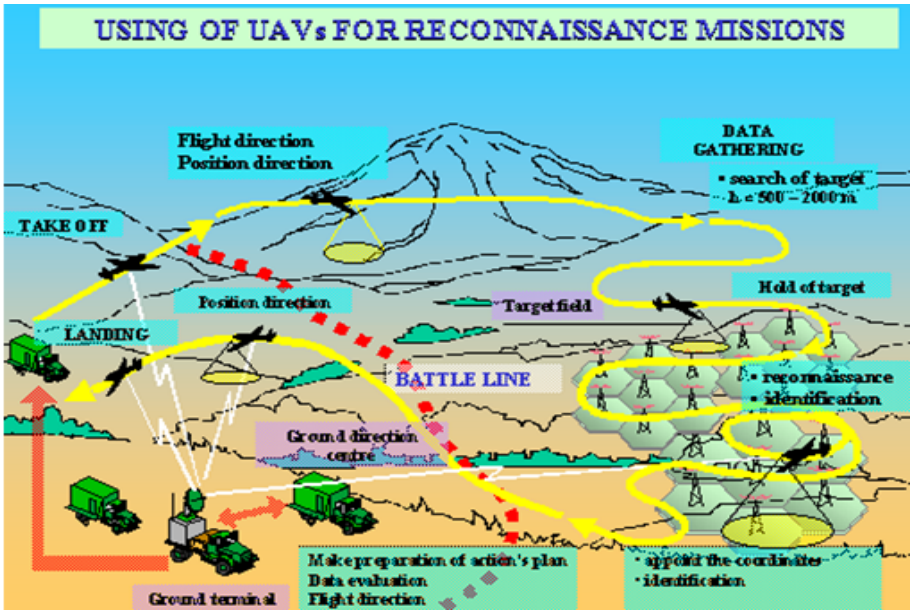


FIGURE 3.1 – Exemple de mission de surveillance.

Les troupes menant la mission se trouvent à gauche de la figure et l'ennemi se trouve à droite de la frontière en pointillée. Avant de s'engager aveuglément dans le terrain hostile, les soldats envoient un UAV qui est catapulté du point " take off " sur la Figure 3.1 et suit une trajectoire qui lui permettra de balayer stratégiquement le terrain ennemi. Durant son exploration, l'UAV est en contact - radio - continu avec le poste " grond terminal " qui collecte les informations. Cette collecte de données permet aux soldats de mieux planifier leurs futures attaques de ce territoire. Le maintien de la communication est primordial.

L'utilisation d'un seul drone pour réaliser une mission militaire est vulnérable, il ne peut pas échapper aux radars et attaques ennemis (détournement, tirs) par sa basse altitude, et la réso-

lution des problèmes de défaillances qu'il peut subir au cours de sa mission sera extrêmement difficile. Cependant, la coopération active de plusieurs UAVs pour la réalisation d'une mission dans un environnement hostile et en présence d'ennemi permet de diminuer les vulnérabilités. Mais les menaces existent toujours.

### 3.3.2 Problématiques

Tous les résultats de la recherche éditée ces dernières années (exemple : rendez-vous coordonné d'UAV, planification cordonnée de chemin, coordination de tâches d'UAVs, etc.) sont basés sur les lieux où les systèmes de navigation fonctionnent dans la normale et les bonnes conditions. Comme il est bien connu, la fiabilité est un souci important dans les systèmes sûreté-critiques comprenant des avions et des UAVs.
les UAVs sont des robots,beaucoup d'entre eux sont équipés du GPS seulement pour la localisation et la navigation. Par conséquent,les comportements arbitraires, les défaillances transitoires ou permanente de GPS, qui peuvent se produire dans certains scénarios, peuvent avoir des effets catastrophiques sur les UAVs pendant la mission du vol.
les problématiques peuvent se résumer à travers les 4 questions suivantes :

1. Si un UAV au cours de la mission perd contact avec la station sol et les satellites GPS alors l'UAV pourra tomber ou être détourné (comme le drone américain) .Y'a-t-il un moyen de récupération de drone ?
2. Dans un groupe d'UAVs coopératif pour réaliser une mission, l'un des UAV perd sa localisation GPS, en possibilité de présence d'UAVs byzantins, y'a t'il un moyen de les tolérer afin de retrouver sa bonne localisation ?
3. Dans un groupe d'UAVs, chaque UAV calcule sa position depuis 4 satellites, si l'un des satellites est byzantin alors l'UAV deviens byzantin, et aura une fausse position, qui, avec cette dernière pourra tomber, ou même tromper ses voisins et ainsi causer des conséquences catastrophique et empêchera la continuation de la mission. Comment pallier à ce problème ?
4. Un groupe de drones coopératifs pour l'attaque d'une cible, sachant que parmi les UAVs on peut y avoir d'UAVs byzantins, qui ont des erreurs sur la position de la cible, ou reçoivent une fausse position de l'adversaire qui fais le spoofing sur les signaux GPS, afin de le tromper et lui donner une position alliée (fausse position), ce qui pose un grand problème. Comment résoudre ce problème ?

Ces problématiques nous motivent à faire une étude sur des récents travaux effectués.

## 3.4 Travaux étudiés

Il y a peu publications étudiées récemment sur la navigation insensible aux défaillances et les méthodes de localisation pour UAVs, des approches intéressantes vont être présentées dans

ce qui suit.

### 3.4.1 Description des approches proposées

#### 3.3.1.1 Première approche

La localisation insensible aux défaillances pour des UAV en utilisant des mesures de la gamme inter-UAV a été au commencement étudiée dedans [21].Puisque seulement une des mesures de distance a été utilisée par la méthode dedans [21], l'exactitude de localisation n'était pas assez bonne. Ce qui a permet d'étudier le problème de localisation à tolérance aux pannes des UAVs avec plus d'informations dans les conditions de vol multi-UAV.
Semblable au principe du GPS, dans lequel l'endroit de l'utilisateur peut être déterminé par des gammes entre les satellites de positionnement et l'utilisateur, l'endroit d'un UAV dans le vol coopératif multi-UAV peut être calculé en mesurant le relatif qui s'étend d'un UAV à d'autres UAV voisins aux endroits connus.
L'approche est basée sur le vol aérien non-piloté de véhicules multiples à une altitude constante, l'auteur a proposé un algorithme coopératif insensible aux défaillances de localisation contre la perte de signal de système de localisation mondial (GPS) due au défaut de fonctionnement de récepteur de GPS. Contrasté aux moyens traditionnels avec l'UAV simple, la méthode proposée est basée sur l'utilisation des mesures relatives de la gamme inter-UAV contre la perte de signal de GPS et plus approprié aux applications d'UAV de petite taille et à moindre coût.
L'auteur a supposé que les UAV multiples, qui sont équipés respectivement d'un récepteur de GPS, volent à une même altitude constante, et le récepteur GPS d'un UAV ne travaille pas correctement en raison d'un échec pendant le vol. En outre, il suppose que l'UAV avec le GPS défectueux peut encore mesurer les distances relatives à d'autres UAV par des mesures de la gamme inter-UAV. Selon la composition des mouvements d'un corps rigide, on sait que dans (un 2D) plan bidimensionnel, l'endroit d'un UAV avec le défaut de fonctionnement peut être calculé en trois autres UAV quelconques qui sont non-situés sur la même droite et dont les endroits sont connus. Semblable au principe du GPS, les trois UAV peuvent être pris en tant que " positionnement des satellites " et de l'UAV avec le défaut de fonctionnement en tant que " utilisateur ". Ainsi, en principe, quand le GPS d'un UAV ne fonctionne pas, il peut encore être situé en les trois autres UAV. Ici, un exemple coopératif de localisation avec quatre UAV est montré dans la Figure.

