UNIVERSITE DE SAAD DAHLEB DE BLIDA 1

Faculté de Technologie

Département d'Électronique

THESE DE DOCTORAT

en Électronique

DETECTION RAPIDE ET LARGE-BANDE DE BROUILLEURS AU NIVEAU DE LA RADIO COGNITIVE

Par

Ahmed MOUMENA

Devant le jury composé de :

A.AISSAT	Professeur, U. de Blida 1	Président
A.AMROUCHE	Professeur, U.S.T.H.B., Alger	Examinateur
M.BENSEBTI	Professeur, U. de Blida 1	Examinateur
M.TRABELSI	Professeur, E.N.P, Alger	Examinateur
M.OULD ZMIRLI	Maître de conférences, U.de Médéa	Examinateur
A.GUESSOUM	Professeur, U. de Blida 1	Directeur de thèse

Blida, le 03 Avril 2016

DEDICACE

A LA MÉMOIRE DE MA CHERE MERE,

A MON CHER PÈRE,

A MES CHERS FRERES, SŒURS.

A TOUTE LA FAMILLE MOUMENA.

A TOUS MES AMIS.

RÉSUMÉ

La communication sans fil est fondamentalement sensible aux attaques de brouilleurs en raison de la nature des systèmes de communication sans fil. Typiquement, les attaquants peuvent être classés comme passif ou actif dans la guerre électronique des communications. Dans le premier, les attaquants visent à perturber la liaison de communication entre l'émetteur et le récepteur, ce qui pose une menace à la sécurité de la communication sans fil. Les brouilleurs actifs, à l'inverse, tentent de dégrader la qualité de la liaison de communication sur les canaux actifs en créant des signaux de brouillage. Dans ce travail, nous souhaitons développer des systèmes de détection intelligents des effets de brouillage dans le spectre d'une façon rapide dans un régime large-bande via une collaboration centralisée d'utilisateurs radios.

Ce travail présente un nouveau schéma coopératif centralisé dans un régime large-bande pour la détection d'anomalies due à l'effet Bruit Blanc Gaussien Additif (BBGA) et la présence des signaux de brouillage d'attaque qui combine la technique d'échantillonnage compressif (EC) avec des détecteurs intelligents via une collaboration centralisée. Le signal reçu par chaque récepteur radio cognitive en présence des signaux de brouillage d'attaque, et du BBGA est passé par un Convertisseur Analogique-Information (CAI) via un Démodulateur Aléatoire (DA) pour avoir le taux d'échantillonnage de sous-Nyquist. L'approche proposée consiste en la détection d'anomalies en utilisant des techniques intelligentes de détection appliquées aux mesures compressées obtenues à partir de chaque utilisateur radio, collectées sous forme d'une matrice appelée matrice d'observations. La coopération large-bande entre les utilisateurs de radio cognitive aide à détecter des anomalies/des attaques en présence du BBGA et des signaux de brouillage intentionnel. En outre, comme solution importante, la coopération entre tous les utilisateurs de radio aide à compresser au maximum le nombre d'échantillons/mesures dans chaque récepteur radio, c'est-à-dire, toutes les radios donnent un nombre minimum d'échantillons noté par $\mathbb{K}$. Des hypothèses sont proposées dans cette thèse de recherche pour savoir s'il y a un problème d'anomalies en utilisant des techniques de détection intelligentes de type

graphique-statistique, clustering, et classification. Les résultats obtenus montrent que ces techniques intelligentes de détection coopérative proposées dans ce mémoire de thèse fonctionnent bien en plus de sa faible complexité. Finalement, la thèse propose un cadre de détecteurs intelligents combiner avec l'échantillonnage compressif via une collaboration centralisée pour détecter rapidement est dans un régime large-bande l'effet de brouillage dans le spectre.

ABSTRACT

Wireless communication is fundamentally susceptible to jammer attacks due to the nature of the wireless communication systems. Typically, attackers may be categorized as either passive or active in Electronic Warfare communications. In the former, attackers aim to disrupt the communication link between transmitter and receiver, thus posing threat to wireless communication security. Active jammers, conversely, try to degrade quality of the communication link on the active channels by creating jamming signals. In this work we would like to develop intelligent detection systems of the jamming effects in the spectrum quickly and wideband via centralized collaborative radios users.

This work presents a new wideband centralized cooperative schemes for anomalies detection which combines the compressive sampling (EC.) technique via collaboration with intelligent detectors based on the decision.The received signal by each cognitive radio (CR) user receiver in the presence of the jamming attack signals, and the Additive White Gaussian Noise (AWGN) passed by an Analog-Information Converter (AIC) via a Random Demodulator (RD) to have the minimum sampling rate based on the sub-Nyquist criterion.The approach proposed consists of the anomalies detection due to the presence of jamming attack signals and AWGN corrupted with primary signal by using intelligent detectors based on the threshold value if there is a problem of anomalies in wireless system. The compressed measurements obtained from each radio user receiver, collected in the form of a matrix called observations matrix.The wideband cooperation between all CR users helps to detect anomalies/attacks in the presence of AWGN and jamming attack signals corrupted with sparse signal in wireless communication systems.Moreover, as significant solution, the cooperation between all the radio users help to compress to the maximum number of observations in each radio user receiver, i.e., all the radios give a minimum number of samples noted by $\mathbb{K}$.Hypotheses are proposed in this work to know if there is a problem of jamming attack effects by using intelligent detectors of type graphic-statistic, clustering, and classification.The results obtained show that these intelligent detectors combined with compressive sampling via collaboration

proposed in this thesis work well in addition to its low complexity.Finally, this original work proposes a framework of intelligent detectors combined with compressive sampling via centralized collaboration to detect quickly and wideband the presence of the effects of jamming attacks in the spectrum.

REMERCIEMENTS

Ce manuscrit conclut nos travaux sur un original projet de recherche, c'est pour cela que je tiens en ces quelques lignes à exprimer ma reconnaissance envers tous ce qui de près ou de loin y ont contribué.

Je tiens à adresser en premier lieu mes plus vifs remerciements à mon directeur de thèse Monsieur Abdelrezzak GUESSOUM, Professeur des universités à l'Université Saad Dahlab-Blida pour la confiance qu'il m'a accordée tout le long de mes travaux de recherche. Et pour m'avoir confié le sujet de cette thèse qu'il a dirigé avec intérêt.

Je remercie Monsieur Abdelkader AISSAT, Professeur à l'Université de Blida (USDB), pour l'honneur qu'il m'a fait en acceptant de présider ce jury.

Je remercie également Monsieur Abdelrahmane AMROUCHE, Professeur à l'Université de Houari Boumediene (USTHB), ainsi que Monsieur Messaoud BENSEBTI, Professeur à l'Université de Blida (USDB) de m'avoir fait l'honneur de bien vouloir participer au jury de cette thèse.

Mes sincères remerciements vont aussi à Monsieur Mohamed TRABELSI, Professeur à l'Ecole National Polytechnique d'Alger (ENP) et Monsieur Mohamed OULD ZMIRLI, Maître de Conférences classe A à l'Université de Médéa de m'avoir fait l'honneur de bien vouloir participer au jury de cette thèse.

Je dédie ce manuscrit à mes parents ainsi qu'à tous les membres de ma famille et à mes amis que je tiens à remercier pour le soutien moral et les nombreux encouragements durant les moments difficiles.

A vous tous, merci.

TABLE DES MATIERES

LISTE DES FIGURES ET DES TABLEAUX

LISTE DES ABREVIATIONS ET DES SYMBOLES

LISTE DES ABREVIATIONS

ACP : Analyse de Composantes Principales.

ADS : Accès dynamique au spectre.

AUCs : Ensemble de l'Aire Sous la Courbe.

AUC : Aire Sous la Courbe.

CAN : Convertisseur Analogique-Numérique.

CAIs : Convertisseurs Analogique-Information.

CAI : Convertisseur Analogique-Information.

CCC : Brouillage sur les canaux de contrôle (control channel jamming)

CF : Centre de fusion.

CoSaMP : Iterative Signal Recovery from Incomplete and Inaccurate Samples.

COR : Caractéristique Opérationnelle de Réception.

CCCOR : Coque convexe de la courbe COR.

CME : Contre-Mesures Électroniques.

CW : Onde Continue (Continue-Wave).

DA : Démodulateur aléatoire.

DARPA : Agence pour les projets de recherche avancée de défense.

DBSCAN : Basé sur la densité, le regroupement spatial des applications avec bruits.

DC : Détecteur cyclo-stationnaire.

DE : Détecteur d’énergie.

DoS : Déni de service (Denial of service).

EA : Électronique d’attaque.

ECS : Écoute Coopérative du Spectre.

EC : Échantillonnage Compressif/ Écoute Compressive.

ECLC : Ecoute coopérative large-bande centralisée.

ECLD : Ecoute coopérative large-bande distribuée.

EM : Expectation-Maximisation.

EP : Électronique de protection.

ES : Électronique de support.

FCC : Carte d’allocation du spectre.

FM : Modulation de Fréquence.

FPB : Filtre passe-bas.

FNR : Taux de faux négatifs.

FPR : Taux de faux positifs.

FR : Fréquence de répétition.

FP : Faux positifs.

FN : Faux négatifs.

GBP : Greedy Basis Pursuit.

GE : Guerre Électronique.

GNPA : Générateur d’un nombre pseudo-aléatoire.

GSM : Système global pour la communication mobile.

FH : Saut de fréquence (Frequency hopping).

KTH : Institut royal de technologie.

KFD : Kernel Fisher Discriminants.

IA : Intelligence Artificielle.

IHT : Iterative Hard Thresholding.

LP : Programmation Linéaire.

MAC : Contrôle d’accès au medium.

MMC : Modèle de Markov caché.

MVS : Machine à vecteurs de support.

NGN : Réseaux de communication de prochaine génération.

OTAN : Organisation du traité de l'Atlantique nord.

OMP : Orthogonal Matching Pursuit.

PHY : Physique.

QoS : Qualité de service (Quality of Service).

QPSK : Quadrature Phase-Shift Keying.

Q-Q : Quantile-Quantile.

RC : Radio Cognitive.

RPA : Reconnaissance de patrons d’anomalies.

ROMP : Regularized Orthogonal Matching Pursuit.

RF : Radio fréquence.

RX : Récepteur.

SDR : Radio logiciel (software defined radio).

SNR : Rapport signal sur bruit.

SJNR : Rapport signal sur bruit plus brouillage.

SJ1R : Rapport signal sur le premier signal de brouillage.

SJ2R : Rapport signal sur le deuxième signal de brouillage.

SP : Subspace Pursuit.

SOM : Carte auto adaptatives.

SNN : Plus Proche Voisins Partagé.

SS : Étalement de spectre (spread spectrum).

TDM : Technique de Distance de Mahalanobis.

TP : Vrais positifs.

TN : Vrais négatifs.

TPR : Taux de vrais positifs.

TNR : Taux de vrais négatifs.

TV : Télévision.

TX : Transmetteur.

UP : Utilisateur Primaire.

UP1 : Premier utilisateur Primaire.

UPs : Utilisateurs primaires.

US : Utilisateur Secondaire.

US1 : Premier utilisateur Secondaire.

USs : Utilisateurs secondaires.

UJ : Utilisateur brouilleur.

UJ1 : Premier utilisateur brouilleur.

UJ2 : Deuxième utilisateur brouilleur.

UHF : Ultra Haute Fréquence.

UJ1 : premier type d’utilisateur brouilleur.

UJ2 : deuxième type d’utilisateur brouilleur.

UEP : Utilisateur Émulateur Primaire.

VUS : Volume Sous l’hyper-surface ROC.

WLAN : Réseau local sans fil.

WRAN : Réseau régional sans fil.

WiFi : Fidélité sans fil.

WiMAX : Interopérabilité mondiale pour un accès par micro-ondes.

LISTE DES SYMBOLES

f_{Nyq} : Fréquence de Nyquist.

f_{max} : Fréquence maximale.

H_0 : Hypothèse signifie l'absence de brouilleurs.

H_1 : Hypothèse signifie la présence de brouilleurs.

H_{00} : Hypothèse signifie une observation normale.

H_{11} : Hypothèse signifie une observation anomalie.

r : Signal reçu au niveau de chaque récepteur radio cognitive.

$\tilde{r}$: Signal reconstruit.

j : Indice du nombre d'échantillons compressés.

i : Indice du nombre de points du signal source.

ℓ : Indice de récepteur radio cognitive.

l : Indice des tonalités.

$\mathbb{i}$: Indice d'utilisateur primaire.

$\mathbb{j}$: Indice d'utilisateur brouilleur.

T_s : Période d'échantillonnage.

$T_{\mathbb{j}1}$: Période d'impulsions sinusoïdales de brouillage.

T : Période.

t : Temps.

$\mathcal{P}_{\mathbb{j}1}$: Pulses du signal de brouillage.

f_{j1} : Fréquence de brouillage d'impulsion sinusoïdale.

θ_{j1} : Phase de brouillage d'impulsion sinusoïdale.

τ_{j1} : Rapport cyclique du signal de brouillage d'impulsions sinusoïdales.

$j1_{\mathcal{P}}$: Amplitude du signal d'impulsions sinusoïdales.

$j1$: Signal de brouillage de type d'impulsions sinusoïdales.

$j2$: Signal de brouillage de type onde continue.

f_{j2l} : Fréquences des tonalites

θ_{j2l} : Phases des tonalités.

$\mathcal{b}$: Nombre de tonalités du brouillage a onde continue.

d : Dimension.

AUC_{global} : Aire Sous la Courbe globale.

$r(t)$: Signal source primaire dans le domaine de base.

$v(t)$: Bruit blanc gaussien additif (BBGA).

j_1 : Premier type du signal de brouillage.

j_2 : Deuxième type du signal de brouillage.

R^N : Ensemble réels.

N : Nombre nécessaire de points qui peuvent représenter le signal source dans le domaine de base.

I : Instance.

$\mathbb{Y}$: Etiquettes d'une classe réelle.

$\mathbb{N}$: Etiquettes d'une classe prédite.

ψ_i : Coefficients des colonnes de la matrice de base.

ϕ_{ji} : Coefficients de la matrice d'écoute.

ϕ_j : Coefficients des lignes de la matrice d'écoute.

Θ : Matrice d'échantillonnage.

$\mathbb{K}$: Nombre minimum d'échantillons.

Φ : Matrice d'écoute.

Ψ : Matrice de base.

$p_c(t)$: Séquence de chipping.

y_ℓ : Vecteurs d'observations compressées.

y : Matrice d'observations.

thr : Seuil.

FR : Fréquence de répétition.

$sort(\,)$: Fonction qui permet d'ordonner les valeurs de la distance de Mahalanobis.

Q_j : Probabilités espacés entre 0 et 1

$\mathcal{K}$: Nombre de clusters/groupes.

G_{i} : Groupe de clusters.

c_{i} : Centres de clusters.

FO : Fonction objective.

MD_j : Distance de Mahalanobis.

x_j : Observations compressées.

$\vec{\mu}$: Moyenne.

Σ : Matrice de covariance.

χ_P^2 : Distribution chi-carrée avec P degrés de liberté.

$\chi^2_{\mathfrak{q}}$: Distribution chi-carrée avec $\mathfrak{q}$ degrés de liberté.

$\mathbb{P}_i$: Classes positives.

α : Niveau de signification.

D : Vecteur de Distances de Mahalanobis.

$\mathrm{Q1}$: Quartile inférieur.

$\mathrm{Q3}$: Quartile supérieur.

$\mathrm{Q3}-\mathrm{Q1}$: Plage-Inter-Quartile.

n_1 : Nombre de bandes de fréquence.

β_1 : Bande-passante de chaque bande de fréquence.

τ_{j_1} : Rapport cyclique du premier type de brouillage d'impulsion sinusoïdale.

$\mathbb{B}$: Ensembles de classes.

ϵ : Erreur.

C^N : Étape de dimension supérieure.

$C^{\mathbb{K}}$: Étape de dimension inferieure.

$\tilde{s}$: Signal source reconstruit.

l_1 : l-un minimisation.

l_2 : l-deux minimisation.

b_i : Classe positive.

b_j : Classe négative.

p : Étiquette de classe positive.

n : Étiquette de classe négative.

$\mathbb{N}_i$: Ensemble de classes négatives.

m : Nombre de classes.

$r_\ell(t)$: Signal reçu dans chaque récepteur radio.

$h_{\mathbb{i}\ell}$: Canaux radio entre les utilisateurs primaires et les utilisateurs secondaires.

$h'_{\mathbb{j}\ell}$: Canaux radio entre les utilisateurs brouilleurs et les utilisateurs secondaires.

$s_{\mathbb{i}\ell}(t)$: Signal source pour chaque utilisateur primaire.

$\jmath_{\mathbb{j}\ell}$: Signal de brouillage pour chaque utilisateur brouilleur.

$R^{\mathbb{K}}$: Ensemble d'observations compressées réels.

$\mathcal{A}$: Nombre d'utilisateurs primaires.

$\mathcal{B}$: Nombre de brouilleurs.

λ_i : Valeurs propres.

$\lambda_{\mathfrak{p}}$: $\mathfrak{p}$ Valeurs propres.

$\lambda_{\mathfrak{q}}$: $\mathfrak{q}$ Valeurs propres.

y_i : Composantes principales.

$y_{\mathfrak{p}}$: $\mathfrak{p}$ Composantes principales.

$y_{\mathfrak{q}}$: $\mathfrak{q}$ Composantes principales.

$\mathcal{G}$: Nombre d'impulsions.

$\mathbb{K}$: Nombre minimum d'observations.

P : Nombre de radios/utilisateurs secondaires.

INTRODUCTION

Le spectre radio fréquence (RF) est une ressource précieuse, mais strictement réglementée en raison de son rôle unique et important dans les communications sans fil. Avec la prolifération des services sans fil, les demandes de spectre RF sont en constante augmentation, ce qui conduit à des ressources de spectre rares. Actuellement, de nouvelles politiques de spectre sont en cours d'élaboration par la Federal Communications Commission (FCC) [1] qui a montré que certaines bandes de fréquences ne sont que partiellement occupées dans des emplacements particuliers et à des moments particuliers. Et c'est pour toutes ces raisons que la Radio Cognitive (RC) est apparue. La RC [2], [3] est devenue une solution prometteuse pour résoudre le problème de la rareté du spectre dans les réseaux cellulaires de prochaine génération, en exploitant les opportunités dans le domaine temporel, fréquentiel, et spatial.

La RC est une forme de communication sans fil dans laquelle un émetteur-récepteur est capable de détecter intelligemment les canaux de communication qui sont en cours d'utilisation et ceux qui ne le sont pas, et peut se déplacer vers les canaux inutilisés. Ceci permet d'optimiser l'utilisation des fréquences radio disponibles du spectre tout en minimisant les interférences avec d'autres utilisateurs.

Le principe de la RC nécessite une gestion alternative du spectre qui est: un utilisateur secondaire (US) pourra, à tout moment, accéder à des bandes de fréquence qu'il trouve libres, c'est-à-dire, non occupées par l'utilisateur primaire (UP) possédant une licence sur cette bande.

La RC est une radio logicielle qui détecte automatiquement ses stimuli RF environnante et adapte intelligemment ses paramètres de fonctionnement au réseau d'infrastructure, tout en répondant aux demandes des utilisateurs. Depuis, les radios cognitives (RCs) sont considérées comme des utilisateurs secondaires (USs) pour l'utilisation du spectre licencié, une exigence cruciale des réseaux de RC, est qu'ils doivent exploiter efficacement le spectre sous-utilisé sans causer d'interférence intentionnelle aux utilisateurs primaires (UPs). En outre, les UPs n'ont aucune obligation de partager et de modifier leurs paramètres de fonctionnement pour le partage du spectre avec les réseaux de RC. Ainsi, les RCs

devraient être en mesure de détecter indépendamment les opportunités spectrales sans l'aide des UPs; cette capacité est appelée détection du spectre, qui est considéré comme l'une des composants les plus critiques dans les réseaux de RC.

La RC offre de nouvelles possibilités d'améliorer les performances d'un système de communication tactique moderne en introduisant des méthodes et des mécanismes pour éviter les interférences intentionnelles, améliorer l'efficacité spectrale de l'ensemble du système, et permettre une utilisation plus souple des ressources.

Dans le domaine de l'industrie, des activités de recherche ont été menées pour étudier l'applicabilité de la RC pour les communications militaires. A titre d'exemple, DARPA (Defense Advanced Research Projects Agency) a lancé plusieurs programmes, liés à la RC aux États-Unis. DARPA programme des systèmes de nouvelle génération (NGN) qui visent à développer des solutions théoriques pour le contrôle dynamique du spectre, et des sous-systèmes qui permettent la redistribution du spectre pour démontrer l'applicabilité des futurs systèmes radio militaires [4].

Beaucoup d'algorithmes d'écoute du spectre à bande-étroite ont été étudiés dans la littérature [5], y compris le filtrage Matched, la détection d'énergie [6], et la détection cyclo-stationnaire. Bien que les algorithmes d'écoute du spectre à bande-étroite avaient été axées sur l'exploitation des opportunités spectrales sur une étroite gamme de fréquences, les réseaux de radiocommunication cognitifs seront éventuellement nécessaires pour exploiter les opportunités spectrales sur une large gamme de fréquences estimées par centaines de Méga-Hertz (MHz) à plusieurs Giga-Hertz (GHz) pour atteindre un débit très élevé. Par conséquent, par rapport à la technique d'écoute du spectre à bande-étroite, la technique d'écoute du spectre à large-bande vise à trouver plus d'opportunités spectrales sur une large gamme de fréquences et obtenir un débit très élevé dans les réseaux de RC. Cependant, les techniques d'écoute du spectre large-bande basées sur le convertisseur Analogique-Numérique (CAN) standard, pourraient conduire à un taux d'échantillonnage très élevé ou à une complexité d'implémentation; Ainsi, les nouvelles techniques d'écoute du spectre large-bande deviennent de plus en plus importantes.

Les dernières guerres électroniques ont mis, en évidence, le besoin des radios tactiques pour la détection de l'effet des brouilleurs. La vie des soldats et le bon déroulement des opérations sont tributaires de la capacité des divers intervenants à communiquer en tout temps et sans perturbation. Pouvoir distinguer la présence de brouilleur est donc d'une importance capitale afin de réagir le plus rapidement possible et de maintenir les communications opérationnelles.

Plusieurs techniques d'écoute du spectre des radios fréquences permettent de discriminer entre un signal et le bruit du canal. Par contre, la majorité de ces techniques ne sont pas efficaces ou sont trop complexes pour être pratiquement réalisables. D'autre part, d'autres techniques de reconnaissance de modulation sont loin d'être aussi performantes que les techniques d'écoute. Il existe, par conséquent, un réel besoin d'un algorithme de détection intelligent qui permet de différencier entre un brouilleur et un signal allié dans un régime large-bande.

Problématique de recherche

La Radio Cognitive a été jusqu'ici accordé une attention particulière de la communauté de recherche comme une technologie habilitante pour l'accès opportuniste au spectre. L'objectif de ce travail présenté dans cette thèse, cependant, suit différents lignes: nous étudions les impacts potentiels de la technologie radio cognitive aux communications électroniques du domaine de la guerre électronique. A savoir, les travaux présentés dans cette thèse porte sur les points suivants: comment une radio cognitive peut être utilisée pour concevoir des détecteurs intelligents dite antibrouillages intelligents contre le problème de brouillage d'attaque dans les systèmes de communication sans fil, avec des probabilités plus élevées de succès en observant les tendances et les événements anormaux dans le spectre RF et agir de façon dynamique sur ces observations?.

La sécurité dans un réseau sans fil de RC devient une question difficile, car plus de chances sont données aux brouilleurs par le concept de RC. La solution serait de résoudre ce problème directement dans la couche physique. Le projet se justifie par la nécessité de maintenir des communications sans fil malgré la présence d'interférence intentionnelle ou non. En effet, ces situations sont de plus

en plus fréquentes et interfèrent grandement avec les opérations d'urgence militaire et civile. De façon plus scientifique, plusieurs techniques d'antibrouillage furent développées au cours de ces dernières années. Elles entraînent toutes une perte d'efficacité que ce soit en puissance consommée ou en efficacité spectrale. Pour une détection fiable des moments où un brouilleur est présent, les systèmes de communication sans fils peuvent donc, de façon efficace, utiliser des techniques dite contre-mesures électronique (CME)/antibrouillages basées sur l'intelligence artificiel et la reconnaissance de patrons d'anomalies, qui sont des techniques de défense robustes et efficaces pour la détection de l'effet de brouillage dans le spectre.

La RC utilise la communication sans fil et hérite de toutes les menaces de sécurité associées, il est d'une importance primordiale d'avoir une enquête approfondie sur l'impact des défauts malveillants comme le brouillage d'attaque sur les réseaux de RC sous différents scénarios de défaut. La flexibilité de la RC la rend vulnérable aux menaces de sécurité telles que les attaques de brouillage, l'utilisateur émulateur primaire (UEP) d'attaque, etc. Le brouillage a attiré l'intention des chercheurs pendant longtemps et beaucoup de travaux ont été effectués dans ce secteur. Les travaux, menés à bien dans le secteur de brouillage se sont focalisés sur la détection de brouillage pour minimiser l'effet de brouillage dans un régime large-bande. Le brouillage, peut sévèrement perturber la capacité de communiquer dans un système de communication militaire ou commercial. Le brouilleur peut affecter la communication en attaquant la couche réseau, la couche physique (PHY layer), ou la couche de contrôle d'accès au medium (MAC layer).

La menace majeure est la présence d'un signal de brouillage d'attaque ou plusieurs signaux d'attaques qui peuvent perturber les liens de communication entre un UP et les USs. Le brouillage est une procédure qui vise à perturber la réception du signal désiré par le récepteur prévu. Les concepteurs, dans le domaine militaire ainsi que des systèmes de communication commerciale ont développé, au fil des années, de nombreuses techniques d'antibrouillages pour faire face aux menaces créées par ce problème de brouillage. Parmi ces techniques, il y a par exemple la technique d'étalement du spectre (SS). Mais, l'effet de brouillage sur la performance d'acquisition des récepteurs radios à

étalement du spectre n'a pas encore assez reçu l'attention générale [7]. Parce que les brouilleurs sont devenus plus intelligents et plus sophistiqués, et génèrent des signaux, qui sont difficiles à combattre [8]. Dans ce travail, nous allons proposer de nouvelles techniques d'antibrouillages intelligentes, basées sur l'intelligence artificielle (IA) et la reconnaissance de patrons d'anomalies (RPA), afin de réduire les effets de brouillage d'attaque dans le spectre.

Méthode de recherche

L'écoute coopérative du spectre (ECS) [9]-[10]-[11]-[12]-[13]-[14]-[15] dans les systèmes de RC large-bande fait face à plusieurs difficultés pratiques importantes. Le taux d'échantillonnage très élevé est requis par les méthodes conventionnelles d'estimation spectrale qui doivent fonctionner au niveau ou au-dessus du taux d'échantillonnage de Nyquist [16].

Le théorème d'échantillonnage de Shannon-Nyquist, indique que pour ne pas perdre d'informations lors de l'échantillonnage d'un signal, on doit l'échantillonner à une fréquence supérieure à deux fois sa bande-passante. Dans de nombreux domaines d'application différents, le taux d'échantillonnage de Nyquist, qui en résulte peut être très élevé et que nous nous retrouvons avec un trop grand nombre d'échantillons qui doivent être compressés afin de les stocker ou de les envoyer. Dans d'autres domaines d'application, y compris les systèmes d'imagerie médicale et les convertisseurs analogique-numérique l'augmentation du taux d'échantillonnage au-delà de l'état de l'art courant est très cher [17]-[18].

Récemment, l'Echantillonnage Compressif/l'écoute compressive (EC) ou l'Echantillonnage Sparse (ES), a été largement utilisé et a attiré l'attention de nombreux travaux de recherche au cours de ces dernières années, en raison du fait que l'EC s'est montré prometteur dans le domaine de la science biomédicale, le traitement du signal, les communications, et les statistiques [16]-[17]. L'EC s'appuie sur les travaux de Candes, Romberg et Tao [19]-[20] et Donoho [21], qui ont démontré que si un signal d'utilisateur primaire large-bande a une représentation sparse dans une base donnée alors il peut être reconstruit à partir d'un petit nombre de projections sur une deuxième base utilisant la l1-minimisation ou des algorithmes linéaires de Greedy par exemple: OMP [22], CoSaMP [23], GBP [24], SP [25], ROMP [26], IHT [27], LP [28], et d'autres

méthodes, mais dans le cadre de cette thèse, on n'utilisera pas la technique de récupération du signal désiré, mais ce que nous voulons est d'utiliser une technique de détection avant l'étape de récupération pour gagner du temps au maximum afin d'avoir une détection plus rapide. L'EC dans de nombreux scénarios d'intérêt devient très efficace dans le cas où l'échantillonnage par le taux de Nyquist n'est pas possible ou n'est pas efficace. L'objectif de l'EC est de réduire le nombre d'échantillons au maximum par rapport au nombre d'échantillons en utilisant le taux de Nyquist.

L'EC semble être une solution pour augmenter de manière significative la bande-passante observée à un taux d'échantillonnage limité, puisque la bande passante observée dépasse la limite du taux de Nyquist. La technique d'EC qui traite des signaux large-bande et ultra-large-bande est basée sur le modèle du Convertisseur Analogique-Information (CAI) via un Démodulateur Aléatoire (DA) [29]. L'utilisation de l'EC afin de réduire le nombre d'échantillons implique la minimisation du problème de la complexité du calcul et également pour réduire au minimum la consommation d'énergie de chaque utilisateur RC et de réduire aussi le temps de détection d'anomalies créé par l'effet de brouillage.

Un schéma d'écoute coopérative large-bande centralisé (ECLC) est proposé dans ce mémoire de thèse, le Centre de Fusion (CF) est nécessaire pour collecter toutes les mesures compressées de tous les utilisateurs de radio intelligente sous forme d'une matrice dite matrice d'observations et pour faire la détection d'anomalies par une collaboration centralisée de tous les récepteurs radios à l'aide des détecteurs intelligents avant l'étape de reconstruction du signal sparse. L'écoute coopérative du spectre large-bande centralisée en utilisant des techniques d'EC sont présentées dans [30].

L'utilisation de l'étape de détection est très importante dans le contexte de l'utilisateur RC. Des techniques intelligentes sont considérées dans cette thèse de recherche pour le problème de la détection d'anomalies et dans ce cas, deux hypothèse (H_0, H_1) sont proposées afin de distinguer sur l'absence ou la présence d'une attaque de brouillage sur les systèmes de communications sans fil, et deux autres hypothèses (H_{00}, H_{11}) sont proposées dans ce manuscrit afin de décider si les observations sont normales ou anomalies par les prédicteurs. Sans passer par

l'étape de récupération du signal désiré corrompu par la présence du bruit, et des signaux de brouillage, nous utilisons directement les mesures compressées à des fins de détection en utilisant des détecteurs intelligents qui peuvent contribuer pour réduire la complexité du calcul et la consommation d'énergie par chaque utilisateur RC.

En effet, il est difficile de détecter la présence du signal de brouillage d'attaque en utilisant des méthodes mathématiques, tels que: détecteur d'énergie (DE) [31]-[32], détecteur cyclo-stationnaire (DC) [33], parce que parfois, il existe des signaux qui arrivent à brouiller au-dessous de la valeur du seuil. Les techniques intelligentes deviennent une solution à ce genre de situations, concernant la détection du problème de brouillage d'attaque, basées sur la détection d'anomalies. Il existe de nombreuses techniques d'intelligence artificielle telles que: supervisées, non-supervisées et semi-supervisées expliquées dans de nombreux articles de recherche et des livres [34]-[35]. Parmi les plus efficaces et les plus connues, il existe beaucoup de méthodes de clustering et de classification tels que: clustering $\mathcal{K}$ −moyennes [36], classifieur machines à vecteurs de support (MVS) [37], et classifieur Modèle de Markov Caché (MMC) [38], ainsi que des techniques graphiques et statistiques tels que: Boxplot, test de Grubbs [39],...ect.

La détection d'anomalies uni-variées et multivariées est confrontée à des problèmes pour trouver des observations dans des données multidimensionnelles qui ne se conforment pas à une notion bien définie d'un comportement normal. Ces observations non-conformes sont souvent désignées comme des valeurs aberrantes, des exceptions, des surprises, des aberrations ou des anomalies dans les différents domaines d'application. Les anomalies et les valeurs aberrantes sont deux concepts les plus couramment utilisées dans le cadre de la détection d'anomalies. La détection d'anomalies trouve une utilisation étendue dans une grande variété d'applications telles que: la santé publique, la science de la médecine, et la fraude des cartes de crédit, la détection d'intrusion pour la cyber-sécurité, la surveillance militaire pour les activités de l'ennemi et la détection de défauts dans les systèmes critiques de sécurité [40], la reconnaissance de la parole [41], la détection de nouveauté dans le comportement du robot [42], la surveillance du trafic [43], la détection des défauts dans les applications web [44], la détection d'anomalies dans les données biologiques [45], la détection d'anomalies dans les données du recensement [46], la détection d'anomalies dans

les données astronomiques [47], et la détection des perturbations de l'écosystème [48].

Objectifs

Les objectifs de cette thèse sont résumés comme suit :

- Le premier objectif consiste à concevoir des techniques intelligentes sensibles à la détection d'anomalies due à l'effet de brouillage dans le spectre.
- Et de Combiner la technique d'échantillonnage compressif via une collaboration centralisée avec des détecteurs intelligents avant l'étape de reconstruction du signal sparse.
- Et de réduire la complexité des calculs et la consommation d'énergie par chaque utilisateur radio.
- Puis de proposer deux hypothèses H_0 et H_1 afin de distinguer la présence ou l'absence d'attaque malveillante.
- Et enfin pour assurer la sécurité électronique intelligente au niveau de la couche physique des utilisateurs radios via une collaboration centralisée dans un régime large-bande.

Contributions et retombées prévues

Contributions

Les contributions de cette thèse sont résumées comme suit :

- Sur le plan scientifique c'est une méthode très originale par rapport aux autres techniques qui ont développées aux cours de ces dernières années.
- Sur le plan technologique, notre travail s'applique à la détection rapide et large-bande du problème d'anomalies en présence de l'effet de brouillage dans un système de communication sans fils tactique et d'urgence.
- Sur le plan économique, il y aura un impact économique dans le domaine militaire et civil,

- Notre contribut permet de développer des systèmes de communication sans fils plus efficaces tels que :
    - L'augmentation du nombre d'utilisateurs.
    - Détection très rapide de l'effet de brouillage dans le spectre avant l'étape de récupération du signal sparse dans un régime large - bande et ulra-large-bande.
    - Amélioration d'un système de sécurité et de défense utilisant des détecteurs intelligents plus robuste et plus sensible.

Retombées prévues

Amélioration d'un système anti-brouilleur/système de défense intelligent afin de sécuriser les systèmes de communications sans fils et ainsi de protéger les intervenants lors d'urgence utilisant l'intelligence artificiel, les techniques d'apprentissage automatique, et la reconnaissance de patrons d'anomalies.

Organisation de la thèse

Cette thèse est structurée comme suit:

Le premier chapitre: présent l'état de l'art de la radio cognitive. Le deuxième chapitre : explique les menaces de la sécurité dans les radios cognitives et les réseaux de radio cognitive. Dans le troisième chapitre: on a présenté les stratégies de brouillages dans les radios cognitives. Le quatrième chapitre: explique les stratégies d'antibrouillages ou les contremesures-électroniques. Dans le cinquième chapitre: on a présenté une nouvelle étude de la détection d'anomalies basée sur l'analyse de la courbe ROC utilisant un seul classifieur ou multi-classifieur dans les systèmes de communication sans fil en présence de brouillages d'attaque. Le sixième chapitre: présent les différentes techniques de détection coopérative centralisée dans un régime large-bande. Le septième chapitre: commente les résultats obtenus et leurs discussions. Enfin, dans le dernier chapitre, on présente une conclusion générale et les perspectives pour ce travail de recherche.

CAHPITRE 1
RADIO COGNITIVE : ETAT DE L'ART

La radio cognitive/radio intelligente est une technologie clé qui offre la possibilité d'utiliser le spectre radio fréquence (RF) d'une manière dynamique [49]-[50]. Une exigence cruciale des radios cognitives est qu'elles doivent rapidement combler les trous du spectre sans causer d'interférences nuisibles à l'utilisateur primaire [51]. Cette tâche est accomplie par la fonction de l'écoute du spectre. Cependant, il existe deux difficultés dans l'écoute du spectre. L'une des d'elles est que, en raison de l'effet de la propagation par trajets-multiples et les obstacles, le résultat de l'écoute d'un seul utilisateur de radio cognitive n'est pas fiable. Ainsi, les techniques d'écoute coopérative du spectre sont souvent utilisées pour lutter contre l'effet de déformation. Un autre défi important est l'écoute de la totalité du spectre à un emplacement physique particulier dans un temps d'observation assez court. Par conséquent, l'écoute du spectre large-bande est d'une importance primordiale pour assurer un fonctionnement efficace des réseaux de radio cognitive à la fois primaire et secondaire.

1.1. Radio cognitive

Historique

L'idée de la radio cognitive a été présentée officiellement par Joseph Mitola III à un séminaire à KTH, l'Institut royal de technologie, en 1998, publié plus tard dans un article de Mitola et Gerald Q. Maguire, Jr en 1999. Connu comme le « Père de la radio logicielle», Dr. Mitola est l'un des auteurs les plus cités dans le domaine. Mitola combine son expérience de la radio logicielle ainsi que sa passion pour l'apprentissage automatique et l'intelligence artificielle pour mettre en place la technologie de la radio cognitive. Et donc d'après lui : Une radio cognitive peut connaître, percevoir et apprendre de son environnement [52].

