الجـــــــــــــمهـوريـــــة الجـــــــــــــزائـريـة الديمـــــــقـراطيـة الشـــــــــعبيـة

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التـــــــــــــــــــــــــــعليـم العـــــــالي و البـــــــــــحث العـــــلـمـــي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جـــــــــــــــامعة أبي بكـــر بـلـقـايد – تـلمســـــــــــــــان –

Université Aboubakr Belkaïd – Tlemcen –

Faculté des Sciences

MEMOIRE

Présenté pour l'obtention du **diplôme** de **MASTER**

En : Informatique

Spécialité : Réseaux et Système Distribué (R.S.D)

Par : Bessaid Fatima Zohra

Thème

Amélioration de la sécurité des réseaux de radio cognitive

Soutenu publiquement, le 30 / 09 / 2024, devant le jury composé de :

Mr. LEHSAINI Mohammed	Univ. Tlemcen	Président
Mme. AMRAOUI Asma	Univ. Tlemcen	Directeur de mémoire
Mr. BENMOUNA Youcef	Univ. Tlemcen	Examinateur

Année Universitaire 2023-2024

Remerciement

Je tiens tout d'abord à exprimer ma profonde gratitude à Dieu tout-puissant pour m'avoir donné la force et la détermination nécessaires à l'achèvement de ce travail.

Je remercie chaleureusement Mme AMRAOUI Asma, encadrante de ce mémoire, pour son encadrement, ses conseils avisés, et ses précieuses discussions qui ont grandement enrichi mes recherches.

Je tiens également à exprimer ma gratitude aux membres du jury Mr BENMOUNA Youcef et Mr LEH-SAINI Mohammed enseignants à l'Université de Tlemcen, pour avoir accepté d'examiner ce travail.

Je souhaite remercier chaleureusement nos enseignants pour l'excellence de l'enseignement qu'ils nous ont offert au cours de ces cinq années, ainsi que le département d'Informatique de la faculté des sciences pour son précieux soutien.

Je souhaite exprimer ma profonde reconnaissance et mes sincères remerciements à tous ceux qui, de près ou de loin, ont participé à la réalisation de ce mémoire de fin d'études. J'adresse également mes remerciements les plus chaleureux à mes chers parents pour leur soutien inestimable, leur contribution, et leur patience tout au long de mes études.

Dédicaces

Je tiens d’abord à remercier le dieu le tout puissant qui m’a donné la force et la patience d’accomplir ce modeste travail.

C’est un plaisir de dédier ce travail à ceux qui ont une source d’inspiration, de volonté et d’encouragement au cours de mes études.

À mes chers parents,

Sources de mon inspiration et gardiens de mon bonheur.

Grâce à vos sacrifices infinis et à votre amour inconditionnel, j'ai pu grandir et m'épanouir dans un environnement rempli de tendresse et de bienveillance.

Ce travail est le fruit de votre dévouement sans bornes et de votre foi inébranlable en mes capacités.

À mon cher mari,

Mon âme sœur, mon confident, mon meilleur ami,

Les mots ne suffiraient jamais à exprimer l'immensité de mon amour pour toi. Depuis le jour où nos chemins se sont croisés, tu as illuminé ma vie d'une lumière que je n'avais jamais connue auparavant. Tu es mon roc, mon pilier de force, l'homme qui me fait rire et qui me sèche les larmes. Avec toi, je sais que je peux affronter n'importe quel obstacle, car je sais que tu seras toujours là pour me soutenir et m'encourager.

À ma chère fille,

Mon soleil, ma raison d'être,

Depuis le jour où tu es née, tu as illuminé ma vie d'une lumière que je n'avais jamais connue auparavant.

Table des matières

Liste des figures

Listes des tableaux

Listes des abréviations

ABAC	Attributs Based Access Contrôle
CCS	Control Channel Saturation
CCSD	Control Channel Saturation DoS
KTH	Kungliga Tekniska Högskolan
MIMO	Multiplexage Input Multiplexage Output
MSU	Malicious Secondary User
OFDM	Orthogonal Frequency-Division Multiplexing
PU	Primary User
PUE	Primary User Emulation
RDL	Radio Définie par Logiciel
RRC	Résaux de Radio Cognitive
RSS	Received Signal Strength
RBAC	Role Based Access Contrôle
SDR	Software Defined Radio
SSDF	Spectrum Sensing Data Falsification
SCN	Selfish Channel Negociation
SU	Secondary User
WSN	Wireless Sensor Network
WSPRT	Weighted Sequential Probability Ratio Test

Introduction générale

De plus en plus, les besoins en communication augmentent constamment, que ce soit à des fins de contrôle, de vidéosurveillance ou pour de nouveaux services à la clientèle. Cela a entraîné des problèmes de coexistence et d'interopérabilité entre les systèmes, ainsi qu'une disponibilité limitée des fréquences.

En outre, ces systèmes doivent répondre à des exigences telles que la disponibilité, la continuité du service, l'hétérogénéité du trafic, la robustesse et la qualité de service pour les applications, même dans des environnements très mobiles, quels que soient les contextes (zones rurales, tranchées, tunnels).

Les normes émergentes (IEEE 802.16m, IEEE 802.20, A-LTE) [1], basées sur la technologie MIMO et l'OFDM multi-porteuses [2], pourraient potentiellement répondre aux besoins des systèmes de transport intelligents (ITS) en termes de débit de données [3]. Cependant, les développements actuels reposent principalement sur la transmission/réception à une seule antenne, ce qui nécessite de nouvelles approches pour intégrer la technologie MIMO-OFDM avec plusieurs antennes.

La gestion statique du spectre des fréquences radio dans les réseaux de communication traditionnels entraîne une pénurie de bandes disponibles, c'est-à-dire que beaucoup de spectres alloués ne sont utilisés que sporadiquement. Afin de résoudre ce problème, l'utilisation du spectre radio implique l'application de la technologie de la radio cognitive (RC). Les principales méthodes pour maximiser les avantages de cette technologie incluent l'allocation efficace des ressources radio et l'analyse de l'environnement radio [4].

La radio cognitive est avancée comme une technologie prometteuse pour concrétiser le concept d'intelligence dans les réseaux de communication, offrant une réponse pertinente au défi de la rareté des ressources. Elle propose une approche opportuniste dans l'utilisation des bandes de fréquences, ouvrant ainsi la voie à une exploitation dynamique du spectre.

L'objectif de ce mémoire est de fusionner deux concepts majeurs : le premier est la radio cognitive, qui vise à encourager l'honnêteté des utilisateurs ; le deuxième est la sécurité dans la radio cognitive, qui cherche à élaborer une méthode robuste pour renforcer la sécurité des réseaux cognitifs.

Dans le premier chapitre, nous présentons une explication détaillée et explicite de la radio cognitive (RC), en mettant en lumière ses composants, ses fonctionnalités et ses différences avec la radio logicielle. Nous abordons également son architecture, en détaillant ses fonctionnalités et ses domaines d'application. De plus, nous examinons les attaques spécifiques qui ciblent chaque couche du réseau.

Dans le deuxième chapitre, nous abordons la sécurité des réseaux de radio cognitive, en soulignant les enjeux clés tels que l'intégrité et la confidentialité des données. Nous présentons différents types d'attaques, comme la radio politique et la radio d'apprentissage, ainsi que les menaces à chaque couche du modèle OSI. La section sur le contrôle d'accès définit ses principes, en discutant des systèmes, des politiques, des modèles et des mécanismes associés. Ces éléments sont essentiels pour garantir la sécurité des réseaux cognitifs dans un environnement en constante évolution.

Le troisième chapitre est dédié à la mise en œuvre de notre application web. Nous y détaillons l'architecture et les étapes clés du processus. Ce chapitre inclut également un aperçu de l'environnement de conception et de développement, ainsi que la présentation des résultats obtenus.

Chapitre I : Radio Cognitive

I.1 Introduction

Les progrès récents dans le domaine des réseaux mobiles et sans fil ont été considérables au cours des dernières années. Les réseaux locaux sans fil, notamment les normes prééminentes telles que WiFi, Bluetooth et autres, sont devenus des composants essentiels de notre quotidien. De plus, les générations successives de réseaux de télécommunication, initialement axées sur la téléphonie, ont évolué vers des infrastructures multimédias.

Le paysage des normes et des standards de télécommunication connaît actuellement une multiplication due aux avancées notables dans ce domaine. Cette prolifération de standards élargit la gamme des offres et des services disponibles pour chaque consommateur, même si la plupart des fréquences radio disponibles ont déjà été attribuées.

Il est désormais largement admis que les systèmes de communication numériques sans fil n'exploitent pas pleinement l'intégralité de la bande de fréquences à leur disposition. Les systèmes sans fil des générations futures devront tirer parti des bandes de fréquences inoccupées en s'appuyant sur leur capacité à surveiller et à s'adapter à leur environnement.

L'évolution des technologies a toujours été influencée par les besoins du moment et la disponibilité des techniques. Cette progression s'est traduite par la transition de la radio analogique à la radio numérique, entraînant des avancées notables en termes de qualité, de rapidité, de fiabilité du transport de l'information et de capacité réseau.

Dans ce chapitre, nous examinerons la radio cognitive sous divers angles : ses principes, son architecture, son cycle cognitif, ses fonctions, ses composants et ses domaines d'application.

I.2 Radio cognitive

I.2.1 Historique

L'idée fondatrice de la radio cognitive a été officiellement présentée par Joseph Mitola III lors d'un séminaire à l'Institut royal de technologie (KTH) en 1998, puis publiée ultérieurement dans un article rédigé par Mitola et Gerald Q. Maguire, Jr en 1999 [5].

Reconnu comme le "Père de la radio logicielle", le Dr. Mitola est l'un des auteurs les plus influents dans ce domaine. Il fusionne son expertise en radio logicielle avec sa passion pour l'apprentissage automatique et l'intelligence artificielle pour développer la technologie de

la radio cognitive. Selon ses propos, « Une radio cognitive peut connaître, percevoir et apprendre de son environnement puis agir pour simplifier la vie de l'utilisateur ».

De plus, Cette recherche visait à détailler les radios intelligentes capables de prendre des décisions de manière autonome en se basant sur les informations collectées sur l'environnement RF grâce à un modèle de raisonnement. De plus, ces radios peuvent également apprendre et planifier en fonction de leur expérience passée. Il est évident que pour atteindre un tel niveau d'intelligence, la radio doit posséder une conscience de soi, être attentive au contexte et comprendre le contenu [6].

I.2.2 Définition

La radio cognitive constitue une modalité de communication sans fil où un émetteur/récepteur peut intelligemment détecter les canaux de communication actuellement utilisés ainsi que ceux qui sont inoccupés, et a la capacité de se déplacer vers les canaux disponibles. Cette approche vise à maximiser l'utilisation des fréquences radio disponibles dans le spectre, tout en réduisant au minimum les interférences avec d'autres utilisateurs [7].

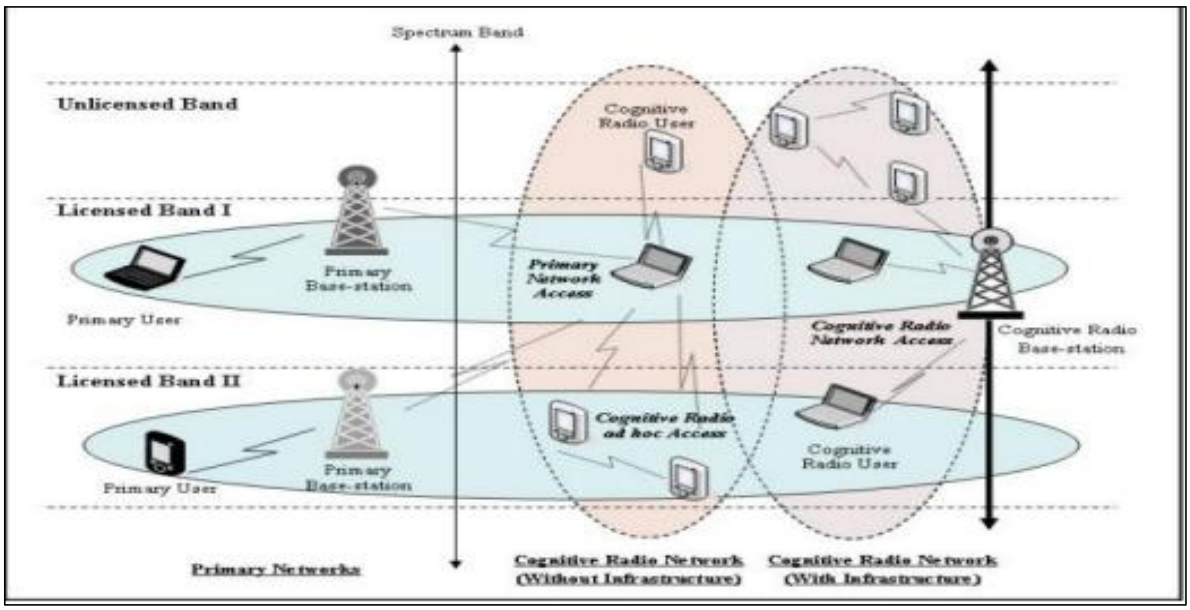

Figure I- 1: Illustration d'un réseau de radio cognitif [8]

I.2.3 Radio logicielle

La radio logicielle est une approche novatrice dans le domaine de la conception des système radio, elle englobe un ensemble de technologies visant à spécifier les paramètres et les caractéristiques des émetteurs-récepteurs radio, tels que la fréquence des opérations, la bande passante de modulation, le codage des canaux, ainsi que l'agilité en termes de fréquence, d'espace, de temps et de code. Dans les générations précédentes de systèmes de télécommunications, bien que certains de ces paramètres et fonctionnalités aient été

occasionnellement personnalisables, ils étaient principalement déterminés par le matériel, avec une programmation limitée au traitement du signal numérique en bande de base [9].

Après un développement de plusieurs années, a émergé un nouveau concept connu sous le nom de radio logicielle restreinte (software defined radio ou SDR). Ce concept englobe un ensemble de technologies matérielles et logicielles dans lesquelles certaines ou toutes les fonctions opérationnelles de la radio, également désignées sous le nom de traitement de couche physique, sont mises en œuvre via un logiciel ou un microprogramme modifiable fonctionnant sur des technologies de traitement programmables. Ces dispositifs comprennent des tableaux de portes programmables sur site, des processeurs de signaux numériques, des processeurs à usage général ou d'autres processeurs programmables spécifiques à l'application. L'utilisation de ces technologies permet l'intégration de nouvelles fonctionnalités et capacités sans fil aux systèmes radio existants, sans nécessiter de nouveau matériel.

I.2.4 Relation entre radio cognitive et radio logicielle restreinte

Les domaines de recherche concernant les systèmes de radio cognitive sont en pleine expansion, et des études et expérimentations sont actuellement en cours.

Certains systèmes intégrant des fonctionnalités cognitives ont déjà été mis en service, et certaines autorités permettent l'utilisation de ces systèmes (par exemple, la modulation dynamique de la fréquence). Ces autorités disposent de processus d'approbation nationaux pour garantir la protection des services existants contre toute interférence nuisible. Néanmoins, l'implémentation de technologies de radio cognitive dans un système radio peut avoir des répercussions sur les pays voisins, et une coordination peut s'avérer nécessaire. Lorsque des applications utilisent la technologie des systèmes radio cognitifs dans une optique de non-interférence et de non-protection, l'administration concernée doit prendre les mesures nécessaires pour éviter la génération d'interférences.

La technologie de radio logicielle restreinte est actuellement opérationnelle dans divers systèmes et réseaux, notamment les services mobiles, de radiodiffusion et de radiodiffusion par satellite, ainsi que les systèmes fixes et mobiles par satellite. Elle apporte une flexibilité dans la conception des systèmes radio et peut contribuer à assurer une compatibilité directe.

Le concept de systèmes de radio logicielle restreinte et de systèmes de radio cognitive est susceptible d'évoluer graduellement en raison de divers facteurs, dont l'état actuel de la technologie. L'intégration de ces technologies au sein de certains groupes peut présenter des défis particuliers et singuliers d'ordre technique ou opérationnel, nécessitant une évaluation minutieuse et approfondie de l'Union internationale des télécommunications.

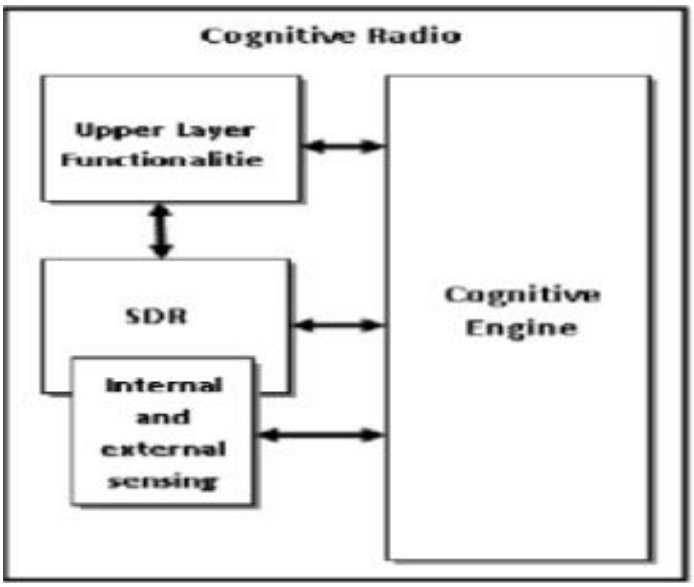

Figure I- 2: Relation entre radio cognitive et SDR [10]

I.2.5 Principe de la radio cognitive

La radio cognitive offre la possibilité d'exploiter des portions de spectre temporairement non utilisées, souvent désignées sous les termes de "trous de spectre" ou "espaces blancs". En cas d'utilisation continue de cette bande par un utilisateur autorisé, la radio cognitive permet de basculer vers un autre espace blanc en ajustant soit la puissance de transmission, soit le schéma de modulation, afin d'éviter toute interférence.Pour cela la RC se divisent en deux catégories distincts:

a) Utilisateurs primaires (PU)

Ils sont également appelés utilisateurs licenciés, sont ceux détenteurs d'une licence qui leur accorde le privilège d'opérer sur des bandes spectrales réservées exclusivement à leur usage. Ils bénéficient ainsi du droit de communiquer librement à tout moment sur leurs fréquences attribuées.

b) Utilisateurs secondaires (SU)

Ils exploitent le spectre de manière opportuniste, mais ils doivent être attentifs à ne pas perturber les utilisateurs principaux. En effet, ils assument la responsabilité de garantir l'absence d'interférences avec ces utilisateurs primaires.

