الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة أبي بكر بلقايد – تلمسان –

Université Aboubakr Belkaïd – Tlemcen –
Faculté de TECHNOLOGIE

THESE

Présentée pour l'obtention du **grade** de **DOCTORAT 3ème Cycle**

En : Télécommunication

Spécialité : Communications et réseaux sans fil

Par : SEGHIRI Naouel

Sujet

Sécurisation des données médicales dans les réseaux de radio cognitive

Soutenue publiquement, le 25 / 09 / 2025, devant le jury composé de :

M Fethi Tarik BENDIMERAD	Professeur Émérite	Univ. Tlemcen	Président
M Mohammed Zakarya BABA-AHMED	MCA	Univ. Tlemcen	Directeur de thèse
M Badr BENMAMMAR	Professeur	Univ. Tlemcen	Co- Directeur de thèse
Mme Asma AMRAOUI	MCA	Univ. Tlemcen	Examinateur 1
M Ghouti ABDELLAOUI	MCA	ESSAT. Tlemcen	Examinateur 2

Année universitaire : 2024-2025.

Remerciements

Je rends grâce à Allah, le Tout-Puissant, pour m'avoir accordé la force, la patience et la persévérance indispensables à l'aboutissement de ce travail. C'est par sa volonté et sa miséricorde que cet accomplissement a été rendu possible.

Je souhaite exprimer ma profonde gratitude à Monsieur Mohammed Zakarya BABA-AHMED, directeur de cette thèse, pour sa disponibilité sans faille, ses encouragements constants, son humilité, sa générosité dans le partage des connaissances, ainsi que pour son remarquable esprit scientifique et pédagogique. Son encadrement attentif et bienveillant a constitué une source précieuse d'inspiration et un soutien déterminant tout au long de mon parcours doctoral.

Je tiens également à remercier Monsieur Badr BENMAMMAR, co-directeur de cette thèse, pour l'attention portée à ce travail, pour sa bienveillance, ses compétences reconnues et sa contribution significative à l'enrichissement scientifique de cette recherche.

J'exprime ma plus profonde reconnaissance aux membres du jury : Pr. Fethi Tarik BENDIMERAD le président du jury, Mme Asma AMRAOUI et Mr Ghouti ABDELLAOUI pour l'honneur qu'ils me font en acceptant d'évaluer ce travail. J'espère que cette thèse saura répondre à leurs attentes et témoignera de mon engagement scientifique.

Enfin, je souhaite adresser mes sincères remerciements aux membres du Laboratoire de Télécommunications de Tlemcen (LTT) pour l'ambiance chaleureuse, l'esprit d'équipe et les précieux échanges scientifiques qui ont contribué à rendre cette aventure humaine et intellectuelle particulièrement enrichissante.

Dédicaces

Je dédie ce travail à mes parents bien-aimés, piliers de ma vie, dont l'amour inconditionnel, les prières constantes et le soutien sans faille ont été le fondement de mon parcours. Leur présence, Leur sagesse et la confiance qu'ils m'ont toujours témoignée ont renforcé ma détermination et m'ont portée jusqu'à l'aboutissement de ce projet qui me tient profondément à cœur.

Je souhaite exprimer toute ma reconnaissance à mon époux pour son soutien moral et professionnel, son appui constant et sa patience, qui ont été essentiels tout au long de ce travail. Ses encouragements et sa présence ont constitué un pilier fondamental dans l'accomplissement de cette thèse.

Je dédie cette thèse à ma petite fille, la lumière de ma vie, dont le sourire, la tendresse et la clarté ont illuminé mes journées et nourri mon courage dans les moments les plus exigeants. Que ce travail soit un jour pour elle une source d'inspiration et de fierté.

Je remercie également mes sœurs pour leur affection, leur soutien indéfectible et leurs encouragements permanents, qui m'ont accompagnée tout au long de ce parcours exigeant.

Une pensée affectueuse à mes neveux, dont la joie et la spontanéité ont été une source de réconfort et de motivation tout au long de ce parcours.

Je n'oublie pas ma famille et mes amies chères, dont l'écoute attentive, le soutien fidèle et la bienveillance m'ont apporté un équilibre précieux au fil de ces années.

Résumé

Dans un contexte où les réseaux de radio cognitive offrent une solution prometteuse pour l'optimisation dynamique du spectre, la sécurité des données échangées devient un enjeu crucial, en particulier pour les applications médicales sensibles. Cette thèse propose une approche innovante pour la sécurisation des données médicales dans les réseaux de radio cognitive, en s'appuyant sur les systèmes multi-agents pour modéliser les interactions et décisions au sein du réseau.

L'architecture développée intègre des mécanismes de sélection des canaux, en utilisant la méthode multicritère TOPSIS, permettant aux utilisateurs secondaires de choisir les ressources optimales selon des critères tels que la technologie, la fiabilité, le coût et la bande passante. Par ailleurs, un mode de chiffrement symétrique optimisé a été appliqué pour garantir la confidentialité des échanges.

Les simulations menées sur la plateforme JADE ont confirmé la robustesse du système face aux menaces internes, sa capacité à détecter les agents malveillants, et l'efficacité de la solution hybride mise en place, combinant authentification, décision et confidentialité. Les résultats obtenus démontrent la pertinence de l'approche pour sécuriser les données médicales dans des environnements distribués complexes.

Mots clés : Sécurité, Radio Cognitive, Données Médicales, Systèmes Multi-Agents, Cryptographie, Méthode Multicritère TOPSIS.

Abstract

In a context where cognitive radio networks offer a promising solution for dynamic spectrum optimization, the security of exchanged data becomes a crucial challenge, particularly for sensitive medical applications. This thesis proposes an innovative approach to securing medical data in cognitive radio networks, relying on multi-agent systems to model interactions and decision-making processes within the network.

The developed architecture integrates channel selection mechanisms using the TOPSIS multi-criteria method, enabling secondary users to choose optimal resources based on criteria such as technology, reliability, cost, and bandwidth. Furthermore, an optimized symmetric encryption mode was applied to ensure the confidentiality of exchanges.

Simulations conducted on the JADE platform confirmed the system's robustness against internal threats, its ability to detect malicious agents, and the effectiveness of the implemented hybrid solution, combining authentication, decision-making, and confidentiality. The results demonstrate the relevance of the proposed approach for securing medical data in complex distributed environments.

Keywords: Security, Cognitive Radio, Medical Data, Multi-Agent Systems, Cryptography, TOPSIS multi-criteria method.

الملخص

في سياقٍ توفر فيه شبكات الراديو المعرفي حلاً واعدًا لتحسين استخدام الطيف بشكل ديناميكي، أصبحت مسألة تأمين البيانات المتبادلة تحديًا أساسيًا، خاصةً بالنسبة للتطبيقات الطبية الحساسة. تقترح هذه الأطروحة منهجًا مبتكرًا لتأمين البيانات الطبية ضمن شبكات الراديو المعرفي، بالاعتماد على أنظمة الوكلاء المتعددين لنمذجة التفاعلات واتخاذ القرارات داخل الشبكة.

تتضمن البنية المطورة آليات اختيار القنوات باستخدام طريقة TOPSIS متعددة المعايير، مما يمكّن المستخدمين الثانويين من اختيار الموارد المثلى بناءً على معايير مثل التكنولوجيا، والموثوقية، والتكلفة، وعرض النطاق الترددي. علاوةً على ذلك، تم تطبيق وضع تشفير متماثل محسّن لضمان سرية التبادلات.

وقد أكدت المحاكاة التي أُجريت على منصة JADE متانة النظام في مواجهة التهديدات الداخلية، وقدرته على كشف العوامل الخبيثة، وفعالية الحل الهجين المُطبق، الذي يجمع بين المصادقة، واتخاذ القرار، وضمان السرية. وتُبرز النتائج المتحصل عليها مدى ملاءمة النهج المقترح لتأمين البيانات الطبية في بيئات موزعة ومعقدة.

الكلمات المفتاحية: الأمان، الراديو المعرفي، البيانات الطبية، أنظمة الوكلاء المتعددين، التشفير،طريقة TOPSIS متعددة المعايير.

Table des matières

Chapitre 2 : Sécurité dans les réseaux radio cognitifs.

Chapitre 3 : Contributions proposées pour la sécurisation des réseaux radio cognitifs.

Liste des figures

Liste des tableaux

Liste des abréviations

3G	La troisième génération
4G	La quatrième génération
5G	la cinquième génération
6G	La sixième génération
ACL	Agent Communication Language
ADC	Analog to Digital Converter
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AHP	Analytic Hierarchy Process
AJLA	Adaptive Jammer Localization Algorithm
AMS	Agent Management System
ANP	Analytic Network Process
AR	Activation des Résultats
BDI	Belief, Desire, Intention
BS	Base Station
CAN	Convertisseur Analogique-Numérique
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CL	Centroid Localization
CNA	Convertisseur Numérique-Analogique
CPU	Central Processing Unit
CR	Cognitive Radio
CRN	Cognitive Radio Network
CRV	Credit Risk Value
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CTR	Counter
DAC	Digital to Analog Converter
DDR	Double Data Rate
DES	Data Encryption Standard
DF	Directory Facilitator
DME	Dossier Médical Électronique
DoS	Denial of Service
DSP	Digital Signal Processor
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie–Hellman
E-Health	Electronic Health
ELECTRE	ELimination Et Choix Traduisant la REalité
FCC	Federal Communications Commission

FI	Fréquence Intermédiaire
FIPA	Foundation for Intelligent Physical Agents
FIPA-ACL	Foundation for Intelligent Physical Agents - Agent Communication Language
FIPS	Federal Information Processing Standards
FPGA	Field Programmable Gate Array
GPU	Graphics Processing Unit
GSM	Global System for Mobile communication
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
IA	Intelligence Artificielle
IBLT	Instance-Based Learning Theory
IDE	Integrated Development Environment
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IGSA	Improved Gravitational Search Algorithm
InteRRaP	Integration of Reactive behavior and Rational Planning
IoT	Internet of Things
ISE	Integrated Synthesis Environment
ISO	International Organization for Standardization
JADE	Java Agent DEvelopment Framework
JMH	Java Microbenchmark Harness
KQML	Knowledge Query and Manipulation Language
LNA	Low Noise Amplifier
LTM	Long-Term Memory
MAC	Media Access Control
MADM	Multi-Attribute Decision Making
MBLA	Multichannel Bayesian Learning Automata
MBWA	Mobile Broadband Wireless Access
MCDM	Multi Criteria Decision Making
MDP	Markov Decision Process
MODM	Multi-Objective Decision Making
NIST	National Institute of Standards and Technology
OFA	Objective Function Attack
OFB	Output Feedback
OS	Operating System
PE	Planification et Exécution
PKCS	Public-Key Cryptography Standards
PNs	Primary Networks
PROMETHEE	Preference Ranking Organization METHod for Enrichment Evaluations
PTS	Processeur de Traitement du Signal
PU	Primary User
PUE	Primary User Emulation
PUs	Primary Users

QoI	Quality of Information
QoS	Quality of Service
RAM	Random Access Memory
RC	Radio Cognitive
RF	Radio Frequency
RGPD	Règlement Général sur la Protection des Données
RLR	Radio Logicielle Restreinte
RMI	Remote Method Invocation
RSA	Rivest–Shamir–Adleman
SCN	Selfish Channel Negotiation
SDR	Software-Defined Radio
SHA	Secure Hash Algorithm
SMA	Systèmes Multi-Agents
SNR	Signal-to-Noise Ratio
SSDF	Spectrum Sensing Data Falsification
SSL	Secure Socket Layer
STM	Short-Term Memory
SU	Secondary User
SU-Receiver	Utilisateur Secondaire Récepteur
SUs	Secondary Users
SWIPT	Simultaneous Wireless Information and Power Transfer
TLS	Transport Layer Security
TOPSIS	Technique for Order of Preference by Similarity to Ideal Solution
TRM	Trust and Reputation Management
TV	Télévision
UFH	Uncoordinated Frequency Hopping
UWB	Ultra Wide Band
VANET	Vehicular Ad Hoc Network
VFIL	Virtual Force Iterative Localization
VHDL	VHSIC Hardware Description Language
VIKOR	VIseKriterijumska Optimizacija I Kompromisno Resenje
WBAN	Wireless Body Area Network
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WRAN	Wireless Regional Area Network
WWAN	Wireless Wide Area Network

Introduction générale

Au cours des dernières décennies, les technologies sans fil ont connu un essor remarquable sous l'effet de la demande croissante en connectivité mobile et de la numérisation des secteurs, notamment celui de la santé. Cette dynamique a vu émerger la e-santé, regroupant l'ensemble des pratiques médicales reposant sur les technologies de l'information et de la communication. L'échange sans fil de données médicales sensibles est ainsi devenu crucial pour la télémédecine, la surveillance continue des patients et le fonctionnement des dispositifs médicaux modernes.

Cependant, cette évolution exerce une forte pression sur le spectre radioélectrique, ressource limitée dont la gestion statique a conduit à des déséquilibres entre bandes saturées et sous-utilisées. La radio cognitive (RC), fondée sur la radio logicielle et l'intelligence artificielle, propose une utilisation dynamique et intelligente du spectre en adaptant en temps réel les communications à l'environnement.

L'introduction de la RC dans les réseaux médicaux soulève toutefois de nouveaux défis en matière de sécurité. La nature dynamique, distribuée et ouverte des réseaux radio cognitifs (CRNs) les rend particulièrement vulnérables aux attaques pouvant compromettre la confidentialité, l'intégrité et la disponibilité des données médicales. Sécuriser efficacement ces échanges devient alors un enjeu stratégique majeur.

Les réseaux radio cognitifs, tout en offrant une gestion optimisée du spectre, introduisent une complexité supplémentaire en matière de sécurité. Les mécanismes traditionnels de protection ne sont pas adaptés à la variabilité et à l'autonomie de ces réseaux. De surcroît, dans le contexte spécifique de la e-santé, l'enjeu de la protection des données médicales sensibles devient particulièrement critique, ces données devant impérativement rester confidentielles, fiables et disponibles en permanence. La question centrale à laquelle cette thèse s'efforce de répondre peut ainsi être formulée comme suit : comment concevoir des mécanismes de sécurisation efficaces, adaptatifs et légers pour protéger les données médicales dans un environnement radio cognitif dynamique et exposé aux menaces multiples ?

La complexité de cette problématique réside dans la nécessité de conjuguer des exigences élevées de sécurité avec les contraintes des réseaux sans fil modernes, telles que la limitation de la bande passante, la mobilité et les faibles délais de transmission imposés par les applications médicales. Ce travail de recherche vise ainsi à développer des solutions intelligentes de sécurisation, basées sur des stratégies multicritères, des mécanismes de chiffrement optimisés et une architecture adaptative, répondant aux évolutions en temps réel du réseau.

Afin de répondre aux défis identifiés, cette thèse propose plusieurs contributions scientifiques majeures, réparties en trois axes complémentaires et cohérents :

- Première contribution : Optimisation de la sélection spectrale multicritère dans les réseaux radio cognitifs : Dans les environnements radio cognitifs, le choix de la meilleure opportunité spectrale doit se faire en tenant compte de multiples critères parfois contradictoires : qualité du canal, temps de location, bande passante disponible, prix, etc. Nous avons ainsi développé une approche basée sur l'algorithme TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution), adaptée au contexte cognitif médical. Ce modèle permet d'évaluer, de classer et de sélectionner dynamiquement l'utilisateur primaire optimal, garantissant une communication sécurisée, fiable et performante pour les utilisateurs secondaires en fonction de leur profil et de leurs exigences de qualité de service (QoS). Cette approche intègre également une capacité d'apprentissage autonome, permettant aux utilisateurs cognitifs d'améliorer leurs décisions au fil du temps selon l'évolution du contexte radioélectrique.
- Deuxième contribution : Amélioration du chiffrement symétrique ECB dédié à la protection des données médicales : Face aux limites connues du mode de chiffrement ECB classique (notamment l'absence d'obfuscation des schémas répétitifs dans les données), nous avons conçu une version optimisée du mode ECB, spécifiquement adaptée aux contraintes des communications médicales dans un environnement cognitif. Notre méthode propose une diversification dynamique des blocs de chiffrement, introduisant une variabilité contrôlée tout en conservant la simplicité et la rapidité d'exécution caractéristiques du mode ECB.
- Troisième contribution : Conception d'une architecture globale de sécurisation basée sur les systèmes multi-agents : Afin d'orchestrer de manière autonome la sécurisation des communications dans les réseaux radio cognitifs, nous avons proposé une architecture distribuée et modulaire, reposant sur des systèmes multi-agents (SMA). Chaque agent est doté d'une capacité de perception, de décision et d'action lui permettant de participer à la détection des opportunités spectrales, à la sélection optimale du canal, à l'application des politiques de chiffrement, et à la négociation avec d'autres utilisateurs du réseau. Cette architecture favorise la résilience, l'adaptation rapide aux changements de l'environnement et l'autonomie locale des dispositifs, réduisant la dépendance vis-à-vis d'une infrastructure centralisée et améliorant la robustesse globale du réseau face aux attaques.

L'ensemble des solutions proposées a été implémenté et validé par le biais de simulations sur la plateforme JADE (Java Agent DEvelopment Framework), spécialisée pour la modélisation de comportements multi-agents. Nous avons défini plusieurs scénarios réalistes

correspondant à des cas d'usage de la e-santé. Les résultats démontrent des améliorations significatives par rapport aux approches classiques de sécurisation et de gestion de spectre.

Cette thèse est structurée en quatre chapitres, chacun répondant à une phase spécifique de notre réflexion scientifique.

Le premier chapitre, intitulé "La radio cognitive au service de l'E-santé : opportunités et défis", présente tout d'abord les concepts fondamentaux relatifs aux réseaux sans fil, aux infrastructures technologiques et à la radio logicielle. Nous introduisons ensuite le principe de la radio cognitive, son historique, ses principales fonctionnalités telles que la détection du spectre, la gestion dynamique du spectre, le partage du spectre et la mobilité du spectre. Ce chapitre souligne enfin comment l'intégration de la radio cognitive dans les infrastructures de e-santé ouvre de nouvelles perspectives tout en soulevant des défis techniques et sécuritaires spécifiques.

Le deuxième chapitre, intitulé "Sécurité dans les réseaux radio cognitifs", est consacré à l'étude des concepts fondamentaux de la sécurité des systèmes d'information, en particulier dans le contexte des réseaux radio cognitifs. Nous y détaillons les principales exigences de sécurité, les vulnérabilités propres aux réseaux radio cognitifs, ainsi que les types d'attaques auxquels ces réseaux sont exposés. Ce chapitre analyse également l'état actuel des normes de sécurité applicables aux données médicales et identifie les défis non résolus en matière de protection dans des environnements dynamiques et distribués.

Le troisième chapitre, intitulé "Contributions proposées pour la sécurisation des réseaux radio cognitifs", présente nos contributions scientifiques. Nous y exposons en détail l'approche multicritère pour la sélection sécurisée des opportunités spectrales, l'optimisation du mode de chiffrement symétrique ECB afin de l'adapter aux contraintes médicales, ainsi que la conception d'une architecture intégrant des systèmes multi-agents pour une gestion autonome de la sécurité dans les réseaux radio cognitifs.

Enfin, le quatrième chapitre, intitulé "Conception et validation d'un réseau radio cognitif sécurisé dédié aux données médicales", est dédié à la description de la plateforme de simulation choisie, à savoir JADE, et à la validation expérimentale de nos contributions. Nous y détaillons les scénarios de simulation, l'initialisation des agents cognitifs, les processus de négociation et de prise de décision multicritère, ainsi que les résultats obtenus, analysés selon plusieurs métriques de performance et de sécurité.

Chapitre 1

La radio cognitive au service de l'E-santé : opportunités et défis

Sommaire

1.1 Introduction

L'essor des technologies sans fil et la multiplication des dispositifs connectés ont entraîné une saturation progressive du spectre radioélectrique. Face à cette problématique, la radio

cognitive apparaît comme une solution innovante permettant une gestion dynamique et intelligente des fréquences. Ce chapitre explore les différentes facettes de cette technologie en commençant par une présentation des réseaux sans fil et leurs classifications. Nous examinerons ensuite la radio logicielle, un élément fondamental de la radio cognitive, avant d'aborder en détail les concepts, principes et architectures des réseaux de radio cognitive. Enfin, nous analyserons l'apport de cette technologie dans le domaine de la e-santé, mettant en lumière son potentiel et les défis qu'elle implique pour améliorer les infrastructures médicales connectées.

1.2 Réseaux sans fil

Les réseaux sans fil représentent un ensemble de technologies qui permettent la communication et l'échange de données entre différents dispositifs électroniques sans nécessiter de connexions filaires physiques. Contrairement aux réseaux câblés traditionnels, qui s'appuient sur des câbles pour transmettre des données, les réseaux sans fil utilisent des ondes radioélectriques pour établir des connexions entre les appareils.

Ces réseaux se caractérisent par leur capacité à fournir une connectivité flexible et à couvrir divers environnements, allant des espaces personnels aux zones géographiques étendues. Les réseaux sans fil permettent aux utilisateurs de se connecter à Internet, d'accéder à des ressources partagées et de communiquer avec d'autres appareils sans être limités par des câbles physiques [1]. Cette liberté de mouvement et cette facilité d'accès sont les principaux avantages qui ont conduit à l'adoption généralisée des technologies sans fil.

Les réseaux sans fil fonctionnent en transmettant des signaux électromagnétiques, généralement des ondes radio, qui transportent des informations sous forme de données numériques. Ces signaux sont émis et reçus par des dispositifs équipés d'antennes, qui convertissent les signaux en informations utilisables, telles que des textes, des images ou des vidéos. La transmission peut se faire sur différentes bandes de fréquence, qui sont régulées par des organismes de réglementation pour éviter les interférences entre les différents utilisateurs du spectre radioélectrique [2].

En résumé, les réseaux sans fil sont des infrastructures de communication basées sur l'utilisation des ondes radio pour permettre une connectivité sans contrainte de câblage physique. Ils jouent un rôle central dans la connectivité moderne, supportant une large gamme d'applications et de services dans divers secteurs, notamment les télécommunications, la santé, les transports, et bien d'autres.

1.2.1 Réseaux sans fil et infrastructures technologiques

Les réseaux sans fil jouent un rôle fondamental dans les technologies modernes en offrant une connectivité flexible, accessible et omniprésente, adaptée aux exigences d'une société de plus en plus dépendante de la connectivité numérique. Leur capacité à faciliter la communication et l'échange de données sans les contraintes des infrastructures filaires est devenue essentielle, en particulier avec la prolifération des dispositifs mobiles tels que les smartphones, tablettes et ordinateurs portables. Ces réseaux permettent aux utilisateurs de se connecter à Internet, d'accéder à des services en ligne et de communiquer librement, indépendamment des restrictions géographiques, transformant ainsi les modes de travail et de

vie quotidienne. En outre, les réseaux sans fil constituent la base de l'Internet des Objets (IoT), une technologie qui interconnecte des milliards d'appareils à travers le monde, allant des objets domestiques intelligents aux systèmes industriels complexes [3]. Cette interconnectivité a permis l'émergence de villes intelligentes et d'infrastructures plus efficaces, stimulant l'innovation dans des secteurs tels que la santé, les transports et l'énergie.

La montée en puissance des réseaux 4G et 5G a renforcé ces tendances, offrant des vitesses de connexion accrues, une latence réduite et la capacité de connecter simultanément un grand nombre d'appareils, ce qui est crucial pour le développement de technologies émergentes telles que les véhicules autonomes et la réalité augmentée et virtuelle. Ces réseaux se sont également révélés essentiels pour l'éducation et le travail à distance, notamment dans le contexte de la pandémie de COVID-19 [4]. Les plateformes de visioconférence, les outils de collaboration en ligne et les ressources éducatives numériques dépendent largement de la connectivité sans fil pour permettre aux étudiants et aux professionnels de poursuivre leurs activités à distance, garantissant ainsi une continuité éducative et professionnelle. Enfin, les réseaux sans fil offrent une adaptabilité remarquable, leur permettant de fonctionner efficacement dans des environnements variés, des zones urbaines densément peuplées aux régions rurales isolées. Cette adaptabilité est cruciale pour réduire les inégalités numériques en fournissant un accès à Internet dans des zones où les infrastructures filaires sont impraticables ou trop coûteuses à déployer. En somme, les réseaux sans fil sont au cœur de l'évolution technologique contemporaine, facilitant l'innovation, l'efficacité et l'interconnexion dans presque tous les aspects de la vie moderne.

1.2.2 Catégories des réseaux sans fil

En fonction de la portée et des débits de transmission, ces réseaux sans fil peuvent évoluer pour répondre à des besoins variés. Par exemple, le WPAN (Wireless Personal Area Network), adapté aux connexions individuelles sur quelques mètres, peut s'étendre à des réseaux WLAN (Wireless Local Area Network), qui offrent une connectivité locale à l'échelle d'un bâtiment ou d'un bureau, voire à des réseaux WWAN (Wireless Wide Area Network), couvrant des zones géographiques plus vastes, comme illustré à la Figure 1.1. Ces différentes technologies, allant du WPAN au WWAN, illustrent la flexibilité et la diversité des solutions sans fil, adaptées à des besoins spécifiques en termes de portée, de débit et d'application [5].

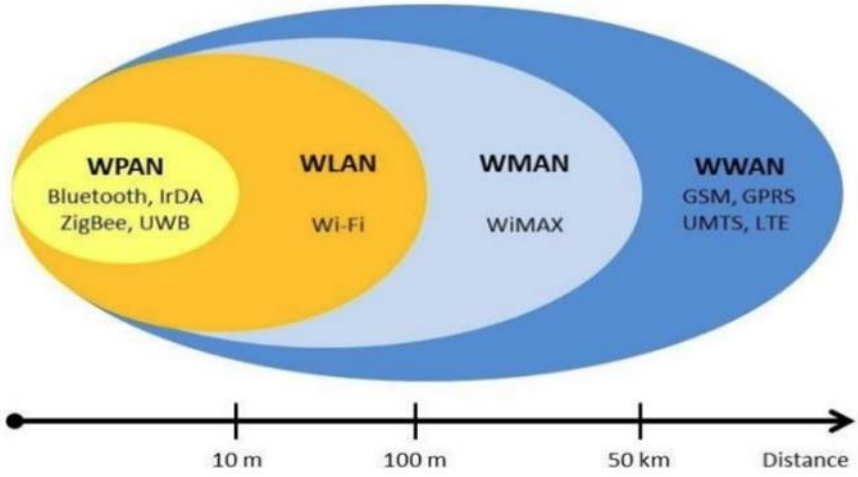


Figure 1.1 : Classification des réseaux sans fil [5].

- **WBAN (Wireless Body Area Network)**

Le WBAN (Wireless Body Area Network) est un réseau sans fil de proximité, installé sur le corps humain ou implanté à l'intérieur. Il est principalement utilisé pour la surveillance des paramètres vitaux (comme la température, le rythme cardiaque, la pression artérielle, etc.) [6]. Ce type de réseau est constitué de plusieurs capteurs interconnectés qui communiquent entre eux grâce à des technologies sans fil telles que Bluetooth (IEEE 802.15.1), ZigBee (IEEE 802.15.4) ou UWB – Ultra Wide Band (IEEE 802.15.3).

Ces capteurs transmettent leurs données à un nœud-maître, un appareil central chargé de recueillir et de traiter les informations. Ensuite, ce nœud-maître envoie les données vers un serveur central via une connexion ADSL (Asymmetric Digital Subscriber Line) pour permettre un suivi à distance, souvent dans un cadre médical.

- **WPAN (Wireless Personal Area Network)**

Les réseaux WPAN (Wireless Personal Area Network), comme leur nom l'indique, sont des réseaux sans fil à portée très limitée (quelques mètres), permettant la communication entre des appareils situés dans le même bureau ou à l'intérieur d'un même domicile. Ces réseaux WPAN font partie de la norme IEEE (Institute of Electrical and Electronics Engineers), spécifiquement dans la famille 802.15. La norme 15.3 est utilisée pour les communications à haut débit, tandis que la norme 15.4 est dédiée aux communications à faible débit. Le Bluetooth, quant à lui, est souvent considéré comme faisant partie de la norme 15.1[7].

- **WLAN (Wireless Local Area Network)**

Les WLAN ont été conçus pour fournir un accès radio à large bande avec des débits atteignant plusieurs Mégabits par seconde, permettant de connecter des équipements tels que des PC et autres dispositifs électroniques ou informatiques dans des environnements professionnels, des bureaux, des bâtiments industriels ou des espaces publics. Ces réseaux se connectent généralement à un réseau principal, comme un réseau Ethernet. Ils sont déployés à la fois dans des lieux privés et dans des espaces publics tels que les gares, les aéroports et les

campus (points d'accès ou hot spots), ainsi que le Wi-Fi (Wireless Fidelity) pour les normes 802.11 (a/b/g/n/ac/ax).

- **WMAN (Wireless Metropolitan Area Network)**

Les WMAN offrent un accès radio à large bande fixe à l'extérieur des bâtiments, en remplacement des réseaux câblés, filaires, optiques ou des connexions ADSL. Leur structure est similaire à celle d'un réseau cellulaire, avec une station de base et une réception via une antenne extérieure au bâtiment. Les WMAN permettent de relier les réseaux WLAN et WPAN situés à l'intérieur du bâtiment, bien que certains protocoles réseau (hors de l'interface radio) puissent assurer une liaison entre la station de base (BS) et les équipements individuels. Les WMAN couvrent une portée de 2 à 50 kilomètres, soit l'étendue d'une ville. Cette technologie est principalement destinée aux opérateurs de télécommunication. Les principales normes associées à ces réseaux sont IEEE 802.16/WiMax (World Wide Interoperability for Microwave Access) et IEEE 802.20/MBWA (Mobile Broadband Wireless Access).

- **WWAN (Wireless Wide Area Network)**

Un WWAN désigne un réseau sans fil couvrant une vaste zone géographique, souvent à l'échelle d'une ville, d'une région ou même d'un pays. Il utilise généralement des technologies cellulaires comme le 3G, 4G, et 5G pour fournir un accès à Internet ou à des services de communication mobile sur de grandes distances. Les WWAN sont utilisés par les opérateurs de télécommunications pour offrir des services de données mobiles aux utilisateurs sur des distances étendues.

- **WRAN (Wireless Regional Area Network)**

Un WRAN est un type de réseau sans fil qui couvre une zone plus large que celle d'un réseau local (WLAN) mais plus petite qu'un réseau métropolitain (WMAN). Les WRAN sont souvent utilisés pour fournir un accès Internet dans des régions rurales ou moins densément peuplées, où les infrastructures filaires traditionnelles sont coûteuses ou difficiles à déployer. Les principales normes associées à ces réseaux sont IEEE 802.22, ils utilisent fréquemment les bandes de fréquences inutilisées, telles que celles du spectre des TV (TV White Spaces), pour offrir un service sans interférer avec les transmissions existantes.

1.3 La radio logicielle

1.3.1 Définition

Le concept de radio logicielle (ou Software-Defined Radio, SDR) a été introduit pour la première fois en 1991 par Joseph Mitola, marquant une étape clé dans l'évolution des technologies radio [8]. Ce terme désigne une classe de radios reprogrammables et reconfigurables capables de modifier leurs fonctionnalités via des changements logiciels, sans nécessiter d'altérations matérielles.

Le principe fondamental de la radio logicielle repose sur la capacité d'un même système matériel à exécuter plusieurs fonctions radio différentes. En d'autres termes, les tâches typiquement réalisées par des circuits matériels, comme la gestion de la fréquence porteuse, la

largeur de bande du signal, la modulation ou encore l'accès au réseau, sont entièrement transférées au logiciel. Cette transition offre une grande flexibilité au système, permettant de l'adapter à un large éventail de réseaux, de protocoles et de techniques de communication radio. Cette flexibilité est essentielle pour répondre à des exigences croissantes en termes de performance, d'interopérabilité et d'adaptabilité entre divers systèmes [9].

La radio logicielle se décline en deux approches principales : la radio idéale et la radio logicielle restreinte. La radio idéale représente un concept théorique où toutes les fonctions radio, de la modulation à la démodulation en passant par la gestion des fréquences, sont entièrement implémentées en logiciel. Ce modèle repose sur un matériel minimaliste, principalement constitué de convertisseurs analogique-numérique (ADC) et numérique-analogique (DAC), associé à une antenne. Bien que cette solution offre une flexibilité totale et une adaptabilité infinie à toutes les bandes de fréquences et standards, elle reste limitée par les contraintes actuelles de traitement numérique et de gestion de l'énergie. En revanche, la radio logicielle restreinte est une version réalisable qui combine des fonctions matérielles dédiées (pour la gestion RF, par exemple) avec des composants programmables, comme les DSP (Digital Signal Processor) ou FPGA (Field Programmable Gate Array), pour le traitement numérique. Elle offre une flexibilité suffisante pour s'adapter à plusieurs standards tout en maintenant une efficacité énergétique et une faisabilité économique, ce qui en fait la solution la plus couramment utilisée dans les applications actuelles.

1.3.2 Architecture

L'architecture des radios logicielles peut être divisée en deux grandes catégories : la radio logicielle idéale et la radio logicielle restreinte (SDR). La radio logicielle idéale est un système entièrement numérique, où tous les processus de réception et d'émission des signaux sont gérés par des composants logiciels, offrant ainsi une grande flexibilité et évolutivité. En revanche, la radio logicielle restreinte combine des éléments matériels dédiés et des fonctions programmables par logiciel. Ce système hybride permet de gérer certaines tâches par des composants matériels, tandis que d'autres, comme le traitement numérique du signal, sont définies par des logiciels, offrant ainsi un compromis entre flexibilité et efficacité.

a) Radio logicielle idéale

Une radio logicielle idéale se compose de plusieurs éléments clés. Elle intègre une ou plusieurs antennes pour capter les signaux radioélectriques, ainsi qu'un système de filtrage RF. Ce filtrage comprend un filtre large bande et, selon le cas, un amplificateur faible bruit (LNA – Low Noise Amplifier) pour la réception ou un amplificateur de puissance pour l'émission. On y trouve également un filtre bande utile, un convertisseur analogique-numérique (CAN) large bande pour le circuit de réception, ou un convertisseur numérique-analogique (CNA) pour le circuit d'émission. Enfin, un processeur de traitement numérique du signal (PTS ou DSP en anglais) est utilisé pour traiter les informations : en réception, il extrait les données utiles via la sélection du canal, la démodulation et le décodage ; en émission, il prépare les informations avec des étapes telles que la modulation et le codage [10]. Le synoptique de la Figure 1.2 illustre l'architecture type d'une radio logicielle idéale.

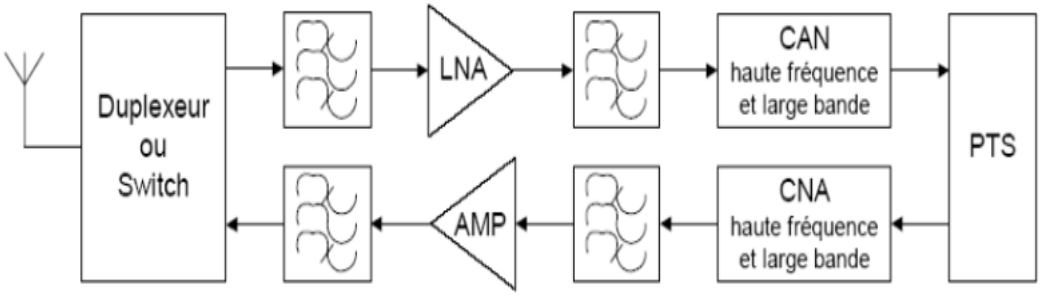


Figure 1.2 : Architecture simplifiée d'une radio logicielle idéale [11].

b) Radio logicielle restreinte

Une radio logicielle restreinte (RLR, ou Software-Defined Radio, SDR) est un système de transmission radio qui combine des composants matériels dédiés et configurables avec des fonctions programmables par logiciel. Ce type de système repose sur une architecture où certaines tâches, telles que le traitement numérique du signal, sont entièrement définies par logiciel, tandis que d'autres, comme la gestion des signaux RF (Radio Fréquence), sont réalisées via du matériel paramétrable. Le schéma de la Figure 1.3 illustre les différents étages de traitement dans une SDR.

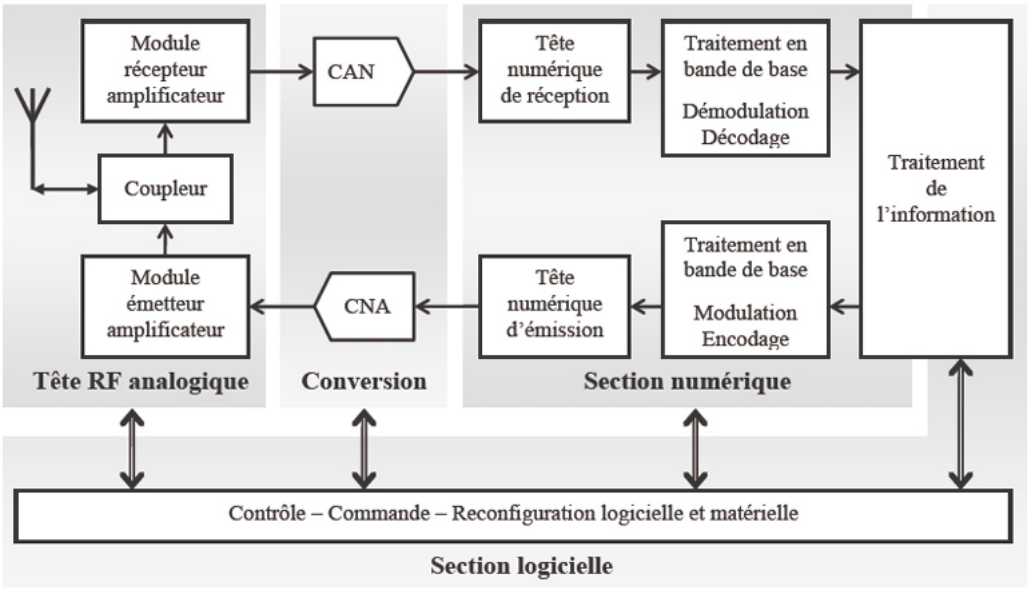


Figure 1.3 : Architecture de radio logicielle restreinte [12].

Cette architecture se décompose en plusieurs composants clés :

- **Tête RF analogique configurable**

La tête RF est responsable de l'acquisition et de la transmission des signaux radiofréquences. Elle comprend plusieurs sous-éléments :

- ✓ *Filtres* : Permettent de sélectionner une bande de fréquences spécifique en bloquant les signaux hors bande.

- ✓ *Coupleurs* : Divisent ou combinent les signaux RF selon les besoins de l'application.
- ✓ *Mélangeurs* : Convertissent un signal RF d'une fréquence à une autre, généralement pour atteindre une fréquence intermédiaire (FI).
- ✓ *Oscillateurs locaux* : Génèrent des fréquences de référence pour le mélangeur, permettant la conversion du signal.
- ✓ *Amplificateurs de puissance* : Augmentent l'amplitude du signal pour garantir une transmission efficace sur de longues distances.
- ✓ *Amplificateurs faible bruit* : Amplifient les signaux faibles reçus tout en minimisant l'introduction de bruit supplémentaire.

- **Étages de conversion analogique-numérique et numérique-analogique (CAN et CNA)**

Ces étages sont essentiels pour le passage entre les domaines analogique et numérique :

- ✓ *Convertisseur analogique-numérique (CAN)* : Échantillonne les signaux RF analogiques reçus et les convertit en données numériques exploitables par les systèmes numériques.
- ✓ *Convertisseur numérique-analogique (CNA) :* Transforme les signaux numériques traités par le processeur en signaux analogiques pour l'émission via l'antenne.

- **Section numérique programmable**

Cette section assure le traitement des signaux numériques après conversion et prépare les données pour l'émission. Elle inclut des fonctions comme :

- ✓ *Mise en forme du spectre :* Adaptation de la largeur de bande et des caractéristiques spectrales du signal.
- ✓ *Adaptation des signaux :* Ajuste les signaux numériques pour correspondre aux spécifications du canal ou du standard de communication utilisé.
- ✓ *Traitement en bande de base :* Effectue des opérations comme la modulation, la démodulation, le filtrage numérique et la correction d'erreurs.

- **Section logicielle de contrôle et de commande**

Cette section supervise l'ensemble des opérations de la radio. Elle est responsable de :

- ✓ *La configuration logicielle :* Détermine les paramètres de fonctionnement des différents composants (par exemple, la fréquence des oscillateurs ou les coefficients des filtres).
- ✓ *Le contrôle des étages :* Assure une coordination efficace entre les composants matériels et les traitements numériques.
- ✓ *La commande des protocoles :* Implémente les règles et les standards de communication pour assurer l'interopérabilité.

1.4 La radio cognitive

1.4.1 Historique

L'expression "radio cognitive" a été introduite par le Dr Joseph Mitola III lors d'un échange de courriels avec Jens Zander et Gerald Q. Maguire. En 1998, Mitola a présenté ce concept lors de son discours de licence à l'Institut Royal de Technologie (KTH). L'année suivante, il a approfondi l'idée de fusionner la technologie sans fil avec l'intelligence computationnelle dans sa thèse de doctorat, définissant ainsi la "radio cognitive" [13]. Mitola envisageait des dispositifs radio et des réseaux capables d'adapter automatiquement leurs paramètres en fonction de l'environnement, grâce à des capacités d'intelligence artificielle. Depuis lors, le concept de radio cognitive a évolué et a été interprété de diverses manières selon les contextes. Le 11 janvier 2010, le centre pour les communications sans fil de l'université d'Oulu a réalisé le premier appel via un réseau de radio cognitive, utilisant un réseau mobile ad hoc assisté par cette technologie [14]. Plus récemment, les avancées en intelligence artificielle ont permis aux radios cognitives de devenir plus intelligentes, promettant un avenir meilleur pour les communications sans fil. En 2025, les systèmes de radio cognitive, assistés par l'IA, devraient être capables de trouver de l'espace pour les signaux dans un environnement spectral de plus en plus encombrer [15].