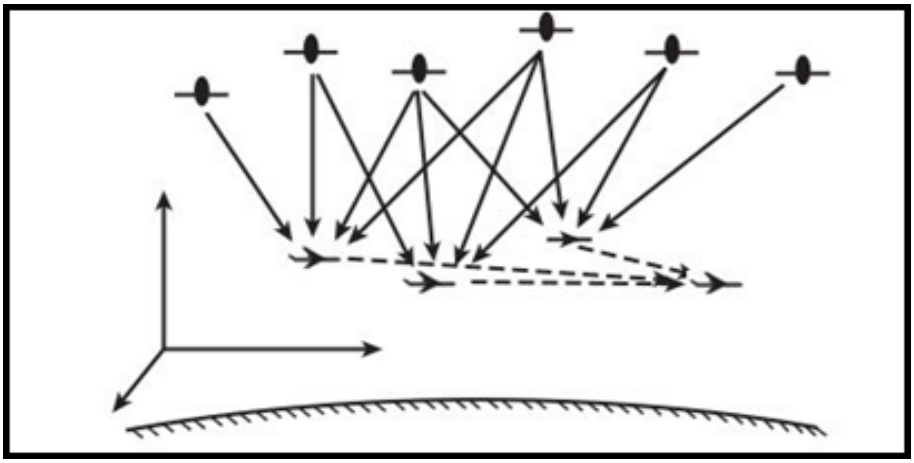

FIGURE 3.2 – Exemple de localisation coopérative avec quatre UAV.

Les bruits et les incertitudes de mesure existent, pour les réduire un filtre de Kalman est appliqué à l'UAV en prenant le résultat de l'auteur comme observation. Le filtre de Kalman est adaptatif. L'auteur a résumé sa méthode de localisation coopérative proposée à travers le Schéma structurel décrit dans la figure 3.3 :

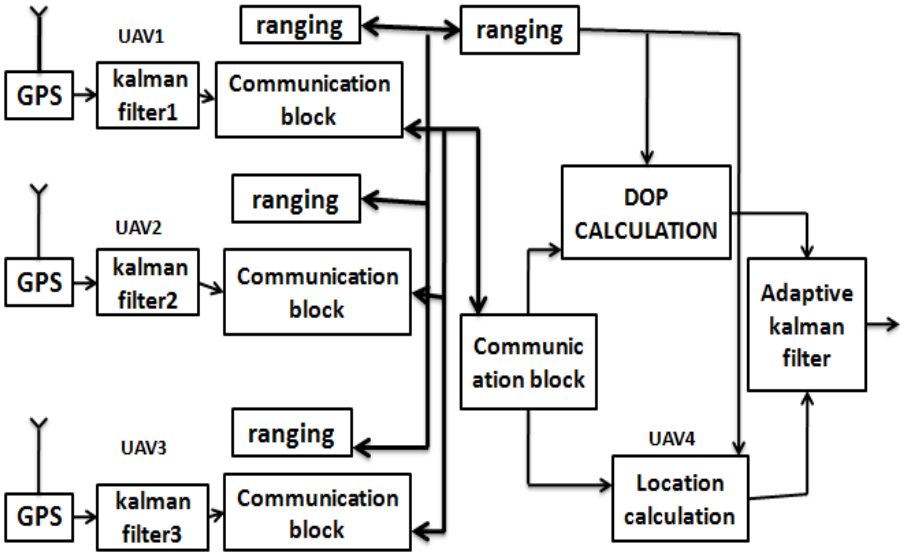


FIGURE 3.3 – Schéma structurel de la méthode de localisation coopérative .

L'inconvénient de cette approche est que, le filtre de Kalman, n'est pas toujours pas assez bon, car ne garantit pas une bonne exactitude de localisation.

#### 3.3.1.2 Deuxième approche

Les deux techniques de base pour la localisation sont la trilatération et la triangulation. Elles reposent sur des propriétés très simples et bien connues des triangles. La trilatération consiste

à s'appuyer sur trois points de référence, c'est à dire des nœuds dont on connaît la position, et sur les distances qui les séparent du nœud dont on cherche à estimer la position. Cette dernière correspond alors au point d'intersection des trois cercles. La triangulation est semblable à la trilatération puisqu'elle s'appuie également sur trois nœuds de référence. La position est calculée à partir de leurs angles d'incidence [22].
La plupart des systèmes de localisation pour les réseaux sans fil reposent sur au moins une de ces deux techniques. Afin de calculer les distances ou les angles, plusieurs paramètres des communications sans fil sont utilisés. Le premier paramètre est le temps de propagation des signaux. En effet, si on connaît l'instant d'émission d'un paquet, en regardant à quel instant celui-ci a été reçu, on peut calculer la distance qui sépare l'émetteur du destinataire grâce au temps de propagation et à la vitesse de propagation.
Lorsque les entités sont parfaitement synchronisées, ce procédé s'appelle Time Of Arrival (TOA). En revanche, lorsqu'il n'y a pas de synchronisation forte, on parle de Time Difference Of Arrival (TDOA) et il s'agit alors d'effectuer le calcul sur plusieurs paquets. Le Global Positioning System (GPS) repose sur cette technique.

#### 3.3.1.3 Troisième approche

L'approche proposée par l'auteur est une exploration de deux algorithmes différents conçus pour la triangulation rapide face à de nombreuses mesures incorrectes. Les mesures peuvent être aléatoirement erronées ou malicieusement convergentes vers une réponse incorrecte. Les deux algorithmes nécessitent un nombre de mesures correctes pour dépasser le seuil de consensus défini par l'utilisateur.
La diffusion de la surveillance dépendante automatique (Automated Dependent Sureveillance Broadcast ADS-B) est l'état de la technologie de pointe utilisée pour la communication inter-avions dans le système d'espace aérien national. Avec beaucoup d'aéronefs équipés d'ADS-B dans une zone, les aéronefs forment un réseau de capteurs diffusant continuellement la position d'aéronef équipé d'ADS-B. L'information de localisation, basée sur la position des nœuds de capteurs, est utile dans les réseaux avec différentes capacités de nœud.
Les réseaux distributifs doivent gérer différents types de nœuds incorrects. L'application de recherche étudiée dans l'approche est le réseau de communication d'aéronefs ADS-B. Le réseau a été choisi en raison des données disponibles (temps précis, position, vitesse) et le fait qu'il existe un certain degré de contrôle du gouvernement sur cette technologie émergente.
Le GPS a apparemment résolu le problème de positionnement pour de nombreux utilisateurs, mais des lacunes existent encore [23]. Une variété de méthodes fondées sur des données de diffusions alternatives a été proposée pour remédier à ces lacunes [24]. La triangulation basée sur les signaux existant doit faire l'objet d'autres mesures robustes pour filtrer les données erronées ou apparemment malveillantes. L'information ADS-B est disponible partout où il ya un important trafic aérien commercial, y compris la plupart des grandes zones urbaines. Au-delà de l'ADS-B,

