< GROUPE DE TRAVAIL DRONES : IDENTIFICATION AMI-ENNEMI >

“FRIEND OR FOE IDENTIFICATION”

CAMPUS CYBER 2025

< SOMMAIRE >

PRÉAMBULE

Ce document est produit par la communauté d'intêret « Cybersécurité des drones et des robots » sur le sujet de « l'identification Ami-Ennemi » appliquée aux drones aériens, terrestres ou navals.
Nous utiliserons dans la suite l'acronyme « FFI » (Friend or Foe Identification) pour désigner la capacité d'identification Ami-Ennemi d'un drone unitaire, d'une escadrille ou d'un essaim de drones.

Ce rapport a pour objectif d'examiner les différentes approches existantes pour l'identification des drones amis et ennemis, en mettant en évidence leurs avantages, leurs limites et les défis techniques qu'elles soulèvent. Il s'agira également d'explorer des solutions innovantes, notamment l'intégration de l'intelligence artificielle, des protocoles de communication sécurisés et des systèmes hybrides d'identification. Enfin, nous proposerons des perspectives d'amélioration visant à renforcer la fiabilité et l'efficacité des systèmes FFI dans un contexte de plus en plus complexe et évolutif.

1. FONDEMENT ET TECHNOLOGIES FFI

1.1 CONTEXTE ET ENJEUX

L'essor des drones, aussi bien dans le domaine civil que militaire, a transformé de nombreux secteurs, allant de la surveillance et la logistique aux opérations militaires complexes. Toutefois, cette prolifération pose un défi majeur : la distinction entre drones amis et ennemis. Dans un environnement opérationnel, une identification erronée peut avoir des conséquences critiques, allant de la neutralisation accidentelle d'un drone allié à l'infiltration de drones hostiles menaçant la sécurité des infrastructures et des personnels.

1.2 PROBLÉMATIQUE

L'identification des drones amis-ennemis (**FFI**) est une problématique centrale dans la gestion et la sécurisation des espaces aériens. Comment assurer une identification fiable des drones en temps réel, tout en tenant compte des contraintes techniques, énergétiques et sécuritaires ? Quels sont les risques associés aux méthodes actuelles et comment les améliorer face à des menaces de plus en plus sophistiquées ?

1.3 TECHNOLOGIES ET PRINCIPES D'IDENTIFICATION FFI

L'identification des drones amis-ennemis (**FFI**) repose sur diverses technologies permettant de différencier un drone allié d'une menace potentielle. Ces approches varient en fonction des besoins opérationnels, des contraintes techniques et des environnements d'utilisation. Nous pouvons classer les méthodes d'identification en trois grandes catégories : l'identification basée sur la communication, l'identification passive et l'identification comportementale.

1.3.1 IDENTIFICATION BASÉE SUR LA COMMUNICATION

L'identification par communication repose sur l'échange d'informations entre le drone et une entité de contrôle (station au sol, autre drone ou satellite). Elle permet une reconnaissance rapide et fiable, à condition que les transmissions soient sécurisées et authentifiées.

a **Protocoles d'authentification cryptographiques :** les drones amis peuvent être équipés de systèmes d'authentification cryptographique, où chaque appareil possède une clé unique permettant de prouver son identité. Ces systèmes incluent :
   - Les certificats numériques utilisant des infrastructures à clé publique (PKI).
   - **Les signatures électroniques** intégrées aux messages échangés entre drones et stations de contrôle.
   - **Les protocoles d'authentification mutuelle**, où un drone et une station vérifient réciproquement leur identité avant d'échanger des données.

Toutefois, ces méthodes nécessitent des ressources de calcul et de communication pouvant être coûteuses en énergie, un facteur critique pour les drones à autonomie limitée.

b **Transpondeurs et balises d'identification à distance (Remote ID) [1]** : dans le cadre des réglementations civiles, des solutions comme le Remote ID permettent à un drone de diffuser en continu son identité et sa position via des balises radio. Cette approche est déjà utilisée dans l'aviation classique avec les transpondeurs FFI pour les aéronefs militaires. Cependant, ces balises peuvent être sujettes au brouillage, à la falsification ou à l'usurpation d'identité par des drones malveillants.

c **Communication sécurisée entre drones et stations de contrôle** : pour empêcher toute interception ou manipulation des messages échangés, les protocoles de communication doivent intégrer des **mécanismes de chiffrement** et de **détection d'anomalies**. L'usage de technologies comme la **blockchain** peut également renforcer l'intégrité des échanges en assurant une traçabilité des interactions entre drones.

1.3.2.IDENTIFICATION PASSIVE

L'identification par communication repose sur l'échange d'informations entre le drone et une entité de contrôle (station au sol, autre drone ou satellite). Elle permet une reconnaissance rapide et fiable, à condition que les transmissions soient sécurisées et authentifiées.

a **Détection et classification via radar [2]** : Les radars spécialisés dans la détection des drones peuvent identifier des signatures spécifiques (taille, vitesse, trajectoire) permettant de différencier un drone connu d'un appareil suspect. Des systèmes avancés intègrent des techniques de machine learning pour améliorer la reconnaissance des drones en fonction de bases de données préexistantes

b **Analyse des signatures électromagnétiques et radiofréquences** : chaque drone émet des signaux électromagnétiques distincts en raison de ses communications internes et de son système de propulsion. En exploitant ces empreintes uniques, il est possible d'identifier un drone sans interagir directement avec lui. Cette approche est cependant limitée par la nécessité d'une base de données complète des signatures des drones amis.

c **Reconnaissance visuelle et thermique** : l'usage de caméras et de capteurs infrarouges permet d'analyser la silhouette et la chaleur émise par un drone. Associée à des algorithmes de **computer vision**, cette méthode peut identifier des modèles de drones spécifiques et les distinguer des menaces potentielles. Toutefois, la reconnaissance visuelle peut être perturbée par des conditions météorologiques défavorables (brouillard, pluie, faible luminosité).