1.4.2 Définition

Un réseau de radio cognitive se caractérise par l'intégration d'utilisateurs sans fil équipés de radios intelligentes et par l'utilisation de mécanismes d'accès dynamique au spectre. Cette technologie a vu le jour pour répondre aux défis posés par la rareté des fréquences et la saturation des réseaux liés à l'exploitation des bandes spectrales non sous licence. En combinant les capacités des dispositifs de communication intelligents et en tenant compte de ces limitations, le concept de réseau de radio cognitive a été développé pour permettre aux utilisateurs dits secondaires (SUs) d'accéder et de partager des bandes spectrales sous licence avec les utilisateurs d'origine, appelés primaires (PUs), tout en garantissant que leurs performances ne seront pas compromises [16].

Contrairement aux réseaux traditionnels, un réseau de radio cognitive n'a pas de spectre dédié. Il fonctionne en coexistence avec un ou plusieurs réseaux primaires dans les bandes sous licence. Ces réseaux intelligents peuvent exploiter les fréquences disponibles en détectant les transmissions des utilisateurs primaires et en assignant les portions inutilisées, ou « trous spectraux », aux utilisateurs secondaires. Cela permet une utilisation plus efficiente du spectre, tout en minimisant les interférences pour préserver la qualité de service des utilisateurs primaires.

Pour qu'un réseau de radio cognitive puisse fonctionner efficacement, certaines fonctionnalités spécifiques sont intégrées. Ces capacités incluent la détection de l'environnement spectral, l'adaptation dynamique aux conditions réseau et l'attribution intelligente des ressources aux utilisateurs.

1.4.3 Principe et capacités

La radio cognitive est une technologie avancée qui associe les capacités des radios définies par logiciel à des fonctionnalités intelligentes et adaptatives. Elle est conçue pour surveiller, interagir et communiquer avec son environnement en collectant des informations telles que l'état des fréquences radio, sa propre condition interne, sa localisation et les besoins des applications. Grâce à cette conscience environnementale, elle peut modifier en temps réel ses paramètres opérationnels, tels que la fréquence de fonctionnement, le schéma de modulation, la puissance d'émission et la technologie de communication, afin d'optimiser ses performances et d'atteindre ses objectifs de communication.

Un concept clé de la radio cognitive est l'accès dynamique au spectre. Ce principe repose sur la capacité de la radio à détecter en temps réel les portions inutilisées des bandes spectrales sous licence (appelées "trous spectraux") et à les exploiter de manière opportuniste, tout en minimisant les interférences avec les utilisateurs primaires du spectre [17]. Cette approche permet une utilisation plus efficace des ressources spectrales, répondant ainsi à la demande croissante en bande passante pour les services sans fil. La Figure 1.4 illustre comment une radio cognitive identifie et exploite un trou spectral entre deux utilisateurs primaires, tout en garantissant une utilisation efficace et non intrusive du spectre disponible :

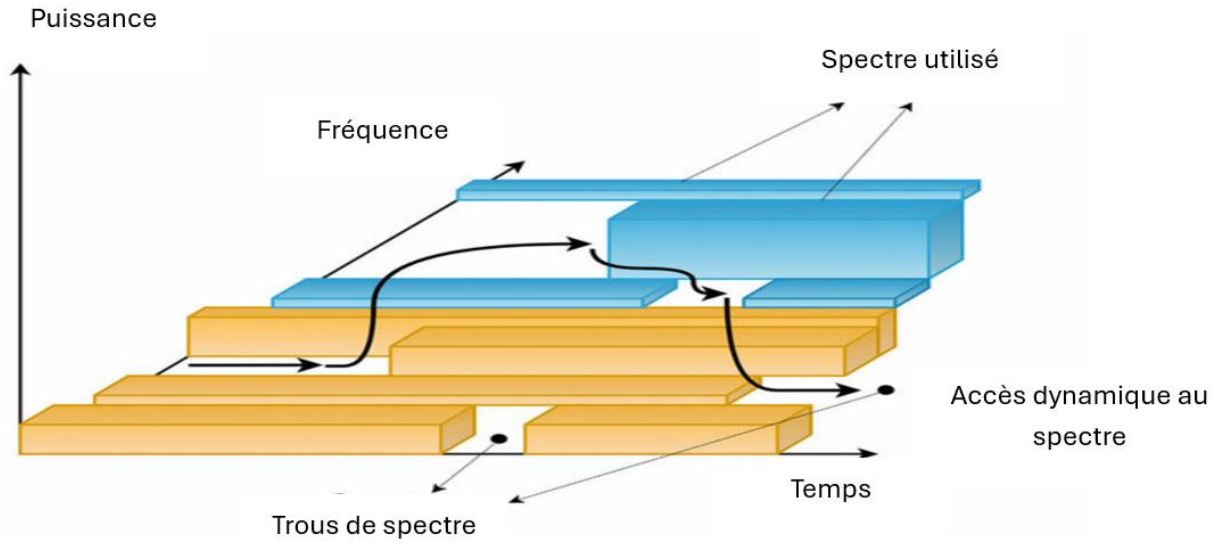


Figure 1.4 : L'accès dynamique au spectre [18].

Les fonctionnalités essentielles de la radio cognitive incluent la détection du spectre, la négociation avec les fournisseurs de services pour obtenir les meilleurs canaux disponibles, et l'adaptation de sa consommation énergétique pour réduire son impact environnemental. Elle doit également être consciente de la localisation des utilisateurs afin de minimiser les interférences entre les utilisateurs primaires et secondaires, et enregistrer les préférences des utilisateurs pour anticiper leurs besoins. La coopération entre radios cognitives est essentielle pour intégrer les informations collectées et exécuter les commandes reçues d'autres dispositifs.

Cependant, l'adoption de la radio cognitive soulève des défis significatifs, notamment en matière de sécurité. Les réseaux de radios cognitives sont vulnérables à des menaces telles que les attaques d'émulation d'utilisateurs primaires, les falsifications de détection, le brouillage et l'écoute clandestine [19]. Ces vulnérabilités peuvent perturber les communications ou compromettre des informations sensibles. Bien que la radio cognitive offre des avantages significatifs en termes d'efficacité spectrale et de flexibilité des communications, il est impératif de surmonter les défis liés à sa sécurité pour garantir des communications fiables et protégées.

1.4.4 Architecture

Avec les avancées de la technologie Radio Cognitive (CR, Cognitive Radio en anglais), les utilisateurs secondaires autorisés (SUs, Secondary Users en anglais) peuvent accéder et exploiter temporairement les portions inutilisées du spectre, même lorsqu'elles sont attribuées à des utilisateurs primaires (PUs, Primary Users en anglais). L'architecture d'un réseau CR est illustrée dans la Figure 1.5 et comprend deux types de réseaux : les réseaux primaires et les réseaux secondaires [20].

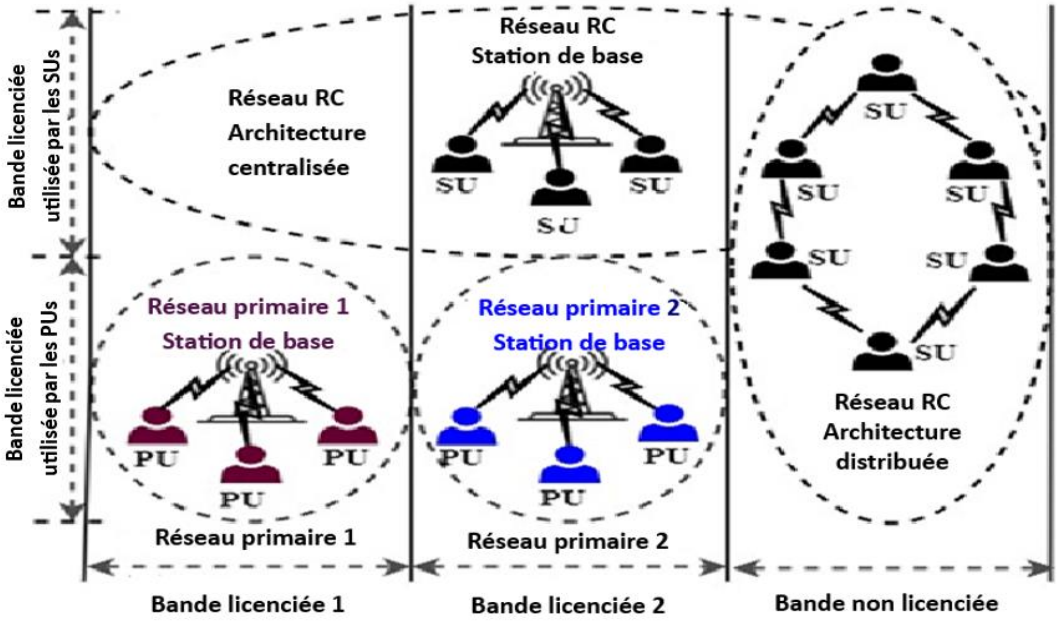


Figure 1.5 : Architecture d'un réseau de radio cognitive [20].

Dans cette architecture, plusieurs PNs (Primary Networks) coexistent au sein de la zone de couverture d'un même réseau CRN (Cognitive Radio Network). Les PNs fonctionnent dans des bandes de fréquences licenciées, appelées réseaux licenciés. Chaque PN regroupe plusieurs utilisateurs, qui ne peuvent accéder qu'aux bandes spectrales spécifiques autorisées pour leur réseau.

En revanche, les SNs (Secondary Networks) sont constitués d'un ensemble d'utilisateurs secondaires (SUs), avec ou sans station de base. Grâce à leur nature non intrusive, les SUs n'interfèrent pas avec les transmissions des PUs. Par conséquent, les PNs imposent des limites strictes sur les opérations des CRNs dans les bandes licenciées, notamment en termes de

puissance maximale, pour garantir que leurs utilisateurs autorisés bénéficient des performances attendues.

De leur côté, les SUs n'ont pas d'autorisation explicite pour utiliser le spectre prédéfini. Toutefois, ils peuvent accéder au spectre licencié de manière opportuniste. En général, cet accès opportuniste est géré par une station de base secondaire, un composant d'infrastructure fixe qui joue le rôle de contrôleur central pour les SNs.

L'architecture des CRNs peut être classée en trois catégories principales :

a) Architecture centralisée

Dans ce type de réseau, une station de base cognitive (CR) joue un rôle central en surveillant les transmissions des utilisateurs secondaires (SUs) sur les bandes spectrales licenciées et non licenciées. Elle recueille les données de détection transmises par divers SUs et prend des décisions optimales concernant la gestion du spectre pour l'ensemble des utilisateurs.

Ces réseaux offrent plusieurs avantages, notamment la réduction des effets d'évanouissement, une efficacité accrue dans la détection du spectre et le support d'une bande passante plus élevée. Cette version améliore la fluidité, met davantage l'accent sur les bénéfices des réseaux et structure l'information de manière claire et concise.

b) *Architecture distribuée*

Les réseaux CRNs distribués fonctionnent sans infrastructure, ce qui signifie qu'ils ne disposent pas de station de base. Ces réseaux sont composés d'un grand nombre d'utilisateurs secondaires (SUs) qui communiquent directement entre eux par des liaisons point à point, en utilisant des bandes spectrales licenciées ou non licenciées.

En l'absence d'une unité de contrôle centralisée, les SUs coopèrent pour prendre des décisions concernant l'accès au spectre, partageant ainsi les opportunités disponibles. Cela nécessite la mise en place d'un processus global permettant de coordonner et de réguler l'accès au spectre.

c) Architecture hybride

L'architecture hybride ou maillée des réseaux radio cognitifs combine les éléments des architectures d'infrastructure et ad hoc, ou encore entre les modèles centralisés et distribués, ce qui la rend similaire aux réseaux sans fil maillés hybrides traditionnels [16].

Dans ce modèle, les fonctionnalités nécessaires pour les réseaux cognitifs radio sont intégrées au sein des entités centrales. Ces entités, qui peuvent être des stations de base ou des points d'accès, agissent comme des routeurs sans fil et peuvent communiquer directement entre elles. Bien qu'elles forment un backbone sans fil, certaines peuvent également se connecter via des liaisons filaires et fonctionner comme des passerelles. Les utilisateurs secondaires peuvent communiquer avec l'entité centrale soit directement via une communication à un seul saut (one-hop), soit en utilisant d'autres utilisateurs secondaires pour une communication multi-sauts (multi-hop).

1.4.5 Cycle de cognition

La cognition est caractérisée par un cycle global qui détaille l'ensemble des réponses adaptatives d'un système. Dans le contexte des radios cognitives, ce cycle leur permet d'atteindre un haut niveau d'autonomie ainsi qu'une capacité de reconfiguration dynamique de leurs paramètres [21]. Ce processus est divisé en plusieurs phases interconnectées : Observation, Orientation, Planification, Décision, et Action, avec un apprentissage continu pour renforcer l'efficacité des décisions futures.

- **Phase d'observation**

Cette phase consiste à détecter et percevoir l'environnement par une collecte de données précises. La radio cognitive analyse des statistiques variées telles que l'emplacement, la température, le niveau de lumière des capteurs, les rapports SNR, le taux d'erreur des paquets, ou encore le temps de parcours. Ces données sont essentielles pour déduire le contexte de communication. La radio cognitive associe les stimuli présents à des expériences antérieures pour identifier des modèles et des tendances au fil du temps. Cette phase est cruciale pour l'acquisition initiale de connaissances et pour nourrir les étapes suivantes du cycle.

- **Phase d'orientation**

La phase d'orientation établit l'importance relative des observations collectées en les reliant à des stimuli connus. Elle fonctionne au sein de structures de données comparables à la mémoire à court terme (STM, Short-Term Memory) et à la mémoire à long terme (LTM, Long-Term Memory), ce qui permet de reconnaître et de classer les stimuli actuels en fonction des expériences passées. Ce processus comprend :

  - ✓ La reconnaissance des stimuli : Identification d'une correspondance entre un stimulus actuel et une expérience antérieure.
  - ✓ La contextualisation : Chaque stimulus est analysé dans un cadre élargi incluant d'autres facteurs externes ou internes (par exemple, le temps ou l'état du système).

Une action immédiate peut être déclenchée dans certains cas critiques, tels qu'une panne d'électricité ou une perte de signal. Ces situations nécessitent des réponses rapides et spécifiques, comme la sauvegarde des données ou la réaffectation des ressources réseau.

- **Phase de planification**

Dans cette phase, la radio cognitive génère des plans d'action pour répondre efficacement aux situations identifiées. Ces plans tiennent compte des priorités établies dans la phase d'orientation et intègrent des réponses réactives (préprogrammées) ou des réactions délibérées basées sur un raisonnement plus approfondi. Par exemple, la réception d'un message réseau pourrait déclencher un processus de planification impliquant le choix optimal d'une interface radio sans fil ou le réglage de paramètres comme la puissance de transmission ou la bande de fréquence.

- **Phase de décision**

La décision est au cœur du processus d'optimisation des performances. À cette étape, le système sélectionne le plan le plus approprié parmi les options disponibles pour maximiser des objectifs définis par l'utilisateur. Ces objectifs incluent des mesures de performance de haut niveau telles que le débit, le retard, la fiabilité, le coût, ou encore la consommation énergétique. La qualité de l'information (Quality of Information, QoI) joue également un rôle clé dans cette sélection. Une radio cognitive peut, par exemple, alerter un utilisateur ou différer une notification selon l'urgence ou les priorités.

- **Phase d'action**

Dans cette phase, la radio cognitive exécute les décisions prises en mobilisant les ressources et effecteurs nécessaires. Cela peut inclure l'envoi de messages dans l'environnement (audio ou autres langages appropriés) ou l'actualisation des modèles internes pour intégrer les nouvelles données. Par exemple, un système peut ajuster ses configurations pour améliorer la qualité de la communication ou enrichir ses modèles internes avec de nouvelles expériences.

- **Phase d'apprentissage**

L'apprentissage est une composante centrale du cycle cognitif, assurant une amélioration continue des décisions et des actions. Cette phase repose sur la perception, les observations, les décisions prises, et les résultats des actions. Elle se déroule initialement lors de la collecte de données dans la phase d'observation, où les perceptions sensorielles sont continuellement comparées aux expériences passées. De nouveaux modèles peuvent être créés en réponse aux résultats obtenus, permettant ainsi au système de tirer des enseignements sur l'efficacité des stratégies adoptées. Par exemple, une radio cognitive peut analyser l'écart entre les états internes antérieurs et actuels pour évaluer l'impact d'un mode de communication et affiner ses choix futurs [22].

Pour une meilleure compréhension de ces concepts, la Figure 1.6 illustre le cycle de cognition détaillé selon Mitola, mettant en évidence toutes les phases et leurs interactions complexes. Ce modèle permet de comprendre comment une radio cognitive s'adapte dynamiquement à son environnement en intégrant des mécanismes avancés d'apprentissage et de décision.

En complément, la Figure 1.7 présente une version simplifiée du cycle de cognition. Cette représentation condensée permet de visualiser les étapes principales du processus tout en restant accessible et didactique.

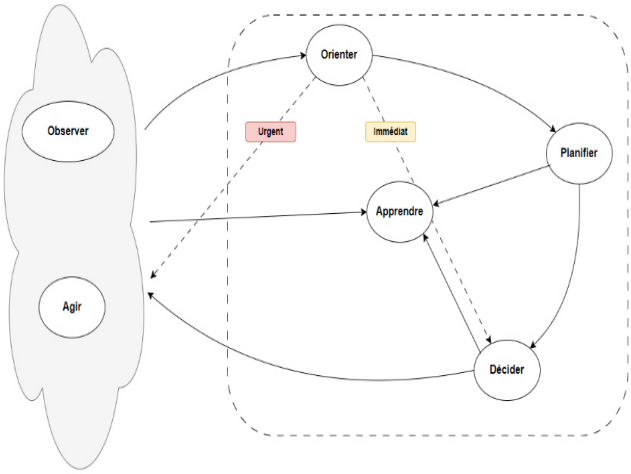


Figure 1.6 : Cycle de cognition.

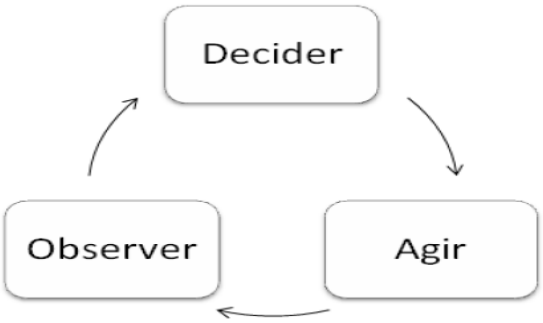


Figure 1.7 : Cycle de cognition simplifié.

1.4.6 Fonctions

Les réseaux radios cognitifs jouent un rôle essentiel dans l'optimisation de l'utilisation du spectre et doivent exécuter les fonctions suivantes :

- **Accès et partage du spectre :** Ils doivent permettre l'accès et le partage de la bande de spectre sous licence avec les réseaux primaires (PU).
- **Observation de l'environnement :** Les réseaux doivent analyser en continu leur environnement pour identifier les opportunités d'utilisation, appelées "trous" ou "lacunes" dans le spectre.
- **Gestion de l'activité des utilisateurs :** En cas d'apparition d'un utilisateur primaire, les utilisateurs secondaires (SU) doivent immédiatement libérer le canal, effectuer un handover spectral et reconfigurer leurs paramètres pour accéder à une nouvelle partie du spectre.

Ces fonctions, qui dépassent les capacités des réseaux classiques, nécessitent l'intégration de fonctionnalités avancées afin que les réseaux radios cognitifs puissent s'adapter dynamiquement à leur environnement radio en modifiant leurs paramètres de communication.

Les principales fonctions des réseaux radios cognitifs sont regroupées en quatre catégories clés, la Figure 1.8 présente ces principales fonctions :

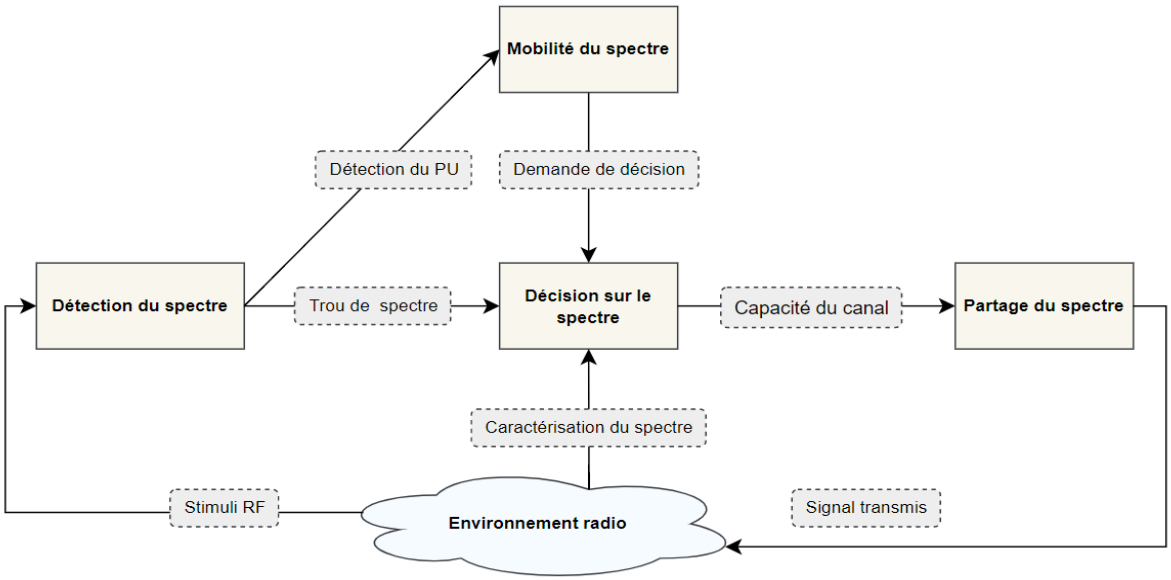


Figure 1.8: Fonctions de la radio cognitive [23].

Une explication détaillée du rôle de chaque fonction permettra une meilleure compréhension de leur importance et de leur fonctionnement :

a) Détection de spectre

La détection de spectre (Spectrum Sensing en anglais) est l'une des fonctions les plus essentielles réalisées par la radio cognitive. Elle permet à la radio cognitive de surveiller son environnement et de détecter tout changement dans celui-ci. Cette fonction consiste à analyser en permanence la bande de spectre sous licence, à collecter des informations, et à identifier les parties inutilisées du spectre, appelées "trous".

Cependant, détecter ces "trous" n'est pas une tâche facile, notamment en raison des difficultés à repérer les transmissions des utilisateurs primaires. De plus, cette détection doit se faire sans provoquer d'interférences avec les transmissions des utilisateurs primaires [24].

Les techniques de détection de spectre sont généralement classées en trois grandes catégories : la détection basée sur l'émetteur, la détection coopérative et la détection fondée sur les interférences.

- **Détection de l'émetteur**

La détection de l'émetteur, aussi appelée détection non-coopérative, permet aux utilisateurs secondaires d'identifier la présence de signaux émis par des utilisateurs primaires. Cette détection repose sur une analyse locale effectuée de manière autonome par les utilisateurs secondaires pour vérifier la présence de tels signaux. La détection de l'émetteur se divise en trois principales catégories [16] :

- ✓ *Détection par filtre adapté :* Considérée comme la méthode la plus efficace pour détecter les signaux des utilisateurs primaires lorsque les utilisateurs secondaires

disposent déjà des caractéristiques du signal transmis. Cette méthode utilise un détecteur optimal conçu pour fonctionner dans un environnement de bruit gaussien stationnaire. Le processus consiste à maximiser le rapport signal sur bruit du signal reçu en associant le filtre adapté avec un signal de référence. Le signal de l'utilisateur primaire est d'abord démodulé, puis analysé par le détecteur de filtre adapté, qui extrait les informations nécessaires pour effectuer la correspondance. L'avantage principal de cette méthode réside dans sa rapidité pour atteindre un gain de traitement élevé grâce à la détection cohérente. Cependant, si les caractéristiques connues du signal de l'utilisateur primaire sont inexactes, la qualité de la détection diminue considérablement.

- ✓ *Détection par énergie :* Également appelée détection non cohérente, cette méthode est utilisée lorsque les utilisateurs secondaires ne disposent pas de suffisamment d'informations sur les caractéristiques du signal des utilisateurs primaires. Elle repose sur la mesure de l'énergie du signal reçu pour déterminer si le canal est libre ou occupé. Le signal est d'abord filtré par un filtre passe-bande, puis le signal de sortie est mis au carré et intégré sur une période d'observation définie. Enfin, le résultat de cette intégration est comparé à un seuil prédéfini pour détecter la présence ou l'absence du signal de l'utilisateur primaire. Bien que cette méthode soit simple à mettre en œuvre, elle présente l'inconvénient majeur de ne pas pouvoir distinguer les signaux des utilisateurs primaires des signaux parasites.
- ✓ *Détection des caractéristiques cyclostationnaires :* Cette méthode nécessite des informations partielles préalables sur les utilisateurs primaires (PUs). Elle exploite la périodicité présente dans l'autocorrélation des signaux modulés et utilise une fonction de corrélation cyclique. Comme le bruit n'est pas corrélé, la méthode s'appuie sur une approche statistique pour différencier le bruit des signaux, ce qui constitue son principal avantage. Toutefois, son principal inconvénient réside dans la complexité des calculs et le temps d'observation prolongé nécessaire à son bon fonctionnement [25].

- **Détection coopérative**

Ce type de détection vise à résoudre le problème de détection erronée qui peut survenir lorsque chaque utilisateur secondaire effectue sa détection de manière indépendante. Au lieu de cela, il collecte les informations provenant de chaque utilisateur secondaire, puis les combine et les corrèle pour prendre la décision correcte quant à la présence ou à l'absence des signaux des utilisateurs primaires. Toutefois, l'inconvénient majeur des techniques de détection coopérative réside dans la charge supplémentaire qu'elles imposent au réseau, car les utilisateurs secondaires doivent coopérer pour réaliser cette détection, ce qui affecte les ressources du réseau. Les techniques de détection coopérative peuvent être classées selon qu'elles fonctionnent de manière centralisée ou distribuée [24].

- **Détection basée sur l'interférence**

Ce modèle, proposé par la Commission fédérale des communications des États-Unis (FCC), vise principalement à mesurer et contrôler l'interférence. Il garantit que l'interférence entre les utilisateurs primaires et secondaires ne dépasse pas une limite de température d'interférence définie. Le but est que le niveau de puissance reçu soit aussi proche que possible du niveau de bruit de fond [26]. Il est à noter que ce niveau de bruit peut varier en fonction de

l'aire de service. Le principal défi de ce modèle réside dans la détermination précise de la limite de température d'interférence.

b) Gestion du spectre

La gestion de spectre (Spectrum management en anglais) concerne l'analyse des bandes de spectre disponibles et la prise de décision sur l'utilisation de celles-ci. Elle consiste à choisir une bande de fréquence importante parmi les options disponibles, après quoi les utilisateurs secondaires (SU) décident s'ils doivent l'exploiter ou non. Diverses méthodes d'optimisation peuvent être employées pour prendre des décisions optimales en fonction des conditions environnementales [27]. Cela inclut des éléments comme la caractérisation du spectre, la sélection du spectre, les protocoles de routage, la reconfiguration, le délai de transmission [28], et la fréquence de fonctionnement. Les trous dans le spectre sont définis à travers plusieurs paramètres, tels que l'interférence du canal, le nombre d'utilisateurs primaires (PU), la perte de signal et la puissance du signal reçu. La sélection du canal est une tâche complexe dans les réseaux de radio cognitive en raison des multiples combinaisons possibles entre les spectres et les itinéraires entre la source et la destination. Il est nécessaire de reconfigurer les paramètres de transmission et les protocoles de routage pour prendre des décisions optimales de spectre dans ces réseaux.

c) Partage du spectre

Le partage de spectre (Spectrum Sharing en anglais) est essentiel pour coordonner l'accès des nombreux utilisateurs secondaires à la bande de fréquence détectée. Cette fonction divise la bande de spectre disponible entre les utilisateurs secondaires via des techniques de planification, similaires au protocole MAC dans les réseaux classiques, mais avec des défis uniques aux réseaux de radio cognitive. Ces défis incluent la nature dynamique du spectre disponible et la coexistence des utilisateurs primaires et secondaires [29].

Les techniques de partage de spectre sont classées selon plusieurs critères : technique, architecture, comportement d'allocation, champ d'application et temps d'accès au spectre.

- **Classification basée sur la technique d'accès au spectre**

Les protocoles de contrôle d'accès au média (MAC, Media Access Control address) dans les réseaux de radio cognitive se divisent en trois catégories selon la méthode d'accès :

- ✓ *Accès aléatoire :* Les utilisateurs n'ont pas besoin de synchronisation avec le réseau, et ces protocoles utilisent souvent le CSMA/CA (Carrier sense multiple access/collision avoidance) pour éviter les collisions.
- ✓ *Créneaux temporels :* Nécessitent une synchronisation ; le temps est divisé en créneaux dédiés au contrôle ou à la transmission de données.
- ✓ *Hybrides :* Combinent les deux approches, par exemple en utilisant les créneaux temporels pour le contrôle et l'accès aléatoire pour les données.

- **Classification basée sur l'architecture du réseau**

Les protocoles MAC des réseaux de radio cognitive peuvent être classés en fonction de l'architecture du réseau :

- ✓ *Protocoles centralisés :* Une entité centrale, telle qu'une station de base, gère l'accès et l'allocation du spectre en analysant les besoins des utilisateurs secondaires et les paramètres des canaux disponibles.
- ✓ *Protocoles distribués :* Sans infrastructure centrale, chaque utilisateur secondaire gère indépendamment l'accès et l'allocation du spectre, adaptés aux réseaux ad hoc sans infrastructure.

- **Classification basée sur le comportement d'allocation du spectre**

Les protocoles MAC des réseaux de radio cognitive peuvent être classés selon le comportement d'allocation du spectre en deux catégories :

- ✓ *Protocoles MAC coopératifs :* Chaque nœud partage ses mesures d'interférences avec les autres, souvent au sein de clusters réseau, avec des processus centralisés ou décentralisés pour une gestion collective.
- ✓ *Protocoles MAC non coopératifs :* Ces protocoles sont égoïstes, car chaque nœud prend en compte uniquement ses propres besoins sans se soucier des interférences des autres nœuds.

- **Classification basée sur le champ d'application**

Les protocoles MAC des réseaux de radio cognitive peuvent être classés en fonction du champ d'application en deux types :

- ✓ *Intranetwork MAC :* Ils distribuent le spectre parmi les utilisateurs secondaires au sein d'un seul réseau de radio cognitive.
- ✓ *Internetwork MAC :* Ils permettent à plusieurs réseaux de radio cognitive d'allouer le spectre et de gérer les chevauchements entre eux, en tenant compte des politiques des différents opérateurs.

- **Classification basée sur la technologie d'accès au spectre**

Les protocoles MAC des réseaux de radio cognitive peuvent être classés en deux types selon la technologie d'accès au spectre :

- ✓ *Overlay MAC :* Les utilisateurs secondaires exploitent les parties inutilisées de la bande de spectre primaire, avec peu d'interférence pour les utilisateurs primaires. En cas de présence d'un utilisateur primaire, ils doivent immédiatement libérer le canal.
- ✓ *Underlay MAC :* Les utilisateurs secondaires transmettent simultanément avec le spectre primaire, mais à faible puissance, de manière à être perçus comme du bruit par les utilisateurs primaires. Bien que cela améliore l'utilisation du spectre, il nécessite des techniques complexes de spectre étendu [16].

d) Mobilité du spectre

La mobilité du spectre (Spectrum Mobility en anglais) désigne le processus permettant à un utilisateur de radio cognitive (RC) de changer de fréquence d'exploitation. Les réseaux de radio cognitive optimisent l'utilisation du spectre de manière dynamique en permettant aux terminaux radio de fonctionner sur la meilleure bande de fréquence disponible, tout en garantissant une transition fluide et continue pour répondre aux exigences de communication.

- **Recherche des bandes de fréquence optimales**

La radio cognitive doit surveiller en permanence les bandes de fréquence disponibles afin de permettre un basculement immédiat vers une autre bande en cas de besoin.

- **Auto-coexistence et synchronisation**

Lorsqu'un utilisateur secondaire effectue un transfert de spectre, deux aspects essentiels doivent être pris en compte :

- ✓ Le canal cible ne doit pas déjà être occupé par un autre utilisateur secondaire.
- ✓ Le récepteur correspondant de la liaison secondaire doit être informé pour éviter toute interférence avec le spectre [30].

1.4.7 Domaines d'application

Les réseaux radio cognitifs trouvent leur utilité dans divers domaines de communication sans fil, offrant des solutions innovantes et efficaces. Cette section présente une brève explication des principales applications de la radio cognitive, en mettant l'accent sur les scénarios les plus pertinents et essentiels où son utilisation est particulièrement nécessaire.

- **Réseaux militaires :** Les réseaux militaires représentent l'une des applications les plus cruciales de la radio cognitive. En raison de la sensibilité des données transmises, il est difficile de les protéger efficacement contre le brouillage ou les tentatives de piratage. Pour répondre à ce défi, les forces armées adoptent les réseaux cognitifs radios, reconnus pour leur flexibilité à fonctionner sur différentes bandes de fréquences. À titre d'exemple, le département de la Défense des États-Unis a développé des systèmes utilisant ces techniques, comme le système radio SPEAKeas [31].
- **Services de santé (eHealth) :** Divers types de technologies sans fil sont utilisés dans les services de santé pour améliorer l'efficacité des soins aux patients et la gestion des services de santé. L'indépendance des patients, rendue possible par des réseaux mobiles tels que les WBAN (Wireless Body Area Networks), devient une réalité. Cependant, la nécessité pour les personnes à risque d'être constamment connectées pour un diagnostic peut poser un défi. La radio cognitive (RC) permet de résoudre ce problème en sélectionnant le spectre optimal, compatible avec les exigences spécifiques de ces services [32].
- **Réseaux de secours et d'urgence :** Lors de catastrophes telles que des tremblements de terre, des ouragans, des incendies de forêt ou d'autres accidents majeurs comme des accidents miniers, les réseaux peuvent subir des pannes partielles ou complètes. Dans ces situations d'urgence, la principale difficulté réside dans l'attribution d'un réseau capable d'envoyer et de recevoir des informations essentielles. Les réseaux de radio cognitive offrent une solution pour établir ces réseaux d'urgence. Ils permettent à ces derniers d'accéder au spectre sous licence de manière opportuniste, assurant ainsi une bande passante suffisante pour la transmission d'informations critiques et fiables [31].
- **Réseaux cellulaires :** L'approche des réseaux cognitifs radios a été intégrée dans les réseaux cellulaires pour résoudre des problèmes tels que la couverture intérieure et l'augmentation constante du trafic de communication. En utilisant des femtocells associées aux réseaux cognitifs radios, une femtocell analyse la bande de spectre pour identifier les "trous" dans le

spectre, garantissant ainsi une couverture optimale tout en évitant les interférences avec d'autres cellules, qu'elles soient des femtocells ou des macrocells.

- **Réseaux de sécurité publique :** Les policiers, pompiers et secouristes dépendent des réseaux de sécurité publique pour assurer leurs communications, notamment lors d'interventions d'urgence. Étant donné la criticité de ces transmissions pour la sécurité et la coordination des équipes, il est essentiel que ces réseaux ne soient jamais confrontés à un manque de spectre. Pour répondre à ce besoin, les réseaux de sécurité publique peuvent intégrer les réseaux cognitifs radios, qui permettent un accès opportuniste à une large portion du spectre sous licence. Cette approche garantit une bande passante suffisante, même en cas de forte demande, assurant ainsi des communications fiables et continues dans des situations critiques.

1.5 Radio cognitive et e-santé

Dans le domaine de la santé numérique, la qualité des communications sans fil joue un rôle crucial pour assurer une prise en charge efficace des patients. La radio cognitive se distingue comme une technologie clé grâce à sa capacité à optimiser l'utilisation du spectre radioélectrique. Elle permet aux réseaux de s'ajuster en temps réel en repérant les fréquences libres et en les attribuant aux services médicaux, garantissant ainsi une transmission plus fluide des données.

Avec la multiplication des objets connectés en santé, tels que les dispositifs de suivi des patients et les systèmes de télésurveillance, la gestion intelligente du spectre devient essentielle. La radio cognitive améliore l'échange d'informations entre ces appareils et les infrastructures de santé, même dans des environnements où la disponibilité des fréquences est restreinte.

Grâce à cette flexibilité, les établissements de santé peuvent bénéficier de réseaux plus adaptatifs. En cas d'urgence, cette technologie permet de réorganiser l'attribution des fréquences pour garantir la priorité aux communications critiques, comme celles entre les équipes médicales et les services d'intervention.

Par ailleurs, l'intégration de la radio cognitive avec les réseaux 5G et les équipements médicaux connectés favorise des échanges de données plus rapides et plus fiables entre les différents acteurs de la santé. Cela contribue au développement d'hôpitaux intelligents et de solutions de soins à distance plus performantes, renforçant ainsi l'efficacité et la réactivité du système de santé.

1.5.1 Définition et évolution de la e-santé

La e-santé, également appelée santé numérique, désigne l'ensemble des technologies de l'information utilisées dans le domaine de la santé. Cela comprend des outils tels que les dossiers médicaux numériques, la télémédecine, les objets connectés pour le suivi de la santé, les applications mobiles spécialisées, ainsi que l'utilisation des données et l'intelligence artificielle pour améliorer la qualité des soins. Son but est d'améliorer la prise en charge des patients, de faciliter les tâches des professionnels de santé et d'optimiser la gestion des établissements médicaux grâce aux avancées technologiques [33].

L'évolution de la e-santé a suivi les progrès technologiques majeurs. Dans les années 1960 à 1980, l'informatisation des hôpitaux a permis une gestion plus fluide des dossiers des patients et une organisation des soins plus efficace. L'apparition d'Internet dans les années 1990-2000 a été un moteur pour le développement de la télémédecine et des logiciels de gestion des dossiers médicaux, permettant un accès plus rapide et sécurisé aux informations de santé [34]. C'est à cette époque que les échanges à distance entre médecins et patients ont commencé à se développer, ouvrant la voie à une médecine plus connectée.

Au début des années 2010, l'arrivée des smartphones et des objets connectés a profondément transformé le secteur. De nouvelles applications ont permis aux patients de suivre leurs signes vitaux, tandis que les dispositifs médicaux intelligents ont facilité le suivi à distance des maladies chroniques. Ces innovations ont permis aux patients de jouer un rôle plus actif dans la gestion de leur santé, tout en offrant aux professionnels une surveillance plus précise, même à distance. De plus, les hôpitaux ont intégré des technologies connectées, permettant une surveillance améliorée des patients et une réactivité accrue des équipes médicales [35].

Aujourd'hui, la e-santé repose sur des technologies avancées telles que l'intelligence artificielle et l'analyse des big data. Ces outils permettent de rendre les diagnostics plus précis, de personnaliser les traitements et de détecter certaines pathologies à un stade précoce. L'intelligence artificielle est particulièrement utilisée pour l'analyse des images médicales, l'assistance à la décision clinique et la prévention des maladies. La médecine prédictive, qui permet d'anticiper les risques de santé avant même l'apparition des symptômes, est également en plein développement, offrant une approche plus préventive et adaptée aux besoins individuels des patients [35].

Avec l'essor des réseaux 5G et des infrastructures numériques, la e-santé se dirige vers un système de santé totalement interconnecté, dans lequel les informations circulent en temps réel entre les différents acteurs médicaux. La télémédecine, qui a gagné en importance notamment après la crise de la COVID-19, continue d'élargir l'accès aux soins et de réduire la pression sur les établissements de santé. Parallèlement, des hôpitaux dits "intelligents" apparaissent, utilisant les technologies les plus récentes pour améliorer l'organisation des soins et l'expérience des patients [36]. La e-santé aide aussi les individus à devenir plus autonomes dans la gestion de leur santé, grâce aux dispositifs connectés et aux plateformes numériques qui offrent un suivi personnalisé et une meilleure prévention des maladies.

En somme, la e-santé transforme de manière significative le secteur médical en rendant les soins plus accessibles, efficaces et mieux adaptés aux besoins des patients. Alimentée par des innovations technologiques continues, elle ouvre la voie à une médecine de plus en plus connectée, préventive et sur-mesure, garantissant une prise en charge optimale et une amélioration continue de la santé publique. La Figure 1.9 présente les principales composantes des systèmes de e-santé.

