Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études
Pour l'obtention du diplôme de Master en Informatique

Option: *Réseaux et Systèmes Distribués (R.S.D)*

Thème

Utilisation de l'apprentissage automatique pour la sécurité d'un réseau de radio cognitive

Réalisé par :

- **GHENNANI Hind Selma**
- **MEDJDOUB Wissam**

Présenté le 01 Juillet 2018 devant la commission composée de MM.

Président : - BENMAMMAR Badr

Encadreur : - AMRAOUI Asma

Examinateur : - BENMOUNA Youcef

Année universitaire: 2017-2018

Remerciements

Nous tenons tout d'abord à remercier Dieu le tout puissant et miséricordieux, qui nous a donné la force et la patience d'accomplir ce Modeste travail.

Nous tenons vivement à remercier Madame

« AMRAOUI Asma » qui a encadré notre travail. Nous sommes très reconnaissantes pour ses conseils, et ses remarques pertinentes. Qu'elle trouve ici l'expression de notre gratitude pour l'expérience et le savoir qu'elle a bien voulu partager avec nous, ainsi que pour tous les efforts qu'elle a déployé pour l'aboutissement de ce mémoire.

Nos vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail et de l'enrichir par leurs propositions.

Nous tenons à exprimer notre profonde gratitude et nos sincères remerciements à tous ceux qui ont contribué, de près ou de loin à l'élaboration de ce mémoire de fin d'étude. Aussi, nous tenons à remercier infiniment : Nos chers parents pour leur contribution, leur soutien et leur patience au long de nos études.

Dédicaces

J'ai tant cherché l'inspiration grâce à laquelle j'allais exprimer toute ma gratitude pour ceux qui m'ont permis d'en arriver là aujourd'hui. Je sais à présent que mes mots ne suffiront jamais.

Du moins je tiens à dédier ce modeste travail à celle qui m'a donné la vie, le symbole de tendresse, qui s'est sacrifié pour mon bonheur et ma réussite, à ma très chère mère.

A mon père, école de mon enfance, qui a été mon ombre durant toutes les années de mes études, et qui a veiller tout au long de ma vie à m'accompagner, à me donner l'aide et à me protéger.

Que dieu les garde et les protège.

A la mémoire de mes Grands-parents Le destin ne nous a pas laissé le temps pour jouir ce bonheur ensemble et de vous exprimer tout mon respect. Puisse Dieu tout puissant vous accorder sa clémence, sa miséricorde et vous accueillir dans son saint paradis.

A mama Téma, Hadja et Grand-Mère maternelle le symbole du respect et d'amour. Que ce modeste travail, soit l'expression des vœux que vous n'avez cessé de formuler dans vos prières. Que Dieu vous préserve santé et longue vie.

A mes oncles Bouziane, Mohamed et Toufik dont je ne cesserai jamais d'exprimer ma reconnaissance, mon respect et mon amour.

A mes chères frères et sœurs qui sont ce que j'ai de plus chers et qui ont toujours été là pour moi.

A mon très chère neveu « Youcef », et son père « Samir » qui serait en réalité un frère.

A mon binôme Wissam à qui je souhaite beaucoup de joie et de bonheur.

A ma famille et à tous mes amis qui m'ont aidé et accompagné.

Je dédie ce modeste travail qui résumera un long, riche et instructif cursus, à vous tous.

Hind Selma

Je dédie ce mémoire

A mes chers parents

Aucun mot, aucune dédicace ne saurait exprimer mon respect, ma considération et l'amour éternel pour les sacrifices que vous avez déployés pour mon instruction, mon éducation et mon bien être dans les meilleures conditions. Votre générosité et votre bonté ont toujours été un exemple pour moi.

Trouvez en ce travail le fruit de votre dévouement et l'expression de ma gratitude et mon profond amour. Puisse Dieu, le tout puissant, vous préserver et vous accorder santé, longue vie et bonheur.

A mon cher mari,

Ta patience, ton soutien et ton encouragement étaient la bouffée d'oxygène qui me ressourçait dans les moments pénibles. Merci pour tout et merci d'être toujours à mes côtés.

A ma chère belle mère

Je ne pourrais jamais exprimer le respect que j'ai pour toi. Tes prières, tes encouragements et ton soutien m'ont toujours été d'un grand secours. Puisse Dieu, le tout puissant te préserver du mal, te combler de santé, de bonheur et te procurer une longue vie.

A mes chers grands parents

Que ce modeste travail, soit l'expression des vœux que vous n'avez cessé de formuler dans vos prières. Je prie dieu le tout puissant pour qu'il vous préserve et pour qu'il vous procure santé et longue vie.

A ma chère sœur et mes chers frères, à qui je souhaite beaucoup de joie et de bonheur et un avenir très brillant.

A mon binôme Selma

Merci pour ta patience, ta tolérance, pour les bons moments qu'on a partagé, aussi pour ton soutien et ton dévouement à ce travail, je te dédie le fruit de nos efforts et te souhaite un avenir à la hauteur de tes ambitions.

***A ma grande famille** : à mes tantes, à mes oncles ainsi que tous mes cousins et cousines.*

*La dernière dédicace est pour mon petit bout de choux **Anas** à qui je souhaite le plus meilleur des parcours et une vie saine et joyeuse.*

Wissam

Résumé

La radio cognitive est une technologie qui permet d'améliorer considérablement l'utilisation du spectre radio en permettant d'exploiter le spectre sans fil de façon opportuniste. Dans notre mémoire, nous nous sommes intéressées à sécuriser un réseau de radio cognitive contre l'attaque PUE (Primary User Emulation). Pour cela, nous avons proposé une méthode Sécur PUE en utilisant l'algorithme TOPSIS pour choisir la meilleure offre et un autre algorithme pour l'apprentissage automatique qui est Naive bayes.

Mots-clés : Radio cognitive – Sécurité – Apprentissage automatique - Algorithme TOPSIS – Sécur PUE.

Abstract

Cognitive radio is a technology that improves the use of the radio spectrum by allowing opportunistic exploitation of the wireless spectrum. In our brieve dissertation, we are interested in securing the cognitive radio network against the PUE (Primary User Emulation) attack. For this, we proposed a Safe PUE method using the TOPSIS algorithm to choose the best offer and another algorithm for machine learning that is Naive bayes.

Keywords: Cognitive radio - Security - Machine Learning - TOPSIS Algorithm - Sécur PUE.

ملخص

الراديو المعرفي (الإدراكي) هو تقنية تعمل بشكل كبير على تحسين استخدام الطيف الراديوي من خلال السماح بالاستغلال الانتهازي للطيف اللاسلكي. في هذه المذكرة نحن مهتمون بتأمين شبكة الراديوية الإدراكية ضد هجوم محاكاة المستخدم الأساسي لهذا ، اقترحنا طريقة محاكاة المستخدم الأساسي المؤمن باستخدام خوارزمية الراديو المعرفي الأمثل لترتيب الافضليات عن طريق التشابه مع الحل المثالي لاختيار أفضل عرض وخوارزمية أخرى لتعلم التلقائي الآلي.

الكلمات المفتاحية : الراديو المعرفي - الأمن - التعلم التلقائي الآلي - خوارزمية الراديو المعرفي الأمثل - محاكاة المستخدم الأساسي المؤمن

Table de matières

Liste des figures

Liste des tableaux

Liste des abréviations

ACL : **A**ccess **C**ontrol **L**ist (Listes de Contrôle d'Accès)

CCS : **C**ontrol **C**hannel **S**aturation DoS (Saturation des canaux de contrôle)

CCSD :Control **C**hannel **S**aturation **D**oS Attack

CSMA : **C**arrier **S**ensing **M**ultiple **A**ccess

DDT : **D**istance **D**ifference **T**est (Test de Différence de Distance)

DoS : **D**enial **o**f **S**ervice (Déni de Service)

DRT : **D**istance **R**eport **T**est (Test de Rapport de Distance)

EG : **E**xponentiated **G**radient

EM: capteurs électromagnétiques

FCC: Commission **F**édérale des **C**ommunications

GKM : **G**roup **K**ey **M**anagement (Gestion de Clé de Groupe)

GPS : **G**lobal **P**ositioning **S**ystem (Géo-Positionnement parSatellite)

H : Utilisateur **H**onnête

IA: **I**ntelligence **A**rtificielle

IDE : Environnement de **D**éveloppement **I**ntégré

IDS : **I**ntrusion **D**etection **S**ystem (Système de détection d'intrusion)

JADE : Java **A**gent **DE**velopment Framework

JAVA : Langage de programmation informatique orienté objet

KTH : **K**ungliga **T**ekniska **H**ögskolan(Institut royal de technologie)

LocDef : **Loc**alization Based **Def**ense (Défense basée sur la localisation)

LV : **V**érificateurs de **L**ocalisation

M : Utilisateur **M**alveillant

MAC : **M**edia **A**ccess **C**ontrol (Couche de contrôle d'accès au support)

OFA : L'attaque de la fonction objective

PU :**P**rimary **U**ser (Utilisateur primaire)

PUE :**P**rimary **U**ser **E**mulation (Emulation de l'utilisateur Primaire)

RC : **R**adio **C**ognitive

RF : **R**adio **F**requency (Fréquence Radio)

RRC : **R**éseaux **R**adio **C**ognitive

RSS : **R**eceived **S**ignal **S**trength (Résistance du signal reçu)

SCN : **S**elfish **C**hannel **N**egociation (Négociation de canal égoïste)

SDR : **S**oftware **D**efind **R**adio (Radio logicielle Restreinte)

SSDF : **S**pectrum **S**ensing **D**ata **F**alsification

SU : **S**econdary **U**ser (Utilisateur secondaire)

TCP : **T**ransmission **C**ontrol **P**rotocol (Protocole de contrôle de transmissions)

TOPSIS : Technique for **O**rder of **P**reference by **S**imilarity to **I**deal **S**olution

WIFI : **WI**reless **FI**delity

WiMax : Worldwide Interoperability for Microwave Access

WSN : **W**ireless **S**ensor **N**etwork

WSPRT : **W**eighted **S**equential **P**robability **R**atio **T**est

WSRT : **W**eighted **S**equential **R**atio **T**est

Introduction générale

L'évolution des technologies sans fil a augmenté de plus en plus en passant d'une génération à une autre. Du mobile cellulaire de la première génération jusqu'à la 4éme génération. Le passage d'une génération à une autre a nécessité des débits plus élevés et des services de plus en plus évolués, ce qui impliqua une forte demande en termes de spectre électromagnétique qui est le support de transmission.

Le critère de vitesse de transmission étant quasi résolu, plusieurs autres paramètres posaient encore problème, comme la protection des données et des informations liés aux utilisateurs, la sécurisation des messages transmis et l'optimisation de l'utilisation des bandes de fréquences par les utilisateurs car il y a un important blocage à cause de la pénurie du spectre.

Pour ce dernier point, la pénurie du spectre, des chercheurs ont remarqué qu'un utilisateur n'est pas connecté 24h/24 et pendant son absence, un potentiel énorme en terme de temps et de débit de connexion est inexploité. Comment pouvions nous alors utilisé ce potentiel, afin d'en faire profiter d'autres utilisateurs ? Comment remédier au problème de saturation du spectre ? Comment reconnaitre les bons des mauvais utilisateurs ?

La radio cognitive (RC) est une nouvelle approche de communications sans fil, elle a ainsi apporté les réponses à toutes ces questions. Elle va permettre à une bande de fréquence d'être la propriété de tout le monde et non d'un seul utilisateur. Un abonné principal dit primaire, peut faire profiter un autre utilisateur, dit secondaire, de son canal lorsqu'il n'en a plus besoin. L'utilisateur primaire peut alors à tout moment récupérer son canal obligeant alors l'utilisateur secondaire à se connecter ailleurs. La connexion au réseau est ainsi optimisée et tous les utilisateurs sont satisfaits.

La radio cognitive permet aussi de résoudre le problème de la rareté du spectre et de garantir une meilleure qualité de service aux utilisateurs.

Reste cependant à aborder l'aspect de la sécurité qui est la problématique majeure de notre travail qui consiste à proposer une méthode pour se défendre contre l'attaque PUE (Primary User Emulation) qui est une attaque spécifique pour les Réseaux de RC.

L'objectif de notre travail est alors d'utiliser la notion d'apprentissage automatique pour détecter la nature de l'utilisateur (honnête ou malveillant) et ensuite proposer une méthode pour sécuriser le réseau RC.

Le mémoire est divisé en trois chapitres: Le premier est spécialement consacré à l'univers de la RC où nous allons introduire le concept de la radio cognitive ainsi que sa frontière avec la radio logicielle. Après cela, nous allons détailler les différents aspects

utilisés par cette technologie : principe, architecture, cycle de cognition, fonctions et composantes. Ensuite nous allons clôturer le chapitre par des notions sur l'apprentissage automatique.

Dans le deuxième chapitre, nous allons aborder l'aspect de sécurisation des réseaux radio cognitive, les principes et fondamentaux d'une sécurité et comment faire face aux menaces et attaques auxquelles sont confrontés les utilisateurs dans les réseaux radio cognitive ainsi que les solutions proposées.

Enfin, nous allons détailler dans le troisième chapitre les étapes de notre contribution par le développement d'une application où l'utilisateur secondaire pourra facilement reconnaître, grâce à des algorithmes que nous avons élaboré, un danger quand il se présentera devant lui et l'éviter ainsi en choisissant l'utilisateur le plus sûr pour sa connexion. Enfin nous allons présenter les résultats obtenus.

CHAPITRE I : Radio cognitive

I. CHAPITRE I : Radio cognitive

I.1 Introduction

Depuis quelques années les systèmes de télécommunication ont évolué d'une façon exponentielle, grâce à la demande croissante des utilisateurs de technologie sans fil qui sont devenues indispensables au quotidien, Mais ce développement est en train d'engendrer un blocage à cause de la pénurie du spectre. Ce qui a conduit à la recherche de solutions destinées à résoudre ce problème, ainsi une nouvelle technologie appelée radio cognitive (RC) est apparue.

La radio cognitive est une technologie clé de la future cinquième génération qui pourrait révolutionner le monde des réseaux sans fil et qui permet aux terminaux comme les téléphones sans fil de communiquer entre eux grâce à l'intelligence artificielle.

La radio cognitive apporte une gestion dynamique du spectre dont l'objectif principal est de résoudre le problème de l'insuffisance du spectre, et de garantir une meilleure qualité de service aux utilisateurs selon leurs nécessités.

Il y a plusieurs techniques pour l'accès dynamique au spectre dont l'apprentissage automatique qui est une technique de science des données qui permet aux ordinateurs d'utiliser des données existantes afin de prévoir les tendances, les résultats et les comportements futurs.

Nous allons étudier dans ce chapitre la radio cognitive dans ses différents aspects: principes, architecture, cycle de cognition, fonctions et composantes, ainsi que l'apprentissage automatique dans la RC.

I.2 Radio logicielle

La Radio logicielle (Software Radio) est une évolution logique inventée par Joseph Mitola en 1991 pour définir une classe de radio reprogrammable et reconfigurable.

La radio logicielle est une convergence des radios numériques et des technologies logicielles dans laquelle les fonctions de l'interface radio généralement réalisées en matériel et les fonctions (fréquence porteuse, la largeur de bande du signal, la modulation et l'accès au réseau) sont réalisés en logicielle. La radio logicielle moderne met également en œuvre l'implantation logicielle des procédés cryptographiques, codage correcteur d'erreur, codage source de la voix, de la vidéo ou des données.

La radio logicielle est le but ultime intégrant toutes les fonctionnalités en logiciel, mais elle impose des phases intermédiaires combinant anciennes et nouvelles techniques, on parle alors de radio logicielle restreinte (SDR : Software Defined Radio). Les contraintes de puissance de calcul, de consommation électrique, de coûts, etc. imposent actuellement de passer par cette phase intermédiaire [1].

I.2.1 Radio logicielle restreinte

Une radio logicielle restreinte est un système de radiocommunication configurable utilisant des techniques de traitement numérique du signal sur des circuits numériques programmables. Sa flexibilité lui permet de s'adapter à différents protocoles de radiocommunication, et de répondre au besoin croissant de performance et d'interopérabilité entre systèmes. L'objectif de la SDR consiste en une dématérialisation complète de l'interface radio. Elle participe à la tendance globale des circuits électroniques à devenir des circuits à haute densité d'intégration [2].

I.2.2 Relation entre RC et SDR

La capacité de s'adapter à modifier les paramètres (fréquence porteuse, puissance, modulation, bande passante) en fonction de : (L'environnement radio, la situation, les besoins de l'utilisateur, l'état du réseau, la géo localisation…) est l'une des principales caractéristiques de la radio cognitive.

La radio logicielle est capable d'offrir les fonctionnalités de flexibilité, de reconfigurabilité et de portabilité inhérente à l'aspect d'adaptation de la radio cognitive.

Par conséquent, cette dernière doit être mise en œuvre autour d'une radio logicielle. En d'autres termes, la radio logicielle est une "technologie habilitante" pour la RC [3].

La RC englobe le concept de la radio logicielle. En effet, elle comporte des fonctions logicielles supplémentaires qui permettent une reconfiguration optimale [12].

La figure I.1 montre la relation entre la RC et la SDR.

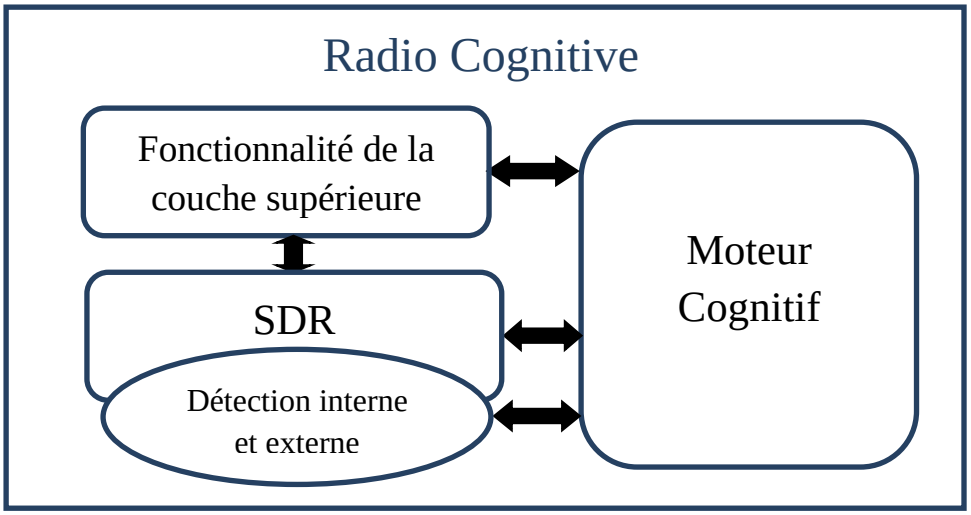

Figure I.1:Relation entre la RC et la SDR.

I.3 Radio Cognitive

I.3.1 Historique

Le terme « radio cognitive » a été créé officiellement par un génie en la matière qui n'est autre que Joe Mitola lors d'un séminaire à l'institut royale de technologie (KTH, Stockholm, Suède) en 1998.

Le concept a été soutenu au départ par la Défense américaine, publié plus tard en 1999 dans un article de Mitola et KTH professeur de communications Gerald Q. Maguire, [4] et en 2000 il l'a publié dans sa Thèse de doctorat [5].

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. D'après lui : « Une radio cognitive peut connaître, percevoir et apprendre de son environnement puis agir pour simplifier la vie de l'utilisateur » [6].

I.3.2 Définition

La cognition a été décrite, à partir des années 1950, comme un système de traitement de l'information créant et manipulant des représentations mentales du monde.

