UNIVERSITÉ DU QUÉBEC À MONTRÉAL

L'APPRENTISSAGE NON SUPERVISÉ POUR LA DÉTECTION DES SIGNAUX D'INTERFÉRENCE RADIO FRÉQUENTIELS

MÉMOIRE PRÉSENTÉ

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN GÉNIE ÉLECTRIQUE

PAR

ALEXANDER AMACHE

JANVIER 2022

REMERCIEMENTS

Je voudrais tout d’abord adresser toute ma gratitude à mon directeur de recherche prof. Wessam Ajib et mon codirecteur de recherche prof. Mounir Boukadoum, pour leur disponibilité et surtout leurs judicieux conseils.

Je remercie tous les membres du jury d’avoir pris le temps d’évaluer mon travail de recherche.

Enfin, j’adresse mes plus sincères remerciements à ma famille : ma mère, mes frères et tous mes proches, qui m’ont accompagné, soutenu et encouragé tout au long de mes études et de la réalisation du mémoire.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ACRONYMES

AUC	L'Aire sous la courbe ROC (en anglais The Area Under the Receiver Operating Characteristic Curve)
CWI	Interférence d'onde continue (en anglais Continuous Wave Interference)
CI	Interférence des signaux Chirp (en anglais Chirp Interference)
DCGAN	Réseau adversaire génératif convolutionnel profond (en anglais Deep Convolutional Generative Adversarial Network)
FFT	Transformée de Fourrier rapide (en anglais Fast Fourrier Transform)
FN	Faux Négatif (en anglais False Negative)
FP	Faux Positif (en Anglais False Positive)
GAN	Réseau adverse génératif (en anglais Generative Adversarial Network)
GNSS	Système de Positionnement par Satellites (en anglais Global Navigation Satellite System)
MCWI	Interférence multiple d'onde continue (en anglais Multi Continuous Wave Interference)
MSE	Erreur Quadratique Moyenne (en anglais Mean Squared Error)
One-Class SVM	Machine à Vecteur de Support à une Classe (en anglais One-Class Support Vector Machine)
RF	Radio Fréquence
RFI	Interférence Radio Fréquence (en anglais Radio-Frequency Interference)
ReLU	Unité de rectification linéaire (en anglais Rectified Linear Units)
SVDD	Description des données du vecteur de support (en anglais Support Vector Data Description)
SVM	Machine à vecteur de support (en anglais Support Vector Machine)
SOI	Signal d'intérêt (en anglais Signal of Interest)
Train	Former
UIT	L'Union Internationale des Télécommunications
VP	Vrai Positif (en anglais True Positive)

RÉSUMÉ

La présence de signaux indésirables dans les ondes radio, appelés interférences RF, peut entraîner une dégradation des performances ou une perte d'information dans les systèmes de communication sans fil. Ainsi, la détection des interférences RF est essentielle pour améliorer la qualité des communications sans fil comme première étape du processus d'élimination de ces interférences. Dans ce mémoire, nous proposons deux approches pour détecter les interférences RF en utilisant l'apprentissage automatique non supervisé. Nous étudions deux approches de détection d'anomalies qui s'appuient sur les vecteurs de support pour la délimitation des frontières de classes normales, c.-à-d., avec l'utilisation de données normales (Sans interférences RF). Tout d'abord, nous étudions la détection d'anomalie à l'aide de l'algorithme appelé machine à vecteur de support à une classe (One-Class SVM), formé avec une base de données normale (c.-à-d., sans interférences RF) constituée par les scalogrammes du signal d'intérêt (en anglais *signal of interest* ou SOI). Ensuite, nous considérons l'algorithme appelé SVDD (en anglais *Support Vector Data Description*). Nos résultats de simulation pour trois types d'interférences RF, en utilisant la mise à l'échelle des caractéristiques sur une plage (en anglais *Scaling Features to a Range*) comme méthode de normalisation, montrent que la détection d'interférences RF par SVDD a une faible complexité de calcul et une précision de détection de 90,74 % contre une précision de 91,67% pour le SVM à une classe.

Mots clés : détection d'anomalies, interférence RF, SVDD, One-Class SVM, Apprentissage non supervisé.

CHAPITRE I

MISE EN CONTEXTE ET MOTIVATIONS

1.1 Introduction

Les ondes radio, qui font partie du spectre électromagnétique, sont un support essentiel pour transmettre des données aux utilisateurs. Sa fiabilité et sa robustesse dépendent de certains facteurs tels que la fréquence, la propagation, la polarisation, mais également les interférences RF. Ces interférences RF peuvent rendre les données inutilisables ou causer une perte d'information, par exemple, dans les systèmes de communications sans fil.

Malgré la gestion du spectre des RF par les différents pays, le problème des interférences RF reste persistant. Par conséquent, afin de garantir une transmission de données fiable, robuste et sécuritaire à tout moment, la détection des interférences RF est essentielle comme première étape du processus d'élimination de ces interférences.

Suite à cette introduction, nous entamerons la mise en contexte de ce mémoire en présentant les motivations de ce projet de recherche. Ensuite, nous présenterons la problématique, les objectifs, la méthodologie et les contributions de ce mémoire. Enfin, le plan du mémoire est présenté.

1.2 Motivation

Les systèmes de communications sans fil sont aujourd'hui utilisés partout à travers le monde dans de nombreux domaines d'application, autant civil que militaire ou gouvernemental. D'ici une décennie, avec l'avènement de nouvelles technologies sans fil comme la 5G (cinquième génération des réseaux cellulaires) et la 6G (Matinmikko-Blue, Yrjölä, et Ahokangas , 2020), l'augmentation du nombre de dispositifs reliés à l'internet des objets (Ido) (Li *et al*., 2021), les applications vont se multiplier et le spectre radio deviendra de plus en plus encombré. Or, le spectre est une ressource limitée.

D'autre part, les données transmises via des signaux RF sont de plus en plus contaminées par des interférences RF. Ces interférences RF sont des signaux RF interférentes qui perturbent les signaux de données d'origine et pénalisent fortement la performance des systèmes de

communication sans fil (Getu, 2019) comme dans la radioastronomie ou la communication dans l'espace lointain, la radiométrie micro-onde (en anglais *Micro-Wave Radiometry* MWR), les systèmes de positionnement par satellites (en anglais *Global Navigation Satellite System* (GNSS)) et les systèmes réflectométrie GNSS (GNSS-R). Un autre problème lié aux interférences RF est que les points d'accès des réseaux locaux (tel que le wifi) et les utilisateurs peuvent devenir incapables de transmettre de données, en causant des retards et une dégradation des performances de transmission.

Selon le projet (AVIO-601, 2018) et (Ghanney, 2019), les principales sources d'interférences RF sont la mauvaise installation des équipements, la défaillance d'équipement, la manque de formation du personnel, des équipements aux normes inférieures, les erreurs humaines, une conception médiocre, des systèmes de transmission RF adjacents, des brouilleurs orbitaux, l'usurpation de liaisons et l'absence d'adhésion à des réglementations communes et à des standards industriels.

Jusqu'à présent, de nombreux algorithmes traditionnels (sans recours à l'apprentissage automatique) ont été proposé pour détecter, localiser et éliminer les interférences RF, mais ils présentent trois limitations importantes, à savoir la complexité, l'absence de détection en temps réel et un champ d'application limité, qui seront examinés en détail au chapitre 2. Les algorithmes d'apprentissage automatique ont apporté une solution à ces trois limitations en présentant une précision de détection d'interférences RF allant de 80% à 99 % (Li, Shao, Zhou, et Zhao, 2020) (Harrison et Mishra, 2019), voir dans certaines applications atteignant une précision de 100 % (Lyu, Han, Zhong, Li, et Liu, 2020), mais ces algorithmes appartenant à une classe d'apprentissage automatique (apprentissage supervisé, apprentissage non supervisé et apprentissage par renforcement) ont certaines limitations liées à la classe à laquelle ils appartiennent, comme nous le verrons au chapitre 2. Une limitation commune à presque tous les algorithmes d'apprentissage automatique est la nécessité de disposer d'une grande base de données pour la phase de formation ou de disposer d'une grande quantité de données anormales (par exemple, avec interférences RF), ce qui n'est pas souvent le cas dans le monde réel. Par conséquent, afin d'éviter une crise dans les systèmes de communications sans fil, nous devons trouver de nouvelles façons de gérer le spectre, et mettre au point des technologies innovatrices

d'apprentissage automatique qui permettront de détecter les interférences RF sans avoir besoin d'une grande base de données ou de données anormales pendant la phase de formation, tout en assurant une détection en temps réel, comme première étape du processus d'élimination de ces interférences qui menacent l'avenir des technologies de transmission sans-fil.

1.3 Problématique

La littérature propose plusieurs solutions et algorithmes pour résoudre le problème des interférences RF en utilisant des approches traditionnelles. Ces approches peuvent être classés en sept groupes : algorithmes de détection temporelle, spectrale, spectro-temporelle, statistique, de polarisation, de filtrage spatial et algorithmes de détection basée sur la transformation de domaine (Getu, 2019). Malgré la richesse de cette littérature, les algorithmes traditionnels de traitement du signal utilisés pour la détection des interférences RF présentent de nombreuses limitations en termes de complexité et de performance (Getu, 2019). Dans le cas des algorithmes d'apprentissage automatique utilisés pour la détection de ces interférences RF, la plupart des solutions proposées utilisent une grande base de données et beaucoup de données anormales (avec des interférences RF) pendant la phase de formation. De plus, dans le monde réel, nous trouvons peu ou pas d'échantillons anormaux (dans notre cas, des échantillons d'interférences RF) et beaucoup d'échantillons normaux (sans interférences RF). Finalement, il est souvent difficile d'obtenir des bases de données de taille importantes et équilibrées comprenant à la fois des données normales et anormales.

Tant que les interférences RF existent, il y aura une perte d'informations, une dégradation des performances et de la fiabilité des systèmes de communications sans fil, comme on l'a vu précédemment. Face à ces inconvénients, il sera efficace d'étudier les différents types d'interférences RF d'une manière rigoureuse afin de déterminer un maximum de caractéristiques utiles à la détection de ces interférences. En prenant en compte ces défis, ce mémoire cherche à mettre au point des technologies innovatrices d'apprentissage automatique qui permettront de détecter tous les types d'interférences RF (ou au moins la majorité) d'une manière simple, efficace, en temps réel et avec l'utilisation d'une petite base de données pendant la phase de formation.

1.4 Objectifs

L'objectif général de ce mémoire est d'étudier et de développer une solution innovatrice, simple et efficace d'apprentissage automatique pour la détection des interférences RF qui soit applicable à tous (ou au moins à la majorité) les systèmes de communications sans fil.

Cet objectif peut être décomposé en deux objectifs spécifiques :

- Développer un algorithme de détection des interférences RF avec les propriétés suivantes : faible complexité computationnelle, grande précision de détection, tolérances aux jeux de données non équilibrées et capacité d'apprentissage avec de base de données de faible taille.
- Valider l'algorithme sur différents types d'interférences RF.

1.5 Méthodologie

Ce mémoire traite le problème de la détection des interférences RF comme un problème de détection d'anomalies. Dans ce but, nous utilisons deux algorithmes d'apprentissage automatique, à savoir le SVM à une classe (en anglais *One-class Support Vector Machine*) et le SVDD (en anglais *One-class Support Vector Data Description*), qui sont capables d'utiliser uniquement des données normales pendant la phase de formation afin de détecter comme anomalie toute nouvelle donnée qui ne présente pas les mêmes caractéristiques que les données utilisées lors de la formation de l'algorithme. Par conséquent, ces algorithmes seront capables de détecter d'une manière simple et efficace tous les types d'interférences RF. D'autre part, afin d'utiliser correctement la base de données pour que les algorithmes fonctionnent efficacement, nous effectuons un prétraitement des données à l'aide de l'outil Google Colab (Carneiro *et al.*, 2018) comme suit :

- Préparation des données : Les données doivent être dans un format accepté par l'algorithme.
- Normalisation des données : Nous normalisons les données, une exigence commune à de nombreux algorithmes d'apprentissage automatique afin d'éviter les erreurs lors de la phase de formation. Par exemple, un algorithme peut être incapable d'apprendre

correctement d'autres caractéristiques si une caractéristique a une variance supérieure de plusieurs ordres de grandeur à celle des autres.

Enfin, le SVM à une classe et le SVDD sont formés uniquement avec des données normales sur un serveur Cloud de Google Colab et testé avec deux sous-ensembles, l'un avec de nouvelles données normales et l'autre avec de nouvelles données anormales en utilisant différentes métriques d'évaluation disponibles sur les librairies de Google Colab.

1.6 Contributions

Ce mémoire tente de résoudre le problème de l'interférence RF qui altère le bon fonctionnement des systèmes de communication sans fil. Par conséquent, ce mémoire :

- propose deux algorithmes d'apprentissage automatique simples et efficaces qui permettent la détection simultanée et en temps réel de plusieurs types d'interférences RF en utilisant une petite base de données ;
- applique l'apprentissage automatique et la technique de détection d'anomalies afin d'atteindre cet objectif ;
- utilise une base de données constituée de données normales et anormales pour tester la précision et la robustesse de la solution proposée via des métriques d'évaluation ; et
- propose une méthode pour générer des images synthétiques d'interférences RF afin d'augmenter et de diversifier la base de données tout en évitant le sur-apprentissage.

1.7 Plan du mémoire

Le plan du mémoire est organisé comme suit. Le chapitre 2 présentera l'état de l'art de la littérature relative aux algorithmes traditionnellement utilisés pour détecter les interférences RF, en montrant leurs limitations. Ensuite, les grandes classes d'apprentissage automatique seront analysées et comparées selon leurs limitations afin de déterminer les algorithmes les plus adaptés à la détection des interférences RF.

Le chapitre 3 vise à montrer une présentation des concepts généraux et l'architecture choisie pour les algorithmes d'apprentissage non supervisé qui permettront de détecter les interférences RF à l'aide de la technique de détection d'anomalies.

Le chapitre 4 présentera la base de données utilisée pour tester les algorithmes choisis via des métriques d'évaluation. Ensuite, les résultats obtenus via des graphiques et tableaux seront analysés et comparés.

Enfin, le dernier chapitre montrera les principales conclusions de ce mémoire et les possibilités de travaux futurs.