les idées au sein de cette approche peuvent être appliquées à de nombreuses applications.
L'approche présente deux algorithmes qui sont tolérants aux fautes à la fois des messages de diffusion d'aéronefs malicieux ou accidentellement défectueux. Face à des pannes purement accidentelles des avions, les algorithmes sont en mesure de se terminer correctement même lorsque le nombre d'aéronefs défectueux dépasse de manière significative les avions correcte. Les algorithmes sont également en mesure de se terminé correctement lorsque le nombre de collusion (complicité ou manœuvre) des balises byzantines reste inférieur aux balises corrects.
Les deux algorithmes ont des régimes où l'un est plus efficace que l'autre, selon le modèle des valeurs extrêmes et les besoins des utilisateurs. Le temps d'exécution de chaque algorithme est exploré par rapport aux intrants et au modèle des balises incorrectes.
Plusieurs algorithmes d'estimation de position populaires qui n'utilisent pas de GPS comme infrastructure sont présentés dans [25], [26], [27]. Li et al. Proposent l'utilisation des modèles statistiques robustes de détection des valeurs extrêmes pour réaliser l'estimation de position robuste [28]. Ils proposent une approximation probabiliste à l'approche de moindre médiane des carrés (LMS) [29] afin de contourner la complexité des calculs. Li et al.ont présenté un algorithme glouton pour filtrer les données de l'attaquant sur la base d'une constante erreur quadratique moyenne minimale (MMSE Minimum Mean Square Error ) critères entre les mesures reçues de plusieurs balises [30].
Le problème des généraux byzantins est l'un des scénarios les plus étudiés en informatique [31], [32], [33], [34]. L'article fondateur de Lamport [35] a démontré que le consensus en présence de défaillances pourrait être atteint dans un système distribué synchrone uniquement si le nombre d'agent défectueux était moins d'un tiers d'agents corrects.
L'ADS-B est, à l'heure actuelle, une diffusion non crypté, les aéronefs d'aviation générale peuvent accéder aux messages diffusés par l'avion activé d'ADS-B. Si un aéronef de l'aviation général est équipé d'un récepteur d'ADS-B, il peut théoriquement espionner tout le trafic ADS-B dans la zone de diffusion. Sur la base de ces messages espionnés, il devient possible pour les aéronefs de l'aviation général de trianguler leur positions, tant qu'il y a suffisamment d'avions activant l'ADS-B au sein de leur proximité.
La diffusion ADS-B contient un certain nombre de paramètres différents qui sont actualisés pour chaque nouveau paquet. Les paramètres inclus sont encore en cours de finalisation, mais la position, la vitesse et le temps (basés sur GPS) forment la couche la plus élémentaire [36]. Quand nombreux avions diffusent des informations ADS-B à portée d'un récepteur, ils forment un réseau de capteurs de balises qui peuvent être utilisés par les récepteurs. En combinant l'horodatage et l'information de localisation les récepteurs peuvent trianguler leur propre position dans le réseau de capteurs des avions.

1. **Triangulation**
   Les méthodes de triangulation existantes [37] sont mise en œuvre pour résoudre le problème de positionnement GPS. Ils prennent la position de chaque balise de diffusion (satellite)

avec un horodatage et calculent un temps de trajet entre la balise et le récepteur. Le temps de déplacement est proportionnel à la distance entre deux nœuds. L'intersection de ces 4 sphères peut définir de façon unique un seul point dans un espace tridimensionnel et est utilisé pour définir une position GPS. La triangulation en deux dimensions se fait en utilisant l'intersection de ces trois cercles pour définir d'une manière unique un point unique. Il ya un certain nombre de cas dégénérés où l'intersection ne résulte pas en un point (i.e. deux cercles sont identiques, etc.). La géométrie est représentée sur la figure1.

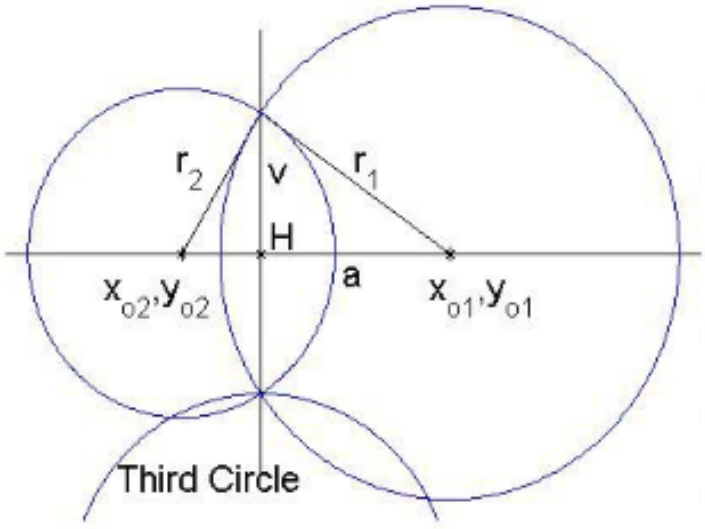


FIGURE 3.4 – La géométrie de l'intersection cercle-cercle.

La pairs de points de l'intersection, appelées p et p', sont largement utilisées dans l'un des algorithmes. Une fois les deux points sont trouvés, le point correct peut être sélectionné en vérifiant la distance de chaque point de potentiel et le troisième cercle. Le point qui se trouve sur le troisième cercle est un point d'intersection. Si les trois cercles n'aboutissent pas à une intersection, alors la triangulation ne parvient pas à trouver un point commun et génère une erreur avec aucun point d'intersection.

2. **Aperçu des algorithmes**
   L'approche commence en choisissant un petit sous ensemble de données et augmentant progressivement le sous ensemble. Le premier algorithme montré dans la figure 3.5, appelé sélection aléatoire, consiste à tirer 3 balises dans un ensemble appelé triplets jusqu'à ce qu'un ensemble de trois balises correctes soit établi.

**Algorithm 1. Random Selection**

**Input:** set $S$ of $N$ messages,
$CI$: the $\delta$-consistency interval
$C_t$: the consensus threshold,
$i_{max}$: maximum number of iterations .

1. Initialize i=1, $L = \emptyset$;
2. **While** $(i < i_{max})$ {
3. Randomly draw a unique subset $Si$ of size 3 from $S \backslash L^1$;
4. Use $Si$ to estimate the position $\hat{s}_0$;
5. Calculate $K$, the number of $\delta$-consistent beacons with respect to the estimate $\hat{s}_0$ in $S \backslash Si$ ;
6. **If** $(K > C_t)$ {
7. Form new estimate $\hat{s}_0$ from $K$ consistent points;
8. Terminate the program and return $\hat{s}_0$;}
9. Increment $L \leftarrow Si$; }
10. Increment $i$; }
11. Terminate program by announcing failure

FIGURE 3.5 – Algorithme de choix aléatoire.

Le second algorithme est montré dans la figure 3.6, de retirage intelligent, traite les balises à un moment jusqu'à ce que l'estimation soit trouvée.

**Algorithm 2. Intelligent Redraw**

**Input:** set $S$ of $m_{i:N}$ messages,
$CI$: $\delta$-consistency interval,
$C_t$: number of delta consistent points to achieve consensus.

**Internal variables:** *ListofPoints* list containing estimated, positions
$m_i$ message contains a unique Beacon ID, $(x,y)$ position and distance.

1. Initialize *ListofPoints*;
2. For $i = 2 : N$ {
3. If $m_i$ agrees with no elements in $ListofPoints^2$ {
4. For $j = 1 : i-1$; {
5. Calculate $p$ and $p'$ from intersection of $m_i$ and $m_j$
6. Append *listofPoints* with $p$ and $p'$;
7. Calculate $K$, the number of $\delta$-consistent beacons with respect to the estimate $p$;
8. **If** $(K > C_t)$ {
9. Form new estimate $\hat{s}_0$ from $K$ consistent beacons;
10. Terminate the program and return $\hat{s}_0$;}
11. Calculate $K$, the number of $\delta$-consistent beacons with respect to the estimate $p'$;
12. **If** $(K > C_t)$ {
13. Form new estimate $\hat{s}_0$ from $K$ consistent beacons;
14. Terminate the program and return $\hat{s}_0$;}
} } }
15. Terminate program by announcing failure;

FIGURE 3.6 – Algorithme de retirage intelligent.

