Critique Sur le GPS-Spoofing Attack Detection Mechanism for UAV Swarms

Aabo-Aljaloo Taif, Fernandes Lopes João

Introduction

Posons-nous d’abord les premières questions :

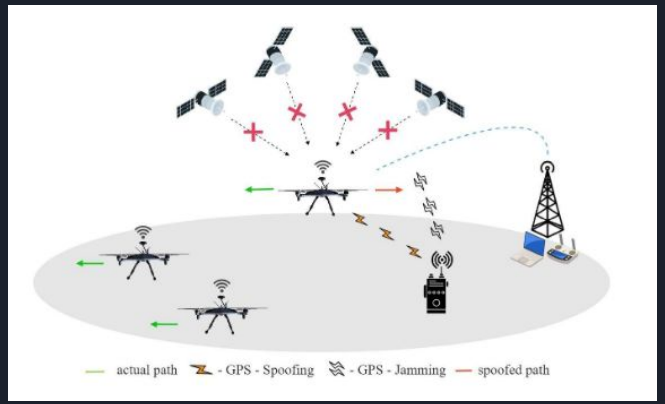
- Que ce qu’un UAV ?
- Où sont-ils utilisés ?
- Comment est-ce qu’ils fonctionnent ?
- Quels risques ça introduit ?

GPS-Spoofing Attacks

Problématiques principales du GPS-Spoofing :

- Que ce que le GPS-Spoofing ?
- Pourquoi est-ce important dans le milieu des UAV ?
- Quels sont les challenges posés ?

Quelles sont alors les solutions trouvées jusqu'à aujourd'hui ?



Solutions Existantes

Plusieurs approches ont déjà été trouvées, mais souvent avec des défauts qui les accompagne :

- Sensor Fusion.
- Multi-Receiver Systems.
- Antenna Arrays.
- Time of Arrival (ToA) and Signal Correlation.
- Cellular Network-Based Approaches.
- Video Stream Analysis.

Solution Apportée Par l'Article

Principe utilisé dans l'approche présentée :

La méthode des chercheurs va consister en la comparaison entre deux distances qui vont être mesurée entre les drones. Une première entre la station de contrôle et la distance avec l'IR-UWB.

Dans l'article, trois scénarios distincts sont étudiés :

- Un UAV affecté avec un seul transmetteur radio.
- Deux UAV ou plus avec un seul transmetteur radio.
- Deux UAV ou plus avec plusieurs transmetteurs radio.

Critique et Discussion

Discussion des avantages :

- Ne demande aucune adaptation ou matériel supplémentaire embarqué.
- Technologie IR-UWB précise et robuste aux interférences.
- Fonctionne bien avec les petits et moyens essaims.

Critiques faisables sur cette approche :

- Tous les drones n'ont pas de technologie IR-UWB à bord.
- Robuste à la majorité des interférences, mais pas toutes, notamment les interférences "multi-path".
- Approche non testée en dehors du cadre théorique.
- Beaucoup de données transmises à chaque instant.
- Aucune solution pour résoudre le spoofing proposée.

Conclusion

C’est une bonne approche théorique, qui permet avec peu de ressources de détecter en théorie une tentative de GPS Spoofing sur un drone ou plusieurs drones d’un essaim. Cependant certains points tel qu’une alternative aux IR-UWB, la quantité de données transmises ou encore la mise en pratique de la théorie sont des points à souligner dans l’approche.

Comme nous l’avons vu, avoir un mécanisme de défense robuste contre les GPS Spoofing est essentiel au sein des drones, étant une technologie en constante évolution, et les missions qu’on leur donne sont de plus en plus vitale.

Références

1 - P. Mykytyn, M. Brzozowski, Z. Dyka, and P. Langendoerfer, GPS- Spoofing Attack Detection Mechanism for UAV Swarms

2 - https://store.potensic.com/fr-fr/products/atom-se