1.3.3.IDENTIFICATION COMPORTEMENTALE

L'identification comportementale repose sur l'analyse des mouvements et des schémas de vol d'un drone pour déterminer s'il adopte un comportement normal ou suspect.

a **Analyse des trajectoires et des schémas de vol** : les drones amis suivent généralement des trajectoires prédéfinies et des protocoles de vol établis. Un drone s'écartant de ces schémas ou adoptant des manœuvres erratiques peut être suspecté d'être un appareil ennemi ou compromis.

b **Détection des comportements anormaux** : l'intelligence artificielle et les **réseaux de neurones récurrents (RNN)** peuvent être utilisés pour détecter les anomalies dans les comportements des drones. Par exemple, un drone militaire tentant d'échapper à la surveillance ou de se rapprocher.

En conclusion, chaque méthode d'identification des drones amis-ennemis présente des avantages et des limites en fonction du contexte d'application. L'identification basée sur la communication offre une reconnaissance rapide mais peut être vulnérable aux cyberattaques.

L'identification passive permet de détecter un drone sans interaction directe, mais sa fiabilité dépend des conditions environnementales. Enfin, l'identification comportementale exploite l'intelligence artificielle pour analyser les trajectoires de vol, mais nécessite des modèles de référence précis.

Dans un environnement opérationnel où les menaces évoluent rapidement, une **approche hybride combinant plusieurs méthodes** apparaît comme la solution la plus robuste pour garantir une identification efficace des drones amis et ennemis. La section suivante abordera les défis et contraintes liés à la mise en place de ces technologies.

2. DÉFIS ET CONTRAINTES

L'identification des drones amis-ennemis (FFI) est une tâche complexe qui implique plusieurs défis techniques, opérationnels et sécuritaires. L'efficacité des solutions actuelles est souvent limitée par des contraintes telles que la fiabilité des systèmes, les ressources énergétiques et matérielles, ainsi que l'absence de normes universelles.

2.1.FIABILITÉ ET PRÉCISION DE L'IDENTIFICATION

L'un des principaux défis du FFI est d'assurer une identification fiable en évitant les **faux positifs** (identification erronée d'un drone ami comme ennemi) et les **faux négatifs** (manque de détection d'un drone hostile). Plusieurs facteurs peuvent compromettre la précision des systèmes FFI :

- **Brouillage**: les transpondeurs et protocoles d'authentification peuvent être brouillés ou usurpés par des attaquants.
- **Changement d'apparence des drones** : les drones ennemis peuvent être modifiés pour imiter les signaux ou l'apparence des drones alliés.

2.2.CONTRAINTES MATÉRIELLES ET ÉNERGÉTIQUES

Les drones ont des ressources limitées, notamment en **puissance de calcul**, en **autonomie énergétique** et en **capacité de communication**. Les protocoles de FFI doivent donc être optimisés pour minimiser leur impact sur les performances du drone.

- **Autonomie réduite** : l'exécution d'algorithmes de reconnaissance (ex. vision par ordinateur, chiffrement avancé) peut consommer une quantité significative d'énergie.
- **Puissance de calcul restreinte** : les drones légers et compacts ne disposent pas de processeurs puissants pour exécuter des algorithmes complexes en temps réel.
- **Bande passante limitée**: les transmissions entre drones et stations de contrôle doivent être réduites pour éviter la saturation du réseau et les risques de détection.

2.3. INTEROPÉRABILITÉ ET STANDARDS

L'absence de **normes universelles** pour l'identification des drones est un obstacle majeur à l'adoption de solutions FFI efficaces.

- **Incompatibilité entre systèmes militaires et civils** : les solutions FFI doivent s'adapter aux différentes infrastructures et protocoles de communication utilisés par divers acteurs.
- **Problèmes de souveraineté technologique** : les pays développent leurs propres solutions FFI, ce qui complique la collaboration et la reconnaissance mutuelle des drones alliés.
- **Évolutivité des menaces** : l'identification doit être adaptable aux nouvelles tactiques et technologies utilisées par les drones malveillants.

3. SOLUTIONS ET PERSPECTIVES

Dans cette section nous faisons une cartographie des premiers systèmes FFI (de 1940 à ce jour), nous présentons aussi l'essentiel des systèmes commercialisés actuellement et enfin nous présentons une synthèse des travaux scientifiques et des perspectives.

3.1.HISTORIQUE DES SYSTÈMES FFI (DE 1940 À AUJOURD'HUI)

Parmi les sources retraçant l'historique des FFI, nous avons sélectionné ces trois rapports [3] [4] qui résument les principales évolutions technologiques depuis 1940.