Les deux algorithmes fonctionnent dans un mode distribué sur tout les avions de triangulation, recevant des données à partir d'un tampon qui assure la diffusion totalement ordonnée. Les algorithmes traitent un pas de temps de données à la fois, calculant la position réelle du récepteur.
L'algorithme de tirage intelligent est plus résistant à des pourcentages plus élevés de balises défectueuses, et exécute plus rapidement dans ces cas plus que l'algorithme de sélection aléatoire.

## 3.5 Conclusion

Dans ce chapitre, on a présenté les problématiques, en suite, on a donné une revue de la littérature discutant les travaux déjà réalisé sur la localisation des UAVs en présence de défauts de fonctionnement de récepteur GPS.

# 4

# Proposition et validation

## 4.1 Introduction

Les UAVs sont un type de robot qui sont souvent utilisés dans des missions civiles de secours des sinistrés et des scénarios militaires pour reconnaitre et fournir une détection dans les zones qui sont dangereuses ou impossible pour les humains. Des équipes d'UAV peuvent avoir besoin de coopérer pour parvenir à une mission particulière, comme la surveillance d'une zone spécifique ou recherche des cibles spécifiques ou mission d'attaque.
Le but de ce chapitre est de répondre à la problématique déjà exposée dans le chapitre précédent d'état de l'art et de valider la solution proposée avec démonstrations mathématiques.

## 4.2 Objectif du problème

L'objectif général de notre problème consiste à contrôler les drones pour la réalisation d'une mission correctement dans un environnement hostile.

## 4.3 Hypothèses générales du travail

- Nous supposons que les avions sans pilote dénotés UAVs (ou noeuds) sont autonomes collaboratifs.
- Chaque UAV possède un identifiant unique i et un récepteur GPS.
- Les UAVs volent sur une même altitude $Z$ et possède des vitesses $v_i$.

– Initialement, un UAV connaît seulement son identité, le fait qu'il soit le seul à posséder cette identité dans le réseau d'UAV.

## 4.4 Proposition et validation

Dans cette partie nous allons réexposer chaque problématique suivie d'une solution qu'on a proposé. les solutions vont être validées par des démonstrations mathématiques.

### 4.4.1 Problème 1

Si un UAV au cours d'une mission (de surveillance par exemple) perd son positionnement GPS, et sa communication avec la station sol, comme le montre la Figure 4.1, et rentre dans une zone de danger, comment récupérer le drone ?

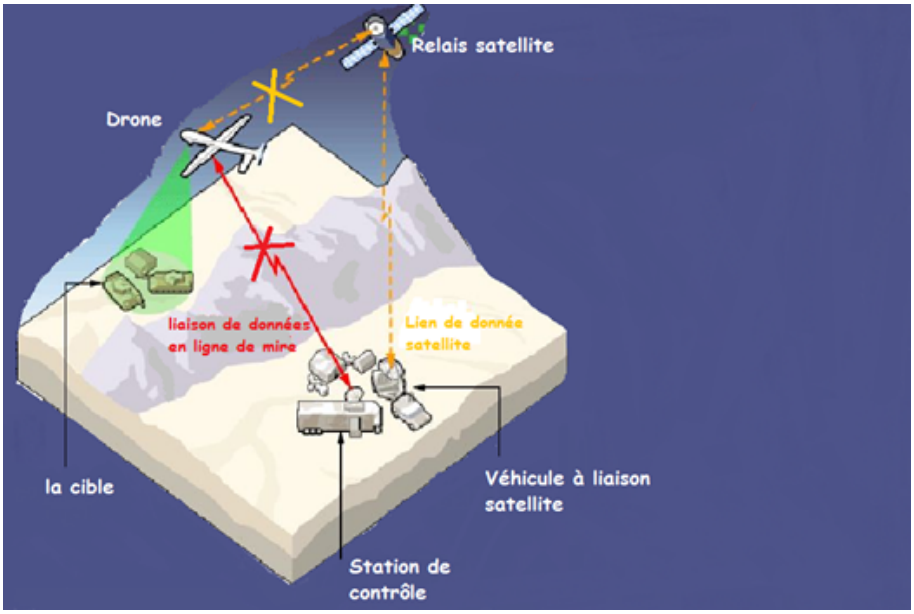


FIGURE 4.1 – Perte de communication du drone.

#### 4.4.1.1 Solution

Nous proposons en cas de perte de communication avec la station sol ou perte de signal GPS, une procédure de retour automatique au sol (station de base) que le drone doit exécuter et ainsi quitter la zone de danger.

#### 4.4.1.2 Validation

Voici la procédure qui permette à l'UAV d'exécuter le retour :
Procédure Retour $UAV_i$ :
Entrée : $List_i$ : $(v, t, \theta)$ est une liste que possède chaque UAV permet d'enregistrer l'historique c-à-d le trajet traversé par l'UAV(dans ce cas :la vitesse et le temps qui donne la distance et l'angle $\theta$ ).

1. le drone au point de perte de contact fait un angle de 180° pour qu'il puisse revenir.
2. le drone utilise l'historique ($List_i$) des mouvements qu'il a effectué (le processus inverse).

La figure ci dessous représente un exemple de chemin traversé par le drone :

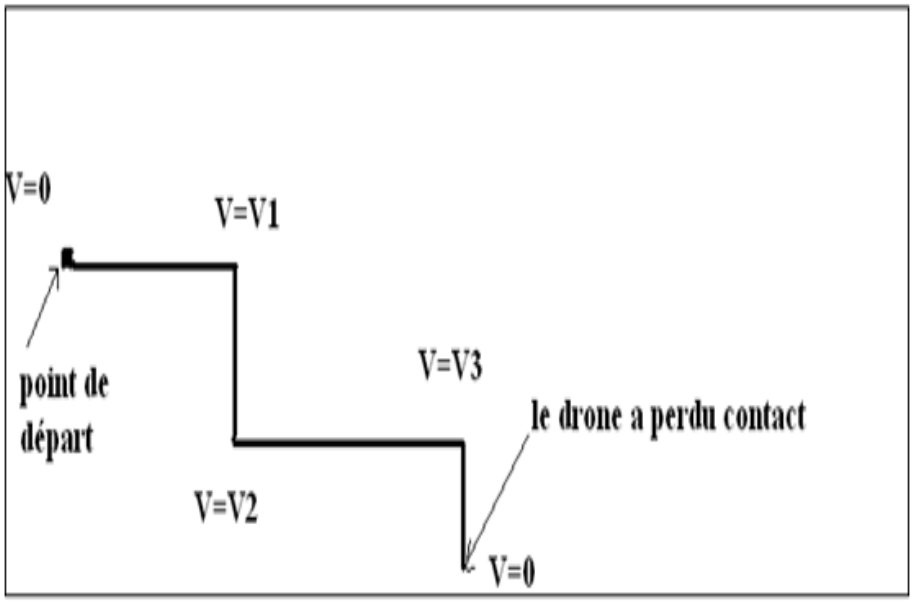


FIGURE 4.2 – Exemple de chemin traversé par le drone.

Dans ce cas le drone va faire un retour avec un angle $\theta = 180°$ et il revient au point de départ en utilisant les paramètres déjà sauvegardés qui sont : le temps et la vitesse pour trouver la distance parcourue à chaque fois avant de changer l'angle de direction $\theta$ (dans cet exemple $\theta = 90°$).

### 4.4.2 Problème 2

Un groupe d'UAVs en cours de mission, si l'un perd sa position (i.e. perte de signal GPS instantanée ou permanente à cause d'une défaillance de récepteur GPS), alors comment le relocaliser et comment s'assurer que sa position est correcte avec la possibilité de présence d'UAVs byzantins ?