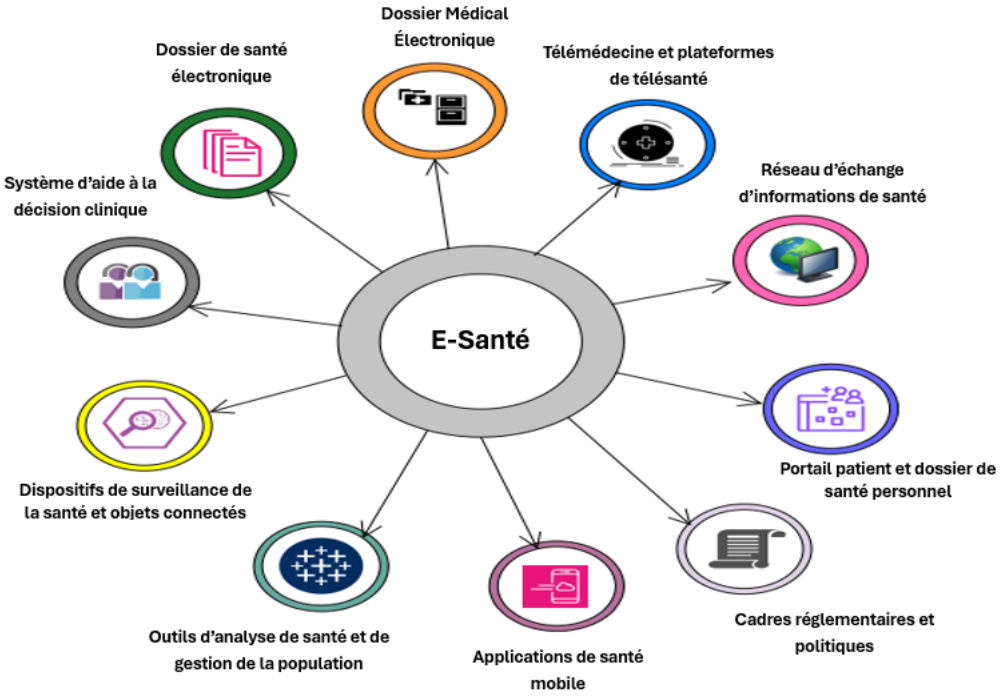


Figure 1.9 : Les principales composantes des systèmes de e-santé [37].

1.5.2 Contraintes et défis des réseaux en e-santé

Avec l'évolution constante des technologies de communication mobile, notamment les générations successives telles que la 3G, la 4G et plus récemment la 5G, l'amélioration des performances réseau reste un enjeu majeur pour les applications de télémédecine. Malgré les débits élevés promis par ces réseaux récents, des défis persistent, notamment en raison de la disparité de la couverture dans certaines zones (bâtiments, régions isolées, etc.) et de l'instabilité des débits en fonction des conditions environnementales et de la congestion du réseau.

Les infrastructures et protocoles actuels des réseaux traditionnels ne sont pas entièrement conçus pour s'adapter en temps réel aux contraintes dynamiques des environnements médicaux. L'allocation de la bande passante reste rigide**,** une fois établie en début de communication, elle ne peut être ajustée dynamiquement selon les variations de la qualité de service (QoS). Cette limitation impacte considérablement les services de télémédecine nécessitant une faible latence et une transmission fiable des données en temps réel, tels que la téléassistance, la téléconsultation, le télé monitoring et le télédiagnostic. L'instabilité des connexions peut entraîner des délais excessifs et compromettre la qualité des soins à distance.

De plus, le coût élevé des bandes de fréquence GSM représente un autre défi, étant donné le volume croissant de données médicales générées et transmises dans les systèmes de santé connectés. Face à ces contraintes, la Radio Cognitive apparaît comme une solution prometteuse pour optimiser la gestion des ressources spectrales et améliorer la connectivité en e-santé.

1.5.3 Apports de la radio cognitive en e-santé

L'intégration de la Radio Cognitive dans les communications médicales constitue une avancée majeure pour l'e-santé, permettant d'optimiser la gestion des ressources spectrales et d'améliorer la transmission des données. Contrairement aux réseaux traditionnels à allocation statique, elle exploite dynamiquement les fréquences sous-utilisées, garantissant ainsi une meilleure qualité de service (QoS) et réduisant la congestion du réseau.

Cette technologie s'adapte aux conditions de transmission en temps réel, améliorant la couverture réseau et la stabilité des débits, notamment dans les zones reculées ou mal desservies [38]. Elle permet également d'assurer une connectivité fiable pour les dispositifs médicaux connectés, essentiels au suivi des patients à distance. En télémédecine, elle favorise des consultations fluides et sans interruption, réduisant la latence et améliorant l'expérience utilisateur.

Dans le domaine du télémonitoring, la Radio Cognitive garantit une transmission continue et stable des données vitales, évitant les pertes critiques. Elle joue aussi un rôle clé dans les interventions médicales à distance en assurant une communication instantanée et sécurisée.

L'évolution vers la 5G et la 6G renforcera encore ses performances, favorisant l'interopérabilité entre les équipements médicaux et les plateformes numériques [39]. Cette technologie représente une solution efficace aux défis des réseaux médicaux, rendant les soins à distance plus accessibles, fiables et performants. Son déploiement progressif annonce une transformation profonde de l'e-santé, en garantissant une prise en charge optimisée des patients, indépendamment des contraintes géographiques ou techniques.

1.5.4 La radio cognitive dans les infrastructures réseaux de e-santé

La radio cognitive permet aux équipements médicaux de sonder l'environnement radio et d'identifier en temps réel les bandes de fréquences inutilisées afin de les exploiter de manière opportuniste. Cette capacité d'adaptation permet non seulement de contourner les problèmes de congestion réseau, mais aussi d'assurer une meilleure continuité des services critiques tels que la téléconsultation, la télémédecine, la télémonitoring et l'ambulance connectée.

Dans une infrastructure e-santé intégrant la radio cognitive, les équipements médicaux intelligents (capteurs, moniteurs de signes vitaux, dispositifs implantables) sont dotés de modules radio permettant de communiquer avec des stations de base radio cognitives. Ces stations de base assurent la gestion dynamique du spectre, optimisant ainsi l'allocation des ressources en fonction des priorités des données transmises. Par exemple, les transmissions urgentes (données de surveillance cardiaque en temps réel) bénéficient d'une priorité élevée avec une bande passante garantie, tandis que les transmissions périodiques (stockage des dossiers médicaux) peuvent s'adapter aux disponibilités spectrales sans impacter la qualité du service.

Une autre application prometteuse est l'intégration des réseaux de capteurs médicaux (WBAN, WPAN) à des infrastructures de radio cognitive. Ces capteurs collectent les paramètres physiologiques des patients et les transmettent vers des plateformes de suivi médical. Grâce à

la radio cognitive, ces données peuvent être acheminées via plusieurs technologies d'accès (Wi-Fi, GSM (Global System for Mobile communication), 5G, WiMAX) selon la disponibilité et la qualité du réseau, garantissant ainsi une continuité de service optimale, même en mobilité.

Les infrastructures de santé intelligentes peuvent également tirer parti de la radio cognitive pour optimiser l'utilisation des réseaux hétérogènes. Un hôpital équipé de cette technologie pourrait gérer de manière plus efficace les communications internes entre le personnel médical, les dispositifs médicaux et les plateformes de stockage, réduisant ainsi les risques de saturation du réseau et améliorant l'efficacité des soins.

Toutefois, malgré son potentiel, l'adoption de la radio cognitive dans la e-santé soulève encore certains défis. Les questions de sécurité et de confidentialité des données médicales doivent être rigoureusement adressées, notamment en ce qui concerne les risques d'interférences et d'intrusions dans les communications sensibles. De plus, la gestion de l'énergie pour les dispositifs médicaux embarqués et la compatibilité avec les infrastructures réseau existantes nécessitent des solutions adaptées pour assurer un fonctionnement optimal.

En somme, la radio cognitive constitue une avancée majeure pour l'amélioration des infrastructures réseaux en e-santé, en apportant des solutions aux problématiques de saturation, d'optimisation du spectre et de connectivité adaptative. En permettant une communication plus flexible et efficace, elle ouvre la voie à un système de santé plus intelligent, interconnecté et accessible, capable de répondre aux exigences croissantes des services médicaux modernes [40].

1.6 Conclusion

La radio cognitive constitue une avancée majeure dans l'optimisation de l'usage du spectre radioélectrique, offrant une flexibilité et une adaptabilité accrues aux réseaux sans fil. Grâce à son intelligence et à sa capacité à s'adapter en temps réel aux conditions du spectre, elle permet d'améliorer l'efficacité des communications et de garantir une meilleure coexistence des différents systèmes radio. Son application dans le domaine de la e-santé ouvre des perspectives prometteuses pour la télémédecine et la surveillance médicale, bien que des défis techniques et réglementaires subsistent. En définitive, la radio cognitive s'impose comme une technologie clé pour l'avenir des communications sans fil, avec un impact considérable sur de nombreux secteurs, notamment la santé, les télécommunications et l'Internet des objets (IoT).

Le chapitre suivant sera dédié à la sécurité de cette technologie afin de pouvoir sécuriser nos données circulant dans les Réseaux Radio Cognitive.

Chapitre 2

Sécurité dans les réseaux radio cognitifs

Sommaire

2.1 Introduction

La sécurité des réseaux radio cognitifs est un enjeu majeur en raison de leur architecture décentralisée et de leur gestion dynamique du spectre. Ces réseaux, bien que flexibles et efficaces, sont vulnérables à diverses menaces, nécessitant des solutions adaptées pour protéger les données qui y circulent. Ce chapitre explore les aspects essentiels de la sécurité dans les CRN, en abordant les exigences de sécurité, les techniques de chiffrement et la cryptographie utilisées pour assurer la confidentialité et l'intégrité des données.

Il met en lumière les vulnérabilités spécifiques des CRN, les menaces potentielles sur les différentes couches de ces réseaux, ainsi que les types d'attaques auxquels ils peuvent être exposés. Un focus particulier est donné à la sécurité des données médicales, qui requiert des protocoles et des normes rigoureux pour garantir la protection des informations sensibles dans les applications de santé. L'analyse des solutions de sécurité et des mesures de protection existantes met en évidence les défis actuels et les avancées nécessaires pour renforcer la sécurité dans ces réseaux complexes.

2.2 Concepts fondamentaux de la sécurité

La sécurité informatique vise à protéger les systèmes, les réseaux et les données contre les accès non autorisés, les altérations et les destructions. Elle repose sur plusieurs principes fondamentaux qui permettent d'assurer la fiabilité des informations et des infrastructures numériques.

2.2.1 Les exigences de sécurité

Les exigences de sécurité dans les réseaux radio cognitifs peuvent varier en fonction des environnements d'application, mais certaines exigences fondamentales restent communes pour garantir un contrôle de sécurité robuste et efficace. Les principales exigences de sécurité dans les CRN sont les suivantes :

- **Contrôle d'accès** : Il s'agit d'une exigence fondamentale qui limite l'utilisation des ressources du réseau aux seules entités autorisées, empêchant ainsi toute tentative d'accès non autorisé.
- **Confidentialité** : Elle assure que seules les personnes ou dispositifs autorisés peuvent consulter les informations échangées au sein du réseau, prévenant toute divulgation involontaire ou malveillante.
- **Authentification** : Cette exigence permet de s'assurer que seules les entités dont l'identité a été vérifiée peuvent participer aux communications, empêchant ainsi toute usurpation d'identité ou intervention d'acteurs non autorisés.
- **Intégrité** : L'intégrité garantit que les données transmises restent exactes et complètes tout au long du processus de communication, sans qu'aucune modification non autorisée ne soit effectuée.

- **Non-répudiation** : Elle empêche les utilisateurs d'annuler ou de nier une action effectuée ou un message envoyé, offrant ainsi une preuve fiable des interactions réalisées au sein du réseau.
- **Détection et prévention des intrusions** : Essentielle dans un environnement dynamique comme les CRN, elle permet d'identifier rapidement les comportements suspects et de réagir efficacement pour protéger le réseau contre les menaces potentielles.
- **Disponibilité** : Elle veille à ce que les services du réseau restent accessibles et opérationnels en tout temps, même en présence de défaillances ou de tentatives d'attaques.
- **Résilience** : La résilience assure que le réseau peut résister et s'adapter face aux menaces, en maintenant son fonctionnement malgré les perturbations.

2.2.2 Chiffrement et cryptographie

La cryptographie est une discipline essentielle dans le domaine de la sécurité de l'information. Elle permet de protéger les données contre les accès non autorisés en les transformant grâce à des techniques de chiffrement. L'objectif principal de la cryptographie est d'assurer la confidentialité, l'intégrité et l'authenticité des informations échangées, notamment dans les communications numériques.

Le chiffrement, qui est une application concrète de la cryptographie, repose sur l'utilisation d'algorithmes permettant de convertir un message en clair en un message chiffré, illisible sans une clé appropriée. Il existe deux grandes catégories de chiffrement : le chiffrement symétrique et le chiffrement asymétrique. Chacun de ces systèmes possède des caractéristiques spécifiques et est utilisé en fonction des exigences de sécurité et de performance.

2.2.3 Algorithmes de chiffrement symétrique

Le chiffrement symétrique, également connu sous le nom de chiffrement à clé privée, est une méthode de cryptographie où une même clé est utilisée à la fois pour le chiffrement et le déchiffrement des données.

Dans ce processus, l'expéditeur applique un algorithme de chiffrement au texte en clair (données d'origine) en utilisant une clé secrète, puis transmet le message chiffré au destinataire. Pour retrouver les informations initiales, le destinataire doit utiliser la même clé secrète et l'algorithme de déchiffrement correspondant afin de reconstituer un texte lisible.

Ainsi, dans un système de chiffrement symétrique, l'expéditeur et le destinataire doivent disposer de la clé secrète avant l'échange des données, garantissant ainsi la protection des informations transmises.

Les algorithmes de chiffrement symétrique possèdent trois caractéristiques principales :

- ✓ Gestion simplifiée des clés : Comme une seule clé est utilisée pour le chiffrement et le déchiffrement, leur gestion est plus simple par rapport aux méthodes asymétriques.

- ✓ Efficacité et rapidité : Ces algorithmes nécessitent peu de ressources de calcul, permettant ainsi un traitement rapide et efficace des données, ce qui les rend particulièrement adaptés aux volumes de données importants.
- ✓ Polyvalence : Grâce à leur rapidité et leur efficacité, ces algorithmes conviennent à différents contextes d'utilisation, notamment lorsque des performances élevées sont requises.

Les algorithmes de chiffrement symétrique les plus connus incluent le DES (Data Encryption Standard), le Triple DES et l'AES (Advanced Encryption Standard), qui sont largement utilisés pour assurer la sécurité des communications et des données.

a) Data Encryption Standard

Le DES est un algorithme de chiffrement fonctionnant par blocs de 64 bits. Il repose sur un même algorithme pour réaliser à la fois le chiffrement et le déchiffrement des données.

Cet algorithme est apprécié pour sa rapidité d'exécution et sa faible consommation de ressources. Toutefois, son niveau de sécurité est limité, ce qui le rend moins adapté aux environnements nécessitant une protection avancée. Il est souvent utilisé pour le traitement de volumes importants de données [1].

b) Triple Data Encryption Algorithm

Le 3DES est une amélioration du chiffrement DES, qui applique trois fois de suite l'algorithme sur chaque bloc de données pour renforcer la sécurité. Avec l'augmentation des capacités de calcul des ordinateurs, la clé utilisée dans le DES classique est devenue vulnérable aux attaques par force brute. Pour pallier cette faiblesse, le 3DES a été développé en allongeant la clé de chiffrement à 112 bits, ce qui réduit le risque d'attaques similaires.

Bien que 3DES offre une meilleure protection que DES, il présente des inconvénients : il est plus lent et consomme davantage de ressources. Pour cette raison, son utilisation est généralement réservée au chiffrement de petites quantités de données sensibles.

Malgré ses avantages, le chiffrement symétrique présente certaines faiblesses, ce qui le rend inadapté à certaines applications.

- Risque lié au partage de la clé secrète : dans le chiffrement symétrique, la même clé est utilisée pour chiffrer et déchiffrer les données. Cela signifie que si un pirate informatique parvient à intercepter cette clé, que ce soit du côté de l'expéditeur ou du destinataire, l'ensemble de la communication devient compromis. L'attaquant pourrait alors lire et modifier les messages sans être détecté.
- Difficulté de gestion des clés : la gestion des clés secrètes est complexe, surtout lorsque plusieurs utilisateurs doivent communiquer de manière sécurisée. Chaque nouvelle paire d'utilisateurs doit générer et conserver une clé unique. Plus le nombre d'échanges sécurisés augmente, plus le nombre de clés à gérer devient important, ce qui complique leur stockage et leur protection.
- Compromis entre taille de la clé, sécurité et performance : Les algorithmes de chiffrement symétrique utilisent généralement des clés dont la taille est inférieure ou égale à 256 bits. Une clé plus longue offre une sécurité renforcée, mais au détriment des performances, car le

temps de calcul nécessaire au chiffrement et au déchiffrement augmente. Une clé trop courte est vulnérable aux attaques par force brute, car elle peut être facilement devinée en un nombre réduit d'essais. À l'inverse, une clé trop longue, bien que difficile à casser, ralentit considérablement le processus de traitement des données, rendant son utilisation peu efficace dans certaines situations. Il est donc crucial de trouver un compromis entre sécurité et performance, tout en veillant à limiter la complexité de gestion des clés.

c) Advanced Encryption Standard

L'AES est un algorithme de chiffrement symétrique conçu pour sécuriser les données par blocs de 128 bits, tout en supportant des longueurs de clé de 128, 192 ou 256 bits selon le niveau de protection requis. Adopté par le NIST en 2001 sous la norme FIPS-197, il est venu remplacer le Data Encryption Standard (DES), devenu vulnérable face aux progrès technologiques en matière de puissance de calcul [2].

Contrairement au DES, l'AES distingue clairement les processus de chiffrement et de déchiffrement, en utilisant des transformations inverses spécifiques pour chaque opération. Il introduit également un mécanisme avancé de génération de sous-clés, appelé Key Expansion, où une série de clés de tour est dérivée de la clé principale, renforçant ainsi la sécurité globale de l'algorithme.

Le processus de chiffrement AES est structuré autour de plusieurs étapes appliquées sur des blocs de données, organisés sous forme d'une matrice 4×4 appelée état. Chaque cycle de chiffrement est composé des transformations suivantes :

1. AddRoundKey : Chaque bit de l'état est combiné par une opération XOR avec une sous-clé spécifique au tour.
2. SubBytes : Chaque octet de la matrice est remplacé par un autre, selon une boîte de substitution non linéaire appelée S-box de Rijndael, introduisant la confusion.
3. ShiftRows : Les lignes de la matrice sont décalées cycliquement vers la gauche, assurant la diffusion des données.
4. MixColumns : Chaque colonne de la matrice est transformée par une multiplication matricielle dans un espace polynomial, renforçant la diffusion.
5. AddRoundKey : Une nouvelle sous-clé est à nouveau combinée avec l'état.

Ce cycle est répété un nombre de fois déterminé par la taille de la clé utilisée. Pour une clé de 128 bits, l'algorithme réalise 10 tours. Lorsqu'une clé de 192 bits est employée, il effectue 12 tours. Enfin, pour une clé de 256 bits, 14 tours sont exécutés, assurant ainsi un niveau de sécurité adapté à la longueur de la clé choisie. À noter que lors du dernier tour, la transformation MixColumns est omise.

Le déchiffrement suit le même nombre de tours, en appliquant les transformations inverses dans l'ordre inverse : Inverse SubBytes, Inverse ShiftRows, Inverse MixColumns, et AddRoundKey.

Grâce à son architecture optimisée, AES est capable d'exploiter le traitement parallèle, ce qui réduit considérablement les temps de traitement tout en maintenant un haut niveau de sécurité. Son temps d'initialisation réduit, sa flexibilité pour différentes tailles de clé, sa faible consommation de ressources et sa résistance aux principales attaques cryptographiques (cryptanalyse différentielle, cryptanalyse linéaire, attaques par clé liée, etc.) en font l'un des algorithmes de chiffrement les plus utilisés dans les systèmes modernes : réseaux sécurisés (SSL/TLS), disques durs chiffrés, communications mobiles, applications embarquées, et bien d'autres.

2.2.4 Algorithmes de chiffrement asymétrique

Le chiffrement asymétrique constitue une alternative plus sécurisée au chiffrement symétrique, notamment en résolvant les problèmes liés à la transmission des clés et à leur vulnérabilité aux attaques. Il repose sur l'utilisation de deux clés distinctes : une clé publique, accessible à tous, et une clé privée, qui doit être strictement conservée par son propriétaire. Ce fonctionnement permet d'assurer une protection plus robuste des données, car le chiffrement s'effectue à l'aide de la clé publique, tandis que seul le détenteur de la clé privée peut déchiffrer le message.

L'un des principaux avantages de ce type de chiffrement est qu'il empêche un attaquant d'utiliser la clé publique pour retrouver le contenu du message, ce qui garantit une sécurité renforcée. En outre, il permet d'authentifier l'origine et l'intégrité des données grâce à l'utilisation des signatures numériques. Toutefois, cette méthode présente également des inconvénients, notamment une complexité accrue et un temps de traitement plus long que le chiffrement symétrique. En raison de cette lenteur, elle est généralement employée pour chiffrer de petites quantités de données.

Plusieurs algorithmes reposent sur ce principe, parmi lesquels le RSA(Rivest–Shamir–Adleman), ElGamal et la cryptographie sur les courbes elliptiques (ECC), chacun offrant des niveaux de sécurité adaptés à différents usages.

a) RSA

L'algorithme RSA, développé par les mathématiciens Rivest, Shamir et Adleman, repose sur l'utilisation de deux nombres premiers entre eux. La difficulté de ce système réside dans le fait qu'il est facile de générer deux grands nombres premiers, mais très difficile de factoriser leur produit. Cette propriété confère au RSA une sécurité robuste. Plus la taille de la clé est grande, plus il devient difficile de le compromettre [3]. Cependant, cet algorithme souffre d'une vitesse de calcul relativement lente et d'une consommation élevée en ressources.

b) ElGamal

Le chiffrement ElGamal est un algorithme asymétrique fondé sur l'échange de clés Diffie-Hellman. Il fonctionne au sein d'un groupe cyclique, et sa sécurité repose sur la difficulté du problème du logarithme discret dans ce groupe. Ce système se compose de trois étapes principales : la génération des clés, le chiffrement et le déchiffrement. Étant plus lent en raison de sa nature asymétrique, il est souvent utilisé dans des systèmes hybrides où la clé secrète est

chiffrée avec ElGamal, tandis que des algorithmes symétriques sont utilisés pour le chiffrement des données, rendant ainsi l'ensemble du processus à la fois plus rapide et plus sécurisé.

c) ECC

La cryptographie sur courbes elliptiques (Elliptic Curve Cryptography, ECC) représente une avancée majeure dans le domaine de la cryptographie asymétrique, en proposant des mécanismes de sécurisation des données basés sur des principes mathématiques solides. À l'inverse des systèmes traditionnels tels que RSA, qui reposent sur la factorisation de grands entiers, l'ECC tire sa robustesse du problème du logarithme discret sur les courbes elliptiques, un problème reconnu pour sa difficulté algorithmique supérieure. Une courbe elliptique est définie, en champ fini, par une équation du type $y^2 = x^3 + ax + b$, où les coefficients a et b doivent satisfaire certaines conditions pour garantir la non-singularité de la courbe (discriminant non nul) [4]. Cette structure permet de doter l'ensemble des points de la courbe d'une opération d'addition, vérifiant les axiomes de groupe abélien (clôture, associativité, élément neutre, élément inverse, commutativité). Le concept d'ordre de la courbe, correspondant au nombre total de points définis sur le champ fini, est essentiel pour dimensionner correctement les paramètres de sécurité.

La génération de clés en ECC repose sur la sélection d'un point de base G et d'un entier secret k, aboutissant à une clé publique $P = kG$. Cette relation, simple à calculer mais pratiquement irréversible sans connaître k, constitue le fondement de la robustesse de l'ECC contre les attaques.

Lors du chiffrement, le message est d'abord encodé sous forme d'un point M sur la courbe ; puis, à l'aide d'un aléa cryptographique r, le chiffrement produit un couple de points $(rG , M + rP)$, exploitant ainsi pleinement la structure du groupe. Le déchiffrement, reposant sur une opération de soustraction dans le groupe elliptique, permet au détenteur de la clé privée de retrouver le message initial.

L'ECC offre un avantage décisif en termes d'efficacité, en procurant un niveau de sécurité équivalent à RSA avec des clés beaucoup plus courtes (par exemple, une clé ECC de 256 bits offre une sécurité comparable à une clé RSA de 3072 bits), ce qui réduit considérablement la charge computationnelle et la consommation énergétique. Cette efficacité, combinée à la flexibilité permise par la variété des courbes (modulation simple par changement de coefficients), rend la cryptographie sur courbes elliptiques particulièrement adaptée à la sécurisation des données médicales, notamment pour protéger les informations sensibles issues des dossiers médicaux électroniques, des dispositifs médicaux connectés et des systèmes d'information hospitaliers. En définitive, l'ECC s'impose aujourd'hui comme une technologie incontournable pour la protection des communications numériques critiques dans les infrastructures modernes de santé.

2.2.5 Comparaison entre la cryptographie symétrique et asymétrique

Les deux algorithmes de chiffrement sont puissants, mais chacun possède des avantages et des inconvénients distincts. Les algorithmes symétriques conviennent mieux au chiffrement de grandes quantités de données, tandis que les algorithmes asymétriques sont davantage

utilisés pour des données plus petites et sensibles. Étant donné que la taille et la criticité des données peuvent varier, il est souvent judicieux de combiner les atouts des deux systèmes afin d'optimiser à la fois la sécurité et l'efficacité. Un tableau 2.1 présente une comparaison entre ces deux approches de cryptographie [5].

Tableau 2.1 : Comparaison des caractéristiques des deux systèmes.

	Algorithme de chiffrement symétrique	**Algorithme de chiffrement asymétrique**
Nombre de clés	Clé secrète unique	Paire de clés
Catégorie de clé	La même clé pour le chiffrement / déchiffrement	Deux clés différentes Publique/Privé
Gestion des clés	Simple mais pas facile	Nécessite un certificat numérique et un tiers de confiance fiable
Vitesse	Très rapide	Lent
Sécurité	Élevée	Plus élevée
Application	Chiffrer des données volumineuses	Chiffrer des données nécessitant une haute confidentialité

2.2.6 Chiffrement hybride

Le chiffrement hybride constitue une approche efficace pour renforcer la sécurité des données et se protéger contre les attaques sur le texte en clair. Il repose sur la combinaison de différents algorithmes de chiffrement, qui peuvent être issus du même système ou de systèmes différents. L'une des méthodes les plus courantes consiste à associer le chiffrement symétrique et le chiffrement asymétrique.

Les algorithmes symétriques et asymétriques présentent chacun des avantages et des limites. Le chiffrement hybride permet d'optimiser la protection des données tout en répondant aux exigences de rapidité de traitement et de gestion des clés secrètes. Cette approche est particulièrement adaptée aux environnements nécessitant un niveau de sécurité élevé, où un algorithme unique ne suffirait pas.

En combinant des algorithmes puissants, le chiffrement hybride complique le travail des attaquants et offre une meilleure résistance aux attaques par force brute. Il tire parti des atouts des deux types de chiffrement tout en réduisant leurs faiblesses. L'une des stratégies les plus efficaces consiste à utiliser un algorithme symétrique pour chiffrer les données, afin de garantir une exécution rapide, tout en s'appuyant sur un algorithme asymétrique pour protéger la clé secrète.

L'un des principaux inconvénients du chiffrement symétrique est la vulnérabilité liée à l'utilisation d'une clé unique pour le chiffrement et le déchiffrement. Si cette clé est

compromise, un attaquant peut facilement récupérer le message. Pour pallier ce problème, un algorithme asymétrique peut être utilisé afin de chiffrer la clé secrète. Bien que cette opération prenne du temps, elle reste bien plus rapide que le chiffrement d'un long message avec un algorithme asymétrique.

Grâce à cette approche, la clé secrète est mieux protégée, et le chiffrement hybride bénéficie à la fois de la rapidité des algorithmes symétriques et de la robustesse des algorithmes asymétriques. Ce procédé améliore considérablement la sécurité des données sans entraîner une augmentation excessive du temps de traitement.

2.2.7 Modes de chiffrement par bloc

Le chiffrement par blocs est une méthode de cryptographie où le message en clair est segmenté en blocs de taille fixe avant d'être chiffré. Pour sécuriser ces blocs, il faut appliquer une stratégie spécifique appelée "mode de chiffrement". Il existe plusieurs modes de fonctionnement pour le chiffrement par blocs, parmi lesquels les plus utilisés sont :

- **Mode Electronic Code Book**

Dans ce mode, le message en clair M est découpé en blocs de taille fixe m_i. Chaque bloc est ensuite chiffré indépendamment à l'aide d'une fonction de chiffrement E_k, qui dépend d'une clé k [6].

Ainsi, un même bloc m_i sera toujours transformé de la même manière (voir Figure 2.1). Bien que simple à mettre en œuvre, ce mode présente une vulnérabilité importante face aux attaques.

Le déchiffrement repose sur l'application de l'inverse de la fonction de chiffrement : $D_k=E_k^{-1}$

Pour chiffrer un texte en mode ECB, l'opération suivante est effectuée :

$$c_i = E_k(m_i)$$

Pour déchiffrer un texte en mode ECB, l'opération suivante est appliquée :

$$m_i = D_k(c_i)$$

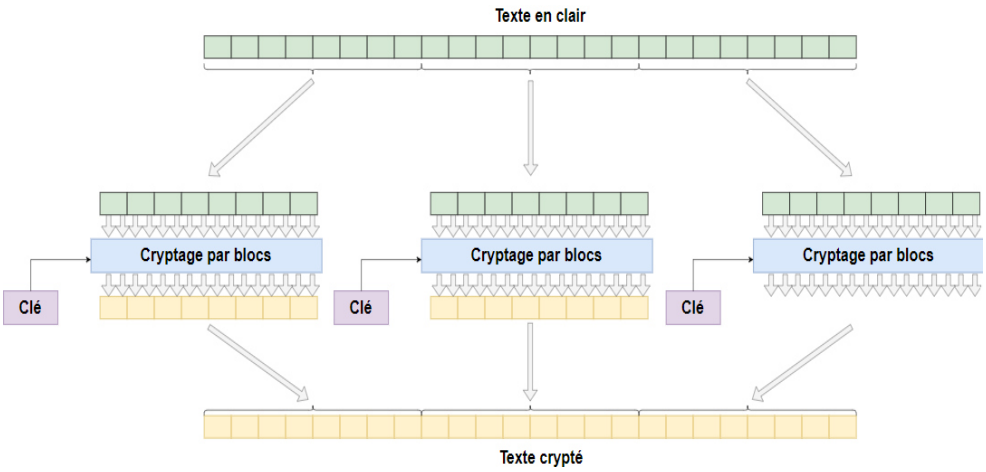


Figure 2.1 : Schéma bloc du mode ECB [7].

- **Mode Cipher Block Chaining**

Le mode CBC a été conçu pour éviter qu'un même bloc soit chiffré de façon identique lorsqu'il apparaît dans différents messages. Pour cela, une valeur initiale aléatoire C_0 (appelée IV pour *Initial Value*) est ajoutée [7].

Avant d'être chiffré, chaque bloc est combiné par une opération XOR avec le bloc chiffré précédent, puis il est encrypté, comme illustré dans la Figure 2.2.

Le déchiffrement repose sur l'inverse de la fonction de chiffrement : $D_k = E_k^{-1}$

Les opérations de chiffrement et de déchiffrement en mode CBC sont définies comme suit :

$$c_i = E_k(m_i \oplus c_{i-1})$$

$$m_i = c_{i-1} \oplus D_k(c_i)$$

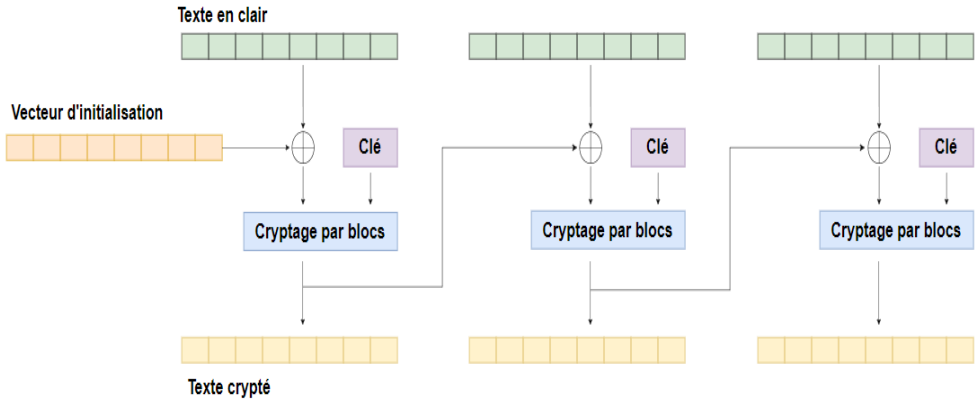


Figure 2.2 : Schéma bloc du mode CBC [7].

- **Mode Cipher Feedback**

L'avantage principal de ce mode est que le déchiffrement n'exige pas l'utilisation de la fonction inverse, soit : $D_k = E_k^{-1}$

Ainsi, ce mode est moins sécurisé que le mode CBC. Le diagramme de chiffrement pour le mode CFB est illustré dans la Figure 2.3.

Les étapes de chiffrement et de déchiffrement en mode CFB sont les suivantes :

$$c_i = m_i \oplus E_k(c_{i-1})$$

$$m_i = c_i \oplus E_k(c_{i-1})$$

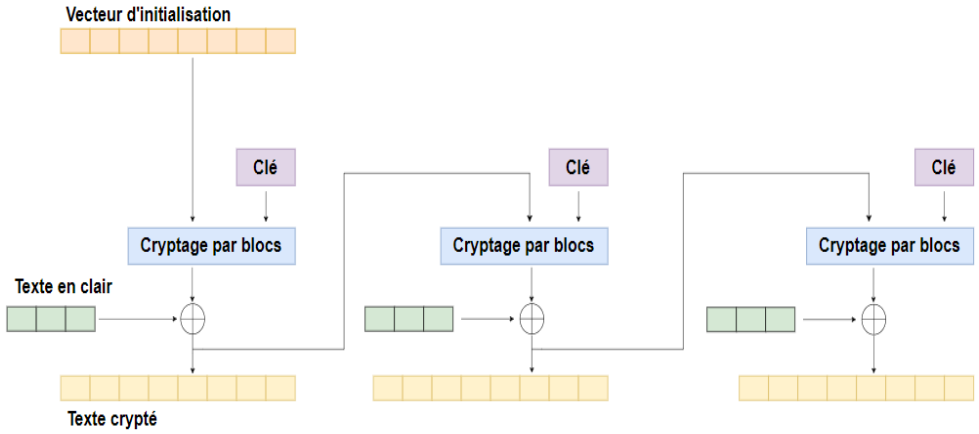


Figure 2.3 : Schéma bloc du mode CFB [7].

- **Mode Output Feedback**

Une variation du mode précédent permet d'obtenir un chiffrement et un déchiffrement complètement symétriques. Il s'agit du mode OFB, présenté dans la Figure 2.4.

$$z_0 = c_0 = IV$$

$$z_i = E_k(z_{i-1}) \; ; \; c_i = m_i \oplus z_i$$

$$z_i = E_k(z_{i-1}) \; ; \; mi = c_i \oplus z_i$$

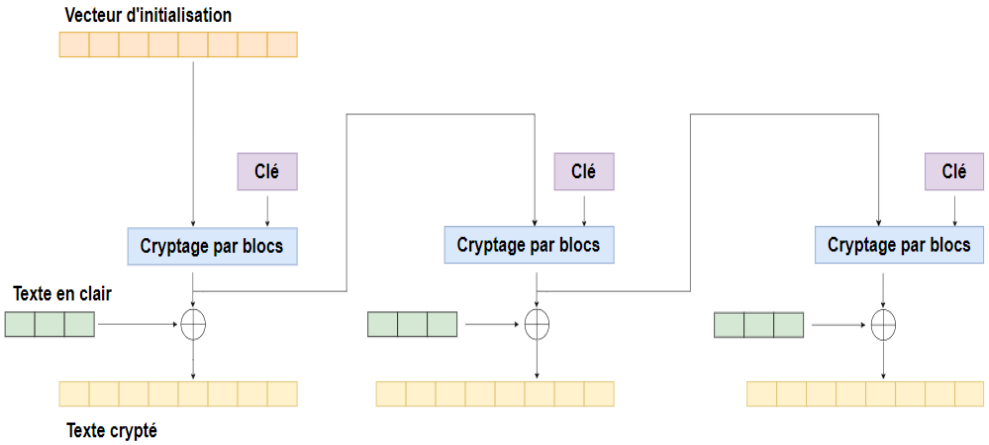


Figure 2.4 : Schéma bloc du mode OFB [7].

- **Mode Counter**

Ce mode est également totalement symétrique, mais il présente l'avantage supplémentaire d'être facilement parallélisable (permettant de chiffrer plusieurs blocs en parallèle), comme illustré dans la Figure 2.5.

Il repose sur le chiffrement d'un compteur avec une valeur initiale T. L'intérêt de ce mode est que, tout comme pour le mode ECB, les calculs sont indépendants, mais ici, le même bloc n'est jamais codé de la même manière.

$$c_i = m_i \oplus E_k(T + i)$$

$$m_i = c_i \oplus E_k(T + i)$$

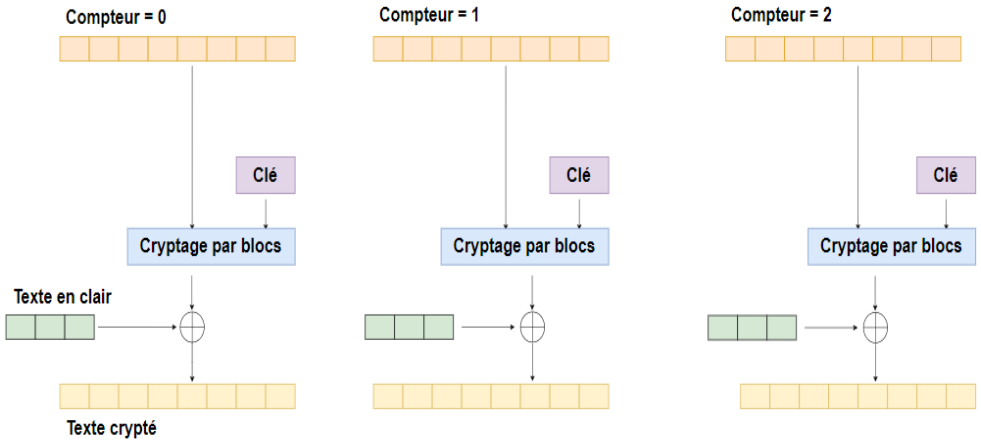


Figure 2.5 : Schéma bloc du mode CTR [7].

2.3 Vulnérabilités dans les réseaux radio cognitifs

Les réseaux radio cognitifs sont exposés à une série de vulnérabilités en raison de leur nature dynamique, de la répartition des responsabilités entre les nœuds, et des caractéristiques spécifiques du spectre radio. Ces vulnérabilités peuvent affecter la sécurité, l'intégrité et la performance du réseau. Voici une présentation des principales vulnérabilités :

- Vulnérabilité des canaux de communication : Les réseaux radio cognitifs fonctionnent principalement sur des canaux de communication sans fil, ce qui les rend plus susceptibles aux attaques que les réseaux filaires. En raison de la nature ouverte de la transmission radio, il est relativement facile pour un attaquant d'intercepter, modifier ou perturber les informations échangées. Les données transmises, qu'elles soient liées au trafic utilisateur ou à la gestion du réseau, peuvent être corrompues, altérées ou détruites, ce qui compromet la sécurité du réseau dans son ensemble.
- Vulnérabilité des nœuds du réseau : Les nœuds des réseaux radio cognitifs, qui peuvent être des dispositifs mobiles ou des équipements installés dans des environnements non sécurisés, sont également vulnérables. Un attaquant peut facilement introduire un nœud malveillant, ou manipuler un nœud existant pour collecter des informations sensibles, perturber les échanges de données, ou usurper l'identité d'autres nœuds. Cette vulnérabilité est

particulièrement critique, car chaque nœud joue un rôle clé dans la gestion des communications et dans l'allocation dynamique des fréquences. Si un nœud est compromis, il peut causer des perturbations à grande échelle dans le réseau.

- Changement dynamique de la topologie : Les réseaux radio cognitifs sont caractérisés par une topologie dynamique, dans laquelle de nouveaux nœuds peuvent rejoindre le réseau et d'autres peuvent en être retirés. Cette flexibilité crée un défi majeur pour le routage et la gestion des ressources. Si un attaquant prend le contrôle de certains nœuds ou falsifie des informations de topologie, il peut perturber la communication et l'allocation du spectre, ce qui affecte la performance globale du réseau. Des informations incorrectes ou des erreurs dues à des nœuds compromis peuvent entraîner des perturbations importantes.
- Exploitation des vulnérabilités liées à la radio définie par logiciel (SDR) : La technologie de la radio logiciel restreinte (SDR) permet une grande flexibilité dans la gestion du spectre, en permettant aux nœuds de reconfigurer dynamiquement leurs paramètres radio. Cependant, cette flexibilité crée des vulnérabilités supplémentaires, car un attaquant ayant accès au logiciel d'un nœud peut facilement manipuler son fonctionnement. Par exemple, l'attaquant pourrait altérer les fonctions de détection du spectre ou de gestion des fréquences, perturbant ainsi l'utilisation du spectre et compromettant le réseau. L'impact de ce type d'attaque peut être étendu, car il peut affecter non seulement un nœud, mais aussi l'ensemble du réseau.
- Risques liés à la coopération entre utilisateurs : Dans les réseaux radio cognitifs, la coopération entre utilisateurs est essentielle pour optimiser l'utilisation du spectre. Les utilisateurs secondaires (SU) sont censés partager les ressources de manière collaborative et non malveillante. Cependant, un attaquant peut exploiter cette coopération en se faisant passer pour un nœud légitime et en interférant dans les décisions collectives prises par les autres nœuds. Par exemple, un nœud malveillant pourrait influencer la sélection des canaux ou perturber les mécanismes de prise de décision, comme la négociation pour l'accès au spectre. Une telle intrusion pourrait avoir des conséquences graves sur l'efficacité et la sécurité du réseau.
- Limites des ressources : Les nœuds des réseaux radio cognitifs fonctionnent souvent sur des ressources limitées, telles que l'énergie et la capacité de traitement. Ces limitations rendent difficile l'implémentation de mécanismes de sécurité complexes et de protocoles de cryptage robustes. Par exemple, des attaques par déni de service (DoS) peuvent être lancées pour épuiser les ressources des nœuds, en les forçant à traiter des requêtes inutiles et à épuiser leur batterie. En raison de la puissance de traitement limitée, la capacité du réseau à détecter et à se défendre contre de telles attaques peut être compromise [8].