3.1.1.TECHNIQUES DES PREMIERS SYSTÈMES FFI (1940-1960)

Les premiers systèmes FFI ont été conçus pour répondre aux besoins militaires pendant la Seconde Guerre mondiale et ont évolué progressivement. Ils ont progressivement évolué pour améliorer la distinction entre forces amies et ennemies tout en réduisant les vulnérabilités aux intercepteurs adverses.

a **Transpondeurs actifs (Mark I & II)** : les premiers systèmes FFI, Mark I et II, reposaient sur l'utilisation de transpondeurs actifs installés à bord des avions alliés. Ces dispositifs fonctionnaient de la manière suivante :
   - Lorsqu'un radar allié interrogeait un appareil équipé, celui-ci répondait en émettant un signal radio spécifique.
   - Cela permettait aux opérateurs radar d'identifier les forces amies et de réduire le risque de tirs fratricides.

Cependant, ces premiers systèmes présentaient des limitations importantes :

- **Vulnérabilité aux interceptions ennemies** : les transmissions pouvaient être captées par l'adversaire, révélant ainsi la présence et la position des forces alliées.
- **Sensibilité au brouillage** : les signaux n'étaient pas chiffrés, ce qui les rendait vulnérables aux contre-mesures électroniques de l'ennemi.

b **Amélioration avec le Mark III & IV** : pour répondre aux faiblesses des systèmes Mark I & II, les modèles Mark III et IV ont été introduits avec plusieurs améliorations significatives :

- **Utilisation de fréquences spécifiques** : afin de minimiser les interférences accidentelles entre les systèmes alliés et de rendre les signaux plus distinctifs.
- **Codage des réponses** : pour empêcher les ennemis de simuler un signal allié, un certain niveau de codage a été introduit, compliquant ainsi la tâche d'identification pour l'ennemi.
- **Amélioration de la résolution radar** : permettant une détection plus précise et rapide des appareils en vol.

Le Mark III a été largement utilisé durant la fin de la Seconde Guerre mondiale et le début de la Guerre froide, marquant une étape majeure dans le développement des systèmes FFI modernes.

c Passage aux fréquences UHF/VHF

Avec l'évolution des systèmes de communication et la nécessité d'améliorer la fiabilité des systèmes FFI, une transition vers des fréquences plus élevées a été effectuée :

- **Passage aux bandes UHF (Ultra High Frequency) et VHF (Very High Frequency)** : ces fréquences offraient une meilleure portée et une réduction des interférences avec d'autres systèmes radio.
- **Introduction du chiffrement rudimentaire**: bien que primitif, ce chiffrement permettait d'augmenter la sécurité des transmissions et de limiter les possibilités d'imitation par l'ennemi.

3.1.2 TECHNIQUES AVANCÉES (1960-2000)

Avec les progrès technologiques réalisés dans les domaines des radars et des systèmes électroniques, de nouvelles solutions ont été mises en place pour renforcer l'identification et la sécurité des communications aériennes.

a FFI Mark XII (militaire) & Mode S (civil)

Les systèmes FFI militaires et civils ont connu une évolution majeure avec l'introduction du Mark XII et du Mode S, apportant plusieurs améliorations significatives :

- **Chiffrement des communications**: Pour pallier les risques de brouillage ou d'usurpation d'identité, des protocoles de chiffrement avancés ont été intégrés aux transmissions. Ces codes dynamiques permettent de sécuriser les échanges et d'empêcher toute interception malveillante.
- **Réponses multifréquences**: Afin de contrer les attaques par répétition, où un adversaire capte et rejoue un signal légitime, les transpondeurs ont été conçus pour émettre sur plusieurs fréquences. Cette approche réduit la vulnérabilité aux tentatives de fraude et améliore la fiabilité des réponses FFI.

b Intégration du GPS et des réseaux de communication

L'essor du positionnement par satellite et des technologies de communication a permis d'accroître la précision et la sécurité des systèmes d'identification aérienne :

- **Ajout de données de position précises**: L'intégration du GPS aux transpondeurs a permis d'associer aux signaux d'identification des informations de positionnement précises, renforçant ainsi l'authenticité des transmissions et la coordination du trafic aérien.
- **Protocoles d'identification dynamique** : Pour limiter les risques d'exploitation des signaux, des méthodes de sécurisation basées sur le renouvellement fréquent des clés de chiffrement ont été introduites, rendant plus difficile toute tentative de manipulation des transmissions.

3.1.3.TECHNIQUES MODERNES ADAPTÉES AUX DRONES (2000 - AUJOURD'HUI)

Avec l'essor rapide des drones, tant dans le domaine militaire que civil, les systèmes FFI ont dû évoluer pour offrir une identification fiable sans nécessiter d'intervention humaine directe.

a Identification par signature radar

- **Empreinte radar unique**: Chaque drone possède une signature spécifique résultant de la façon dont il réfléchit les ondes radar. Cette caractéristique permet de distinguer un drone allié d'un appareil inconnu.
- **Bases de données radar** : Les signaux entrants sont comparés à des profils de référence stockés, facilitant la détection d'éventuelles anomalies ou comportements suspects.

b Communication par protocole sécurisé (Mode 5 & ADS-B amélioré)

- **Chiffrement fort et signatures numériques (Mode 5)** : le Mode 5 repose sur l'utilisation de techniques de chiffrement avancées et de signatures numériques, empêchant toute falsification des signaux.
- **ADS-B renforcé** : destiné à la surveillance aérienne civile, l'ADS-B (Automatic Dependent Surveillance–Broadcast) a été amélioré pour sécuriser la transmission de la position des drones via satellite, prévenant ainsi les risques de piratage.

