Détection d'anomalies pour les données radars du système de contrôle aérien en utilisant la prédiction de données

Théobald de Riberolles

THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par :

l'Institut National des Sciences Appliquées de Toulouse (INSA de Toulouse)

Présentée et soutenue le *08/07/2021* **par :**

Théobald de RIBEROLLES

Détection d'anomalies pour les données radars du système de contrôle aérien en utilisant la prédiction de données

---

JURY

Christophe CHASSOT	Professeur d'Université	Président du Jury
Damien MAGONI	Professeur d'Université	Examinateur
Anne SABOURIN	Maître de Conférences	Examinateur
Cherifa BOUCETTA	Maître de Conférences	Examinateur
Guillaume URVOY-KELLER	Professeur d'Université	Rapporteur
Sidi Mohammed SENOUCI	Professeur d'Université	Rapporteur
Guthemberg DA SILVA SILVESTRE	Enseignant chercheur	Co-encadrant
Jiefu SONG	Docteur	Co-encadrant

École doctorale et spécialité :

EDSYS : Informatique 4200018

Unité de Recherche :

Laboratoire de Recherche ENAC

Directeur(s) de Thèse :

Nicolas LARRIEU et *Guthemberg DA SILVA SILVESTRE*

Rapporteurs :

Guillaume URVOY-KELLER et *Sidi Mohammed SENOUCI*

Détection d'anomalies pour les données radars du système de contrôle aérien en utilisant la prédiction de données

Théobald de RIBEROLLES

Remerciements

J'aimerai, tout d'abord remercier vivement le Docteur Guthemberg Da Silva Silvestre, enseignant chercheur à l'ENAC, qui bien que co-Directeur de Thèse a su prendre en main la responsabilité de Direction de thèse et qui a su par ses encouragements, ses conseils et ses remarques judicieuses me donner confiance et me pousser à donner le meilleur de moi même pour la réalisation de cette thèse. Une pensée particulière pour le Docteur Nicolas Larrieu, enseignant chercheur à l'ENAC, mon Directeur de Thèse qui malheureusement pour des raisons de santé n'a pas pu m'accompagner autant qu'il l'aurait souhaité mais a su initié le sujet et m'accompagnait au début de la recherche. Je tiens particulièrement à remercier le Docteur Emmanuel Lochin, enseignant chercheur à l'ENAC, qui en toute discrétion, avec efficacité et rigueur s'est démené pour m'apporter le support et les conseils au niveau de la préparation d'articles mais aussi principalement pour assurer la qualité de la rédaction de ce manuscrit et la préparation de la soutenance.

Je tiens à remercier vivement le Professeur Guillaume Urvoy-Keller, Professeur des Universités à l'université Côte d'Azur et le Professeur Mohammed Senouci, Professeur des Universités à l'université de Bourgogne pour l'honneur qu'ils me font en acceptant d'être les rapporteurs de cette thèse.

Toute ma gratitude va également au Professeur Christophe Chassot du LAAS-CNRS pour avoir accepter de présider le jury de ma thèse ainsi qu'au Professeur Damien Magoni et aux Docteurs Anne Sabourin et Cherifa Boucetta examinateurs du présent travail.

Mes remerciements s'adressent également à la société ACTIVUS Group pour m'avoir accueilli au sein de leur équipe, m'avoir fait confiance et m'avoir donner les conditions nécessaires pour réaliser cette thèse CIFRE. je tiens ainsi à remercier tout particulièrement mon encadrant au sein de la société, le Docteur Jiefu Song, qui su m'accompagner, me soutenir et m'encourager pour la réalisation de cette thèse. je remercie également le Docteur Christelle Bidouil et le Docteur Jérémy Bascans ainsi que Nicolas Cavasa qui m'ont accompagné au sein de la société au cours de la thèse et qui m'ont permis de m'améliorer. Enfin je n'oublie pas Pascal Diogo et Audrey Picco qui m'ont permis d'être intégré pleinement au sein d'ACTIVUS.

Je ne saurai oublié les membres du groupe RESCO du l'équipe Télécommunication du laboratoire de l'ENAC qui m'ont accueilli, écouté et conseillé tout au long de cette thèse. Je remercie tout particulièrement le directeur de ce groupe, le Docteur Alain Pirovano,

Enseignant Chercheur, qui m'a apporté tant un soutien administratif que personnel. Je remercie également Michel Soler et Serge Roux de l'ENAC pour avoir pris le temps de partagé avec moi leurs connaissances sur les données radars et m'avoir apporté leur expertise tout au long de ce travail.

Je ne peux oublier Pierre-Marie Besserer de la DSNA-DTI, initiateur du projet, qui m'a apporté des connaissances supplémentaires sur le fonctionnement de la DGAC, la sécurité existante et celle qui manque. Il a été mon point de contact industrielle et m'a permis de donner un but concret et attendu à mes travaux de recherche.

Ma reconnaissance s'adresse à mes compagnons de route que j'ai pu côtoyer tant à ACTIVUS qu'à l'ENAC. Je les remercie vivement pour la bonne ambiance de travail et la solidarité qu'ils m'ont témoignés. Je remercie également Mme Hélène Thirion de l'EDSYS qui m'a accompagné administrativement et humainement pendant ces trois ans.

Je suis particulièrement redevable au Professeur André-Luc Beylot, Professeur des Universités à l'INP-ENSEEIHT pour m'avoir encouragé à entreprendre ce travail de thèse et m'avoir aidé à trouver les membres du jury.

Ces remerciements ne peuvent s'achever qu'en ayant une pensée particulière pour ma famille, mes parents, frères, sœurs et mes amis pour l'accompagnement lors de mes travaux, qui ont su trouver les mots justes pour m'accompagner et qui n'ont pas hésité à me prodiguer leurs conseils . Enfin je remercie tout spécialement ma femme qui a été soumise à rude épreuve pendant ces trois ans et notamment lors des phases de rédaction et de rendu mais qui a toujours cru en moi et m'a apporté un soutien inconditionnel. Merci également à mes enfants, qui bien que peu âgés, m'ont permis d'avoir le temps nécessaire de réaliser ces travaux.

Merci à tous ceux qui m'ont aidé et soutenu donc j'ai oublié de citer les noms.

Je dédie ce travail à mon grand-père qui a su développer ma curiosité et mon esprit scientifique.

Résumé

Les données radars transportées au sein du système ATM (Air Traffic Management) permettent aux contrôleurs de l'aviation civile d'effectuer le contrôle aérien et ainsi d'assurer la sécurité des avions et de leurs passagers. Cependant, l'émergence récente d'attaques sur des systèmes similaires couplée avec la haute criticité de ces données conduit à se poser la question d'assurer la sécurité des données radars. Bien qu'il existe physiquement des moyens mis en œuvre pour se protéger de potentielles attaques, les mécanismes de prédictions d'anomalies traditionnellement utilisés dans le monde des réseaux IP ne permettent pas d'obtenir des résultats satisfaisants car non conçus pour des besoins avioniques. En effet, les systèmes utilisés ne permettent pas de considérer des données spatio-temporelles en prenant en compte la mémoire des traces des avions. De plus, malgré la criticité caractérisant les échanges radars, la détection d'anomalies relatives à ces données a été peu étudiée jusqu'à présent. C'est donc face à ce manque que s'est inscrite cette thèse avec pour but le développement d'une méthodologie de détection d'anomalies dédiée au système du contrôle aérien. L'idée est d'utiliser le comportement régulier du trafic aérien pour identifier un schéma dans le comportement des données radars, puis d'utiliser ensuite ce schéma normal pour identifier des anomalies.

La première partie se concentre sur la mise en place d'une méthode de détection par identification de profil au niveau du radar en lui-même. L'étude est faite de manière statistique sur l'évolution de la donnée radar au niveau temporel. L'objectif est de pouvoir caractériser un comportement qui statistiquement va présenter des tendances dans le temps, puis mettre en place une méthode de détection basée sur un mécanisme de prédiction de données. Cette méthode permet de faire de la détection d'anomalies sur le comportement global d'un radar, mais ne permet pas d'aller jusqu'au niveau de détail d'un avion.

Afin de rentrer plus en profondeur dans les données nous nous basons sur une détection par le biais des modèles de machine Learning. Par ces modèles, nous prévoyons le comportement des données radars et par le biais d'un seuil de détection nous identifions quand le comportement réel diffère du comportement prédit. Dans le cadre de l'aviation civile, peu d'anomalies sont connues ou répertoriées. Il faut donc travailler sur des jeux de données non labellisées, il est alors nécessaire d'utiliser une approche d'apprentissage non supervisée. Pour cela, nous utilisons un mécanisme d'auto-encodeur, basé sur du Long Short Term Memory (LSTM) qui nous permet de nous adapter aux caractéristiques spatio-temporelles de nos données et de répondre à cette approche non supervisée. La méthode a été testée sur un jeu de données opérationnelles qui nous a permis d'identifier des anomalies présentes sur le jeu de données. Afin de pouvoir comparer notre méthode

avec d'autres méthodes de détection et pour pouvoir répondre aux besoins spécifiques de l'aviation civile relatifs à certaines attaques qui n'étaient pas présentes dans le jeu de données, nous avons simulé des attaques réalistes sur le système radar en se plaçant au niveau d'un attaquant qui se serait infiltré sur le système. Ces simulations nous ont permis de nous assurer de l'efficacité de notre mécanisme de détection par rapport à ces attaques, mais surtout de pouvoir tester notre mécanisme en condition opérationelle.

Mots-clés : Détection d'anomalies, Gestion du Trafic Aérien, Système de détection d'Intrusion, Caractérisation, Réseau, Data Science.

Abstract

The radar data transported within the ATM (Air Traffic Management) system enables civil aviation controllers to carry out air traffic control and thus safety of planes and passengers's safety. However, the recent emergence of attacks on similar systems coupled with the high criticality of this data raises the question of ensuring the radar data security. Although there are physical means implemented to protect against potential attacks, the anomaly prediction mechanisms traditionally used in the world of IP networks do not allow satisfactory results to be obtained because they do not consider aviation needs. Indeed, the systems used do not make it possible to consider spatio-temporal by taking into account the memory of aircraft tracks. In addition, despite the criticality characterizing radar exchanges, the detection of anomalies relating to these data has been few studied so far. It is therefore in the face of this lack that this thesis took place, with the aim of developing an anomaly detection methodology dedicated to the air traffic control system. The idea is to use the regular behavior of air traffic to identify a pattern in the behavior of the radar data, and then use that normal pattern to identify anomalies.

The first part focuses on the implementation of a detection method by profile identification at the level of the radar itself. The study is done statistically on the evolution of radar data over time. The objective is to be able to characterize a behavior that will statistically show trends over time, then set up a detection method based on a data prediction mechanism. This method makes it possible to detect anomalies in the overall behavior of a radar, but does not go down to the level of detail of an aircraft.

In order to go deeper into the data, we are basing ourselves on detection through machine learning models. By these models we predict the behavior of the radar data and by means of a detection threshold we identify when the actual behavior differs from the predicted behavior. In the context of civil aviation, few anomalies are known or listed. It is therefore necessary to work on unlabelled datasets, so it is necessary to use an unsupervised learning approach. For this, we use an auto-encoder mechanism, based on Long Short Term Memory (LSTM) which allows us to adapt to the spatio-temporal characteristics of our data and to respond to this unsupervised approach. The method was tested on an operational dataset which allowed us to identify anomalies present on the dataset. In order to be able to compare our method with other detection methods and to be able to meet the specific needs of civil aviation relating to certain attacks that were not present in the data set, we simulated realistic attacks on the radar system by placing himself at the level of an attacker who has infiltrated the system. These simulations have enabled us to ensure the efficiency of our detection mechanism

in relation to these attacks, but above all to be able to test our mechanism in operational condition.

Keywords : Anomaly Detection,Air Traffic Management, Intrusion Detection System, Characterization, Network, Data Science.

Table des matières

Table des figures

Liste des tableaux

Liste de Sigles

La liste suivante décrit les différents sigles qui seront plus tard utilisé dans le corps de ce document

$ADS-B$ Automatic Dependent Surveillance Broadcast

$ANSP$ Fournisseur de Services de la Navigation Aérienne

$ASTERIX$ STructured Eurocontrol suRveillance Information eXchange

ATC Air Traffic Control

ATM Air Traffic Management

CGS Calculated Ground Speed

$CHDG$ Calculated Heading

$CRNA$ Centre en Route de la Navigation Aérienne

$DGAC$ Direction Générale de l'Aviation Civile

$DGAC$ Direction des Services de la Navigation aérienne

EDA Analyse Exploratoire de données

FL Niveau de vol

$FSPEC$ Field SPECification

ICS Système de Contrôle Industriel

IDS Système de Détection d'Intrusion

$LSTM$ Long Short Term Memory

$MITM$ Man In The Middle

PSR Radars Primaire de Surveillance

RNN Réseau Neuronal Récurrent

SAC Source Area Code

SIC Source Identification Code

SSR Radars Secondaire de Surveillance

ToD Time of Day

TPN Track Plot Number

TS Timestamp

UAP User Application Profile

1 Introduction

1.1 L'aéronautique et les menaces cyber

La diminution drastique d'année en année des accidents aéronautiques font de l'aérien un des moyens de transport le plus sûr. C'est également un moyen qui ne cesse de s'améliorer et qui, pour gagner en efficacité, se connecte de plus en plus grâce à des moyens de communications modernes et ce, aussi bien pour les passagers que pour les systèmes aux sols permettant d'assurer le guidage des avions. Cependant, cette connectivité résulte en l'accroissement du risque concernant la sécurité des avions puisqu'elle augmente de manière significative la surface d'attaque du transport aérien. Guillaume Poupard, le directeur général de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Informations), disait en 2018 [60] que, si une attaque cyber faisait tomber un avion, "dans la foulée, il n'y a plus aucun avion qui décolle ! [...] il faut impérativement que cela ne soit pas possible", car les conséquences en terme humains et économiques seraient énormes.

Le milieu aéronautique n'est pas isolé des problématiques cybe ; croire que le transport aérien est à l'abri de ce genre de menaces est une illusion, il peut faire face à des attaques de plus en plus élaborées motivées par le terrorisme, l'aspect financier ou le *hacktivisme*. Bien qu'à ce jour aucun événement d'une telle ampleur n'ait été enregistré, le monde du transport aérien doit accompagner sa transformation digitale vers des modèles de sûreté et de sécurité qui s'équilibrent pour prendre en compte la menace cyber. Kandera et al. [48] nous présentent dans leur document un ensemble de menaces sur les systèmes de surveillance qui seront développés dans le chapitre 2. Nous pouvons prendre l'exemple de l'opération *Orchard* en 2007 au cours de laquelle l'aviation israélienne a pu détruire un site syrien, semble-t-il, par le biais d'un code malveillant ayant faussé les données des écrans radars provoquant ainsi la disparition de certains vols [31]. Même si cette menace est principalement militaire à l'heure actuelle, elle peut s'étendre au trafic civil.

1.2 Le contexte cyber pour le contrôle aérien

Les Fournisseurs de Services de la Navigation Aérienne (ANSP) sont les organismes responsables de la gestion du trafic aérien. En France, l'ANSP est la Direction Générale de l'Aviation Civile (DGAC) et plus particulièrement la Direction des Services de la Navigation aérienne (DSNA) . C'est un Organisme d'Importance Vitale (OIV) pour le pays. En effet, elle a pour mission de suivre les aéronefs à travers l'espace aérien, de leur transmettre des informations, d'adapter leurs trajectoires de vol aux conditions météorologiques et de les guider dans les phases délicates de décollage et d'atterrissage, etc. Elle assure ainsi la sécurité de l'espace aérien par la gestion de son trafic (ATM) et son contrôle (ATC). Une défaillance sur ce système peut donc avoir de graves conséquences. En effet, de plus en plus connecté aux compagnies aériennes, aux aéroports et aux autres prestataires de contrôle du trafic aérien, le système ATC est de facto de plus en plus vulnérable aux cyberattaques. La cybersécurité devient ainsi un enjeu majeur pour la DSNA.

Afin d'assurer sa mission, la DSNA a donc besoin d'avoir un système ATC fiable et robuste. Pour cela, elle s'appuie sur un ensemble de centres de contrôle, de capteurs (principalement des radars), de moyens de communication (centres, contrôle et gestion du trafic aérien) et de systèmes de radionavigation, répartis sur l'ensemble du territoire (métropolitain et ultra-marin).

Ce système, développé à la fin des années 1980, début des années 1990, était auparavant considéré comme isolé, mais suite à des évolutions technologiques et à des changements concernant sa réglementation, ce système isolé, et ainsi en un sens protégé, se retrouve considéré comme potentiellement attaquable.

Une analyse de risque interne au sein de la DGAC fixe la criticité du système ATC comme étant élevée. En effet, une attaque sur la liaison de communication peut s'apparenter à un leurre, visant la transmission de fausses données ou de données modifiées au contrôleur. Si aucun moyen de vérification de la disponibilité, de l'authenticité, de l'intégrité, de la confidentialité et de la traçabilité de ces informations n'est prévu, cela peut amener le contrôleur à prendre une mauvaise décision de guidage ce qui peut conduire au détournement d'un aéronef ou engendrer une collision. Il est donc primordial de s'assurer de la sécurité sur ces échanges d'informations.

Les échanges entre le sol et le bord ainsi que les échanges sol-sol pour guider les avions évoluent afin de permettre une meilleure efficacité pour le contrôle aérien. Une plus grande interconnexion entre les entités transforme les centres de contrôle isolés en nœud d'un réseau interne. Ce développement se fait par le biais d'utilisation de matériel et

de protocoles standards. Néanmoins, il en résulte une cohabitation avec des systèmes, des moyens et des protocoles déjà existants et propres à l'aviation civile, augmentant ainsi la vulnérabilité en cas d'intrusion. Actuellement, la sécurité au sein d'un système de surveillance se base sur plusieurs principes [44]

— le réseau utilisé est physiquement isolé des réseaux plus ouverts ;
— le système est situé dans un bâtiment sécurisé avec accès restreint ;
— le système est utilisé par des opérateurs entrainés et certifiés ;
— une sécurité logicielle et physique de base est opérée contre des malveillances classiques des SI.

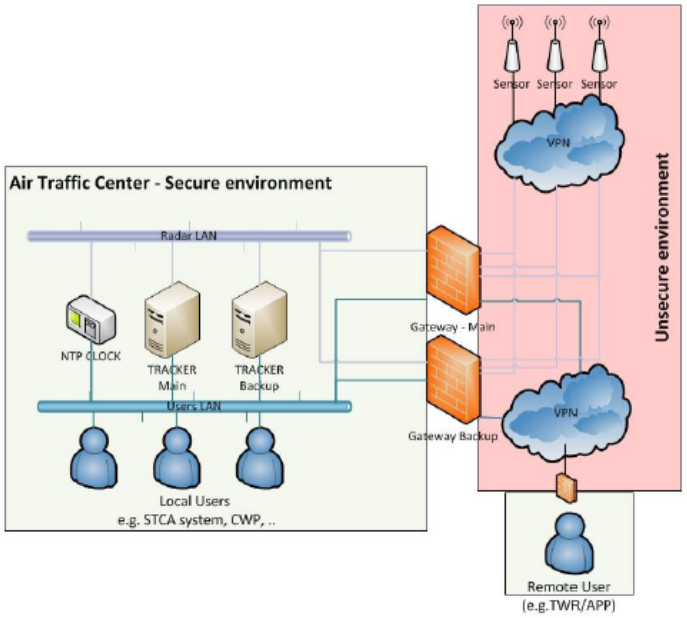


FIGURE 1.1 – Représentation schématique de l'isolation du réseau

Bien qu'existants, ces mécanismes ne permettent plus de répondre à des exigences de sécurité élevées. Pour répondre à ces exigences, la DSNA souhaite développer une détection d'anomalies sur ses systèmes notamment par le biais de sonde. Cela fait écho aux recommandations [1] de l'Académie de l'Air et de l'Espace qui, pour faire face aux menaces cyber visant l'espace aérien, préconisent "d'être capable de détecter en temps réel si le fonctionnement d'un système est normal ou anormal et de faire remonter les informations de non-cohérence vers les opérateurs". Ainsi ce travail de thèse porte sur le développement d'un mécanisme de sécurité servant à détecter des anomalies afin de pouvoir répondre à ces préconisations et développer un Système de Détection d'Intrusion pour l'aviation civile (IDS).

1.3 Focus sur les données radars

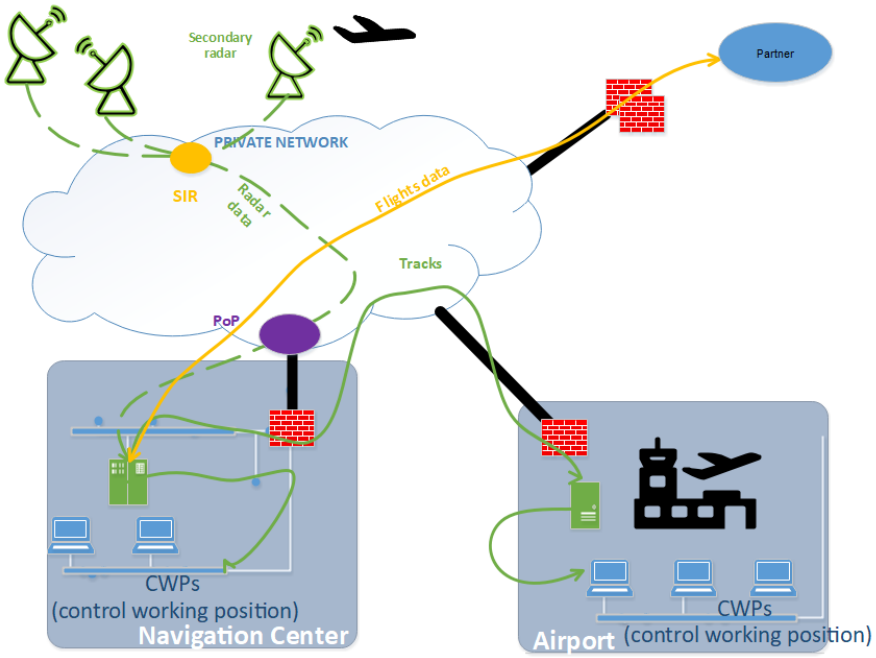


FIGURE 1.2 – Représentation schématique du réseau ATM

Le système radar est au cœur du système ATC. Les données radars fournissent la position en temps réel de chaque aéronef et permet à un contrôleur d'assurer la sécurité des passagers, en assurant la séparation horizontale et en exécutant des fonctions ATC [1]. Le système ATC (voir figure 1.2) permet d'assurer le transport de l'information des radars. Par leur biais, le système collecte des informations sur un aéronef, notamment sa position, sa vitesse, son identifiant, le type d'aéronef et tout ce qui peut être utile à un contrôleur. Il envoie ces informations sur un réseau privé qui achemine les paquets à différents centres de navigation, les CRNA , "Centre en Route de la Navigation Aérienne" [2] . Dans ce centre, la trace de l'avion est reconstruite et affichée sur un écran face au contrôleur resposnable de leur guidance. Une analyse de risque réalisée au sein de la DSNA a montré que les données de surveillance radar sont des données clés dans le service rendu. Les données radars sont ainsi considérées comme valeurs métiers [3].

1. www.eurocontrol.int/node/4931/
2. Un CRNA est un centre de contrôle régional, assurant la sécurité du trafic aérien dans une zone définie - en France, il y a cinq CRNA
3. La méthode EBIOS Risk Manager présente valeurs métiers comme "une composante importante pour l'organisation dans l'accomplissement de sa mission" https ://www.ssi.gouv.fr/uploads/2018/10/guide-methode-ebios-risk-manager.pdf

En effet, le DICT [4] montre une disponibilité et une intégrité critique : étant la donnée principale sur laquelle s'appuient les contrôleurs pour faire leur travail, la modification ou la perte de données radars a une conséquence directe sur la réalisation du contrôle aérien et donc potentiellement sur la sécurité des aéronefs. Il y a donc un risque humain qui permet de placer le curseur de criticité comme élevé critique. Nous avons donc choisi par la suite de nous concentrer essentiellement sur les données radars afin d'assurer un niveau de sécurité sur le cœur du système ATM.

Afin de transmettre les données radar, le système ATC utilise un protocole open-source unique : le protocole ASTERIX [26], qui encapsule les données des avions transmises. Malgré une utilisation majoritaire par les ANSP au niveau mondial, le protocole n'a pas été conçu avec des mécanismes de sécurité [44], ce qui expose l'ensemble du système à des vulnérabilités. De plus, du fait de son utilisation très particulière pour la surveillance, ASTERIX n'est pas connu par les IDS du marché qui le considére comme du trafic conventionnel. Selon la DSNA, les méthodes de détection d'anomalies classiquement utilisées ne donnent pas de résultats suffisamment satisfaisants de fiabilité et de robustesse car ils n'ont pas été développés pour des données de type surveillance.

1.4 Définition du problème

La DSNA souhaite donc protéger son système ATC contre les menaces croissantes qui peuvent être dirigées vers celui-ci. Néanmoins, à ce jour, elle ne dispose pas d'outils spécifiques qui soient en mesure de détecter les anomalies dans le trafic radar. Il est donc nécessaire de développer des mécanismes de détection d'anomalies dédié au trafic ASTERIX.

1.5 Méthodologie de réponse

Pour cela, Chandola et al. [13] nous indiquent qu'il existe deux approches principales : l'approche par signature et l'approche comportementale.

— L'approche par signature consiste à définir des scénarios d'attaque afin d'identifier des signatures dans les échanges de données. Cette approche nécessite de pouvoir connaître à l'avance les attaques redoutées, sinon leurs signatures seraient inconnues.

4. Le DICT est un indicateur concernant la Disponibilité, l'Intégrité, la Confidentialité et la Traçabilité

— L'approche comportementale est la capacité de construire un modèle de référence, dit "normal" du système surveillé et à le comparer avec le comportement observé. Les différences entre les deux déclenchent une alerte pour signaler une anomalie ou une intrusion potentielle. Cependant, il n'est pas facile de définir ce qui peut être représentatif du comportement normal d'un système, et donc ces méthodes génèrent souvent un grand nombre de faux positifs ou de faux négatifs.

Ces limites peuvent néanmoins être contournées lorsque les flux de données proviennent de réseaux spécifiques pour lesquels nous avons une bonne connaissance des caractéristiques du trafic échangé sur ce dernier. C'est particulièrement le cas pour les réseaux dont les échanges de données présentent un comportement reconnaissable dans le temps. Il est ainsi envisageable de proposer des techniques de détection des anomalies basées sur une connaissance du réseau pour repérer des événements potentiellement anormaux. Il est également possible de simuler des attaques et des anomalies afin de déterminer comment se comportera le réseau lors de cas réels.

Suite à cela, nous avons envisagé une approche auto-supervisée pour les données de l'aviation civile en couplant une approche comportementale par l'étude du comportement du réseau radar et une approche par signature en simulant des attaques redoutées par les experts de la navigation aérienne.

1.6 Réponse au besoin

Les travaux de cette thèse se sont donc placés dans le contexte présenté dans le chapitre 2, c'est-à-dire la nécessité d'assurer la sécurité du réseau ATC en développant de la détection d'anomalies spécifiques aux données transportées. En effet, les mécanismes de sécurité mis en place dans le réseau opérationnel ne permettent pas de prendre en compte le manque de sécurité du protocole radar.

Comme la littérature n'a pas encore beaucoup abordé le problème d'analyse du trafic radar ASTERIX, nous avons tout d'abord travaillé, dans le chapitre 4, sur cette analyse et sur le comportement des données radars à travers le temps afin de pouvoir dégager des caractéristiques reconnaissables que nous pouvons considérer comme normales. Cela nous a également permis de rapprocher la problématique de détection d'anomalies pour les données radars à celle pour les ICS.

Par la suite nous avons également travaillé sur le protocole en lui-même afin de proposer et tester des attaques redoutées par les opérationnels sur le système. En se basant sur celles-ci dans le chapitre 5 nous avons pu proposer et tester des mécanismes de détection d'anomalies. Pour cela, nous nous plaçons à deux niveaux, celui des flux radars et ce-

lui des traces des avions pour être en mesure de détecter ces attaques. La méthode de détection s'appuie sur les caractéristiques des données radars issues de l'analyse qui nous pousse à mettre en place une détection d'anomalies par prédiction de données. Pour cela, nous nous sommes appuyés sur des modèles de Machine Learning, Fbprophet, LSTM et auto-encodeur, traditionnellement utilisés pour la détection d'anomalies sur des séries temporelles comme les données radars. Cette méthode de détection d'anomalies nous permet de faire une ouverture de nos travaux vers la détection d'anomalies pour d'autres ICS et la caractérisation d'anomalies présentes dans le jeu de données opérationnelles en lien avec des experts du contrôle aérien dans le chapitre 6.