Définitions

Simon Haykin :

‘’La radio cognitive est considérée comme une nouvelle approche pour améliorer l’utilisation d'une ressource naturelle précieuse du spectre radio électromagnétique’’ [53].

L'Institut d’Électrique et d’Électronique des Ingénieurs (IEEE) :

‘’Un Émetteur/Récepteur radio fréquence qui est conçu pour détecter de manière intelligente si un segment particulier du spectre radio est actuellement en cours d’utilisation, et de sauter dans le spectre temporairement inutilisé très rapidement, sans interférer avec les transmissions des autres utilisateurs autorisés’’.

Groupe d'études des radiocommunications:

‘’Une radio ou un système qui écoute et est conscient, de son environnement opérationnel et peut dynamiquement et de manière autonome ajuster ses paramètres de fonctionnement de la radio en conséquence’’.

Afin d'améliorer l'efficacité d'utilisation du spectre et de fournir une bande-passante élevée aux utilisateurs mobiles, les réseaux de communication de nouvelles générations (NGN) [49] ont été élaborés pour mettre en œuvre les radios intelligentes en matière du spectre, aussi connu comme des radios cognitives [54], par des techniques d’accès dynamique au spectre comme le montre la Figure 1.1.

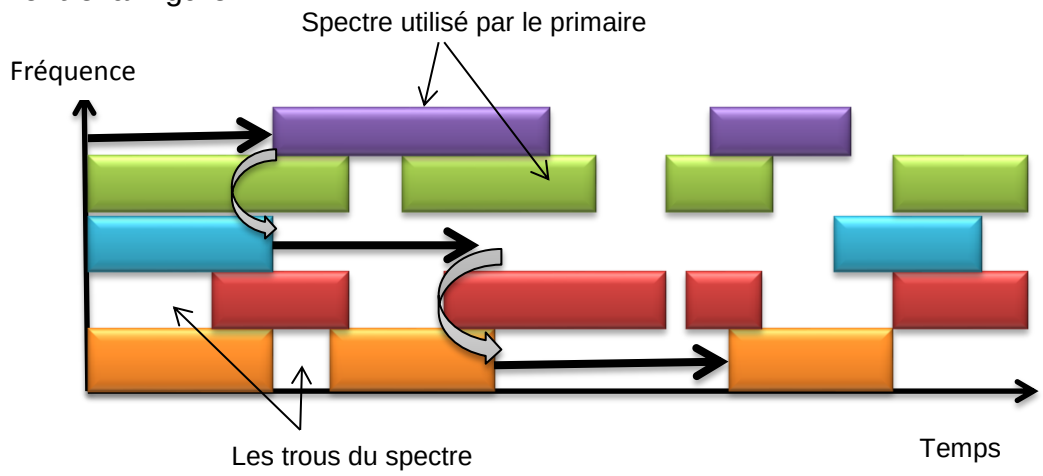


Figure 1.1: Illustration des trous du spectre et l’accès dynamique au spectre [55].

Le terme radio cognitive a été inventé par Mitola dans [54] et a une définition formelle suivante [53] :

Joseph Milota :

‘’La radio cognitive est un système de communication sans fil intelligent qui est conscient de son environnement (c'est-à-dire du monde extérieur), et elle utilise la méthodologie de compréhension pour apprendre de l'environnement et d'adapter ses états internes aux variations statistiques dans les stimuli RF entrants par des changements correspondants dans certains paramètres de fonctionnement en temps-réel (par exemple, la puissance transmise, la fréquence porteuse, et la stratégie de modulation), avec deux objectifs principaux à l'esprit:

- Une communication extrêmement fiable où et quand nécessaire.
- L’utilisation efficace du spectre radio. S. Haykin [53]’’

1.2. Protocoles utilisés par la radio cognitive

L'architecture de la radio cognitive est représentée dans la Figure 1.2 ci-dessous. Dans la couche physique, le spectre radiofréquence est mis en œuvre à base de radio définie par logiciel. Les protocoles d'adaptation de la couche MAC, réseau, transport, et applications doivent être conscients des variations de l'environnement radio cognitif. En particulier, les protocoles d'adaptation devraient envisager l'activité du trafic des principaux utilisateurs, les exigences de transmission d'utilisateurs secondaires, et les variations de qualité du canal [56].

Pour relier tous les modules, un contrôle radio cognitif est utilisé pour établir des interfaces entre l'émetteur/récepteur SDR et les applications et services sans fil. Ce module radio cognitif utilise des algorithmes intelligents pour traiter le signal mesuré à partir de la couche physique, et de recevoir des informations sur les conditions de transmission à partir des applications pour contrôler les paramètres de protocole dans les différentes couches. La Figure 1.3 présente les protocoles utilisés par la radio cognitive [57].

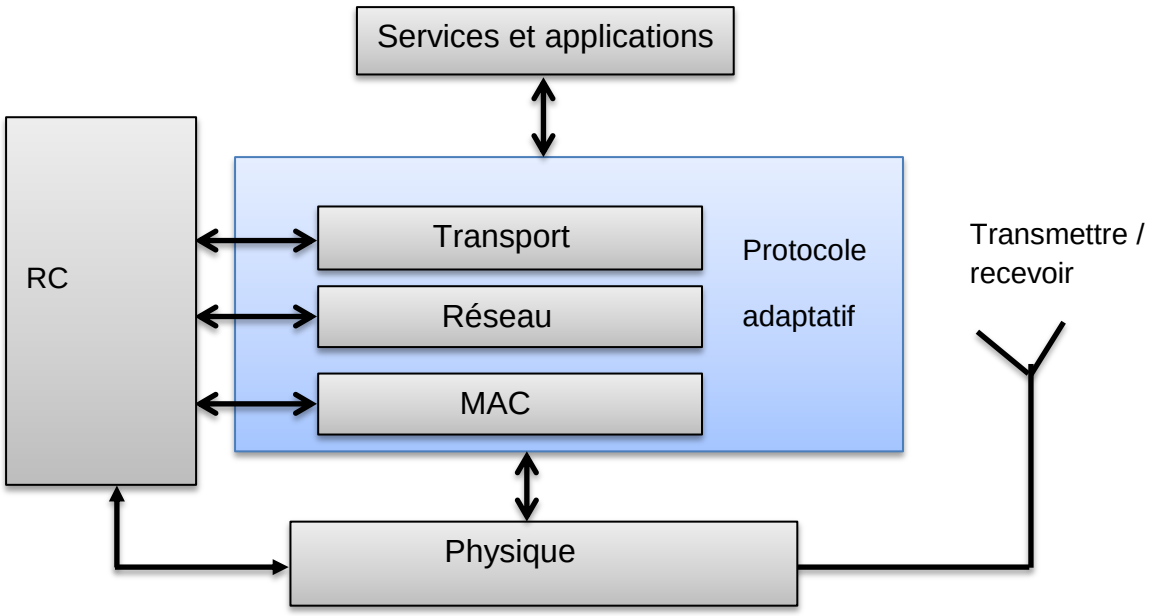


Figure 1.2 : Architecture d'un nœud radio cognitive [57].

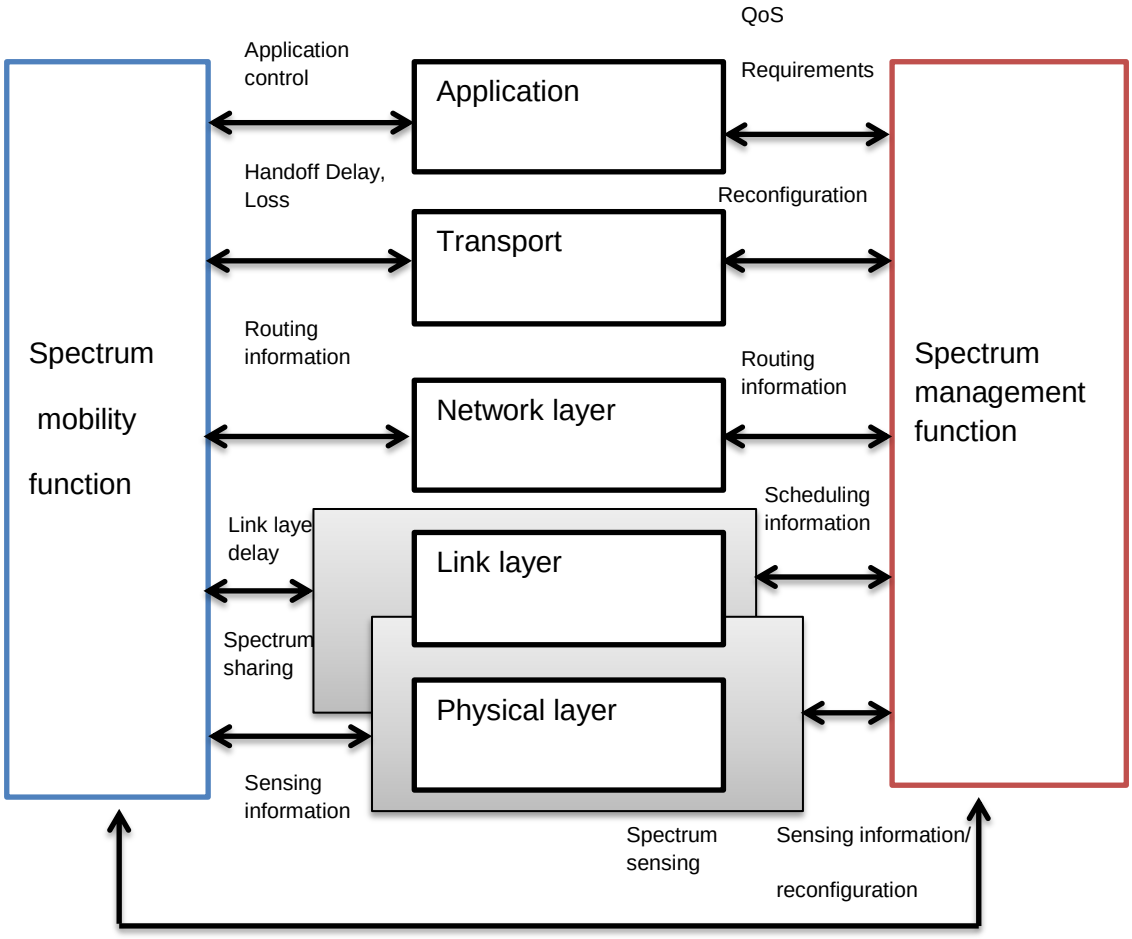


Figure 1.3: Différents protocoles utilisés par la radio cognitive [54].

1.3. Reconfiguration de la radio cognitive

Un autre élément clé de la radio cognitive est la reconfiguration. Afin de s'adapter à l'environnement RF, la radio cognitive devrait modifier ses paramètres de fonctionnement [49] :

Fréquence de fonctionnement: la radio cognitive est capable de changer sa fréquence de fonctionnement afin d'éviter l'utilisateur primaire ou afin de partager le spectre avec d'autres utilisateurs.

Schéma de modulation: la radio cognitive devrait de manière adaptative reconfigurer le schéma de modulation, en fonction des besoins d'utilisateurs et les conditions du canal.

Puissance de transmission: dans les limites de puissance, la puissance de transmission peut être reconfigurée afin de limiter les interférences ou d'améliorer l'efficacité spectrale.

Technologie de communication: la radio cognitive peut également être utilisée pour assurer l'interopérabilité entre les différents systèmes de communication en changeant son schéma de modulation, etc.

1.4. Cycle de cognition

Un cycle de cognition pouvant contrôler la circulation de l'information dans l'environnement radio est illustré dans la Figure 1.4.

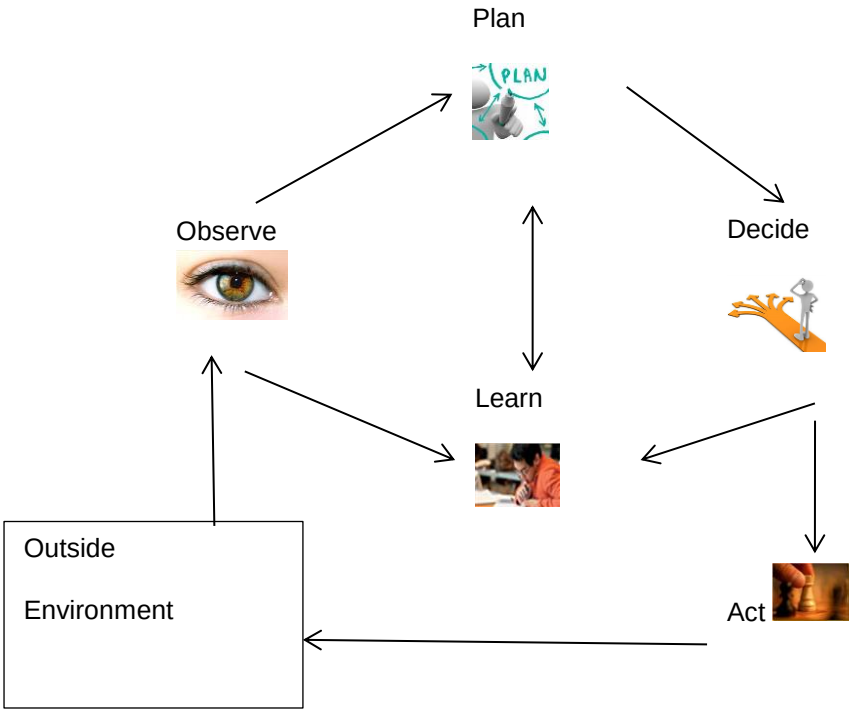


Figure 1.4: Etapes du cycle de cognition.

C'est une pratique très courante de l'interprétation du cycle de cognition comme un problème d'optimisation [58] comme représenté sur la Figure 1.4. Selon cette interprétation, les différentes phases assument la forme suivante:

- **Phase d'action :** consiste de reconfigurer la RC pour fournir une meilleure qualité de communication en ce qui concerne des objectifs définis par l'utilisateur. Cette configuration peut être, par exemple, le choix de l'interface radio sans fil à utiliser pour la communication, ou le réglage des paramètres du système de communication.
- **Phase d'observation :** implique la collection des statistiques du dispositif qui caractérise l'environnement externe, tel que les mesures de rapport SNR, le taux d'erreur du paquet, le temps de parcours,…,etc.
- **Phase d'orientation :** consiste à comprendre l'impact sur les performances de communication de l'environnement externe et les configurations possibles du système. Ceci est réalisé par l'identification d'une relation fonctionnelle entre les mesures, les paramètres de configuration, et les différents aspects de la performance de communication (par exemple, débit, retard, fiabilité).

- **Phase de décision :** est la solution du problème d'optimisation de la performance, c'est-à-dire, c'est la recherche dans l'espace de configurations possibles qui vise à trouver celui qui satisfait mieux les objectifs définis par l'utilisateur, qui sont exprimés en termes de mesures de performance de haut niveau tels que le débit de la couche d'application, le retard, la fiabilité, ainsi que le coût, et la consommation de puissance, …, etc.
- **Phase d'apprentissage :** consiste à évaluer le résultat des décisions qui ont été faites, ce qui collecte ainsi des connaissances à exploiter dans les futures phases d'orientation dans le but d'être plus efficace dans la phase de décision.

1.5. Composantes d'un émetteur-récepteur radio cognitive

Les différentes composantes d'un émetteur/récepteur de radio cognitive sont présentées dans la figure 1.5.

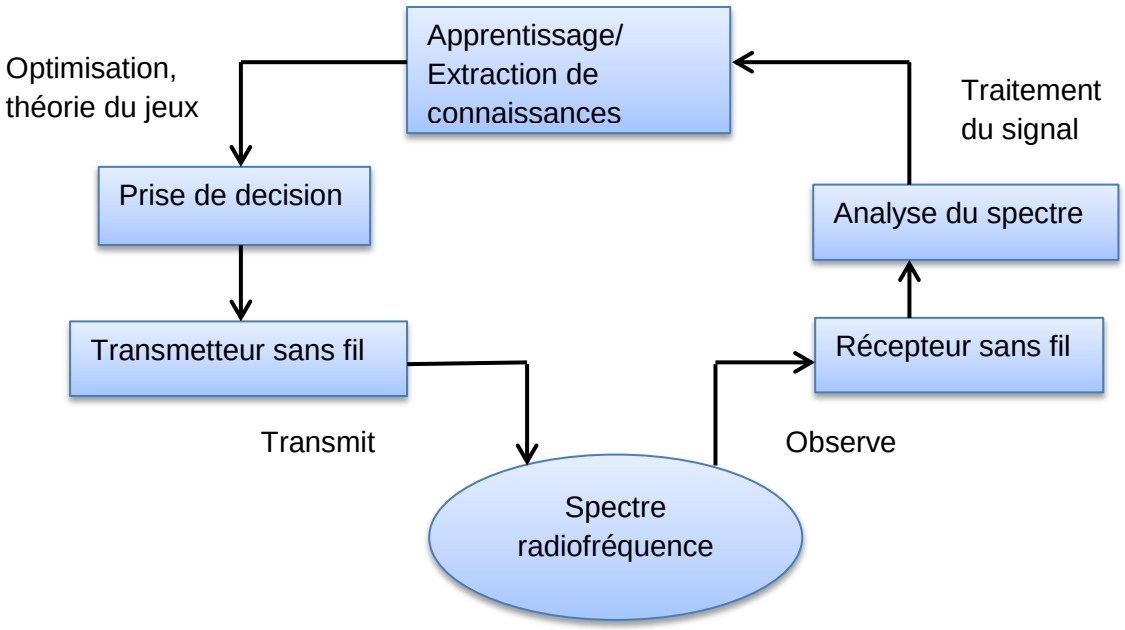


Figure 1.5 : Différentes composantes d'un émetteur-récepteur de radio cognitive [57].

- **Emetteur-récepteur :** Un récepteur radio cognitive est utilisé aussi pour observer l'activité sur le spectre de fréquence (détection du spectre). Les

paramètres de ce composant peuvent être modifiés dynamiquement comme dicté par les protocoles de couche supérieure [59].

- **Analyse du spectre :** L'analyseur de spectre utilise les signaux mesurés pour analyser l'utilisation du spectre (pour détecter la signature d'un utilisateur primaire et trouver les espaces blancs du spectre pour les utilisateurs secondaires).
- **Apprentissage et extraction de connaissance :** L'apprentissage et l'extraction de connaissance utilisent les algorithmes d'apprentissage et les informations sur l'utilisation du spectre pour comprendre l'environnement ambiant RF (le comportement des utilisateurs sous licence comme utilisateur primaire).
- **Prise de décision :** La décision sur l'accès au spectre doit être faite après que la connaissance de l'utilisation du spectre soit disponible. La décision optimale dépend du comportement coopératif ou compétitif des utilisateurs secondaires et dépend du milieu environnant ambiant RF. Les méthodes d'optimisation stochastique (le processus de décision de Markov) sont utilisées pour modéliser et résoudre le problème d'accès au spectre dans un environnement radio aléatoire.

1.6. Fonctions de la radio cognitive

Les fonctionnalités de la radio cognitive peuvent être résumées comme suit [55] :

- **Détection du spectre (spectrum sensing):** Le but de l'écoute du spectre est de détecter le spectre non utilisé et le partager sans interférence avec d'autres utilisateurs. La détection des utilisateurs primaires est la façon la plus efficace pour détecter les trous dans le spectre.

  L'écoute du spectre représente beaucoup d'aspects de la radio cognitive (voir figure ci-dessous Figure 1.6)

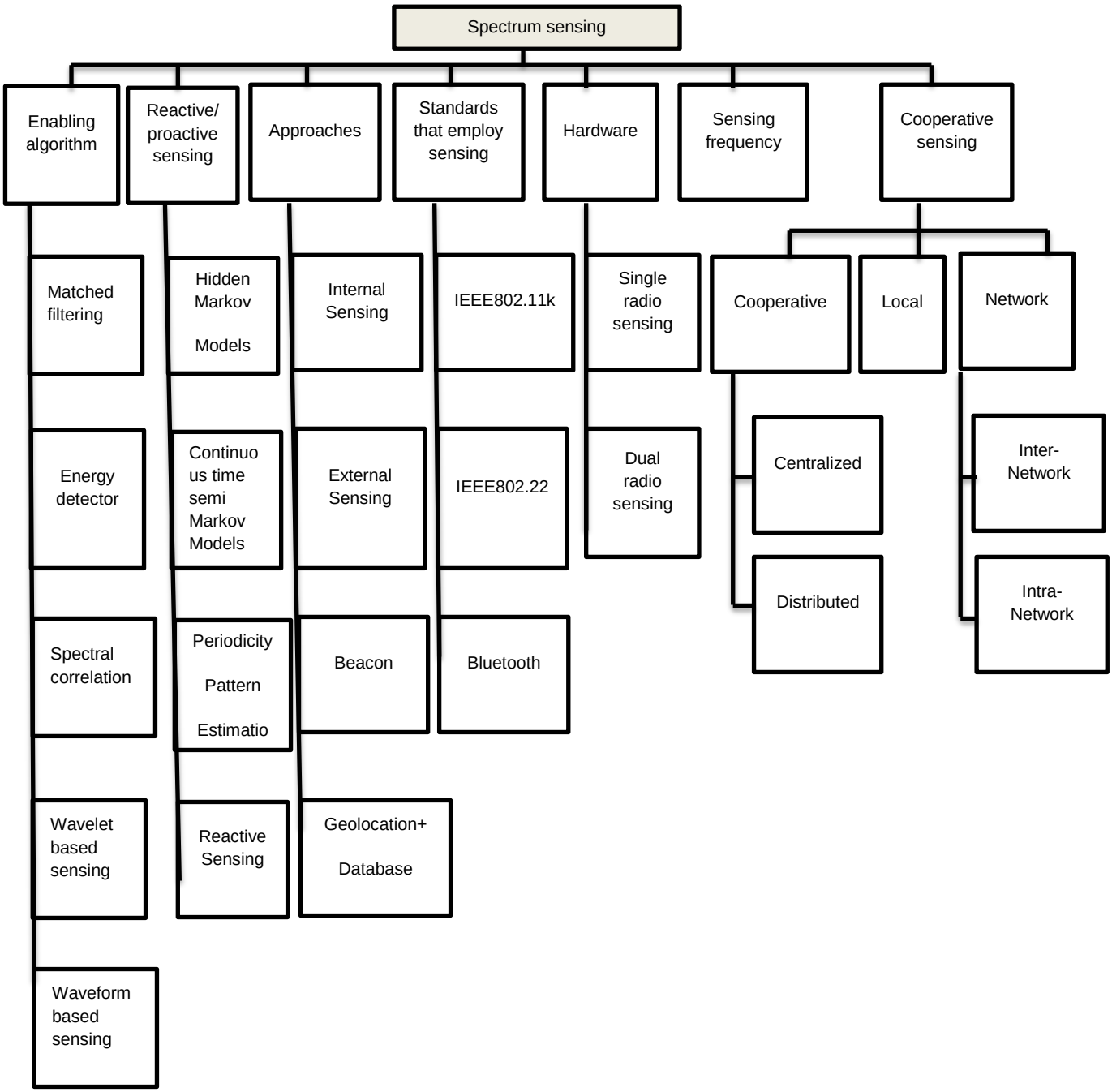


Figure 1.6: Plusieurs aspects de l'écoute du spectre pour la radio cognitive [54].

- **<u>Partage du spectre (spectrum sharing):</u>** Bien qu'il existe plusieurs utilisateurs coexistant de radio cognitive, le partage du spectre tout en tenant compte de l'efficacité spectrale est très important. Ces stratégies de partage devraient dépendre non seulement de la disponibilité du spectre, mais aussi des exigences des utilisateurs de la qualité du service.

- **Gestion du spectre (spectrum management):** L'objectif de la gestion du spectre est de fournir une utilisation souple, équitable et efficace des ressources radio. Capter les meilleures fréquences disponibles pour répondre aux besoins de communications des utilisateurs. Les radios cognitives devraient décider de la meilleure bande du spectre pour répondre aux exigences de QoS sur toutes les bandes de fréquences.

- **Mobilité du spectre (spectrum mobility):** c'est l'opération qui permet à l'utilisateur de la radio cognitive de changer sa fréquence de fonctionnement. Les réseaux de radio cognitive essayent d'utiliser le spectre de manière dynamique en permettant à des terminaux radio de fonctionner dans la meilleure bande fréquence disponible.

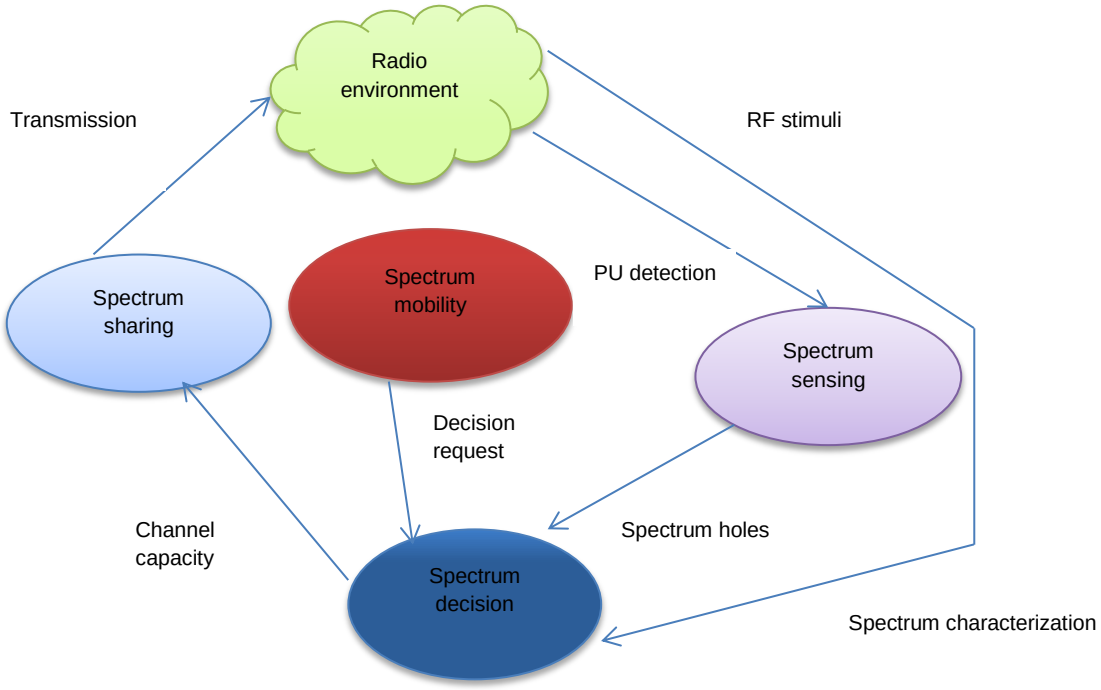


Figure 1.7 : Fonctions de la radio cognitive [60].

1.7. Réseaux de radio cognitive

Dans les réseaux sans fil d'aujourd'hui, des bandes de fréquences sont attribuées par les autorités gouvernementales pour l'utilisation sous-licence dans les grandes zones géographiques. Il a été réalisé par des mesures récentes que la plupart des bandes de fréquences allouées ne sont pas utilisées efficacement.

Malgré cette sous-utilisation du spectre, il y a pénurie de fréquences dans la communauté sans fil en raison de l'apparition de nouveaux technologies et services sans fil. Comme il peut être observé dans la Federal Communications Commission (FCC) tableau d'attribution des fréquences, comme montre la Figure 1.8 ci-dessous, la plupart des bandes de fréquences utiles sont déjà affectées à différents services sans fil. Puisque la demande du spectre augmente et la tendance est envisagée de poursuivre à l'avenir ainsi, de nouvelles techniques sont étudiées pour utiliser les espaces non utilisés du spectre à travers le temps, la fréquence, et l'espace. Ces portions temporairement libres du spectre sont appelées des trous du spectre ou des espaces blancs du spectre. Par conséquent, différentes approches novatrices ont été proposées récemment pour profiter des portions inutilisées du spectre par l'accès dynamique au spectre [54].

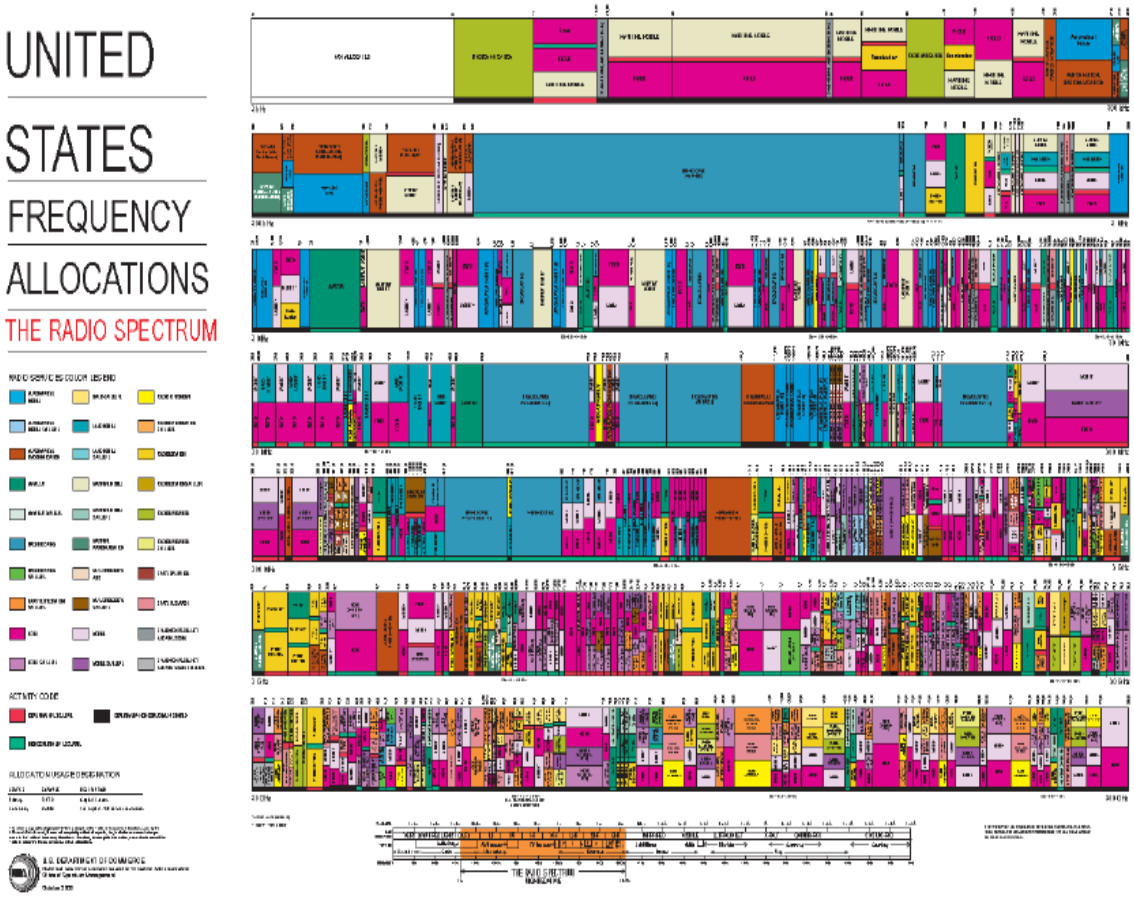


Figure 1.8 : Carte d’allocation du spectre FCC.

1.7.1. Architecture de réseaux de radio cognitive

L'Architecture d'un réseau de RC comprend des unités primaires et secondaires et les équipements qui sont utilisés pour faciliter leurs communications tels que les stations de base ou les courtiers spectrales. En général, deux groupes de réseaux constituent cette architecture: réseaux primaires et réseaux de RC. Ces deux réseaux pourraient avoir une station de base pour coordonner leurs communications ou fonctionner sans une infrastructure par exemple sur une base ad-hoc. Les réseaux de RC peuvent utiliser un courtier spectral qui est impliqué dans la distribution des ressources du spectre entre les différents réseaux de RC [54]. Une architecture typique pour un réseau radio cognitif est présentée dans la figure 1.9 ci-dessous.

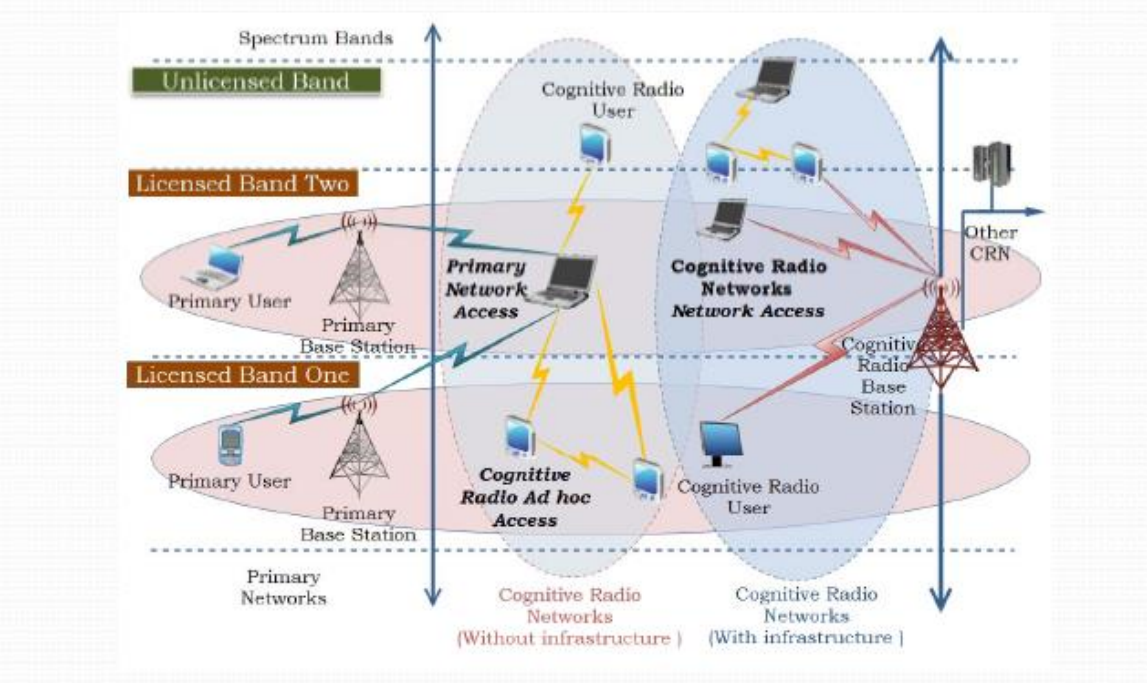


Figure 1.9 : Architecture d'un réseau de radio cognitif.

Dans la bande non-licenciée, puisque tous les USs ont des droits égaux pour utiliser le spectre, le principal devoir d'un réseau de RC est de coordonner les communications entre eux d'une manière équitable et efficace. Dans le spectre licencié, les UPs dans un réseau primaire ont des droits exclusifs de communication dans les bandes de fréquences spécifiques tandis que les USs dans un réseau de RC ne peuvent pas occuper le spectre licencié si elles ne sont pas employées par les UPs. Par conséquent, la responsabilité la plus critique d'un

réseau de RC est de reconnaître la présence d'activités des UPs. En outre, les USs devrait être en mesure de communiquer de façon continue et sans heurts. Un réseau de RC bien conçu doit également tenir compte des exigences spécifiques de la qualité de service (QoS) de différentes applications utilisées par les USs. Afin de répondre à ces exigences, il est essentiel de définir de nouvelles techniques de gestion du spectre [54].

1.8. Radios cognitives interactives

Les radios cognitives sont très prometteuses. Elles peuvent néanmoins avoir un impact négatif sur les performances du réseau. Cet impact peut ne pas être immédiatement apparent sur le cycle de cognition comme le montre la Figure 1.4. Un schéma plus réaliste des processus d'une radio cognitive dans un réseau est illustré à la figure 1.10 où les radios cognitives réagissent à la fois de façon ‘’muettes’’ et ‘’intelligentes’’. De nombreuses radios cognitives sont, en particulier, en réaction avec un monde extérieur dont l'état est déterminé conjointement par les adaptations de plusieurs radios cognitives, Ce réseau d’adaptation constitue un processus de décision interactif [61].

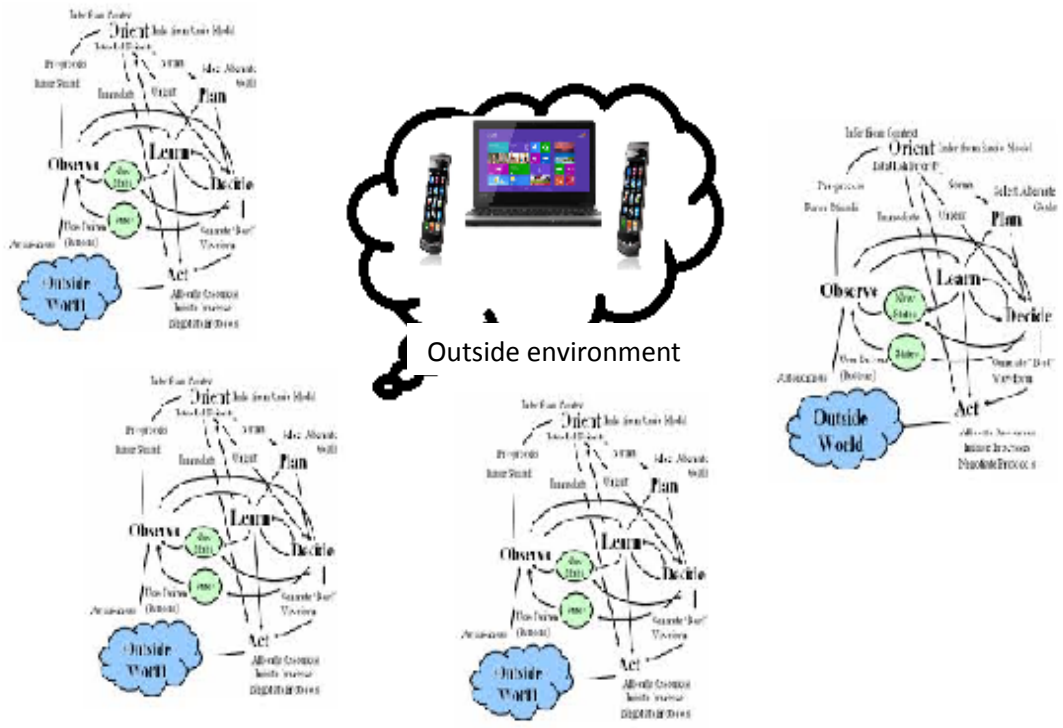


Figure 1.10: Modèle interactif de la radio cognitive reproduit de la Figure 1.4 [61].