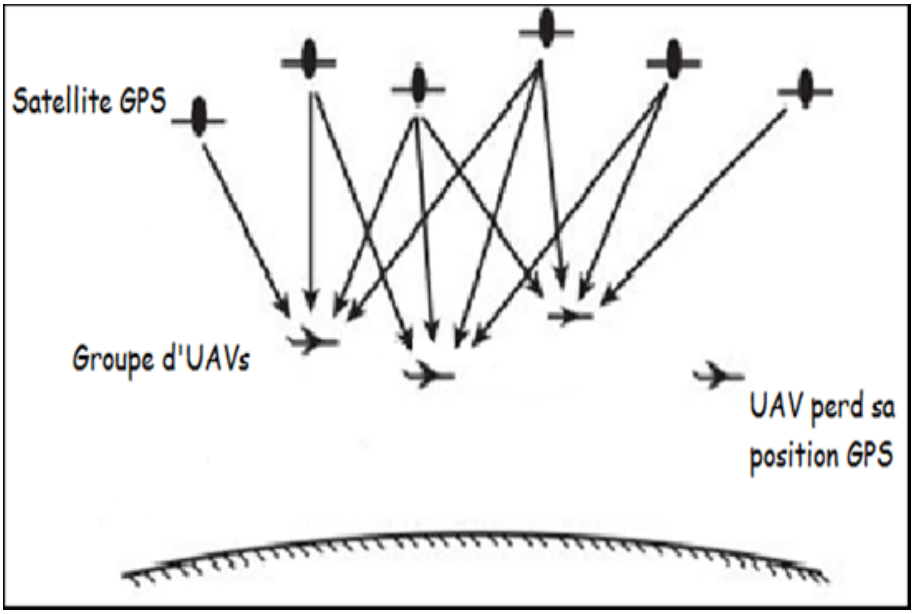


FIGURE 4.3 – Perte de signal GPS.

#### 4.4.2.1 Hypothèses

- Le groupe de drones est modélisé sous frome de graphe connexe qui veut dire que pour tout couple de sommets il existe une chaine les reliant, tel que chaque nœud représente un UAV.
- Les UAVs sont déjà authentifiés c'est à dire il existe des canaux sécurisés entre eux.
- Possibilité d'existence d'UAVs byzantins qui sont des UAVs qui se comportent arbitrairement.

Comme le montre l'exemple de la figure ci-dessous :

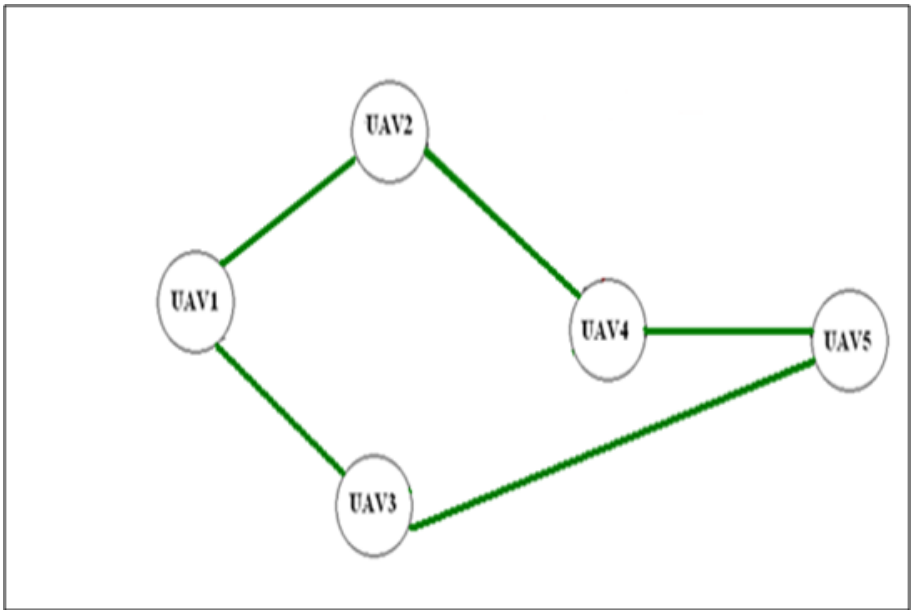


FIGURE 4.4 – Réseau d'UAVs sous forme de graphe connexe(Topologie en anneau).

#### 4.4.2.2 Solution et démonstration

Pour tolérer l'existence d'UAVs byzantins dans le réseau, on utilise le théorème des systèmes distribués déjà démontré suivant :
**"Pour tolérer t fautes byzantines, il faut au moins t+1 liens corrects dans le graphe (connectivité)".**
Dans l'exemple de graphe qu'on a considéré, on suppose que le nombre d'UAVs byzantins=1, alors le nombre de liens correctes=2. Pour la relocalisation, l'UAV défaillant (perte de signal GPS instantanée ou permanente), utilise un principe semblable au principe de GPS, tel que 3UAV vont jouer un rôle de satellites pour la relocalisation de l'UAV défaillant.

### 4.4.3 Problème 3

Pallier au problème d'existance de satellite byzantin.

#### 4.4.3.1 Hypothèses

Les UAVs utilisent 4 satellites pour la localisation, parmi les 4 satellites qui donnent la position au récepteur GPS, nous supposons qu'il existe un seul qui peut être byzantin.

#### 4.4.3.2 Solution et démonstration

Puisque l'utilisation de 4 satellites nous fournit une position 3D avec coordonnées $(x, y, z)$ et comme l'utilisation de 3satellites de ce groupe de 4 nous fournira une position 2D $(x, y)$ sachant que les UAVs volent à une même altitude $z$ ne change rien, alors pour détecter le satellite byzantin et avoir une position correcte, nous proposons de répliquer les modules émetteurs de signal GPS (4 modules) avec des fréquences différentes (tel que la basse fréquence peut être détruite par spoofing sans détruire les autres c.à.d. les autres signaux vont arriver correctement à l'UAV) de chaque satellite, notre solution est basée sur le théorème des systèmes distribués démontré suivant :

**"Pour tolérer t fautes, il faut 3t+1 réplicas".**

Utiliser le principe de triangulation pour trouver la position.

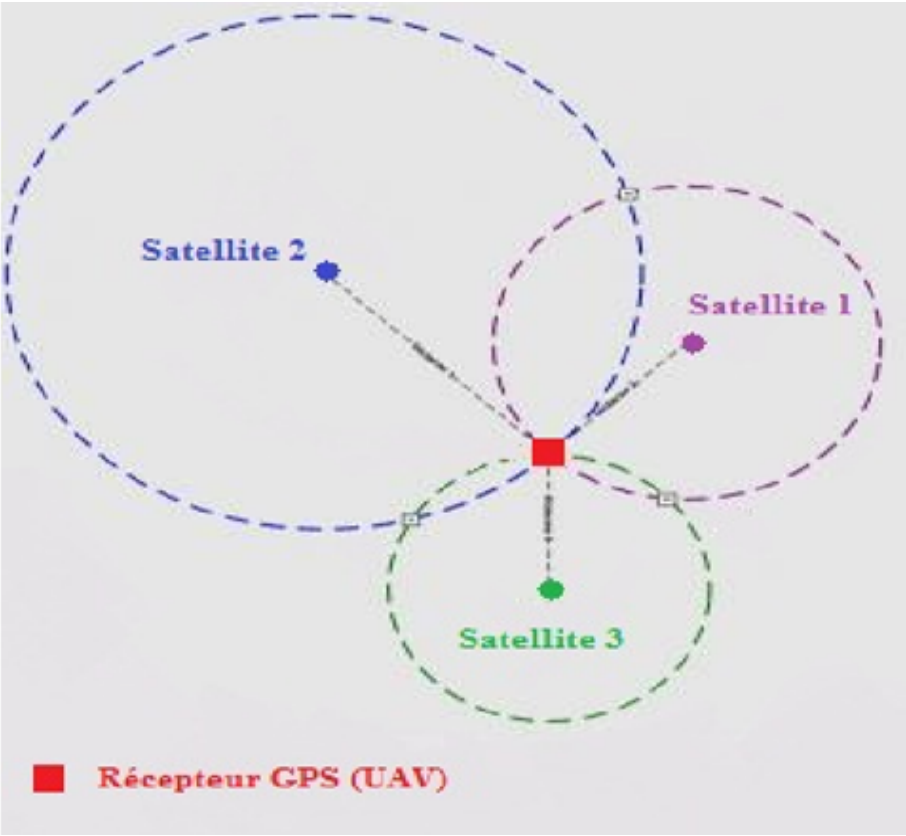


FIGURE 4.5 – Triangulation réussie (bonne triangulation).