En se basant sur les prédictions, l'analyse du protocole et des attaques, nous sommes en mesure de proposer un système de détection d'anomalies prédictif dédié aux données de la surveillance aérienne capable de répondre aux attentes opérationnelles de la DSNA, en comparaison à d'autres mécanismes de détection d'anomalies.

1.7 Contributions

Les travaux de cette thèse ont permis trois contributions majeures dans le domaine radar pour l'aéronautique :

— Une caractérisation sur l'évolution temporelle des flux de données radars comme série temporelle. Grâce à cette caractérisation, nous avons identifié une signature qui se répète quotidiennement au niveau radar et la définition d'un trafic normal pour les données radars.

— Le développement d'une méthode de détection d'anomalies prédictives au niveau des flux radars et des traces des avions. Cette méthode, se basant sur les modèles Fbprohet, LSTM et autoencodeur, peut être élargie aux séries temporelles avec des attributs similaires aux données radars, telles que celles issues les ICS.

— La détection d'anomalies présentes sur un jeu de données opérationnelles de l'aviation civile.

La réalisation de ces travaux nous ont permis également deux avancées techniques dans le domaine des radars :

— La création d'un jeu de données radars du 19-04-2019 au 31-12-2020, issu du système opérationnel ATC français qui pourra être utilisé dans d'autres travaux tels que l'analyse plus approfondie sur le comportement des données radars ou l'impact de la Covid19 sur le trafic aérien.

— La création d'un outil d'injection de données radars, qui permet de forger ses propres données radars à partir de rien et donc de créer facilement des attaques,

pouvant modifier le système radar, dans le but de les étudier et s'en prémunir.

2 Contexte

2.1 Fonctionnement du système ATC

La Figure 2.1 représente schématiquement le fonctionnement d'un réseau opérationnel ATC. Le système de contrôle du trafic aérien est divisé en plusieurs entités :

— Le centre de régulation de la navigation aérienne (CRNA) chargé de fournir les services de la circulation aérienne aux aéronefs qui se trouvent en dehors de la proximité d'un aéroport. En France, il existe 5 CRNA, à Paris, Reims, Brest, Bordeaux et Aix.

— Les centres de contrôle d'approche chargés de fournir les services de la circulation aérienne autour d'un aéroport. Pour cela, ils utilisent TRACON avec notamment l'aide des radars.

Les radars sont répartis à travers tout le territoire afin d'avoir une couverture complète de l'espace aérien. Les secteurs de radars se coupent même afin d'être en mesure de recouper l'information.

Il existe plusieurs types de radars dans le système ATC français :

— Les radars primaires de surveillance (PSR) qui sont principalement utilisés pour le contrôle du trafic aérien militaire et pour les approches d'aéroport. Ce sont des capteurs radars classiques envoyant des ondes électromagnétiques dans un large espace réfléchies par les cibles à détecter. Ils présentent les avantages de ne nécessiter aucun équipement embarqué dans l'aéronef. Cependant ils ne permettent pas l'identification des cibles et leurs altitudes. Avec le PSR, on mesure : la distance entre le radar et la cible, l'angle en fonction de la position du radar et une vitesse radiale.

— Les radars secondaires de surveillance (SSR) qui sont le plus largement utilisés dans l'aviation civile, et donnent l'identification des pistes et la visualisation des vols pertinents. Parmi la variété des modes existants (A, B, C, etc.), le mode Sierra C permet une véritable liaison de données avec les avions, et transporte plus d'informations. Toutes les données peuvent être transmises à la fois de l'avion au sol et du sol à l'avion. Ces SSR ont plusieurs avantages : ils ne transmettent

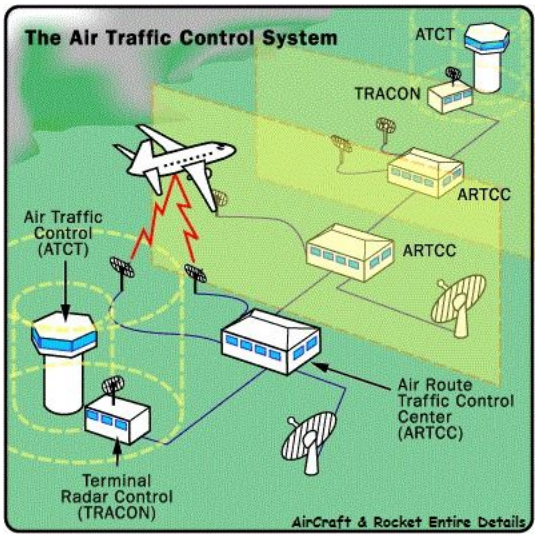


FIGURE 2.1 – Représentation schématique de la surveillance aérienne

que les plots pertinents (les obstacles n'apparaissent pas) représentant des avions et des informations supplémentaires (par rapport à la position et la vitesse radiale pour le PSR) envoyées par le transpondeur de l'avion en fonction du mode.

Les PSR et les SSR travaillent en redondance. A proximité des aéroports, il y a nécessairement la présence des deux pour s'assurer de ne pas manquer de détecter un aéronef. En revanche, sur l'ensemble du territoire, pour l'ATC, nous retrouvons principalement des SSR pour détecter les aéronefs.

Lorsqu'un avion est dans la zone de surveillance d'un radar, celui-ci le détecte en émettant des impulsions électromagnétiques qui vont soit lui renvoyer la présence de l'avion, soit questionner le transpondeur embarqué dans chaque avion. Le transpondeur répond avec les informations le concernant. Suivant le mode de fonctionnement, ces informations transmises peuvent être plus ou moins nombreuses et peuvent informer sur des données comme la position, l'heure, l'identifiant de vol, le niveau de vol. Le radar intègre ces informations dans un enregistrement et l'encapsule dans un paquet pour l'envoyer dans le réseau opérationnel présenté dans le schéma de la figure 1.2. Ce réseau achemine par le biais de nœud du réseau, les *Server Of Information* (SIR), les paquets avec les enregistrements jusqu'au Centre de Contrôle. Au sein de ces centres de contrôle, il existe un traqueur et un serveur de surveillance du trafic aérien (ARTAS). Celui-ci est un calculateur concaténant les enregistrements d'un avion provenant des différents radars, permettant ainsi de fournir une position précise de l'avion qui est appelé un plot

radar. Ce plot radar est envoyé au poste de contrôle où il est affiché sur l'écran radar du contrôleur semblable à celui de la figure 2.2. En recevant plusieurs plots dans le temps, nous avons ainsi la trace de l'avion qui représente sa position et sa trajectoire. A partir de ces données précises et des données issues des plans de vol, les contrôleurs sont en mesure de faire leurs contrôles.

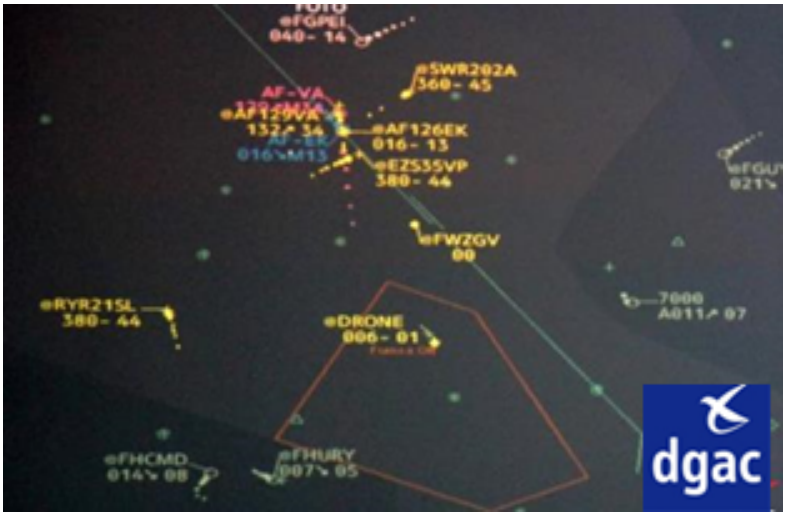


FIGURE 2.2 – Capture d'écran d'un système de visualisation IRMA de la DGAC

Lorsqu'un radar fonctionne, il émet deux types de messages :

— Les messages de détection qui contiennent les informations transmises par l'avion détaillées précédemment. Ces messages représentent donc la situation d'occupation du ciel en temps réel.

— Les messages de service qui vont être spécifiques au fonctionnement du radar et qui procurent des informations sur son état. Ces messages de service constituent notamment des informations pour indiquer le secteur que le radar est en train d'observer. Un radar observant sur 360 degrés est divisé en 32 secteurs de 11,25degrés. A chaque fois qu'il passe à un nouveau secteur, il envoie un message de service pour l'indiquer. Le temps de rotation d'un radar est d'environ 4 sec ; ainsi, toutes les 0,125 sec le radar envoie ce message de service.

2.2 Fonctionnement du protocole radar

Pour transmettre les données radars, les systèmes du réseau ATC utilisent le protocole open-source développé par Eurocontrol (l'organisation européenne pour la sûreté de

la navigation aérienne) qui est "STructured Eurocontrol suRveillance Information eXchange" ou ASTERIX. ASTERIX est un protocole utilisé pour la gestion du trafic aérien, mais il sert également pour des domaines militaires, météorologiques ou expérimentaux. Il permet de transmettre un échange d'informations structurées.

Les informations de l'avion envoyé par le transpondeur sont encapsulées dans un message Astérix. Ce protocole est conçu comme un protocole d'application du modèle TCP/IP qui permet d'avoir une transmission efficace et rapide du paquet avec une bande passante limitée pour répondre au besoin opérationnel du contrôle aérien. C'est pourquoi il suit des règles qui lui permet de transmettre toutes les informations nécessaires avec le plus petit *payload* possible.

La première version de ASTERIX a été approuvée par le RSSP, un panel de spécialistes sur les systèmes radars, en juillet 1986. Depuis, il a été adopté par le reste du monde aéronautique comme le standard pour les communications radars dans ce domaine [24].

En France, le réseau longue distance de la navigation arienne est un réseau à commutation par paquets de type X.25 qui sert à offrir un service de liaison longue distance aux systèmes de la navigation aérienne. Le réseau est également basé en local sur de l'ETHERNET. Les équipes de l'innovation de la DGAC travaillent actuellement au remplaçant du réseau en utilisant le protocole IP dans le but de pouvoir s'interconnecter avec les centres européens et apporter de nouvelles fonctionnalités. Par conséquent, le protocole ASTERIX est transporté soit par des paquets IP, soit par des trames ETHERNET. Pour une meilleure compréhension, nous parlerons par la suite de message ASTERIX ou de message radar.

Le type de données transmises par le protocole est normalisé par EUROCONTROL et défini suivant le type d'utilisation. Pour les différencier, on les classe suivant un identifiant que l'on nomme des catégories ASTERIX.

L'identificateur CAT définit la catégorie utilisée et nous permet d'identifier le type d'information transmise dans les enregistrements. Elles vont de 0 à 2255 :

— Les catégories 0 à 127 : pour les applications standard civile et militaire
— Les catégories 128 à 240 : pour les applications spéciales du domaine militaire
— Les catégories 241 à 255 : pour les applications non standard telles que les tests, la recherche, les expérimentations.

Pour le cas de l'ATC, seuls deux types de catégories correspondant au fonctionnement

des radars sont utilisés : les catégories de détection et les catégories de services. Les différentes catégories sont détaillées sur le site d'Eurocontrol [1]

Avec l'utilisation des PSR et des SSR, plusieurs catégories sont principalement utilisées pour l'ATC en France :

— Deux pour la détection : catégorie 01 pour PSR et 48 pour SSR.
— Deux pour les messages de service : catégorie 02 pour PSR et 34 pour SSR.
— La catégorie 30 et 255, en sortie des serveur ATC, après corrélation à la sortie des calculateurs pour l'affichage sur l'écran des contrôleurs.

Au sein de l'aviation civile, d'autres catégories existent mais ne concernent pas directement le flux de trafic aérien :

— La catégorie 08 : Les radars météo
— La catégorie 10 : Monosensor Surface Movement Data
— La catégorie 11 : SMGCS Data
— La catégorie 21 : Les données ADS-B
— La catégorie 32 : Des alertes sur le serveur ATC
— La catégorie 246 : Des requêtes sur des serveurs spécifiques
— La catégorie 00 : Synchronisation horaire
— La catégorie 03 : Distribution of synthetic Air Traffic Data
— La catégorie 17 : Mode S , fonction : surveillance/coordination
— La catégorie 18 : Mode S Data-link
— La catégorie 22 : TIS-B
— La catégorie 31 : SensorsInformation (biais)
— La catégorie 61 : SDPS Session and service control
— La catégorie 62 : Données du système de traqueur
— La catégorie 63 : SDPS status
— La catégorie 241 : Message technique RMCDE/S
— La catégorie 252 : Message de controle ARTAS
— La catégorie 253 : RemoteStation Monitoring (RMM/RDMS)
— La catégorie 254 : Information Up-line memorydump

Cependant, les catégories principales pour l'envoi des données radars aux contrôleurs et assurer les missions de l'ATC restent les 01,02,34,48,30 et 255.

Un message ASTERIX commence avec une adresse source multicast qui permet l'envoi du message sur tout le réseau. Vient ensuite l'adresse destination qui correspond à l'adresse du radar émettant le message.

1. https ://www.eurocontrol.int/services/asterix

Deux octets définissent ensuite la longueur du message. Vient ensuite la sous-couche de contrôle de la liaison logique (LLC) avec le DSAP et le SSAP qui sont à 28 pour les données radar et enfin un octet de commande.

Arrive ensuite le message en lui-même. La figure 2.3 - représente une vue d'ensemble du format d'un message ASTERIX ; la figure 2.4 détaille plus la composition d'un bloc de données ASTERIX.

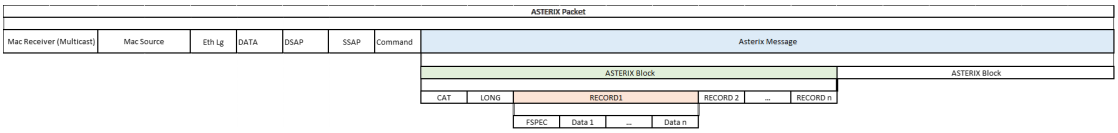


FIGURE 2.3 – Format d'un message ASTERIX

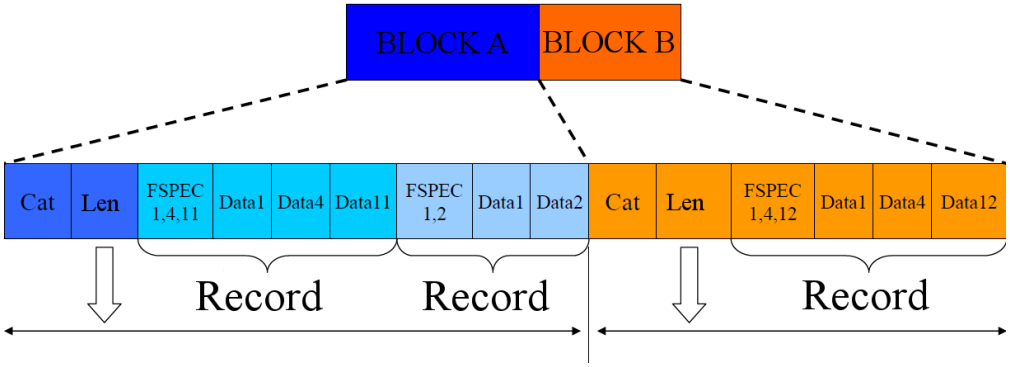


FIGURE 2.4 – Format d'un bloc ASTERIX

Un message ASTERIX est divisé en blocs, qui est la base du message, contenant chacun des informations propres. Un message ASTERIX peut contenir un ou plusieurs blocs. Le bloc change suivant le type de message : Service ou Détection.

Un bloc commence toujours par un octet spécifique, l'identificateur CAT. L'identificateur est codé de 00 à FF (en hexadécimal) ; après l'octet de catégorie, il y a 2 octets pour la longueur du bloc.

Au sein de chaque bloc, il y a plusieurs enregistrements qui vont contenir l'information pour chaque avion. Un enregistrement commence par un champ FSPEC (Field SPECification). Chaque bit du FSPEC indique la présence ou l'absence de la donnée du rang "i" pour la catégorie en cours. Il s'agit en quelque sorte de la table des matières ou le sommaire des données qui vont suivre.

Les données et leurs constructions sont définies par des documents standards fournis sur le site d'EUROCONTROL. On y retrouve l'ordre des données dans l'User Application Profile (UAP) 2.5 qui va permettre au FSPEC de nous communiquer les données présentes. Chaque champ de l'UAP décrit un Data Item. Ce Data Item décrit techniquement la manière dont donnée est écrite dans un message ASTERIX opérationnel. Ce sont ces Data Item qui vont contenir les informations de l'enregistrement de l'avion et qui de manière pratique vont être affichées sur l'écran du contrôleur.

Exemple de décodage d'un message de catégorie 1 sur de l'Ethernet La catégorie 1 collecte les informations issues des radars primaires et secondaires ; L'UAP de la catégorie 1 est défini dans le tableau 2.1

Table 2.1 – UAP de la catégorie 1

Octet1	8	7	6	5	4	3	2	1
	IDEN	ESC	UM	OSU	OSX	VIT	MODA	EXT
Octet 2	8	7	6	5	4	3	2	1
	MCD	PTU	LOT	UIS	OPP	IST	UAL	EXT
Octet 3	8	7	6	5	4	3	2	1
	OD2	QA	QC	Q2	WEC	SP	FS	EXT
Octet 4	8	7	6	5	4	3	2	1
	0	0	0	0	0	0	0	EXT

Une trame ETHERNET contenant un paquet ASTERIX a été capturée au sein du réseau opérationnel :

FD FF FF FF 08 02 00 80 02 00 00 15 00 92 34 34 03 01 00 83 **F7 84** 08 05 A8 01 A8 70 21 BD 88 09 09 26 68 00 89 85 50 68 **77 84** A8 00 21 68 BC B9 D4 08 1B A7 28 4D A0 45 C8 48 **77 84** A8 01 7D 57 A9 B8 70 08 0E FE 0E 0A E8 05 78 48 77 84 A8 00 88 48 3E ...

La première chose à faire est d'examiner le FSPEC . Dans ce message, le premier FSPEC vaut F7 84. Nous le retrouvons à la figure 2.6.

Nous pouvons ainsi voir que dans le premier enregistrement, nous aurons les champs : IDEN, DESC, NUM, POSU, VIT, MODA, MCD, PLOT et PIST.

La figure 2.7 nous présente donc les différents champs que nous retrouvons dans le message.

Le Champ IDEN se décompose en deux sous-champs très importants :

Table 2 - Standard UAP

FRN	Data Item	Data Item Description	Length in Octets
1	I048/010	Data Source Identifier	2
2	I048/140	Time-of-Day	3
3	I048/020	Target Report Descriptor	1+
4	I048/040	Measured Position in Slant Polar Coordinates	4
5	I048/070	Mode-3/A Code in Octal Representation	2
6	I048/090	Flight Level in Binary Representation	2
7	I048/130	Radar Plot Characteristics	1+1+
FX	n.a.	Field Extension Indicator	n.a.
8	I048/220	Aircraft Address	3
9	I048/240	Aircraft Identification	6
10	I048/250	Mode S MB Data	1+8*n
11	I048/161	Track Number	2
12	I048/042	Calculated Position in Cartesian Coordinates	4
13	I048/200	Calculated Track Velocity in Polar Representation	4
14	I048/170	Track Status	1+
FX	n.a.	Field Extension Indicator	n.a.
15	I048/210	Track Quality	4
16	I048/030	Warning/Error Conditions	1+
17	I048/080	Mode-3/A Code Confidence Indicator	2
18	I048/100	Mode-C Code and Confidence Indicator	4
19	I048/110	Height Measured by 3D Radar	2
20	I048/120	Radial Doppler Speed	1+
21	I048/230	Communications / ACAS Capability and Flight Status	2
FX	n.a.	Field Extension Indicator	n.a.
22	I048/260	ACAS Resolution Advisory Report	7
23	I048/055	Mode-1 Code in Octal Representation	1
24	I048/050	Mode-2 Code in Octal Representation	2
25	I048/065	Mode-1 Code Confidence Indicator	1
26	I048/060	Mode-2 Code Confidence Indicator	2
27	SP-Data Item	Special Purpose Field	1+1+
28	RE-Data Item	Reserved Expansion Field	1+1+
FX	n.a.	Field Extension Indicator	n.a.

FIGURE 2.5 – Exemple d'UAP pour la catégorie 48 fournis par EUROCONTROL

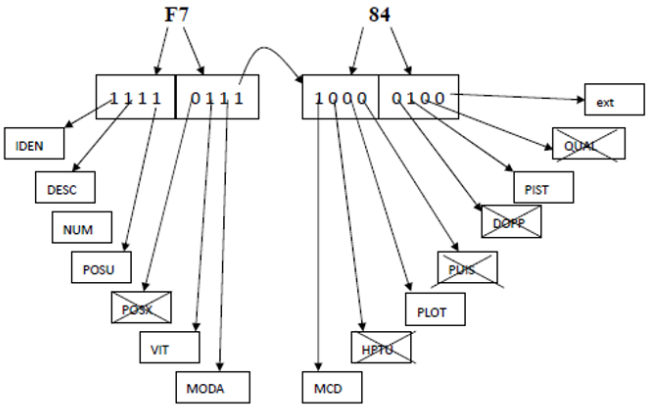


FIGURE 2.6 – FSPEC du message d'exemple

FD FF FF FF 08 02 @ MAC dest	**00 80 02 00 00 15** @ MAC source	**00 92** Long Ethernet	**34** SSAP	**34** DSAP

03 cmde	**01** CAT	**00 83** longueur	**F7 84** FSPEC	**08 05** SAC SIC	**A8** DESC

01 A8 N° piste	**70 21 BD 88** POSU	**09 09 26 68** VITESSE	**00 89** Mode A	**85 50** Mode C

68 Piste	**77 84** FSPEC suivant

A8 00 21 68 BC B9 D4 08 1B A7 28 4D A0 45 C8 48 77 84 A8 01 7D 57 A9 B8 70 08 0E
FE 0E 0A E8 05 78 48 *77 84* **A8** 00 88 48 .....

FIGURE 2.7 – Détail de l'enregistrement de l'exemple

— Le SAC, Source Area Code qui définit l'origine géographique de l'émetteur (0x08 pour la France)
— Le SIC, Source Identification Code (numéro du radar source (0 à 255). Ce numéro est européen.)

En détaillant ces champs, nous obtenons ainsi les informations transmises par l'enregistrement dont la description figure dans le tableau 2.2.

TABLE 2.2 – Détails des informations contenues dans le premier enregistrement de l'exemple

Champ	Données	commentaires
SAC SIC	08 05	Monopulse Mont Ventoux
DESC	A8	Piste,vraie,secondaire,TPR2,pas SPI,non transpondeur fixe
N° piste	01 A8	Piste n° 424
POSU	70 21 BD 88	Rho=224 Nm(7021), Théta=266°(BD88)
Vitesse	09 09 26 68	Vitesse=508Kts ou 0,14 Nm/s (0909) ; cap=54 ° (2668)
Mode A	00 89	Mode A valide, pas de garbling, mode A brut, mode A= 1120
Mode C	85 50	Mode C valide,pas de garbling, FL=340
Piste	68	Piste confirmée, radar sec, avion en manoeuvre

2.3 Etat de sécurité de l'ATC

Jusqu'à ce jour, comme le système ATC était considéré comme fermé avec des systèmes propriétaires, il était bien protégé des cybers attaques. Néanmoins, le risque sur ce système est accru à cause de plusieurs facteurs :

— L'augmentation de l'utilisation de l'automatisation et de l'utilisation de système numérique.
— Le besoin croissant d'interopérabilité entre les systèmes.
— L'utilisation de composants communs sur le marché et des normes ouvertes.
— Le mélange d'anciens et de nouveaux systèmes.
— L'ouverture à de nouveaux utilisateurs.
— La montée en capacité des attaquants potentiels.

Les cibles d'attaque, quant à elles, sont nombreuses [1] ; autant des attaques sur la liaison de données que sur des équipements de communication aux liaisons permettant d'assurer la gestion de la circulation aérienne.

Nous pouvons néanmoins distinguer deux profils d'attaquants :

— Les *insiders* : qui sont présents au sein du système et qui possèdent un accès relativement facile aux données.
— Les *outsiders* : qui sont en dehors du système.

Bien que la catégorie des *insiders* soit la plus menaçante du fait de leurs accès, le danger reste minime puisqu'il s'agit principalement de motivation de vengeance de la part d'employés.

En ce qui concerne les *outsiders* les motivations sont différentes :

— Les pirates informatiques qui d'une part peuvent chercher à pénétrer le système pour découvrir les failles et se faire rémunérer pour ça (*white hat*), d'autre part peuvent exploiter les vulnérabilités pour soutirer de l'argent de manière illégalle (*black hat*). Leur dangerosité dépend de leur niveau de compétences et et des accès qu'ils réussissent à obtenir.

— Les cybercriminels agissant la plupart du temps comme une bande organisée qui sont motivés par le gain financier. Ils peuvent soit être engagés comme mercenaires dans le but d'affaiblir la concurrence, soit lancer des attaques afin d'exprimer une opinion politique, environnementale, etc ... ce sont les *hacktivists*. Ces profils d'attaquants sont particulièrement dangereux, notamment pour l'aviation civile, car ils recherchent le maximum de nuisances.

— La catégorie la plus dangereuse, les "cyber guerriers" présents dans certains pays disposant de moyens financiers importants et utilisant le monde cyber comme un terrain d'attaque et une arme potentielle pour déstabiliser un pays. Une variante de cette catégorie sont les "cyber terroristes" qui recherchent à provoquer des accidents ou des incidents graves. L'espace aérien et le milieu aéronautique étant un OIV avec un risque humain important, il s'agit d'une cible potentielle pour ces attaquants.

Les capteurs de surveillance et le réseau de surveillance sont donc fondamentaux pour assurer la sûreté de l'espace aérien [23]. Une attaque sur le système ATC a un risque humain important et peut être une cible d'attaque prioritaire. Il faut considérer le risque le plus important et assurer la sécurité en fonction de ce risque.

Parmi les attaques redoutées, cinq évènements le sont particulièrement [1] :

— collision avec le sol
— perte de contrôle en vol
— collision en vol
— collision sur piste
— sortie de piste à atterrissage ou au décollage (Runway Excursion)

Les conséquences d'une attaque sur le système peuvent être graves et imprévisibles, d'autant plus que l'espace aérien est un système complexe. Les attaques envisagées sont assez difficiles à mettre en œuvre, elles nécessitent un équipement spécialisé et une connaissance des systèmes, mais sont plausibles pour un attaquant déterminé. Un

attaquant se plaçant sur le réseau ne peut pas directement contrôler un avion dans des montées ou des descentes arbitraires. Il va devoir mener des actions sur les plots radars pour amener le contrôleur à mener les avions dans des situations dangereuses, en les dirigeant par exemple dans des espaces aériens occupés par d'autres aéronefs et à les rapprocher entre eux en déviant leur trajectoire, augmentant ainsi le risque de collisions.

Ces événements sont particulièrement plausibles lorsque nous modifions les données radars et que le contrôleur donne des indications erronées à l'aéronef. C'est pourquoi par la suite nous prendrons en compte des attaques permettant de recréer ce type d'événements.

Le protocole ASTERIX, transportant les messages radars, n'est pas implicitement sécurisé en lui même. La sécurité dépend de la couche de transport. Comme indiqué précédemment, il existe même une preuve de concept qui exploite ce manque de sécurité [11]. Les auteurs ont développé un logiciel "MITMAST" (Man In The Middle ASTERIX) qui utilise une technique d'attaque classique "d'Empoisonnement ARP" entre deux utilisateurs pour permettre de manipuler les données radars.

Pour pallier à ce manque de sécurité du protocole, les ANSP, qui ont une obligation légale d'assurer la sécurité de la donnée transportée, ont mis en place des barrières physiques et logiques pour isoler la donnée et la transporter dans des canaux sécurisés [45] ce qui protège notamment des attaques extérieures. Il existe donc bien entendu des sécurités mises en place par la séparation des réseaux, des règles de firewall spécifiques ainsi que des vérifications de sécurité appliquées sur les réseaux informatiques. Cependant, ces règles-là ne prennent pas en compte l'éventuelle modification des données radars. Si un paquet est bien construit avec une source connue, il n'est pas filtré. De plus, à l'intérieur des centres ATC, les données sont transportées sur des réseaux locaux séparés non chiffrés. Par conséquent, des attaques ou une mauvaise manipulation des données à l'intérieur des centres peuvent avoir un impact significatif sur le système. Même si une sécurité est assurée au niveau protocole réseau, les potentiels attaquants exploitent les failles de ces protocoles. Il est donc nécessaire d'avoir un mécanisme de sécurité supplémentaire et de détecter les anomalies pouvant subvenir sur le réseau.