1.9. Domaines d'application de la radio cognitive

Le concept de la radio cognitive peut être appliqué à une variété de scénarios de communication sans fil, nous allons décrire quelques-uns :

- **Coexistence de différentes technologies sans fil [56]:** Les nouvelles technologies sans fil (IEEE 802.22) sont en cours d'élaboration pour la réutilisation des fréquences radio allouées à d'autres services sans fil (service TV). La radio cognitive est une solution qui fournit la coexistence de ces différentes technologies et services sans fil. Par exemple, IEEE 802.22, basée sur les utilisateurs WRAN peut utiliser efficacement la bande TV quand il n'y a pas d'utilisation du téléviseur à proximité ou quand une station de télévision ne diffuse pas.

  Réseaux militaires [56]: Avec la radio cognitive, les paramètres de la communication sans fil peuvent être adaptés de manière dynamique en fonction du temps et de l'emplacement ainsi que de la mission des soldats.

  Réseaux sans fil de prochaine génération [56]: La radio cognitive devrait être une technologie clé pour la prochaine génération de réseaux sans fil hétérogènes. La radio cognitive fournira des renseignements intelligents à la fois pour l'utilisateur et pour le fournisseur d'équipements. Pour l'utilisateur, un dispositif mobile avec des interfaces d'air multiples (WiFi, WiMAX, cellulaires) peut observer l'état des réseaux d'accès sans fil (la qualité de transmission, le débit, et le délai) et prendre une décision sur la sélection de l'accès au réseau pour communiquer avec.

  Services de cyber santé [59] : Dans ce cas, les équipements et appareils utilisent la transmission RF. L'utilisation du spectre doit être choisie avec soin pour éviter toute interférence, donc les concepts de la radio peuvent être appliqués.

  Réseaux d'urgence [59] : Les réseaux d'urgence peuvent profiter des concepts de la radio pour fournir la fiabilité et la flexibilité de communication sans fil.

D’autres applications citant par exemple : les réseaux mobiles, les réseaux véhiculaires, les smart grids, la sécurité publique, et la gestion du désastre.

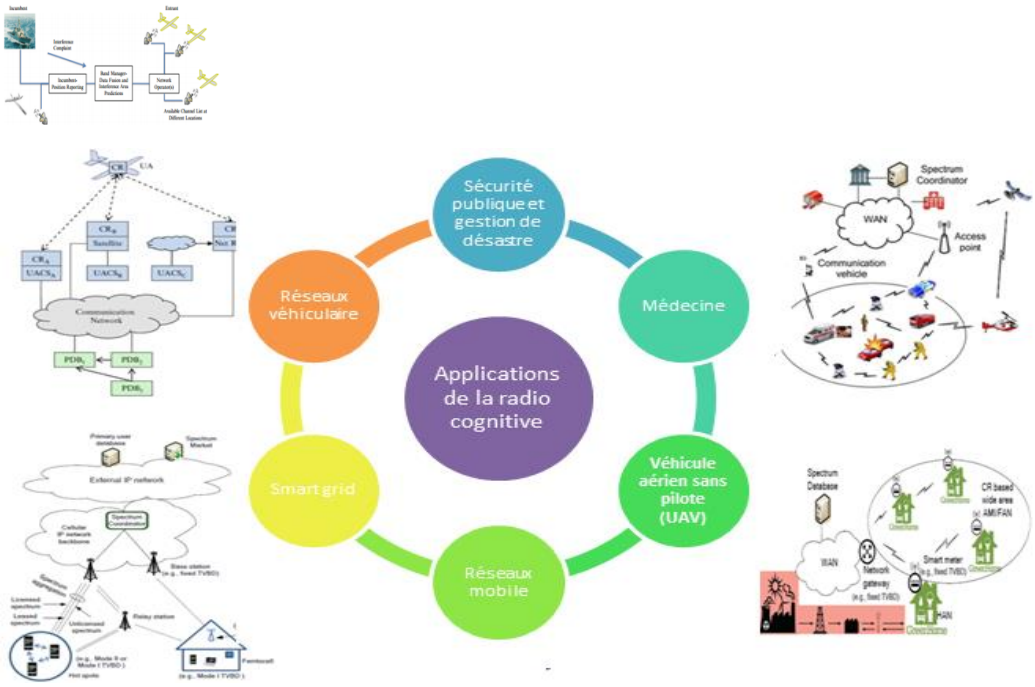


Figure 1.11: Applications de la radio cognitive [62].

1.10. Accès dynamique au spectre

La croissance explosive des appareils sans fil ces dernières années montre la demande croissante des communications, ainsi le spectre devient plus encombré. Nous savons que l’allocation du spectre statique est un problème majeur dans les réseaux sans fil. Généralement, ces allocations conduisent à une utilisation inefficace du spectre et elles créent ce que l’on appelle des trous ou des espaces blancs dans le spectre. Pour résoudre le problème de l’encombrement, les réseaux radio cognitive utilisent l’accès dynamique au spectre (ADS) [57, 63].

L’accès au spectre dynamique est l'application la plus importante des radios cognitives. Il a attiré beaucoup d'intérêt parmi les décideurs, les opérateurs de réseaux, et les chercheurs [64, 65]. Bien que la cognition est un terme très large et a des applications dans tous les niveaux d'une pile de protocole, dans cette thèse

on concentre uniquement sur l'application de la cognition dans la couche physique (PHY).

La communication coopérative est connue comme un moyen pour surmonter les limites des systèmes sans fil. Cependant, puisque les utilisateurs ont généralement une connaissance limitée de leur environnement, nous prétendons que le comportement coopératif peut leur fournir les informations nécessaires pour résoudre les problèmes globaux.

1.11. Écoute du spectre large-bande

Les techniques d'écoute de spectre large-bande ont pour but de détecter une largeur de bande de fréquence qui est supérieure à la largeur de bande du canal. Par exemple, pour exploiter les opportunités spectrales dans toute la bande ultra-haute fréquence (UHF) (entre 300 MHz et 3 GHz), les techniques d'écoute du spectre large-bande devraient être employées. Nous notons que les techniques d'écoute du spectre de bande-étroite ne peuvent pas être utilisées directement pour effectuer l'écoute du spectre large-bande, parce qu'ils prennent une décision binaire unique pour l'ensemble du spectre et donc ne peuvent pas identifier les opportunités spectrales individuelles qui se situent dans le spectre large-bande. L'écoute de spectre large-bande peut être classée en deux types : l'écoute du spectre large bande de Nyquist, et l'écoute du spectre large-bande sous-Nyquist. Le premier type traite les signaux numériques prises au niveau ou au-dessus de la fréquence de Nyquist, alors que le deuxième type acquiert des signaux en utilisant le taux inférieur au taux d'échantillonnage de Nyquist [66].

Algorithme d'écoute du spectre de bande-étroite	Avantages	Inconvénients
Filtrage Matched	Performance optimale. Faible coût de calcul.	N'exige pas une information préalable de l'utilisateur primaire.
Détection d'énergie	N'exige pas une information préalable. Faible coût de calcul.	Mauvaise performance pour faible SNR. Ne peut pas différencier les utilisateurs.

Détection cyclo-stationnaire	Valable dans une région de faible SNR. Robuste contre les interférences.	Exige une information préalable partielle. Coût élevé de calcul.

Tableau 1.1 : Avantages, inconvénients, et algorithmes d'écoute du spectre de bande-étroite.

Type	Écoute large-bande de Nyquist	Écoute large-bande sous-Nyquist
Algorithme	Convertisseur standard CAN	Écoute compressive
Avantage	Structure simple	Taux d'échantillonnage faible, Coût d'acquisition du signal
Inconvénient	Taux d'échantillonnage élevé, Coût d'énergie.	Sensible aux imperfections de conception
Défis	Réduire le taux d'échantillonnage, Économiser l'énergie	Améliorer la robustesse aux imperfections de conception

Tableau 1.2 : Avantages, inconvénients, et défis des algorithmes d'écoute du spectre large-bande.

1.12. Ecoute coopérative du spectre large-bande

Dans un environnement multi-trajets ou obstacles, le signal primaire reçu au niveau des récepteurs radios cognitives peut être sévèrement dégradé, conduisant à des résultats d'écoute large-bande incertain dans chaque radio cognitive. Dans cette situation, les futurs réseaux de radios cognitives doivent employer des stratégies de coopération pour l'amélioration de la fiabilité d'écoute du spectre à large-bande en exploitant la diversité spatiale. En fait, dans un réseau de radio cognitive basé sur cluster, les spectres large-bande observés par différentes radios cognitives pourraient partager certaines composantes spectrales communes, tandis-que chaque radio cognitive peut observer certaines composantes spectrales innovantes. Ainsi, il est possible de fusionner des mesures compressées des différents utilisateurs et exploiter les corrélations

spectrales entre les radios cognitives afin d'économiser le nombre total de mesures et donc la consommation d'énergie dans les radios cognitives. Une telle technique coopérative basée sur une fusion de données, peut cependant, conduire à la charge de transmission de données lourd dans les canaux de contrôle communs. Une solution consiste à développer des techniques d'écoute à large-bande basées sur la fusion de décision si chaque radio cognitive est capable de détecter le spectre large-bande de façon indépendante. En raison de la ressource du calcul limitée dans les réseaux cellulaires, le défi qui reste dans l'approche coopérative basée sur la fusion de décision est de savoir comment combiner de manière appropriée des informations en temps-réel. L'écoute du spectre coopérative à large-bande peut être mise en œuvre en deux modes : centralisée, et distribuée [66] :

1.12.1. Ecoute coopérative large-bande centralisée (ECLC)

Dans l'écoute centralisée, une unité centrale recueille l'information d'écoute à partir d'appareils cognitifs, identifie le spectre disponible, et diffuse cette information à d'autres radios cognitives ou contrôle directement le trafic radio cognitive, voir la Figure 1.12 ci-dessous.

1.12.2. Ecoute coopérative large-bande distribuée (ECLD)

Dans l'écoute distribuée, les nœuds cognitifs partagent des informations entre eux, mais ils prennent leurs propres décisions quant à la partie du spectre qu'ils peuvent utiliser. L'écoute distribuée est plus avantageuse que l'écoute centralisée dans le sens où il n'y a pas besoin d'une infrastructure de base à moindre coût, voir Figure la 1.13 ci-dessous.

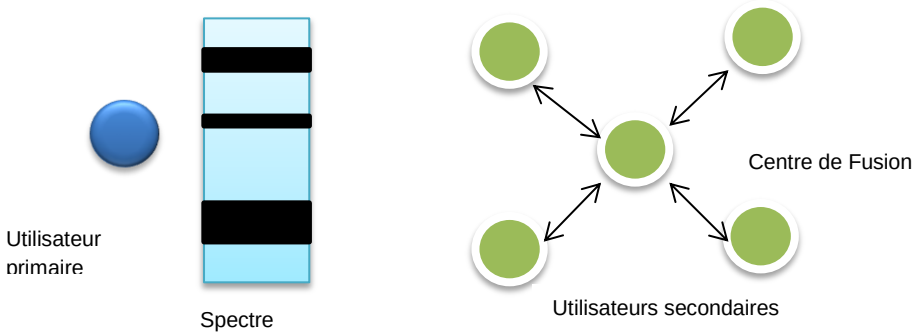


Figure 1.12: Ecoute coopérative centralisée large-bande de la radio [67]

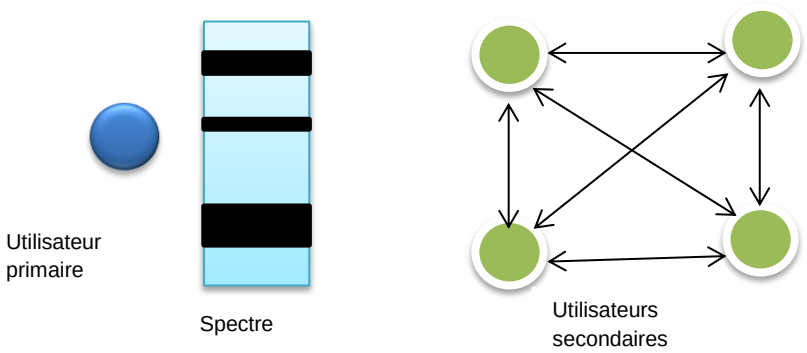


Figure 1.13: Ecoute coopérative distribuée large-bande de la radio [67]-[68]-[69]-[70]-[71].

1.13. Conclusion

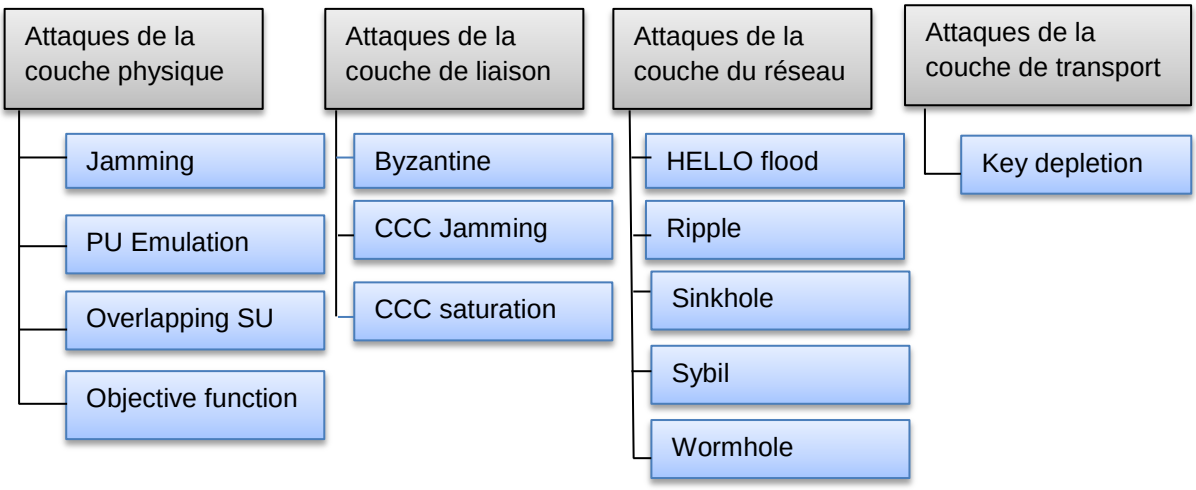
- La radio cognitive est un concept sensible au spectre RF
- Très utile pour réseaux de la troisième génération, la quatrième génération, et la cinquième génération.
- Les techniques de partage du spectre peuvent nous aider à remplir les espaces blancs dans un environnement d'interférence intentionnel particulier.
- Une grande partie de la recherche doit être encore faite sur la simulation et d'explorer explorer les réseaux intelligents.
- La technologie radio cognitive peut résoudre le problème du spectre sous-utilisé.
- Le but principal de ce premier chapitre est d'analyser et aussi d'améliorer des solutions de sécurité et de fournir un débit plus élevé.

CHAPITRE 2
MENACES DE LA SECURITE DANS LES RADIOS COGNITIVES ET LES RESEAUX DE RADIO COGNITIVE

2.1. Introduction

Les radios cognitives peuvent être considérées comme des dispositifs intelligents qui sont capables d'apprendre des expériences et de s'adapter dynamiquement à l'environnement extérieur. Les efforts de recherche importants ont été consacrés à l'étude et le développement des techniques d'apprentissage automatique et de reconnaissance de patrons sans tenir compte des questions liées à la sécurité en détail. En règle générale, les problèmes de la sécurité sont abordés par le biais de l'ajout d'une authentification sur un mécanisme de chiffrement de la communication de données au sein du réseau. Toutefois, cela ne suffit pas toujours en raison des capacités améliorées du modèle cognitif. En particulier, les moteurs d'intelligence artificielle que représentent le noyau des dispositifs cognitifs, les menaces potentielles qui sont en mesure de nourrir les radios cognitives avec des fausses entrées sensorielles ainsi affectent volontairement leurs connaissances et par la suite leurs comportement doit être considérés. Voir ci-dessous, différents types d'attaques dans les couches de la radio cognitive.

2.2. Différents types d'attaques dans les couches de la radio cognitive



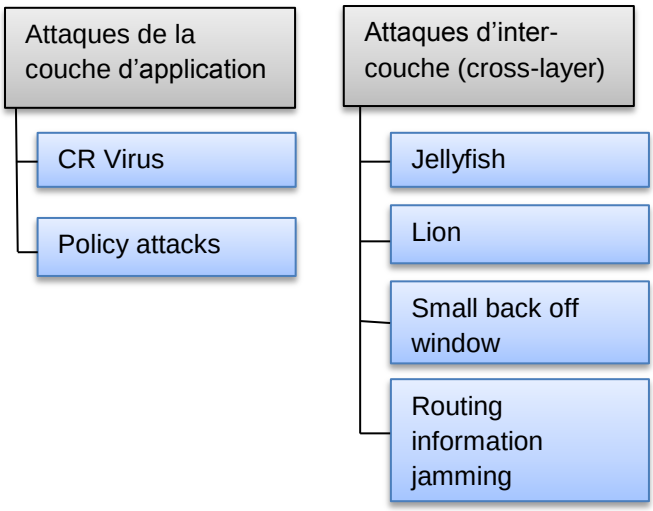


Figure 2.1: Différents types d'attaques dans les couches de la radio cognitive [62].

2.3. Différents types d'attaques et les contremesures électroniques

Les différents types d'attaques et les contremesures électroniques dans la technologie radio cognitive comme montre le Tableau 2.1 ci-dessous [72]:

Attaques	**Contremesures électroniques**
Attaque de brouillage sur les canaux de contrôle CCC (control channel jamming)	Saut de fréquence CCC, distribution de la clé CCC
Attaque de l'utilisateur émulateur primaire (malveillant ou utilisateur secondaire Selfish)	Caractéristiques déjà connues des signaux d'utilisateur primaire, Techniques de détermination de location, Accès à la géolocalisation de l'information sur la base que les utilisateurs primaires sont connus a priori.
Attaque de la falsification des données de l'écoute du spectre (attaque Byzantine)	Authentification mutuelle, Intégrité des données, Chiffrement des données, Déploiement de capteurs sans fil dédiés, Mécanismes d'oublier sélectivement les informations passées.
Attaque de brouillage (trigger DoS)	Saut de fréquence, Utilisateurs légitimes change leurs emplacements pour échapper à la plage d'interférence imposée par l'attaquant.
Attaque de la fonction objective (manipule les valeurs des paramètres de la radio).	Aucune bonne solution n'a été proposée, Simple proposition est de définir des valeurs de seuil pour chaque paramètre radio.

Attaque Lion est une attaque multicouche dans le but de causer un DoS à la couche de transport	Ensemble de lignes directrices générales pour réduire l'efficacité de l'attaque
802.22 spécifique	Sécurité sous-couche traite certains vulnérabilités, principalement par: Confidentialité de la gestion de la clé v2; Message d'authentification des codes; Standard de chiffrement avancé
Perturbation des mécanismes d'apprentissage des radios cognitives	Ensemble de directives générales, par Exemple : Multi-module de programmation Objective vérifie toutes les paramètres de reconfiguration dans chaque itération.

2.4 Conclusion

La radio cognitive, et certaines caractéristiques les plus importantes qui leur sont associées: l'accès opportuniste au spectre et l'accès dynamique au spectre. Sans doute, elle est particulièrement innovante, passionnante, et surtout un sujet de recherche très pertinent. Cependant, l'avancée caractéristique liée à la technologie radio cognitive apporte de nouveaux groupes de problèmes concernant la sécurité potentielle. Aborder adéquatement ces problèmes est primordial pour construire des réseaux de nouvelle génération dite de radio cognitive efficaces et protégés. Ce chapitre a donné un résumé, des différents problèmes d'attaques et les solutions contre-attaques correspondantes pour : les réseaux sans fil existants, les réseaux de radio logiciel, et les réseaux de radio cognitive. La plupart des problèmes de sécurité considérés découlent du déploiement d'une technique d'occupation du spectre, généralement l'une des techniques d'écoute du spectre, et l'auto-reconfigurabilité des radios. Les principales menaces au spectre sont les attaques malveillantes de l'utilisateur émulateur primaire, les attaques byzantines, et les attaques de brouillage intelligents. Selon le type du mécanisme d'apprentissage déployé, un risque majeur pour la sécurité est présent sous la forme d'une attaque de la fonction objective, qui vise le mécanisme de l'apprentissage d'une radio cognitive.

CHAPITRE 3
STRATEGIES DE BROUILLAGE DANS LES RADIOS COGNITIVES

La Guerre Electronique (GE) est l'utilisation de l'énergie électromagnétique pour déterminer, exploiter, réduire ou empêcher l'utilisation hostile du spectre [73], Voir les deux Figures (3.1) et (3.2) ci-dessous.

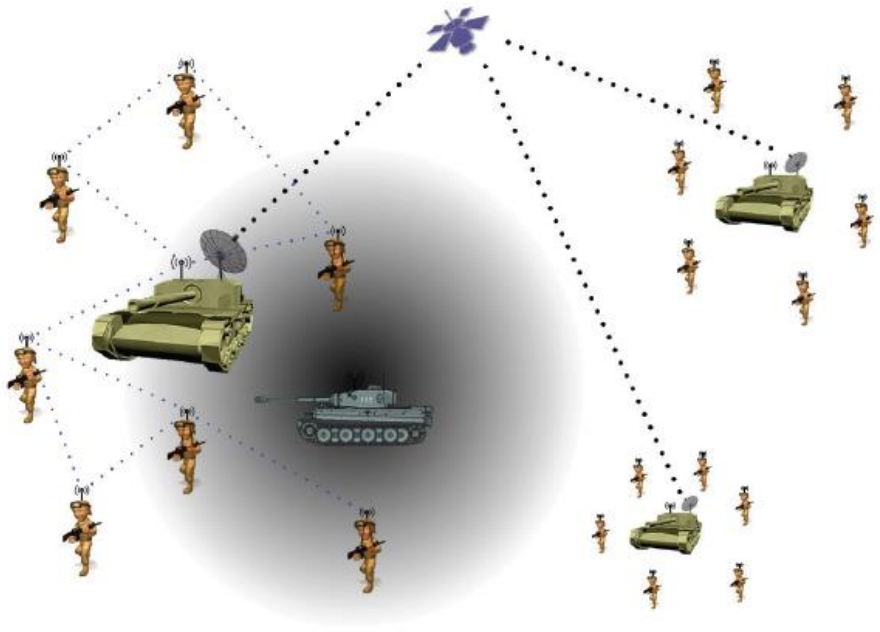


Figure 3.1: Enquête d'un scénario WLAN sans fil: Un cadre militaire où plusieurs entités mobiles communiquent entre eux utilisant un réseau sans fil. L'attaque de brouillage (représentée comme indique le cercle gris) doit être détectée [74].

L'acceptation de l'idée que la GE peut jouer un rôle majeur dans les conflits militaires remonte à plusieurs années. La plupart des efforts visant à utiliser la GE se sont portés sur les radars et produit des résultats importants dans ce domaine particulier. Ces dernières années ont entraîné une prise de conscience croissante qu'il y a des besoins et des opportunités similaires pour les exploitations concernant les systèmes de communication sans fil.

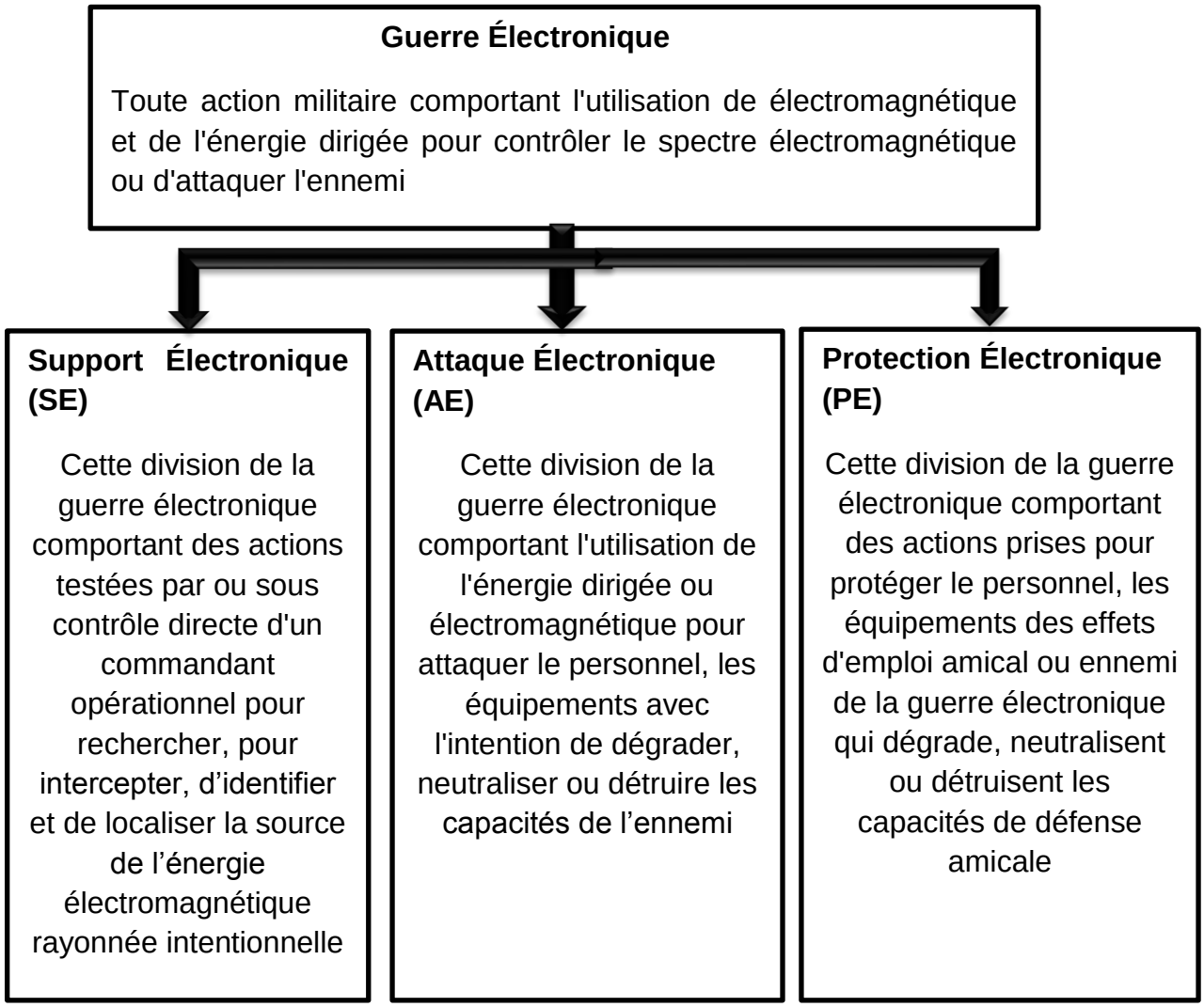


Figure 3.2 : Définitions de la guerre électronique d'après l'OTAN [75].

La GE comporte trois catégories principales, qui sont:

- Support Electronique (SE)
- Attaque Electronique (AE)
- Protection Electronique (PE)

Le SE consiste à détecter l'activité du signal de l'ennemi, la classification des signaux et l'extraction intelligente, et déterminer l'emplacement de l'émetteur. L'AE comprend l'utilisation d'armes à énergie dirigée (lasers, micro-ondes, des faisceaux de particules), les missiles antiradiation et des impulsions électromagnétiques pour détruire les équipements électroniques de l'ennemi. La

PE implique l'utilisation des techniques de comptage pour réduire l'efficacité des activités d'AE de l'ennemi.

En général, le brouillage est réussi lorsque le signal de brouillage perturbe le processus de communication. Ce chapitre décrit ces méthodes dites techniques de brouillage en détails.

3.1. Stratégies de brouillage

Dans cette section, nous rappelons les stratégies de brouillage classiques et nous introduisons un modèle de brouillage récent, c'est-à-dire, le brouilleur radio cognitive, qui s'adapte de façon dynamique des stratégies de brouillage standard pour un environnement dynamique afin de maximiser son efficacité.

3.1.1. Brouillage basé sur l'acteur

On considère un scénario de communication classique tel que représenté dans la Figure 3.3: un émetteur (TX) veut livrer un message à un récepteur (RX), tandis que l'utilisateur brouilleur (UJ) veut empêcher la communication de se produire.

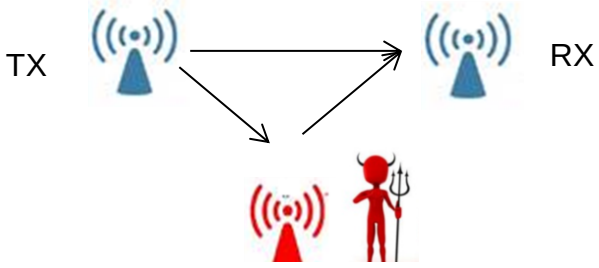


Figure 3.3: Système de communication de base dans un environnement de brouillage: l'utilisateur brouilleur (UJ) veut empêcher la communication entre un émetteur (TX) et un récepteur (RX).

Le scénario classique consiste à un utilisateur brouilleur pour être en mesure d'écouter le canal radio (afin de trouver une communication active) et de transmettre des signaux ou messages (à grande puissance). A l'inverse, l'émetteur détecte le spectre radio et, s'il reconnaît le spectre radio libre, il

commence par le processus de transmission. Le spectre, ou plus précisément le canal impliqué dans la communication, est reconnu comme libre si le rapport signal sur interférence plus bruit (SJNR) est sous un certain seuil. Tous les dispositifs radio sont équipés d'un indicateur d'intensité du signal reçu qui est utilisé pour déduire l'état du canal, et des seuils SJNR dépendent des systèmes de communication particuliers. Enfin, nous supposons que le récepteur est capable de recevoir et de décoder correctement le message émis si seulement le rapport SJNR est au-dessus d'un certain seuil [76].

Le brouillage peut être classé en fonction de l'appareil ciblé: l'émetteur ou le récepteur, c'est-à-dire, nous nous référons à un Bruit-Émulateur lorsque l'utilisateur brouilleur vise l'émetteur (prévention de la transmission), tandis que nous nous référons à un bruit-brouillage lorsque l'utilisateur brouilleur cible un ou plusieurs récepteurs radio (empêchant la réception correcte du message) [77]. La Figure 3.4 résume l'activité de brouilleur en fonction de l'appareil ciblé: l'Émulateur, lorsque l'utilisateur brouilleur fait apparaître le canal occupé à l'émetteur, et le brouillage, lorsque l'utilisateur brouilleur empêche la bonne réception du message par le récepteur. La première est effectuée en saturant le canal radio avec un signal d'émulation d'attaque, tandis que la seconde est obtenue par l'envoi aux récepteurs d'un signal à puissance élevée au moins supérieure à la prétendue dans le but de perturber par l'interférence intentionnelle de la réception correcte du message. Pour faciliter l'exposition, dans la suite nous nous référons à un brouillage pour les deux activités le Bruit-Émulateur (Spoofing) et le Bruit-Brouillage (Jamming).

3.1.2. Brouillage de la couche de communication

Le brouillage peut également être classé en fonction de la couche de communication sur laquelle il est exécuté. Nous distinguons le brouillage de la couche physique et la couche de liaison. En particulier, l'hypothèse d'un système de communication spécifique, par exemple : 802.11, Bluetooth ou GSM, le brouillage de la couche de liaison est effectué par la diffusion en continu des paquets bien formés, et donc, afin que l'émetteur présumé ne puisse jamais écouter un canal libre. Une telle attaque peut être facilement réalisée avec des

périphériques matériels à bas prix en inondant tout simplement un canal sans fil ciblé avec de grands paquets de données, c'est-à-dire, en gardant un canal sans fil occupé aussi longtemps que cela est possible [76].

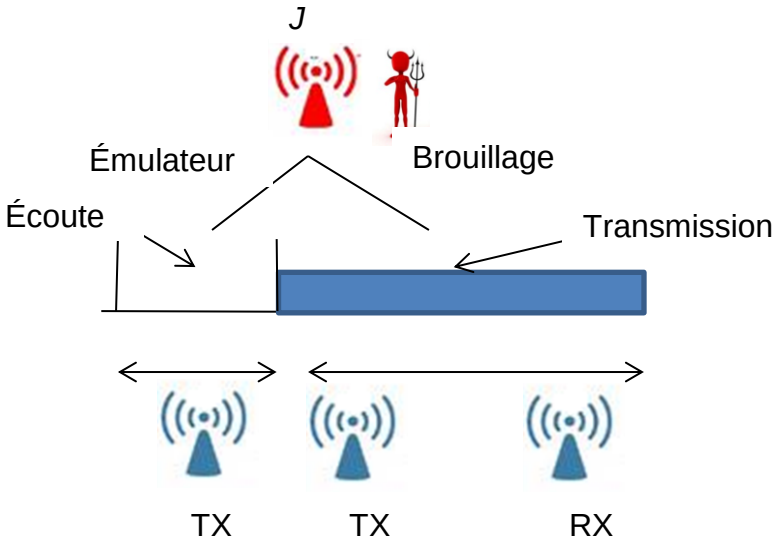


Figure 3.4 : Emetteur (TX) écoute le canal radio, et transmet le signal radio au récepteur (RX). Le brouilleur transmis un signal radio au cours de la phase d'écoute (Spoofing) ou au cours de la phase de transmission (Jamming).

Le brouillage de la couche physique est quel que soit le système de communication actuel vise à produire une interférence intentionnelle perturbatrice sur le côté du récepteur: cela peut être réalisé en utilisant un brouillage de tonalité, c'est-à-dire, par génération d'une forme d'onde sinusoïdale dont la puissance est concentrée sur la fréquence porteuse ciblée. Une telle attaque pourrait être plus perturbateur et nécessite du matériel plus spécifique.

3.1.3. Brouillage dans les réseaux de radios cognitives

Une stratégie-fixée de brouilleur effectue la même activité pour tous les intervalles de temps de communication. Par exemple, supposant que la Figure 3.4, est un système de communication sans fil 802.11g, le brouilleur peut écouter la scène radio, identifier le canal de communication utilisé par l'émetteur et le récepteur, et commence par la suite son activité de brouillage à émettre un signal de forte puissance sur le canal de communication. Bien que ce comportement pourrait être efficace (et perturbateur) dans un réseau de communication

standard, il s'avère inefficace dans les réseaux de radio cognitive, qui sont intrinsèquement robustes pour un tel type d'attaque. En fait, les appareils de radio cognitive changent dynamiquement leur configuration radio en fonction du comportement de la scène de la radio; c'est-à-dire, ils sont toujours à la recherche de bandes de fréquences disponibles, ils reconfigurent leurs paramètres de communication à plusieurs reprises, tels que la fréquence, la bande, et le protocole. Par conséquent, une stratégie-fixée de brouilleur standard peut ne pas être efficace ou, il pourrait être efficace pour seulement une courte période du temps [76].

Néanmoins, de nouveaux modèles de l'adversaire ont été récemment mis en place [77]-[78]. En fait, l'attaqueur peut également être équipé d'une technologie de radio cognitive, et peut s'adapter dynamiquement sa stratégie selon l'environnement dynamique ainsi que la stratégie des utilisateurs secondaires. Nous nous référons à un adversaire comme un brouilleur cognitif: il dispose d'un comportement cognitif typique, c'est-à-dire, l'écoute en temps réel du spectre radio, la caractérisation et l'analyse rapide de l'environnement, la détermination de la meilleure stratégie d'attaque et enfin l'adaptation des paramètres de SDR à la chaîne de communication pour être brouillée.

A titre d'exemple, rappelons-nous l'exemple simple de l'utilisation du spectre de la Figure 3.3. Un adversaire cognitif prêt à ne cibler que les utilisateurs secondaires: doit effectuer une écoute du spectre continu, le saut entre les différentes bandes de fréquences; doit pouvoir faire la distinction entre les communications des utilisateurs primaires et secondaires, et, enfin, doit "précisément" brouiller les communications des utilisateurs secondaires.

3.2. Applications des Brouilleurs

1. **Civil**

- Brouillage d'une station radio.
- Brouillage de l'Internet.
- Brouillage du convoi.
- Brouillage des stations de TV par satellite.

- Brouillages des réseaux de téléphonie mobile.

2. Militaire

- Brouillage des Radars.
- Brouillage des systèmes de communication sans fil.

3.3. Différents modèles d'un brouilleur d'attaque

3.3.1. Brouillage d'impulsions sinusoïdales : Le signal de brouillage sinusoïdal d'impulsion peut être représenté par [7] :

$$\jmath 1 = \sqrt{2\jmath 1_{\mathcal{P}}} \sum_{\mathcal{G}=-\infty}^{\infty} \mathcal{P}_{\jmath 1}\left(t - \mathcal{G}T_{\jmath 1}\right) sin(2.pi.f_{\jmath 1}t + \theta_{\jmath 1}) \quad (1)$$

$$\mathcal{P}_{\jmath 1}(t) = \begin{cases} 1 & 0 \leq t \leq \tau_{\jmath 1} \\ 0 & autre \end{cases}$$

Où, $f_{\jmath 1}$ et $\theta_{\jmath 1}$ sont la fréquence et la phase de l'onde du brouilleur respectivement et $\tau_{\jmath 1}$ est le rapport cyclique.

