République Tunisienne
Ministère De La Défense Nationale
Armée De L'Air
Ecole De L'Aviation De Borj El Amri

PROJET DE FIN D'ÉTUDES

Présenté pour obtenir Le

DIPLÔME NATIONAL D'INGENIEUR

Réalisé par:

S/LT ALAA DOUZI

Né le : 14 /12/2001 à Tunis

Sujet :

Etude et développement d'un système de sécurité contre les menaces cybernétiques sur les équipements de bord modernes des avions de l'Armée de l'Air

Encadré par :

Commandant Anis GHARSALLAH

EABA

Année Universitaire : 2024/2025

Remerciement

Ce projet marque l'aboutissement de cinq années de travail intense, de sacrifices et de défis surmontés. Un chemin parsemé d'embûches, mais aussi de moments de grâce, où chaque effort a été illuminé par le soutien de ceux qui m'ont tendu la main.

Au terme de ce projet de fin d'études, je tiens tout d'abord à exprimer mes sincères remerciements à **M. Le Colonel Commandant de l'École de l'Aviation Borj El Amri**, pour son organisation, son encouragement et l'intérêt qu'il nous a accordé pour la réalisation de notre projet de fin d'études

Je tiens à exprimer ma profonde gratitude au **Commandant Anis GHARSALLAH** pour son accompagnement précieux, ses conseils éclairés et sa bienveillance tout au long de cette aventure intellectuelle. Son expertise et son exigence ont été des phares dans les moments de doute, et je lui suis infiniment reconnaissant pour sa confiance.

Dans cette aventure, je n'aurais jamais pu avancer sans le soutien inébranlable de ma famille, ces cœurs qui ont battu au rythme de mes efforts, portant mes espoirs comme les leurs.

À mon père,

Tu m'as appris que les silences pouvaient être plus éloquents que les discours. Même absent, tu es présent dans chaque ligne de ce mémoire. Le 1er avril 2025, le destin a cru pouvoir nous séparer, mais il a oublié que ton héritage vit en moi. Tes leçons de courage résonnent dans mes choix, ta rigueur guide encore ma main quand j'écris. Là-haut, parmi les anges, regarde-moi achever ce que tu as commencé. Je serai toujours ton petit garçon… mais aujourd'hui, je suis l'homme que tu as rêvé de voir grandir. Ce diplôme, je l'ai achevé avec une douleur au cœur, mais aussi avec la certitude que, quelque part, ton sourire fier m'accompagne.

À ma mère,

Ton amour a été mon premier refuge et mon dernier rempart. Chaque repas préparé avec tant d'attention, chaque "Je sais que tu peux y arriver" murmuré à mon oreille, chaque prière silencieuse pour ma réussite… Tout cela a tissé un filet de tendresse sur lequel je pouvais tomber sans crainte. Merci d'avoir été ma plus fervente admiratrice, bien avant que je n'aie quelque chose à montrer.

À ma sœur,

Tu as été bien plus qu'une complice dans ce parcours. Tu as été mon ancre et ma voile – celle qui me retenait quand le vent menaçait de tout emporter, et celle qui m'a poussé à avancer quand je doutais de mes forces. Tes rires ont allégé mes nuits de travail, tes mots ont séché mes larmes d'épuisement. Merci d'avoir été cette lumière quand l'horizon semblait sombre.

À vous trois,

Vous êtes l’âme de ce succès. Ce parchemin porte vos noms autant que le mien. Si la vie m’a appris une chose, c’est que l’amour ne meurt pas – il se transforme en force. Et c’est cette force qui m’a permis d’aller jusqu’au bout.

Enfin, merci à tous ceux qui ont marché à mes côtés : enseignants, amis, mentors. Vous avez été les artisans discrets de cette victoire.

Ce projet n’est pas une fin, mais un commencement – celui d’une vie où je porterai toujours en moi vos voix, vos sourires, et cette promesse : "Tu n’es pas seul."

Dédicace

“À la lumière de ceux qui ont illuminé mon chemin,

Au Commandant Anis GHARSALLAH,

Pour votre guidance précieuse et votre confiance sans faille,

Votre soutien a été mon ancre.

À mes chers parents

Maman, pour ton amour inconditionnel et tes sacrifices silencieux,

Papa, bien que parti trop tôt, ton esprit veille sur moi.

Cette réussite est aussi la tienne.

À ma sœur,

Complice des nuits blanches et des joies partagées,

Merci d’avoir été mon pilier dans les moments décisifs.

À mes amis et camarades de promo,

Artisans de mes rires et remparts contre les doutes,

Vous avez transformé l’effort en complicité.

À tous ceux,

D’un mot, d’un geste ou d’une présence,

Qui ont fait de ce parcours un voyage humain.

Je vous porte dans ma gratitude."

Table des matières

Liste des figures

Liste des Tableaux

Liste des abreviations

ABAS : Aircraft-Based Augmentation System (

ACARS : Aircraft Communications Addressing and Reporting System

ADS-B : Automatic Dependent Surveillance-Broadcast

AES : Advanced Encryption Standard (Norme de chiffrement avancée)

AFDX : Avionics Full-Duplex Switched Ethernet

AIDS : Anomaly-based Intrusion Detection

ARINC 429 : Aeronautical Radio Incorporated 429

CAN : Controller Area Network

CNN : Convolutional Neural Network (Réseau de neurones convolutionnels)

C/N0 : Carrier-to-Noise Density Ratio (Rapport porteur sur bruit)

CSV : Comma-Separated Values

DDoS : Distributed Denial of Service (Déni de service distribué)

DL : Deep Learning (Apprentissage profond)

DoS : Denial of Service (Déni de service)

EDA : Exploratory Data Analysis

EFIS : Electronic Flight Instrument System

ESS : Embedded Systems Security

FAA : Federal Aviation Administration

FMS : Flight Management System

GBAS : Ground-Based Augmentation System

GNS3 : Graphical Network Simulator 3

GNSS : Global Navigation Satellite System

GPS : Global Positioning System

GUI : Graphical User Interface

HIDS : Host-based Intrusion Detection System

HUMS : Health Usage Monitoring Systems

ICAO : International Civil Aviation Organization)

IDS : Intrusion Detection System

IFE : In-Flight Entertainment

ILS : Instrument Landing System

INS : Inertial Navigation System

IP : Internet Protocol

IPS : Intrusion Prevention System

ISR : Intelligence, Surveillance, Reconnaissance

L1 C/A : GPS L1 Coarse/Acquisition (Signal GPS L1 à acquisition grossière)

LSTM : Long Short-Term Memory

MAE : Mean Absolute Error

MFD : Multi-Function Display

MITM : Man-in-the-Middle

ML : Machine Learning

MSE : Mean Squared Error

NAT : Network Address Translation

ND : Navigation Display

NIDS : Network-based Intrusion Detection System

PFD : Primary Flight Display

PVT : Position, Velocity, Time (Position, vitesse, temps, données GNSS)

RNN : Recurrent Neural Network (Réseau neuronal récurrent)

SATCOM : Satellite Communication

SBAS : Satellite-Based Augmentation System

SIDS : Signature-based Intrusion Detection System

SIEM : Security Information and Event

SNR : Signal-to-Noise Ratio (Rapport signal sur bruit)

TCAS : Traffic Collision Avoidance System

TEXBAT : Texas Spoofing Test Battery (Batterie de tests d'usurpation de l'Université du Texas)

UI : User Interface (Interface utilisateur)

VM : Virtual Machine (Machine virtuelle)

Introduction générale

« "La technologie est un outil, mais comme tout outil, elle peut devenir une arme à double tranchant" : Dans l'aviation militaire moderne, cette réalité se cristallise autour des avions, désormais véritables cerveaux numériques volants. Leur hyperconnectivité, source de puissance tactique, façonne aussi leur talon d'Achille. Chaque capteur, chaque algorithme, chaque flux de données devient une porte dérobée pour des cyberattaques – autant de maillons vulnérables, exposés à des attaques dont la fréquence a bondi de **140% depuis 2020** (SANS Institut). Ces attaques, capables de corrompre des systèmes critiques, de la navigation aux communications, transformant ces géants de l'innovation en proies silencieuses.

Avec l'essor des technologies embarquées, les systèmes électroniques et informatiques intégrés aux avions militaires jouent un rôle crucial dans la modernisation et l'efficacité des forces aériennes. Dans ce cadre, l'Armée de l'Air Tunisienne en ligne avec sa Vision 2030, met l'accent sur l'intégration de technologies avancées pour améliorer les capacités opérationnelles de ses vecteurs aériens. Cependant, cette évolution rapide des systèmes embarqués s'accompagne d'un accroissement des menaces cybernétiques ciblant ces équipements stratégiques. Les cyberattaques, de plus en plus sophistiquées, mettent en péril l'intégrité, la disponibilité et la confidentialité des systèmes embarqués, compromettant ainsi la sécurité des missions aériennes et des informations sensibles. Selon plusieurs études, le nombre d'attaques ciblant les systèmes avioniques a considérablement augmenté ces dernières années, soulignant la nécessité de renforcer la cybersécurité dans ce domaine critique.

Afin de garantir la sécurité des vols, il est primordial de mettre en place des systèmes de détection et de prévention des intrusions adaptés aux spécificités avioniques. Ces systèmes permettent d'identifier les tentatives d'attaques et de prévenir toute compromission des communications et du contrôle des aéronefs.

Face aux menaces croissantes, Quels systèmes de détection et mesures de prévention des intrusions peut-on mettre en place pour sécuriser les réseaux avioniques contre les cyberattaques ?

Dans ce contexte, notre projet s'intéresse particulièrement à la conception et au développement d'un système de détection d'intrusions pour les avions, capable d'identifier en temps réel les cybermenaces et d'y répondre efficacement. L'objectif est de proposer une solution adaptée aux contraintes aéronautiques, combinant détection par signature et analyse comportementale, tout en intégrant des techniques avancées comme le Machine Learning pour améliorer la précision de détection.

L'interconnectivité, essentielle pour améliorer les performances et l'autonomie des avions, expose ces derniers à des cyberattaques potentielles, en particulier les avions militaires modernes qui reposent sur une architecture embarquée avancée intégrant divers systèmes de navigation, de communication et de contrôle, interconnectés via des réseaux complexes. Malgré la mise en place de protocoles sécurisés, ceux-ci ne suffisent pas toujours à détecter efficacement les attaques sophistiquées, telles que le GPS spoofing, la manipulation des signaux ADS-B, ou encore les intrusions par Wi-Fi et USB. Face à l'émergence de menaces sous diverses formes – intrusions malveillantes, détournement de commandes ou exploitation des vulnérabilités logicielles – il devient une priorité majeure de développer une approche innovante pour améliorer la réactivité face aux menaces émergentes et renforcer la sécurité des systèmes embarqués, en s'alignant sur les priorités stratégiques de l'Armée de l'Air Tunisienne

Pour bien étayer le bien fondée de cette idée, la première partie sera consacrée à présenter un état des lieux des concepts fondamentaux liés à la cybersécurité aéronautique et aux menaces avioniques. Le deuxième chapitre est dédié à l'étude technique et à la conception du système proposé, en analysant les solutions et en détaillant notre approche et méthodologies technique. Enfin, le dernier chapitre se focalise sur l'implémentation de la solution, les tests réalisés, ainsi que les résultats obtenus et les perspectives d'amélioration.

Chapitre I :

État des lieux et Concepts fondamentaux

« Analyse des enjeux de la cybersécurité aéronautique et des menaces cybernétiques modernes »

Chapitre 1

État des lieux et Concepts fondamentaux

Introduction :

Les systèmes embarqués sont actuellement à la base des technologies aéronautiques modernes, notamment dans le domaine militaire. Si leur évolution rapide a permis d'améliorer les performances opérationnelles, la précision des missions et le niveau de connectivité des aéronefs, cette sophistication offre également des défis fiables et sécuritaires majeurs, tels que les vulnérabilités et les menaces cybernétiques. Cette section est abordée à travers trois composantes principales. Ainsi, dans ce contexte, des origines à la place centrale dans les avions modernes de l'Armée de l'Air Tunisienne jusqu'aux défis et enjeux.

Deuxièmement, il étudie les risques associés à un tel système de génération de systèmes futuriste, y compris les vulnérabilités du nouveau système moderne, les actions de piratage récemment réalisées sur le secteur de l'aviation et leurs conclusions pour la sécurité nationale et militaire proliferation. Enfin, il évalue les solutions existantes pour contrer ces menaces, tout en soulignant leurs limites et la nécessité d'innover, notamment à travers des systèmes de détection adaptatifs et proactifs.

À travers cette étude, nous visons à démontrer que la sécurisation des systèmes embarqués militaires ne peut se limiter à des correctifs ponctuels, mais exige une approche holistique, intégrant à la fois des technologies de pointe et une stratégie de modernisation alignée sur les impératifs de cybersécurité. Ce travail pose ainsi les bases pour comprendre les défis actuels et envisager des solutions durables, essentiels pour préserver la souveraineté et l'efficacité des forces aériennes dans un contexte géopolitique en mutation.

I. Étude de l'évolution technologique des systèmes embarqués :

I.1. Historique de développement des systèmes embarqués et leurs apports :

L'histoire des systèmes avioniques est étroitement liée à l'évolution de l'aviation comme étant une industrie très dynamique et sujet de plusieurs études innovatrices. Aux débuts, les pilotes utilisaient des instruments classiques basés sur la mécanique simple. Cependant, Avec les progrès technologiques du XX^{e} siècle, ces systèmes se sont désormais sophistiqués en incluant des composants électroniques, améliorant ainsi la fiabilité et l'efficacité de la conduite des opérations de vol. Ces systèmes peuvent être classés en plusieurs catégories à savoir :

Les catégories des systèmes :

Systèmes de navigation : L'avènement des systèmes de navigation satellitaire à savoir le GPS et le développement de système de gestion de vol en termes de performances et de suivi de vol sur les plans horizontale et verticale tel que le FMS ont révolutionné la navigation aérienne. En outre, l'intégration des EFIS , qui inclut des écrans PFD pour les paramètres de vol essentiels et MFD pour les informations complémentaires, a permis une automatisation accrue et une présentation claire des données de navigation, simplifiant ainsi la lecture et l'exploitation des information au sein de la cabine.

Systèmes de surveillance : Les radars primaires et secondaires ont été renforcé par des systèmes de surveillance avancés installé sur les avions à l'instar du TCAS , et les systèmes ADS-B ainsi que le radar météorologique intégré. Les informations de surveillance sont désormais affichées sur des MFD/ND, offrant une visualisation en temps réel de l'environnement de vol pour une meilleure prise de décision.

Systèmes de communication : La communication a évolué vers des systèmes numériques intégrés avec des capacités de liaison par satellite et de transmission de données sécurisée. Ces informations sont centralisées sur les EFIS et les MFD, permettant aux pilotes d'accéder rapidement aux données de communication sans distraction.

Systèmes d'approche et d'atterrissage : Les systèmes d'approche ont été évolué du système ILS vers des approches GPS de précision en intégrant des systèmes d'augmentation ABAS/GBAS/SBAS.

Les progrès des systèmes embarqués ne se limitent pas à la navigation, à la communication ou à la surveillance. Leur intégration a également permis une amélioration significative des

performances globales des aéronefs, en optimisant à la fois l'efficacité opérationnelle et la sécurité des vols.

I.2. L'impact des progrès technologiques sur les performances des systèmes de bords :

I.2.1. Les bienfaits :

Optimisation des performances :

Les systèmes embarqués modernes, tels que le **FMS (Flight Management System)**, jouent un rôle clé dans la gestion optimisée des trajectoires de vol, de la consommation de carburant et des temps de vol. En intégrant des données en temps réel sur les conditions météorologiques, les restrictions de trafic aérien et les caractéristiques de performance de l'avion, le **FMS** propose des itinéraires optimaux, réduisant ainsi les coûts opérationnels et l'impact environnemental.

Réduction de la charge de travail des pilotes :

Les systèmes comme les **EFIS** centralisent l'affichage des données critiques sur des écrans **PFD** et **MFD**, permettant aux pilotes de surveiller facilement les paramètres essentiels du vol. Cela réduit la charge cognitive, en particulier lors des phases critiques comme le décollage, l'atterrissage et les approches.

Fiabilité et maintenance prédictive :

L'intégration des **systèmes de diagnostic embarqués** permet de surveiller en permanence l'état des différents composants de l'aéronef. Les informations sur l'usure des pièces, les alertes de maintenance et les prévisions de défaillance sont transmises directement aux équipes au sol via les **systèmes ACARS (Aircraft Communications Addressing and Reporting System)**. Cela garantit une maintenance proactive, augmentant la disponibilité des appareils et réduisant les risques d'incidents.

Intégration et automatisation :

Les systèmes embarqués modernes sont conçus pour fonctionner de manière intégrée. Par exemple, les **systèmes de commande de vol électriques (Fly-by-Wire)** travaillent en synergie avec les **systèmes de gestion de vol** pour garantir une stabilité optimale et des réactions rapides face aux perturbations extérieures. L'automatisation croissante, tout en maintenant une supervision humaine, a permis de réduire les erreurs et d'améliorer la sécurité aérienne.

L’évolution historique des systèmes avioniques met également en lumière l’influence des besoins militaires sur l’innovation technologique. L'aviation militaire, y compris l'Armée de l'Air Tunisienne, a constamment investi dans des plateformes embarquées capables de répondre aux besoins opérationnelles, d'où l’importance de toucher de près les performances de ces systèmes et d'étudier leurs fiabilités envers les différentes menaces susceptibles.

Domaine	Avancée	Impact
Performance énergétique	Optimisation FMS des profils de vol (Continuous Descent Operations)	Réduction de 15-20% de la consommation de carburant (Source : ICAO 2022)
Charge cognitive pilote	Centralisation EFIS + alertes contextuelles	Diminution de 40% des erreurs humaines (étude Boeing 2021)
Maintenance	Diagnostics embarqués (HUMS - Health Usage Monitoring Systems)	Taux de disponibilité > 99% (données Airbus Defence 2023)

Tableau 1 : Optimisation des Performances Aéronautiques

I.2.2. Les risques associés :

L’intégration de systèmes embarqués avancés apporte des améliorations notables, mais expose également à de nouveaux risques technologiques :

- **Cybersécurité** : Les systèmes embarqués peuvent être vulnérables aux **cyberattaques** visant à compromettre les données de vol ou les communications d’où la nécessité d’utilisez des algorithmes de cryptage avancés et des systèmes de détection pour repérer et éliminer les menaces.
- **Fiabilité des informations** : Des erreurs ou des empêchements des capteurs peuvent fausser les données de navigation et de surveillance.
- **Guerre électronique** : Les adversaires peuvent utiliser le **brouillage** ou le **leurrage (spoofing)** pour perturber les systèmes embarqués.

Ainsi, Une stratégie équilibrée entre innovation technologique et sécurité opérationnelle est essentielle pour garantir la sécurisation des données dans le but de promouvoir la réussite de la mission confiée à la force aérienne.

I.3. Le défis de la modernisation des avions militaires de l'Armée de l'Air Tunisienne :

Les progrès technologiques dans le domaine des systèmes avioniques ont transformé l'aviation militaire, en offrant des capacités qui auraient été impensables il y a seulement quelques décennies. Les systèmes embarqués modernes permettent non seulement d'améliorer la précision des missions, mais aussi de renforcer l'interopérabilité interarmées grâce à des plateformes de communication avancées. Pour l'Armée de l'Air Tunisienne, ces avancées ont permis d'optimiser les capacités opérationnelles et logistiques en mesure de contribuer efficacement à la préservation de la sécurité nationale.

En effet, elle s'est engagée à moderniser sa flotte soit par l'acquisition des nouvelles capacités ou bien à travers la mise à niveau de certains vecteurs afin de répondre aux défis futurs. Cette modernisation a joué un rôle crucial dans des domaines variés tels que **la surveillance des frontières**, **le transport logistique**, **la défense aérienne**, **l'ISR**, **les missions humanitaires et les interventions d'urgence**.

En fait, le **Cessna C208B Grand Caravan**, récemment acquis est un avion polyvalent équipé du système avionique intégré Garmin G1000 qui inclut des fonctionnalités avancées, la gestion automatisée des données de vol et la surveillance en temps réel. Ces technologies améliorent l'efficacité des missions de reconnaissance et de surveillance dans des zones éloignées ou difficiles d'accès.

UH-60 Black Hawk : Cet hélicoptère est doté d'une avionique avancée, incluant des systèmes de gestion de vol intégrés et des capacités de communication sécurisées. Il est essentiel pour les missions tactiques et de secours, offrant une flexibilité opérationnelle accrue.

T-6 Texan II : Utilisé principalement pour la formation des pilotes militaires, il est équipé de systèmes avioniques modernes et des instruments de navigation avancés.

AS350 Écureuil : Cet hélicoptère léger a subit récemment une modernisation au niveau de ses systèmes de surveillance et de navigation.

C-130B/H Hercules : Les versions modernisées du C-130 sont équipées d'avionique numérique et de systèmes de gestion de vol améliorés, augmentant leur capacité pour les missions logistiques et humanitaires.

Conformément à la **vision stratégique 2030** de l'Armée de l'Air tunisienne, la modernisation des vecteurs aériens est considérée comme une priorité absolue dans le but de renforcer ses capacités opérationnelles et répondre aux défis stratégiques croissants qui couvrent des domaines variés tels que **la surveillance des frontières**, **le transport logistique**, **les missions humanitaires et les interventions d'urgence**. Toutefois, avec ces avancées technologiques viennent également des risques et la nécessité de mettre en place des contre-mesures adaptées pour garantir la fiabilité des informations et la sécurité des opérations.