Cette description a été fortement influencée par le développement rapide de l'informatique à la fin des années 1940 [7].

La radio cognitive est donc un système doté de capacités cognitives qui permettent à un terminal d'acquérir une connaissance sur son environnement, d'avoir une vision des ressources radio disponibles et enfin de lui donner la possibilité d'exploiter ces bandes inutilisées pour aboutir à une gestion plus efficace du spectre radio.

Plusieurs définitions ont été présentées par d'autres auteurs pour décrire la radio cognitive. Parmi elles, celle d'Akyildiz [8] qui considère la radio cognitive comme étant la technologie clé qui permettra aux réseaux de nouvelle génération d'utiliser et de partager le spectre de manière opportuniste.

Selon Haykin [9], la radio cognitive représente un système de communication sans fil intelligent qui est conscient de son environnement et qui utilise les méthodologies "understanding-by-building" (compréhension par construction) afin d'étudier son environnement et de s'adapter aux différentes variations statistiques. Ainsi, deux principaux objectifs sont pris en compte dans cette définition : (1) la communication fortement fiable au besoin, et (2) l'utilisation efficace du spectre radio.

La Commission Fédérale des Communications (FCC) [10] définit la radio cognitive comme étant une radio qui peut changer les paramètres de son émetteur sur la base des interactions avec l'environnement dans lequel elle opère.

I.3.3 Principe

Le concept d'accès dynamique au spectre est assuré par deux acteurs principaux

a) Utilisateurs Primaires (PU)

Connu aussi comme « utilisateurs licenciés ou utilisateurs prioritaires », sont des utilisateurs qui disposent d'une licence et des droits de communications en toute autonomie qui leur permet d'opérer à n'importe quel moment sur des bandes spectrales qui leurs sont réservées.

L'accès est contrôlé uniquement par ces stations de base et ne doit pas subir d'interférences extérieures nuisibles. Les PU (Primary Users) ne doivent subir aucune

modification pour permettre la coexistence avec les utilisateurs ou réseaux de radio cognitive ou leur station de base [11].

b) Utilisateurs Secondaires (SU)

C'est les utilisateurs qui n'ont pas de licence, Ils accèdent au spectre de façon opportuniste et ils doivent veiller à ne pas interagir avec les utilisateurs primaires, Les SU(Secondary users) devront céder une fois le service est achevé et devront surveiller à ne pas gêner les utilisateurs primaires.

La radio cognitive a l'objectif globale d'ouvrir les bandes licenciées au niveau du spectre à ces SU sans brouiller les communications des PU qui sont seuls admis de l'utiliser.

I.4 Architecture de la radio cognitive

La radio cognitive est définie par un ensemble cohérent de règles de conception par lequel un ensemble spécifique de composants réalise une série de fonctions de produits et de services, comme décrit la figure I.2 :

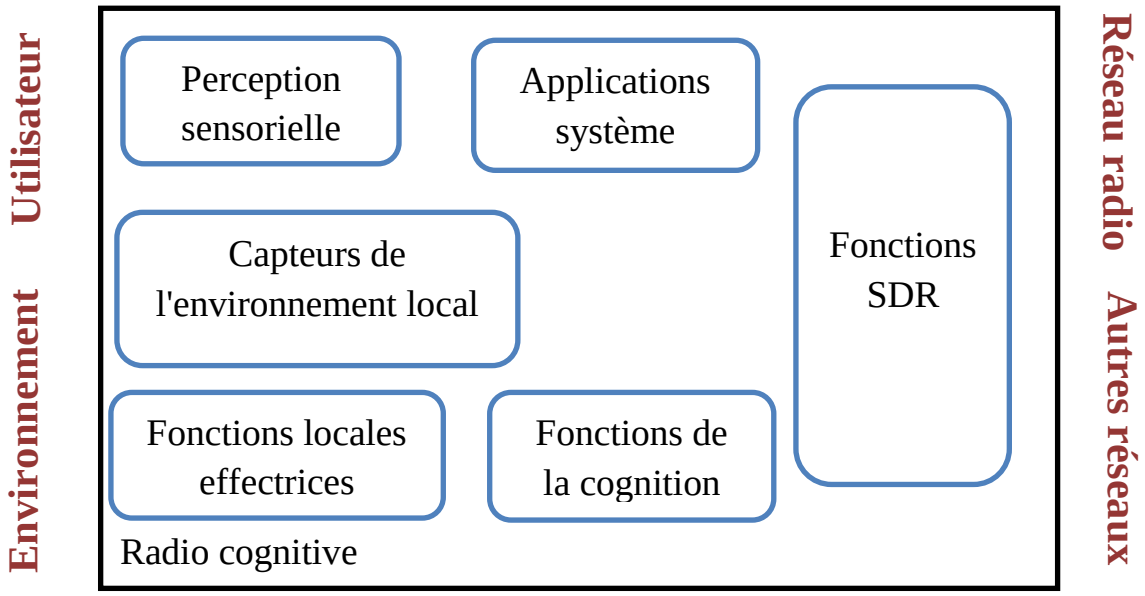

Figure I.2 : Architecture de la radio cognitive.

Les six composantes fonctionnelles de l'architecture d'une radio cognitive sont :

- La perception sensorielle de l'utilisateur intègre l'interface haptique (du toucher), acoustique, la vidéo et les fonctions de détection et de la perception.

- Les capteurs de l'environnement local (emplacement, la température, l'accéléromètre, compas, etc.).
- Les applications système (les services médias indépendants comme un jeu en réseau).
- Les fonctions SDR (qui comprennent la détection RF et les applications radio de la SDR).
- Les fonctions de la cognition (pour les systèmes de contrôle, de planification, de l'apprentissage).
- Les fonctions locales effectrices (synthèse de la parole, du texte, des graphiques et des affiches multimédias).

I.5 Cycle de cognition

La composante cognitive de l'architecture de la radio cognitive comprend une organisation temporelle, des flux d'inférences et des états de contrôle. Ce cycle synthétise cette composante de manière évidente. Les stimuli entrent dans la radio cognitive comme des interruptions sensorielles envoyées sur le cycle de la cognition pour une réponse. Une telle radio cognitive observe l'environnement, s'oriente, crée des plans, décide, et puis agit [13] comme le montre la figure ci-dessous.

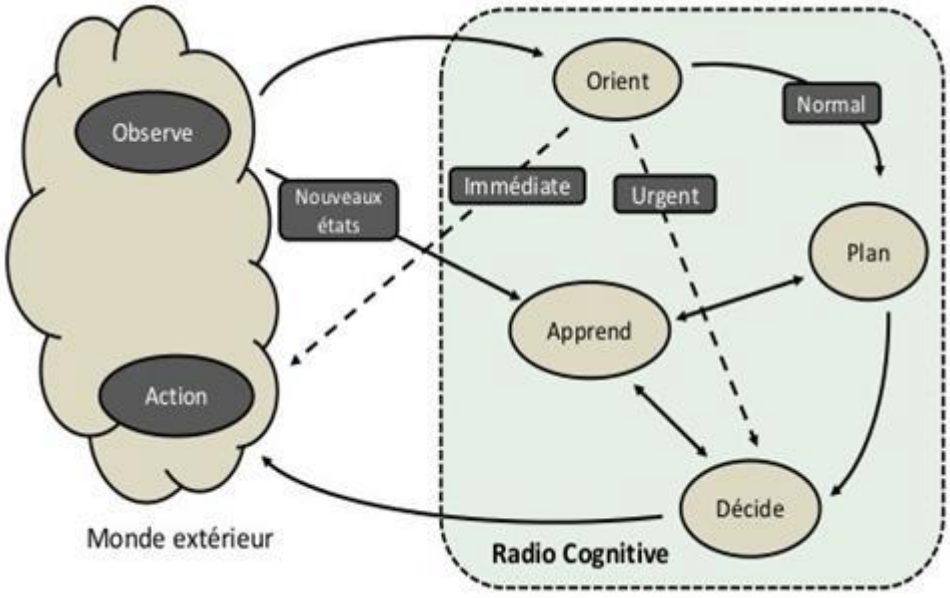

Figure I.3: Cycle de cognition.

Les différentes étapes du cycle cognitif sont les suivantes :

- **Observation:** Extraire plusieurs informations à partir de l'environnement comme la fréquence radio, le type de données transmises (audio, vidéo, etc.), la position, etc.

Exemples de capteurs électromagnétiques (EM) :

- Détecteur de bande libre,
- Radiomètre,
- Reconnaissance aveugle de standards,
- Estimateur de réponse impulsionnelle de canal,
- Détecteur d'angles d'arrivées,
- Détecteur de positionnement,
- Détection d'autres personnes ou équipements radio [14]

- **Orientation:** Cette étape est majeure dans l'établissement des priorités, la classification par affinité ou en fonction de la demande et du besoin, et elle fait référence à la façon de déterminer s'il y a besoin d'une action urgente ou si une planification à long terme est plutôt nécessaire.
- **Planification:** Identifier les actions alternatives à prendre et consiste en la prise de décisions à long terme.
- **Décision:** Décider entre les actions candidates, en choisissant la meilleure d'entre elles.

  Exemples de prise de décision et apprentissage en lien avec l'EM :
  - Taux d'occupation des bandes de fréquence,
  - Libération de la bande pour un utilisateur primaire,
  - Coordination avec d'autres utilisateurs secondaires…
- **Action:** Agir sur l'environnement en effectuant, par exemple, des modifications au niveau de la fréquence radio.

  Exemples de reconfiguration (radio logicielle) en lien avec l'EM :
  - Fréquence d'émission et/ou réception,
  - Conversion de fréquence d'échantillonnage,
  - Filtrage mono/multi-canal…

- **Apprentissage :** dépend de la perception, des observations, des décisions et des actions. L'apprentissage initial est réalisé à travers la phase d'observation dans laquelle toutes les perceptions sensorielles sont continuellement comparées à l'ensemble de l'expérience antérieure pour continuellement compter les événements et se souvenir du temps écoulé depuis le dernier évènement.

L'apprentissage peut se produire quand un nouveau modèle est créé en réponse à une action [3].

I.6 Composantes de la radio cognitive

Les différentes composantes d'un émetteur/récepteur radio cognitive qui mettent en œuvre ces fonctionnalités sont présentées dans la figure ci-dessous [15]

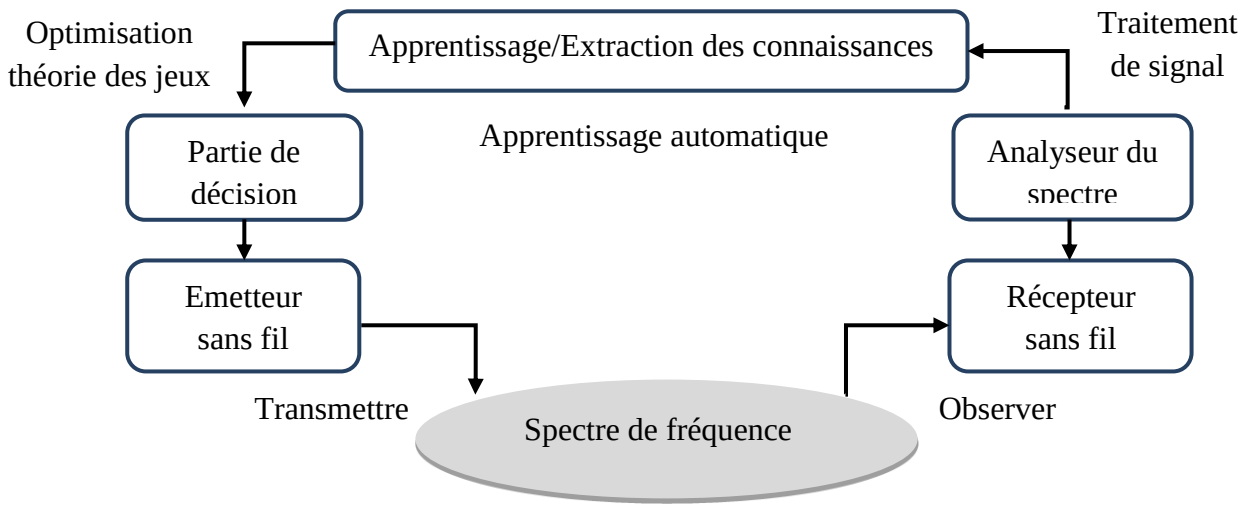

Figure I.4:Composantes de la radio cognitive.

- **Emetteur/Récepteur :** un émetteur/récepteur SDR sans fil est le composant majeur avec les fonctions du signal de transmission de données et de réception. En outre, un récepteur sans fil est également utilisé pour observer l'activité sur le spectre de fréquence (spectre de détection).

- **L'analyseur de spectre (Spectrum analyser) :** doit s'assurer que la transmission d'un utilisateur primaire n'est pas perturbée si un utilisateur secondaire décide d'accéder au spectre. Dans ce cas, diverses techniques de

traitement du signal peuvent être utilisées pour obtenir des informations sur l'utilisation du spectre.

- **L'apprentissage et l'extraction de connaissances (learnig / Knowledge extraction)** : Utilisent les informations du spectre pour comprendre l'environnement ambiant RF (par exemple le comportement des utilisateurs sous licence). Une base de connaissances de l'environnement d'accès au spectre est construite et entretenue, qui est ensuite utilisée pour optimiser et adapter les paramètres de transmission pour atteindre l'objectif désiré sous diverses contraintes. Les algorithmes d'apprentissage peuvent être appliqués pour l'apprentissage et l'extraction de connaissances.

- **Prise de décision (Decisionmaking) :** Après que la connaissance de l'utilisation du spectre soit disponible, la décision sur l'accès au spectre doit être faite. La décision optimale dépend du milieu ambiant, elle dépend du comportement coopératif ou compétitif des utilisateurs secondaires. Différentes techniques peuvent être utilisées pour obtenir une solution optimale.

I.7 Fonction de la Radio cognitive

L'objectif principal de la radio cognitive consiste à gérer le spectre de manière opportuniste de manière à optimiser l'exploitation des ressources radio disponibles.

Les fonctions principales de la RC sont :

I.7.1 Détection du spectre (Spectrum Sensing)

Détecter le spectre non utilisé et le partager avec d'autres utilisateurs sans interférences. La détection des utilisateurs sous licence PU est la façon la plus efficace pour détecter les spectres temporellement inutilisés.

I.7.2 Gestion du spectre (Spectrum Management)

Capter les meilleures fréquences disponibles pour répondre aux besoins de communication des utilisateurs.

Les radios cognitives devraient décider de la meilleure bande de spectre pour répondre aux exigences de qualité de service sur toutes les bandes de fréquences disponibles, donc les fonctions de gestion du spectre sont nécessaires pour les radios cognitives. Ces fonctions de gestion peuvent être classées comme suit : [16].

a) Analyse du spectre

Analyser les résultats de la détection du spectre pour estimer la qualité du spectre (la durée moyenne, le taux d'erreur dans le canal, la disponibilité des espaces blancs du spectre, l'activité du PU et le débite). De nombreuses techniques sont employées par les utilisateurs de la radio cognitive pour analyser le spectre, tel que les algorithmes d'apprentissages de l'intelligence artificielle.

b) Décision sur le spectre

Cette fonction est nécessaire pour l'accès au spectre, elle dépend des résultats retenus par la phase d'analyse du spectre ; une multitude de règles décisionnelles sont appliquées dans le but de déterminer la ou les bandes les plus adaptées à la transmission en cours [17].

I.7.3 Partage du spectre (Spectrum Sharing)

Lorsque plusieurs utilisateurs (à la fois primaires et secondaires) sont dans le système, leur préférence va influer sur la décision du spectre d'accès. Ces utilisateurs peuvent être coopératifs ou non coopératifs dans l'accès au spectre. Dans un environnement non-coopératif, chaque utilisateur a son propre objectif, tandis que dans un environnement coopératif, tous les utilisateurs peuvent collaborer pour atteindre un seul objectif [16].

I.7.4 Mobilité du spectre (Spectrum mobility)

C'est le processus qui permet à l'utilisateur de la radio cognitive de changer sa fréquence de fonctionnement.

Les réseaux radio cognitives essayent d'utiliser le spectre de manière dynamique en permettant à des terminaux radio de fonctionner dans la meilleure bande de

fréquence disponible, de maintenir les exigences de communication transparentes au cours de la transition à une meilleure fréquence [18].

I.8 Apprentissage automatique dans la RC

I.8.1 Définition

L'apprentissage automatique connue aussi comme (Apprentissage artificiel ou machine learning) qui est un sous-domaine de l'intelligence artificielle (IA) fait référence au développement, à l'analyse et à l'implémentation de méthodes qui permettent à une machine d'évoluer grâce à un processus d'apprentissage, et ainsi de remplir des tâches qu'il est difficile ou impossible de remplir par des moyens algorithmiques plus classiques. D'après Marvin Minsky « L'apprentissage permet des modifications utiles dans notre cerveau ». [68]

Objectif : extraire et exploiter automatiquement l'information présente dans un jeu de données.

I.8.2 Architecture de la RC avec l'apprentissage automatique

L'apprentissage automatique peut être appliqué à la RC pour la maximisation des capacités d'accès au spectre dynamique comme le montre la figure I.5.

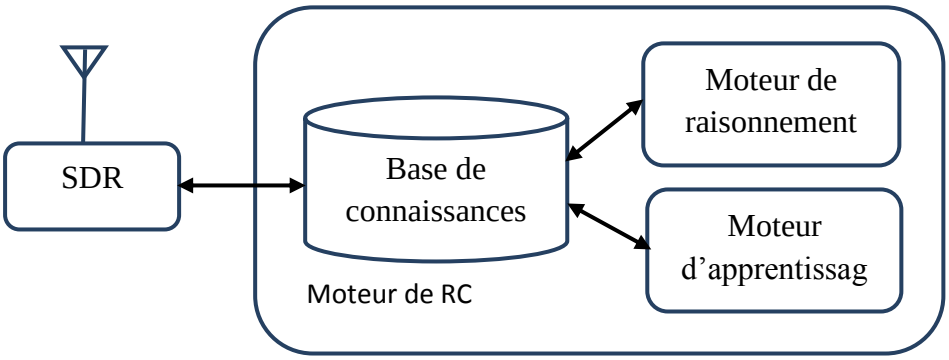

Figure I.5: Architecture de la RC avec l'apprentissage automatique.

- **<u>Le moteur de raisonnement (Reasoning engine)</u> :** utilise la base de connaissances pour choisir la meilleure action.

- **Le moteur d'apprentissage (Learning engine) :** Effectue la manipulation des connaissances basées sur l'information observée (par exemple des informations sur la disponibilité des canaux, le taux d'erreur dans le canal).
- **La base de connaissances (knowledge base) :** Maintient les états du système et les actions disponibles. Elle contient deux structures de données :
  - Le prédicat (règle d'inférence) est utilisé pour représenter l'état de l'environnement. Sur la base de cet état.
  - L'action qui peut être effectuée pour modifier l'état de telle sorte que les objectifs du système peuvent être réalisés.

I.8.3 Méthodes d'apprentissage automatique

Les algorithmes d'apprentissage peuvent se catégoriser selon la méthode d'apprentissage qu'ils emploient :

a) Apprentissage supervisé

L'apprentissage supervisé est formé avec des algorithmes basés sur des données d'entrée et de sortie étiquetées par un expert. Le processus se passe en deux phases :

- **1ère phase (Phase d'apprentissage) :** Déterminer un modèle des données étiquetées c'est-à-dire des données composées d'exemples de réponses souhaitées.
- **2ème phase (Phase de test):** Prédire l'étiquette d'une nouvelle donnée, connaissant le modèle préalablement appris.