En plus, à une période précise et à une localisation géographique particulière, il peut arriver qu'un utilisateur principal cesse d'utiliser sa plage de fréquences. Par conséquent,

d'autres utilisateurs secondaires peuvent tirer parti de ces fréquences en exploitant des lacunes dans le spectre. La figure I.3 montre que, sans causer de perturbations aux communications des utilisateurs principaux, les systèmes sans fil actuels ont néanmoins été développés pour opérer sur des fréquences spécifiques, ce qui limite leur capacité à bénéficier de cette flexibilité envisagée.

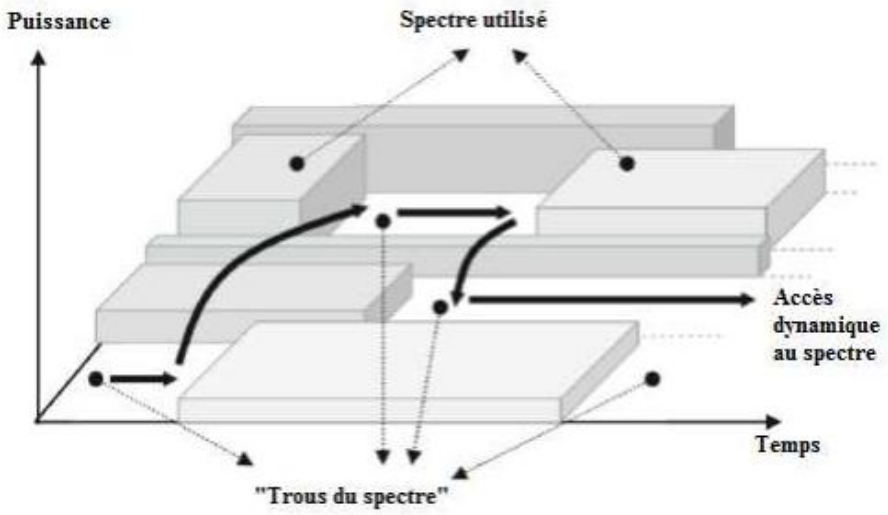

Figure I- 3: Principe des "trous du spectre" [11]

I.2.6 Architecture de la radio cognitive

L'architecture de la radio cognitive montrée dans la figure I.4 se caractérise par l'uniformité résultant de diverses lois de conception. C'est grâce à cette uniformité que différents composants interagissent pour générer une série de fonctions, de produits et de services, comme expliqué par [12].

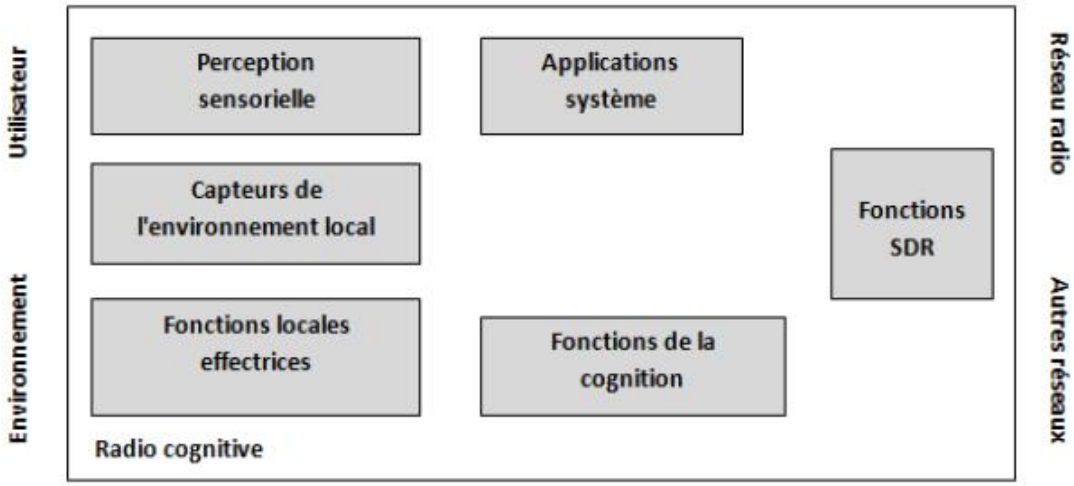

Figure I- 4: Architecture de la radio cognitive

Les six éléments fonctionnels qui forment l'architecture d'une radio cognitive sont :

- La perception sensorielle de l'utilisateur englobe l'interface haptique (relatif au toucher), les éléments acoustiques, la vidéo, ainsi que les fonctions de détection et de perception.
- Les capteurs de l'environnement local (emplacement, température, accéléromètre, etc.)
- Les applications système (services médias autonomes tels qu'un jeu en réseau).
- Les fonctions SDR (qui comportent la détection RF et les applications radio de la SDR).
- Les fonctions de la cognition (dédiés aux systèmes de contrôle, de planification et d'apprentissage).
- Les fonctionnalités locales effectives (comprenant la synthèse de la parole, du texte, des graphiques et l'affichage multimédia).

I.2.7 Cycle cognitif

Le cycle cognitif implique plusieurs étapes, comme illustré dans la figure I.5. Cette représentation détaille le cycle, débutant par l'observation et se poursuivant jusqu'à l'action, permettant ainsi à la radio cognitive d'interagir avec son environnement. Les systèmes cognitifs, tout en évoluant au fil du temps, accomplissent les phases d'observation, d'orientation, de planification, de prise de décision et d'action. Ils apprennent continuellement de leur environnement pour accroître leur efficacité. Les différentes phases du cycle cognitif se déroulent de la manière suivante :

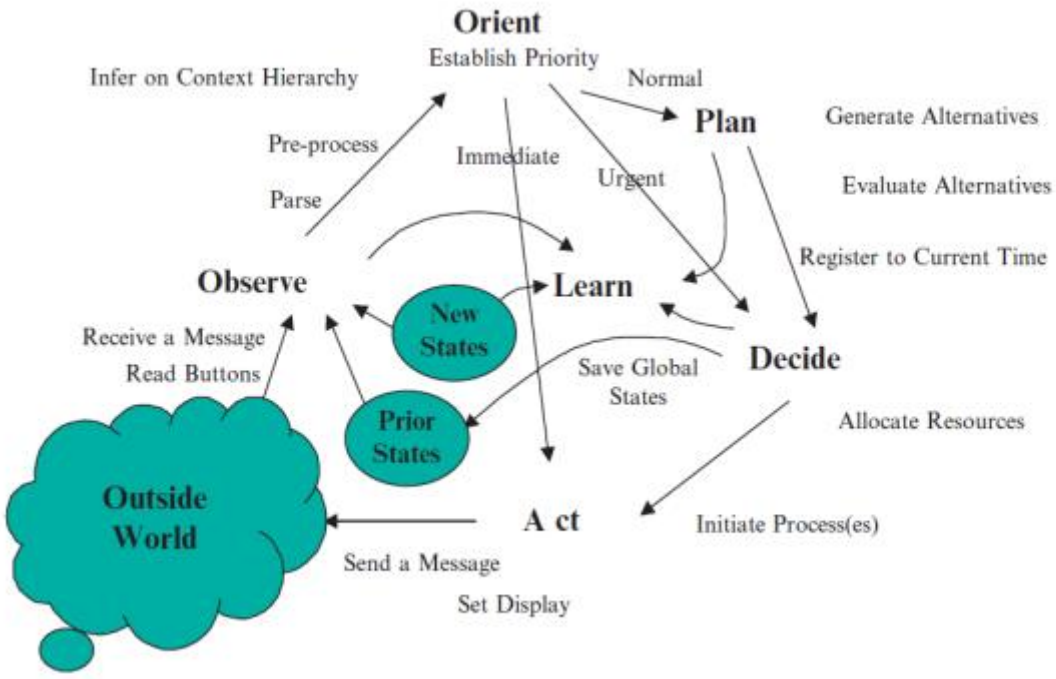

Figure I- 5: Cycle cognitif [13]

- **Phase observation (observe)**

Lors de la phase d'observation, la radio cognitive examine l'environnement et analyse le flux entrant pour repérer les éléments nouveaux.

- **Phase orientation (Orient)**

Au cours de la phase d'orientation, la radio cognitive évalue l'importance de l'observation et la vigueur de la réponse, parfois entraînant une action immédiate sous forme de comportement réactif.

- **phase planification (Plan)**

Durant la phase de planification, un message provenant du réseau serait généralement traité par la création d'un plan. Pour garantir une qualité industrielle des radios cognitives, des modèles formels de causalité seraient intégrés dans les outils de planification. Le plan devrait également englober la phase de raisonnement dans le temps.

- **Phase decision (Decide)**

Un plan est choisi parmi plusieurs plans potentiels. La radio peut avertir l'utilisateur d'un message entrant ou différer l'interruption en fonction des niveaux prédéfinis de la Qualité de l'Information (QoI) au cours de cette phase.

- **Phase action (Act)**

Cette étape initie les processus choisis, qui peuvent être orientés soit vers le monde extérieur, soit vers les états internes de la radio cognitive. L'interaction avec le monde extérieur implique initialement la composition de messages destinés à être transmis dans l'environnement sous forme audio ou exprimés dans divers langages. Les actions sur les états internes englobent la gestion de ressources telles que les canaux radio. De plus, une action de la radio cognitive peut également mettre à jour les modèles internes, comme l'ajout de nouveaux modèles aux modèles existants

- **Phase apprentissage (Learn)**

La phase d'apprentissage, dénommée "Learn", est tributaire de la perception, des observations, des décisions et des actions. Elle se manifeste lorsqu'un nouveau modèle est élaboré en réaction à une action, dans le but d'améliorer la compréhension des diverses fonctionnalités de la radio cognitive.

I.2.8 Les composants de la radio cognitive

Les divers éléments d'un émetteur/récepteur radio cognitive qui intègrent ces fonctionnalités sont détaillées dans la figure I.6.

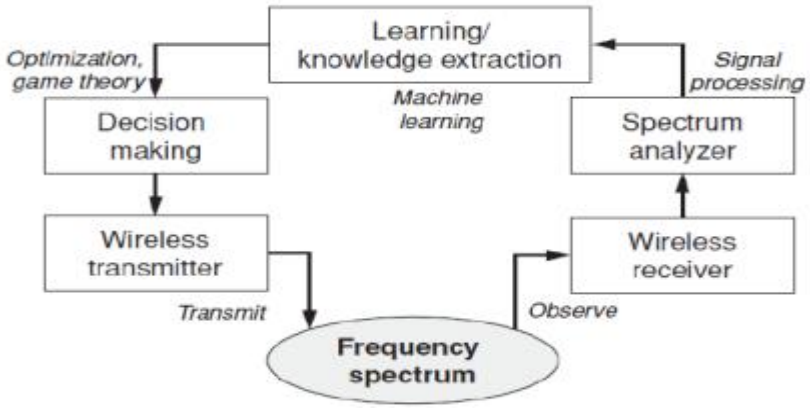

Figure I- 6: Composants de la radio cognitive [14]

- **L'émetteur/récepteur**

Dans ce contexte, un récepteur RC est également employé pour surveiller l'activité sur le spectre de fréquences, ce qu'on appelle la détection de spectre. Les caractéristiques de ce composant peuvent être ajustées en temps réel selon les directives des protocoles de la couche supérieure.

- **Analyse de spectre (Spectrum analyser)**

L'analyse spectrale englobe diverses méthodes de traitement du signal afin d'obtenir des informations sur l'utilisation du spectre. Elle vise à détecter la signature d'un utilisateur primaire, à repérer les "espaces blancs" du spectre pour les utilisateurs secondaires, et à garantir que la transmission de données d'un utilisateur primaire ne soit pas perturbée si un utilisateur secondaire choisit d'accéder au spectre.

- **Apprentissage et extraction de connaissances (Learning/Knowledge Extraction)**

Ce composant exploite des algorithmes d'apprentissage et aux données issues de l'analyse spectrale pour saisir le contexte de l'environnement RadioFréquence(RF), y compris le comportement des utilisateurs autorisés, tels que les utilisateurs primaires.

- **Décision (Decision-making)**

Le choix concernant l'accès au spectre doit être pris une fois que l'information sur l'utilisation du spectre est accessible. La sélection optimale dépend du degré de coopération ou de compétition entre les utilisateurs secondaires (SU) et varie en fonction du contexte de

l'environnement radiofréquence. Les méthodes d'optimisation stochastique (telles que le processus décisionnel de Markov) sont employées pour modéliser et résoudre le problème d'accès au spectre dans un environnement RC.

I.2.9 Fonctions de la radio cognitive

L'élaboration et la réalisation des communications se heurtent à un ensemble de défis techniques qui reposent principalement sur la nécessité d'apporter des ajustements aux modèles et équipements de communication existants À un niveau plus fondamental, il est essentiel d'adapter les terminaux et d'adopter de nouveaux algorithmes plus performants, tout en contrôlant la consommation d'énergie. Le terminal radio cognitif doit être en mesure d'intégrer des fonctionnalités de reconfiguration automatique. Les principales fonctions de la radio cognitive incluent :

I.2.9.1 Détection du spectre (spectrum sensing)

C'est une fonction essentielle qui implique la détection des zones inoccupées du spectre en identifiant les signaux des utilisateurs sous licence. Ses principales actions sont les suivantes :

- Détecter les parties du spectre non utilisées ;
- Partager le spectre de manière non perturbée avec d'autres utilisateurs. L'objectif principal de cette fonction est de repérer les interférences afin de déterminer l'état du spectre (libre ou occupé) pour les utilisateurs secondaires (SU).

I.2.9.2 Gestion du spectre (Spectrum management)

Acquérir la bande de fréquences disponible pour répondre aux exigences de communication des utilisateurs, organisées selon les catégories suivantes :

- **Analyse du spectre**

Évaluer les conclusions de l'analyse spectrale afin d'estimer la qualité du spectre, notamment en ce qui concerne la disponibilité des "espaces blancs" ainsi que leur durée moyenne.

- **Décision sur le spectre**

La détermination de l'accès au spectre repose sur les résultats issus de l'analyse spectrale. Les sections du spectre identifiées sont partagées avec d'autres utilisateurs ou coexistent avec eux sur la même bande, grâce à des techniques telles que l'optimisation stochastique. Dans un environnement de système radio cognitif, qu'il soit coopératif ou non coopératif, deux catégories d'utilisateurs (PU et SU) peuvent influencer l'accès au spectre.

Dans un contexte non coopératif, chaque utilisateur poursuit ses propres objectifs, tandis que dans un cadre coopératif, tous les utilisateurs travaillent ensemble pour atteindre un objectif commun. Par exemple, plusieurs utilisateurs secondaires peuvent rivaliser pour accéder au spectre (par exemple, O1, O2, O3, O4 dans la figure I.8), visant à maximiser leur débit individuel.

Durant cette procédure, chacun s'engage à maintenir l'interférence causée à l'utilisateur principal en dessous du seuil de brouillage correspondant. Dans cette optique, la théorie des jeux se révèle être un instrument pertinent pour parvenir à un équilibre dans un contexte similaire.

Dans un cadre collaboratif, les radios cognitives collaborent entre elles afin de décider de l'accès au spectre et d'optimiser une fonction objectif commune en prenant en compte les contraintes pertinentes. Dans ce schéma, un contrôleur central peut assurer la coordination de la gestion du spectre [15]**.**

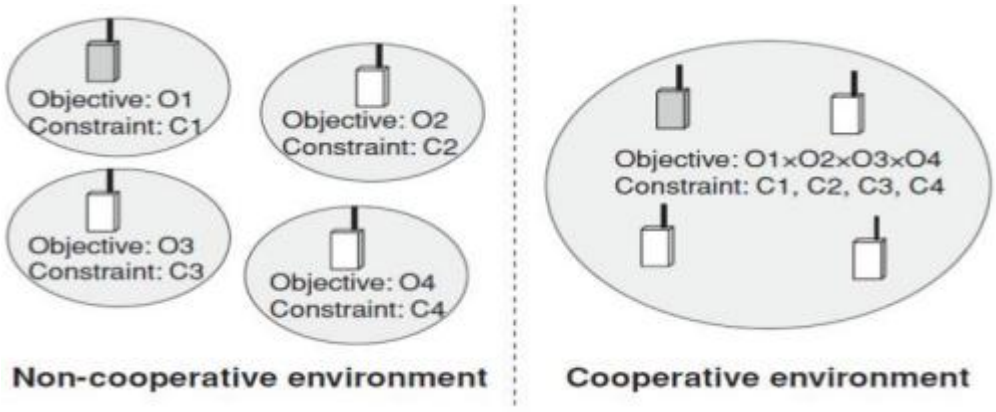

Figure I- 7: Accès au spectre coopératif et non-coopératif

I.2.9.3 Mobilité du spectre (spectrum mobility)

La capacité de mobilité des dispositifs de radio cognitive facilite le changement de bande de fréquences, permettant ainsi une utilisation dynamique du spectre.

- **Recherche des meilleures bandes de fréquences :** La radio cognitive doit surveiller en permanence les plages de fréquences disponibles, de sorte que si nécessaire (par exemple, lors de la détection d'un utilisateur autorisé), elle puisse basculer instantanément vers d'autres plages de fréquences disponibles. Pendant la transmission par un utilisateur secondaire, il est impératif de respecter l'état de la bande de fréquences.

- **Auto-coexistance et synchronisation** : Lorsqu'un utilisateur secondaire effectue un transfert de spectre, deux considérations essentielles doivent être prises en compte. Tout d'abord, il est nécessaire de vérifier que le canal cible n'est pas déjà utilisé par un autre utilisateur secondaire (condition d'auto-coexistence). Ensuite, le récepteur de la liaison secondaire doit être informé de l'inactivité du spectre (demande de synchronisation) [16].