Les efforts doivent être ainsi effectués pour assurer le maximum de disponibilité et de sécurité pour ASTERIX. Dans le rapport de Janvcik et al. [45], des recommandations en terme d'authentification, d'intégrité et de confidentialité du protocole ASTERIX sont proposées afin d'assurer un niveau de sécurité nécessaire au maintien opérationnel. Les solutions envisagées sont l'ajout de chiffrage ou de marquage du message radar pour en assurer une identité unique et la non modification de celui-ci. Néanmoins il est nécessaire de s'assurer que les implémentations des solutions proposées puissent être compatibles

avec les versions des systèmes utilisés par chaque ANSP.

Une autre faille majeure en terme de sécurité pour le système ATC est le manque de sécurité par rapport au calculateur concaténant les données radars dans les centres de contrôle, le système ARTAS. Tout comme ASTERIX, ARTAS a été développé dans les années 1990. Les exigences de sécurité étaient alors moins importantes. Le système a même été développé pour retirer certaines défenses afin de laisser plus de liberté à l'opérateur et réduire le temps de réaction en cas de problème de suivi de trace [45].

En 2017, le système ARTAS a fait l'objet d'une évaluation de sécurité et des scénario d'attaques en sont ressortis :

— Le premier est une attaque sur le système opérationnel en compromettant le système ARTAS par de multiples vulnérabilités. Bien que celles-ci soient connues, elles ont été conservées pour faciliter l'utilisation de l'opérateur et les solutions d'isolement du système ont été préférées.
— Le deuxième est une attaque directe sur l'application en envoyant des données érronées pour générer des exceptions et faire planter ARTAS. Même si lors de cette évaluation le systèmeARTAS a resisté à ce scénario, on peut toujours envisager d'utiliser le principe pour tenter d'autres attaques, en essayant notamment de faire un empoisonnement ("*poisoning*" : envoyer de fausses informations) ou un "*flooding*" (saturer le système de message pour le faire planter).
— Le troisième en utilisant directement les failles du protocole ASTERIX pour se faire passer pour un radar ou un utilisateur existant et modifier des messages légitimes après le système ARTAS. Il est ainsi possible de faire disparaître des plots radars, et d'en faire apparaître [18].

Le sujet des améliorations en terme de sécurité dans l'ATC est un sujet actuel et de plus en plus préoccupant [58], [19], [39]. De nombreux systèmes de traitement de données aéronautiques, comme ARTAS, n'ont pas pris en compte la cyber sécurité dès la conception, ce qui fait que l'on se retrouve avec des failles majeures en terme de sécurité dûes notamment au protocole de transport de données radars.

Il est vrai que le protocole ASTERIX est amené à être remplacé en partie par le protocole ADS-B (Automatic Dependent Surveillance Broadcast), non mis en place en France pour le moment, pour décongestionner certains canaux de communication. L'ADS-B est plus indépendant qu'ASTERIX et permet un fonctionnement plus simple des radars sans interroger en permanence le transpondeur de l'avion [65]. Cependant, le protocole

ADS-B présente également des failles importantes de sécurité et des vulnérabilités qui sont exploitables par des attaquants.

2.4 Travaux précédents dans l'ATC

Dans la littérature, nous trouvons peu de travaux sur les données radar et le protocole ASTERIX en lui-même.

Nous pouvons trouver les normes développées par l'autorité de contrôle Eurocontrol sur leur site [2]. Ils y présentent le protocole lui-même et sa spécification.

Dans le domaine ATC, les recherches les plus nombreuses se sont davantage concentrées sur le retard ou la trajectoire du trafic aérien [8] en utilisant des données radars, que sur le transport de messages radars par le réseau informatique en lui-même et sur la détection d'anomalies au sein du système ATC.

Les travaux portant sur la détection d'anomalies à partir des données radars dans le domaine aéronautique utilisent des méthodes basées sur l'apprentissage automatique. Celles-ci permettent d'identifier des comportements anormaux principalement concentrés sur la trajectoire des avions. Cependant, ces travaux ne prennent pas en compte le protocole radar en lui-même et son comportement sur le réseau.

— Gariel et al. [33] ont appliqué des techniques de regroupement de trajectoires avec les traces radar afin d'identifier les comportements opérationnels des avions et leur variabilité.
— Conde et al. [17] eux ont développé des travaux sur la caractérisation des flux de trafic aérien afin d'identifier les trajectoires des aéronefs et pouvoir détecter les comportements non conformes en vol.
— Evans et al. [27] quant à eux, ont appliqué diverses techniques d'exploration de données à celles de plan de vol pour entrainer un prédicteur de réorientation des avions en vol.

C'est pourquoi lors de ce travail, nous avons souhaité aller au-delà de la position des avions et de la trajectoire des aéronefs, afin de développer une méthode permettant de faire de la détection d'anomalies pour la donnée radar au sens global de ce qu'elle peut transmettre.

En ce qui concerne les données ASTERIX, il y a peu de travail sur la détection des

2. https ://www.eurocontrol.int/services/asterix

anomalies en elle-même. Dans sa thèse, Nanduri [57] traite de ce type de détection d'anomalies, comme de la détection de vols atypiques et d'anomalies basées sur des signatures statistiques ou de la détection d'anomalies dans les données dans l'espace vectoriel. Plus récemment, [46] traite de la détection d'anomalies en ce qui concerne les approches des aéronefs au niveau des aéroports en faisant de l'analyse de différents composants pour détecter des variations d'énergie, permettre une optimisation des approches et assurer la sûreté des avions. Dans leur rapport technique intitulé "Using "ASTERIX" in accident investigation" [29], Farrel et Schuurman expliquent que les données radars sont souvent utilisées pour les enquêtes sur les accidents aériens, et utilisent les données ASTERIX pour des raisons de sûreté dans le cadre de l'analyse d'accidents. Néanmoins, Casanovas et al. [11] présentent une validation de principe sur la vulnérabilité du protocole ASTERIX. Ils ont pu mettre en place une attaque *Man In the Middle* consacrée à ce type de trafic dans le but de supprimer, modifier ou ajouter des avions à l'intérieur du trafic. Cette étude souligne la nécessité d'avoir un niveau de sécurité supplémentaire pour ce protocole contre une attaque survenue depuis l'intérieur du réseau.

Ainsi, les données ASTERIX sont peu étudiées en elles-mêmes, cependant cela n'est pas étonnant puisqu'il s'agit d'un protocole à usage spécifique comme les protocoles industriels. c'est pourquoi, dans un premier temps, nous avons articulé notre travail autour de l'étude des comportements des données radars.

De ce que l'on a pu voir, nos travaux correspondent à la première étude d'une caractérisation du trafic réseau ATC radar qui se concentre sur le protocole et qui identifie des caractéristiques sur ces données. Ces caractéristiques permettent de développer un module de détection d'anomalies dédié au protocole ASTERIX.

Notre travail porte donc sur le protocole ASTERIX avec la mise en place d'un système de détection d'anomalies pour être en mesure de se prémunir d'attaques sur le système ATC en lui-même.

2.5 Conclusion

Dans ce chapitre, nous avons explicité le contexte aéronautique pour le contrôle aérien. Étant donné que le système ATC est à la base de ce contrôle aérien, son bon fonctionnement doit être assuré. Suite à une évolution récente de ce système et son interconnexion avec des réseaux informatiques plus classiques, de nouvelles menaces de sécurité apparaissent. Bien que des mécanismes de sécurité existent au sein du système, la particularité

de l'ATC d'avoir un protocole spécifique traitant des séries temporelles de radars non étudiées pour le moment, ne permet pas de transposer des mesures de sécurité classiques des systèmes informatiques. Nous avons donc identifié la nécessité de mettre en place des mesures de sécurité pertinente, comme la détection d'anomalie pour les données radars. Cette mesure s'est justifié par la discussion des mécanismes d'attaques récents sur le protocole qui permet de transporter les données radars. Dans le chapitre suivant, nous explorons l'état de l'art en matière de détection d'anomalies pour les données radars qui se présentent comme des séries temporelles.

3 Travaux Connexes

Ce chapitre définit ce qu'est une anomalie et fournit un état de l'art sur la détection d'anomalies pour les séries temporelles.

Lors de l'analyse d'un jeu de données issues de milieu opérationnel, nous constatons qu'un besoin commun est de déterminer quelles instances se démarquent comme étant différentes de toutes les autres afin de pouvoir dire ce qu'on considère comme un trafic normal. Dans la littérature sur l'exploration des données et les statistiques [2], ces instances sont appelées anomalies ou valeurs aberrantes. Les anomalies peuvent être causées par des erreurs de données, mais sont parfois illustratives d'un nouveau processus sous-jacent, auparavant inconnu. Ces processus sont généralement la cause d'une attaque qui peut avoir lieu sur le système lui-même.

La détection d'anomalies fait référence au problème de la recherche de modèle dans des données qui ne se conforment pas à un comportement attendu [13]. Le but de la détection d'anomalies est donc d'évaluer la distance entre les données collectées sur un système réel et un comportement standard que l'on peut qualifier de référence. On utilise la détection d'anomalies comme méthode de défense depuis des années dans les réseaux afin de détecter des intrusions et se protéger d'attaques [3].

3.1 La détection d'anomalies

La détection d'anomalies est un contrôle de sécurité réactif ou a posteriori qui cherche à identifier automatiquement les violations de la politique de sécurité d'un système surveillé. Ensuite, grâce à une méthode de détection, l'IDS détecte la présence d'une intrusion et déclenche une alerte. Les IDS peuvent être classés en fonction du type de source de données et de la méthode de détection [20].

Comme vu dans le chapitre 1, il existe deux méthodes de détection d'anomalies : par signature et par comportement.

L'approche basée sur le comportement permet la détection d'éventuels écarts par rapport à un comportement normal. Le principal avantage de ces approches est leur capacité théorique à détecter des attaques inconnues. Cependant, la difficulté réside dans le fait représenter de manière exhaustive le comportement normal d'un système qui peut être complexe. Ces approches ont donc tendance à générer une quantité importante de fausses alertes [32].
Pour les approches par la signature, le principe repose en la création d'une base de connaissances sur les comportements anormaux et la reconnaissance de celles-ci dans le trafic. Les méthodes utilisant cette approche utilisent des algorithmes de correspondance pour reconnaitre ces signatures. Cette approche présente l'avantage de générer moins de fausses alertes, mais l'inconvénient de devoir connaître les signatures des attaques. Par conséquent, elles présentent moins de chances de détecter de nouveaux types d'anomalies.

Ces méthodes de détection dépendent du jeu de données et de la connaissance ou non que l'on a sur ces jeux de données et leurs anomalies potentielles. En effet, dans leur survey [13], Chandola et al. nous indique que la détection d'anomalies peut se baser sur des méthodes avec des algorithmes de Machine Learning supervisés, non-supervisés et semi-supervisés et plus récemment grâce à une sous-classe des algorithmes non-supervisés, les méthode auto-supervisées [47].

Les techniques non supervisées sont basées sur des jeux de données non étiquetés et supposent que les données d'entraînement incluent à la fois des données anormales et non anormales.

Les méthodes supervisées nécessitent des jeux de données avec des anomalies étiquetées pour les prédire, tandis que la méthode semi-supervisée recquiert une combinaison de données étiquetées et non étiquetées et est requise dans les cas où les données étiquetées sont insuffisantes. Cependant, dans la plupart des domaines, les jeux de données étiquetées ne sont pas facilement disponibles.

La méthode avec une approche auto-supervisée reproduit les données d'entrée de manière probabiliste à travers un modèle ; la cible est l'échantillon d'entrée. Nous avons donc une méthode supervisée puisque l'apprentissage se fait avec une variable cible mais que le jeu de données n'est pas étiqueté. Un exemple de technique auto-supervisée est la méthode d'auto-encodeur, que nous développons dans la section 3.4.

Du fait que nous nous basions sur un jeu de données opérationelles, les travaux de cette thèse utiliseront des techniques auto-supervisées, le jeu de données n'étant pas labelisé.

Des algorithmes traditionnels pour la détection d'anomalies Dans son étude [34], Goldstein et al. nous détaille un certain nombre d'algorithmes non supervisés qui peuvent être utilisés pour des données multivariées. Nous en sélectionnons trois reprenant trois familles de modèles qui peuvent être adaptés pour faire de la détection d'anomalies avec les contraintes des données radars, des données critiques, en temps réel, traitant de séries temporelles. Pour ce faire, nous choisissons :

— Modèle linéaire : "One-Class Support Vector Machine" (OC-SVM) [61] [75]
— Modèle de Proximité : "Local Outlier Factor" (LOF) [9] [37]
— Techniques d'ensemble : "Isolation Forest" (IF) [51] [21]

Nous détaillons ces algorithmes à la sous-section 5.4.4.

Evaluation de la performance des systèmes de détection d'anomalies La performance d'un système de détection d'anomalies peut être évaluée sur la base des :

— Vrais positifs (TP) qui correspondent à des anomalies correctement identifiées,
— Faux positifs (FP) qui correspondent à un comportement normal identifié comme malveillant,
— Vrais négatifs (VN) qui correspondent au rejet correct d'un comportement normal,
— Faux négatifs (FN) qui correspondent à des anomalies non identifiées ;

Nous pouvons ainsi définir deux métriques qui mesurent les performances d'un mécanisme de détection d'anomalies :

— Le taux de vrais positifs (égal à 1 si pas de faux négatif) qui mesure la sensibilité du système

$$Tauxdevraipositif = TP/(TP + FN)$$

— Le taux de faux positifs (égal à 0 si pas de faux positifs) qui mesure la spécificité du système

$$Tauxdefauxpositif = FP/(FP + TN)$$

Ainsi, un système de détection efficace consiste à avoir un taux de vrais positifs proche de 1 et un taux de faux positifs proche de 0.

3.2 La détection d'anomalies pour les séries temporelles

Une approche pour la détection des anomalies temporelles a été de construire des modèles de prédiction et de mesurer la différence entre les valeurs prédites et les valeurs réelles, donnant ainsi un score d'anomalie [37].

En effet, la prédiction de séries temporelles est liée à la détection des anomalies, car les anomalies sont des points ou des séquences qui s'écartent des valeurs attendues [71]. Plusieurs modèles ont été proposés par la suite dans la littérature statistique, notamment la moyenne mobile autorégressive (ARMA), la moyenne mobile intégrée autorégressive (ARIMA), la moyenne mobile pondérée de façon exponentielle, etc. ...Tous ces modèles se basent sur une étude et une détection *d'outlier* statistique, par le biais notamment de mesures de moyennes, de valeurs extrêmes et de seuils. Les modèles ARIMA sont particulièrement populaires en raison de leur capacité à lisser les moyennes mobiles pour éliminer le bruit et à l'inclusion de termes qui expriment la dérive, le bruit et la non-stationnarité dans le temps. Les anomalies ponctuelles au sein de points de données consécutives sont facilement identifiées.

Une méthode statistique efficace présentée est une méthode auto-supervisée se basant sur des données issues d'un pattern normal. Ces méthodes se montrent efficace avec des données statiques qui ont un pattern identifiable. De nombreuses méthodes ont été mises en place pour faire cette prédiction :

- L'utilisation d'une approche sur "fenêtre" en calculant la médiane des valeurs récentes comme valeurs prédites et en déterminant un seuil de détection.
- L'utilisation de modèles autorégressifs multivariés pour prédire la prochaine mesure dans le flux de données [69].
- L'utilisation de réseaux de neurones artificiels nécessitant une bonne connaissance des données pour les classes anormales ou non [28] [56].
- L'utilisation de score de confiance pour chaque prédiction [52]
- L'utilisation de méthodes de prédiction évolutive, dans lesquelles les paramètres ou les composants du modèle sont mis à jour au fur et à mesure au cours de l'arrivée de nouvelles données, et ce afin de mieux saisir les tendances normales des données. A partir de cette tendance normale, nous sommes en mesure de définir des seuils et des scores d'anomalies basés sur des mesures de distance entre deux points qui nous permettent d'identifier des anomalies dans les données prédites [73].
- L'utilisation des réseaux neuronaux récurrents (RNN) [54].

Parmi tous ces modèles de prédiction pour les séries temporelles, la méthode par réseaux neuronaux récurrents permet d'avoir des résultats efficaces. Nous décrivons davantage la problématique dans la détection d'anomalies pour les ICS 3.4 et la méthode dans 5.2.2.

3.3 La détection d'anomalies dans le domaine aéronautique

Si nous prenons le cas des données radars, un attaquant peut continuellement modifier l'information sur la position de l'aéronef donnée par le message radar, comme c'est le cas pour une attaque par *spoofing* "*bubbling*" [12]. Le système de surveillance radar aura des difficultés à détecter les différences subtiles, ce qui entraînera de mauvaises indications de la part des contrôleurs de la circulation aérienne ou des retards dans l'intervention du système d'évitement des collisions, ce qui pourrait être un véritable danger pour des vies humaines.

Peu d'études publiées ont appliqué les techniques de détections des anomalies RNN au domaine du trafic aérien, la plupart s'étant concentrées sur de la détection d'anomalies statistiques. Tanner et Strohmeier [67] utilisent le réseau OpenSky pour détecter les anomalies dans les modèles de trafic aérien et l'utilisation des pistes. D'autres études utilisent des données satellitaires visuelles combinées au réseau OpenSky pour construire un ensemble de données de détections d'anomalies de vol [49].

3.4 Les travaux relatifs aux ICS

L'analyse que nous menons dans le chapitre 4 nous permet de rapprocher la problématique de détection d'anomalies des données ATC à celles issues des ICS.

Un Système de Contrôle Industriel (ICS) est un terme utilisé pour décrire différents types de systèmes de contrôle et d'instrumentation qui comprennent des dispositifs qui vont être utilisés pour faire fonctionner un processus industriel et ainsi fournir des services ou exécuter des taches de fabrication complexe [63]. Par définition, il s'agit d'une combinaison de composants de contrôle (électriques , mécaniques , hydrauliques , pneumatiques , etc.) qui agissent ensemble pour atteindre un objectif industriel (fabrication, transport de matière et d' énergie , etc.). De fait, le terme ICS englobe une large dénomination comprenant plusieurs types de systèmes tels que SCADA (Supervision Control And Data Acquisition), DCS (Distributed Control System), IACS (Industrial

Automation and Control Systems) ou PCS (Process Control System).

Une des particularités des ICS est que les systèmes se basent sur des données qui sont au cœur de leur système et qui transportent des informations critiques pour le système opérationnel. De plus, les données issues des ICS présentent la singularité d'avoir une signature prédictible et régulière dans le temps [30] pour faire fonctionner le système.

Par ce biais, nous pouvons considérer que les données réseaux radars, étant au cœur du système ATC, avec une haute criticité, fonctionnant avec un protocole qui lui est propre et présentant une signature se répétant dans le temps, peuvent être assimilés à des données d'ICS.

3.4.1 La sécurité dans les ICS

Les propriétés apportées par la sécurité des systèmes d'informations changent des systèmes informatiques de par la particularité des ICS . On constate une inversion entre les systèmes informatiques et les ICS. Traditionnellement, les propriétés de sécurité souhaitées pour les systèmes informatiques sont, par ordre d'importance, la confidentialité, l'intégrité et la disponibilité. Dans les ICS, l'ordre est inversé en privilégiant la disponibilité, suivi par l'intégrité et la confidentialité [10].

- La confidentialité fait référence à la non-divulgation d'informations à des personnes ou des systèmes non autorisés. Dans les ICS, cela revient à protéger :
  - Les données relatives aux performances, à la planification et à la mise en place des opérations
  - Les échanges de données entre les composants d'instrumentation au niveau terrain, et les automates au niveau contrôle [10]
- L'intégrité est la prévention de toute modification ou destruction d'informations par des personnes ou des systèmes non autorisés. Pour les ICS, nous cherchons à protéger l'intégrité des données envoyées par les capteurs ou l'intégrité des commandes. [10]
- La disponibilité est ce qui permet aux personnes ou aux systèmes autorisés d'accéder à tout moment aux services ou aux ressources proposés par le système. Pour les ICS, la disponibilité est particulièrement importante pour faire fonctionner le système.

Pour répondre à ces propriétés, il faut mettre en place des mesures de sécurité dans les ICS. Pour cela, il est important de s'assurer à ne pas perturber le fonctionnement normal du système. Les contrôles de sécurité ne doivent pas introduire de latences temporelles susceptibles de perturber les boucles de contrôle, et doivent également être compatibles

avec les ressources de calcul et de mémoire limitées des composants ICS.

Traditionnellement, les ICS sont considérés pour être un bien protégé par une séparation « air-gapped », c'est-à-dire que l'on considère ces systèmes comme isolés et donc protégés. En effet, en raison de leur criticité élevée et de l'importance de leur fonctionnement face au processus industriel, les ICS sont généralement installés sur des réseaux privés opérationnels, indépendamment de tout autre réseau administratif, censés être isolés de tout accès depuis l'extérieur. Il n'est donc pas courant de développer pour ce type de système des IDS dédiés.

Cependant, il existe de plus en plus de passerelles entre les réseaux ICS et d'autres réseaux qui sont considérés comme plus ouverts et donc potentiellement ciblés par des attaques externes ou internes. Comme pour le système ATC, cette évolution vers une meilleure interconnexion entre réseaux rend donc les systèmes ICS potentiellement vulnérables aux attaques cyber.

Selon la ICS-CERT (ICS Cyber Emergency Response équipe, une équipe de la Cybersecurity and Infrastructure Security Agency (CISA), une agence fédérale américaine), les attaques ciblées sur les ICS ont augmenté au cours des dernières années. En 2015 [1], 295 incidents ont été signalés à l' ICS-CERT par rapport à 73 en 2013 [2]. Par conséquent, il est nécessaire de contrecarrer cette tendance.

Le NIST (National Institute of Standards and Technology) fait l'état des lieux des principales préaoccupations en terme de sécurité pour les ICS modernes [3] :

— Des protocoles de communication propres au système et non sécurisés par construction [25] ;
— Une séparation de réseau non sécurisée et des problèmes de contrôle d'accès [59] ;
— L'absence de pare-feu et d'IDS spécifiques aux ICS [70].

En ce qui concerne la DGAC et le réseau ATC, le dernier point n'est pas comparable ; il y a de plus en plus d'IDS, de pare-feux et de services de contrôle d'accès. Cependant, la problématique reste similaire avec les deux premiers points.

1. https://us-cert.cisa.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf
2. https://us-cert.cisa.gov/sites/default/files/Annual_Reports/Year_In_Review_FY2013_Final.pdf
3. https://us-cert.cisa.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf

3.4.2 Détection d'anomalies pour les ICS

Le document de survey [76] présente les difficultés à développer une détection d'anomalies spécifique au système comme celui de l'ATC, les ICS et en particulier le SCADA, car ils peuvent avoir des ressources limitées, des composants non sécurisés ou anciens, et de fortes exigences de disponibilité. Ils définissent les approches existantes telles que les approches basées sur le savoir, le comportement ou les approches hybrides. Steven Chung présente dans son article [14] l'un des premiers IDS pour SCADA construisant des modèles utilisés pour étudiés le comportement normal du système basé sur des mesures statistiques à destination d'un protocole de communication spécifique. Une autre approche, proche d'une approche conventionnelle, est basée sur une méthode supervisée avec des anomalies connues [64] et construit ainsi des comportements normaux au fil du temps en corrélant les différentes anomalies. Ces méthodes sont donc basées à la fois sur le système et leurs connaissances. Elles présentent l'avantage de donner des résultats efficaces. Néanmoins, elles nécessitent la possession d'un jeu de données avec des anomalies identifiées et une bonne connaissance sur le comportement des ICS, ce qui est rarement le cas pour ce type de données.

Afin de pallier cette mauvaise connaissance des données, des techniques basées sur des méthodes d'apprentissage automatique (Machine Learning) sont utilisées.

Basés sur les données disponibles et les anomalies identifiées ou non, des modèles de prédiction créent des profils du comportement normal du réseau ICS. La détection des anomalies se fait ensuite en calculant la distance du trafic avec les profils normaux. De telles approches sont prometteuses dans les ICS en raison de la dynamique de réseau relativement plus simple en terme de topologies fixes, de population limitée d'utilisateurs et de modèles de communication réguliers [10].

Il existe de nombreux choix pour la partie prédiction de données : Les auteurs dans [43] présentent des méthodes qui sont régulièrement utilisées pour de nombreuses tâches telles que la prédiction de données sur des séries temporelles. Nous pouvons citer notamment la prédiction basée sur une moyenne mobile intégrée autorégressive ARIMA, ou alors sur un SVM (Support Vector Machine), ou bien encore sur un réseau de mémoire à long terme (LSTM .

En particulier, le réseau LSTM-AD (Long Short Term Memory networks for Anomaly Detection) est utilisé principalement comme modèle de prédiction dans des séries temporelles telles que les ECG (électrocardiogramme) via des réseaux de mémoire à long terme profonds où la probabilité d'erreur de prédiction est utilisée pour mesurer les ano-

malies [68].

Compte tenu de la capacité d'apprentissage à long terme des LSTM, leur utilisation fréquente et leur capacité d'apprendre des situations inconnues font que ces réseaux sont de bons candidats pour résoudre les problèmes de détection d'anomalies pour les séries temporelles telles que celles présentes dans les ICS [54] [30].

Dans [54], nous voyons bien que chaque prédiction par le modèle LSTM se fait à partir des événements passés. On y teste le modèle sur quatre jeux de données, notamment sur des données de séries temporelles issues d'électrocardiogrammes ; il en résulte des scores de précision et de rappel qui encouragent l'utilisation de ce RNN LSTM pour la détection d'anomalies sur les séries temporelles avec une dépendance à long terme comme cela est fait dans [7] pour la sécurité des réseaux informatiques sur le jeu de données KDD 1999.

Les modèles LSTM Encoder-Decodeur ou "autoencodeur" sont présentés comme une extension naturelle des modèles LSTM pour des séries temporelles, tout en offrant de meilleures capacité d'apprentissages [66]. Ils ont récemment été utilisés pour de la détection d'anomalies dans des données multi-capteurs [53], permettant ainsi la détection d'anomalies sur des données prédictibles ou sur celles qui le sont difficilement, telles que l'évolution de la température du liquide de refroidissement sur un moteur.

Les LSTM sont donc toute à fait indiqués pour la détection anomalies dédié pour les ICS. De plus, comme il y a la nécessité d'une détection la plus précise possible dans la cadre des ICS, compte tenu de la criticité des données transportées, nous avons décidé de baser nos méthodes au niveau des traces des avions sur les modèles LSTM et autoencodeur.

3.5 Conclusion

Ce chapitre nous a permis d'identifier des mécanismes de détection d'anomalies qui permet de répondre à la problématique de sécurité pour les données radars. En faisant le rapprochement de la problématique de détection d'anomalies pour les données radars avec celle pour les ICS, nous pouvons nous appuyer sur les travaux de ces derniers pour mettre en oeuvre notre détection d'anomalies. Comme les données radars sont des séries temporelles pour lesquelles il y a une signature normale qui va se répéter dans le temps, mais dont les valeurs vont également varier dans le temps, nous pouvons

appuyer nos travaux sur des mécanismes de prédiction évolutive, notamment l'emploi de réseaux de neurones récurrents, qui donnent des résultats efficace pour les ICS avec des séries temporelles contextuelles. Néanmoins,cette approche nécessite de mieux connaitre le type de données radars que nous pourrons étudier. C'est la raison pour laquelle dans le chapitre suivant, nous menons une étude sur le comportement des données radars, justifiant ensuite l'emploi des méthodes de détection vu dans l'état de l'art.

4 Analyse exploratoire des données radars

Afin de pouvoir mettre en œuvre un mécanisme de détection d'anomalies conçu pour les données radars, nous devons auparavant étudier le comportement de ces données afin de pouvoir choisir la méthode de détection appropriée. Pour cela, nous avons commencé notre travail par une analyse exploratoire des données afin d'identifier statistiquement des caractéristiques. Afin de réaliser cette exploration, nous présentons en premier, dans la section 4.1, notre jeu de données pour les analyses. Grâce à cela, nous avons pu sortir des caractéristiques des données radars dans la section 4.2. Ces caractéristiques nous servent à mettre en oeuvre des mécanismes de détection d'anomalies dans le chapitre 5 en s'appuyant notamment sur une problématique similaire avec celle des ICS.

4.1 Jeu de données et outils utilisés

Les données utilisées dans le cadre de ce travail sont des données au format pcap collectées sur le système ATC français du 19 avril 2019 au 31 décembre 2020. Les données collectées n'ont pas fait l'objet de signalements ou d'attaques de la part de la DGAC ; cependant elles peuvent contenir des anomalies "normales" de fonctionnement que nous détaillerons plus tard dans la section 6.2. Dans un premier temps, pour l'analyse statistique des données, nous prenons en compte que ces dernières sont considérées comme "normales" en terme de fonctionnement par la DGAC.

Le point de collecte est un SIR (le SIR est présenté dans la figure 1.2 de la section 2) qui se situe sur le réseau ATC français et qui se trouve au sein de l'Ecole Nationale de l'Aviation Civile (ENAC) à Toulouse. A partir de ce point de collecte, comme les données radars sont envoyées en multicast, nous avons accès à l'ensemble des données radars du système ATC français.