### 4.4.4 Problème 4

Un groupe de drones coopératifs pour l'attaque d'une cible, sachant que parmi les UAVs on peut y avoir d'UAVs byzantins, qui ont des erreurs sur la position de la cible, ou reçoivent une fausse position de l'adversaire qui fais le spoofing sur les signaux GPS, afin de le tromper et lui donner une position alliée (fausse position), ce qui pose un grand problème. Comment résoudre ce problème ?
La figure 4.6 ci-dessous montre une mission d'attaque de cible par un groupe de drone.

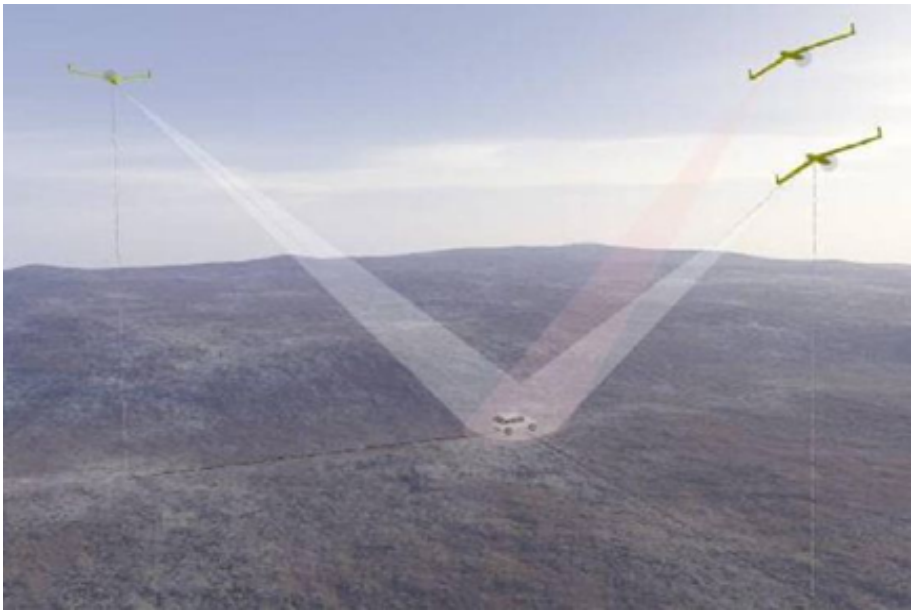

FIGURE 4.6 – Mission d'attaque de cible par un groupe de drone.

#### 4.4.4.1 Solution

Nous proposons lors de l'exécution d'une mission d'attaque par un groupe de drone d'utiliser un algorithme synchrone d'accord approximatif pour détecter la position correcte de la cible afin de l'attaquer. La figure 4.7 illustre un schéma détaillé qui représente la détection d'une cible par un groupe de drone.

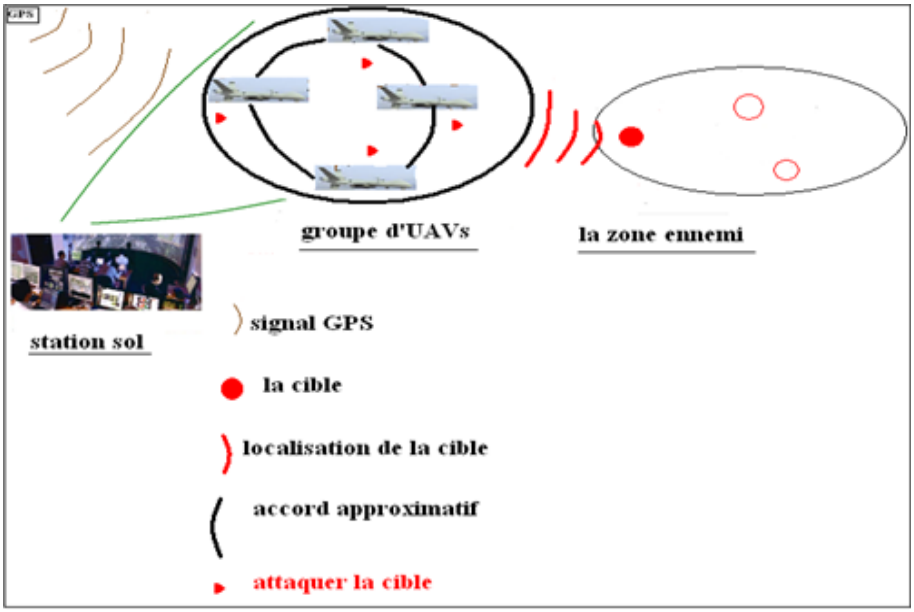


FIGURE 4.7 – Détection d'une cible par un groupe d'UAVs.

Voici l'algorithme synchrone byzantin qui permet cet accord approximatif pour trouver la position approximative de la cible en présence de t UAVs fautif de l'ensemble de n UAV vérifiant l'inégalité :$n > 3t + 1$ .

---

**Tour** 1 (Premier tour d'approximation) :
**Input** $(X, Y, Z)$ ;
$V \leftarrow SynchExchange((X, Y, Z))$ ;
$(X, Y, Z) \leftarrow f_{t,t}(V)$ ;
$H \leftarrow \lceil log_c(\delta(V)/\epsilon) \rceil$, où $c = c(n - 2t, t)$.
**Tour** $h(2 \leq h \leq H)$ (tours d'approximation) :
$V \leftarrow SynchExchange((X, Y, Z))$ ;
$(X, Y, Z) \leftarrow f_{t,t}(V)$ ;
**Tour** $H + 1$ (Tour de terminaison) :
$Broadcast(< (X, Y, Z), stop >)$ ;
**Output** $(X, Y, Z)$ ;
**Sous Programme** $SynchExchange(X, Y, Z)$ ;
$Broadcast(X, Y, Z)$ ;
Collecter n réponses :
– Remplir les valeurs des processus arrêtés ;
– Remplir les valeurs par défaut, si nécessaire ;
Retourner le multi ensemble de réponses.