CHAPITRE II

REVUE DE LITTÉRATURE

2.1 Introduction

Les systèmes de communication sans fil représentent l'un des technologies qui enregistre la plus forte croissance en innovation, recherche et développement dans les diverses technologies d'aujourd'hui (Getu, 2019), en raison de leur implication dans différents domaines d'applications telles que : en santé, en industrie et en transport. Nos sociétés se dirigent de plus en plus vers un monde sans fil en utilisant les téléphones mobiles, les systèmes de localisation GPS (en anglais *Global Positioning Systems*), les réseaux locaux Wifi (WLAN), etc. Par conséquent, il y a beaucoup de facteurs qui altèrent la transmission des données sans fil ou plus précisément la bonne réception d'un signal radio comme nous l'avons vu dans le chapitre précédent ; par exemple, quand le spectre électromagnétique devient trop encombré ou la présence de signaux d'interférence RF, qui dégradent ou perturbent la performance d'un récepteur sans fil. Vu ces inconvénients, un objectif général de la recherche et de l'industrie des télécommunications est de proposer une communication sans fil très performante, fiable et robuste pour transmettre des données de façon sécuritaire.

Suite à cette introduction, nous entamerons une brève revue de la majorité des techniques et approches traditionnellement utilisées pour la détection d'interférences RF. Ensuite, nous présenterons les techniques les plus fréquemment proposées et étudiées dans les articles scientifiques récents dans le domaine de l'apprentissage automatique pour détecter l'interférence RF. Une fois les différentes techniques et approches sont présentées, nous passerons à une analyse critique afin de proposer une solution adéquate à nos objectifs. De plus, nous étudierons les réseaux adverses génératifs (en anglais *Generative Adversarial Networks* ou GANs) et leur extension comme techniques possibles de détection d'anomalies.

2.2 État de l'art

2.2.1 Techniques de détection des interférences RF

L'état de l'art au sujet de la détection des interférences RF comporte différents algorithmes. Ces algorithmes ont été développés notamment pour des applications telles que la radioastronomie ou la communication dans l'espace lointain, la radiométrie micro-onde (en anglais *Micro-Wave Radiometry* MWR), les systèmes de positionnement par satellites (en anglais *Global Navigation Satellite System* (GNSS)) et les systèmes réflectométrie GNSS (GNSS-R). Il existe plusieurs méthodes utilisées pour détecter et combattre les interférences RF, mais le choix de la technique dépend de plusieurs facteurs tels que la consommation d'énergie et l'environnement où ces techniques sont utilisées. Il est important de souligner qu'il n'y a pas de méthode qui fonctionne bien dans tous les cas. Donc, dans la suite nous subdiviserons les techniques de détection des interférences RF en deux groupes : (i) des techniques conventionnelles pour la détection des interférences RF et (ii) des techniques récentes pour la détection des interférences RF basées sur les approches d'apprentissage automatique (en anglais *Machine Learning* ou ML). Ensuite, nous présenterons quelques-uns de ces algorithmes.

2.2.1.1 Les techniques conventionnelles de détection des interférences RF

La difficulté de détection des interférences RF est que ces interférences impliquent, dans la plupart des cas, des signaux stochastiques avec, à priori, des paramètres inconnus. Ces algorithmes de détection peuvent être classés en sept groupes : algorithmes de détection temporelle, spectrale, spectro-temporelle, statistique, de polarisation, de filtrage spatial et algorithmes de détection basée sur la transformation de domaine.

2.2.1.1.1 Les algorithmes de détection temporelle

Lorsque le signal est illustré dans le domaine temporel, un algorithme de détection temporelle essaye d'explorer les composants d'interférences RF focalisés dans des parties déterminées du domaine temporel qui présentent une valeur de puissance plus élevée que le signal sans interférence RF (Güner, Johnson, et Niamsuwan , 2007).

Une des techniques les plus utilisées est la suppression d'impulsion asynchrone (en anglais *Asynchronous Pulse Blanking* ou APB). Cette technique présente deux avantages : (i) elle est efficace lorsqu'il s'agit de courtes rafales de haute puissance d'interférence RF et (ii) un échantillonnage à haute fréquence et un seuil approprié aident généralement à fournir des bonnes performances. D'autre part, cette technique présente deux inconvénients : (i) il est compliqué de détecter l'interférence RF dans le cas où la puissance de celle-ci est similaire ou inférieure à la puissance du bruit et (ii) si la durée des maximums RFI est plus courte que le temps d'intégration, ces RFI peuvent passer inaperçus.

Le principe de fonctionnement de l'APB est illustré ci-dessous.

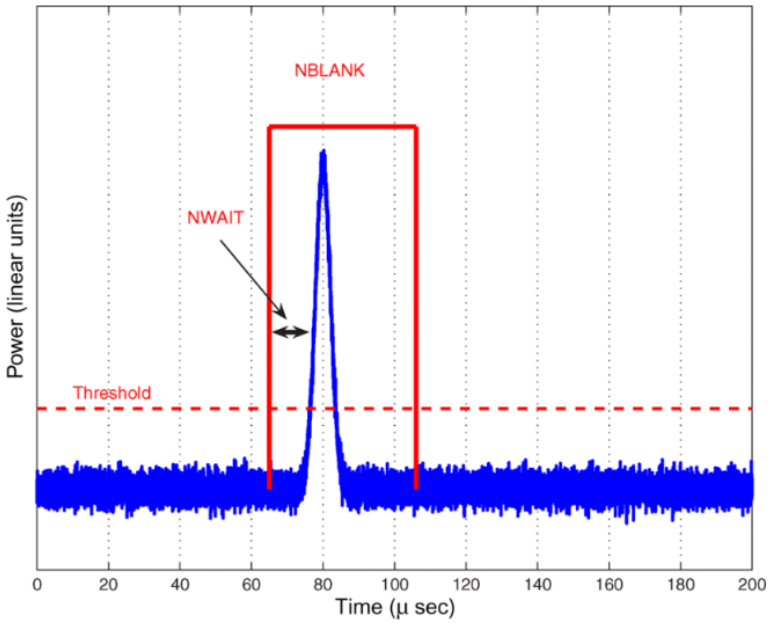

Figure 2.1 Principe de fonctionnement de l'APB (Güner *et al*., 2007).

On observe dans la figure 2.1 que la partie où l'amplitude du signal dépasse un certain seuil par rapport au bruit, celle-ci est supprimé par un bloc de longueur dit NBLANK, commençant à partir d'une période dite NWAIT prédéterminée avant le déclencheur.

2.2.1.1.2 Les algorithmes de détection spectrale

En général, les interférences RF qui appartiennent au groupe de signaux à bande étroite CW (en anglais *Continuous Wave*) sont très susceptibles d'être reçues par les récepteurs sans fil en

milieu urbain. Donc, les algorithmes de détection spectrale proposés en (Forte, 2014) sont plus complexes que celles de la détection temporelle, puisqu'une décomposition en sous-bandes est nécessaire. Deux approches peuvent être distinguées : (i) une approche d'estimation spectrale non paramétrique du signal d'entrée, obtenue à partir des techniques de traitement de signal telle que la transformée de Fourier discrète (en anglais *Discret Fourier Tranform* ou DFT) et (ii) une approche d'estimation spectrale paramétrique pour l'atténuation des brouilleurs générant des signaux de type chirp.

La première approche ne peut être considérée comme la meilleure option pour atténuer des interférences RF non stationnaires, en raison de l'apparition de signaux impulsionnels et le changement rapide dans le temps des caractéristiques spectrales. Par conséquent, cette approche devient incomplète et incapable de suivre ce type d'interférence RF.

La deuxième approche est basée sur les filtres coupe-bande adaptatifs (Borio et Camoriano, 2008). Par exemple, on utilise un filtre dont la fonction de transfert a la forme suivante :

$$H_n(z) = \frac{1 - z_0[n]z^{-1}}{1 - k\, z_0[n]z^{-1}} \qquad (2.1),$$

où k est le facteur de contraction du pôle et $z_0[n]z^{-1}$ est le zéro du filtre.

Ces filtres sont très efficaces contre les brouilleurs à bande étroite et peuvent être utilisés dans des applications qui nécessitent une faible puissance. Par contre, leur principal inconvénient est qu'ils ne peuvent pas être utilisés lorsque le brouilleur n'a pas de structure de signal prévisible.

2.2.1.1.3 Les algorithmes de détection spectro-temporelle

Afin de détecter et d'atténuer (ou éliminer) les interférences RF non-stationnaires, les techniques de détection spectro-temporelle représentent la meilleure option et elles sont les plus utilisées (Borio et Camoriano, 2008). En effet, cette approche tient compte des interférences RF dans les deux domaines : temporel et fréquentiel, c'est-à-dire, ces techniques permettent de détecter les signaux à bande étroite CW aussi bien que les signaux impulsionnels. Différentes distributions temporelle-fréquentielle (TF) telles que le spectrogramme et la

distribution de Wigner-Ville peuvent être utilisées pour représenter le signal dans le domaine temporel-fréquentiel (TF).

La technique de spectrogramme utilise les techniques de traitement d'image telles que la détection de bord et les algorithmes de lissage pour détecter la présence d'anomalies qui sont ensuite supprimées. L'image obtenue est le graphe d'intensité de la magnitude de la transformée de Fourier à court terme (TFCT, en anglais STFT *Short-Time Fourier Transform*). L'avantage de cette technique par rapport aux algorithmes de détection temporelle ou spectrale est qu'elle ne supprime que des fréquences occupées au moment précis où elles se produisent, et non l'interférence de toute la bande de fréquence ou de toute l'intervalle de temps.

La distribution de Wigner-Ville ne subit pas d'effets de fuite comme c'est le cas pour les techniques basées sur la transformée de Fourier à court terme (TFCT). Donc, elle offre la meilleure résolution spectrale. Cependant, si les signaux analysés ont plusieurs composantes de fréquence, cette distribution subit des termes croisés (en anglais *Cross-Terms*). Par contre, ces termes croisés peuvent être partiellement supprimés en lissant la distribution de Wigner-Ville (WVD) avec des fenêtres 2D passe-bas (Akansu et Haddad, 2001).

2.2.1.1.4 Les algorithmes de détection statistique

Étant donné que l'interférence RF et le signal désiré sont supposés être des processus stochastiques indépendants, ils ont des propriétés statistiques qui peuvent être utilisées pour les séparer. Alors, cette technique est basée sur le fait que le signal radiométrique sans interférence RF devrait être une variable gaussienne aléatoire de moyenne zéro (Forte, 2014).

Parmi les nombreux tests statistiques, la méthode de la détection de kurtosis (KD) est le meilleur algorithme statistique de détection d'interférence RF pour presque tous les types de signaux interférents (Tarongi et Camps, 2009) (Roo, Misra, et Ruf, 2007).

Le kurtosis est calculé comme suit :

$$K = \frac{\mu_4}{\sigma^4} = \frac{E\left[(X-E[X])^4\right]}{E[(X-E[X])^2]^2} \qquad (2.2)$$

où μ_4 est le quatrième moment du processus aléatoire X et σ est l'écart type du processus aléatoire X.

Alors, d'après l'équation (2.2), on voit que le kurtosis est un paramètre défini comme le quatrième moment central normalisé par le carré du deuxième moment central. Ainsi, les anomalies correspondent aux valeurs qui diffèrent du kurtosis d'un signal distribué de façon gaussienne.

2.2.1.1.5 Les algorithmes de détection polarimétrique

Afin de distinguer les signaux d'interférence RF et le signal désiré, la technique de détection polarimétrique (Forte, 2014) utilise la propriété physique unique des champs électromagnétiques qui est la polarisation. Par exemple, dans la radiométrie, cette technique cherche des anomalies dans le 3ème et 4ème paramètres de Stokes, et si elles sont trouvées, les correspondants 1er et 2ème paramètres de Stokes sont écartés. L'avantage de cette technique par rapport aux filtres spatiaux est qu'elle ne nécessite qu'un seul élément d'antenne (avec double polarisation). Par conséquent, elle devrait être considérablement moins chère à implémenter.

2.2.1.1.6 Les algorithmes de détection basés sur le filtrage spatial

Afin d'éliminer les signaux de brouillage, les antennes de type adaptative utilisent des techniques de filtrage spatial. Comme le filtrage adaptatif vu ci-dessus, cette technique tente d'optimiser une fonction de coût.

Le filtrage spatial permet d'éliminer l'interférence RF en angle, plutôt qu'en fréquence, et il peut offrir une grande marge antiblocage contre la plupart des formes d'onde d'interférence, y compris le bruit à large bande. Toutefois, l'inconvénient majeur de ce filtrage est qu'il a besoin de réseaux d'antennes multiéléments, qui sont significativement plus grandes que les antennes à seul élément.

Cette technique a d'abord été utilisée en radioastronomie (Leshem, Van Der Veen, et Boonstra, 2000) et puis en radiométrie avec un algorithme de détection d'interférence RF de type DOA (en anglais Direction of Arrival) (Misra et Ruf, 2011).

2.2.1.1.7 Les algorithmes de détection basés sur la transformation de domaine

Dans le cas où l'estimation du signal de brouillage peut être obtenue quand le signal de brouillage est orthogonal au signal désiré, les interférences RF peuvent être détectées en comparant la nouvelle estimation ou représentation avec un seuil prédéfini (Kandangath, 2003). Les deux transformations les plus utilisées sont :

- La transformée en ondelette (en anglais *Wavelet Tranform* ou WT) : Cette transformée est une généralisation des transformations linéaires qui ont un noyau à temps fini, comme la transformée de Fourier à court terme (en anglais *Short Term Fourrier Transform* ou STFT). Dans ce cas, le signal désiré sans interférence RF est obtenue à l'aide d'une transformée en ondelettes inverse.
- La transformée de Karhunen-Loeve (dit KLT) : Cette méthode est basée sur la décomposition du signal dans un espace vectoriel en utilisant des fonctions propres obtenues à l'aide de l'estimation de sa fonction d'autocorrélation et le calcul de la matrice de Toeplitz. Dans ce cas, le signal peut avoir n'importe quelle forme, et donc il sera mieux adapté au signal traité et cela augmentera les performances de détection de l'interférence RF.

2.2.1.1.8 Limitations

Les méthodes traditionnelles pour détecter et atténuer les interférences RF comportent plusieurs inconvénients mentionnés dans (Ghanney, 2019) et (Getu, 2019), tels que :

- La complexité : Les non-linéarités présentes dans le processus de détection et d'atténuation des interférences RF rendent les algorithmes plus complexes, c'est-à-dire, le nombre d'opérations élémentaires (telles que affectations, comparaisons, opérations arithmétiques) effectuées par un algorithme est plus grand.
- Pas de détection à temps réel : Ces algorithmes, dû au fait qu'il y a un volume impressionnant de données produites, collectées, rassemblées et structurées ne produisent pas une détection des interférences RF en temps réel.