L'apprentissage supervisé utilise des modèles pour prédire les valeurs d'étiquettes sur des données non étiquetées supplémentaires. [1]

La figure I.6 montre le fonctionnement de l'apprentissage supervisé.

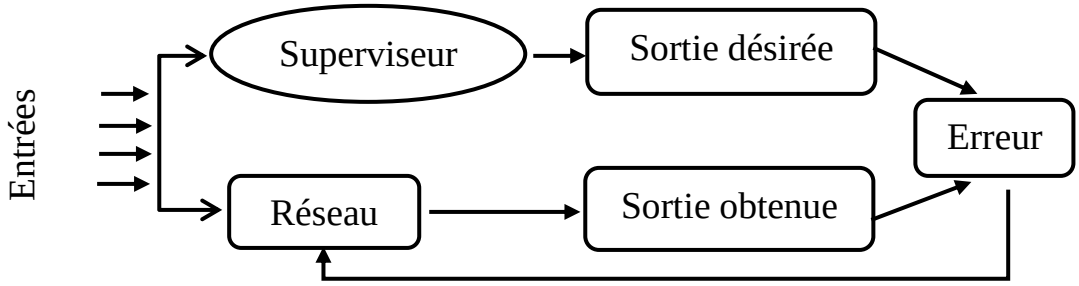

Figure I.6:Apprentissage supervisé.

b) Apprentissage non supervisé

L'apprentissage non supervisé est utilisé sur les données non étiquetées, de sorte que l'algorithme d'apprentissage doit découvrir par lui-même les points communs parmi ses données d'entrée. Il ne nécessite aucun expert.

La figure I.7 montre le fonctionnement de l'apprentissage non supervisé.

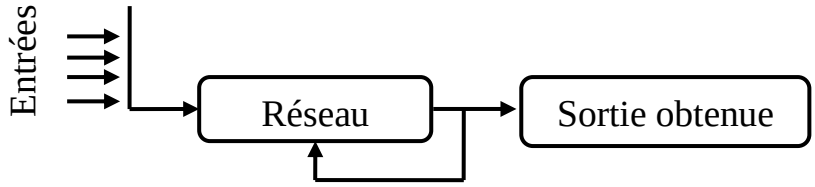

Figure I.7: Apprentissage non supervisé.

c) Apprentissage par renforcement

- L'agent intelligent observe les effets de ses actions, déduit de ses observations la qualité de ses actions et améliore ses actions futures.
- L'agent intelligent décide d'effectuer une action en fonction de son état pour interagir avec son environnement. L'environnement lui renvoie un renforcement sous la forme d'une récompense positive ou négative. Charge ensuite à l'agent de maximiser ce renforcement.
- L'algorithme apprend un comportement étant donné une observation.
- L'action de l'algorithme sur l'environnement produit une valeur de retour qui guide l'algorithme d'apprentissage.
- Les décisions sont prises séquentiellement à des intervalles de temps discrets.
- L'apprentissage par renforcement se distingue des autres approches d'apprentissage par plusieurs aspects :
- L'apprentissage se fait sans supervision
- Il repose sur le principe d'essai/erreur

I.8.4 Données d'Apprentissage

Les données d'apprentissage sont réparties en 3 catégories :

- **Ensemble d'apprentissage ou population d'entrainement :** constitue l'ensemble des candidats ou exemples (images, attributs…) utilisés pour générer le modèle d'apprentissage.

- **Ensemble de Test :** est constitué des candidats sur lesquels sera appliqué le modèle d'apprentissage (pour tester et corriger l'algorithme).
- **Ensemble de validation :** peut être utilisé lors de l'apprentissage (comme sous population de l'ensemble d'apprentissage) afin de valider (intégrer) le modèle et d'éviter le sur apprentissage.

I.8.5 Applications

Comme application de l'apprentissage automatique dans la RC, nous pouvons citer un travail de C. Clancy et al, [27] où un modèle concret pour une radio cognitive générique a été décrit pour utiliser un moteur d'apprentissage. L'objectif est d'intégrer les résultats du moteur d'apprentissage dans un moteur de raisonnement basé sur le calcul des prédicats afin que les radios puissent se souvenir des leçons apprises dans le passé et agir rapidement dans le futur.

Les auteurs ont essayé de formaliser l'application des algorithmes d'apprentissage automatique à la radio cognitive, et de développer un cadre dans lequel ils peuvent être utiles ainsi le moteur cognitif générique proposé, peut résoudre des problèmes tels que la maximisation de la capacité et l'accès dynamique au spectre. Plusieurs algorithmes d'apprentissage dédiés à la RC ont été évoqués par les auteurs tel que : « hidden Markov models » [28], « neural networks » [29], and « genetic algorithms » [30].

L'algorithme de Perceptron [20, 21, 22] est peut-être le premier et le plus simple algorithme d'apprentissage et il servira de point de départ. Le Perceptron est conçu pour répondre aux questions oui / non.

L'utilisation de l'apprentissage automatique pour des problèmes de prédiction plus complexes a été davantage abordée par plusieurs auteurs. Quelques exemples notables sont la régression multidimensionnelle [26], l'entraînement discriminatif des modèles de Markov cachés [23], et les problèmes de classement [24, 25].

Une autre étude sur la prédiction des spectres a été réalisée par Zhang et al, [31] où les auteurs ont proposé une nouvelle stratégie de prédiction de spectre et de sélection de canal utilisant des techniques d'apprentissage automatique, qui comprend trois étapes:

1) SU utilise des techniques d'apprentissage automatique pour la régression de la puissance émise.
2) SU prédit la probabilité de l'état de chaque utilisateur principal (occupé / inactif) en fonction des résultats de la régression de puissance.
3) SU optimise la sélection des canaux en termes de capacités ergodiques attendues à partir des résultats de prédiction.

La stratégie de prédiction de spectre souple basée sur la régression de puissance permet au SU d'exploiter les historiques de puissance de transmission des PU et de prédire les probabilités des statuts des PU. Le SU appliquera ensuite une stratégie de sélection de canal optimisée pour maximiser son attente de débit à l'intervalle de temps suivant. Les résultats de la simulation valident la supériorité de la stratégie proposée par rapport à d'autres classiques.

I.9 Conclusion

Dans ce chapitre, nous avons présenté l'apprentissage automatique dans la RC, les différents aspects de la radio cognitive et expliqué le principe de son fonctionnement ainsi que sa frontière avec la radio logicielle. Nous avons vu aussi les domaines d'application de l'apprentissage automatique.

La RC va garantir une bande passante plus large aux utilisateurs grâce aux techniques d'accès dynamique au spectre. Elle permet d'exploiter le spectre de façon opportuniste et permet de résoudre les problèmes des réseaux sans fil actuels résultant de la limitation et de l'utilisation inefficace du spectre. Toutes ces techniques doivent être coordonnées avec des algorithmes hautement sophistiqués afin d'avoir la technologie la plus aboutie possible.

L'apprentissage automatique est un domaine en constante innovation, il est important de garder à l'esprit que les algorithmes, les méthodes et les approches continueront de changer.

Dans le chapitre suivant on va présenter les notions fondamentales de la sécurité ainsi que les différentes attaques contre le Réseau Radio Cognitive.

CHAPITRE II : Sécurisation du Réseau Radio Cognitive

II. CHAPITRE II : Sécurisation du Réseau Radio Cognitive

II.1 Introduction

Le réseau de radio cognitive est une nouvelle technologie qui se caractérise par son intelligence et qui s'adapte aux changements de son environnement pour mieux utiliser le spectre. Les RRC (Réseaux Radio Cognitive) aident à résoudre le problème de la pénurie de spectre en permettant aux SU de coexister avec les PU sans causer d'interférence. Cette technologie permet la coexistence et le partage de ressources de spectre sous licence entre deux types d'utilisateurs, PU et SU. Les nœuds radio cognitive ont des capacités uniques qui leur permettent de profiter des espaces blancs disponibles dans un spectre.

L'utilisation des réseaux de radio cognitive comprend la correction et la construction des mesures de sécurité pour lutter contre les attaques. Nous catégorisons les attaques sur les RRC en quatre classes principales : les attaques de la couche physique, les attaques de la couche de liaison, les attaques de couche de réseau et les attaques de la couche de transport [33].

Dans ce chapitre, une brève introduction sur la sécurité est étudiée suivi par les différentes attaques qui ciblent le réseau de radio cognitive. Nous classons les attaques en fonction de la couche qu'elles ciblent en commençant par la couche physique et en remontant vers la couche transport.

II.2 Fondamentaux sur la sécurité informatique

II.2.1 Définition de la sécurité

La sécurité est un enjeu majeur des technologies numériques modernes (Infrastructures de télécommunication, Internet, réseaux sans fils (Bluetooth, Wifi, WiMax), routeurs, ordinateurs, téléphones, décodeurs de télévision, systèmes d'exploitation, applications informatiques...) toutes ces entités présentent des vulnérabilités : faille de sécurité, défaut de conception ou de configuration.

La sécurité est un ensemble de mécanisme destinés à protéger l'information des utilisateurs n'ayant pas l'autorisation de la manipuler et d'assurer les accès autorisés, son objectif est :

- Eliminer / réduire les risques posant sur la sécurité informatique.
- Sensibiliser les menaces et enjeux.
- Présenter le problème de la sécurité posé par les ressources informatique et réseau.

II.2.2 Les principes de la sécurité

II.2.2.1 Authentification

L'authentification est le processus effectué par une entité pour confirmer l'identité d'une autre entité. Comme les mots de passe, les signatures numériques ou les codes d'authentification de message qui sont des techniques communes d'authentification.

II.2.2.2 Autorisation

L'autorisation est le processus où on accorde des privilèges aux utilisateurs sur l'accès à un ensemble de ressources selon ce qu'on leurs permet. Les techniques les plus populaires pour imposer l'autorisation sont de maintenir les listes de contrôle d'accès (ACL) énumérant les droits d'accès de l'entité.

II.2.2.3 Disponibilité

La propriété qu'un bien doit être disponible au moment voulu. L'objectif des attaques sur la disponibilité est de rendre le système inexploitable ou inutilisable.

II.2.2.4 Intégrité

L'intégrité vise à assurer que les ressources et les informations ne soient pas corrompues, altérées ou détruites par des sujets (des personnes, des machines ou des logiciels) non autorisés.

II.2.2.5 Confidentialité

Vise à assurer que seuls les sujets (les personnes, les machines ou les logiciels) autorisés aient accès aux ressources et aux informations auxquelles ils ont droit. La confidentialité a pour objectif d'empêcher que des informations secrètes soient divulguées à des sujets non autorisés.

II.3 Sécurité dans la Radio Cognitive

II.3.1 Les attaques de la couche physique (physical layer attacks)

La couche physique est constituée de tout support physique utilisé pour communiquer entre eux deux dispositifs de réseau, tels que les cartes réseau, la fibre, les câbles ou l'atmosphère, comme dans les réseaux de radio cognitive. Le fonctionnement du RRC est plus compliqué que d'autres réseaux de communication sans fil car la RC utilise dynamiquement le spectre de fréquences. La détection du spectre est la première étape pour utiliser les bandes de spectre non attribuées, et comme l'atmosphère est le milieu de ce qui est ouvert au public, la couche physique est vulnérable à de nombreuses menaces qui attaquent le processus de détection du spectre.
Les attaques réseau visant à perturber la communication en ciblant la couche physique du RRC sont :

II.3.1.1 Emulation de l'utilisateur Primaire (PUE : Primary User Emulation)

Un attaquant PUE peut se faire passer pour un PU en transmettant des signaux spéciaux dans la bande sous licence, empêchant ainsi d'autres utilisateurs secondaires d'accéder à cette bande. Dans les attaques PUE, l'attaquant ne transmet que sur les canaux qui ne sont pas utilisés par les utilisateurs primaires. Par conséquent, les utilisateurs secondaires considèrent les attaquants comme des utilisateurs primaires et n'essaient pas d'accéder aux canaux non utilisés par les utilisateurs primaires.[31] La figure ci-dessous montre le mécanisme de l'attaque PUE :

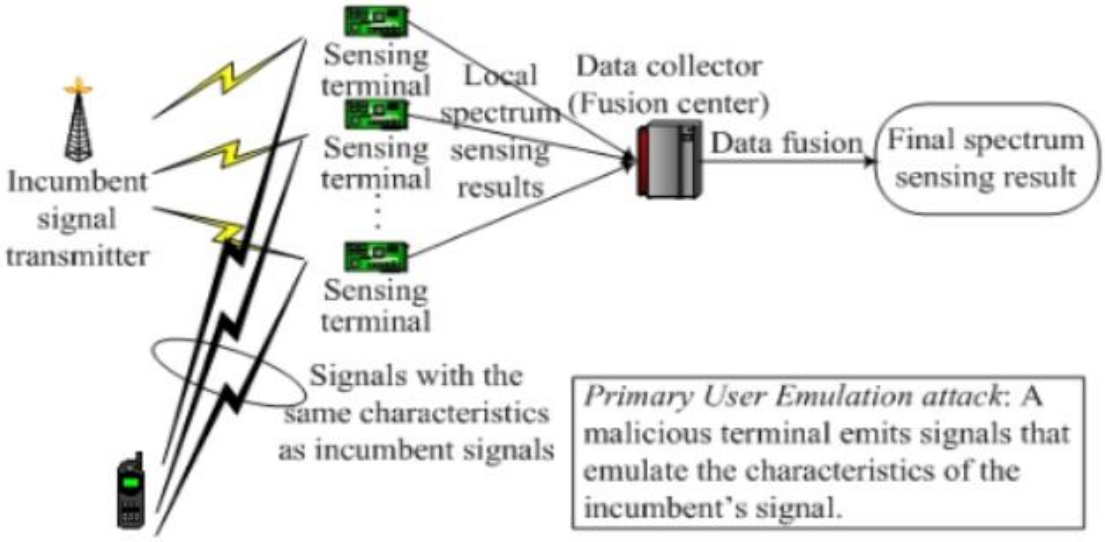

Figure II.1 : l'attaque PUE.

En lançant une attaque PUE dans plusieurs bandes de manière circulaire, un attaquant peut effectivement limiter les utilisateurs secondaires légitimes à l'identification et à l'utilisation des espaces blancs d'un spectre.

Les informations sur le RRC facilitent le fonctionnement des attaques PUE. Un exemple sur l'attaque PUE : l'attaquant profite du temps où les SU se refusent la transmission pour bien détecter le spectre. Un deuxième exemple quand le dispositif radio cognitive fait un changement de fréquence (Handoff), l'attaque peut être conduite à un faible débit ou entièrement à un DoS [36].

❖ **Types d'attaque PUE**

- **L'attaque PUE égoïste :** Lorsque l'attaquant détecte la bande du spectre non utilisée il transmet des signaux qui émulent les caractéristiques du signal d'un PU et empêchent les SU de l'utiliser. Ainsi, l'attaquant peut utiliser les canaux qui ne sont pas utilisés par les PU.
- **L'attaque PUE malveillant :** l'attaquant essaie simplement d'empêcher les SU autorisés d'utiliser les espaces blancs d'un spectre.

Il existe d'autres attaques PUE plus complexes. Certains attaquants peuvent même attaquer uniquement lorsque le PU est éteint, ce qui signifie que les attaquants peuvent économiser de l'énergie[32].

❖ **Solutions contre l'attaque PUE**

Les solutions pour se défendre contre l'attaque PUE sont :

- **Test de Rapport de Distance (DRT) :** basé sur les mesures de la force du signal reçu.
- **Test de Différence de Distance (DDT) :** basé sur la différence de la phase du signal.

Les deux approches sont basées sur une procédure de vérification de la source PU. L'objectif de cette procédure est de séparer entre les signaux primaires et les signaux secondaires malveillants.

DRT et DDT sont effectués par des vérificateurs de localisation fiable (LV)qui sont classés en deux catégories :

- ✓ **Un maître LV :** possède une base de données avec les coordonnées des tours de télévisions. Ils connaissent leur emplacement à partir d'un système GPS[1] (Géo-positionnement par satellite) sécurisé.
- ✓ **Un esclave LV :** qui calcule la distance entre lui et le transmetteur par force du signal et le compare avec celui de la tour TV, les données ici doivent être cryptées et authentifiées pour ne pas les modifier ou les intercepter. [44]

- **Défense basée sur la localisation (LocDef):**effectue la vérification de l'émetteur en trois étapes : (Vérification des caractéristiques du signal, Mesure du niveau d'énergie du signal reçu, et Localisation de la source du signal).

Cette méthode utilise RSS-Based[2] localisation qui exploite la relation entre la force du signal et la position de l'utilisateur, quand la force du signal diminue cela veut dire que la distance entre l'émetteur et le récepteur est grande.[32] Si un nœud est capable de collecter suffisamment de données de force de signal à partir des nœuds répartis dans un réseau, il peut créer un modèle de puissance du signal qu'il peut ensuite

[1]GPS : un système de géo localisation fonctionnant au niveau mondial et reposant sur l'exploitation de signaux radio émis par des satellites dédiés.

[2]RSS-Based : La localisation basée sur la puissance du signal reçu (RSS) est une méthode clé pour localiser les objets dans les réseaux de capteurs sans fil (WSN).

utiliser pour estimer l'emplacement de l'émetteur. Et pour collecter les mesures RSS, un réseau de capteur sans fil sous-jacent WSN (Wireless Sensor Network) est utilisé pour la collecte des mesures RSS.[33]

II.3.1.2 L'attaque de la fonction objectif (Objective Function Attack)

Le moteur cognitif de la radio adaptative est celui qui est responsable de l'ajustement des paramètres radio afin de répondre à des exigences spécifiques telles qu'une faible consommation d'énergie, un débit de données élevé et une sécurité élevée. Le moteur cognitif calcule ces paramètres radio (la fréquence centrale, la bande passante, la puissance, le type de cryptage, le protocole d'accès au canal, le type de modulation et la taille de trame …etc.) en résolvant une ou plusieurs fonctions objectives, par exemple trouver les paramètres radio qui maximisent le débit et minimisent la puissance.

Le temps où le moteur cognitif est entrain de trouver les paramètres radio, un attaquant peut cibler ces paramètres pour que les résultats soient adaptés à son intérêt. [37]

L'attaque de la fonction objective (OFA) nommée aussi « attaque de manipulation de croyance »s'applique sur des algorithmes d'apprentissage qui utilisent des fonctions objectives.

Un exemple détaillé qui explique l'attaque de la fonction objective. Cette attaque n'affecte que le type Learning radio, le scénario de l'attaque est qu'à chaque fois que le moteur cognitif tente d'utiliser un niveau élevé de sécurité, l'attaquant lance un brouillage sur la radio en réduisant le taux de transmission **R** et réduisant aussi la fonction Objective $\mathbf{F = w_1.R + w_2.S}$ où **S** taux de sécurité et $\mathbf{w_1}$, **w2** représente les poids de **R** et **S**. Cette fonction objective est utilisée par le moteur cognitif, De cette façon l'attaquant force la radio à utiliser un niveau faible de sécurité. [37]

- **Solution contre l'attaque de la fonction objective**

Définir des valeurs de seuil pour chaque paramètre radio, si les paramètres ne respectent pas les seuils, la communication s'arrête. Ils ont également suggéré d'obtenir de l'aide d'un système de détection d'intrusion (IDS).