3.3.2. Brouillage à onde-continue (Continue-Wave : CW) [7] : Dans le brouillage à onde continue, une ou plusieurs tonalités de brouillage sont stratégiquement placées dans le spectre :

$$\jmath 2 = \sum_{l=1}^{\mathcal{C}} \sqrt{2\jmath 2_l}.sin(2.pi.f_{\jmath 2_l}.t + \theta_{\jmath 2_l}) \quad (2)$$

Où, $f_{\jmath 2l}$ et $\theta_{\jmath 2l}$ sont les fréquences et les phases de l'onde du brouilleur respectivement.

3.3.3. **Brouillage de barrage :** Dans le brouillage de barrage, une gamme de fréquence est brouillée en même temps. Son avantage principal est qu'il est capable de bloquer multiples fréquences à la fois avec une puissance suffisante pour diminuer le rapport SNR des récepteurs de l'ennemi [79].

3.3.4. Brouillage spot : La méthode de brouillage la plus populaire est le brouillage Spot, l'attaquant de ce type de brouillage dirige toute sa puissance d'émission sur une seule fréquence de la cible. Il utilise la même modulation et assez de puissance pour remplacer le signal original [79].

3.3.5. **Brouillage Sweep :** Dans le brouillage Sweep, un brouilleur avec une grande puissance déplace rapidement d'une fréquence à une autre. Bien que cette méthode de brouillage a l'avantage de pouvoir brouiller multiples fréquences dans une succession rapide, il ne les affecte pas tous en même temps [79].

3.3.6. Brouillage follower : Ce brouilleur tente de localiser la fréquence à laquelle le saut de fréquence d'émetteur est envoyé, pour identifier le signal comme cible, et de le brouiller à la nouvelle fréquence. Cette forme d'onde de brouillage pourrait être sous la forme de tonalités ou il pourrait moduler les tonalités avec le bruit, par exemple, utilisant la modulation de fréquence (FM). Le brouillage Follower est également aussi appelé brouillage répéteur [80].

3.3.7. Brouillage à bruit étroit : Ce genre de brouillage place toute l'énergie de brouillage dans un seul canal. La bande-passante de cette injection de l'énergie pourrait être la totalité de la largeur du canal ou ce pourrait être seulement la largeur du signal de données [80].

3.3.8. Brouillage à bruit d'une bande-partielle : Ce type brouillage place l'énergie de brouillage du bruit à travers multiples canaux, mais pas tous les canaux du spectre utilisé par les cibles [80]. Ces canaux peuvent ou ne peuvent pas être contigus.

3.4. Conclusion

- Le brouillage restera un problème majeur dans tous les systèmes de communications sans fils.
- Il existe une différence entre un brouillage à stratégie fixée et un brouillage à stratégie cognitive.
- Il existe plusieurs applications pour le brouillage que ce soit dans le domaine civil ou militaire.

- Il existe plusieurs types de brouillages d’attaques pour les différentes couches de la technologie radio.

CHAPITRE 4
STRATEGIES D'ANTIBROUILLAGE DANS LES RADIOS COGNITIVES

Afin d'atténuer les attaques de brouillage intentionnel, plusieurs solutions ont été proposées dans les communications sans fil standard. Les antennes directionnelles ont été proposées comme une solution de la couche physique en vue de réduire efficacement l'interférence provenant des directions n'impliquant pas la position actuelle de l'émetteur. Aussi les techniques d'étalement du spectre (SS) [81] et le saut de fréquence (FH) [82] s'avèrent efficaces contre les attaques de brouillage intentionnel: cependant que l'étalement du spectre rend le signal plus robuste aux interférences en la répartissant sur une large-bande de fréquence, le saut de fréquence réduit la probabilité que la fréquence impliquée dans la communication en cours est ciblée par le brouilleur. Une solution de la couche réseau a été proposée dans [83] impliquant zapping et retraites spatiales. Des techniques de codage réseaux [84, 85] ont été également proposées afin d'atténuer les effets de brouillage dans les réseaux de radios cognitives. Dans [84], les auteurs ont introduit JENNA : un algorithme de brouillage évasif codage-réseau découverte-voisin qui combine un codage de réseau linéaire aléatoire et la découverte de voisin complet pour un réseau de radio cognitive. Les auteurs dans [85] mettent l'accent sur l'attaque de l'utilisateur émulateur primaire (UEP): ils modélisent l'attaque d'UEP et le saut de fréquence comme un jeu à somme nulle entre l'attaquant et les utilisateurs secondaires. L'approche ci-dessus n'est possible que si les statistiques du canal, comme la disponibilité des probabilités, sont connues a priori.

Beaucoup de solutions d'antibrouillage actuel se révèlent efficaces dans les réseaux de radios cognitives seulement pour brouilleurs de stratégie-fixée, qui ont le même comportement hostile tout le temps, mais pas contre les brouilleurs cognitifs. Comme présenté ci-dessus, les brouilleurs cognitifs sont en mesure d'augmenter leur efficacité en combinant la connaissance de la scène de la radio et le réglage des paramètres de communication de leurs radios logiciel restreinte (SDR). Néanmoins, de nouveaux modèles de contre-mesures électroniques ont été introduits récemment. En particulier, dans l'article [86] le brouillage est traité

comme un jeu stochastique entre le brouilleur et les utilisateurs secondaires (les défenseurs). A chaque tour de jeu, les utilisateurs secondaires écoutent le spectre radio et récupère des informations sur l'UP et les brouilleurs cognitifs.

4.1. Nouvelles tendances de contre-mesures électroniques (CME) pour faire face aux attaques de brouillage intentionnel utilisant le problème d'anomalies

L'importance de la détection d'anomalies est de trouver des patrons qui se comportent d'une façon anormale par rapport aux autres patrons de données dans une grande variété de domaines d'application. Par exemple, un modèle de trafic anormal dans un réseau informatique pourrait signifier que l'ordinateur piraté envoie des données sensibles vers une destination non autorisée [87]. Des lectures anormales d'un capteur d'engin spatial pourraient signifier un défaut de certaines composantes de l'engin spatial [88].

La détection d'anomalies dans les données a été étudiée dans la communauté des statistiques dès le 19ème siècle [89]. Au fil du temps, une variété de techniques de détection d'anomalies ont été développées dans plusieurs communautés de recherche. Plusieurs de ces techniques ont été spécialement mis au point pour certains domaines d'application, tandis que d'autres sont plus génériques.

Il existe de nombreux algorithmes de détection d'anomalies proposés dans la littérature. Ils diffèrent selon l'information utilisée pour l'analyse et selon des techniques qui sont utilisées pour détecter les déviations par rapport à un comportement normal.

4.2. Composantes clés associées avec n'importe quelle technique de détection d'anomalies

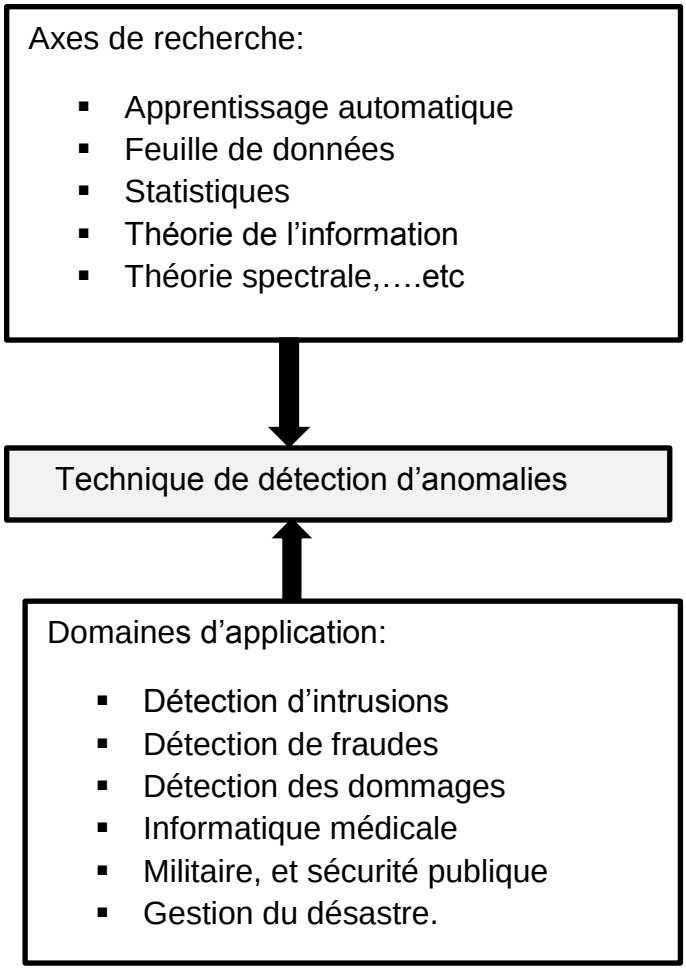


Figure 4.1: Composantes clés associées avec une technique de détection d'anomalies.

4.3. Définition d'une anomalie : Dans la littérature des définitions différentes de la valeur aberrante existent, et chaque auteur a donné une définition aux patrons d'anomalies comme suit: Une valeur aberrante est une observation qui s'écarte largement par rapport aux autres observations et qui a été généré par un mécanisme différent [90]. Une valeur aberrante est une observation qui semble être incompatible avec le reste de l'ensemble des données [91]. Une valeur aberrante est une observation qui se trouve en dehors de la tendance générale d'une distribution [92]. Les valeurs aberrantes sont des données qui ne suivent aucun modèle dans une application [93]. Une valeur aberrante dans un ensemble

de données est une observation ou un point qui est considérablement différent ou incompatible avec le reste de données [94].

4.4. Techniques intelligentes de détection d'anomalies

4.4.1. Techniques de détection d'anomalies basées sur le plus proche voisin ppv

Le concept de l'analyse du plus proche voisin a été utilisé dans plusieurs techniques de détection d'anomalies. Ces techniques sont basées sur l'hypothèse fondamentale suivante:

Hypothèse.1: des instances de données normales se produisent dans des voisins denses, tandis que des anomalies se produisent loin de leurs plus proches voisins [40].

Les techniques de détection d'anomalies basées sur le plus proche voisin nécessitent une mesure de distance ou de similarité définie entre deux instances de données. Une distance (ou similarité) entre deux instances de données peut être calculée de différentes manières. Pour les attributs continus, la distance euclidienne est un choix populaire, mais d'autres mesures peuvent être utilisées [40]. Pour les attributs catégoriques, un coefficient d'adaptation est souvent utilisé, mais des mesures de distance plus complexes peuvent être utilisées. Pour les instances de données multivariées, la distance ou la similarité est habituellement calculée pour chaque attribut, puis combinés. La plupart des techniques de détection n’exigent pas la mesure de distance à être strictement métrique. Les mesures sont généralement nécessaires pour être définies positives et symétriques.

Les techniques de détection d’anomalies basées sur le plus proche voisin peuvent être largement groupées dans deux catégories :

- Des techniques qui utilisent la distance d’une instance de données au son k-ième plus proche voisin comme un score d’anomalie.
- Des techniques qui calculent la densité relative de chaque instance de données pour calculer son score d’anomalie.

4.4.1.1. Avantages et inconvénients des techniques basées sur le plus proche voisin ppv

Les avantages des techniques basées sur le plus proche voisin sont les suivants:

- L'avantage clé des techniques basées sur le plus proche voisin, qu'elles sont non-supervisées dans la nature et ne font pas d'hypothèses concernant la distribution générative pour les données. Au lieu de cela, ils sont purement des données guidées.
- Les techniques semi-supervisées donnent de meilleurs résultats que les techniques non-supervisées en termes d'anomalies manquées.

Les inconvénients des techniques basées sur le plus proche voisin sont les suivants:

- Pour les techniques non-supervisées, si les données ont des instances normales qui n'ont pas assez de proches voisins ou si les données présentes des anomalies qui ont assez de proches voisins, la technique ne parvient pas à les étiqueter correctement, entraînant des anomalies manquées.
- Pour les techniques semi-supervisées, si les instances normales dans les données de test n'ont pas suffisamment d'instances normales similaires dans les données d'entrainement (training data), le taux de faux positif de de ces techniques est élevé.
- La performance d'une technique basée sur le plus proche voisin s'appuie grandement sur une mesure de distance, définie entre une paire d'instances de données, qui peut effectivement distinguer entre les instances normales et anormales. Définition des mesures de distance entre les instances peut être difficile lorsque les données sont complexes, par exemple : graphes, séquences,… etc.

4.4.2. Techniques de détection d'anomalies basées sur le clustering

Le clustering (regroupement) est utilisé pour regrouper des instances de données similaires dans des clusters. Le clustering est essentiellement une technique non-supervisée bien que le clustering semi-supervisé [95] a été

également exploré récemment. Alors même que le clustering et la détection d'anomalies semblent être fondamentalement différents de l'autre, plusieurs techniques de détection d'anomalies basées sur le clustering ont été développées. Les techniques de détection d'anomalies basées sur le clustering peuvent être regroupées en deux catégories.

La première catégorie des techniques basées sur le clustering repose sur l'hypothèse suivante:

Hypothèse.2: les instances de données normales appartiennent à un cluster de données, tandis que les anomalies n'appartiennent pas à aucun cluster [40].

Des techniques basées sur l'hypothèse 2 ci-dessus s'appliquent à un algorithme connu basé sur le clustering de l'ensemble de données et déclare n'importe quelle instance de données qui n'appartient pas à n'importe quel cluster comme anomalie. Plusieurs algorithmes de clustering qui n'obligent pas chaque instance de données d'appartenir à un cluster, comme le clustering DBSCAN (Density-Based Spatial Clustering of Applications with Noise) [96], le clustering SNN [40] peuvent être utilisés. L'inconvénient de ces techniques est qu'elles ne sont pas optimisées pour trouver des anomalies, car l'objectif principal de l'algorithme de clustering fondamental est de trouver des clusters.

La deuxième catégorie des techniques basées sur le clustering repose sur l'hypothèse suivante:

Hypothèse.3: des instances de données normales se trouvent à proximité de leur centre de gravité du cluster le plus proche, tandis que des anomalies sont loin de leur centre de gravité du cluster le plus proche [40].

Des techniques basées sur l'hypothèse 3 ci-dessus consistent en deux étapes. Dans la première étape, les données sont regroupées en utilisant un algorithme de regroupement. Dans la seconde étape, pour chaque instance de données, sa distance par rapport à son centre de gravité du cluster le plus proche est calculé en tant que son score d'anomalie.

Un certain nombre de techniques de détection d'anomalies qui suivent cette approche en deux étapes ont été proposées d'utiliser des algorithmes de

clustering différents. Les auteurs dans [97] ont étudié les cartes auto-organisées SOM (Self-Organizing-Maps), le clustering K-Moyennes, et Espérance-Maximisation (EM) pour regrouper les données d'entraînement et ensuite utiliser les clusters pour classer les données de test. En particulier, SOM a été largement utilisé pour détecter les anomalies dans un mode semi-supervisé dans plusieurs applications telles que la détection d'intrusions, la détection de défaut, et la détection de la fraude. Les auteurs dans [98] proposent une technique qui est robuste aux anomalies dans les données d'entrainement.

Notez que si les anomalies dans les données forment des clusters par eux-mêmes, les techniques discutées ci-dessus ne seront pas en mesure de détecter de telles anomalies. Pour adresser ce problème, la troisième catégorie des techniques basées sur le clustering ont été proposés dans qui comptent sur l'hypothèse suivante:

Hypothèse.4: les instances de données normales appartiennent à des clusters de taille larges et denses, tandis que les anomalies appartiennent à des clusters de petite taille. Les techniques basées sur l'hypothèse ci-dessus déclarent des cas appartenant à des groupes dont la taille et/ou la densité est inférieure à un seuil comme anomalies [40].

4.4.2.1. Avantages et inconvénients des techniques basées sur le clustering

Les avantages des techniques basées sur le clustering sont comme suit:

- Les techniques basées sur le clustering peuvent fonctionner dans un mode non-supervisé. De telles techniques peuvent souvent être adaptées à d'autres types de données complexes par simplement les brancher dans un algorithme de clustering qui peut gérer le type de données particulier.

Les inconvénients des techniques basées sur le clustering sont comme suit:

- La performance des techniques basées sur le clustering est très dépendante de l'efficacité des algorithmes de clustering à capturer une structure de cluster des instances normales.
- Plusieurs techniques basées sur le clustering sont efficaces que lorsque les anomalies ne forment pas des clusters significatifs entre eux.

4.4.3. Techniques de détection d'anomalies basées sur la classification

La classification dans [99] est utilisée pour étudier un modèle (classifieur) à partir d'un ensemble d'instances de données étiquetées (entrainement) et ensuite, classifier une instance de test dans l'une des classes en utilisant le modèle appris (test). Des techniques de détection d'anomalies basées sur la classification fonctionnent dans un mode similaire à deux phases :

- La phase d'entrainement (d'apprentissage) apprend un classifieur en utilisant les données d'entraiment étiquetées disponibles.
- La phase de test classifie un test d'instance comme normal ou anomalie en utilisant le classifieur.

Des techniques de détection d'anomalies basées sur la classification fonctionnent sous l'hypothèse générale suivante :

Hypothèse.5: Un classifieur qui permet de distinguer entre les classes normales et anormales peut être appris dans un espace caractéristique donné [40].

Basé sur les étiquettes disponibles pour la phase d'entrainement, les techniques de détection d'anomalies basées sur la classification peuvent être groupées en deux grandes catégories: les techniques de détection d'anomalies multi-classes et une seule classe.

Des techniques de détection d'anomalies basées sur une classification multi-classes supposent que les données d'entrainement contiennent des instances étiquetées appartenant à de multiples classes normales**.** Ces techniques de détection d'anomalies apprennent à un classifieur de distinguer

chaque classe normale contre le reste des classes. Un test d'instance est considéré comme anomalie s'il n'est pas classé comme normale par l'un des classifieurs. Certaines techniques dans cette sous-catégorie associent un score de confiance avec la prédiction faite par le classifieur. Si aucun des classifieurs n'est confiant en classifiant le test d'instance comme normal, l'instance est déclarée à être une anomalie (voir Figure 4.2(a)).

Des techniques de détection d'anomalies basées sur la classification d'une seule classe supposent que toutes les instances d'entrainement ont une étiquette d'une seule classe. Ces techniques apprennent une limite discriminatoire autour des instances normales en utilisant un algorithme de classification d'une seule classe, par exemple, une seule classe MVS (Machines à vecteurs de support), une seule classe KFD (Kernel Fisher Discriminants**)** [100]. Tout test d'instance qui ne relève pas de la frontière appris est déclaré comme anomalie (voir Figure 4.2(b)).

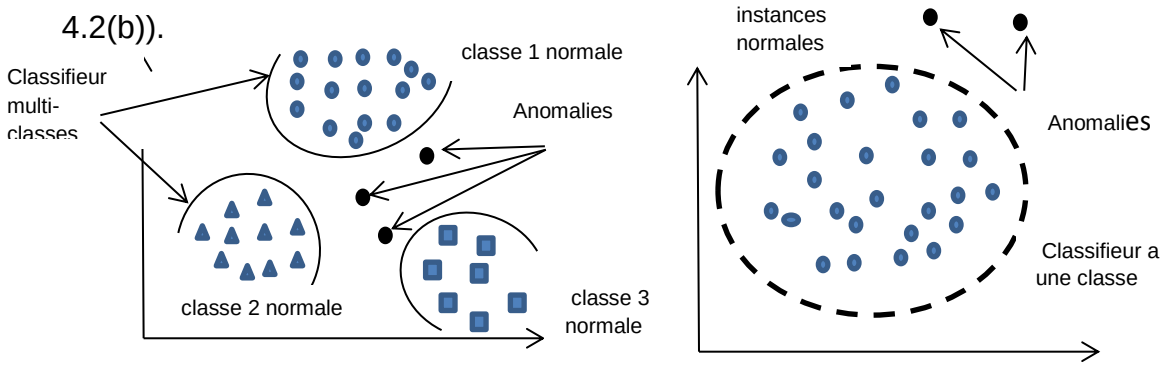


Figure 4.2(a) : Détection d'anomalies multi-classe, Figure 4.2(b) : Détection d'anomalie d'une seule-classe. Figure 4.2: Utilisation de la classification pour la détection d'anomalies.

4.4.3.1. Avantages et inconvénients des techniques basées sur la classification

Avantages des techniques basées sur la classification sont comme suit :

- Les techniques basées sur la classification, en particulier les techniques de classification multi-classe, peuvent utiliser des algorithmes puissants qui peuvent distinguer entre les instances appartenant à des différentes classes.

Les inconvénients des techniques basées sur la classification

- Les techniques basées sur la classification multi-classe s'appuient sur la disponibilité des étiquettes pour diverses classes normales, ce qui est souvent impossible.

4.4.4. Techniques de détection d'anomalies statistiques

Le principe fondamental de n'importe quel technique de détection d'anomalie statistique est: ‘'une anomalie est une observation qui est soupçonnée d'être partiellement ou totalement hors de propos, parce qu'elle n'est pas générée par le modèle stochastique supposé'' [101]. Des techniques de détection d'anomalies statistiques sont basées sur l'hypothèse clé suivante:

Hypothèse.6: des instances de données normales se produisent dans des régions de forte probabilité d'un modèle stochastique, alors que des anomalies se produisent dans des régions de faible probabilité du modèle stochastique [40].

Des techniques statistiques s'adaptent à un modèle statistique (généralement pour un comportement normal) pour des données fournies, puis appliquer un test d'inférence statistique pour déterminer si une instance invisible appartient à ce modèle ou pas. Des instances qui ont une faible probabilité d'être générées à partir du modèle appris, basées sur le test statistique appliqué, sont déclarées comme des anomalies. Les deux techniques paramétriques et non-paramétriques ont été appliquées pour s'adapter à un modèle statistique. Bien que les techniques paramétriques supposent la connaissance de la distribution fondamentale et d'estimer les paramètres à partir des données fournies [102], des techniques non-paramétriques ne supposent généralement pas la connaissance de la distribution fondamentale [103].

4.4.4.1. Avantages et inconvénients des techniques statistiques

Les avantages des techniques statistiques sont:

- Si les hypothèses concernant la distribution fondamentale de données se vérifient, les techniques statistiques fournissent une solution statistiquement justifiable pour la détection d'anomalies.

- Si l’étape d’estimation de la distribution est robuste aux anomalies dans les données, les techniques statistiques peuvent fonctionner dans un cadre non-supervisé sans aucune nécessité de données étiquetées. .

Les inconvénients des techniques statistiques sont:

- L’inconvénient clé des techniques statistiques est qu’elles s’appuient sur l’hypothèse que les données sont générées à partir d’une distribution particulière. Cette hypothèse souvent n’est pas vraie, en particulier pour l’ensemble de données réelles de grande dimension.

4.4.5. Techniques de détection d'anomalies spectrales

Des techniques spectrales essayent de trouver une approximation de données en utilisant une combinaison d'attributs qui captent l'essentiel de la variabilité dans les données. Ces techniques sont basées sur l'hypothèse fondamentale suivante:

Hypothèse.7: des données peuvent être intégrées dans un sous-espace de dimension inférieure dans laquelle les instances normales et les anomalies apparaissent significativement différente [40].

Ainsi, l'approche générale adoptée par les techniques de détection d'anomalies spectrales est de déterminer de tels sous-espaces (projections, etc) dans lequel les instances anomalies peuvent être facilement identifiées [104]. De telles techniques peuvent travailler dans un contexte non-supervisé et semi-supervisé.

Plusieurs techniques utilisent l’Analyse en Composantes Principales (ACP) [105], pour la projection des données dans un espace de dimension inférieure. Une telle technique dans [106] analyse la projection de chaque instance de données le long des composantes principales à faible variance. Une instance normale qui satisfaite de la structure de corrélation des données, aura une faible valeur pour de telles projections; tandis que les instances anomalies qui s’écartent de la structure de corrélation auront une grande valeur. L’article dans [107] adopte cette approche pour détecter les anomalies dans les catalogues d’astronomie [40].

Les auteurs dans [108] présentent une technique de détection d'anomalie où les auteurs effectuent un ACP robuste pour estimer les composantes principales de la matrice de covariance des données d'entrainement normales. La phase de test consiste à comparer chaque point avec les composantes et à attribuer un score d'anomalie sur la base de la distance de points à partir des composantes principales. Ainsi, si la projection de l'observation x sur les composantes principales sont : $y_1, y_2, \dots, y_p$ et les valeurs propres correspondantes sont :$\lambda_1, \lambda_2, \dots, \lambda_p$,

$$\sum_{i=1}^{q} \frac{y_i^2}{\lambda_i} = \frac{y_1^2}{\lambda_1} + \frac{y_2^2}{\lambda_2} + \cdots + \frac{y_q^2}{\lambda_q}; q \leq p, \quad (3)$$

A une distribution chi–carrée. En utilisant ce résultat, les auteurs proposent que, pour un niveau de signification donné, une observation x est une anomalie si

$$\sum_{i=1}^{q} \frac{y_i^2}{\lambda_i} > \chi_q^2(\alpha), \quad (4)$$

On peut montrer que la quantité calculée dans l'équation 3 est égale à la distance de Mahalanobis d'une instance x. La technique basée sur un ACP robuste a été appliquée au domaine de la détection d'intrusions du réseau [108] et pour détecter des anomalies dans l'espace des composants d'artisanat [109].

4.4.5.1. Avantages et inconvénients des techniques spectrales

Les avantages des techniques de détection d'anomalies spectrales sont les suivantes:

- Les techniques spectrales effectuent automatiquement la réduction de la dimensionnalité et donc sont adaptées pour la manipulation d'un ensemble de données de grande dimension. En outre, elles peuvent aussi être utilisées comme une étape de prétraitement suivi par l'application de n'importe quelle technique de détection d'anomalies.
- Les techniques spectrales peuvent être utilisées dans un environnement non-supervisé.

Les inconvénients des techniques de détection d'anomalies spectrales sont comme suit:

- Les techniques spectrales sont utiles que si les instances normales et anormales sont séparables dans une dimension de données inferieur.
- Les techniques spectrales ont généralement une complexité de calcul très élevée.

4.5. Conclusion

Il existe trois types d’antibrouillage ou contremesure électronique (CME) :

- Le premier type c’est d’éviter le problème de brouillage mais cette solution, ce n’est pas possible.
- Le deuxième type c’est de réduire son effet.
- Le troisième type c’est de le détecter, puis de le supprimer.

CHAPITRE 5

DÉTECTION D'ANOAMLIES BASÉE SUR L'ANALYSE COR UTILISANT UN SEUL CLASSIFIEUR ET MULTI-CLASSIFIEUR DANS LES SYSTEMES DE COMMUNICATION SANS FIL

La Caractéristique Opérationnelle du Récepteur (COR) est utilisée pour évaluer et visualiser la performance des classifieurs pour la détection d'anomalies dues à l'effet d'attaques malveillantes. Ce chapitre donne un aperçu de l'analyse de la courbe COR basée sur la détection d'anomalies en utilisant des classifieurs et un guide détaillé pour les utiliser dans la recherche et le développement (R&D). Au cours de ces dernières années l'analyse de la courbe COR a été de plus en plus adoptée dans les milieux de la recherche d'apprentissage automatique (Machine Learning) et de feuilles données (Data Mining). Cette étude donne des définitions de la théorie de la détection d'anomalies et la façon d'utiliser une courbe COR, c'est quoi une courbe COR?, quand on utilise-t-on des courbes COR?. Elle donne des exemples de la façon de construire des courbes COR pour des classifieurs ainsi que la façon de les mesurer et de les comparer tous.

5.1. Théorie de la détection d'anomalies

Supposons que, un seul utilisateur primaire (UP) produit un signal source primaire noté, $r = \{r(t): t \in [0, T]\}$, sur un intervalle de temps d'observation $[0, T]$, les utilisateurs secondaires (USs) reçoivent ce signal primaire par chaque utilisateur radio. On suppose deux hypothèses H_0 et H_1 : l'hypothèse (H_1) : signifie que le signal reçu $r(t)$ peut avoir été produit par la présence du signal de brouillage d'attaque, le signal primaire source, et le bruit ambiant de type blanc gaussien. L'hypothèse (H_0): signifie que la présence du signal source et le bruit uniquement dans le système. Deux possibilités sont appelées pour la détection des observations normales (hypothèse : H_{00}) et la détection des observations d'anomalies (hypothèse : H_{11}), et sont couramment écrites dans la notation compacte: La première hypothèse: H_{00} : événement.1: des observations normales. La seconde hypothèse: H_{11} : événement.2: des observations d'anomalies.

Pour décider entre les deux hypothèses (H_{00}, H_{11}), on peut appliquer un seuil à la sortie du classifieur et prendre une décision que les anomalies sont présentes si est seulement si la valeur de l'observation dépasse la valeur du seuil ou la valeur critique. Les ingénieurs sont alors confrontés à la question pratique de savoir comment fixer la valeur du seuil de façon à veiller à ce que le nombre d'erreurs de décision sont petit. Il existe deux types d'erreurs possibles: l'erreur manquée (c.-à-d. décider H_{00} sous H_{11} (problème d'anomalies est présent)) et l'erreur de fausse alarme (c.-à-d. décider H_{11} sous H_{00} (pas de problème d'anomalies présent)), voir la Figure 5.1 ci-dessous.

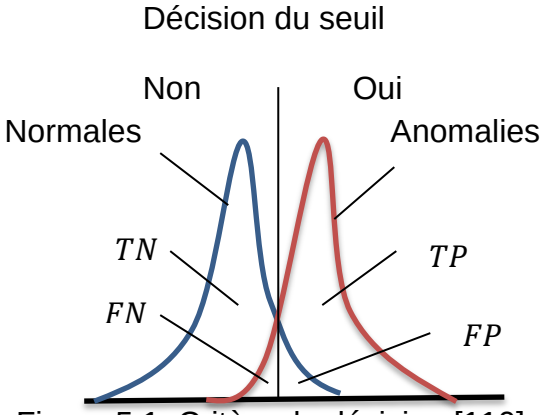


Figure 5.1: Critère de décision [110].

5.2. Performance d'un classifieur

La matrice de confusion: qui montre les prédictions correctes et incorrectes. Il existe quatre sorties pour la classification de chaque instance.

	Evènement	Evènement
Décision	Anomalie	Normale
Oui	TP : Vrais Positifs	FP : Faux Positifs
Non	FN : Faux Négatifs	TN : Vrais Négatifs

Tableau 5.1: Matrice de confusion [111]-[112].

Nous commençons par examiner les problèmes de classification à l'aide seulement de deux classes. Formellement, chaque instance/observation I est mappée par un élément de l'ensemble des étiquettes de classe positive et négative $\{p, n\}$. Un modèle de classification (classifieur) est une cartographie à partir d'instances aux classes prévues. Certains modèles de classification produisent une sortie continue à laquelle différents seuils peuvent être appliqués pour prédire l'appartenance de classe. D'autres modèles produisent une étiquette

de classe discrète indiquant uniquement la classe prédite de l'instance. Pour faire la distinction entre une classe réelle et une classe prédite, nous utilisons les étiquettes $\{\mathbb{Y}, \mathbb{N}\}$ pour les prédictions de classe produites par un modèle.

Compte tenu d'un classifieur et d'une instance/observation, il existe quatre sorties possibles. Si l'instance est positive et classifiée comme positive, elle est comptée comme un vrai positif; si elle est classifiée comme négative, elle est considérée comme un faux négatif. Si l'instance est négative et classifiée comme négative, elle est considérée comme un vrai négatif; si elle est classifiée comme positive, elle est comptée comme un faux positif. Compte tenu d'un classifieur et d'un ensemble d'instances/d'observations (l'ensemble de test), une matrice de confusion de deux par deux peut être construite représentant les dispositions de l'ensemble d'instances. Cette matrice constitue la base de nombreux paramètres communs [112]. TP=Vrais Positifs: une observation anomalie est classifiée correctement comme une observation anomalie, ce qui signifie qu'elle est présente et détectée. FP=Faux Positifs: une observation normale est classifiée comme une observation anomalie, ce qui signifie qu'elle n'est pas présente mais détectée. TN=Vrais Négatifs: une observation normale est classifiée comme une observation normale, ce qui signifie qu'elle n'est pas présente et non détectée. FN=Faux Négatifs: une observation anomalie est classifiée comme une observation normale, ce qui signifie qu'elle est présente mais pas détectée. Le taux de vrais positifs (aussi appelé taux de succès et de rappel) d'un classifieur est estimé par :

$TPR = \frac{TP}{TP+FN}$= positives correctement classifiés sur le totale des positives (5)

Le taux de faux positifs (aussi appelé taux de fausse alarme) d'un classifieur est estimé par:

$FPR = \frac{FP}{FP+TN}$= négatives incorrectement classifiés sur le total des négatives (6)

Le taux de vrais négatifs : $TNR = \frac{TN}{FP+TN}$ (7)

Le taux de faux négatifs : $FNR = \frac{FN}{FN+TP}$ (8)

Des termes additionnels associés de la courbe ROC sont :

$$Sensibilité = rappel = taux\ de\ détection = TPR, \quad (9)$$

$$specificite = \frac{TN}{TN+FP} = 1 - FPR, \quad (10)$$

$$Precision = \frac{TP}{TP+FP} \quad (11)$$

$$Exactitude = \frac{TP+TN}{TP+FN+FP+TN}\ ,\ F - mesure = \frac{2}{{}^{1}/_{precision} + {}^{1}/_{rappel}} \quad (12)$$

Tous les classifieurs, qui sont situés sur la diagonale, ont la même performance. Il est dit qu'ils n'avaient pas l'information sur le problème. Tous les classifieurs, situés au-dessus de la diagonale, sont utiles.

5.3. Espace COR

Les graphes COR sont des graphes à deux dimensions (2d) dans lesquelles le taux de détection d'anomalies (TPR) est tracé sur l'axe des-y et le taux de fausses alarmes (FPR) sur l'axe des-x. La courbe COR représente une relation entre les bénéfices (Vrais Positifs) et les coûts (Faux Positifs). La Figure 5.2: montre la courbe COR avec cinq classifieurs étiquetés de A à E. Un classifieur discret est celui qui fournit en sortie seulement une étiquette de classe. Chaque classifieur discret, produit une paire (FPR, TPR) correspondant à un simple point dans l'espace COR. Les classifieurs dans la Figure 5.2 sont tous des classifieurs discrets. Plusieurs points dans l'espace COR sont importants à noter. Le point inférieur à gauche (0,0) représente la stratégie de ne jamais délivrer un classement positif; un tel classifieur ne commet pas des erreurs fausses positives, mais aussi ne gagne pas de vrais positifs. La stratégie opposée de délivrance inconditionnelle des classifications positives, est représentée par le point en haut à droite (1,1). Le point (0,1) représente une classification parfaite. La performance de D est parfaite comme montre la figure ci-dessous. Un point dans l'espace COR est meilleure qu'un autre s'il est au nord-ouest (le taux d'anomalies est plus élevé, le taux de fausses alarmes est plus faible). Des classifieurs apparaissant sur le côté gauche du graphe COR, près de l'axe des-y, peuvent être considérés comme "Conservateur": ils établissent des classifications positives seulement avec des preuves solides de sorte qu'ils fassent quelques erreurs de fausses positives, mais

ils ont souvent un faible taux de détection d'anomalies. Les classifieurs sur le côté supérieur droit d'un graphe COR peuvent être considérés comme "Libérale": ils établissent des classifications positives avec de faibles preuves afin qu'ils classifient presque tous les positives correctement, mais ils ont souvent un grand taux de fausses alarmes. Dans la Figure 5.2, A est plus conservateur que B. De nombreux domaines du monde réel sont dominées par un grand nombre d'instances négatives, si la performance de l'autre côté de gauche du graphe COR devient plus intéressante [112].

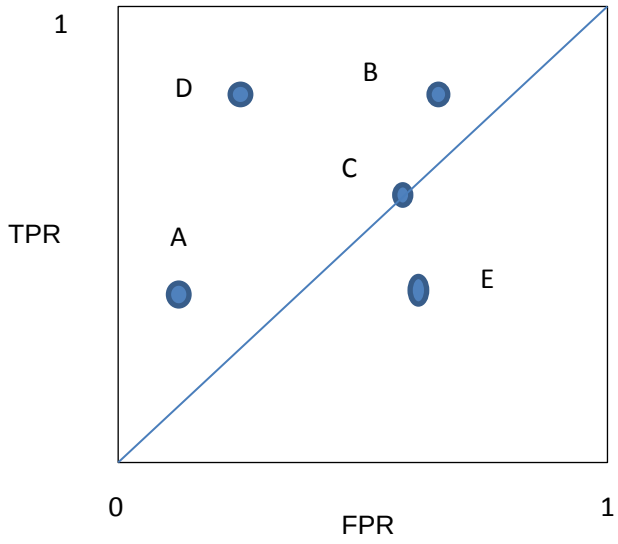


Figure 5.2: Courbe COR avec cinq classifieurs discrets étiquetés de A à E [112].

5.4. Avantages de l'utilisation de l'analyse de la courbe COR : Parmi les avantages de l'analyse de la courbe COR, sont comme suit :

Visualiser l'exactitude du classifieur pour la détection d'anomalies. Faciliter la comparaison de multi-classifieur. Reconnaître l'importance de la valeur du seuil de décision [113].

5.5. Mesures de la courbe COR pour la détection d'anomalies

5.5.1. Mesures de précision

La visualisation de la courbe COR fournit une précision globale d'un classifieur. La nature de la courbe COR est plus raide ce qui signifie que le taux d'observations d'anomalies est plus élevé que le taux d'observations normales. La

nature de la courbe COR est plus plate ce qui signifie que le taux d'observations normales est supérieur que le taux d'observations anormales. On peut voir que la courbe COR se rapproche au point de perfection (0,1) [113].