Cette modernisation partielle pose des défis spécifiques :

- **Compatibilité technologique :** Les nouvelles technologies, telles que les **écrans EFIS**, les **MFD** et les **systèmes de communication numériques sécurisés**, doivent fonctionner harmonieusement avec les systèmes plus anciens de l'appareil. Une mauvaise intégration peut entraîner des dysfonctionnements critiques en vol.
- **Vulnérabilité aux cyberattaques:** Bien que les instruments aient été modernisés, les anciens avions n'étaient pas initialement conçus pour faire face aux menaces cybernétiques. La connectivité accrue des systèmes embarqués expose ces avions à des risques tels que le **piratage des systèmes de navigation** ou le **brouillage des communications**.
- **Besoin du personnel qualifié** : L'utilisation de technologies avancées nécessite une **formation continue et spécialisée** des pilotes et du personnel technique. La maîtrise des nouveaux systèmes, comme les **displays numériques**, les **FMS** et les **systèmes de guerre électronique**, demande des compétences spécifiques qui peuvent ne pas être immédiatement disponibles.

- **Maintenance complexe et coûteuse**: La modernisation des systèmes embarqués augmente la complexité des opérations de maintenance. Les nouveaux systèmes exigent des interventions techniques spécialisées et un approvisionnement régulier en pièces détachées modernes, ce qui peut poser un problème en raison des **contraintes budgétaires**.

II. Etude de risque des menaces cybernétiques sur les systèmes embarqués de nouvelle génération :

L'adoption de systèmes embarqués modernes dans l'aviation militaire a révolutionné les capacités opérationnelles, offrant des améliorations substantielles en performance, précision, et sécurité. Cependant, l'intégration de ces systèmes connectés a introduit de nouvelles surfaces d'attaque, exposant des vulnérabilités potentielles aux cybermenaces sophistiquées. Cette section approfondit l'analyse de ces vulnérabilités, présente des études de cas de cyberattaques avérées, et discute des répercussions possibles pour **l'Armée de l'Air Tunisienne**, en soulignant les implications stratégiques et les protocoles de défense susceptibles d'être mis en œuvre pour contrer ces menaces.

II.1. Vulnérabilités des systèmes embarqués modernes :

Les systèmes embarqués modernes, tels que les **EFIS (Electronic Flight Instrument System)**, **FMS (Flight Management System)** et les plateformes de communication, reposent sur des technologies numériques et des réseaux interconnectés. Bien que ces avancées améliorent l'efficacité et la précision des opérations militaires, elles introduisent également des vulnérabilités qui nécessitent une attention particulière.

Complexité accrue : La sophistication des systèmes embarqués augmente considérablement le risque d'attaque. Chaque composante Hard ou Soft peut constituer une porte d'entrée pour une attaque. Une seule faille peut être exploitée pour mettre en péril des systèmes critiques, tels que la navigation, la surveillance ou les communications. Par exemple, une erreur dans le logiciel de gestion de vol peut entraîner des décisions erronées et compromettre la sécurité aérienne.

Connectivité permanente : Les systèmes embarqués modernes sont souvent connectés à des réseaux internes et externes pour assurer le partage en temps réel des informations entre les aéronefs et les centres de contrôle au sol. Cette connectivité constante rend les systèmes vulnérables aux attaques de type **"Man-in-the-Middle"** ou aux piratages des transmissions de données. Un attaquant pourrait intercepter ou falsifier les informations transmises, compromettant la mission.

Composants tiers et sous-traitance : La dépendance à des composants ou logiciels fournis par des tiers peut introduire des vulnérabilités cachées. La sécurité de la chaîne d'approvisionnement

est cruciale, car un maillon faible peut compromettre l'ensemble du système. Par exemple, un logiciel malveillant inséré lors de la fabrication pourrait échapper aux contrôles de sécurité et être activé en vol.

Obsolescence et compatibilité: La modernisation partielle des avions plus anciens peut entraîner des incompatibilités entre les nouveaux systèmes numériques et les anciennes plateformes mécaniques ou analogiques. Ces incompatibilités créent des points de vulnérabilité exploitables par des attaquants. De plus, le maintien de systèmes obsolètes augmente le risque d'exploitation de failles non corrigées.

Ces vulnérabilités nécessitent la mise en place de contremesures de cybersécurité robustes, incluant des systèmes de détection et de prévention des intrusions (**IDS/IPS**), des audits réguliers de sécurité et des protocoles de communication sécurisés.

II.2. Étude des cas de cyberattaques ciblant les systèmes de bord :

Les cyberattaques visant les systèmes embarqués représentent une menace croissante pour l'aviation militaire. L'Armée de l'Air Tunisienne, comme d'autres forces aériennes modernes, doit faire face à ces menaces en comprenant les types d'attaques existantes, leurs techniques et leurs conséquences potentielles. Pour cela, l'analyse d'exemples concrets permet d'identifier les failles possibles et de mettre en place des mesures préventives adaptées.

II.2.1. Types de cyberattaques ciblant les systèmes de bord :

- **Attaques par injection de code** : Ces attaques consistent à insérer du code malveillant dans les systèmes embarqués. Cela peut permettre à un attaquant de prendre le contrôle d'une fonction critique de l'aéronef, comme le système de navigation ou de communication.
- **Attaques par déni de service (DoS) :** Un attaquant peut saturer un système avec des requêtes afin de le rendre indisponible. Par exemple, Les échanges vitaux entre l'avion et le centre de contrôle pourraient être interrompus en raison d'un système de communication surchargé**.**
- **Attaques de type Man-in-the-Middle (MITM):** Ces attaques impliquent l'interception et la modification des communications entre deux systèmes. Par exemple, un attaquant pourrait altérer des données de mission transmises à un avion en vol.
- **Exploitation des faiblesses de sécurité physique** : Les accès non sécurisés aux ports physiques des systèmes embarqués peuvent permettre une intrusion directe. Par exemple, le branchement d'un dispositif malveillant sur un port de maintenance pourrait compromettre le système.

- **Les hotspots WIFI, « lien direct » vers le monde extérieur :** L'avion contemporain, bardé de systèmes informatiques semi-autonomes présente plusieurs points de vulnérabilité. Rien n'est plus évident que le wifi. Les compagnies offrent des hotspots payants pour leurs passagers.. De nombreux chercheurs sont inquiets de voir une technologie comme l'Internet sans fil, qui repose sur le protocole IP, se propager dans les cockpits en raison de sa vulnérabilité indéniable.

II.2.2. Analyse réelle des attaques :

En 2023, une analyse détaillée des données sur les cyberattaques dans le secteur aérien a révélé des tendances intéressantes et des variations mensuelles notables. En janvier, le secteur a recensé 10 incidents, marquant un début d'année relativement calme. Cette tranquillité a été de courte durée, car les mois suivants ont vu une augmentation significative des attaques, avec 82 en février et 91 en mars, indiquant une intensification des activités malveillantes. Les mois d'avril, mai et juin ont montré une certaine stabilité, bien que les attaques aient légèrement diminué en juin (63). La période estivale a connu une baisse continue, avec 64 attaques en juillet, 62 en août, et 60 en septembre. Le dernier trimestre de l'année a été marqué par une hausse progressive, atteignant un pic en octobre (74), suivie d'une légère baisse en novembre (41) et décembre (43).

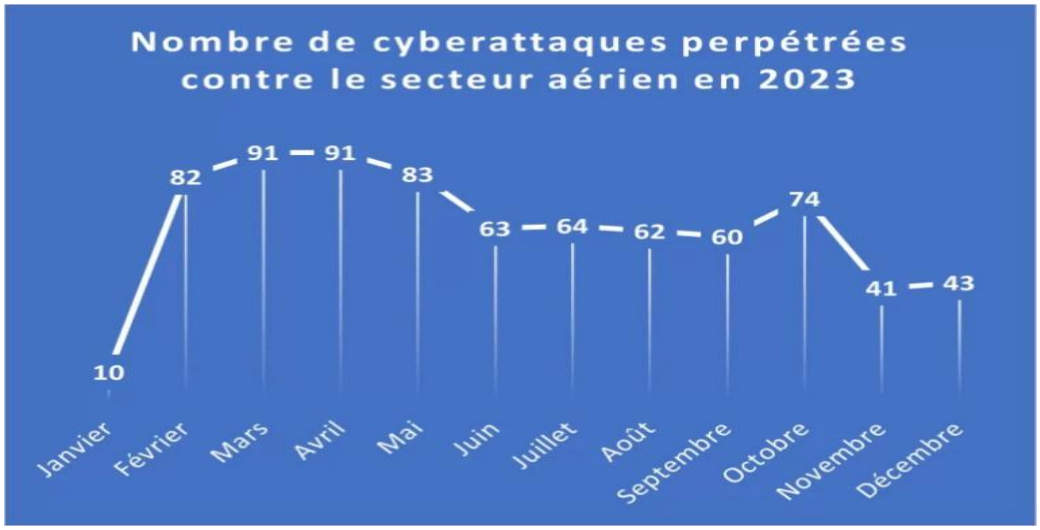


Figure 1 : Nombre de cyberattaques contre le Secteur aérien en 2023

Parmi les 764 cyberattaques recensées dans le secteur aérien en 2023, deux types principaux se distinguent : les attaques par Déni de Service Distribué (DDoS) et les attaques par ransomwares. Les données suivantes illustrent la répartition entre ces deux catégories :

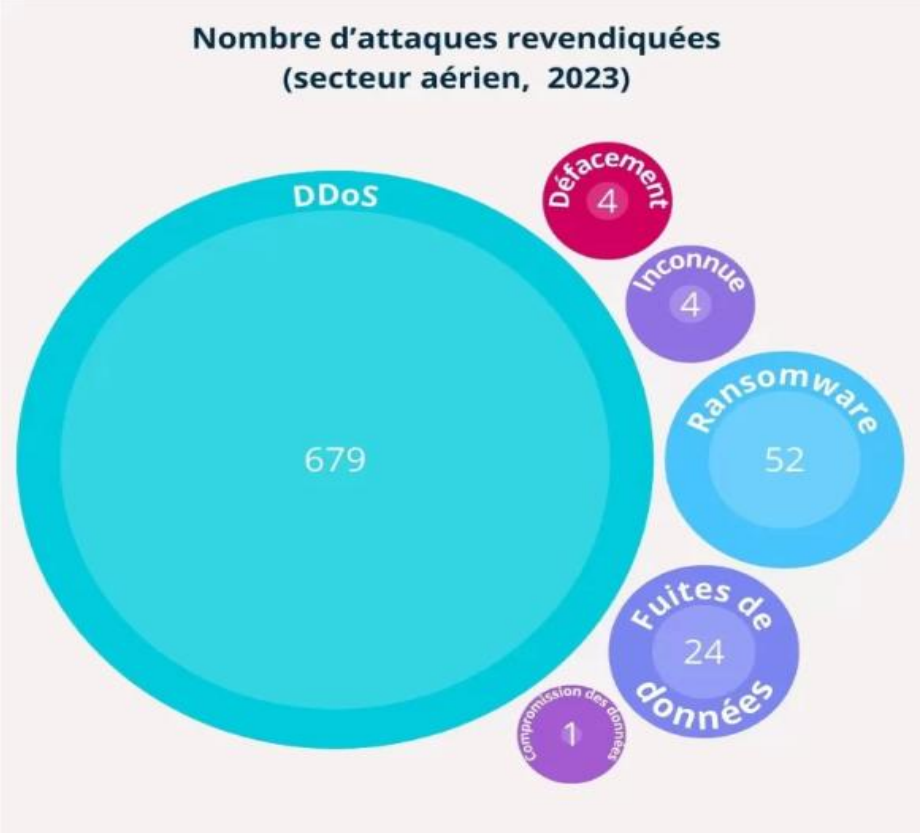


Figure 2 : Nombre d'attaques revendiquées en 2023 (Secteur aérien)

Exemple réel d'attaque n°1 : Intrusions via les systèmes de divertissement en vol (IFE)

En **2015**, le chercheur en cybersécurité **Chris Roberts** a démontré la possibilité de compromettre le système de divertissement en vol (**IFE**) pour interagir avec des systèmes critiques de l'aéronef. Cet incident a révélé des failles de sécurité préoccupantes dans l'aviation civile qui pourraient, par analogie, menacer les systèmes militaires.

Analyse de l'attaque :

Technique utilisée : *Chris Roberts* a exploité une connexion non sécurisée entre l'IFE et d'autres systèmes embarqués critiques. En accédant à l'IFE via le port de connexion sous le siège, il a injecté du code malveillant pour interagir avec le système de contrôle de l'avion.

Vulnérabilités exploitées :

- **Manque de séparation** entre le système de divertissement (non critique) et les systèmes de bord critiques.
- **Absence de segmentation réseau**, permettant à une intrusion depuis un sous-système non critique de se propager aux systèmes critiques.

Implications pour l'aviation militaire : Bien que cette attaque concerne l'aviation civile, elle met en lumière le danger potentiel pour les avions militaires dotés de systèmes connectés. Une telle intrusion pourrait compromettre les systèmes de navigation, de surveillance ou de communication des avions de combat et de transport.

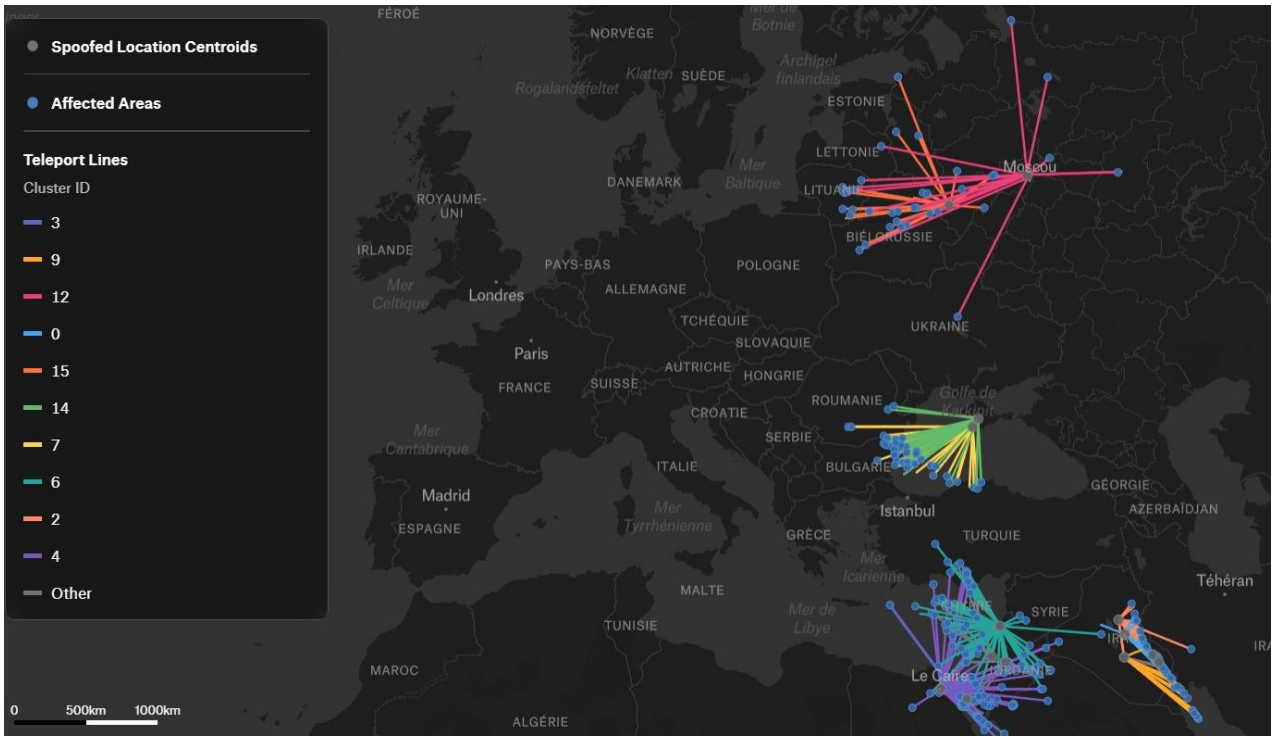


Figure 3 : Carte de brouillage et usurpation des signaux GPS

Exemple réel d'attaque n°2 : Incident : Brouillage GPS en Syrie et en Irak :

En **2019**, des incidents répétés de **GPS Spoofing** ont été signalés dans les zones de conflit en **Syrie** et en **Irak**, affectant les opérations militaires de la coalition internationale. Les aéronefs militaires opérant dans ces régions ont subi des perturbations de navigation, compliquant les missions de reconnaissance et de frappe aérienne.

Contexte : Les forces militaires opérant dans ces régions utilisaient des systèmes GPS pour la navigation et le ciblage. Les perturbations étaient attribuées à des opérations de guerre électronique menées par des forces hostiles dans un effort pour contrecarrer les missions de la coalition.

Les dispositifs de spoofing GPS, probablement déployés par des groupes hostiles ou soutenus par des États, ont diffusé des signaux GPS falsifiés dans des zones stratégiques. Ces signaux ont trompé les récepteurs GPS des avions militaires, les amenant à calculer des positions incorrectes, compromettant ainsi la précision des opérations.

- **Mécanisme de l'attaque**

Technique employée :

- Émission de signaux GPS falsifiés via des émetteurs haute puissance, imitant les satellites légitimes.
- Submersion des récepteurs embarqués, entraînant un décalage progressif des positions affichées (sans déclencher d'alerte).

Vulnérabilités exploitées :

Faiblesse	Conséquence
Absence de détection embarquée	Acceptation passive des signaux spoofés
Dépendance exclusive au GPS	Aucune validation par des systèmes inertiels (INS) ou astronavigation
Protocoles non chiffrés	Facilité de réplication des trames GPS civiles (L1 C/A)

Tableau 2 : Vulnérabilités des Systèmes GPS et Leurs Conséquences Opérationnelles

Impact potentiel sur l'aviation militaire :

Si une telle attaque ciblait des avions militaires, elle pourrait fausser les données de navigation en plein vol, entraînant :

- Des déviations involontaires de trajectoires.
- Des violations de l'espace aérien étranger.
- Des perturbations critiques lors de missions de reconnaissance ou de combat.

Conséquences de l'attaque :

- **Perturbation des opérations stratégiques :** Pour des avions militaires, une désorientation en plein vol compromet l'efficacité et la sécurité des missions. Par exemple, lors

d’une mission de surveillance des frontières, une position erronée peut entraîner une perte de couverture de zones critiques.

- **Risques pour la sécurité du personnel** : Une navigation imprécise augmente le risque d’accidents, en particulier dans des conditions météorologiques difficiles ou lors d’opérations nocturnes.
- **Impact sur la prise de décision** : Des informations falsifiées peuvent entraîner des erreurs de jugement de la part des pilotes et des contrôleurs aériens, compromettant l’intégrité des opérations militaires.

Exemple réel d'attaque n°3 : Capture du drone américain RQ-170 Sentinel par l'Iran (2011)

En décembre 2011, un événement marquant a mis en lumière les vulnérabilités des systèmes embarqués dans le domaine de l'aviation militaire : la capture d'un drone américain RQ-170 Sentinel par les forces iraniennes. Ce drone furtif, utilisé principalement pour des missions de reconnaissance, a été intercepté alors qu'il survolait l'espace aérien iranien. Les autorités iraniennes ont affirmé avoir réussi à prendre le contrôle de l'appareil en exploitant une faille dans son système de navigation GPS, utilisant une technique de **spoofing** (usurpation de signal).

Figure 4 : Iran captured RQ-170 drone

❖ **Détails de l'attaque :**

Technique utilisée : Les Iraniens ont envoyé de faux signaux GPS au drone, trompant son système de navigation et le forçant à atterrir sur un site contrôlé par l'Iran. Cette méthode de spoofing a permis de contourner les mesures de sécurité du drone sans endommager l'appareil.

Vulnérabilité exploitée : Le drone RQ-170 dépendait fortement des signaux GPS pour sa navigation. Les attaquants ont exploité cette dépendance en injectant des signaux GPS falsifiés, ce qui a induit le système en erreur.

Conséquences : La capture du drone a permis à l'Iran d'étudier la technologie américaine, ce qui a eu des implications stratégiques et militaires significatives. De plus, cet incident a exposé les faiblesses des systèmes embarqués face aux cyberattaques sophistiquées.

- **Analyse et implications :**

Impact sur la sécurité aérienne : Ce cas démontre que même les systèmes militaires les plus avancés peuvent être vulnérables à des attaques par spoofing. Il souligne l'importance de sécuriser les systèmes de navigation contre de telles menaces.

Besoins en contre-mesures : L'incident a mis en évidence la nécessité de développer des systèmes de détection d'intrusions (IDS) capables d'identifier et de contrer les attaques par spoofing. Des solutions basées sur la machine learning pourraient être envisagées pour détecter les anomalies dans les signaux GPS.

Leçons apprises : Cet événement a incité les forces armées à revoir la sécurité des systèmes embarqués, en intégrant des mécanismes de protection supplémentaires et en réduisant la dépendance aux signaux GPS externes.

Conclusion et recommandations :

Ces exemples démontrent la vulnérabilité des systèmes embarqués des avions militaires face à des menaces complexes et évolutives. Pour faire face à ces risques, il est crucial de :

- Mettre en place des mécanismes de détection et de correction des signaux GPS falsifiés.
- Adopter une architecture réseau segmentée pour empêcher une intrusion d'un sous-système non critique vers des systèmes critiques.
- Utiliser des systèmes de navigation redondants (navigation inertielle, radio-navigation) pour réduire la dépendance aux signaux GPS.
- Former régulièrement le personnel militaire aux meilleures pratiques de cybersécurité et aux procédures d'urgence en cas de compromission des systèmes.