Ces données sont issues de vingt-trois radars secondaires de surveillance (SSR) et neuf radars primaires de surveillance (PSR) recueillies avant qu'elles ne soient traitées par les calculateurs des centres de contrôle.

Les données étant issues du réseau local de la DGAC, elles sont encapsulées sur des trames Ethernet.

Comme vu dans la section 2 avec le fonctionnement du protocole ASTERIX, les données sont envoyées en multicast par le biais des adresses sources. Nous pouvons identifier les radars par deux moyens :

— Par les adresses ETHERNET de destination qui correspondent aux adresses mac des radars.
— Par les champs SAC et SIC définis dans la section 2

L'étude de ces données s'est faite en utilisant le langage de programmation python qui permet de faire des scripts d'analyses sur des fichiers pcap. Afin de pouvoir analyser ces données radars, nous avons utilisé plusieurs outils spécifiques :

— TCPdump [35] permettant de sniffer un réseau nous a permis de capturer le trafic et de l'enregistrer au format PCAP.
— La bibliothèque libpcap a été utilisée pour lire les fichiers pcap via les scripts python.
— Comme ASTERIX n'est pas un protocole régulièrement utilisé, nous avons du employer et adapter le module python ASTERIX [1] développé par Damir Salantic pour la Croatie Control Ltd., afin de parser les données ASTERIX des fichiers pcap et ensuite les analyser.

A partir de ce parseur, nous pouvons enregistrer les données utiles dans un fichier csv nous permettant par la suite de faire nos analyses. Pour les PSR et les SSR ensemble nous n'enregistrons que :

— Les adresses mac source
— Les adresses destination nous permettant d'identifier le radar
— Le Timestamp (TS), c'est-à-dire la date UTC à laquelle le message radar a été envoyé
— La catégorie (CAT)
— Le Time of Day (ToD), c'est-à-dire l'heure de la journée à laquelle le message a été envoyé
— Le SAC et le SIC
— Le Rho (distance entre l'avion et le radar) et le Theta (angle entre l'avion et le radar) qui nous permettent d'avoir la position de l'avion
— Le CGS (Calculated Ground Speed), la vitesse calculée de l'avion
— Le CHDG (Calculated Heading), le cap calculé de l'avion

1. https ://github.com/CroatiaControlLtd/asterix

— Le Track Plot Number (TPN) qui permet d'identifier la trace radar et donc l'avion

Pour les SSR nous avons des informations supplémentaires, comme :
— Le niveau de vol (FL)
— L'adresse de l'avion
— L'identification de l'avion

Toutes ces données étant classées en fonction de leur "timestamp", nous pourrons donc les traiter comme des séries temporelles. Avant analyse (requêtage, apprentissage, prédiction) et visualisation, nous avons apporté des modifications aux données reçues, notamment celles de convertir au format numérique les variables quantitatives ou de remplacer toutes les valeurs manquantes par le champ NULL.

4.2 Caractérisation du trafic réseau des flux radars

Afin de déterminer des caractéristiques sur le comportement des données radars, nous utilisons des informations sélectionnées dans le périmètre des informations disponibles pour un message radar. Nous commençons tout d'abord par identifier les données qui seront les plus à mêmes d'être caractéristiques des données radars du système ATC pour ensuite mettre en évidence une signature du comportement sans anomalie d'un réseau radar. Pour réaliser cette caractérisation, nous effectuons une analyse exploratoire des données (EDA).

4.2.1 Identification d'une métrique caractéristique

Cette première analyse statistique des messages radars nous aide à mieux comprendre le trafic et à définir le type de données sur lequel nous pourrons faire nos analyses. Comme défini dans la section 2, les données radars de l'ATC sont réparties entre des messages de service par rapport au fonctionnement du radar (CAT 02 pour PSR et CAT 34 pour SSR) et des messages de détection qui permettent de donner des informations sur les avions (01 pour PSR et 48 pour SSR) présents dans l'espace aérien.

La répartition des catégories de service et de détection pour l'ensemble de notre jeu de données, présenté dans la figure 4.1, nous indique que la catégorie de détection est présente en majorité : 55% pour les PSR et 75% pour les SSR. Nous pouvons ainsi dire que les données de détection représentent la majorité du trafic radar ATC.
Comme nous avons vu dans la section 2 que les radars étaient redondants, que l'utilisation des SSR et des PSR se faisait en parallèle et que les SSR fournissaient plus

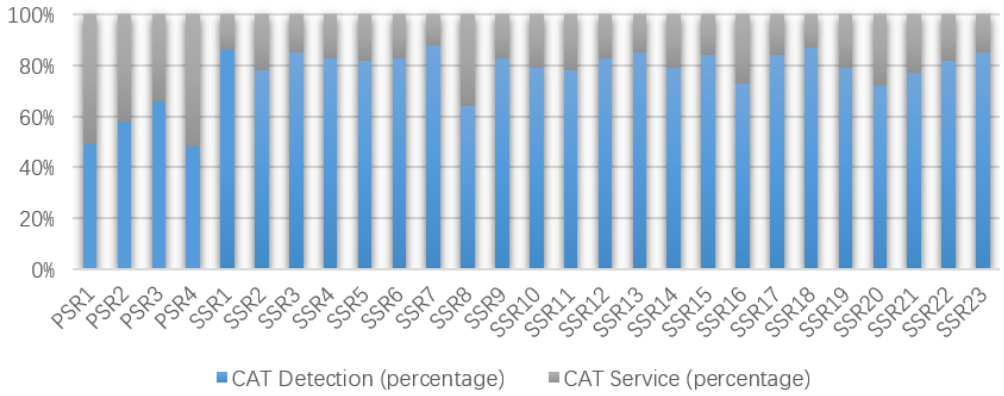


FIGURE 4.1 – Distribution des données de service et de détection dans notre ensemble de données.

d'informations au niveau des enregistrements que les PSR, nous avons décidé pour la suite de l'analyse de nous concentrer sur les données des radars SSR.

Pour ces radars, les données de détection sont issues de la catégorie 48 et celles de service de la catégorie 34. La figure 4.1 nous indique que les données de service sont minoritaires dans le réseau par rapport aux données de détection. Cela est dû au fait que les messages de détection envoient les informations des avions présents dans l'espace aérien qu'ils détectent, tandis que les messages de service ne sont envoyés que toutes les 0,125s par le radar lorsqu'ils changent de secteur.

Ainsi, nous nous sommes intéressés à l'impact du trafic aérien sur le trafic réseau, c'est-à-dire aux métriques du trafic réseau représentant le mieux l'évolution dans l'espace aérien.

Sur notre jeu de données, nous avons analysé l'évolution moyenne dans le temps du nombre de paquets sur une journée pour les messages de détection et les messages de service (figure 4.2).

Les données de services présentent une évolution continue dans le temps tandis que les données de détection sont beaucoup plus variables au fil de la journée. Cela est dû au fait que par nature, les messages de service sont envoyés régulièrement. Il est donc normal d'observer toutes les 4 secondes 32 messages de données de service. Si ce n'est pas le cas, nous pouvons dire qu'il y a potentiellement une anomalie par rapport à ces données.

Ainsi, bien que les données de service soient essentielles dans le fonctionnement du

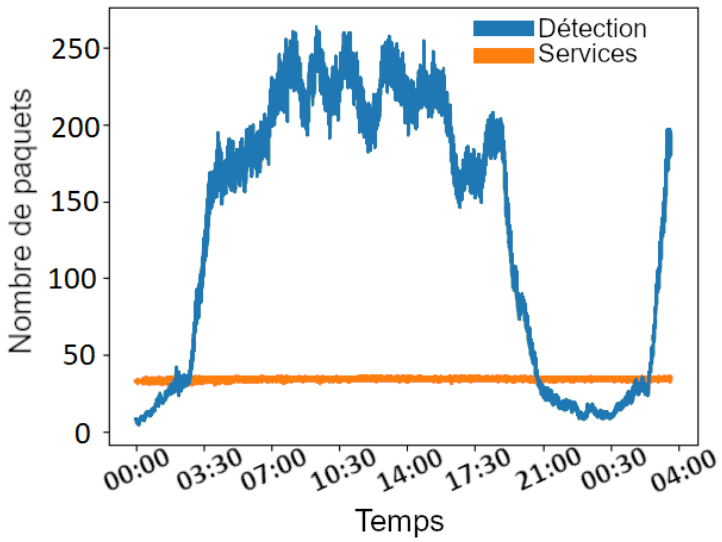


FIGURE 4.2 – Evolution des données de service et de détection en une journée

système ATC, nous pouvons considérer que les métriques réseau représentant le mieux l'évolution de l'espace aérien seront les messages de détection. Grâce à cette observation, durant le reste de l'étude, nous avons choisi de nous concentrer sur l'évolution dans le temps des données de détection.

4.2.2 Recherche d'une signature dans le temps

Étant donné que les données radar du réseau représentent l'image réseau de l'espace aérien à un instant précis, nous soumettons l'hypothèse que le flux de trafic de données radar suivra la signature du trafic aérien qui présente une tendance dans le temps. Des articles [62], [4], [55] ont déjà traité la question concernant l'activité aérienne. Ainsi, dans une journée considérée comme normale, le trafic aérien voit un pic d'activités au début de la journée, à la fin de la matinée, en début de l'après-midi et dans la soirée. Il y a ensuite une accalmie au cours de la nuit pour reprendre ensuite la même tendance. Pour les flux réseau de données radar, nous nous attendons donc à observer une tendance similaire qui va se répéter suivant les jours et les radars que nous pouvons observer. Afin d'étudier cette signature, nous nous sommes intéressés à l'évolution du nombre de paquets radars pendant une journée.

Nous avons commencé par faire une analyse sur deux semaines de données sur une adresse radar pour voir cette évolution. La figure 4.3 représente l'évolution du nombre

de paquets de détection pour les 15 premiers jours de mai 2019 pour un radar donné. Visuellement, le trafic radar semble suivre la même tendance que le flux du trafic aérien : une baisse de l'activité au cours de la nuit, un pic élevé à 2 heures, une variation plutôt stable au cours de la journée avec des pics d'activité et une baisse des activités le soir. Ce résultat est dû au fait que l'évolution des données radar est en corrélation avec l'activité dans l'espace aérien. Ainsi, si le trafic aérien suit une tendance, comme définie précédemment, on s'attend à trouver une tendance similaire dans le flux de données radar.

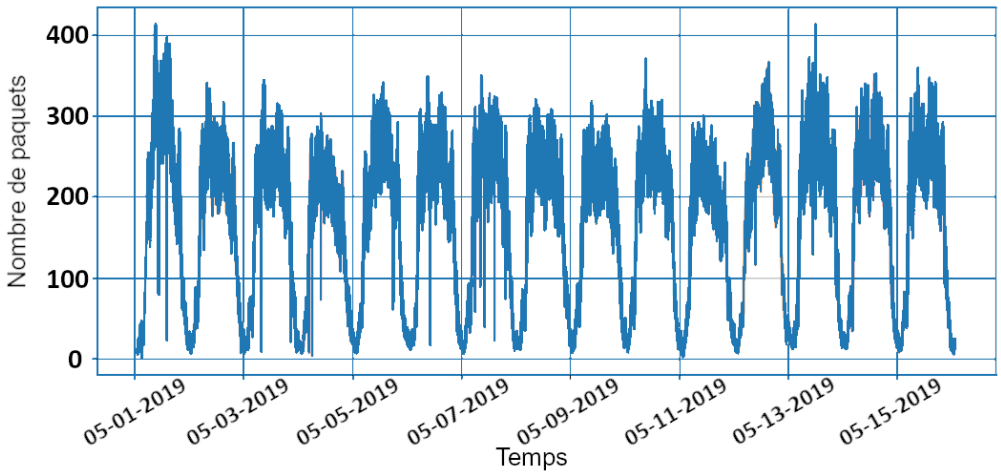


FIGURE 4.3 – Evolution des données de détection au cours des 15 premiers jours de mai

En traçant simultanément l'évolution du nombre de paquets de messages de détection moyen dans le temps, nous pouvons constater qu'une tendance semble ainsi se répéter.

Ainsi, nous notons visuellement que cette signature semble être similaire suivant les jours. En calculant la similarité cosinus entre ces observations, nous obtenons un score de 0,97 qui nous confirme que l'évolution du nombre de paquets de messages de détection moyen présente une signature dans le temps semblant suivre une tendance quotidienne.

Afin de voir si cette évolution se confirme dans le temps, nous avons ensuite calculé l'évolution du nombre de paquets de messages de détection moyen sur deux mois pour l'ensemble des radars SSR présents dans notre jeu de données. Ainsi, par le biais de mesures de minimum, de maximum et de moyenne nous avons pu établir pour chaque radar une moyenne sur deux mois de l'évolution des minimums, des maximums et des moyennes des données observées.

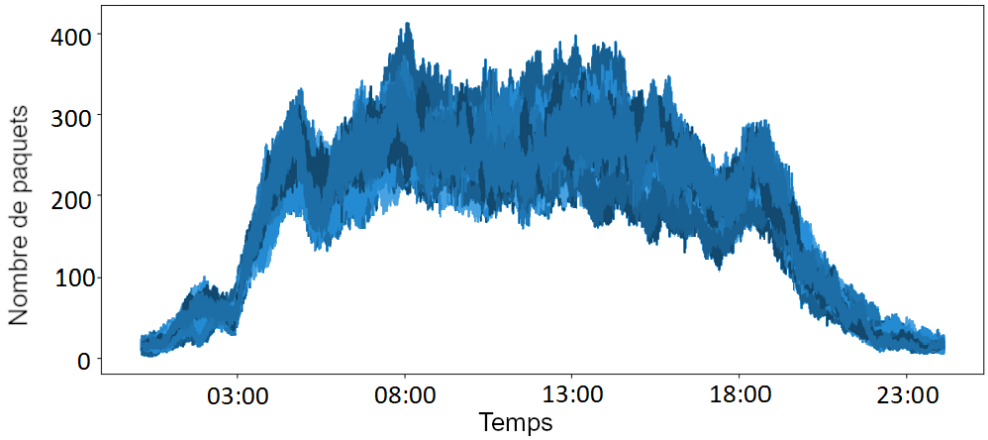


FIGURE 4.4 – Evolution des données de détection pendant une journée les 15 premiers jours de mai simultanément

Nous avons donc pour chaque radar SSR de notre jeu de données, trois courbes d'évolution différentes : une courbe de minimum, une courbe de maximum et une courbe de la moyenne. Nous avons ensuite mesuré la similarité cosinus entre chaque radar que nous avons représenté dans la figure 4.5. L'ensemble des scores de similarité cosinus est proche de 1 pour l'ensemble des radars. Ainsi, les évolutions moyennes du trafic radar dans le temps sont semblables les unes aux autres pour l'ensemble des radars.
Par cela, nous pouvons dire que l'évolution temporelle du trafic aérien dans une journée ne va pas dépendre du radar qui l'observe. De plus, il existe une évolution dans une journée qui semble se répéter dans le temps. Elle se caractérise par la moyenne de l'évolution des messages de détection dans le temps. En se basant sur un ensemble de données qui a été caractérisé sans anomalie et sur un temps relativement long, nous pouvons fixer ces valeurs moyennes et définir une signature pour les radars.

De plus, comme nous l'avons dit précédemment, les données radar sont corrélées du fait du domaine de détection croisée des radars, c'est à dire que les informations d'un avion ne sont pas transmises nécessairement par un seul radar, mais par plusieurs. Par exemple, si nous prenons le cas de l'avion avec l'adresse mode S 3985a1 qui correspond à un Airbus A320-214 de la compagnie AirFrance, qui fait entre autre le trajet Paris-Toulouse, pour un créneau de 4h sur notre jeu de données, nous recevons 11466 enregistrements concernant cet avion, mais ces 11466 enregistrements ont été envoyé par 7 radars différents répartis tels que présentés dans le tableau 4.1.

Nous pouvons donc voir que les différents radars de notre jeu de données vont traiter

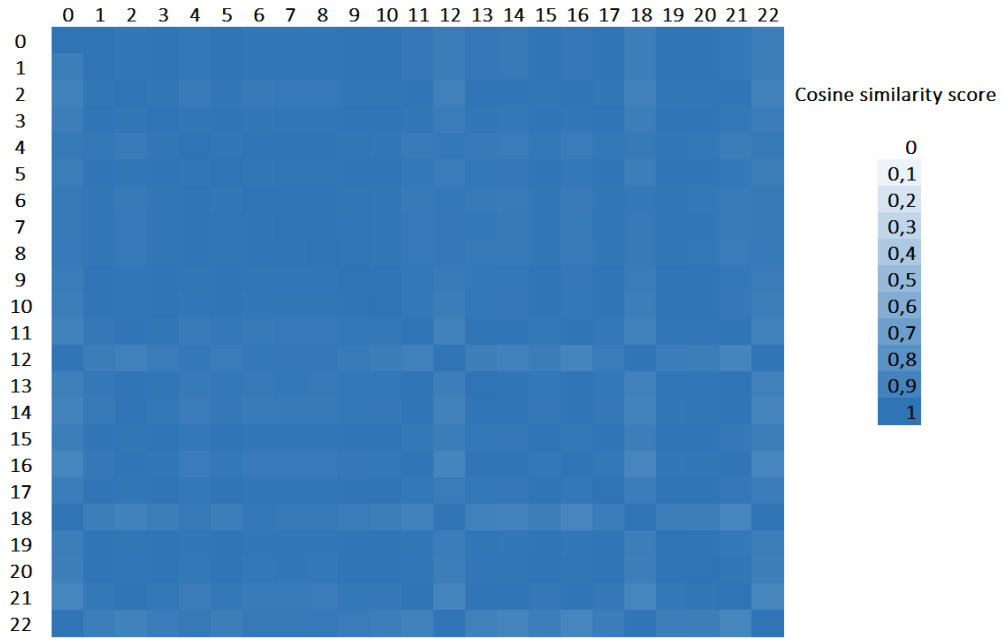


FIGURE 4.5 – Heatmap du score de similitude cosinus entre la moyenne de la signature pour les 23 radars

TABLE 4.1 – Répartition des données de l'avion 3985a1 dans un jeu de données de 4h

Adresse de l'avion :	**3985a1**
Radar 1	15,85%
Radar 2	27,80%
Radar 3	6,48%
Radar 4	29,95%
Radar 5	6,86%
Radar 6	6,38%
Radar 7	6,67%

plusieurs fois les avions. Ainsi, par la suite, nous regarderons l'évolution temporelle correspondant à un seul radar.

Nous nous sommes ensuite intéressés sur le trafic aérien plus en détails avec l'évolution du nombre d'avions dans l'espace aérien. Pour cela, nous sommes allés plus profondément dans les données ASTERIX pour en ressortir les identifiants des avions et pouvoir analyser cette évolution dans le temps. La figure 4.6 représente l'évolution du nombre d'avions

dans l'espace aérien français de novembre 2019 à décembre 2020. Nous pouvons constater dans un premier temps que ce nombre semble varier en fonction du jour.

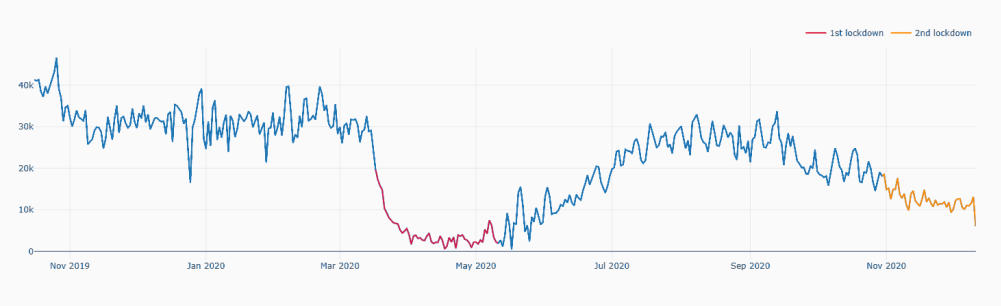


FIGURE 4.6 – Evolution du nombre d'avions dans l'espace aérien de novembre 2019 à décembre 2020

Cependant, en traçant la répartition du nombre d'avions en fonction du jour de la semaine pour le jeu de données dans la figure 4.7, nous pouvons constater que nous avons une répartition équitable suivant les jours de la semaine. L'évolution ne dépendra donc pas du jour considéré.

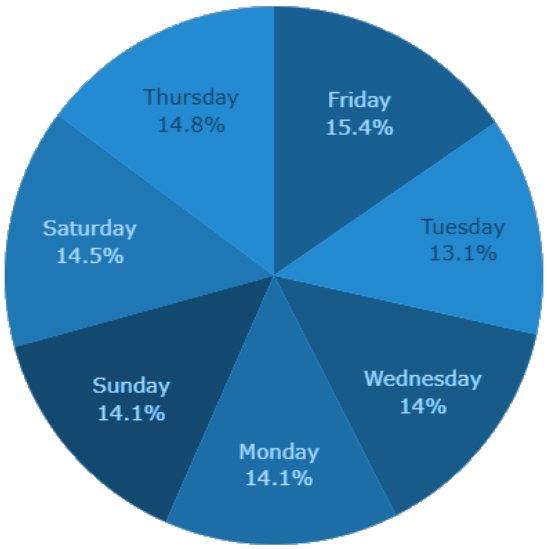


FIGURE 4.7 – Répartition du nombre d'avions dans une semaine

La figure 4.6 nous fait également constater que le trafic a chuté de manière importante durant le premier confinement en France du 17 mars 2020 au 11 mai 2020, du à la

COVID19, passant de 20000 avions par jour à moins de 5000, voire moins de 1000 les jours les plus bas, comme l'illustre la figure 4.8.

Nous pouvons donc dire que la COVID19 a eu un impact important sur l'évolution du trafic aérien en terme de densité d'avions dans l'espace aérien. On pourrait se demander si cela a également eu un impact sur la signature observée précédemment.

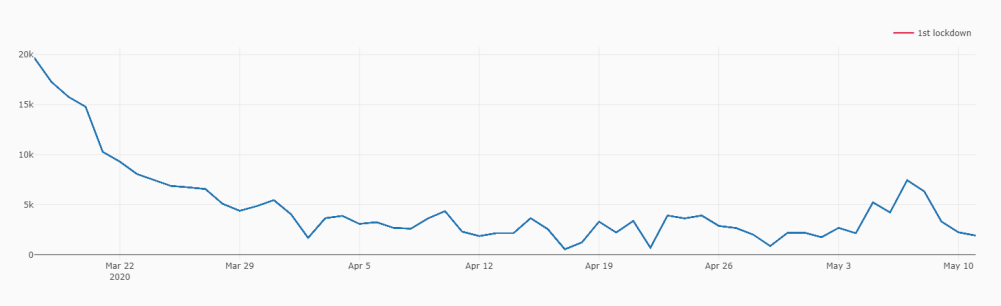


FIGURE 4.8 – Evolution du nombre d'avion dans l'espace aérien pendant le premier confinement en France

Lorsque nous analysons l'évolution du nombre des avions dans une journée répartis suivant les heures pour le confinement par rapport à celui pour tout le jeu de données 4.9, nous constatons que, bien que le nombre d'avions soit moins important pendant le confinement qu'en temps normal (valeur maximale de 450 avions pendant le confinement pour 2000 en temps normal), les comportements dans une journée sont proportionnellement similaires à la signature que nous avons pu observer précédemment. Cela est dû au fait que, bien que le confinement ait eu lieu, les règles en terme d'utilisation de l'espace aérien ainsi que les créneaux de vol prévus sont restés similaires dans une journée. Nous avions donc un comportement "normal" avec seulement moins d'avions .

Nous pouvons ainsi dire que, malgré des événements tels qu'un confinement, l'évolution du trafic radar dans le temps va présenter dans une journée une évolution, proportionnelle au trafic aérien en cours, avec une signature reconnaissable.

Cette analyse nous a permis de définir que l'évolution du trafic radar dans le réseau est défini par l'évolution des messages de détection dans le temps. A partir de cette évolution dans le temps, nous pouvons établir une signature 4.10 du comportement normal reconnaissable dans le temps et proportionnelle à l'occupation de l'espace aérien. Ainsi, une des caractéristiques du trafic radar sur le réseau ATC est qu'il est représentatif du trafic dans l'espace aérien en terme d'évolution dans le temps. Ils présentent tous les

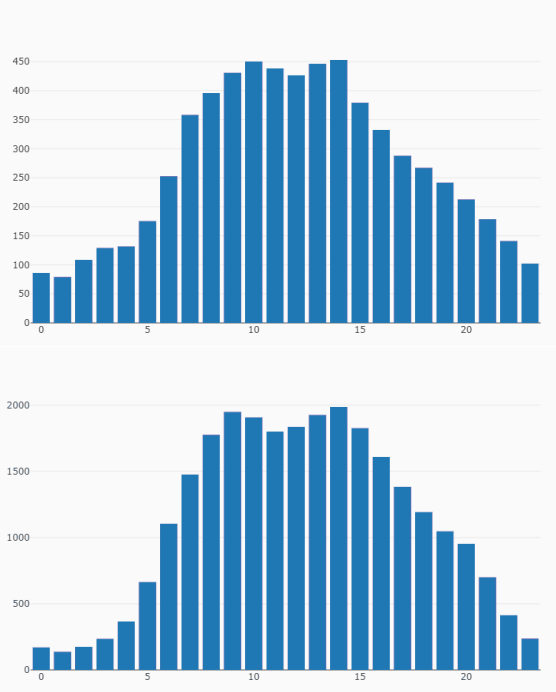


FIGURE 4.9 – Evolution moyenne par jour du nombre d'avions dans l'espace aérien pendant le premier confinement(en haut) et sur l'ensemble du jeu de données (en bas)

deux une signature qui va se répéter quotidiennement et qui permet de caractériser ce trafic.

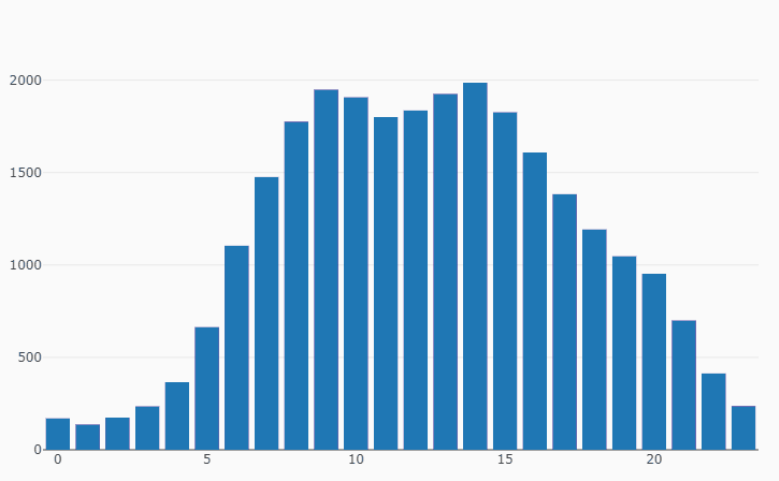


FIGURE 4.10 – Evolution moyenne par jour du nombre d'avions dans l'espace aérien sur l'ensemble du jeu de données

4.3 Corrélation des attributs entre eux

Cependant, nous ne nous intéressons pas seulement à l'évolution dans le temps du nombre de messages de détection reçu sur un radar. Afin de rentrer plus profondément dans les données, nous nous intéressons également au positionnement des avions. Le tableau 4.2 présente les informations extraites des données de détection que nous utiliserons pour nos travaux de détection d'anomalies par analyse prédictive.

TABLE 4.2 – Attributs des messages radars utilisés dans l'étude

Attribut	**Description**	**Unité**	**Plage**
Track plot number (TPN)	Une référence unique pour indiquer une trace d'avion	–	[0,65535]
TS	Heure standard au temps UTC	s	variable
THETA	Position mesurée d'un avion en coordonnées polaires locales	deg	[0,360]
RHO	Position mesurée d'un avion en coordonnées polaires locales	nautical mile	[0,250]
Calculated Ground Speed (CGS)	Vitesse calculée exprimée en coordonnées polaires	Knt	[0,500]
Calculated Heading (CHDG)	Le cap calculé	deg	[0,360]
Flight Level (FL)	Information de niveau de vol	hft	[0,400]

Avant de faire notre étude sur la détection d'anomalies, nous nous intéressons à la corrélation entre chaque attribut des données radars. En effet, ces mesures de corrélation nous aident à définir le modèle d'apprentissage le plus approprié. Dans le cas d'une forte corrélation entre variables, nous pouvons utiliser un modèle de régression et prédire les données à partir de ce modèle. Néanmoins, le calcul des coefficients de corrélation présenté dans la figure 4.11 nous montre que pour les attributs des données radars, la corrélation est faible. La régression ne semble donc pas être la méthode la plus efficiente. Cependant, il y a une forte dépendance entre les données et la temporalité du fait que

l'on soit en présence de séries temporelles. Ainsi, nous choisissons par la suite des modèles de prédiction adaptés aux séries temporelles.