c Utilisation de l'intelligence artificielle (IA) et des modèles comportementaux

- **Algorithmes d'apprentissage machine** : les trajectoires de vol et les comportements des drones sont analysés en temps réel pour repérer d'éventuelles irrégularités, par exemple un drone hostile tentant d'imiter un drone ami.
- **Profils comportementaux**: Chaque drone se voit attribuer un historique de vol et un profil de fonctionnement, facilitant la détection d'anomalies et le déclenchement de contre-mesures adaptées.

d Techniques anti-brouillage et anti-usurpation

- **Sauts de fréquence** : les communications entre le drone et la station de contrôle changent régulièrement de fréquence, rendant le brouillage ou l'écoute illicite plus complexe.
- **Certificats numériques embarqués**: chaque drone dispose d'une identité numérique délivrée par une autorité de confiance, empêchant ainsi la contrefaçon ou la manipulation de ses signaux d'identification.

En conclusion, les technologies d'identification des drones ami/ennemi ont évolué depuis les simples transpondeurs jusqu'aux systèmes chiffrés et basés sur l'IA. L'avenir du FFI pourrait inclure **la blockchain pour la gestion des identités de drones, l'IA pour la reconnaissance comportementale, et des méthodes avancées de détection radar passive**.

3.2. L'OFFRE COMMERCIALE FFI DRONES EN 2024

Avec l'essor des drones dans les applications civiles et militaires, l'identification ami-ennemi (FFI) s'impose comme un élément clé de la gestion du trafic aérien et de la sécurité des opérations. Plusieurs solutions technologiques ont été développées pour répondre aux besoins spécifiques des UAV, combinant légèreté, autonomie et compatibilité avec les standards internationaux.

3.2.1 TECHNOLOGIES ET PRODUITS PROPOSÉS

Voici une liste non exhaustive des principaux produits commercialisés classifiées selon l'usage et la performance.

a Transpondeurs légers et compacts pour UAV tactiques

Ces transpondeurs sont conçus pour les drones légers et de reconnaissance, où l'optimisation du poids, de la consommation énergétique et de l'intégration est cruciale.

Exemple 1 : uAvionix ZPX-1 [5]

- **Format optimisé** : ultra-compact et léger, facilitant l'intégration sur les UAV tactiques.
- **Certification en cours** : développement conforme aux normes **AIMS Mark XIIB**, assurant une compatibilité avec les protocoles militaires modernes.
- **Capacités avancées** : intégration d'un **GPS certifié** et d'un **récepteur FFI passif**, améliorant l'autonomie et la résistance aux interférences.
- **Interopérabilité étendue** : compatible avec les standards civils et militaires pour une intégration sur diverses plateformes.
- **Sécurité des communications** : chiffrement avancé pour empêcher toute tentative d'usurpation ou de brouillage des signaux.

Exemple 2 : MX12B de Sagetech Avionics [6]

- **Transpondeur FFI Mode 5** : développé pour assurer une identification sécurisée dans un format réduit.
- **Normes militaires** : conforme aux exigences **DoD AIMS 17-1000 XIIB**, garantissant son utilisation dans les opérations modernes.
- **Polyvalence des modes** : prise en charge des **modes A, C, S et ADS-B Out**, garantissant une compatibilité avec les infrastructures aériennes civiles et militaires.
- **Optimisation SWaP** : ultra-léger et compact, idéal pour une intégration sur des UAV avec des contraintes de poids.
- **Évolutivité** : mise à niveau possible vers **Mode 5 Niveau 2B**, facilitant l'adaptation aux futures normes.

b Transpondeurs haute performance pour missions critiques

Ces modèles sont dédiés aux UAV opérant dans des environnements hostiles ou nécessitant une portée étendue.

Exemple : Modèle MD500L [7]

- **Conçu pour les missions critiques** : dédié aux **drones cibles, UAV tactiques et missiles de croisière**.
- **Format optimisé** : volume de **90 pouces cubes**, garantissant une intégration compacte et discrète.
- **Puissance d'émission élevée** : **500W**, offrant une portée étendue pour une identification efficace.
- **Fonctionnalités avancées** : supporte le **Mode C** (report d'altitude) et **suppression des signaux FFI/TACAN** pour éviter les interférences.
- **Résistance aux conditions extrêmes** : conforme à la **norme MIL-STD-810**, assurant un fonctionnement fiable dans des environnements hostiles.

c Transpondeurs multi-usage pour drones et aéronefs civils/militaires

Ces transpondeurs offrent une compatibilité étendue avec les aéronefs civils et militaires, intégrant des standards réglementaires variés.

Exemple 1 : TSC 4000 de Thales [8]

- **Mini transpondeur FFI Mode 5/Mode S** : conçu pour les **plateformes légères** nécessitant une identification avancée.
- **Certification multi-usage** : conforme à la **norme DO-260B** pour la transmission et réception **ADS-B.**
- **Connectivité avancée** : interfaces variées (**ARINC485, ARINC 429, Ethernet, option MIL-STD-1553**), facilitant son intégration.
- **Format optimisé** : **136 x 89 x 212 mm, poids de 2,1 kg**, permettant une installation simplifiée sur diverses plateformes.
- **Puissance d'émission** : **320W**, assurant une couverture efficace pour l'identification longue portée.