II.3.1.3 L'attaque de Brouillage(Jamming)

Le brouillage est une attaque qui peut être effectuée dans les couches physiques et MAC. L'attaquant (brouilleur) envoie de manière malveillante des paquets pour empêcher les participants légitimes dans une session de communication d'envoyer ou de recevoir des données ; par conséquent, créer une situation de DoS (rendre le service indisponible, perturbation des communications…etc.). Dans cette attaque le brouilleur transmet intentionnellement et continuellement sur une bande sous licence, la rendant inutilisable par le PU ou d'autres SU. L'attaque est amplifiée en transmettant à haute puissance dans plusieurs bandes spectrales.

- **Types de brouilleurs**
  - ✓ **Brouilleur constant :** permet d'envoyer les paquets de données en continu sans tenir compte des protocoles de la couche MAC et sans attendre que le canal soit libre.
  - ✓ **Brouilleur trompeur:** son but est de tromper les SU en envoyant des paquets de façon continue afin de les rendre dans un état de réception pendant une durée, il reste dans cet état lorsqu'il détecte un flux constant de données entrants.
  - ✓ **Brouilleur aléatoire :** il prend des pauses entre les signaux de brouillage, et pendant sa phase de brouillage, il peut se comporter comme un brouilleur constant ou trompeur. Il faut un certain temps pour réserver de l'énergie au cas où le brouilleur ne dispose pas d'une alimentation électrique illimitée.
  - ✓ **Brouilleur réactif :** détecte le canal à tout moment et dès qu'il détecte une communication dans le canal, il commence à transmettre les signaux de brouillage. Ce brouilleur est plus difficile à détecter car il ne transmet pas tout le temps.
- **Solutions contre l'attaque Jamming**

DoS peut être effectué sur les deux couches physiques et liaison, chaque couche a sa méthode de détection :

Détection couche physique : les dispositifs légitimes devraient être capables de faire la distinction entre le niveau de bruit normal et anormal dans un canal. Ils peuvent le faire en collectant suffisamment de données sur le niveau de bruit dans le réseau et en

construisant un modèle statistique à utiliser pour la comparaison lorsqu'une attaque par déni de service se produit [38].

Détection couche Liaison : les périphériques peuvent détecter une attaque par DoS en détectant le canal sur lequel ils souhaitent transmettre leurs paquets. Les dispositifs légitimes utilisent le protocole d'accès au medium CSMA (Carrier Sensing Multiple Access) qui ne transmet les données qu'après un certain temps (délai de propagation). Si l'attaquant envoi les paquets sur le même canal que le périphérique légitime, le dispositif n'exécute jamais le protocole CSMA et il sera forcé de reculer. Par conséquent, l'appareil saura qu'il est victime d'une attaque par déni de service.

Deux stratégies sont utilisées pour se défendre contre le brouillage (DoS) :

- **Déplacement des canaux ou changement de fréquence (Channel Surfing):**l'utilisation d'un canal différent une fois qu'une attaque par déni de service est détectée.
- **Retraite spatiale (Spatial Retreat) :** les utilisateurs légitimes changent leur emplacement pour échapper à la gamme d'interférence imposée par l'attaquant. Deux choses doivent être gardées à l'esprit dans cette approche, les utilisateurs doivent quitter la région où se trouve l'attaquant et ils doivent rester à portée l'un de l'autre pour continuer la communication [38].

II.3.1.4 Menaces sur la couche physique

Le tableau suivant montre les contre-mesures effectuées pour chaque attaque ainsi que leur évaluation.

Attaques	Contre-mesure	Évaluation
PUE	Authentification cryptographique des utilisateurs principaux.	Ne fonctionne pas car il nécessite de modifier le système utilisateur principal qui viole les règlements de la FCC.
	(DRT)– basé sur les mesures de force du signal [39].	Dépend de nœuds approuvés appelés Vérificateurs d'emplacement (LV). L'inconvénient majeur est qu'une synchronisation étroite entre les LV est requise et qu'elle peut être bornée si

		l'attaquant est proche de la tour.
	(DDT) – basé sur la différence de phase du signal.	Même que DRT.
	Approches d'empreintes digitales utilisées pour authentifier la source de transmission [40].	Cette approche est considérée comme la meilleure, mais il y a une augmentation probable des besoins de stockage et du temps total de détection en raison des frais généraux possibles des opérations de traitement de signal supplémentaires.
OFA	Définir des valeurs de seuil pour chaque paramètre radio pouvant être mis à jour. Si les paramètres ne respectent pas les seuils, la communication s'arrête [36].	L'inconvénient majeur de cette approche est que cela dépend de seuils fixes. Une amélioration considérable sera de rendre ces seuils adaptatifs.
	Utiliser le système de détection d'intrusion (IDS) [36].	L'utilisation d'un IDS est une contre-mesure très générale qui ne se défend pas contre toutes sortes d'OFA.
Jamming	Recueillir suffisamment de données sur le niveau de bruit dans le réseau et construire un modèle statistique à utiliser pour faire la distinction entre le niveau de bruit normal et anormal [38].	L'inconvénient réside dans la définition de « données suffisantes », c'est-à-dire, quelle est la quantité appropriée de données qui doit être utilisée pour construire le mode.
	Vérifications de cohérence d'emplacement [41].	L'emplacement des voisins est important et peut être acquis par GPS, mais l'inconvénient est que le GPS peut ne pas toujours exister dans un RRC.
	Saut de fréquence.	Bonne solution pour le brouillage.

Tableau II-1: Menaces sur la couche physique, contre-mesures et évaluations [33]

II.3.2 Les attaques de la couche liaison (Link Layer Attack)

La couche de liaison est responsable de la gestion du flux de trafic et du contrôle des erreurs sur le support physique. De plus, la couche liaison prend en charge plusieurs

utilisateurs sur un support partagé au sein du même réseau. Chaque ordinateur reçoit sa propre adresse MAC unique. La plupart des attaques présentées dans cette couche ciblent les adresses MAC.[34]

II.3.2.1 Falsification de données de détection de spectre (SSDF)

La falsification des données de détection du spectre, également connue sous le nom d'attaque byzantine, survient lorsqu'un attaquant envoie de faux résultats de détection du spectre local à ses voisins ou au centre de diffusion, ce qui amène le récepteur à prendre une mauvaise décision de détection du spectre [42].

Cette attaque cible les RRC centralisés et distribués. :

- **RRC centralisé :** un centre d'intégration est chargé de collecter toutes les données détectées et l'allocation des bandes de fréquences. L'attaque SSDF trompe le centre d'intégration pour empêcher certaine utilisateurs légitimes d'accéder à des bandes de fréquences libre, ou ils peuvent accéder à des stations de base qui sont occupées.
- **RRC distribué :** les décisions concernant les bandes de fréquences sont prises via la collaboration entre les réseaux radio cognitifs. Mais une attaque SSDF est extrêmement malveillante dans les RRC distribué car les fausses informations peuvent se propager rapidement sans aucun moyen de les contrôler.

La figure II.2 montre le mécanisme de l'attaque SSDF :

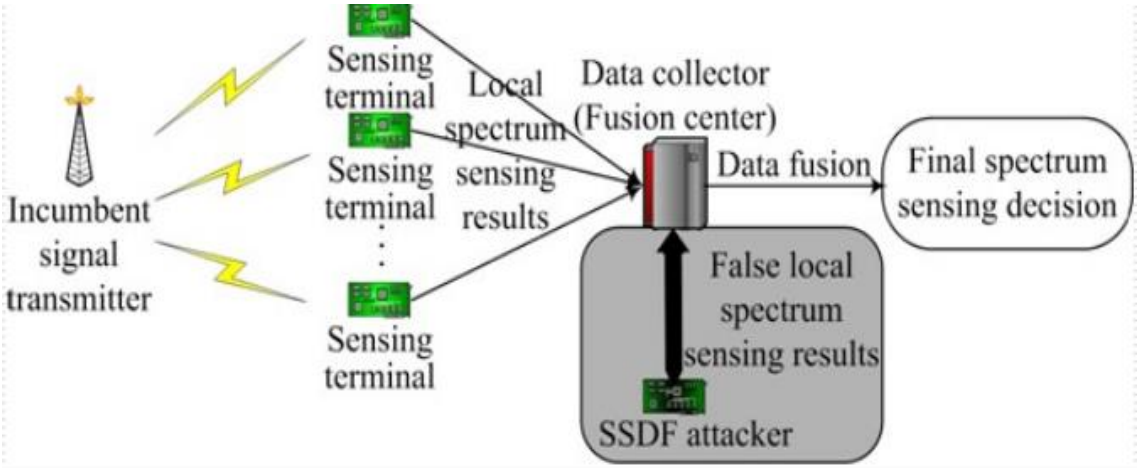

Figure II.2: SSDF attaque.

Donc, dans le RRC centralisé l'effet de données malveillantes est moins diminué car le centre d'intégration compare les données reçues de la RC avec quelques techniques intelligentes pour bien connaitre RC légitime. [43]

❖ **Solution contre l'attaque SSDF**

Plusieurs techniques de fusion de données ont été proposées pour détecter l'attaque SSDF. Parmi ces techniques : fusion de données nommée aussi « Test de Rapport Séquentiel Pondéré » WSRT (Weighted Sequential Probability Ratio Test) est une stratégie qui a été suggérée pour se défendre contrer les attaques byzantines. Dans une architecture ad hoc, les nœuds qui détectent le spectre vont collecter les données et les rapports de détection locaux à partir des nœuds voisins. Les deux étapes principales de cette technique sont :

- ✓ **Maintenance de la valeur:** chaque nœud à une valeur initiale égale à zéro, la valeur sera augmentée de 1 si le spectre est correct. [45]
- ✓ **Hypothèse d'essai de WSPRT:** cette phase suppose que le test de probabilité de séquence et la valeur du terminal WSRT ressemble à la technique des réseaux de capteurs sans fils (WSN). [46]

Un mécanisme de détection est proposé pour identifier les attaques byzantines en comptant les décalages entre leurs décisions locales et la décision globale au centre de fusion sur une fenêtre temporelle, puis en retirant les Byzantins du processus de fusion des données. Le système proposé a été montré pour être robuste contre les attaques byzantines et il a réussi à éliminer les Byzantins dans un laps de temps très court.[33]

Un algorithme de détection d'utilisateur malveillant qui calcule le niveau suspect des utilisateurs secondaires sur la base de leurs rapports antérieurs a été proposé dans [33]. Cet algorithme calcule les valeurs de confiance ainsi que les valeurs de cohérence utilisées pour éliminer l'influence des utilisateurs malveillants sur les résultats de détection de l'utilisateur principal. Tous ces systèmes de défense qui ont été cités ci-dessus sont des techniques et des mécanismes robustes et sécurisées, mais toujours la dégradation des performances. [47]

II.3.2.2 Négociation de canal égoïste (SCN)

Dans un RRC multi-hop, un hôte RC peut refuser de transférer des données pour d'autres hôtes. Cela lui permettra de conserver son énergie et d'augmenter son propre débit grâce à la dissimulation égoïste des canaux. Des objectifs similaires peuvent être atteints si l'hôte égoïste était capable de modifier le comportement MAC correct des dispositifs RC. Par exemple, si l'hôte diminue sa propre taille de fenêtre de back-off, il aura plus de chance de revendiquer le canal au détriment d'autres hôtes RC. Cette attaque peut également gravement dégrader le débit de bout en bout de l'ensemble du RRC [48].

- **Solution contre la saturation du canal de contrôle (CCS) et SCN**

L'atténuation des CCSD et SCN (Selfish Channel Négociation) peut être effectuée en adaptant une architecture de confiance où tout hôte RC suspicieux sera surveillé et évalué par ses voisins. Un voisin peut ensuite effectuer une analyse séquentielle sur l'ensemble des données d'observation, et conclure une décision finale s'il se comporte mal ou non. Le test de rapport de probabilité séquentielle peut être utilisé à cette fin car il a prouvé son efficacité en termes de temps de détection [48].

II.3.2.3 Contrôle de la saturation du canal

Le canal de contrôle dans RRC est utilisé pour acheminer le trafic de contrôle entre les utilisateurs du réseau. Ils ont une limite de données à transporter et à transmettre.

Le canal de contrôle sera dans un mode saturé une fois qu'il ne sera pas en mesure de transporter plus de trafic de contrôle. Un attaquant peut diffuser un grand nombre de paquets dans le but de saturer le canal de contrôle. En envoyant différents types de paquets, un nœud malveillant réduit le risque de détection. Les attaquants visent à réduire le nombre des nœuds légitimes qui peuvent utiliser le spectre et se donner la possibilité d'utiliser les bandes de fréquences de manière optimale.[34]

Pour atténuer cette attaque, un réseau RC pourrait être classé en plusieurs groupes. Dans chaque groupe, un canal de contrôle commun est utilisé. Si un attaquant cible un canal de contrôle, les nœuds des autres groupes ne seront pas affectés ; par conséquent, la zone de réseau affectée est réduite [49].

II.3.3 Les attaques de la couche Réseau (Network Layer Attack)

Les RRC rencontre des problèmes de routage qui proviennent du besoin de transparence dans l'existence des activités de RC pour les PU. Le RRC avec ces trois architectures: maillée, ad hoc et infrastructure rendent le réseau vulnérable à certaines anciennes attaques de réseaux sans fil. Les attaquants ciblent la fonctionnalité de routage car c'est la plus compliquée et la plus vulnérable à l'écoute.

II.3.3.1 Attaques de puits (Sinkhole Attacks)

Dans une attaque de puits, un attaquant s'annonce comme la meilleure route vers une destination spécifique, motivant les nœuds voisins à l'utiliser pour transmettre leurs paquets [50]. L'attaquant peut perpétrer l'attaque de transfert sélectif en transmettant, supprimant ou modifiant les paquets reçus à partir de nœuds sélectionnés. Cette attaque est particulièrement efficace avec les architectures de maillage et d'infrastructure puisque tout le trafic local cherchant à être relayé vers un autre réseau à la même destination ; tout le trafic quittant le réseau local doit passer par la station de base.[35]

- **Solution contre l'attaque de puits**

Une attaque de puits est difficile à détecter car elle exploite la conception de l'architecture réseau et du protocole de routage. Cependant, il existe des protocoles de routage géographique qui construisent une topologie en utilisant seulement des communications locales et des informations non initialisées à partir de la station de base. Ainsi, le trafic sera acheminé vers l'emplacement physique de la station de base et sera difficile de créer un puits.

II.3.3.2 Sybil Attack

Dans l'attaque Sybil, l'attaquant utilise différentes fausses identités pour représenter une entité. L'attaquant utilise le même nœud avec ses différentes fausses identités pour tromper les nœuds légitimes. L'effet de cette attaque est clair dans la technique coopérative de détection de spectre dans laquelle tous les nœuds participent en coopération pour prendre la décision concernant la présence ou l'absence d'un PU sur son spectre. En cela, l'attaquant peut envoyer des informations de détection erronées qui

conduisent à une mauvaise décision de détection et donc laisser les canaux PU non utilisés ou utilisés exclusivement par l'attaquant lui-même.[34]

II.3.3.3 Attaque Hello Flood

L'attaque d'inondation de HELLO est accomplie quand un attaquant envoie un message diffusé à tous les nœuds d'un réseau avec assez de puissance pour les convaincre que c'est leur voisin [51]. Par exemple, un attaquant qui envoie un paquet faisant la publicité d'un lien de haute qualité vers une destination spécifique encouragera des nœuds même très éloignés à utiliser cette route pour les convaincre qu'il est leur voisin. Cependant, leurs paquets seront perdus, et si un nœud découvre l'attaque, il n'aura aucun voisin pour transmettre ses paquets car tous utiliseront le même chemin.[33]

II.3.4 Les attaques de la couche transport (Transport Layer Attack)

La couche de transport est responsable de contrôle du flux, contrôle de congestion et la récupération d'erreur de bout en bout. La couche de transport dans le RRC est soumise à de nombreuses vulnérabilités qui ciblent les réseaux ad hoc sans fil.

II.3.4.1 Attaque de Lion (Lion Attack)

L'attaque de Lion utilise des attaques PUE pour réduire efficacement le débit. De plus, si l'attaquant sait ou peut deviner certains des paramètres de connexion, il peut même effectuer une DoS simplement en émulant une transmission primaire à des instants spécifiques qui peuvent être facilement prédits. Pour cette raison, l'attaque de Lion est plus rentable en réduisant le débit TCP qui effectue de simples attaques PUE ou tout simplement le brouillage[52].

L'attaque de lion est considérée comme une attaque multicouche effectuée sur la couche physique, liaison et ciblée sur la couche de transport où le PUE forcera un RRC à effectuer des transferts de fréquence et dégrader les performances TCP (Transmission Control Protocol).

- **Solution contre Lion Attack**

Pour atténuer l'attaque du Lion, Hernandez-Serrano et Al. suggèrent un mécanisme qui commence par rendre le protocole TCP conscient de ce qui se passe

dans la couche physique en utilisant un partage de données entre les couches physiques /liaisons et de transport [52].

Les dispositifs RRC seront capables de geler les paramètres de connexion TCP pendant les transferts de fréquence et de les adapter aux nouvelles conditions du réseau après le transfert. Pour sécuriser les données de contrôle afin d'empêcher l'attaquant d'écouter les actions actuelles et futures du RRC, une gestion de clé de groupe (GKM[3]) peut être utilisée pour permettre aux membres du RRC de crypter, décrypter et s'authentifier. Enfin, un ID Sinter-couches spécifiquement adapté aux RRC peut être utilisé comme technique pour trouver la source d'attaque si elle existe encore [33].

II.4 Conclusion

Dans ce chapitre, nous avons présenté la sécurité dans la RC et traité les différentes attaques qui ciblent les réseaux de radio cognitive.

Le réseau de radio cognitive consiste à augmenter l'utilisation du spectre en permettant aux SU non autorisés d'accéder de manière opportuniste à la bande de fréquences détenue par les PU. Mais cette nouvelle technologie souffre aussi des attaques réalisées par des utilisateurs malveillants dont le but est d'affecter de manière externe l'utilisation du spectre en se faisant passer pour un utilisateur principal, de capturer ou de changer le message (brouillage du canal de contrôle, la menace byzantine, l'attaque PUE…..).

[3]GKM une gestion de clé dans une communication de groupe. La plupart des communications de groupe utilisent la communication multidiffusion de sorte que si le message est envoyé une fois par l'expéditeur, il sera reçu par tous les utilisateurs. Le principal problème dans la communication de groupe multicast est sa sécurité. Afin d'améliorer la sécurité, différentes clés sont données aux utilisateurs. En utilisant les touches, les utilisateurs peuvent crypter leurs messages et les envoyer en secret.

CHAPITRE III : Contribution et résultats

III. CHAPITRE III : Contribution et résultats

III.1 Introduction

L'attaque PUE est réalisée par un utilisateur secondaire malveillant émulant un utilisateur primaire en se faisant passer par un PU pour obtenir les ressources d'un canal donné sans avoir à les partager avec d'autres utilisateurs secondaires [53]. Ainsi, il faut savoir que le comportement d'un PUE est toujours mensonger, il essaye de mimer le comportement d'un PU et essaye toujours de proposer les meilleures offres.

L'étude qui a été faite par [44] concerne à sécuriser le réseau radio cognitive, cela en proposant deux méthodes : Secure CR et Optimal CR en utilisant l'algorithme TOPSIS pour choisir la meilleure offre et l'algorithme Blowfish pour l'authentification. Ils supposent également que tous les PU présents dans cet intervalle de temps sont fiables ce qui n'est pas logique car à tout moment, il peut y avoir des utilisateurs malhonnêtes.