Les deux points de vue les plus courants de la précision sont : la première mesure non-paramétrique qui n'exige pas une hypothèse pour faire la distribution est le taux de détection d'anomalies à un taux de fausse alarme fixé, également connu sous le critère de Neyman-Pearson, et une autre mesure non-paramétrique de plus en plus renommée, est l'aire sous la courbe (AUC). Le premier est utile lorsque vous avez un taux de fausses alarmes fixées à l'esprit, et la seconde est utile comme une mesure de précision très généralisée.

La mesure AUC est préférable, car elle n'exige pas l'hypothèse de symétrie.

Le critère de Neyman-Pearson: signifie un taux de détection d'anomalies à un taux de fausse alarme fixé.

Les critères de Neyman-Pearson et l'AUC seront expliqués dans les sections ci-dessous.

5.5.1.1. Critère de Neyman-Pearson

L'importance du critère de Neyman-Pearson pour la détection d'anomalies est de maximiser le taux de détection (TPR) à un taux de fausse-alarme (FPR) fixé. Il est possible de voir la figure générale de la courbe COR, et de décider à un taux de fausse alarme fixé. La courbe COR fournit une idée essentielle, si elle est raide dans la région d'intérêt. Avec l'utilisation de la mesure de précision, il est facile de trouver la courbe COR avec un plus grand taux de détection d'anomalies pour un taux de fausse alarme fixé donné [113].

5.5.1.2. Aire sous la courbe COR – AUC

Dans le cas le plus simple, un classifieur à deux classes forme une zone de 4 segments à partir de la courbe COR, voir Figure 5.3, avec le point donné par le classifieur, deux points triviaux (le classifieur qui prédit toujours la classe positive et qui prédit toujours la classe négative) et l'origine du repère (0,0). L'aire de cette zone est appelée "Aire sous la courbe COR ou AUC" ("Area Under the ROC

Curve") et est devenue une meilleure mesure par rapport à l'exactitude (accuracy) ou l'erreur pour évaluer des classifieurs. L'AUC d'un classifieur est équivalente à la probabilité qu'un classifieur donne un meilleur rang à un élément positif par rapport à un élément négatif, tous deux choisis aléatoirement dans la base, ce qui est équivalent au test de Wilcoxon. L'AUC est également très proche du coefficient de Gini, qui correspond à l'aire entre la courbe COR et la diagonale de l'espace. Dans [114], la relation entre AUC et coefficient de Gini a été précisée pour donner.

$$Gini + 1 = 2 \times AUC \tag{13}$$

Soit l'exemple de la Figure 5.3 présentant l'aire sous deux courbes COR. Dans la Figure 5.3a, le classifieur B dispose en moyenne, de l'aire la plus grande donc des meilleures performances. La Figure 5.3b montre l'AUC pour un classifieur binaire, A, et un classifieur de mesure, B. Le classifieur A représenté les performances de B lorsque B est utilisé avec un seuil fixé. Bien que les performances des deux soient égales à un point donné (seuil de A), A est tout de même moins performant pour les autres points [114].

La simplicité d'utilisation et les propriétés de l'AUC font de cette mesure un élément central utilisé par la communauté scientifique comme critère de comparaison des performances des systèmes.

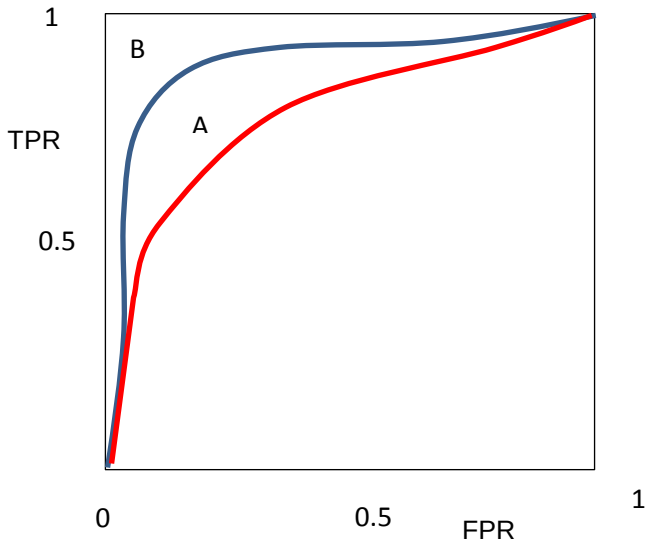


Figure 5.3.a: (a) AUC pour deux courbes.

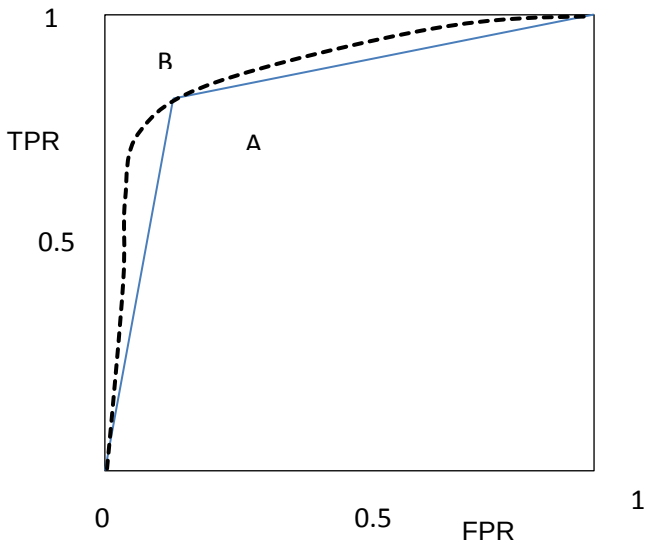


Figure 5.3.b: (b) AUC pour un classifieur discret (A), et un classifieur probabiliste(B).

Figure 5.3: Courbes COR et AUC [115].

4.6. Généralisation de l'analyse COR à des problèmes multi-classes

4.6.1. ROC Multi-classe

Avec plus de deux classes, la situation devient très complexe car l'espace global doit être géré. La matrice de confusion, avec $m > 2$ classes, devient une matrice de dimension $(m \times m)$, dont m classifications correctes et les $(m^2 - m)$ erreurs possibles. Par exemple, pour $m = 3$ classes, on obtient 6 espaces de dimension. Les auteurs de l'article [116] ont montré que l'analyse, derrière la coque convexe de la courbe ROC (ROCCH), s'étend à de multiples classes et des coques convexes multidimensionnelles.

Les auteurs dans [117] et [118] proposent de manipuler m classes en générant m courbes ROC, une pour chaque classe. Sur l'ensemble de toutes les classes, la $i^{th}(i \in \{1, \ldots, m\})$ courbe COR correspond à l'évaluation des performances utilisant la classe b_i comme classe positive et toutes les autres classes comme négatives, noté $\mathbb{N}_i$:

$$\mathbb{P}_i = b_i \tag{14}$$

$$\mathbb{N}_i = \bigcup_{j \neq i} b_j \in \mathbb{B}$$

Avec $i, j \in \{1,2, \dots, m\}$ et $\mathbb{B}$ est l'ensemble de toutes les classes.

Le coût de mauvaise classification est, pour cette approche, fixé pour chaque classe car on ne cherche pas à différencier les erreurs. Dans ces conditions, l'espace d'évaluation des performances est à m dimensions, ce qui revient à n'utiliser que les éléments de la diagonale principale de la matrice de confusion. Par exemple, pour trois classes $(m = 3)$, nous obtenons un espace à trois dimensions facilement représentable [112].

A présent, nous allons nous positionner dans un contexte de comparaison des performances de classifieurs. Nous devons pour cela comparer deux hyper-plans. Le problème est que, selon les zones de l'espace, les performances des classifieurs peuvent varier. On peut avoir sur une zone un hyper-plan qui est meilleur qu'un autre et sur une autre zone le second hyper-plan qui est meilleur que le premier. C'est pour cela que, dans la littérature lorsque l'on souhaite comparer différents systèmes de classifications, on réduit les hyper-plans à des valeurs scalaires. Dans le cas général, la valeur scalaire, qui est utilisée pour caractériser les performances COR multi-classes, est le volume sous l'hyper-surface COR, "Volume Under the ROC hyper-Surface, VUS".

5.6.2. AUC Multi-classe

L'aire sous la courbe (AUC) est une mesure de la discriminabilité d'une paire de classes. Dans un problème à deux classes, l'AUC est une simple valeur scalaire, mais un problème multi-classes introduit la question de combiner multiples valeurs de discriminabilité [119].

Une méthode pour calculer les AUCs multi-classes a été prise par les auteurs dans [117], dans leur travail sur l'arbre de probabilité d'estimation. Ils ont calculé les AUCs pour des problèmes multi-classes en générant chaque classe de référence de la courbe COR à son tour, et en mesurant l'aire sous la courbe, puis en additionnant les pondérés des AUCs par la prévalence de de classe de référence dans les données. Plus précisément, ils définissent

$$AUC_{global} = \sum_{b_i \in \mathbb{B}} AUC(b_i)\,(p_i) \quad (15)$$

Où $AUC(b_i)$ est l'aire sous la courbe COR de référence de classe pour : b_i, comme dans l'équation ci-dessus. Cette définition exige seulement les calculs : $|\mathbb{B}|\ AUC$, si sa complexité globale est $O(|\mathbb{B}|mlogm)$.

L'avantage de la formulation AUC de Provost et Domingos's est que AUC_{global} est généré directement à partir des courbes COR de référence de classe, et ces courbes peuvent être générées et visualisées facilement. L'inconvénient est que la courbe COR de la référence de classe est sensible à la distribution de classe et aux coûts d'erreur, si cette formulation de AUC_{global} est aussi bonne.

Les auteurs dans [119] prennent une technique différente dans leur dérivation d'une généralisation multi-classes de l'aire sous la courbe. Ils voulaient une mesure qui soit insensible à la distribution de classe et aux coûts d'erreur. La dérivation est trop détaillée, mais elle est basée sur le fait que l'aire sous la courbe (AUC) est équivalente à la probabilité que le classifieur classera une instance/observation positive choisie, au hasard, supérieure par rapport à une instance négative choisie au hasard. De cette forme probabiliste, elle dérive une formulation qui mesure la discriminabilité paire non pondérée de classes. Leur mesure est donnée par $\mathbb{M}$, et équivalente à:

$$AUC_{global} = \frac{2}{|\mathbb{B}|(|\mathbb{B}|-1)} \sum_{(b_i,b_j) \in C} AUC(b_i, b_j) \quad (16)$$

Où m est le nombre de classes et $AUC(b_i, b_j)$ est l'aire sous la courbe COR à deux classes impliquant des classes b_i et b_j. La somme est calculée sur toutes les paires de classes distinctes. Il y a $\frac{2}{|\mathbb{B}|(|\mathbb{B}|-1)}$ paires, de sorte que la complexité en temps de leur mesure soit $O(|\mathbb{B}|^2 mlogm)$. Alors que les formules de Hand et Tills sont bien décrites et sont insensibles aux changements dans la répartition des classes, il n'existe aucun moyen facile de visualiser la surface dont la superficie est calculée [112].

5.7. Comparaison de multi-classifieur utilisant CCCOR pour la détection d'anomalies

Quand de multiples classifieurs sont employés sur le même ensemble de données, on peut tracer leurs courbes COR sur la même figure. Ceci facilite les conclusions au sujet de la dominance.

5.7.1. Dominance de la courbe COR

Dans la Figure 5.4, on remarque que la courbe ''A'' domine complètement les courbes B, C, D, et E; cela signifie que le classifieur ''A'' a dépassé les autres classifieurs B, C, D, et E. Les courbes A, B, C, et D dominent sur une région sélectionnée de la courbe COR [113].

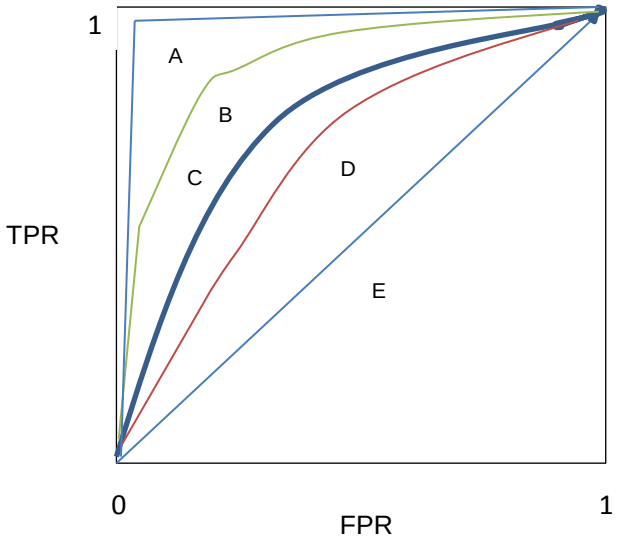


Figure 5.4: Courbes COR avec différentes valeurs d'AUC.

5.7.2. Coque Convexe de la courbe COR (CCCOR)

La courbe CCCOR montre la meilleure performance possible d'un ensemble de classifieurs, si on prend le maximum de précision de chaque classifieur et interpoler entre les différents classifieurs chaque fois que nécessaire pour corriger toutes les coques. La ligne droite joignant deux ou plusieurs classifieurs est une interpolation. Les points (0,0) et (1,1) peuvent également être utilisés dans la construction de CCCOR. S'il y a beaucoup de courbes ROC, la meilleure méthode pour les comparer est de construire la courbe CCCOR et de voir quelles courbes dominent sur quelles régions de la figure. On peut utiliser la

CCCOR pour guider la construction d'un classifieur hybride par rapport à un seul classifieur

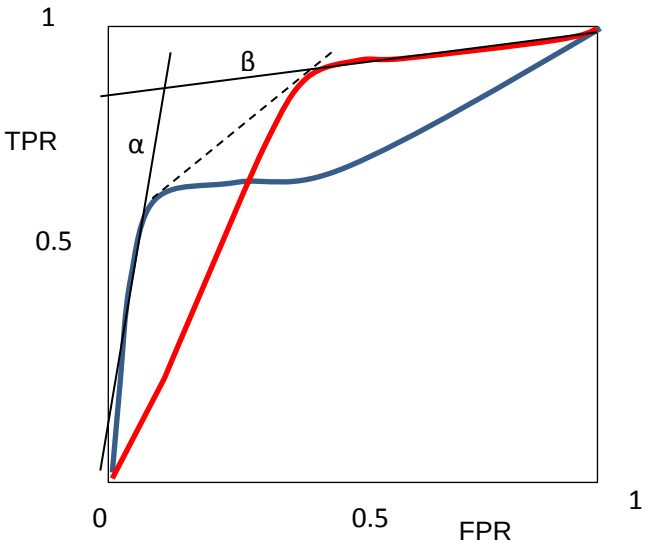


Figure 5.5: Lignes α et β montrent un classifieur optimal sous différentes conditions [115].

Si on vise à couvrir juste 40% des vrais positifs, on doit choisir la méthode A, ce qui donne un taux de faux positifs de 5%. Si on vise à couvrir 70% de vrais positifs, on doit choisir la méthode B, ce qui donne un taux de faux positifs de 30%. Si on vise à couvrir 60% de vrais positifs, alors on doit combiner A et B.

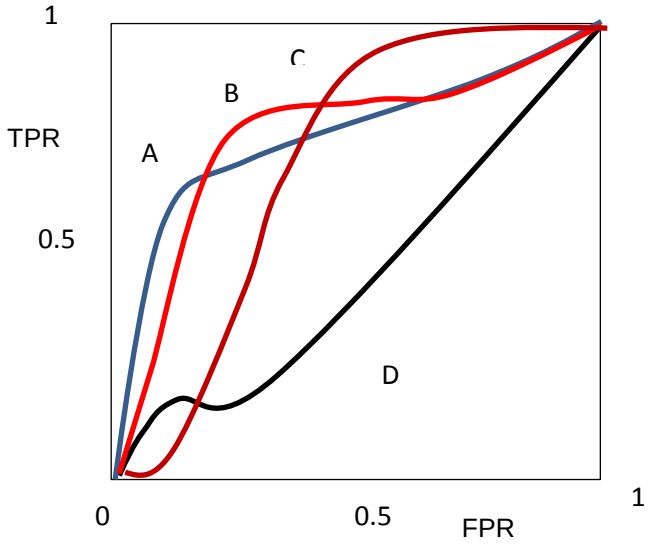


Figure 5.6: Coque convexe de la courbe COR identifie des classifieurs optimaux [115].

5.8. Combiner les classifieurs

La combinaison de classifieurs est une excellente alternative à l'utilisation d'un unique classifieur et est devenue au fil du temps un domaine de recherche très riche. Les techniques de sélection et de combinaison de classifieurs montrent leur intérêt ainsi que leurs performances dans de nombreuses applications, telles que la reconnaissance de patrons d'anomalies, par rapport à l'utilisation d'un seul classifieur. Une multitude de recherches sont menées dans ce domaine d'après les auteurs dans [120].

5.8.1. Techniques de combinaison de classifieurs

La multiplication des travaux sur la combinaison a entraîné la mise au point de nombreux schémas traitant les données de manières différentes. Quatre approches pour la combinaison de classifieurs peuvent être envisagées : parallèle, séquentielle, conditionnelle, et hybride. Mais, malgré la diversité des schémas de combinaison, la détermination de la meilleure organisation reste un problème ouvert? [120].

5.9. Points culminants et Informations sur l'analyse de la courbe COR

L'analyse de la courbe COR est un domaine de recherche vaste en intelligence artificielle et reste un domaine très intéressant. Il commence à apparaître dans les années cinquante dans de nombreuses applications telles que: les statistiques, pour la classification, l'estimation, et pour calculer les mesures du graphe COR. L'analyse COR a continué le progrès. Dans la littérature, de nombreux livres [121]-[122]-[123]-[124] ont écrit sur la courbe COR. Chacun de ces livres fournit une introduction complète à la théorie de la détection, y compris l'utilisation de la courbe COR.

Le graphe COR a été défini lors de la Seconde Guerre Mondiale pour aider à la détection pour identifier les navires et les avions d'ennemis sur un radar. On va développer l'analyse COR dans la guerre électronique utilisant la théorie de détection d'anomalies dans la présence de brouilleurs cognitifs d'attaques et les brouilleurs de stratégie-fixée.

5.10. Conclusion

Ce chapitre a introduit la forme et le sens de l'analyse de la courbe COR, et une étude sur la détection d'anomalies en utilisant des techniques d'apprentissage automatique comme un seul classifieur ou multi-classifieur.

L'analyse de la courbe COR permet de visualiser et comparer la performance d'un seul ou multi-classifieur.

Les avantages de l'analyse de la courbe COR :

- Peut aider à définir une valeur de seuil ou de critique de décision idéale.
- Peut aider à évaluer le taux global d'erreurs et le coût global de détection.
- Peut aider à construire une meilleure précision en utilisant la collaboration de multi-classifieur pour la détection d'anomalies.
- Peut aider à visualiser la précision d'un simple classifieur ou de multi-classifieur pour la détection d'anomalies.
- Peut aider à résumer la précision globale des classifieurs individuels.

Il peut être utilisé pour montrer la détection d'anomalies en utilisant un seul classifieur ou multi-classifieur.

L'analyse de la courbe COR peut comparer multi-classifieur pour la détection d'anomalies en utilisant le même test de données d'apprentissage. Ce chapitre recommande d'utiliser la courbe AUC comme une mesure unique à plus de précision lors d'évaluation et la comparaison d'un ensemble de classifieurs. La méthode de la coque convexe de la courbe COR (CCCOR) est une solution efficace et robuste au problème de la comparaison de plusieurs classifieurs dans des environnements imprécis et changeants.

CHAPITRE 6

ÉCHANTILLONNAGE DU SPECTRE COMPRESSIF COOPÉRATIF LARGE-BANDE CENTRALISÉ DES RADIOS COGNITIVES UTILISANT DES TECHNIQUES INTELLIGENTES POUR LA DÉTECTION D'ANOMALIES

L'Échantillonnage compressif (EC) est une nouvelle technique dans le traitement du signal de l'information. L'EC propose un nouveau schéma d'écoute du spectre à large-bande dans la radio cognitive. Ce projet de recherche présente un nouveau schéma de détection coopérative, basé sur des techniques intelligentes combinées avec la technique d'échantillonnage compressif appliquée pour chaque récepteur radio dans un mode de coopération centralisé. Les mesures compressées obtenues sont collectées à partir des convertisseurs CAIs pour chaque radio intelligente. Une fois le centre de fusion obtient suffisamment de mesures compressées de chaque radio, des techniques intelligentes de détection sont ensuite utilisées pour prendre une décision sur la présence de problème d'anomalies ou non basées sur la valeur du seuil défini.

6.1. Modèle du système et du signal

On propose un schéma de coopération centralisé large-bande où les utilisateurs radio envoient leurs mesures compressées au centre de fusion. Dans les canaux radio entre l'utilisateur primaire et les utilisateurs secondaires (radios), on évalue les multi-trajets et les obstacles avec une distribution de Rayleigh. De même, on n'estime que les canaux radio parfaits entre les utilisateurs secondaires et le centre de fusion.

Le signal source reçu en temps continu par chaque utilisateur radio corrompu par la présence du bruit blanc gaussien. Etant donné l'hypothèse suivante H_0:

$$r_\ell(t)|H_0 = \sum_{\mathbb{i}=1}^{\mathcal{A}} h_{\mathbb{i}\ell} s_{\mathbb{i}}(t) + v_\ell(t) \qquad (17)$$

Le signal source sparse reçu en temps continu par chaque récepteur radio corrompu par la présence du bruit blanc gaussien et des signaux de brouillage d'attaque, compte tenu de l'hypothèse suivante H_1:

$$r_\ell(t)|H_1 = \sum_{\mathbb{i}=1}^{\mathcal{A}} h_{\mathbb{i}\ell} s_{\mathbb{i}\ell}(t) + \sum_{\mathbb{j}=1}^{\mathcal{B}} h'_{\mathbb{j}\ell} \jmath_{\mathbb{j}\ell}(t) + v_\ell(t) \quad (18)$$

$s_{\mathbb{i}\ell}(t)$: les signaux source dans le domaine de base, $v_\ell(t)$: est le bruit gaussien ; $\jmath_{\mathbb{j}\ell}$: les signaux de brouillages d'attaques intentionnels, $h_{\mathbb{i}\ell}$: les canaux radio entre les utilisateurs primaires (UPs) et les utilisateurs secondaires (USs) , $h'_{\mathbb{j}\ell}$: les canaux radio entre les utilisateur brouilleurs (UJs) et les USs. $r_\ell \in R^N$: est le signal reçu par chaque récepteur radio.

Dans cette étape, on évalue un simple utilisateur radio cognitive qui échantillonne un signal reçu à un taux inférieur au taux de Nyquist utilisant le théorème d'échantillonnage sous-Nyquist et on va généraliser cette technique dans le cas d'un régime coopératif. Chaque simple radio cognitive observe $r(t)$ en large-bande avec une large bande-passante et envoie ses mesures compressées au centre de fusion pour la détection d'anomalies sans passer par l'étape de récupération du signal désiré pour éviter la complexité du calcul. Alors que, chaque simple utilisateur radio cognitive peut observer le signal reçu r par compression avec un taux très petit par rapport au taux d'échantillonnage de Nyquist utilisant l'échantillonnage compressif tels que:

$$y = \Phi r + v \quad (19)$$

$y \in R^{\mathbb{K}}$: mesures/observations compressées obtenues sous forme d'une matrice obtenue par la collaboration de tous les utilisateurs P radios cognitives, Φ est la matrice d'écoute.

Chaque simple RC donne des mesures compressées en utilisant l'échantillonnage compressif et toutes ces mesures sont collectées sous forme d'une matrice, appelée matrice d'observations ou matrice de patrons représentée par (y) par la collaboration de P radios tel que décrit ci-dessous dans l'équation (20).

$$y = \begin{vmatrix} y_{1,1} & \cdots & y_{1,\mathbb{K}} \\ \vdots & \ddots & \vdots \\ y_{P,1} & \cdots & y_{P,\mathbb{K}} \end{vmatrix}_{(P\times\mathbb{K})} \quad (20)$$

$\mathbb{K}$*:* est le nombre minimum d'observations.

P : est le nombre de radios/utilisateurs secondaires.

Toutes les radios cognitives employées peuvent utiliser la même matrice d'écoute Φ ou bien différentes matrices. La matrice Φ de dimension $\mathbb{K} \times N$ est appliquée par chaque utilisateur radio cognitive et elle a la représentation sparse suivante [125].

$$\Phi \sim \begin{vmatrix} 1 & 0 & 0 & & 0 & 0 & 0 \\ 0 & 0 & 0 & \ldots & 1 & 0 & 0 \\ 0 & 0 & 1 & & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \ldots & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & & 0 & 0 & 1 \end{vmatrix}_{(\mathbb{K}\times N)} \quad (21)$$

N: est le nombre nécessaire de points qui peuvent représenter le signal source primaire dans le domaine de base.

6.2.Coopération large-bande de radios cognitives utilisant l'échantillonnage compressif

6.2.1. Échantillonnage compressif pour un seul utilisateur radio cognitive

6.2.1.1. Signal sparse

Un signal est appelé sparse quand il est représenté par un petit nombre de coefficients non-nuls dans tous les domaines de la pratique. Plus précisément, un signal r d'une dimension $N \times 1$ est appelé $S - sparse$ si r est représenté par la multiplication d'une matrice de transformations de base Ψ de dimension $N \times N$ et un vecteur $N \times 1$ de coefficient $s,$ et s a uniquement S coefficients non-nuls. La définition de ''sparsity'' n'est pas limitée au domaine de transformation orthogonal (par exemple: transformée en ondelettes ou transformée de Fourier). Si un signal est représenté dans un domaine non-orthogonale, y compris n'importe quelle application définie par l'utilisateur, le signal est également appelé sparse [126].

6.2.1.2. Processus de mesures

Considérons un signal à temps discret r, de longueur fini, unidimensionnel, qui peut être considéré comme un vecteur colonne d'une dimension $N \times 1$ dans R^N avec des éléments $r[t]$, $t = 1, 2, \ldots, N$. Tout signal dans R^N peut être représenté en termes de base de $N \times 1$ vecteurs de coefficients $\{\psi_i\}_{i=1}^{N}$. Pour simplifier, on suppose que la base est orthonormée. En utilisant une matrice de base Ψ $(N \times N)$ [17] :

$$\Psi = \langle \psi_1 | \psi_2 | \ldots\ldots\ldots \psi_N \rangle \tag{22}$$

On suppose, la présence d'un seul utilisateur primaire (UP1) et la présence de deux utilisateurs brouilleurs (UJ1, UJ2).

On veut d'abord expliquer un schéma d'écoute coopérative large-bande basé sur les principes de l'EC via la collaboration. Le signal analogique large-bande $r(t), 0 \leq t \leq T$, $r \in R^N$, est représenté comme une somme finie de fonctions de base $\psi_i(t)$ tel que décrit ci-dessous.

$$r(t) = \sum_{i=1}^{N} s_i \psi_i(t),\ t = 1, \ldots, N; \tag{23}$$

Lorsque quelques coefficients s_i sont très larges que zéro en raison de la compressibilité de $r(t)$. Spécialement, avec un temps discret d'échantillonnage compressif, nous considérons un vecteur d'une dimension $N \times 1$ alors $r = \Psi s$, où Ψ [16] est la matrice de base d'une dimension $N \times N$ et s un vecteur de $N \times 1$ avec $S < \mathbb{K} \ll N$, ce qui signifie que $S - sparse$ est le nombre de coefficients non-nuls s_i. Il a été démontré que r peut être récupéré en utilisant $\mathbb{K} = SO(logN)$ vecteurs de projection linéaire non-adaptatifs sur $\Phi \in R^{\mathbb{K} \times N}$ qui est incohérente avec la matrice $\Psi \in R^{N \times N}$.

Considérons que nous tenons à reconstruire toutes les N coefficients de r, à partir d'échantillons compressées y_j sur r tel que démontré ci-dessous

$$y_j = \langle r, \phi_j \rangle = \sum_{i=1}^{N} \phi_{ji} r(i),\ j = 1, \ldots, \mathbb{K}; \tag{24}$$

Hypothèse (H_0) (signifie l'absence des signaux de brouillage d'attaque)

$$y|H_0 = \Phi r = \Phi\Psi s = \Theta s \tag{25}$$

Hypothèse (H_1) (signifie la présence des signaux de brouillage)

$$y|H_1 = \Phi r = \Phi\Psi(s + j_1 + j_2) = \Theta(s + j_1 + j_2) \quad (26)$$

Où nous sommes intéressés dans le cas où $\mathbb{K} \ll N$ et les lignes de la matrice Φ sont incohérentes avec les colonnes de la matrice Ψ. Ensuite, il est montré que le signal sparse r reçu peut être récupéré avec précision en présence du bruit blanc gaussien. Nous considérons que le signal récupéré $\tilde{r}$ est donné par $\tilde{r} = \Psi\tilde{s}$.

L'étape de récupération est obtenue en résolvant le problème d'optimisation $l1$-norm.

$$\tilde{s} = arg\ min\|s\|_{l1} \qquad \text{s.t} \quad y = \Phi\Psi s = \Theta s \quad (27)$$

Des algorithmes de Greedy linéaires [127], [128], comme BP (Basis Pursuit) ou des algorithmes de Greedy itératives peuvent être utilisés pour résoudre (25).

En cas de mesures bruitées, $y = \Phi r + v$, où v est le bruit avec $\|v\|_{l2} \leq \epsilon$, montre que la solution de

$$arg\ min\|s\|_{l1} \ \text{ s.t } \ \|\Theta s - y\|_{l2} \leq \epsilon, \Theta \in R^{\mathbb{K}\times N} \text{ , [129]} \quad (28)$$

Chaque utilisateur radio transmet les mesures compressées dans le centre de fusion. Dans le centre de fusion, les observations compressées de chaque utilisateur radio sont collectées sous forme d'une matrice appelée matrice d'observations d'une dimension $y(P \times \mathbb{K})$ qui est considérée comme l'entrée du détecteur intelligent pour savoir s'il y a un problème d'anomalies ou pas.

Notre objectif principal est de détecter des anomalies en utilisant des détecteurs intelligents directement après l'échantillonnage compressif sans passer par la récupération en utilisant des échantillons compressées en présence du bruit et des signaux de brouillage. Pour cette raison, nous devons trouver la matrice de patrons qui est considérée comme une entrée des techniques intelligentes de détection. Ces techniques utilisent les mesures compressées du signal observé par chaque utilisateur radio pour détecter la présence d'anomalies dans le spectre observé.

Où, $\Theta = \Phi\Psi$ est une matrice d'échantillonnage d'une dimension $\mathbb{K} \times N$. Il convient de noter que le processus de mesure est non-adaptatif, c'est-à-dire, Φ ne dépend en aucune façon du signal r. La Figure 6.1, comme indiquée ci-dessous, peut expliquer les deux équations 25 et 26, en proposant les deux hypothèses comme illustré ci-dessus.

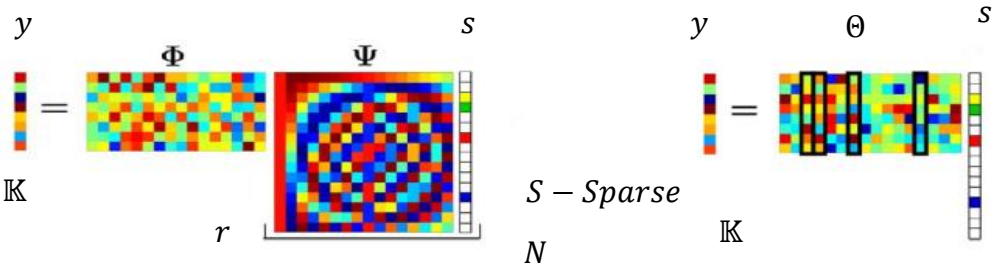


Figure 6.1: Processus de mesure d'échantillonnage compressif pour la reconstruction du signal sparse [126].

Il y a deux étapes principales. La première étape: une matrice d'écoute stable est conçue pour s'assurer que l'information ne soit pas endommagée par la réduction de la dimensionnalité $r \in C^N$ bas pour $y \in C^{\mathbb{K}}$. Dans la deuxième étape: des détecteurs intelligents, pour la détection d'anomalies, basés sur la valeur du seuil sont proposés dans ce travail de recherche.

6.3. Modèle du convertisseur analogique-information

6.3.1. Convertisseur analogique-information en cas d'un seul utilisateur

Radio

Le schéma ci-dessous représente le modèle d'un Convertisseur Analogique-Information pour chaque utilisateur radio.

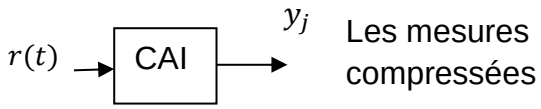


Figure 6.2: Modèle du convertisseur CAI. L'opérateur Φ prend des mesures linéaires du signal analogique large-bande $r(t)$ pour créer les mesures compressées y_j.

L’échantillonnage compressif a mis l'accent sur des signaux de longueur finie et à temps discret. Ainsi, les technologies innovantes sont nécessaires pour élargir l’échantillonnage compressif pour les signaux en temps continu qui implémente l’échantillonnage compressif dans le domaine analogique. Pour réaliser l’échantillonnage compressif analogique, Sami Kirolos, dans [29] a proposé un modèle du convertisseur CAI via un démodulateur aléatoire (DA). Comme le montre la Figure 6.3, le modèle basé sur un convertisseur CAI consiste en un générateur d’un nombre pseudo-aléatoire (GNPA) d’une séquence (±1), ce qu’on appelle la séquence de chipping notée $p_c(t)$, un mixeur, un accumulateur, et un sous-échantillonneur de sous-Nyquist. Le générateur d’un nombre pseudo-aléatoire produit une séquence en temps discret qui démodule le signal $r(t)$ par un mixeur. Le filtre est utilisé pour résumer le signal démodulé pour T_s secondes, tandis que son signal de sortie est échantillonné utilisant un faible taux d'échantillonnage. Après cela, le problème d'anomalies peut être détecté directement à partir des mesures compressées par la collaboration sans passer pour récupérer le signal sparse corrompu par la présence des signaux de brouillage intentionnel, et le bruit blanc gaussien additif.

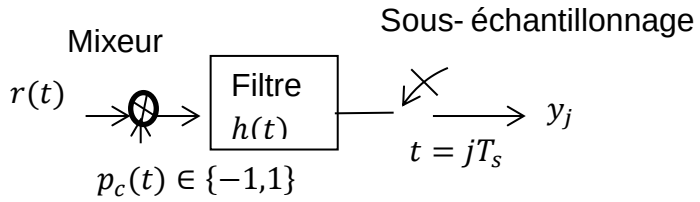


Figure 6.3: Convertisseur CAI via un DA pour chaque utilisateur radio cognitive [29].

6.3.2. Modèle d’un convertisseur CAI dans le cas de coopération de radios

Dans un schéma d’écoute coopérative, multiples canaux d’échantillonnage compressif, avec l'accumulateur dans chaque canal remplacé par un filtre passe bas anti-aliasing (FPB). Le principal avantage est d'introduire le convertisseur CAI en parallèle via la coopération comme le montre la Figure 6.4.

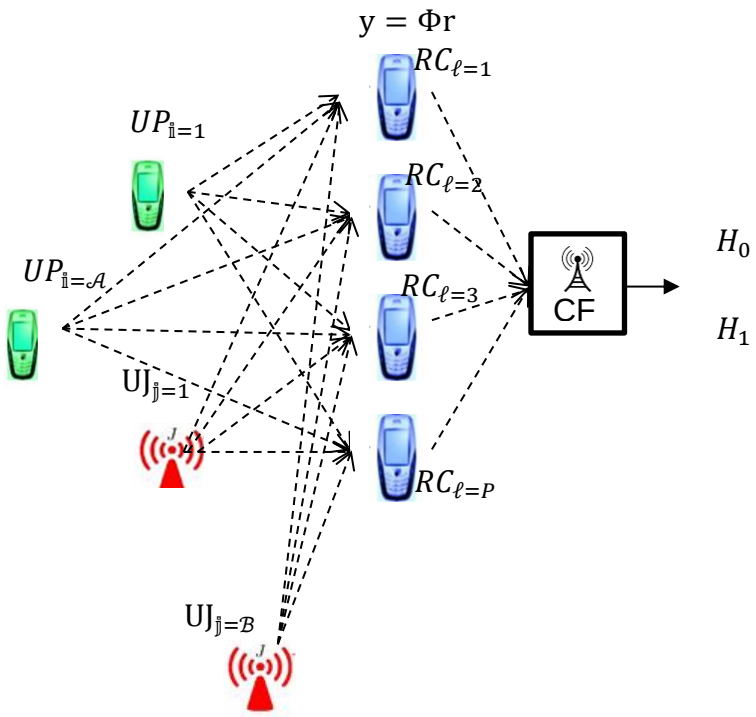


Figure 6.4: Coopération centralisée large-bande de radios en présence des signaux de brouillages, de bruit blanc gaussien additif, et des signaux primaires.

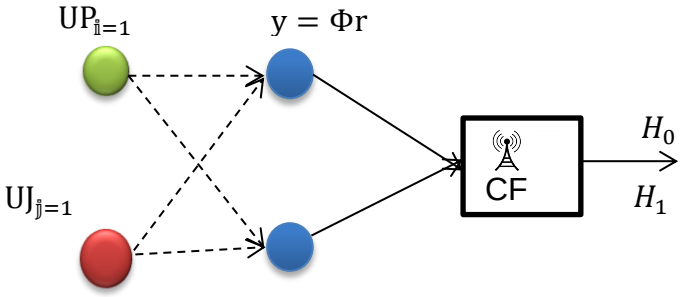


Figure 6.5: Coopération centralisée large-bande d'échantillonnage compressif du spectre des radios pour la détection dans le centre de fusion utilisant le regroupement $\mathcal{K}$ −moyennes bi-variable.