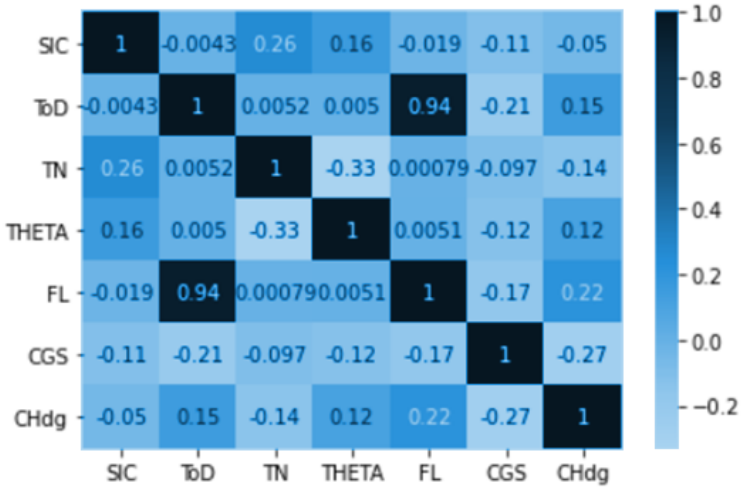


FIGURE 4.11 – Tableau des coefficients de corrélation entre chaque variable

4.4 Conclusion

Ce chapitre nous a permis de mener une analyse haut niveau du comportement des flux radars dans le temps. Nous avons ainsi pu déterminer que le comportement d'un flux radar va dépendre des messages de détection qui seront transmis par les radars. De plus, comme les informations des avions sont envoyés par plusieurs radars, il n'est pas nécessaire d'étudier l'ensemble des radars pour être en mesure de mettre en place un mécanisme de détection d'anomalies. Ce comportement des flux radars dans le temps nous a ainsi permis de reconnaitre une signature. Cette signature nous pousse à mettre en place une méthode de détection d'anomalies par prédiction car nous pouvons nous appuyer sur la connaissance de ce comportement pour prédire le comportement futur. De plus, lorsque nous regardons plus en détail les attributs des messages, nous pouvons voir une faible dépendance des attributs entre eux, mais une forte corrélation entre les données et le temps. Dans le chapitre suivant, en s'appuyant sur les résultats de cette analyse, nous mettons en place une méthode de détection d'anomalies prédictives à deux niveaux : celui des flux radars et celui des traces des avions.

5 Détection d'anomalies sur le réseau ATC

Après avoir mis en exergue le caractère répétitif d'une signature temporelle pour les données radars dans le chapitre 4, nous utilisons cette signature pour détecter des anomalies sur ces données. Pour cela, nous nous appuyons sur des modèles prédictifs. Ce chapitre traite donc de la détection d'anomalies pour les données radars. Dans un premier temps, dans la section 5.1, nous décrivons la méthode employée pour générer des attaques, ainsi que le traitement effectué sur les données. Nous mettons ensuite en œuvre des mécanismes de détection et les évaluons dans la section 5.3 puis 5.4.

5.1 Principe des attaques mises en oeuvre

Avant de développer une méthode de détection des anomalies dans les données radars, nous avons créé des attaques afin de s'assurer que nos méthodes puissent être en mesure de détecter celles qui peuvent être craintes dans le domaine aéronautique.

Comme nous l'avons vu dans le chapitre 4, les attaques les plus craintes sont celles qui vont modifier les données radars envoyées aux contrôleurs, car ce sont celles qui ont potentiellement les conséquences les plus importantes sur le contrôle aérien.

Une de manière de réaliser cette attaque est de faire du *spoofing* par *Man In the Middle* (MITM). Un attaquant se place entre l'émetteur (ici le radar) et le récepteur (ici l'écran du contrôleur) dans le but de faire une modification artificielle et volontaire d'une partie des données dans l'ensemble du jeu de données.

A partir du moment où un attaquant a accès au réseau, s'il a un minimum de connaissances sur le fonctionnement d'un réseau ATC, il a la possibilité de modifier tout ou partie des données radars transmises. Bien que la DGAC a mis en place des protections physiques et logiques sur son réseau, nous nous plaçons dans l'hypothèse qu'un attaquant ait accès au réseau ATC, soit par le biais d'une attaque physique en se connectant directement sur le réseau au niveau des radars, sur le réseau de transmission ou après le calculateur ; soit par le biais d'une attaque informatique qui lui permettrait d'accéder à ce réseau à distance.

Par ce biais, un attaquant pourrait modifier l'ensemble des caractéristiques des données radars que nous avons présenté dans la section 4.1 du chapitre 4.

Cependant, nous nous sommes concentrés sur la modification des données RHO et THETA qui permettent d'afficher la position de l'avion ainsi que sur la vitesse CGS, car ce sont ces données qui une fois modifiées, permettraient à un attaquant de causer un accident.

Formation des attaques Avant tout, afin de nous permettre de visualiser les données radars et voir les conséquences de notre attaque sans avoir accès à un équipement opérationnel, nous avons développé un affichage, grâce au module pygame [1] de python, couplé avec un layer ASTERIX sur SCAPY [2] (un outil de manipulation de paquets pour les réseaux informatiques) que nous avons développé afin de visualiser le trafic radar.

Notre outil nous permet une visualisation basique au niveau de plot radar, ainsi qu'une visualisation des trajectoires des avions pour un radar donné, comme sur la figure 5.1.
8

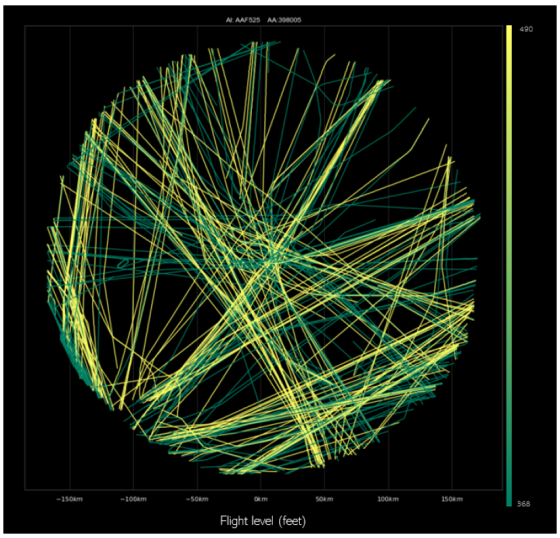


FIGURE 5.1 – Visualisation des trajectoires sur une journée pour un radar donné

Pour réaliser l'attaque MITM décrite précédemment, nous rejouons des données radars du jeu de données opérationnel, grâce au module TCPReplay [3] de python. Afin de se placer dans un contexte normal, nous choisissons de rejouer des données en dehors du

1. https ://www.pygame.org/
2. https ://scapy.net/
3. https ://github.com/appneta/tcpreplay

contexte du Covid19. Nous nous concentrons donc sur des données issues de l'année 2019. En utilisant un parser ASTERIX et notre module de visualisation, nous pouvons simuler l'affichage des ces données sur un écran de visualisation radar. Nous avons ainsi un réseau de test simulant la transmission radar et la visualisation des données.

Nous nous plaçons ensuite dans le rôle d'un attaquant présent sur le réseau de transmission radar. Pour réaliser l'attaque Man In The Middle, nous recevons toutes les données radars transmises sur le réseau ; puis nous les retransmettons sans modification dans un premier temps. A un moment donné, nous choisissons de modifier un ou plusieurs paramètres des données radars pour un ou plusieurs avions grâce à un script python utilisant notre layer SCAPY. Ces modifications seront transmises sur le réseau à destination de la visualisation.

La figure 5.3 montre un exemple de réalisation de cette attaque en changeant la trajectoire d'un avion par la modification de l'attribut THETA. L'écran de gauche nous montre les données non modifiées transmises par le radar. L'écran de droite représente les données modifiées que nous envoyons vers la visualisation. Nous pouvons également représenter une attaque de ce type en visualisant l'impact sur sa trajectoire, comme montré dans la figure 5.2.

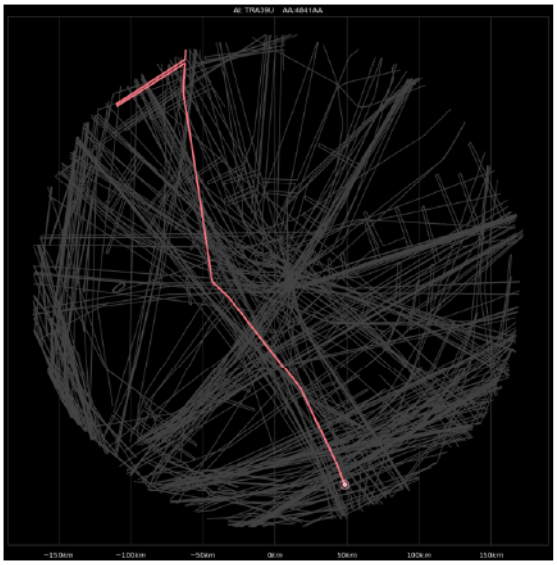


FIGURE 5.2 – Visualisation de la trajectoire modifiée d'un avion

Par le biais de cette attaque Man In The Middle, à partir du moment où nous avons accès aux données radars, nous pouvons mener toutes les attaques que nous voulons sur

la visualisation du contrôleur :

— Nous pouvons modifier la trajectoire d'un ou plusieurs avions comme dans l'exemple de la figure 5.3.

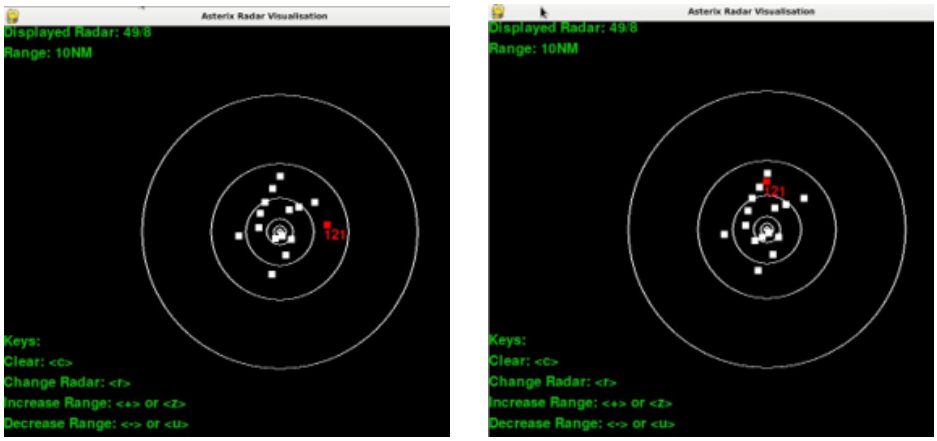


FIGURE 5.3 – Visualisation d'un trafic attaqué par spoofing

— Nous pouvons ajouter ou supprimer des avions comme dans l'exemple de la figure 5.4 (sur l'écran de droite nous ajoutons une grande quantité de plots radars pour rendre la visualisation de plots légitimes plus complexes).

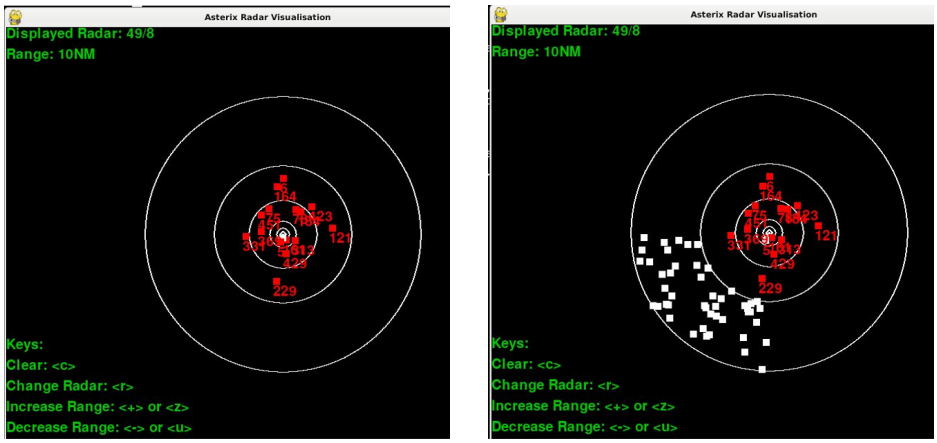


FIGURE 5.4 – Visualisation d'un trafic attaqué par flooding

— Nous pouvons figer tout ou partie des plots radars sur la visualisation, le contrôleur ne saura donc plus la position de l'avion.

Par la suite, comme le principe des attaques reste identique, c'est à dire la modification des données radars transmises, nous nous concentrons sur l'attaque la plus fine, soit la

modification d'un ou plusieurs attributs pour un ou plusieurs avions dans un jeu de données.

5.2 Les modèles de Machine Learning utilisés pour la prédiction de données

Dans la suite de l'étude, afin de mettre en oeuvre nos méthodes de détection d'anomalies, nous nous plaçons à deux niveaux :

— Le premier, plus général, au niveau du radar en lui-même. Nous faisons de la prédiction de données sur le nombre de messages de détection reçus dans le temps au niveau du radar. Nous utilisons pour cela le modèle de prévision Fbprohet. La méthode est présentée dans 5.2.1 et l'utilisation dans 5.3.1.

— Le deuxième, plus précis, au niveau des traces d'un avion où nous faisons de la prédiction sur l'évolution des attributs pour un avion. Nous utilisons pour cela les méthodes LSTM et d'auto-encodeur. La méthode est présenté dans 5.2.2 pour LSTM, 5.2.3 pour l'auto-encodeur et l'utilisation dans 5.3.3 pour LSTM et 5.3.4 pour l'auto-encodeur.

5.2.1 Le modèle de prévision Fbprophet

Fbprophet est un framework open-source développé par Facebook en 2017. Il met en œuvre une procédure de prévision des données de séries temporelles basée sur un modèle additif où les tendances non linéaires sont adaptées à la saisonnalité annuelle, hebdomadaire et quotidienne, plus les effets des vacances. Cela convient parfaitement aux séries temporelles qui ont de forts effets saisonniers et plusieurs saisons de données historiques. Son utilisation permet de prédire des données futures, mais de également détecter des anomalies et combler des valeurs manquantes. Son efficacité a été prouvé pour la prédiction de tendance sur l'évolution du cours de cryptomonnaies telles que le Bitcoin [74], mais également sur l'évolution de la pandémie du Covid19 [5], ou bien encore l'évolution à court-terme d'un trafic routier [15]. Comme les données radars présentent une saisonnalité quotidienne au niveau de l'évolution du trafic des messages, Fbprophet se montre comme un modèle efficace pour prédire ces données.

Son principe est d'utiliser un modèle de série temporelle décomposable en trois composantes principales du modèle : tendance, saisonnalité et vacances.

La mise en œuvre et les résultats de cette méthode sont présentés en 5.3.1.

5.2.2 Le modèle LSTM

En s'appuyant sur l'état de l'art de détection d'anomalies pour les ICS, nous nous intéressons au Réseau Neuronal Récurrent (RNN) basé sur le modèle LSTM (Long-Short Term Memory). En effet, un RNN est réseau de neurones qui est adapté au traitement de données séquentielles grâce à son vecteur d'état qui garde une mémoire de tous les éléments précédents de la séquence. Cependant, il a été montré que les RNN standards ne sont pas efficients pour les dépendances sur les longs intervalles [6] [42] à cause de l'inexactitude des résultats ou du temps trop important de prédiction dû au fait de la multiplication de l'erreur à chaque étape avec la même valeur de même poids, causant ainsi soit un gradient d'erreur trop important, soit trop faible.

Pour traiter ce problème d'apprentissage à long terme dans les RNN, il a été introduit dans la formation du RNN des scores permettant d'éviter ce problème d'explosion ou de disparition des gradients, c'est le modèle LSTM [43]. Ce modèle permet d'obtenir de meilleurs résultats que les RNN en apprentissage pour les dépendances à long terme. Depuis lors, les chercheurs ont également proposé un certain nombre de variantes de LSTM, dont la plus populaire est décrite par Graves et Schmidhuber dans [36] en 2005 qui met en place une porte d'oubli pour pallier un problème de non réinitialisation de la mémoire. L'architecture LSTM se compose de cellules de mémoire utilisées pour apprendre les modes à long terme, chaque cellule contenant son état actuel et trois portes non linéaires :

— la porte d'oubli
— la porte d'entrée
— la porte de sortie

La porte d'oubli est chargée de déterminer la quantité d'informations de mémoire à oublier. On la détermine par une fonction non linéaire qui génère un nombre compris entre 0 et 1, (avec 0 on oublie toutes les informations en mémoire et 1 on conserve toutes les informations en mémoire). La porte d'entrée est chargée de décider comment mettre à jour l'ancien état de la cellule, c'est-à-dire que les nouvelles informations sont enregistrées sélectivement dans l'état de cellule. La porte de sortie est chargée de décider de la quantité d'informations à transmettre à la cellule suivante. La structure de LSTM est illustrée à la figure 5.5.

Une donnée radar peut-être considérée comme une séquence avec dépendance à long terme. en effet, bien que les données soient indépendantes, les flux représentant les traces et donc la trajectoire de l'avion, vont dépendre de chaque plot radar précédents. Par

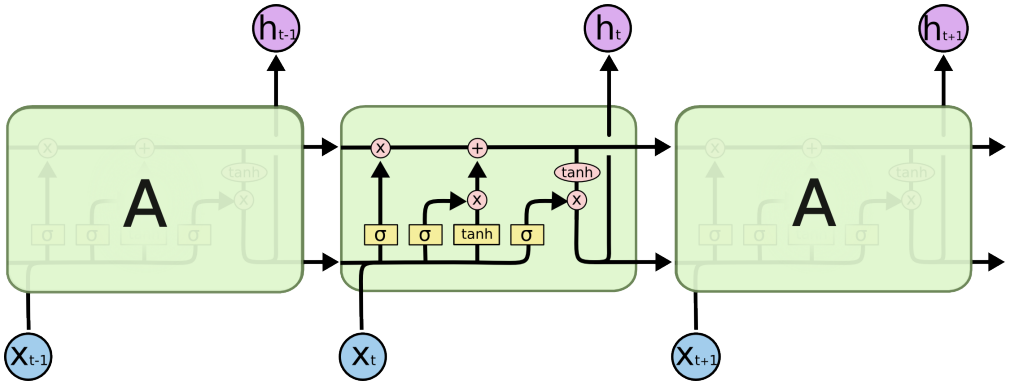


FIGURE 5.5 – Le module extensible d'un LSTM contient quatre couches d'interactions

conséquent, en se plaçant au niveau d'un avion nous utilisons la méthode LSTM dont les résultats sont présentés dans 5.3.3 pour prédire les traces dans le temps.

5.2.3 Le modèle de l'auto-encodeur

Un auto-encodeur vise à reproduire un vecteur d'entrée S à n dimensions par un vecteur de $\hat{S}$ à n dimensions (Hinton et al [41]). Il comprend deux composants : un **encodeur** et un **décodeur**.

- L'encodeur transforme un vecteur d'entrée S en un vecteur intermédiaire F à m dimensions.
- Le décodeur transforme le vecteur F à un vecteur de sortie $\hat{S}$ qui doit se rapprocher du vecteur d'entrée S.

Ils sont formellement définis par les fonctions :

$$\textbf{Encodeur} : \varphi : R^n \rightarrow R^m$$

.

$$\textbf{Décodeur} : \phi : R^m \rightarrow R^n$$

.

La fonction objective de l'auto-encodeur peut alors être définie par :

$$argmin_{\varphi,\phi} \|S - \phi(\varphi(S))\|_2^2$$

L'objectif est de déterminer la fonction appropriée pour minimiser l'erreur entre le vec-

teur d'entrée S et le vecteur de sortie $\hat{S} = \phi(\varphi(S))$. Dans la phase de codage, on définit

$$F = \sigma_1(W_1 S + B_1)$$

Avec

— $W_1 \in R^{m \times n}$ une matrice de poids.
— $B_1 \in R^m$ un vecteur de décalage.
— σ_1 la fonction d'activation, c'est-à-dire la fonction ReLU ou sigmod.

Dans la phase de décodage, on définit :

$$\hat{S} = \sigma_2(W_2 F + B_2)$$

Avec

— $W_2 \in R^{n \times m}$ une matrice de poids.
— $B_2 \in R^n$ un vecteur de décalage.
— σ_2 la fonction d'activation, c'est-à-dire la fonction ReLU ou sigmod.

La figure 5.6 illustre un modèle d'auto-encodeur.

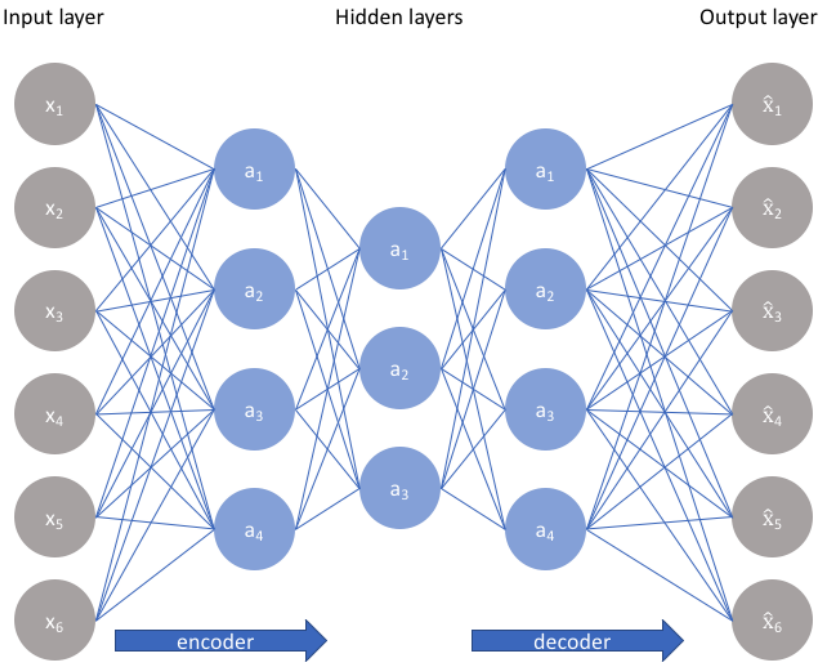


FIGURE 5.6 – Modèle d'auto-encodeur

En ce qui concerne les données traitées issues de séries temporelles, l'espace des ca-

ractéristiques est beaucoup plus grand que dans les données brutes d'une série temporelle. Cela permet à l'auto-encodeur d'identifier les caractéristiques les plus représentatives pour un petit espace.

Afin d'effectuer le traitement sur des données brutes d'une série temporelle, nous faisons auparavant des opérations. Nous définissons en premier lieu une fenêtre $T_i =< S_i, S_{i+1}, \ldots, S_{i+c-1} >$ qui est la série temporelle sur l'intervalle $[t_i, t_{i+c-1}]$, avec $S_i = s_1, s_2, \ldots s_n$ un vecteur à n dimensions. Nous mettons ensuite en place une procédure en trois étapes pour traiter les données brutes d'une série temporelle et faire une extraction profonde des caractéristiques :

1. Nous prenons ensuite une fenêtre coulissante avec une taille de pas [b](b>1). Deux fenêtres consécutives ont une taille de pas de b/2. Nous obtenons ainsi une série temporelle de longueur $C^{'} = (2C - b)/b$ à partir d'une série temporelle de longueur C. Pour chaque fenêtre nous calculons deux caractéristiques dérivées à partir des caractéristiques de la série temporelle :
   — **NOR** (norme) :

   $$NOR^j(T_i) = \sqrt{(s_i^j)^2 + (s_{i+1}^j)^2 + \cdots + (s_{i+b-1}^j)^2}$$

   avec $s_i^j, s_{i+1}^j, \ldots, s_{i+b-1}^j$ la j-ième fonction de $S_i, S_{i+1}, \ldots, S_{i+b-1}$.NOR capture les informations de taille des caractéristiques dans la séquence contenue dans la fenêtre.
   — **DON** (différence de norme) :

   $$DON^j(T_i) = NOR^j(T_i) - NOR^j(T_{i-1})$$

   avec i la i-ème fenêtre. DON capture les informations de modification de la taille des caractéristiques dans deux fenêtres consécutives, c'est-à-dire la dépendance temporelle. Nous obtenons ainsi, la série temporelle : $T^{'} =< G_1, G_2 \ldots G_{'C} >$, avec G_i dans $R^{d \times n}$, une matrice.
2. Pour effectuer la conversion de la deuxième étape, nous utilisons une fenêtre glissante de taille f, avec la longueur de chevauchement entre deux fenêtres consécutives f/2. Pour chaque fenêtre, on calcule une série de caractéristiques statistiques des deux caractéristiques dérivées (NOR et DON) de la séquence. Cette série de caractéristiques permet de capturer efficacement la variation des caractéristiques dérivées en fonction du temps.

   D'après Dong et al. [22], huit caractéristiques statistiques correspondant aux ca-

ractéristiques dérivées peuvent être calculées :

— La moyenne
— Le minimum
— Le maximum
— Les quartiles (25Q, 50Q, 75Q)
— L'écart type
— La valeur crête à crête

Nous obtenons donc la série temporelle : $T^{''} =< H_1, H_2 \dots H_{C^{''}} >$, avec H_i dans $R^{(e \bullet d)} \times n$, une matrice.

3. Enfin, nous développons et vectorisons cette matrice pour obtenir la série temporelle finale :

$$T''' =< H_1^{'}, H_2^{'}, \dots, H_{C^{''}}^{'} >$$

avec $H_i^{'}$ dans $R^{1 \times (e \bullet d \bullet n)}$, un vecteur.

Les différentes étapes sont illustrées dans la figure 5.7.

En exemple, dans la figure 5.8, nous prenons une série temporelle de données radar T qui contient 6 caractéristiques. Nous avons donc un vecteur à n=6 dimensions. Nous obtenons ainsi une série temporelle $T^{'}$ après la première conversion et une série $T^{''}$ après la seconde. Pour les deux conversions, nous choisissons une taille de fenêtre glissante respectivement de b=4 et f=2. Nous vectorisons $T^{''}$ pour obtenir $T^{'''}$. Ainsi nous obtenons une série temporelle avec des vecteurs de dimensions 96 (contre 6 au départ), tandis que la longueur totale de la série temporelle est divisée par 2 par rapport à celle de départ.

Comme pour la méthode LSTM dans 5.2.2, afin de prédire les traces radars des avions dans le temps, nous utilisons la méthode d'auto-encodeur dont les résultats sont présentés dans 5.3.4.

De plus, les données issues d'une série temporelle sont souvent interdépendantes plutôt qu'indépendantes. En s'inspirant des travaux de Kieu et al. [50], nous décidons d'utiliser des fenêtres coulissantes dans nos modèles prédictifs pour tenir compte de ces dépendances entre vecteurs et calculer des caractéristiques statistiques dans chaque fenêtre pour obtenir des informations plus détaillées.