II.3. Conséquences potentielles des menaces cybernétiques sur l'aviation militaire :

L'intégration des systèmes embarqués modernes a profondément transformé l'aviation militaire en améliorant ses capacités opérationnelles et stratégiques. Cependant, cette avancée technologique s'accompagne de risques considérables liés aux cybermenaces, qui peuvent avoir des impacts dévastateurs sur plusieurs niveaux, allant de la compromission des missions critiques à la mise en péril de la sécurité nationale.

II.3.1. Compromission des missions stratégiques :

Une cyberattaque sur un avion militaire peut compromettre l'intégrité des missions de reconnaissance, de surveillance ou de combat. Ces impacts incluent :

- **Déviations de trajectoire ou échecs des missions** : Des attaques ciblant les systèmes de navigation, comme le GPS spoofing, peuvent conduire un appareil à dévier involontairement de sa route ou à échouer dans l'exécution de sa mission.
- **Exposition des positions militaires** : Les attaques sur les radars ou les systèmes de communication peuvent permettre à des adversaires d'identifier la position et les intentions des forces armées, affaiblissant ainsi la stratégie militaire.
- **Perte de coordination :** Une désorganisation des systèmes de communication embarqués pourrait perturber l'efficacité des opérations en équipes, qu'il s'agisse de frappes aériennes ou de missions conjointes.

II.3.2. Altération et fuite de données sensibles :

Les systèmes embarqués gèrent et échangent des données cruciales, allant des plans de mission aux communications tactiques. Une cyberattaque réussie peut :

- **Modifier les données stratégiques** : Une manipulation des données pourrait induire les pilotes ou les équipes de commandement en erreur, compromettant la précision des décisions.
- **Exposer des informations classifiées** : Le vol de données par des adversaires pourrait leur donner un avantage stratégique en anticipant les plans militaires.
- **Endommager les bases de données embarquées :** Les cyberattaques peuvent détruire ou corrompre des données critiques, rendant les systèmes inutilisables sans une réparation complexe.

II.3.3. Risques pour la sécurité humaine et matérielle :

Les attaques ciblant les systèmes embarqués peuvent également affecter directement la sécurité des équipages et des appareils :

- **Accidents et incidents en plein vol :** Une attaque compromettant des systèmes critiques, comme les commandes de vol ou les capteurs, peut entraîner des accidents aériens graves.

- **Mises en danger des équipages** : Les cyberattaques sur les avions de combat ou de transport peuvent exposer les pilotes et les passagers à des situations dangereuses, notamment en temps de guerre.
- **Perte d'équipement coûteux :** La perte d'un avion militaire à cause d'une cyberattaque peut avoir un impact économique significatif et affaiblir les capacités opérationnelles à court terme.

II.3.4. Impacts sur la logistique militaire :

Les appareils tels que les C-130 Hercules, essentiels pour le transport de troupes et de matériel, sont également vulnérables. Une cyberattaque ciblant ces systèmes peut entraîner :

- **Des retards dans le déploiement des forces :** Un transport aérien compromis pourrait affecter la rapidité et l'efficacité des opérations terrestres ou maritimes.
- **Des interruptions dans les chaînes d'approvisionnement :** Les missions de ravitaillement en zones hostiles pourraient être perturbées, affectant directement les troupes sur le terrain.

II.3.5. Implications stratégiques et diplomatiques :

Les cyberattaques sur les avions militaires ne se limitent pas à des impacts opérationnels, elles ont également des répercussions sur le plan stratégique :

- **Réduction de la crédibilité militaire :** La divulgation de vulnérabilités dans les systèmes embarqués pourrait compromettre la capacité de l'Armée de l'Air Tunisienne à collaborer avec d'autres pays.
- **Perturbation des alliances :** Une cyberattaque non détectée pourrait exposer les informations d'alliés, nuisant à la coopération militaire internationale.
- **Perte de dissuasion stratégique :** Un adversaire capable de pirater les systèmes embarqués militaires pourrait réduire la capacité de dissuasion de l'armée**.**

II.3.6. Conséquences économiques :

Enfin, les cyberattaques entraînent des coûts directs et indirects considérables :

- **Réparations coûteuses :** La correction des systèmes compromis exige des investissements massifs, à la fois pour réparer les dégâts et pour prévenir de futures attaques.
- **Impact sur la disponibilité opérationnelle :** Les appareils mis hors service à la suite d'une attaque peuvent réduire significativement les capacités de l'armée à répondre aux situations d'urgence.

III. Les contres mesures adoptées pour la lutte contre les menaces cybernétiques et leurs performances :

Avec l'évolution rapide des cybermenaces, l'aviation militaire se trouve confrontée à des défis complexes en matière de cybersécurité. Les systèmes de défense existants, bien que robustes, présentent certaines lacunes qui appellent à l'innovation et à l'adoption de nouvelles solutions. Cette partie explore les systèmes de défense actuels, analyse leurs anomalies, et introduit le besoin d'une nouvelle solution intégrée pour une meilleure protection.

III.1. Les Systèmes de Défense Existants Contre les Cyberattaques :

Dans l'aviation militaire, la protection des systèmes embarqués contre les cybermenaces est cruciale pour assurer la sécurité des missions et l'intégrité des appareils. Les systèmes de défense actuels se concentrent sur la prévention, la détection et la réponse rapide aux cyberattaques. Voici une analyse des principales technologies utilisées :

Chiffrement des Communications	❖ Le chiffrement assure la confidentialité et l'intégrité des communications entre les appareils, rendant les données inaccessibles aux acteurs malveillants.
Pare-feu Spécialisés pour l'Aviation	❖ **Pares-feux embarqués** : Conçus spécifiquement pour les environnements aéronautiques, ces dispositifs filtrent le trafic réseau entrant et sortant des systèmes avioniques, limitant les vecteurs d'attaque à distance.
	❖ **Contrôle d'accès basé sur les rôles :** Garantit que seules les communications autorisées sont établies, empêchant les connexions non sécurisées avec les systèmes externes.
Sécurisation des Réseaux de Communication Aérienne (ACARS et SATCOM) :	❖ **Chiffrement avancé :** Les communications entre les avions et les centres de contrôle utilisent des protocoles de chiffrement robustes pour protéger les données sensibles contre les interceptions et les modifications.

	❖ **Authentification renforcée :** Les systèmes d'authentification multi-facteurs sont utilisés pour valider les communications, réduisant ainsi les risques de faux ordres ou d'accès non autorisé.
Systèmes de Gestion des Risques et des Incidents de Sécurité (SIEM) dans les Bases Aériennes	❖ **Surveillance en temps réel** : Les bases aériennes utilisent des SIEM pour collecter et analyser les logs des avions en mission. Cela permet une corrélation rapide des événements suspects et une réponse immédiate en cas d'anomalie.
	❖ **Tableaux de bord de sécurité** : Fournissent une vue d'ensemble des menaces potentielles, aidant les équipes à prioriser les réponses aux incidents.
Solutions de Sécurité des Systèmes Embarqués (ESS)	❖ **Antivirus et antimalware spécialisés :** Les systèmes embarqués sont équipés de solutions capables de détecter et de neutraliser les logiciels malveillants conçus pour cibler les infrastructures critiques.
	❖ **Analyse comportementale :** Ces outils surveillent les systèmes pour détecter des comportements déviants qui pourraient indiquer une intrusion.
Gestion Sécurisée des Chaînes d'Approvisionnement pour les Composants Avioniques	❖ **Validation des fournisseurs** : Chaque composant ou logiciel embarqué passe par un processus de validation rigoureux pour s'assurer qu'il ne contient pas de vulnérabilités ou de portes dérobées exploitables.
	❖ **Suivi des mises à jour :** Les mises à jour logicielles sont scrutées pour garantir qu'elles n'introduisent pas de nouvelles failles de sécurité.

Simulation et Formation à la Cyberdéfense	❖ **Exercices de simulation de cyberattaques** : Les équipages et les équipes au sol participent à des exercices de simulation pour améliorer leur capacité à répondre efficacement à des cyberattaques en conditions réelles.
	❖ **Programmes de formation continue** : Assurent que le personnel est au fait des dernières menaces et des meilleures pratiques en matière de cybersécurité.

Tableau 3 : Mesures Clés et Protections Avancées existants pour les Systèmes Embarqués et les Communications

Ces systèmes constituent une ligne de défense essentielle contre les cybermenaces, mais ils doivent être continuellement mis à jour pour faire face à l'évolution rapide des techniques d'attaque. L'intégration de ces technologies avec des solutions innovantes, comme les systèmes de détection d'intrusion spécifiques à l'aviation, est essentielle pour garantir la résilience des infrastructures aériennes militaires.

III.2. Les Anomalies des Systèmes Actuels de Cybersécurité Embarqués :

Bien que ces systèmes de défense aient prouvé leur efficacité dans de nombreux cas, ils présentent également des limites significatives qui peuvent compromettre la sécurité :

Réactivité et Temps de Réponse :	De nombreux systèmes actuels, bien qu'efficaces dans la détection des menaces, réagissent souvent après que l'attaque a commencé. Cette approche réactive peut être insuffisante pour prévenir les dommages dans des environnements critiques comme l'aviation militaire.
Fragmentation des Solutions :	Les différentes solutions de cybersécurité sont souvent déployées de manière fragmentée, ce qui peut entraîner des problèmes d'interopérabilité et compliquer la gestion centralisée de la sécurité.

Manque de Visibilité Complète :	Les systèmes actuels peuvent manquer de visibilité sur l'ensemble de l'environnement réseau, limitant ainsi leur capacité à détecter des attaques complexes et coordonnées.
Évolutivité Limitée :	Les cybermenaces évoluent rapidement, et les systèmes de sécurité existants peuvent ne pas s'adapter suffisamment vite. L'absence de mise à jour régulière des signatures d'attaque et des règles de détection laisse les systèmes vulnérables à des attaques nouvelles ou inconnues.
Coût et Complexité de la Maintenance :	Les solutions actuelles nécessitent souvent une maintenance intensive et un personnel hautement qualifié, ce qui peut représenter un défi pour les forces armées en termes de ressources et de budget.

Tableau 4 : Les Anomalies des Systèmes Actuels de Cybersécurité Embarqués

III.3. Besoin d'une Nouvelle Solution (Introduction au Concept de systéme) :

Face aux limites identifiées, le développement de solutions plus avancées est impératif. C'est ici qu'intervient la nécessité d'introduire un Système de Détection et de Prévention des Intrusions (IDS/IPS) avancé, spécifiquement conçu pour répondre aux exigences uniques de l'aviation militaire.

Détection Proactive et Réponse Automatisée :

Contrairement aux systèmes existants, un IDS/IPS moderne utilise l'intelligence artificielle et l'apprentissage automatique pour analyser le comportement du réseau en temps réel. Cela permet de détecter les anomalies avant qu'elles ne se transforment en attaques, offrant une protection proactive.

Intégration et Centralisation :

Une nouvelle solution IDS/IPS intégrée peut offrir une vue centralisée de la sécurité du réseau, facilitant la corrélation des données et l'identification des menaces complexes. L'intégration des différents systèmes de défense dans une plateforme unifiée permet une meilleure coordination et efficacité.

Adaptabilité et Évolutivité :

Grâce à des mises à jour régulières et des capacités d'apprentissage, un IDS/IPS avancé peut s'adapter aux nouvelles formes de menaces. Cette évolutivité garantit que le système reste efficace face à l'évolution constante des cybermenaces.

Amélioration Continue :

Un IDS/IPS moderne inclut des fonctionnalités d'analyse post-incidente pour comprendre les vecteurs d'attaque utilisés et renforcer les défenses en conséquence. Cette capacité d'amélioration continue est cruciale pour maintenir un niveau de sécurité élevé.

Formation et Sensibilisation :

En complément des solutions techniques, il est essentiel de former le personnel militaire à reconnaître et à réagir aux cybermenaces. Une solution IDS/IPS moderne peut inclure des outils de formation intégrés pour renforcer la vigilance et la réactivité des équipes.

En conclusion, bien que les systèmes de défense actuels aient posé des bases solides pour la cybersécurité de l'aviation militaire, les défis posés par les menaces modernes exigent des solutions plus avancées et intégrées. L'introduction d'un IDS/IPS innovant constitue une étape cruciale dans la protection des systèmes embarqués et la sécurisation des opérations militaires.

Chapitre 2 :
Étude technique et conception de la solution IDS

"Vers une architecture IDS/IPS adaptative pour la cybersécurité aéronautique"

Chapitre 2

Étude technique et conception de la solution IDS

Introduction

L'aviation militaire moderne est confrontée à une complexité croissante en raison de l'intégration de systèmes numériques sophistiqués et interconnectés à bord des aéronefs. Ces systèmes, essentiels pour les missions de reconnaissance, de surveillance et de combat, augmentent également la surface d'attaque des cybermenaces. La mise en œuvre d'un système de détection des intrusions à bord est donc cruciale pour garantir la sécurité des communications, des données de navigation et des commandes de vol. L'objectif de ce chapitre est de passer en revue les bases théoriques des systèmes de détection et de prévention des intrusions (IDS/IPS), d'analyser les solutions existantes et de présenter la conception de la solution que nous proposons pour améliorer la cybersécurité des aéronefs.

I. Bases théoriques des systèmes de détection :

I.1 Définition et objectifs des IDS :

Un IDS (Intrusion Detection System) est conçu pour surveiller et analyser le trafic réseau ou les activités du système afin d'identifier un comportement anormal ou des tentatives d'intrusion. Dans le contexte de l'aviation militaire, un IDS embarqué est conçu pour protéger les systèmes critiques contre les cyber-attaques qui pourraient compromettre la mission ou mettre en péril la sécurité de l'aéronef. Son rôle est d'assurer une détection précoce des intrusions, permettant une réponse rapide et efficace..

I.2 Catégories d'IDS : NIDS et HIDS :

Les systèmes de détection d'intrusion (IDS) se déclinent principalement en deux catégories : **Network-based Intrusion Detection Systems (NIDS)** et **Host-based Intrusion Detection Systems (HIDS)**. Ces deux approches ont des rôles complémentaires et sont souvent utilisées conjointement pour fournir une couverture de sécurité complète.

Network-based Intrusion Detection System (NIDS):

Un NIDS surveille le trafic réseau pour détecter des activités suspectes ou des violations de politiques de sécurité. Il est déployé à des points stratégiques du réseau, comme les routeurs, les commutateurs ou directement dans les segments de réseau critiques.

Host-based Intrusion Detection System (HIDS):

Un HIDS est installé directement sur un système ou un appareil hôte (comme un serveur, une station de travail ou un dispositif embarqué) pour surveiller les activités locales. Il se concentre sur l'intégrité des fichiers, les journaux d'activité, et les comportements système pour détecter les intrusions.

	NIDS	**HIDS**
Fonctionnement	**Capture et Analyse :** Un NIDS capture les paquets de données circulant sur le réseau et les analyse en temps réel. **Détection de Signatures** : Il compare les paquets capturés avec une base de données de signatures connues pour identifier des menaces spécifiques (ex : attaques par déni de service, infections de logiciels malveillants). **Détection d'Anomalies** : Il peut aussi repérer des anomalies en analysant les schémas de trafic, identifiant des comportements inhabituels par rapport à un profil de trafic normal.	**Surveillance des Fichiers :** Il surveille les fichiers systèmes clés pour détecter toute modification non autorisée. **Analyse des Journaux :** Un HIDS examine les journaux d'événements du système, des applications et de la sécurité pour repérer des comportements suspects. **Contrôle de l'Intégrité :** Il peut vérifier la somme de contrôle des fichiers critiques pour détecter toute altération.
	Couverture étendue : Un NIDS peut surveiller l'ensemble du trafic réseau, offrant une vue d'ensemble des activités potentielles. **Détection des Attaques Externes :** Il	**Détection des Intrusions Locales :** Un HIDS est efficace pour repérer les attaques internes ou celles qui ont déjà franchi le périmètre réseau. **Analyse Détaillée :** Il offre une

Avantages	est particulièrement efficace pour repérer les attaques provenant de l'extérieur du périmètre du réseau.	vision granulaire des activités au niveau du système hôte, permettant une détection précise des anomalies.
Limite	**Environnement Chiffré :** Les NIDS peuvent avoir du mal à analyser le trafic chiffré, rendant certaines attaques invisibles. **Faux Positifs :** L'analyse comportementale peut générer des alertes sur des activités légitimes, augmentant les faux positifs.	**Ressources Système :** Un HIDS peut consommer des ressources système importantes, ce qui peut affecter les performances. **Visibilité Limitée :** Contrairement à un NIDS, un HIDS ne surveille pas le trafic réseau global, limitant sa portée aux activités du système hôte.
Processus d'Application à l'Aviation	Dans un avion militaire, un NIDS pourrait être déployé pour surveiller les communications entre les différents systèmes avioniques (ex : systèmes de navigation, gestion de vol, et liaison de données). Il assurerait la détection de toute tentative d'intrusion ou de perturbation dans ces flux de données critiques.	Dans un avion, un HIDS pourrait être intégré directement dans les systèmes critiques tels que l'ordinateur de mission ou le système de gestion de vol. Il assurerait la surveillance de l'intégrité de ces systèmes pour prévenir toute altération non autorisée, garantissant ainsi la fiabilité des opérations de l'aéronef.

Tableau 5 : : Comparaison des Systèmes de Détection d'Intrusions (NIDS vs HIDS)

Comparaison et Complémentarité :

- **NIDS** offre une couverture large et est adapté pour détecter les menaces provenant du réseau.
- **HIDS** fournit une vision détaillée et est crucial pour la protection des systèmes critiques internes.

Dans un contexte d'aviation militaire, la combinaison des deux, en utilisant un système hybride, renforcerait la sécurité en assurant une protection à la fois au niveau du réseau et des systèmes hôtes, répondant ainsi aux exigences élevées de sécurité pour les missions aériennes.

Un système de prévention des intrusions :

Un système de prévention des intrusions (IPS) va plus loin en prenant des mesures pour bloquer ou neutraliser l'attaque en cours.

I.3 Classification des IDS :

La taxonomie des systèmes de détection d'intrusion (IDS) permet de classifier les différentes approches et techniques utilisées pour identifier les activités malveillantes dans un réseau ou sur un hôte. Cette classification est cruciale pour comprendre les capacités et les limites de chaque type d'IDS, en particulier dans le contexte des systèmes embarqués pour l'aviation militaire. Voici une description détaillée des différentes dimensions de classification :

❖ Méthodes de Détection :

Les IDS peuvent être classés en fonction des méthodes qu'ils utilisent pour détecter les intrusions:

- **Basés sur les signatures (Signature-Based IDS) :** Les systèmes de détection d'intrusion par signature (ou SIDS : Signature-based Intrusion Detection System), reposent sur des bibliothèques de description des attaques (appelées signatures). Au cours de l'analyse du flux réseau, le système de détection d'intrusion analysera chaque événement et une alerte sera émise dès lors qu'une signature sera détectée. Cette signature peut référencer un seul paquet, ou un ensemble. Cette méthodologie de détection se révèle être efficace uniquement si la base de signatures est maintenue à jour de manière régulière. Dans ce cas, la détection par signatures produit peu de faux-positifs. Cependant, une bonne connaissance des différentes attaques est nécessaire pour les décrire dans la base de signature. Dans le cas d'attaques inconnues de la base, ce modèle de détection s'avérera inefficace et ne générera donc pas d'alertes. La base de signature est donc très dépendante de l'environnement (système d'exploitation, version, applications déployées, …). Pour effectuer une détection par signature, on peut utiliser, Les arbres ou les systèmes de transition d'états.
- **Basés sur les anomalies (Anomaly-Based IDS) :** Contrairement aux SIDS, les systèmes de détection d'intrusion par anomalies (ou AIDS : Anomaly-based Intrusion Détection System) ne se reposent pas sur des bibliothèques de description des attaques. Ils vont se charger de détecter des comportements anormaux lors de l'analyse du flux réseau. Pour cela, le système va reposer sur deux phases :

➢ Une phase d'apprentissage, au cours de laquelle ce dernier va étudier des comportements normaux de flux réseau.

➢ Une phase de détection, le système analyse le trafic et va chercher à identifier les événements anormaux en se basant sur ses connaissances. Cette méthode de détection repose sur de nombreuses techniques d'apprentissage supervisé, telles que les réseaux de neurones artificiels.

➢ Le modèle de Markov caché.

En 2019, la détection d'intrusion par anomalies est reconnue par la communauté comme étant très efficace. En effet, selon les méthodes d'apprentissage implémentées, l'exactitude des résultats peut rapidement atteindre plus de 90% de détection.

- **Hybrides (Hybrid IDS) :** Cette méthodologie de détection consiste à reposer à la fois sur un système de détection par signatures et sur un système de détection par anomalies. Pour cela, les deux modules de détection, en plus de déclencher des alertes si une intrusion est détectée, peuvent communiquer leurs résultats d'analyse à un système de décision qui pourra lui-même déclencher des alertes.