6.4. Détection coopérative centralisée large-bande dans le centre de fusion utilisant des techniques intelligentes

6.4.1. Technique d'échantillonnage compressif coopérative combinée avec la méthode de clustering $\mathcal{K}$ −moyennes pour la détection de la présence du signal d'attaque dans le spectre

Le clustering (regroupement) est une méthode utilisée pour trouver des similarités de groupes (clusters) dans les observations de données. Cet algorithme de regroupement est un processus itératif et nécessite un certain nombre de groupes $\mathcal{K}$. Il regroupe des observations de données qui sont à proximité de toutes les autres dans un groupe et des observations de données qui sont différentes les unes des autres dans des groupes différents. La technique de clustering $\mathcal{K}$ −moyennes partitionne les observations dans $\mathcal{K}$ groupes identifiés par leurs centres de gravité basés sur la distance mesurée entre les observations du vecteur de mesures et le centre du groupe.

$$y \in G_{\mathrm{i}}, \quad if \qquad d(y, G_{\mathrm{i}}) < d\big(y, G_{\mathrm{j}}\big), \quad \forall \mathrm{i} = 1, \dots \mathcal{K}, \mathrm{i} \neq \mathrm{j} \tag{29}$$

Le clustering est toujours appelé une technique d'apprentissage automatique non-supervisé [130]. Il est l'un des techniques de fouille de données (data mining) les plus fréquemment utilisées et il est utilisé dans de nombreuses applications telles que: la science du traitement d'imagerie médicale, la psychologie, l'astronomie, la biologie, etc. Le clustering $\mathcal{K}$ −moyennes dans [131], est sensible à un comportement anormal d'observations. Les observations anormales sont des observations qui ont un comportement anormal par rapport aux autres observations de données dans le spectre. Les observations anormales peuvent être des erreurs causées entre les bandes de radio fréquences à cause des effets de la présence de brouillage d'attaque et le bruit blanc gaussien. La Figure 6.6 ci-dessous explique toutes les étapes de l'algorithme de regroupement $\mathcal{K}$ −moyennes.

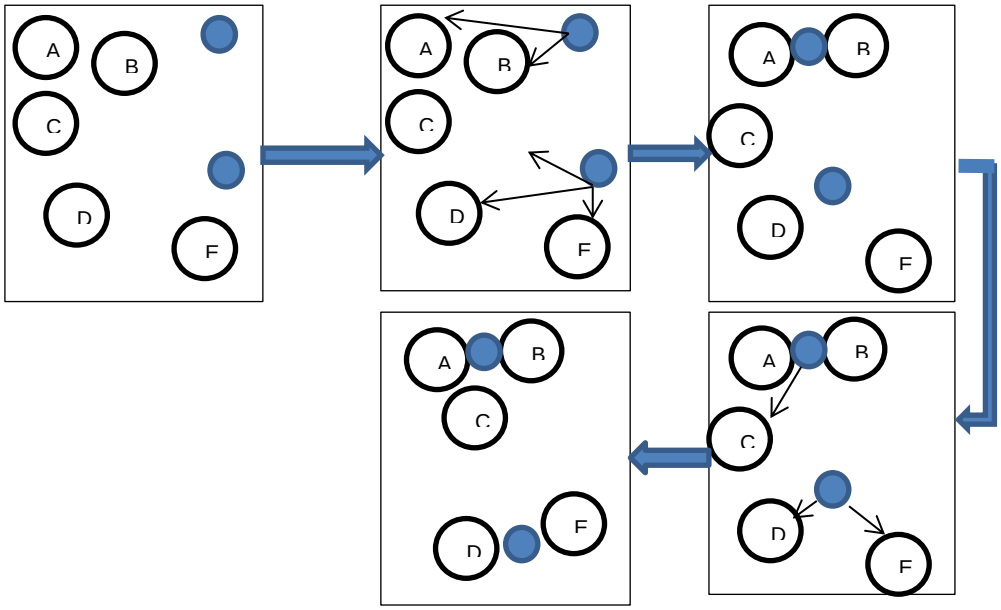


Figure 6.6: Regroupement $\mathcal{K}$ −moyennes.

6.4.1.1. Détection d'un comportement anormale dans le spectre en utilisant le clusteirng $\mathcal{K}$ −moyennes rapide et efficace

La détection du comportement anormal dans le spectre se réfère au problème de découvrir des observations qui ne sont pas conformes à un comportement prévu par rapport aux autres observations de données normales. La détection du comportement anormal est basée sur une technique de regroupement k-moyennes en se basant sur les deux hypothèses expliquées dans ce travail. L'algorithme ci-dessous explique toutes les étapes à suivre.

6.4.1.2. Algorithme de clustering $\mathcal{K}$ −moyennes pour la détection

Entrée: Une matrice d'observations d'une dimension : $y\ (P \times \mathbb{K})$, le nombre de groupe: $\mathcal{K}$, et le seuil de convergence ε par défaut.

Sortie: Un groupe de $\mathcal{K}$ clusters, $G = \{G_i, i = 1, \dots, \mathcal{K}\}$.

Initialisation: Sélectionner un ensemble de $\mathcal{K}$ centres de gravité du clusters d'une façon initial: $c_i,\ i = 1, \dots, \mathcal{K}$.

Début

Répéter

1. Pour chaque vecteur d'observations compressées $y_\ell, \ell = (1, \dots, P = 2)$
2. Calculer la distance de chaque centre de groupe: c_i , $\mathrm{i} = 1, \dots, \mathcal{K}$. Et attribuer chaque observation dans le centre du groupe le plus proche.
3. Calculer la fonction objective FO définie par :

$$FO = \sum_{\mathrm{i}=1}^{\mathcal{K}} FO_i$$

$$= \sum_{\mathrm{i}=1}^{\mathcal{K}} \sum_{\forall y \in G_i} (\|y - c_\mathrm{i}\|)^2 \qquad (30)$$

4. Recalculer le groupe des centres c_i pour $\mathcal{K}$ groupes, ou le nouveau centre c_i est la moyenne de toutes les observations dans le groupe G_i.

Jusqu'à la convergence (la fonction objective est moins que ou égale à epsilon (seuil) puis arrêter.

Retour

La complexité du calcul de regroupement $\mathcal{K}-$moyennes, déterminée par le nombre de vecteurs d'observations, correspond au nombre d'utilisateurs de radio utilisées dans ce cette section. Voir l'organigramme de cette méthode dans l'annexe.A.

6.4.1.3. Avantages et inconvénients de la technique de clustering $\mathcal{K}$-moyennes

Avantages

- Très rapide, robuste, et facile à comprendre.
- Donne le meilleur résultat lorsque le groupe de données sont séparées les uns les autres ou distinctes.
- Le clustering $\mathcal{K}$-moyennes produit des clusters plus stricts que le clustering Hiérarchique, surtout si les clusters sont globulaires.
- Le temps de calcul est plus rapide dans le clustering $\mathcal{K}$-moyennes que le clustering Hiérarchique, si on garde $\mathcal{K}$ petit.

Inconvénients

- N'utilise pas plus de deux entrées.
- Avec un seul cluster global, il ne fonctionne pas bien.

- Il ne fonctionne pas bien avec des clusters (dans les données originales) de différentes tailles et de différentes densités.

6.4.2. Technique d'échantillonnage compressif coopérative combinée avec la méthode de la distance de Mahalanobis (TDM) pour la détection d'anomalies

Les observations compressées de chaque utilisateur radio sont collectées dans une matrice de patrons dans le centre de fusion comme une entrée du détecteur de distance de Mahalanobis. La TDM est une nouvelle technique sensible pour détecter les anomalies en utilisant deux estimateurs robustes pour la détection qui sont (la moyenne et la covariance).

6.4.2.1. Technique de la distance de Mahalanobis proposée pour la détection d'anomalies

La forme et la taille de données à plusieurs variables sont quantifiées par la matrice de covariance. Une mesure de distance connue, qui tient compte de la matrice de covariance, est la distance de Mahalanobis. Pour les observations compressées x_j $(j = 1, \dots, \mathbb{K})$ la mesure de la distance de Mahalanobis MD_j est définie comme suit

$$MD_j^2 = (x_j - \vec{\mu})' \Sigma^{-1} (x_j - \vec{\mu}), \tag{31}$$

Où, $\vec{\mu}$ est la moyenne et Σ la matrice de covariance. Pour un ensemble de données multi-variées sont normalement distribués. Les aberrantes multi-variées peuvent être définies comme des échantillons x_j ayant de grandes valeurs MD_i quand on les compare avec la valeur du seuil défini par : $thr = inv(\chi^2_{P,1-\alpha})^{1/2}$. Où, $\chi^2_{P,1-\alpha}$ est la distribution chi-carrée pour un niveau de signification α, et P signifie degrés de liberté et on suppose $((1-\alpha) = 0.975 = 97.5\%$ quantile, avec $\alpha = 0.025)$, voir l'Annexe.B. Les distances MD_j doivent être estimées par des estimateurs robustes qui sont très sensibles à la reconnaissance des anomalies qui sont la moyenne et la covariance [132], [133]:

$$\mu_j = \frac{1}{\mathbb{K}} \sum_{l=1}^{P} x_{\ell j} \ , \ \Sigma = \frac{1}{\mathbb{K}-1} \sum_{j=1}^{\mathbb{K}} (x_j - \vec{\mu})(x_j - \vec{\mu})', \tag{32}$$

$$x_j = \{x_{j1}, \dots, x_{jP}\},, \ell = 1, \dots, P,$$

Compte tenu d'un niveau de signification d'erreur α; le critère de détection d'anomalies est donné comme suit:

Une observation x_j est classée comme une anomalie si est seulement si cette condition ci-dessous est vérifiée:

$$MD_j > inv(\chi^2_{P,1-\alpha})^{1/2}, \quad (33)$$

Sinon l'observation est considérée comme normale

Dans la technique de détection d'anomalies proposée dans cette thèse, on suppose que les anomalies sont qualitativement différentes des observations normales et qu'un grand écart par rapport à ces observations normales peuvent être déterminées comme des attaques (des activités suspectes). Pour réaliser l'algorithme de détection d'anomalies, on effectue la distance MD_j qui mesure la moyenne et la matrice de covariance, parce que la moyenne et la matrice de covariance ont un impact significatif sur la solution de la distance MD_j pour une détection robuste et efficace.

En commençant par les estimateurs robustes, la distance MD_j pour $x_j(j = 1,2, \dots, \mathbb{K})$ sont calculées. L'opération peut être répétée afin d'assurer que les estimateurs robustes proposés sont résistants à la reconnaissance de patrons d'anomalies. Voir l'organigramme de cette méthode dans l'Annexe.C.

6.4.2.2. Algorithme de distance de Mahalanobis pour la détection d'anomalies multi-variées

Entrée: $y(P \times \mathbb{K})$: une matrice d'observations.

Sortie: Les candidats d'anomalies.

Début

Calculer la moyenne (μ) et la matrice de covariance(Σ).

Soit: D un vecteur de mesures d'une dimension $(\mathbb{K} \times 1)$ constitué de la distance de Mahalanobis pour chaque observation.

Trouver les anomalies dans le vecteur: $D = (MD_1, \dots, MD_{\mathbb{K}})$ dont la valeur est supérieure à la valeur du seuil estimée par $(inv(\chi^2_{P,1-\alpha})^{1/2})$ pour chaque observation: x_j $(j = 1,2, \dots, \mathbb{K})$. Pour une erreur de signification donnée $(\alpha = 0.025)$; le critère de détection d'anomalies est alors:

Une observation x_j est classée comme une observation anomalie si:

$$\text{Hypothèse } (H_{11}):\ MD_j > inv(\chi^2_{P,1-\alpha})^{1/2}, \tag{34}$$

Une observation x_j est classée comme une observation normale si:

$$\text{Hypothèse } (H_{00}):\ MD_j \leq inv(\chi^2_{P,1-\alpha})^{1/2}, \tag{35}$$

Retour

6.4.2.3. Avantages et inconvénients de la technique de distance de Mahalanobis

Avantages

- L'avantage de la distance de Mahalanobis et qu'elle prenne en considération les corrélations entre les variables et cette considération est importante dans l'analyse des patrons.

Inconvénients

- L'inconvénient de la distance de Mahalanobis est que le temps de calcul peut atteindre $\mathcal{O}(P^2)$pour des vecteurs caractéristiques.

6.4.3. Technique d'échantillonnage compressif coopérative combinée avec la méthode Q-Q plot chi-carrée pour la détection d'anomalies multi-variées

La distribution statistique Q-Q plot chi-carrée de la distance de Mahalanobis au carrée MD_j^2: Une procédure graphique, largement utilisée, est basée sur la distribution des distances de Mahalanobis ordonnées. Tracer les distances aux carrées ordonnées MD_j^2 et $100(\frac{j-0.5}{\mathbb{K}})$ quantiles de la distribution chi-carrée avec P degrés de liberté utilisant Q-Q plot chi-carrée. Où, $MD_j^2 = (x_j - \vec{\mu})'\Sigma^{-1}(x_j - \vec{\mu})$, $j = 1, \dots, \mathbb{K}$, et $x_1, x_2, \dots, x_{\mathbb{K}}$ sont des observations compressées pour chaque

variable P. La distance MD_j^2, a une distribution χ_P^2 (chi-carrée sur P degrés de liberté). Cette méthode est très efficace lorsque la valeur des deux nombres $\mathbb{K}$ et $\mathbb{K} - P$ sont plus grands que 30.

La procédure suivante explique cette technique pour construire une distribution Q-Q plot chi-carrée.

- Ordonne les carrées des distances de Mahalanobis MD_j^2 du plus petit au plus grand $MD_1^2 < MD_2^2 <, \ldots, < MD_{\mathbb{K}}^2$, utilisant la fonction $sort()$.
- Tracer la distance MD_j^2 par rapport aux points de probabilité chi-carré $\chi_P^2(1 - Q_j)$, où les Q_j sont également des probabilités espacés entre 0 et 1. Calculer les quantiles $Q_j(\frac{j-0.5}{\mathbb{K}})$ liées aux percentiles supérieurs d'une distribution chi-carrée.
- Tracer les paires $(Q_j\left(\frac{j-0.5}{\mathbb{K}}\right), MD_j^2)$ pour obtenir un Q-Q plot chi-carré pour la détection d'anomalies.

Q-Q plot devrait ressembler à une droite passant par l'origine qui représente le seuil dans cette section [134]. Voir l'organigramme de cette méthode dans l'annexe D.

6.4.3.1. Avantages et inconvénients de la technique graphique et statistique Q-Q plot

Avantages

- De nombreux aspects de la distribution peuvent être testés simultanément. Par exemple : le changement de la symétrie, la présence d'anomalies peuvent être détectées par ce type de plot,…etc.
- L'asymétrie peut être plus apparente.

Inconvénients

- Demande de la pratique.

6.4.4. Technique d'échantillonnage compressif coopérative combinée avec la méthode graphique Boxplot pour la détection d'anomalies

Des techniques graphiques/statistiques plus complexes ont également été utilisées pour détecter les anomalies, comme a été expliquées dans [40]. La technique Boxplot présentée dans la Figure 6.7, ci-dessous est une technique graphique simple qui a été appliquée pour détecter des anomalies multivariées et univariées dans de nombreux domaines de recherche telles que: sciences médicales, communications, traitement du signal. Boxplot également connu comme une boîte de moustache. Boxplot représente graphiquement les données multi-variables, utilisant des observations compressées tels que la plus petite observation non-anomalie (Min), quartile inférieur $(Q1)$, quartile supérieur $(Q3)$, et la plus grande observation non-anomalie (Max). La quantité $(Q3 - Q1)$ est appelée plage-inter-quartile (IQR). La méthode graphique Boxplot indique également les limites au-delà desquelles toute observation sera traitée comme une anomalie. La région entre $(Q1 - 1.5 * IQR)$ et $(Q3 - 1{,}5 * IQR)$ contient des observations normales et les autres régions contiennent la présence d'anomalies.

6.4.4.1. Technique Boxplot pour la détection d'anomalies

Le test IQR: pour la détection d'anomalies,

$$Q25 = Q1 = 25\%,$$
$$Q75 = Q3 = 75\%,$$
$$IQR = Q75 - Q25 = Q3 - Q1,$$
$$IQR \text{ (Plage-Inter -Quartile)},$$

Si $abs(observation(x_j) - Q3) > 1{,}5 * IQR$, alors l'observation est une anomalie moyenne.

Si $abs(observation(x_j) - Q3) > 3.0 * IQR$, alors l'observation est une anomalie extrême.

Si $abs(observation(x_j) - Q1) < 1{,}5 * IQR$, alors l'observation est une anomalie moyenne.

Si $abs(observation(x_j) - Q1) < 3.0 * IQR$, alors l'observation est une anomalie extrême.

Voir l'organigramme de cette méthode dans l'Annexe.E.

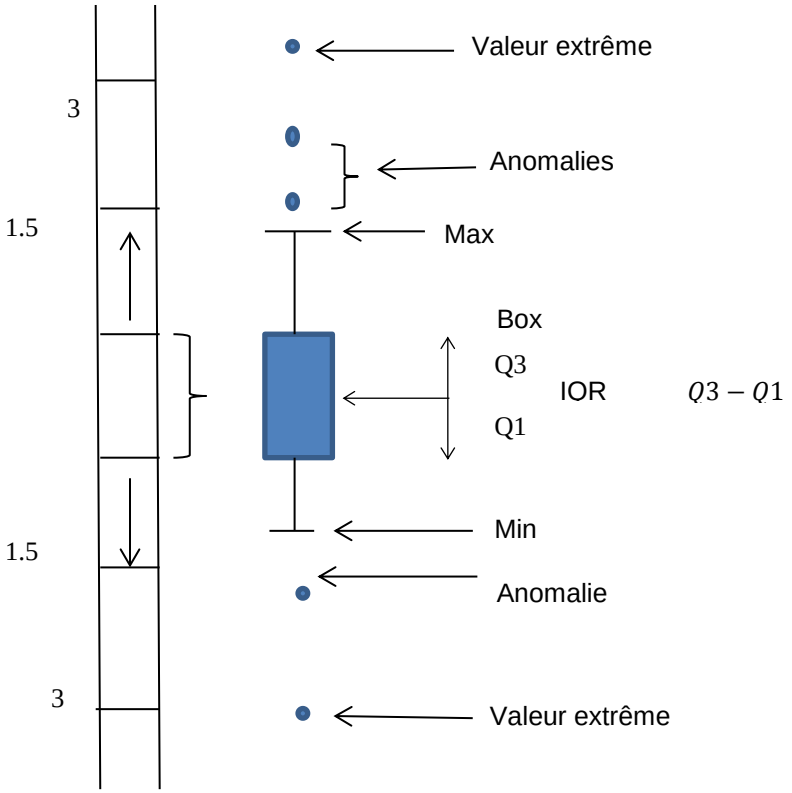


Figure 6.7 : Détecteur graphique-statistique Boxplot pour la détection d'anomalies.

6.4.4.2. Avantages et inconvénients de la technique graphique Boxplot

Avantages

- Montre un résume de 5 points et des anomalies.
- Compare facilement deux ou plusieurs groupes de données.
- Gère un très grand groupe de données facilement.
- Fournir une certaine indication de la symétrie et l'asymétrie des données.
- Affiche graphiquement l'étalement d'un variable à un coup d'œil.
- Par rapport à d'autres méthodes de visualisation de données, Boxplot montre des anomalies.
- En utilisant un Boxplot pour chaque variable côte-à-côte dans le même graphe, on peut comparer rapidement l'ensemble de données.

Inconvénients

- Cache de nombreux détails de la distribution.

6.5. Conclusion

Dans ce chapitre on a pu combiner la technique d'échantillonnage compressif via une collaboration centralisée avec quatre types de détecteurs intelligents avant l'étape de récupération du signal sparse et ça dans un régime large-bande. La complexité des calculs et la consommation d'énergie par chaque utilisateur radio a été réduite. Deux hypothèses H_0 et H_1 ont été proposées afin de distinguer la présence ou l'absence d'attaques de brouillage et deux autres hypothèses ont été proposées H_{00} et H_{11} afin de décider si les observations sont des anomalies ou normales.

CHAPITRE 7

RESULTATS ET DISCUSSION

Dans un schéma coopératif centralisé large-bande de radio cognitive, on génère un signal source de type QPSK corrompu par la présence d'un bruit blanc gaussien additif (BBGA), et par la présence de deux type de signaux de brouillage : un signal de brouillage d'impulsions sinusoïdale généré par le premier utilisateur brouilleur (UJ1) avec deux fréquences de brouillage différentes $f_{j_1} = 10\ MHz, f_{j_1} = 2.4\ GHz,$ un rapport cyclique noté τ_{j_1}, une fréquence de répétition notée FR. Aussi en présence d'un autre type de signal de brouillage à onde-continue (Continue-Wave : CW) de tonalités multiple généré par le deuxième utilisateur brouilleur (UJ2) qui contient trois fréquences successives $(f_{j_{21}} = 0.4\ GHz, f_{j_{22}} = 0.6\ GHz, f_{j_{23}} = 1\ GHz)$. Le signal reçu $r(t)$ est observé par chaque utilisateur radio. On suppose le nombre de bandes de fréquence $n_1 = 6$, et le nombre de canaux radio supposés: $P = 2,\ P = 10,\ P = 40,\ P = 50$. La fréquence de Nyquist est donnée par : $fNyq = 2.4\ GHz$, la fréquence maximale est $f_{max} = 1.2\ GHz$, et la bande-passante de chaque bande de fréquence est donnée par: $\beta_1 = 50\ MHz$. Après l'application de la technique d'échantillonnage compressif pour chaque radio intelligente, chaque récepteur radio donne un nombre minimum d'échantillons noté $\mathbb{K}$. Le model du canal supposé est le canal de Rayleigh. Différents types de rapports sont supposés dans ce travail comme: le rapport signal sur bruit SNR, le rapport signal sur le premier signal de brouillage $SJ1R$, et le rapport signal sur le deuxième signal de brouillage $SJ2R$. Des valeurs du rapport cyclique sont supposées comme suit : τ_{j_1} =10%, τ_{j_1} =20%. Le nombre de clusters supposés pour la méthode de clustering est donné par: $\mathcal{K} = 5$. On prend en considération les hypothèses expliquées dans cette thèse $(H_{00},\ H_{11})$ et (H_0, H_1). On suppose dans ce travail un réseau sans fil de type WiFi 2.4 Ghz.

7.1. Résultats et discussion pour une détection basée sur le clustering

La présence du signal source généré par l'utilisateur primaire de type QPSK. La présence du bruit blanc gaussien additif. La présence d'un signal de brouillage d'impulsions sinusoïdales généré par le premier utilisateur brouilleur (UJ1) avec deux rapport cyclique : $\tau_{j1} = 10\%, \tau_{j1} = 20\%$, trois fréquences de répétition : $FR = 1MHz$, $FR = 100KHz$, $FR = 0.5MHz$, et deux fréquences du premier type de brouilleur : $f_{j_1} = 10MHz$, $f_{j_1} = 2.4\,GHz$. On suppose le nombre de cluster : $\mathcal{K} = 5$.

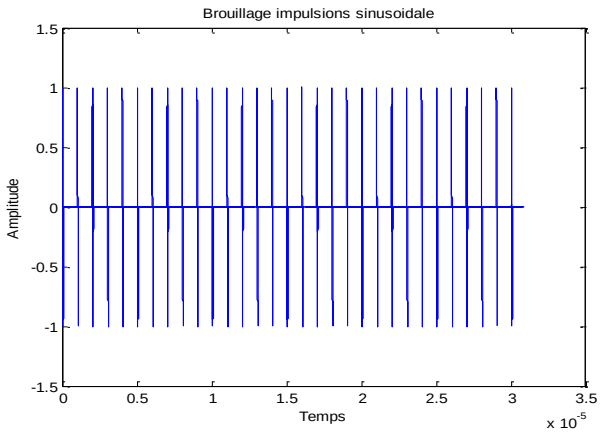


Figure 7.1: Montre le signal de brouillage d'impulsions sinusoïdales avec $\tau_{j1} = 10\%, FR = 1MHz, f_{j_1} = 10\ MHz$.

Hypothèse H_0:

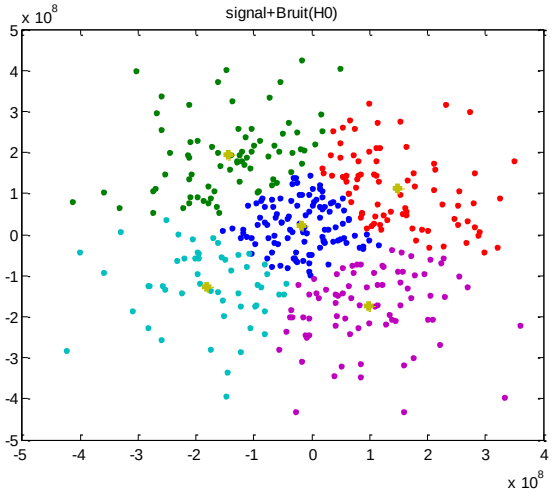


Figure 7.2: Spectre du signal source, et du bruit dans le cas de l'hypothèse H_0: $SNR = 10$ dB, $\mathbb{K} = 400$, $P = 2$.

Hypothèse H_1:

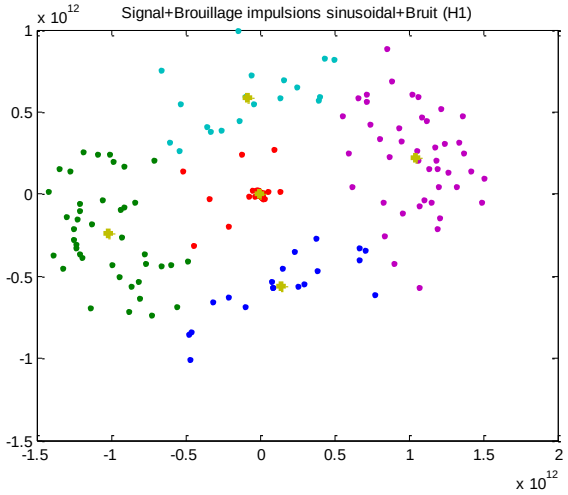


Figure 7.3: Spectre du signal source, du bruit, et du signal de brouillage d'impulsions sinusoïdales dans le cas de l'hypothèse H_1 $SNR = 10\,dB, SJ1R = -20dB, FR = 20\,KHz, \tau_{j1} = 20\%, \mathbb{K} = 400, f_{j1} = 10\,Mhz, P = 2.$

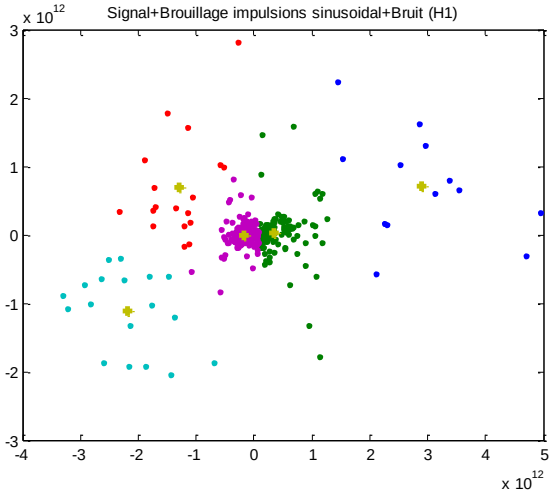


Figure 7.4: Spectre du signal source, du bruit, et du signal de brouillage d'impulsions sinusoïdales dans le cas de l'hypothèse H_1: $SNR = 10\,dB, SJ1R = -20dB, FR = 1MHz, \tau_{j1} = 10\%, \mathbb{K} = 400, f_{j1} = 10\,MHz, P = 2.$

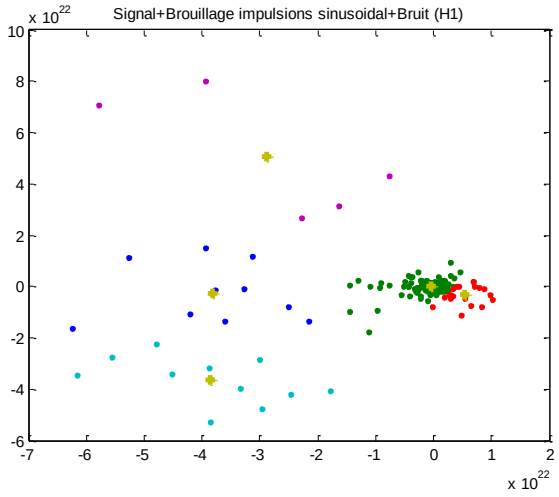


Figure 7.5: Spectre du signal source, du bruit, et du signal de brouillage d'impulsions sinusoïdales dans le cas de l'hypothèse H_1: $SNR = 10\,dB, SJ1R = -20dB, FR = 0.5\,MHz,\ \mathbb{K} = 400, \tau_{j1} = 10\%, f_{j1} = 2.4\,GHz, P = 2$.

Hypothèse H_0:

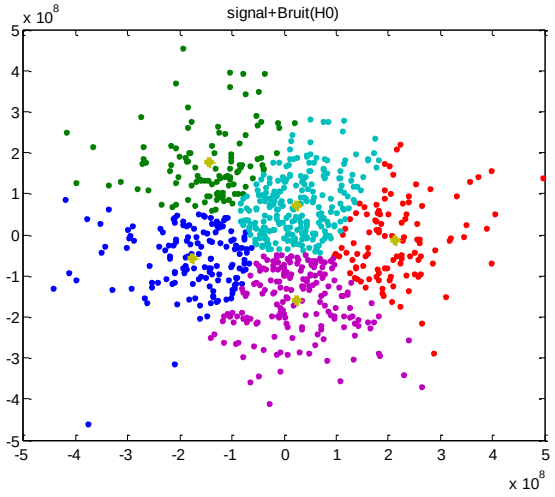


Figure 7.6: Spectre du signal source, et du bruit dans le cas de l'hypothèse H_0: avec $SNR = 10\,dB$, $\mathbb{K} = 800, P = 2$.

Hypothèse H_1:

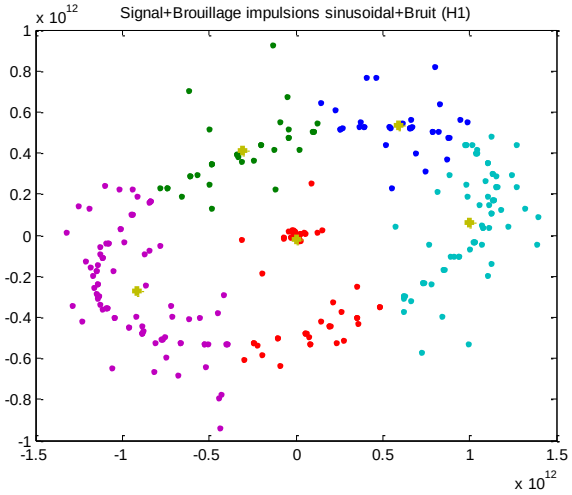


Figure 7.7: Spectre du signal source, du bruit, et du signal de brouillage d'impulsions sinusoïdales dans le cas de l'hypothèse H_1: $SNR = 10\,dB, SJ1R = -20dB, FR = 20KHz, \tau_{j1} = 20\%$, $\mathbb{K} = 800$, $f_{j1} = 10\,MHz, P = 2$.

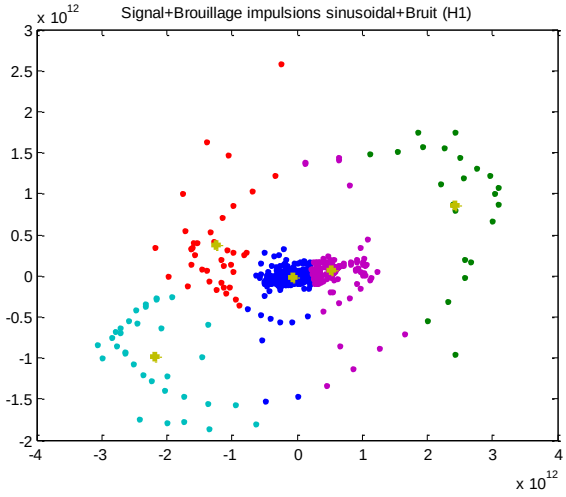


Figure 7.8: Spectre du signal source, du bruit, et du signal de brouillage d'impulsions sinusoïdales dans le cas de l'hypothèse H_1: $SNR = 10\,dB, SJ1R = -20dB$, $FR = 1\,MHz, \tau_{j1} = 10\%$, $\mathbb{K} = 800$, $f_{j1} = 10\,MHz, P = 2$.

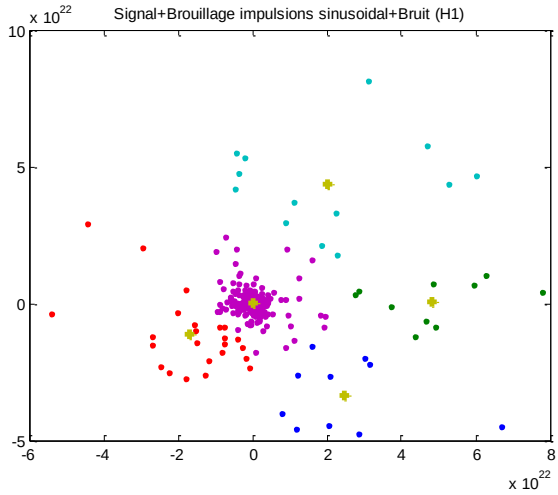


Figure 7.9: Spectre du signal source, du bruit, et du signal de brouillage d'impulsions sinusoïdales dans le cas de l'hypothèse H_1: avec $SNR = 10\,dB$, $SJ1R = -20dB, FR = 0.5\,MHz, \tau_{j1} = 10\%, f_{j1} = 2.4\,GHz,\ \mathbb{K} = 800, P = 2$.

Hypothèse H_0:

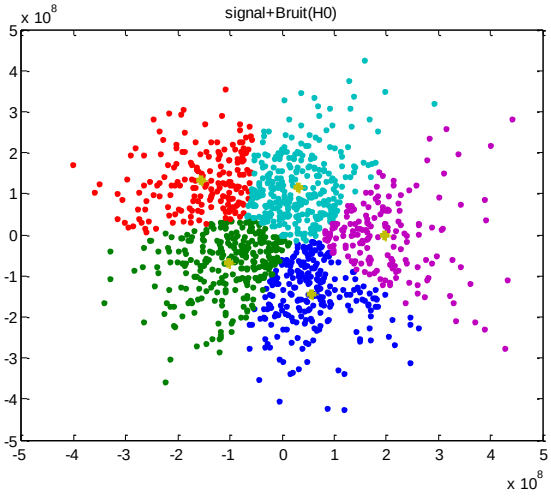


Figure 7.10: Spectre du signal source, et du bruit dans le cas de l'hypothèse H_0: avec $SNR = 10\,dB, \mathbb{K} = 1200, P = 2$.

Hypothèse H_1:

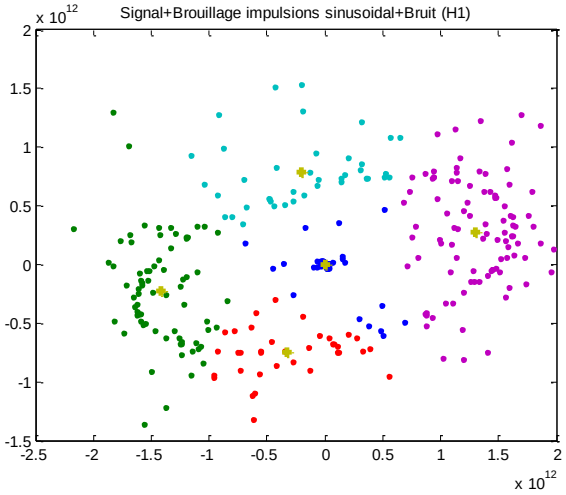


Figure 7.11: Spectre du signal source, du bruit, et du signal de brouillage d'impulsions sinusoïdales dans le cas de l'hypothèse H_1: $SNR = 10\,dB, SJ1R = -20dB, FR = 20KHz, \tau_{j1} = 20\%, \mathbb{K} = 1200, f_{j1} = 10\,MHz, P = 2$.

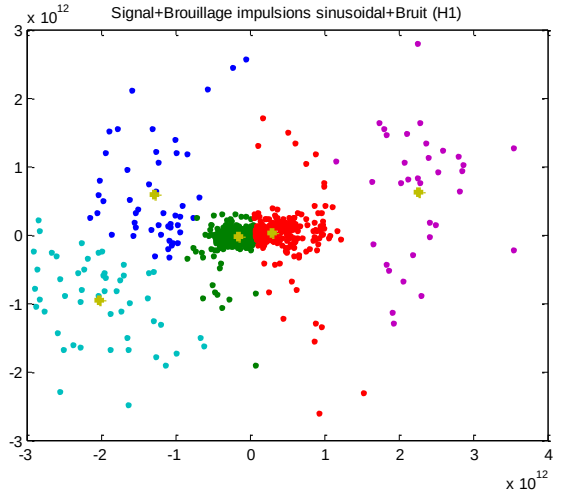


Figure 7.12: Spectre du signal source, du bruit, et du signal de brouillage d'impulsions sinusoïdales dans le cas de l'hypothèse H_1: $SNR = 10\,dB, SJ1R = -20dB, FR = 1\,MHz, \tau_{j1} = 10\%, \mathbb{K} = 1200, f_{j1} = 10\,MHz, P = 2$.