- Champ d'application limité : La plupart de ces algorithmes ont été conçus pour des environnements et applications spécifiques telles que la radiométrie, la radioastronomie et les systèmes de positionnement par satellites (GNSS), comme a été présenté précédemment. Alors, il faut un algorithme qui soit applicable à tous (ou au moins la majorité) les systèmes de communications sans fil.

2.2.1.2 Techniques de détection d'interférence RF basées sur l'apprentissage automatique

L'objectif de l'apprentissage automatique est de créer ou former un modèle ou un algorithme qui apprend comment combiner des entrées pour formuler des prédictions efficaces sur des données qui n'ont encore jamais été observées, c'est-à-dire, à des exemples sans étiquette. Donc, ce que nous cherchons à faire ici à l'aide de ces techniques, c'est de concevoir un algorithme qui nous permettra de détecter de façon simple, efficace, efficiente et avec une grande performance les interférences RF.

Par exemple, dans l'apprentissage automatique supervisé, on peut distinguer deux types de modèle :

- Les modèles de régression : Ces modèles prédisent des valeurs continues. Par exemple, une prédiction qui répond à la question suivante « Quelle est la valeur d'un logement à Montréal ? »
- Les modèles de classification : Ces modèles prédisent des valeurs discrètes. Par exemple une prédiction qui répond à la question suivante « Ce signal radio fréquence donné est-il considéré comme ayant subi une interférence RF ou non ? »

Donc, il est possible de traiter le problème de détection d'interférence RF comme un problème de classification binaire, dans lequel l'objectif est de prédire correctement l'une des deux étiquettes possibles, par exemple « Interférence RF » ou « pas d'interférence RF ». Toutefois, cette approche ne fonctionne pas si on dispose de peu ou pas d'exemples positifs (interférence RF ou anomalie), et d'un vaste échantillon de négatifs (pas d'interférence RF ou données normales). Donc, il est convenable de régler ce problème à l'aide de la technique de détection d'anomalies. En apprentissage automatique, cette technique consiste à apprendre ou à définir ce qui est normal, et à utiliser ce modèle de normalité pour détecter les anomalies intéressantes.

D'autre part, les algorithmes de détection d'anomalies peuvent fonctionner soit comme des détecteurs de valeurs aberrantes (en anglais *Outlier Detectors*) (Damer, Grebe, Zienert, kirchbuchner, et Kuijper, 2019), ce qui correspond à repérer les anomalies dans les données de formation, soit comme des détecteurs de nouveautés (en anglais *Novelty Detection*) (Damer *et al*., 2019), ce qui correspond à repérer les anomalies dans des nouvelles données qui n'ont pas été observées à la phase de formation.

Par conséquent, la technique de détection d'anomalies paraît comme une bonne solution pour détecter les interférences RF à l'aide de l'apprentissage automatique. Toutefois, il faut déterminer entre les grandes classes d'apprentissage automatique, la plus convenable pour la détection d'interférence RF, en tenant compte des critères tels que : i) la performance, ii) la faible complexité computationnelle, iii) la tolérance aux jeux de données non équilibrées et iv) la capacité d'apprentissage avec de base de données de faible taille. Dans la suite, nous présenterons les trois grandes classes d'apprentissage automatique :

- L'apprentissage supervisé (en anglais *Supervised Learning*) : Ce type d'apprentissage est le plus couramment utilisé. Un algorithme d'apprentissage automatique supervisé crée un modèle en examinant de nombreux exemples déjà étiquetés, puis tente de trouver un modèle qui minimise la perte (Simeone, 2018). Des algorithmes tels que la régression logistique ou linéaire et la classification multi-classes sont des exemples d'apprentissage supervisé.

- L'apprentissage non supervisé (en anglais *Unsupervised Learning*) : Ces algorithmes utilisent une approche plus indépendante, c'est-à-dire, le modèle est formé par un ensemble des données qui n'ont pas d'étiquettes (Simeone, 2018). L'algorithme statistique k-means, la catégorisation à noyaux et spectrale, le réseau adversaire génératif convolutionnel profond (DCGAN), le clustering profond et les mélanges de Gaussiennes (GMMs) sont des exemples d'apprentissage non supervisé.

- L'apprentissage par renforcement (en anglais *Reinforcement Learning* ou RL) : Il s'agit d'une méthode d'apprentissage sans supervision pour les algorithmes d'apprentissage

automatique (Sutton et Barto, 2015). Cette méthode consiste à laisser l'algorithme apprendre de ses propres erreurs (principe d'essai/erreur). Afin d'apprendre à prendre les bonnes décisions, l'algorithme se trouve directement confronté à des choix. S'il se trompe, il est pénalisé. Au contraire, s'il prend la bonne décision, il est récompensé. Donc, le but est de déterminer la stratégie optimale pour optimiser la prise de décisions afin d'obtenir toujours plus de récompenses. Pour cela, un simple retour des résultats (le signal de renforcement) est nécessaire pour apprendre comment l'algorithme doit agir pour accomplir systématiquement la tâche qui lui est confiée.

Entre les trois grandes classes d'apprentissage automatique présentées ci-dessus, les plus populaires dans la littérature pour traiter la détection d'interférence RF sont : l'apprentissage supervisé et l'apprentissage non supervisé. Ce choix dépend principalement des facteurs tels que : la structure et le volume des données, l'efficacité et efficience de l'algorithme et l'application qui est souvent la détection d'anomalies ou la classification d'images.

Afin de déterminer quels algorithmes sont les plus prometteurs pour détecter les interférences RF, nous entamerons une brève revue des algorithmes d'apprentissage supervisé, d'apprentissage non supervisé et d'apprentissage par renforcement utilisés pour la détection d'anomalies et la détection d'interférences RF.

2.2.1.2.1 Algorithmes d'apprentissage supervisé pour la détection d'interférence RF et la détection d'anomalies

De nombreux algorithmes d'apprentissage supervisé sont proposés pour la détection d'anomalies, tels que la méthode des K voisins les plus proches (en anglais *k-Nearest Neighbor* ou KNN) (Portela, Mendoza, et Benavides, 2019) (Guo et Shui, 2020), l'algorithme NB (en anglais *Naive Bayesian Classifier*) (Ding, Gao, Bu, et Ma, 2018), l'algorithme DT (en anglais *Decision Tree*) (Sahu et Mehtre, 2015) (Wang, Yang, et Ren, 2009), et les machines à support vectoriel (en anglais *Support Vector Machines* ou SVM) (Portela *et al*., 2019) (Lei, 2017). Nous pouvons noter que tous ces algorithmes atteignent une bonne précision pour détecter les anomalies et que le SVM a la meilleure performance selon (Portela *et al*., 2019) et (Eltanbouly,

Bashendy, AlNaimi, Chkirbene, et Erbad, 2020). À titre d'exemple, dans cette section, on présentera certains de ces algorithmes pour la détection d'anomalies et pour la détection d'interférences RF présentent dans la littérature. Ensuite, on verra quelques limitations de l'apprentissage supervisé.

Algorithmes d'apprentissage supervisé pour la détection d'anomalies :

- Le KNN: Cette méthode est l'un des algorithmes d'apprentissage automatique les plus simples avec plusieurs hyperparamètres comme la valeur de K ou le type de distance utilisé pour comparer les exemples telles que : i) Euclidien, ii) Manhattan, iii) Minkowski ou iv) Chebyshev (Taneja, Gupta, Goyal, & Gureja, 2014). Ce réseau présenté dans (Portela *et al*., 2019) est utilisé pour détecter les anomalies dans une base de données de 82332 exemples, en utilisant $K = 100$ et la distance de Chebyshev. L'algorithme atteint une précision de prédiction de 89,4% et un AUC (en anglais *Area Under the receiver operating characteristic curve (ROC Curve))* de 0,97 selon (Portela *et al*., 2019). Les auteurs ont montré que l'algorithme a une probabilité de 97% de distinguer correctement entre les données normales et les données anormales (ayant une anomalie).

- Le SVM : Ce modèle est un algorithme d'apprentissage automatique qui peut être utilisé pour des problèmes de classification, de régression et de détection d'anomalies. Il permet de séparer les données en classe à l'aide d'un hyperplan de marge optimale dont la marge correspond à la plus petite distance entre le plan séparateur et un des exemples de formation (Xiaofeng et Xiaohong, 2017). Ce réseau présenté dans (Portela *et al*., 2019) est utilisé pour détecter les anomalies dans une base de données divisée selon la méthode d'exclusion (en anglais *Holdout*), où 70% ont été utilisé dans l'ensemble d'apprentissage et les 30% restants ont été utilisé comme ensemble de test. L'algorithme atteint une précision de prédiction de 92% et un AUC de 0,97 selon (Portela *et al*., 2019). Les auteurs ont observé que l'algorithme a une probabilité de 97% de distinguer correctement entre les données normales et les données anormales (ayant une anomalie).

Algorithmes d'apprentissage supervisé pour la détection d'interférence RF :

- Réseaux de neurones (en anglais *Neural Networks* ou NN) : Ce modèle présenté dans (Harrison et Mishra, 2019) est utilisé pour détecter les interférences RF dans les données de type temps/fréquence durant la post-corrélation et post-calibration. Il est optimisé pour le nombre de couches et de nœuds, dans ce cas, une seule couche avec 512 nœuds s'avère la plus efficace en matière de précision et de rappel. Cet effet est probablement dû au fait que l'hyperplan pour la détection des interférences RF n'existe pas dans un espace dimensionnel élevé. L'algorithme atteint une précision de prédiction de 82,8%.

- Réseaux de neurones à convolution (CNN) U-net : Ce réseau présenté dans (Akeret, Chang, Lucchi, et Refregier, 2017) est un type de CNN qui est utilisé pour détecter et atténuer les interférences RF dans les données ordonnées dans le temps (TOD) d'un radiotélescope.

  L'U-net modifie l'architecture traditionnelle d'un CNN. Le réseau se compose d'une partie contractante et d'une voie expansive. La partie contractante est composée d'une application répétée de convolutions, chacune suivi d'une unité de transformation ReLU (unité de rectification linéaire) afin d'introduire une non-linéarité dans le modèle, et d'une opération de pooling maximal 2x2 dans laquelle le réseau de neurones convolutif sous-échantillonne la caractéristique convoluée. Cela produit une réduction du nombre de dimensions de la carte de caractéristiques tout en préservant les informations les plus critiques de la caractéristique. Par contre, dans la voie expansive, l'opération de pooling maximal est remplacée par une convolution ascendante qui divise en deux le nombre de caractéristiques de la couche précédente et concatène le résultat avec les caractéristiques de la couche de contraction correspondante. Finalement, afin d'obtenir une classification binaire si un pixel est contaminé ou non par une interférence RF, il est appliqué une convolution 1x1 pour mapper les caractéristiques de la dernière couche au nombre d'étiquettes de classe. Et si on veut obtenir la probabilité d'un pixel

d'appartenir à une certaine classe, la carte de sortie résultante doit être convertie avec une couche soft-max. Enfin, l'algorithme atteint un AUC (en anglais *Area Under the ROC Curve)* de 0,809 selon (Akeret *et al*., 2017).

2.2.1.2.1.1 Limitations de l'apprentissage supervisé

Les algorithmes d'apprentissage supervisé étudiés ci-dessus nécessitent une grande base de données pendant la phase de formation, telles que Kyoto 2006 + (en anglais *Kyoto 2006 + Dataset*) dans (Sahu et Mehtre, 2015), KDDCUP99 (en anglais *KDDCUP99 Dataset)* dans (Lei, 2017), IPIX (en anglais *IPIX Dataset of McMaster University in Canada*) dans (Guo et Shui, 2020), NAB (en anglais *Numenta Anomaly Benchmark Dataset*) dans (Ding *et al*., 2018), CSIR (en anglais *CSIR Dataset of South Africa*) dans (Guo et Shui, 2020) et UNSW-NB15 (en anglais *UNSW-NB15 Dataset from the Australian Cyber Security Center*) dans (Portela *et al*., 2019). En général, nous observons que les algorithmes d'apprentissage supervisé atteignent une excellente précision, mais ils présentent aussi d'autres inconvénients :

- L'étiquetage des données de formation : La phase d'annotation de données est coûteuse et prend beaucoup de temps.
- Le surapprentissage : Afin d'obtenir une meilleure performance et d'éviter le surapprentissage, il faut avoir une grande base de données et avec des données diversifiées.
- Temps d'exécution : La phase de formation nécessite beaucoup de temps de calcul.

2.2.1.2.2 Algorithmes d'apprentissage non supervisé pour la détection d'interférence RF et la détection d'anomalies

Les algorithmes d'apprentissage non supervisé ont l'avantage d'être formés sur des données non étiquetées, contrairement à l'apprentissage supervisé. D'ailleurs, la majeure partie des données qui sont recueillies en intelligence artificielle sont de ce type.

Parmi les algorithmes d'apprentissage non supervisé les plus couramment utilisés pour la détection d'anomalies figurent l'algorithme K-means (en anglais *K-Means Algorithm*) (Portela *et al*., 2019) (Li, 2010), l'algorithme Isolation Forest (en anglais *Isolation Forest algorithm*) (Zhang, Kang, et Li, 2019) (Zhong *et al*., 2019), le réseau de neurones récurrents (en anglais

Recurrent Neural Networks) (Goh, Adepu, Tan, et Lee, 2017), le SVDD (en anglais *Support Vector Data Description*) (Banerjee, Burlina, et Meth, 2007) (Dong et Zhang, 2019), et la machine à vecteurs de supports à classe unique (en anglais *One-Class SVM*) (Inoue, Yamagata, Cheng, Poskitt, et Sun, 2017) (Budiarto, Permanasari, et Fauziati, 2019). Nous pouvons noter que tous ces algorithmes atteignent une bonne précision sur la base des références précédentes. À titre d'exemple, dans cette section, on présentera certains de ces algorithmes pour la détection d'anomalies et pour la détection d'interférences RF présente dans la littérature. Ensuite, on verra une possible limitation de l'apprentissage non supervisé.

Algorithmes d'apprentissage non supervisé pour la détection d'anomalies :

- Algorithme K-means : Il s'agit de l'algorithme de clustering centroïde le plus utilisé. Il permet d'identifier des clusters dans un ensemble de points en regroupant les échantillons dans un des *K* clusters, où chaque cluster est représenté par un prototype (Xu et Tian, 2015). Cet algorithme présenté dans (Portela *et al*., 2019) est utilisé pour détecter les anomalies dans une base de données de 82332 échantillons. Pendant la phase d'entrainement une valeur de *K*=5 a été obtenu, étant le nombre de clusters adéquat pour la base de données.