I.2.10 Domaine d'application de la radio cognitive

- **Les réseaux sans fil de prochaine génération**

La radio cognitive est envisagée comme une technologie clé pour les futures générations de réseaux sans fil hétérogènes. Elle permettra de fournir des informations intelligentes à la fois aux utilisateurs et aux fournisseurs d'équipements. Du point de vue des utilisateurs, un dispositif mobile équipé de multiples interfaces sans fil telles que le WiFi, le WiMAX et les réseaux cellulaires pourra surveiller l'état des réseaux d'accès sans fil, incluant la qualité de transmission, le débit et les délais, afin de prendre des décisions éclairées sur la sélection du réseau d'accès pour leurs communications. Du côté des fournisseurs, la radio cognitive offre la possibilité d'optimiser les ressources radio de différents réseaux afin de répondre aux exigences en matière de qualité de service (QoS) de l'ensemble des utilisateurs mobiles.

- **La coexistence entre différentes technologies sans fil**

Elle est facilitée par l'utilisation de la radio cognitive, permettant ainsi l'intégration harmonieuse de nouvelles technologies sans fil en développement. Son rôle essentiel est de réutiliser les fréquences radio allouées à d'autres services sans fil, comme par exemple le service de télévision, afin d'optimiser l'utilisation du spectre.

- **Les services de cyber santé (eHealth services)**

Se caractérisent généralement par l'utilisation de dispositifs médicaux sans fil, lesquels sont sensibles aux interférences électromagnétiques (EMI). Par ailleurs, divers dispositifs biomédicaux tels que les équipements chirurgicaux, de diagnostic et de suivi, recourent à la transmission par radiofréquence (RF). Dans ce contexte, la radio cognitive peut être mise en œuvre pour la gestion du spectre utilisé par ces dispositifs, tout en veillant à éviter toute forme d'interférence nuisible [42]**.**

- **Secours aux sinistrés et les réseaux d'urgence**

Les phénomènes naturels tels que les ouragans, les tremblements de terre ou les incendies de forêt ont souvent pour conséquence la rupture des infrastructures de

communication existantes. Cela entraîne l'isolement des réseaux qui étaient précédemment en place, les rendant partiellement ou totalement inaccessibles. Dans ces circonstances critiques, il devient impératif de disposer d'un moyen de communication efficace pour assister les équipes de secours dans leurs efforts d'organisation de l'aide et de localisation des survivants. Dans ce contexte, un Réseau Radio Cellulaire (RRC) pourrait être utilisé comme solution adaptée à de telles situations d'urgence [43].

- **Réseaux militaires**

Dans les réseaux militaires, la radio cognitive offre la capacité d'ajuster dynamiquement les paramètres de communication sans fil en fonction du temps, de l'emplacement et des missions des soldats. Par exemple, en cas de brouillage ou de bruit sur certaines fréquences, les dispositifs radio cognitifs (émetteurs/récepteurs) peuvent entreprendre des recherches afin de trouver des bandes de fréquences alternatives pour la communication.

I.3 Conclusion

Ce chapitre a présenté la radio cognitive, en détaillant son historique, sa définition et son lien avec la radio logicielle. Nous avons exploré son fonctionnement, en mettant l'accent sur les utilisateurs primaires et secondaires, ainsi que les fonctions de détection et de gestion du spectre. La radio cognitive se révèle essentielle pour optimiser l'utilisation des ressources spectrales, répondant ainsi aux défis croissants de la bande passante dans les communications modernes.

Chapitre II : Sécurité des réseaux de radio cognitive

II.1 Introduction

Le concept du réseau radio cognitif vise à résoudre le problème de la rareté des fréquences en permettant aux utilisateurs secondaires (SU) d'accéder à la bande de fréquences sans perturber les utilisateurs principaux (PU). Cependant, cette approche présente des risques, car elle ouvre la possibilité à des utilisateurs malveillants de manipuler le réseau cognitif et de lancer diverses attaques, telles que l'usurpation d'identité, la falsification de données ou les attaques par déni de service. Ces actions pourraient causer des dommages considérables au fonctionnement du réseau radio cognitif, en plus des menaces de sécurité spécifiques associées à ce type de réseau.

L'objectif de la sécurité est de minimiser, voire d'éliminer, les menaces qui pèsent sur le système d'information afin de prévenir toute perturbation dans le fonctionnement et les opérations commerciales des organisations.

Dans ce chapitre, nous examinons les principaux objectifs de sécurité dans le contexte des réseaux de radio cognitive. Nous explorons en détail les différents types d'attaques auxquelles ces réseaux sont confrontés, en mettant en évidence les risques potentiels tels que l'usurpation d'identité, le brouillage et l'interception de données. Nous analysons également les attaques spécifiques à chaque couche du modèle OSI et proposons des solutions pour renforcer la sécurité à chaque niveau. En outre, nous définissons le contrôle d'accès et examinons les systèmes, les modèles et les mécanismes de contrôle d'accès utilisés dans les réseaux de radio cognitive. Enfin, nous discutons des différents types de contrôle d'accès.

II.2 Objectifs principaux de la sécurité

- **Intégrité des données**

Il est essentiel de constamment assurer l'intégrité des données en transit, en veillant à ce qu'elles ne subissent aucune altération, qu'elle soit intentionnelle ou non, tout au long de la communication.

- **Confidentialité**

La préservation de la confidentialité implique que seules les personnes autorisées puissent accéder aux données. Tout accès non autorisé doit être empêché grâce au cryptage

des données, et seuls les participants disposant de la clé de déchiffrement doivent être en mesure de les comprendre.

- **Disponibilité**

Elle nécessite de garantir que le système fonctionne correctement et que les services ainsi que les ressources sont accessibles à tout moment.

- **Authentification**

L'authentification restreint l'accès aux individus autorisés en vérifiant l'identité d'un utilisateur avant tout échange de données.

- **Non-répudiation**

La non-répudiation garantit qu'aucun des intervenants ne peut contester une transaction. Elle confirme également l'authenticité de l'envoi et de la réception des données, établissant ainsi qu'elles ont été effectivement reçues.

II.3 Types des attaques dans les réseaux de radio cognitive

Les attaques visent les deux types de radios suivants :

a) La radio politique (Policy Radio) : permet de réguler le comportement de la radio en fonction d'une stratégie définie, transformant ainsi les données de l'environnement en statistiques pour évaluer son état.

b) La radio d'apprentissage (Learning Radio) : il intègre un moteur d'apprentissage qui élabore une stratégie basée sur ses connaissances. Si les données évoluent, la stratégie s'adapte en conséquence. Elle assure un réglage optimal des paramètres dans un environnement donné, mais elle est réputée pour être résistante aux attaques en raison de sa complexité.

Il est important de mentionner les différents types de radio-communication afin d'identifier les diverses attaques potentielles. Par exemple, dans le cas de la radio politique, en comprenant le processus de calcul des statistiques, un attaquant pourrait manipuler et contraindre les résultats selon ses désirs [17].

Les attaques dans les Réseaux de Radio Cognitive (RRC) sont catégorisées selon les strates OSI qu'ils visent : la couche physique, la couche de liaison, la couche réseau et la couche transport. Ces attaques ciblent spécifiquement les réseaux Ad hoc, et puisque les RRC

sont perçus comme une variante de ce type de réseau, il en résulte que ces assauts peuvent également être dirigés contre un RRC [18].

II.4 Attaques de chaque couche OSI

II.4.1 Attaque de la couche physique

Les principales faiblesses résident au niveau de la couche physique, étant donné que la détection du spectre représente une phase critique des RRC. Les attaques qui altèrent la capacité de détection du spectre des utilisateurs secondaires peuvent être utilisées pour une utilisation excessive du système ou pour perturber les communications des utilisateurs légitimes. Les types d'attaques les plus communs et ceux régulièrement déployés à l'encontre de la détection du spectre des RRC incluent :

II.4.1.1 Émulation de l'utilisateur primaire (PUE)

Ce type d'attaque est habituellement mené par un ensemble d'utilisateurs secondaires mal intentionnés, qui émettent des signaux particuliers dans le but d'occuper toutes les plages de spectre non utilisées. La figure **II.8** illustre comment un utilisateur malveillant envoie des signaux présentant les mêmes caractéristiques qu'un utilisateur principal, dans le but de se faire passer pour le propriétaire de ces fréquences.

Dans ce scénario, les attaquants peuvent perturber l'exploitation opportuniste du spectre par les utilisateurs secondaires (SU) et monopoliser les ressources disponibles à leur profit, ce qui leur confère un avantage sur les autres SU [19]**.**

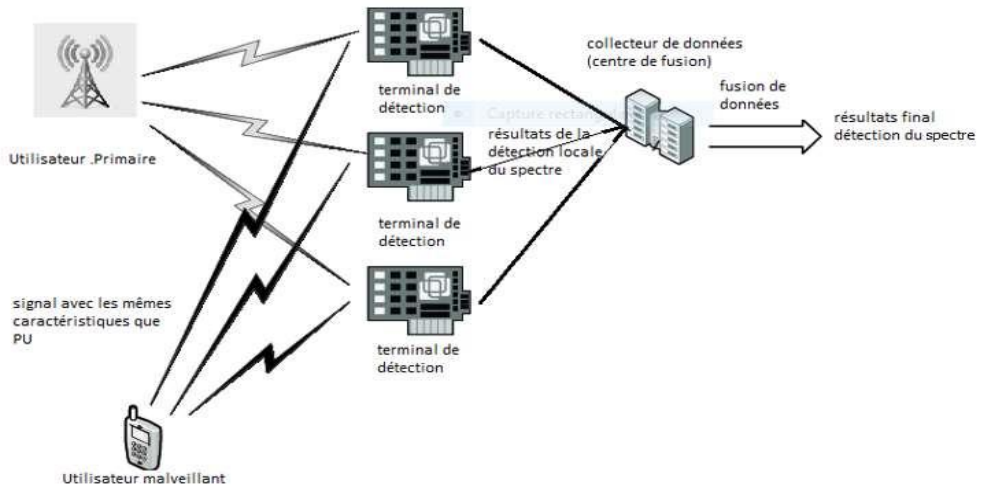

Figure II- 1: Les attaques PUE [19]

Types d'attaque PUE:

- **L'attaque PUE égoïste :** Lorsque l'attaquant repère une portion du spectre inutilisée, il transmet des signaux qui imitent les caractéristiques du signal d'un utilisateur principal (PU), bloquant ainsi l'accès des utilisateurs secondaires (SU). Par conséquent, l'assaillant peut exploiter les canaux non utilisés par les PUs.
- **L'attaque PUE malveillant :** L'attaque malveillante d'interférence utilisateur vise simplement à gêner l'accès des utilisateurs secondaires autorisés aux plages de fréquences inutilisées dans un spectre.

Il se trouve d'autres formes d'attaques PUE plus sophistiquées. Certains attaquants peuvent choisir d'agir uniquement lorsque l'utilisateur principal est inactif, leur permettant ainsi d'économiser de l'énergie [20].

✔ **Solution contre l'attaque PUE:**

Pour se prémunir contre l'attaque PUE, il est essentiel de déterminer en premier lieu si le canal provient d'un utilisateur primaire (PU) légitime ou d'un utilisateur secondaire malveillant (MSU) imitant un PU.

La détection d'un émetteur PU est cruciale pour distinguer un PU légitime d'un PU malveillant. Bien que l'authentification cryptographique puisse permettre d'identifier l'origine du PU, les réglementations de la FCC interdisent la modification du système PU. Par conséquent, les chercheurs ont élaboré une solution efficace pour vérifier l'emplacement de la source du PU, en mettant en place une méthode pour faire correspondre l'emplacement de la source avec celui du PU [21].

Deux méthodes sont utilisées pour déterminer l'emplacement de la source du PU :

- **Le Test du Rapport de Distance (DRT):** qui implique le calcul de la force du signal reçu.
- **Le Test de Différence de Distance (DDT):** qui consiste à mesurer la variation de phase du signal.

Les deux méthodes emploient un processus de validation de l'origine du PU. Le but de cette démarche est de distinguer les signaux primaires légitimes des signaux malveillants.

Les évaluations DRT et DDT sont réalisées par des dispositifs de localisation fiables, désignés comme des vérificateurs de localisation LV, qui se répartissent en deux catégories :

a - Un maître LV :détient une base de données contenant les coordonnées des tours de télévision, grâce à un système GPS[1].

b - Un esclave LV: est chargé de déterminer la distance entre lui-même et le transmetteur en utilisant la force du signal, puis de comparer cette distance avec celle de la tour TV. Pour assurer l'intégrité et la confidentialité des données, celles-ci doivent être cryptées et authentifiées afin d'éviter toute altération ou interception indésirable [22].

Les deux classes sont interconnectées pour superviser leur échange d'informations. Si la vérification échoue, une attaque de l'émetteur est envisagée [23]. Cependant, un inconvénient de cette approche est que sa mise en œuvre peut être coûteuse, d'autant plus qu'elle peut être limitée à un contexte ad hoc en raison de la qualité médiocre du signal transmis [24]**.**

Une autre solution a été suggérée pour contrer l'attaque PUE, appelée Défense Basée sur la Localisation (LocDef), qui implique trois étapes principales :

- Vérification des attributs du signal
- Évaluation du niveau d'énergie du signal capté.
- Détermination de l'emplacement de la source du signal.

Cette méthode se fonde sur la localisation basée sur les signaux RSS-Based,[2] qui tire parti de la corrélation entre l'intensité du signal et la position de l'utilisateur. Lorsque l'intensité du signal diminue, cela indique une distance accrue entre l'émetteur et le récepteur [25].

Lorsqu'un nœud rassemble des données sur la puissance du signal à partir de nœuds répartis dans le réseau, il est en mesure de construire un modèle de ce signal. Ce modèle lui permet ensuite de déterminer la localisation de l'émetteur. Parallèlement, pour recueillir les mesures du RSS (Received Signal Strength), un réseau de capteurs sans fil (WSN - Wireless Sensor Network) est mis en place. Ce réseau de capteurs constitue le fondement de la collecte des mesures RSS.

Un autre but pour les WSN est de participer à la détection du spectre et de fournir des informations sur les potentialités du réseau [26].

---

[1] **GPS :** Il s'agit d'un système de géolocalisation qui se base sur l'utilisation des signaux radio émis par des satellites dédiés à cet effet.

[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).

II.4.1.2 Attaque de la fonction objectif (Objective Function Attack)

Le cœur cognitif de la radio adaptative est chargé de régler les paramètres de transmission afin de satisfaire des besoins spécifiques, tels que la minimisation de la consommation d'énergie, l'optimisation du débit de données et le renforcement de la sécurité.il détermine ces paramètres (tels que la fréquence centrale, la largeur de bande, la puissance, le niveau de cryptage, le protocole d'accès au canal, le type de modulation et la taille des trames) en résolvant une ou plusieurs fonctions objectives. Par exemple, il cherche à déterminer les paramètres de transmission qui maximisent le débit tout en réduisant au minimum la consommation d'énergie.

La manipulation de la fonction objective (OFA), également connue sous le nom d'attaque de manipulation de croyance", cible les algorithmes d'apprentissage qui se basent sur des fonctions objectives. Voici la formule de cette fonction :

$$F(\ ,\ ,\ ) = \alpha P + \beta R + \gamma S$$

La fonction objectif F, utilisée par le moteur cognitif, est illustrée par un exemple pratique détaillé. Dans cet exemple, un attaquant lance une interférence sur la radio, réduisant ainsi le taux de transmission R et impactant également la fonction objectif F. Les poids α, β et γ représentent respectivement les poids de la force P, du taux de transmission R et de la sécurité S.

Supposons qu'un attaquant cherche à contraindre le moteur cognitif à utiliser un niveau de sécurité spécifique, noté S1, où S1 < S2.

Chaque fois que le moteur cognitif tente d'utiliser S2, l'attaquant peut perturber le canal en réduisant le taux de transmission de R2 à R1, où R1 < R2. Ainsi,

$$\alpha P + \beta R2 + \gamma S1 > \alpha P + \beta R1 + \gamma S2$$

on résoudre R1 comme ça:

$$R1 < \ 2\ - \beta/\gamma(s2 - s1)$$

Ainsi, à chaque tentative d'adopter un niveau de sécurité plus élevé, la fonction objective du système est affectée [27].

- ✔ **Solution contre l'attaque de la fonction objectif**

Pour contrer l'attaque de la fonction objective, plusieurs solutions ont été suggérées. Parmi celles-ci, l'une consiste à établir des seuils pour chaque paramètre radio. Si ces

paramètres ne respectent pas les seuils prédéfinis, la communication est interrompue. Une autre recommandation, mentionnée dans [28], implique le recours à un système de détection d'intrusions (IDS).

II.4.1.3 L'attaque de brouillage (Jamming)

La nature "ouverte" de la philosophie du paradigme de la radio cognitive rend le réseau RC susceptible aux attaques de brouillage initiées par des utilisateurs malveillants intelligents.

Un attaquant peut scanner les canaux, repérer les communications légitimes des utilisateurs secondaires, puis émettre un signal de brouillage sur le même canal ou une partie de celui-ci, entraînant des interférences perturbatrices pour les SU. Cette perturbation des SU peut entraîner une situation de déni de service (DoS), rendant ainsi le service indisponible et bloquant complètement la transmission des SU légitimes [29].

Ces types d'attaques ciblent à la fois les couches physiques ainsi que les couches de liaison (MAC) du système.

Afin de démontrer l'impact du brouillage, une expérience a été menée par Suman Bhunia et Shamik Sengupta [29], impliquant deux ordinateurs configurés pour communiquer via un canal de 36 MHz (centré sur 5,180 MHz) du WLAN (IEEE 802.11-a) [29].