Notre travail consiste à introduire la notion d'apprentissage automatique pour faire des prédictions sur la nature de l'utilisateur (fiable ou malhonnête) et ensuite sécuriser la communication entre les utilisateurs contre l'attaque PUE afin d'avoir une meilleure utilisation du spectre sans interférences. Dans ce chapitre nous allons étudier le cas où il y a un seul SU et un nombre fixe de PU. Nous précisons que la simulation est développée avec le langage JAVA sous l'environnement de développement intégré Netbeans.

Pour réaliser ce travail nous avons implémenté la méthode d'analyse multicritères TOPSIS [Annexe A] pour l'aide à la prise de décision et un algorithme d'apprentissage automatique Naive Bayes [Annexe B] ainsi que l'implémentation de code de césar qui est une méthode de chiffrement par décalage. Enfin, nous allons instaurer notre algorithme de sécurité dans le contexte d'un réseau radio cognitif.

III.2 Présentation du scénario

Pour la réalisation et l'implémentation de notre application, nous nous sommes basées sur un modèle typique de négociation : celui de « un à plusieurs » où les PU sont fixes et ne changent pas. A l'aide de l'algorithme TOPSIS, le SU et les PU négocient

leur accord sur une base de multiples critères tels que le nombre de canaux, le prix, le temps d'allocation, la technologie utilisée et le débit.

La figure ci-dessous montre les messages échangés entre le SU et les PU.

- ❖ Le SU contacte les PU pour signaler le nombre de canaux, le temps d'allocation, la technologie et le débit dont il a besoin.
- ❖ Chaque PU propose : le nombre de canaux libres, la technologie utilisée, le temps d'allocation, le prix, le débit.
- ❖ Le SU reçoit les offres des PU et choisit la meilleure offre en appliquant l'algorithme TOPSIS.

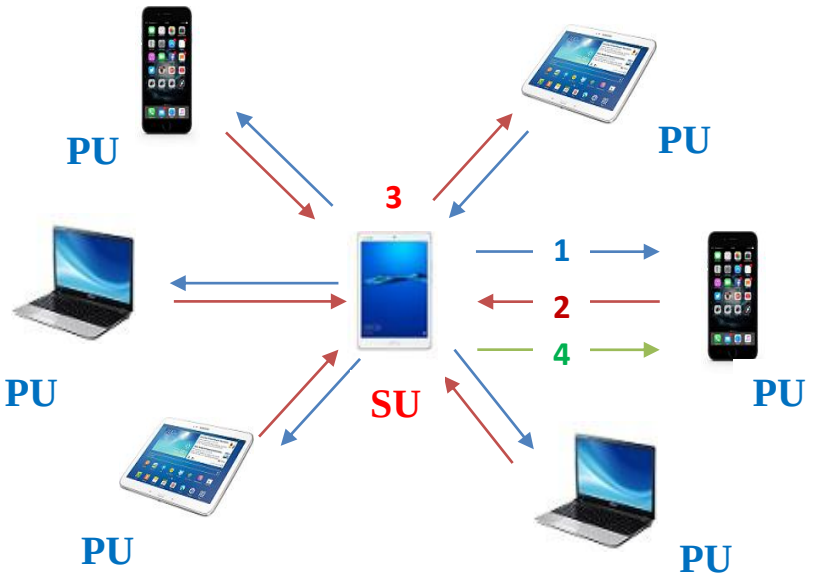

Figure III.1:Scénario proposé.

1	Le SU contacte les PU et leur envoie sa demande
2	Chaque PU renvoi au SU son offre
3	Le SU sélectionne la meilleure offre en appliquant TOPSIS
4	Le SU vérifie la nature du PU sélectionné (Honnête/Malveillant)

Tableau III-1:fonctionnement du scénario proposé.

III.3 Outils utilisés

III.3.1 Netbeans

Netbeans est un IDE qui offre un meilleur support pour le développement des applications web et le coté serveur qui utilise la plateforme Java EE. Cet IDE a été développé en étroite collaboration avec les équipes Java EE et Glass Fish pour fournir une intégration et une utilisation plus simple de la spécification Java EE. L'utilisation de Netbeans est un moyen d'apprendre rapidement et de devenir productif dans la programmation Java EE [54].

III.3.2 SQLite

SQLite est une bibliothèque en cours qui implémente un moteur de base de données SQL transactionnel autonome sans configuration. SQLite est la base de données la plus largement déployée au monde .[55] Grâce à son environnement intégré au programme et le fait que le code source ne soit régit par aucune licence, SQLite est utilisé dans de nombreux logiciels et systèmes bien connus tels que Firefox, Skype, Android, IPhone et divers produits et projets[56].

Contrairement à la plupart des bases de données, SQLite ne repose pas sur une architecture traditionnelle client/serveur, mais lit et écrit directement depuis un fichier classique. En d'autres termes, SQLite intègre une base de données SQL complète (tables, index, déclarations et données) dans un fichier indépendant de la plateforme[57]. Elle accède directement à ses fichiers de stockage.

III.3.3 Jade

JADE (Java Agent DEvelopment Framework) est un framework logiciel entièrement implémenté en langage Java. Il simplifie la mise en œuvre de systèmes multi-agents grâce à un middleware conforme aux spécifications FIPA et à un ensemble d'outils graphiques prenant en charge les phases de débogage et de déploiement. Un système basé sur JADE peut être distribué sur plusieurs machines (qui n'ont même pas besoin de partager le même système d'exploitation) et la configuration peut être contrôlée via une interface graphique distante. La configuration peut même être

modifiée au moment de l'exécution en déplaçant les agents d'une machine à l'autre, selon les besoins. [58]

III.4 Travail effectué

Le but de notre travail est de sécuriser la communication entre le SU et les PU en proposant une méthode de sécurité pour prévenir l'attaque PUE Nous avons utilisé l'apprentissage automatique dans un premier lieu pour faire des prédictions sur la nature de l'utilisateur et ensuite nous avons proposé un algorithme de sécurité qui va tester si l'utilisateur est honnête en plusieurs étapes. A la fin, nous comparons si nous avons obtenu les mêmes résultats avec les prédictions faites au départ.

III.4.1 Base de données utilisée et critères

Vu qu'il n'y a pas de Benchmark préétablit pour les données de la radio cognitive, nous étions obligés de jouer le rôle de l'expert et ainsi nous avons créé une petite base de données qui contient les critères suivants : Nombre de canaux, Prix, Durée d'utilisation, Récompense, Pénalité, Technologie, le Débit (relatif à la technologie utilisée).

Le choix des critères pour la base de données qui servira pour l'apprentissage automatique a été très difficile, et donc nous avons ajouté de nouveaux critères par rapport au travail effectué dans [44] qui sont la technologie et le débit. En effet, nous pensons que la technologie utilisée par le SU a un très grand rôle car il est important d'assurer une bonne qualité de service.

Nous avons aussi introduit le concept de récompense et pénalité en s'inspirant du procédé d'apprentissage par renforcement. Nous pensons que pour faire des prédictions, il est important pour le SU d'avoir une idée sur les pénalités et récompenses reçus par chaque PU.

Pour les critères on a utilisé les intervalles suivants:

- Nombre de canaux [1-10]
- Prix [1-30]
- Durée [1-30] en minutes

- Technologie [1-6] : on a intégré la [3G, 3,5G, 3,75G, 4G, 4G+, 5G].
- Débit [9, 1000000] kbps.
- Récompense et pénalité sont des valeurs incrémentées via notre programme et mises à jour à l'aide de notre mécanisme de sécurité.
    - ✓ Si la prédiction = résultat =>récompense ++
      sinon pénalité ++

Sachant que:

- 3G : [144kbps -1,9Mbps]
- 3,5G : [3,6-14,4] Mbps
- 3,75G : [5-21] Mbps
- 4G : [40-150] Mbps
- 4G+ : 1Gbps
- 5G : 10Gbps

III.4.2 Contribution

Notre travail consiste à permettre au SU de différencier entre les PU honnête et malveillants en comparant le résultat prédit par l'algorithme Naive Bayes avec celui de notre algorithme de sécurité.

Notre contribution consiste à réaliser un algorithme comprenant plusieurs étapes (figure III.2) dont un algorithme de sécurité appelé Sécur PUE qui a pour rôle de renforcer la sécurité de la communication entre les différents utilisateurs dans la RC en effectuant plusieurs tests.

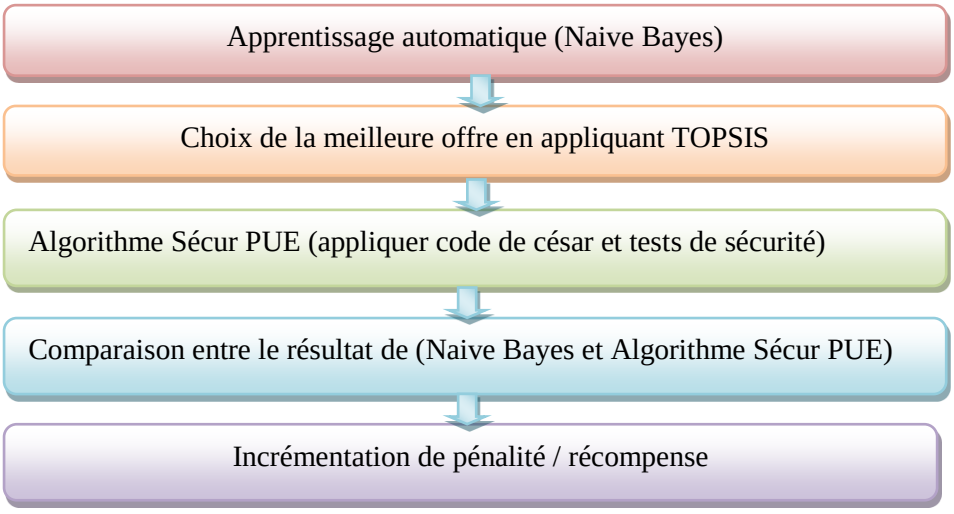

Figure III.2:Démarche suivie pour la sécurité

III.4.2.1 Apprentissage automatique

Nous avons choisi l'algorithme Naive Bayes comme algorithme d'apprentissage automatique, qui est l'une des méthodes les plus simples en apprentissage supervisé et il est très largement utilisé car l'un des principaux avantages de ce classifieur est qu'il obtient de bons résultats même avec un petit jeu d'apprentissage. L'algorithme va se servir de la BDD d'apprentissage et des propositions des PU pour prédire leurs type ; et effectue des calculs afin de déterminer la classe qui a le plus grand pourcentage (H/M) .Ce résultat sera enregistré dans la table « Résultat_NaiveBayes », comme indiqué dans la figure III.3.

Table : Résultat_NaiveBayes

	Nom	Résultat_H	Résultat_M	Type
	Filtre	Filtre	Filtre	Filtre
1	PU1	80.690031582...	19.309968417...	H
2	PU4	76.177701670...	23.822298329...	H
3	PU2	52.854375007...	47.145624992...	H
4	PU0	51.606268106...	48.393731893...	H
5	PU3	15.156705173...	84.843294826...	M
6	PUM	42.810634116...	57.189365883...	M

Figure III.3: Table Résultat_NaiveBayes.

III.4.2.2 Sécurité

a) Algorithme de sécurité proposé

Nous rappelons que dans notre travail, nous avons traité l'attaque PUE avec un scénario fixe.

Pour sécuriser la communication entre le SU et les PU nous avons procédé comme suit :

- Le SU reçoit plusieurs offres de la part des PU.
- Le SU applique TOPSIS pour choisir la meilleure offre, ensuite trie ces résultats obtenus par ordre décroissant pour une prochaine simulation.

1er Test :

- Le SU vérifie la fidélité du PU choisi (celui qui a émis la meilleure offre)

a) Si la fidélité est supérieure à 2, le SU conclue directement que ce PU est honnête.
b) Sinon le SU devra procéder à d'autres tests pour déterminer la nature du PU.

2ème Test :

- Le PU reçoit un message fictif de la part du SU :
  a) Si le PU répond dans un délai supérieur à 2 secondes, le SU conclue qu'il est malveillant.
  b) Si le PU répond par un message différent que **NOT_UNDERSTOOD** le SU saura qu'il n'a pas compris sa requête et le considère ainsi comme un PU malveillant.
  c) Sinon (si délai respecté et réponse du PU est de type **NOT_UNDERSTOOD**) le SU va procéder à un dernier test.

3ème Test:

- Le SU renvoie un message crypté au PU :
  a) Si le PU dépasse le délai de réponse de 2 secondes, le SU saura qu'il est malveillant.
  b) Si le PU ne renvoie pas le bon message (décrypté) cela signifie aussi qu'il est malveillant.
  c) Sinon (délai respecté et message décrypté) le SU confirme que le PU applique le code César et il a la bonne clé de décryptage et donc, il est honnête.

Nous avons choisi de passer par les trois tests pour renforcer la sécurité et ainsi se protéger de l'attaque PUE.

La figure suivante montre l'algorithme **Sécur PUE** que nous avons suggéré :

Algorithm 1 Algorithme Sécur PUE

```
1: procedure SÉCURITÉ(RésTopsis)
2:     if Fidelité > 2 then
3:         PU Honnête
4:         Fidelité++
5:     else
6:         Envoyer message fictif
7:         if (réponse = NOT UNDERSTOOD and durée < 2000ms) then
8:             Appel fonction césar
9:             Envoyer message crypté
10:            if (réponse = Message décrypté and durée < 2000ms) then
11:                PU Honnête
12:                Fidelité++
13:            else
14:                PU Malveillant
15:                Fidelité - -
16:                Appel procédure Sécurité
17:            end if
18:        else
19:            PU Malveillant
20:            Fidelité - -
21:            Appel procédure Sécurité
22:        end if
23:    end if
24: end procedure
```

Figure III.4:Algorithme Sécur PUE.

❖ **Code de césar (chiffre de césar)**

Le chiffre de César est la méthode de cryptographie la plus ancienne communément admise par l'histoire. Il consiste en une substitution mono-alphabétique : chaque lettre est remplacée ("substitution") par une seule autre ("mono-alphabétique"), selon un certain décalage dans l'alphabet ou de façon arbitraire. D'après Suétone, César avait coutume d'utiliser un décalage de 3 lettres : A devient D, B devient E, C devient F, etc. Il écrivait donc son message normalement, puis remplaçait chaque lettre par celle qui lui correspondait : [59]

CLAIR	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
-> décalage = 3																										
CODE	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Exemple : d'après cette méthode, "VIVE LES MATHS" devient donc "YLYH OHV PDWKV».

III.5 Comportement des Utilisateurs

III.5.1 Côté PU

La figure III.5 décrit le comportement du PU lors de l'application de l'algorithme de sécurité.

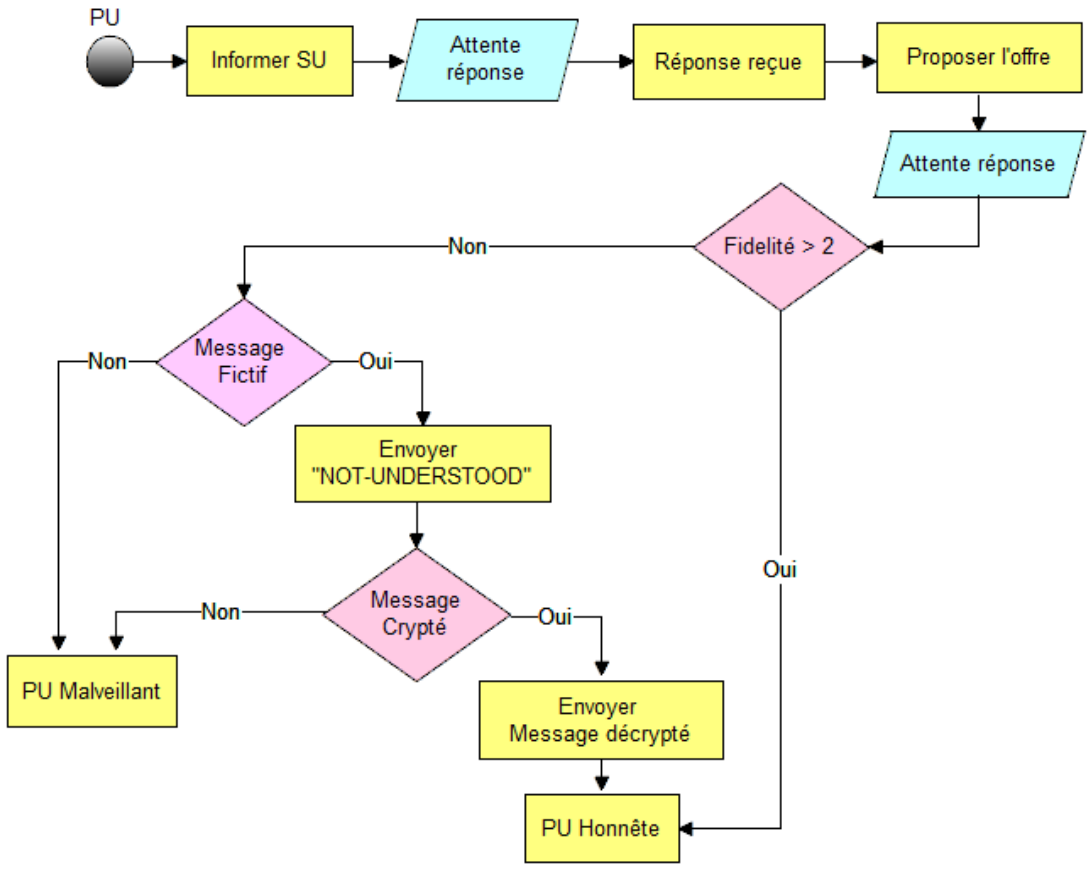

Figure III.5: Comportement du PU.

Le PU envoie le message **INFORM** au SU pour l'informer qu'il est présent, ce dernier lui répond par le message **REQUEST** qui contient ses besoins, ensuite chacun des PU lui répond par sa propre proposition avec un message de type **PROPOSE** qui contient certains critères (le nombre de canaux, le prix, la durée, la technologie utilisée et le débit), ces critères vont être enregistrés dans la table « Historique » comme le montre la figure III.6.

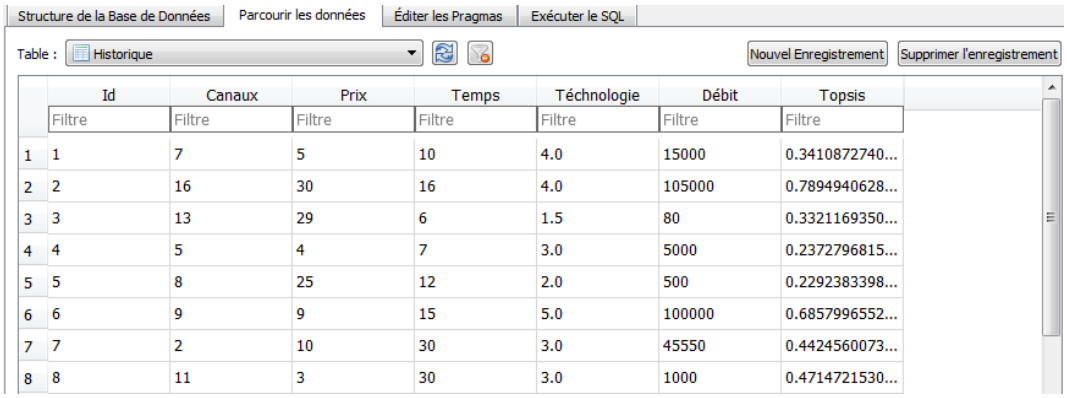
Structure de la Base de Données | Parcourir les données | Éditer les Pragmas | Exécuter le SQL

Table : Historique — Nouvel Enregistrement — Supprimer l'enregistrement

	Id	Canaux	Prix	Temps	Téchnologie	Débit	Topsis
	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre
1	1	7	5	10	4.0	15000	0.3410872740...
2	2	16	30	16	4.0	105000	0.7894940628...
3	3	13	29	6	1.5	80	0.3321169350...
4	4	5	4	7	3.0	5000	0.2372796815...
5	5	8	25	12	2.0	500	0.2292383398...
6	6	9	9	15	5.0	100000	0.6857996552...
7	7	2	10	30	3.0	45550	0.4424560073...
8	8	11	3	30	3.0	1000	0.4714721530...