Exemple 2 : uAvionix ZPX-A [9]

- **Solutions micro SWaP** : idéales pour les UAV tactiques nécessitant des systèmes **légers et performants**.
- **Conformité avec l'espace aérien civil** : fonctionnement en **Mode S / 1090ES ADS-B**, garantissant une compatibilité avec les infrastructures de surveillance civile.
- **Puissance optimisée** : transmission à **250W**, permettant une **identification fiable** sans impacter l'autonomie énergétique des UAV.
- **Sécurisation des communications** : compatible avec les **systèmes de cryptographie avancés** pour prévenir toute falsification des signaux d'identification.

Le tableau présenté dans la page suivante, provenant du rapport de DSIAC de 2018 [10] présente un survey des transpondeurs FFI.

IFF Manufacturer & Name		Modes Available‡						Characteristics												Existing Certifications					Other		
Company	Nomenclature	1	2	3A	3C	4	5	S/ADS-B In/Out	Peak Power Out§ (W)	Weight (lbs)	Length (inch)	Width (inch)	Height (inch)	Volume (cu. inch)	Crypto Capable	Requires Crypto Applique (CA)	Crypto Applique Weight** (lbs)	Crypto Applique Volume (cu. inch)	Total Weight (lbs)	Total Volume (inch³)	AIMS	ETSO ††	FAA ‡‡	NSA §§	STANAG ***	Currently Integrated on	Unit Cost (USD)	Notes
AIR Avionics [6]	VT-01 ultra-compact	—	—	—	—	—	—	Yes	220	1.30	6.69	2.42	2.42	39.18	No	Not CA Compat.	—	—	1.30	39.18	—	Yes	—	—	—	—	$1,950	ADS-B/Mode-S only. No Mode 4/5 capability.
BAE Systems [5]	AN/APX-123	Yes	Yes	Yes	Yes	Yes	Yes	Yes	500	12.00	5.38	5.38	8.38	241.96	Yes	No	—	—	12.00	241.96	Yes	—	Yes	Yes	—	Manned aircraft	$35,000	Current manned aircraft transponder.
BAE Systems [7]	AN/DPX-7 (with GPS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	500	6.00	5.38	5.38	4.00	115.56	Yes	Yes	1.00	14.90	7.00	130.46	Yes	—	Yes	Yes	—	New smaller unit	—	Current, smaller-sized unit for UAS and small aircraft; Raytheon KIV-77 Crypto Applique ‡‡‡
Intelligent Automation [8]	Micro Trx	Yes	Yes	Yes	Yes	Yes	Yes	Yes	250	1.00	1.62	3.28	0.63	3.35	Yes	No	—	—	1.00	3.35	—	—	—	—	—	SBIR II	—	Embedded crypto; Small Business Innovation Research (SBIR) N142-102, Phase I & II [2, 3].
Leonardo [9]	M428	Yes	Yes	Yes	Yes	Yes	Yes	Yes	500	5.50	4.88	3.31	7.87	127.12	Yes	Yes	1.10	21.20	6.60	148.32	Yes	—	—	—	Yes	Manned aircraft	—	Current manned aircraft transponder; Leonardo SIT2010 Crypto Applique. †††
Micro Systems Inc. [10]	MD500L	Yes	Yes	Yes	Yes	—	—	—	500	4.00	5.00	5.13	2.52	64.64	No	Not CA Compat.	—	—	4.00	64.64	—	—	Yes	—	—	—	—	No Mode 4/5 capability.
Naval Air Warfare Center Aircraft Division 4.11.2 [11]	Organic transponder	Yes	Yes	Yes	Yes	Yes	Yes	Yes	157	2.00	3.50	4.25	2.70	40.16	Yes	Yes	0.00	0.00	2.00	40.16	—	—	—	Yes	—	Prototype	$12,000	Integrated with KIV-77.
R Cubed Engineering [1–4]	Micro Trx	Yes	Yes	Yes	Yes	Yes	Yes	Yes	500	1.00	3.50	2.00	0.30	2.10	Yes	No	—	—	1.00	2.10	—	—	—	—	—	SBIR II	—	Embedded crypto; SBIR N142-102, Phase I & II, [2, 3]; also see SBIR Phase I, A3.02, [4].
Raytheon (Korean Air) [12]	Mini XP Mark IIA Trx	Yes	Yes	Yes	Yes	Yes	Yes	Yes	150	5.00	—	—	—	100.00	Yes	Yes	1.00	14.90	6.00	114.90	—	—	—	Yes	—	Korean Air Lines UAS	—	Requires KIV-77 CA. ‡‡‡
Sagetech [13]	MX12A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	316	0.33	3.30	2.40	0.91	7.21	Yes	Yes	1.00	14.90	1.33	22.11	Yes	—	Yes	—	—	Certified units were to be shipped late 2018	—	SBIR N142-02, Phase I [3], noncertified MXS and MXS-G Mode S/ADS-B variants now available. Certified MXS and MXS-G units were to be shipped mid-2018. Certified MX12 units were to be shipped late 2018.
Sagetech [13]	MX12A-G (with GPS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	316	0.51	3.30	2.40	0.91	7.21	Yes	Yes	1.00	14.90	1.51	22.11	Yes	—	Yes	—	—	Certified units were to be shipped late 2018	$16,675	SBIR N142-02, Phase I [3], noncertified MXS and MXS-G Mode S/ADS-B variants now available. Certified MXS and MXS-G units were to be shipped mid-2018. Certified MX12 units were to be shipped late 2018.
Sagetech [13]	MXS	—	—	Yes	Yes	—	—	Yes	316	0.33	3.30	2.40	0.91	7.21	No	Not CA Compat.	—	—	0.33	7.21	—	—	Yes	—	—	Certified units were to be shipped mid-2018	$6,100	SBIR N142-02, Phase I [3], noncertified MXS and MXS-G Mode S/ADS-B variants now available. Certified MXS and MXS-G units were to be shipped mid-2018. Certified MX12 units were to be shipped late 2018.
Sagetech [13]	MXS-G (with GPS)	—	—	Yes	Yes	—	—	Yes	316	0.51	3.30	2.40	0.91	7.21	No	Not CA Compat.	—	—	0.51	7.21	—	—	Yes	—	—	Certified units were to be shipped mid-2018	$6,665	SBIR N142-02, Phase I [3], noncertified MXS and MXS-G Mode S/ADS-B variants now available. Certified MXS and MXS-G units were to be shipped mid-2018. Certified MX12 units were to be shipped late 2018.
Sagetech [14]	XPC-TR	—	—	Yes	Yes	—	—	—	250	0.22	3.50	1.80	0.70	4.41	No	Not CA Compat.	—	—	0.22	4.41	Yes	—	No	—	—	—	—	Also see parent company Unmanned Systems Technology (UST) [15].
Sagetech [14]	XPC-TR-50	—	—	Yes	Yes	—	—	—	250	0.22	3.50	1.80	0.70	4.41	No	Not CA Compat.	—	—	0.22	4.41	—	—	No	—	—	ScanEagle; RQ-21A	$4,350	Also see parent company UST [15].
Sagetech [14]	XPG-TR (with GPS)	—	—	Yes	Yes	—	—	Yes	250	0.32	4.00	1.80	1.00	7.20	No	Not CA Compat.	—	—	0.32	7.20	—	—	No	—	—	Aerial Targets	$5,200	Also see parent company UST [15].