Type de brouilleurs (Jammers)

a) **Brouilleur constant :** Cela autorise l'envoi continu de paquets de données sans prendre en compte les protocoles de la couche MAC et sans nécessiter d'attendre que le canal soit libre.

b) **Brouilleur trompeur :** Il envoie de manière continue des paquets de données réguliers au lieu de transmettre des bits de manière aléatoire. Cela induit en erreur les autres nœuds en leur faisant croire qu'une transmission légitime est en cours, ce qui les pousse ainsi à rester en mode réception.

c) **Brouilleur aléatoire** : Il prend des intervalles entre les signaux de brouillage, et peut fonctionner de manière constante ou trompeuse, imitant ainsi un brouilleur constant ou trompeur.

d) **Brouilleur réactif** : Il ne se met à brouiller que lorsqu'il détecte une activité sur un canal spécifique. Par conséquent, un brouilleur réactif cherche à compromettre la

réception d'un message, pouvant ainsi perturber les paquets de taille variée, qu'ils soient petits ou grands.

✔ **Solution contre l'attaque de brouillage :**

Les attaques de déni de service (DoS) peuvent cibler à la fois les couches physiques et de liaison. Possédant sa propre méthode de détection :

1. **Détection couche physique** :

Dans cette détection, les appareils légitimes doivent être en mesure de différencier le bruit normal du bruit anormal sur un canal. Pour ce faire, ils collectent une quantité suffisante de données sur le niveau de bruit dans le réseau, puis établissent un modèle statistique pour la comparaison lorsqu'une attaque par déni de service se produit [30]**.**

2. **Détection couche liaison :**

Chacune Dans la détection au niveau de la couche liaison, les appareils légitimes utilisent le protocole largement adopté d'accès au support CSMA (Carrier Sensing Multiple Access). Un périphérique détermine la disponibilité d'un canal en utilisant ce protocole, retardant la transmission des données jusqu'à ce qu'un délai de propagation soit écoulé. Si un attaquant envoie des paquets de manière continue, le dispositif ne peut jamais exécuter le protocole CSMA et sera contraint de reculer. Ainsi, le dispositif détecte qu'il est victime d'une attaque par déni de service (DoS).

Pour se protéger contre le brouillage (DoS), deux stratégies sont mises en œuvre :

a - Déplacement des canaux ou changement de fréquence (Channel Surfing) : Le recours à un canal alternatif dès la détection d'une attaque par déni de service.

b - Retraite spatiale (Spatial Retreat) : Les utilisateurs autorisés modifient leur position pour éviter l'interférence causée par l'attaquant. Il est important de noter deux aspects de cette approche : les utilisateurs doivent se déplacer hors de la zone où se trouve l'attaquant, tout en maintenant une proximité suffisante pour maintenir la communication [30].

II.4.2 Les attaques de la couche liaison (Link Layer Attack)

La couche de liaison assure la gestion du trafic et la correction d'erreurs sur le support physique. Elle permet également de prendre en charge plusieurs utilisateurs sur un réseau partagé. Chaque ordinateur dispose de sa propre adresse MAC unique. La plupart des attaques au sein de cette couche sont dirigées contre les adresses MAC [31].

II.4.2.1 La falsification des données de détection de spectre (FDSD)

Egalement appelée attaque byzantine, se produit lorsque des résultats de détection de spectre falsifiés sont transmis par un attaquant à ses voisins ou au centre de diffusion. Cela induit le récepteur à prendre une décision erronée en matière de détection de spectre [32].

Cette attaque vise à compromettre à la fois les RRC centralisés et distribués :

- **RRC centralisé : U**n centre d'intégration est responsable de recueillir toutes les données de détection et de gérer l'attribution des bandes de fréquences. L'attaque SSDF manipule le centre d'intégration afin d'empêcher certains utilisateurs légitimes d'accéder à des bandes de fréquences disponibles, ou de les diriger vers des stations de base déjà occupées.
- **RRC distribué : L**es choix relatifs aux bandes de fréquences sont faits en coopération entre les réseaux radio cognitifs. Toutefois, une attaque SSDF est particulièrement nocive dans ce contexte, car les fausses informations peuvent se propager rapidement sans qu'il y ait moyen de les contrôler.

La figure suivante montre un schéma d'un attaquant SSDF avec un faux spectre local, ainsi l'attaquant SSDF injecte un faux spectre local dans le système de détection. Ce faux spectre est conçu pour tromper le centre de fusion de données en lui faisant croire qu'il n'y a pas d'activité malveillante dans le spectre.

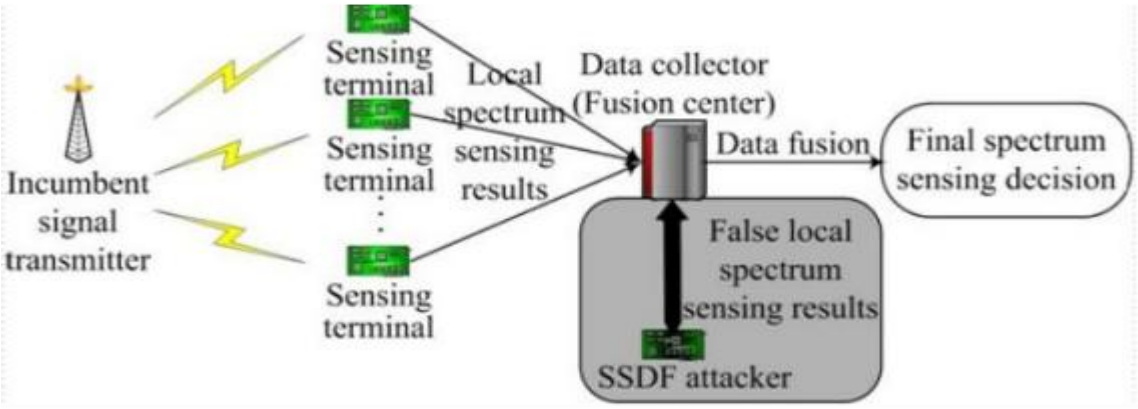

Figure II- 2: Mécanisme de l'attaque SSDF

Par conséquent, dans un RRC centralisé, l'impact des données malveillantes est moins atténué car le centre d'intégration compare les données reçues de la RC avec des techniques intelligentes afin de mieux distinguer les RC légitimes [33].

✔ **Solution contre l'attaque SSDF**

Diverses approches de fusion de données ont été avancées pour détecter l'attaque SSDF. Parmi celles-ci, le Test de Rapport Séquentiel Pondéré (WSPRT - Weighted Sequential Probability Ratio Test) se distingue comme une stratégie de défense contre les attaques byzantines. Dans une architecture ad hoc, les nœuds effectuant la détection de spectre recueillent les données ainsi que les rapports de détection locaux des nœuds voisins. Les deux principales étapes de cette méthode sont :

- Maintenance de la valeur : Initialement, chaque nœud a une valeur égale à zéro, qui sera incrémentée de 1 en cas de détection correcte du spectre [34].

- **Hypothèse d'essai de WSPRT :** Cette étape suppose que le test de probabilité séquentielle et la valeur du seuil de test WSRT sont similaires à la technique utilisée dans les réseaux de capteurs sans fil (WSN) [35]**.**

Une méthode de détection est proposée pour repérer les attaques byzantines en analysant les écarts entre leurs décisions locales et la décision globale au sein du centre de fusion sur une période temporelle donnée, suivie de l'exclusion des nœuds byzantins du processus de fusion des données. Cette approche s'est avérée résiliente contre les attaques byzantines, parvenant à les éliminer en un laps de temps très court [36].

Un algorithme de détection des utilisateurs malveillants a été présentée dans, où un algorithme évalue le niveau de suspicion des utilisateurs secondaires en se basant sur leurs rapports précédents [36].

Cet algorithme évalue les niveaux de confiance et de cohérence afin de neutraliser l'impact des utilisateurs malveillants sur les résultats de détection du principal utilisateur. Bien que ces systèmes de défense mentionnés soient robustes et sécurisés, ils peuvent toutefois entraîner une diminution des performances [37].

II.4.2.2 Négociation de canal égoïste (SCN)

Dans un réseau de radio cognitive multi-sauts, un hôte RC peut choisir de ne pas acheminer les données pour d'autres hôtes. Ceci lui permet d'économiser de l'énergie et d'optimiser son propre débit en utilisant une stratégie égoïste de gestion des canaux. Des résultats comparables pourraient être obtenus si l'hôte égoïste était en mesure d'altérer le comportement MAC approprié des dispositifs RC. Par exemple, en réduisant sa propre taille de fenêtre de back-off, l'hôte accroît ses chances de monopoliser le canal aux dépens des autres hôtes RC. Cette attaque peut aussi altérer le débit global de bout en bout de l'intégralité du réseau RC [38].

II.4.2.3 Contrôle de la saturation du canal (CCS)

Le canal de contrôle dans RRC est dédié à l'acheminement du trafic de contrôle entre les utilisateurs du réseau. Il est soumis à une capacité limitée pour le transport et la transmission des données.

Le canal de contrôle atteindra un état de saturation lorsqu'il ne pourra plus transporter de trafic de contrôle supplémentaire. Un attaquant pourrait déployer un grand volume de paquets dans le but de saturer ce canal. En variant les types de paquets envoyés, un nœud malveillant minimise les risques de détection. L'objectif des attaquants est de restreindre le nombre de nœuds légitimes pouvant accéder au spectre, leur permettant ainsi d'exploiter les bandes de fréquences de manière plus efficace [39].

- ✔ **Solution contre l'attaque CCS**

Pour contrer cette attaque, il est envisageable de segmenter un réseau de routeurs-relais en plusieurs groupes distincts. Chaque groupe utiliserait alors un canal de contrôle commun. Ainsi, si un attaquant cible un canal de contrôle spécifique, seuls les nœuds appartenant à ce groupe seraient impactés, réduisant ainsi la surface d'attaque sur le réseau [40]**.**

✔ **Solution contre CCSD et SCN**

On peut atténuer les problèmes liés aux CCSD et SCN (Négociation de Canal Égoïste) en adoptant une architecture de confiance, dans laquelle tout routeur-relais suspect serait surveillé et évalué par ses voisins. Ces derniers pourraient ensuite effectuer une analyse séquentielle des données d'observation et tirer une conclusion définitive quant à son comportement. Le test de rapport de probabilité séquentielle se révèle efficace dans ce contexte, ayant démontré sa capacité à détecter rapidement les anomalies [38]**.**

II.4.3 Les attaques de la couche réseau (Network Attack Layer)

Le développement du RRC a principalement porté sur les couches physique et liaison, ce qui a entraîné des difficultés de routage. Malgré ses trois architectures, le RRC reste vulnérable aux attaques classiques des réseaux sans fil. Dans la suite, nous aborderons deux des attaques les plus significatives contre le RRC : l'attaque de Sinkhole (puits) et l'attaque de Flood Hello (inondation Hello) [33] [18]**.**

II.4.3.1 Attaques de puits (Sinkhole Attacks)

Dans ce type d'attaque, l'attaquant se fait passer pour le chemin le plus optimal vers une destination précise, attirant ainsi les nœuds voisins et détournant leurs paquets de données. Cette manœuvre peut servir de point de départ à d'autres attaques, car elle ouvre la voie à la lecture, la modification et la suppression des données. Cette tactique est particulièrement efficace dans les réseaux dotés d'architectures centralisées ou maillées, où le trafic est dirigé via des stations de base [18][33]**.**

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

La détection de l'attaque de puits peut poser des défis, car elle exploite la conception similaire des protocoles de routage et de l'architecture réseau. Cependant, certains protocoles, tels que le protocole Géographique, ont été conçus pour contrer cette menace. Ce protocole repose sur le principe de construire une topologie en fonction des besoins, en se basant uniquement sur des communications et des informations locales, sans nécessiter d'initialisation depuis une station de base [18]**.**

II.4.3.2 L'attaque Hello Flood

L'attaque Hello Flood est une tactique plus insidieuse que celle mentionnée précédemment. Dans cette stratégie, l'attaquant diffuse des messages à tous les nœuds du réseau en garantissant une qualité de service élevée, afin de les convaincre qu'il s'agit de leurs voisins. Par exemple, l'envoi par l'attaquant d'un paquet publicitaire vantant la qualité exceptionnelle d'un lien vers une destination spécifique incitera même les nœuds distants à emprunter cette route et à croire que l'attaquant est leur voisin, En revanche, leurs paquets seront perdus. Si un nœud parvient à identifier l'attaque, il se retrouvera sans voisin vers lequel acheminer ses paquets, puisque tous les nœuds sont induits à emprunter le même chemin malveillant [18].

✔ **Solution contre l'attaque Hello Flood**

Afin de contrer cette attaque, une solution consiste à recourir à une clé symétrique partagée avec une station de base de confiance. Cette dernière agira comme une tierce partie de confiance, à l'instar de Kerberos[3], facilitant ainsi l'établissement des clés de session entre les différents nœuds du réseau. Cette clé symétrique peut être employée par les nœuds pour vérifier l'identité de chacun, ainsi que pour authentifier et chiffrer les échanges entre eux. Il est crucial de limiter le nombre de ces clés partagées afin d'empêcher les nœuds intrus de créer une clé avec chaque nœud du réseau.

De plus, tout nœud prétendant être le voisin de plusieurs autres dans le réseau devrait déclencher une alarme. Les algorithmes de clés symétriques sont particulièrement recommandés en raison de leur rapidité.

II.4.4 Attaques de couche transport (Transport Attack Layer)

La couche de transport gère le contrôle du flux, la gestion de la congestion et la correction des erreurs de bout en bout. Dans le contexte des réseaux ad hoc sans fil, cette couche est confrontée à plusieurs vulnérabilités.

II.4.4.1 L'attaque Lion

L'attaque de Lion exploite des techniques d'attaque PUE pour diminuer de manière significative le débit. De plus, si l'attaquant dispose ou peut deviner certains paramètres de

[3] **Kerberos :** est un protocole d'authentification conçu pour authentifier, autoriser et surveiller les utilisateurs cherchant à accéder à des ressources ou des services du réseau. Son objectif principal est de résoudre les défis liés à la sécurité, à l'administration et à la productivité associés à l'authentification des services réseau.

connexion, il peut même mener une attaque par déni de service (DoS) en émulant une transmission primaire à des moments précis, facilement prévisibles. Par conséquent, l'attaque de Lion se révèle plus efficace pour réduire le débit TCP que de simples attaques PUE ou du brouillage [41].

L'attaque de Lion est classée comme une attaque multicouche, ciblant les couches physiques et de liaison, avec un impact particulier sur la couche de transport. Elle exploite le protocole PUE (Physical Unclonable Function) pour forcer un RRC à effectuer des changements de fréquence, entraînant ainsi une dégradation des performances du protocole TCP (Transmission Control Protocol).

✔ **Solution contre l'attaque Lion**

Pour contrer l'attaque du Lion, Hernandez-Serrano et ses collègues proposent un mécanisme qui commence par sensibiliser le protocole TCP aux événements survenant dans la couche physique. Cela est réalisé grâce à un partage de données entre les couches physique, liaison et transport [41]**.**

Les dispositifs RRC seront en mesure de geler les paramètres de connexion TCP lors des transferts de fréquence, et de les ajuster aux nouvelles conditions du réseau une fois le transfert effectué. Afin de sécuriser les données de contrôle et d'empêcher les attaques d'écoute sur les actions présentes et futures du RRC, une gestion de clés de groupe GKM[4] peut être mise en œuvre. Cette approche permet aux membres du RRC de crypter, décrypter et s'authentifier mutuellement. De plus, l'utilisation d'un identifiant inter-couches spécifiquement conçu pour les RRC peut servir de technique pour identifier la source de l'attaque, le cas échéant [36]**.**

II.5 Contrôle d'accès

II.5.1 Définition

Un système visant à protéger les données et les ressources doit prévenir leur divulgation et leur altération non autorisée, tout en assurant leur accessibilité aux utilisateurs légitimes. Le

[4] **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.

contrôle d'accès permet de réguler qui peut accéder à quoi, de quelle manière et selon quelles règles, garantissant ainsi la sécurité et l'intégrité des ressources.

II.5.2 Système de contrôle d'accès

Le contrôle d'accès se divise principalement en deux catégories : physique et logique.

- **Contrôle d'accès physique** : Il concerne la régulation de l'accès aux locaux et aux ressources matérielles. Il repose sur trois éléments clés : le dispositif de contrôle d'accès (ex. badge, serrure électronique), la surveillance (caméras, gardiens) et les évaluations (audits de sécurité). Ce type de contrôle est essentiel pour protéger les biens physiques sensibles ou privés.
- **Contrôle d'accès logique** : Il se concentre sur la régulation de l'accès aux logiciels et aux données informatiques. Ce contrôle est souvent centralisé, avec des administrateurs ayant des droits étendus pour gérer les ressources. Les systèmes actuels stockent généralement les données sur des serveurs centralisés.

II.5.3 Politique de contrôle d'accès

Un ensemble de directives ou de mesures prescrites pour un système ou une entité organisationnelle, visant à influencer et orienter les décisions et actions de ses composants. Typiquement définies par une organisation ou une application, ces politiques sont souvent liées à la gestion des autorisations d'accès entre différents utilisateurs en fonction de règles logiques déterminées par l'usage. Voici quelques exemples courants de politiques de contrôle d'accès : le contrôle d'accès discrétionnaire (DAC) et le contrôle d'accès obligatoire (MAC) [44].

✓ **Contrôle d'accès discrétionnaire (DAC)**

Les créateurs des ressources détiennent le contrôle total sur les autorisations associées à leurs créations. Les règles d'accès, déterminées par les politiques, régissent l'accès en fonction de l'identité du demandeur et des actions spécifiques qu'il est autorisé (ou non) à entreprendre [44].

✓ **Contrôle d'accès mandataire (MAC)**

Contrairement au DAC, le MAC met en œuvre des politiques centralisées pour toutes les ressources système, ce qui le rend idéal pour les organisations. Cependant, son application nécessite une planification préalable détaillée, avec des règles spécifiques pour chaque

ressource du système. Les politiques MAC garantisse un contrôle d'accès conforme aux réglementations obligatoires établies par une autorité centrale [44].