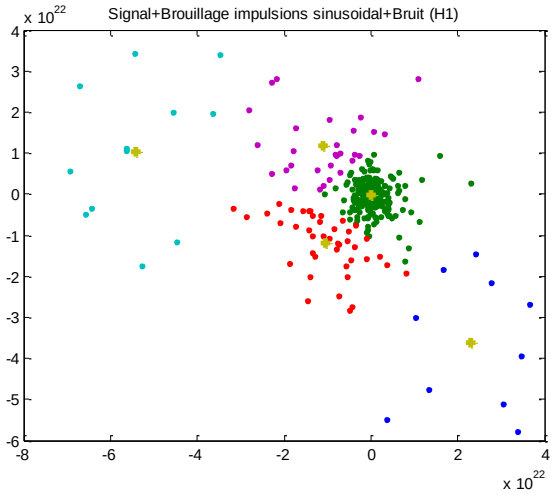


Figure 7.13: Spectre du signal source, du bruit, et du signal de brouillage d'impulsions sinusoïdales dans le cas de l'hypothèse H_1: $SNR = 10\,dB$, $SJ1R = -20dB$, $FR = 0.5\,MHz, \tau_{j1} = 10\%$, $f_{j1} = 2.4\,GHz$, $\mathbb{K} = 1200$, $P = 2$.

Si on compare les trois figures (Fig.7.2—Fig.7.6--Fig.7.10), comme illustrées ci-dessus obtenues dans le cas de l'hypothèse H_0 qui signifie l'absence du signal de brouillage intentionnel d'attaque avec les figures (Fig.7.3—Fig.7.4—Fig.7.5—Fig.7.7—Fig.7.8—Fig.7.9-Fig.7.11—Fig.7.12—Fig.7.13), obtenues dans le cas de l'hypothèse H_1, qui signifie la présence du signal de brouillage intentionnel de type d'impulsions sinusoïdales, on remarque bien que dans les spectres obtenus, il y a un comportement anormal de la distribution d'observations utilisant le détecteur intelligent dit clustering $\mathcal{K}$-moyennes bi-variable basé sur la valeur du seuil de convergence. Et ce comportement anormales des observations dans le spectre due à la présence de l'effet de brouillage corrompu avec le bruit et le signal source qui crie des erreurs en changeant les valeurs des observations par rapport au cas de l'hypothèse H_0. On voit bien une déviation et une distribution anormales des patrons dans différentes directions dans le spectre. Ça nous amène à prouver que ce type de clustering et très rapide et efficace à détecter l'effet de brouillage dans le spectre.

7.2. Résultats et discussion pour une détection basée sur la technique de distance de Mahalanobis (TDM)

La présence du signal source généré par l'utilisateur primaire de type $\frac{\pi}{2}$QPSK. La présence du bruit blanc gaussien additif. La présence d'un signal de brouillage d'impulsions sinusoïdale généré par le premier utilisateur brouilleur (UJ1) avec un rapport cyclique donné par, $\tau_{j1} = 20\%$, et d'une fréquence de répétition : $FR = 200\ MHz$, ainsi que la fréquence du premier type de brouilleur : $f_{j1} = 2.4\ GHz$.

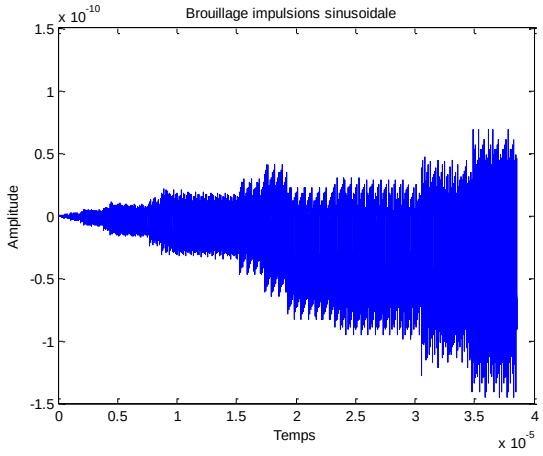


Figure 7.14: Montre le signal de brouillage d'impulsions sinusoïdales avec : $\tau_{j1} = 20\%,\ FR = 200MHz,\ f_{j_1} = 2.4\ GHz$.

Hypothèse H_1:

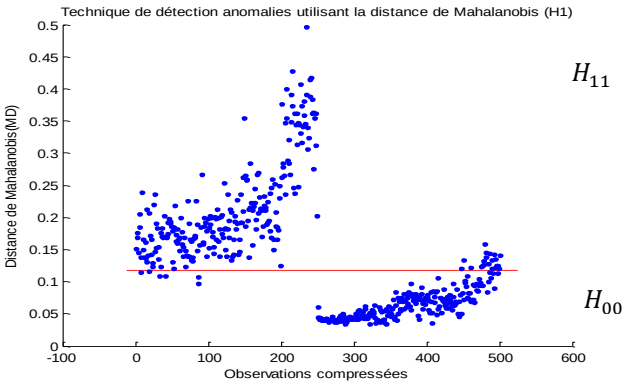


Figure 7.15: Montre la détection d'anomalies utilisant un détecteur intelligent (TDM) dans le cas de l'hypothèse H_1 avec $P = 50$ radios, $NR = 10dB$, $\tau_{j1} = 20\%$, $\mathbb{K} = 500, FR = 200\ MHz, f_{j1} = 2.4\ GHz$.

Hypothèse H_0:

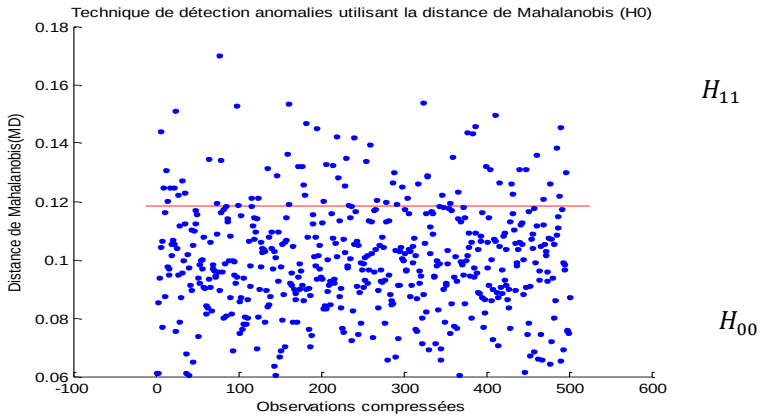


Figure 7.16: La détection d'anomalies utilisant un détecteur intelligent (TDM) dans le cas de l'hypothèse H_0 avec $P = 50$ radios, $SNR = 10dB$, $\mathbb{K} = 500$.

La ligne rouge dans les figures représente la valeur du seuil pour faire une différence entre une observation anomalie et une observation normale pour $P = 50$ radios, avec $\alpha = 0.025$, et la valeur du seuil est donnée par :

$$thr = inv(\chi^2_{P,1-\alpha=0.975})^{1/2},$$

$$\mathbb{K} = taux\ d'anomalies + taux\ normales$$

Utilisant la technique d'échantillonnage compressif dans l'écoute coopérative large-bande donne un nombre minimum de mesures pour accélérer le processus de détection d'anomalies. Les trois figures suivantes : Figure 7.15, Figure 7.16 donnent des résultats détaillés montrant que la technique de distance de Mahalanobis performe le mieux pour distinguer entre une observation anomalie et une observation normale pour toutes les observations x_j $(j = 1,2, \dots, \mathbb{K})$, dans le cas des deux hypothèses décrites ci-dessus basées sur la valeur du seuil défini. On suppose la présence ou l'absence du signal de brouillage d'attaque intentionnel selon les deux hypothèses. Dans le cas de la présence du bruit et du signal source uniquement (H_0: absence du signal de brouillage) et par l'application du détecteur de distance de Mahalanobis, on remarque bien dans la figure 6.16, la présence d'un nombre restreint d'anomalies estimé par (13.2%) à cause de la présence du bruit et du signal source uniquement. Ce taux d'anomalie obtenue à chaque opération, n'est pas fixé à 13.2%. Dans le cas de la présence du bruit, du

signal source, et du signal de brouillage ensemble le cas de (H_1: présence du signal de brouillage) et par l'application du détecteur intelligent, on remarque, comme montre la Figure 7.15 obtenue, la présence d'un grand nombre d'anomalies estimé par (48.8%) à cause de la présence du bruit et de la présence du signal de brouillage d'attaque de type brouilleur d'impulsions WiFi 2.4 GHz, et le signal source ensemble et les paramètres du signal de brouillage utilisé est définit par

$$\tau_{j1} = 20\%, FR = 200\ MHz, f_{j1} = 2.4\ GHz.$$

	Hypothèse $\boldsymbol{H_0}$	Hypothèse $\boldsymbol{H_1}$
Taux d'anomalies	13.2%	48.8%
Taux normales	86.8%	51.2%

Tableau 7.1 : Taux d'anomalies et taux normales obtenus.

Ces résultats expérimentaux obtenus montrent que le nouveau schéma de détection d'anomalies proposé est basé sur la distance de Mahalanobis notée (MD_j) qui fonctionne mieux dans l'identification d'anomalies/d'attaques. Le détecteur intelligent de distance de Mahalanobis a une sensibilité suffisante pour détecter les anomalies parce qu'il contient deux estimateurs robustes et sensibles qui sont la moyenne et la covariance. Un autre avantage de la TDM est que lors de l'étape de détection, les statistiques peuvent être calculées en moins de temps, ce qui rend possible l'utilisation de cette technique dans les scenarios en temps-réel dans le cas des applications civiles et militaires.

7.3. Résultats et discussion pour une détection basée sur la technique

Q-Q plot chi-carrée

La présence du signal source généré par l'utilisateur primaire de type $\frac{\pi}{4}$QPSK. La présence du bruit blanc gaussien additif. La présence d'un signal de brouillage d'impulsions sinusoïdale généré par le premier utilisateur brouilleur (UJ1) avec un rapport cyclique ($\tau_{j1} = 20\%$), et une fréquence de répétition $FR = 1MHz$, et une fréquence de brouilleur $f_{j_1} = 10\ MHz$. Aussi par la présence d'un autre type de signal de brouillage à onde continue (Continue-Wave (CW)) à tonalités multiple

généré par le deuxième type d'utilisateur brouilleur (UJ2) qui contient trois fréquences successives ($f_{j_{21}} = 0.4\ GHz, f_{j_{22}} = 0.6\ GHz, f_{j_{23}} = 1\ GHz$).

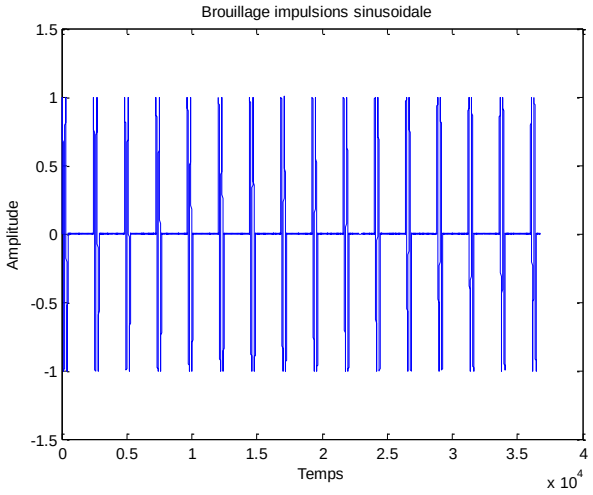


Figure 7.17: Le signal de brouillage d'impulsions sinusoïdales avec $\tau_{j1} = 20\%$, $FR = 1MHz,\ f_{j_1} = 10\ MHz$.

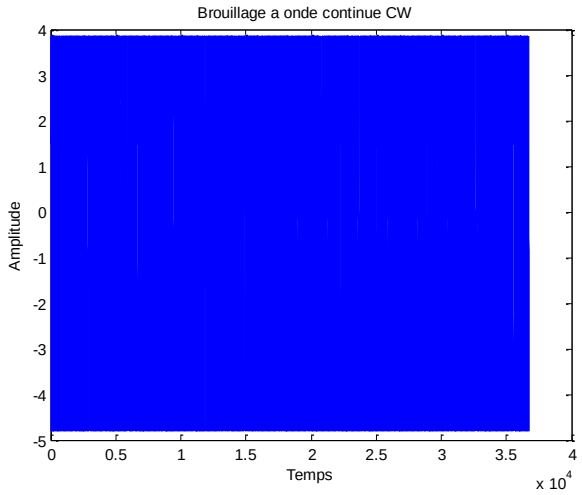


Figure 7.18: Le signal de brouillage à onde-continue.

Hypothèse H_0: La présence du signal source $\frac{\pi}{4}$QPSK, et le bruit uniquement.

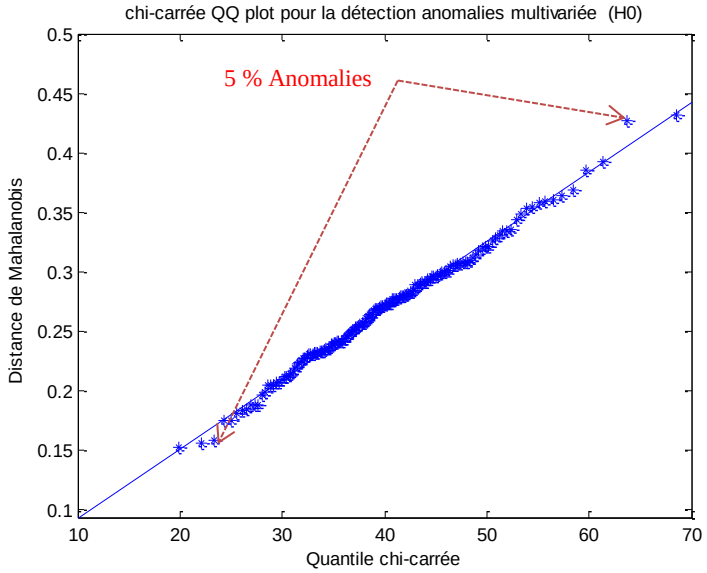


Figure 7.19: La détection d'anomalies utilisant un détecteur intelligent Q-Q plot dans le cas de l'hypothèse H_0, avec : $SNR = 10dB$, $P = 40, \mathbb{K} = 150$.

Hypothèse H_1: La présence du signal source $\frac{\pi}{4}$QPSK, le bruit, et les deux types de signaux de brouillage.

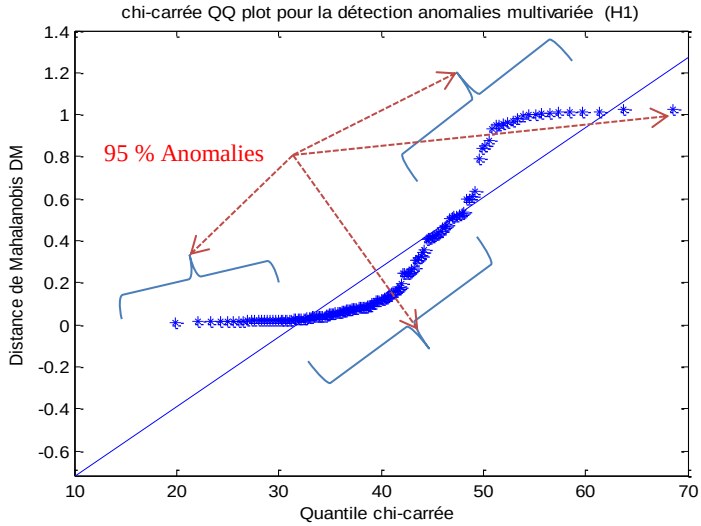


Figure 7.20: La détection d'anomalies utilisant un détecteur intelligent QQ plot dans le cas de l'hypothèse H_1, avec: $SNR = 10dB, SJ1R = -30dB, SJ2R = -20dB, P = 40, \tau_{j_1} = 20\%, FR = 1\ MHz,\ f_{j1} = 10\ MHz,\ f_{j_{21}} = 0.4\ GHz,\ f_{j_{22}} = 0.6\ GHz,\ f_{j_{23}} = 1\ GHz, \mathbb{K} = 150$.

Nous tenons à comparer les résultats obtenus concernant les deux hypothèses H_0 et H_1 considérées dans cette section. On remarque qu'il y a un problème d'anomalies en utilisant un détecteur intelligent de type graphique et statistique Q-Q plot chi-carré appliqué pour un nombre ($P = 40$) radios comme indiqué dans la Figure 7.19, et la Figure 7.20. Dans la Figure 7.19, qui signifie H_0, on remarque qu'il y a un problème de présence d'anomalies estimé par 5% qui s'écartent fortement de la ligne droite (le seuil) qui est définit par QQ plot en raison de la présence de l'effet du bruit uniquement. Mais dans la Figure 7.20, comme illustrée ci-dessus qui signifie H_1, on remarque qu'il y a un problème de la présence d'anomalies estimé à 95% qui s'écartent fortement de la ligne droite en raison de l'effet du bruit, et de la présence de deux types de brouilleurs différents (UJ1), (UJ2) de type d'impulsions sinusoïdales et à onde-continue. Ce détecteur intelligent montre qu'il est sensible et robuste à la présence de patrons d'anomalies basé sur le seuil expliqué par la ligne droite depuis l'origine comme montre les résultats obtenus ci-dessus. Ça nous amène à prouver que cette méthode est efficace pour détecter l'effet de brouillage dans le spectre parce qu'elle contienne deux estimateurs robuste pour la détection des anomalies qui sont la moyenne et la covariance.

7.4. Résultats et discussion pour une détection basée sur la technique graphique et statistique Boxplot

La présence du signal source généré par l'utilisateur primaire de type QPSK.

La présence du bruit blanc gaussien additif.

La présence d'un signal de brouillage d'impulsions sinusoïdale généré par le premier utilisateur brouilleur (UJ1) avec deux valeurs du rapport cyclique : $\tau_{j1} = 10\%, \tau_{j1} = 20\%$, trois fréquences de répétition données par : $FR = 1MHz$, $FR = 20KHz, FR = 0.5\,MHz$, et deux fréquences de brouillage du premier type de brouilleur : $f_{j_1} = 10\,MHz, f_{j1} = 2.4GHz$.

Hypothèse H_1

Le signal source de type QPSK avec la présence du bruit, et du signal de brouillage d'impulsions sinusoïdale ensemble.

On va combiner le schéma coopératif large-bande centralisé d'échantillonnage du spectre compressif avec un détecteur intelligent de type graphique : Boxplot robuste, les résultats ont été obtenus, comme illustrés ci-dessous:

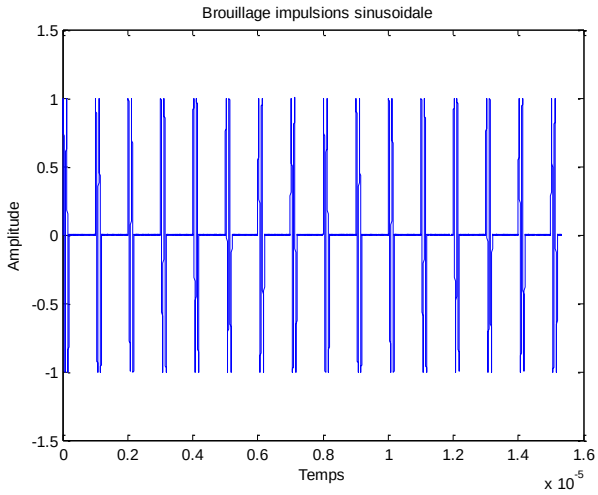


Figure 7.21: Signal de brouillage d'impulsions sinusoïdales avec: $\tau_{j1} = 20\%, FR = 1MHz, f_{j_1} = 10\ MHz.$

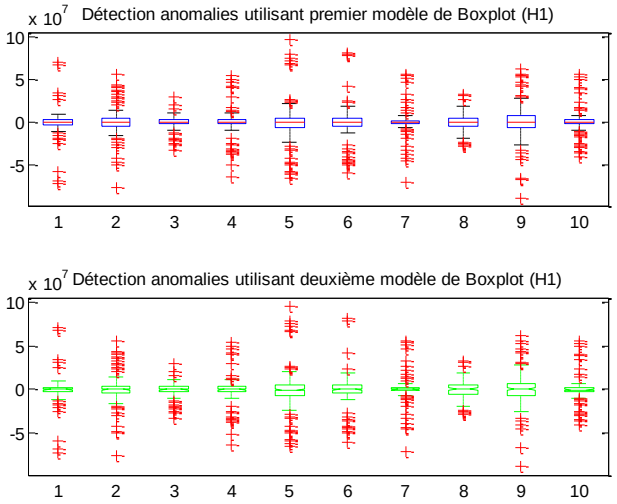


Figure 7.22: La détection d'anomalies utilisant le détecteur Boxplot pour 10 radios, avec : $SNR = 10dB, SJ1R = -40dB, \tau_{j1} = 10\%,\ FR = 1MHz, \mathbb{K} = 150, f_{j_1} = 10\ MHz.$

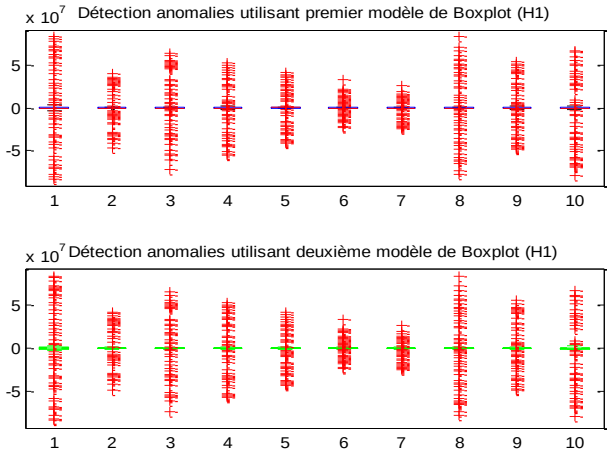


Figure 7.23: La détection d'anomalies utilisant le détecteur Boxplot pour 10 radios, avec: $SNR = 10dB,\ SJ1R = -40dB, \tau_{j1} = 10\%,\ FR = 20\ KHz, \mathbb{K} = 150,\ f_{j_1} = 10\ MHz.$

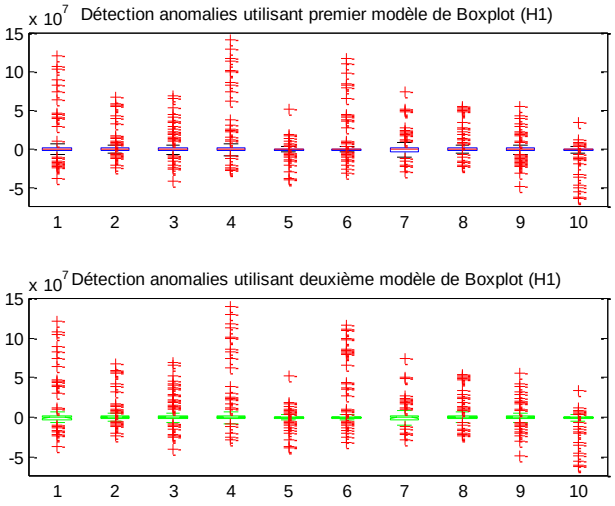


Figure 7.24: La détection d'anomalies utilisant le détecteur Boxplot pour 10 radios, avec $NR = 10dB,\ SJ1R = -40dB,\ \tau_{j1} = 20\%,\ FR = 0.5\ MHz,\ \mathbb{K} = 150,\ f_{j1} = 2.4GHz.$

Hypothèse H_0

Le signal source QPSK avec la présence du bruit uniquement.

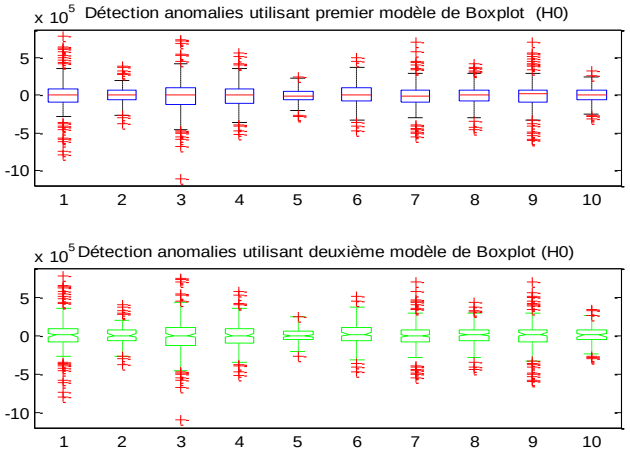


Figure 7.25: La détection d'anomalies utilisant Boxplot pour 10 radios, avec : $SNR = 10dB, \mathbb{K} = 150.$

Pour les résultats obtenus comme montrent les figures illustrées ci-dessus dans le cas des deux hypothèses décrites ci-dessus H_0 et H_1 en appliquant un détecteur intelligent de type graphique et statistique Boxplot. Dans cette technique on a testé deux modèles de Boxplot (simple et compacte) pour savoir s'ils donnent le même résultat ou non. On remarque qu'il existe un problème d'anomalies dans les deux cas d'hypothèses que ce soit par la présence ou l'absence de brouillage à cause des effets du signal de brouillage d'attaque et le bruit blanc gaussien additif. Sur la base de l'hypothèse H_0 (comme indiqué dans la Figure 7.25), la présence d'un signal d'utilisateur primaire de type QPSK corrompu avec le bruit, donne un nombre minimum d'anomalies uni-variées pour chaque vecteur d'observations à cause de l'effet de bruit. Sur la base de l'hypothèse H_1 (comme indiqué dans les trois Figures suivantes: 7.22 ; 7.23 ; et 7.24), la présence d'un signal d'utilisateur primaire de type QPSK, le bruit, et le signal de brouillage d'attaque d'impulsions, donne un grand nombre d'anomalies par rapport aux résultats obtenus dans le cas de l'hypothèse H_0, parce qu'il a présence du signal de brouillage d'impulsions d'attaque et le bruit additif dans ce cas. On remarque aussi que le nombre d'anomalies dans les trois Figures 7.22 ; 7.23 ; et 7.24 est plus élevé par rapport aux résultats obtenus dans le cas de la Figure 7.25 à cause

de la présence de l’effet de brouillage d’impulsions en change à chaque fois les paramètres du signal de brouillage d’impulsions tels que le rapport cyclique, la fréquence de fonctionnement et la fréquence de répétition. Ça nous amène à prouver que cette méthode est efficace à détecter les anomalies due à l’effet de brouillage dans le spectre.

7.5. Comparaison avec les résultats de la littérature

Pour la comparaison des résultats obtenus avec des techniques de d'autres auteurs : plusieurs techniques classiques de détection de l'effet de brouillage furent développées au cours de ces dernières années mais tous ont montrées une perte d'efficacités que ce soit en consommation d'énergie par chaque utilisateur radio ou la complexité des calculs ainsi que la performance de ces techniques. Citant comme exemple des techniques basées sur l'étalement du spectre, les réseaux, les antennes, …etc. Dans notre travail, on a combiné la technique d'échantillonnage compressif via une collaboration centralisée avec des détecteurs intelligents avant l'étape de récupération du signal sparse, au niveau de la couche physique des utilisateurs radios. On se basant sur des hypothèses pour distinguer l'existence de l'effet d'attaques dans le spectre, on a pu minimiser la consommation d'énergie, la complexité des calculs et la détection rapide de l'effet d'attaques dans un régime large-bande.

7.6. Comparaison entre les méthodes proposées et leurs résultats

Les deux méthodes graphiques et statistiques Boxplot et Q-Q plot chi-carrée proposées dans ce travail donnent de bons résultats et montrent que le taux d'anomalies obtenu est grand dans le cas de l'hypothèse H_1 (présence de brouillage) par rapport au taux obtenu dans le cas de l'hypothèse H_0 (absence de brouillage), ce qui signifie qu'il y a présence de brouillage dans le spectre.

La méthode de clustering $\mathcal{K}-$moyennes la plus rapide parmi les différentes méthodes de clustering qui existe dans la littérature montre qu'il y a présence de brouillage dans le spectre dans le cas de l'hypothèse H_1 qui explique qu'il y a une distribution anormale de patrons dans le spectre par rapport aux résultats obtenus dans le cas de l'hypothèse H_0. Ça prouve que cette méthode utilisée est très efficace à la détection rapide de l'effet de brouillage dans le spectre.

Une autre méthode de classification a été proposée basée sur la distance de Mahalanobis qui prouve qu'il existe le problème de présence de brouillage dans le spectre en se basant sur la valeur du seuil déterminée. Le taux de détection d'anomalies obtenu est très élevé dans le cas de l'hypothèse H_1 par rapport au taux d'anomalies obtenu dans le cas de l'hypothèse H_0 . Ce qui signifie que cette

méthode utilisée et aussi efficace pour la détection de l'effet de brouillage dans le spectre parce qu'elle contienne de estimateurs statistiques qui sont robustes a la détection d'anomalies.

On peut utiliser cette méthode de classification pour dessiner la courbe COR qui donne une relation entre le taux de détection d'anomalies (TPR) en fonction du taux de fausse-alarme (FPR), utilisant la théorie de Newman-Pearson.

Chaque méthode proposée dans ce travail montre son efficacité de détecter rapidement la présence du problème de brouillage dans le spectre sous forme d'anomalies lorsque le signal source est corrompu avec le bruit et le brouillage et de réduire la consommation d'énergie par chaque récepteur radio. Enfin, les méthodes de classification sont les meilleurs pour faire une détection de la présence de brouillage en temps-réel basée sur le problème de reconnaissance d'anomalies.

CHAPITRE 8
CONCLUSIONS ET PERSPECTIVES

Conclusions

Le brouillage radio fréquence est défini comme une transmission RF illicite visant à désactiver la communication sur le système ciblé. La radio cognitive est une radio qui conscient, et est capable de façon autonome de reconfigurer ses paramètres de transmission, afin d'améliorer son efficacité. Quand les radios cognitives sont utilisées dans le domaine des systèmes de brouillage et antibrouillage, de tels systèmes sont considérés comme intelligents. Dans cette thèse, on a étudié l'impact des radios cognitives dans le domaine du brouillage intelligent et le brouillage à une stratégie fixée et les solutions antibrouillage intelligentes. Cette thèse a étudié l'impact des radios cognitives dans le domaine de brouillage et des solutions proposées d'antibrouillage intelligent. Elle a présenté des solutions et des idées concrètes dans le domaine de la guerre électronique des communications.

Dans cette thèse, on a présenté un schéma coopératif centralisé large-bande de radios intelligentes qui combine la technique d'échantillonnage compressif avec différentes techniques intelligentes pour détecter les anomalies dues à l'effet du signal de brouillage, et de bruit. Chaque utilisateur radio dans le mode de coopération utilise une matrice d'écoute et transmet ses mesures compressées au centre de fusion pour la détection. Le centre de fusion collecte les mesures compressées sous forme d'une matrice de données de chaque utilisateur radio et utilise cette matrice comme une entrée pour les détecteurs intelligents pour la détection d'anomalies basée sur des mesures compressées ($y_{\ell=1\dots P}$). La performance de ces nouveaux schémas conçus donne de bonnes performances tout en minimisant la complexité du calcul et la consommation d'énergie par chaque utilisateur radio. Aussi, comme une solution importante, l'augmentation du nombre de radio en mode de coopération large-bande, implique que le taux d'échantillonnage à chaque utilisateur radio diminue. Cela donne une grande réduction en termes de complexité du schéma et d'implémentation.

Pour le coût de ces techniques proposées et les moyens importants de communication, elles sont justifiées par la résolution des problèmes de sécurité et de défense dans les systèmes de communication sans fils tactique et d'urgence contre les attaques malveillants générées par des signaux électronique indésirables.

Perspectives

- Parmi les perspectives de cette thèse on peut citer des détecteurs intelligentes basées sur un seul classifieur ou multi-classifieur de type discret ou probabiliste pour la détection d'anomalies comme montre le chapitre 4 utilisant l'analyse de la courbe COR qui explique le taux de détection d'anomalies (TPR) en fonction du taux de fausse alarme (FPR). Cela se fait aussi par l'utilisation d'une autre technique intelligente dite apprentissage par renforcement pour la détection d'anomalies, l'analyse des composantes principales, et la machine à vecteurs de support,….etc.
- On pourra étudier la simplification de ces méthodes pour diminuer les coûts en faisant un compromis avec l'efficacité.
- Utilisation des prédicteurs intelligents pour détecter l'effet de brouillage dans les systèmes de communication sans fil de MIMO radio et la collaboration de MIMO radios.
- Détection très rapide, intelligente et ultra-large-bande de l'effet de brouillage au niveau de la radio avant l'étape de récupération du signal.

PUBLICATIONS

Un article a été accepté dans un journal

A Moumena, A Guessoum. Fast anomaly detection using Boxplot rule for multivariate data in cooperative wideband cognitive radio in the presence of jammer. Security and Communication Networks Journal, Volume 8, Issue 2, pages 212–219, 25 January 2015, DOI: 10.1002/sec.974; with IF=0.72.

Deux articles qui sont en cours d'évaluation

A.Moumena. ''Anomalies detection based on the ROC analysis using classifiers in tactical cognitive radio systems: A survey''. Submitting in journal, 2015.

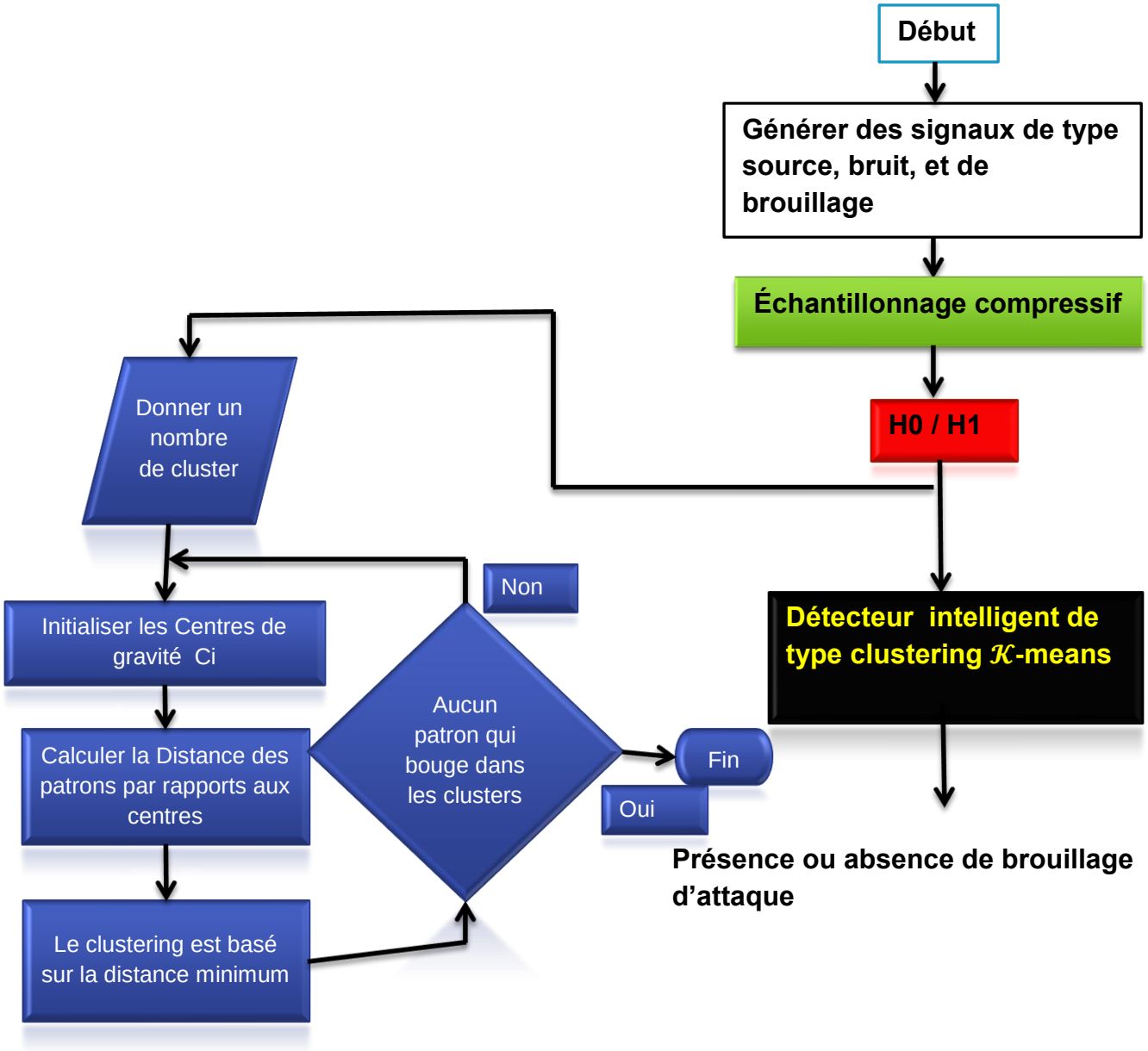
A.Moumena, A.Guessoum. ''Using chi-square Q-Q plot for detecting multivariate anomalies in wideband cooperative sensing in the presence of jammers''. Revised with resubmission in IET communication journal. 2015.

Un seul article dans une conférence international

A.Moumena. ''Abnormal behavior detection of jamming signal in the spectrum using a combination of compressive sampling and intelligent bivariate k-means clustering technique in wideband cognitive radio systems''. Is Accepted in ICEE 2015 - The 4th International Conference on Electrical Engineering, Boumerdes, Algeria.

ANNEXE.A

L'organigramme ci-dessous explique la technique d'échantillonnage compressif combinée avec un détecteur intelligent de type clustering $\mathcal{K}$-moyennes.