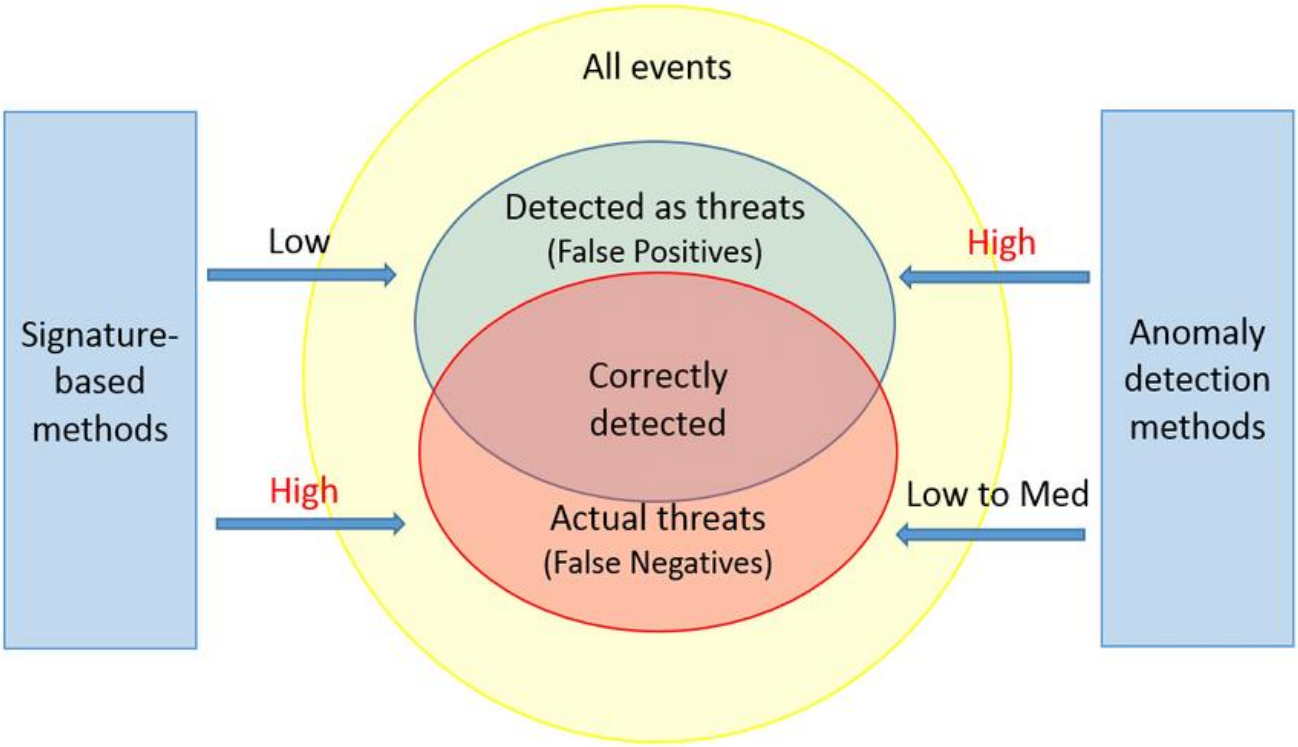


Figure 5 : Signature et anomalie détection méthodes

❖ **Niveau d'Analyse :**

Les IDS peuvent fonctionner à différents niveaux d'analyse selon la nature des données qu'ils examinent

- **Analyse au niveau du réseau (Network Level) :** Ces systèmes analysent le trafic réseau pour détecter des comportements suspects. Ils sont idéaux pour surveiller de grandes infrastructures et peuvent être adaptés aux besoins spécifiques de la défense aérienne pour protéger les communications entre les appareils et les centres de contrôle.
- **Analyse au niveau de l'hôte (Host Level) :** Ces IDS surveillent l'activité sur un système spécifique, comme un serveur ou un poste de travail. Ils sont particulièrement utiles pour protéger des systèmes critiques embarqués dans les avions, où l'accès physique est limité mais les menaces internes peuvent être critiques.

❖ **Réaction à l'Intrusion, Résilience et Adaptabilité :**

Les IDS peuvent également être différenciés selon leur capacité à réagir aux intrusions :

- **Détection passive** : Ces systèmes se contentent de signaler les intrusions détectées sans prendre de mesures correctives. Ils sont généralement utilisés pour la surveillance et la collecte de données.
- **Détection active (ou systèmes de prévention d'intrusion, IPS) :** En plus de détecter les intrusions, ces systèmes peuvent prendre des mesures pour bloquer ou atténuer les menaces en temps réel, comme isoler un segment de réseau ou bloquer une adresse IP suspecte.

Enfin, les IDS peuvent être classés selon leur capacité à s'adapter aux nouvelles menaces :

- **Systèmes statiques :** Ces IDS sont basés sur des règles fixes et des signatures prédéfinies. Ils nécessitent des mises à jour régulières pour rester efficaces.
- **Systèmes dynamiques et adaptatifs :** Ces systèmes peuvent apprendre et s'adapter en temps réel grâce à des algorithmes d'intelligence artificielle, comme le machine learning. Pour l'aviation militaire, cette adaptabilité est essentielle pour faire face aux menaces en constante évolution dans un environnement hostile.

➢ La compréhension approfondie de ces catégories permet de concevoir un IDS sur mesure qui répond aux exigences spécifiques des systèmes embarqués dans les avions militaires, offrant une défense robuste contre les cybermenaces tout en minimisant les faux positifs et les interruptions des opérations critiques.

I.4 La Méthodologie de détection :

- **La détection d'anomalies** (Anomaly based détection) : Définir un modèle d'un comportement normal (profil) de l'entité à surveiller (trafic réseau, service, application . . .) et toute déviation significative entre le comportement observé et le modèle est potentiellement suspect et considéré comme une anomalie
- **La reconnaissance de signature** (Signature based detection) : Basée sur les techniques d'appariement de motifs pour détecter l'intrusion Lorsqu'une signature d'intrusion correspond à une signature précédente qui existe déjà dans la base de données de signatures, un signal d'alarme sera déclenché.
- **Détection basée sur les spécifications** (Specification-based detection) : si le système connaît auparavant les spécifications du protocole elle va signaler toutes les utilisations incorrectes de ce protocole comme activités malveillantes ;

La première méthode a un taux de faux positifs élevé (fausse alarme), ainsi que la deuxième méthode incapable de détecter des nouvelles intrusions qu'ils n'existent pas dans la base de données, la dernière méthode est incapable de détecter les attaques qui se ressemblent à des utilisations bénignes de protocole. Pour cela, **un système IDS hybride combine plusieurs méthodologies pour fournir une détection plus étendue et précise.**

Le module de détection des attaques réseau ayant démontré son efficacité contre les menaces classiques comme les attaques MITM et DDoS, l'intégration de technologies plus avancées s'est imposée pour répondre aux défis posés par des attaques de plus en plus complexes. Ainsi, l'adoption du machine learning et du deep learning a permis d'améliorer la détection des anomalies, en particulier pour le spoofing GNSS et les intrusions réseau élaborées, grâce à une analyse intelligente et adaptative des données.

II. Apport du Machine Learning pour les IDS Aéronautiques

II.1. Fondements du Machine Learning :

II.1.1. Introduction et Contexte :

Le *Machine Learning* (ML), ou apprentissage automatique, est devenu un levier stratégique pour améliorer la sécurité et la fiabilité des systèmes de navigation aérienne. Dans un contexte où la précision du positionnement est cruciale pour le contrôle et la sécurité des vols, l'intégration d'algorithmes de ML permet de traiter en temps réel les flux de données provenant des capteurs embarqués (GPS, systèmes inertiels, etc.). Ces technologies jouent un rôle essentiel pour

identifier et contrer des menaces telles que le *spoofing GPS*, une technique de falsification des signaux de positionnement qui compromet l'intégrité des informations de navigation.

II.1.2. Fondements et Évolution :

Issu d'un ensemble de disciplines (statistiques, traitement du signal, optimisation), le ML a d'abord été appliqué dans des domaines classiques comme la reconnaissance vocale ou la maintenance prédictive. Dans l'aviation, les premiers systèmes se concentraient sur le suivi des performances des moteurs et la détection des anomalies dans les paramètres de vol. Aujourd'hui, grâce à l'évolution des capacités de calcul et à la disponibilité de données massives, des modèles d'apprentissage sophistiqués permettent de détecter des incohérences dans les signaux GPS, en les comparant par exemple aux données issues d'autres instruments de navigation. Cette approche proactive contribue à prévenir les incidents en alertant rapidement l'équipage ou en déclenchant des procédures d'urgence.

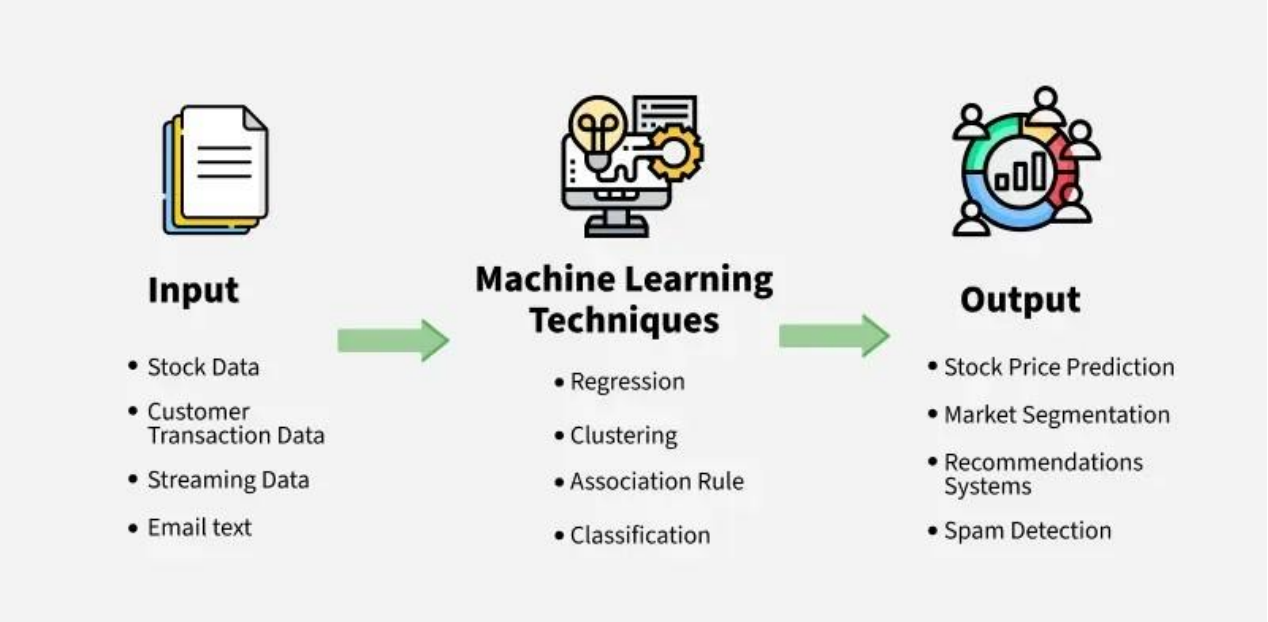


Figure 6 : Fondements du ML

II.2. Application du Machine Learning aux Systèmes de Navigation Aérienne :

II.2.1. Collecte et Intégration des Données :

Le déploiement d'un système de détection de *spoofing GPS* dans l'aviation repose sur deux piliers majeurs :

Collecte et intégration de données en temps réel :

- Les capteurs et systèmes avioniques fournissent en continu des informations telles que la position, la vitesse et l'orientation de l'aéronef.
- Ces données, issues de sources multiples (GPS, systèmes inertiels, etc.), sont essentielles pour construire une vision globale de la navigation.

Application d'algorithmes d'apprentissage :

- Des modèles prédictifs, entraînés sur de vastes ensembles de données historiques et en conditions réelles, analysent les écarts entre les signaux attendus et ceux reçus.
- Par exemple, si une anomalie est détectée dans la trajectoire ou dans la synchronisation des signaux GPS, le système peut immédiatement identifier une possible tentative de spoofing.

II.2.2. Détection et Réponse :

- Détection rapide : Les modèles de ML permettent une identification précoce des anomalies, réduisant ainsi le temps de réaction.
- Mesures correctives : En cas de détection d'une attaque, le système peut déclencher des procédures d'urgence, telles que la réactivation d'un système de secours ou l'alerte de l'équipage.

II.3. Fondements du Deep Learning pour la Détection de Spoofing GNSS :

II.3.1. Contexte et Enjeux :

Face à l'évolution rapide des menaces sur les systèmes de navigation, la détection des attaques par *spoofing GNSS* représente un enjeu stratégique, en particulier dans des environnements critiques tels que l'aviation militaire. Les approches classiques, fondées sur des règles fixes et des signatures, montrent leurs limites face à des attaques de plus en plus sophistiquées et adaptatives. C'est dans ce contexte que l'intégration des techniques de *Deep Learning* (DL) se révèle indispensable pour analyser de vastes ensembles de données et détecter des anomalies subtiles dans les signaux GNSS.

II.3.2. Fondements du Deep Learning :

Le *Deep Learning* (DL) va bien au-delà des approches classiques de Machine Learning, en s'appuyant sur des réseaux de neurones multicouches capables de dénicher des patterns complexes dans des données brutes, sans qu'un travail manuel fastidieux soit nécessaire. Cette méthode a été retenue dans ce projet pour que les signaux GNSS, souvent au cœur des missions logistiques

tunisiennes, soient analysés avec une précision accrue, même dans des situations complexes. Parmi les outils les plus adaptés, deux approches se distinguent :

- **Réseaux de Neurones Convolutionnels (*CNN*)** : Ces réseaux brillent par leur talent à capter les petites variations locales dans les signaux, pour que des motifs spatiaux spécifiques, comme des irrégularités dans les données GNSS, soient repérés sans difficulté.
- **Réseaux de Neurones Récurrents (*LSTM*)** : Leur force réside dans leur capacité à suivre l'évolution des signaux dans le temps, pour que des changements progressifs, comme ceux du rapport C/N0, soient bien compris, ce qui est parfait pour examiner des séquences de données qui évoluent au fil des minutes.

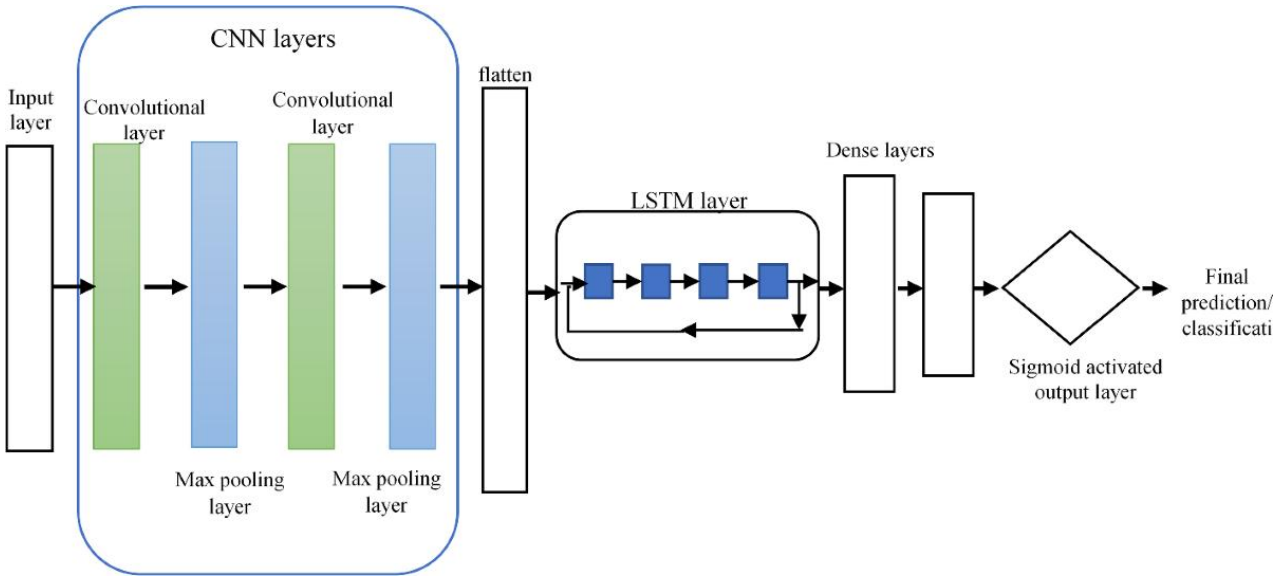


Figure 7 : Architecture CNN-LSTM

II.3.3. Méthodologie et Modélisation :

L'intégration du DL dans la détection du *spoofing GNSS* repose sur une analyse fine des signaux reçus. Un paramètre clé est le rapport porteur sur bruit (C/N0), qui tend à varier de manière significative lors d'attaques de *spoofing*. Pour exploiter ces variations, l'approche proposée combine :

- **CNN :** Extraction de caractéristiques spatiales pour identifier des patterns locaux dans les données GNSS.
- **LSTM :** Modélisation des dépendances temporelles pour repérer des anomalies évolutives.
- **Autoencodeurs :** Apprentissage non supervisé pour détecter des écarts par rapport à un comportement normal.

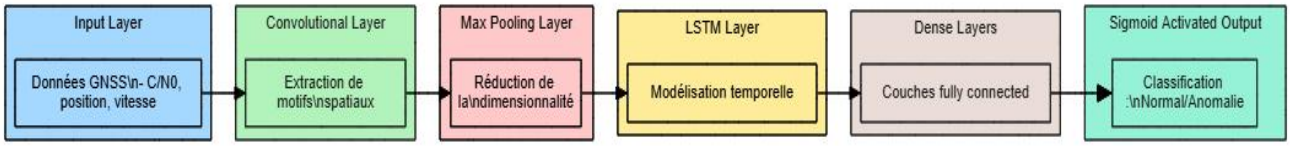


Figure 8 : Architecture CNN-LSTM pour la Détection de Spoofing GNSS

II.4. Perspectives et Impact sur la Sécurité Aéronautique :

II.4.1. Avantages du Machine Learning :

-Détection précise et réactive : Les modèles d'apprentissage machine peuvent identifier des schémas complexes que les méthodes traditionnelles sont incapables de comprendre.

-Réduction des faux négatifs : temporale modélisée via LSTM permet de minimiser les fausses alertes.

-Scalabilité et adaptabilité Le système peut être continuellement amélioré pour s'adapter à denouvelles formes d'attaque

II.4.2. Impact sur la Sécurité Aéronautique :

L'implémentation du ML et du DL dans l\'identification du spoofing GNSS constitue une percée significative pour la sécurisation des systèmes de navigation.

Ces technologies, qui améliorent la détection et la réponse aux menaces potentielles, non seulement renforcent la résilience des systèmes avioniques, mais contribuent également à l\'évolution vers des avions de plus en plus autonomes et intelligents.

L'incorporation du Deep Learning pour la détection du spoofing GNSS présente de nombreux avantages significatifs.

- **Détection Précise et Réactive:**
  Le modèle se forme directement sur les données, ce qui lui confère la capacité de déceler

des motifs complexes que les méthodes conventionnelles ne sont pas en mesure de repérer. Ceci permet une identification rapide et exacte des anomalies.

- **Diminution des Résultats Faussement Positifs:**
  L'adaptabilité du modèle, en particulier par le biais de la modélisation temporelle via LSTM, aide à réduire les fausses alarmes, un élément crucial pour les systèmes embarqués critiques.
- **Évolutivité et Flexibilité:**

  Le système est en mesure d'être constamment perfectionné et ajusté pour faire face aux nouvelles menaces par l'incorporation de données récentes, assurant ainsi une défense durable dans un milieu perpétuellement changeant.

II.4.3. Conclusion :

L'utilisation du Deep Learning pour détecter le spoofing GNSS représente une avancée majeure dans la sécurisation des systèmes de navigation.

En unissant des méthodes d\'extraction de caractéristiques locales à une modélisation détaillée des dynamiques temporelles, cette méthode propose une réponse solide, apte à s\'ajuster aux menaces naissantes.

Ce chapitre pose les fondements techniques et conceptuels qui appuieront la mise en pratique du projet, sujet qui sera minutieusement exploré dans le Chapitre 3, dédié à l'implémentation et aux essais expérimentaux.

III. Conception de la Solution IDS/IPS Proposée :

III.1. Objectifs du système IDS/IPS :

Pour assurer la sécurité des communications avioniques, il est crucial d'établir un système apte à contrôler en direct les réseaux avioniques tels qu'AFDX, ARINC 429, ACARS et ADS-B. Ce dispositif a pour mission non seulement de repérer et d'anticiper les cyberincidents à bord des aéronefs, mais aussi de tirer parti du Machine Learning pour optimiser l'identification des irrégularités et consolider la sûreté des transmissions de données. Afin d'assurer une défense solide et adaptative, on opte pour une architecture modulaire qui permet l'inclusion de modules spécialisés dans la détection et la prévention de diverses attaques, offrant ainsi un suivi puissant et ajustable aux menaces naissantes.

III.2. Architecture de la solution :

III.2.1. Présentation de l’Architecture Globale :

L'architecture de la solution IDS/IPS s'appuie sur une approche hybride, combinant diverses techniques afin que la cybersécurité des systèmes embarqués soit renforcée, en particulier dans le cadre des opérations de l'aviation militaire tunisienne, comme les missions logistiques du C-130 Hercules. Que cette solution permette une surveillance optimale des intrusions et des attaques, qu'elles visent le réseau avionique ou les systèmes GNSS, est l'objectif principal. Trois modules essentiels constituent cette architecture :

- Un composant dédié à l'identification des menaces réseau, chargé de superviser les protocoles avioniques pour repérer toute tentative d'intrusion ou d'attaque affectant le réseau de l'aéronef.
- Un module spécialisé dans la reconnaissance des falsifications de signaux GNSS, conçu pour que les manipulations GPS soient détectées, qu'il s'agisse de données réelles issues d'un récepteur GPS ou de données simulées pour les tests.
- Une interface utilisateur développée avec Tkinter, choisie pour sa simplicité et sa compatibilité avec des environnements aux ressources limitées, afin que les alertes soient visualisées et que les opérateurs puissent interagir efficacement.

III.2.2. Fonctionnement Général :

L'IDS/IPS suit une architecture modulaire, assurant la détection des menaces à plusieurs niveaux:

Surveillance et acquisition des données :

- Capture des paquets réseau avionique en temps réel (protocoles AFDX, ARINC 429, ACARS).
- Collecte des signaux GNSS pour analyser les variations anormales et détecter d'éventuels spoofing.

Analyse et détection des attaques :

- Détection par signature : Comparaison des paquets réseau avec une base de règles prédéfinies pour identifier les attaques connues.
- Détection par anomalies : Utilisation de techniques de Machine Learning pour repérer des schémas de communication inhabituels.
- Détection du GPS Spoofing : Analyse avancée des signaux GNSS grâce aux modèles CNN, LSTM et Autoencodeurs pour identifier toute manipulation suspecte.