II.5.4 Modèles de Contrôle d'accès

Les modèles de contrôle d'accès offrent une structure pour mettre en œuvre les politiques de sécurité. Ils permettent de maintenir les propriétés de sécurité et de s'adapter aux évolutions organisationnelles. Parmi les modèles les plus courants figurent :

- **RBAC (Role-Based Access Control)** : Contrôle basé sur les rôles [45].
- **ABAC (Attribute-Based Access Control)** : Contrôle basé sur les attributs [46].
- **VBAC (View-Based Access Control)**,
- **TBAC (Task-Based Access Control) [47]**,
- **TMAC (Temporal Access Control) [49],**
- **ORBAC (Organization-Based Access Control) [50]**.

II.5.5 Mécanisme de contrôle d'accès

Les mécanismes de contrôle d'accès englobent les fonctions opérationnelles de niveau bas (tant au niveau logiciel que matériel) qui appliquent les règles établies par la politique et formalisées dans le modèle. Parmi les exemples de ces mécanismes bien établis, on trouve les listes de contrôle d'accès (ACL) [51] et les capacités.

II.5.6 Architecture

Toutes les solutions de contrôle d'accès visent à accomplir la même tâche fondamentale, assurer la protection des systèmes contre les intrusions non autorisées. Par conséquent, elles partagent toutes les mêmes éléments de base, qui sont essentiellement des fonctions logiques. La manière dont ces éléments sont distribués entre les parties prenantes et leur réplication déterminent l'architecture globale.

- **Le Point de Décision Politique (PDP)** [52] **:** est le lieu où les choix politiques sont formulés.
- **Le Point d'Application de la Politique (PEP)** [52] **:** est l'endroit où ces décisions sont mises en œuvre.

- **Point d'Information sur les Politiques (PIP)** [46] **:**il joue le rôle de source d'extraction des attributs ou des données nécessaires à l'évaluation des politiques, fournissant ainsi les informations essentielles au PDP pour la prise de décisions**.**
- **Le Point d'Administration de la Politique (PAP)** [53] : désigne l'entité du système responsable de la création d'une politique ou d'un ensemble de politiques.

Tout d'abord, le PAP établit la règle et la transmet au PDP. Prenons l'exemple d'une situation où Belinda se rend au travail un lundi matin. Lorsqu'elle utilise son badge pour accéder au parking, qui est le PEP, celui-ci récupère d'abord son identité à partir du badge. Ensuite, il interroge un serveur situé quelque part dans le bâtiment, agissant en tant que PDP. Le PDP consulte ensuite une base de données qui agit comme un PIP pour vérifier si Belinda est une employée. Une fois que le PIP confirme que Belinda est bien une employée, une réponse positive est renvoyée au PEP, lui permettant ainsi d'ouvrir la porte [54].

La figure II.11 ci-dessous représente un modèle simplifié d'un système de contrôle d'accès qui régit les interactions entre un sujet, un objet et un ensemble de politiques. Chaque composant joue un rôle crucial dans l'application des autorisations d'accès et la garantie de la sécurité du système, tel que le sujet est une entité qui initie une action ou demande l'accès à une ressource, L'objet représente une ressource ou un élément de données auquel le sujet cherche à accéder et les **politiques** jouent un rôle crucial en définissant les règles qui régissent l'accès aux objets et aux ressources du système.

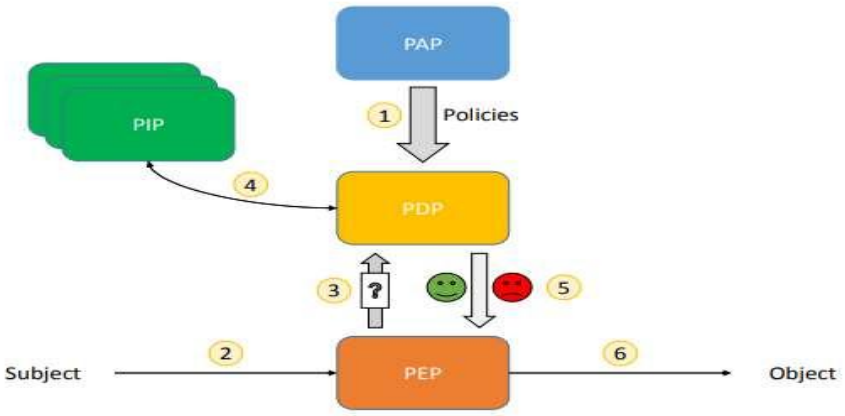

Figure II- 3: Instance de demande de contrôle d'accès [54].

II.5.7 Types des modèles de contrôle d'accès

Il y a quatre types principaux de modèles de contrôle d'accès :

II.5.7.1 Modèles de contrôle d'accès discrétionnaire (DAC)

Le modèle de contrôle d'accès discrétionnaire, ou DAC (Discretionary Access Control), est l'un des modèles de contrôle d'accès les plus couramment utilisés. Il restreint l'accès aux ressources en fonction de l'identité des utilisateurs et des permissions qui leur sont attribuées.

La politique de contrôle d'accès dans le modèle DAC est représentée sous la forme d'un triplet (objet, sujet, opération). Chaque entrée de ce triplet définit le sujet, l'objet et l'opération afin de spécifier les actions autorisées (par exemple, lire, écrire ou exécuter) que les sujets peuvent effectuer sur les objets du système. Ce modèle part du principe que les utilisateurs possèdent les ressources et peuvent accorder et transférer les droits d'accès à celles-ci.

II.5.7.2 Modèles de contrôle d'accès obligatoire (MAC)

Pour pallier les insuffisances du modèle de contrôle d'accès discrétionnaire, le modèle de contrôle d'accès obligatoire (MAC, Mandatory Access Control) a été mis au point. Ce modèle est plus strict que le modèle discrétionnaire. Dans le cadre du MAC, les utilisateurs n'ont pas la possibilité d'influencer l'attribution des droits d'accès. Le modèle multi niveaux associe aux sujets et aux objets du système des niveaux de sécurité qui ne peuvent être modifiés par les utilisateurs.

II.5.7.3 Modèle de contrôle d'accès basé sur les attributs (ABAC)

Le modèle de contrôle d'accès basé sur les attributs (ABAC) est devenu l'un des modèles et des standards les plus étudiés ces dernières années. Dans ce système, les règles d'accès sont définies à partir d'un ensemble d'attributs provenant essentiellement des utilisateurs, des objets et de l'environnement. Une demande d'accès est acceptée ou refusée après évaluation des attributs et des règles de contrôle d'accès correspondantes, permettant ainsi de fournir une décision d'accès.

- **Le sujet** : est l'entité qui sollicite l'accès pour réaliser des opérations sur des objets. Ces opérations peuvent inclure la lecture, la modification, la suppression, l'exécution, entre autres.

- **L'objet** : c'est une ressource du système nécessitant une gestion et un contrôle d'accès, comme des périphériques, des fichiers, des enregistrements, des programmes, etc. C'est la ressource que le sujet souhaite utiliser.
- **Conditions environnementales** : elles représentent le contexte opérationnel dans lequel les utilisateurs font leurs demandes d'accès. Cela peut englober l'heure du jour, le jour de la semaine, la localisation de l'utilisateur, ou le niveau de menace en cours.
- **Politique d'accès** : c'est l'ensemble des règles permettant de décider si une demande d'accès doit être accordée ou refusée, en fonction des valeurs des attributs des sujets, des objets et des conditions environnementales.

II.5.7.4 Le modèle de contrôle d'accès basé sur les rôles (RBAC)

Ce modèle a été conçu pour offrir une nouvelle manière d'organiser les droits, en mettant l'accent sur le concept de rôle. Un rôle reflète une fonction au sein d'une organisation. En se servant des rôles comme intermédiaires entre les utilisateurs et les permissions, ce modèle rend l'administration plus simple et efficace, car il réduit le nombre d'attributions à gérer [56].

Figure II.12 présente le fonctionnement du modèle RBAC : les utilisateurs accèdent à des permissions sur des ressources par le biais des rôles qui leur sont assignés, ces rôles étant liés à un groupe spécifique de permissions. Étant donné qu'il y a généralement beaucoup moins de rôles que d'utilisateurs ou de ressources, cela facilite considérablement la gestion des autorisations [57].

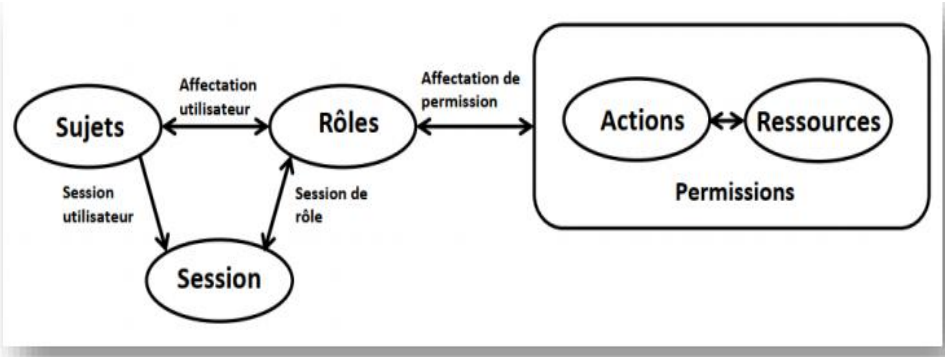

Figure II- 4: Modèle RBAC

II.6 Conclusion

En conclusion, ce chapitre a examiné en détail la sécurité des réseaux de radio cognitive (RC), en analysant les différentes menaces auxquelles ces réseaux sont exposés ainsi que les solutions pour y faire face. De plus, nous avons abordé les mécanismes de contrôle d'accès

visant à assurer la sécurité de ces réseaux RC. Ces contrôles d'accès, indispensables pour protéger les données et les ressources, présentent une variété de méthodes et de niveaux de robustesse. Ainsi, nous avons identifié plusieurs types de contrôles d'accès qui contribuent à renforcer la sécurité des réseaux de radio cognitive.

Chapitre III : Contribution et Résultats

III.1 Introduction

Dans ce chapitre, nous exposerons notre méthode pour garantir la sécurité de l'accès au spectre dans les réseaux de radio cognitive.

Dans ce travail, nous avons envisagé une technique de contrôle d'accès dédiée à l'utilisateur secondaire, lui permettant d'accéder uniquement aux offres de points d'accès (PU) honnêtes. Nous avons également intégré le chiffrement des données pour garantir la sécurité et la fiabilité des échanges entre les PU et les utilisateurs secondaires (SU). Cette approche vise à protéger les informations sensibles tout en assurant un accès équitable aux ressources disponibles.

III.2 Les acteurs du système

1. **Utilisateur primaire** : Il capte des bandes de fréquences assignées par l'opérateur.
2. **Utilisateur secondaire** : il achète les bandes de fréquence mises à disposition par les utilisateurs primaires.
3. **Un opérateur :** c'est le responsable qui est chargé de l'allocation des bandes de fréquences aux utilisateurs principaux et surveille l'utilisation des ressources en fréquences.

III.3 Scénario

Dans ce chapitre, nous examinerons le scénario où il y a un seul opérateur principal et quatre utilisateurs primaires ainsi que quatre utilisateurs secondaires.

a) Relation entre l'opérateur et PU

L'opérateur doit créer des bandes de fréquence qui sont ensuite mises à disposition des utilisateurs prioritaires. Ces derniers sélectionnent la bande de fréquence en fonction de critères tels que le prix, la bande de départ, la bande de fin, le trafic et la date d'expiration. Ensuite, le paiement est effectué à l'opérateur.

b) Relation entre PU et SU

L'utilisateur prioritaire (PU) qui a acquis une bande de fréquence peut créer des sous-bandes de fréquence inutilisées et les mettre à disposition des utilisateurs secondaires (SU).

Ces derniers peuvent alors sélectionner une sous-bande en fonction de critères tels que le prix, la bande de départ, la bande de fin, le trafic et la date d'expiration, puis effectuer le paiement au PU.

III.4 Travail réalisé

Notre objectif est d'assurer la sécurité des interactions entre le SU et les PU en mettant en place une méthode de sécurisation. Cette méthode utilise deux types de contrôles d'accès : un contrôle basé sur les rôles et un autre basé sur les attributs, afin de protéger les données et les ressources.

III.4.1 Les outils utilisés

Netbeans : NetBeans est un environnement de développement intégré (IDE) offrant un support optimisé pour la création d'applications web et serveur basées sur la plateforme Java EE. Cet IDE a été conçu en collaboration étroite avec les équipes de Java EE et de GlassFish, assurant une intégration fluide et une utilisation simplifiée des spécifications Java EE. L'utilisation NetBeans permet d'apprendre efficacement et de gagner rapidement en productivité dans le développement avec Java EE [55]**.** Aussi il améliore la collaboration et assure la qualité du code. Il supporte les langages Java, PHP, C, C++, HTML5, JavaScript et CSS.

MySql : MySqL est un système de gestion de bases de données développé par Oracle, largement utilisé à travers le monde. Basé sur l'algèbre relationnelle, il est principalement employé pour le stockage de données dans divers services Web. Parmi les CMS les plus populaires qui utilisent MySQL, on trouve WordPress et TYPO3.

III.4.2 Implémentation du système

Notre objectif est de permettre au SU de distinguer efficacement entre les PU honnêtes et les PU malveillants. Pour cette distinction, nous avons utilisé 2 types de contrôle d’accès :

1. **RBAC**: qui se compose de trois rôles:
    - PU : utilisateur principal qui reçoit des bandes de fréquences attribués par l’opérateur.
    - SU : qui achète des bandes de fréquence attribués au PU.

- Opérateur : qui gère l'attribution des bandes de fréquences et supervise l'utilisation des ressources.

	Accès	**Conditions**	**Règle**
Politique pour PU	Peut accéder aux bandes de fréquence attribuées par l'opérateur	Accès aux bandes spécifiques attribuées par l'opérateur	Si rôle == PU et bande de fréquence attribuée, alors accès = accordé
Politique pour SU	Peut accéder aux bandes de fréquence lorsque les PUs ne les utilisent pas	- Heure : Accès autorisé entre 18h00 et 6h00 (heures creuses). - Adresse IP : Doit être dans la plage d'adresses IP autorisées (par exemple, 192.168.1.0/24).	Si rôle == SU et heure entre 18h00 et 6h00 et adresse IP dans 192.168.1.0/24 et bande de fréquence non utilisée par PU, alors accès = accordé.
Politique pour l'Opérateur	Peut attribuer les bandes de fréquence aux PUs et surveiller l'utilisation des ressources.	Heure : Accès autorisé entre 8h00 et 20h00. Adresse IP : Doit être dans la plage d'adresses IP du réseau administratif (par exemple, 10.0.0.0/24).	Si rôle = opérateur et heure entre 8h00 et 20h00 et adresse IP dans 10.0.0.0/24, alors accès = accordé.

Tableau III- 1: Tableau explicatif du scénario du système.

III.5.2.1 **ABAC** : nous avons utilisé les attributs suivants :

- Heure : Plage horaire pendant laquelle l'accès est autorisé.
- Adresse IP : Adresses IP spécifiques ou plages d'adresses autorisées.
- Politiques d'Accès Hybrides

III.4.2.1 Sécurité

Algorithme de sécurité : Nous avons proposé le cryptage des données comme algorithme pour assurer la sécurité voici l'algorithme de cryptage des données.

```
Public Function EncryptData(ByVal plaintext As String) As String

    'convertissez la chaîne de texte brut en un tableau d'octets
    Dim plaintextBytes() As Byte =
    System.Text.Encoding.Unicode.GetBytes(plaintext)

    ' creer le flux
    Dim ms As New System.IO.MemoryStream
    ' créez l'encodeur pour écrire dans le flux
    Dim encStream As New CryptoStream(ms,
    TripleDes.CreateEncryptor(),
    System.Security.Cryptography.CryptoStreamMode.Write)
    'utilisez le flux cryptographique pour écrire le tableau d'octets dans le flux
    encStream.Write(plaintextBytes, 0, plaintextBytes.Length)
    encStream.FlushFinalBlock()
    'convertir le flux crypte en une chaîne imprimable
    Return Convert.ToBase64String(ms.ToArray)
End Function
```

```
Private Function TruncateHash(
ByVal key As String,
ByVal length As Integer) As Byte()

    Dim sha1 As New SHA1CryptoServiceProvider

    ' Hacher la cle
    Dim keyBytes() As Byte =
    System.Text.Encoding.Unicode.GetBytes(key)
    Dim hash() As Byte = sha1.ComputeHash(keyBytes)

    ' completer le hachage
    ReDim Preserve hash(length - 1)
    Return hash
End Function
```

```
Public Function DecryptData(ByVal encryptedtext As String) As String

    Dim encryptedBytes() As Byte = Convert.FromBase64String(encryptedtext)
    Dim ms As New System.IO.MemoryStream
    Dim decStream As New CryptoStream(ms,
    TripleDes.CreateDecryptor(),
    System.Security.Cryptography.CryptoStreamMode.Write)
    decStream.Write(encryptedBytes, 0, encryptedBytes.Length)
    decStream.FlushFinalBlock()


    Return System.Text.Encoding.Unicode.GetString(ms.ToArray)
End Function
```

L'algorithme précédent sert à chiffrer les données des utilisateurs primaires et secondaires, ainsi que celles de l'opérateur dans la base de données, afin d'assurer la sécurité et la confidentialité des informations sensibles. Cela protège les utilisateurs contre

d'éventuelles violations de données et garantit que seules les personnes autorisées peuvent accéder à des informations spécifiques.

a) Algorithme d'alerte d'adresse IP

Dans cet algorithme nous avons détecté l'anomalie à base de ces étapes :

1) Si une adresse IP non autorisé est détectée tentant d'accéder aux fréquences PU

-L'utilisateur demande la connexion au système.

-Le système passe le message à la configuration d'alerte (système demande la permission d'adresse IP).

-La configuration d'alerte fait l'algorithme de test :

Si l'adresse IP figure dans le tableau des adresses IP autorisées, alors la connexion est réussie.

Sinon si adresse IP refusé, alors la connexion est bloquée.

Les adresses IP refusées sont enregistrées dans un calculateur afin de renforcer la sécurité du système.