Figure III.6:Table Historique.

Une fois que le PU reçoit un message fictif, il envoie une réponse de Type **NOT_UNDERSTOOD** au bout de 2 sec pour dire au SU qu'il n'a pas compris la requête, le SU saura que ce PU peut être honnête et lui renvoie un message crypté, ensuite si le PU lui répond au bout d'une durée de 2secondes par le bon message décrypté cela signifie qu'il a la bonne clé de décryptage(code de César) et donc il sera considéré comme utilisateur honnête.

III.5.2 Côté SU

a) Apprentissage avec Naive Bayes

L'apprentissage se fait au niveau du SU en appliquant l'algorithme de Naive Bayes sur les propositions du PU choisis par l'algorithme TOPSIS pour prédire si cet utilisateur est honnête ou malveillant. Ensuite le résultat sera enregistré dans la table Résultat_NaiveBayes (Figure III.3).

a) Fonctionnement de l'Algorithme de sécurité

A un certain moment, le SU va envoyer une requête qui contient ses besoins en terme de (nombre de canaux, durée, technologie utilisée et débit) à tous les PU qui ont envoyé un message de type **INFORM**. Ensuite les PU qui peuvent satisfaire cette offre vont répondre par des propositions avec un message **PROPOSE**, à ce moment-là le SU applique l'algorithme TOPSIS avec les poids (Nombre de canaux :**0.3**, Prix :**0.1**, Durée :**0.2**, Technologie :**0.2**, Débit : **0.2**) pour choisir la meilleure offre, ensuite doit sécuriser sa communication avec le PU sélectionné en vérifiant si sa fidélité est supérieur à 2, il lui envoie un message fictif, et s'il reçoit le **NOT_UNDERSTOOD** au

bout de 2 secondes, il renvoie au PU un message crypté car si ce dernier lui répond par le bon message décrypté avant 2 secondes alors le SU confirme que c'est un PU honnête, incrémente sa fidélité et lui envoie le message **ACCEPT- PROPOSAL**, sinon s'il lui envoie un message quelconque ou dépasse le délai il sera considéré comme malveillant et sa fidélité sera décrémentée et enregistrée dans la table de prédiction « Tb_prédiction ».

La figure III.7 décrit le comportement du SU lors de l'application de l'algorithme de sécurité.

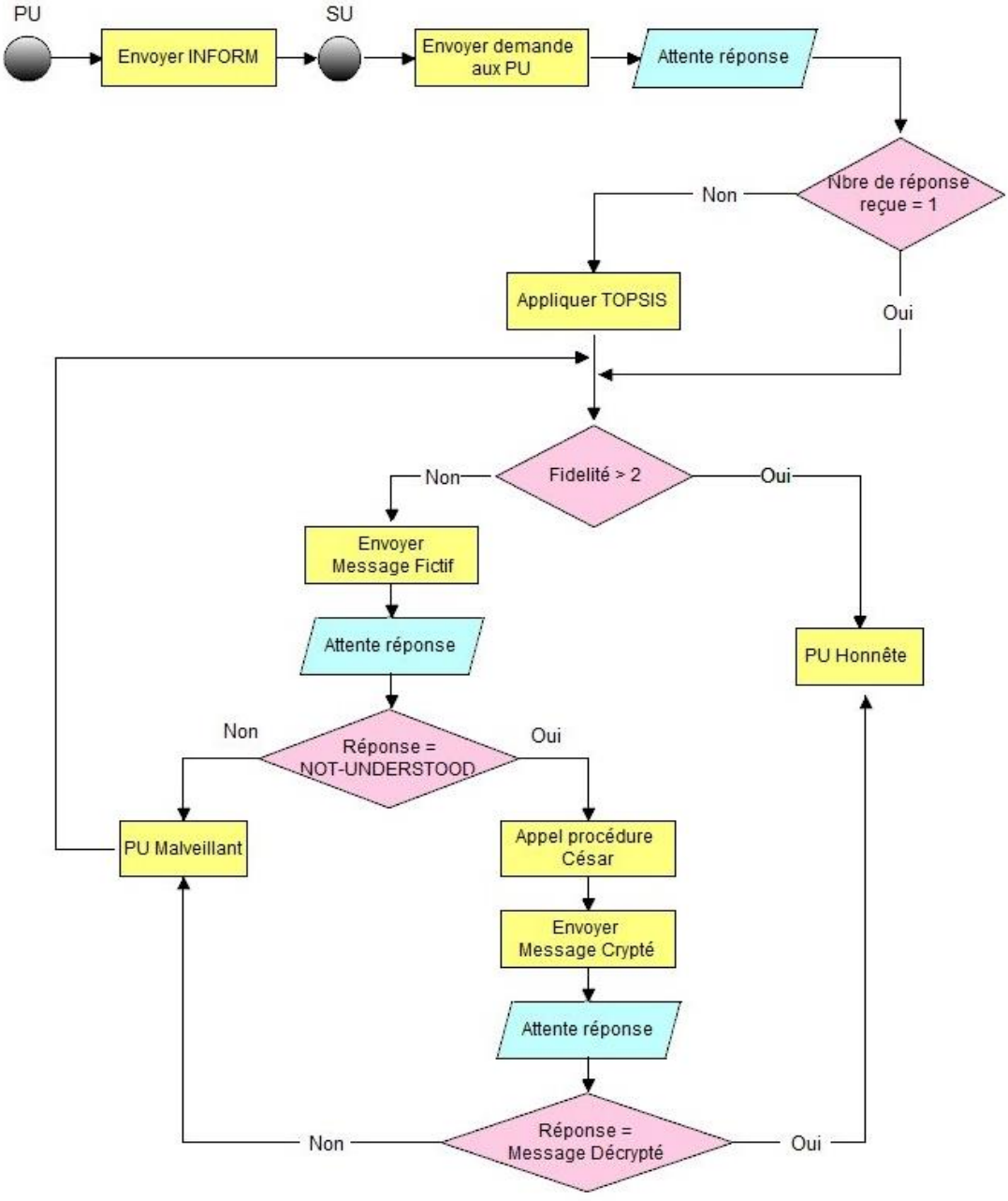

Figure III.7:Comportement du SU avec l'algorithme « Sécur PUE »

b) Comparaison des résultats

Dans la Figure III.8, le SU applique l'algorithme de Naive Bayes en premier pour prédire le type de chaque PU puis l'algorithme Sécur PUE en second pour le choix des PU et la sécurité de la communication afin de détecter les PU honnêtes et malveillants, ensuite il compare les résultats obtenus des deux algorithmes pour incrémenter la récompense (si les résultats sont identiques) ou la pénalité (dans le cas contraire)**.**

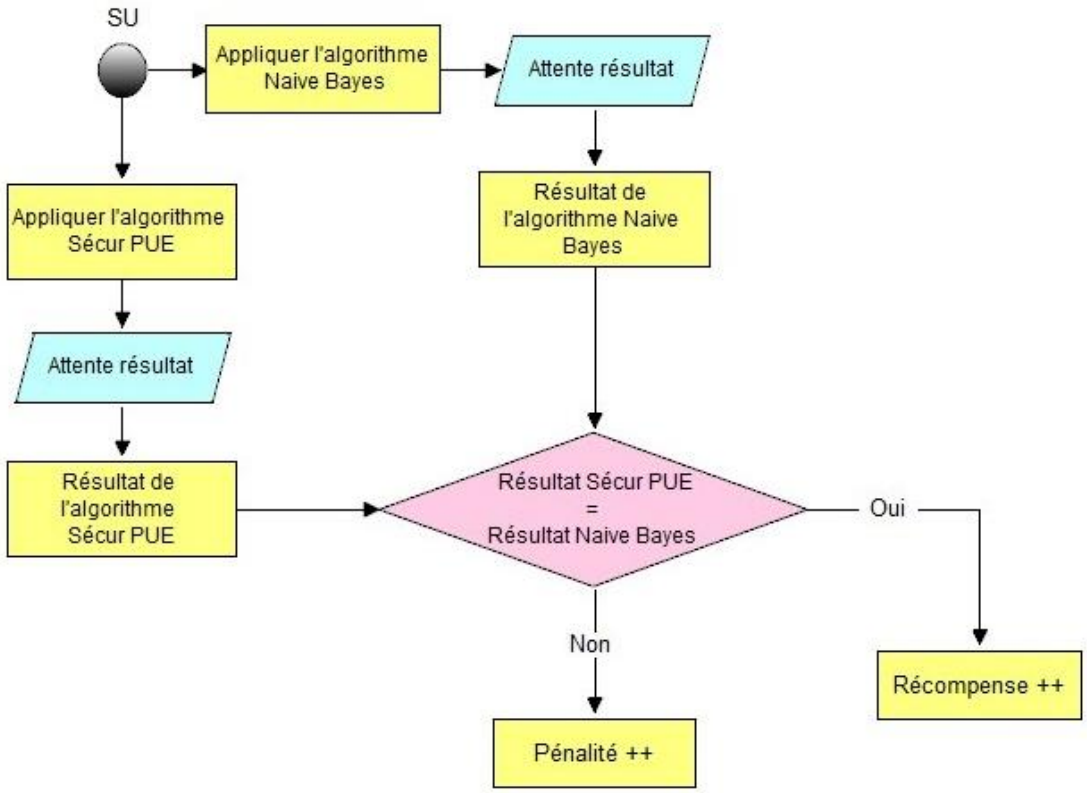

Figure III.8: Comportement du SU après l'application des algorithmes Naive Bayes et Sécur PUE.

La figure ci-dessous montre le résultat des différentes interactions possibles entre le SU et les PU lors de l'application de l'algorithme Sécur PUE.

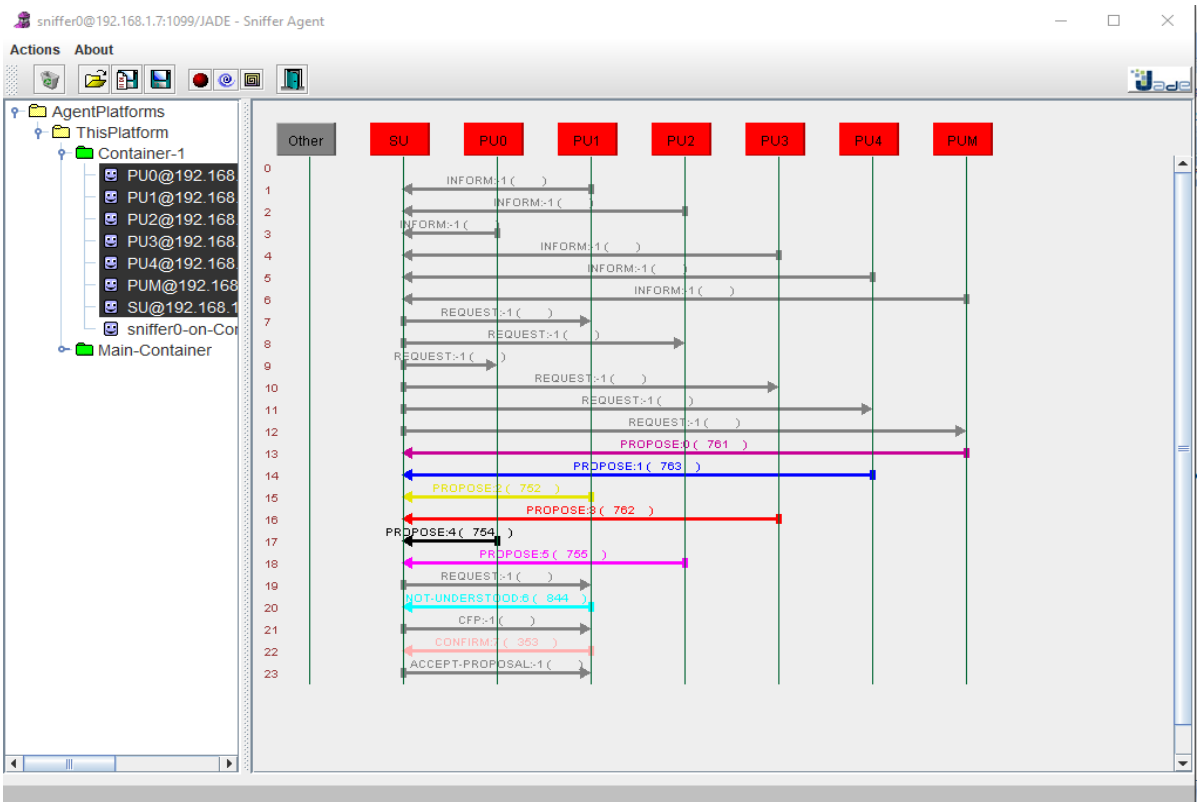

Figure III.9: Agent Sniffer pour l'algorithme Sécur PUE.

III.6 Résultats obtenus

a) Evaluation de l'algorithme NAIVE BAYES

Pour évaluer l'algorithme de Naive Bayes nous avons pris comme critères de performance la matrice de confusion suivante :

Classe Réelle

Classe Prédite	PU Honnête	PU Malveillant	TOTAL
PU Honnête	Vrais positifs (VP) **2**	Faux positifs (FP) **0**	**2**
PU Malveillant	Faux négatifs (FN) **1**	Vrais négatifs (VN) **3**	**4**
TOTAL	**3**	**3**	**6**

Tableau III-2: Matrice de confusion.

La sensibilité représente la proportion des PU honnêtes parmi les malveillants.

Sensibilité = VP / (VP + FN) = 2/ (2+1) = 66%

La spécificité représente la proportion des PU malveillants parmi les honnêtes.

Spécificité = VN / (VN + FN) = 3 / (3+1) = 75%

Accuracy représente le taux des utilisateurs biens classés sur le nombre total des utilisateurs.

Accuracy = (VP+VN) / (VP+VN+FP+FN) = 5 / 6 = 83%

Nous pensons qu'avec une base de données plus grande, nous aurons de meilleurs résultats car l'apprentissage se fera sur plus d'éléments.

b) Nombre de messages échangés

Le tableau suivant représente l'impact du nombre de PU sur le nombre des messages échangés, nous remarquons que plus il y a de PU, plus le nombre de message échangés entre le SU et ces PU augmente ce qui est logique.

Nombre de PU	**6**	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**	**100**
Messages Envoyée	7	11	21	31	41	53	63	73	83	91	103
Messages Reçus	12	20	40	60	80	102	122	142	162	178	202
Nombre de Messages Total	19	31	61	91	121	155	185	215	245	269	305

Tableau III-3: Nombre de messages échangés

La figure suivante montre l'évolution des messages échangés par rapport au nombre des PU.

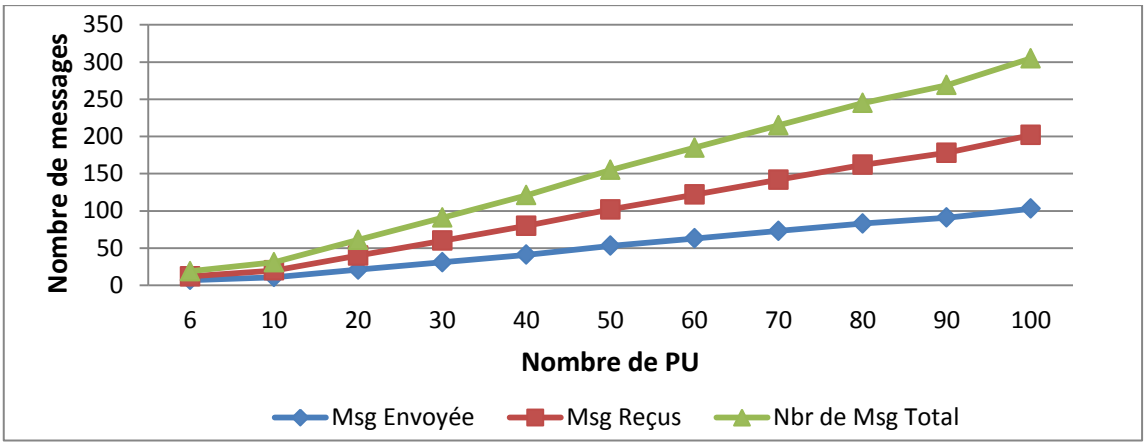

Figure III.10: Impact du Nombre de PU sur le Nombre de messages échangés.

c) Temps d'exécution

Dans le tableau suivant, nous constatons que le temps d'exécution de notre programme n'est pas influencé par l'augmentation du nombre de PU ce qui est un critère de qualité dans les applications temps réel Dans ce cas, on peut dire que notre application permet le passage à l'échelle ce qui est expliqué par le fait que notre application est distribuée sur les différents agents.

Nombre de PU	6	10	20	30	40	50	60	70	80	90	100
Temps d'exécution (ms)	60185	60282	60389	60464	60616	60750	60845	60931	61097	61300	61438

Tableau III-4: Temps d'exécution obtenus.

La figure ci-dessous montre les résultats obtenus en termes de temps d'exécution par rapport au nombre de PU.

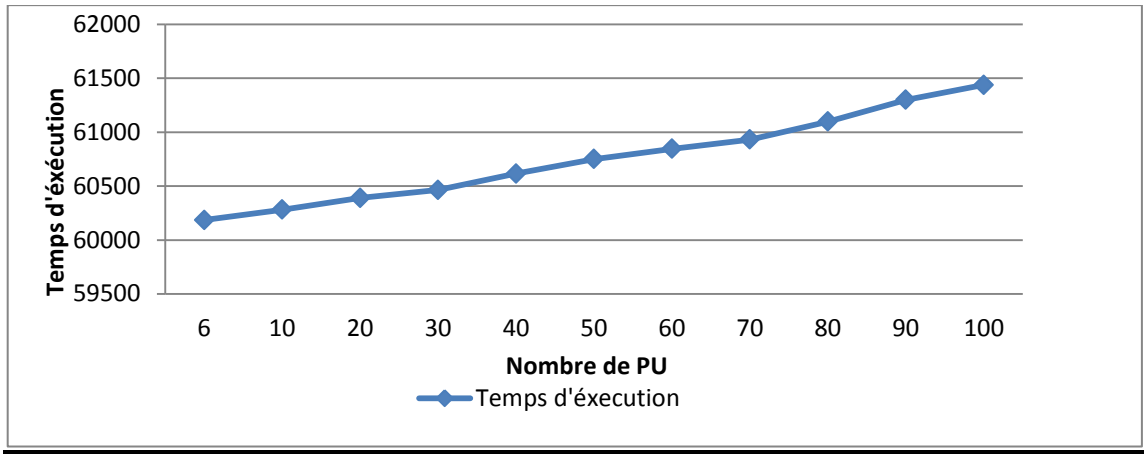

Figure III.11: Impact du nombre de PU sur le temps d'exécution.

III.7 Présentation de l'application

Pour terminer notre travail, nous avons développé une application avec Netbeans 8.0.1 codée en java. Pour cela, nous avons réalisé deux interfaces graphiques, la première représente une interface d'accueil (figure III.12) qui va nous rediriger avec un simple clic, vers la deuxième interface (figure III.13) qui va permettre à l'utilisateur de lancer la simulation.

Figure III.12: Interface d'accueil.