2.4 Menaces de sécurité dans les réseaux radio cognitifs

Les réseaux radio cognitifs sont exposés à plusieurs menaces qui compromettent leur bon fonctionnement et leur sécurité. Ces menaces exploitent les spécificités de ces réseaux, notamment leur capacité d'adaptation et leur dépendance aux décisions cognitives.

- Menace liée à la détection du spectre : Les CRNs reposent sur un processus de détection du spectre permettant aux utilisateurs non autorisés de déterminer si une bande de fréquence est libre ou occupée. Toutefois, cette fonctionnalité peut être exploitée par des attaquants pour

altérer les résultats de détection, perturbant ainsi le fonctionnement du réseau. Une falsification des données de détection peut paralyser la communication et perturber le trafic global. D'autres menaces associées concernent le partage du spectre, la prise de décision et la gestion de la mobilité dans le spectre.

- Menace du terminal caché : Identifier la présence d'utilisateurs primaires (PUs) à travers un large spectre est un défi majeur. La diversité des schémas de modulation, des puissances d'émission et des débits de transmission complique cette tâche. De plus, les pertes de propagation et le bruit thermique introduisent des incertitudes qui peuvent être exploitées par des attaquants, causant des interférences et des erreurs de détection. Ce problème, connu sous le nom de terminal caché, peut engendrer des conflits d'accès aux ressources du réseau.
- Menace liée aux politiques de gestion du spectre : Pour garantir une communication efficace, les réseaux cognitifs doivent adapter leur fonctionnement en fonction de l'environnement et des conditions spécifiques. Cependant, un attaquant peut interférer en modifiant les règles de gestion du spectre ou en introduisant de fausses politiques, ce qui peut compromettre la fiabilité du réseau et engendrer de nouvelles vulnérabilités.
- Menace liée à l'apprentissage : Certains CRNs possèdent des capacités d'apprentissage leur permettant d'optimiser leur utilisation du spectre en s'appuyant sur des expériences passées. Cependant, un attaquant peut manipuler les données historiques ou les informations en temps réel afin de fausser les prévisions du système, réduisant ainsi son efficacité et sa capacité d'adaptation.
- Menace sur les paramètres du réseau : Un adversaire peut forcer un CRN à modifier ses paramètres afin de dégrader ses performances ou de limiter l'accès à des services essentiels. Cette manipulation peut entraîner une allocation inefficace des ressources et affaiblir la qualité du réseau [9].

En plus de ces menaces spécifiques, les CRNs restent vulnérables à diverses attaques qui ciblent les différentes couches des protocoles de communication. Ces attaques seront examinées plus en détail dans la section suivante.

2.5 Les attaques dans les réseaux radio cognitifs

Les réseaux radio cognitifs sont vulnérables à diverses attaques en raison de leur nature dynamique et de leur architecture flexible. Contrairement aux réseaux traditionnels, les CRNs reposent sur la reconfiguration du spectre et des prises de décision autonomes, ce qui ouvre de nouvelles opportunités aux attaquants pour exploiter ces mécanismes. Ces attaques peuvent cibler différentes couches du réseau et compromettre des aspects essentiels tels que la communication, la gestion du spectre et la coopération entre les nœuds. Bien que certaines attaques soient similaires à celles observées dans les réseaux sans fil classiques, d'autres sont propres aux CRN en raison de leurs caractéristiques uniques. Pour mieux comprendre ces menaces, nous classons les attaques en fonction des couches de protocole qu'elles ciblent, notamment les couches Physique, Liaison, Réseau et Transport.

2.5.1 Attaques sur la couche physique

La couche physique des réseaux radio cognitifs constitue la première ligne de défense contre les menaces qui ciblent les transmissions sans fil et l'accès dynamique au spectre. En raison de la nature ouverte des communications et de la reconfigurabilité du réseau, cette couche est particulièrement vulnérable à diverses attaques visant à perturber, intercepter ou manipuler les transmissions. Ces attaques exploitent les spécificités des CRN, telles que le partage opportuniste du spectre et la détection dynamique des fréquences disponibles, afin de compromettre la sécurité et l'efficacité du réseau. Dans ce qui suit, nous présentons les principales attaques affectant la couche physique des CRN ainsi que leurs impacts potentiels sur le fonctionnement du réseau.

L'attaque d'émulation de l'utilisateur primaire : L'un des principes fondamentaux des réseaux radio cognitifs est qu'un utilisateur secondaire peut exploiter une bande de fréquences tant qu'aucun utilisateur primaire ne l'occupe. Toutefois, dès qu'un utilisateur secondaire détecte la présence d'un utilisateur primaire, il doit immédiatement libérer la bande et basculer vers une autre fréquence afin d'éviter toute interférence. Lorsque plusieurs utilisateurs secondaires souhaitent accéder à la même bande, des mécanismes de partage du spectre doivent être mis en place pour assurer une répartition équitable des ressources.

L'attaque par émulation de l'utilisateur primaire (Primary User Emulation - PUE) consiste en une tentative frauduleuse d'un utilisateur secondaire malveillant qui imite un utilisateur primaire ou usurpe son identité dans le but d'accaparer les ressources d'un canal sans les partager avec d'autres utilisateurs secondaires. Grâce à cette attaque, l'attaquant peut monopoliser des portions entières du spectre radio [10] [11]. La Figure 2.6 montre un exemple d'attaque PUE, où un utilisateur secondaire malveillant imite un utilisateur primaire pour monopoliser le spectre, empêchant ainsi l'accès des autres utilisateurs secondaires.

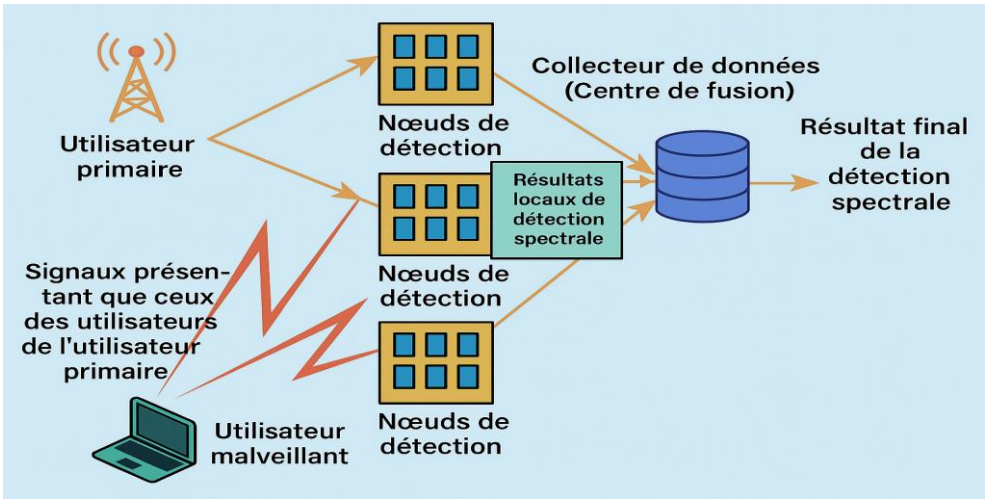


Figure 2.6 : L'attaque d'émulation de l'utilisateur primaire PUE.

Cette attaque peut être motivée par deux objectifs distincts :

- **Attaque PUE égoïste** : L'attaquant cherche à maximiser son accès aux ressources du spectre en simulant la présence d'un utilisateur primaire. Cette stratégie peut également être utilisée par deux attaquants coordonnés afin d'établir une liaison exclusive entre eux.

- **Attaque PUE malveillante** : L'attaquant vise ici à empêcher les utilisateurs secondaires légitimes d'accéder aux fréquences disponibles en les trompant sur l'occupation du spectre [12].

L'attaque PUE peut affecter les systèmes radio cognitifs de différentes manières selon leur mode de fonctionnement :

- ✓ Dans les systèmes basés sur des règles prédéfinies, l'attaque cesse d'avoir un impact dès que l'attaquant quitte le canal, car les utilisateurs secondaires pourront alors détecter la disponibilité du spectre et le réutiliser.
- ✓ Dans les systèmes basés sur l'apprentissage, les utilisateurs secondaires analysent les comportements passés des utilisateurs primaires pour anticiper la disponibilité des fréquences [13]. Si un attaquant exploite ces informations en simulant un signal pendant les périodes d'inactivité des utilisateurs primaires, l'attaque peut avoir un effet durable, rendant certaines fréquences inutilisables par les utilisateurs secondaires sur le long terme.

Certaines caractéristiques des réseaux radio cognitifs peuvent être exploitées pour renforcer l'efficacité des attaques PUE :

- ✓ Exploitation des périodes de silence : Pendant ces intervalles, tous les utilisateurs secondaires cessent temporairement leur transmission afin de faciliter la détection du spectre. Un attaquant peut alors émettre un signal trompeur pendant ces périodes, faisant croire aux autres utilisateurs qu'un utilisateur primaire occupe la bande.
- ✓ Perturbation lors du changement de fréquence : Lorsque le réseau bascule d'une fréquence à une autre pour éviter des interférences ou optimiser l'utilisation du spectre, un attaquant peut exploiter cette transition pour mener une attaque PUE. En anticipant la prochaine fréquence utilisée par le réseau, il peut perturber la transmission des utilisateurs secondaires, entraînant une dégradation significative du débit de données, voire une interruption totale du service.

L'attaque par Brouillage : L'attaque par brouillage (*jamming attack*) est l'une des menaces les plus répandues et dangereuses dans les réseaux radio cognitifs. Son objectif principal est de perturber la communication entre les utilisateurs en occupant le canal de transmission, empêchant ainsi les nœuds légitimes d'envoyer ou de recevoir des données. Cette attaque peut entraîner une dégradation significative du réseau, voire un déni de service (Denial of Service - DoS).

Le brouillage est particulièrement préoccupant dans les CRN en raison de la nature dynamique de ces réseaux, où les utilisateurs secondaires exploitent les portions du spectre laissées libres par les utilisateurs primaires [14]. En saturant ces fréquences, un attaquant peut empêcher les utilisateurs cognitifs d'accéder au spectre disponible, rendant ainsi inefficace le concept même de radio cognitive.
Un brouilleur est un dispositif malveillant qui émet des signaux parasites sur une fréquence spécifique ou sur plusieurs fréquences afin de perturber la communication. Contrairement à d'autres types d'attaques nécessitant une connaissance préalable du réseau, le brouillage peut

être effectué sans aucune information sur l'infrastructure cible. Un attaquant disposant de ressources suffisantes peut facilement bloquer l'ensemble d'une bande spectrale, paralysant ainsi toute transmission de données.

L'attaque par brouillage peut être mise en œuvre de différentes manières, selon la stratégie adoptée par l'attaquant [15] :

- **Brouillage ciblé, balayé et en rafale**
  - ✓ Brouillage ciblé (*Spot Jamming*) : L'attaquant choisit une fréquence précise et y émet un signal puissant en continu, empêchant ainsi toute communication sur cette fréquence spécifique.
  - ✓ Brouillage balayé (*Sweep Jamming*) : L'attaque consiste à balayer plusieurs fréquences de manière séquentielle, perturbant ainsi la communication sur une large bande spectrale.
  - ✓ Brouillage en rafale (*Barrage Jamming*) : L'attaquant cible simultanément plusieurs fréquences afin d'augmenter l'impact du brouillage sur le réseau.
- **Brouillage simple et collaboratif**
  - ✓ Brouillage simple : Un seul brouilleur agit indépendamment pour perturber le réseau.
  - ✓ Brouillage collaboratif : Plusieurs brouilleurs travaillent ensemble pour maximiser leur impact en coordonnant leurs transmissions. Cette approche leur permet de mieux comprendre la structure du réseau et d'adapter leurs attaques en conséquence.
- **Brouillage constant et aléatoire**
  - ✓ Brouillage constant : Le brouilleur émet un signal en continu sur une fréquence spécifique, empêchant ainsi toute autre transmission légitime.
  - ✓ Brouillage aléatoire : Le brouilleur alterne entre des périodes de transmission et des périodes de silence. Cette variation rend l'attaque plus difficile à détecter et permet à l'attaquant de gérer efficacement sa consommation d'énergie.
- **Brouillage trompeur et réactif**
  - ✓ Brouillage trompeur (*Deceptive Jamming*) : L'attaquant émet des signaux imitant ceux d'un utilisateur primaire ou légitime. Cela trompe les autres utilisateurs cognitifs et les empêche d'accéder au spectre disponible.
  - ✓ Brouillage réactif (*Reactive Jamming*) : Le brouilleur surveille en permanence le canal et n'émet un signal de brouillage que lorsqu'il détecte une transmission en cours. Cette approche permet de provoquer des collisions et de perturber sélectivement les communications, tout en restant difficile à repérer.

Le brouillage dans les CRNs entraîne de nombreuses conséquences négatives sur le réseau et ses utilisateurs. Parmi les effets les plus notables :

- ✓ Réduction du débit des utilisateurs cognitifs : En empêchant les transmissions normales, le brouillage diminue considérablement la capacité du réseau à transmettre des données.
- ✓ Perturbation du processus de détection du spectre : Les radios cognitives doivent continuellement analyser leur environnement pour identifier les bandes de fréquences disponibles. Un brouillage constant ou réactif peut fausser ces analyses et empêcher les utilisateurs secondaires d'exploiter efficacement le spectre.
- ✓ Détérioration de la qualité de service : Le brouillage peut entraîner des interruptions de communication, des pertes de paquets et une latence accrue, rendant les services basés sur le CRN moins fiables.

- ✓ Augmentation de la consommation d'énergie : Pour contrer le brouillage, les utilisateurs cognitifs doivent effectuer davantage d'opérations de détection et de changement de canal, ce qui accroît leur consommation énergétique.

L'attaque sur la fonction objectif (OFA) : L'attaque sur la fonction objectif (Objective Function Attack) dans les réseaux radio cognitifs cible le moteur cognitif, qui est responsable de l'ajustement des paramètres de transmission en fonction de l'environnement et des exigences du réseau. En effet, ce moteur a pour mission de sélectionner les paramètres tels que la fréquence, la bande passante, la puissance d'émission, la modulation, le protocole d'accès au canal, le taux de codage, et la taille des trames afin d'optimiser des critères tels que la consommation d'énergie, la vitesse de transmission ou la sécurité.

Lorsqu'un attaquant manipule certains de ces paramètres, par exemple en perturbant la vitesse de transmission ou en affectant la sécurité de la communication, il peut induire des résultats biaisés, forçant ainsi la radio cognitive à adopter des configurations sous-optimales. L'attaquant pourrait ainsi obtenir des performances de réseau qui lui sont favorables, tout en diminuant la sécurité, ce qui rend le système plus vulnérable aux attaques [16]. Cette attaque peut principalement affecter les réseaux radio cognitifs qui utilisent l'apprentissage en ligne, où les paramètres sont ajustés dynamiquement en fonction des changements dans l'environnement. Les radios qui n'emploient pas un tel système d'apprentissage en temps réel seraient, quant à elles, moins sensibles à ce type de manipulation. Les méthodes pour contrer cette forme d'attaque incluent l'amélioration des algorithmes de prise de décision du moteur cognitif, le renforcement des contrôles de sécurité et l'utilisation de mécanismes de détection des manipulations extérieures.

2.5.2 Attaques sur la couche liaison

La couche de liaison joue un rôle essentiel dans l'encapsulation des données sous forme de trames, régulant ainsi leur accès à la couche physique. Elle assure également la gestion des transmissions et optimise l'utilisation des canaux de communication. Dans un réseau sans fil conventionnel, cette couche fonctionne différemment par rapport à un réseau radio cognitif. En effet, les canaux de communication dans un CRN possèdent des caractéristiques dynamiques et variables, ce qui complique la gestion des transmissions. De plus, les utilisateurs cognitifs exploitent plusieurs canaux simultanément afin d'augmenter le débit et d'optimiser l'accès aux ressources spectrales disponibles [9].

Toutefois, cette flexibilité et cette capacité d'adaptation rendent la couche de liaison vulnérable à diverses attaques. Les assaillants peuvent exploiter les spécificités de cette couche pour perturber la communication, provoquer des collisions de données ou manipuler les mécanismes de contrôle d'accès au média. Ces attaques peuvent gravement impacter la fiabilité du réseau et compromettre son bon fonctionnement. Dans ce qui suit, nous allons présenter les différentes attaques visant la couche de liaison, en expliquant leurs mécanismes et leurs effets sur la communication dans les réseaux radio cognitifs.

L'attaque de falsification des données de détection du spectre : L'attaque de falsification des données de détection du spectre (SSDF), également appelée attaque byzantine [17], est une menace spécifique aux réseaux cognitifs. Elle consiste en l'envoi, par un attaquant malveillant, de fausses informations sur l'état du spectre radio, faussant ainsi le processus de prise de décision.

Dans un réseau cognitif centralisé, le centre de traitement des informations collecte les données de détection du spectre provenant de plusieurs nœuds avant de décider quelles fréquences sont libres ou occupées. Un attaquant exploitant cette vulnérabilité peut manipuler le centre de décision en lui faisant croire qu'une bande libre est occupée, empêchant ainsi les utilisateurs légitimes de l'utiliser, ou inversement, en signalant qu'une bande occupée est libre, entraînant ainsi des interférences.

Dans un réseau cognitif distribué, où les décisions sont prises de manière collaborative entre les utilisateurs, cette attaque est encore plus dangereuse. En effet, les fausses informations peuvent rapidement se propager sans contrôle centralisé, rendant leur détection et leur correction plus complexes.

Toutefois, dans un réseau centralisé, il est possible d'atténuer les effets de l'attaque en comparant les données reçues de différents nœuds afin d'identifier les incohérences et d'isoler les sources suspectes d'informations erronées [8].

L'attaque de saturation du canal de contrôle DoS : Dans un réseau cognitif multi-sauts, les nœuds doivent d'abord négocier l'accès au canal avant d'établir une communication. Cette négociation repose sur l'échange de trames de contrôle MAC pour réserver le canal. Cependant, lorsque plusieurs nœuds tentent de communiquer simultanément, le canal de contrôle commun devient rapidement un point de congestion, car il ne peut gérer qu'un nombre limité de connexions actives. Un attaquant peut exploiter cette vulnérabilité en générant de fausses trames de contrôle MAC, provoquant ainsi une saturation du canal de contrôle. Cette surcharge entraîne des collisions au niveau de la couche de liaison et une diminution drastique des performances du réseau.

Il est important de noter que cette attaque affecte uniquement les CRNs fonctionnant de manière distribuée. En revanche, dans un CRN centralisé, chaque trame de contrôle MAC est authentifiée et validée par la station de base, ce qui empêche toute falsification des trames et rend cette attaque inefficace [18].

L'attaque de négociation égoïste du canal (SCN) : Dans les réseaux cognitifs à routage multi-sauts, certains nœuds peuvent adopter un comportement égoïste en refusant de relayer les messages vers les autres nœuds. Cette stratégie leur permet de préserver leur propre débit en limitant l'utilisation de leurs ressources, un phénomène connu sous le nom de dissimulation égoïste du canal (Selfish Channel Negotiation, SCN). Ce type d'attaque compromet la transmission des données et peut affecter considérablement les performances globales du réseau [19].

2.5.3 Attaques sur la couche réseau

Les réseaux radio cognitifs utilisent des topologies similaires à celles des réseaux de communication sans fil classiques, notamment des réseaux sans infrastructure, des réseaux basés sur une infrastructure et des réseaux hybrides, comme les réseaux de capteurs sans fil. Cependant, en raison de leur ouverture nécessaire pour permettre l'accès aux utilisateurs primaires, ces réseaux sont particulièrement vulnérables à diverses menaces de sécurité, notamment au niveau du routage. Ces attaques affectent la construction de la table de routage en envoyant de fausses informations, ce qui peut provoquer des collisions et la perte de paquets dans la couche réseau [20]. Les attaques de sécurité les plus courantes à ce niveau sont les attaques Hello, Sinkhole et Sybil.

L'attaque Hello : Cette attaque a des effets nuisibles sur les réseaux radio cognitifs en raison des similitudes et des complémentarités avec les technologies de routage utilisées dans les réseaux de capteurs sans fil. L'attaquant émet un signal à haute puissance pour pénétrer dans les nœuds du réseau ayant une forte densité de signal, créant ainsi une fausse impression que l'attaquant est un voisin légitime. Lorsque le nœud transmet des paquets à cet appareil, il découvre qu'il n'a plus de voisins valides et réalise que l'attaquant a trompé le système [19].

L'attaque Sinkhole : Dans le cadre d'une attaque Sinkhole, un attaquant se présente comme le chemin le plus rapide vers une destination particulière. Les nœuds voisins redirigent leurs paquets via cet attaquant, qui peut alors modifier ou supprimer les paquets qui transitent par lui. Une attaque supplémentaire, comme l'acheminement sélectif, peut aussi être menée par l'attaquant, qui peut choisir de manipuler ou de rejeter les paquets des nœuds du réseau. Cette attaque est particulièrement efficace dans les réseaux d'infrastructure et maillés, surtout lorsque tout le trafic transite par la station de base [21].

L'attaque Sybil : Dans un réseau CRN, chaque nœud doit avoir une identité valide pour se connecter et utiliser le canal. L'attaque Sybil exploite cette exigence en générant plusieurs fausses identités, ce qui perturbe la phase de prise de décision du spectre. Cela empêche les utilisateurs légitimes d'accéder au canal et permet à l'attaquant d'effectuer des transmissions opportunistes, perturbant ainsi l'intégralité du canal de contrôle [19].

2.5.4 Attaques sur la couche transport

La couche transport assure la gestion du trafic, le contrôle de la congestion, et la récupération des erreurs entre les nœuds d'un réseau. Dans un réseau radio cognitif (CRN), cette couche est vulnérable aux mêmes problèmes que ceux rencontrés dans les réseaux sans fil ad hoc [20].

L'attaque par épuisement des clés : Les réseaux radio cognitifs sont particulièrement sensibles aux sessions de transport de courte durée, ce qui entraîne la création d'un grand nombre de sessions. À chaque début de session, des clés cryptographiques sont générées par des protocoles de sécurité comme SSL (Secure Socket Layer) et TLS (Transport Layer Security). Avec l'énorme quantité de clés générées, la probabilité qu'une clé soit répliquée

augmente [20]. Cette répétition de clés constitue une opportunité pour les attaquants de manipuler et de compromettre le système de chiffrement.

L'attaque Jellyfish : Les attaques Jellyfish visent à perturber le fonctionnement du protocole TCP (Transmission Control Protocol) au sein de la couche transport. Elles se produisent généralement au niveau de la couche réseau avant la phase de transmission suivante dans la couche transport, ce qui a un impact direct sur la performance de la transmission de données [19].

L'attaque Lion : L'attaque Lion se distingue des autres attaques, notamment dans le cadre des réseaux radio cognitifs, car elle cible spécifiquement la couche transport. En se faisant passer pour un utilisateur légitime, l'attaquant exploite les mêmes simulations utilisées par l'utilisateur principal. Ce type d'attaque peut se produire tant à l'intérieur qu'à l'extérieur du réseau [20].

2.6 Modèles de sécurité pour les réseaux radio cognitifs

La sécurité des réseaux radio cognitifs est un domaine qui a fait l'objet de nombreuses recherches afin de contrer les différentes menaces qui pèsent sur ces systèmes dynamiques. Plusieurs approches ont été proposées pour assurer une communication fiable et sécurisée tout en optimisant l'utilisation du spectre. Diverses méthodes exploitent la gestion de la confiance, l'apprentissage automatique, la sécurité de la couche physique ou encore des stratégies spécifiques contre le brouillage et l'usurpation d'identité. Voici un ensemble de techniques et protocoles identifiés dans les recherches récentes.

Les auteurs de [22] ont conçu une technique étendue pour la détection coopérative du spectre, prenant en compte la présence d'utilisateurs malveillants. Une contrainte est imposée à la probabilité de fausse détection afin de minimiser l'interférence et d'éviter une perturbation excessive des utilisateurs sous licence. Une autre approche repose sur un système de gestion de confiance distribué ne nécessitant pas de centre de fusion, démontrant son efficacité contre la manipulation de croyances [23].

L'attaque par émulation d'utilisateur primaire (PUE) est une autre menace courante dans les CRN. Pour se défendre contre cette attaque, une approche basée sur l'algorithme d'Automate d'Apprentissage Bayésien Multicanal (MBLA) a été proposée [24]. Cette méthode permet d'optimiser la sélection de canaux en s'adaptant aux environnements non stationnaires. Une stratégie complémentaire repose sur le saut de fréquence non coordonné (UFH), permettant d'échapper aux attaquants.

Le brouillage représente une menace sérieuse pour les réseaux radio cognitifs. Une technique exploitant l'impact du brouilleur sur la zone d'interférence et l'occupation du point d'accès a été développée pour identifier ces attaques [25]. Différents algorithmes ont été testés, notamment l'algorithme de localisation de brouilleur adaptatif (AJLA), qui sélectionne une méthode de détection en fonction du type d'antenne utilisé par le brouilleur [26]. Les antennes omnidirectionnelles utilisent les techniques de localisation par centroïde (CL) et par itération

de force virtuelle (VFIL), tandis que les antennes directionnelles adoptent l'algorithme amélioré de recherche gravitationnelle (IGSA).

Une approche alternative consiste à utiliser un honeynet pour analyser les tactiques des attaquants et ajuster les contre-mesures en temps réel [27]. Ce système a prouvé son efficacité en réduisant l'impact des attaques de brouillage et en augmentant le taux de livraison des paquets.

Une méthode de protection supplémentaire repose sur l'apprentissage automatique. Un protocole anti-brouillage basé sur l'apprentissage Q a été proposé, exploitant un processus de décision de Markov (MDP) pour optimiser la sélection des sous-bandes de fréquence [28]. La table Q apprise pour la gamme de fréquences entre [2 - 2,2 GHz] est présentée dans [29].

Dans le cadre des réseaux mobiles de cinquième génération (5G), les utilisateurs primaires et secondaires peuvent coexister dans la même bande sous licence [29]. Toutefois, l'interférence des utilisateurs secondaires doit être minimisée afin de ne pas perturber les communications des utilisateurs primaires [30]. Étant donné que les canaux sans fil sont diffusés, la protection de ces communications est essentielle pour éviter les écoutes clandestines et les manipulations de signaux [31].

La sécurité de la couche physique constitue une méthode efficace pour garantir la confidentialité des communications dans les réseaux radio cognitifs [32]. En exploitant la distinction entre le canal principal et le canal d'espionnage, cette approche permet d'améliorer la transmission secrète. Certaines techniques, telles que le beamforming et l'injection de bruit synthétique, renforcent la protection contre les interceptions [33]. La modulation directionnelle est également utilisée pour cibler la transmission des signaux dans une direction spécifique, réduisant ainsi le risque d'écoute malveillante [34].

Les auteurs de [35] se sont concentrés sur les attaques de perturbation du routage au niveau de la couche réseau des CRN, tandis que ceux de [36] ont proposé une approche basée sur la valeur du risque de crédit (CRV) pour identifier les nœuds auto-servants dans le réseau. Avant d'envoyer des paquets, cette méthode calcule la valeur CRV et la met à jour après chaque routage.

Dans le domaine des radios logicielles (SDR), plusieurs vulnérabilités ont été identifiées. Weinmann [37] a démontré l'exploitation d'une implémentation de bande de base GSM, tandis que des chercheurs de Google Project Zero et Exodus Intelligence ont révélé des failles critiques dans le micrologiciel des puces Wi-Fi Broadcom [38][39]. Les auteurs de [40] ont dressé une analyse complète des menaces de sécurité affectant les radios logicielles, incluant notamment les attaques par déni de service (DoS) et les compromissions de données utilisateur. À travers leur étude, Ahuja et al. [40] mettent en évidence les vulnérabilités critiques aux niveaux physique et réseau dans les réseaux radios cognitifs, tout en proposant des mesures de détection et de contre-mesure adaptées.

Selon [41], certains utilisateurs secondaires (SUs) malveillants enfreignent les règles d'accès aux canaux en les utilisant même en présence d'une activité des utilisateurs primaires (PUs), ce qui peut entraîner des interférences et compromettre la fiabilité du réseau. De leur côté, les techniques TRM présentées dans [42] permettent de détecter les SUs qui, volontairement ou involontairement, transmettent de fausses informations de détection en ignorant les erreurs dans leurs propres résultats d'analyse.

L'apprentissage automatique est également utilisé dans les réseaux véhiculaires ad hoc (VANET) pour détecter les attaques de brouillage [43]. En analysant les variations de vitesse entre le brouilleur et le récepteur, le système peut différencier un brouillage intentionnel d'un brouillage accidentel.

Enfin, l'intégration des technologies de communication avancées dans les réseaux cognitifs ouvre la voie à de nouvelles stratégies de sécurité. Le brouillage amical (Fri-jam) protège les données médicales sensibles en générant un brouillage contrôlé contre les espions [44]. De plus, des approches comme la duplexité complète et la transmission simultanée d'énergie et d'information (SWIPT) peuvent être utilisées pour améliorer la résilience des CRN face aux attaques.

Ces différentes méthodes illustrent la diversité des stratégies mises en place pour protéger les réseaux radio cognitifs contre les menaces actuelles et émergentes. Les recherches dans ce domaine continuent d'évoluer afin de proposer des solutions toujours plus efficaces et adaptées aux nouvelles formes d'attaques.

2.7 Sécurité des données médicales dans les réseaux radio cognitifs

L'essor des réseaux radio cognitifs représente une avancée technologique majeure dans le domaine des communications sans fil, en optimisant l'utilisation du spectre électromagnétique de manière dynamique et efficace. Ces réseaux intelligents permettent d'adapter en temps réel l'allocation des fréquences en fonction des disponibilités et des besoins. Toutefois, leur intégration dans les systèmes de santé soulève des défis critiques en matière de sécurité des données médicales, qui sont parmi les informations les plus sensibles et confidentielles.

Dans un environnement médical connecté, les dossiers médicaux électroniques (DME), les résultats d'examens, les prescriptions numériques, ainsi que les données en temps réel issues des dispositifs médicaux intelligents sont transmis, stockés et traités via ces réseaux. Une protection rigoureuse contre les menaces émergentes est donc essentielle pour garantir la confidentialité, l'intégrité et la disponibilité de ces informations critiques. Cependant, la nature ouverte et adaptative des réseaux radio cognitifs introduit de nouvelles vulnérabilités qui peuvent être exploitées par des attaquants pour intercepter, manipuler ou bloquer la transmission des données médicales. Pour répondre à ces défis, il est impératif de mettre en place des modèles de sécurité avancés, combinant chiffrement, authentification renforcée et surveillance en temps réel.

2.7.1 Contexte de la sécurité des données médicales

La sécurité des données médicales ne se limite pas seulement à la confidentialité des informations des patients, mais englobe également la disponibilité et l'intégrité des données stockées et transmises à travers les réseaux de communication. Dans un environnement où la télémédecine, les dispositifs médicaux connectés et les systèmes d'information hospitaliers jouent un rôle crucial, toute faille de sécurité peut entraîner des conséquences graves, allant de la violation de la vie privée des patients à des erreurs médicales pouvant mettre des vies en danger.

Les attaques informatiques ciblant les infrastructures de santé sont en augmentation, avec des cybercriminels exploitant les vulnérabilités des réseaux pour accéder aux bases de données médicales. Les rançongiciels (ransomware), par exemple, ont déjà paralysé plusieurs hôpitaux, empêchant les médecins d'accéder aux dossiers médicaux des patients et retardant ainsi les soins. De plus, des attaques sophistiquées, comme l'interception des communications entre capteurs médicaux et serveurs de stockage, peuvent altérer les informations transmises, compromettant la prise de décision clinique.

Dans le cadre des réseaux radio cognitifs, la situation est encore plus complexe. Ces réseaux utilisent des techniques d'allocation dynamique du spectre, ce qui signifie que les canaux de communication ne sont pas fixes et peuvent être réattribués en fonction de la disponibilité et de la demande. Cette caractéristique, bien qu'efficace pour optimiser l'utilisation du spectre, introduit des vulnérabilités qui peuvent être exploitées par des attaquants pour perturber la transmission des données médicales ou usurper l'identité de dispositifs médicaux autorisés.

Ainsi, la mise en place de solutions de sécurité adaptées aux CRNs dans le domaine médical est indispensable. Cela implique l'adoption de protocoles de chiffrement avancés, de mécanismes d'authentification robustes, ainsi que de systèmes de détection d'intrusion spécialisés capables d'identifier et de neutraliser les menaces en temps réel. De plus, l'intégration de technologies émergentes telles que l'intelligence artificielle et la blockchain peut jouer un rôle clé dans l'amélioration de la traçabilité et de la protection des données de santé dans ces environnements dynamiques et sensibles.

2.7.2 Normes et réglementations en matière de sécurité des données médicales

Avec la numérisation croissante des systèmes de santé, la sécurisation des données médicales est devenue une priorité pour les gouvernements et les organismes internationaux. Plusieurs réglementations et normes ont été mises en place afin d'encadrer la collecte, le stockage et la transmission des informations de santé, garantissant ainsi leur confidentialité, intégrité et disponibilité. Parmi les principales normes figurent :

- **HIPAA (Health Insurance Portability and Accountability Act) :** Adoptée en 1996, l'HIPAA impose des règles strictes sur la protection des dossiers médicaux électroniques et

la gestion des informations de santé. Elle établit des normes pour limiter l'accès non autorisé aux données médicales et garantir leur chiffrement et anonymisation [45].

- **RGPD (General Data Protection Regulation) :** Le RGPD, mis en vigueur en 2018, impose un cadre juridique rigoureux pour le traitement des données personnelles, y compris les informations médicales. Il exige le consentement explicite des patients, la mise en place de mesures de sécurité renforcées et la notification obligatoire en cas de violation de données [46].
- **ISO/IEC 27001 et ISO/IEC 27799 (International Organization for Standardization/International Electrotechnical Commission) :** Ces normes de (ISO) définissent les bonnes pratiques pour la gestion de la sécurité de l'information dans les systèmes de santé. L'ISO/IEC 27799 est une extension de l'ISO/IEC 27001, spécifique aux organismes médicaux, fournissant des recommandations pour la protection des données de santé électroniques [47].
- **HITECH Act (Health Information Technology for Economic and Clinical Health Act) :** Cette loi, adoptée en 2009, renforce les dispositions de l'HIPAA en introduisant des sanctions plus strictes en cas de fuite de données médicales. Elle encourage également l'adoption des dossiers médicaux électroniques sécurisés et impose des obligations de notification en cas d'atteinte à la confidentialité des informations [48].
- **NIST SP 800-53 (National Institute of Standards and Technology Special Publication) :** Cette directive fournit un ensemble de mesures de cybersécurité pour les systèmes d'information, y compris les réseaux médicaux intelligents. Elle recommande l'utilisation de chiffrement avancé, d'authentification multifactorielle et de détection d'intrusion pour sécuriser les données médicales [49].

Dans les réseaux radio cognitifs appliqués à la santé, ces réglementations doivent être intégrées aux protocoles de sécurité afin de protéger la transmission des données médicales contre les cyberattaques. L'adoption de chiffrement de bout en bout, de protocoles d'authentification robustes de solutions de détection d'intrusion est essentielle pour assurer la sécurité des échanges médicaux et garantir leur conformité aux exigences légales et normatives.

2.7.3 Étude de cas sur les violations de la sécurité des données médicales dans les réseaux radio cognitifs

Les infrastructures de santé sont des cibles privilégiées pour les cyberattaques en raison de la valeur et de la sensibilité des données médicales qu'elles manipulent. Les réseaux radio cognitifs, bien qu'innovants en matière de gestion du spectre, présentent des vulnérabilités exploitables par des attaquants cherchant à compromettre la confidentialité, l'intégrité et la disponibilité des données médicales. Plusieurs incidents illustrent ces menaces :

- Cyberattaque contre un hôpital via le réseau radio cognitif : L'exploitation des failles de gestion des fréquences dans un réseau radio cognitive a permis à des cybercriminels d'intercepter et de modifier des prescriptions électroniques. En manipulant les transmissions entre les dispositifs médicaux connectés, les attaquants ont introduit des erreurs dans les dossiers patients, compromettant la sécurité des soins administrés. Cet incident met en

lumière l'importance de mécanismes robustes de chiffrement et d'authentification pour empêcher l'accès non autorisé aux communications médicales.

- Attaque par saturation du canal de contrôle : Le bon fonctionnement des CRN repose sur l'échange de signaux de contrôle permettant une allocation dynamique et efficace du spectre. Cependant, des attaquants ont utilisé une attaque de saturation du canal de contrôle en envoyant un grand nombre de requêtes falsifiées à travers des nœuds cognitifs compromis. Cette surcharge artificielle a entraîné une congestion du réseau, retardant ou bloquant la transmission de données critiques, telles que les signaux vitaux des patients en soins intensifs. Une telle attaque démontre la nécessité de solutions de détection d'anomalies et de gestion des priorités pour garantir la continuité des services médicaux.
- Exploitation des identités multiples dans un environnement médical : Dans cette attaque, un cybercriminel a généré plusieurs identités fictives au sein du réseau radio cognitif, perturbant ainsi les processus de routage et d'allocation du spectre. En conséquence, des flux de données médicales ont été redirigés vers des nœuds malveillants, permettant le vol ou la falsification des informations confidentielles des patients. Cette compromission de la confidentialité souligne l'urgence d'adopter des mécanismes d'authentification capables de détecter ces comportements anormaux.

2.7.4 Renforcement de la sécurité des CRNs pour la protection des données médicales

Face aux nombreuses menaces pesant sur la sécurité des données médicales dans les réseaux radio cognitifs, il est essentiel de mettre en place des stratégies de cybersécurité robustes et adaptées à leur nature dynamique. Plusieurs approches peuvent être adoptées pour garantir la confidentialité, l'intégrité et la disponibilité des informations échangées.

Tout d'abord, la mise en œuvre de mécanismes avancés de protection des communications est primordiale afin d'empêcher toute interception ou altération des données médicales sensibles. Assurer une gestion rigoureuse des accès au réseau à travers des méthodes d'authentification strictes permet également de limiter les risques d'intrusion et de falsification des identités.

Par ailleurs, la surveillance continue du réseau à l'aide de systèmes capables de détecter et d'analyser les comportements suspects est indispensable pour réagir rapidement aux tentatives d'attaques. Ces solutions doivent être couplées à des politiques de gestion intelligente du trafic, permettant de hiérarchiser les transmissions en fonction de leur criticité, notamment pour les applications médicales nécessitant une faible latence et une grande fiabilité.

En somme, l'optimisation de la sécurité des CRNs dans le domaine médical repose sur une approche globale intégrant des mesures de prévention, de détection et de réaction face aux cybermenaces. L'adoption de stratégies adaptées aux exigences spécifiques du secteur de la santé est essentielle pour garantir la protection des données des patients et assurer la continuité des services médicaux en toute sécurité.

2.7.5 Défis actuels et futurs de la sécurité des données médicales dans les réseaux radio cognitifs

Les réseaux radio cognitifs offrent des opportunités considérables pour optimiser l'utilisation du spectre et améliorer la connectivité dans le domaine de la santé. Cependant, leur intégration soulève d'importants défis en matière de cybersécurité. L'une des principales difficultés réside dans l'absence de standardisation des protocoles de sécurité, rendant complexe la mise en place de mécanismes de protection uniformes. De plus, le caractère dynamique du spectre limite l'efficacité des approches de défense traditionnelles, qui reposent souvent sur des règles fixes et statiques. L'hétérogénéité des dispositifs médicaux connectés constitue un autre défi majeur, ces équipements étant parfois dotés de capacités de calcul limitées, ce qui restreint l'implémentation de solutions de sécurité avancées.

L'essor de l'intelligence artificielle et du machine learning dans le domaine de la cybersécurité représente une avancée prometteuse pour la protection des CRN, mais il apporte également de nouvelles vulnérabilités. En effet, des attaques adversaires peuvent être dirigées contre les algorithmes de détection d'intrusion, faussant leurs analyses et rendant plus difficile l'identification des menaces réelles. De plus, l'usage de modèles d'IA malveillants pour manipuler les décisions d'allocation du spectre constitue un risque grandissant. Malgré ces défis, l'amélioration continue des systèmes d'apprentissage automatique permet de développer des mécanismes de sécurité plus intelligents, capables d'anticiper et de contrer efficacement les cyberattaques émergentes.