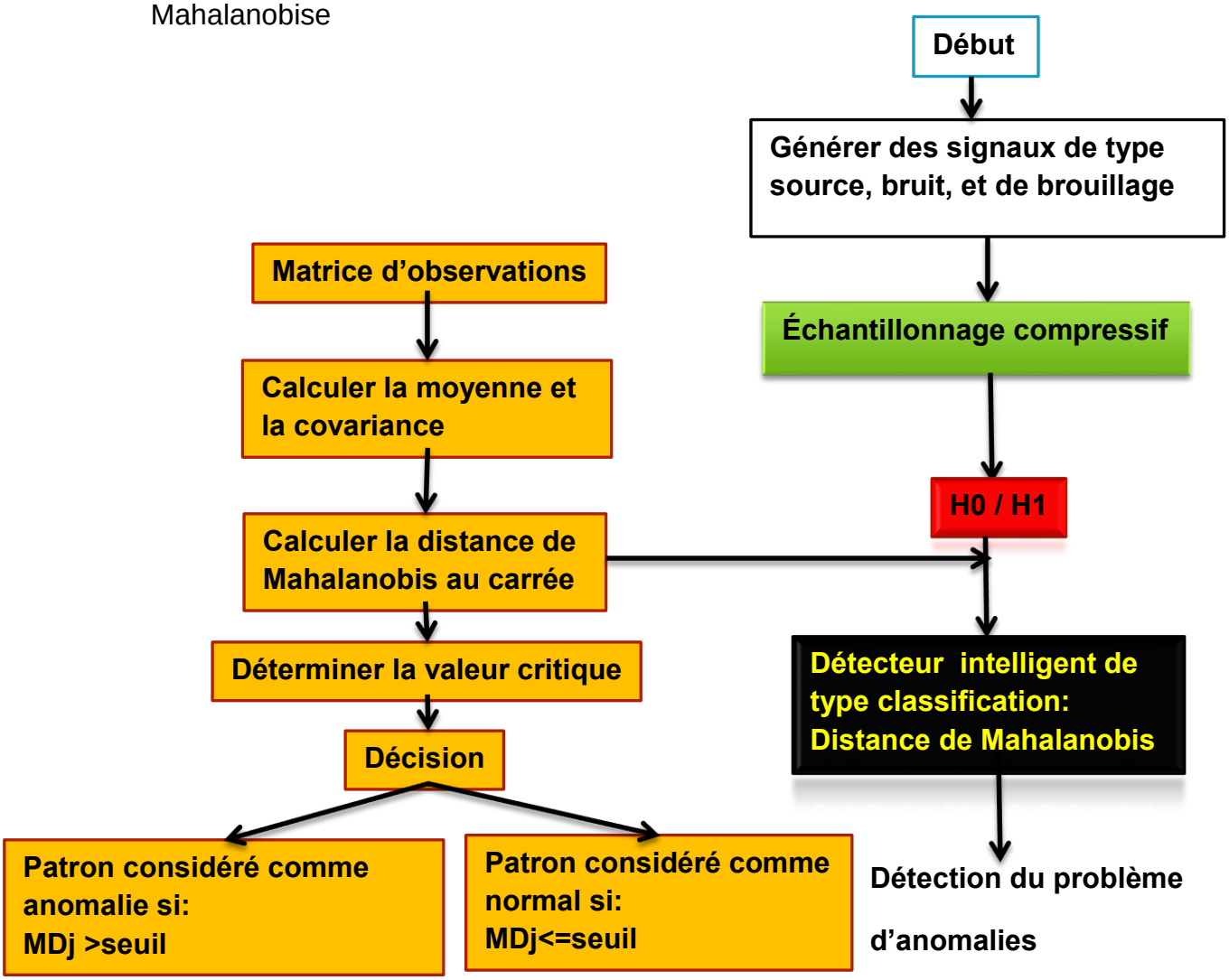
ANNEXE.B

df $/\alpha$	0.005	0.01	0.025	0.05	0.1	0.9	0.95	0.975	0.99	0.995
1	7.844	6.635	5.024	3.841	2.706	0.016	0.004	0.001	0.000	0.000
2	10.557	9.210	7.378	5.991	4.605	0.211	0.103	0.051	0.020	0.010
3	12.796	11.345	9.348	7.815	6.251	0.581	0.352	0.216	0.115	0.072
4	14.815	13.277	11.143	9.488	7.779	1.064	0.711	0.484	0.297	0.207
5	16.702	15.086	12.833	11.070	9.236	1.610	1.145	0.831	0.554	0.412
6	18.499	16.812	14.449	12.592	10.645	2.204	1.635	1.237	0.872	0.676
7	20.227	18.475	16.013	14.067	12.017	2.833	2.167	1.690	1.239	0.969
8	21.902	20.090	17.535	15.507	13.362	3.490	2.733	2.180	1.646	1.344
9	23.535	21.666	19.023	16.919	14.684	4.168	3.325	2.700	2.088	1.735
10	25.132	23.209	20.483	18.307	15.987	4.865	3.940	3.247	2.558	2.156
11	26.700	24.725	21.920	19.675	17.275	5.578	4.575	3.816	3.053	2.603
12	28.241	26.217	23.337	21.026	18.549	6.304	5.226	4.404	3.571	3.074
13	29.760	27.688	24.736	22.362	19.812	7.042	5.892	5.009	4.107	3.565
14	31.258	29.141	26.119	23.685	21.064	7.790	6.571	5.629	4.660	4.075
15	32.739	30.578	27.488	24.996	22.307	8.547	7.261	6.262	5.229	4.601
20	39.929	37.566	34.170	31.410	28.412	12.443	10.851	9.591	8.260	7.434
30	53.594	50,892	46.979	43.773	40.256	20.599	18.493	16.791	14.953	13.787
40	66.680	63.691	59.342	55.758	51.805	29.051	26.051	24.433	22.164	20.707
50	79.397	76.154	71.420	67.505	63.167	37.689	34.674	32.357	29.707	27.991

Table de la distribution chi-carrée (chi-squared)

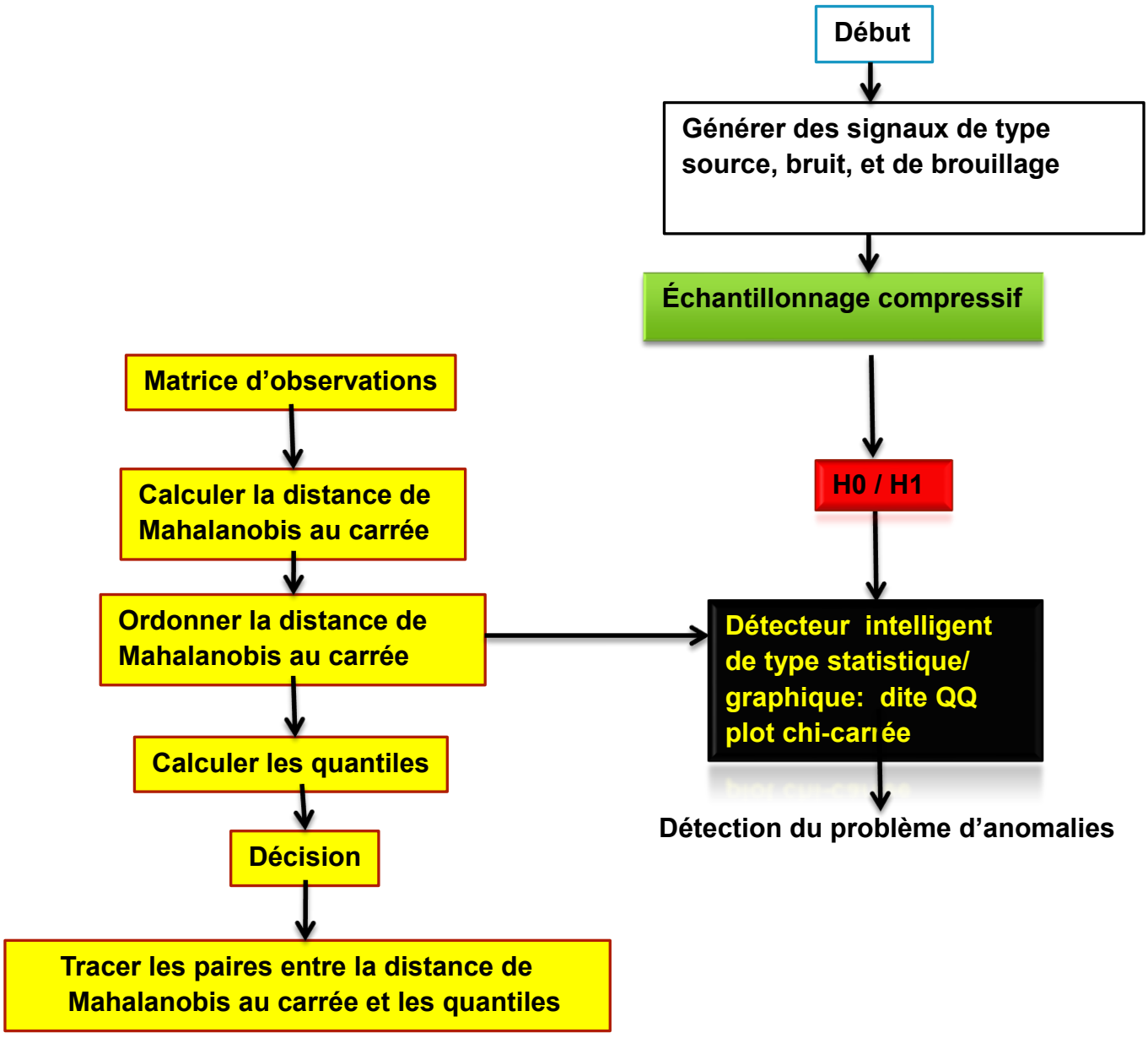
ANNEXE.C

L'organigramme ci-dessous explique la technique d'échantillonnage compressif combinée avec un détecteur intelligent de type classification distance de Mahalanobise



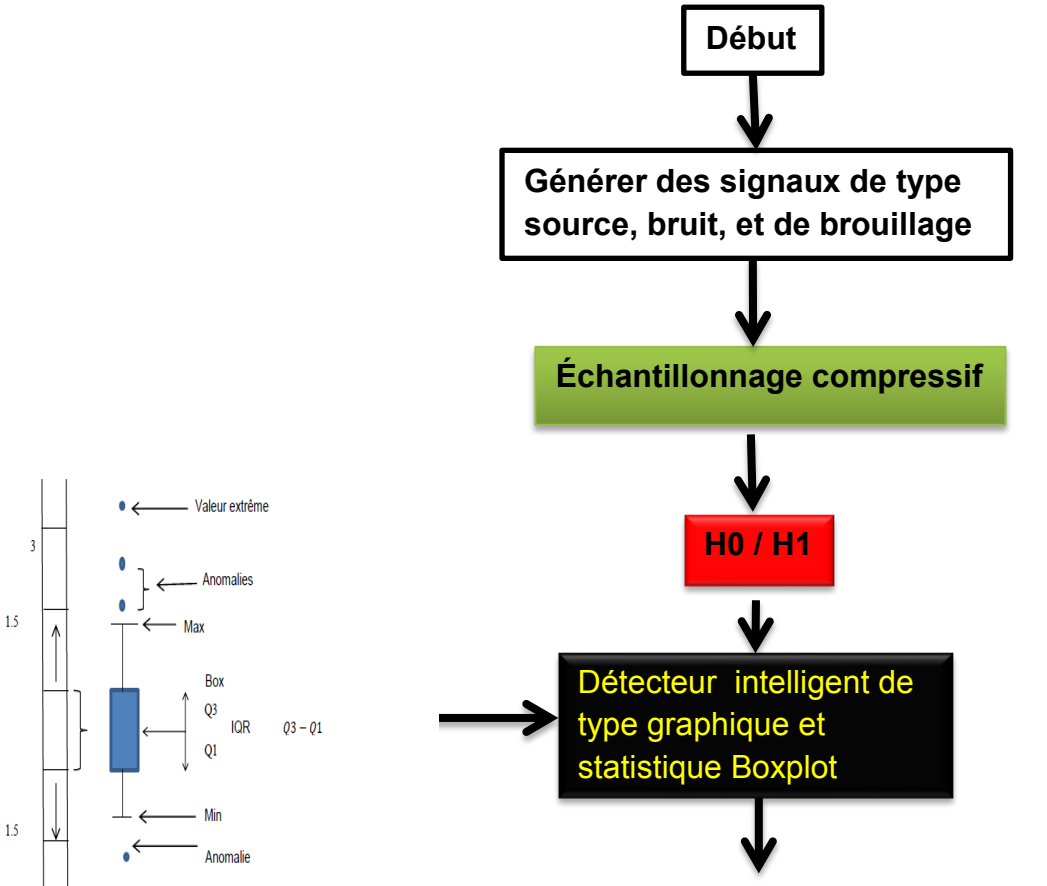
ANNEXE.D

L'organigramme ci-dessous explique la technique d'échantillonnage compressif combinée avec un détecteur intelligent de type QQplot chi-carrée.



ANNEXE.E

L'organigramme ci-dessous explique la technique d'échantillonnage compressif combinée avec un détecteur intelligent de type Boxplot**.**



Détection du problème d'anomalies

REFERENCES

1. M. McHenry, “NSF spectrum occupancy measurements project summary,” Shared Spectrum Company, Tech. Rep., (Aug. 2005).
2. C.-X. Wang, X. Hong, H.-H. Chen, and J. S. Thompson, “On capacity of cognitive radio networks with average interference power constraints,” IEEE Transaction. Wireless Communication., vol. 8, no. 4, (Apr. 2009), 1620–1625.
3. X. Hong, C.-X. Wang, H.-H. Chen, and Y. Zhang, “Secondary spectrum access networks: recent developments on the spatial models,” IEEE Vehicular. Technology. Magazine., vol. 4, no. 2, (June 2009), 36–43.
4. O. Younis, L. Kant, A. McAuley, K. Manousakis, D. Shallcross, K. Sinkar, K. Chang, and K. Young, "Cognitive Tactical Network Models", IEEE Communications Magazine, (October 2010), 70-77.
5. T. Yucek and H. Arslan, “A survey of spectrum sensing algorithms for cognitive radio applications,” IEEE Commun. Surveys and Tutorials, V.11, n.1, (Jan. 2009), 116–130.
6. H. Sun, D. Laurenson, and C.-X. Wang, “Computationally tractable model of energy detection performance over slow fading channels,” IEEE Communication Letters, V.14, n.10, (Oct. 2010), 924–926.
7. Ravi K. V., ‘’Effect of CW and pulse jamming on direct sequence spread spectrum code acquisition using a sequential detector’’, MILCOM 92, Military Communications Conference, (1992), V.2, 638-643.
8. Liang Zhao, Moeness G. Amin, Alan R. Lindsey: Mitigation of periodic interferers in GPS receivers using subspace projection techniques, AFRL-FI-RS-TR-2001-186, final technical report, (September 2001).
9. Lu Lu, Xiangwei Zhou, and Uzoma Onunkwo, Geoffrey Ye Li, ’’Ten years of research in spectrum sensing and sharing in cognitive radio’’, EURASIP Journal on Wireless Communications and Networking, (2012), V.28, 1-16, DOI: 10.1186/1687-1499-2012-28.

10. E. Hossain, and B. Bhargava, Eds., ‘’Cognitive Wireless Communication Networks’’, New York: Springer, (2007), 440 pages.

11. E. Biglieri, A. Goldsmith, L. Greenstein, N. Mandayam, and H. Poor, ‘’Eds. Principles of Cognitive Radio’’. Cambridge (Preprint), 2013), 352 pages.

12. T. Yucek and H. Arslan, “A survey of spectrum sensing algorithms for cognitive radio applications,” IEEE Communications Surveys Tutorials, (2009), V.11, n.1, 116–130**.**

13. J. Lundén, “Spectrum sensing for cognitive radio and radar systems,” Ph.D. dissertation, Helsinki University of Technology (TKK), Espoo, Finland, (2009).

14. R. Viswanathan and B. Ahsant, “A review of sensing and distributed detection algorithms for cognitive radio systems,” International Journal on Smart Sensing and Intelligent Systems, (Mar 2012), V.5, n.1, 177–190.

15. R. Viswanathan, “Cooperative spectrum sensing for primary user detection in cognitive radio,” in Proc. of the International Conference on Sensing Technology (ICST), (Nov. 28 – Dec. 1- 2011), 79–84.

16. Polo Y L, Technol Delft, Ying Wang, Pandharipande A, and Leus G, ‘’Compressive Wideband Spectrum Sensing’’, IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP-2009; (2009), 2337–2340.

17. RG Baraniuk, ‘’Compressive Sensing’’, IEEE Signal Processing Magazine, (2007), V.24, n.4, 118–121.

18. Volkan Cevher, Marco F Duarte, Chinmay Hegde, and Richard Baraniuk, ‘’Sparse signal recovery using Markov random fields’’, Advances in Neural Information Processing Systems conference, (2008), 257-264.

19. E Candes, J Romberg, T Tao, ‘’Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information’’, IEEE Transactions on Information Theory, (2006), V.52, n.2, 489-509.

20. E. Candes, J. Romberg, ‘’Sparsity and incoherence in compressive sampling’’, Inverse Problems, (June 2007), V.23, n.3, 969-985.

21. D. L. Donoho, ‘’Compressed sensing’’, IEEE Transactions on Information Theory, (April 2006), V.52, n.4, 1289-1306, DOI: 10.1109/TIT.2006.871582

22. J. Tropp and A. Gilbert, “Signal Recovery from Random Measurements via Orthogonal Matching Pursuit,” (2007).

23. D. Deedell andJ. Tropp, “COSAMP: Iterative Signal Recovery from Incomplete and Inaccurate Samples,” (2008).

24. P. Huggins and S. Zucker, “Greedy Basis Pursuit,” (2006).

25. W. Dai and O. Milenkovic, “Subspace Pursuit for Compressive Sensing Signal Reconstruction,” (2009).

26. D. Needell and R. Vershynin, “Uniform Uncertainty Principle and Signal Recovery via Regularized Orthogonal Matching Pursuit,” (2007).

27. T. Blumensath and M. Davies, “Iterative Hard Thresholding for Compressed Sensing,” (2008).

28. E. Candes and J. Romberg, “l1-Magic: Recovery of Sparse Signals via Convex Programming,” (2005).

29. Sami Kirolos, et al, ‘’Analog-to-Information-Conversation via Random-Demodulation’’, In Proc. IEEE Dallas Circuits and Systems Workshop (DCAS), (2006).

30. Hessam Guibene, Wael Hayar, Aawatif, ‘’Centralized collaborative compressed sensing of wideband spectrum for cognitive radios’’, International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops, (2010), 246–252, Moscow, Russia.

31. H. Urkowitz, ‘’Energy detection of unknown deterministic signal’’, Proceedings IEEE, (1967), V.55, n.4, 523 -531.

32. F. Digham, M. S. Alouini, M. K. Simon, ‘’On the energy detection of unknown signals over fading channels’’, IEEE Transactions on Communications, (2007), V.55, n.1, 21-24.

33. A. Dandawate, G. B. Giannakis, ‘’Statistical tests for presence of cyclostationarity, IEEE Transactions on Signal Processing, (1994), V.42, n.9, 2355-2369.

34. Christopher M. Bishop, ‘’Pattern Recognition and Machine Learning’’, Springer, (2007-10-01), 738.

35. Richard O. Duda, Peter E. Hart, David G. Stork, ‘’Pattern Classification (2nd Edition)’’, Wiley-Interscience, (2000), 680.

36. Hartigan J. A., Wong M. A., ‘’Algorithm AS 136: A K-Means Clustering Algorithm’’, Journal of the Royal Statistical Society, (1979), Series C V.28, n.1, 100–108.

37. Wenjie Hu, Y. Liao, V. Vemuri, ‘’Robust support vector machines for anomaly detection in computer security’’, International Conference on Machine, (2003).

38. Sultana A., Hamou Lhadj A., Couture M, ‘’An improved Hidden Markov Model for anomaly detection using frequent common patterns’’, IEEE Conference on communications ICC, (2012), 1113–1117.

39. Benjamini Y, ‘’Opening the Box of a Boxplot’’, The American Statistician, (1988), V.42, n.4, 257–262.

40. Varun Chandola, Arindam Banerjee, Vipin Kumar, ‘’Anomaly Detection: A Survey’’, ACM Computing Surveys, (2009), 1-72.

41. Albrecht, S., Busch, J., Kloppenburg, M., Metze, F., and Tavan, P., ‘’Generalized radial basis function networks for classification and novelty detection: self-organization of optional bayesian decision. Neural Networks 13, 10, (2000), 1075-1093.

42. Crook, P. A., Marsland, S., Hayes, G., and Nehmzow, U., ‘’A tale of two filters-on-line novelty detection’’, In Proceedings of International Conference on Robotics and Automation, (2002), 3894-3899.

43. Shekhar, S., Lu, C.-T., and Zhang, P., ‘’Detecting graph-based spatial outliers: algorithms and applications (a summary of results)’’, In Proceedings of the 7th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM Press, New York, NY, USA, (2001), 371-376.

44. Sun, J., Qu, H., Chakrabarti, D., and Faloutsos, C., ‘’ Neighborhood formation and anomaly detection in bipartite graphs’’, In Proceedings of the 5th IEEE International Conference on Data Mining. IEEE Computer Society, Washington, DC, USA, (2005), 418-425.

45. MacDonald, J. W. and Ghosh, D., ‘’Copa-cancer outlier profile analysis’’, Bioinformatics 22, 23, (2006), 2950-2951.

46. Lu, C.-T., Chen, D., and Kou, Y., ‘’Algorithms for spatial outlier detection’’, In Proceedings of 3rd International Conference on Data Mining, (2003), 597-600.

47. Dutta, H., Giannella, C., Borne, K., and Kargupta, H., ‘’Distributed top-k outlier detection in astronomy catalogs using the demac system’’, In Proceedings of 7th SIAM International Conference on Data Mining, (2007).

48. Kou, Y., Lu, C.-T., and Chen, D., ‘’Spatial weighted outlier detection. In Proceedings of SIAM Conference on Data Mining’’, (2006).

49. I. F. Akyildiz,W.-Y. Lee,M. C. Vuran, and S.Mohanty, “NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey,” Computer Networks, (2006), V.50,n.13, 2127–2159.

50. C.-X. Wang, X. Hong, H.-H. Chen, and J. Thompson, “On capacity of cognitive radio networks with average interference power constraints”, IEEE Transactions on Wireless Communications, (April 2009), V.8, 1620 –1625.

51. W. Zhang and K. B. Letaief, “Cooperative communications for cognitive radio networks”, Proceedings of the IEEE, (May 2009). V.97, 878–893.

52. J. Mitola and G. Maguire, “Cognitive radio: Making software radios more personal’’, IEEE Personal Communications, (1999), 13-18.

53. S. Haykin, “Cognitive radio: brain-empowered wireless communications”, IEEE Journal on Selected Areas in Communications, (Feb.2005), V.23, 201 – 220.

54. Joseph Mitola III, ‘’Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio’’, PhD thesis, Dept. of Teleinformatics, Royal Institute of Technology Stockholm, Sweden, (8 May, 2000).

55. I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, “Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey,” *Comput. Netw.*, (May 2006), V.50, 2127–2159.

56. Badr Benmammar, Asma Amraoui, ‘’Réseaux de radio cognitive : Allocation des ressources radio et accès dynamique au spectre’’, hal-00738289, version 1, (Octobre 2012), 1-86.

57. Hossain, Ekram, Dusit Niyato, and Zhu Han, ‘’Dynamic spectrum access and management in cognitive radio networks’’, Cambridge: Cambridge University Press, (2009).

58. T. R. Newman, B. A. Barker, A. M.Wyglinski, A. Agah, J. B. Evans, and G. J. Minden, ‘’Cognitive engine implementation for wireless multicarrier transceivers’’,. Wiley Wireless Communications and Mobile Computing, (Sept. 2006).

59. Badr Benmammar. ‘’Présentation de la radio cognitive’’, (Décembre 2013), première journée doctorale en informatique décisionnelle et informatique distribuée (IDID’1), Université de Bourdj Bou Arreridj.

60. I. F. Akyildiz, W.-Y. Lee, K. R., ‘’Chowdhury: "CRAHNs: Cognitive Radio Ad Hoc Networks", Ad Hoc Networks, Elsevier, (July 2009). V.7, n.5, 810-836.

61. J. Neel. J. Reed, A. MacKenzie, ‘’Cognitive Radio Network Performance Analysis in Cognitive Radio Technology’’, B. Fette, ed., Elsevier, (2006).

62. Deanna Hlavacek, , J. Morris Chang1. ‘’A layered approach to cognitive radio network security: A survey’’, Computer Networks, Volume 75, Part A, 24 December 2014, 414–436.

63. UsamaMir, Leila Merghem-Boulahia, and Dominique Gaïti. “COMAS: ACooperative Multiagent Architecture for Spectrum Sharing”. EURASIP Journal on Wireless Communications and Networking,Volume 2010, Article ID 987691. 2010.

64. E. Hossain and B. Bhargava, Eds., Cognitive Wireless Communication Networks.New York: Springer, (2007), 440 pages.

65. E. Biglieri, A. Goldsmith, L. Greenstein, N. Mandayam, and H. Poor, Eds.,Principles of Cognitive Radio. Cambridge (Preprint), (2013), 352 pages.

66. Hongjian Sun, Arumugam Nallanathan, Cheng-Xiang Wang, Yunfei Chen, ‘’Wideband Spectrum Sensing for Cognitive Radio Networks: A Survey’’, IEEE Wireless Communications, (2013), V.20, n.2, 74 – 81.

67. Nora Tarano, ‘’Compressive Sensing Techniques in Cognitive Radio Networks’’, EE359 Final Project, (2012), 1-11**.**

68. P. Varshney, ‘’Distributed detection and data fusion’’. New York: Springer-

Verlag, (1997), 276 pages.

69. R. Blum, S. Kassam, and H. Poor, “Distributed detection with multiple sensors: Part II – Advanced topics,” Proceedings of the IEEE, (Jan. 1997), V.85, n.1, 64–79.

70. J. Tsitsiklis, “Distributed detection,” in Advances in Statistical Signal Processing-Vol. 2: Signal Detection, H. Poor and J. Thomas, Eds. Greenwich, CT: JAI, (1993).

71. R. Viswanathan and P. Varshney, “Distributed detection with multiple sensors: Part I — fundamentals,” Proceedings of the IEEE, (Jan. 1997), V.85, n.1, 54–63.

72. Kresimir Dabcevic, ‘’ Intelligent jamming and anti-jamming techniques using Cognitive Radios’’. PhD thesis, Computational Intelligence, University of Genoa, Italy, (15 Avril, 2015), 171 pages.

73. Pettit, Ray H., ‘’ECM and CCME techniques for Digital communication Systems’’, Wadsworth, Inc., Belmont, (CA), (1982).

74. Markus Schafroth, ‘’Jamming Detection in Wireless Ad Hoc Networks’’. Master thesis. (MA-2008-21), 1-123. Ecole polytechnique fédérale de Zurich.

75. U.S. Department of Defense, ‘’Joint Pub. 1–02: DOD Dictionary of Military and Associated Terms’’ (Apr. 2010).

76. Roberto Di Pietro, Gabriele Oligeri, ‘’Jamming Mitigation in Cognitive Radio Networks’’, (2013), IEEE Network. V.27, issue.3, 10-15.

77. Q. Peng, P. Cosman, and L. Milstein, “Spoofing or jamming: Performance analysis of a tactical cognitive radio adversary,” Selected Areas in Communications, IEEE Journal on, (April 2011), V.29, n.4, 903 –911.

78. B. Wang, Y. Wu, K. Liu, and T. Clancy, “An anti-jamming stochastic game for cognitive radio networks,” Selected Areas in Communications, IEEE Journal on, (April 2011), V.29, n.4, 877 –889.

79. Paris kistos, ‘’Security in RFID and sensor networks’’, Wireless networks and mobile communications journal, (2009), 560 pages.

80. Richard Poisel, ‘’Modern Communications Jamming Principles and Techniques’’, Artech House, (2004), 479 pages.

81. A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. M. Leung, “A survey of security challenges in cognitive radio networks: Solutions and future research directions,” Proceedings of the IEEE, (2012), n.99, 1–15.

82. S. Liu, L. Lazos, and M. Krunz, “Thwarting inside jamming attacks on wireless broadcast communications,” in WISEC, (2011), 29–40.

83. W. Xu, T. Wood, W. Trappe, and Y. Zhang, “Channel surfing and spatial retreats: defenses against wireless denial of service,” in Proceedings of the 3rd ACM workshop on Wireless security, ser. WiSe ’04. New York, NY, USA: ACM, (2004), 80–89.

84. A. Asterjadhi and M. Zorzi, “Jenna: a jamming evasive network-coding neighbor-discovery algorithm for cognitive radio networks,” Wireless Commun., (Aug 2010), V.17, n.4, 24–32.

85. H. Li and Z. Han, “Dogfight in spectrum: combating primary user emulation attacks in cognitive radio systems, part i: known channel statistics,” Trans. Wireless. Comm., (Nov 2010), V.9, n.11, 3566–3577.

86. Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, “Anti-jamming games in multi-channel cognitive radio networks,” IEEE Journal on Selected Areas in Communications, (2012), V.30, n.1, 4–15.

87. Kumar, V.,‘’Parallel and distributed computing for cybersecurity’’, Distributed Systems Online, IEEE 6, 10.

88. Fujimaki, R., Yairi, T., and Machida, K., ‘’An approach to spacecraft anomaly detection problem using kernel feature space’’, In Proceeding of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining, ACM Press, New York, NY, USA, (2005), 401-410.

89. Edgeworth, F. Y., ‘’On discordant observations’’, Philosophical Magazine, (1887), V.23, n.5, 364-375.

90. Hawkins, D.M, ‘’Identification of Outliers’’, Chapman and Hall, London and New York, (1980), V.188, 10-00.

91. V. Barnett and T. Lewis, ‘’3rd edition’’, (John Wiley & Sons, Chichester), (1994), 584 pages.

92. Moore, D. S. and G. P. McCabe,''Introduction to the practice of statistics, 3rd ed'', 1999.

93. Chen, Z.; Fu, A. & Tang, J., ''Detection of outlier Patterns'', Dept. of CSE, Chinese University of Hong Kong, (2002).

94. Ramasmawy R.; Rastogi R. & Kyuseok S., ''Efficient algorithms for mining outliers from large data sets'', Proceedings of the ACM SIGMOD International Conference on Management of Data, (2000), 427-438, ISBN 1-58113-217-4, Dallas, Texas, United States.

95. Basu, S., Bilenko, M., and Mooney, R. J., ''A probabilistic framework for semi-supervised clustering'', In Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining. ACM Press, New York, NY, USA, (2004), 59-68.

96. Ester, M., Kriegel, H.-P., Sander, J., and Xu, X., ''A density-based algorithm for dis-covering clusters in large spatial databases with noise'', In Proceedings of Second International Conference on Knowledge Discovery and Data Mining, E. Simoudis, J. Han, and U. Fayyad, Eds. AAAI Press, Portland, Oregon, (1996), 226-231.

97. Smith, R., Bivens, A., Embrechts, M., Palagiri, C., and Szymanski, B., ''Clustering approaches for anomaly based intrusion detection'', In Proceedings of Intelligent Engineering Systems through Artificial Neural Networks. ASME Press, (2002), 579-584.

98. Barbara, D., Li, Y., Couto, J., Lin, J.-L., and Jajodia, S., ''Bootstrapping a data mining intrusion detection system'', In Proceedings of the 2003 ACM symposium on Applied computing. ACM Press, (2003), 421-425.

99. Tan, P.-N., Steinbach, M., and Kumar, V., ''Introduction to Data Mining'', Addison-Wesley, (2005).

100. Roth,V.,''Kernel fisher discriminants for outlier detection'', Neural Computation (2006), V.18, n.4, 942-960.

101. Anscombe, F. J. and Guttman, I., ‘’Rejection of outliers’’, Technometrics 2, (1960), V.2, 123-147.

102. Eskin, E.,‘’Anomaly detection over noisy data using learned probability distributions’’, In Proceedings of the Seventeenth International Conference on Machine Learning. Morgan Kauf- mann Publishers Inc., (2000), 255-262.

103. Desforges, M., Jacob, P., and Cooper, J.,‘’Applications of probability density estimation to the detection of abnormal conditions in engineering’’, In Proceedings of Institute of Mechanical Engineers. (1998), V. 212. 687-703.

104. Agovic, A., Banerjee, A., Ganguly, A. R., and Protopopescu, V., ‘’Anomaly detection in transportation corridors using manifold embedding’’, In First International Workshop on Knowledge Discovery from Sensor Data. ACM Press, (2007).

105. Jolliffe, I. T., ‘’Principal Component Analysis’’, 2nd ed. Springer, (2002).

106. Parra, L., Deco, G., and Miesbach, S., ‘’Statistical independence and novelty detection with information preserving nonlinear maps’’, Neural Computing, (1996), V.8, n.2, 260-269.

107. Dutta, H., Giannella, C., Borne, K., and Kargupta, H., ‘’Distributed top-k outlier detection in astronomy catalogs using the demac system’’, In Proceedings of 7th SIAM International Conference on Data Mining, (2007).

108. Shyu, alShyu, M.-L., Chen, S.-C., Sarinnapakorn, K., and Chang, L., ‘’A novel anomaly detection scheme based on principal component classifier’’, In Proceedings of 3rd IEEE International Conference on Data Mining, (2003), 353-365.

109. Fujimaki, R., Yairi, T., and Machida, K., ‘’An approach to spacecraft anomaly detection problem using kernel feature space’’, In Proceeding of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining. ACM Press, New York, NY, USA, (2005), 401-410.

110. Harold Stanislaw, Natasha Todorov, ‘’Calculation of signal detection theory measures’’, Behavior Research Methods, Instruments, & Computers, (1999), V.31, n.1, 137-149.

111. Jesse Davis , Mark Goadrich, ‘’The Relationship Between Precision-Recall and ROC Curves’’, Proceedings of the 23 rd International Conference on Machine Learning, Pittsburgh, PA, (2006), 1-8.

112. Tom Fawcett, ‘’ROC Graphs: Notes and Practical Considerations for Researchers’’, HP Laboratories, MS 1143, 1501 Page Mill Road, Palo Alto, CA 94304, (March 16, 2004).

113. R. A. Maxion and R. R. Roberts, ‘’Proper Use of ROC Curves in Intrusion/Anomaly Detection’’, Technical Report Series, CS-TR-871, (November 2004), School of Computing Science, University of Newcastle upon Tyne.

114. Yannick Oufella, ‘’Évolution du concept de front ROC et combinaison de classifieur’’, Mémoire de master, université de rouen, France, (2008), Pages.110.

115. Tom Fawcett, ‘’An introduction to ROC analysis’’, Pattern Recognition Letters, (2006), V.27, n.8, 861–874.

116. Srinivasan A, ‘’Note on the location of optimal classifiers in n-dimensional ROC space’’, Technical Report PRG-TR-2-99, Oxford University Computing Laboratory, Oxford, England, (1999).

117. Provost F., Domingos P., ‘’Well-trained PETs: Improving probability estimation trees’’, CeDER Working Paper #IS-00-04, Stern School of Business, New York University, NY, NY 10012, (2001).

118. Landgrebe T., Duin R., ‘’Combining accuracy and prior sensitivity for classifier design under prior uncertainty’’, Lecture Notes in Computer Science (LNCS), (2006), 4109, 512-521.

119. David J Hand, Robert J Till, ‘’A Simple Generalization of the Area Under the ROC Curve for Multiple Class Classification Problems’’, Machine Learning, (2011), V.45, n.2, 171-186.

120. Guillaume Temblay, ‘’Optimisation d’ensembles de classifieurs non-paramétriques avec apprentissage par représentation partielle de l’information’’, École de technologie supérieure (ETS), Université de Québec, Mémoire de Maitrise, (2004), Montréal, Canada.

121. Thomas D. Wickens, ‘’Elementary Signal Detection Theory’’, Book, Oxford University press, (2001), 276 pages.

122. Vyacheslav P. Tuzlukov, ‘’Signal Detection Theory’’, Springer, (2001), 725 pages.

123. John C. Hancock, Paul A. Wintz, ‘’Signal Detection Theory’’, McGraw-Hill, (1966), 247 pages.

124. Swets, al, ‘’Better decisions through science’’, Scientific American, (2000), 283, 82-87.

125. Doohwan Lee, Takayuki Yamada, Hiroyuki Shiba, Yo Yamaguchi, Kazuhiro Uehara, ‘’Compressed Sensing Technology for Flexible Wireless System’’, NTT Technical Review, Yokosuka-shi, (2011), 239-0847, Japan.

126. A. Cohen, W. Dahmen, R. Devore, ‘’Compressed Sensing and Best k-term Approximation’’, Journal of the American Mathematical Society, (Jan 2009), V.22, n.1, 211–231.

127. S S Chen, D L Donoho, and M A Saunders. Atomic decomposition by basis pursuit. SIAM Journal on Scientific Computing, 2001, 43(1):129-159, DOI: 10.1137/S003614450037906X.

128. C La and M Do. Signal reconstruction using sparse tree representations. SPIE Wavelets XI, 2005, vol. 5914: 59140W.1- 59140W.11.

129. E Candes, J Romberg and T Tao. Stable signal recovery from incomplete and inaccurate measurements. Comm. Pure Appl. Math, 2006, 59(8):1207-1223, DOI: 10.1002/cpa.20124.

130. T.Velmurugan and T.Santhanam, ‘’Computational Complexity between KMean and K-Medoids Clustering Algorithms for Normal and Uniform Distribution of Data Points’’, Journal of Computer Science, (2010), V.6, n.3, 363-368.

131. A Jain, M Murty, P Flynn, ‘’Data Clustering’’, A Review. ACM computing surveys, (1999), V.31, 264-323.

132. V Hodge, J Austin, ‘’A survey of outlier detection methodologies’’, Artificial intelligence review, (2004), V.22, n.2, 85-126.

133. P C Mahalanobis, ‘’On the generalized distance in statistics’’, In proceedings of the national institute of science, (1936), 49-55.

134. Shahla Ramzan, Faisal Maqbool Zahid and Shumila Ramzan, ‘’Evaluating Multivariate Normality: A Graphical Approach’’, Middle-East Journal of Scientific Research, (2013), V.13, n.2, 254-263,