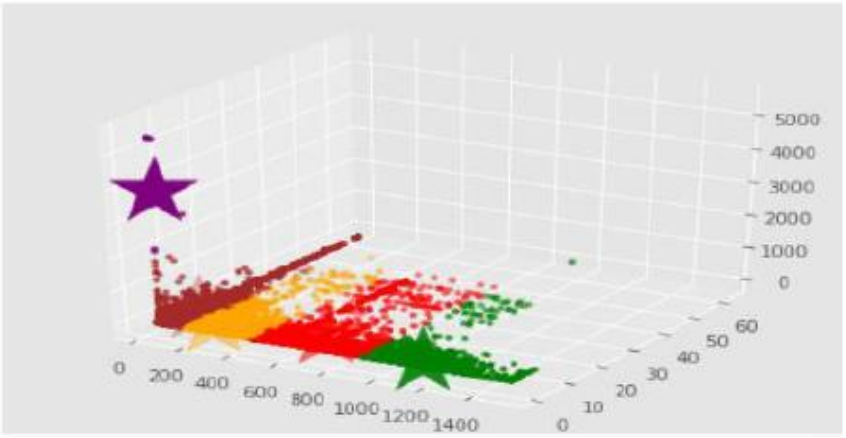

Figure 2.2 Les clusters (Portela *et al*., 2019)

La figure 2.2 montre les clusters obtenus par l'algorithme. Les clusters en rouge et orange sont des données normales et les clusters en marron, vert et violette sont des données anormales.

- Algorithme Isolation Forest : Il s'agit d'un algorithme efficace qui cherche à isoler les observations avec des coupures successives et aléatoires (arbres de décision) dans une vaste base de données. Les points faciles à isoler qui sont seuls ou dans une région à faible densité sont considérés comme des anomalies. Au contraire, les points issus de zones à forte densité sont considérés comme normaux (Portela *et al*., 2019). Cet algorithme présenté dans (Zhang *et al*., 2019) est utilisé pour détecter les anomalies dans les images hyper-spectrales, en isolant directement les pixels d'anomalie de l'arrière-plan. L'algorithme atteint un AUC (en anglais *Area Under the ROC Curve)* de 0.99, ce qui signifie que l'algorithme a une probabilité de 99% de distinguer correctement entre les données normales (ne contiennent pas d'anomalies) et les données anormales (ayant une anomalie).

Algorithme d'apprentissage non-supervisé pour la détection d'interférences RF :

- Auto-encodeur convolutionnel (en anglais *Convolutional Autoencoder* ou CAE) : Il s'agit d'un algorithme qui permet de copier son entrée dans sa sortie en apprenant à compresser les données tout en minimisant l'erreur de reconstruction (Goodfellow, Bengio, et Courville, 2016). Cet algorithme présenté dans (Ghanney et Ajib, 2020) est utilisé pour détecter les interférences RF dans une base de données provenant d'un convertisseur analogique-numérique dont la source et l'une des antennes du Very Large Array (VLA). L'algorithme atteint une précision moyenne de 78%, ce qui signifie que l'apprentissage non-supervisé peut être utilisé de façon efficace pour la détection des interférences RF.

2.2.1.2.2.1 Limitation de l'apprentissage non supervisé

Les algorithmes d'apprentissage non supervisé vus précédemment ont besoin également d'une grande base de données comme dans le cas de l'apprentissage supervisé pendant la phase de formation. Par exemple, la base de données SWaT (en anglais *Secure Water Treatment Dataset*) dans (Inoue *et al*., 2017). En revanche, le One-Class SVM (Schölkopf, Platt, Taylor, Smola, et Williamson, 2001) et le SVDD (Tax et Duin, 2004) montrent d'excellents résultats en termes de précision dans la détection d'anomalies, sans avoir besoin

d'une grande base de données. D'autre part, les algorithmes d'apprentissage non supervisé présentent l'inconvénient possible suivant :

- Généralement, la précision obtenue pour la détection d'anomalies n'est pas aussi bonne que celle obtenue en utilisant l'apprentissage supervisé (Wankhede, 2019) (Portela *et al*., 2019). Mais il y a quelques exceptions, par exemple, l'algorithme Isolation Forest qui atteint un AUC de 0.99 dans (Zhang *et al*., 2019).

2.2.1.2.3 Algorithmes d'apprentissage par renforcement pour la détection d'interférence RF et la détection d'anomalies

Dans la détection d'anomalies basée sur l'apprentissage par renforcement, l'apprentissage par renforcement antagoniste (en anglais *Adversarial Reinforcement Learning* ou ARL) (Ma et Shi, 2020) (Suwannalai et Polprasert, 2020) et l'apprentissage par renforcement profond (en anglais *Deep Reinforcement Learning* ou DRL) (Aberkane et Elarbi, 2019) (Hsu et Matsuoka, 2020) sont les algorithmes les plus couramment utilisés à cette fin. Nous pouvons noter que tous ces algorithmes atteignent une bonne précision pour détecter les anomalies dans des bases de données du monde réel. À titre d'exemple, dans cette section, on présentera certains de ces algorithmes pour la détection d'anomalies et pour la détection d'interférences RF présentent dans la littérature. Ensuite, nous verrons une possible limitation de l'apprentissage par renforcement.

Algorithmes d'apprentissage par renforcement pour la détection d'anomalies :

- Apprentissage par renforcement antagoniste avec la technique de suréchantillonnage des minorités synthétiques (en anglais *Adversarial Reinforcement Learning with Synthetic Minority Oversampling Technique* ou AESMOTE) : Dans l'algorithme AESMOTE l'apprentissage par renforcement parvient à diminuer l'écart entre la simulation et le monde réel en utilisant un agent d'environnement pour faire face à une propriété dite déséquilibre, laquelle produit un déséquilibre dans la base de données. De plus, la technique SMOTE (en anglais *Synthetic Minority Oversampling Technique*) permet de générer des exemples synthétiques de la classe minoritaire, ainsi l'algorithme peut apprendre efficacement la frontière de décision, ce qui signifie une amélioration

de la performance de l'algorithme (Ma, 2020). Cet algorithme présenté dans (Ma et Shi, 2020) est utilisé pour détecter les anomalies dans la base de données NSL-KDD, laquelle présente des données déséquilibrées. L'algorithme atteint une précision de 82.43%. Les auteurs observent que l'algorithme AESMOTE atteint une meilleure précision que l'algorithme AE-RL (en anglais *Adversarial Reinforcement Learning*) grâce à la technique d'augmentation de données SMOTE.

- Apprentissage par renforcement profond (en anglais *Deep Reinforcement Learning* ou DRL) : L'algorithme DRL est une combinaison d'apprentissage par renforcement et d'apprentissage profond, où les réseaux de neurones profonds peuvent apprendre des comportement complexes en les formant avec des données générées dynamiquement à partir des modèles de simulation qui représente l'environnement (Li *et al*., 2019). Cet algorithme présenté dans (Aberkane et Elarbi, 2019) nommé DQN (en anglais *Deep Q Learning* Network) est utilisé pour détecter les anomalies dans une base de données d'environ 1900 vidéos de surveillance du monde réel, avec 13 cas d'anomalies réalistes. L'algorithme atteint une précision de 78.2%, ce qui donne une performance de reconnaissance vidéo très compétitive.

Algorithmes d'apprentissage par renforcement pour la détection d'interférences RF :

- L'algorithme Q-learning : Cet algorithme d'apprentissage par renforcement présenté dans (Li, Shao, Zhou, et Zhao, 2020) permet la détection et la prévention des interférences RF dans les stations de communication. Pour cela, ils proposent deux méthodes : i) Lorsqu'un canal de données utilisé est contaminé par des interférences RF, la station peut éviter les interférences en passant de ce canal vers un autre canal de meilleure qualité de transmission et ii) Lorsqu'un canal « n » utilisé est contaminé par des interférences RF, la station peut éviter les interférences en augmentant la puissance d'émission de la station sur le canal « n ». Si cela n'est pas suffisant, la station passera du canal « n » vers d'autres canaux ayant une meilleure qualité de transmission. Dans

les deux cas, l'algorithme atteint une précision supérieure à 96%, ce qui démontre l'efficacité de l'apprentissage par renforcement pour détecter et éviter les interférences RF dans les systèmes de communication.

- L'algorithme DDQN (en anglais *Double Deep Q-learning*) : Cet algorithme d'apprentissage par renforcement profond présenté dans (Aref et Jayaweera, 2019) permet de détecter et d'éviter les interférences RF dans un environnement à large bande partiellement observable. La performance de cet algorithme a été comparée avec trois autres approches : i) l'apprentissage par renforcement profond ou DRL, ii) l'algorithme par renforcement Q-learning et iii) l'utilisation de la technique dite *random* qui utilise la radio cognitive autonome à large bande (en anglais *Wideband autonomous cognitive radio* ou WACR) pour choisir un canal de façon aléatoire. L'algorithme atteint 97,5% de la récompense maximale possible, tandis que le DRL, Q-learning et random atteignent respectivement 92,5 %, 87,5% et 77,5% respectivement. Par conséquent, cet algorithme s'avère prometteur dans le domaine de détection des interférences RF.

2.2.1.2.3.1 limitations et avantages de l'apprentissage par renforcement

En général, nous observons que l'apprentissage par renforcement présente deux avantages. Premièrement, il est capable de traiter des grandes bases de données et en temps réel, par exemple, la base de données NSL-KDD dans (Ma et Shi, 2020). Deuxièmement, il est capable d'apprendre par lui-même sans supervision. Cependant, ces algorithmes nécessitent une grande base de données pendant la phase de formation comme dans le cas de l'apprentissage supervisé et l'apprentissage non supervisé. De plus, les algorithmes d'apprentissage par renforcement comportent une possible limitation qui pourrait affecter la performance de l'algorithme en termes de détection d'interférences RF :

- Possible risque de surapprentissage de l'environnement par les agents de l'algorithme RL. C'est-à-dire, ils peuvent fonctionner de façon inefficace dans des environnements légèrement différents (Kanagawa et Kaneko, 2019).

2.2.1.2.4 Les réseaux adverses génératifs (GANs) et leur extension pour la détection d'anomalie

Le but d'un GAN standard (Goodfellow *et al*., 2014) est d'apprendre la distribution réelle des données de formation, et il a été appliqué avec succès pour modéliser des distributions complexes et de grande dimension des données du monde réel. Donc, cette caractéristique suggère qu'il peut être utilisé avec une grande performance pour la détection d'anomalie en utilisant un seuil qui permet de distinguer entre l'image générée et l'image cible, étant donné qu'une observation est considérée comme une anomalie s'il est difficile de produire une donnée similaire au moyen d'un générateur (Schlegl, Seebock, Waldstein, Erfurth, et Langs, 2017).

Par la suite, nous commencerons par définir le principe de fonctionnement du GAN standard et nous montrerons l'utilisation de leur extension pour la détection d'anomalie en indiquant les avantages et les inconvénients.

2.2.1.2.4.1 Réseaux adverses génératifs (GANs) standard

Le GAN standard est composé : i) d'un réseau discriminatif D qui est un CNN avec classification binaire et ii) d'un réseau génératif G qui est un réseau de sur-échantillonnage. Le réseau génératif essaie de confondre le réseau discriminatif et le réseau discriminatif essaie de distinguer entre les images réelles et les fausses.

La structure générale du GAN standard est illustrée dans la figure 2.3. On observe que le réseau discriminatif a comme entrée des images réelles et des images générées par le réseau génératif. Par ailleurs, le réseau génératif a comme entrée un bruit aléatoire et tente de produire une sortie que le discriminateur classifiera comme étant de la base de données des images réelles.

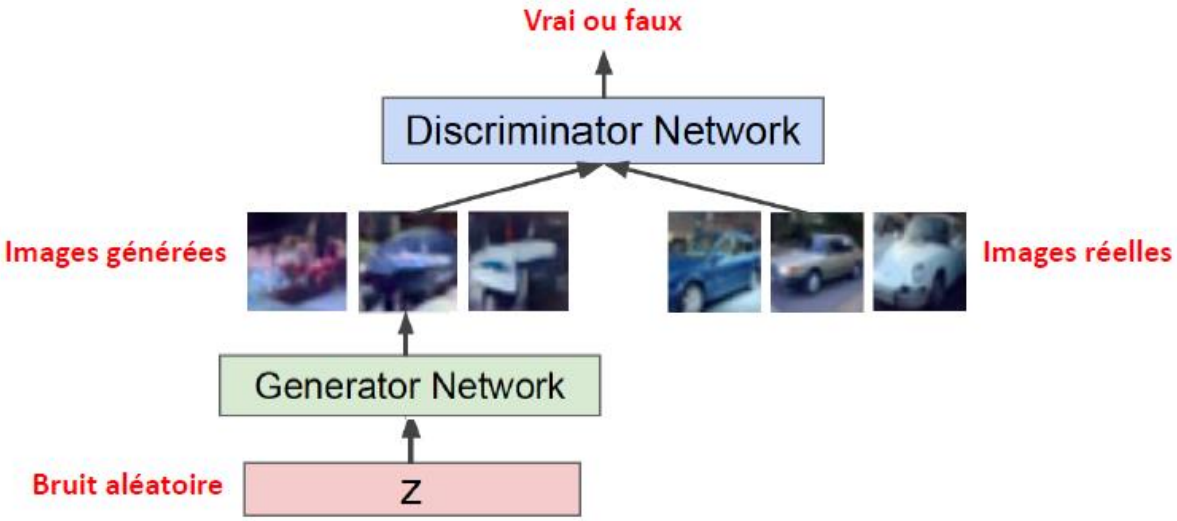

Figure 2.3 Structure générale du GAN (Denton, Chintala, Szlam, et Fergus, 2015)

Une fois le GAN standard est formé, le réseau génératif et le réseau discriminatif peuvent être utilisés séparément. Par exemple : i) le réseau génératif permettra de générer des images synthétiques qui ressemblent aux images réelles de la base de données et ii) le réseau discriminatif sera vu comme un classificateur binaire déjà formé avec un modèle qui minimise la perte.

Un autre avantage du GAN standard est la capacité à apprendre des modèles génératifs mappant de simples distributions latentes à des distributions de données arbitrairement complexes qui peut être très utiles dans la détection d'anomalies. Cependant, le GAN standard n'a aucun moyen d'apprendre la cartographie inverse en projetant des données dans l'espace latente. De plus, il peut présenter des problèmes d'instabilité durant la phase de formation.

2.2.1.2.4.2 L'utilisation des extensions du GAN standard pour la détection d'anomalie

Les extensions d'un GAN standard utilisées pour la détection d'anomalie est un domaine actif de recherche. Dans ce cas, le générateur et le discriminateur du GAN standard sont conditionnés sur des informations supplémentaires telles que : i) d'autres données, ii) des couches supplémentaires et/ou iii) la modification de l'architecture du modèle.