La figure **III.1** représente une vue simplifiée d'un système qui gère des demandes d'accès et prend des décisions en fonction de l'adresse IP.

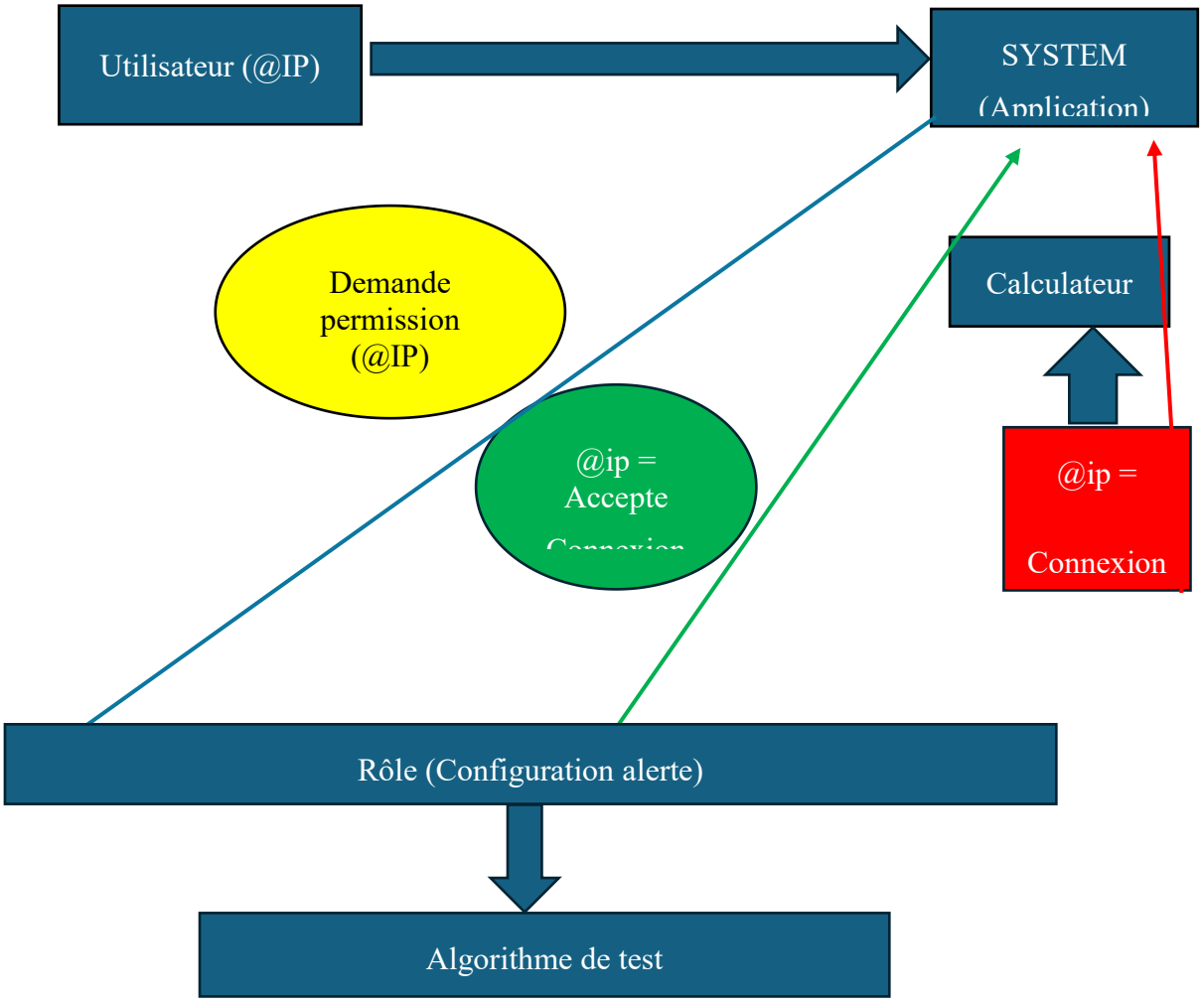

Figure III- 1: Architecture de l'algorithme d'alerte d'adresse IP

2) Si le volume de trafic dépasse un seuil maximal pendant les heures non critiques

L'utilisateur dispose de deux éléments dans la base de données :

1. **Calculateur de trafic** : Cet outil calcule le débit de données et évalue la quantité de trafic générée par l'utilisateur pour vérifier le respect des limites imposées.

2. Moniteur : Ce composant suit la consommation de débit par heure et enregistre les moments de connexion de l'utilisateur.

Lorsque l'utilisateur demande une connexion au réseau, le calculateur de trafic analyse cette demande en se basant sur les données actuelles.

Si le débit mesuré est inférieur à un seuil prédéfini, la connexion est autorisée.

En revanche, si le débit dépasse les limites acceptables, la connexion est bloquée. Par exemple, par exemple si la base de données stipule qu'une heure d'utilisation correspond à 1 Go de données, toute utilisation dépassant cette limite entraînera un refus d'accès au réseau.

La figure **III.2** illustre l'architecture qui assure une gestion efficace et dynamique du trafic, garantissant que les utilisateurs respectent les limites de bande passante tout en maintenant la performance du réseau.

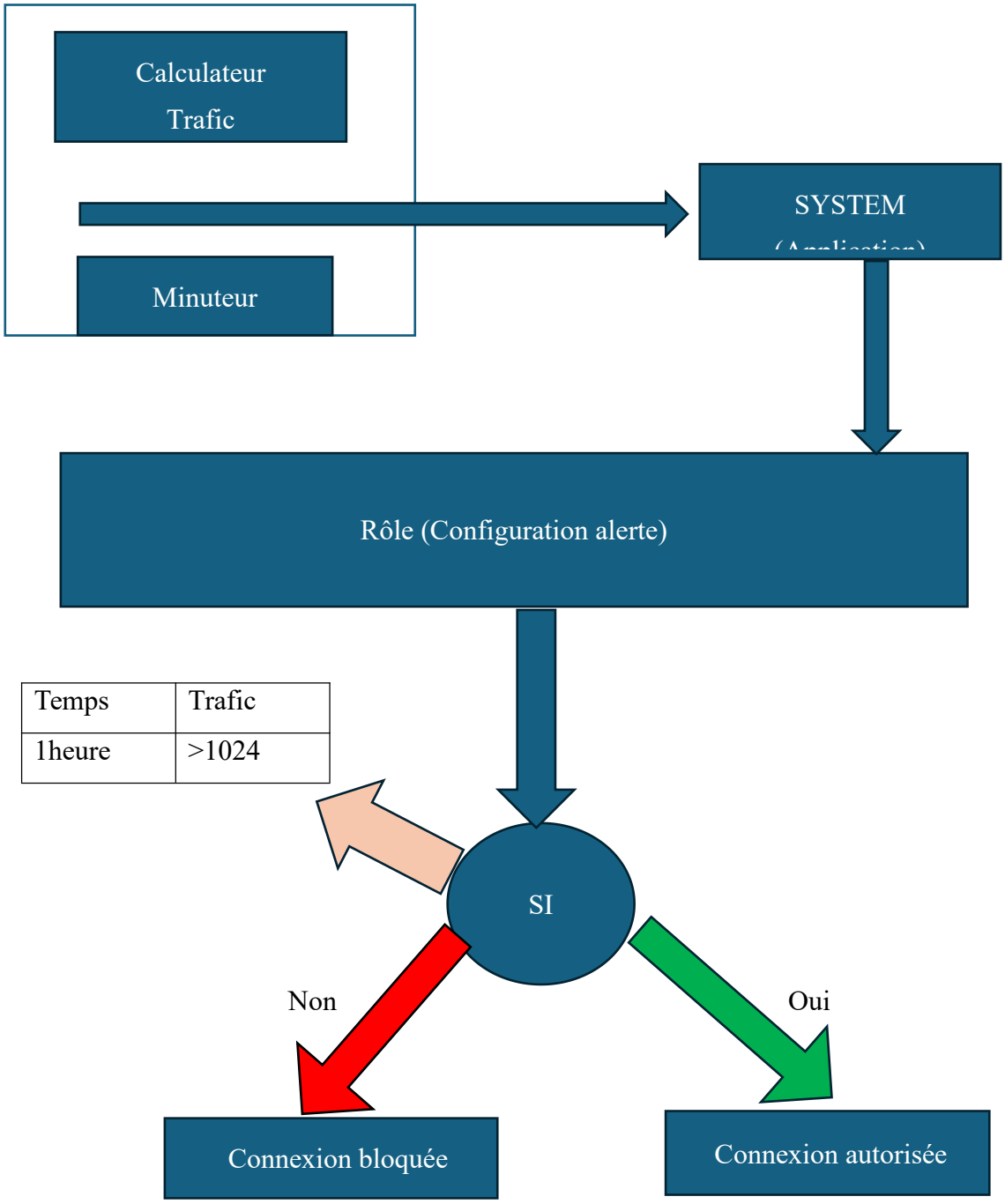

Figure III- 2: Architecture de l'algorithme du volume de trafic

3) Si des tentatives répétées d'accès avec des adresse IP non autorisées observées

-Le système détecte plusieurs tentatives d'accès avec des adresses IP non autorisées.

-Lorsqu'un utilisateur essaie de se connecter à plusieurs reprises avec une adresse IP non autorisée, le système envoie une alerte à la configuration de sécurité.

-La configuration de sécurité vérifie si l'adresse IP a été utilisée plusieurs fois pour des tentatives d'accès non autorisées.

-Le calculateur analyse la fréquence des tentatives avec cette adresse IP non autorisée. Si les tentatives répétées avec l'adresse IP non autorisée sont confirmées, la configuration de sécurité bloque l'accès au système pour cette adresse IP. La figure **III.3** représente le mécanisme d'authentification d'un utilisateur souhaitant accéder à un système. Il met en évidence les différentes vérifications effectuées pour garantir la sécurité des données.

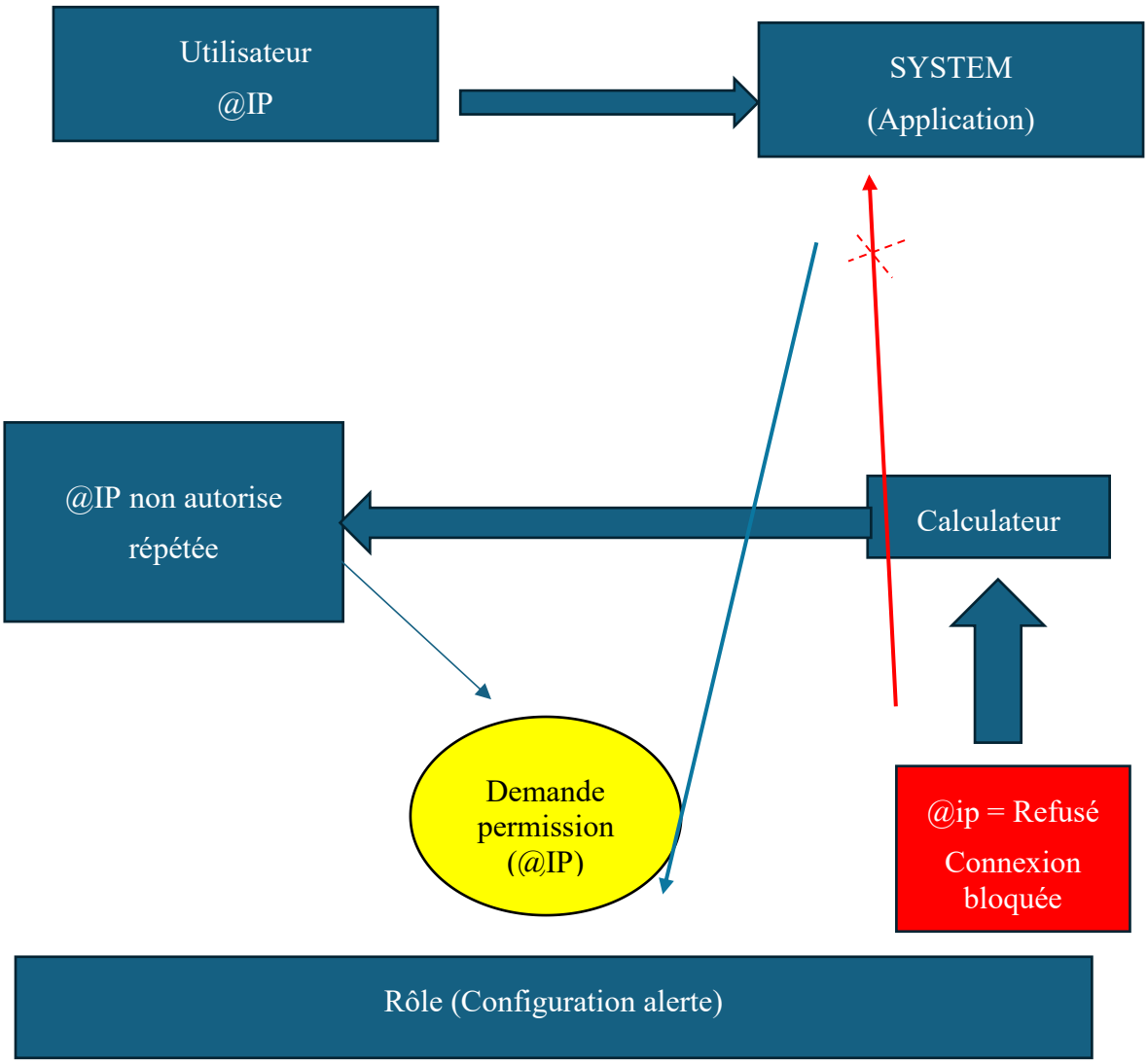

Figure III- 3: Algorithme d'adresse IP non autorisé

III.4.2.3 Architecture du système

L'architecture d'un système est une discipline fondamentale dans le développement logiciel, offrant une base solide pour la réalisation et la gestion efficace d'une application, la figure suivante qui représente l'architecture de notre système :

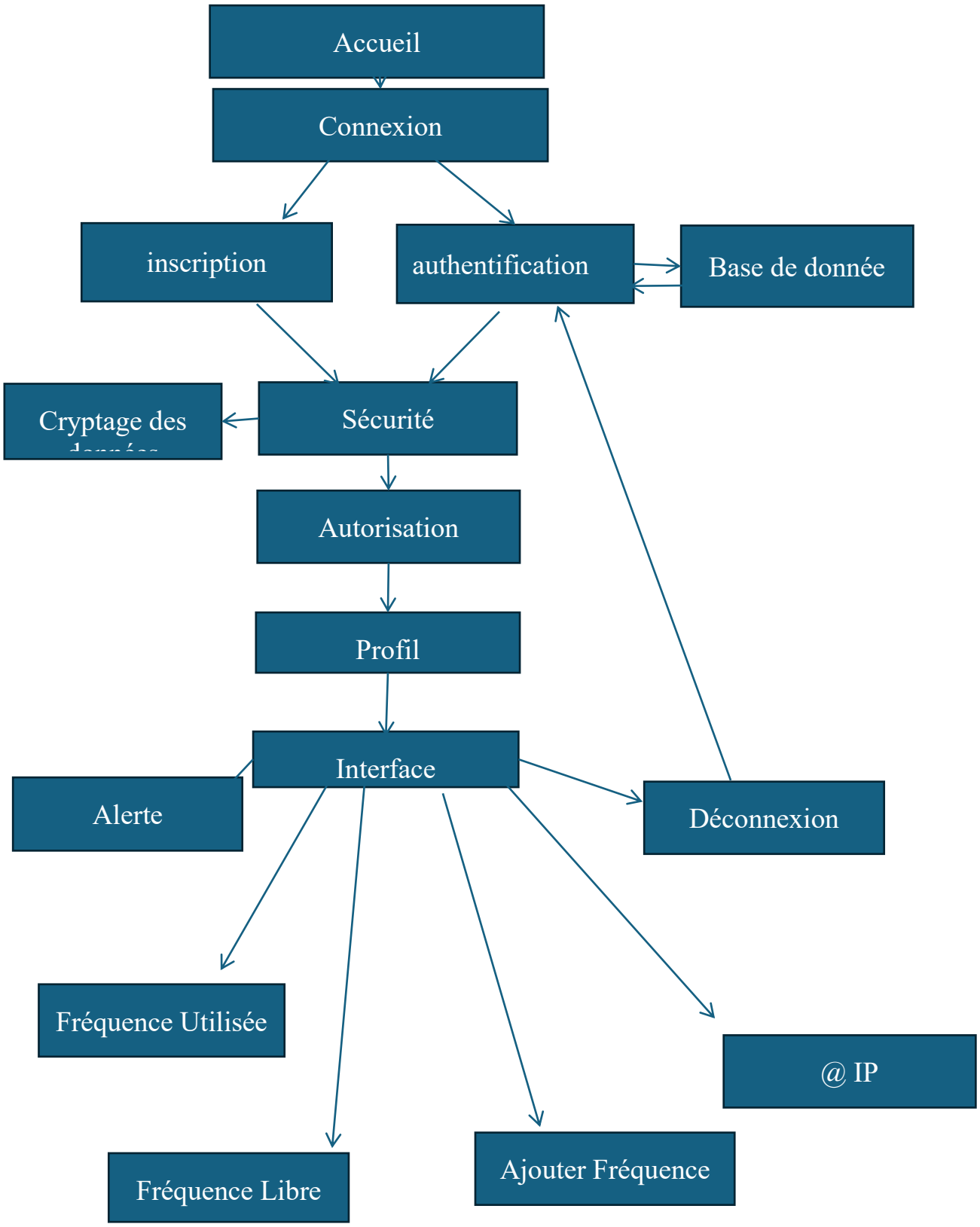

Figure III- 4: Architecture du système (application)

III.5 Conception système (les diagrammes)

Dans cette section, nous allons présenter la conception de l'application, qui offre une plateforme complète pour gérer l'allocation du spectre.