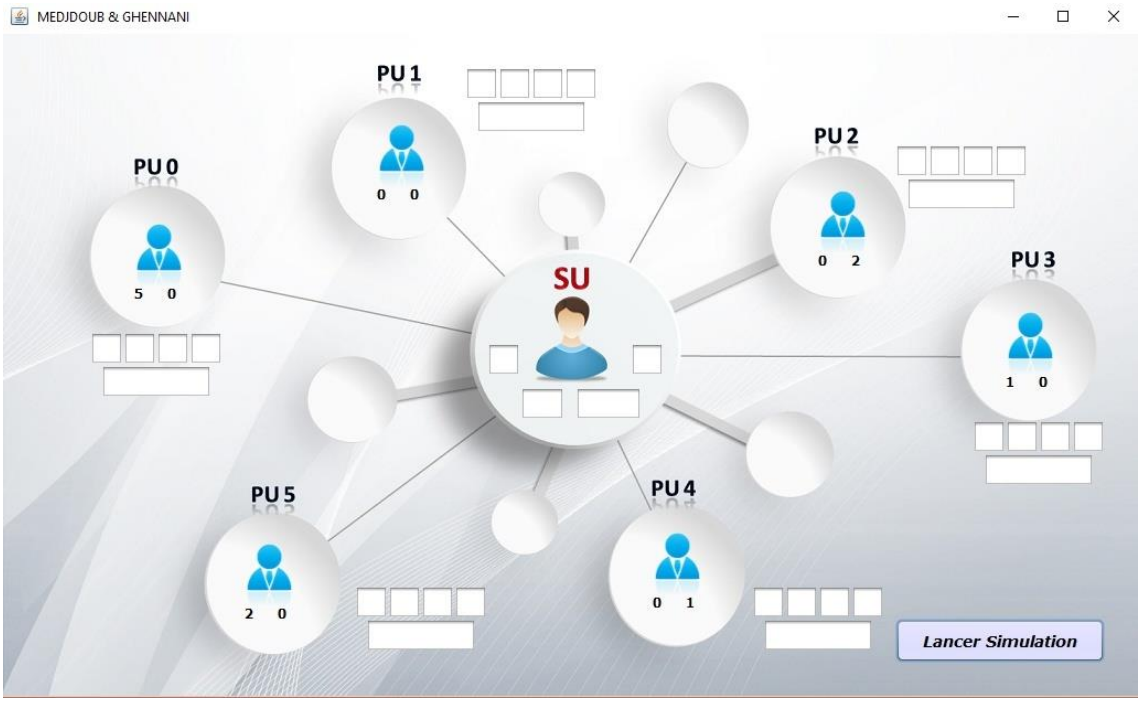

Figure III.13: Interface de simulation

Le développement des interfaces a été réalisé à l'aide de la bibliothèque SWING. L'exécution de la simulation peut être lancée à partir du bouton « **Lancer Simulation** ».

Notre interface se compose d'un SU et de plusieurs PU. Le SU a quatre critères de demande (nombre de canaux, durée, technologie et débit) et Chaque PU à cinq critères de proposition (nombre de canaux, prix, durée, technologie et débit) ainsi que deux autres valeurs (récompense et pénalité).

Au départ, tous les PU sont représentés d'une couleur « **bleue** » et en cliquant sur le bouton « **Lancer Simulation** », la couleur de ces derniers sera modifiée, un PU devient « **vert** » si Le SU l'a désigné comme honnête ou devient « **rouge** » si le SU l'a identifié comme malveillant. Les valeurs récompense et pénalité seront incrémentées en conséquence, la valeur de récompense (affichée en vert) sera incrémentée si le choix du SU correspond à la prédiction de l'algorithme, sinon c'est la valeur de pénalité (affichée en rouge) qui sera incrémentée. La figure III.14 illustre les résultats d'une simulation avec un SU et 06 PU.

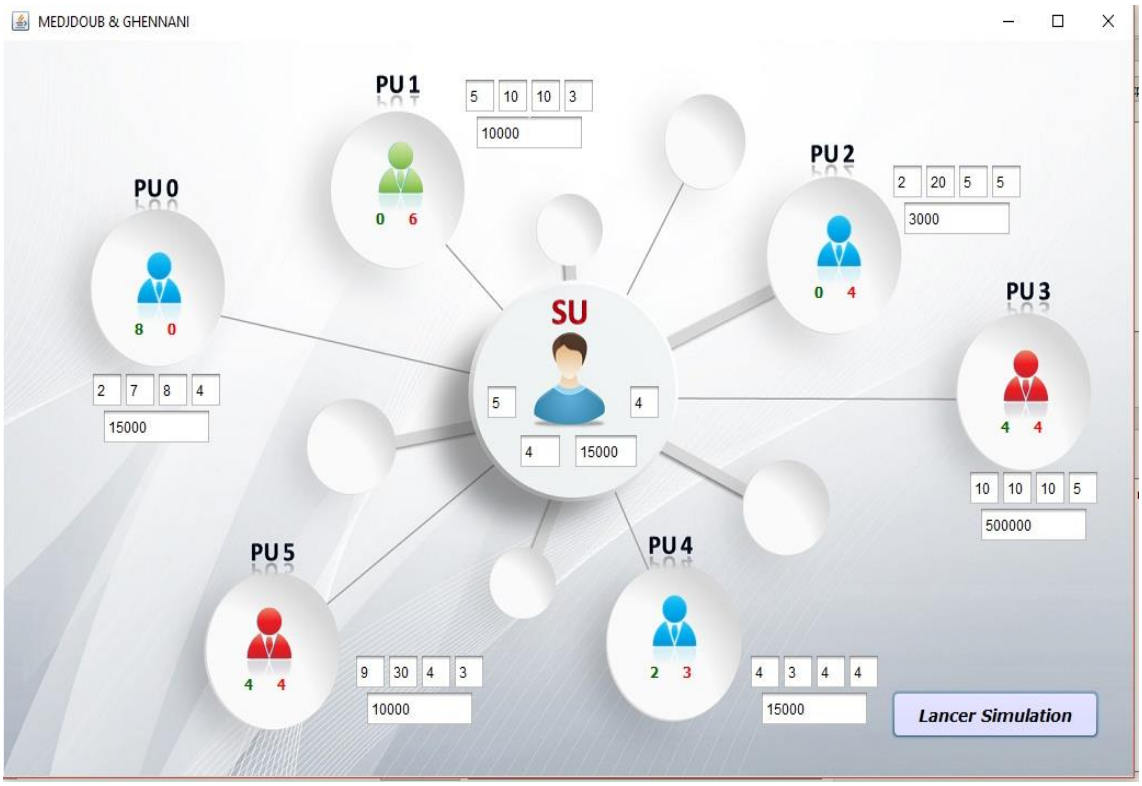

Figure III.14: Exécution de l'algorithme.

Nous remarquons dans cet exemple que le SU a effectué une demande de 5 canaux pour une durée de 4 minutes en utilisant la technologie 4 G avec un débit de 15000 Mb, ensuite chaque PU a indiqué le prix de l'offre qu'il a proposé au SU. Le résultat de la simulation indique clairement que le SU a identifié deux PU malveillants (PU3, PU5 en rouge) et un PU honnête (PU1, en vert) comme présentant la meilleure offre. Les valeurs « récompense, en vert » ou « pénalité, en rouge » seront incrémentées en conséquence.

III.8 Conclusion

Nous avons pu présenter dans ce chapitre la topologie du réseau utilisé (d'un SU à plusieurs PU), le fonctionnement de notre application et les différents algorithmes que nous avons étudié tels que l'algorithme d'apprentissage supervisé NAIVE BAYES qui permet de classifier un ensemble d'observations selon des règles déterminées par l'algorithme lui-même et l'algorithme de la décision multicritère TOPSIS pour aboutir à un choix optimal. Ensuite, nous avons proposé une méthode pour sécuriser la communication entre les utilisateurs primaire et l'utilisateur secondaire dans un réseau radio cognitive.

Nous avons enfin, représenté le tout dans une interface que nous avons réalisé en développant une application qui va afficher les résultats de la simulation selon des couleurs bien spécifiques à l'état des PU, ainsi nous pouvons distinguer entre un PU honnête par la couleur verte et un PU malveillant par la couleur rouge.

Nous avons aussi ajouté sur l'interface, des valeurs récompensant ou pénalisant ainsi les PU choisi par le SU. La valeur « récompense » représentée par des chiffres en vert sera ainsi incrémentée si le choix du SU correspond à la prédiction de l'algorithme. La valeur « pénalité » représentée par des chiffres en rouge sera incrémentée à son tour si le choix du PU par le SU était différent de celui de la prédiction.

Conclusion générale

La radio cognitive est une technologie émergente en matière d'accès 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, chaque utilisateur secondaire pourra à tout moment accéder à des bandes de fréquence qu'il trouve libres, et qui ne sont pas occupées par l'utilisateur primaire qui possède une licence sur cette bande. L'utilisateur secondaire devra les céder une fois le service terminé ou une fois qu'un utilisateur primaire aura besoin de se connecter.

Le concept de radio cognitive est en réalité une interaction entre la technologie sans fil et l'intelligence artificielle. Elle doit jouer un rôle exceptionnel pour combiner entre la capacité de détection, d'apprentissage, de raisonnement, de sécurisation, de prise de décision et de reconfiguration pour s'adapter au changement de l'environnement.

Dans ce travail, nous nous sommes intéressées au concept de la sécurité et de l'apprentissage automatique dans les réseaux radio cognitive, nous avons utilisé l'apprentissage automatique dans un premier lieu pour faire des prédictions sur la nature de l'utilisateur, pour cela, nous avons utilisé un algorithme d'apprentissage automatique nommé « Naive Bayes » pour prédire si les PU sont honnêtes ou malveillants. Ensuite et dans un but de sécuriser l'accès dynamique au spectre, nous avons proposé une méthode de sécurité pour prévenir l'attaque PUE avec un algorithme de sécurité que nous avons développé et que nous avons nommé « Sécur PUE ». Ce dernier a pour rôle de renforcer la sécurité de la communication entre les différents utilisateurs, le SU devra alors choisir la meilleure offre en appliquant TOPSIS et devra aussi effectuer plusieurs tests de sécurité. A la fin, nous avons comparé les résultats que nous avons obtenus avec ceux des prédictions faites au départ.

Nous avons ensuite développé une application de simulation, et le résultat a été assez convaincant, d'un côté, nous avons assuré la sécurisation de la connexion entre le SU et les différents PU et d'un autre côté, l'algorithme Naive bayes a permis de faire de bonnes prédictions car la majorité des résultats obtenus par notre algorithme Sécur PUE correspondait parfaitement aux résultats de la prédiction.

Comme perspectives, nous pouvons utiliser les mêmes algorithmes suggérés en essayant de réduire le nombre de message échangés ainsi que le temps d'exécution, nous pouvons également insérer les résultats obtenus par l'algorithme de sécurité dans la base de données des prédictions pour renforcer l'apprentissage.

Il serait même intéressant de penser à la gestion de la mobilité qui est primordiale dans les réseaux actuels et futurs et il est nécessaire de garantir la continuité et la qualité de service lors du déplacement des utilisateurs ce qui rend la tâche de gestion des ressources spectrales plus complexe.

RÉFÉRENCES BIBLIOGRAPHIQUES

[1] Metref, Adel. «Contribution à l'étude du problème de synchronisation de porteuse dans le contexte de la Radio Intelligente ». Thèse de Doctorat. Université Rennes 1, 2010.

[2] N. J. Drew, P. Tottle, « IC Technologies and Architectures to Support the Implementation of Software Define Radio Terminals », ACTS, Mobile Communications Summit, Rhodes, June 8-11, 1998.

[3] Ngom I. et Diouf L., « La radio cognitive », mémoire de Master, université Lille 1 USTL, 2008.

[4] Mitola, J., & Maguire Jr, G. Q. « Cognitive radio: making software radios more personal. Personal Communications », IEEE Personal Communications, volume 6 issue 4, page 13-18. 1999.

[5] Mitola, J. « Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio». Thèse de Doctorat. 2000.

[6] Amraoui Asma, Wassila Baghli, and Badr Benmammar. « Amélioration de la fiabilité du lien sans fil pour un terminal radio cognitive mobile ».Les 12èmes Journées Doctorales en Informatique et Réseaux (JDIR'11). 2011.

[7] T. W Malone, « Organizing information processing systems: parallels between human organizations and computer systems», Cognition, Computation and Cooperation, page.56-86. 1990.

[8] I.F. Akyildiz, W-Y. Lee, M.C. Vuran et S. Mohanty, « Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey, Computer Networks», vol.50, n°13, page 2127–2159. 2006

[9] S. Haykin, « Cognitive radio: Brain-empowered wireless communications», IEEE Journal on Selected Areas in Communications, vol. 23, pp. 201–220. 2005.

[10] ET Docket N° 04-186, « The FCC's Office of Engineering and Technology Releases Report On Tests of Prototype TV White Space DEVICES (Executive Summary) », Octobre 2008.

[11] A. Ben Dhaou, « Allocation dynamique des bandes spectrales dans les réseaux sans-fil à radio cognitive », mémoire de Maitrise en Informatique, Université du Québec à Montréal, Septembre 2011.

[12] Y. LAKYS, « Filtres à fréquence agile totalement actifs : théorie générale et circuits de validation en technologie SiGeBiCMOS 0.25µm ». Thèse présentée à l'université bordeaux 1, 3 décembre 2009.

[13] Glisic S., «ADVANCED WIRELESSNETWORKS Cognitive, Cooperative and Opportunistic 4G Technology», Second Edition, University of Oulu, Finland

[14] Moy, C., & Palicot, J.. Titre (français) : « Mieux analyser les ondes pour mieuxcommuniquer : la radio intelligente » Title (English) : « Betteranalyzewaves in order to bettercommunicate : cognitive radio », page 35-37. 2013.

[15] E. Hossain, D. Niyan and Zhu Han, « Dynamic Spectrum Access and management incognitive radio networks», Cambridge University Press 2009

[16] S. A. Ratsirarson, T. Rakotonirina, N. M. V Ravonimanantsoa, L. De Télécommunication, D. Signal, and I. L. Tasi, « Analyse Des Différents Types Des Fonctions De La Radio Cognitive. ». Rapport de recherche, Université d'Antananarivo, Madagascar, p. 06-06. 2015.

[17] Y. Hssaine, « Optimisation de la QOS dans un réseau de radio cognitive en utilisant les algorithmes génétiques », mémoire de Master, Université de Abou Bakr Belkaid, Tlemcen, Juin 2014

[18] Mitola J.and Maguire G., « Cognitive radio: Making software radios more personal», IEEE Personal Communications, Page: 13-18, August 1999.

[19] https://www.supinfo.com/articles/single/6041-machine-learning-introduction-apprentissage-automatique [Accessed: 26-May-2018].

[20] F. Rosenblatt. The perceptron: « A probabilistic model for information storage and organization in the brain. Psychological Review », 65:386–407, 1958. (Reprinted in Neurocomputing (MIT Press, 1988).).

[21] A. B. J. Novikoff. « On convergence proofs on perceptrons. In Proceedings of the Symposium on the Mathematical Theory of Automata », volume XII, pages 615–622, 1962.

[22] S. Agmon. « The relaxation method for linear inequalities ». Canadian Journal of Mathematics, 6(3):382–392, 1954.

[23] M. Collins. « Discriminative training methods for hidden markov models: Theory and experiments with perceptron algorithms». In Conference on Empirical Methods in Natural Language Processing, 2002.

[24] K. Crammer, O. Dekel, J. Keshet, S. Shalev-Shwartz, and Y. Singer. « Online passive aggressive algorithms ». Journal of Machine Learning Research, 7:551–585, Mar 2006.

[25] K. Crammer and Y. Singer. « A new family of online algorithms for category ranking ». In Proceedings of the 25th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, 2002.

[26] J. Kivinen and M.Warmuth. « Relative loss bounds for multidimensional regression problems». Journal of Machine Learning, 45(3):301–329, July 2001.

[27] C. Clancy, J. Hecker, E. Stuntebeck, and T. O'Shea, « Applications of Machine Learning to Cognitive Radio Networks, » IEEE Wirel. Commun. vol. 14, no. 4, pp. 47–52, 2007.

[28] L. Rabiner, « A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition, » Proc. IEEE, 1989.

[29] S. Haykin, «Neural Networks: A Comprehensive Foundation», Prentice Hall, 1998.

[30] D. Goldberg, « Genetic Algorithms in Search, Optimization, and Machine Learning », Addison Wesley, 1989.

[31] Z. Shu, Y. Qian, and S. Ci, «On physical layer security for cognitive radio networks, »IEEE Netw, vol. 27, no. 3, pp. 28–33, 2013.

[32] R. Chen, J. M. Park, and J. H. Reed, «Defense against primary user emulation attacks in Cognitive Radio networks,» IEEE J. Sel. Areas Commun, vol. 26, no. 1, pp. 25–37, 2008.

[33] I. Technology, «Survey of Security Issues in Cognitive Radio Networks Survey of Security Issues in Cognitive Radio Networks, » no. November 2014, 2011.

[34] M. Khasawneh and A. Agarwal, « A survey on security in cognitive radio networks, » 2014 6th Int. Conf. Comput. Sci. Inf. Technol. CSIT 2014 - Proc., no. July, pp. 64–70, 2014.

[35] D. Hlavacek and J. M. Chang, «A layered approach to cognitive radio network security: A survey, Comput. » Networks, no. PartA, pp. 414–436, 2014.

[36] Olga León, Juan Hernández-Serrano and Miguel Soriano, «Securing Cognitive Radio Networks, International Journal of Communication Systems, » Vol.23, No.5, page.633-652. 2010.

[37] T. C. Clancy et N. Goergen, « Security in cognitive radio networks: Threats and mitigation », in Cognitive Radio Oriented Wireless Networks and Communications. CrownCom 2008. 3rd International Conference on, page: 1–8. 2008

[38] Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang, Channel Surfng and Spatial Retreats: «Defenses Against Wireless Denial of Service, Proceedings of the 3rd ACM Workshop on Wireless Security, » Philadelphia, PA, January, page.80-89. 2004

[39] Ruiliang Chen and Jung-Min Park, «Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks, » First IEEE Workshop on Networking Technologies for Software Defined Radio Networks (SDR), Reston, VA, September, page.110-119, 2006

[40] O. Richard Afolabi, Kiseon Kim and Aftab Ahmad, «On Secure Spectrum Sensing in Cognitive Radio Networks Using Emitters Electromagnetic Signature, » Proceedings of 18th International Conference on Computer Communications and Networks (ICCCN 2009), San Francisco, CA, August, page.1-5. 2009

[41] Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood, «The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks, »Proceedings of ACM MobiHoc, Urbana, IL, page: 46-57. May, 2005

[42] Chetan Mathur and Koduvayur Subbalakshmi, «Security Issues in Cognitive Radio Networks, Cognitive Networks: Towards Self-Aware Networks, » Wiley, New York, page:.284-293. 2007

[43] C. Karlof ET D. Wagner, « Secure routing in wireless sensor networks: Attacks and countermeasures », Ad Hoc Netw., vol. 1, no 2, page: 293–315, 2003.

[44] F. Ouassini et B .Samira « Instauration d'un algorithme de sécurité pour l'accès dynamique au spectre dans un réseau radio cognitif », mémoire de Master, Université de Abou Bakr Belkaid, Tlemcen, Juillet 2017

[45] R. Chen, J.-M. Park, Y. T. Hou, et J. H. Reed, « Toward secure distributed spectrum sensing in cognitive radio networks », IEEE Commun. Mag., vol. 46, no 4, 2008.