AnoGAN (Schlegl *et al*., 2017) est la première extension du GAN standard proposée pour la détection d'anomalie, mais il présente quelques problèmes de performance. Afin de régler ces problèmes, une approche basée sur BiGAN (Donahue, Krähendühl, et Darrel, 2017) appelée EGBAD a été proposée par (Zenati, Foo, Lecouat, Manek, et Chandrasekhar, 2018). Ensuite, une approche basée sur l'auto-encodeur GAN + a été plus performante que l'EGBAD en termes de métriques d'évaluation et de vitesse d'exécution. Finalement DCGAN (Radford et Metz, 2016), a été aussi utilisé pour la détection d'anomalies.

Dans la suite, nous aborderons l'architecture, les métriques, les avantages et les inconvénients de chaque extension du GAN standard.

2.2.1.2.4.2.1 Détection d'anomalies non supervisée par des réseaux adverses génératifs (AnoGAN)

AnoGAN (Schlegl *et al*., 2017) permet de détecter des anomalies dans les images. Pour cela, l'algorithme qui a comme modèle de base le GAN standard est formé uniquement sur des échantillons positifs, pour apprendre un mappage de la représentation de l'espace latent z à l'échantillon réaliste $x' = \mathrm{G}(z)$. Cette représentation apprise est utilisée pour mapper de nouveaux échantillons invisibles vers l'espace latent. En formant le GAN avec une base de données normale (qui ne contient pas d'anomalies), le générateur peut apprendre la variété X d'images normales. Lorsqu'une image anormale est codée, sa reconstruction peut être anormale. Pendant la phase de validation, on trouve le vecteur latent qui mappe les images de validation à sa représentation latente. Pour désigner la région anormale, l'image reconstruite montrera les anomalies à l'aide d'un détecteur qui calcule le score d'anomalie des images invisibles. Donc, le mappage des échantillons d'entrées vers l'espace latent est un processus itératif qui est défini comme la minimisation à travers les étapes de rétro-propagation $\gamma = 1, 2, \dots, \Gamma$ de la fonction de perte définie comme la somme pondérée de la perte résiduelle et de la perte de discrimination.

Les deux étapes d'apprentissage et de détection des anomalies sont illustrées ci-dessous.

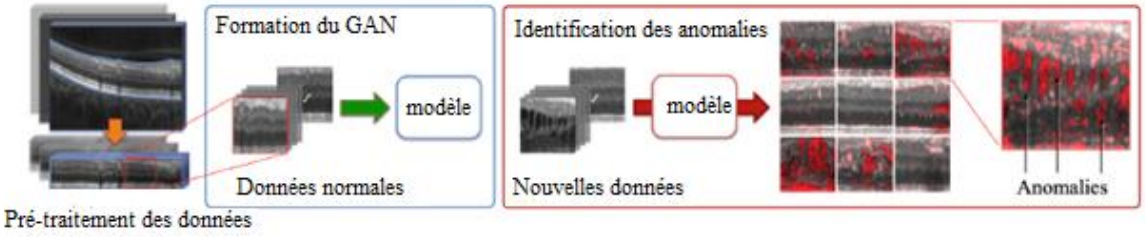

Figure 2.4. Les étapes d'apprentissage et de détection des anomalies en utilisant l'AnoGAN (Schlegl *et al*., 2017)

D'après la figure 2.4, on observe que l'étape de prétraitement consiste en l'extraction et l'atténuation des données, l'extraction du patch et la normalisation de l'intensité. Puis, le GAN effectue la phase de formation avec une base de données normale. Et finalement, lorsque des données invisibles arrivent, le modèle essaye de trouver la variable latente z qui génère une image d'entrée à l'aide de la rétro-propagation. Etant donné que le générateur apprend à générer des échantillons normaux, lorsqu'une image anormale est codée, sa reconstruction ne sera pas normale. Par conséquent, la différence entre l'entrée et l'image reconstruite mettra en évidence les anomalies.

Le score d'anomalies calculé par le détecteur est basé sur les pertes résiduelles et sur la discrimination. Ces dernières sont définies comme suit :

- La perte résiduelle est la mesure de dissimilarité visuelle entre l'image de la requête x et l'image générée par le générateur G(z) du GAN.

$$\int_R(z_y) = \sum|x - G(z_y)| \tag{2.3}$$

  Où x est l'image de la requête et $G(z_y)$ est l'image générée par le réseau génératif du GAN.

- La perte de discrimination est la mesure de dissimilarité entre les représentations cachées de l'image générée et de validation, extraite par de discriminateurs.

$$\int_D(z_y) = \sum|f(x) - f(G(z_y))|. \tag{2.4}$$

  Où la sortie d'une couche intermédiaire $f(\cdot)$ du réseau discriminatif du GAN est utilisée pour spécifier les statistiques de l'image d'entrée x ou de l'image générée par le réseau génératif du GAN $G(z_y)$.

Alors, la perte totale pour trouver la variable latente z est la somme pondérée des deux pertes, avec λ = 0,1 par défaut.

$$\int(z_y) = (1-\lambda)\cdot\int_R(z_y) + \lambda\cdot\int_D(z_y). \quad (2.5)$$

Donc, d'après l'approche décrite ci-dessus le score d'anomalies n'est pas facile à interpréter et il y a Γ étapes d'optimisation pendant l'inférence.

La performance de l'AnoGAN a été évaluée en le comparant avec GAN_R (Réseau adversaire génératif avec score de référence) et avec aCAE (Réseau adversaire génératif convolutionnel auto-encodeurs). Les performances des réseaux de neurones sont également évaluées.

Les résultats de l'évaluation ont démontré selon (Schlegl *et al*., 2017) que l'AnoGAN est capable de détecter les anomalies avec une précision plus élevées. Cependant, selon l'aire sous la courbe ROC (AUC), l'AnoGAN et GAN_R montrent des résultats similaires parce que tous les deux ont une bonne performance du score résiduel. Donc, nous pouvons conclure que la détection d'anomalies peut être effectuée à l'aide des réseaux de type GAN.

2.2.1.2.4.2.2 Détection des anomalies basée sur le GAN (EGBAD)

EGBAD (Zenati *et al*., 2018) est basé sur les réseaux adverses génératifs bidirectionnels BiGAN afin de détecter des anomalies dans les images. L'architecture du BiGAN est illustrée ci-dessous :

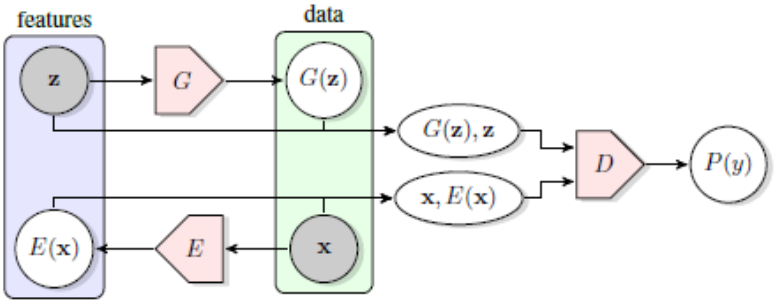

Figure 2.5 L'architecture du BiGAN (Donahue *et al*., 2017)

D'après la figure 2.5, BiGAN (Donahue *et al*., 2017) ajoute un codeur E à l'architecture standard du générateur G et discriminateur D du GAN qui cartographie (en anglais *map*) les

données x aux représentations latentes z, et il apprend l'inverse du générateur $E = G^{-1}$. Ici, le discriminateur distingue non seulement entre les données réelles et les échantillons générés par le générateur G, mais il distingue également la divergence entre le codeur E et le générateur G.

Comme vu dans la section précédente, l'AnoGAN présente quelques inconvénients et ces inconvénients sont corrigés par EGBAD qui permet d'apprendre un encodeur qui mappe les échantillons d'entrée x à une représentation latente z, avec un générateur et un discriminateur pendant la phase de formation. Donc, cela permet d'éviter l'étape coûteuse en calcul consistant à récupérer une représentation latente z au moment de la phase de validation. Un autre avantage important est qu'il permet de calculer le score d'anomalies sans les étapes d'optimisation Γ lors de l'inférence comme cela se passe dans l'AnoGAN.

La performance de EGBAD a été évaluée en faisant une comparaison avec l'AnoGAN et d'autres algorithmes, en utilisant la base de données de haute dimension KDD99.

Les résultats indiquent selon (Zenati *et al*., 2018) que EGBAD est capable de détecter les anomalies avec une précision plus élevées que l'AnoGAN. Nous pouvons ainsi conclure que la détection d'anomalies sur une base de données complexe de grande dimension peut être effectuée à l'aide des GAN.

2.2.1.2.4.2.3 Détection d'anomalies semi-supervisée via une formation contradictoire (GANomaly)

La méthode GANomaly (Akcay, Abarghouei, et Breckon, 2018) est basée sur l'hypothèse selon laquelle l'utilisation d'auto-encodeurs et de l'architecture du GAN s'avère prometteuse dans le domaine de détection d'anomalies, comme vu dans les approches précédentes AnoGAN et EGBAD.

L'architecture du GANomaly est illustrée ci-dessous.

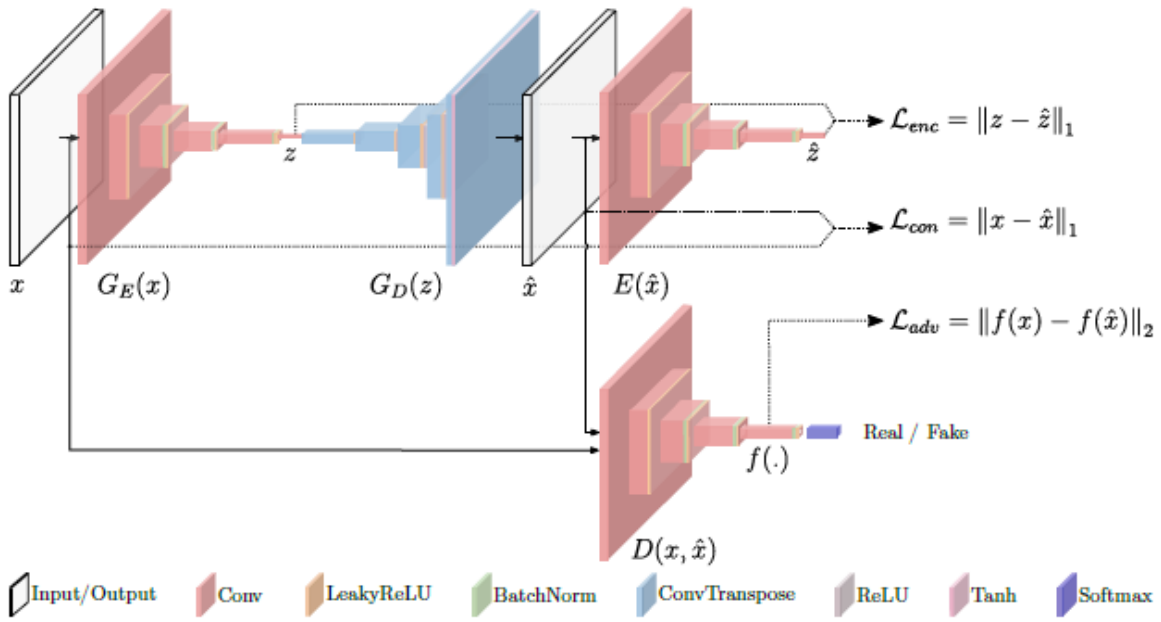

Figure 2.6 L'architecture du GANomaly (Akcay *et al*., 2018)

D'après la figure 2.6, GANomaly est composé d'un générateur qui est constitué de trois éléments en série : i) l'encodeur G_E ii) le décodeur G_D et iii) l'encodeur E. Et finalement d'un discriminateur D comme le GAN standard.

Cette architecture forme le générateur G sur des images normales afin qu'il puisse apprendre leur variété X tandis qu'en parallèle l'auto-encodeur (l'encodeur G_E plus le décodeur G_D) est formé pour apprendre l'encodage des images dans leur représentation latente de façon efficiente. Ici, G_E a comme entrée une image x et donnera une version codé z de cette image en sortie. Par conséquent, z devient l'entrée du décodeur G_D qui donnera $\hat{x}$, la version reconstruite de x. Finalement, $\hat{x}$ devient l'entrée de l'encodeur E qui donnera $\hat{z}$. Avec cette architecture pour le générateur, on obtient deux contributions importantes : i) le principe de fonctionnement de la détection d'anomalies est basé sur la structure de l'auto-encodeur qui mettra en évidence où se trouvent les anomalies de façon claire et visible et ii) l'encodeur E, pendant la phase de formation, permet d'apprendre à encoder les images afin d'avoir la meilleure représentation de x qui pourrait conduire à sa reconstruction $\hat{x}$.

Donc, l'architecture de GANomaly diminue le temps de formation en utilisant l'auto-encodeur et le score d'anomalies est plus facile à interpréter. La performance de GANomaly a été évaluée en faisant une comparaison avec l'AnoGAN et EGBAD, en utilisant les bases de données MNIST et CIFAR (Akcay *et al*., 2018). Il est montré que GANomaly a la meilleure performance du point de vue de l'AUC (aire sous la courbe ROC). De plus, GANomaly présente la meilleure performance en termes de temps d'exécution.

2.2.1.2.4.2.4 Détection d'anomalies avec le réseau adversaire génératif convolutionnel profond (DCGAN)

Le DCGAN a été utilisé comme approche de détection d'anomalies pour les composants de soutien caténaire (en anglais *catenary support components* ou CSC) (Lyu, Han, Zhong, Li, et Liu, 2020) dans le système ferroviaire afin de diminuer l'interruption de service car plusieurs pannes sont dues au CSC.

Dans ce domaine d'application, l'apprentissage supervisé n'est pas convenable car le nombre d'échantillons d'anomalies disponible est petit, et pour éviter le surapprentissage on a besoin d'une grande base de données afin d'obtenir une performance acceptable sur un nouvel ensemble de données. Donc, afin de surmonter ce problème, le DCGAN est utilisé pour générer des images synthétiques. De plus, il est entraîné pour trouver la distribution de probabilité stable de la base de données d'images normales du CSC ; laquelle sera utilisée pour un détecteur d'anomalies pour distinguer entre une image normale (similaire à la basse de données d'images normales selon la distribution de probabilité trouvée par le DCGAN) ou une image anormale (contient des anomalies) sur les nouvelles images capturées.