5.3 Détection d'anomalies par prédiction de trafic

Grâce aux travaux présentés dans le chapitre 3 section et aux méthodes présentées dans la section 5.2, nous avons mené une détection d'anomalies par prédiction de trafic. Dans cette section, comme dit dans la section 5.2, nous nous plaçons à deux niveaux

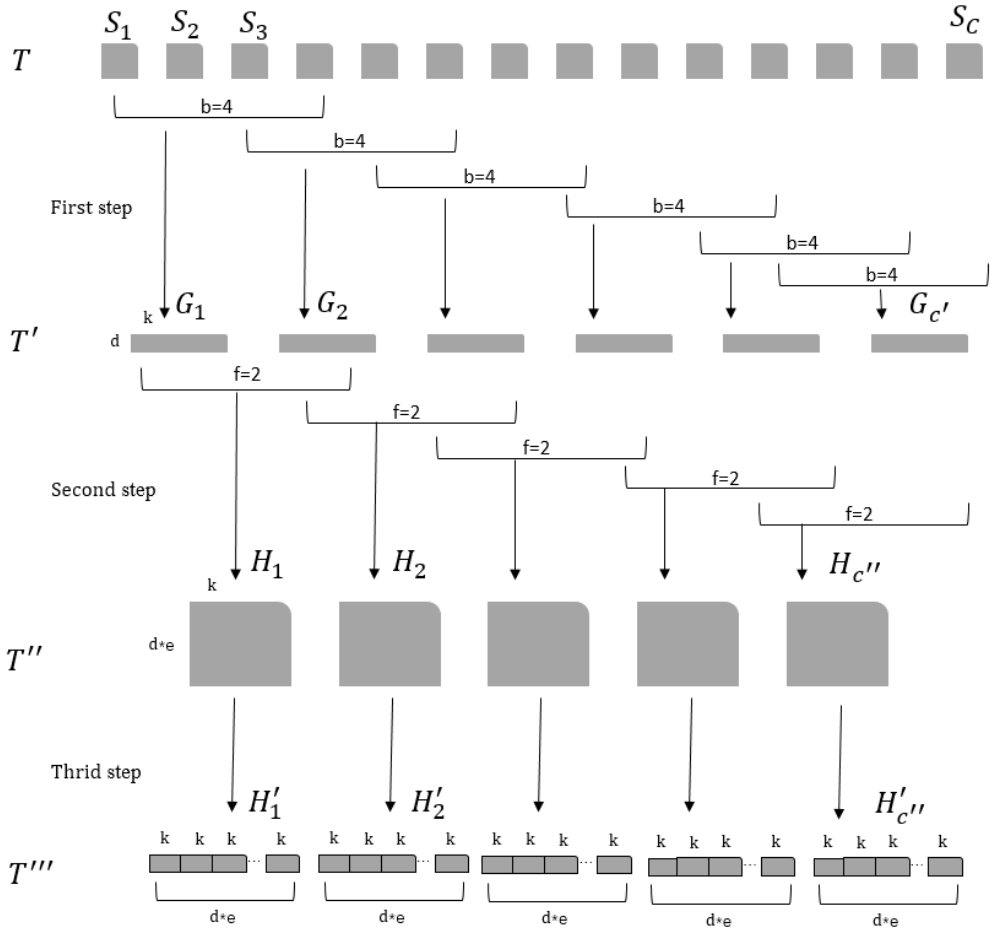


FIGURE 5.7 – Trois étapes de l'enrichissement de données

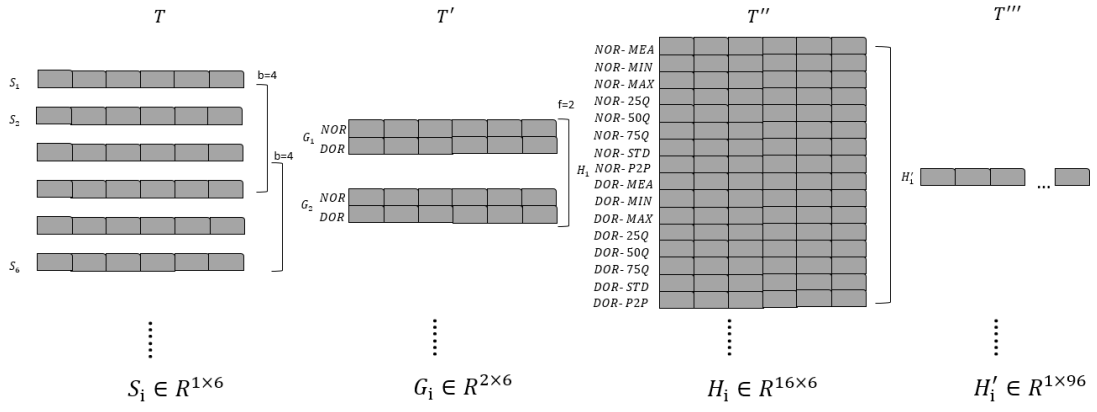


FIGURE 5.8 – Exemple d'enrichissement de données avec les paramètres n=6, b=4, f=2.

pour faire de la détection d'anomalies.

La première utilisation au niveau de l'évolution du trafic de messages de détection pour un radar est présenté en 5.3.1.

La deuxième utilisation, afin de rentrer plus en détails dans les données, concerne l'évolution de la trace radar d'un avion dans le temps . La prédiction se fait avec la méthode LSTM, puis la méthode d'auto-encodeur. Les résultats sont présentés respectivement en 5.3.3 et 5.3.4.

5.3.1 Prévisions de tendance préliminaire par le procédé Fbprohet

Comme vu dans la section 4, l'évolution temporelle des messages de détection a une signature quotidienne qui va se reconnaître dans le temps. Dans la sous-section 5.2.1, nous avons présenté le procédé Fbprophet permettant de faire de la détection d'anomalies sur des séries temporelles contextuelles. Nous présentons ici le résultat de la prédiction pour un radar, les données correspondant au nombre de messages radars de détection dans l'espace aérien pour un moment donné. Nous avons choisi cependant de ne pas évaluer la détection d'anomalies, pour rentrer davantage dans le détails des messages comme dans les sections 5.3.3 et 5.3.4. Dans cette sous-section, nous axerons notre étude sur la capacité pour le procédé Fbprophet à prédire efficacement les données.

Prétraitement des données pour Fbprohet

Le modèle Fbprophet nécessite que les données d'entrée soient sous une forme fixe. Nous avons utilisé un fichier csv (tel que présenté dans le tableau 5.9) pour stocker deux colonnes de données :

— la première « ds » représentant l'horodatage de la série temporelle

— la deuxième «y» exposant les valeurs de la série temporelle.

Ici, y représente le nombre de messages radar de détection après une normalisation moyenne. La méthode Fbprophet décrit y tel que :

$$y(t) = g(t) + s(t) + h(t) + \epsilon_t$$

avec :

— g(t) la fonction de tendance modélisant les changements non périodiques de la valeur de la série temporelle

— s(t) les changements périodiques (comme la saisonnalité hebdomadaire et annuelle)

— h(t) les effets des vacances qui se produisent sur des horaires potentiellement irréguliers sur un ou plusieurs jours.

— ϵ_t le terme d'erreur représentant tout changement particulier qui n'est pas pris en compte par le modèle. Nous ferons par la suite l'hypothèse que ϵ_t est normalement distribué

.

	ds	y
0	2019-04-27 01:18:18.501500130	-1.326395
1	2019-04-27 01:23:30.901999950	-1.294584
2	2019-04-27 01:23:40.901999950	-1.342300
3	2019-04-27 01:23:50.901999950	-1.302537
4	2019-04-27 01:24:00.901999950	-1.342300

FIGURE 5.9 – Données en entrée du modèle

En sortie d'algorithme, nous obtenons un fichier csv (tel que présenté dans le Tableau 5.10) avec des valeurs « yhat », « yhat_lower » et «yhat_upper», qui représentent respectivement la valeur prédite du nombre de messages radar de détection, la borne inférieure de la valeur prédite et la borne supérieure de la valeur prédite.

Méthode et résultats pour Fbprohet

Nous avons testé cette méthode avec un jeu de données radars du 27-04-2019 au 04-05-2019 pour prédire la journée du 05-05-2019. Les résultats sont donnés dans la Figure 5.11.

Les points noirs représentent les données de la série temporelle d'origine, c'est à dire le

	ds	trend	yhat_lower	yhat_upper
0	2019-04-27 01:18:18.501500130	0.083911	-1.790747	-0.873355
1	2019-04-27 01:23:30.901999950	0.077270	-1.774174	-0.869495
2	2019-04-27 01:23:40.901999950	0.077058	-1.773778	-0.904737
3	2019-04-27 01:23:50.901999950	0.076845	-1.782339	-0.887392
4	2019-04-27 01:24:00.901999950	0.076633	-1.762371	-0.855957

FIGURE 5.10 – Echantillon de données de sortie

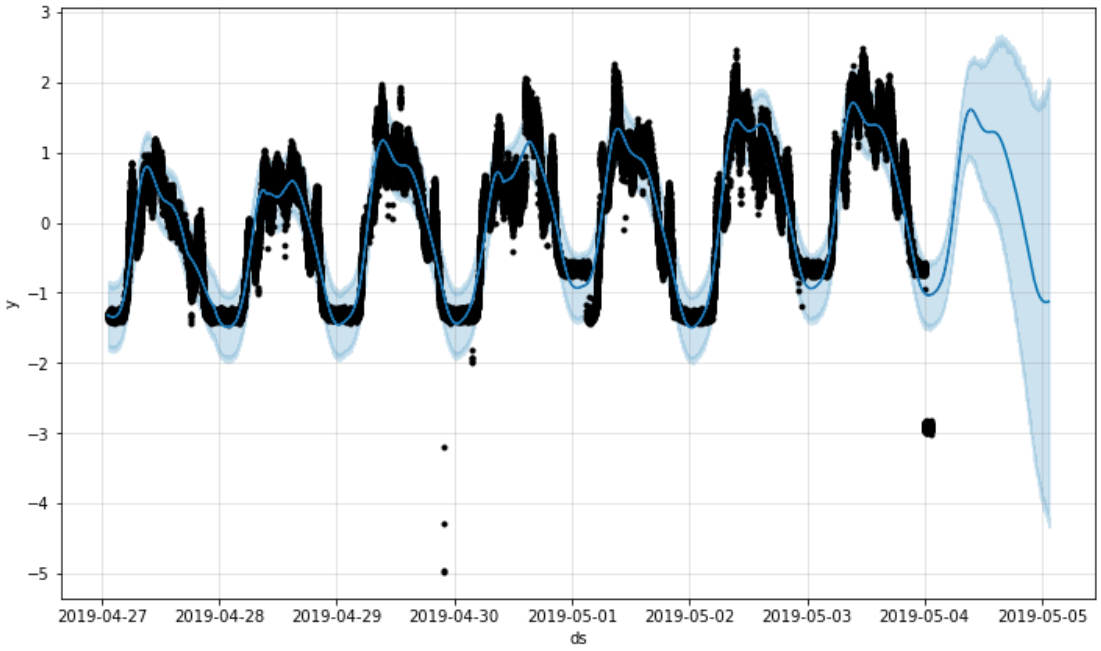


FIGURE 5.11 – Prévisions de tendance du trafic radar

nombre de messages de détection du radar. Les courbes bleues sont les mêmes données après avoir été normalisées pour correspondre aux données prédites. Les courbes bleu clair aux extrémités représentent ce qui a été prédit, c'est à dire l'intervalle de confiance pour la série temporelle. Ce sont les limites supérieures et inférieures raisonnables. Nous pouvons constater dans notre exemple que le procédé est en mesure de prédire correctement des valeurs pour l'évolution du nombre de message de détection sur une journée. Nous pouvons donc l'utiliser pour mettre en place un algorithme de détection qui va fonctionner ainsi :

— En entrée il prend un jeu de données avec les données temporelles et le nombre de paquets radars.
— On indique la durée de la série temporelle à prévoir.
— On sort ensuite les tendances futures des séries temporelles prédites.
— On peut également faire ressortir des indicateurs statistiques, comme la courbe ajustée, les limites supérieure et inférieure.
— On compare la donnée réelle avec cette courbe. En dehors des limites supérieure et inférieure, nous pouvons supposer qu'il y a eu une anomalie.

La méthode de Fbprophet peut ainsi être utilisée pour faire de la détection d'anomalies par rapport à l'évolution du nombre de messages de détection dans le temps de manière

efficace. Cependant, cette méthode ne permet pas de rentrer assez dans le détail des aéronefs. En effet, nous pourrions détecter des attaques par "*flooding*", c'est à dire par l'ajout massif d'avions dans les données véhiculées, ou au contraire par une suppression importante d'avions. Cependant, nous ne pourrions pas être en mesure de détecter des attaques plus fines par "*spoofing*" modifiant les données de quelques avions.

Cette méthode nous permet donc d'assurer un premier niveau de sécurité pour éviter une saturation du réseau ou une attaque cherchant à saturer ARTAS. Néanmoins, afin de se prémunir d'attaques plus fines, il est nécessaire d'avoir des méthodes de prédiction de données sur les caractéristiques des avions transportées dans les messages de détection.

5.3.2 Définition pour les modèles de Machine Learning

Description du problème Nous définissons une série temporelle à n dimensions $S = \{S_1, S_2, ..., S_C\}$, qui représente une fenêtre de séquence radar, où C est taille de la série temporelle.

$s_i = \{s_{i,1}, s_{i,2}, ...s_{i,n}\}(1 \leq i \leq C)$ est un vecteur à n dimensions, chaque dimension correspondant à un attribut du message.

Plus précisément, S représente une fenêtre composée de C message radar continu, et chaque vecteur S_i contient les informations obtenues à partir du message radar correspondant, à savoir la position, l'altitude et la vitesse.

Pendant la phase d'apprentissage, la série temporelle radar nomale est utilisée comme entrée de données d'apprentissage dans le modèle de détection d'anomalies, ce qui force la reconstruction de la séquence. Une fois l'entraînement terminé, lorsque la série temporelle correcte du radar est en entrée, l'erreur de reconstruction se situera dans une certaine plage. Cependant, lorsque la séquence contenant l'anomalie est utilisée comme entrée, l'erreur de reconstruction sera amplifiée, obtenant ainsi l'effet d'une détection anormale.

Définition du score anormal La similitude cosinus est utilisée pour représenter l'erreur de reconstruction entre le vecteur de sortie $\hat{S}$ et le vecteur d'entrée S, qui est défini comme suit (n est la dimension de l'entité) :

$$\cos\left(S_i, \hat{S}_i\right) = \frac{\sum_{j=1}^{n}\left(s_j \times \hat{s}_j\right)}{\sqrt{\sum_{j=1}^{n} s_j^2} \times \sqrt{\sum_{j=1}^{n} \hat{s}_j^2}}$$

.

Sur cette base, nous pouvons définir le score d'anomalies de reconstruction de la série

temporelle (avec C la longueur de la fenêtre en entrée) :

$$\text{Score d'anomalies} = \sum_{i=k}^{k+C} 1 - \cos\left(S_i, \hat{S}_i\right)$$

5.3.3 Détection d'anomalies basée sur le modèle LSTM

Pré-traitement des données

La série temporelle d'entrée est, dans un premier temps, une fenêtre composée de vecteurs à 4 dimensions, avec les informations TPN, TIME, RHO et THETA tels que présentés dans la section 4 dans le tableau 4.2. Nous utilisons ces données, car elles nous permettent d'identifier l'avion et de reproduire sa trace. Nous normalisons le temps "TIME" en numéro de série, car ce qui nous intéresse ici est l'enchainement des données.

Nous prenons ensuite les données d'un avion issues de notre jeu de données sur 500 valeurs. Comme un radar a un temps de rotation de 4sec, nous avons donc une représentation de l'évolution des valeurs pour 30 min. Nous leur injectons ensuite, par le biais de notre outil présenté dans 5.1, des données anormales. Nous choisissions de modifier les informations de position de ces appareils entre la centième et la cent cinquième valeurs, ce qui représente donc 6 données modifiées. Dans un premier temps, pour tester le principe de notre mécanisme de détection, nous modifions de 45 degrés la valeur de THETA et de 25 milles marins pour RHO.

Méthode et résultats pour la détection d'anomalies avec le modèle LSTM

Nous utilisons le réseau neuronal LSTM pour prédire les valeurs de Rho et de Theta, et nous entrainons le modèle sur des données de Rho et de Theta pour 10 jours afin d'avoir un temps suffisament long pour avoir un historique de l'évolution des Rho et des Theta. Grâce à ces données d'entrainement, nous sommes en mesure de prédire les valeurs de Rho et de Theta pour notre avion. Afin de prédire la séquence radar, nous utilisons le principe d'une fenêtre coulissante.

Après essai, nous choisissons une fenêtre d'une longueur de 10 qui nous permet de prédire efficacement nos données et qui de manière générale permet d'avoir des prédictions avec le moins d'erreurs, comme présenté dans [72].

Comme nous pouvons le voir dans le tableau 5.1, nous utilisons les 10 premières données pour prédire la 11e donnée, 2 à 11 pour prédire la 12e donnée, etc.

TABLE 5.1 – Exemple d'une fenêtre glissante

Données en entrée	Données prédites
[1,10]	[11]
[2,11]	[12]
...	...
[n,n+9]	[n+10]

Nous comparons cette valeur avec la valeur réelle et nous calculons le résidu. Nous déterminons ensuite les caractéristiques statistiques du résidu :

— la moyenne μ

— la variance σ

Grâce à la moyenne et à la variance, nous pouvons calculer le score d'anomalies qui correspons à la différence entre le résidu de l'ensemble du jeu de données de test et μ.

Le seuil anormal nous permettant d'affirmer s'il y a ou non une anomalie est définie comme étant 3σ (suivant la règle empirique de détection d'outlier des 3σ .

La figure 5.15 expose les résultats de notre exemple en représentant le score d'anomalie pour notre avion après une injection d'anomalies, les séquences modifiées étant marquées en rouge.

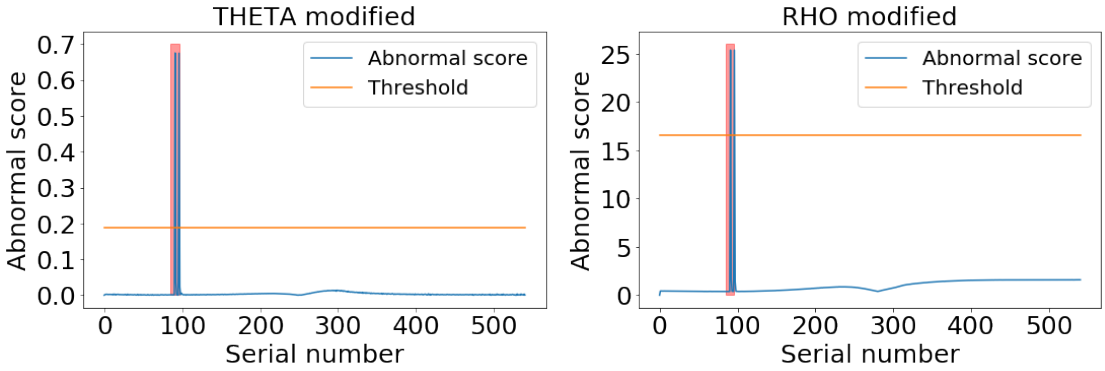


FIGURE 5.12 – Score d'anomalies de deux avions après injection d'une attaque par Spoofing

Notre procédé par méthode LSTM nous permet donc de détecter efficacement des séquences anormales sur l'évolution des caractéristiques RHO et THETA des avions.

Limites de la méthode

Même si la méthode LSTM présente des résultats efficaces pour un vecteur d'entrée à 4 dimensions, les données radars des avions ne se limitent pas à ces 4 attributs comme vu dans la section 4. En augmentant la dimension des séries temporelles, en ajoutant d'autres attributs d'une donnée radar tels que la vitesse, le cap ou les informations d'altitude, le taux de fausses alarmes générées dues à la reconstruction par la méthode LSTM se retrouve augmenté (voir Figure 5.13).

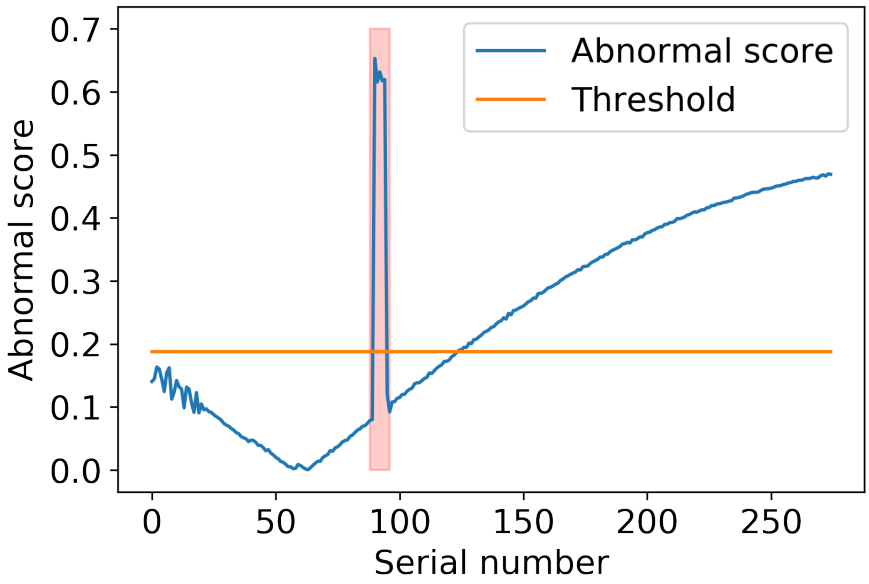


FIGURE 5.13 – Prédiction avec la méthode LSTM pour une modification de THETA de 45°

La méthode LSTM est donc un modèle efficace pour les données radars PSR qui ne vont transporter que les données de RHO et de THETA. Mais pour des données plus riches en attributs telles que ceux des SSR, il est donc nécessaire développer un autre modèle de reconstruction de série temporelle de données radars qui puisse prendre en entrée des séries temporelles de plus grandes dimensions sans augmenter en même temps le taux de fausses alarmes.

5.3.4 Détection d'anomalies basée sur le modèle de l'auto-encodeur

Afin de répondre à la problématique présenté dans la sous-section 5.3.3, nous avons développé un modèle basé sur un auto-encodeur, qui lui-même est intégré dans une unité

LSTM.

La figure 5.14 illustre le processus de détection d'anomalies mis en place.

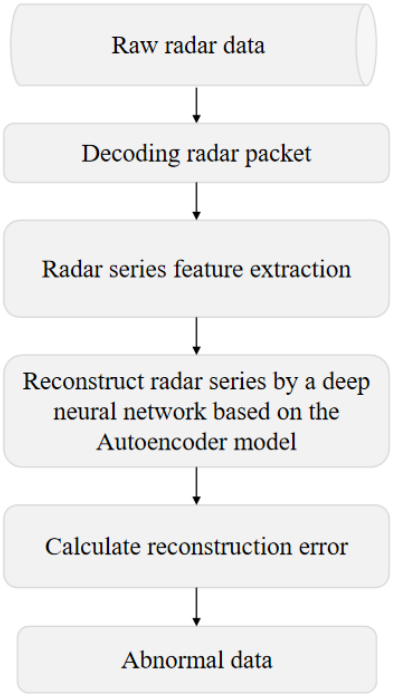


FIGURE 5.14 – Processus de détection d'anomalies

Prétraitement des données

Pour le modèle d'auto-encodeur, nous avons récupéré des données radars les attributs suivants :

- TPN : l'identifiant de la trace
- TS : le temps
- RHO et THETA : les coordonnées polaire du plot radar
- CGS : la vitesse
- CHDG : le cap

Nous exportons en CSV et les convertissons en une forme tridimensionnelle comprenant le numéro d'échantillon, la longueur de la fenêtre et enfin le nombre d'attributs. Nous utilisons ensuite le modèle sous la forme d'une fenêtre coulissante de taille 10 comme pour le LSTM. Le tableau 5.2 montre un exemple de données en entrée pour l'autoencodeur.

TABLE 5.2 – Exemple de données pour une fenêtre glissante.

INDEX	TPN	TS	THETA	RHO	CGS	CHDG	FL
0	3	1555729447	209.0533447	22.203125	453.2	218.704834	330.5
1	3	1555729451	209.2730713	22.69140625	457.6	218.7322998	330.5
2	3	1555729455	209.465332	23.171875	452.54	218.5015869	330.5
3	3	1555729459	209.6685791	23.66015625	454.08	218.5235596	330.5
4	3	1555729463	209.866333	24.140625	452.98	218.7432861	330.5
5	3	1555729467	210.0201416	24.6328125	456.06	218.1445313	330.5
6	3	1555729471	210.1904297	25.125	457.16	218.0291748	330.5
7	3	1555729475	210.3717041	25.61328125	455.4	218.4960938	330.5
8	3	1555729479	210.50354	26.10546875	454.74	218.0731201	330.5
9	3	1555729483	210.6793213	26.59765625	456.06	218.5180664	330.5
10	3	1555729487	210.8166504	27.08984375	456.06	218.4356689	330.5

Nous entrainons notre modèle sur un échantillonnage de 800 000 éléments de données comportant 100 vols distincts comme échantillons d'apprentissage.

Par la suite, nous reprenons le jeu de données utilisées dans la partie limite de la méthode LSTM présénté dans 5.3.3, et nous effectuons une attaque par Spoofing sur ce jeu de données. Plus précisément, par le biais de notre outil présenté dans 5.1, nous avons augmenté l'ensemble des attributs d'un taux de 10% (excepté le paramètre temps) . Nous faisons cette fois-ci deux attaques sur deux avions différents entre les numéros de séries 100 à 110 et 140 à 150 afin d'évaluer notre méthode.

Résultats pour l'utilisation de l'auto-encodeur

Nous représentons le score d'anomalies de ces deux avions après injection de l'attaque dans la figure 5.15. Les séquences modifiées sont marquées en rouge.
Dans un premier temps, nous pouvons constater que le modèle d'auto-encodeur que nous

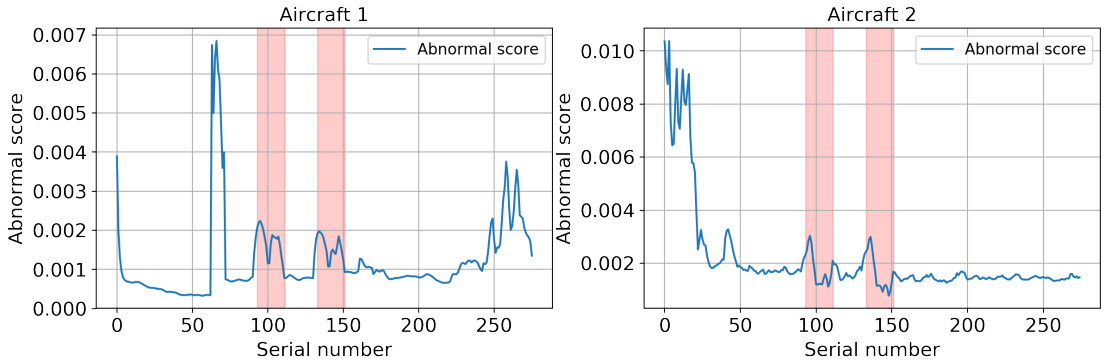


FIGURE 5.15 – Score d'anomalies de deux avions après injection d'une attaque par Spoofing

avons développé ne permet pas de faire ressortir les données modifiées. En effet, celles-ci peuvent être confondues avec des fluctuations déjà présentes dans le jeu de données (des cas de données anormales que nous pouvons trouver dans notre jeu de données que nous

présentons dans la section 6.2).

Comme nous l'avons vu dans 5.2.3, ce problème est intrinsèquement lié à la détection d'anomalies à partir des séries temporelles, telles que les données radars, pour l'auto-encodeur, c'est pour cela qu'il est nécessaire d'amplifier les anomalies pour être en mesure de les détecter, en faisant l'enrichissement des paramètres que nous avons présentés dans 5.2.3.

Reprenons les deux avions de notre exemple de la figure 5.15 pour lesquels nous avons enrichi nos données. Nous pouvons remarquer dans la figure 5.16 qu'après une extraction profonde des données, l'impact de l'anomalie injectée sur le score d'anomalies est considérablement agrandi. Nous sommes donc en mesure de résoudre la problématique de détecter l'anomalie dans un trafic avec des événements normaux provoquant une fluctuation du score d'anomalies en reprenant un seuil de détection de 3σ.

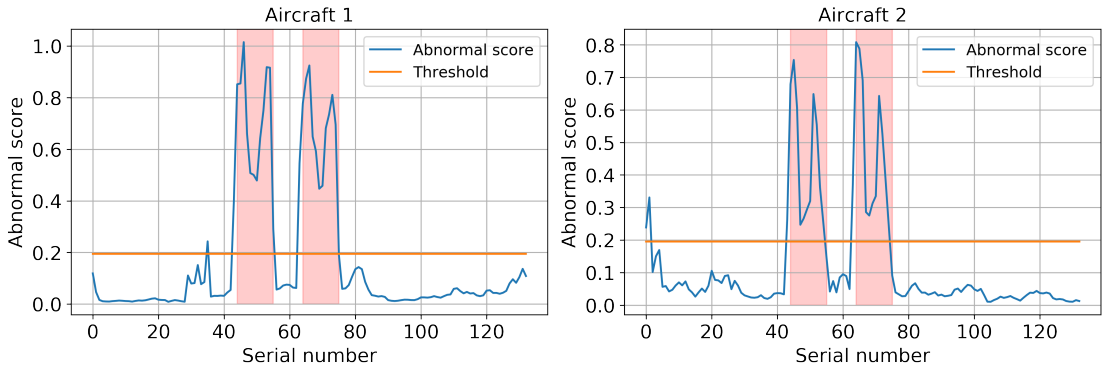


FIGURE 5.16 – Score d'anomalies de deux avions après l'injection d'une attaque par Spoofing (après extraction profonde des données)

Notre méthode de détection d'anomalies basée le modèle d'auto-encodeur semble donc présenter des résultats encourageants pour détecter les attaques par usurpation d'identité sur les attributs des données radars. En effet, il résout le problème de dimensionnement du vecteur d'entrée existant pour la méthode LSTM, et permet de conserver les propriétés de mémoire de cette méthode qui semble nécessaire aux données radars.

Dans la section suivante, nous confirmons l'efficacité de ce modèle par l'évaluation de résultats portants sur un ensemble d'anomalies d'usurpation de données qui peuvent être la conséquence d'une attaque par Spoofing que nous pouvons rencontrer dans le milieu radar.

5.4 Evaluation de la méthode

Dans cette section, nous évaluons notre modèle de détection basé sur un auto-encodeur en comparaison avec d'autres méthodes de détection utilisées pour les séries temporelles.