IFF Manufacturer & Name		Modes Available‡						Characteristics												Existing Certifications					Other		
Company	Nomenclature	1	2	3A	3C	4	5	S/ADS-B In/Out	Peak Power Out§ (W)	Weight (lbs)	Length (inch)	Width (inch)	Height (inch)	Volume (cu. inch)	Crypto Capable	Requires Crypto Applique (CA)	Crypto Applique Weight** (lbs)	Crypto Applique Volume (cu. inch)	Total Weight (lbs)	Total Volume (inch³)	AIMS	ETSO ††	FAA ‡‡	NSA §§	STANAG ***	Currently Integrated on	Unit Cost (USD)	Notes
Sagetech [14]	XPS-TR	—	—	Yes	Yes	—	—	Yes	250	0.22	3.50	1.80	0.70	4.41	No	Not CA Compat.	—	—	0.22	4.41	—	—	No	—	—	—	$5,264	Also see parent company UST [15].
Seamatica Aerospace [16]	Micro-IFF Trx	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	—	—	—	—	—	Yes	Yes	—	—	—	—	—	—	—	—	—	—	—	Appears to be the same as the R Cubed Engineering version; website literature notes that development is a joint partnership among SMA, R Cubed Engineering, and Kratos Lancaster.
Telephonics [17]	Small lightweight Trx (SLT)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	500	4.00	5.00	4.60	5.20	119.60	Yes	Yes	1.00	14.90	5.00	134.50	Yes	Yes	Yes	—	Yes	—	—	Requires KIV-77 Crypto Applique. ‡‡‡
Thales [18]	TSC 1430	Yes	Yes	Yes	Yes	Yes	Yes	Yes	150	3.50	2.40	7.24	8.88	154.30	Yes	Yes	1.00	14.90	4.50	169.20	—	—	—	—	Yes	Aircraft, UAS	—	Current aircraft and UAS transponder; Raytheon KIV-77 Crypto Applique. ‡‡‡
Trig Avionics [19]	TT26 (with GPS)	—	—	Yes	Yes	—	—	Yes	250	1.04	6.02	2.83	2.44	41.57	No	Not CA Compat	—	—	1.04	41.57	—	Yes	—	—	—	Manned aircraft	—	No Mode 4/5 capability. GPS/Alt incorporated.
uAvionix [20]	ECHOESX 11-15207	—	—	Yes	Yes	—	—	Yes	250	0.17	1.77	2.76	0.67	3.27	No	Not CA Compat	—	—	0.17	3.27	—	—	Yes	—	—	Commercial UAS	$1,675	No Mode 4/5 capability.
uAvionix [21]	PING-2020	—	—	Yes	Yes	—	—	Yes	30	0.04	0.98	1.54	0.47	0.71	No	Not CA Compat	—	—	0.04	0.71	—	—	Yes	—	—	Commercial UAS	—	No Mode 4/5 capability.