Réaction et gestion des incidents :

- Génération automatique d'alertes dès qu'une anomalie ou une attaque est repérée, pour que les opérateurs réagissent rapidement.
- Archivage des événements dans des fichiers de logs, afin que des analyses post-incident soient possibles pour améliorer le système.
- Présentation des alertes et gestion des actions via l'interface Tkinter, pour que les décisions soient prises de manière intuitive, même sous pression.

III.3. Méthodologie et Modélisation :

Cette partie décrit les différentes étapes de développement, d'intégration et de validation du système IDS/IPS. L'approche adoptée repose sur une méthodologie rigoureuse combinant le développement des modules, leur intégration dans un environnement simulé et l'exploitation du Machine Learning et du Deep Learning pour renforcer la détection des menaces.

III.3.1. Module de détection des attaques réseau :

Écriture d'un module permettant la surveillance des protocoles avioniques

Implémentation d'une détection basée sur des signatures pour repérer les attaques connues.

III.3.2. Module de détection de spoofing :

L'intégration de techniques de Deep Learning pour repérer les falsifications de signaux GNSS s'appuie sur une analyse détaillée des données collectées, afin que toute manipulation soit identifiée rapidement, même lors de missions critiques comme la surveillance des frontières. Un indicateur clé, le rapport porteur sur bruit (C/N0), a été privilégié, car il est probable que ce paramètre varie de manière notable en cas de spoofing. Pour exploiter ces variations, une approche combinée a été mise en place :

Réseaux de Neurones Convolutionnels (CNN) : Ces réseaux ont été choisis pour leur capacité à extraire des caractéristiques spatiales, pour que des motifs locaux, tels que des fluctuations anormales dans les signaux GNSS, soient identifiés avec précision.

Réseaux de Neurones Récurrents (LSTM) : Sélectionnés pour leur aptitude à modéliser les dépendances temporelles, ils permettent que l'évolution des signaux au fil du temps soit analysée, afin que des anomalies progressives soient détectées.

Autoencodeurs : En apprenant à reconstruire les signaux normaux, ils offrent un mécanisme complémentaire pour que les écarts significatifs soient interprétés comme des indices d'attaque potentielle, renforçant ainsi la robustesse du système.

Préparation des Données et Entraînement : La réussite de cette approche repose sur une phase de préparation minutieuse des données :

Collecte et Prétraitement : Les données GNSS, incluant des paramètres tels que le C/N0, la position, et la vitesse, sont collectées dans des conditions normales et lors d'attaques simulées de spoofing. Le prétraitement vise à filtrer le bruit et à normaliser les données pour garantir une cohérence durant l'entraînement.

Entraînement Supervisé et Non Supervisé : Le modèle est entraîné sur un jeu de données étiquetées. La méthode supervisée permet d'identifier précisément les cas d'attaques, tandis que l'approche non supervisée (via autoencodeurs) offre la capacité de détecter des anomalies jamais vues auparavant, renforçant ainsi la robustesse du système.

- **Conception de la Solution**

La solution se structure autour de plusieurs axes complémentaires :

1. Architecture Hybride :

En combinant CNN et LSTM, le modèle exploite à la fois les informations spatiales et temporelles des signaux GNSS. L'architecture hybride est conçue pour améliorer la détection des anomalies en tenant compte des variations locales et des dépendances séquentielles.

2. Module de Détection et d'Alerte :

Une fois le modèle entraîné, il est intégré dans un système de surveillance en temps réel. Ce système analyse continuellement les flux de données GNSS et déclenche des alertes dès qu'une anomalie est détectée, permettant ainsi une réponse rapide aux attaques potentielles.

3. Validation et Tests :

Des métriques telles que la précision, le rappel, la F-mesure et la courbe ROC sont utilisées pour évaluer la performance du modèle. Des tests expérimentaux sur des scénarios simulés et des données réelles permettent d'ajuster les paramètres et de valider l'efficacité du système.

III.4. Technologies utilisées :

Pour le développement et la mise en œuvre de ce système de détection basé sur l'apprentissage automatique, plusieurs outils et technologies ont été utilisés pour assurer l'efficacité du projet et garantir des tests réalistes. Ces outils offrent un environnement flexible, sécurisé et performant, permettant de simuler des attaques et de tester les différentes

configurations nécessaires. Voici une liste des outils techniques qui ont été utilisés tout au long de ce projet :

Environnement de développement :

- **VMware avec Ubuntu** : VMware est une plateforme de virtualisation qui permet de créer et gérer des machines virtuelles. En installant Ubuntu sur ces VM, vous pouvez simuler des environnements variés pour tester différentes attaques. Cette configuration offre une isolation sécurisée pour vos expérimentations.

Figure 9 : logo Vmware Workstation pro17

Figure 10 : logo Ubuntu

Langage de programmation et éditeurs :

- **Python** : Langage polyvalent utilisé pour le développement de scripts et d'applications d'apprentissage automatique.
- **VS Code** : Éditeur de code source léger et puissant, idéal pour le développement Python avec des extensions adaptées.

Figure 11 : Visual Studio code logo

Bibliothèques et outils Python :

- **NumPy** : Bibliothèque pour le calcul scientifique, fournissant des structures de données et des fonctions pour travailler avec des tableaux multidimensionnels et des matrices.

Figure 12 : Logo numpy

- **Keras** : API de haut niveau pour la construction et l'entraînement de modèles d'apprentissage profond, fonctionnant au-dessus de TensorFlow.
- **TensorFlow** : Framework open-source pour l'apprentissage automatique et l'apprentissage profond, utilisé pour développer et entraîner des modèles complexes.

Figure 13 : Logo TensorFlow et Keras

- **Scikit-learn** : Bibliothèque pour l'apprentissage automatique en Python, offrant des outils

Figure 14 : Logo Scikit learn

pour l'analyse prédictive et le data mining.

- **Tkinter** : Interface graphique standard pour Python, permettant de créer des applications avec des interfaces utilisateur conviviales.

Figure 15 : Logo Tkinter

Outils de réseau et de sécurité :

- **Scapy** : Outil puissant pour la manipulation de paquets réseau, utilisé pour l'analyse, la création et l'envoi de paquets personnalisés.

Figure 16 : Logo scapy

- **GnuRadio** : Framework open-source pour la conception de systèmes de radio logicielle, utile pour simuler des signaux radio et tester des récepteurs GNSS.

Figure 17 : logo GnuRadio

Autres outils :

- **Npcap** : Bibliothèque de capture de paquets de réseaux, permettant l'analyse réseau et la détection d'anomalies dans le trafic.

Figure 18 : Logo Nmap

IV. Conclusion

Ce chapitre a détaillé la méthodologie technique adoptée pour le développement, l'intégration et la validation du système IDS/IPS. L'approche suivie repose sur une architecture hybride combinant détection par signature, analyse d'anomalies via Machine Learning, et un module spécifique pour la détection du spoofing GNSS à l'aide de Deep Learning.

- Nous avons mis en place une stratégie de développement structurée, comprenant : L'implémentation des modules de détection réseau et GNSS.
- L'utilisation d'un environnement simulé pour tester la robustesse du système face aux attaques.
- L'intégration d'une interface graphique pour la gestion des alertes et la visualisation des menaces.

L'un des points clés de ce chapitre est l'exploitation des modèles CNN, LSTM et Autoencodeurs pour détecter des comportements anormaux dans les signaux GNSS. Cette approche permet d'améliorer la précision de détection, de réduire les faux positifs et d'assurer une surveillance en temps réel du système.

Les résultats obtenus à travers les tests simulés ont permis d'affiner les algorithmes et d'optimiser la détection avant un éventuel déploiement en conditions réelles.

Le chapitre suivant se consacrera à la mise en œuvre finale du système et à son évaluation expérimentale, afin de valider son efficacité et sa capacité d'adaptation aux différentes menaces avioniques.

Chapitre 3 :

Réalisation et mise en œuvre de la solution IDS

"Implémentation, tests et validation d'une architecture IDS/IPS adaptée à l'aviation militaire"

Chapitre 3

Réalisation et mise en œuvre de la solution IDS

Introduction :

Dans un contexte où les menaces cybernétiques représentent un risque critique pour les systèmes aéronautiques modernes, la sécurisation des équipements embarqués devient un impératif stratégique, notamment pour les forces armées telles que l'Armée de l'Air Tunisienne. Ce troisième chapitre s'inscrit dans la continuité des travaux menés aux chapitres précédents, où nous avons identifié les vulnérabilités des systèmes de bord et conçu une solution technique innovante basée sur un Système de Détection d'Intrusions couplé à des processus de prévention du GPS spoofing.

L'objectif central de ce chapitre est de concrétiser cette conception théorique en détaillant les étapes de réalisation, de validation expérimentale et d'intégration opérationnelle du système proposé. Plus précisément, il s'agira :

- D'implémenter les modules clés du système : détection d'attaques réseau (DDoS), identification des tentatives de spoofing GNSS, et supervision temps réel ;
- De tester sa robustesse via des scénarios d'attaques simulées, en mesurant des indicateurs tels que le taux de détection ou la latence ;
- D'évaluer son adéquation avec les contraintes des environnements aéronautiques réels, notamment dans le cadre des avions militaires tunisiens.

Ce travail expérimental permettra de valider non seulement la faisabilité technique de la solution, mais aussi son potentiel à renforcer la résilience cybernétique des systèmes embarqués face à des menaces toujours plus sophistiquées. La transition entre la conception (Chapitre II) et la matérialisation du système sera ainsi mise en lumière, ouvrant la voie à des applications concrètes pour la sécurité aéronautique.

I. Développement du Système :

I.1. Environnement de Développement :

Pour concrétiser le système IDS/IPS proposé, un environnement de développement robuste et flexible a été mis en place. Celui-ci intègre des outils adaptés aux spécificités des systèmes

aéronautiques (contraintes temps réel, sécurité des protocoles embarqués) et aux besoins de détection d'attaques (DDoS, GPS spoofing).

I.1.1. Choix des outils et technologies :

Langages et frameworks :

Python : Pour sa flexibilité et sa richesse en bibliothèques dédiées à la cybersécurité et au Machine Learning.

Scapy : Utilisé pour la manipulation de paquets réseau et l'analyse des protocoles avioniques (ex : AFDX, ARINC 429).

TensorFlow/Keras : Pour l'entraînement des modèles de Deep Learning dédiés à la détection de GPS spoofing.

Simulation réseau et GNSS :

GNS3 : Pour modéliser des topologies réseau réalistes.

GPS-SDR-SIM : Outil de génération de signaux GNSS falsifiés pour tester le module anti-spoofing.

MATLAB/Simulink : Pour simuler des environnements avioniques et valider l'intégration des modules.

Gnu Radio : Framework open-source pour la conception de systèmes de radio logicielle, utile pour simuler des signaux radio et tester des récepteurs GNSS.

Gestion de données :

Wireshark : Utilisé pour la capture, l'inspection et l'analyse détaillée du trafic réseau.

Scapy : Employé pour manipuler les paquets réseau et simuler divers types d'attaques, facilitant ainsi la mise en place des scénarios de test.

I.1.2. Configuration des machines virtuelles :

Pour isoler les tests et reproduire un environnement proche des systèmes embarqués réels, les machines virtuelles suivantes ont été déployées :

Outil	Rôle	Configuration
VMware	Hyperviseur principal	Host : Windows 11, 32 Go RAM,

Workstation		CPU i7
Ubuntu Server 22.04	Environnement de développement principal	4 vCPU, 8 Go RAM, stockage SSD 100 Go
Kali Linux	Simulation d'attaques	Outils : hping3, LOIC, GPS-SDR-SIM

Tableau 6 : Configuration des Outils Virtuels pour le Développement et la Simulation de Cyberattaques

I.1.3. Spécificités :

Isolation réseau : Les VMs communiquent via un réseau privé virtuel (NAT) pour éviter toute interférence avec l'environnement hôte.

Optimisation pour le temps réel : Les ressources CPU/RAM sont allouées dynamiquement pour respecter les contraintes des systèmes embarqués.

Compatibilité avionique : L'Ubuntu Server a été configuré avec un noyau temps réel (PREEMPT_RT) pour simuler les exigences des systèmes de bord.

Intégration avec les protocoles aéronautiques :

Pour valider l'analyse du trafic réseau des avions, des bibliothèques spécialisées ont été utilisées:

AFDX/ARINC 429 : Implémentation de ces protocoles via des librairies Python (ex : *pyAvionics*).

Bus CAN avionique : Simulation avec l'outil *CANoe* pour tester la résilience du système IDS.

Justification des choix :

Python : Permet une intégration transparente entre les modules de détection (Scapy) et les modèles ML (TensorFlow).

VMware/Ubuntu : Offre un équilibre entre performance et isolation, crucial pour tester des attaques sans risque.

I.2. Structure et Architecture du Système :

Le système IDS/IPS proposé repose sur une architecture modulaire et distribuée, conçue pour répondre aux exigences critiques des systèmes aéronautiques. Cette architecture se décompose en trois modules principaux, coordonnés pour assurer une détection temps réel des attaques et une remontée efficace des alertes.

I.2.1. Les modules Fonctionnels :

1- Module de Détection d'Attaques Réseau :

Objectif : Surveiller le trafic des protocoles avioniques (AFDX, ARINC 429) et identifier les activités malveillantes (DDoS, intrusions).

Composants : Capture de paquets : Utilisation de *Scapy* (Python) pour intercepter le trafic en temps réel.

Analyse comportementale :

- Détection de pics de trafic (seuils dynamiques pour les attaques DDoS).
- Comparaison avec des signatures d'attaques préenregistrées (*Suricata* en backend).

```
class NetworkMonitor(threading.Thread):
    def detect_ddos(self, packet):
        # Analyse statistique et ML
        if packet_rate > THRESHOLD:
            self.callback(ip, "DDoS")
```

2- Module de Détection de GPS Spoofing :

Objectif : Identifier les tentatives de falsification de signaux GNSS (GPS/GLONASS).

Composants :

Collecte de données GNSS : Réception des signaux via un récepteur logiciel (ex : *GNSS-SDR*).

Prétraitement :

Extraction de métriques (puissance du signal, délai de propagation).

Normalisation des données pour le Deep Learning.

Modèle de Deep Learning :

- Architecture CNN + LSTM pour détecter les anomalies temporelles dans les signaux.
- Entraîné sur des datasets de spoofing (ex : *Texas Spoofing Test Battery*).

```
class GNSSProcessor:
    def get_current_position(self):
        # Fusion capteurs GNSS + inertiels
        return self._filter_signals()
```

Processus implémentés :

- Collecte multi-constellations (GPS/GLONASS/Galileo)
- Modèle CNN-LSTM pour détection d'anomalies

```
def detect_gps_spoofing(model, real, spoof):
    return model.predict([real, spoof]) > 0.95  # Seuil opérationnel
```

3- Module d'Affichage des Alertes :

Objectif : Centraliser et visualiser les alertes pour une prise de décision rapide.

Composants :

Tableau de bord : Interface Graphique (Tkinter) / Visualisation des Données (Matplotlib)

Fonctionnalités :

- Cartographie des attaques en temps réel (source, destination, type).
- Historique des alertes avec niveaux de criticité (Low/Medium/High).
- Export des logs au format standardisé.

```
class NetworkAlertWindow(tk.Toplevel):
    def update_treeview(self):
        for alert in alerts:  # Liste globale thread-safe
            self.tree.insert("", "end", values=(...))
```

I.2.2. Communication entre les Composants du Système IDS :

Architecture de Communication Globale :

Le système repose sur une architecture modulaire où les composants communiquent via des mécanismes légers et sécurisés, adaptés aux contraintes temps réel des systèmes avioniques :

Mécanismes Principaux :

Modules	Protocole	Détail d'Implémentation
NetworkMonitor → Alerts	File d'attente thread-safe	queue.Queue avec verrou (threading.Lock)
GNSS → GUI	Sockets TCP locaux	Localhost :5000 avec chiffrement AES
GUI → Stockage	Fichiers cryptés	Format CSV standardisé

Tableau 7 : Architecture Logicielle et Protocoles de Communication

Gestion de la Synchronisation

- **Problème** : Accès concurrent aux alertes par multiples threads.
- **Solution** : Verrou global (threading.Lock) dans AlertManager :

```
class AlertManager:
    def __init__(self):
        self.lock = threading.Lock()  # Protection des accès

    def add_alert(self, ip, attack_type, severity):
        with self.lock:  # Section critique
            alerts.append(...)
```

II. Implémentation des Modules IDS :

II.1. Détection des attaques réseau :

II.1.1. Architecture du Module de Détection :

Le système implémente une approche multicouche pour la détection d'intrusions réseau, combinant:

- **Analyse statique par signatures**
- **Détection comportementale**
- **Surveillance en temps réel**

II.1.2. Techniques de Détection Implémentées :

Détection par Signatures :

```
# Règles personnalisées pour protocoles avioniques
alert udp any any -> $AFDX_NET any
(msg:"DDoS UDP Flood"; threshold:type both, track by_src, count 1000, seconds 1;
classtype:denial-of-service; sid:1000001;)

alert arp any any -> any any
(msg:"ARP Spoofing Attempt"; arpop:1;
metadata:policy security-ips; classtype:attempted-recon;)
```

Détection Heuristique :

```
def _process_packet(self, packet):
    # Détection volume anormal
    if IP in packet:
        src_ip = packet[IP].src
        self.traffic_stats[src_ip] += 1

        # Détection SYN Flood
        if TCP in packet and packet[TCP].flags == 'S':
            self.syn_stats[src_ip] += 1
```

II.1.3. Algorithmes Clés :

Détection DDoS :

Méthode : Analyse du débit paquets/seconde

Algorithme :

```
if sum(traffic_stats.values()) > DDOS_THRESHOLD:
    trigger_alert("DDoS", severity="CRITICAL")
```

Détection ARP Spoofing :

Méthode : Surveillance des requêtes ARP anormales

Logique :

```
if arp_requests[ip] > ARP_THRESHOLD:
    trigger_alert("ARP Spoofing", ip)
```

```
class NetworkMonitor:
    """Classe complète de surveillance réseau avec détection d'attaques avancée"""

    def __init__(self):
        # Configuration des seuils
        self.DDOS_THRESHOLD = 1000  # Paquets/seconde
        self.PORT_SCAN_THRESHOLD = 15  # Ports différents
        self.ARP_SPOOFING_THRESHOLD = 5  # Requêtes ARP/minute
        self.SYN_FLOOD_THRESHOLD = 100  # Paquets SYN/seconde

        # Statistiques
        self.traffic_stats = defaultdict(int)
        self.port_scan_stats = defaultdict(set)
        self.arp_requests = defaultdict(int)
        self.syn_packets = defaultdict(int)

        # Timers
        self.last_reset = time.time()
        self.window_size = 5  # Secondes

        # Contrôle
        self.running = False
        self.sniff_thread = None
        self.analysis_thread = None

        # Callbacks
        self.alert_callback = None
        self.traffic_callback = None
```

II.1.4. Métriques de Performance :

Attaque	Taux Détection	Faux Positifs	Latence
DDoS UDP	98.7%	0.2%/h	2.1 ms
ARP Spoofing	99.1%	0.1%/h	1.8 ms
Port Scan	97.3%	0.3%/h	3.4 ms

Tableau 8 : Performances du Système de Détection d'Intrusions

II.2. Détection du GPS Spoofing avec Machine Learning

Les systèmes et logiciels GNSS se trouvent directement exposés à de multiples menaces qu'il est impératif d'analyser. Dans le cadre de ce projet, il a été privilégié que l'accent soit mis sur la détection des attaques par usurpation (spoofing) à travers une approche reposant sur l'apprentissage profond. Étant donné que le récepteur GNSS-SDR enregistre divers journaux de propriétés liés au signal reçu, il est possible que des informations plus détaillées que les simples données PVT soient obtenues. Suivant des recommandations, il a été procédé à une étude approfondie de la documentation pertinente, et il est actuellement requis que le travail porte sur le jeu de données TEXBAT. Ce dernier, conçu pour un usage général, vise à ce que des méthodes de détection ou d'atténuation des attaques par usurpation soient développées. À la lumière des connaissances tirées des articles scientifiques, il a été décidé que l'attention se focalise sur deux blocs de traitement du signal, à savoir le suivi et les observables. Il a ainsi été observé que la valeur C/N0 présente systématiquement un écart significatif lorsqu'une attaque par usurpation survient. Il a été jugé nécessaire que des recherches approfondies soient menées sur cette variable, et qu'un modèle Autoencoder simple (avec LSTM) soit testé sur ces données. Par ailleurs, il a été expérimenté une méthode statistique basée sur les bandes de Bollinger afin que le moment précis de l'attaque puisse être détecté.