5.4.1 Description des anomalies d'usurpation de données.

Habler dans son document [38], décrit un certain nombre d'attaques pour les données radars ADS-B qui peuvent également être utilisées pour les données radars ASTERIX :

- **Déviation de tous les paramètres (ALL)** : Les anomalies sont générées en modifiant tous les paramètres (sauf le paramètre de temps) de 10%.
- **Déviation de theta (THETA)** : les anomalies sont générées en modifiant le paramètre THETA ; nous modifions de 45° les valeurs d'origine de ce paramètre.
- **Déviation de RHO (RHO)** : les anomalies sont générées en modifiant le paramètre RHO ; nous modifions de 25 miles marins les valeurs d'origine du paramètre.
- **Bruit aléatoire (RND)** : les anomalies sont générées en ajoutant du bruit aléatoire ; nous multiplions les valeurs d'origine des caractéristiques des données radars par un nombre aléatoire entre 0 et 2.
- **Route différente (ROUTE)** : les anomalies sont générées en remplaçant un segment des messages radar du vol testé par un segment de messages provenant d'une route différente (légitime). Dans l'expérience, nous avons remplacé 15 données d'un vol.
- **Dérive progressive de niveau de vol (DRIFT_FL)** : les anomalies sont générées sous forme d'une dérive progressive dans la fonction de niveau de vol. Cela se fait en modifiant le niveau de vol d'un segment de messages en augmentant ou abaissant continuellement le niveau de vol par un multiplicateur croissant de 400 pieds (c'est-à-dire que pour le premier message dans le segment anormal, le niveau de vol sera augmenté ou diminué de 400 pieds, le deuxième message sera augmenté ou diminué de 800 pieds, etc.). Pour l'expérience nous avons généré deux types de dérives progressives en augmentant la valeur d'altitude et en la diminuant.
- **Dérive progressive de vitesse (DRIFT_CGS)** : le fonctionnement est le même que pour la modification des niveaux de vol. Plus précisément, pour le premier message dans le segment anormal, la vitesse sera augmentée ou diminuée de 10 nœuds, le deuxième message sera augmenté ou diminué de 20 nœuds, etc. Pour l'expérience, nous avons également généré les deux types de dérives progressives en augmentant la valeur d'altitude et en la diminuant.

En reprenant le fonctionnement de ces attaques, nous les avons injectées par le biais de notre outil sur un jeu de données de tests avant de l'utiliser pour évaluer les méthodes de détection.

5.4.2 Métriques d'évaluation

Afin de pouvoir évaluer notre méthode, nous définissons nos métriques d'évaluation :

— Precision : La précision est le rapport des anomalies correctement prédites et détectées sur le total des anomalies prévues.

$$Precision = TP/(TP + FP)$$

— Recall (Sensibilité) : Le recall est le rapport des anomalies correctement prédites sur l'ensemble des anomalies effectivement présentes dans le jeu de données.

$$Recall = TP/(TP + FN)$$

— Score F1 : Le score F1 est la moyenne pondérée de la précision et du recall.

$$F1Score = 2 \times (Recall \times Precision)/(Recall + Precision)$$

TP, FP et FN définissent respectivement les Vrais Positifs (True Positif) , les Faux Positifs (False Positif) et les Faux Négatif (False Negatif). F1-Score construit l'équilibre entre la précision et le recall ; nous l'utilisons donc comme mesure principale d'évaluation dans nos expériences.

5.4.3 Résultat expérimental

La figure 5.17 nous permet de visualiser l'impact des attaques présentées précédemment sur le score d'anomalies des différents attributs d'un avion pendant sa phase de croisière.

Les résultats sont présentés dans le tableau 5.3.

Les mesures dans ce tableau nous montrent donc que l'utilisation de notre modèle d'auto-encodeur nous permet de détecter de manière efficace les anomalies injectées dans les données radars par des attaques redoutées par le monde de l'aviation civile. Le modèle d'auto-encodeur est donc un modèle efficace pour la détection d'anomalies

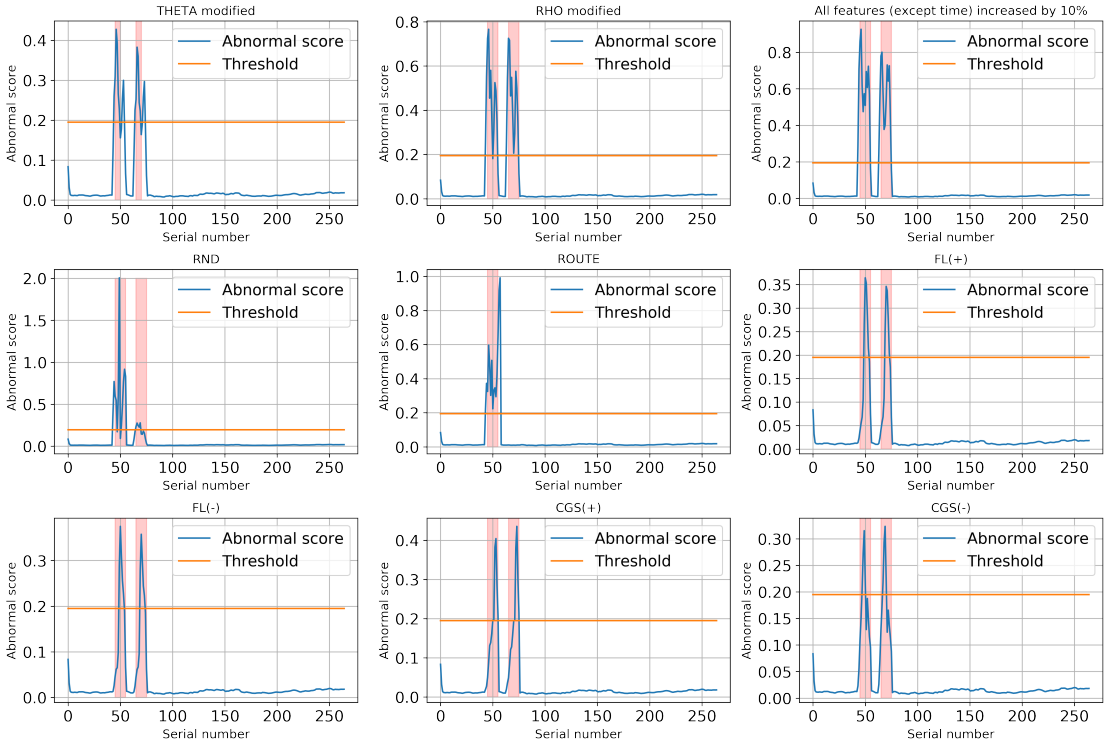


FIGURE 5.17 – Scores d'anomalies des caractéristiques modifiées d'un avion attaqué

TABLE 5.3 – Résultats Expérimentaux

	Precision	**Recall**	**F1 score**
THETA	0.8789	0.9835	0.9101
RHO	0.8893	0.9959	0.9288
ALL	0.8885	0.9959	0.9286
RND	0.8870	0.9969	0.9108
ROUTE	0.8887	0.9958	0.9289
FL(+)	0.8116	0.9669	0.8574
FL(-)	0.8337	0.9835	0.8792
CGS(+)	0.8199	0.9793	0.8730
CGS(-)	0.8290	0.9876	0.8788

dédiée à l'ATC.

Par la suite, nous comparons notre modèle avec d'autres modèles courants de détection

d'anomalies pour les séries temporelles.

5.4.4 Comparaison avec d'autres modèles courants de détections d'anomalies

Comparaison avec le LSTM

Dans un premier temps, nous comparons nos modèles de LSTM et d'auto-encodeur, afin de déterminer si effectivement l'auto-encodeur se révèle être plus efficace pour les données radars. Les résultats du tableau 5.4, nous montre donc bien l'efficacité des deux méthodes mais avec des résultats plus significatifs pour l'auto-encodeur.

TABLE 5.4 – Comparaison des résultats des méthodes LSTM et auto-encodeur

Method	Evaluation	THETA	RHO	ALL	RND	ROUTE	FL(+)	FL(-)	CGS(+)	CGS(-)	MEAN
LSTM	Precision	**0.9074**	**0.9983**	0.8884	**0.8915**	**0.9220**	**0.9339**	**0.9972**	0.7741	0.7782	**0.8990**
	Recall	0.8884	**1.0000**	0.9587	0.8760	0.7833	0.9008	**1.0000**	0.9669	**0.9959**	0.9300
	F1 score	0.8944	**0.9991**	0.9014	0.8585	0.8141	**0.9118**	**0.9983**	0.8169	0.8293	0.8915
Autoencoder	Precision	0.8789	0.8893	**0.8885**	0.8870	0.8887	0.8116	0.8337	**0.8199**	**0.8290**	0.8585
	Recall	**0.9835**	0.9959	**0.9959**	**0.9669**	**0.9958**	**0.9669**	0.9835	**0.9793**	0.9876	**0.9839**
	F1 score	**0.9101**	0.9288	**0.9286**	**0.9108**	**0.9289**	0.8574	0.8792	**0.8730**	**0.8788**	**0.8995**

Comparaison avec des modèles de détection non supervisée

Nous comparons ensuite notre modèle avec trois autres modèles de détections d'anomalies pour les séries temporelles, présentés dans l'Etat de l'Art à la section 3 :

SVM Le modèle SVM est un modèle d'apprentissage supervisé qui analyse les données et reconnait des modèles, et qui peut être utilisé pour les tâches de classification et de régression. Le modèle SVM reçoit un ensemble de donnés d'apprentissage exemples étiquetés comme appartenant à l'une des deux classes. Il représente les données sous forme de points dans l'espace, mappés de manière à ce que les données de catégories distinctes soient divisées par un espace clair aussi large que possible. De nouvelles données sont ensuite mappées dans ce même espace et sont réparties suivant une catégorie ou une autre, en fonction de côté de l'écart sur lequel ils tombent. Si les données nouvellement rencontrées sont trop différentes selon certaines mesures, de ce modèle, elles sont étiquetées comme hors classe.

LOF (Local outlier factor) Le LOF est basé sur un concept de densité locale, où la localité est donnée par k voisins les plus proches, dont la distance est utilisée pour estimer

la densité. En comparant la densité locale d'un objet aux densités locales de ses voisins, on peut identifier des régions de densité similaire, et des points qui ont une densité sensiblement plus faible que leurs voisins. Ceux-ci sont considérés comme des valeurs aberrantes. La densité locale est estimée par la distance typique à laquelle un point peut être « atteint» par ses voisins.

Isolation Forest Le modèle d'Isolation Forest est une méthode « classique » de détection d'anomalies non supervisée adaptée aux données continues. Il a été proposé pour la première fois par le professeur Zhou Zhihua de l'Université de Nanjing en 2008, puis une version améliorée a été proposée en 2012. D'autres modèles de détection d'anomalies décrivent le degré d'aliénation entre les échantillons par des indicateurs quantitatifs tels que la distance et la densité, tandis que le modèle d'Isolation Forest détecte les valeurs aberrantes en isolant les points d'échantillonnage. Plus précisément, le modèle isole l'échantillon à l'aide d'une structure d'arbre de recherche binaire appelée arbre isolé. Étant donné que le nombre de valeurs aberrantes est petit et éloigné de la plupart des échantillons, les valeurs aberrantes sont isolées plus tôt, c'est-à-dire qu'elles sont plus proches du nœud racine et que les valeurs normales sont plus éloignées du nœud racine.

Résultat expérimental Nous avons comparé les performances de notre modèle suivant les différentes anomalies présentées précédemment avec les performances de ces différents modèles. Les résultats globaux sont présentés dans le tableau 5.5. Les résultats montrent que notre modèle d'auto-encodeur basé sur l'apprentissage en profondeur donne de meilleurs résultats dans la plupart des cas.

Table 5.5 – Comparaison des méthodes de détection

Method	Evaluation	THETA	RHO	ALL	RND	ROUTE	FL(+)	FL(-)	CGS(+)	CGS(-)	
OCSVM	Precision	0.8387	0.5532	0.8744	0.9128	0.8433	0.6173	0.4737	0.8713	0.8188	
	Recall	0.4333	0.1083	0.7542	0.8292	0.7063	0.2083	0.0750	0.6208	0.4708	
	F1 score	0.5714	0.1812	0.8098	0.8690	0.7687	0.3115	0.1295	**0.7251**	**0.5979**	
LOF	Precision	0.2149	0.1756	0.3988	0.4628	0.3106	0.1860	0.1921	0.3843	0.3492	
	Recall	0.4333	0.3542	0.8042	0.9333	0.8333	0.3705	0.3875	0.7750	0.7042	
	F1 score	0.2873	0.2348	0.5331	0.6188	0.4525	0.2486	0.2570	0.5138	0.4669	
IF	Precision	0.7653	0.6207	0.8812	0.9020	0.7349	0.2810	0.2745	0.5183	0.5504	
	Recall	0.3125	0.2250	0.7417	0.9208	0.3815	0.1417	0.1167	0.3542	0.2958	
	F1 score	0.4438	0.3303	0.8054	0.9113	0.5021	0.1884	0.1637	0.4208	0.3848	
LSTM	Precision	**0.9074**	**0.9983**	0.8884	**0.8915**	**0.9220**	**0.9339**	**0.9972**	0.7741	0.7782	**0.8990**
	Recall	0.8884	**1.0000**	0.9587	0.8760	0.7833	0.9008	**1.0000**	0.9669	**0.9959**	0.9300
	F1 score	0.8944	**0.9991**	0.9014	0.8585	0.8141	**0.9118**	**0.9983**	0.8169	0.8293	0.8915
Autoencoder	Precision	0.8789	0.8893	**0.8885**	0.8870	0.8887	0.8116	0.8337	**0.8199**	**0.8290**	0.8585
	Recall	**0.9835**	0.9959	**0.9959**	**0.9669**	**0.9958**	**0.9669**	0.9835	**0.9793**	0.9876	**0.9839**
	F1 score	**0.9101**	0.9288	**0.9286**	**0.9108**	**0.9289**	0.8574	0.8792	**0.8730**	**0.8788**	**0.8995**

5.5 Conclusion

Dans ce chapitre, nous avons proposé trois méthodes de détection d'anomalies dédié aux données radars. La première, en se plaçant au niveau des flux radars nous permet de s'appuyer sur la signature caractéristique de l'évolution des messages de détection dans le temps pour prédire les données futures. Cette méthode s'appuie sur le modèle Fbprophet qui donne des résultats efficace en terme de prédiction pour les séries temporelles avec des caractéristiques qui se répètent dans le temps. La deuxième et la troisième méthode rentre plus dans le détail des informations des avions puisqu'elles permettent de faire de la détection d'anomalies au niveau des attributs des données radars. Ces méthodes s'appuient sur les algorithmes DNN LSTM et d'auto-encodeur. Bien que la méthode LSTM permette de donner des résultats efficace en terme de détection d'anomalies sur les données radars qui ont subies une attaque par *Spoofing*, celle-ci présente des limitations lorsque le vecteur d'entrée au niveau des données est trop grand. Or, lorsque nous utilisons les données radars, nous avons un vecteur d'entrée avec plusieurs attributs. C'est pourquoi, nous avons continué l'emploi des algorithmes DNN en utilisant un auto-encodeur basé sur des couches LSTM. Cette méthode de détection nous permet de détecter efficacement les anomalies dans un jeu de donnée attaqué. En comparant notre méthode de prédiction avec d'autres méthodes de détection d'anomalies statistiques pour les séries temporelles, nous pouvons voir que la méthode avec auto-encodeur permet une meilleure détection d'anomalies pour les données radars. En effet, le score F1, permettant de mesurer l'efficacité de la détection, pour notre méthode est supérieur dans la majorité des attaques testés. Le chapitre suivant fait une ouverture sur d'autres utilisations de cette méthode d'auto-encodeur.

6 Ouverture

Ce chapitre présente deux applications de notre méthode de détection d'anomalies. La première pour caractériser notre jeu de données, la deuxième pour tester la méthode sur d'autres type de données.

6.1 Utilisation de la méthode sur d'autres jeux de données.

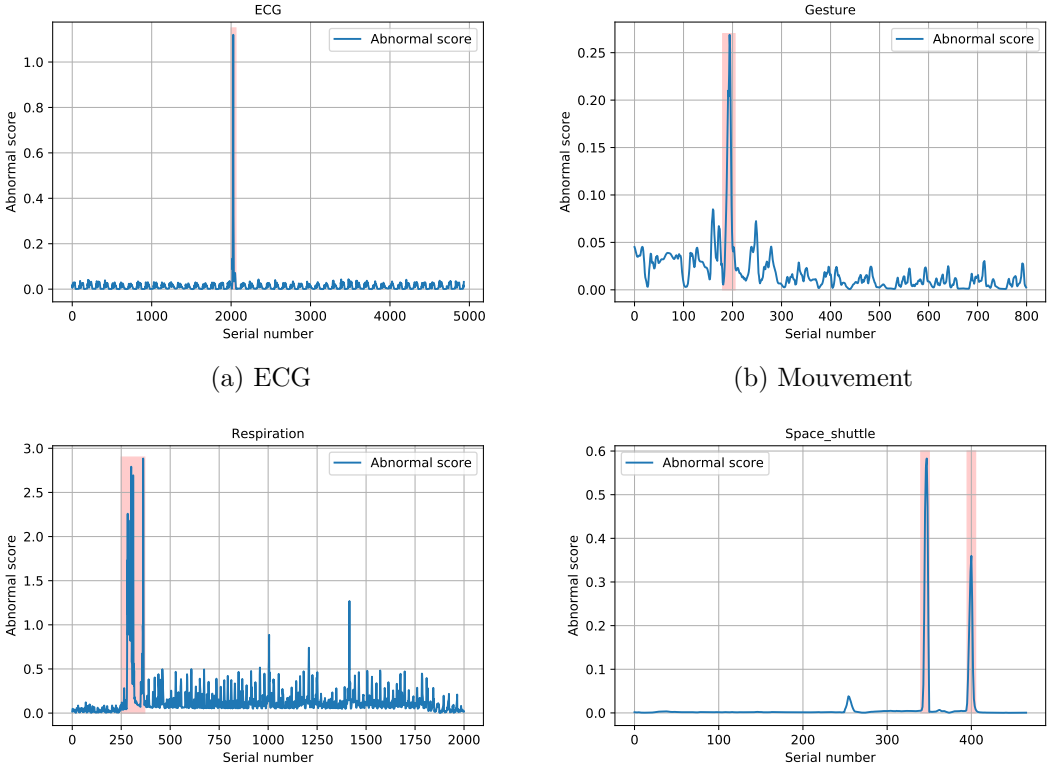
Afin de voir si notre méthode pourrait s'adapter à d'autres données, nous avons effectué des tests de détection d'anomalies préliminaires sur des jeux de données publics issus d'ICS [54] : les données traitées sont des séries temporelles issues d'électrocardiogramme, de données de reconnaissance de mouvement, de données respiratoires et d'autres issues de différents capteurs d'une navette spatiale.

Lorsque nous avons fait le test à partir des données d'ECG, nous avons constaté que des anomalies peuvent être détectées sans enrichir les fonctionnalités. Cependant, pour vérifier que l'enrichissement des fonctionnalités n'altère pas l'effet de détection, nous avons testé le jeux de données avec cette étape. Les résultats obtenus sont illustrés dans la figure 6.1, avec la zone rouge, une zone présentant potentiellement des anomalies.

Nous pouvons donc voir que la méthode d'auto-encodeur dévelopée dans nos travaux a un effet de détection sur ces données. Ces résultats sont prometteurs et montrent que la méthode proposée peut être appliquée à un contexte différent avec des données aux propriétés similaires à celles des données radars. Une étude plus approfondie sur ces jeux de données pourra faire l'objet de travaux futurs.

6.2 Analyse des données suspectes

Nous avons utilisé un jeu de données opérationnelles issu directement du réseau ATC français qui subit les aléas système réel. Ainsi, ces données, n'ayant pas fait l'objet de signalements particuliers de la part de la DGAC, que nous considérons donc comme "normales" d'un point de vue d'un fonctionnement opérationnel, peuvent comporter des anomalies.



(a) ECG

(b) Mouvement

(c) Respiration

(d) Navette spatiale

FIGURE 6.1 – Détection d'anomalie par autoencodeur appliquée à d'autres jeu de données

Nous avons décidé d'analyser ces données à l'aide d'une expertise aéronautique pour être en mesure d'identifier des séquences anormales.

En utilisant notre méthode de détection à l'aide du modèle d'auto-encodeur, nous identifions dans notre jeu de données quatre cas susceptibles de provoquer un score d'anomalies élevé et donc de déclencher une détection d'anomalie.

— **Un changement d'angle normal** : Lorsqu'un avion traverse une zone radar verticalement, la valeur de du THETA peut passer de 0° à 360° ou inversement. Numériquement, cela crée un écart important (comme nous pouvons le voir dans le Tableau 6.1). Ainsi, même si cette situation est normale, elle provoquera une augmentation du score d'anomalies.

— **Point de changement** : Lorsqu'un avion va changer de vitesse de manière anormale, cela va déclencher un score d'anomalies élevé et donc la possibilité pour nous de le détecter. Ce cas est illustré dans notre jeu de données grâce au Tableau 6.2.

Table 6.1 – Cas 1 : Exemple de changement d'angle

INDEX	TPN	TS	THETA	RHO	CGS	CHDG	FL
72	0	1555734236	0.565795898	134.703125	495.66	223.7475586	380
73	0	1555734244	**0.236206055**	133.9023438	496.76	224.0222168	380
74	0	1555734252	**359.967041**	133.1054688	496.32	223.6322021	380
75	0	1555734260	359.5770264	132.3085938	497.42	223.8409424	380

Table 6.2 – Cas 2 : Exemple de point de changement

INDEX	TPN	TS	THETA	RHO	CGS	CHDG	FL
0	0	1555733675	15.92468262	197.0742188	**345.4**	218.1994629	380
1	0	1555733683	15.77636719	196.1289063	**401.28**	219.5507813	380

— **Interruption dans la continuité des données** : Dans un ensemble de données, il se peut que des données soient perdues. Ces pertes peuvent être dues à la transmission, à une perte normale (le cône radar du silence) ou à une anomalie. Nous sommes donc en mesure de le détecter par l'augmentation des scores d'anomalies que cela génère (voir le Tableau 6.3).

Table 6.3 – Cas 3 : Exemple d'interruption dans la continuité des données

INDEX	TPN	TS	THETA	RHO	CGS	CHDG	FL
261	0	1555735758	287.3638916	135.2265625	275.22	222.5500488	46.5
262	0	**1555735767**	287.2595215	135.4921875	276.98	222.62146	46.5
263	0	**1555735799**	286.3970947	135.8164063	259.82	182.543335	46.5
264	0	1555735807	286.1169434	135.7304688	249.92	188.5968018	46.5

— **Séries temporelles avec de violentes fluctuations** : Il peut y avoir des cas où la vitesse de l'avion continue de fluctuer alors qu'elle ne le devrait pas, des valeurs qui semblent être aberrantes par rapport aux autres, etc, ce qui semble indiquer des anomalies du jeu de données. (Tableau 6.4). La méthode par auto-encodeur permet de détecter cela.

Ces cas peuvent être anormaux ou faire partie du comportement normal d'un trafic radar. Néanmoins, il est utile dans tous les cas de pouvoir détecter ces comportements. Dans notre jeu de données, nous pouvons trouver ces quatre cas avec deux avions iden-

TABLE 6.4 – Cas 4 : Exemple de séries temporelles avec de violentes fluctuations

INDEX	TPN	TS	THETA	RHO	CGS	CHDG	FL
0	2	1555727016	347.9919434	129.9882813	**339.9**	266.2701416	149
1	2	1555727020	347.8381348	129.9140625	**362.12**	276.1248779	150.5
2	2	1555727024	347.6513672	129.8359375	**437.14**	230.6689453	152.25
3	2	1555727028	347.2338867	129.7695313	**524.26**	235.1239014	154
4	2	1555727032	347.409668	129.6914063	**330.44**	262.4798584	155.75
5	2	1555727036	347.041626	129.6171875	**427.24**	265.9240723	157.5
6	2	1555727040	346.9812012	129.546875	**405.24**	233.2672119	159
7	2	1555727044	346.706543	129.4804688	**378.18**	227.9278564	160.75
8	2	1555727048	346.4978027	129.4140625	**498.96**	265.8251953	162.5
9	2	1555727052	346.3879395	129.3476563	**341.88**	264.5562744	164.5
10	2	1555727056	346.1737061	129.28125	**401.94**	229.3341064	166.5
11	2	1555727060	346.0144043	129.2226563	**377.74**	230.2624512	168.25
12	2	1555727064	345.8551025	129.1601563	**318.34**	262.4414063	169.75
13	2	1555727068	345.6298828	129.0976563	**399.08**	265.0012207	171.25
14	2	1555727072	345.4760742	129.0390625	**384.34**	231.8444824	172.75
15	2	1555727076	345.2508545	128.9804688	**403.48**	230.355835	174.25
16	2	1555727080	345.0091553	128.9257813	**478.94**	266.2481689	175.75
17	2	1555727084	344.9926758	128.875	**303.82**	261.7327881	177
18	2	1555727088	344.6520996	128.8164063	**388.52**	227.9553223	178.5
19	2	1555727092	344.6081543	128.7617188	**378.84**	232.3168945	180
20	2	1555727095	344.3939209	128.7109375	**291.28**	262.3260498	181.25
21	2	1555727099	344.1467285	128.65625	**472.78**	264.3859863	182.75
22	2	1555727103	343.9874268	128.609375	**388.3**	232.4761963	184

tifiés.

Nous représentons donc les scores d'anomalies de ces deux avions dans la Figure 6.2.

Les pics représentés sur ces figures correspondent aux quatre cas d'anomalies identifiés, ce qui nous permet de distinguer efficacement avec la méthode d'auto-encodeur ces anomalies des données normales.

A la vue de ces différents cas, des contrôleurs aériens ont pu nous dire que le cas de

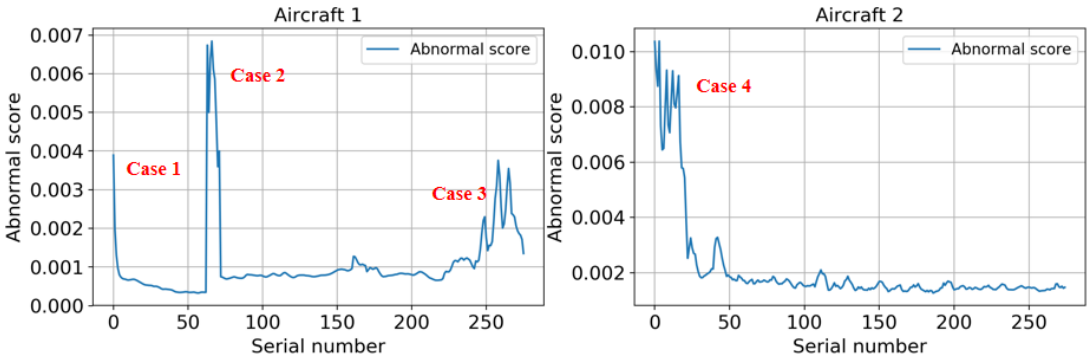


FIGURE 6.2 – Score d'anomalies de deux avions illustrant les quatre cas d'anomalies

changement d'angle n'avait pas besoin d'être qualifié comme anormal comme cela arrive régulièrement. Nous utilisons donc une fonction sinus pour représenter le paramètre THETA, afin d'éviter de lever une anomalie à chaque changement et donc ainsi augmenter le taux de faux positifs.

Les résultats expérimentaux montrent que les effets de changement d'angle sont ainsi complètement éliminés, comme nous pouvons le voir dans la figure 6.3 sur laquelles les données en bleu représentent le score d'anomalie pour un avion avec des pics causé par les oscillations d'angle pour THETA et CHDG et celles en rouge, le le score d'anomalies pour le même avion après avoir utilisé la fonction sinus.

Pour ce qui est des autres cas , nous pouvons expliquer les anomalies comme l'interruption dans la continuité des données par des contraintes opérationnelles. Néanmoins, cela ne veut pas dire que toutes les interruptions de données et toutes celles détectées puissent être expliquées ou se régler pour le moment.

Des prochains travaux pourraient donc porter sur la caractérisation du jeu de données et l'identification des anomalies détectées à l'aide de notre auto-encodeur. Ces travaux sont à mener en lien avec des experts de la navigation aérienne, afin de développer une meilleure connaissance des cas que nous pouvons rencontrer dans un jeu de données radars opérationnelles et ainsi affiner notre méthode de détection à la lumière de ces anomalies.