Par ailleurs, la mise en place de solutions de chiffrement adaptées est essentielle pour garantir la confidentialité et l'intégrité des données médicales transitant dans les CRN. Dans ce contexte, le chiffrement hybride apparaît comme une approche efficace combinant les avantages du chiffrement symétrique et asymétrique. Cette méthode permet d'accélérer le processus de chiffrement grâce aux algorithmes symétriques tout en assurant une gestion sécurisée des clés via des techniques asymétriques. Son utilisation dans les CRN renforce ainsi la protection des échanges de données médicales sensibles, tout en maintenant un bon niveau de performance et d'efficacité énergétique pour les dispositifs médicaux aux ressources limitées.

Pour renforcer la résilience des CRNs dans les environnements médicaux, des efforts de normalisation sont indispensables. L'élaboration de nouvelles normes et protocoles sécurisés garantira une meilleure interopérabilité entre les dispositifs médicaux connectés et les infrastructures de communication cognitives. Par ailleurs, des technologies innovantes, telles que la blockchain et la cryptographie post-quantique, sont actuellement explorées afin d'apporter des garanties supplémentaires en matière de protection des données médicales. Face aux menaces en constante évolution, une approche proactive et multidimensionnelle s'impose pour assurer la sécurité des informations médicales et préserver la confiance des utilisateurs dans ces systèmes intelligents.

2.8 Conclusion

En conclusion, la sécurité des réseaux radio cognitifs est un enjeu majeur pour garantir la confidentialité, l'intégrité et la disponibilité des données, en particulier dans des domaines sensibles comme la santé. Ces réseaux, bien qu'innovants et dynamiques, présentent des vulnérabilités spécifiques, notamment en raison de leur capacité d'adaptation constante aux changements du spectre et de la diversité des dispositifs utilisés. Les menaces qui pèsent sur les CRN, telles que les attaques par interception, usurpation d'identité, ou saturation des canaux, peuvent compromettre la sécurité des données sensibles comme les dossiers médicaux électroniques, les prescriptions ou les résultats d'examens.

Pour assurer la protection de ces données, qui revêtent une importance capitale dans le secteur de la santé, il est impératif d'adopter des mécanismes de sécurité adaptés aux spécificités des CRN. Le chiffrement des données, la gestion des accès, ainsi que la surveillance continue à travers des systèmes de détection d'intrusions sont des solutions essentielles pour préserver la confidentialité et l'intégrité des informations médicales. De plus, la segmentation du trafic et la priorisation des données critiques permettent de maintenir une qualité de service optimale, surtout lorsqu'il s'agit de transmettre des informations sensibles en temps réel.

À mesure que les technologies évoluent, les défis liés à la sécurité des données médicales dans les réseaux radio cognitifs se multiplient, notamment avec l'intégration de l'intelligence artificielle et des systèmes autonomes. L'adoption de mesures de sécurité innovantes, combinées à une approche proactive de gestion des risques, est donc essentielle pour protéger les informations médicales contre les cyberattaques. Le développement de nouvelles normes et de protocoles de sécurité, prenant en compte l'hétérogénéité des dispositifs et des infrastructures, est crucial pour garantir une sécurité continue et fiable dans ces réseaux de plus en plus utilisés dans le secteur de la santé.

Dans le prochain chapitre nous allons proposer des contributions de sécurisation des données médicales dans le cadre de l'optimisation des réseaux radio cognitifs.

Chapitre 3

Contributions proposées pour la sécurisation des réseaux radio cognitifs

Sommaire

3.1 Introduction

La problématique de la sécurité s'impose aujourd'hui comme une priorité majeure dans les réseaux radio cognitifs, en particulier en raison de leur fonctionnement dynamique et de l'accès opportuniste au spectre. Cette nature ouverte et flexible les rend vulnérables à diverses menaces, d'où la nécessité de mettre en place des mécanismes de protection fiables et adaptatifs.

Dans cette optique, les SMA (Systèmes Multi-Agents) offrent une approche pertinente pour gérer de manière intelligente et autonome les ressources disponibles dans les RRC. Grâce à leur capacité à négocier, coopérer et prendre des décisions distribuées, les SMA s'intègrent naturellement dans cet environnement complexe.

Ce chapitre présente nos contributions proposées pour renforcer la sécurité dans les RRC. Nous commençons par explorer les notions clés liées aux SMA, telles que les types d'agents, leur architecture, leur environnement d'interaction, ainsi que les formes d'organisation possibles. Ensuite, nous abordons les méthodes de décision multicritère, essentielles pour guider les processus de sélection et d'allocation des ressources. Enfin, nous détaillons les différentes approches développées dans ce travail, combinant négociation, filtrage des utilisateurs malveillants, sélection optimale par TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution) qui est une approche d'aide à la décision multicritère. Enfin, le chapitre se conclut par la sécurisation des données médicales via des techniques de chiffrement avancées.

3.2 Systèmes multi-agents dans la radio cognitive

Les SMA jouent un rôle clé dans la gestion distribuée et intelligente des environnements dynamiques. Dans le contexte de la radio cognitive, ils permettent de modéliser des entités autonomes capables d'observer leur environnement, de prendre des décisions localement, et de coopérer entre elles afin d'optimiser l'utilisation des ressources. Chaque agent agit de manière autonome tout en interagissant avec les autres pour coordonner les actions, résoudre d'éventuels conflits, et s'adapter en temps réel aux changements. Cette approche offre une grande flexibilité, améliore la robustesse du système global et permet une meilleure réactivité face à la variabilité des conditions, en supprimant le besoin d'un contrôle centralisé.

3.2.1 Définition et concept de base des systèmes multi-agents

Les SMA sont des systèmes composés d'un ensemble d'agents intelligents et autonomes, capables d'interagir entre eux ainsi qu'avec leur environnement pour atteindre des objectifs spécifiques, qu'ils soient individuels ou collectifs [1]. Chaque agent dispose d'une vision locale du problème et de compétences propres, et leur collaboration permet de distribuer l'intelligence dans le système [2].

Les (SMA) sont particulièrement adaptés aux environnements dynamiques, distribués et complexes, où les approches centralisées deviennent limitées. Grâce à leur capacité à coopérer, à s'adapter et à coordonner leurs actions, les SMA offrent des solutions décentralisées, réactives

et robustes, favorisant une meilleure répartition des tâches et une gestion efficace de la complexité.

L'approche des voyelles (A, E, I, O) proposée par Demazeau [3] constitue un cadre d'analyse structuré pour la conception des systèmes multi-agents. Elle repose sur quatre dimensions essentielles : les Agents (A), l'Environnement (E), les Interactions (I) et l'Organisation (O), permettant ainsi une modélisation claire et cohérente des SMA.

3.2.2 Notion d'agent

Le concept d'agent est omniprésent dans le domaine des systèmes distribués et intelligents, et son interprétation varie selon les perspectives théoriques et les domaines d'application. Dans le domaine de la radio cognitive, un agent est généralement défini comme une entité autonome capable de percevoir son environnement radio, de traiter les informations reçues et d'agir pour accomplir des objectifs spécifiques, comme l'optimisation de l'utilisation du spectre ou la gestion dynamique des ressources. Cette capacité à agir indépendamment et de manière dirigée en fonction de l'environnement fait de l'agent un élément central dans les systèmes multi-agents. Parmi les caractéristiques essentielles d'un agent, on retrouve l'autonomie (fonctionnement sans supervision externe), la proactivité (initiation d'actions selon ses objectifs), la réactivité (adaptation aux changements de l'environnement), la sociabilité (capacité à interagir avec d'autres agents), et, parfois, l'apprentissage (adaptation par l'expérience). Ces attributs sont cruciaux pour modéliser des comportements intelligents et adaptatifs, en particulier dans des contextes complexes et dynamiques, comme le soulignent des travaux récents sur les systèmes multi-agents appliqués à la radio cognitive [4]. En définitive, les agents offrent un cadre puissant pour la conception de systèmes distribués, coopératifs et flexibles, capables de s'adapter à des environnements en constante évolution.

a) Categories d'agents

Dans les (SMA), les agents sont généralement classés en trois catégories principales : les agents réactifs, les agents cognitifs et les agents hybrides [5]. Cette classification repose sur leur complexité, leurs capacités de raisonnement et leur mode d'interaction avec l'environnement.

- **Agents réactifs :** Les agents réactifs fonctionnent selon un modèle *stimulus-réponse*, réagissant directement aux stimuli de l'environnement sans mémoire des actions passées ni raisonnement complexe. Ils n'ont pas de représentation interne de l'environnement et opèrent selon des règles prédéfinies. Individuellement simples, ils peuvent collectivement engendrer des comportements complexes.

Cependant, leur absence de but explicite ou de stratégie globale peut rendre incertaine la convergence vers une solution optimale ou stable. Néanmoins, leur rapidité de réaction les rend adaptés aux environnements dynamiques où la vitesse est primordiale.

- **Agents cognitifs :** Les agents cognitifs possèdent des capacités avancées de traitement de l'information et de prise de décision. Ils disposent d'une représentation explicite de leur

environnement, d'une mémoire et souvent d'une base de connaissances leur permettant d'adopter un comportement réfléchi [6]. Ces agents sont capables de planifier des actions en fonction de leurs objectifs et de leurs perceptions, et peuvent ajuster leur comportement à partir d'expériences passées. Inspirés des travaux en intelligence artificielle, ils sont souvent dits "intentionnels", car guidés par des buts et utilisent des plans pour les atteindre.Des recherches récentes ont exploré l'intégration de modèles cognitifs dans les SMA pour améliorer la coordination et l'apprentissage collectif. Par exemple, Nguyen et al dans [7] ont proposé des variantes de l'apprentissage basé sur la théorie de l'apprentissage par instances (Instance-Based Learning Theory - IBLT) pour améliorer la coordination dans des tâches multi-agents dynamiques avec des récompenses stochastiques.

- **Agents hybrides :** Les agents hybrides combinent les avantages des agents réactifs et cognitifs pour pallier leurs limites respectives. Ils intègrent généralement une architecture en couches : une couche réactive pour répondre rapidement aux événements urgents, et une ou plusieurs couches cognitives pour gérer des décisions plus complexes ou stratégiques. Cette approche permet une adaptabilité et une efficacité accrues, notamment dans des environnements hétérogènes où réactivité et planification doivent coexister.

b) Modèles d'architecture pour agents

L'architecture d'un agent correspond à son organisation interne, c'est-à-dire la manière dont sont structurées ses données, ses mécanismes de traitement de l'information, ainsi que le contrôle de ses actions. Le choix de l'architecture dépend fortement du type d'agent et des exigences de l'application cible, en particulier dans des contextes dynamiques comme la radio cognitive.

- **Architecture réactive :** Les architectures réactives sont conçues pour fournir des réponses rapides à des stimuli provenant de l'environnement, sans recourir à une représentation symbolique ou à un raisonnement complexe. L'agent se comporte de manière réflexe selon un schéma stimulus-réponse. La plus célèbre de ces architectures est celle de subsomption, proposée par Rodney Brooks, où les comportements sont organisés en couches hiérarchiques [8]. Chaque couche gère un ensemble de tâches simples et peut inhiber ou subsumer les actions des couches inférieures, favorisant des comportements adaptatifs. La Figure 3.1 illustre le principe de l'architecture de subsomption, mettant en évidence l'organisation en couches hiérarchisées et leur mode d'interaction.

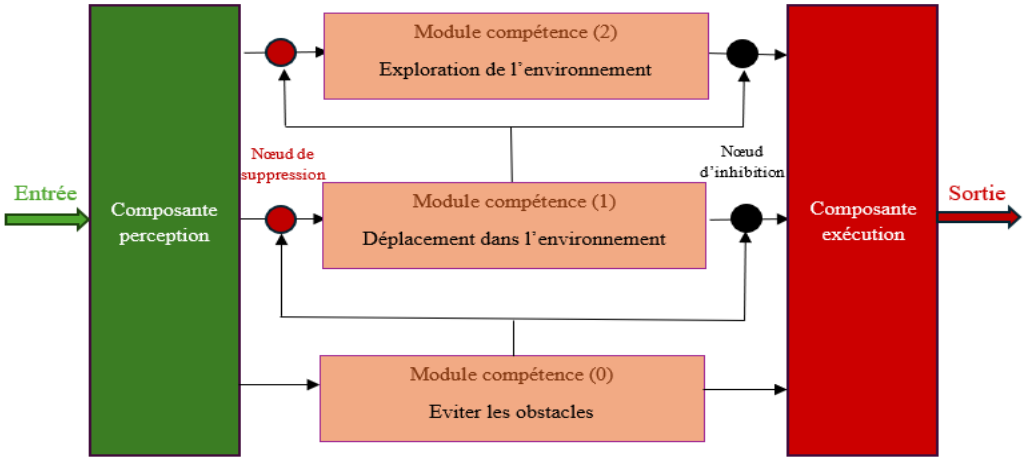


Figure 3.1: Schéma de l'architecture réactive de type subsomption.

Ce schéma illustre une architecture en couches hiérarchisées où chaque module, appelé « comportement », est responsable d'une tâche spécifique. Les couches inférieures gèrent des comportements simples et rapides, tandis que les couches supérieures encadrent des actions plus abstraites. Chaque couche peut inhiber ou subsumer les actions des couches sous-jacentes pour générer un comportement global adaptatif. L'interaction directe avec l'environnement se fait via les entrées sensorielles et les sorties motrices, sans modélisation symbolique explicite.

- **Architecture cognitive :** Les agents cognitifs reposent sur des modèles mentaux explicites. L'architecture BDI (Belief, Desire, Intention) est l'un des cadres les plus influents. Elle modélise le comportement d'un agent à partir de ses croyances (informations sur l'environnement), désirs (objectifs ou états souhaités) et intentions (plans que l'agent décide de poursuivre). L'agent met à jour ses croyances via la perception, génère des désirs selon ses motivations, puis sélectionne les intentions à exécuter en tenant compte de contraintes contextuelles et de préférences. Cette approche permet une prise de décision plus réfléchie, adaptée aux environnements complexes, mais exige davantage de ressources computationnelles. La Figure 3.2 illustre l'architecture fonctionnelle d'un agent BDI, mettant en évidence le flux d'informations entre croyances, désirs, intentions, et plans d'action [9].

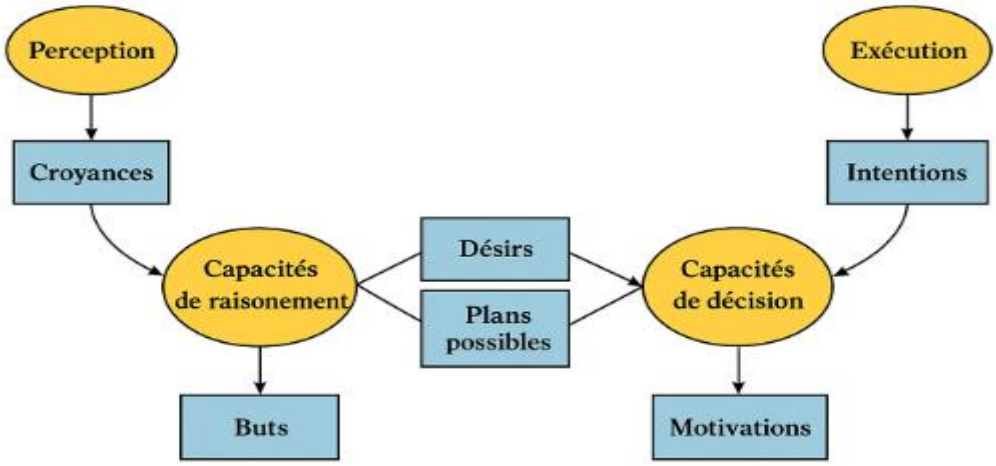


Figure 3.2 : Schéma de l'architecture cognitive de type BDI [9].

L'architecture BDI structure le raisonnement de l'agent autour d'un cycle de perception, de mise à jour des croyances, de génération de désirs et de sélection d'intentions [10]. Elle permet de formaliser la prise de décision à partir d'attitudes mentales, ce qui rend l'agent capable d'agir de manière autonome dans un environnement dynamique.

- **Architecture hybride :** Pour pallier les limites des architectures purement réactives ou cognitives, des architectures hybrides ont été développées. Elles intègrent à la fois des modules réactifs (pour la rapidité) et des composants cognitifs (pour la délibération), souvent organisés en couches. Une architecture bien connue est InteRRaP (Integration of Reactive behavior and Rational Planning), qui combine raisonnement délibératif, planification et réactivité. La Figure 3.3 représente cette architecture, illustrant l'organisation hiérarchique des couches de contrôle et des bases de connaissances associées.

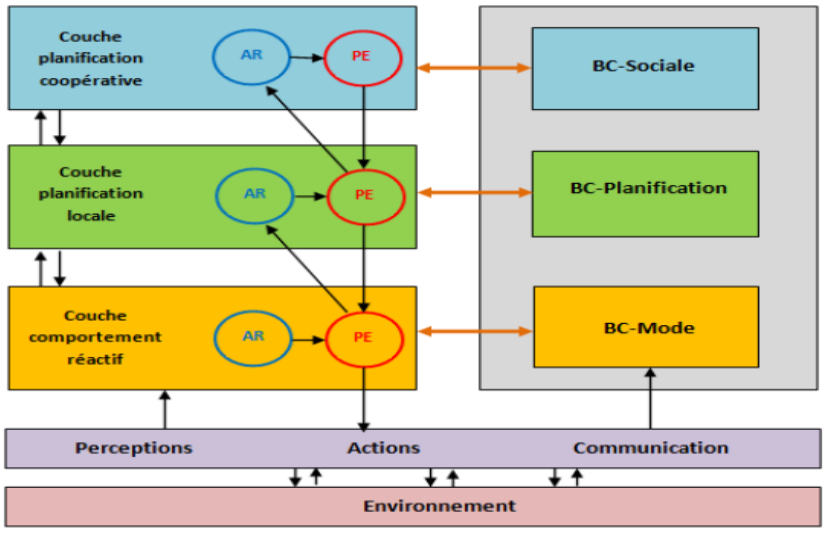


Figure 3.3 : Schéma de l'architecture hybride InteRRaP [9].

L'architecture InteRRaP repose sur trois couches hiérarchiques, chacune étant dotée de sa propre base de connaissances et de modules fonctionnels. Ces couches représentent différents niveaux d'abstraction de l'agent et de son environnement. Le contrôle se transmet de bas en haut : lorsqu'une couche ne peut plus progresser vers l'objectif, la couche supérieure prend le relais. Chaque niveau intègre deux modules : un pour la reconnaissance des situations et l'activation des buts (AR), l'autre pour la planification et l'exécution (PE).

Les perceptions circulent du bas vers le haut dans la hiérarchie, tandis que les actions sont décidées en haut puis descendues vers l'environnement pour exécution. Les bases de connaissances sont réparties comme suit :

- ✓ **BC-Monde** : croyances sur l'environnement,
- ✓ **BC-Planification** : plans disponibles pour atteindre les buts,
- ✓ **BC-Sociale** : connaissances sur les autres agents et leur capacité à coopérer.

InteRRaP s'avère performant dans des contextes dynamiques. Toutefois, son principal inconvénient reste l'absence de formalisme rigoureux et de méthodologie standard pour sa conception, contrairement à l'approche BDI classique [11].

3.2.3 Environnement

Dans un système multi-agents (SMA), l'environnement joue un rôle central, il constitue le cadre dans lequel les agents évoluent, interagissent et agissent. La relation entre un agent et son environnement est bidirectionnelle : l'agent perçoit l'environnement à travers ses capteurs, prend des décisions via ses mécanismes internes, puis agit à l'aide de ses effecteurs. En retour, l'environnement peut influencer ou modifier le comportement de l'agent.

L'environnement peut être modélisé comme un ensemble d'états possibles, et ses caractéristiques impactent directement la conception des agents, notamment leur capacité à s'adapter aux changements ou à anticiper les actions des autres agents. Par exemple, dans un environnement partagé par plusieurs agents, les perceptions deviennent incertaines et l'évolution de l'état peut dépendre de multiples facteurs extérieurs.

Selon la classification de Russell et Norvig [12], plusieurs propriétés permettent de caractériser un environnement :

- **Accessibilité** : Un environnement est dit accessible si l'agent peut obtenir toutes les informations pertinentes pour ses décisions. Sinon, il est considéré comme partiellement observable.
- **Déterminisme** : Si chaque action entraîne un résultat prévisible et unique, l'environnement est déterministe. Sinon, il est indéterministe, introduisant une incertitude dans la prise de décision.
- **Épisodicité** : Dans un environnement épisodique, les décisions de l'agent sont indépendantes des épisodes précédents. À l'inverse, un environnement non-épisodique nécessite une mémoire et une planification plus avancées.

- **Dynamisme** : Un environnement est statique si ses changements ne dépendent que des actions de l'agent. Il devient dynamique s'il évolue également en l'absence d'intervention de l'agent.
- **Discrétisation** : Un environnement est discret s'il comporte un nombre fini d'états, d'actions et de perceptions. Il est continu lorsque les transitions entre états sont graduelles et potentiellement infinies.

3.2.4 Interactions

Dans (SMA), chaque agent peut influencer le comportement des autres agents à travers des interactions. Ces interactions, qui sont des échanges d'actions réciproques, peuvent être divisées en trois phases : la réception d'informations, l'analyse de ces informations par les agents, et l'exécution d'actions ou l'envoi de messages qui modifient l'environnement.
La **coopération** désigne un processus où les agents travaillent ensemble pour atteindre un objectif commun. Elle est caractérisée par l'interdépendance des actions des agents et la fréquence de leurs communications.
La **coordination** est essentielle pour organiser l'action des agents afin d'éviter des comportements chaotiques. Elle implique l'allocation des ressources rares et la communication des résultats intermédiaires entre agents. Une coordination centralisée, par un agent unique, n'est pas toujours viable dans un système décentralisé, car elle limiterait l'autonomie des agents.
La **négociation** permet aux agents autonomes de parvenir à un accord sur des objectifs partagés, surtout lorsque des conflits d'intérêts surviennent. Le protocole de négociation, qui varie en fonction du contexte, définit la manière dont les agents échangent des propositions et tentent de trouver un compromis.
Concernant la **communication**, les agents peuvent interagir en envoyant des messages ou en accédant à une base de données partagée. Le succès de cette communication repose sur l'utilisation d'un langage commun et de protocoles d'interaction. Les protocoles garantissent que les messages envoyés entre agents respectent certaines règles et sont interprétés correctement.
Pour le **transport de messages**, les agents utilisent diverses technologies, comme les sockets ou RMI (Remote Method Invocation), afin de garantir un échange efficace des données entre eux.
Enfin, des **langages de communication** comme KQML (Knowledge Query and Manipulation Language) et FIPA-ACL (Foundation for Intelligent Physical Agents - Agent Communication Language) permettent d'assurer une communication structurée entre agents. KQML se concentre sur des actes de langage standard, tandis que FIPA-ACL introduit une sémantique pour clarifier la signification des messages échangés [13].

3.2.5 Organisation

L'organisation des agents dans un système multi-agents définit la manière dont ils sont structurés et interagissent entre eux pour accomplir des tâches communes. Plusieurs types d'organisation existent [14] :

- **Hiérarchies :** Les agents sont organisés en structure arborescente, chaque agent ayant un lien d'autorité sur ses sous-ordonnés, permettant ainsi de décomposer les tâches globales du système.
- **Holarchies :** Similaire à la hiérarchie, mais sans relation d'autorité directe. Les sous-groupes sont formés physiquement par les agents eux-mêmes.
- **Coalitions :** Des alliances temporaires où les agents unissent leurs forces lorsque leurs intérêts individuels se rencontrent, avec une valeur collective supérieure à la somme des valeurs individuelles.
- **Équipes :** Les agents travaillent ensemble pour atteindre des objectifs communs, cherchant à maximiser les intérêts de l'équipe plutôt que ceux de l'individu.
- **Congrégations :** Similaires aux coalitions et équipes, mais permanentes et ayant plusieurs objectifs. Les agents peuvent y entrer ou en sortir et appartenir à plusieurs congrégations.
- **Sociétés :** Un ensemble d'agents variés avec différents objectifs, niveaux de rationalité et capacités, mais soumis à des règles communes.
- **Fédérations :** Les agents cèdent une partie de leur autonomie à un délégué, avec des interactions limitées entre les agents et leurs délégués.
- **Marchés :** Un modèle où des agents vendeurs et acheteurs échangent des biens, simulant des marchés réels ou testant des stratégies de négociation.
- **Matrices :** Les agents sont hiérarchisés, mais contrairement à la hiérarchie classique, chaque agent peut être subordonné à plusieurs autres agents.
- **Combinaisons :** Mélange de plusieurs types d'organisation, comme une fédération de coalitions ou une hiérarchie d'équipes.

3.3 Décision multicritère dans la radio cognitive

Dans les réseaux radio cognitifs, la prise de décision est souvent complexe en raison de la variabilité de l'environnement radio, de la coexistence de multiples utilisateurs, et des contraintes techniques en temps réel. Pour y faire face, les systèmes multi-agents sont de plus en plus utilisés, chaque agent étant chargé d'observer, d'analyser et d'agir de manière autonome ou en coopération avec d'autres agents.

La décision multicritère dans ce contexte désigne un processus dans lequel un ou plusieurs agents évaluent un ensemble d'alternatives (par exemple, des canaux, des bandes de fréquence, des stratégies d'accès) selon plusieurs critères souvent conflictuels, tels que : la qualité du signal, le taux d'occupation du canal, le prix, la consommation d'énergie, le délai de transmission, ou encore l'interférence générée [15]. Chaque critère est pondéré selon son importance relative pour le système ou les objectifs de l'agent, et les différentes alternatives sont évaluées globalement afin de sélectionner celle qui optimise le compromis entre ces critères. Des méthodes comme TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution), AHP (Analytical Hierarchy Process), ELECTRE (ELimination Et Choix Traduisant la REalité), PROMETHEE (Preference Ranking Organization METHod for Enrichment of Evaluations), ANP (Analytical Network Process) ou VIKOR (VIseKriterijumska Optimizacija I Kompromisno Resenje) peuvent être intégrées dans l'architecture décisionnelle des agents pour assurer une sélection optimale et adaptative dans

des environnements dynamiques. La Figure 3.4 illustre les principales méthodes de décision multicritère (MCDM) couramment utilisées dans divers secteurs. Chacune de ces méthodes se distingue par ses spécificités propres et offre une grande flexibilité d'application à travers de nombreux contextes.

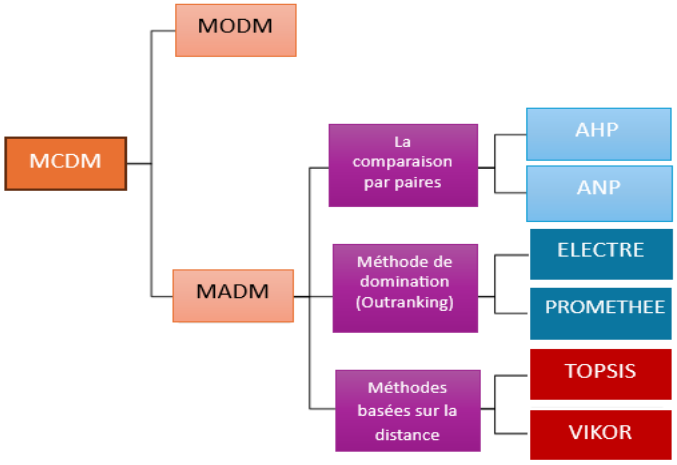


Figure 3.4 : Vue d'ensemble des approches de décision multicritère (MCDM).

Les approches de décision multicritère MCDM (Multi Criteria Decision Making) se déclinent principalement en deux sous-catégories : la prise de décision multi-attributs MADM (Multi-Attribute Decision Making) et la prise de décision multi-objectifs MODM (Multi-Objective Decision Making). La MADM s'applique lorsque le décideur doit choisir parmi un ensemble fini d'alternatives, en tenant compte de plusieurs critères évalués individuellement ou comparativement. Elle regroupe des méthodes comme AHP, ANP, ELECTRE, PROMETHEE ainsi que TOPSIS et VIKOR. En revanche, la MODM concerne des situations où les alternatives sont infinies et où plusieurs fonctions objectives doivent être optimisées simultanément.

La MCDM permet aux agents d'un réseau radio cognitif de prendre des décisions intelligentes, robustes et justifiables, même en présence d'incertitudes, de contraintes multiples et d'informations partielles.

- **Méthode AHP**

L'Analytic Hierarchy Process (AHP), ou processus hiérarchique analytique en français, est une méthode d'aide à la décision développée par Thomas Saaty dans les années 1970[16]. Elle est particulièrement adaptée à la résolution de problèmes complexes impliquant plusieurs critères, parfois contradictoires. Son principal atout réside dans sa capacité à structurer un problème en une hiérarchie claire et logique, facilitant ainsi l'analyse et la prise de décision.

La méthode repose sur la décomposition du problème en plusieurs niveaux hiérarchiques : l'objectif global au sommet, suivi des critères (et éventuellement des sous-critères), puis des alternatives à évaluer. À chaque niveau, l'AHP utilise des comparaisons par paires entre les éléments, en se basant sur l'appréciation subjective du décideur, pour établir une matrice de jugement. Ces comparaisons permettent de quantifier l'importance relative des éléments en jeu grâce à une échelle fondamentale de Saaty (généralement de 1 à 9). Une fois les comparaisons

effectuées, des calculs mathématiques (notamment à l'aide de vecteurs propres) permettent d'obtenir des poids ou priorités relatifs pour chaque critère et alternative. L'alternative ayant le score global le plus élevé est alors considérée comme la meilleure option selon les préférences exprimées.

- **Méthode ANP**

La méthode ANP est une extension de l'AHP conçue pour traiter des problèmes de décision plus complexes où les critères ou alternatives ne sont pas indépendants. Développée par Thomas Saaty, cette approche repose sur une structure en réseau plutôt qu'en hiérarchie, ce qui permet de modéliser les interactions et dépendances entre les éléments du système décisionnel [17]. Contrairement à l'AHP, où les relations entre critères sont supposées unidirectionnelles et indépendantes, l'ANP permet de représenter des influences réciproques (feedback) entre critères, sous-critères et alternatives.

Le processus ANP se déroule en plusieurs étapes clés : d'abord, le problème est structuré sous forme de réseau ; ensuite, des comparaisons par paires sont réalisées entre les éléments liés ; une super-matrice est ensuite construite pour intégrer les résultats ; enfin, une synthèse est effectuée pour déterminer les alternatives les plus adaptées. Ce modèle se montre particulièrement efficace dans des contextes où la complexité et les relations croisées entre facteurs jouent un rôle crucial, comme dans les systèmes multi-agents ou les environnements dynamiques tels que les réseaux radio cognitifs.

Il convient toutefois de noter que l'ANP requiert un certain niveau d'expertise et peut impliquer un investissement important en temps, notamment en raison de la nécessité de recourir à des outils spécialisés tels que Super Decisions ou ANPSolver[18]. En dépit de ces exigences, l'ANP se démarque par sa grande flexibilité et sa capacité à modéliser finement les dépendances entre critères, ce qui en fait un excellent choix pour les situations nécessitant une décision multicritère rigoureuse et bien informée.

- **Méthode ELECTRE**

La méthode ELECTRE appartient à la famille des méthodes de sur classement (ou outranking), largement utilisées en décision multicritère lorsqu'il s'agit de comparer des alternatives selon plusieurs critères, parfois contradictoires [19]. Plutôt que de rechercher une solution optimale unique, cette approche vise à identifier les alternatives qui surpassent les autres selon un certain nombre de critères, tout en tenant compte des désaccords éventuels. Elle repose sur trois éléments fondamentaux : la fonction seuil, l'indice de concordance (mesurant à quel point une alternative est au moins aussi bonne qu'une autre sur un ensemble de critères), et l'indice de discordance (détectant s'il existe un critère sur lequel une alternative est nettement inférieure à une autre).

Il existe plusieurs variantes d'ELECTRE, chacune conçue pour répondre à un type précis de problème : choix, classement ou tri [15]. Ces variantes sont récapitulées dans le tableau 3.1 qui associe chaque méthode à la nature du problème qu'elle permet de traiter.

Tableau 3.1 : Les variantes de la méthode ELECTRE selon le type de problème décisionnel.

Problème	Méthode
Problème de choix	ELECTRE I ELECTRE Iv ELECTRE IS
Problème de classement	ELECTRE II ELECTRE III ELECTRE IV ELECTRE SS
Problème de tri	ELECTRE TRI

Grâce à sa capacité à gérer des critères hétérogènes et des préférences parfois imprécises, ELECTRE s'avère particulièrement adapté aux systèmes complexes et dynamiques comme les réseaux radio cognitifs ou les systèmes multi-agents. En contrepartie, sa mise en œuvre peut nécessiter des outils spécialisés (ex. : DecisionLab, JElectre, MATLAB, Python), notamment pour le traitement des matrices de décision.

- **Méthode PROMETHEE**

La méthode PROMETHEE, développée par Jean-Pierre Brans en 1982, est une approche d'analyse multicritère utilisée pour classer des alternatives en fonction de plusieurs critères [20]. Elle repose sur des fonctions de préférence pour évaluer les différences entre les alternatives. PROMETHEE permet de traiter à la fois des critères qualitatifs et quantitatifs, en produisant un classement global des alternatives, du meilleur au moins bon.
Il existe plusieurs variantes de PROMETHEE adaptées à différents types de problèmes : PROMETHEE I pour le classement partiel, PROMETHEE II pour le classement complet, et d'autres versions comme PROMETHEE III et PROMETHEE IV pour des cas spécifiques.
La méthode suit un processus en plusieurs étapes : évaluation des alternatives, comparaison par paires, calcul des indices de dominance, et classement des alternatives. Bien que puissante et utilisée dans divers domaines, PROMETHEE peut devenir complexe lorsque de nombreux critères ou alternatives sont impliqués, et souffrir de l'inversion de rang lorsque de nouvelles alternatives sont ajoutées. Malgré ces défis, elle reste une méthode populaire pour la prise de décision multicritère.

- **Méthode VIKOR**

La méthode VIKOR est une technique d'aide à la décision multicritère particulièrement utile dans le domaine de la radio cognitive, où il est nécessaire de trouver un équilibre entre plusieurs objectifs souvent conflictuels, tels que la qualité de service, la sécurité du réseau, la

consommation d'énergie et l'efficacité spectrale. En évaluant les différentes alternatives selon plusieurs critères pondérés, VIKOR permet d'identifier une solution de compromis optimale en tenant compte à la fois de l'utilité collective (performance globale) et du regret individuel (écart par rapport à l'idéal). Grâce à sa capacité à hiérarchiser des solutions dans des environnements complexes, cette méthode s'avère pertinente pour la gestion dynamique du spectre, la sélection de canaux ou encore l'allocation des ressources dans les réseaux cognitifs [21]. Des variantes comme VIKOR flou peuvent également être utilisées lorsque les données disponibles sont imprécises ou incertaines, ce qui est fréquent dans les environnements radioélectriques dynamiques.

- **Méthode TOPSIS**

L'algorithme TOPSIS, proposé par Hwang et Yoon en 1981 [22], constitue une méthode de décision multicritère fondée sur l'analyse des distances euclidiennes. Son principe repose sur l'idée que la meilleure alternative est celle qui présente la plus grande proximité avec la solution idéale et, simultanément, l'éloignement maximal par rapport à la solution anti-idéale [23].
Dans ce contexte, les concepts de solution idéale et de solution anti-idéale sont définis de la manière suivante :

- ✓ **La solution idéale** correspond à un scénario dans lequel tous les critères bénéfiques sont maximisés, tandis que les critères de coût ou de désavantage sont minimisés [24]. Elle représente un point de référence optimal vers lequel tend la meilleure alternative.
- ✓ **La solution anti-idéale**, en revanche, se caractérise par les pires performances possibles, elle maximise les critères négatifs et minimise les critères positifs [24]. Elle symbolise l'option la moins souhaitable.

L'approche TOPSIS se distingue par sa simplicité de mise en œuvre et par sa capacité à fournir un classement relatif des alternatives en fonction de leur proximité relative aux solutions de référence. Elle est généralement structurée en plusieurs étapes successives [25], allant de la normalisation des données à la détermination des distances par rapport aux solutions idéales, jusqu'au calcul de l'indice de similarité qui permet de classer les options étudiées. Les étapes méthodologiques de l'algorithme TOPSIS sont présentées ci-après.

Étape 1 : Construction et normalisation de la matrice de décision

La première étape de l'algorithme TOPSIS consiste à construire une matrice de décision initiale $X=[x_{ij}]$, dans laquelle chaque élément x_{ij} représente la performance de l'alternative j selon le critère i.
Afin d'assurer la comparabilité des critères exprimés dans des unités différentes, cette matrice est ensuite normalisée. Une méthode couramment utilisée est la normalisation vectorielle, définie comme suit :

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \tag{3.1}$$

$$i = 1 \dots m \qquad j = 1 \dots n$$

Étape 2 : Élaboration de la matrice de décision normalisée pondérée

On applique les poids des critères à la matrice normalisée obtenue à l'étape 1.

$$v_{ij} = w_j * r_{ij} \tag{3.2}$$

$$i = 1 \dots m \qquad j = 1 \dots n$$

$$V = \begin{bmatrix} v_{11} & \cdots & v_{1n} \\ \vdots & \ddots & \vdots \\ v_{m1} & \cdots & v_{mn} \end{bmatrix} = \begin{bmatrix} w_1 \cdot r_{11} & \cdots & w_n \cdot r_{1n} \\ \vdots & \ddots & \vdots \\ w_1 \cdot r_{m1} & \cdots & w_n \cdot r_{mn} \end{bmatrix} \tag{3.3}$$

w_j: le poids du critère j

v_{ij} : l'élément de la matrice pondérée

Étape 3 : Calcul des solutions idéales et anti-idéales

$$V_j^+ = \{(\max(v_{ij}) \,|j \in J_1), (min(v_{ij})|j \in J_2)\} \tag{3.4}$$

$$V_j^- = \{(\min(v_{ij}) \,|j \in J_1), (max(v_{ij})|j \in J_2)\} \tag{3.5}$$

J_1: ensemble des critères de bénéfice

J_2: ensemble des critères de coût

Étape 4 : Calcul de la distance aux solutions idéales

Distance entre chaque alternative et la solution idéale :

$$S_i^+ = \sqrt{\sum_{j=1}^{n} (V_j^+ - V_{ij})^2} \tag{3.6}$$

Distance entre chaque alternative et la solution anti-idéale :

$$S_i^- = \sqrt{\sum_{j=1}^{n} (V_j^- - V_{ij})^2} \tag{3.7}$$

Étape 5 : Calcul de la proximité relative à la solution idéale

$$P_i^* = \frac{S_i^-}{S_i^- + S_i^+} \qquad 0 < P_i^* < 1 \tag{3.8}$$

Étape 6 : Classement selon l'indice de préférence

- Choisir l'alternative ayant le **plus grand indice de similarité** (problème de choix).
- Classer les alternatives par **ordre décroissant des indices de similarité** (problème de classement) [26].

3.4 Première contribution : Optimisation d'un utilisateur de radio cognitive multicritère par apprentissage autonome

3.4.1 Approche proposée

Notre approche repose sur un processus structuré visant à optimiser la négociation entre les utilisateurs secondaires (SUs) et les utilisateurs primaires (PUs) dans un environnement radio cognitive. Elle intègre à la fois des mécanismes de filtrage, de sélection et d'évaluation multicritère afin de garantir une attribution fiable et adaptée des ressources disponibles. Pour ce faire, un ensemble d'étapes est mis en place, chacune permettant d'affiner le processus de sélection du PU le plus approprié pour répondre aux besoins du SU :

Étape 1 : Identification des acteurs et mise en place du scénario

Dans notre approche, nous distinguons deux types d'acteurs dans l'environnement cognitif : les utilisateurs primaires, détenteurs des ressources spectrales, et les utilisateurs secondaires, qui cherchent à y accéder temporairement en fonction de leurs besoins spécifiques.

Nous avons adopté une stratégie de négociation de type un-à-plusieurs, dans laquelle un SU initie simultanément une négociation avec plusieurs PUs. Cette approche permet au SU de comparer plusieurs offres et de choisir celle qui répond le mieux à ses critères.

Dans notre scénario expérimental, le processus de négociation implique 10 utilisateurs primaires (PUs), comme illustré dans la Figure 3.5.

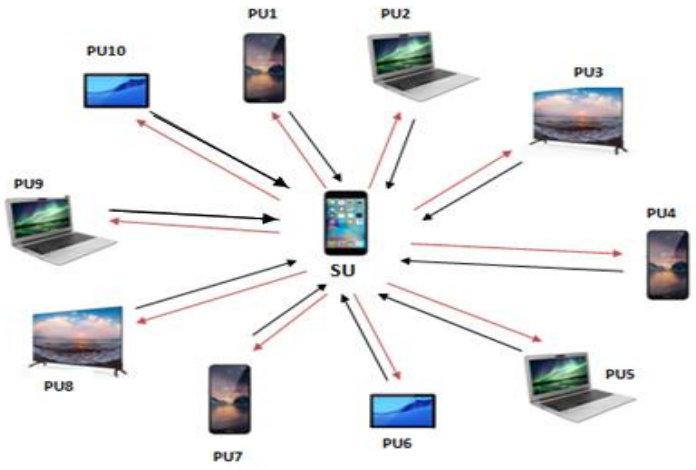


Figure 3.5 : Scénario proposé.