3.3. SYNTHÈSE DES TRAVAUX SCIENTIFIQUES SUR LE FFI

Les recherches récentes sur l'identification ami-ennemi (FFI) appliquée aux drones mettent en lumière des avancées majeures en intelligence artificielle, en cybersécurité et en optimisation énergétique. Ces travaux visent à renforcer la fiabilité et la sécurité des systèmes FFI dans un contexte où les UAV deviennent omniprésents dans les opérations civiles et militaires.

3.3.1 MÉTHODES BASÉES SUR L'INTELLIGENCE ARTIFICIELLE

L'essor du **machine learning** a permis d'améliorer considérablement les capacités de classification et d'identification des drones à partir de leurs signaux radar et de leurs trajectoires de vol [11]. Parmi les approches les plus prometteuses :

- **Analyse des signatures radar Doppler** : l'utilisation de modèles avancés permet de différencier un drone ami d'un appareil inconnu en fonction de sa signature radar unique [12].
- **Détection d'anomalies via deep learning** : l'intelligence artificielle peut analyser en temps réel les schémas de vol et identifier des comportements suspects, facilitant ainsi la détection de drones ennemis imitant des trajectoires alliées [13].

3.3.2 SÉCURISATION DES COMMUNICATIONS FFI

Les systèmes FFI modernes nécessitent des protocoles de communication robustes pour contrer les cyberattaques et garantir l'intégrité des transmissions [14]. Parmi les solutions étudiées :

- **Authentification par cryptographie quantique** : cette approche révolutionnaire utilise les principes de la mécanique quantique pour empêcher toute tentative d'interception et de falsification des signaux FFI [15].
- **Clés de chiffrement dynamiques** : afin d'empêcher le piratage des transpondeurs, des systèmes adaptatifs modifient les clés de chiffrement à chaque interrogation radar, rendant toute tentative d'usurpation inefficace [16].

3.3.3 FFI POUR LES DRONES AUTONOMES

L'intégration de FFI aux **flottes de drones collaboratifs** représente un défi majeur, nécessitant des solutions innovantes pour garantir une identification fiable entre appareils autonomes [17]. Les axes de recherche incluent :

- **Protocoles légers et basse consommation** : minimiser l'impact énergétique des systèmes FFI pour prolonger l'autonomie des drones tout en assurant une identification continue [18].
- **Algorithmes décentralisés** : réduire la dépendance à une infrastructure centralisée en développant des **protocoles peer-to-peer**, où chaque drone peut valider en temps réel l'identité de ses homologues sans nécessiter de connexion permanente à un serveur central [19].

3.4. PERSPECTIVES FUTURES

Les recherches actuelles suggèrent que l'avenir de FFI pour les drones repose sur des innovations technologiques visant à renforcer la fiabilité, la sécurité et l'efficacité des systèmes d'identification. Plusieurs axes de développement sont envisagés pour répondre aux défis posés par la prolifération des UAV et la complexification des menaces.

3.4.1 DÉVELOPPEMENT DE SYSTÈMES HYBRIDES

Une approche combinant plusieurs méthodes d'identification semble être une solution prometteuse pour maximiser la fiabilité des systèmes FFI. Parmi les stratégies explorées :

- **Fusion de capteurs** : intégration de plusieurs sources de données (radar, vision, radiofréquence) afin d'améliorer la précision et la robustesse de l'identification.
- **Systèmes à double validation** : association de méthodes actives (balises, transpondeurs) et passives (analyse comportementale et signatures électromagnétiques) pour éviter les erreurs et les tentatives d'usurpation.
- **Analyse multi-niveau** : vérification de l'identité d'un drone à différentes étapes de son vol (détection initiale, validation continue, mise à jour en temps réel des identités).

3.4.2 UTILISATION DE L'INTELLIGENCE ARTIFICIELLE ET DU MACHINE LEARNING

L'intelligence artificielle joue un rôle croissant dans l'identification des drones, permettant d'analyser en temps réel les schémas de vol, les signatures électromagnétiques et les communications radio pour détecter les menaces potentielles.

- **Modèles prédictifs** : comparaison des trajectoires de drones avec des modèles normaux afin de repérer les anomalies et comportements suspects.
- **Apprentissage adaptatif** : mise à jour continue des bases de données des drones amis et ennemis, permettant aux systèmes FFI de s'adapter aux nouvelles stratégies adverses.
- **Systèmes autonomes** : capacité pour les drones de pré-identifier eux-mêmes leurs homologues avant de relayer les informations aux stations de contrôle, réduisant ainsi les délais de validation.

3.4.3 MISE EN PLACE DE PROTOCOLES SÉCURISÉS ET ÉVOLUTIFS

Avec l'augmentation des risques cybernétiques, la cybersécurité devient un élément clé des systèmes FFI. Plusieurs solutions sont envisagées pour prévenir les tentatives de brouillage, d'usurpation et de piratage des transmissions entre drones :

- **Chiffrement avancé** : utilisation d'algorithmes de cryptographie de dernière génération pour sécuriser les échanges et empêcher toute interception malveillante.
- **Authentification par blockchain** : enregistrement des identifiants des drones dans une blockchain sécurisée afin d'assurer leur intégrité et d'éliminer les risques de falsification [20].
- **Protocoles à faible latence** : développement de méthodes de vérification d'identité rapides et efficaces, garantissant une réaction immédiate en cas de menace, sans compromettre la sécurité des communications.