III.5.1 Exigences fonctionnelles

Dans cette section, nous énonçons les exigences fonctionnelles essentielles que notre application web doit remplir. Voici les besoins fonctionnels détaillés :

- L'authentification des utilisateurs se fait via une adresse et une clé privée pour accéder aux différentes fonctionnalités.
- Gérer la création, la publication, le retrait et la suppression des bandes de fréquences par l'opérateur.
- Acheter, solliciter des bandes de fréquences et créer des sous-bandes de fréquence par l'utilisateur principal.
- Acquérir des sous-bandes de fréquence par l'utilisateur secondaire.

III.5.2 Modélisation des exigences

III.5.2.1 Conception

1. Diagramme de cas d'utilisation :

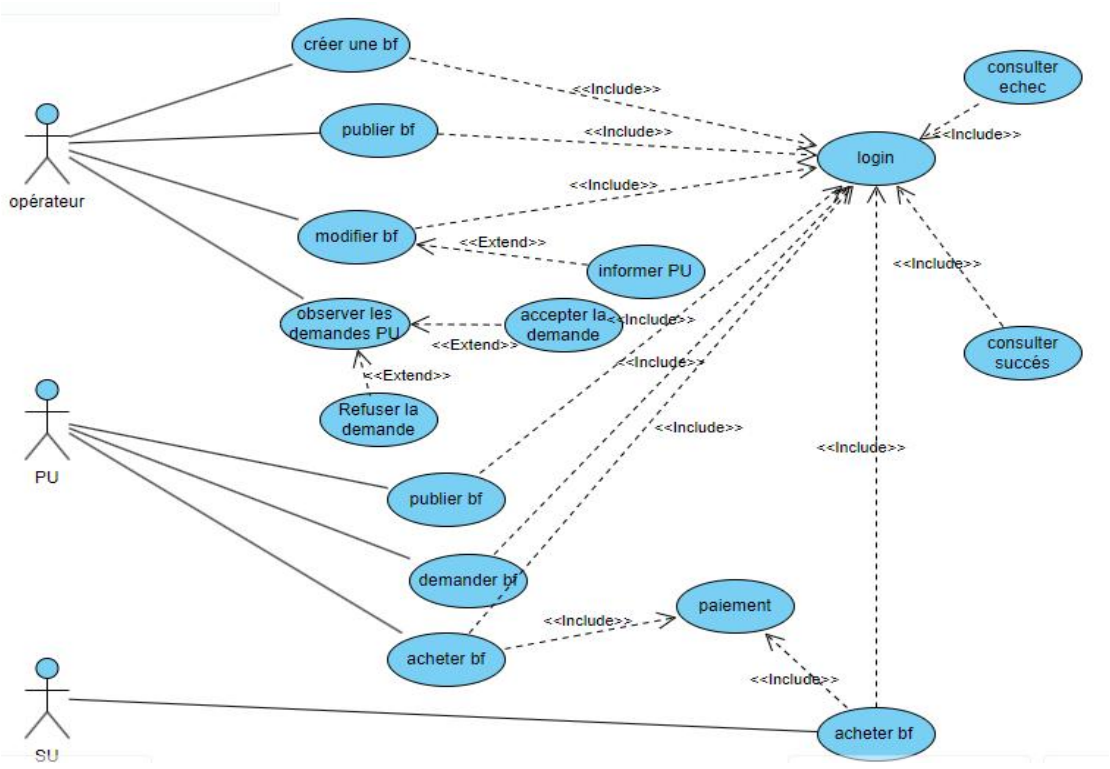

Figure III- 5: Diagramme de cas d'utilisation

2. Diagramme de séquence de cas <PU acheter une BF>

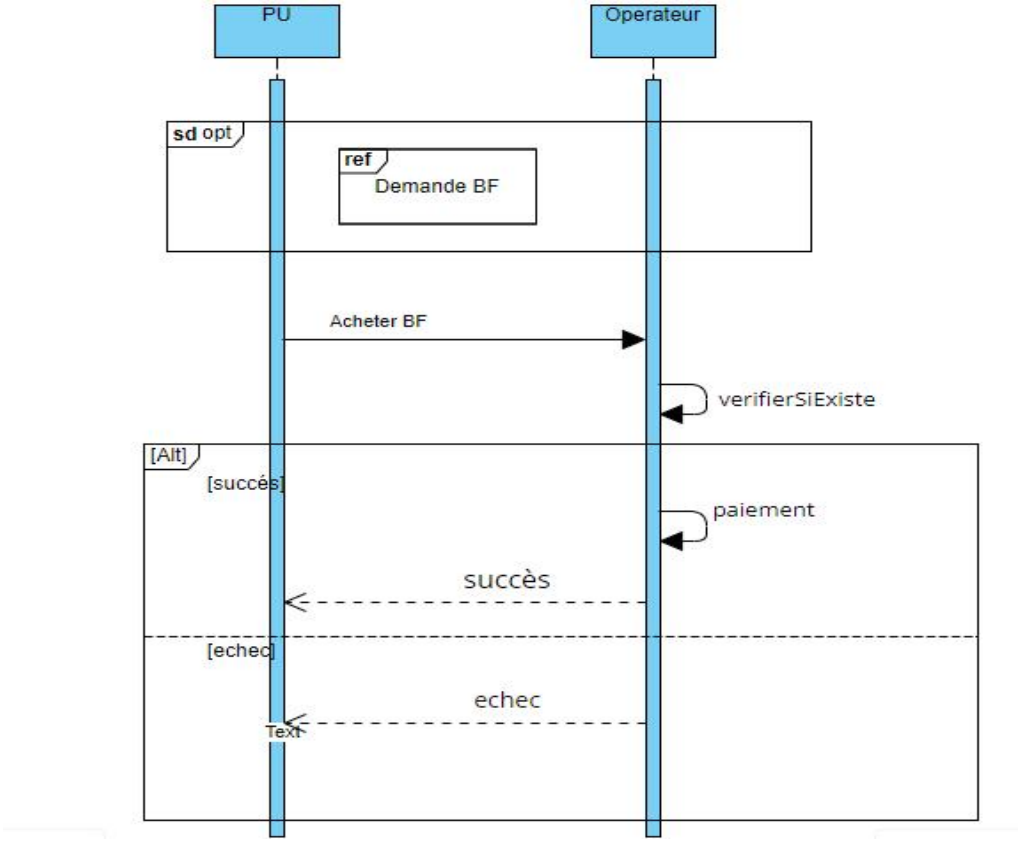

Figure III- 6: Diagramme de séquence de cas (PU acheter une BF)

3. Diagramme de séquence de cas <Demande BF>

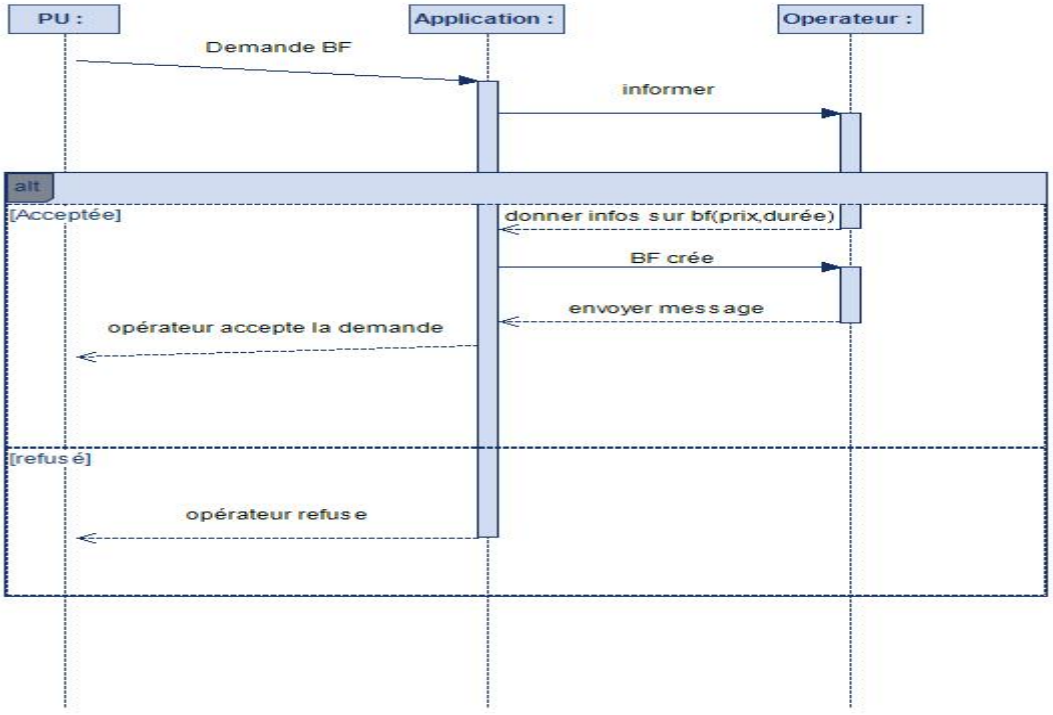

Figure III- 7: Diagramme de séquence de cas (Demande BF)

4. Diagramme de séquence de cas<SU acheter une BF>

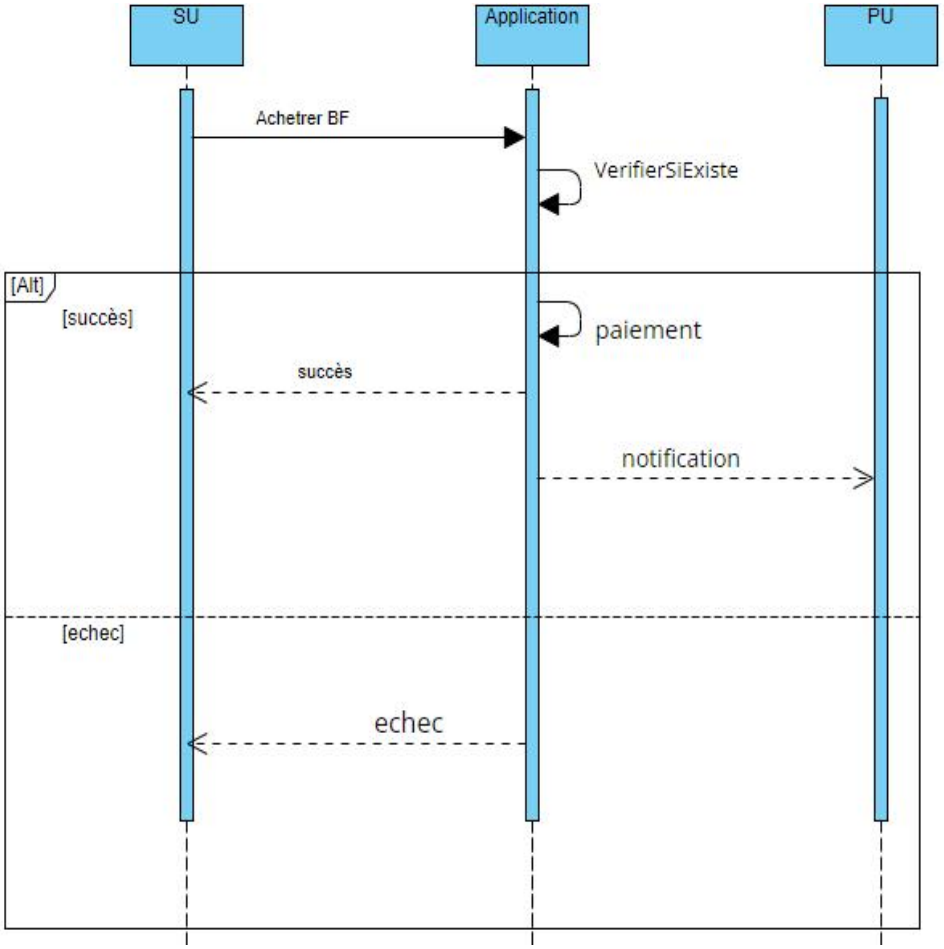

Figure III- 8: Diagramme de séquence de cas (SU acheter BF)

III.6 Résultats obtenus

IV.6 Temps d'exécution :

Ce tableau illustre comment le nombre de PU augmente au fur et à mesure que le temps d'exécution progresse, mesuré en milliseconde, Ce qui sert de critère de qualité pour notre application.

Tableau III- 2: Nombre de pu en fonction du temps d'exécutions

Temps d'exécution (ms)	Nombre de pu
0	2
1000	8
2000	12
3000	15
4000	18
5000	22
6000	25

Voici l'histogramme qui illustre les données de tableau III.1, mettant en évidence l'augmentation du temps d'exécution en fonction de l'accroissement du nombre de PU. (PU).

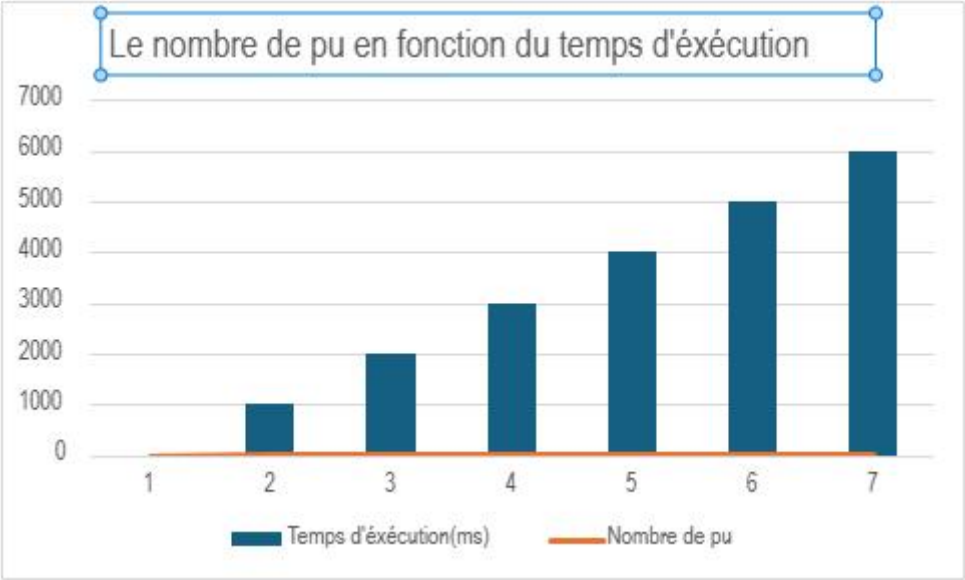

Figure III- 9: Histogramme de nombre de pu en fonction du temps d'éxécution

III.7 Présentation de l'application

III.3 Page accueil : la page d'accueil est le point d'accès principal à notre application ou site web. Elle est soigneusement conçue pour fournir aux utilisateurs une vue d'ensemble complète et enrichissante dès leur première visite.

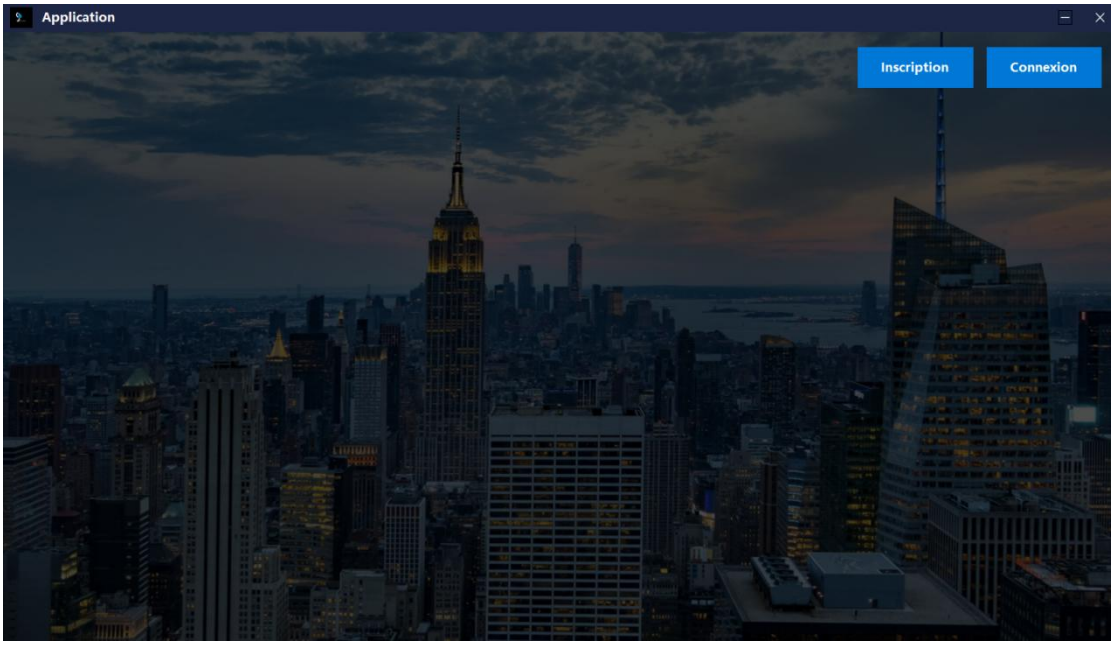

Figure III- 10: Page d'accueil

IV.3 Les interfaces

a. **Interface PU :** est une plate-forme numérique conçue pour fournir à ses utilisateurs une expérience sur mesure dans la gestion de leurs services.

Fonctionnalités Principales :

- **Gestion des Fréquences :**

- Fréquences Utilisées : Affichage de l'historique des fréquences consommées, incluant la date, la durée et le prix.

- Fréquences libres : Liste des fréquences encore disponibles à l'achat, avec des détails sur la date, la durée et le prix.

- **Profil Utilisateur :**

- Informations Personnelles : Détails tels que l'identifiant utilisateur (PU1) et l'adresse e-mail.

- État de Connexion : Indication du statut de connexion (Connecté ou Déconnecté).

- **Actions Disponibles** :

- Achat de Fréquences : Bouton "Acheter" permettant l'acquisition de fréquences disponibles.

- Modification de l'Adresse : Option pour mettre à jour l'adresse ip associée au compte.