Étape 2 : Détection des utilisateurs primaires malveillants

Avant d'entamer toute négociation, il est primordial de s'assurer que seuls les utilisateurs primaires fiables participent au processus. Pour cela, nous avons intégré un mécanisme de détection basé sur la confiance, qui attribue à chaque PU un score de fiabilité. Ce score est établi en fonction de plusieurs critères :

- L'exactitude des informations fournies lors des négociations antérieures,

- La stabilité et la régularité du comportement du PU,
- Les évaluations fournies par d'autres SUs.

Les PUs dont le score de confiance est inférieur à un seuil prédéfini sont automatiquement considérés comme malveillants et sont exclus du processus de sélection. Cette étape garantit que seules les entités dignes de confiance peuvent interagir avec les utilisateurs secondaires, renforçant ainsi la sécurité du réseau.

Étape 3 : Envoi de la requête et réception des offres

Une fois les PUs malveillants filtrés, le SU peut envoyer une requête de négociation à l'ensemble des PUs restants, dans laquelle il spécifie le nombre de canaux requis.

À la réception de cette demande, chaque PU vérifie sa capacité à répondre à l'exigence en nombre de canaux. Ceux qui peuvent satisfaire cette condition retournent une offre détaillée comportant :

- Le nombre exact de canaux disponibles,
- La bande passante,
- La technologie utilisée,
- Le prix proposé,
- Le temps d'allocation possible.

Les PUs qui ne disposant pas du nombre de canaux requis seront rejeté dans l'étude suivante.

Étape 4 : Sélection du PU optimal à l'aide de TOPSIS

Après l'élimination des PUs non éligibles et malveillants, le SU dispose d'une liste restreinte de PUs fiables, répondant à ses critères techniques et économiques. À ce stade, nous appliquons l'algorithme multicritère TOPSIS, afin de déterminer le PU le plus adapté.

L'algorithme prend en entrée les valeurs des critères pour chaque utilisateur primaire (PU), à savoir : le nombre de canaux, la bande passante, la technologie, le prix et le temps d'allocation, ainsi que les poids relatifs attribués à chacun de ces critères en fonction des priorités définies par l'utilisateur secondaire (SU). En sortie, l'algorithme établit une classification des PUs selon leur proximité avec la solution idéale, et permet ainsi d'identifier celui qui répond le mieux aux besoins du SU.

3.4.2 Choix de l'algorithme TOPSIS et ses fonctions-objectifs dans la prise de décision multicritère

L'algorithme TOPSIS a été choisi pour cette approche en raison de ses avantages distinctifs par rapport à d'autres méthodes de décision multicritère. Bien qu'il existe un éventail d'algorithmes capables de traiter des problèmes de décision impliquant plusieurs critères,

TOPSIS se distingue par sa simplicité, son efficacité et sa capacité à fournir des solutions intuitives et compréhensibles.

Une des raisons principales de ce choix est que TOPSIS permet une comparaison directe des alternatives en fonction de leur proximité avec la solution idéale, une approche particulièrement adaptée aux décisions complexes qui impliquent plusieurs critères. Contrairement à d'autres méthodes comme l'AHP (Analytic Hierarchy Process) ou le VIKOR, qui exigent une hiérarchisation complexe des critères ou des pondérations souvent difficiles à définir de manière précise, TOPSIS simplifie le processus décisionnel en se basant exclusivement sur la distance euclidienne, facilitant ainsi l'analyse et la prise de décision.

En outre, TOPSIS est robuste et s'adapte facilement aux contextes où plusieurs critères doivent être pris en compte simultanément, ce qui est essentiel dans le cadre de notre approche de sélection des utilisateurs primaires (PU) dans les réseaux de radio cognitive. Cette capacité à traiter efficacement les compromis entre des critères variés — tels que la bande passante, le prix, la technologie et la durée d'allocation — permet d'assurer une sélection optimale du PU qui répond le mieux aux besoins du SU. L'algorithme TOPSIS se distingue également par sa rapidité et son faible coût de calcul, des caractéristiques cruciales dans des environnements dynamiques comme les réseaux de radio cognitive, où les décisions doivent souvent être prises en temps réel ou dans des délais très courts.

Ainsi, bien qu'il existe d'autres méthodes de décision multicritère, le choix de TOPSIS repose sur sa simplicité, sa rapidité, sa flexibilité et sa capacité à fournir des solutions claires et efficaces adaptées à la problématique spécifique de la gestion des ressources dans les réseaux de radio cognitive.

3.5 Deuxième contribution : Optimisation du mode de chiffrement symétrique ECB dédié à la sécurisation des données médicales

3.5.1 Approche proposée

Le mode ECB est l'un des modes de chiffrement les plus simples. Il se distingue par sa capacité à chiffrer ou déchiffrer les blocs de données de manière totalement indépendante. Cette indépendance permet, par exemple, de traiter les blocs dans n'importe quel ordre, en commençant par la fin, le milieu ou le début, ce qui représente un atout considérable, notamment dans le contexte des bases de données [27].

Ce mode présente également l'avantage de limiter la propagation des erreurs : une erreur sur un bloc n'affecte pas les autres, ce qui renforce la fiabilité du processus. Néanmoins, cette autonomie entre les blocs constitue également une faille de sécurité. En effet, un attaquant pourrait remplacer un bloc chiffré par un autre, sans avoir besoin de connaître la clé, ou encore réintroduire un ancien bloc intercepté pour tromper le système et en modifier le comportement.

De plus, le mode ECB présente un autre inconvénient majeur : les blocs de texte clair identiques produisent des blocs chiffrés identiques. Ce phénomène est particulièrement problématique pour les images numériques, qui contiennent souvent des motifs répétitifs et des zones de redondance. Cette faiblesse rend les données vulnérables à une analyse visuelle ou statistique. C'est pour cette raison que l'utilisation du mode ECB est généralement déconseillée dans les systèmes de sécurité modernes.

Dans le cadre de notre travail, nous proposons une amélioration de ce mode de chiffrement afin d'en corriger les limites. L'idée est de générer une clé différente pour chaque bloc du message, ce qui empêche la production de blocs chiffrés identiques pour des données identiques. La Figure 3.6 illustre un exemple pratique de ce mécanisme.

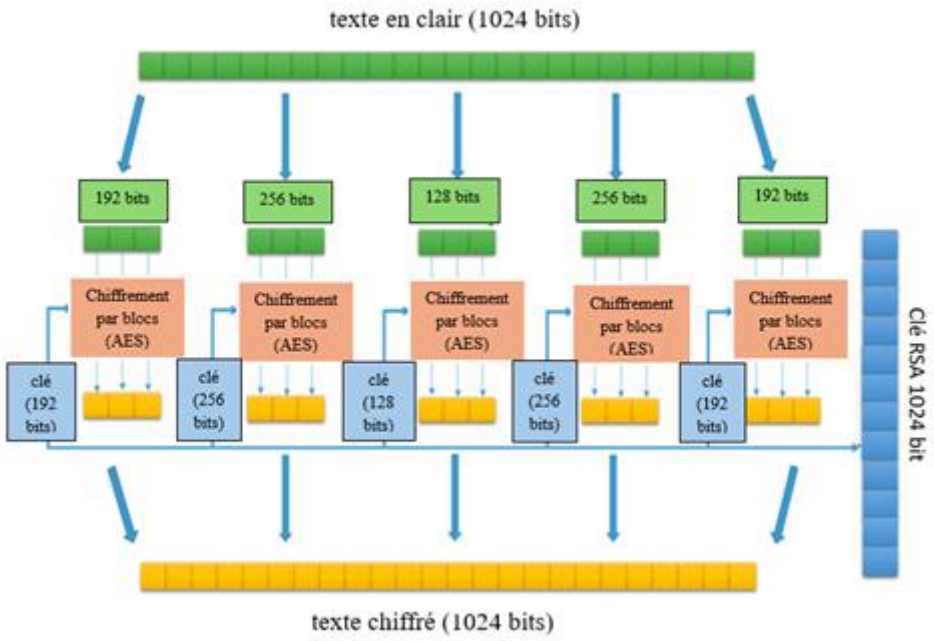


Figure 3.6 : Le mode ECB optimisé.

Concrètement, notre approche consiste à chiffrer un message de 1024 bits en utilisant l'algorithme AES pour le traitement des données et RSA pour le chiffrement des clés. Le message est divisé en blocs de 128, 192 et 256 bits, chacun étant chiffré avec une clé correspondante de même taille (128, 192 ou 256 bits). Cette stratégie garantit une meilleure sécurité en assurant une unicité du chiffrement bloc par bloc.

De plus ce mode ECB optimisé permet non seulement de sécuriser l'ancien mode ECB mais de garde la rapidité de chiffrement des blocs qui est un atout majeur pour le cas de notre étude, ceci permettra de combler la lenteur des algorithmes asymétrique comme le RSA ou l'ECC pour le chiffrement des clé secrètes de l'algorithme AES afin de sécuriser l'ensemble du système.

3.5.2 Comparaison entre le mode ECB classique et le mode ECB optimisé

Le tableau 3.2 met en évidence les différences entre le mode ECB classique et sa version optimisée, en comparant leurs principales caractéristiques et performances.

Tableau 3.2 : Comparaison des deux modes (ECB classique et ECB optimisé).

	ECB classique	ECB optimisé
Avantages	-Offre la possibilité de chiffrer simultanément les différents blocs d'un message. -Plus rapide.	-Plus sûr et plus complexe pour un attaquant de deviner la clé utilisée pour déchiffrer le message chiffré. -Même si l'attaquant parvient à déchiffrer un bloc, cela ne lui permet pas de déchiffrer l'intégralité du message, car chaque bloc est chiffré avec une clé différente.
Inconvénients	-Un attaquant actif pourra facilement déchiffrer le message en identifiant la clé répétée utilisée pour chaque bloc.	-Nécessite un peu plus de temps pour générer une clé pour chaque bloc de données, contrairement au mode ECB classique qui utilise une seule clé pour tous les blocs.

3.6 Troisième contribution : Sécurité des données d'un réseau radio cognitif pour des utilisateurs secondaires multicritères

3.6.1 Approche proposée

Dans cette troisième contribution, nous avons consolidé les mécanismes de négociation et de sélection mis en place dans les étapes précédentes, pour nous concentrer sur un enjeu crucial : la confidentialité des données médicales, qu'elles soient sous forme textuelle ou visuelle (images médicales).

À la suite de la sélection du PU optimal via l'algorithme multicritère TOPSIS, une couche de sécurité renforcée a été intégrée afin de sécuriser les échanges. Cette couche repose sur une combinaison de trois techniques cryptographiques complémentaires :

a) Chiffrement AES avec mode ECB optimisé

Nous avons utilisé l'algorithme AES (Advanced Encryption Standard) pour le chiffrement des données et des images médicales. Cependant, au lieu d'utiliser le mode ECB

classique, connu pour ses vulnérabilités (notamment les répétitions sur des blocs identiques), nous avons adopté une version optimisée du mode ECB, dans laquelle chaque bloc est chiffré avec une clé distincte. Cette optimisation permet d'éliminer les similarités entre blocs chiffrés à contenu identique, offrant ainsi une protection plus robuste contre les attaques visuelles ou par analyse statistique, un enjeu particulièrement important pour la protection des images médicales souvent redondantes.

b) Utilisation du chiffrement par courbes elliptiques

Pour protéger les clés AES générées pour chaque bloc, nous avons recours au chiffrement ECC. Ce choix s'explique par la capacité de l'ECC à fournir un haut niveau de sécurité avec des clés de taille réduite, ce qui le rend idéal pour les systèmes médicaux embarqués, où les ressources sont souvent limitées (en termes de calcul et de mémoire).

c) Sécurité renforcée et maintien de la qualité de service

La combinaison du chiffrement symétrique AES avec le chiffrement asymétrique basé sur les courbes elliptiques ECC constitue une solution hybride particulièrement performante pour répondre aux enjeux de confidentialité des données dans les réseaux de radio cognitive, notamment dans le domaine de la e-santé.

Le choix de l'AES repose sur ses nombreux atouts : il s'agit d'un algorithme de chiffrement symétrique reconnu pour sa rapidité, son efficacité en traitement de gros volumes de données, et sa robustesse face aux attaques. Grâce à son mode de fonctionnement optimisé (tel que le mode ECB amélioré que nous avons proposé), il permet un chiffrement bloc par bloc tout en limitant la redondance des motifs, ce qui est particulièrement important pour protéger les images médicales ou les dossiers médicaux contenant des structures répétitives.

Cependant, comme tout algorithme symétrique, l'AES nécessite un échange préalable de clé secrète entre les parties communicantes, ce qui peut constituer une faille si cet échange n'est pas sécurisé. C'est pourquoi nous avons intégré l'ECC dans notre approche, un système de cryptographie asymétrique offrant un très haut niveau de sécurité avec des clés plus courtes que les autres méthodes asymétriques classiques (comme RSA), ce qui le rend idéal pour les dispositifs médicaux souvent limités en capacité de calcul et en mémoire. L'ECC est utilisé ici pour chiffrer et transmettre la clé AES de manière sécurisée, assurant ainsi que seule la partie autorisée pourra déchiffrer les données sensibles. Ce mécanisme garantit la confidentialité de bout en bout, y compris dans un environnement partagé comme les réseaux de radio cognitive.

En réunissant les forces de ces deux techniques – l'efficacité de l'AES pour le traitement des données et la sécurité de l'ECC pour la gestion des clés – notre solution parvient à protéger les données médicales sensibles tout en maintenant une qualité de service (QoS) élevée, indispensable dans des contextes critiques comme les systèmes de santé intelligents, où la latence, la fiabilité et la sécurité doivent coexister harmonieusement.

3.6.2 Architecture globale de la solution de sécurisation des données dans un environnement radio cognitif

L'organigramme présenté dans la Figure 3.7 illustre de manière synthétique l'ensemble des étapes de notre approche, depuis l'authentification des utilisateurs primaires jusqu'à la sélection du PU optimal et à la sécurisation des données échangées. Il offre une vue globale et structurée du processus proposé, mettant en évidence la logique de traitement adoptée pour garantir à la fois efficacité, fiabilité et confidentialité.

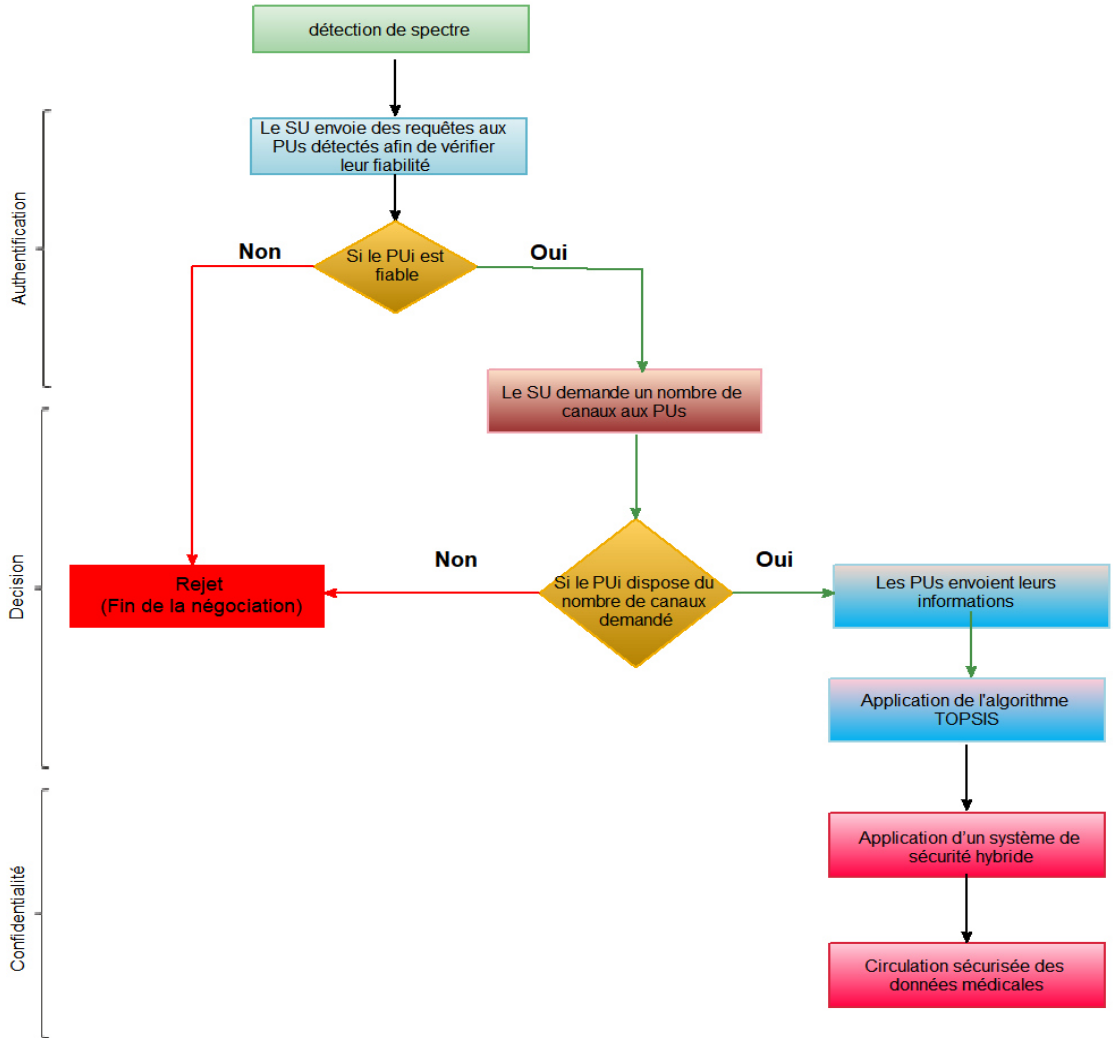


Figure 3.7 : Organigramme globale de scénario proposé.

La Figure 3.7 nous explique notre approche globale pour l'architecture du réseau radio cognitive sécurisé proposé sur trois parties complémentaires :

- Authentification

Détection de spectre : Le système commence par détecter les fréquences non utilisées (spectre disponible), une étape essentielle dans un réseau radio cognitif pour permettre aux utilisateurs secondaires (Secondary Users, SUs) d'exploiter les ressources sans interférer avec les utilisateurs primaires (Primary Users, PUs).

Vérification de fiabilité des PUs : Le SU envoie des requêtes aux PUs détectés afin de s'assurer qu'ils sont fiables et dignes de confiance.

- ✓ Si le PU n'est pas fiable, le processus est interrompu (voir étape de rejet plus loin).
- ✓ Si le PU est fiable, le processus continue.

- Décision

Demande de canaux : Le SU fait une requête spécifique concernant le nombre de canaux nécessaires auprès du PU.

Validation de la disponibilité des canaux ; Le PU vérifie s'il peut répondre à cette demande :

- ✓ Non : Le processus est rejeté → Rejet (Fin de la négociation)
- ✓ Oui : Le PU transmet les informations nécessaires

- Confidentialité

Application de l'algorithme TOPSIS : Une fois les informations reçues, l'algorithme multicritère TOPSIS est appliqué pour effectuer une sélection optimale des ressources (canaux, configurations, etc.), en se basant sur les préférences et les conditions idéales.

Sécurisation des données médicales : Après l'allocation optimale :

- ✓ Mise en place d'un système de sécurité hybride (combinant chiffrement symétrique AES et asymétrique ECC ainsi que le mode de chiffrement ECB optimisé).
- ✓ Ensuite, les données médicales peuvent circuler de manière sécurisée à travers le réseau radio cognitive.

3.7 Conclusion

Ce chapitre a mis en évidence l'importance de la sécurité dans les (RRC), en particulier dans des contextes où les utilisateurs secondaires accèdent dynamiquement aux ressources spectrales partagées avec les utilisateurs primaires. Dans cette optique, l'intégration des (SMA) s'est révélée pertinente pour une gestion intelligente, adaptative et sécurisée de ces ressources.

L'exploitation conjointe des SMA avec des mécanismes de négociation et de coopération a permis de concevoir une stratégie efficace assurant à la fois une allocation optimale du spectre et la protection des échanges. Par ailleurs, l'adoption d'outils d'aide à la décision multicritères, tels que l'algorithme TOPSIS, a renforcé le processus de sélection du PU le plus adapté aux besoins spécifiques du SU.

Sur le plan de la confidentialité, les solutions proposées, en particulier l'optimisation du mode ECB et le recours au chiffrement par courbes elliptiques, ont permis de garantir une sécurisation fine des données, tant textuelles qu'images, sans dégrader les performances du réseau. L'utilisation conjointe du chiffrement symétrique AES pour les données et de l'ECC pour l'échange sécurisé des clés a constitué un équilibre efficace entre sécurité, légèreté et respect de la qualité de service (QoS).

Les contributions exposées dans ce chapitre apportent ainsi une réponse cohérente et adaptée aux défis de la sécurisation dans les RRC, notamment dans des domaines sensibles comme la e-santé, où la protection des données revêt une importance stratégique.

Dans le prochain chapitre, nous allons concrétiser ses approches par des simulations et des résultats concrets destinées aux réseaux radio cognitifs dans le but de la sécurisation des données médicales.

Chapitre 4

Conception et validation d'un réseau radio cognitif sécurisé dédié aux données médicales

Sommaire

4.1 Introduction

L'évaluation expérimentale des solutions proposées repose sur des simulations réalisées avec la plateforme multi-agents JADE. Cette approche permet de valider l'efficacité des mécanismes de décision multicritère et des stratégies de sécurisation des échanges dans un environnement distribué.

La plateforme JADE, conforme aux spécifications FIPA, offre un cadre robuste pour le développement d'applications multi-agents, facilitant la communication entre agents et la gestion des ressources dans des systèmes complexes.

À travers différentes simulations, ce chapitre explore l'optimisation des décisions d'un utilisateur secondaire, l'amélioration du mode de chiffrement ECB, et la mise en œuvre d'une solution hybride de sécurité intégrant plusieurs phases : authentification, décision, et confidentialité. Chaque scénario est analysé en termes de performances, de fiabilité et de sécurité des données échangées.

L'évaluation globale de la solution de sécurisation proposée est également abordée, mettant en lumière l'intégration de la détection d'agents malveillants, la négociation multicritère, le chiffrement optimisé et la validation des flux sécurisés dédiées à des données médicales. Cette analyse permet de tirer des enseignements sur l'efficacité et la robustesse des approches développées.

4.2 Plateforme JADE

4.2.1 Définition

La plateforme JADE (Java Agent DEvelopment Framework) est un environnement logiciel open-source, développé en Java, conçu pour faciliter le développement et le déploiement de systèmes multi-agents conformes aux spécifications de la FIPA (Foundation for Intelligent Physical Agents) [1]. Elle permet de programmer des agents autonomes capables de percevoir, de raisonner et d'interagir de manière coopérative. Grâce à sa flexibilité et sa portabilité, JADE est largement utilisé dans les milieux académiques, industriels et de recherche [2].
Dans le domaine des réseaux radio cognitifs, JADE est particulièrement pertinent car il permet de modéliser des agents intelligents capables de gérer dynamiquement les ressources spectrales, d'adapter leur comportement en fonction de l'environnement radio, et de collaborer pour optimiser l'utilisation du spectre de manière autonome et décentralisée.

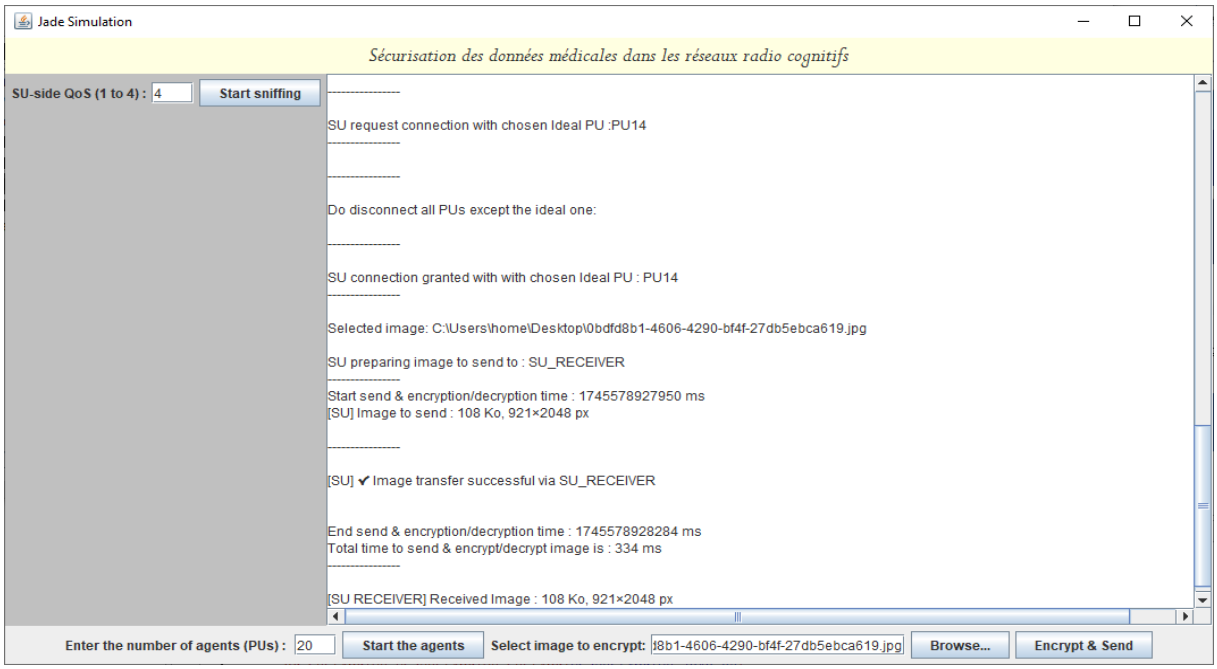


Figure 4.1 : Plateforme JADE de l'approche proposé.

4.2.2 Architecture

JADE est un middleware entièrement distribué, doté d'une infrastructure souple qui peut être facilement enrichie à l'aide de modules complémentaires (*add-ons*) [3]. Il simplifie la création d'applications orientées agents en offrant un environnement d'exécution prenant en charge les principales fonctionnalités liées au cycle de vie des agents, à leur logique interne, ainsi qu'un ensemble complet d'outils graphiques pour le développement et le suivi. La Figure 4.2 illustre l'architecture générale d'une plateforme JADE.

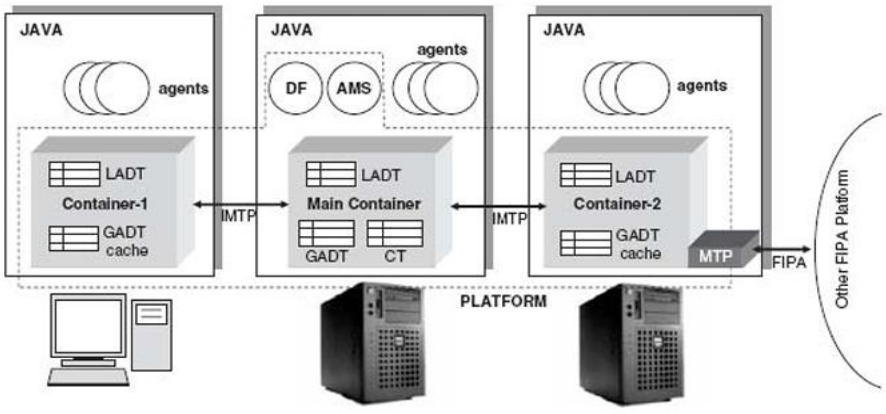


Figure 4.2 : Architecture du système JADE [4].

L'architecture d'une plateforme JADE repose sur une organisation en conteneurs, qui sont des environnements d'exécution pour les agents. Le conteneur principal est le point de départ de toute plateforme JADE. Il est lancé automatiquement au démarrage et héberge les agents système essentiels, notamment :

- AMS (Agent Management System), qui gère le registre des agents et fournit le service de pages blanches (informations sur les agents existants).
- DF (Directory Facilitator), qui offre le service de pages jaunes, permettant aux agents de publier ou rechercher des services.

Autour de ce conteneur principal, on peut connecter d'autres conteneurs secondaires, éventuellement répartis sur d'autres machines. Ensemble, ils forment une plateforme multi-agents distribuée.

4.3 Simulation et résultats d'un utilisateur de radio cognitive multicritère par apprentissage autonome

4.3.1 Initialisation des agents et spécification des ressources

La simulation a été réalisée dans l'environnement Apache NetBeans IDE 12.0, en s'appuyant sur la plateforme JADE pour la gestion des interactions entre agents. Dans ce cadre, un scénario a été conçu mettant en œuvre un agent cognitif représentant un utilisateur secondaire (SU), interagissant avec dix agents représentant des utilisateurs primaires (PU1 à PU10).

Chacun de ces agents primaires possède des caractéristiques spécifiques, simulant ainsi un environnement radio dynamique. L'agent SU engage des communications parallèles avec l'ensemble des agents PU, dans le but d'identifier un utilisateur primaire dont les paramètres d'accès au spectre répondent à ses critères de sélection. Ce processus vise à illustrer la capacité des agents cognitifs à opérer dans un contexte distribué, en évaluant de manière autonome les opportunités disponibles tout en tenant compte des contraintes du système. La Figure 4.3 présente l'interface de simulation développée sous JADE, permettant de spécifier le nombre d'agents primaires (PUs) ainsi que le nombre de canaux souhaités par l'agent secondaire (SU), avant le lancement du processus de négociation.

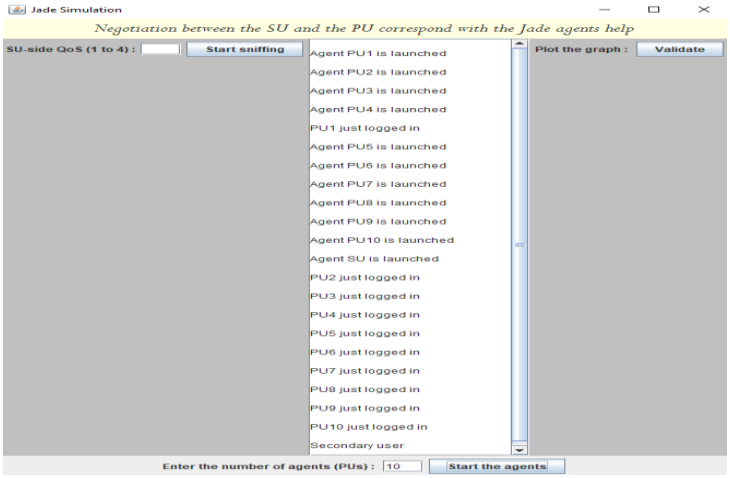


Figure 4.3 : Interface de simulation JADE de notre approche.

4.3.2 Négociation entre les utilisateurs secondaires et primaires

Dans le scénario étudié, un agent cognitif secondaire (SU) initie un processus de communication visant à identifier un utilisateur primaire (PU) apte à répondre à ses besoins en ressources spectrales. Pour assurer la qualité de service (QoS) nécessaire au transfert d'un fichier, l'agent SU exprime une demande de trois canaux. Cette requête est adressée à l'ensemble des dix agents Pus présents dans l'environnement simulé.

Les agents primaires disposant du nombre de canaux demandé répondent de manière positive en envoyant un message ACL contenant plusieurs informations essentielles pour le processus de décision. Ces informations comprennent le nombre de canaux disponibles, le prix proposé pour l'allocation, la technologie utilisée, la durée prévue de l'allocation, ainsi que la bande passante mise à disposition. Ces paramètres permettent à l'agent secondaire d'évaluer la pertinence de chaque réponse en fonction de ses exigences et des critères de qualité de service requis. Ces informations permettent à l'agent SU de procéder à une évaluation multicritère afin d'identifier l'alternative la plus avantageuse parmi les propositions reçues.

À l'inverse, les Pus ne satisfaisant pas les exigences minimales, à savoir la disponibilité de trois canaux, rejettent la demande. Dans ce cas précis, huit agents Pus ont répondu favorablement avec des offres aux caractéristiques variées, tandis que deux agents (PU2 et PU7) ont émis un refus, ne disposant pas de la capacité requise. La Figure 4.4 illustre le processus de négociation entre l'agent SU et les différents agents Pus, en représentant l'ensemble des requêtes envoyées ainsi que les réponses reçues. Les agents primaires ayant répondu favorablement à la demande de trois canaux sont indiqués en jaune, tandis que les Pus ayant rejeté la demande (PU2 et PU7) sont signalés en rouge, soulignant leur indisponibilité en ressources.

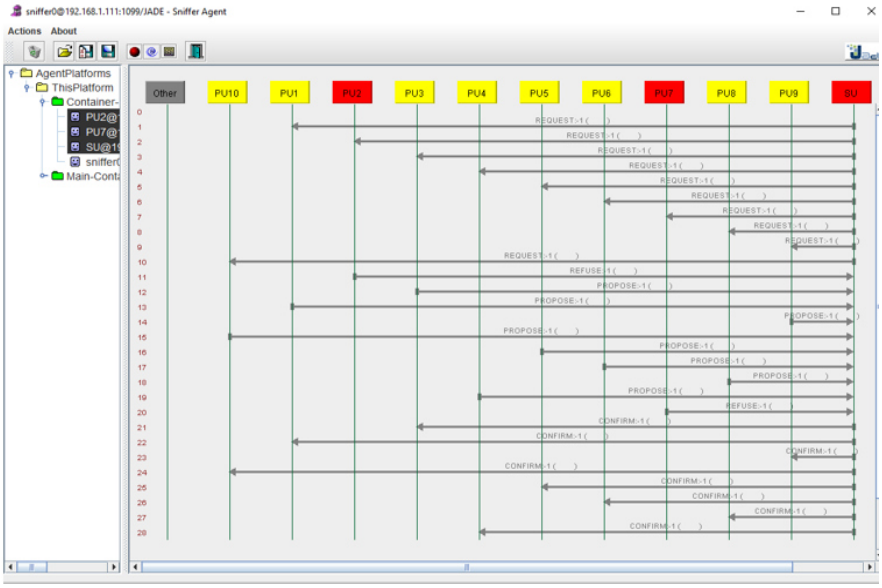


Figure 4.4 : Négociation entre l'utilisateur secondaire (SU) et les 10 utilisateurs primaires (Pus).

4.3.3 Application de l'algorithme TOPSIS pour le choix de l'utilisateur primaire optimal

Dans cette simulation, une échelle de notation standardisée, allant de 1 à 8, a été utilisée afin d'évaluer chaque critère associé aux utilisateurs primaires (PU). Chaque valeur de cette échelle est liée à un niveau d'intérêt, exprimé linguistiquement de « pas du tout intéressant » à

« parfaitement intéressant », et permet de quantifier objectivement tant les critères favorables que défavorables.

À partir de cette échelle, une matrice de données Alternatives × Critères a été construite. Elle associe à chaque PU une note pour chacun des critères considérés, selon les caractéristiques de ses ressources.

Pour les critères positifs (temps d'allocation, technologie, bande passante), une note élevée indique un avantage certain. À l'inverse, pour le critère négatif (le prix), une note élevée correspond à une alternative moins avantageuse.

Chaque critère a été pondéré en fonction de son importance relative dans le processus de décision, en veillant à ce que la somme des pondérations soit égale à 1. Les poids attribués dans ce cadre sont les suivants :

- Temps d'allocation : 0,25
- Technologie : 0,25
- Bande passante : 0,20
- Prix : 0,30

Les intervalles de variation retenus pour chacun de ces critères sont les suivants :

- Temps d'allocation : entre 1 et 24 heures
- Technologie : de la 3G à la 5G
- Bande passante : de 144 Mbps à 10 Gbps
- Prix : de 120 à 300 DA par heure

Les résultats issus de cette phase d'évaluation sont présentés dans le Tableau 4.1. Ces données serviront de base à l'application de l'algorithme TOPSIS en vue de sélectionner l'utilisateur primaire optimal.

Tableau 4.1 : Classification des utilisateurs primaires après application de l'algorithme TOPSIS.

Pus	valeurs du critères
PU1	Nbre de canaux = 6 ; Temps alloué (h) = 3 ; Technologie = 5G ; Bande passante = 10788.112 ; Prix = 153.
PU6	Nbre de canaux = 4 ; Temps alloué (h) = 6 ; Technologie = 4G ; Bande passante = 6602.962 ; Prix = 132.
PU8	Nbre de canaux = 3 ; Temps alloué (h) = 13 ; Technologie = 3.75G ; Bande passante = 13.385 ; Prix = 238.
PU9	Nbre de canaux = 4 ; Temps alloué (h) = 14 ; Technologie = 3G ; Bande passante = 0.7641 ; Prix = 155.
PU10	Nbre de canaux = 7 ; Temps alloué (h) = 7 ; Technologie = 3.75G ; Bande passante = 5.0514 ; Prix = 271.
PU5	Nbre de canaux = 3 ; Temps alloué (h) = 7 ; Technologie = 3G ; Bande passante = 0.635 ; Prix = 220.
PU3	Nbre de canaux = 8 ; Temps alloué (h) = 3 ; Technologie = 3.75G ; Bande passante = 11.056 ; Prix = 253.
PU4	Nbre de canaux = 6 ; Temps alloué (h) = 4 ; Technologie = 4G ; Bande passante = 66.441 ; Prix = 201.

La Figure 4.5 présente les résultats de la simulation sur la plateforme JADE du programme Java, illustrant l'évaluation des utilisateurs primaires en fonction de différents critères, et la sélection des utilisateurs les plus et les moins adaptés pour le partage du spectre avec l'utilisateur secondaire.

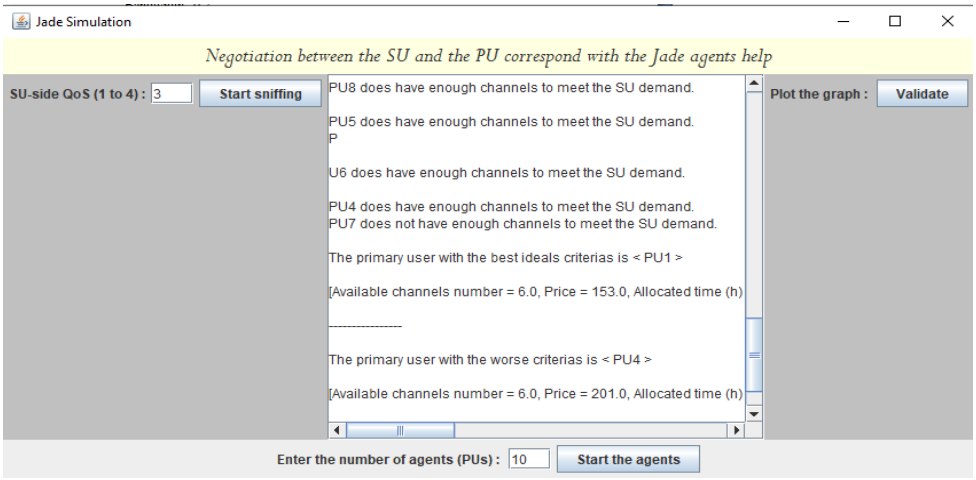


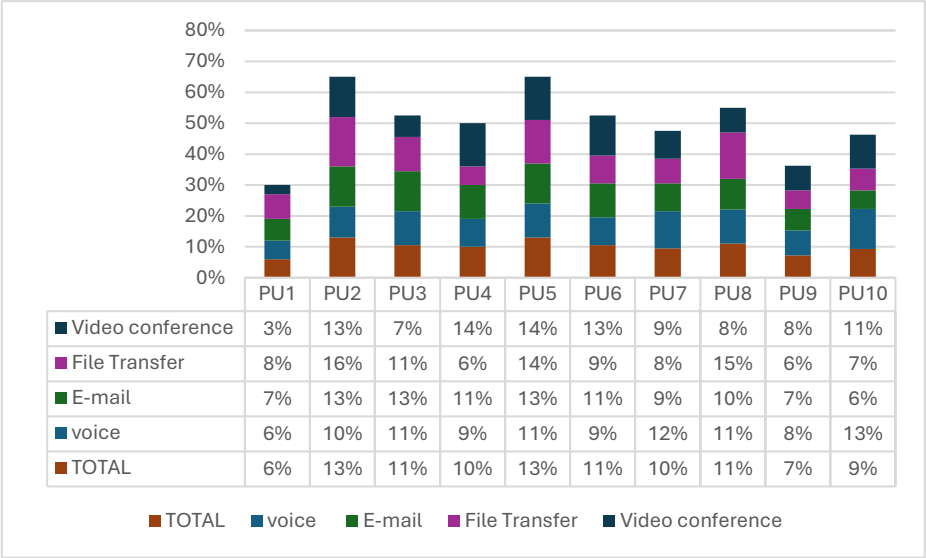
Figure 4.5 : Les résultats de la simulation s'affichent sur la plateforme JADE.

Le classement des huit utilisateurs primaires (PUs) a été effectué en fonction de leur capacité à offrir une qualité de service optimale pour le transfert de fichiers, allant du plus satisfaisant au moins satisfaisant. Ainsi, PU1 est classé comme le plus favorable, suivi de PU6, PU8, PU9, PU10, PU5, PU3, et enfin PU4, qui est le moins favorable. Il est important de souligner que les utilisateurs primaires PU2 et PU7 ne disposent pas du nombre de canaux requis pour partager le spectre avec l'utilisateur secondaire, ce qui les rend inéligibles à la négociation.

4.3.4 Résultats et discussion

Afin d'approfondir notre analyse, nous avons choisi de mener une étude par étapes, par un passage à l'échelle afin de favoriser un apprentissage plus complet et de meilleure qualité. Cette approche repose sur l'évaluation de quatre critères de qualité de service (QoS) pour quatre technologies distinctes : la voix, le courrier électronique, le transfert de fichiers et la visioconférence, dans un scénario impliquant un utilisateur secondaire (SU) communiquant avec plusieurs utilisateurs primaires (PUs) totalement autonome avec des caractéristiques ainsi que des prises de décision différentes, pour des tentatives sur des instances de temps différents.