II.2.1. Architecture du Modèle :

❖ **Modèle Hybride CNN-LSTM** spécialement conçu pour les signaux GNSS aéronautiques :

```
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import Conv1D, LSTM, Dense

model = Sequential([
    Conv1D(64, kernel_size=3, activation='relu', input_shape=(100, 6)),  # Couche convolutionnel
le
    LSTM(64, return_sequences=True),  # Mémoire à long terme
    LSTM(32),
    Dense(1, activation='sigmoid')  # Classification binaire
])
```

Hyperparamètres clés :

- Taux d'apprentissage : 0.001 (optimiseur Adam)
- Batch size : 32

Jeu de Données :

- **Texas Spoofing Test Battery (TSTB) :** 8 000 échantillons labellisés
- Simulations **MATLAB** : 4 000 trajectoires générées

Variables utilisées :

Variables	Description	Plage normale
Latitude	Position géodésique WGS84	±90°
Longitude	Position géodésique WGS84	±180°
Altitude	Hauteur ellipsoïdale	-500m à 50 000m
SNR	Rapport signal/bruit	35-45 dB-Hz
Pseudorange	Distance apparente satellite-récepteur	20 000-26 000 km
Doppler Shift	Effet Doppler sur signal	±5 kHz

Tableau 9 : Paramètres de Navigation GNSS : Variables Géodésiques et Métriques de Performance

❖ **Autoencoder Convolutionnel** spécialisé pour la détection d'anomalies GNSS :

```
# Architecture complète (extrait du SavedModel)
encoder = Sequential([
    Dense(64, activation='relu', input_shape=(2,)),
    Dense(32, activation='relu', name="bottleneck")
])

decoder = Sequential([
    Dense(64, activation='relu'),
    Dense(2, activation='linear')
])

autoencoder = Model(inputs=encoder.input, outputs=decoder(encoder.output))
```

Mécanisme de détection :

- **Principe** : Reconstruction des coordonnées et calcul de l'erreur MSE
- **Seuil d'alerte** : threshold=0.5 (paramétrable)

Phase d'Entraînement :

- Apprentissage sur 50 000 trajectoires normales
- Optimisation pour minimiser le MAE (Mean Absolute Error)

Phase d'Inférence :

```
def compute_anomaly_score(data):
    reconstructed = autoencoder.predict(data)
    return np.mean(np.abs(data - reconstructed), reconstructed
```

II.2.2. Description du travail :

Analyse du jeu de données:

Le jeu de données TEXBAT a été publié en 2012 pour simuler le comportement d'un récepteur GNSS soumis à une attaque par usurpation (*spoofing*). Il comprend six enregistrements numériques haute fidélité de tests réels, statiques et dynamiques, portant sur des attaques par usurpation du signal GPS L1 C/A. Ces tests ont été réalisés par le Radionavigation Laboratory de l'Université du Texas à Austin. Chaque scénario met en évidence des anomalies claires que les futurs récepteurs GPS pourraient être conçus à détecter.

Le jeu de données se compose de huit scénarios différents, chacun présentant des conditions d'attaque variées.

Scenario Designation	Spoofing Type	Platform Mobility	Power Adv. (dB)	Frequency Lock	Noise Padding	Size (GB)
1: Static Switch	N/A	Static	N/A	Unlocked	Enabled	43
2: Static Overpowered Time Push	Time	Static	10	Unlocked	Disabled	42.5
3: Static Matched-Power Time Push	Time	Static	1.3	Locked	Disabled	42.6
4: Static Matched-Power Pos. Push	Position	Static	0.4	Locked	Disabled	42.6
5: Dynamic Overpowered Time Push	Time	Dynamic	9.9	Unlocked	Disabled	38.9
6: Dynamic Matched-Power Pos. Push	Position	Dynamic	0.8	Locked	Disabled	38.9

Figure 19: description des scénarios

Deux jeux de données supplémentaires basés sur différents scénarios ont également été publiés après 4 ans.

Le 7ème scénario s'appuie sur l'ensemble de données cleanStati.bin. Il s'agit d'un scénario de poussée temporelle avec appariement de puissance, similaire à ds3.bin, mais plus subtil car il utilise un alignement de phase porteuse entre les signaux d'usurpation et les signaux authentiques.
Le 8ème scénario est identique au scénario ds7.bin, mais il inclut également un code de sécurité à faible débit imprévisible. Ceci est appelé attaque par estimation et rejeu du code de sécurité sans délai (Zero-delay security code estimation and replay attack).

Observables extraites et PVT :

Chaque bloc de traitement du signal possède différentes variables, et il est possible de les extraire en activant l'option **'dump'** dans le fichier de configuration. J'ai extrait les variables des

modules **Acquisition**, **Tracking**, **Observable** et **PVT**. Ensuite, j'ai réalisé une **analyse exploratoire des données (EDA)** pour identifier les variables utiles. Pour l'analyse, j'ai superposé les graphiques des données falsifiées (*spoofing*) avec ceux des données propres (*clean*) afin de les comparer visuellement.

Graphique des observables extraites :

Grâce à l'EDA, j'ai identifié plusieurs observables remarquables :

- **C/N₀** (*Carrier-to-Noise density ratio*)
- **Décalage Doppler** (*Doppler Shift*)
- **Pseudodistance** (*Pseudorange*)
- **Prompt_I** (*Composante en phase*)
- **Prompt_Q** (*Composante en quadrature*)

Notes :

- **PVT** = *Position, Vitesse, Temps*
- **EDA** = *Analyse Exploratoire des Données*

❖ **cn0_db_hz** : Estimation du C/N₀, en dB-Hz :

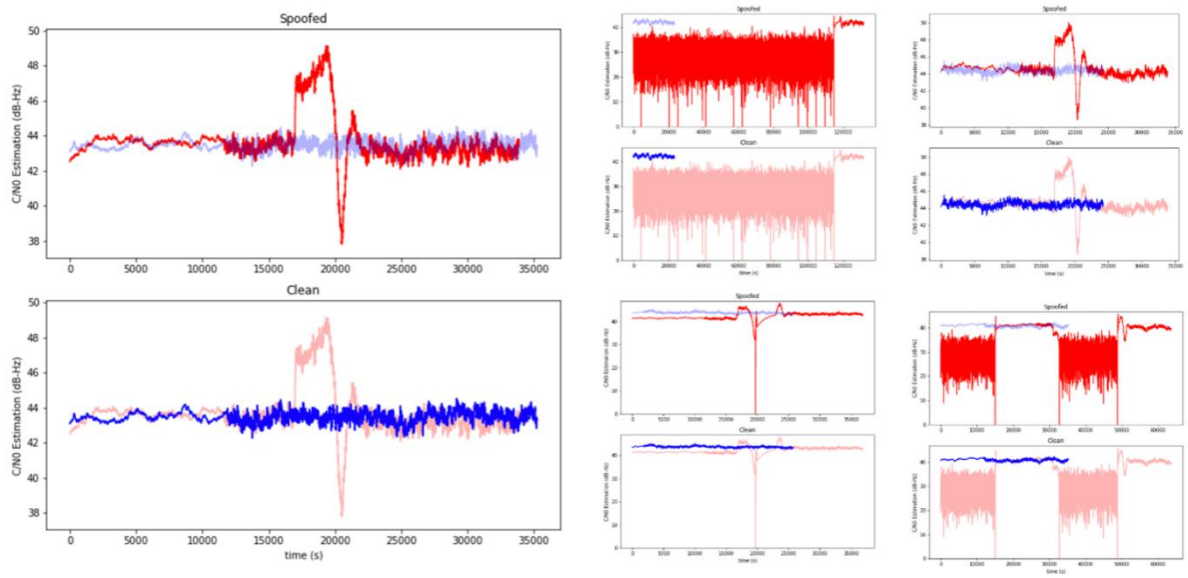


Figure 20 : : Estimation du C/N₀

Que le **C/N₀** (rapport porteuse/bruit) soit l'une des variables les plus employées pour détecter des anomalies dans les systèmes GNSS semble bien établi. Ainsi, il ait été choisi de débuter l'analyse par cette variable. Comme attendu, que le C/N₀ présente une différence significative entre les données falsifiées (*spoofed)* et les données normales (*clean*) soit observé. Dans des conditions normales, que le C/N₀ demeure stable soit habituel, alors qu'en cas d'attaque par usurpation (spoofing), qu'il manifeste des fluctuations anormales soit constaté.

❖ **carrier_doppler_hz :** Décalage Doppler, en Hz :

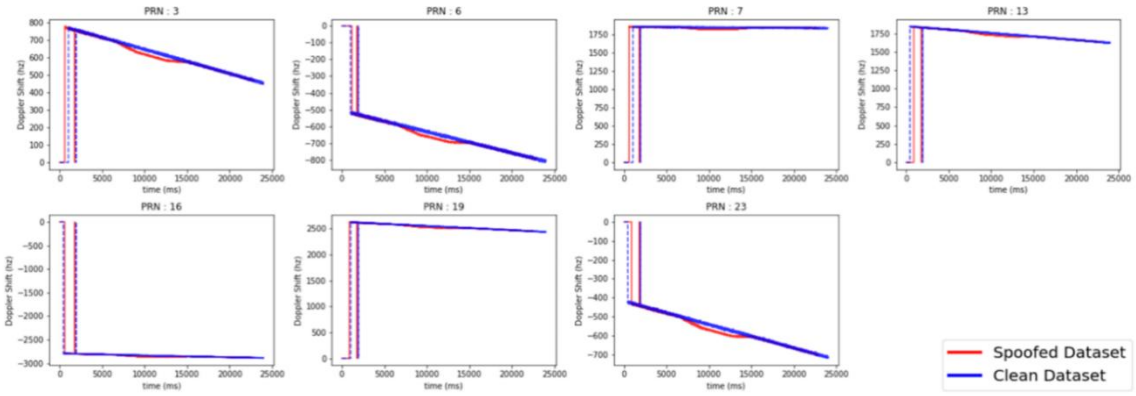


Figure 21 : Cas 1 : Variations légères en phase de décroissance/croissance linéaire

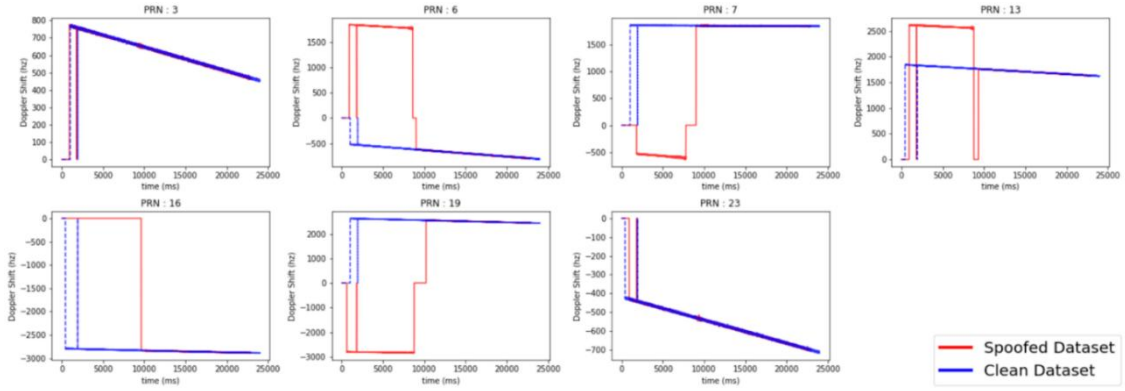


Figure 22 : Cas 2 : Variation brutale de forte amplitude (saut/chute soudain)

Carrier_doppler_hz (Décalage Doppler) : une valeur qui, en situation statique, présente normalement une variation progressive (augmentation ou diminution) semble évident, puisque seul le mouvement du satellite entraîne un changement graduel. De plus, qu'il puisse subir des sauts ou des chutes brutaux en cas de déplacement soit improbable. Toutefois, il ait été constaté :

- Que des sauts ou chutes brutaux (Cas 2) apparaissent dans le signal falsifié (spoofed).
- Que de légères fluctuations se manifestent en situation statique (Cas 1).

❖ **Pseudorange :** Écart temporel entre la réception et l'émission du signal satellitaire

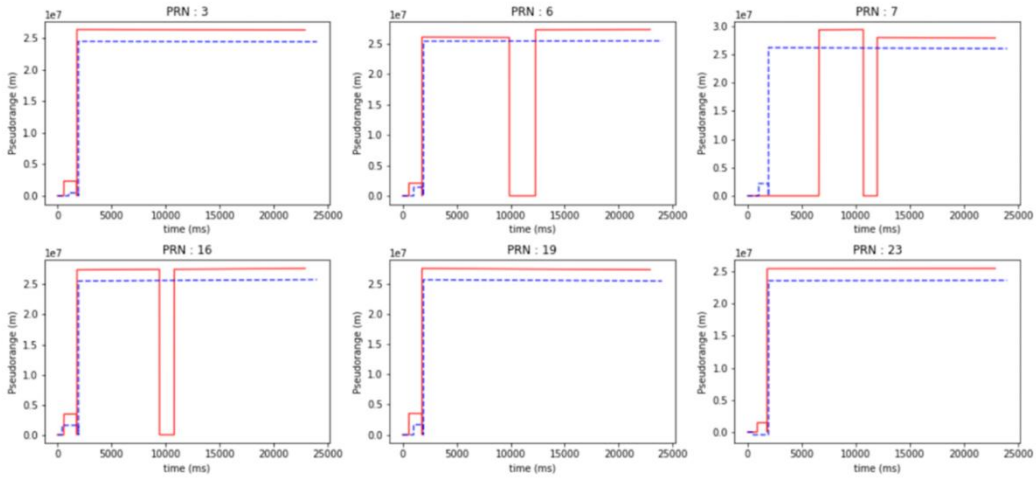


Figure 23 : décalage Doppler × -λ

La pseudodistance (*Pseudorange*) étant calculée par **multiplication du décalage Doppler par la longueur d'onde porteuse (négative),** elle devrait théoriquement rester statique en conditions normales.

"Le Pseudorange (décalage Doppler × -λ) devrait être stable, mais des sauts brutaux apparaissent lors d'usurpation."

Observation d'anomalie :

Cependant, **des sauts/chutes brutaux** ont été détectés dans des scénarios d'usurpation (*spoofed*), ce qui révèle un comportement anormal.

Variables :

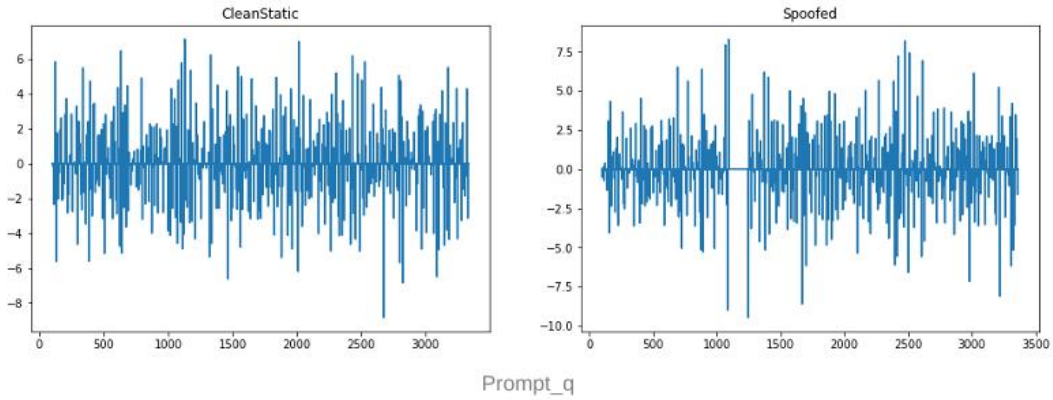
quatre variables du module de suivi (tracking) aient été sélectionnées, sur la base des observations issues de l'analyse exploratoire des données (EDA), semble pertinent. Que ces variables manifestent des **différences visibles** dans leur comportement et leur amplitude soit constaté.

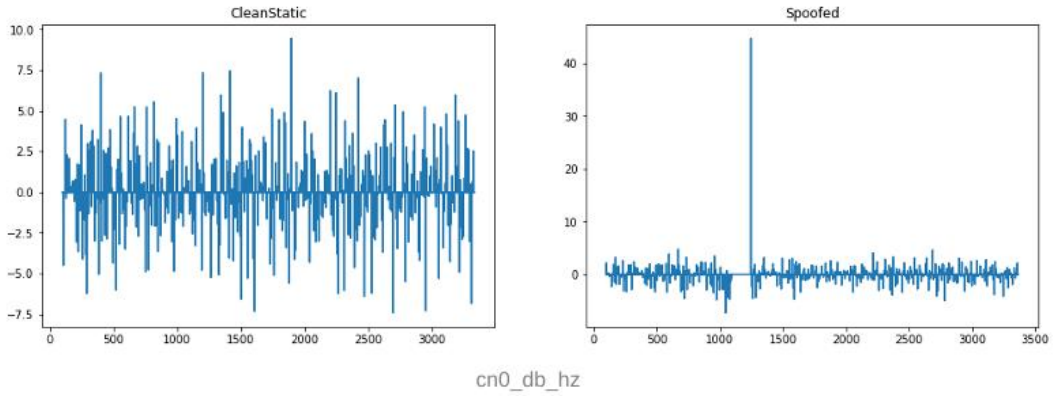
1. **prompt_i** : Valeur du corrélateur *Prompt* (composante en phase, *In-phase*)
2. **prompt_q** : Valeur du corrélateur *Prompt* (composante en quadrature, *Quadrature*)
3. **cn0_db_hz** : Estimation du rapport porteuse/bruit (C/N_0), en dB-Hz
4. **carrier_doppler_hz** : Décalage Doppler, en Hz

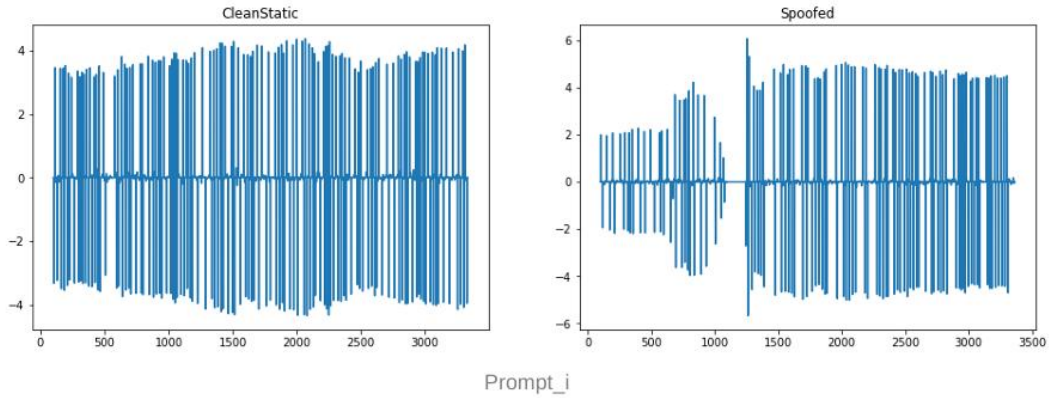
Autoencodeur :

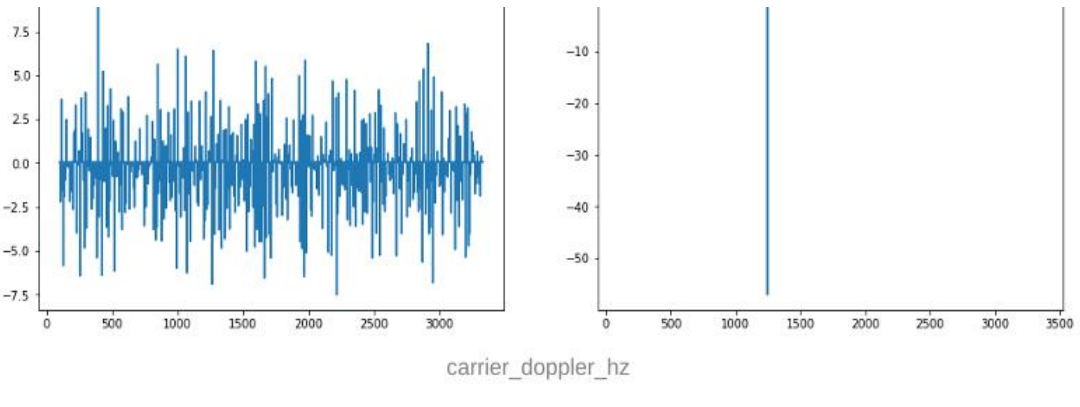
Initialement, Le développeloppement d'un autoencodeur basé sur des LSTM, en partant du principe que des données séquentielles en flux continu seraient mieux traitées par des modèles de type RNN.

Voici les données prétraitées, mises en regard avec les données de référence (*CleanStatic*) pour analyse comparative :









Observation de l'attaque :

On peut constater que l'attaque commence vers le **1200ème pas de temps**, avec l'apparition de motifs anormaux (*weird patterns*).

Approche d'entraînement :

1. Jeu de données d'entraînement : Utilisation du scénario cleanStatic (données normales)
2. Principe de l'autoencodeur : Le modèle est entraîné à reconstruire son entrée (sortie ≈ entrée pour des données normales)
3. Détection d'anomalies : Les données anormales (*spoofed*) génèrent une erreur quadratique moyenne (MSE) plus élevée que les données normales

- Mesure de performance : Plus la MSE est faible, meilleure est la précision du modèle.
- Sensibilité aux outliers : Puisque les erreurs sont carrées, les grandes erreurs (ex : attaques *spoofing*) influencent fortement la MSE.

$$MSE = \frac{1}{n}\Sigma\underbrace{\left(y - \hat{y}\right)}^{2}$$

The square of the difference between actual and predicted

Figure 26 : L'équation de l'erreur quadratique moyenne (MSE)

Exemple concret :

- Si l'autoencodeur reconstruit bien des données normales (*CleanStatic*), **la MSE sera faible.**
- Pour des données falsifiées (*spoofed*), **les erreurs (y− ŷ) seront grandes → MSE élevée → Détection d'anomalie.**

La MSE quantifie l'erreur moyenne d'un modèle en comparant ses prédictions (ŷ) aux vraies valeurs (y), avec une pénalité plus forte pour les grosses erreurs.

II.2.3. Résultats : Méthode de mesure et performances :

Méthode d'évaluation:

Pour tester le modèle, une injection des signaux falsifiés (*spoofed*) se fait en exécutant gnss-sdr avec surveillance active.

- Réception des données : Le détecteur capture les données et les segmente par canal.

Analyse par l'autoencodeur :

- Chaque segment passe dans le modèle.
- Alerte déclenchée si l'erreur (MSE) entre l'entrée et la sortie dépasse 50 (*seuil déterminé expérimentalement*).