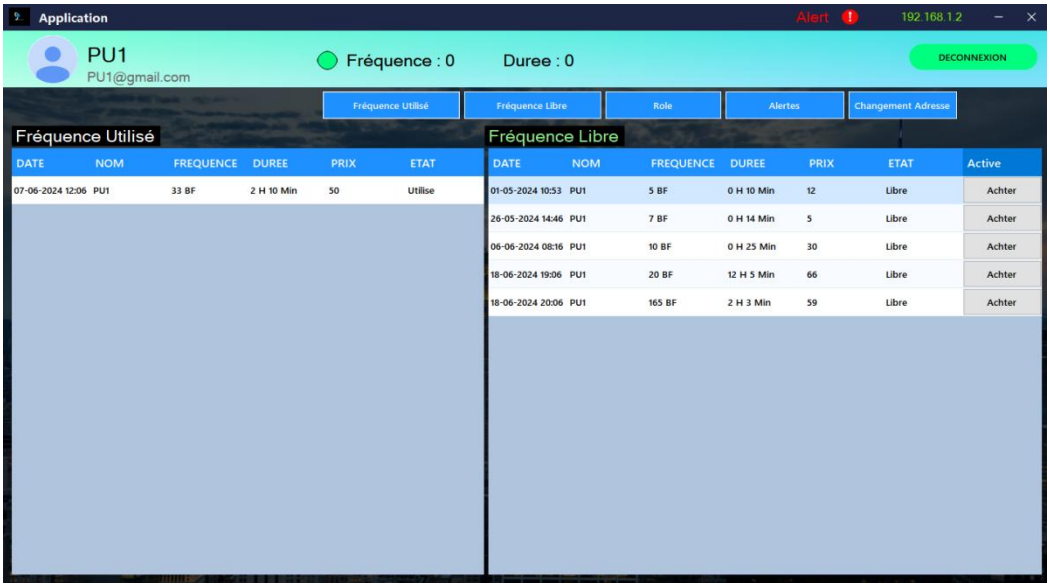

Figure III- 11: Interface PU

b. **Interface SU :** L'interface SU offre un potentiel prometteur, mais elle pourrait bénéficier d'améliorations sur plusieurs points. l'utilisateur a le droit de voir les fréquence utilisés et libres de l'utilisateur primaire pour choisir le meilleur offre qui base sur les critères de (prix ,nombre de canaux ,durée ...) selon le besoin, voici la figure qui la représente:

Figure III- 12: Interface SU

c. **Interface opérateur :**est un outil essentiel pour assurer une gestion optimale et un contrôle rigoureux des opérations, voici la figure suivante:

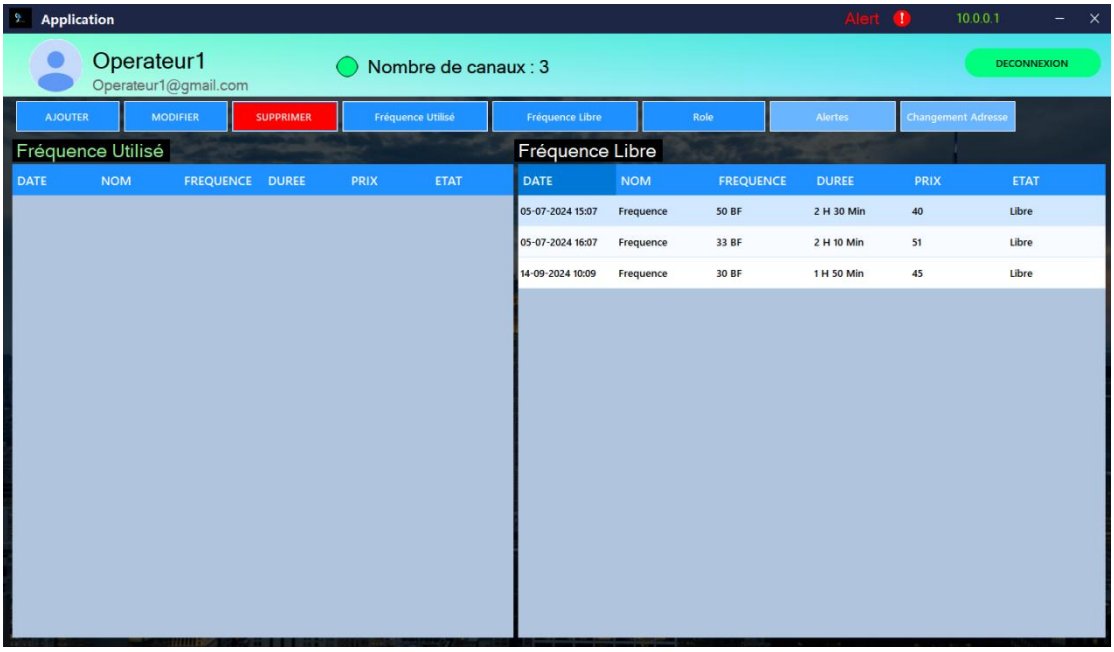

Figure III- 13: Interface opérateur

III.8 Conclusion

Dans ce chapitre, nous avons détaillé le fonctionnement de notre application ainsi que l'implémentation de contrôles d'accès, qui assurent l'intégrité des utilisateurs via leur clé privée. Nous avons également proposé d'intégrer le cryptage des données pour renforcer la sécurité des communications entre les utilisateurs primaires (PU) et secondaires (SU) dans le cadre d'un réseau de radio cognitive.

Nous avons également introduit trois interfaces au sein de cette application pour atténuer le problème des limites de bande de fréquence. La première interface est dédiée à l'opérateur, permettant la création, la publication, l'ajout, la suppression et la modification des bandes de fréquence. La deuxième interface est réservée aux utilisateurs primaires (PU) pour acheter et demander des bandes de fréquence.

Enfin, la troisième interface est conçue pour les utilisateurs secondaires (SU), facilitant l'achat de bandes de fréquence.

Conclusion générale

La radio cognitive est une technologie sans fil innovante qui permet aux utilisateurs de repérer intelligemment les canaux de communication disponibles. Chaque utilisateur secondaire a la possibilité d'exploiter les fréquences inoccupées, tout en respectant les droits de l'utilisateur primaire, qui détient l'accès à ces bandes. Lorsque l'utilisateur primaire en a besoin, les utilisateurs secondaires doivent libérer la fréquence après avoir terminé leur utilisation.

Dans ce travail, nous avons exploré en profondeur le domaine de la radio cognitive à travers trois chapitres complémentaires. Cette étude a permis d'explorer de manière approfondie le domaine de la radio cognitive, en abordant ses principes fondamentaux, sa structure et ses applications dans le premier chapitre. Nous avons ensuite examiné les enjeux de la sécurité des réseaux de radio cognitive, en mettant en évidence les menaces potentielles et l'importance des mécanismes de protection.

Enfin, notre contribution a été illustrée à travers le développement d'une application intégrant des solutions de cryptage des données et de contrôle d'accès, démontrant ainsi l'application concrète des concepts théoriques abordés, et consacré

Principalement d’assurer la communication entre différents SU avec différents PUs

En résumé, ce travail souligne l'importance d'intégrer sécurité et innovation dans le domaine de la radio cognitive, garantissant ainsi des communications efficaces et sûres dans un environnement technologique en constante évolution.

Références Bibliographiques

[1] M. D. Katz et F. H. P. Fitzek, *WiMAX Evolution*. John Wiley & Sons Ltd., Royaume-Uni, 2009.

[2] H. Bölcskei, "Principles of MIMO-OFDM wireless systems," *CRC Handbook on Signal Processing for Communications*, 2004.

[3] P. Lytrivis et A. Amditis, "Intelligent Transport Systems: Co-Operative Systems (Vehicular Communications)," *INTECH Open Access Publisher*, 2012.

[4] L. S. Cardoso, et al., "Ecoute coopérative de spectre pour la radio cognitive," *GRETSI-09*, 2009.

[5] G. M. J. Mitola, "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13-18, Aug. 1999.

[6] "Developments in cognitive radio," *Center for Telecommunications Research (CTR), King's College London*, [Online]. Available: http://www.ctr.kcl.ac.uk/crblog/CR.html. Accessed: Apr. 2013.

[7] A. Amraoui, B. Benmammar, et F. T. Bendimerad, "Accès Dynamique au Spectre dans le Contexte de la Radio Cognitive," in *Proc. 2ème édition de la conférence nationale de l'informatique (JEESI 2012)*, ESI, Oued-Smar (Alger), Algérie, Apr. 2012.

[8] M. B. Sajjan, et al., "Spectrum Aware Mobility Management In Cognitive Radio-A Survey," *International Journal for Innovative Research in Science and Technology*, vol. 1, no. 9, pp. 78-84, 2015.

[9] J. Mitola, "Encyclopedia of Telecommunications," Apr. 15, 2003.

[10] I. Larbi et B. Benmammar, "Négociation de spectre dans les réseaux de radio cognitive," *arXiv preprint arXiv:1407.2217*, 2014.

[11] I. F. Akyildiz, W. Y. Lee, et K. R. Chowdhury, "CRAHNs: Cognitive radio ad hoc networks," *Ad Hoc Networks*, vol. 7, no. 5, pp. 810-836, 2009.

[12] J. Mitola et G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13-18, 1999.

[13] P. Charalampidis, "Cognitive radio architecture: the engineering foundations of radio XML," *Wiley*, 2006.

[14] E. Hossain, D. Niyato, et Z. Han, *Dynamic Spectrum Access and Management in Cognitive Radio Networks*. Cambridge: Cambridge University Press, 2009.

[15] B. Benmammar et A. Amraoui, *Radio Resource Allocation and Dynamic Spectrum Access*. Wiley-ISTE, 2012.

[16] E. Hossain, D. Niyato, et Z. Han, *Dynamic Spectrum Access and Management in Cognitive Radio Networks*. Cambridge University Press, 2009.

[17] Y. Zhang, G. Xu, et X. Geng, "Security threats in cognitive radio networks," in *High Performance Computing and Communications*, IEEE International Conference on, pp. 1036–1041, 2008.

[18] W. El-Hajj, H. Safa, et M. Guizani, "Survey of security issues in cognitive radio networks," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 2, pp. 181–198, 2011.

[19] Ö. Cepheli et G. K. Kurt, "Physical layer security in cognitive radio networks: A beamforming approach," in *Proc. 2013 First International Black Sea Conference on Communications and Networking (BlackSeaCom)*, IEEE, pp. 233-237, 2013.

[20] R. Chen, J. M. Park, et J. H. Reed, "Defense against primary user emulation attacks in Cognitive Radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25–37, 2008.

[21] W. El-Hajj, H. Safa, et M. Guizani, "Survey of security issues in cognitive radio networks," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 2, pp. 181-198, 2011.

[22] 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.

[23] R. Chen, J. M. Park, Y. T. Hou, et J. H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Communications Magazine*, vol. 46, no. 4, 2008.

[24] R. Chen, J. M. Park, Y. T. Hou, et J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25–37, 2008.

[25] R. Chen, J. M. Park, et J. H. Reed, "Defense against primary user emulation attacks in Cognitive Radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25–37, 2008.

[26] R. Chen, J. M. Park, et J. H. Reed, "Defense against primary user emulation attacks in Cognitive Radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25–37, 2008.

[27] 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, pp. 1–8, 2008.

[28] O. León, J. Hernández-Serrano, et M. Soriano, "Securing cognitive radio networks," *International Journal of Communication Systems*, vol. 23, no. 5, pp. 633–652, 2010.

[29] S. Bhunia, S. Sengupta, et F. Vázquez-Abad, "Cr-honeynet: A learning & decoy based sustenance mechanism against jamming attack in CRN," in *Proc. 2014 IEEE Military Communications Conference*, IEEE, pp. 1173-1180, 2014.

[30] W. Xu, T. Wood, W. Trappe, et Y. Zhang, "Channel surfing and spatial retreats: Defenses against wireless denial of service," in *Proc. of the 3rd ACM Workshop on Wireless Security*, Philadelphia, PA, pp. 80-89, 2004.

[31] M. Khasawneh et A. Agarwal, "A survey on security in cognitive radio networks," in *Proc. 2014 6th International Conference on Computer Science and Information Technology (CSIT 2014)*, pp. 64–70, 2014.

[32] C. Mathur et K. Subbalakshmi, "Security Issues in Cognitive Radio Networks," in *Cognitive Networks: Towards Self-Aware Networks*, Wiley, New York, pp. 284-293, 2007.

[33] C. Karlof et D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2, pp. 293–315, 2003.

[34] R. Chen, J. M. Park, Y. T. Hou, et J. H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Communications Magazine*, vol. 46, no. 4, 2008.

[35] Y. Shei et Y. T. Su, "A sequential test based cooperative spectrum sensing scheme for cognitive radios," in *Proc. 2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2008)*, pp. 1–5, 2008.

[36] I. Technology, "Survey of Security Issues in Cognitive Radio Networks," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 2, 2011.

[37] W. Wang, H. Li, Y. Sun, et Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Proc. Information Sciences and Systems (CISS 2009)*, 43rd Annual Conference on, pp. 130–134, 2009.

[38] K. Bian et J. M. Park, "MAC-Layer Misbehaviors in Multi-hop Cognitive Radio Networks," in *Proc. 2006 US-Korea Conference

on Science, Technology, and Entrepreneurship (UKC 2006)*, Aug. 2006.

[39] M. Khasawneh et A. Agarwal, "A survey on security in cognitive radio networks," in *Proc. 2014 6th International Conference on Computer Science and Information Technology (CSIT 2014)*, pp. 64–70, 2014.

[40] L. Lazos, S. Liu, et M. Krunz, "Mitigating control-channel jamming attacks in multi-channel ad hoc networks," in *Proc. of the Second ACM Conference on Wireless Network Security*, pp. 169–180, 2009.

[41] J. Hernández-Serrano, O. León, et M. Soriano, "Modeling the Lion Attack in Cognitive Radio Networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, Article ID 242304, 10 pages, 2011.

[42] B. Benmammar, A. Amraoui, et F. Krief, "A survey on dynamic spectrum access techniques in cognitive radio networks," *International Journal of Communication Networks and Information Security*, vol. 5, no. 2, pp. 68, 2013.

[43] A. Khattab, D. Perkins, et M. Bayoumi, *Cognitive Radio Networks: From Theory to Practice*. Springer Science & Business Media, 2012.

[44] P. Samarati et S. De Capitani di Vimercati, "Access control: Policies, models, and mechanisms," in *Foundations of Security Analysis and Design (LNCS 2171)*, Springer-Verlag, 2001.

[45] D. F. Ferraiolo, R. Sandhu, S. Gavrila, et al., "Proposed NIST standard for role-based access control," *ACM Transactions on Information and System Security (TISSEC)*, vol. 4, no. 3, pp. 224-274, 2001.

[46] V. C. Hu, D. Ferraiolo, R. Kuhn, et al., "Guide to attribute based access control (ABAC) definition and considerations," *NIST Special Publication 800-162*, vol. 1, no. 54, 2013.

[47] T. Fink, M. Koch, et C. Oancea, "Specification and enforcement of access control in heterogeneous distributed applications," in *Proc. International Conference on Web Services*, Springer, pp. 88-100, 2003.

[48] R. K. Thomas et R. S. Sandhu, "Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management," in *Database Security XI*, Springer, pp. 166-181, 1998.

[49] R. K. Thomas, "Team-based access control (TMAC) a primitive for applying role-based access controls in collaborative environments," in *Proc. of the Second ACM Workshop on Role-based Access Control*, pp. 13-19, 1997.

[50] A. A. E. Kalam, R. E. Baida, P. Balbiani, et al., "Organization based access control," in *Proc. POLICY 2003 IEEE 4th International Workshop on Policies for Distributed Systems and Networks*, IEEE, pp. 120-131, 2003.

[51] S. Crane, A. Homescu, P. Larsen, et al., "The continuing arms race: Code-reuse attacks and defenses," *MIT Lincoln Laboratory, Lexington*, 2018.

[52] R. Yavatkar, D. Pendarakis, et R. Guerin, "A framework for policy-based admission control," *RFC 2753*, 2000.

[53] A. Westerinen, J. Schnizlein, J. Strassner, et al., "Terminology for policy-based management," *RFC 3198*, 2001.

[54] S. Dramé-Maigné, *Blockchain and Access Control: Towards a More Secure Internet of Things*. Thèse de doctorat, Université Paris-Saclay, 2019.

[55] C. Marwan, "Un cadre de spécification et de déploiement de politiques d'autorisation," Thèse de doctorat, Toulouse III : École Doctorale EDMITT, 2012.

[56] P. T. Van, "Partage de documents sécurisés dans le Cloud Personnel," *Université Paris-Saclay*, 2018.

Résumé

La radio cognitive est une technologie qui améliore significativement l'utilisation du spectre radio en permettant une exploitation dynamique et opportuniste des fréquences sans fil. Dans ce mémoire, nous avons exploré la sécurisation d'un réseau de radio cognitive contre les attaques PUE (Primary User Emulation). Pour cela, nous avons mis en œuvre des mécanismes de contrôle d'accès et cryptage de données pour assurer l'intégrité et la fiabilité des utilisateurs.

Mots-clé : radio cognitive – contrôle d'accès – sécurité – cryptage de donnée – Attaque PUE.

Abstract

Cognitive radio is a technology that significantly improves the use of the radio spectrum by allowing dynamic and opportunistic exploitation of wireless frequencies. In this dissertation, we explored securing a cognitive radio network against PUE (Primary User Emulation) attacks. For this, we have implemented access control and data encryption mechanisms to ensure the integrity and reliability of users.

Keywords: cognitive radio – access control – security – data encryption – PUE attack.

ملخص

الراديو الإدراكية هو تقنية تعمل على استخدام الطيف الراديوي بشكل كبير من خلال السماح بالاستغلال الديناميكي الانتهازي للترددات اللاسلكية. في هذه المذكرة استكشفنا تامين شبكة راديو معرفية ضد هجوم محاكاة المستخدم الاساسي. وللقيام بذلك قمنا بتنفيذ اليات التحكم في الوصول وتشفير البيانات لضمان سلامة وموثوقية المستخدمين.

الكلمات المفتاحية: الراديو المعرفي - التحكم في الوصول - الامان - تشفير البيانات - محاكاة المستخدم الاساسي