[46] Y. Shei et Y. T. Su, « A sequential test based cooperative spectrum sensing scheme for cognitive radios », in Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on, page. 1–5. 2008

[47] W. Wang, H. Li, Y. Sun, et Z. Han, « Attack-proof collaborative spectrum sensing in cognitive radio networks », in Information Sciences and Systems, CISS 2009. 43rd Annual Conference on, page: 130–134. 2009.

[48] KaiguiBian and Jung-Min Park, «MAC-Layer Misbehaviors in Multi-hop Cognitive Radio Networks, » 2006 US-Korea Conference on Science, Technology, and Entrepreneurship (UKC2006), August, 2006

[49] L. Lazos, S. Liu, and M. Krunz. «Mitigating control-channel jamming attacks in multi-channel ad hoc networks». In Proceedings of the second ACM conference on Wireless network security, pages 169–180. ACM, 2009.

[50] L. Akter and B. Natarajan, «Distributed Approach for Power and Rate Allocation to Secondary Users in Cognitive Radio Networks, » IEEE Trans. Vehicular Technology, vol. 60, no. 4, page:. 1526- 1538, May 2011.

[51] Chris Karlof and David Wagner, «Secure Routing in Wireless Networks: Attacks and Countermeasures, » Ad Hoc Networks, Vol.1, page:.293-315. 2003

[52] Juan Hernandez-Serrano, «Olga León and Miguel Soriano, Modeling the Lion Attack in Cognitive Radio Networks, » EURASIP Journal on Wireless Communications and Networking, Vol.2011, Article ID 242304, 10 pages, 2011.

[53] I. Technology, « Survey of Security Issues in Cognitive Radio Networks Survey of Security Issues in Cognitive Radio Networks, » no. November 2014.

[54] «NetBeans IDE - Java EE Development. » [Online]. Available: https://netbeans.org/features/java-on-server/java-ee.html#. [Accessed: 05-Apr-2018].

[55] «About SQLite. » [Online]. Available: https://www.sqlite.org/about.html. [Accessed: 05-Apr-2018].

[56] «SQLite. » [Online]. Available: http://sql.sh/sgbd/sqlite. [Accessed: 05-Apr-2018].

[57] «Télécharger SQLite - 01net.com - Telecharger.com.» [Online]. Available: http://www.01net.com/telecharger/windows/Programmation/base_de_donne/fiches/133382.html. [Accessed: 05-Apr-2018].

[58] « Jade Site | Java Agent DEvelopment Framework. [Online] ». Available: http://jade.tilab.com/. [Accessed: 05-Apr-2018].

[59] « Chiffre de César. [Online] ». Available: http://www.cryptage.org/chiffre-cesar.html. [Accessed: 21-May-2018].

[60] « Outil Classifieur bayésien naïf. » [Online]. Available: https://help.alteryx.com/11.8/fr/Naive_Bayes.htm. [Accessed: 26-May-2018].

[61] O. François, « Comment Améliorer le Classifieur de Bayes Naïf ? » ,INSA Rouen - Laboratoire PSI - FRE CNRS 2645. IC 2005.

[62] https://github.com/AlexLusitania/BayesClassifier[Accessed: 26-May-2018].

[63] Spiegelhalter D. «Probabilistic prediction in patient management and clinical trials». Statistics in Medecine, 5, 421_433. 1986.

[64] Androutspoulos I., Palouras G., Karkaletsis V., Sakkis G., Spyro-poulos C. & Stamatopoulos P. « Learning to Filter Spam E-Mail: A Comparaison of a Naive Bayesian and a Memory-Based Approach». Rapport interne DEMO 2000/5, Dept. of Informatics, University of Athens. 2000.

[65] Sebe N., Lew M., Cohen I., Garg A. & T.S. H. « Emotion recognition using a cauchy naive bayes classifier ». In Proceedings of the International Conference on Pattern Recognition. 2002.

[66] Keren D. « Painter recognition using local features in naive bayes ». In Proceedings on the International Conference on Pattern Recognition. 2002.

[67] Zhou L., Feng J. & Sears A. « Applying the naive bayes classifier to assist user in detectind speech recognition errors ». In Proceedings of the 38th Hawaï International Conference on System Science. 2005.

[68] B. Lavoie, « Apprentissage automatique de règles, » 2006.

Annexe A

L’algorithme TOPSIS

La méthode « TOPSIS » (Technique for Order Preference by Similarity to Ideal Solution) a été développée à l'origine par Hwang et Yoon en 1981 avec, notamment, d'autres développements de Yoon en 1987, et Hwang, Lai et Liu en 1993.

TOPSIS est une méthode d’analyse multicritères pour l'aide à la prise de décision. L’idée principale de cette méthode est de choisir l’action ayant :

- La plus petite distance à l’action dite « idéale » (positive-ideal solution).
- La plus grande distance à l’action dite « anti-idéale » (negative-ideal solution).

Exemple de l'algorithme TOPSIS

A. Données

- Le client désire acheter une voiture et ne sait pas laquelle choisir parmi les marques et les modèles suivantes (Renault Scenic, Volkswagen Golf, Ford Focus, Peugeot 407, Citroen C3 Picasso). L'algorithme TOPSIS peut aider le client à faire le meilleur choix en se basant sur les critères suivants: Style, Fiabilité, Consommation, Coût.

Pour les critères positifs (Style, Fiabilité), plus le score est important plus le critère est positif (favorable).

Pour les critères négatifs (Consommation, Coût), plus le score est important plus le critère est négatif (défavorable).

Nous avons attribué pour chaque critère une pondération (un poids qui reflète l'importance du critère dans notre choix final). Les pondérations doivent être définies de sorte est ce que leur somme soit égale à 1. Généralement elles sont définies en %. Même si les poids ne sont pas compris entre **0** et **1**, on peut toujours les ramener à l'intervalle **[0, 1]** en divisant tout simplement chaque poids par la somme de tous les poids. Les pondérations suivantes sont attribuées aux 4 critères cités auparavant dans l'ordre : Poids $\mathbf{w_j}$ **= {0.1, 0.4, 0.2, 0.3}**.

Matrice des données

	Alternative	Style	Fiabilité	Consommation	Coût
Alternatives	Renault Scenic	**6**	**5**	**5**	**5**
	Volkswagen Golf	**6**	**7**	**6**	**6**
	Ford Focus	**7**	**7**	**5**	**6**
	Peugeot 407	**7**	**7**	**5**	**7**
	Citroen C3Picasso	**5**	**5**	**4**	**4**

B. Analyse

Étape 1: Calcul des préférences normalisées

Nous voulons maintenant normaliser tous les scores de la matrice des niveaux attribués aux critères. Pour cela nous allons appliquer la formule indiquée ci dessous pour obtenir les nouvelles entrées $\mathbf{r_{ij}}$ de la matrice.

$$\mathbf{r_{ij}} = \frac{\mathbf{x_{ij}}}{\sqrt{\sum_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{x_{ij}}^{\mathbf{2}}}}$$

Alternative	Style	Fiabilité	Consommation	Coût
Renault Scenic	**0,430**	**0,356**	**0,444**	**0,393**
Volkswagen Golf	**0,430**	**0,499**	**0,532**	**0,471**
Ford Focus	**0,501**	**0,499**	**0,444**	**0,471**
Peugeot 407	**0,501**	**0,499**	**0,444**	**0,550**
Citroen C3Picasso	**0,358**	**0,356**	**0,355**	**0,314**

Étape 2: Calcul des préférences normalisées avec des poids associés aux critères

Dans cette étape, on multiplie simplement toutes les entrées ($\mathbf{r_{ij}}$) de la matrice normalisée par la pondération associée à chaque critère.

$$\mathbf{r_{ij}} = \mathbf{w_j} \times \mathbf{x_{ij}}$$

Poids (w) / Alternative	0.1	0.4	0.2	0.3
	Style	Fiabilité	Consommation	Coût
Renault Scenic	**0,043**	**0,142**	**0,089**	**0,118**
Volkswagen Golf	**0,043**	**0,199**	**0,106**	**0,141**
Ford Focus	**0,050**	**0,199**	**0,089**	**0,141**
Peugeot 407	**0,050**	**0,199**	**0,089**	**0,165**
Citroen C3Picasso	**0,036**	**0,142**	**0,071**	**0,094**

Étape 3: Identification des solutions idéales et anti-idéales

	j^+		j^-	
Alternative	**Style**	**Fiabilité**	**Consommation**	**Coût**
Renault Scenic	**0.043**	**0.142**	**0.089**	**0.118**
Volkswagen Golf	**0.043**	**0.199**	**0.106**	**0.141**
Ford Focus	**0.050**	**0.199**	**0.089**	**0.141**
Peugeot 407	**0.050**	**0.199**	**0.089**	**0.165**
Citroen C3Picasso	**0.036**	**0.142**	**0.071**	**0.094**

Déterminer la solution idéale	**Déterminer la solution anti-idéale**
$\mathbf{A^+} = \{0.050, 0.199, 0.071, 0.094\}$	$\mathbf{A^-} = \{0.036, 0.142, 0.106, 0.165\}$
$\mathbf{A^+} = \{\mathbf{max_i x_{ij}(i \in j^+) \mid min_i x_{ij}(i \in j^-)}\}$	$\mathbf{A^-} = \{\mathbf{min_i x_{ij}(i \in j^+) \mid max_i x_{ij}(i \in j^-)}\}$
$\mathbf{A^+} = \{\mathbf{r_j{}^+ j = 1, \dots, m}\}$	$\mathbf{A^-} = \{\mathbf{r_j{}^- j = 1, \dots, m}\}$

Alternative	Style	Fiabilité	Consommation	Coût
Renault Scenic	$\mathbf{(0,043 - 0.050)^2}$	$\mathbf{(0,142 - 0.199)^2}$	$\mathbf{(0,089 - 0.071)^2}$	$\mathbf{(0,118 - 0.094)^2}$
Volkswagen Golf	$\mathbf{(0,043 - 0.050)^2}$	$\mathbf{(0,199 - 0.199)^2}$	$\mathbf{(0,106 - 0.071)^2}$	$\mathbf{(0,141 - 0.094)^2}$
Ford Focus	$\mathbf{(0,050 - 0.050)^2}$	$\mathbf{(0,199 - 0.199)^2}$	$\mathbf{(0,089 - 0.071)^2}$	$\mathbf{(0,141 - 0.094)^2}$
Peugeot 407	$\mathbf{(0,050 - 0.050)^2}$	$\mathbf{(0,199 - 0.199)^2}$	$\mathbf{(0,089 - 0.071)^2}$	$\mathbf{(0,165 - 0.094)^2}$
Citroen C3Picasso	$\mathbf{(0,036 - 0.050)^2}$	$\mathbf{(0,142 - 0.199)^2}$	$\mathbf{(0,071 - 0.071)^2}$	$\mathbf{(0,094 - 0.094)^2}$

Étape 4: Calcul des distances de séparation

Alternative	E^+
Renault Scenic	**0,064580**
Volkswagen Golf	**0,059442**
Ford Focus	**0,050370**
Peugeot 407	**0,072904**
Citroen C3Picasso	**0,058770**

$$E^+{}_i = \sqrt{\sum_{j=1}^{m} (r_j{}^+ - r_{ij})^2}$$

Alternative	Style	Fiabilité	Consommation	Coût
Renault Scenic	$(0,043 - 0.036)^2$	$(0,142 - 0.142)^2$	$(0,089 - 0.106)^2$	$(0,118 - 0.165)^2$
Volkswagen Golf	$(0,043 - 0.036)^2$	$(0,199 - 0.142)^2$	$(0,106 - 0.106)^2$	$(0,141 - 0.165)^2$
Ford Focus	$(0,050 - 0.036)^2$	$(0,199 - 0.142)^2$	$(0,089 - 0.106)^2$	$(0,141 - 0.165^2$
Peugeot 407	$(0,050 - 0.036)^2$	$(0,199 - 0.142)^2$	$(0,089 - 0.106)^2$	$(0,165 - 0.165)^2$
Citroen C3Picasso	$(0,036 - 0.036)^2$	$(0,142 - 0.142)^2$	$(0,071 - 0.106)^2$	$(0,094 - 0.165)^2$

Alternative	E^-
Renault Scenic	**0,050877**
Volkswagen Golf	**0,062093**
Ford Focus	**0,065760**
Peugeot 407	**0,061391**
Citroen C3Picasso	**0,079119**

$$E^-{}_i = \sqrt{\sum_{j=1}^{m} (r_j{}^- - r_{ij})^2}$$

Étape 5: Calcul de l'index de similarité à la solution idéale

$$S^*{}_i = E^-{}_i / (E^-{}_i + E^+{}_i)$$

Alternative	S*	Ordre de choix
Renault Scenic	**0,44066**	**5**
Volkswagen Golf	**0,51091**	**3**
Ford Focus	**0,56626**	**2**
Peugeot 407	**0,45714**	**4**
Citroen C3Picasso	**0,57379**	**1**

→ **Meilleure solution**

Annexe B

Le classifieur NAIVE BAYES

Le classifieur naïf bayésien est l'une des méthodes les plus simples en apprentissage supervisé basée sur le théorème de Bayes. C'est un résultat de base en théorie des probabilités, issu des travaux du révérend Thomas Bayes (1702-1761), présenté à titre posthume en 1763.

Il crée un modèle de classification probabiliste binomial ou multinomial de la relation entre un jeu de variables prédictives et une variable cible catégorielle. Le classifieur bayésien naïf suppose que toutes les variables prédictives sont indépendantes l'une de l'autre, et prédit, en fonction d'une entrée d'échantillon, une distribution de probabilité sur un jeu de classes. Il calcule ainsi la probabilité d'appartenance à chaque classe de la variable cible.

L'un des principaux avantages du classifieur bayésien naïf est qu'il obtient de bons résultats même avec un petit jeu d'apprentissage. Cet avantage est lié au fait que le classifieur bayésien naïf est paramétré par la moyenne et la variance de chaque variable indépendante de toutes les autres variables. [60]

Le classifieur de Bayes naïf est très largement utilisé. Ce modèle est aisé à mettre en œuvre et a prouvé son efficacité pour de nombreuses applications. Par exemple, Spiegelhalter [63] l'avait utilisé dans un cadre médical. Androutspoulos et al. [64] a utilisé ce modèle pour faire de la détection de courriers électroniques indésirables. Et récemment, il a été incorporé à des clients de messageries électroniques de renom. Sebe et al. [65] a utilisé ce modèle pour faire de la détection d'émotion à partir de l'image du visage d'une personne. De l'identification de peintre a été faite sur la base de classifieur naïf Keren [66]. Ou encore, Zhou et al. [67] l'a utilisé pour automatiser la détection d'erreur d'un système de reconnaissance de la parole. [61]

Une classification bayésien se fait en 3 étapes :

- **Une phase d'apprentissage** : Elle permet de déterminer les probabilités a priori, la moyenne et la matrice de covariance de chaque classe.

- **Une phase de développement** : Elle compare les différentes variantes du classifieur afin de minimiser son taux d'erreur.
- **Une phase d'évaluation** : C'est la partie qui intéresse le client, elle permet à partir des données d'apprentissage de déterminer la classe d'un exemple donné. [62]

Exemple de l'algorithme Naive Bayes

Utiliser le modèle Naive Bayes pour classer les journées futures :

- **oui** (jouer au tennis).
- **Non** (ne pas jouer au tennis).

Perspective			Temps		Humidité		Vent			Jouer	
	oui	non	Oui	Non	oui	non		oui	non	oui	non
Ensoleillé	**2**	**3**	**64.68**	**65.71**	**65.70**	**70.85**	**Faux**	**6**	**2**		
Pleuvoir	**3**	**2**	**69.70**	**72.80**	**70.75**	**90.91**	**Vrai**	**3**	**3**	**9**	**5**
Couvert	**4**	**0**	**72**	**85**	**80**	**95**					

Calcule de L'espérance μ et la variance σ^2

$$\mu = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad \sigma = \frac{1}{(N-1)}\sum_{i=1}^{N}(x_i - \mu)^2$$

Où N est le nombre d'échantillons et x_i est la valeur d'un échantillon donné.

Note: On divise par N-1 car c'est une estimation de la variance.

Perspective			Temps		Humidité		Vent			Jouer	
	oui	non	Oui	Non	oui	non		oui	non	oui	non
Ensoleillé	**2/9**	**3/5**	**μ = 73**	**μ = 75**	**μ = 79**	**μ = 85**	**Faux**	**6/9**	**2/5**	**9/14**	**5/14**
Pleuvoir	**3/9**	**2/5**	**σ = 6.2**	**σ = 7.9**	**σ = 10.2**	**σ = 9.7**	**Vrai**	**3/9**	**3/5**		
Couvert	**4/9**	**0/5**									

Perspective	Temps	Humidité	Vent	Jouer
Ensoleillé	66	90	Vrai	?

Nous pouvons à présent savoir si le joueur peut jouer ou non on appliquant la formule suivant :

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{(x-\mu)^2}{2\sigma^2}\right]$$

P (oui) = 2/9 * 0.0340 * 0.0221 * 3/9 * 9/14 = 0.000036

P (non) = 3/5 * 0.0291 * 0.0380 *3/5 * 5/14 = 0.000136

P (instance | oui) = P (oui)/(P (oui) + P (non))*100 = 0.000036/(0.000036+0.000136)*100 = 20.9 %

P (instance | non) = P (non)/(P (oui) + P (non))*100 = 0.000136/(0.000036+0.000136)*100 = 79.1 %

Conclusion : puisque P (instance | non)> P (instance | oui) donc jouer = non le joueur ne peux pas jouer.

Résumé

La radio cognitive est une technologie qui permet d'améliorer considérablement l'utilisation du spectre radio en permettant d'exploiter le spectre sans fil de façon opportuniste. Dans notre mémoire, nous nous sommes intéressées à sécuriser un réseau de radio cognitive contre l'attaque PUE (Primary User Emulation). Pour cela, nous avons proposé une méthode Sécur PUE en utilisant l'algorithme TOPSIS pour choisir la meilleure offre et un autre algorithme pour l'apprentissage automatique qui est Naive bayes.

Mots-clés : Radio cognitive – Sécurité – Apprentissage automatique - Algorithme TOPSIS – Sécur PUE.

Abstract

Cognitive radio is a technology that improves the use of the radio spectrum by allowing opportunistic exploitation of the wireless spectrum. In our brieve dissertation, we are interested in securing the cognitive radio network against the PUE (Primary User Emulation) attack. For this, we proposed a Safe PUE method using the TOPSIS algorithm to choose the best offer and another algorithm for machine learning that is Naive bayes.

Keywords: Cognitive radio - Security - Machine Learning - TOPSIS Algorithm - Sécur PUE.

ملخص

الراديو المعرفي (الإدراكي) هو تقنية تعمل بشكل كبير على تحسين استخدام الطيف الراديوي من خلال السماح بالاستغلال الانتهازي للطيف اللاسلكي. في هذه المذكرة نحن مهتمون بتأمين شبكة الراديوية الإدراكية ضد هجوم محاكاة المستخدم الأساسي لهذا ، اقترحنا طريقة محاكاة المستخدم الأساسي المؤمن باستخدام خوارزمية الراديو المعرفي الأمثل لترتيب الافضليات عن طريق التشابه مع الحل المثالي لاختيار أفضل عرض وخوارزمية أخرى لتعلم التلقائي الآلي.

الكلمات المفتاحية : الراديو المعرفي - الأمن - التعلم التلقائي الآلي - خوارزمية الراديو المعرفي الأمثل - محاكاة المستخدم الأساسي المؤمن