---

Dans cet algorithme le vecteur $(X, Y, Z)$ représente la position de la cible à attaquer. $V =< v_1, v_2, \ldots, v_n >$ est un multi ensemble de valeurs $v_i$ tel que $v_i = (X_i, Y_i, Z_i) \in R^3$ . La constante $c = c(n - 2t, t)$ est un facteur de convergence pour le protocole synchrone. Pour $k > 0$ et $t \geq 0$ la fonction d'approximation utilisée est :

$$\mathrm{f}_{k,t}(V) = mean(select_k(reduce^t(V))) \quad (4.1)$$

Tel que cette fonction est paramétré par $t$ le nombre de processus fautifs. $k$ est une constante de choix qui dépends de t et du fait que l'algorithme est synchrone ou asynchrone. Dans notre algorithme, la fonction d'approximation pour le protocole synchrone avec pas plus de t processus fautifs et $|V| > 2t$ est :

$$\mathrm{f}_{t,t}(V) = mean(select_t(reduce^t(V))) \quad (4.2)$$

Où :
– *mean* est la moyenne du multi ensemble non vide $V$ définit par :

$$\mathrm{mean(V)}{=}\textstyle\sum_{r\in R^3} rV(r)/|V| \quad (4.3)$$

– $Select_t$ est une fonction définie comme suit :
Supposant $V$ est un multi ensemble non vide, soit $m = |V|$ et soit $v_0 \leq v_1 \leq ... \leq v_{(m-1)}$ des éléments de $V$ en ordre non décroissant. Si $t > 0$ alors définir $Select_t(V)$ pour être le multi ensemble composé des éléments $v_0, v_k, v_{2k}, \ldots, v_{jk}$. Où $j = \lfloor (m-1)/t \rfloor$ . Donc, $Select_t(V)$ choisis le plus petit élément de $V$ et chaque $t^{ime}$ élément de la suite.
– $reduce^t(V)$ est une fonction qui supprime les $t$ plus grandes valeurs et les $t$ plus petites valeurs du multi ensemble $V$.

Pour montrer que cet algorithme est correct, nous devons montrer que tous les processus se terminent, et que les conditions d'accord et de validité sont satisfaites qui sont définies comme suit :
Pour tout pré attribué $\epsilon > 0$ (aussi petit que souhaité), l'algorithme d'accord approximatif doit satisfaire les deux conditions suivantes :

– **L'accord** : Tous les processus non fautifs finalement arrêtent avec les valeurs de sortie qui sont dans $\epsilon$de chacun d'autre.
– **La validité** : la valeur de sortie de chaque processus non fautif doit être dans l'intervalle de valeur initial des processus non fautif.

#### 4.4.4.2 Démonstration

Il est clair que tous les processus se terminent car le nombre totale de tours qui dois être exécuté (y compris le $1^{er}$ tour) est donné par $log_c(\delta(V)/\epsilon)$ , où $V$ est le multi ensemble de valeurs reçues en premier tour et $c = c(n - 2t, t)$.

Considérons la propriété de l'accord. Lors du $1^{er}$ tour au cours duquel certains processus non fautifs s'arrêtent, il est déjà le cas où les valeurs de tous les processus non fautifs sont dans $\epsilon$ de chacun d'autre.
Par le lemme 1, ce diamètre n'augmente plus aux tours suivants, de sorte que les valeurs finales de tous les processus non fautifs sont aussi dans $\epsilon$ de chacun d'autre.
La propriété de validité résulte aussi de l'application du lemme 1.

- **Lemme 1**
  Considérons que $n \geq 3t + 1$. Soit $T$ un ensemble de processus, avec $|T| \geqslant n - t$. Soit $h$ un entier positif.
  Soit $U$ et $U'$ les multi ensembles de valeurs des processus dans $T$, immédiatement avant et après le tour $h$, respectivement, dans un $T$-calcul particulier de $S$. alors $\rho(U') \subseteq \rho(U)$.
- **Démonstration du lemme 1**
  Soit $P$ un processus arbitraire dans $T$. soit $v$ et $v'$ les valeurs détenues par $P$ immédiatement avant et après le tour $H$, respectivement. Il suffit, puisque $P$ est arbitraire, de montrer que $v' \in \rho(U)$. Si $P$ est terminé avant le début de tour $h$, alors $v' = v \in \rho(U)$.
  Si $P$ n'a pas terminé avant le début du tour $h$, alors soit $V$ le multi ensemble de valeurs reçues par $P$ dans le tour $h$. Alors $V$ et $U$ satisfont les hypothèses du lemme 2, et, depuis $v' = f_{(t,t)}(V)$ , il s'ensuit que $v' \in \rho(U)$.
- **Lemme 2**
  Supposant que $k > 0$ et $t >= 0$ sont des nombres entiers. Supposant que $U$ et $V$ sont des multi-ensembles non vides tels que $|V - U| \leq t$ et $|V| > 2t$. Alors $f_{k,t}(V) \in \rho(U)$.
- **Démonstration du lemme 2**
  Supposant $\rho(reduce^t(V)) \nsubseteq \rho(U)$.
  Alors soit $min(reduce^t(V)) < min(U)$ ou $max(reduce^t(V)) > max(U)$.
  Si $min(reduce^t(V)) < min(U)$,alors $\sum_{r<min(U)} V(r) \geq t + 1$.
  Par conséquent, $|V - U| \geq t+1$, qui contredit les hypothèses. Le cas $max(reduce^t(V)) > max(U)$ est symétrique.

## 4.5 Conclusion

Dans ce chapitre nous avons donné notre proposition à chacune des problématiques et valider ces dernières par des démonstrations mathématiques.

# Conclusion générale

Le présent mémoire qui porte sur le contrôle d'un groupe d'avions sans pilote est consacré à l'étude de quatre problématiques. Ces dernières sont importantes et d'actualités, car l'utilisation de ces drones est en forte croissance, tant dans le domaine militaire que civil.

Le but de ce mémoire est de résoudre les quatre problématiques qui présentent de nombreuses difficultés. Le chapitre 1 dégage des généralités sur les drones s'ensuit d'une deuxième partie (chapitre 2) " Sûreté et fiabilité dans les systèmes UAS" qui rapproche le domaine de drones, domaine purement aéronautique au domaine d'informatique, en détaillant le système, les communications, les fautes et pannes, ainsi que des concepts de systèmes distribués tels que le consensus et l'accord approximatif , qui nous seront utile dans la partie proposition.

Dans la troisième partie de ce manuscrit, "Etat de l'art", nous avons présenté les problématiques,en suite,nous avons investigué quelques travaux de -recherches déjà effectués- dans le domaine des drones et qui ont des objectifs semblables aux notres, et enfin, dans la dernière partie (chapitre 4) nous avons donné des solutions à toutes nos problématiques posées ainsi que les avons validé en utilisant des démonstrations mathématiques.

Nos solutions offrent aux drones un niveau d'autonomie et de capacité décisionnelle élevée ainsi qu'une tolérance aux fautes byzantines et défaillances (transitoire et permanente) de récepteur GPS, et une réalisation de mission correctement dans un environnement hostile.

Cependant, notre résolution s'est basée sur des hypothèses sans prendre en compte certains obstacles et contraintes tels que les changements climatiques, les obstacles, les collisions entre drones, l'intégration dans l'espace aérien etc... qui devient dans ce cas extrêmement difficile à résoudre et nécessite beaucoup d'études.

Par nos connaissances universitaires associées à nos recherches, et notre volonté, et en dépit du manque de temps et de moyens, nous avons pu atteindre l'objectif de notre mémoire.

# Bibliographie


[1] M.Asencio,P.Gros,J.Patry, *les drones tactiques à voilure tournante dans les engagement contemporains,* Fondation pour la recherche stratégique 27 rue Damesme,(2010).

[2] M.Daniel,*Drones : Application militaire et débats politiques,*Juillet (2010).

[3] ONERA,*Mieux connaitre les drones,*(2004).

[4] Centre interarmées de concepts de doctrines et d'expérimentations,*Documment cadre interarmées pour l'emploie des drones en service,*6 Octobre (2008).

[5] G.Debionne,*le système GPS*,12 janvier (2008).

[6] Reynolds, Craig W. Flocks,*herds and schools : a distributed behavioral model,* Proceedings of the 14th Annual Conference on Computer Graphics and Interactive Techniques (1987).

[7] Cruz, D., McClintock, J., Perteet, B., Orqueda, O.A.A., Yuan, C. and Fierro, R.*"Decentralized cooperative control-a multivehicle platform for research in networked embedded systems"*, Control Systems Magazine, IEEE, 27, pp. 58-78 (2007).