La performance de l'approche basée sur DCGAN a été évaluée et comparée avec celle de deux algorithmes de segmentation d'image traditionnels EM/MPM et ICM (Lyu *et al*., 2020), en utilisant une base de données de 100000 images. Après 25 époques de formation du DCGAN, des images synthétiques de la ligne isoélectrique et l'isolateur sont obtenues (Lyu *et al*., 2020). Les auteurs de (Lyu *et al*., 2020) ont observé la grande qualité des images synthétiques générées par le DCGAN à partir d'un ensemble de données des images de haute dimension et complexes. Donc, nous pouvons conclure que le DCGAN peut être utilisé pour générer une

base de données des images synthétiques et par conséquent éviter le surapprentissage dans plusieurs domaines, où il est difficile d'obtenir une grande base de données. De plus, l'approche proposée présente une grande précision (100 %) pour la détection d'anomalies. L'approche basée sur le DCGAN montre la meilleure performance du point de vue de la précision pour la détection d'anomalies. Cependant, il a besoin d'une grande base de données pendant la phase de formation.

2.3 Conclusion

Dans ce chapitre, nous avons présenté une revue de littérature contenant plusieurs méthodes de détection d'interférences RF et de détection d'anomalies et qui possèdent leurs avantages et leurs inconvénients. Nous avons vu que les technologies de détection d'interférences RF conventionnelles comportent plusieurs limitations. Par contre, l'apprentissage automatique apparaît comme une alternative innovante et plus efficace pour détecter les interférences RF ou les anomalies. Cependant, nous allons utiliser une approche non supervisée plutôt qu'une approche supervisée car nous voulons éviter les limitations de cette dernière.

En supposant qu'il n'y a pas assez d'information sur les interférences RF ou que nous n'avons qu'une petite base de données, le GAN standard et leur extension ne peuvent pas être utilisés pour la détection d'anomalies car ils ont besoin d'une grande base de données pendant la phase de formation. En revanche, il est possible de repérer les interférences RF comme un problème de classification à une classe grâce à la technique de détection d'anomalies vue dans la section 2.2.1.2 et en utilisant une petite base de données à l'aide du One-Class SVM et du SVDD vus dans la section 2.2.1.2.2. Donc, le One-Class SVM et le SVDD seront utilisés pour détecter les interférences RF provenant d'un signal radio FFT (Transformée de Fourier rapide) et un scalogramme des signaux RFI, et nous calculerons son temps d'exécution ainsi que ses performances et sa précision afin de pouvoir les comparer concrètement via des graphiques et des résultats avec d'autres algorithmes.

Dans le chapitre suivant, nous présenterons le fonctionnement du One-Class SVM et du SVDD pour détecter les interférences RF.

CHAPITRE III

ALGORITHMES D'APPRENTISSAGE NON SUPERVISÉ UTILISÉS

3.1 Introduction

Dans ce chapitre, nous présenterons le fonctionnement du One-Class SVM et du SVDD vu qu'ils vont être utilisés dans ce mémoire comme un outil de détection des interférences RF.

3.2 One-Class SVM

One-Class SVM a été proposé pour la première fois dans (Schölkopf *et al*., 2001). Il est basé sur la détection de nouveautés (en anglais *Novelty Detection*), en essayant d'apprendre une frontière proche délimitant le contour de la distribution des données observées, en partant d'une base de données de formation de *N* observations de la même distribution décrite par *P* caractéristiques. Étant donnée la base de données de formation $X = \{x_i\}$, qui sont des vecteurs $\boldsymbol{x}_i \in R^l$, où $l \in \mathbb{N}$, le modèle est estimé de la manière suivante selon (Lukashevich, Nowak, et Dunker, 2009) :

$$\min_{\boldsymbol{w}, \varepsilon_i, \rho} \frac{1}{2}\boldsymbol{w}^T\boldsymbol{w} - \rho + \frac{1}{vl}\sum_{i=1}^{l}\varepsilon_i$$

$$sous\ contrainte\ \boldsymbol{w}^T\phi(\boldsymbol{x}_i) \geq \rho - \varepsilon_i, \varepsilon_i \geq 0\,, \tag{3.1}$$

où le vecteur $\boldsymbol{w}$ comprend les paramètres de l'hyperplan, ϕ est une fonction qui permet aux données d'être linéairement séparable, ε_i sont les variables d'écart (en anglais *Slack Variables*) $\varepsilon \in R^l$ introduites qui permettent à certaines données de se situer à l'intérieur de la frontière, l est le nombre total de variables d'écart, ρ est la frontière de classe (en anglais *Class Boundary*), et $v \in (0,1]$ est un paramètre de compromis (en anglais *Trade-Off Parameter*).

La solution du problème quadratique (3.1) est la fonction de décision :

$$sgn\left(\sum_{i=1}^{l}\alpha_i K(\boldsymbol{x}_i, \boldsymbol{x}) - \rho\right)\,, \tag{3.2}$$

où $K(\boldsymbol{x}_i, \boldsymbol{x}_j)$ est une fonction noyau qui permet de travailler avec des données non linéairement séparables en les cartographiant (en anglais *Mapping*) dans un espace de dimension supérieure où elles deviennent linéairement séparables, sgn est la fonction signe, et le vecteur $\boldsymbol{\alpha} = \{\alpha_i\}$ comprend les multiplicateurs de Lagrange.

Dans ce mémoire, nous utiliserons la fonction noyau à base radiale (en anglais *The Radial Basis Function Kernel* ou RBF) définie dans (3.3) et le paramètre scalaire γ pour définir une frontière.

$$K(\boldsymbol{x}_i, \boldsymbol{x}_j) = exp\left(-\gamma \|\boldsymbol{x}_i - \boldsymbol{x}_j\|^2\right). \tag{3.3}$$

Il est également nécessaire de spécifier le paramètre de compromis v dans (3.1), appelé la marge du One-Class SVM. Ce paramètre correspond à la probabilité de trouver une observation nouvelle, mais régulière, en dehors de la frontière. Selon (3.2), si les nouvelles données se situent à l'intérieur de la frontière, elles sont considérées comme des données normales ; sinon, elles sont considérées comme des données anormales. Dans ce contexte, nous utilisons le One-Class SVM car une seule classe est définie et l'apprentissage de cet algorithme est non supervisé, ce qui évite les inconvénients de l'apprentissage supervisé vus dans le chapitre précédent.

3.3 SVDD

SVDD a été proposé dans (Tax et Duin, 2004). Il est basé sur la recherche de l'hypersphère ayant le plus petit rayon qui entoure la base de données de formation x_i, où $x_i \in R^s$ est un vecteur de caractéristiques à « s » dimensions de chaque échantillon de données i. Ensuite, afin de trouver cette hypersphère, l'algorithme SVDD définit une frontière à l'aide des vecteurs de support (en anglais *Support Vectors*). Ces vecteurs de support sont un ensemble de données appartenant à la base de données de formation qui se trouvent sur la frontière séparant les données normales des celles anormales qui résident en dehors de l'hypersphère.

L'hypersphère est définie par son centre « a » et un rayon donné $R > 0$. Alors, le problème d'optimisation consiste à minimiser le volume de cette hypersphère en minimisant R^2, et exiger que l'hypersphère contienne tous les vecteurs de formation x_i. De toute façon, lorsque la base

de données de formation contient des valeurs aberrantes (en anglais *Outliers*), une variable d'écart est introduite $\varepsilon_i \geq 0$, et le problème d'optimisation est exprimé selon (3.4).

$$\min F(a, R) = R^2 + C \sum_i \varepsilon_i$$

$$sous\ contrainte\ \|\varphi(\boldsymbol{x}_i) - a\|^2 \leq R^2 + \varepsilon_i \quad \forall i \tag{3.4}$$

$$\varepsilon_i \geq 0\ et\ \forall i$$

où le paramètre *C* contrôle le compromis entre le volume de l'hypersphère et les erreurs, $F(.,.)$ est la fonction objective, φ est la fonction qui fait correspondre la caractéristique d'entrée à un espace à haute dimension avec une fonction noyau. Cette fonction φ permet de travailler avec une description de données plus flexible au lieu d'une hypersphère rigide. Par conséquent, les échantillons de données sont représentés après la transformation comme $\varphi(\boldsymbol{x}_i)$ et la fonction noyau est exprimée selon (3.5).

$$k(\boldsymbol{x}_i, \boldsymbol{x}_j) = \big(\varphi(\boldsymbol{x}_i), \varphi(\boldsymbol{x}_j)\big)\ . \tag{3.5}$$

En utilisant les multiplicateurs de Lagrange présentés dans (Tax et Duin, 2004) et la fonction de noyau dans (3.5), le centre de l'hypersphère est donné par :

$$a = \textstyle\sum_i \alpha_i^*\ \varphi(\boldsymbol{x}_i)\ . \tag{3.6}$$

Seuls les vecteurs ayant des multiplicateurs de Lagrange correspondants $0 < \alpha_i^* < C$ sont nécessaires dans la description. Ils sont appelés vecteurs de support de la description. Ensuite, comme R^2 est lié à la distance entre le centre de l'hypersphère et l'un de ces vecteurs de support sur la frontière, le rayon de l'hypersphère est donné par :

$$R^2 = \tfrac{1}{N_s} \textstyle\sum_{k=1}^{N_s} \big\{k(\boldsymbol{x}_k, \boldsymbol{x}_k) - 2 \sum_i \alpha_i^* k(\boldsymbol{x}_k, \boldsymbol{x}_i) + \sum_{ij} \alpha_i^* \alpha_j^* k\big(\boldsymbol{x}_i, \boldsymbol{x}_j\big)\big\}, \tag{3.7}$$

où N_s est le nombre total de vecteurs de support.

Dans ce mémoire, nous utiliserons le noyau polynomial. Par conséquent, (3.5) est remplacée par :

$$k(\boldsymbol{x}_i, \boldsymbol{x}_j) = \Big(\varphi(\boldsymbol{x}_i), \varphi\big(\boldsymbol{x}_j\big)\Big)^d\ , \tag{3.8),}$$

où d désigne le degré du noyau polynomial. Nous utilisons $d = 2$ pour avoir un compromis entre la valeur de précision dans la phase de formation et la valeur de précision dans la phase de test.

Selon (3.7), si les nouvelles données se trouvent à l'intérieur de la frontière, elles sont considérées comme des données normales, sinon, elles sont considérées comme des données anormales. Par conséquent, nous utilisons l'algorithme SVDD comme un classificateur à une classe et l'apprentissage de cet algorithme devient non supervisé, évitant les inconvénients de l'apprentissage supervisé.

3.4 Conclusion

Dans le cadre de ce mémoire, deux algorithmes d'apprentissage non supervisé dans le domaine des algorithmes de détection d'anomalies vont être appliqués pour la détection des interférences RF. Bien que les détecteurs d'anomalies à deux classes offrent une grande précision dans la détection des objets, ils ont besoin d'une très grande base de données à la phase de formation. Au lieu de cela, nous adoptons deux détecteurs à une classe, à savoir le SVDD et le One-Class SVM, qui offrent le meilleur compromis entre précision et taille de base de données.

Dans le chapitre suivant, nous présenterons les résultats obtenus avec les algorithmes proposés et les comparerons avec d'autres algorithmes récents utilisés pour la détection des interférences RF.

CHAPITRE IV

SOLUTION PROPOSÉE ET RÉSULTATS

4.1 Introduction

Dans ce mémoire, nous proposons d'utiliser le One-Class SVM et le SVDD comme algorithmes de détection d'objets pour détecter et localiser les différents types d'interférences RF.

Dans ce chapitre, nous commencerons par décrire les différentes étapes suivies pour la réalisation de la phase d'expérimentation, c-à-d, la formation du One-Class SVM et la formation du SVDD. Par la suite, nous évaluerons le rendement de l'approche proposée en fonction des métriques disponibles sur Google Colab (Carneiro *et al.*, 2018) pour juger des performances de nos algorithmes.

4.2 L'ensemble de données

Dans ce mémoire, nous utilisons l'ensemble de données suivant :

- L'ensemble de données des images de scalogramme des données réelles RF : Cette base de données de 4800 images format PNG contient le scalogramme de quatre types de signaux RF : i) le signal d'intérêt (en anglais *Signal of Interest* ou SOI), ii) les interférences d'ondes continues (en anglais *Continuous Wave Interference* ou CWI), iii) les interférences multiples d'ondes continues (en anglais *Multiple Continuous Wave Interference* ou MCWI), et iv) l'interférence Chirp (en anglais *Chirp Interference* ou CI). Ces données sont obtenues à partir d'un flux vidéo en temps réel, qui est modulé et traité par le logiciel GNU Radio (Ujan, Navidi, et Landry, 2020).

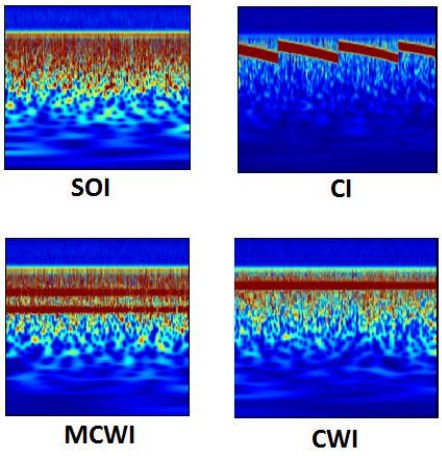

Figure 4.1 Images de scalogramme de quatre types de signaux RF (format PNG de dimension 224 x 224 pixels)

Afin d'utiliser correctement les deux ensembles de données pour que les algorithmes fonctionnent efficacement, nous effectuons un prétraitement des données des signaux RF illustrés sur la figure 4.1, comme suit :

- Préparation des données : Les données doivent être dans un format accepté par l'algorithme. D'abord, nous redimensionnons les images pour qu'elles correspondent à la dimension de la couche d'entrée de l'algorithme. De plus, nous transformons les images de format JPG ou PNG en format tenseur et tableau numpy (en anglais *Numpy Array*) afin que l'algorithme puisse reconnaître les données dans Google Colab.

- Normalisation des données : Nous normalisons les données, une exigence commune à de nombreux algorithmes d'apprentissage automatique afin d'éviter les erreurs lors de la phase de formation. Par exemple, un algorithme peut être incapable d'apprendre correctement d'autres caractéristiques si une caractéristique a une variance supérieure de plusieurs ordres de grandeur à celle des autres. Donc, premièrement, nous normalisons les valeurs du canal RVB (en anglais *Red Green Blue* ou RGB) qui sont dans l'intervalle $[0, 255]$, ce qui n'est pas idéal pour un réseau de neurones, pour qu'elles soient dans l'intervalle $[0, 1]$ en utilisant une couche de redimensionnement. Cette méthode de normalisation est appelée mise à l'échelle des caractéristiques sur

une plage (en anglais *Scaling Features to a Range*) qui permet d'ajouter de la robustesse aux très petits écarts types ou caractéristiques et de préserver les entrées nulles dans les données éparses. Deuxièmement, nous utilisons la normalisation standard (en anglais *Standard Scaler*) (Yeo et Johnson, 2000) pour normaliser les caractéristiques en supprimant la moyenne et en mettant à l'échelle la variance unitaire. Dans ce cas, le score standard d'un échantillon i est calculé comme suit :

$$z = (i - u)/s \,, \tag{4.1}$$

où u est la moyenne des échantillons d'apprentissage et s est l'écart-type des échantillons d'apprentissage.