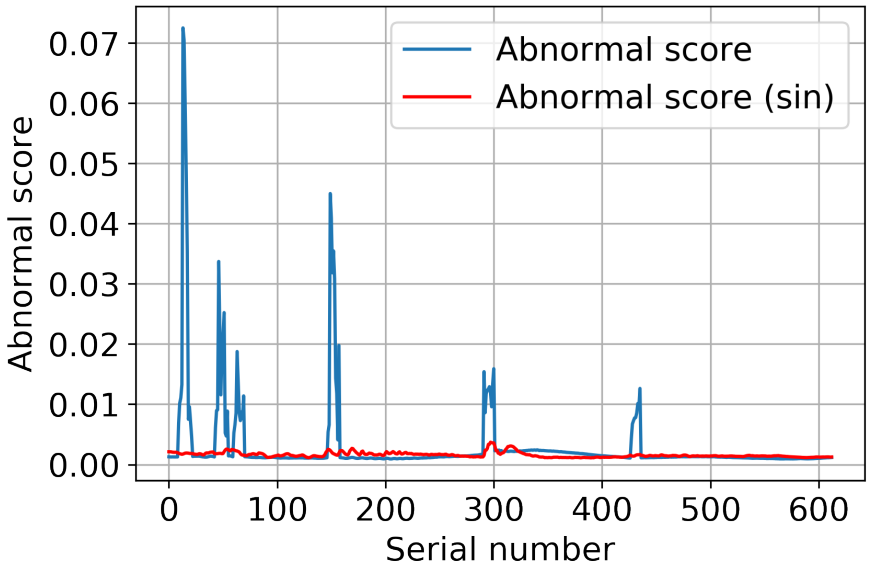


FIGURE 6.3 – Score d'anomalies reconstruit pour un avion après un mapping sinusoïdal

6.3 Conclusion

Dans ce chapitre, nous avons pu utiliser notre méthode d'auto-encodeur sur notre jeu de données radars. Nous avons pu ainsi identifier plusieurs anomalies existantes sur ce jeu de données. En travaillant avec des experts de l'aviation civile, nous avons identifier la cause de certaines de ces anomalies qui sont présentées comme "normales" pour des données radars. Néanmoins, il reste certaines anomalies qui n'ont pas pu être identifiées. Il est donc nécessaire lors d'un prochain travail de labelliser ce jeu de données, en lien avec des experts du contrôle aérien, afin d'avoir un jeu de données qui puissent être utiliser dans d'autres travaux. Nous avons également pu utiliser notre méthode de détection avec auto-encodeur sur d'autres jeux de données d'ICS présentant des caractéristiques similaires aux données radars. Nous avons vu que cette méthode peut-être un mécanisme de détection d'anomalies prometteurs pour ce type de donnée.

7 Conclusion et perspectives

7.1 Conclusion

Dans cette thèse, nous avons présenté trois contributions majeures dans le domaine radar pour l'aéronautique :

— Une caractérisation sur l'évolution temporelle des flux de données radars comme série temporelle. Grâce à cette caractérisation, nous avons identifié une signature qui se répète quotidiennement au niveau radar et la définition d'un trafic normal pour les données radars.

— Le développement d'une méthode de détection d'anomalies prédictives au niveau des flux radars et des traces des avions. Cette méthode, se basant sur les modèles Fbprohet, LSTM et autoencodeur, peut être élargie aux séries temporelles avec des attributs similaires aux données radars, telles que celles issues des ICS.

— La détection d'anomalies présentes sur un jeu de données opérationnelles de l'aviation civile.

La réalisation de ces travaux nous ont permis également deux avancées techniques dans le domaine des radars :

— La création d'un jeu de données radars du 19-04-2019 au 31-12-2020, issu du système opérationnel ATC français qui pourra être utilisé dans d'autres travaux tels que l'analyse plus approfondie sur le comportement des données radars ou l'impact de la Covid19 sur le trafic aérien.

— La création d'un outil d'injection de données radars, qui permet de forger ses propres données radars à partir de rien et donc de créer facilement des attaques, pouvant modifier le système radar, dans le but de les étudier et de s'en prémunir.

Ces travaux ont été orientés par le contexte de cyber menace de plus en plus préoccupant dans le système aéronautique. En effet, ces systèmes dédiés deviennent, par leur importance stratégique, de nouvelles cibles d'attaques. Il y a donc une nécessité de trouver des moyens de protéger les systèmes aéronautiques, en particulier le système de contrôle aérien, des attaques potentielles qu'ils peuvent craindre.

Au cours de nos travaux, notre principale préoccupation était de prendre en compte

les spécificités du réseau radar par rapport à un système informatique traditionnel. Ces spécificités comportent notamment des contraintes en termes de ressources. Par conséquent, nous avons identifié la détection d'anomalies comme une solution encourageante pour se prémunir des attaques dans un système ATC, car elle présente la particularité d'être non intrusive.

Une analyse de risques ayant été faite au sein du système ATC, nous pouvons voir que le système radar est au cœur du contrôle aérien ; les modifications au niveau des données radars pourraient entraîner des accidents aboutissant à un bilan humain, stratégique ou financier important. Dans cet esprit, notre principale préoccupation était de savoir comment détecter au mieux les attaques au sein de ce système radar.

Grâce à une revue de la littérature, nous avons identifié plusieurs approches qui tentent de répondre à cette question. La détection d'anomalies pour les données radars ne fonctionnent pas avec des méthodes de détection d'anomalies que l'on peut retrouver habituellement dans les systèmes informatiques. En effet, du fait que les données radars ont été peu étudiées, les méthodes existantes d'IDS ne considèrent leur particularité. De plus, il faut prendre en compte le fait que les données soient des séries temporelles avec des attributs indépendants entre eux, mais une forte corrélation avec le temps. Il faut également noter que la mémoire des données est importante, puisque les données présentes sont corrélées avec les données futures. Ces défis par rapport aux données radars nous permettent de nous rapprocher des défis qui existent pour les données issues des ICS. Ainsi, par rapport à la littérature sur les ICS, nous sommes en mesure de faire des propositions qui ont été appliquées dans nos contributions.

Nous nous sommes ainsi intéressés à la détection d'anomalies par prédiction. En effet, comme les données radars ont une forte corrélation dans le temps et que chaque attribut a une corrélation avec ses valeurs passées, nous pouvons prédire les données futures. Grâce à cette prédiction, nous comparons les valeurs prédites et les valeurs réelles ; l'écart entre les deux nous permet de déterminer si nous avons potentiellement des anomalies.

Néanmoins, avant de faire nos prédictions, nous nous sommes intéressés aux données radars et à leur comportement. En menant une analyse exploratoire sur les données, nous avons été en mesure de déterminer une signature sur l'évolution temporelle des flux de messages de détection pour les données radars. Cette signature va se retrouver quotidiennement et permet de définir le comportement normal d'un flux radar.

En se basant sur cette signature, nous avons développé un premier mécanisme de détection au niveau des flux grâce au modèle Fbprophet. Celui-ci permet de prédire

efficacement des données présentant une signature qui se répètent dans le temps. Ce mécanisme de détection d'anomalies basé sur un modèle de prédiction de flux permet de se prémunir d'attaques de type *flooding* qui inonderaient le système de fausses données ou au contraire d'attaques qui supprimeraient un nombre important d'avions. Néanmoins, lorsque nous avons des attaques par *spoofing* entraînant des modifications plus fines des avions au niveau des attributs, nous avons besoin de rentrer plus en profondeur dans les données.

Pour rentrer plus en profondeur dans les attributs des données radars et être en mesure de se prémunir de ces attaques par *spoofing*, en se basant sur la littérature pour les ICS, nous avons développé une méthode de détection par apprentissage en se basant sur les DNN.

— Dans un premier temps, nous avons utilisé un algorithme de LSTM pour prédire les données. Bien que cet algorithme nous permettait de prédire efficacement les données radars PSR et donc mettre en place de la détection d'anomalies, lorsque nous passions avec des données SSR, comprenant plus d'attributs et un vecteur d'entrée de dimension plus importante, les résultats ne permettaient pas de faire de la détection d'anomalies efficacement.
— Pour répondre à ce problème de dimension, nous sommes passés dans un second temps avec un modèle d'auto-encodeur basé sur des couches LSTM. Grâce à ce modèle, nous pouvons répondre à nos attentes en termes de détection pour les données radars.

Les propositions ci-dessus ont été mises en œuvre et évaluées à partir de données issues du réseau opérationnel de l'aviation civile française. Nous avons simulé sur ce jeu de données des attaques redoutées par les experts du contrôle aérien, à partir d'un outil que nous avons développé, afin de mesurer l'efficacité de notre approche par rapport à d'autres approches plus classiques. Nous avons également été en mesure d'utiliser notre approche sur d'autres données issues des ICS avec des caractéristiques similaires aux données radars. Si les résultats montrent que les approches proposées sont prometteuses pour les données radars et pour les ICS, de nouvelles perspectives pour ces travaux peuvent être envisagées pour améliorer leur portée et leur applicabilité.

7.2 Perspective

Nous présentons ici de potentiels travaux futurs par rapport à nos approches de détection d'anomalies pour les données radars.

— Dans un premier temps, nos travaux ont été effectués à posteriori, c'est à dire que nous avons mis en place notre méthode de détection d'anomalies sur des données extraites du réseau et que nous les avons analysées à posteriori. La prochaine étape consisterait à prendre en compte l'étape de temps réel et tester notre mécanisme sur un système opérationnel.

— Nous avons également l'intention de développer d'autres attaques dédiées au système radar, toujours dans le but de tester nos méthodes. L'idée est de réaliser les attaques les plus réalistes possible, en partenariat avec un contrôleur aérien, pour se rapprocher d'un contexte opérationnel et des attentes sur le terrain. Par la suite nous testerons nos outils d'injection et de détection sur des réseaux et machines proches d'un contexte opérationnel dans le contexte temps réel. Cela nous permettra de mieux caractériser le trafic réel et de pouvoir tester la réaction des outils déjà en place sur le réseau opérationnel.

— Au cours de nos travaux, nous avons pu collecter un jeu de données importantes issues l'aviation civile. Ce jeu de données brutes mériterait d'être étudié, en lien avec des experts aéronautiques, avec notre méthode de détection d'anomalies afin de le labelliser et l'utiliser dans d'autres travaux de recherches pour l'aviation civile. Ce jeu de données labellisé, nous pourrions mener une analyse plus fine sur les données radars afin d'être en mesure de mieux comprendre leur fonctionnement et ainsi proposer des outils encore plus adaptés à leur comportement. De plus, nous avons la chance d'avoir pu collecter notre jeu de données pendant la crise du Covid19 ; nous pourrions envisager une étude sur l'impact de cette pandémie sur le trafic aérien.

— Nous avons pu voir que la problématique des données radars s'étendait à certaines données d'ICS issues de séries temporelles. Bien que nous avons fait des tests préliminaires sur certains jeux de données d'ICS, nous pourrions mener une étude plus approfondie sur l'efficacité de notre approche par rapport aux autres approches plus récentes pour les ICS.

— Notre méthode de détection s'est basée entre autre sur un seuil de détection d'anomalies fixe que nous avons défini de manière empirique. Une autre méthode pourrait être de mettre en place un seuil adaptatif [16] en fonction du temps et des différents attributs. Dans le cas d'un seuil fixe, si nous avons un flux de données en temps

réel, il se peut que la distribution change violemment ; par conséquent une anomalie peut-être détectée alors que ça n'en est pas vraiment une, augmentant ainsi le taux de fausses alarmes. Nous pourrions utiliser le principe de fenêtre glissante, comme pour l'auto-encodeur, afin de mettre à jour notre seuil. Cela se fait déja pour l'utilisation des voitures autonomes [40].

— Un projet différent en cours de discussion est de pouvoir utiliser notre outil d'injection d'attaques sur le système opérationnel, en lien avec notre détection d'anomalies, afin de voir l'impact que cela pourrait avoir sur un contrôleur aérien. En effet, le contrôleur peut faire son travail à partir du moment où il a confiance dans les données affichées sur son écran. Si, à un moment donné nous lui montrons que son système n'est pas entièrement fiable, cela aura-t-il un impact sur sa concentration et sa charge de travail ? De même, qu'en est-il si le système peut lui remonter des alertes sur des anomalies potentielles ?

8 Publications de l'auteur

Conférences Internationales

de Riberolles, Théobald, Guthemberg Silvestre, et Nicolas Larrieu. Design, Development and Implementation of a Network Intrusion Detection Tool for Air Traffic Management Systems. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, 96-99. IEEE, 2018.

de Riberolles, Théobald de, Jiefu Song, Yunkai Zou, Guthemberg Silvestre, et Nicolas Larrieu. Characterizing Radar Network Traffic : a first step towards spoofing attack detection. In *2020 IEEE Aerospace Conference*, 1-8. IEEE, 2020.

Revue internationale en cours de soumission

En cours de révision majeure dans la SI Cybersécurité :
de Riberolles, Théobald, Yunkai Zou, Guthemberg Silvestre, Emmanuel Lochin, et Jiefu Song. *Anomaly Detection for ICS Based on Deep Learning : A Use Case for Aeronautical Radar Data* . 19 p . Soumis à Annals of Telecommunications - special issue ≪Interactions between artificial intelligence and cybersecurity to protect future networks≫, 2021.

Bibliographie

[1] Académie nationale de l'air et de l'espace (France). *Cybermenaces : visant le transport aérien = berthreats : targeting air transport : Dossier 45*. 2019.

[2] Charu C Aggarwal. An introduction to outlier analysis. In *Outlier analysis*, pages 1–34. Springer, 2017.

[3] Mohiuddin Ahmed, Abdun Naser Mahmood, and Jiankun Hu. A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 60 :19–31, 2016. Publisher : Elsevier.

[4] Cynthia Barnhart, Douglas Fearing, Amedeo Odoni, and Vikrant Vaze. Demand and capacity management in air transportation. *EURO Journal on Transportation and Logistics*, 1(1-2) :141, 2012.

[5] Gopi Battineni, Nalini Chintalapudi, and Francesco Amenta. Forecasting of COVID-19 epidemic size in four high hitting nations (USA, Brazil, India and Russia) by Fb-Prophet machine learning model. *Applied Computing and Informatics*, 2020. Publisher : Emerald Publishing Limited.

[6] Yoshua Bengio, Patrice Simard, and Paolo Frasconi. Learning long-term dependencies with gradient descent is difficult. *IEEE transactions on neural networks*, 5(2) :157–166, 1994. Publisher : IEEE.

[7] Loic Bontemps, James McDermott, Nhien-An Le-Khac, and others. Collective anomaly detection based on long short-term memory recurrent neural networks. In *International Conference on Future Data and Security Engineering*, pages 141–152. Springer, 2016.

[8] Christabelle S Bosson and Tasos Nikoleris. Supervised Learning Applied to Air Traffic Trajectory Classification. In *2018 AIAA Information Systems-AIAA Infotech@ Aerospace*, page 1637. 2018.

[9] Markus M Breunig, Hans-Peter Kriegel, Raymond T Ng, and Jörg Sander. LOF : identifying density-based local outliers. In *Proceedings of the 2000 ACM SIGMOD international conference on Management of data*, pages 93–104, 2000.

[10] Alvaro Cardenas, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig, Shankar Sastry, and others. Challenges for securing cyber physical systems. In *Workshop on future directions in cyber-physical systems security*, volume 5. Citeseer, 2009. Issue : 1.

[11] Eduardo Esteban Casanovas, Tomas Exequiel Buchaillot, and Facundo Baigorria. Vulnerability of radar protocol and proposed mitigation. In *ITU Kaleidoscope : Trust in the Information Society (K-2015), 2015*, pages 1–6. IEEE, 2015.

[12] Eric Chan-Tin, Victor Heorhiadi, Nicholas Hopper, and Yongdae Kim. The frog-boiling attack : Limitations of secure network coordinate systems. *ACM Transactions on Information and System Security (TISSEC)*, 14(3) :1–23, 2011.

[13] Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection : A survey. *ACM computing surveys (CSUR)*, 41(3) :1–58, 2009.

[14] Steven Cheung, Bruno Dutertre, Martin Fong, Ulf Lindqvist, Keith Skinner, and Alfonso Valdes. Using model-based intrusion detection for SCADA networks. In *Proceedings of the SCADA security scientific symposium*, volume 46, pages 1–12. Citeseer, 2007.

[15] Naveen Kumar Chikkakrishna, Chitirala Hardik, Kancherla Deepika, and Narendula Sparsha. Short-term traffic prediction using sarima and FbPROPHET. In *2019 IEEE 16th India Council International Conference (INDICON)*, pages 1–4. IEEE, 2019.

[16] James Clark, Zhen Liu, and Nathalie Japkowicz. Adaptive threshold for outlier detection on data streams. In *2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA)*, pages 41–49. IEEE, 2018.

[17] Mayara Conde Rocha Murca, Richard DeLaura, R John Hansman, Richard Jordan, Tom Reynolds, and Hamsa Balakrishnan. Trajectory clustering and classification for characterization of air traffic flows. In *16th AIAA Aviation Technology, Integration, and Operations Conference*, page 3760, 2016.

[18] Théobald de Riberolles, Jiefu Song, Yunkai Zou, Guthemberg Silvestre, and Nicolas Larrieu. Characterizing Radar Network Traffic : a first step towards spoofing attack detection. In *2020 IEEE Aerospace Conference*, pages 1–8. IEEE, 2020.

[19] Tommaso De Zan, Fabrizio d'Amore, and Federica Di Camillo. The defence of civilian air traffic systems from cyber threats. *Istituto Affari Internazionali*, 2016.

[20] Hervé Debar, Marc Dacier, and Andreas Wespi. A revised taxonomy for intrusion-detection systems. In *Annales des télécommunications*, volume 55, pages 361–378. Springer, 2000. Issue : 7.

[21] Zhiguo Ding and Minrui Fei. An anomaly detection approach based on isolation forest algorithm for streaming data using sliding window. *IFAC Proceedings Volumes*, 46(20) :12–17, 2013.

[22] Weishan Dong, Ting Yuan, Kai Yang, Changsheng Li, and Shilei Zhang. Autoencoder regularized network for driving style representation learning. *arXiv preprint arXiv :1701.01272*, 2017.

[23] M Dzunda, D Cekanova, L Cobirka, P Zak, and P Dzurovcin. Protection against high-frequency radiation of aviation electronic support systems used in air transport. *TransNav : International Journal on Marine Navigation and Safety of Sea Transportation*, 12, 2018.

[24] M Dzunda and A Hrban. Accuracy of the passive tracking systems. In *12th International Conference on Microwaves and Radar. MIKON-98. Conference Proceedings (IEEE Cat. No. 98EX195)*, pages 216–220. IEEE, 1998.

[25] Dacfey Dzung, Martin Naedele, Thomas P Von Hoff, and Mario Crevatin. Security for industrial communication systems. *Proceedings of the IEEE*, 93(6) :1152–1177, 2005.

[26] All Purpose Structured Eurocontrol. SURVEILLANCE DATA EXCHANGE Part 1 All Purpose Structured Eurocontrol Surveillance Information Exchange (ASTERIX).

[27] Antony D Evans and Paul U Lee. Predicting the Operational Acceptability of Route Advisories. In *17th AIAA Aviation Technology, Integration, and Operations Conference*, page 3078, 2017.

[28] Paolo F Fantoni and Alessandro Mazzola. Multiple-failure signal validation in nuclear power plants using artificial neural networks. *Nuclear technology*, 113(3) :368–374, 1996. Publisher : Taylor & Francis.

[29] Paul Farrell and Michiel Schuurman. *Using ASTERIX in accident investigation.* September 2012.

[30] Cheng Feng, Tingting Li, and Deeph Chana. Multi-level anomaly detection in industrial control systems via package signatures and LSTM networks. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 261–272. IEEE, 2017.

[31] David A Fulghum. Why Syria's Air Defenses Failed to Detect Israelis. *Aviation Week & Space Technology*, 3 :2007, 2007.

[32] Pedro Garcia-Teodoro, Jesus Diaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. Anomaly-based network intrusion detection : Techniques, systems and challenges. *computers & security*, 28(1-2) :18–28, 2009. Publisher : Elsevier.

[33] Maxime Gariel, Ashok N Srivastava, and Eric Feron. Trajectory clustering and an application to airspace monitoring. *IEEE Transactions on Intelligent Transportation Systems*, 12(4) :1511–1524, 2011.

[34] Markus Goldstein and Seiichi Uchida. A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. *PloS one*, 11(4) :e0152173, 2016. Publisher : Public Library of Science San Francisco, CA USA.

[35] Piyush Goyal and Anurag Goyal. Comparative study of two most popular packet sniffing tools-Tcpdump and Wireshark. In *2017 9th International Conference on Computational Intelligence and Communication Networks (CICN)*, pages 77–81. IEEE, 2017.

[36] Alex Graves and Jürgen Schmidhuber. Framewise phoneme classification with bidirectional LSTM and other neural network architectures. *Neural networks*, 18(5-6) :602–610, 2005.

[37] Manish Gupta, Jing Gao, Charu C Aggarwal, and Jiawei Han. Outlier detection for temporal data : A survey. *IEEE Transactions on Knowledge and Data Engineering*, 26(9) :2250–2267, 2013.

[38] Edan Habler and Asaf Shabtai. Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages. *Computers & Security*, 78 :155–173, 2018.

[39] Kerri A Heitner. *Cyber threats within civil aviation.* PhD Thesis, Utica College, 2014.

[40] Maryam Hemmati, Morteza Biglari-Abhari, and Smail Niar. Adaptive vehicle detection for real-time autonomous driving system. In *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 1034–1039. IEEE, 2019.

[41] Geoffrey E Hinton and Ruslan R Salakhutdinov. Reducing the dimensionality of data with neural networks. *science*, 313(5786) :504–507, 2006.

[42] Sepp Hochreiter, Yoshua Bengio, Paolo Frasconi, Jürgen Schmidhuber, and others. *Gradient flow in recurrent nets : the difficulty of learning long-term dependencies.* A field guide to dynamical recurrent neural networks. IEEE Press, 2001.

[43] Sepp Hochreiter and Jürgen Schmidhuber. Long short-term memory. *Neural computation*, 9(8) :1735–1780, 1997.

[44] Marian Jancik, Milan Dzunda, Peter Dzurovcin, Alena Moravcikova, and Simon Holoda. Cyber Security in "ATM Surveillance Tracker and Server" System. *DEStech Transactions on Engineering and Technology Research*, (mcaee), 2020.

[45] Marián Jančík, Šimon Holoda, Milan DŽUNDA, and Branislav Kandera. Current Status of Cyber Security in the Surveillance Data Processing Systems in Europe. In *2018 XIII International Scientific Conference-New Trends in Aviation Development (NTAD)*, pages 59–63. IEEE, 2018.

[46] Gabriel Jarry, Daniel Delahaye, Florence Nicol, and Eric Feron. Aircraft atypical approach detection using functional principal component analysis. *Journal of Air Transport Management*, 84 :101787, 2020.

[47] Longlong Jing and Yingli Tian. Self-supervised visual feature learning with deep neural networks : A survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2020. Publisher : IEEE.

[48] Branislav Kandera, Marian Jančík, and Šimon Holoda. Penetration testing of Surveillance Data Distribution System. In *2020 New Trends in Aviation Development (NTAD)*, pages 123–126. IEEE, 2020.

[49] Marko Kastelic and Janez Pers. Building Visual Anomaly Dataset from Satellite Data using ADS-B. In *OpenSky*, pages 44–50, 2019.

[50] Tung Kieu, Bin Yang, and Christian S Jensen. Outlier detection for multidimensional time series using deep neural networks. In *2018 19th IEEE International Conference on Mobile Data Management (MDM)*, pages 125–134. IEEE, 2018.

[51] Fei Tony Liu, Kai Ming Ting, and Zhi-Hua Zhou. Isolation forest. In *2008 Eighth IEEE International Conference on Data Mining*, pages 413–422. IEEE, 2008.

[52] Junshui Ma and Simon Perkins. Online novelty detection on temporal sequences. In *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 613–618, 2003.

[53] Pankaj Malhotra, Anusha Ramakrishnan, Gaurangi Anand, Lovekesh Vig, Puneet Agarwal, and Gautam Shroff. LSTM-based encoder-decoder for multi-sensor anomaly detection. *arXiv preprint arXiv :1607.00148*, 2016.

[54] Pankaj Malhotra, Lovekesh Vig, Gautam Shroff, and Puneet Agarwal. Long short term memory networks for anomaly detection in time series. In *ESANN proceedings, European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning*. Presses universitaires de Louvain, April 2015.

[55] Hermann Mannstein, Andreas Brömser, and Luca Bugliaro. Ground-based observations for the validation of contrails and cirrus detection in satellite imagery. *Atmospheric Measurement Techniques*, 3(3) :662, 2010.

[56] Alexandre Nairac, Neil Townsend, Roy Carr, Steve King, Peter Cowley, and Lionel Tarassenko. A system for the analysis of jet engine vibration data. *Integrated Computer-Aided Engineering*, 6(1) :53–66, 1999. Publisher : IOS Press.

[57] Syam Kiran Anvardh Nanduri. Anomaly Detection in Aircraft Performance Data. 2016.

[58] Calvin Nobles. Cyber threats in civil aviation. In *Emergency and Disaster Management : Concepts, Methodologies, Tools, and Applications*, pages 119–141. IGI Global, 2019.

[59] Luciana Obregon. Secure architecture for industrial control systems. *SANS Institute InfoSec Reading Room*, 2015.

[60] Guerric Poncet. *Piratage d'un avion : un cauchemar plausible.* April 2018.

[61] Bernhard Schölkopf, Robert C Williamson, Alexander J Smola, John Shawe-Taylor, John C Platt, et al. Support vector method for novelty detection. In *NIPS*, volume 12, pages 582–588. Citeseer, 1999.

[62] Michael Schultz, Sandro Lorenz, Reinhard Schmitz, and Luis Delgado. Weather Impact on Airport Performance. *Aerospace*, 5(4) :109, 2018.

[63] Franck Sicard, Éric Zamaï, and Jean-Marie Flaus. Cyberdéfense des systèmes de contrôle-commande industriels : une approche par filtres basée sur la distance aux états critiques pour la sécurisation face aux cyberattaques. In *C&esar 2017-La protection des données face à la menace cyber*, 2017.

[64] Florian Skopik, Ivo Friedberg, and Roman Fiedler. Dealing with advanced persistent threats in smart grid ICT networks. In *ISGT*, pages 1–5. IEEE, 2014.

[65] Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. On the security of the automatic dependent surveillance-broadcast protocol. *IEEE Communications Surveys & Tutorials*, 17(2) :1066–1087, 2014.

[66] Ilya Sutskever, Oriol Vinyals, and Quoc V Le. Sequence to sequence learning with neural networks. In *Advances in neural information processing systems*, pages 3104–3112, 2014.

[67] Axel Tanner and Martin Strohmeier. Anomalies in the Sky : Experiments with traffic densities and airport runway use. In *OpenSky*, pages 51–62, 2019.

[68] Markus Thill, Sina Däubener, Wolfgang Konen, THW Bäck, P Barancikova, M Holena, T Horvat, M Pleva, and R Rosa. Anomaly detection in electrocardiogram readings with stacked LSTM networks. In *Proceedings of the 19th Conference Information Technologies-Applications and Theory (ITAT 2019)*, pages 17–25. CEUR-WS, 2019.

[69] BR Upadhyaya, O Glockler, and J Eklund. Multivariate statistical signal processing technique for fault detection and diagnostics. *ISA transactions*, 29(4) :79–95, 1990. Publisher : Elsevier.

[70] Dayu Yang, Alexander Usynin, and J Wesley Hines. Anomaly-based intrusion detection for SCADA systems. In *5th intl. topical meeting on nuclear plant instrumentation, control and human machine interface technologies (npic&hmit 05)*, pages 12–16, 2006.

[71] Qiang Yang and Xindong Wu. 10 challenging problems in data mining research. *International Journal of Information Technology & Decision Making*, 5(04) :597–604, 2006. Publisher : World Scientific.

[72] Yifan Yao and Lina Wang. Combination of window-sliding and prediction range method based on LSTM model for predicting cryptocurrency. *arXiv preprint arXiv :2102.05448*, 2021.

[73] Yuan Yao, Abhishek Sharma, Leana Golubchik, and Ramesh Govindan. Online anomaly detection for sensor systems : A simple and efficient approach. *Performance Evaluation*, 67(11) :1059–1075, 2010. Publisher : Elsevier.

[74] Işil Yenidoğan, Aykut Çayir, Ozan Kozan, Tuğçe Dağ, and Çiğdem Arslan. Bitcoin forecasting using ARIMA and prophet. In *2018 3rd International Conference on Computer Science and Engineering (UBMK)*, pages 621–624. IEEE, 2018.

[75] Rui Zhang, Shaoyan Zhang, Yang Lan, and Jianmin Jiang. Network anomaly detection using one class support vector machine. In *Proceedings of the International MultiConference of Engineers and Computer Scientists*, volume 1. Citeseer, 2008.

[76] Bonnie Zhu and Shankar Sastry. SCADA-specific intrusion detection/prevention systems : a survey and taxonomy. In *Proceedings of the 1st workshop on secure control systems (SCS)*, volume 11, page 7, 2010.