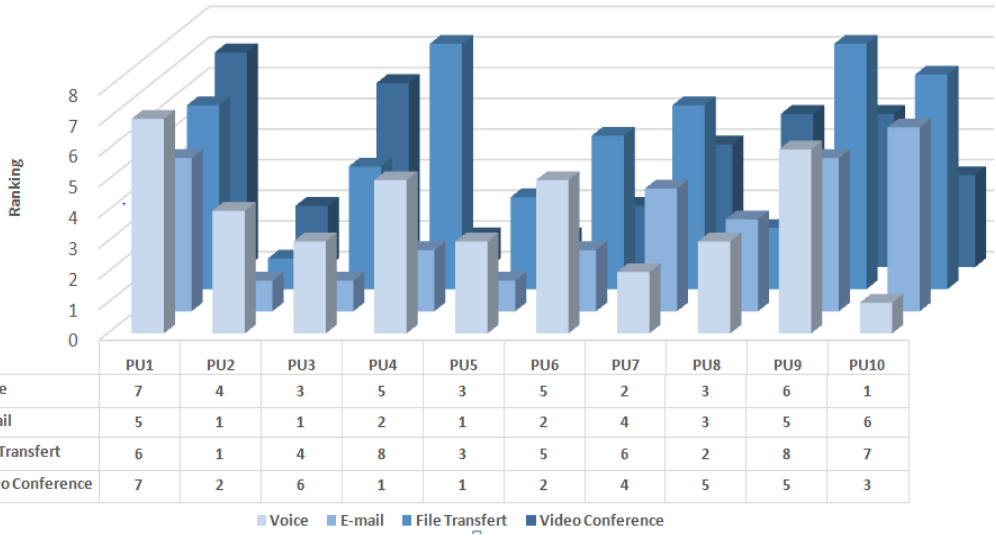
Le passage à l'échelle a été réalisée à travers 100 essais de communication entre le SU et dix PUs, sollicitant successivement un canal pour la voix, deux canaux pour le courrier électronique, trois canaux pour le transfert de fichiers et quatre canaux pour la visioconférence. L'objectif étant d'identifier le PU optimal en fonction de ces différentes configurations. La Figure 4.6 illustre les résultats des meilleures propositions obtenues entre le SU et les dix PUs pour les quatre technologies évaluées.



	PU1	PU2	PU3	PU4	PU5	PU6	PU7	PU8	PU9	PU10
Video conference	3%	13%	7%	14%	14%	13%	9%	8%	8%	11%
File Transfer	8%	16%	11%	6%	14%	9%	8%	15%	6%	7%
E-mail	7%	13%	13%	11%	13%	11%	9%	10%	7%	6%
voice	6%	10%	11%	9%	11%	9%	12%	11%	8%	13%
TOTAL	6%	13%	11%	10%	13%	11%	10%	11%	7%	9%

Figure 4.6 : Résultats des meilleures suggestions pour le SU choisissant parmi 10 PUs sur 100 tentatives de communication.

Une analyse comparative des technologies a révélé que les utilisateurs primaires PU4 et PU5 offrent les meilleures performances pour la vidéoconférence, tandis que PU2 se distingue pour le transfert de fichiers. En ce qui concerne les emails, les PU2, PU3 et PU5 présentent les meilleures options, tandis que PU10 est le plus performant pour les communications vocales. Dans une perspective globale couvrant toutes les technologies, les PU2 et PU5 se classent comme les meilleurs choix.



	PU1	PU2	PU3	PU4	PU5	PU6	PU7	PU8	PU9	PU10
Voice	7	4	3	5	3	5	2	3	6	1
E-mail	5	1	1	2	1	2	4	3	5	6
File Transfert	6	1	4	8	3	5	6	2	8	7
Video Conference	7	2	6	1	1	2	4	5	5	3

Figure 4.7 : Classement des meilleures propositions pour l'utilisateur secondaire (SU) parmi 10 utilisateurs primaires (PUs) après 100 tentatives de communication.

La Figure 4.7 présente le classement des utilisateurs primaires (PUs) après 100 tentatives de négociation entre un utilisateur secondaire (SU) et 10 PUs, en fonction des différentes technologies utilisées.

Ensuite, une autre dimension importante de cette étude concerne le temps de convergence. La Figure 4.8 illustre le temps de convergence moyen observé au cours des 100 tentatives de communication entre le SU et les 10 PUs pour la technologie de la vidéoconférence.

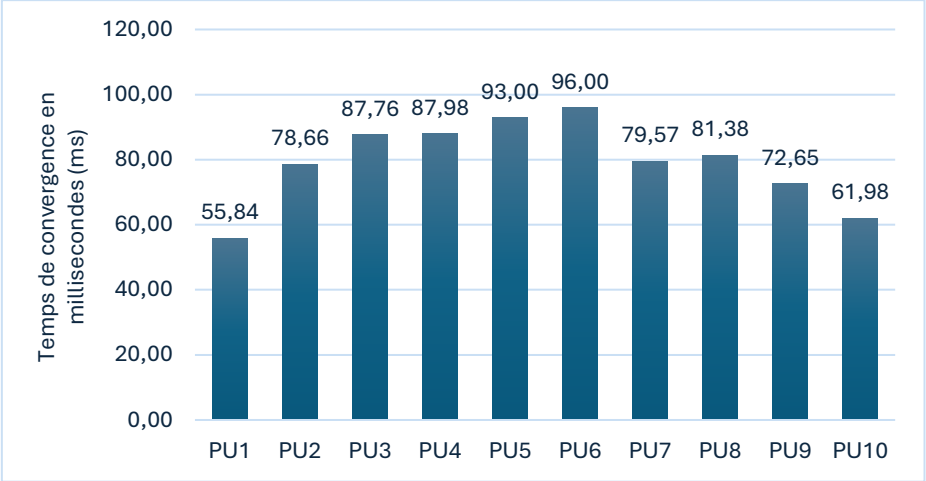


Figure 4.8 : La moyenne du temps de convergence sur 100 tentatives de communication entre l'utilisateur secondaire (SU) et les différents utilisateurs primaires (PUs), exprimée en millisecondes pour la vidéoconférence.

La Figure 4.8 illustre le temps de convergence moyen entre l'utilisateur secondaire (SU) et les 10 utilisateurs primaires (PUs) pour le partage du spectre. Pour la vidéoconférence, PU1 affiche le meilleur temps avec 55,84 ms, tandis que PU6 présente le temps le plus élevé avec 96 ms. Cependant, il est à noter que tous les utilisateurs respectent un temps de convergence inférieur à 150 ms, ce qui correspond aux exigences de la QoS pour la vidéoconférence, et garantit ainsi la qualité de service requise selon les références de la littérature [5].

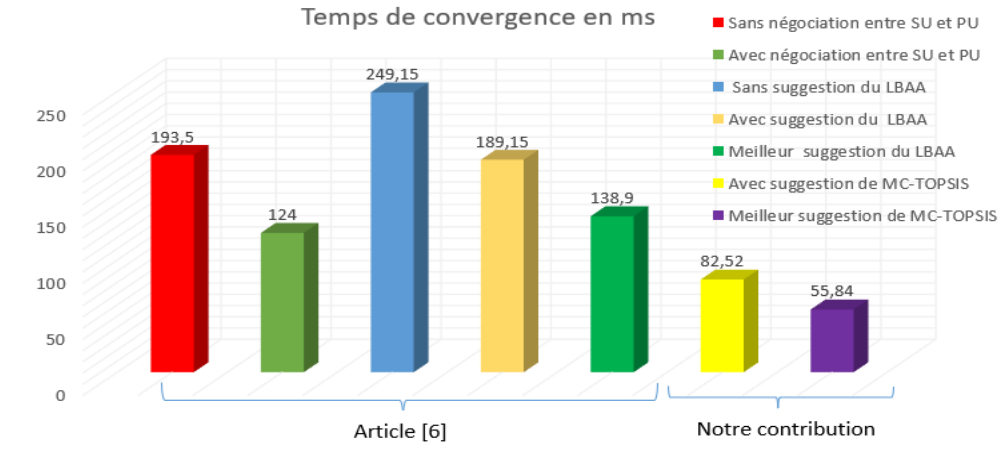


Figure 4.9 : Comparaison du temps de convergence moyen avec les travaux existants.

La Figure 4.9 présente une comparaison entre notre contribution et celle de l'article [6] en termes de temps moyen de convergence. Il ressort de cette comparaison que le meilleur

temps de convergence obtenu dans notre approche est significativement plus rapide et optimal par rapport à celui de l'article, qui est de 138,9 ms.

Les résultats obtenus démontrent que l'algorithme TOPSIS joue un rôle crucial dans le processus de négociation au sein des systèmes multi-agents, en assurant une qualité de service optimale dans un environnement de radio cognitive.

4.4 Simulation et Résultats d'Optimisation du mode de chiffrement symétrique ECB

Cette étude vise à améliorer les performances du mode de chiffrement ECB en le rendant plus sécurisé tout en gardant à la fois sa rapidité de chiffrement. Pour ce faire, une nouvelle architecture a été conçue, reposant sur l'utilisation de l'algorithme AES avec l'utilisation de cinq clés de chiffrement symétrique de tailles variées : deux de 192 bits, une de 128 bits et deux de 256 bits. Cette configuration a été appliquée au chiffrement et au déchiffrement d'un message de 1024 bits symétrique avec une clé de chiffrement asymétrique à 1024 bits aussi. La mise en œuvre de l'architecture a été réalisée en langage de description matériel VHDL (VHSIC Hardware Description Language), à l'aide de l'environnement de développement ISE 14.7 de Xilinx. Les expérimentations ont été conduites sur une machine équipée d'un processeur Intel® Core i5 (double cœur) cadencé à 2,50 GHz (avec une fréquence turbo de 2,7 GHz), accompagnée de 12 Go de mémoire RAM, fonctionnant sous le système d'exploitation Windows 10 Professionnel 64 bits. La Figure 4.10 présente l'interface de développement ISE correspondant au programme VHDL principal de la partie chiffrement.

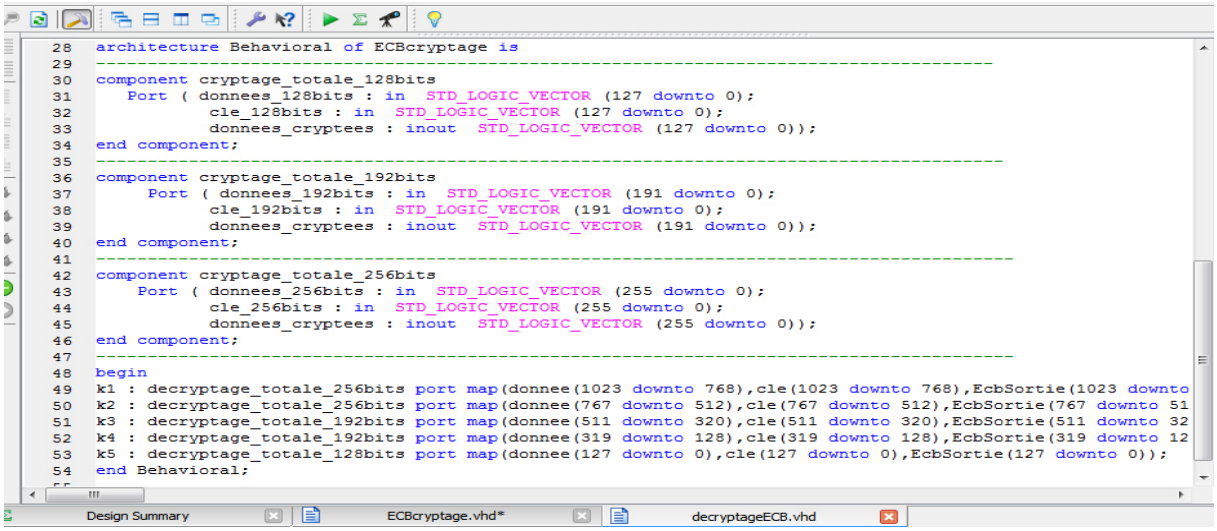


Figure 4.10 : Interface ISE du chiffrement en mode ECB optimisé.

Une fois l'architecture de chiffrement/déchiffrement définie, une simulation comportementale a été effectuée à l'aide de l'outil Xilinx ISim. Les chronogrammes présentés dans la Figure 4.11, issus de la simulation comportementale, illustrent les résultats obtenus lors de la phase de chiffrement, en mettant en évidence le fonctionnement interne et la synchronisation des signaux de l'architecture proposée.

Figure 4.11 : Résultats de la simulation de chiffrement à 1024 bits, en hexadécimal.

La Figure 4.12 représente les résultats de la simulation de la phase de déchiffrement.

Figure 4.12 : Résultats de la simulation de déchiffrement à 1024 bits, en hexadécimal.

4.5 Solution hybride entre l'ECB optimisé pour le chiffrement des données avec l'AES et L'ECC pour le chiffrement de la clé secrète

Afin de valider l'efficacité de l'approche proposée pour la sécurisation des réseaux radio cognitifs, une série de simulations a été menée en tenant compte des différentes phases définies précédemment, à savoir : l'authentification, la prise de décision, et la confidentialité. Ces simulations ont pour objectif de démontrer la robustesse du système face aux enjeux de fiabilité des utilisateurs primaires (PUs), d'optimisation de l'allocation des ressources via l'algorithme

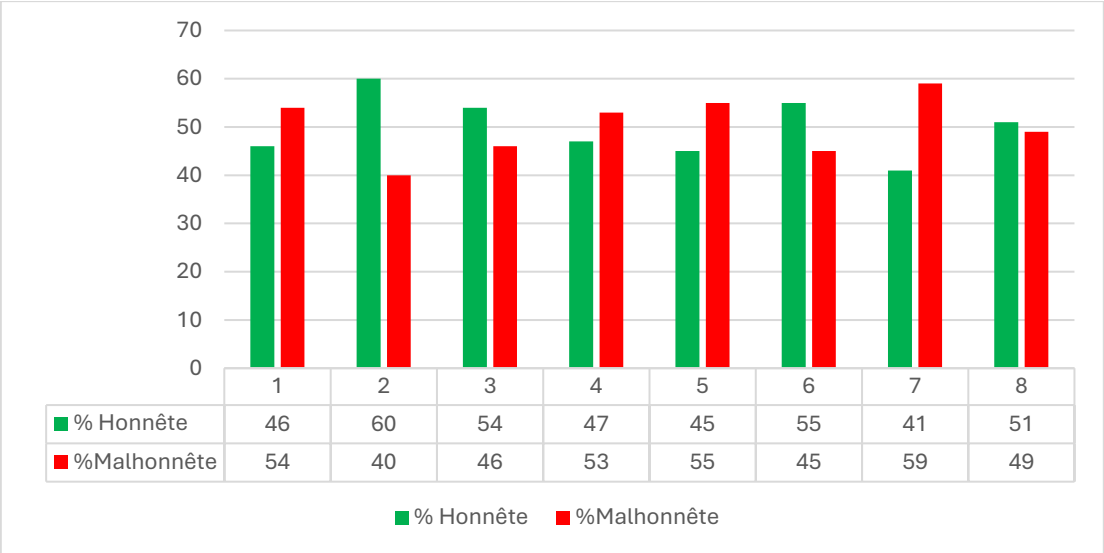
TOPSIS, ainsi que de protection des données sensibles, notamment médicales, grâce à une solution de chiffrement hybride.

La simulation s'appuie sur un scénario dans lequel un utilisateur secondaire (SU) tente d'établir une communication sécurisée avec un ensemble de PUs, tout en respectant les exigences de qualité de service (QoS) propres aux applications critiques telles que la visioconférence. Le processus de simulation comprend plusieurs étapes clés : détection du spectre libre, évaluation de la fiabilité des PUs sur la base de tests d'authentification, négociation de canaux disponibles, sélection optimale via TOPSIS, et enfin transmission sécurisée des données chiffrées.

4.5.1 Phase d'authentification

Dans le cadre de la phase d'authentification, une pré-simulation a été réalisée afin d'identifier les utilisateurs primaires (PUs) les plus fiables. Cette étape repose sur cent (100) tentatives de communication entre un utilisateur secondaire (SU) et huit PUs. Le taux de fiabilité obtenu pour chaque PU à l'issue de cette phase est ensuite intégré comme nouveau critère d'évaluation dans une nouvelle simulation.

Dans ce cadre, le SU transmet des requêtes chiffrées aux huit PUs. L'analyse des réponses reçues permet d'évaluer leur comportement : Les PUs dont le score de confiance est inférieur à un seuil prédéfini sont considérés comme malveillants, tandis que ceux dépassant ce seuil sont jugés fiables. À l'issue des cent tentatives, un taux de fiabilité est calculé pour chaque PU, servant à établir un classement hiérarchique du plus fiable au moins fiable. Les résultats issus de cette évaluation sont synthétisés dans la Figure 4.13.



	1	2	3	4	5	6	7	8
% Honnête	46	60	54	47	45	55	41	51
%Malhonnête	54	40	46	53	55	45	59	49

Figure 4.13 : Taux de fiabilité et de non-fiabilité de chaque PU sur 100 tentatives de communication entre le SU et les différents PUs.

Le graphique de la Figure 4.13 illustre le pourcentage de fiabilité attribué à chaque utilisateur primaire (PU) sur un total de cent (100) tentatives. Il en ressort que le PU2, avec un taux de fiabilité de 60 % contre 40 % d'irrégularité, se distingue comme le plus honnête. À l'inverse, le PU7 présente le taux de fiabilité le plus faible, avec seulement 41 %, ce qui en fait l'agent le moins digne de confiance.

4.5.2 Phase de décision

Dans la suite du processus, ce taux de fiabilité est introduit comme cinquième critère dans le mécanisme d'allocation dynamique entre le SU et les différents PUs. Les poids attribués à chaque critère sont précisés comme suit :

- Taux de fiabilité : 0.25
- Prix : 0.24
- Bande passante : 0.15
- Technologie : 0.18
- Durée d'allocation : 0.18

La phase de négociation débute par l'envoi, par le SU, d'une requête. Les réponses reçues sont analysées : un message de type *INFORM* signifie que le PU est honnête. À l'inverse, une réponse de type *FAILURE* indique le PU est malveillant.

Seuls les PUs identifiés comme fiables poursuivent le processus. Le SU leur transmet alors une nouvelle requête précisant le nombre minimal de canaux requis. Les PUs en mesure de répondre favorablement envoient un message de type *PROPOSE*, contenant une offre détaillée : nombre de canaux disponibles, coût, durée de l'allocation, technologie utilisée et bande passante. L'ensemble de ces offres est ensuite évalué à l'aide de l'algorithme multicritère TOPSIS, permettant un classement objectif du plus avantageux au moins pertinent, en s'appuyant sur les cinq critères précédemment définis. La Figure 4.14 illustre un exemple de négociation entre le SU et les huit PUs.

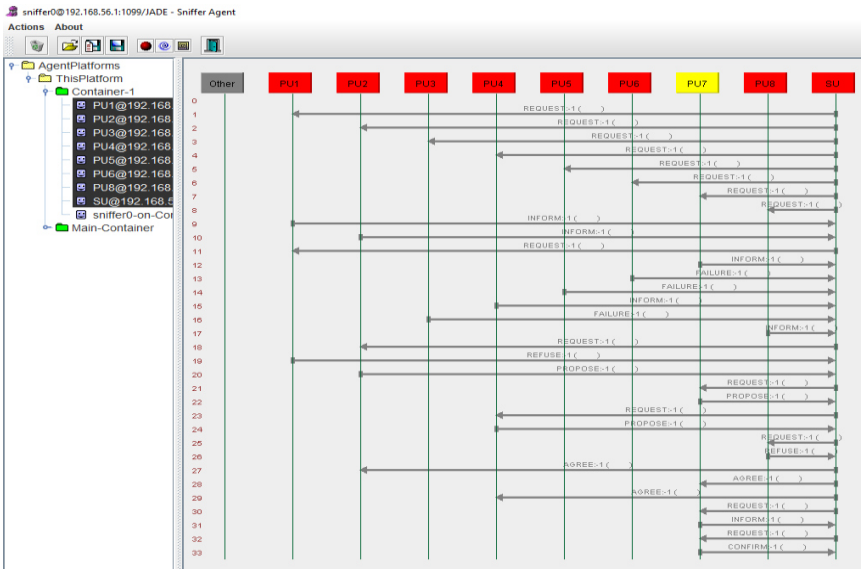
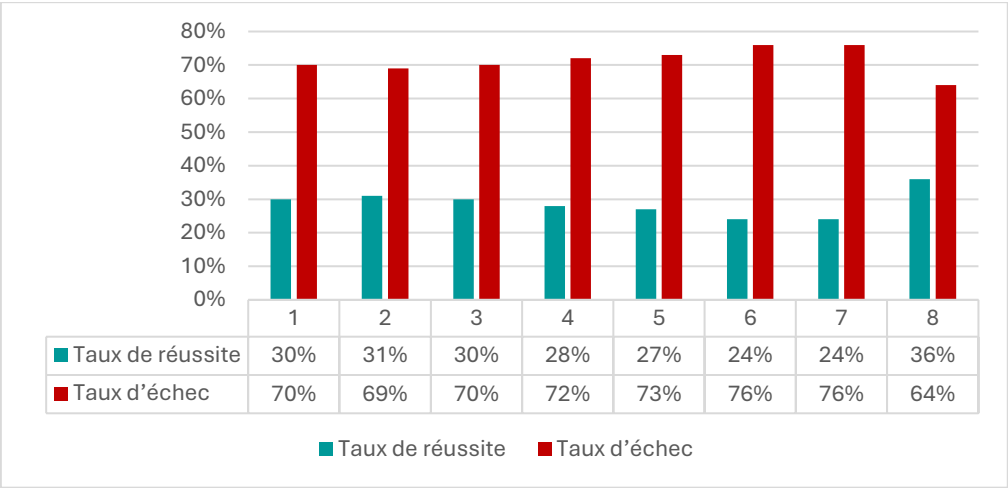


Figure 4.14 : Négociation entre l'utilisateur secondaire (SU) et les huit utilisateurs primaires (PUs).

Les résultats sont présentés en trois parties : d'abord en fonction des taux de réussite et d'échec, ensuite en termes de pourcentages de récompense et de pénalité, et enfin, en fonction du temps de convergence.

- **Résultats des taux de réussite et d'échec**

Les résultats des taux de réussite et d'échec concernant le partage du spectre entre le SU et chaque PU, selon les exigences multicritères, sont illustrés dans la Figure 4.15.



	1	2	3	4	5	6	7	8
Taux de réussite	30%	31%	30%	28%	27%	24%	24%	36%
Taux d'échec	70%	69%	70%	72%	73%	76%	76%	64%

Figure 4.15 : Le taux de succès/échec des propositions de partage de spectre de chaque PU avec le SU.

Le graphique révèle que le PU8 obtient le meilleur taux de réussite avec 36 %, mais il enregistre également un taux d'échec élevé de 64 %. En revanche, les PUs les moins performants sont le PU6 et le PU7, chacun ayant un taux de réussite de 24 % et un taux d'échec de 76 %.

- **Résultats des pourcentages de récompense et de pénalité**

La Figure 4.16 présente les résultats des PUs en fonction des pourcentages de récompense et de pénalité.

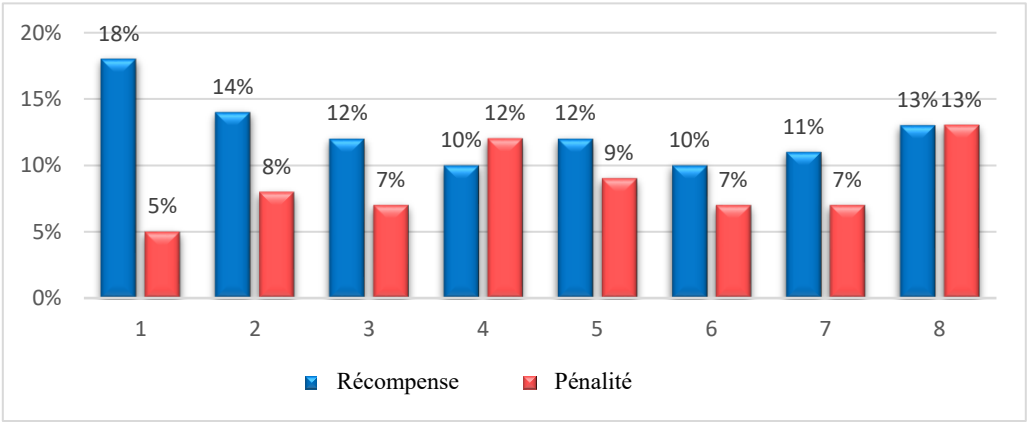


Figure 4.16 : Taux de récompense et de pénalité pour chaque PU.

Il en ressort que le PU1 est le plus performant, avec un taux de récompense de 18 % (ayant proposé la meilleure offre) et un faible taux de pénalité de 5 % (ayant proposé la mauvaise offre). À l'opposé, les PU4 et PU6 enregistrent les plus faibles taux de récompense, soit 10 %, tandis que le PU8 présente le taux de pénalité le plus élevé à 13 %.

- **Résultats du temps de convergence**

Le temps de convergence représente la durée écoulée entre le début et la fin de la négociation entre le SU et le PU. Les résultats de cette mesure sont présentés dans la Figure 4.17.

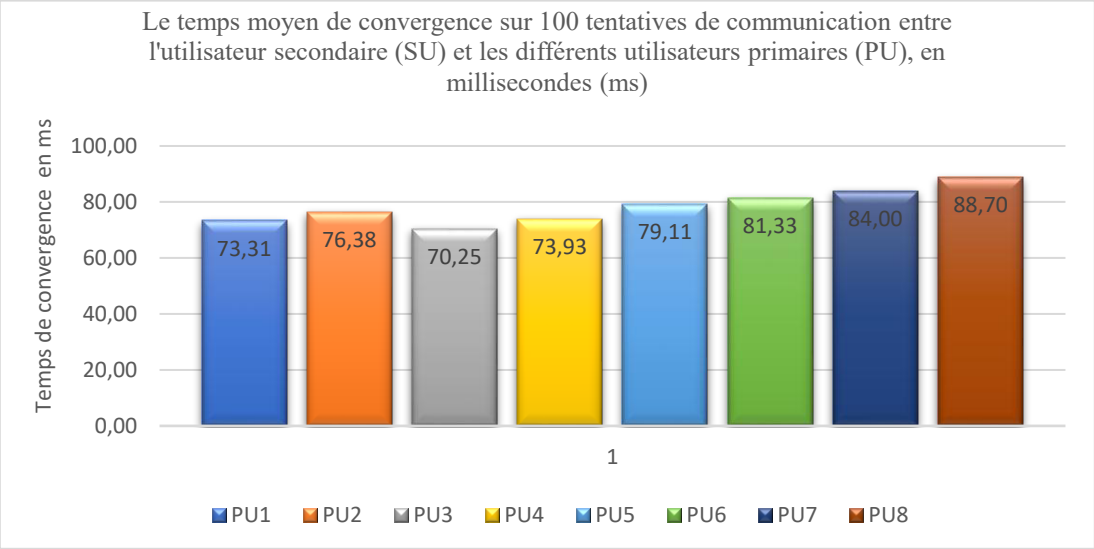


Figure 4.17 : Temps de convergence moyen pour chaque PU.

Les données montrent que le PU3 est le plus performant en termes de temps de convergence, avec un temps moyen de 70,25 millisecondes (ms), ce qui en fait le PU le plus rapide parmi les huit analysés. En revanche, le PU8 affiche le temps de convergence le plus élevé, avec une moyenne de 88,70 ms, représentant ainsi la moins bonne performance.

4.5.3 Phase de confidentialité

Après avoir déterminé quel PU est le plus adapté à l'allocation du spectre, il est impératif de garantir la sécurité des flux de données médicales transitant sur le réseau radio cognitif. Ces informations sensibles doivent rester à la fois

- **Confidentielles**, pour empêcher tout accès non autorisé,
- **Intègres**, afin d'assurer la fiabilité des décisions cliniques qui en découlent.

Dans un premier temps, le SU s'authentifie auprès du PU choisi et interrompt toute communication avec les autres PU. Dès que l'authentification réussit, le SU commence à préparer les données médicales confidentielles à envoyer au récepteur SU, que nous appellerons SU-Receiver.

À titre d'exemple, pour le transfert d'une image médicale, celle-ci est d'abord convertie en octets, puis encodée en Base64 afin de garantir l'intégrité des données lors du transport. Le résultat de cette opération est ensuite chiffré via notre système de chiffrement hybride ECC/AES-ECB optimisé, exploitant plusieurs clés AES de longueurs différentes (192, 256, 128, 256, 192 bits), chacune dérivée dynamiquement à partir d'un secret ECC.

Étape 1 : Négociation et établissement d'un secret partagé (ECC)

1. Cryptographie à courbes elliptiques

Lors de l'établissement d'une session d'échange, chaque pair (SU / SU-Receiver) négocie un secret partagé via l'échange ECDH (Elliptic Curve Diffie–Hellman). La courbe elliptique secp192r1 est utilisée, offrant un bon compromis entre sécurité et performance, tout en réduisant la charge computationnelle par rapport à l'algorithme RSA utilisé précédemment dans l'approche de l'ECB Optimisé. De plus, la propriété de perfect forward secrecy, illustrée dans la Figure 4.18, garantit que la compromission ultérieure d'une clé privée n'affecte en rien la confidentialité des échanges antérieurs.

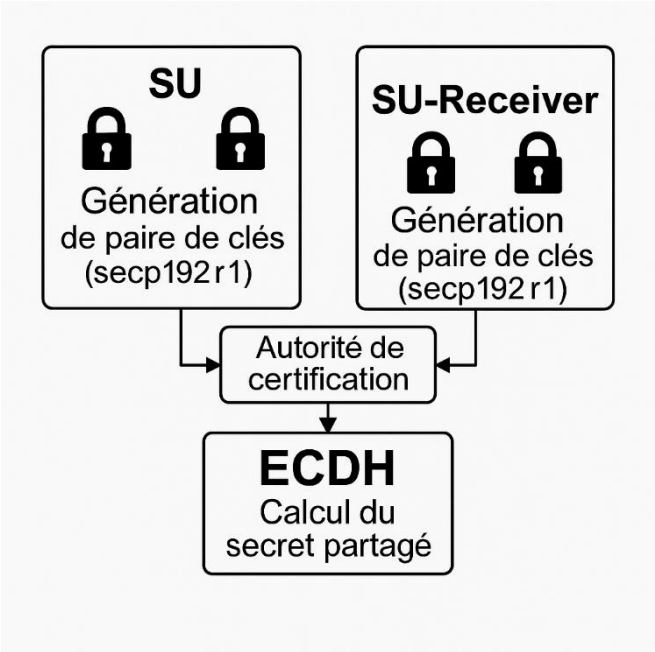


Figure 4.18 : Schéma du calcul du secret partagé.

2. Génération des clés ECC

Chaque agent (SU et SU-Receiver) génère une clé privée par un générateur de nombres aléatoires cryptographiquement sécurisé, puis calcule la clé publique associée par multiplication scalaire sur la courbe.

3. Distribution authentifiée

Les clés publiques sont échangées de manière sécurisée via l'Autorité de Certification intégrée à JADE, assurant leur authenticité et empêchant les attaques de type man-in-the-middle.

4. Échange ECDH et dérivation du secret

Lors de l'échange de clés par ECDH (Elliptic Curve Diffie–Hellman), chaque agent combine sa clé privée avec la clé publique de l'autre partie pour calculer un point partagé P_{ecc} sur la courbe elliptique. Ce point est composé de deux coordonnées (x,y), mais seule l'abscisse x est utilisée pour dériver le secret partagé. L'abscisse x est convertie en une séquence binaire, puis

cette séquence est traitée à l'aide d'une fonction cryptographique (comme SHA-512) pour produire un flux de bits. À partir de ce flux, plusieurs clés AES de tailles différentes (128, 192, et 256 bits) sont dérivées par segmentation du flux binaire, garantissant ainsi des clés indépendantes et sécurisées sans que le secret partagé ne soit jamais transmis directement. Ce processus permet d'obtenir des clés symétriques robustes pour le chiffrement des données, tout en s'appuyant sur la sécurité de l'échange elliptique initial.

5. Renouvellement de session

À chaque nouvelle session, une nouvelle paire de clés ECC est générée, assurant une rotation automatique du secret et renforçant la confidentialité rétroactive des données.

Étape 2 : Dérivation et chiffrement symétrique multi-clé (AES-ECB optimisé)

1. Dérivation des clés AES

À partir du secret ECC, cinq clés AES sont dérivées en extrayant directement des segments disjoints du flux binaire obtenu. Ces clés ont des tailles différentes : la première clé est de 192 bits, la deuxième de 256 bits, la troisième de 128 bits, la quatrième de 256 bits et la cinquième de 192 bits.

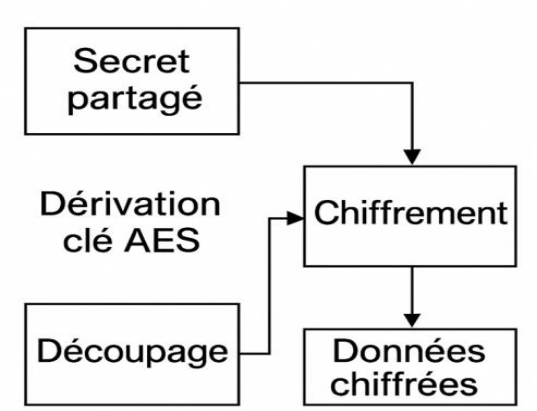


Figure 4.19 : Schéma de la dérivation et du chiffrement symétrique optimisé.

2. Préparation et Encodage des données

Les données sont d'abord divisées en blocs de 16 octets. Si le dernier bloc est incomplet, un bourrage conforme au standard PKCS#7 est appliqué pour garantir que tous les blocs ont la taille appropriée. Ensuite, les données médicales (images, mesures, rapports) sont encodées en Base64, assurant leur transport fiable dans un environnement textuel. Cette étape garantit à la fois la conformité au format de chiffrement et la compatibilité pour le transfert sécurisé des informations.

3. Segmentation et chiffrement parallèle

Le message est découpé en plusieurs segments, chacun étant chiffré indépendamment avec l'une des cinq clés AES dans des threads parallèles pour optimiser le temps de traitement.

4. Mesure QoS

Les performances sont mesurées en temps réel (débit, latence) afin de garantir le respect des contraintes temporelles critiques du domaine médical.

5. Réassemblage du flux chiffré

Les segments chiffrés sont rassemblés dans l'ordre d'origine pour former le message global à transmettre.

Étape 3 : Transport sécurisé via la plateforme multi-agents JADE

1. Encapsulation et Transmission Asynchrone des Données Chiffrées

Le flux chiffré AES est encapsulé dans un message JADE de type INFORM, portant un identifiant explicite "Medical-Data" et une ontologie propre au contexte. Ce message est ensuite routé de manière distribuée et non bloquante vers l'agent destinataire (SU-Receiver) via le système de messagerie de JADE, assurant ainsi une transmission asynchrone et sécurisée des données.

2. Réception et déchiffrement

À l'arrivée, le message est filtré selon son identifiant, puis les données chiffrées sont extraites. Les cinq clés AES sont régénérées à partir du secret ECC partagé, et le déchiffrement est appliqué segment par segment. Enfin, les données sont décodées en Base64 pour reconstituer l'information initiale, comme une image médicale, assurant ainsi la récupération correcte des données transmises.

3. Vérification de réception

Un accusé de réception est envoyé pour confirmer le succès du déchiffrement. En cas d'erreur, un message spécifique est émis pour signaler l'échec de la transaction. La Figure 4.20 présente un exemple de simulation réalisée avec JADE, illustrant l'envoi d'une image médicale du SU vers le SU-Receiver.

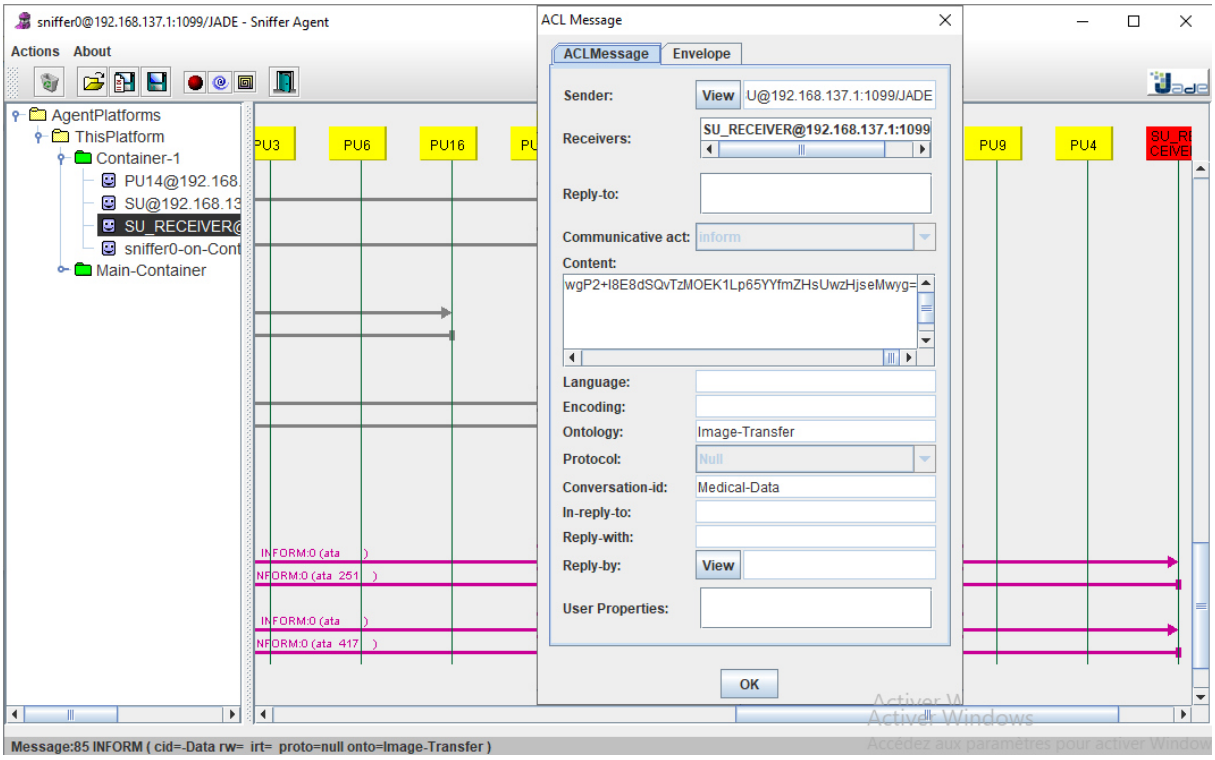


Figure 4.20 : Exemple de simulation avec JADE d'envoi d'image du SU vers SU-Receiver.

4.6 Validation des résultats de simulation

Cette section analyse les résultats de notre simulation, qui évalue l'échange sécurisé d'images médicales entre deux utilisateurs secondaires (SU et SU-Receiver) dans un réseau radio cognitif. L'objectif est de valider l'efficacité du protocole de chiffrement hybride (ECC-AES/ECB optimisé) pour protéger les données sensibles, tout en maintenant une performance optimale. Les résultats mesurent le temps de chiffrement et de déchiffrement, ainsi que l'impact de l'optimisation du mode AES-ECB optimisé sur la latence et le débit de transmission.

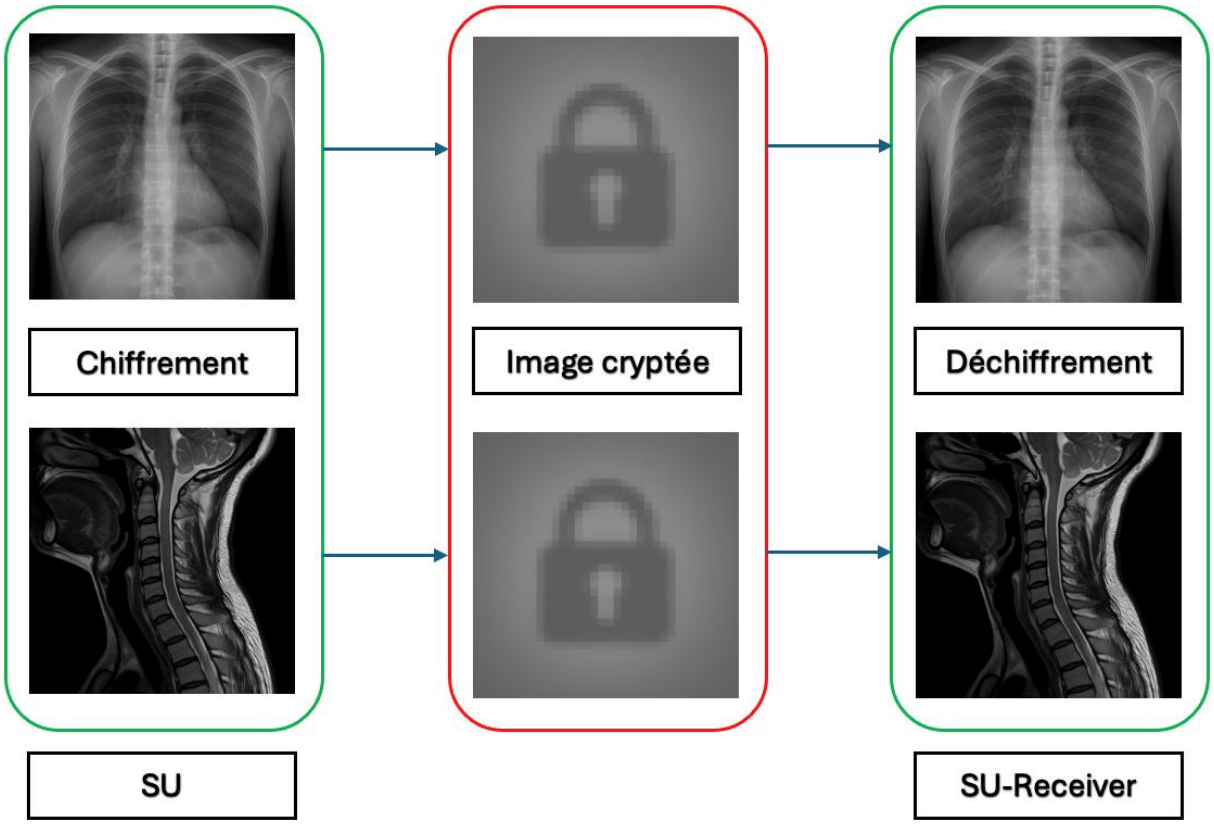


Figure 4.21 : Illustration des échanges de notre scénario.