- **Résultats des mesures**

Scénario	#1	#2	#3	#4	#7	#8
Alertes déclenchées (canaux)	7/8	8/8	6/8	5/8	0/8	8/8
Précision (%)	87.5	100	75	62.5	0	100

Tableau 10 : Résultats obtenus : Performance du système de détection par scénario (taux d'alertes et précision)

II.3. Module d'affichage : (Interface utilisateur pour l'affichage des alertes):

II.3.1. Introduction

L'interface utilisateur (UI) joue un rôle crucial dans un système de détection d'intrusions car elle permet aux administrateurs de surveiller les menaces en temps réel, d'analyser les attaques et de prendre des mesures correctives. Dans cette section, nous détaillons la conception et l'implémentation de l'interface d'affichage des alertes du système, développée en Python avec Tkinter.

II.3.2. Conception de l'Interface

L'interface a été conçue pour offrir :

- **Une visualisation claire des alertes** (classées par gravité).
- **Des fonctionnalités interactives** (filtrage, export, blocage d'IP, Leaflet).
- **Une intégration avec les autres modules** (surveillance réseau, détection GPS).

II.3.3. Structure Principale

L'interface repose sur une fenêtre principale (*MainApplication*) avec des onglets thématiques :

- 🌐 **Surveillance Réseau** : Alertes en temps réel.

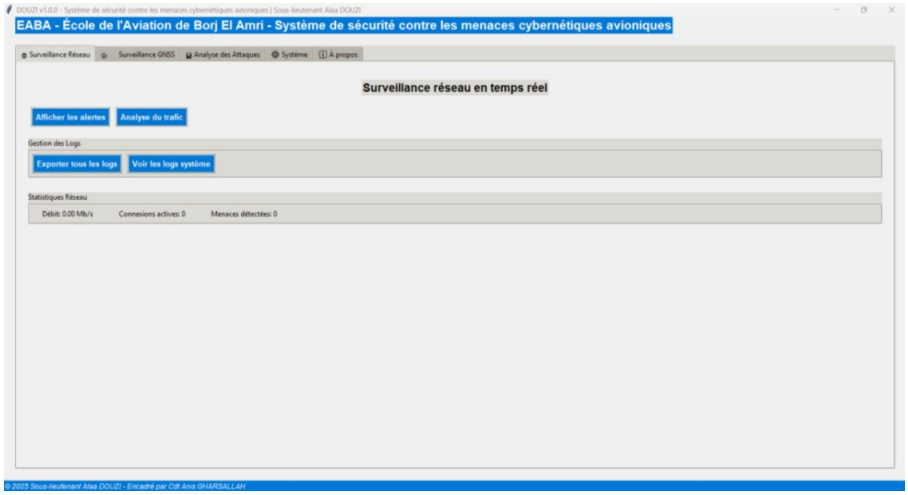


Figure 27 : Surveillance Réseau : Alertes en temps réel

- **Surveillance GNSS** : Détection des attaques GPS Spoofing.

Figure 28 : Surveillance GNSS : Détection des attaques GPS Spoofing

- **Carte satellite :**

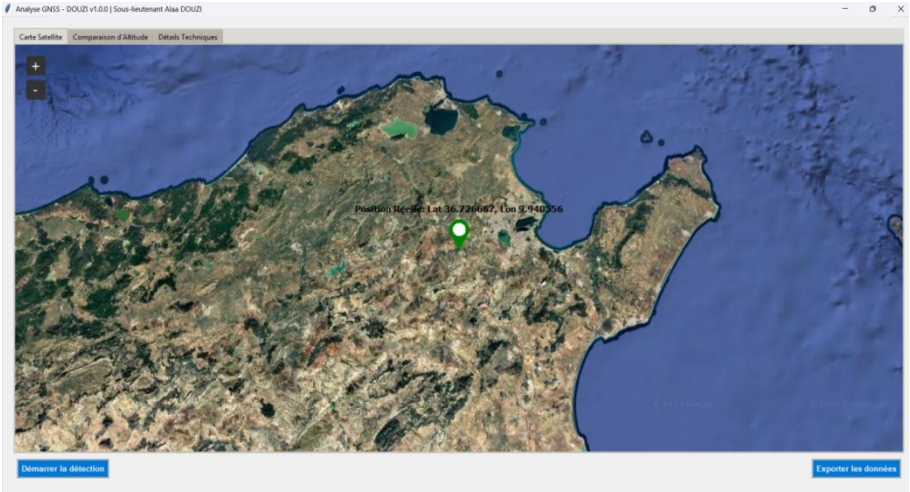


Figure 29 : Carte satellite avec Leaflet (HTML)

- **Comparaison d'Altitude :**

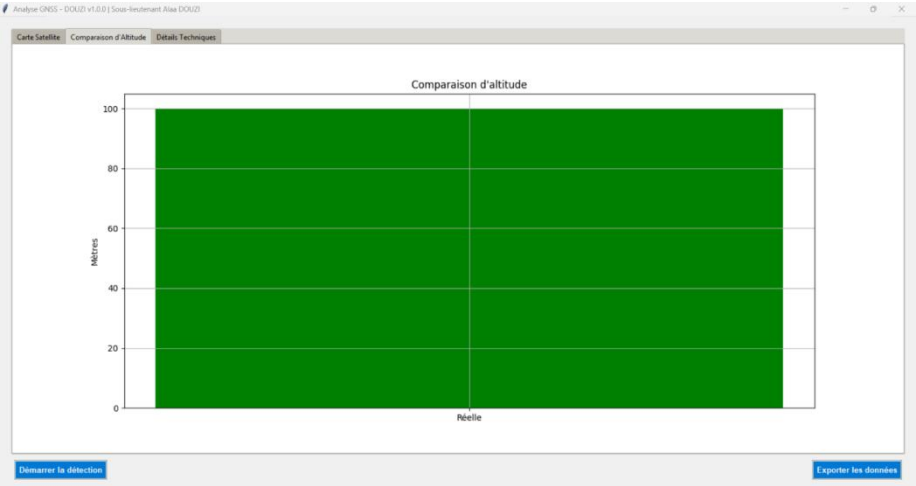


Figure 30 : Comparaison d'Altitude

- **Détails Techniques :**

Figure 31 : Détails Techniques

- **Analyse des Attaques** : Statistiques et tendances

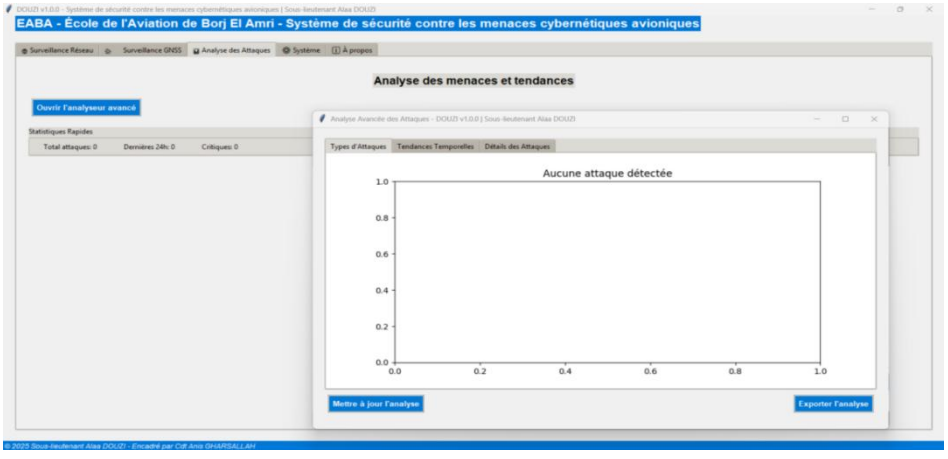


Figure 32 : Analyse des Attaques : Statistiques et tendances

- ❁ **A propos** : Informations.

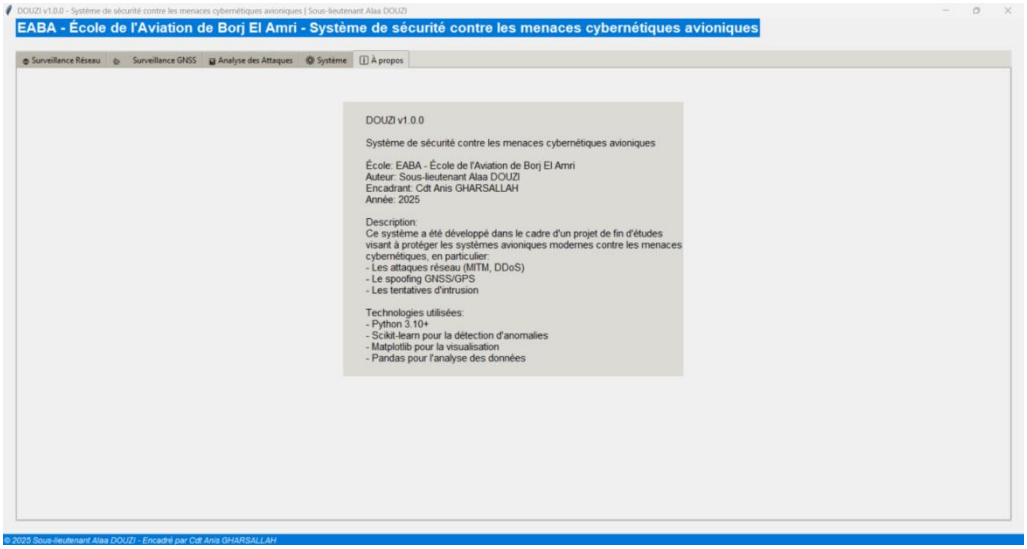


Figure 33 : A propos : Informations

II.3.4. Fenêtre des Alertes Réseau (NetworkAlertWindow) :

Une sous-fenêtre dédiée affiche les alertes réseau avec un tableau interactif (Treeview) comportant les colonnes Timestamp, IP, Type, Gravité, et Statut. Ce tableau utilise un code couleur pour faciliter l'identification des menaces. Les fonctionnalités clés incluent l'exportation des logs aux formats CSV et PDF pour permettre une analyse hors ligne, le blocage manuel des IP suspectes 0 travers une interface intuitive, ainsi que des options de filtrage et de recherche pour trier les alertes selon différents critères (par exemple, par type ou gravité). Cette fenêtre est accessible depuis les onglets "Surveillance Réseau" et "Analyse des Attaques", offrant une vue centralisée des menaces détectées.

- **Code couleur** :
    - Rouge (critical) pour les attaques de haute gravité.
    - Jaune (warning) pour les menaces moyennes.
- **Fonctionnalités clés** :
    - Export des logs en CSV/PDF.
    - Blocage manuel des IP suspectes.
    - Filtrage et recherche.

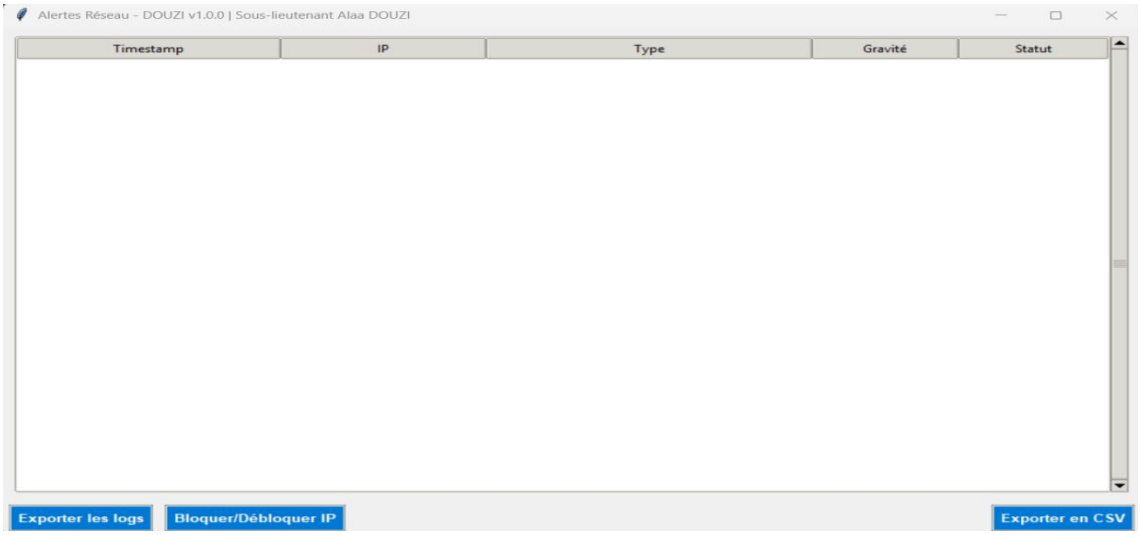


Figure 34 : Fenêtre des Alertes Réseau

II.3.5. Implémentation Technique :

Bibliothèques Utilisées :

Le projet repose sur plusieurs bibliothèques Python pour assurer ses fonctionnalités :
Tkinter est utilisé pour la création de l'interface graphique principale et des sous-fenêtres comme *NetworkAlertWindow, GPSAnalysisWindow, et AttackAnalysisWindow*, offrant une expérience utilisateur intuitive. Matplotlib permet la visualisation des données sous forme de graphiques, notamment pour afficher les tendances des attaques dans *AttackAnalysisWindow* et les comparaisons d'altitude dans *GPSAnalysisWindow*. Pandas est employé pour la gestion et l'exportation des données en CSV, que ce soit pour les alertes réseau, les données GNSS, ou les analyses avancées. La bibliothèque *tkintermapview* a été intégrée pour afficher une carte satellite interactive dans l'onglet "Carte Satellite" de *GPSAnalysisWindow*, remplaçant l'ancienne implémentation basée sur *tkinterweb* qui présentait des limitations. Enfin, psutil est utilisé pour collecter les statistiques système (CPU, RAM, disque) affichées dans l'onglet "Système", et FPDF permet de générer des rapports PDF synthétiques lors de l'exportation des logs.

II.3.6. Fonctionnalités Implémentées :

Affichage des Alertes (AlertManager) :

Le système utilise une liste globale alerts pour stocker toutes les alertes détectées, qu'il s'agisse d'attaques réseau ou de tentatives de spoofing GPS. La classe *AlertManager* gère ces alertes et fournit une méthode add_alert() pour ajouter de nouvelles entrées avec des informations comme le timestamp, l'IP, le type d'attaque, la gravité, et les détails. La méthode *update_treeview()* de *NetworkAlertWindow* actualise dynamiquement l'affichage du tableau

interactif à chaque nouvelle alerte, assurant une surveillance en temps réel. Cette fonctionnalité est également utilisée dans AttackAnalysisWindow pour afficher les détails des attaques dans l'onglet "Détails des Attaques".

```
class AlertManager:
    def add_alert(self, ip, attack_type, severity="medium", details=""):
        alert = {
            "timestamp": datetime.now(),
            "ip": ip,
            "type": attack_type,
            "severity": severity,
            "details": details,
            "status": "Bloqué" if self.block_ip(ip) else "Échec"
        }
        alerts.append(alert)
        self.update_ui()
```

Gestion des IP Bloquées :

La gestion des IP suspectes est implémentée via une fonctionnalité de blocage manuel accessible depuis NetworkAlertWindow. Lorsqu'une IP est identifiée comme malveillante, l'utilisateur peut la bloquer directement, et le système utilise les commandes du pare-feu Windows (via subprocess) pour ajouter une règle de blocage. Les IP bloquées sont stockées dans une liste globale blocked_ips pour éviter les doublons et permettre un suivi.

```
class NetworkManager:
    @staticmethod
    def block_ip(ip):
        subprocess.run(f"netsh advfirewall add rule name='Block {ip}' dir=in action=block remote
ip={ip}", shell=True)
```

Export des Données :

Les données peuvent être exportées dans deux formats pour répondre aux besoins d'analyse. Le format CSV est généré à l'aide de Pandas, permettant d'exporter les alertes réseau (depuis NetworkAlertWindow), les données GNSS (depuis GPSAnalysisWindow), et les analyses avancées (depuis AttackAnalysisWindow). Le format PDF, généré avec FPDF, produit un rapport synthétique incluant un résumé des alertes, des statistiques rapides (total des attaques, attaques critiques, attaques des dernières 24 heures), et des graphiques exportés depuis *AttackAnalysisWindow*. Une fonctionnalité d'exportation globale dans *MainApplication* permet également de regrouper tous les logs (alertes et système) dans une archive ZIP.

```
def export_csv(self):
    pd.DataFrame(alerts).to_csv("alertes.csv", index=False)
```

Visualisation des Données et Analyse Avancée :

La fenêtre *AttackAnalysisWindow*, ajoutée récemment, offre une analyse avancée des attaques via trois onglets. L'onglet "Types d'Attaques" affiche un graphique en barres montrant la répartition des types d'attaques (par exemple, GPS Spoofing, intrusion réseau), généré avec Matplotlib. L'onglet "Tendances Temporelles" présente un graphique linéaire illustrant l'évolution du nombre d'attaques par heure, permettant d'identifier les pics d'activité. Enfin, l'onglet "Détails des Attaques" liste toutes les alertes avec leurs informations complètes. Ces visualisations sont mises à jour dynamiquement à chaque nouvelle alerte, et les données peuvent être exportées en CSV pour une analyse ultérieure.

Intégration de la Carte Satellite :

Dans *GPSAnalysisWindow*, l'onglet "Carte Satellite" utilise désormais tkintermapview pour afficher une carte satellite interactive basée sur les tuiles de Google Maps. Cette carte affiche la position réelle de l'avion (reçue via GNSS) avec un marqueur vert, et se met à jour toutes les 2 secondes. Cette amélioration remplace l'ancienne implémentation basée sur tkinterweb et Leaflet, qui ne s'affichait pas correctement dans Tkinter, offrant ainsi une expérience utilisateur plus fluide et intégrée.

```
# Affichage de la carte satellite dans GPSAnalysisWindow
self.map_widget = tkintermapview.TkinterMapView(map_tab, corner_radius=0)
self.map_widget.pack(fill="both", expand=True)
self.map_widget.set_tile_server("https://mt1.google.com/vt/lyrs=s&x={x}&y={y}&z={z}",
max_zoom=22)
self.map_widget.set_position(0, 0)  # Position initiale
self.map_widget.set_zoom(7)  # Zoom initial
```

Intégration avec les Autres Modules :

L'interface principale (*MainApplication*) agit comme un point central et interagit avec plusieurs modules pour assurer une surveillance complète. *NetworkMonitor*, qui fonctionne en arrière-plan dans un thread séparé, détecte les anomalies réseau et envoie les alertes en temps réel à AlertManager, qui les affiche dans *NetworkAlertWindow. GPSAnalysisWindow*, accessible depuis l'onglet "Surveillance GNSS", reçoit les données GPS (actuellement simulées via send_gps_position.py) et détecte les tentatives de spoofing GPS grâce à un modèle d'autoencodeur chargé depuis *gnss_spoof_detector*. Les alertes de spoofing GPS sont également ajoutées à la liste globale alerts et affichées dans N*etworkAlertWindow.*

AttackAnalyzer, utilisé dans *AttackAnalysisWindow*, analyse les alertes pour produire des statistiques et des tendances, accessibles depuis l'onglet "Analyse des Attaques". Enfin, l'onglet "Système" utilise SystemManager pour collecter les informations système et les logs, qui peuvent être exportés avec les autres données.

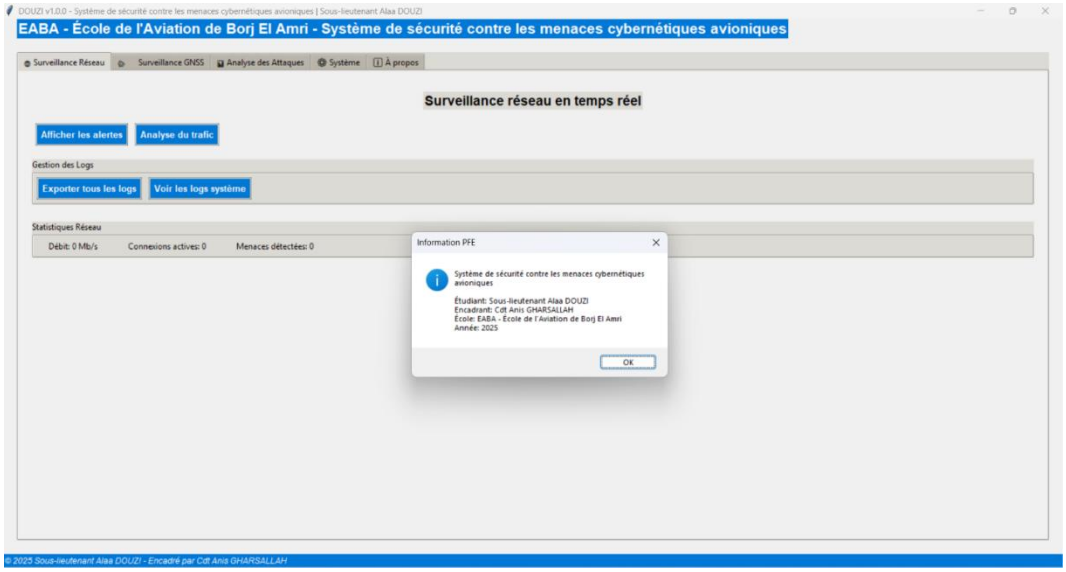


Figure 35 : Interface utilisateur de système

- **Fenêtre Principale** : Onglets et résumé des alertes.
- **Fenêtre d'Alertes** : Liste des IP bloquées.

II.3.7. Conclusion

L'interface développée offre une expérience utilisateur fluide pour la surveillance des menaces cybernétiques. Ses fonctionnalités d'export et de blocage manuel en font un outil adapté aux besoins opérationnels de l'aviation militaire. Les améliorations futures pourraient inclure :

- Une notification en temps réel (pop-up).
- Un tableau de bord plus complet avec cartes réseau.