Enfin, nous utilisons la normalisation robuste (en anglais *Robust Scaler*) (Yeo et Johnson, 2000), qui est utilisé lorsque la base de données contient de nombreuses valeurs aberrantes qui peuvent influencer la moyenne/variance de l'échantillon de manière négative. Dans ce cas, la normalisation robuste supprime la médiane et met les données à l'échelle selon l'intervalle des quantiles.

Après la normalisation de la base de données, nous formons le One-Class SVM et le SVDD en utilisant uniquement des données normales. Ces algorithmes sont testés avec deux sous-ensembles : l'un avec de nouvelles données normales et l'autre avec de nouvelles données anormales.

4.3 Les métriques de mesure de performance des algorithmes d'apprentissage automatique

Il est très important de définir les critères à utiliser pour l'évaluation de la performance de nos algorithmes, car ils servent aussi à comparer la performance de nos algorithmes avec ceux vus aux chapitre 2. Donc, nous utiliserons les critères d'évaluation suivants :

- Classe positive : Signaux non contaminés par des interférence RF.
- Classe négative : Signaux contaminés par des interférences RF.

- VP (vrai-positifs) : Ce critère mesure quand l'algorithme prédit correctement la classe positive, c.-à-d., le nombre des signaux non contaminés par des interférences RF correctement classifiés.

- VN (vrai-négatifs) : Ce critère mesure quand l'algorithme prédit correctement la classe négative, c.-à-d., le nombre des signaux contaminés par des interférences RF correctement classifiés.

- FP (faux-positifs) : Ce critère mesure quand l'algorithme prédit incorrectement la classe positive, c.-à-d., le nombre des signaux non contaminés par des interférences RF classifiés comme des signaux contaminés.

- FN (faux-négatifs) : Ceci mesure quand l'algorithme prédit incorrectement la classe négative, c.-à-d., le nombre des signaux contaminés par des interférences RF classifiés comme des signaux non contaminés.

- Précision : Cette statistique correspond à la fréquence à laquelle l'algorithme de classification prédit correctement la classe positive. Elle est définie comme suit :

$$Précision = \frac{VP}{VP+FP} \quad . \tag{4.2}$$

  Où VP sont les vrai-positifs et FP sont les faux-positifs.

- Rappel : Cette statistique correspond au pourcentage des instances positives correctement identifiées. Le rappel est défini comme suit :

$$Rappel = \frac{VP}{VP+FN}. \tag{4.3}$$

  Où VP sont les vrai-positifs et FN sont les faux-négatifs.

- La courbe ROC (en anglais *receiver operating characteristic*): Il s'agit d'une courbe où on trace le taux de vrais positifs en fonction du taux de faux positifs pour différents seuils de classification. Le taux de vrais positifs (dit TVP) est équivalent au rappel et le taux de faux positifs (dit TFP) est défini comme suit :

$$TFP = \frac{FP}{FP+VN}. \quad (4.4)$$

Où FP sont les faux-positifs et VN sont les vrai-négatifs.

- L'AUC (en anglais *area under the ROC Curve*) : L'AUC fournit une mesure de performance pour tous les seuils de classification possibles. Les valeurs d'AUC sont comprises entre 0 et 1. Si toutes les prédictions sont correctes, l'AUC est de 1; par contre, si toutes les prédictions sont erronées, alors l'algorithme aura un AUC de 0.

4.4 Résultats de simulation

L'expérimentation de test est réalisée sur Google Colab (Carneiro *et al.*, 2018). Cet environnement interactif nous permet de programmer en Python et d'exécuter nos algorithmes sur les serveurs cloud de Google, y compris les GPU et les TPU, quelle que soit la puissance de notre ordinateur. Ainsi, Google Colab nous permet d'importer l'ensemble de données d'image, former et évaluer l'algorithme en utilisant les critères d'évaluation décrits ci-dessus. Par la suite, nous montrerons et discuterons les résultats obtenus sur Google Colab pour l'approche proposée.

4.4.1 Résultats et analyse du SVDD pour la détection des interférences RF

Les images d'entrée sont d'abord normalisées comme décrit dans la section 4.2. Afin de tester l'efficacité du SVDD, la précision est obtenue pour les différentes types d'interférences RF pendant la phase de test. L'évaluation de performance du SVDD est présentée dans le tableau 4.1. Nous pouvons remarquer que les interférences RF de type CWI et MCWI ont des valeurs de précision inférieurs à celles de type CI en utilisant la mise à l'échelle des caractéristiques sur une plage comme méthode de normalisation. Cela est dû au fait que ces interférences RF présentent des caractéristiques similaires aux données normales (signaux d'entrée) tel qu'indiqué par la figure 4.2. Par conséquent, ces données RFI sont plus proches de la frontière de l'hypersphère, et certaines d'entre elles sont considérées comme des données normales. Les figures 4.3, 4.4 et 4.5 illustrent ce problème.

Tableau 4.1 Résultats du SVDD

	Formation		Test: Nouvelles données normales		Test: CI		Test: CWI		Test: MCWI		Test: CI, CWI et MCWI	
Méthode de normalisation	Précision (%)	Temps de calcul (s)	Précision (%)	Temps de calcul (s)	Précision (%)	Temps de calcul (s)	Précision (%)	Temps de calcul (s)	Précision (%)	Temps de calcul (s)	Précision (%)	Temps de calcul (s)
Mise à l'échelle des caractéristiques sur une plage	94,25	3,815	94,583	0,7891	100	0,4025	95	0,4178	80	0,3915	90,74	0,3397
Normalisation standard	94,25	3,906	94,58	0,7902	100	0,4055	100	0,4001	100	0,4019	100	0,3757

Le tableau 4.1 montre qu'une solution à ce problème consiste à utiliser la normalisation standard comme méthode de normalisation, ce qui produit des valeurs de précision plus élevées, mais présente en même temps une plus grande complexité de calcul par rapport à la mise à l'échelle des caractéristiques sur une plage. Ces résultats montrent l'efficacité et l'efficience de l'algorithme SVDD pour détecter tous les types d'interférences RF.

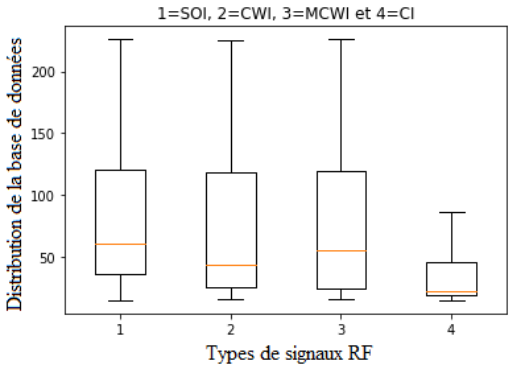

Figure 4.2 Le box-plot du signal d'intérêt et des interférences RF

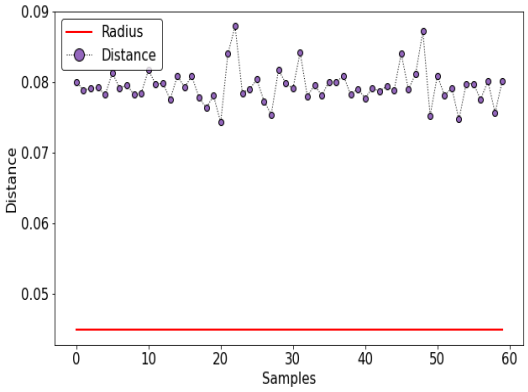

Figure 4.3 Distance entre les données de type CI et l'hypersphère du SVDD en utilisant la mise à l'échelle des caractéristiques sur une plage

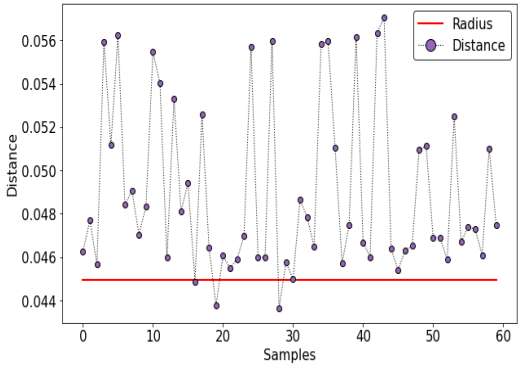

Figure 4.4 Distance entre les données de type CWI et l'hypersphère du SVDD en utilisant la mise à l'échelle des caractéristiques sur une plage

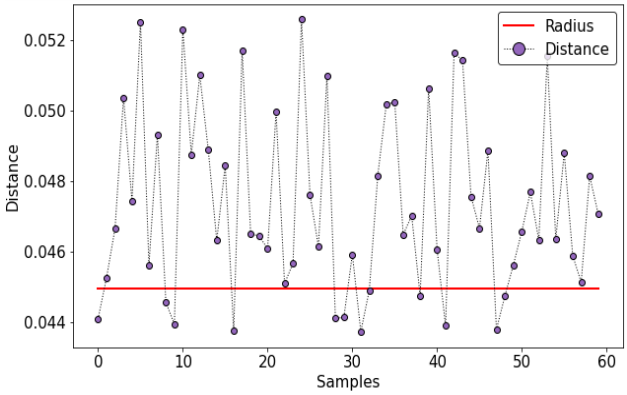

Figure 4.5 Distance entre les données de type MCWI et l'hypersphère du SVDD en utilisant la mise à l'échelle des caractéristiques sur une plage

4.4.2 Résultats et analyse du One-Class SVM pour la détection des interférences RF

L'algorithme One-Class SVM est formé en utilisant la fonction noyau à base radiale, avec un paramètre scalaire γ donné par :

$$\gamma = \frac{1}{N_F}, \tag{4.5}$$

où N_F est le nombre de caractéristiques et le paramètre v est défini dans (3.6) avec une valeur de 0,1.

Les images d'entrée sont d'abord normalisées comme décrit dans la section 4.2. Afin de tester l'efficacité du One-Class SVM, la précision est obtenue pour les différents types d'interférences RF pendant la phase de test. Les performances du One-Class SVM sont résumées dans le tableau 4.2. Comme pour les résultats du SVDD, les interférences RF de type CWI et MCWI ont des valeurs de précision inférieurs à celles de type CI en utilisant la mise à l'échelle des caractéristiques sur une plage comme méthode de normalisation. Une fois de plus, les données RFI liées aux interférences CWI et MCWI présentent des caractéristiques plus similaires aux données normales (SOI), ce qui diminue la distance entre ces données et la frontière définie par la fonction noyau à base radiale. Cette diminution de la distance fait que certaines de ces données RFI seront considérées comme des données normales.

Le tableau 4.2 montre qu'une solution à ce problème consiste à utiliser la normalisation standard et la normalisation robuste comme méthodes de normalisation, ce qui produit des valeurs de précision plus élevées dans la détection des interférences RF. Nous remarquons que la précision pendant la phase de formation et pendant la phase de test en utilisant de nouvelles données normales est toujours inférieure à celle du SVDD.

Les tableaux 4.1 et 4.2 montrent que l'algorithme SVDD a une plus grande précision dans la détection des interférences RF que le One-Class SVM, tant pendant la phase de formation que pendant la phase de test, en utilisant de nouvelles données normales. Dans le cas, où nous utilisons la mise à l'échelle des caractéristiques sur une plage comme méthode de normalisation, l'algorithme SVDD obtient également une meilleure précision avec les nouvelles données anormales (CI, CWI et MCWI).

Tableau 4.2 Résultats du One-Class SVM

	Formation		Test: Nouvelles données normales		Test: CI		Test: CWI		Test: MCWI		Test: CI, CWI et MCWI	
Méthode de normalisation	Précision (%)	Temps de calcul (s)	Précision (%)	Temps de calcul (s)	Précision (%)	Temps de calcul (s)	Précision (%)	Temps de calcul (s)	Précision (%)	Temps de calcul (s)	Précision (%)	Temps de calcul (s)
Mise à l'échelle des caractéristiques sur une plage	89,48	12,485	86,67	5,43	100	1,337	53,33	1,395	43,33	1,735	91,67	1,134
Normalisation robuste	90	11,184	87,5	3,815	100	0,938	100	0,917	100	0,992	100	1,05

CONCLUSION

La détection des interférences RF est un enjeu essentiel de nos jours afin que les systèmes de communications sans fils fonctionnent correctement, c-à-d, sans une détérioration de leur performance. Il est donc essentiel de trouve une approche capable de détecter ces interférences RF tout en évitant les limitations vues aux chapitres 1 et 2. Pour cette raison, nous avons comparé deux algorithmes de détection d'anomalies qui utilisent une petite base de données pendant la phase de formation. Les deux algorithmes considérés sont des approches d'apprentissage non supervisés. Nous les avons comparés expérimentalement dans le cadre d'une tâche de détection d'interférence RF en utilisant trois types de signaux d'interférence, à savoir CI, CWI et MCWI. Nous avons commencé par une description des deux algorithmes, puis de notre méthodologie. Dans les expériences réalisées, nous avons évalué la capacité du SVDD et du One-Class SVM à détecter les signaux d'interférence anormaux. Pour faire la comparaison entre les deux algorithmes, nous avons utilisé la métrique de précision. Les résultats prouvent que l'utilisation d'une méthode de normalisation, telle que la mise à l'échelle des caractéristiques sur une plage ou la normalisation robuste, produit une plus grande précision dans la détection des interférences RF. En outre, il est important de noter que SVDD performe mieux que le One-Class SVM.

Pour les travaux futurs, nous nous concentrerons sur l'étude des étapes de prétraitement des données. Ces étapes doivent se dérouler juste avant la détection des interférences RF afin d'augmenter la précision pendant la phase de formation et pendant la phase de test en utilisant de nouvelles données normales.

RÉFÉRENCES

Akansu, A. N. et Haddad, R. A. (2001). Multiresolution Signal Decomposition: Transforms, Subbands, and Wavelets. Academic Press.

Aberkane, S. et Elarbi, M. (2019). Deep Reinforcement Learning for Real-world Anomaly Detection in Surveillance Videos. International Conference on Image and Signal Processing and their Applications (ISPA), 1(1), 1-5. doi: 10.1109 / ISPA48434.2019.8966795

Akeret, J., Chang, C., Lucchi, A. et Refregier, A. (2017). Radio frequency interference mitigation using deep convolutional neural networks. Astronomy and Computing, 1(1), 1-8.