[8] Fax, J.A. and Murray, R.M.*"Information flow and cooperative control of vehicle formations"*, IEEE Transactions on Automatic Control, 49, pp. 1465-1476 (2004).

[9] X. C. Ding, A. Rahmani, and M. Egerstedt,*"Optimal multi-UAV convoy protection"*, Conference on Robot Communication and Configuration, volume 9, pages 1–6, April 2009.

[10] J. Tisdale, Z. Kim, J. Hedrick, *"Autonomous UAV path planning and estimation"*. IEEE Robotics and Automation Magazine, 16 :35–42, 2009.

[11] Ethan M Puchaty and Daniela A DeLaurentis,*"A Performance Study of UAV-based Sensor Networks Under Cyber Attack"*,Proceedings of the 2011 6th International Conference on System of Systems Engineering, Albuquerque, New Mexico, USA - June 27-30, 2011.

[12] Z. Goraj, *"UAV Platform designed in WUT for border surveillance"*,AIAA paper 2965, 2007.

[13] *Safety and Reliability in cooperating Unmaned Aerial Systems.*

[14] R. Strong *"Problems in fault-tolerant distributed systems",* Publication IEEE ISBN 135-/85/0000/0300s01.00

[15] Wei, Ren, Beard, R.W. and Atkins, E.M. *"Information consensus in multivehicle cooperative control"*, Control Systems Magazine, IEEE, 27, pp. 71–82 (2007)

[16] D. Dolev, N. -4. Lynch, S. S. Pinterand E. W. Stark, and W. E. Weihl. *Reaching Approximate Agreement in the Presence of Faults.* Journal of the ACM, 33(3) :499-516, 1986.

[17] J.C. Laprie, B. Courtois, M.C. Gaudel , D. Powell, *"Sûreté de fonctionnement des systèmes informatiques matériels et logiciels",* AFCET Dunod Informatique 1989.

[18] Anon.,*"Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System,"* Tech. rep., John A. Volpe National Transportation Systems Center, 2001.

[19] Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., and Kintner, Jr., P. M., *"Assessing the spoofing threat : development of a portable GPS civilian spoofer,"* Proceedings of the ION GNSS Meeting, Institute of Navigation, Savannah, GA, 2008.

[20] Rawnsley, A., *"Iran's Alleged Drone Hack : Tough, but Possible,"* Dec. 2011, http ://www.wired.com/ dangerroom/2011/12/iran-drone-hack-gps/.

[21] Qu.Yaohong, Y. Zhang. *Cooperative localization against GPS signal loss in multiple UAVs flight* Journal of Systems Engineering and Electronics Vol. 22, No. 1, February 2011, pp.103–112.

[22] L. Merino, J. Wiklund, F. Caballero, et al. *Vision-based multi- UAV position estimation.* IEEE Robotics  Automation Magazine, 2006, 13(3) : 53-62.

[23] Y. Cui and S. S. Ge, *"Autonomous Vehicle Positioning With GPS in Urban Canyon Environments,"*IEEE Transactions on Robotics and Automation, vol. 19, pp. 15-28, 2003.

[24] J. Dittmer, *"Solving the GPS Urban Canyon Problem,"* Frost  Sullivan Market Insight, 2005.

[25] N. Priyantha, A. Chakraborty, and H. Balakrishnan, *"The Cricket Location-Support System,"* in Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom), 2000, pp.32-43.

[26] A. Savvides, C. Han, and M. Strivastava, *"Dynamic fine-grained localization in ad-hoc networks of sensors,"* in Proceedings of AC International Conference on Mobile Computing and Networking (MobiCom), 2001, pp. 166-179.

[27] D. Niculescu and B. Nath, *"Ad hoc positioning system (APS) using AoA,"* in Proceedings of IEEE Conference on Computer Communications (INFOCOM), 2003, pp. 1734 - 1743.

[28] Z. Li, W. Trappe, Y. Zhang, and B. Nath, *"Robust statistical methods for securing wireless localization in sensor networks."* in Proceedings of The International Symposium on Information Processing in Sensor Networks (IPSN), 2005, pp. 91-98.

[29] P. Rousseeuw and A. Leroy, *Robust Regression  Outlier Detection.* New York, NY : John Wiley  Sons, 1987.

[30] D. Liu, P. Ning, and W. Du, *"Attack-resistant location estimation in sensor networks,"* in Proceedings of International Symposium on Information Processing in Sensor Networks (IPSN), 2005, pp. 99-106.

[31] M. Barborak, A. Dahbura, and M. Malek, *"The consensus problem in fault-tolerant computing,"* ACM Comput. Surv., vol. 25, no. 2, pp. 171-220, 1993.

[32] K. Driscoll, B. Hall, H. Sivencrona, and P. Zumsteg, *"Byzantine fault tolerance, from theory to reality,"* in Computer Safety, Reliability, and Security, Lecture Notes in Computer Science, 2003, pp. 235-248.

[33] M. J. Fischer and N. A. Lynch, *"A lower bound for the time to assure interactive consistency,"* Information Processing Letters, vol. 14, pp. 183-186, 1982.

[34] R. Turpin and B. A. Coan, *"Extending binary Byzantine Agreement to multivalued Byzantine Agreement,"* vol. 18, no. 2, pp. 73-76, Feb. 1984.

[35] R. S. L. Lamport and M. Pease, *"The byzantine generals problem."* ACM Trans. Prog. Lang. Sys., vol. 4, pp. 382-401, 1982.

[36] E. Valovage, *"Enhanced ADS-B Research,"* IEEE AE Systems Magazine, pp. 35-39, 2006.

[37] J. L. Awange and E. W. Grafarend, *"Algebraic Solution of GPS Pseudo Ranging,"* GPS Solutions, vol. 5, pp. 20-32, 2002.

*Résumé*

*Dans ce projet, on a définit les concepts généraux sur les UAVs, le système GPS et son fonctionnement ; ensuite, on a donné quelques outils nécessaires dans la partie proposition tel que le consensus, le spoofing et la communication dans les systèmes UAS ; puis, on a introduit la problématique qui est composée de quatre parties. La première est lorsque le drone perd contact avec la station sol et les satellites ; la deuxième est la relocalisation de la position d'un drone défaillant dans son récepteur GPS avec la possibilité de présence d'UAVs byzantins ; la troisième est la réception de fausses positions à partir d'un satellite byzantin et la dernière problématique est la localisation de la cible afin de l'attaquer, Il faut trouver un moyen qui permet aux drones d'avoir la même position de la cible qui est la position réelle, sachant que ces problématiques n'ont jamais été traitées auparavant. Pour cela, nous avons investigué quelques travaux déjà effectués qui sont proches de notre problématique ; nous avons ensuite proposé des solutions pour chaque problématique et on les a validé par des démonstrations mathématiques.*

**Mots clefs :** les UAVs byzantins, satellite byzantin, les UAVs, le système GPS, le spoofing, le système UAS, drone.

*Abstract*

*In this project, we have defined the general concepts about the UAVs, the system GPS and its operation ; then, we have given some necessary tools in the proposal part such as the consensus, the spoofing and the communication in the systems UAS ; then, we have introduced the problems which are composed of four parts. The first is when the drone loses contact with the station ground and the satellites, the second is the relocalization of the position of a defective drone in its receiver GPS with the possibility of presence of Byzantin UAVs, the third is the reception of false positions from a Byzantine satellite and the last problem is the localization of the target in order to attack it, It is necessary to find a mean to permit to the drones to have the same position of the target which is the real position, knowing that these problems were never treated before. For this, we have investigated some already carried out works which are close to our problem, we have then proposed solutions for each problem and we have validated them by mathematical demonstrations.*

**Key words :** UAVs Byzantins , satellite Byzantin ,UAVs, system GPS, spoofing, systeme UAS, drone.