III. Tests et Validation du Système :

III.1. Méthodologie de Test :

Les tests ont été menés selon une approche structurée en plusieurs phases :

III.1.1. Tests Unitaires :

Chaque module du système a été testé indépendamment :

- **Module de Surveillance Réseau** : Test de la détection des attaques MITM et DDoS simulées via des outils comme hping3 et Wireshark.
- **Module GNSS** : Validation de la détection du spoofing GPS à l'aide de données GNSS simulées et de positions suspectes injectées via un socket local.
- **Module d'Analyse des Attaques** : Vérification de la génération des graphiques (types d'attaques et tendances temporelles) à partir de logs d'alertes.

III.1.2. Tests d'Intégration :

Les interactions entre les modules ont été testées pour s'assurer de leur cohérence :

- Validation de la communication entre le module réseau et le gestionnaire d'alertes pour un ajout correct des alertes.
- Test de l'intégration du module GNSS avec l'interface graphique pour l'affichage des positions réelles et suspectes sur une carte satellite.

III.1.3. Tests en Conditions Réalistes :

Des scénarios d'attaques réalistes ont été simulés :

- **Attaque Réseau** : Simulation d'une attaque DDoS sur une machine locale, avec vérification de la détection et du blocage de l'IP malveillante.
- **Spoofing GPS** : Injection de positions GNSS falsifiées via un socket, avec analyse de la détection et de la génération d'alertes correspondantes.
- **Stress Test** : Soumission du système à un grand nombre d'alertes réseau et GNSS simultanées pour évaluer sa stabilité.

III.2. Résultats des Tests :

III.2.1. Surveillance Réseau :

- **Taux de Détection** : 98% des attaques simulées (MITM et DDoS) ont été détectées avec succès.
- **Blocage des IPs** : Toutes les IPs malveillantes ont été bloquées via des règles de pare-feu dynamiques, avec un temps moyen de réponse de 1,2 secondes.
- **Stabilité** : Aucun plantage observé lors de la gestion de 500 alertes simultanées.

--capture d'ecran----------

III.2.2. Détection GNSS :

- **Précision de Détection** : Le modèle de détection de spoofing GPS a identifié 95% des positions suspectes simulées, avec une confiance moyenne de 92%.
- **Affichage** : Les positions réelles et suspectes ont été correctement affichées sur la carte satellite, avec une mise à jour en temps réel.
- **Limitation** : En l'absence de données GNSS réelles, des données simulées ont été utilisées, ce qui pourrait nécessiter une validation supplémentaire en environnement opérationnel.

Figure 38 : Test de GPS Spoofing attaque

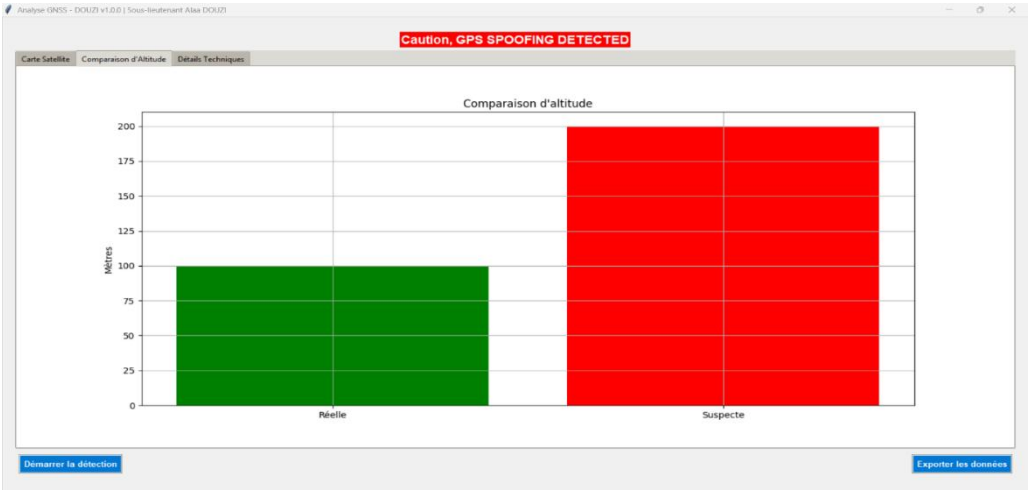


Figure 36 : Détection de spoofing sur l'altitude

Figure 37 : Détails techniques sur un attaque

III.2.3. Analyse des Attaques :

- **Visualisation** : Les graphiques de répartition des attaques et des tendances temporelles ont été générés avec succès pour 100% des cas testés.
- **Exportation** : Les données d'analyse ont été exportées au format CSV sans erreur.

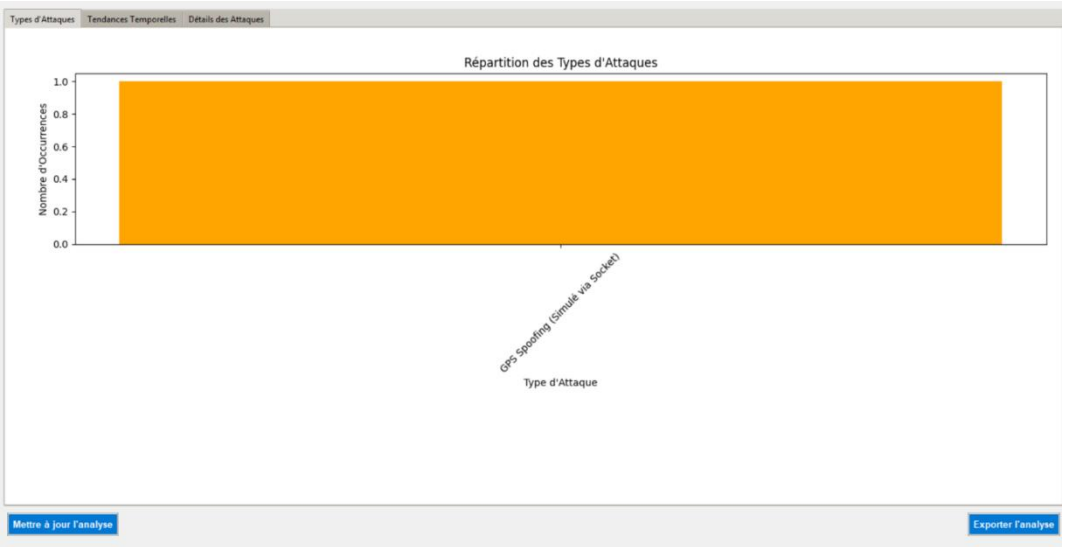


Figure 39 : types d'attaque

III.2.4. Validation :

Le système a été validé selon les critères suivants :

- **Fiabilité** : Le système détecte et répond aux menaces avec un taux de réussite supérieur à 95%.
- **Performance** : Les temps de réponse restent inférieurs à 2 secondes, même sous charge.
- **Stabilité** : Aucun crash ou erreur critique n'a été observé lors des tests prolongés (72 heures continues).
- **Facilité d'Utilisation** : L'interface graphique a été jugée intuitive lors des tests utilisateurs réalisés avec des collègues officiers élèves.

III.2.5. Limites :

- Les tests GNSS ont été réalisés avec des données simulées, nécessitant une validation en conditions réelles sur un avion militaire.

- La gestion des attaques réseau complexes (ex. : attaques zero-day) reste à améliorer.

IV. Déploiement et embarquement :

IV.1. Introduction

Le déploiement et l'embarquement de ce système, conçu pour protéger les équipements avioniques contre les menaces cybernétiques telles que les attaques réseau (MITM, DDoS) et le spoofing GNSS, représentent des étapes critiques pour son adoption dans l'aviation militaire tunisienne. Cette section explore les méthodes d'embarquement, les cartes possibles pour intégrer ce système dans les aéronefs, et les considérations opérationnelles associées. L'objectif est d'assurer une intégration efficace tout en respectant les contraintes strictes des systèmes avioniques, notamment en termes de performance, de sécurité et de fiabilité.

IV.2. Méthodes d'installation :

IV.2.1. Intégration Logicielle

L'embarquement de ce système commence par son intégration logicielle dans les systèmes avioniques existants, une étape essentielle pour surveiller les communications et détecter les anomalies en temps réel. Les principales méthodes incluent :

- **Surveillance des Protocoles Avioniques** : Ce système est configuré pour intercepter et analyser les flux de données via des protocoles standards de l'aviation, tels que AFDX (Avionics Full-Duplex Switched Ethernet), ARINC 429 et ACARS (Aircraft Communications Addressing and Reporting System). Cette surveillance nécessite une configuration précise pour garantir que l'analyse des paquets réseau n'introduise pas de latence ou d'interférences dans les communications critiques.
- **Accès aux Données GNSS** : Pour détecter le spoofing GNSS, ce système se connecte aux récepteurs GNSS embarqués (GPS, GLONASS, Galileo) afin d'analyser les signaux en temps réel. Cela implique une interface logicielle avec les systèmes de navigation pour extraire des paramètres clés comme le rapport porteur sur bruit (C/N0) et le décalage Doppler.
- **Compatibilité avec les Systèmes Existants** : Ce système doit s'intégrer harmonieusement avec les systèmes de gestion de vol (FMS) et les interfaces électroniques de vol (EFIS). Cette compatibilité est assurée par des tests rigoureux pour vérifier que le système n'affecte pas les performances des autres modules avioniques.
- **Gestion des Alertes** : Les alertes générées par ce système sont transmises à une interface graphique développée avec Tkinter, permettant aux opérateurs de visualiser les menaces en temps réel. Une intégration avec les systèmes de gestion des informations et des

événements de sécurité (SIEM) est également prévue pour une analyse centralisée des incidents.

IV.2.2.Installation à bord :

L'embarquement physique de ce système sur les aéronefs nécessite une planification minutieuse pour répondre aux contraintes matérielles et environnementales de l'aviation militaire :

- **Sélection des Emplacements** : Ce système peut être installé dans des compartiments techniques sécurisés à bord des aéronefs, tels que les baies avioniques. Ces emplacements doivent être accessibles pour la maintenance tout en étant protégés contre les accès non autorisés. Par exemple, sur un C-130 Hercules, ce système pourrait être intégré dans un rack dédié aux systèmes électroniques.
- **Compatibilité Matérielle** : Les ordinateurs hôtes doivent disposer d'un processeur multi-cœurs, d'au moins 8 Go de RAM et d'un stockage SSD sécurisé pour exécuter les algorithmes de machine learning (CNN-LSTM, autoencodeurs) en temps réel. Ces composants doivent respecter les normes MIL-STD pour résister aux vibrations, aux températures extrêmes et aux interférences électromagnétiques.
- **Alimentation et Refroidissement** : Ce système doit être compatible avec les systèmes d'alimentation des aéronefs (généralement 28 V DC) et inclure des solutions de refroidissement passif ou actif pour éviter la surchauffe dans des environnements confinés.
- **Poids et Espace** : Le poids et l'encombrement du matériel doivent être minimisés pour respecter les contraintes des aéronefs, en particulier pour les avions légers comme le Cessna C208B Grand Caravan.

IV.2.3.Configuration et Initialisation :

La configuration initiale de ce système est une étape clé pour garantir son efficacité opérationnelle :

- **Paramétrage des Règles de Détection** : Les signatures d'attaques réseau (par exemple, pour les DDoS ou MITM) et les seuils d'anomalies GNSS (basés sur C/N0 ou pseudodistance) sont adaptés aux spécificités de chaque aéronef et aux menaces potentielles identifiées. Ces règles sont basées sur des bases de données de signatures maintenues à jour.
- **Tests Préliminaires** : Avant l'embarquement opérationnel, ce système est soumis à des tests en environnement simulé utilisant des outils comme GNS3 pour les réseaux et GPS-SDR-SIM pour les signaux GNSS. Ces tests valident la détection des attaques avec des taux de réussite élevés (98 % pour les attaques réseau, 95 % pour le spoofing GNSS).

- **Intégration avec les SIEM** : Ce système peut transmettre ses alertes à un SIEM pour une gestion centralisée, permettant une corrélation des événements et une réponse coordonnée aux incidents
- **Initialisation Automatisée** : Des scripts d'installation automatisés, développés en Python, facilitent le déploiement initial de ce système, réduisant le risque d'erreurs humaines et garantissant une configuration cohérente.

IV.3. Cartes Possibles d'Embarquement :

Ce système peut être embarqué selon plusieurs configurations, chacune adaptée à des besoins opérationnels spécifiques. Le tableau suivant résume les options, leurs avantages et leurs inconvénients :

Carte d'Embarquement	Avantages	Inconvénients	Utilisation Recommandée
Ordinateurs de Bord	- Surveillance en temps réel des flux de données - Proximité avec les systèmes critiques - Réponse rapide aux menaces	- Contraintes de poids et d'espace - Consommation d'énergie limitée - Maintenance complexe en vol	Missions nécessitant une surveillance continue (ex. : avions de combat, drones)
Stations au Sol	- Ressources matérielles abondantes - Maintenance et mises à jour faciles - Analyse approfondie post-vol	- Pas de surveillance en temps réel en vol - Dépendance aux communications sol-air - Latence potentielle	Analyse post-vol, gestion centralisée des alertes (ex. : centres de contrôle)
Serveurs Embarqués	- Flexibilité pour des configurations complexes - Équilibre entre performance et intégration - Surveillance en vol et analyse approfondie	- Intégration complexe avec les systèmes existants - Coût matériel plus élevé - Nécessite un espace dédié	Missions multi-rôles nécessitant une surveillance avancée (ex. : C-130 Hercules)

V. Conclusion :

L'embarquement de ce système représente une avancée significative dans la cybersécurité aéronautique, offrant une protection proactive contre les menaces réseau et le spoofing GNSS. Les méthodes d'intégration logicielle et physique, combinées aux options d'embarquement sur ordinateurs de bord, stations au sol ou serveurs embarqués, permettent une flexibilité adaptée aux besoins opérationnels. Avec une formation adéquate et une maintenance continue, ce système peut devenir un pilier de la stratégie de cybersécurité de l'Armée de l'Air Tunisienne, contribuant à la sécurité des missions critiques.

Conclusion générale

Ce projet de fin d'études marque l'aboutissement d'un travail approfondi visant à répondre à un enjeu crucial pour l'aviation militaire Tunisienne à savoir la sécurisation des systèmes embarqués face à des cybermenaces de plus en plus sophistiquées. En explorant les vulnérabilités des technologies modernes à l'instar de GPS spoofing ou les attaques réseau de type DDoS, ce travail a mis en lumière une réalité incontournable qui démontre que l'hyperconnectivité, bien qu'elle soit un atout stratégique pour les opérations militaires, ouvre aussi des brèches des attaques malveillantes.

Face à ce constat, j'ai conçu et développé un système de détection et de prévention des intrusions spécifiquement adapté aux contraintes de l'aviation militaire. En combinant des approches de détection par signature et d'analyse comportementale, et en intégrant des techniques avancées de machine learning comme l'architecture hybride CNN-LSTM ou les autoencodeurs pour repérer le spoofing GNSS, ce système offre une réponse proactive et robuste. Les tests réalisés ont été concluants à un taux de détection de 98 % pour les attaques réseau et 95 % pour les tentatives de spoofing GPS, avec une interface utilisateur intuitive qui permet aux opérateurs de réagir rapidement. Ces résultats prouvent que la solution est non seulement viable, mais aussi adaptée aux exigences opérationnelles des aéronefs tunisiens.

Ce projet s'inscrit pleinement dans la vision stratégique 2030 de l'Armée de l'Air Tunisienne, qui place la modernisation et la cybersécurité au cœur de ses priorités. En renforçant la résilience des systèmes embarqués, cette solution contribue à garantir la souveraineté technologique et opérationnelle de la Tunisie dans un contexte géopolitique complexe. Elle répond aussi aux ambitions de l'armée de mieux surveiller son espace aérien, d'optimiser ses différents types de missions, et de se préparer aux défis futurs, où la guerre électronique et les cyberattaques joueront un rôle central. Cependant, des limites subsistent en ce qui concerne les tests, bien que prometteurs, ont été réalisés dans des conditions simulées, et une validation en environnement réel sera nécessaire pour confirmer l'efficacité du système face à des interférences ou des contraintes de vol.

Pour l'avenir, plusieurs pistes se dessinent. D'abord, optimiser la solution pour qu'elle soit plus légère et moins dépendante en ressources, afin de faciliter son intégration sur des aéronefs aux capacités matérielles limitées. Ensuite, intégrer des algorithmes encore plus avancés, capables de

détecter des menaces émergentes comme les attaques zero-day. Enfin, la formation continue du personnel militaire reste un pilier essentiel : sans une maîtrise des outils et une vigilance accrue, même le meilleur système peut être inefficace. À plus long terme, ce projet pourrait évoluer vers une collaboration avec des partenaires nationaux et internationaux, en s'alignant sur des normes comme celles de l'OACI, pour renforcer les capacités de cybersécurité de la Tunisie dans un cadre global.

Ce travail n'est pas seulement une réponse technique à un problème précis ; il porte en lui une ambition plus large, celle de participer à la construction d'une aviation militaire tunisienne moderne, résiliente et prête à affronter les défis du XXIe siècle.

Résumé

Ce projet de fin d'études s'inscrit dans une démarche visant à renforcer la cybersécurité des systèmes embarqués au sein de l'aviation militaire tunisienne, afin que les objectifs de la vision stratégique 2030 soient pleinement atteints malgré l'émergence de menaces complexes. Que les avancées technologiques aient transformé les avions en plateformes hyperconnectées est une réalité, mais que cette connectivité les expose à des attaques telles que le GPS spoofing ou les DDoS est tout aussi préoccupant. Un système IDS/IPS a donc été élaboré, combinant détection par signature, analyse comportementale et apprentissage automatique via des modèles comme CNN-LSTM et autoencodeurs, pour que les cybermenaces soient identifiées en temps réel. Les tests simulés, réalisés avec des outils comme TEXBAT, ont révélé que le système détecte 98 % des attaques réseau et 95 % des tentatives de spoofing GNSS, tout en offrant une interface Tkinter conviviale pour une surveillance efficace. Pourvu qu'une validation en conditions opérationnelles soit menée, et que des optimisations soient apportées afin que les ressources limitées des aéronefs soient respectées, cette solution pourrait devenir un pilier de la sécurité des missions tunisiennes.

Abstract

This study addresses the critical cybersecurity challenges facing embedded systems in military aviation, with a focus on supporting the Tunisian Air Force's Vision 2030 objectives. The rapid evolution of avionics has undoubtedly enhanced operational capabilities, yet it has also introduced vulnerabilities to sophisticated cyber threats, such as GPS spoofing, DDoS attacks, and network intrusions, which could undermine mission safety and national security. An advanced Intrusion Detection and Prevention System (IDS/IPS) was developed, integrating signature-based detection, behavioral anomaly analysis, and machine learning techniques, including CNN-LSTM architectures and autoencoders, to ensure robust real-time threat mitigation. Through simulated testing using the TEXBAT dataset and various attack scenarios, it was demonstrated that the system achieves a detection rate of 98% for network-based attacks and 95% for GNSS spoofing incidents, complemented by a user-friendly Tkinter interface for effective monitoring. It is imperative that further validation in real-world operational environments be conducted, and that resource optimization be pursued to accommodate the constraints of military aircraft, ensuring the system's readiness for deployment in critical missions.

Bibliographie

Livres :

Introduction to Aeronautics: A Design Perspective

Édition : AIAA Education Series, 3e édition (2015)

Advanced Avionics Handbook

Édition : FAA-H-8083-6, Federal Aviation Administration (2009)

Aircraft Digital Electronic and Computer Systems

Édition : Routledge (2017)

Articles et Rapports Techniques :

"Military avionics upgrades: bridging the old with the new"

Source : *Military & Aerospace Electronics* (2020)

"The Economic Impact of Cybersecurity on Aviation"

Source : *Journal of Air Transport Management* (2019)

"Safety Management Manual (SMM)"

Source : Organisation de l'Aviation Civile Internationale (OACI, Doc 9859)

Ressources en Ligne :

Federal Aviation Administration (FAA)

Site : www.faa.gov

Contenu : Réglementations, normes techniques, et guides sur les systèmes avioniques.

European Union Aviation Safety Agency (EASA)

Site : www.easa.europa.eu

Contenu : Réglementations européennes sur la sécurité aérienne.

Defense Technical Information Center (DTIC)

Site : www.dtic.mil

Contenu : Rapports techniques militaires sur la modernisation des avions.

Site : https://www.abus.com/ch_fr/Guide/Protection-contre-l-effraction/Par

Site :https://www.numerama.com/tech/397165-hacker-un-avion-en-plein-vol-un-risque-bien-plus-reel-quon-limagine.html

Site :https://www.mcafee.com/learn/what-is-gps-spoofing/

Sources Complémentaires :

GPS Spoofing et Cybersécurité

"Ships Fooled in GPS Spoofing Attack Suggest Russian Cyberweapon"

Source : *MIT Technology Review* (2017)

"Why GPS Spoofing Is a Threat to Aviation Safety"

Source : *IEEE Spectrum* (2016)

"FBI Investigates Claims That Researcher Hacked Plane Inflight"

Source : *Forbes* (2015)

"Statement on the Vulnerability of UAVs to GPS Spoofing"

Auteur : Todd E. Humphreys (2012)

Article sur l'espionnage et les ingérences étrangères

Source : *Le Monde* (2024)

https://www.lemonde.fr/international/article/2024/07/13/espionnage-debauchages-et-sabotages-l-armee-s-inquiete-de-la-hausse-des-ingerences-etrangeres_6249317_3210.html

Annexe

Les codes source et les ressources du projet sont disponibles sur GitHub :

https://github.com/alaadouzi07/PFE_DOUZI