Akcay, S., Abarghouei, A. A. et Breckon, T. P. (2018). GANomaly: Semi-Supervised Anomaly Detection via Adversarial Training. ACCV 2018, 1(1), 1-16.

Alipour-Fard, T. et Arefi, H. (2020). Structure Aware Generative Adversarial Networks for Hyperspectral Image Classification. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 13(1), 5398-5412.

Aref, M. A., et Jayaweera, S. K. (2019). Robust Deep Reinforcement Learning for Interference Avoidance in Wideband Spectrum. IEEE Cognitive Communications for Aerospace Applications Workshop (CCAAW), 1(1), 1-5.

AVIO-601 (2018). AVIO-601 project: Interference mitigation in satellite communications. Récupéré de https://lassena.etsmtl.ca/IMG/pdf/-6.pdf.

Borio, D., et Camoriano, L. (2008). Two-Pole and Multi-pole Notch Filters: A Computationally Effective Solution for GNSS Interference Detection and Mitigation. IEEE Systems Journal, 2(1), 38-47.

Banerjee, A., Burlina, P. et Meth, R. (2007). Fast hyperspectral anomaly detection via SVDD. IEEE Int. Conf. on Image Processing, 1(1), 1-4.

Budiarto, E. H., Permanasari, A. E. et Fauziati, S. (2019). Unsupervised anomaly detection using K-means, Local Outlier Factor and One Class SVM. IEEE Int. Conf. Science and Technology, 1(1), 1-5.

Carneiro, T., Da Nóbrega, R. V. M., Nepomuceno, T., Bian, G., De Albuquerque et Filho, P. P. R. (2018). Performance analysis of Google Colaboratory as a tool for accelerating deep learning applications. IEEE Access, 6(1), 61677-61685.

Damer, N., Grebe, J., H., Zienert, S., Kirchbuchner, F., et Kuijper, A. (2019). On the generalization of detecting face morphing attacks as anomalies: novelty vs. outlier detection. IEEE Int. Conf. on Biometrics Theory, Applications and Systems, 1(1), 1-5.

Denton, E., Chintala, S., Szlam, A. et Fergus, R. (2015). Deep Generative Image Models using a Laplacian Pyramid of Adversial Networks. Cornell University, 1(1), 1-10.

Di Mattia, F., Galeone, P., De Simoni, M., et Ghelfi, E. (2019). A Survey on GANs for Anomaly Detection. Cornell University, 1(1), 1-16.

Ding, N., Gao, H., Bu, H. et Ma, H. (2018). RADM: Real-time anomaly detection in multivariate time series based on bayesian network. IEEE Int. Conf. on Smart Internet of Things, 1(1), 1-6.

Donahue, J., Krähendühl, P. et Darrel, T. (2017). Adversarial Feature Learning. Conference paper at ICLR 2017, 1(1), 1-18.

Dong, S. et Zhang, B. (2019). SVDD-based network traffic anomaly detection method with high robustness. IEEE Int. Conf. on Computer and Communications (ICCC), 1(1), 1-5.

Eltanbouly, S., Bashendy, M., AlNaimi, N., Chkirbene, Z. et Erbad, A. (2020). Machine learning techniques for network anomaly detection: A survey. IEEE Int. Conf. on Informatics, IoT, and Enabling Technologies (ICIoT), 1(1), 1-7.

Forte, G. F. (2014). Contributions to Radio Frequency Interference Detection and Mitigation in Earth Observation. (Thèse de doctorat, Universitat Politècnica de Catalunya, Barcelona, Espagne).

Ghanney, Y. (2019). L'apprentissage Profond pour la Détection des Signaux D'interférences Radio Fréquentiels. (Mémoire, Université du Québec à Montréal, Canada).

Ghanney, Y. et Ajib, W. (2020). Radio Frequency Interference Detection using Deep Learning. IEEE, 1(1), 1-5.

Getu, T. M. (2019). Advanced RFI Detection, RFI Excision, and Spectrum Sensing: Algorithms and Performance Analyses. (Thèse de doctorat, École de Technologie Supérieure, Montréal, Canada).

Goh, J., Adepu, S., Tan, M. et Lee, Z. S. (2017). Anomaly detection in cyber physical systems using recurrent neural networks. IEEE Int. Symp. High Assurance Systems Engineering, 1(1), 1-6.

Guner, B., Johnson, J. T. et Niamsuwan, N. (2007). Time and Frequency Blanking for Radio Frequency Interference Mitigation in Microwave Radiometry. IEEE Trans. Geosci. Remote Sens., 45(11), 3672-3679. doi: 10.1109/TGRS.2007.903680.

Guo, Z. et Shui, P. (2020). Anomaly based sea-surface small target detection using k-nearest neighbor classification. IEEE Trans. Aerosp. Electron. Syst., 56(6), 4947-4964.

Goodfellow, I. J., Abadie, J. P., Mirza, M., Farley, D. W., Ozair, S., Courville, A. et Bengio, Y. (2014). Generative Adversial Nets. Université de Montréal, 1(1), 1-9.

Goodfellow, I., Bengio, Y. et Courville, A. (2016). Deep Learning. MIT press. Repéré de http://www.deeplearningbook.org

Harrison, K. et Mishra, A. K. (2019). Supervised Neural Networks for RFI Flagging. IEEE Xplorer. 1(1), 1-8. doi: 10.23919/RFI48793.2019.9111748.

Hsu, Y. et Matsuoka, M. (2020). A deep reinforcement learning approach for anomaly network intrusion detection system. IEEE Int. Conf. on Cloud Networking, 1(1), 1-6.

Inoue, J., Yamagata, Y., Chen, Y., Poskitt, C. M. et Sun, J. (2017). Anomaly detection for a water treatment system using unsupervised machine learning. IEEE Int. Conf. on Data Mining Workshops, 1(1), 1-8.

Kay, S. M. (1998). Fundamentals of Statistical Signal Processing: Detection Theory, Vol. II. Prentice-Hall, Englewood Cliffs, NJ.

Kandangath, A. (2003). Jamming Mitigation Techniques for Spread Spectrum Communication Systems. Signal Processing for Wireless Communications. 1-13.

Kanagawa, Y. et Kaneko, T. (2019). Rogue-Gym: A New Challenge for Generalization in Reinforcement Learning. IEEE Conference on Games (CoG), 1(1), 1-8. doi: 10.1109/CIG.2019.8848075

Kim, J., Cha, S., Ryu, M. et Jo, M. (2019). Pre-training Framework for Improving Learning Speed of Reinforcement Learning Based Autonomous Vehicles. International Conference on Electronics, Information, and Communication (ICEIC), 1(1), 1-2. doi: 10.23919/ELINFOCOM.2019.8706441

Lei, Y. (2017). Network anomaly traffic detection algorithm based on SVM. IEEE Int. Conf. on Robots & Intelligent System, 1(1), 1-4.

Leshem, A., Van Der Veen, A. J. et Boonstra, A. J. (2000). Multichannel interference mitigation techniques in radio astronomy. Astrophysical Journal Supplements, 131(1), 355-374.

Lyu, Y., Han, Z., Zhong, J., Li, C. et Liu, Z. (2020). A Generic Anomaly Detection of Catenary Support Components Based on Generative Adversarial Networks. IEEE Transactions on instrumentation and measurement, 69(5), 2439-2448.

Li, Y., Hu, X., Zhuang, Y., Gao, Z., Zhang, P. et EI-Sheimy, N. (2019). Deep Reinforcement Learning (DRL): Another Perspective for Unsupervised Wireless Localization. IEEE Internet of Things Journal, 7(7), 6279-6287. doi: 10.1109/JIOT.2019.2957778

Li, F., Shao, W., Zhou, Q. et Zhao, J. (2020). Interference Avoidance Scheme Based on Reinforcement Learning. IEEE 3rd International Conference on Information Systems and Comuter Aided Education (ICISCAE), 1(1), 1-4.

Li, H. (2010). Research and implementation of an anomaly detection model based on clustering analysis. IEEE Int. Symp. Intelligence Information Processing and Trusted Computing, 1(1), 1-5.

Li, Y., Zhuang, Y., Hu, X., Gao, Z., Hu, J., Chen, L., He, Z., Pei, L., Chen, K., Wang, M., Niu, X., Chen, R., Thompson, J., Ghannouchi, F. et EI-Sheimy, N. (2021). Toward Location-Enabled IoT (LE-IoT): IoT Positioning Techniques, Error Sources, and Error Mitigation. IEEE Internet of Things Journal, 8(6), 4035-4062.

Lukashevich, H., Nowak, S. et Dunker P. (2009). Using One-Class SVM outliers detection for verification of collaboratively tagged image training sets. IEEE Int. Conf. Multimedia Expo, 1(1), 682-685.

Ma, W. (2020). SMOTE-based Category Imbalance for Radar Radiation Source Sorting and Identification. IEEE International Conference on Information Technology Big Data and Artificial Intelligence (ICIBA), 1(1), 1-8. doi: 10.1109/ICIBA50161.2020.9277341

Ma, X. et Shi, W. (2020). AESMOTE : Adversarial reinforcement learning with SMOTE for anomaly detection. IEEE Trans. on Network Science and Engineering, 1(1), 1-1.

Matinmikko-Blue, M., Yrjölä, S. et Ahokangas, P. (2020). Spectrum management in the 6G era: The role of regulation and spectrum sharing. IEEE 2nd 6G Wireless Summit, 1(1), 1-5.

Misra, S. et Ruf, C. S. (2011). Analysis of Radio Frequency Interference Detection Algorithms in the Angular Domain for SMOS. IEEE Trans. Geosci. Remote Sens., 49(12), 1-10.

Portela, F. G., Mendoza, F. A. et Benavides L. C. (2019). Evaluation of the performance of supervised and unsupervised machine learning techniques for intrusion detection. IEEE Int. Conf. on Applied Science and Advanced Technol. (iCASAT), 1(1), 1-8.

Roo, R. D., Misra, S. et Ruf, C. S. (2007). Sensitivity of the Kurtosis Statistic as a Detector of Pulsed Sinusoidal RFI. IEEE Trans. Geosci. Remote Sens., 45(7), 1938-1946.

Radford, A. et Metz, L. (2016). Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks. ICLR 2016, 1(1), 1-16.

Sahu, S. et Mehtre, B. M. (2015). Network intrusion detection system using J48 Decision Tree. IEEE Int. Conf. on Advances in Computing, Commun. and Informatics, 1(1), 1-4.

Schlegl, T., Seebock, P., Waldstein, S. M., Erfurth, U. S. et Langs, G. (2017). Unsupervised Anomaly Detection with Generative Adversarial Networks to Guide Marker Discovery. Proceedings of IPMI, 1(1), 1-12.

Schölkopf, B., Platt, J. C., Taylor, J. S., Smola, A. J. et Williamson, R. C. (2001). Estimating the support of a high-dimensional distribution. MIT Press, 13(7), 1443-1471.

Simeone, O. (2018). A Very Brief Introduction to Machine Learning With Applications to Communication Systems. IEEE Transactions on Cognitive Communications and Networking, 4(4), 648-664. doi: 10.1109/TCCN.2018.2881442

Sutton, R. S. et Barto, A. G. (2015). Reinforcement Learning: An Introduction. The MIT press Cambridge, Massachusetts London, England.

Suwannalai, E. et Polprasert C. (2020). Network intrusion detection systems using adversarial reinforcement learning with deep Q-network. IEEE Int. Conf. on ICT and knowledge Engineering , 1(1), 1-7.

Tarongi, J. M. et Camps, A. (2009). Normality análisis for RFI detection in microwave radiometry. Remote Sens., 2(1), 191-210.

Taneja, S., Gupta, C., Goyal, K. et Gureja, D. (2014). An Enhanced K-Nearest Neighbor Algorithm Using Information Gain and Clustering. Fourth International Conference on Advanced Computing & Communication Technologies, 1(1), 1-5. doi: 10.1109/ACCT.2014.22

Tax, D. M. J. et Duin, R. P. W. (2004). Support vector data description. Machine Learning, 54(1), 45-66.

Ujan, S., Navidi, N. et Landry, R. (2020). Hierarchical Classification Method for Radio Frequency Interference Recognition and Characterization in Satcom. MDPI, 1(1), 1-18.

Vinsen, K., Foster, S. et Dodson, R. (2019). Using Machine Learning for the detection of Radio Frequency Interference. Asia-Pacific Radio Science Conference, 1(1), 1-4. doi: 10.23919/URSIAP-RASC.2019.8738332.

Wankhede, S., B. (2019). Anomaly Detection using Machine Learning Techniques. 5th International Conference for Convergence in Technology, 1(1), 1-3.

Wang, J., Yang, Q. et Ren, D. (2009). An intrusion detection algorithm based on Tree technology. IEEE Asia-Pacific Conf. on Information Processing, 2(1), 1-3.

Walton, M., Ayache, M., Straatemeier, L., Gebhardt, D. et Migliori, B. (2017). Unsupervised Anomaly Detection for Digital Radio Frequency Transmissions. IEEE Int. Conf. on Machine Learning and Applications (ICMLA), 1(1), 1-7.

Xiaofeng, Z. et Xiaohong, H. (2017). Research on Intrusion Detection Based on Improved Combination of K-means and Multi-Level SVM. IEEE 17th International Conference on Communication Technology (ICCT), 1(1), 1-4.

Xu, D. et Tian, Y. (2015). A Comprehensive Survey of Clustering Algorithms. Annals of Data Science 2, 2(2), 165-193. doi: 10.1007/s40745-015-0040-1

Yeo, I. K. et Johnson, R. A. (2000). A new family of power transformation to improve normality or symmetry. Biometrika, 87(4), 954-959.

Zhang, K., Kang, X. et Li, S. (2019). Isolation Forest for Anomaly Detection in Hyperspectral Images. IEEE International Geoscience and Remote Sensing Symposium, 1(1), 1-4.

Zhang, Z. et Zhao, T. (2017). A Method to Detect and Mitigate Radio Frequency Interference of Aquarius Data. IEEE Int. Geoscience and Remote Sensing Symposium (IGARSS), 1(1), 1-3.

Zhong, S., Fu, S., Lin, L., Fu, X., Cui, Z. et Wang, R. (2019). A novel unsupervised anomaly detection for gas turbine using Isolation Forest. IEEE Int. Conf. on Prognostics and health management, 1(1), 1-6.

Zenati, H., Foo, C. S., Lecouat, B., Manek, G. et Chandrasekhar, V. R. (2018). Efficient GAN-Based Anomaly detection. ICDM 2018, 1(1), 1-13.