Figure 4.22 : Console jade avec les logs des échanges des images médicales avec des métriques.

L'utilisateur secondaire (SU) établit une connexion exclusive avec le PU idéal pour louer un spectre de fréquence, mettant ainsi fin à toute communication avec les autres utilisateurs

primaires. Dans ce contexte sécurisé, plusieurs images médicales, de tailles et résolutions variées, sont transmises au SU-Receiver. Cette phase de transfert a permis d'évaluer les performances du système de chiffrement hybride mis en place, en mesurant notamment les temps de chiffrement et de déchiffrement pour chaque fichier. Les résultats obtenus offrent des indicateurs précis sur la réactivité et l'efficacité du protocole dans un environnement de réseau radio cognitif dédié aux applications de santé connectée. Le Tableau 4.2 présente les métriques de performance relevées lors des échanges d'images médicales entre agents via la plateforme JADE. Il met en évidence les temps totaux nécessaires au chiffrement et au déchiffrement (encrypt + decrypt) pour des images de tailles et de résolutions variées.

Tableau 4.2 : Tableau des métriques restitués de la console JADE.

Taille image	Résolution	Temps total (encrypt+decrypt)
669 Ko	1181 × 1873 px	287 ms
18 Ko	88 × 87 px	13 ms
1 871 Ko	4032 × 3024 px	492 ms
1 681 Ko	1024 × 1024 px	285 ms
669 Ko	1181 × 1873 px	166 ms
1 601 Ko	1024 × 1024 px	293 ms

Nous observons que, malgré la grande diversité des fichiers — allant de très petites images de 18 Ko à des fichiers haute résolution dépassant 1 800 Ko — les temps de traitement restent particulièrement faibles, ne dépassant jamais 500 ms. La latence moyenne observée est d'environ **289 ms**. Même pour des fichiers volumineux (> 1 Mo), le temps de traitement complet reste bien en dessous de la seconde, ce qui témoigne de l'efficacité de la parallélisation mise en œuvre avec le mode AES/ECB optimisé. Ces résultats confirment la capacité du système à concilier sécurité renforcée et réactivité, répondant ainsi aux exigences strictes des applications médicales critiques en environnement de réseau radio cognitif.

4.7 Scalabilité

Pour évaluer les performances de notre solution, deux séries de benchmarks ont été réalisées :

- **Benchmark TOPSIS**, mesurant le coût en temps de l'algorithme multicritère selon la taille du problème (nombre d'alternatives (PUs) et de critères (dans notre implémentation on a utilisé 5 critères : technologie, prix, temps, bande passante et canaux).
- **Benchmark End-to-End**, mesurant le temps total d'une session sécurisée (authentification ECC + chiffrement/déchiffrement AES-ECB optimisé) en fonction du volume de données et de la courbe elliptique utilisée.

Matériels et logiciels utilisés :

- CPU : 2,6 GHz Intel Core i7 6 cœurs
- GPU : AMD Radeon Pro 5500M 4 Go (Intel UHD Graphics 630 1536 Mo)
- RAM : 32 Go 2667 MHz DDR4
- OS : MacOs 15.4.1 (24E263)
- Librairie Java utilisée : JMH (version 1.37)
- IDE : IntelliJ IDEA 2025.1

Dans cette section, nous analysons la capacité de notre solution à évoluer selon la taille du problème (nombre d'alternatives (PUs), nombre de critères, volume de données) et à maintenir des performances satisfaisantes. Pour ce faire, nous nous appuyons sur les résultats des benchmarks TOPSIS et End-to-End présentés précédemment, afin de dégager les tendances de croissance du temps de traitement en fonction de la complexité croissante.

Tout d'abord, le Tableau 4.3 récapitule le temps moyen nécessaire à l'exécution de l'algorithme TOPSIS en fonction du nombre d'alternatives (PUs) et de critères :

Tableau 4.3 : Comparaison des résultats du Benchmark de l'algorithme TOPSIS.

Alternatives (Pus)	Critères	Temps moyen (ms/op)
10	3	0,003 ± 0,001
10	5	0,003 ± 0,001
10	7	0,004 ± 0,001
100	3	0,026 ± 0,001
100	5	0,027 ± 0,002
100	7	0,030 ± 0,003
500	3	0,129 ± 0,006
500	5	0,140 ± 0,009
500	7	0,152 ± 0,008

```
Benchmark                        (numAlternatives)  (numCriteria)  Mode  Cnt  Score    Error  Units

TopsisBenchmark.benchTopsis                     10              3  avgt    5  0,003 ±  0,001  ms/op
TopsisBenchmark.benchTopsis                     10              5  avgt    5  0,003 ±  0,001  ms/op
TopsisBenchmark.benchTopsis                     10              7  avgt    5  0,004 ±  0,001  ms/op
TopsisBenchmark.benchTopsis                    100              3  avgt    5  0,026 ±  0,001  ms/op
TopsisBenchmark.benchTopsis                    100              5  avgt    5  0,027 ±  0,002  ms/op
TopsisBenchmark.benchTopsis                    100              7  avgt    5  0,030 ±  0,003  ms/op
TopsisBenchmark.benchTopsis                    500              3  avgt    5  0,129 ±  0,006  ms/op
TopsisBenchmark.benchTopsis                    500              5  avgt    5  0,140 ±  0,009  ms/op
TopsisBenchmark.benchTopsis                    500              7  avgt    5  0,152 ±  0,008  ms/op

                                                                  ms/op : millisecondes par opérations
                                                                  avgt : temps moyen
                                                                  Cnt : nombre d'itérations mesurées
```

Figure 4.23 : Résultat brutes du benchmark du TopsisBenchmark.java.

On constate que le temps de calcul croît presque linéairement avec le nombre d'alternatives (PUs) : il passe de quelques microsecondes pour 10 alternatives (PUs) à environ

0,15 ms pour 500 alternatives. L'impact du nombre de critères reste secondaire, puisque l'augmentation de 3 à 7 critères modifie le temps de l'ordre de 0,001 ms seulement.

Ensuite, le Tableau 4.4 présente les temps moyens de bout en bout (SU – SU-Receiver) pour différents volumes de données et courbes ECC utilisées :

Tableau 4.4 : Comparaison des résultats du Benchmark chiffrement hybride.

Courbe	Taille des données	Temps moyen (ms/op)
secp192r1	1 048 576 octets	1 730 ± 180
secp192r1	10 485 760 octets	28 539 ± 4 876
secp192r1	104 857 600 octets	638 311 ± 112 749
secp256r1	1 048 576 octets	1 881 ± 449
secp256r1	10 485 760 octets	29 083 ± 3 278
secp256r1	104 857 600 octets	676 683 ± 91 523
secp521r1	1 048 576 octets	1 846 ± 140
secp521r1	10 485 760 octets	28 569 ± 2 234
secp521r1	104 857 600 octets	649 079 ± 53 646

```
Benchmark                          (curveName)  (dataSize)  Mode  Cnt    Score     Error  Units

EndToEndBenchmark.benchEndToEnd      secp192r1     1048576  avgt    5    1,730 ±   0,180  ms/op
EndToEndBenchmark.benchEndToEnd      secp192r1    10485760  avgt    5   28,539 ±   4,876  ms/op
EndToEndBenchmark.benchEndToEnd      secp192r1   104857600  avgt    5  638,311 ± 112,749  ms/op
EndToEndBenchmark.benchEndToEnd      secp256r1     1048576  avgt    5    1,881 ±   0,449  ms/op
EndToEndBenchmark.benchEndToEnd      secp256r1    10485760  avgt    5   29,083 ±   3,278  ms/op
EndToEndBenchmark.benchEndToEnd      secp256r1   104857600  avgt    5  676,683 ±  91,523  ms/op
EndToEndBenchmark.benchEndToEnd      secp521r1     1048576  avgt    5    1,846 ±   0,140  ms/op
EndToEndBenchmark.benchEndToEnd      secp521r1    10485760  avgt    5   28,569 ±   2,234  ms/op
EndToEndBenchmark.benchEndToEnd      secp521r1   104857600  avgt    5  649,079 ±  53,646  ms/op

                                                          ms/op : millisecondes par opérations
                                                          avgt : temps moyen
                                                          Cnt : nombre d'itérations mesurées
```

Figure 4.24 : Résultat brutes du benchmark du TopsisBenchmark.java.

Pour les petits volumes (jusqu'à 1 Mo), le surcoût lié à l'échange ECC et au chiffrement hybride reste très faible (1–2 ms). À partir de 10 Mo, le temps de traitement augmente fortement (×15), et devient considérable (> 600 ms) pour 100 Mo, en raison de la partie asymétrique ECC et du traitement parallèle AES/ECB.

En conclusion de cette étude de scalabilité, on peut dire que :

- L'algorithme TOPSIS peut gérer efficacement jusqu'à plusieurs centaines d'alternatives en moins de 0,2 ms par exécution.
- Le pipeline de chiffrement hybride reste parfaitement adapté aux fichiers médicaux de taille modérée (< 5 Mo), avec des délais totaux inférieurs à 150 ms, garantissant ainsi la QoS requise.

- Pour des volumes très importants (> 100 Mo), des optimisations complémentaires (parallélisation GPU, segmentation AES plus fine, ou profilage plus poussé) pourraient être envisagées.

Dans le contexte des réseaux cognitifs dédiés à la santé, ces résultats confirment que notre solution offre déjà un bon compromis entre performance et sécurité, tout en laissant la porte ouverte à de futures améliorations pour des cas d'usage plus exigeants.

4.8 Conclusion

Les simulations réalisées avec la plateforme JADE ont permis de valider l'efficacité des mécanismes de décision multicritère et des stratégies de sécurisation des échanges dans un environnement multi-agents. L'intégration de l'algorithme TOPSIS a optimisé les choix des utilisateurs secondaires en tenant compte de divers critères tels que la fiabilité, le coût, la durée d'allocation, la technologie et la bande passante.

Par ailleurs, l'amélioration du mode de chiffrement symétrique ECB a renforcé la sécurité des données échangées, notamment les données médicales sensibles. La mise en place d'une solution hybride, combinant phases d'authentification, de décision et de confidentialité, a montré son efficacité pour sécuriser les échanges tout en maintenant des performances satisfaisantes.

L'évaluation globale a mis en évidence la capacité du système à détecter et neutraliser les agents malveillants, à mener des négociations spectrales multicritères efficaces, à appliquer des mécanismes de sélection robustes et à garantir l'intégrité des données échangées. Ces résultats confirment la pertinence des approches développées et leur applicabilité dans des environnements distribués complexes, en particulier pour la protection des données médicales.

Conclusion générale

La progression rapide des technologies sans fil et l'essor exponentiel des applications connectées, notamment dans le domaine de la santé, ont profondément transformé les besoins en matière de communication mobile sécurisée. Dans ce contexte, la radio cognitive s'est imposée comme une solution innovante, en introduisant flexibilité et intelligence dans l'utilisation du spectre électromagnétique. Cette capacité d'adaptation dynamique est particulièrement précieuse dans les applications de e-santé, où la fiabilité et la confidentialité des communications sont des exigences fondamentales.

Néanmoins, si la radio cognitive améliore l'efficacité spectrale, elle engendre également de nouveaux défis, notamment en matière de sécurité des données échangées dans des environnements ouverts, dynamiques et distribués. La nature même des réseaux radio cognitifs, caractérisés par leur architecture flexible et leur capacité d'auto-organisation, les rend particulièrement vulnérables aux attaques. La confidentialité, l'intégrité et la disponibilité des données médicales peuvent être compromises si des mécanismes de sécurisation efficaces ne sont pas intégrés. Ce constat a orienté l'objectif principal de cette thèse : proposer des solutions adaptées pour garantir la sécurité des communications médicales dans les réseaux radio cognitifs.

Pour atteindre cet objectif, un travail de recherche structuré a été mené, débutant par une analyse approfondie du contexte technologique. Les bases théoriques des réseaux sans fil, de la radio logicielle et de la radio cognitive ont été détaillées, permettant d'identifier les opportunités et les défis posés par l'intégration de la radio cognitive dans les infrastructures de santé numérique. Un état de l'art rigoureux sur les vulnérabilités, les attaques potentielles et les normes de sécurité en vigueur pour la protection des données médicales a ensuite été établi.

Le cœur de notre contribution scientifique repose sur plusieurs axes complémentaires. Nous avons tout d'abord proposé une approche d'optimisation de la sélection spectrale basée sur la décision multicritère. À travers l'utilisation de l'algorithme TOPSIS, adapté aux environnements cognitifs médicaux, il a été possible d'offrir aux utilisateurs secondaires une capacité de choix intelligent du canal optimal en fonction de plusieurs critères tels que la qualité du signal, la sécurité et les interférences. Ensuite, nous avons procédé à l'optimisation du mode de chiffrement symétrique ECB. Notre version améliorée de ce mode de chiffrement assure une protection renforcée des données médicales sensibles tout en conservant la rapidité et l'efficacité énergétique, des critères essentiels dans des environnements mobiles et contraints.

Parallèlement, nous avons conçu une architecture de sécurisation distribuée reposant sur les systèmes multi-agents. Ce modèle confère au réseau des capacités d'autonomie, de résilience et de prise de décision locale, renforçant ainsi la robustesse du système face aux menaces et

garantissant une meilleure adaptation aux changements de l'environnement radio. Pour valider les propositions théoriques avancées, une implémentation complète sur la plateforme JADE a été réalisée. Des scénarios réalistes simulant des cas d'usage médical ont permis de mesurer l'efficacité des solutions proposées en termes de sécurité, de robustesse, et de qualité de service.

Les résultats obtenus sont très encourageants. Ils montrent une nette amélioration de la sécurisation des communications médicales, de la gestion intelligente des ressources spectrales et de la capacité d'adaptation des utilisateurs cognitifs face à un environnement radio fluctuant. L'approche intégrée combinant optimisation multicritère, chiffrement symétrique optimisé et autonomie des systèmes multi-agents s'est révélée particulièrement efficace pour répondre aux exigences critiques du secteur de la e-santé.

Malgré ces résultats prometteurs, plusieurs pistes d'approfondissement peuvent être envisagées. La validation des solutions proposées sur des plateformes matérielles basées sur des cartes FPGA constitue une étape importante pour évaluer les performances en environnement réel. Il serait également pertinent d'étendre nos travaux aux réseaux de capteurs médicaux, aux réseaux 5G et 6G, où les contraintes de latence et de fiabilité sont encore plus fortes. De plus, l'optimisation avancée des mécanismes de détection du spectre et l'intégration de méthodes d'authentification distribuée, voire de blockchain, pourraient renforcer la sécurité globale du système.

En définitive, cette thèse a permis d'apporter des contributions scientifiques originales à la sécurisation des données médicales dans les réseaux radio cognitifs. Elle illustre que la combinaison judicieuse de l'intelligence artificielle, de la prise de décision multicritère et de l'architecture multi-agents constitue une voie prometteuse pour répondre aux défis des réseaux sans fil de demain. Ce travail, nous l'espérons, servira de socle pour de futures recherches dans un domaine aussi exigeant qu'enthousiasmant, au service d'une santé connectée plus fiable et plus sécurisée.

Liste des publications

Revues internationales

1) Naouel, Seghiri, Baba-ahmed Mohammed Zakarya, Benmammar Badr, Houari Nadhir, Khellafi Mohammed Kamal, and Abdelgherfi Mohammed Ayyoub. "Data security of a cognitive radio network for multicriteria secondary users." Journal of Electrical and Electronics Engineering 15, no. 2 (2022): 82-87.
2) Naouel, Seghiri, Baba-Ahmed Mohammed Zakarya, and Benmammar Badr. "Optimization of the symmetric encryption mode ECB dedicated to securing medical data." Journal of Electrical and Electronics Engineering 14, no. 1 (2021): 48-52.

Conférence internationale

1) Seghiri, N., Baba-Ahmed, M.Z., Benmammar, B., Houari, N. (2022). Optimization of a Multi-criteria Cognitive Radio User Through Autonomous Learning. NISS2021: The 4th International Conference on Networking, Information Systems & Security, KENITRA, Morocco, April 1 - 2, 2021. ACM 2021, ISBN 978-1-4503-8871-9 https://doi.org/10.1007/978-981-16-3637-0_9

Conférence nationale

1) Seghiri Naouel, Mohammed Belhadj Khouloud, Baba-Ahmed Mohammed Zakarya, and Ziani-Kerarti Djalal, Performance Optimization of Cognitive Radio Networks Using Reconfigurable Printed Antennas. Conférence Nationale sur les Télécommunications et ses Applications (CNTA'21). Ain-Témouchent, Algérie, December 20-21, 2021

Références bibliographiques

Chapitre 1

[1] Burbank, Jack L., et al. *Wireless networking : Understanding internetworking challenges*. John Wiley & Sons, 2013.

[2] Islam, Mohaiminul, and Shangzhu Jin. "An overview research on wireless communication network." *Networks* 5.1 2019 : 19-28.

[3] Chin, Jeannette, Vic Callaghan, and Somaya Ben Allouch. "The Internet-of-Things: Reflections on the past, present and future from a user-centered and smart environment perspective." *Journal of Ambient Intelligence and Smart Environments* 11.1 (2019) : 45-69.

[4] Saeed, Nasir, et al. "When wireless communication responds to COVID-19 : Combating the pandemic and saving the economy." *Frontiers in communications and networks* 1 (2020) : 566853.

[5] Koripi, Malyadri. "A review on secure communications and wireless personalarea networks (WPAN)." *Wutan Huatan Jisuan Jishu* 17 (2021).

[6] Qu, Yating, et al. "A survey of routing protocols in WBAN for healthcare applications." *Sensors* 19.7 (2019) : 1638.

[7] Sable, Adhitya. "Comparative Study on IEEE Standard of WPAN 802.15. 1/3/4." *International Journal for Research in Emerging Science and Technology* 1.1 (2014).

[8] Mitola, Joseph. "The software radio architecture." *IEEE Communications magazine* 33.5 (1995) : 26-38.

[9] Benmammar, Badr, and Asma Amraoui. "Radio resource allocation and dynamic spectrum access." ISTE, (2013)

[10] Michaël Nicolas. "Radio logicielle : analyse d'architectures matérielles et outils informatiques." Electronique. 2011. dumas-00693426

[11] Kenington, Peter. "*RF and baseband techniques for software defined radio*. " Artech, 2005.

[12] Barrandon, Ludovic. *Synthèse architecturale analogique/numérique appliquée aux systèmes sur puce dans un contexte radio logicielle*. Diss. Université Rennes 1, 2005.

[13] J III, M. I. T. O. L. A. "Cognitive radio: an integrated agent architecture for software defined radio." *Ph. D. Thesis, KTH Royal Inst. Technology* (2000).

[14] Harada, Hiroshi, et al. "A software defined cognitive radio system : cognitive wireless cloud." *IEEE GLOBECOM 2007-IEEE Global Telecommunications Conference*. IEEE, 2007.

[15] "2025's Top Trends : Cognitive Radios Deftly Park Signals." *Microwaves & RF*, 14 Nov. 2024, https://www.mwrf.com/technologies/embedded/systems/article/55245485/microwaves-rf-2025s-top-trends-cognitive-radios-deftly-park-signals. Consulté le 14 novembre 2024.

[16] Hafez, Dina Tarek Mohamed Ibrahim. *Development of Spectrum Sharing Protocol for Cognitive Radio Internet of Things*. Diss. Université d'Avignon ; American university in Cairo, 2020.

[17] Hilal, Waleed, S. Andrew Gadsden, and John Yawney. "Cognitive dynamic systems : A review of theory, applications, and recent advances." *Proceedings of the IEEE* 111.6 (2023) : 575-622.

[18] Akyildiz, Ian F., Won-Yeol Lee, and Kaushik R. Chowdhury. "CRAHNs: Cognitive radio ad hoc networks." *AD hoc networks* 7.5 (2009) : 810-836.

[19] Gayathri, N., et al. "An analysis of network security attacks and their mitigation for cognitive radio communication." *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*. Vol. 1. IEEE, 2023.

[20] Agrawal, Sumit Kumar, Abhay Samant, and Sandeep Kumar Yadav. "Spectrum sensing in cognitive radio networks and metacognition for dynamic spectrum sharing between radar and communication system : A review." *Physical Communication* 52 (2022) : 101673.

[21] Moumena, Ahmed. "Detection rapide et large-bande de brouilleurs au niveau de la radio cognitive." (2016).

[22] Amraoui, Asma. *Vers une architecture Multi-agents pour la Radio Cognitive opportuniste*. Diss. Université de Tlemcen-Abou Bekr Belkaid, 2015.

[23] Almasoud, Abdullah M., and Ahmed E. Kamal. "Robust provisioning of multicast sessions in cognitive radio networks." *2014 International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2014.

[24] Akhtar, Ahmad Naeem, Fahim Arif, and Adil Masood Siddique. "Spectrum Decision Framework to Support Cognitive." *Cognitive Radio in 4G/5G Wireless Communication Systems* (2018) : 73.

[25] Yawada, Prince Semba, and An Jian Wei. "Cyclostationary Detection Based on Non-cooperative spectrum sensing in cognitive radio network." *2016 IEEE international conference on cyber technology in automation, control, and intelligent systems (CYBER)*. IEEE, 2016.

[26] Zhao, Jianli, and Jinsha Yuan. "An improved centralized cognitive radio network spectrum allocation algorithm based on the allocation sequence." *International Journal of Distributed Sensor Networks* 9.10 (2013): 875342.

[27] Ramzan, Muhammad Rashid, et al. "Multi-objective optimization for spectrum sharing in cognitive radio networks : A review." *Pervasive and Mobile Computing* 41 (2017) : 106-131.

[28] Qin, Yongrui, et al. "When things matter: A survey on data-centric internet of things." *Journal of Network and Computer Applications* 64 (2016) : 137-153.

[29] Kumar, Krishan, Arun Prakash, and Rajeev Tripathi. "A spectrum handoff scheme for optimal network selection in cognitive radio vehicular networks : A game theoretic auction theory approach." *Physical Communication* 24 (2017) : 19-33.

[30] Wajhal, Gaurav, et al. "Proactive handoff of secondary user in cognitive radio network using machine learning techniques." *Proceedings of international conference on intelligent computing, information and control systems : ICICCS 2020*. Springer Singapore, 2021.

[31] Khattab, Ahmed, et al. "Cognitive radio networking preliminaries." *Cognitive Radio Networks : From Theory to Practice* (2013): 11-20.

[32] Sultana, Rogina, et al. "A Comprehensive Review on the Cognitive Radio for the Implementation in 5G Wireless Communication for the Development of Healthcare." *Industry 5.0 for Smart Healthcare Technologies* (2024) : 107-117.

[33] Lydia, T. A. Z. I. *Le rôle du digital dans l'amélioration de la qualité de service santé*. Diss. École supérieure de gestion et d'économie numérique, 2023.

[34] Agence du Numérique en Santé, *Les 50 ans d'histoire de la e-santé*. [En ligne]. Disponible sur : https://esante.gouv.fr/les-50-ans-dhistoire-de-la-e-sante . Consulté le : 04 janvier 2025.

[35] Lemelle, Séverine. "Conférence 3-La révolution technologique des objets connectés et son impact sur la prise en charge des maladies rares." (2016) : 40-41.

[36] Siriwardhana, Yushan, et al. "The role of 5G for digital healthcare against COVID-19 pandemic: Opportunities and challenges." *Ict Express* 7.2 (2021) : 244-252.

[37] Nankya, Mary, et al. "Security and privacy in E-health systems: a review of AI and machine learning techniques." *IEEE Access* (2024).

[38] Bennaceur, Jihen, Hanen Idoudi, and Leila Azouz Saidane. "Toward Trustworthy Cognitive Radio-Based Internet of Medical Things." *Smart Systems for E-Health : WBAN Technologies, Security and Applications* (2021): 135-160.

[39] Nasralla, Moustafa M., et al. "Exploring the role of 6G technology in enhancing quality of experience for m-health multimedia applications : a comprehensive survey." *Sensors* 23.13 (2023): 5882.

[40] Ouattara, Dramane. "*Apport des réseaux intelligents aux usages et pratiques en e-santé : Une architecture flexible basée sur la technologie radio cognitive pour un suivi efficace et temps réel des patients*." Diss. Université de Bordeaux, 2014.

Chapitre 2

[1] Dey, Soubhik Kumar, et Tarak Nandy. "A Symmetric Key Cryptographic. " *IPASJ International Journal of Computer Science (IIJCS)*, vol. 2, no 1, janvier 2014.

[2] Sood, Roopali, and Harpreet Kaur. "A literature review on rsa, des and aes encryption algorithms." *Emerging Trends in Engineering and Management* (2023): 57-63.

[3] Rivest, Ronald L., Adi Shamir, and Leonard M. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." *Secure Communications and Asymmetric Cryptosystems*, 2019, pp. 217–239.

[4] Yan, Yuhan. "The overview of elliptic curve cryptography (ECC)." *Journal of Physics: Conference Series*. Vol. 2386. No. 1. IOP Publishing, 2022

[5] Zhang, Qixin. "An overview and analysis of hybrid encryption: the combination of symmetric encryption and asymmetric encryption." 2021 2nd international conference on computing and data science (CDS). IEEE, 2021.

[6] Almuhammadi, Sultan, and Ibraheem Al-Hejri. "A comparative analysis of AES common modes of operation." *2017 IEEE 30th Canadian conference on electrical and computer engineering (CCECE)*. IEEE, 2017.

[7] Hameed, Mustafa Emad, et al. "Comparative study of several operation modes of AES algorithm for encryption ECG biomedical signal." *International Journal of Electrical and Computer Engineering* 9.6 (2019) : 4850.

[8] Trubin, I. S. "Security threats in mobile cognitive radio networks." *2018 IEEE East-West Design & Test Symposium (EWDTS)*. IEEE, 2018.

[9] Raj, Shekhar, and O. P. Sahu. "Security Threats and Challenges on Different Protocol Layers in Cognitive Radio Networks : An Overview." *2017 International Conference on Innovations in Control, Communication and Information Systems (ICICCI)*. IEEE, 2017.

[10] Olaleru, Grace Idowu, et al. "A Systematic Review of the Primary User Emulation Attack in the Cognitive Radio Network." *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)*. IEEE, 2024.

[11] Gupta, Ishu, and O. P. Sahu. "An Overview of primary user emulation attack in cognitive radio networks." *2018 Second International Conference on Computing Methodologies and Communication (ICCMC)*. IEEE, 2018.

[12] Khaliq, Saim Bin Abdul, et al. "Defence against PUE attacks in ad hoc cognitive radio networks: a mean field game approach." *Telecommunication Systems* 70 (2019) : 123-140.

[13] Ezhilarasi, I. Evelyn, J. Christopher Clement, and Joseph M. Arul. "A survey on cognitive radio network attack mitigation using machine learning and blockchain." *EURASIP Journal on Wireless Communications and Networking* 2023.1 (2023): 98.

[14] Sohu, Izhar Ahmed, et al. "Analogous study of security threats in cognitive radio." *2019 2nd International conference on computing, mathematics and engineering technologies (iCoMET)*. IEEE, 2019.

[15] Slimeni, Feten, et al. "Jamming mitigation in cognitive radio networks using a modified Q-learning algorithm." *2015 International Conference on Military Communications and Information Systems (ICMCIS)*. IEEE, 2015.

[16] Feng, Guangsheng, et al. "A differential game based approach against objective function attack in cognitive networks." *Chinese Journal of Electronics* 27.4 (2018) : 879-888.

[17] Chouhan, Ankit, et al. "Defending against Byzantine attacks in CRNs: PCA-based malicious user detection and weighted cooperative spectrum sensing." *IEEE Wireless Communications Letters* (2024).

[18] Jasim, Doaa K., and Sattar B. Sadkhan. "Cognitive radio network: Security and reliability trade-off-status, challenges, and future trend." *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*. IEEE, 2021.

[19] Hamood, Ameer Sameer, and Sattar B. Sadkhan. "Cognitive radio network security status and challenges." *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*. IEEE, 2017.

[20] Bouabdellah, Mounia, et al. "Network layer attacks and countermeasures in cognitive radio networks: A survey." *Journal of information security and applications* 38 (2018): 40-49.

[21] Bhattacharjee, Suchismita, Roshni Rajkumari, and Ningrinla Marchang. "Cognitive radio networks security threats and attacks: a review." *International Journal of Computer Applications* 975 (2014): 8887.

[22] Zeng, Fanzi, et al. "A trust-based cooperative spectrum sensing scheme against SSDF attack in CRNs." *2016 IEEE Trustcom/BigDataSE/ISPA*. IEEE, 2016.

[23] Ding, Lei, et al. "Securing cognitive radio networks with distributed trust management against belief manipulation attacks." *2015 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2015.

[24] Mahmoudi, Mohsen, Karim Faez, and Abdorasoul Ghasemi. "Defense against primary user emulation attackers based on adaptive Bayesian learning automata in cognitive radio networks." *Ad Hoc Networks* 102 (2020): 102147.

[25] Wang, Bo, and al. "Jamming Mitigation in Cognitive Radio Networks." *IEEE Network*, vol. 27, no. 3, pp. 10–15. IEEE, 2013.

[26] Cai, Yifeng, et al. "Joint reactive jammer detection and localization in an enterprise WiFi network." *Computer Networks* 57.18 (2013): 3799-3811.

[27] Bhunia, Suman, et al. "CR-Honeynet: A cognitive radio learning and decoy-based sustenance mechanism to avoid intelligent jammer." *IEEE Transactions on Cognitive Communications and Networking* 4.3 (2018): 567-581.

[28] Jayaweera, Sudharman K. "*Signal processing for cognitive radios*." John Wiley & Sons, 2014.

[29] Lv, Lu, Jian Chen, and Qiang Ni. "Cooperative non-orthogonal multiple access in cognitive radio." *IEEE Communications Letters* 20.10 (2016): 2059-2062.

[30] Alrjoob, Ayat M., et al. "Securing Primary Users in IoT 5G Cognitive Radio Networks." *2024 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. IEEE, 2024.

[31] Shu, Zhihui, Yi Qian, and Song Ci. "On physical layer security for cognitive radio networks." *IEEE Network* 27.3 (2013): 28-33.

[32] Nguyen, Van-Dinh, Tiep M. Hoang, and Oh-Soon Shin. "Secrecy capacity of the primary system in a cognitive radio network." *IEEE Transactions on Vehicular Technology* 64.8 (2014): 3834-3843.

[33] Yan, Shihao, et al. "Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation." *IEEE Transactions on wireless Communications* 15.12 (2016): 8286-8297.

[34] Hu, Jinsong, et al. "Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays." *IEEE Access* 5 (2017): 1658-1667.

[35] Hou, Ling, et al. "Using trust management to defend against routing disruption attacks for cognitive radio networks." *2016 IEEE International Conference on Consumer Electronics-China (ICCE-China)*. IEEE, 2016.

[36] Priyadharshini, R. Ahila, and K. Uma Haimavathi. "Detection of attacks and countermeasures in cognitive radio network." *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE, 2016.

[37] Weinmann, Ralf-Philipp. "Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks." *WOOT*. 2012.

[38] G. Beniamini; "Over The Air : Exploiting Broadcoms Wi-Fi Stack (Part 1)." *Google Project Zero*, 4 avril 2017, https://googleprojectzero.blogspot.com/2017/04/over-air-exploiting-broadcoms-wi-fi_4.html. Consulté le 5 janvier 2025.

[39] Artenstein, Nitay. "Broadpwn: Remotely compromising Android and iOS via a bug in Broadcom's Wi-Fi chipsets." *Exodus Intelligence Blog*, 26 juillet 2017, https://blog.exodusintel.com/2017/07/26/broadpwn/. Consulté le 5 janvier 2025.

[40] Ahuja, Pooja, Preeti Sethi, and Naresh Chauhan. "A comprehensive survey of security threats, detection, countermeasures, and future directions for physical and network layers in cognitive radio networks." *Multimedia Tools and Applications* 83.11 (2024): 32715-32738.

[41] Ezhilarasi, I. Evelyn, J. Christopher Clement, and Joseph M. Arul. "A survey on cognitive radio network attack mitigation using machine learning and blockchain." *EURASIP Journal on Wireless Communications and Networking* 2023.1 (2023): 98.

[42] Qureshi, Muhammad Anjum, and Cem Tekin. "Rate and channel adaptation in cognitive radio networks under time-varying constraints." *IEEE Communications Letters* 24.12 (2020): 2979-2983.

[43] Wang, Tongxiang, et al. "Adaptive jammer localization in wireless networks." *Computer Networks* 141 (2018): 17-30.

[44] Li, Xuran, Hong-Ning Dai, Qubeijian Wang, Muhammad Imran, Dengwang Li, and Muhammad Ali Imran. "Securing internet of medical things with friendly-jamming schemes." Computer Communications (2020).

[45] Centers for Medicare & Medicaid Services. "Health Insurance Portability and Accountability Act (HIPAA)". *CMS.gov*, 2020, https://www.cms.gov. Consulté le 25 janvier 2025.

[46] General Data Protection Regulation (GDPR) ». *GDPR.eu*, 2018, https://gdpr.eu. Consulté le 25 janvier 2025

[47] ISO. *ISO/IEC 27799 : Health Informatics — Information Security Management in Health.* Genève, International Organization for Standardization, 2016.

[48] U.S. Department of Health & Human Services. « Health Information Privacy ». *HHS.gov*, 2021, https://www.hhs.gov/hipaa/index.html. Consulté le 25 janvier 2025.

[49] National Institute of Standards and Technology (NIST). *Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53).* Version 5, 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. Consulté le 25 janvier 2025.

Chapitre 3

[1] Vercouter, Laurent, and Gauthier Picard. "Actes des 23es Journées Francophones sur les Systèmes Multi-Agents (JFSMA 2015)." *Journées Francophones sur les Systèmes Multi-Agents*. Cépaduès, 2015.

[2] Prema, S., et al. "Cognitive Radio Networks: An AI Enabled Approach." *2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*. IEEE, 2024.

[3] Demazeau, Yves. "From interactions to collective behaviour in agent-based systems." *European Conference on Cognitive Science*. Vol. 95. 1995.

[4] Tan, Xiang, et al. "Cooperative multi-agent reinforcement-learning-based distributed dynamic spectrum access in cognitive radio networks." *IEEE Internet of Things Journal* 9.19 (2022): 19477-19488.

[5] El Ghouch Nihad, Kouissi Mohamed, and En-Naimi El Mokhtar. "Designing and modeling of a multi-agent adaptive learning system (MAALS) using incremental hybrid case-based reasoning (IHCBR)." *International Journal of Electrical and Computer Engineering (IJECE)* 10.2 (2020): 1980-1992.

[6] Red'ko, Vladimir G., and Zarema B. Sokhova. "Model of an autonomous agent forming its own simple knowledge base." *Procedia Computer Science* 213 (2022): 477-485.

[7] Nguyen, Thuy Ngoc, Duy Nhat Phan, and Cleotilde Gonzalez. "Learning in cooperative multiagent systems using cognitive and machine models." *ACM Transactions on Autonomous and Adaptive Systems* 18.4 (2023): 1-22.

[8] Pore, Ameya. *Reactive Reinforcement learning for Robotic Manipulation*. Diss. 2019.

[9] Amraoui, Asma. "*Vers une architecture Multi-agents pour la Radio Cognitive opportuniste*. " Diss. Université de Tlemcen-Abou Bekr Belkaid, 2015.

[10] De Silva, Lavindra, Felipe Rech Meneguzzi, and Brian Logan. "BDI agent architectures: A survey." *Proceedings of the 29th International Joint Conference on Artificial Intelligence (IJCAI), 2020, Japão.*. 2020.

[11] Sankhyadhar, Shubhangi, and Mohit Pandey. "Test Beds for Distributed AI Research." *Distributed Artificial Intelligence*. CRC Press, 2020. 179-194.

[12] Russell, Stuart J., and Peter Norvig. "*Artificial intelligence: a modern approach*. " pearson, 2016.

[13] Soon, Gan Kim, et al. "A review on agent communication language." *Computational Science and Technology: 5th ICCST 2018, Kota Kinabalu, Malaysia, 29-30 August 2018* (2019): 481-491.

[14] Marcantoni, Alessandro. "*Visual Programming Paradigm for Organizations in Multi-Agent Systems*. " Laurea magistrale, Università di Bologna, Corso di Studio in Ingegneria e Scienze Informatiche [LM-DM270] - Cesena, 2023. Disponible à : https://amslaurea.unibo.it/id/eprint/28105.

[15] Azhar, Nayli A., Nurul AM Radzi, and Wan Siti Halimatul Munirah Wan Ahmad. "Multi-criteria decision making: a systematic review." *Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering)* 14.8 (2021): 779-801.

[16] Kulakowski, Konrad. *Understanding the analytic hierarchy process*. CRC Press, 2020.

[17] Penadés-Plà, Vicent, et al. "A review of multi-criteria decision-making methods applied to the sustainable bridge design." *Sustainability* 8.12 (2016): 1295.

[18] Azhar, Nayli A., Nurul AM Radzi, and Wan Siti Halimatul Munirah Wan Ahmad. "Multi-criteria decision making: a systematic review." *Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering)* 14.8 (2021): 779-801.

[19] Agrebi, Maroi, Mourad Abed, and Mohamed Nazih Omri. "ELECTRE I Based Relevance Decision-Makers Feedback to the Location Selection of Distribution Centers." *Journal of Advanced Transportation* 2017.1 (2017): 7131094.

[20] Hodosi, Gergely, Edit Sule, and Tamas Bodis. "Multi-criteria decision making: A comparative analysis." *Economic and Social Development (Book of Proceedings), 103rd International Scientific Conference on Economic and Social Development*. 2023.

[21] Bhatia, Jitesh Kumar, and Praveen Mittal. "Trusted Channel Selection in Cognitive Radio Network using VIKOR method." *2023 1st International Conference on Cognitive Computing and Engineering Education (ICCCEE)*. IEEE, 2023.

[22] Hwang, Ching-Lai, and K. Yoon. "*Multiple Objective Decision Making: Methods and Applications*. " Springer-Verlag, 1981, pp. 58–191.

[23] Balioti, Vasiliki, Christos Tzimopoulos, and Christos Evangelides. "Multi-criteria decision making using TOPSIS method under fuzzy environment. Application in spillway selection." *Proceedings*. Vol. 2. No. 11. MDPI, 2018.

[24] Penadés-Plà, Vicent, et al. "A review of multi-criteria decision-making methods applied to the sustainable bridge design." *Sustainability* 8.12 (2016): 1295.

[25] Villacreses, Geovanna, et al. "Wind farms suitability location using geographical information system (GIS), based on multi-criteria decision making (MCDM) methods: The case of continental Ecuador." *Renewable energy* 109 (2017): 275-286.

[26] Beg, Ismat, and Tabasam Rashid. "Multi-criteria trapezoidal valued intuitionistic fuzzy decision making with Choquet integral based TOPSIS." *Opsearch* 51 (2014): 98-129.

[27] Tarigan, Philipus Tarigan. "Use of Electronic Code Book (Ecb) Algorithm in File Security." *Jurnal Info Sains : Informatika dan Sains* 10.1 (2020) : 19-23.

Chapitre 4

[1] Wrona, Zofia, et al. "Overview of software agent platforms available in 2023." *Information* 14.6 (2023): 348.

[2] Bergenti, Federico, et al. "The first twenty years of agent-based software development with JADE." *Autonomous Agents and Multi-Agent Systems* 34 (2020): 1-19.

[3] Abbas, Hosny, Samir Shaheen, and Mohammed Amin. "Providing a transparent dynamic organization technique for efficient aggregation of multiple JADE agent platforms." *2018 International Conference on Innovative Trends in Computer Engineering (ITCE)*. IEEE, 2018.

[4] Bellifemine, Fabio, Agostino Poggi, and Giovanni Rimassa. "JADE–A FIPA-compliant agent framework." *Proceedings of PAAM*. Vol. 99. No. 97-108. 1999.

[5] Szigeti, Tim, et al. *End-to-End QoS network design: Quality of Service for rich-media & cloud networks*. Cisco press, 2013.

[6] Baba-Ahmed, M. Z., et al. "Self-management of autonomous agents dedicated to cognitive radio networks." *International Conference in Artificial Intelligence in Renewable Energetic Systems*. Cham: Springer International Publishing, 2019.