3.4.4 AUTRES ÉVOLUTIONS TECHNOLOGIQUES PROMETTEUSES

Les avancées scientifiques et technologiques ouvrent également de nouvelles perspectives pour améliorer la détection et l'identification des drones :

- **Détection passive par interférences WiFi** : exploitation des perturbations des signaux WiFi pour identifier et suivre les drones sans émettre d'ondes radar supplémentaires [21].
- **Fusion multi-capteurs** : association des technologies radar, vision et acoustique pour améliorer la robustesse de l'identification et réduire les risques de brouillage [22].

Ces avancées positionnent le FFI comme un élément central de la gestion du trafic aérien des drones, garantissant une meilleure coordination et une sécurité accrue sur les théâtres d'opérations modernes.

Les publications scientifiques montrent une **transition vers des systèmes FFI autonomes**, i**ntelligents et sécurisés**, capables de faire face aux **menaces cybernétiques émergentes**. L'intégration de l'**IA, du chiffrement avancé et des protocoles optimisés** constitue l'axe principal des recherches actuelles.

4. CONCLUSION

L'identification des drones amis-ennemis est un enjeu stratégique pour la sécurité aérienne. Si les technologies actuelles offrent des solutions partielles, elles sont confrontées à des défis majeurs liés à la fiabilité, aux contraintes matérielles et à l'absence de standards internationaux.

Les avancées en **fusion de capteurs, intelligence artificielle et cybersécurité** ouvrent la voie à des solutions plus robustes et adaptatives. Toutefois, pour garantir l'efficacité des systèmes FFI, il est essentiel d'adopter une **approche hybride** combinant identification active et passive, tout en mettant en place des **protocoles sécurisés** et évolutifs.

Enfin, l'évolution rapide des menaces impose une **coopération internationale** et le **développement de normes unifiées** pour assurer une reconnaissance fiable des drones dans les environnements les plus complexes.

Ce rapport a été rédigé pour service de point de départ et pour permettre de pouvoir comprendre les enjeux de l'identification des drones amis-ennemis, les défis et contraintes auxquels sont soumises ces solutions, l'évolution des technologies utilisées (au fil des années) pour répondre à la problématique ainsi que les ouvertures et perspectives des travaux futurs. Les références citées viennent compléter les informations mentionnées.

RÉFÉRENCES

< RÉFÉRENCES >

[1] https://www.faa.gov/uas/getting_started/remote_id

[2] Tang Z, Ma H, Qu Y, Mao X (2025). UAV Detection with Passive Radar: Algorithms, Applications, and Challenges. *Drones*.

[3] https://www.princeton.edu/~ota/disk1/1993/9351/9351.PDF

[4] https://artillerie.asso.fr/docs/RADARS/IFF%20LK.pdf

[5] https://uavionix.com/defense/zpx/

[6] https://sagetech.com/wp-content/uploads/2021/02/MX12B-Datasheet-Certified-Mode-5-IFF-Micro-Transponder.pdf

[7] https://www.kratosdefense.com/products/uav/radios/avionics/identify-friend-or-foe

[8] https://www.thalesgroup.com/fr/tsc-4000-family

[9] https://uavionix.com/defense/zpx-1/

[10] https://dsiac.dtic.mil/wp-content/uploads/2018/02/dsiac-2187511.pdf

[11] Al-Sa'd, M. F., Daoud, M. I., & Mallat, K. (2018). Machine learning for UAV identification using RF signatures. Journal of Communications.

[12] Kim, J., Park, S., & Lee, H. (2021). Doppler radar and AI for IFF in drone swarms. Sensors.

[13] Zhao, L., Wang, H., & Chen, P. (2022). Anomaly detection in UAV swarms using deep learning. IEEE Transactions onAerospace and Electronic Systems.

[14] Wang, Y., Liu, B., & Zhang, R. (2021). Cybersecurity challenges in IFF: A review. IEEE Access.

[15] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics.

[16] Sun, Y., Zhao, X., & Li, J. (2020). Dynamic encryption techniques for secure IFF communication. Future Generation Computer Systems.

[17] Rahman, A., Tan, C., & Ho, Y. (2023). Scalable IFF protocols for UAV swarms. IEEE Internet of Things Journal.

< RÉFÉRENCES >

[18] Bhatt, P., Kumar, R., & Prasad, A. (2021). Lightweight authentication schemes for drone networks. Wireless Personal Communications.

[19] Chen, L., Xu, M., & Zhang, Q. (2022). Decentralized IFF using federated learning. IEEE Transactions on Networking.

[20] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Blockchain for IoT security: A review. IEEE Internet of Things Journal.

[21] Youssef, M., Ibrahim, M., & Agrawal, P. (2021). Passive sensing for IFF using WiFi signals. ACM MobiCom.

[22] Abdelrahman, M., Said, A., & Hanafi, S. (2022). Multi-modal IFF using radar, acoustic and visual sensors. IEEE Sensors Journal.

< Studio des Communs >

CAMPUS CYBER

Campus Cyber Nouvelle-Aquitaine

POUR EN SAVOIR PLUS : **WIKI.CAMPUSCYBER.FR**
ADRESSE MAIL DE CONTACT : **COMMUNAUTES@CAMPUSCYBER.FR**
5 - 7 RUE BELLINI 92800, PUTEAUX

Ce projet a été financé par le gouvernement dans le cadre du Programme d'investissements d'avenir.

INVESTIR L'AVENIR